On a family of abelian codes and their state complexities [*]

Tim Blackmore and Graham H. Norton
Algebraic Coding Research Group
Centre for Communications Research, University of Bristol, England.

August 22, 2001

Abstract

We study Reed-Muller codes and 'Berman' codes as abelian codes. We show that the duals of Berman codes and Reed-Muller codes can be considered as belonging to the same family of abelian codes. We also determine the minimum distance and state complexity (SC) of the duals of Berman codes. Each of the classical parameters generalizes that of Reed-Muller codes in the obvious way, but the state complexity does not. We conclude by comparing the asymptotic behaviour of the SC of the duals of Berman codes with that of the obvious generalization of the SC of Reed-Muller codes.

Keywords Abelian codes, Reed-Muller codes, ideal generators, state complexity.

1 Introduction

1.1 Abelian codes. All the codes that we consider are binary (linear block) codes. Abelian codes can be thought of as 'm-dimensional cyclic codes'. Thus a cyclic code is an ideal in $\mathbb{F}_2[X]/(X^n-1)$ and an abelian code is an ideal in

$$\frac{\mathbb{F}_2[X_1,\ldots,X_m]}{(X^{n_1}-1,\ldots,X^{n_m}-1)}.$$

Abelian codes were introduced by Berman in [4, 5]. They have been studied in [1, 11, 12, 13, 17, 20] and elsewhere; for an overview see [9, Section 4.8]. The abelian codes that we are interested in have $n_1=\cdots=n_m=p$, where p is prime. Such an abelian code is semisimple if p is odd and modular if $p=2$.

In [4] Berman shows that Reed-Muller ($\mathcal{RM}$) codes are modular abelian codes. Evidence that the generalization from semisimple cyclic codes to semisimple abelian codes is a valuable one is

[*] This research was supported by the U. K. Engineering and Physical Research Council under grant K27728.

presented in [5]. In particular, Berman gives an explicit description of a family of semisimple *abelian* codes, which he shows contains codes which are asymptotically better than any family of semisimple *cyclic* codes with the same lengths. In showing this, Berman determines the rates and minimum distances of the family of codes containing the asymptotically superior codes. We refer to this family of codes as Berman ($\mathcal{B}$) codes. We give Berman's definition of $\mathcal{B}$ codes in Section 2. Here we note that a $\mathcal{B}$ code with parameters $[p^m, \sum_{i=r+1}^{m} \binom{m}{i}(p-1)^i, 2^{r+1}]$ exists for each *odd* prime p and integers $m \geq 1$, $0 \leq r \leq m$. We denote this code by $\mathcal{B}_p(r,m)$. We show that the minimum distance of $\mathcal{B}_p(r,m)^\perp$ is p^{m-r}. Thus the parameters of $\mathcal{B}_p(r,m)^\perp$ are $[p^m, \sum_{i=0}^{r} \binom{m}{i}(p-1)^i, p^{m-r}]$, generalizing the parameters of $\mathcal{RM}$ codes from the case p is 2 to the case p is an odd prime.

1.2 State complexity. Subsequent to Berman's papers, the state complexity (SC) of a code has been introduced and considered as the fourth code parameter, [21]. SC is used as a measure of the complexity of trellis decoding algorithms, such as the Viterbi and sequential decoding algorithms, [22]. Thus it is desirable that the SC of a code be small. It is known that the SC of a code is equal to the SC of its dual, [15]. The Wolf bound, implicit in [23], says that the SC of an $[n,k]$ code is no more than $\min\{k, n-k\}$. Unlike the classical code parameters, the SC of a code can differ according to the way that the coordinates are ordered.

The SCs of cyclic, shortened cyclic and extended cyclic codes reach the Wolf bound, [18]. However, the SC of composite length cyclic codes can be reduced by considering them as two-dimensional cyclic codes, [3]. The SC of $\mathcal{RM}$ codes can also be reduced by regarding them as abelian codes rather than as extended cyclic codes. In fact, the standard coordinate order of an $\mathcal{RM}$ code as an abelian code is optimal with respect to SC, [19]. Thus, as well as the generalization from cyclic to abelian codes being valuable with regard to the classical code parameters, abelian codes can also have lower SC than cyclic codes. Here we consider the SC of $\mathcal{B}$ codes with their standard coordinate order.

Ever since the early days of trellis theory, the trellis structure of $\mathcal{RM}$ and related codes has received a lot of attention, [2, 8, 6, 7, 15, 16, 19, 22] among others. In particular, a closed form for the SC of $\mathcal{R}M$ codes (with their their standard coordinate order as abelian codes) is given in [2] and a closed form for the SC of q-ary $\mathcal{RM}$ codes is given in [6]. Since the classical parameters of $\mathcal{B}^\perp$ codes generalize those of $\mathcal{RM}$ codes it is natural to consider the SC of $\mathcal{B}_p(r,m)^\perp$. Since a code and its dual have the same SC, this will also give the SC of $\mathcal{B}_p(r,m)$.

1.3 Organization of the paper. In Section 2 we describe $\mathcal{B}_p(r,m)$, $\mathcal{B}_p(r,m)^\perp$ and the close connection between these codes and $\mathcal{RM}$ codes as abelian codes. We also show here that the minimum distance of $\mathcal{B}_p(r,m)^\perp$ is p^{m-r} so that the parameters of $\mathcal{B}_p(r,m)^\perp$ generalize those of $\mathcal{RM}(r,m)$. In Section 3, we give a closed form for the SC of $\mathcal{B}_p(r,m)^\perp$ with its standard coordinate order as an abelian code. The closed form is a combinatorial sum depending on p, r and m, which we denote $s_p^2(r,m)$. In Section 4 we compare the asymptotic behaviour of $s_p^2(r,m)$ and another combinatorial sum, $s_p^1(r,m)$; $s_p^1(r,m)$ yields the SC of $\mathcal{RM}(r,m)$ when $p=2$. The comparison is done for $r = \lfloor \lambda m \rfloor$, where $0 < \lambda < 1$. Our analysis in particular applies to the asymptotic behaviour of the SC of $\mathcal{RM}$ codes. We are led to a new measure of the asymptotic behaviour of SC that may prove useful for other codes. With this measure, the asymptotic behaviours of $s_p^1(r,m)$ and $s_p^2(r,m)$ are both equal to $H_p(\lambda)$, where H_p is the p-ary entropy function.

A preliminary account of these results and some others appeared in [7].

