Analysis of quantum error-correcting codes: symplectic lattice codes and toric codes

Thesis by
James William Harrington

Advisor
John Preskill

In Partial Fulfillment of the Requirements
for the Degree of
Doctor of Philosophy

California Institute of Technology
Pasadena, California

2004

(Defended May 17, 2004)

Acknowledgements

I can do all things through Christ, who strengthens me. Phillipians 4:13 (NKJV)

I wish to acknowledge first of all my parents, brothers, and grandmother for all of their love, prayers, and support.

Thanks to my advisor, John Preskill, for his generous support of my graduate studies, for introducing me to the studies of quantum error correction, and for encouraging me to pursue challenging questions in this fascinating field.

Over the years I have benefited greatly from stimulating discussions on the subject of quantum information with Anura Abeyesinge, Charlene Ahn, Dave Bacon, Dave Beckman, Charlie Bennett, Sergey Bravyi, Carl Caves, Isaac Chenchiah, Keng-Hwee Chiam, Richard Cleve, John Cortese, Sumit Daftuar, Ivan Deutsch, Andrew Doherty, Jon Dowling, Bryan Eastin, Steven van Enk, Chris Fuchs, Shohini Ghose, Daniel Gottesman, Ted Harder, Patrick Hayden, Richard Hughes, Deborah Jackson, Alexei Kitaev, Greg Kuperberg, Andrew Landahl, Chris Lee, Debbie Leung, Carlos Mochon, Michael Nielsen, Smith Nielsen, Harold Ollivier, Tobias Osborne, Michael Postol, Philippe Pouliot, Marco Pravia, John Preskill, Eric Rains, Robert Raussendorf, Joe Renes, Deborah Santamore, Yaoyun Shi, Peter Shor, Marcus Silva, Graeme Smith, Jennifer Sokol, Federico Spedalieri, Rene Stock, Francis Su, Jacob Taylor, Ben Toner, Guifre Vidal, and Mas Yamada.

Thanks to Chip Kent for running some of my longer numerical simulations on a computer system in the High Performance Computing Environments Group (CCN-8) at Los Alamos National Laboratory. Some simulations were also run on the Pentium Pro based Beowulf Cluster (naegling) computer system operated by the Caltech CACR.

I am very grateful for helpful comments from Charlene Ahn, Chris Lee, and Graeme Smith on draft versions of my thesis chapters.

A special thanks to Francis Su, Winnie Wang, Dawn Yang, and Esther Yong for working alongside me while I was writing parts of this thesis. Also, thanks to Robert Dirks for being such a patient and fun bridge partner to play with this

past year, which provided a welcome break from work.

I would like to acknowledge some of the teachers that have encouraged me and helped lead me to this point: David Crane, Fred DiCesare, Maureen Dinero, Autumn Finlan, Dan Gauthier, Linda Hagreen, Calvin Howell, David Kraines, Jane LaVoie, Harold Layton, Claude Meyers, Mary Champagne-Myers, Kate Ross, Anthony Ruggieri, David Schaeffer, Roxanne Springer, and Stephanos Venakides.

Additionally, I want to acknowledge the sharpening role of the accountability partners in my life over the past few years: James Bowen, Isaac Chenchiah, Brenton Chinn, Gene Chu, Tony Chu, Stephan Ichiriu, Frank Reyes, and Kenji Shimibukuro. I also appreciate my brothers and sisters in the Sedaqah groups I have belonged to at Evergreen, as well as my fellow grad students in the Caltech Christian Fellowship and UCLA Graduate Christian Fellowship.

Soli Deo Gloria.

Analysis of quantum error-correcting codes:
symplectic lattice codes and toric codes

by

James William Harrington

In Partial Fulfillment of the
Requirements for the Degree of
Doctor of Philosophy

Abstract

Quantum information theory is concerned with identifying how quantum mechanical resources (such as entangled quantum states) can be utilized for a number of information processing tasks, including data storage, computation, communication, and cryptography. Efficient quantum algorithms and protocols have been developed for performing some tasks (*e.g.*, factoring large numbers, securely communicating over a public channel, and simulating quantum mechanical systems) that appear to be very difficult with just classical resources. In addition to identifying the separation between classical and quantum computational power, much of the theoretical focus in this field over the last decade has been concerned with finding novel ways of encoding quantum information that are robust against errors, which is an important step toward building practical quantum information processing devices.

In this thesis I present some results on the quantum error-correcting properties of oscillator codes (also described as symplectic lattice codes) and toric codes. Any harmonic oscillator system (such as a mode of light) can be encoded with quantum information via symplectic lattice codes that are robust against shifts in the system's continuous quantum variables. I show the existence of lattice codes whose achievable rates match the one-shot coherent information over the Gaussian quantum channel. Also, I construct a family of symplectic self-dual lattices and

search for optimal encodings of quantum information distributed between several oscillators.

Toric codes provide encodings of quantum information into two-dimensional spin lattices that are robust against local clusters of errors and which require only local quantum operations for error correction. Numerical simulations of this system under various error models provide a calculation of the accuracy threshold for quantum memory using toric codes, which can be related to phase transitions in certain condensed matter models. I also present a local classical processing scheme for correcting errors on toric codes, which demonstrates that quantum information can be maintained in two dimensions by purely local (quantum and classical) resources.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Overview

This thesis analyzes the error-correcting properties of symplectic lattice codes and toric codes. Section 1.2 provides a brief introduction to quantum error correction and its terminology. Section 1.3 introduces some key features of lattices.

Chapters 2 and 3 are concerned with oscillator codes (also described as symplectic lattice codes), which encode the states of a finite-dimensional quantum system into a continuous variable system, such as a mode of light. These codes are analyzed under a restricted class of the Gaussian quantum channel, where the continuous variables describing the system of oscillators each receive a random kick governed by a Gaussian distribution. Chapter 2 calculates achievable rates over this channel, based on the existence of symplectic lattices with special properties in a large number of dimensions. Chapter 3 analyzes the error-correcting properties of specific low-dimensional symplectic lattice codes.

Chapters 4 and 5 are concerned with toric codes, which encode quantum information in a topological manner on two-dimensional surfaces, so that they are robust against local clusters of errors. Chapter 4 relates the accuracy threshold of toric codes to the phase transitions of condensed matter systems (namely the two-dimensional random-bond Ising model and the three-dimensional random-

plaquette gauge model). The threshold for quantum memory is calculated numerically by running Monte Carlo simulations. Chapter 5 restricts the error processing to purely local communication and control and demonstrates numerically and analytically that an accuracy threshold still exists for toric codes. Thus, it is possible to maintain quantum information in a two-dimensional system (such as a lattice of spins) with only local controls.

Chapters 2 and 4 have previously been published [40, 84]. I have updated the numerics in Section 4.5 and revised the conclusions in Sections 2.9 and 4.6.

Appendix A contains my rough translation of a paper (written in French) on symplectic lattices by Christophe Bavard [8]. The mathematical community has begun researching symplectic lattices over the last decade or so, which interestingly coincides with the development of quantum error-correcting codes, although these two forays of study have mostly been unconnected. Bavard is one of the experts in this field, and it was very helpful to have my numerical search in the space of symplectic lattices be confirmed by his work.

1.2 Introduction to quantum error correction

Quantum information processing promises the ability to perform certain tasks that are hard to achieve classically, such as simulating quantum systems [30, 54], factoring large numbers [78], or securely distributing private shared keys for encryption [10, 79] (without restricting the computational power of an adversary). To carry out these tasks, we need a quantum system which can be evolved in a controlled manner while not interacting very much with its environment. Fault-tolerant quantum computation is concerned with designing quantum circuits out of imperfect components in such a way that when errors inevitably occur, their propagation is controlled and they are removed in a timely manner, provided that the underlying errors are restricted to some typical set of errors and that the error rate is below the *accuracy threshold* of the system. If the error correction can be done by purely

local controls (in terms of measuring and processing error syndromes), then such a system should be scalable to handle large tasks.

Quantum bits (called *qubits*) must be protected against not only bit flips (as in classical systems) but also phase flips. Qubits can be expressed as a unit vector in $\mathbb{C}^2$, when in a pure state (a state of minimal entropy). A mixed state is expressed as a 2×2 density matrix, which has unit trace and nonnegative eigenvalues. We can define the states of a qubit in the standard basis $|0\rangle = \left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)$ and $|1\rangle = \left(\begin{smallmatrix}0\\1\end{smallmatrix}\right)$.

The Pauli matrices form a basis of unitary operators acting on a qubit and are defined in the standard basis by

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

We observe that $X|0\rangle = |1\rangle$ and $X|1\rangle = |0\rangle$, so we can interpret X as a bit flip operator. Also, $Z|0\rangle = |0\rangle$ and $Z|1\rangle = -|1\rangle$, so we can interpret Z as a phase flip operator. Since $Y = iXZ$, we can interpret Y as both a phase flip and a bit flip. The Pauli group P_n consists of tensor products of Pauli operators and provides a basis for unitary operators acting on a system of n qubits:

$$P_n = \{1, i, -1, -i\} \times \{I, X, Y, Z\}^{\otimes n}$$

All of these definitions can be generalized to d-dimensional quantum systems, which we refer to as *qudits*. Let $\{|0\rangle, |1\rangle, \ldots, |d-1\rangle\}$ be a basis for a qudit system. Pure states are unit vectors in $\mathbb{C}^d$, and Pauli operators can be expressed in the form $Z^a X^b$ for some $a, b \in \mathbb{Z}$, where we define $X|j\rangle = |(j+1) \mod d\rangle$ and $Z|j\rangle = \omega^j |j\rangle$ with $\omega = \exp\{2i\pi/d\}$ (a dth root of unity). Note that $X^d = I = Z^d$, so there are d^2 distinct Pauli operators of the form $Z^a X^b$. The Pauli group is similarly defined as tensor products of operators of the form $Z^a X^b$, along with possible phases. We can define the *weight* of a Pauli operator to be the number of qudits on which a non-identity operation (where a and b are not both zero (mod d)) is being applied.

We can now introduce the stabilizer formalism developed by Gottesman [36].

(All of the quantum error-correcting codes discussed in this thesis fit into the stabilizer description.) We choose an Abelian subgroup of the Pauli group P_n to define a quantum error-correcting code known as a *stabilizer code*. Let $\{S_1, S_2, \ldots, S_{n-k}\}$ be generators of the Abelian subgroup, known as the *stabilizer group*. Note that by definition, $S_a S_b = S_b S_a \ \forall \ a, b$. The codespace consists of all n-qudit states $|\psi\rangle$ that satisfy $S_a|\psi\rangle = |\psi\rangle \ \forall \ S_a$. That is, all of the generators act as the identity on (and thus *stabilize*) codewords. The codewords are joint eigenvectors of all of the stabilizer operators, with eigenvalue 1. It turns out that the dimension of the codespace is equivalent to that of k encoded qudits. We can repeatedly measure the S_a operators to verify that the state of the system is within the codespace.

For example, the well-known five-qubit code (which encodes one logical qubit and protects against arbitrary single qubit errors) has generators

$$\begin{aligned} S_1 &= Z \otimes X \otimes X \otimes Z \otimes I \\ S_2 &= I \otimes Z \otimes X \otimes X \otimes Z \\ S_3 &= Z \otimes I \otimes Z \otimes X \otimes X \\ S_4 &= X \otimes Z \otimes I \otimes Z \otimes X \end{aligned}$$

All sixteen stabilizer operators (including the identity) can be expressed in the form $(S_1)^{c_1}(S_2)^{c_2}(S_3)^{c_3}(S_4)^{c_4}$ for $c_j \in \{0, 1\}$. This code has the nice property of being able to choose generators which are cyclic shifts of one another. In all of the following, I will drop the explicit tensor products and simply refer to the stabilizer operators by $S_1 = ZXXZI$, $S_2 = IZXXZ$, and so on.

Consider a Pauli operator E_a that does not commute with at least one stabilizer element S_b. In particular, suppose that $S_b E_a = \omega^c E_a S_b$ for some integer c (with c not congruent to 0 (mod d)). We then observe that for any codeword $|\psi\rangle$,

$$S_b \left(E_a|\psi\rangle\right) \ = \ \left(S_b E_a\right)|\psi\rangle \ = \ \left(\omega^c E_a S_b\right)|\psi\rangle \ = \ \omega^c E_a \left(S_b|\psi\rangle\right) \ = \ \omega^c E_a|\psi\rangle \, .$$

Therefore, $E_a|\psi\rangle$ cannot be in the codespace, since it is an eigenvector of S_b with

eigenvalue ω^c, instead of 1. If we initially prepare the system of n qudits into some superposition of codewords, an application of E_a (which may be an error caused by the environment or a faulty circuit) moves the system into a state orthogonal to the codespace, and this action can be detected by measuring S_b. We denote the outcomes of measuring all of the stabilizer generators as the *syndrome* of the code. We can correct a set of errors $\{E_a\}$ if they have distinct syndromes.

For example, the five-qubit code has unique nontrivial syndromes for the set of single-qubit errors $\{XIIII, YIIII, ZIIII, \ldots, IIIIX, IIIIY, IIIIZ\}$. That is, a different subset of $\{S_1, S_2, S_3, S_4\}$ anticommute with each single-qubit error. We can maintain quantum information in the system as long as no more than one of the five physical qubits decoheres in between each error correction step.

To analyze the error-correcting properties of a stabilizer code, it is important to also identify the *normalizer group*. This is the set of Pauli operators (elements of P_n) that commute with all of the stabilizer operators. The normalizer group includes all stabilizer operators, in addition to other Pauli operators. In fact, the normalizer group has d^{2k} as many elements as the stabilizer group.

There are two main interpretations of the normalizer operators that are not contained in the stabilizer group. First, any such operator $\bar{S}$ is a logical operator on the encoded qudits in the system. We see this by observing that for any codeword $|\psi\rangle$,

$$S_a\left(\bar{S}|\psi\rangle\right) \;=\; \left(S_a\bar{S}\right)|\psi\rangle \;=\; \left(\bar{S}S_a\right)|\psi\rangle \;=\; \bar{S}\left(S_a|\psi\rangle\right) \;=\; \bar{S}|\psi\rangle\,.$$

Codewords are mapped to codewords under the action of $\bar{S}$. The second interpretation is that of undetectable errors. If the environment were to apply $\bar{S}$ on the system, the encoded quantum information could be altered without our even being able to detect this action.

For example, we can choose generators for the normalizer group of the five-qubit code to be $\{S_1, S_2, S_3, S_4, \bar{X}, \bar{Z}\}$, with $\bar{X} = ZZIXI$ and $\bar{Z} = IXZXI$. These last two are logical operators acting on the encoded qubit. Furthermore, because the

minimum weight of a normalizer operator not contained in the stabilizer group is 3 (which we have not proven here), this implies that the *distance* of the code is 3. That is, there exist weight-3 errors (such as $\bar{X}$ and $\bar{Z}$) that are undetectable by the code. Futhermore, some weight-2 errors are indistinguishable (in terms of having identical syndromes) from weight-1 errors. In general, errors acting on no more than t qubits can be detected if the stabilizer code has distance at least $(t+1)$, and they can be corrected if the distance is at least $(2t+1)$.

More in-depth descriptions of quantum error-correcting codes are provided in [72, 62].

1.3 Key features of lattices

Let us also identify some key features of *lattices*, which will provide compact mathematical descriptions of oscillator codes.

Given a set of m basis vectors $\{\vec{v}_j\} \in \mathbb{R}^n$ (with $m \leq n$), we can define an m-dimensional lattice as the set of points

$$\mathcal{L} \;=\; \left\{ \sum_{j=1}^{m} c_j \vec{v}_j \right\} \text{ with } c_j \in \mathbb{Z}\,.$$

That is, the lattice points are given by every integer combination of basis vectors (including the origin). We can represent the lattice $\mathcal{L}$ by an $m \times n$ matrix

$$M \;=\; \begin{pmatrix} \longleftarrow & v_1 & \longrightarrow \\ \longleftarrow & v_2 & \longrightarrow \\ & \vdots & \\ \longleftarrow & v_m & \longrightarrow \end{pmatrix}$$

whose row vectors provide a basis for the lattice. We can define the determinant of $\mathcal{L}$ to be $|\det M|$.

Sometimes it is helpful to be able to define a lattice within a subspace of a

higher-dimensional vector space. However, in all of the examples in Section 3.5, we will choose $m = n$.

An important property of a lattice is its *minimum distance*, which is the smallest distance between any two lattice points, or equivalently, the norm of the lattice vector closest to the origin (because the set of lattice points is closed under addition or subtraction). The minimum distance of $\mathcal{L}$ is thus

$$\min_{\vec{x} \in \mathcal{L} \setminus \{\vec{0}\}} \sqrt{\vec{x} \cdot \vec{x}}\,,$$

where $\mathcal{L} \setminus \{\vec{0}\}$ denotes the lattice $\mathcal{L}$ excluding the origin. In order to properly compare minimum distances, we restrict ourselves to lattices with determinant one. Such lattices are sometimes described as *self-dual* or *unimodular*.

An active area of mathematical research for over a hundred years has been to identify which lattices in $\mathbb{R}^n$ have the largest minimum distance possible for a given n. This is closely connected to the problem of finding arrangements of non-overlapping n-dimensional unit spheres that maximize the enclosed volume of the spheres (known as the sphere-packing problem), which has broad applications from fruit packing to data compression to providing better reception for cell phones. If we scale a lattice (multiply its basis vectors by a common factor) such that the distance between all lattice points is at least 1, then we can construct such a sphere packing by placing the centers of n-dimensional unit spheres at all of the lattice points. The lattice with largest minimum distance will give a sphere packing with greatest density.

The *kissing number* problem is also closely related to this area of research. In this case, we are seeking to maximize the number of n-dimensional unit spheres that touch (or kiss) a unit sphere centered at the origin, without overlapping. This is a problem of local geometry, while the sphere-packing problem deals with global properties of an arrangement. Nevertheless, in some dimensions, both the best known sphere packing and kissing number arrangements are given by the lattice with largest minimum distance.

Another property of a lattice that will be useful in our work is the *Voronoi cell*. This is the region around a lattice point $\vec{x}$ whose interior is closer to $\vec{x}$ than to any other lattice point. In the square lattice Z_2, which consists of the set of points (a, b) for integers a, b, the Voronoi cell of any lattice point is a square centered at that point.

In this thesis, we will be interested in *symplectic self-dual* lattices, whose basis vectors satisfy an additional constraint, in order to construct quantum error-correcting codes. Specifically, the *symplectic inner product* of any pair of lattice points must be an integer. This will be explained in more detail in the following chapters. Recent mathematical work [17, 8] has begun to identify how the optimal minimum distance of symplectic lattices compares with the optimal minimum distance of all Euclidean lattices. A good overview of symplectic lattices is presented in [13].

Chapter 2

Achievable rates for the Gaussian quantum channel

2.1 Abstract

We study the properties of quantum stabilizer codes whose finite-dimensional protected code space is embedded in an infinite-dimensional Hilbert space. The stabilizer group of such a code is associated with a symplectic integral lattice in the phase space of $2N$ canonical variables. From the existence of symplectic integral lattices with suitable properties, we infer a lower bound on the quantum capacity of the Gaussian quantum channel that matches the one-shot coherent information optimized over Gaussian input states.

2.2 Introduction

A central problem in quantum information theory is to determine the quantum capacity of a noisy quantum channel—the maximum rate at which coherent quantum information can be transmitted through the channel and recovered with arbitrarily good fidelity [62, 72]. A general solution to the corresponding problem for classical noisy channels was found by Shannon in the pioneering paper that launched clas-

sical information theory [75, 22]. With the development of the theory of quantum error correction [76, 80], considerable progress has been made toward characterizing the quantum channel capacity [12], but it remains less well understood than the classical capacity.

The asymptotic coherent information has been shown to provide an upper bound on the capacity [74, 7] and a matching lower bound has been conjectured, but not proven [55]. Unfortunately, the coherent information is not subadditive [27], so that its asymptotic value is not easily computed. Therefore, it has been possible to verify the coherent information conjecture in just a few simple cases [11].

One quantum channel of considerable intrinsic interest is the Gaussian quantum channel, which might also be simple enough to be analytically tractable, thus providing a fertile testing ground for the general theory of quantum capacities. A simple analytic formula for the capacity of the Gaussian classical channel was found by Shannon [75, 22]. The Gaussian quantum channel was studied by Holevo and Werner [41], who computed the one-shot coherent information for Gaussian input states, and derived an upper bound on the quantum capacity.

Lower bounds on the quantum capacity of the Gaussian quantum channel were established by Gottesman, Kitaev, and Preskill [38]. They developed quantum error-correcting codes that protect a finite-dimensional subspace of an infinite-dimensional Hilbert space, and showed that these codes can be used to transmit high-fidelity quantum information at a nonzero asymptotic rate. In this paper, we continue the study of the Gaussian quantum channel begun in [38]. Our main result is that the coherent information computed by Holevo and Werner is in fact an achievable rate. This result lends nontrivial support to the coherent information conjecture.

We define the Gaussian quantum channel and review the results of Holevo and Werner [41] in Section 2.3. In Section 2.4 we describe the stabilizer codes for continuous quantum variables introduced in [38], which are based on the concept of a symplectic integral lattice embedded in phase space. In Sections 2.5 and

2.6 we apply these codes to the Gaussian quantum channel, and calculate an achievable rate arising from lattices that realize efficient packings of spheres in high dimensions. This achievable rate matches the one-shot coherent information I_Q of the channel in cases where 2^{I_Q} is an integer. Rates achieved with concatenated coding are calculated in Section 2.7; these fall short of the coherent information but come close. In Section 2.8 we consider the Gaussian classical channel, and again find that concatenated codes achieve rates close to the capacity. Section 2.9 contains some concluding comments about the quantum capacity of the Gaussian quantum channel.

2.3 The Gaussian quantum channel

The Gaussian quantum channel is a natural generalization of the Gaussian classical channel. In the classical case, we consider a channel such that the input x and the output y are real numbers. The channel applies a displacement to the input by distance ξ,

$$y = x + \xi \ , \tag{2.1}$$

where ξ is a Gaussian random variable with mean zero and variance σ^2; the probability distribution governing ξ is

$$P(\xi) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\xi^2/2\sigma^2} \ . \tag{2.2}$$

Similarly, acting on a quantum system described by canonical variables q and p that satisfy the commutation relation $[q, p] = i\hbar$, we may consider a quantum channel that applies a phase-space displacement described by the unitary operator

$$D(\alpha) = \exp\left(\alpha a^\dagger + \alpha^* a\right) \ , \tag{2.3}$$

where α is a complex number, $[a, a^\dagger] = 1$, and q, p can be expressed in terms of a

and $a^\dagger$ as

$$q = \sqrt{\frac{\hbar}{2}}\left(a + a^\dagger\right) \ , \quad p = -i\sqrt{\frac{\hbar}{2}}\left(a - a^\dagger\right) \ . \tag{2.4}$$

This quantum channel is Gaussian if α is a complex Gaussian random variable with mean zero and variance $\tilde{\sigma}^2$. In that case, the channel is the superoperator (trace-preserving completely positive map) $\mathcal{E}$ that acts on the density operator ρ according to

$$\rho \to \mathcal{E}(\rho) = \frac{1}{\pi\tilde{\sigma}^2}\int d^2\alpha \ e^{-|\alpha|^2/\tilde{\sigma}^2} D(\alpha)\rho D(\alpha)^\dagger \ . \tag{2.5}$$

In other words, the position q and momentum p are displaced independently,

$$q \to q + \xi_q \ , \quad p \to p + \xi_p \ , \tag{2.6}$$

where ξ_q and ξ_p are real Gaussian random variables with mean zero and variance $\sigma^2 = \hbar\tilde{\sigma}^2$.

To define the capacity, we consider a channel's nth extension. In the classical case, a message is transmitted consisting of the n real variables

$$\vec{x} = (x_1, x_2, \ldots, x_n) \ , \tag{2.7}$$

and the channel applies the displacement

$$\vec{x} \to \vec{x} + \vec{\xi} \ , \quad \vec{\xi} = (\xi_1, \xi_2, \ldots, \xi_n) \ , \tag{2.8}$$

where the ξ_i's are independent Gaussian random variables, each with mean zero and variance σ^2. A code consists of a finite number m of n-component input signals

$$\vec{x}^{(a)} \ , \quad a = 1, 2, \ldots, m \tag{2.9}$$

and a decoding function that maps output vectors to the index set $\{1, 2, \ldots, m\}$. We refer to n as the *length* of the code.

If the input vectors were unrestricted, then for fixed σ^2 we could easily construct

a code with an arbitrarily large number of signals m and a decoding function that correctly identifies the index (a) of the input with arbitrarily small probability of error; even for $n = 1$ we merely choose the distance between signals to be large compared to σ. To obtain an interesting notion of capacity, we impose a constraint on the *average power* of the signal,

$$\frac{1}{n}\sum_i \left(x_i^{(a)}\right)^2 \leq P \ , \tag{2.10}$$

for each a. We say that a rate R (in bits) is achievable with power constraint P if the there is a sequence of codes satisfying the constraint such that the βth code in the sequence contains m_β signals with length n_β, where

$$R = \lim_{\beta\to\infty} \frac{1}{n_\beta}\log_2 m_\beta \ , \tag{2.11}$$

and the probability of a decoding error vanishes in the limit $\beta \to \infty$. The capacity of the channel with power constraint P is the supremum of all achievable rates.

The need for a constraint on the signal power to define the capacity of the Gaussian classical channel can be understood on dimensional grounds. The classical capacity (in bits) is a dimensionless function of the variance σ^2, but σ^2 has dimensions. Another quantity with the dimensions of σ^2 is needed to construct a dimensionless variable, and the power P fills this role.

In contrast, no power constraint is needed to define the quantum capacity of the quantum channel. Rather, Planck's constant $\hbar$ enables us to define a dimensionless variance $\tilde{\sigma}^2 = \sigma^2/\hbar$, and the capacity is a function of this quantity. In the quantum case, a code consists of an encoding superoperator that maps an m-dimensional Hilbert space $\mathcal{H}_m$ into the infinite-dimensional Hilbert space $\mathcal{H}^{\otimes N}$ of N canonical quantum systems, and a decoding superoperator that maps $\mathcal{H}^{\otimes N}$ back to $\mathcal{H}_m$. We say that the rate R (in qubits) is achievable if there is a sequence of codes such that

$$R = \lim_{\beta\to\infty} \frac{1}{N_\beta}\log_2 m_\beta \ , \tag{2.12}$$

where arbitrary states in $\mathcal{H}_m$ can be recovered with a fidelity that approaches 1 as $\beta \to \infty$. The quantum capacity C_Q of the channel is defined as the supremum of all achievable rates.

Holevo and Werner [41] studied a more general Gaussian channel that includes damping or amplification as well as displacement. However, we will confine our attention in this paper to channels that apply only displacements. Holevo and Werner derived a general upper bound on the quantum capacity by exploiting the properties of the "diamond norm" (norm of complete boundedness) of a superoperator. The diamond norm is defined as follows: First we define the trace norm of an operator X as

$$\|X\|_{\mathrm{tr}} \equiv \mathrm{tr}\sqrt{X^\dagger X} \ , \tag{2.13}$$

which for a self-adjoint operator is just the sum of the absolute values of the eigenvalues. Then a norm of a superoperator $\mathcal{E}$ can be defined as

$$\|\mathcal{E}\|_{\mathrm{so}} = \sup_{X \neq 0} \frac{\|\mathcal{E}(X)\|_{\mathrm{tr}}}{\|X\|_{\mathrm{tr}}} \ . \tag{2.14}$$

The superoperator norm is not stable with respect to appending an ancillary system on which $\mathcal{E}$ acts trivially. Thus we define the diamond norm of $\mathcal{E}$ as

$$\|\mathcal{E}\|_{\diamond} = \sup_n \|\mathcal{E} \otimes I_n\|_{\mathrm{so}} \ , \tag{2.15}$$

where I_n denotes the n-dimensional identity operator. (This supremum is always attained for some n no larger than the dimension of the Hilbert space on which $\mathcal{E}$ acts.) Holevo and Werner showed that the quantum capacity obeys the upper bound

$$C_Q(\mathcal{E}) \leq \log_2 \|\mathcal{E} \circ T\|_{\diamond} \ , \tag{2.16}$$

where T is the transpose operation defined with respect to some basis. In the case of the Gaussian quantum channel, they evaluated this expression, obtaining

$$C_Q(\sigma^2) \leq \log_2 \left(\hbar/\sigma^2\right) \tag{2.17}$$

for $\hbar/\sigma^2 > 1$, and $C_Q(\sigma^2) = 0$ for $\hbar/\sigma^2 \leq 1$.

Holevo and Werner [41] also computed the *coherent information* of the Gaussian quantum channel for a Gaussian input state. To define the coherent information of the channel $\mathcal{E}$ with input density operator ρ, one introduces a reference system R and a *purification* of ρ, a pure state $|\Phi\rangle$ such that

$$\mathrm{tr}_R\left(|\Phi\rangle\langle\Phi|\right) = \rho \ . \tag{2.18}$$

Then the coherent information I_Q is

$$I_Q(\mathcal{E},\rho) = S\left(\mathcal{E}(\rho)\right) - S\left(\mathcal{E}\otimes I_R(|\Phi\rangle\langle\Phi|)\right) \ , \tag{2.19}$$

where S denotes the Von Neumann entropy,

$$S(\rho) = -\mathrm{tr}\left(\rho\log_2\rho\right) \ . \tag{2.20}$$

It is *conjectured* [55, 74, 7] that the quantum capacity is related to the coherent information by

$$C_Q(\mathcal{E}) = \lim_{n\to\infty} \ \frac{1}{n}\cdot C_n(\mathcal{E}) \ , \tag{2.21}$$

where

$$C_n(\mathcal{E}) = \sup_{\rho} I_Q(\mathcal{E}^{\otimes n},\rho) \ . \tag{2.22}$$

Unlike the mutual information that defines the classical capacity, the coherent information is not subadditive in general, and therefore the quantum capacity need not coincide with the "one-shot" capacity C_1. Holevo and Werner showed that for the Gaussian quantum channel, the supremum of I_Q over Gaussian input states is

$$\left(I_Q\right)_{\max} = \log_2(\hbar/e\sigma^2) \tag{2.23}$$

(where $e = 2.71828..$) for $\hbar/e\sigma^2 > 1$, and $\left(I_Q\right)_{\max} = 0$ for $\hbar/e\sigma^2 \leq 1$. According to the coherent-information conjecture, eq. (2.23) should be an achievable rate.

2.4 Lattice codes for continuous quantum variables

The lattice codes developed in [38] are stabilizer codes [35, 18] that embed a finite-dimensional code space in the infinite-dimensional Hilbert space of N "oscillators," a system described by $2N$ canonical variables $q_1, q_2, \ldots q_N, p_1, p_2, \ldots, p_N$. That is, the code space is the simultaneous eigenstate of $2N$ commuting unitary operators, the generators of the code's stabilizer group. Each stabilizer generator is a *Weyl operator*, a displacement in the $2N$-dimensional phase space.

Such displacements can be parametrized by $2N$ real numbers $\alpha_1, \alpha_2, \ldots, \alpha_N$, $\beta_1, \beta_2, \ldots, \beta_N$, and expressed as

$$U(\alpha, \beta) = \exp\left[i\sqrt{2\pi} \left(\sum_{i=1}^{N} \alpha_i p_i + \beta_i q_i \right) \right] \ . \tag{2.24}$$

Two such operators obey the commutation relation

$$U(\alpha, \beta) U(\alpha', \beta') = e^{2\pi i \omega(\alpha\beta, \alpha'\beta')} U(\alpha', \beta') U(\alpha, \beta) \ , \tag{2.25}$$

where

$$\omega(\alpha\beta, \alpha'\beta') \equiv \alpha \cdot \beta' - \alpha' \cdot \beta \tag{2.26}$$

is the symplectic form (or symplectic inner product). Thus Weyl operators commute if and only if their symplectic form is an integer.

The $2N$ generators of a stabilizer code are commuting Weyl operators

$$U\left(\alpha^{(a)}, \beta^{(a)}\right) \ , \quad a = 1, 2, \ldots, 2N \ . \tag{2.27}$$

Thus the elements of the stabilizer group are in one-to-one correspondence with the points of a lattice $\mathcal{L}$ generated by the $2N$ vectors $v^{(a)} = (\alpha^{(a)}, \beta^{(a)})$. These

vectors can be assembled into the generator matrix M of $\mathcal{L}$ given by

$$M = \begin{pmatrix} v^{(1)} \\ v^{(2)} \\ . \\ . \\ v^{(2N)} \end{pmatrix} . \tag{2.28}$$

Then the requirement that the stabilizer generators commute, through eq. (2.25), becomes the condition that the antisymmetric matrix

$$A = M\omega M^T \tag{2.29}$$

has integral entries, where M^T denotes the transpose of M, ω is the $2N \times 2N$ matrix

$$\omega = \begin{pmatrix} 0 & I_N \\ -I_N & 0 \end{pmatrix} \tag{2.30}$$

and I_N is the $N \times N$ identity matrix. If the generator matrix M of a lattice $\mathcal{L}$ has the property that A is an integral matrix, then we will say that the lattice $\mathcal{L}$ is *symplectic integral*.

Encoded operations that preserve the code subspace are associated with the code's *normalizer* group, the group of phase space translations that commute with the code stabilizer. The generator matrix of the normalizer is a matrix $M^\perp$ that can be chosen to be

$$M^\perp = A^{-1}M \ , \tag{2.31}$$

so that

$$M^\perp \omega M^T = I \ ; \tag{2.32}$$

and

$$\left(M^\perp\right) \omega \left(M^\perp\right)^T = \left(A^{-1}\right)^T \ . \tag{2.33}$$

We will refer to the lattice generated by $M^{\perp}$ as the *symplectic dual* $\mathcal{L}^{\perp}$ of the lattice $\mathcal{L}$.

Another matrix that generates the same lattice as M (and therefore defines a different set of generators for the same stabilizer group) is

$$M' = RM \ , \tag{2.34}$$

where R is an integral matrix with $\det R = \pm 1$. This replacement changes the matrix A according to

$$A \to RAR^T \ . \tag{2.35}$$

By Gaussian elimination, an R can be constructed such that

$$A = \begin{pmatrix} 0 & D \\ -D & 0 \end{pmatrix} \ , \tag{2.36}$$

and

$$\left(A^{-1}\right)^T = \begin{pmatrix} 0 & D^{-1} \\ -D^{-1} & 0 \end{pmatrix} \ , \tag{2.37}$$

where D is a positive diagonal integral $N \times N$ matrix. In the important special case of a *symplectic self-dual* lattice, both A and $\left(A^{-1}\right)^T$ are integral matrices; therefore $D = D^{-1}$ and the standard form of A is

$$A = \begin{pmatrix} 0 & I_N \\ -I_N & 0 \end{pmatrix} = \omega \ . \tag{2.38}$$

Hence the generator matrix of a symplectic self-dual lattice can be chosen to be a real symplectic matrix: $M\omega M^T = \omega$.

If the lattice is rotated, then the generator matrix is transformed as

$$M \to MO \ , \tag{2.39}$$

where O is an orthogonal matrix. Therefore, it is convenient to characterize a

lattice with its Gram matrix

$$G = MM^T \ , \tag{2.40}$$

which is symmetric, positive, and rotationally invariant. In the case of a symplectic self-dual lattice, the Gram matrix G can be chosen to be symplectic, and two symplectic Gram matrices G and G' describe the same lattice if

$$G' = RGR^T \ , \tag{2.41}$$

where R is symplectic and integral. Therefore, the moduli space of symplectic self-dual lattices in $2N$ dimensions can be represented as

$$\mathcal{A}_N = H(2N)/Sp(2N, Z) \ , \tag{2.42}$$

where $H(2N)$ denotes the space of real symplectic positive $2N \times 2N$ matrices of determinant 1. The space $\mathcal{A}_N$ can also be identified as the moduli space of principally polarized abelian varieties in complex dimension N [17].

The encoded operations that preserve the code space but act trivially within the code space comprise the quotient group $\mathcal{L}^\perp/\mathcal{L}$. The order of this group, the ratio of the volume of the unit cell of $\mathcal{L}$ to that of $\mathcal{L}^\perp$, is m^2, where m is the dimension of the code space. The volume of the unit cell of $\mathcal{L}$ is $|\det M| = |\det A|^{1/2}$ and the volume of the unit cell of $\mathcal{L}^\perp$ is $|\det M^\perp| = |\det A|^{-1/2}$; therefore the dimension of the code space is

$$m = |\mathrm{Pf}\ A| = |\det M| = \det D \ , \tag{2.43}$$

where Pf A denotes the Pfaffian of A, the square root of its determinant. Thus, a symplectic self-dual lattice, for which $|\det M| = |\det M^\perp| = 1$, corresponds to a code with a one-dimensional code space. Given a $2N \times 2N$ generator matrix M of a symplectic self-dual lattice, we can rescale it as

$$M \to \sqrt{\lambda} M \ , \tag{2.44}$$

where λ is an integer, to obtain the generator matrix of a symplectic integral lattice corresponding to a code of dimension

$$m = \lambda^N \ . \tag{2.45}$$

The rate of this code, then, is

$$R = \log_2 \lambda \ . \tag{2.46}$$

When an encoded state is subjected to the Gaussian quantum channel, a phase space displacement

$$(\vec{q}, \vec{p}) \to (\vec{q}, \vec{p}) + (\vec{\xi}_q, \vec{\xi}_p) \tag{2.47}$$

is applied. To diagnose and correct this error, the eigenvalues of all stabilizer generators are measured, which determines the value of $(\vec{\xi}_q, \vec{\xi}_p)$ modulo the normalizer lattice $\mathcal{L}^\perp$. To recover, a displacement of minimal length is applied that returns the stabilizer eigenvalues to their standard values, and so restores the quantum state to the code space. We can associate with the origin of the normalizer lattice its *Voronoi cell*, the set of points in $\mathbb{R}^{2N}$ that are closer to the origin than to any other lattice site. Recovery is successful if the applied displacement lies in this Voronoi cell. Thus, we can estimate the likelihood of a decoding error by calculating the probability that the displacement lies outside the Voronoi cell.

2.5 Achievable rates from efficient sphere packings

One way to establish an achievable rate for the Gaussian quantum channel is to choose a normalizer lattice $\mathcal{L}^\perp$ whose shortest nonzero vector is sufficiently large. In this Section, we calculate an achievable rate by demanding that the Voronoi cell surrounding the origin contain all typical displacements of the origin in the limit of large N. In Sec. V, we will use a more clever argument to improve our estimate of the rate.

The volume of a sphere with unit radius in n dimensions is

$$V_n = \frac{\pi^{n/2}}{\Gamma\left(\frac{n}{2}+1\right)} \ , \tag{2.48}$$

and from the Stirling approximation we find that

$$V_n \leq \left(\frac{2\pi e}{n}\right)^{n/2} \ . \tag{2.49}$$

It was shown by Minkowski [61] that lattice sphere packings exist in n dimensions that fill a fraction at least $1/2^{(n-1)}$ of space. Correspondingly, if the lattice is chosen to be unimodular, so that its unit cell has unit volume, then kissing spheres centered at the lattice sites can be chosen to have a radius r_n such that

$$V_n \left(r_n\right)^n \geq 2^{-(n-1)} \ , \tag{2.50}$$

or

$$r_n^2 \geq \frac{1}{4}(2/V_n)^{2/n} \geq \frac{n}{8\pi e} \ . \tag{2.51}$$

This lower bound on the efficiency of sphere packings has never been improved in the nearly 100 years since Minkowski's result. More recently, Buser and Sarnak [17] have shown that this same lower bound applies to lattices that are symplectic self-dual.

Now consider the case of $n = 2N$-dimensional phase space. For sufficiently large n, the channel will apply a phase space translation by a distance which with high probability will be less than $\sqrt{n(\sigma^2+\varepsilon)}$, for any positive ε. Therefore, a code that can correct a shift this large will correct all likely errors. What rate can such a code attain? If the code is a lattice stabilizer code, and the dimension of the code space is m, then the unit cell of the code's normalizer lattice has volume

$$\Delta = \frac{1}{m} \cdot (2\pi\hbar)^N \ . \tag{2.52}$$

Nonoverlapping spheres centered at the sites of the normalizer lattice can be chosen

to have radius $r = \sqrt{n(\sigma^2 + \varepsilon)}$, where

$$\left(\frac{2\pi e}{n}\right)^{n/2} \left(n(\sigma^2+\varepsilon)\right)^{n/2} \geq \frac{1}{m} \cdot 2^{-n} \cdot (2\pi\hbar)^{n/2} \ , \tag{2.53}$$

or

$$m \geq \left(\frac{\hbar}{4e}(\sigma^2+\varepsilon)\right)^N \ . \tag{2.54}$$

The error probability becomes arbitrarily small for large N if eq. (2.54) is satisfied, for any positive ε. We conclude that the rate

$$R \equiv \frac{1}{N} \cdot \log_2 m = \log_2 \left(\frac{\hbar}{4e\sigma^2}\right) \ , \tag{2.55}$$

is achievable, provided $\hbar/4e\sigma^2 \geq 1$. However, as noted in Sec. III, the rates that can be attained by this construction (rescaling of a symplectic self-dual lattice) are always of the form $\log_2 \lambda$, where λ is an integer.

2.6 Improving the rate

The achievable rate found in eq. (2.55) falls two qubits short of the coherent information eq. (2.23). We will now show that this gap can be closed by using tighter estimates of the error probability. We established eq. (2.55) by filling phase space with nonoverlapping spheres, which is overly conservative. It is acceptable for the spheres to overlap, as long as the overlaps occupy an asymptotically negligible fraction of the total volume, as suggested in Figure 2.1.

Our improved estimate applies another result obtained by Buser and Sarnak [17]. They note that the moduli space of symplectic self-dual lattices is compact and equipped with a natural invariant measure. Therefore, it makes sense to consider averaging over all lattices. Denote by $\langle\cdot\rangle$ the average over all symplectic self-dual lattices with specified dimension $n = 2N$, and let $f(x)$ denote an integrable rotationally-invariant function of the vector x (that is a function of the

length $|x|$ of x). Then Buser and Sarnak [17] show that

$$\Big\langle \sum_{x \in \mathcal{L} \setminus \{0\}} f(x) \Big\rangle = \int f(x)\ d^n x\ . \tag{2.56}$$

(Note that the sum is over all *nonzero* vectors in the lattice $\mathcal{L}$.) It follows that there must exist a *particular* symplectic self-dual lattice $\mathcal{L}$ such that

$$\sum_{x \in \mathcal{L} \setminus \{0\}} f(x) \leq \int f(x)\ d^n x\ . \tag{2.57}$$

The statement that a *unimodular* lattice exists that satisfies eq. (2.57) is the well-known Minkowski-Hlawka theorem [20]. Buser and Sarnak established the stronger result that the lattice can be chosen to be symplectic self-dual.

We can use this result to bound the probability of a decoding error, and establish that a specified rate is achievable. Our argument will closely follow de Buda [23], who performed a similar analysis of lattice codes for the Gaussian classical channel. However, the quantum case is considerably easier to analyze, because we can avoid complications arising from the power constraint [24, 53, 83].

A decoding error occurs if the channel displaces the origin to a point outside the Voronoi cell centered at the origin. The Voronoi cell has a complicated geometry, so that the error probability is not easy to analyze. But we can simplify the analysis with a trick [23]. Imagine drawing a sphere with radius

$$a = \sqrt{n(\sigma^2 + \varepsilon)} \tag{2.58}$$

around each lattice site, where $\varepsilon > 0$; this value of a is chosen so that the typical displacement introduced by the channel has length less than a; the probability of a shift larger than a thus becomes negligible for large n. It may be that these spheres overlap. However, a vector that is contained in the sphere centered at the origin, and is not contained in the sphere centered at any other lattice site, must be closer to the origin than any other lattice site. Therefore, the vector is contained

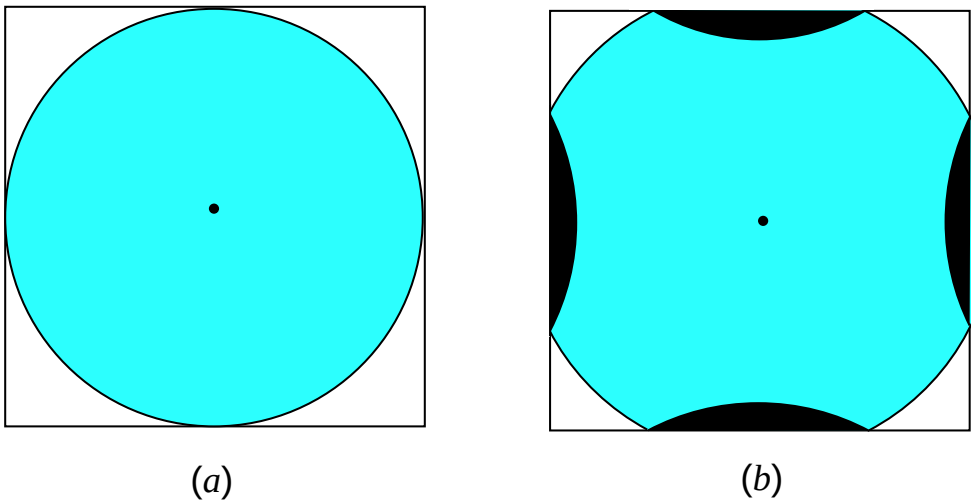

Figure 2.1: Two ways to estimate the rate achieved by a lattice code. Each site of the normalizer lattice has a Voronoi cell (represented here by a square) containing all points that are closer to that site than any other site. Displacements that move a site to a position within its Voronoi cell can be corrected. The volume of the Voronoi cell determines the rate of the code. In (a), the ball containing typical displacements lies within the cell, so that the error probability is small. In (b), the ball of typical displacements is not completely contained within the cell, but the region where neighboring balls overlap (shown in black) has a small volume, so that the error probability is still small.

in the origin's Voronoi cell, and is a shift that can be corrected successfully. (See Figure 2.1.)

Hence (ignoring the possibility of an atypical shift by $\xi > a$) we can upper bound the probability of error by estimating the probability that the shift moves any other lattice site into the sphere of radius a around the origin. We then find

$$P_{\text{error}} \leq \sum_{x \in \mathcal{L}^{\perp} \setminus \{0\}} \int_{|r| \leq a} P(x - r) d^n r \ , \tag{2.59}$$

where $P(\xi)$ denotes the probability of a displacement by ξ.

The Buser-Sarnak theorem [17] tells us that there exists a lattice whose unit cell has volume Δ, and which is related by rescaling to a symplectic self-dual lattice, such that

$$P_{\text{error}} \leq \frac{1}{\Delta} \int d^n x \int_{|r| \leq a} P(x - r) d^n r \ ; \tag{2.60}$$

by interchanging the order of integration, we find that

$$P_{\text{error}} \leq \frac{1}{\Delta} \cdot V_n \cdot a^n \ , \tag{2.61}$$

the ratio of the volume of the n-dimensional sphere of radius a to the volume of the unit cell.

Now the volume Δ of the unit cell of the normalizer lattice $\mathcal{L}^{\perp}$, and the dimension m of the code space, are related by

$$\Delta = (2\pi\hbar)^N m^{-1} = \left(2\pi\hbar \cdot 2^{-R}\right)^N \ , \tag{2.62}$$

where R is the rate, and we may estimate the volume of the sphere as

$$V_n \cdot a^n \leq \left(\frac{2\pi e}{n}\right)^{n/2} \left(n(\sigma^2 + \varepsilon)\right)^{n/2} \ , \tag{2.63}$$

where $n = 2N$. Thus we conclude that

$$P_{\text{error}} \leq \left(\frac{e}{\hbar}(\sigma^2 + \varepsilon) \cdot 2^R\right)^N \ . \tag{2.64}$$

Therefore, the error probability becomes small for large N for any rate R such that

$$R < \log_2 \left(\frac{\hbar}{e}(\sigma^2 + \varepsilon)\right) \ , \tag{2.65}$$

where ε may be arbitrarily small. We conclude that the rate

$$R = \log_2 \left(\frac{\hbar}{e\sigma^2}\right) \tag{2.66}$$

is achievable in the limit $N \to \infty$, provided that $\hbar/e\sigma^2 > 1$. This rate matches the optimal value eq. (2.23) of the one-shot coherent information for Gaussian inputs. We note, again, that the rates that we can obtain from rescaling a symplectic self-dual lattice are restricted to $R = \log_2 \lambda$, where λ is an integer. Thus for specified σ^2, the achievable rate that we have established is really the maximal value of

$$R = \log_2 \lambda \ , \quad \lambda \in Z \ , \tag{2.67}$$

such that the positive integer λ satisfies

$$\lambda < \frac{\hbar}{e\sigma^2} \ . \tag{2.68}$$

2.7 Achievable rates from concatenated codes

Another method for establishing achievable rates over the Gaussian quantum channel was described in [38], based on *concatenated coding*. In each of N "oscillators" described by canonical variables p_i and q_i, a d-dimensional system ("qudit") is encoded that is protected against sufficiently small shifts in p_i and q_i. The encoded qudit is associated with a square lattice in two-dimensional phase space. Then a

stabilizer code is constructed that embeds a k-qudit code space in the Hilbert space of N qudits; these k encoded qudits are protected if a sufficiently small fraction of the N qudits are damaged. Let us compare the rates achieved by concatenated codes to the rates achieved with codes derived from efficient sphere packings.

We analyze the effectiveness of concatenated codes in two stages. First we consider how likely each of the N qudits is to sustain damage if the underlying oscillator is subjected to the Gaussian quantum channel. The area of the unit cell of the two-dimensional square normalizer lattice that represents the encoded operations acting on the qudit is $2\pi\hbar/d$, and the minimum distance between lattice sites is $\delta = \sqrt{2\pi\hbar/d}$. A displacement of q by $a \cdot \delta$, where a is an integer, is the operation X^a acting on the code space, and a displacement of p by $b \cdot \delta$ is the operation Z^b, where X and Z are the Pauli operators acting on the qudit; these act on a basis $\{|j\rangle,\ j = 0, 1, 2, \ldots, d-1\}$ for the qudit according to

$$\begin{aligned} X : |j\rangle &\rightarrow |j+1 \ (\mathrm{mod}\ d)\rangle \ , \\ Z : |j\rangle &\rightarrow w^j |j\rangle \ , \end{aligned} \tag{2.69}$$

where $\omega = \exp(2\pi i/d)$.

Shifts in p or q can be corrected successfully provided that they satisfy

$$|\Delta q| < \delta/2 = \sqrt{\frac{\pi\hbar}{2d}} \ , \quad |\Delta p| < \delta/2 = \sqrt{\frac{\pi\hbar}{2d}} \ . \tag{2.70}$$

If the shifts in q and p are Gaussian random variables with variance σ^2, then the probability that a shift causes an uncorrectable error is no larger than the probability that the shift exceeds $\sqrt{\pi\hbar/2d}$, or

$$\begin{aligned} p_X, p_Z \leq & \quad 2 \cdot \frac{1}{\sqrt{2\pi\sigma^2}} \int_{\sqrt{\pi\hbar/2d}}^{\infty} dx e^{-x^2/2\sigma^2} \\ = & \quad \mathrm{erfc}(\sqrt{\pi\hbar/4d\sigma^2}) \ , \end{aligned} \tag{2.71}$$

where erfc denotes the complementary error function. Here p_X is the probability

of an "X error" acting on the qudit, of the form X^a for $a \not\equiv 0 \pmod{d}$, and p_Z denotes the probability of a "Z error" of the form Z^b for $b \not\equiv 0 \pmod{d}$. The X and Z errors are uncorrelated, and errors with $a, b = \pm 1$ are much more likely than errors with $|a|, |b| > 1$. By choosing $d \sim \hbar/\sigma^2$, we can achieve a small error probability for each oscillator.

