A Study of $(0,n,n+1)$-Sets and Other Solutions of the Isoperimetric Problem in Finite Projective Planes

Thesis by

Patricia K. Ure

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

California Institute of Technology
Pasadena, California
1996

(Submitted December 5, 1995)

Acknowledgments

I am very grateful to my adviser Rick Wilson for imparting to me his rich understanding of mathematics and mathematical thought. It has made me a much better mathematician. I also thank my fellow students and other members of the mathematics department at Caltech for the large part they have played in my intellectual development. Appreciation is also given to the Caltech administration for their general philosophy of cooperation and helpfulness, and in particular to the mathematics department staff who are always happy to help. I will always be grateful to the Mathematics Department at Reed College for showing me what mathematics really is. Finally, I thank my parents for their good advice and unswerving support.

Abstract

This treatise deals with the isoperimetric problem in finite projective planes. We prove that certain sets, called $(0, n, n+1)$-sets, are solutions to this problem. This class of sets includes all the previously known solutions to the isoperimetric problem, as well as two new types of solutions which exist in every finite projective plane. We prove a characterization theorem for $(0, n, n+1)$-sets with many points. We solve the isoperimetric problem for large set size, and for $q+3$ points if q is even. We find all the $(0, n, n+1)$-sets in planes of order at most 8 and develop techniques for proving that some $(0, n, n+1)$-sets in larger order planes do not exist. We solve the isoperimetric problem in the planes of order at most 7 (the solution was known only for planes of order at most 4), proving that nested solutions exist in these planes. We prove that no nested solutions exist in $PG(2, 8)$. We give examples of (0,2,3)-sets in planes of order 7, 8 and 16 which are new solutions to the isoperimetric problem not included in the infinite classes mentioned above, and we investigate Latin squares and Steiner triple systems associated with these examples.

Contents

Chapter 1. Introduction and Definitions

This chapter is intended as a review of the combinatorial structures which are used in the following chapters. We begin with a brief review of some definitions and ideas in finite projective planes (§1.1). The next section (§1.2) is devoted to the known results on arcs and (m, k)-arcs because they are such important constructions for our work. Section 1.3 is a review of the few ideas in lattice theory which are relevant to the discussion in §3.1. In §1.4 we discuss blocking sets and multiple blocking sets, which are used in sections 3.5 and 3.7.1. In §1.5 we define the isoperimetric problem and give the results which were known prior to the work contained herein.

1.1 Finite Projective Planes

Let q be a prime power. We use the notation

$$\begin{aligned} F_q &: = \text{the finite field with } q \text{ elements} \\ F_q^* &: = F_q \setminus \{0\} \\ F_q^3 &: = \text{the 3-dimensional vector space over } F_q \\ &= \{(x, y, z) : x, y, z \in F_q\}. \end{aligned}$$

We presume the reader is familiar with: the definition of a finite projective plane of order q, some examples of such planes, the definition of a desarguesian plane and the fact that all such planes are isomorphic to $PG(2, q)$ for some prime power q, the fact that all planes of order at most 8 are desarguesian, and the definition of an affine (sub)plane.

For a review of projective planes, see [Bat], §3.2; [vLW], chapters 23 and 26; or [Dem], chapter 3.

We will denote a general projective plane by π or π_q.

We mention here that we take our affine points to have 1 in their third coordinate. For example, the points and lines of $PG(2,q)$ are

$$\mathcal{P} := \{(x,y,1) : x,y \in F_q\} \cup \{(1,m,0) : m \in F_q\} \cup \{(0,1,0)\}$$
$$\mathcal{L} := \{y = mx + k : m,k \in F_q\} \cup \{x = c : c \in F_q\} \cup \{\ell_\infty\}.$$

Incidence obeys the obvious rule, namely, an affine point $\underline{x} = (x,y,1)$ is on an affine line ℓ whenever the equation defining ℓ is true at $\underline{x}$, while ℓ_∞ consists exactly of the slope points (those points with third coordinate zero).

Recall that three projective points (x_1,y_1,z_1), (x_2,y_2,z_2), and (x_3,y_3,z_3) are collinear if and only if the matrix of their coordinates has determinant zero:

$$\begin{vmatrix} x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \\ x_3 & y_3 & z_3 \end{vmatrix} = 0.$$

For example, two points on the line $y = mx + b$ will be incident with the point $(1,m,0)$. It is for this reason that the points $(1,m,0)$ are called **slope points with slope m**. The point (0,1,0) is incident with the lines $x = c$, corresponding to the slope ∞.

Recall also that the **dual** of a plane π, denoted π^*, is the projective plane with points equal to the lines $\mathcal{L}$ of π, lines equal to the points $\mathcal{P}$ of π, and having the point ℓ^* in π^* incident with the line x^* in π^* if and only if the point x is incident with the line ℓ in π.

We will show (Theorem 3.5) that most solutions to the isoperimetric problem obey a sort of duality. For that reason, and following [Ha], we define the dual complement of a set to be the 0-lines of that set, as points in the dual plane:

Definition: For a set A of points in a projective plane π, the **dual complement** of A is the set

$$A^{dc} := \{\ell^* : \ell \text{ is a 0-line of } A\}$$

of points in π^*.

For example, the dual complement of a singleton set $\{x\}$ is the affine subspace of π^* which has x^* as the line at infinity. The dual complement of affine space is the singleton set $\{\ell^*_\infty\}$ in π^*.

1.2 Arcs

Perfect arcs and k-arcs are solutions to the isoperimetric problem ([Ha]), and in this sense $(0, n, n+1)$-sets are generalizations of them. We therefore include a brief review of the relevant facts about arcs; for a more detailed account see, e.g. [Th1]; [Hi], chapter 8; or [Mar].

For the rest of this section assume π is a finite projective plane of order q. Recall that an (m, k)**-arc** in π is m points, some k but no $k+1$ collinear. An **arc** or m**-arc** is an (m, i)-arc with $i \leq 2$, i.e., m points with no more than 2 collinear. Thus, for our purposes, 0-arcs (the empty set) and 1-arcs (singleton sets) are arcs.

The largest value of m for which an (m, k)-arc exists in $PG(2, q)$ is usually denoted $m_k(2, q)$ and the known values for various k and small q are given in [HV] and [B1].

For a subset A of points of a plane, a line with no points of A is called an **external line**, a line with exactly one point is a **tangent**, a line with exactly two points is called a **secant**, and a line with i points is called an i**-line**.

In chapter 12 of [Hi], (m,k)-arcs in $PG(2,q)$ are discussed at length. Many of the results obtained therein are true in arbitrary projective planes. See also [vLW], chapter 26 for results about perfect arcs in arbitrary planes. We summarize the results which are well-known and relevant to our problem.

If there is an (m,k)-arc K then $m \leq (q+1)(k-1)+1$. K is called **perfect** or **maximal** when equality holds. In this case every line intersects K in exactly k points. If there is a perfect (m,k)-arc then k divides q or $k = q+1$ (in which case $K = \pi$). In an abuse of notation, we call a perfect (m,k)-arc a **perfect k-arc** when we do not wish to specify m.

There are perfect (m,k)-arcs in $PG(2,2^t)$ for every $t \geq 1$ whenever k divides 2^t (see [Den1] or [vLW], p. 314) but it is proved in [Th2] that there are no $(m,3)$-arcs in $PG(2,3^t)$ other than affine space in $PG(2,3)$. If K is a perfect (m,k)-arc then K^{dc} is a perfect $\left(\frac{q(q+1-k)}{k}, \frac{q}{k}\right)$-arc. Consequently, there are no $\left(\frac{q(q-2)}{3}, \frac{q}{3}\right)$-arcs in $PG(2,3^t)$ for $t \geq 2$.

If $m = (q+1)(k-1)$ (the size of a perfect k-arc minus a point) and K is an (m,k)-arc for some $k > 2$ then there is a point which lies only on $(k-1)$-lines of K, i.e., there is a unique point x such that $K \cup \{x\}$ is a perfect k-arc ([Bar]). Notice that this theorem is not true when $k = 2$, since that would imply that an oval is always contained in a hyperoval; see below.

An arc is called **complete** if it is not properly contained in any other arc. For an arc K, a point $x \notin K$ is a **completion point** of K if $K \cup \{x\}$ is also an arc. Thus an arc is complete if and only if it has no completion points, if and only if every $x \in \mathcal{P}$ lies on at least one secant of K.

A k-arc K satisfies $k \leq q+2$ and if $k = q+2$ then K is a perfect $(q+2,2)$-arc, which is called a **hyperoval**. Thus hyperovals exist only in even-order planes. An **oval** in a plane of any order q is a $(q+1)$-arc. In planes of even order, an oval K always has a completion point x, called the **nucleus** (see [Hi], Lemma 8.1.4; the desarguesian hypothesis is not necessary).

Examples of ovals in $PG(2,q)$ arise as the solutions of nondegenerate quadrics. (See [vLW], p. 317 for a discussion of quadrics.) That is, for most choices of $a_i \in F_q$, the set of all projective points (x,y,z) satisfying

$$a_1x^2 + a_2xy + a_3xz + a_4y^2 + a_5yz + a_6z^2 = 0$$

is an oval. An oval that arises as the solution of a quadric is sometimes called a **conic**.

It is an important theorem of Segre that in $PG(2,q)$ when q is odd the ovals are exactly the conics. In $PG(2,2^t)$, however, not all hyperovals arise this way. If a hyperoval can be written as a conic plus its nucleus, it is called a **regular hyperoval**. It is known that if $t \geq 4$, then $PG(2,2^t)$ contains irregular hyperovals. See [G] or [C] for examples of infinite classes of irregular hyperovals.

We use the term **(hyper)oval** as shorthand for "an oval when q is odd, a hyperoval when q is even". Specifically, we exclude the possibility of a $(q+1)$-arc when q is even.

In $PG(2,q)$ for any q, a q-arc can always be completed to an oval. (See [Dem], result 3.2.28 for a reference.) The hypothesis that the plane be desarguesian is necessary (see, e.g., [Den2]).

If K is an oval in $PG(2,q)$ where q is odd, the points off K are partitioned into $\binom{q+1}{2}$ **external points** which are on two tangents and $\binom{q-1}{2}$ secants, and $\binom{q}{2}$ **internal points** which are on no tangents and $\binom{q+1}{2}$ secants.

In $PG(2,q)$ where $q > 2$ is even, the hyperovals are exactly the sets

$$\mathcal{D}(f) := \{(x, f(x), 1) : x \in F_q\} \cup \{(0,1,0), (1,0,0)\}$$

where f is an o-polynomial. A polynomial f of degree at most $q-1$ is an ***o*-polynomial** if it is a permutation polynomial, $f(0) = 0$, $f(1) = 1$, and for each $s \in F$, F_s is also a permutation polynomial, where $F_s(0) := 0$ and when $x \neq 0$ we have

$$F_s(x) := \frac{f(x+s) + f(s)}{x}.$$

(See [Hi], p. 174, or [O'KP] for further characterizations of o-polynomials.)

1.3 Lattices

Except as noted, the material in this section can be found in [DP], sections 2.1 through 2.21. It is intended to be only a review of the few facts from lattice theory which we will need.

A lattice is a partially ordered set in which meets and joins always exist. Let X be a set. A map cl from the power set of X to the power set of X is a **closure operator** on X if for all $A, B \subseteq X$ we have

(i) $A \subseteq cl(A)$

(ii) if $A \subseteq B$ then $cl(A) \subseteq cl(B)$

(iii) $cl(cl(A)) = cl(A)$

A subset A of X is called **closed** if $A = cl(A)$.

A closure operator on a set X gives a lattice whose elements are the closed sets, order is containment, the meet ($\wedge$) is defined as the intersection, and the join ($\vee$) is defined as the closure of the union.

An element a of a lattice **covers** an element b if $a > b$ and there is no c with $a > c > b$. A lattice is called **semimodular** ([vLW], p. 271) if whenever distinct elements a and b both cover some element c, then $a \vee b$ covers both a and b.

1.4 Blocking Sets

A **blocking set** in a finite projective plane is a set T of points such that every line contains at least one point in T and one point not in T. It is immediately obvious that the complement $\overline{T} := \mathcal{P} \setminus T$ is also a blocking set. It is also immediate that the secants of a complete arc form a blocking set in the dual (see, e.g., [Br]). It is an area of active research to find the size of a smallest blocking set in a given plane. The answer is known in some cases, for example, in [Br] it is shown that if S is a blocking set in a plane π of order q then $|S| \geq q + \sqrt{q} + 1$ with equality if and only if q is a square and S is a Baer subplane, that is, a plane of order $\sqrt{q}$ with incidence inherited from π. In [BS] it is shown that if q is not a square and S is a blocking set in $PG(2, q)$, then $|S| \geq q + \sqrt{2q} + 1 - \frac{1}{2q}$. It is an open question what the best possible lower bound is in the case of non-square q.

For a fountain of examples of blocking sets, as well as a discussion in the affine setting, see [Ta].

An r**-fold blocking set** is a set T of points such that every line intersects T in at least r points, where $r \geq 1$. (An r-fold blocking set may contain a line.) A **multiple blocking set** is an r-fold blocking set for some r. Multiple blocking sets have been recently studied by Ball and Blokhuis using Rédei's theory of lacunary polynomials ([B1], [BB], [B2]). Their most general result generalizes Bruen's result, as follows. If B is an r-blocking set in $PG(2, q)$ for some $r \geq 1$ and if B contains no line then it has at least $rq + \sqrt{rq} + 1$ points.

1.5 The Isoperimetric Problem

The material in this section is taken from [Ha].

Given a bipartite graph with disjoint vertex sets A and B, the general isoperimetric problem is as follows. Fix $0 \leq m \leq |A|$, consider all of the m-sets of A, and find one which has the least possible number of edges incident with it. The neighborhood of an m-set T in a graph is defined as the edges incident with some point of T, and is denoted by $N(T)$. With this notation, the isoperimetric problem is to find

$$\min_{T \subseteq A : |T| = m} |N(T)|.$$

For our purposes the bipartite graph is the one whose disjoint vertex sets are $\mathcal{P}$ and $\mathcal{L}$, the sets of points and lines of a projective plane. The neighborhood of a set T of projective points is then all of the lines incident with (at least one point of) T.

Definition: Given a set T of points in a projective plane, the **neighborhood of** T is defined to be

$$\begin{aligned} N(T) :&= \text{the set of lines incident with } T \\ &= \{\ell \in \mathcal{L} : \ell \cap T \neq \emptyset\}. \end{aligned}$$

We wish to find, for each m, the sets which have the least number of lines incident with them, and what that least number is. For this purpose we define

$$\partial_m := \min_{T \subseteq \mathcal{P} : |T| = m} |N(T)|.$$

Definition: The **isoperimetric problem** refers to either of the following: (1) Given a projective plane and an integer $0 \leq m \leq q^2 + q + 1$, find ∂_m; (2) Given a projective plane, find ∂_m for each $0 \leq m \leq q^2 + q + 1$. It should be clear from context which definition is being used.

Definition: Given a projective plane and an integer $0 \leq m \leq q^2 + q + 1$, **the solution to the isoperimetric problem** is ∂_m, or any set T achieving this minimum. Again, no confusion should arise in practice from this double definition.

Suppose we wish to build a solution T to the isoperimetric problem. We would start with a point x_1, add another point x_2, and then as our third point x_3 we would take a point on few 0-lines to the 2-set $\{x_1, x_2\}$ (because all the 0-lines on x_3 become new lines in $N(T)$ when we add x_3 to the 2-set), and so on.

So if we want to build a solution to the isoperimetric problem from a given set T we should add points, one at a time, which lie on few 0-lines to the points already chosen, i.e. points which lie on many of the lines incident with the points already chosen. One way of doing this is to make sure T does not have lines containing "too many" points of T. For example, if T is a set which has all 1- and 2-lines except for one 5-line, we could replace a point x of that 5-line with a point y off the 5-line. The point y will probably be on three fewer 0-lines of $T \setminus \{x\}$ than x is on (because there are probably about three more lines to $T \setminus \{x\}$ from y than from x), and hence we should expect $|N(\{y\} \cup T \setminus \{x\})| < |N(T)|$.

What we are suggesting is that a set T where the lines intersecting T all have approximately the same number of points of T, should be a solution to the isoperimetric problem. Theorem 2.1 further supports this idea. In all the solutions to the isoperimetric problem known before this investigation, this is true. The known classes of solutions were: For $0 \leq m \leq q + 1$ (or $q + 2$ if q is even), the solutions to the isoperimetric problems are exactly the m-arcs. Perfect k-arcs are solutions to the isoperimetric problem. We will define closed sets in §3.1, but for now we just mention that arcs are closed sets, therefore closed solutions, and that dual complements of closed solutions are closed solutions ([Ha], Theorem 1) and so the dual complements of arcs are exactly the solutions to the isoperimetric problems for the appropriate m.

We will generalize this idea that equalizing line intersection sizes solves the isoperimetric problem, by proving that if T is a set such that every non-external line intersects T in n or $n+1$ points (for some n), then T is a solution to the isoperimetric problem (Theorem 2.1). We will also show that this idea is limited by giving an example (in §4.3.2) of a solution to the isoperimetric problem which is not constructable as described in the above greedy algorithm which builds up a set one point at a time. Our example has the property that every line intersects it in zero, two or four points.

In the language of §1.2, we generally expect solutions of the isoperimetric problem for m points in a plane π_q to be $(m, n+1)$-arcs for the smallest possible n, but our example in §4.3.2 shows that this is not a necessary condition to be a solution to the isoperimetric problem.

Chapter 2. (0,n,n+1)-Sets

In this chapter we define $(0,n,n+1)$-sets, and prove (Theorem 2.1) that given m, $(0,n,n+1)$-sets with m points are solutions to the isoperimetric problem for m points. Furthermore, when such sets exist they are the only solutions. We then develop necessary conditions for the existence of a $(0,n,n+1)$-set of size m in a plane of order q (§2.2), give some general examples of $(0,n,n+1)$-sets (§2.3), and list all the $(0,n,n+1)$-sets in planes of order at most 5 (Table 2.1).

2.1 Proof That (0,n,n+1)-Sets Are Solutions

The following observation was suggested by R. Wilson. Given a projective plane π, a set of points T, and a line ℓ, let

$$\mu_\ell := |T \cap \ell|.$$

Then because μ_ℓ is an integer, for any integer n we have

$$0 \leq \sum_{\ell \in N(T)} (\mu_\ell - n)\big(\mu_\ell - (n+1)\big). \tag{2.1}$$

Let $m := |T|$. In the proof of Theorem 2.1 we will obtain a lower bound on $|N(T)|$ where equality holds if and only if $\mu_\ell = n$ or $n+1$ for each $\ell \in N(T)$. We are thus motivated to make the following definition before stating Theorem 2.1:

Definition: A set T of points in a projective plane π is called a $(0,n,n+1)$**-set** if $\mu_\ell = 0$, n, or $n+1$ for every line ℓ of π.

These sets are often called sets of type $[0,n,n+1]$ (see, e.g., [Ta]).

Theorem 2.1. *If there exist $(0, n, n+1)$-sets of size m in a projective plane π, then the solutions to the isoperimetric problem for m points are exactly the $(0, n, n+1)$-sets. In any case,*

$$\partial_m \geq \frac{m}{n(n+1)}\big(2n(q+1)+1-m\big)$$

with equality if and only if there exist $(0, n, n+1)$-sets of size m.

