Contents lists available at ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc

Improved partial permutation decoding for Reed–Muller codes

J.D. Key, T.P. McDonough, V.C. Mavron

Institute of Mathematics, Physics and Computer Science, Aberystwyth University, Aberystwyth SY23 3BZ, UK

ARTICLE INFO

Article history:
Received 13 April 2016
Received in revised form 26 September 2016
Accepted 27 November 2016
Available online xxxx

Keywords:
Reed–Muller codes
Permutation decoding

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 rth-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 sets of 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.

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, 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 Eq. (2).*

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

E-mail address: keyj@clemson.edu (J.D. Key).

http://dx.doi.org/10.1016/j.disc.2016.11.031
0012-365X/© 2016 Elsevier B.V. All rights reserved.

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 $3 \le d \le 15$ 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 $d \ge 1$ 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 $1 \le s \le \lfloor \frac{2^n}{n+1} \rfloor - 1$ for $\mathcal{R}(1, n)$ is given as Corollary 4 in Section 5. Any computations were done with Magma [4,7] 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** ($\boldsymbol{v}$) 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. $C^\perp = \{v \in \mathbb{F}_q^n \mid (v, c) = 0 \; \forall \, c \in C\}$. A **check matrix** for C is a generator matrix for $C^\perp$. The **all-one vector** is denoted by $\boldsymbol{\jmath}$.

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 [13,16] 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 $s \le t$ 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 $1 < s \le t$ then we can order S as follows: find an s-PD-set S_s for each $0 \le s \le t$ 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]: