# Absolutely Irreducible Curves with Applications to Combinatorics and Coding Theory

Thesis by

Gary M. McGuire

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

California Institute of Technology
Pasadena, California
1995

(Submitted May 16, 1995)

# Acknowledgements

I sincerely thank my adviser Richard M. Wilson for his guidance and encouragement and his constant willingness to spend many long hours explaining mathematics to me. It is a pleasure to listen to his insights, which have been a major influence. I can safely say I learned more about mathematics from him than any other person.

Special thanks go to Robert Calderbank for his generous encouragement and advice, and for his invitation to spend the summer of 1994 at Bell Labs where I learned much from him.

I thank the members of the combinatorics seminar at Caltech who have all contributed to my combinatorial education. I also thank the members of the Caltech mathematics department and my graduate student colleagues for many enjoyable discussions, both mathematical and otherwise.

I am grateful to all of you for teaching me what it means to be a mathematician.

Thanks to the Caltech mathematics department, the Bohnenblust fund, and AT&T Bell Labs for financial support.

# Abstract

We investigate some problems in algebraic coding theory and finite geometry by relating them to polynomials in two variables and applying Weil's theorem. We prove absolute irreducibility of polynomials arising in this way using Bezout's theorem.

In Chapter 2 we investigate certain cyclic codes, and we show that there are codewords of a certain weight by proving that some polynomials are absolutely irreducible and applying Weil's theorem.

In Chapter 3 we investigate the existence of hyperovals which have the form $\{(1, x, f(x))\}$ in finite projective planes of even order, and we show that there must be three collinear points by proving that some polynomials are absolutely irreducible and applying Weil's theorem.

In Chapter 4 we discuss Galois rings of order $4^m$. We construct a relative difference set from these, and hence an affine plane, which we prove is Desarguesian. We also construct binary codes from the Galois rings, and we prove that there are codewords of a certain weight in the natural generalization of the Preparata and Goethals codes by proving that some polynomials are absolutely irreducible and applying Weil's theorem.

# Contents

# CHAPTER 0

## Introduction and Summary

In this thesis we will study how the existence of certain objects in combinatorial structures can be related to solutions of a system of polynomial equations in several variables. A form of the Weil bound due to W. Schmidt [SC] on the number of rational points on curves over finite fields shows that one can weaken the hypothesis of nonsingularity of a curve $f(x,y)$ over $F_q$ to absolute irreducibility, and still obtain a bound essentially the same as that of Weil. We show that some questions in (1) algebraic coding theory and (2) finite geometry can be answered by finding absolutely irreducible factors of certain polynomials and utilising the bound. We also develop various methods for establishing the absolute irreducibility of polynomials in two variables over finite fields using techniques from algebra and classical algebraic geometry.

In Chapter 2 we consider binary cyclic codes which are generated by a polynomial of the same degree as that which generates the 2-error-correcting BCH code of length $n = 2^s - 1$, which has minimum distance 5 for all $n$. The codes we study are indexed by an odd integer $t$, the 2-error-correcting BCH codes $C_s^{(3)}$ being the case $t = 3$. We prove that the other codes $C_s^{(t)}$ are different:

**Theorem 2.1.** *For fixed $t \equiv 3 \pmod 4$, $t > 3$, the codes $C_s^{(t)}$ of length $n = 2^s - 1$ have minimum distance at most 4 for all but finitely many values of $s$.*

The proof involves relating codewords of weight 4 to solutions of a polynomial equation $g_t(x, y, z) = 0$. We use algebraic geometry, in particular Bezout's theorem, to show that $g_t(x, y, z)$ is absolutely irreducible.

We also consider values of $t \equiv 1 \pmod 4$, where the analysis is much more complicated. It becomes harder to show that $g_t(x, y, z)$ is absolutely irreducible, partly due to that fact that there are infinitely many exceptions.

Theorem 2.1 is due to the author of this thesis. It and the results in section 2.4 up to and including Theorem 7 will appear in a paper to be published in the Journal of Algebra and co-authored with H. Janwa and R. M. Wilson. The results from Theorem 8 onward do not appear in that paper and are solely due to this author.

In Chapter 3 we consider hyperovals of the form $\{(1, x, x^k)\}$ (as $x$ runs through $GF(q)$, plus two more points) in the finite projective plane $PG(2, q)$ where $q$ is even. We show that such a hyperoval exists provided a polynomial equation $g_k(x, y, z) = 0$ has no solutions over $GF(q)$. However, we show:

**Theorem 3.1.** *For any fixed $k \equiv 2$ (mod 4), $k > 6$, the set $D(k)$ is a hyperoval in $PG(2, q)$ for at most a finite number of values of $q$.*

The proof involves showing that the polynomials $g_k(x, y, z)$ are absolutely irreducible, which involves analysis of the singular points and resolving those singularities.

We also consider values of $k \equiv 0$ (mod 4), where things are more complicated. There are infinitely many exceptions, namely when $k$ is a power of 2, and we conjecture that these are the only exceptions.

Most of our results, including Theorem 3.1, were also obtained by Segre and Segre-Bartocci much earlier. We did not know about the Segre-Bartocci paper at the time these results were found. Segre and Bartocci's methods differ slightly from ours.

In Chapter 4 we introduce Galois rings $GR(4^m)$, which have recently become of great interest to coding theorists. We give a complete, brief introduction to the subject. These rings have become of interest because they give simple constructions of excellent binary codes, for example the Preparata codes.

From a proof that the Preparata codes have minimum distance 6, we construct a relative difference set in a Galois ring. From this relative difference set we construct an affine plane. We prove that this affine plane is Desarguesian.

We investigate the most obvious generalizations of the Preparata and the Goethals codes. One such family of codes consists of all vectors in $(\mathbf{Z}_4)^{2^m}$ which are orthogonal to every row of the matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 & \cdots & 1 \\ 0 & 1 & \xi & \xi^2 & \cdots & \xi^i & \cdots & \xi^{2^m-2} \\ 0 & 1 & \xi^3 & \xi^6 & \cdots & \xi^{3i} & \cdots & \xi^{3(2^m-2)} \\ 0 & 2 & 2\xi^5 & 2\xi^{10} & \cdots & 2\xi^{5i} & \cdots & 2\xi^{5(2^m-2)} \end{pmatrix}$$

where $\xi$ is a primitive $(2^m-1)$ root of unity in the Galois ring $GR(4^m)$.

Codewords of a certain weight in this generalization $C$ are related to the solutions of a certain polynomial equation $h(x,y)=0$. We prove that $h(x,y)$ is absolutely irreducible, which enables us to determine the exact minimum distance of these codes for $m \geq 9$. In fact,

**Theorem 4.4.** *The code $C$ has minimum Lee weight 8 for all values of $m$, except when $m=5$, in which case the minimum Lee weight is 12.*

The $m=5$ case is the best known $(64, 2^{37})$ code, the previously best known has distance 10. This code also has more codewords than any known binary code of length 64 and distance 12. It appears in a paper co-authored with A. R. Calderbank [CMG2], and the proof that the distance is 12 is given in that paper and is not given in this thesis.

We obtain similar results (Corollary 4.5 and Theorem 4.6) for other families of such codes, which are the $\mathbf{Z}_4$ analogues of the 2- and 3-error-correcting binary BCH codes.

Some of these coding theory results in this chapter will appear in a paper co-authored with A. R. Calderbank, P. V. Kumar, T. Helleseth [CMGKH]. Theorem 4.3, Corollary 4.5 and Theorem 4.6 are part of this author's contribution to that paper.

# CHAPTER 1

# Preliminaries

In this chapter we give some definitions and results which will be used in each of the following chapters.

Let $h(x,y)$ be a polynomial that is defined over a field $k$, and let $P = (\alpha, \beta)$ where $\alpha, \beta \in \overline{k}$, the algebraic closure of $k$. Write

$$h(x+\alpha, y+\beta) = H_0(x,y) + H_1(x,y) + H_2(x,y) + \cdots$$

where each $H_i(x,y)$ is 0 or homogeneous of degree $i$. If $m$ is the smallest integer such that $H_m \neq 0$ but $H_i = 0$ for $i < m$, then $m$ is called the *multiplicity of $h$ at $P$*, and is denoted by $m_P(h)$. In particular, $P$ is on the curve associated to $h$ if and only if $m_P(h) \geq 1$. Also, by definition, $P$ is a singular point of $h$ if and only if $m_P(h) \geq 2$. The $m$ linear factors of $H_m$, with $x$ replaced by $x - \alpha$ and $y$ replaced by $y - \beta$, are the tangent lines to $h(x, y)$ at $P$.

If $P = (\alpha, \beta)$ is a singular point of $h$, then the equations

$$h(\alpha,\beta) = 0, \quad \frac{\partial h}{\partial x}(\alpha,\beta) = 0, \quad \frac{\partial h}{\partial y}(\alpha,\beta) = 0$$

are simultaneously satisfied. However, to include points at infinity we should consider the projective homogeneous version of $h(x, y)$, which we denote by $h(x, y, z)$. Then all singular points of $h(x, y, z)$ are found by simultaneously solving

$$h(x,y,z) = 0, \quad \frac{\partial h}{\partial x}(x,y,z) = 0, \quad \frac{\partial h}{\partial y}(x,y,z) = 0, \quad \frac{\partial h}{\partial z}(x,y,z) = 0.$$

Now let $u$ and $v$ be projective plane curves over $k$, and assume that $u$ and $v$ have no common component. The *intersection multiplicity* $I(P, u, v)$ of $u$ and $v$ at $P$ is the unique nonnegative integer satisfying and determined by the seven properties listed on pages 74–75 of Fulton [F]. For our purposes, there are two important properties. The first is that $I(P, u, v) \neq 0$ if and only if both $m_P(u)$ and $m_P(v)$ are nonzero. The second important property is that $I(P, u, v) \geq m_P(u) \cdot m_P(v)$, with equality occurring if and only if $u$ and $v$ do not have a common tangent at $P$.

We will use the following theorem from classical algebraic geometry, whose proof can be found in Fulton [F].

**Bezout's Theorem.** *Let $u$ and $v$ be projective plane curves of degrees $m$ and $n$ respectively having no components in common. Then*

$$\sum_P I(P, u, v) = m \cdot n,$$

*where the sum is extended over all points $P = (\alpha, \beta)$ and $\alpha, \beta \in \overline{k}$.*

We will use Bezout's theorem to prove that certain polynomials $h(x, y, z)$, which arise from combinatorial problems, are absolutely irreducible, i.e., irreducible over the algebraic closure of $GF(2)$. Our most common method of proving the absolute irreducibility of $h(x, y, z)$ will be to assume that it is reducible, say $h(x, y, z) = u(x, y, z) \cdot v(x, y, z)$, and obtain a contradiction by applying Bezout's theorem to the curves $u$ and $v$. Of course, $h(x, y, z)$ is absolutely irreducible if and only if $h(x, y)$ is absolutely irreducible.

The reason the absolute irreducibility of $h(x, y)$ is useful is that we can then apply the following theorem of Weil, which guarantees us zeroes of $h(x, y)$ with distinct coordinates over all $GF(2^m)$, except for possibly a finite number of values of $m$.

Here we give the following stronger statement of Weil's theorem, proved in [FJ, p.51].

**Theorem.** *Let $f(x, y)$ be an absolutely irreducible polynomial of degree $d$ with coefficients in $GF(q)$ and let $\Gamma$ be the affine curve defined by the equation*

*$f(x,y)=0$. Then*

$$q+1-(d-1)(d-2)\sqrt{q}-d \leq |\Gamma(GF(q))| \leq q+1+(d-1)(d-2)\sqrt{q},$$

*where $\Gamma(GF(q))$ denotes the number of rational points $(x,y)$ over $GF(q)$ on $\Gamma$.*

We will use this theorem to guarantee us the required zeroes of $h(x,y,z)$. The existence of such zeroes will be related to the combinatorial problems under consideration. In chapters 2 and 4 the existence of zeroes of a polynomial $h(x,y,z)$ will be related (in different ways) to the existence of codewords of a certain weight in some codes. In chapter 3 the existence of zeroes will be related to the existence of hyperovals in finite projective planes of even order.

The following two Propositions will be used frequently in the sequel.

**Proposition A.** *Let $h(x,y)$ be an affine curve. Write $h(x+\alpha,y+\beta)=H_m+H_{m+1}+\cdots$ where $P=(\alpha,\beta)$ is a point on $h(x,y)$ of multiplicity $m$. Suppose that $H_m$ and $H_{m+1}$ are relatively prime, and that there is only one tangent direction at $P$. If $h=uv$ is reducible, then $I(P,u,v)=0$.*

*Proof:* Since $h=uv$ we have

$$h(x+\alpha,y+\beta)=u(x+\alpha,y+\beta)v(x+\alpha,y+\beta)$$

$$H_m+H_{m+1}+\cdots=(U_a+U_{a+1}+\cdots)(V_b+V_{b+1}+\cdots).$$

If $a = 0$ or $b = 0$ ( i.e. $P \notin u$ or $P \notin v$) then we are done, so assume $a, b \geq 1$. We claim that $U_a$ and $V_b$ are relatively prime: for if $t(x, y)$ is a nonconstant polynomial that divides both of them, since $H_m = U_a V_b$ and $H_{m+1} = U_a V_{b+1} + U_{a+1} V_b$ we would have that $t(x, y)$ divides $H_m$ and $H_{m+1}$, a contradiction. But also $U_a V_b = H_m = (cx + dy)^m$ for some constants $c$ and $d$. Therefore either $U_a$ or $V_b$ is constant, and $I(P, u, v) = 0$. □

We now present some other results in a different direction, which can also be used in irreducibility arguments. Bezout's theorem is useful when dealing with the algebraic closure because it lives there. One might also reduce the problem to a finite number of extensions of $GF(q)$, and eliminate possible factorizations over these extensions. We will use the next proposition, which is a well known Frobenius automorphism argument.

**Proposition B.** *Let $h(x, y)$ be an affine curve of degree $n$ defined over $GF(q)$. For parts 2 and 3 assume $h(x, y)$ is irreducible over $GF(q)$.*

1) *If $P = (\alpha, \beta)$ is a point on $h$ of multiplicity 1 (a nonsingular point) with coordinates $\alpha, \beta \in GF(q^r)$, then $h$ has an absolutely irreducible factor over $GF(q^r)$.*

2) *If $P = (\alpha, \beta)$ is a point on $h$ of multiplicity $m$ with coordinates $\alpha, \beta \in GF(q^r)$, then $h$ has an absolutely irreducible factor over $GF(q^{rm})$.*

3) *If $h$ has an absolutely irreducible factor defined over $GF(q^r)$ (and no subfield), then $r$ divides $n$.*

*Proof:* The first assertion follows from the second. To prove the second assertion, let $h_1(x, y)$ be an absolutely irreducible factor of $h(x, y)$ with $m_P(h_1) \geq 1$. We may suppose that the coefficients of $h_1$ lie in some extension of $GF(q^r)$, say $GF(q^{rt})$, and no intermediate subfield. We show that $t$ divides $m$.

If $\sigma$ is the Frobenius automorphism of $GF(q^{rt})$ fixing $GF(q^r)$, then the $t$ distinct conjugates of $h_1$ under $\sigma$ will contain $P$ with the same multiplicity. Since the product of the conjugates is $h$, there are at most $m$ distinct conjugates, and in fact the number of distinct conjugates is $m/m_P(h_1) = t$.

For part 3, there are $r$ distinct conjugates, their product is $h$, and so each must have degree $n/r$. □

We remark that if $m = 2$ in part 2, then the hypothesis of irreducibility can be dropped, as in part 1 where $m = 1$.

# CHAPTER 2

# Double-Error-Correcting Cyclic Codes and Absolutely Irreducible Polynomials over $GF(2)$

## 2.1 Introduction.

A binary cyclic code $C$ of odd length $n$ may be thought of as the set of all polynomials $p(x)$ over $GF(2)$ of degree $< n$ so that $p(\zeta) = 0$ for all $\zeta$ in some given set $S$ of $n$-th roots of unity in some extension of $GF(2)$. The minimum distance of $C$ is the least number of terms (monomials) that appear in any of these polynomials $p(x)$. To say a code is $e$-error-correcting means that the minimum distance is $\geq 2e+1$. Elements of $C$ are called codewords. The least common multiple $g(x)$ of the minimal polynomials over $GF(2)$ of members of $S$ is a divisor of $x^n - 1$ called the generator polynomial for $C$.

A fundamental problem in coding theory is to determine or bound the minimum distance of a cyclic code given its root set $S$ or given its generator polynomial. We will consider codes of length $n = 2^s - 1$ for positive integers $s$. It is well known and easy to see that the code with root set $S$ consisting of a single element $\zeta$ has minimum distance 3 if $\zeta$ is a primitive $n$-th root of unity and 2 otherwise; the former are called cyclic Hamming codes and the latter are of little interest.

Let $\omega$ be a primitive element in the finite field $GF(2^s)$ and let $C_s^{(t)}$ be the binary cyclic code of length $n = 2^s - 1$ consisting of all binary polynomials $p(x)$ so that $p(\omega) = p(\omega^t) = 0$. That is, $C_s^{(t)}$ is the cyclic code whose generating polynomial is the product $m_1(x)m_t(x)$ where $m_i(x)$ denotes the minimal polynomial of $\omega^i$ over $GF(2)$ (assuming $m_1(x) \neq m_t(x)$). We will assume that $t$ is odd. The degree of $m_1(x)m_t(x)$ is $\leq 2s$ and is 'usually' equal to $2s$, for example when $s$ is large with respect to $t$, so when we think of $t$ as fixed and consider the sequence $C_s^{(t)}$, these codes have dimension $n - 2s$, i.e., they contain $2^{n-2s}$ codewords, with a finite number of exceptions. Our main result here is the following theorem.

**Theorem 2.1.** *For fixed $t \equiv 3 \pmod 4$, $t > 3$, the codes $C_s^{(t)}$ of length $n = 2^s - 1$ have codewords of weight 4 for all but finitely many values of $s$.*

When $t = 3$, the codes $C_s^{(3)}$ have minimum distance $\geq 5$ and are the classical 2-error-correcting BCH codes. For a fixed $t > 3$, the codes $C_s^{(t)}$ will never again have distance 5 for *all* values of $s$. We can, however, still ask for distance 5 for infinitely many values of $s$, e.g. for all $s$ odd. Such values of $t$ do exist; $t = 5$ has been known for a long time. In contrast, when $t = 7$ the codes $C_s^{(7)}$ have distance $< 5$ once $s$ is larger than 17, see [VLW1]. For $t = 2^i + 1$, the codes $C_s^{(t)}$ have been shown to have minimum distance $\geq 5$ when $(i, s) = 1$, and these codes play a role in the construction of generalized Preparata codes [BVLW]. It was noticed in [VLW2] that for $t = 2^{2i} - 2^i + 1$ the codes $C_s^{(t)}$ also have minimum distance $\geq 5$ when $s$ is odd and $(i, s) = 1$; in [JW] the condition that $s$ be odd was shown to be unnecessary. It is not hard to see [VLW2] that the minimum distance of $C_s^{(t)}$ cannot exceed 5 when $s \geq 3$.

It would be interesting if there were other values of $t$ for which infinitely many of the codes $C_s^{(t)}$ are 2-error-correcting, but we think this is not the case.