Proof: Let T be a set of m points in π. Counting in two ways the pairs (ℓ, x) where ℓ is a line and $x \in \ell \cap T$, and the triples (x, y, ℓ) with $x, y \in \ell \cap T$, proves that

$$\begin{aligned}\sum_{\ell \in N(T)} \mu_\ell &= m(q+1) \\ \sum_{\ell \in N(T)} \mu_\ell(\mu_\ell - 1) &= m(m-1).\end{aligned} \tag{2.2}$$

Substituting this into equation (2.1), we get

$$\begin{aligned} 0 &\leq \sum_{\ell \in N(T)} \big(\mu_\ell - n\big)\big(\mu_\ell - (n+1)\big) \\ &= m\big(m - 1 - 2n(q+1)\big) + n(n+1)|N(T)| \\ \Rightarrow\ |N(T)| &\geq \frac{m}{n(n+1)}\big(2n(q+1)+1-m\big)\end{aligned} \tag{2.3}$$

with equality if and only if $\mu_\ell = n$ or $n+1$ for every line $\ell \in N(T)$.

For the rest of the proof, suppose there is a $(0, n, n+1)$-set S of size m. Then $|N(S)| = \frac{m}{n(n+1)}\big(2n(q+1)+1-m\big) \leq |N(T)|$ for all other sets T of m points in π, so S is a solution to the isoperimetric problem: $\partial_m = |N(S)|$. If T is also a solution to the isoperimetric problem for m points in π, then $|N(T)| = \partial_m = \frac{m}{n(n+1)}\big(2n(q+1)+1-m\big)$, that is, equality holds in equation (2.3) and so T must be a $(0, n, n+1)$-set. □

A quick glance at the Appendix shows that, for small q anyway, Theorem 2.1 is a pretty good bound.

We observe that given m, π_q, and $n := \left\lfloor \frac{q+m}{q+1} \right\rfloor$, equation (2.3) proves that solving the isoperimetric problem for m points in π_q, i.e. minimizing $|N(T)|$, or equivalently, minimizing the sum in (2.3), is accomplished by taking a set with as many μ_ℓ as close to n as possible. This is the point we made in §1.5.

2.2 Combinatorial Properties of (0,n,n+1)-Sets

For this section, let S denote a $(0, n, n+1)$-set of size m.

Fix a point $x \in S$. The other points in S are each on a line with x and so the $q+1$ lines through x partition the other points into sets of size $n-1$ and n. Thus $n-1 = \left\lfloor \frac{m-1}{q+1} \right\rfloor$ and $n = \left\lfloor \frac{q+m}{q+1} \right\rfloor$.

Define t by $n = \frac{q+m-t}{q+1}$, so that $0 \leq t \leq q$. Actually t has a geometric interpretation, which can be seen as follows. Fixing $x \in S$, let u and v denote the number of n and $(n+1)$-lines, respectively, on x. Then

$$u + v = q + 1$$

$$(n-1)u + nv = m - 1.$$

Adding $1 - n$ times the first equation to the second shows that

$$v = q + m - n(q+1) = t,$$

that is, t represents the number of $(n+1)$-lines on a point $x \in S$.

Equations (2.2) become

$$n\tau_n + (n+1)\tau_{n+1} = m(q+1)$$

$$n(n-1)\tau_n + n(n+1)\tau_{n+1} = m(m-1).$$

Solving these equations for τ_n and τ_{n+1} and recalling that $\tau_0+\tau_n+\tau_{n+1} = q^2+q+1$, we know how many lines of each size there are:

$$\begin{aligned} \tau_{n+1} &= \frac{m}{n+1}\big(q+m-n(q+1)\big) \\ \tau_n &= \frac{m}{n}\big(1-m+n(q+1)\big) \\ \tau_0 &= q^2+q+1-\frac{m}{n(n+1)}\big(2n(q+1)+1-m\big). \end{aligned} \tag{2.4}$$

In particular, τ_n and τ_{n+1} must be integers. We address the question: if the quantities on the right hand side of equations (2.4) are integers for some q, m and $n = \left\lfloor \frac{q+m}{q+1} \right\rfloor$, is there a $(0, n, n+1)$-set of size m in some plane of order q? The answer seems to be a difficult one, and in the general case the answer is "no". For example, $m = q+2$ always results in integers on the right hand side, but then S would have $\tau_3 = 0$, that is, S would be a hyperoval which we know does not exist if q is odd.

The following definition is equivalent to the condition that τ_n and τ_{n+1} are integers.

Definition: We shall say m, n, and q are **feasible parameters**, or that $\{m, n, q\}$ is a **feasible parameter set**, when the following conditions all hold:

$$n = \left\lfloor \frac{q+m}{q+1} \right\rfloor$$

$$n \text{ divides } m(m-1)$$

$$(n+1) \text{ divides } tm$$

where $t := q+m-n(q+1) =$ the number of $(n+1)$-lines incident with a point of a $(0, n, n+1)$-set, if one exists. Table 2.1 lists all the feasible parameters for $q \leq 5$. In the last column we show an example of a $(0, n, n+1)$-set of size m if one exists, or give a proof that one does not exist.

Table 2.1 The feasible parameters for $q = 2, 3, 4, 5$.

q	n	m	τ_n	τ_{n+1}	τ_0	Example
2	1	1	3	0	4	point
2	1	2	4	1	2	2-arc
2	1	3	3	3	1	3-arc, or $AG(2,2)$ minus a point
2	2	4	6	0	1	4-arc, or $AG(2,2)$
2	2	6	3	4	0	$PG(2,2)$ minus a point
2	3	7	7	0	0	$PG(2,2)$
3	1	1	4	0	9	point
3	1	2	6	1	6	2-arc
3	1	3	6	3	4	3-arc
3	1	4	4	6	3	oval
3	2	5	10	0	3	does not exist (would be a perfect 2-arc)
3	2	6	9	2	2	dual complement of an oval
3	2	8	4	8	1	$AG(2,3)$ minus a point
3	3	9	12	0	1	$AG(2,3)$
3	3	12	4	9	0	$PG(2,3)$ minus a point
3	4	13	13	0	0	$PG(2,3)$
4	1	1	5	0	16	point
4	1	2	8	1	12	2-arc
4	1	3	9	3	9	3-arc
4	1	4	8	6	7	4-arc
4	1	5	5	10	6	5-arc
4	2	6	15	0	6	hyperoval, or the dual complement of a hyperoval
4	2	9	9	9	3	dual complement of a 3-arc
4	3	12	16	3	2	dual complement of a 2-arc
4	3	15	5	15	1	$AG(2,4)$ minus a point
4	4	16	20	0	1	$AG(2,4)$
4	4	20	5	16	0	$PG(2,4)$ minus a point
4	5	21	21	0	0	$PG(2,4)$
5	1	1	6	0	25	point
5	1	2	10	1	20	2-arc
5	1	3	12	3	16	3-arc
5	1	4	12	6	13	4-arc
5	1	5	10	10	11	5-arc
5	1	6	6	15	10	oval
5	2	7	21	0	10	does not exist (would be a perfect 2-arc)
5	2	9	18	6	7	does not exist (see the example, §2.3)
5	2	10	15	10	6	dual complement of an oval
5	2	12	6	20	5	does not exist (Theorem 3.10)
5	3	13	26	0	5	does not exist (Theorem 3.10)
5	3	16	16	12	3	dual complement of a 3-arc
5	4	20	25	4	2	dual complement of a 2-arc
5	4	24	6	24	1	$AG(2,5)$ minus a point

5	5	25	30	0	1	$AG(2,5)$
5	5	30	6	25	0	$PG(2,5)$ minus a point
5	6	31	31	0	0	$PG(2,5)$

2.3 Examples of $(0,n,n+1)$-Sets

1. Perfect (m,n)-arcs are technically $(0,n-1,n)$-sets as well as $(0,n,n+1)$-sets, but we will adopt the convention that we refer to them only as $(0,n,n+1)$-sets. That way we preserve the property that $n = \left\lfloor \frac{q+m}{q+1} \right\rfloor$. We call a $(0,n,n+1)$-set **strict** when it is not a perfect arc.

   We now list the commonly known perfect arcs, as examples of $(0,n,n+1)$-sets. The empty set is a $(0,0,1)$-set. A point is a $(0,1,2)$-set. An affine subplane is a $(0,q,q+1)$-set of size q^2. The projective plane is a $(0,q+1,q+2)$-set. When q is even, $PG(2,q)$ contains perfect k-arcs for any k which divides q and these are $(0,k,k+1)$-sets.

2. A k-arc with $k \leq q+1$ is a $(0,1,2)$-set of size k.

3. Deleting any point or line from a perfect n-arc results in a $(0,n-1,n)$-set.

4. The complement of a point is a $(0,q,q+1)$-set of size q^2+q.

5. Two lines intersect every other line in one or two points, so the complement of two lines is a $(0,q-1,q)$-set of size q^2-q.

6. The complement of three nonconcurrent lines is a $(0,q-2,q-1)$-set of size $(q-1)^2$.

Since a $(0,n,n+1)$-set is a solution to the isoperimetric problem, all of the examples given above are solutions. With the exception of Example **3**, they were all previously known solutions (many are dual complements of arcs; see §1.4).

Taking an affine subplane as the perfect arc in Example 3 gives two new classes of solutions to the isoperimetric problem which exist in every finite projective plane.

Chapter 3. Existence of $(0,n,n+1)$-Sets

Section 3.2 contains theorems which are useful in solving the isoperimetric problem, and which will be used in sections 3.4, 3.5 and 4.3. For these theorems it is important to know whether a set is as large as it can be and have the same neighborhood, so we define a set to be closed when this situation holds. The term "closed" has several mathematical connotations and we justify its use in this case, in the context of lattices. Our only lattice theory result (in §3.1) is that this lattice-theoretic approach is not worth pursuing.

3.1 The Closure and Lattice Theory

Definition: For a set of points $T \subseteq \mathcal{P}$, the **closure** $cl(T)$ of T is defined as $T \cup \{x \in \mathcal{P} : x \text{ lies on no 0-lines of } T\}$.

Then a set is **closed** when every point off it lies on at least one external line.

Notice that cl is a closure operator in the lattice-theoretic sense (see §1.3). The closed sets therefore form a lattice with inclusion as the partial order. This lattice is not "nice", it is not even semimodular. For example take two points $x, y \in \pi$ and let ℓ be the line they determine. Define $a := \ell \setminus \{x\}$, $b := \ell \setminus \{y\}$, $c := \ell \setminus \{x,y\}$. Then a, b, c are distinct elements of the lattice of closed sets, a and b each cover c, but $a \vee b = cl(\ell) = \pi$. To be semimodular it is required that π cover a and b, but we can find a closed set that lies properly between a and π, for example, as follows. Take $z \notin \ell$, and let ℓ' be the line on x and z. Then

$$a \subset cl(\{z\} \cup a) \subseteq \pi \setminus \ell' \subset \pi$$

and so π does not cover a.

Note that all solutions T to the isoperimetric problem of size m are closed if $\partial_m < \partial_{m+1}$. This is independent of T and, unlike our definition of closed, applies only to sets which are solutions to the isoperimetric problem. The term "closed" was originally introduced in this context ([Ha]). We introduced the definition of the closure operator as given above and followed through the lattice investigations.

3.2 Theorems Involving the Closure

Lemma 3.1. *A $(0, n, n+1)$-set of size m is either a perfect $(n+1)$-arc minus a point, or it is closed.*

Proof: Let S be a $(0, n, n+1)$-set of size m and suppose S is not closed. Then there exists a point x such that $T := S \cup \{x\}$ has $\partial_{m+1} \leq |N(T)| = |N(S)| = \partial_m$ (the last equality is because $(0, n, n+1)$-sets are solutions to the isoperimetric problem), and since ∂_m is increasing with m, this says $\partial_m = \partial_{m+1}$. Then by Theorem 2.1:

$$\frac{m}{n(n+1)}(2n(q+1)+1-m) = \partial_m = \partial_{m+1} \geq \frac{m+1}{n'(n'+1)}(2n'(q+1)-m)$$

where $n = \left\lfloor \frac{q+m}{q+1} \right\rfloor$ and $n' = \left\lfloor \frac{q+m+1}{q+1} \right\rfloor$.

If $n = n'$ this implies

$$\frac{m}{q+1} \geq n = n' = \left\lfloor \frac{q+m+1}{q+1} \right\rfloor = 1 + \left\lfloor \frac{m}{q+1} \right\rfloor$$

a contradiction. So we must have $n' = n+1$. Now $n' = \frac{q+m+1-t'}{q+1}$ and $n = \frac{q+m-t}{q+1}$ for some $0 \leq t', t \leq q$, so we have $t' = t - q$ where $0 \leq t, t' \leq q$. It must be that $t' = 0$ and $t = q$ and so $m = n(q+1) - q + t = n(q+1)$. By the results mentioned in §1.2, if $n > 1$ then S is a perfect $(n+1)$-arc minus a point, and if $n = 1$ then S is a hyperoval minus a point, still a perfect arc minus a point. □

Corollary 3.2. *If K is a k-arc in a plane of order q, and $k \le q$, then K is closed. A $(q+1)$-arc is closed iff q is odd. A hyperoval is closed.*

Proof: The first statement follows because a k-arc with $k \le q$ is a (0,1,2)-set not of the form "perfect arc minus a point". The second and third statements are true by well-known results on ovals and hyperovals; see e.g. [Hi], Lemmas 8.2.1 and 8.1.4 whose proofs work as well in non-desarguesian planes. □

Recall from §1.1 that the dual complement of a set T is the dual of its set of 0-lines, so T^{dc} is a set of $q^2+q+1-|N(T)|$ points in the dual plane.

Lemma 3.3. *For any subset T of points in a projective plane, $cl(T) = (T^{dc})^{dc}$. Furthermore, $T \subseteq (T^{dc})^{dc}$ with equality if and only if T is closed.*

Proof:

$$\begin{aligned} x \in (T^{dc})^{dc} &\Leftrightarrow x^* \text{ is a 0-line of } T^{dc} \\ &\Leftrightarrow x^* \cap T^{dc} = \emptyset. \end{aligned}$$

Equivalently,

$$\begin{aligned} x \notin (T^{dc})^{dc} &\Leftrightarrow \exists\, \ell^* \in T^{dc} \text{ with } \ell^* \text{ incident with } x^* \\ &\Leftrightarrow \exists\, \ell \text{ a 0-line of } T \text{ through } x. \end{aligned}$$

So $x \in (T^{dc})^{dc}$ iff x lies on no 0-lines of T, proving $cl(T) = (T^{dc})^{dc}$. Certainly points of T lie on no 0-lines of T, so $T \subseteq (T^{dc})^{dc}$. Equality holds if and only if $\big(x \notin T \Rightarrow x \notin (T^{dc})^{dc} = cl(T)\big)$ if and only if T is closed. □

The next lemma seems quite technical but is often useful for increasing the lower bound on ∂_m as given in Theorem 2.1 (see §4.3), and (with Corollary 3.6) it is very important to our characterization theorem (Theorem 3.10).

Lemma 3.4. *Let a projective plane π of order q be given and suppose that T is a solution to the isoperimetric problem for m in π. Then*

$$\partial_{q^2+q+1-\partial_m} \leq q^2+q+1-m.$$

Equality holds if and only if $T=(T^{dc})^{dc}$ and T^{dc} is a solution to its isoperimetric problem.

Proof: By Lemma 3.3,

$$\begin{aligned} m=|T| \leq |(T^{dc})^{dc}| &= q^2+q+1-|N(T^{dc})| \\ &\leq q^2+q+1-\partial_{|T^{dc}|} \\ &= q^2+q+1-\partial_{q^2+q+1-\partial_m}. \end{aligned}$$

□

In [Ha] it is shown that if S is a closed solution to the isoperimetric problem in a bipartite graph, then S^{dc} is also a closed solution. The following theorem is our proof of this fact, in the context of projective planes and using our definition of "closed".

Theorem 3.5. *Let a projective plane π of order q be given. If T is a closed set of points in π then T^{dc} is a closed set. If T is a closed solution to the isoperimetric problem then T^{dc} is a closed solution.*

Proof: T closed $\Rightarrow T=(T^{dc})^{dc} \Rightarrow T^{dc}=((T^{dc})^{dc})^{dc}=cl(T^{dc}) \Rightarrow T^{dc}$ is closed.

Now suppose T is a closed solution. By Lemma 3.4,

$$\partial_{q^2+q+1-\partial_{|T^{dc}|}} \leq q^2+q+1-|T^{dc}|=|N(T)|=\partial_{|T|}$$

because T is a solution. But ∂_m is an increasing function of m and so

$$q^2+q+1-\partial_{|T^{dc}|} \leq |T| = q^2+q+1-|N(T^{dc})|$$

because $T = (T^{dc})^{dc}$. Thus $|N(T^{dc})| \leq \partial_{|T^{dc}|}$ so equality must hold and T^{dc} is a solution. □

Corollary 3.6. *Equality holds in Lemma 3.4 if and only if T is a closed solution.*

Proof: Suppose equality holds. Then by Lemma 3.4, T is closed and T^{dc} is a solution. By Theorem 3.5, T^{dc} is a closed solution and so $T = (T^{dc})^{dc}$ is a (closed) solution.

Now suppose T is a closed solution. Then $T = (T^{dc})^{dc}$ and (by Theorem 3.5) T^{dc} is a solution, so equality holds in Lemma 3.4. □

Corollary 3.7. *Fix a finite projective plane π_q and m. The solutions to the isoperimetric problem for m points in π_q are either all closed or all not closed.*

Proof: Corollary 3.6 depends only upon the size of a solution and that it is a solution, not on the set itself.

More rigorously, suppose S and T are solutions to the isoperimetric problem for m points and that T is closed. Then Corollary 3.6 for T says

$$\partial_{q^2+q+1-\partial_m} = q^2 + q + 1 - m$$

and so Corollary 3.6 for S says S is a closed solution. □

3.3 The Method of Typing Points

This method is described in [Hi], §12.1 for sets of points in a projective plane. It is most useful when it is applied to sets T with few possibilities for $|\ell \cap T|$, and for $|x^* \cap T^{dc}|$ in π^*. Fortunately, this situation pertains in many cases of our study, and we have exploited manipulation of equations (3.2) below. In particular, the technique is used in the proof of Theorem 3.11 and in §4.3.

Suppose for this section that S is a $(0, n, n+1)$-set of size m in a projective plane of order q. For a point x and for $i = n$ or $n+1$ define

$$\rho_i^x := \text{the number of } i\text{-lines incident with } x \text{ when } x \in S$$

$$\sigma_i^x := \text{the number of } i\text{-lines incident with } x \text{ when } x \notin S,$$

We use ρ_i or σ_i when x is understood. Then for $x \in S$ one can solve equations (3.1) for ρ_n^x and ρ_{n+1}^x (as in the proof of Lemma 3.1):

$$\rho_n^x + \rho_{n+1}^x = q + 1$$

$$(n-1)\rho_n + n\rho_{n+1}^x = m - 1 \tag{3.1}$$

showing that all points of S are of the same type, that is, they all have the same number of n-lines and the same number of $(n+1)$-lines through them.

For $x \notin S$ we have a more difficult situation, because there are two equations in three unknowns:

$$\sigma_0^x + \sigma_n^x + \sigma_{n+1}^x = q + 1$$

$$n\sigma_n^x + (n+1)\sigma_{n+1}^x = m$$

and points off S may be any of several types. We are led to consider nonnegative integer solutions for u, v and w to the equations

$$u + v + w = q + 1$$

$$nu + (n+1)v = m. \tag{3.2}$$

These equations have few solutions for large n, because if u, v, w and u', v', w' are two solutions then

$$n(u - u') = (n+1)(v' - v)$$

$$\Rightarrow n + 1 \mid u - u' \quad \text{and} \quad n \mid v - v'.$$

Pick (u, v, w) a solution of (3.2) with w minimum, i.e. so that all the solutions are of the form $(u_i, v_i, w_i) := (u - i(n+1), v + in, w + i)$ for some $i \geq 0$.

