Partial Partitions of Vector Spaces Arising from the Construction of Byte Error Control Codes

W. Edwin Clark
Department of Mathematics
University of South Florida
Tampa, Florida
U.S.A. 33620-5700

Larry A. Dunning[1] Department of Computer Science
Bowling Green State University
Bowling Green, Ohio
U.S.A. 43403-0214

Abstract. We investigate collections $H = \{H_1, H_2, \ldots, H_n\}$ of pairwise disjoint w-subsets H_i of an r-dimensional vector space V over $GF(q)$ that arise in the construction of byte error control codes. The main problem is to maximize m for fixed w, r, and q when H is required to satisfy a subset of the following properties: (i) each H_i is linearly independent; (ii) $H_i \cap \langle H_j \rangle = \phi$ if $i \neq j$; (iii) $\langle H_i \rangle \cap \langle H_j \rangle = \{0\}$ if $i \neq j$; (iv) any two elements of $H_1 \cup H_2 \cup \cdots \cup H_m$ are linearly independent; (v) any three elements of $H_1 \cup H_2 \cup \cdots \cup H_m$ are linearly independent. Here $\langle x \rangle$ denotes the subspace of V spanned by X. Solutions to these problems yield linear block codes which are useful in controlling various combinations of byte and single bit errors in computer memories. For $r = w + 1$ and for small values of w the problem is solved or nearly solved. We list a variety of methods for constructing such partial partitions and give several bounds on m.

1. Introduction

In recent years a number of researchers have investigated the structure of error-correcting codes for byte organized computer memories. We mention for example the papers [4], [15], [24]. Problems analogous to those we raise here have been studied in the theory of matroids and in the theory of finite geometries; some connections to those topics will be discussed below.

We will be concerned with collections

$$H = \{H_1, H_2, \ldots, H_m\} \tag{1}$$

of pairwise disjoint w-subsets H_i of an r-dimensional vector space V over a finite field $F = GF(q)$. H will be called a *partial w-partition of V of length m.* With a few exceptions F will be $GF(2)$. The partitions of concern to us will be required to satisfy one or more of the following properties:

(i) Each H_i is linearly independent.

[1] Dr Dunning's work was supported, in part, by the Center for Microelectronics Research, College of Engineering, University of South Florida, Tampa, Florida, 33620.

(ii) $H_i \cap \langle H_j \rangle = \phi$ if $i \neq j$.
(iii) $\langle H_i \rangle \cap \langle H_j \rangle = \{0\}$ if $i \neq j$.
(iv) Any two elements of $H_1 \cup H_2 \cup \cdots \cup H_m$ are linearly independent.
(v) Any three elements of $H_1 \cup H_2 \cup \cdots \cup H_m$ are linearly independent.

Here $\langle X \rangle$ denotes the subspace of V spanned by X.

Let Ω be a subset of the four properties listed above. We always assume that Ω contains property (i). The principal question we discuss is the following:

A. For fixed r and w what is the largest partial partition (1) satisfying the conjunction of the properties in Ω? We call such a partial partition *optimal* with respect to Ω and we call this the *optimality problem* for Ω.

In a few cases we consider problems of the following type:

B. Given a particular subset S of V find the largest partial partition (1) satisfying the properties in Ω such that every component H_i of H is contained in the set S.

In Section 2 we discuss the relationship between various types of partial partitions and byte error control codes which motivate them.

In Section 3 we discuss the optimality problem for partial partitions which satisfy conditions (i) and (iii). Partial partitions satisfying these two properties are called *partial w-spreads.* As pointed out to us by Jack Hayden, in the special case $r = 2w$, such partial partitions have been extensively investigated in the theory of translation planes [20]. Investigation of the general case, $r > w$ and r not divisible by w, was apparently initiated independently by Hong and Patel [15] for the binary case only and by Beutelspacher [1] for arbitrary finite field size q. Both of these papers obtained the same lower bound for the size of optimal partial w-spreads. The best known upperbounds are due to Drake and Freeman [10]. We state these bounds in Section 3. Additional results are obtained concerning the optimality of partial spreads satisfying condition (v).

Section 4 is devoted to the optimality problem for partial partitions satisfying conditions (i) and (ii). We call such partial partitions *quilts*. In this section we consider only the case $F = GF(2)$. We present a number of methods for constructing quilts that have appeared in the literature. The known construction methods for quilts are facilitated by the study of quilts that satisfy property (v) and quilts that have the property that all vectors in each H_i have odd (Hamming) weight. We study both of these types of quilts. For $r = w + 1$ or $w = 2$ the optimality problem is completely solved for all three types of quilts. For $w = 3$ and 4 we come very close to a complete solution using some new bounds that we establish for quilt sizes. However, the general optimality problem for quilts remains open.

In Section 5 we solve completely the optimality problem for partial partitions satisfying condition (i) only and solve problem B above in case S is the set of columns of the parity check matrix for a cyclic or extended cyclic code.

2. Connections with Byte Error Control Codes

We assume familiarity in this section with the basic ideas of linear error correcting/detecting codes [21]. An (n, k, d) code, or simply (n, k) code, over $F = GF(q)$ is a k-dimensional subspace C of F^n with minimum (Hamming) weight d. We are interested in the case where each codeword $\mathbf{x}$ in C is partitioned into m *bytes* with w *bits* per byte, i.e.,

$$\begin{aligned}\mathbf{x} &= (x_{1,1}, x_{1,2}, \ldots, x_{1,w}, x_{2,1}, \ldots, x_{2,w}, \ldots, x_{m,1}, \ldots, x_{m,w}) \\ &= (\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_m).\end{aligned}$$

An error pattern confined to t of the m bytes is called a t-byte error, whereas an error pattern involving t of the $n = mw$ bits x_{ij} is called a t-bit error. The code C is said to be

single error correcting (SEC), if it can be used to correct any 1-bit error;
double error detecting (DED), if it can detect any 2-bit error;
byte error correcting (BEC), if it can correct any 1-byte error;
byte error detecting (BED), if it can detect any 1-byte error.

