Stopping Sets in Codes from Designs[1]

Navin Kashyap Alexander Vardy

Department of Electrical and Computer Engineering
University of California – San Diego, La Jolla, CA 92093-0407, USA
{nkashyap,vardy}@ece.ucsd.edu

Abstract

In this paper, we study stopping sets in LDPC codes arising from 2-designs, of which codes derived from projective and euclidean geometries are a subset. The size of the smallest stopping set in LDPC codes helps in analyzing the performance of such codes under iterative decoding, just as minimum distance helps in analyzing their performance under maximum likelihood decoding. We derive upper and lower bounds on the size of the smallest stopping sets in such codes, and provide examples of codes that actually achieve these bounds.

1 Introduction

Recently, a number of constructions of low-density parity check (LDPC) codes based on finite geometries and combinatorial designs have appeared in the literature, starting with the work of Kou *et al* [1]. These constructions are interesting and useful because they are based on a structured, geometric approach, and yield codes with relatively good minimum distance properties. Furthermore, these codes can be encoded with low complexity and perform very well with iterative decoding. However, there is no real understanding of why these structured LDPC codes perform as well as they do with iterative decoding.

A first step in the process of analyzing the performance of such codes is to study their performance over the binary erasure channel (BEC). As has been shown by Di *et al* [2], the performance of LDPC codes over the BEC is determined by certain combinatorial objects called *stopping sets*. A stopping set $\mathcal{S}$ in an LDPC code is a subset of the variable nodes of the associated Tanner graph such that all neighbors of $\mathcal{S}$ are connected to $\mathcal{S}$ at least twice. The size of the smallest stopping set in an LDPC code plays a role in understanding the performance of the code with iterative decoding over the BEC akin to the role played by the minimum distance of the code in understanding the performance of the code with maximum likelihood decoding over a binary symmetric channel.

In this paper, we study stopping sets in LDPC codes arising from 2-designs, of which the finite-geometry codes of Kou *et al* are a subset. In particular, we derive upper and lower bounds on the size of the smallest stopping sets, and provide examples of codes that actually achieve these bounds.

Since the study of stopping sets is essentially combinatorial in nature, our approach involves design theory only, and we have chosen to write this paper from a design theory viewpoint. Thus, instead of studying stopping sets in codes derived from designs, we define and analyze an equivalent notion of stopping sets in the underlying design. We have tried to make this exposition as self-contained as possible, assuming only the definition and standard notation of t-(v, k, λ) designs (*cf.* [3], Chap. 19).

The structure of the paper is as follows. In Section 2, we introduce the definitions and notation used in the later sections. Section 3 develops a lower bound for the size of the smallest stopping set in a 2-design. In Section 4, we provide examples of 2-designs that have stopping sets whose size achieves the lower bound. Finally, in Section 5, we present a general construction of stopping sets in 2-designs, which yields an upper bound to the size of the smallest stopping set.

2 Definitions and Notation

Definition 1 (2-Design) *A 2-(v, k, λ) design is an incidence structure $(\mathcal{P}, \mathcal{B}, \mathcal{I})$ of a set of* points $\mathcal{P}$, *a set of* blocks $\mathcal{B}$, *and an incidence relation $\mathcal{I} \subset \mathcal{P} \times \mathcal{B}$, with the following properties:*
(i) $|\mathcal{P}| = v$,

[1] Originally written in September 2003; fiddled with several times thereafter. This work was supported by a research grant from Applied Micro Circuits Corporation, San Diego, CA. Parts of this work were presented at the 2003 IEEE International Symposium on Information Theory (ISIT'03), Yokohama, Japan.

(ii) $|B| = k$ *for each* $B \in \mathcal{B}$*, and*
(iii) for any set $T \subset \mathcal{P}$ *with* $|T| = 2$*, there are exactly* λ *blocks incident with all points in* T*,* i.e., $|\{B \in \mathcal{B} : (p, B) \in \mathcal{I} \ \ \forall p \in T\}| = \lambda$.

The number of blocks in a design is conventionally denoted by b, and the number of blocks incident with an arbitrary point is denoted by r (r is called the *replication number*).

We shall only be dealing with *simple* 2-designs, *i.e.*, those without repeated blocks, so we can consider blocks to be subsets of $\mathcal{P}$. As a result, we shall often say that the point p is 'contained in' block B, instead of 'incident with' block B. Also, given a set of blocks $\Sigma \subset \mathcal{B}$ in a design, we shall sometimes be a little loose in our language by writing "a point in Σ" when we mean a point contained in some block in Σ (*i.e.*, a point in $\bigcup_{B \in \Sigma} B$), if this does not create any ambiguity.

For 2-designs, the following relations hold for the parameters v, k, λ, b, r:

$$bk = vr \tag{1}$$

$$\lambda(v-1) = r(k-1) \tag{2}$$

The *incidence matrix* of a design is a $v \times b$ $(0,1)$-matrix N, the rows of which represent the points of the design and the columns represent the blocks of the design. The (i,j)-th entry in N is a one if and only if the ith point is contained in the jth block. Given a design $\mathcal{D}$, we may associate a linear code $\mathcal{C}$ (over $\mathbb{F}_2$) with it, whose parity check matrix is the incidence matrix, N, of $\mathcal{D}$. To be precise, the code $\mathcal{C} \subset {\mathbb{F}_2}^b$ associated with $\mathcal{D}$ is the nullspace, over $\mathbb{F}_2$, of N.

In this paper, we are concerned with special structures called stopping sets that exist within designs.

Definition 2 (Stopping Set) *A set* $\Sigma = \{B_1, B_2, \ldots, B_s\}$ *of blocks in a design* $\mathcal{D}$ *is defined to be a stopping set if for each point* $p \in \bigcup_{i=1}^{s} B_i$*, the set* $\Sigma_p = \{B_i \in \Sigma : p \in B_i\}$ *has cardinality at least 2.*

Note that this definition allows the empty set $\emptyset$ to be a stopping set, but we shall only be concerned with non-empty stopping sets. We shall denote by $s_{\min}$ or $s_{\min}(\mathcal{D})$ the smallest size of a (non-empty) stopping set in $\mathcal{D}$. Stopping sets of size $s_{\min}$ will be called *minimal* stopping sets.

Clearly, the stopping sets in a design $\mathcal{D}$ correspond precisely to the stopping sets in the associated code $\mathcal{C}$. Furthermore, since (the support of) any codeword of weight w in $\mathcal{C}$ is a stopping set of size w in $\mathcal{C}$, and hence in $\mathcal{D}$, it follows that $d_{\min}(\mathcal{C}) \geq s_{\min}(\mathcal{D})$, where $d_{\min}(\mathcal{C})$ denotes the minimum distance of $\mathcal{C}$.

3 Lower Bound for $s_{\min}$

Note that the above definition of a stopping set remains valid for any incidence structure consisting of points and blocks. The following theorem provides a lower bound on the size of stopping sets in a fairly general kind of incidence structure.

Theorem 1 *Let* $\mathcal{S}$ *be an incidence structure of points and blocks such that each block contains exactly* k *points, and each pair of distinct blocks intersects in at most* γ *points. If* Σ *is a stopping set in* $\mathcal{S}$*, then* $|\Sigma| \geq \frac{k}{\gamma} + 1$.

