J. Algebra Comb. Discrete Appl.
10(2) • 105–113

Received: 5 January 2022
Accepted: 14 March 2022

Journal of Algebra Combinatorics Discrete Structures and Applications

Sequences of linear codes where the rate times distance grows rapidly

Research Article

Faezeh Alizadeh, S. P. Glasby, Cheryl E. Praeger

Abstract: For a linear code C of length n with dimension k and minimum distance d, it is desirable that the quantity kd/n is large. Given an arbitrary field $\mathbb{F}$, we introduce a novel, but elementary, construction that produces a recursively defined sequence of $\mathbb{F}$-linear codes $C_1, C_2, C_3, \ldots$ with parameters $[n_i, k_i, d_i]$ such that $k_i d_i/n_i$ grows quickly in the sense that $k_i d_i/n_i > \sqrt{k_i} - 1 > 2i - 1$. Another example of quick growth comes from a certain subsequence of Reed-Muller codes. Here the field is $\mathbb{F} = \mathbb{F}_2$ and $k_i d_i/n_i$ is asymptotic to $3n_i^c/\sqrt{\pi \log_2(n_i)}$ where $c = \log_2(3/2) \approx 0.585$.

2010 MSC: 94B65, 94B05, 94B15

Keywords: Linear code, Parameters, Reed Muller, Rate

1. Introduction

Let $\mathbb{F}$ be an arbitrary field and let $\mathbb{F}^n$ denote the space of all vectors of length n over $\mathbb{F}$. An $\mathbb{F}$-linear code C of length n is a subspace of the vector space $\mathbb{F}^n$, see [4, Section 1.2], and elements of C are called *codewords*. Denote the dimension of C by k. Given a codeword $x \in C$, the *(Hamming) weight* of x, denoted by $\mathrm{wt}(x)$, is the number of non-zero coordinates in x. The *(minimum) distance* of C, denoted by d or $d(C)$, is $d(C) = \min\{d(x, y) \mid x, y \in C, x \neq y\}$ where $d(x, y) = \mathrm{wt}(x - y)$ is the number of coordinate entries where x and y differ. An $\mathbb{F}$-linear code of length n, dimension k and distance d is abbreviated an $[n, k, d]$-linear code. The *(information) rate* of an $[n, k, d]$-linear code C is $R(C) = k/n$. We henceforth consider only linear codes.

Let $C_1, C_2, C_3, \ldots$ be a sequence of $\mathbb{F}$-linear codes where C_i has parameters $[n_i, k_i, d_i]$. We are interested in the question: How quickly can $k_i d_i/n_i$ approach infinity? It is easiest to understand the

Faezeh Alizadeh; Shahid Rajaee Teacher Training University, Tehran, Iran (email: Faezeh.Alizadeh2@gmail.com).
S. P. Glasby (Corresponding Author); Centre for the Mathematics of Symmetry and Computation, University of Western Australia, 35 Stirling Highway, Perth 6009, Australia (email: Stephen.Glasby@uwa.edu.au).
Cheryl E. Praeger; Centre for the Mathematics of Symmetry and Computation, University of Western Australia, 35 Stirling Highway, Perth 6009, Australia (email: Cheryl.Praeger@uwa.edu.au).

growth as a function of one variable, such as k_i, d_i or n_i. Since $k_i d_i/n_i \leqslant \min\{k_i, d_i\} \leqslant n_i$ such functions will be at most linear. Asymptotically good code sequences are ones which satisfy both $k_i/n_i \geqslant c$ and $d_i/n_i \geqslant c$ for some constant $c > 0$, see [2, (1.1)] and [10], and hence these code sequences achieve linear growth in n_i since $k_i d_i/n_i \geqslant c^2 n_i$. Such code sequences have been known to exist since [1], but they are not well understood, and the existence of asymptotically good *cyclic* codes has been a long standing open problem [7, 10] related to the uncertainty principle [2]. Other code sequences with reasonably good growth rates include the quadratic residue codes, see [4, Section 6.6]. These have parameters $[p, (p+1)/2, d]$ where p is a prime, and $d \geqslant \sqrt{p}$ by [6, p. 483, Theorem 1] so kd/n is at least $O(\sqrt{n})$. In Example 2.1, we describe a subsequence of Reed-Muller codes over $\mathbb{F}_2$ (*c.f.* [5]) with faster growth *viz.* $kd/n = O(n^{\log_2(3/2)})$. On the other hand, we might ask about 'non-examples', that is, code sequences for which $k_i d_i/n_i$ does not grow. There are such examples even among well-known code families. For example, for any fixed prime-power q, there is an $\mathbb{F}_q$-linear Reed-Solomon code [9] with parameters $[n, k, n-k+1]$ provided $q \geqslant n$. The family of all such codes has kd/n bounded as $kd/n \leqslant \min\{k, d\} \leqslant n \leqslant q$.

We want k to be large (relative to n) to transmit a lot of information, and d to be large to correct many errors, see Section 2 for more details. For linear codes over a finite field, the Singleton bound $(d \leqslant n-k+1)$ exhibits the tension between k and d, and Maximum Distance Separable (MDS) codes have $d = n-k+1$, see [8]. In Theorem 1.1 we exhibit an explicit construction for a sequence $C_1, C_2, C_3, \ldots$ of $\mathbb{F}$-linear codes, where $\mathbb{F}$ is a fixed but arbitrary field, and where C_i has parameters $[n_i, k_i, d_i]$ and $k_i d_i/n_i = O(\sqrt{k_i})$.