Analogously we shall use *triple error detecting (TED)*, and *2-byte error detecting (2-BED)*.

The (n, k, d) code C may be described as the null space of a parity check matrix H which is an r by n matrix of rank r where $n = mw$ and $r = n - k$. Let H be partitioned in the form

$$H = [H_1 H_2 \ldots H_m] \qquad (2)$$

where each submatrix H_i is r by w. If the columns of H are distinct we may view (2) as a partial w-partition of the vector space F^r of all column vectors of length r.

Table I below gives the relationship between the various subsets of the properties (i)–(v) and the error control abilities of a code with parity check matrix (2). Since we shall always assume condition (i) and because of obvious implications between the conditions we have only seven distinct cases. Table I also gives the *minimum distance profile* as defined in [23] and [25]. This is an analogue of the minimum distance for codes providing byte as well as bit error protection.

	Partial Partition Properties	Error Control Properties	Min. Distance Profile	References
1.	(i)	BED	(2,1)	
2.	(i), (ii)	SEC-BED	(3.2)	**[4, 11, 12]**
3.	(i), (iii)	BED	(3,2,1)	**[15]**
4.	(i), (iv)	DED-BED	(3,1)	
5.	(i), (v)	TED-BED	(4,1)	
6.	(i), (ii), (v)	SEC-DED-BED	(4,2)	**[7,13,14,17,18,24]**
7.	(i), (iii), (v)	(2-BED)-TED	(4,2,1)	

Table 1

In each instance save one the partial partition properties listed in Table 1 are necessary and sufficient for the code defined by the parity check matrix (2) to be able to perform all of the error control properties listed. The exception is line 1 where for BED codes the H_i need not be disjoint. These equivalences are quite easy to verify and are well-known.

3. Partial Spreads

In this section we discuss partial w-partitions H satising the two properties:

(i) Each H_i is linearly independent.

(iii) $\langle H_i \rangle \cap \langle H_j \rangle = \{0\}$ if $i \neq j$.

Let $W_i = \langle H_i \rangle$. In this way we obtain m w-dimensional subspaces

$$W_1, W_2, \ldots, W_m \text{ satisfying } W_i \cap W_j = \{0\} \text{ if } i \neq j. \tag{3}$$

Such a collection of subspaces of V will be said to be a *partial w-spread in V with components W_i*. If also

$$W_1 \cup W_2 \cup \cdots \cup W_m = V$$

then (3) is called a *w-spread* or a *full w-spread*, for emphasis. It is clear that if we have a partial w-spread (3) and we chose a basis H_i for W_i for each i, then (i) and (iii) will hold.

The term *spread* was coined by Bruck and Bose [5]. If the dimension of V is $2w$ such a w-spread determines a translation plane and conversely. The case $\dim(V) = 2w$ has been studied extensively (see, e.g., [20]). With regard to the case $r > 2w$ see [[1],[3],[10],[15]].

We say that a partial w-spread in V is *maximal* if it cannot be extended to a larger partial w-spread and is optimal if no larger partial w-spread exists. Let V be r-dimensional over $F = GF(q)$. Since V contains $q^r - 1$ non-zero elements and each W_i contains $q^w - 1$ non-zero elements it is clear that a partial w-spread in V has at most

$$f(r, w, q) = \left[\frac{q^r - 1}{q^w - 1}\right]$$

components where $[.]$ denotes the greatest integer function. It is convenient to note that

$$f(r, w, q) = \frac{q^r - q^c}{q^w - 1} = \sum_{i=0}^{a-1} q^{iw+c} \text{ if } r = aw + c, 0 \leq c < w \tag{4}$$

We now present a class of partial w-spreads which have size

$$m = L(r, w, q) = f(r, w, q) - (q^c - 1) \tag{5}$$

The Hong-Patel Partial w-Spreads. The spreads defined here for $F = GF(q)$ are a straightforward generalization of those defined for $GF(2)$ by Hong and Patel in [15]. Partial spreads with the same parameters for prime fields may also be constructed by recursively applying Lemma 2 of Linstrom [19] and reducing the dimension of the last subspace produced by that construction.

Let $r = aw + c, 0 \leq c < w$. We assume $a \geq 2$, otherwise there is no non-trivial spread. The Hong-Patel partial w-spread is the union

$$H = H^1 \cup H^2 \cup \cdots \cup H^{a-1} \cup H^a \tag{6}$$

of a partial w-spreads H^t. We define H^t, $1 \leq t \leq a-1$, as follows. Write each vector in F^r in the form (x, y, z), x in $F^{(a-t-1)w}$, y in F^w, and z in F^{tw+c}. If $t = a-1$, this reduces to (y, z). Identify F^{tw+c} with $K = GF(q^{tw+c})$ and let α be a primitive element of K. Let $m(t) = q^{tw+c}$. Since $w \leq tw + c$ the sets

$$\{\alpha^i, \alpha^{i+1}, \ldots, \alpha^{i+w-1}\}, \quad 1 \leq i \leq m(t) - 1,$$

are linearly independent. Let

$$H_0^t = \{(0, e_1, 0), (0, e_2, 0), \ldots, (0, e_w, 0)\}$$

where $e_1, e_2, \ldots, e_w$ is the standard basis for F^w. For $1 \leq i \leq m(t) - 1$ set

$$H_i^t = \{(0, e_1, \alpha^i), (0, e_2, \alpha^{i+1}), \ldots, (0, e_w, \alpha^{i+w-1})\}.$$

These $m(t)$ sets form a w-spread H^t. Finally, we define H^a to be the w-partial spread with just one subset

$$H_1^a = \{(0, e_1, 0), (0, e_2, 0), \ldots, (0, e_w, 0)\},$$

where *in this case* (x, y, z) indicates x in $F^{(a-1)w}$, y in F^w, z in F^c. Now one easily verifies that the union (6) of these a partial w-spreads is a partial w-spread with

$$m = m(1) + m(2) + \cdots + m(a-1) + 1 = L(r, w, q)$$

components. It is easy to check that these spreads are maximal. It is an open question whether or not they are optimal.