Proof: Let Σ be a stopping set containing s blocks in $\mathcal{S}$, and let n be the total number of points in $\bigcup_{B \in \Sigma}$. We shall count, in two different ways, pairs (p, B) with $B \in \Sigma$ and $p \in B$. There are n points in $\bigcup_{B \in \Sigma}$, and each point is in at least two blocks $B \in \Sigma$ by definition of a stopping set. Hence, the total number of such pairs (p, B) is at least $2n$.

On the other hand, there are s blocks in Σ and each block contains k points. So, there are ks such pairs (p, B), and hence $ks \geq 2n$.

Now, by the inclusion-exclusion principle,

$$\begin{aligned} n &\geq ks - \sum_{B, B' \in \Sigma, \ B \neq B'} |B \cap B'| \\ &\geq ks - \binom{s}{2}\gamma \end{aligned}$$

the second inequality arising from the fact that any two blocks of $\mathcal{S}$ meet in at most γ points.

Therefore, we have $ks \geq 2\left(ks - \binom{s}{2}\gamma\right)$, from which we obtain $s \geq \frac{k}{\gamma} + 1$. ■

The following corollary restricts the result of the above theorem to stopping sets in 2-$(v, k, 1)$ designs.

Corollary 2 *Let Σ be a stopping set in a 2-$(v, k, 1)$ design $\mathcal{D}$. Then, $|\Sigma| \geq k + 1$ with equality only if each point in Σ is incident with exactly 2 blocks in Σ.*

Proof : In a 2-$(v, k, 1)$ design, any two blocks meet in at most one point, so the bound of the above theorem applies with $\gamma = 1$. To obtain the necessary condition for equality, we note that in the proof of the theorem, the inequality $ks \geq 2n$ holds with equality only if each point in Σ is contained in exactly 2 blocks in Σ. ■

Thus, for a 2-$(v, k, 1)$ design, $s_{\min} \geq k + 1$. We shall show later that there do exist families of 2-$(v, k, 1)$ designs for which $s_{\min} = k + 1$. However, before doing so, we provide a useful characterization of precisely when a set of $k + 1$ blocks can form a stopping set in a 2-$(v, k, 1)$ design.

Lemma 3 *Let Σ be a set of $k + 1$ blocks in a 2-$(v, k, 1)$ design. Then, the following statements are equivalent:*
(a) Σ is a stopping set.
(b) Each point in Σ belongs to exactly two blocks in Σ.
(c) The blocks in Σ altogether contain exactly $\binom{k+1}{2}$ points.

Proof: It is clear that the statements (a) and (b) are equivalent since (a) ⇒ (b) is the necessary condition for equality in Corollary 2, and (b) ⇒ (a) follows from the definition of a stopping set. We shall now show that (b) and (c) are equivalent as well.

(b) ⇒ (c): Suppose that each point in Σ belongs to exactly 2 blocks in Σ. If we list out all the points contained in the blocks of Σ, then each point is listed exactly twice. Since there are $k + 1$ blocks in Σ and k points in each block, there are precisely $(k + 1)k/2$ points in Σ.

(c) ⇒ (b): Suppose that the total number of points contained in the blocks of Σ is $\binom{k+1}{2}$. Let $\Sigma = \{B_1, B_2, \ldots, B_{k+1}\}$. By the inclusion-exclusion principle, the number of points in $\bigcup_{i=1}^{k+1} B_i$ is at least $(k + 1)k - \sum_{i<j} |B_i \cap B_j|$. Hence, we have

$$\begin{aligned}\binom{k+1}{2} &\geq (k+1)k - \sum_{i<j} |B_i \cap B_j| \\ &\geq (k+1)k - \binom{k+1}{2} = \binom{k+1}{2}\end{aligned}$$

the second inequality above following from the fact that any two blocks in a 2-$(v, k, 1)$ design intersect in at most one point. Thus, all the above inequalities are in fact equalities. Now, the first inequality can be an equality only if all triple intersections $B_i \cap B_j \cap B_k$ of distinct blocks $B_i, B_j, B_k \in \Sigma$ are empty. So, any point in Σ is contained in at most two blocks in Σ. The second inequality above can be an equality only if $|B_i \cap B_j| = 1$ for all pairs of distinct blocks $B_i, B_j \in \Sigma$. So, any two distinct blocks in Σ meet in exactly one point.

Thus, we can define a mapping ψ that uniquely assigns a point in Σ to each pair of distinct blocks $B_i, B_j \in \Sigma$, via $\psi(B_i, B_j) = B_i \cap B_j$. This mapping is injective as no point can belong to more than two blocks, and is also surjective because the number of pairs of distinct blocks in Σ is $\binom{k+1}{2}$, which is the same as the number of points in Σ. Hence, each point in Σ belongs to precisely two blocks in Σ. ■

In design theory, a set of l blocks containing a total of p points is referred to as a (p, l) configuration. So, the above lemma shows that in a 2-$(v, k, 1)$ design, stopping sets of size $k + 1$ are precisely the $(\binom{k+1}{2}, k + 1)$ configurations. Thus, we have the following corollary to Theorem 1.

Corollary 4 *For a 2-$(v, k, 1)$ design $\mathcal{D}$, $s_{\min}(\mathcal{D}) = k + 1$ if and only if $\mathcal{D}$ contains a $(\binom{k+1}{2}, k + 1)$ configuration. Moreover, if $s_{\min}(\mathcal{D}) = k + 1$, then the minimal stopping sets are precisely all the $(\binom{k+1}{2}, k + 1)$ configurations.*

In a Steiner triple system, STS(v) (*i.e.*, a 2-$(v,3,1)$ design), a $(6,4)$ configuration is known as a Pasch configuration (*cf.* [4], Chap. 13). So, for an STS(v), $s_{\min} = 4$ if and only if it contains a Pasch configuration. Since a $(\binom{k+1}{2}, k+1)$ configuration in a 2-$(v,k,1)$ design generalizes the notion of a Pasch configuration, we shall give it the name *generalized Pasch configuration (GPC).*

As noted in Section 2, if $\mathcal{C}$ is the linear code associated with a design $\mathcal{D}$, then any codeword of weight w in $\mathcal{C}$ gives rise to a stopping set of size w in $\mathcal{D}$, and hence $d_{\min}(\mathcal{C}) \geq s_{\min}(\mathcal{D})$. In particular, if $d_{\min}(\mathcal{C}) = k+1$, then Corollary 2 shows that $s_{\min}(\mathcal{D}) = k+1$ as well.

The converse may not be true, that is, stopping sets of $\mathcal{D}$ may not always arise from codewords in $\mathcal{C}$. However, the converse does hold for stopping sets of size $k+1$ in 2-$(v,k,1)$ designs. Indeed, let N be the incidence matrix of a 2-$(v,k,1)$ design $\mathcal{D}$. If Σ is a stopping set of size $k+1$ in $\mathcal{D}$, then let $\mathbf{x} \in \mathbb{F}_2^b$ be such that the support of $\mathbf{x}$ corresponds exactly to the columns of N that represent the blocks in Σ. It follows from the equivalence of (a) and (b) in Lemma 3 that $N\mathbf{x}^T = \mathbf{0} \pmod 2$, which shows that $\mathbf{x} \in \mathcal{C}$. Hence, if $s_{\min}(\mathcal{D}) = k+1$, then we must also have $d_{\min}(\mathcal{C}) = k+1$, since the $\mathbf{x}$ constructed above is a codeword of weight $k+1$. We have thus proved the following result.