Theorem 1.1. *For each field $\mathbb{F}$, there exists an infinite sequence $C_1, C_2, C_3, \ldots$ of $\mathbb{F}$-linear codes such that C_i has parameters $[n_i, k_i, d_i]$ that satisfy*

$$\frac{k_i d_i}{n_i} = 2i > \sqrt{k_i} - 1 > 2i - 1 \qquad \text{for } i \geqslant 1.$$

The codes $C_1, C_2, C_3, \ldots$ in Theorem 1.1 are described in Definitions 4.4 and 4.6. They involve a novel construction described in Section 3, and their parameters $[n_i, k_i, d_i]$ are determined in Theorem 4.7. The codes are $\mathbb{F}$-linear, where $\mathbb{F}$ is an arbitrary field, and their limiting properties are similar to well-known codes, see Examples 2.1 and 2.2.

New codes can also be constructed from old codes via "direct sums" and "repetition". Both of these constructions fix the quantity kd/n, for suppose that C is an $\mathbb{F}$-linear code with parameters $[n, k, d]$, and s is a positive integer. The direct sum code $\bigoplus_{i=1}^{s} C \leqslant \mathbb{F}^{ns}$ has parameters $[ns, ks, d]$, and the quantity $(ks)d/(ns) = kd/n$ is independent of s. Similarly, the repetition code $\mathrm{diag}(\bigoplus_{i=1}^{s} C) = \{(u, \ldots, u) \mid u \in C\}$ has parameters $[ns, k, ds]$, and again $k(ds)/(ns) = kd/n$ is independent of s. By contrast, repeated application of the construction introduced to prove Theorem 4.7 allows kd/n to grow without bound.

2. Further remarks

We represent the vectors in $\mathbb{F}^n$ by n-dimensional column vectors over $\mathbb{F}$. Let C be an $[n, k, d]$-linear code in $\mathbb{F}^n$ and let $B = (a_1, \ldots, a_k)$ be an ordered basis of C. Let $H = [a_1, \ldots, a_k]$ be the $n \times k$ matrix formed by this basis. Then the code C is equal to the set $\{Hx \mid x \in \mathbb{F}^k\}$, and we regard an element $x \in \mathbb{F}^k$ as an information vector which is encoded as a codeword Hx. As H has rank k, by permuting the coordinates of $\mathbb{F}^n$ if necessary, we will assume that the $k \times k$ sub-matrix formed by the first k rows of H is invertible. Thus the information vector x is uniquely determined by the first k entries of the associated codeword Hx and the last $n-k$ entries of Hx may be regarded as redundancy added to enable transmission errors to be corrected.

The proportion k/n is called the *rate* $R(C)$ of C, and is a measure of the efficiency of C in encoding information. The third parameter, the minimum distance d of C is directly related to the error correction capability of C: if strictly less than $d/2$ entries in a codeword are changed during transmission then the received n-tuple is closer (in the Hamming metric) to the original codeword transmitted than to any other codeword, and hence these 'errors' can be corrected and the correct codeword determined. A high value of d relative to n denotes high reliability in transmitting information correctly.

Both k/n and the *relative distance* d/n are less than 1: the larger the rate k/n the more efficient is the code, while the larger the relative distance d/n the more reliable is the code. The question addressed in this paper is: How quickly can the quantity $k_i d_i/n_i$ approach infinity? Our construction demonstrates that this quantity kd/n can grow as fast as $\sqrt{k}$ for codes over any field $\mathbb{F}$.

Example 2.1. *A Reed-Muller code* $\mathrm{RM}(m,r)$ *is an* $\mathbb{F}_2$*-linear code, with parameters* $[2^m, \sum_{j=0}^{r}\binom{m}{j}, 2^{m-r}]$ *by [4, Theorem 1.10.1]. Thus* $k_r d_r/n_r = 2^{-r}\sum_{j=0}^{r}\binom{m}{j}$ *for* $\mathrm{RM}(m,r)$*. The subsequence* $(\mathrm{RM}(2r{+}1,r))_{r\geqslant 1}$ *has* $\dim(\mathrm{RM}(2r{+}1,r)) = k_r = \sum_{j=0}^{r}\binom{2r+1}{j} = 2^{2r}$ *and parameters* $[2^{2r+1}, 2^{2r}, 2^{r+1}]$*. Therefore* $k_r d_r/n_r = \sqrt{k_r} = O(\sqrt{n_r})$*. It turns out that the Reed Muller codes* $\mathrm{RM}(2r{+}1,r)$*, and the codes* C_r *in the Theorem 4.7 have* $k_r d_r/n_r = O(\sqrt{k_r})$*, and the quadratic residue codes have* $k_r d_r/n_r$ *at least* $\sqrt{k_r}$*.*

A faster growing subsequence is $(\mathrm{RM}(m, \lfloor \frac{m}{3} \rfloor + 1))_{m\geqslant 1}$*. It follows from [3, Theorem 2] that the parameters* $[n_m, k_m, d_m]$ *of* $\mathrm{RM}(m, \lfloor \frac{m}{3} \rfloor + 1)$ *have* $k_m d_m/n_m$ *asymptotic to*

$$\frac{3}{\sqrt{\pi m}}\left(\frac{3}{2}\right)^m = O\left(\frac{n_m^{\log_2(3/2)}}{\sqrt{\log_2(n_m)}}\right) \qquad \text{where } n_m = 2^m \text{ and } \log_2\left(\frac{3}{2}\right) \approx 0.585.$$

Example 2.2. *The codes in Theorem 1.1 are similar to simplex codes [6, Section 1.9] in that* n *and* d *are very large compared to* k*; and simplex codes give another family for which* kd/n *grows. The simplex codes over* $\mathbb{F}_q$ *have parameters* $[q^k - 1, k, q^{k-1}]$ *and* $kd/n > k/q$*.*

3. Bounded linear codes

In this section we present and investigate a construction which, given a linear code as input, produces a linear code with strictly larger length, dimension and minimum distance. We will be concerned with the extent to which the construction preserves the property of being bounded, which is defined as follows.

