Maximum-Rank Array Codes and their Application to Crisscross Error Correction

Ron M. Roth, *Member, IEEE*

***Abstract*—A μ-$[n \times n, k]$ array code C over a field F is a k-dimensional linear space of $n \times n$ matrices over F such that every nonzero matrix in C has rank $\geq \mu$. It is first shown that the dimension of such array codes must satisfy the Singleton-like bound $k \leq n(n-\mu+1)$. A family of so-called maximum-rank μ-$[n \times n, k = n(n-\mu+1)]$ array codes is then constructed over every finite field F and for every n and μ, $1 \leq \mu \leq n$. A decoding algorithm is presented for retrieving every $\Gamma \in C$, given a "received" array $\Gamma + E$, where $\operatorname{rank}(E) = t \leq (\mu-1)/2$. Maximum-rank array codes can be used for decoding crisscross errors in $n \times n$ bit arrays, where the erroneous bits are confined to a number t of rows or columns (or both). Our construction proves to be optimal also for this model of errors, which can be found in a number of applications, such as memory chip arrays or magnetic tape recording. Finally, it is shown that the behavior of linear spaces of matrices is quite unique compared with the more general case of linear spaces of $n \times n \times \cdots \times n$ hyper-arrays.**

***Index Terms*—Array codes, decoding, matrix spaces, tensor rank.**

I. Introduction

In a number of applications, we encounter the following error protection problem: Information bits are to be stored in $n \times n$ bit arrays, with the possibility of some of the bits recorded erroneously. The error patterns are such that all corrupted bits are confined to a prespecified number t of rows or columns (or both). We shall refer to such an error model as *crisscross errors*. Crisscross errors can be found in memory chip arrays, where row or column failures occur because of the malfunctioning of row drivers, or column amplifiers (see for instance [7], [9], [15]). Another application of crisscross error correcting codes can be found in magnetic tapes, where the errors usually occur *along* the tracks, whereas the information units (bytes) are recorded *across* the tracks. Computation of check bits is equivalent to decoding of erasures at the check bit locations, and in this case these erasures are perpendicular to the erroneous tracks. There exist known easily-correctable codes for magnetic recording when the number of track errors is small [6], [16], [17].

To present a more rigorous statement of the problem, we make use of the following definitions. Let $E = [e_{ij}]_{i,j=0}^{n-1}$ be an $n \times n$ matrix over a field F. A *cover* of E is a pair (X,Y) of sets $X, Y \subseteq \{0, 1, \cdots, n-1\}$, such that $e_{ij} \neq 0 \Rightarrow ((i \in X)$ or $(j \in Y))$ for all $0 \leq i, j \leq n-1$. The size of a cover (X,Y) is defined by $|(X,Y)| = |X| + |Y|$. The *weight* of E, denoted by $w(E)$, is the minimum size $|(X,Y)|$ of any cover (X,Y) of E. Note that a minimum-size cover of a given matrix E is not always unique.

Example 1: Consider the 4×4 array

$$E = \begin{array}{|c|c|c|c|c} \hline 1 & 0 & 0 & 0 & \multicolumn{1}{|c}{0} \\ \hline 0 & 1 & 0 & 0 & \multicolumn{1}{|c}{1} \\ \hline 1 & 0 & 1 & 1 & \multicolumn{1}{|c}{2} \\ \hline 0 & 1 & 0 & 0 & \multicolumn{1}{|c}{3} \\ \hline \multicolumn{1}{c}{0} & \multicolumn{1}{c}{1} & \multicolumn{1}{c}{2} & \multicolumn{1}{c}{3} & \end{array}$$

over GF(2). It is easy to verify that E has two covers of size 3, namely, $(\{0,2\},\{1\})$ and $(\{2\},\{0,1\})$. Furthermore, since the three nonzero elements on the main diagonal of E belong to distinct rows and columns, the weight of E must be at least 3. Therefore, $w(E) = 3$.

Let $\Gamma = [c_{ij}]_{i,j=0}^{n-1}$ be an $n \times n$ matrix over F, denoting the correct array to be stored, and let $\Gamma + E$ denote the array actually recorded, with $E = [e_{ij}]_{i,j=0}^{n-1}$ standing for the error array and the addition sign denoting matrix addition over F. Our crisscross error model assumes that $w(E) \leq t$ for some prespecified t.

An $[n \times n, k, d]$ linear array code C over a field F is a k-dimensional linear space of $n \times n$ matrices over F with d being the minimum weight of any nonzero matrix in C. Adopting the terminology of conventional linear codes, we call d the *minimum distance* of C. An $[n \times n, k, d]$ array code C can correct any pattern of t crisscross errors if and only if $t \leq (d-1)/2$. The "if" part follows from the fact that the weight of a matrix is a metric and, as such, it satisfies the triangle inequality: for any two $n \times n$ matrices A and B, $w(A+B) \leq w(A) + w(B)$. Now, decoding would fail only if for some two code arrays Γ, $\tilde{\Gamma} \in C$, and for some two matrices $E, \tilde{E}$ of weight $\leq t$, we would have $\Gamma + E = \tilde{\Gamma} + \tilde{E}$. However, this would mean $w(\Gamma - \tilde{\Gamma}) = w(\tilde{E} - E) \leq w(\tilde{E}) + w(E) \leq 2t < d$, implying $\Gamma = \tilde{\Gamma}$. As for the "only if" part, assume that $w(\Gamma) \leq 2t$ for some nonzero $\Gamma \in C$. Then we can write $\Gamma = \Sigma_{i=1}^{2t} E_i$, where $w(E_i) \leq 1$ for all i. Let $E = -\Sigma_{i=1}^{t} E_i$ and $\tilde{E} = \Sigma_{i=t+1}^{2t} E_i$. Both E and $\tilde{E}$ have weight $\leq t$. Hence, if the recorded array is $\Gamma + E$ $(= 0 + \tilde{E})$, there is no way to decide whether the correct array is 0 or Γ.

In Section II we extend the Singleton bound [12, p. 33] to array codes and show that evefy $[n \times n, k, d]$ array code must satisfy the inequality $k \leq n(n-d+1)$. It can be readily verified that this bound is attained for every n and d, $1 \leq d \leq n$,

Manuscript received March 20, 1990.

IBM Research Division, Almaden Research Center, 650 Harry Road, San Jose, CA 95120, on leave from the Technion—Israel Institute of Technology, Haifa 32000, Israel.

IEEE Log Number 9040585.

when the field F is *infinite*. Let $\mathscr{C}$ be an $[n, n-d+1, d]$ (conventional) linear code over F. Such codes are maximum-distance separable (MDS) and, when F is infinite, they exist for every n and d, $1 \le d \le n$. In particular, if $\alpha_0, \alpha_1, \cdots, \alpha_{n-1}$ are distinct elements of F, then the Reed–Solomon code, generated by $G = [g_{ij}]_{i=0, j=0}^{n-d, n-1}$, $g_{ij} = \alpha_j^i$, is MDS [12, Ch. 11]. Let $A(l, m)$, $0 \le l \le n-d$, $0 \le m \le n-1$, be the $n \times n$ matrices defined by $(A(l,m))_{ij} = g_{l,j}\delta_{i,j-m}$, where $\delta\cdot,\cdot$ stands for the Kronecker delta function modulo n. For example, the matrix $A(2,1)$ corresponding to a [4,3,2] Reed–Solomon code over F is given by

$$A(2,1) = \begin{bmatrix} 0 & \alpha_0^2 & 0 & 0 \\ 0 & 0 & \alpha_1^2 & 0 \\ 0 & 0 & 0 & \alpha_2^2 \\ \alpha_3^2 & 0 & 0 & 0 \end{bmatrix}.$$

Now, let $C_{n,d}$ be the array code spanned by $\{A(l,m)\}_{l,m}$; that is, for every $\Gamma = [c_{ij}]_{i,j=0}^{n-1} \in C_{n,d}$, and every m, $0 \le m \le n-1$, the diagonals defined by $[c_{0,m} c_{1,m+1} \cdots c_{n-1,m-1}]'$ are all codewords of $\mathscr{C}$. Since the $A(l,m)$ are linearly independent over F, $C_{n,d}$ is of dimension $n(n-d+1)$. Also, no two entries on any such diagonal belong to the same row or column and, therefore, each nonzero array in $C_{n,d}$ has weight $\ge d$. Hence, $C_{n,d}$ is an $[n \times n, n(n-d+1), d]$ array code. Now, any row or column error intersects each diagonal exactly once and, therefore, if the number of crisscross errors is at most $(d-1)/2$, there exist at most $(d-1)/2$ erroneous symbols on each diagonal, which can be readily decoded using the Reed–Solomon decoding algorithm [3, Section 7.4], [13].

This simple construction generally fails when F is finite, since their exist no MDS codes over a given finite field when n is sufficiently large, unless $d \in \{1, 2, n\}$ [12, Ch. 11]. In Section III we present a family of $[n \times n, k, d]$ array codes over finite fields, with k attaining the bound $n(n-d+1)$ for every n and d, $1 \le d \le n$. As a matter of fact, the capability of this finite-field construction (unlike its infinite-field counterpart!) tends to go far beyond our original crisscross error motivation: in these codes, d turns out to be not only a lower bound on the *weights* of the nonzero matrices in the code, but rather a lower bound on their *ranks* (note that a rank of a matrix is never greater than its weight). Such array codes will therefore be called *maximum-rank* array codes. Since the rank of a matrix is also a metric, we have $\operatorname{rank}(A+B) \le \operatorname{rank}(A) + \operatorname{rank}(B)$ for every two matrices A and B; therefore, any error array of rank $\le (d-1)/2$ is correctable while using such codes. For instance, an $[n \times n, n(n-4), 5]$ maximum-rank array code over GF(2) can correct any number of inverted (= Boolean NOT) rows or columns, since in this case the error array E is of rank ≤ 2.