Let $A_i := \{x \notin S : x \text{ has } u_i \text{ } n\text{-lines and } v_i \text{ } (n+1)\text{-lines}\}$. The A_i partition $\pi \setminus S$. We say a point is of **type A_i** when it is in A_i. Let $a_i := |A_i|$. If there are $t + 1$ solutions to (3.2), we get the following:

$$\begin{aligned}\sum_{i=0}^{t} a_i &= q^2 + q + 1 - m \\ \sum_{i=0}^{t} a_i w_i &= \tau_0(q+1) \\ \sum_{i=0}^{t} a_i \binom{w_i}{2} &= \binom{\tau_0}{2}.\end{aligned} \tag{3.3}$$

Substituting $w_i = w + i$, this translates into the system of equations

$$\begin{pmatrix} 1 & 1 & \dots & 1 \\ w & w+1 & \dots & w+t \\ \binom{w}{2} & \binom{w+1}{2} & \dots & \binom{w+t}{w} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_t \end{pmatrix} = \begin{pmatrix} q^2 + q + 1 - m \\ \tau_0(q+1) \\ \binom{\tau_0}{2} \end{pmatrix}.$$

Left multiplying both sides of the equation by the matrix

$$\begin{pmatrix} 1 & 0 & 0 \\ -w & 1 & 0 \\ \binom{w+1}{2} & -w & 1 \end{pmatrix}$$

we arrive at the conclusion that if there is a $(0, n, n+1)$-set of size m then there is a solution to the matrix equation

$$\begin{pmatrix} 1 & 1 & 1 & \dots & 1 & \dots & 1 \\ 0 & 1 & 2 & \dots & i & \dots & t \\ 0 & 0 & 1 & \dots & \binom{i}{2} & \dots & \binom{t}{2} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_t \end{pmatrix} =$$

$$\begin{pmatrix} q^2 + q + 1 - m \\ (q+1)\tau_0 - w(q^2 + q + 1 - m) \\ \binom{w+1}{2}(q^2 + q + 1 - m) - w\tau_0(q+1) + \binom{\tau_0}{2} \end{pmatrix} \tag{3.4}$$

where the a_i are all nonnegative integers.

Example: In the case $q = 5$, $n = 2$, $m = 9$ which is feasible, we have $\tau_0 = 7$, and we consider solutions to

$$u + v + w = 6$$

$$2u + 3v = 9.$$

Thus if S is a (0,2,3)-set of size 9 in $PG(2,5)$, then for each $x \notin S$ we have $(u, v, w) = (3, 1, 2)$ or (0,3,3). The smallest w is 2 and equation (3.4) becomes

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \end{pmatrix} = \begin{pmatrix} 22 \\ 1 \\ 18 \end{pmatrix}$$

which must have solutions $a_0, a_1 \geq 0$, a contradiction. There can be no such (0,2,3)-set in the plane of order 5.

3.4 The Existence of (0,n,n+1)-Sets of Size m $\geq \binom{q}{2}$.

We will eventually characterize all the "large" $(0, n, n + 1)$-sets (Theorem 3.10) by showing that most of them are dual complements of arcs. First we have to characterize those arcs whose dual complements are $(0, n, n + 1)$-sets.

We will show in the proof of Corollary 3.9 that dual complements of ovals are $(0, n, n + 1)$-sets, so for now we restrict our attention to smaller arcs. Suppose K is a k-arc in a plane π^*, $k \leq q$ and $S := K^{dc}$ is a $(0, n, n+1)$-set for some n. Then $m := |S| = q^2 - qk + q + 1 + k(k - 3)/2$ which implies that for m, n and q to be feasible it must be that

$$n = q + 1 - k + \left\lfloor \frac{\binom{k}{2}}{q + 1} \right\rfloor.$$

K is closed (Corollary 3.2) and a solution to the isoperimetric problem (by Theorem 2.1), so (by Theorem 3.5) S is a closed solution and the points off K are the duals of the non-external lines of S. In π, S is a $(0, n, n+1)$-set for some n if and only if in π^* every point off K lies on n or $n+1$ external lines to K if and only if in π^* every ℓ^* off K lies on s or $s+1$ secants for some s. Thus K^{dc} is a $(0, n, n+1)$-set if and only if there is such an s. If so, fix an external line to K. Each of the $\binom{k}{2}$ secants of K meets it, so the secants are divided into $q+1$ sets of size s and $s+1$. Thus $s = \left\lfloor \frac{\binom{k}{2}}{q+1} \right\rfloor$.

Theorem 3.8. *If K is a k-arc and K^{dc} is a $(0, n, n+1)$-set in a plane of order q, then $k \leq 3$ or $k \geq q+1$.*

Proof: By contradiction. Assume there is a K satisfying (*) for some k and q with $4 \leq k \leq q$. Because $k \geq 4$, there are two secants intersecting off K, so $s \geq 1$, and we may assume $k \leq q \leq \binom{k}{2} - 1$. With notation as in §3.3, we have

$$\sum_{x \notin K} \sigma_2^x(\sigma_2^x - 1) = \binom{k}{2}\binom{k-2}{2}$$

$$\sum_{x \notin K} \sigma_2^x = \binom{k}{2}(q-1)$$

by counting in two ways pairs of secants intersecting off K, and counting in two ways (secant, point off K) incidence flags. So we have

$$\begin{aligned} 0 &= \sum_{x \notin K} (\sigma_2^x - s)(\sigma_2^x - s - 1) \\ &= \binom{k}{2}\binom{k-2}{2} - sk(q-1)(k-1) + s(s+1)(q^2+q+1-k) \qquad (3.5) \end{aligned}$$

for some $4 \leq k \leq q \leq \binom{k}{2} - 1$ and $s = \left\lfloor \frac{\binom{k}{2}}{q+1} \right\rfloor$.

It seems difficult to show that equation (3.5) cannot be true. We prove something apparently more difficult, namely, we forget the information that $s = \left\lfloor \frac{\binom{k}{2}}{q+1} \right\rfloor$ and, viewing the right hand side as a quadratic in s, we show that equation (3.5) has no real roots if $k \leq q \leq \binom{k}{2} - 1$. It suffices to show that the discriminant $\Delta(q)$ is negative for these q. That is, we fix k and consider the discriminant as a function of q.

$$\Delta(q) = q^4 + 2q^3(-k^2 + k + 1) + q^2(4k^3 - 10k^2 + 4k + 3) +$$
$$q(-3k^4 + 12k^3 - 15k^2 + 4k + 2) + k^5 - 6k^4 + 13k^3 - 11k^2 + 2k + 1.$$

We record also

$$\Delta'(q) = 4q^3 + 6q^2(-k^2+k+1) + 2q(4k^3 - 10k^2 + 4k + 3) - 3k^4 + 12k^3 - 15k^2 + 4k + 2$$

$$\Delta''(q) = 12q^2 + 12q(-k^2 + k + 1) + 2(4k^3 - 10k^2 + 4k + 3).$$

We claim that it suffices to show the following:

(i) $\Delta'(k) < 0$

(ii) $\Delta''(k) < 0$

(iii) $\Delta(k) < 0$

(iv) $\Delta\left(\binom{k}{2} - 1\right) < 0.$

This is because (i) and (ii) imply that the point $(k, \Delta(k))$, on the graph of Δ as a function of q, is in the dashed region of the graph in Figure 3.1.

Conditions (iii) and (iv) then prove that for q in the interval $k \leq q \leq \binom{k}{2} - 1$ we have $\Delta(q) < 0$ and so equation (3.5) has no real (let alone integer) roots.

We now prove (i). $\Delta'(k) = -k^4 + 2k^3 - k^2 + 10k + 2$ is a fourth degree polynomial in k, call it $f(k)$. Its derivative $f'(k)$ is a cubic with leading coefficient -4 and $f'(0) = f'(1) > 0$ and $f'(4) < 0$. The graph of f' as a function of k must be approximately as in Figure 3.2.

All the zeros of f' are less than 4, so $f(k)$ has all its extrema less than 4.

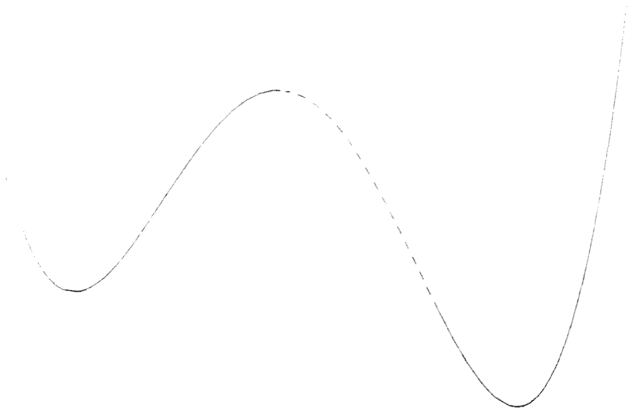

Figure 3.1 Conditions (i) and (ii) imply $\left(k, \Delta(k)\right)$ lies in the dashed region of the graph of $\Delta(q)$.

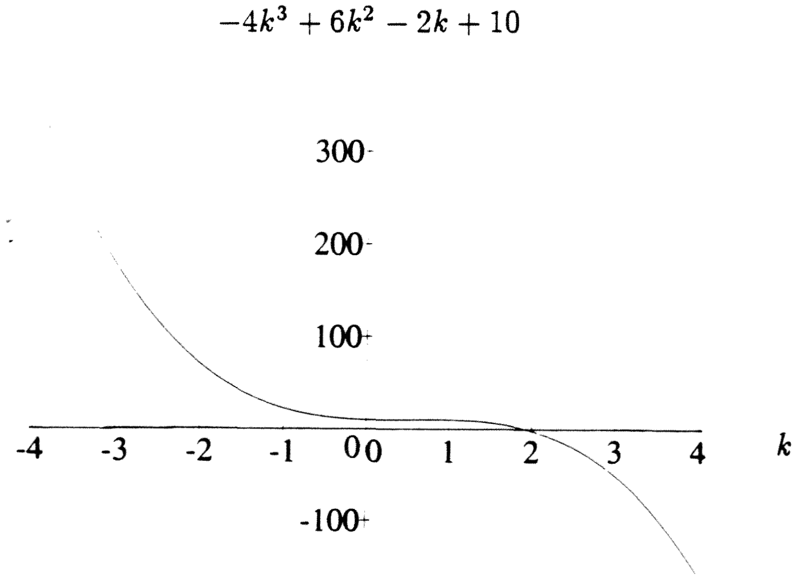

Figure 3.2. The graph of $\frac{d}{dk}(\Delta'(q)$ evaluated at $q = k)$, as a function of k.

Since $f(4) < 0$, we have $\Delta'(k) < 0$ for all $k > 4$, establishing (i).

Now to prove (ii) let f represent the cubic in k given by $\Delta''(q)$ evaluated at

$q = k$. That is, $f = -4k^3 + 4k^2 + 20k + 6$. The graph of f is shown in Figure 3.3, from which it is easily seen that $f(k) < 0$ for all $k \geq 4$.

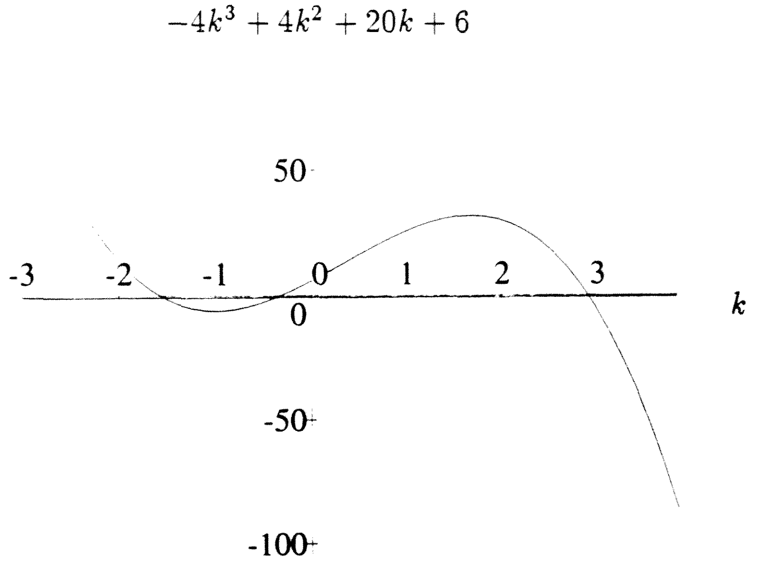

Figure 3.3. The graph of Δ'' evaluated at k, showing that condition (ii) holds for $k \geq 4$.

Now let f represent the fourth-degree polynomial $\Delta(q)$ evaluated at $q = k$, $f(k) = -k^4 + 4k^3 - 4k^2 + 4k + 1$. $f'(k)$ has only one real root, so Figure 3.4 shows the graph of f (including all finite extrema), showing that condition (iii) holds for $k \geq 4$.

Now let f represent the eighth-degree polynomial $\Delta(q)$ evaluated at $q = \binom{k}{2} - 1$, $f(k) = \left(-\frac{3}{16}k^8 + \frac{7}{4}k^7\right) + \left(-\frac{47}{8}k^6 + \frac{17}{2}k^5\right) + \left(-\frac{91}{16}k^4 + \frac{19}{4}k^3\right) + \left(-\frac{21}{4}k^2 + k + 1\right)$. The summands are grouped into terms (within each pair of parentheses) so that each term is negative when $k \geq 10$, and it is easy to check that $f(k) < 0$ when $1 \leq k \leq 9$, thus establishing (iv). □

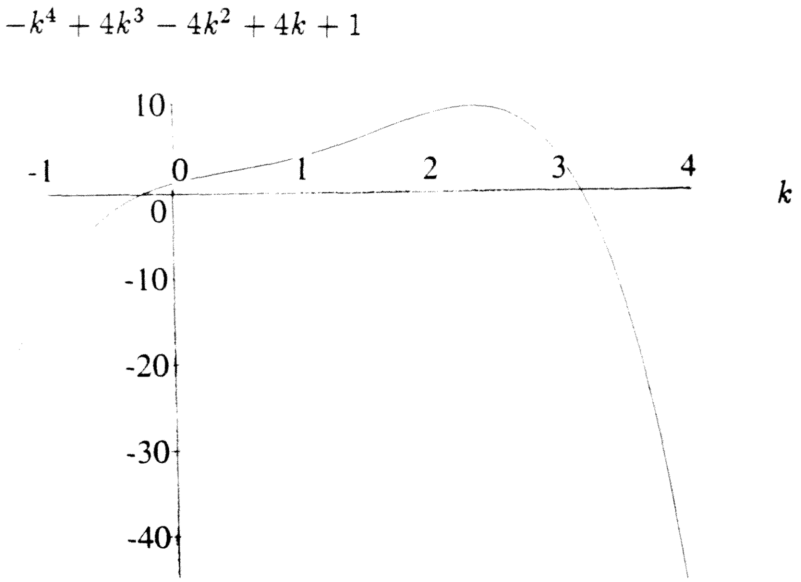

Figure 3.4. The graph of Δ evaluated at $q = k$, as a function of k, showing that condition (iii) holds.

Corollary 3.9. *A k-arc K yields a $(0, n, n+1)$-set in a projective plane of order q iff k is one of the following:* 0, 1, 2, 3, $q + 1$, *or* $q + 2$ *if q is even.*

Proof: That the dual complement of a (hyper)oval is a $(0, n, n+1)$-set was known (see, e.g., [Hi], pp. 166 and 325, which we have restated in terms of $(0, n, n+1)$-sets). We include new proofs which depend on lemmas from §3.2. If k =0, 1, 2, or 3 one easily checks that K^{dc} is $(0, n, n+1)$-set for $n = q+1$, q, $q-1$, or $q-2$ respectively.

If $k = q+1$, or (in the case of q even) $q+2$, then $|N(K)| = \binom{q+2}{2}$. In any case $S := K^{dc}$ has $m = \binom{q+2}{2}$.

If q is odd then $n = \frac{q-1}{2}$. Using first Theorem 2.1 and then (because an oval is a closed solution for q odd) Corollary 3.6 says

$$\begin{aligned} q^2 &= \frac{\frac{q(q-1)}{2}}{\frac{q-1}{2}\frac{q+1}{2}}\left(q^2 - 1 + 1 - \frac{q^2}{2} + \frac{q}{2}\right) \\ &\leq \partial_m = \partial_{q^2+q+1-\partial_{|K|}} = q^2 + q + 1 - |K| = q^2. \end{aligned}$$

Since equality holds in Theorem 2.1, S must be $(0, \frac{q-1}{2}, \frac{q+1}{2})$-set.

For q even, a $q+2$-arc is a perfect 2-arc and so its dual complement is a perfect $\frac{q}{2}$-arc. A $q+1$-arc K has the same 0-lines as the $q+2$-arc obtained by adding its nucleus, and hence has the same dual complement, so K^{dc} is also a $(0, \frac{q}{2}, \frac{q}{2}+1)$-set. □

We now prove our main result, the classification of large $(0, n, n+1)$-sets. The idea is to prove that a large $(0, n, n+1)$-set must be the dual complement of an arc, or be a perfect arc minus a point, or a perfect arc. We know which arcs' dual complements are $(0, n, n+1)$-sets in a plane π by Corollary 3.9, and we will show that the only large perfect arcs are affine subspaces of π, or π itself, thereby establishing Theorem 3.10.

Theorem 3.10. *A set S in a projective plane π of order q with $m \geq \binom{q}{2}$ points is a $(0, n, n+1)$-set if and only if one of the following cases holds:*

(1) *$m = \binom{q}{2}$ and either*

  (a) *$S = \mathcal{O}^{dc}$ where $\mathcal{O}$ is an oval, or*

  (b) *$S = \mathcal{H}^{dc}$ where $\mathcal{H}$ is a hyperoval and q is even*

(2) *$m = (q-1)^2$ and $S = K^{dc}$ where K is a 3-arc*

(3) *$m = q(q-1)$ and $S = K^{dc}$ where K is a 2-arc*

(4) *$m = q^2 - 1$ and S is affine space minus a point*

(5) *$m = q^2$ and S is affine space, i.e. $S = K^{dc}$ where K is a 1-arc*

(6) *$m = q(q+1)$ and S is $\pi \setminus \{x\}$ for some point x*

(7) *$m = q^2 + q + 1$ and $S = \pi = K^{dc}$ where K is a 0-arc.*

For q even, cases (1a) and (1b) describe the same set S.

Proof: Corollary 3.9 shows that cases 1, 2, 3, 5 and 7 are all $(0, n, n+1)$-sets. In examples 3 and 4 of §2.3 it was shown that case 4 is a $(0, q-1, q)$-set and case 6 is a $(0, q, q+1)$-set.

Now suppose S is a $(0, n, n+1)$-set with $m \geq \binom{q}{2}$ points. By Lemma 3.1, S is either a perfect $(n+1)$-arc minus a point, or closed. If S is a perfect $(n+1)$-arc minus a point then $n+1$ divides q, or $n+1 = q+1$. In the latter case we are in case 6 above, so suppose $n+1$ divides q. Now $n := \left\lfloor \frac{q+m}{q+1} \right\rfloor \geq \left\lfloor \frac{q+\binom{q}{2}}{q+1} \right\rfloor = \left\lfloor \frac{q}{2} \right\rfloor$, and so we must have $n+1 = q$ and we are in case 4.

We may now suppose S is closed. By Theorem 3.5, S^{dc} is a solution to the isoperimetric problem for τ_0 points. Now because ∂_m is increasing with m,

$$\begin{aligned}\tau_0 &= q^2 + q + 1 - \partial_m \\ &\leq q^2 + q + 1 - \partial_{\binom{q}{2}} \\ &= \text{the number of 0-lines of (a (hyper)oval)}^{dc} \\ &= \begin{cases} q+1 & \text{if } q \text{ is odd} \\ q+2 & \text{if } q \text{ is even} \end{cases}\end{aligned}$$

because (hyper)ovals are closed by Corollary 3.2.