Hong and Patel showed that in the binary case the above partial spreads are optimal if $r \equiv 0$ or $1 \pmod{w}$. Beutelspacher [1] independently showed the existence of partial w-spreads with these same parameters and proved that they are in fact optimal for any q when $r \equiv 0$ or $1 \pmod{w}$. It follows that an optimal partial w-spread in an r-dimensional vector space over $GF(q)$ has size m satisfying:

$$L(r, w, q) \leq m \tag{7}$$

Furthermore if $r \equiv 0$ or 1 (mod w) then we have equality.

Let θ be defined by

$$2\theta = \sqrt{1 + 4q^w(q^w - q^c)} - (2q^w - 2q^c + 1),$$

where c is as in (4); and set

$$U(r,w,q) = f(r,w,q) - ([\theta] + 1).$$

Drake and Freeman [10] showed that this is an upper bound for optimal partial w-spreads. We summarize these results in the following theorem.

Theorem 1. (Hong, Patel, Beutelspacher, Drake, Freeman). *If H is an optimal partial w-spread of size m, then*

$$L(r,w,q) \leq m \leq U(r,w,q),$$

and equality holds if $r \equiv 0$ or $1 \pmod{w}$.

Hong and Patel conjectured that their spreads are optimal in the binary case. However, the upperbound in the above theorem is not trivial. The smallest case of this conjecture that is unresolved is the case $q = 2$, $w = 3$ and $r = 8$. Hours of computer search have failed to reveal a counter-example even in this case. The Hong-Patel partial spread with these parameters has length $m = 33$. From Theorem 1 we deduce that the optimal size in this case is at most 34.

Remarks on Maximal Partial Spreads.

It is easy to see that the Hong-Patel partial spreads are maximal. For the case $r = 2w$, Mesner [22] notes the existence of maximal partial spreads that are not full spreads. In the case $r = 2w$, full spreads always exist and correspond to translation planes. Some additional results on this topic may be found in Bruen's article in [6].

Partial Spreads Satisfying Condition (v).

Here we consider only the case $F = GF(2)$. Let

$$H = \{H_1, H_2, \ldots, H_m\} \tag{8}$$

be a partial w-spread and let $S = H_1 \cup H_2 \cup \cdots \cup H_m$. We are interested in finding the largest spread (8) subject to condition (v): every set of three vectors in S is linearly independent. We call such a spread a four spread, since it corresponds to a linear code with minimum distance $d \geq 4$. One way to guarantee this is to choose the spread so that all vectors in S have odd Hamming weight. Let us call such a spread an *odd spread*. Let W_i be the space spanned by H_i. If each H_i consists of odd (weight) vectors only then W_i contains 2^{w-1} odd vectors. Since there are 2^{r-1} odd vectors in F^r we must have

$$m \leq 2^{r-w} \tag{9}$$

This bound can be attained by using the spreads H^{a-1} described in the construction of the Hong-Patel spread. While the spread H^{a-1} need not be an odd spread if we apply the linear automorphism

$$(x_1, x_2, \ldots, x_r) \rightarrow (x_1 + x_{w+1} + x_{w+2} + \cdots + x_r, x_2, \ldots, x_r)$$

we obtain an odd spread. Thus we have

Theorem 2. *An optimal odd spread has size $m = 2^{r-w}$, whereas an optimal four spread has size $m \geq 2^{r-w}$.*

The next theorem will be used several times in what follows:

Theorem 3. (Clark, Dunning and Rogers [8]). *Let S be a set of vectors in $GF(2)^r$ such that every subset of three or less vectors in S is linearly independent. If either*

(i) $|S| > 5 \cdot 2^{r-4}$, *or*
(ii) $1 \leq r \leq 3$,

then, there is a linear automorphism of $GF(2)^r$ which carries S into the set of all odd weight vectors.

Theorem 4. *If $w = 2$ or 3, then optimal four spreads have size $m = 2^{r-w}$.*

Proof: If $w = 2$ or 3 and an optimal four spread has size $m > 2^{r-w}$, then the union of the components of the spread contains mw vectors and we have

$$mw > w2^{r-w} > 5 \cdot 2^{r-4}$$

But this implies by Theorem 3 that there is an odd spread of this size which contradicts Theorem 2.

This leaves open the question of existence for four spreads with $w \geq 4$ exceeding the bound (9).

4. Quilts

In this section we shall always assume that $F = GF(2)$.

A partial w-partition $H = \{H_1, H_2, \ldots, H_m\}$ in F^r will be called a *quilt* with parameters (w, r, m) when it satisfies the two properties:

(i) Each H_i is linearly independent;
(ii) $H_i \cap \langle H_j \rangle = \phi$ if $i \neq j$.

As with spreads we call m the *size* or *length* of H. Similarly, if $S = H_1 \cup \cdots \cup H_m$ consists entirely of odd (weight) vectors we call H an ***odd quilt*** and if every 3-subset of S is linearly independent we call H a *four quilt*. The existence of a quilt with parameters (w, r, m) is equivalent to the existence of a collection of w-dimensional subspaces $W_1, W_2, \ldots, W_m$ such that for each i there is a basis for W_i that does not intersect any other subspace in the collection. The following notation will be useful.

quilt (w, r, m)	$\Leftrightarrow$	there is a quilt with parameters (w, r, m)
fourquilt (w, r, m)	$\Leftrightarrow$	there is a four quilt with parameters (w, r, m)
oddquilt (w, r, m)	$\Leftrightarrow$	there is an odd quilt with parameters (w, r, m)
spread (w, r, m)	$\Leftrightarrow$	there is a partial spread with parameters (w, r, m)

4.1 Constructions

We now list several known methods for constructing new quilts from given quilts.

