Reed-Muller codes and permutation decoding

J. D. Key, T. P. McDonough and V. C. Mavron
Institute of Mathematics and Physics
Aberystwyth University, Aberystwyth, Ceredigion SY23 3BZ, U.K.

13th May, 2009

Abstract

We show that the first- and second-order Reed-Muller codes, $\mathcal{R}(1,m)$ and $\mathcal{R}(2,m)$, can be used for permutation decoding by finding, within the translation group, $(m-1)$- and $(m+1)$-PD-sets for $\mathcal{R}(1,m)$ for $m \geq 5, 6$, respectively, and $(m-3)$-PD-sets for $\mathcal{R}(2,m)$ for $m \geq 8$. We extend the results of Seneviratne [14].

1 Introduction

The first- and second-order Reed-Muller codes, $\mathcal{R}(1,m)$ and $\mathcal{R}(2,m)$, are binary codes with large minimum weight, being the codes of the affine geometry designs over $\mathbb{F}_2$ of points and $(m-1)$-flats or $(m-2)$-flats, respectively, and with the minimum words the incidence vectors of the blocks. Furthermore, they each have a large automorphism group containing the translation group, making them good candidates for permutation decoding. Seneviratne [14] found 4-PD-sets for the first-order Reed-Muller codes $\mathcal{R}(1,m)$ for $m \geq 5$. We extend his method to find $(m-1)$-PD-sets of size $\frac{1}{2}(m^2+m+4)$ for $\mathcal{R}(1,m)$ for $m \geq 5$, $(m+1)$-PD-sets of size $\frac{1}{6}(m^3+5m+12)$ for $\mathcal{R}(1,m)$ for $m \geq 6$, and $(m-3)$-PD-sets of size $\frac{1}{6}(m^3+5m+12)$ for $\mathcal{R}(2,m)$ for $m \geq 8$.

We prove the following theorem.

Theorem 1 *Let $V = \mathbb{F}_2^m$ and $C_i = \{v \mid v \in V, \mathrm{wt}(v) = i\}$ for $0 \leq i \leq m$. Let T_u denote the translation of V by $u \in V$,*

$$A_m = \{T_u \mid u \in C_0 \cup C_1 \cup C_2 \cup C_m\},\ B_m = A_m \cup \{T_u \mid u \in C_3\},$$

then

1. *A_m is an $(m-1)$-PD-set of size $\frac{1}{2}(m^2+m+4)$ for $\mathcal{R}(1,m)$ and $m \geq 5$ using the information set $C_0 \cup C_1$;*

2. *B_m is an $(m+1)$-PD-set of size $\frac{1}{6}(m^3+5m+12)$ for $\mathcal{R}(1,m)$ and $m \geq 6$ using the information set $C_0 \cup C_1$;*

3. *B_m is an $(m-3)$-PD-set of size $\frac{1}{6}(m^3+5m+12)$ for $\mathcal{R}(2,m)$ and $m \geq 8$ using the information set $C_0 \cup C_1 \cup C_2$.*

The theorem will follow from Propositions 1, 2 and 3 in Sections 4 and 5. Before stating and proving these propositions, we give some background results and definitions.

2 Background and terminology

Most of the notation will be as in [1], with some exceptions noted. An incidence structure $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$, with point set $\mathcal{P}$, block set $\mathcal{B}$ and incidence $\mathcal{I}$ is a t-(v,k,λ) design, if $|\mathcal{P}| = v$, every block $B \in \mathcal{B}$ is incident with precisely k points, and every t distinct points are together incident with precisely λ blocks. We deal here with the design of points and t-flats, where $t \geq 1$, of the affine space $AG_m(\mathbb{F}_2)$, which we will denote by $AG_{m,t}(\mathbb{F}_2)$, and in particular with the case of $t = m-1$ (points and hyperplanes or $(m-1)$-flats) and $t = m-2$ (points and $(m-2)$-flats).

For $F = \mathbb{F}_p$, where p is a prime, the code $C_F = C_p(\mathcal{D})$ of the design $\mathcal{D}$ over the finite field F is the space spanned by the incidence vectors of the blocks over F. We take F to be a prime field $\mathbb{F}_p$ where p must divide the order of the design. If the incidence vector of a subset $\mathcal{Q}$ of points is denoted by $v^{\mathcal{Q}}$, then $C_F = \langle v^B \mid B \in \mathcal{B} \rangle$, and is a subspace of $F^{\mathcal{P}}$, the full vector space of functions from $\mathcal{P}$ to F.

A linear code over $\mathbb{F}_q$ of length n, dimension k, and minimum weight d, is denoted by $[n,k,d]_q$. If c is a codeword then the **support** of c, $\mathrm{Supp}(c)$, is the set of non-zero coordinate positions of c, and the **weight** (or Hamming weight) of c, $\mathrm{wt}(c)$, is the size of its support. A **constant word** in the code is a codeword all of whose non-zero coordinate entries are equal. The all-one vector $\boldsymbol{\jmath}$ is the constant vector with all entries equal to 1. The value of c at the coordinate position P will be denoted by $c(P)$. An **automorphism** of a code C is an isomorphism from C to C.

