Improved partial permutation decoding for Reed-Muller codes

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

November 28, 2016

Abstract

It is shown that for $n \geq 5$ and $r \leq \frac{n-1}{2}$, if an $(n, M, 2r+1)$ binary code exists, then the r^{th}-order Reed-Muller code $\mathcal{R}(r, n)$ has s-PD-sets of the minimum size $s+1$ for $1 \leq s \leq M-1$, and these PD-sets correspond to translations of the vector space $\mathbb{F}_2^n$. In addition, for the first order Reed-Muller code $\mathcal{R}(1, n)$, s-PD-sets of size $s+1$ are constructed for s up to the bound $\lfloor \frac{2^n}{n+1} \rfloor - 1$. The results apply also to generalized Reed-Muller codes.

Keywords: Reed-Muller codes; permutation decoding
Mathematics Subject Classifications: 05C45, 05B05, 94B05

1 Introduction

In [15] it was shown that partial permutation decoding can be used for the first and second order Reed-Muller codes $\mathcal{R}(1, n)$ and $\mathcal{R}(2, n)$, which are $[2^n, n+1, 2^{n-1}]_2$ and $[2^n, 1+n+\binom{n}{2}, 2^{n-2}]_2$ codes, respectively, by obtaining s-PD-sets for $s = n-1, n+1, n-3$ (see Result 3 in Section 4). These sets were quite large, and consisted of special collections of translations of $\mathbb{F}_2^n$. Since the efficiency of permutation decoding is highest if the PD-set is small, the smallest possible such set to correct a specific number of errors is sought; to correct s errors, the smallest size of a set is $s+1$ according to the Gordon-Schönheim bound [10, 20]. Here we show that a set of translations of size M will provide an $(M-1)$-PD-set for $\mathcal{R}(r, n)$, for $1 \leq r \leq \frac{n-1}{2}$, provided that an $(n, M, 2r+1)$ binary code exists.

In addition, we use a construction due to [3] for $\mathcal{R}(1, n)$, which is an extension of a construction in [8] for simplex codes, to describe s-PD-sets of the minimum size $s+1$ for all s such that $1 \leq s \leq \lfloor \frac{2^n}{n+1} \rfloor - 1$. The upper bound here is greater than the size M of the code used for the construction using translations mentioned above, except in the case when $n = 2^m - 1$.

Since there are many constructions of $(n, M, 2r+1)$ binary codes for $r \geq 1$, for all n the method of Theorem 1 below, with translations of $\mathbb{F}_2^n$, will provide partial permutation decoding for large values of s and using the most efficient size decoding set, i.e. of size $s+1$. Note that the maximum number of errors that $\mathcal{R}(r, n)$ can correct is $2^{n-r-1} - 1$. The

maximum value of s for which an s-PD-set of size $s+1$ for $\mathcal{R}(r,n)$ can exist is $F_{n,r} = \lfloor \frac{2^n}{d} \rfloor - 1$, where $d = \sum_{i=0}^{r} \binom{n}{i}$, (i.e. $\dim(\mathcal{R}(r,n))$), as is shown in Lemma 1, Section 2.

The main theorem is:

Theorem 1. *For $n \geq 5$, $1 \leq r \leq \frac{n-1}{2}$, let C be an $(n, M, 2r+1)$ binary code. For each $c \in C$, let T_c denote the translation of $V = \mathbb{F}_2^n$ by c. Then $P_C = \{T_c \mid c \in C\}$ is an $(M-1)$-PD-set of size M for $\mathcal{R}(r,n)$ using the information set $\mathcal{I}_{n,r}$ defined in Equation (2).*

For $\mathcal{R}(1,n)$, s-PD-sets of size $s+1$ exist for $1 \leq s \leq \lfloor \frac{2^n}{n+1} \rfloor - 1$.

Note: 1. The results of the theorem easily extend to generalized Reed-Muller codes, $\mathcal{R}_{\mathbb{F}_q}(\rho, n)$: see Section 7.

2. The special construction for $\mathcal{R}(1,n)$ was posted at arXiv.org (see full reference in the footnote at the end of Section 5) while this paper was under review. The construction in that posting is virtually identical to the one in this paper.