Lemma 5 *Let $\mathcal{C}$ be the code whose parity check matrix is the $v \times b$ incidence matrix of a 2-$(v,k,1)$ design $\mathcal{D}$. Then, the number of codewords of weight $k+1$ in $\mathcal{C}$ is equal to the number of stopping sets of size $k+1$ in $\mathcal{D}$. Hence, $d_{\min}(\mathcal{C}) = k+1$ if and only if $s_{\min}(\mathcal{D}) = k+1$.*

4 Designs Achieving Lower Bound

Two important families of 2-$(v,k,1)$ designs are projective planes and affine planes. These provide examples of designs where the minimal stopping set size is $k+1$, and also examples of designs which do not contain any stopping set of size $k+1$.

Definition 3 (Projective and Affine Planes) *A projective plane of order q is a 2-$(q^2+q+1, q+1, 1)$ design, while an affine (or euclidean) plane of order q is a 2-$(q^2, q, 1)$ design.*

In the language commonly used in the context of projective and affine planes (*cf.* [3], Chap. 19 or [5], Appendix B), blocks of the design are referred to as *lines*. From equations (1) and (2), we find that in a projective plane of order q, there are q^2+q+1 points and q^2+q+1 lines, each line contains $q+1$ points and each point lies on $q+1$ lines. It is a fact that any two distinct lines in a projective plane intersect at a unique point. Thus, if N is the (square) incidence matrix of a projective plane, Π, of order q, then N^T is also the incidence matrix of a "dual" projective plane, Π^T, of order q. The points and lines of Π have their roles reversed in Π^T.

In an affine plane of order q, there are q^2 points and $q(q+1)$ lines. Each line contains q points and each point lies on $q+1$ lines. The $q(q+1)$ lines in the affine plane fall into $q+1$ "parallel classes", each containing q lines. The lines in a parallel class are mutually disjoint (hence the name). It is worth observing that if we delete a line and all the points on it from a projective plane of order q, we obtain an affine plane of order q. In fact, the converse also holds: given an affine plane, $\mathcal{A}$, of order q, there exists a projective plane, Π, of order q such that $\mathcal{A}$ can be obtained from Π by deleting a suitable line and all the points on it. Such a projective plane Π can be constructed as follows: first, enlarge the affine plane $\mathcal{A}$ by adding $q+1$ points to it, in one-to-one correspondence with the $q+1$ parallel classes, and defining each new point to be incident with all the q lines in the corresponding parallel class. Then, add a new line l_∞ that is defined to be incident with all the new points. The resulting structure is a projective plane of order q, and by deleting the line l_∞ along with all the points on it, we obtain the original affine plane $\mathcal{A}$. Thus, an affine plane of order q exists if and only if a projective plane of order q exists.

The most important construction of a projective plane is that of the *desarguesian* plane PG$(2,q)$ for q a prime power. This is obtained by considering the vector space $\mathbb{F}_q^3$ over the finite field $\mathbb{F}_q$, and taking $\mathcal{P}$ to be the set of all 1-dimensional subspaces and $\mathcal{B}$ to be the set of all 2-dimensional subspaces of $\mathbb{F}_q^3$. If a 1-dimensional subspace is contained in a 2-dimensional subspace, then we say that the two are incident.

All the affine planes obtained by deleting a line from $PG(2,q)$ are isomorphic. This affine plane is called the *desarguesian* affine plane AG$(2,q)$. Another contruction of AG$(2,q)$ is obtained by considering the vector space $\mathbb{F}_q^2$ over $\mathbb{F}_q$, and taking $\mathcal{P}$ to be the set of points of $\mathbb{F}_q^2$ and $\mathcal{B}$ to be the set of lines (1-dimensional affine subspaces) in $\mathbb{F}_q^2$.

A generalized Pasch configuration (GPC) in a projective plane, Π, of order q is the dual of a configuration called a hyperoval in the dual plane Π^T.

Definition 4 (Hyperoval) *A hyperoval in a projective plane of order q is a set, $\mathcal{O}$, of $q+2$ points with the property that any line that meets $\mathcal{O}$ meets it in exactly two points.*

From the above definition and the equivalence of statements (b) and (c) in Corollary 2, we see that GPC's in Π are in one-to-one correspondence with hyperovals in Π^T. The following well-known fact about hyperovals, whose proof we include for completeness, shows that a projective plane of odd order q cannot contain a GPC, or equivalently, a stopping set of size $q+2$. Thus, for such a projective plane, $s_{\min} \geq q+3$.

Lemma 6 *If a projective plane of order q contains a hyperoval, or equivalently, a GPC, then q must be even.*

Proof: Let $\mathcal{O}$ be a hyperoval in a projective plane of order q, and let p' be a point not in $\mathcal{O}$. Let $\mathcal{L}$ be the set of lines through p' that meet $\mathcal{O}$. We shall count, in two different ways, the total number of pairs (p, L) such that $L \in \mathcal{L}$ and $p \in \mathcal{O}$ is incident with L. For any $p \in \mathcal{O}$, there exists exactly one line L that contains both p and p'. Hence, there are exactly $q+2$ such pairs (p, L). On the other hand, since each $L \in \mathcal{L}$ meets $\mathcal{O}$, it must meet it in exactly two points by the definition of a hyperoval. Hence, the number of such (p, L) pairs is $2|\mathcal{L}|$. So, we must have $q+2 = 2|\mathcal{L}|$, which shows that q is even. ■

An easy consequence of the above lemma is that an affine plane, $\mathcal{A}$, of odd order q cannot contain a GPC (*i.e.*, a stopping set of size $q+1$) as well, so that $s_{\min}(\mathcal{A}) \geq q+2$.

Corollary 7 *If an affine plane of order q contains a GPC, then q must be even.*

Proof: Suppose that $\mathcal{A}$ is an affine plane of order q that contains a GPC, Σ. So, Σ is a set of $q+1$ lines that contain a total of $\binom{q+1}{2}$ points. Recall that we can construct a projective plane, Π, of order q from $\mathcal{A}$ by adjoining $q+1$ new points to $\mathcal{A}$, along with a new line l_∞ containing all the new points. Defining $\Sigma' = \Sigma \cup l_\infty$, we see that Σ' is a set of $q+2$ lines containing a total of $\binom{q+1}{2} + q + 1 = \binom{q+2}{2}$ points. So, Σ' is a GPC in Π, and hence q must be even. ■

Among projective and affine planes of even order, we restrict our attention to the desarguesian planes PG$(2, 2^s)$ and AG$(2, 2^s)$ for some integer $s > 0$. It is easily seen that any PG$(2, q)$ is isomorphic to its dual PG$(2, q)^T$, via the isomorphism induced by associating subspaces V of $\mathbb{F}_q^3$ with their duals $V^\perp = \{x \in \mathbb{F}_q^3 : x \cdot y = 0 \, \forall \, y \in V\}$. As a result, the GPC's in PG$(2, q)$ are in one-to-one correspondence with the hyperovals in PG$(2, q)$. Furthermore, a GPC in PG$(2, q)$ (if it exists) induces a GPC in AG$(2, q)$, as shown below.