Permutation decoding was introduced by MacWilliams [10] and Prange [12] and involves finding a set of automorphisms of a code called a PD-set. The method is described fully in MacWilliams and Sloane [11, Chapter 15] and Huffman [4, Section 8]. The concept of PD-sets was extended to s-PD-sets for s-error-correction in [6] and [8]:

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 efficiency of the algorithm for permutation decoding (see [4, Section 8], or [7, Section 2]) requires that the set $\mathcal{S}$ is small; there is a combinatorial lower bound on its size due to Gordon [3] and Schönheim [13] (see [4] or [7]). A partial survey of known results concerning s-PD-sets for codes from designs and geometries can be found in [5] or at the website:

`http://www.ces.clemson.edu/~keyj/` and, in particular,
`http://www.ces.clemson.edu/~keyj/Key/c2008.pdf`.

3 Reed-Muller codes

We use the notation of [1, Chapter 5] or [2] for generalized Reed-Muller codes. Let $q = p^t$, where p is a prime, and let V be the vector space $\mathbb{F}_q^m$ of m-tuples, with standard basis. The codes will be q-ary codes with ambient space the function space $\mathbb{F}_q^V$, with the usual basis of characteristic functions of the vectors of V. We can denote the elements f of $\mathbb{F}_q^V$ by functions of the m-variables denoting the coordinates of a variable vector in V, i.e. if $\mathbf{x} = (x_1, x_2, \ldots, x_m) \in V$, then $f \in \mathbb{F}_q^V$ is given by $f = f(x_1, x_2, \ldots, x_m)$ and the x_i take values in $\mathbb{F}_q$. Since $a^q = a$ for $a \in \mathbb{F}_q$, the polynomial functions can be reduced modulo $x_i^q - x_i$. Furthermore, every polynomial can be written uniquely as a linear combination of the q^m monomial functions

$$\mathcal{M} = \{x_1^{i_1} x_2^{i_2} \ldots x_m^{i_m} \mid 0 \leq i_k \leq q-1, \text{ for } 1 \leq k \leq m\}.$$

For any such monomial the degree ρ is the total degree, i.e. $\rho = \sum_{k=1}^m i_k$ and clearly $0 \leq \rho \leq m(q-1)$.

The **generalized Reed-Muller** codes are defined as follows (see [1, Definition 5.4.1]):

Definition 2 *Let $V = \mathbb{F}_q^m$ be the vector space of m-tuples, for $m \geq 1$, over $\mathbb{F}_q$, where $q = p^t$ and p is a prime. For any ρ such that $0 \leq \rho \leq m(q-1)$, the* $\boldsymbol{\rho^{th}}$**-order generalized Reed-Muller code** $\mathcal{R}_{\mathbb{F}_q}(\rho, m)$ *is the subspace of $\mathbb{F}_q^V$ (with basis the characteristic functions of vectors in V) of all m-variable polynomial functions (reduced modulo $x_i^q - x_i$) of degree at most ρ. Thus*

$$\mathcal{R}_{\mathbb{F}_q}(\rho, m) = \langle x_1^{i_1} x_2^{i_2} \cdots x_m^{i_m} \mid 0 \leq i_k \leq q-1, \textit{ for } 1 \leq k \leq m, \sum_{k=1}^{m} i_k \leq \rho \rangle.$$

These codes are thus codes of length q^m and the codewords are obtained by evaluating the m-variable polynomials in the subspace at all the points of the vector space $V = \mathbb{F}_q^m$.

The code $\mathcal{R}_{\mathbb{F}_p}((m-r)(p-1), m)$ is the p-ary code of the affine geometry design $AG_{m,r}(\mathbb{F}_p)$: see [1, Theorem 5.7.9].

The Reed-Muller codes are the codes $\mathcal{R}_{\mathbb{F}_2}(r, m)$ and are usually written simply as $\mathcal{R}(r, m)$, where $0 \leq r \leq m$. The standard well-known facts concerning $\mathcal{R}(r, m)$ (see, for example, [1, Theorem 5.3.3]), can be summarized as:

Result 1 *For $0 \leq r \leq m$, $\mathcal{R}(r, m)$ is a $[2^m, \binom{m}{0} + \binom{m}{1} + \cdots + \binom{m}{r}, 2^{m-r}]_2$ binary code. Furthermore, $\mathcal{R}(r, m) = C_2(AG_{m,m-r}(\mathbb{F}_2))$ and the minimum-weight vectors are the incidence vectors of the $(m-r)$-flats. The automorphism group of $\mathcal{R}(r, m)$ is the affine group $AGL_m(\mathbb{F}_2)$ for $0 < r < m-1$.*

For permutation decoding, the following is Proposition 1 of [7] stated for generalized Reed-Muller codes:

Result 2 *Let $f_{\nu,m,q}$ denote the dimension and $d_{\nu,m,q}$ the minimum weight of $\mathcal{R}_{\mathbb{F}_q}(\nu, m)$. If $s = \min(\lfloor (q^m - 1)/f_{\nu,m,q} \rfloor, \lfloor (d_{\nu,m,q} - 1)/2 \rfloor)$, then the translation group $T_m(\mathbb{F}_q)$ is an s-PD-set for $\mathcal{R}_{\mathbb{F}_q}(\nu, m)$.*

