Matrix-product codes over $\mathbb{F}_q$ *

Tim Blackmore, Infineon Technologies, Stoke Gifford, BS34 8HP, U.K.
Graham H. Norton, Dept. Mathematics, Univ. of Queensland, Brisbane 4072.

October 2, 2001

Abstract

Codes $C_1, \ldots, C_M$ of length n over $\mathbb{F}_q$ and an $M \times N$ matrix A over $\mathbb{F}_q$ define a *matrix-product code* $C = [C_1 \ \cdots \ C_M] \cdot A$ consisting of all matrix products $[c_1 \ \cdots \ c_M] \cdot A$. This generalizes the $(u|u+v)$-, $(u+v+w|2u+v|u)$, $(a+x|b+x|a+b+x)$-, $(u+v|u-v)$- etc. constructions.

We study matrix-product codes using Linear Algebra. This provides a basis for a unified analysis of $|C|$, $\mathrm{d}(C)$, the minimum Hamming distance of C, and $C^\perp$. It also reveals an interesting connection with MDS codes.

We determine $|C|$ when A is non-singular. To underbound $\mathrm{d}(C)$, we need A to be 'non-singular by columns (NSC)'. We investigate NSC matrices. We show that Generalized Reed-Muller codes are iterative NSC matrix-product codes, generalizing the construction of Reed-Muller codes, as are the ternary 'Main Sequence codes'. We obtain a simpler proof of the minimum Hamming distance of such families of codes. If A is square and NSC, $C^\perp$ can be described using $C_1^\perp, \ldots, C_M^\perp$ and a transformation of A. This yields $\mathrm{d}(C^\perp)$. Finally we show that an NSC matrix-product code is a generalized concatenated code.

Keywords

Binary $(u|u+v)$-construction, ternary $(u+v+w|2u+v|u)$-construction, generalized Reed-Muller codes, generalized concatenated codes.

1 Introduction

If C_1 is an (n, K_1, d_1) code and C_2 is an (n, K_2, d_2) code, Plotkin's $(u|u+v)$-construction gives a $(2n, K_1K_2, \min\{2d_1, d_2\})$ code, [10]. It is a standard iterative way of defining the Reed-Muller ($\mathcal{RM}$-)codes. The ternary $(u+v+w|2u+v|u)$-construction produces good codes, giving a $(3n, K_1K_2K_3, \min\{3d_1, 2d_2, d_3\})$ code, where C_i is an (n, K_i, d_i) for $i = 1, \ldots, 3$, [5]. This construction is iterated to produce a 'Main Sequence (MS)' subfamily of the ternary Reed-Muller codes in

*Research funded by the U. K. Engineering and Physical Sciences Research Council under grant GR/K27728.

[5, Section IV.C], which we write as $\mathcal{MS}_3$. The matrices

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \text{ and } \begin{bmatrix} 1 & 2 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$$

are associated with the $(u|u+v)$- and $(u+v+w|2u+v|u)$-constructions. More generally, it was conjectured in [5, Section IV.D] that for any prime p a family ('Main-Sequence') $\mathcal{MS}_p$ codes over $\mathbb{F}_p$ 'having properties similar to those of the binary $\mathcal{RM}$-codes' would be obtained using a construction with associated upper-triangular $p \times p$ $\mathbb{F}_p$-matrix $MS_p = [\binom{p-i}{j-1} \bmod p]$. A $(u+v|u-v)$-construction (see [12, Theorem 6]) has also been applied to construct new codes in [4] and generalizations of Turyn's $(a+x|b+x|a+b+x)$-construction appear in a study of quasi-cyclic codes in [6].

We define *matrix-product codes* which include the above as special cases. The matrix-product code $C = [C_1 \ \cdots \ C_M] \cdot A$ consists of all matrix products $[c_1 \ \cdots \ c_M] \cdot A$ where $c_i \in C_i$ and A is an $M \times N$ matrix over $\mathbb{F}_q$. Here $M \leq N$ and C_i is $(n, |C_i|, d_i)$ code over $\mathbb{F}_q$ for $i = 1, \ldots, M$. We show that $|C| = |C_1| \cdots |C_M|$ if A has a right inverse and $\mathrm{d}(C) \geq \min\{Nd_1, \ldots, (N-M+1)d_M\}$, provided A is 'non-singular by columns (NSC)'; see Definition 3.1 for precise details. We show that the generalized Reed-Muller ($\mathcal{GRM}$)-codes (which are not equivalent to the p-ary Reed-Muller codes of [7]) are iterative NSC matrix-product codes, thus generalizing the iterative construction of $\mathcal{RM}$-codes and the iterative description of their generator and parity check matrices. Our approach based on Linear Algebra gives a new proof of the minimum distance of $\mathcal{GRM}$-codes (see Theorem 3.7), which is simpler than [1, Corollary 5.5.4]. We also show that MS_p is an NSC matrix, and in fact our proof of Theorem 3.7 is valid for any iterative 'triangular' NSC matrix-product code. Thus we also obtain the minimum distance of the 'Main Sequence Codes'.

In Section 6 we show that for square matrices, the dual of an NSC matrix-product code is an explicit NSC matrix-product code. This yields $\mathrm{d}(C^{\perp})$, see Theorem 6.6. In Section 7 we show that NSC matrix-product codes are generalized concatenated codes, as was already known for codes obtained by the $(u|u+v)$- and $(u+v+w|2u+v|u)$-constructions. Thus in particular $\mathcal{GRM}$-codes are generalized concatenated codes.

Viewing $\mathcal{GRM}$-codes as iterative NSC matrix-product codes may be useful in studying other aspects of these codes. For example, it follows that $\mathcal{GRM}$-codes are decomposable and hence can be decoded by multistage decoding in the terminology of [3]. Studying matrix-product codes using e.g. [8] may yield interesting codes over finite rings.

A preliminary version of this paper was presented at the 23^{rd} Australasian Conference on Combinatorial Mathematics and Combinatorial Computing, July 1998 in Brisbane.

Conventions: Throughout this paper, p is a fixed prime and q denotes a prime power; J_N the elementary matrix formed by reversing the rows of I_N, the $N \times N$ identity matrix. When N is understood we put $I = I_N$ and $J = J_N$.

2 Matrix-product codes

2.1 First steps

DEFINITION 2.1 *Let $A = [a_{ij}]$ be an $M \times N$ matrix A with entries in $\mathbb{F}_q$ and let $C_1, \ldots, C_M$ be codes of length n over $\mathbb{F}_q$. The* **matrix-product code** *$[C_1 \ \cdots \ C_M] \cdot A$ is the set of all matrix products $[c_1 \ \cdots \ c_M] \cdot A$, where $c_i \in C_i$ is an $n \times 1$ column vector for $i = 1, \ldots, M$.*

We shall also say that a code C over $\mathbb{F}_q$ is a **matrix-product code** if $C = [C_1 \ \cdots \ C_M] \cdot A$ for commensurate codes $C_1, \ldots, C_M$ and matrix A. The codewords of $[C_1 \ \cdots \ C_M] \cdot A$ are $n \times N$ matrices

$$c = \begin{bmatrix} c_{11}a_{11} + \cdots + c_{1M}a_{M1} & \cdots & c_{11}a_{1N} + \cdots + c_{1M}a_{MN} \\ \vdots & \ddots & \vdots \\ c_{n1}a_{11} + \cdots + c_{nM}a_{M1} & \cdots & c_{n1}a_{1N} + \cdots + c_{nM}a_{MN} \end{bmatrix}$$

and we regard $[C_1 \ \cdots \ C_M] \cdot A$ as a code of length nN by reading the entries of the matrix in column-major order: for $1 \le k \le nN$, $c_k = \sum_{i=1}^{M} c_{hi}a_{ij}$ where $h-1 = (k-1) \bmod n$ and $1 \le j \le N$.

We begin with a number of examples:

EXAMPLE 2.2 *The matrices*

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix},$$

give the $(u|u+v)$- and $(u+v+w|2u+v|u)$-constructions respectively.

EXAMPLE 2.3 *Let $q = p$ and MS_p be the $p \times p$ matrix with entries $(MS_p)_{ij} = \binom{p-i}{j-1} \bmod p$, let*

$$\mathcal{M}S_p(r,0) = \begin{cases} \{0\} & \text{if } r < 0 \\ \mathbb{F}_q & \text{if } r \ge 0 \end{cases}$$

and for $m \ge 1$, let $\mathcal{M}S_p(r,m) = [\mathcal{M}S_p(r,m-1) \ \cdots \ \mathcal{M}S_p(r-p+1,m-1)] \cdot MS_p$. For $p = 2$, MS_2 is the $(u|u+v)$ matrix and $\mathcal{M}S_2(r,m) = \mathcal{RM}(r,m)$. For $p = 3$, MS_p is the $(u+v+w|2u+v|u)$ matrix and we have the ternary 'Main Sequence' codes of [5].

EXAMPLE 2.4 *For $q = 3$, the matrix*

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

gives the $(u+v|u-v)$-construction.

EXAMPLE 2.5 *If $q = 2$ and*

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

then $[C_1\ C_1\ C_2]\cdot A$ *is Turyn's* $[a+x|b+x|a+b+x]$*-construction.*

EXAMPLE 2.6 *The code* $[C_1,\ \cdots\ , C_M]\cdot I_M$ *is the 'direct sum' of* $C_1,\ldots,C_M$*, [9, p. 76]. If* C_1 *and* C_2 *are linear with* $C_1\cap C_2=\{(0\cdots 0)\}$ *and* $A=[11]^T$ *then* $[C_1\ C_2]\cdot A$ *is the vector space direct sum of* C_1 *and* C_2*.*

In Section 5, we shall show that the generalised Reed-Muller codes $\mathcal{GRM}(r,m)$ are iterative matrix-product codes via a certain matrix GRM_q.

If $C_1,\ldots,C_M$ are linear with generator matrices $G_1,\ldots,G_M$ respectively then $[C_1\ \cdots\ C_M]\cdot A$ is linear with generator matrix

$$G=\begin{bmatrix} G_1a_{11} & \cdots & G_1a_{1N}\\ \vdots & \ddots & \vdots\\ G_Ma_{M1} & \cdots & G_Ma_{MN}\end{bmatrix}.$$

We shall need to discuss codes arising from row and column permutations of A; we say that A_ρ is a row permutation of $A=[a_{ij}]$ if ρ permutes $\{1,\ldots,M\}$ and $A_\rho=[a_{\rho(i)j}]$.