Lemma 8 *If a GPC exists in PG$(2, q)$, then one exists in AG$(2, q)$ as well.*

Proof: Let Σ be a GPC in PG$(2, q)$. Recall that AG$(2, q)$ can be obtained by deleting any line in PG$(2, q)$ along with all the points on that line. In particular, deleting some $l \in \Sigma$ yields AG$(2, q)$ and $\Sigma' = \Sigma \setminus \{l\}$ is a GPC in AG$(2, q)$. ■

Thus, in order to show the existence of GPC's in PG$(2, q)$ and AG$(2, q)$, it suffices to show that hyperovals exist in PG$(2, q)$. Indeed, several constructions of hyperovals are known [6] in PG$(2, q)$, with $q = 2^s$. The simplest of these is the hyperoval consisting of the $q+2$ points $\langle(0, 0, 1)\rangle$, $\langle(0, 1, 0)\rangle$ and $\big\langle(1, x, x^2)\big\rangle$, $x \in \mathbb{F}_q$, where $\langle(a, b, c)\rangle$ denotes the one-dimensional subspace of $\mathbb{F}_q^3$ spanned by (a, b, c). Thus, we have the following theorem.

Theorem 9 *When $q = 2^s$, the projective plane PG$(2, q)$ and the affine plane AG$(2, q)$ both contain GPC's. Consequently, $s_{\min}(PG(2, q)) = q+2$ and $s_{\min}(AG(2, q)) = q+1$.*

Actually, we can also obtain the above theorem from Lemma 5, as it is known (see *eg.* [1]) that the minimum distance of the code derived from PG$(2, 2^s)$ is $2^s + 2$, and the minimum distance of the code derived from AG$(2, 2^s)$ is $2^s + 1$.

5 Upper Bounds for $s_{\min}$

Explicit constructions of stopping sets in a 2-$(v, k, 1)$ design, $\mathcal{D}$, give us upper bounds for $s_{\min}(\mathcal{D})$. We present a method of constructing stopping sets that yields reasonably good upper bounds.

We introduce some notation first. If $P \subset \mathcal{P}$ is a set of points in a design $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$, we denote by Σ_P the set of blocks incident with at least one point in P, and by $\overline{\Sigma}_P$ the set, $\mathcal{B} \setminus \Sigma_P$, of blocks disjoint from P. The following theorem shows that for a suitable choice of P in a 2-$(v, k, 1)$ design, $\overline{\Sigma}_P$ is a stopping set. Recall that r denotes the number of blocks incident with an arbitrary point in a design.

Theorem 10 *Let $\mathcal{D}$ be a 2-$(v, k, 1)$ design, and let P be a set containing at most $r - 2$ points of the design. Then, $\overline{\Sigma}_P$ is a stopping set.*

Proof: Let P be a set of $m \leq r - 2$ points in $\mathcal{D}$. We shall show that any point in $\overline{\Sigma}_P$ can be incident with at most m blocks in Σ_P. Since each point in $\mathcal{D}$ is incident with r blocks, this shows that each point in $\overline{\Sigma}_P$ must be incident with at least $r - m \geq 2$ blocks in $\overline{\Sigma}_P$, so that $\overline{\Sigma}_P$ is a stopping set.

Suppose, to the contrary, that some point, p, in $\overline{\Sigma}_P$ is incident with $m + 1$ blocks in Σ_P. Let $B_1, B_2, \ldots, B_{m+1}$ be these blocks. Being in Σ_P, each B_i, $1 \leq i \leq m + 1$, contains a point in P. Since P has m points and there are $m + 1$ blocks B_i, by the pigeon-hole principle, there exists a $p' \in P$ such that p' is contained in two of the blocks B_i, $1 \leq i \leq m + 1$. Hence, there are two blocks in Σ_P that contain both the points p and p', contradicting the fact that in a 2-$(v, k, 1)$ design, each pair of points is incident with exactly one block. Therefore, each point in $\overline{\Sigma}_P$ can be incident with at most m blocks in Σ_P, thus proving the theorem. ■

Remark: The above theorem also holds for more general kinds of incidence structures. For the result of the theorem to be valid, it is enough for the incidence structure to be such that each point belongs to at least r blocks and each pair of points belongs to at most one block.

To make good use of Theorem 10 to derive upper bounds on $s_{\min}$, the set of points P need to be chosen in such a way as to make Σ_P large. For example, the following bound is useful in some situations.

Corollary 11 *In a 2-$(v, k, 1)$ design, $s_{\min} \leq b - (r - 1)\min(k, r - 2) - 1$.*

Proof: Let $m = \min(k, r - 2)$. Pick any block B from the design, and let P be any m-subset of B. Since $\overline{\Sigma}_P$ is a stopping set by Theorem 10, it suffices to show that $|\overline{\Sigma}_P| = b - m(r - 1) - 1$, or equivalently, $|\Sigma_P| = m(r - 1) + 1$. Note that each of the m points in P belongs to $r - 1$ blocks other than B, and all these blocks are distinct since no two blocks can contain the same pair of points. Thus, P meets $m(r - 1)$ blocks distinct from B. Thus, Σ_P consists of B and $m(r - 1)$ blocks distinct from B, and the result follows. ■

For a projective plane, Π, of order q, the above corollary shows that $s_{\min}(\Pi) \leq 2q$, and for an affine plane, $\mathcal{A}$, of order q, we have $s_{\min}(\mathcal{A}) \leq 2q - 1$. Comparing these bounds with the lower bounds obtained in the previous section for planes of odd order, we see that the upper bounds differ from the lower bounds roughly by a factor of 2. For $q = 3$, however, these bounds actually meet, and hence we find that $s_{\min} = 6$ for a projective plane of order 3, and $s_{\min} = 5$ for an affine plane of order 3.

The bound in Corollary 11 is reasonable when $r - 2 \leq k$. However, if $r - 2 > k$, then there is much room for improvement in the way the set, P, of points was picked in the proof of the bound. For example, it may be verified that for $r > 2k$, the following bound is better than that of Corollary 11.

Corollary 12 *In a 2-$(v, k, 1)$ design, $s_{\min} \leq b - (r + 3)(r - 2)/2$.*

Proof: Let P be any set of $r - 2$ points. By the inclusion-exclusion principle, $|\Sigma_P| \geq r(r - 2) - \binom{r-2}{2} = (r - 2)(r + 3)/2$. The result now follows from Theorem 10. ■

Stopping Sets in Projective Planes

This section contains a compilation of results on stopping sets in projective planes.

Theorem 13 *If a projective plane of order q contains a stopping set of size $q+3$, then $3|q$.*

Proof: Let Σ be a stopping set of size $q+3$ in a projective plane, Π, of order q, and let $L = \{p_1, p_2, \ldots, p_{q+1}\}$ be an arbitrary line (block) in Σ. For each $p_i \in B$, there exists a line $L_i \in \Sigma$, $L_i \neq L$ such that $p_i \in L_i$. These L_i's are all distinct, for if $L_i = L_j$ for some $i \neq j$, then p_i, p_j would be a pair of points belonging to the two lines L and L_i. Thus, Σ contains the $q+2$ distinct lines $\{L, L_1, \ldots, L_{q+1}\}$. Since $|\Sigma| = q+3$, there is one other line, L_{q+2}, in Σ. Since any two lines in Π must intersect at precisely one point, L_{q+2} intersects L at, say, p_1. Thus, p_1 belongs to exactly three lines in Σ, namely, L, L_1 and L_{q+1}, while each of the remaining points $p_j \in L$ belongs to exactly two lines — L and L_j.

Since L is arbitrary, this shows that each line L in Σ contains exactly one point that belongs to exactly three lines in Σ, while each of the remaining q points in L belongs to exactly two lines in Σ.