Let $H = \{H_1, H_2, \ldots, H_m\}$ be a given quilt with parameters (w, r, m).

The Doubling Construction (Chen [7]).

quilt $(w, r, m) \Rightarrow$ *quilt* $(w, r+1, 2m)$
fourquilt $(w, r, m) \Rightarrow$ *fourquilt* $(w, r+1, 2m)$
oddquilt $(w, r, m) \Rightarrow$ *oddquilt* $(w, r+1, 2m)$

The Widening Construction (Chen [7]).

quilt $(w, r, m) \Rightarrow$ *quilt* $(w+1, r+1, m)$
fourquilt $(w, r, m) \Rightarrow$ *fourquilt* $(w+1, r+1, m)$
oddquilt $(w, r, m) \Rightarrow$ *oddquilt* $(w+1, r+1, m)$

Odd Quilt → Quilt Construction (Dunning and Varanasi [13]).

oddquilt $(w, r, m) \Rightarrow$ *quilt* $(w, r+a, (2^{a+1}-1)m)$

We now record a few methods of constructing quilts from scratch.

Trivial Quilts.

$$quilt(1, r, m = 2^r - 1)$$
$$oddquilt(1, r, m = 2^{r-1})$$
$$fourquilt(1, r, m = 2^{r-1})$$

If $w = 1$, an optimal quilt of size m can be obtained by taking the $m = 2^r - 1$ singleton sets $\{v\}$ where v is any non-zero element of F^r. An optimal odd quilt of size $m = 2^{r-1}$ can be obtained by taking the $m = 2^{r-1}$ singleton sets $\{v\}$ where v is any odd (weight) vector of F^r; this is also optimal as a four quilt. If $r = w$, then the quilt $H = \{H_1\}$, with $m = 1$, where H_1 is the standard basis for F^r is optimal as a quilt, an odd quilt and as a four quilt.

By applying the above constructions to these trivial quilts many examples of quilts may be obtained, some of which are even optimal.

The Coset Construction (Bossen, Chang, Chen [4] and Reddy [24]).

$$quilt(w, r, m = 2^{r-w+1} - 1).$$
$$fourquilt(w, r, m = 2^{r-w+1} - 1), \; if w \geq 5.$$

We note that quilts with the same parameters may be obtained by use of the Odd Quilt → Quilt Construction given above. [This methods extends easily to the non-binary case $F = GF(q)$ to obtain a quilt with $m = (q^{r-w+1} - 1)/(q - 1)$.]

The Partial Steiner System Construction (Even w [9]).

$$oddquilt(w, r, m = A(n(r, 2w), 4, w)), \; for\, even\, w.$$

Here $n = n(r, d)$ is the maximum possible length of a binary linear code with redundancy r, minimum distance d and having codewords of even weight only, and $A(n, 4, w)$ is the maximum possible number of codewords in a binary code of length n, constant weight w and minimum distance 4.

The $r = m = w+2$ Odd Quilt Construction (Dunning [14], Kaneda [17][18]).

$$oddquilt(w, r = w + 2, m = w + 2)$$

The Spread Construction of Odd Quilts (A generalization of Chen [7]).

$$spread(w - 1, r - 1, m) \Rightarrow oddquilt(w, r, m)$$

Let $r > w \geq 3$ and let $H = \{H_1, H_2, \ldots, H_m\}$ be a partial $(w-1)$-spread in F^{r-1}. For each $i = 1, \ldots, m$ given that $H_i = \{v_1, v_2, \ldots, v_{w-1}\}$, set

$$H_i' = \{(v_1, 1), (v_2, 1), \ldots, (v_{w-1}, 1), (v_1 + v_2, 1)\}.$$

Using the fact that H is a spread, one easily sees that these sets form a quilt with parameters (w, r, m). Applying the linear automorphism

$$(x_1, x_2, \ldots, x_r) \rightarrow (x_1, \ldots, x_{r-1}, x_1 + x_2 + \cdots + x_r)$$

one obtains an odd quilt with the same parameters.

We record here a useful implication that follows directly from Theorem 3.

Four Quils *to* Odd Quilts.

$$fourquilt(w, r, m) \; and\, mw > 5 \cdot 2^{r-4} \Rightarrow oddquilt(w, r, m)$$

4.2 Upper Bounds

Theorem 5 *If a quilt H has parameters (w, r, m), we have the following upper bounds on m.*

$$wm \le 2^r - 1, w \ge 2, \tag{10}$$

$$wm \le 2^r - 1 - (3 \cdot 2^{w-1} - 2w - 1), w \ge 3, \tag{11}$$

$$(2^{w-1} - w)wm \le \binom{2^r - 1 - wm}{2}, w \ge 3. \tag{12}$$

If in addition H is an odd quilt (or a four quilt with $w \ge 3, r \ge w + 2$), we have the following:

$$wm \le 2^{r-1}, w \ge 2 \tag{13}$$

$$wm \le 2^{r-1} - (2^{w-1} - w + 1), \text{ if } w = 4, \tag{14}$$

$$wm \le 2^{r-1} - (2^{w-1} - w + 2^{w-2} - w), \text{ if } w > 4, \tag{15}$$

$$wm \le (2^{r-1} - 1)\left(\frac{2^{r-1}}{2^{r-1} + 2^{w-1} - w - 1}\right), w \ge 3. \tag{16}$$

Proof: We let $S = H_1 \cup H_2 \cup \cdots \cup H_m$ and let W_i denote the subspace of F^r generated by H_i. (10) is clear since $mw = |S|$ and F^r contains exactly $2^r - 1$ non-zero vectors. Let X denote the set of all non-zero vectors in F^r that are not in S. Let W^* denote the set of non-zero vectors in any set W of vectors.

