Partial permutation decoding for simplex codes

W. Fish, J.D. Key and E. Mwambene*
Department of Mathematics and Applied Mathematics
University of the Western Cape
7535 Bellville, South Africa

November 10, 2012

Abstract

We show how to find s-PD-sets of size $s+1$ that satisfy the Gordon-Schönheim bound for partial permutation decoding for the binary simplex codes $\mathcal{S}_n(\mathbb{F}_2)$ for all $n \geq 4$, and for all values of s up to $\left\lfloor \frac{2^n-1}{n} \right\rfloor - 1$. The construction also applies to the q-ary simplex codes $\mathcal{S}_n(\mathbb{F}_q)$ for $q > 2$, and to s-antiblocking information systems of size $s+1$, for s up to $\left\lfloor \frac{(q^n-1)/(q-1)}{n} \right\rfloor - 1$ for all q.

Keywords: Hamming codes, simplex codes, permutation decoding, antiblocking decoding
Mathematics Subject Classifications (2010): 05B05, 94B05

1 Introduction

The binary simplex code $\mathcal{S}_n(\mathbb{F}_2)$ is the dual of the binary Hamming code $\mathcal{H}_n(\mathbb{F}_2)$, and is a $[2^n-1, n, 2^{n-1}]_2$ linear code with all non-zero vectors having weight 2^{n-1}: see, for example, [1, Section 2.5]. Any generator matrix for $\mathcal{S}_n(\mathbb{F}_2)$ has for columns the 2^n-1 non-zero vectors in the vector space $V_n(\mathbb{F}_2) = \mathbb{F}_2^n$, and each coordinate position is labelled by the row vector of the corresponding column. The standard basis for $V_n(\mathbb{F}_2)$, i.e. $e_1, \ldots, e_n$, forms an information set $\mathcal{I}_n$ for $\mathcal{S}_n(\mathbb{F}_2)$, as indeed will any basis for $V_n(\mathbb{F}_2)$. The code can correct $2^{n-2}-1$ errors and has for automorphism group the general linear group $GL_n(\mathbb{F}_2)$.

In this paper we establish the existence of nested s-PD-sets of size $s+1$, for $1 \leq s \leq \left\lfloor \frac{2^n-1}{n} \right\rfloor - 1$, for permutation decoding up to s errors for the binary simplex codes for $n \geq 4$, using the information set $\mathcal{I}_n$. This means finding sets of $s+1$ matrices that will act as these s-PD-sets. (The full definitions of PD-sets and s-PD-sets are given in Section 2.) In particular, Result 1 in Section 2, gives a combinatorial lower bound for the size of a PD-set; this formula (due to Gordon and Schönheim) generalises to a formula for the lower bound for the size of an s-PD-set. Since small PD-sets are the most efficient, there has been some interest in finding codes with PD-sets that satisfy these bounds. For example, such PD-sets were found by Gordon [4] and Wolfman [16] for the binary Golay codes, and by Kroll and Vincenti [9, 10] for the dual binary Hamming code $\mathcal{H}_4^{\perp}(\mathbb{F}_2) = \mathcal{S}_4(\mathbb{F}_2)$.

When applied to the simplex code $\mathcal{S}_n(\mathbb{F}_2)$, the Gordon-Schönheim bound for s-PD-sets is $s+1$ for s up to some number depending on n and less than $2^{n-2}-1$, the full error-correction

*Email:wfish@uwc.ac.za, keyj@clemson.edu, emwambene@uwc.ac.za

capability of the code. We have denoted this limit by f_n here, and we show in Lemma 2 that $f_n = \lfloor \frac{2^n-1}{n} \rfloor - 1$. What we have done here is to show how to find s-PD-sets of size $s+1$ for s up to f_n for all n. This gives an infinite number of examples of s-PD-sets of size $s+1$ meeting the Gordon-Schönheim bound. Furthermore these sets are nested in a sense explained in Section 2, making the decoding algorithm more efficient. A similar construction applies to the q-ary simplex codes $S_n(\mathbb{F}_q)$ for any $q \geq 2$, and leads also to s-antiblocking information systems (definition given in Section 2) of size $s+1$ for any q.

We state our main result for the binary simplex codes as a theorem:

Theorem 1. *Let C denote the binary simplex code $\mathcal{S}_n(\mathbb{F}_2)$ with the set $\mathcal{I}_n$ of standard basis elements as row vectors for information set. C is a $[2^n-1, n, 2^{n-1}]_2$ code.*

If $n \geq 4$ and $Q_k = \{N_i \mid 0 \leq i \leq k\}$, where $k \geq 1$, is a set of $k+1$ matrices in $GL_n(\mathbb{F}_2)$ such that N_i and N_j for $i \neq j$ have no row in common, then $k \leq \lfloor \frac{2^n-1}{n} \rfloor - 1$ and $P_k = \{N_i^{-1} \mid 0 \leq i \leq k\}$ is a k-PD-set of $k+1$ elements for C that meets the Gordon-Schönheim bound for k-PD-sets. Such sets exist for all k such that $1 \leq k \leq \lfloor \frac{2^n-1}{n} \rfloor - 1$.

Conversely, if R_k is a k-PD-set for C of size $k+1$, then for $M, N \in R_k$, $M \neq N$, the rows of M^{-1} and N^{-1} are distinct.

Furthermore, a set of $k+1$ matrices in $GL_m(\mathbb{F}_2)$ for any $m \geq n$ can be constructed from Q_k such that the set of inverses will give a k-PD-set of size $k+1$ for $\mathcal{S}_m(\mathbb{F}_2)$ for information set $\mathcal{I}_m$ that also meets this bound.

Note that the action of the matrices on the coordinate positions of the code is via matrix multiplication vA where v is a row vector in $\mathbb{F}_2^n$ and $A \in GL_n(\mathbb{F}_2)$. As mentioned above, an analogous result holds for the q-ary simplex codes $S_n(\mathbb{F}_q)$ for any $q \geq 2$, and the action of the matrices will be described in Section 4.