2 Berman codes, their duals and Reed-Muller codes

We begin this section by describing 'Berman' ($\mathcal{B}$) codes and their duals, $\mathcal{B}^\perp$ codes. As noted in the Introduction, our original interest in $\mathcal{B}$ codes is as a family of semisimple *abelian* codes that contains codes asymptotically superior to any family of semisimple *cyclic* codes with the same lengths. More precisely, it is shown in [5] (see also [9]) that

- if $(C_i)_{i\geq 1}$ is a sequence of semisimple cyclic codes with parameters $([n_i, k_i, d_i])_{i\geq 1}$ such that (i) $n_i = p_1^{\alpha_{1i}} \cdots p_s^{\alpha_{si}}$ for some fixed primes $p_1, \ldots, p_s$ and (ii) k_i/n_i is asymptotically non-zero, then there exists a K such that $d_i \leq K$ for all i; and
- for each odd prime p, there exist a sequence $(B_i)_{i\geq 1}$ of semisimple abelian codes with parameters $([p^i, k_i, d_i])_{i\geq 1}$ such that $k_i/p^i \longrightarrow 1$ and $d_i \longrightarrow \infty$.

We continue by showing that $\mathcal{RM}$ codes and $\mathcal{B}^\perp$ codes are together those abelian codes generated by $E_p(r,m)$ (defined below) for all primes p. Of these codes, $\mathcal{RM}$ codes are the modular ones ($p = 2$) and $\mathcal{B}^\perp$ codes are the semisimple ones (p an odd prime). We also determine the minimum distance of $\mathcal{B}^\perp$ codes, thus showing that their parameters generalize those of $\mathcal{RM}$ codes from the case $p = 2$ to the case p is an odd prime in the obvious way. Most of the results of this section are stated and proved in the appendix.

2.1 $\mathcal{B}$, $\mathcal{B}^\perp$ and $\mathcal{RM}$ codes as abelian codes. For a prime p and integer $m \geq 1$ we write $A_{p,m}$ for

$$\frac{\mathbb{F}_2[X_1, \ldots, X_m]}{(X_1^p - 1, \ldots, X_m^p - 1)}.$$

We identify a polynomial

$$\sum_{i_1=0}^{p-1} \cdots \sum_{i_m=0}^{p-1} f_{i_1 \cdots i_m} X_1^{i_1} \cdots X_m^{i_m} \in A_{p,m}$$

with its vector of coefficients ordered lexicographically with $X_1 < X_2 < \cdots < X_m$,

$$(f_{00\cdots 0}, \ldots, f_{(p-1)0\cdots 0}, \ldots, f_{i_1\cdots i_m}, \ldots, f_{0(p-1)\cdots(p-1)}, \ldots, f_{(p-1)(p-1)\cdots(p-1)}).$$

Then an ideal of $A_{p,m}$ is an abelian code.

For an abelian code C, we write $C^\vee$ for the check code of C,

$$C^\vee = \{g \in A_{p,m} : f \cdot g = 0 \text{ for all } f \in C\}.$$

Also, for $G \subseteq A_{p,m}$, we write $\langle G\rangle$ for the ideal of $A_{p,m}$ generated by G.

Now, for $1 \leq j \leq m$, we put $e_p(X_j) = 1 + X_j + \cdots + X_j^{p-1}$. Then, for $m \geq 1$ and $0 \leq r \leq m$ we define $E_p(r,m)$ to be the set of all products of the form

$$(1+e_p(X_{j_1}))\cdots(1+e_p(X_{j_s}))\cdot e_p(X_{j_{s+1}})\cdots(e_p(X_{j_m}),$$

where $\{j_1,\ldots,j_m\} = \{1,\ldots,m\}$ and $0 \leq s \leq r$. For odd primes p, the codes $\langle E_p(r,m)\rangle^\vee$ are studied in [5]. Thus, when p is an odd prime, we call $\langle E_p(r,m)\rangle^\vee$ a *Berman ($\mathcal{B}$) code* and denote it by $\mathcal{B}_p(r,m)$. In fact, $\langle E_p(r,m)\rangle^\vee = \langle E_p(r,m)\rangle^\perp$ (Proposition A.1 in the appendix), so that $\mathcal{B}_p(r,m)^\perp = \langle E_p(r,m)\rangle$. Since we have a set of ideal generators for $\mathcal{B}_p(r,m)^\perp$, it is easier to work with $\mathcal{B}_p(r,m)^\perp$ than with $\mathcal{B}_p(r,m)$. Thus, for example, in Section 3 we determine the state complexity of $\mathcal{B}_p(r,m)$ by finding the state complexity of $\mathcal{B}_p(r,m)^\perp$.

Example 2.1 *We take $p=3$, $m=2$ and $r=1$. Then*

$$\begin{aligned}E_3(1,2) &= \langle(1+X_1+X_1^2)(1+X_2+X_2^2),(X_1+X_1^2)(1+X_2+X_2^2),(X_2+X_2^2)(1+X_1+X_1^2)\rangle\\ &= \mathbb{F}_2\text{-Span}\{(1+X_1+X_1^2)(1+X_2+X_2^2),(X_1+X_1^2)(1+X_2+X_2^2),\\ &\qquad (X_2+X_2^2)(1+X_1+X_1^2),(1+X_1)(1+X_2+X_2^2),(1+X_2)(1+X_1+X_1^2)\}.\end{aligned}$$

Thus

$$\begin{bmatrix} 1&1&1&1&1&1&1&1&1\\ 0&1&1&0&1&1&0&1&1\\ 0&0&0&1&1&1&1&1&1\\ 1&0&1&1&0&1&1&0&1\\ 1&1&1&0&0&0&1&1&1 \end{bmatrix}$$

is a generator matrix for $\mathcal{B}_3(1,2)^\perp$ and $\mathcal{B}_3(1,2)^\perp$ is a $[9,5,3]$ code. Since $e_p(X)(1+X)=0$ in $A_{3,2}$, we have that $(1+X_1)(1+X_2) \in E_3(1,2)^\vee = \mathcal{B}_3(1,2)$. Since $\mathcal{B}_3(1,2)$ is a $[9,4]$ code, we get the generator matrix

$$\begin{bmatrix} 1&1&0&1&1&0&0&0&0\\ 0&1&1&0&1&1&0&0&0\\ 0&0&0&1&1&0&1&1&0\\ 0&0&0&0&1&1&0&1&1 \end{bmatrix}$$

for $\mathcal{B}_3(1,2)$ (by multiplying $(1+X_1)(1+X_2)$ by 1, X_1, X_2 and X_1X_2). Thus $\mathcal{B}_3(1,2)$ is a $[9,4,4]$ code.