Thus S^{dc} is a solution to the isoperimetric problem in π^* for k points, with $k \leq |\text{(hyper)oval}|$, and the only such solutions are the k-arcs, so $S = (S^{dc})^{dc} = K^{dc}$ for some k-arc K. By Corollary 3.9, $k = q+1$, or $q+2$ if q is even (case 1), or $k \leq 3$ (cases 2, 3, 5, and 7). □

3.5 Elimination Methods and The Existence Question for (0,n,n+1)-Sets for Small q

Table 3.1 lists the feasible parameter sets for $q = 7, 8, 9, 11, 16$ with $q + 2 < m < \binom{q}{2}$. (No interesting information or techniques are yet known for the $q = 13$ case. For $q \leq 5$ see Table 2.1.) For $m \leq q+1$ $(q+2)$ when q is odd (even), (0,1,2)-sets are arcs, which are well-studied. In particular they always exist in $PG(2,q)$. There is never a (0,2,3)-set of size $q + 2$ for q odd because such a set would have $\tau_3 = 0$, i.e. it would be a perfect 2-arc, which cannot exist as 2 does not divide q in this case. For $m \geq \binom{q}{2}$, Theorem 3.10 describes all the $(0, n, n + 1)$-sets.

We have answered the existence question for $(0, n, n + 1)$-sets in the planes of order at most 8, and nearly answered the question for $PG(2, 9)$. For larger q very little is known. Following the proof that Table 3.1 is accurate, we give some theorems (Theorems 3.12–3.15) that can be used to eliminate some feasible parameter sets for larger q.

The last sections in this chapter mention dual complement pairs (another method for showing non-existence of certain $(0, n, n + 1)$-sets) and give examples of sporadic $(0, n, n + 1)$-sets which are known to exist, as listed in Table 3.1.

Table 3.1. The feasible parameters with $q + 2 < m < \binom{q}{2}$ and $q = 7, 8, 9, 11, 16$.

q	n	m	τ_n	τ_{n+1}	τ_0	Example ($\mathcal{O}$ is an oval, $\mathcal{H}$ is a hyperoval) or proof of nonexistence (see Theorem 3.11)
7	2	12	30	12	15	Example, §3.7.2
7	2	15	15	30	12	Example, §3.7.2
8	2	12	42	8	23	1
8	2	13	39	13	21	2
8	2	15	30	25	18	Example, §3.7.3
8	2	16	24	32	17	3

8	2	18	9	48	16	1
8	3	19	57	0	16	4
8	3	24	32	30	11	Perfect 4-arc minus a line
8	3	27	9	54	10	Perfect 4-arc minus a point
9	2	12	54	4	33	5
9	2	14	49	14	28	6
9	2	15	45	20	26	
9	2	17	34	34	23	
9	2	18	27	42	22	7
9	2	20	10	60	21	8
9	3	21	70	0	21	4
9	3	24	56	18	17	1
9	3	25	50	25	16	2
9	3	28	28	49	14	2
11	2	15	75	10	48	1
11	2	16	72	16	45	
11	2	18	63	30	40	9
11	2	19	57	38	38	
11	2	21	42	56	35	
11	2	22	33	66	34	
11	2	24	12	88	33	8
11	3	25	100	0	33	4
11	3	28	84	21	28	
11	3	33	44	66	23	
11	3	36	12	99	22	8
11	4	37	111	0	22	4
11	4	40	90	24	19	1
11	4	45	45	72	16	
11	5	51	102	17	14	2
16	2	21	147	21	105	10
16	2	24	132	48	93	
16	2	27	108	81	84	Example, §3.7.3
16	2	30	75	120	78	
16	2	33	33	165	75	
16	3	36	192	9	72	1
16	3	39	169	39	65	
16	3	40	160	50	63	1
16	3	43	129	86	58	
16	3	48	64	156	53	Perfect 4-arc minus a line
16	3	51	17	204	52	Perfect 4-arc minus a point
16	4	52	221	0	52	Perfect 4-arc
16	4	57	171	57	45	1
16	4	60	135	96	42	1
16	4	65	65	169	39	
16	5	75	165	75	33	

16	5	81	81	162	30	1
16	6	91	182	65	26	1
16	6	93	155	93	25	2
16	6	100	50	200	23	2
16	7	112	128	126	19	Perfect 8-arc minus a line
16	7	119	17	238	18	Perfect 8-arc minus a point

Theorem 3.11. *The existence of* $(0, n, n+1)$*-sets in the desarguesian planes of order* $q = 7, 8, 9, 11, 16$ *with* $q + 2 < m < \binom{q}{2}$ *as given in Table 3.1 is correct.*

Proof: Examples are given in Table 3.1 when they are known to exist. Proofs of nonexistence are given in the table by reference to the numbers below, in the cases where the proofs are known.

1. The method of typing the points off S, as in §3.3, results in a system of equations (equation (3.4)) that has no nonnegative integer solutions, contradicting the existence of such a $(0, n, n+1)$-set of size m in the plane of order q.

2. If there were a $(0, n, n+1)$-set S of size m then typing the points off S shows that every point is on w or $w+1$ lines, i.e. S^{dc} is a $(0, w, w+1)$-set of size τ_0. But τ_0 is not a feasible size for a $(0, w, w+1)$-set (for any w).

3. In [B1] and [HV] is quoted an unpublished result of Bierbrauer that an $(m, 3)$-arc in $PG(2, 8)$ has $m \leq 15$.

4. If there were a set S of $n(q+1)+1$ points with at most $n+1$ points per line, S would be a perfect $(n+1)$-arc. If $n+1$ does not divide q or if $n+1 = 3$, there can be no such S.

5. Suppose there is a (0,2,3)-set S of size 12 in a plane of order 9. Then by equations (3.1) every point of S is on a unique 3-line. Deleting one point from each 3-line results in an 8-arc. So S is an 8-arc plus four points. Each

of these four points must have been on six tangents to the 8-arc. In [Hi] (p. 412) it is proven that there are only two projectively distinct types of 8-arcs in $PG(2, 9)$ and one easily checks by computer that every point off an 8-arc lies on at most four tangets to the 8-arc, except the two completion points of the 8-arc contained in an oval. Thus there can be no (0,2,3)-set of size 12 in $PG(2, 9)$.

6. In [BSW], p. 44 it is reported that exhaustive search shows that there does not exist a no-tangent set of size 14 in $PG(2, 9)$. To our knowledge, nothing is known in the other planes of order 9.

7. In [Hi], p. 178 and [HV] it is stated that a 3-arc in $PG(2, 9)$ has at most 17 points. To our knowledge, nothing is known about 3-arcs in the other planes of order 9.

8. If there were a set S of $n(q + 1)$ points with at most $n + 1$ points per line ($n \geq 2$), S would be a perfect $(n + 1)$-arc less a point, hence completable to a perfect $(n + 1)$-arc. If $n + 1$ does not divide q or if $n + 1 = 3$, there can be no such S.

9. If there were a (0,2,3)-set S of size 18 in a plane of order 16 then typing points off S shows that every point off S is on four or five 0-lines, i.e. S^{dc} is a (0,4,5)-set of size 40 which (although 40 is feasible) does not exist by reason (1).

10. If there were a (0,2,3)-set of size 21 in a plane of order 16 then points off it are of type $(\sigma_0, \sigma_2, \sigma_3) = (7, 9, 1)$, (8,6,3), (9,3,5), or (10,0,7) and there are $252 - a_3$, $3a_3 - 21$, $21 - 3a_3$, and a_3 of each type, respectively. Now a_1 and a_2 are both nonnegative, implying $a_3 = 7$, $a_1 = a_2 = 0$ and $a_0 = 249$.

Fix a 0-line ℓ. All 3-lines cross it. If there are b_0 points of type 0 on ℓ and b_3 of type 3, then

$$b_0 + b_3 = 17$$

$$b_0 + 7b_3 = \tau_3 = 21$$

which has no integer solutions. □

The "first unknown case" is $q = 9$, $m = 15$. Suppose T is a (0,2,3)-set of size 15 in a plane π of order 9. Typing points off T shows that every point of π has zero, three or six 2-lines on it. There is a unique point on no 2-lines, call it P. There are thirty points on three 2-lines, and there are sixty points (including the fifteen points of T) on six 2-lines. If we take P^* as the line at infinity in the dual π^*, the 2-lines form a 45-set of type (3,6). The 45-sets of type (3,6) have been characterized in all the affine planes of order 9 ([PR]), and so we believe it will soon be settled, by computer search if necessary, whether there is a (0,2,3)-set of size 15 in any plane of order 9.

We now mention some theorems that apply to larger order planes to show that there are no $(0, n, n+1)$-sets for certain parameters not previously eliminated. The first two theorems are from the literature, but Theorem 3.14 is new.

Theorem 3.12. ([Hi], p. 355, Corollary to Theorem 12.4.6) *A (k,n)-arc with $n \geq 4$ in $PG(2,q)$, $q \not\equiv 0$ mod n, satisfies $k \leq (n-1)q + n - 3$.* □

For example when $q = 59$ and $n = 5$ Theorem 3.12 says a (0,4,5)-set has at most 238 points, eliminating the feasible $m = 240$. When $n = 6$, a (0,5,6)-set in $PG(2,59)$ has at most 298 points, eliminating the feasible $m = 300$.

Theorem 3.13. ([BSW], p. 39) *Let S be a set of points in the desarguesian projective plane $PG(2,q)$, q odd, such that no line intersects S in precisely one* *point. Then* $|S| \geq q + \frac{1}{4}\sqrt{2q} + 2$. □

Theorem 3.13 often applies to planes of order $q \geq 47$ when $n = 2$. For example when $q = 47$, Theorem 3.13 says that a (0,2,3)-set must have at least 52 points, eliminating the feasible $m = 51$. When $q = 125$, a (0,2,3)-set must have at least 131 points, eliminating the feasible $m = 130$.

Theorem 3.14. *Although* $m = q + 4$ *is feasible if (and only if)* $q \equiv 2 \bmod 3$, *there are no* $(0, 2, 3)$*-sets of size* $q + 4$ *in any projective plane of even order* $q > 2$.

Proof: One easily checks the feasibility statement.

Suppose S is a (0,2,3)-set of size $q+4$. Type the points off S to get $w = \frac{q}{2} - 1$. Equations (2.4) show that $\tau_0 = \frac{3q^2-7q+2}{6}$. Now equation (3.4) becomes

$$\begin{pmatrix} 1 & 1 & 1 & \dots & 1 & \dots & 1 \\ 0 & 1 & 2 & \dots & i & \dots & t \\ 0 & 0 & 1 & \dots & \binom{i}{2} & \dots & \binom{t}{2} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_t \end{pmatrix} = \begin{pmatrix} q^2 - 3 \\ (q+1)\tau_0 - w(q^2 - 3) \\ f(q) \end{pmatrix}$$

where $f(q) = -(q+4)(q-2)/36$, so $f(q) < 0$ for $q > 2$, and this contradicts that $f(q)$ is a nonnegative sum of $\binom{i}{2}$'s. □

For $q \geq 47$, Theorem 3.13 implies Theorem 3.14, but for smaller q Theorem 3.14 gives the better bound.

The most useful method to show nonexistence of a $(0, n, n+1)$-set of size m with n, m and q feasible seems to be showing that the system of equations obtained by typing the points off such a set, as in equation (3.4), has no nonnegative solutions. This works for most values of n between about $q/4$ and $q/2$, and rarely works for other values of n. Theorems 3.13 and 3.14 are only useful when $n = 2$. There is another technique (Theorem 3.15) which occasionally applies to values of n between 2 and $q/4$ to prove nonexistence of a particular $(0, n, n+1)$-set in the desarguesian plane, although this technique is more likely to work for larger n.

This theorem uses Ball's lower bound on the size of a multiple blocking set, as discussed in §1.4. There are two ways in which one might use this bound. The first, more obvious way is that if T is a $(0, n, n+1)$-set of size m, then it is an $(m, n+1)$-arc and so its complement $\overline{T} := \mathcal{P} \setminus T$ must be a $(q-n)$-fold blocking set. Ball's results prove that in $PG(2, q)$ it must be that $|\overline{T}| \geq (q-n)q + \sqrt{(q-n)q} + 1$. Writing $n = \frac{q+m-t}{q+1}$ for some $0 \leq t \leq q$, this is equivalent to $2q - t - n \geq -\sqrt{q(q-n)}$ which holds if $n < q$ because $t \leq q$. So this application of Ball's bound can never prove nonexistence of a $(0, n, n+1)$-set for the unknown cases, $n < \frac{q}{2}$.

The second application of Ball's bound is motivated by the following curious fact. If K is a complete arc in a plane π, then in π^* the 2-lines of K are a blocking set (as discussed in §1.4), while K's 0-lines are a solution to the isoperimetric problem (by Theorem 3.5 and Corollary 3.2). We find this fact curious because a solution to the isoperimetric problm is a set with the fewest possible lines meeting it, while a blocking set is a set with the most possible lines (q^2+q+1) meeting it. It is unexpected that the same set K spawns a solution to each of these opposite extremal problems.

The proof of Theorem 3.15 is a generalization of the above discussion, obtained by thinking of the arc K as a (0,1,2)-set and finding r and r' so that for every $x \in \mathcal{P}$, the number of $(n+1)$-lines on x is at least r, and the number of n-lines on x is at least r'. Then the $(n+1)$-lines (n-lines) are an r-fold (r'-fold) blocking set in the dual plane. For example, in the proof that the 2-lines of K are a blocking set, one uses the completeness condition to prove that $r = 1$.

Before proving Theorem 3.15, we illustrate the method with an example. Let $q = 37$ and $m = 196$, so $n = 6$ and $\tau_7 = 140$. If there is a $(0,6,7)$-set S of size 196 in $PG(2,37)$, type the points off S as in §3.3. They are of type $(\sigma_6, \sigma_7, \sigma_0)$ =(30,4,4), (23,10,5), (16,16,6), (9,22,7), or (2,28,8). That is, every point off S is on at least four 7-lines of S. Points of S are on five 7-lines and thirty-three 6-lines. Thus, every point of $PG(2,37)$ is on at least four 7-lines. The set of 7-lines is a 4-blocking set in $\left(PG(2,37)\right)^*$, and it cannot contain a line, since this corresponds to the 7-lines being concurrent but $\sigma_7 < 38$ in all cases. So the result of Ball leads to the contradiction $140 \geq 148 + \sqrt{148} + 1$. Thus there can be no (0,6,7)-set of size 196 in $PG(2,37)$.

For integers a and b, we define $\overline{a}$ (mod b) by $\overline{a} \equiv a \pmod{b}$ and $0 \leq \overline{a} < b$.

Theorem 3.15. *Let S be a strict $(0, n, n+1)$-set of size m in $PG(2,q)$. Define t by $n = \frac{q+m-t}{q+1}$. Let*

$$r := \min\{\overline{m} \pmod{n},\, t\}$$

$$r' := \min\{\overline{-m} \pmod{n+1},\, q+1-t\}.$$

Then

$$\tau_{n+1} \geq rq + \sqrt{rq} + 1 \qquad \textit{and}$$

$$\tau_n \geq r'q + \sqrt{r'q} + 1.$$

Proof: The equations (3.1) show that for $x \in S$, the number of $(n+1)$-lines (n-lines) on x is at least t $(q+1-t)$. The equations (3.2) show that every point off S is of type $(\sigma_n, \sigma_{n+1}, \sigma_0) = (u_i, v_i, w_i)$ for some i, where $v_i \equiv m \bmod n$ and $u_i \equiv -m \bmod n+1$. That is, the $(n+1)$-lines form an r-blocking set and the n-lines form an r'-blocking set.

If $r = 0\,(r' = 0)$ then because S is strict we have τ_n, $\tau_{n+1} \geq 1$ and the result is true. If $r, r' > 0$ then the result follows immediately from Ball's lower bound if the set of $(n+1)$-lines (n-lines) in the dual plane does not contain a line. This is equivalent to the condition that no $q+1\,(n+1)$-lines (n-lines) are concurrent. But if there are $q+1$ concurrent $(n+1)$-lines then $m = (n+1)(q+1)$ which implies $n = \left\lfloor \frac{q+m}{q+1} \right\rfloor = \left\lfloor \frac{q+(n+1)(q+1)}{q+1} \right\rfloor = n+1$, a contradicition. If there are $q+1$ concurrent n-lines then $m = n(q+1)$, S is a perfect $n+1$-arc minus a point, so $\tau_n = q+1$ and $\tau_{n+1} > 1$. But in this case $t = 0$, so $r = 0$ and $r' \leq 1$ and the result still holds. □

Corollary 3.16. *The following do not exist: A (0,6,7)-set of size 142 in $PG(2,23)$, a (0,6,7)-set of size 154 in $PG(2,29)$, a (0,6,7)-set of size 196 in $PG(2,37)$, and a (0,6,7)-set of size 226 in $PG(2,37)$ (although all parameter sets are feasible).*

Proof: Parameters $q = 23$, $m = 142$ would have $\tau_6 = 71$ (by equation (2.4)) but $t = 21$, $r' = 3$ so the 6-lines are a 3-blocking set and Theorem 3.15 gives the contradiction $71 \geq 70 + \sqrt{69}$.

For $q = 29$, $m = 154$ we would have $\tau_7 = 66$, $t = 3$, $r = 3$ and so the 7-lines are a 3-blocking set in the dual, giving the contradiction $66 \geq 88 + \sqrt{87}$.

Both of these parameter sets could also have been eliminated by showing that the system in equation (3.4) has no nonnegative solutions. In the next two examples it is not so obvious whether equation (3.4) has no nonnegative solutions.

The case $q = 37$, $m = 196$ was done previous. The case $q = 37$, $m = 226$ would have $\tau_6 = 113$, $t = 35$, $r' = 3$ and we have the contradiction $113 \geq 112 + \sqrt{111}$.

3.6 Dual Complement Pairs

In examining a table of feasible parameter sets (like Table 3.1), there are some cases in which for a fixed q there is M an m-value with τ_0 0-lines, and τ_0 is an m-value with M 0-lines. For example, when $q = 7$ a (0,2,3)-set of size 12 would have fifteen 0-lines, and a (0,2,3)-set of size 15 would have twelve 0-lines. If there is a (0,2,3)-set S with $m = 12$ then it is closed (Lemma 3.1) and a solution to the isoperimetric problem (by Theorem 2.1), so by Corollary 3.6 and Theorem 2.1,

$$\frac{15}{6}(33 - 15) \leq \partial_{15} = \partial_{57-\partial_{12}} = 57 - 12$$

i.e., equality holds in Theorem 2.1 and so S^{dc} is a (0,2,3)-set with $m = 15$. A similar argument proves that a (0,2,3)-set of size 15 has its dual complement a (0,2,3)-set of size 12, so **there exists a (0,2,3)-set of size 12 in** $PG(2,7)$ **if and only if there exists a (0,2,3)-set of size 15, and they are dual complements of each other**.

Likewise in π_{11} there is a (0,2,3)-set with $m = 16$ if and only if there is a (0,4,5)-set with $m = 45$, and they are dual complements. A (0,3,4)-set with $m = 28$ in π_{11} would have to have another (0,3,4)-set with $m = 28$ as its dual complement. Reason (8) in the proof of Theorem 3.11 demonstrates how in a dual complement pair situation (as described at the beginning of this section) one can sometimes eliminate a feasible parameter set by eliminating its dual complement mate.

3.7 Examples of Particular (0,n,n+1)-Sets, and Designs Derived From Them

In this section we present the new solutions to the isoperimetric problem which we have found. They are (0,2,3)-sets of size 12 and 15 in the plane of order 7, size 15 in the plane of order 8, and size 27 in the plane of order 16. The examples for $q = 8$ and 16 are two of what should be a larger family of examples, and consideration of this family raises some questions about hyperovals. We begin with a result about sets of hyperovals with large pairwise intersection sizes (Theorem 3.18) to set the stage for these examples, and we prove a related coding theory result (Theorem 3.19). We also discuss some interesting designs which can be derived from our (0,2,3)-sets.