The theorem is proved via a series of lemmas and propositions in Section 3. The relationship between these k-PD-sets of size $k+1$ and the k-antiblocking information systems introduced by Kroll and Vincenti [11] is shown in Corollary 3 to Proposition 1 for the binary case, and in Proposition 4 for the q-ary simplex codes for $q > 2$.

The paper is arranged in the following way. All the necessary definitions and terminology for codes, PD-sets and antiblocking information systems are given in Section 2. Section 3 contains the main results and constructions for permutation decoding for the binary simplex codes, in particular Proposition 1 describing the k-PD-sets of size $k+1$. Also in Section 3 it is shown in Lemma 6 that these k-PD-sets of size $k+1$ can be chosen in many different ways for $k < \frac{2^{n-1}}{n}$, which is approximately half the upper bound $\lfloor \frac{2^n-1}{n} \rfloor - 1$. In fact there is always at least one such set of the maximal size $\left\lfloor \frac{(q^n-1)/(q-1)}{n} \right\rfloor - 1$, for the binary and the q-ary case (the latter covered in Section 4).[1] We describe this construction in Lemma 5.

In Section 4 we state the analogues for the q-ary simplex code $\mathcal{S}_n(\mathbb{F}_q)$ for $q > 2$, and show in Proposition 4 that for $\mathcal{S}_n(\mathbb{F}_q)$, k-antiblocking information systems of size $k+1$ can be constructed in a way that is similar to that for $q = 2$ in Corollary 3. In Corollary 5 we show the analogue of Proposition 1 for the q-ary case for the k-PD-sets.

Finally, a program that will construct sets P_k of size $k+1$ for $\mathcal{S}_n(\mathbb{F}_2)$ for a given value of n, and that will run immediately in Magma [2, 3], is given as a web link in Section 5, along with a sample run, for $n = 6$, as another link. A program that will run the construction of a particular set of maximal size is also given in another link.

[1] We thank T. McDonough [14] for pointing out a special construction of such a set.

2 Background and terminology

The notation for codes is standard and can be found in [1]. The codes here are all **linear codes**, and the notation $[n, k, d]_q$ will be used for a q-ary code C of length n, dimension k, and minimum weight d, where the **weight wt(v)** of a vector v is the number of non-zero coordinate entries. The **support**, Supp(v), of a vector v is the set of coordinate positions where the entry in v is non-zero. So $|\text{Supp}(v)| = \text{wt}(v)$. A **generator matrix** for $C = [n, k, d]_q$ is a $k \times n$ matrix whose rows form a basis for C, and the **dual** code $C^\perp$ is the orthogonal under the standard inner product $(,)$, i.e. $C^\perp = \{v \in F^n \mid (v, c) = 0 \text{ for all } c \in C\}$. A **check matrix** for C is a generator matrix for $C^\perp$.

Following [1, Definition 2.2.3], two linear codes over the same field are called **equivalent** if each can be obtained from the other by permuting the coordinate positions and multiplying each coordinate by a non-zero field element. The codes will be said to be **isomorphic** if a permutation of the coordinate positions suffices to take one to the other. Generally, an **automorphism** of a code C is a code equivalence from C to C, and the set of all these gives the automorphism group of the code, written Aut(C) or MAut(C) (following [6, Chapter 7,Section 1.3]), since they are given by monomial matrices, and we do not consider here the more general case that includes field automorphisms, or the Galois groups. If only permutations of the coordinate positions are allowed then the group of permutation automorphisms is, again following [6, Chapter 7,Section 1.3], called the permutation automorphism group, written PAut(C). Any code is isomorphic to a code with generator matrix in so-called **standard form**, i.e. the form $[I_k \mid A]$; a check matrix then is given by $[-A^T \mid I_{n-k}]$. The set of the first k coordinates in the standard form is called an **information set** for the code, and the set of the last $n - k$ coordinates is the corresponding **check set**.

Permutation decoding was first developed by MacWilliams [12] and involves finding a set of automorphisms of a code called a PD-set. The method is described fully in MacWilliams and Sloane [13, Chapter 16, p. 513] and Huffman [6, Section 8]. In [7] and [9] the definition of PD-sets was extended to that of s-PD-sets for s-error-correction:

Definition 1. *If C is a t-error-correcting code with information set $\mathcal{I}$ and check set $\mathcal{C}$, then a* **PD-set** *for C is a set $\mathcal{S}$ of automorphisms of C which is such that every t-set of coordinate positions is moved by at least one member of $\mathcal{S}$ into the check positions $\mathcal{C}$.*

For $s \leq t$ an **s-PD-set** *is a set $\mathcal{S}$ of automorphisms of C which is such that every s-set of coordinate positions is moved by at least one member of $\mathcal{S}$ into $\mathcal{C}$.*

The algorithm for permutation decoding is as follows: we have a t-error-correcting $[n, k, d]_q$ code C with check matrix H in standard form. Thus the generator matrix $G = [I_k|A]$ and $H = [-A^T|I_{n-k}]$, for some A, and the first k coordinate positions correspond to the information symbols. Any vector v of length k is encoded as vG. Suppose x is sent and y is received and at most t errors occur. Let $S = \{g_1, \ldots, g_s\}$ be the PD-set. Compute the syndromes $H(yg_i)^T$ for $i = 1, \ldots, s$ until an i is found such that the weight of this vector is t or less. Compute the codeword c that has the same information symbols as yg_i and decode y as cg_i^{-1}.

Notice that this algorithm actually uses the PD-set as a sequence. Thus it is expedient to index the elements of the set S by the set $\{1, 2, \ldots, |S|\}$ so that elements that will correct a small number of errors occur first. Thus if **nested s-PD-sets** are found for all $1 < s \leq t$ then we can order S as follows: find an s-PD-set S_s for each $0 \leq s \leq t$ such that $S_0 \subset S_1 \ldots \subset S_t$

and arrange the PD-set S as a sequence in this order:

$$S = [S_0, (S_1 - S_0), (S_2 - S_1), \ldots, (S_t - S_{t-1})].$$

(Usually one takes $S_0 = \{id\}$.)