Let P be the set of points in Σ that are incident with three lines in Σ. We shall count, in two different ways, pairs (p, L) with $p \in P \cap L$ and $L \in \Sigma$. Since each $L \in \Sigma$ contains precisely one point in P, there are $|\Sigma| = q+3$ such pairs. On the other hand, each $p \in P$ belongs to three L's in Σ, so that there are $3|P|$ such (p, L) pairs. We thus have $3|P| = q+3$, which proves the result. ■

Note that by the above result, $\mathrm{PG}(2, 2^s)$ cannot contain any stopping set of size $2^s + 3$. Theorem 13 should be compared with the fact (*cf.* Lemma 6) that a projective plane of order q contains a stopping set of size $q+2$ only if $2|q$. It is tempting to conjecture that stopping sets of size $q+n$ exist only if $n|q$, but this is not true since $\mathrm{PG}(2,7)$ contains a stopping set of size 12, as we shall see later.

Theorem 14 *A projective plane of odd order q cannot contain a stopping set of size $q+4$.*

Proof: Suppose that Σ is a stopping set of size $q+4$ in a projective plane, Π, of odd order q. Let $L = \{p_1, p_2, \ldots, p_{q+1}\}$ be an arbitrary line in Σ, and for $1 \leq i \leq q+1$, pick an $L_i \in \Sigma$, $L_i \neq L$, such that $p_i \in L_i$. Note that each p_i is incident with exactly two of the lines in the set $\mathcal{L} = \{L, L_1, \ldots, L_{q+1}\}$. The set $\mathcal{L}$ accounts for $q+2$ of the lines in Σ, leaving two other lines L_{q+2} and L_{q+3}. Now, either L_{q+2} and L_{q+3} meet L at the same point or they meet L at distinct points. In the former case, L contains exactly one point that is incident with four lines in Σ (L_{q+2}, L_{q+3} and two lines from $\mathcal{L}$), while each of the remaining q points in L is incident with only two lines in Σ. If L_{q+2} and L_{q+3} meet L at distinct points, then L contains precisely two points incident with exactly three lines in Σ, while each of the remaining $q-1$ points in L is incident with only two lines in Σ.

Thus, each point in Σ is incident with either 2, 3 or 4 lines in Σ. For $i = 2, 3, 4$, let P_i be the set of all points in Σ that belong to exactly i lines in Σ. Note that as shown above, any $L \in \Sigma$ satisfies one of the following: (i) L contains 1 point from P_4 and q points from P_2; or (ii) L contains 2 points from P_3 and $q-1$ points from P_2.

We shall count, in two different ways, pairs (p, L) with $L \in \Sigma$ and $p \in L \cap P_3$. Since for each $p \in P_3$, there are exactly 3 lines in Σ containing p, the number of such pairs is precisely $3|P_3|$. On the other hand, any $L \in \Sigma$ contains at most two points from P_3, so that the number of such (p, L) pairs is at most $2|\Sigma| = 2(q+4)$. We thus have $3|P_3| \leq 2(q+4)$ from which we obtain

$$|P_3| \leq \frac{2}{3}(q+4) \tag{3}$$

Now, let $\overline{\Sigma}$ be the set of blocks of Π that are not in Σ. Fix an arbitrary $\overline{L} \in \overline{\Sigma}$, and let x_i, $i = 2, 3, 4$, be the number of points in $\overline{L}$ that are in P_i. Counting, in two different ways, pairs (p, L) such that $L \in \Sigma$ and $p \in L \cap \overline{L}$, we find that $2x_2 + 3x_3 + 4x_4 = q+4$. Since q is odd, we must have $x_3 \neq 0$. In other words, $\overline{L}$ contains a point from P_3. Since $\overline{L}$ is an arbitrary line in $\overline{\Sigma}$, we see that P_3 meets every line in $\overline{\Sigma}$.

By definition, each $p \in P_3$ is incident with exactly 3 lines in Σ, and hence, each $p \in P_3$ is incident with exactly $q+1-3 = q-2$ lines in $\overline{\Sigma}$. Thus, P_3 can meet at most $|P_3|(q-2)$ lines in $\overline{\Sigma}$. Since P_3 meets every line in $\overline{\Sigma}$, it follows that $|\overline{\Sigma}| \leq |P_3|(q-2)$. Hence, applying (3), we find that $|\overline{\Sigma}| \leq \frac{2}{3}(q+4)(q-2)$. But now, we have

$$q^2 + q + 1 = |\Sigma| + |\overline{\Sigma}| \leq q + 4 + \frac{2}{3}(q+4)(q-2)$$

which upon some re-arrangement yields $(q-2)^2 + 3 \leq 0$, which is absurd. ■

It should be noted that the statements of Theorems 13 and 14 are valid for *any* projective plane, not just for the desarguesian planes $\mathrm{PG}(2,q)$. These results yield an improved lower bound on $s_{\min}$ for projective planes of odd order. Specifically, Lemma 6, along with Theorems 13 and 14, show that if Π is a projective plane of odd order q such that q is not divisible by 3, then $s_{\min}(\Pi) \geq q+5$. This is sufficient to determine $s_{\min}$ for $\mathrm{PG}(2,5)$, which happens to be the unique projective plane of order 5. As 5 is odd and not divisible by 3, $s_{\min}(\mathrm{PG}(2,5)) \geq 10$. But, on the other hand, for a projective plane, Π, of order q, we saw earlier (Corollary 11) that $s_{\min}(\Pi) \leq 2q$. Therefore, $s_{\min}(\mathrm{PG}(2,5)) \leq 10$, implying that $s_{\min}(\mathrm{PG}(2,5)) = 10$.

Similarly, for $\mathrm{PG}(2,7)$, we have the lower bound $s_{\min}(\mathrm{PG}(2,7)) \geq 12$, and in fact, by means of a computer search, we can show that a stopping set of size 12 does indeed exist in $\mathrm{PG}(2,7)$. Thus, we have $s_{\min}(\mathrm{PG}(2,7)) = 12$.

It becomes harder to use the techniques used in this section to prove other non-existence results along the lines of Theorems 13 and 14. However, there is one other useful result that can be squeezed out of such arguments. Note that a stopping set, Σ, of size s contains one of size $s-1$ iff there exists a $B \in \Sigma$ such that for each point $p \in B$, the set $\Sigma_p = \{B_i \in \Sigma : p \in B_i\}$ has cardinality at least 3.

Lemma 15 *In a projective plane of order q, a stopping set of size s does not contain stopping sets of size $s-1$, for $s \leq 2q+2$.*

Proof: Let Σ be a (non-empty) stopping set of size $s \leq 2q+2$ in a projective plane Π of order q. Let $L = \{p_1, p_2, \ldots, p_{q+1}\}$ be an arbitrary line in Σ, and for $1 \leq i \leq q+1$, pick an $L_i \in \Sigma$, $L_i \neq L$ such that $p_i \in L_i$. The L_i's are all distinct, and so the set $\mathcal{L} = \{L, L_1, \ldots, L_{q+1}\}$ accounts for $q+2$ lines in Σ. There are $s-(q+2) \leq q$ lines in $\Sigma \setminus \mathcal{L}$. Thus, the lines in $\Sigma \setminus \mathcal{L}$ are incident with at most q points in L, so there exists a point, say, $p_1 \in L$, that does not meet any of the lines in $\Sigma \setminus \mathcal{L}$. Thus, $p_1 \in L$ is incident with exactly one other line in Σ, namely, L_1. ■

Codes from Projective and Affine Planes

The results presented so far show that projective and affine planes of odd order have comparatively larger $s_{\min}$'s than those of even order. Thus, the linear codes associated with planes of odd order have better stopping set properties than those associated with planes of even order. Unfortunately, the linear codes associated with planes of odd order turn out to have poor rates, as we shall show in this section. On the other hand, it is well known that the codes associated with $\mathrm{PG}(2,2^s)$ and $\mathrm{AG}(2,2^s)$ have rates approaching one as s increases.