As well as being a useful tool for the study of the state complexity of $\mathcal{B}$ codes, $\mathcal{B}^\perp$ codes are a natural generalization of $\mathcal{RM}$ codes. Firstly $\mathcal{RM}(r,m) = \langle E_2(r,m)\rangle$ (Proposition A.2 of the appendix). Thus $\mathcal{RM}$ codes and $\mathcal{B}^\perp$ codes can be considered together as a single family of binary abelian codes—those generated by $E_p(r,m)$ in $A_{p,m}$ for all primes p. Secondly we will show that the parameters of $\mathcal{B}^\perp$ codes generalize those of $\mathcal{RM}$ codes.

2.2 The minimum distance of $\mathcal{B}_p(r,m)^\perp$. We begin by giving an iterative description of $\mathcal{B}_p(r,m)^\perp$ that allows us to easily determine its minimum distance by induction. This iterative description is also convenient for the determination of the state complexity of $\mathcal{B}_p(r,m)^\perp$, which we do in Section 3. As usual, for vector spaces $V, W \subseteq A_{p,m}$ with $V \cap W = \{0\}$ we write $V \oplus W$ for the direct sum of V and W.

It is well-known that $\mathcal{RM}$ codes can be defined iteratively by means of the $(u|u+v)$ construction. Thus

$$\mathcal{RM}(r,m) = \{(u|u) : u \in \mathcal{RM}(r,m-1)\} \oplus \{(0|v) : v \in \mathcal{RM}(r-1,m-1)\},$$

where $(a|b)$ denotes the concatenation of a and b. It is not immediately clear how the $(u|u+v)$ construction should be generalized for the concatenation of $a_1, \ldots, a_p$ when $p \geq 3$. For our purposes it is better to rewrite the decomposition of $\mathcal{RM}(r,m)$ as

$$\begin{aligned}\mathcal{RM}(r,m) \quad &= \quad \{(u|u) : u \in \langle E_2(r,m-1) \setminus E_2(r-1,m-1)\rangle\} \\ &\qquad \oplus\{(v_1|v_2) : v_1, v_2 \in \mathcal{RM}(r-1,m-1)\}.\end{aligned}$$

(That the sum is direct is easy to show using the facts that $e_2(X_j)^2 = 0$ and $e_2(X_j)(1+e_2(X_j)) = e_2(X_j)$.) We generalize this decomposition to $\mathcal{B}^\perp$ codes.

We adopt the conventions that $\mathcal{B}_p(-1,m)^\perp = \{0\}$ and $\mathcal{B}_p(m+1,m)^\perp = A_{p,m}$. Then for $m \geq 2$ and $0 \leq r \leq m$ we put

$$B_p^1(r,m) = \left\{ \sum_{l=0}^{p-1} f_l \cdot X_m^l : f_0, \ldots, f_{p-1} \in \mathcal{B}_p(r-1,m-1)^\perp \right\}$$

and

$$B_p^2(r,m) = \{f \cdot e_p(X_m) : f \in \langle E_p(r,m-1) \setminus E_p(r-1,m-1)\rangle\}.$$

In terms of vectors we have that

$$B_p^1(r,m) = \{(f_0|\cdots|f_p) : f_0, \ldots, f_p \in \mathcal{B}_p(r-1,m-1)^\perp\}$$

and

$$B_p^2(r,m) = \{(f|\cdots|f) : f \in \langle E_p(r,m-1) \setminus E_p(r-1,m-1)\rangle\}.$$

Then, (Lemma A.3 of the appendix),

$$\mathcal{B}_p(r,m)^\perp = B_p^1(r,m) \oplus B_p^2(r,m).$$

EXAMPLE 2.2 *We have that* $B_3^1(1,2) = \{\sum_{l=0}^2 f_l \cdot X_2^l : f_0, f_1, f_2 \in \mathcal{B}_3(0,1)^\perp\}$. *Since* $\mathcal{B}_3(0,1)^\perp = \{0, e_3(X_1)\} = \{(000),(111)\}$ *we get*

$$\begin{aligned}B_3^1(1,2) \quad &= \quad \{e_p(X_1)(\alpha_0 + \alpha_1 X_2 + \alpha_2 X_2^2) : \alpha_0, \alpha_1, \alpha_2 \in \mathbb{F}_2\} \\ &= \quad \{(\alpha_0\alpha_0\alpha_0|\alpha_1\alpha_1\alpha_1|\alpha_2\alpha_2\alpha_2) : \alpha_0, \alpha_1, \alpha_2 \in \mathbb{F}_2\}.\end{aligned}$$

Also $B_3^2(1,2) = \{f \cdot e_p(X_m) : f \in \langle E_3(1,1) \setminus E_3(0,1)\rangle\}$. *Since* $E_3(1,1) \setminus E_3(0,1) = \langle 1 + e_3(X_1)\rangle = \{(000),(011),(101),(110)\}$, *we get*

$$\begin{aligned} B_3^2(1,2) &= \{X_1^{i_1}(1+e_p(X_1))(1+e_p(X_2)) : 0 \leq i_1 \leq 2\} \\ &= \{(000000000),(011011011),(101101101),(110110110)\}, \end{aligned}$$

and $\mathcal{B}_3(1,2)^\perp = B_3^1(1,2) \oplus B_3^2(1,2)$.

We conclude this section by determining the minimum distance of $\mathcal{B}_p(r,m)^\perp$.

PROPOSITION 2.3 *For* $m \geq 1$ *and* $0 \leq r \leq m$, *the minimum distance of* $\mathcal{B}_p(r,m)$ *is* p^{m-r}.

PROOF. The proof is by induction on m. The result clearly holds for $m = 1$, so we assume that the minimum distance of $\mathcal{B}_p(r,k)^\perp$ is p^{k-r} for all $0 \leq r \leq k$.

Take $0 \leq r \leq k+1$. We show that, for $f_0, \ldots, f_{p-1} \in \mathcal{B}_p(r-1,k)^\perp$ and $f \in \langle E_p(r,k) \setminus E_p(r-1,k)\rangle$, not all zero, the weight of $f' = \left(\sum_{l=0}^{p-1} f_l \cdot X_{k+1}^l\right) + f \cdot e_p(X_{k+1})$ is at least p^{k+1-r}, and that some such f' has weight p^{k+1-r}. The result then follows from Lemma A.3. There are two cases.

(i) If $f \neq 0$ then $0 \leq r \leq k$. We can write $f' = \sum_{l=0}^{p-1}(f_l + f) \cdot X_{k+1}^l$ and since each of the $f_l + f$ are in $\mathcal{B}_p(r,k)^\perp$ and non-zero, the weight of f' is at least $p \cdot p^{k-r}$.