It is easy to relate codewords of weights 3 and 4 in $C_s^{(t)}$ to the zeros $(\alpha, \beta, \gamma)$ over $GF(2^s)$ of the polynomial

$$f_t(X, Y, Z) = X^t + Y^t + Z^t + (X + Y + Z)^t$$

over $GF(2)$. The code $C_s^{(t)}$ has codewords of weight 4 if and only if there exist distinct nonnegative integers $i, j, k, \ell < n$ so that $\omega$ and $\omega^t$ are roots of $p(x) = x^i + x^j + x^k + x^\ell = 0$. If we write $\alpha = \omega^i$, $\beta = \omega^j$, $\gamma = \omega^k$,

$\delta = \omega^\ell$, this is equivalent to the existence of four distinct nonzero elements $\alpha, \beta, \gamma, \delta \in GF(2^s)$ so that

$$\begin{aligned} \alpha + \beta + \gamma + \delta &= 0, \\ \alpha^t + \beta^t + \gamma^t + \delta^t &= 0. \end{aligned}$$

A codeword of weight 3 is equivalent to four distinct elements $\alpha, \beta, \gamma, \delta \in GF(2^s)$, one of which is zero, satisfying the above system of equations. In summary, there are codewords of weight 3 or 4 in $C_s^{(t)}$ if and only if $f_t(\alpha, \beta, \gamma) = 0$ for some distinct $\alpha, \beta, \gamma, \in GF(2^s)$.

We are only interested in points on $f_t(X, Y, Z)$ with distinct coordinates and as $f_t(X, Y, Z)$ is clearly divisible by $(X+Y)(X+Z)(Y+Z)$, we consider the polynomial

$$g_t(X, Y, Z) = \frac{X^t + Y^t + Z^t + (X+Y+Z)^t}{(X+Y)(X+Z)(Y+Z)}.$$

It is shown in [JW] by an application of Weil's theorem that if $g_t(X, Y, Z)$ is absolutely irreducible, i.e., irreducible over the algebraic closure of $GF(2)$, then $g_t(X, Y, Z)$ has zeros $(\alpha, \beta, \gamma)$ with distinct coordinates except for a finite number of values of $s$.

Factorizations of $g_t(X, Y, Z)$ for $t = 2^i + 1$ and $t = 2^{2i} - 2^i + 1$ were described in [JW] where it was also shown that $g_t(X, Y, Z)$ was absolutely irreducible for infinitely many values of $t$. For example, it was shown that $g_t(X, Y, Z)$ is nonsingular, and hence absolutely irreducible, whenever $t = 2p + 1$ where $p \equiv \pm 3 \pmod 8$ is a prime. Here we prove that $g_t(X, Y, Z)$ is absolutely irreducible for all $t > 3$ with $t \equiv 3 \pmod 4$, as well as for infinitely many values of $t \equiv 1 \pmod 4$. These cases give us ample evidence to make the following conjecture.

**Conjecture 1.** *The polynomial $g_t(X, Y, Z)$ is absolutely irreducible for all $t$ not of the form $2^i + 1$ or $2^{2i} - 2^i + 1$.*

As we have pointed out, by Weil's theorem Conjecture 1 implies the following.

**Conjecture 2.** *For fixed odd $t \geq 3$, $t \neq 2^i + 1$ or $2^{2i} - 2^i + 1$, the codes $C_s^{(t)}$ of length $n = 2^s - 1$ have codewords of weight 4 for all but finitely many values of $s$. In particular, these codes would have minimum distance at most 4.*

### 2.2 Singularity Analysis of the Polynomials.

It will be more convenient to work with the affine parts of the homogeneous polynomials $f_t$ and $g_t$. We use the same names:

$$\begin{aligned} f_t(X,Y) &= X^t + Y^t + 1 + (X+Y+1)^t, \\ g_t(X,Y) &= \frac{X^t + Y^t + 1 + (X+Y+1)^t}{(X+1)(Y+1)(X+Y)}, \end{aligned}$$

and we consider the algebraic curves defined by these polynomials over the algebraic closure of $GF(2)$.

Write $t = 2^i\ell + 1$ where $\ell$ is odd and $i \geq 1$. Let $\lambda = \alpha + \beta + 1$. Over a field of characteristic 2,

$$(x+a)^t = (x+a)(x^{2^i}+a^{2^i})^\ell = a^t + a^{t-1}x + a^{t-2^i}x^{2^i} + a^{t-2^i-1}x^{2^i+1} + \cdots$$

where the dots indicate terms of higher degree in $x$. So we have

$$f_t(X+\alpha, Y+\beta) = F_0 + F_1(X,Y) + F_{2^i}(X,Y) + F_{2^i+1}(X,Y) + \cdots$$

where

$$\begin{aligned} F_0 &= f_t(\alpha,\beta) = \alpha^t + \beta^t + 1 + \lambda^t, \\ F_1(X,Y) &= (\alpha^{t-1}+\lambda^{t-1})X + (\beta^{t-1}+\lambda^{t-1})Y, \\ F_{2^i}(X,Y) &= (\alpha^{t-2^i}+\lambda^{t-2^i})X^{2^i} + (\beta^{t-2^i}+\lambda^{t-2^i})Y^{2^i}, \qquad (*) \\ F_{2^i+1}(X,Y) &= (\alpha^{t-2^i-1}+\lambda^{t-2^i-1})X^{2^i+1} + (\beta^{t-2^i-1}+\lambda^{t-2^i-1})Y^{2^i+1} \\ &\quad + \lambda^{t-2^i-1}(X^{2^i}Y + XY^{2^i}). \end{aligned}$$

From [JW], or directly from the above with a few simple computations, $P = (\alpha,\beta)$ is a singular point of $f_t(X,Y)$ if and only if $\alpha$, $\beta$, and $\lambda = \alpha+\beta+1$ are $\ell$-th roots of unity. The multiplicity $m_P(f_t)$ of such a singular point is either $2^i$ or $2^i+1$ since $\lambda \neq 0$ implies $F_{2^i+1} \neq 0$.

If $g_t = uv$ and a point $P$ has $I(P,u,v) \neq 0$, then $m_P(g_t) = m_P(u) + m_P(v) \geq 2$, and so $P$ is a singular point of $g_t(X,Y,Z)$. It is straightforward to check that the projective curves $g_t(X,Y,Z)$ have no singular points at infinity. Therefore, since the only points $P$ that give a nonzero contribution to the sum in Bezout's theorem are singular points of $g_t(X,Y,Z)$, we may just work with the affine part of $g_t(X,Y,Z)$.

Suppose that $P = (\alpha, \beta) \neq (1,1)$ is a singular point of $g_t(X,Y)$. Furthermore, in the expansion of $f_t(X+\alpha, Y+\beta)$, suppose that $F_{2^i}(X,Y) \neq 0$ at $P$. To apply Proposition A to $g_t$ we need to know the greatest common divisor of $(G_m(X,Y)$ and $G_{m+1}(X,Y))$, where $m = m_P(g_t)$. This can be found from $(F_{2^i}(X,Y), F_{2^i+1}(X,Y))$ as follows.

Letting $w(X,Y) = (X+Y)(X+1)(Y+1)$, we have

$$f_t(X+\alpha, Y+\beta) = w(X+\alpha, Y+\beta) \cdot g_t(X+\alpha, Y+\beta),$$

so

$$F_{2^i}(X,Y) + F_{2^i+1}(X,Y) + \cdots = (W_0 + W_1(X,Y) + \cdots)(G_m(X,Y) \\ + G_{m+1}(X,Y) + \cdots)$$

where polynomials with subscript $i$ are 0 or homogeneous of degree $i$.

**Remark 1.** Suppose that $W_0 \neq 0$, which is equivalent to assuming that $m = 2^i$. Multiplying out and using $(*)$ gives

$$F_{2^i} = W_0 G_{2^i} = (\sigma X + \tau Y)^{2^i},$$

$$F_{2^i+1} = W_0 G_{2^i+1} + W_1 G_{2^i},$$

where $\sigma^{2^i} = \alpha^{1-2^i} + \lambda^{1-2^i}$ and $\tau^{2^i} = \beta^{1-2^i} + \lambda^{1-2^i}$. It follows from these equations that $(F_{2^i}, F_{2^i+1}) = (G_{2^i}, G_{2^i+1})$. □

**Remark 2.** Suppose that $W_0 = 0$, which is equivalent to $m = 2^i - 1$. As in Remark 1 we get

$$F_{2^i} = W_1 G_{2^i-1} = (\sigma X + \tau Y)^{2^i},$$

$$F_{2^i+1} = W_1 G_{2^i} + W_2 G_{2^i-1}.$$

It is clear that (up to scalars) $W_1 = \sigma X + \tau Y$, and so $(F_{2^i}, F_{2^i+1}) = \sigma X + \tau Y$ by Lemma 3 (see next section). Hence $(G_{2^i-1}, G_{2^i}) = 1$. □

For the record we record that $W_0 = (\alpha+1)(\beta+1)(\alpha+\beta)$ and $W_1 = (1+\beta)^2 X + (1+\alpha)^2 Y$.

### 2.3 The Case $t \equiv 3 \pmod 4$.

The following theorem is equivalent to Theorem 2.1, as stated in section 2.1, by the remarks made there.

**Theorem 2.1′.** *If $t \equiv 3 \pmod 4$, $t > 3$, then $g_t(X,Y)$ is absolutely irreducible.*

*Proof:* Let $t = 2\ell + 1$, $\ell$ odd, be given. Suppose $g_t(X,Y) = u(X,Y) \cdot v(X,Y)$ over some extension of $GF(2)$ with the degrees of $u$ and $v$ both $\geq 1$. Let $P = (\alpha, \beta)$ be a singular point of $g_t(X,Y)$ and hence of $f_t(X,Y)$. From $(*)$ and using the notation there,

$$F_2(X,Y) = (\alpha^{-1} + \lambda^{-1})X^2 + (\beta^{-1} + \lambda^{-1})Y^2,$$

$$F_3(X,Y) = (\alpha^{-2} + \lambda^{-2})X^3 + (\beta^{-2} + \lambda^{-2})Y^3 + \lambda^{-2}(X^2Y + XY^2).$$

The point $P = (1,1)$ has multiplicity 3 on $f_t$, but also has multiplicity 3 on $w(X,Y) = (X+1)(Y+1)(X+Y)$, and so is not on $g_t$. Thus $F_2(X,Y) \neq 0$, so $m_P(f_t) = 2$.

From Remarks 1 and 2 above, it suffices to show that $(F_2, F_3) = 1$ at every $P$. Once we know this, applying Proposition A and Bezout's theorem to $u$ and $v$ completes the proof.

Suppose that $F_2(X,Y) = (\sigma X + \tau Y)^2$ and $F_3(X,Y)$ are not relatively prime. It is then clear that $F_3(X,Y)$ is divisible by $\sigma X + \tau Y$, so $F_3(\tau, \sigma) = 0$. But this leads to a contradiction:

$$F_3(X,Y) = \sigma^4 X^3 + \tau^4 Y^3 + \lambda^{-2}(X^2 Y + Y^2 X),$$

$$0 = F_3(\tau, \sigma) = \sigma^4 \tau^3 + \tau^4 \sigma^3 + \lambda^{-2}\sigma\tau(\sigma + \tau),$$

$$0 = \sigma^2\tau^2 + \lambda^{-2} = (\alpha^{-1} + \lambda^{-1})(\beta^{-1} + \lambda^{-1}) + \lambda^{-2},$$

$$0 = \alpha + \beta + \lambda = 1,$$

where the last equation is obtained from the preceding one by multiplication by $\alpha\beta\lambda$. □

### 2.4 The Case $t \equiv 1 \pmod 4$.

The situation when $t \equiv 1 \pmod 4$ is complicated by the fact that there are the interesting exceptions stated in section 2.1. Another complication is that there are many more singular points. We present some partial results towards our conjectures here. Throughout this section, $t = 2^i\ell + 1$, $\ell > 1$ is odd, and $P = (\alpha, \beta)$ is a point on $f_t$. We carry over the same notation from section 2.2.

First we gather some facts about the homogeneous polynomials $F_{2^i}(X,Y)$ and $F_{2^i+1}(X,Y)$ as in $(*)$.

**Lemma 3.** *$F_{2^i+1}(X,Y)$ has distinct linear factors.*

*Proof:* For the proof let $F(X) = F_{2^i+1}(X,1)$. By differentiating, we get

$$F'(X) = (\alpha^{-2^i} + \lambda^{-2^i})X^{2^i} + \lambda^{-2^i} = (cX + d)^{2^i},$$

where $c = \alpha^{-1} + \lambda^{-1}$ and $d = \lambda^{-1}$. Assume $\beta \neq 1$ so that $c \neq 0$. Then $F$ has distinct roots if and only if $d/c = \alpha/(1+\beta)$ is not a root of $F$. It turns out that $F(d/c) = 0$ implies that $\lambda = 0$, a contradiction. If $\beta = 1$ then $\alpha \neq 1$ and reverse the roles of $X$ and $Y$. □

Referring to the properties of $I(P,u,v)$, we note that if $F_{2^i}(X,Y) = 0$ at $P$, Lemma 3 implies that $I(P,u,v) = m_P(u)m_P(v)$, i.e., equality occurs.

**Lemma 4.** *Suppose $P = (\alpha,\alpha)$ is a singular point on $g_t(X,Y)$ where $\alpha \notin GF(2^i)$. If $g_t = uv$, then $I(P,u,v) = 0$.*

*Proof:* It is clear from $(*)$ that $X+Y$ divides $F_{2^i}(X,Y)$ and $F_{2^i+1}(X,Y)$. But then by Remark 2, $(G_{2^i-1}, G_{2^i}) = 1$. By Proposition A, if $g_t = uv$ then $I(P,u,v) = 0$. □

**Lemma 5.** *Suppose that exactly one of the coefficients in $F_{2^i}(X,Y)$ is 0. If $g_t = uv$, then $I(P,u,v) = 0$.*

*Proof:* Recall from $(*)$ that

$$F_{2^i}(X,Y) = (\alpha^{1-2^i} + \lambda^{1-2^i})X^{2^i} + (\beta^{1-2^i} + \lambda^{1-2^i})Y^{2^i},$$

$$F_{2^i+1}(X,Y) = (\alpha^{-2^i} + \lambda^{-2^i})X^{2^i+1} + \lambda^{-2^i}X^{2^i}Y + \lambda^{-2^i}XY^{2^i} \\ + (\beta^{-2^i} + \lambda^{-2^i})Y^{2^i+1}.$$

Suppose the coefficient of $Y^{2^i}$ is 0, the same argument works in the other case. We now distinguish two cases: first, if $\beta^{-2^i} + \lambda^{-2^i} \neq 0$ then clearly $(F_{2^i}, F_{2^i+1}) = 1$. It follows that $(G_{2^i}, G_{2^i+1}) = 1$ (by Remark 1) and Proposition A implies that $I(P, u, v) = 0$.

Next suppose that $\beta^{-2^i} + \lambda^{-2^i} = 0$, which means that $\beta = \lambda$ and $\alpha = 1$. It is clear that $(F_{2^i}, F_{2^i+1}) = X$, which implies $(G_{2^i-1}, G_{2^i}) = 1$ (by Remark 2) and again Proposition A implies that $I(P, u, v) = 0$. □

The *maximal cyclic code* $B_\ell$ of odd length $\ell$ consists of all binary polynomials $p(x)$ of degree $< \ell$ so that $p(\zeta_\ell) = 0$ where $\zeta_\ell$ is some fixed primitive $\ell$-th root of unity in an extension of $GF(2)$. In [JW], it was shown that singular points $P = (\alpha, \beta)$ for $f_t$ where $\alpha, \beta, 1$ are distinct exist if and only if $B_\ell$ has codewords of weight 4. For many values of $\ell$ it is possible to see that $B_\ell$ has no codewords of weight 4, for example, if $\ell$ is a prime congruent to ±3 modulo 8, and more generally if either $-1$ or 3 is congruent to a power of 2 modulo $\ell$. For more infinite classes, see [JW].

**Theorem 6.** *Suppose that $t \equiv 5 \pmod 8$, $t > 13$, and that the maximal cyclic code $B_\ell$ has no codewords of weight 4. Then $g_t(X, Y)$ is absolutely irreducible.*

*Proof:* By the remark above there are no singular points $P = (\alpha, \beta)$ where

$\alpha, \beta, 1$ are distinct. Suppose $g_t = uv$. Write $t = 4\ell + 1$ where $\ell > 3$ is odd. If $P = (\alpha, \alpha)$ is a singular point where $\alpha \notin GF(4)$, then $I(P, u, v) = 0$ by Lemma 4. If $P = (\alpha, 1)$ or $(1, \alpha)$ and $\alpha \notin GF(4)$, then $I(P, u, v) = 0$ by Lemma 5. Hence the only singular points $P$ which could possibly have $I(P, u, v) \neq 0$ are $(\alpha, \alpha)$ or $(\alpha, 1)$ or $(1, \alpha)$ where $\alpha^3 = 1$ in all cases. Also, $m_P(f_t) = 5$ in all cases.

If $\alpha \neq 1$, we have $m_P(g_t) = 5 - 1 = 4$, and then using Lemma 3, $I(P, u, v) = m_P(u) m_P(v) \leq 4$. If $\alpha = 1$, $m_P(g_t) = 5 - 3 = 2$ and so $I(P, u, v) \leq 1$.

Combining all this and applying Bezout's theorem gives (deg $u$)(deg $v$) $\leq 6 \cdot 4 + 1 = 25$. If $\ell = 5$, then $t = 21$ and this case was proved in [JW]. So we may assume that $\ell \geq 9$ and $t \geq 37$, which implies deg $u$ + deg $v \geq 34$ which is impossible. □

The values of $t \equiv 1 \pmod 4$ and less than 100 satisfying the hypotheses of Theorem 6 are 21,37,45,53,69,77,93. We mention that if $t \equiv 5 \pmod 8$ then $P = (1, 1)$ is a singular point of multiplicity 2. Applying Proposition B shows that $g_t(X, Y)$ has an absolutely irreducible factor over $GF(4)$.

**Theorem 7.** *Suppose that the maximal cyclic code $B_\ell$ has no codewords of weight 4, and that $GF(2^i)$ does not contain a nontrivial $\ell$-th root of unity, i.e. $(\ell, 2^i - 1) = 1$. Then $g_t(X, Y)$ is absolutely irreducible.*

*Proof:* By the remark before Theorem 6, there are no singular points $P = (\alpha, \beta)$ where $\alpha, \beta, 1$ are distinct. Recall that the coordinates of a singular point must be $\ell$-th roots of unity, and as before suppose that $g_t = uv$. If $P = (\alpha, \alpha)$ is a singular point where $\alpha \notin GF(2^i)$, then $I(P, u, v) = 0$ by Lemma 4. If $P = (\alpha, 1)$ or $(1, \alpha)$ and $\alpha \notin GF(2^i)$, then $I(P, u, v) = 0$ by Lemma 5. Since $GF(2^i)$ does not contain any nontrivial $\ell$-th roots of unity, we see that the only possible point with a nonzero intersection multiplicity is $P = (1, 1)$. Now we have

$$(\deg u)(\deg v) = I(P, u, v) = m_P(u) m_P(v),$$

where the first equality is by Bezout's theorem, the second by Lemma 3. It follows that $\deg u = m_P(u)$ and $\deg v = m_P(v)$, but then

$$2^i - 2 = m_P(u) + m_P(v) = \deg u + \deg v = 2^i \ell - 2,$$

which is impossible. □

The values of $t \equiv 1 \pmod 4$ and less than 100 satisfying the hypotheses of Theorem 7 are 21, 25, 41, 45, 53, 69, 73, 77, 89, 93, 97.