EXAMPLE 2.7 *Let* ρ *interchange the rows of* MS_2*,* $C_1=\mathbb{F}_2$ *and* $C_2=\{0\}$*. Then* $[C_1\ C_2]\cdot MS_2=\mathcal{RM}(0,1)=\{00,11\}$ *whereas* $[C_1\ C_2]\cdot(MS_2)_\rho=\{00,01\}=[C_2\ C_1]\cdot MS_2$*. Thus matrix-product codes depend on the order of the codes and* $[C_1\ C_2]\cdot A_\rho$ *need not be equivalent to* $[C_1\ C_2]\cdot A$*.*

A column permutation A_κ of A is defined similarly. The following is immediate:

PROPOSITION 2.8 *(i) If* A_ρ *is a row permutation of* A*, then* $[C_1\ \cdots\ C_M]\cdot A=[C_{\rho(1)}\ \cdots\ C_{\rho(M)}]\cdot A_\rho$

(ii) If A_κ *is a column permutation of* A *then* $[C_1\ \cdots\ C_M]\cdot A_\kappa$ *is equivalent to* $[C_1\ \cdots\ C_M]\cdot A$*.*

2.2 $|[C_1\ \cdots\ C_M]\cdot A|$

Here we determine $|[C_1\ \cdots\ C_M]\cdot A|$. Recall that a right inverse of A is an $N\times M$ matrix A^{-1} such that $A\cdot A^{-1}=I_M$. In this case we say that A is **non-singular**. We have $MS_2^{-1}=MS_2$ and

$$MS_3^{-1}=\begin{bmatrix}0&0&1\\0&1&-1\\1&-2&-1\end{bmatrix}.$$

In fact, it follows from Proposition 5.12 that $MS_p^{-1}=J\cdot GRM_p$, where J denotes the elementary matrix formed by reversing the rows of an identity matrix. For the $(u+v|u-v)$ matrix, $A^{-1}=\frac{1}{2}A$ if 2 is invertible.

Note that a necessary condition for A to have a right inverse is that $M\le N$, *so from now on we assume that* $M\le N$. Let us write $A(1,\ldots,M)$ for the matrix consisting of the first M columns

of A. Then if $A(1,\ldots,M)$ is non-singular with inverse $A(1,\ldots,M)^{-1}$, the $N \times M$ matrix whose first M rows are $A(1,\ldots,M)^{-1}$ and whose last $N-M$ rows are zero is a right inverse for A.

Throughout, if A is non-singular then A^{-1} denotes a right inverse of A.

PROPOSITION 2.9 *If a matrix consisting of some M columns of A is non-singular then*

$$|[C_1 \ \cdots \ C_M] \cdot A| = |C_1| \cdots |C_M|.$$

PROOF. By Proposition 2.8, we can assume that $A(1,\ldots,M)$ is non-singular. It is sufficient to show that $[\ \cdots\ ] \cdot A : C_1 \times \cdots \times C_M \to [C_1 \ \cdots \ C_M] \cdot A$ is 1-1. This is almost immediate, since if

$$[c_1 \ \cdots \ c_M] \cdot A = [c'_1 \ \cdots \ c'_M] \cdot A,$$

multiplying both sides on the right by A^{-1} gives $[c_1 \ \cdots \ c_M] = [c'_1 \ \cdots \ c'_M]$. □

If A is as in Example 2.5,

$$A^{-1} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$

so that $|[C_1 C_1 C_2] \cdot A| = |C_1|^2 |C_2|$.

3 Non-singular by columns matrices

This section discusses a strictly stronger condition than non-singularity which is required for estimating the minimum distance of matrix-product codes in Theorem 3.7 below.

For $1 \le t \le M$ we write A_t for the matrix consisting of the first t rows of A and for $1 \le j_1 < \cdots < j_t \le N$, we write $A(j_1,\ldots,j_t)$ for the $t \times t$ matrix consisting of columns $j_1,\ldots,j_t$ of A_t.

DEFINITION 3.1 *We call A* **non-singular by columns (NSC)** *if $A(j_1,\ldots,j_t)$ is non-singular for each $1 \le t \le M$ and $1 \le j_1 < \cdots < j_t \le N$.*

The matrices of Example 2.2 are NSC. It is clear that an NSC matrix is non-singular; however the matrix of Example 2.5 is non-singular but is not NSC. We shall say that a matrix-product code is NSC if its matrix is NSC. Thus Reed-Muller codes are iterative NSC matrix-product codes.

EXAMPLE 3.2 *Let $\mathbb{F}_q = \{\alpha_1,\ldots,\alpha_q\}$. For $1 \le M \le q$ the Vandermonde matrix*

$$V_M = \begin{bmatrix} 1 & \cdots & 1 \\ \alpha_1 & \cdots & \alpha_q \\ \vdots & \ddots & \vdots \\ \alpha_1^{M-1} & \cdots & \alpha_q^{M-1} \end{bmatrix}$$

is an NSC matrix, as is $V_M(j_1, \ldots, j_N)$ *for any* $M \leq N \leq q$ *and* $1 \leq j_1 < \cdots < j_N \leq q$. *Thus there exist NSC* $M \times N$ *matrices over* $\mathbb{F}_q$ *for all* $1 \leq M \leq N \leq q$.

We shall see in Section 5.2 that the 'Main Sequence Codes' and the generalised Reed-Muller codes are iterative NSC matrix-product codes.

We conclude this subsection with the possible values of M and $N \geq M$ for which there is an $M \times N$ NSC matrix over $\mathbb{F}_q$. First we note that for $M = 1$ there is no restriction on N, since the $1 \times N$ all 1 vector is clearly NSC. For $M \geq 2$ however, there is a severe restriction.

PROPOSITION 3.3 *For* $M \geq 2$ *there is an NSC* $M \times N$ *matrix over* $\mathbb{F}_q$ *if and only if* $M \leq N \leq q$.

PROOF. Example 3.2 demonstrates the sufficiency. Let A be a $2 \times N$ NSC matrix. We assume that $N \geq q + 1$ and derive a contradiction. We know that there are no zeroes in the first row of A and at most one in the second row, for otherwise A is not NSC. Without loss of generality we assume that $a_{22}, \ldots, a_{2N}$ are non-zero. For $2 \leq j \leq N$ we put $a_{1j} = \alpha^{r_j}$ and $a_{2j} = \alpha^{s_j}$ where α is a primitive element of $\mathbb{F}_q$. Then by hypothesis,

$$\begin{vmatrix} a_{1j} & a_{1k} \\ a_{2j} & a_{2k} \end{vmatrix}$$

is non-zero for $2 \leq j < k \leq N$, which is to say

$$r_j + s_k \not\equiv r_k + s_j \mod (q-1) \quad \text{for } 2 \leq j < k \leq N. \tag{1}$$

In particular $r_2 \not\equiv r_k - s_k + s_2$ for any $3 \leq k \leq N$. Thus $r_k - s_k + s_2$ takes at most $q-2$ different values $(\mathrm{mod}(q-1))$ as k takes at least $q-1$ values from 3 to $N \geq q+1$. Thus there exist k_1 and k_2, $3 \leq k_1 < k_2 \leq N$, such that

$$r_{k_1} - s_{k_1} + s_2 \equiv r_{k_2} - s_{k_2} + s_2 \mod (q-1),$$

which implies that $r_{k_1} + s_{k_2} \equiv r_{k_2} + s_{k_1}$ $(\mathrm{mod}(q-1))$, contradicting (1). □

It follows that no row permutation of the $(a + x | b + x | a + b + x)$ matrix can be NSC (as can be easily checked directly).

REMARK 3.4 *In Section 7 we shall see that NSC matrices can be characterised as generator matrices for certain MDS codes. Thus, in view of the Main conjecture for MDS codes, it is not surprising that the possible size of an NSC matrix is restricted by the size of the field over which it is defined.*

3.1 Triangular matrices

Recall that A is an upper-triangular matrix if $a_{ij} = 0$ for all $i > j$. A column permutation of an NSC matrix is an important special case in Theorem 3.7(iii), so we call a matrix **triangular** if it

is a column permutation of an upper-triangular matrix. Clearly MS_p is upper-triangular for all p, but the $(u+v|u-v)$ matrix is not triangular.

We shall see below that MS_p is an NSC matrix over $\mathbb{F}_p$ for each p. We shall also see that there are NSC triangular $q \times q$ matrices—and hence NSC triangular $M \times N$ matrices for all $1 \leq M \leq N \leq q$—over $\mathbb{F}_q$ for each q.

PROPOSITION 3.5 *A triangular NSC matrix has exactly $i-1$ zeroes in row i for $1 \leq i \leq M$ and no NSC matrix can have more.*

PROOF. If row i of A has more than $i-1$ zero entries then A is not NSC, since if $a_{ij_1}, \ldots, a_{ij_i}$ are zero then $\det A(j_1, \ldots, j_i) = 0$. □

We also have

LEMMA 3.6 *If A is triangular then $J \cdot (A^{-1})^T$ is triangular.*

PROOF. If A is triangular then $A \cdot P$ is upper-triangular for some permutation matrix P. Thus $(A \cdot P)^{-1} = P^T \cdot A^{-1}$ is upper-triangular so that $(P^T \cdot A^{-1})^T = (A^{-1})^T \cdot P$ is lower-triangular and $J(A^{-1})^T \cdot P \cdot J$ is upper-triangular. Hence

$$J \cdot (A^{-1})^T = J \cdot (A^{-1})^T \cdot (P \cdot J) \cdot (P \cdot J)^T$$

is triangular since $(P \cdot J)^T$ is a permutation matrix. □

3.2 A minimum distance theorem

THEOREM 3.7 *If A is NSC and $C = [C_1 \ \cdots \ C_M] \cdot A$ then*

(i) $|C| = |C_1| \cdots |C_M|$

(ii) $\mathrm{d}(C) \geq d^* = \min\{Nd_1, (N-1)d_2, \ldots, (N-M+1)d_M\}$

(iii) if A is also triangular then $\mathrm{d}(C) = d^*$.