For the Reed-Muller codes this becomes:

Result 3 *For $0 \le r \le m$, the translation group $T_m(\mathbb{F}_2)$ is an s-PD-set for $\mathcal{R}(r,m)$, for $s = \min(\lfloor (2^m-1)/\rho_{r,m} \rfloor, 2^{m-r-1}-1)$, where $\rho_{r,m} = \binom{m}{0} + \binom{m}{1} + \cdots + \binom{m}{r}$.*

These results hold for any information set for the code. As an illustration of Result 3, Table 1 shows the value of s for which the translation group is an s-PD-set (of size 2^m) for $\mathcal{R}(1,m)$ or $\mathcal{R}(2,m)$, and $4 \le m \le 16$, using any information set.

m	4	5	6	7	8	9	10	11	12	13	14	15	16
$\mathcal{R}(1,m)$	3	5	9	15	28	51	93	170	315	585	1092	2047	3855
$\mathcal{R}(2,m)$	1	1	2	4	6	11	18	30	51	89	154	270	478

Table 1: Translation group as s-PD-set

We will use coding-theoretic terminology and notation for vectors in $V = \mathbb{F}_2^m$; we do not expect that any confusion should arise with the vectors in the code $\mathcal{R}(r,m)$ since we will not need to deal with the latter vectors in our search for PD-sets. Thus, using the standard basis $\{e_1, \ldots, e_m\}$ for $V = \mathbb{F}_2^m$, and writing e_0 for $0 \in V$, for each $v = \sum_{i=1}^m \lambda_i e_i \in V$, let $\mathrm{wt}(v)$ be the weight of v, i.e. the number of non-zero λ_i. The support of $v = \sum_{j=1}^r e_{i_j} \in V$ will be denoted by $\mathrm{Supp}(v) = \{i_1, \ldots, i_r\}$. If $X \subseteq \{1, \ldots, m\}$, then $v(X)$ will denote the vector with support X, and if $X = \{i_1, \ldots, i_r\}$ we will write simply $v(i_1, \ldots, i_r)$, for convenience. (This contrasts with notation v^X for codewords described in Section 2 above.)

Following the notation in [14], for $0 \le i \le m$, let

$$C_i = \{v \mid v \in V,\ \mathrm{wt}(v) = i\}. \tag{1}$$

Let $f = x_{i_1} \ldots x_{i_r}$ be a monomial function of degree r. If $i < r$ and $v \in C_i$ then $f(v) = 0$. Also, if $i = r$, $v \in C_i$ and $v \neq e_{i_1} + \ldots + e_{i_r}$ then $f(v) = 0$. So, it is easily seen that

$$\mathcal{I}_r = C_0 \cup C_1 \cup \ldots \cup C_r \tag{2}$$

is an information set for $\mathcal{R}(r,m)$. (Alternatively, see [7, Corollary 2].)

The translation group $T_m(\mathbb{F}_2)$ acts on $\mathcal{R}(r,m)$ in the following way: for each $u \in V$, denote by T_u the translation of V given by $T_u : v \mapsto v + u$. This mapping acts on $\mathcal{R}(r,m)$ by $f \mapsto f_u = f_\circ T_u$, i.e. $f_u(v) = f(u+v)$ for all $v \in V$.

4 s-PD-sets for $\mathcal{R}(1,m)$

We now look for subsets of the translation group that will be s-PD-sets for $\mathcal{R}(1,m)$ for some s. Using the notation from the previous section, let

$$A_m = \{T_u \mid u \in C_0 \cup C_1 \cup C_2 \cup C_m\}. \tag{3}$$

Then $|A_m| = \binom{m+1}{2} + 2 = \frac{1}{2}(m^2 + m + 4)$. We will use the information set $\mathcal{I} = \mathcal{I}_1$ with check set $\mathcal{C} = V \setminus \mathcal{I}$. We write $e = e_1 + e_2 + \ldots + e_m$ for the all-one vector of $V = \mathbb{F}_2^m$. In [14], the following result is proved.

Result 4 *For $m \geq 5$, A_m is a 4-PD-set of size $\binom{m+1}{2} + 2$ for $\mathcal{R}(1, m)$ with respect to the information set $\mathcal{I}$.*

It is also conjectured in [14] that A_m is a 5-PD-set for $\mathcal{R}(1, m)$. This is true for $m \geq 6$ but not for $m = 5$. There are further results for PD-sets for punctured first-order Reed-Muller codes for small m in [9].

We prove the following:

Proposition 1 *If $m \geq 5$ then A_m is a $(m-1)$-PD-set, but not an m-PD-set, for the $[2^m, m+1, 2^{m-1}]_2$ code $\mathcal{R}(1, m)$ with respect to the information set $\mathcal{I}$.*

Proof: Let $S = \{0, e_1, \ldots, e_{m-3}, e_{m-2} + e_{m-1} + e_m, e\}$. It is immediate that $ST_u = \{u, e_1 + u, \ldots, e_{m-3} + u, e_{m-2} + e_{m-1} + e_m + u, e + u\}$ has an element of weight at most 1 if $u \in C_0 \cup C_1 \cup C_2 \cup C_m$. Hence, $S\theta \not\subseteq \mathcal{C}$ for all $\theta \in A_m$, and so A_m is not an m-PD-set for any m.

