Probabilistic Crisscross Error Correction

Ron M. Roth*

Abstract

The crisscross error model in data arrays is considered, where the corrupted symbols are confined to a prescribed number of rows or columns (or both). Under the additional assumption that the corrupted entries are uniformly distributed over the channel alphabet, and by allowing a small decoding error probability, a coding scheme is presented where the redundancy can get close to one half the redundancy required in minimum-distance decoding of crisscross errors.

Keywords: Crisscross errors, Rank metric, Probabilistic coding.

*Hewlett-Packard Laboratories, 1501 Page Mill Road, Palo Alto, CA 94304, USA. On sabbatical leave from the Computer Science Department, Technion, Haifa 32000, Israel. e-mail: ronny@cs.technion.ac.il. Part of this work was done at Hewlett-Packard Israel Science Center, Haifa, Israel.

1 Introduction

Consider an application where information symbols (such as bits or bytes) are stored in $m \times n$ arrays, with the possibility of some of the symbols recorded erroneously. The error patterns are such that all corrupted symbols are confined to a prescribed number of rows or columns (or both). We refer to such an error model as *crisscross errors*. A crisscross error pattern that is confined to two rows and three columns is shown in Figure 1.

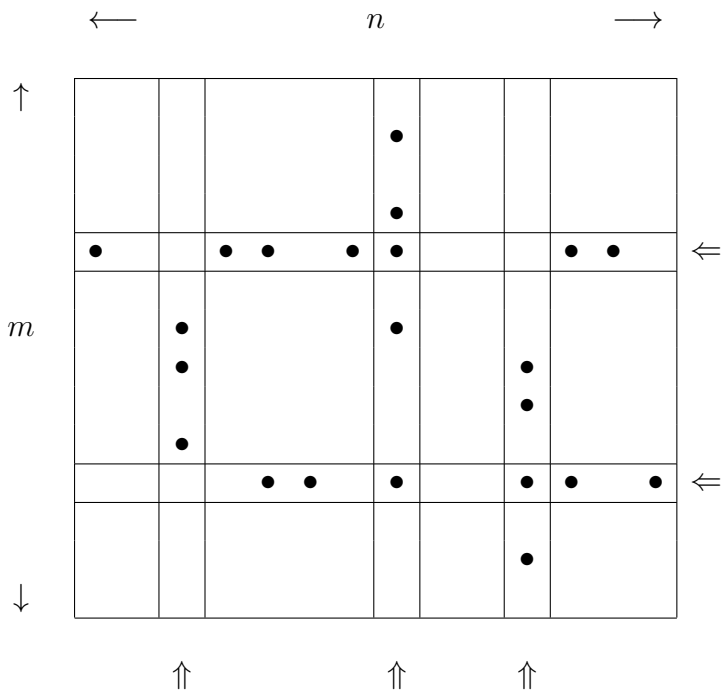

Figure 1: Typical crisscross error pattern.

Crisscross errors can be found in various data storage applications; see, for instance, [3], [5], [6], [11], [16], [17], [18], [19]. Such errors may occur in memory chip arrays, where row or column failures occur due to the malfunctioning of row drivers or column amplifiers. Crisscross errors can also be found in helical tapes, where the tracks are recorded in a direction which is (conceptually) perpendicular to the direction of the movement of the tape; misalignment of the reading head causes burst errors to occur along the track (and across the tape), whereas scratches on the tape usually occur along the tape (and across the tracks). Crisscross error-correcting codes can also be applied in linear magnetic tapes, where the tracks are written along the direction of the movement of the tape and, therefore, scratches cause bursts to occur along the tracks; still, the information and check symbols are usually recorded across the tracks. Computation of check symbols is equivalent to decoding of erasures at the check locations, and in this case these erasures are perpendicular to the erroneous tracks.

Crisscross errors can be analyzed through the following cover metric. A *cover* of an $m \times n$ array Γ over a field F is a set of rows or columns that contain all the nonzero entries in Γ. The *cover weight* of Γ, denoted $\mathsf{w}_{\mathrm{cov}}(\Gamma)$, is the size of the smallest cover of Γ. The *cover distance* between two $m \times n$ arrays over F is the cover weight of their difference. An $[m \times n, k, d_{\mathrm{cov}}]$ array code over F is a k-dimensional linear subspace $\mathcal{C}$ of the vector space of all $m \times n$ matrices over F such that d_{cov} is the smallest cover distance between any two distinct elements of $\mathcal{C}$ or, equivalently, the smallest cover weight of any nonzero element of $\mathcal{C}$. The parameter d_{cov} is referred to as the *minimum cover distance* of $\mathcal{C}$ and the term $mn-k$ stands for the *redundancy* of $\mathcal{C}$.

The Singleton bound on the minimum cover distance states that the minimum cover distance and the redundancy of any $[m \times n, k, d_{\mathrm{cov}}]$ array code over a field F satisfy the relation

$$mn - k \;\geq\; (d_{\mathrm{cov}} - 1)\, n \;, \tag{1}$$

where we assume that $m \leq n$ (see [9] and [19]).

Let Γ be the "transmitted" array and $Y = \Gamma + E$ be the "received" array, where E is the error array. The number of crisscross errors is bounded from below by $\mathsf{w}_{\mathrm{cov}}(E)$. Since cover distance is a metric, then by using an $[m \times n, k, d_{\mathrm{cov}}]$ array code, we can recover any pattern of up to $(d_{\mathrm{cov}}-1)/2$ crisscross errors. On the other hand, if we wish to be able to recover *any* pattern of up to t crisscross errors, then we *must* use an array code with minimum cover distance which is at least $2t+1$. The Singleton bound on the minimum cover distance implies that the number of redundancy symbols must be at least $2tn$, namely, at least twice the maximum number of erroneous symbols that need to be corrected.

A simple constructive technique to combat crisscross errors is through the *skewing method* which we explain next (see [9], [19], [20]). Let C be a conventional linear $[m, \ell, d_{\mathrm{cov}}]$ code over F, namely, C has length m, dimension ℓ, and minimum Hamming distance d_{cov}. We define the array code $\mathcal{C}$ as the set of all $m \times n$ arrays $\Gamma = [\,\Gamma_{i,j}\,]_{i,j=1}^{m,n}$ over F in which for each integer $h = 0, 1, \ldots, n-1$, the vector $[\,\Gamma_{1,h+1}\;\Gamma_{2,h+2}\;\ldots\Gamma_{m,h+m}\,]$ is a codeword of C (indexes are reduced modulo n into the range $\{1, 2, \ldots, n\}$). It is easy to verify that $\mathcal{C}$ is an $[m \times n, k = n\ell, d_{\mathrm{cov}}]$ array code whenever $m \leq n$. Furthermore, if C is a maximum-distance separable (MDS) code, then $d_{\mathrm{cov}} = m-\ell+1$ and so $\mathcal{C}$ attains the Singleton bound (1) on the cover distance. Yet, for nontrivial values of ℓ, the code C can be taken to be MDS only when its code length is small, i.e., $m \leq |F|+2$ [14, Ch. 11].

In [9] and [19], it was shown how crisscross errors can be handled by applying array codes for the *rank metric*. This approach yields array codes that attain the Singleton bound (1) without any restrictions on m. A μ-$[m \times n, k]$ array code $\mathcal{C}$ over a field F is a k-dimensional linear subspace of the vector space of all $m \times n$ matrices over F such that μ is the smallest rank of any nonzero matrix in $\mathcal{C}$. The parameter μ is referred to as the *minimum rank* of $\mathcal{C}$.

The Singleton bound on the minimum rank takes the form

$$mn - k \;\geq\; (\mu - 1)\, n \;, \tag{2}$$

where we assume that $m \leq n$. This bound was stated by Delsarte in [4]; see also Gabidulin [8] and Roth [19]. Furthermore, those references contain a construction of μ-$[n \times n, k]$ array codes over the field $\mathsf{F}_q = GF(q)$ that attain this bound for every $\mu \leq n$. We describe next this optimal construction, which we denote by $\mathcal{C}_q(n, s)$, where $\mu = s{+}1$. Let $\boldsymbol{\alpha} = [\,\alpha_i\,]_{i=1}^{n}$ be a row vector over $\mathsf{F}_{q^n} = GF(q^n)$ and $\boldsymbol{\omega} = [\,\omega_j\,]_{j=1}^{n}$ be a column vector over F_{q^n}, each vector having entries that are linearly independent over F_q. The array code $\mathcal{C}_q(n, s)$ consists of all $n \times n$ matrices $\Gamma = [\,\Gamma_{i,j}\,]_{i,j=1}^{n}$ over F_q such that

$$\sum_{i,j=1}^{n} \Gamma_{i,j}\, \alpha_i^{q^\ell}\, \omega_j \;=\; 0\;, \qquad 0 \leq \ell < s\;. \tag{3}$$

Two polynomial-time decoding algorithms for $\mathcal{C}_q(n, s)$ are presented in [8] and [19] for recovering any error pattern of rank $\leq s/2$. The construction $\mathcal{C}_q(n, s)$ can be generalized to obtain optimal $(s{+}1)$-$[m \times n, k]$ array codes by means of code shortening. Namely, to form an $(s{+}1)$-$[m \times n, (m{-}s)n]$ array code for $m \leq n$ out of an $(s{+}1)$-$[n \times n, (n{-}s)n]$ code, we take the $m \times n$ upper blocks of all the arrays of the latter code in which the last $n{-}m$ rows are zero.

The application of μ-$[m \times n, k]$ array codes to crisscross error correction is based upon the observation that matrix rank is a metric and that the cover weight of an array is bounded from below by its rank. By using the elements of a μ-$[m \times n, k]$ array code for transmission (or recording), we can recover any error array of rank $\leq (\mu{-}1)/2$ and, therefore, we can correct any pattern of up to $(\mu{-}1)/2$ crisscross errors. Thus, every μ-$[m \times n, k]$ array code is also an $[m \times n, k, \mu]$ array code. The array codes defined by (3) are optimal with respect to the bound (2) and, as such, they are optimal with respect to (1).

Still, such an optimality criterion is based upon a worst-case decoding strategy where we are interested in being able to decode *any* pattern of up to t crisscross errors, thus requiring to have at least $2tn$ redundancy symbols. The purpose of this work is to show that, by assuming a uniform distribution on the error values in each error location, and by allowing an acceptable small decoding error probability, significant savings in the redundancy can be obtained. (By decoding error we mean that the decoded array is different from the transmitted array.) More specifically, we assume that the noisy channel acts on the transmitted $n \times n$ array Γ over $\mathsf{F}_q = GF(q)$ as follows:

(P1) The noisy channel selects a set $\mathcal{X}_{\rm r}$ of row indexes and a set $\mathcal{X}_{\rm c}$ of column indexes such that $|\mathcal{X}_{\rm r}| + |\mathcal{X}_{\rm c}| \leq t$. Note that no assumption is made on the selection of $\mathcal{X}_{\rm r}$ and $\mathcal{X}_{\rm c}$ other than limiting the sum of their sizes to be at most t. In particular, we do not assume any a priori probabilistic behavior on such a selection.

(P2) The channel marks entries in Γ within the rows and columns that were selected in (P1). Again, except for their confinement to the rows and columns indexed by $\mathcal{X}_{\rm r}$ and $\mathcal{X}_{\rm c}$, no a priori assumption is made on the location of the entries that are marked.

(P3) Each marked entry in Γ is set to a value which is uniformly distributed over F_q and is statistically independent of the values chosen for the other marked entries in Γ. (In particular, a marked entry may still maintain the correct value with probability $1/q$.)