PROOF. The first part follows from Proposition 2.9 since an NSC matrix is non-singular. In particular C consists of a single codeword, and hence has minimum distance ∞, if and only if each of $C_1, \ldots, C_M$ does, so that the result follows in this case.

For the rest of the proof we take $|C| > 1$. Take distinct codewords c and c' in C. Then $c = [c_1 \ \cdots \ c_M] \cdot A$ and $c' = [c'_1 \ \cdots \ c'_M] \cdot A$ for distinct $[c_1 \ \cdots \ c_M]$ and $[c'_1 \ \cdots \ c'_M]$. We wish to show that $\mathrm{d}(c, c') \geq d^*$ i. e. that

$$c_{h1}a_{1j} + \cdots + c_{hm}a_{mj} \neq c'_{h1}a_{1j} + \cdots + c'_{hm}a_{mj} \tag{2}$$

for at least d^* values of h and j.

Put $t = \max\{i : c_i \neq c'_i\}$. Then (2) holds if $c_{h1}a_{1j} + \cdots + c_{ht}a_{tj} \neq c'_{h1}a_{1j} + \cdots + c'_{ht}a_{tj}$. We show that if $c_{ht} \neq c'_{ht}$ then $c_{h1}a_{1j} + \cdots + c_{ht}a_{tj} \neq c'_{h1}a_{1j} + \cdots + c'_{ht}a_{tj}$ for at least $(N - t + 1)$ values of j between 1 and N. Since $c_{ht} \neq c'_{ht}$ for at least d_t values of h between 1 and n, it follows that $\mathrm{d}(c, c') \geq (N - t + 1)d_t$.

So take h with $c_{ht} \neq c'_{ht}$. To obtain a contradiction we assume that $c_{h1}a_{1j} + \cdots + c_{ht}a_{tj} = c'_{h1}a_{1j} + \cdots + c'_{ht}a_{tj}$ for at least t values of j, $1 \leq j_1 < j_2 < \cdots < j_t \leq N$, say. Then

$$\begin{array}{ccccccc} (c_{h1} - c'_{h1})a_{1j_1} & + & \cdots & + & (c_{ht} - c'_{ht})a_{tj_1} & = & 0 \\ (c_{h1} - c'_{h1})a_{1j_2} & + & \cdots & + & (c_{ht} - c'_{ht})a_{tj_2} & = & 0 \\ \vdots & & \ddots & & \vdots & & \vdots \\ (c_{h1} - c'_{h1})a_{1j_t} & + & \cdots & + & (c_{ht} - c'_{ht})a_{tj_t} & = & 0 \end{array}$$

so that the linear system

$$\begin{bmatrix} x_1 & x_2 & \cdots & x_t \end{bmatrix} \begin{bmatrix} a_{1j_1} & \cdots & a_{1j_t} \\ a_{2j_1} & \cdots & a_{2j_t} \\ \vdots & \ddots & \vdots \\ a_{tj_1} & \cdots & a_{tj_t} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

has a non-trivial solution and the $t \times t$ coefficient matrix is singular. This matrix is however $A(j_1, \ldots, j_t)$, which by assumption is non-singular. Thus we have the required contradiction and $\mathrm{d}(c, c') \geq (N - t + 1)d_t \geq d^*$.

For part (iii), we can assume that A is upper-triangular by Proposition 2.8. We need only show that there are codewords at most d^* from each other. Let $(N - t + 1)d_t$ be the smallest value of the $(N - i + 1)d_i$ (so that in particular $d_t < \infty$). Let c and c' be codewords of $[C_1 \ \cdots \ C_M] \cdot A$ with $c_t, c'_t \in C_t$ such that $\mathrm{d}(c_t, c'_t) = d_t$ and $c_i = c'_i \in C_i$ for $i \neq t$. Then

$$\mathrm{d}(c \cdot A, c' \cdot A) = \mathrm{d}(c_t a_{tt}, c'_t a_{tt}) + \mathrm{d}(c_t a_{tt+1}, c'_t a_{tt+1}) + \cdots + \mathrm{d}(c_t a_{tN}, c'_t a_{tN}) \leq (N - t + 1)d_t.$$

□

For $p = 2, 3$, MS_p is triangular and NSC, so that MS_p-product codes have minimum distance $\min\{2d_1, d_2\}$ and $\min\{3d_1, 2d_2, d_3\}$ respectively, as expected.

EXAMPLE 3.8 *Let A be the $(u + v|u - v)$ matrix. Any ternary cyclic code C of even length can be written as $C = [C_1 \ C_2] \cdot A$ for certain codes C_1, C_2, [12, Theorem 6]. In Example 22.10,* loc. cit.*, we have* $\mathrm{d}(C) = \mathrm{d}(C_2) = 12$ *from Table 1,* loc. cit.*. Thus d^* is a tight lower-bound in Theorem 3.7 for matrix-product codes with non-triangular matrix. See also [4, Example 8.3].*

EXAMPLE 3.9 *Let* $q = 3$,

$$A = \begin{bmatrix} 1 & 2 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 2 \end{bmatrix},$$

which is NSC, C_1 *be the* $(3,2,2)$ *ternary parity-check code and let* C_2, C_3 *be the* $(3,1,3)$ *ternary repetition code. Theorem 3.7 gives* $d([C_1\ C_2\ C_3] \cdot A) \geq 3$. *In fact with* $c_1 = (000)^T$ *and* $c_2 = c_3 = (111)^T$, $[c_1\ c_2\ c_3] \cdot A = [(000)^T\ (222)^T\ (000)^T]$. *Again,* d^* *is a tight lower-bound in Theorem 3.7 for matrix-product codes with non-triangular matrix.*

REMARKS 3.10

1. *We can slightly strengthen Theorem 3.7 by noting that if some row permutation* A_ρ *of* A *is NSC then, applying the theorem to* $[C_{\rho(1)}\ \cdots\ C_{\rho(M)}] \cdot A_\rho$ *and using Proposition 2.8,*

$$\mathrm{d}([C_1\ \cdots\ C_M] \cdot A) \geq \min\{Nd_{\rho(1)}, (N-1)d_{\rho(2)}, \ldots, (N-M+1)d_{\rho(M)}\}.$$

2. *If the* i^{th} *row of* A *has strictly more than* $i-1$ *zero entries, then* A *is not NSC by Proposition 3.5; however* $\mathrm{d}([C_1\ \cdots\ C_M] \cdot A) \leq d^* - 1$.

3. *The statement of Theorem 3.7 would be the same if we just considered* $N \times N$ *matrices* A *and took* $C_{M+1}, \ldots, C_N$ *to be one-word codes.*

4. *Ordering* $C_1, \ldots, C_M$ *such that* $d_i \leq d_j$ *if* $i \leq j$ *ensures that* d^* *is maximised. To see this let* $(N-t+1)d_t$ *minimise the* $(N-i+1)d_i$. *If there is an* $s < t$ *such that* $d_s > d_t$ *then both* $(N-t+1)d_s$ *and* $(N-s+1)d_t$ *are strictly greater than* $(N-t+1)d_t$, *so that swapping the positions of* C_s *and* C_t *will not reduce* d^* *and will increase* d^* *unless there is* $t' \neq t$ *with* $(N-t'+1)d'_t = (N-t+1)d_t$.

5. *Let* A *be the* $(a+x|b+x|a+b+x)$ *matrix. Since no row permutation of* A *is NSC, so we cannot apply Theorem 3.7 or Remark 1 to underbound its minimum distance. (It is known that in general there is no simple formula for the minimum distance of codes obtained by the* $(a+x|b+x|a+b+x)$*-construction, [9, p. 587].)*

4 NSC and matrix operations

We now give some examples to show that matrix operations which preserve NSC are quite special. One particular operation (hinted at in Lemma 3.6) will be of particular interest in discussing the dual of a matrix-product code in Section 6.

Obviously a non-zero scalar multiple of an NSC matrix is NSC. Being NSC is clearly independent of the ordering of the columns, but is dependent on the ordering of the rows (consider MS_2). The transpose of an NSC matrix need not be NSC (consider MS_2) and the product of two NSC matrices need not be NSC (since $MS_2^{-1} = MS_2$ and $MS_2 \cdot MS_2^{-1} = I$).

EXAMPLE 4.1 *Let A be as in Example 3.9. Then A is NSC but*

$$A^{-1} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 2 & 2 \\ 0 & 2 & 1 \end{bmatrix}$$

so the inverse of an NSC matrix need not be NSC.

We note that $J \cdot B$ is B with its rows reversed and that for MS_2 and Example 3.9, $J \cdot (A^{-1})^T$ is NSC. We shall now show that this is true in general. The proof uses the following standard result e. g. [2, p. 198].

LEMMA 4.2 *If X and Y are square matrices, X non-singular, such that*

$$X = \begin{bmatrix} Y & Y_1 \\ Y_2 & Z \end{bmatrix}$$

for some matrices Y_1, Y_2, Z of appropriate size (Z being square) and

$$X^{-1} = \begin{bmatrix} Z' & Y_1' \\ Y_2' & Y' \end{bmatrix}$$

where Y' is the same size as Z then $\det(Y) = \det(Y')\det(X)$.