There is a bound on the minimum size that a PD-set S may have, due to Gordon [4], from a formula due to Schönheim [15], and quoted and proved in [6]:

Result 1. *If S is a PD-set for a t-error-correcting $[n,k,d]_q$ code C, and $r = n-k$, then*

$$|S| \geq \left\lceil \frac{n}{r} \left\lceil \frac{n-1}{r-1} \left\lceil \ldots \left\lceil \frac{n-t+1}{r-t+1} \right\rceil \ldots \right\rceil \right\rceil \right\rceil. \tag{1}$$

This result can be adapted to s-PD-sets for $s \leq t$ by replacing t by s in the formula.

In [11], Kroll and Vincenti introduced the concept of **antiblocking decoding**, which is closely related to permutation decoding: for a given code C with coordinate set $\mathcal{P}$, a set $\mathfrak{A}$ of information sets for C is called a **t-antiblocking information system** (**t-AI-system**) if for each t-set $T \subset \mathcal{P}$, there is a $B \in \mathfrak{A}$ such that $B \cap T = \emptyset$. The decoding algorithm using these sets is fully described in [11].

3 s-PD-sets of size $s+1$ for $\mathcal{S}_n(\mathbb{F}_2)$

In the following we will write $\mathcal{S}_n$ for $\mathcal{S}_n(\mathbb{F}_2)$; if q is not specifically 2 we will write $\mathcal{S}_n(\mathbb{F}_q)$.

We now show how to find s-PD-sets for $\mathcal{S}_n$ that satisfy the Gordon-Schönheim bound for s-PD-sets. Recall that $\mathcal{S}_n = [2^n - 1, n, 2^{n-1}]_2$, and that we take the set of standard basis elements of $V_n(\mathbb{F}_2) = \mathbb{F}_2^n$ to be the information set $\mathcal{I}_n$, and denote the corresponding check set by $\mathcal{C}_n$. So

$$\mathcal{I}_n = \{e_1, \ldots, e_n\} = \{(1,0,\ldots,0), \ldots, (0,\ldots,0,1)\}. \tag{2}$$

Thus the generator matrix for $\mathcal{S}_n$ will have for columns the $2^n - 1$ non-zero vectors from $V_n(\mathbb{F}_2)$, with the basis elements e_i^T in the first n positions. The labelling of the coordinate positions is simply by the columns they represent; the matrix is thus given in standard form. That $\mathrm{Aut}(\mathcal{S}_n) = GL_n(\mathbb{F}_2)$ follows most easily from the fact that $\mathrm{Aut}(\mathcal{H}_n(\mathbb{F}_2)) = GL_n(\mathbb{F}_2)$, since $\mathcal{H}_n(\mathbb{F}_2)$ is the code of the projective geometry design of points and lines in $PG_{n-1}(\mathbb{F}_2)$. We will write our vectors as row vectors, and thus vA will give the image of the vector $v \in V_n(\mathbb{F}_2)$ under the matrix $A \in GL_n(\mathbb{F}_2)$, and for any A the resulting permutation of the coordinate positions gives an automorphism of the code S_n.

We first look at this bound for $\mathcal{S}_n$, taking $n \geq 4$ since $\mathcal{S}_3$ only corrects a single error and permutation decoding is not necessary. For the simplex code $\mathcal{S}_n(\mathbb{F}_2)$, we will write $g_n(t)$ for the right-hand side of Equation (1), and $g_n(s)$ for the bound for the s-PD-set, i.e. just replacing t by s in the formula.

Lemma 1. *For the binary simplex code $\mathcal{S}_n$, and $n \geq 4$, for $1 \leq s \leq 2^{n-2} - 1$,*

$$g_n(s) = \left\lceil \frac{2^n - 1}{2^n - 1 - n} \left\lceil \frac{2^n - 2}{2^n - 2 - n} \left\lceil \ldots \left\lceil \frac{2^n - s}{2^n - s - n} \right\rceil \ldots \right\rceil \right\rceil \right\rceil \geq s + 1. \tag{3}$$

In particular, $g_n(1) = 2, g_n(2) = 3$ for all $n \geq 4$.

Proof: The innermost term in the formula for the bound is $\left\lceil \frac{2^n-s}{2^n-s-n} \right\rceil$. It is clear that this has value 2 for all $n \geq 4$ for all $1 \leq s \leq 2^{n-2}-1$. At each stage of the computation of the ceiling, starting at the innermost, the fraction is greater than 1, so the term will increase in value by at least 1. Thus $g_n(s) \geq s+1$ as asserted. The two examples given show that for small s this is indeed the value of $g_n(s)$. ■

Note: It is shown in [8, Proposition 1] that this result is true for all codes.

Definition 2. *For $\mathcal{S}_n$, $n \geq 4$, define*

$$f_n = \max\{s \mid 2 \leq s, g_n(s) = s+1\}.$$

Lemma 2. *For $n \geq 4$,*

$$f_n = \left\lfloor \frac{2^n-1}{n} \right\rfloor - 1.$$

Proof: There are s steps in the computation of the formula in Equation (3), and by Lemma 1, the innermost term is 2. Thus we must ensure that at each stage, working from the inside, the increase is exactly 1.