Condition (P3) is where we insert a probabilistic characterization into our channel model, whereas conditions (P1) and (P2) still follow the conservative (worst-case) setting. (Note however that in practice, the parameter t will also be set by probabilistic arguments, namely, requiring that the probability of having more than t crisscross errors be sufficiently small.) With the introduction of an allowable decoding error probability, we will take advantage of condition (P3) in our construction to reduce the code redundancy. More specifically, we show in Theorem 2 below that for a range of values of t which is linear in n, there is an explicit array coding scheme that attains decoding error probability which is exponentially decreasing with n, while requiring redundancy which is close to tn. Note that we must have at least tn redundancy symbols if the allowed decoding error probability of an array is less than $1-(1/q)$. This follows from the fact that conditions (P1) and (P2) in our model of the channel allow to have as many as tn marked entries in the array.

Condition (P3) in our model of the channel seems to approximate rather well the situation in reality, where crisscross errors are caused mainly by bursts. Bursts tend to overwrite the original data in Γ independently of that data. In some cases, however, the retrieved bursty stream, which appears as rows or columns in $\Gamma + E$, might have a relatively small number of typical patterns (e.g., tendency of the patterns to contain runs of the same symbol). In such cases, we make the array Γ appear random by the use of pseudo-random generators (i.e., scramblers), thus forcing the error values in the error array E to look random.

For other models of errors, the study of codes that exploit the probabilistic nature of the channel is, of course, not new. For symmetric memoryless channels (i.e., random errors), Forney's concatenated construction [7] provides codes that attain the Shannon capacity with decoding error probability which decreases exponentially with the code length. Forney's codes can be *decoded* in polynomial time; however, in order to construct those codes, we need to search over the best inner code which, in turn, requires super-polynomial time complexity (see the discussion in [15, pp. 125–127]). For the decoding error probability of algebraic geometric codes, see [10].

The case of phased burst errors is more tractable through the use of product codes (which are, in effect, concatenated codes) [13, pp. 274–278]. Assuming that bursts cause rows (but not columns) in the array to be corrupted and that a corrupted entry is uniformly distributed over F_q, then the horizontal code in the product-code scheme can be used to detect the corrupted rows with sufficiently high probability, thus marking those rows as erasures for the vertical code. Improvements on this basic strategy exist (see [21]) where the redundancy can get close to one half the redundancy of worst-case coding where no assumption is made on the uniformity of the corrupted entries. Yet, such a strategy seems to fail when we attempt to apply it to the crisscross case where both rows and columns can

get corrupted. We also do not know how to exploit the probabilistic model of the channel to obtain any savings in the redundancy while using the skewing method that we previously discussed.

The construction presented in this paper is based on the rank-metric approach. Section 2 contains the description of our new codes and an upper bound on their redundancy. An analysis of the correction capability of those codes is given in Section 3, followed by a decoding algorithm in Section 4.

2 Code construction

In this section, we describe a construction of $[n \times n, k]$ array codes $\mathsf{C}_q(n, t, \mathsf{p})$ over F_q that can correct patterns of up to t crisscross errors with decoding error probability which is less than p. By this probability we mean that for any selection of marked entries according to conditions (P1) and (P2), the probability that the values that are chosen according to (P3) result in an uncorrectable error array is less than p. The full analysis of the correction capability of $\mathsf{C}_q(n, t, \mathsf{p})$ is deferred to Section 3. For the sake of simplicity we deal here with constructions of $[m \times n, k]$ array codes where $m = n$. The general case can be handled by code shortening.

Let the following parameters be given: a field size q, an order n of code arrays, a parameter t which is the maximum number of crisscross errors that may need correction, and a probability p of failing to decode an array.

Definition 1 *Given n, t, p, and q, let d be given by*

$$d \;=\; \left\lceil \tfrac{3}{2}t \right\rceil + 1 + \left\lceil \log_q \binom{n}{\lceil t/2 \rceil} + \log_q \tfrac{1}{\mathsf{p}} - \log_q \tfrac{q-1}{2} \right\rceil \;. \tag{4}$$

Also, let r be an integer such that that there exists a conventional linear $[n, n-r, d]$ code over F_q and let H_1 and H_2 be $r \times n$ parity-check matrices over F_q of such a code (i.e., every $d-1$ columns in each of those matrices are linearly independent). The array code $\mathsf{C}_q(n, t, \mathsf{p})$ is defined as the set of all $n \times n$ arrays Γ over F_q such that

$$\Gamma \in \mathcal{C}_q(n, t) \quad \textit{and} \quad H_1 \Gamma H_2^T \in \mathcal{C}_q(r, 2t) \;.$$

Clearly, the code $\mathsf{C}_q(n, t, \mathsf{p})$ is a linear space over F_q (and, hence, can be encoded as any linear code through a generator matrix). The following proposition immediately follows from the definition of $\mathsf{C}_q(n, t, \mathsf{p})$.

Proposition 1 *The redundancy of $\mathsf{C}_q(n, t, \mathsf{p})$ is bounded from above by $tn + 2tr$.*

Example 1 Suppose that H_1 and H_2 are taken to be parity-check matrices of (extended) BCH codes over F_q. For such codes we have

$$r \;\le\; (d-1)\cdot\lceil \log_q n\rceil \;\le\; \left\lceil \left\lceil \tfrac{3}{2}t\right\rceil + \left\lceil \tfrac{t}{2}\right\rceil \log_q n + \log_q \tfrac{1}{\mathsf{p}} - \log_q \tfrac{q-1}{2}\right\rceil \cdot \lceil \log_q n\rceil \;. \tag{5}$$

Let δ be a positive real and suppose that

$$t \;<\; \lfloor \delta n/(\log_q n)^2\rfloor \quad \text{and} \quad \mathsf{p} \;=\; 2^{-\delta n/\log_2 n} \;. \tag{6}$$

Plugging those values into (5), we obtain

$$r \;\le\; f(\delta)\cdot n \;, \quad \text{where} \quad \lim_{\delta\to 0} f(\delta) = 0 \;.$$

Hence, by Proposition 1 it follows that for every $\epsilon > 0$ there is $\delta > 0$ such that we can attain redundancy less than $tn(1+\epsilon)$ with values of t and p that satisfy (6). □

Asymptotically better codes can be obtained if H_1 and H_2 are taken as parity-check matrices of 'good' conventional codes such as Justesen codes [14, Ch. 10]. We state this in the next theorem.

Theorem 2 *For every $\epsilon > 0$ there is $\delta > 0$ such that the redundancy of $\mathsf{C}_q(n,t,\mathsf{p})$ is less than $tn(1+\epsilon)$ whenever t and p satisfy*

$$t \;<\; \lfloor \delta n\rfloor \quad \textit{and} \quad \mathsf{p} \;=\; q^{-\delta n} \;. \tag{7}$$

Proof. Recall that for every $\epsilon_0 > 0$ there is $\delta_0 > 0$ such that there exist $[n, n-r, d]$ Justesen codes over F_q with $r \le \lceil \epsilon_0 n\rceil$ and $d > \lceil \delta_0 n\rceil$. Let H_1 and H_2 be parity-check matrices of Justesen codes over F_q and, for $\delta > 0$, let t and p satisfy (7). The value of d which is given by (4) satisfies the inequality

$$d \;\le\; \left\lceil \tfrac{3}{2}\delta n + \mathsf{H}_q(\delta/2)n + \delta n - \log_q \tfrac{q-1}{2}\right\rceil \;,$$

where $\mathsf{H}_q(x)$ is the base-q entropy function $-x\log_q x - (1-x)\log_q(1-x)$ and where we have used the inequality $\log_q \binom{n}{m} \le n\mathsf{H}_q(m/n)$ [14, p. 309]. The theorem now follows from Proposition 1. □

In Section 3 we show that $\mathsf{C}_q(n,t,\mathsf{p})$ can be decoded with decoding error probability less than p. Combining that result with Theorem 2, it will follow that for a range of values of t which is linear in n, we can attain with $\mathsf{C}_q(n,t,\mathsf{p})$ decoding error probability which is exponentially decreasing with n, while requiring redundancy which is close to tn, namely one half the redundancy of $\mathcal{C}_q(n,2t)$.

We point out that the decoding error probability in Theorem 2 decreases exponentially with n, and not with the array size, n^2. Recall, however, that the selection of the rows

and columns in (P1) is governed in practice by an underlying probabilistic model (from which we compute the parameter t), and such a model will typically dictate a decoding error probability which decreases no faster than $2^{-O(n)}$. As an example, suppose that a row or column is selected by the channel with a fixed probability π, independently of the other rows or columns, and that all entries in a selected row or column are marked. Under such a model, the probability of having more than tn marked entries in the array is at least the probability of having more than t selected rows, which, in turn, as at least $\binom{n}{t+1}\pi^{t+1}(1-\pi)^{n-t-1} = 2^{-O(n)}$ (assuming $t < n$).

A numerical example for specific channel parameters is given in Appendix A.

3 Analysis of correction capability

Suppose that $\Gamma \in \mathsf{C}_q(n,t,\mathsf{p})$ is the transmitted array and that $Y = \Gamma + E$ is the received array where E is an error array which is generated by the channel according to conditions (P1)–(P3). Let $\hat{E}$ denote the $r \times r$ matrix $H_1 E H_2^T$, where H_1 and H_2 are the matrices as in Definition 1. Clearly, $\mathsf{rank}(\hat{E}) \leq \mathsf{rank}(E) \leq t$. Using the decoding algorithm for $\mathcal{C}_q(r,2t)$ [8],[19] we can recover the array $\hat{E}$. Our goal in this section is to show that, with probability of success greater than $1-\mathsf{p}$, we can recover E out of $\hat{E}$ and the syndrome values of E (which are computed for $\mathcal{C}_q(n,t)$), given our assumption (P3) on the distribution of the entries of E.

For a matrix B over F_q, we denote by $\mathsf{span}_{\mathrm{c}}(B)$ the linear space over F_q which is spanned by the columns of B. Similarly, we denote by $\mathsf{span}_{\mathrm{r}}(B)$ the linear space which is spanned by the rows of B. The rank of B will be denoted by $\mathsf{rank}(B)$. Clearly, $\mathsf{rank}(B) = \dim \mathsf{span}_{\mathrm{c}}(B) = \dim \mathsf{span}_{\mathrm{r}}(B)$.

Denote by $\mathcal{S}_q(n,s)$ the set of all vectors $\mathbf{u} \in \mathsf{F}_q^n$ with Hamming weight $\leq s$.

Definition 2 *Let t be a fixed nonnegative integer and H_1 and H_2 be fixed $r \times n$ matrices over F_q (such as those in Definition 1). For an $r \times r$ array $\hat{B}$ over F_q and a nonnegative integer w, denote by $\mathcal{M}(\hat{B},w)$ the set of all pairs of matrices (U_0,D_0) that satisfy the following conditions:*

(a) U_0 is an $n \times \sigma_0$ matrix over F_q whose columns are linearly-independent elements in $\mathcal{S}_q(n,w)$ and $\mathsf{span}_{\mathrm{c}}(H_1 U_0) \subseteq \mathsf{span}_{\mathrm{c}}(\hat{B})$.

(b) D_0 is a $\tau_0 \times n$ matrix over F_q whose rows are linearly-independent elements in $\mathcal{S}_q(n,w)$ and $\mathsf{span}_{\mathrm{r}}(D_0 H_2^T) \subseteq \mathsf{span}_{\mathrm{r}}(\hat{B})$.

(c) $\sigma_0 + \tau_0 + t \geq 2\,\mathsf{rank}(\hat{B})$.

As long as (c) holds, U_0 or D_0 can be taken also as 'empty' matrices, in which case σ_0 or

τ_0 is zero. The set $\mathcal{M}(\hat{E}, \lceil t/2 \rceil)$ will play a role in the analysis of the correction capability of $\mathsf{C}_q(n, t, \mathsf{p})$.