Another virtue of the presented maximum-rank array codes is having an efficient decoding algorithm. In Section IV we describe such an algorithm for correcting any $n \times n$ error array of rank $\le (d-1)/2$ over GF(q), requiring $O(dn + d^3)$ arithmetic operations over GF(q^n).

The existence of such linear spaces of high-rank matrices gives rise to several questions of theoretical significance. A μ-$[n \times n, k, d]$ array code over a field F is an $[n \times n, k, d]$ array code with μ being the *minimum rank* of any nonzero matrix in the code. Observe that we always have $\mu \le d$, implying $k \le n(n-\mu+1)$. Now, our maximum-rank construction, satisfying these bounds with equality, depends crucially on the structure of finite fields. The question now is how close can k get to $n(n-\mu+1)$ in any μ-$[n \times n, k]$ code over *infinite* fields. The answer to this question is known in part for certain fields, e.g., algebraically closed fields or the real field [1], [2], [14], [20]. In particular, when $\mu = n$ (a linear space of nonsingular matrices), the maximum value of k is usually much smaller than $n(n-\mu+1) = n$. This means that there is a range of parameters n and d for which $[n \times n, k = n(n-d+1), d]$ infinite-field codes exist, while d-$[n \times n, k]$ codes do not. A short summary of these results is given in Section V.

These questions can be raised also in a more general context of $\overbrace{n \times n \times \cdots \times n}^{\Delta \text{ times}}$ hyper-arrays (in short, $n^{\times\Delta}$ arrays). In Section VI we address the problem of constructing $[n^{\times\Delta}, k, d]$ codes of large minimum distance d. First, we present a hyper-array generalization of the infinite-field construction $C_{n,d}$ previously mentioned. The hyper-array codes thus obtained attain the Singleton bound (now taking the form $k \le n(n^{\Delta-1} - d + 1))$ for every n and d, $1 \le d \le n^{\Delta-1}$. When the field is finite, the Singleton bound can be approached for sufficiently large n; however, unlike matrix spaces ($\Delta = 2$), there exists a range of values of n for which the maximum attainable value of k is strictly smaller than the Singleton bound.

Finally, in Section VII we obtain bounds on the dimension k of μ-$[n^{\times\Delta}, k]$ hyper-array codes in terms of μ (rather than d). It turns out that when $\Delta > 2$, the minimum-rank version of the Singleton bound ($k \le n(n^{\Delta-1} - \mu + 1)$) is usually far from being tight, regardless of the size of the field. Hence, the two aforementioned problems, one of constructing optimal-minimum-rank codes and the other of constructing optimal-minimum-distance codes, become diverse in nature when Δ is greater than 2, even when the field is finite.

The results of Sections V, VI, and VII provide quite a convincing evidence for the unique behavior of linear spaces of matrices over finite fields, compared with such spaces over infinite fields, or with spaces of $n^{\times\Delta}$ hyper-arrays for $\Delta > 2$.

II. Singleton Bound for Array Codes

Theorem 1: For any $[n \times n, k, d]$ array code over a field F,

$$k \le n(n-d+1).$$

Proof: Let C be an $[n \times n, k, d]$ array code over F and assume, to the contrary, that $k > n(n-d+1)$. We show the existence of a nonzero matrix Γ in C whose weight is less than d.

Let $A_0, A_1, \cdots, A_{k-1}$ be a basis of C and let B be the $k \times (n(n-d+1))$ matrix whose mth row is the concatenation of the last $n-d+1$ rows of A_m, $0 \le m \le k-1$. Now, $\operatorname{rank}(B) \le n(n-d+1) < k$ and, therefore, there exists a nonzero row vector $y = [y_0 y_1 \cdots y_{k-1}]$ over F such that $yB = \mathbf{0}$. Hence, the last $n-d+1$ rows of the nonzero matrix $\Gamma \triangleq \sum_{m=0}^{k-1} y_m A_m$ are all zero, implying that $w(\Gamma) \le d-1$. □

For every μ-$[n \times n, k, d]$ array code we have $\mu \le d$ and, therefore the following corollary.

Corollary 1: For any μ-$[n \times n, k]$ array code over a field F,

$$k \le n(n-\mu+1).$$

The definitions of cover and weight and the formulation of Theorem 1 can be extended to $n^{\times\Delta}$ hyper-arrays as well. Given a hyper-array $E = [e_{i_0 i_1 \cdots i_{\Delta-1}}]_{i_0, i_1, \cdots, i_{\Delta-1}=0}^{n-1}$, a cover of E

is a Δ-tuple $(X_0, X_1, \cdots, X_{\Delta-1})$, where each X_j is a set of $(\Delta-1)$-tuples over $\{0,1,\cdots,n-1\}$ such that $e_{i_0 i_1 \cdots i_{\Delta-1}} \neq 0$ implies $[i_0 i_1 \cdots i_{j-1} i_{j+1} \cdots i_{\Delta-1}] \in X_j$ for at least one j. The size of a cover $(X_0, X_1, \cdots, X_{\Delta-1})$ is defined by $\Sigma_{j=0}^{\Delta-1}|X_j|$, and the weight of E is the minimum size of any cover of E. The Singleton bound now takes the form $k \leq n(n^{\Delta-1} - d + 1)$, the proof of which is similar to that of Theorem 1.

III. Construction of Maximum-Rank Array Codes

In this section we present a construction of μ-$[n \times n, k]$ array codes over $F = \mathrm{GF}(q)$ with $k = n(n - \mu + 1)$. Let $\Phi = \mathrm{GF}(q^n)$ and let the entries of $\boldsymbol{\alpha} = [\alpha_0 \alpha_1 \cdots \alpha_{n-1}]$ form a basis of Φ over F. That is, $\Sigma_{j=0}^{n-1} a_j \alpha_j = 0$, $a_j \in F$, implies $a_j = 0$ for all j. Let $C_\Phi(n,r)$ be the conventional linear code of length n over Φ defined by the $r \times n$ parity-check matrix

$$H = \begin{bmatrix} \alpha_0 & \alpha_1 & \alpha_2 & \cdots & \alpha_{n-1} \\ \alpha_0^q & \alpha_1^q & \alpha_2^q & \cdots & \alpha_{n-1}^q \\ \alpha_0^{q^2} & \alpha_1^{q^2} & \alpha_2^{q^2} & \cdots & \alpha_{n-1}^{q^2} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha_0^{q^{r-1}} & \alpha_1^{q^{r-1}} & \alpha_2^{q^{r-1}} & \cdots & \alpha_{n-1}^{q^{r-1}} \end{bmatrix}.$$

First, we verify that $\mathrm{rank}(H) = r$, implying that the dimension of $C_\Phi(n,r)$ is $n - r$. As a matter of fact, it turns out that *every* $r \times r$ submatrix of H has rank r and, therefore, $C_\Phi(n,r)$ is an MDS code [12, Ch. 11]. This is a direct corollary of Part a) of the following lemma.

Lemma 1: Let $\boldsymbol{\alpha} = [\alpha_0 \alpha_1 \cdots \alpha_{n-1}]$ and $\boldsymbol{\omega} = [\omega_0 \omega_1 \cdots \omega_{n-1}]'$ be two bases of $\Phi = \mathrm{GF}(q^n)$ over $F = \mathrm{GF}(q)$. Given a vector $\boldsymbol{\beta} = [\beta_0 \beta_1 \cdots \beta_{m-1}] \in \Phi^m$, let U be the $n \times m$ matrix over F defined by $\boldsymbol{\beta} = \boldsymbol{\alpha} U$, and let $\mathscr{B}$ be the $m \times m$ matrix over Φ defined by $\mathscr{B} = [\beta_j^{q^i}]_{i,j=0}^{m-1}$. Then, a) $\mathrm{rank}(\mathscr{B}) = \mathrm{rank}(U)$ and b) the right null space of $\mathscr{B}$ over Φ is given by

$$\ker_\Phi(\mathscr{B}) = \left\{ \sum_{i=0}^{n-1} z_i \omega_i \,|\, z_0, z_1, \cdots, z_{n-1} \in \ker_F(U) \right\},$$

where $\ker_F(U)$ is the right null space of U over F.

Special cases of Lemma 1 can be found in [6] and [12, p. 117].

Proof:

a) Let $s = \mathrm{rank}(\mathscr{B})$ (> 0) and assume, without loss of generality, that the first s columns of $\mathscr{B}$ are linearly independent. We claim that the first s columns of U are linearly independent as well. Otherwise, there exists a nonzero column vector $z = [z_0 z_1 \cdots z_{s-1} 00 \cdots 0]' \in F^m$ such that $Uz = \mathbf{0}$. This implies $\boldsymbol{\beta} z = 0$ and, by raising this equality to the powers q^i, $i = 0, 1, \cdots, m-1$, we have a vanishing linear combination of the first s columns of $\mathscr{B}$, which is a contradiction. Hence, $\mathrm{rank}(\mathscr{B}) \leq \mathrm{rank}(U)$.