The second stage of the argument is to determine the rate that can be achieved by a qudit code if p_X and p_Z satisfy eq. (2.71). We will consider codes of the Calderbank-Shor-Steane (CSS) type, for which the correction of X errors and Z errors can be considered separately [19, 81]. A CSS code is a stabilizer code, in which each stabilizer generator is either a tensor product of I's and powers of Z (measuring these generators diagnoses the X errors) or a tensor product of I's and powers of X (for diagnosing the Z errors).

We can establish an achievable rate by averaging the error probability over CSS codes; we give only an informal sketch of the argument. Suppose that we fix the block size N and the number of encoded qudits k. Now select the generators of the code's stabilizer group at random. About half of the $N-k$ generators are of the Z type and about half are of the X type. Thus the number of possible values for the eigenvalues of the generators of each type is about

$$d^{\frac{1}{2}(N-k)} \ . \tag{2.72}$$

Now we can analyze the probability that an uncorrectable X error afflicts the encoded quantum state (the probability of an uncorrectable Z error is analyzed in exactly the same way). Suppose that X errors act independently on the N qudits in the block, with a probability of error per qudit of p_X. Thus for large N, the typical number of damaged qudits is close to $p_X \cdot N$. A damaged qudit can be damaged in any of $d-1$ different ways (X^a, where $a = 1, 2, \ldots, (d-1)$). We will suppose, pessimistically, that all $d-1$ shifts of the qudit are equally likely. The actual situation that arises in our concatenated coding scheme is more favorable—small values of $|a|$ are more likely—but our argument will not exploit this feature.

Thus, with high probability, the error that afflicts the block will belong to a typical set of errors that contains a number of elements close to

$$N_{\text{typ}} \sim \binom{N}{Np_X} (d-1)^{Np_X} \sim d^{N(H_d(p_X)+p_X \log_d(d-1))} \ , \tag{2.73}$$

where

$$H_d(p) = -p \log_d p - (1-p) \log_d (1-p) \ . \tag{2.74}$$

If a particular typical error occurs, then recovery will succeed as long as there is no other typical error that generates the same error syndrome. It will be highly unlikely that another typical error has the same syndrome as the actual error, provided that the number of possible error syndromes $d^{\frac{1}{2}(N-k)}$ is large compared to the number of typical errors. Therefore, the X errors can be corrected with high probability for

$$\begin{aligned} &\frac{1}{2}\left(1 - \frac{k}{N}\right) \\ &\quad > \frac{1}{N} \cdot \log_d N_{\text{typ}} \sim H_d(p_X) + p_X \log_d(d-1) \ , \end{aligned} \tag{2.75}$$

or for a rate R_d in qudits satisfying

$$R_d \equiv \frac{k}{N} < 1 - 2H_d(p_X) - 2p_X \log_d(d-1) \tag{2.76}$$

Similarly, the Z errors can be corrected with high probability by a random CSS code if the rate satisfies

$$R_d < 1 - 2H_d(p_Z) - 2p_Z \log_d(d-1) \ . \tag{2.77}$$

Converted to qubits, the rate becomes

$$R = \log_2 d \cdot R_d \tag{2.78}$$

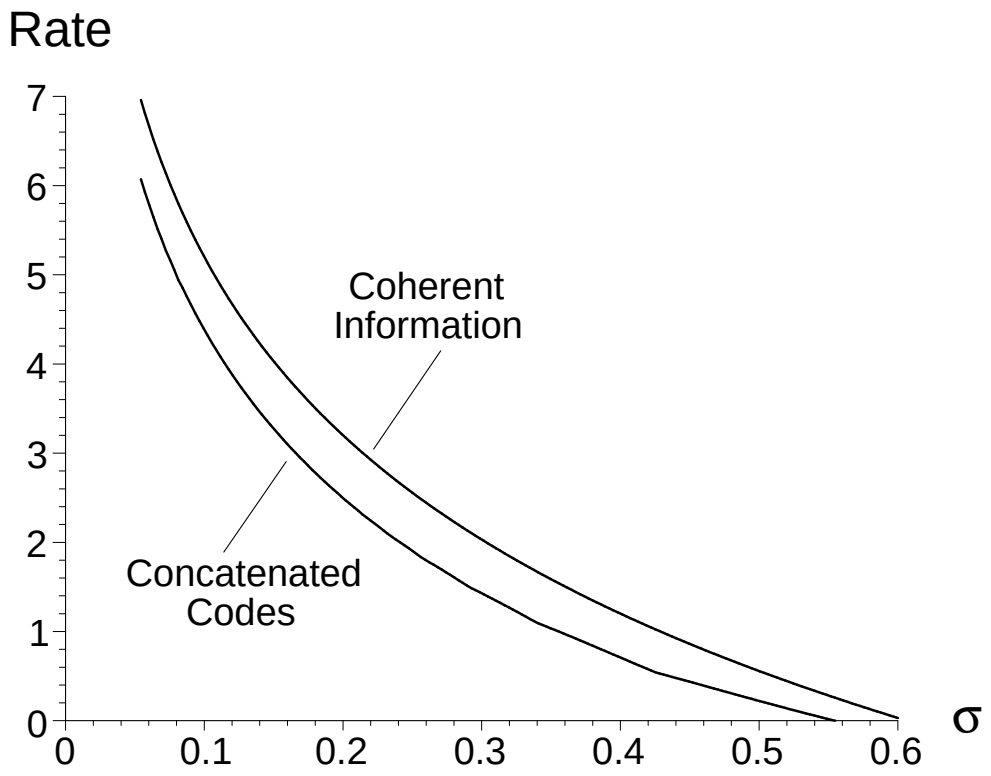

Figure 2.2: Rates achieved by concatenated codes, compared to the one-shot coherent information optimized over Gaussian input states. Here σ is the standard deviation of the magnitude of the phase-space displacement introduced by the channel, in units with $\hbar = 1$.

Under these conditions, the probability of error averaged over CSS codes becomes arbitrarily small for N large. It follows that there is a particular sequence of CSS codes with rate approaching eq. (2.76-2.78), and error probability going to zero in the limit $N \to \infty$.

For given σ^2, the optimal rate that can be attained by concatenating a code that encodes a qudit in a single oscillator with a random CSS code, is found by estimating p_X and p_Z using eq. (2.71) and then choosing d to maximize the rate R given by eq. (2.76-2.78). The results are shown in Figure 2.2. This rate (in qubits)

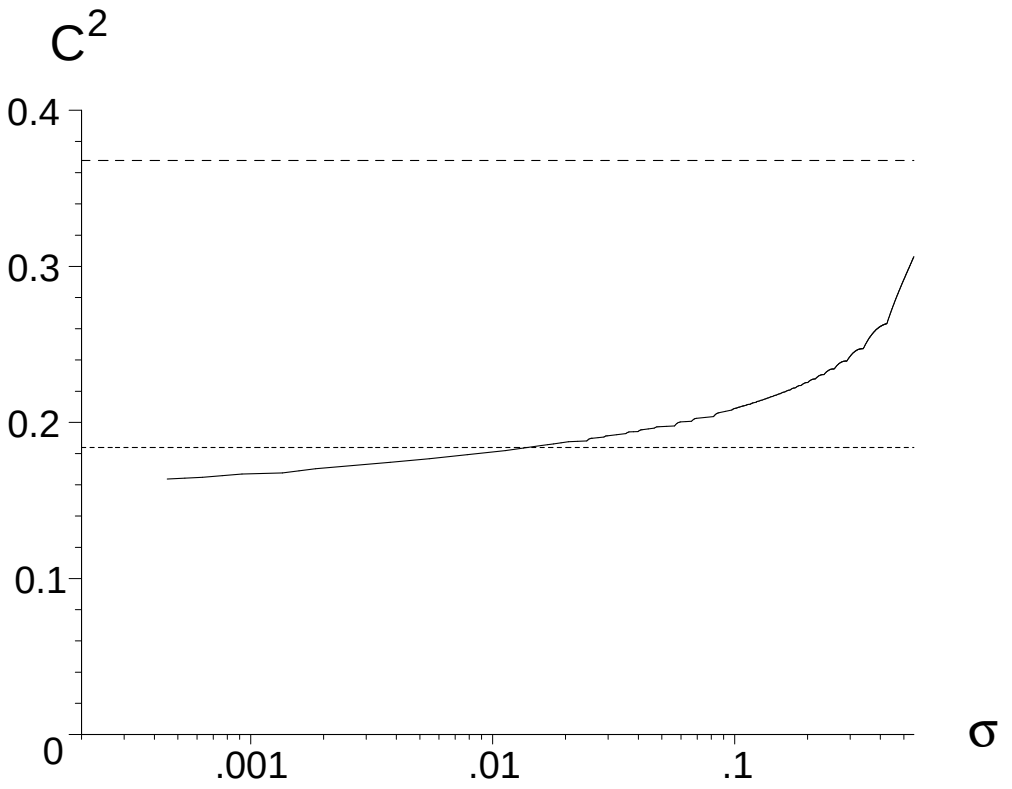

Figure 2.3: The slowly varying function C^2, defined by $R = \log_2(C^2/\sigma^2)$, where R is the rate achievable with concatenated codes. Units have been chosen such that $\hbar = 1$. The horizontal lines are at $C^2 = 1/e$, corresponding to a rate equal to the coherent information, and at $C^2 = 1/2e$, corresponding to one qubit below the coherent information.

can be expressed as

$$R = \log_2 \left(C^2 \hbar / \sigma^2 \right) \ , \tag{2.79}$$

where C^2 is a slowly varying function of $\sigma^2/\hbar$ plotted in Figure 2.3. It turns out that this rate is actually fairly close to $\log_2 d$; that is, the optimal dimension d of the qudit encoded in each oscillator is approximately $C^2\hbar/\sigma^2$. With this choice for d, the error rate for each oscillator is reasonably small, and the random CSS code reduces the error probability for the encoded state to a value exponentially small in N at a modest cost in rate. The rate achieved by concatenating coding lies strictly below the coherent information I_Q, but comes within one qubit of I_Q for $\sigma^2 > 1.88 \times 10^{-4}$.

Both the concatenated codes and the codes derived from efficient sphere packings are stabilizer codes, and therefore both are associated with lattices in $2N$-dimensional phase space. But while the sphere-packing codes have been chosen so that the shortest nonzero vector on the lattice is large relative to the size of the unit cell, the concatenated codes correspond to sphere packings of poor quality. For the concatenated codes, the shortest vector of the normalizer lattice has length ℓ, where

$$\ell^2 = 2\pi\hbar/d \tag{2.80}$$

and the rate R is close to $\log_2 d$. The efficient sphere packings have radius $r = \ell/2$ close to $\sqrt{n\sigma^2}$, or

$$\ell^2 = \frac{8N\hbar}{e} \cdot 2^{-R} \ . \tag{2.81}$$

Hence, if we compare sphere-packing codes and concatenated codes with comparable rates, the sphere-packing codes have minimum distance that is larger by a factor of about $\sqrt{4N/\pi e}$. The concatenated codes achieve a high rate not because the minimum distance of the lattice is large, but rather because the decoding procedure exploits the hierarchical structure of the code.

2.8 The Gaussian classical channel

We have found that quantum stabilizer codes based on efficient sphere packings can achieve rates for the Gaussian quantum channel that match the one-shot coherent information, and that concatenated codes achieve rates that are below, but close to, the coherent information. Now, as an aside, we will discuss the corresponding statements for the Gaussian classical channel. We will see, in particular, that concatenated codes achieve rates that are close to the classical channel capacity.

Shannon's expression for the capacity of the Gaussian classical channel can be understood heuristically as follows [75, 22]. If the input signals have average power P, which is inflated by the Gaussian noise to $P+\sigma^2$, then if n real variables are transmitted, the total volume occupied by the space of output signals is the volume of a sphere of radius $\sqrt{n(P+\sigma^2)}$, or

$$\text{total volume} = V_n \cdot \left(n(P+\sigma^2)\right)^{n/2} \ . \tag{2.82}$$

We will decode a received message as the signal state that is the minimal distance away. Consider averaging over all codes that satisfy the power constraint and have m signals. When a message is received, the signal that was sent will typically occupy a decoding sphere of radius $\sqrt{(n(\sigma^2+\varepsilon)}$ centered at the received message, which has volume

$$\text{decoding sphere volume} = V_n \cdot \left(n(\sigma^2+\varepsilon)\right)^{n/2} \ . \tag{2.83}$$

A decoding error can arise if another one of the m signals, aside from the one that was sent, is also contained in the decoding sphere. The probability that a randomly selected signal inside the sphere of radius $\sqrt{n(P+\sigma^2)}$ is contained in a particular decoding sphere of radius $\sqrt{n(\sigma^2+\varepsilon)}$ is the ratio of the volume of the spheres, so the probability of a decoding error can be upper bounded by m times

that ratio, or

$$P_{\text{error}} < m \cdot \left(\frac{\sigma^2 + \varepsilon}{\sigma^2 + P} \right)^{n/2} = \left(2^{2R} \cdot \frac{\sigma^2 + \varepsilon}{\sigma^2 + P} \right)^{n/2} \ , \tag{2.84}$$

where R is the rate of the code. If the probability of error averaged over codes and signals satisfies this bound, there is a particular code that satisfies the bound when we average only over signals. If $P_{\text{error}} < \delta$ when we average over signals, then we can discard at most half of all the signals (reducing the rate by at most $1/n$ bits) to obtain a new code with $P_{\text{error}} < 2\delta$ for *all* signals. Since ε can be chosen arbitrarily small for sufficiently large n, we conclude that there exist codes with arbitrarily small probability of error and rate R arbitrarily close to

$$C = \frac{1}{2} \log_2 \left(1 + \frac{P}{\sigma^2} \right) \ , \tag{2.85}$$

which is the Shannon capacity. Conversely, for any rate exceeding C, the decoding spheres inevitably have nonnegligible overlaps, and the error rate cannot be arbitrarily small.

Suppose that, instead of Shannon's random coding, we use a lattice code based on an efficient packing of spheres. In this case, the power constraint can be imposed by including as signals all lattice sites that are contained in an n-dimensional ball of radius $\sqrt{nP}$, and the typical shifts by distance $\sqrt{n\sigma^2}$ must be correctable. Thus decoding spheres of radius $\sqrt{n\sigma^2}$ are to be packed into a sphere of total radius $\sqrt{n(P + \sigma^2)}$. Suppose that the lattice is chosen so that nonoverlapping spheres centered at the lattice sites fill a fraction at least $2^{-(n-1)}$ of the total volume; the existence of such a lattice is established by Minkowski's estimate [61]. Then the number m of signals satisfies

$$m \cdot V_n \cdot (n\sigma^2)^{n/2} \geq 2^{-(n-1)} \cdot V_n \cdot \left(n(P + \sigma^2) \right)^{n/2} \ , \tag{2.86}$$

or

$$m \geq 2^{-n} \left(1 + \frac{P}{\sigma^2}\right)^{n/2} , \tag{2.87}$$

corresponding to the rate

$$R \equiv \frac{1}{n} \cdot \log_2 m = \frac{1}{2} \log_2 \left(1 + \frac{P}{\sigma^2}\right) - 1 , \tag{2.88}$$

which is one bit less than the Shannon capacity.

Much as in the discussion of quantum lattice codes in Sec. 2.6, an improved estimate of the achievable rate is obtained if we allow the decoding spheres to overlap [23, 24, 53, 83]. In fact, there are classical lattice codes with rate arbitrarily close to the capacity, such that the probability of error, *averaged* over signals, is arbitrarily small [83]. Unfortunately, though, because of the power constraint, the error probability depends on which signal is sent, and the trick of deleting the worst half of the signals would destroy the structure of the lattice. Alternatively, it can be shown that for any rate

$$R < \frac{1}{2} \log_2 (P/\sigma^2) , \tag{2.89}$$

there are lattice codes with maximal probability of error that is arbitrarily small [23]. This achievable rate approaches the capacity for large P/σ^2.

Now consider the rates that can be achieved for the Gaussian classical channel with concatenated coding. A d-state system (dit) is encoded in each of n real variables. If each real variable takes one of d possible values, with spacing $2\Delta x$ between the signals, then a shift by Δx can be corrected. By replacing the sum over d values by an integral, which can be justified for large d, we find an average power per signal

$$P \sim \frac{1}{2d\Delta x} \int_{-d\Delta x}^{d\Delta x} x^2 dx = \frac{1}{3} (d\Delta x)^2 ; \tag{2.90}$$

thus the largest correctable shift can be expressed in terms of the average power

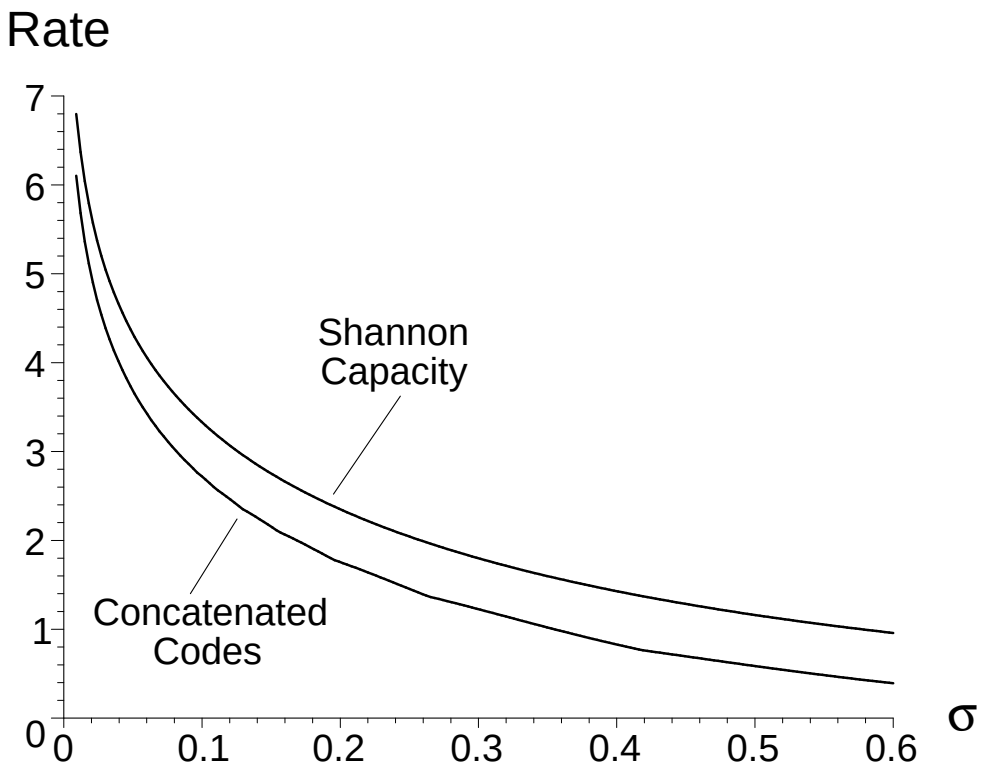

Figure 2.4: Rates for the Gaussian classical channel achievable with concatenated codes, compared to the Shannon capacity. Here σ is the standard deviation of the displacement, in units with the power $P = 1$.

as

$$\Delta x = \sqrt{3P}/d \ . \tag{2.91}$$

For the Gaussian channel with mean zero and variance σ^2, the probability p of an error in each real variable transmitted is no larger than the probability of a shift by a distance exceeding Δx, or

$$p \leq \mathrm{erfc}\left(\sqrt{3P/2d^2\sigma^2}\right) \ , \tag{2.92}$$

where erfc denotes the complementary error function.

We reduce the error probability further by encoding $k < n$ dits in the block of n dits. Arguing as in Sec. 2.7, we see that a random code for dits achieves an asymptotic rate in bits given by

$$R = \log_2 d \cdot (1 - H_d(p) - p \log_d(d-1)) \ . \tag{2.93}$$

Given σ^2, using the expression eq. (2.92) for p, and choosing d to optimize the rate in eq. (2.93), we obtain a rate close to the Shannon capacity, as shown in Figure 2.4. As for the concatenated quantum code, the rate of the concatenated classical code is close to $\log_2 d$, where $d \sim C(\sigma^2) \cdot \sqrt{P/\sigma^2}$, and $C(\sigma^2)$ is a slowly varying function.

2.9 Conclusions

We have described quantum stabilizer codes, based on symplectic integral lattices in phase space, that protect quantum information carried by systems described by continuous quantum variables. With these codes, we can establish lower bounds on the capacities of continuous-variable quantum channels.

For the Gaussian quantum channel, the best rate we know how to achieve with stabilizer coding matches the one-shot coherent information optimized over Gaussian inputs, at least when the value of the coherent information is $\log_2$ of an integer. That our achievable rate matches the coherent information only for isolated values of the noise variance σ^2 seems to be an artifact of our method of analysis, rather than indicative of any intrinsic property of the channel. Hence it is tempting to speculate that this optimal one-shot coherent information actually is the quantum capacity of the channel. Sam Thomsen continued this line of work as a SURF project during the summer of 2002. He found a way to modify the Buser-Sarnak theorem [17] that seems to show the existence of symplectic lattices whose achievable rates would match the coherent information everywhere our proof is

valid (specifically, for small σ).

Conceivably, better rates can be achieved with *nonadditive* quantum codes that cannot be described in terms of symplectic integral lattices. We don't know much about how to construct these codes, or about their properties.

In the case of the depolarizing channel acting on qubits, Shor and Smolin discovered that rates exceeding the one-shot coherent information could be achieved. Their construction used concatenated codes, where the "outer code" is a random stabilizer code, and the "inner code" is a degenerate code with a small block size [27]. The analogous procedure for the Gaussian channel would be to concatenate an outer code based on a symplectic integral lattice with an inner code that encodes one logical oscillator in a block of several oscillators. This inner code, then, embeds an infinite-dimensional code space in a larger infinite-dimensional space, as do codes constructed by Braunstein [16] and Lloyd and Slotine [56]. However, we have not been able to find concatenated codes of this type that achieve rates exceeding the one-shot coherent information of the Gaussian channel.

Chapter 3

Family of symplectic self-dual lattice codes

3.1 Abstract

The continuous variable quantum error-correcting codes introduced in [38] provide a means for robustly storing and processing quantum information in systems described by harmonic oscillators, such as a mode of light. These codes protect the encoded information from random kicks to the oscillator variables, provided that the magnitude of the kicks is not too strong. In this work, we present several explicit encodings and calculate their achievable rates over the Gaussian quantum channel. These encodings were found by searching for symplectic self-dual lattices with large minimum distance, and we present the general algorithm used to construct these codes.

3.2 Introduction

Lattice (or oscillator) quantum error-correcting codes for continuous quantum variables were defined in Section 2.4. In Section 3.3 we present a general mapping of a d-dimensional quantum system into N oscillators, which is defined by a symplectic integral lattice in $\mathbb{R}^{2N}$. We restrict ourselves to a parameterization of symplectic

self-dual lattices with $3N$ real parameters in Section 3.4, and present a program to search for "good" instances. The results of our search for $1 \leq N \leq 6$ are described in Section 3.5, and the error-correcting properties of several of these codes over the Gaussian quantum channel are analyzed in Section 3.6. We conclude with a presentation of the achievable rates over this channel in Section 3.7.

3.3 Constructing oscillator codes

Consider a system of N oscillators whose canonical variables $\{\hat{p}_j, \hat{q}_j\}$ satisfy the commutation relation $[\hat{p}_j, \hat{q}_k] = i\delta_{jk}$. We can define vectors $\vec{p} = (\hat{p}_1, \hat{p}_2, \ldots, \hat{p}_N)$ and $\vec{q} = (\hat{q}_1, \hat{q}_2, \ldots, \hat{q}_N)$.

Let $\vec{x}_j, \vec{y}_j \in \mathbb{R}^N$ for $1 \leq j \leq 2N$. If $\forall j, k$

$$(\vec{x}_j \cdot \vec{y}_k - \vec{x}_k \cdot \vec{y}_j) \in \mathbb{Z}\,, \tag{3.1}$$

then for any $d \in \mathbb{Z}^+$, we can define a code with the following set of stabilizers:

$$\begin{aligned} S_1 &= \exp\left\{i\sqrt{2\pi d}\,(\vec{x}_1 \cdot \vec{q} + \vec{y}_1 \cdot \vec{p})\right\} \\ S_2 &= \exp\left\{i\sqrt{2\pi d}\,(\vec{x}_2 \cdot \vec{q} + \vec{y}_2 \cdot \vec{p})\right\} \\ &\vdots \\ S_j &= \exp\left\{i\sqrt{2\pi d}\,(\vec{x}_j \cdot \vec{q} + \vec{y}_j \cdot \vec{p})\right\} \\ &\vdots \\ S_{2N} &= \exp\left\{i\sqrt{2\pi d}\,(\vec{x}_{2N} \cdot \vec{q} + \vec{y}_{2N} \cdot \vec{p})\right\} \end{aligned} \tag{3.2}$$

The normalizer for this stabilizer code has a basis of $2N$ operators of the form

$$\bar{S}_j = \exp\left\{i\sqrt{\frac{2\pi}{d}}\,(\vec{x}_j \cdot \vec{q} + \vec{y}_j \cdot \vec{p})\right\}. \tag{3.3}$$

Note that the stabilizer operators commute with one another, as well as with

the normalizer operators:

$$S_j S_k \;=\; \exp\left\{2\pi i d(\vec{x}_j \cdot \vec{y}_k - \vec{x}_k \cdot \vec{y}_j)\right\} S_k S_j \;=\; S_k S_j \tag{3.4}$$

$$\bar{S}_j S_k \;=\; \exp\left\{2\pi i (\vec{x}_j \cdot \vec{y}_k - \vec{x}_k \cdot \vec{y}_j)\right\} S_k \bar{S}_j \;=\; S_k \bar{S}_j \tag{3.5}$$

We can express the relations given by equation (3.1) more compactly in the following manner. Suppose we glue each pair of vectors $\vec{x}_j$ and $\vec{y}_j$ together into a single vector $\vec{v}_j \in \mathbb{R}^{2N}$ as

$$\vec{v}_j \;\equiv\; (x_j^{(1)}, x_j^{(2)}, \ldots, x_j^{(N)}, y_j^{(1)}, y_j^{(2)}, \ldots, y_j^{(N)}) \tag{3.6}$$

where $x_j^{(k)}$ and $y_j^{(k)}$ are the kth components of $\vec{x}_j$ and $\vec{y}_j$, respectively.

Let $J \equiv \begin{pmatrix} 0 & I_N \\ -I_N & 0 \end{pmatrix}$, where I_N is the $N \times N$ identity matrix. We can define the *symplectic inner product* of vectors $\vec{v}_j$ and $\vec{v}_k$ to be

$$\omega(\vec{v}_j, \vec{v}_k) \;\equiv\; \vec{v}_j^{\mathrm{T}} J \vec{v}_k \;=\; \vec{x}_j \cdot \vec{y}_k - \vec{x}_k \cdot \vec{y}_j \,. \tag{3.7}$$

Thus, we can define a stabilizer code that embeds a d-dimensional codespace into the system of N oscillators for any choice of $2N$ vectors $\vec{v}_j \in \mathbb{R}^{2N}$ satisfying

$$\omega(\vec{v}_j, \vec{v}_k) \in \mathbb{Z} \;\forall j, k \,. \tag{3.8}$$

This code can correct any phase space shift that lies within the origin's *Voronoi cell* of the normalizer lattice (the region of points located closer to the origin than any other lattice point). This implies that we want to find a lattice whose basis vectors satisfy equation (3.8) with a large minimum distance between lattice points. If we can find a self-dual lattice code (whose stabilizer and normalizer lattices coincide), we can then scale by $\sqrt{d}$, for any postive integer d.

3.4 Program

In this section we present an algorithm for finding good symplectic self-dual codes. The parameterization described below may or may not encompass the entire set of symplectic self-dual lattices, but we have found that our implementation of searching through this parameter space has converged on the best-known symplectic self-dual lattices in even dimensions 2 through 12. This lends some support to the conjecture that the parameterization below always includes the optimal symplectic lattices.

3.4.1 Parameterization

First, consider $4N$ real parameters, which we will denote as $\{\alpha_1, \alpha_2, \ldots, \alpha_N\}$, $\{\beta_1, \beta_2, \ldots, \beta_N\}$, $\{\gamma_1, \gamma_2, \ldots, \gamma_N\}$, and $\{\delta_1, \delta_2, \ldots, \delta_N\}$. Let us define the following set of $4N$ vectors in $\mathbb{R}^N$ (with $1 \leq j \leq N$):

$$\begin{aligned}
\vec{a}_j &= (\alpha_j, \alpha_{j+1}, \ldots, \alpha_N, \alpha_1, \ldots, \alpha_{j-1}) \\
\vec{b}_j &= (\beta_j, \beta_{j+1}, \ldots, \beta_N, \beta_1, \ldots, \beta_{j-1}) \\
\vec{c}_j &= (\gamma_j, \gamma_{j+1}, \ldots, \gamma_N, \gamma_1, \ldots, \gamma_{j-1}) \\
\vec{d}_j &= (\delta_j, \delta_{j+1}, \ldots, \delta_N, \delta_1, \ldots, \delta_{j-1})
\end{aligned}$$

To simplify notation, we will also identify $\vec{a}_0 \equiv \vec{a}_N$, $\vec{b}_0 \equiv \vec{b}_N$, $\vec{c}_0 \equiv \vec{c}_N$, $\vec{d}_0 \equiv \vec{d}_N$.

Note that the Euclidean inner product of certain pairs of these vectors are

identical (since they involve cyclic shifts of one another). For example:

$$\begin{aligned}
\vec{a}_j \cdot \vec{b}_{N-k+1} &= \sum_{l=1}^{N} \left(\alpha_{(l+j) \bmod N}\right) \left(\beta_{(l-k+1) \bmod N}\right) \\
&= \sum_{l=1}^{N} \left(\alpha_{(l+j+k) \bmod N}\right) \left(\beta_{(l+1) \bmod N}\right) \\
&= \sum_{l=1}^{N} \left(\alpha_{(l+k) \bmod N}\right) \left(\beta_{(l-j+1) \bmod N}\right) \\
\vec{a}_j \cdot \vec{b}_{N-k+1} &= \vec{a}_k \cdot \vec{b}_{N-j+1}
\end{aligned} \tag{3.9}$$

Similarly, for any j and k, $\vec{c}_{N-k+1} \cdot \vec{d}_j = \vec{c}_{N-j+1} \cdot \vec{d}_k$.

Next, let us define four $N \times N$ matrices:

$$M_1 = \begin{pmatrix} \longleftarrow \vec{a}_1 \longrightarrow \\ \longleftarrow \vec{a}_2 \longrightarrow \\ \vdots \\ \leftarrow \vec{a}_{N-1} \rightarrow \\ \longleftarrow \vec{a}_N \longrightarrow \end{pmatrix}, \quad M_2 = \begin{pmatrix} \longleftarrow \vec{b}_N \longrightarrow \\ \leftarrow \vec{b}_{N-1} \rightarrow \\ \vdots \\ \longleftarrow \vec{b}_2 \longrightarrow \\ \longleftarrow \vec{b}_1 \longrightarrow \end{pmatrix}$$

$$M_3 = \begin{pmatrix} \longleftarrow \vec{c}_N \longrightarrow \\ \leftarrow \vec{c}_{N-1} \rightarrow \\ \vdots \\ \longleftarrow \vec{c}_2 \longrightarrow \\ \longleftarrow \vec{c}_1 \longrightarrow \end{pmatrix}, \quad M_4 = \begin{pmatrix} \longleftarrow \vec{d}_1 \longrightarrow \\ \longleftarrow \vec{d}_2 \longrightarrow \\ \vdots \\ \leftarrow \vec{d}_{N-1} \rightarrow \\ \longleftarrow \vec{d}_N \longrightarrow \end{pmatrix}$$

Note that successive rows of M_1 and M_4 are left-shifted, and successive rows of M_2 and M_3 are right-shifted. Because of the relations given in equation (3.9), gluing together the matrices M_1 and M_2 gives a matrix in which any pair of rows has a symplectic inner product of zero. Gluing together M_3 and M_4 produces row vectors with the same property. This leads us to construct the following matrix as

a candidate for a basis of a symplectic lattice:

$$M = \begin{pmatrix} M_1 & M_2 \\ M_3 & M_4 \end{pmatrix} \tag{3.10}$$

We can enforce the constraints $\det M = 1$ and $MJM^T = J$ (so that M is in standard form, as described by equation (2.38) in Section 2.4) by choosing:

$$\begin{pmatrix} \delta_1 \\ \delta_2 \\ \vdots \\ \delta_N \end{pmatrix} = M_1^{-1} \left[M_2 \begin{pmatrix} \gamma_1 \\ \gamma_2 \\ \vdots \\ \gamma_N \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \right] \tag{3.11}$$

Any pair of rows of M then has an integral symplectic inner product. The rows of M play two distinct roles. They form a set of basis vectors for a symplectic self-dual lattice, and they also form a set of vectors $\vec{v}_j$ satisfying equation (3.8), which can be used to define the stabilizer code described by equation (3.2).

3.4.2 Algorithm

Consequently, we have the following program for searching for good self-dual symplectic lattices:

1. Choose values for the $3N$ free parameters $\{\alpha_j, \beta_j, \gamma_j\}$ (*e.g.,* initially at random and later by perturbing some or all of the parameters away from the currently best-known values).

2. Solve for $\{\delta_j\}$ by equation (3.11), and construct M as given by equation (3.10). Consider the rows of M to be a basis for a lattice in $\mathbb{R}^{2N}$.

3. Compute a "reduced basis" for the lattice by the LLL algorithm [51]. This algorithm has running time $O(N^{12})$ and constructs a set of basis vectors that are all at least 60° apart from one another.

4. Find the (approximately) closest lattice point to the origin by exhausting over adding and subtracting the reduced basis vectors.

5. If the minimum distance of the lattice is larger than in previous rounds, save the values of the free parameters as the currently best-known. Return to step one.

Computing the closest lattice point to the origin, given a basis for a lattice, is in general a hard problem [3, 60]. We only perform an approximate computation in our code, but we are fairly confident that it is accurate in practice, because our program converged toward several lattices, such as D_4 and E_8 (see Section 3.5), that are suspected to be optimal among all Euclidean lattices (not just among symplectic lattices).

The initial values of the free parameters can be chosen more or less at random. The only constraint is that the rows of M need to be linearly independent. This program (which introduces perturbations away from the currently best-known values during each round) is basically a simulated annealing process, which may converge toward local maxima in the parameter space, so it is necessary to start at various initial positions or provide ways to move away from these localized traps. We found that instead of isolated global maxima, there appears to be a continuous curve (or perhaps even multi-dimensional surface) in the parameter space that defines symplectic lattices with the optimal minimum distance. This suggests that there are further symmetries in our parameterization (probably of a rotational nature) that are not being utilized. One explicit expression of such a symmetry is exhibited for D_4 in the next section, which was found with the help of Dave Beckman [9].

Table 3.1: Best-known symplectic self-dual lattices

lattice	(min. dist.)^4	min. dist.
A_2	$\frac{4}{3}$	1.075
D_4	2	1.189
F_6	$\frac{12}{5}$	1.245
E_8	4	1.414
D_{10}	4	1.414
K_{12}	$\frac{16}{3}$	1.520

3.5 Results

The symplectic self-dual lattices with largest known minimum distances are given in Table 3.1 (see also Table A.3). All of the lattice notations follow that of Conway and Sloane [21], except for the six-dimensional lattice F_6, which belongs to Bavard's family of lattices presented in appendix A.

These best-known symplectic self-dual lattices correspond to optimal Euclidean lattices, except in dimensions 6 and 10, where E_6 has minimum distance $(\frac{64}{3})^{\frac{1}{12}} \approx 1.290$ and P_{10_c} has minimum distance $(40)^{\frac{1}{10}} \approx 1.446$ [21]. Furthermore, it has been claimed that the Barnes-Wall lattice Λ_{16} and the Leech lattice Λ_{24}, which are presumed to be optimal among lattices in dimensions 16 and 24 (with minimum distances $(2)^{\frac{3}{4}} \approx 1.682$ and 2, respectively), can be expressed as symplectic lattices (see appendix of [17]). However, it remains an open question of finding a symplectic basis for these lattices whose generator matrix has determinant 1. Nevertheless, we conjecture that in dimensions that are a multiple of four, the optimal symplectic self-dual lattices correspond to optimal Euclidean lattices. Rains has an argument in favor of this in terms of searching for Hermitian lattices over $\mathbb{Z}[\sqrt{-n}\,]$ (the ring of integers extended by the number $\sqrt{-n}$) for various values of n [73]. It is also interesting to note that the minimum distances of each of these optimal symplectic

lattices is the fourth root of a rational number (see Table A.3 for more examples).

We can explicitly show a symplectic self-dual form for most of these lattices. Any two-dimensional self-dual lattice is automatically symplectic, because the symplectic inner product of the two rows of its basis matrix is simply equal to its determinant, which is one, by definition. We can represent A_2 as:

$$A_2 = \frac{1}{\sqrt[4]{12}} \begin{pmatrix} 2 & 0 \\ 1 & \sqrt{3} \end{pmatrix}$$

For D_4, we first will choose parameters to define a rotation matrix in $O(4)$. Let $a, b \in (0, \frac{1}{\sqrt{2}})$ with $a \neq b$, and let $m, n \in \{\pm 1\}$. We then define:

$$\begin{aligned} c &= \pm\sqrt{\frac{1}{2} - a^2}\,, & d &= \pm\sqrt{\frac{1}{2} - b^2} \\ e &= -\frac{1}{\sqrt{2}}(am - bn)\,, & f &= -\frac{1}{\sqrt{2}}(am + bn) \\ g &= -\frac{ac}{e+f} - \frac{bd}{e-f}\,, & h &= -\frac{ac}{e+f} + \frac{bd}{e-f} \end{aligned}$$

We can now express D_4 in a rotated version of its standard basis:

$$D_4 = \frac{1}{\sqrt[4]{8}} \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} a & a & c & c \\ b & -b & d & -d \\ g & h & e & f \\ h & g & f & e \end{pmatrix}$$

For F_6, we simply provide a numerical basis found by our search program (along with the reduced lattice given by the LLL algorithm [51]), which was found later

to match the geometry of a member of Bavard's family of lattices:

$$F_6 = \begin{pmatrix} 0.83490 & 0.18699 & -0.11630 & 0.64916 & 0.50833 & 0.35192 \\ 0.18699 & -0.11630 & 0.83490 & 0.35192 & 0.64916 & 0.50833 \\ -0.11630 & 0.83490 & 0.18699 & 0.50833 & 0.35192 & 0.64916 \\ 1.88321 & 0.46591 & 1.01245 & 3.06472 & 2.24387 & 1.39866 \\ 1.01245 & 1.88321 & 0.46591 & 2.24387 & 1.39866 & 3.06472 \\ 0.46591 & 1.01245 & 1.88321 & 1.39866 & 3.06472 & 2.24387 \end{pmatrix}$$

$$F_6' = \begin{pmatrix} 0.83490 & 0.18699 & -0.11630 & 0.64916 & 0.50833 & 0.35192 \\ 0.18699 & -0.11630 & 0.83490 & 0.35192 & 0.64916 & 0.50833 \\ -0.11630 & 0.83490 & 0.18699 & 0.50833 & 0.35192 & 0.64916 \\ -0.16057 & 0.32454 & -0.42474 & 1.06257 & -0.07111 & -0.32183 \\ 0.22317 & 0.14273 & -0.62666 & 0.22613 & -0.46266 & 0.90616 \\ 0.02124 & 0.52646 & -0.80847 & -0.16542 & 0.76533 & 0.06972 \end{pmatrix}$$

$$(F_6')(F_6')^{\mathrm{T}} = \frac{1}{15} \begin{pmatrix} 6 & 3 & 3 & 2 & 2 & 2 \\ 3 & 6 & 3 & -1 & -1 & -1 \\ 3 & 3 & 6 & 2 & 2 & 2 \\ 2 & -1 & 2 & 6 & 1 & 1 \\ 2 & -1 & 2 & 1 & 6 & 1 \\ 2 & -1 & 2 & 1 & 1 & 6 \end{pmatrix}$$

The actual parameters output by our program are reported to around 14 significant digits, and they agree with the Euclidean inner products reported above to better than 1 part in 10^9. Similar convergence was observed for the other lattices (although somewhat less in higher dimensions, due to the greatly increased running time required to search in the larger parameter spaces).

E_8 is symplectic self-dual in its standard basis:

$$E_8 = \frac{1}{2}\begin{pmatrix} 2 & -2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & -2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & -2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & -2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & -2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & -2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & -2 \\ 1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 \end{pmatrix}$$

For K_{12}, we express it in block matrix form, after first defining two submatrices:

$$X_6 = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & -1 \\ 1 & 0 & 1 & 1 & 1 & -1 \\ 1 & 1 & 0 & 1 & 1 & -1 \\ 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$

$$Y_6 = \sqrt{3}\begin{pmatrix} -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$K_{12} = \frac{1}{\sqrt[4]{12}}\begin{pmatrix} X_6 & Y_6 \\ \frac{1}{2}\left(X_6 + \sqrt{3}Y_6\right) & \frac{1}{2}\left(Y_6 - \sqrt{3}X_6\right) \end{pmatrix}$$

3.6 Error models

Given a $2N$-dimensional symplectic self-dual lattice described by basis matrix M, we can construct a stabilizer code encoding N qudits (d-dimensional quantum systems) into N oscillators. The stabilizer lattice, with basis operators S_j given by equation (3.2), is simply $\sqrt{d}M$, and the normalizer lattice, with basis operators $\bar{S}_j$ given by equation (3.3), is simply $\frac{1}{\sqrt{d}}M$.

Let $A = MJM^T$ be the Gram matrix of M, where $J = \begin{pmatrix} 0 & I_N \\ -I_N & 0 \end{pmatrix}$, and let $\omega = \exp\{2\pi i/d\}$ be a dth root of unity. We can compute the commutation relations of the normalizer basis operators:

$$\bar{S}_j \bar{S}_k = \omega^{A_{jk}} \bar{S}_k \bar{S}_j \tag{3.12}$$

We can then assign any set of independent logical operators (which act nontrivially on the N encoded qudits) to the normalizer basis operators $\bar{S}_j$, as long as they obey the above commutation relations. We will restrict ourselves to tensor products of generalized Pauli operators (of the form $Z^a X^b$, for some integers a, b).

If the probability of a shift in phase space is governed by a Gaussian distribution (as in the Gaussian quantum channel, which was described in Section 2.3), we may be able to consider just the nearest (first shell) lattice points about the origin in the normalizer lattice, in order to identify what errors typically occur when error correction fails. In the following subsections, we examine some logical operator assignments to the smallest normalizer basis elements and consider how the Gaussian channel acting on the oscillators is transformed into an effective channel on the encoded qudits.

3.6.1 The square lattice Z_2

As comparison, we first consider the simplest encoding of a qudit into an oscillator (see Section VIII of [38] for more detailed calculations). The Z_2 lattice is

rectangular with minimum distance 1 between lattice points. A basis for the lattice is given by the rows of $M = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, and its Gram matrix (which contains the symplectic inner product relations) is $A = MJM^T = J = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$. Note that $S_1 = \exp\left\{i\sqrt{2\pi d}\hat{p}\right\}$ and $S_2 = \exp\left\{i\sqrt{2\pi d}\hat{q}\right\}$. See Figure 3.1 for a picture of this lattice.

We can associate with $\bar{S}_1$ and $\bar{S}_2$ any pair of Pauli operators acting on a qudit that obey $\bar{S}_1\bar{S}_2 = \omega\bar{S}_2\bar{S}_1$. For example, let $\bar{S}_1 = \bar{Z}$ and let $\bar{S}_2 = \bar{X}$. The nearest points to the origin in the Z_2 normalizer lattice are then associated with $\bar{Z}, \bar{X}, \bar{Z}^{-1}$, and $\bar{X}^{-1}$. Under the Gaussian quantum channel, the probability of kicks in phase space with large magnitude is greatly suppressed. If typical shifts have a magnitude less than half the minimum distance of the normalizer lattice (which is $1/\sqrt{d}$ for Z_2), then on the rare occasions that error correction fails due to an atypically large shift, it is most likely that the resulting logical error will be one of these four (which are equally likely to occur).

Let p_{fail} be the probability that there is a kick in the oscillator's phase space that extends beyond the Voronoi cell about the origin (which for Z_2's normalizer lattice is a square of side length $1/\sqrt{d}$ centered about the origin). Effectively, the Gaussian quantum channel is then converted into a Pauli channel described by

$$\rho \longrightarrow (1 - p_{fail})\rho + \left(\frac{p_{fail}}{4}\right)\left(\bar{Z}\rho\bar{Z}^{-1} + \bar{Z}^{-1}\rho\bar{Z} + \bar{X}\rho\bar{X}^{-1} + \bar{X}^{-1}\rho\bar{X}\right) . \quad (3.13)$$

For qubits ($d = 2$), this is just the binary independent Pauli channel (if we ignore higher order terms in p_{fail}). The next few closest points in the normalizer lattice could also be included, but this would only be needed for noisier Gaussian channels (or for larger d). (These additional error terms are included when we calculate achievable rates in the regime of high noise.)

3.6.2 The hexagonal lattice A_2

The A_2 lattice corresponds to the densest packing of spheres in two dimensions. As seen previously, we can express its basis vectors as the rows of $M = \frac{1}{\sqrt[4]{12}}\left(\begin{smallmatrix} 2 & 0 \\ 1 & \sqrt{3} \end{smallmatrix}\right)$,

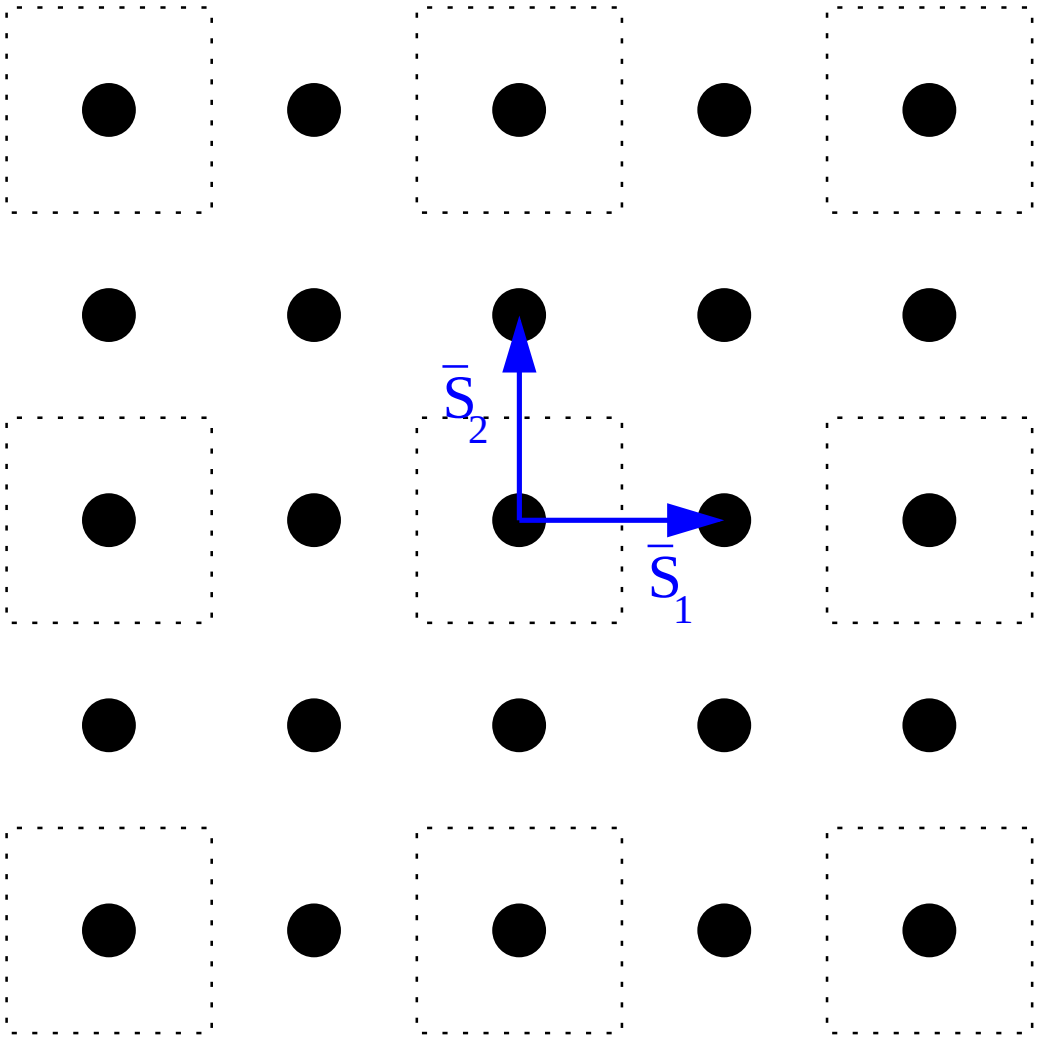

Figure 3.1: The normalizer lattice of the Z_2 encoding. The black circles denote the lattice points. The stabilizer lattice is a sublattice of the normalizer lattice (shown here with $d = 2$). The Voronoi cells of the stabilizer lattice points are indicated by dashed lines. The normalizer basis elements $\bar{S}_1$ and $\bar{S}_2$ are drawn in blue.

and like Z_2, its Gram matrix is $A = MJM^T = J = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$. See Figure 3.2 for a picture of this lattice.

The Voronoi cell of the normalizer lattice of A_2 is a hexagon, and there are six points of minimum distance from any lattice point. If a sphere (circle) with diameter $\sqrt[4]{12}$ was centered about every lattice point of A_2, its *kissing number* would be six. Since $\bar{S}_1\bar{S}_2 = \omega\bar{S}_2\bar{S}_1$, we can choose $\bar{S}_1 = \bar{Z}$ and $\bar{S}_2 = \bar{X}$. The six points closest to the origin are then represented by (in counterclockwise order) $\bar{Z}, \bar{X}, \bar{Z}^{-1}\bar{X}, \bar{Z}^{-1}, \bar{X}^{-1}$, and $\bar{Z}\bar{X}^{-1}$. If we are encoding qubits ($d = 2$), this is simply the depolarizing channel, with equiprobable $\bar{X}$, $\bar{Y}$, and $\bar{Z}$ errors. For larger d, the effective channel is a Pauli channel with six distinct and equiprobable errors (other than the identity).

3.6.3 The checkerboard lattice D_4

For the single oscillator encodings (with two-dimensional lattices), the effective error channel is unique up to symmetries in our choice of assigning the logical operators $\bar{S}_1$ and $\bar{S}_2$. However, for D_4 and higher dimensions, we will find that there are distinct choices.