(ii) If $f = 0$ then $f_l \neq 0$ for some $0 \leq l \leq p-1$ and the weight of $f' = \sum_{l=0}^{p-1} f_l \cdot X^l$ is at least $p^{k-(r-1)}$. Moreover taking a single non-zero f_l of weight p^{k+1-r} gives an f' of this weight. □

In [5] it is shown that, for all odd primes p and integers $m \geq 1$, $0 \leq r \leq m$, $\mathcal{B}_p(r,m)$ is a $[p^m, \sum_{i=r+1}^m \binom{m}{i}(p-1)^i, 2^{r+1}]$ code. Thus, for all primes p, the classical code parameters of the abelian code $\langle E_p(r,m)\rangle$ are $[p^m, \sum_{i=0}^r \binom{m}{i}(p-1)^i, p^{m-r}]$ and those of its dual are $[p^m, \sum_{i=r+1}^m \binom{m}{i}(p-1)^i, 2^{r+1}]$.

REMARK 2.4 *The proofs of Lemma A.3 and Proposition 2.3 do not use the fact that* p *is odd or prime. Thus starting with* $[n,1,n]$ *and* $[n,n,1]$ *codes and defining* $B_n^1(r,m)$ *and* $B_n^2(r,m)$ *analogously to* $B_p^1(r,m)$ *and* $B_p^2(r,m)$, *we could iteratively construct a family of codes having parameters* $[n^m, \sum_{i=0}^r \binom{m}{i}(n-1)^i, n^{m-r}]$ *for each* $n \geq 2$, $m \geq 1$ *and* $0 \leq r \leq m$.

3 State complexity of Berman codes

Let C be a length n linear code. For $1 \leq i \leq n$ the i^{th} *past truncated code* of C is $P_i(C) = \{(c_1, \ldots, c_i) : (c_1, \ldots, c_n) \in C\}$ and the i^{th} *future truncated code* of C is $F_i(C) = \{(c_{i+1}, \ldots, c_n) : (c_1, \ldots, c_n) \in C\}$, [15]. The *state space dimension of* C *at level* i is then given by

$$s_i(C) = \dim(P_i(C)) + \dim(F_i(C)) - \dim(C). \tag{1}$$

The *state complexity (SC) of* C, $s(C)$, is defined by

$$s(C) = \max\{s_i(C) : 1 \leq i \leq n\}.$$

It is known that the SC of $\mathcal{RM}$ codes is minimised by their standard coordinate order and that under this coordinate order $s(\mathcal{RM}(r,m)) = s_2^1(r,m)$, where

$$s_p^1(r,m) := \sum_{i=0}^{\min\{r,m-r-1\}} \binom{m-2i-1}{r-i} (p-1)^{r-i}$$

[18, 19]. The coordinate order of abelian codes given in Section 2 (given by ordering the monomials of $A_{p,m}$ lexicographically with $X_1 < X_2 < \cdots < X_m$), generalizes the standard coordinate order of $\mathcal{RM}$ codes, and so we refer to it as the *standard coordinate order of abelian codes.* Given the results of Section 2, it could be expected that the SC of $\mathcal{B}_p(r,m)^\perp$ with its standard coordinate order would be $s_p^1(r,m)$. We show here that, in fact, the SC of $\mathcal{B}_p(r,m)^\perp$ with its standard coordinate order is

$$s_p^2(r,m) := \sum_{i=0}^{r} \binom{m-i-1}{r-i} (p-1)^{r-i}.$$

It seems important that the dual of a $\mathcal{RM}$ code is a $\mathcal{RM}$ code, but that the dual of $\mathcal{B}^\perp$ code is not a $\mathcal{B}^\perp$ code. We always have that $s_p^1(r,m) \leq s_p^2(r,m)$ and the inequality is strict when $2 \leq r \leq m-1$. However, $s_p^2(r,m)$ is less than the Wolf bound and, as we shall see, is asymptotically similar to $s_p^1(r,m)$.

We use the decomposition of $\mathcal{B}_p(r,m)^\perp$ as $B_p^1(r,m) \oplus B_p^2(r,m)$ described in Section 2 by applying the following easily-proved lemma.

Lemma 3.1 *If C_1 and C_2 are length n linear codes over $\mathbb{F}_q$ and $C_1 \cap C_2 = \{0\}$ then*

$$s_i(C_1 \oplus C_2) \leq s_i(C_1) + s_i(C_2),$$

with equality if and only if $P_i(C_1) \cap P_i(C_2) = \{0\}$ and $F_i(C_1) \cap F_i(C_2) = \{0\}$.

Now for each i, $s_i(C) = s_i(C^\perp)$ and hence $s(C) = s(C^\perp)$, [15]. When $\mathcal{B}_p(r,m)$ and $\mathcal{B}_p(r,m)^\perp$ have their standard coordinate order, we write $s_i(p,r,m)$ for $s_i(\mathcal{B}_p(r,m)) = s_i(\mathcal{B}_p(r,m)^\perp)$ and $s(p,r,m)$ for $s(\mathcal{B}_p(r,m)) = s(\mathcal{B}_p(r,m)^\perp)$. We determine $s(p,r,m)$ by considering $\mathcal{B}_p(r,m)^\perp$. The proof uses Lemmas A.3 and 3.1 and induction on m. The main inductive step is given by

Lemma 3.2 *For p an odd prime, $m \geq 2$ and $0 \leq r \leq m$,*

$$s(p,r,m) = s(p,r-1,m-1) + \binom{m-1}{r} (p-1)^r.$$

Proof. For $1 \leq i \leq p^m$, we can uniquely write $i = Qp^{m-1} + R$ for some $0 \leq Q \leq p-1$ and $1 \leq R \leq p^{m-1}$. Then

$$\dim\left(P_i(B_p^1(r,m))\right) = Q \cdot \left(\sum_{i=0}^{r-1} \binom{m-1}{i} (p-1)^i\right) + \dim\left(P_R(\mathcal{B}_p(r-1,m-1)^\perp)\right)$$

and

$$\dim\left(F_i(B_p^1(r,m))\right) = (p-1-Q)\cdot\left(\sum_{i=0}^{r-1}\binom{m-1}{i}(p-1)^i\right) + \dim\left(F_R(\mathcal{B}_p(r-1,m-1)^\perp)\right),$$

so that from (1), $s_i\left(B_p^1(r,m)\right) = s_R(p,r-1,m-1)$. Also

$$\dim\left(P_i(B_p^2(r,m))\right) \le \binom{m-1}{r}(p-1)^r,$$

with equality if $1 \le Q \le p-1$,

$$\dim\left(F_i(B_p^2(r,m))\right) \le \binom{m-1}{r}(p-1)^r,$$

with equality if $0 \le Q \le p-2$. Thus from (1), $s_i\left(B_p^2(r,m)\right) \le \binom{m-1}{r}(p-1)^r$, with equality if $1 \le Q \le p-2$.