   Now, let $t = \mathrm{rank}(U)$ and, without loss of generality, assume that the first t columns of U are linearly independent. Let $\mathscr{B}_h \triangleq [\beta_j^{q^i}]_{i,j=0}^{h-1}$. We show by induction on h that $\mathscr{B}_h$ is nonsingular for all $1 \leq h \leq t$, implying a). Clearly, this holds for $h = 1$, or else $t = 0$. Now, assume the validity of the claim for $h - 1$ and consider the $h \times h$ matrix $\mathscr{B}_h(x)$ of the indeterminate x, given by

$$\mathscr{B}_h(x) = \begin{bmatrix} \beta_0 & \beta_1 & \cdots & \beta_{h-2} & x \\ \beta_0^q & \beta_1^q & \cdots & \beta_{h-2}^q & x^q \\ \beta_0^{q^2} & \beta_1^{q^2} & \cdots & \beta_{h-2}^{q^2} & x^{q^2} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \beta_0^{q^{h-1}} & \beta_1^{q^{h-1}} & \cdots & \beta_{h-2}^{q^{h-1}} & x^{q^{h-1}} \end{bmatrix}.$$

   By the induction hypothesis, $\det(\mathscr{B}_h(x))$ is a polynomial of degree q^{h-1} over Φ. Furthermore, the q^{h-1} roots of $\det(\mathscr{B}_h(x))$ in Φ are given by $\{\Sigma_{j=0}^{h-2} a_j \beta_j \,|\, a_j \in F\}$. Now, for every $h \leq t$, β_{h-1} is not in the linear span (over F) of $\beta_0, \beta_1, \cdots, \beta_{h-2}$ and, therefore, $\det(\mathscr{B}_h) = \det(\mathscr{B}_h(x))|_{x=\beta_{h-1}} \neq 0$, $1 \leq h \leq \mathrm{rank}(U)$.

b) For any $z \in F^m$, $z \in \ker_F(U) \Rightarrow Uz = \mathbf{0} \Rightarrow \mathscr{B}z = \mathbf{0} \Rightarrow z \in \ker_\Phi(\mathscr{B})$ and, therefore,

$$\left\{ \sum_{i=0}^{n-1} z_i \omega_i \,|\, z_0, z_1, \cdots, z_{n-1} \in \ker_F(U) \right\} \subseteq \ker_\Phi(\mathscr{B}). \quad (1)$$

   Now, the number of distinct vectors over Φ at the left-hand side of (1) is $|\ker_F(U)|^n$. By a) we have $\dim(\ker_\Phi(\mathscr{B})) = \dim(\ker_F(U))$ and, so,

$$|\ker_\Phi(\mathscr{B})| = |\Phi|^{\dim(\ker_\Phi(\mathscr{B}))} = q^{n \cdot \dim(\ker_F(U))} = |\ker_F(U)|^n,$$

   implying equality in (1). □

Remark 1: Let $\boldsymbol{\gamma} = [\gamma_0 \gamma_1 \cdots \gamma_{n-1}] \in \Phi^n$ be the *dual* basis of $\boldsymbol{\alpha}$, that is, $\Sigma_{l=0}^{n-1}(\gamma_i \alpha_j)^{q^l} = \delta_{i,j}$, where $\delta\cdot,\cdot$ is the Kronecker delta function [12, p. 117–118]. In other words, the matrix $[\gamma_i^{q^j}]_{i,j=0}^{n-1}$ is the inverse of $[\alpha_j^{q^i}]_{i,j=0}^{n-1}$. Since a right inverse of a matrix is also its left inverse, we have $\Sigma_{l=0}^{n-1} \alpha_l^{q^i} \gamma_l^{q^j} = \delta_{i,j}$. Hence, $G = [(\gamma_j^{q^r})^{q^i}]_{i,\ j=0}^{n-r-1,n-1}$ is a generator matrix of $C_\Phi(n,r)$.

A variation of the code $C_\Phi(n,r)$ was suggested by Blaum and McEliece in [6], as a generalization of the Patel-Hong error-correcting code for magnetic recording [16], where they also presented a decoding algorithm for specific small values of r. These results will turn out to be direct corollaries of the forthcoming discussion of maximum-rank codes.

Let $\boldsymbol{\omega} = [\omega_0 \omega_1 \cdots \omega_{n-1}]'$ be a basis of Φ over F ($\boldsymbol{\omega}'$ need not necessarily be equal to the basis $\boldsymbol{\alpha}$ used to define $C_\Phi(n,r)$). For every (column) codeword $c \in C_\Phi(n,r)$, we associate an $n \times n$ matrix Γ over F corresponding to the unique representation $c = \Gamma \boldsymbol{\omega}$. The $[n \times n, k = n(n-r)]$ linear array code $C(n,r)$ over F is now defined by

$$C(n,r) = \{\Gamma \,|\, \Gamma \boldsymbol{\omega} \in C_\Phi(n,r)\}.$$

Theorem 2: The rank of any nonzero matrix in $C(n,r)$ is at least $r+1$.

Proof: Let $\Gamma \in C(n,r)$ and assume that the rank ρ of Γ is at most r. We show that $\Gamma = 0$. Since $\Gamma \boldsymbol{\omega} \in C_\Phi(n,r)$, we have

$$H \Gamma \boldsymbol{\omega} = \mathbf{0}. \quad (2)$$

Let $U = [u_{ik}]_{i=0,k=0}^{n-1,\rho-1}$ be an $n \times \rho$ matrix over F whose columns span the columns of Γ, and write

$$\Gamma = UD, \quad (3)$$

where D is a $\rho \times n$ matrix over F. Defining $\boldsymbol{\delta} = [\delta_0 \delta_1 \cdots$

$\delta_{\rho-1}]' \triangleq D\boldsymbol{\omega}$, and plugging (3) into (2), both yield $HU\boldsymbol{\delta} = HUD\boldsymbol{\omega} = \mathbf{0}$, which can be written explicitly as

$$\sum_{i=0}^{n-1} \alpha_i^{q^l} \sum_{k=0}^{\rho-1} u_{ik}\delta_k = 0, \qquad 0 \le l \le r-1,$$

or

$$\sum_{k=0}^{\rho-1} \delta_k \sum_{i=0}^{n-1} (\alpha_i u_{ik}) q^l = 0, \qquad 0 \le l \le \rho - 1 \tag{4}$$

(note the range of l). Now let $\beta = [\beta_0 \beta_1 \cdots \beta_{\rho-1}] \triangleq \boldsymbol{\alpha} U$ and rewrite (4) as

$$\sum_{k=0}^{\rho-1} \delta_k \beta_k^{q^l} = 0, \qquad 0 \le l \le \rho - 1.$$

Hence, $\boldsymbol{\delta} \in \ker_\Phi([\beta_k^{q^l}]_{l,k=0}^{\rho-1})$ and, therefore, by Part b) of Lemma 1, the columns of D belong to $\ker_F(U)$, implying $\Gamma = UD = 0$. □

Theorem 2 thus establishes the fact that $C(n,r)$ is an $(r+1)$-$[n \times n, n(n-r), r+1]$ array code over GF(q), defined for every n and r, $0 \le r \le n-1$.

Given a generator matrix G of $C_\Phi(n,r)$ (say, the one described in Remark 1), we can obtain a basis of $C(n,r)$ in the following manner: Let $\mathbf{g}_0, \mathbf{g}_1, \cdots, \mathbf{g}_{n-r-1}$ denote the rows of G and define the $n \times n$ matrices $B(l,m)$ over F by

$$B(l,m)\boldsymbol{\omega} = \omega_m \mathbf{g}_l', \qquad 0 \le l \le n-r-1, \qquad 0 \le m \le n-1. \tag{5}$$

Now, if Γ is in the linear span of $\{B(l,m)\}_{l,m}$ over F, then

$$\begin{aligned} \Gamma\boldsymbol{\omega} &= \sum_{l=0}^{n-r-1} \sum_{m=0}^{n-1} a_{lm} B(l,m)\boldsymbol{\omega} \\ &= \sum_{l=0}^{n-r-1} \mathbf{g}_l' \sum_{m=0}^{n-1} a_{lm}\omega_m \in C_\Phi(n,r), \end{aligned}$$

that is, $\Gamma \in C(n,r)$. Furthermore, $\Gamma = 0$ implies $a_{lm} = 0$ and, so, $\{B(l,m)\}_{l,m}$ is a basis of $C(n,r)$.

Example 2: Consider the case $r = n-1$ i.e., $\mu = n$. Let β be a root in Φ of an irredicible polynomial $p(x) = x^n + \sum_{j=0}^{n-1} p_j x^j$ over F, and let $\boldsymbol{\omega}$ be defined by $\omega_m = \beta^m$, $0 \le m \le n-1$. By Remark 1, we can choose the basis $\boldsymbol{\alpha}$ so that $\boldsymbol{\omega}'$ is also a generator matrix of $C_\Phi(n, n-1)$. In this case, (5) becomes

$$B(0,m)\boldsymbol{\omega} = \beta^m \boldsymbol{\omega}, \qquad 0 \le m \le n-1. \tag{6}$$

Let Q_p be the companion matrix of $p(x)$ [12, p. 106] i.e.,

$$Q_p = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ \vdots & 0 & 1 & & \vdots \\ 0 & \vdots & & \ddots & 0 \\ 0 & 0 & \cdots & 0 & 1 \\ -p_0 & -p_1 & -p_2 & \cdots & -p_{n-1} \end{bmatrix}.$$

It is easy to verify that $\boldsymbol{\omega}$ is an eigenvector of Q_p corresponding to the eigenvalue β and, therefore, $Q_p^m \boldsymbol{\omega} = \beta^m \boldsymbol{\omega}$ for every $m \ge 0$. Comparing with (6) we thus conclude that, for the above choice of $\boldsymbol{\omega}$ and $\boldsymbol{\alpha}$, $C(n, n-1)$ has a basis of the form $B(0,m) = Q_p^m$, $0 \le m \le n-1$. In fact, the set of matrices $\{\sum_{m=0}^{n-1} a_m Q_p^m \,|\, a_m \in F\}$ is isomorphic to GF(q^n), which means that every nonzero matrix in that set has an inverse.