Here is an infinite family where $B_\ell$ does have codewords of weight 4.

**Theorem 8.** *If* $t = 2^i(2^{i+1} - 1) + 1$ *then* $g_t(X, Y, Z)$ *is absolutely irreducible.*

*Proof:* Recall that the coordinates of a singular point must be $\ell$-th roots of unity, and as before suppose that $g_t = uv$. If $P = (\alpha, \alpha)$ is a singular point where $\alpha \notin GF(2^i)$, then $I(P,u,v) = 0$ by Lemma 4. If $P = (\alpha, 1)$ or $(1, \alpha)$ and $\alpha \notin GF(2^i)$, then $I(P,u,v) = 0$ by Lemma 5.

If $P = (\alpha, \beta)$ is a singular point, then $\alpha, \beta \in GF(2^{i+1})$. Since $GF(2^i) \cap GF(2^{i+1}) = GF(2)$, it is clear that if $\alpha$ and $\beta$ are in $GF(2^i)$, then the only possible point with a nonzero intersection multiplicity is $Q = (1,1)$. If $\alpha \in GF(2^i)$, $\beta \notin GF(2^i)$, then $\alpha = 1$. Hence by Lemma 5, $I(P,u,v) = 0$. Similarly if $\beta \in GF(2^i)$, $\alpha \notin GF(2^i)$.

The remaining case is where $\alpha, \beta \notin GF(2^i)$ and $\alpha \neq \beta$. We now show that $I(P,u,v) = 0$ for these $P$.

Suppose that $F_{2^i}(X,Y) = (\sigma X + \tau Y)^{2^i}$ and $F_{2^i+1}(X,Y)$ are not relatively prime. It is then clear that $F_{2^i+1}(X,Y)$ is divisible by $\sigma X + \tau Y$, so $F_{2^i+1}(\tau, \sigma) = 0$. Note that $\sigma^{2^i} = \alpha^{1-2^i} + \lambda^{1-2^i} = \alpha^{2^i} + \lambda^{2^i}$, and hence $\sigma = \alpha + \lambda = 1 + \beta$. Similarly $\tau = 1 + \alpha$. But this leads to a contradiction:

$$F_{2^i+1}(X,Y) = (\alpha^{-2^i} + \lambda^{-2^i})X^{2^i+1} + \lambda^{-2^i}X^{2^i}Y + \lambda^{-2^i}XY^{2^i} + (\beta^{-2^i} + \lambda^{-2^i})Y^{2^i+1}$$

and as we have said,

$$0 = F_{2^i+1}(\tau,\sigma) = (\alpha^{-2^i} + \lambda^{-2^i})(1+\alpha)^{2^i+1} + \lambda^{-2^i}(1+\alpha)^{2^i}(1+\beta) + \lambda^{-2^i}(1+\alpha)(1+\beta)^{2^i} + (\beta^{-2^i} + \lambda^{-2^i})(1+\beta)^{2^i+1}.$$

Multiply this by $\lambda^{2^i}$ and noting that $\lambda^{2^i}\alpha^{-2^i} + 1 = \left(\frac{1+\beta}{\alpha}\right)^{2^i}$ we get

$$0 = \left(\frac{1+\beta}{\alpha}\right)^{2^i}(1+\alpha)^{2^i+1} + (1+\alpha)^{2^i}(1+\beta) + (1+\alpha)(1+\beta)^{2^i} + \left(\frac{1+\alpha}{\beta}\right)^{2^i}(1+\beta)^{2^i+1}.$$

Now divide by $(1+\alpha)(1+\beta)$ and simplify:

$$\begin{aligned}0 =&\alpha^{-2^i}(1+\beta)^{2^i-1}(1+\alpha)^{2^i}+(1+\alpha)^{2^i-1}+(1+\beta)^{2^i-1}\\ &+\beta^{-2^i}(1+\alpha)^{2^i-1}(1+\beta)^{2^i}\\ =&(1+\beta)^{2^i-1}\left(\alpha^{-2^i}(1+\alpha)^{2^i}+1\right)+(1+\alpha)^{2^i-1}\left(\beta^{-2^i}(1+\beta)^{2^i}+1\right)\\ =&(1+\beta)^{2^i-1}\alpha^{-2^i}+(1+\alpha)^{2^i-1}\beta^{-2^i}.\end{aligned}$$

Hence

$$\begin{aligned}\alpha^{2^i}(1+\alpha)^{2^i-1}&=\beta^{2^i}(1+\beta)^{2^i-1}\\ \frac{\alpha^{2^i}}{(1+\alpha)^{2^i}}&=\frac{\beta^{2^i}}{(1+\beta)^{2^i}}\\ \frac{\alpha}{\alpha+1}&=\frac{\beta}{\beta+1}\\ \alpha&=\beta\end{aligned}$$

which is a contradiction.

The upshot of all the above is that

$$(\text{deg } u)(\text{deg } v)=I(Q,u,v)=m_Q(u)m_Q(v),$$

where the first equality is by Bezout's theorem, the second by Lemma 3. It follows that deg $u=m_Q(u)$ and deg $v=m_Q(v)$, but then

$$2^i-2=m_Q(u)+m_Q(v)=\text{deg } u+\text{deg } v=2^i(2^{i+1}-1)-2,$$

which is impossible. □

The first four values of $t$ in this infinite sequence are 7, 29, 121, 497.

## 2.5 Some More Values of $t$.

The values of $t < 100$ not covered by the above theorems are $t = 49, 61, 81, 85$. We have used other methods including Hensel's Lemma implemented on a computer to prove that $g_t(X, Y)$ is absolute irreducible for all $3 < t < 100$, except when $t = 5, 9, 13, 17, 33, 57, 65$ where it is not true!

Before we analyze some specific values of $t$, let us make a remark.

**Remark 3.** Let $t = 2^i\ell + 1$. Let $P = (\alpha, \beta)$ be a singular point such that $\alpha$ and $\beta$ are not both elements of $GF(2^i)$. In this case we have

$$F_{2^i}(X,Y) = (\alpha^{1-2^i} + \lambda^{1-2^i})X^{2^i} + (\beta^{1-2^i} + \lambda^{1-2^i})Y^{2^i},$$

and

$$\begin{aligned} F_{2^i+1}(X,Y) = (\alpha^{-2^i} + \lambda^{-2^i})X^{2^i+1} + \lambda^{-2^i}X^{2^i}Y \\ + \lambda^{-2^i}XY^{2^i} + (\beta^{-2^i} + \lambda^{-2^i})Y^{2^i+1}. \end{aligned}$$

Note that $F_{2^i} = 0 \iff$ both $\alpha, \beta \in GF(2^i)$, in which case both $\alpha$ and $\beta$ are in $GF(2^i)$. So $F_{2^i} \neq 0$. If one coefficient of $F_{2^i}$ is 0, see Lemma 5.

Assume now that both coefficients of $F_{2^i}$ are nonzero. We can rewrite $F_{2^i}$ as

$$F_{2^i}(X,Y) = (\sigma X + \tau Y)^{2^i}$$

where $\sigma^{2^i} = \alpha^{1-2^i} + \lambda^{1-2^i}$ and $\tau^{2^i} = \beta^{1-2^i} + \lambda^{1-2^i}$. By Lemma 3, the GCD of $F_{2^i}$ and $F_{2^i+1}$ is either $\sigma X + \tau Y$ or 1. Also, as $\alpha, \beta \neq 1$ it follows from Remark

1 that $(F_{2^i}, F_{2^i+1}) = (G_{2^i}, G_{2^i+1})$. So if the GCD is 1, then Proposition A implies that $I(P, u, v) = 0$.

Suppose that $F_{2^i}(X, Y)$ and $F_{2^i+1}(X, Y)$ are not relatively prime, and that neither $\alpha$ or $\beta$ is in $GF(2^i)$. Setting $Y = 1$, this is equivalent to saying that $a = \tau/\sigma$ (the only root of $F_{2^i}(X, 1)$) is a root of $F_{2^i+1}(X, 1)$. Combining the two equations and simplifying gives

$$a = \frac{\alpha^{2^i} + \alpha}{\beta^{2^i} + \beta}. \tag{2.1}$$

This does not lead to a contradiction in general. We can show that (2.1) gives a contradiction in the following special cases.

If $\alpha \in GF(2^i)$, $\beta \notin GF(2^i)$, the simplification above reduces to $a = \alpha/(1+\beta)$. But as in the proof of Lemma 3, $F_{2^i+1}(a) \neq 0$, and so $I(P, u, v) = 0$ in this case. Similarly if $\beta \in GF(2^i)$, $\alpha \notin GF(2^i)$, then $a = (1 + \alpha)/\beta$ and $F_{2^i+1}(a) = 0$ implies that $\lambda = 0$, a contradiction. So $I(P, u, v) = 0$ here too.

Finally, in case $\alpha, \beta \notin GF(2^i)$ but $\lambda \in GF(2^i)$, then we can write

$$a = \frac{\alpha^{2^i} + \alpha + \lambda^{2^i} + \lambda}{\beta^{2^i} + \beta} = 1.$$

But $F_{2^i+1}(1) = 0 \Rightarrow \alpha^{-2^i} = \beta^{-2^i} \Rightarrow \alpha = \beta$, a contradiction. Hence $I(P, u, v) = 0$ in this case. □

We will now do these four values of $t$ (namely 49,61,81,85) by hand. First let us see what the Frobenius automorphism arguments give. Let $GF(4) =$

$\{0,1,a,b\}$, and suppose that 3 does not divide $t$. It is easy to check that $(a,b)$ is a point of multiplicity 1 on $g_t$ (since $1+a+b=0$). It follows from Proposition B in Chapter 1 that $g_t(X,Y,Z)$ has an absolutely irreducible factor over $GF(4)$. We also have:

**Proposition 9.** *Suppose $g_t(X,Y,Z)$ is irreducible over $GF(2)$, and let $t = 2^i\ell+1$. If $g_t(X,Y,Z)$ factors into $r$ absolutely irreducible factors over $GF(2^r)$, then $r$ divides the GCD of $t-3$ and $2^i-2$.*

*Proof:* Each absolutely irreducible factor contains the point $(1,1)$ with the same multiplicity. Hence $r$ divides the multiplicity of $(1,1)$, which is $2^i-2$. By Proposition B, $r$ also divides $t-3$. □

For example, if $t \equiv 5 \pmod 8$, then $i=2$ so $r=1$ or 2. This includes $t=61$ and 85. If $t=49$ then $(46,14)=2$ so $r=1$ or 2. If $t=81$ then $(78,14)=2$ so $r=1$ or 2. Hence for these values of $t$, $g_t(X,Y,Z)$ can only factor over $GF(2)$ or $GF(4)$.

We can finish off these values of $t$ using a computer. One way is to implement Hensel's Lemma. Another way is to compute the product of $g_t(X,\gamma)$ and its Galois conjugates, where $\gamma$ is an element of some extension of $GF(2)$. Then factor this binary polynomial in one variable into irreducibles over $GF(2)$ and draw conclusions (if possible) about the factorization of $g_t(X,Y)$ into *binary* factors.

**Theorem 10.** *$g_{49}(X, Y)$ is absolutely irreducible.*

*Proof:* Taking $\gamma$ to be an element of $GF(2^7)$ gives a binary factorization of the product into two irreducibles of degree 161. This implies that if $g_{49} = uv$ over $GF(2)$, then $u$ and $v$ have degree 23. But viewing the factorization when $\gamma \in GF(2^5)$ leads to the conclusion that this is impossible.

It remains to eliminate the possibility that $g_t = uv$ over $GF(4)$, in which case $u$ and $v$ must have degree 23 and are conjugates.

We shall use Bezout's theorem to eliminate this possibility. If this happened, the product of the degrees would be $23^2 = 529$. Since $t = 49 = 2^4 3 + 1$ the coordinates of a singular point must be elements of $GF(4) = \{0, 1, a, b\}$. Hence the only possible singular points are $(1,1), (a,a), (b,b)$ and $(1,a), (1,b), (a,1), (b,1)$. These all have multiplicity 16 except $(1,1)$ which has multiplicity 14. Since $F_{16} = 0$ at all these points, $I(P,u,v) = m_P(u)m_P(v)$ by Lemma 3. Since $m_P(u)+m_P(v) \leq 16$ we know that $I(P,u,v) \leq 64$. Hence $\Sigma I(P,u,v) \leq 7 \cdot 64 = 448$ so it cannot possibly equal 529. □

**Theorem 11.** *$g_{81}(X, Y)$ is absolutely irreducible.*

*Proof:* Write $t = 81 = 2^4 5 + 1$ and note that $B_5$ has no codewords of weight 4. By the remark before Theorem 6, there are no singular points $P = (\alpha, \beta)$ where $\alpha, \beta, 1$ are distinct. Recall that the coordinates of a singular point must be 5-th roots of unity, and as before suppose that $g_t = uv$. If $P = (\alpha, \alpha)$

is a singular point where $\alpha \notin GF(2^4)$, then $I(P,u,v) = 0$ by Lemma 4. If $P = (\alpha, 1)$ or $(1, \alpha)$ and $\alpha \notin GF(2^4)$, then $I(P,u,v) = 0$ by Lemma 5. Since $GF(2^4)$ contains all the 5-th roots of unity, we see that the only possible points with a nonzero intersection multiplicity are $P = (\alpha, \alpha)$ where $\alpha^5 = 1$. At these points $I(P,u,v) = m_P(u)m_P(v)$ because $F_{16} = 0$ and Lemma 3.

If $\alpha = 1$, then $m_P(g_{81}) = 14 = m_P(u) + m_P(v)$ and so $I(P,u,v) \leq 49$. If $\alpha \neq 1$, then $m_P(g_{81}) = 16 = m_P(u) + m_P(v)$ and so $I(P,u,v) \leq 64$. By Bezout's theorem,

$$(\deg u)(\deg v) = \sum_P I(P,u,v) \leq 4 \cdot 64 + 49 = 305.$$

But (deg $u$)+(deg $v$)=78, and so the only possibilities are deg $u$=1,2,3,4. If deg $u$=4, then $m_P(u) \leq 4$, and hence $I(P,u,v) = m_P(u)m_P(v) \leq 48$. Then $\Sigma_P I(P,u,v) \leq 5 \cdot 48 = 240$ but $4 \cdot 74 = 296$, a contradiction. The cases deg $u$=1,2,3 are done in exactly the same way. □

**Theorem 12.** *$g_{61}(X,Y)$ is absolutely irreducible.*

*Proof:* Write $t = 61 = 2^2 15 + 1$, and note that $B_{15}$ is a Hamming code and therefore has codewords of weight 4. Recall that the coordinates of a singular point must be 15-th roots of unity, and as before suppose that $g_t = uv$. If $P = (\alpha, \alpha)$ is a singular point where $\alpha \notin GF(2^2)$, then $I(P,u,v) = 0$ by Lemma 4. If $P = (\alpha, 1)$ or $(1, \alpha)$ and $\alpha \notin GF(4)$, then $I(P,u,v) = 0$ by Lemma 5.

If we show that $I(P,u,v)=0$ for all singular points $(\alpha,\beta)$ where $\alpha,\beta,1$ are distinct, then the only possible points with a nonzero intersection multiplicity are $P=(\alpha,\beta)$ where $\alpha,\beta\in GF(4)$. There are seven such singular points, namely $(1,1),(a,a),(b,b)$ and $(1,a),(1,b),(a,1),(b,1)$, where $GF(4)=\{0,1,a,b\}$. These all have multiplicity 4 except $(1,1)$ which has multiplicity 2.

Hence $I(P,u,v)\le 4$ for all these points except $(1,1)$ when $I(P,u,v)\le 1$, and so

$$(\deg\ u)(\deg\ v)=\sum_P I(P,u,v)\le 4\cdot 4+1=25.$$

But (deg $u$)+(deg $v$)=58, and so we have a contradiction.

It remains to show that $I(P,u,v)=0$ for all singular points $(\alpha,\beta)$ where $\alpha,\beta,1$ are distinct. Suppose $P$ is such a point. We will use Remark 3, and so we have to obtain a contradiction to

$$a=\frac{\tau}{\sigma}=\frac{\alpha^4+\alpha}{\beta^4+\beta}$$

being a common root of $F_4(X)$ and $F_5(X)$.

Note that $a^4=a$ and so $a\in GF(4)$. Since $\sigma^4=\alpha^{-3}+\lambda^{-3}$ and $\tau^4=\beta^{-3}+\lambda^{-3}$. and $\alpha,\beta,\lambda\in GF(16)$ in this case, we get $\sigma=\alpha^3+\lambda^3$ and $\tau=\beta^3+\lambda^3$. Hence

$$\frac{(\lambda/\beta)^3+1}{(\lambda/\alpha)^3+1}=\frac{\alpha^4+\alpha}{\beta^4+\beta}$$

from which we get

$$\alpha\lambda^3+\alpha^4+\alpha(\lambda/\alpha)^3+\alpha=\beta\lambda^3+\beta^4+\beta(\lambda/\beta)^3+\beta.$$

Using $\alpha + \beta = \lambda + 1$ this becomes

$$\lambda^3(\lambda + 1) + (\lambda^4 + 1) + (\lambda + 1) + \lambda^3\alpha^{-2} + \lambda^3\beta^{-2} = 0.$$

Taking square roots we get $\lambda^2 + 1 + \lambda/\alpha + \lambda/\beta = 0$. This gives

$$\alpha + \beta + \frac{1+\beta}{\alpha} + \frac{1+\alpha}{\beta} = 0.$$

Multiplying this equation by $\alpha\beta$ and dividing by $\alpha+\beta$ yields $\alpha\beta+\alpha+\beta+1 = 0$, whence $(\alpha + 1)(\beta + 1) = 0$, which is impossible. □

**Theorem 13.** *$g_{85}(X, Y)$ is absolutely irreducible.*

*Proof:* Write $t = 85 = 2^2 21 + 1$. If $P = (\alpha, \alpha)$ is a singular point where $\alpha \notin GF(2^2)$, then $I(P, u, v) = 0$ by Lemma 4. If $P = (\alpha, 1)$ or $(1, \alpha)$ and $\alpha \notin GF(4)$, then $I(P, u, v) = 0$ by Lemma 5.

If we show that $I(P, u, v) = 0$ for all singular points $(\alpha, \beta)$ where $\alpha, \beta, 1$ are distinct, then the only possible points with a nonzero intersection multiplicity are $P = (\alpha, \beta)$ where $\alpha, \beta \in GF(4)$. There are seven such singular points, namely $(1, 1), (a, a), (b, b)$ and $(1, a), (1, b), (a, 1), (b, 1)$, where $GF(4) = \{0, 1, a, b\}$. These all have multiplicity 4 except $(1, 1)$ which has multiplicity 2.

Hence $I(P, u, v) \leq 4$ for all these points except $(1, 1)$ when $I(P, u, v) \leq 1$, and so

$$(\deg u)(\deg v) = \sum_P I(P, u, v) \leq 4 \cdot 4 + 1 = 25.$$

But (deg $u$)+(deg $v$)=82, and so we have a contradiction.

It remains to show that $I(P, u, v) = 0$ for all singular points $(\alpha, \beta)$ where $\alpha, \beta, 1$ are distinct. We have verified this on a computer using Remark 3 (showing that $a$ cannot be a root of $F_5$).