Now, if $1 \le Q \le p-2$ then $P_i(B_p^1(r,m)) \cap P_i(B_p^2(r,m)) = \{0\}$ and $F_i(B_p^1(r,m)) \cap F_i(B_p^2(r,m)) = \{0\}$. Hence from the decomposition of $\mathcal{B}_p(r,m)^\perp$ (Lemma A.3) and Lemma 3.1 we have

$$s_i(p,r,m) \le s_R(p,r-1,m-1) + \binom{m-1}{r}(p-1)^r,$$

with equality if $1 \le Q \le p-2$. Thus clearly $s(p,r,m) \le s(p,r-1,m-1) + \binom{m-1}{r}$ and taking $i = Qp^{m-1} + R$ with $1 \le Q \le p-2$ and R such that $s_R(p,r-1,m-1) = s(p,r-1,m-1)$ gives equality. □

The determination of the following closed form for $s(p,r,m)$ follows easily from Lemma 3.2 by induction.

PROPOSITION 3.3 *For p an odd prime, $m \ge 1$ and $0 \le r \le m$, $s(p,r,m) = s_p^2(r,m)$.*

Table 1 gives $s(3,r,m)$ for small values of r and m (cf. [22, Table 2] for $\mathcal{RM}$ codes). We include the Wolf bound for comparison. The first component of each entry is $s(3,r,m)$ and the second component is the Wolf bound.

REMARKS 3.4 *1. For $1 \le i \le p^m$ we have the p-expansion of i, $i = \sum_{l=1}^{m} i_l p^{l-1}$, where $0 \le i_l \le p-1$ for $1 \le l \le m$. It is clear from the proofs of Lemma 3.2 and Proposition 3.3 that $s_i(p,r,m) = s(p,r,m)$ for all i with p-expansion $\sum_{l=1}^{m} i_l p^{l-1}$ such that $1 \le i_l \le p-2$ for all $1 \le l \le m$.*

2. The proofs of Lemma 3.2 and Proposition 3.3 used Lemma A.3 and the fact that $p \ge 3$. Thus for $n \ge 3$ the $[n^m, \sum_{i=0}^{r}\binom{m}{i}(n-1)^i, n^{m-r}]$ code of Remark 2.4 has SC equal to $s_n^2(r,m)$.

3. We recall that $s_p^1(r,m)$, defined in the Introduction, generalizes the SC of $\mathcal{RM}(r,m)$ from $p=2$ to any prime p. It is quite straightforward to see that if $2 \le r \le m-1$ then $s_p^2(r,m) > s_p^1(r,m)$. For all other values of m and r, $s_p^2(r,m) = s_p^1(r,m)$.

Table 1: $s(3,r,m)$ and Wolf bound for $\mathcal{B}_3(r,m)$

Order				Length m			
r	1	2	3	4	5	6	7
0	(1,1)	(1,1)	(1,1)	(1,1)	(1,1)	(1,1)	(1,1)
1		(3,4)	(5,7)	(7,9)	(9,11)	(11,13)	(13,15)
2			(7,8)	(17,33)	(31,51)	(49,73)	(71,99)
3				(15,16)	(49,112)	(111,233)	(209,379)
4					(31,32)	(129,256)	(351,939)
5						(63,64)	(321,576)
6							(127,128)

Although the standard coordinate order of $\mathcal{RM}$ codes is known to minimise their SC, we do not know whether the same is true for $\mathcal{B}$ and $\mathcal{B}^\perp$ codes. (According to [22], $\mathcal{RM}$ codes were the only infinite family of codes for which a 'uniformly optimum' coordinate order was known, although a uniformly optimum coordinate order for q-ary $\mathcal{RM}$ codes is also now known, [16]. Both of these results depend on complete knowledge of the weight hierarchies for these codes.) However, the results of [7] suggest that the discrepancy between $s(\mathcal{B}_p(r,m)^\perp)$ and $s_p^1(r,m)$ is due to the codes, rather than their coordinate order. Thus in [7] the SC of another generalization of $\mathcal{RM}$ codes, due to Dwork and Heller in [14], is given. A 'Dwork-Heller' code, $\mathcal{DH}_n^q(r,m)$, is defined over $\mathbb{F}_q$, for integers $n \geq 1$, $m \geq 1$ and $0 \leq r \leq m$. For $q = n = 2$ they correspond to $\mathcal{RM}$ codes. Generally $\mathcal{DH}_n^q(r,m)$ is an $[n^m, \sum_{i=0}^r \binom{m}{i}(n-1)^i, 2^{m-r}]$ code, so that for p an odd prime, $\mathcal{DH}_p^2(r,m)$ and $\mathcal{B}_p(r,m)^\perp$ both have dimension $\sum_{i=0}^r \binom{m}{i}(p-1)^i$ but their minimum distances are 2^{m-r} and p^{m-r} respectively. In [7] an outline of a proof that $s\left(\mathcal{DH}_p^q(r,m)\right) = s_p^1(r,m)$ is given (where $\mathcal{DH}_p^q(r,m)$ has its natural coordinate order generalizing the standard coordinate order of $\mathcal{RM}$ codes). Thus, it is $\mathcal{DH}$ codes, rather then $\mathcal{B}^\perp$ codes, that generalize $\mathcal{RM}$ codes with respect to SC.

4 Asymptotic analysis

The asymptotic behaviour of SCs has received some attention, [22] and work cited there. However, little seems to be known about the asymptotic behaviour of SCs for particular families of codes. Here we investigate the asymptotic behaviour of the SCs of $\mathcal{RM}(\lfloor \lambda m \rfloor, m)$ and $\mathcal{B}_p(\lfloor \lambda m \rfloor, m)$, where $0 < \lambda < 1$. In fact it is no harder to look at the asymptotic behaviours of $s_n^1(\lfloor \lambda m \rfloor, m)$ and $s_n^2(\lfloor \lambda m \rfloor, m)$ for all $n \geq 2$.

For a sequence of linear codes $(C_i)_{i\geq 1}$ with parameters $([n_i, k_i, d_i])_{i\geq 1}$, the asymptotic measure of SC used in [22] is relative SC, $\lim_{i\to\infty} s(C_i)/n_i$. Our first result of this section (Proposition 4.1) shows that relative SC fails to distinguish between the asymptotic behaviours of $s_n^1(\lfloor \lambda m \rfloor, m)$ and

$s^2(\lfloor \lambda m \rfloor, m)$. We begin with some preliminaries.