Remark 2: Let $p(x)$ and β be as in Example 2, and suppose that $\boldsymbol{\alpha} = \boldsymbol{\omega}' = [1 \;\; \beta \;\; \beta^2 \cdots \beta^{n-1}]$. In this case, (2) becomes

$$\sum_{i=0}^{n-1} \beta^{iq^l} (\Gamma)_i \boldsymbol{\omega} = 0, \qquad 0 \le l \le r-1,$$

where $(\Gamma)_i$ stands for the ith row of Γ. Now, $\beta^{iq^l}(\Gamma)_i\boldsymbol{\omega} = (\Gamma)_i Q_p^{iq^l}\boldsymbol{\omega}$; hence, for the previous particular choice of $\boldsymbol{\omega}$ and $\boldsymbol{\alpha}$, we obtain the following equivalent definition for $C(n,r)$ in terms of parity-check conditions over F:

$$\sum_{i=0}^{n-1} (\Gamma)_i Q_p^{iq^l} = \mathbf{0}, \qquad 0 \le l \le r-1.$$

It is interesting to observe that if we "transpose" the code $C(n,r)$, we obtain an array code $C'(n,r) = \{\Gamma' \,|\, \Gamma \in C(n,r)\}$, which is essentially the same as $C(n,r)$. Indeed, let $\Gamma = [c_{ij}]_{i,j=0}^{n-1}$ be a code array in $C(n,r)$. Rewriting (2) explicitly, we obtain

$$\sum_{i=0}^{n-1} \alpha_i^{q^l} \sum_{j=0}^{n-1} c_{ij}\omega_j = 0, \qquad 0 \le l \le r-1. \tag{7}$$

Raising (7) to the q^{n-l}th power yields

$$\sum_{i=0}^{n-1} \alpha_i \sum_{j=0}^{n-1} c_{ij}\omega_j^{q^{n-l}} = 0, \qquad 0 \le l \le r-1. \tag{8}$$

Now, define the new bases $\hat{\alpha}_j \triangleq \omega_j^{q^{n-r+1}}$ and $\hat{\omega}_i \triangleq \alpha_i$ of Φ over F, and substitute m for $r-1-l$ in (8). We thus have

$$\sum_{j=0}^{n-1} \hat{\alpha}_j^{q^m} \sum_{i=0}^{n-1} c_{ij}\hat{\omega}_i = 0, \qquad 0 \le m \le r-1,$$

which has the same form as (7).

This symmetry property of $C(n,r)$ implies that if we regard the *columns* of each $\Gamma \in C(n,r)$ as elements of Φ, with respect to the basis $\hat{\boldsymbol{\omega}}$, the resulting $[n, n-r]$ conventional linear code over Φ is MDS. This means that any r rows, or, equivalently, any r columns in Γ, can serve as parity checks (note, however, that we cannot mix rows and columns here, since the number of check symbols would otherwise be less than $r \cdot n$ because of the entries in the intersections of rows and columns).

We end this section by pointing out that, by shortening the code $C(n,r)$, one can derive linear spaces of $l \times n$ arrays where l is not necessarily equal to n. Suppose that $r < l \le n$, and consider the linear subcode that consists of the arrays in $C(n,r)$ whose last $n-l$ rows are zero. Omitting these last zero rows, we obtain an $[l \times n, n(l-r)]$ array code where each nonzero matrix has rank $\ge r+1 = \mu$. The dimension of such an array code thus equals $n(l-\mu+1)$, which is also an upper bound, obtained by a straightforward generalization of Theorem 1.

IV. Decoding Algorithm for Maximum-Rank Array Codes

Let $C(n,r)$ be the $(r+1)$-$[n \times n, n(n-r)]$ maximum-rank array code over F defined in Section III and let $H = [\alpha_i^{q^l}]_{l=0,i=0}^{r-1,n-1}$ be a parity-check matrix for $C(n,r)$. Assume that an array code $\Gamma \in C(n,r)$ has been "transmitted" and that an array $Z = \Gamma + E$ has been received, with $E = [e_{ij}]_{i,j=0}^{n-1}$ being an error array of rank $\le r/2$. In this section we present an algorithm that retrieves Γ, or rather E, out of Z.

The syndrome column vector $\mathbf{s} \in \Phi^r$ associated with Z, or E, is given by

$$\mathbf{s} = [s_0 s_1 \cdots s_{r-1}]' = HZ\boldsymbol{\omega} = HE\boldsymbol{\omega},$$

or

$$s_l = \sum_{i,j=0}^{n-1} \alpha_i^{q^l} e_{ij} \omega_j, \qquad 0 \le l \le r-1,$$

where $\boldsymbol{\omega} = [\omega_0 \omega_1 \cdots \omega_{n-1}]'$ is a basis of Φ over F.

Let $\rho \triangleq \operatorname{rank}(E)$ and let $U = [u_{ik}]_{i,k}$ be an $n \times \rho$ matrix over F of rank ρ whose columns span the columns of E. Write $E = UD$, where $D = [d_{kj}]_{k,j}$ is a $\rho \times n$ matrix over F of rank ρ. The syndrome can now be rewritten as $\mathbf{s} = HUD\boldsymbol{\omega}$, or

$$s_l = \sum_{k=0}^{\rho-1} \sum_{j=0}^{n-1} d_{kj} \omega_j \sum_{i=0}^{n-1} \alpha_i^{q^l} u_{ik}, \qquad 0 \le l \le r-1. \tag{9}$$

Defining the two vectors $\boldsymbol{\beta} = [\beta_0 \beta_1 \cdots \beta_{\rho-1}] \triangleq \boldsymbol{\alpha} U$ and $\boldsymbol{\delta} = [\delta_0 \delta_1 \cdots \delta_{\rho-1}]' \triangleq D\boldsymbol{\omega}$, both over Φ, we can simplify (9) to

$$s_l = \sum_{k=0}^{\rho-1} \delta_k \beta_k^{q^l}, \qquad 0 \le l \le r-1, \tag{10}$$

or, in matrix notation,

$$\mathbf{s} = B\boldsymbol{\delta}, \tag{11}$$

with $B \triangleq [\beta_k^{q^l}]_{l=0,k=0}^{r-1,\rho-1}$. The decoding process thus reduces to finding two vectors $\boldsymbol{\beta}$ and $\boldsymbol{\delta}$ of length $\le r/2$ satisfying (11).

The *error span polynomial* $\Lambda(x)$ over Φ, associated with E, is defined by

$$\Lambda(x) = \prod_{y \in \operatorname{span}(E)} (x - \boldsymbol{\alpha} y),$$

where $\operatorname{span}(E)$ stands for the linear subspace of F^n spanned by the columns of E. The error span polynomial will play a similar role as the error locator polynomial in the BCH decoding algorithm. By the definition of $\boldsymbol{\beta}$, $\Lambda(x)$ can also be written as

$$\Lambda(x) = \prod_{z \in F^\rho} (x - \boldsymbol{\beta} z).$$

Clearly, $\deg \Lambda(x) = q^\rho$, which is the number of (simple) roots of $\Lambda(x)$ in Φ. Furthermore, since these roots form a linear space over F, $\Lambda(x)$ is a *linearized* polynomial of the form

$$\Lambda(x) = \sum_{m=0}^{\rho} \lambda_m x^{q^m}$$

with $\lambda_\rho = 1$ [12, pp. 118–119].

Once having the syndrome $\mathbf{s} = HZ\boldsymbol{\omega}$, the next decoding step is finding $\Lambda(x)$. For every integer L, $0 \le L \le r-1$, define the $(r-L)\times(L+1)$ matrix $\mathscr{A}_L$ over Φ by

$$\mathscr{A}_L = \begin{bmatrix} s_0^{q^n} & s_1^{q^n} & \cdots & s_L^{q^n} \\ s_1^{q^{n-1}} & s_2^{q^{n-1}} & \cdots & s_{L+1}^{q^{n-1}} \\ s_2^{q^{n-2}} & s_3^{q^{n-2}} & \cdots & s_{L+2}^{q^{n-2}} \\ \vdots & \vdots & \vdots & \vdots \\ s_{r-L-1}^{q^{n-(r-L-1)}} & s_{r-L}^{q^{n-(r-L-1)}} & \cdots & s_{r-1}^{q^{n-(r-L-1)}} \end{bmatrix}, \qquad 0 \le L \le r-1. \tag{12}$$

The significance of $\mathscr{A}_L$ will become apparent in the next two lemmas.