In order to correct as many errors as possible using this method, we would like M to be as large as possible. The number $A_2(n,d)$ is defined to be the largest value of M for which there exists a binary (n, M, d) code. Tables of values and/or bounds for $A_2(n,d)$ can be found in most coding theory text books, and for values of n up to 27 and $3 \leq d \leq 15$ at `http://www.win.tue.nl/~aeb/codes/binary-1.html` ([5]). For our theorem, the sphere-packing bound gives an upper bound for $A_2(n, 2r+1)$ of $\lfloor 2^n / (\sum_{i=0}^{r} \binom{n}{r}) \rfloor$. Linear (n, M, d) binary codes, for $d \geq 1$ odd, are obtained for all suitably large n in [6]. For $\mathcal{R}(1,n)$ we construct these s-PD-sets of size $s+1$ for s up to the maximum value for which s-PD-sets of size $s+1$ can exist, *viz.* $F_n = \lfloor \frac{2^n}{n+1} \rfloor - 1$.

After describing general background concepts and terminology in Section 2, and information on the Reed-Muller codes in Section 3, we prove the first part of Theorem 1 in Section 4 as Proposition 1. The construction of the s-PD-sets of size $s+1$ for $1 \leq s \leq \lfloor \frac{2^n}{n+1} \rfloor - 1$ for $\mathcal{R}(1,n)$ is given as Corollary 4 in Section 5. Any computations were done with Magma [7, 4] or GAP [9], and a link to a Magma program to obtain some of these sets and to test their error correction ability is given in Section 6. The extension to generalized Reed-Muller codes is briefly outlined in Section 7.

2 Background and terminology

The notation for codes is standard and can be found in [1]. For **linear codes** 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 **distance**, $d(u,v)$, between two vectors u, v is $\mathrm{wt}(u-v)$, i.e. the number of coordinate places in which they differ. The minimum distance of a code is the smallest distance between distinct codewords. For a code, not necessarily linear, of length n containing M codewords, of minimum distance d, we write (n, M, d). A **generator matrix** for an $[n, k, d]_q$ code C 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. $C^\perp = \{v \in \mathbb{F}_q^n \mid (v, c) = 0 \text{ for all } c \in C\}$. A **check matrix** for C is a generator matrix for $C^\perp$. The **all-one vector** is denoted by $\boldsymbol{j}$.

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. Our codes here are all binary, i.e. over $\mathbb{F}_2$, so multiplication by field elements need not be taken into consideration, and equivalent codes will be said to be **isomorphic**. An **automorphism** of a code C is an isomorphism from C to C, and the set of all these gives the automorphism group of the code, written $\mathrm{Aut}(C)$. 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 coordinate positions in the standard form is called an **information set** for the code, and the set of the last $n-k$ coordinate positions is the corresponding **check set**.

Permutation decoding was developed by MacWilliams [17] and Prange [19] and involves finding a set of automorphisms of a code called a PD-set. The method is described fully in MacWilliams and Sloane [18, Chapter 16, p. 513] and Huffman [12, Section 8]. In [13] and [16] 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 $S = \{t_1, \ldots, t_r\}$ be the PD-set. Writing yt_i for the image of y under the automorphism t_i, compute the syndromes $H(yt_i)^T$ for $i = 1, \ldots, r$ 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 yt_i and decode y as ct_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 [10], from a formula due to Schönheim [20], and quoted and proved in [12]:

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

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

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

The following lemma is a generalization of specific results from [8, 3].

Lemma 1. *If C is a t-error-correcting $[n,k,d]_q$ code, $1 \leq s \leq t$, and S is an s-PD-set of size $G(s)$ then $G(s) \geq s+1$. If $G(s) = s+1$ then $s \leq \lfloor \frac{n}{k} \rfloor - 1$.*