The D_4 lattice has a kissing number of 24. (If the lattice points are centers of spheres with diameter $\sqrt[4]{2}$, then 24 spheres touch each sphere.) We can choose a basis M for the D_4 lattice such that its Gram matrix is $A = MJM^T = J$. This tells us that $\bar{S}_1\bar{S}_3 = \omega\bar{S}_3\bar{S}_1$ and $\bar{S}_2\bar{S}_4 = \omega\bar{S}_4\bar{S}_2$, while all other pairings of basis normalizer operators commute.

We exhaustively find that there are 17312 ways consistent with the commutation relations to map 2-qudit Pauli operators (of the form $(Z^aX^b) \otimes (Z^cX^d)$ with $a, b, c, d \in \{-1, 0, 1\}$) to these basis elements. (If we restrict to qubits, there are 720 distinct mappings.) Some of the error operators are correlated errors on the two encoded qudits, and others act nontrivially on just one of the qudits. If we ignore any correlations between the qudits (which can only decrease the achievable rate by throwing away some knowledge of the errors), we could consider what

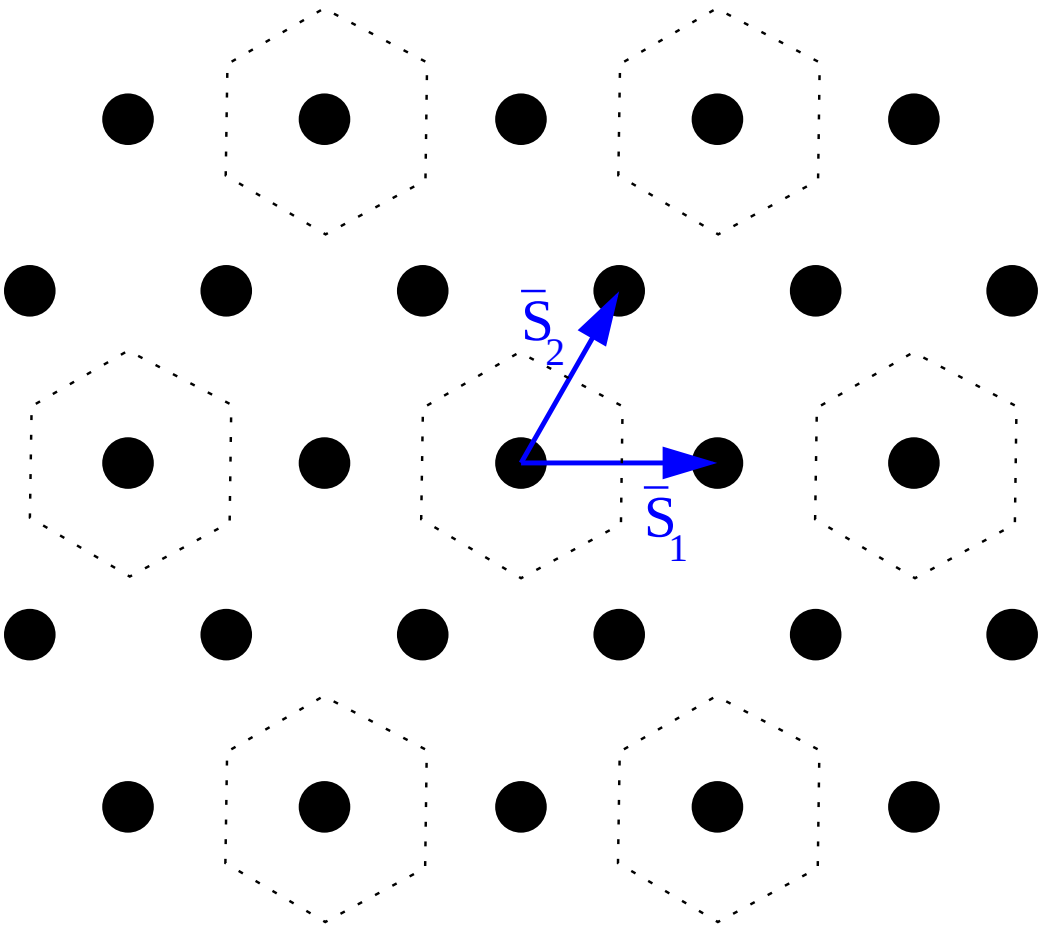

Figure 3.2: The normalizer lattice of the A_2 encoding. The black circles denote the lattice points. The stabilizer lattice is a sublattice of the normalizer lattice (shown here with $d = 2$). The Voronoi cells of the stabilizer lattice points are indicated by dashed lines. The normalizer basis elements $\bar{S}_1$ and $\bar{S}_2$ are drawn in blue.

the effective channel is on each encoded qudit separately. When we examine the resulting logical errors of the 24 nearest points in the normalizer lattice, we find that there are only two distinct effective channels, once symmetries are accounted for.

As an example with qubits ($d = 2$), we could choose $\bar{S}_1 = \bar{Z}_A\bar{Z}_B$, $\bar{S}_2 = \bar{Z}_A\bar{I}_B$, $\bar{S}_3 = \bar{I}_A\bar{X}_B$, $\bar{S}_4 = \bar{X}_A\bar{X}_B$ (acting on qubits A and B). We then find that the logical operators for the normalizer lattice points in the first shell are $\{\bar{I}_A\bar{X}_B$, $\bar{I}_A\bar{Z}_B$, $\bar{X}_A\bar{X}_B$, $\bar{X}_A\bar{Z}_B$, $\bar{Y}_A\bar{I}_B$, $\bar{Y}_A\bar{X}_B$, $\bar{Y}_A\bar{Y}_B$, $\bar{Y}_A\bar{Z}_B$, $\bar{Z}_A\bar{I}_B$, $\bar{Z}_A\bar{X}_B$, $\bar{Z}_A\bar{Y}_B$, $\bar{Z}_A\bar{Z}_B\}$. Looking at each qubit separately, we would expect that when error correction fails, the effective channel is a pair of Pauli channels with the following probabilities:

$$\begin{aligned}
\text{qubit } A:\ p_I &= \left(1 - \frac{5}{6}p_{fail}\right),\ p_X = \frac{1}{6}p_{fail},\ p_Y = \frac{1}{3}p_{fail},\ p_Z = \frac{1}{3}p_{fail} \\
\text{qubit } B:\ p_I &= \left(1 - \frac{5}{6}p_{fail}\right),\ p_X = \frac{1}{3}p_{fail},\ p_Y = \frac{1}{6}p_{fail},\ p_Z = \frac{1}{3}p_{fail}
\end{aligned}$$

Or, we could assign instead $\bar{S}_1 = \bar{Z}_A\bar{I}_B$, $\bar{S}_2 = \bar{I}_A\bar{Z}_B$, $\bar{S}_3 = \bar{X}_A\bar{I}_B$, $\bar{S}_4 = \bar{I}_A\bar{X}_B$, in which case the most likely errors become $\{\bar{I}_A\bar{X}_B$, $\bar{I}_AY_B$, $\bar{I}_A\bar{Z}_B$, $\bar{X}_A\bar{I}_B$, $\bar{X}_A\bar{X}_B$, $\bar{X}_AY_B$, $Y_A\bar{I}_B$, Y_AY_B, $Y_A\bar{Z}_B$, $\bar{Z}_A\bar{I}_B$, $\bar{Z}_A\bar{X}_B$, $\bar{Z}_A\bar{Z}_B\}$. This leads to effective error channels described by:

$$\begin{aligned}
\text{qubit } A:\ p_I &= \left(1 - \frac{3}{4}p_{fail}\right),\ p_X = \frac{1}{4}p_{fail},\ p_Y = \frac{1}{4}p_{fail},\ p_Z = \frac{1}{4}p_{fail} \\
\text{qubit } B:\ p_I &= \left(1 - \frac{3}{4}p_{fail}\right),\ p_X = \frac{1}{4}p_{fail},\ p_Y = \frac{1}{4}p_{fail},\ p_Z = \frac{1}{4}p_{fail}
\end{aligned}$$

It is worth noting that for any value of p_{fail}, the Shannon entropy of the set of probabilities in the first assignment is always higher than in the second, so we can achieve a higher rate with the latter choice.

When encoding qudits with $d > 2$, the best effective channel is similar to the depolarizing channel. For example, with $\bar{S}_1 = \bar{Z}_A\bar{I}_B$, $\bar{S}_2 = \bar{I}_A\bar{Z}_B$, $\bar{S}_3 = \bar{X}_A\bar{I}_B$, $\bar{S}_4 = \bar{I}_A\bar{X}_B$, the resulting error probability vector for each qudit channel is $(1 - \frac{3}{4}p$, $\frac{1}{8}p$, $\frac{1}{8}p$, $\frac{1}{8}p$, $\frac{1}{8}p$, $\frac{1}{8}p$, $\frac{1}{8}p)$ with $p = p_{fail}$.

3.6.4 Bavard's symplectic lattice F_6

Using the expression found by our program for a basis of F_6, its Gram matrix is

$$A \;=\; MJM^T \;=\; \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 & -1 & 0 \\ 0 & -1 & 0 & 1 & 0 & 1 \\ 0 & 0 & -1 & 1 & -1 & 0 \end{pmatrix}.$$

There are too many assignments to exhaust over to find the optimal effective qudit error channels, as we did for D_4. (We generated close to a million unique assignments that are consistent with these commutation relations, but we estimate that this was only about 1% of the possibilities, even with the Pauli operators limited to the form (Z^aX^b) with $a, b \in \{-1, 0, 1\}$.) However, we will present the best effective channel (in terms of lowest Shannon entropy of its probability vectors) that we found. Suppose we set $\bar{S}_1 = \bar{X}_A\bar{X}_B\bar{I}_C$, $\bar{S}_2 = (\bar{Z}\bar{X})_A(\bar{Z}^{-1}\bar{X}^{-1})_B\bar{X}_C$, $\bar{S}_3 = (\bar{Z}^{-1}\bar{X}^{-1})_A\bar{Z}_B(\bar{Z}\bar{X})_C$, $\bar{S}_4 = (\bar{Z}^{-1}\bar{X}^{-1})_A\bar{I}_B\bar{I}_C$, $\bar{S}_5 = \bar{X}_A\bar{I}_B\bar{X}_C$, and $\bar{S}_6 = \bar{I}_A\bar{X}_B(\bar{Z}^{-1}\bar{X}^{-1})_C$. The resulting logical errors associated with the nearest 44 points produce three effective Pauli channels each with error probability vector $(1 - \frac{30}{44}p,\ \frac{6}{44}p,\ \frac{6}{44}p,\ \frac{6}{44}p,\ \frac{6}{44}p,\ \frac{3}{44}p,\ \frac{3}{44}p)$ with $p = p_{fail}$.

3.6.5 The exceptional Lie algebra lattice E_8

There is an incredibly large set of logical operator assignments consistent with required commutation relations for the E_8, and we could only sample a small fraction of these. The E_8 lattice has a kissing number of 240. The best effective error channel we could find (when examining each qudit separately) has an error probability vector $(1 - \frac{168}{240}p,\ \frac{27}{240}p,\ \frac{27}{240}p,\ \frac{27}{240}p,\ \frac{27}{240}p,\ \frac{27}{240}p,\ \frac{27}{240}p,\ \frac{1}{240}p,\ \frac{1}{240}p,\ \frac{1}{240}p,\ \frac{1}{240}p,\ \frac{1}{240}p,\ \frac{1}{240}p)$ with $p = p_{fail}$.

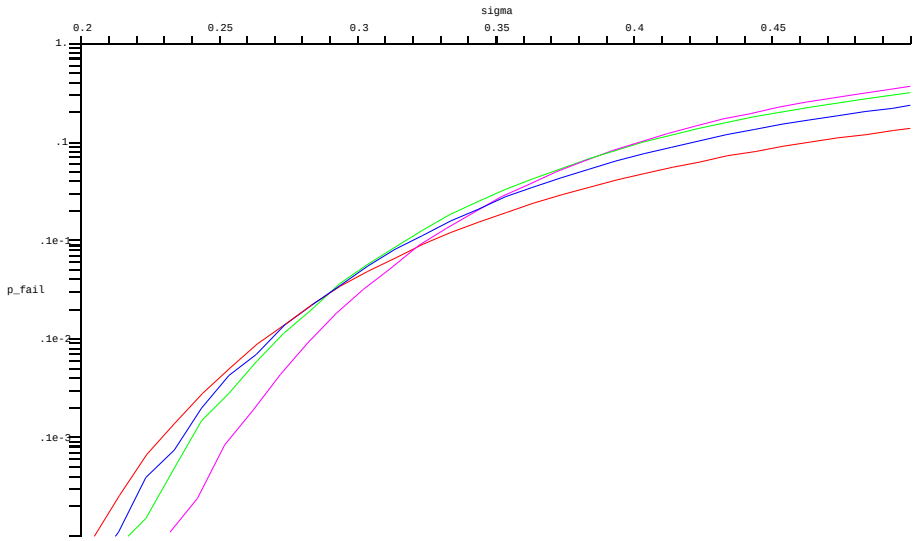

Figure 3.3: Failure probability of A_2, D_4, F_6, and E_8 lattice encodings over the Gaussian channel. Sigma along the horizontal axis denotes the standard deviation of the magnitude of the kicks by the channel in each oscillator's phase space. The red, blue, green, and magenta lines are respectively the plots of the probability of a phase space kick being outside the Voronoi cell of the A_2, D_4, F_6, and E_8 lattice encodings of qubits.

3.7 Achievable rates

In order to compute achievable rates over the Gaussian quantum channel, we first computed (via Monte Carlo simulations) the fidelities of the A_2, D_4, F_6, and E_8 lattice encodings of qubits ($d = 2$). We calculated the failure probability p_{fail} of these encodings by sampling how often a phase space shift governed by a Gaussian distribution fell outside of the Voronoi cell of the origin. Our results are plotted in FIgure 3.3 over a moderate range of the channel's standard deviation σ. Note that there is something like a threshold in this range, below which more sophisticated encodings have much better fidelity, and above which the simplest encodings fail

least often. The jaggedness of some of the curves for small values of p_{fail} are due to statistical noise in our samplings; we expect the real curves to be smooth and convex. From these curves, we can compute the fidelity for encoding any d-dimensional system simply by scaling σ by $\sqrt{\frac{2}{d}}$.

If we are concerned with sending quantum information faithfully over a Gaussian quantum channel, we could consider implementing another level of encoding on the logical qudits encoded in the oscillators, such as a random stabilizer code. When the effective channel is a Pauli channel (which is the case for all of the examples given in the previous section), we can make a random coding argument that good stabilizer codes exist that achieve a rate (in faithful qubits sent per use of the channel)

$$R \;=\; (\log_2 d)\,(1 - H_d(\vec{p}) - \epsilon) \;=\; (\log_2 d)\,(1-\epsilon) + \sum_{k=1}^{M} p_k \log_d p_k \qquad (3.14)$$

when the channel has M Pauli errors (including the identity), with corresponding error probabilities p_k (where $H_d(\vec{p})$ is the Shannon entropy of probability vector $\vec{p}$ in terms of logarithms base d).

We have plotted the resulting achievable rates for the A_2, D_4, F_6, and E_8 lattice encodings, using the best found logical operator mappings, for several values of d in Figure 3.4. For each lattice encoding, we approximated the success probability of error correction through Monte Carlo simulations of sampling the Gaussian distribution over the corresponding normalizer lattice Voronoi cell. We then selected the best found effective error channel described in the previous section and computed an asymptotically achievable rate with random stabilizer codes on the encoded qudits (in the limit of large block size).

For noisy Gaussian quantum channels (those with relatively large standard deviation σ of oscillator kicks), the A_2 encoding is almost always the best choice. Although not shown on the plot, the A_2 encoding beats out the Z_2 encoding almost everywhere (due to its larger minimum distance). The only exception is the region around $0.5 < \sigma < 0.555$, where Z_2 achieves slightly higher rates, due to its simpler

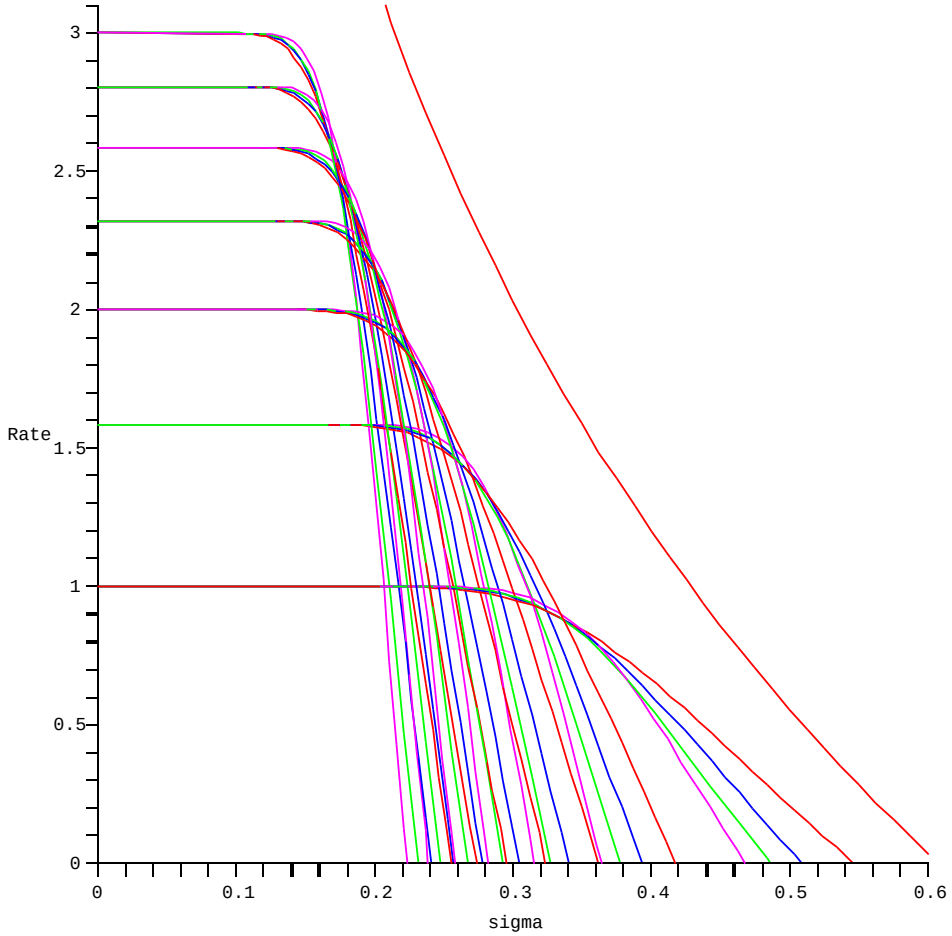

Figure 3.4: Achievable rates of A_2, D_4, F_6, and E_8 lattice encodings over the Gaussian channel. Sigma along the horizontal axis denotes the standard deviation of the magnitude of the kicks by the channel in each oscillator's phase space. The upper curve corresponds to the channel's one-shot coherent information optimized over Gaussian input states, which is conjectured to be additive and thus equal the channel's quantum capacity. The red, blue, green, and magenta lines below are respectively plots of the achievable rates (in qubits per oscillator) for A_2, D_4, F_6, and E_8 lattice encodings of qudits with dimensions 2, 3, 4, 5, 6, 7, and 8.

effective error channel. The ability to encode qudits over several oscillators only provides a rate gain for less noisy channels. In particular, the E_8 encoding appears to win over the others for $\sigma < 0.2$. We know from Section 2.6 that in the regime of small noise (small σ) there exist symplectic lattice encodings that allow us to achieve rates matching the one-shot coherent information for Gaussian inputs, which is the upper curve in the plot. However, for moderately noisy channels, there is a discernable gap, on the order of one qubit. Perhaps there exist better quantum error-correcting codes for this noisy regime.

3.8 Conclusion

We presented an algorithm to search for symplectic self-dual lattices with large minimum distance, and expressed bases for the optimal symplectic self-dual lattices in two, four, six, eight, and twelve dimensions, which provide explicit descriptions of quantum error-correcting codes protecting against shifts in the phase space of oscillators. We have found effective Pauli error channels when encoding qudits into oscillators over the Gaussian quantum channel for several of these lattices. By concatenating with random stabilizer codes, we computed achievable rates over the channel.

Chapter 4

Accuracy threshold for toric codes

4.1 Abstract

We study the $\pm J$ random-plaquette Z_2 gauge model (RPGM) in three spatial dimensions, a three-dimensional analog of the two-dimensional $\pm J$ random-bond Ising model (RBIM). The model is a pure Z_2 gauge theory in which randomly chosen plaquettes (occurring with concentration p) have couplings with the "wrong sign" so that magnetic flux is energetically favored on these plaquettes. Excitations of the model are one-dimensional "flux tubes" that terminate at "magnetic monopoles" located inside lattice cubes that contain an odd number of wrong-sign plaquettes. Electric confinement can be driven by thermal fluctuations of the flux tubes, by the quenched background of magnetic monopoles, or by a combination of the two. Like the RBIM, the RPGM has enhanced symmetry along a "Nishimori line" in the p-T plane (where T is the temperature). The critical concentration p_c of wrong-sign plaquettes at the confinement-Higgs phase transition along the Nishimori line can be identified with the accuracy threshold for robust storage of quantum information using topological error-correcting codes: if qubit phase errors, qubit bit-flip errors, and errors in the measurement of local check operators all occur at rates below p_c, then encoded quantum information can be protected perfectly from damage in the limit of a large code block. Through Monte Carlo

simulations, we measure p_{c0}, the critical concentration along the $T = 0$ axis (a lower bound on p_c), finding $p_{c0} = .0293 \pm .0002$. We also measure the critical concentration of antiferromagnetic bonds in the two-dimensional RBIM on the $T = 0$ axis, finding $p_{c0} = .1031 \pm .0001$. Our value of p_{c0} is incompatible with the value of $p_c = .1093 \pm .0002$ found in earlier numerical studies of the RBIM, in disagreement with the conjecture that the phase boundary of the RBIM is vertical (parallel to the T axis) below the Nishimori line. The model can be generalized to a rank-r antisymmetric tensor field in d dimensions, in the presence of quenched disorder.

4.2 Introduction

Spin systems with quenched randomness have been extensively studied, leading to valuable insights that apply to (for example) spin glass materials, quantum Hall systems, associative memory, error-correcting codes, and combinatorial optimization problems [59, 85, 65]. Gauge systems with quenched randomness, which have received comparatively little attention, will be studied in this paper.

The gauge models we consider are intrinsically interesting because they provide another class of simple systems with disorder-driven phase transitions. But our investigation of these models has a more specific motivation connected to the theory of quantum error correction.

In practice, coherent quantum states rapidly decohere due to uncontrollable interactions with the environment. But in principle, if the quantum information is cleverly encoded [76, 80], it can be stabilized and preserved using fault-tolerant recovery protocols [77]. Kitaev [47, 48] proposed a particularly promising class of quantum error-correcting codes (*surface codes*) in which the quantum processing required for error recovery involves only *local* interactions among qubits arranged in a two-dimensional block, and the protected information is associated with global topological properties of the quantum state of the block. If the error rate is small, then the topological properties of the code block are well protected, and error

recovery succeeds with a probability that rapidly approaches one in the limit of a large code block. But if the error rate is above a critical value, the *accuracy threshold*, then quantum error correction is ineffective.

In [26], a precise connection was established between the accuracy threshold achievable with surface codes and the confinement-Higgs transition in a three-dimensional Z_2 lattice gauge model with quenched randomness. The model has two parameters: the temperature T and the concentration p of "wrong-sign" plaquettes. On wrong-sign plaquettes (which are analogous to antiferromagnetic bonds in a spin system) it is energetically favorable for the Z_2 magnetic flux to be nontrivial. In the mapping between quantum error recovery and the gauge model, the quenched fluctuations correspond to the actual errors introduced by the environment; these impose sites of frustration, *magnetic monopoles*, corresponding to an "error syndrome" that can be measured by executing a suitable quantum circuit. Thermally fluctuating magnetic flux tubes, which terminate at magnetic monopoles, correspond to the ensemble of possible error patterns that could generate a particular error syndrome. (The temperature T is tied to the strength p of the quenched fluctuations through a *Nishimori relation* [63].) When the disorder is weak and the temperature low (corresponding to a small error rate), the system is in a magnetically ordered Higgs phase. In the surface code, magnetic order means that all likely error patterns that might have produced the observed error syndrome are topologically equivalent, so that the topologically encoded information resists damage. But at a critical value p_c of the disorder strength (and a temperature determined by Nishimori's relation), magnetic flux tubes condense and the system enters the magnetically disordered confinement phase. In the surface code, magnetic disorder means that the error syndrome cannot point to likely error patterns belonging to a unique topological class; therefore topologically encoded information is vulnerable to damage.

Although the code block is two-dimensional, the gauge model is three dimensional because one dimension represents *time*. Time enters the analysis of recovery because measurements of the error syndrome might themselves be faulty; there-

fore measurements must be repeated on many successive time slices if they are to provide reliable information about the errors that have afflicted the code block. If qubit phase errors, qubit bit-flip errors, and errors in the measurement of local check operators all occur at rates below p_c, then encoded quantum information can be protected perfectly from damage in the limit of a large code block. As we consider more and more reliable measurements of the syndrome, the corresponding three-dimensional gauge model becomes more and more anisotropic, reducing in the limit of perfect measurements to the two-dimensional random-bond Ising model.

The numerical value p_c of the accuracy threshold is of considerable interest, since it characterizes how reliably quantum hardware must perform in order for a quantum memory to be robust. In the three-dimensional Z_2 gauge model, p_c is the value of the wrong-sign plaquette concentration where the confinement-Higgs boundary crosses the Nishimori line in the p-T plane. A lower bound on p_c is provided by the critical concentration p_{c0} on the $T = 0$ axis. In [26], an analytic argument established that $p_{c0} \geq .0114$. In this paper we report on a numerical calculation that finds $p_{c0} = .0293 \pm .0002$.

In the case where the error syndrome can be measured flawlessly, the critical error rate is given by the critical antiferromagnetic bond concentration on the Nishimori line of the two-dimensional random-bond Ising model (RBIM). Numerical calculations performed earlier by other authors [42, 58] have established $p_c = .1093 \pm .0002$. According to a conjecture of Nishimori [64] and Kitatani [49], this value of p_c should agree with the critical bond concentration p_{c0} of the 2-D RBIM on the $T = 0$ axis. The same reasoning that motivates this conjecture for the RBIM indicates that $p_c = p_{c0}$ for the 3-D random-plaquette gauge model (RPGM) as well. However, we have calculated p_{c0} in the 2-D RBIM numerically, finding $p_{c0} = .1031 \pm .0001$. Our value of p_{c0} agrees with an earlier numerical calculation by Kawashima and Rieger [44], but disagrees with the conjecture that $p_c = p_{c0}$.

In Section 4.3 we describe in more detail the properties of the 2-D RBIM

and the 3-D RPGM, emphasizing the importance of the Nishimori line and the inferences that can be made about the behavior of order parameters on this line. Section 4.4 reviews the connection between the models and error recovery using surface codes. Our numerical results for p_{c0} and for the critical exponent ν_0 at the $T = 0$ critical point are presented in Section 4.5. Section 4.6 summarizes our conclusions.

4.3 Models

4.3.1 Random-bond Ising model

The two-dimensional $\pm J$ random-bond Ising model (RBIM) has a much studied multicritical point at which both the temperature and the strength of quenched disorder are nonzero. This model is an Ising spin system on a square lattice, with a variable $S_i = \pm 1$ residing at each lattice site i. Its Hamiltonian is

$$H = -J \sum_{\langle ij \rangle} \tau_{ij} S_i S_j \ , \tag{4.1}$$

where J is the strength of the coupling between neighboring spins, and $\tau_{ij} = \pm 1$ is a quenched random variable. (That is, τ_{ij} depends on what *sample* of the system is selected from a certain ensemble, but is not subject to thermal fluctuations.) The τ_{ij}'s are independently and identically distributed, with the antiferromagnetic choice $\tau_{ij} = -1$ (favoring that neighboring spins anti-align) occurring with probability p, and the ferromagnetic choice τ_{ij}=+1 (favoring that neighboring spins align) occurring with probability $1 - p$. We refer to p as the concentration of antiferromagnetic bonds, or simply the bond concentration.

The free energy F of the model at inverse temperature β, averaged over samples, is

$$[\beta F(K, \tau)]_{K_p} = -\sum_{\tau} P(K_p, \tau) \ln Z(K, \tau) \tag{4.2}$$

where

$$Z(K,\tau) = \sum_S \exp\left(K \sum_{\langle ij\rangle} \tau_{ij} S_i S_j\right) \tag{4.3}$$

is the partition function for sample τ (with $K = \beta J$), and

$$P(K_p,\tau) = (2\cosh K_p)^{-N_B} \times \exp\left(K_p \sum_{\langle ij\rangle} \tau_{ij}\right) \tag{4.4}$$

is the probability of the sample τ; here

$$\frac{p}{1-p} = e^{-2K_p} \tag{4.5}$$

and N_B is the number of bonds.

The partition function $Z(K,\tau)$ is invariant under the change of variable

$$S_i \to \sigma_i S_i \ , \quad \tau_{ij} \to \sigma_i \sigma_j \tau_{ij} \ , \tag{4.6}$$

where $\sigma_i = \pm 1$. Thus τ itself has no invariant meaning — samples τ and τ' that differ by the change of variable have equivalent physics. The only invariant property of τ that cannot be modified by such a change of variable is the *distribution of frustration* that τ determines. If an odd number of the bonds contained in a specified plaquette have $\tau = -1$ then that plaquette is frustrated — an *Ising vortex* resides at the plaquette. For purposes of visualization, we sometimes will find it convenient to define the spin model on the dual lattice so that the spins reside on plaquettes and the Ising vortices reside on sites. Then excited bonds with $\tau_{ij} S_i S_j = -1$ form one-dimensional chains that terminate at the frustrated sites.

Changes of variable define an equivalence relation on the set of 2^{N_B} τ configurations: there are the 2^{N_S} elements of each equivalence class (the number of changes of variable, where N_S is the number of sites) and there are 2^{N_S} classes (the number of configurations for the Ising vortices — note that $N_B = 2N_S$ for

a square lattice on the 2-torus, and that the number of plaquettes is $N_P = N_S$). Denote a distribution of Ising vortices, or equivalently an equivalence class of τ's, by η. The probability $P(K_p, \eta)$ of η is found by summing $P(K_p, \tau)$ over all the representatives of the class; hence

$$\begin{aligned}(2\cosh K_p)^{N_B} P(K_p, \eta) &= (2\cosh K_p)^{N_B} \sum_{\tau \in \eta} P(K_p, \tau) \\ &= \sum_{\sigma} \exp\left(K_p \sum_{\langle ij \rangle} \tau_{ij}\sigma_i\sigma_j \right) = Z(K_p, \eta) \ . \end{aligned} \tag{4.7}$$

Apart from a normalization factor, the probability of a specified distribution of frustration is given by the partition function of the model, but with $K = \beta J$ replaced by K_p.

In this model, we can define an order parameter that distinguishes the ferromagnetic and paramagnetic phases. Let

$$m^2(K, K_p) = \lim_{|i-j| \to \infty} \left[\langle S_i S_j \rangle_K \right]_{K_p} \ , \tag{4.8}$$

where $\langle \cdot \rangle_K$ denotes the average over thermal fluctuations, $[\cdot]_{K_p}$ denotes the average over samples, and $|i - j|$ denotes the distance between site i and site j; then in the ferromagnetic phase $m^2 > 0$ and in the paramagnetic phase $m^2 = 0$. But the two-point correlation function $\langle S_i S_j \rangle_K$ is not invariant under the change of variable eq. (4.6), so how should m^2 be interpreted?

Following [26], denote by E the set of bonds that are antiferromagnetic ($\tau_{ij} = -1$), denote by E' the set of excited bonds with $\tau_{ij} S_i S_j = -1$, and denote by D the set of bonds with $S_i S_j = -1$ (those whose neighboring spins anti-align) — see Figure 4.1. Then $D = E + E'$ is the disjoint union of E and E' (containing bonds in E or E' but not both). Furthermore, D contains an even number of the bonds that meet at any given site; that is, D is a *cycle*, a chain of bonds that has no boundary points. The quantity $S_i S_j$ just measures whether a line connecting i and j crosses D an even number ($S_i S_j = 1$) or an odd number ($S_i S_j = -1$) of times.

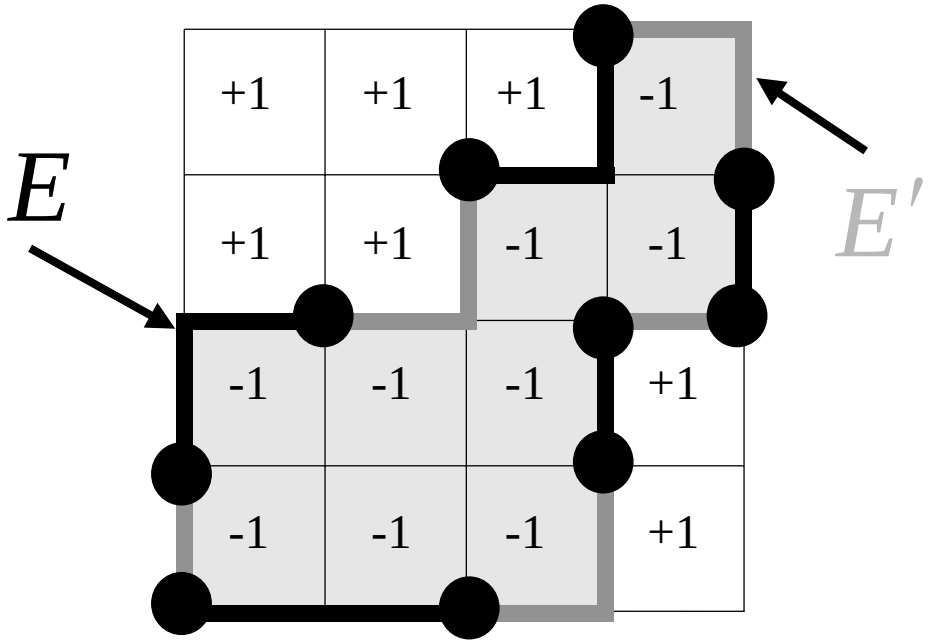

Figure 4.1: The chain E of antiferromagnetic bonds (darkly shaded) and the chain E' of excited bonds (lightly shaded), in the two-dimensional random-bond Ising model. Ising spins taking values in $\{\pm 1\}$ reside on plaquettes; Ising vortices (boundary points of E) are located on the sites marked by filled circles. The bonds of E' comprise a one-dimensional defect that connects the vortices. The cycle $D = E + E'$ encloses a domain of spins with the value -1.

Now D consists of disjoint "domain walls" that form closed loops. If loops that are arbitrarily large appear with appreciable weight in the thermal ensemble, then the two-point function $\langle S_i S_j \rangle_K$ decays like $\exp(-|i-j|/\xi)$ — fluctuations far from the sites i and j contribute to the correlation function. Thus the spins are disordered and $m^2 = 0$. But if large loops occur only with negligible probability, then only fluctuations localized near i and j contribute significantly; the spin correlation persists at large distances and $m^2 > 0$. Thus, the order parameter probes whether the chain E' of excited bonds can wander far from the chain E of ferromagnetic bonds; that is, whether $D = E + E'$ contains arbitrarily large connected closed loops, for typical thermal fluctuations and typical samples.

Nishimori [63] observed that the random-bond Ising model has enhanced symmetry properties along a line in the p-T plane (the *Nishimori line*) defined by $K = K_p$ or $\exp(-2\beta J) = p/(1-p)$. In this case, the antiferromagnetic bond chain E and the excited bond chain E' are generated by sampling the same probability distribution, subject to the constraint that both chains have the same boundary points. This feature is preserved by renormalization group transformations, so that renormalization group flow preserves Nishimori's line [28]. The *Nishimori point* (p_c, T_c) where the Nishimori line crosses the ferromagnetic-paramagnetic phase boundary, is a renormalization group fixed point, the model's multicritical point.

When the temperature T is above the Nishimori line, excited bonds have a higher concentration than antiferromagnetic bonds, so we may say that thermal fluctuations play a more important role than quenched randomness in disordering the spins. When T is below the Nishimori line, antiferromagnetic bonds are more common than excited bonds, and the quenched randomness dominates over thermal fluctuations. Right on the Nishimori line, the effects of thermal fluctuations and quenched randomness are in balance [66].

By invoking the change of variable eq. (4.6), various properties of the model on the Nishimori line can be derived [65, 63]. For example, the internal energy

density (or "average bond") can be computed analytically,

$$[\tau_{ij}\langle S_i S_j\rangle_{K_p}]_{K_p} = 1 - 2p \ , \tag{4.9}$$

where i and j are neighboring sites; averaged over thermal fluctuations and samples, the concentration of excited bonds is p as one would expect (and the internal energy has no singularity at the Nishimori point). Furthermore, after averaging over disorder, the $(2m-1)$st power of the k-spin correlator has the same value as the $(2m)$th power, for any positive integer m:

$$\left[\langle S_{i_1} S_{i_2} \cdots S_{i_k}\rangle_{K_p}^{2m-1}\right]_{K_p} = \left[\langle S_{i_1} S_{i_2} \cdots S_{i_k}\rangle_{K_p}^{2m}\right]_{K_p} \ . \tag{4.10}$$

It follows in particular that the spin-glass order parameter

$$q^2(K_p, K_p) \equiv \lim_{|i-j|\to\infty} \left[\langle S_i S_j\rangle_{K_p}^2\right]_{K_p} \tag{4.11}$$

coincides with the ferromagnetic order parameter $m^2(K_p, K_p)$ along the Nishimori line, reflecting the property that thermal fluctuations and quenched randomness have equal strength on this line.

Comparing eq. (4.2) and (4.7), we see that for $K = K_p$ the free energy of the model coincides with the *Shannon entropy* of the distribution of vortices, apart from a nonsingular additive term:

$$\begin{aligned} &[\beta F(K_p, \tau)]_{K_p} \\ &= -\sum_{\eta} P(K_p, \eta) \ln P(K_p, \eta) - N_B \ln\left(2\cosh K_p\right) \ . \end{aligned} \tag{4.12}$$

Since the free energy is singular at the Nishimori point (p_c, T_c), it follows that the Shannon entropy of frustration (which does not depend on the temperature) is singular at $p = p_c$ [64]. This property led Nishimori to suggest that the boundary between the ferromagnetic and paramagnetic phases occurs at $p = p_c$ at sufficiently low temperature, and thus that the phase boundary is vertical in the p-T plane be-

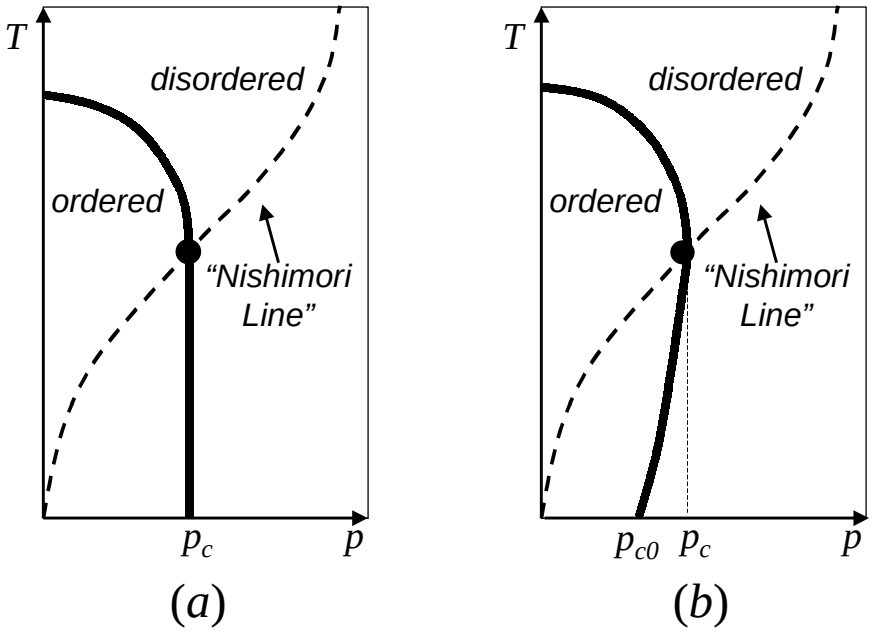

Figure 4.2: The phase diagram of the random-bond Ising model (shown schematically), with the temperature T on the vertical axis and the concentration p of antiferromagnetic bonds on the horizontal axis. The solid line is the boundary between the ferromagnetic (ordered) phase and the paramagnetic (disordered) phase. The dotted line is the Nishimori line $e^{-2\beta J} = p/(1-p)$, which crosses the phase boundary at the Nishimori point (the heavy black dot). It has been conjectured, but not proven, that the phase boundary from the Nishimori point to the p-axis is *vertical*, as in (a). The numerics reported in Section 4.4 favor the reentrant phase diagram shown in (b). The deviation of the critical bond concentration p_c on the Nishimori line from the critical bond concentration p_{c0} on the $T = 0$ axis has been exaggerated in (b) for clarity.

low the Nishimori point, as in Figure 4.2a. Later, Kitatani [49] arrived at the same conclusion by a different route, showing that the verticality of the phase boundary follows from an "appropriate condition." These arguments, while suggestive, do not seem compelling to us. There is no known rigorous justification for Kitatani's condition, and no rigorous reason why the ferro-para boundary must coincide with the singularity in the entropy of frustration, even at low temperature. Hence we regard the issue of the verticality of the phase boundary as still unsettled. Nishimori did argue convincingly that the phase boundary cannot extend to any value of p greater than p_c [63], and Le Doussal and Harris argued that the *tangent* to the phase boundary is vertical at the Nishimori point [28], but these results leave open the possibility of a "reentrant" boundary that slopes back toward the T axis below the Nishimori point, as in Figure 4.2b.

The RBIM can also be defined in d dimensions. Much of the above discussion still applies, with minor modifications. Consider, for example, $d = 3$. On the dual lattice, spins reside on lattice cubes and the bonds become plaquettes shared by two neighboring cubes. The set of antiferromagnetic bonds E is dual to a two-dimensional surface, and its boundary ∂E consists of one-dimensional loops — the Ising *strings* where the spins are frustrated. The set of excited bonds E' is dual to another two-dimensional surface that is also bounded by the Ising strings: $\partial E' = \partial E$. The spins are disordered if the two-cycle $D = E + E'$ contains arbitrarily large closed connected surfaces for typical thermal fluctuations and typical samples. Similarly, in d dimensions, frustration is localized on closed surfaces of dimension $d - 2$, and the thermally fluctuating defects are dimension-$(d - 1)$ surfaces that terminate on the locus of frustration. For any d, the model has enhanced symmetry along the Nishimori line $K = K_p$, where antiferromagnetic bonds and excited bonds are drawn from the same probability distribution.

In the absence of quenched disorder, the two-dimensional Ising model is mapped to itself by a duality relation that can be used to infer properties of the critical theory. When quenched disorder is introduced, however, the two-dimensional random bond Ising model is mapped under duality to a model with Boltzmann weights that

are not positive definite [67], so that it is not easy to draw any firm conclusions.

4.3.2 Random-plaquette gauge model

In the d-dimensional RBIM, excitations have codimension 1 and terminate on a closed surface of codimension 2. The Z_2 random-plaquette gauge model (RPGM) is defined in an entirely analogous manner, except that the excitations are objects of codimension 2 ("magnetic flux tubes") that terminate on codimension-3 objects ("magnetic monopoles").

More concretely, the variables of the model are $U_\ell = \pm 1$ residing on each link ℓ of the lattice, and the Hamiltonian is

$$H = -J \sum_P \tau_P U_P \ , \tag{4.13}$$

where J is the coupling strength,

$$U_P = \prod_{\ell \in P} U_\ell \tag{4.14}$$

is the Z_2-valued "magnetic flux" through the plaquette P, and $\tau_P = \pm 1$ is a quenched random variable. The τ_P's are independently and identically distributed, with the "wrong-sign" choice $\tau_P = -1$ (favoring nontrivial flux) occurring with probability p, and the "right-sign" choice τ_P=+1 (favoring trivial flux) occurring with probability $1-p$. We refer to p as the concentration of wrong-sign plaquettes, or simply the plaquette concentration.

The free energy F of the model at inverse temperature β, averaged over samples, is

$$[\beta F(K,\tau)]_{K_p} = -\sum_\tau P(K_p,\tau) \ln Z(K,\tau) \tag{4.15}$$

where

$$Z(K,\tau) = \sum_U \exp\left(K \sum_P \tau_P U_P \right) \tag{4.16}$$

is the partition function for sample τ (with $K = \beta J$), and

$$P(K_p, \tau) = (2\cosh K_p)^{-N_P} \times \exp\left(K_p \sum_P \tau_P \right) \tag{4.17}$$

is the probability of the sample τ; here

$$\frac{p}{1-p} = e^{-2K_p} \tag{4.18}$$

and N_P is the number of plaquettes.

The partition function $Z(K, \tau)$ is invariant under the change of variable

$$U_\ell \to \sigma_\ell U_\ell \ , \quad \tau_P \to \sigma_P \tau_P \ , \tag{4.19}$$

where $\sigma_\ell = \pm 1$ and $\sigma_P = \prod_{\ell \in P} \sigma_\ell$. While τ itself has no invariant meaning, τ determines a distribution of frustration that cannot be altered by a change of variable. If an odd number of the plaquettes contained in a specified cube have $\tau = -1$ then that cube is frustrated — a Z_2 *magnetic monopole* resides in the cube. For purposes of visualization, we will sometimes find it convenient to define the gauge model on the dual lattice so that the gauge variables U_ℓ reside on plaquettes, the magnetic flux on bonds, and the magnetic monopoles on sites. Then excited bonds with $\tau_P U_P = -1$ form one-dimensional strings that terminate at monopoles.

We can define an order parameter that distinguishes the Higgs (magnetically ordered) phase and the confinement (magnetically disordered) phase. Consider the Wilson loop operator associated with a closed loop C (on the original lattice, not the dual lattice):

$$W(C) = \prod_{\ell \in C} U_\ell \ . \tag{4.20}$$

and consider the behavior of the expectation value of $W(C)$, averaged over thermal fluctuations and over samples. In the Higgs phase, for a large loop C the Wilson

loop operator decays exponentially with the perimeter of the loop,

$$[\langle W(C)\rangle_K]_{K_p} \sim \exp\left[-\mu \cdot \text{Perimeter}(C)\right] \ , \tag{4.21}$$

while in the confinement phase it decays exponentially with the area of the minimal surface bounded by C,

$$[\langle W(C)\rangle_K]_{K_p} \sim \exp\left[-\kappa \cdot \text{Area}(C)\right] \ . \tag{4.22}$$

The interpretation is that on the dual lattice the wrong-sign plaquettes correspond to a one-chain E bounded by magnetic monopoles, and the excited plaquettes correspond to another one-chain E' with the same boundary; hence $D = E + E'$ is a cycle, a sum of disjoint closed "flux tubes." If arbitrarily large loops of flux appear with appreciable weight in the thermal ensemble for typical samples, then magnetic fluctuations spanning the entire surface bounded by C contribute to the expectation value of $W(C)$, and the area-law decay results. If large flux tubes are suppressed, then only the fluctuations localized near the loop are important, and the perimeter-law decay applies. Thus, the Wilson-loop order parameter probes whether the chain E' of excited plaquettes can wander far from the chain E of wrong-sign plaquettes; that is, whether $D = E + E'$ contains arbitrarily large connected closed loops.

The one-chain E bounded by the magnetic monopoles is analogous to a Z_2-valued *Dirac string* — the change of variable eq. (4.19) deforms the strings while leaving invariant the boundary of E (the locations of the monopoles). One should notice that these strings are *not* invisible to our Wilson loop operator; that is $W(C)$ is not invariant under the change of variable. It is possible to modify $W(C)$ to obtain an invariant object [4], but that would not be appropriate if the order parameter is supposed to probe the extent to which the thermally fluctuating defects (the excited plaquettes) depart from the quenched disorder (the Dirac strings).

Like the RBIM, the RPGM has enhanced symmetry on the Nishimori line $K = K_p$, and the change of variable eq. (4.19) may be invoked to derive properties of the model on this line. The Nishimori line is preserved by renormalization group flow, and crosses the confinement-Higgs boundary at a multicritical point (p_c, T_c). The internal energy (or average plaquette) can be computed on this line,

$$\left[\tau_P \langle U_P \rangle_{K_p}\right]_{K_p} = 1 - 2p \tag{4.23}$$

(excited plaquettes have concentration p) and for each positive integer m, the $(2m-1)$'st power of W(C) and the $2m$'th power are equal when averaged over samples,

$$\left[\langle W(C)\rangle_{K_p}^{2m-1}\right]_{K_p} = \left[\langle W(C)\rangle_{K_p}^{2m}\right]_{K_p} \ . \tag{4.24}$$

Furthermore, the free energy on the Nishimori line, apart from a nonsingular additive term, is equal to the Shannon entropy of the distribution of magnetic monopoles, so that the latter is singular at $p = p_c$.

In principle, the RPGM could have what might be called a "gauge glass" phase. In this phase, the Wilson loop, averaged over thermal and quenched fluctuations, has area-law behavior,

$$\left[\langle W(C)\rangle_K\right]_{K_p} \sim \exp\left[-\kappa \cdot \mathrm{Area}(C)\right] \ , \tag{4.25}$$

but the *square* of its thermal expectation value, averaged over quenched fluctuations, has perimeter-law behavior:

$$\left[\langle W(C)\rangle_K^2\right]_{K_p} \sim \exp\left[-\mu \cdot \mathrm{Perimeter}(C)\right] \ . \tag{4.26}$$

This means that thermal fluctuations do not induce magnetic disorder for each typical sample, but that the magnetic fluctuations are large when we compare one sample to another. However, the identity eq. (4.24) shows that, along the Nishimori line $K = K_p$, there can be no gauge glass phase. Since $\langle W(C)\rangle$ and

$\langle W(C)\rangle^2$ have the same average over samples, both order parameters cross from perimeter to area law at the same point on the Nishimori line. (Nishimori [63] used the analogous argument to show that there is no spin glass behavior in the RBIM along the Nishimori line.)

Another useful identity that can be derived using the change of variable is

$$[\langle W(C)\rangle_K]_{K_p} = \left[\langle W(C)\rangle_K \langle W(C)\rangle_{K_p}\right]_{K_p} \ . \tag{4.27}$$

Since $-1 \leq W(C) \leq 1$, it follows that

$$\left|\ [\langle W(C)\rangle_K]_{K_p}\ \right| \leq \left[\ \left|\langle W(C)\rangle_{K_p}\right|\ \right]_{K_p} \ . \tag{4.28}$$

From this inequality, we may infer that if the point on the Nishimori line with concentration p is in the confinement phase, then the point (p, T) is in the confinement phase for any temperature T. (Again, the reasoning is exactly analogous to Nishimori's argument for the RBIM [63].) Since there is no gauge-glass behavior on the Nishimori line, if a point on the Nishimori line is in the confinement phase, then $\langle W(C)\rangle_{K_p}$ already exhibits area-law decay before averaging over samples. Therefore the right-hand side of eq. (4.28) shows area-law decay and so must the left-hand side. We conclude that, as for the RBIM, the phase boundary of the RPGM below the Nishimori line must either be vertical (parallel to the T axis as in Figure 4.2a) or reentrant (tipping back toward the T axis as T decreases as in Figure 4.2b).