Lemma 2: Given an error array E of rank ρ, let $\boldsymbol{\lambda} = [\lambda_0 \lambda_1 \cdots \lambda_\rho]'$ be the vector of coefficients of the error span polynomial $\Lambda(x) = \sum_{m=0}^{\rho} \lambda_m x^{q^m}$ associated with E, and let $\mathscr{A}_\rho$ be the $(r-\rho)\times(\rho+1)$ matrix obtained by setting $L = \rho$ in (12). Then

$$\mathscr{A}_\rho \boldsymbol{\lambda} = \mathbf{0}.$$

Proof: Let $(\mathscr{A}_\rho \boldsymbol{\lambda})_l$ denote the lth entry of $\mathscr{A}_\rho \boldsymbol{\lambda}$, $0 \le l \le r - \rho - 1$. We have,

$$\begin{aligned} (\mathscr{A}_\rho \boldsymbol{\lambda})_l &= \sum_{m=0}^{\rho} \lambda_m s_{l+m}^{q^{n-l}} \overset{(10)}{=} \sum_{m=0}^{\rho} \lambda_m \left(\sum_{k=0}^{\rho-1} \delta_k \beta_k^{q^{l+m}} \right)^{q^{n-l}} \\ &= \sum_{k=0}^{\rho-1} \delta_k^{q^{n-l}} \sum_{m=0}^{\rho} \lambda_m \beta_k^{q^m} \\ &= \sum_{k=0}^{\rho-1} \delta_k^{q^{n-l}} \Lambda(\beta_k) = 0, \qquad 0 \le l \le r - \rho - 1. \qquad \square \end{aligned}$$

Let L_0 be the smallest L for which $\operatorname{rank}(\mathscr{A}_L) \le L$. By Lemma 2 we thus have $L_0 \le \rho$. Let $v(x) = \sum_{m=0}^{L_0} v_m x^{q^m}$ be a polynomial over Φ, corresponding to a nontrivial solution $\mathbf{v} = [v_0 v_1 \cdots v_{L_0}]'$ for the equation $\mathscr{A}_{L_0} \mathbf{v} = \mathbf{0}$. In the next lemma we show that any such polynomial must vanish at the set $\{\boldsymbol{\alpha} y \mid y \in \operatorname{span}(E)\}$; that is, the roots of $\Lambda(x)$ are all roots of $v(x)$. Hence, $L_0 \ge \rho$, implying the equality $L_0 = \rho$. Furthermore, $\mathbf{v}$ must be a scalar multiple of $\boldsymbol{\lambda}$ and, therefore, $\operatorname{rank}(\mathscr{A}_\rho) = \rho$.

Lemma 3: Let E be an error array of rank ρ and let L be an integer for which

$$\operatorname{rank}(\mathscr{A}_L) \le L \le r - \rho.$$

Let $\mathbf{v} = [v_0 v_1 \cdots v_L]'$ be a nontrivial solution over Φ for the equation $\mathscr{A}_L \mathbf{v} = \mathbf{0}$. Then the polynomial $v(x) = \sum_{m=0}^{L} v_m x^{q^m}$ vanishes at all points $\{\boldsymbol{\alpha} y \mid y \in \operatorname{span}(E)\}$.

Note that when $\rho \le r/2$ we always have

$$\operatorname{rank}(\mathscr{A}_\rho) \le \rho \le r - \rho.$$

Proof: Let $\mathbf{v}$ be a nontrivial solution for $\mathscr{A}_L \mathbf{v} = \mathbf{0}$; that is,

$$\sum_{m=0}^{L} v_m s_{l+m}^{q^{n-l}} = 0, \qquad 0 \le l \le r - L - 1.$$

By (10) we can write

$$\sum_{m=0}^{L} v_m \left(\sum_{k=0}^{\rho-1} \delta_k \beta_k^{q^{l+m}} \right)^{q^{n-l}} = \sum_{k=0}^{\rho-1} \delta_k^{q^{n-l}} \sum_{m=0}^{L} v_m \beta_k^{q^m} = 0, \qquad 0 \le l \le r - L - 1. \tag{13}$$

Let $\boldsymbol{\eta}$ be a row vector in Φ^ρ whose kth component is given by $\eta_k \triangleq \sum_{m=0}^{L} v_m \beta_k^{q^m} = v(\beta_k)$. By (13) we obtain

$$\sum_{k=0}^{\rho-1} \delta_k^{q^{n-l}} \cdot \eta_k = 0, \qquad 0 \le l \le r - L - 1,$$

or

$$\sum_{k=0}^{\rho-1} \delta_k \eta_k^{q^l} = 0, \qquad 0 \le l \le \rho - 1$$

(recall that $r - L \ge \rho$). By Lemma 1, $\boldsymbol{\delta} = D\boldsymbol{\omega}$ implies $\boldsymbol{\eta} D = \mathbf{0}$ and, since $\operatorname{rank}(D) = \rho$, we must have $\boldsymbol{\eta} = \mathbf{0}$. Hence, $v(\beta_k) =$

0 for all $0 \leq k \leq \rho - 1$. Now, $\upsilon(x)$ is a linearized polynomial and, therefore, for every vector $y \in F^n$ of the form $y = Uz$, $z = [z_0 z_1 \cdots z_{\rho-1}]' \in F^\rho$, we have

$$\upsilon(\boldsymbol{\alpha} y) = \upsilon(\boldsymbol{\alpha} Uz) = \upsilon(\boldsymbol{\beta} z) = \sum_{k=0}^{\rho-1} z_k \upsilon(\beta_k) = 0. \qquad \square$$

Lemma 3 thus establishes a way to obtain $\Lambda(x)$: we find the smallest L for which $\operatorname{rank}(\mathscr{A}_L) \leq L$, in which case we have $L = \rho = \operatorname{rank}(E)$ and $\operatorname{rank}(\mathscr{A}_\rho) = \rho$. Now, $\boldsymbol{\lambda} = [\lambda_0 \lambda_1 \cdots \lambda_\rho]'$ is the unique solution for $\mathscr{A}_\rho \boldsymbol{\lambda} = \mathbf{0}$ with $\lambda_\rho = 1$.

Having found $\Lambda(x)$, our next step is finding a basis of the linear space of roots of $\Lambda(x)$ in Φ. In this case it is convenient to represent Φ as a vector space over F with respect to the basis $\boldsymbol{\alpha}$. Now, multiplication by a scalar in Φ and raising to the power q^i, are both linear operations in Φ (regarded as a vector space over F). Hence, finding the root space of $\Lambda(x)$ reduces to finding a basis of a null space of a certain $n \times n$ matrix over F [5]. We can now set U to be an $n \times \rho$ matrix whose columns form a basis of that null space. Indeed, the columns of U span the columns of E, and we have $\Lambda(\gamma) = 0$ if and only if $\gamma = \boldsymbol{\alpha} Uz$ for some $z \in F^\rho$.

It remains to find an $n \times \rho$ matrix D over F such that $E = UD$. Recalling that $\boldsymbol{\delta} = D\boldsymbol{\omega}$, D can be found by extracting the first ρ equations in (11), yielding

$$s = \mathscr{B}\boldsymbol{\delta}, \tag{14}$$

where $\mathscr{B} \triangleq [\beta_k^{q^l}]_{l,k=0}^{\rho-1}$. Since $\operatorname{rank}(U) = \rho$, the entries of $\boldsymbol{\beta} = \boldsymbol{\alpha} U$ are linearly independent over F. Hence, by Lemma 1, $\mathscr{B}$ is nonsingular, allowing us to solve (14) for $\boldsymbol{\delta}$ and, consequently D.

Following is a summary of the decoding procedure to retrieve Γ out of $Z = \Gamma + E$, provided that $\operatorname{rank}(E) \leq r/2$.

a) Calculate the syndrome $s \leftarrow HZ\boldsymbol{\omega}$.
b) Find the smallest value ρ of L for which $\operatorname{rank}(\mathscr{A}_L) \leq L$, where $\mathscr{A}_L$ is given by (12).
c) Find a nontrivial solution $\boldsymbol{\lambda} = [\lambda_0 \lambda_1 \cdots \lambda_\rho]'$ over Φ for the equation $\mathscr{A}_\rho \boldsymbol{\lambda} = \mathbf{0}$.
d) Find a basis $\boldsymbol{\beta} = [\beta_0 \beta_1 \cdots \beta_{\rho-1}]$ of the root space in Φ of the error span polynomial $\Lambda(x) = \sum_{m=0}^{\rho} \lambda_m x^{q^m}$. This involves solving an n-variable homogeneous set of linear equations over F.
e) Solve $s = \mathscr{B}\boldsymbol{\delta}$ for $\boldsymbol{\delta}$, where $\mathscr{B} = [\beta_j^{q^i}]_{i,j=0}^{\rho-1}$.
f) Let $E \leftarrow UD$, where $\boldsymbol{\beta} = \boldsymbol{\alpha} U$ and $\boldsymbol{\delta} = D\boldsymbol{\omega}$ and, finally, let $\Gamma \leftarrow Z - E$.

A few improvements on this algorithm, along with a time complexity analysis, are given in the Appendix. In particular, it is shown that this algorithm requires $O(rn + r^3)$ arithmetic operations over Φ (each operation over Φ, in turn, can be implemented using $O(n^2)$ "naïve" operations over F, or by $O(n \log n \log\log n)$ operations over F if more sophisticated algorithms are used [18]). It is worthwhile noting that this is also the time-complexity required for decoding $[n, n-r, r+1]$ Reed–Solomon codes over Φ while using the Peterson–Gornstein–Zierler algorithm [4, Section 7.2]. Such Reed–Solomon codes can be regarded also as $[n \times n, n(n-r)]$ array codes over F for correcting up to $r/2$ erroneous rows. However, using the Berlekamp–Massey algorithm [3, Section 7.4] [12], the $O(r^3)$ complexity term reduces to only $O(r^2)$ operations over Φ. It remains open whether there exists an analog of the Berlekamp–Massey algorithm for carrying out Steps b), c), and e).

V. Maximum-Rank Codes over Infinite Fields

In Section I we presented a simple construction of $[n \times n, k, d]$ array codes $C_{n,d}$ over infinite fields for which $k = n(n-d+1)$. The question now is whether the Singleton bound can be attained also with respect to the minimum rank. In other words, can we construct μ-$[n \times n, k]$ array codes over infinite fields with $k = n(n - \mu + 1)$?