It should be emphasized that we are only interested in *binary* codes associated with projective and affine planes, *i.e.*, the nullspaces over $\mathbb{F}_2$ of the incidence matrices of the planes. We could also associate non-binary codes with these planes by considering the nullspaces over a non-binary field of the incidence matrices of the planes. Indeed, non-binary codes associated with $\mathrm{PG}(2,q)$ and $\mathrm{AG}(2,q)$ for odd q may have good rates (see *e.g.*, [5, Chapter 13, Theorem 13]).

Let $\mathcal{C}_q$ be the binary linear code associated with $\mathrm{PG}(2,q)$, and let $\mathbb{C}_q$ be that associated with $\mathrm{AG}(2,q)$. It is known (again, see *e.g.*, [5, Chapter 13, Theorem 13]) that for $q = 2^s$, $\mathcal{C}_q$ is a code of length $q^2+q+1 = 4^s+2^s+1$ and dimension $4^s-3^s+2^s$, while $\mathbb{C}_q$ is a code of length $q(q+1) = 4^s+2^s$ and dimension $4^s-3^s+2^s$. Thus, both $\mathcal{C}_q$ and $\mathbb{C}_q$ have rates approaching one as s increases.

We now provide purely combinatorial derivations of the dimensions of the codes associated with projective and affine planes of odd order. Thus, the results are not restricted to the desarguesian planes alone.

Theorem 16 *The binary linear code associated with a projective plane of odd order q is the repetition code of length q^2+q+1.*

Proof: Let Π be a projective plane of odd order q, and let $\mathcal{C}$ be the associated binary linear code. We need to show that $\mathcal{C}$ consists of the all-zeros and all-ones codewords alone.

Let N be the incidence matrix of Π. Since each row of N contains $q+1$ ones, and $q+1$ is even, the all-ones word, $\mathbf{1}$, is in $\mathcal{C}$. Now, suppose that there exists a codeword $\mathbf{c} \in \mathcal{C}$ such that $0 < w_H(\mathbf{c}) < q^2+q+1$, where $w_H(\mathbf{c})$ denotes the Hamming weight of $\mathbf{c}$. We may assume that $w_H(\mathbf{c})$ is odd, for otherwise, we could consider the codeword $\mathbf{1} \oplus \mathbf{c}$ instead. So, there exists a set, Σ, of lines in Π such that $|\Sigma|$ is odd, $0 < |\Sigma| < q^2 + q + 1$, and each point in Π is incident with an even number of lines in Σ. Since $|\Sigma| < q^2 + q + 1$, there exists a line $\overline{L} \notin \Sigma$. We count, in two different ways, pairs (p, L) such that $L \in \Sigma$ and $p \in L \cap \overline{L}$. Since each $L \in \Sigma$ meets $\overline{L}$ in a unique point p, there are $|\Sigma|$ such pairs. On the other hand, each $p \in \overline{L}$ belongs to an even number of lines in Σ, implying that the number of (p, L) pairs under consideration is even. Thus, $|\Sigma|$ must be even, which is a contradiction. ■

Thus, the binary linear code associated with any projective plane of odd order q has dimension 1, which shows that the rate of such a code is $\frac{1}{q^2+q+1}$. Correspondingly, the rate of a code associated with an affine plane of odd order q is $\frac{1}{q+1}$, as is clear from the next result.

THEOREM 17 *The binary linear code associated with an affine plane of odd order q has dimension q.*

In what follows, we fix an affine plane, $\mathcal{A}$, of odd order q, and let $\mathcal{L}_1, \mathcal{L}_2, \ldots, \mathcal{L}_{q+1}$ denote the $q + 1$ parallel classes of $\mathcal{A}$. Furthermore, we denote by $\mathcal{C}$ the binary linear code associated with $\mathcal{A}$, and given a codeword $\mathbf{c} \in \mathcal{C}$, we let $\Sigma_{\mathbf{c}}$ denote the set of lines of $\mathcal{A}$ corresponding to the support set of $\mathbf{c}$. Observe that the all-ones word, $\mathbf{1}$, is in $\mathcal{C}$, since each row of the incidence matrix of $\mathcal{A}$ contains $q + 1$ ones, and $q + 1$ is even. The proof of Theorem 17 relies on the following lemma.

LEMMA 18 *For each $\mathbf{c} \in \mathcal{C}$, there exists an $I \subset \{1, 2, \ldots, q + 1\}$ such that $\Sigma_{\mathbf{c}} = \bigcup_{i \in I} \mathcal{L}_i$.*

Proof: Fix an arbitrary $\mathbf{c} \in \mathcal{C}$, and let $\Sigma = \Sigma_{\mathbf{c}}$. To prove the lemma, it suffices to show that for each $i \in \{1, 2, \ldots, q + 1\}$, either $\mathcal{L}_i \subset \Sigma$ or $\mathcal{L}_i \cap \Sigma = \emptyset$.

For $i = 1, 2, \ldots, q+1$, let $x_i = |\mathcal{L}_i \cap \Sigma|$. Suppose that there exists an i such that $0 < x_i < q$. We first claim that we may take $|\Sigma| - x_i$ to be odd, for otherwise, we may replace $\mathbf{c}$ with the codeword $\mathbf{1} \oplus \mathbf{c}$. Indeed, setting $\overline{\Sigma} = \Sigma_{\mathbf{1} \oplus \mathbf{c}}$ and $\overline{x}_i = |\mathcal{L}_i \cap \overline{\Sigma}|$, $i = 1, 2, \ldots, q+1$, we see that $\overline{x}_i = q - x_i$. Hence, $0 < x_i < q$ iff $0 < \overline{x}_i < q$. Furthermore, $|\overline{\Sigma}| - \overline{x}_i = q(q + 1) - |\Sigma| - (q - x_i) = q^2 - (|\Sigma| - x_i)$, showing that $|\Sigma| - x_i$ is even iff $|\overline{\Sigma}| - \overline{x}_i$ is odd.

So, we have an $i \in \{1, 2, \ldots, q + 1\}$ such that $0 < x_i < q$ and $|\Sigma| - x_i$ is odd. Since $x_i < q$, there exists an $\overline{L} \in \mathcal{L}_i \setminus \Sigma$. As usual, we count pairs (p, L) with $L \in \Sigma$ and $p \in L \cap \overline{L}$, in two different ways. If $L \in \Sigma \cap \mathcal{L}_i$, then L and $\overline{L}$ do not intersect as they belong to the same parallel class. However, if $L \in \Sigma \setminus \mathcal{L}_i$, then L and $\overline{L}$ intersect in exactly one point. Thus, the number of (p, L) pairs being counted is $|\Sigma \setminus \mathcal{L}_i| = |\Sigma| - x_i$. On the other hand, each $p \in \overline{L}$ is incident with an even number of lines in Σ, since Σ supports a codeword. Thus, there must be an even number of (p, L) pairs of interest, which contradicts the fact that $|\Sigma| - x_i$ is odd.