4.3.3 Further generalizations

In d dimensions, the magnetic order parameter of the RBIM explores whether a thermally excited chain E' of codimension 1 (domain walls) deviates far from a quenched codimension-1 chain E (antiferromagnetic bonds), where both E and E' have the same codimension-2 boundary (the Ising vortices). Similarly, the RPGM can be defined in d dimensions, and its Wilson-loop order parameter probes

whether a thermally excited chain E' of codimension 2 (flux tubes) deviates far from a quenched codimension-2 chain E (Dirac strings), where both E and E' have the same codimension-3 boundary (the magnetic monopoles).

This concept admits further generalizations. In d-dimensions, we may consider the lattice theory of a "rank-r antisymmetric tensor field" with quenched disorder. Then variables reside on the r-cells of the lattice, and the Hamiltonian is expressed in terms of a field strength defined on $(r+1)$-cells. The sign of the coupling is determined by a random variable τ taking values ± 1 on $(r+1)$-cells; cells with the "wrong sign" have concentration p. On the dual lattice, τ corresponds to a codimension-$(r+1)$ chain E, and the excited cells to a codimension-$(r+1)$ chain E', where E and E' are bounded by the same codimension-$(r+2)$ chain of frustration. An operator analogous to the Wilson loop can be defined that detects the flux through the dimension-$(r+1)$ "surface" bounded by a dimension-r "loop" C; this operator serves as the order parameter for an order-disorder transition. The order parameter probes whether the thermally fluctuating codimension-$(r+1)$ chain E' deviates far from the quenched codimension-$(r+1)$ chain E.

For any d and r, the model has enhanced symmetry on the Nishimori line, where $K = K_p$. Properties of the model on this line can be derived, analogous to those discussed above for the RBIM and the RPGM.

4.4 Accuracy threshold for quantum memory

How the RBIM and RPGM relate to the performance of topological quantum memory was extensively discussed in [26]. Here we will just briefly reprise the main ideas.

4.4.1 Toric codes

Quantum information can be protected from decoherence and other possible sources of error using quantum error-correcting codes [76, 80] and fault-tolerant error

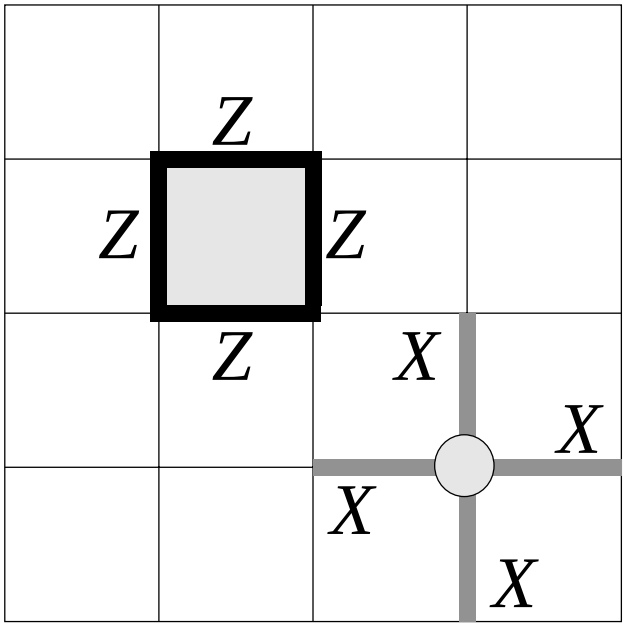

Figure 4.3: The check operators of the toric code. Each plaquette operator is a tensor product of Z's acting on the four links contained in the plaquette. Each site operator is a tensor product of X's acting on the four links that meet at the site.

recovery protocols [77]. Topological codes (or *surface codes*) are designed so that the quantum processing needed to control errors has especially nice locality properties [47, 48].

Specifically, consider a system of $2L^2$ qubits (a qubit is a two-level quantum system), with each qubit residing at a link of an $L \times L$ square lattice drawn on a two-dimensional *torus*. (Other examples of surface codes, including codes defined on planar surfaces, are discussed in [26].) This system can encode two qubits of quantum information that are well protected from noise if the error rate is low enough. The two-qubit code space, where the protected information resides, can

be characterized as a simultaneous eigenspace with eigenvalue one of a set of check operators (or "stabilizer generators"); check operators are associated with each site and with each elementary cell (or "plaquette") of the lattice, as shown in Figure 4.3. We use the notation

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \ , \ X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \ , \ Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \ , \ Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{4.29}$$

for the 2×2 identity and Pauli matrices. The check operator at site i acts nontrivially on the four links that meet at the site; it is the tensor product

$$X_i = \otimes_{\ell \ni s} X_\ell \tag{4.30}$$

acting on those four qubits, times the identity acting on the remaining qubits. The check operator at plaquette P acts nontrivially on the four links contained in the plaquette, as the tensor product

$$Z_P = \otimes_{\ell \in P} Z_\ell \ , \tag{4.31}$$

times the identity on the remaining links.

The check operators can be simultaneously diagonalized, and the toric code is the space in which each check operator acts trivially. Because of the periodic boundary conditions on the torus, the product of all L^2 site operators or all L^2 plaquette operators is the identity — each link operator occurs twice in the product, and $X^2 = Z^2 = I$. There are no further relations among these operators; therefore, there are $2 \cdot (L^2 - 1)$ independent check operators constraining the $2L^2$ qubits in the code block, and hence two encoded qubits (the code subspace is four dimensional).

Since the check operators are spatially local, it is useful to think of a site or plaquette where the check operator has the eigenvalue -1 as the position of a localized excitation or "defect." The code space contains states with no defects,

which are analogous to vacuum states of a Z_2 gauge theory on the torus: $Z_P = 1$ means that there is no Z_2 magnetic flux at plaquette P, and $X_i = 1$ means that there is no Z_2 electric charge at site i. (This Z_2 gauge theory on the two-torus should not be confused with the three-dimensional Z_2 gauge theory, described in Section 4.4.3, that arises in the analysis of the efficacy of error correction!)

Consider applying to the vacuum state an operator that is a tensor product of Pauli matrices $\{Z_\ell\}$ acting on each of a set of links forming a connected chain $\{\ell\}$. This operator creates isolated site defects at the ends of the chain. Similarly, if we apply to the vacuum a tensor product of Pauli matrices $\{X_\ell\}$ acting on a connected chain of the dual lattice, isolated plaquette defects are created at the ends of the chain, as in Figure 4.4. A general "Pauli operator" (tensor product of Pauli matrices) can be expressed as tensor product of X_ℓ's and I_ℓ's times a tensor products of Z_ℓ's and I_ℓ's; this operator preserves the code space if and only if the links acted upon by Z's comprise a *cycle* of the lattice (a chain with no boundary) and the links acted upon by X's comprise a cycle of the dual lattice.

Cycles on the torus are of two types. A *homologically trivial* cycle is the boundary of a region that can be tiled by plaquettes. A product of Z's acting on the links of the cycle can be expressed as a product of the enclosed plaquette operators, which acts trivially on the code space. A *homologically nontrivial* cycle wraps around the torus and is not the boundary of anything. A product of Z's acting on the links of the cycle preserves the code space, but acts nontrivially on the encoded quantum information. Associated with the two fundamental nontrivial cycles of the torus are encoded operations $\bar{Z}_1$ and $\bar{Z}_2$ acting on the two encoded qubits. Similarly, associated with the two dual cycles of the dual lattice are the corresponding encoded operations $\bar{X}_1$ and $\bar{X}_2$, as shown in Figure 4.5.

A general error acting on the code block can be expanded in terms of Pauli operators. Therefore, we can characterize the efficacy of error correction by considering how well we can protect the encoded state against Pauli operator errors. With the toric code, X errors (bit flips) and Z errors (phase flips) can be corrected independently; this suffices to protect against general Pauli errors, since a Y error

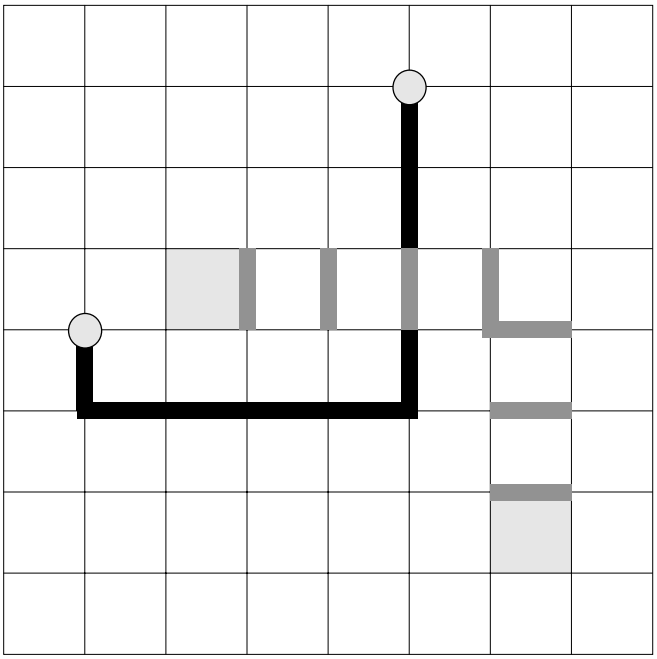

Figure 4.4: Site defects and plaquette defects in the toric code. Applied to the code space, Z's acting on a connected chain of links (darkly shaded) create site defects (electric charges) at the ends of the chain. Similarly, X's applied to a connected chain of dual links (lightly shaded) create plaquette defects (magnetic fluxes) at the ends of the chain.

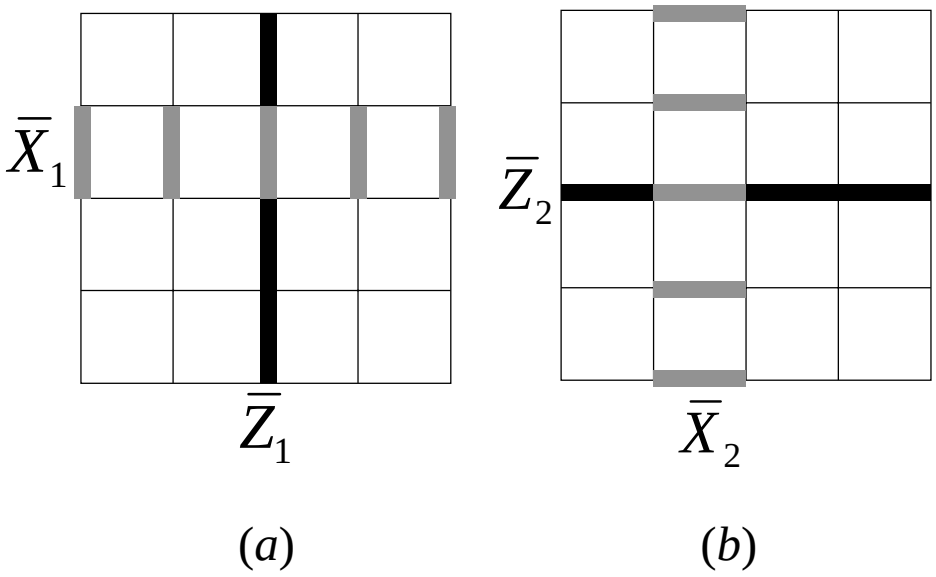

Figure 4.5: Basis for the operators that act on the two encoded qubits of the toric code. (a) The encoded $\bar{Z}_1$ is a tensor product of Z's acting on lattice links comprising a cycle of the torus, and the encoded $\bar{X}_1$ is a tensor product of X's acting on dual links comprising the complementary cycle. (b) $\bar{Z}_2$ and $\bar{X}_2$ are defined similarly.

is just a bit flip and a phase flip acting on the same qubit. We may therefore confine our attention to Z errors; the X errors may be dealt with in essentially the same way, but with the lattice replaced by its dual.

4.4.2 Perfect measurements and the random-bond Ising model

To be concrete, suppose that the Z errors are independently and identically distributed, occurring with probability p on each qubit. Noise produces an *error chain* E, a set of qubits acted upon by Z. To diagnose the errors, the code's local check operators are measured at each lattice site, the measurement outcomes providing a "syndrome" that we may use to diagnose errors. However, the syndrome is highly ambiguous. It does not completely characterize where the errors occurred; rather it only indicates whether the number of damaged qubits adjacent to each site is even or odd. That is, the measurement determines the *boundary* ∂E of the error chain E.

To recover from the damage, we choose a *recovery chain* E' that has the same boundary as the measured boundary of E, and apply Z to all the qubits of E'. Since $\partial E = \partial E'$, the chain $D = E + E'$ is a cycle with $\partial D = 0$. Now, if D is homologically trivial, then the recovery successfully protects the two encoded qubits — the effect of the errors together with the recovery step is just to apply a product of check operators, which has trivial action on the code space. But if D is homologically nontrivial, then recovery fails — the encoded quantum information suffers an error.

Error recovery succeeds, then, if we can guess the homology class of the randomly generated chain E, knowing only its boundary ∂E — we succeed if our guess $E' = E + D$ differs from E by a homologically trivial cycle D. If the error rate p is below a certain critical value p_c called the *accuracy threshold*, it is possible to guess correctly, with a probability of failure that approaches zero for a sufficiently large linear size L of the lattice. But if p is above p_c, the failure probability approaches a nonzero constant as $L \to \infty$. The numerical value of p_c is of considerable interest,

since it characterizes how reliably quantum hardware must perform for a quantum memory to be robust.

Let prob(E) denote the probability that the error chain is E, and let prob$[(E+D)|E]$ denote the normalized conditional probability for error chains $E' = E + D$ that have the same boundary as E. Then, the probability of error per qubit lies below threshold if and only if, in the limit $L \to \infty$,

$$\sum_E \text{prob}(E) \cdot \sum_{D \text{ nontrivial}} \text{prob}[(E+D)|E] = 0 \ . \tag{4.32}$$

Eq. (4.32) says that error chains that differ from the actual error chain by a homologically nontrivial cycle have probability zero. Therefore, the outcome of the measurement of the check operators is sure to point to the correct homology class, in the limit of an arbitrarily large code block.

This criterion is identical to the criterion for long-range order in the two-dimensional RBIM, along the Nishimori line. The error chain E can be identified with the chain of antiferromagnetic bonds of a sample, bounded by Ising vortices that are pinned down by the measurement of the local check operators. The ensemble of all the chains $\{E'\}$ with a specified boundary can be interpreted as a thermal ensemble. If the temperature T and the error rate p obey Nishimori's relation, then the chain E' and the chain E have the same bond concentration. At low temperature along the Nishimori line, the cycle $D = E + E'$ contains no large connected loops for typical samples and typical thermal fluctuations — the spin system is magnetically ordered and error recovery succeeds with high probability. But at higher temperature, the quenched chain E and the thermal chain E' fluctuate more vigorously. At the Nishimori point, D contains loops that "condense," disordering the spins and compromising the effectiveness of error correction. Thus, the critical concentration p_c at the Nishimori point of the two-dimensional RBIM coincides with the accuracy threshold for quantum memory using toric codes (where p_c is the largest acceptable probability for either an X error or a Z error).

The optimal recovery procedure is to choose a recovery chain E' that belongs to the most likely homology class, given the known boundary of the chain $\partial E' = \partial E$. For $p < p_c$, the probability distribution has support on a single class in the limit $L \to \infty$, and the optimal recovery procedure is sure to succeed. In the language of the RBIM, for a given sample with antiferromagnetic chain E, a chain E' of excited bonds can be classified according to the homology class to which the cycle $D = E + E'$ belongs, and a free energy can be defined for each homology class. For $p < p_c$ along the Nishimori line, the trivial homology class has lowest free energy, and the free energy cost of choosing a different class diverges as $L \to \infty$.

An alternative recovery procedure is to choose the single most likely recovery chain E', rather than a chain that belongs to the most likely *class*. In the language of the RBIM, this most likely recovery chain E' for a given sample is the set of excited links that minimizes energy rather than free energy. This energy minimization procedure is sure to succeed if the error rate is $p < p_{c0}$, where p_{c0} is the critical bond concentration of the RBIM at $T = 0$. Since minimizing energy rather than free energy need not be optimal, we see that $p_{c0} \leq p_c$. However, the energy minimization procedure has advantages: it can be carried out efficiently using the Edmonds perfect matching algorithm [29, 6], and without any prior knowledge of the value of p.

4.4.3 Faulty measurements and the random-plaquette gauge model

But the RBIM applies only to an unrealistic situation in which the outcomes of measurements of check operators are known with perfect accuracy. Since these are four-qubit measurements, they must be carried out with a quantum computer and are themselves degraded by noise. To obtain reliable information about the positions of the Ising vortices, we must repeat the measurements many times, assembling a measurement history from which we can infer the world lines of the vortices in three-dimensional spacetime.

To visualize the world lines in three dimensions, consider a three-dimensional

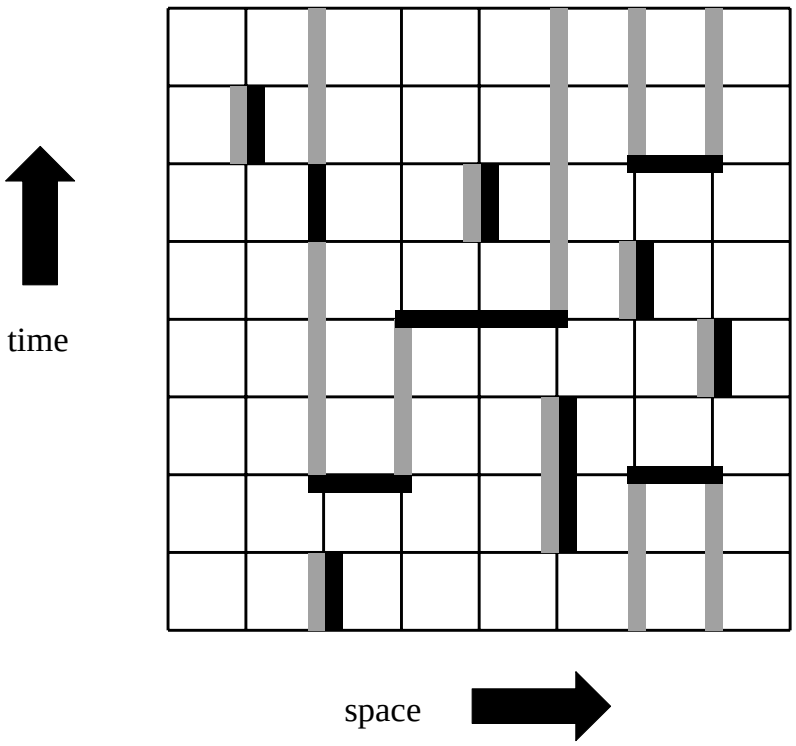

Figure 4.6: An error history shown together with the syndrome history that it generates, for the toric code. For clarity, the three-dimensional history of the two-dimensional code block has been compressed to two dimensions. Qubits reside on plaquettes, and four-qubit check operators are measured at each vertical link. Links where errors have occurred are darkly shaded, and links where the syndrome is nontrivial are lightly shaded. Errors on horizontal links indicate where a qubit flipped between successive syndrome measurements, and errors on vertical links indicate where the syndrome measurement was wrong. Vertical links that are shaded both lightly and darkly are locations where a nontrivial syndrome was found erroneously. The chain S of lightly shaded links (the syndrome) and the chain E of darkly shaded links (the errors) both have the same boundary.

simple cubic lattice on $T^2 \times R$, where T^2 is the two-torus and R is the real line. The error operation acts at each integer-valued time t, and check operators are measured between each t and $t+1$. Qubits in the code block are associated with timelike plaquettes, those lying in the tx and ty planes. A qubit error that occurs at time t is associated with a horizontal (spacelike) bond that lies in the time slice labeled by t. An error in the measurement of a check operator at site j between time t and time $t+1$ is associated with the vertical (timelike) bond connecting site j at time t and site j at time $t+1$. Qubit errors on horizontal bonds occur with probability p, and measurement errors on vertical links occur with probability q. The set of all errors, both horizontal and vertical, defines a one-chain E, shown darkly shaded in Figure 4.6. The set of all syndrome measurements with nontrivial outcomes (those where the observed value of the check operator is -1 rather than $+1$) defines a (vertical) one-chain S, shown lightly shaded in Figure 4.6. The chains E and S share the same boundary; therefore the (possibly faulty) measurements of the check operators reveal the boundary of the error chain E.

Error recovery succeeds if we can guess the homology class of the error chain E, given knowledge of its boundary ∂E; that is, we succeed if our guess $E' = E + D$ differs from E by a cycle D that is homologically trivial on $T^2 \times R$. Thus, the accuracy threshold can be mapped to the confinement-Higgs transition of the RPGM. The error one-chain E on the dual lattice becomes the set of wrong-sign plaquettes on the lattice; its boundary points are magnetic monopoles, whose locations are determined by the measurements of local check operators. Since q need not equal p, the gauge model can be anisotropic — on the original lattice, the concentration of spacelike wrong-sign plaquettes is q (spacelike plaquettes are dual to timelike bonds) and the concentration of timelike wrong-sign plaquettes is p (timelike plaquettes are dual to spacelike bonds). The ensemble of error chains $\{E'\}$ that have the same boundary as E becomes the thermal ensemble determined by an anisotropic Hamiltonian, with the coupling $K_{\rm space}$ on spacelike plaquettes obeying the Nishimori relation $K_{\rm space} = K_q$ and the coupling $K_{\rm time}$ on timelike plaquettes the relation $K_{\rm time} = K_p$.

For small p and q, the cycle $D = E + E'$ contains no large connected loops for typical samples and typical thermal fluctuations — the gauge system is magnetically ordered and error recovery succeeds with high probability. But there is a critical curve in the (p, q) plane where the magnetic flux tubes "condense," magnetically disordering the system and compromising the effectiveness of error correction. For the sort of error model described in [26], the qubit error rate and the measurement error rate are comparable, so the isotropic model with $p = q$ provides useful guidance. For that case, the critical concentration p_c at the Nishimori point of the three-dimensional RPGM coincides with the accuracy threshold for quantum memory using toric codes (where p_c is the largest acceptable probability for an X error, a Z error, or a measurement error). In the extreme anisotropic limit $q \to 0$, flux on spacelike plaquettes is highly suppressed, and the timelike plaquettes on each time slice decouple, with each slice described by the RBIM.

For both the 2-D RBIM and the 3-D (isotropic) RPGM, we may infer (as Nishimori argued for the RBIM [63]) that the phase boundary lies in the region $p \leq p_c$, i.e., does not extend to the right of the Nishimori point. From the perspective of the error recovery procedure, this property reflects that the best hypothesis about the error chain, when its boundary is known, is obtained by sampling the distribution prob$[(E + D)|E]$. Thus, for each value of p, the fluctuations of D are best controlled (the spins or gauge variables are least disordered) by choosing the temperature on the Nishimori line. For $p > p_c$ the magnetization of the 2-D RBIM vanishes on the Nishimori line, and so must vanish for all T. A similar remark applies to the Wilson-loop order parameter of the 3-D RPGM.

In particular, the critical value of p on the $T = 0$ axis (denoted p_{c0}) provides a lower bound on p_c. Rigorous arguments in [26] established that $p_{c0} \geq .0373$ in the 2-D RBIM and $p_{c0} \geq .0114$ in the 3-D RPGM. (A similar lower bound for the 2-D RBIM was derived by Horiguchi and Morita many years ago [43].) We have estimated the value of p_{c0} using numerical simulations that we will now describe.

4.5 Numerics

4.5.1 Method

For the RBIM in two dimensions (but not in higher dimensions), and for the RPGM in three dimensions (but not in higher dimensions), it is numerically tractable to study the phase transition on the $T = 0$ axis. Specifically, for the RBIM, we proceed as follows: Consider an $L \times L$ lattice on the torus, and generate a sample by choosing a random τ_{ij} at each bond (where $\tau_{ij} = -1$ occurs with probability p). Consider, for this sample, the one-chain E on the dual lattice containing bonds with $\tau_{ij} = -1$, and compute its boundary ∂E to locate the Ising vortices.

Then, to find the ground state of the Hamiltonian for this sample, construct the one-chain E' of the dual lattice, bounded by the Ising vortices, with the minimal number of bonds. This minimization can be carried out in a time polynomial in L using the Edmonds perfect matching algorithm [29, 6]. (If the ground state is not unique, choose a ground state at random.) Now examine the one-cycle $D = E + E'$ on the torus and compute whether its homology class is trivial. If so, we declare the sample a "success"; otherwise the sample is a "failure." Repeat for many randomly generated samples, to estimate the probability of failure $P_{\text{fail}}(p)$.

We expect $P_{\text{fail}}(p)$ to be discontinuous at $p = p_{c0}$ in the infinite volume limit. For $p < p_{c0}$, large loops in D are heavily suppressed, so that P_{fail} falls exponentially to zero for L sufficiently large compared to the correlation length ξ. But for $p > p_{c0}$, arbitrarily large loops are not suppressed, so we anticipate that the homology class is random. Since there are four possible classes, we expect P_{fail} to approach $3/4$ as $L \to \infty$.

This expectation suggests a finite-size scaling ansatz for the failure probability. Let the critical exponent ν_0 characterize the divergence of the correlation length ξ at the critical point $p = p_{c0}$:

$$\xi \sim |p - p_{c0}|^{-\nu_0} \ . \tag{4.33}$$

For a sufficiently large linear size L of the sample, the failure probability should be controlled by the ratio L/ξ; that is, it is a function of the scaling variable

$$x = (p - p_{c0})L^{1/\nu_0} \ . \tag{4.34}$$

Thus the appropriate ansatz is

$$P_{\text{fail}} \sim \frac{3}{4} f(x) \ , \tag{4.35}$$

where the function f has the properties

$$\lim_{x\to-\infty} f(x) = 0 \ , \quad \lim_{x\to\infty} f(x) = 1 \ . \tag{4.36}$$

Though the scaling ansatz should apply asymptotically in the limit of large L, there are systematic corrections for finite L that are not easily estimated.

According to eq. (4.35), the failure probability at $p = p_{c0}$ has a universal value $(3/4)f(0)$ that does not depend on L. Thus, by plotting P_{fail} vs. p for various values of L, we can estimate p_{c0} by identifying the value of p where all the curves cross. To find ν_0, we observe that

$$\log\left(\frac{\partial P_{\text{fail}}}{\partial p}\Big|_{p=p_{c0}}\right) = \frac{1}{\nu_0}\log L + \text{constant} \ . \tag{4.37}$$

Hence, if we estimate the slope of P_{fail} at $p = p_{c0}$, we can extract ν_0 from a linear fit to a plot of log(slope) vs. $\log L$.

The three-dimensional RPGM can be analyzed by the same method. A sample is generated by randomly choosing τ_P on each plaquette of an L^3 cubic lattice on the 3-torus. The wrong-sign plaquettes define a one-chain E on the dual lattice, whose boundary defines the locations of the magnetic monopoles. The ground state of the sample is constructed by finding the one-chain E' with the same boundary that has the minimal length, and the one-cycle $D = E + E'$ is examined to determine if it is homologically trivial. Since there are eight homology classes

on the 3-torus, the scaling ansatz becomes

$$P_{\rm fail} \sim \frac{7}{8}\tilde{f}(x) \ , \tag{4.38}$$

and p_{c0} and ν_0 are estimated as described above.

For the RBIM in three dimensions, or the RPGM in four dimensions, E and E' become two-chains. To construct the ground state, then, we must find the minimal two-dimensional surface that has a specified boundary. Unfortunately, this problem is known to be NP-hard [5] and so appears to be computationally intractable.

Detailed numerical studies of the two-dimensional RBIM in the vicinity of the Nishimori point have been done earlier by other authors [42, 58], using methods that are not very effective at low temperature. The $T = 0$ phase transition has been studied using methods related to ours [6, 44], but with less numerical accuracy. As far as we know, numerical studies of the RPGM have not been previously attempted.

4.5.2 Random-bond Ising model

We measured $P_{\rm fail}$ by generating 10^6 samples for each value of L from 2 to 36, and for each value of p increasing in increments of .001 from .100 to .107; in addition we generated 10^6 samples at $L = 37, 38, 40, 42$ for $p = .102, .103, .104$. Values of $P_{\rm fail}$ for even L lie slightly but systematically above the values for odd L at the same p; therefore we analyzed the data for even and odd L separately. Data for $L = 16, 20, 24, 28, 32, 36$ are shown in Figure 4.7, and data for $L = 15, 19, 23, 27, 31, 35$ are shown in Figure 4.8. Crudely, the point of concordance of the data sets provides an estimate of p_{c0}, while the trend of the data with L determines the exponent ν_0.

We did a global fit of the data to the form

$$P_{\rm fail} = A + Bx + Cx^2 \ , \tag{4.39}$$

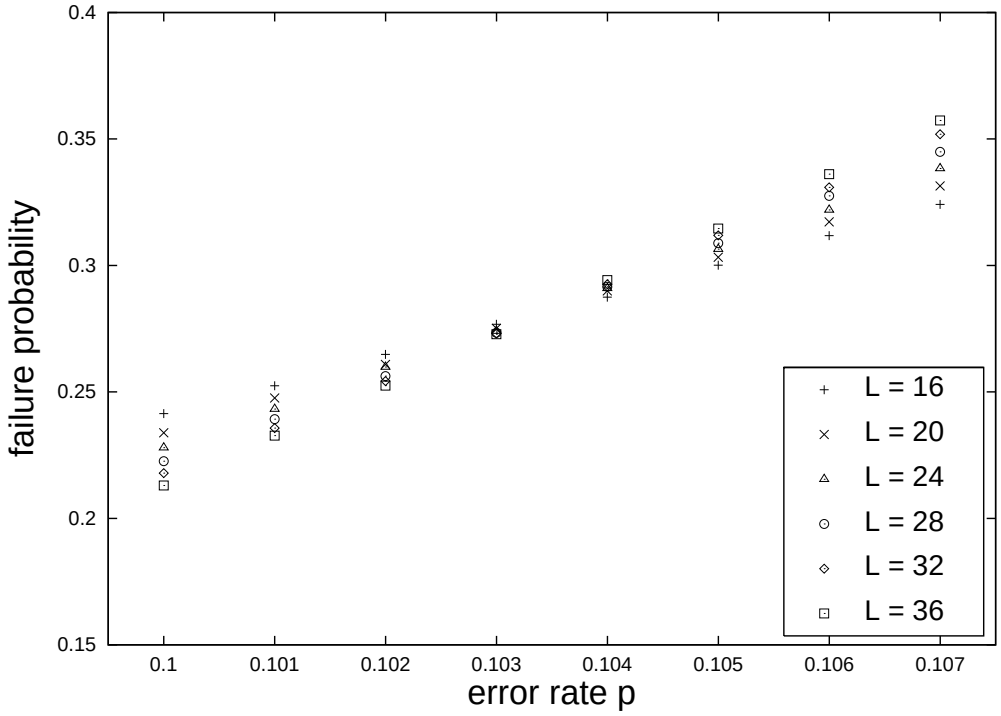

Figure 4.7: The failure probability P_{fail} as a function of the error probability p for linear size $L = 16, 20, 24, 28, 32, 36$, in the two-dimensional random-bond Ising model. Each data point was generated by averaging 10^6 samples.

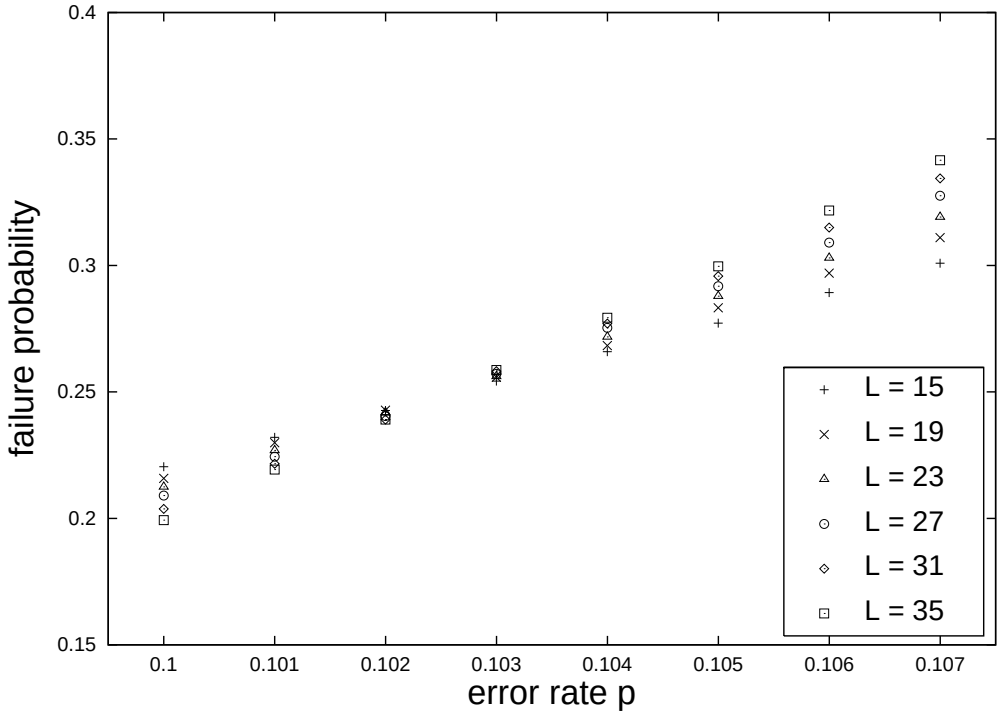

Figure 4.8: The failure probability P_{fail} as a function of the error probability p for linear size $L = 15, 19, 23, 27, 31, 35$, in the two-dimensional random-bond Ising model. Each data point was generated by averaging 10^6 samples.

where $x = (p - p_{c0})L^{1/\nu_0}$, adopting a quadratic approximation to the scaling function $f(x)$ in the vicinity of $x = 0$. (In the range of x we considered, the quadratic term is small but not quite negligible.) For even L ranging from 22 to 42, our fit found

$$\begin{aligned} p_{c0} &= .10330 \pm .00002 \ , \\ \nu_0 &= 1.49 \pm .02 \ , \end{aligned} \tag{4.40}$$

where the quoted errors are one-sigma statistical errors. For odd L ranging from 21 to 37, our fit found

$$\begin{aligned} p_{c0} &= .10261 \pm .00003 \ , \\ \nu_0 &= 1.46 \pm .02 \ . \end{aligned} \tag{4.41}$$

The discrepancy between the values of p_{c0} for even and odd L indicates a non-negligible finite-size effect.

On closer examination, we see evidence for small but detectable violations of our scaling ansatz in both the even and odd data sets. These violations are very well accounted for by the modified ansatz

$$\begin{aligned} P_{\rm fail} &= A + Bx + Cx^2 \\ &\quad + \begin{cases} D_{\rm even} \cdot L^{-1/\mu_{\rm even}} & \text{(L even)} \ , \\ D_{\rm odd} \cdot L^{-1/\mu_{\rm odd}} & \text{(L odd)} \ , \end{cases} \end{aligned} \tag{4.42}$$

which includes a nonuniversal additive correction to $P_{\rm fail}$ at criticality, different for even and odd sizes. Fitting the modified ansatz to the data for even L ranging

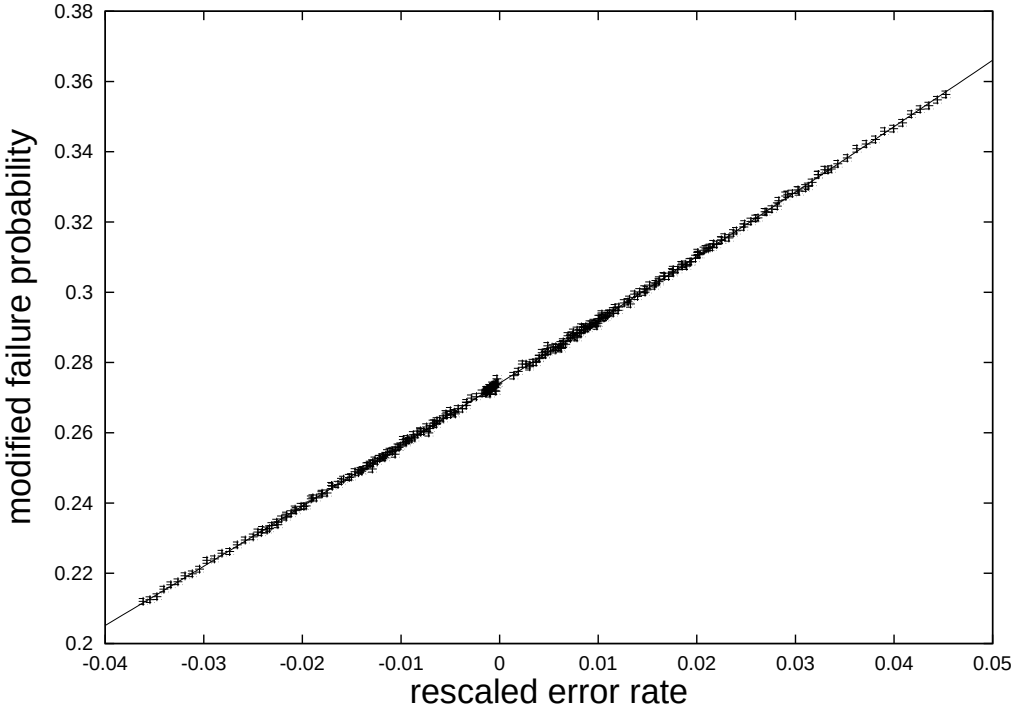

Figure 4.9: The failure probability P_{fail}, with the nonuniversal correction of eq. (4.42) subtracted away, as a function of the scaling variable $x = (p - p_{c0})L^{1/\nu_0}$ for the two-dimensional random-bond Ising model, where p_{c0} and ν_0 are determined by the best fit to the data. A two-sigma error bar is shown for each point. The data for values of L from 2 to 42 lie on a single line, indicating that the (small) scaling violations are well accounted for by our ansatz.

from 2 to 42, we find

$$\begin{aligned} p_{c0} &= .10309 \pm .00003 \ , \\ \nu_0 &= 1.461 \pm .008 \ , \\ D_{\rm even} &= 0.165 \pm .002 \ , \quad \mu_{\rm even} = 0.71 \pm .01 \ . \end{aligned} \tag{4.43}$$

Fitting to the data for odd L ranging from 3 to 37, we find

$$\begin{aligned} p_{c0} &= .10306 \pm .00008 \ , \\ \nu_0 &= 1.463 \pm .006 \ , \\ D_{\rm odd} &= -.053 \pm .003 \ , \quad \mu_{\rm odd} = 2.1 \pm .3 \ . \end{aligned} \tag{4.44}$$

In Figure 4.9 we show the data for all values of L and p; using the values of p_{c0}, ν_0, D, and μ found in our fits, we have plotted $P_{\rm fail}$, with the nonuniversal correction of eq. (4.42) subtracted away, as a function of the scaling variable $x = (p - p_{c0})L^{1/\nu_0}$. All of the data lie on a single line, indicating that residual scaling violations are quite small. Furthermore, the agreement between the values of p_{c0} and ν_0 extracted from the even and odd data sets, which were fit independently, indicates that our extrapolation to large L is reasonable, and that the statistical errors in eq. (4.43, 4.44) do not seriously underestimate the actual errors in our measurement. A plausible conclusion is that

$$\begin{aligned} p_{c0} &= .1031 \pm .0001 \ , \\ \nu_0 &= 1.46 \pm .01 \ . \end{aligned} \tag{4.45}$$

An earlier measurement reported by Kawashima and Rieger found [44]

$$\begin{aligned} p_{c0} &= .104 \pm .001 \ , \\ \nu_0 &= 1.30 \pm .02 \ ; \end{aligned} \tag{4.46}$$

their value of p_{c0}, but not of ν_0, is compatible with ours. An important reason why our value of p_{c0} has a smaller statistical error than theirs is that they computed a different observable (the domain wall energy) for which the finite-size scaling analysis is more delicate than for the failure probability (another critical scaling exponent is involved).

In a recent study of the Nishimori point, Merz and Chalker found [58]

$$\begin{aligned} p_c = &\quad .1093 \pm .0002 \ , \\ \nu = &\quad 1.50 \pm .03 \ . \end{aligned} \tag{4.47}$$

There is a clear discrepancy between the values of p_c and p_{c0}, in disagreement with the conjecture of Nishimori [64] and Kitatani [49]. Evidence for a reentrant phase diagram has also been found by Nobre [68], who reported

$$p_{c0} = .1049 \pm .0003 \ . \tag{4.48}$$

In principle, the phase transitions at $T = 0$ and at the Nishimori point could be in different universality classes, so that the critical exponents ν_0 and ν could have different values. However, our measurement of ν_0 at $T = 0$ is consistent with the value of ν at the Nishimori point reported by Merz and Chalker [58].

4.5.3 Random-plaquette gauge model

We measured P_{fail} by generating 10^7 samples for each value of L from 10 to 19, and for each value of p increasing in increments of .0004 from .02805 to .03005. Values of P_{fail} for even L lie slightly but systematically above the values for odd L at the same p; therefore we analyzed the data for even and odd L separately. Data for even L are shown in Figure 4.10, and data for odd L are shown in Figure 4.11. Crudely, the point of concordance of the data sets provides an estimate of p_{c0}, while the trend of the data with L determines the exponent ν_0.

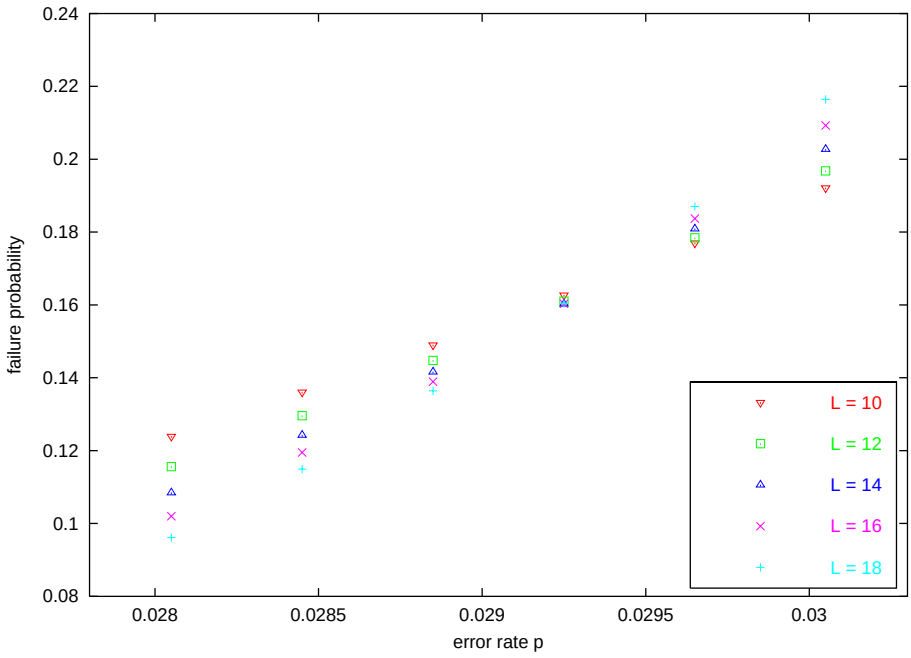

Figure 4.10: The failure probability P_{fail} as a function of the error probability p for linear size $L = 10, 12, 14, 16, 18$, in the three-dimensional random-plaquette gauge model. Each data point was generated by averaging 10^7 samples.

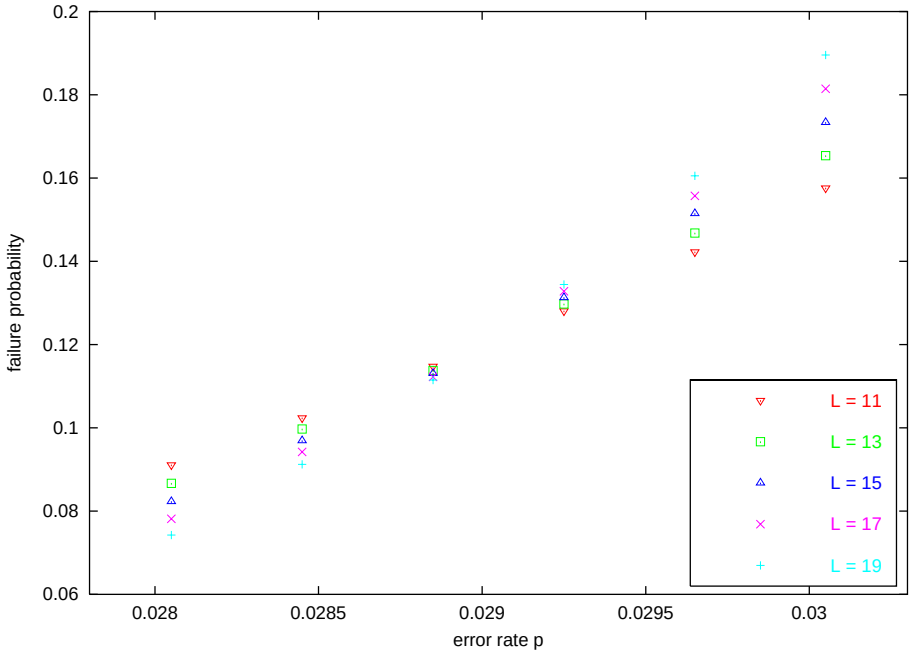

Figure 4.11: The failure probability P_{fail} as a function of the error probability p for linear size $L = 11, 13, 15, 17, 19$, in the three-dimensional random-plaquette gauge model. Each data point was generated by averaging 10^7 samples.

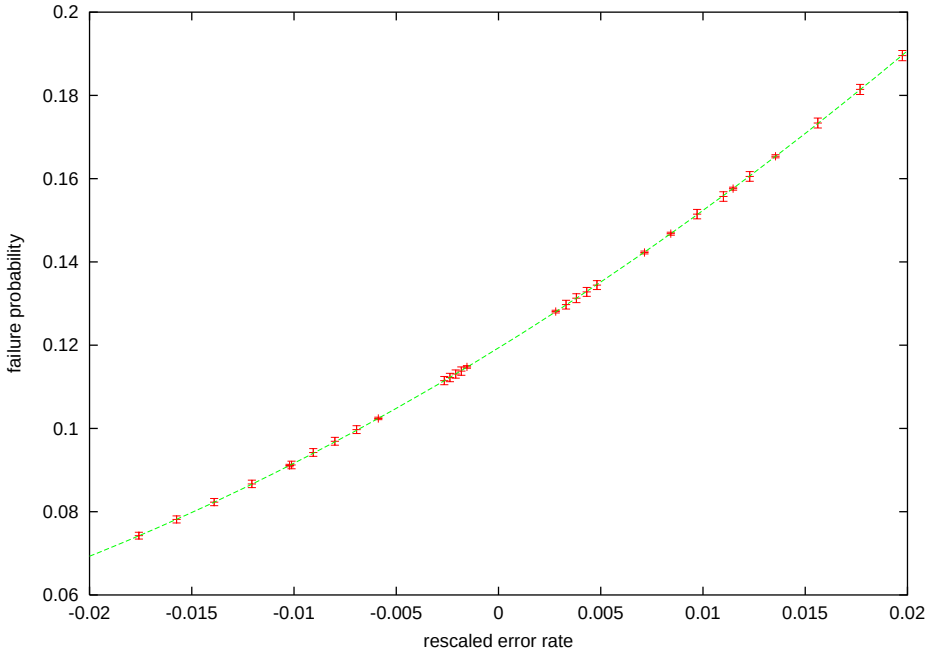

Figure 4.12: The failure probability P_{fail} as a function of the scaling variable $x = (p - p_{c0})L^{1/\nu_0}$ for the random-plaquette gauge model, where p_{c0} and ν_0 are determined by the best fit to the data. A ten-sigma error bar is shown for each point (to demonstrate how well the points fit the given quadratic curve). Those points with smaller error bars were averaged from 10^8 samples (as opposed to 10^7 samples for the other points). The data for all odd values of L from 11 to 19 lie on a single curve, indicating that scaling violations are small at these lattice sizes.

We did a global fit of the data to the form

$$P_{\text{fail}} = A + Bx + Cx^2 \ , \tag{4.49}$$

where $x = (p - p_{c0})L^{1/\nu_0}$, adopting a quadratic approximation to the scaling function $f(x)$ in the vicinity of $x = 0$. For L ranging from 10 to 19, our fit found

$$\begin{aligned} p_{c0} &= .029351 \pm .000014 \ , \quad \nu_0 = 0.980 \pm .018 \ (L \text{ even}) \ , \\ p_{c0} &= .028992 \pm .000002 \ , \quad \nu_0 = 1.006 \pm .003 \ (L \text{ odd}) \ , \end{aligned} \tag{4.50}$$

where the quoted errors are one-sigma statistical errors. The results for even and odd L are incompatible, indicating a non-negligible finite-size effect.

We believe that our analysis for odd L is likely to be more reliable; finite size effects are enhanced for even L, the case in which the failure probability is larger. All of the odd-L data are shown in Figure 4.12, with P_{fail} plotted as a function of $x = (p - p_{c0})L^{1/\nu_0}$, where p_{c0} and ν_0 are determined by our fit. The data fit a single curve, indicating that scaling violations are small. (Scaling violations are more discernable in the even-L data set.) A reasonable conclusion is that

$$\begin{aligned} p_{c0} = &\quad .0290 \pm .0001 \ , \\ \nu_0 = &\quad 1.00 \pm .02 \ . \end{aligned} \tag{4.51}$$

4.5.4 Anisotropic random-plaquette gauge model

We also measured P_{fail} for differing values of the bit-flip (or phase-flip) error probability p and the measurement error probability q. This corresponds to a three-dimensional random-plaquette gauge model with differing disorder strength in the horizontal and vertical plaquettes.