Consider first the case $\mu = n$, i.e., linear spaces of $n \times n$ nonsingular matrices (and the zero matrix), and assume that the field F is algebraically closed. We show that any n-$[n \times n, k]$ array code over F must have dimension $k = 1$. Otherwise, let A and B be two linearly independent matrices which span an n-$[n \times n, 2]$ array code over F. Clearly, both A and B are nonsingular and, therefore, without loss of generality, we can assume that $B = I$ (the identity matrix). Now, $A - \lambda I$ is nonzero and singular for any eigenvalue $\lambda \in F$ of A, contradicting the fact that every nontrivial linear combination of A and B is nonsingular.

The same proof applies also the real field $\mathbb{R}$ when n is odd. As for even values of n, we have the following result of Adams [1], [2]. Let b be the exponent of 2 in the prime factorization of n. Then, the maximum dimension of any n-$[n \times n, k]$ code over $\mathbb{R}$ equals $2b + \epsilon$, where $\epsilon = 1$ when $b \equiv 0 \pmod 4$, $\epsilon = 2$ when $b \equiv 3 \pmod 4$, and $\epsilon = 0$ otherwise. In particular, when $n = 2$ there exists an array code of dimension 2 over $\mathbb{R}$, which is isomorphic to the complex field, and when $n = 4$ there exists such a code of dimension 4, isomorphic to the ring of quaternions [11, p. 253].

This discussion on the case $\mu = n$ over algebraically closed fields is a simple special case of the upper bound $k \leq (n - \mu + 1)^2$, which applies to μ-$[n \times n, k]$ array codes for any μ over such fields. This bound has been obtained by Meshulam [14], using a result due to Westwick [20] which characterizes the set of $n \times n$ matrices of rank $\leq \mu - 1$ over algebraically closed fields as an irreducible variety of dimension $n^2 - (n - \mu + 1)^2$. In fact, the above upper bound turns out to be tight, in view of the following constructive lower bound.

Theorem 3: There exists a μ-$[n \times n, k = (n - \mu + 1)^2]$ array code over any infinite field F for any n and μ, $1 \leq \mu \leq n$.

Proof: The construction attaining the value $k = (n - \mu + 1)^2$ resembles the code $C_{n,d}$ given in Section I, except that the indexes of the diagonal entries are not extended cyclically modulo n. That is, for every code array $\Gamma = [c_{ij}]_{i,j=0}^{n-1}$, and for every integer m, $0 \leq m \leq n - \mu$, the diagonals $[c_{0,m} c_{1,m+1} \cdots c_{n-1-m,n-1}]'$ and $[c_{m,0} c_{m+1,1} \cdots c_{n-1,n-1-m}]'$ (coinciding with the main diagonal when $m = 0$) are codewords of an $[n - m, k = n - m - \mu + 1, \mu]$ MDS code over F. The rest of the entries of Γ are set to zero. The dimension of the resulting array code is given by

$$\begin{aligned} k &= (n - \mu + 1) + 2 \sum_{m=1}^{n-\mu} (n - m - \mu + 1) \\ &= (n - \mu + 1) + 2 \sum_{l=1}^{n-\mu} l = (n - \mu + 1)^2. \end{aligned}$$

Now, every nonzero Γ contains a lowest ("southwest") diagonal, which is nonzero. Such a diagonal contains at least μ nonzero elements, implying that $\operatorname{rank}(\Gamma) \geq \mu$. $\square$

Determining the maximum dimension of any μ-$[n \times n, k]$ array code over any infinite field for arbitrary μ remains still an open problem.

VI. Hyper-Array Codes: The Minimum-Distance Case

As mentioned in Section II, the general form of the Singleton bound with respect to d for $[n^{\times\Delta},k,d]$ hyper-array codes takes the form $k \le n(n^{\Delta-1}-d+1)$. Assume first that the underlying field is infinite. In this case, the Singleton bound is attained for every n and d, $1 \le d \le n^{\Delta-1}$, by a construction that is a generalization of the code $C_{n,d}$ presented in Section I. Given a hyper-array $\Gamma = [c_{i_0 i_1 \cdots i_{\Delta-1}}]_{i_0,i_1,\cdots,i_{\Delta-1}}$, the mth diagonal in Γ, $0 \le m \le n-1$, is defined as the $n^{\Delta-1}$-vector whose components are the entries $c_{i_0 i_1 \cdots i_{\Delta-1}}$ with $i_{\Delta-1} \equiv (m+\Sigma_{j=0}^{\Delta-2} i_j) \pmod n$, arranged according to some prespecified ordering of indexes. An $[n^{\times\Delta}, k=n(n^{\Delta-1}-d+1),d]$ hyper-array code is now obtained by setting every such diagonal to be a codeword of an $[n^{\Delta-1},n^{\Delta-1}-d+1,d]$ MDS code. It is easy to verify that any "row," obtained by fixing the values of any $\Delta-1$ indexes i_j, intersects each diagonal at exactly one entry. Hence, the weight of every nonzero hyper-array in the code is at least d. Clearly, the dimension of the resulting hyper-array code is $n(n^{\Delta-1}-d+1)$.

This construction can be applied to $F=\mathrm{GF}(q)$ whenever an $[n^{\Delta-1},n^{\Delta-1}-d+1,d]$ MDS code exists. However, this happens only when $d \in \{1,2,n^{\Delta-1}\}$, or when $n^{\Delta-1}$ is smaller than (say) $2q$. As for other values of d, we do not know yet of a general construction over F that attains the Singleton bound for $\Delta \ge 3$ (we can, of course, use other linear $[n^{\Delta-1},k,d]$ codes of relatively high minimum distance, but this leads to hyper-array codes of dimensions considerably below the Singleton bound). In fact, when $d=3$ (presumably the first nontrivial case), there exists a range of q, Δ and n for which the Singleton bound *cannot* be attained.

To show this, consider an $[n^{\times\Delta},k,3]$ hyper-array code C over $F=\mathrm{GF}(q)$, with $k=n(n^{\Delta-1}-2)$. The redundancy of C is therefore $2n$, and the number of cosets of C (excluding C) is $q^{2n}-1$. Let $\mathscr{W}_1$ be the set of all distinct weight-one $n^{\times\Delta}$ hyper-arrays over F. We must have $|\mathscr{W}_1| \le q^{2n}-1$, or else, there would be two distinct hyper-arrays $A,B \in \mathscr{W}_1$, belonging to the same coset of C, implying the existence of a weight-two hyper-array $A-B$ in C. Now, the number of hyper-arrays in $\mathscr{W}_1$, which contain exactly one nonzero entry is $n^\Delta(q-1)$, and the number of such arrays, containing at least two nonzero entries, is given by $\Delta n^{\Delta-1}(q^n-n(q-1)-1)$. Hence,

$$|\mathscr{W}_1| = n^\Delta(q-1)+\Delta n^{\Delta-1}(q^n-n(q-1)-1)$$
$$= \Delta n^{\Delta-1}(q^n-1)-(\Delta-1)n^\Delta(q-1).$$

This leads to the following "sphere-packing bound" on the parameters of C:

$$\Delta n^{\Delta-1}(q^n-1)-(\Delta-1)n^\Delta(q-1) \le q^{2n}-1. \qquad (15)$$

When q and Δ are fixed, (15) is satisfied for sufficiently large n; however, there might exist a (finite) range of n for which (15) does not hold. For example, when $\Delta=3$ and $q=2$, (15) is false for every $n<8$. Therefore, for this range of n, we cannot have binary $[n \times n \times n,k,3]$ codes attaining the Singleton bound. Sphere packing bounds like (15) can be obtained also for larger values of d, now bounding the number of hyper-arrays of weight $\le (d-1)/2$.

The following theorem presents a nonconstructive existence result for "good" hyper-array codes over finite fields.

Theorem 4: Given n and d, let k be an integer satisfying

$$\sum_{i=0}^{d-1}\binom{\Delta n^{\Delta-1}}{i}(q^n-1)^i < q^{n^\Delta-k+1}. \qquad (16)$$

Then there exists an $[n^{\times\Delta},k,d]$ hyper-array code over $F=\mathrm{GF}(q)$.

Proof: The proof is similar to that of the well-known Gilbert–Varshamov bound (see for instance, [3, pp. 321–322]). Let $K(n,d)$ denote the largest integer k satisfying (16). The idea of the proof is showing the existence of $[n^{\times\Delta},k,d]$ hyper-array codes C_k for all $1 \le k \le K(n,d)$, where C_k is obtained from C_{k-1} by adjoining certain cosets of the latter.

We start with the code C_1 consisting of the scalar multiples over F of the all-one hyper-array. Clearly, the minimum distance of C_1 is at least d (assuming $d \le n^{\Delta-1}$). We now show how to construct the code $C_k, k \le K(n,d)$, out of C_{k-1}. Given an $n^{\times\Delta}$ array A, we define the *projective coset* $\mathscr{H}(A)$ of C_{k-1} by

$$\mathscr{H}(A) = \{\lambda A+\Gamma \mid \lambda \in F-\{0\}, \Gamma \in C_{k-1}\}.$$

Let $\mathscr{H}_m$, $0 \le m \le M$, denote the distinct projective cosets of C_{k-1}. The $\mathscr{H}_m$ induce a partition on the space of $n^{\times\Delta}$ hyper-arrays over F, with $\mathscr{H}_0 \triangleq \mathscr{H}(0)=C_{k-1}$; any other $\mathscr{H}_m$ is a union of $q-1$ (conventional) distinct cosets of C_{k-1} and, therefore, the number of these $\mathscr{H}_m$ is $M=(q^{n^\Delta-k+1}-1)/(q-1)$. It remains to show that there exists a projective coset $\mathscr{H}_{m_0}$, $m_0>0$, containing hyper-arrays of weight $\ge d$ only. Having shown this, we then set $C_k \triangleq C_{k-1} \cup \mathscr{H}_{m_0}$, which is an $[n^{\times\Delta},k,d]$ linear hyper-array code.