Sections 3.1 and 3.2 below are devoted to showing that $\mathsf{C}_q(n, t, \mathsf{p})$ can be decoded with decoding error probability less than p, given that the error arrays are generated according to conditions (P1)–(P3). We prove this in two steps:

1. Showing that with probability greater than $1-\mathsf{p}$ we have that $\mathsf{rank}(E) = \mathsf{rank}(\hat{E})$ and that the linear spans of the elements of $\mathcal{M}(\hat{E}, \lceil t/2 \rceil)$ satisfy certain containments. We do this in Proposition 3 in Section 3.1.

2. Showing that given that the conditions in 1 are satisfied, then the error array is completely specified. We do this in Theorem 10 in Section 3.2.

Throughout the analysis in the remaining parts of Section 3, we assume the following. Given n, t, and q, we fix sets $\mathcal{X}_{\mathrm{r}}$ and $\mathcal{X}_{\mathrm{c}}$ in (P1) and locations to corrupt as in (P2). (We fix those locations for the purpose of the analysis only; the decoder, of course, does not have a priori information about those locations other than that $|\mathcal{X}_{\mathrm{r}}| + |\mathcal{X}_{\mathrm{c}}| \leq t$.) We will denote $|\mathcal{X}_{\mathrm{r}}|$ and $|\mathcal{X}_{\mathrm{c}}|$ by x_{r} and x_{c}, respectively. We let E be an $n \times n$ random array over F_q with the probability measure defined in (P3), given the fixed selected locations of the corrupted entries; this will be the measure with respect to which we will compute all our probabilities. For each array E, we define $\hat{E} = H_1 E H_2^T$, where H_1 and H_2 are two fixed $r \times n$ matrices over F_q in which every $d-1$ columns are linearly independent (instead of requiring (4), we will regard d as one of the design parameters and compute the decoding error probability as a function of n, t, q, and d). The rank of E will be denoted by ρ.

For our analysis we will also make use of the following notations.

Denote by E_{c}^{+} the $n \times x_{\mathrm{c}}$ submatrix of E consisting of columns which are indexed by $\mathcal{X}_{\mathrm{c}}$, and by E_{c}^{-} the $n \times (n - x_{\mathrm{c}})$ submatrix whose columns are indexed by $[n] - \mathcal{X}_{\mathrm{c}}$, where hereafter $[n]$ stands for $\{1, 2, \ldots, n\}$. Similarly, the notations E_{r}^{+} and E_{r}^{-} will stand for submatrices of E consisting of rows which are indexed by $\mathcal{X}_{\mathrm{r}}$ and $[n] - \mathcal{X}_{\mathrm{r}}$, respectively.

Example 2 Consider the array in Figure 1 where $x_{\mathrm{c}} = 3$ and $x_{\mathrm{r}} = 2$. The matrix E_{c}^{+} is an $n \times 3$ submatrix which consists of the three columns marked by the double-arrows. The matrix E_{c}^{-} is an $n \times (n-3)$ submatrix which consists of the remaining columns of the array. Notice that the number of nonzero *rows* in E_{c}^{-} is bounded from above by $x_{\mathrm{r}} = 2$. Hence, $\mathsf{rank}(E_{\mathrm{c}}^{-}) \leq x_{\mathrm{r}} = 2$. Similarly, $\mathsf{rank}(E_{\mathrm{r}}^{-}) \leq x_{\mathrm{c}} = 3$. □

3.1 Linear span containments

We prove in this section the following result.

Proposition 3 *With probability greater than* $1 - \binom{n}{\lceil t/2 \rceil} \frac{2}{q-1} \cdot q^{\lceil \frac{3}{2} t \rceil - d + 1}$, *the following conditions hold:*

(C1) $\mathsf{rank}(\hat{E}) = \mathsf{rank}(E)$.
(C2) *For every* $(U_0, D_0) \in \mathcal{M}(\hat{E}, \lceil t/2 \rceil)$, $\mathsf{span}_{\mathrm{c}}(U_0) \subseteq \mathsf{span}_{\mathrm{c}}(E)$.
(C3) *For every* $(U_0, D_0) \in \mathcal{M}(\hat{E}, \lceil t/2 \rceil)$, $\mathsf{span}_{\mathrm{r}}(D_0) \subseteq \mathsf{span}_{\mathrm{r}}(E)$.

Note that (4) implies

$$\binom{n}{\lceil t/2 \rceil} \frac{2}{q-1} \cdot q^{\lceil \frac{3}{2} t \rceil - d + 1} \;\leq\; \mathsf{p}$$

and that (C2)–(C3) imply that σ_0 ($= \mathsf{rank}(U_0)$) and τ_0 ($= \mathsf{rank}(D_0)$) do not exceed t.

We prove Proposition 3 through a series of lemmas.

For a subset $Z \subseteq [n]$, denote by $\mathcal{S}_q(n, Z)$ the set of all vectors in F_q^n whose support is contained in Z.

Lemma 4 *Fix a column vector* $\mathbf{y} \in \mathsf{F}_q^{x_c}$ *and let* $\mathbf{e}_{\mathrm{c}}$ *denote the random vector* $E_{\mathrm{c}}^{+}\mathbf{y}$. *Then, for every subset* Z *of* $[n]$,

$$\mathsf{Prob}\left\{ \bigcup_{\mathbf{z} \in \mathcal{S}_q(n,Z)} \{\, \mathbf{e}_{\mathrm{c}} \neq \mathbf{z} \;\; \textit{and} \;\; H_1 \mathbf{e}_{\mathrm{c}} = H_1 \mathbf{z} \,\} \right\} \;<\; q^{|Z| - d + 1} \;. \tag{8}$$

Proof. Write the ith entry of $\mathbf{e}_{\mathrm{c}}$ explicitly as $e_i = \sum_{j=1}^{x_c} (E_{\mathrm{c}}^{+})_{i,j} y_j$, where y_j denotes the jth entry of $\mathbf{y}$. We say that e_i is *marked* if an entry $(E_{\mathrm{c}}^{+})_{i,j}$ was marked in (P2) for at least one index j for which $y_j \neq 0$. Obviously, any unmarked entry in $\mathbf{e}_{\mathrm{c}}$ is identically zero, and all the marked entries in $\mathbf{e}_{\mathrm{c}}$ are statistically independent random variables which are uniformly distributed over F_q.

Let X denote the set of indexes of the marked entries in $\mathbf{e}_{\mathrm{c}}$ and let $\mathcal{L}$ be the set of all pairs $(\mathbf{x}, \mathbf{z})$ such that $\mathbf{x} \in \mathcal{S}_q(n, X)$ and $\mathbf{z} \in \mathcal{S}_q(n, Z)$. Clearly, $\mathcal{L}$ is a vector space of dimension $|X| + |Z|$ over F_q. Next, let $\mathcal{K}$ be the linear subspace of $\mathcal{L}$ which is given by

$$\mathcal{K} \;=\; \left\{ (\mathbf{x}, \mathbf{z}) \in \mathcal{L} \mid H_1 \mathbf{x} = H_1 \mathbf{z} \right\} .$$

Now, as $(\mathbf{x}, \mathbf{z})$ ranges over $\mathcal{L}$, the difference $\mathbf{x} - \mathbf{z}$ ranges over all the elements of $\mathcal{S}_q(n, X \cup Z)$ (yet not necessarily in a one-to-one manner: if $X \cap Z \neq \emptyset$ then $|\mathcal{L}| > |\mathcal{S}_q(n, X \cup Z)|$). Recalling that every $d-1$ columns in H_1 are linearly independent, it follows that

$$H_1(\mathbf{x} - \mathbf{z}) \;=\; \mathbf{0}$$

defines at least $\min\{|X \cup Z|, d-1\}$ linearly independent homogeneous equations over $\mathcal{L}$ and, so,

$$\dim \mathcal{K} \;\leq\; |Z| + |X| - \min\{|X \cup Z|, d-1\} \;. \tag{9}$$

Denote by $\mathcal{K}_0$ the linear space $\{\,(\mathbf{x},\mathbf{z}) \in \mathcal{L} \mid \mathbf{x}=\mathbf{z}\,\}$. It is easy to see that $\dim \mathcal{K}_0 = |X \cap Z|$ and that $\mathcal{K}_0 \subseteq \mathcal{K}$ which, combined with (9), yields

$$|\mathcal{K}-\mathcal{K}_0| \;=\; \begin{cases} 0 & \text{if } |X\cup Z| < d \\ q^{|X|+|Z|-d+1} - q^{|X\cap Z|} & \text{otherwise} \end{cases} \quad . \tag{10}$$

Hence,

$$\begin{aligned} &\mathsf{Prob}\left\{ \bigcup_{\mathbf{z}\in\mathcal{S}_q(n,Z)} \{\, \mathbf{e}_{\rm c} \neq \mathbf{z} \;\text{ and }\; H_1\mathbf{e}_{\rm c} = H_1\mathbf{z} \,\} \right\} \\ &\quad = \;\mathsf{Prob}\left\{ \bigcup_{(\mathbf{x},\mathbf{z})\in\mathcal{L}} \{\, \mathbf{e}_{\rm c} = \mathbf{x} \;\text{ and }\; \mathbf{x}\neq\mathbf{z} \;\text{ and }\; H_1\mathbf{x} = H_1\mathbf{z} \,\} \right\} \\ &\quad \leq \;\sum_{(\mathbf{x},\mathbf{z})\in\mathcal{L}} \mathsf{Prob}\left\{ \mathbf{e}_{\rm c} = \mathbf{x} \;\text{ and }\; \mathbf{x}\neq\mathbf{z} \;\text{ and }\; H_1\mathbf{x} = H_1\mathbf{z} \right\} \\ &\quad = \;\sum_{(\mathbf{x},\mathbf{z})\in\mathcal{K}-\mathcal{K}_0} \mathsf{Prob}\left\{ \mathbf{e}_{\rm c} = \mathbf{x} \right\} \;=\; |\mathcal{K}-\mathcal{K}_0| \cdot q^{-|X|} \;<\; q^{|Z|-d+1} \,, \end{aligned}$$

where the last inequality follows from (10). □

Lemma 5 *For every subset $T \subseteq [n]$,*

$$\mathsf{Prob}\left\{ \bigcup_{\mathbf{u}\in\mathcal{S}_q(n,T)} \bigcup_{\mathbf{a}\in\mathsf{F}_q^n} \{\, E\mathbf{a}\neq\mathbf{u} \;\textit{ and }\; H_1E\mathbf{a} = H_1\mathbf{u} \,\} \right\} \;<\; \frac{1}{q-1}\cdot q^{t+|T|-d+1} \,. \tag{11}$$

Proof. For $\mathbf{a}\in\mathsf{F}_q^n$, we denote by $\mathbf{a}_{\rm c}$ the subvector of $\mathbf{a}$ which is indexed by $\mathcal{X}_{\rm c}$. Suppose that $\mathbf{a}$ is such that $\mathbf{a}_{\rm c} = \mathbf{0}$ (in particular, this includes the case $\mathcal{X}_{\rm c} = \emptyset$). In this case, the vector $E\mathbf{a}-\mathbf{u}$ has Hamming weight $\leq x_{\rm r}+|T| \leq t+|T|$. Assuming $t+|T| \leq d-1$ (or else the lemma trivially holds) and recalling that every $d-1$ columns in H_1 are linearly independent, we have that $H_1E\mathbf{a} = H_1\mathbf{u}$ implies $E\mathbf{a}=\mathbf{u}$ with probability 1. Hence, it suffices to consider in (11) only vectors $\mathbf{a}$ whose respective $\mathbf{a}_{\rm c}$ is nonzero. Furthermore, we can assume that $\mathbf{a}_{\rm c}$ is normalized, i.e., its first nonzero entry is 1. So, denoting by $(\mathsf{F}_q^m)^*$ the set of the nonzero normalized vectors in F_q^m, we have

$$\begin{aligned} &\mathsf{Prob}\left\{ \bigcup_{\mathbf{u}\in\mathcal{S}_q(n,T)} \bigcup_{\mathbf{a}\in\mathsf{F}_q^n} \{\, E\mathbf{a}\neq\mathbf{u} \;\text{ and }\; H_1E\mathbf{a} = H_1\mathbf{u} \,\} \right\} \\ &\quad \leq \;\sum_{\mathbf{y}\in(\mathsf{F}_q^{x_{\rm c}})^*} \mathsf{Prob}\left\{ \bigcup_{\mathbf{u}\in\mathcal{S}_q(n,T)} \bigcup_{\mathbf{a}\in\mathsf{F}_q^n\,:\,\mathbf{a}_{\rm c}=\mathbf{y}} \{\, E\mathbf{a}\neq\mathbf{u} \;\text{ and }\; H_1E\mathbf{a} = H_1\mathbf{u} \,\} \right\} . \end{aligned} \tag{12}$$