For fixed values of p and q, P_{fail} was computed for lattices over a range of horizontal sizes, each with an optimal vertical size (corresponding to the number of measurements performed on the lattice before performing error correction by

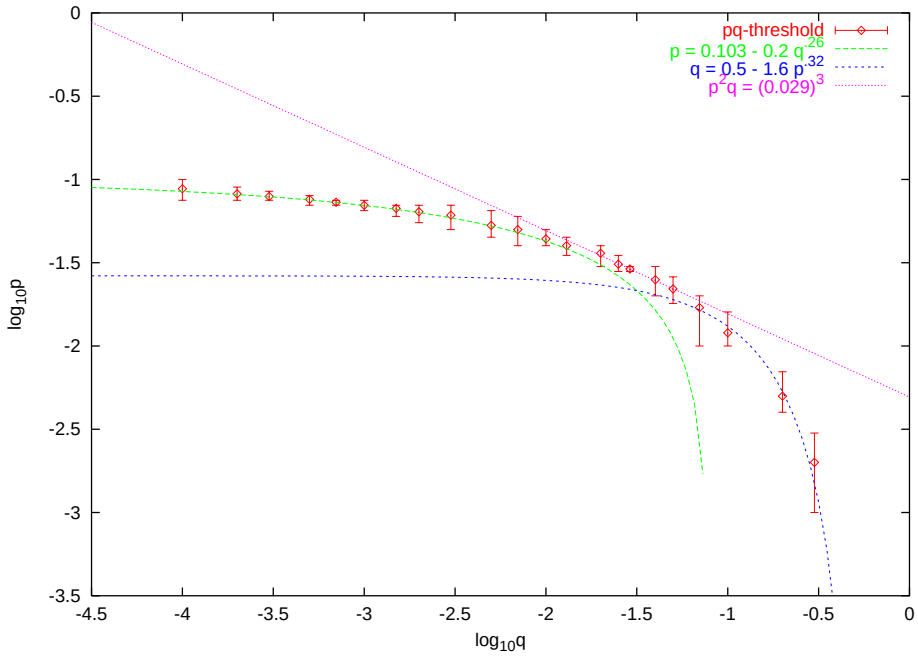

Figure 4.13: A log-log plot of the accuracy threshold curve for varying qubit and measurement error probabilities p and q. The horizontal axis is $\log_{10} q$ and the vertical axis is $\log_{10} p$. Data points are calculated by observing where error correction transitions from becoming more and more to less and less successful for increasing lattice sizes. The errorbars signify the region of high confidence for the placement of the threshold curve. The blue and green dashed lines are power fits in the regions of small p and small q, as given by eqs. (4.52, 4.53). The magenta dotted line is the curve $p^2 q =$ constant, using the the threshold value $p = q = 0.029$ found in the isotropic model.

the Edmonds perfect matching algorithm [29, 6]). By observing whether P_{fail} got larger or smaller with increasing lattice sizes, we could infer whether a particular pair of values for p and q was above or below the threshold curve. From this data, we could then generate a (rough) plot of the accuracy threshold curve in the pq-plane. Our conclusions are summed up in Figure 4.13. We have included the isotropic point $p = q = 0.029$ determined from the previous section.

We have fit our data to various curves involving either powers or entropies of p and q, but given the levels of uncertainty in the data, we cannot conclude that any of these generated fits really describes the threshold curve. However, we can separately state the small p and small q behavior of this curve:

$$q \approx 0.5 - 1.6p^{0.32} \quad \text{(for small } p\text{)} \tag{4.52}$$

$$p \approx 0.103 - 0.2q^{0.26} \quad \text{(for small } q\text{)} \tag{4.53}$$

Also, we observe that for moderate values of p and q (close to the isotropic point $p = q = 0.029$), the threshold data is well fit by $p^2q = \text{constant}$.

4.5.5 The failure probability at finite temperature

Our numerical studies of the RBIM and the RPGM were restricted to the $T = 0$ axis. We calculated the failure probability to estimate the critical disorder strength p_{c0} and the critical exponent ν_0. Here we will describe how the calculation of the failure probability could be extended to nonzero temperature.

To calculate the failure probability in the zero-temperature RBIM, we generate a sample by specifying a one-chain E of antiferromagnetic links, and then we construct the one-chain E' of minimal energy with the same boundary as E. Failure occurs if the cycle $D = E + E'$ is homologically nontrivial.

At nonzero temperature we should construct E' to belong to the homology class that minimizes free energy rather than energy. For a given sample with antiferromagnetic one-chain E, the free energy $F(E, h)$ of homology class h is

found by summing over domain wall one-chains $\{E'\}$ such that $E + E' \in h$:

$$\exp[-\beta F(E,h)] = Z(E,h) = \sum_{E' : E+E' \in h} e^{-\beta H_E} \ , \tag{4.54}$$

where H_E denotes the Hamiltonian eq. (4.1) with antiferromagnetic chain E. If the trivial homology class $h = e$ has the lowest free energy, then the sample is a "success"; otherwise it is a "failure." We can estimate the failure probability $P_{\text{fail}}(p,T)$ by randomly generating many samples, and determining for each whether it is a success or a failure.

For the random bond Ising model on a torus, the sum eq. (4.3) includes only the chains E' such that $E + E'$ is in the trivial homology class. To sum over the class h, we can augment E by adding to it a representative of h. For each h, we can compute

$$\frac{Z(E,h)}{Z(E,e)} = \exp\big[-\beta\big(F(E,h) - F(E,e)\big)\big] \ ; \tag{4.55}$$

the sample E is a success if this ratio of partition functions is less than one for each $h \neq e$.

The ratio is the thermal expectation value $\langle \mathcal{O}_h \rangle_K$ of an observable $\mathcal{O}_h$ that "inserts a domain wall" wrapping around a cycle C representing h. That is, the effect of $\mathcal{O}_h$ is to flip the sign of the bond variable τ_{ij} for each bond $\langle ij \rangle$ in C:

$$\mathcal{O}_h = \exp\left[-2K \sum_{\langle ij \rangle \in C} \tau_{ij} S_i S_j \right] \ . \tag{4.56}$$

In principle, we could measure $\langle \mathcal{O}_h \rangle_K$ by the Monte Carlo method, generating typical configurations in the thermal ensemble of H_E, and evaluating $\mathcal{O}_h$ in these configurations. Unfortunately, this method might not produce an accurate measurement, because the configurations that dominate $\langle \mathcal{O}_h \rangle_K$ may be exponentially rare in the thermal ensemble — a configuration with excited bonds on C can have an exponentially large value of $\mathcal{O}_h$ that overcomes exponential Boltzmann suppression.

One solution to this problem is to express $Z(E,h)/Z(E,e)$ as a product of quantities, each of which *can* be evaluated accurately by Monte Carlo. Let $\{e = P_0, P_1, P_2, \ldots P_{k-1}, P_k = C\}$ be a sequence of open chains interpolating between the empty chain and the cycle C, where $P_{j+1} - P_j$ contains just a single bond. We may write

$$\frac{Z(E,h)}{Z(E,e)} = \frac{Z(E,P_1)}{Z(E,P_0)} \cdot \frac{Z(E,P_2)}{Z(E,P_1)} \cdot \cdots \cdot \frac{Z(E,P_k)}{Z(E,P_{k-1})} \ . \tag{4.57}$$

Each ratio $Z(E,P_{j+1})/Z(E,P_j)$ is the expectation value of an operator that acts on a single bond, evaluated in the thermal ensemble of the Hamiltonian with antiferromagnetic bonds on the chain $E + P_j$; this expectation value can be evaluated by Monte Carlo with reasonable computational resources. (For an application of this trick in a related setting, see [25].)

Using this method, we can determine whether $Z(E,h)/Z(E,e)$ exceeds one for any $h \neq e$ and hence whether the sample E is a success or a failure. Generating many samples, we can estimate $P_{\text{fail}}(p,T)$. In principle, then we can calculate the failure probability for the optimal recovery scheme, in which p and T obey Nishimori's relation. By a similar method, we can calculate the failure probability for the RPGM. However, we have not attempted this calculation.

4.6 Conclusions

The three-dimensional random-plaquette gauge model, and the analogous antisymmetric tensor models in higher dimensions, provide new examples of multicritical points with strong disorder. These models have phase diagrams that qualitatively resemble the phase diagram of the two-dimensional random-bond Ising model.

Our results indicate that the boundary between the ferromagnetic and paramagnetic phases of the RBIM is reentrant rather than vertical below the Nishimori line. If the disorder strength p satisfies $p_{c0} < p < p_c$, then the ground state of the spin system does not have long-range order. As the temperature T increases with

p fixed, long-range order is first restored, and then lost again as the temperature increases further. At $T = 0$ the spins are frozen in a disordered state driven by quenched randomness. But apparently this ground state is entropically unfavorable — at low but nonzero temperature typical states in the thermal ensemble have long-range ferromagnetic order.

This behavior seems less remarkable when considered from the viewpoint of our error recovery protocol. For given p and a specified error syndrome, the recovery method with optimal success probability proceeds by inferring the most likely homology class of errors consistent with the syndrome. There is no *a priori* reason for the most likely single error pattern (the ground state) to belong to the most likely error homology class (the class with minimal free energy) even in the limit of a large sample. Our numerical results indicate that for error probability p such that $p_{c0} < p < p_c$, the probability that the ground state does not lie in the most likely homology class remains bounded away from zero as $L \to \infty$.

In our numerical studies of the RBIM and RPGM at zero temperature, we have computed a homological observable, the failure probability. This observable has advantages over, say, the domain wall energy, because it obeys a particularly simple finite-size-scaling ansatz. Therefore, we have been able to determine the critical disorder strength p_{c0} and the critical exponent ν_0 to good accuracy with relatively modest computational resources.

Not surprisingly, our numerical values for p_{c0} are notably larger than rigorous lower bounds derived using crude combinatoric arguments in [26]: $p_{c0} \approx .1031$ compared with the bound $p_{c0} \geq .0373$ in the RBIM, and $p_{c0} \approx .0290$ compared with $p_{c0} \geq .0114$ in the RPGM.

The zero-temperature critical disorder strength p_{c0} is a lower bound on the value of the critical disorder strength p_c along the Nishimori line, and of special interest because of its connection with the accuracy threshold for robust storage of quantum information. Our result means that stored quantum data can be preserved with arbitrarily good fidelity if, in each round of syndrome measurement, qubit errors and syndrome measurement errors are independently and identically

distributed, with error probability per qubit and per syndrome bit both below 2.9%. For qubit errors and measurement errors occurring at differing rates, an accuracy threshold has been inferred by analyzing an anisotropic random-plaquette gauge model, with differing disorder strength for horizontal and vertical plaquettes. Future work is needed to more conclusively identify the tradeoff curve in this model. Relating these threshold error rates to fidelity requirements for quantum gates requires further analysis of the sort discussed in [26].

We have also measured the critical exponent ν_0 that controls the divergence of the correlation length as p approaches p_{c0}, finding $\nu_0 \approx 1.46$ in the RBIM and $\nu_0 \approx 1.0$ in the RPGM. The value of ν_0 is also relevant to the efficacy of quantum error correction — through its connection with finite-size scaling, ν_0 determines how large the code block should be to achieve a specified storage fidelity, for p less than but close to p_{c0}.

Quantum computers are believed to be more powerful than classical computers — classical computers are unable to simulate quantum computers efficiently. The accuracy threshold for quantum memory is a fascinating phase transition, separating a low-noise quantum phase from a high-noise classical phase. In this paper, we have described one way to analyze this phase transition using methods from traditional statistical physics. Furthermore, the connection with quantum memory provides an enlightening new perspective on local spin and gauge systems with strong quenched disorder.

Chapter 5

Protecting topological quantum information by local rules

5.1 Abstract

Kitaev's surface codes (*e.g.,* toric codes and planar codes) [48] are two-dimensional topological quantum error-correcting codes which have the attractive features of requiring only local measurements and being robust to local clusters of errors. Previously [26], processing the error syndromes required global communication and reasonably fast classical computation, with a resource cost (in processing time) that scaled polynomially with the size of the lattice. In this work, we present a fairly simple set of local rules that handle the error syndrome processing (so that much of the computation and communication can be done in parallel). We make use of several ideas from a proof by Gács [31, 33, 39] of the existence of robust one-dimensional classical cellular automata to demonstrate analytically that an accuracy threshold exists for storing quantum memory in our system. We show numerical results that suggest that the threshold for bit flip or phase flip errors per time step is at least 10^{-4}.

5.2 Introduction

Our aim is to present a fault-tolerant scheme for preserving quantum memory with only local controls on a two-dimensional lattice of spins. We begin with a discussion of robust classical cellular automata in Section 5.3 and highlight work by Gács. In Section 5.4 we outline our model and illustrate how the quantum error syndromes in toric codes are similar to those in a classical one-dimensional array. The syndrome error processing is detailed in Section 5.5, and the main rules for local error correction are laid out in Section 5.6. Our analytical proof of an accuracy threshold is developed in sections 5.7 and 5.8, and we present results from numerical simulations in Section 5.9. We conclude in Section 5.10 with a comparison of required resources for local error correction in classical and quantum memory, as well as suggestions for future work.

5.3 Robust cellular automata

There are numerous examples of *cellular automata* (networks of cells with local update rules) which exhibit complex behavior, rich structures, and even universal computation. For example, Conway's game of Life [14] defines a very simple set of rules on a rectangular grid of cells, each storing only one bit, where each cell updates based on its present state and the sum of its eight nearest neighbors. It is possible to create configurations which will, for example, continuously grow at an ever increasing rate or implement an arbitrary computation. (See [71] for a fascinating overview of this topic.) In a one-dimensional array of binary cells with nearest-neighbor interactions, Cook has demonstrated that a particular simple set of rules can carry out universal computation [57]. While not strictly a cellular automaton, determining consistency of a partial revealing of a Minesweeper game has been shown by Kaye [46] to be equivalent to the NP-complete SAT problem.

Kaye has also demonstrated how to build a Turing computer out of an infinite Minesweeper grid [45].

However, most of these examples break down if the rules are allowed to fail occasionally. If we presume an error model where each cell independently (in space and in time) has some nonzero probability of executing any possible update rule (with the same interaction range as the default rule), then the specially crafted configurations mentioned above tend to fall apart after a short while. In other words, most cellular automata are not robust to faults in their evolution. A significant issue is that any cell can only directly communicate within some restricted interaction range (also known as its *neighborhood*). Cells on the boundary of an affected region may not be able to determine which are correct and which need to be fixed. Furthermore, if a cluster of errors occurs that is larger than the size of a cell's neighborhood, an interior cell may not even know that its data has been corrupted. Robust cellular automata seem to require a means for long-range communication and collective decisions on which cells need to be corrected; this must be accomplished solely by passing local messages around (which is a process that could also be corrupted occasionally).

If we're only concerned with memory, there is a set of stabilizing local rules known as Toom's rule [82] that can protect a bit of memory within a rectangular block of cells, each storing one copy of the bit. One form of Toom's rule is to update a cell by taking the majority vote of itself, its northern neighbor, and its eastern neighbor. If a cluster of errors is introduced (flipping the stored bit in a cluster of cells), this rule will tend to "eat away" at the error cluster in a preferred direction. This introduces an asymmetry that gives a preference to an "ocean" of correct cells over an "island" of altered cells. Given an infinite grid of cells and an error rate below some threshold, any error would eventually get corrected. Gács and Reif proved that (finite) sheets of cells evolving under this rule can maintain memory well enough to implement computation in a three-dimensional lattice with high fidelity [34].

Toom's rule works great for two-dimensional arrays, but there doesn't appear

to be any direct analogue in one-dimensional arrays. It had been conjectured that robust one-dimensional cellular automata for storing memory did not exist [52] (known as the "Positive Rates Conjecture"). Eventually, large clusters of errors would occur that would be uncorrectable, because the boundaries in one-dimensional arrays are zero-dimensional points, and it seems impossible to make a reliable local decision around the boundary of which side is valid and which side needs to be corrected. Gács proved this conjecture wrong in some amazing work [31, 33] that is unfortunately hard to read through. We highly recommend Gray's reader's guide [39] as a source for learning about the main ideas of Gács's proof, along with a simplified model of his construction.

5.4 Toric codes and implementation

Here we briefly review the structure of toric codes in the stabilizer formalism and suggest how to construct a quantum system with this encoding.

5.4.1 Toric code stabilizers

Toric codes are discussed in Section 4.4.1. The important features are repeated here. Qubits are placed on the edges of an $L \times L$ rectangular lattice. The stabilizers are generated by $X \otimes X \otimes X \otimes X$ around each plaquette and $Z \otimes Z \otimes Z \otimes Z$ around each site. (See Figure 4.3 for a diagram of these operators.) An odd number of phase flips acting on the qubits around a given lattice site causes the $XXXX$ syndrome measurement to change sign. Likewise, an odd number of bit flips acting on the qubits around a plaquette (or equivalently, around a site on the dual lattice) causes the corresponding $ZZZZ$ measurement to change sign. A long chain of errors is detected only at its endpoints, because there are an even number of errors around interior sites, which commute with those syndrome measurements. The bit flip and phase flip errors appear as one-dimensional chains with zero-dimensional (point) boundaries, which can be related to classical errors

in a one-dimensional array. The primary difference is that these errors live on a two-dimensional surface, and any trivial loop of errors (a closed chain that can be contracted down to a point) is in the stabilizer group and thus acts as the identity on the encoded subspace.

5.4.2 Hardware layout

We consider implementing a toric code by arranging a rectangular lattice of spins on a torus. For sufficiently large lattices, the behavior of toric codes is well approximated by that of planar codes (in particular, in terms of the value of the accuracy threshold), so it is possible to use a planar lattice in practice, but we will assume a toric layout in this work. The spin-$\frac{1}{2}$ particles are placed on each edge, or *link*, of the lattice. Thus, an $L \times L$ lattice consists of $2L^2$ spins. At each vertex, or *site*, we place a classical processor that will be responsible for measuring the four spins on its neighboring links and executing phase flips on those links when needed.

We also place a classical processor at every site of the dual lattice (which is obtained by rotating all of the links by 90 degrees). This set of processors is responsible for measuring the four neighboring spins around each site (on the dual lattice), as well as executing bit flips when needed. Since the phase flip and bit flip error correction can be performed independently of one another, we will focus on just phase flip errors in this model, recognizing that an identical process is going on simultaneously to handle bit flip errors.

5.4.3 Error model

In between each error correction step, we assume that every spin independently has a probability p_{phase} of undergoing a phase flip (and likewise, independently a probability p_{bit} of undergoing a bit flip). Since we will focus on phase flips (with bit flips being handled separately and simultaneously), we will simply describe the phase flip error rate as p. Also, we assume that each syndrome measurement of $XXXX$ independently has a probability q of being incorrect. We wish to

demonstrate that there exist thresholds for p and q which allow arbitrarily high fidelity for local error correction. We will assume that the classical processors and memory are very reliable. (In Section 5.8.3, we briefly discuss how this assumption could be relaxed.)

5.5 Processor memory

Following Gács's constructions [31, 33, 32], we impart a hierarchy on the layout of processors. We treat each processor as a *cell*, which will update its state based on its memory contents along with the memory contents of its eight nearest neighbors (north, northeast, east, southeast, south, southwest, west, and northwest). Rectangular groups of $Q \times Q$ cells are identified as belonging to a *colony*. Rectangular groups of $Q \times Q$ colonies are identified as belonging to a *super-colony*. This hierarchy continues on to higher and higher levels (until the whole lattice is included). We will assume that the linear lattice size $L = Q^k$ for some integer k. Errors will later be classified within a hierarchy of levels as well, and we will demonstrate how each level of errors will be handled by the corresponding level of colonies.

Several constants are hardcoded into the device, which will be explained below. They include Q (the colony size), U (the work period), f_C (the threshold for a cell's count), and f_N (the threshold for a neighboring cell's count). As a reference, we will later choose $Q = 16$, $U = 400$, $f_C = 4/5$, and $f_N = 1/5$ for deriving an accuracy threshold.

5.5.1 Memory fields

Every cell has the following fields of memory: `Address`, `Age`, and `Syndromes`. `Address` has two subfields `x` and `y` that identify the horizontal and vertical address of the cell in its colony. `Age` is a local "clock" that counts the number of time steps in a work period (of length U). `Syndromes` has nine subfields (each just a bit), which store the most recent syndrome measurements at this site and its eight

Table 5.1: Processor memory fields for local error correction of toric codes

field name	size	description
`Address`	$2\lceil \log Q \rceil$	horizontal and vertical address in colony
`Age`	$\lceil \log U \rceil$	local clock running from 0 to (U - 1)
`Syndromes`	9	syndrome at this site and its neighbors
`Count`	$9\lceil \log U \rceil$	coarse-grained count of syndrome history
`CountSignal`	8	value of neighboring colony's syndrome
`NewCountSignal`	8	temporary storage of value for `CountSignal`
`FlipSignal`	8	signal for flipping at end of a work period
`NewFlipSignal`	8	temporary storage of value for `FlipSignal`

neighboring sites. A cell's most recent measurement is denoted `Syndromes.C`, and the other subfields are `Syndromes.N`, `Syndromes.E`, `Syndromes.S`, `Syndromes.W`, `Syndromes.NE`, `Syndromes.SE`, `Syndromes.SW`, and `Syndromes.NW`, referring to the cell's northern, eastern, southern, western, and four diagonal neighbors, respectively.

The following fields of memory are also needed at some particular cells: `Count`, `CountSignal`, `NewCountSignal`, `FlipSignal`, and `NewFlipSignal`. The `Count` field has nine subfields (similar to `Syndromes`) which keep track of how often a syndrome is present at the center of a colony (either the current colony or one of its eight neighboring colonies) during a work period. The four "signal" fields provide a means of communication between colonies (traveling one cell per time step). They each have eight subfields corresponding to the eight directions making up the neighborhood of a cell. The `CountSignal` field contains the information of whether syndromes are present or absent at a particular time step in the centers of neighboring colonies. The `FlipSignal` field contains a signal for controlling flips across colonies at the end of a work period. The `NewCountSignal` and `NewFlipSignal` fields provide temporary storage of neighbors' values, before up-

dating `CountSignal` and `FlipSignal`. More specifically, during each time step the values in `CountSignal` for each cell are copied into its neighbors' `NewCountSignal` fields, which then replace `CountSignal`, and similarly `FlipSignal` is copied into neighboring cells via the `NewFlipSignal` field.

These additional fields could be included in every processor's memory (so that the required resources remain homogenous), but only the colony centers and a few other cells actually use their contents for decision making in our model. These extra memory contents could instead be utilized for increasing the reliability of the center sites' data through redundancy, if we considered faulty classical memory storage (which we mostly ignore in this present work).

The processor memory fields are summarized in Table 5.1. The size column reports the number of bits needed to store a field. For each level of the hierarchy, another set of all of these fields must be present (with Q and U replaced by Q^n and U^n for the nth level). Note that for typical values of the constants, the required memory for each processor is less than a kilobyte if only a few levels are implemented (as would likely be the case for any practical device). The device is initialized by setting all of the `Address` fields to each cell's relative position in its colony, and resetting all other fields to zero.

Gács [33] (see also Gray's description in [39]) avoids this increase in memory requirements for larger and larger lattices by implementing self-simulation in the classical processors. In his model, each level of the hierarchy of colonies (after the first) is simulated by the next lower level. In effect, each colony simulates a cell of a super-colony, and so on. However, an incredible amount of work needs to go into showing how such a simulation is possible with only local update rules and furthermore how it is robust to errors. Since the memory requirements to handle a few levels of colonies without self-simulation are very modest, we have decided to avoid these torturous details in order to focus on how our device handles quantum errors. We believe that it should be possible in principle to fully implement the ideas in his work so that the memory requirements become constant (independent of the size of the lattice or the amount of time desired to maintain memory), but

we have not worked through the details explicitly.

5.5.2 Memory processing

We assume that the processors are synchronized in our model. That is, the local clocks represented by the `Age` field march in lock step with one another. Gács [33] demonstrated that asynchronous classical processors can still robustly compute in a one-dimensional cellular array, but again we have decided to forego a lot of the burdensome details by not considering the most general model.

The general framework of the processing during each time step (and in parallel at each site) is as follows.

- The `Age` field is incremented by one (mod U).
- The syndrome $XXXX$ is measured, and its value is stored in `Syndromes.C`.
- The neighbors' syndrome measurements are copied into the respective subfields of `Syndromes`.
- The `CountSignal` subfields from neighboring cells are copied into the corresponding `NewCountSignal` subfields.
- The `FlipSignal` subfields from neighboring cells are copied into the corresponding `NewFlipSignal` subfields.
- At the center of a colony (which is determined from `Address` information), all `CountSignal` subfields are replaced with the value of `Syndromes.C`. Elsewhere, `CountSignal` is replaced with `NewCountSignal`.
- At the center of a colony, the `Count` field is updated based on `Syndromes.C` and `NewCountSignal` (details below). Elsewhere, `FlipSignal` is replaced with `NewFlipSignal`.
- Finally, the processor follows the basic rules outlined in Section 5.6 to possibly flip one of its neighboring spins or, if located at the center of a colony at the end of a work period, set its `FlipSignal` field.

Rather than just keeping a simple running total of error syndromes being present or absent (denoted as *on* or *off*), we have the `Count` field keep a coarse-grained count in the following manner. We choose $U = b^2$ (where b will be determined by the definition of low-level errors in our proof) and divide the work period U into b intervals of length b. The `Count` subfields are each divided into two sections of size $\lceil \log b \rceil$. The first section stores a running count of syndrome measurements during each interval. At the end of each interval (when `Age` $\equiv 0 \pmod{b}$), the second section is incremented if the first section totals at least $f_C b$ (for `Count.C`) or at least $f_N b$ (for the other eight `Count` subfields). The first section is then reset to 0. Finally, at the end of the work period, a `Count` subfield is considered to be on if its second section is at least $f_C b$ or $f_N b$, as before. Thus, a syndrome is considered to be present in the colony during a work period if, during at least f_C of the intervals, it is present at the center for at least f_C of the time steps.

The `FlipSignal` field stores the decision of a colony center at the end of a work period of whether to introduce a flip along a path to a neighboring colony. This signal is propagated cell by cell until it reaches another colony center after Q time steps. All sites with a `FlipSignal` on then perform the desired flip in unison, and `FlipSignal` is reset to zero (or off). In this manner, a colony center can affect a chain of flips between two neighboring colonies. An analogous process occurs every U^2 time steps between neighboring super-colonies, and similarly for higher levels in the hierarchy.

5.6 Local rules

The basic rules are as follows. The first two sets of rules handle flips of qubits along the border of neighboring colonies. The remaining rules handle the interior qubits in a colony. Each qubit is only ever controlled by a single processor. When there is an option in terms of which qubit to flip (*e.g.,* north or east), the direction

could be chosen either at random or always to be a fixed value. In our simulations, we chose the direction that pointed away from the closest border to the colony (which was determined by `Address` information).

(W border) If `Address.x` $== 0$, then:

if `Syndromes.C` is off,	do nothing
else if `Syndromes.NW` is on,	flip west
else if `Syndromes.W` is on,	flip west
else if `Syndromes.SW` is on,	flip west
else,	continue below

(S border) If `Address.y` $== 0$, then:

if `Syndromes.C` is off,	do nothing
else if `Syndromes.SW` is on,	flip south
else if `Syndromes.S` is on,	flip south
else if `Syndromes.SE` is on,	flip south
else,	continue below

(SW quadrant) If `Address.x` $< \lfloor \frac{Q}{2} \rfloor$ and `Address.y` $< \lfloor \frac{Q}{2} \rfloor$, then:

if `Syndromes.C` is off,	do nothing
else if `Syndromes.S` is on,	do nothing
else if `Syndromes.W` is on,	do nothing
else if `Syndromes.N` is on,	flip north
else if `Syndromes.E` is on,	flip east
else if `Syndromes.SW` is on,	do nothing
else if `Syndromes.NW` is on,	flip north
else if `Syndromes.SE` is on,	flip east
else,	flip north or east

(W corridor) If `Address.x` $< \lfloor \frac{Q}{2} \rfloor$ and `Address.y` $== \lfloor \frac{Q}{2} \rfloor$, then:

if `Syndromes.C` is off,	do nothing
else if `Syndromes.S` is on,	do nothing
else if `Syndromes.W` is on,	do nothing
else if `Syndromes.N` is on,	do nothing
else if `Syndromes.E` is on,	flip east
else if `Syndromes.SW` is on,	do nothing
else if `Syndromes.NW` is on,	do nothing
else,	flip east

(NW quadrant) If `Address.x` $< \lfloor \frac{Q}{2} \rfloor$ and `Address.y` $> \lfloor \frac{Q}{2} \rfloor$, then:

if `Syndromes.C` is off,	do nothing
else if `Syndromes.W` is on,	do nothing
else if `Syndromes.N` is on,	do nothing
else if `Syndromes.E` is on,	flip east
else if `Syndromes.S` is on,	flip south
else if `Syndromes.NW` is on,	do nothing
else if `Syndromes.NE` is on,	flip east
else if `Syndromes.SW` is on,	flip south
else,	flip east or south

(N corridor) If `Address.x` $== \lfloor \frac{Q}{2} \rfloor$ and `Address.y` $> \lfloor \frac{Q}{2} \rfloor$, then:

if `Syndromes.C` is off,	do nothing
else if `Syndromes.W` is on,	do nothing
else if `Syndromes.N` is on,	do nothing
else if `Syndromes.E` is on,	do nothing
else if `Syndromes.S` is on,	flip south
else if `Syndromes.NW` is on,	do nothing
else if `Syndromes.NE` is on,	do nothing
else,	flip south

(NE quadrant) If `Address.x` $> \lfloor \frac{Q}{2} \rfloor$ and `Address.y` $> \lfloor \frac{Q}{2} \rfloor$, then:

if `Syndromes.C` is off,	do nothing
else if `Syndromes.N` is on,	do nothing
else if `Syndromes.E` is on,	do nothing
else if `Syndromes.S` is on,	flip south
else if `Syndromes.W` is on,	flip west
else if `Syndromes.NE` is on,	do nothing
else if `Syndromes.SE` is on,	flip south
else if `Syndromes.NW` is on,	flip west
else,	flip south or west

(E corridor) If `Address.x` $> \lfloor \frac{Q}{2} \rfloor$ and `Address.y` $== \lfloor \frac{Q}{2} \rfloor$, then:

if `Syndromes.C` is off,	do nothing
else if `Syndromes.N` is on,	do nothing
else if `Syndromes.E` is on,	do nothing
else if `Syndromes.S` is on,	do nothing
else if `Syndromes.W` is on,	flip west
else if `Syndromes.NE` is on,	do nothing
else if `Syndromes.SE` is on,	do nothing
else,	flip west

(SE quadrant) If `Address.x` $> \lfloor \frac{Q}{2} \rfloor$ and `Address.y` $< \lfloor \frac{Q}{2} \rfloor$, then:

if `Syndromes.C` is off,	do nothing
else if `Syndromes.E` is on,	do nothing
else if `Syndromes.S` is on,	do nothing
else if `Syndromes.W` is on,	flip west
else if `Syndromes.N` is on,	flip north
else if `Syndromes.SE` is on,	do nothing
else if `Syndromes.SW` is on,	flip west
else if `Syndromes.NE` is on,	flip north
else,	flip west or north

(S corridor) If `Address.x` $== \lfloor \frac{Q}{2} \rfloor$ and `Address.y` $< \lfloor \frac{Q}{2} \rfloor$, then:

if `Syndromes.C` is off,	do nothing
else if `Syndromes.E` is on,	do nothing
else if `Syndromes.S` is on,	do nothing
else if `Syndromes.W` is on,	do nothing
else if `Syndromes.N` is on,	flip north
else if `Syndromes.SE` is on,	do nothing
else if `Syndromes.SW` is on,	do nothing
else,	flip north

(colony center) If `Address.x` $== \lfloor \frac{Q}{2} \rfloor$ and `Address.y` $== \lfloor \frac{Q}{2} \rfloor$, then:

if `Age` $== 0$, execute rules for colony neighbors and update `FlipSignal`

else, do nothing

5.7 Error decomposition proof

In this section, we define a hierarchy of sets of errors and derive a bound in equation (5.3) on the underlying error rates that will guarantee that higher-level errors become increasingly rarer. In the following section, we will show how the local update rules correct each level of errors. This section follows very closely the proof given in Gray [39].

As introduced previously, the colony size and the work period are denoted as Q and U. The following steps hold true provided that $Q \geq 4(a+2)$ and $U \geq 4(b+2)$, for some positive integers a and b.

Phase flip errors occur on the edges of the lattice, where the qubits are located. Errors in measuring the $XXXX$ syndrome occur at the vertices of the lattice. (Bit flip errors and $ZZZZ$ measurement errors can be treated as occurring on the edges and vertices of the dual lattice and can be handled analogously.) We can represent an error as a point (x, y, t), where t corresponds to the time step we are considering, and (x, y) corresponds to the coordinates in space of an error (either a site or the midpoint of an edge). Both x and y are integers for measurement errors, while one is a half-integer for phase flip errors.

Let us define two collections of points A, B as (l, m, n)-linked if there exists a spacetime box $[x, x + l) \times [y, y + m) \times [t, t + n)$ that contains at least one member of A and at least one member of B. Otherwise we will say that A and B are (l, m, n)-separated.

Let E be the set of phase flip errors and $XXXX$ measurement errors. We will

call a nonempty subset S of E a *candidate level-0 error* if S consists of either phase flip errors or $XXXX$ measurement errors, but not both, and if it is contained in a spacetime box $[x, x+1] \times [y, y+1] \times [t, t]$. S will be an *actual level-0 error* if S and $E \setminus S$ are (a, a, b)-separated, where a and b are fixed positive integers. The union of all actual level-0 errors is called *level-0 noise*, which we denote by E_0.

Now we proceed to define candidate and actual level-n errors inductively. For $n > 0$, suppose that candidate level-k errors, actual level-k errors, and level-k noise E_k have been defined for $k < n$.

A nonempty set $S \subseteq E \setminus E_{n-1}$ is a *candidate level-n error* if

(i) S is contained in a spacetime box of size $Q^n \times Q^n \times U^n$, and

(ii) S contains at least two disjoint candidate level-(n-1) errors that are $(aQ^{n-1}, aQ^{n-1}, bU^{n-1})$-linked.

S will be an *actual level-n error* if, additionally,

(iii) S does not contain two candidate level-n errors that are $(4(a+2)Q^{n-1}, 4(a+2)Q^{n-1}, 4(b+2)U^{n-1})$-separated, and

(iv) S and $E \setminus (S \cup E_{n-1})$ are (aQ^n, aQ^n, bU^n)-separated.

Level-n noise E_n is defined as the union of E_{n-1} and all actual level-n errors in E.

We will further define a candidate level-n error S as *minimal* if S contains exactly 2^n points. Now we will proceed to show by induction that every point in $E \setminus E_{n-1}$ belongs to at least one minimal candidate level-n error S. The base case of $n = 1$ is true provided that $Q \geq a$ and $U \geq b$ (so that two points that are (a, a, b)-linked fit inside a box of size $Q \times Q \times U$).

For the inductive step, let us assume that the hypothesis holds true for $(n-1)$. Let $\vec{x}_1 \equiv (x_1, y_1, t_1)$ be a spacetime point that is a member of $E \setminus E_{n-1}$; we will show that this point must belong to a minimal candidate level-n error. The point must be a member of $E \setminus E_{n-2}$, so by the inductive hypothesis it belongs to some minimal candidate level-(n-1) error S_1. The minimality implies that S_1 consists of

two disjoint minimal candidate level-(n-2) errors that are $(aQ^{n-2}, aQ^{n-2}, bU^{n-2})$-linked. Therefore, S_1 must fit into a box of size $(a+2)Q^{n-2} \times (a+2)Q^{n-2} \times (b+2)U^{n-2}$. Now, if any point in S_1 were part of an actual level-(n-1) error, then all of S_1 would be contained in that actual level-(n-1) error. But $\vec{x}_1 \in S_1$ and $\vec{x}_1 \notin E_{n-1}$, which means that S_1 must not be contained in any actual level-(n-1) error. Since S_1 satisfies condition (iii), it must not satisfy condition (iv). Then there exists some $\vec{x}_2 \in E \setminus E_{n-1}$ such that $\vec{x}_2 \notin S_1$ and $\vec{x}_2, S_1$ are $(aQ^{n-1}, aQ^{n-1}, bU^{n-1})$-linked. Now, it is true that $\vec{x}_2$ must belong to the set of points in $E \setminus E_{n-1}$ that are not in S_1 such that $\vec{x}_2, \vec{x}_1$ are $((a+1)Q^{n-1}, (a+1)Q^{n-1}, (b+1)U^{n-1})$-linked. The inductive hypothesis says that there must be a minimal candidate level-(n-1) error S_2 containing $\vec{x}_2$.

We can also choose S_2 such that S_1 and S_2 are disjoint. There are two cases to be considered. The first case is to suppose that there exists some $\vec{x}_2$ such that $\vec{x}_2$ is $2(a+2)Q^{n-2}$-separated from $\vec{x}_1$. Then the size restrictions on S_1 and S_2 force them to be disjoint. The second case is to suppose that the first case does not hold; i.e., there does not exist such an $\vec{x}_2$. Then at worst $S \equiv S_1 \cup S_2$ fits in a box of size $4(a+2)Q^{n-2} \times 4(a+2)Q^{n-2} \times 4(b+2)U^{n-2}$ which is $((a+1)Q^{n-1} - 4(a+2)Q^{n-2}, (a+1)Q^{n-1} - 4(a+2)Q^{n-2}, (b+1)U^{n-1} - 4(b+2)U^{n-2})$-separated from the rest of $E \setminus E_{n-1}$. Since $Q \geq 4(a+2)$ and $U \geq 4(b+2)$, S satisfies (i) and (iv) in the definition of an actual level-(n-1) error. But S also satisfies (ii) (since it contains S_1) and (iii). Then S must be an actual level-(n-1) error. However, we have already shown that S_1 cannot be in an actual level-(n-1) error, so the second case leads to a contradiction and cannot occur; then S_1 and S_2 can be chosen to be disjoint, and the set S is a minimal candidate level-n error containing $\vec{x}_1$.

This argument actually allows us to place more restrictive bounds on level-n errors. By replacing $(n-1)$ with n in the argument above, we can see that a minimal candidate level-n error S_1 fits into a box of size $(a+2)Q^{n-1} \times (a+2)Q^{n-1} \times (b+2)U^{n-1}$. Also, given a point $\vec{x}$ in $E \setminus E_{n-1}$ that is $(2(a+2)Q^{n-1}, 2(a+2)Q^{n-1}, 2(b+2)U^{n-1})$-separated from at least one member of S_1, the point $\vec{x}$ lies in a second minimal candidate level-n error S_2 that is disjoint from S_1. If S_1, S_2 are

$(4(a+2)Q^{n-1}, 4(a+2)Q^{n-1}, 4(b+2)U^{n-1})$-separated and also (aQ^n, aQ^n, bU^n)-linked, we can see from conditions (iii) and (iv) that S_1 and S_2 cannot be part of an actual level-n error. Thus, if S_1 is part of a actual level-n error, any point in $S \setminus S_1$ must be $(5(a+2)Q^{n-1}, 5(a+2)Q^{n-1}, 5(b+2)U^{n-1})$-linked with S_1. This means that the entire error will fit into a box of size $7(a+2)Q^{n-1} \times 7(a+2)Q^{n-1} \times 7(b+2)U^{n-1})$. We can take the intersection of this box with the bounding box of size $Q^n \times Q^n \times U^n$ from condition (i). This reveals that an actual level-n error fits inside a box of size $\min\{Q, 7(a+2)\}Q^{n-1} \times \min\{Q, 7(a+2)\}Q^{n-1} \times \min\{U, 7(b+2)\}U^{n-1}$. We will use this result in the proof demonstrating correction of higher level errors in Section 5.8.2.

Finally, let us define the level-n error rate ϵ_n as the probability that a box of size $Q^n \times Q^n \times U^n$ has nonempty intersection with at least one candidate level-n error. A spacetime box of unit size cannot include more than four edges and four vertices of the lattice, so clearly $\epsilon_0 \leq 4(p+q)$, where p and q are the phase flip and measurement error probabilities per time step. An upper bound on ϵ_n can be found by considering the probability that a box of size $Q^n \times Q^n \times U^n$ has nonempty intersection with at least one candidate level-(n-1) error. This probability must be bounded above by $Q^2 U \epsilon_{n-1}$. Gray asserts that by the Kesten-Vandenberg inequality, since each candidate level-n error is composed of at least two candidate level-(n-1) errors,

$$\epsilon_n \leq (Q^2 U \epsilon_{n-1})^2 \,. \tag{5.1}$$

Then we can see that

$$\epsilon_n \leq (Q^2U)^{2^{n+1}-2}(4(p+q))^{2^n} < (Q^4U^2 4(p+q))^{2^n} \text{for } n > 0 \,. \tag{5.2}$$

That is to say, level-n errors get progressively more rare (in fact, double exponentially) as n gets larger, as long as

$$(p+q) < Q^{-4}U^{-2}/4 \,. \tag{5.3}$$

Now, Gray further asserts that a simple Borel-Cantelli argument shows that given this condition, with probability 1 every error belongs to an actual level-n error for some $n \geq 0$.

5.8 Lower bound on accuracy threshold

5.8.1 Correction of level-0 errors

Any actual level-0 error (a set of only phase flip errors or only measurement errors fitting inside a $2 \times 2 \times 1$ spacetime box and (a, a, b)-separated from any other errors) get corrected automatically by the basic local rules (as laid out in Section 5.6). We can demonstrate this explicitly for several examples in figures 5.1 and 5.2. In the selected examples, we assume that these sites (denoted by black circles in the figures) are located in the southwest quadrant of a colony. (Errors located elsewhere in the colony would be handled similarly.) In the third example of Figure 5.1, the southwest site inside the dotted box decides to flip the qubit to its north in the first update, and the northwest site then flips the qubit to its east in the second update, which closes the chain of errors. In the fourth example of Figure 5.2, the southwest site flips the qubit to its east in the first time step, while all other sites do nothing, and during the second time step these actions are repeated. Note that a trivial loop of flips is a stabilizer operator of the toric code, and thus acts as the identity on the encoded qubits.

By exhausting over all possible configurations of actual level-0 errors, we see that they are always corrected within two time steps, provided that $a \geq 2$ and $b \geq 2$ (so as to be sufficiently isolated from any other noise).

5.8.2 Correction of higher level errors

An actual level-1 error fits inside a spacetime box of size $Q \times Q \times U$. It may be contained inside a single colony, or at worst, it is contained within a 2×2 grouping

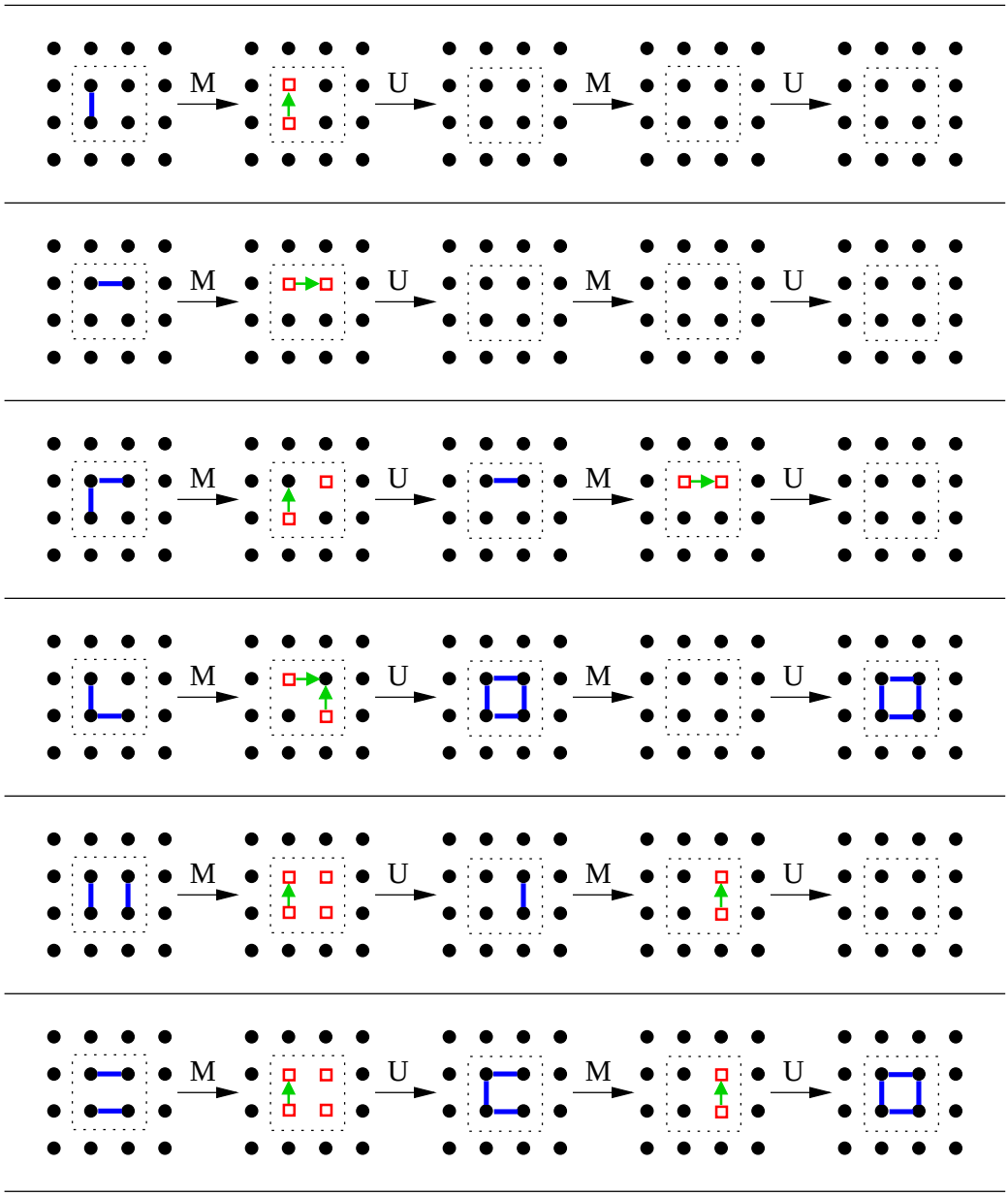

Figure 5.1: Examples of level-0 flip errors being corrected. The leftmost diagram in each row contains a distinct level-0 error. The blue lines are bit flip or phase flip errors. The red squares are sites with a nontrivial syndrome measurement. The green arrows are controlled flips based on the local update rules. Measurement and update steps are denoted by M and U.

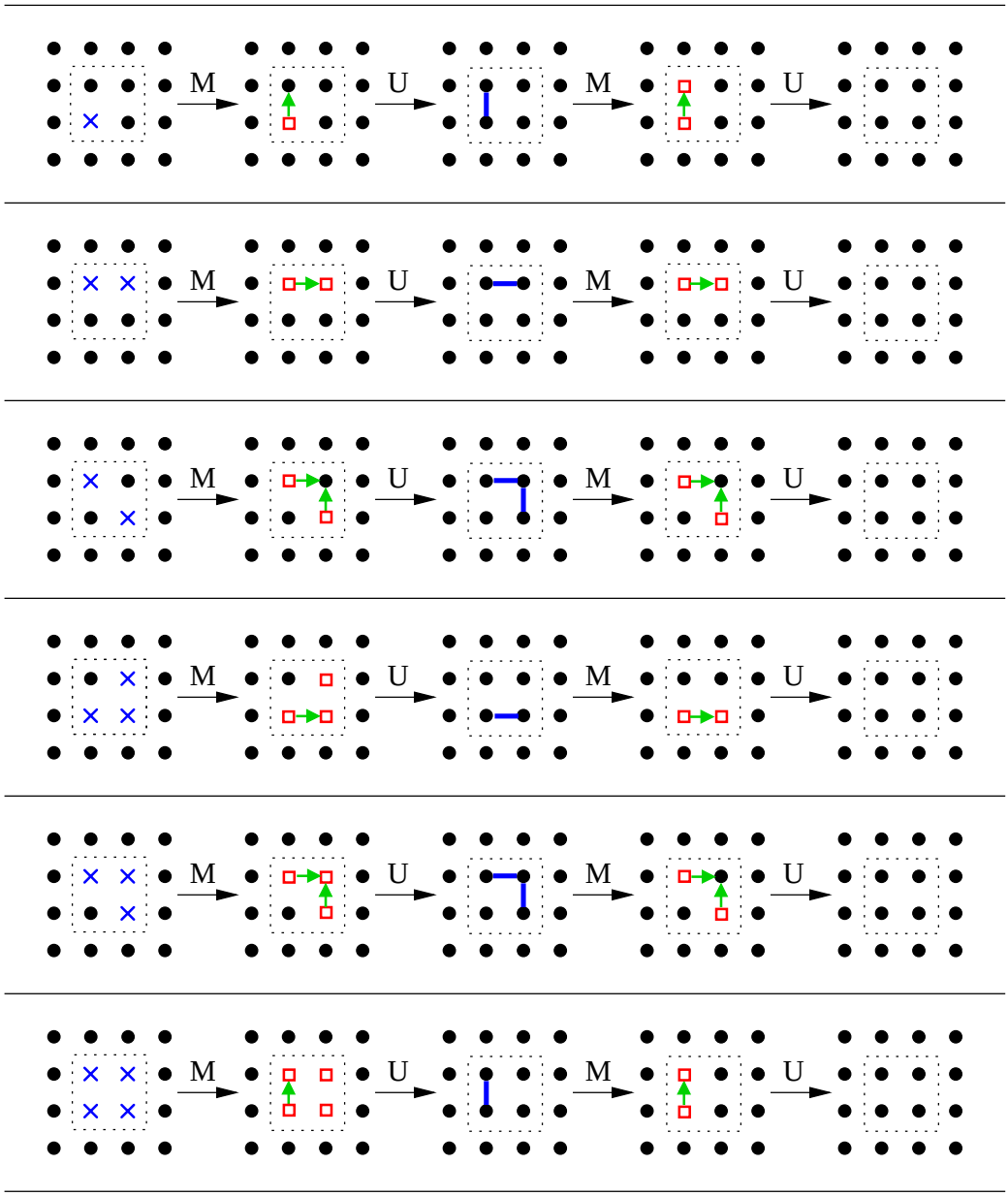

Figure 5.2: Examples of level-0 measurement errors being corrected. The leftmost diagram in each row contains a distinct level-0 error. The blue x's are measurement errors, and the blue lines are qubit errors. The red squares are sites with a nontrivial syndrome measurement. The green arrows are controlled flips based on the local update rules. Measurement and update steps are denoted by M and U.

of colonies. Any level-1 error (or higher-level error) that is completely contained within a single colony will be corrected in a straightforward manner by the basic local rules (Section 5.6). The two endpoints of such an error chain would drift toward the center of the colony, where they will meet up and form a trivial loop.

Error chains across colonies, however, require more sophisticated processing. We will show in the following argument that any actual level-n error will be corrected within $3U^n$ time steps, and that it will always be contained inside a space of $2Q^n \times 2Q^n$. Since actual level-n errors are (aQ^n, aQ^n, bU^n)-separated from one another, they will always get corrected before another one occurs (provided $a \geq 2$ and $b \geq 3$).

Suppose a level-1 error occurs that stretches across neighboring colonies. At the end of the current work period, let x_C and x_N be the computed syndromes (according to the `Count` field) at one of the affected colonies of itself and of its neighbor. There are four possible values for x_C and x_N, depending on at what point during the work period the ends of the error chain migrated to the centers of each colony, and also depending on how the colony centers were affected by level-0 noise. If x_C is zero (off), then this colony will do nothing. If both x_C and x_N are one (on), then the colony will make the proper decision to deal with this error by following the basic rules in Section 5.6 (based on the computed syndromes instead of its local neighborhood). The only dangerous case is when x_C is on, but x_N is off. The colony may then execute a flip (via `FlipSignal`) that moves its syndrome in the wrong direction and thereby increases the size of the level-1 error.