Here is another argument. Such singular points are related to codewords of weight 4 in the code $B_{21}$, which has 84 such codewords. Each codeword gives rise to 6 singular points, so there are 504 such points. Each of these points has multiplicity 5 on $g_{85}$. By Theorem 14 if $I(P, u, v)$ is nonzero then $I(P, u, v) = 4$. But recall that $I(P, u, v) \geq m_P(u)m_P(v)$ and $m_P(u)+m_P(v) = 5$. The only way this can happen is if $m_P(u) = 4$ and $m_P(v) = 1$. But this means that $I(P, u, v) = m_P(u)m_P(v)$, and this can only happen if $u$ and $v$ have distinct tangents at $P$. But $F_4 \neq 0$, so this is impossible. □

This argument can be generalized to give some stronger results, see for example Corollary 15 and its consequences.

### 2.6 Verification of Bezout's Theorem.

In this section we show that Bezout's theorem can be verified directly in the cases $t = 2^i + 1$ and $t = 2^{2i} - 2^i + 1$ where $g_t(X, Y, Z)$ is not absolutely irreducible, in the hope that this will provide some insight into why it does not work in the other cases.

**1.** $t = 2^i + 1$**.**

Let $t = 2^i + 1$ and suppose that $P = (\alpha, \beta)$ is a singular point of $g_t$. Then $\alpha$ and $\beta$ are $(t-1)$-th roots of unity, and so they are both 1. So $g_t$ has only one singular point $Q = (1,1)$. From the factorization of $g_t$ given in [JW] we can see that $Q$ has multiplicity 1 on each of the $2^i - 2$ linear factors $X + \alpha Y + 1 + \alpha$. If we write $g_t = GH$ for any $G$ and $H$, then

$$m_Q(G) + m_Q(H) = m_Q(g_t) = 2^i - 2 = \text{deg } (g_t) = \text{deg } G + \text{deg } H,$$

and so $m_Q(G) = \text{deg } G$ and $m_Q(H) = \text{deg } H$.

By Lemma 5 we get that all the tangent directions at $Q$ are distinct, and so $I(Q, G, H) = m_Q(G)m_Q(H)$. It follows that

$$I(Q, G, H) = (\text{deg } G)(\text{deg } H),$$

which is what Bezout's theorem gives in this case.

**2.** $t = 13$**.**

We know from [JW] that $g_{13}(X, Y)$ factors into 2 absolutely irreducible factors over $GF(4)$ as follows:

$$A(X,Y) = 1 + a + aX + aX^4 + X^5 + (1 + X + aX + aX^2 + X^3 + X^4$$
$$+ aX^4)Y + (X + X^2 + aX^2)Y^2 + aXY^3 + (1 + X + aX)Y^4 + aY^5$$

and

$$B(X,Y) = a + X + aX + X^4 + aX^4 + X^5 + (1 + aX + X^2 + aX^2 + X^3 +$$
$$aX^4)Y + (X + aX^2)Y^2 + (X + aX)Y^3 + (1 + aX)Y^4 + (1 + a)Y^5,$$

where $a$ satisfies $a^2 + a + 1 = 0$ in $GF(4)$. If $P = (\alpha, \beta)$ is a singular point of $g_{13}$, then $\alpha$ and $\beta$ are cube roots of unity. So there are 9 possible singular points, but $(a, a^2)$ and $(a^2, a)$ are ruled out because $1 + \alpha + \beta$ must also be a cube root of unity. Using Mathematica, one can compute the multiplicities on $A$ and $B$ of the 7 singular points:

| $P$ | $(1,1)$ | $(a,a)$ | $(a^2,a^2)$ | $(1,a)$ | $(1,a^2)$ | $(a,1)$ | $(a^2,1)$ |
|---|---|---|---|---|---|---|---|
| $m_P(g_{13})$ | 2 | 4 | 4 | 4 | 4 | 4 | 4 |
| $m_P(A)$ | 1 | 2 | 2 | 2 | 2 | 2 | 2 |
| $m_P(B)$ | 1 | 2 | 2 | 2 | 2 | 2 | 2 |
| $I(P,A,B)$ | 1 | 4 | 4 | 4 | 4 | 4 | 4 |

The figures for $m_P(g_{13}) = m_P(A) + m_P(B)$ follow from the fact that $f_4 = 0$, and so $m_P(f_{13}) = 5$. In calculating $I(P, A, B)$ we use Lemma 5, which implies that $I(P, A, B) = m_P(A)m_P(B)$. It is now clear that

$$(\deg A)(\deg B) = 25 = \sum_P I(P, A, B),$$

verifying Bezout.

**3.** $t = 57$**.**

This is the next case in the family $t = 2^i(2^i - 1) + 1$, when $i = 3$. We know from [JW] that $g_{57}(X, Y)$ factors into 6 absolutely irreducible factors of degree 9 over $GF(8)$. Hence it factors into two irreducibles of degree 27 over $GF(2)$. Call these $A$ and $B$. If $P = (\alpha, \beta)$ is a singular point of $g_{57}$, then $\alpha$

and $\beta$ are in $GF(8)$. There are 43 singular points, 24 with $\alpha, \beta, 1$ distinct, 6 each with $\alpha = 1$, $\beta = 1$, or $\alpha = \beta$, and also there is $(1,1)$. The respective multiplicities on $g_{57}$ are 9,8,8,8,6.

Using Mathematica, one can compute the multiplicities on $A$ and $B$ of the 43 singular points: In calculating $I(P, A, B)$ we use Lemma 5, which implies that $I(P, A, B) = m_P(A)m_P(B)$.

| $P$ | $m_P(A)$ | $m_P(B)$ | $I(P, A, B)$ |
|---|---|---|---|
| $(1,1)$ | 3 | 3 | 9 |
| $(1, a^i)$ | 4 | 4 | $16 \cdot 6 = 96$ |
| $(a^i, 1)$ | 4 | 4 | $16 \cdot 6 = 96$ |
| $(a^i, a^i)$ | 4 | 4 | $16 \cdot 6 = 96$ |
| $(a^2, a)^\sigma$ | 3 | 6 | $18 \cdot 3 = 54$ |
| $(a^6, a)^\sigma$ | 3 | 6 | $18 \cdot 3 = 54$ |
| $(a^2, a^3)^\sigma$ | 3 | 6 | $18 \cdot 3 = 54$ |
| $(a^5, a^3)^\sigma$ | 3 | 6 | $18 \cdot 3 = 54$ |
| $(a^4, a)^\sigma$ | 6 | 3 | $18 \cdot 3 = 54$ |
| $(a^5, a)^\sigma$ | 6 | 3 | $18 \cdot 3 = 54$ |
| $(a^4, a^3)^\sigma$ | 6 | 3 | $18 \cdot 3 = 54$ |
| $(a^6, a^3)^\sigma$ | 6 | 3 | $18 \cdot 3 = 54$ |

In this table the entry $(a^2, a)^\sigma$ denotes the point and its Frobenius images. Also, $i$ runs from 1 to 6. We now see that

$$(\deg A)(\deg B) = 729 = \sum_P I(P, A, B),$$

verifying Bezout's theorem.

We also computed the multiplicities when $A$ is an absolutely irreducible factor of degree 9 and $B$ is the complementary factor.

## 2.7 Resolution of Singularities

In this section we resolve the singularities on the curve $g_t(X, Y, Z)$ and thereby compute the intersection multiplicity $I(P, u, v)$ at a singular point $P$. A reference for this is [F] or [A].

**Theorem 14.** *Let $t = 2^i\ell + 1$ and $P = (\alpha, \beta)$ be a singular point on $g_t$ such that 1, $\alpha$, $\beta$ are distinct and $G_{2^i} \neq 0$. If $g_t = uv$ then either $I(P, u, v) = 0$ or $2^i$.*

*Proof:* By Remark 2 we know that $(F_{2^i}, F_{2^i+1}) = (G_{2^i}, G_{2^i+1})$. By Lemma 3, either $(F_{2^i}, F_{2^i+1}) = 1$ or $\sigma X + \tau Y$. If $(F_{2^i}, F_{2^i+1}) = 1$ then $I(P, u, v) = 0$ by Proposition A. If $(F_{2^i}, F_{2^i+1}) = \sigma X + \tau Y$ then $F_{2^i+1}(\tau, \sigma) = 0$. Assume this from now on.

$$g_t(X + \alpha, Y + \beta) = u(X + \alpha, Y + \beta)v(X + \alpha, Y + \beta)$$

$$G_{2^i} + G_{2^i+1} + \cdots = (U_a + U_{a+1} + \cdots)(V_b + V_{b+1} + \cdots).$$

Hence

$$U_a V_b = G_{2^i} = (\sigma X + \tau Y)^{2^i} \quad \text{and} \quad G_{2^i+1} = U_a V_{b+1} + U_{a+1} V_b.$$

But $F_{2^i+1}$ has distinct linear factors by Lemma 3, so either $a = 1$ or $b = 1$ (if both $a$ and $b$ are $> 1$, then $(\sigma X + \tau Y)^2$ divides $G_{2^i+1}$ and hence $F_{2^i+1}$ by Remark 1). So we may assume that $m_P(u) = 1$ and $m_P(v) = 2^i - 1$ as $m_P(f_t) = 2^i$, and $m_P(w) = 0$ where $f_t = uvw$.

Now $u$ and $v$ have a common tangent at $P$, so

$$I(P,u,v) > m_P(u)m_P(v) = 2^i - 1.$$

In fact, by Bezout's theorem,

$$I(P,u,v) = m_P(u)m_P(v) + \sum_Q m_Q(u)m_Q(v)$$

where the sum is over all $Q$ infinitely near to $P$. We will show that this sum is equal to 1.

Since $g_t$ and $f_t$ are locally the "same" at $P$ (the factors $(X+1)(Y+1)(X+Y)$ do not pass through $P$ so $m_P(f_t) = m_P(g_t))$ we will work with $f_t$. Resolving the singularity of one will resolve it for the other.

We have $F_{2^i}(X,Y) = A^*(Y - AX)^{2^i}$, where $A = \sigma/\tau$, and so there is only one point in the first neighborhood, namely $P_1 = (0, A)$. Next we compute $f'(X, Y + A)$, where $f_t(X + \alpha, XY + \beta) = X^{2^i} f'(X,Y)$.

$$\begin{aligned} f'(X, Y+A) &= F_{2^i}(1, Y+A) + XF_{2^i+1}(1, Y+A) + \cdots \\ &= A^*Y^{2^i} + X\big(F_{2^i+1}(1,A) + X(\cdots)\big) + \text{ higher order terms} \\ &= X\big((\alpha^{-2^i} + \lambda^{-2^i}) + \lambda^{-2^i}A + \lambda^{-2^i}A^{2^i} + (\beta^{-2^i} + \lambda^{-2^i})A^{2^i+1}\big) \\ &\quad + XY\big(\lambda^{-2^i} + (\beta^{-2^i} + \lambda^{-2^i})A^{2^i}\big) + \text{ higher order terms.} \end{aligned}$$

We see that the degree one term in this expansion is zero if and only if $F_{2^i+1}(\tau,\sigma) = 0$, which we are assuming.

But the degree two term is not zero. To see this, note that it is zero if and only if $\lambda^{-1} = (\beta^{-1} + \lambda^{-1})A$ if and only if $\tau/\sigma = (1+\alpha)/\beta$. But if this is true, then $\tau/\sigma$ is not a root of $F_{2^i+1}$, as in the proof of Lemma 3.

Hence $m_{P_1}(f') = 2$, and this implies $m_{P_1}(u) = m_{P_1}(v) = 1$, as $m_{P_1}(w) = 0$.

The important observation here is that the coefficient of $XY$ is nonzero. This means that $f'$ has two different tangent directions at $P_1$, and so any points $Q$ in the first neighborhood of $P_1$ (the second neighborhood of $P$) are to be considered simple points on $f_t$. So either $m_Q(u) = 0$ or $m_Q(v) = 0$ for these points $Q$. By the refined version of Bezout's theorem, see [A] or [F], we get

$$I(P, u, v) = m_P(u)m_P(v) + m_{P_1}(u)m_{P_1}(v) = (2^i - 1) + 1 = 2^i,$$

and this completes the proof. □

The following Corollary is extremely useful.

**Corollary 15.** *Let $t = 2^i\ell + 1$ and $P = (\alpha, \beta)$ be a singular point on $g_t$ such that $1, \alpha, \beta$ are distinct and $G_{2^i} \neq 0$. If $g_t = uv$, then $I(P, u, v) = 0$.*

*Proof:* If $I(P, u, v) \neq 0$ then $I(P, u, v) = 2^i$ by Theorem 14. But $m_P(g_t) = 2^i + 1 = m_P(u) + m_P(v)$ and $I(P, u, v) \geq m_P(u)m_P(v)$. The only way this can happen is if $m_P(u) = 2^i$ and $m_P(v) = 1$. But this implies $I(P, u, v) = m_P(u)m_P(v)$, which implies that the factors $u$, $v$ have distinct tangents at $P$, which is not true. □

The preceding Corollary implies that if $\ell$ is sufficiently large with respect to $i$, then $g_t$ is absolutely irreducible. This is because the product of the degrees of $u$ and $v$ is at least $2^i\ell - 3$, but $\Sigma_P I(P, u, v)$ is bounded by a function of the form $f(i)$.

The preceding Corollary also implies that if $t \equiv 5 \pmod 8$ then $g_t$ is absolutely irreducible, because the assumption in Theorem 6 that $B_\ell$ has no codewords of weight 4 can be dropped. The same assumption can be dropped in Theorem 7.

We now study a different type of singular point, where both coordinates are in the field $GF(2^i)$. These are the only possible singular points that have nonzero intersection multiplicity.

**Theorem 16.** *Let $t = 2^i\ell + 1$ and $P = (\alpha, \beta)$ be a singular point on $g_t$ such that both $\alpha, \beta \in GF(2^i)$, and so $F_{2^i} = 0$. The roots of $F_{2^i+1}(X, 1)$ lie in $GF(2^{2i})$.*

*Proof:* Denoting $\lambda^{2^i} F_{2^i+1}(X, 1)$ by $f(X)$, we calculate

$$f(X) = \left(\frac{1+\beta}{\alpha}\right)^{2^i} X^{2^i+1} + X^{2^i} + X + \left(\frac{1+\alpha}{\beta}\right)^{2^i}.$$

Let $c = ((1+\beta)/\alpha)^{2^i} = (1+\beta)/\alpha$ and $b = ((1+\alpha)/\beta)^{2^i} = (1+\alpha)/\beta$, so that

$$\begin{aligned} f(X) &= cX^{2^i+1} + X^{2^i} + X + b \\ &= (cX+1)X^{2^i} + X + b. \end{aligned}$$

Define $T(x) = (x+b)/(cx+1)$. Then calculate that $T^2(x) = x$. Let $\theta$ be a root of $f(X)$, which means $\theta^{2^i} = (\theta + b)/(c\theta + 1)$. Hence

$$\theta = T^2(\theta) = \frac{\theta^{2^i} + b}{c\theta^{2^i} + 1} = \frac{\theta^{2^i} + b^{2^i}}{c^{2^i}\theta^{2^i} + 1} = T(\theta)^{2^i} = (\theta^{2^i})^{2^i} = \theta^{2^{2i}}$$

completing the proof. □

Note that the only fixed point of $T$ is the square root of $(\alpha^2+\alpha)/(\beta^2+\beta)$. For suppose $T(x) = x$, then $(x+b)/(cx+1) = x$ and so $x^2 = b/c = (\alpha^2 + \alpha)/(\beta^2+\beta)$.

**Corollary 17.** *All the irreducible factors of $F_{2^i+1}(X,Y)$ over $GF(2^i)$ have degree two, except for one factor which has degree one.*

*Proof:* Linear factors over $GF(2^i)$ correspond to fixed points of $T$, and there is only one fixed point. □

We can prove a general theorem from the methods above, and then we give another proof of Proposition A using resolution of singularities.

**Theorem 18.** *If $P = (\alpha, \beta)$ is a singular point of a curve defined by $F(x,y) = 0$, write*

$$F(x+\alpha, y+\beta) = F_m(x,y) + F_{m+1}(x,y) + \cdots$$

*where $m = m_P(F)$. Suppose there is only one tangent direction at $P$, and that $(F_m, F_{m+1}) = 1$. Then $P$ has only one infinitely near point, which is in its first neighborhood and is simple.*

*Proof:* We have $F_m(x,y) = A^*(y - Ax)^m$, and so there is only one point in the first neighborhood, namely $P_1 = (0, A)$. Next we compute $F'(x, y+A)$, where $F(x+\alpha, xy+\beta) = x^m F'(x,y)$.

$$\begin{aligned} F'(x, y+A) &= F_m(1, y+A) + xF_{m+1}(1, y+A) + \cdots \\ &= A^* y^m + x\big(F_{m+1}(1, A) + y(\cdots)\big) + \text{ higher order terms.} \end{aligned}$$

It is clear that $P_1$ is simple if and only if $F_{m+1}(1, A) \neq 0$ if and only if $y - Ax$ does not divide $F_{m+1}$ if and only if $(F_m, F_{m+1}) = 1$. □

This gives another proof of Proposition A.

**Corollary 19=Proposition A.** *With the hypotheses of Theorem 13, if $F = uv$ then $I(P, u, v) = 0$.*

*Proof:* By the refined version of Bezout's Theorem,

$$I(P, u, v) = m_P(u) m_P(v) + \sum_Q m_Q(u) m_Q(v)$$

where the sum is over all $Q$ that are infinitely near to $P$. Hence $I(P, u, v) = m_P(u) m_P(v)$ by Theorem 18. This equality implies that $u$ and $v$ have distinct tangents at $P$. Since there is only one tangent direction at $P$, one of $m_P(u)$ or $m_P(v)$ is zero and hence $I(P, u, v) = 0$. □

### 2.8 The Genus of $g_t(X, Y, Z)$.

If $C$ is an absolutely irreducible curve given by $F(X, Y) = 0$ of degree $n$, then the genus of $C$ is given by

$$g(C) = \frac{(n-1)(n-2)}{2} - \sum_P \delta(P),$$

where the sum is over all distinct points $P \in C$, and

$$\delta(P) = \sum_i \frac{m_{P_i}(F)(m_{P_i}(F) - 1)}{2}$$

where this sum is over all points $P_i$ such that $P_i = P$ or $P_i$ is infinitely near to $P$.

**Theorem 20.** *If $t \equiv 3 \pmod 4$, $t > 3$, then the genus of $g_t(X, Y)$ is given by*

$$g = \frac{(t-4)(t-5)}{2} - N$$

*where $N$ is the number of singular points of $g_t(X, Y)$.*

*Proof:* By Theorem 18, every singular point $P$ has just one point infinitely near to it, which is simple. □

**Corollary 21.** *If $B_\ell$ has no codewords of weight 4, then $g_t(X, Y)$ is nonsingular.*

**Corollary 22.** *If $t = 2^i - 1$, $t > 7$, then the genus is $g = (t-5)(t-7)/4$.*

*Proof:* If $t = 2^i - 1 = 2\ell + 1$, then $\ell = 2^{i-1} - 1$ and so $\alpha, \beta \in GF(2^{i-1})$. There are $\ell - 1$ choices for $\alpha$ and $\ell - 3$ choices for $\beta$ ($\beta$ cannot be $1, \alpha, \alpha + 1$). Hence the genus

$$\begin{aligned} g &= \frac{(t-4)(t-5)}{2} - (\ell - 1)(\ell - 3) \\ &= \frac{(t-4)(t-5)}{2} - \frac{(t-3)}{2}\frac{(t-7)}{2} \\ &= \frac{(t-5)(t-7)}{4}. \end{aligned}$$

□

# CHAPTER 3

# Hyperovals in Projective Planes and Absolutely Irreducible Polynomials in Characteristic 2

## 3.1. Introduction.

An *oval* in the finite projective plane $PG(2, q)$ is a set of $q+1$ points with the property that no 3 are collinear. If $q$ is odd then such a set is maximal with that property. A celebrated theorem of Segre (1955) states that all such ovals are given algebraically by irreducible conics. If $q$ is even however, the situation is much more interesting. Here a set of points in $PG(2, q)$ of largest possible size such that no 3 are collinear has cardinality $q+2$, and is called a *hyperoval.* No classification analagous to Segre's for $q$ odd is known.