Proof: Since $n-m+1 \geq n-k-m+1$ for each $1 \leq m \leq s$, the innermost term is at least 2 and each term must increase by at least 1, and thus $G(s) \geq s+1$. If $G(s) = s+1$ then each term increases by exactly 1, and the innermost term is exactly 2, so we have $\left\lceil \frac{n-s+1}{n-k-s+1} \right\rceil = 2$, i.e. $s \leq n-2k+1$ for the innermost term. So $\left\lceil 2(\frac{n-s+2}{n-k-s+2}) \right\rceil = 2 + \left\lceil \frac{2k}{n-k-s+2} \right\rceil = 3$ for the next inner term, and thus $s \leq n-3k+2$. Continuing like this gives $s \leq n-(m+1)k+m$ for the m^{th} inner term, and finally $s \leq n-(s+1)k+s$ for the s^{th} and final term, and thus $s \leq \lfloor \frac{n}{k} \rfloor - 1$. ■

A simple argument yields that the worst-case time complexity for the decoding algorithm using an s-PD-set of size m on a code of length n and dimension k is $\mathcal{O}(nkm)$. This is best done using the nested PD-sets, since the assumption on the channel is that correct data is more likely to arrive than incorrect. Thus for the correction of s errors, the smaller the size of the s-PD-set the better, and $s+1$ is the best one can do, as shown above. Clearly our new sets to correct the same number of errors as were corrected by the sets in our earlier paper [15] are smaller and thus the complexity is lower.

We aim to find s-PD-sets of size $s+1$ as far as the upper bound $\lfloor \frac{n}{k} \rfloor - 1$, if possible. Note that the choice of information set is important.

3 Reed-Muller codes

We use the notation of [1, Chapter 5] or [2] for Reed-Muller codes; see also [18, Chapter 13]. Let V be the vector space $\mathbb{F}_2^n$ of n-tuples, with standard basis. The codes will be binary codes with ambient space the function space $\mathbb{F}_2^V$, with the usual basis of characteristic functions of the vectors of V. Since the characteristic function of a vector $(a_1, ..., a_n)$ has the same values as the polynomial product $\prod_{i=1}^{n} x_i^{a_i}(1+x_i)^{1-a_i}$ in the commuting indeterminates $x_1, ..., x_n$, where the a_i are interpreted as integers when being used as exponents, the elements of $\mathbb{F}_2^V$ may be considered as polynomials and may be reduced modulo the ideal generated by $x_i^2 - x_i$, $1 \leq i \leq n$, as $a^2 = a$ for every $a \in \mathbb{F}_2$. Furthermore, every polynomial can be written uniquely as a linear combination of the 2^n monomial functions

$$\mathcal{M} = \{x_1^{i_1} x_2^{i_2} \dots x_n^{i_n} \mid 0 \leq i_k \leq 1, \text{ for } 1 \leq k \leq n\}.$$

For any such monomial the degree r is the total degree, i.e. $r = \sum_{k=1}^{n} i_k$ and clearly $0 \leq r \leq n$.

The **Reed-Muller** codes can be defined as follows (see [1, Definition 5.2.1]):

Definition 2. *Let $V = \mathbb{F}_2^n$ be the vector space of n-tuples, for $n \geq 1$, over $\mathbb{F}_2$. For any r such that $0 \leq r \leq n$, the* ***r^{th}*-order Reed-Muller code** *$\mathcal{R}(r,n)$ is the subspace of*

$\mathbb{F}_2^V$ *(with basis the characteristic functions of vectors in* V*) of all* n*-variable polynomial functions (reduced modulo* $x_i^2 - x_i$*) of degree at most* r*. Thus*

$$\mathcal{R}(r,n) = \langle x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n} \mid 0 \le i_k \le 1, \text{ for } 1 \le k \le n, \sum_{k=1}^{n} i_k \le r \rangle.$$

These codes are thus codes of length 2^n and the codewords are obtained by evaluating the n-variable polynomials in the subspace at all the points of the vector space $V = \mathbb{F}_2^n$.

The code $\mathcal{R}(n-r,n)$ is the binary code of the affine geometry design $AG_{n,r}(\mathbb{F}_2)$ of points (vectors) and r-flats in $\mathbb{F}_2^n$, i.e. the row span over $\mathbb{F}_2$ of an incidence matrix of points against r-flats of this geometry, denoted by $C_2(AG_{n,r}(\mathbb{F}_2))$: see [1, Theorem 5.7.9].