For the term after the innermost, this would require that

$$\left\lceil 2\left(\frac{2^n-s+1}{2^n-s+1-n}\right)\right\rceil = \left\lceil 2+\frac{2n}{2^n-s+1-n}\right\rceil = 3,$$

so $\frac{2n}{2^n-s+1-n} \leq 1$, i.e. $s \leq 2^n-3n+1$. For the next term (the third term) we get similarly $s \leq 2^n-4n+2$, and for the ℓ^{th}, $s \leq 2^n-(\ell+1)n+\ell-1$. Thus for $\ell = s$ we have $s \leq 2^n-(s+1)n+s-1$, and so

$$s \leq \left\lfloor \frac{2^n-1}{n} \right\rfloor - 1.$$

This final bound implies all the intermediate bounds since if at the ℓ^{th} stage we have $s \leq 2^n-(\ell+1)n+\ell-1 = 2^n-((\ell+1)n-(\ell+1)+2)$, then since $(\ell+1)n-(\ell+1)+2 \geq \ell n-\ell+2$ for $n \geq 1$, the previous $(\ell-1)^{th}$ bound will also be satisfied. Thus $f_n = \left\lfloor \frac{2^n-1}{n} \right\rfloor - 1$. ■

Note: These two lemmas hold also for the q-ary simplex codes, $\mathcal{S}_n(\mathbb{F}_q)$, with the formula for f_n, writing this as $f_n(\mathbb{F}_q)$, being $\left\lfloor \frac{(q^n-1)/(q-1)}{n} \right\rfloor - 1$.

For any $s \leq f_n$ an s-PD-set of size $s+1$ will meet the Gordon-Schönheim bound for correction of s errors. We now find conditions on sets of matrices from $GL_n(\mathbb{F}_2)$ for this to happen.

Proposition 1. *Let $C = \mathcal{S}_n$, where $n \geq 4$, with information set $\mathcal{I}_n$, check set $\mathcal{C}_n$.*

If $P_k = \{M_i \mid 0 \leq i \leq k\}$ is a set of $k+1$ matrices in $GL_n(\mathbb{F}_2)$ such that no two matrices M_i^{-1} and M_j^{-1} for $i \neq j$ have a row in common, then P_k is a k-PD-set of $k+1$ elements for C. Furthermore, any subset of P_k of size $s+1$ where $1 \leq s \leq k$ is an s-PD-set for C.

Conversely, if $R_k = \{N_i \mid 0 \leq i \leq k\}$ is a k-PD-set for C then no two matrices N_i^{-1} and N_j^{-1} for $i \neq j$ have a row in common.

Proof: Suppose $P_k = \{M_i \mid 0 \leq i \leq k\}$ and no two matrices M_i^{-1} and M_j^{-1} for $i \neq j$ have a row in common. Let $T = \{v_1, \ldots, v_k\}$ be a set of k distinct vectors in $V_n(\mathbb{F}_2)$. Suppose that

we cannot map T into $\mathcal{C}_n$ by any element of P_k. Then for each i such that $0 \le i \le k$, there is a v_j, for $1 \le j \le k$, such that $v_j M_i \in \mathcal{I}_n$. Since there are $k+1$ values of i but only k of j we must have $v_j M_i$ and $v_j M_l$, for some j, and $i \ne l$, both of weight 1. Suppose $v_j M_i = e_r$ and $v_j M_l = e_t$; then $v_j = e_r M_i^{-1} = e_t M_l^{-1}$, so the r^{th} row of M_i^{-1} is the t^{th} row of M_l^{-1}, contradicting our assumption.

For the converse, suppose that $R_k = \{N_i \mid 0 \le i \le k\}$ is a k-PD-set for C and that some $v \in V_n(\mathbb{F}_2)$ is the r^{th} row of N_i^{-1} and the t^{th} row of N_j^{-1}. So $v = e_r N_i^{-1} = e_t N_j^{-1}$, and $vN_i = e_r$, $vN_j = e_t$. Let $J = \{m \mid 0 \le m \le k, m \ne i, j\}$. For each $m \in J$, choose a row v_m of N_m^{-1}. We have a set of at least $k-1$ vectors v_m for each of which $v_m N_m = e_t$, some t, and so $v_m N_m$ has weight 1. The set $T = \{v_m \mid m \in J\} \cup \{v\}$ has size at most k (since some of the v_m may repeat), but no matrix in R_k will map every member of T into $\mathcal{C}_n$, contradicting the assumption that R_k is a k-PD-set.

Finally, the statement about subsets of P_k of size $s+1$ is clear for the same reason that it is true for k. ■

Corollary 1. *For $n \ge 4$, if P_k of size $k+1$ is a k-PD-set for $\mathcal{S}_n$ with information set $\mathcal{I}_n$ then any ordering of the elements of P_k gives nested s-PD-sets for $1 \le s \le k$.*

To illustrate the corollary using the algorithm for permutation decoding, we can order the elements of P_k arbitrarily as $[M_{i_0}, \ldots, M_{i_k}]$. Then, if no errors occur, M_{i_0} will decode; if one error occurs, either M_{i_0} or M_{i_1} will decode; if three errors occur one of the first three will decode; and so on, so that for s errors one of the first $s+1$ will perform the decoding. Thus the fewer errors that occur (which is assumed for a good channel), the sooner the vector will be decoded.

From the proposition we also get another proof of the formula for f_n as found in Lemma 2:

Corollary 2. *For $n \ge 4$, a k-PD-set of $k+1$ elements of $GL_n(\mathbb{F}_2)$ for S_n with information set $\mathcal{I}_n$ must satisfy $k \le \left\lfloor \frac{2^n-1}{n} \right\rfloor - 1$.*

Proof: From Proposition 1, the k-PD-set of $k+1$ matrices will have for its set of inverses, $k+1$ matrices with no row occurring twice. Thus counting the rows we have $(k+1)n \le 2^n - 1$ and hence $k \le \left\lfloor \frac{2^n-1}{n} \right\rfloor - 1$. ■

Related to the concept of antiblocking decoding, we have another corollary to our proposition, noticing first that the rows of any matrix in $GL_n(\mathbb{F}_2)$ form an information set for $\mathcal{S}_n$:

Corollary 3. *Suppose $n \ge 4$ and $Q_k = \{N_i \mid 0 \le i \le k\}$, where $k \ge 1$, is a set of $k+1$ matrices in $GL_n(\mathbb{F}_2)$ such that N_i and N_j for $i \ne j$ have no row in common. If R_i is the set of rows of N_i for $0 \le i \le k$, the set $\mathfrak{Q} = \{R_i \mid 0 \le i \le k\}$ is a k-antiblocking information system of size $k+1$ for $\mathcal{S}_n$.*

Conversely, any k-antiblocking information system $\mathfrak{A} = \{A_i \mid 0 \le i \le k\}$ for S_n of $k+1$ elements must have the property that $A_i \cap A_j = \emptyset$ for $i \ne j$.