From now on in this chapter we assume that $q$ is even. A hyperoval can be constructed from a (nonsingular) conic by adjoining the point at which all the tangents of the conic meet, the nucleus. Such hyperovals are generally called regular hyperovals. However for $q > 8$ there also exist irregular hyperovals which are not of the form conic plus nucleus, see [G1],[G2],[OKP] for example.

We represent the points of $PG(2,q)$ as homogeneous triples with coordinates from $GF(q)$. It is well known that all hyperovals can be written in the form

$$\{(1,x,f(x)) : x \in GF(q)\} \cup \{(0,0,1),(0,1,0)\}$$

where $f(x)$ is a polynomial with certain properties, see [H],[G2]. Denote the above set by $D(f(x))$ for any $f$. In this chapter we shall examine the case where $f(x)$ is a monomial, say $f(x) = x^k$. If $q = 2^e$, Segre showed that the set $D(x^k)$ is a hyperoval for the following values of $k$ and the values of $e$ indicated:

$$k = 2^i, \text{ when } (i,e) = 1 \text{ ([S1], 1957)},$$

$$k = 6, \text{ when } (2,e) = 1 \text{ ([S2], 1962)}.$$

We wish to consider other values of $k$. In particular, we wish to consider the question of whether there are other such infinite sequences, i.e., other fixed values of $k$ for which $D(x^k)$ is a hyperoval for infinitely many $q$. Our main result is the following theorem, which was proved by Segre and Bartocci in [SB]. Our work was completed before we found out about this paper of Segre and Bartocci.

**Theorem 3.1.** *For any fixed $k \equiv 2 \pmod 4$, $k > 6$, the set $D(x^k)$ is a hyperoval in $PG(2,q)$ for at most a finite number of values of $q$.*

In [M] the permutation properties of $1 + x + \cdots + x^{k-1}$ on $GF(q)$ are studied. It follows from [LN, p.505] that this polynomial is a permutation polynomial if and only if $D(x^k)$ is a hyperoval. Hence our result sheds some light on this problem. It is now trivial to see that $k$ must be even in order for $D(x^k)$ to be a hyperoval, since $1 + x + \cdots + x^{k-1}$ maps both 0 and 1 to 1 if $k$ is odd. So we assume $k$ is even from now on. Values of $k$ which are functions of $e$ have been studied, see [G1], but we do not consider this here.

In case $D(x^k)$ is a hyperoval, we might call it a monomial hyperoval in honour of $f(x)$ being a monomial. The main thrust of this chapter is that apart from Segre's examples, monomial hyperovals (for fixed $k$) are rare. Following [H], we will write $D(k)$ instead of $D(x^k)$.

In section 3.2 we shall prove the connection between the polynomials $g_k(X,Y,Z)$ and the hyperovals $D(k)$. Section 3.3 contains singularity analysis of the polynomials $g_k(X,Y,Z)$. We shall completely factorize $g_k(X,Y,Z)$ for $k = 2^i$ and $k = 6$ in section 3.4, and there we will reprove Segre's theorems. In sections 3.5 (and 3.7) we will use Bezout's theorem to prove the main theorem. Section 3.6 contains consequences of the results in this paper. Finally section 3.8 presents a conjecture and some more evidence, namely some values of $k \equiv 0 \pmod 4$ for which $D(k)$ is a hyperoval for only a "few" small values of

$q$.

### 3.2. Hyperovals and Absolute Irreducibility.

The set $D(k)$ being a hyperoval in $PG(2,q)$ is equivalent to the determinant

$$det \begin{pmatrix} 1 & 1 & 1 \\ X & Y & Z \\ X^k & Y^k & Z^k \end{pmatrix}$$

being nonzero for all distinct $X, Y, Z \in GF(q)$. Divide the determinant by $(X+Y)(X+Z)(Y+Z)$ and call the resulting polynomial $g_k(X,Y,Z)$. In other words, we define a binary polynomial $g_k(X,Y,Z)$ by

$$g_k(X,Y,Z) := \frac{XY^k + YX^k + XZ^k + ZX^k + YZ^k + ZY^k}{(X+Y)(X+Z)(Y+Z)}.$$

Our main theorem rests on the following, which is similar to Proposition 1 in [JW].

**Theorem 3.2.** *If the polynomial $g_k(X,Y,Z)$ is absolutely irreducible over $GF(2)$, then $D(k)$ is a hyperoval in $PG(2,q)$ for only a finite number of values of $q$.*

*Proof:* If the polynomial $g_k(X,Y,Z)$ of degree $k-2$ is absolutely irreducible over $GF(2)$, then applying Weil's theorem (from Chapter 1) shows that the number $N_e$ of (projective) rational points $(x,y,z)$ on $g_k(X,Y,Z)$ where $x,y,z$ are in $GF(2^e)$ satisfies

$$|N_e - 2^e| < (k-3)(k-4)2^{e/2} + (k-2)^2 \qquad (1)$$

for every $e$. Once we show that the number of such rational points where some of the coordinates are equal is at most $3k-2$, it will follow that there are rational points over $GF(2^e)$ with $x, y, z$ distinct for all $e$ sufficiently large.

To this end we let $p(X, Y, V) = g_k(X, Y, X+V)$, and note that projective points $(x, y, z)$ on $g_k(X, Y, Z)$ with $x = z$ are in $1-1$ correspondence with projective points $(x, y, 0)$ on $p(X, Y, V)$. A simple computation (using the fact that $k$ is even) shows that

$$p(X, Y, 0) = \frac{X^k + Y^k}{(X+Y)^2}.$$

Again we let $q(X, W) = p(X, X+W, 0)$, and note that projective points $(x, y, z)$ on $g_k(X, Y, Z)$ with $x = z \neq y$ are in $1-1$ correspondence with affine points $(x, 1)$ on $q(X, W)$. Since $q(X, 1) = X^k + (X+1)^k$, there are at most $k-1$ projective points $(x, y, z)$ on $g_k(X, Y, Z)$ with $x = z \neq y$. A similar argument holds for points $(x, y, z)$ with $x = y \neq z$ and $y = z \neq x$. Counting the projective point $(1, 1, 1)$ we get that there are at most $3k-2$ rational points $(x, y, z)$ on $g_k(X, Y, Z)$ with $x, y, z$ not all distinct. □

From the form of the Weil bound in (1), we can compute the value of $e$, say $e_0$, for which $N_e > 3k-2$ for all $e \geq e_0$. See section 6 for small $k$.

Armed with this theorem, our task now is to demonstrate the absolute irreducibility of the polynomials $g_k(X, Y, Z)$ over $GF(2)$. This is how we shall prove the results alluded to in section 3.1.

Bearing in mind Segre's results, $g_k(X,Y,Z)$ cannot be absolutely irreducible when $k = 2^i$ or $k = 6$. We shall completely factorize $g_k(X,Y,Z)$ for these values of $k$ in section 3.4, and there we will reprove Segre's theorems. In section 3.5 we prove that $g_k(X,Y,Z)$ is absolutely irreducible for all $k \equiv 2 \pmod 4$, $k > 6$. In section 3.8 we prove absolute irreducibility for some values of $k \equiv 0 \pmod 4$.

### 3.3. Singularity analysis of the polynomials.

It will be shown later in this section that (fortunately) we are allowed to work with the affine parts of the homogeneous polynomials $f_k(X,Y,Z)$ and $g_k(X,Y,Z)$. There will be no confusion if we use the same names, and so

$$f_k(X,Y) := XY^k + YX^k + X^k + Y^k + X + Y$$
$$g_k(X,Y) := \frac{XY^k + YX^k + X^k + Y^k + X + Y}{(X+Y)(X+1)(Y+1)},$$

and we consider the algebraic curves defined by these polynomials over the algebraic closure of $GF(2)$.

The singular points can be found by equating the first partial derivatives to zero. We easily calculate ($k$ is even)

$$\frac{\partial f_k}{\partial X}(X,Y) = Y^k + 1, \qquad \frac{\partial f_k}{\partial Y}(X,Y) = X^k + 1.$$

Hence if $P = (\alpha, \beta)$ is a singular point of $f_k(X,Y)$, then $\alpha$ and $\beta$ are $k$-th roots of unity. Write $k = 2^i\ell$ where $\ell$ is odd and $i \geq 1$. Then $\alpha$ and $\beta$ are $\ell$-th roots of unity, and so $f_k(X,Y)$ has $\ell^2$ singular points (it is easy to check that there are no singular points at infinity — the three partial derivatives of $f_k(X,Y,Z)$ are $X^k+Y^k$, $X^k+Z^k$, $Y^k+Z^k$, and if these all vanish and $Z=0$ then $X=Y=0$ which is impossible).

Next we pin down the multiplicities of these singular points $P=(\alpha,\beta)$ on $f_k(X,Y)$, and how things change for $g_k(X,Y)$. We compute that

$$\begin{aligned} f_k(X+\alpha,Y+\beta) &= \sum_{j=1}^{k}\binom{k}{j}\big(\alpha^{-j}X^jY+\beta^{-j}Y^jX+(\beta+1)\alpha^{-j}X^j \\ &\quad +(\alpha+1)\beta^{-j}Y^j\big) \\ &= F_1(X,Y)+F_2(X,Y)+\cdots \end{aligned}$$

using $\alpha^k=1=\beta^k$. Since $\binom{k}{j}$ is even for $1\le j<2^i$ and odd for $j=2^i$, we see that all singular points of $f_k(X,Y)$ have multiplicity $2^i$, except $(1,1)$ which has multiplicity $2^i+1$. This claim follows from

$$\begin{aligned} F_{2^i}(X,Y) &= (\beta+1)\alpha^{-2^i}X^{2^i}+(\alpha+1)\beta^{-2^i}Y^{2^i}, \\ F_{2^i+1}(X,Y) &= \alpha^{-2^i}X^{2^i}Y+\beta^{-2^i}Y^{2^i}X, \end{aligned} \tag{2}$$

where the second equation owes itself to the evenness of $\binom{k}{2^i+1}$.

Defining $w(X,Y):=(X+Y)(X+1)(Y+1)$ we note the following multiplicities on $w$: $m_P(w)=3$ if $P=(1,1)$, $m_P(w)=1$ if $P=(1,\alpha)$ or $(\alpha,1)$ or $(\alpha,\alpha)$ where $\alpha\neq1$, and $m_P(w)=0$ for all other singular points $P=(\alpha,\beta)$. At long last we arrive at the multiplicities for $g_k(X,Y)$.

| $P$ | $m_P(g_k)$ |
|---|---|
| $(1,1)$ | $2^i-2$ |
| $(\alpha,1)$ | $2^i-1$ |
| $(1,\alpha)$ | $2^i-1$ |
| $(\alpha,\alpha)$ | $2^i-1$ |
| $(\alpha,\beta)$ | $2^i$ |

There are $3(\ell-1)$ points of multiplicity $2^i-1$, and so there are $(\ell-1)(\ell-2)$ singular points of multiplicity $2^i$ on $g_k(X,Y)$.

Our method of proving absolute irreducibility will be to assume that $g_k(X,Y,Z)$ is reducible, say $g_k(X,Y,Z) = u(X,Y,Z)v(X,Y,Z)$, and obtain a contradiction by applying Bezout's theorem to the curves $u$ and $v$. If a point $P$ has $I(P,u,v) \neq 0$, then $m_P(g_k) = m_P(u)+m_P(v) \geq 2$, and so $P$ is a singular point of $g_k(X,Y,Z)$. We have seen that the projective curves $g_k(X,Y,Z)$ have no singular points at infinity. Therefore, since the only points $P$ that give a nonzero contribution to the sum in Bezout's theorem are singular points of $g_k(X,Y,Z)$, we may just work with the affine part of $g_k(X,Y,Z)$.

Let us see what the Frobenius automorphism arguments give. The following is a Corollary of Proposition B in Chapter 1.

**Corollary 3.3.** *If $k \equiv 4 \pmod 8$ or if $k \equiv 1 \pmod 3$ or if $k \equiv 2 \pmod 4$, then $g_k(X,Y)$ has an absolutely irreducible factor over $GF(4)$.*

*Proof:* If $k \equiv 4 \pmod 8$ then by the table above, the point $(1,1)$ has multiplicity 2 on $g_k$. If 3 divides $k-1$ then check that the point $(\omega, \omega^2)$ has multiplicity 1 on $g_k$, where $GF(4) = \{0, 1, \omega, \omega^2\}$. If $k \equiv 2 \pmod 4$, then $(1, \omega)$ is a point of multiplicity 1. □

### 3.4. The Case $k = 2^i$ or 6.

In this section we study the polynomials $g_k(X,Y)$ when $k = 2^i$ and $k = 6$. First let us examine $k = 2^i$.

$$\begin{aligned} f_k(X+1, Y+1) &= (X+1)^{2^i} Y + (Y+1)^{2^i} X + X + Y \\ &= X^{2^i} Y + Y^{2^i} X \\ &= XY \prod_{\gamma \in GF(2^i)^*} (X + \gamma Y). \end{aligned}$$

Replace $X$ by $X+1$, $Y$ by $Y+1$, and divide by $(X+Y)(X+1)(Y+1)$ to get

**Theorem 3.4.** *When $k = 2^i$ we have the following factorization,*

$$g_k(X,Y) = \prod_{\gamma \in GF(2^i) \setminus \{0,1\}} (X + \gamma Y + \gamma + 1).$$

**Corollary (Segre).** *When $k = 2^i$ the set $D(k)$ is a hyperoval in $PG(2, 2^e)$ if and only if $(i, e) = 1$.*

*Proof:* We have to show that $g_k(X,Y)$ has the necessary rational points over $GF(2^e)$ if and only if $(i, e) > 1$.

Suppose that $i$ and $e$ are relatively prime and that there exists $a, b \in GF(2^e)$ with $a \neq b, a \neq 1, b \neq 1$ such that $g_k(a,b) = 0$. By Theorem 4, there exists $\gamma \in GF(2^i)\backslash\{0,1\}$ such that $a + \gamma b + \gamma + 1 = 0$. But this implies $\gamma = (a+1)/(b+1) \in GF(2^i) \cap GF(2^e) = GF(2)$, a contradiction.

Conversely suppose $(i,e) > 1$, and choose $a, b$ distinct in $GF(2^i) \cap GF(2^e)$ but not in $GF(2)$. Letting $\gamma = (a+1)/(b+1)$ shows that $g_k(a,b) = 0$ by Theorem 4. □

We remark that $P = (1,1)$ is the only singular point in this case, and it has multiplicity $2^i - 2$.

---

Next we consider $k = 6$. We could just plonk down the factors here and say no more about it, but we feel that finding them is instructive, and so we describe the process. We use two little results from section 3.8 that could easily be placed here, but we feel they are more at home there. Here (using Lemma 3.9) is the polynomial under consideration:

$$\begin{aligned} g_6(X,Y) =& Y^4 + Y^3(1+X) + Y^2(1+X+X^2) + Y(1+X+X^2+X^3) \\ &+ 1 + X + X^2 + X^3 + X^4. \end{aligned}$$

First, from section 3.3 the only singular points are $P = (\alpha, \beta)$ where $1, \alpha, \beta$ are distinct and $\alpha^3 = 1 = \beta^3$. If $GF(4) = \{0, 1, \omega, \omega^2\}$ this means there are two singular points, namely $(\omega, \omega^2)$ and $(\omega^2, \omega)$, which have multiplicity 2. Also $(1, \omega)$ is a point of multiplicity 1, and applying Proposition B shows that $g_6(X,Y)$ has an absolutely irreducible factor over $GF(4)$.

Next compute $g_6(X,0) = 1+X+X^2+X^3+X^4$ which is irreducible over $GF(2)$. This and the previous paragraph forces (by Proposition 3.8) $g_6(X,Y)$ to either be absolutely irreducible or to have two absolutely irreducible factors of degree 2 over $GF(4)$.

In fact the latter is true. The factors are

$$A(X,Y) = 1+\omega X + X^2 + (\omega + \omega X)Y + Y^2$$

and its conjugate

$$B(X,Y) = 1+\omega^2 X + X^2 + (\omega^2 + \omega^2 X)Y + Y^2.$$

These can be found using a version of Hensel's lemma, which lifts the factorization of $g_6(X,0) = A(X,0)B(X,0)$ into irreducibles over $GF(4)$ to the factorization $g_6(X,Y) = A(X,Y)B(X,Y)$. We will explain this further in section 3.8. This "lifting" was implemented using *Mathematica.* We have proved:

**Theorem 3.5.** *When $k=6$ the polynomial $g_6(X,Y)$ is not absolutely irreducible, and we have the factorization $g_k(X,Y) = A(X,Y)B(X,Y)$, where $A(X,Y)$ and $B(X,Y)$ are absolutely irreducible and are given above.*

**Corollary (Segre).** *When $k=6$ the set $D(k)$ is a hyperoval in $PG(2,2^e)$ if and only if $(2,e)=1$.*

*Proof:* We have to show that $g_6(X,Y)$ has the necessary rational points over $GF(2^e)$ if and only if $e$ is even.

If $e$ is even, then $g_6(\omega^2, \omega) = 0$. Done.

Suppose now that $e > 1$ is any odd integer. We claim that $A(X,Y)$ and $B(X,Y)$ have no rational points over $GF(2^e)$. For suppose that $A(a,b) = 0$ where $a, b \in GF(2^e)$. Visibly we can assume $(a,b) \neq (0,0)$. Then

$$b^2 + b\omega + ab\omega + a^2 + a\omega + 1 = 0,$$

and provided $a + b + ab \neq 0$ this implies $\omega = (a+b+1)^2/(a+b+ab) \in GF(4) \cap GF(2^e)$, which is a contradiction. But if $a+b+ab = 0$ then $a+b+1 = 0 \Rightarrow ab = 1 \Rightarrow 1 + b^{-1} + b = 0 \Rightarrow 1 + b + b^2 = 0$ which is impossible. Similarly for $B(X,Y)$. □

### 3.5. The Case $k \equiv 2 \pmod 4$.

We first make two quick remarks to aid us in moving between $f_k(X,Y)$ and $g_k(X,Y)$. Recall the notation of section 3.3, and suppose that $P = (\alpha, \beta) \neq (1,1)$ is a singular point of $g_k(X,Y)$ such that $F_{2^i}(X,Y) \neq 0$ at $P$. To apply Proposition A to $g_k$ we need to know the greatest common divisor $(G_m(X,Y), G_{m+1}(X,Y))$ where $m = m_P(g_t)$. This can be found from $(F_{2^i}(X,Y), F_{2^i+1}(X,Y))$ as follows.