Proof of (11): Since $H_i \cap W_j = \phi$ if $i \ne j$ the vectors

$$Y = (W_1^* \backslash H_1) \cup (W_2^* \backslash H_2) \cup \cdots \cup (W_m^* \backslash H_m)$$

are contained in X. It follows that $mw \le 2^r - 1 - |Y|$. A lower bound on Y is obtained by using the first two terms only and observing that

$$(W_1^* \backslash H_1) \cap (W_2^* \backslash H_2) = (W_1^*) \cap (W_2^*)$$

which has at most $2^{w-1} - 1$ elements:

$$|Y| \ge (2^w - w - 1) + (2^w - w - 1) - (2^{w-1} - 1),$$

and (11) follows.

Proof of (12): Note that if $w \ge 3$ and $H_i = \{v_1, v_2, \ldots, v_w\}$, then v_i is a sum of $2^{w-1} - w$ two element subsets $\{s_1, s_2\}$ where each s_i lies in $(W_1^* \backslash H_1)$, namely, $v_i = s_1 + s_2$ if $s_1 = \sum_{j \in I} v_j$ and $s_2 = \sum_{j \in I} v_j + v_i$, where I is any subset of $\{1, 2, \ldots, w\} \backslash \{i\}$ with $|I| > 1$. Thus, each element of S is a sum of at least

$2^{w-1} - w$ pairs of elements from X. Since $|X| = 2^r - 1 - mw$ elements (12) follows.

Proof of (13)–(16) for four quilts: One easily checks that if $w \geq 3$ and $r \geq w + 2$, then the bounds (13)–(16) are each greater than $5 \cdot 2^{r-4}$ and it follows from Theorem 3 that it suffices to establish these bounds for odd quilts.

Proof of (13) for odd quilts: This is obvious since there are in F^r exactly 2^{r-1} odd vectors.

Proof of (14) for odd quilts: In the notation above, W_i contains 2^{w-1} odd vectors. If $w \geq 4$ then W_i is generated by the odd vectors in $W_i \backslash H_i$ since given four odd vectors $\mathbf{h}_i$, $1 \leq i \leq 4$, in H_i we may write any one of them, say, $\mathbf{h}_1$ as the sum of the three odd vectors $\mathbf{h}_1 + \mathbf{h}_2 + \mathbf{h}_3, \mathbf{h}_1 + \mathbf{h}_2 + \mathbf{h}_4, \mathbf{h}_1 + \mathbf{h}_3 + \mathbf{h}_4$ which are not in H_i. It follows that at least one odd vector in $W_2 \backslash H_2$ is not contained in W_1. This shows that there are at least $2^{w-1} - w + 1$ odd vectors that are not in S and (14) follows.

Proof of (15) for odd quilts: Continuing the argument in (14) let Y denote set of odd vectors in

$$(W_1 \backslash H_1) \cup (W_2 \backslash H_2) \cup \cdots \cup (W_m \backslash H_m)$$

Note that these vectors are not in S. A lower bound on Y is obtained by using the first two terms only and observing that

$$(W_1 \backslash H_1) \cap (W_2 \backslash H_2) = (W_1) \cap (W_2)$$

which has at most 2^{w-2} odd vectors. Since each $W_i \backslash H_i$ has $2^{w-1} - w$ odd vectors we obtain:

$$|Y| \geq (2^{w-1} - w) + (2^{w-1} - w) - 2^{w-2}$$

and (15) follows.

Proof of (16) for odd quilts: As in the proof of (12) each $\mathbf{v}$ in H_i can be written as a sum of $2^{w-1} - w$ pairs in X. Since each such $\mathbf{v}$ is odd, one vector in each pair is even and one is odd. Now in X there are $2^{r-1} - 1$ even vectors and $2^{r-1} - wm$ odd vectors. Hence there are $(2^{r-1} - 1)(2^{r-1} - wm)$ pairs $(\mathbf{s}_1, \mathbf{s}_2)$ with $\mathbf{s}_1$ even and $\mathbf{s}_2$ odd. It follows that $(mw)(2^{w-1} - w) \leq (2^{r-1} - 1)(2^{r-1} - wm)$ which is equivalent to (16).

4.3 Optimal and Near Optimal Quilts

Theorem 6. *If a quilt H has parameters $(w, r = w + 1, m)$ with $w \geq 2$, then*

a) $m = 3$ *if H is an optimal quilt;*
b) $m = 3$ *if H is an optimal four quilt with $w \geq 5$;*
c) $m = 2$ *if H is an optimal four quilt with $w = 2, 3$, or 4; and*
d) $m = 2$ *if H is an optimal odd quilt.*

Proof of (a) and (b): Parts (a) and (b) were established in [[12],[24]]. However the proof we give here is conceptually simpler. Suppose H is a quilt with parameters $(w, r = w+1, m = 4)$. Let W_i be the subspace generated by H_i. Then each W_i is a hyperspace in $V = F^{w+1}$. It follows that the intersection $S = W_1 \cap W_2$ has dimension $w - 1$. Let $\mathbf{u} \in H_1$ and $\mathbf{v} \in H_2$. Then by definition of quilt $\mathbf{u} \notin S$ and $\mathbf{v} \notin W_1$. It follows that

$$W_1 = S \cup (S + \mathbf{u}), W_2 = S \cup (S + \mathbf{v}) \text{ and } V = W_1 \cup (W_1 + \mathbf{v})$$

and hence

$$V = S \cup (S + \mathbf{u}) \cup (S + \mathbf{v}) \cup (S + \mathbf{u} + \mathbf{v}).$$

Now since H_3 does not intersect $W_1 \cup W_2$, we must have H_3 contained in $S + \mathbf{u} + \mathbf{v}$, and it follows by comparison of dimensions that $W_3 = S \cup (S + \mathbf{u} + \mathbf{v})$. It follows that $V = W_1 \cup W_2 \cup W_3$. This leaves no room for H_4 which is disjoint from $W_1 \cup W_2 \cup W_3$. Since the Coset Method gives quilts with $m = 3$ and when $w \geq 5$ its improvement due to Reddy gives four quilts with $m = 3$, we have established (a) and (b).