To prevent this last case from ever happening, we want to guarantee that if a level-1 error occurs with enough time left in the work period for the computed syndrome of a colony to be on, then the computed syndromes of its neighbors must be valid. So we will want to set the self-count threshold f_C to be as high as possible and the neighbor-count threshold f_N to be as low as possible. However, if f_C is too high, then level-0 noise could prevent a syndrome from ever turning on in a colony (by temporarily moving a syndrome away from the center), or if f_N is too low, then level-0 noise could masquerade as a higher-level syndrome (by

temporarily creating a syndrome at the center of a neighboring colony). Since actual level-0 errors are (a, a, b)-separated from one another, and since they are always corrected within two time steps, we could choose

$$f_N \;=\; \frac{4}{b}\,, \quad f_C \;=\; \frac{b-4}{b}\,. \tag{5.4}$$

Level-0 noise can then never affect the coarse-grained count of higher-level syndromes, because the presence or absence of syndromes at a colony center will never be changed by more than two during an interval of b time steps. (See the discussion of the `Count` field in Section 5.5.2.) Note that we could have chosen $f_N b = 3$ and $f_C b = (b-3)$, which would have been sufficient for dealing with level-0 noise, but we will need the choices of equation (5.4) to deal with higher level noise.

It now remains for us to find a bound on b that will guarantee the neighbor counts to be valid whenever a colony's syndrome is on. Near the end of Section 5.7, we derived another bound on the size of an actual level-1 error. In particular, we found that all of the points in the set of errors differ in time by no more than $7(b+2)$ time steps. If our level-1 error was a long chain of errors connecting the center of one colony to some site in a neighboring colony, the endpoint of the error chain in the neighboring colony should migrate to its center no later than $7(b+2)+2Q$ time steps after the appearance of a syndrome in the center of the first colony. It will also take Q time steps for the signal from the neighboring colony to reach the first colony center.

Suppose that the earliest point in the level-1 error occurs with T time steps remaining in the current work period. Then whenever

$$f_C b \le \left\lceil \frac{T}{b} \right\rceil \tag{5.5}$$

we require that

$$f_N b \le \left\lfloor \frac{T - 7(b+2) - 3Q}{b} \right\rfloor . \tag{5.6}$$

If we choose $a = 2$ (which is consistent with all previous bounds on a), then we

can choose colony size $Q = 4(a+2) = 16$. We can then rearrange equations (5.4), (5.5), and (5.6) to read

$$\left\lfloor \frac{T}{b} \right\rfloor \geq \left(11 + \frac{62}{b}\right) \quad \text{whenever} \quad \left\lceil \frac{T}{b} \right\rceil \geq (b-4)\,. \tag{5.7}$$

We can satisfy condition (5.7) for all values of T if we choose b such that

$$(b-5) \geq \left(11 + \frac{62}{b}\right)\,. \tag{5.8}$$

This holds true for $b \geq 20$. Previously we wanted $U = b^2$ (for the coarse-grained count), and we also required $U \geq 4(b+2)$ (for the error decomposition proof). We could choose $b = 20, U = 400$, or if we prefer working with powers of two, let $b = 32$ and $U = 1024$. In the first case $f_N = 1 - f_C = 1/5$ and in the second case $f_N = 1 - f_C = 1/8$.

Since the same rules are followed for correcting level-1 errors across neighboring colonies as are responsible for correcting level-0 errors across neighboring cells, we know that any actual level-1 error will be corrected within two workperiods, once the syndromes are reported at their colony centers. Depending on the value of T (the number of time steps remaining in the current work period when a level-1 error occurs), the computed syndromes may not be on until after a full work period. Consequently, the worst case for correcting actual level-1 errors requires no more than $3U$ time steps.

All of the above reasoning is valid for higher-level errors as well. In particular, the coarse-grained count was defined in such a way that level-(n-1) noise will not disrupt the counting of syndromes in a level-n colony. The only noteworthy change is that for correcting a level-n error, the $3Q$ term appearing in equation (5.6) gets replaced by $\frac{3Q^n}{U^{n-1}}$, which is strictly less than $3Q$ (if $Q < U$), so the bound on b becomes more relaxed for higher-level errors (eventually approaching $b \geq 17$).

Finally, we have a lower bound on the accuracy threshold of our local error correction scheme. From equation (5.3) and our choices of Q and U, we can

maintain quantum memory in our system for arbitrarily long times (by increasing the size of the lattice) provided that

$$(p+q) \;<\; \frac{1}{4Q^4U^2} \;=\; \frac{1}{4(16)^4(400)^2} \;=\; 2^{-22}10^{-4} \;\approx\; 2.4\times 10^{-11}\,. \qquad (5.9)$$

If we instead use $U = 1024$, the threshold becomes $2^{-38} \approx 3.6 \times 10^{-12}$.

While it may be disturbing to derive such an impractically small number, this is not unusual in these types of proofs, at least in an initial version focusing on existence above other considerations and always assuming the worst case. The proof of stability of Toom's medium for reliable computation in [34] gave a threshold lower bound of 10^{-28} (and only then at the request of a referee), which was next improved by [15] to 10^{-7}, although numerical simulations by Bennett suggested a threshold around 0.05. In Section 5.9 we will also show evidence of a much higher value of the threshold from numerical simulations of our model.

5.8.3 Classical errors

We have assumed that our classical memory and processing is very reliable. In practice, we should be able to allow these components to fail on occasion without damaging our threshold result (provided that the rate and correlations of classical errors satisfy some bound). The `Address` and `Age` fields can easily be maintained by Toom's rule, because their information can be checked for consistency between neighboring cells. Even if a classical processor executes the wrong rules from time to time, this is usually no worse than introducing a single qubit error (bit flip or phase flip), which would get corrected within two time steps if isolated from other errors. A mistake in one of the `CountSignal` fields would also have the same effect as a single qubit error around the center of the originating colony. Since we expect that classical errors would happen much less frequently than quantum errors in our system, most of the effects of classical errors would just be a slight increase in p and q.

However, there is one area of the classical processing that could be especially

fragile to classical errors. Namely, the center of each colony (and super-colony, and so forth) needs to be able to reliably store and process the counts of its syndrome history and its neighbors' syndrome histories during each work period. If a center cell's memory gets scrambled just prior to the end of the work period, it could conceivably send out the wrong flip signal and introduce a large error into the system. Furthermore, the `FlipSignal` field needs to be reliably communicated from one colony to another. These issues are really within the realm of reliable classical computation and communication, and we are confident that there should be ways to build in redundancy using the memory contents of neighboring cells that would implement fault-tolerant schemes for carrying out the correction of higher-level errors.

5.9 Numerical results

We ran Monte Carlo simulations of our model for various choices of Q, U, and lattice size L. Phase flip errors were generated with probability p and syndrome measurement errors with probability q on the lattice during each time step, and the local update rules were simulated at each site. We computed a fidelity measure by calculating the fraction of rows and columns of the lattice which would give a proper expectation value, despite the presence of phase flip errors. Once this fidelity dropped to one half or below, we would assume that one of the encoded qubits has been damaged. We found that for small values of p and q, the distribution of the lengths of time passing before damage occurs looks just like the distribution of times for radioactive decay, so we termed the mean number of time steps to be the "decay time" of the lattice. (For noisy lattices above the threshold, the distribution is noticeably different.)

The best results (in terms of high decay times for a given error rate) came from small colony sizes, especially for $Q = 3$. We ran extensive simulations for $Q = 3$ and $U = 48$ (which was determined by trial to be near optimal). Figure 5.3

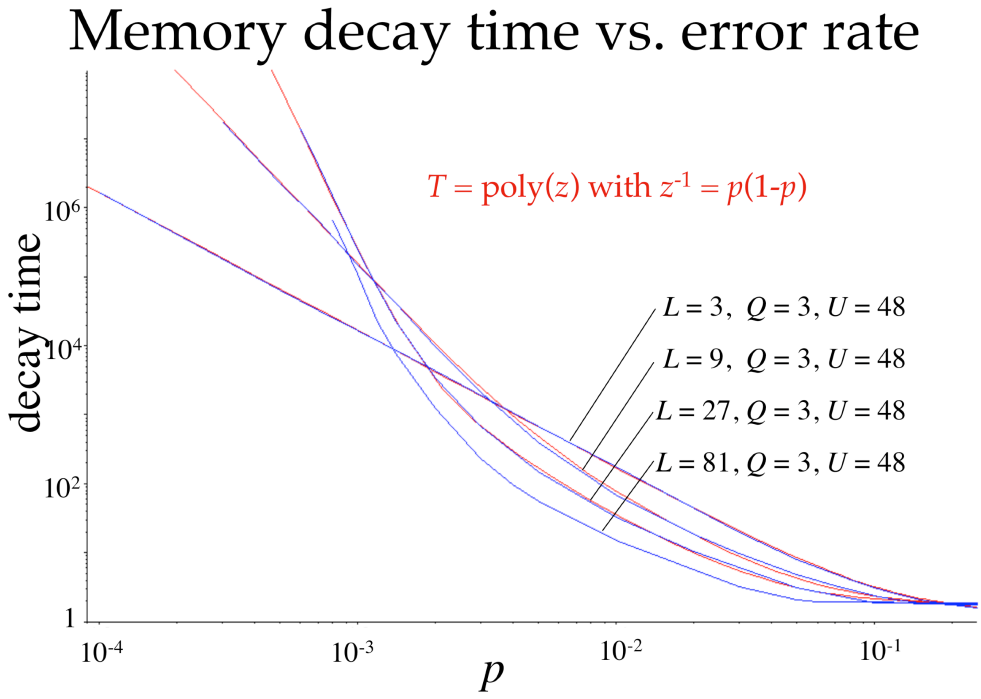

Figure 5.3: The mean decay time of quantum memory versus phase flip (or bit flip) error probability per time step. The four curves in blue plot the average decay times (sampled by Monte Carlo simulations) for lattices of linear size $L = 3$, 9, 27, and 81, as indicated, over a range of phase flip (or bit flip) error rates. The decay time is measured by observing how many time steps pass until the fidelity of an encoded quantum state is degraded to the point that at least half of the rows or columns of the lattice have the wrong expectation value. The curves in red are polynomial fits (by hand) of the variable $z = (p(1-p))^{-1}$. These polynomials are of degree 2, 4, and 8 for $L = 3$, 9, and 27, respectively.

displays our numerical simulations of lattices with linear size $L = 3$, 9, 27, and 81 over a range of error probabilities p, with perfect measurements ($q = 0$).

Although not shown, it is worth remarking that the plots do not appear to change much if we allow small measurement errors, such as $q < p^2$. Also, we observe qualitatively the same behavior of the decay times as a function of q for the cases $p = 0$ and $p = q$.

We have only been able to analytically show the existence of an accuracy threshold for local control of quantum memory in our model with very large lattice sizes and $Q \geq 16$. However, our numerical results support the suggestion that small colony sizes (such as $Q = 3$) also exhibit an accuracy threshold, and that errors on the order of 10^{-4} or even 10^{-3} can be tolerated. The asymptotic slopes of the curves for $L = 3$, 9, and 27 can be measured to show that the decay time grows as $T \propto p^{-2}$, $T \propto p^{-4}$, and $T \propto p^{-8}$, respectively. This is very encouraging because it supports a double exponential growth in memory storage time as a function of the number of levels implemented in the lattice. It took too much running time to sufficiently test $L = 81$ at low values of p, but the plot appears to be consistent with $T \propto p^{-16}$ around the purported threshold. More generally, we expect based on these numerical results that the decay time of quantum memory goes as $T \propto p^{-2^k}$ for p below threshold when k levels of the hierarchy are implemented. If true, then the required spatial resources scale as $O((\log T)^2)$ physical qubits and classical processors with $O((\log \log T)^2)$ memory per processor. The amount of processing required per time step, however, is independent of the lattice size or desired memory storage time.

5.10 Conclusion

We make the following observation about designing systems to protect classical or quantum information. In either a two-dimensional lattice of classical bits or a four-dimensional toric code protecting quantum bits, there exists a local rule (*e.g.*,

Toom's rule) that removes error clusters in a robust manner, because the errors are two-dimensional surfaces with one-dimensional boundaries. These boundaries can be eaten away in a preferred direction, so that the size of error clusters will shrink over time. Provided that the underlying error rate is low enough and that errors are mostly uncorrelated in space and time, then errors of arbitrary size will get removed on average before new errors of comparable size are generated. An accuracy threshold thus exists for local error correction in these systems [82, 2].

There is a further analogy between classical and quantum systems. In a one-dimensional array of bits, or a two-dimensional toric code of qubits, a cluster of errors forms a one-dimensional string, with zero-dimensional (point) boundaries. In these cases, Gács [33] and this present work show that there exists a local rule with an accuracy threshold for error correction, although the procedures and proofs are much more complex than as needed for Toom's rule. Protecting classical information in n dimension by purely local controls appears to be comparable (in terms of the scaling of resources) to protecting information in $2n$ dimensions.

But do we really need a minimum of two dimensions to robustly store quantum information? Gottesman [37] and Aharonov and Ben-Or [1] argue that there should exist a one-dimensional stabilizer or polynomial code requiring only local operations (acting in parallel) and perhaps global (classical) processing of error syndromes that would possess an accuracy threshold, but no explicit construction has been given. We have also experimented to some extent with quantum convolutional codes, as described in [69, 70], but they appear to lack a means for correcting arbitrarily large errors. It still remains open whether a one-dimensional array of qubits could have an accuracy threshold under some error-correcting scheme that is local in both quantum and classical processing, although it seems unlikely.

Now that purely local control of quantum information has been demonstrated in two dimensional structures, there remains great room for improving on the value of the accuracy threshold. Our lower bound is based on some pessimistic assumptions in deriving equation (5.3), and by no means has our protocol been completely optimized. Our model could also be improved in handling faults in the classical

memory and processing. Additionally, future work could relate our qubit and measurement error probabilities p and q to gate errors and ancilla preparation errors (which are perhaps more directly connected to an experimental implementation).

Kuperberg [50] has suggested that there may be a sequence of local error-correcting schemes of toric codes with progressively larger neighborhoods whose accuracy thresholds would transition from those reported in this work up to a few percent, as achieved by the global error syndrome processing scheme described in Section 4.5. It would be interesting to determine what would be good choices for local rules with larger neighborhoods that could quickly correct a larger set of level-0 errors.

Appendix A

Translation of Bavard's "Hyperbolic families of symplectic lattices" [8]

A.1 Introduction

A *symplectic lattice* in a complex Hermetian postive definite vector space $(\mathcal{V}, H)$ is a lattice Λ of $\mathcal{V}$ which admits a symplectic basis for $\operatorname{Im} H$. For example, the period lattice of a manifold of genus ≥ 1 is a symplectic lattice for the Riemann form. The symplectic lattices Λ in complex dimension $g \geq 1$ correspond to *principally polarized abelian varieties* $\mathcal{V}/\Lambda$ and are thus parameters for Siegel's space $\mathfrak{H}_g$.

The study of Hermite's constant μ of symplectic lattices (defined by $\mu(\Lambda) = \inf H(\lambda, \lambda)$ for $\lambda \in \Lambda \backslash \{0\}$) was approached in [B-S] and followed in [B-M1] and [Bv]. The maximal value of μ on $\mathfrak{H}_g$, which is the analog of the classical Hermite's constant, is not known except for $g = 1$, 2 or 4 for the usual theory. One is interested in the lattices which realize a local maximum of μ on $\mathfrak{H}_g$, or *extremal* lattices in the symplectic sense. These lattices are characterized in [B-M1]; however, the known examples of such lattices are very few and, with a lone exception (J_W, see below), are already extremal in the usual sense (D_4, E_8, Leech's lattice Λ_{24}, ...).

We study here the symplectic lattice families that present a two-fold interest. Firstly, they provide new examples of extremal symplectic lattices which gener-

ally are not extremal in the usual sense. The extremal symplectic lattices are a particular case of *perfect symplectic* lattices (see Section A.2.4). We obtain many examples of perfect symplectic lattices (300 with $g \leq 6$) among which we find certain traditional lattices: D_4, E_8, K_{12}, Λ_{16}, Λ_{24}; we also describe several extensions of extremal symplectic lattices. In small dimensions, we find in particular a new extremal point of $\mathfrak{H}_3$ and five new perfect points of $\mathfrak{H}_4$ of which three are extremal. Secondly, these families permit the testing of the general counting proposed in [Bv]. We establish for each one of them a complete theory analogous to classical lattice theory: Voronoï's theorem (Proposition A.2.3), Voronoï's algorithm (Proposition A.2.10), Morse's theory (Proposition A.2.13). These *hyperbolic families* are defined as follows. Let $\mathbb{H}$ be the Poincaré half plane and let M be a symmetric real positive definite $g \times g$ matrix. We define

$$\mathbb{H}M = \{zM; z \in \mathbb{H}\} \subset \mathfrak{H}_g. \qquad (*)$$

The family $\mathbb{H}M$ is a completely geodesic subvariety of Siegel's space $\mathfrak{H}_g$, isometric (up to a factor) to $\mathbb{H}$ provided by the Poincaré metric (Section A.2.1), which justifies the adjective "hyperbolic."

Hermite's constant defines by restriction on $\mathbb{H}M$ two dual geodesic tilings of the hyperbolic plane (Figure A.3), of the types Dirichlet-Voronoï ($\mathcal{DV}^M$) and Delaunay ($\mathcal{D}el^M$), and there is a supplementary dictionary between these tilings and the relative properties with $\mathbb{H}M$ of corresponding lattices (for example, perfection and relative eutaxy: see Theorem A.2.1). The vertices of $\mathcal{DV}^M$ are the perfect points of the family, while the vertices of $\mathcal{D}el^M$, called *principal points*, are naturally bound to a geometric interpretation of length functions (Proposition A.2.2). On this point the theory of hyperbolic families presents two new phenomena compared to the case of classical lattices. Firstly, certain principal points belong here to the parameter space $\mathbb{H}$ whereas for the lattices they are all situated at infinity (see [Bv, section 1.3]). Secondly, we present the notion of *principal length functions*: they are the length functions necessary for describing the situation and, contrary

to the lattice case, they do not coincide with the functions that realize Hermite's constant (see section A.2.5).

The search for examples is guided by the following idea: if the matrix M is rather "interesting" (for example, if M and its inverse have many minimal vectors), the family (*) has some chance of containing marked points. One will find in Section A.3.6 a remarkable family which alone contains 16 (non-isomorphic) perfect symplectic lattices of $\mathfrak{H}_8$. The fact that the space of parameters $\mathbb{H}$ is of small dimension and of a very familiar geometry renders the determination of interesting points of $\mathbb{H}M$ particularly simple to put into practice. In certain cases one can even connect the relative properties with the global properties. Thus when M has a sufficient number of automorphisms, the relative eutaxy with $\mathbb{H}M$ (which tests itself in dimension 2) is equivalent to the ordinary eutaxy (Proposition A.2.6).

When M is rational, the family (*) admits a *complete* symplectic action of a subgroup congruent to $PSL(2,\mathbb{Z})$. We study the behavior of $\mu|\mathbb{H}M$ near the points (Proposition A.2.11) and we establish a definitive result (Corollary A.2.12) like that of two of Euler's formulas (A.2.32), (A.2.36) and a mass formula (A.2.33). A particularly interesting case is $M = A_n$. We give here a more complete description (part 2) which leads to 3 extensions F_{2n}, G_{2n}, J_{2n} and a family $H_{2n}(\varphi)$ ($\varphi \in SL(2,\mathbb{Z})$) of extremal lattices (in the symplectic sense only for F_{2n}, J_{2n} and $H_{2n}(\varphi)$). The group which acts on the situation is $\Gamma_0(n+1)$, and at the same time the number of marked points of the augmented family is the index of $\Gamma_0(n+1)$ in $PSL(2,\mathbb{Z})$.

The complex dimension 3 merits some commentary. The lattice F_6 is a new example of an extremal point in $\mathfrak{H}_3$. Two other extremal points were known previously: the Jacobian J_K of the Klein manifold K (or the lattice $A_6^{(2)}$) which is one of the six extremal lattices of real dimension 6, and the Jacobian J_W of the exceptional Wiman manifold W. The situation therefore appears to be analogous to that of Riemann surfaces of genus 3. In [Sc], P. Schmutz exhibits three local maxima of the systole in genus 3: K, W and a less remarkable surface of which the Jacobian seems to correspond to F_6. In terms of numeric values of μ, we have

$\mu(J_W) = 1 + 1/\sqrt{3} \simeq 1.5773$ and we remark that $\mu(F_6) = 6/\sqrt{15} \simeq 1.5491$ is also larger than $\mu(J_K) = 4/\sqrt{7} \simeq 1.5118$, the value presented in [B-S] as a global maximum of μ on $\mathfrak{H}_3$.

Acknowledgements. I thank Anne-Marie Bergé for her remarks on a first version of this article that was presented at the Luminy conference on lattices (September 1996). I also thank Christian Batut for initiating me in the PARI system of calculation and furthermore thank the other authors of PARI for their availability.

A.2 General study of hyperbolic families

Notations. If M is a matrix, we will denote M' as its transpose.

For a square $m \times m$ matrix A and $u \in \mathbb{R}^m$ we define $A[u] = u'Au$.

We denote $S_m(\mathbb{R})$ (resp. $S_m(\mathbb{C})$) as the space of *symmetric* $m \times m$ matrices with real (resp. complex) coefficients, I as the identity matrix, $J = \left(\begin{smallmatrix} 0 & I \\ -I & 0 \end{smallmatrix}\right)$ and $\langle u, v\rangle = u'v$ $(u, v \in \mathbb{R}^m)$ as the usual Euclidean scalar product.

A.2.1 Symplectic lattices and hyperbolic families

The lattices of the usual Euclidean space of dimension m $(m \geq 1)$ will be here parameters, via the Gram matrices, for the symmetric space P_m of real positive $m \times m$ matrices with determinant 1. One has a correspondance between the matrices $A = PP'$ of P_m $(P \in SL(m, \mathbb{R}))$ and the marked lattices (*i.e.,* provided with a basis) $\Lambda = P'\mathbb{Z}^m$ considered except for direct isometry. *Length functions* are defined on P_m by

$$l_u(A) = A[u] \quad (A \in P_m, u \in \mathbb{R}_m). \tag{A.2.1}$$

Hermite's constant $\mu(A)$, or norm of Λ, is the minimum of $l_u(A)$ for nonzero vectors u. The special linear group $SL(m,\mathbb{R})$ acts isometrically on P_m by

$$P.A = PAP' \quad (A \in P_m, P \in SL(m,\mathbb{R})), \tag{A.2.2}$$

and therefore acts to the right on the length functions.

Consider a symplectic lattice Λ in a complex Hermetian postive definite vector space $(\mathcal{V}, H)$ of dimension g, *i.e.,* Λ admits a symplectic basis for $\operatorname{Im} H$. We can also call $\mathcal{V}/\Lambda$ a *principally polarized abelian variety* for H. There are several ways to describe these objects. If one connects $(\mathcal{V}, H)$ to the usual Hermitian space $(\mathbb{C}_g, H_0)$ $(H_0(u,v) = \overline{u}'v,\ u,v \in \mathbb{C}_g)$, the marked symplectic lattices for a symplectic basis are written $\Lambda = P'\mathbb{Z}^m$ with $P \in Sp(2g,\mathbb{R})$ and thus correspond with the symplectic Gram matrices $(A = PP')$. In addition they are also parameterized for Siegel's space $\mathfrak{H}_g = \{X + iY; X, Y \in S_g(\mathbb{R}), Y > 0\}$. Indeed we can always suppose that $\mathcal{V} = \mathbb{C}_g$, $\Lambda = \mathbb{Z}_g \oplus \tau\mathbb{Z}_g$ with τ in $\mathfrak{H}_g$ and $H(u,v) = \overline{u}'(\operatorname{Im}\tau)^{-1}v$ for $u, v \in \mathbb{C}_g$ (see, for example, [Mu, p.72]). To connect the two points of view, it is enough to clarify the Gram matrix $\varphi_g(\tau)$ of Λ in its natural basis, for the scalar product $\operatorname{Re} H$:

$$\varphi_g(\tau) = \begin{pmatrix} Y^{-1} & Y^{-1}X \\ XY^{-1}Y & XY^{-1}X \end{pmatrix} \quad (\tau = X + iY \in \mathfrak{H}_g). \tag{A.2.3}$$

Recall that $\mathfrak{H}_g$ is a symmetric space for the Riemann metric

$$ds^2 = \operatorname{Tr}(Y^{-1}dXY^{-1}dX + Y^{-1}dYY^{-1}dY) \quad (X + iY \in \mathfrak{H}_g). \tag{A.2.4}$$

The formula (A.2.3) defines an isometric embedding (up to a factor) of $\mathfrak{H}_g$ on the ensemble of symplectic Gram matrices, that we will denote as $\mathfrak{S}_g$ ($\mathfrak{S}_g = Sp(2g,\mathbb{R}).I = P_{2g} \cap Sp(2g,\mathbb{R})$), and which is a completely geodesic subvariety of P_{2g}. The length functions l_u of the marked symplectic lattices, like their gradients ∇_u, are useful for the notions of perfection and of eutaxy and are expressed in

Siegel's space by the following formulas (see [Bv]):

$$\begin{cases} l_u(\tau) = Y^{-1}[a + Xb] + Y[b] \\ \nabla_u(\tau) = -i(a + \tau b)(a + \tau b)' \end{cases} \quad (\tau = X + iY \in \mathfrak{H}_g,\ u = \begin{pmatrix} a \\ b \end{pmatrix} \in \mathbb{R}^{2g}). \quad \text{(A.2.5)}$$

With each element M of P_g we associate a *hyperbolic family* parameterized by the Poincaré half plane $\mathbb{H}$:

$$\mathbb{H}M = \{zM; z \in \mathbb{H}\}. \quad \text{(A.2.6)}$$

The intersection W of hyperbolic families is a subvariety of $\mathfrak{H}_g$ with dimension $g(g+1)/2+1$. The metric induced on W at the point zM is written as

$$g\left(|dz|/\operatorname{Im} z\right)^2 + \left(|z|/\operatorname{Im} z\right)^2 \operatorname{Tr}\left(M^{-1}dM\right)^2, \quad \text{(A.2.7)}$$

so that the two natural coverings carried by W (defined by the product structure $\mathbb{H} \times P_g$) are orthogonal. The hyperbolic families are all isometric with the same homothetic of $\mathbb{H}$, and they are *completely geodesic*. Recall that if $\mathcal{Q}$ is a Lie subgroup related to $SL(n, \mathbb{R})$, stable under transposition, then $\mathcal{Q}.I$ is completely geodesic in P_n (see [Eb, p.131]). However, $\varphi_g(\mathbb{H}I)$ is of the form $\mathcal{Q}.I$ with

$$\mathcal{Q} = \left\{ \begin{pmatrix} \delta I & \gamma I \\ \beta I & \alpha I \end{pmatrix}; \alpha, \beta, \gamma, \delta \in \mathbb{R},\ \alpha\delta - \beta\gamma = 1 \right\}. \quad \text{(A.2.8)}$$

When $M = PP'$ is unspecified, we see that $\mathbb{H}M = \left(\begin{smallmatrix} P & 0 \\ 0 & P'^{-1} \end{smallmatrix}\right).\mathbb{H}I$ is an isometric image of $\mathbb{H}I$. In the orthogonal covering, $zP_g = \{zM; M \in P_g\}$ is completely geodesic for $\operatorname{Re} z = 0$ (by a similar argument) and only in this case.

Remark A.2.1. (1) In the following we will study the families $\mathbb{H}M$ where M has an unspecified positive determinant. We can restrict ourselves to the case of determinant 1 by way of an isometry in the parameter space $\mathbb{H}$.

(2) There exist other interesting "hyperbolic families." For example,

$$\tau_z = z\begin{pmatrix}1&0&1\\0&0&0\\1&0&1\end{pmatrix} + \begin{pmatrix}1/2+i/4 & -1/2 & -i/4\\ -1/2 & 1/2+i/2 & 1/2\\ -i/4 & 1/2 & 1/2+i/4\end{pmatrix} \quad (z\in\mathbb{H}) \qquad \text{(A.2.9)}$$

defines a completely geodesic hyperbolic plane in $\mathfrak{H}_3$ which contains the Jacobian J_W of the exceptional Wiman manifold mentioned in the introduction (with $z = -1/2 + i\sqrt{3}/4$, see [Bv, Section 3.5]). This family comes, via the whole homology of dimension 1, from a topological action on the closed surface of genus 3 (as with $\mathbb{H}A_3$). It is not symplectically equivalent (under the action (A.2.10)) to any family of the form (*).

A.2.2 Symplectic actions on the families

Let us recall the isometric action "by homographies" of the symplectic group $Sp(2g,\mathbb{R})$ on $\mathfrak{H}_g$: for $\left(\begin{smallmatrix}A&B\\C&D\end{smallmatrix}\right) \in Sp(2g,\mathbb{R})$, *i.e.,* $A'C = C'A$, $B'D = D'B$ and $A'D - C'B = I$, one defines

$$\begin{pmatrix}A&B\\C&D\end{pmatrix}.\tau = (A\tau+B)\,(C\tau+D)^{-1} \qquad (\tau\in\mathfrak{H}_g). \qquad \text{(A.2.10)}$$

The embedding (A.2.3) satisfies a property of invariance for the natural actions. Let θ be an automorphism of $Sp(2g,\mathbb{R})$ defined by $\theta\left(\begin{smallmatrix}A&B\\C&D\end{smallmatrix}\right) = \left(\begin{smallmatrix}D&C\\B&A\end{smallmatrix}\right)$. One can then check the following relation:

$$\varphi_g(\Phi.\tau) = \theta(\Phi).\varphi_g(\tau) \qquad \Phi\in Sp(2g,\mathbb{R}), \tau\in\mathfrak{H}_g. \qquad \text{(A.2.11)}$$

As a result, we have a formula for transforming lengths:

$$l_{a,b}(\tau) = l_{Aa-Bb,-Ca+Db}(\Phi.\tau) \qquad (\tau\in\mathfrak{H}_g), \qquad \text{(A.2.12)}$$

with $l_u = l_{a,b}$ for $u = \left(\begin{smallmatrix}a\\b\end{smallmatrix}\right) \in \mathbb{R}^{2g}$ and $\Phi = \left(\begin{smallmatrix}A&B\\C&D\end{smallmatrix}\right) \in Sp(2g,\mathbb{R})$.

We will call the *group of automorphisms of the family* $\mathbb{H}M$ the subgroup of $Sp(2g,\mathbb{Z})$ which fixes $\mathbb{H}M$ point by point, denoted $Aut(\mathbb{H}M)$.

Proposition A.2.1. *(1) The group of automorphisms of* $\mathbb{H}M$ *is isomorphic to the group of automorphisms of* M*.*

(2) The family $\mathbb{H}M$ *is symplectically equivalent to the family* $\mathbb{H}M^{-1}$*.*

Proof. (1) One can quickly verify that all automorphisms of $\mathbb{H}M$ are of the form $\left(\begin{smallmatrix} P & 0 \\ 0 & P'^{-1} \end{smallmatrix}\right)$ with $P \in GL(g,\mathbb{Z})$ and $PMP' = M$, *i.e.,* $P \in Aut(M)$; the isomorphisms are then evident.

(2) The families $\mathbb{H}M$ and $\mathbb{H}M^{-1}$ are exchanged by a complete symplectic transformation:

$$\begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix} .zM = -\frac{1}{z}M^{-1}. \tag{A.2.13}$$

In addition, each family $\mathbb{H}M$ admits a symplectic action of $PSL(2,\mathbb{R})$:

$$\begin{pmatrix} \alpha I & \beta M \\ \gamma M^{-1} & \delta I \end{pmatrix} .zM = \frac{\alpha z+\beta}{\gamma z+\delta}M \quad (\alpha,\beta,\gamma,\delta \in \mathbb{R}, \alpha\delta-\beta\gamma = 1), \tag{A.2.14}$$

which induces the usual action of $PSL(2,\mathbb{R})$ on the plane of parameters $\mathbb{H}$. When M is rational, we thus have a *complete* symplectic action of a subgroup of finite index $\Gamma \subset PSL(2,\mathbb{Z})$ and we can restrict our study to a fundamental domain of Γ in $\mathbb{H}$. Let $m \in \mathbb{N}^*$ such that mM and mM^{-1} are complete: one takes $\Gamma = \Gamma(m)$ to be the subgroup of principal congruence ($\Gamma = PSL(2,\mathbb{Z})$ if M has determinant 1). But one can often choose Γ to contain $\Gamma(m)$: for example, $\mathbb{H}A_n$ (resp. $\mathbb{H}D_n$) admits a complete symplectic action of the group $\Gamma_0(n+1)$ (resp. $\Gamma_0(4)$) with

$$\Gamma_0(m) = \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in PSL(2,\mathbb{Z}); \gamma \equiv 0(m) \right\}. \tag{A.2.15}$$

The fixed points of Γ are in general interesting because they have more automorphisms than a "generic" point of the family (examples: $\frac{1+i}{2}D_{2n}$, $\frac{1+i}{2}D_4 \simeq \frac{2+i}{5}A_4 \simeq E_8$, $\frac{5+i\sqrt{3}}{14}A_6 \simeq K_{12}$, $\frac{5+i}{13}A_{12}^{(2)} \simeq \Lambda_{24}$, ...).

There is a also a symmetry coming from the anti-symplectic action of $\Phi_0 = \left(\begin{smallmatrix} -I & 0 \\ 0 & I \end{smallmatrix}\right)$ on P_{2g} which fixes $\mathfrak{S}_g$. In $\mathfrak{H}_g$, the action is written $\Phi_0.\tau = -\overline{\tau}$ ($\tau \in \mathfrak{H}_g$); it fixes each hyperbolic family and respects the length function gradients: $\nabla_u(\Phi_0.\tau) = \Phi_0(\nabla_{\Phi_0' u}(\tau))$ ($\tau \in \mathfrak{H}_g$, $u \in \mathbb{R}^{2g}$). *The forms $\varphi_g(\tau)$ and $\varphi_g(-\overline{\tau})$ ($GL(2g,\mathbb{Z})$ equivalent) therefore have the same symplectic nature.* □

Remark A.2.2. If $P \in GL(g,\mathbb{Z})$, the families $\mathbb{H}M$ and $\mathbb{H}(PMP')$ are exchanged by a complete symplectic transformation which induces the identity on $\mathbb{H}$. The symplectic nature of zM therefore does not depend upon the specific lattice used to define M.

A.2.3 Geometric study of lengths

With the postive definite matrix M being fixed, we study the length functions and Hermite's constant restricted to the family $\mathbb{H}M$, such as functions on the parameter space $\mathbb{H}$. We therefore define

$$\mu^M(z) = \mu(zM) \quad (z \in \mathbb{H}), \tag{A.2.16}$$

and $l_u^M(z) = l_u(zM)$ with $u = \left(\begin{smallmatrix} a \\ b \end{smallmatrix}\right)$ a nonzero vector of $\mathbb{R}^{2g}$. We also define

$$\Delta_u^M = M^{-1}[a]M[b] - \langle a,b\rangle^2 \text{ and } z_u^M = \frac{-\langle a,b\rangle + i\sqrt{\Delta_u^M}}{M[b]} \tag{A.2.17}$$

(with $z_u^M = \infty$ if $M[b] = 0$). We observe that $\Delta_u^M \geq 0$ from (A.3.3). The point z_u^M is in $\mathbb{H}$ if $\Delta_u^M > 0$ and in $\mathbb{R} \cup \{\infty\} = \partial\mathbb{H}$ (the boundary of $\mathbb{H}$) if $\Delta_u^M = 0$. It is the point of $\mathbb{H} \cup \partial\mathbb{H}$ which zeroes the gradient of l_u^M (see (A.2.21)).

One notes that d is the hyperbolic distance in $\mathbb{H}$ and h_p is the Busemann function associated with a point at infinity $p \in \partial\mathbb{H}$, normalized for $h_p(i) = 0$.

Proposition A.2.2. *The length function l_u^M is expressed geometrically by*

$$\begin{cases} l_u^M = 2\sqrt{\Delta_u^M}\cosh(d(.,z_u^M)) & \text{if } z_u^M \in \mathbb{H}, \\ l_u^M = (M^{-1}[a] + M[b])\exp(h_{z_u^M}) & \text{if } z_u^M \in \partial\mathbb{H} \end{cases} \quad (z \in \mathbb{H}).$$

Consequently, if $z_u^M \in \mathbb{H}$ (resp. $z_u^M \in \partial\mathbb{H}$), the level curves of l_u^M are hyperbolic circles (resp. horocycles) centered at z_u^M, and their gradient lines are, for close parameters, the half-geodesic (resp. geodesic) exits of z_u^M.

Proof. Recall that $l_u^M(z) = (M^{-1}[a] + 2x\langle a, b\rangle + |z|^2 M[b])y^{-1}$ for $z = x + iy \in \mathbb{H}$. Hyperbolic distance is given by

$$\cosh(d(z,w)) = \frac{|z-\overline{w}|^2 + |z-w|^2}{|z-\overline{w}|^2 - |z-w|^2} \quad (z, w \in \mathbb{H}), \tag{A.2.18}$$

Also, recall the expression of Busemann functions:

$$h_p(z) = \log \frac{|z-p|^2}{\operatorname{Im} z(1+p^2)} \quad h_\infty(z) = \log \frac{1}{\operatorname{Im} z} \quad (p \in \mathbb{R}, z \in \mathbb{H}). \tag{A.2.19}$$

The verification of the formulas is then elementary. □

Proposition A.2.2 also shows that the length functions are *strictly convex* on the hyperbolic families. The condition (C) is therefore verified (see [Bv, 2.2 Example 2]) and one has the relative Voronoï's theorem.

Proposition A.2.3. *A point zM is extremal in the family $\mathbb{H}M$ if and only if it is relatively perfect and relatively eutactic.*

We note also that the extremal points in $\mathbb{H}M$ are isolated in $\mathbb{H}M$ ([Bv, Proposition 2.4]). Here is another consequence of Proposition A.2.2: if γ is a geodesic of $\mathbb{H}$, the function $l_u^M \circ \gamma$ is *proper* ($\lim_{|t|\to\infty} l_u^M \circ \gamma(t) = \infty$) except if z_u^M is one of the points at infinity on γ.

Proposition A.2.4. *Let u and v be two nonzero vectors of $\mathbb{R}^{2g}$ and let k be a positive real number. Then the ensemble of points z of $\mathbb{H}$ such that $l_u^M(z) = k l_v^M(z)$, if it is nonempty, is a geodesic which crosses orthogonally the geodesic joining the points z_u^M and z_v^M (assumed to be distinct).*

Proof. One works with the model of the hyperboloid and the associated projective model. The space $S_2(\mathbb{R})$ of real symmetric 2×2 matrices is provided by

the quadratic form $q(A) = -\det(A)$ of signature (2,1). The hyperbolic plane corresponds to the projection of the negative cone of q (cone of defined matrices): the matrix $A = \left(\begin{smallmatrix} U & V \\ V & W \end{smallmatrix}\right)$ with $\det(A) > 0$ is associated with the point $U^{-1}(V + i[\det(A)]^{1/2})$ of $\mathbb{H}$; this identification is consistent with (A.2.3). The length functions are defined by linear forms on $S_2(\mathbb{R})$:

$$l_u^M(A) = -2\mathcal{B}(A, Z_u^M) \quad \text{with} \quad Z_u^M = \begin{pmatrix} M[b] & -\langle a, b\rangle \\ -\langle a, b\rangle & M^{-1}[a] \end{pmatrix}, \tag{A.2.20}$$

where $\mathcal{B}$ indicates the polar bilinear form of q and $u = \left(\begin{smallmatrix} a \\ b \end{smallmatrix}\right) \in \mathbb{R}^{2g}$. The matrix Z_u^M is associated with the point z_u^M defined by (A.2.17). Suppose that Z_u^M is not colinear with Z_v^M. The equation $l_u^M(A) = kl_v^M(A)$ therefore defines a projective line D_k, and when k varies all these projections pass by the polar point (compared to q) of the projective line $Z_u^M Z_v^M$, and this point is in the projection of the positive cone of q. Depending on whether or not D_k crosses the projection of the negative cone of q, the sought ensemble of $z \in \mathbb{H}$ is a geodesic orthogonal to the geodesic joining z_u^M and z_v^M, or it is empty.

We could also write the equations in $\mathbb{H}$: the ensemble of z satisfying $l_u^M(z) = kl_v^M(z)$ is a geodesic (if it is nonempty), and orthogonality with the geodesic $z_u^M z_v^M$ is verified by an elementary calculation. □

A.2.4 Relative eutaxy

Let us briefly recall the general definitions of perfection and eutaxy, which are equivalent to the usual definitions in the classical case (see [Bv, Section 2.1]). Let V be a Riemann variety provided by a system of length functions $(f_s)_{s\in C}$ with action on a discrete group Π of isometries of V. For all $x \in V$, we denote S_x as the ensemble (assumed to be finite) of elements of C of minimal length in x. A point $x \in V$ is *eutactic* (resp. *semi-eutactic*, resp. *weakly eutactic*) if the gradients $X_s(x) = \nabla f_s(x)$ $(s \in S_x)$ satisfy the relation $\sum_{s\in S_x} \lambda_s X_s(x) = 0$ with coefficients λ_s strictly positive (resp. nonnegative and summing to one, resp. summing to one).

We say that $x \in V$ is *perfect* if $X_s(x)$ ($s \in S_x$) affinely generates the tangent space T_xV. For example, we can take $V = P_n$, $C = \mathbb{Z}_n$, $\Pi = SL(2, \mathbb{Z})$ for the lattices and $V = \mathfrak{H}_g$, $C = \mathbb{Z}^{2g}$, $\Pi = Sp(2g, \mathbb{Z})$ for the symplectic lattices (with the usual lengths).

By projecting the gradients orthogonally, these notions can be extended to relative ones of a vector subspace T_xV. For a subvariety W, relative perfection and eutaxy of T_xW coincide with the notions of perfection and eutaxy defined in W with the induced length functions.

The stabilizer of a point $x \in V$ by the action of Γ is called the *group of automorphisms* of x and denoted as $Aut(x)$. When $Aut(x)$ is rather rich, one can reduce the verification of global eutaxy to verification of eutaxy in a subspace of smaller dimension according to the following remark.

Proposition A.2.5. *Let G be a subgroup of $Aut(x)$ and let $(T_xV)^G$ be the subspace of fixed points of G in T_xV ($x \in V$). Let F be a vector subspace of T_xV which contains $(T_xV)^G$. Then x is eutactic (resp. semi-eutactic, resp. weakly eutactic) in V if and only if x is eutactic (resp. semi-eutactic, resp. weakly eutactic) relative to F.*

Proof. We must verify that eutaxy in F involves global eutaxy (the inverse being evident by projection), and we can assume that $F = (T_xV)^G$. Let p_F be the orthogonal projection on F. We observe that the ensemble $(X_s)_{s \in S_x}$ of gradients in x is stabilized by G and that $p_F(X)$ is the average of $g.X$ for $g \in G$ ($x \in T_xV$). Consequently, every relation of eutaxy (resp. semi-eutaxy, resp. weak eutaxy) binding the $p_F(X_s)$ implies an analagous relation between the X_s. □

Let us return to the study of hyperbolic families.

Proposition A.2.6. *Let $M \in P_g$ be such that the action of $Aut(M)$ on $\mathbb{R}_g$ is irreducible. Then for all $z \in \mathbb{H}$:*
(1) zM is eutactic in $\mathfrak{H}_g$ if and only if zM is eutactic in $\mathbb{H}M$. Suppose also that $Aut(M)$ contains an element of determinant -1 (which is always the case if g is

odd). Then:

(2) $\varphi_g(zM)$ is eutactic in P_{2g} if and only if zM is eutactic in $\mathbb{H}M$,

(3) the relative weakly eutactic points (for example, perfect) in $\mathbb{H}M$ are insulated in P_{2g}.

The statements (1) and (2) hold true when replacing eutactic with semi-eutactic or weakly eutactic.

Lemma A.2.7. *Let H be a subgroup of $GL(n,\mathbb{R})$ for which the action on $\mathbb{R}^n$ is irreducible, and let $M \in P_n$ be fixed under H (i.e., $PMP' = M$ for all $P \in H$). Then every symmetric matrix fixed under H is a multiple of M; in particular, M is the unique point in P_n fixed under H. Furthermore, if n is even, H contains an element with negative determinant. Then every matrix fixed under H is a multiple of M.*

Proof of the proposition. The assertion (3) can be derived from (2) and the theorem of finitude of weakly eutactic lattices ([B-M2, Theorem 3-5]). It remains then to prove (1) and (2). The group $G = \theta(Aut\mathbb{H}M)$ (elements of the lattice $\left(\begin{smallmatrix} P'^{-1} & 0 \\ 0 & P \end{smallmatrix}\right)$ with $P \in Aut(M)$) fixes $A = \varphi_g(zM)$ and $T_A\mathfrak{S}_g$ (G is included in $Sp(2g,\mathbb{R})$). As in the first part of the lemma, the vector space fixed in $T_A\mathfrak{S}_g$ corresponds via φ_g to the complex line generated for M, *i.e.,* precisely to the tangent space of the family $\mathbb{H}M$ at the point zM. Then assertion (1) results by way of Proposition A.2.5.

Now let $X = \left(\begin{smallmatrix} U & V \\ V' & W \end{smallmatrix}\right) \in T_AP_{2g}$ (where U and W are symmetric) be fixed under G. We then have $P'^{-1}UP^{-1} = U$ (from where $PMUMP' = MUM$), $PV'P^{-1} = V'$ (from where $PMVP' = MV$) and $PWP' = W$ for all $P \in Aut(M)$. Applying the lemma leads to $U = \alpha M^{-1}$, $W = \beta M$ and (knowing that if g is even, $Aut(M)$ is not included in $SL(g,\mathbb{Z})$) $V = \lambda I$ with $\alpha, \beta, \lambda \in \mathbb{R}$. Moreover, if X is orthogonal to $T_A\mathfrak{S}_g$, *i.e.,* $XJA - AJX = 0$ and $\mathrm{Tr}\,(A^{-1}X) = 0$, it is easy to see that $\alpha = \beta = \lambda = 0$ ($X = 0$), which completes the proof of the proposition (Proposition A.2.6). Note that the set of fixed points under G in P_{2g} is reduced to the hyperbolic family $\varphi_g(\mathbb{H}M)$. □

Proof of the lemma. Let Y be a matrix that is invariant under H. The ensemble $\mathcal{K}$ of matrices commuting with all the elements of H is a field (Schur's lemma); therefore $\mathcal{K}$ is isomorphic to $\mathbb{R}$ or it contains an element which squares to $-I$ (so it has complex structure). This last possibility is excluded if n is odd or if H contains an element with negative determinant. In this case Y is a multiple of M ($YM^{-1} \in \mathcal{K} = \mathbb{R}I$).

Suppose now that H is unspecified but Y is symmetric, and let $M = QQ'(Q \in SL(n, \mathbb{R}))$. Then $Z = Q^{-1}YQ'^{-1}$ is symmetric and commutes with all the elements of $Q^{-1}HQ$. Following the proof of Schur's lemma (and noting that Z admits a proper value), one has $Z = \lambda I$ ($\lambda \in \mathbb{R}$), *i.e.,* $Y = \lambda M$. □

For the M that pass the hypotheses of Proposition A.2.6, one will be able to test global eutaxy in P_{2g} while restricting the family $\mathbb{H}M$ to dimension 2 only. The orthogonal projection on the complex line $\mathbb{C}M$ of the gradient of the length function $l_{a,b}$ is equal to $\frac{1}{g}\mathrm{Tr}\,(M^{-1}\nabla_{a,b}(zM))M$. Consequently the gradient $\nabla^M_{a,b}(z)$ of $l^M_{a,b}$ for the Poincaré metric is given by (see (A.2.7)):

$$i\nabla^M_{a,b}(z) = M^{-1}[a] + 2z\langle a, b\rangle + z^2 M[b]. \tag{A.2.21}$$

A.2.5 Principal length functions. Principal points

We introduce now the notion of a *principal length function*, which will allow us to describe μ^M via a geometric interpretation of Section A.2.3. Contrary to the case of classical lattices, the ensemble of these functions do not coincide in general with the ensemble of functions which realize the minimum μ^M (see the examples and Remark 1.4 below).

The length function $l^M_{a,b}$ depends only on $M^{-1}[a], M[b]$ and $\langle a, b\rangle$, and it often happens that associated length functions of distinct vectors coincide. In the following we consider the *ensemble* $\mathcal{L}^M$ of length functions. Note that the point z^M_u associated with $f = l^M_u \in \mathcal{L}^M$ for (A.2.17) depends only on f and will be denoted z^M_f or simply z_f. It is very easy to compare length functions:

Lemma A.2.8. *(of comparison) Let γ be a geodesic of $\mathbb{H}$ parameterized by arclength, and let $\varphi = l_u^M \circ \gamma$ and $\psi = l_v^M \circ \gamma$.*
(1) If $\varphi(0) = \psi(0)$ and $\varphi'(0) = \psi'(0)$ then $\varphi = \psi$.
(2) If $\varphi(0) = \psi(0)$ and $\varphi'(0) > \psi'(0)$ then $\varphi(t) - \psi(t)$ has the same sign as t.
(3) If φ and ψ are equal at two distinct points of γ, they coincide.
(4) Let $z_1, z_2 \in \mathbb{H}$. If $\mu^M(z_i) = l_u^M(z_i)$ $(i = 1, 2)$, then for all points z pertaining to the geodesic segment $[z_1, z_2]$ one has $\mu^M(z) = l_u^M(z)$.

Proof. One can map $\gamma(t)$ to $\exp(t)i$ for an element of $PSL(2, \mathbb{R})$; thanks to (A.2.12) one sees that

$$l_u^M \circ \gamma(t) = M^{-1}[c] \exp(-t) + M[d] \exp(t) \tag{A.2.22}$$

with suitable $(c, d) \neq (0, 0)$. The assertions (1) and (2) result immediately from (A.2.22), (3) results from (2). Finally (4) shows itself by the absurdity while using (2). □

Definition A.2.1. *A length function l_s^M is known as principal if there exists a point $z \in \mathbb{H}$ for which l_s^M is the unique length function $f \in \mathcal{L}^M$ such that $\mu^M(z) = f(z)$. The point z_s^M associated with l_s^M for (A.2.17) will be called a principal point.*

Remark A.2.3. The concept of principal function makes sense within the general framework of Section A.2.4.

For all $z \in \mathbb{H}$ we will denote $\mathcal{L}_z (= \mathcal{L}_z^M)$ as the ensemble of length functions equal to μ^M at point z, and $K_z (= K_z^M)$ as the convex hull of gradients $\nabla f(z)$ in the tangent space, with $f \in \mathcal{L}_z$. The function μ^M, the convex hulls K_z $(z \in \mathbb{H})$, and the properties of eutaxy are determined by the ensemble $\mathcal{P}^M$ of *principal* length functions.

Proposition A.2.9. *For all $z \in \mathbb{H}$ the extremal points of the convex hull K_z are precisely the gradients $\nabla f(z)$ with $f \in \mathcal{P}^M \cap \mathcal{L}_z$. In particular, $\mathcal{P}^M \cap \mathcal{L}_z$ is nonempty:*

$$\mu^M(z) = \min_{f \in \mathcal{P}^M} f(z), \tag{A.2.23}$$

K_z is the convex hull of "principal gradients" in z, and every eutaxy relation in z is equivalent to a eutaxy relation between the "principal gradients."