Now suppose that S is an $(m-1)$-subset of V. We write $S_i = \{v \mid v \in S,\ \mathrm{wt}(v) = i\} = S \cap C_i$ and $l_i = |S_i|$, $0 \leq i \leq m$. Then $m - 1 = \sum_{i=0}^{m} l_i$. For every choice of S we need to find a translation $T_u \in A_m$ such that $ST_u \subset \mathcal{C}$.

If $l_{m-1} + l_m = 0$, then $ST_e \subseteq \mathcal{C}$. This includes the case $l_1 = m-1$. If $l_{m-1} + l_m = 1$ and $l_1 = m - 2$, then $0 \notin S$ and $C_1 \setminus S_1 = \{e_i, e_j\}$ for some i and j. In this case, $ST_{e_i} \subseteq \mathcal{C}$.

Now, suppose that $l_{m-1} + l_m \geq 1$ and $l_1 \leq m - 3$. Let $n = m - l_1$. Thus, $n \geq 3$. By relabelling the elements of the basis of V, we may suppose that $C_1 \setminus S_1 = \{e_1, \ldots, e_n\}$. Since $m \geq 5$, $m - 1 \geq l_0 + l_1 + l_2 + l_3 + l_{m-1} + l_m \geq m - n + 1 + l_0 + l_2 + l_3$. Hence, $l_2 + l_3 \leq n - 2 - l_0$. Note that $l_0 = 0$ or 1.

Let $[1, n] = \{1, \ldots, n\}$. For $i, j \in [1, n]$ with $i < j$, we define: (i) $a_{i,j}$ to be 1 if $e_i + e_j \in S$ and 0 otherwise; (ii) $b_{i,j}$ to be the number of k with $1 \leq k \leq n$ and $\{i, j, k\}$ a 3-set for which $e_i + e_j + e_k \in S$; (iii) $c_{i,j}$ to be the number of k with $k > n$ and $\{i, j, k\}$ a 3-set for which $e_i + e_j + e_k \in S$. The sum $l_2^* = \sum_{1 \leq i < j \leq n} a_{i,j}$ counts the number of elements in S_2 of the form $e_i + e_j$ with $1 \leq i, j \leq n$. The sum $l_3^{**} = \frac{1}{3} \sum_{1 \leq i < j \leq n} b_{i,j}$ counts the number of elements in S_3 of the form $e_i + e_j + e_k$ with $1 \leq i, j, k \leq n$. The sum $\sum_{1 \leq i < j \leq n} c_{i,j}$ counts the number of elements in S_3 of the form $e_i + e_j + e_k$ with exactly two of the indices i, j, k in $[1, n]$. Hence, $l_3^* = \sum_{1 \leq i < j \leq n} \left(\frac{1}{3} b_{i,j} + c_{i,j}\right)$ counts the number of elements in S_3 of the form $e_i + e_j + e_k$ with $|\{i, j, k\} \cap [1, n]| \geq 2$.

Hence, writing $f_{i,j} = a_{i,j} + \frac{1}{3} b_{i,j} + c_{i,j}$, we get

$$\sum_{1 \leq i < j \leq n} f_{i,j} = l_2^* + l_3^* \leq l_2 + l_3 \leq n - 2 - l_0 \tag{4}$$

Suppose that $f_{i,j} > 0$ for all 2-sets i, j with $1 \leq i < j \leq n$. Then, the left hand side of equation (4) is at least $\frac{1}{3}\binom{n}{2}$. Moreover, $\frac{1}{3}\binom{n}{2} - (n - 2) = \frac{1}{3}\binom{n-3}{2} \geq 0$ for $n \geq 3$. Hence, the inequalities in (4) are equalities, $l_0 = 0$ and $n = 3$ or 4. Also, for every pair $\{i, j\}$ in $[1, n]$, either $e_i + e_j \in S_2$ or $e_i + e_j + e_k \in S_3$ for some k different from i and j.

If $n = 3$, then $l_2^* + l_3^* = l_2 + l_3 = 1$. Hence, $l_2^* = 0$, $l_3^{**} = 1$, $S_2 = \emptyset$ and $S_3 = \{e_1 + e_2 + e_3\}$. But then $ST_{e_3} \subseteq \mathcal{C}$.

If $n = 4$, then $l_2 + l_3 = 2$. By the condition $f_{i,j} > 0$ for every pair i, j in $[1, 4]$, all six pairs must occur in the support of vectors of weight 2 or 3. However, since at most five pairs can occur in two vectors of weight 2 or 3, this case cannot occur.