Definition 3.1. *Let* u *be a positive integer,* C *an* $\mathbb{F}$*-linear* $[n,k,d]$*-code, and* $B = (a_1, \ldots, a_k)$ *an ordered basis for* C*. Then* C *is said to be* u-bounded relative to B *if the following three conditions hold:*

(i) $\mathrm{wt}(a_j) = u$ *for each* j*;*

(ii) $\mathrm{wt}(\sum_{j=1}^{k} a_j) = d$*; and*

(iii) $u \geqslant d(1 + k^{-1})$*.*

We say that C *is* bounded *if there exist* u *and* B *such that* C *is* u*-bounded relative to* B*.*

3.1. The construction

Here we present the construction applied to an arbitrary linear code, and examine when the boundedness property is preserved.

Construction 3.2. *We have the following input and output.*
INPUT: *Let* C *an* $\mathbb{F}$*-linear* $[n,k,d]$*-code in* $\mathbb{F}^n$ *with ordered basis* $B = (a_1, \ldots, a_k)$*.*
OUTPUT: *The* $\mathbb{F}$*-linear code* $\mathsf{Code}(B)$ *in* $\mathbb{F}^{n(k+1)}$ *which is the* $\mathbb{F}$*-linear span of the sequence* $\mathsf{Basis}(B) = (a'_1, \ldots a'_{k+1})$*, where*

$$a'_1 = \begin{bmatrix} 0 \\ a_1 \\ a_2 \\ \vdots \\ a_k \end{bmatrix}, \; a'_2 = \begin{bmatrix} a_k \\ 0 \\ a_1 \\ \vdots \\ a_{k-1} \end{bmatrix}, \; \ldots, \; a'_{k+1} = \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_k \\ 0 \end{bmatrix},$$

and 0 *denotes the zero vector in* $\mathbb{F}^n$.

We show that the output $\mathsf{Basis}(B)$ from Construction 3.2 is linearly independent, determine the parameters of the code $\mathsf{Code}(B)$, and find conditions under which $\mathsf{Code}(B)$ is bounded relative to $\mathsf{Basis}(B)$.

Proposition 3.3. *Let* $\mathbb{F}, C, n, k, d, B$ *be as in Construction* 3.2.

(a) Then $\mathsf{Basis}(B)$ *is an ordered basis for* $\mathsf{Code}(B)$*, and* $\mathsf{Code}(B)$ *is an* $\mathbb{F}$*-linear* $[n', k', d']$*-code, where*

$$n' = (k+1)n, \quad k' = k+1 \quad \text{and } d' \text{ satisfies} \quad d' \geqslant kd.$$

(b) Further, if C *is* u*-bounded relative to* B*, then* $d' = (k+1)d$*, and, setting* $u' = ku$*,* $\mathsf{Code}(B)$ *is* u'*-bounded relative to* $\mathsf{Basis}(B)$ *if and only if* $u \geqslant d(1+2k^{-1})$.

Proof. (a) By Construction 3.2, $\mathsf{Code}(B)$ has length $n' = (k+1)n$. Further, the fact that the a_j are linearly independent implies that the a'_j are linearly independent, so $\mathsf{Basis}(B)$ is an ordered basis for $\mathsf{Code}(B)$, and therefore $\mathsf{Code}(B)$ has dimension $k' = k+1$. It remains to bound the minimum distance d'. An arbitrary non-zero codeword w in $\mathsf{Code}(B)$ has the form $w = \sum_{j=1}^{k+1} c_j a'_j$ for elements $c_j \in \mathbb{F}$, not all zero. We will prove that $\mathrm{wt}(w) \geqslant kd$, whence $d' \geqslant kd$. Write

$$w = \begin{bmatrix} w_1 \\ w_2 \\ \vdots \\ w_{k+1} \end{bmatrix},$$

where each $w_i \in \mathbb{F}^n$. Then by the definition of the a'_j in Construction 3.2,

$$w_i = \sum_{j=1}^{k} c_{i-j} a_j, \quad \text{for } i = 1, \ldots, k+1, \text{ reading subscripts modulo } k+1. \tag{1}$$

In particular each w_i is a codeword of C. Thus if each of the w_i is nonzero, then $\mathrm{wt}(w) = \sum_{i=1}^{k+1} \mathrm{wt}(w_i) \geqslant (k+1)d$. Suppose now that, for some i, $w_i = 0$. Since the a_j are linearly independent, it follows from (1) that $c_{i-j} = 0$ for $j = 1, \ldots, k$. Then since $w \neq 0$, we must have $c_i \neq 0$ so $w = c_i a'_i$, and hence

$$\mathrm{wt}(w) = \mathrm{wt}(a'_i) = \sum_{j=1}^{k} \mathrm{wt}(a_j) \geqslant kd \tag{2}$$

since each a_i is a codeword of C and so has weight at least d. This proves part (a).