We now apply Lemma 4 for every $\mathbf{y}\in(\mathsf{F}_q^{x_{\rm c}})^*$ with $\mathbf{e}_{\rm c} = E_{\rm c}^+\mathbf{y}$ and $Z = \mathcal{X}_{\rm r}\cup T$ to obtain

$$\begin{aligned} &\mathsf{Prob}\left\{ \bigcup_{\mathbf{u}\in\mathcal{S}_q(n,T)} \bigcup_{\mathbf{a}\in\mathsf{F}_q^n\,:\,\mathbf{a}_{\rm c}=\mathbf{y}} \{\, E\mathbf{a}\neq\mathbf{u} \;\text{ and }\; H_1E\mathbf{a} = H_1\mathbf{u} \,\} \;\middle|\; E_{\rm c}^- \right\} \\ &\quad = \;\mathsf{Prob}\left\{ \bigcup_{\mathbf{u}\in\mathcal{S}_q(n,T)} \bigcup_{\mathbf{b}\in\mathsf{span}_{\rm c}(E_{\rm c}^-)} \{\, \mathbf{e}_{\rm c}+\mathbf{b}\neq\mathbf{u} \;\text{ and }\; H_1(\mathbf{e}_{\rm c}+\mathbf{b}) = H_1\mathbf{u} \,\} \;\middle|\; E_{\rm c}^- \right\} \\ &\quad \leq \;\mathsf{Prob}\left\{ \bigcup_{\mathbf{z}\in\mathcal{S}_q(n,\mathcal{X}_{\rm r}\cup T)} \{\, \mathbf{e}_{\rm c}\neq\mathbf{z} \;\text{ and }\; H_1\mathbf{e}_{\rm c} = H_1\mathbf{z} \,\} \;\middle|\; E_{\rm c}^- \right\} \;<\; q^{|T|+x_{\rm r}-d+1} \,, \end{aligned} \tag{13}$$

where $\mathsf{Prob}\{\cdot \mid E_{\rm c}^-\}$ stands for the probability measure conditioned on $E_{\rm c}^-$. Now, the last inequality in (13) yields a bound which does not depend on $E_{\rm c}^-$, so we also have

$$\mathsf{Prob}\left\{ \bigcup_{\mathbf{u}\in\mathcal{S}_q(n,T)} \bigcup_{\mathbf{a}\in\mathsf{F}_q^n\,:\,\mathbf{a}_{\rm c}=\mathbf{y}} \{\, E\mathbf{a}\neq\mathbf{u} \;\text{ and }\; H_1E\mathbf{a} = H_1\mathbf{u} \,\} \right\} \;<\; q^{|T|+x_{\rm r}-d+1} \,.$$

Combining this with (12) yields

$$\begin{aligned}&\mathsf{Prob}\Big\{\bigcup_{\mathbf{u}\in\mathcal{S}_q(n,T)}\bigcup_{\mathbf{a}\in\mathsf{F}_q^n}\{\,E\mathbf{a}\neq\mathbf{u}\ \text{ and }\ H_1E\mathbf{a}=H_1\mathbf{u}\,\}\Big\}\\ &\quad\leq\ |(\mathsf{F}_q^{x_{\rm c}})^*|\cdot q^{|T|+x_{\rm r}-d+1}\ =\ \frac{q^{x_{\rm c}}-1}{q-1}\cdot q^{|T|+x_{\rm r}-d+1}\ \leq\ \frac{q^t-1}{q-1}\cdot q^{|T|-d+1}\ ,\end{aligned}$$

thus implying (11). □

Recall that hereafter ρ stands for $\mathsf{rank}(E)$.

Lemma 6 *If* $\mathsf{rank}(H_1E)=\mathsf{rank}(EH_2^T)=\rho$, *then* $\mathsf{rank}(\hat{E})=\rho$.

Proof. Suppose that $\rho=\mathsf{rank}(H_1E)=\mathsf{rank}(EH_2^T)$ and let U be an $n\times\rho$ matrix whose columns form a basis of $\mathsf{span}_{\rm c}(E)$. Then there is a unique $\rho\times n$ matrix D of rank ρ such that $E=UD$. Now, $\mathsf{rank}(H_1U)=\mathsf{rank}(H_1E)=\rho$ and $\mathsf{rank}(DH_2^T)=\mathsf{rank}(EH_2^T)=\rho$, i.e., both H_1U and DH_2^T have full rank ρ. Hence, $\mathsf{rank}(H_1EH_2^T)=\mathsf{rank}((H_1U)(DH_2))=\rho$. □

Proof of Proposition 3. Define $\mathcal{B}_{\rm c}$ and $\mathcal{B}_{\rm r}$ as the following 'bad events':

$$\begin{aligned}\mathcal{B}_{\rm c}\ &=\ \bigcup_{T\subseteq[n]\,:\,|T|=\lceil t/2\rceil}\bigcup_{\mathbf{u}\in\mathcal{S}_q(n,T)}\bigcup_{\mathbf{a}\in\mathsf{F}_q^n}\{\,E\mathbf{a}\neq\mathbf{u}\ \text{ and }\ H_1E\mathbf{a}=H_1\mathbf{u}\,\}\\ \mathcal{B}_{\rm r}\ &=\ \bigcup_{T\subseteq[n]\,:\,|T|=\lceil t/2\rceil}\bigcup_{\mathbf{u}\in\mathcal{S}_q(n,T)}\bigcup_{\mathbf{a}\in\mathsf{F}_q^n}\{\,\mathbf{a}E\neq\mathbf{u}\ \text{ and }\ \mathbf{a}EH_2^T=\mathbf{u}H_2^T\,\}\ .\end{aligned}$$

By Lemma 5 we have

$$\mathsf{Prob}\Big\{\,\mathcal{B}_{\rm c}\cup\mathcal{B}_{\rm r}\,\Big\}\ <\ \binom{n}{\lceil t/2\rceil}\frac{2}{q-1}\cdot q^{\lceil\frac{3}{2}t\rceil-d+1}\ .$$

Hence, it suffices to show that the complement of each of the events (C1), (C2), and (C3) is contained in $\mathcal{B}_{\rm c}\cup\mathcal{B}_{\rm r}$. We do this next, starting with (C1). First,

$$\begin{aligned}\{\,\mathsf{rank}(E)\neq\mathsf{rank}(H_1E)\,\}\ &=\ \{\,\dim\mathsf{span}_{\rm c}(E)\ >\ \dim\mathsf{span}_{\rm c}(H_1E)\,\}\\ &\subseteq\ \bigcup_{\mathbf{a}\in\mathsf{F}_q^n}\{\,E\mathbf{a}\neq\mathbf{0}\ \text{ and }\ H_1E\mathbf{a}=\mathbf{0}\,\}\ \subseteq\ \mathcal{B}_{\rm c}\end{aligned}$$

and, similarly, $\{\,\mathsf{rank}(E)\neq\mathsf{rank}(EH_2^T)\,\}\subseteq\mathcal{B}_{\rm r}$. Hence, by Lemma 6, the event $\{\,\mathsf{rank}(\hat{E})\neq\mathsf{rank}(E)\,\}$ is contained in $\mathcal{B}_{\rm c}\cup\mathcal{B}_{\rm r}$, thus establishing (C1).

Let (U_0,D_0) be a pair in $\mathcal{M}(\hat{E},\lceil t/2\rceil)$. We next show that the event $\{\,\mathsf{span}_{\rm c}(U_0)\not\subseteq\mathsf{span}_{\rm c}(E)\,\}$ is contained in $\mathcal{B}_{\rm c}$, thus proving (C2). Note that if $\mathsf{span}_{\rm c}(U_0)\not\subseteq\mathsf{span}_{\rm c}(E)$, then there is in particular a column $\mathbf{u}$ in U_0 which is not in $\mathsf{span}_{\rm c}(E)$. On the other hand, by Definition 2, that column is in $\mathcal{S}_q(n,\lceil t/2\rceil)$ and $H_1\mathbf{u}\in\mathsf{span}_{\rm c}(\hat{B})$. Therefore,

$$\begin{aligned}&\{\,\mathsf{span}_{\rm c}(U_0)\not\subseteq\mathsf{span}_{\rm c}(E)\,\}\\ &\quad\subseteq\ \bigcup_{\mathbf{u}\in\mathcal{S}_q(n,\lceil t/2\rceil)}\{\,\mathbf{u}\notin\mathsf{span}_{\rm c}(E)\ \text{ and }\ H_1\mathbf{u}\in\mathsf{span}_{\rm c}(\hat{E})\,\}\\ &\quad\subseteq\ \bigcup_{\mathbf{u}\in\mathcal{S}_q(n,\lceil t/2\rceil)}\{\,\mathbf{u}\notin\mathsf{span}_{\rm c}(E)\ \text{ and }\ H_1\mathbf{u}\in\mathsf{span}_{\rm c}(H_1E)\,\}\\ &\quad\subseteq\ \bigcup_{T\subseteq[n]\,:\,|T|=\lceil t/2\rceil}\bigcup_{\mathbf{u}\in\mathcal{S}_q(n,T)}\{\,\mathbf{u}\notin\mathsf{span}_{\rm c}(E)\ \text{ and }\ H_1\mathbf{u}\in\mathsf{span}_{\rm c}(H_1E)\,\}\ \subseteq\ \mathcal{B}_{\rm c}\ .\end{aligned}$$

The containment of the event $\{\, \mathsf{span}_{\mathrm{r}}(D_0) \not\subseteq \mathsf{span}_{\mathrm{r}}(E) \,\}$ in $\mathcal{B}_{\mathrm{r}}$ (which yields (C3)) is obtained in a similar manner. $\square$

The following lemma implies that the set $\mathcal{M}(\hat{E}, \lceil t/2 \rceil)$ referred to in Proposition 3 is nonempty.

Lemma 7 *Let B be an $n \times n$ array over F_q with $\mathsf{w}_{\mathrm{cov}}(B) = t^* \leq t$ and let $\hat{B} = H_1 B H_2^T$ be such that $\mathsf{rank}(\hat{B}) = \mathsf{rank}(B) = \rho^*$. Then, there exists a pair $(U_0^*, D_0^*) \in \mathcal{M}(\hat{B}, t^* - \rho^* + 1)$ such that $\mathsf{span}_{\mathrm{c}}(U_0^*) \subseteq \mathsf{span}_{\mathrm{c}}(B)$ and $\mathsf{span}_{\mathrm{r}}(D_0^*) \subseteq \mathsf{span}_{\mathrm{r}}(B)$.*

In particular, $\mathcal{M}(\hat{B}, \lceil t/2 \rceil) \neq \emptyset$.