Otherwise, we can find $i, j \in [1, n]$ with $i < j$ and $f_{i,j} = 0$. Hence, $a_{i,j} = b_{i,j} = c_{i,j} = 0$. Let $u = e_i + e_j$. Then neither u nor any $u + e_l$, with $1 \le l \le m$, $l \ne i, j$, is in S. So, if $v \in S_2 \cup S_3$ we get $\mathrm{wt}(v + u) \ge 2$ by the choice of u. If $v \in S_i$ with $i \ge 4$, $\mathrm{wt}(v + u) \ge i - 2 \ge 2$. If $v \in S_1$, we have $v = e_k$ with $k > n$ and consequently $\mathrm{wt}(v + u) = 3$. Finally, $\mathrm{wt}(0 + u) = 2$. Hence, $ST_u \subseteq \mathcal{C}$. ■

We now improve on this, but we need to increase the set of translations. Thus let

$$B_m = \{T_u \mid u \in C_0 \cup C_1 \cup C_2 \cup C_3 \cup C_m\}. \tag{5}$$

Then $|B_m| = 2 + m + \binom{m}{2} + \binom{m}{3} = \frac{1}{6}(m^3 + 5m + 12)$.

Proposition 2 *If $m \ge 6$ then B_m is an $(m+1)$-PD-set for the $[2^m, m+1, 2^{m-1}]_2$ code $\mathcal{R}(1, m)$ with respect to the information set $\mathcal{I}$.*

Proof: Use the notation of Proposition 1. The check set $\mathcal{C}$ corresponding to $\mathcal{I}$ consists of all vectors of weight at least 2. Here S is an $(m+1)$-subset of V, and $m+1 = \sum_{i=0}^{m} l_i$. We need to show that for every choice of S, there is a translation $T_u \in B_m$ such that $ST_u \subset \mathcal{C}$. As before, $S_i = S \cap C_i$ for $0 \le i \le m$.

If $l_{m-1} + l_m = 0$, then $ST_e \subseteq \mathcal{C}$. So suppose $l_{m-1} + l_m \ge 1$. If $l_1 = m$ and $S \setminus C_1 = \{u\}$ where $\mathrm{wt}(u) \ge m - 1$, then $T_{e_1+e_2+e_3}$ will work, since $m \ge 6$. If $l_1 = m - 1$ and $C_1 \setminus S_1 = \{e_i\}$ then T_{e_i} will work unless the remaining element in S is 0 or $e_i + e_j$, for some $j \ne i$. In either case $T_{e_i+e_k+e_l}$, where $k, l \ne j$, will do.

Thus we take $l_1 \le m - 2$. As in the proof of Proposition 1, let $n = m - l_1$ where $n \ge 2$. Since $m \ge 6$, $m + 1 \ge l_0 + l_1 + l_2 + l_3 + l_{m-1} + l_m \ge m - n + 1 + l_0 + l_2 + l_3$. Hence, $l_2 + l_3 \le n - l_0$ where $l_0 = 0$ or 1.

By relabelling the elements of the basis for V, we may suppose that $C_1 \setminus S_1 = \{e_1, \ldots, e_n\}$. We continue with the notation introduced in the proof of Proposition 1. We can write $S = \{0, e_{n+1}, \ldots, e_m, u_1, \ldots, u_n\}$ or $S = \{e_{n+1}, \ldots, e_m, u_1, \ldots, u_n, u_{n+1}\}$, according as $l_0 = 1$ or 0, where the first $l_2^* + l_3^*$ of the u_i's are the elements of $S_2 \cup S_3$ meeting $[1, n]$ in at least two points, the next $l_2 + l_3 - l_2^* - l_3^*$ of the u_i's are the remaining elements of $S_2 \cup S_3$, and the remaining u_i's, of which there is at least one, have weight at least 4. Also, $\mathrm{wt}(u_n) \ge m - 1 \ge 5$ or $\mathrm{wt}(u_{n+1}) \ge m - 1 \ge 5$ according as $l_0 = 1$ or 0.

Arguing as in the proof of Proposition 1, if $f_{i,j} > 0$ for all pairs $i, j \in [1, n]$, then $\frac{1}{3}\binom{n}{2} \le n - 1$ if $l_0 = 1$, and $\frac{1}{3}\binom{n}{2} \le n$ if $l_0 = 0$. We deal with these two cases separately. Note that $f_{i,j} > 0$ implies that $l_2 + l_3 \ge l_2^* + l_3^* > 0$.

1. $l_0 = 1$. Then $\frac{1}{3}\binom{n}{2} \le l_2^* + l_3^* \le l_2 + l_3 \le n - 1$. In particular, $2 \le n \le 6$.

   The number $l_2^* + l_3^*$ of 2-sets and 3-sets in $[1, n]$ needed to contain all 2-sets is at least $n - 1$ for $n = 2$ or $4 \le n \le 5$, at least 1 if $n = 3$ and at least 6 for $n = 6$. Hence, the case $n = 6$ cannot occur and, for $n = 2$, 4 and 5, $l_2^* = l_2$, $l_3^* = l_3$. Moreover, for $n = 4$ and 5, $l_3^{**} \ge n - 2$.

For $n = 2$, 4 and 5, at most one of the elements $u_1, \ldots, u_{n-1}$ has a support meeting $[1, n]$ in 2 points. Hence, $T_{v(1,n+1,m)}$ will map S into $\mathcal{C}$ unless $n = 5$ and $m = 6$. In this case, each of u_1, u_2, u_3 and u_4 must have weight 3 and their supports must lie in $[1, 5]$. Hence, $T_{v(1,2,6)}$ will map S into $\mathcal{C}$.