(b) Now assume that C is u-bounded relative to B. Let $w = \sum_{j=1}^{k+1} c_j a'_j$ be an arbitrary non-zero codeword in $\mathsf{Code}(B)$, and define the w_i as above so that $\mathrm{wt}(w) = \sum_{i=1}^{k+1} \mathrm{wt}(w_i)$, and equation (1) holds. If each of the w_i is nonzero then $\mathrm{wt}(w) \geqslant (k+1)d$. On the other hand if some $w_i = 0$, then we showed above that equation (2) holds, so $\mathrm{wt}(w) = \sum_{j=1}^{k} \mathrm{wt}(a_j)$. In this case, by Definition 3.1(i), we have $\mathrm{wt}(a_j) = u$ for each j, and hence $\mathrm{wt}(w) = ku$. Further, by Definition 3.1(iii), $u \geqslant d(1+k^{-1})$, and hence $\mathrm{wt}(w) = ku \geqslant (k+1)d$. Thus the minimum distance d' of $\mathsf{Code}(B)$ satisfies $d' \geqslant (k+1)d$. To see that equality holds, consider the codeword w obtained by taking $c_1 = \cdots = c_{k+1} = 1$. For each i, equation (1) shows that $w_i = \sum_{j=1}^{k} a_j$, and hence $\mathrm{wt}(w_i) = d$ by Definition 3.1(ii). Therefore, for this codeword w we have $\mathrm{wt}(w) = \sum_{i=1}^{k+1} \mathrm{wt}(w_i) = (k+1)d$, and we conclude that $d' = (k+1)d$.

Now set $u' = ku$. First, from the definition of the a'_j we have $\mathrm{wt}(a'_j) = \sum_{i=1}^{k} \mathrm{wt}(a_i)$, which is equal to $ku = u'$ by Definition 3.1(i). Second, we showed in the previous paragraph that $\mathrm{wt}(\sum_{i=1}^{k+1} a'_i) = (k+1)d = d'$. Third, since $u' = ku$ and $d'(1+(k')^{-1}) = (k+1)d(1+(k+1)^{-1}) = d(k+2)$, it follows that $u' \geqslant d'(1+(k')^{-1})$ if and only if $u \geqslant d(k+2)/k = d(1+2k^{-1})$. Thus, by Definition 3.2, $\mathsf{Code}(B)$ is u'-bounded relative to $\mathsf{Basis}(B)$ if and only if $u \geqslant d(1+2k^{-1})$. This completes the proof. □

3.2. Recursive applications of the construction

By Proposition 3.3(a), the output code $\mathsf{Code}(B)$ of Construction 3.2 is always a linear code with ordered basis $\mathsf{Basis}(B)$, and hence Construction 3.2 may be applied repeatedly, producing larger and larger codes. Moreover, Proposition 3.3(b) implies that, provided the parameter u is sufficiently large, $\mathsf{Code}(B)$ is bounded relative to $\mathsf{Basis}(B)$. We investigate how many times we may apply Construction 3.2 recursively and still obtain a bounded code. To keep track of these repeated applications of Construction 3.2 we introduce some natural notation for the output codes and bases.

Definition 3.4. *Let i be a positive integer, and let C be an $\mathbb{F}$-linear code with an ordered basis B. In terms of the output of Construction 3.2 applied repeatedly to C, B, for $i = 1$, let*

$$\mathsf{Code}(B,1) = \mathsf{Code}(B) \quad \textit{and} \quad \mathsf{Basis}(B,1) = \mathsf{Basis}(B),$$

and for $i \geqslant 2$, define recursively,

$$\mathsf{Code}(B,i) = \mathsf{Code}(\mathsf{Basis}(B,i-1)) \quad \textit{and} \quad \mathsf{Basis}(B,i) = \mathsf{Basis}(\mathsf{Basis}(B,i-1)).$$

We examine the parameters and boundedness of $\mathsf{Code}(B,i)$ for various values of i.

Proposition 3.5. *Let i be a positive integer, and let C be an $\mathbb{F}$-linear $[n,k,d]$-code with an ordered basis B.*

(a) Then $\mathsf{Code}(B,i)$ is an $\mathbb{F}$-linear $[n_i,k_i,d_i]$-code, where

$$n_i = n\prod_{j=1}^{i}(k+j), \quad k_i = k+i, \quad d_i \geqslant d\prod_{j=1}^{i}(k+j-1).$$

(b) Further, suppose that C is u-bounded relative to B, and $u \geqslant d(1+ik^{-1})$, that is $i \leqslant k(ud^{-1}-1)$. Then the minimum distance d_i of $\mathsf{Code}(B,i)$ is

$$d_i = d\prod_{j=1}^{i}(k+j), \quad \textit{and setting} \quad u_i = u\prod_{j=1}^{i}(k+j-1),$$

$\mathsf{Code}(B,i)$ is u_i-bounded relative to $\mathsf{Basis}(B,i)$ if and only if $u \geqslant d(1+(i+1)k^{-1})$.