Thus, for each $i \in \{1, 2, \ldots, q + 1\}$, $x_i = 0$ or q, so that either $\mathcal{L}_i \cap \Sigma_{\mathbf{c}} = \emptyset$ or $\mathcal{L}_i \subset \Sigma_{\mathbf{c}}$, which proves the lemma. ■

Proof of Theorem 17: We shall show that there exists a bijection between the sets $\mathcal{C}$ and $\mathcal{E} = \{I \subset \{1, 2, \ldots, q + 1\} : |I| \text{ is even}\}$. It follows that $|\mathcal{C}| = |\mathcal{E}| = 2^q$, and hence, $\dim(\mathcal{C}) = q$.

Consider an arbitrary $I \subset \{1, 2, \ldots, q + 1\}$ and set $\mathcal{L}_I = \bigcup_{i \in I} \mathcal{L}_i$. Recall that there are q disjoint lines in a parallel class $\mathcal{L}_i$, each containing q points, and so the lines in $\mathcal{L}_i$ cover all of $\mathcal{A}$, with each point in $\mathcal{A}$ incident with exactly one line in $\mathcal{L}_i$. Thus, each point in $\mathcal{A}$ is incident with exactly $|I|$ lines in $\mathcal{L}_I$, one from each $\mathcal{L}_i$ with $i \in I$. Hence, $\mathcal{L}_I = \Sigma_{\mathbf{c}}$ for some $\mathbf{c} \in \mathcal{C}$ iff $|I|$ is even. This fact, in conjunction with Lemma 18, establishes the required one-to-one correspondence between the sets $\mathcal{C}$ and $\mathcal{E}$. ■

In summary, binary codes associated with projective and affine planes of odd order q have rates approaching zero as q increases. So, even though such codes have good stopping set properties, they are not of much practical use.

Enumerating Stopping Sets

Our investigations so far have focused on the issue of existence or non-existence of stopping sets of certain sizes in a design. A far more difficult problem is one of actually determining the number of stopping sets of various sizes in a design or its associated code. In other words, given a design, we would ideally like to be able to determine its *stopping set weight distribution* (analogous to the notion of codeword weight distribution), as this would enable us to analyze the performance of the associated code more precisely.

Definition 5 (Stopping Set Weight Enumerator (SSWE)) *The stopping set weight enumerator of a design $\mathcal{D}$ with b blocks is the polynomial*

$$E_{\mathcal{D}}(z) = \sum_{i=0}^{b} e_i(\mathcal{D})\, z^i,$$

where $e_i(\mathcal{D})$ is the number of stopping sets of size i in $\mathcal{D}$.

Observe that we always have $e_0(\mathcal{D}) = 1$, as the empty set is a stopping set, and $e_i(\mathcal{D}) = 0$ for $0 < i < s_{\min}(\mathcal{D})$.

In this section, we illustrate the difficult nature of the problem of analytically determining the SSWE of a design by attempting the computations for two small projective planes, PG$(2,2)$ and PG$(2,4)$. For PG$(2,2^s)$, some of the coefficients $e_i(\text{PG}(2,2^s))$ are easily determined, and we list these in the following lemma.

Lemma 19 *Let $e_i = e_i(PG(2,2^s))$. Then,*

(i) $e_0 = 1$; $e_i = 0$ for $0 < i < 2^s + 2$;

(ii) for $i = 2^s + 2$, e_i is the number of codewords of weight $2^s + 2$ in the binary linear code associated with $PG(2,2^s)$;

(iii) for $i = 2^s + 3$, $e_i = 0$;

(iv) for $4^s + 2 \leq i \leq 4^s + 2^s + 1$, $e_i = \binom{4^s+2^s+1}{i}$.

Proof: (i) follows from the fact that $s_{\min}(\text{PG}(2,2^s)) = 2^s + 2$, (ii) from Lemma 5, and (iii) from Theorem 13. For (iv), we note that any set, Σ, of i lines, $4^s + 2 \leq i \leq 4^s + 2^s + 1$, forms a stopping set. This is because any point in PG$(2,2^s)$ belongs to at most $4^s + 2^s + 1 - i \leq 2^s - 1$ lines not in Σ, and hence to at least $2^s + 1 - (2^s - 1) = 2$ lines in Σ. ■

The above lemma is enough to completely determine the SSWE for PG$(2,2)$:

$$E_{PG(2,2)}(z) = 1 + 7z^4 + 7z^6 + z^7.$$

Only the fact that $e_4(\text{PG}(2,2)) = 7$ needs some explanation: the code associated with PG$(2,2)$ is the [7,3,4] simplex code in which all seven non-zero codewords have weight 4.

In the case of PG$(2,4)$, Lemma 19 determines the coefficients $e_i(\text{PG}(2,4))$ for $0 \leq i \leq 7$ and $18 \leq i \leq 21$. The only nontrivial coefficient among these is $e_6(\text{PG}(2,4))$. The code associated with PG$(2,4)$ is a [21,11,6] code, which can be shown to have 168 codewords of weight 6, implying that $e_6(\text{PG}(2,4)) = 168$. The coefficients $e_8(\text{PG}(2,4))$ and $e_9(\text{PG}(2,4))$ can also be determined analytically, but it requires a lot more effort to do so, as we show next.

Recall the notation introduced in Section 5: if P is a set of points in a design $\mathcal{D}$, we denote by $\overline{\Sigma}_P$ the set of blocks disjoint from P.

Lemma 20 *Let Σ be a set of lines in $PG(2,4)$. The following statements are all equivalent:*

(i) Σ is a stopping set of size 8.

(ii) Σ supports a codeword of weight 8 in the associated [21,11,6] code.

(iii) $\Sigma = \overline{\Sigma}_P$ for some set P consisting of 3 points that are collinear.

Proof: We first prove the implications $(ii) \Rightarrow (i)$ and $(iii) \Rightarrow (i)$. The first of these is clear since the lines corresponding to the support set of any codeword form a stopping set. For the second implication, we first note that if P is a set of 3 points in PG$(2,4)$, then $\overline{\Sigma}_P$ is a stopping set by Theorem 10. Furthermore, if the 3 points in P are collinear, then applying the inclusion-exclusion principle, we obtain $|\overline{\Sigma}_P| = 21 - 3 \times 5 + \binom{3}{2} - 1 = 8$.

$(i) \Rightarrow (ii), (iii)$: Let Σ be a stopping set of size 8 in PG$(2,4)$. Let P_i, $i \geq 2$, be the set of points in Σ that are incident with exactly i lines in Σ. As argued in the proof of Theorem 14, each line $L \in \Sigma$ satisfies one of the following: (a) L contains 3 points from P_2 and 2 from T_3, or (b) L contains 4 points from P_2 and 1 from P_4. Let x be the number of lines in Σ satisfying (a), y be the number of lines in Σ that satisfy (b). We then have

$$x + y = 8 \tag{4}$$

For $i = 2, 3, 4$, we count pairs (p, L) with $L \in \Sigma$ and $p \in L \cap P_i$ to obtain the three equations

$$\begin{aligned} 2|P_2| &= 3x + 4y & (5)\\ 3|P_3| &= 2x & (6)\\ 4|P_4| &= y & (7) \end{aligned}$$

Now, (7) implies that $4|y$, and hence, from (4), we find that $4|x$ as well. Moreover, from (6), we see that $3|x$, from which we conclude that $12|x$. However, since $x \leq 8$, we must have $x = 0$, so that $y = 8$.