LEMMA 4.3 *If A is a square NSC matrix then $J \cdot (A^{-1})^T$ is NSC.*

PROOF. Let $B = J \cdot (A^{-1})^T$. We need to show that $B(j_1, \ldots, j_t)$ is non-singular for each $1 \leq t \leq N$ and $1 \leq j_1 < \cdots < j_t \leq N$. If $(A^{-1})_{ij} = \beta_{ij}$ then $B_{ij} = \beta_{j(N-i+1)}$ and so

$$B(j_1, \ldots, j_t) = \begin{bmatrix} \beta_{j_1 N} & \cdots & \beta_{j_t N} \\ \vdots & \ddots & \vdots \\ \beta_{j_1 N-t+1} & \cdots & \beta_{j_t N-t+1} \end{bmatrix}.$$

We put $\{1, \ldots, N\} \setminus \{j_1, \ldots, j_t\} = \{k_1, \ldots, k_{N-t}\}$ and

$$A_\kappa = \begin{bmatrix} a_{1k_1} & \cdots & a_{1k_{N-t}} & a_{1j_1} & \cdots & a_{1j_t} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{Nk_1} & \cdots & a_{Nk_{N-t}} & a_{Nj_1} & \cdots & a_{Nj_t} \end{bmatrix}.$$

Since A_κ is a column permutation of A it is NSC. Also

$$A_\kappa^{-1} = \begin{bmatrix} \beta_{k_1 1} & \cdots & \beta_{k_1 N} \\ \vdots & \ddots & \vdots \\ \beta_{k_{N-t} 1} & \cdots & \beta_{k_{N-t} N} \\ \beta_{j_1 1} & \cdots & \beta_{j_1 N} \\ \vdots & \ddots & \vdots \\ \beta_{j_t 1} & \cdots & \beta_{j_t N} \end{bmatrix}.$$

Now in Lemma 4.2 we take X to be A_κ, Y to be the first $N-t$ rows and columns of A_κ and Y' to be the last t rows and columns of A_κ^{-1}. Since A_κ is NSC we have that Y is non-singular and so Y' is non-singular. Also $B(j_1,\ldots,j_t) = J\cdot(Y')^T$ and so $B(j_1,\ldots,j_t)$ is non-singular and the lemma is proved. □

5 $\mathcal{G}RM$-codes are matrix-product codes

5.1 An iterative description of $\mathcal{G}RM$-codes

From now on we take $\mathbb{F}_q = \{\alpha_1,\ldots,\alpha_q\}$ where for q prime, $\alpha_i = i-1 \in \mathbb{Z}_q$ and order $\mathbb{F}_q$ by $\alpha_1 < \cdots < \alpha_q$.

We begin this section with a brief discussion of 'polynomial codes'. Put

$$E_q[X_1,\ldots,X_m] = \begin{cases} \mathbb{F}_q & \text{if } m=0 \\ \frac{\mathbb{F}_q[X_1,\ldots,X_m]}{(X_1^q-X_1,\ldots,X_m^q-X_m)} & \text{if } m\geq 1. \end{cases}$$

Let $m\geq 0$ and $\mathcal{P}$ a subspace of $E_q[X_1,\ldots,X_m]$. For $P\in\mathcal{P}$ we have the evaluation of P,

$$\mathrm{ev}(P) = (P(\gamma_1),\ldots,P(\gamma_{q^m})) \quad \text{where } \mathbb{F}_q^m = (\gamma_1,\ldots,\gamma_{q^m}).$$

Thus $\mathcal{P}$ gives rise to a length q^m code over $\mathbb{F}_q$, $\mathrm{ev}(\mathcal{P}) = \{\mathrm{ev}(P) : P\in\mathcal{P}\}$. Since no two polynomials of $E_q[X_1,\ldots,X_m]$ have the same evaluation there is often no need to distinguish between $\mathrm{ev}(\mathcal{P})$ and $\mathcal{P}$. Thus we refer to the code $\mathcal{P}$.

The ordering of the codewords of $\mathcal{P}$ is determined by the ordering of $\mathbb{F}_q^m$. Throughout $\mathbb{F}_q^m$ will be ordered lexicographically. Thus the k^{th} element of $\mathbb{F}_q^m$ is $(\alpha_{k_1+1},\ldots,\alpha_{k_m+1})$ where $\sum_{l=1}^m k_l q^{l-1}$ is the q-ary expansion of $k-1$ and the k^{th} symbol of $c(X_1,\ldots,X_m)\in\mathcal{P}$ is $c(\alpha_{k_1+1},\ldots,\alpha_{k_m+1})$.

For $P\in E_q[X_1,\ldots,X_m]$ we write $\deg(P)$ for the total degree of P. Then

$$\mathcal{G}RM_q(r,m) = \{P\in E_q[X_1,\ldots,X_m] : \deg(P)\leq r\}.$$

In particular for $r<0$, $\mathcal{G}RM_q(r,m) = \{0\}$ and for $r\geq m(q-1)$, $\mathcal{G}RM_q(r,m) = E_q[X_1,\ldots,X_m]$. In the case $q=2$ lexicographic order of $\mathbb{F}_2^m$ gives the standard bit-ordering of $\mathcal{R}M$-codes.

We give a polynomial version of Definition 2.1 when A is a $q\times q$ matrix. For this we need a polynomial description of the point functions on $\mathbb{F}_q$. We note that the product of the distinct non-zero elements of a finite field is -1 (e. g. since $X^{q-1}-1 = \prod_{\alpha\in\mathbb{F}_q\setminus\{0\}}(X-\alpha)$) so for $1\leq j\leq q$ we can take

$$\chi_j(X) = -\frac{(X-\alpha_1)\cdots(X-\alpha_q)}{(X-\alpha_j)} = \begin{cases} 1 & \text{for } X=\alpha_j \\ 0 & \text{for } X=\alpha_k\neq\alpha_j. \end{cases}$$

Then we have

DEFINITION 5.1 (POLYNOMIAL VERSION OF MATRIX-PRODUCT CODE) *Given a $q \times q$ matrix A and q polynomial codes $C_1, \ldots, C_q \subseteq E_q[X_1, \ldots, X_{m-1}]$ we define $[C_1 \ \cdots \ C_q] \cdot A \subseteq E_q[X_1, \ldots, X_m]$ by*

$$[C_1 \ \cdots \ C_q] \cdot A = \left\{ \sum_{j=1}^{q} \chi_j(X_m) \sum_{i=1}^{q} c_i(X_1, \ldots, X_{m-1}) a_{ij} : c_1 \in C_1, \ldots, c_q \in C_q \right\}.$$

PROPOSITION 5.2 *For a $q \times q$ matrix A and codes $C_1, \ldots, C_q \subseteq E[X_1, \ldots X_{m-1}]$, Definitions 2.1 and 5.1 are equivalent.*

PROOF. We show that the k^{th} symbol of $c \in [C_1 \ \cdots \ C_q] \cdot A$ does not depend on which Definition is used. We write c^k for the k^{th} symbol of c where $1 \leq k \leq q^m$. We put $n = q^{m-1}$ (the length of $C_1, \ldots, C_q$) and $k = (j-1)n + h$ for some $1 \leq j \leq q$ and $1 \leq h \leq n$. Also we write $h - 1 = \sum_{l=1}^{m-1} h_l q^{l-1}$ so that $k_l = h_l$ for $0 \leq l \leq m-1$ and $k_m = j - 1$.

Firstly if $c = [c_1 \ \cdots \ c_q] \cdot A$ is as in Definition 2.1 then $c^k = \sum_{j=1}^{q} c_{hi} a_{ij}$. Now take

$$c = \sum_{j=1}^{q} \chi_j(X_m) \sum_{i=1}^{q} c_i(X_1, \ldots, X_{m-1}) a_{ij}$$

as in Definition 5.1. For $1 \leq i \leq q$, $c_{hi} = c_i(\alpha_{h_1+1}, \ldots, \alpha_{h_{m-1}+1})$ and

$$c^k = c(\alpha_{h_1+1}, \ldots, \alpha_{h_{m-1}+1}, \alpha_j) = \sum_{j'=1}^{q} \chi_{j'}(\alpha_j) \sum_{i=1}^{q} c_i(\alpha_{h_1+1}, \ldots, \alpha_{h_{m-1}+1}) a_{ij'} = \sum_{i=1}^{q} c_{hi} a_{ij}$$

□

We generalize the iterative description of $\mathcal{RM}$-codes by showing that for $m \geq 1$, $\mathcal{GRM}_q(r, m) = [\mathcal{GRM}_q(r, m-1) \ \cdots \ \mathcal{GRM}_q(r-q+1, m-1)] \cdot A$ for a certain $q \times q$ matrix A.

The matrix we use will need a 'choice function' defined on $\mathbb{F}_q \times \mathbb{F}_q$ which generalizes $\binom{j}{i} \bmod p$. The following notation will be useful here and later. For $0 \leq k \leq q-1$ we put

$$\overline{X}^k = (X - \alpha_1) \cdots (X - \alpha_k) \quad \text{so that} \quad \overline{\alpha_j}^k = (\alpha_j - \alpha_1) \cdots (\alpha_j - \alpha_k).$$

Also for $1 \leq i \leq q$ we put

$$\binom{X}{\alpha_i} = \frac{\overline{X}^{i-1}}{\overline{\alpha_i}^{i-1}} \quad \text{so that} \quad \binom{\alpha_j}{\alpha_i} = \frac{(\alpha_j - \alpha_1) \cdots (\alpha_j - \alpha_{i-1})}{(\alpha_i - \alpha_1) \cdots (\alpha_i - \alpha_{i-1})}.$$

We note that if $k = 0$ then $\overline{\alpha_j}^k = 1$ and if $i = 1$ or $i = j$ then $\binom{\alpha_j}{\alpha_i} = 1$. Also $\overline{\alpha_j}^{i-1} = \binom{\alpha_j}{\alpha_i} = 0$ if and only if $1 \leq j \leq i-1$.