The standard well-known facts concerning $\mathcal{R}(r,n)$ (see, for example, [1, Theorem 5.3.3]), can be summarized as:

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

With $V = \mathbb{F}_2^n$ and $C_i = \{v \in V \mid \mathrm{wt}(v) = i\}$, it is easily seen (see [15]) that, for all $n \ge 0$, and $0 \le r \le n$,

$$\mathcal{I}_{n,r} = \bigcup_{i=0}^{r} C_i = \{v \in V \mid 0 \le \mathrm{wt}(v) \le r\} = \{\nu_i \mid 1 \le i \le 1 + \binom{n}{1} + \ldots \binom{n}{r}\} \qquad (2)$$

is an information set for $\mathcal{R}(r,n)$.

In [15] we proved the following:

Result 3. *Let* $V = \mathbb{F}_2^n$ *and let* T_u *denote the translation of* V *by* $u \in V$*,*

$$A_n = \{T_u \mid u \in C_0 \cup C_1 \cup C_2 \cup C_n\},\ B_n = A_n \cup \{T_u \mid u \in C_3\},$$

then

1. A_n *is an* $(n-1)$*-PD-set of size* $\frac{1}{2}(n^2+n+4)$ *for* $\mathcal{R}(1,n)$ *and* $n \ge 5$ *using the information set* $\mathcal{I}_{n,1}$*;*
2. B_n *is an* $(n+1)$*-PD-set of size* $\frac{1}{6}(n^3+5n+12)$ *for* $\mathcal{R}(1,n)$ *and* $n \ge 6$ *using the information set* $\mathcal{I}_{n,1}$*;*
3. B_n *is an* $(n-3)$*-PD-set of size* $\frac{1}{6}(n^3+5n+12)$ *for* $\mathcal{R}(2,n)$ *and* $n \ge 8$ *using the information set* $\mathcal{I}_{n,2}$*.*

The translation group $T_n(\mathbb{F}_2)$ acts on $\mathcal{R}(r,n)$ 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 $\mathcal{R}(r,n)$ 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 of size $s+1$ for $\mathcal{R}(r,n)$

As noted in Section 1, we denote by $A_2(n,d)$ the largest value of M for which there exists a binary (n,M,d) code.

We now prove the first part of Theorem 1:

Proposition 1. *For $n \geq 4$, $1 \leq r \leq \frac{n-1}{2}$, let C be an $(n,M,2r+1)$ binary code. For each $c \in C$, let T_c be the translation defined by c on $V = \mathbb{F}_2^n$. Then $P_C = \{T_c \mid c \in C\}$ is an $(M-1)$-PD-set of size M for $\mathcal{R}(r,n)$ with information set $\mathcal{I}_{n,r}$.*

Proof: We use a pigeon-hole argument: let $\mathcal{T} = \{u_k \mid 1 \leq k \leq M-1\}$ be a set of $M-1$ vectors in the coordinate set that cannot be taken into the check set by any member of P_C. Then for each $c \in C$ there is a $u \in \mathcal{T}$ such that $uT_c \in \mathcal{I}_{n,r}$. Since there are M vectors c and only $M-1$ members of $\mathcal{T}$, there must be a $u \in \mathcal{T}$ which is such that $uT_c \in \mathcal{I}_{n,r}$ and $uT_d \in \mathcal{I}_{n,r}$ where $c \neq d$. Thus $uT_c = \nu_k$, $uT_d = \nu_l$, so $u = \nu_k T_c = \nu_l T_d$, since $T_e^{-1} = T_e$ for all vectors e. Now $\nu_k T_c = \nu_k + c = c + x$, where $\mathrm{wt}(x) \leq r$, i.e. a vector in a sphere of radius r with centre $c \in C$. Since spheres of radius r with centres the codewords $c \in C$ cannot overlap, due to C having minimum distance $2r+1$, we cannot have $\nu_k T_c = \nu_l T_d$ for distinct c and d. Thus we have an $(M-1)$-PD-set. ■

Corollary 2. *For $n \geq 5$, $1 \leq r \leq \frac{n-1}{2}$, $\mathcal{R}(r,n)$ has s-PD-sets of size $s+1$ for $1 \leq s \leq A_2(n,2r+1)-1$. In particular, if $n = 2^m - 1$, $r = 1$, then this holds up to the maximum $s = F_{n,1} = 2^{n-m} - 1$.*