Proof. When $2\rho^* \leq t$ we can take $\sigma_0 = \tau_0 = 0$ in Definition 2 and we are done. So we assume from now on in the proof that $2\rho^* > t$. Next we effectively construct from B a pair $(U_0^*, D_0^*) \in \mathcal{M}(\hat{B}, t^* - \rho^* + 1)$ with the claimed set containments.

Let a minimum cover of B be given by a set $\mathcal{X}_{\mathrm{r}}^*$ of size x_{r}^* of row indexes and a set $\mathcal{X}_{\mathrm{c}}^*$ of size x_{c}^* of column indexes where $x_{\mathrm{r}}^* + x_{\mathrm{c}}^* = t^*$. The submatrices B_{c}^- and B_{r}^- will be defined here with respect to the sets $\mathcal{X}_{\mathrm{c}}^*$ and $\mathcal{X}_{\mathrm{r}}^*$. We will also introduce the notations $\mathcal{L}_{\mathrm{c}}$ and $\mathcal{L}_{\mathrm{r}}$ for $\mathcal{S}_q(n, \mathcal{X}_{\mathrm{r}}{}^*) \cap \mathsf{span}_{\mathrm{c}}(B)$ and $\mathcal{S}_q(n, \mathcal{X}_{\mathrm{c}}{}^*) \cap \mathsf{span}_{\mathrm{r}}(B)$, respectively, and define $\sigma_0^* = \dim \mathcal{L}_{\mathrm{c}}$ and $\tau_0^* = \dim \mathcal{L}_{\mathrm{r}}$.

We first show that

$$\mathsf{rank}(B_{\mathrm{c}}^-) \;\leq\; \sigma_0^* \;=\; \rho^* - \mathsf{rank}(B_{\mathrm{r}}^-) \;\leq\; x_{\mathrm{r}}^* \,. \tag{14}$$

The inequality $\mathsf{rank}(B_{\mathrm{c}}^-) \leq \sigma_0^*$ follows from the containment $\mathsf{span}_{\mathrm{c}}(B_{\mathrm{c}}^-) \subseteq \mathcal{L}_{\mathrm{c}}$ and the inequality $\sigma_0^* \leq x_{\mathrm{r}}^*$ follows from the containment $\mathcal{L}_{\mathrm{c}} \subseteq \mathcal{S}_q(n, \mathcal{X}_{\mathrm{r}}{}^*)$. As for the equality $\sigma_0^* = \rho^* - \mathsf{rank}(B_{\mathrm{r}}^-)$, write $\mathsf{span}_{\mathrm{c}}(B)$ as a direct sum $\mathcal{L}_{\mathrm{c}} \oplus \mathcal{P}$, where $\mathcal{L}_{\mathrm{c}} \cap \mathcal{P} = \{\mathbf{0}\}$. For a linear space $M \subseteq \mathsf{F}_q^n$, denote by $\overline{M}$ the linear space obtained by shortening the elements of M through the deletion of the coordinates which are indexed by $\mathcal{X}_{\mathrm{r}}{}^*$. Then,

$$\mathsf{span}_{\mathrm{c}}(B_{\mathrm{r}}^-) \;=\; \overline{\mathsf{span}_{\mathrm{c}}(B)} \;=\; \overline{\mathcal{L}_{\mathrm{c}} \oplus \mathcal{P}} \;=\; \overline{\mathcal{L}_{\mathrm{c}}} \oplus \overline{\mathcal{P}} \;=\; \overline{\mathcal{P}} \,.$$

Therefore, $\dim \overline{\mathcal{P}} = \mathsf{rank}(B_{\mathrm{r}}^-)$. On the other hand, since $\mathcal{L}_{\mathrm{c}} \cap \mathcal{P} = \{\mathbf{0}\}$, it follows that every nonzero element in $\mathcal{P}$ corresponds (through the shortening operation) to a nonzero element in $\overline{\mathcal{P}}$. Hence, $\dim \mathcal{P} = \dim \overline{\mathcal{P}}$ and, so,

$$\sigma_0^* \;=\; \dim \mathsf{span}_{\mathrm{c}}(B) - \dim \mathcal{P} \;=\; \dim \mathsf{span}_{\mathrm{c}}(B) - \dim \overline{\mathcal{P}} \;=\; \rho^* - \mathsf{rank}(B_{\mathrm{r}}^-) \,,$$

as claimed in (14). By similar arguments we also have

$$\mathsf{rank}(B_{\mathrm{r}}^-) \;\leq\; \tau_0^* \;=\; \rho^* - \mathsf{rank}(B_{\mathrm{c}}^-) \;\leq\; x_{\mathrm{c}}^* \,. \tag{15}$$

Next we show that $\mathcal{L}_{\mathrm{c}}$ has a basis in which each element has Hamming weight $\leq x_{\mathrm{r}}^* - \sigma_0^* + 1$. Indeed, $\mathcal{L}_{\mathrm{c}}$ can be regarded as a conventional linear code over F_q with support x_{r}^* and

dimension σ_0^*, and such a code has an $n \times \sigma_0^*$ (transposed) systematic generator matrix U_0^* in which each column has Hamming weight $\leq x_{\rm r}^* - \sigma_0^* + 1$. Similarly, $\mathcal{L}_{\rm r}$ is spanned by the rows of a $\tau_0^* \times n$ matrix D_0^* in which each row has Hamming weight $\leq x_{\rm c}^* - \tau_0^* + 1$. Now, by (14) and (15) we have

$$\sigma_0^* + \tau_0^* \;\geq\; \mathsf{rank}(B_{\rm c}^-) + (\rho^* - \mathsf{rank}(B_{\rm c}^-)) \;=\; \rho^*$$

and so,

$$(x_{\rm r}^* - \sigma_0^* + 1) \;+\; (x_{\rm c}^* - \tau_0^* + 1) \;\leq\; t^* - \rho^* + 2 \; . \tag{16}$$

Hence, each column in U_0^* and each row in D_0^* has Hamming weight $\leq t^* - \rho^* + 1$. Also,

$$\sigma_0^* + \tau_0^* + t \;\geq\; \rho^* + t \;\geq\; 2\rho^* \; ,$$

which is condition (c) in Definition 2. So, in order to show that (U_0^*, D_0^*) is in $\mathcal{M}(\hat{B}, t^* - \rho^* + 1)$, it remains to prove that $\mathsf{span}_{\rm c}(H_1 U_0^*) \subseteq \mathsf{span}_{\rm c}(\hat{B})$ (and that $\mathsf{span}_{\rm r}(D_0^* H_2^T) \subseteq \mathsf{span}_{\rm r}(\hat{B})$). Now, by construction, $\mathsf{span}_{\rm c}(U_0^*) = \mathcal{L}_{\rm c} \subseteq \mathsf{span}_{\rm c}(B)$, so it suffices to show that $\mathsf{span}_{\rm c}(H_1 B) \subseteq \mathsf{span}_{\rm c}(\hat{B})$. Indeed, recall that $\mathsf{rank}(B) \geq \mathsf{rank}(H_1 B) \geq \mathsf{rank}(H_1 B H_2^T)$ and that the inequalities in this chain become equalities when $\mathsf{rank}(\hat{B}) = \mathsf{rank}(B)$; this, in turn, implies $\mathsf{span}_{\rm c}(H_1 B) = \mathsf{span}_{\rm c}(H_1 B H_2^T)$.

Finally, for $\rho^* > t/2$ we have $t^* - \rho^* + 1 \leq \lceil t/2 \rceil$ and so $(U_0^*, D_0^*) \in \mathcal{M}(\hat{B}, \lceil t/2 \rceil)$. □

3.2 Uniqueness of the error array

Our goal in this section is to show that, given that (C1)–(C3) hold, the error array E can be uniquely determined. Hereafter, by a full-rank matrix we mean an $\ell \times m$ matrix whose rank equals $\min\{\ell, m\}$.

Definition 3 *Let B be an $n \times n$ array over F_q. A decomposition of B is a triple $\langle U, A, D \rangle$, where U is an $n \times \mathsf{rank}(B)$ full-rank matrix whose columns span $\mathsf{span}_{\rm c}(B)$, D is a $\mathsf{rank}(B) \times n$ full-rank matrix whose rows span $\mathsf{span}_{\rm r}(B)$, and A is a $\mathsf{rank}(B) \times \mathsf{rank}(B)$ nonsingular matrix such that*

$$B \;=\; UAD \; .$$

We call A the intermediate matrix of the decomposition.

The decomposition $\langle U, A, D \rangle$ of B is not unique since U and D can be any bases of $\mathsf{span}_{\rm c}(B)$ and $\mathsf{span}_{\rm r}(B)$, respectively, and for every choice of bases we have a unique intermediate matrix A such that $B = UAD$.

Definition 4 *Given an $n \times n$ array B over F_q, let U_1 and D_1 be full-rank matrices over F_q such that $\mathsf{span}_{\rm c}(U_1) \subseteq \mathsf{span}_{\rm c}(B)$ and $\mathsf{span}_{\rm r}(D_1) \subseteq \mathsf{span}_{\rm r}(B)$. A decomposition $\langle U, A, D \rangle$*

of B is called systematic with respect to (U_1, D_1) if U_1 occupies the left-most columns of U and D_1 occupies the upper-most rows of D; namely, there exist matrices U_2 and D_2 such that

$$U = \begin{bmatrix} U_1 \; U_2 \end{bmatrix} \quad \text{and} \quad D = \begin{bmatrix} D_1 \\ D_2 \end{bmatrix} . \tag{17}$$

Lemma 8 *Let B be an $n \times n$ array over F_q and let $\hat{B} = H_1 B H_2^T$. Further, suppose that $\mathsf{rank}(B) = \mathsf{rank}(\hat{B})$ and let U_1 and D_1 be full-rank matrices over F_q such that $\mathsf{span}_{\mathrm{c}}(U_1) \subseteq \mathsf{span}_{\mathrm{c}}(B)$ and $\mathsf{span}_{\mathrm{r}}(D_1) \subseteq \mathsf{span}_{\mathrm{r}}(B)$.*

(a) Let $\langle U, A, D \rangle$ be a systematic decomposition of B w.r.t. (U_1, D_1) and define $\hat{U} = H_1 U$ and $\hat{D} = D H_2^T$. Then, $\langle \hat{U}, A, \hat{D} \rangle$ is a decomposition of $\hat{B}$ where, for some matrices $\hat{U}_2$ and $\hat{D}_2$,

$$\hat{U} = \begin{bmatrix} H_1 U_1 \; \hat{U}_2 \end{bmatrix} \quad \text{and} \quad \hat{D} = \begin{bmatrix} D_1 H_2^T \\ \hat{D}_2 \end{bmatrix} . \tag{18}$$

(b) The mapping $\langle U, A, D \rangle \mapsto \langle H_1 U, A, D H_2^T \rangle$ from all systematic decompositions of B w.r.t. (U_1, D_1) is onto all possible decompositions $\langle \hat{U}, A, \hat{D} \rangle$ of $\hat{B}$ of the form (18).

Proof. (a) Clearly, $B = UAD$ implies $\hat{B} = (H_1 U) A (D H_2^T)$. Furthermore, since we assume that $\mathsf{rank}(B) = \mathsf{rank}(\hat{B})$, then $\mathsf{rank}(H_1 U) = \mathsf{rank}(D H_2^T) = \mathsf{rank}(\hat{B})$. Hence, $\langle H_1 U, A, D H_2^T \rangle$ is a decomposition of $\hat{B}$.