DEFINITION 5.3 *We put*

$$GRM_q = \begin{bmatrix} \binom{\alpha_1}{\alpha_1} & \binom{\alpha_2}{\alpha_1} & \cdots & \binom{\alpha_q}{\alpha_1} \\ \binom{\alpha_1}{\alpha_2} & \binom{\alpha_2}{\alpha_2} & \cdots & \binom{\alpha_q}{\alpha_2} \\ \vdots & \vdots & \ddots & \vdots \\ \binom{\alpha_1}{\alpha_q} & \binom{\alpha_2}{\alpha_q} & \cdots & \binom{\alpha_q}{\alpha_q} \end{bmatrix}.$$

We note that GRM_q is upper-triangular and has 1's on its leading diagonal. In particular it is non-singular; it is the matrix we use in our iterative description of $\mathcal{G}RM_q$-codes. Polynomials of the form

$$\frac{(X-\alpha_i)\cdots(X-\alpha_q)}{(X-\alpha_j)} \quad \text{where} \quad 1 \le i \le j \le q$$

will occur in the proof that the description is valid. We note that for $0 \le t \le q-i$ the coefficient of X^{q-i-t} in this polynomial is the sum of all products $(-1)^t \alpha_{j_1} \cdots \alpha_{j_t}$ such that $j_1, \ldots, j_t \in \{i, \ldots, q\} \setminus \{j\}$. For $1 \le i \le j \le q$ and $0 \le t \le q-i$ we put

$$S_i(t) = \sum_{j_1,\ldots,j_t \in \{i,\ldots,q\}} \alpha_{j_1} \cdots \alpha_{j_t} \quad \text{and} \quad S_{ij}(t) = \sum_{j_1,\ldots,j_t \in \{i,\ldots,q\}\setminus\{j\}} \alpha_{j_1} \cdots \alpha_{j_t}.$$

Then

LEMMA 5.4 *For $1 \le i \le j \le q$ and $0 \le t \le q-1-i$, $S_{ij}(t) = \sum_{k=0}^{t} (-\alpha_j)^k S_i(t-k)$.*

PROOF. We note that $S_i(t+1) = S_{ij}(t+1) + \alpha_j S_{ij}(t)$. The proof is then a straightforward induction on t. □

We also use

LEMMA 5.5 *If $\deg(P) \le q-2$ then $\sum_{j=1}^{q} P(\alpha_j) = 0$.*

PROOF. It suffices to show that $\sum_{j=1}^{q} \alpha_j^k = 0$ for $0 \le k \le q-2$. For $k=0$, $\sum_{j=1}^{q} 1 = 0$, so we take $1 \le k \le q-2$. Now it suffices to show that $\sum_{l=0}^{q-2} \alpha^{lk} = 0$ for a primitive element α of $\mathbb{F}_q$. To see this we have $(1-\alpha^k)\sum_{l=0}^{q-2} \alpha^{lk} = 1 - \alpha^{(q-1)k} = 0$ and $1-\alpha^k \ne 0$ since $1 \le k \le q-2$. □

THEOREM 5.6 *The $\mathcal{G}RM$-codes can be iteratively defined by*

$$\mathcal{G}RM(r,0) = \begin{cases} \{0\} & \text{if } r < 0 \\ \mathbb{F}_q & \text{if } r \ge 0 \end{cases}$$

and for $m \ge 1$

$$\mathcal{G}RM_q(r,m) = [\mathcal{G}RM_q(r,m-1) \cdots \mathcal{G}RM_q(r-q+1,m-1)] \cdot GRM_q.$$

PROOF. Only the $m \ge 1$ part of the statement requires proof. So we take $m \ge 1$ and put $C = [\mathcal{G}RM_q(r,m-1) \ \cdots \ \mathcal{G}RM_q(r-q+1,m-1)] \cdot GRM_q$. Since GRM_q is invertible, Proposition 2.9 implies that $\dim(C) = \sum_{i=1}^{q} \dim(\mathcal{G}RM_q(r+1-i,m-1))$. Also $\mathcal{G}RM_q(r,m)$ is spanned by monomials of the form $\underline{X} X_m^{i-1}$ where $1 \le i \le q$ and $\underline{X} \in \mathcal{G}RM_q(r+1-i,m-1)$ so that

$$\dim(\mathcal{G}RM_q(r,m)) = \sum_{i=1}^{q} \dim(\mathcal{G}RM_q(r+1-i,m-1)) = \dim(C).$$

Thus it suffices to show that $C \subseteq \mathcal{GRM}_q(r,m)$ i. e. that $\deg(c) \leq r$ for all $c \in C$.

Now from Definition 5.1 if $c \in C$ then

$$c = \sum_{j=1}^{q} -\frac{(X_m - \alpha_1)\cdots(X_m - \alpha_q)}{(X_m - \alpha_j)} \sum_{i=1}^{j} \binom{\alpha_j}{\alpha_i} c_i,$$

where $c_i \in \mathcal{GRM}_q(r+1-i, m-1)$. Reversing the order of summation we get

$$c = -\sum_{i=1}^{q} \binom{X_m}{\alpha_i} c_i \left(\sum_{j=i}^{q} \overline{\alpha_j}^{i-1} \frac{(X_m - \alpha_i)\cdots(X_m - \alpha_q)}{(X_m - \alpha_j)} \right).$$

Since $\deg(\binom{X_m}{\alpha_i} c_i) \leq i - 1 + (r + 1 - i) = r$ it is sufficient to show that for $1 \leq i \leq q$

$$\sum_{j=i}^{q} \overline{\alpha_j}^{i-1} \frac{(X_m - \alpha_i)\cdots(X_m - \alpha_q)}{(X_m - \alpha_j)} = \sum_{t=0}^{q-i} (-1)^t \left(\sum_{j=i}^{q} \overline{\alpha_j}^{i-1} S_{ij}(t) \right) X_m^{q-i-t}$$

has degree 0 i. e. that

$$\sum_{j=i}^{q} \overline{\alpha_j}^{i-1} S_{ij}(t) = \sum_{j=0}^{q} \overline{\alpha_j}^{i-1} S_{ij}(t) = 0$$

for $0 \leq t \leq q - 1 - i$.

Now by Lemma 5.4

$$\sum_{j=1}^{q} \overline{\alpha_j}^{i-1} S_{ij}(t) = \sum_{j=1}^{q} \overline{\alpha_j}^{i-1} \left(\sum_{k=0}^{t} (-\alpha_j)^k S_i(t-k) \right) = \sum_{k=0}^{t} (-1)^k S_i(t-k) \sum_{j=1}^{q} \alpha_j^k \overline{\alpha_j}^{i-1}$$

which is zero for $0 \leq t \leq q - 1 - i$ by Lemma 5.5 since for $0 \leq k \leq t$, $P(X) = X^k \overline{X}^{i-1}$ has degree $k + i - 1 \leq t + i - 1 \leq q - 2$. □

REMARKS 5.7 *1. It is clear from the proof of Theorem 5.6 that we could also take* $(GRM_q)_{ij} = \overline{\alpha_j}^{i-1}$. *The choice of* $(GRM_q)_{ij} = \binom{\alpha_j}{\alpha_i}$ *means that* $(GRM_q)_{ii} = 1$ *for* $1 \leq i \leq q$.

2. The identity $\dim(\mathcal{GRM}_q(r,m)) = \sum_{i=1}^{q} \dim(\mathcal{GRM}_q(r+1-i, m-1)$ *used in the proof of Theorem 5.6 also follows from the fact that if* $(1 + z + \cdots + z^{q-1})^m = \sum_{l=0}^{m(q-1)} P_l z^l$ *then* $\dim(\mathcal{GRM}_q(r,m)) = \sum_{l=0}^{r} P_l$ *(cf. [9, Section 13.3], [1, Theorem 5.4.1] and [11, Exercise 13(a) p. 104]).*

Finally here we note that if $G_q(r+1-i, m-1)$ are generator matrices for $\mathcal{GRM}_q(r+1-i, m-1)$ where $1 \leq i \leq q$ then by Theorem 5.6

$$G_q(r,m) = \begin{bmatrix} G_q(r,m-1) & \cdots & G_q(r,m-1)\binom{\alpha_{q-1}}{\alpha_1} & G_q(r,m-1)\binom{\alpha_q}{\alpha_1} \\ 0 & \ddots & \vdots & \vdots \\ \vdots & \cdots & G_q(r-q+2) & G_q(r-q+2, m-1)\binom{\alpha_q}{\alpha_{q-1}} \\ 0 & \cdots & 0 & G_q(r-q+1, m-1) \end{bmatrix}$$

is a generator matrix for $\mathcal{GRM}_q(r,m)$.

5.2 GRM_q and MS_p are NSC

It is clear that GRM_q and MS_p are upper-triangular. We now show that they are also NSC. This will mean that we can apply Theorem 3.7 to determine the minimum distance of the corresponding codes in the next subsection.

PROPOSITION 5.8 *For $1 \leq t \leq q$ and $0 \leq j_1 < \cdots < j_t \leq q$,*

$$\begin{vmatrix} \binom{\alpha_{j_1}}{\alpha_1} & \cdots & \binom{\alpha_{j_t}}{\alpha_1} \\ \vdots & \ddots & \vdots \\ \binom{\alpha_{j_1}}{\alpha_t} & \cdots & \binom{\alpha_{j_t}}{\alpha_t} \end{vmatrix} = \prod_{1 \leq r < s \leq t} \frac{(\alpha_{j_s} - \alpha_{j_r})}{(\alpha_s - \alpha_r)}.$$

PROOF. This is similar to a proof for the Vandermonde determinant and is by induction on t. For $t = 1$ and $1 \leq j_1 \leq q$, both sides of the equation in the statement are 1. Thus we assume the statement holds for $t = u \leq q - 1$ and each $1 \leq j'_1 < \cdots < j'_u \leq q$. Take $1 \leq j_1 < \cdots < j_{u+1} \leq q$ and put

$$D(X) = \begin{vmatrix} \binom{\alpha_{j_1}}{\alpha_1} & \cdots & \binom{\alpha_{j_u}}{\alpha_1} & \binom{X}{\alpha_1} \\ \vdots & \ddots & \vdots & \vdots \\ \binom{\alpha_{j_1}}{\alpha_u} & \cdots & \binom{\alpha_{j_u}}{\alpha_u} & \binom{X}{\alpha_u} \\ \binom{\alpha_{j_1}}{\alpha_{u+1}} & \cdots & \binom{\alpha_{j_u}}{\alpha_{u+1}} & \binom{X}{\alpha_{u+1}} \end{vmatrix}.$$

We wish to show that $D(\alpha_{j_{u+1}}) = \prod_{1 \leq r < s \leq u+1} \frac{(\alpha_{j_s} - \alpha_{j_r})}{(\alpha_s - \alpha_r)}$.