Again letting $w(X,Y) = (X+Y)(X+1)(Y+1)$, we have

$$f_k(X+\alpha, Y+\beta) = w(X+\alpha, Y+\beta) g_k(X+\alpha, Y+\beta),$$

and so

$$F_{2^i}(X,Y) + F_{2^i+1}(X,Y) + \cdot\cdot = (W_0 + W_1(X,Y) + \cdots)(G_m(X,Y) + G_{m+1}(X,Y) + \cdots)$$

where polynomials with subscript $i$ are 0 or homogeneous of degree $i$.

**Remark 1.** Here we assume $W_0 \neq 0$ which is equivalent to $m = 2^i$. Multiplying out and using (2) gives

$$F_{2^i} = W_0 G_{2^i} = (\sigma X + \tau Y)^{2^i}$$

$$F_{2^i+1} = W_0 G_{2^i+1} + W_1 G_{2^i},$$

where $\sigma^{2^i} = (\beta+1)\alpha^{-2^i}$ and $\tau^{2^i} = (\alpha+1)\beta^{-2^i}$. It follows from these equations that $(F_{2^i}, F_{2^i+1}) = (G_{2^i}, G_{2^i+1})$. □

**Remark 2.** Here we assume $W_0 = 0$ which is equivalent to $m = 2^i - 1$. As in Remark 1 we get

$$F_{2^i} = W_1 G_{2^i-1} = (\sigma X + \tau Y)^{2^i}$$

$$F_{2^i+1} = W_1 G_{2^i} + W_2 G_{2^i-1}.$$

It is clear that (up to scalars) $W_1 = \sigma X + \tau Y$, and so $(F_{2^i}, F_{2^i+1}) = \sigma X + \tau Y$ because $F_{2^i+1}(X,Y)$ has distinct linear factors (an easy exercise, as in Lemma 3 of Chapter 2). Hence $(G_{2^i-1}, G_{2^i}) = 1$. □

Remark 2 will not be used; we include it for completeness.

By Theorem 3.2, the following theorem is equivalent to Theorem 3.1.

**Theorem 3.6.** *If $k \equiv 2 \pmod 4$, $k > 6$, then $g_k(X,Y)$ is absolutely irreducible.*

*Proof:* Suppose $g_k(X,Y) = u(X,Y)v(X,Y)$ over some extension of $GF(2)$

with the degrees of $u$ and $v$ both $\geq 1$. We wish to apply Bezout's theorem to $u$ and $v$, and so we want to compute the intersection multiplicities $I(P, u, v)$.

Write $k = 2\ell$ where $\ell$ is odd. From the table in Section 3.3 we know that the singular points on $g_k$ are $P = (\alpha, \beta) \neq (1,1)$ where $\alpha \neq \beta$, $\alpha \neq 1$, $\beta \neq 1$. Furthermore, there are $(\ell - 1)(\ell - 2)$ of these points, they all have multiplicity 2 on $g_k$ and $f_k$, and $W_0 \neq 0$.

From equation (2) we get

$$F_2(X, Y) = (\sigma X + \tau Y)^2$$

$$F_3(X, Y) = XY(\alpha^{-2} X + \beta^{-2} Y),$$

where $\sigma^2 = (\beta + 1)\alpha^{-2}$ and $\tau^2 = (\alpha + 1)\beta^{-2}$. We would like to know the GCD $(F_2, F_3)$. Clearly this GCD is either 1 or a scalar multiple of $\alpha^{-2}X + \beta^{-2}Y$. If $(F_2, F_3) = 1$, then Remark 1 and Proposition A imply that $I(P, u, v) = 0$.

Suppose for the moment that $F_2(X, Y)$ and $F_3(X, Y)$ are not relatively prime. It follows that $F_2(\beta^{-2}, \alpha^{-2}) = 0$, which implies $(\beta + 1)\beta^{-2} = (\alpha + 1)\alpha^{-2}$. This in turn implies $\alpha^{-1} + \beta^{-1} = (\alpha^{-1} + \beta^{-1})^2 \Rightarrow \alpha^{-1} + \beta^{-1} = 0$ or $1 \Rightarrow \alpha^{-1} + \beta^{-1} = 1 \Rightarrow \beta = \alpha/(\alpha + 1)$. Hence, for each $\alpha$ there is at most one $\beta$ such that $(F_2, F_3) \neq 1$ at $P = (\alpha, \beta)$. Note that if this $\beta$ exists, $(\alpha + 1)^\ell = 1$ because $\alpha$ and $\beta$ are $\ell$-th roots of unity.

This tells us that there are at most $\ell - 1$ points $(\alpha, \beta)$ where $(F_2, F_3) \neq 1$. These points are $(\alpha, \alpha/(\alpha + 1))$ where $\alpha^\ell = 1 = (\alpha + 1)^\ell$.

For all other singular points $P$, Remark 1 and Proposition A imply

$I(P, u, v) = 0$.

To maintain the flow of the argument, we will postpone until the section 3.7 the proof of the following claim. The proof involves performing a resolution of the singularities.

CLAIM: If $P$ is a singular point such that $I(P, u, v) \neq 0$, then $I(P, u, v) = 2$.

Assuming the validity of this statement, we finish the proof as follows. This claim along with the above calculation gives

$$\sum_P I(P, u, v) \leq 2(\ell - 1),$$

(and in fact equality holds if and only if $(\alpha + 1)^\ell = 1$ for all $\ell$-th roots of unity $\alpha \neq 1$). If equality does not hold, then $\sum_P I(P, u, v) \leq 2(\ell - 2)$ since $I(P, u, v) = 0$ or 2. But deg $u$ + deg $v$ = deg $g_k = 2\ell - 2 \Rightarrow$ (deg $u$)(deg $v$) $\geq 2\ell - 3$, and so Bezout's theorem gives a contradiction.

Hence equality must hold, and Bezout's theorem now says

$$(\deg u)(\deg v) = 2\ell - 2 = \deg u + \deg v,$$

which can only happen if deg $u$ = deg $v$ =2. This is precisely what happens when $k = 6$. As $k > 6$, this completes the proof. □

### 3.6. Some Consequences

We state explicitly some consequences of the previous sections for particular values of $k$, including the previously known results of Segre.

First we note some projective equivalences among these hyperovals. If $D(k)$ is a hyperoval, then so is $D(m)$ where $m = 1/k,\ 1-k,\ 1/(1-k),\ (k-1)/k,\ k/(k-1)$, and everything is modulo $q-1$. (If $(k, q-1) \neq 1$ then $D(k)$ is not a hyperoval.) These hyperovals are all projectively equivalent. This follows from manipulations with the determinant in section 3.2, or see [H].

$k = 2$. Then $D(2)$ is a hyperoval in $PG(2, 2^e)$ for all $e$.

This follows from the Corollary to Theorem 3.4.

$k = 4$. Then $D(4)$ is a hyperoval in $PG(2, 2^e)$ if and only if $e$ is odd.

This follows from the Corollary to Theorem 3.4.

$k = 6$. Then $D(6)$ is a hyperoval in $PG(2, 2^e)$ if and only if $e$ is odd.

This follows from the Corollary to Theorem 3.5.

$k = 8$. Then $D(8)$ is a hyperoval in $PG(2, 2^e)$ if and only if $(e, 3) = 1$.

This follows from the Corollary to Theorem 3.4.

$k = 10$. Then $D(10)$ is a hyperoval in $PG(2, 2^e)$ if and only if $e = 5$.

From Theorem 3.6, we can be sure that $D(10)$ is not a hyperoval for all $e \geq e_0$, for some $e_0$. We can compute $e_0$ from equation (1), which says that $e_0$ is the smallest positive integer satisfying $2^{e_0} - (10-3)(10-4)2^{e_0/2} - (10-2)^2 > 3 \cdot 10 - 2$. This gives $e_0 = 11$. From a (computer generated) table [W] of values of $k$ for which $1 + x + \cdots + x^{k-1}$ is a permutation polynomial on $GF(2^e)$, we see that the only value of $e < 11$ is $e = 5$.

In $PG(2, 32)$, $D(10)$ is projectively equivalent to $D(4)$ and $D(8)$.

$k = 12$. Then $D(12)$ is never a hyperoval in $PG(2, 2^e)$.

In section 3.8 we will show that $g_{12}(X, Y)$ is absolutely irreducible. Arguing as above for $k = 10$, we find that $e_0 = 13$ and the statement follows from the table in [W].

$k = 14$. Then $D(14)$ is a hyperoval in $PG(2, 2^e)$ if and only if $e = 4$.

Same proof as for $k = 10$, except here we find that $e_0 = 14$. In $PG(2, 16)$, $D(14)$ is projectively equivalent to $D(2)$ and $D(8)$.

$k = 16$. Then $D(16)$ is a hyperoval in $PG(2, 2^e)$ if and only if $(e, 4) = 1$.

This follows from the Corollary to Theorem 3.4.

$k = 18$. Then $D(18)$ is a hyperoval in $PG(2, 2^e)$ if and only if $e = 7$.

Same proof as for $k = 10$, except here we find that $e_0 = 16$. In $PG(2, 128)$, $D(18)$ is projectively equivalent to $D(16)$ and $D(8)$.

$k = 20$. Then $D(20)$ is a hyperoval in $PG(2, 2^e)$ if and only if $e = 7$, and possibly $e = 16$.

Same proof as for $k = 10$, except here we find that $e_0 = 17$. In $PG(2, 128)$, $D(20)$ is not projectively equivalent to any of Segre's hyperovals, see [H2]. It is equivalent to one of the hyperovals of Glynn [G1].

We can make such a statement and find the value of $e_0$ for any $k \equiv 2 \pmod 4$, but if $k$ is large it becomes harder to check the values of $e < e_0$ by computer.

### 3.7. A Technical Lemma

In this section we prove the claim made in the proof of Theorem 3.6, upon which we have long been procrastinating. The proof will involve "resolving" the singular points $P$ which have the property that $I(P, u, v) \neq 0$. A reference for this is [F] or [A].

Assume the same notation as section 3.5 and the proof of Theorem 3.6. So we are assuming $k = 2\ell$, $\ell$ is odd, $g_k = uv$ is reducible, $P = (\alpha, \beta)$ is a singular point of $g_k(X, Y)$ and has multiplicity 2. Let $P$ be a singular point such that $I(P, u, v) \neq 0$. This implies that $m_P(u) = 1 = m_P(v)$.

To begin we observe that the tangent directions to $u$ and $v$ at $P$ are equal (by the properties of $I(P, u, v)$, this will imply $I(P, u, v) > m_P(u)m_P(v) = 1$). This follows from

CLAIM: $U_1$ is a scalar multiple of $V_1$.

*Proof:* As $I(P, u, v) \neq 0$, we must have $(G_2, G_3) \neq 1$, and so by Remark 1 $(F_2, F_3) \neq 1$. We also have $\beta = \alpha/(\alpha + 1)$ and $W_0 = \alpha + \beta = \alpha\beta$. Because $W_0U_1V_1 = F_2$ we see that $U_1V_1 = (\alpha^{-2}X + \beta^{-2}Y)^2$. It is then easy to see that $U_1$ and $V_1$ are scalar multiples. This completes the proof of the claim. □

Next we compute $G_2(X,Y)$ and $G_3(X,Y)$ explicitly where

$$g_k(X+\alpha, Y+\beta) = G_2 + G_3 + G_4 + \cdots$$

is the expansion of $g_k$ about $P$. We know from the claim that $G_2 = U_1V_1 = (\alpha^{-2}X + \beta^{-2}Y)^2$. As in the beginning of section 3.5 we have $F_3 = W_0G_3 + W_1G_2$, and since $W_1 = (1+\beta)^2X + (1+\alpha)^2Y$ this gives

$$\begin{aligned} W_0G_3 &= \alpha\beta G_3 = F_3 + W_1G_2 \\ \alpha\beta G_3 &= XY(\alpha^{-2}X + \beta^{-2}Y) + \left((1+\beta)^2X + (1+\alpha)^2Y\right)\left(\alpha^{-2}X + \beta^{-2}Y\right)^2 \\ &= (\alpha^{-2}X + \beta^{-2}Y)\left(\frac{1}{\alpha(\alpha+1)}X + \frac{(\alpha+1)^2}{\alpha}Y\right)^2 \end{aligned}$$

after some simplification. This gives $G_3$ in the form we need. Now we may proceed with the blow-up at $P$.

**Lemma.** *If we have $I(P,u,v) \neq 0$ at $P$, then $I(P,u,v) = 2$.*

*Proof:* Compute

$$\begin{aligned} g_k(X+\alpha, XY+\beta) &= G_2(X,XY) + G_3(X,XY) + G_4(X,XY) + \cdots \\ &= X^2 g_k'(X,Y) \end{aligned}$$

where in this proof the omitted terms signified by $\cdots$ will always be monomials of total degree at least 3, and

$$g_k'(X,Y) = G_2(1,Y) + XG_3(1,Y) + X^2G_4(1,Y) + \cdots$$

$$= \alpha^{-4} + \beta^{-4}Y^2 + \frac{X}{\alpha\beta}(\alpha^{-2} + \beta^{-2}Y)\left(\frac{1}{\alpha^2(\alpha+1)^2} + \frac{(\alpha+1)^4}{\alpha^2}Y^2\right)$$

$$+X^2G_4(1,Y)+\cdots$$

is the proper transform of $g_k(X,Y)$. From the expression for $G_2(1,Y)$ we get that $P_1=(0,\alpha^{-2}/\beta^{-2})$ is the only point in the first neighborhood of $P$.

We next want $m_{P_1}(g'_k)$, the multiplicity of $P_1$ on $g'_k$. So compute (where $A=\alpha^{-2}/\beta^{-2}$)

$$\begin{aligned}
g'_k(X,Y+A) &= \alpha^{-4}+\beta^{-4}\,(Y+A)^2+\frac{X}{\alpha\beta}\Big(\alpha^{-2}\\
&\quad+\beta^{-2}(Y+A)\Big)\left(\frac{1}{\alpha^2(\alpha+1)^2}+\frac{(\alpha+1)^4}{\alpha^2}\,(Y+A)^2\right)\\
&\quad+X^2G_4\,(1,Y+A)+\cdots\\
&=\frac{X}{\alpha\beta}(\beta^{-2}Y)\left(\frac{1}{\alpha^2(\alpha+1)^2}+\frac{(\alpha+1)^4}{\alpha^2}Y^2+\frac{(\alpha+1)^4}{\alpha^2}\frac{\alpha^{-4}}{\beta^{-4}}\right)\\
&\quad+\beta^{-4}Y^2+X^2D+\cdots\\
&=\left(\beta^{-2}Y^2+\frac{1}{\alpha(\alpha+1)^2\beta^3}XY+DX^2\right)+\cdots
\end{aligned}$$

after some simplification, and where $D$ is the constant term in $G_4(1,Y+A)$.

This shows that $m_{P_1}(g'_k)=2$, but the key observation here is that the coefficient of $XY$ is nonzero. This means that $g'_k$ has two different tangent directions at $P_1$, and so any points $Q$ in the first neighborhood of $P_1$ (the second neighborhood of $P$) are to be considered simple points on $g_k$. So either $m_Q(u)=0$ or $m_Q(v)=0$ for these points $Q$. By the refined version of Bezout's theorem, see [A] or [F], we get

$$I(P,u,v)=m_P(u)m_P(v)+m_{P_1}(u)m_{P_1}(v)=1+1=2,$$

and this completes the proof. □

## 3.8. A Conjecture and Some Evidence

With limited but nonzero confidence we advance the following conjecture:

*For any even positive integer $k$, $k \neq 2^i$ or 6, the polynomial $g_k(X,Y)$ is absolutely irreducible.*

This would imply that there are at most a finite number of $q$ such that $D(k)$ is a hyperoval in $PG(2,q)$. The preceding sections provide evidence for the conjecture. This conjecture itself provides evidence for conjecture B in [G1] concerning monomial hyperovals.

Now we fulfill the promise of section 3.6, and prove the absolute irreducibility of $g_{12}(X,Y)$. We shall prove the same result for $k = 20, 24, 28$ at the same time. The methods can be used for other values of $k$ and other polynomials in general.

We will use the following proposition, a form of Hensel's lemma (see [JW]). We say that a polynomial $h(X,Y)$ is *regular* in $X$ when the degree of $h(X,0)$ as a polynomial in $X$ is equal to the total degree of $h(X,Y)$. We remark that all factors $q(X,Y)$ of such a polynomial $h(X,Y)$ must also be regular in $X$.

**Proposition 3.7.** *Let $h(X,Y)$ be a polynomial over a field $\mathbf{F}$ that is regular in $X$. If*

$$h(X,0) = a_0(X)b_0(X)$$

*where $a_0(X)$ and $b_0(X)$ are relatively prime polynomials in $\mathbf{F}[X]$, then there* *is at most one pair $A(X,Y), B(X,Y)$ of polynomials over any extension of* $\mathbf{F}$ *with the properties that*

$$h(X,Y) = A(X,Y)B(X,Y), \quad A(X,0) = a_0(X), \quad \textit{and} \quad B(X,0) = b_0(X).$$

*If such polynomials $A(X,Y)$ and $B(X,Y)$ exist, then all their coefficients lie in* $\mathbf{F}$.

For a proof see [JW]. The construction of $A(X,Y)$ and $B(X,Y)$ can be implemented with *Mathematica.* This is what we did in section 3.4 when we found the factors of $g_6(X,Y)$.

Next we give another well known criterion for irreducibility.

**Proposition 3.8.** *Let $h(X,Y)$ be a polynomial of degree $n$ over a field* $\mathbf{F}$ *that is regular in $X$. Writing*

$$h(X,Y) = \sum_{i=0}^{n} c_i(X)Y^i,$$

*if $c_0(X)$ is irreducible over* $\mathbf{F}$*, then $h(X,Y)$ is irreducible over* $\mathbf{F}$.

*Proof:* Suppose $p(X,Y) = \sum_{i=0}^{r} p_i(X)Y^i$, $q(X,Y) = \sum_{i=0}^{s} q_i(X)Y^i$, and that $h(X,Y) = p(X,Y)q(X,Y)$ in $\mathbf{F}[X,Y]$, $0 < r, s < n$. Clearly then $c_0(X) = p_0(X)q_0(X)$. By regularity of $h$, $p_0(X)$ has degree $r$ and so is a proper divisor of $c_0(X)$. □

We will also use the following Lemma about the structure of the polynomials $g_k(X,Y)$.

**Lemma 3.9.** *If we write*

$$g_k(X,Y) = \sum_{i=0}^{k-2} c_i(X)Y^i,$$

*then* $c_i(X) = 1 + X + X^2 + \cdots + X^{k-2-i}$.

*Proof:* First calculate

$$c_0(X) = g_k(X,0) = \frac{X^k + X}{X(X+1)} = 1 + X + X^2 + \cdots + X^{k-2}.$$

Then check from the definitions that $g_k(X,Y) = c_0(X) + Yg_{k-1}(X,Y)$. □

**Corollary 3.10.** *If* 2 *is primitive modulo* $k-1$, *then* $g_k(X,Y)$ *is irreducible over* $GF(2)$.

*Proof:* Immediate from the last two results and the fact that $1 + X + \cdots + X^n$ is irreducible over $GF(2)$ if and only if 2 is primitive modulo $n+1$. □

For example, when $k$=12,20,60,68,84, if we apply Corollary 3.10 and Corollary 3.3 we may conclude that $g_k(X,Y)$ is either absolutely irreducible or has two absolutely irreducible factors over $GF(4)$.