Firstly, we recall that for each n we have an entropy function, $H_n : (0,1) \to (0,1]$, defined by

$$H_n(\lambda) = \lambda \log_n(n-1) - \lambda \log_n \lambda - (1-\lambda)\log_n(1-\lambda).$$

Also we recall Stirling's formula, which can be written

$$\log_n m! = (m + \frac{1}{2}) \log_n m - m \log_n e + \frac{1}{2} \log_n 2\pi + o(1).$$

A simple consequence of Stirling's formula is that, for $0 < \lambda < 1$,

$$\log_n \binom{m}{\lfloor \lambda m \rfloor} = -m(\lambda \log_n \lambda + (1-\lambda)\log_n(1-\lambda)) - \frac{1}{2}\log_n m + O(1). \tag{2}$$

The $O(1)$ term in Equation (2) accounts for terms due to the discrepancy between λm and $\lfloor \lambda m \rfloor$, as well as $-\frac{1}{2}\log_n 2\pi$, $-\frac{1}{2}\log_n \lambda$ and $-\frac{1}{2}\log_n(1-\lambda)$ terms. (Our use of o and O is standard e.g. [10], where Stirling's formula can also be found.)

PROPOSITION 4.1 *For $n \geq 2$ and $0 < \lambda < 1$,*

$$\lim_{m\to\infty} \frac{s_n^1(\lfloor \lambda m \rfloor, m)}{n^m} = \lim_{m\to\infty} \frac{s_n^2(\lfloor \lambda m \rfloor, m)}{n^m} = 0.$$

PROOF. It follows from (2) that

$$\log_n \left(\binom{m}{\lfloor \lambda m \rfloor} \lambda^{\lambda m} (1-\lambda)^{(1-\lambda)m} \right) = -\frac{1}{2}\log_n m + O(1). \tag{3}$$

Since the limit on the right-hand side of (3) is $-\infty$ as $m \longrightarrow \infty$ we have that

$$\lim_{m\to\infty} \binom{m}{\lfloor \lambda m \rfloor} \lambda^{\lambda m}(1-\lambda)^{(1-\lambda)m} = 0. \tag{4}$$

Now, using the identity $\sum_{i=0}^{k} \binom{l+i}{i} = \binom{l+k+1}{k}$, we have that

$$s_n^2(r,m) \leq (n-1)^r \sum_{i=0}^{r} \binom{m-r-1+i}{i} = \binom{m}{r}(n-1)^r.$$

Thus, since $n^{-mH_n(\lambda)} = \frac{\lambda^{\lambda m}(1-\lambda)^{(1-\lambda)m}}{(n-1)^{\lambda m}}$, we have

$$s_n^2(\lfloor \lambda m \rfloor, m) n^{-mH_n(\lambda)} \leq \binom{m}{\lfloor \lambda m \rfloor} \lambda^{\lambda m}(1-\lambda)^{(1-\lambda)m}$$

so that

$$\frac{s_n^2(\lfloor \lambda m \rfloor, m)}{n^m} \leq n^{(H_n(\lambda)-1)m} \binom{m}{\lfloor \lambda m \rfloor} \lambda^{\lambda m}(1-\lambda)^{(1-\lambda)m} \leq \binom{m}{\lfloor \lambda m \rfloor} \lambda^{\lambda m}(1-\lambda)^{(1-\lambda)m}.$$

Therefore, the proposition follows from (4) and the fact that $0 \leq s_n^1(\lfloor \lambda m \rfloor, m) \leq s_n^2(\lfloor \lambda m \rfloor, m)$ (as noted in Remark 3.4.3). □

We note that the limit involving $s_n^2(\lfloor \lambda m \rfloor, m)/n^m$ in Proposition 4.1 trivially implies the limit involving $s_n^1(\lfloor \lambda m \rfloor, m)/n^m$. Thus Proposition 4.1 does not really provide a comparison of the asymptotic behaviours of $s_n^1(\lfloor \lambda m \rfloor, m)$ and $s_n^2(\lfloor \lambda m \rfloor, m)$. It is also possible to show that

$$\frac{s_n^2(\lfloor \lambda m \rfloor, m)}{m} \geq \frac{s_n^1(\lfloor \lambda m \rfloor, m)}{m} \longrightarrow \infty,$$

which similarly does not provide a real comparison. A non-trivial comparison is given by

Proposition 4.2 *For $n \geq 2$ and $0 < \lambda < 1$,*

$$\lim_{m\to\infty} \frac{\log_n s_n^1(\lfloor \lambda m \rfloor, m)}{m} = \lim_{m\to\infty} \frac{\log_n s_n^2(\lfloor \lambda m \rfloor, m)}{m} = H_n(\lambda).$$

Proof. We first show that

$$\binom{m-1}{r}(n-1)^r \leq \sum_{i=j}^{r} \binom{m-kr-1+ki}{i}(n-1)^i \leq \binom{m}{r}(n-1)^r. \qquad (5)$$

The lower-bound in (5) follows from the $i = r$ term of the sum and the upper-bound follows from

$$\begin{aligned}\sum_{i=j}^{r} \binom{m-kr-1+ki}{i}(n-1)^i &\leq (n-1)^r \sum_{i=0}^{r} \binom{m-kr-1+(k-1)i+i}{i} \\ &\leq (n-1)^r \sum_{i=0}^{r} \binom{m-kr-1+(k-1)r+i}{i} = \binom{m}{r}(n-1)^r.\end{aligned}$$

Now with $j = 0$ and $k = 1$, the middle expression of (5) is $s_n^2(r, m)$ and with $j = r - \min\{r, m-r-1\}$ and $k = 2$, the middle expression of (5) is $s_n^1(r, m)$. Thus to prove the proposition it suffices to show that

$$\lim_{m\to\infty} \frac{\log_n \binom{m-1}{\lfloor \lambda m \rfloor}(n-1)^{\lfloor \lambda m \rfloor}}{m} = \lim_{m\to\infty} \frac{\log_n \binom{m}{\lfloor \lambda m \rfloor}(n-1)^{\lfloor \lambda m \rfloor}}{m} = H_n(\lambda).$$

The first equality follows from the fact that $\binom{m-1}{r} = \frac{m-r}{m}\binom{m}{r}$ and the second equality follows directly from (2). □

Acknowledgments The authors gratefully acknowledge financial support from the U.K. Engineering and Physical Sciences Research Council. The first author was supported by the EPSRC. We would also like to thank the referees and the Associate Editor for their helpful comments and suggestions.

A Proofs for Section 2

Here we collect the formal statements and proofs of the results of Section 2.