(b) Suppose that $\langle \hat{U}, A, \hat{D} \rangle$ is a decomposition of $\hat{B}$ where $\hat{U}$ and $\hat{D}$ have the form (18), and let $\langle \tilde{U}, \tilde{A}, \tilde{D} \rangle$ be *some* systematic decomposition of B w.r.t. (U_1, D_1). Since $\mathsf{span}_{\mathrm{c}}(H_1 \tilde{U}) = \mathsf{span}_{\mathrm{c}}(\hat{U})$ and $\mathsf{span}_{\mathrm{r}}(\tilde{D} H_2^T) = \mathsf{span}_{\mathrm{r}}(\hat{D})$, we can apply elementary operations to the columns of $\tilde{U}$ and to the rows of $\tilde{D}$ to obtain a systematic decomposition $\langle U, \bar{A}, D \rangle$ of B such that $\hat{U} = H_1 U$ and $\hat{D} = D H_2^T$. Furthermore, since $\langle \hat{U}, \bar{A}, \hat{D} \rangle$ yields a decomposition of $\hat{B}$, then we must also have $\bar{A} = A$. □

We will refer to a decomposition $\langle \hat{U}, A, \hat{D} \rangle$ that satisfies (18) as a systematic decomposition of $\hat{B}$ w.r.t. (U_1, D_1). Clearly, once we have $\hat{B}$, U_1, and D_1, it is easy to compute a systematic decomposition $\langle \hat{U}, A, \hat{D} \rangle$ of $\hat{B}$ w.r.t. (U_1, D_1).

Proposition 9 *Let E be an instance of an error array for which $\mathsf{rank}(\hat{E}) = \mathsf{rank}(E) = \rho$ and let (U_1, D_1) be a pair of matrices over F_q that satisfy the following requirements:*

- *(a) U_1 is a full-rank $n \times \sigma$ matrix over F_q such that $\mathsf{span}_{\mathrm{c}}(U_1) \subseteq \mathsf{span}_{\mathrm{c}}(E)$.*
- *(b) D_1 is a full-rank $\tau \times n$ matrix over F_q such that $\mathsf{span}_{\mathrm{r}}(D_1) \subseteq \mathsf{span}_{\mathrm{r}}(E)$.*
- *(c) $\sigma + \tau + t \geq 2\rho$.*

Let $\tilde{E}$ be an $n \times n$ array over F_q that satisfies the following conditions:

(i)	$\hat{E} = H_1 \tilde{E} H_2^T$.	*(iv)*	$\mathsf{span}_{\mathrm{c}}(U_1) \subseteq \mathsf{span}_{\mathrm{c}}(\tilde{E})$.
(ii)	$E - \tilde{E} \in \mathcal{C}_q(n,t)$.	*(v)*	$\mathsf{span}_{\mathrm{r}}(D_1) \subseteq \mathsf{span}_{\mathrm{r}}(\tilde{E})$.
(iii)	$\mathsf{rank}(\tilde{E}) = \rho$.		

Under those conditions, $E = \tilde{E}$.

Proof. We first show that E and $\tilde{E}$ have systematic decompositions w.r.t. (U_1, D_1) with the same intermediate matrix. Let $\langle U, A, D \rangle$ be a systematic decomposition of E w.r.t. (U_1, D_1). Applying Lemma 8(a) with $B = E$ yields that $\langle H_1 U, A, D H_2^T \rangle$ is a systematic decomposition of $\hat{E}$ w.r.t. (U_1, D_1). On the other hand, we also have $\hat{E} = H_1 \tilde{E} H_2^T$, so we can apply Lemma 8(b) with $B = \tilde{E}$ to obtain that $\tilde{E}$ has a systematic decomposition $\langle \tilde{U}, A, \tilde{D} \rangle$ w.r.t. (U_1, D_1) with the same intermediate matrix A, where

$$\tilde{E} \;=\; \left[U_1 \; \tilde{U}_2 \right] A \left[\begin{array}{c} D_1 \\ \tilde{D}_2 \end{array} \right] . \tag{19}$$

Write

$$A \;=\; \left[\begin{array}{cc} A_{1,1} & A_{1,2} \\ A_{2,1} & A_{2,2} \end{array} \right] , \tag{20}$$

where $A_{1,1}$ occupies the upper-left $\sigma \times \tau$ block of A. Using the notation (17), we have

$$E \;=\; U_1 A_{1,1} D_1 \;+\; U_1 A_{1,2} D_2 \;+\; U_2 A_{2,1} D_1 \;+\; U_2 A_{2,2} D_2 \, .$$

On the other hand, by (19) we have

$$\tilde{E} \;=\; U_1 A_{1,1} D_1 \;+\; U_1 A_{1,2} \tilde{D}_2 \;+\; \tilde{U}_2 A_{2,1} D_1 \;+\; \tilde{U}_2 A_{2,2} \tilde{D}_2 \, .$$

Subtracting the last two equations, we obtain

$$E \;-\; \tilde{E} \;=\; \underbrace{(U_1 A_{1,2} + \tilde{U}_2 A_{2,2})(D_2 - \tilde{D}_2)}_{B_1} \;+\; \underbrace{(U_2 - \tilde{U}_2)(A_{2,1} D_1 + A_{2,2} D_2)}_{B_2} \, .$$

Now, $\mathsf{rank}(B_1)$ is bounded from above by the number of rows in $D_2 - \tilde{D}_2$; this number equals $\rho - \tau$. Similarly, $\mathsf{rank}(B_2) \leq \rho - \sigma$. Hence,

$$\mathsf{rank}(E - \tilde{E}) \;\leq\; \mathsf{rank}(B_1) + \mathsf{rank}(B_2) \;\leq\; 2\rho - \sigma - \tau \;\leq\; t \, , \tag{21}$$

where the latter inequality follows from requirement (c). Combining condition (ii) with (21) yields $E = \tilde{E}$. □

The following theorem, when combined with Proposition 3, establishes the unique decoding of E.

Theorem 10 *Let $Y = \Gamma + E$ be the received array where E is an instance of an error array for which conditions (C1)–(C3) hold, and let $\tilde{E}$ be an $n \times n$ array over F_q that satisfies the following conditions:*

1. *$H_1 Y H_2^T$ and $H_1 \tilde{E} H_2^T$ have the same syndrome values with respect to $\mathcal{C}_q(r, 2t)$, i.e., $H_1(Y - \tilde{E})H_2^T \in \mathcal{C}_q(r, 2t)$.*
2. *Y and $\tilde{E}$ have the same syndrome values with respect to $\mathcal{C}_q(n, t)$, i.e., $Y - \tilde{E} \in \mathcal{C}_q(n, t)$.*
3. *$\mathsf{rank}(\tilde{E}) = \mathsf{rank}(H_1 \tilde{E} H_2^T)$.*
4. *$\mathsf{w}_{\mathrm{cov}}(\tilde{E}) \leq t$.*

Under those conditions, $E = \tilde{E}$.

Proof. First note that conditions 1 and 2 are equivalent to $H_1(E - \tilde{E})H_2^T \in \mathcal{C}_q(r, 2t)$ and $E - \tilde{E} \in \mathcal{C}_q(n, t)$, respectively. Furthermore, since we assume that $\mathsf{w}_{\mathrm{cov}}(E), \mathsf{w}_{\mathrm{cov}}(\tilde{E}) \leq t$, it follows that $\mathsf{rank}(H_1(E - \tilde{E})H_2^T) \leq 2t$ and so condition 1 implies $\hat{E} = H_1 \tilde{E} H_2^T$. Hence, conditions 1–4 imply conditions (i)–(iii) in Proposition 9. Conditions (iv)–(v) therein are satisfied by the pair $(U_1, D_1) = (U_0^*, D_0^*)$ which is obtained by applying Lemma 7 to $B = \tilde{E}$ and $\hat{B} = \hat{E}$. Moreover, since (U_0^*, D_0^*) is in $\mathcal{M}(\hat{E}, \lceil t/2 \rceil)$ then, by (C2)–(C3) we also have requirements (a)–(c) in Proposition 9. Finally, (C1) provides the remaining assumption in that proposition — namely, $\mathsf{rank}(\hat{E}) = \mathsf{rank}(E)$ — and so we can apply Proposition 9 to conclude that $E = \tilde{E}$. □

3.3 Simplified decomposition

Proposition 9 will be instrumental in designing our decoding algorithm in Section 4. The decoding process will involve computing matrices (U_1, D_1) from $\hat{E}$ that satisfy requirements (a)–(c) in the proposition (e.g., $(U_1, D_1) \in \mathcal{M}(\hat{E}, \lceil t/2 \rceil)$), and then reconstructing a systematic decomposition of E w.r.t. (U_1, D_1). To simplify the decoding of E, it will be convenient to consider decompositions in which the intermediate matrix is a permutation matrix (in particular, the identity matrix). We show next how any systematic decomposition $\langle U, A, D \rangle$ of E w.r.t. (U_1, D_1) as in (17) can be transformed into such a simplified decomposition in which the information about U_1 and D_1 is preserved, even when U_2 and D_2 are unknown.

Let U_1 and D_1 satisfy requirements (a)–(c) in Proposition 9 and let $\langle U, A, D \rangle$ be a systematic decomposition of E w.r.t. (U_1, D_1), with $\sigma = \mathsf{rank}(U_1)$ and $\tau = \mathsf{rank}(D_1)$. Denote by γ the rank of the $(\rho - \sigma) \times (\rho - \tau)$ lower-right block of A (i.e., the block $A_{2,2}$ in (20)). We

now perform elementary operations on the rows and columns of A which transform A into the $\rho \times \rho$ permutation matrix

$$A^* \;=\; \left[\begin{array}{c|c} A^*_{1,1} & A^*_{1,2} \\ \hline A^*_{2,1} & A^*_{2,2} \end{array}\right] \;=\; \left[\begin{array}{cc|cc} I_{\sigma+\tau-\rho+\gamma} & 0 & 0 & 0 \\ 0 & 0 & I_{\rho-\tau-\gamma} & 0 \\ \hline 0 & I_{\rho-\sigma-\gamma} & 0 & 0 \\ 0 & 0 & 0 & I_\gamma \end{array}\right] ,$$

where I_b denotes the $b \times b$ identity matrix. More specifically, A is transformed into A^* as follows:

(i) Applying elementary operations on the last $\rho-\sigma$ rows and the last $\rho-\tau$ columns of A to obtain the lower-right $(\rho-\sigma) \times (\rho-\tau)$ block $A^*_{2,2}$ in A^*.

(ii) Applying row operations that change only the first σ rows and column operations that change only the first τ columns of A, to obtain the upper-right $\sigma \times (\rho-\tau)$ block $A^*_{1,2}$ and the lower-left $(\rho-\sigma) \times \tau$ block $A^*_{2,1}$.

(iii) Applying row and column operations that affect only the upper-left $\sigma \times \tau$ block of A, to obtain the upper-left $\sigma \times \tau$ block $A^*_{1,1}$.

Write $A^* = LAP$, where L and P are nonsingular matrices that represent the mentioned elementary row and column operations. Now, in all those operations, we never added any of the first σ rows of A to any of its last $\rho-\sigma$ rows. Therefore, L has the block-upper-triangular form

$$L \;=\; \left[\begin{array}{cc} L_{1,1} & L_{1,2} \\ 0 & L_{2,2} \end{array}\right] ,$$

where $L_{1,1}$ is the upper-left $\sigma \times \sigma$ block of L. Hence, the inverse of L^{-1} is also block-upper-triangular with $L^{-1}_{1,1}$ being its upper-left diagonal block. It can be easily verified in a similar mannner that P^{-1} is block-lower-triangular, with a $\tau \times \tau$ matrix, $P^{-1}_{1,1}$, as its upper-left diagonal block.

Clearly, $\langle UL^{-1}, A^*, P^{-1}D \rangle$ is a decomposition of E in which the intermediate matrix, A^*, is a permutation matrix. Furthermore, the first σ columns of UL^{-1} are given by $U_1 L^{-1}_{1,1}$ and so they can be computed from U_1. Similarly, the first τ rows of $P^{-1}D$ are given by $P^{-1}_{1,1} D_1$.