From Lemma 1 we saw that the maximum value of s for which an s-PD-set of size $s+1$ for $\mathcal{R}(r,n)$ can exist is

$$F_{n,r} = \left\lfloor \frac{2^n}{k} \right\rfloor - 1 \text{ where } k = \sum_{i=0}^{r} \binom{n}{i}. \tag{3}$$

For $\mathcal{R}(1,n)$ we write

$$F_n = F_{n,1} = \left\lfloor \frac{2^n}{n+1} \right\rfloor - 1. \tag{4}$$

By the sphere-packing bound, $A_2(n,3) \leq F_n + 1$. From the various values for $A_2(n,3)$ that have been determined, it appears that we only have $A_2(n,3) = F_n + 1$ if $n = 2^m - 1$ for some m, and here we have the perfect Hamming code for C, i.e. $\mathcal{H}_m$ (see [1, Chapter 2]). Thus this method will never give sets all the way up to the upper bound and hence the sets constructed in Section 5 below do not arise from a code of minimum distance 3. The construction there is quite different, and the automorphisms are not translations.

To show that the new results are an improvement over those in Result 3, as an example, according to [5] (and many standard texts on coding theory, for example [11]), for $n = 13$, $A_2(13,3) = 512$, so for $s \leq 511$ the proposition gives s-PD-sets of size $s+1$, and in particular, for $s = n - 1 = 12$, whereas Result 3 gives a set of size 93, and for $s = n + 1 = 14$, the result gives a set of size 379 as opposed to 13 and 15, respectively. Thus our new results are a considerable improvement, as long as the codes $C = (n,M,3)$ can be found.

In [6, Theorem 5] there is given at least one code C of length n and minimum distance 3 for each $n > 6$ whose dimension is $n - 1 - \lfloor \log_2(n) \rfloor$. Thus:

Corollary 3. *For $n \geq 7$, $\mathcal{R}(1, n)$ has s-PD-sets of size $s + 1$ consisting of translations for $1 \leq s \leq 2^d - 1$ where $d = n - 1 - \lfloor \log_2(n) \rfloor$.*

A simple program run on Magma[7, 4] (or GAP [9]) using the greedy codes method of [6] gave the sizes of M for an $(n, M, 2r + 1)$ for $r = 1, 2, 3$: see Table 1.

n	4	5	6	7	8	9	10	11	12	13	14	15	16
$r = 1$	2	4	8	16	16	32	64	128	256	512	1024	2048	2048
$r = 2$		2	2	2	4	4	8	16	16	32	64	128	256
$r = 3$				2	2	2	2	4	4	8	16	32	32

Table 1: Sizes of M for $(n, M, 2r + 1)$ codes constructed for $r = 1, 2, 3$

The website [5] gives values for $A_2(n, 5)$ giving the maximum size of M, and similarly [6, Theorem 5] gives at least one code C of length n and minimum distance 5 for each $n \geq 5$. In fact for $n \geq 10$ this construction give better sets than Result 3.

5 Other s-PD-sets of size $s + 1$ for $\mathcal{R}(1, n)$

We give now a description of the PD-sets for $\mathcal{R}(1, n)$ described in [3]. The method proposed there depends on an earlier idea from [8] for the simplex codes, so we first describe this method.

The q-ary simplex code $\mathcal{S}_n(\mathbb{F}_q)$, for any prime-power 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 $V_n(\mathbb{F}_q)$, i.e. the points of the projective space $PG_{n-1}(\mathbb{F}_q)$: see, for example, [1, Section 2.5]. Thus for $q > 2$ the actual code depends on the representatives chosen, but the codes are of course all equivalent. It follows that $\mathcal{S}_n(\mathbb{F}_q)$ 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 [1, Section 2.5]. The coordinate positions are labelled by the projective points in $PG_{n-1}(\mathbb{F}_q)$. The automorphism group is isomorphic to $\Gamma L_n(q)$, as shown in [12, Section 7], and thus for $q = 2$ it is $GL_n(\mathbb{F}_2)$.