Proof. (a) Our proof is by induction on i. It follows from Proposition 3.3(a) that $\mathsf{Code}(B,1)$ is an $\mathbb{F}$-linear $[n_1,k_1,d_1]$-code where $n_1 = n(k+1), k_1 = k+1$ and $d_1 \geqslant dk$. Suppose that $i \geqslant 2$ and assume that the assertions of part (a) hold for $\mathsf{Code}(B,i-1)$. Proposition 3.3(a) implies that $n_i = n_{i-1}(k_{i-1}+1), k_i = k_{i-1}+1$ and $d_i \geqslant d_{i-1}k_{i-1}$. Hence the assertions of part (a) hold for also for $\mathsf{Code}(B,i)$.

(b) Now suppose that C is u-bounded relative to the ordered basis B. Then $u \geqslant d(1+k^{-1})$ by Definition 3.1(iii), and by Proposition 3.3(b), the minimum distance d_1 of $\mathsf{Code}(B,1)$ is $d_1 = d(k+1)$; also $\mathsf{Code}(B,1)$ is u_1-bounded, where $u_1 = ku$, if and only if $u \geqslant d(1+2k^{-1})$. Thus part (b) holds for $i = 1$. Assume now that $i \geqslant 2$ and $i \leqslant k(ud^{-1}-1)$, and also that part (b) holds for $\mathsf{Code}(B,i-1)$, that is,

$$d_{i-1} = d\prod_{j=1}^{i-1}(k+j), \quad \text{and setting} \quad u_{i-1} = u\prod_{j=1}^{i-1}(k+j-1),$$

$\mathsf{Code}(B,i-1)$ is u_{i-1}-bounded relative to $\mathsf{Basis}(B,i-1)$ if and only if $u \geqslant d(1+ik^{-1})$. Since we are assuming that the inequality $u \geqslant d(1+ik^{-1})$ holds, we conclude that $\mathsf{Code}(B,i-1)$ is u_{i-1}-bounded relative to $\mathsf{Basis}(B,i-1)$. Thus applying Proposition 3.3(b) to $\mathsf{Code}(B,i-1)$ with $\mathsf{Basis}(B,i-1)$, shows that $d_i = d_{i-1}(k_{i-1}+1)$ and that $\mathsf{Code}(B,i)$ is $(u_{i-1}k_{i-1})$-bounded relative to $\mathsf{Basis}(B,i)$ if and only if

$u_{i-1} \geqslant d_{i-1}(1+2k_{i-1}^{-1})$. Since $k_{i-1}+1 = k+i$ by part (a), we conclude that d_i is as in part (b). Also, since $u_{i-1}k_{i-1} = u\prod_{j=1}^{i}(k+j-1)$ is equal to u_i, $\mathsf{Code}(B,i)$ is u_i-bounded relative to $\mathsf{Basis}(B,i)$ if and only if the inequality $u_{i-1} \geqslant d_{i-1}(1+2k_{i-1}^{-1})$ holds. Substituting the values above for $u_{i-1}, d_{i-1}, k_{i-1}$, this inequality is

$$u\prod_{j=1}^{i-1}(k+j-1) \geqslant \left(d\prod_{j=1}^{i-1}(k+j)\right)\frac{k+i+1}{k+i-1},$$

that is, $u \geqslant dk^{-1}(k+i+1) = d(1+(i+1)k^{-1})$. Thus part (b) is proved by induction. □

Remark 3.6. *We note that, the quantity mentioned in the introduction, namely the rate times the minimum distance, grows slowly with the number i of applications of Construction 3.2: for $1 \leqslant i \leqslant k(ud^{-1}-1)$ we have, by Proposition 3.5, that*

$$\frac{k_i d_i}{n_i} = \frac{(k+i)d}{n} = \frac{kd}{n} + \frac{id}{n}.$$

4. Explicit instances of the construction

In this section we construct a family of linear codes which are defined as column spaces of a certain family of square matrices. First we introduce the matrices.

4.1. A family of matrices

As always $\mathbb{F}$ denotes an arbitrary field. We introduce an infinite family of matrices over $\mathbb{F}$, and explore some of their properties. We denote the space of $m \times n$ matrices over $\mathbb{F}$ by $\mathbb{F}^{m\times n}$; we denote the zero matrix in this ring by $0_{m\times n}$, or sometimes just by 0; and if $m = n$ we denote the identity matrix by I_m, and the determinant of $\mathcal{A} \in \mathbb{F}^{m\times m}$ by $\det(\mathcal{A})$. For a matrix $\mathcal{A} \in \mathbb{F}^{m\times n}$, its ij-entry is denoted $\mathcal{A}_{ij}$, and its *transpose* obtained by interchanging rows and columns is denoted $\mathcal{A}^T$, that is $(\mathcal{A}^T)_{ij} = \mathcal{A}_{ji}$ for all i, j. For simplicity of the exposition we will sometimes represent matrices as block matrices where some $(a \times b)$-block may be an *empty matrix*, that is $a = 0$ or $b = 0$ are allowed.

Definition 4.1. *For a positive integer i, we define matrices $\mathcal{A}_i$ and $\mathcal{B}_i$ as follows. For $i = 1$, these are*

$$\mathcal{A}_1 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \quad \text{and} \quad \mathcal{B}_1 = \begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix},$$

and recursively, for $i \geqslant 1$, if $\mathcal{A}_i, \mathcal{B}_i$ have been defined, then we let

$$\mathcal{A}_{i+1} = \begin{bmatrix} \mathcal{A}_1 & \mathcal{B}_i \\ -\mathcal{B}_i^T & \mathcal{A}_i \end{bmatrix}, \quad \text{and} \quad \mathcal{B}_{i+1} = \begin{bmatrix} \mathcal{B}_1 & \mathcal{B}_i \end{bmatrix}.$$

Our first observations about the family are given in this lemma. The idea behind the proof of Lemma 4.2 we found in [11, Section 5, Acknowledgements].