Partition $[\rho]$ into $\cup_{a,b \in \{1,2\}} \mathcal{Y}_{a,b}$ where

$$\begin{array}{rclcrcl} \mathcal{Y}_{1,1} &=& \{\, j \mid 0 < j \leq \sigma+\tau-\rho+\gamma \,\} & \qquad & \mathcal{Y}_{2,1} &=& \{\, j \mid \sigma < j \leq \rho-\gamma \,\} \\ \mathcal{Y}_{1,2} &=& \{\, j \mid \sigma+\tau-\rho+\gamma < j \leq \sigma \,\} & & \mathcal{Y}_{2,2} &=& \{\, j \mid \rho-\gamma < j \leq \rho \,\} \end{array} . \qquad (22)$$

The size of each $\mathcal{Y}_{a,b}$, denoted $\rho_{a,b}$, is given by

$$\rho_{1,1} = \sigma+\tau-\rho+\gamma \;, \quad \rho_{1,2} = \rho-\tau-\gamma \;, \quad \rho_{2,1} = \rho-\sigma-\gamma \;, \quad \text{and} \quad \rho_{2,2} = \gamma \;.$$

Write $U^* = UL^{-1}$ and let $U_{a,b}$ be the $n \times \rho_{a,b}$ submatrix of U^* whose columns are indexed by $\mathcal{Y}_{a,b}$. Also, write $D^* = A^* P^{-1} D$ and let $D_{a,b}$ be the $\rho_{a,b} \times n$ submatrix of D^* whose rows

are indexed by $\mathcal{Y}_{a,b}$. Then $\langle U^*, I_\rho, D^* \rangle$ is a decomposition of E and we have

$$E \;=\; U^* D^* \;=\; \sum_{a,b \in \{1,2\}} U_{a,b} D_{a,b} \;.$$

Furthermore, the four matrices $U_{1,1}$, $U_{1,2}$, $D_{1,1}$, and $D_{2,1}$ can be computed from U_1, D_1, and A by

$$[\, U_{1,1} \; U_{1,2} \,] \;=\; U_1 L_{1,1}^{-1} \quad \text{and} \quad \begin{bmatrix} D_{1,1} \\ D_{2,1} \end{bmatrix} \;=\; P_{1,1}^{-1} D_1 \;. \tag{23}$$

Let $Y = [\, y_{i,j} \,]_{i,j=1}^{n} = \Gamma + E$ be the received array and let $e_{i,j}$ denote the (i,j)th entry of E. The syndrome vector $\mathbf{s} \in \mathsf{F}_{q^n}^t$ of Y (or E), when computed for $\mathcal{C}_q(n,t)$ with respect to the equations (3), is given by

$$s_\ell \;=\; \sum_{i,j=1}^{n} y_{i,j}\, \alpha_i^{q^\ell} \omega_j \;=\; \sum_{i,j=1}^{n} e_{i,j}\, \alpha_i^{q^\ell} \omega_j \;, \qquad 0 \le \ell < t \;. \tag{24}$$

Define the vectors $\boldsymbol{\beta} = [\, \beta_k \,]_{k \in [\rho]} = \boldsymbol{\alpha} U^*$ and $\boldsymbol{\delta} = [\, \delta_k \,]_{k \in [\rho]} = D^* \boldsymbol{\omega}$. By (24) and the equality $E = U^* D^*$ we have

$$s_\ell \;=\; \sum_{k \in [\rho]} \beta_k^{q^\ell} \delta_k \;, \qquad 0 \le \ell < t \;. \tag{25}$$

Knowing U_1, D_1, and A, we can compute the values $\{\beta_k\}_{k \in \mathcal{Y}_{1,1} \cup \mathcal{Y}_{1,2}}$ and $\{\delta_k\}_{k \in \mathcal{Y}_{1,1} \cup \mathcal{Y}_{2,1}}$. So the recovery of E (which is guaranteed by Proposition 9) will be complete once we find the remaining entries of $\boldsymbol{\beta}$ and $\boldsymbol{\delta}$ so that (25) holds. We show how this can be done in polynomial time in Section 4.

We end this section by observing that when we consider the set of pairs $\{(\beta_k, \delta_k)\}_{k \in [\rho]}$, then $\rho_{1,1}$ of them — namely, $\{(\beta_k, \delta_k)\}_{k \in \mathcal{Y}_{1,1}}$ — are fully known, $\rho_{2,2}$ of them are fully unknown, and the remaining $\rho_{1,2} + \rho_{2,1}$ are 'half-known' (namely, one element of the pair is known). In analogy with conventional error correction, the pairs of the last type can be considered as 'erasures', whereas those of the second type are 'full errors'. We also have the inequality

$$(\rho_{1,2} + \rho_{2,1}) + 2\rho_{2,2} \;=\; 2\rho - \sigma - \tau \;\le\; t \;.$$

4 Decoding

The decoding algorithm for $\mathsf{C}_q(n,t,\mathsf{p})$ consists of the following steps, applied to the received array $Y = \Gamma + E$:

Step 1 Compute $\hat{Y} = H_1 Y H_2^T$.

Step 2 Decode the matrix $\hat{E} = H_1 E H_2^T$ from the syndrome values of $\hat{Y}$ which are computed for the code $\mathcal{C}_q(r, 2t)$.

Step 3 Compute matrices (U_1, D_1) that satisfy requirements (a)–(c) in Proposition 9, e.g., find a pair in $\mathcal{M}(\hat{E}, \lceil t/2 \rceil)$.

Step 4 Compute the matrix A for a systematic decomposition $\langle \hat{U}, A, \hat{D} \rangle$ of $\hat{E}$ w.r.t. (U_1, D_1) (as in (18)).

Step 5 Compute the matrices $U_{1,1}$, $U_{1,2}$, $D_{1,1}$, and $D_{2,1}$ from (23) and obtain the entries of $\boldsymbol{\beta} = \boldsymbol{\alpha} U^*$ and $\boldsymbol{\delta} = D^* \boldsymbol{\omega}$ which are indexed by $\mathcal{Y}_{1,1} \cup \mathcal{Y}_{1,2}$ and $\mathcal{Y}_{1,1} \cup \mathcal{Y}_{2,1}$, respectively (see (22)).

Step 6 Compute the syndrome values of Y for the code $\mathcal{C}_q(n, t)$ and solve (25) for the remaining entries of $\boldsymbol{\beta}$ and $\boldsymbol{\delta}$ to obtain $E = U^* D^*$.

Step 1 is straightforward and requires $O(rn^2)$ arithmetic operations over F_q. Step 2 can be carried out by one of the decoding algorithms for $\mathcal{C}_q(r, 2t)$ [8], [19] and requires $O(tr + t^3)$ arithmetic operations over F_{q^r}.

As for Step 3, this step needs to be processed only when $(\rho =) \, \mathsf{rank}(\hat{E}) > \frac{t}{2}$; otherwise we can take $\sigma = \tau = 0$ in Proposition 9. We can find $(U_1, D_1) \in \mathcal{M}(\hat{E}, t{-}\rho{+}1)$ by a brute-force approach as follows: (i) enumerate over all subsets $T \subseteq [n]$ of size $\leq t{-}\rho{+}1 \leq \lceil t/2 \rceil$ — say, according to increasing values of $|T|$; (ii) for each T, solve for the vectors $\mathbf{u} \in \mathcal{S}_q(n, T)$ that satisfy $H_1 \mathbf{u} \in \mathsf{span}_{\mathrm{c}}(\hat{E})$ (or $\mathbf{u} H_2^T \in \mathsf{span}_{\mathrm{r}}(\hat{E})$): this involves solving linear equations over F_q in at most $t{+}1$ variables, namely, the $|T| \leq t{-}\rho{+}1$ unknown entries of $\mathbf{u}$ and the linear combination of the ρ columns of $\hat{U}$ that yields $H_1 \mathbf{u}$.

In Appendix B, we present an algorithm for finding an eligible pair (U_1, D_1) by using a search over subsets $T \subseteq [n]$ of size $|T| \leq \lfloor \frac{t-\rho}{2} \rfloor + 1 \leq \lceil \frac{t}{4} \rceil$. Furthermore, we also show therein that when the crisscross errors are not too short, then there is high probability to have matrices U_1 (or D_1) that consist wholly of unit vectors. In such a case, the required search is *linear* in n, amounting to $O(t^3 n)$ arithmetic operations over F_q. It is still an open problem to find an algorithm for computing (U_1, D_1) in the general case in time complexity which is polynomial in both t and n.

Step 4 involves linear operations on the matrices $H_1 U_1$ and $D_1 H_2^T$ (which are available from Step 3) and A. Such operations can be carried out using $O(t^2 r)$ arithmetic operations over F_q. Similarly, Step 5 involves linear operations on A, U_1, and D_1 and requires $O(t^2 n)$ arithmetic operations over F_q.

We turn now to Step 6, where we need to recover the values $\{\beta_k\}_{k \in \mathcal{Y}_{2,1} \cup \mathcal{Y}_{2,2}}$ and $\{\delta_k\}_{k \in \mathcal{Y}_{1,2} \cup \mathcal{Y}_{2,2}}$. We present next a procedure to solve for those values. The solution is not unique, but from Proposition 9 it follows that all solutions correspond to the same error

array E. The algorithm presented in [19] is a special case of the procedure presented here for $\sigma = \tau = 0$.

Let $\mathcal{Y}'$ denote the set $[\rho] - \mathcal{Y}_{1,1}$. Since the pairs (β_k, δ_k) are known for $k \in \mathcal{Y}_{1,1}$, we can compute the following *modified* syndrome vector $\tilde{\mathbf{s}}$,

$$\tilde{s}_\ell \;=\; s_\ell - \sum_{k \in \mathcal{Y}_{1,1}} \beta_k^{q^\ell} \delta_k \;, \qquad 0 \le \ell < t \;, \tag{26}$$

and from (25) we have

$$\tilde{s}_\ell = \sum_{k \in \mathcal{Y}'} \beta_k^{q^\ell} \delta_k \;, \qquad 0 \le \ell < t \;. \tag{27}$$

We now introduce the following polynomials over F_{q^n}:

$$\begin{aligned}
\Phi(x) &= \sum_{m=0}^{\rho_{1,2}} \phi_m x^{q^m} = \prod_{\zeta \in \mathsf{span}\{\beta_k \,:\, k \in \mathcal{Y}_{1,2}\}} (x - \zeta) \;, \\
\Psi(x) &= \sum_{m=0}^{\rho_{2,1}} \psi_m x^{q^m} = \prod_{\zeta \in \mathsf{span}\{\delta_k \,:\, k \in \mathcal{Y}_{2,1}\}} (x - \zeta) \;, \\
\Lambda(x) &= \sum_{m=0}^{\rho-\tau} \lambda_m x^{q^m} = \prod_{\zeta \in \mathsf{span}\{\beta_k \,:\, k \in \mathcal{Y}_{1,2} \cup \mathcal{Y}_{2,2}\}} (x - \zeta)
\end{aligned}$$

(here $\mathsf{span}\{\cdot\}$ stands for linear span over F_q). Those three polynomials are *linearized* polynomials over F_{q^n}, namely, they have the form $\sum_m a_m x^{q^m}$ where $a_m \in \mathsf{F}_{q^n}$. Several properties of linearized polynomials are summarized in [14, Section 4.9]. In particular, if $a(x) = \sum_m a_m x^{q^m}$ is a linearized polynomial over F_{q^n}, then the mapping $x \mapsto a(x)$ over the domain F_{q^n} is a linear transformation over F_q. Thus, the set of roots of $a(x)$ in F_{q^n} forms a linear vector space over F_q, as this set is a null space of a linear transformation.