Proof: By Proposition 1, $P_k = \{N_i^{-1} \mid 0 \le i \le k\}$ is a k-PD-set for information set $\mathcal{I}_n$, so for any k-set of vectors $T = \{v_i \mid 1 \le i \le k\}$ there is an N_i^{-1} such that $v_j N_i^{-1} \in \mathcal{C}_n$ for $1 \le j \le k$. Then $T \cap R_i = \emptyset$. So $\mathfrak{Q}$ is a k-antiblocking information system for $\mathcal{S}_n$.

Conversely, if given a k-AI-system $\mathfrak{A} = \{A_i \mid 0 \le i \le k\}$ for S_n of $k+1$ elements, the proof that there can be no vector in common to two members of $\mathfrak{A}$ is precisely as in the proof

of the converse in Proposition 1, since each A_i consists of n vectors that form a basis for $V_n(\mathbb{F}_2)$ and thus define an invertible matrix. ■

Note: Corollary 3 also follows from [8, Proposition 1].

In practice we usually take $M_0 = I_n$ to deal with the case of no errors. For this case we first define

$$\mathcal{A}_n = \{M \mid M \in GL_n(\mathbb{F}_2), \text{ all rows of } M \text{ have weight at least } 2\}. \tag{4}$$

Then we have the following:

Proposition 2. *Let $C = \mathcal{S}_n$ where $n \geq 4$, with information set $\mathcal{I}_n$, check set $\mathcal{C}_n$.*
If $P_k = \{M_0 = I_n, M_1, \ldots M_k\}$ is a set of $k+1$ matrices in $GL_n(\mathbb{F}_2)$ which is such that for every pair (i,j), $i \neq j$, $M_i^{-1}M_j \in \mathcal{A}_n$, then P_k is a k-PD-set of $k+1$ elements for C.

Proof: First note that $M \in \mathcal{A}_n$ if and only if $M^{-1} \in \mathcal{A}_n$. For suppose $M \in \mathcal{A}_n$. If M^{-1} has a row of weight 1, say e_j in the i^{th} row, then the i^{th} row of $I_n = M^{-1}M$ is the j^{th} row of M, and thus has weight more than 1, which is impossible. Thus $M^{-1} \in \mathcal{A}_n$.

The condition implies that $M_i = M_0^{-1}M_i \in \mathcal{A}_n$ for $i \geq 1$. We next prove that rows of M_i^{-1} and M_j^{-1} for $i \neq j$ are distinct. Clearly the rows of any M_i^{-1} for $i \geq 1$ are distinct from those of I_n, so suppose that the vector v is a row of both M_i^{-1} and M_j^{-1} where $0 \neq i \neq j \neq 0$. Then $v = e_r M_i^{-1} = e_s M_j^{-1}$ for some r, s. So $vM_j = e_r M_i^{-1} M_j = e_s$ which is a contradiction since $M_i^{-1}M_j \in \mathcal{A}_n$. Now we can use Proposition 1 to complete the proof. ■

We now show how we can build these s-PD-sets for any n by defining them recursively.

Definition 3. *For $M \in GL_n(\mathbb{F}_2)$, $M = [m_{i,j}]$, and $u = (u_1, \ldots, u_n) \in V_n(\mathbb{F}_2)$, $u \neq 0$, let $M(u) = [a_{i,j}]$ be the $(n+1) \times (n+1)$ matrix such that:*
$a_{1,1} = 1$; $a_{1,1+i} = u_i$ for $1 \leq i \leq n$; $a_{i,1} = 0$ for $2 \leq i \leq n+1$; $a_{i+1,j+1} = m_{i,j}$ for $1 \leq i, j \leq n$.

Thus

$$M(u) = \left[\begin{array}{c|ccc} 1 & u_1 & \ldots & u_n \\ \hline 0 & & & \\ \vdots & & M & \\ 0 & & & \end{array}\right].$$

Example 1. If $M = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$, $u = (1,0,0,0) = e_1$ then $M(u) = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{bmatrix}$.

Lemma 3. *If $Q_k = \{A_i \mid 0 \leq i \leq k\}$ is a set of matrices in $GL_n(\mathbb{F}_2)$ such that the rows of A_i are distinct from those of A_j for $i \neq j$, then if $u_0, u_1, \ldots, u_k$ are distinct vectors in $V_n(\mathbb{F}_2)$, the set $Q_k^* = \{A_i(u_i) \mid 0 \leq i \leq k\}$ is a set of matrices in $GL_{n+1}(\mathbb{F}_2)$ with the same property.*

Proof: This is immediate. ■

Thus to find these k-PD-sets of size $k+1$ one needs to find $k+1$ invertible $n \times n$ matrices with no rows in common, i.e. $k+1$ mutually disjoint bases sets for $V_n(\mathbb{F}_2)$. This needs

computational help in general, but then using Lemma 3 (and Corollary 4 below) will give a set of $k+1$ such bases for any $m \geq n$. For $n = 4$ we can do this without computational help for $k = 2$, as the next proposition shows:

Proposition 3. *If* $N_1 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$, $N_2 = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}$, *then* $P_3 = \{I_4, N_1^{-1}, N_2^{-1}\}$ *is a 2-PD set for* $\mathcal{S}_4$ *using the information set* $\mathcal{I}_4$. *If* $(N_1)_1 = N_1(e_1)$, $(N_2)_1 = N_2(e_2)$, *and recursively* $(N_1)_r = (N_1)_{r-1}(e_1)$, $(N_2)_r = (N_2)_{r-1}(e_2)$, *for* $r \geq 2$, *where* e_1, e_2 *are the standard basis elements of the relevant length, then for* $n \geq 5$,

$$P_3(n) = \{I_n, (N_1)_{n-4}^{-1}, (N_2)_{n-4}^{-1}\}$$

is a 2-PD set for $\mathcal{S}_n$ *with the information set* $\mathcal{I}_n$.