Proof. If $X = \nabla f(z)$ ($f \in \mathcal{L}_z$) is an extremal point of K_z, then there exists a tangent vector Y such that $\langle X, Y\rangle < \langle V, Y\rangle$ for all points $V \in K_z$ distinct from X. In the direction of Y, μ^M can only be achieved by the length function f, which is thus principal.

Reciprocally, $f \in \mathcal{P}^M \cap \mathcal{L}_z$. The ensemble C_f of points $w \in \mathbb{H}$ such that $\mu^M(w) = f(w)$ is a convex hull (Lemma 1.8 assertion (4)) with nonempty interior (definition of a principal function). Suppose that $\nabla f(z)$ is not an extramal point of K_z. Let Ω be a small neighborhood of z. By a variatonal argument, one sees that $C_f \cap \Omega$ is resticted to z (resp. to a geodesic segment) if $\nabla f(z)$ is interior to K_z (resp. at an edge of K_z), which is absurd. □

Examples. (1) $M = A_4, z = (2+i)/5$. The lattice zM is isomorphic to E_8. There exist six minimal length functions at the point z corresponding to (A.3.2) with $(M^{-1}[a],\ 2\langle a, b\rangle,\ M[b]) = (0,\ 0,\ 2)$, (2, -8, 8), (6/5, -6, 8), (4/5, -2, 2), (4/5, -4, 6) and (6/5, -4, 4). Their gradients in z, given by (A.2.21), are (up to a factor) $\pm(4-3i)$, $\pm(1+3i)$, $\pm(2+i)$ and Kz is a parallelogram of vertices $\pm(4-3i)$, $\pm(1+3i)$. The gradients $\pm(2+i)$ are located within the interior of K_z and the associated non-principal functions therefore minimize, following the proof of Proposition A.2.9, only one segment of the geodesic (for example, the segment joining $(2+i)/5$ and $(3+i)/5$ for $(6/5, -4, 4)$). Consult Section A.3.5 for an indepth global study of the family $\mathbb{H}A_4$.

(2) $M = A_6$, $z = (5+i\sqrt{3})/14$. The lattice zM is isomorphic to K_{12}. One finds six minimal length functions at the point z given by $(M^{-1}[a],\ 2\langle a, b\rangle,\ M[b]) = (0,\ 0,\ 2)$, (2, -8, 8), (2, -12, 18), (6/7, -4, 6), (10/7, -8, 12), (12/7, -8, 10). The convex hull K_z is an equliateral triangle generated by the first three gradients. The last three (nonprincipal) functions minimize only at the point z because their gradients are inside K_z.

Remark A.2.4. In the case of lattices or of symplectic lattices, the gradients of

minimal length functions l_u at a point are connected to the orthogonal projection matrices on the minimal vectors u. Being all situated on a sphere of the tangent space (see [Bv, Section 1.4 and Section 3.2]), they are the extremal points of the convex hull which they generate. Thus, the length functions which realize the usual or symplectic Hermite's constant are all principal in the sense of the preceding definition.

A.2.6 Dirichlet-Voronoï and Delaunay decompositions (associated with the principal points)

Having the ensemble $\{z_f\}_{f\in\mathcal{P}^M}$ of principal points one associates dual decompositions of the hyperbolic plane. Tort of abord one decomposition in regions *of type Dirichlet-Voronoï*, *i.e.,* one defines

$$C_f = \left\{z \in \mathbb{H}; \mu^M(z) = f(z)\right\} \qquad (f \in \mathcal{P}^M). \tag{A.2.24}$$

Traditionally, the Dirichlet-Voronoï regions are constructed with the distance (see for example, [C-S, ch. 2, Section 1.2] for this notion in the Euclidean context). If A is a discrete ensemble of points of $\mathbb{H}$, the region of a point $a \in A$ is defined with the hyperbolic distance d for $\{z \in \mathbb{H}; d(z, A) = d(z, a)\}$. Ici the situation is analog: the relation $\mu^M(z) = f(z)$ defines C_f for of inequalities between the distances or the functions of Busemann associated with the principal points $(z_g)_{g\in\mathcal{P}^M}$ (see Proposition A.2.2). The $(C_f)_{f\in\mathcal{P}^M}$ are of *convex hyperbolic polygons* (Lemma 1.8 (4), Proposition A.2.4) and form a tiling of the hyperbolic plane that we will denote $\mathcal{DV}^M$. The areas and the vertices of C_f will also be considered as tiling regions of respective dimensions 1 and 0.

One defines the *Delaunay type* decomposition, denoted $\mathcal{D}el^M$, which is dual to $\mathcal{DV}^M$. Given a region C of dimension k of $\mathcal{DV}^M$ $(k = 0, 1, 2)$ the dual region, of dimension $2 - k$, is defined by

$$C^* = \operatorname{conv}\left\{z_f; C \subset C_f\right\}, \tag{A.2.25}$$

where "conv" indicates the convex hull in the hyperbolic plane. The decomposition $\mathcal{D}el^M$ is also a tiling of $\mathbb{H}$ with hyperbolic polygons of which the vertices are the principal points, possibly located at infinity (see Figure A.1).

Let us establish a link between the two preceding tilings and the notions of "minimal classes" and of "rank of perfection." These notions are classic for the lattices (see [Ma]) and can be extended in the following way, with the notations of 1.4. The parameter space V is partitioned into *minimal classes*: two points x and y of V are in the same minimal class if and only if $S_x = S_y$. It is clear that this condition is equivalent to the equality of *ensembles* of length functions $\{f_s; s \in S_x\} = \{f_s; s \in S_y\}$. When a discrete group Π acts on the situation, one has the notion of minimal classes modulo Π. In addition, we will call the *rank of perfection* of a point $x \in V$ to be the dimension of the affine subspace of T_xV generated for the gradients $(X_s(x))_{s\in S(x)}$; when x is weakly eutactic, this dimension is also that of the vector subspace generated for $(X_s(x))_{s\in S(x)}$ (the affine subspace passe for 0).

Here is the dictionary between the tilings $\mathcal{DV}^M$ and $\mathcal{D}el^M$ and the properties of points of $\mathbb{H}$ for μ^M (perfection, eutaxy, ...), *i.e.,* the properties of lattices of $\mathbb{H}M$ relatively with this family. In this statement, the interiors are to be taken *in the cellular sense.*

Theorem A.2.1. *Let $M \in P_g$ and let $\mathcal{DV}^M$ be the Dirichlet-Voronoï tiling associated with the principal points.*

(1) The minimal classes coincide with the interiors of regions of $\mathcal{DV}^M$.

(2) The rank of perfection is constantégal with $2-k$ on the interior of regions of dimension k of $\mathcal{DV}^M$. In particular the perfect points for μ^M are the vertices of $\mathcal{DV}^M$.

(3) Let z be in the interior C° of a region of $\mathcal{DV}^M$. Then z is eutactic for μ^M if and only if $z \in C^\circ \cap (C^*)^\circ$ where C^* is the dual region of C in the tiling $\mathcal{D}el^M$.

(4) All the edges of $\mathcal{DV}^M$ are (geodesics) of finite length, and their union is a locally connected finite graph.

Proof. (1) Let us recall the notation $\mathcal{L}_z = \{f \in \mathcal{L}^M; f(z) = \mu^M(z)\}$. The minimal classes are defined by $\mathcal{L}_z = \mathcal{L}_w$ $(z, w \in \mathbb{H})$ and the open regions of $\mathcal{DV}^M$ for $\mathcal{L}_z \cap \mathcal{P}^M = \mathcal{L}_w \cap \mathcal{P}^M$ ($\mathcal{P}^M$ is the ensemble of principal length functions). One must therefore verify that the ensemble $\mathcal{L}_z$ is the same for all the points of an open region of $\mathcal{DV}^M$. If z is in the interior of C_f $(f \in \mathcal{P}^M)$ one has $\mathcal{L}_z = \{f\}$ from the lemma of comparison. Let $C = C_f \cap C_g$ $(f, g \in \mathcal{P}^M)$ be an edge of $\mathcal{DV}^M$, $z \in C^\circ$ and $h \in \mathcal{L}_z$. Along C° one has $h \geq f = g$ with equality in z; therefore (by the lemma of comparison) h coincides with f and g on C°. Finally for the vertices of $\mathcal{DV}^M$ there is nothing to show.

(2) Following Proposition A.2.9 the convex hull K_z of gradients $\nabla f(z)$ $(f \in \mathcal{L}_z)$ is equal to the convex hull of principal gradients $\nabla f(z)$ $(f \in \mathcal{L}_z \cap \mathcal{P}^M)$ and the latter are all distinct (the opposés point towards distinct principal points). The rank of perfection, *i.e.,* the affine dimension of K_z, is therefore equal to 0, 1 or 2 according to the number (1, 2 or $l \geq 3$) of principal gradients, corresponding to the interior of regions of dimension 2, 1 or 0.

(3) This assertion results simply from the fact that $-\nabla f$ is always directed towards the principal point z_f $(f \in \mathcal{P}^M)$. Note that the eutactic points of rank 0 are the principal points z_f situated in $\mathbb{H}$ with the interior of C_f, and that if z is eutactic of rank 1, the interiors C° and $(C^\star)^\circ$ meet perpendicularly at the point z.

(4) Let $C = C_f \cap C_g$ be an edge of $\mathcal{DV}^M$ and let γ be the (complete) geodesic containing it. One knows that γ is orthogonal to the geodesic $z_f z_g$ (Proposition A.2.4), and therefore its two points at infinity are distinct from z_f and z_g. As a result, $f \circ \gamma$ $(= g \circ \gamma)$ is proper (see Section A.2.3). Since μ^M is bounded, C is necessarily of finite length. □

Locally, there are only a finite number of length functions which contribute to the minimum; therefore, the vertices of $\mathcal{DV}^M$ are isolated and finite in number.

The boundary of each region C_f $(f \in \mathcal{P}^M)$ is connected, with an infinite number of edges if z_f is at infinity, and two of its vertices can be junctions for a finite number of edges. Let z and w be two arbitrary vertices of $\mathcal{DV}^M$. The geodesic segment $[zw]$

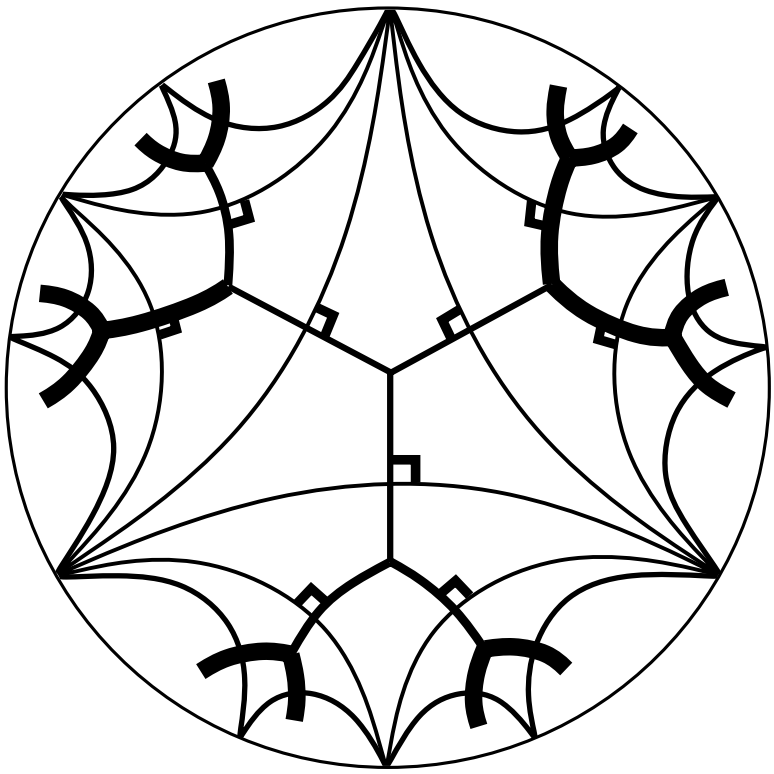

Figure A.1: All the principal points, ad infinitum, for $g = 1$, $M = (1)$.

is covered by a finite set of regions $C_{f_1}, \ldots, C_{f_N}$ with $z \in C_{f_1}, w \in C_{f_N}$ and C_{f_i} neighboring $C_{f_{i+1}}$; note that z_i a common vertex of C_{f_i} and $C_{f_{i+1}}$ $(i = 1, \ldots, N-1)$. One can join z and z_1 (resp. z_i and z_{i+1}, z_{N-1} and w) in the boundary of C_{f_1} (resp. $C_{f_{i+1}}$, C_{f_N}), therefore z and w are junctions for a finite path of edges of $\mathcal{DV}^M$.

Remark A.2.5. There exist semi-eutactic points ($M = A_3$, $z = 1/2 + i\sqrt{2}/4$) and even perfect semi-eutactic or weakly eutactic points (see Section A.3.6).

Example. The lattices of the Euclidean plane ($g = 1$, $M = (1)$). We mention this well-known example in order to make some comments on the terminology. Figure A.1 represents the two dual tilings in the Poincaré disc; it is centered at an extremal point. The "decomposition of Voronoï" which is conventionally associated with

this classical case is the image by the symmetry of center i in $\mathbb{H}$ (*i.e.,* $w = -1/z$) of our Delaunay decomposition associated with the principal points. In this last the extremal points belong with their Delaunay region, which is not the case for the conventional Voronoï regions. The 1-skeleton of the $\mathcal{DV}$ tiling is the Voronoï graph of lattices of the Euclidean plane.

Proposition A.2.10. *(Determination of perfect points)*
(1) There exists an algorithm which gives a perfect point for μ^M ($M \in P_g$).
(2) There exists an algorithm which allows one to determine the neighbors of a given perfect point in $\mathcal{DV}^M$.

Proof. (1) We want to find a vertex of $\mathcal{DV}^M$. Starting with an arbitrary non-principal point z, we successively increase the rank of perfection of z. If z is of rank 0, *i.e.,* in the interior of a region C_f ($f \in \mathcal{P}^M$), the gradient line L of f passing through z leads to a point z_1 of the 1-skeleton of ($\mathcal{DV}^M$) (because μ^M is bounded). To determine z_1, we choose $w \in L$ in the direction of ∇f and far enough from z so that $\mu^M(w) < f(w)$. Let $\mathcal{G}$ be the *finite* ensemble of length functions g such that $g(w) < f(w)$. We choose $g \in \mathcal{G}$ and calculate the point $w_1 \in L$ (lying between z and w) such that $g(w_1) = f(w_1)$. If $\mu^M(w_1) < f(w_1)$, we start the procedure over, replacing w with w_1; the ensemble $\mathcal{G}$ is strictly decreasing according to Lemma 1.8, so at the end of a finite number of steps, we will have $g(w_1) = f(w_1) = \mu^M(w_1)$ *i.e.,* $w_1 = z_1$. The point z_1 is lying on the edge $C = C_f \cap C_g$, contained in an explicit geodesic (Proposition A.2.4). We then determine a vertex of C by the same procedure.
(2) Let w be a perfect point of μ^M. Its Delaunay region D_w is generated by the principal points z_f ($f \in \mathcal{L}_w \cap \mathcal{P}^M$). Let α be a face of D_w, contained in a geodesic $\hat{\alpha}$; let $\gamma(t)$ be the geodesic parameterized by w, perpendicular to $\hat{\alpha}$ and directed towards the half plane of border $\hat{\alpha}$ not containing D_w (*i.e.,* $w \in D_w$ is directed towards the exterior of D_w). The study of lengths on γ shows that this geodesic includes an edge $C = [\gamma(0), \gamma(t_0)]$ of $\mathcal{DV}^M$ (of finite length), with $t_0 > 0$ and $\gamma(t_0)$ perfect. We calculate t_0 by the algorithm described above. Note that if the interior

of C crosses α, the intersection point is eutactic and is a local minimum of μ^M along C. □

Remark A.2.6. For (1), one can start with $z = i(\mu(M^{-1})/\mu(M))^{1/2}$ which is of rank 1 (see Section A.2.7): there is always a perfect point on the geodesic $|z|^2 = \mu(M^{-1})/\mu(M)$.

A.2.7 Study in the neighborhood of points. Voronoï's algorithm and finitude

In the following, one provides $\mathbb{H} \cup \partial\mathbb{H}$ of the usual topology for which the neighborhoods of $p \in \partial\mathbb{H}$ ("point") are generated by the horocycles centered at p (for example, $y \geq$ *constant* for $p = \infty$).

Recall the expression of length functions for the hyperbolic families (see (A.2.5)):

$$l^M_{a,b}(z) = \frac{1}{y} M^{-1}[a + xMb] + yM[b] \quad (z = x + iy \in \mathbb{H}). \tag{A.2.26}$$

Consequently, we can bound $\mu^M(z)$:

$$\min(y\mu(M), y^{-1}\mu(M^{-1})) \leq \mu^M(z) \leq y^{-1}\mu(M^{-1}) \quad (z \in \mathbb{H}), \tag{A.2.27}$$

which shows that for large y ($y^2 \geq \mu(M^{-1})/\mu(M)$), $\mu^M(z)$ equals $y^{-1}\mu(M^{-1})$ and is attained uniquely by the length function $l^M_{a,0}$ where a is a minimal vector of M^{-1}; in the same way, working with the symplectic transformation (A.2.13) one finds that

$$l^M_{a,b}(z) = \frac{|z|^2}{y} M[b + \frac{x}{|z|^2} M^{-1}a] + \frac{y}{|z|^2} M^{-1}[a] \quad (z \in \mathbb{H}). \tag{A.2.28}$$

Hence, in the neighborhood of the point 0 (for $y^2/|z|^4 \geq \mu(M)/\mu(M^{-1})$), $\mu^M(z)$ equals $|z|^2 y^{-1}\mu(M)$ and is attained uniquely by the length function $l^M_{0,b}$ where b is a minimal vector of M. *The points 0 and ∞ are therefore always principal points, and the point $i(\mu(M^{-1})/\mu(M))^{1/2}$ is always of rank 1 with principal points 0 and*

∞.

We now consider a vector $\binom{c}{d} \in \mathbb{Z}^{2g}$ such that $\Delta^M_{c,d} = M^{-1}[c]M[d] - \langle c,d\rangle^2 = 0$ and $M[d] \neq 0$. The associated point $p = -\langle c,d\rangle/M[d]$ and we define a positive quadratic form q_p on $\mathbb{R}^{2g}$ by

$$q_p(\xi,\nu) = M[M^{-1}\xi + p\nu] \qquad \begin{pmatrix}\xi\\ \nu\end{pmatrix} \in \mathbb{R}^{2g}. \tag{A.2.29}$$

The kernel of q_p is of dimension g and contains the vector $\binom{c}{d}$.

Proposition A.2.11. *Let $p = -\langle c,d\rangle/M[d] \in \mathbb{R}$ be a point associated with a vector $\binom{c}{d} \in \mathbb{Z}^{2g}$ such that $\Delta^M_{c,d} = 0$ and $M[d] \neq 0$.*
(1) $\mu^M(z)$ tends towards 0 when z tends towards p.
(2) If the kernel of q_p (defined by (A.2.29)) admits a basis of whole vectors, the point p is a principal point and μ^M is uniquely attained in the neighborhood of p by a length function; in particular the level lines of μ^M near p are of horocycles centered at p.
(3) If M is rational, the principal points situated on the edge of $\mathbb{H}$ are precisely the rational points and they verifiy assertion (2).

Remark A.2.7. Let M be rational. The analog of (2) does not hold true for the principal points situated in $\mathbb{H}$: it is possible that such a point does not belong inside the cell which it defines (example $M = A_3$, $z = 1/2 + i\sqrt{2}/4$).

Proof of the proposition. (1) The neighborhoods of the point p are generated by the horocycles images inverses of $y \geq$ *constant* for the element $\left(\begin{smallmatrix}0 & -1\\ 1 & -p\end{smallmatrix}\right)$ which maps p to ∞. One transforms the lengths by (A.2.12) in utilizing the action (A.2.14) of $PSL(2,\mathbb{R})$ on the family $\mathbb{H}M$:

$$l^M_{a,b}(z) = \frac{1}{\mathcal{Y}} M[b + \mathcal{X}(-M^{-1}a - pb)] + \mathcal{Y} q_p(a,b) \qquad \begin{pmatrix}a\\ b\end{pmatrix} \in \mathbb{R}^{2g},\ z \in \mathbb{H}, \tag{A.2.30}$$

where we define $\mathcal{X} + i\mathcal{Y} = -(z-p)^{-1} (\mathcal{X}, \mathcal{Y} \in \mathbb{R})$. Therefore $\mu^M(z) \leq l^M_{c,d}(z) =$

$M[d]/\mathcal{Y}$, which is assertion (1).

(2) The assumption on the kernel assures that q_p admits on the whole vectors a smaller nonzero value that we will denote μ_1. Let μ_2 be the minimum of $M[b]$ for *whole* nonzero vector $\binom{a}{b}$ in the kernel of q_p ($b \neq 0$ because $a = -pMb$). Relation (A.2.30) implies the inequalities

$$\min(\mathcal{Y}\mu_1, \mathcal{Y}^{-1}\mu_2) \leq \mu^M(z) \leq \mathcal{Y}^{-1}\mu_2 \quad (z \in \mathbb{H}). \tag{A.2.31}$$

From where it results that $\mu^M(z) = \mu_2/\mathcal{Y}$ for $\mathcal{Y}^2 \geq \mu_2/\mu_1$. The length functions associated with the vectors $\binom{a}{b}$ of kernel N of q_p are all proportional to $l_{c,d}$ (because $(M^{-1}[a], M[b], \langle a, b\rangle) = M[b]M[d]^{-1}(M^{-1}[c], M[d], \langle c, d\rangle)$), therefore for large $\mathcal{Y}$, $\mu^M(z)$ is uniquely attained by the length function $l_{a,b}$ with $\binom{a}{b} \in N \cap \mathbb{Z}^{2g}$ and $M[b] = \mu_2$. An explicit example is given by Proposition A.3.2, Section A.3.3.

(3) If M is rational, the principal points are obviously rational. Let $p \in \mathbb{Q}$ be a rational point distinct from ∞. Then there exist two *whole* vectors $(c, d) \neq (0, 0)$ such that $M^{-1}c + pd = 0$, so that $\Delta^M_{c,d} = 0$ and p is associated with (c, d). The assumption in assertion (2) on the kernel of q_p is clearly satisfied: p is *principal* and μ^M is attained in the neighborhood of p by a unique length function. □

Corollary A.2.12. *Let M be rational.*

(1) Modulo the action of a subgroup Γ of finite index of $PSL(2, \mathbb{Z})$, the tilings $\mathcal{DV}^M$ and $\mathcal{D}el^M$ have only one finite number of regions of each dimension. In particular the number of weakly eutactic points for μ^M is finite modulo Γ.

(2) There exists a "Voronoi" algorithm that can determine all of the perfect points modulo Γ.

(3) Let C be a finite system of representatives modulo Γ of minimal classes of dimension 0, 1 and of two-dimensional minimal classes associated with the principal points situated in $\mathbb{H}$; let Γ_c be the stabilizer of $c \in \mathcal{C}$. If χ indicates the Euler

character, one has the relation

$$\sum_{c\in\mathcal{C}} \frac{(-1)^{\dim\ c}}{\text{card }\Gamma_c} = \chi(\Gamma). \tag{A.2.32}$$

(4) Let $\mathcal{P}f$ be a finite system of representatives of perfect points modulo Γ. For $z \in \mathcal{P}f$ one notes that A_z is the hyperbolic surface of the dual region of $\mathcal{D}el^M$ of z. With the notations of (3), one has the mass formula

$$\sum_{z\in\mathcal{P}f} \frac{A_z}{\text{card }\Gamma_z} = 2\pi\,|\chi(\Gamma)|\,. \tag{A.2.33}$$

Proof. One recalls that the family $\mathbb{H}M$ admits a complete symplectic action of a subgroup of congruence $\Gamma(m)$ (see Section A.2.2) and possibly of a subgroup Γ of $PSL(2,\mathbb{Z})$ containing $\Gamma(m)$.

(1) From the proposition (assertions (2) and (3)) the skeleton of dimension 1 of $\mathcal{DV}^M$, denoted $(\mathcal{DV}^M)^1$, remain far from the rational points (which are finite in number modulo Γ), *i.e.,* in a compact part of $\Gamma\setminus\mathbb{H}$. The result follows.

(2) Assertion (1) and Theorem 1.1(4) show that the quotient $\Gamma\setminus(\mathcal{DV}^M)^1$ is a *finite and connected* graph, of which the vertices are the perfect points for μ^M modulo Γ. One can describe this graph thanks to Proposition A.2.10. One seeks initially a perfect point and its neighbors, then the neighbors of new pefect points obtained by the action of Π. At the end of a finite number of steps, one will have determined all of the vertices of $\Gamma\setminus(\mathcal{DV}^M)^1$. Note that one also obtains all of the eutactic points modulo Γ (see Section A.2.5).

(3) Let us suppose initially that Γ acts without fixed points on $\mathbb{H}$. Let c_k ($k = 0,1,2$) be the number of k-dimensional regions of $\mathcal{DV}^M$ modulo Γ (c_0 is the number of perfect points, and c_2 is the number of principal points) and let c_2^F be the number of two-dimensional regions associated with the principal points situated in $\mathbb{H}$. The Euler-Poincaré relation for the surface $\Gamma\setminus\mathbb{H}$ supplemented by the points is written

$$c_2 - c_1 + c_0 \;=\; 2 - 2g_\Gamma, \tag{A.2.34}$$

where g_Γ is the genus of Γ. The character of Γ is given by $\chi(\Gamma) = c_2^F - c_1 + c_0$.

The general case (Γ with torsion) is easily obtained by passage to a subgroup without torsion of finite index.

(4) The dual region of a perfect point z is a hyperbolic polygon generated by a finite number of points of $\mathbb{H} \cup \delta\mathbb{H}$ (the principal points associated with z). Its surface A_z is therefore finite. As in (3), one begins by supposing that Γ is without torsion, in which case one obviously has $\sum_{z\in\mathcal{P}f} A_z = \text{Surface}(\Gamma \setminus \mathbb{H}) = 2\pi|\chi(\Gamma)|$. The general case results immediately. Note that the stabilizer of a perfect point for the action of Γ coincides with that of its dual region. □

Example. For $\Gamma = \Gamma(m)$ $(m \leq 2)$ one has $c_2 - c_1 + c_0 = 2 - 2g_m$, where $g_m = 1 + k_m(m-6)/(12m)$ with $k_2 = 6$ and $k_m = (m^3/2)\Pi_{p|m}(1 - 1/p^2)$ for $m \geq 3$ (see [Sh, p.22]).

Relations (A.2.32) and (A.2.33) (like (A.2.36)) are illustrated in Section A.3.5 with $M = A_n$ and $\Gamma = \Gamma_0(n+1)$ $(1 \leq n \leq 16)$.

Remark A.2.8. (1) Let M be rational and $z = x + iy$ be a perfect or eutactic point for μ^M. Then *x and $|z|^2$ are rational* (hence, y^2 is rational). Indeed, the principal points verify this property, and the geodesics which carry the edges of the graph as those which join the principal points have an equation of the form $\alpha|z|^2 + \beta x + \gamma$ with $\alpha, \beta, \gamma \in \mathbb{Q}$. Consequently, the Gram matrix is proportional to a whole matrix:

$$\phi_g(zM) = \lambda A \quad A \text{ whole}, \lambda^2 \in \mathbb{Q}, \tag{A.2.35}$$

and, in particular, $\mu(zM)^2$ is rational.

(2) All that preceded also applies to matrices M which satisfy the hypotheses of Proposition A.2.6: such a matrix is rational up to a factor as a single projective solution of a homogeneous linear system with rational coefficients.

(3) If $M = (1)$, (A.2.33) shows that the hexagonal lattice is the unique perfect lattice in two dimensions. For the lattices of larger dimensions, we have a formula analogous to (A.2.33), but we do not explicitly know the volumes.

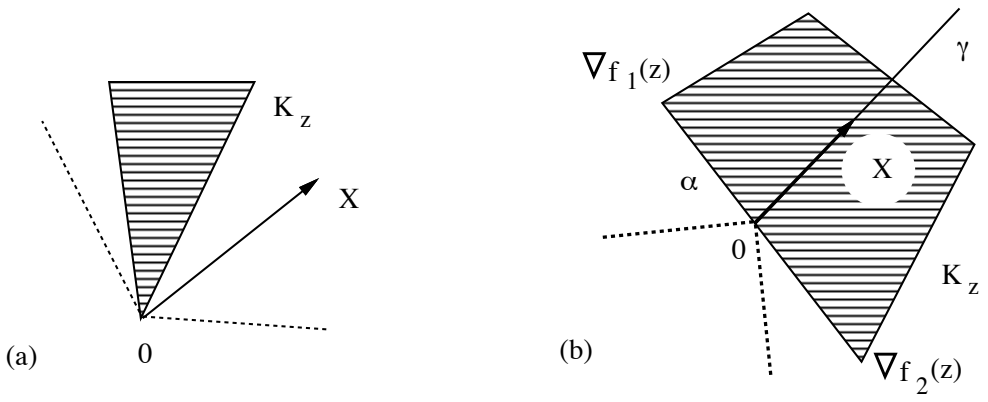

Figure A.2: Semi-eutactic points.

A.2.8 Morse's theory

One knows that Hermite's constant of lattices is a Morse function on P_n and that its critical points are the eutactic lattices ([As]). It is the same for each hyperbolic family.

Proposition A.2.13. *For every lattice $M \in P_g$, the function $\mu^M : \mathbb{H} \to \mathbb{R}^+$ is Morse and its critical points are the z with zM relatively eutactic in $\mathbb{H}M$. The Morse index of such a point is equal to its rank of perfection.*

Proof. Recall that a function ϕ is toplogically Morse if any point of the source admits a topological Morse coordinate.

If there exists in the vicinity of a point a local oriented covering of dimension 1 such that ϕ is strictly increasing along each sheet, then the point is regular for ϕ. For example, if $z \in \mathbb{H}$ is not semi-eutactic, there exists a nonzero vector X such that $\langle X, \nabla f(z) \rangle > 0$ for every length function $f \in \mathcal{P}^M \cap L_z$ (see A.1.5 for the notations); the right-hand local oriented covering parallel to X verifies the preceding condition, and z is regular for μ^M.

Let z be semi-eutactic but not eutactic, and let K_z be the convex hull of principal gradients of z. The neighborhood of z is divided into sectors for the edges of the tiling $\mathcal{DV}^M$ and in each sector μ^M is given as a principal function.

Two cases are presented: 0 is a vertex of K_z or 0 is in the interior of an edge of K_z. In the first case z is a principal point of the lattice $z = z_f$ ($f \in \mathcal{P}^M$). There exists a nonzero vector X such that $\langle X, Y\rangle > 0$ for all $Y \in K_z \setminus \{0\}$; X is inevitably inside the sector $\sum_f$ associated with f (Figure A.2a). For w close to z, we define $\mathcal{X}(w) = X$. If $w \in \sum_f \setminus \{z\}$, we have $\langle \mathcal{X}(w), \nabla f(w) > 0$ because ∇f is radial from z. The same inequality holds true for any point w for the other principal functions in z (by choice of X). This implies that μ^M is strictly increasing along the orbits of $\mathcal{X}$. Now consider the case where 0 is in the interior of an edge α of K_z, the convex hull of two principal gradients $\nabla f(z)$ and $\nabla g(z)$. We denote $\sum_f$ and $\sum_g$ as the assoicated closed sectors, separated by a semi-geodesic $\gamma(t)$ ($t \geq 0$) with initial direction $X = \gamma'(0)$ orthogonal to α (Figure A.2b). We then define a champ of vectors $\mathcal{X}$ continuous by pieces in the vicinity of z. If $w = \gamma(t)$ we take $\mathcal{X}(w) = \gamma'(t)$; if $w \in \sum_f \cup \sum_g \setminus \gamma$ there exists a choice $\mathcal{X}(w)$ of class C^1 such that $\lim_{w\to\gamma(t)} \mathcal{X}(w) = \gamma'(t)$; finally, if $w \notin \sum_f \cup \sum_g$ we define $\mathcal{X}(w) = X$. The orbits of $\mathcal{X}$ piecewise form an oriented covering C^1 and μ^M is strictly increasing along the sheets. This is true for the orbit of z results due to the strict convexity of the length functions and for theothers due to the condition $\langle \mathcal{X}(w), \nabla h(w)\rangle > 0$ ($h \in \mathcal{P}^M \cap \mathcal{L}_z$). We conclude that z is regular. Note that the level of the point z admits a cusp at z.

To achieve the proof of the proposition, one observes that the eutactic points of rank k have Morse index k ($k = 0, 1, 2$). For example, in the neighborhood of a eutactic point z of rank 1, μ^M is the minimum of two strictly convex functions and the singular level is the intersection of two curves (circles or horocycles) tangent to z. □

Remark A.2.9. Hermite's constant on Siegel's space $\mathfrak{H}_g$ is not a Morse function ([Bv]).

Corollary A.2.14. *Suppose M is rational and μ^M is invariant for a subgroup Γ of finite index in $PSL(2, \mathbb{Z})$. Let $\mathcal{E}_\Gamma$ be a system of representatives of eutactic points modulo Γ; we will denote Γ_z as the stabilizer of z ($z \in \mathcal{E}_\Gamma$) and* ind_z *as its*

Morse index. These data determine the Euler character of Γ*:*

$$\sum_{z\in\mathcal{E}_\Gamma} \frac{(-1)^{\mathrm{ind}_z}}{\mathrm{card}\ \Gamma_z} = \chi(\Gamma). \tag{A.2.36}$$

Proof. Even if it means to take a subgroup of finite index, one can suppose that Γ acts without fixed points. From Proposition A.2.11 (3), μ^M induces a Morse function on the compact surface $\Gamma \setminus (\mathbb{H} \cup \mathbb{Q} \cup \{\infty\})$. Let e_k be the number of eutactic points of rank $k = 0, 1, 2$ modulo Γ; e_2 is the number of extremal points modulo Γ. We have the following relation:

$$e_2 - e_1 + e_0 + \nu_\Gamma \ = \ 2 - 2g_\Gamma, \tag{A.2.37}$$

where ν_Γ is the number of points of Γ and g_Γ is its genus. This proves the formula for the case without torsion and the general case easily follows. □

Remark A.2.10. The two relations of Euler (A.2.32) and (A.2.36) are analogous but not always identical, because *the number of eutactic points can be strictly lesser than the number of minimal classes* (modulo Γ). For example, this is the case for the family $\mathbb{H}A_3$ (see Section A.3).

A.3 Examples

A.3.1 Families A_n. Forms F_{2n}

This is the principal example of this article. As usual, A_n is the matrix defined by $A_n(j,k) = 1$ (resp. 2) if $j \neq k$ (resp. $j = k$) for $n \geq 2$ and one agrees to set $A_1 = (1)$. The lattice A_n verifies the hypotheses of Proposition A.2.6: all the eutactic (resp. semi-eutactic) points relative to $\mathbb{H}A_n$ are eutactic (resp. semi-eutactic) in P_{2n}, therefore also in $\mathfrak{H}_n$. One draws aside the value $n = 1$ which corresponds to

the well-known case of two-dimensional lattices. The most interesting point is

$$z_{1,n} = \frac{1}{2(n+1)}\left(n + i\sqrt{n(n+2)}\right) \quad (n \geq 2), \tag{A.3.1}$$

lying on the geodesic $|z|^2 = n/2(n+1)$ where the lengths associated with the points 0 and ∞ (*i.e.,* $l_0(z) = 2|z|^2/y$ and $l_\infty(z) = n/(n+1)y$) are equal (see A.1.7).

Theorem A.3.1. *The lattice $F_{2n} = z_{1,n}A_n (n \geq 2)$ is extremal symplectic in $\mathfrak{H}_n$. It admits $(n+1)(3n+2)/2$ pairs of minimal vectors of norm $2\sqrt{n/(n+2)}$.*

Proof. Here is initially a method for determining the length functions taking a small value at one point. The techniques used in this method will also be necessary for the other examples studied in this article. $M, z = x + iy$ and $\lambda \in \mathbb{R}$ are given, to find all the pairs (a, b) such that $l^M_{a,b}(z) \leq \lambda$ where

$$l^M_{a,b}(z) = \frac{1}{y}(M^{-1}[a] + 2x\langle a, b\rangle + |z|^2 M[b]) \quad (z \in \mathbb{H}). \tag{A.3.2}$$

One starts by bounding $M[b]$ and $M^{-1}[a]$ with the relations (A.2.26) and (A.2.28). Then, for further limiting the possibilities, one bounds $\langle a, b\rangle$ using the inequality:

$$\langle a, b\rangle^2 \leq M^{-1}[a]M[b]. \tag{A.3.3}$$

Note that the equality in (A.3.3) occurs if and only if $(M^{-1}[a])^{1/2}b = \pm M[b]^{1/2}$ $M^{-1}a$ (one writes $\langle a, b\rangle = \langle M^{-1/2}a, M^{1/2}b\rangle$ where $M^{1/2}$ is a square root of M). The explicit knowledge of M then provides a finite number of pairs (a, b),including the minimum (and the minimal vectors) of the lattice zM.

For $F_{2n} = z_{1,n}A_n$ and $\lambda = 2(n/(n+2))^{1/2}$, one is quickly led to $a = 0$, or $b = 0$, or (knowing that $A_n[b]$ is even) $A_n[b] = 2$, $\langle a, b\rangle = -1$ and $A_n^{-1}[a] = n/(n+1)$. On all these pairs (a, b), F_{2n} has the value λ, which is therefore the minimum.

Thus $z_{1,n}$ admits three principal points: ∞, 0 and $p_n = (1 + i[(n-1)/(n+1)]^{1/2})/2$. The associated minimal vectors (a, b) are respectively, expressed in the natural basis $(e_j)_{1\leq j\leq n}$ of $\mathbb{Z}^n$, $(e_j, 0)$ and $(\sum e_j, 0)$ $(n+1$ vectors), $(0, e_j)$ and

$(0, e_j - e_k)$ ($j \neq k$, $n(n+1)/2$ vectors), $(e_j, -e_j)$, $(\sum e_j, -e_j)$, $(-e_j, e_j - e_k)$ and $(e_k, e_j - e_k)$ ($j \neq k$, $n(n+1)$ vectors).

We remark in summary that $z_{1,n}$ lies in the interior of its Delaunay region (a triangle with vertices ∞, 0, p_n); therefore F_{2n} is eutactic in $\mathbb{H}A_n$ (Theorem 1.1 (3)). This also results in the relation $\nabla^\infty + \nabla^0 + n\nabla^{p_n} = 0$ among the three relative gradients (A.2.21). Consequently, F_{2n} is eutactic in $\mathfrak{H}_n$ and even in P_{2n} (Proposition A.2.5). It remains to be verified that the gradients of minimal vectors in $\mathfrak{H}_n$ generate their tangent space $S_n(\mathbb{C})$. From (A.2.5) and the quadratic equation $2(n+1)z^2 - 2nz + n = 0$ satisfied by $z_{1,n}$, one easily finds that

$$\begin{aligned} i\nabla_{a,b}(z_{1,n}A_n) &= [aa' + \frac{1}{2}(A_nba' + ab'A_n)] \\ &\quad + z_{1,n}^2[A_nbb'A_n + \frac{n+1}{n}(A_nba' + ab'A_n)]. \end{aligned} \tag{A.3.4}$$

The $\mathbb{R}$-vector space $S_n(\mathbb{C})$ can be decomposed as $S_n(\mathbb{C}) = S_n(\mathbb{R}) \oplus z_{1,n}^2 S_n(\mathbb{R})$. The gradients (A.3.4) of the vectors associated with the point 0 generate the component of $z_{1,n}^2$ (because A_n is perfect in P_n) and the first components of the other "minimal" gradients (A.3.4) generate $S_n(\mathbb{R})$; therefore F_{2n} is perfect in the symplectic sense. As in [B-M1] (see also [Bv, Section 3.3]) one concludes that F_{2n} is extremal in $\mathfrak{H}_n$. □

Remark A.3.1. We know that $F_4 \simeq D_4$. For $n \geq 3$ the lattice F_{2n} is not perfect in P_{2n} for lack of minimal vectors.

A.3.2 Families A_n (continued). Forms G_{2n}

Let us pass now to the study of the neighbors of $z_{1,n}$ for $n \geq 3$. For reasons of symmetry, two neighbors are obvious ($-\overline{z_{1,n}}$ and $1 - \overline{z_{1,n}}$); the third is given by

$$z_{2,n} = \frac{1}{2(n+1)}\left(n + i\sqrt{(n^2-4)/3}\right) \quad (n \geq 4, n \neq 5) \tag{A.3.5}$$

with $z_{2,3} = (3 + i\sqrt{7})/8$ and $z_{2,5} = (5 + i\sqrt{11})/12$. For $n \neq 4$, $z_{2,n}$ has principal points 0, 1/2 and p_n (see Lemma A.3.1).

Theorem A.3.2. *The lattice $G_{2n} = z_{2,n}A_n$ $(n \geq 3)$ is extremal in P_{2n}. For $n \geq 6$, its minimum value is $4(n-1)/\sqrt{3(n^2-4)}$ and it admits $2n(n+1)$ (resp. 147) pairs of minimal vectors if $n \neq 7$ (resp. if $n = 7$).*

Remark A.3.2. For $n = 3$, 4 and 5 one will be able to consult Table A.2 ($G_6 \simeq J_K$, Jacobian of the Klein manifold, and $G_8 \simeq E_8$). These particular cases show the existence of small exceptional values of A_n^{-1} (see Lemma A.3.1): for $n = 4$ there are more minimal vectors and for $n = 3$ or 5 the principal function associated with the point 1/2 is "non-generic" (see Proposition A.3.2).

Proof. Let us suppose that $n \geq 6$; the cases of $n = 3$, 4 and 5 are treated analagously. For (A.3.2) one has that $l_{0,b}(z_{2,n}) \geq \lambda_n = 4(n-1)(3n^2-12)^{-1/2}$ with equality for $A_n[b] = 2$ (function associated with the point 0) and $l_{a,0}(z_{2,n}) > \lambda_n$. We now consider $a \neq 0$ and $b \neq 0$ such that $l_{a,b}(z_{2,n}) \leq \lambda_n$. The method shown in Section A.3.1 gives the following bounds:

$$A_n[b] \leq 8, \quad A_n^{-1}[a] \leq \frac{8(n-1)^2}{3(n^2-4)} \quad \text{and} \quad -4 \leq \langle a, b \rangle \leq -1. \tag{A.3.6}$$

Next one examines the four possible values of a, b, and for each case the values of $A_n[b]$, knowing that the small values of $A_n^{-1}[a]$ are defined by Lemma A.3.1. After a rather long discussion (which also uses $l_{a,b}(z_{2,n}) \leq \lambda_n$ and the inequality (A.3.3)), one is led to two possibilities for $(\langle a, b \rangle, M[b], A_n^{-1}[a])$: $(-1, 2, n/(n+1))$ which correspond to the principal point p_n (see Lemma A.3.1) and (-4, 8, 2) which gives a new principal point 1/2. The number of minimal vectors associated with this point 1/2, given explicitly by Lemma A.3.1, is $n(n+1)/2$ (although there are 35 for $n = 7$). For $n = 8$, there are exceptional vectors such that $A_n^{-1}[a] = 2$ but the b determined by the equality in (A.3.3) are not complete.

It is still necessary to establish that G_{2n} is extremal in P_{2n}. Eutaxy is verified in $\mathbb{H}A_n$ (Proposition A.2.6) in the same manner as for $z_{1,n}$ (see Lemma A.3.1). For perfection, one considers the subspace of $S_{2n}(\mathbb{R})$ generated by $\left(\begin{smallmatrix} aa' & ab' \\ ba' & bb' \end{smallmatrix}\right)$ (with minimal vector $\left(\begin{smallmatrix} a \\ b \end{smallmatrix}\right)$) and one shows that its orthogonal for $\mathrm{Tr}(XY)$ is reduced to

the zero vector. Let $X = \left(\begin{smallmatrix} U & V \\ V' & W \end{smallmatrix}\right) \in S_{2n}(\mathbb{R})$ (where U and W are symmetric) be such that

$$U[a] + 2a'Vb + W[b] = 0 \tag{A.3.7}$$

for all minimal vectors $\binom{a}{b}$ of G_{2n}. In solving the linear equations, one finds that $W = 0$ with the vectors of the point 0, and $U = V = 0$ with the other vectors. Up to demonstrating Lemma A.3.1, this completes the proof of the theorem. □

Lemma A.3.1. *(small values of A_n^{-1}) Let $n \geq 2$, $a \in \mathbb{Z}^n$ let $(a \neq 0)$, let $(e_j)_{1\leq j\leq n}$ be the canonical basis of $\mathbb{Z}^n$ and let $u = \sum_{1\leq j\leq n} e_j$. If $A_n^{-1}[a] \leq 8/3$ there are three possibilities:*

- $A_n^{-1}[a] = n/(n+1)$ *and* $a = e_j$ *or* $a = u$ $(n \geq 2)$,
- $A_n^{-1}[a] = 2(n-1)/(n+1)$ *and* $a = e_j + e_k$ $(j \neq k)$ *or* $a = u - e_j$ $(n \geq 3)$,
- $A_n^{-1}[a] = 2$ *and* $a = e_j - e_k$ $(j \neq k)$ *or* $a = u + e_j$ $(n \geq 2)$,

with the following exceptions:

- $a = (2,0)$ *or* $a = (2,2)$, $A_n^{-1}[a] = 8/3$,
- $a = e_{i_1} + \ldots + e_{i_p}$ *with*
  $5 \leq n \leq 26$, $p = 3$ *or* $n-2$ *and* $A_n^{-1}[a] = 3(n-2)/(n+1)$,
  or $7 \leq n \leq 11$, $p = 4$ *or* $n-3$ *and* $A_n^{-1}[a] = 4(n-3)/(n+1)$,
  or $n = 9$, $p = 5$ *and* $A_n^{-1}[a] = 5/2$.

Proof of the lemma. Let us define $a = \sum_{1\leq j\leq n} a_j e_j$ and $\|a\|_\infty = \max_{1\leq j\leq n} |a_j|$. Recall the expression

$$A_n^{-1}[a] = \sum_{1\leq j\leq n} a_j^2 - \left(\sum_{1\leq j\leq n} a_j\right)^2 /(n+1). \tag{A.3.8}$$

The values of the coordinates a_j are restricted according to the inequality (A.3.3) by successively taking $b = e_j, e_j - e_k, e_j + e_k + e_l$ $(n \geq 3)$ and $e_j + e_k - e_l - e_m$

$(n \geq 4)$:

$$|a_j| \leq 2, |a_j - a_k| \leq 2, |a_j + a_k + a_l| \leq 5 \text{ and } |a_j + a_k - a_l - a_m| \leq 3. \quad \text{(A.3.9)}$$

From (A.3.8) and (A.3.9), one then discusses the possibilities of $\|a\|_\infty = 1$ or 2. □

A.3.3 Families A_n (continued). Forms $H_{2n}(\varphi)$ ($\varphi \in SL_2(\mathbb{Z})$)

In this paragraph, we pursue the exploration of perfect points of $\mathbb{H}A_n$. To each element $\varphi = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$ we associate the point z_φ of $\mathbb{H}$ defined by

$$z_\varphi = \frac{2\alpha\beta + \alpha\delta + 2\gamma\delta + \beta\gamma + i\sqrt{3}}{2\,(\beta^2 + \beta\delta + \delta^2)} \quad \text{(A.3.10)}$$

When n is large compared to the coefficients of φ, the point z_φ is perfect and even gives an extremal point of $\mathfrak{H}_n$ (Theorem 2.3). Its Delaunay region is the hyperbolic triangle formed by the points γ/δ, $(\alpha+\gamma)/(\delta+\beta)$ and α/β $(\alpha\delta - \beta\gamma = 1)$. In particular the successive neighbors of $z_{2,n}$ associated with the point 0 are of the form

$$z(m) = \frac{2m - 1 + i\sqrt{3}}{2\,(m^2 - m + 1)} \quad (m \geq 3), \quad \text{(A.3.11)}$$

which are perfect points when $n \geq 2m$; $z(m)$ is associated with $\varphi = \left(\begin{smallmatrix} 1 & m-1 \\ 0 & 1 \end{smallmatrix}\right)$ and therefore with the region $(0, 1/m, 1/(m-1))$. We define $H_{2n}(m) = z(m)A_n$ and $H_{2n}(\varphi) = z_\varphi A_n$. The principal length functions of z_φ are made explicit in the following proposition:

Proposition A.3.2. *(principal functions associated with the points)*

Let $n \geq 8$ and let α/β be a rational point with $\beta \neq 0$, α and β relatively prime. If n is even (resp. odd) suppose that $n+1$ does not divide β (resp. 2β). Then the principal length function f associated with the point α/β is given by

$$f(z) = \frac{1}{y}\left(2\alpha^2 - 4\alpha\beta x + 2\beta^2|z|^2\right) \quad (z \in \mathbb{H}). \quad \text{(A.3.12)}$$

This is realized by $n(n+1)/2$ pairs of vectors $\left(\begin{smallmatrix} a \\ b \end{smallmatrix}\right) \in \mathbb{Z}_{2n}$ ($a = \alpha a_0$ with $A_n^{-1}[a_0] = 2$

and $b = -\beta A_n^{-1} a_0$*).*

For $2 \leq n \leq 7$*, the corresponding result is valid provided that* $\beta \notin 2\mathbb{Z}$ *(resp.* $7\mathbb{Z}$*,* $8\mathbb{Z}$*) if* $n = 5$ *(resp. 6, 7).*

Proof. Recall that the minimal vectors $\binom{a}{b} \in \mathbb{Z}^{2n}$ near the point α/β are determined by the relations $A_n^{-1}[a]A_n[b] = \langle a, b\rangle^2, -\langle a, b\rangle/A_n[b] = \alpha/\beta$ with $A_n[b]$ a minimum for these properties (see A.1.7). Suppose that $\alpha \neq 0$ (see Lemma A.3.1 for $\alpha = 0$). One also has that $b = -(\beta/\alpha)A_n^{-1}a = -(\beta/\alpha)(a - \langle a, u\rangle u/(n+1))$ with $u = \sum_{j=1}^{n} e_j$ ((A.3.3) in the case of equality), and of course b *must be whole.* In calculating $\langle b, u\rangle$ one sees that (β/α) $(\langle a, u\rangle/(n+1))$ is whole; therefore $\beta a/\alpha$ is whole and α divides a. We define $a = \alpha a_0$ with $a_0 \in \mathbb{Z}^n$ and remark that $A_n^{-1}[a_0] = 2$ gives the values indicated in the statement. There remains the possibility of $A_n^{-1}[a_0] < 2$. The corresponding vectors a_0 are explicit for Lemma A.3.1, and one notes that $n+1$ divides β (resp. 2β) if $A_n^{-1}[a_0] = n/(n+1)$ (resp. $2(n-1)/(n+1)$). There are three exceptional values of $A_n^{-1}[a_0] < 2$ of the lattice $3(n-2)/(n+1)$ for $n = 5$, 6 or 7 (Lemma A.3.1), and by writing that b is whole one finds the conditions announced for β. □

Theorem A.3.3. *Let* $n \geq 9$ *and let* $\varphi = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in SL(2, \mathbb{Z})$ *with nonnegative* $\alpha, \beta, \gamma, \delta$ *and with* $0 \leq \frac{\gamma}{\delta} \leq \frac{\alpha}{\beta} \leq \frac{1}{2}$*. If* $n \geq 2(\beta + \delta)$ *then the lattice* $H_{2n}(\varphi) = z_\varphi A_n$ *is extremal in* $\mathfrak{H}_n$ *and has* $3n(n+1)/2$ *pairs of minimal vectors with norm* $4/\sqrt{3}$*.*

Remark A.3.3. For $6 \leq n \leq 8$ the forms we're concerned with, *i.e.,* due to the isomorphism of $H_{12}(3) \simeq K_{12}$, $H_{14}(3)$ and $H_{16}(3)$ are also extremal symplectic extremal with minimum $4/\sqrt{3}$, but with more minimal vectors (see Table A.2).