Proposition A.1 *For all primes p and integers $m \geq 1$, $0 \leq r \leq m$, $\langle E_p(r,m)\rangle^\vee = \langle E_p(r,m)\rangle^\perp$.*

PROOF. First we show that $\langle E_p(r,m)\rangle^\perp = \pi(\langle E_p(r,m)\rangle^\vee)$, where π is the permutation $\pi(i) = p^m - i+1$ (so that π reverses the codewords of $\langle E_p(r,m)\rangle$). Since $\dim(\langle E_p(r,m)\rangle^\perp) = \dim(\pi(\langle E_p(r,m)\rangle^\vee))$ it suffices to show that $\langle E_p(r,m)\rangle^\perp \subseteq \pi(\langle E_p(r,m)\rangle^\vee)$, i.e. that if

$$f = \sum_{i_1=0}^{p-1} \cdots \sum_{i_m=0}^{p-1} f_{i_1\cdots i_m} X_1^{i_1} \cdots X_m^{i_m} \in \langle E_p(r,m)\rangle$$

and

$$g = \sum_{j_1=0}^{p-1} \cdots \sum_{j_m=0}^{p-1} g_{j_1\cdots j_m} X_1^{j_1} \cdots X_m^{j_m} \in \langle E_p(r,m)\rangle^\vee$$

then

$$\sum_{i_1=0}^{p-1} \cdots \sum_{i_m=0}^{p-1} f_{i_1\cdots i_m} \cdot g_{(p-1-i_1)\cdots(p-1-i_m)} = 0.$$

This follows from the coefficient of $X_1^{p-1}\cdots X_m^{p-1}$ in $f \cdot g$, since $2p-2 \equiv p-2 \bmod p$. Hence $\langle E_p(r,m)\rangle^\perp \subseteq \pi(\langle E_p(r,m)\rangle^\vee)$ and so $\langle E_p(r,m)\rangle^\perp = \pi(\langle E_p(r,m)\rangle^\vee)$. Therefore $\pi(\langle E_p(r,m)\rangle^\perp) = \langle E_p(r,m)\rangle^\vee$.

Next we show that $\langle E_p(r,m)\rangle = \pi(\langle E_p(r,m)\rangle)$, so that $\langle E_p(r,m)\rangle^\perp = \pi(\langle E_p(r,m)\rangle^\perp) = \langle E_p(r,m)\rangle^\vee$, as required. As π is linear, it suffices to show that if

$$\begin{aligned} h &= X_1^{a_1}\cdots X_m^{a_m} \cdot (1+e_p(X_{j_1}))\cdots(1+e_p(X_{j_s}))\cdot e_p(X_{j_{s+1}})\cdots e_p(X_{j_m}) \\ &= X_{j_1}^{a_{j_1}}\cdots X_{j_s}^{a_{j_s}} \cdot (1+e_p(X_{j_1}))\cdots(1+e_p(X_{j_s}))\cdot e_p(X_{j_{s+1}})\cdots e_p(X_{j_m}), \end{aligned}$$

where $\{j_1,\ldots,j_m\} = \{1,\ldots,m\}$ and $0 \le s \le r$, then $\pi(h) \in \langle E_p(r,m)\rangle$. Writing

$$h = \sum_{i_1=0}^{p-1} \cdots \sum_{i_m=0}^{p-1} h_{i_1\cdots i_m} X_1^{i_1} \cdots X_m^{i_m}$$

we have that $h_{i_1\cdots i_m} = 0$ if and only if $i_{j_k} = a_{j_k}$ for some $1 \le k \le s$. We put

$$h^* = X_{j_1}^{p-1-a_{j_1}}\cdots X_{j_s}^{p-1-a_{j_s}} \cdot (1+e_p(X_{j_1}))\cdots(1+e_p(X_{j_s}))\cdot e_p(X_{j_{s+1}})\cdots e_p(X_{j_m}).$$

We note that $h^* \in \langle E_p(r,m)\rangle$. Writing

$$h^* = \sum_{i_1=0}^{p-1} \cdots \sum_{i_m=0}^{p-1} h^*_{i_1\cdots i_m} X_1^{i_1} \cdots X_m^{i_m} \in \langle E_p(r,m)\rangle$$

we have that $h^*_{(p-1-i_1)\ldots(p-1-i_m)} = 0$ if and only if $(p-1-i_{j_k}) = p-1-a_{j_k}$ for some $1 \le k \le s$ if and only if $i_{j_k} = a_{j_k}$ for some $1 \le k \le s$ if and only if $h_{i_1\cdots i_m} = 0$, so that $h^* = \pi(h)$. □

PROPOSITION A.2 *For $0 \le r \le m$, $\mathcal{RM}(r,m) = \langle E_2(r,m)\rangle$.*

PROOF. Since $A_{2,m}$ is modular it has a radical, R_m. In [4] it is stated that R_m^{m-r} is equal to $\mathcal{RM}(r,m)$—an elementary proof of this appears in [1]. Thus it suffices to show that R_m^{m-r} is generated by $E_2(r,m)$.

It is known (e.g. [4]) that $R_m^{m-r} = \langle G(m-r,m)\rangle$, where

$$G(m-r,m) = \{(1+X_{j_1})\cdots(1+X_{j_t}) : m-r \le t \le m,\ 1 \le j_1 < \cdots < j_t \le m\}.$$

Thus it suffices to show that $G(m-r,m) \subseteq \langle E_2(r,m)\rangle$ and that $E_2(r,m) \subseteq \langle G(m-r,m)\rangle$, which we do by induction on r.

For $r = 0$ we have $G(m,m) = \{(1+X_1)\cdots(1+X_m)\} = E_2(0,m)$. Thus we assume that $G(m-k,m) \subseteq \langle E_2(k,m)\rangle$ and $E_2(k,m) \subseteq \langle G(m-k,m)\rangle$ for some $k \le m-1$. Since $E_2(k,m) \subseteq E_2(k+1,m)$ and $G(m-k-1,m) \subseteq G(m-k,m)$, it is enough to show that (i) $G(m-k-1,m) \setminus G(m-k,m) \subseteq \langle E_2(k+1,m)\rangle$ and (ii) $E_2(k+1,m) \setminus E_2(k,m) \subseteq \langle G(m-k-1,m)\rangle$.