Lemma 4.2. *Let i be a positive integer and $\mathcal{A}_i, \mathcal{B}_i$ be as in Definition 4.1. Then*

(a) $\mathcal{B}_i = [\mathcal{B}_1 \cdots \mathcal{B}_1] \in \mathbb{F}^{2\times 2i}$; for $a \in \{1,2\}$ and $b \in \{1,\ldots,2i\}$ we have $(\mathcal{B}_i)_{ab} = (-1)^{a+b}$ and $\mathcal{B}_i^T\mathcal{A}_1\mathcal{B}_i = \mathcal{B}_i^T\mathcal{A}_1^{-1}\mathcal{B}_i = 0_{2\times 2}$.

(b) $\mathcal{A}_i \in \mathbb{F}^{2i\times 2i}$ satisfies $\det(\mathcal{A}_i) = 1$.

Proof. (a) A straightforward inductive argument, based on the definition of $\mathcal{B}_{i+1}$ in Definition 4.1 shows that $\mathcal{B}_i = [\mathcal{B}_1 \cdots \mathcal{B}_1] \in \mathbb{F}^{2\times 2i}$ for each $i \geqslant 1$. Then it is easy to see that $(\mathcal{B}_i)_{ab} = (-1)^{a+b}$ for all a, b. It follows from $\mathcal{B}_i = [\mathcal{B}_1 \cdots \mathcal{B}_1]$ that $\mathcal{B}_i^T \mathcal{A}_1 \mathcal{B}_i = \sum_{j=1}^{i} \mathcal{B}_1^T \mathcal{A}_1 \mathcal{B}_1$, and computing we see that $\mathcal{B}_1^T \mathcal{A}_1 \mathcal{B}_1 = \mathcal{B}_1 \mathcal{A}_1 \mathcal{B}_1 = 0_{2\times 2}$. Hence $\mathcal{B}_i^T \mathcal{A}_1 \mathcal{B}_i = 0_{2\times 2}$, and the final assertion $\mathcal{B}_i^T \mathcal{A}_1^{-1} \mathcal{B}_i = 0_{2\times 2}$ follows from the fact that $\mathcal{A}_1^{-1} = -\mathcal{A}_1$.

(b) It is easy to see that $\det(\mathcal{A}_1) = 1$, and $\mathcal{A}_i \in \mathbb{F}^{2i\times 2i}$ for each $i \geqslant 1$. Assume that $i \geqslant 1$, assume inductively that $\det(\mathcal{A}_i) = 1$, and consider $\mathcal{A}_{i+1}$ as defined in Definition 4.1. Modifying an idea from [11, Section 5], we see by direct computation that

$$\begin{bmatrix} \mathcal{A}_1 & \mathcal{B}_i \\ -\mathcal{B}_i^T & \mathcal{A}_i \end{bmatrix} \begin{bmatrix} I_2 & -\mathcal{A}_1^{-1}\mathcal{B}_i \\ 0_{2i\times 2} & I_{2i} \end{bmatrix} = \begin{bmatrix} \mathcal{A}_1 & 0_{2\times 2i} \\ -\mathcal{B}_i^T & \mathcal{B}_i^T \mathcal{A}_1^{-1} \mathcal{B}_i + \mathcal{A}_i \end{bmatrix} = \begin{bmatrix} \mathcal{A}_1 & 0_{2\times 2i} \\ -\mathcal{B}_i^T & \mathcal{A}_i \end{bmatrix}$$

where the last equality follows from part (a). Since the second matrix on the left side has determinant 1, it follows that $\det(\mathcal{A}_{i+1}) = \det(\mathcal{A}_1)\det(\mathcal{A}_i) = 1$ where the last equality uses the inductive hypothesis. Thus part (b) follows by induction. □

The next lemma looks at properties of the columns of the $\mathcal{A}_i$.

Lemma 4.3. *Let i be a positive integer, and let $\mathcal{A}_i = [a_1, a_2, \ldots, a_{2i}]$ be as in Definition 4.1, where a_j is the jth column of $\mathcal{A}_i$. Then*

(a) $\mathrm{wt}(a_j) = 2i - 1$ *for* $j \in \{1, \ldots, 2i\}$,

(b) $a_{2j-1} + a_{2j} = [0_{1\times 2(j-1)}, -1, 1, 0_{1\times 2(i-j)}]^T \in \mathbb{F}^{2i\times 1}$ *for* $j \in \{1, \ldots, i\}$,

(c) $\sum_{j=1}^{2i-1} a_j = [0, \ldots, 0, 1]^T \in \mathbb{F}^{2i\times 1}$, *and in particular,* $\mathrm{wt}(\sum_{j=1}^{2i-1} a_j) = 1$.

Proof. (a) Part (a) follows immediately from Definition 4.1.