We need the following Corollary to ensure that we can use Proposition 3.7.

**Corollary 3.11.** 1) *The polynomials* $g_k(X,Y)$ *are regular in* $X$ *for all* $k$.
2) *If* $g_k(X,Y) = A(X,Y)B(X,Y)$ *is reducible, then* $A(X,0)$ *and* $B(X,0)$ *are relatively prime.*

*Proof:* The first assertion is obvious. The second assertion is due to the fact that $c_0(X)$ and $c_1(X)$ are relatively prime, and this is because their roots are the nontrivial $k-1$ and $k-2$ roots of unity respectively. Then note that any divisor of $A(X,0)$ and $B(X,0)$ would also divide $c_0(X) = A(X,0)B(X,0)$ and $c_1(X)$. □

**Theorem 3.12.** *$g_k(X,Y)$ is absolutely irreducible for $k = 12, 20, 24, 28$.*

*Proof:* As we stated after Corollary 3.10, for $k = 12, 20$, $g_k(X,Y)$ is either absolutely irreducible or has two absolutely irreducible factors over $GF(4)$ of degrees 5,9 respectively.

For $k = 12$, factor $c_0(X) = 1 + X + X^2 + \cdots + X^{10} = (1 + \omega^2 X + X^2 + X^3 + \omega X^4 + X^5)(1 + \omega X + X^2 + X^3 + \omega^2 X^4 + X^5)$ into irreducibles over $GF(4)$, and try to lift this factorization to a factorization of $g_{12}(X,Y)$ with Proposition 3.7. This was checked with *Mathematica* and did not work. Hence $g_{12}(X,Y)$ is absolutely irreducible.

For $k = 20$, factor $c_0(X) = 1 + X + X^2 + \cdots + X^{18} = a(X)\overline{a}(X)$ into irreducibles over $GF(4)$, where $a(X) = 1 + \omega^2 X + \omega^2 X^3 + \omega^2 X^4 + \omega X^5 + \omega X^6 + \omega X^8 + X^9$. Again try to lift the factorization — it does not work. Hence $g_{20}(X,Y)$ is absolutely irreducible by Proposition 3.7.

For $k = 24$ we have a slightly different argument. Factor $c_0(X) = 1 + X + X^2 + \cdots + X^{22} = a_0(X)b_0(X)$ into irreducibles over $GF(2)$, where $a_0$ and

$b_0$ have degree 11. Attempting to lift $a_0(X)$ and $b_0(X)$ to find a factorization fails, so we conclude from Proposition 3.7 that $g_{24}(X, Y)$ is irreducible over $GF(2)$. Then Proposition B (3) implies that if $g_{24}$ is not absolutely irreducible, it must factor into eleven quadratics over $GF(2^{11})$ or two degree 11 factors over $GF(4)$. The latter is impossible by the factorization of $c_0(X)$.

By the table in section 3, the point $(1, 1)$ has multiplicity 6 on $g_{24}(X, Y)$. Proposition B shows that there must be an absolutely irreducible factor with coefficients in $GF(2^6)$, and possibly a subfield.

The previous two paragraphs imply that $g_{24}(X, Y)$ is absolutely irreducible.

For $k = 28$, factor $c_0(X) = 1 + X + X^2 + \cdots + X^{26} = (1 + X^9 + X^{18})(1 + X^3 + X^6)(1 + X + X^2)$ into irreducibles over $GF(2)$. Trying to lift each possibility fails, so $g_{28}(X, Y)$ is irreducible over $GF(2)$ by Proposition 3.7.

Since $28 \equiv 4 \pmod 8$, there is an absolutely irreducible factor over $GF(4)$ by Corollary 3.3.

The previous two paragraphs force $g_{28}$ to either be absolutely irreducible or to have two absolutely irreducible factors over $GF(4)$ of degree 13. Factoring $c_0(X)$ over $GF(4)$ and trying to lift all possibilities (there are only four) fails. By Proposition 3.7, $g_{28}(X, Y)$ is absolutely irreducible. □

We can also prove the above cases by hand.

Proposition B proves the hyperoval result for $k \equiv 4 \pmod 8$ or $k \equiv 1 \pmod 3$, and $e$ even. This provides evidence for conjecture A of [G1], which states that the only hyperovals of the form $D(k)$ when $e$ is even occur when $k = 2^i$.

It seems that the argument of Theorem 3.6 does not easily generalise to the case $k \equiv 0 \pmod 4$. Not least of the complications is that it is not true — some exceptions are $k = 2^i$. We conjecture that these are the only exceptions. Another complication is that there are many more singular points, and the intersection multiplicities become harder to handle.

# CHAPTER 4

# Binary Codes and Relative Difference Sets From the Integers Modulo 4

## 4.1. Introduction.

In this chapter we shall use Galois rings over the integers modulo 4 to construct a relative difference set and also some binary codes. We shall use the techniques of the previous chapters to determine exactly the minimum distance of these binary codes.

We now give an introduction to the theory of Galois rings over $\mathbf{Z}_4$, the integers modulo 4, which can be found for example in [HKCSS].

The Galois ring $GR(4^m)$ is an extension of $\mathbf{Z}_4$ of degree $m$ containing a $(2^m - 1)^{\text{st}}$ root of unity. To begin, let $h_2(X) \in GF(2)[X]$ be a primitive irreducible polynomial of degree $m$. Then there is a unique monic polynomial $h(X) \in \mathbf{Z}_4[X]$ of degree $m$ such that $h(X) \equiv h_2(X) \pmod 2$, and $h(X)$ divides $X^{2^m-1} - 1$ in $\mathbf{Z}_4[X]$. Let $\xi$ be a root of $h(X)$, i.e., $\xi$ is the congruence class of $X$ in the ring $\mathbf{Z}_4[X]/(h(X))$, so that $\xi^{2^m-1} = 1$. The *Galois ring* $GR(4^m)$ is defined to be $\mathbf{Z}_4[\xi]$, which is the ring $\mathbf{Z}_4[X]/(h(X))$. Every element $c \in GR(4^m)$ has a unique 2-adic representation $c = a + 2b$, where $a$ and $b$ are taken from the set $D = \{0, 1, \xi, \xi^2, \ldots, \xi^{2^m-2}\}$. The *Frobenius map* $f$ from $GR(4^m)$ to itself is the ring automorphism that takes any element $c = a + 2b \in GR(4^m)$ to $c^f = a^2 + 2b^2$. This map $f$ generates the Galois group of $GR(4^m)$ over $\mathbf{Z}_4$, and $f^m = 1$. The *relative trace* from $GR(4^m)$ to $\mathbf{Z}_4$ is defined by

$$T(c) = c + c^f + \cdots + c^{f^{m-1}}, \quad c \in GR(4^m).$$

One essential difference between the Galois ring $R = GR(4^m)$ and the Galois field $F = GF(2^m)$ is that $R$ contains zero divisors. These are elements of the radical $2R$ which is the unique maximal ideal in $R$. Let $\mu : R \to R/2R$ denote reduction modulo 2. Then $\omega = \mu(\xi)$ is a root of $h_2(x)$, and we can identify $R/2R$ with $GF(2^m)$, taking the elements of $GF(2^m)$ to be $\mu(D) = \{0, 1, \omega, \omega^2, \ldots, \omega^{2^m-2}\}$. We shall often denote $\mu(x)$ by $\overline{x}$.

### 4.2. Relative Difference Sets and the Desarguesian Plane.

In this section we use the Galois ring to construct a relative difference set. From this we construct an affine plane, and we prove that this plane is Desarguesian.

A *relative difference set* with parameters $(n, n, n, 1)$ is an $n$-subset $D$ of a group $G$ of order $n^2$ with a normal subgroup $N$ of order $n$ such that an element $g \neq 0$ of $G$ has a (necessarily unique) representation $g = d - d'$ $(d, d' \in D)$ if and only if $g \notin N$.

It is shown in [G] (see also [J]) that if $n$ is even and $G$ is abelian, then $n$ must be a power of 2, $G$ must be isomorphic to a direct sum of copies of $\mathbf{Z}_4$, and $N$ must be elementary abelian.

Let $G = R = \mathbf{Z}_4[\xi]$, let $N = 2R$ be the maximal ideal, and let

$$D = \{0, 1, \xi, \xi^2, \ldots, \xi^{2^m - 2}\}$$

be as above. We claim that $D$ is a $(2^m, 2^m, 2^m, 1)$ relative difference set in $R$. Of course, $R$ is isomorphic to $(\mathbf{Z}_4)^m$ as an additive group.

To show that $D$ is a relative difference set in $R$, we must show 1) that the differences $\xi^i - \xi^j$ are distinct, and also 2) that $\xi^i - \xi^j$ is never an element of $N = 2R = 2D$. This was shown in [HKCSS], page 308. It is also used in proving that the 'Preparata' codes have minimum distance 6.

The proof of 2) is simple: if $\xi^i - \xi^j = 2y$, then reducing modulo 2 gives $\omega^i + \omega^j = 0$ in the finite field $GF(2^m)$, which is impossible.

We can now construct an affine plane of order $2^m$, whose points are the

$4^m$ elements of $R$, and whose lines are the $4^m$ translates of $D$ by elements of $R$, and also the $2^m$ cosets of $N$ in $R$. Call this affine plane $A$. Note that by the difference set property, the elements of $D$ are a set of coset representatives for $N$ in $R$.

We introduce some notation: since $\xi^i + \xi^j \in R$, we may write it in the form $a + 2b$, say

$$\xi^i + \xi^j = \xi^{g(i,j)} + 2\sqrt{\xi^{i+j}}.$$

The fact that the 2-ish part is $\sqrt{\xi^{i+j}}$ follows by squaring $\xi^i + \xi^j$, applying Frobenius and subtracting these two equations. We remark that reducing this equation mod 2 gives $\omega^i + \omega^j = \omega^{g(i,j)}$ in $GF(2^m)$.

**Theorem 4.1.** *The affine plane $A$ is isomorphic to the Desarguesian affine plane $AG_2(2^m)$.*

*Proof:* We define a $1-1$ correspondence $\psi\colon GR(4^m) \to GF(2^m)^2$ by

$$\psi(\xi^i + 2\xi^j) = \left(\omega^{2j}, \omega^i\right)$$

with the convention that either $\xi^i$ or $\xi^j$ could be zero. We claim that $\psi$ is an isomorphism of the affine planes $A$ and $AG_2(2^m)$.

We must show that $\psi$ takes lines of $A$ to lines of $AG_2(2^m)$. Let $r = \xi^i + 2\xi^j$

and consider the line

$$\begin{aligned} D+r &= \{r, r+1, r+\xi, r+\xi^2, \ldots, r+\xi^k, \ldots\} \\ &= \{\xi^i+2\xi^j, 1+\xi^i+2\xi^j, \xi+\xi^i+2\xi^j, \ldots, \xi^k+\xi^i+2\xi^j, \ldots\} \\ &= \{\xi^i+2\xi^j, \xi^{g(0,i)}+2(\xi^j+\sqrt{\xi^i}), \ldots, \xi^{g(k,i)}+2(\xi^j+\sqrt{\xi^{i+k}}), \ldots\}. \end{aligned}$$

Then

$$\psi(D+r) = \{(\omega^{2j}, \omega^i), (\omega^{2j}+\omega^i, \omega^{g(0,i)}), \ldots, (\omega^{2j}+\omega^{i+k}, \omega^{g(k,i)}), \ldots\}.$$

Translating the first point to the origin, this is

$$\begin{aligned} &= \{(0,0), (\omega^i, \omega^{g(0,i)}+\omega^i), \ldots, (\omega^{i+k}, \omega^{g(k,i)}+\omega^i), \ldots\} \\ &= \{(0,0), (\omega^i, 1), \ldots, (\omega^{k+i}, \omega^k), \ldots\}. \end{aligned}$$

But this is certainly a line in $AG_2(2^m)$ since the ratio of the first to the second coordinate of each point is $\omega^i$.

It is clear that

$$\psi(N) = \{(0,0), (1,0), (\omega, 0), \ldots, (\omega^k, 0), \ldots\}$$

and that any coset $N+\xi^i$ of $N$ is mapped under $\psi$ to the translate of this line by $(0, \omega^i)$. □

We remark that $A$ has $4^m$ obvious automorphisms of order 4, namely the translations by elements of $A$, and so $Aut(AG_2(2^m))$ contains a copy of $(\mathbf{Z_4})^m$.

In fact, these automorphisms are contained in the subgroup

$$\left\{f \in Aut(AG_2(2^m)) : f(x) = Bx + v, B = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}\right\}$$

where $a \in GF(2^m), v \in GF(2^m)^2$. This subgroup has order $2^{3m}$. Any automorphism of the form $f(x) = Bx + v$ has order 4, provided $B$ is a matrix over $GF(2^m)$ of order 2 and $v \neq 0$.

### 4.3. Cyclic Codes over $\mathbf{Z_4}$ and Absolute Irreducibility.

In this section we determine the exact minimum distance of some binary codes which are obtained from codes over $\mathbf{Z_4}$ via the Gray map. First we explain this construction. More details can be found in [HKCSS].

A linear code over $\mathbf{Z_4}$ with block length $N$ is an additive subgroup of $(\mathbf{Z_4})^N$. We define an inner product on $(\mathbf{Z_4})^N$ by $(a, b) = a_1 b_1 + \cdots + a_N b_N$ (mod 4), and then the notions of *dual code* ($C^{\perp}$), *self-orthogonal code* ($C \subseteq C^{\perp}$) and *self-dual code* ($C = C^{\perp}$) are defined in the standard way. We shall say that two $\mathbf{Z_4}$-linear codes are *equivalent* if one can be obtained from the other by permuting the coordinates and (if necessary) changing the signs of certain coordinates. The *automorphism group* $Aut(C)$ consists of all monomial transformations (coordinate permutations and sign changes) that preserve the set of codewords.

Several weight enumerators are associated with a $\mathbf{Z_4}$-linear code $C$. The *complete weight enumerator* (or c.w.e.) of $C$ is

$$cwe_C(W,X,Y,Z) = \sum_{a\in C} W^{n_0(a)} X^{n_1(a)} Y^{n_2(a)} Z^{n_3(a)} ,$$

where $n_i(a)$ is the number of components of $a$ that are congruent to $i$ modulo 4. Since a monomial transformation may change the sign of a component, the appropriate weight enumerator for an equivalence class of codes is the *symmetrized weight enumerator* (or s.w.e.) given by

$$swe_C(W,X,Y) = cwe_C(W,X,Y,X) .$$

The *MacWilliams identity* over $\mathbf{Z_4}$ expresses the symmetrized weight enumerator of the dual code $C^{\perp}$ in terms of $swe_C(W,X,Y)$:

$$swe_{C^{\perp}}(W,X,Y) = \frac{1}{|C|} swe_C(W+2X+Y, W-Y, W-2X+Y) .$$

In [HKCSS] they define the Gray map $\phi$, which is a distance preserving map or isometry from $((\mathbf{Z_4})^N$, Lee distance) to $(GF(2)^{2N}$, Hamming distance). Recall that the *Lee weights* of the elements $0,1,2,3$ of $\mathbf{Z_4}$ are respectively $0,1,2,1$, and that Lee weight of a vector $a \in (\mathbf{Z_4})^N$ is just the rational sum of the Lee weights of its components. This weight function defines the *Lee metric* on $(\mathbf{Z_4})^N$.

The Gray map $\phi$ is defined on $\mathbf{Z_4}$ to $GF(2)^2$ by

$$0 \mapsto 00$$

$$1 \mapsto 01$$

$$2 \mapsto 11$$

$$3 \mapsto 10$$

and $\phi$ is extended to $(\mathbf{Z}_4)^N$ in the obvious way. It is evidently distance preserving. Note that this definition is not quite the same as in [HKCSS]; they would compose this definition with the permutation

$$(2, N+1)(3,2)(4, N+2)(5,3)\cdots(2i, N+i)(2i+1, i+1)\cdots(N, 2N).$$

If $C$ is $\mathbf{Z}_4$-linear, since $c \in C$ implies $-c \in C$ it follows that $\phi(C)$ is fixed under the "swap" map $\sigma$ that interchanges the $2i-1$ and $2i$ coordinates in each codeword. In other words, $\sigma$ applies the permutation

$$(1,2)(3,4)\cdots(2i-1, 2i)\cdots(2N-1, 2N)$$

to the coordinates. This is a fixed point free involution in the automorphism group of $\phi(C)$.

The binary image $\phi(C)$ of a $\mathbf{Z}_4$-linear code $C$ under the Gray map need not be $GF(2)$-linear, so that the dual code may not even be defined.

A binary code $C_2$ is said to be *distance invariant* if the Hamming weight distribution of the translate $u+C_2$, $u \in C_2$ is independent of $u$. A binary linear code is clearly distance invariant, but so is the binary image $\phi(C)$ of a $\mathbf{Z}_4$-linear code $C$ under the Gray map. It is shown in [HKCSS] that the Hamming weight distributions of $\phi(C)$ and $\phi(C^{\perp})$ are MacWilliams transforms of one another.

Necessary and sufficient conditions for a binary code to be the Gray image of a $\mathbf{Z}_4$-linear code, and for the Gray image of a $\mathbf{Z}_4$-linear code to be $GF(2)$-linear, are given in [HKCSS]. They proved that binary Reed-Muller codes of length $2^m$ and orders $0, 1, 2, m-1, m$ are Gray images of $\mathbf{Z_4}$-linear codes, but that extended Hamming codes and the $[24, 12, 8]$ binary Golay code are not. Another theorem on such restrictions on a binary code is given in [CMG1].

We now use parity checks over the Galois ring $R$ to define cyclic codes over $\mathbf{Z_4}$. For example, we may consider the code which consists of all $2^m$-tuples over $\mathbf{Z_4}$ which are orthogonal to every row of the matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 & \cdots & 1 \\ 0 & 1 & \xi & \xi^2 & \cdots & \xi^i & \cdots & \xi^{2^m-2} \end{pmatrix}.$$

The Gray image of this code is the 'Preparata' code, an optimal code of minimum distance 6.

Also shown in [HKCSS] is that the code with parity check matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 & \cdots & 1 \\ 0 & 1 & \xi & \xi^2 & \cdots & \xi^i & \cdots & \xi^{2^m-2} \\ 0 & 2 & 2\xi^3 & 2\xi^6 & \cdots & 2\xi^{3i} & \cdots & 2\xi^{3(2^m-2)} \end{pmatrix}$$

is the Goethals code of minimum distance 8.

We wish to consider the $\mathbf{Z_4}$-linear codes $C_2$, $C$, and $C_3$, of length $2^m$, with respective parity check matrices

$$\begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 & \cdots & 1 \\ 0 & 1 & \xi & \xi^2 & \cdots & \xi^i & \cdots & \xi^{2^m-2} \\ 0 & 1 & \xi^3 & \xi^6 & \cdots & \xi^{3i} & \cdots & \xi^{3(2^m-2)} \end{pmatrix},$$

$$\begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 & \cdots & 1 \\ 0 & 1 & \xi & \xi^2 & \cdots & \xi^i & \cdots & \xi^{2^m-2} \\ 0 & 1 & \xi^3 & \xi^6 & \cdots & \xi^{3i} & \cdots & \xi^{3(2^m-2)} \\ 0 & 2 & 2\xi^5 & 2\xi^{10} & \cdots & 2\xi^{5i} & \cdots & 2\xi^{5(2^m-2)} \end{pmatrix},$$

and

$$\begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 & \cdots & 1 \\ 0 & 1 & \xi & \xi^2 & \cdots & \xi^i & \cdots & \xi^{2^m-2} \\ 0 & 1 & \xi^3 & \xi^6 & \cdots & \xi^{3i} & \cdots & \xi^{3(2^m-2)} \\ 0 & 1 & \xi^5 & \xi^{10} & \cdots & \xi^{5i} & \cdots & \xi^{5(2^m-2)} \end{pmatrix}.$$

The codes $C_2$ and $C_3$ are the Hensel lifts of the extended 2- and 3-error-correcting BCH codes respectively.