Proof: It is easy to check that N_1, N_2 are non-singular and clearly they have distinct rows of weight at least 2. So the set of inverses is a 2-PD-set by Proposition 1, and by the same proposition, this holds for $P_3(n)$ for $n \geq 5$. ■

Note: A third matrix N_2 does not exist if the first two are I_4 and $N_1 = I_4 + J$, where J is the all-ones matrix, since all the remaining vectors are of even weight and so there are at most three in a linearly independent set.

Example 2. In Proposition 3, for $n = 6$,

$$N_1(e_1) = \left[\begin{array}{c|c|cccc} 1 & 1 & 0 & 0 & 0 & 0 \\ \hline 0 & 1 & 1 & 0 & 0 & 0 \\ \hline 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{array}\right], \text{ and } N_2(e_2) = \left[\begin{array}{c|c|cccc} 1 & 0 & 1 & 0 & 0 & 0 \\ \hline 0 & 1 & 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{array}\right].$$

Corollary 4. *For* $n \geq 4$, *if a k-PD-set of* $k+1$ *matrices for* $\mathcal{S}_n$ *with information set* $\mathcal{I}_n$ *can be found then a k-PD-set of* $k+1$ *matrices for* $\mathcal{S}_m$ *with information set* $\mathcal{I}_m$ *can be found for all* $m \geq n$.

Proof: Let $P_k = \{M_i \mid 0 \leq i \leq k\}$ be a k-PD-set for $\mathcal{S}_n$ and let $N_i = M_i^{-1}$ for $i = 0, \ldots, k$. Let $\{u_i \mid 0 \leq i \leq k\}$ be a set of $k+1$ distinct vectors of $V_n(\mathbb{F}_2)$. Such a set clearly exists: for example, u_i could be taken to be the binary representation of the number i for $0 \leq i \leq k$. Since k is at most $t = 2^{n-2} - 1$, all the numbers $i \leq k$ will have binary representations with non-zero entries only in the first (left-most) $n-1$ positions at most. As in Proposition 3, define recursively, for any $r \geq 1$, and adding 0 at the end of u_i at each stage, $(N_i)_1 = N_i(u_i)$, $(N_i)_r = (N_i)_{r-1}(u_i)$ for each $0 \leq i \leq k$, and for $1 \leq r \leq m$. Then for any $m > n$,

$$Q_k = \{(N_0)_{m-n}^{-1}, (N_1)_{m-n}^{-1}, \ldots, (N_k)_{m-n}^{-1}\}$$

is a nested k-PD-set of $k+1$ elements for $\mathcal{S}_m$, with information set $\mathcal{I}_m$. ■

The following lemma gives the size of the set $\mathcal{A}_n$ of matrices from which the PD-sets are chosen if I_n is taken to be a member of the set.

Lemma 4. *For $n \geq 3$, writing $\mathcal{A}_n$ for the set of matrices in $GL_n(\mathbb{F}_2)$ having every row of weight at least 2, we have*

$$|\mathcal{A}_n| = |GL_n(\mathbb{F}_2)| - \sum_{i=1}^{n} (-1)^{i-1} \binom{n}{i} 2^{i(n-i)} |GL_{n-i}(\mathbb{F}_2)| \prod_{j=1}^{i} (n-j+1),$$

where $|GL_n(\mathbb{F}_2)| = \prod_{j=0}^{n-1}(2^n - 2^j)$ and $|GL_0(\mathbb{F}_2)| = 1$.

Proof: We count the number of matrices in $GL_n(\mathbb{F}_2)$ that have a row of weight 1, and subtract this number from $|GL_n(\mathbb{F}_2)|$ to get the size of $\mathcal{A}_n$.

Let S_i, for $1 \leq i \leq n$, denote the number of matrices in $GL_n(\mathbb{F}_2)$ that have one row equal to the basis element e_i. Then

$$|S_i| = n 2^{n-1} |GL_{n-1}(\mathbb{F}_2)|.$$

For any subset $\{i_1, \ldots, i_m\}$ of $\{1, \ldots, n\}$ of size m where $1 \leq m \leq n$,

$$|\bigcap_{i=1}^{m} S_i| = \prod_{j=1}^{m} (n-j+1) 2^{m(n-m)} |GL_{n-m}(\mathbb{F}_2)|.$$

Thus counting using inclusion-exclusion gives the stated result. ■

Note: Since $GL_n(\mathbb{F}_2)$ is transitive on bases of $V_n(\mathbb{F}_2)$, this also counts the matrices in $GL_n(\mathbb{F}_2)$ that do not contain as a row any member of a set of n linearly independent vectors of $V_n(\mathbb{F}_2)$.

A set of $f_n + 1$ matrices that form an f_n-PD-set can be found if and only if all but $2^n - 1 \bmod n$ of the non-zero vectors of $V_n(\mathbb{F}_2)$ can be partitioned into $f_n + 1$ mutually disjoint sets of n linearly independent vectors of $V_n(\mathbb{F}_2)$. Such a partition also gives an f_n-antiblocking information system of size $f_n + 1$, as pointed out in Corollary 3.