(b) We use induction on i. For $i = 1$, $a_1 + a_2 = [-1, 1]^T$ by Definition 4.1, so (b) holds in this case (as $i = j = 1$ and the first and last entries in this vector in (b) are empty matrices). Now let $i \geqslant 1$ and assume inductively that (b) holds for $\mathcal{A}_i = [a_1, \ldots, a_{2i}]$, and consider $\mathcal{A}_{i+1} = [a'_1, \ldots, a'_{2i+2}]$. By Definition 4.1 and the structure of $\mathcal{B}_i$ given by Lemma 4.2(a), it follows that $a'_1 + a'_2 = [-1, 1, 0_{1\times 2i}]^T \in \mathbb{F}^{2(i+1)\times 1}$. For $j \in \{2, \ldots, i+1\}$, it follows from Definition 4.1 that

$$a'_{2j-1} + a'_{2j} = \begin{bmatrix} 0_{2\times 1} \\ a_{2j-3} + a_{2j-2} \end{bmatrix}.$$

Hence the structure of $a'_{2j-1} + a'_{2j}$ follows from the inductive hypothesis. Thus part (b) is proved by induction.

(c) This part is also proved by induction on i. The case $i = 1$ follows from the definition of $\mathcal{A}_1$. So assume that $i \geqslant 1$ and that part (c) holds for $\mathcal{A}_i$, that is $b := \sum_{\ell=1}^{2i-1} a_\ell = [0, \ldots, 0, 1]^T \in \mathbb{F}^{2i\times 1}$. Suppose that $\mathcal{A}_i$ and $\mathcal{A}_{i+1}$ have columns a_j and a'_j as in the proof of part (b). Using the structure of $\mathcal{B}_i$ from Lemma 4.2(a), the form of $a'_1 + a'_2$ above, and the inductive hypothesis, we have

$$\sum_{j=1}^{2i+1} a'_j = (a'_1 + a'_2) + \begin{bmatrix} 1 \\ -1 \\ \sum_{\ell=1}^{2i-1} a_\ell \end{bmatrix} = \begin{bmatrix} -1 \\ 1 \\ 0_{2i\times 1} \end{bmatrix} + \begin{bmatrix} 1 \\ -1 \\ b \end{bmatrix} = [\ 0,\ \ldots\ ,\ 0,\ 1\ ]^T \in \mathbb{F}^{2(i+1)\times 1}.$$

Part (c) follows by induction. □

4.2. Codes constructed from matrices

We now construct $\mathbb{F}$-linear codes from the matrices in Subsection 4.1, noting that the columns of $\mathcal{A}_i$ are linearly independent by Lemma 4.2(b) .

Definition 4.4. *Let i be a positive integer, let $\mathcal{A}_i = [a_1, a_2, \ldots, a_{2i}] \in \mathbb{F}^{2i\times 2i}$ be as in Definition 4.1, where a_j is the jth column of $\mathcal{A}_i$, and let $C(i)$ be the $\mathbb{F}$-linear code in $\mathbb{F}^{2i}$ with ordered basis $B(i) = (a_1, \ldots, a_{2i-1})$.*

We use the results from Subsection 4.1 to determine the properties of $C(i)$, and the results from Section 3 to study the codes obtained using Proposition 3.5.

Proposition 4.5. *For a positive integer i, let $C(i)$ and $B(i)$ be as in Definition 4.4.*

(a) For $i \geqslant 2$, the code $C(i)$ is an $\mathbb{F}$-linear $[2i, 2i-1, 1]$-code which is $(2i-1)$-bounded relative to the ordered basis $B(i)$.

(b) For $1 \leqslant j \leqslant 4i^2 - 6i + 1$, the code $\mathsf{Code}(B(i), j)$, as defined in Definition 3.4, is an $\mathbb{F}$-linear $[n_j, k_j, d_j]$-code that is u_j-bounded relative to the ordered basis $\mathsf{Basis}(B(i), j)$, where

$$n_j = 2i\prod_{\ell=1}^{j}(2i-1+\ell), \quad k_j = 2i-1+j, \quad d_j = \prod_{\ell=1}^{j}(2i-1+\ell), \text{ and } u_j = (2i-1)\prod_{\ell=1}^{j}(2i-2+\ell).$$

Proof. (a) By Lemma 4.2(b), $B(i)$ is an ordered basis for $C(i)$. Thus $C(i)$ has length $2i$ and dimension is $2i-1$. Moreover, $d(C(i)) = 1$ as $[0, \ldots, 0, 1]^T \in C(i)$ by Lemma 4.3(c). By Lemma 4.3(a), $\mathrm{wt}(a_j) = 2i-1$ for each $j \leqslant 2i-1$, and $\mathrm{wt}(\sum_{j=1}^{2i-1} a_j) = 1$. To see that $C(i)$ is $(2i-1)$-bounded relative to $B(i)$ for each $i \geqslant 2$ we use Definition 3.1 and note that $2i-1 \geqslant 1 + (2i-1)^{-1}$ holds (this is true for $i \geqslant 2$). This proves part (a).