3.7.1 Hyperovals

Two hyperovals can intersect in at most half their points ([Hi], p. 165) and their union T is a (0,2,3,4)-set. If they intersect in exactly half their points and if there are no 4-lines, then T is a (0,2,3)-set of size $\frac{3(q+2)}{2}$. The fact that whenever two hyperovals intersect in exactly half their points, then there are no 4-lines, is proven in Lemma 3.17. So if we can find two hyperovals intersecting in half their points, we have a (0,2,3)-set of size $3(q + 2)/2$.

A 5-arc determines a conic ([Hi], p. 141) so in desarguesian planes of odd order at least 9, where the answer to the existence question for $(0, n, n + 1)$-sets is unknown, this technique will not provide (0,2,3)-sets. Furthermore in desarguesian planes of even order larger than 8, a (0,2,3)-set of size $3(q + 2)/2$ constructed as the union of two hyperovals intersecting in half their points, will have to have at least one of the hyperovals be irregular. If $q = 8$ all hyperovals are regular, but two regular hyperovals may share five points if (at least) one of these five points is a nucleus of one of the conics. We present an example of two hyperovals in $PG(2,16)$ which meet in nine points, and an example of two hyperovals in $PG(2,8)$ which meet in five points (§3.7.3).

Lemma 3.17. *If two hyperovals $\mathcal{H}_1$ and $\mathcal{H}_2$ in a projective plane of even order q intersect in half their points, then their symmetric difference $\mathcal{H}_1 \triangle \mathcal{H}_2$ is also a hyperoval.*

Proof: This theorem is known (a consequence of [AK], Corollary 6.3.1) but our proof is original.

Let $T := \mathcal{H}_1 \cup \mathcal{H}_2$. Since every line is secant to $\mathcal{H}_i$ for $i = 1$ and 2, T has 2-lines, 3-lines and possibly 4-lines. The incidence possibilities are shown in Figure 3.5.

There are $\binom{(q+1)/2}{2}$ 2-lines with both points contained in $\mathcal{H}_1 \cap \mathcal{H}_2$, and $(\frac{q+2}{2})^2$ 3-lines because a 3-line contains exactly two points of $\mathcal{H}_1$ and exactly two points of $\mathcal{H}_2$, so one point is in $\mathcal{H}_1 \cap \mathcal{H}_2$, one is in $\mathcal{H}_1 \setminus \mathcal{H}_2$, and one is in $\mathcal{H}_2 \setminus \mathcal{H}_1$. If we count pairs of points contained in $\mathcal{H}_1 \setminus \mathcal{H}_2$ plus pairs of points contained in $\mathcal{H}_1 \cap \mathcal{H}_2$ plus pairs of points contained in $\mathcal{H}_2 \setminus \mathcal{H}_1$, we get $3(\frac{q+2}{2})$. On the other hand, we have counted all the 4-lines twice, the 3-lines zero times, and all the other lines in $N(T)$ exactly once. Thus we have proven that

$$3\binom{\frac{q+2}{2}}{2} - \tau_4 = |N(T)| - \tau_3.$$

Now use (Theorem 2.1) $|N(T)| \geq \frac{m}{n(n+1)}\big(2n(q+1)+1-m\big)$, to get

$$3\binom{\frac{q+2}{2}}{2} - \tau_4 \geq \frac{q+2}{4}\left(\frac{5}{2}q+2\right) - \left(\frac{q+2}{4}\right)(q+2) = 3\binom{\frac{q+2}{2}}{2}.$$

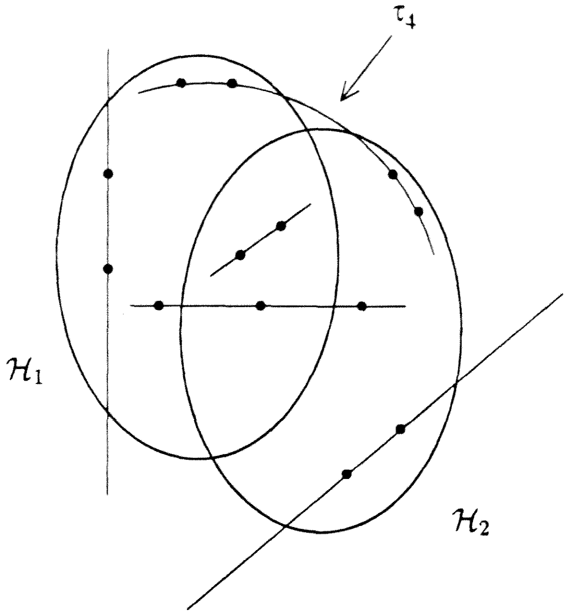

Figure 3.5. The possible intersections for lines with $\mathcal{H}_1 \cup \mathcal{H}_2$.

That is, $\tau_4 = 0$.

Referring back to Figure 3.5, this shows that each line contains exactly zero or two points of $\mathcal{H}_1 \Delta \mathcal{H}_2$. □

Theorem 3.18. *Suppose there are k hyperovals in a plane of even order q with the property that they all contain the same set K_0 of $\frac{q+2}{2}$ points. Then:*

(i) *If $q = 2$ then $k \leq 2$. Equality is possible.*

(ii) *If $q = 4$ then $k \leq 3$. Equality is possible.*

(iii) *If $q = 8$ then $k \leq 2$. Equality is possible.*

(iv) *If $q = 16$ then $k \leq 3$.*

In any case $k \leq 4$.

Proof: Suppose $\mathcal{H}_1, \ldots, \mathcal{H}_k$ are k hyperovals with $K_0 \subseteq \mathcal{H}_i$ for each i. For $i = 1, \ldots, k$ let $K_i := \mathcal{H}_i - K_0$. The K_i for $i = 0, 1, \ldots, k$ are now $k+1$ disjoint sets such that (by Lemma 3.17) any two together make a hyperoval. (The set K_0 is no longer distinguished from the others.) Fix $x_0 \in K_0$ and $x_1 \in K_1$ and let $\ell :=$ the line determined by x_0 and x_1. Then ℓ contains no other points of K_0 or K_1, since $K_0 \cup K_1$ is a hyperoval. Now for any $i > 1$, K_i makes a hyperoval with K_0 to which ℓ must be secant. Since ℓ cannot contain another point of K_0 it must contain exactly one point of K_i.

That is, each K_i contains exactly one point of the line ℓ.

We have proven that $\bigcup_{i=0}^{k}$ is a $(0, 2, k+1)$-set of size $\frac{k+1}{2}(q+2)$. In fact, we have shown that k hyperovals intersecting in the same set of $\frac{q+2}{2}$ points yield $k-1$ mutually orthogonal Latin squares of size $\frac{q+2}{2}$, as follows. Let K_0 label the rows, K_k the columns, and for $i = 1, \ldots, k-1$ in the ith Latin square, into box (a, b), put the element of K_i which is on the $k+1$-line containing the ath element of K_0 and the bth element of K_k. (See §3.7.3 for examples of this construction.) The fact that two points uniquely determine a line shows that the squares are mutually orthogonal.

We know how many lines of each size there are:

$$\tau_2 = (k+1)\binom{\frac{q+2}{2}}{2}$$
$$\tau_{k+1} = \left(\frac{q+2}{2}\right)^2$$

because specifying $x_0 \in K_0$ and $x_1 \in K_1$ determines a unique $k+1$-line, and all $k+1$-lines contain such an x_0 and x_1; whereas a 2-line is determined by selecting one of the $k+1$ K_i's and then picking any two of its $\frac{q+2}{2}$ points.

Thus

$$q^2 + q + 1 \geq \left(\frac{q+2}{2}\right)^2 + (k+1)\binom{\frac{q+2}{2}}{2}$$

$$\Rightarrow k+1 \leq \frac{6q}{q+2} < 6 \tag{3.6}$$

and since k is an integer, this proves $k \leq 4$.

If $q = 2$, equation (3.6) proves $k \leq 2$; Figure 3.6 shows equality is possible.

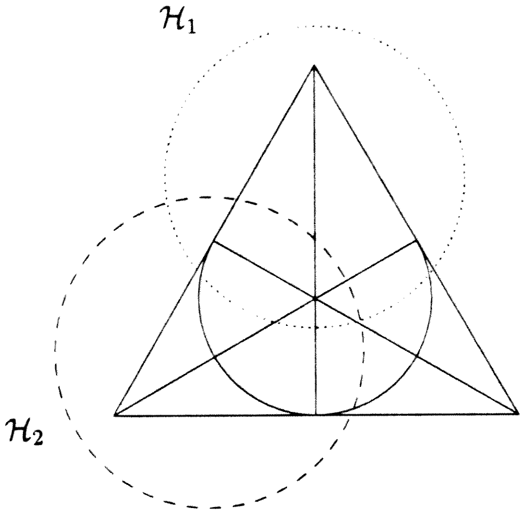

Figure 3.6. Two hyperovals which intersect in half their points in the case $q = 2$.

If $q = 4$, equation (3.6) proves $k \leq 3$. This was previously known ([Hi], p. 396). Equality holds if we let the 3-sets K_i be

$$\{(0,0,1),(1,\alpha,1),(\alpha,1,1)\},\{(0,\alpha,1),(1,1,1),(\alpha,0,1)\}$$

$$\{(\alpha^2,\alpha^2,1),(0,1,0),(1,0,0)\},\{(0,1,1),(1,0,1),(\alpha,\alpha,1)\}$$

where α is as root of x^2+x+1 over F_2.

Now suppose $q = 8$ and consider the quadrics $xy = z^2$ and $x^2+xz+z^2 = y^2$ together with their nuclei. These form two hyperovals intersecting in half their points (five). Thus the upper bound on k is at least 2. Now suppose there are three hyperovals $\mathcal{H}_1$, $\mathcal{H}_2$ and $\mathcal{H}_3$ meeting the hypotheses of this theorem. With labeling as in Theorem 3.15, $K_0 \cup K_1 \cup K_2 \cup K_3$ is a (0,2,4)-set and each $x \in K_3$

lies on five 3-lines of $T := \mathcal{H}_1 \cup \mathcal{H}_2$. Now T is a (0,2,3)-set. Typing the points off T proves that there are only three which lie on five 3-lines, but there would have to be five such points to add to K_0 to complete $\mathcal{H}_3$. So $k \leq 2$ when $q = 8$.

Now suppose $q = 16$ and there are four hyperovals containing the same 9-set, and thus their union is a (0,2,5)-set T of size 45. Typing the points off T results in a matrix equation with no nonnegative solutions. □

Suppose there are a number of hyperovals all of which contain the same set of $\frac{q+2}{2}$ points. With notation as above, by Lemma 3.17, one can take the K_i two at a time and get a set of pairwise disjoint hyperovals. In our consideration of Theorem 3.18, we wondered if an arbitrary set of disjoint hyperovals could be split into $\frac{q+2}{2}$-sets with the property that any two together make a hyperoval (in which case a set of pairwise disjoint hyperovals has at most two hyperovals in it, by Theorem 3.18), and quickly found a counterexample. We were interested then in the question, how big can a set of pairwise disjoint hyperovals be? Corollary 3.20 gives an upper bound.

First we prove a coding theoretic result of use in finding weight enumerators of projective codes. As this result has little bearing on $(0, n, n+1)$-sets or the isoperimetric problem, we forego a discussion of basic coding theory, and mention the result for the reader familiar with the subject, for completeness' sake.

It is known (see, e.g., [AK], p. 260) that the minimum weight codewords in the dual of a projective code correspond to the hyperovals. This theorem addresses the maximum weight codewords.

Theorem 3.19. *Let C be the code of a finite projective plane π of order q even. The largest weight codewords of $C^{\perp}$ have weight q^2 and are the characteristic* *vectors of the affine planes. The next largest weight possible is $q^2 - \sqrt{q}$ which is possible if and only if there is a Baer subplane of π (and the $(q^2 - \sqrt{q})$-weight codewords are the complements of the Baer subplanes). If π is desarguesian and q is not square, the second largest weight possible is at most $q^2 - \sqrt{2q} + \frac{1}{2q}$.*

Proof: A word is in $C^{\perp}$ if and only if it corresponds to a set T with the property that every line intersects T in an even number of places, if and only if every line intersects its complement in an odd number of places. Such sets are called **odd** sets. Every line intersects an odd set in at least one point, so an odd set contains a line or is a blocking set. Thus the vectors of $C^{\perp}$ are the characteristic vectors of complements of odd sets B that are blocking sets or contain a line.

If an odd set B contains a line ℓ and a point x off ℓ, all $q+1$ of the lines from x to ℓ must have another point of B on them, so $|B| \geq 2q+3 \geq q+\sqrt{2q}+1-\frac{1}{2q}$. Now a blocking set has $q+\sqrt{q}+1$ points, with equality if and only if it is a Baer subplane ([Br]). If π is desarguesian and q is not square, then a blocking set has at least $q+\sqrt{2q}+1-\frac{1}{2q}$ points ([BS]). So an odd set B that is blocking or contains a line, has at least $q+\sqrt{q}+1$ points with equality if and only if it is a Baer subplane, and if π is desarguesian and q is not square then $|B| \geq q+\sqrt{2q}+1-\frac{1}{2q}$. Since a word in $C^{\perp}$ is the characteristic vector of $\pi - B$, the result follows. □

The research on minimum sized blocking sets in projective planes is by no means complete. Further results in the area will improve the upper bounds on maximum weight codewords, using the methods described above.

Corollary 3.20. *Suppose A is a set of k pairwise disjoint hyperovals in a plane of order q even.*

(i) *If $q = 2$ then $k = 1$.*

(ii) *If $q = 4$ then $k \leq 2$. Equality is possible.*

(iii) *If $q = 8$ then $k \leq 6$.*

(iv) *If $q = 16$ then $k \leq 14$ with equality if and only if the complement of a Baer subplane can be partitioned into hyperovals.*

(v) *If the plane is desarguesian and $q > 16$ then $k \leq q - 3$.*

Proof: Suppose there are k pairwise disjoint hyperovals. The characteristic vector χ of their union is in the dual code $C^{\perp}$ of the code determined by $PG(2, q)$, and has weight $k(q+2)$. Since $k(q+2)$ does not divide q^2, the previous theorem gives

$$k(q+2) \leq q^2 - \sqrt{q} \tag{3.7}$$

which implies $k \leq q - 3$, or $q < 16$, or $q = 16$ and χ is the characteristic vector of the complement of a Baer subplane.

If $q = 2$ then two disjoint hyperovals would constitute eight points, but there are only seven in the plane of order 2. If $q = 4$, equation (3.7) says $6k \leq 12 \Rightarrow k \leq 2$ and the example of three hyperovals intersecting in half their points given in the proof of Theorem 3.19 suffices to show equality; take two of the 3-sets mentioned in that example as one hyperoval, and the other two as the other hyperoval. If $q = 8$, Theorem 3.19 says $10k \leq 60$ which implies $k \leq 6$. □

3.7.2 The Cases $q = 7$, $m = 12$ or 15

The case $q = 7, m = 12$ is the smallest one for which the previous techniques do not either provide an example of a $(0, n, n+1)$-set or prove there does not exist one. The next case is $q = 7, m = 15$. As discussed in §3.6, there is a (0,2,3)-set of size 12 if and only if there is a (0,2,3)-set of size 15 and they are dual complements. It suffices to find a (0,2,3)-set of size 15, or prove such a set does not exist. In fact we have found such a set. We first present a description of it from [Hi] (p. 356–7) although his only interest in it is as a (15,3)-arc. He knew it had no tangents, but the other interesting combinatorial properties of it which we discuss below are new.

"If $\mathcal{D}$ is a general Desargues' configuration, then each of the ten lines meets three others at no point of the configuration. The 15 points formed in this way are the points of" a (0,2,3)-set of size 15. Call this set T (see Figure 3.7).

We discovered that the set (in homogeneous coordinates)

$$\{(x, \pm x^2, 1) : x \in F_7^*\}$$

is a (0,2,3)-set of size 12. Addition of the points (0,0,1), (0,1,0), and (1,0,0) results in a (0,2,3)-set of size 15. While this 15-set is not the dual complement of the 12-set, it is projectively equivalent to it and to the Hirschfeld example.

The curious thing about this (0,2,3)-set of size 15 is that all the 2-lines form triangles. This allows to create a Steiner triple system on fifteen points as follows. The points are those of T and the blocks consist of the 3-lines plus the sets of three points of a triangle of 2-lines.

There are eighty nonisomorphic Steiner triple systems on fifteen points. They have been catalogued in [Mat] and we have checked that this particular system is number 7 in that catalogue.

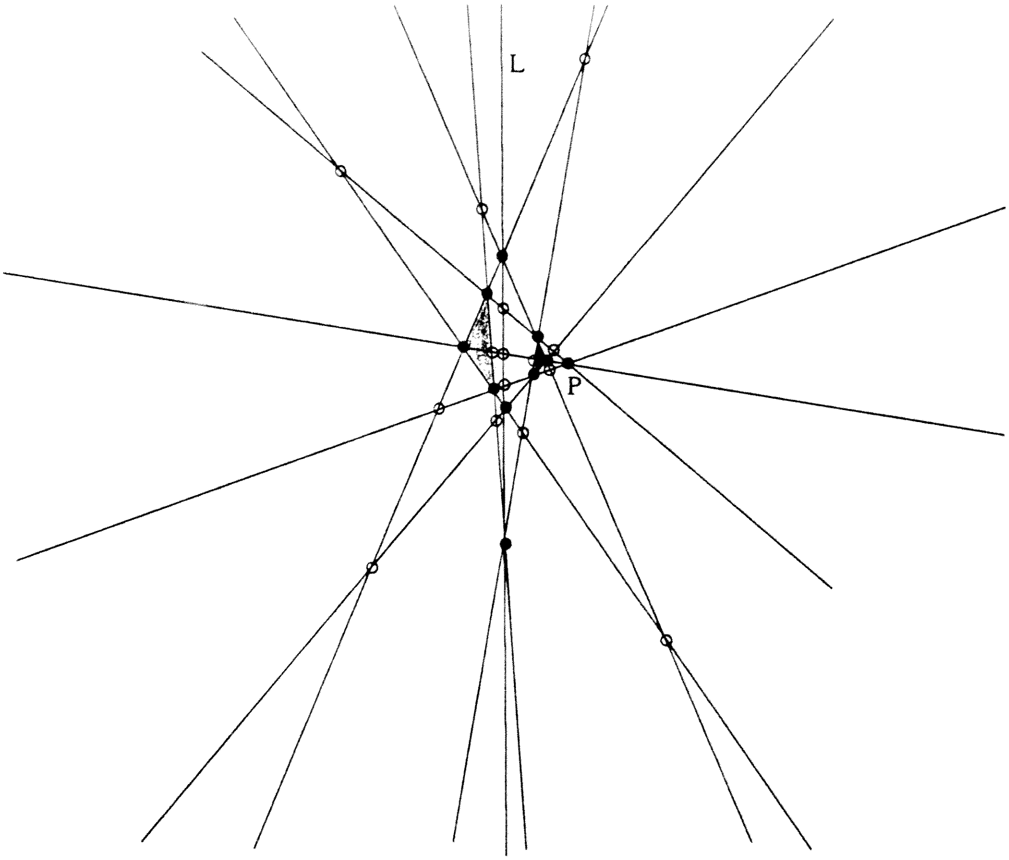

Figure 3.7. The description of T given by Hirschfeld. Points of the Desargues's configuration are marked by solid dots (•) and points of T are marked by open dots (∘). The shaded triangles are perspective with respect to the point **P** and the line **L**.