We will first study the code $C$. It is proved in [CMG2] that $C$ is invariant under the affine group, which we now define. It is well known (see [MWS]) that the extended BCH codes are invariant under the doubly transitive group $\mathcal{G}$ of affine permutations of $GF(2^m)$ given by

$$\overline{x} \rightarrow \overline{a}\,\overline{x} + \overline{b}\ , \tag{4.1}$$

where $\overline{a}, \overline{b} \in GF(2^m)$ and $\overline{a} \neq 0$. Following [HKCSS] we can describe $\mathcal{G}$ in terms of $D = \{0, 1, \xi, \xi^2, \ldots, \xi^{2^m-2}\}$ rather than the field $GF(2^m)$. Now $\mathcal{G}$ consists of permutations of $D$ given by

$$x \rightarrow (ax+b)^{2^m}\ , \tag{4.2}$$

where $a, b \in D$ and $a \neq 0$. Note that

$$\mu(ax+b) = \mu((ax+b)^{2^m}) = \overline{ax} + \overline{b}\ ,$$

so that equations (4.1) and (4.2) are describing the same permutation. The order of $\mathcal{G}$ is $2^m(2^m-1)$.

We now study conditions under which $C$ has a codeword of weight 8 with 8 entries equal to $+1$ and the rest 0, i.e., a codeword of type $1^8 0^{2^m-8}$.

We suppose that the entries +1 are indexed by elements $x_1, \ldots, x_8$ in $D$ and we write

$$f(z) = \prod_{i=1}^{8}(z - x_i) = z^8 - \sigma_1 z^7 + \sigma_2 z^6 - \sigma_3 z^5 + \sigma_4 z^3 + \sigma_6 z^2 - \sigma_7 z + \sigma_8 \ .$$

After applying an affine permutation we may suppose $x_1 = 0$ so that $\sigma_8 = 0$. The parity checks that define $C$ give

$$S_1 = S_2 = S_3 = S_4 = S_6 = 0 \quad \text{and} \quad 2S_5 = 0 \ .$$

Now we apply Newton's Identities:

$$S_1 - \sigma_1 = 0$$

gives $\sigma_1 = 0$.

$$S_2 - S_1\sigma_1 + 2\sigma_2 = 0$$

gives $2\sigma_2 = 0$.

$$S_3 - S_2\sigma_1 + S_1\sigma_2 + \sigma_3 = 0$$

gives $\sigma_3 = 0$.

$$S_5 - S_4\sigma_1 + S_3\sigma_2 - S_2\sigma_3 + S_1\sigma_4 - \sigma_5 = 0$$

gives $2\sigma_5 = 0$.

$$S_6 - S_5\sigma_1 + S_4\sigma_2 - S_3\sigma_3 + S_2\sigma_4 - S_1\sigma_5 + 2\sigma_6 = 0$$

gives $2\sigma_6 = 0$. The reduction of $f(z)$ modulo 2 is the linearized polynomial

$$\overline{f}(z) = z^8 + \overline{\sigma}_4 z^4 + \overline{\sigma}_7 z \ .$$

Since $\overline{f}(z)$ is a linearized polynomial, the set of roots is closed under addition and $\overline{x}_1, \ldots, \overline{x}_8$ is a 3-dimensional subspace. After applying an affine transformation we may suppose

$$\{\overline{x}_1, \ldots, \overline{x}_8\} = \{0, 1, x, 1+x, y, 1+y, x+y, x+y+1\} ,$$

for some $x, y \in GF(2^m)$. However it is not true that every 3-dimensional subspace of this form determines a codeword of weight 8. Direct calculation gives

$$\overline{f}(z) = z^8 + \overline{\sigma}_4 z^4 + \overline{\sigma}_6 z^2 + \overline{\sigma}_7 z ,$$

where

$$\begin{aligned} \overline{\sigma}_4 &= 1 + x^2 + x^4 + xy + x^2y + y^2 + xy^2 + x^2y^2 + y^4 , \\ \overline{\sigma}_6 &= x^2 + x^4 + y^2 + y^4 + xy + x^2y^2 + x^4y + xy^4 + x^4y^2 + x^2y^4 , \\ \text{and} \quad \overline{\sigma}_7 &= x^2y + xy^2 + x^4y + xy^4 + x^4y^2 + x^2y^4 . \end{aligned}$$

The field elements $x, y$ must be such that $\overline{\sigma}_6 = 0$.

**Lemma 4.2.** *There exists a codeword in $C$ with Lee composition $1^8 0^{2^m-8}$ if and only if there exist distinct $x, y \in GF(2^m)$, neither of which is 0 or 1, such that*

$$x^2 + x^4 + y^2 + y^4 + xy + x^2y^2 + x^4y + xy^4 + x^4y^2 + x^2y^4 = 0 .$$

*Proof:* Necessity has already been proven, since this polynomial is the elementary symmetric function $\overline{\sigma}_6$ that appears above. The entries $+1$ in $c$ are indexed by field elements taken from the set $S = \{0, 1, x, 1+x, y, 1+y, x+y, 1+x+y\}$. We suppose that $s \in S$ is obtained from $z_s \in D$ by reduction modulo 2. To prove sufficiency we need to show

$$S_1 = \sum_{s \in S} z_s = 0 \ , \tag{4.3}$$

$$S_3 = \sum_{s \in S} z_s^3 = 0 \ , \tag{4.4}$$

$$2S_5 = 2\sum_{s \in S} z_s^5 = 0 \ . \tag{4.5}$$

Now let $S_r \in GR(4^m)$ denote the $r^{\text{th}}$ power sum symmetric function of the elements $z_s$, and let $\sigma_r \in GR(4^m)$ denote the $r^{\text{th}}$ elementary symmetric function of the elements $z_s$. We may reduce $S_r$ and $\sigma_r$ modulo 2 to obtain $\overline{S}_r$ and $\overline{\sigma}_r$ respectively. We have previously shown that

$$\overline{\sigma}_1 = \overline{\sigma}_2 = \overline{\sigma}_3 = \overline{\sigma}_5 = \overline{\sigma}_6 = 0 \ .$$

We apply Newton's Identities to obtain

$$S_1 - \sigma_1 = 0 \tag{4.6}$$

$$S_2 - S_1\sigma_1 + 2\sigma_2 = 0 \tag{4.7}$$

$$S_3 - S_2\sigma_1 + S_1\sigma_2 + \sigma_3 = 0 \tag{4.8}$$

$$S_5 - S_4\sigma_1 + S_3\sigma_2 - S_2\sigma_3 + S_1\sigma_4 - \sigma_5 = 0 \ . \tag{4.9}$$

We begin by writing $S_1 = a + 2b$, where $a, b \in D$. Passing modulo 2 gives $\overline{a} = \overline{S}_1 = \sigma_1 = 0$, and so $a = 0$. Now $2b^2 = 2\sigma_2$, and since $\overline{\sigma}_2 = 0$ we have $b = 0$. This proves equation (4.3).

Now (4.7) and (4.8) imply $S_2 = 0$ and $S_3 = \sigma_3$, so we need to prove that $\sigma_3 = 0$. Again we write $\sigma_3 = a+2b$, where $a, b \in D$. Then $\overline{a} = \overline{\sigma}_3 = 0$ so $a = 0$. Direct calculation gives $2b^2 = 2(\sigma_1\sigma_5 + \sigma_2\sigma_4 + \sigma_6)$, and since $\overline{\sigma}_1 = \overline{\sigma}_2 = \overline{\sigma}_6 = 0$ we have $b = 0$. This proves (4.4).

Now (4.9) implies $S_5 = \sigma_5$. To prove (4.5) we need to show $2S_5 = 0$, but this follows directly from $\overline{\sigma}_5 = 0$. This completes the proof. □

**Remark.** The proof of Lemma 4.2 shows that $S_5 = 2b$ for some $b \in D$. We have

$$2b^2 = 2(\sigma_1\sigma_9 + \sigma_2\sigma_8 + \sigma_3\sigma_7 + \sigma_4\sigma_6 + \sigma_{10}) ,$$

and each of the terms on the right-hand side is equal to 0. Hence $S_5 = 0$. This proves that if there exist $x$, $y$ as in the statement of Lemma 4.2, then there is a codeword of type $1^8 0^{2^m-8}$ in the Hensel lift of the extended 3-error-correcting BCH code. This is the linear code over $\mathbf{Z_4}$ consisting of all sequences $(c_x)$ satisfying

$$\sum_{x \in D} c_x = \sum_{x \in D} c_x x = \sum_{x \in D} c_x x^3 = \sum_{x \in D} c_x x^5 = 0 .$$

We now apply Bezout's Theorem to prove that

$$h(x,y) = x^2 + x^4 + y^2 + y^4 + xy + x^2y^2 + x^4y + xy^4 + x^4y^2 + x^2y^4$$

is absolutely irreducible. First we check that $h(x,y)$ has no linear factors over the algebraic closure $\overline{GF(2)}$. This is easily verified by checking that

$h(x, cx + d)$ cannot be identically zero for any $c, d \in \overline{GF(2)}$. Since Bezout's Theorem applies to projective plane curves, we must consider the projective version of $h(x, y)$, which we denote by

$$h(x, y, z) = x^2z^4+y^2z^4+x^4z^2+y^4z^2+x^4y^2+x^2y^4+x^4yz+xy^4z+xyz^4+x^2y^2z^2 .$$

If $h(x, y, z)$ is not absolutely irreducible, then

$$h(x, y, z) = u(x, y, z)v(x, y, z)$$

where $u(x, y, z)$ has degree 2 or 3, and $v(x, y, z)$ has degree 4 or 3 respectively. Bezout's Theorem implies $\sum_P I(P, u, v) = 8$ or 9.

If a point $P$ has intersection multiplicity $I(P, u, v) \neq 0$, then the multiplicity $m_P(h) = m_P(u) + m_P(v) \geq 2$, and so $P$ is a singular point of $h(x, y, z)$. This means we need only sum over singular points of $h(x, y, z)$. These are found by simultaneously solving

$$\frac{\partial h}{\partial x} = y^4z + yz^4 = 0, \quad \frac{\partial h}{\partial y} = x^4z + xz^4 = 0, \quad \frac{\partial h}{\partial z} = x^4y + xy^4 = 0 .$$

The only solutions that also lie on the curve, i.e., also satisfy $h(x, y, z) = 0$, are $(x, y, z) =$ (1,0,0), (0,1,0), (0,0,1), (1,1,0), (1,0,1), (0,1,1) and (1,1,1).

The lowest degree forms in $h(x + 1, y, z)$, $h(x + 1, y + 1, z)$, and $h(x + 1, y + 1, z + 1)$ are $y^2 + yz + z^2$, $x^2 + z^2 + xz + yz$ and $x^2 + y^2 + z^2 + xy + xz + yz$ respectively. Symmetry of $h(x, y, z)$ implies that all singular points $P$ have multiplicity 2, that is, $m_P(h) = 2 = m_P(u) + m_P(v)$.

Since each of these forms has distinct linear factors, it follows that

$$I(P,u,v) = m_P(u)m_P(v) = 0 \text{ or } 1 .$$

Since there are only 7 singular points we have $\sum_P I(P,u,v) \le 7$, which is the desired contradiction.

**Theorem 4.3.** *For $m \ge 7$, there exist distinct field elements $a, b \in GF(2^m)$, with $a, b \ne 0$ or 1, such that $h(a,b) = 0$.*

*Proof:* Let $N_m$ denote the number of rational points $(a,b)$, $a,b \in GF(2^m)$ on $h(x,y)$. Since $h(x,y)$ is absolutely irreducible over $GF(2)$, we may apply Weil's Theorem from Chapter 1 to prove

$$N_m \ge 2^m + 1 - 20\sqrt{2^m} - 6 .$$

It is easy to verify that there are at most 4 rational points $(a,b)$ where $a = b$ or one of $a,b$ is 0 or 1. We observe that $N_m > 4$ if $m \ge 9$. For $m = 7$, we verified the result by direct calculation. □

Now we combine this theorem with Lemma 4.2.

**Theorem 4.4.** *The code $C$ has minimum Lee weight 8 for all values of $m$, except when $m = 5$, in which case the minimum Lee weight is 12.*

We have proved this theorem for $m \ge 7$. The particular case $m = 5$ was first obtained by Calderbank and McGuire [CMG2] using the group and a computer. It was also proved by hand in [CMGKH]. We do not prove it here. It is shown there that $h(x,y)$ has no rational points over $GF(32)$. Note that codewords of weight 6 in the extended binary 2-error-correcting BCH code $B_2$ determine codewords in $C$ with Lee weight 12. The Gray image in the $m = 5$ case is a $(64, 2^{37}, 12)$ binary code, which is the best $(64, 2^{37})$ code presently known. The highest theoretical minimum distance possible is 13. It would be extremely interesting if the other codes in this family (which have $2^{2^{m+1}} - 5m - 2$ codewords) also had minimum distance 12. But they don't.

**Corollary 4.5.** *The Hensel lift of the extended binary* 2*-error-correcting BCH code,* $C_2$*, has minimum Lee weight* 8 *for all values of* $m$*.*

*Proof:* This Hensel lift consists of all codewords $(c_x)$ satisfying

$$\sum_{x \in D} c_x = \sum_{x \in D} c_x x = \sum_{x \in D} c_x x^3 = 0 \ .$$

It contains the code $C$ and it is contained in the Goethals code which has minimum Lee weight 8. For $m \geq 7$, the corollary follows directly from Theorem 4.4. The particular case $m = 5$ was proved by Calderbank and McGuire via computer calculation. □

The codes in this family have $2^{2^{m+1}} - 4m - 2$ codewords, and are much worse than the Goethals codes.

We also have the following theorem about $C_3$.

**Theorem 4.6.** *The code $C_3$, the Hensel lift of the extended binary 3-error-correcting BCH code, has minimum Lee weight 8 for all values of $m \geq 7$.*

*Proof:* The minimum Lee weight is at least 8, because this code is a subcode of the Goethals code. The rest of the theorem follows from the remark after Lemma 4.2 and Theorem 4.4. □

We remark that when $m = 5$, the code $C_3$ has minimum distance 14. This was proved (by hand) in [CMGKH]. The Gray image in the $m = 5$ case is a $(64, 2^{32}, 14)$ binary code, which is the best $(64, 2^{32})$ code presently known. The highest theoretical minimum distance possible is 16. It would be extremely interesting if the other codes in this family (which have $2^{2^{m+1}} - 6m - 2$ codewords) also had minimum distance 14. But they don't.

# REFERENCES

[A] S. S. Abhyankar, *Algebraic Geometry for Scientists and Engineers*, AMS Mathematical Surveys and Monographs, Volume 35, American Mathematical Society, 1990.

[BVLW] R. D. Baker, J. H. van Lint, and R. M. Wilson, On the Preparata and Goethals codes, *I.E.E.E. Trans. Info. Th.* **IT-29** (1983), 342–345.

[CMG1] A. R. Calderbank and G. McGuire, $Z_4$-Linear Codes Obtained as Projections of Kerdock and Delsarte-Goethals Codes, to appear in *Linear Algebra and its Applications.*

[CMG2] A. R. Calderbank and G. McGuire, Construction of a $(64, 2^{37}, 12)$ Code via Galois Rings, preprint, 1994.

[CMGKH] A. R. Calderbank, G. McGuire, P. V. Kumar, and T. Helleseth, Cyclic Codes over $Z_4$, Locator Polynomials and Newton's Identities, preprint, 1995.

[FJ] M.D. Fried and M. Jarden, *Field Arithmetic.* Springer-Verlag, 1986.

[F] W. Fulton, *Algebraic Curves*, Benjamin, New York, 1969.

[G] M. J. Ganley, On a Paper of Dembowski and Ostrom, *Arch. Math.* **27** (1976), 93–98.

[G1] D. G. Glynn, "Two New Sequences of Ovals in Finite Desarguesian

Planes of Even Order," in *Combinatorial Mathematics* X, Springer Lecture Notes in Mathematics **1036**, Springer-Verlag, 1983, 217–229.

[G2] D. G. Glynn, "A Condition for the Existence of Ovals in $PG(2, q)$, $q$ Even," *Geometriae Dedicata* **32** (1989), 247–252.

[HKCSS] A. R. Hammons Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane and P. Solé, The $Z_4$-linearity of Kerdock, Preparata, Goethals and Related Codes, *I.E.E.E. Trans. Inform. Theory* **IT-40** (1994), 301–319.

[H] J. W. P. Hirschfeld, *Projective Geometries over Finite Fields*, Clarendon Press, Oxford, 1989.

[H2] J. W. P. Hirschfeld, "Ovals in Desarguesian Planes of Even Order," *Ann. Mat. Pura Appl.* **102** (1975), 79–89.

[JW] H. Janwa and R. M. Wilson, "Hyperplane Sections of Fermat Varieties in $P^3$ in char. 2 and some Applications to Cyclic Codes," in: *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes* (Proceedings AAECC-10), Gérard Cohen, Teo Mora, Oscar Moreno (Eds.), Lecture Notes in Computer Science **673**, Springer-Verlag, 1993.

[J] D. Jungnickel, On a Theorem of Ganley, *Graphs and Comb.* **3** (1987), 141–143.

[LN] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia Math. Appl., vol.20, Addison-Wesley, Reading, MA, 1983.

[M] R. Matthews, "Permutation Properties of the Polynomials $1 + x + \cdots + x^k$ over a Finite Field," *Proc. A.M.S.*, **120** (1994), 47–51.

[MWS] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, Amsterdam, North-Holland, 1977.

[OKP] C. M. O'Keefe and T. Penttila, "Hyperovals in $PG(2, 16)$," *European J. Combin.* **12** (1991), 51–59.

[S1] B. Segre, "Sui $k$-archi nei piani finiti di caratteristica 2," *Revue de Math. Pures Appl.* **2** (1957), 289–300.

[S2] B. Segre, "Ovali e curve $\sigma$ nei piani di Galois di caratteristica due," *Atti Accad. Naz. Lincei Rend.* **8**, 32 (1962), 785–790.

[SB] B. Segre and U. Bartocci, "Ovali ed altre curve nei piani di Galois di caratteristica due," *Acta Arithmetica* **18** (1971), 423–449.

[SC] W. M. Schmidt, *Equations over Finite Fields*, Springer Lecture Notes in Mathematics, **536**, Springer-Verlag, 1976, 210.

[VLW1] J. H. van Lint and R. M. Wilson, Binary Cyclic Codes Generated by $m_1 m_7$, *I.E.E.E. Trans. Info. Th.* **IT-32** (1986), 283.

[VLW2] J. H. van Lint and R. M. Wilson, On the Minimum Distance of Cyclic Codes, *I.E.E.E. Trans. Info. Th.* **IT-32** (1986), 23–40.

[W] R. M. Wilson, Private Communication.