The problem of producing PD-sets of the minimal size was addressed in [8] for the simplex codes $\mathcal{S}_n(\mathbb{F}_q)$ for $n \geq 4$ and all prime powers q. The bound of our Lemma 1 was written in [8] as

$$f_n(\mathbb{F}_q) = \left\lfloor \frac{(q^n - 1)/(q - 1)}{n} \right\rfloor - 1, \tag{5}$$

and we write simply $f_n = f_n(\mathbb{F}_2) = \lfloor \frac{2^n-1}{n} \rfloor - 1$. It was shown that for $1 \leq s \leq f_n(\mathbb{F}_q)$ s-PD-sets of size $s + 1$ can be constructed for $\mathcal{S}_n(\mathbb{F}_q)$, using the information set with columns labelled by the standard basis elements $e_1 \ldots, e_n$ for $V_n(\mathbb{F}_q)$. The construction is outlined in [8, Theorem 1] for the binary case and extends to the q-ary case.

The first order Reed-Muller code $\mathcal{R}(1,n)$ is an extension of the simplex code $\mathcal{S}_n(\mathbb{F}_2)$ and has an $(n+1)\times 2^n$ generator matrix of the form

$$G_n = \begin{bmatrix} 1 & \mathbf{1} \\ \mathbf{0} & S_n \end{bmatrix} \tag{6}$$

where S_n is an $n\times(2^n-1)$ generator matrix of $\mathcal{S}_n(\mathbb{F}_2)$. The coordinate set for $\mathcal{R}(1,n)$ is the set of transposed columns of G_n, i.e. the set of the vectors in $V_{n+1}=\mathbb{F}_2^{n+1}$ of the form $(1,x_1,\ldots,x_n)$, for $x_i\in\mathbb{F}_2$, $1\le i\le n$. The information set is the set $\mathcal{I}_{n+1}$ consisting of $n+1$ vectors from V_{n+1} labelled $w_1,\ldots,w_{n+1}$ where, taking e_i for $i=1,\ldots,n+1$ as the standard basis for V_{n+1}, $w_1=e_1$ and $w_i=e_1+e_i$ for $2\le i\le n+1$, i.e.

$$\mathcal{I}_{n+1}=\{e_1,e_1+e_2,\ldots,e_1+e_{n+1}\}=\{w_i\mid 1\le i\le n+1\}. \tag{7}$$

Matrices in $GL_{n+1}(\mathbb{F}_2)$ will act on the code in the same way as described in [8] if they have the form

$$B=\begin{bmatrix} 1 & b \\ \mathbf{0} & A \end{bmatrix},$$

via $v\mapsto vB$, where v is a row vector corresponding to the column v^T, $b\in\mathbb{F}_2^n$, and $A\in GL_n(\mathbb{F}_2)$. Denote the set of matrices of this form by ML_{n+1}. This is the full automorphism group of $\mathcal{R}(1,n)$ and corresponds to the affine group $AGL_n(\mathbb{F}_2)$ with the action $x\mapsto xA+b$ for $x\in\mathbb{F}_2^n$. If $A=I_n$ these are translations by the vector b.

Define for any matrix $M\in GL_{n+1}(\mathbb{F}_2)$, with rows r_i for $1\le i\le n+1$, the matrix M^* with rows $r_1, r_1+r_2,\ldots,r_1+r_{n+1}$; that is, $M^*=D_{n+1}M$ where $D_{n+1}=\begin{bmatrix} 1 & 0 \\ \jmath^T & I_n \end{bmatrix}$, $\jmath$ is the all-one vector, and $e_iD_{n+1}=w_i$, $1\le i\le n+1$. For $M\in ML_{n+1}$, clearly $M^*\in GL_{n+1}(\mathbb{F}_2)$ and also $M^{**}=M$.