Now D has degree u and zeroes $\alpha_{j_1}, \ldots, \alpha_{j_u}$. Thus,

$$D(X) = L_D \prod_{k=1}^{u} (X - \alpha_{j_k}),$$

where

$$L_D = \begin{vmatrix} \binom{\alpha_{j_1}}{\alpha_1} & \cdots & \binom{\alpha_{j_u}}{\alpha_1} \\ \vdots & \ddots & \vdots \\ \binom{\alpha_{j_1}}{\alpha_u} & \cdots & \binom{\alpha_{j_u}}{\alpha_u} \end{vmatrix} \prod_{k=1}^{u} \frac{1}{(\alpha_{u+1} - \alpha_k)},$$

is the leading coefficient of D. Thus by the inductive hypothesis

$$D(X) = \prod_{1 \leq r < s \leq u} \frac{(\alpha_{j_s} - \alpha_{j_r})}{(\alpha_s - \alpha_r)} \prod_{k=1}^{u} \frac{(X - \alpha_{j_k})}{(\alpha_{u+1} - \alpha_k)}.$$

and $D(\alpha_{j_{u+1}})$ is as required. □

COROLLARY 5.9 *GRM_q is NSC.*

REMARK 5.10 *It would be interesting to know if there are NSC $q \times q$ matrices over $\mathbb{F}_q$ other than GRM_q, the Vandermonde matrix and their $J \cdot ((\ )^{-1})^T$ transformations.*

We also use Proposition 5.8 to show that MS_p is NSC.

COROLLARY 5.11 *MS_p is NSC.*

PROOF. Since MS_p is NSC if and only if $MS_p \cdot J$ is NSC, it suffices to show that $MS_p \cdot J$ is NSC. Thus we need to show that for each $1 \le t \le p$ and each $0 \le j_1 < \cdots < j_t \le p-1$,

$$D'(j_1, \ldots, j_t) = \begin{vmatrix} \binom{p-1}{p-1-j_1} & \cdots & \binom{p-1}{p-1-j_t} \\ \binom{p-2}{p-1-j_1} & \cdots & \binom{p-2}{p-1-j_t} \\ \vdots & \ddots & \vdots \\ \binom{p-t}{p-1-j_1} & \cdots & \binom{p-t}{p-1-j_t} \end{vmatrix}$$

is non-zero. Since p is prime

$$\binom{p-r}{p-1-j_s} = \binom{p-1}{p-1-j_s}\binom{p-1}{r-1}^{-1}\binom{j_s}{r-1}$$

for each $1 \le s \le t$ and $1 \le r \le t$. Thus

$$D'(j_1, \ldots, j_t) = \prod_{s=1}^{t} \binom{p-1}{p-1-j_s}\binom{p-1}{s-1}^{-1} \begin{vmatrix} \binom{j_1}{0} & \cdots & \binom{j_t}{0} \\ \binom{j_1}{1} & \cdots & \binom{j_t}{1} \\ \vdots & \ddots & \vdots \\ \binom{j_1}{t-1} & \cdots & \binom{j_t}{t-1} \end{vmatrix},$$

since in the product on the right-hand side, the first term is independent of r and the second term is independent of s. Finally the right-hand side is non-zero for each $1 \le t \le p$ and $0 \le j_1 < \cdots < j_t \le p-1$ by Proposition 5.8. □

PROPOSITION 5.12 *$GRM_p^{-1} = MS_p \cdot J$.*

PROOF. We have

$$((MS_p \cdot J) \cdot GRM_p)_{ij} = \sum_{k=0}^{p-1} \binom{p-i}{p-1-k}\binom{j-1}{k} \equiv \binom{p-i+j-1}{p-1} \pmod{p}$$

by Vandermonde's identity, which is 0 if $j-i<0$ (since then $p-i+j-1<p-1$) or if $j-i>0$ (since then p divides the integer-valued $\binom{p-i+j-1}{p-1}$), and is 1 if $j=i$. □

5.3 The minimum distance of $\mathcal{G}RM$- and $\mathcal{M}S$-codes

We now use Theorem 3.7 to obtain a simple proof of the minimum distances of $\mathcal{G}RM_q(r,m)$ and $\mathcal{M}S_p(r,m)$. In fact, let $\mathcal{F}(r,m)$ be any family of codes over $\mathbb{F}_q$ defined for $m=0$ by

$$\mathcal{F}(r,0) = \begin{cases} \{0\} & \text{for } r<0 \\ \mathbb{F}_q & \text{for } r \ge 0 \end{cases}$$

and for $m \geq 1$ by $\mathcal{F}(r,m) = [\mathcal{F}(r,m-1) \ \cdots \ \mathcal{F}(r-q+1,m-1)] \cdot F$, where F is an NSC $q \times q$ triangular matrix over $\mathbb{F}_q$. (Recall that $\mathcal{G}RM$-codes are of this form by Theorem 5.6 and Corollary 5.9; $\mathcal{M}S$-codes are of this form by definition and Corollary 5.11.)

Clearly

$$\mathrm{d}(\mathcal{F}(r,m)) = \begin{cases} \infty & \text{for } r < 0 \\ 1 & \text{for } r \geq m(q-1). \end{cases}$$

PROPOSITION 5.13 *For $0 \leq r \leq m(q-1)$ write $r = Q(q-1)+S$ with $0 \leq S \leq q-2$. Then*

$$\mathrm{d}(\mathcal{F}(r,m)) = (q-S)q^{m-1-Q}.$$

PROOF. We first note that for $r = m(q-1)$, $S = 0$, $Q = m$ and $(q-S)q^{m-1-Q} = 1 = \mathrm{d}(\mathcal{F}(r,m))$. In particular the result holds for $m = 0$ and $0 \leq r \leq m(q-1)$. We assume that the result holds for $m = k$ and $0 \leq r' \leq k(q-1)$ and need to show that it holds for $m = k+1$ and $0 \leq r \leq (k+1)(q-1)-1$ (since we know it holds for $r = (k+1)(q-1)$).

So we take $0 \leq r \leq (k+1)(q-1)-1$ and write $r = Q(q-1)+S$ where $0 \leq S \leq q-2$. We know that

$$\mathrm{d}(\mathcal{F}(r,k+1)) = \min\{q\mathrm{d}(r,k), \ldots, \mathrm{d}(r-q+1,k)\}.$$

Thus $\mathrm{d}(\mathcal{F}(r,k+1))$ is no more than $(q-S)\mathrm{d}(\mathcal{F}(r-S,k))$ which is $(q-S)(q-0)q^{k-1-Q} = (q-S)q^{k-Q}$ since $0 \leq r-S \leq k(q-1)$. Thus we need to show that for $0 \leq j \leq q-1$, $(q-j)\mathrm{d}(\mathcal{F}(r-j,k)) \geq (q-S)q^{k-Q}$. For $r < j \leq q-1$ this is clearly true so we take $0 \leq j \leq \min\{r, q-1\}$. We write $r-j = Q_j(q-1)+S_j$.

Firstly we take $k(q-1) \leq r \leq (k+1)(q-1)-1$. We need to show that $(q-j)\mathrm{d}(\mathcal{F}(r-j,k)) \geq q-S$. For $0 \leq j \leq S$ this is clearly true. For $S+1 \leq j \leq \min\{r, q-1\}$ we have $Q_j = k-1$ and $S_j = S-j+q-1$ so that from the inductive assumption $(q-j)\mathrm{d}(\mathcal{F}(r,m)) = (q-j)(j-S+1)$ and

$$(q-j)(j-S+1)-(q-S) = (q-j)(j-S)-(j-S) = (q-j-1)(j-S) \geq 0 \tag{3}$$

since $S+1 \leq j \leq q-1$.

Next we take $0 \leq r \leq k(q-1)-1$. If $S+1 \leq j \leq \min\{r, q-1\}$ then $Q_j = Q-1$ and again $S_j = S-j+q-1$ and from the inductive assumption

$$(q-j)\mathrm{d}(\mathcal{F}(r-j,k)) = (q-j)(j-S+1)q^{k-Q}$$

which is at least $(q-S)q^{k-Q}$ by (3). If $0 \leq j \leq S$ then $Q_j = Q$ and $S_j = S-j$ and from the inductive assumption

$$\begin{aligned} (q-j)\mathrm{d}(\mathcal{F}(r-j,k)) &= (q-j)(q-S+j)q^{k-1-Q} \\ &= q(q-S)q^{k-1-Q} + qjq^{k-1-Q} - j(q-S+j)q^{k-1-Q} \\ &= (q-S)q^{k-Q} + j(S-j)q^{k-1-Q} \geq (q-S)q^{k-Q} \end{aligned}$$

since $0 \le S \le j$. $\square$

6 On the dual of $[C_1 \ \cdots \ C_M] \cdot A$

6.1 The dual when A is square

For linear codes $C_1, \ldots, C_M$ and a square matrix A we show that $([C_1 \ \cdots \ C_M] \cdot A)^\perp$ is also a matrix-product code.

Let A and B be $M \times N$ matrices and $C_1, \ldots, C_M, D_1, \ldots, D_M$ length n linear codes. Then $[C_1 \ \cdots \ C_M] \cdot A$ and $[D_1 \ \cdots \ D_M] \cdot B$ are linear, and are dual to each other if and only if $\dim([D_1 \ \cdots \ D_M] \cdot B) = Nn - \dim([C_1 \ \cdots \ C_M] \cdot A)$ and

$$\sum_{h=1}^{n} \sum_{j=1}^{N} \left(\sum_{i=1}^{M} c_{hi} a_{ij} \right) \left(\sum_{k=1}^{M} d_{hk} b_{kj} \right) = 0 \text{ for all } c_1 \in C_1, \ldots, c_m \in C_M, \ d_1 \in D_1, \ldots, d_M \in D_M.$$

Now

$$\sum_{h=1}^{n} \sum_{j=1}^{N} \left(\sum_{i=1}^{M} c_{hi} a_{ij} \right) \left(\sum_{k=1}^{M} d_{hk} b_{kj} \right) = \sum_{i=1}^{M} \sum_{k=1}^{M} \sum_{j=1}^{N} a_{ij} b_{kj} \sum_{h=1}^{n} c_{hi} d_{hk} = \sum_{i=1}^{M} \sum_{k=1}^{M} \sum_{j=1}^{N} a_{ij} b_{kj} c_i^T d_k.$$