Let $\mathscr{W}_i$ denote the set of all hyper-arrays of weight i. It is easy to verify that

$$|\mathscr{W}_i| \le \binom{\Delta n^{\Delta-1}}{i}(q^n-1)^i.$$

Now let $\mathscr{U}$ be the set of all nonzero hyper-arrays of weight $<d$ whose leading entry (according to some prespecified ordering of indexes) is 1. Clearly,

$$|\mathscr{U}| \le \frac{1}{q-1}\sum_{i=1}^{d-1}\binom{\Delta n^{\Delta-1}}{i}(q^n-1)^i.$$

To guarantee the existence of the coset $\mathscr{H}_{m_0}$, it suffices to require $|\mathscr{U}|<M$. The latter inequality is now implied by (16). □

Corollary 2: Let n, k, and d be integers satisfying

$$k \le n\left(n^{\Delta-1}-(d-1)\left(1+\frac{\log_q(\Delta n^{\Delta-1})}{n}\right)\right). \qquad (17)$$

Then there exists an $[n^{\times\Delta},k,d]$ hyper-array code over $F=\mathrm{GF}(q)$.

Proof: It is easy to verify that

$$\sum_{i=0}^{d-1}\binom{\Delta n^{\Delta-1}}{i}(q^n-1)^i \le \binom{\Delta n^{\Delta-1}}{d-1}q^{n(d-1)}$$
$$\le (\Delta n^{\Delta-1})^{d-1}q^{n(d-1)}.$$

Hence, (16) is implied by the inequality

$$n(d-1)+(d-1)\log_q(\Delta n^{\Delta-1}) < n^\Delta-k+1$$

which, in turn, is implied by (17). □

Observe that for fixed q and Δ, (17) becomes

$$k \leq n\left(n^{\Delta-1}-(d-1)(1+\epsilon_n)\right),$$

where $\lim_{n\to\infty}\epsilon_n = 0$, thus approaching the Singleton bound when n tends to infinity.

VII. Hyper-Array Codes: The Minimum-Rank Case

In this last section we obtain bounds on the dimension of μ-$[n^{\times\Delta}, k]$ hyper-array codes, in terms of the minimum rank μ. Unlike the case $\Delta = 2$, these bounds differ significantly from their minimum-distance counterparts, even when the underlying field is finite. To facilitate the forthcoming derivations, we shall concentrate on the *tensor* case ($\Delta = 3$), as a representative of the general hyper-array case.

We start by recalling the conventional definition of tensor rank. An $l \times m \times n$ nonzero tensor $T = [t_{ijh}]_{i=0,j=0,h=0}^{l-1,m-1,n-1}$ over a field F is called a *rank-one* tensor, if there exist $\boldsymbol{u} = [u_0 u_1 \cdots u_{l-1}] \in F^l$, $\boldsymbol{v} = [v_0 v_1 \cdots v_{m-1}] \in F^m$ and $\boldsymbol{w} = [w_0 w_1 \cdots w_{n-1}] \in F^n$, such that $t_{ijh} = u_i v_j w_h$ for all i, j, and h. The *rank* of an $l \times m \times n$ tensor Γ, denoted by $\operatorname{rank}(\Gamma)$, is defined as the smallest number ρ of rank-one tensors T_m, $0 \leq m \leq \rho-1$, such that $\Gamma = \sum_{m=0}^{\rho-1} T_m$. This definition of tensor rank extends in a straightforward manner to $n^{\times\Delta}$ hyper-arrays for larger Δ as well.

The following lemma is a direct generalization of a result obtained by Howell in [8]:

Lemma 4: The rank of any $l \times n \times n$ tensor over a field F, $l \leq n$, is at most $nl - \lfloor l^2/4 \rfloor$.

Here $\lfloor\cdot\rfloor$ and $\lceil\cdot\rceil$ stand for the floor and ceiling functions, respectively.

Theorem 5: For any μ-$[n \times n \times n, k]$ tensor code over a field F,

$$k \leq n(n^2 - \mu + 1 - \sigma^2),$$

where

$$\sigma \triangleq n - \left\lceil \sqrt{n^2-\mu+1} \right\rceil .$$

Theorem 5 implies that k is usually strictly smaller than the Singleton bound.

Proof: Let C be a μ-$[n \times n \times n, k]$ tensor code and suppose, to the contrary, that $k > n(n^2 - \mu + 1 - \sigma^2)$. Let τ be given by

$$\tau \triangleq \left\lceil \sqrt{n^2-\mu+1} \right\rceil^2 - (n^2-\mu+1).$$

Both σ and τ are nonnegative integers, satisfying the relation $n^2 - \mu + 1 + \tau = (n-\sigma)^2$, or

$$2n\sigma + \tau = \mu - 1 + \sigma^2. \tag{18}$$

We also verify that $2n\sigma + \tau < n^2$. Indeed, by Lemma 4, $\mu - 1 < \frac{3}{4}n^2$ and, so, $\sqrt{n^2-\mu+1} > n/2$. Hence,

$$n < \sqrt{n^2-\mu+1} + \left\lceil \sqrt{n^2-\mu+1} \right\rceil$$

which, by the definition of σ, implies $\sigma^2 < n^2 - \mu + 1$. Therefore, $2n\sigma + \tau = \mu - 1 + \sigma^2 < n^2$.

Our contrary assumption can now be rewritten as

$$k > n(n^2 - 2n\sigma - \tau) \tag{19}$$

(where the right-hand side of (19) is positive).

The rest of the proof resembles that of the Singleton bound. For a tensor $T = [c_{ijh}]_{i=0,j=0,h=0}^{l-1,n-1,n-1}$, let $T(s)$ denote the $n \times n$ matrix defined by $T(s) = [c_{sjh}]_{j=0,h=0}^{n-1,n-1}$, $0 \leq s \leq l-1$. That is, $T(s)$ stands for the sth *slice* of T. Let $T_0, T_1, \cdots, T_{k-1}$ be a basis of the code C. Also, let B be the $k \times (n(n^2 - 2n\sigma - \tau))$ matrix whose mth row is the concatenation of the last $n^2 - 2n\sigma - \tau$ rows of T_m, where we start with the n rows of $T_m(n-1)$, continue with the rows of $T_m(n-2)$, and so forth. Since $\operatorname{rank}(B) \leq n(n^2 - 2n\sigma - \tau) < k$, there exists a nonzero vector $\boldsymbol{y} = [y_0 y_1 \cdots y_{k-1}]$ over F such that $\boldsymbol{y}B = \boldsymbol{0}$. Hence, the last $n^2 - 2n\sigma - \tau$ rows of the nonzero tensor $\Gamma \triangleq \sum_{m=0}^{k-1} y_m T_m$ are all zero. Let Γ_0 be the $(2\sigma) \times n \times n$ tensor consisting of the first 2σ slices of Γ i.e., $\Gamma_0(s) = \Gamma(s)$, $0 \leq s \leq 2\sigma - 1$, and let Γ_1 be the $(n-2\sigma) \times n \times n$ tensor given by the rest of the slices of Γ ($\Gamma_1(s) = \Gamma(s + 2\sigma)$, $0 \leq s \leq n - 2\sigma - 1$). By Lemma 4, $\operatorname{rank}(\Gamma_0) \leq 2n\sigma - \sigma^2$. As for Γ_1, we have just shown that the number of nonzero rows in Γ_1 is at most τ, and therefore $\operatorname{rank}(\Gamma_1) \leq \tau$. From the definition of tensor rank we have, $\operatorname{rank}(\Gamma) \leq \operatorname{rank}(\Gamma_0) + \operatorname{rank}(\Gamma_1)$ and, so,

$$\operatorname{rank}(\Gamma) \leq 2n\sigma - \sigma^2 + \tau .$$

Hence, by (18), $\operatorname{rank}(\Gamma) \leq \mu - 1$, contradicting the definition of μ. □

It can be shown that the tight upper bound on k is usually strictly smaller than the Singleton bound also for larger values of Δ. For sufficiently large n, Δ, and μ, we have the following asymptotic result.

Theorem 6: For μ-$[n^{\times\Delta}, k]$ codes over a field F,

$$k \leq n\left(n^{\Delta-1} - 2\mu(1-\epsilon_{n,\theta})\right),$$

where $\theta \triangleq \lfloor \log_n \mu \rfloor$ $(\leq \Delta - 1)$ and $\lim_{n,\theta\to\infty}\epsilon_{n,\theta} = 0$.

Proof: Let $\rho(n,\theta)$ denote the maximum rank of any $n^{\times\theta}$ hyper-array over F. It is known that

$$\rho(n,\theta) \leq \tfrac{1}{2}\cdot n^{\theta-1}\cdot(1+\delta_{n,\theta}),$$

where $\lim_{n,\theta\to\infty}\delta_{n,\theta} = 0$ [8]. Now, let $m \triangleq \lfloor(\mu-1)/\rho(n,\theta)\rfloor$, and suppose there exists a μ-$[n^{\times\Delta}, k]$ code C such that $k > n^\Delta - m\cdot n^\theta$. As in the proofs of Theorems 1 and 5, there must exist a nonzero $n^{\times\Delta}$ array $\Gamma \in C$ which, when sliced into $n^{\times\theta}$ hyper-arrays, contains at most m such nonzero slices. Hence,

$$\operatorname{rank}(\Gamma) \leq m\cdot\rho(n,\theta) \leq \mu - 1,$$

a contradiction. We thus have

$$\begin{aligned}
k &\leq n^\Delta - m\cdot n^\theta = n^\Delta - \left\lfloor \frac{\mu-1}{\rho(n,\theta)} \right\rfloor \cdot n^\theta \\
&< n^\Delta - \frac{(\mu-1)n^\theta}{\rho(n,\theta)} + n^\theta \leq n^\Delta - \frac{2n(\mu-1)}{1+\delta_{n,\theta}} + \mu \\
&\leq n\left(n^{\Delta-1} - 2\mu(1-\epsilon_{n,\theta})\right),
\end{aligned}$$

where $\lim_{n,\theta\to\infty}\epsilon_{n,\theta} = 0$. □

A nonconstructive existence result is given by the following theorem.