The following result, based on the construction in [8], is announced in [3]; since no proof is given in [3], we give a brief proof here of the sufficiency, which simply follows that in [8] and a pigeon-hole argument:

Result 4. *For $n\ge 4$ a set $P_s=\{M_i\mid 0\le i\le s\}$ of $s+1$ matrices in ML_{n+1} is an s-PD-set for $\mathcal{R}(1,n)$ with information set $\mathcal{I}_{n+1}$ if and only if no two matrices $(M_i^{-1})^*$ and $(M_j^{-1})^*$, where $i\ne j$, $0\le i,j\le s$, have a row in common.*

Proof: Let $\mathcal{T}=\{u_k\mid 1\le k\le s\}$ be a set of s vectors in the coordinate set that cannot be taken into the check set by any member of P_s. Then for each i for $0\le i\le s$ there is a $u\in\mathcal{T}$ such that $uM_i\in\mathcal{I}_n$. Since there are $s+1$ values of i and only s members of $\mathcal{T}$, there must be a $u\in\mathcal{T}$ which is such that $uM_i\in\mathcal{I}_{n+1}$ and $uM_j\in\mathcal{I}_{n+1}$ where $i\ne j$. Thus $uM_i=w_k$, $uM_j=w_l$, so $u=w_kM_i^{-1}=w_lM_j^{-1}$. This says that the k^{th} row of $(M_i^{-1})^*$ is the l^{th} row of $(M_j^{-1})^*$, which is a contradiction. ■

In [3] an example of a set of three matrices to correct two errors for $n=4$ is given, and this generalizes by recursion to all n, but no explicit construction is given for the general n for any other values of s.

In [8, Lemma 5] the following result was used to get the s-PD-sets of size $s+1$ for s up to the upper bound $f_n(\mathbb{F}_q)$ for the simplex codes:

Result 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 $V_n(\mathbb{F}_q)$.*

For the application to $\mathcal{R}(1,n)$ we take $q = 2$ and then notice that since it is clear that $\lfloor \frac{2^n-1}{n} \rfloor - 1 = f_n \geq F_n = \lfloor \frac{2^n}{n+1} \rfloor - 1$ for $n \geq 2$, so we can always find $F_n + 1$ of these bases.

Now let $n \geq 2$, $K = \mathbb{F}_{2^n}$ and let ζ be a primitive element of K^*. Let $\mathcal{B}$ be an $\mathbb{F}_2$-basis of K.

Lemma 2. *For $i = 0, \ldots, 2^n - 2$, let N_i be the $(n+1) \times (n+1)$ matrix over $\mathbb{F}_2$ where, for $j = 1, \ldots, n+1$, the j-th row of N_i is $[\ 1\ \zeta^{i+j-1}\ ]$ where ζ^{i+j-1} is interpreted as its list of n coordinates with respect to the basis $\mathcal{B}$. Then each N_i is invertible.*

Proof: Clearly, the first n rows of N_i are linearly independent since $\zeta^i, \ldots, \zeta^{i+n-1}$ are linearly independent in K over $\mathbb{F}_2$. So, N_i has rank at least n.

Now suppose that $\sum_{j=1}^{n+1} a_j r_j = 0$ where r_j denotes the j-th row of N_i and $a_j \in \mathbb{F}_2$. Then $\sum_{j=1}^{n+1} a_j = 0$ for the first entry, and $\sum_{j=1}^{n+1} a_j \zeta^{i+j-1} = 0$ from the remaining entries. The polynomial $p(x) = \sum_{j=1}^{n+1} a_j x^{j-1}$, if non-zero, must be the unique irreducible polynomial for ζ of degree n. But this leads to a contradiction since $p(1) = 0$. Hence, $p(x)$ must be the zero polynomial and the relation between the rows of N_i must be trivial. ■

Taking the matrices $N_{i(n+1)}$ for $0 \leq i \leq F_n$ gives a set of $F_n + 1$ mutually disjoint bases for $V_{n+1}(\mathbb{F}_2)$, as was done in the simplex case for $V_n(\mathbb{F}_2)$ from Result 5, and hence leads to the following corollary, which now proves the second part of Theorem 1:

Corollary 4. *For $n \geq 4$, the set of matrices $\{N_{i(n+1)} \mid 0 \leq i \leq F_n\}$ is a set of $F_n + 1 = \lfloor \frac{2^n}{n+1} \rfloor$ matrices, no two of which have a row in common. Thus the set of matrices*

$$\mathcal{S} = \{(N^*_{i(n+1)})^{-1} \mid 0 \leq i \leq F_n\}$$

is an F_n-PD-set of size $F_n + 1$ for $\mathcal{R}(1,n)$ with information set $\mathcal{I}_{n+1}$.