Thus, all 8 lines in Σ have 4 points from P_2 and 1 from P_4. In other words, each point in Σ is incident with an even number of lines in Σ, which shows that Σ supports a codeword in the [21,11,6] code, thus proving $(i) \Rightarrow (ii)$.

Plugging in $x = 0$ and $y = 8$ into (5)–(7), we obtain $|P_2| = 16$, $|P_3| = 0$ and $|P_4| = 2$. Hence, the total number of points in Σ is $|P_2| + |P_3| + |P_4| = 18$. Therefore, there are $21 - 18 = 3$ points of PG$(2,4)$ that lie outside Σ. Let P be the set consisting of these 3 points. We thus have $\Sigma \subset \overline{\Sigma}_P$, and $\overline{\Sigma}_P$ is a stopping set by Theorem 10.

Now, if there is no line containing all 3 points in P, then applying the inclusion-exclusion principle, we see that $|\overline{\Sigma}_P| = 21 - 3 \times 5 + \binom{3}{2} = 9$. So, Σ is a proper subset of $\overline{\Sigma}_P$, which is impossible by Lemma 15. Therefore, there must be a line containing all 3 points in P, which proves the implication $(i) \Rightarrow (iii)$. ■

It follows from the above lemma that $e_8(\text{PG}(2,4)) = 210$, since the number of ways of choosing three points from the same line in PG$(2,4)$ is $21 \cdot \binom{5}{3} = 210$.

Lemma 21 *Σ is a stopping set of size 9 in PG$(2,4)$ if and only if $\Sigma = \overline{\Sigma}_P$ for some P consisting of 3 points that are not collinear.*

Proof: If P is a set containing 3 points that are not collinear, then $|\overline{\Sigma}_P| = 9$ by the inclusion-exclusion principle, and $\overline{\Sigma}_P$ is a stopping set by Theorem 10.

For the converse, let Σ be a stopping set of size 9, and let P_i, $2 \leq i \leq 5$, be the set of points in Σ that are incident with exactly i lines in Σ. Setting $\tau_i = |P_i|$, we put down the inequality

$$\sum_{i=2}^{5} \tau_i \leq 21 \tag{8}$$

Each line $L \in \Sigma$ satisfies one of the following: (i) L contains 3 points from P_3 and 2 points from P_2; (ii) L contains 1 point from P_4, 1 point from P_3 and 3 points from P_2; or (iii) L contains 1 points from P_5 and 4 points from P_2.

Counting, in two different ways, pairs (p, L) with $p \in$ Ł and $L \in \Sigma$, we get

$$\sum_{i=2}^{5} i\tau_i = 45 \tag{9}$$

Counting in two different ways, triples (p, L_1, L_2) with $p \in L_1 \cap L_2$ and $L_1, L_2 \in \Sigma$, $L_1 \neq L_2$, yields

$$\sum_{i=2}^{5} \binom{i}{2} \tau_i = \binom{9}{2} = 36 \tag{10}$$

It is not hard to see that there are three valid solutions, $(\tau_2, \tau_3, \tau_4, \tau_5)$, to (8)–(10): (9,9,0,0), (14,4,0,1) and (15,1,0,3). We further whittle down the solution space as follows.

Let $\overline{\Sigma}$ be the set of lines not in Σ, and fix a line $\overline{L} \in \overline{\Sigma}$. Let x_i, $2 \leq i \leq 5$, be the number of points in $\overline{L} \cap P_i$. Note that $x_5 = 0$ as any point in P_5 belongs to 5 lines in Σ, and hence cannot belong to any line in $\overline{\Sigma}$. Now, counting in two ways, pairs (p, L) with $L \in \Sigma$ and $p \in L \cap \overline{L}$, we obtain $2x_2 + 3x_3 + 4x_4 = 9$. The LHS of this equation can be odd only if $x_3 > 0$. Hence, each line $\overline{L} \in \overline{\Sigma}$ contains at least one point from P_3. But since each point in P_3 is incident with $5 - 3 = 2$ lines in $\overline{\Sigma}$, the points in P_3 can be incident with at most $2\tau_3$ lines in $\overline{\Sigma}$. Therefore, as P_3 meets every line in $\overline{\Sigma}$, we must have $2\tau_3 \geq |\overline{\Sigma}| = 21 - 9 = 12$, from which we obtain $\tau_3 \geq 6$. So, the only possible solution to (8)–(10) is $(\tau_2, \tau_3, \tau_4, \tau_5) = (9, 9, 0, 0)$.

Thus, Σ contains $9 + 9 = 18$ points in all, leaving 3 points outside Σ. Let P be the set of 3 points outside Σ. Since $\Sigma \subset \overline{\Sigma}_P$, we have $|\overline{\Sigma}_P| \geq 9$. On the other hand, from the inclusion-exclusion principle, we can infer that $|\overline{\Sigma}_P| \leq 9$, with equality only if the 3 points in P are not collinear. Thus, we are forced to conclude that $\Sigma = \overline{\Sigma}_P$, and the points in P are not collinear. ■

It follows from Lemmas 20 and 21 that $e_8(\text{PG}(2,4)) + e_9(\text{PG}(2,4)) = \binom{21}{3}$, since this is the number of ways of choosing 3 points out of the 21 in PG(2, 4). Thus, $e_9(\text{PG}(2,4)) = \binom{21}{3} - 210 = 1120$.

We did not consider it worthwhile to analytically determine the remaining coefficients $e_i(\text{PG}(2,4))$, $10 \leq i \leq 17$. We used a computer search to determine these coefficients, thus completing the SSWE for PG(2, 4):

$$\begin{aligned} E_{PG(2,4)}(z) &= 1 + 168z^6 + 210z^8 + 1120z^9 + 4788z^{10} + 8568z^{11} + 29330z^{12} + 52920z^{13} \\ &\quad + 60840z^{14} + 41664z^{15} + 18669z^{16} + 5880z^{17} + 1330z^{18} + 210z^{19} + 21z^{20} + z^{21} \end{aligned}$$

References

[1] Y. Kou, S. Lin and M.P.C. Fossorier, "Low-Density Parity Check Codes Based on Finite Geometries: A Rediscovery and New Results," *IEEE Trans. Inform. Theory*, vol. 47, no. 7, Nov. 2001, pp. 2711–2735.

[2] C. Di, D. Proietti, I.E. Telatar, T.J. Richardson and R.L. Urbanke, "Finite-Length Analysis of Low-Density Parity-Check Codes on the Binary Erasure Channel," *IEEE Trans. Inform. Theory*, vol. 48, no. 6, June 2000, pp. 1570–1579.

[3] J.H. van Lint and R.M. Wilson, *A Course in Combinatorics*, 2nd ed., Cambridge University Press, 2001.

[4] C.J. Colbourn and A. Rosa, *Triple Systems*, Oxford University Press, 1999.

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

[6] W. Cherowitzo, "Hyperovals in Desarguesian Planes: An Electronic Update", available online at `http://www-math.cudenver.edu/∼wcherowi/research/hyperoval/hyintro.htm`.

[7] J.W.P. Hirschfeld, *Projective Geometries over Finite Fields*, 2nd ed., Oxford University Press, 1998.