Also $(A \cdot B^T)_{ik} = \sum_{j=1}^{N} a_{ij} b_{kj}$ so that

LEMMA 6.1 *For $N \times M$ matrices A and B and linear codes $C_1, \ldots, C_M, D_1, \ldots, D_M$ of length n over $\mathbb{F}_q$, $[C_1 \ \cdots \ C_M] \cdot A$ and $[D_1 \ \cdots \ D_M] \cdot B$ are dual codes if and only if*

$$\dim([D_1 \ \cdots \ D_M] \cdot B) = Nn - \dim([C_1 \ \cdots \ C_M] \cdot A)$$

and

$$\sum_{i=1}^{M} \sum_{k=1}^{M} (A \cdot B^T)_{ik} c_i^T d_k = 0 \quad \textit{for each } c_1 \in C_1, \ldots, c_M \in C_M \textit{ and } d_1 \in D_1, \ldots, d_M \in D_M.$$

We begin with the case that A is non-singular with right inverse A^{-1}. Then by Proposition 2.9, $\dim([C_1 \ \cdots \ C_M] \cdot A) = k_1 + \cdots + k_M$. Putting $B = (A^{-1})^T$ we get

$$\sum_{i=1}^{M} \sum_{k=1}^{M} (A \cdot B^T)_{ik} c_i^T d_k = \sum_{i=1}^{M} c_i^T d_i$$

which is zero for all $c_1 \in C_1, \ldots, c_M \in C_M$ and $d_1 \in D_1, \ldots, d_M \in D_M$ if we put $D_i = C_i^\perp$ for $1 \le i \le M$. Also B has right inverse A^T so by Proposition 2.9

$$\dim([C_1^\perp \ \cdots \ C_M^\perp] \cdot B]) = (n - k_1) + \cdots + (n - k_M) = Mn - (k_1 + \cdots + k_M).$$

Thus when $M = N$, i. e. when A is square, Lemma 6.1 implies that $[C_1^\perp \ \cdots \ C_M^\perp] \cdot B$ and $[C_1 \ \cdots \ C_M] \cdot A$ are dual codes. In summary we have

PROPOSITION 6.2 *If A is an non-singular $N \times N$ matrix and $C_1, \ldots, C_N$ linear codes then*

$$([C_1 \ \cdots \ C_N] \cdot A)^\perp = [C_1^\perp \ \cdots \ C_N^\perp] \cdot (A^{-1})^T.$$

EXAMPLE 6.3 *We have $(MS_2^{-1})^T = MS_2^T$ and so $([C_1 \ C_2] \cdot MS_2)^\perp = \{(u+v|v) : u \in C_1^\perp, v \in C_2^\perp\}$ as in [9, p. 77].*

EXAMPLE 6.4 *For the $(u+v|u-v)$-construction we have $(A^{-1})^T = \frac{1}{2}A$ and so $([C_1 \ C_2] \cdot A)^\perp = \{\frac{1}{2}(u+v|u-v) : u \in C_1^\perp, v \in C_2^\perp\}$, cf. [4, Lemma 9.1(iii)].*

EXAMPLE 6.5 *For the $(a+x|b+x|a+b+x)$-construction we have*

$$A = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}, \quad A^{-1} = (A^{-1})^T = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}.$$

Thus $([C_1 \ C_1 \ C_2] \cdot A)^\perp = \{(b+x|a+x|a+b+x) : a, b \in C_1^\perp, x \in C_2^\perp\}$ as in [9, p. 78].

As we have seen for MS_2, A square and NSC need not imply that $(A^{-1})^T$ is NSC. Thus, while the description of $([C_1 \ \cdots \ C_N] \cdot A)^\perp$ in Proposition 6.2 is quite natural in the context of Proposition 2.9, it is not very useful in the context of Theorem 3.7. As suggested by Lemmas 3.6 and 4.3, a better choice is $J \cdot (A^{-1})^T$ since it will be triangular and NSC if A is.

So let A be a square NSC matrix and take $B = J \cdot (A^{-1})^T$. Then $A \cdot B^T = J$ and

$$\sum_{i=1}^{N} \sum_{k=1}^{N} (A \cdot B^T)_{ik} c_i^T d_k = \sum_{i=1}^{N} c_i^T d_{N-i}$$

which will be zero for all $c_1 \in C_1, \ldots, c_N \in C_N$ and $d_1 \in D_1, \ldots, d_N \in D_N$ if we put $D_i = C_{N-i}^\perp$. Also since B is NSC Theorem 3.7 yields

$$\dim([C_N^\perp \ \cdots \ C_1^\perp] \cdot B) = (n - k_N) + \cdots + (n - k_1) = Nn - (k_1 + \cdots + k_N)$$

so that from Lemma 6.1 we see that $[C_N^\perp \ \cdots \ C_1^\perp] \cdot B$ is the dual of $[C_1 \ \cdots \ C_N] \cdot A$.

We write $d_i^\perp$ for the minimum distance of $C_i^\perp$. Thus Theorem 3.7 gives us that

$$\mathrm{d}([C_N^\perp \ \cdots \ C_1^\perp] \cdot B) \geq (d^\perp)^* = \min\{Nd_N^\perp, \ldots, d_1^\perp\}.$$

Moreover by Lemma 3.6 if A is triangular then so is B. Thus in this case Theorem 3.7 yields $\mathrm{d}([C_N^\perp \ \cdots \ C_1^\perp] \cdot B) = (d^\perp)^*$.

In summary we have

THEOREM 6.6 *If $C_1, \ldots, C_N$ are linear codes, A is an $N \times N$ NSC matrix and $C = [C_1 \ \cdots \ C_N] \cdot A$ then*

(i) $J \cdot (A^{-1})^T$ *is NSC*

(ii) $C^\perp = [C_N^\perp \ \cdots \ C_1^\perp] \cdot (J \cdot (A^{-1})^T)$

(iii) $\mathrm{d}(C^\perp) \geq (d^\perp)^* = \min\{Nd_N^\perp, \ldots, d_1^\perp\}$

(iv) if A *is also triangular then so is* $J \cdot (A^{-1})^T$ *and* $\mathrm{d}(C^\perp) = (d^\perp)^*$.

REMARKS 6.7 *1. Remark 3.10.4 says that* d^* *is maximised with the* C_i *ordered such that* $d_i \leq d_j$ *for* $i \leq j$. *For nested codes then* $d_{N-i}^\perp \leq d_{N-j}^\perp$ *for* $i \leq j$. *In this case* $(d^\perp)^*$ *is also maximised when the* C_i *are ordered this way.*

2. Proposition 6.2 and Theorem 6.6 imply that for an NSC matrix A *and linear codes* $C_1, \ldots, C_N$

$$[C_1^\perp \ \cdots \ C_N^\perp] \cdot (A^{-1})^T = [C_N^\perp \ \cdots \ C_1^\perp] \cdot (J \cdot (A^{-1})^T).$$

This is a special case of Proposition 2.8.

6.2 The dual of $\mathcal{G}RM_q(r, m)$

Of course we can apply Theorem 6.6 to $\mathcal{G}RM$-codes. Here $N = q$, $A = GRM_q$ and $C_i = \mathcal{G}RM(r + 1 - i, m - 1)$ for $1 \leq i \leq q$. When q is prime, Remark 5.12 implies that A^{-1} is $MS_q \cdot J = J \cdot A^T \cdot J$ (it is not true that $A^{-1} = J \cdot A^T \cdot J$ for all q). Thus in the prime case Theorem 6.6 gives the dual of $([C_1 \ \cdots \ C_q] \cdot A)^\perp = [C_q^\perp \ \cdots \ C_1^\perp] \cdot B$ where $B = J \cdot (J \cdot A^T \cdot J)^T = A \cdot J$. We now show that we can take $B = A$ *for all* q.

Firstly we note that Proposition 2.9 implies that

$$\dim([C_q^\perp \ \cdots \ C_1^\perp] \cdot A) = qn - (k_1 + \cdots + k_q)$$

so from Lemma 6.1 it suffices to show that

$$\sum_{i=1}^{q} \sum_{k=1}^{q} (A \cdot A^T)_{ik} c_i^T c_{q+1-k}^\perp = 0 \quad \text{for all } c_1 \in C_1, \ldots, c_q \in C_q \text{ and } c_q^\perp \in C_q^\perp, \ldots, c_1^\perp \in C_1^\perp. \qquad (4)$$

Now $c_{q+1-k} c_{q+1-k}^\perp = 0$ for all $c_{q+1-k} \in C_{q+1-k}$ and all $c_{q+1-k}^\perp \in C_{q+1-k}^\perp$. Thus if $C_i \subseteq C_{q+1-k}$, i. e. if $i \geq q + 1 - k$, then $c_i c_{q+1-k}^\perp = 0$ for all $c_i \in C_i$ and $c_{q+1-k}^\perp \in C_{q+1-k}^\perp$. Thus $\sum_{i=1}^q \sum_{k=q+1-i}^q (A \cdot A^T)_{ik} c_i c_{q+1-k}^\perp = 0$ and to show that (4) is satisfied, it suffices to show that

$$\sum_{i=1}^{q-1} \sum_{k=1}^{q-i} (A \cdot A^T)_{ik} c_i c_{q+1-k}^\perp = 0 \quad \text{for all } c_1 \in C_1, \ldots, c_{q-1} \in C_{q-1} \text{ and } c_q^\perp \in C_q^\perp, \ldots, c_2^\perp \in C_2^\perp. \qquad (5)$$

We take $1 \leq i \leq q - 1$ and $1 \leq k \leq q - i$ and show that $(A \cdot A^T)_{ik} = 0$, from which (5) follows. Now $1 \leq i + k \leq q$ and

$$(A \cdot A^T)_{ik} = \sum_{j=1}^{q} \binom{\alpha_j}{\alpha_i} \binom{\alpha_j}{\alpha_k} = \frac{\sum_{j=1}^q \prod_{s=1}^{i-1} (\alpha_j - \alpha_s) \prod_{r=1}^{k-1} (\alpha_j - \alpha_r)}{\left(\prod_{s=1}^{i-1} (\alpha_i - \alpha_s) \prod_{r=1}^{k-1} (\alpha_k - \alpha_r) \right)}$$

so that $(A \cdot A^T)_{ik} = 0$ if and only if

$$\sum_{j=1}^{q} \prod_{s=1}^{i-1} (\alpha_j - \alpha_s) \prod_{r=1}^{k-1} (\alpha_j - \alpha_r) = 0. \tag{6}$$

But $P(X) = \prod_{s=1}^{i-1}(X - \alpha_s) \prod_{r=1}^{k-1}(X - \alpha_r)$ is a polynomial of degree $i + k - 2 \leq q - 2$ so (6) holds by Corollary 5.4. Thus we have proved

PROPOSITION 6.8 *The dual of* $([\mathcal{G}RM(r, m-1) \ \cdots \ \mathcal{G}RM(r-q+1, m-1)] \cdot GRM_q$ *is* $[\mathcal{G}RM(r-q+1, m-1)^{\perp} \ \cdots \ \mathcal{G}RM(r, m-1)^{\perp}] \cdot GRM_q$.