3.7.3 The Cases $q = 8$ or 16 and $m = 3(q+2)/2$

Suppose F_8 is generated by a root of $x^3 + x + 1$ over F_2. Any two hyperovals intersecting in half their points make a (0,2,3)-set of size 15. Take the examples given in the proof of Theorem 3.16(iii), namely $\mathcal{H}_1$ determined by $x^2+xz+z^2 = y^2$ and $\mathcal{H}_2$ determined by $xy = z^2$ (plus their nuclei). Define $K_1 := \mathcal{H}_1 - \mathcal{H}_2$, $K_2 := \mathcal{H}_2 - \mathcal{H}_1$ and $K_3 := \mathcal{H}_1 \cap \mathcal{H}_2$ and construct a Latin square of size 5 where rows are labeled by K_1, columns by K_2 and entries by K_3.

There are two Latin squares of size 5, the circulant and one with a 2×2 subsquare ([vLW], p. 159). The Latin square obtained from our (0,2,3)-set of size 15 is the noncirculant one. The circulant one cannot be embedded in the plane of order 8, by computer search as described in [S].

In $PG(2,16)$ we have found that the following o-polynomials (see §1.2) determine hyperovals which intersect in half their points:

$$f_1 := x^{12} + x^{10} + \alpha^{11}x^8 + x^6 + \alpha^2x^4 + \alpha^9x^2$$

$$f_2 := \alpha^3x^{14} + x^{12} + \alpha^2x^8 + x^6 + \alpha^8x^4 + \alpha^3x^2$$

where α is a primitive for F_{16} generated by a root of $x^4 + x + 1$ over F_2. The first of these is given in [K] (beware of a typographical error therein) and the second was found by a computer search.

The Latin square determined by these hyperovals is:

$$\begin{pmatrix} 1 & 3 & 2 & 6 & 7 & 9 & 4 & 8 & 5 \\ 3 & 2 & 1 & 8 & 6 & 5 & 7 & 9 & 4 \\ 2 & 1 & 3 & 9 & 8 & 6 & 5 & 4 & 7 \\ 6 & 7 & 5 & 3 & 2 & 4 & 8 & 1 & 9 \\ 7 & 9 & 8 & 2 & 4 & 3 & 1 & 5 & 6 \\ 5 & 8 & 9 & 4 & 3 & 2 & 6 & 7 & 1 \\ 9 & 4 & 6 & 5 & 1 & 7 & 3 & 2 & 8 \\ 4 & 5 & 7 & 1 & 9 & 8 & 2 & 6 & 3 \\ 8 & 6 & 4 & 7 & 5 & 1 & 9 & 3 & 2 \end{pmatrix}$$

where the rows are indexed from top to bottom by the affine points (α, α^8), (α^6, α^{14}), $(\alpha^{11}, \alpha^{12})$, (α^9, α^6), (α^3, α^7), $(\alpha^{12}, \alpha^{11})$, (α^4, α^2), (α^8, α^{10}), (α^7, α^{13}), the columns are indexed left to right by the points (α^{11}, α^8), (α^6, α^{12}), (α, α^{14}), (α^3, α^{10}), (α^9, α^2), $(\alpha^{12}, \alpha^{13})$, (α^8, α^7), (α^4, α^6), (α^7, α^{11}), and the entries $1, \ldots, 9$ correspond respectively to the points (1,0,0), (0,1,0), (1,1,1), $(\alpha^{13}, \alpha^3, 1)$, $(\alpha^5, \alpha, 1)$, (0,1,1), $(\alpha^{10}, \alpha^4, 1)$, $(\alpha^2, \alpha^5, 1)$, $(\alpha^{14}, \alpha^9, 1)$.

Chapter 4. Solutions to the Isoperimetric Problem

We know that the solutions to the isoperimetric problem for $m \leq q+1$ $(q+2)$ if q is odd (even) are the m-arcs. The next case to solve is $m = q+2$ $(q+3)$.

4.1 The Case q Even, $m = q + 3$

Theorem 4.1. *Let a projective plane of even order q be given. Then a hyperoval plus a point is a solution to the isoperimetric problem for $m = q+3$ points. Furthermore, all solutions for $q+3$ points are of this form.*

Proof: First we count $|N(S)|$ where $S = \mathcal{H} \cup \{x\}$ where $\mathcal{H}$ is a hyperoval and x is a point not on it. Since all lines are either 0-lines or 2-lines to $\mathcal{H}$, x must have $\frac{q+2}{2}$ of the latter and hence $\frac{q}{2}$ of the former. So the lines meeting S either meet $\mathcal{H}$, and there are $\binom{q+2}{2}$ of these, or they meet S only at x, and there are $\frac{q}{2}$ of these.

Now let T be any solution to the isoperimetric problem for $m = q+3$. Then

$$|N(T)| \leq |N(S)| = \frac{q^2+4q+2}{2}. \tag{4.1}$$

We will show that equality holds and that T is of the form $\mathcal{H} \cup \{x\}$ for some x.

Call a line ℓ **odd** when $|T \cap \ell|$ is odd, and (as in §3.3) $\sigma_i^x :=$ the number of i-lines on $x \notin T$.

Since $|T|$ is odd, any external line ℓ to T has the property that every point on it has an odd number of odd lines, in particular at least one. We thus have

$$\begin{aligned} q+1 \leq \text{number of odd lines } &\leq \sum_{i\geq 1}(i-2)^2\tau_i \\ &= \sum_{i\geq 1} i(i-1)\tau_i - 3\sum_{i\geq 1} i\tau_i + 4\sum_{i\geq 1}\tau_i \\ &= 4|N(T)| - (q+3)(2q+1) \\ &\leq q+1\,. \end{aligned}$$

The second equality follows from $\sum_{i\geq 1} i(i-1)\tau_i = (q+3)(q+2)$ and $\sum_{i\geq 1} i\tau_i = (q+1)(q+3)$, the last inequality follows from equation (4.1).

It must be that equality holds in each of the inequalities. We consider these from right to left. Equality holding in the last inequality means that $\mathcal{H} \cup \{x\}$ is a solution for any hyperoval $\mathcal{H}$ and any external point x. Equality holding in the middle inequality means that $\tau_i = 0$ for $i > 3$. Finally, we claim that equality holding in the first inequality means that all the odd-lines intersect within T. Now since there are $q+1$ odd lines, no line external to T can have a point with more than one odd line through it. It suffices to show that every point off T lies on a line external to T (for then no odd lines can intersect off T). Solving the incidence equations for τ_1, τ_2, τ_3 gives $\tau_1 = q/2$. So suppose there is a point $y \notin T$ which has no external lines through it. Then

$$\sigma_1^y + \sigma_2^y + \sigma_3^y = q+1$$

$$\sigma_1^y + 2\sigma_2^y + 3\sigma_3^y = q+3$$

which implies $\sigma_1^y = q-1$ or q, contradicting $\sigma_1^y \leq \tau_1$. So every odd line intersects in T, in particular all the 1-lines intersect in T, i.e., they are concurrent, say at z. Then

$$\frac{q}{2} + \sigma_2^z + \sigma_3^z = q+1$$

$$\sigma_2^z + 2\sigma_3^z = q+2$$

so $\sigma_3^z = \frac{q}{2} + 1 = \tau_3$, that is, all the three lines go through z, $T - z$ is a hyperoval, so T is of the form hyperoval plus a point. □

4.2 The Case q Odd, $m = q + 2$

The answer to the isoperimetric problem for $q + 2$ points, odd q is known only for $q \leq 7$ (see §4.3). In the general case the solution will not be as simple as its even-q counterpart given in Theorem 4.1. One indication of this is that in the Hughes plane of order 9, there is a set T of eleven points that is not of the form $K \cup \{x\}$ where K is a 10-arc and x is a point not in S. But T has $|N(T)| = 59 = |N(K \cup \{x\})|$. In the standard (Denniston) notation, it is:

$$T := \{F, N_3, N_4, O_3, O_6, U_4, U_5, S_4, W_7\} \cup \{V_7, V_4\}.$$

T was found as follows. Following the logic in the next section, we started with a complete 9-arc from [Den2], which is the first nine points listed. (Of course there is no complete 9-arc in $PG(2,9)$, so this construction will not transfer to that plane.) We then sought two points off the arc, and on few (the minimum being three) 0-lines, and which shared a 0-line. As luck would have it, two such points existed. We then checked that $T \setminus \{x\}$ is not an arc, for every $x \in T$.

Suppose T is a solution to the isoperimetric problem for $m = q+2$ with q odd. We can say something about T, namely, that no line contains too many points of T (cf. §1.5). This is the substance of the following theorem.

Theorem 4.2. *If T is a solution to the isoperimetric problem for $q+2$ points in a finite projective plane of odd order q, then each line contains less than $\frac{3}{2} + \sqrt{q - \frac{3}{4}}$ points of T.*

Proof: Let $w := \max_{\ell \in N(T)} \mu_\ell$. By equations (2.3),

$$\begin{aligned} \frac{q^2+4q+1}{2} &\geq |N(T)| \\ &= \frac{\sum_{\ell \in N(T)} (\mu_\ell - 1)(\mu_\ell - 2) + q^2 + 3q + 2}{2} \\ &> \frac{(w-1)(w-2) + q^2 + 3q + 2}{2} \\ \Rightarrow w^2 - 3w + 3 - q < 0. \end{aligned}$$

The roots of this quadratic in w are

$$r_\pm = \frac{3 \pm \sqrt{-3+4q}}{2}$$

and $w < r_+$. □

4.3 Nested Solutions

When solving a sequence of extremal problems, such as the isoperimetric problem (given π_q, what is ∂_m for $m = 0, 1, \ldots, q^2 + q + 1$?), one hopes that a greedy algorithm will work. That is, one hopes that a solution for m gives a solution for $m+1$. In the isoperimetric problem case, this means a solution T_{m+1} for $m+1$ points can be obtained by adding a point to a solution T_m for m points. If π is a plane for which this is true for all values of m then π is said to admit a nested solution to the isoperimetric problem, or a nested set of solutions.

Definition: Given a projective plane π of order q, π has a **nested solution** to the isoperimetric problem if there is an ordering $x_1, x_2, \ldots, x_{q^2+q+1}$ of the points of π so that when $T_m := \{x_1, x_2, \ldots, x_m\}$, the T_m satisfy $|N(T_m)| = \partial_m$.

We will show that the planes of order at most 7 have nested solutions and that the plane of order 8 does not.

The existence of nested solutions to the isoperimetric problem in the planes of order 2,3,4 were known ([Ha]). We include nested solutions for these planes because we could not find them in print. The isoperimetric problem was previously unsolved in the planes of order $q = 5, 7$, and in particular it was not known whether there existed nested solutions to the isoperimetric problem in planes of order greater than 4.

4.3.1 The Case $q \geq 7$

The appendix contains a number of tables. Those labeled A.ja give the adjacency matrix of the plane of order q where q is the jth prime power. The adjacency matrices have their rows labeled by points and their columns labeled by lines. The number i associated with a row indicates the order in which the points should be added to get a nested solution. For example in the plane of order 2, each T_m consists of the first m points (rows), whereas in the plane of order 3 one should construct the nested set by starting with the fifth point (the row where $i = 1$), then adding the sixth ($i = 2$), then the eighth ($i = 3$), the ninth ($i = 4$) and so on.

The tables A.ja thereby give the nested sets T_m, and the tables A.jb constitute the bulk of the proofs that for each m, $|N(T_m)| = \partial_m$. We know from Theoreom 2.1 that $\partial_m \geq \left\lceil \frac{m}{n(n+1)}(2n(q+1)+q-m) \right\rceil$ where $n = \left\lfloor \frac{q+m}{q+1} \right\rfloor$, and it is this lower bound for ∂_m which is reported in the tables A.jb. When $|N(T_m)|$ equals this lower bound we need look no further, we have a solution to the isoperimetric problem for that m. For those values of m (marked by an $*$) for which $|N(T_m)|$ is greater than the lower bound given by Theorem 2.1, the rest of this section is dedicated to proving, on a case-by-case basis, that in fact $\partial_m = |N(T_m)|$. First we prove two theoreoms which we will need.

The first theorem is important in its own right. It is in fact the solution to the isoperimetric problem in any plane, for $m \geq \binom{q}{2}$.

Theorem 4.3. *Suppose π is a projective plane of order q. For $1 \leq i \leq q+1$, if*

$$\binom{q}{2} + \binom{i}{2} < m \leq \binom{q}{2} + \binom{i+1}{2}$$

then $\partial_m = q^2 + i$.

Proof: First suppose $m = \binom{q}{2} + \sum_{j=1}^{i} j = \binom{q}{2} + \binom{i+1}{2}$ for some $i \geq 1$. Let K be a k-arc in π^*, where $k = q+1-i$. Then K^{dc} is $q^2+q+1-\binom{k}{2}-k(q+2-k) = \binom{q}{2}+\binom{i+1}{2}$ points. By Lemma 3.1, K is a closed solution; so then is K^{dc} by Theorem 3.5, and by Lemma 3.6 then

$$\begin{aligned} \partial_m &= \partial_{|K^{dc}|} = \partial_{q^2+q+1-\partial_{|K|}} \\ &= q^2+q+1-k = q^2+i \end{aligned}$$

and the theorem is true in this case.

Now suppose $\binom{q}{2} + \sum_{j=1}^{i-1} j < m < \binom{q}{2} + \sum_{j=1}^{i} j$ for some i, necessarily $i > 1$. Then the solution for $\binom{q}{2} + \sum_{j=1}^{i-1} j$ is q^2+i-1 and is closed, so $q^2+i-1 < \partial_m \leq q^2+i$. □

Theorem 4.4. *The only solutions to the isoperimetric problem for $q = 7$, $m = 9$ are of the form $\mathcal{O} \cup \{x\}$ where $\mathcal{O}$ is an oval and x is an exterior point to it.*

Proof: By Lemma 3.4, Theorem 2.1 with $m = 20$, and because ∂_m is increasing with m, we have

$$\begin{aligned} \partial_{57-\partial_9} \leq 48 < \partial_{20} &\Rightarrow 57 - \partial_9 < 20 \\ &\Rightarrow \partial_9 \geq 38, \end{aligned}$$

If $\partial_9 = 38$ then let T be a solution and use equation (2.1) with $n = 1$ and $n = 2$:

$$\sum_{\ell \in N(T)} (\mu_\ell - 1)(\mu_\ell - 2) = 4$$
$$\sum_{\ell \in N(T)} (\mu_\ell - 2)(\mu_\ell - 3) = 12.$$

By the first equation there are exactly two 3-lines and $\mu_\ell \geq 4$ cannot occur. By the second equation, there are six 1-lines, hence thirty 2-lines to round out $N(T)$. The two 3-lines intersect in a point, say x. If $x \in T$ then $T = \mathcal{O} \cup \{x\}$ for some oval $\mathcal{O}$. Now x had either zero or two tangents to $\mathcal{O}$, respectively four or three secants and so four or three 3-lines, but there are only two 3-lines.

So it must be that $x \notin T$. Then x has these two 3-lines, and either a tangent and a secant, or three tangents to T. But the six T-tangents lie one on each of the six points comprising the 3-lines (each such point is on a unique 3-line, hence six secants and so one tangent), giving the desired contradiction.

By our example with $|N(T_9)| = 39$, it must be that $\partial_9 \geq 39$.

Now proceed by contradiction. Suppose T_9 is a solution (that is, a 9-set with $|N(T_9)| = 39$), and that T_9 is not of the form $\mathcal{O} \cup \{x\}$. If T_9 contains a 7-arc T_7, then it is uniquely completable to an oval T_8 so the points off T_7 are either interior points of T_8 (having exactly one T_7-tangent and so four T_7-externals), exterior points (having exactly three tangents and so three externals), or completion points of T_7. There is only one of the latter, and we are assuming neither of the points we add to T_7 to get T_9 is this point. But adding two of the other types of points converts at least five 0-lines of T_7 to lines in $N(T_9)$. Because $|N(T_7)| = 35$, this contradicts $N(T_9) = 39$. So we may assume T_9 contains no 7-arc.

By equation (2.1) with $n = 1, 2$:

$$\sum_{\ell \in N(T_9)} (\mu_\ell - 1)(\mu_\ell - 2) = 6$$
$$\sum_{\ell \in N(T_9)} (\mu_\ell - 2)(\mu_\ell - 3) = 18.$$

Consider the first equation. Every 3-line contributes 2, every 4-line contributes 6 and $\mu_\ell \geq 5$ gives a contradiction. Similar analysis of the second equation results in the fact that T_9 must have either three 3-lines, twenty-seven 2-lines, and nine 1-lines; or a 4-line, thirty 2-lines and eight 1-lines. In the latter case, deleting two points of the 4-line would result in a 7-arc contained in T_9 so we may assume the former case holds. It follows that every point of T_9 lies on the same number of 1-lines as 3-lines.

If the 3-lines do not partition T_9, there will be two points on two 3-lines, or a point on all three 3-lines. In any case there are two points which, when deleted from T_9, leave a 7-arc. It must be that the 3-lines partition T_9.

Case I: The three 3-lines are concurrent. Then we can assume they are concurrent at the point ∞, and label T_9 with homogeneous affine coordinates as shown in Figure 4.1:

Here a, b, c and the y_i are elements of F_7, not 0 or 1, to be determined. The secants between affine points of T_9 on $x = 0, 1$ do not intersect the line $x = c$, so we have that the y_i are not in the following multiset:

$$M := \{0,\ 1,\ c,\ 1 - c,\ (b-1)c + 1,\ bc,\ (b-a)c + a,\ -ac + a,\ (1-a)c + a\}.$$

Yet there are three y_i which satisfy this criterion, so these nine elements must represent only four distinct elements of F_7.

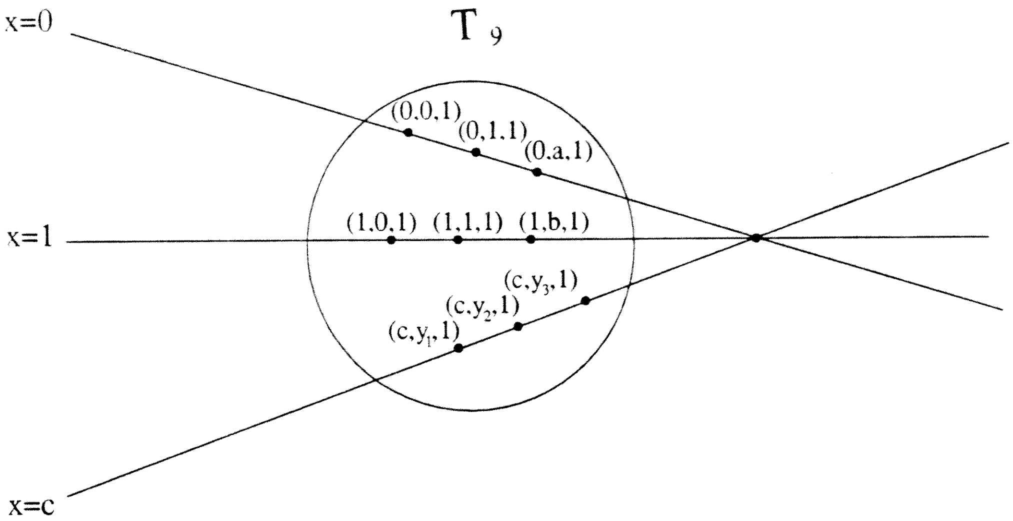

Figure 4.1. Homogeneous coordinates of T_9 if the 3-lines are concurrent.