A construction described to us by McDonough [14], regarding $\mathbb{F}_{q^n}$ as $V_n(\mathbb{F}_q)$, shows that there always exists at least one such partition of the projective points in $PG_{n-1}(\mathbb{F}_q)$, for any n and q, into a set of $f_n(\mathbb{F}_q) + 1$ mutually disjoint bases sets for $V_n(\mathbb{F}_q)$, where $f_n(\mathbb{F}_q) = \left\lfloor \frac{(q^n-1)/(q-1)}{n} \right\rfloor - 1$:

Lemma 5. *For $n \geq 2$, $q \geq 2$ a prime power, let $K = \mathbb{F}_{q^n}$ and let ζ be a primitive element of K^*. For $0 \leq i \leq f_n(\mathbb{F}_q)$, if $B_i = \{\zeta^{j+in} \mid 0 \leq j \leq n-1\}$, then $\{B_i \mid 0 \leq i \leq f_n(\mathbb{F}_q)\}$ is a set of $f_n(\mathbb{F}_q) + 1$ mutually disjoint bases for $V_n(\mathbb{F}_q)$.*

Proof: Notice that for $v \in K^*$, if $v\zeta^r = \lambda v$ where $\lambda \in \mathbb{F}_q^*$, then r is a multiple of $(q^n-1)/(q-1)$. Thus $\{v\zeta^r \mid 0 \leq r < (q^n-1)/(q-1)\}$ define distinct points in $PG_{n-1}(\mathbb{F}_q)$. Since $B_0 = \{1, \zeta, \ldots, \zeta^{n-1}\}$, it defines the standard basis for $V_n(\mathbb{F}_q)$, and thus each B_i is a basis. They are mutually disjoint by the earlier comment. ■

A rather rough count shows that it is always possible to get approximately $\frac{1}{2} f_n$ such mutually disjoint bases by many other choices:

Lemma 6. *For $n \geq 4$, if $k < \frac{2^{n-1}}{n}$ and if $\mathcal{B}_k$ is a set of k mutually disjoint bases for $V_n(\mathbb{F}_2)$, then a further basis that is mutually disjoint from all the members of $\mathcal{B}_k$ exists. Thus a set of $k+1$ mutually disjoint bases for $V_n(\mathbb{F}_2)$ exist.*

Proof: We can start with $k = 1$ by taking any basis for $V = V_n(\mathbb{F}_2)$. Suppose we have a set $\mathcal{B}_k$ of k mutually disjoint bases. To form a further basis disjoint from any of those in $\mathcal{B}_k$, we can choose the first vector in $2^n - 1 - nk$ ways, the next in $2^n - 2 - nk$ ways and so on until the n^{th} in at least $2^n - 2^{n-1} - nk$ ways. So as long as this last number is greater than zero, another basis, disjoint from all the members of $\mathcal{B}_k$, will exist. Thus $k < \frac{2^{n-1}}{n}$ will suffice. ■

Note: The upper bound $b_n < \frac{2^{n-1}}{n}$ in Lemma 6 is $\frac{1}{2}f_n$ if n is a power of 2 or if $2^{n-1} \bmod n \geq \frac{n+1}{2}$, and is $\frac{1}{2}(f_n + 1)$ if $2^{n-1} \bmod n < \frac{n+1}{2}$. Equivalently, $b_n = \frac{1}{2}f_n$ if f_n is even, and $b_n = \frac{1}{2}(f_n + 1)$ if f_n is odd.

4 The codes $\mathcal{S}_n(\mathbb{F}_q)$, $q > 2$

The q-ary simplex code $\mathcal{S}_n(\mathbb{F}_q)$ is a q-ary code with generator matrix having for columns any set of $\frac{q^n-1}{q-1}$ representatives of the distinct 1-dimensional subspaces of $V_n(\mathbb{F}_q)$. Thus for $q > 2$ the actual code depends on the representatives chosen, but the codes are of course all equivalent. Here $\mathcal{S}_n(\mathbb{F}_q)$ is a $[\frac{q^n-1}{q-1}, n, q^{n-1}]_q$ code and all the non-zero words have weight q^{n-1}: see, for example, [1, Section 2.5]. The automorphism group is isomorphic to $\Gamma L_n(q)$, as shown in [6, Section 7].

The permutation group $\mathrm{PAut}(\mathcal{S}_n(\mathbb{F}_q))$ of the code has not in general been computed, except for the case where all the columns are normalized in which case Gorkunov [5] has shown that the permutation group is isomorphic to the group of lower (or upper) triangular matrices. However we only need the permutation part of an automorphism for permutation decoding, so we can still use the matrices as before. We describe how this follows below in Corollary 5.

The antiblocking decoding of [11] can be applied for $q > 2$ as in the case $q = 2$:

Proposition 4. *For $n \geq 2$, let $C = \mathcal{S}_n(\mathbb{F}_q)$ where $q \geq 2$. Suppose that $Q_k = \{N_i \mid 0 \leq i \leq k\}$, where $k \geq 1$, is a set of $k + 1$ matrices in $GL_n(\mathbb{F}_q)$ such that the rows of each matrix are normalized, and such that N_i and N_j for $i \neq j$ have no row in common. If R_i is the set of rows of N_i for $0 \leq i \leq k$, the set $\mathfrak{Q} = \{R_i \mid 0 \leq i \leq k\}$ is a k-antiblocking information system of size $k + 1$ for C. The converse holds as well.*

Proof: We may assume that the set of coordinate positions of C is normalized. Let $T = \{v_i \mid 1 \leq i \leq k\}$ be a set of distinct normalized vectors. Since the sets R_i are disjoint, any $v \in T$ can be in at most one member R of $\mathfrak{Q}$. Since there are k members of T and $k + 1$ members of $\mathfrak{Q}$, there must be at least one that is not met by T, so we have a k-AI-system.

The converse can be proved similarly, as in Corollary 3. ■

Note that the construction for $q = 2$ in Corollary 4 also applies for $q > 2$ (modifying Definition 3 suitably by taking $M \in GL_n(\mathbb{F}_q)$ to be normalised) and thus to s-AI-systems, so if an s-AI-system of $s + 1$ elements can be found for $\mathcal{S}_n(\mathbb{F}_q)$, then an s-AI-system of $s + 1$ elements can be found for $\mathcal{S}_m(\mathbb{F}_q)$ for any $m \geq n$.