Proof. The point z_φ is l'image of $z(3) = \frac{5+i\sqrt{3}}{14}$ for $\psi = \left(\begin{smallmatrix} \alpha-2\gamma & \gamma \\ \beta-2\delta & \delta \end{smallmatrix}\right) \in SL(2, \mathbb{Z})$. This transformation envoie the points 0, 1/3, 1/2 on γ/δ, $(\alpha+\gamma)/(\delta+\beta)$, α/β. Following (A.2.11), the lattice $H_{2n}(\varphi)$ is the image of $z(3)A_n$ under the action in P_{2n} of the element

$$P = \left(\begin{smallmatrix} \delta I_n & (\beta-2\delta)A_n^{-1} \\ \gamma A_n & (\alpha-2\gamma)I_n \end{smallmatrix}\right) \in Sp(2n, \mathbb{Q}). \tag{A.3.13}$$

It is elementary to verify that the minimal vectors of points 0, 1/3 and 1/2 are mapped by P'^{-1} to the points γ/δ, $(\alpha+\gamma)/(\delta+\beta)$ and α/β; all these vectors are made explicit by Proposition A.3.2 (for example, for α/β: $a=\alpha(e_j-e_k)$ and $b=-\beta(e_j-e_k)$ or $a=\alpha(e_j+u)$ and $b=-\beta e_j$ up to a sign). We also remark that the principal length functions of these three points take the same value $4/\sqrt{3}$ at the point z_φ, independently of φ. With these observations made, we can prove the theorem by verifying that the minimum of $H_{2n}(\varphi)$ equals $4/\sqrt{3}$ (with the good number of minimal vectors) and that $H_{2n}(3)$ is extremal symplectic. Indeed, the $3n(n+1)/2$ minimal vectors of $H_{2n}(3)$ (associated with the points 0, 1/3 and 1/2) form an extremal symplectic configuration and are transformed, in a nonwhole way (which does not matter), in an extremal symplectic configuration of minimal vectors of $H_{2n}(\varphi)$.

To determine the minimum of $H_{2n}(\varphi)$, we start by placing the length functions in a form which reveals in a symmetrical way the three points γ/δ, $(\alpha+\gamma)/(\delta+\beta)$ and α/β. Let $X=\delta a+\gamma A_n b$ and $Y=\beta a+\alpha A_n b$. A small calculation allows us to verify that

$$l^{A_n}_{a,b}(z_\varphi)=\frac{1}{\sqrt{3}}\left(A_n^{-1}[X]+A_n^{-1}[Y]+A_n^{-1}[X+Y]\right). \tag{A.3.14}$$

This formula also arises rather naturally starting with relation (A.2.12) for the transformation of lengths knowing that $z_\varphi=\psi(\frac{5+i\sqrt{3}}{14})$. One is therefore led to the following inequality:

$$A_n^{-1}[X]+A_n^{-1}[Y]+A_n^{-1}[Z]\leq 4 \tag{A.3.15}$$

with X, Y and Z satisfying $X+Y+Z=0$. One sees with Lemma A.3.1 that there exist two possibilities (for $n\geq 9$): either one of the vectors X, Y or Z is zero, or two of these vectors are minimal for A_n^{-1}. Let us examine the first possibility, with for example $Z=-X-Y=0$, *i.e.*, $(\beta+\delta)a+(\gamma+\alpha)A_nb=0$. Since $(\beta+\delta)$ and $(\gamma+\alpha)$ are relatively prime, a is divisible by $(\gamma+\delta)$ and necessarily $a=(\gamma+\alpha)X$, $b=-(\beta+\delta)A_n^{-1}X$. Following (A.3.15), one has $A_n^{-1}[X]\leq 2$. If

$A_n^{-1}[X] = 2(n-1)/(n+1)$ (resp. $n/(n+1)$) then the vector $2(\beta+\delta)u/(n+1)$ (resp. $(\beta+\delta)u/(n+1)$) must be whole, which is impossible since $n \geq 2(\beta+\delta)$. The only possible value possible is therefore $A_n^{-1}[X] = 2$ which gives the minimal vectors of the point $(\alpha+\delta)/(\beta+\gamma)$, with equality in (A.3.15). The case $X = 0$ or $Y = 0$ is treated analagously and leads to the minimal vectors of points γ/δ or α/β (with equality in (A.3.15)). Suppose now that X and Y are minimal vectors of A_n^{-1}. One has $b = A_n^{-1}(\delta Y - \beta X)$, where $(\beta \pm \delta)u/(n+1)$ is whole, which is absurd. The other cases are eliminated by the same method and finally the minimum of $H_{2n}(\varphi)$ is shown to be $4/\sqrt{3}$ for $n \geq 2(\beta+\delta)$.

It remains to be established that $H_{2n}(3)$ is extremal. Eutaxy in P_{2n} results from the relative eutaxy in $\mathbb{H}A_n$ (Proposition A.2.6), which is clear either geometrically via Theorem A.2.1 (3), or algebraically (the sum of the three relative gradients (A.2.21) is zero for $z(3)$). For perfection, one proceeds as in Section A.3.1 by decomposing the gradients (A.2.5) in $\mathfrak{H}_n$ as $S_n(\mathbb{R}) \oplus z(3)^2 S_n(\mathbb{R})$. The gradients associated with the point 0 generate the component of $z(3)^2$ (see Section A.3.1). For those of the point 1/2, the other component equals aa' since $A_n b = -2a$. Let $T = (t_{jk}) \in S_n(\mathbb{R})$ such that $\mathrm{Tr}\,(aa'T) = T[a] = 0$ for $a = e_j - e_k$ $(j < k)$ and $a = e_j + \sum e_j$. One easily checks that $T = 0$, and therefore the gradients of points 0 and 1/2 generate their tangent space $S_n(\mathbb{C})$ at the point $z(3)$. Since $z(3)A_n$ is already eutactic (thanks to the third point!) one concludes that it is also perfect, which completes the proof of the theorem. □

Remark A.3.4. The forms $H_{2n}(\varphi)$ are rather similar at first sight because their ensembles of minimal vectors are interchangeable by rational symplectic transformations (see (A.3.13)). They therefore have the same minimum, the same rank of usual or symplectic perfection and the same usual or symplectic "spectrum" (values of the (symplectic) lattice on the pairs of minimal vectors). However, they are not always isomorphic: for $n \leq 16$, the $H_{2n}(\varphi)$ coming from distinct points $z(\varphi)$ modulo $\Gamma_0(n+1)$ are pairwise nonisomorphic (see the comments that follow Table A.2).

A.3.4 Families A_n (continued). Forms J_{4m-2}

The perfect points of the preceding paragraph have every Delaunay region generated by three regular points in the sense of Proposition A.3.2. We give here an example with an "irregular" point: $1/m$ with $n = 2m-1$. The associated principal function equals $2(m-1)(1/m-2x+m|z|^2)/y$; this is realized by $n(n+1)/2$ vectors $\binom{a}{b} \in \mathbb{Z}^{2n}$ such that $A_n^{-1}[a] = 2(n-1)/(n+1)$ and $b = -mA_n^{-1}a$, entirely due to the relation $n+1 = 2m$. We define

$$w(m) = \frac{2m-3+i\sqrt{3-4/m}}{2(m-1)^2} \quad (m \geq 4). \tag{A.3.16}$$

Theorem A.3.4. *Let $m \geq 4$. The form $J_{4m-2} = w(m)A_{2m-1}$ is extremal in $\mathfrak{H}_{2m-1}$ with minimum $4(m-1)/\sqrt{m(3m-4)}$ for $3m(2m-1)$ pairs of minimal vectors.*

Proof. One proceeds as in the proof of Theorem 2.3. The point $w(m)$ will have two regular principal points (0 and $1/(m-1)$) and one irregular principal point $(1/m)$. The lengths are written in a form adapted to these points:

$$\begin{aligned} l_{a,b}^{A_n}(w(m)) \quad = \quad & \frac{1}{m\sqrt{3-4/m}}(mA_n^{-1}[a] + mA_n^{-1}[(m-1)a + A_n b] \\ & + (m-2)A_n^{-1}[ma + A_n b]). \end{aligned} \tag{A.3.17}$$

In setting $X = a$ and $Y = (m-1)a + A_n b$ one is led to the inequality

$$mA_n^{-1}[X] + mA_n^{-1}[Y] + (m-2)A_n^{-1}[X+Y] \leq 4(m-1) \tag{A.3.18}$$

analogous to (A.3.15) and which allows one to determine the minimum of J_{4m-2} and its minimal vectors.

The point $w(m)$ satisfies the equation $m(m-1)^2z^2 - m(2m-3)z + m - 1 = 0$, and eutaxy of J_{4m-2} results from $(m-1)\nabla^0 + (m-2)\nabla^{\frac{1}{m}} + (m-1)\nabla^{\frac{1}{m-1}} = 0$, relation between the relative gradients (of the point $w(m)$) associated with the three principal points of $w(m)$. Finally for the perfection of J_{4m-2} in $\mathfrak{H}_{2m-1}$,

one proceeds as in Section A.3.3 by decomposing the tangent space in the form $S_n(\mathbb{C}) = S_n(\mathbb{R}) \oplus w(m)^2 S_n(\mathbb{R})$. □

A.3.5 Extremal points of families A_n for $1 \leq n \leq 16$

Here are some numeric data and some commentary on the families $\mathbb{H}A_n$ for small values of n. Table A.1 gives the number of eutactic points of families $\mathbb{H}A_n$ for $1 \leq n \leq 16$. The subgroup Γ of $PSL(2,\mathbb{Z})$ which acts by complete symplectic transformations on the family is $\Gamma = PSL(2,\mathbb{Z})$ for $n = 1$ and $\Gamma = \Gamma_0(n+1)$ for $n \geq 2$ (see (A.2.14) and (A.2.15)). The notations of Table A.1 are as following: ind is the index of Γ in $PSL(2,\mathbb{Z})$, (g,ν) its signature (genus, number of points) and $\chi(\Gamma)$ its Euler character; e'_k $(k = 0,1,2)$ designates the number (dependent on the stabilizers) of eutactic points of Morse index k counted modulo Γ. The two Euler relations (A.2.32) and (A.2.36) are identical for all these examples except for $n = 3$; in this case the number of classes is given by $c_0 = 4$, $c_1 = 6$ and $c_2^F = 1$ (with the notations of Section A.2.7).

We indicate now the local maxima of μA_n for $1 \leq n \leq 16$, which gives all extremal symplectic forms in $\mathfrak{H}_n$. In order to have the supplementary list of these maxima modulo $\Gamma_0(n+1)$ it is appropriate to add the symmetries $\sigma(z) = -\overline{z}$; we mention only the points with $\mathrm{Re}\,(z) > 0$ since the forms associated with z and $\sigma(z)$ have the same symplectic nature (Section A.2.2).

In Table A.2 one gives successively: n, the dimension of the parameter spaces P_{2n} and $\mathfrak{H}_n$, the points in $\mathbb{H}$ with the convention $z = x + iy = [x, y^2]$, the square of Hermite's constant μ of the lattice zA_n and a value approaching μ, the number of pairs of minimal vectors (vm), the rank of perfection in P_{2n} ("rg.u") and the rank of perfection in $\mathfrak{H}_n$ ("rg.s"). In the last column ("not.") one recalls the notations used in this article.

The ranks of perfection of a lattice $A \in \mathfrak{S}_n$ are determined starting from the ensemble $S(A)$ of its minimal vectors. The usual rank is equal to one less than the vector rank of the system $\{ss'; s \in S(A)\}$. For the symplectic rank, one can

Table A.1: Number of eutactic points in $\mathbb{H}A_n$ ($1 \leq n \leq 16$).

n	ind	(g,ν)	$\chi(\Gamma)$	e_2'	e_1'	e_0'
1	1	(0,1)	-1/6	1/3	1/2	0
2	4	(0,2)	-2/3	2	3	1/3
3	6	(0,3)	-1	4	5	0
4	6	(0,2)	-1	3	5	1
5	12	(0,4)	-2	6	9	1
6	8	(0,2)	-4/3	14/3	7	1
7	12	(0,4)	-2	6	9	1
8	12	(0,4)	-2	6	9	1
9	18	(0,4)	-3	8	12	1
10	12	(1,2)	-2	6	9	1
11	24	(0,6)	-4	10	15	1
12	14	(0,2)	-7/3	20/3	10	1
13	24	(1,4)	-4	10	15	1
14	24	(1,4)	-4	10	15	1
15	24	(0,6)	-4	10	15	1
16	18	(1,2)	-3	8	12	1

utilize the gradients in $\mathfrak{S}_n$ and (following [Bv, Section 3.4]) it is the affine rank of the system of matrices

$$\left\{ss' + JAss'AJ; s \in S(A)\right\} \tag{A.3.19}$$

with $J = \left(\begin{smallmatrix} 0 & I \\ -I & 0 \end{smallmatrix}\right)$; one can also write $A = \varphi_n(\tau)$ ($\tau \in \mathfrak{H}_n$) and work with the gradients (A.2.5) in $\mathfrak{H}_n$. From the point of view of doing calculations, the second solution is more advantageous because the dimension of $\mathfrak{H}_n$ is half of that of P_{2n}.

All these calculations can be reduced to operations on the rational numbers (see Remark A.2.8, Section A.2.7) and have been implemented with the PARI system.

The embedding (A.2.3) permits explicit Gram matrices for the lattices in Table A.2. One finds in particular rather simple matrices for D_4, $A_6^{(2)} \simeq J_K$ (Jacobian of the Klein quartic) and E_8 (compare with [B-S, Appendix 2]).

All of the lattices in this list, with the exception of $\frac{29+i\sqrt{167}}{84}A_5$, are of the type F_{2n}, G_{2n}, $H_{2n}(m)$ or J_{2n} (see Sects. 2.1, 2.2, 2.3 and 2.4). We can classify without difficulty the perfect points of $\mathbb{H}A_n$ for the following small values of n by utilizing Voronoï's algorithm (Corollary A.2.12 (2)). Another proof consists of verifying by aid of the formula (A.2.33) which are of the forms F, G, H or J. For example, for $9 \leq n \leq 16$ one finds (modulo the action of the symmetry σ) the forms F_{2n}, G_{2n}, $H_{2n}(3)$ ($9 \leq n \leq 16$), $H_{2n}(4)$ ($11 \leq n \leq 16$), J_{2n} ($n = 9, 11, 13, 15$), as well as $H_{22}(5)$ ($n = 11$), $H_{28}(5)$, $H_{28}(6)$ ($n = 14$) and $H_{30}(7)$ ($n = 15$). All these lattices are extremal symplectic and no two are isomorphic to one another. The $H_{2n}(m)$ cited here are always distinguished by the number of vectors with norm $\leq 2\mu$ and sometimes by Smith's constant (see Remark 2.4).

Remark A.3.5. The study of eutactic points of $\mathbb{H}A_2$ leads to two eutactic forms $(i/\sqrt{3})A_2$ and $(1/2 + i/\sqrt{12})A_2$ which are equivalent by $SL(4,\mathbb{Z})$, but are not so symplectically, *i.e.,* by $Sp(4,\mathbb{Z})$, because they differ by the rank of perfection symplectic (which are resp. 3 and 4). One has therefore a flat torus which carries two structures of distinct principally polarized abelian varieties.

The cases $n = 3$ and $n = 4$ are illustrated in Figure A.3 which describes the

Table A.2: Extremal symplectic points in $\mathbb{H}A_n$ $(1 \leq n \leq 8)$

$2n$	P_{2n}	$\mathfrak{H}_n$	z	μ^2	$\mu \simeq$	vm	rg.u	rg.s	rem.	not.
1	2	2	[1/2, 3/4]	4/3	1.1547	3	2	2	A_2	F_2
2	9	6	[1/3, 2/9]	2	1.4142	12	9	6	D_4	F_4
3	20	12	[3/8, 15/64]	36/15	1.5491	22	18	12		F_6
			[3/8, 7/64]	16/7	1.5118	21	20	12	J_K	G_6
4	35	20	[2/5, 6/25]	8/3	1.6329	35	30	20		F_8
			[2/5, 1/25]	4	2.0000	120	35	20	E_8	G_8
5	54	30	[5/12, 35/144]	20/7	1.6903	51	45	30		F_{10}
			[5/12, 11/144]	36/11	1.8090	55	54	30		G_{10}
			[29/84, 167/84^2]	576/167	1.8571	40	39	30		
6	77	42	[3/7, 12/49]	3	1.7320	70	63	42		F_{12}
			[3/7, 8/147]	25/6	2.0412	84	77	42		G_{12}
			[5/14, 3/196]	16/3	2.3094	378	77	42	K_{12}	$H_{12}(3)$
7	104	56	[7/16, 63/256]	28/9	1.7638	92	84	56		F_{14}
			[7/16, 15/256]	64/15	2.0655	147	104	56		G_{14}
			[5/14, 3/196]	16/3	2.3094	119	83	56		$H_{14}(3)$
			[5/18, 1/162]	9/2	2.1213	84	83	56		J_14
8	135	72	[4/9, 20/81]	16/5	1.7888	117	108	72		F_{16}
			[4/9, 5/81]	196/45	2.0870	144	135	72		G_{16}
			[5/14, 3/196]	16/3	2.3094	192	107	72		$H_{16}(3)$

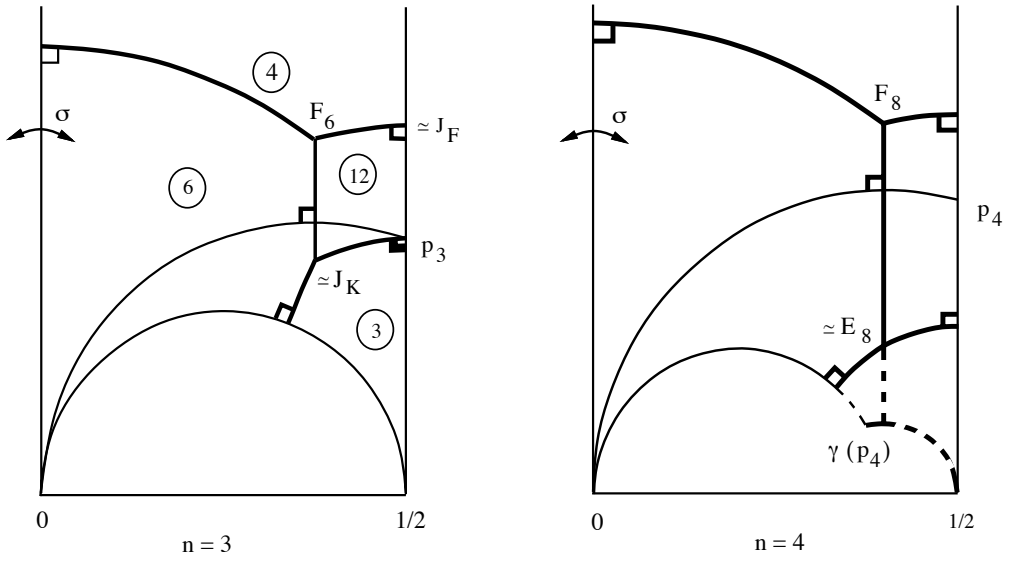

Figure A.3: The families $\mathbb{H}A_3$ and $\mathbb{H}A_4$.

global geometric situation. Only half of the fundamental domain is represented (the rest is defined by the symmetry σ). The identifications operated by $\Gamma_0(4)$ and $\Gamma_0(5)$ are clear. For $n = 3$, the group $\Gamma_0(4)$ is of index 6 with three points 0, ∞ and 1/2. There are four principal points: 0, ∞, 1/2 and $p_3 = (2 + i\sqrt{2})/4$, and therefore four regions of maximal dimension of which one is bounded (that of p_3). Each region comes with a principal length function (Section A.2.5) and a certain number of minimal vectors, namely 6, 4, 3 and 12 associated with 0, ∞, 1/2 and p_3, respectively (see Figure A.3). In this example, all minimizing length functions are principal. One obtains therefore the number of minimal vectors on the edges (which are always geodesic arcs in P_{2n} of isodual symplectic forms) and at the vertices of $\mathcal{DV}^M$ by adding the contributions of neighboring regions. For example the forms of the edge F_6J_K have eighteen minimal vectors. The principal points of F_6 are (0, ∞, p_3), and those of J_K are (p_3, 0, 1/2) (the same modulo $\Gamma_0(4)$, for $\sigma(F_6)$ and $\sigma(J_K)$). The point $(1 + i)/2$ is denoted J_F because $\frac{1+i}{2}A_3$ is isomorphic to the Jacobian of the Fermat quartic. The relation (A.2.33) here becomes $2(\pi - \theta) + 2\theta = 2\pi|\chi(\Gamma_0(4))|$ with $\cos\theta = 1/3$. Finally, one remarks that

p_3 is semi-eutactic (s.e.), and because of this fact the Euler formulas (A.2.32) and (A.2.36) for $\mathbb{H}A_3$ are distinct.

Let us quickly comment on the case $n = 4$. $\Gamma_0(5)$ is of index 6 with two points 0 and ∞, and two fixed points $(\pm 2 + i)/5$ which give an isomorphic lattice to E_8. One computes three principal points modulo $\Gamma_0(5)$ (0, ∞ and $p_4 = (1 + i\sqrt{3}/5)/2$) with 10, 5 and 20 associated minimal vectors, respectively. The point $(2 + i)/5$ is fixed by $\gamma = \left(\begin{smallmatrix} 2 & -1 \\ 5 & -2 \end{smallmatrix}\right)$ and its region (clearly fixed by γ) has vertices p_4, 0, $\gamma(p_4)$, 1/2. Furthermore, $(2 + i)/5$ *admits two minimizing but non-principal length functions* (this must be true since E_8 has 120 minimal vectors!) of which the gradients are in the convex hull of principal gradients.

A.3.6 An interesting hyperbolic family

A particularly rich example is obtained by $lh_8^{271} = [[4, 2, 1, -1, -1, -1, 1, 2]]$ (see (A.3.20)) which is one of 1171 perfect forms of dimension 8 found by Laïhem ([La]). It is rather special because its inverse has a large number of minimal vectors.

The family $\mathbb{H}\, lh_8^{271}$ is invariant for the group $\Gamma_0(21)$ of relatively small index 32 in $PSL(2, \mathbb{Z})$. However it contains only sixteen perfect points each of which give a perfect lattice in $\mathfrak{H}_8$:

$$\begin{aligned}
z_1 &= [2/7, 2/147] \text{ (of density } \mu^2 = 6), \\
z_2 &= [19/42, 31/42^2], \\
z_3 &= [25/84, 551/84^2], \\
z_4 &= [2/7, 1/245], \\
z_5 &= [1/3, 5/63]], \\
z_6 &= [43/252, 41/252^2], \\
z_7 &= [11/42, 47/42^2], \\
z_8 &= [17/42, 47/42^2], \\
z_9 &= [31/84, 47/84^2],
\end{aligned}$$

$$
\begin{aligned}
z_{10} &= [25/84, 47/84^2]], \\
z_{11} &= [3/7, 1/147], \\
z_{12} &= [5/14, 3/196], \\
z_{13} &= [1/4, 1/48], \\
z_{14} &= [25/147, 4/3(49)^2], \\
z_{15} &= [7/60, 17/7(60)^2], \\
z_{16} &= [88/567, 761/567^2].
\end{aligned}
$$

One recalls the convention $[x, u] = x + i\sqrt{u}$. Among these sixteen forms, twelve are perfect in P_{16} (of which eleven are extremal) and twelve are extremal in $\mathfrak{H}_8$. The family $\mathbb{H}\,lh_8^{271}$ presents many interesting phenomena: perfect points of which the Delaunay region is entirely contained in $\mathbb{H}$ (z_1 with five principal points, or z_{12}), semi-eutactic perfect points (z_5, z_{13}) and even weakly eutactic perfect points (z_6, z_{14}). Note that a perfect form of $\mathfrak{H}_n$ defined for a weakly eutactic point of a family $\mathbb{H}M$ can be only weakly eutactic in $\mathfrak{H}_n$.

A.3.7 Other examples

After A_n, the second classical set of lattices is D_n ($n \geq 4$). The associated families are a little disappointing because the group which acts is $\Gamma_0(2)$ or $\Gamma_0(4)$ according to the parity of n. One finds only one extremal lattice $\frac{1+i}{2}D_n$ isomorphic to D_{2n}^+ which is already extremal in P_{2n}. For $n = 4$ one finds E_8 again.

Here to finish is a list of examples of perfect symplectic lattices (Table A.3). From dimension 10 and onwards, we give only some examples chosen for their good density; there exist a large number of others (we have obtained 64 perfect points in $\mathfrak{H}_5$ and 230 perfect points in $\mathfrak{H}_6$).

Recall that the forms F_{2n}, G_{2n} and $H_{2n}(m)$ are defined from A_n for (A.3.1), (A.3.5) and (A.3.11). One notes that FG_{2n} is the eutactic form $n(1+i)/(2n+2)A_n$; FG_4 is isomorphic to the eutactic form of the class a_9 of [B-M2]. We also use Craig's difference lattices built starting from $A_n \simeq A_n^{(1)}$ (see for example [Ma]):

Table A.3: Some examples of perfect symplectic forms

$2n$	P_{2n}	M	z	μ^2	$\mu \simeq$	vm	rg.u	rg.s	rem.	not.
8	35	D_4	$[1/2, 1/4]$	4	2.0000	120	35	20	E_8	G_8
		M_4^a	$[2/21, 1/5(21)^2]$	16/5	1.7888	60	34	20	ex.	
		FG_4	$[7/18, 23/324]$	64/23	1.6681	33	28	20	ex.	
		A_4	$[2/5, 6/25]$	8/3	1.6329	35	30	20	ex.	F_8
		M_4^b	$[41/231, 1/6(231)^2]$	8/3	1.6329	29	26	20	w.e.	
		M_4^c	$[62/495, 2/3(165)^2]$	8/3	1.6329	27	26	20	w.e.	
10	54	M_5^a	$[9/25, 1/4(25)^2]$	4	2.0000	130	54	30	ex.	
		D_5	$[1/2, 1/4]$	4	2.0000	90	54	30	D_{10}	
		M_5^b	$[1/6, 1/108]$	100/27	1.9245	81	50	30	ex.	T_{10}^3
		M_5^c	$[21991/481200, 1919/481200^2]$	$82^2/1919$	1.8718	45	44	30	w.e.	
		M_5^d	$[1957/33(29)^2, 65/33^2 29^4]$	45/13	1.8605	46	40	30	w.e.	
12	77	A_6	$[5/14, 3/196]$	16/3	2.3094	378	77	42	K_{12}	$H_{12}(3)$
		M_6^a	$[19/56, 31/56^2]$	144/31	2.1552	172	75	42	ex.	
		M_6^b	$[1/3, 1/18]$	9/2	2.1213	192	75	42	ex.	
		M_6^c	$[60/451, 8/451^2]$	9/2	2.1213	180	77	42	ex.	
		M_6^d	$[14/153, 8/153^2]$	9/2	2.1213	135	71	42	ex.	
14	104	P_7^{30}	$[61/196, 3/196^2]$	16/3	2.3094	378	104	56	ex.	T_{14}^1
		M_7^a	$[1/2, 1/12]$	16/3	2.3094	189	104	56	ex.	
		A_7	$[5/14, 3/196]$	16/3	2.3094	119	83	56	ex.	$H_{12}(3)$
		M_7^b	$[77/848, 7/848^2]$	36/7	2.2677	280	104	56	ex.	
		M_7^c	$[157/4110, 11/4110^2]$	225/44	2.2613	140	97	56	w.e.	
16	135	$A_8^{(2)}$	$[5/27, 2/729]$	8	2.8284	2160	135	72	Λ_{16}	
		lh_8^{179}	$[5/21, 1/5(21)^2]$	36/5	2.6832	1200	135	72	ex.	T_{16}^2
		M_8	$[5/24, 23/576]$	144/23	2.5021	456	129	72	ex.	
18	170	M_9^a	$[3/10, 13/300]$	256/39	2.5620	480	170	90		
		M_9^b	$[11/40, 39/40^2]$	256/39	2.5620	315	170	90		
		M_9^c	$[11/40, 39/40^2]$	256/39	2.5620	189	146	90		
20	209	$A_{10}^{(2)}$	$[9/22, 7/484]$	64/7	3.0237	3080	209	110	ex.	
		T_{10}^3	$[5/27, 2/729]$	8	2.8284	1980	209	110	ex.	
		M_{10}^a	$[1/3, 1/18]$	8	2.8284	1500	209	110		
		M_{10}^b	$[1/3, 1/18]$	8	2.8284	1020	209	110		
		T_{10}^3	$[2/9, 1/162]$	8	2.8284	765	209	110	ex.	
22	252	M_{11}^a	$[9/41, 1/41^2]$	9	3.0000	1232	252	132		
		M_{11}^b	$[11/27, 1/2(27)^2]$	8	2.8284	891	252	132		
24	299	$A_{12}^{(2)}$	$[5/13, 1/169]$	16	4.0000	98280	299	156	Λ_{24}	
		M_{12}	$[3/14, 1/588]$	256/27	3.0792	2187	296	156		
26	350	M_{13}^a	$[5/14, 3/196]$	12	3.4641	10920	350	182		
		M_{13}^b	$[1/3, 1/45]$	45/4	3.3541	1716	350	182		
28	405	T_{14}^1	$[4/9, 11/81]$	144/11	3.6181	9492	405	210		
		M_{14}	$[2/5, 1/25]$	100/9	3.3333	6048	405	210		
30	464	M_{15}^a	$[3/10, 1/100]$	49/4	3.5000	6720	464	240		
		M_{15}^b	$[5/12, 19/288]$	441/38	3.4066	1245	464	240		
32	527	Λ_{16}	$[1/2, 1/4]$	16	4.0000	73440	527	272		
		T_{16}^2	$[9/20, 39/400]$	192/13	3.8430	22800	527	272		

if $(e_j)_{0\leq j\leq n}$ is the canonical basis for $\mathbb{R}^{n+1}$, one notes that $A_n^{(k)}$ $(1 \leq k \leq n)$ is the Gram matrix of n vectors $u_i = \sum_{0\leq j\leq k}(-1)^j \binom{k}{j} e_{i+j}$ $(1 \leq i \leq n)$ of $\mathbb{R}^{n+1}$ (the indices are to be taken modulo $n+1$). In the last column "not." we identify the lattices of type F, G or H and we introduce some lattices T_{2n}^k useful for the higher dimensions. The other basic used matrices are defined below.

For small dimensions, we specify in the column "rem." the symplectic nature of the forms (ex. = extremal, s.e. = semi-eutactic and w.e. = weakly eutactic). The tests of eutaxy were carried out in MAPLE. For large dimensions, in order to reduce the number of vectors to be considered, we replaced all the gradients which have the same projection on $\mathbb{H}M$ with their sum, which allowed us to conclude the eutaxy in certain cases. The calculation is even simpler when one can apply Proposition A.2.6, such as for example, for $A_{p-1}^{(k)}$ with p prime (see in [Ma] p.138 the proof of Proposition 4.6).

To conclude, we mention the following question, suggested by the results of our study.

Question. Let p be a prime number and let $A_{p-1}^{(k)}(1 \leq k \leq p-1)$ be the Craig difference lattices. Up to $p = 11$, one notes that a relatively perfect point of the family $\mathbb{H}A_{p-1}^{(k)}$ is always perfect in $\mathfrak{H}_{p-1}$. Is this true for all p?

The list below (where we write "perf." for perfect) supplements the data in Table A.3, with the notation

$$[[a_1, \ldots, a_n]] = (a_{|i-j|+1})_{1\leq i,j\leq n}. \tag{A.3.20}$$

$M_4^a = [[4, 2, 1, 1]]$,
$M_4^b = [[14, 11, 8, 8]]$,
$M_4^c = [[6, 1, 1, 1]]$,
$M_5^a = [[4, 2, 1, 1, 2]]$,
$M_5^b = [[5, 2, -1, -1, -1]]$ (one of 136 eutactic quintic forms classified in [Bt]),
$M_5^c = [[10, 4, 1, 1, 4]]$,
$M_5^d = [[7, 1, 1, 1, 1]]$,

$M_6^a = [[8, 3, 4, 6, 4, 3]]$,

$M_6^b = [[4, 1, 0, 1, -2, -2]]$,

$M_6^c = [[4, 0, -1, 0, 3, 1]]$,

$M_6^d = [[12, 1, 6, -2, 9, 1]]$,

$P_7^{30} = [[4, 1, 2, 2, 2, 2, 1]]$ (perf., see [Ja]),

$M_7^a = [[3, 2, 1, 1, 1, 0, 0]]$,

$M_7^b = [[6, 3, 0, -1, 1, 1, -1]]$,

$M_7^c = [[9, 1, 1, 1, 1, 1, 1]]$,

$lh_8^{179} = [[6, 2, -2, -3, -1, -1, 0, 2]]$ (perf., see [The]),

$M_8 = [[6, 3, 1, 0, -3, -3, -2, -3]]$,

$M_9^a = [[5, 3, 2, 2, 0, 0, 1, 0, 0]]$,

$M_9^b = [[4, 2, 1, 0, 1, 0, 0, 0, 1]]$ (perf.),

$M_9^c = [[4, 1, 0, 2, 2, 1, 0, 1, 2]]$,

$M_{10}^a = [[4, 1, 0, -2, -1, 1, 1, 1, -1, -2]]$,

$M_{10}^b = [[4, 1, -1, -2, 0, 1, 2, 1, -2, -2]]$,

$M_{11}^a = [[4, 1, 0, 0, 0, 0, -2, -1, -2, -2, 1]]$,

$M_{11}^b = [[4, 1, 0, -1, -2, -2, 0, 0, 0, 2, 2]]$ (perf.),

$M_{12} = [[3, 1, -1, -1, 0, 1, 0, -1, 0, 1, 0, -1]]$,

$M_{13}^a = [[3, 1, -1, -1, 0, 1, 0, -1, 0, 1, 0, -1, -1]]$,

$M_{13}^b = [[4, -2, 0, 1, -1, 1, 0, 0, -1, 1, -1, 0, 2]]$ (perf.),

$M_{14} = [[4, 1, -1, 1, 1, -1, 0, 2, 1, 0, 0, 0, 0, -1]]$,

$M_{15}^a = [[4, 2, 1, 0, 1, 1, 1, 1, 0, -1, -2, -1, 0, 0, -1]]$,

$M_{15}^b = [[4, -2, 2, -1, 0, 1, -1, 1, -2, 1, -2, 2, -2, 1, -1]]$.

References

[As] Ash A. On eutatic forms. *Canad. J. Math.* **29**, 5 (1977), 1040–1054

[Bt] Batut C. Classification of quintic eutactic forms. *Math. Comp.* **70**, 233 (2001), 395–417

[Bv] Bavard C. Systole et invariant d'Hermite. *J. Reine Angew. Math.* **482** (1997), 93–120

[B-M1] Bergé A.-M., Martinet J. Densité dans de familles de réseaux. Application aux réseaux isoduaux. *Enseign. Math.* **41** (1995), 335–365

[B-M2] Bergé A.-M., Martinet J. Sur la classification des réseaux eutactiques. *J. London Math. Soc.* (2) **53** (1996), 417–432

[B-S] Buser P., Sarnak P. On the period matrix of a Riemann surface of large genus (with an appendix by J. H. Conway and N. J. A. Sloane). *Invent. Math.* **117** (1994), 27–56

[C-S] Conway J. H., Sloane N. J. A. Sphere packings, lattices and groups, 3rd ed. Springer-Verlag, NewYork, 1999

[Eb] Eberlein P. Structure of manifolds of nonpositive curvature. In Global differential geometry and global analysis 1984 (Berlin, 1984). Springer, Berlin, 1985, 86–153. Springer L. N., Vol. 1156

[Ja] Jaquet-Chiffelle D. -O. Énumération complète des classes de formes parfaites en dimension 7. *Ann. Inst. Forrier* (Grenoble) **43**, 1 (1993), 21–55

[La] Laïhem M. Construction algorithmique de réseaux parfaits. Thèse, Université Bordeaux I, Dec. 1992

[Ma] Martinet J. Les réseaux parfaits des espaces euclidiens. Masson, Paris, 1996

[Mu] Mumford D. Curves and their jacobians. The University of Michigan Press, Ann Arbor, 1975

[Sc] Schmutz P. Riemann surfaces with shortest geodesic of maximal length. *Geom. Funct. Anal.* **3**, 6 (1993), 564–631

[Sh] Shimura G. Introduction to the arithmetic theory of automorphic functions, vol. **11** of Publications of the Mathematical Society of Japan. The Mathematical Society of Japan, 1971

Bibliography

[1] Dorit Aharonov and Michael Ben-Or. Fault-tolerant quantum computation with constant error rate. 1999, quant-ph/9906129.

[2] Charlene Ahn and John Preskill. Cost of quantum fault-tolerance. In preparation, 2004.

[3] Miklos Ajtai. The shortest vector problem in L_2 is NP-hard for randomized reductions. *Proceedings of the 30th Annual ACM Symposium on Theory of Computing*, pages 10–19, May 1998.

[4] Mark Alford, Kai-Ming Lee, John March-Russell, and John Preskill. Quantum field theory of nonabelian strings and vortices. *Nuclear Physics B*, 384:251–317, 1992, hep-th/9112038.

[5] Francisco Barahona. On the computational complexity of Ising spin-glass models. *Journal of Physics A*, 15:3241–3253, 1982.

[6] Francisco Barahona, R. Maynard, R. Rammal, and J. P. Uhry. Morphology of ground states of a two-dimensional frustration model. *Journal of Physics A*, 15:673–699, 1982.

[7] Howard Barnum, Michael Nielsen, and Benjamin Schumacher. Information transmission through a noisy quantum channel. *Physical Review A*, 57:4153–4175, 1998, quant-ph/9702049.

[8] Christophe Bavard. Familles hyperboliques de réseaux symplectiques. *Mathematische Annalen*, 320(4):799–833, 2001.

[9] Dave Beckman, December 2000. Private communication.

[10] Charles Bennett and Giles Brassard. Quantum cryptography: Public key distribution and coin tossing. *Proceedings of IEEE International Conference on Computers Systems and Signal Processing*, pages 175–179, December 1984, www.research.ibm.com/people/b/bennetc/bennettc198469790513.pdf.

[11] Charles Bennett, David DiVincenzo, and John Smolin. Capacities of quantum erasure channels. *Physical Review Letters*, 78:3217–3220, 1997, quant-ph/9701015.

[12] Charles Bennett, David DiVincenzo, John Smolin, and William Wootters. Mixed state entanglement and quantum error correction. *Physical Review A*, 54:3824–3851, 1996, quant-ph/9604024.

[13] Anne-Marie Bergé. Symplectic lattices. *Contemporary Mathematics*, 272:9–22, 2000, www.math.u-bordeaux.fr/∼berge/symplectic.ps.

[14] Elwyn Berlekamp, John Conway, and Richard Guy. *Winning Ways for Your Mathematical Plays*. Academic Press, London, 1982.

[15] Piotr Berman and Janos Simon. Investigations of fault-tolerant networks of computers. *Proceedings of the 20th Annual ACM Symposium on the Theory of Computing*, pages 66–77, 1988.

[16] Samuel Braunstein. Error correction for continuous quantum variables. *Physical Review Letters*, 80:4084–4087, 1998, quant-ph/9711049.

[17] Peter Buser and Peter Sarnak. On the period matrix of a Riemann surface of large genus. *Inventiones mathematicae*, 117:27–56, 1994.

[18] Rob Calderbank, Eric Rains, Peter Shor, and Neil Sloane. Quantum error correction and orthogonal geometry. *Physical Review Letters*, 78:405, 1997, quant-ph/9605005.

[19] Rob Calderbank and Peter Shor. Good quantum error-correcting codes exist. *Physical Review A*, 54:1098–1105, 1996, quant-ph/9512032.

[20] John W. S. Cassels. *An introduction to the geometry of numbers*. Springer-Verlag, New York, 1971.

[21] John Conway and Neil Sloane. *Sphere Packing, Lattices and Groups*. Springer-Verlag, New York, 3 edition, 1998.

[22] Thomas Cover and Joy Thomas. *Elements of Information Theory*. Wiley, New York, 1991.

[23] Rudi de Buda. The upper error bound of a new near-optimal code. *IEEE Transactions in Information Theory*, IT-21:441–445, 1975.

[24] Rudi de Buda. Some optimal codes have structure. *IEEE Journal on Selected Areas in Communications*, 7(6):893–899, 1989.

[25] Philippe de Forcrand, Massimo D'Elia, and Michele Pepe. A study of the 't Hooft loop in SU(2) Yang-Mills theory. *Physical Review Letters*, 86:1438–1441, 2001, hep-lat/0007034.

[26] Eric Dennis, Alexei Kitaev, Andrew Landahl, and John Preskill. Topological quantum memory. *Journal of Mathematical Physics*, 43:4452–4505, 2002, quant-ph/0110143.

[27] David DiVincenzo, Peter Shor, and John Smolin. Quantum channel capacity of very noisy channels. *Physical Review A*, 57:830–839, 1998, quant-ph/9706061.

[28] Pierre Le Doussal and Brooks Harris. Location of the Ising spin-glass multicritical point on Nishimori's line. *Physical Review Letters*, 61:625–628, 1988.

[29] Jack Edmonds. Paths, trees and flowers. *Canadian Journal of Mathematics*, 17:449–467, 1965.

[30] Richard Feynman. Simulating physics with computers. *International Journal of Theoretical Physics*, 21:467–488, 1982.

[31] Peter Gács. Reliable computation with cellular automata. *Journal of Computer and System Sciences*, 32(1):15–78, 1986.

[32] Peter Gács. Self-correcting two-dimensional arrays. *Advances in Computing Research*, 5:223–326, 1989.

[33] Peter Gács. Reliable cellular automata with self-organization. *Journal of Statistical Physics*, 103(1/2):45–267, 2001, math.PR/0003117.

[34] Peter Gács and John Reif. A simple three-dimensional real-time reliable cellular array. *Journal of Computer and System Sciences*, 36(2):125–147, April 1988.

[35] Daniel Gottesman. A class of quantum error-correcting codes saturating the quantum Hamming bound. *Physical Review A*, 54:1862, 1996, quant-ph/9604038.

[36] Daniel Gottesman. Stabilizer codes and quantum error correction. Caltech Ph.D. Thesis, 1997, quant-ph/9705052.

[37] Daniel Gottesman. Fault-tolerant quantum computation with local gates. *Journal of Modern Optics*, 47:333–345, 2000, quant-ph/9903099.

[38] Daniel Gottesman, Alexei Kitaev, and John Preskill. Encoding a qubit in an oscillator. *Physical Review A*, 64:012310, 2001, quant-ph/0008040.

[39] Lawrence Gray. A reader's guide to Gács's "Positive Rates" paper. *Journal of Statistical Physics*, 103(1/2):1–44, 2001.

[40] Jim Harrington and John Preskill. Achievable rates for the Gaussian quantum channel. *Physical Review A*, 64:062301, 2001, quant-ph/0105058.

[41] Alexander Holevo and Reinhard Werner. Evaluating capacities of bosonic Gaussian channels. *Physical Review A*, 63:032312, 2001, quant-ph/9912067.

[42] Andreas Honecker, Marco Picco, and Pierre Pujol. Universality class of the Nishimori point in the 2D $\pm J$ random-bond Ising model. *Physical Review Letters*, 87:047201, 2001, cond-mat/00010143.

[43] Tsuyoshi Horiguchi and Tohru Morita. Existence of the ferromagnetic phase in a random-bond Ising model on the square lattice. *Journal of Physics A*, 15:L75–L80, 1982.

[44] Naoki Kawashima and Heiko Rieger. Finite size scaling analysis of exact ground states for $\pm J$ spin glass models in two dimensions. *Europhysics Letters*, 39:85–90, 1997, cond-mat/9612116.

[45] Richard Kaye. Infinite versions of minesweeper are Turing complete. 2000, http://web.mat.bham.ac.uk/R.W.Kaye/minesw/infmsw.pdf.

[46] Richard Kaye. Minesweeper is NP-complete. *Mathematical Intelligencer*, 22(2):9–15, 2000, web.mat.bham.ac.uk/R.W.Kaye/minesw/ordmsw.htm.

[47] Alexei Kitaev. Quantum error correction with imperfect gates. *Proceedings of the Third International Conference on Quantum Communication and Measurement*, 1997.

[48] Alexei Kitaev. Fault-tolerant quantum computation by anyons. *Annals of Physics*, 303:2–30, 2003, quant-ph/9707021.

[49] Hidetsugu Kitatani. The verticality of the ferromagnetic-spin glass phase boundary of the $\pm J$ Ising model in the p-t plane. *Journal of the Physical Society of Japan*, 61:4049–4055, 1992.

[50] Greg Kuperberg, January 2004. Private communication.

[51] Hendrik Lenstra, Arjen Lenstra, and László Lovász. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261:515–534, 1982.

[52] Thomas Liggett. *Interacting particle systems*. Springer-Verlag, New York, 1985.

[53] Tamás Linder, Christian Schlegel, and Kenneth Zeger. Corrected proof of de Buda's theorem. *IEEE Transactions in Information Theory*, 39:1735–1737, 1993.

[54] Seth Lloyd. Universal quantum simulators. *Science*, 273:1073–1078, 1996.

[55] Seth Lloyd. The capacity of the noisy quantum channel. *Physical Review A*, 55:1613–1622, 1997, quant-ph/9604015.

[56] Seth Lloyd and Jean-Jacques Slotine. Analog quantum error correction. *Physical Review Letters*, 80:4088–4091, 1998, quant-ph/9711021.

[57] Genaro Martínez, Harold McIntosh, and Juan Mora. Production of gliders by collisions in Rule 110. *Advances in Artificial Life*, 2801:175–182, 2003.

[58] Florian Merz and John Chalker. Two-dimensional random-bond Ising model, free fermions, and the network model. *Physical Review B*, 65:054425, 2002, cond-mat/0106023.

[59] Marc Mézard, Giorgio Parisi, and Miguel Virasoro. *Spin Glass Theory and Beyond*. World Scientific, Singapore, 1987.

[60] Daniele Micciancio. The shortest vector in a lattice is hard to approximate to within some constant. *IEEE Symposium on Foundations of Computer Science*, pages 92–98, 1998, theory.lcs.mit.edu/∼miccianc/papers/svp.ps.

[61] Hermann Minkowski. Über Geometrie der Zahlen. *Gesammelte Abhandlungen*, 1:264–265, 270, 277, 1911.

[62] Michael Nielsen and Isaac Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, 2000.

[63] Hidetoshi Nishimori. Internal energy, specific heat, and correlation function of the bond-random Ising model. *Progress of Theoretical Physics*, 66:1169–1181, 1981.

[64] Hidetoshi Nishimori. Geometry-induced phase transition in the $\pm J$ Ising model. *Journal of the Physical Society of Japan*, 55:3305–3307, 1986.

[65] Hidetoshi Nishimori. *Statistical Physics of Spin Glasses and Information Processing*. Oxford University Press, Oxford, 2001.

[66] Hidetoshi Nishimori. Derivatives and inequalities for order parameters in the Ising spin glass. *Journal of Phyiscs A: Mathematical and General*, 35:9541–9548, 2002, cond-mat/0206438.

[67] Hidetoshi Nishimori and Koji Nemoto. Duality and multicritical point of two-dimensional spin glasses. *Journal of the Physical Society of Japan*, 71:1198–1199, 2002, cond-mat/0111354.

[68] Fernando Nobre. Phase diagram of the two-dimensional $\pm J$ Ising spin glass. *Physical Review E*, 64:046108, 2001.

[69] Harold Ollivier and Jean-Pierre Tillich. Description of a quantum convolutional code. *Physical Review Letters*, 91:177902, 2003, quant-ph/0304189.

[70] Harold Ollivier and Jean-Pierre Tillich. Quantum convolutional codes: fundamentals. 2004, quant-ph/0401134.

[71] William Poundstone. *The Recursive Universe : Cosmic Complexity and the Limits of Scientific Knowledge*. Contemporary Books, Chicago, 1985.

[72] John Preskill. *Lecture Notes for Physics 229: Quantum Information and Computation*. 1998, www.theory.caltech.edu/people/preskill/ph229.

[73] Eric Rains, November 2000. Private communication.

[74] Benjamin Schumacher and Michael Nielsen. Quantum data processing and error correction. *Physical Review A*, 54:2629–2635, 1996, quant-ph/9604022.

[75] Claude Shannon. A mathematical theory of communication. *Bell System Technical Journal*, 27:379–423, 623–656, 1948.

[76] Peter Shor. Scheme for reducing decoherence in quantum computer memory. *Physical Review A*, 52:2493–2496, 1995.

[77] Peter Shor. Fault-tolerant quantum computation. *Proceedings of the 37th Annual Symposium on Foundations of Computer Science*, pages 56–65, 1996, quant-ph/9605011.

[78] Peter Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, 1997, quant-ph/9508027.

[79] Peter Shor and John Preskill. Simple proof of security of the BB84 quantum key distribution protocol. *Physical Review Letters*, 85:441–444, 2000, quant-ph/0003004.

[80] Andrew Steane. Error-correcting codes in quantum theory. *Physical Review Letters*, 77:793–797, 1996.

[81] Andrew Steane. Multiple particle interference and quantum error correction. *Proceedings: Mathematical, Physical and Engineering Sciences*, 452(1954):2551–2577, 1996, quant-ph/9601029.

[82] Andrei Toom. Stable and attractive trajectories in multicomponent systems. *Advances in Probability*, 6:549–575, 1980.

[83] Rüdiger Urbanke and Bixio Rimoldi. Lattice codes can achieve capacity on the AWGN channel. *IEEE Transactions in Information Theory*, 44:273–278, 1998.

[84] Chenyang Wang, Jim Harrington, and John Preskill. Confinement-Higgs transition in a disordered gauge theory and the accuracy threshold for quantum memory. *Annals of Physics*, 303:31–58, 2003, quant-ph/0207088.

[85] Peter Young. *Spin Glasses and Random Fields*. World Scientific, Singapore, 1997.

Index