If $n = 3$, then we have $u_1 = e_1 + e_2 + e_3$. If possible, choose $i \in [1, 3]\backslash\mathrm{Supp}(u_2)$ and let $v = v(i, 4, 5)$. This will certainly be the case if $\mathrm{wt}(u_2) \leq 3$. If $\mathrm{wt}(u_2) = 4$ and $[1, 3] \subseteq \mathrm{Supp}(u_2)$, let $v = v(1, j, k)$ with $j, k \in [4, m]\backslash\mathrm{Supp}(u_2)$ and $j \neq k$. If $\mathrm{wt}(u_2) \geq 5$, let $v = v(1, 4, 5)$. In all cases, T_v will map S into $\mathcal{C}$.

2. $l_0 = 0$. Then $\frac{1}{3}\binom{n}{2} \leq l_2^* + l_3^* \leq l_2 + l_3 \leq n$. In particular, $2 \leq n \leq 7$. Also, if there is an $i \in [1, n]$ which is not in the support of any u_j of weight 2 then T_{e_i} will map S into $\mathcal{C}$. So, we may suppose that every $i \in [1, n]$ is in the support of some u_j of weight 2. We will refer to this as assumption (*).

   As for the case $l_0 = 1$, we see that $l_2^* + l_3^* \geq 1$, 1, 3, 4 or 6 according as $n = 2$, 3, 4, 5 or 6. Moreover, $l_3^{**} \geq 2$, 3 or 6 according as $n = 4$, 5 or 6. Additionally, when $n = 7$ we see that $l_2^* + l_3^* \geq 7$ and $l_3^{**} \geq 7$.

   (i) $n = 2$. If $|\mathrm{Supp}(u_1) \cup \mathrm{Supp}(u_2)| \leq m - 2$, let $v = v(i, j, k)$ where $j, k \notin \mathrm{Supp}(u_1) \cup \mathrm{Supp}(u_2)$ and $i \neq j$ and k. Otherwise, $|\mathrm{Supp}(u_1) \cup \mathrm{Supp}(u_2)| \geq m - 1 \geq 5$. Hence, $\mathrm{wt}(u_1)$ and $\mathrm{wt}(u_2)$ are not both 2. By assumption (*), $u_1 = e_1 + e_2$.

   If possible, choose $i \in \mathrm{Supp}(u_1)\backslash\mathrm{Supp}(u_2)$ and $j, k \in \mathrm{Supp}(u_2)\backslash\mathrm{Supp}(u_1)$ with $j \neq k$, and let $v = v(i, j, k)$. If this is not possible, then $\mathrm{Supp}(u_1) \subset \mathrm{Supp}(u_2)$ and $|\mathrm{Supp}(u_2)| \geq m - 1 \geq 5$. We can then choose distinct $i, j, k \in \mathrm{Supp}(u_2)\backslash\mathrm{Supp}(u_1)$ and let $v = v(i, j, k)$.

   In all cases, T_v maps S into $\mathcal{C}$.

   (ii) $n = 3$. Suppose first that $e_1 + e_2 + e_3 = u_1 \in S$. By assumption (*), $\mathrm{wt}(u_i) = 2$ and $\mathrm{Supp}(u_i) \subseteq [1, 3] \cup \{j\}$ for some $j \in [4, m]$ and for $i = 2$ and 3. Let $v = v(1, k, l)$, where $k, l \in [4, m]\backslash\{j\}$ and $k \neq l$.

   If $e_1 + e_2 + e_3 \notin S$ then $l_2^* + l_3^* = 3$ and $u_1 = e_1 + e_2 + \delta_1 e_j$, $u_2 = e_2 + e_3 + \delta_2 e_k$ and $u_3 = e_1 + e_3 + \delta_3 e_l$, where $\delta_i \in \{0, 1\}$ for $i \in [1, 3]$ and $j, k, l \in [4, m]$ but not necessarily distinct. Let $v = v(4, 5, 6)$.

   In all cases, T_v maps S into $\mathcal{C}$.

   (iii) $n = 4$ or 5. We may now assume that $\mathrm{wt}(u_1) = 2$.

   At most two of the u_i, $1 \leq i \leq n$, have supports meeting $[1, n]$ in sets of size at most 2. By (*), we must have $n = 4$, $\mathrm{wt}(u_2) = 2$ and $\mathrm{Supp}(u_1) \cup \mathrm{Supp}(u_2) = [1, 4]$. Then $l_2^* + l_3^* = l_2 + l_3 = 4$ and $\mathrm{wt}(u_i) = 3$ and $\mathrm{Supp}(u_i) \subseteq [1, 4]$ for $i = 3$ and 4. Let $v = v(1, 4, 5)$. Then T_v maps S into $\mathcal{C}$.

   (iv) $n = 6$ or 7. Here $l_2^* + l_3^* = n$ and all n elements of $S_2 \cup S_3$ have weight 3. This is excluded by assumption (*).

Thus there is a pair i, j for which $f_{i,j} = 0$ and we can complete the proof as in Proposition 1. ■

5 s-PD-sets for $\mathcal{R}(2, m)$

We now adapt the method of proof of Propositions 1 and 2 to establish the following proposition for $\mathcal{R}(2, m)$. Here the information set is $\mathcal{I} = \mathcal{I}_2$ and the check set is $\mathcal{C} = V \setminus \mathcal{I}$; the latter consists of all vectors of weight at least 3. Other notation is as in Section 4.