If $c = 4$ we have $M = \{0, 1, 4, 4(b+1), 4(a+1), 4b, 4a, 4(a+b)\}$ in some order. Since $4b \neq 0, 4$ or $4(b+1)$, and $4(b+1) \neq 1, 4$ or $4b$, either $4b = 1$ $(b = 2)$ or $4(b+1) = 0$ $(b = 6)$. Likewise $a = 2$ or 6, and $a \neq b$. In either case M contains $\{0, 1, 3, 4, 5\}$, more than four elements, a contradiction. So we may assume $c \neq 4$, and so the first four elements of M are distinct. Let $M' := \{0, 1, c, 1-c\}$, the distinct elements of M. Since $bc \neq 0$ or c we have one of two subcases:

<u>If $bc = 1$</u>, then $b = 1/c$, and $(b-1)c + 1$ must be in M'; all possibilities $c = 3, 5, 6$ lead to contradictions, so it must be that $b = 4$, $c = 2$ and $M' = \{0, 1, 2, 6\}$. Now $(b-a)c + a = 1 - a \in M'$ which implies that $1 - a = 2$ or 6 with $a = 6$ or 2 respectively. Then $-ac + a = -a$ =1 or 5 respectively, but it must be in M', so it must be 1, with $a = 6$. This gives a contradiction to $(1-a)c + a \in M'$.

<u>If $bc = 1 - c$</u>, then $(1+b)c = 1$ so $1 + b \neq 0$, $c = \frac{1}{1+b}$. Analysis similar to the above shows that $b = 4$, $c = 3$, $M' = \{0, 1, 3, 5\}$, and $a = 2$, contradicting $(1-a)c + a \in M'$. So we must be in Case II.

Case II: The three 3-lines are not concurrent. Fix a point $x \in T_9$. It has a tangent, a 3-line and six secants – to the six points off its 3-line. Fix a 3-line off x, call it ℓ. The incidence and labeling is shown in Figure 4.2 (x is any of the x_i).

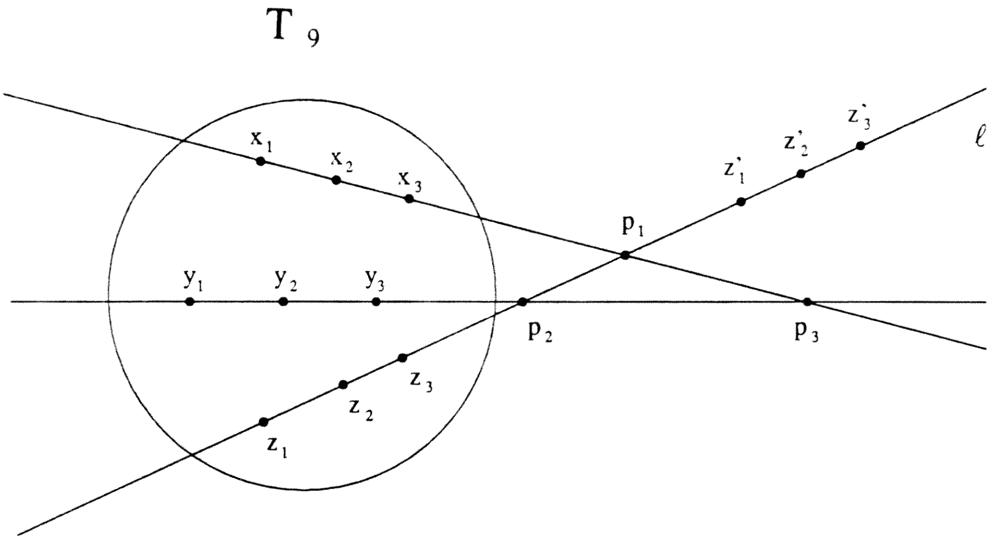

Figure 4.2. The incidences of T_9 if the 3-lines are not concurrent.

The lines on x intersect ℓ at distinct points. The 3-line intersects at p_1, the six secants intersect at y_i and z_i', which are not p_2, and so the tangent must intersect at p_2. All the x_i have their tangents intersecting ℓ at p_2. Each p_i lies on two 3-lines, three 1-lines and so three 0-lines of T_9. The three 0-lines on p_3 must then go through the z_i'. This is true for each vertex p_i of the triangle $\mathcal{T} = \{p_1, p_2, p_3\}$: the 0-lines on a vertex go through the three points on the opposite side of the triangle. Thus we may assign homogeneous coordinates as shown in Figure 4.3 (no three of the points labeled (0,0,1), (0,1,0), (1,0,0) and (1,1,1) are collinear).

Here $x_i \neq 0, 1$; $a, b \neq 0, 1$ or each other, and $c, d \neq 0, 1$ or each other. As in Case I, the nine secant lines between points on $x = 0$ and $x = 1$ contain no points on $y = 0$. That is, there are three $x_i \in F_7$, not 0 or 1, so that $(x_i, 0, 1)$ is not on

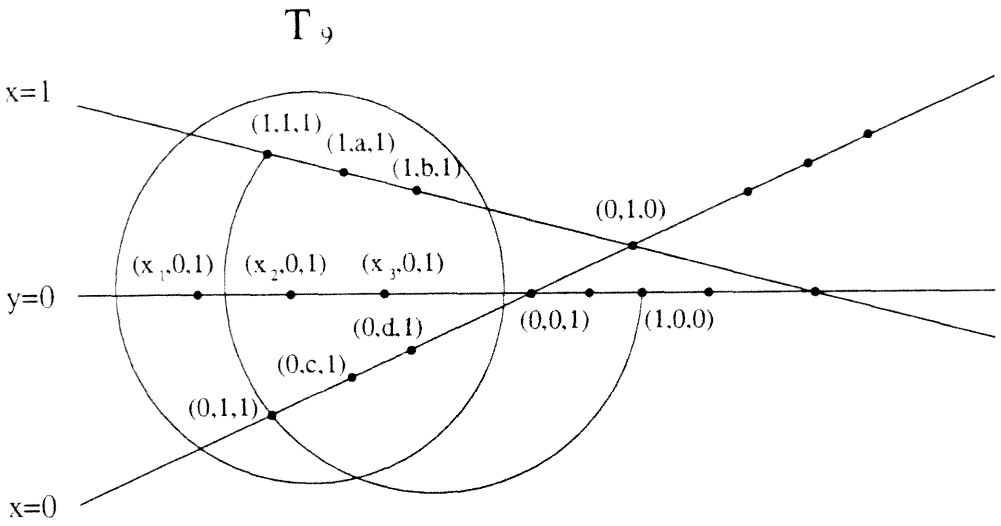

Figure 4.3. Homogeneous coordinates of T_9 if the 3-lines are not concurrent.

any of the lines: $y = 1$, $y = (a-1)x+1$, $y = (b-1)x+1$, $y = (1-c)x+c$, $y = (a-c)x+c$, $y = (b-c)x+c$, $y = (1-d)x+d$, $y = (a-d)x+d$, $y = (b-d)x+d$. The multiset

$$\left\{0, 1, \frac{1}{1-a}, \frac{1}{1-b}, \frac{c}{c-1}, \frac{c}{c-a}, \frac{c}{c-b}, \frac{d}{d-1}, \frac{d}{d-a}, \frac{d}{d-b}\right\}$$

really contains only four distinct elements of F_7.

None of $\frac{c}{c-1}$, $\frac{d}{d-1}$, $\frac{c}{c-a}$, $\frac{d}{d-a}$ are 0 or 1, so these represent at most two elements of F_7. But $c \neq d$ means $\frac{c}{c-1} \neq \frac{d}{d-1}$ so there are at least two elements represented. Thus there are exactly two, represented by $\frac{c}{c-1}$ and $\frac{d}{d-1}$. Since $\frac{d}{d-a} \neq \frac{d}{d-1}$ we have $\frac{d}{d-a} = \frac{c}{c-1}$ and so $d = ac$. Likewise $c = ad$ which implies $a^2 = 1$ and so $a = 6$. But the same result applies to $\frac{c}{c-1}$, $\frac{d}{d-1}$, $\frac{c}{c-b}$, $\frac{d}{d-b}$ with the result that $b = 6$, contradicting $a \neq b$. □

We now proceed with the case-by-case proofs of the discrepancies in the tables A.jb.

For $q = 3$ and $m = 5$: If ∂_m equals the lower bound in Theorem 2.1 then the solutions are (0,1,2)-sets with $\tau_1 = 0$, or perfect 2-arcs which do not exist in odd order planes. So ∂_m is at least one greater than the lower bound; in this case that equals $|N(T_5)|$.

For $q = 5$ and $m = 7$: There is no perfect 2-arc in $PG(2,5)$ so $\partial_7 \geq 22$. Suppose $\partial_7 = 22$ and let T be a solution. Then by equation (2.1):

$$\sum_{\ell \in N(T)} (\mu_\ell - 1)(\mu_\ell - 2) = 44 - 7 \cdot 6 = 2$$

and, as in the proof of Theorem 4.3, it must be that T has exactly one 3-line, and no lines have four or more points of T. Deleting one point x of the 3-line leaves an oval $\mathcal{O}$. Now x was on zero or two tangents to $\mathcal{O}$, thus three or two secants, and so $\mathcal{O} \cup \{x\}$ would have at least two 3-lines, a contradiction. So $\partial_7 \geq 23$ and, by our example, $\partial_7 = 23$.

For $q = 5$ and $m = 8$: $\partial_8 \geq 23$ by Theorem 2.1. If $\partial_8 = 23$ then let T be a solution and use equation (2.1) with $n = 1$ and 2:

$$\sum_{\ell \in N(T)} (\mu_\ell - 1)(\mu_\ell - 2) = 6$$

$$\sum_{\ell \in N(T)} (\mu_\ell - 2)(\mu_\ell - 3) = 2 .$$

By the second equation, either there is one 4-line and no 1-lines, or one 1-line and no 4-lines. With the help of the first equation and $|N(T)| = 23$, we find that T has either: one 4-line and twenty-two 2-lines, or one 1-line, nineteen 2-lines and three 3-lines. But there cannot be a 4-line (each point on it would have to have a tangent, but there are no tangents), so we may assume T has three 3-lines. They cannot be concurrent (if they were, deleting the point of concurrency would result in an arc of size 7), yet there is a point on two of them. It must have a tangent, and since there is a unique tangent, there can be no other points on two 3-lines. The third 3-line meets the other two off T (see Figure 4.4).

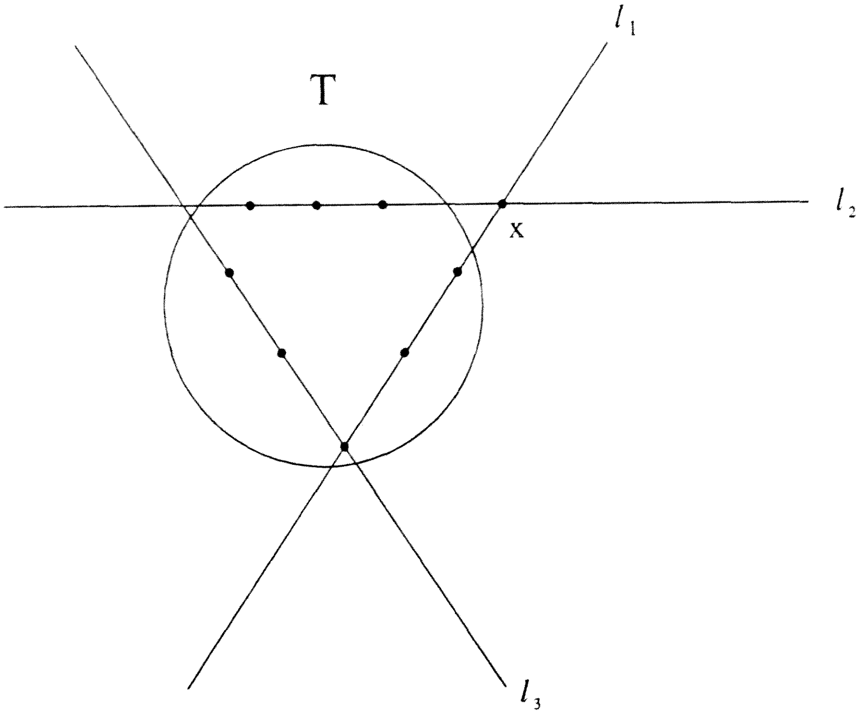

Figure 4.4. The incidence of points if $\partial_8 = 23$ in π_5.

Say $x \notin T$ is on two 3-lines, ℓ_1 and ℓ_2. Then it must have tangents to points on ℓ_3, a contradiction. $\partial_8 \geq 24$ and by our example, $\partial_8 = 24$.

For $q = 5$ and $m = 9$: By Lemma 3.4 and because ∂_m is increasing we have

$$\begin{aligned} \partial_{31-\partial_9} \leq 22 < \partial_7 &\Rightarrow 31 - \partial_9 < 7 \\ &\Rightarrow \partial_9 \geq 25. \end{aligned}$$

By our example, $\partial_9 = 25$.

For $q = 5$ and $m = 12,13,14$: ∂_m is given by Theorem 4.2.

For $q = 7$ and $m = 9$: See Theorem 4.4.

For $q = 7$ and $m = 10$: If $\partial_{10} = 39$ then let T be a solution. Equation

(2.1) with $n = 1$ and 2 gives

$$\sum_{\ell \in N(T)} (\mu_\ell - 1)(\mu_\ell - 2) = 8$$

$$\sum_{\ell \in N(T)} (\mu_\ell - 2)(\mu_\ell - 3) = 4$$

so T has either one 4-line, one 3-line, thirty-six 2-lines and one 1-line; or four 3-lines, thirty-three 2-lines and two 1-lines. With notation as in §3.3, every $x \in T$ satisfies

$$\rho_1^x + \rho_2^x + \rho_3^x + \rho_4^x = 8$$

$$\rho_2^x + 2\rho_3^x + 3\rho_4^x = 9.$$

In particular for x not on a 4-line, $\rho_3^x = \rho_1^x + 1$ is at least one. The 3- and 4-lines therefore cover the points, which cannot happen in the first case above, where there is only one 4-line and one 3-line. So there must be four 3-lines. If they were all concurrent in T then they would not cover the points, so the 3-line incidences are either as in Figure 4.5 or as in Figure 4.6.

First suppose three 3-lines are concurrent in T. Introduce homogeneous coordinates onto these three 3-lines as shown in Figure 4.5. The fourth 3-line is disjoint from the others (in order that the 3-lines cover the points of T) and so is not of the form $x = \mathit{constant}$, nor $y = \mathit{constant}$, so it has the equation $y = mx + k$ for some m and k. Notice $k \neq 0$ because (0,0,1) is not on this line.

The 3-line $x = 0$ meets $y = mx + k$ outside T, at $(0, k, 1)$. Likewise the line $x = 1$ meets $y = mx + k$ at $(1, m + k, 1)$, outside T, and the line ℓ_∞ meets $y = mx + b$ at $(1, m, 0)$, outside T, as shown in Figure 4.5.

The line from $(0, k, 1)$ through (1,0,0) is a secant at (1,0,0) (because (1,0,0) has no tangents) and hence intersects $x = 1$ at (1,1,1) or $(1, b, 1)$; the line through $(0, k, 1)$ and $(1, a, 0)$ then goes through either $(1, b, 1)$ or (1,1,1), respectively. So either (1) $k = 1$ and $b = 1 - a$, or (2) $k = b$ and $b = 1 + a$.

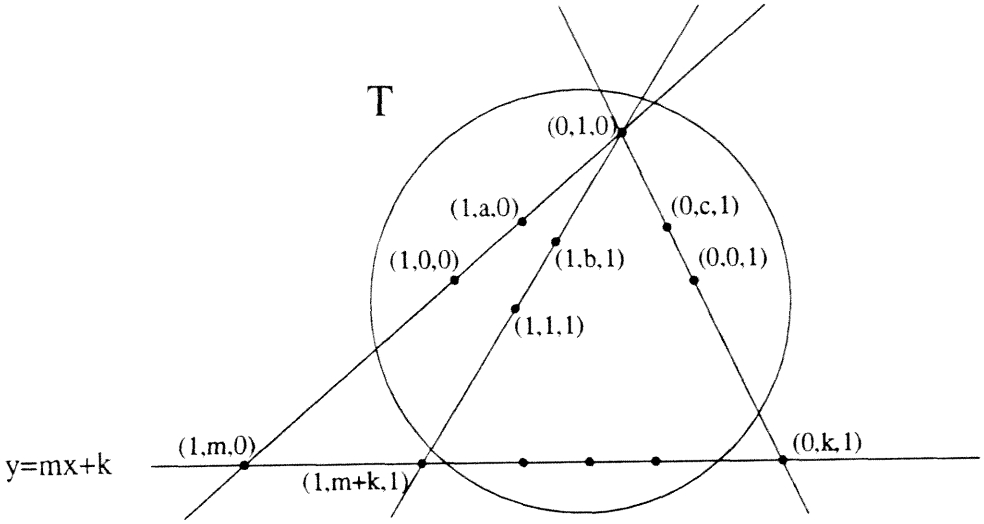

Figure 4.5. Homogeneous coordinates of a solution if $\partial_{10} = 39$ and three 3-lines are concurrent.

Similarly, the two secants on $(1, m+k, 1)$ go through either $(1, a, 0)$, (0,0,1) and (1,0,0), $(0,-c,1)$; or $(1, a, 0)$, $(0, c, 1)$ and (0,0,1), (1,0,0). The first case leads to the contradiction $m+k = a = c$ so it must be that the second case holds, which implies $m = -k$ and $a = -c$.

The secants on $(1, m, 0)$ go through either (1,1,1), (0,0,1) and $(1, b, 1)$, $(0, c, 1)$ or $(1, b, 1)$, (0,0,1) and $(0, c, 1)$, (1,1,1). Thus either (3) $m = 1$ and $b = c+1$ or (4) $m = b = 1 - c$.

Since $m = -k$ we cannot have both (1) and (3), but because $a \neq c$ we cannot have both (1) and (4), a contradiction.

We can now assume the 3-lines are not concurrent, so they must be arrayed as in Figure 4.6. Again there is a 3-line disjoint from the others, and with homogeneous coordinates as shown in Figure 4.6. that disjoint 3-line is $y = mx + k$ where $m, k \neq 0$. Furthermore, the five points of this line which are not in T are $(1, m, 0)$, $(c, mc + k, 1)$, $(0, k, 1)$, $(1, m + k, 1)$, and $(d, md + k, 1)$ for some d. The line $y = 0$ goes through either $(1, m + k, 1)$ or $(d, md + k, 1)$. If it goes through $(1, m + k, 1)$ then the line determined by $(1, m + k, 1)$ and $(1, a, 0)$ is tangent at $(1, a, 0)$, which has only one 3-line and hence no tangents, a contradiction. So $y = 0$ goes through $(d, md + k, 1)$. Then at least two of the three pairs $(d, md + k, 1)$, $(1, b, 1)$ or $(d, md + k, 1)$, (1,1,1) or $(d, md + k, 1)$, (0,1,0) is tangent, again a contradiction.