Now, for $\{i_1,\ldots,i_s\} \subseteq \{1,\ldots,m\}$, it is straightforward to see by induction that

$$\sum_{l=1}^{s} \left((1+X_{i_l})\cdot X_{i_{l+1}}\cdots X_{i_s}\right) = 1 + X_{i_1}\cdots X_{i_s}.$$

Thus taking $g = (1+X_{j_1})\cdots(1+X_{j_{m-k-1}}) \in G(m-k-1,m) \setminus G(m-k,m)$ we can write

$$\begin{aligned} g &= (1+X_{j_1})\cdots(1+X_{j_{m-k-1}})\cdot X_{j_{m-k}}\cdots X_{j_m} \\ &+ (1+X_{j_1})\cdots(1+X_{j_{m-k-1}})\cdot \sum_{l=m-k}^{m} \left((1+X_{j_l})\cdot X_{j_{l+1}}\cdots X_{j_m}\right), \end{aligned}$$

so that $g \in E_2(k+1,m) + \langle G(m-k,m)\rangle \subseteq \langle E_2(k+1,m)\rangle$ by the inductive hypothesis and (i) is proven. Also taking $e = X_{j_1}\ldots X_{j_{k+1}}\cdot(1+X_{j_{k+2}})\cdots(1+X_{j_m}) \in E_2(k+1,m) \setminus E_2(k,m)$ we can write

$$e = (1+X_{j_{k+2}})\cdots(1+X_{j_m}) + (1+X_{j_{k+2}})\cdots(1+X_{j_m})\cdot \sum_{l=1}^{k+1}\left((1+X_{j_l})\cdot X_{j_{l+1}}\cdots X_{j_{k+1}}\right),$$

so that $e \in \langle G(m-k-1,m)\rangle$ and (ii) is proven. □

Lemma A.3 *For $m \ge 2$ and $0 \le r \le m$, $\mathcal{B}_p(r,m)^\perp = B_p^1(r,m) \oplus B_p^2(r,m)$.*

Proof. First, the fact that $e_p(X_j)$ and $1+e_p(X_j)$ are orthogonal idempotents easily implies that $B_p^1(r,m) \cap B_p^2(r,m) = \{0\}$. Now, it follows directly from the definition of $\mathcal{B}_p(r,m)^\perp$ that if $f \in \langle E_p(r,m-1)\rangle$ then $f\cdot e_p(X_m) \in \mathcal{B}_p(r,m)^\perp$. Also, since $X_m^l = e_p(X_m) + (1+e_p(X_m))\cdot X_m^l$ in $A_{p,m}$, $f_l \in \mathcal{B}_p(r-1,m-1)^\perp$ implies that $f_l \cdot X_m^l \in \mathcal{B}_p(r,m)^\perp$. Hence $B_p^1(r,m) \oplus B_p^2(r,m) \subseteq \mathcal{B}_p(r,m)^\perp$. Now, $\dim(B_p^1(r,m)) = p\cdot\sum_{i=0}^{r-1}\binom{m-1}{i}(p-1)^i$ and $\dim(B_p^2(r,m)) = \binom{m-1}{r}(p-1)^r$. The identity $\binom{m-1}{i} + \binom{m-1}{i-1} = \binom{m}{i}$ then implies that $\dim(B_p^1(r,m) \oplus B_p^2(r,m)) = \dim(\mathcal{B}_p(r,m)^\perp)$. □

References

[1] E. F. Assmus, Jr. On Bermans characterization of the Reed-Muller codes. *J. of Stat. Planning and Inference*, 56:17–21, 1996.

[2] Y. Berger and Y. Be'ery. Bounds on the trellis size of linear block codes. *IEEE Trans. Information Theory*, 39:203–209, 1993.

[3] Y. Berger and Y. Be'ery. Trellis-orientated decomposition and trellis complexity of composite-length cyclic codes. *IEEE Trans. Information Theory*, 41:1185–1191, 1995.

[4] S. D. Berman. On the theory of group codes. *Kibernetika*, 3:31–39, 1967.

[5] S. D. Berman. Semisimple cyclic and abelian codes II. *Kibernetika*, 3:21–30, 1967.

[6] T. Blackmore and G. H. Norton. On the trellis structure of GRM codes. In *Proc. of the Sixth Int. Workshop on Algebraic and Combinatorial Coding Theory*, pages 26–29, 1998.

[7] T. Blackmore and G. H. Norton. On the state complexity of some long codes. In *Finite Fields: Theory, Applications and Algorithms*, volume 225 of *Contemporary Mathematics*, pages 203–214. American Mathematical Society, Rhode Island, 1999.

[8] T. Blackmore and G. H. Norton. On trellis structures for Reed-Muller codes. *J. of Finite Fields and their Applications*, 6:39–70, 2000.

[9] I. F. Blake and R. C. Mullin. *The Mathematical Theory of Coding.* Academic Press, New York, 1975.

[10] J. C. Burkill and H. Burkill. *A Second Course in Mathematical Analysis.* Cambridge University Press, 1970.

[11] P. Camion. Abelian codes. Technical Report 1059, Mathematics Research Center, University of Wisconsin, 1971.

[12] P. Delsarte. Automorphisms of abelian codes. *Phillips Res. Rep.*, 25:389–403, 1970.

[13] P. Delsarte. Weights of p-ary abelian codes. *Phillips Res. Rep.*, 26:145–156, 1971.

[14] B. M. Dwork and R. M. Heller. Results of a geometric approach to the theory and construction of non–binary multiple error and failure correcting codes. *IRE Nat. Conv. Rec*, pages 123–129, 1959.

[15] G. D. Forney, Jr. Coset codes–part II: Binary lattices and related codes. *IEEE Trans. Information Theory*, 34:1152–1187, 1988.

[16] P. Heijnen and R. Pellikaan. Generalized Hamming weights of q-ary Reed-Muller codes. *IEEE Trans. Information Theory*, 44:181–196, 1998.

[17] J. M. Jensen. On the concatenated nature of cyclic and abelian codes. *IEEE Trans. Information Theory*, 31:788–793, 1985.

[18] T. Kasami, T. Takata, T. Fujiwara, and S. Lin. On complexity of trellis structure of linear block codes. *IEEE Trans. Information Theory*, 39:1057–1064, 1993.

[19] T. Kasami, T. Takata, T. Fujiwara, and S. Lin. On the optimum bit orders with respect to state complexity of trellis diagrams for binary linear codes. *IEEE Trans. Information Theory*, 39:242–245, 1993.

[20] F. J. MacWilliams. Binary codes which are ideals in the group algebra af an abelian group. *Bell System Tech. J.*, 44:987–1011, 1970.

[21] D. J. Muder. Minimal trellises for block codes. *IEEE Trans. Information Theory*, 34:1049–1053, 1988.

[22] A. Vardy. Trellis structure of codes. In V. S. Pless and W. C. Huffman, editors, *Handbook of Coding Theory*, chapter 24. Elsevier, 1998.

[23] J. K. Wolf. Efficient maximum likelihood decoding of linear block codes using a trellis. *IEEE Trans. Information Theory*, 24:76–80, 1978.