Proof of (d): The Doubling Construction applied to the odd quilt with $w = r$ and $m = 1$ and H_1 consisting of the standard basis for F^r gives an odd quilt with parameters $w, r = w + 1$, and $m = 2$. So to establish d) it suffices to show that there is no odd quilt with parameters $(w, r = w + 1, m = 3)$. Let H be such a quilt. Continuing the above argument we have since H_3 does not intersect S that H_3 is contained in $S + \mathbf{u} + \mathbf{v}$. Since the sum of two odd vectors is odd, if all vectors in S are even (weight) then $S + \mathbf{u} + \mathbf{v}$ contains only even-vectors, but this cannot be since H_3 contains only odd vectors. Hence S contains a $w - 2$ dimensional subspace U of even vectors and an odd vector $\mathbf{x}$ such that $S = U \cup (U + \mathbf{x})$. It follows that

$$W_1 = U \cup (U + \mathbf{x}) \cup (U + \mathbf{u}) \cup (U + \mathbf{x} + \mathbf{u}).$$

Now, H_1 does not intersect S and $U + \mathbf{x} + \mathbf{u}$ contains no odd vectors so H_1 is contained in $U + \mathbf{u}$. It follows that H_1 and hence W_1 is contained in $U \cup (U + \mathbf{u})$, which is a $w - 1$ dimensional subspace. This contradiction completes the proof of (d).

Proof of (c): For $w = 3$ or 4, a four quilt with $r = w + 1$, $m = 3$ satisfies $mw > 5 \cdot 2^{r-4}$, implying by Theorem 3 the existence of odd quilts with these parameters. This cannot be by (d) which we have just proved. For $w = 2$ and $r = 3$ by Theorem 3 again every four quilt is an odd quilt so we must have $m \leq 2$ by (d). This completes the proof of (c) and the theorem.

Theorem 7 (Dunning and Varanasi [11]). *If $w = 2$ an optimal quilt has size $m = 2^{r-1} - 1$ and an optimal odd quilt or four quilt has $m = 2^{r-2}$.*

Proof: The coset construction gives quilts with $m = 2^{r-1} - 1$ when $w = 2$. This is best possible since the bound (10) gives $m \leq [\frac{2^r-1}{2}] = 2^{r-1} - 1$.

In the case of odd quilts we have by (13) that $m \leq 2^{r-2}$. So it suffices to show that an odd quilt exists that attains this bound. To do this let **e** be any non-zero even vector. Say that the odd vectors **u** and **v** are equivalent if their sum is **e**. The reflexive closure of this relation is an equivalence relation on the 2^{r-1} odd vectors with 2^{r-2} two element equivalence classes. These equivalence classes form the desired odd quilt.

For $w = 2$, if a four quilt satisfies $m > 2^{r-2}$, then $wm > 5 \cdot 2^{r-4}$. It follows from Theorem 3, that there is an odd quilt with these parameters, which contradicts the previous paragraph. This completes the proof.

Theorem 8 (Chen [7]). *If $w = 3$, an optimal four quilt or odd quilt has size*

$$m = \left[\frac{2^{r-1}}{3}\right]. \tag{17}$$

Proof: If $r = 4$, the result follows from Theorem 6 (c) and (d). So we let $r \geq 5$. First we consider the case when r is odd and $r-1$ is even. Then by Theorem 1 there is a spread with $w = 2$ and m given by (17). Thus, by the Spread Construction of Odd Quilts described above there is an odd quilt with $w = 3$ and m given by (17). By applying the Doubling Construction we obtain from these odd quilts, odd quilts with parameters ($w' = 3, r' = r + 1, m' = 2m$). One may verify that these parameters also satisfy (17) if all parameters are primed. By (13) these quilts are optimal. This completes the odd quilt case.

To complete the proof one checks that $3m > 5 \cdot 2^{r-4}$ for $r \geq 4$, so by Theorem 3 optimal four quilts are optimal odd quilts. The case $r = 3 = w$ is trivial.

Only partial results have been obtained for optimal quilts when $w = 3$:

Theorem 9. *For $w = 3$ optimal quilts for $r = 3, 4$ and 5 have sizes $m = 2^{r-2} - 1$.*

Proof: The coset construction when $w = 3$ yields quilts with $m = 2^{r-2} - 1$. The optimality of these bounds follows for $r = 4$ from Theorem 6 (a) and for $r = 5$ from the upper bound (12).

The inequalities (10) and (12) may be solved and in the case $w = 3$ yield the bound

$$m \leq \frac{1}{3}\left(2^r - \frac{1}{2} - \sqrt{2^{r+1} - \frac{7}{4}}\right) \approx \frac{1}{3}\left(2^r - \sqrt{2} \cdot 2^{r/2}\right) \tag{18}$$

which compares favorably with $w = 3$ quilts which may be obtained by applying the "Odd Quilt $\rightarrow$ Quilt Construction" to the optimal odd quilts of Theorem 8. For example if $r \equiv 0 \pmod 4$ there are optimal $w = 3$ odd quilts with parameters $(w' = 3, r' = r/2 + 1, m' = \frac{1}{3}(2^{r/2} - 1)$. Applying this construction with $a = r/2 - 1$ we obtain a quilt with parameters $(w = 3, r, m)$ where

$$m = \frac{1}{3}(2^{r/2} - 1)(2^{r/2} - 1) = \frac{1}{3}(2^r - 2 \cdot 2^{r/2} + 1). \quad (19)$$

The difference between (18) and (19) is $O(2^{r/2})$. For example, when $r = 8$, we get a bound $m \leq 77$, and a quilt with $m = 75$. Similarly near optimal quilts are obtained when $r \equiv 1, 2$, or $3 \pmod 4$.