Clearly any subset of $\mathcal{S}$ of size $s+1$ for $1 \leq s \leq F_n$ will be an s-PD-set of size $s+1$, and nested PD-sets can be constructed in this way.[1]

6 Computational

A Magma program for finding the codes of minimum weight r for the PD-sets for first statement of Proposition 1 and for finding the sets for $\mathcal{R}(1,n)$ for Corollary 4 up to $s = F_n$ is located at

`http://www.ces.clemson.edu/~keyj/Key/PDsets/RM_PPD4.m`

[1]The authors acknowledge that one referee has pointed out to them that the unrefereed paper arXiv:1512.01839v1.pdf, uploaded on 6 December 2015 (R.D. Barrolleta and M. Villanueva, Partial permutation decoding for binary linear and $\mathbb{Z}_4$-linear Hadamard codes), contains a proof of Result 4 and that the unrefereed paper arXiv:1512.01839v2.pdf, uploaded on 30 April 2016, by the same authors and with the same title, contains almost identical proofs of Lemma 2 and Corollary 4 though neither the corresponding statements nor proofs appear in the first version. The referee informs us that the 30 April 2016 paper has since been submitted for publication.

7 Generalized Reed-Muller codes

The arguments here apply also to the generalized Reed-Muller codes $\mathcal{R}_{\mathbb{F}_q}(\rho, n)$ (see [1, Chapter 5]) using information sets established in [14, Theorem 1] giving s-PD-sets of minimal size $s+1$. Proposition 1 holds in precisely the same way for $q > 2$ and the proof needs no modification. Corollary 4, i.e. the result for first-order Reed-Muller codes, giving s-PD-sets all the way to the upper bound, needs slight modification: instead of the matrix M^* we need two matrices, *viz.* M^+ and M^-, where, if $M \in GL_{n+1}(\mathbb{F}_q)$, with rows r_i for $1 \leq i \leq n+1$, the matrix M^+ has rows $r_1, r_1 + r_2, \ldots, r_1 + r_{n+1}$, and the matrix M^- has rows $r_1, -r_1 + r_2, \ldots, -r_1 + r_{n+1}$. For $M \in ML_{n+1}$, clearly $M^+, M^- \in GL_{n+1}(\mathbb{F}_q)$ and also $(M^+)^- = M = (M^-)^+$. Note that $M^+ = M^*$ of Section 5. The $F_{n,q,1}$-PD-set of size $F_n + 1$ in Corollary 4 is then

$$\mathcal{S} = \{(N^-_{i(n+1)})^{-1} \mid 0 \leq i \leq F_{n,q,1}\},$$

where $F_{n,q,1} = \lfloor \frac{q^n}{n+1} \rfloor - 1$.

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] ———, *Polynomial codes and finite geometries*, Handbook of Coding Theory (V. S. Pless and W. C. Huffman, eds.), Amsterdam: Elsevier, 1998, Volume 2, Part 2, Chapter 16, pp. 1269–1343.

[3] R. D. Barrolleta and M. Villanueva, *Partial permutation decoding for binary linear Hadamard codes*, Electron. Notes Discrete Math. **46** (2014), 35–42.

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

[5] Andries Brouwer, http://www.win.tue.nl/ aeb/codes/binary-1.html.

[6] Richard A. Brualdi and Vera S. Pless, *Greedy codes*, J. Combin. Theory, Ser. A **64** (1993), 10–30.

[7] 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.

[8] Washiela Fish, Jennifer D. Key, and Eric Mwambene, *Partial permutation decoding for simplex codes*, Adv. Math. Commun. **6** (2012), 505–516.

[9] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version* 4.4.12, 2008, http://www.gap-system.org.

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

[11] Raymond Hill, *A first course in coding theory*, Oxford Applied Mathematics and Computing Science Series, Oxford: Oxford University Press, 1986.

[12] W. Cary 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.

[13] 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.

[14] ———, *Information sets and partial permutation decoding for codes from finite geometries*, Finite Fields Appl. **12** (2006), 232–247.

[15] ———, *Reed-Muller codes and permutation decoding*, Discrete Math. **310** (2010), 3114–3119.

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

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

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

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

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