Proposition 3 *If $m \geq 8$ then B_m is an $(m-3)$-PD-set for the $[2^m, 1+m+\binom{m}{2}, 2^{m-2}]_2$ code $\mathcal{R}(2, m)$ with respect to the information set $\mathcal{I}_2$.*

Proof: We first observe that B_m is not an $(m-2)$-PD-set, since the $(m-2)$-set $S = \{e_1 + e_2 + e_3 + e_4, e_5, \ldots, e_m, e\}$ is not mapped into $\mathcal{C}$ by translation with any element of B_m.

Now let S be a set of size $(m-3)$ in V. As before, $S_i = S \cap C_i$ and $l_i = |S_i|$, for $0 \leq i \leq m$. Thus $m - 3 = \sum_{i=0}^{m} l_i$. We let $n = m - l_1$ and arrange the notation so that $C_1 \backslash S_1 = \{e_1, \ldots, e_n\}$. We have to show that there is an element $v \in B_m$ so that $ST_v \subseteq \mathcal{C}$.

If $l_{m-2} + l_{m-1} + l_m = 0$, then we may take $v = e$. For the rest of the proof, we assume that $l_{m-2} + l_{m-1} + l_m \geq 1$. If $l_1 = m - 4$, then $l_0 = 0$ and we may take $v = e_1 + e_2$. Thus, we may assume that $l_1 \leq m - 5$, that is, $n \geq 5$. Since $m \geq 8$, $m - 3 \geq l_0 + l_1 + l_2 + l_3 + l_4 + l_5 + l_{m-2} + l_{m-1} + l_m \geq m - n + 1 + l_0 + l_2 + l_3 + l_4 + l_5$. Hence, $l_2 + l_3 + l_4 + l_5 \leq n - 4 - l_0$.

We now define a collection of functions defined on the triples $\{i, j, k\}$ of $[1, n]$. To simplify notation we will suppose that $1 \leq i < j < k \leq n$. Then (i) $a_{i,j,k}$ is the number of pairs $\{i', j'\}$ with $v(i', j') \in S_2$ and $i', j' \in \{i, j, k\}$; (ii) $b^{(p)}_{i,j,k}$ is the number of triples $\{i', j', k'\} \subseteq [1, m]$ with $v(i', j', k') \in S_3$ and $|\{i', j', k'\} \cap \{i, j, k\}| = p = |\{i', j', k'\} \cap [1, n]|$, for $p = 2$ and 3; (iii) $c^{(p)}_{i,j,k}$ is the number of quadruples $\{i', j', k', l'\} \subseteq [1, m]$ with $v(i', j', k', l') \in S_4$, $\{i, j, k\} \subseteq \{i', j', k', l'\}$ and $|\{i', j', k', l'\} \cap [1, n]| = p$, for $p = 3$ or 4; (iv) $d^{(p)}_{i,j,k}$ is the number of quintuples $\{i', j', k', l', m'\} \subseteq [1, m]$ with $v(i', j', k', l', m') \in S_5$, $\{i, j, k\} \subseteq \{i', j', k', l', m'\}$ and $|\{i', j', k', l', m'\} \cap [1, n]| = p$, for $p = 3$, 4 or 5.

If l'_2 is the number of pairs $\{i', j'\} \subseteq [1, n]$ with $v(i', j') \in S_2$, then $\sum_{1 \leq i<j<k \leq n} a_{i,j,k} = l'_2(n-2)$.

Clearly, $\sum_{1 \leq i<j<k \leq n} b^{(3)}_{i,j,k}$ is the number l'_3 of elements of S_3 with support in $[1, n]$. If l''_3 denotes the number of elements of S_3 whose support meets $[1, n]$ in a set of size 2, then $\sum_{1 \leq i<j<k \leq n} b^{(2)}_{i,j,k} = l''_3(n-2)$.

If l'_4 and l''_4 denote the numbers of elements of S_4 whose support meets $[1, n]$ in sets of size 3 and 4, respectively, then $\sum_{1 \leq i<j<k \leq n} c^{(3)}_{i,j,k} = l'_4$ and $\sum_{1 \leq i<j<k \leq n} c^{(4)}_{i,j,k} = 4l''_4$.

If l'_5, l''_5 and l'''_5 denote the numbers of elements of S_5 whose support meets $[1, n]$ in sets of size 3, 4 and 5, respectively, then $\sum_{1 \leq i<j<k \leq n} d^{(3)}_{i,j,k} = l'_5$, $\sum_{1 \leq i<j<k \leq n} d^{(4)}_{i,j,k} = 4l''_5$. and $\sum_{1 \leq i<j<k \leq n} d^{(5)}_{i,j,k} = 10l'''_5$.