Corollary 5. *For $n \geq 2$, let $C = \mathcal{S}_n(\mathbb{F}_q)$ where $q \geq 2$. Suppose that $Q_k = \{N_i \mid 0 \leq i \leq k\}$, where $k \geq 1$, is a set of $k + 1$ matrices in $GL_n(\mathbb{F}_q)$ such that the rows of each matrix are normalized, and such that N_i and N_j for $i \neq j$ have no row in common. Then the set $P_k = \{N_i^{-1} \mid 0 \leq i \leq k\}$ define a set of automorphisms of C that form a PD-set of size $k+1$.*

Proof: The proof that any $t \leq k$ positions will be moved by some N_i^{-1} is as before in the binary case. The algorithm for permutation decoding concerns automorphisms that need not be permutation automorphisms. The automorphism corresponding to a matrix $N \in GL_n(q)$ is defined by the monomial matrix M that satisfies $G^T N = MG^T$, where G is a generator matrix, and we take it to be in standard form for permutation decoding. Then M acts on a codeword x by $x \mapsto xM$. ■

By the construction of Lemma 5, sets of bases of maximal size always exist. Also, a count similar to that used in Lemma 6 shows that for $k < \frac{q^{n-1}}{n}$ many other sets of $k+1$ mutually disjoint bases of projective points for $V_n(\mathbb{F}_q)$ exist. For $n = 2$, where $\mathcal{S}_2(\mathbb{F}_q)$ is the extended Reed-Solomon code, $[q+1, 2, q]_q$, other explicit sets of maximal size can be described:

Corollary 6. *Let $C = \mathcal{S}_2(\mathbb{F}_q)$, where $q > 2$. Suppose $\mathbb{F}_q^* = \{a_i \mid 1 \leq i \leq q-1\}$. If*

$$Q = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right\} \cup \left\{ \begin{bmatrix} 1 & a_{2j+1} \\ 1 & a_{2j} \end{bmatrix} \mid 0 \leq j \leq m \right\}$$

where $m = \frac{q-1}{2}$ for q odd, $\frac{q}{2} - 1$ for q even, then Q is a set of $f_2(\mathbb{F}_q)+1$ matrices that satisfies Proposition 4.

Proof: Note that $f_2(\mathbb{F}_q) = \frac{q-1}{2}$ for q odd, $\frac{q}{2} - 1$ for q even. The proof is immediate. ■

5 Computational

The web links given below are to some programs that will find sets P_k for $\mathcal{S}_n$ using Magma, and a run of these for $n = 6$. Essentially the programs look for $k+1$ matrices in $GL_n(\mathbb{F}_2)$ that have no row in common, and then take the set of inverses as the k-PD-set. More efficient ways of finding such a set result in approaching nearer to the bound f_n. This was done for $n = 8$, where the program as given only easily gave 30 matrices; the program was stopped and a remaining matrix was then easily found from the 15 vectors not amongst the rows of the 30 already found. Similar computations were done for the q-ary codes.

A program to construct the particular set described in Lemma 5 is also included at the link below.

```
The program:  http://www.ces.clemson.edu/~keyj/bin_simplex1.m
A run for n=6:  http://www.ces.clemson.edu/~keyj/6log
Extension field construction: http://www.ces.clemson.edu/~keyj/ext_field.m
```

The links: binsimplex1.m; 6log; extfield.m.

Acknowledgements

The authors thank the reviewers for their careful reading and useful comments, and Dr T.P. McDonough for helpful discussions that have improved the results of the original manuscript.

References

[1] E. F. Assmus, Jr and J. D. Key, *Designs and their codes*, Cambridge: Cambridge University Press, 1992, Cambridge Tracts in Mathematics, Vol. 103 (Second printing with corrections, 1993).

[2] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system I: The user language*, J. Symbolic Comput. **24, 3/4** (1997), 235–265.

[3] J. Cannon, A. Steel, and G. White, *Linear codes over finite fields*, Handbook of Magma Functions (J. Cannon and W. Bosma, eds.), Computational Algebra Group, Department of Mathematics, University of Sydney, 2006, V2.13, http://magma.maths.usyd.edu.au/magma, pp. 3951–4023.

[4] D. M. Gordon, *Minimal permutation sets for decoding the binary Golay codes*, IEEE Trans. Inform. Theory **28** (1982), 541–543.

[5] E. V. Gorkunov, *The group of permutation automorphisms of a q-ary Hamming code*, Probl. Inf. Transm. **45** (2009), 309 – 316.

[6] W. C. Huffman, *Codes and groups*, Handbook of Coding Theory (V. S. Pless and W. C. Huffman, eds.), Amsterdam: Elsevier, 1998, Volume 2, Part 2, Chapter 17, pp. 1345–1440.

[7] J. D. Key, T. P. McDonough, and V. C. Mavron, *Partial permutation decoding for codes from finite planes*, European J. Combin. **26** (2005), 665–682.

[8] H.-J. Kroll and R. Vincenti, *How to find small antiblocking systems*, http://dx.doi.org/10.1016/j.disc.2011.06.014.

[9] ———, *PD-sets related to the codes of some classical varieties*, Discrete Math. **301** (2005), 89–105.

[10] ———, *PD-sets for binary RM-codes and the codes related to the Klein quadric and to the Schubert variety of* $PG(5, 2)$, Discrete Math. **308** (2008), 408–414.

[11] ———, *Antiblocking decoding*, Discrete Appl. Math. **158** (2010), 1461–1464.

[12] F. J. MacWilliams, *Permutation decoding of systematic codes*, Bell System Tech. J. **43** (1964), 485–505.

[13] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes*, Amsterdam: North-Holland, 1983.

[14] T.P. McDonough, Private communication, 2012.

[15] J. Schönheim, *On coverings*, Pacific J. Math. **14** (1964), 1405–1411.

[16] J. Wolfmann, *A permutation decoding of the* $(24, 12, 8)$ *Golay code*, IEEE Trans. Inform. Theory **29** (1983), 748–750.