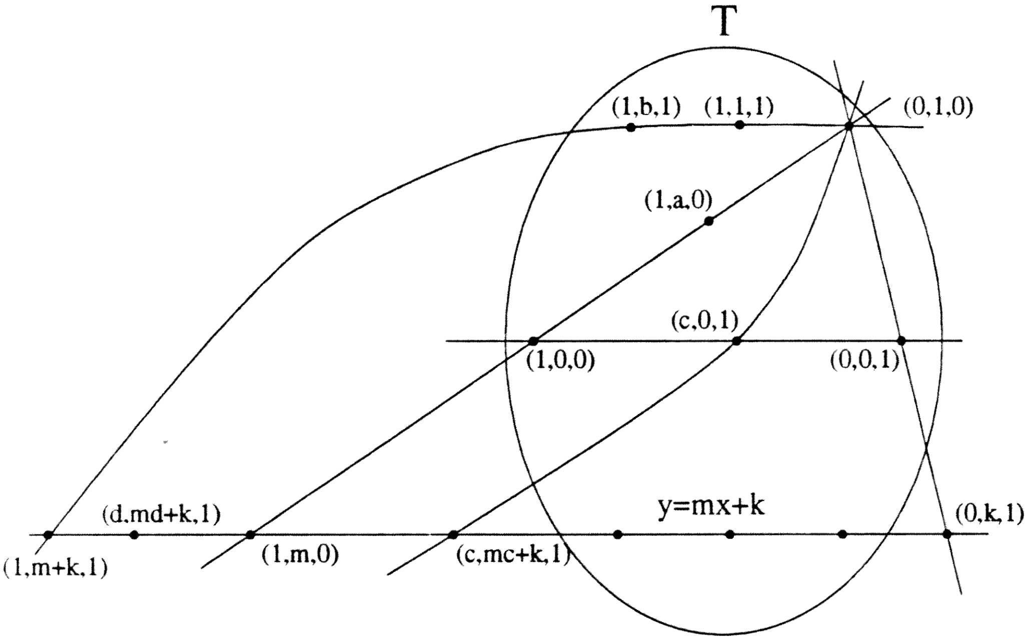

Figure 4.6. Homogeneous coordinates of a solution if $\partial_{10} = 39$ and the 3-lines are not concurrent.

So $\partial_{10} > 39$.

Suppose T is a solution with $|N(T)| = 40$.

$$\sum_{\ell \in N(T)} (\mu_\ell - 1)(\mu_\ell - 2) = 10 = \sum_{\ell \in N(T)} (\mu_\ell - 2)(\mu_\ell - 3).$$

There must be either one 4-line, two 3-lines, thirty-three 2-lines and four 1-lines; or five 3-lines, thirty 2-lines and five 1-lines. In either case pick a point $x \in T$ lying on a tangent. We are assuming $\partial_9 = \partial_{10} - 1$, and since deleting x would decrease the neighborhood by at least one, it must decrease it by exactly one, so there is a unique T-tangent on x. Also, $T \setminus \{x\}$ is a solution to the isoperimetric problem for 9 points. By Theorem 4.4, $T \setminus \{x\}$ is of the form $\mathcal{O} \cup \{y\}$ for some y. But x and y have either three or four lines external to $\mathcal{O}$, so adding them adds at least five lines to $|N(\mathcal{O})|$=36, contradicting $|N(T)| = 40$. By our example, then, $\partial_{10} = 41$.

For $q = 7$ and $m = 11$: If $\partial_{11} = 41 = \partial_{10}$ and T is a solution to the isoperimetric problem for $m = 11$ then no point of T lies on a tangent, or else we could delete that point and get a solution for ten points with neighborhood strictly smaller than ∂_{10}. Thus $\mu_\ell > 1$ for all ℓ. Equation (2.1) with $n = 1, 2$ gives

$$\sum_{\ell \in N(T)} (\mu_\ell - 1)(\mu_\ell - 2) = 16$$

$$\sum_{\ell \in N(T)} (\mu_\ell - 2)(\mu_\ell - 3) = 4$$

and so T has two 4-lines and hence two 3-lines. There must be a point on a 3-line and a 4-line, call it x. If u, v, w are the numbers of 2-lines, 3-lines and 4-lines respectively, on x, then the system

$$u + v + w = 8$$

$$u + 2v + 3w = 10$$

shows that $v + 2w = 2$, contradicting $v, w \geq 1$. By our example then, $\partial_{11} = 42$.

For $q = 7$ and $m = 16$: By Lemma 3.4 and because ∂_m is increasing, we have

$$\partial_{57-\partial_{16}} \leq 41 < \partial_{11} \Rightarrow 57 - \partial_{16} < 11$$

$$\Rightarrow \partial_{16} \geq 47.$$

By our example, $\partial_{16} = 47$.

For $q = 7$, $m = 17$: By Lemma 3.4 and because ∂_m is increasing, we have

$$\begin{aligned} \partial_{57-\partial_{17}} \leq 40 < \partial_{10} &\Rightarrow 57 - \partial_{17} < 10 \\ &\Rightarrow \partial_{17} \geq 48. \end{aligned}$$

By our example, $\partial_{17} = 48$.

For $q = 7$, $m = 18$: By Lemma 3.4 and because ∂_m is increasing, we have

$$\begin{aligned} \partial_{57-\partial_{18}} \leq 39 < \partial_{10} &\Rightarrow 57 - \partial_{18} \leq 9 \\ &\Rightarrow \partial_{18} \geq 48. \end{aligned}$$

By our example, $\partial_{18} = 48$.

For $q = 7$ and $m = 19$: By Lemma 3.4 and because ∂_m is increasing, we have

$$\begin{aligned} \partial_{57-\partial_{19}} \leq 38 < \partial_{9} &\Rightarrow 57 - \partial_{19} < 9 \\ &\Rightarrow \partial_{19} \geq 49. \end{aligned}$$

By our example, $\partial_{19} = 49$.

For $q = 7$, $m = 23,24,25,26,28,32,33$: ∂_m is given by Theorem 4.3.

4.3.2 The Case $q = 8$

Theorem 4.5. *There can be no nested solution to the isoperimetric problem in $PG(2,8)$.*

Proof: If there is a set of nested solutions, $T_{11} \subset T_{12}$. We know from Theorem 4.1 that T_{11} is a hyperoval plus a point, so $T_{12} = \mathcal{H} \cup \{x, y\}$ where $\mathcal{H}$ is a hyperoval and $x, y \notin \mathcal{H}$. x is on at least four 0-lines of $\mathcal{H}$, and y is on at least three others, so $|N(\mathcal{H} \cup \{x, y\})| \geq \partial_{10} + 4 + 3 = 52$.

As in §3.7.1 let α be a primitive element in F_8 generated over F_2 by x^3+x+1. The set of affine points

$$T := \{(0,0,1),(0,1,1),(0,\alpha^4,1),(0,\alpha^5,1),(1,0,1),(1,1,1),$$
$$(1,\alpha^2,1),(1,\alpha^6,1),(\alpha,\alpha^2,1),(\alpha,\alpha^6,1),(\alpha,\alpha^4,1),(\alpha,\alpha^5,1)\}$$

makes a (0,2,4)-set in $PG(2,8)$ which has $|N(T)|$=51, beating 52 for a hyperoval plus two points.

We have just shown that no solution to the isoperimetric problem for 12 points can contain a solution for 11 (since $\partial_{12} < |N(T_{11} \cup \{x\})|$ for all solutions T_{11} for 11 points, and all $x \notin T$). So there can be no nested solutions to the isoperimetric problem in $PG(2,8)$. □

Notice that the set T given above is in fact a solution to the isoperimetric problem, since Table 3.1 (Theorem 3.11) shows that $\partial_{12} \geq 51$.

Appendix

Nested Solutions to the Isoperimetric Problem for Planes of Order q ≤ 7

See section 4.3 for an explanation of the tables.

Table A.1a. An ordering of the points of $PG(2,2)$ giving a nested set of solutions to the isoperimetric problem.

x_i	i
1010100	1
0101100	2
1001010	3
0110010	4
1100001	5
0011001	6
0000111	7

Table A.1b. Solution to the isoperimetric problem for $PG(2,2)$.

m	$\|N(T)_m\|$	Lower Bound Given By Theorem 2.1
1	3	3
2	5	5
3	6	6
4	6	6
5	7	7
6	7	7
7	7	7

Table A.2a. An ordering of the points of $PG(2,3)$ giving a nested set of solutions to the isoperimetric problem.

x_i	i
1001001001000	7
0100100101000	5
0010010011000	6
1000010100100	8
0101000010100	1
0010101000100	2
1000100010010	9
0100011000010	3
0011000100010	4
1110000000001	10
0001110000001	11
0000001110001	12
0000000001111	13

Table A.2b. Solution to the isoperimetric problem for $PG(2,3)$.

m	$\lvert N(T_m)\rvert$	Lower Bound Given By Theorem 2.1
1	4	4
2	7	7
3	9	9
4	10	10
5	*11	10
6	11	11
7	12	12
8	12	12
9	12	12
10	13	13
11	13	13
12	13	13
13	13	13

Table A.3a. An ordering of the points of $PG(2,4)$ giving a nested set of solutions to the isoperimetric problem.

x_i	i
100010001000100010000	1
010001000100010010000	11
001000100010001010000	13
000100010001000110000	17
100001000010000101000	2
010010000001001001000	7
001000011000010001000	14
000100100100100001000	18
100000100001010000100	10
010000010010100000100	3
001010000100000100100	15
000101001000001000100	19
100000010100001000010	9
010000101000000100010	4
001001000001100000010	16
000110000010010000010	20
111100000000000000001	21
000011110000000000001	5
000000001111000000001	8
000000000000111100001	12
000000000000000011111	6

Table A.3b. Solution to the isoperimetric problem for $PG(2,4)$.

m	$\lvert N(T_m)\rvert$	Lower Bound Given By Theorem 2.1
1	5	5
2	9	9
3	12	12
4	14	14
5	15	15
6	15	15
7	17	17
8	18	18
9	18	18
10	19	19
11	19	19
12	19	19
13	20	20
14	20	20
15	20	20
16	20	20
17	21	21
18	21	21
19	21	21
20	21	21
21	21	21

Table A.4a. An ordering of the points of $PG(2,5)$ giving a nested set of solutions to the isoperimetric problem.

x_i	i
1000010000100001000010000100000	11
0100001000010000100001000100000	7
0010000100001000010000100100000	12
0001000010000100001000010100000	26
0000100001000010000100001100000	17
1000000001000100010001000010000	14
0100010000000010001000100010000	21
0010001000100000000100010010000	27
0001000100010001000000001010000	8
0000100010001000100010000010000	1
1000000010010000000100100001000	9
0100000001001001000000010001000	28
0010010000000100100000001001000	2
0001001000000010010010000001000	18
0000100100100000001001000001000	22
1000000100000010100000010000100	29
0100000010100000010000001000100	13
0010000001010000001010000000100	23
0001010000001000001010000000100	3
0000101000000101000000100000100	10
1000001000001000001000001000010	24
0100000100000100001100000000010	4
0010000010000011000001000000010	19
0001000001100000100000100000010	15
0000110000010000010000010000010	30
1111100000000000000000000000001	5
0000011111000000000000000000001	16
0000000000111110000000000000001	20
0000000000000001111100000000001	25
0000000000000000000011111000001	31
0000000000000000000000000111111	6

Table A.4b. Solution to the isoperimetric problem for $PG(2,5)$.

m	$\lvert N(T_m)\rvert$	Lower Bound Given By Theorem 2.1
1	6	6
2	11	11
3	15	15
4	18	18
5	20	20
6	21	21
7	*23	21
8	*24	23
9	*25	24
10	25	25
11	26	26
12	*27	26
13	*27	26
14	*28	27
15	28	28
16	28	28
17	29	29
18	29	29
19	29	29
20	29	29
21	30	30
22	30	30
23	30	30
24	30	30
25	30	30
26	31	31
27	31	31
28	31	31
29	31	31
30	31	31
31	31	31

Table A.5a. An ordering of the points of $PG(2,7)$ giving a nested set of solutions to the isoperimetric problem.

x_i	i
100000010000001000000100000010000001000000100000010000000	22
010000001000000100000010000001000000100000010000010000000	25
001000000100000010000001000000100000010000001000010000000	13
000100000010000001000000100000010000001000000100010000000	9
000010000001000000100000010000001000000100000010010000000	10
000001000000100000010000001000000100000010000001010000000	43
000000100000010000001000000100000010000001000000110000000	28
100000000000010000010000010000010000010000010000001000000	32
010000010000000000001000001000001000001000001000001000000	24
001000001000001000000000000100000100000100000100001000000	16
000100000100000100000100000000000010000010000010001000000	44
000010000010000010000010000010000000000001000001001000000	26
000001000001000001000001000001000001000000000000101000000	19
000000100000100000100000100000100000100000100000001000000	18
100000000000100001000010000000000010000100001000000100000	29
010000000000010000100001000010000000000010000100000100000	45
001000010000000000010000100001000010000000000010000100000	33
000100001000000000001000010000100001000000000001000100000	1
000010000100001000000000001000010000100000000000100100000	2
000001000010000100000000000100001000010000100000000100000	17
000000100001000010000100000000000100001000010000000100000	14
100000000001000100000000001000100000000001000100000010000	11
010000000000100010000000000100010001000000000010000010000	23
001000000000010001000100000000001000100000000001000010000	3
000100010000000000100010000000000100010000000000100010000	27
000010001000000000010001000000000010001000100000000010000	34
000001000100000000001000100010000000000100010000000010000	4
000000100010001000000000010001000000000010001000000010000	46
100000000010000000001001000000000100100000000010000001000	12
010000000001001000000000100000000010010000000001000001000	30
001000000000100100000000010010000000001000000000100001000	5
000100000000010010000000001001000000000100100000000001000	20
000010010000000001000000000100100000000010010000000001000	47
000001001000000000100100000000010000000001001000000001000	6
000000100100000000010010000000001001000000000100000001000	35
100000000100000000100000000101000000001000000001000000100	21
010000000010000000010100000000100000000100000000100000100	36
001000000001000000001010000000010000000010100000000000100	48
000100000000101000000001000000001000000001010000000000100	7
000010000000010100000000100000000101000000001000000000100	8
000001010000000010000000010000000010100000000100000000100	31
000000101000000001000000001000000001010000000010000000100	15

```
100000001000000010000000100000001000000010000000100000010    49
010000000100000001000000010000000100000001100000000000010    37
001000000010000000100000001000000011000000010000000000010    38
000100000001000000010000000110000000100000001000000000010    39
000010000000100000001100000001000000010000000100000000010    40
000001000000011000000010000000100000001000000010000000010    41
000000110000000100000001000000010000000100000001000000010    42
111111100000000000000000000000000000000000000000000000001    50
000000011111110000000000000000000000000000000000000000001    51
000000000000001111111000000000000000000000000000000000001    52
000000000000000000000111111100000000000000000000000000001    53
000000000000000000000000000011111110000000000000000000001    54
000000000000000000000000000000000001111111000000000000001    55
000000000000000000000000000000000000000000111111100000001    56
000000000000000000000000000000000000000000000000011111111    57
```

Table A.5b. Solution to the isoperimetric problem for $PG(2,7)$.

m	$\lvert N(T_m)\rvert$	Lower Bound Given By Theorem 2.1
1	8	8
2	15	15
3	21	21
4	26	26
5	30	30
6	33	33
7	35	35
8	36	36
9	*39	36
10	*41	39
11	*42	41
12	42	42
13	44	44
14	45	45
15	45	45
16	*47	46
17	*48	46
18	*48	47
19	*49	48
20	49	49
21	49	49
22	50	50
23	*51	50

24	*51	50
25	*52	50
26	*52	51
27	52	52
28	*53	52
29	53	53
30	53	53
31	53	53
32	*54	53
33	*54	53
34	54	54
35	54	54
36	54	54
37	55	55
38	55	55
39	55	55
40	55	55
41	55	55
42	55	55
43	56	56
44	56	56
45	56	56
46	56	56
47	56	56
48	56	56
49	56	56
50	57	57
51	57	57
52	57	57
53	57	57
54	57	57
55	57	57
56	57	57
57	57	57

References

[AK] Assmus, E.F. and Key, J.D.: **Designs and Their Codes** (Cambridge Tracts in Mathematics #103). Cambridge University Press, New York, 1992.

[B1] Ball, S.: Multiple blocking sets and arcs in finite planes, *manuscript submitted*, 1995.

[B2] Ball, S.: On the size of triple blocking sets in $PG(2, 8)$, *manuscript submitted*, 1995.

[BB] Ball, S. and Blokhuis, A.: On the size of a double blocking set in $PG(2, 8)$, *manuscript submitted*, 1995.

[Bar] Barlotti, A.: Sui $\{k; n\}$-archi di un piano lineare finito, *Boll. Un. Mat. It. (3)*, **11** (1956), 553–556.

[Bat] Batten, L.M.: **Combinatorics of Finite Geometries**. Cambridge University Press, New York, 1986.

[BSW] Blokhuis, A., Seress, À. and Wilbrink, H.A.: On sets of points in $PG(2, q)$ without tangents, *Mitt. Math. Sem. Giessen*, **201** (1991), 39–44.

[Br] Bruen, A.A.: Arcs and multiple blocking sets, *Symp. Math.*, **28** (1986), 15–29.

[BS] Bruen, A.A. and Silverman, R.: Arcs and blocking sets II, *Eur. J. Comb.*, **8** (1987), 351–356.

[C] Cherowitzo, W.: Hyperovals in desarguesian planes of even order, *Ann. Disc. Math.*, **37** (1988), 87–94.

[DP] Davey, B.A. and Priestley, H.A.: **Introduction to Lattices and Order**. Cambridge University Press, New York, 1990.

[Dem] Dembowski, P.: **Finite Geometries**. Springer-Verlag, New York, 1968.

[Den1] Denniston, R.H.F.: Some maximal arcs in finite projective planes, *J. Comb. Theory*, **6** (1969), 317–319.

[Den2] Denniston, R.H.F.: On arcs in projective planes of order 9, *Manusc. Math.*, 4 (1971), 61–89.

[G] Glynn, D.G.: Two new sequences of ovals in finite desarguesian planes of even order. In: **Combinatorial Mathematics X** (Lecture Notes in Mathematics #1036), pp. 217–229. Springer-Verlag, New York, 1983.

[Ha] Harper, L.: The isoperimetric problem in finite projective planes. Submitted to *Cong. Num.* (Proceedings of the 25th Southeastern Graph Theory Conference).

[Hi] Hirschfeld, J.W.P.: **Projective Geometries Over Finite Fields**. Oxford University Press, New York, 1979.

[HV] Hirschfeld, J.W.P. and Voloch, J.F.: Group-Arcs of prime power order on cubic curves. In: **Finite Geometry and Combinatorics**, pp. 177–185. F. De Clerk et al. eds., Cambridge University Press, Cambridge, 1993.

[K] Korchmáros, G.: Old and new results on ovals in finite projective planes. In: **Surveys in Combinatorics** (London Mathematical Society Lecture Notes Series #166), pp. 41–72. A.D. Keedwell ed., Cambridge University Press, New York, 1991.

[vLW] van Lint, J.H. and Wilson, R.M.: **A Course in Combinatorics**. Cambridge University Press, New York, 1992.

[Mar] Martin, G.E.: On arcs in a finite projective plane, *Can. J. Math.*, **19** (1967), 376–393.

[Mat] Mathon, R.A., Phelps, K.T. and Rosa, A.: Small Steiner triple systems and their properties, *Ars Comb.*, **15** (1983), 3–110.

[O'KP] O'Keefe, C.M. and Penttila, T.: Polynomials for hyperovals of desarguesian planes, *J. Austral. Math. Soc. (A)*, **51** (1991), 436–447.

[PR] Penttila, T. and Royle, G.F.: Sets of type (m, n) in the affine and projective planes of order nine, *Designs, Codes and Crypt.*, **6** (1995), 229–245.

[S] Simonis, J.: Configuraties en computers. In: **Meetkundige Structuren** (CWI Syllabus 28), pp. 43–55. CWI, Amsterdam, 1991.

[Ta] Tallini, G.: On blocking sets in finite projective and affine spaces, *Ann. Disc. Math.*, **37** (1988), 433–450.

[Th1] Thas, J.A.: Projective geometry over a finite field. In: **Handbook of Incidence Geometry**, pp. 295–347. F. Buekenhout ed., Elsevier Science B.V., New York, 1995.

[Th2] Thas, J.A.: Some results concerning $\{(q+1)(n-1)+1; n\}$-arcs in finite projective planes of order q, *J. Comb. Theory (A)*, **19** (1975), 228–232.