Theorem 10. *For $w = 4$, optimal odd quilts and four quilts for $r = 6$ have $m = 6$, and for $r = 7$ the optimal size is $m = 14$.*

Proof: The existence of an odd quilt with $w = 4$, $r = m = 6$ comes from the "$r = m = w+2$ Construction" described above. These are optimal by (14). These are also optimal four quilts by Theorem 3. An optimal $(4, 7, 14)$ odd quilt was given in [13] and shown in [9] to follow from the Steiner System Construction. By (14) it is optimal as an odd quilt and by Theorem 3 it is optimal as a four quilt.

Kaneda's Odd Quilts for $w = 4$ [[17],[18]]. *Let $r = 2t$ and for each pair $\{\mathbf{x}, \mathbf{y}\}$ of odd weight vectors in F^t form the set*

$$H_{\mathbf{x},\mathbf{y}} = \{(\mathbf{x}, \mathbf{x} + \mathbf{y}), (\mathbf{y}, \mathbf{x} + \mathbf{y}), (\mathbf{x} + \mathbf{y}, \mathbf{x}), (\mathbf{x} + \mathbf{y}, \mathbf{y})\}$$

in F^r. Since there are 2^{t-1} odd weight vectors in F^t there are

$$m = \binom{2^{t-1}}{2} = 2^{r-3} - 2^{(r-4)/2} \quad (20)$$

such sets, which form an odd quilt.

In [9] a generalization to larger w of this construction is obtained using partial Steiner systems; however, except for a few isolated examples at $r = 7$ and 12 (see [9]), the Kaneda quilts are the longest known odd quilts with $w = 4$.

Now, solving (10) and (12) when $w = 4$ yields the upper bound for quilts

$$m \leq 2^{r-2} + \frac{5}{8} - \sqrt{2^{r-1} + \frac{17}{64}} \approx 8 \cdot 2^{r-5} - (2^{-(1/2)}) \cdot 2^{r/2}. \quad (21)$$

Applying the "Odd Quilt $\rightarrow$ Quilt" construction to the Kaneda odd quilts with $a = 2$ we obtain quilts with parameters $(w = 4, r, m)$ where

$$m = (2^3 - 1)(2^{r-5} - 2^{(r-6)/2}) = 7 \cdot 2^{r-5} - (7/8)2^{r/2}. \quad (22)$$

Using $a = (2t-2)/3$ with $t \equiv 1 \pmod 3$ instead of $a = 2$, one may obtain quilts within $O(2^{2r/3})$ of the bound (21).

Aside from the trivial cases $r = w$, the cases $r = w + 1$ covered by Theorem 6, and the above cases for $w = 2, 3$ and 4 we know of no additional proven examples of optimal quilts, odd quilts or four quilts.

5. BED Partitions

A partial w-partition $H = \{H_1, H_2, \ldots, H_m\}$ satisfying only the condition that the sets H_i are linearly independent will be called a *bed partition* since the corresponding codes as described in Section 2 are byte error detecting (BED). We note that in the binary case condition (iv) is automatically true.

We observe that an optimal bed partition is not an optimal BED code since if we simply take in (2) each H_i to be the w by w identity matrix we obtain a BED code of arbitrary length. However, a somewhat less trivial question is: Given a parity check matrix H for an arbitrary linear code, may it be partitioned as in (2) so that the columns of the submatrices are linearly independent, thus possibly introducing the additional property of BED on top of other error control properties the code might have already? In case the entire matrix cannot be so partitioned, what is the least number of columns that one need delete to obtain such a partition? We establish below that at least in the case that H is the parity check matrix of a cyclic or extended cyclic code of length n, such partial w-partitions always exist with $m = [n/w]$. We note also that there exists a matroid partitioning algorithm ([27],ch. 19) which can be used to, in polynomial time, find an optimal bed partition of a given set of vectors.

Theorem 10. *An optimal bed partition with parameters* (w, r, m), $r \geq w$, *over* $F = GF(q)$ *satisfies*

$$m = \left[\frac{q^r - 1}{w}\right]. \tag{23}$$

Proof: Clearly an optimal bed partition cannot have size greater than that given by (23). We may take $F^r = K = GF(q^r)$. If α is a primitive element of K, since $w \leq r$, the set $H_0 = \{\alpha^1, \alpha^{i+1}, \ldots, \alpha^{w-1}\}$ is linearly independent. Since multiplication by α^i is a non-singular linear map the sets $H_i = \{\alpha^0, \alpha^1, \ldots, \alpha^{i+w-1}\}$ are also linearly independent. It follows that the sets $H_0, H_w, H_{2w}, \ldots, H_{(m-1)w}$ form the desired bed partition in F^r.

Theorem 11. *Let S be the set of columns of the parity check matrix H of a cyclic or extended cyclic (n, k) code over $F = GF(q)$. If $w \leq r = n - k$, then there is a bed partition contained in S with parameters $(w, r, m = [n/w])$.*

Proof: Since the dual $C^\perp$ of a cyclic code C is a cyclic code we may take H to be the generator matrix of a cyclic code with generator polynomial

$$h(x) = h_0 + h_1 x + \cdots + h_r x^r,\ h_0 h_r \neq 0.$$

Then H has the form:

$$H = \begin{pmatrix} h(x) \\ xh(x) \\ x^2 h(x) \\ \vdots \\ x^{r-1} h(x) \end{pmatrix}.$$

It follows that the first r, *a fortiori* the first w columns of H, are linearly independent. Since the code is cyclic any w consecutive columns of H are linearly independent. Thus, we may form a bed partition of the columns by taking for the sets $H_1, H_2, \ldots$, respectively, the first w columns, the second w columns,... This yields the desired bed partition.