Theorem 7: Given n and μ, let k be an integer satisfying

$$\sum_{i=0}^{\mu-1} \binom{(q^n-1)^3/(q-1)^2}{i} < q^{n^3-k+1}. \tag{20}$$

Then there exists a μ-$[n \times n \times n, k]$ tensor code over $F = \mathrm{GF}(q)$.

Proof: The proof is similar to that of Theorem 4, except that here we count the number of tensors whose rank (rather than weight) is smaller than μ. The number of $n \times n \times n$ tensors of rank i is bounded from above by the number of (unordered) sets of i distinct rank-one tensors. Now, the number of $n \times n \times n$ rank-one tensors is equal to the number of ordered triples $(\boldsymbol{u},\boldsymbol{v},\boldsymbol{w})$, where $\boldsymbol{u}$, $\boldsymbol{v}$, and $\boldsymbol{w}$ are nonzero vectors in F^n and, in addition, $\boldsymbol{v}$ and $\boldsymbol{w}$ are normalized to have a leading nonzero coefficient one. The number of tensors of rank $< \mu$ is now upper-bounded by the left-hand side of (20). □

The left-hand side of (20), in turn, is bounded from above by $q^{3n(\mu-1)}$, leading to the following corollary.

Corollary 3: Let n, k, and μ be integers satisfying

$$k \le n(n^2 - 3(\mu - 1)).$$

Then there exists a μ-$[n \times n \times n, k]$ tensor code over $F = \mathrm{GF}(q)$.

The lower bound on the maximum tensor rank obtained by Howell in [8] can be viewed as a special case of Corollary 3, corresponding to $k = 1$. The extension of Theorem 7 and Corollary 3 to larger Δ is straightforward, yielding $k \le n(n^{\Delta-1} - \Delta(\mu - 1))$ as a sufficient condition for the existence of a μ-$[n^{\times\Delta}, k]$ hyper-array code over $\mathrm{GF}(q)$. Using the proof techniques introduced in [8], it can be shown that Corollary 3 holds for infinite fields as well (this generalization will not be presented here). Finding explicit constructions for tensor codes of high minimum rank for any value of n is still an open problem, even when $k = 1$. For related work see, for instance [8], [10], [19].

Acknowledgment

The results of this paper have been motivated by the numberless discussions I have had with Mario Blaum, to whom I am deeply grateful. I also wish to thank Noga Alon and Roy Meshulam for the helpful discussions, especially regarding the known results summarized in Section V.

Appendix

This Appendix contains a time complexity estimate and some implementation considerations regarding the decoding algorithm of maximum-rank array codes. We refer to the notations and the algorithm steps as they appear in Section IV.

Step a): Calculating the syndrome requires $O(rn)$ operations over $\Phi = \mathrm{GF}(q^n)$ for multiplying the $r \times n$ matrix H by the input vector $Z\boldsymbol{\omega}$.

Steps b) and c): To find the rank of $\mathscr{A}_L$, $L \le r/2$, and solve for $\boldsymbol{\lambda}$, it suffices to consider the $\lfloor r/2 \rfloor \times (L+1)$ matrix $\mathscr{A}_L{}^*$ consisting of the first $\lfloor r/2 \rfloor$ rows of $\mathscr{A}_L$. Note that $\mathscr{A}_L{}^*$ consists also of the first $L+1$ columns of $\mathscr{A}_{\lceil r/2 \rceil}$, and therefore, by Lemma 3, any solution for $\mathscr{A}_L{}^* \boldsymbol{v} = \boldsymbol{0}$ represents a polynomial $v(x)$, which is divisible by $\Lambda(x)$. Hence, Step b) can be performed by Gaussian elimination, starting with $\mathscr{A}_0{}^*$, and adding each column of $A_{\lceil r/2 \rceil}$ at a time, until the resulting matrix $\mathscr{A}_L{}^*$ has rank $\le L$. This procedure, along with solving $\mathscr{A}_L{}^* \boldsymbol{\lambda} = \boldsymbol{0}$ for $\boldsymbol{\lambda}$, requires $O(r^3)$ operations over Φ.

The entries of $\mathscr{A}_L{}^*$, in turn, can be obtained by first finding the values $s_l^{q^{n-l}}$, $0 \le l \le r-1$, as images of s_l under the fixed linear transformations $x \mapsto x^{q^{n-l}}$ over Φ, requiring $O(rn^2)$ operations over $F = \mathrm{GF}(q)$. The rest of the entries of $\mathscr{A}_L{}^*$, $L = 1, 2, \cdots, \lfloor r/2 \rfloor$, can now be obtained by $O(r^2)$ raises to the power q over Φ.

Step d): A basis $\boldsymbol{\beta} = \boldsymbol{\alpha} U$ of the roots of $\Lambda(x)$ in Φ can be found by first representing the mapping $x \mapsto \Lambda(x)$ as an $n \times n$ matrix T_Λ over F, the jth column of which is the representation of $\Lambda(\alpha_j)$, $0 \le j \le n-1$, with respect to some basis of Φ over F. Using (fixed) tables for the values of $\alpha_j^{q^m}$, $0 \le j \le n-1$, $0 \le m \le r/2$, the computation of T_Λ requires $O(rn)$ operations over Φ. A basis U of the right null space of T_Λ can now be obtained by Gaussian elimination on the rows of T_Λ, involving $O(rn^2)$ operations over F.

Steps e) and f): Calculating the matrix $\mathscr{B}$ and solving for $\boldsymbol{\delta}$ sum up to $O(r^3)$ operations over Φ; finally, multiplying U and D requires $O(rn^2)$ operations over F.

Adding the time complexities of Steps a)–f), and recalling that the implementation of every arithmetic operation over Φ requires at least n operations over F, we end up with $O(rn + r^3)$ operations over Φ.

References

[1] J. F. Adams, "Vector fields on spheres," *Ann. Math.*, vol. 75, pp. 603–632, 1962.

[2] J. F. Adams, P. D. Lax, and R. S. Phillips, "On matrices whose real linear combinations are nonsingular," *Proc. AMS*, vol. 16, 1965, pp. 318–322.

[3] E. R. Berlekamp, *Algebraic Coding Theory*. New York: McGraw-Hill, 1968.

[4] R. E. Blahut, *Theory and Practice of Error Control Codes*. Reading, MA: Addison-Wesley, 1983.

[5] E. R. Berlekamp, H. Rumsey, and G. Solomon, "On the solution of algebraic equations over finite fields," *Inform Contr.*, vol. 10, pp. 553–564, 1967.

[6] M. Blaum and R. J. McEliece, "Coding protection for magnetic tapes: a generalization of the Patel–Hong code," *IEEE Trans. Inform. Theory*, vol. IT-31, no. 5, pp. 690–693, Sept. 1985.

[7] S. A. Elkind and D. P. Siewiorek, "Reliability and performance of error-correcting memory and register codes," *IEEE Trans. Comput.*, vol. C-29, pp. 920–927, 1980.

[8] T. D. Howell, "Global properties of tensor rank," *Linear Algebra Appl.*, vol. 22, pp. 9–23, 1978.

[9] L. Levine and W. Meyers, "Semiconductor memory reliability with error detecting and correcting codes," *Comput.*, vol. 9, pp. 43–50, Oct. 1976.

[10] T. Lickteig, "Typical tensorial rank," *Linear Algebra Appl.*, vol. 69, pp. 95–120, 1985.

[11] S. MacLane and G. Birkhoff, *Algebra*. New York: Macmillan, 1967.

[12] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1977.

[13] J. L. Massey, "Shift-register synthesis and BCH decoding," *IEEE Trans. Inform. Theory*, vol. IT-15, pp. 122–127, 1969.

[14] R. Meshulam, Private communication.

[15] W. F. Mikhail, R. W. Bartoldus, and R. A. Rutledge, "The reliability of memory with single-error correction," *IEEE Trans. Comput.*, vol. C-31, pp. 560–564, 1983.

[16] A. M. Patel and S. J. Hong, "Optimal rectangular code for high density magnetic tapes," *IBM J. Res. Dev.*, vol. 18, pp. 579–588, 1974.

[17] P. Prunsinkiewicz and S. Budkowski, "A double track error-correction code for magnetic tape," *IEEE Trans. Comput.*, vol. C-25, pp. 642–645, 1976.

[18] V. Schönhage, "Schnelle Multiplikation von Polynomen über Körpern der Charakteristik 2," *Acta Informatica*, vol. 7, pp. 395–398, 1977.

[19] V. Strassen, "Rank and optimal computation of generic tensors," *Linear Algebra Appl.*, vol. 52/53, pp. 645–685, 1983.

[20] R. Westwick, "Spaces of linear transformations of equal rank," *Linear Algebra Appl.*, vol. 5, pp. 49–64, 1972.