Combining Theorem 5.6 and Proposition 6.8 gives an easy inductive proof of

COROLLARY 6.9 *The dual of* $\mathcal{G}RM(r, m)$ *is* $\mathcal{G}RM(m(q-1) - r - 1, m)$.

7 Matrix-product and generalized concatenated codes

It is well-known that for $p = 2, 3$, MS_p product codes are generalized concatenated codes (GCC). We show that NSC matrix-product codes are GCC. This leads to a natural characterisation of an NSC matrix. For this section it will simplify notation to take $\alpha_1 = 0 \in \mathbb{F}_q$.

We start with a family $\{\mathcal{M}_M, \ldots, \mathcal{M}_1\}$ of $1 \leq M \leq N$ MDS codes over $\mathbb{F}_q$ such that $\mathcal{M}_r$ is an $[N, r, N-r+1]$ code and $\mathcal{M}_M \supset \cdots \supset \mathcal{M}_1$. (For $N \leq q$ we could take $\mathcal{M}_r = \mathcal{RS}(N, r)$, the $[N, r, N-r+1]$ Reed-Solomon code.) For such a family of codes there exists a generator matrix

$$A = \begin{bmatrix} a_1 \\ \vdots \\ a_M \end{bmatrix} = \begin{bmatrix} a_{11} & \ldots & a_{1N} \\ \vdots & \ddots & \vdots \\ a_{M1} & \ldots & a_{MN} \end{bmatrix}.$$

of $\mathcal{M}_M$ such that A_r is a generator matrix for $\mathcal{M}_r$ (recall that A_r is the matrix consisting of the first r rows of A).

DEFINITION 7.1 *We call* $\{\mathcal{M}_M, \ldots, \mathcal{M}_1\}$ *a* **close nested family of MDS codes** *and* A *a* **nested generator matrix**.

With the notation of [9, p. 590–592] we use $\mathcal{M}_M, \ldots, \mathcal{M}_1$ and their cosets as the inner-codes of a GCC in the following way. For $0 \leq i \leq M-1$ we put $\mathcal{B}^i_{0\ldots0} = \mathcal{M}_{M-i}$, where there are i zeroes in the subscript. Then $\mathcal{B}^0 = \{\alpha a_M + \mathcal{B}^1_0 : \alpha \in \mathbb{F}_q\}$ so it is natural to put $\mathcal{B}^1_{k_1} = \alpha_{k_1} a_M + \mathcal{B}^1_0$ for $0 \leq k_1 \leq q-1$. Similarly $\mathcal{B}^1_0 = \{\alpha a_{M-1} + \mathcal{B}^2_{00} : \alpha \in \mathbb{F}_q\}$ and it is natural to put $\mathcal{B}^2_{0k_2} = \alpha_{k_2} a_{M-1} + \mathcal{B}^2_{00}$ and then $\mathcal{B}^2_{k_1 k_2} = \alpha_{k_1} a_M + \alpha_{k_2} a_{M-1} + \mathcal{B}^2_{00}$. Continuing in this way,

$$\mathcal{B}^i_{k_1 \ldots k_i} = \alpha_{k_1} a_M + \cdots + \alpha_{k_i} a_{M-i+1} + \mathcal{M}_{M-i} \text{ for } 0 \leq i \leq M-1.$$

Then $\mathcal{B}^M_{k_1\dots k_M} = \{\alpha_{k_1}a_M + \cdots + \alpha_{k_M}a_1\}$ so that $b_{k_1\dots k_M} = \alpha_{k_1}a_M + \cdots + \alpha_{k_M}a_1$ (really this is $b_{\alpha_{k_1+1}\dots\alpha_{k_M+1}}$). We note that the inner codes are determined by A.

The outer codes can be any M length n codes $C_M, \dots, C_1$ over $\mathbb{F}_q$—in the notation of [9] $\mathcal{A}_i = C_{M-i+1}$. We write $\langle C_M \ \cdots \ C_1\rangle \cdot A$ for the GCC so formed.

If C_i is an (n, K_i, d_i) code then $\langle C_M \ \cdots \ C_1\rangle \cdot A$ is an $(nN, K_1 \cdots K_M, d^* \geq \min\{(N - M + 1)d_M, \dots, Nd_1\})$ code by [9, Theorem 14, p. 591]. The central observation of this section is

PROPOSITION 7.2 *Let $C_1, \dots, C_M$ be length n codes over $\mathbb{F}_q$ and A an $M \times N$ matrix. Then A is NSC if and only if it is a nested generator matrix for a close nested family of MDS codes and in this case*

$$[C_1 \ \cdots \ C_M] \cdot A = \langle C_M \ \cdots \ C_1\rangle \cdot A.$$

PROOF. Let $\mathcal{M}_r$ be the linear code generated by A_r. If A is NSC then A_r has rank r so that $\mathcal{M}_r$ is an $[N, r]$ code. That $\mathcal{M}_r$ is MDS follows from the definition of NSC and [9, Corollary 3 p. 319], which also implies that a nested generator matrix is NSC.

Now the codewords of $\langle C_M \ \cdots \ C_1\rangle \cdot A$ are the $n \times N$ arrays of the form

$$\begin{bmatrix} b_{c_{1M}\dots c_{11}} \\ \vdots \\ b_{c_{nM}\dots c_{n1}} \end{bmatrix}$$

where $c_M \in C_M, \dots, c_1 \in C_1$ and for $1 \leq h \leq n$, $b_{c_{hM}\dots c_{h1}} = c_{hM}a_M + \cdots + c_{h1}a_1$, i. e. those $n \times N$ arrays of the form

$$\begin{bmatrix} c_{1M}a_{M1} + \cdots + c_{11}a_{11} & \cdots & c_{1M}a_{MN} + \cdots + c_{11}a_{1N} \\ \vdots & \ddots & \vdots \\ c_{nM}a_{M1} + \cdots + c_{n1}a_{11} & \cdots & c_{nM}a_{MN} + \cdots + c_{n1}a_{1N} \end{bmatrix},$$

as are the codewords of $[C_1 \ \cdots \ C_M] \cdot A$. □

REMARK 7.3 *In view of Propositions 3.3 and 7.2 there exists no family of close nested MDS codes of length greater than q over $\mathbb{F}_q$.*

EXAMPLES 7.4 *We take $M \leq N = q - 1$. Since*

$$H_r = \begin{bmatrix} 1 & \cdots & 1 \\ \alpha_1 & \cdots & \alpha_q \\ \vdots & \ddots & \vdots \\ \alpha_1^{q-1-r} & \dots & \alpha_q^{q-1-r} \end{bmatrix}$$

is a parity check matrix for $\mathcal{RS}(r,q)$ it follows from Lemma 5.5 (with $P_k(X) = X^k$ for $0 \le k \le q-2$) that the Vandermonde matrix

$$V_r = \begin{bmatrix} 1 & \dots & 1 \\ \alpha_1 & \dots & \alpha_q \\ \vdots & \vdots & \vdots \\ \alpha_1^{r-1} & \dots & \alpha_q^{r-1} \end{bmatrix}$$

is a generator matrix for $\mathcal{RS}(r,q)$. Thus V_M is an NSC matrix and for length n codes $C_1, \dots, C_M$, $[C_M \ \cdots \ C_1] \cdot V_M = \langle C_1 \ \cdots \ C_M \rangle \cdot V_M$.

It also follows from Lemma 5.5 that $(GRM_q)_r$ is a generator matrix for $\mathcal{RS}(r,q)$.

COROLLARY 7.5 *Generalized Reed-Muller codes are generalized concatenated codes.*

PROOF. Use Theorem 5.6, Corollary 5.9 and Proposition 7.2. □

E-mail address: tim.blackmore@infineon.com, ghn@maths.uq.edu.au
URL: http://www.maths.uq.edu.au/∼ghn

References

[1] Assmus, E., Key, J. (1992) *Designs and their Codes.* Cambridge University Press.

[2] Cohn, P.M. (1982) *Algebra Vol. 1,* John Wiley.

[3] Fossorier, M.P.C., Lin, S. (1997) *Some decomposable codes: the $|a+x|b+x|a+b+x|$ construction,* IEEE Trans. Information Theory **43**, 1663–1667.

[4] G. Hughes (2000) *Constacyclic codes, cocycles and a $(u+v|u-v)$ construction*, IEEE Trans. Information Theory, **46**, 674–680.

[5] Kschischang, F.R., Pasupathy, S. (1992) *Some ternary and quaternary codes and associated sphere packings,* IEEE Trans. Information Theory **38**, 227-246.

[6] S. Ling and P. Solé, *Decomposing quasi-cyclic codes*, April, 2001, Workshop on Coding and Cryptography, Paris 2001. Electronic Notes in Discrete Mathematics, *http://www.elsevier.nl:80/inca/publications/store/5/0/5/6/0/9/*, **6**.

[7] Massey, J.L, Costello, D.J., Justesen, J. (1973) *Polynomial weights and code constructions,* IEEE Trans. Information Theory **19**, 101-110.

[8] McDonald, B. R., (1984). *Linear Algebra over Commutative Rings.* Marcel Dekker, New York.

[9] MacWilliams F.J., Sloane N.J.A. (1977) *The Theory of Error-Correcting Codes,* North-Holland Mathematics Library.

[10] Plotkin, M. (1960) *Binary codes with specified minimum distance.* IEEE Trans. Information Theory **6**, 445–450.

[11] Riordan, J. (1958). *An introduction to Combinatorial Analysis,* John Wiley.

[12] E. van Eupen and J.H. van Lint (1993), *On the minimum distance of ternary cyclic codes*, IEEE Trans. Information Theory, **39**, 409–422.