The parity check matrix of the extended code can be obtained by first adding a column of 0's to the left of H to obtain the r by $n+1$ matrix H' and finally adding a row of 1's at the bottom of H' to obtain the $r+1$ by $n+1$ matrix H^*. By the reasoning in the previous paragraph we may partition the columns of H as before except we take for H_1, just the first $w-1$ consecutive columns of H. Thereafter we choose the columns in groups of w until there are less than w left. It becomes clear that we may obtain a bed partition $\{H_1^*, H_2^*, \ldots, H_m^*\}$ of the columns of H^* where H_1^* consists of the first w columns of H^*, H_2^*, of the second w columns of H^*, etc. It is easy to verify that this is a bed partition.

Acknowledgements

We are grateful to Gur Dial, Jack Hayden, Frederick Rickey, and Douglas Rogers for useful discussions on these matters. We are also indebted to Albrecht Beutelspacher, David Drake and Hansjoachim Groh for references on partial w-spreads.

References

1. Albrecht Beutelspacher, *Partial spreads in finite projective spaces and partial designs*, Mat. Z. **14S** (1975), 211–229.
2. Albrecht Beutelspacher, *Parallelismen in unendlichen projektiven raumen enlicher dimension*, Geometriae Dedicata 7 (1978), 499–506.
3. Albrecht Beutelspacher and Franco Eugeni, *On the type of partial t-spreads in finite projective spaces*, Discrete Math. **54** (1985), 241–257.
4. D.C. Bossen, L.C. Chang, and C. Chen, *Measurement and generation of error correcting codes for package failures*, IEEE Trans. Comput. **C-27** (1978), 201–204.
5. R.H. Bruck and R.C. Bose, *The construction of translation planes from projective spaces*, J. Alg. (1964), 85–102.
6. A.A. Bruen, *Blocking sets and translation nets*, in "Lecture notes in pure and applied mathematics: Finite Geometries", edited by N.L. Johnson, et al, Marcel Dekker, New York, 1983.
7. C.L. Chen, *Error correcting codes with byte error detection capability*, IEEE Trans. Comput. **C-32** (1983), 615–621.
8. W.E. Clark, L.A. Dunning and D.G. Rogers, *Binary set functions and parity check matrices*, Discrete Math. **80** (1990), 249–265.
9. W.E. Clark, L.A. Dunning and D.G. Rogers, *The construction of some byte error control codes using partial Steiner systems*, IEEE Trans. Information Th. **IT-35** (1989), 1305–1310.

10. David A. Drake and J.W. Freeman, *Partial t-spreads and group constructible* (s, r, m)*-Nets*, Journal of Geometry 13/2 (1979), 210–216.
11. L.A. Dunning and M.R. Varanasi, SEC-BED codes for short byte lengths, Research Report 82-1, Department of Computer Science, Bowling Green State University, (1982).
12. L.A. Dunning and M.R. Varanasi, *Code constructions for error control in byte organized memory systems*, IEEE Trans. Comput. **C-32** (1983), 535–542.
13. L.A. Dunning and M.R. Varanasi, *A rotational* $(14 \cdot 4, 49)$ *SEC-DED-S4ED code for byte organized fault tolerant memory applications*, Proc. 14th Inter. Conf. on Fault-Tolerant Computing (1984), 330–333.
14. L.A. Dunning, *SEC-BED-DED codes for error control in byte-organized memory systems*, IEEE Trans. Comput. **C-34** (1985), 557–562.
15. S.J. Hong and A.M. Patel, *A general class of maximal codes for computer applications*, IEEE Trans. Comput. **C-21** (1972), 1322–1331.
16. M.Y. Hsiao, *A class of optimal minimum odd-weight-column SEC-DED codes*, IBM J. Res. Devel. **14** (1970), 395–401.
17. S. Kaneda, *A class of odd-weight -column SEC-DED-SbED codes for memory systems applications*, IEEE Trans. Comput. **C-33** (1984), 737-739.
18. S. Kaneda, *A class of odd-weight -column SEC-DED-SbED codes for memory systems applications*, Proc. 14th Int. Conf. Fault-Tolerant Comput. (1984), 88–93.
19. B. Linstrom, *Group partitions and mixed prefect codes*, Canad. Math. Bull. 18/1 (1975), 57–60.
20. H. Luneburg, "Translation Planes", Springer-Verlag, New York, 1980.
21. F.J. MacWilliams and N.J.A. Sloane, "The Theory of Error-Correcting Codes", Amsterdam, North-Holland, 1977.
22. D.M. Mesner, *Sets of disjoint lines in* $PG(3, q)$, Canadian J. Math. **19** (1967), 273–280.
23. P. Piret, *Binary codes for compound channels*, IEEE Trans. Inform. Theory **IT-31** (1985), 436–440.
24. A class of linear codes for error control in byte-per-card organized digital systems, IEEE Trans. Comput. **C-27** (1978), 455–459.
25. W.J. van Gils and J.P. Boly, *On combined symbol-and-bit error-control* $[4, 2]$ *codes over* $\{0, 1\}8$ *to be used in the* $(4, 2)$ *concept fault-tolerant computer*, IEEE Trans. Info. Theory, **IT-33** (1987), 911–917.
26. T. Verhoeff, *An updated table of minimum-distance bounds for binary linear codes*, IEEE Trans. Inform. Theory **IT-33** (1987), 665–680.
27. D.J.A. Welsh, "Matroid Theory", Academic Press, New York, 1976.