For each triple i, j, k with $1 \leq i < j < k \leq n$, define

$$f_{i,j,k} = \tfrac{1}{n-2} a_{i,j,k} + \tfrac{1}{n-2} b^{(2)}_{i,j,k} + b^{(3)}_{i,j,k} + c^{(3)}_{i,j,k} + \tfrac{1}{4} c^{(4)}_{i,j,k} + d^{(3)}_{i,j,k} + \tfrac{1}{4} d^{(4)}_{i,j,k} + \tfrac{1}{10} d^{(5)}_{i,j,k}.$$

Since $l'_2 \leq l_2$, $l'_3 + l''_3 \leq l_3$, $l'_4 + l''_4 \leq l_4$ and $l'_5 + l''_5 + l'''_5 \leq l_5$,

$$\sum_{1 \leq i < j < k \leq n} f_{i,j,k} \leq l_2 + l_3 + l_4 + l_5 \leq n - 4 - l_0 \tag{6}$$

We will show that there is a triple i, j, k with $1 \leq i < j < k \leq n$ such that $f_{i,j,k} = 0$, or find an element $v \in B_m$ with $ST_v \in \mathcal{C}$. Suppose that $f_{i,j,k} > 0$ for all triples i, j, k with $1 \leq i < j < k \leq n$. Then, the left hand side of equation (6) is at least $\frac{1}{10}\binom{n}{3}$ if $n < 12$ and at least $\frac{1}{n-2}\binom{n}{3}$ if $n \geq 12$. Since $\frac{1}{n-2}\binom{n}{3} = \frac{n(n-1)}{6} > n - 4$ if $n \geq 12$, we must have $n < 12$. Also, $\frac{1}{10}\binom{n}{3} > n - 4$ if $7 \leq n \leq 11$. So we must have $n = 5$ or 6.

If $n = 5$ or 6, $\frac{1}{10}\binom{n}{3} = n - 4$ so that $l_0 = 0$ and all terms in the definition of $f_{i,j,k}$ are 0 with the exception of $\frac{1}{10} d^{(5)}_{i,j,k}$ which is $\frac{1}{10}$. Then $d^{(5)}_{i,j,k} = 1$ for every triple i, j, k in $[1, n]$ implies that $l_5 \geq 1$ if $n = 5$ and $l_5 \geq 4$ if $n = 6$, since every triple in $[1, n]$ is in the support of an element of S_5. The latter is impossible since $l_5 \leq n - 4 - l_0 = 2$. When $n = 5$, for each triple i, j, k with $1 \leq i < j < k \leq n$, $a_{i,j,k} = 0$, $b^{(p)}_{i,j,k} = 0$ if $p = 2$ and 3, and $c^{(p)}_{i,j,k} = 0$ if $p = 3$ and 4. Thus no element of S_2 has support in $[1, n]$, no element of S_3 has a support meeting $[1, n]$ in more than one point and no element of S_4 has a support meeting $[1, n]$ in more than two points. Since $l_4 \leq n - 4 - l_5$ we have $l_4 = 0$. We may choose $v = v(1, 2)$ and then $ST_v \in \mathcal{C}$.

It remains to deal with those cases in which there is a triple i, j, k with $1 \leq i < j < k \leq n$ such that $f_{i,j,k} = 0$. For such a triple, (i) it contains the support of no element of S_2, (ii) it does not meet the support of any element of S_3 in more than one point, and (iii) it does not meet the support of any element of $S_4 \cup S_5$ in more than two points. Hence, if we set $v = v(i, j, k)$ then $ST_v \in \mathcal{C}$. This completes the proof. ■

Note: We cannot take $m = 7$ in Proposition 3 since the set $S = \{0, e_1, e_2, e_3 + e_4 + e_5 + e_6 + e_7\}$ cannot be moved into $\mathcal{C}$ by B_7.

Acknowledgement

J. D. Key thanks the Institute of Mathematics and Physics at Aberystwyth University for their hospitality.

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] E. F. Assmus, Jr and J. D. Key. Polynomial codes and finite geometries. In V. S. Pless and W. C. Huffman, editors, *Handbook of Coding Theory*, pages 1269–1343. Amsterdam: Elsevier, 1998. Volume 2, Part 2, Chapter 16.

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

[4] W. Cary Huffman. Codes and groups. In V. S. Pless and W. C. Huffman, editors, *Handbook of Coding Theory*, pages 1345–1440. Amsterdam: Elsevier, 1998. Volume 2, Part 2, Chapter 17.

[5] J. D. Key. Recent developments in permutation decoding. *Notices of the South African Mathematical Society*, 37:2–13, 2006. No. 1, April.

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

[7] J. D. Key, T. P. McDonough, and V. C. Mavron. Information sets and partial permutation decoding for codes from finite geometries. *Finite Fields Appl.*, 12:232–247, 2006.

[8] Hans-Joachim Kroll and Rita Vincenti. PD-sets related to the codes of some classical varieties. *Discrete Math.*, 301:89–105, 2005.

[9] Hans-Joachim Kroll and Rita Vincenti. 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.*, 308:408–414, 2008.

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

[11] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes.* Amsterdam: North-Holland, 1983.

[12] E. Prange. The use of information sets in decoding cyclic codes. *IRE Trans.*, IT-8:5–9, 1962.

[13] J. Schönheim. On coverings. *Pacific J. Math.*, 14:1405–1411, 1964.

[14] P. Seneviratne. Partial permutation decoding for the first-order Reed-Muller codes. *Discrete Math.*, 309:1967–1970, 2009.