(b) We apply Proposition 3.5(b) to $C(i)$ and $B(i)$. By part (a) the parameters n, u, k, d of that result are: $n = 2i, u = k = 2i-1, d = 1$, and we wish to apply Proposition 3.5(b) with a positive integer parameter j satisfying $u \geqslant d(1 + (j+1)k^{-1})$, or equivalently $j + 1 \leqslant k(ud^{-1} - 1) = (2i-1)(2i-2) = 4i^2 - 6i + 2$. This latter inequality is our assumption on j, so we may therefore apply Construction 3.2 j times and conclude, by Proposition 3.5(b), that $\mathsf{Code}(B(i), j)$ is an $\mathbb{F}$-linear $[n_j, k_j, d_j]$-code that is u_j-bounded relative to the ordered basis $\mathsf{Basis}(B(i), j)$, where the parameters n_j, k_j, d_j, u_j are as in the statement. This proves part (b). □

In Proposition 4.5(b) we have $n_j = 2id_j$ and $u_j(2i + j - 1) = (2i-1)d_j$, respectively. Note that setting $j = 0$ in the expressions for n_j, k_j, d_j, u_j in Proposition 4.5(b), we obtain the parameters n, k, d, u, respectively, for the code $C(i)$ examined in Proposition 4.5(a). Thus if we set $\mathsf{Code}(B(i), 0) := C(i)$, then all the assertions of Proposition 4.5(b) hold with $j = 0$. Thus we have constructed explicitly a two-parameter family of bounded linear codes over an arbitrary field $\mathbb{F}$, namely:

$$\mathsf{Code}(B(i), j) \text{ for all } i \geqslant 2 \text{ and all integers } j \text{ satisfying } 0 \leqslant j \leqslant 4i^2 - 6i + 1.$$

We write $\mathsf{Code}_{\mathbb{F}}(B(i), j)$ and $\mathsf{Basis}_{\mathbb{F}}(B(i), j)$ if we wish to emphasize the field $\mathbb{F}$ of scalars. To prove our main result we investigate a one-parameter subfamily of these codes, choosing, for each value of i, the code with the largest value of j. We now replace i with $i + 1$.

Definition 4.6. *For a field $\mathbb{F}$ of scalars, and each $i \geqslant 1$, define*

$$C_i := \mathsf{Code}_{\mathbb{F}}(B(i+1), 4i^2 - 2i - 1) \quad \text{and} \quad \mathcal{B}_i := \mathsf{Basis}_{\mathbb{F}}(B(i+1), 4i^2 - 2i - 1).$$

The following theorem follows immediately from Proposition 4.5.

Theorem 4.7. *Given a field $\mathbb{F}$ and an integer $i \geqslant 1$, the code C_i is a linear $[N_i, K_i, D_i]$-code over $\mathbb{F}$, which is U_i-bounded relative to its ordered basis $\mathcal{B}_i$, where*

$$N_i = 2(i+1)\prod_{\ell=1}^{4i^2-2i-1}(2i+1+\ell), \quad K_i = 4(i+1)i, \quad D_i = \prod_{\ell=1}^{4i^2-2i-1}(2i+1+\ell),$$

and $U_i = (2i+1)\prod_{\ell=1}^{4i^2-2i-1}(2i+\ell)$. Moreover, $\dfrac{K_iD_i}{N_i} = 2i$ grows linearly with i.

Proof. The first assertions follow immediately from Proposition 4.5 by replacing i with $i+1$. Finally, from these parameters we see that $\dfrac{K_iD_i}{N_i} = \dfrac{4(i+1)i}{2i} = 2i$. □

Proof of Theorem 1.1. By Proposition 4.7 there are $[n_i, k_i, d_i]$-codes C_i, $i \geqslant 1$, where $k_id_i/n_i = 2i$ and $k_i = 4(i+1)i$. A simple calculation shows that

$$2i > \sqrt{4i(i+1)} - 1 > \sqrt{4i^2} - 1 = 2i - 1.$$

□

Acknowledgement: The authors thank Patrick Solé for his remarks and for alerting us to [10]. The first author is grateful to UWA and the Centre for the Mathematics of Symmetry and Computation, and also to Shahid Rajaee Teacher Training University for their financial support when she was a visiting scholar. The second and third authors acknowledge support from the Australian Research Council Discovery Project DP190100450.

References

[1] C. L. Chen, W. W. Peterson, E. J. Weldon, Jr., Some results on quasi-cyclic codes, Information and Control 15 (1969) 407–423.
[2] S. Evra, E. Kowalski, A. Lubotzky, Good cyclic codes and the uncertainty principle, Enseign. Math. 63 (2017) 3–4.
[3] S. P. Glasby, G. R. Paseman, On the maximum of the weighted binomial sum $2^{-r}\sum_{i=0}^{r}\binom{m}{i}$,Electron. J. Combin. 29(2) (2022) 2–5.
[4] W. C. Huffman and V. Pless, Fundamentals of Error-Correcting Codes, Cambridge University Press, Cambridge, 2003.
[5] G. Lachaud, Projective Reed-Muller codes, Coding theory and applications, 1986 Lecture Notes in Comput. Sci., vol. 311, Springer, Berlin (1988) 25–129.
[6] F. J. MacWilliams, N. J. A. Sloane, The theory of error-correcting codes. I, North-Holland Mathematical Library, Vol. 16, North-Holland Publishing Co., Amsterdam-New York-Oxford, 1977.
[7] Conchita Martínez-Pérez, W. Willems, Is the class of cyclic codes asymptotically good?, IEEE Trans. Inform. Theory 52(2) (2006) 696–700.
[8] San Ling, Chaoping Xing, Coding theory: A first course, Cambridge University Press, Cambridge, 2004.
[9] G. Quintin, M. Barbier, C. Chabot, On generalized Reed-Solomon codes over commutative and noncommutative rings, IEEE Trans. Inform. Theory 59 (2013) 5882–5897.
[10] M. Shi, R. Wu, P. Solé, Asymptotically good additive cyclic codes exist, IEEE Communications Letters 22(10) (2018) 1980–1983.
[11] J. R. Silvester, Determinants of block matrices, The Mathematical Gazette 84 (2000) 460–467.