Recalling that the values $\{\beta_k\}_{k \in \mathcal{Y}_{1,2}}$ are known, the decoder can compute the polynomial $\Phi(x)$ by solving the following set of $\rho_{1,2}$ linear equations over F_{q^n} for the coefficients ϕ_m:

$$\Phi(\beta_k) \;=\; \sum_{m=0}^{\rho_{1,2}} \phi_m \beta_k^{q^m} \;=\; 0 \;, \qquad k \in \mathcal{Y}_{1,2} \;, \tag{28}$$

with $\phi_{\rho_{1,2}} = 1$. Indeed, the solution for the coefficients ϕ_m is unique since the equations (28) are linearly independent [14, p. 117]. Similarly, the polynomial $\Psi(x)$ can be computed by solving the equations

$$\Psi(\delta_k) \;=\; \sum_{m=0}^{\rho_{2,1}} \psi_m \delta_k^{q^m} \;=\; 0 \;, \qquad k \in \mathcal{Y}_{2,1} \;, \tag{29}$$

with $\psi_{\rho_{2,1}} = 1$.

As for $\Lambda(x)$, when $\gamma = 0$, this polynomial coincides with $\Phi(x)$. Yet, when $\gamma > 0$, we will need additional constraints in order to determine $\Lambda(x)$ uniquely.

Let S be the $(t-\rho+\tau) \times (\rho-\tau+1)$ matrix over F_{q^n} which is defined by

$$S \;=\; \left[\, \tilde{s}_{i+j}^{\,q^{n-i}} \,\right]_{i=0\qquad ,j=0}^{t-\rho+\tau-1\,,\,\rho-\tau} \;, \tag{30}$$

and let R denote the $(t+\sigma+\tau-2\rho+\gamma) \times (t-\rho+\tau)$ matrix over F_{q^n} which is given by

$$R \;=\; \left[\, \psi_{g+i-j}^{\,q^{n-i-g}} \,\right]_{i=0\qquad\qquad ,j=0}^{t-\rho+\tau-1-g\,,\,t-\rho+\tau-1} \;, \tag{31}$$

where $g = \rho_{2,1} = \rho-\sigma-\gamma$ and $\psi_m = 0$ if $m \notin \{0, 1, \ldots, \rho-\sigma-\gamma\}$. We denote by R_b the submatrix consisting of the first b rows of R.

Lemma 11 *Let $\boldsymbol{\lambda} = [\,\lambda_m\,]_{m=0}^{\rho-\tau}$ be the column vector of coefficients of the polynomial $\Lambda(x) = \sum_{m=0}^{\rho-\tau} \lambda_m x^{q^m}$. Then,*

$$RS\boldsymbol{\lambda} \;=\; \mathbf{0}\,.$$

Proof. Let $(S\boldsymbol{\lambda})_\ell$ denote the ℓth entry of $S\boldsymbol{\lambda}$. By (27) we have

$$\begin{aligned}
(S\boldsymbol{\lambda})_\ell \;&=\; \textstyle\sum_{m=0}^{\rho-\tau} \lambda_m \tilde{s}_{\ell+m}^{\,q^{n-\ell}} \;=\; \sum_{m=0}^{\rho-\tau} \lambda_m \Big(\sum_{k\in\mathcal{Y}'} \beta_k^{q^{\ell+m}} \delta_k\Big)^{q^{n-\ell}} \\
&=\; \textstyle\sum_{k\in\mathcal{Y}'} \delta_k^{q^{n-\ell}} \sum_{m=0}^{\rho-\tau} \lambda_m \beta_k^{q^m} \;=\; \sum_{k\in\mathcal{Y}'} \delta_k^{q^{n-\ell}} \Lambda(\beta_k) \\
&=\; \textstyle\sum_{k\in\mathcal{Y}_{2,1}} \delta_k^{q^{n-\ell}} \Lambda(\beta_k)\,, \qquad 0 \le \ell < t-\rho+\tau\,,
\end{aligned} \tag{32}$$

where the last equality follows from having $\Lambda(\beta_k) = 0$ for $k \in \mathcal{Y}_{1,2} \cup \mathcal{Y}_{2,2}$. We thus obtain,

$$\begin{aligned}
(RS\boldsymbol{\lambda})_m \;&=\; \textstyle\sum_{\ell=m}^{m+g} \psi_{g+m-\ell}^{\,q^{n-g-m}} (S\boldsymbol{\lambda})_\ell \;=\; \sum_{\ell=0}^{g} \psi_{g-\ell}^{\,q^{n-g-m}} (S\boldsymbol{\lambda})_{m+\ell} \\
&=\; \textstyle\sum_{\ell=0}^{g} \psi_{g-\ell}^{\,q^{n-g-m}} \sum_{k\in\mathcal{Y}_{2,1}} \delta_k^{q^{n-m-\ell}} \Lambda(\beta_k) \\
&=\; \textstyle\sum_{k\in\mathcal{Y}_{2,1}} \Lambda(\beta_k) \left(\sum_{\ell=0}^{g} \psi_{g-\ell} \delta_k^{q^{g-\ell}}\right)^{q^{n-g-m}} \\
&=\; \textstyle\sum_{k\in\mathcal{Y}_{2,1}} \Lambda(\beta_k) \left(\Psi(\delta_k)\right)^{q^{n-g-m}}\,, \qquad 0 \le m < t-\rho+\tau-g\,.
\end{aligned} \tag{33}$$

The lemma now follows by observing that $\Psi(\delta_k) = 0$ for $k \in \mathcal{Y}_{2,1}$. □

Lemma 12 *Let $\mathbf{v} = [\,v_m\,]_{m=0}^{\rho-\tau}$ be the column vector of coefficients of a linearized monic polynomial $v(x) = \sum_{m=0}^{\rho-\tau} v_m x^{q^m}$ such that $v(\beta_k) = 0$ for $k \in \mathcal{Y}_{1,2}$ and*

$$R_\gamma S\mathbf{v} \;=\; \mathbf{0}\,.$$

Then $v(x) = \Lambda(x)$.

Proof. Since $v(x)$ is a linearized polynomial, it suffices to show that $v(\beta_k) = 0$ for $k \in \mathcal{Y}_{2,2}$. The equality $R_\gamma S\mathbf{v} = \mathbf{0}$ implies

$$\sum_{\ell=0}^{g} \psi_{g-\ell}^{q^{n-g-m}} (S\mathbf{v})_{m+\ell} = 0 \ , \qquad 0 \le m < \gamma$$

(compare with (33)). On the other hand, following (32), we have

$$(S\mathbf{v})_\ell \ = \ \sum_{k \in \mathcal{Y}'} \delta_k^{q^{n-\ell}} v(\beta_k) \ , \qquad 0 \le \ell < t-\rho+\tau \ .$$

Noting that $g + \gamma \le t - \rho + \tau$, we can combine the last two equations to obtain

$$\sum_{k \in \mathcal{Y}'} v(\beta_k) \Big(\sum_{\ell=0}^{g} \psi_{g-\ell} \delta_k^{q^{g-\ell}} \Big)^{q^{n-g-m}} \ = \ 0 \ , \qquad 0 \le m < \gamma \ ,$$

namely,

$$\sum_{k \in \mathcal{Y}'} v(\beta_k) \left(\Psi(\delta_k) \right)^{q^{n-g-m}} \ = \ 0 \ , \qquad 0 \le m < \gamma \ .$$

By assumption we have $v(\beta_k) = 0$ for $k \in \mathcal{Y}_{1,2}$. Since we also have $\Psi(\delta_k) = 0$ for $k \in \mathcal{Y}_{2,1}$, we end up with

$$\sum_{k \in \mathcal{Y}_{2,2}} v(\beta_k) \left(\Psi(\delta_k) \right)^{q^{n-g-m}} \ = \ 0 \ , \qquad 0 \le m < \gamma \ .$$

Now, the elements $\{\Psi(\delta_k)\}_{k \in \mathcal{Y}_{2,2}}$ are linearly independent over F_q, or else $\Psi(x)$ would vanish at a nontrivial linear combination of the elements $\{\delta_k\}_{k \in \mathcal{Y}_{2,2}}$, which is impossible. By [14, p. 117] we conclude that the elements $v(\beta_k)$ must be zero for every $k \in \mathcal{Y}_{2,2}$. □

It follows from Lemmas 11 and 12 that for any integer b in the range $\gamma \le b \le t+\sigma+\tau-2\rho+\gamma$, there is a unique monic linearized polynomial $v(x)$ that vanishes at β_k for all $k \in \mathcal{Y}_{1,2}$ and satisfies the set of equations

$$R_b S\mathbf{v} \ = \ \mathbf{0} \ .$$

That unique polynomial equals $\Lambda(x)$.

Lemma 13 *Let $v(x) = \sum_{m=0}^{\rho-\tau} v_m x^{q^m}$ be a linearized polynomial over F_{q^n}. Then $v(\beta_k) = 0$ for $k \in \mathcal{Y}_{1,2}$ if and only if there is a polynomial $\Theta(x) = \sum_{m=0}^{\gamma} \theta_m x^{q^m}$ over F_{q^n} such that*

$$v(x) \ = \ \Theta(\Phi(x)) \ . \tag{34}$$

Proof. Clearly, the polynomial $\Theta(\Phi(x))$ vanishes at β_k for all $k \in \mathcal{Y}_{1,2}$. The "only if" part can be proved by using symbolic division [12, p. 108]. Namely, given $v(x)$ and $\Theta(x)$, we can find linearized polynomials $\Theta(x)$ and $\Delta(x)$ such that $v(x) = \Theta(\Phi(x)) + \Delta(x)$ and

$\deg \Delta < \deg \Phi = q^{\rho-\tau-\gamma}$. Now, if $v(x)$ vanishes at $\{\beta_k\}_{k\in\mathcal{Y}_{1,2}}$, then so does $\Delta(x)$. This means that $\Delta(x)$ has at least $q^{\rho-\tau-\gamma}$ roots in F_{q^n}, which implies that $\Delta(x) \equiv 0$. □

Let Q denote the $(\gamma+1) \times (\rho-\tau+1)$ matrix over F_{q^n} which is given by

$$Q \;=\; \left[\, \phi_{j-i}^{q^i} \,\right]_{i=0\,,\,j=0}^{\gamma\;\;,\rho-\tau} \;, \tag{35}$$

where $\phi_m = 0$ if $m \notin \{0, 1, \ldots, \rho-\tau-\gamma\}$. Then (34) is equivalent to having

$$\mathbf{v} \;=\; Q^T \boldsymbol{\theta} \;,$$

where $\mathbf{v} = [\, v_m \,]_{m=0}^{\rho-\tau}$ and $\boldsymbol{\theta} = [\, \theta_m \,]_{m=0}^{\gamma}$.

Lemmas 11, 12, and 13 provide the means by which we can compute the elements $\{\beta_k\}_{k\in\mathcal{Y}_{2,2}}$. We first find the coefficients of $\Theta(x)$ by solving the set of equations

$$R_\gamma S\, Q^T \boldsymbol{\theta} \;=\; \mathbf{0} \tag{36}$$

for $\boldsymbol{\theta} = [\, \theta_m \,]_{m=0}^{\gamma}$ with $\theta_\gamma = 1$. By those lemmas we have $Q^T\boldsymbol{\theta} = \boldsymbol{\lambda}$. Denote by $\ker \Lambda$ the root space of $\Lambda(x)$. Since the mapping $x \mapsto \Lambda(x)$ is linear over F_q, finding a basis of $\ker \Lambda$ (over F_q) is equivalent to finding a basis of the null space of an $n \times n$ matrix over F_q which represents the mapping $x \mapsto \Lambda(x)$ [1]. The set $\{\beta_k\}_{k\in\mathcal{Y}_{2,2}}$ is chosen so that it extends $\{\beta_k\}_{k\in\mathcal{Y}_{1,2}}$ to span the root space of $\Lambda(x)$. (In fact, since $\Lambda(x)$ is already given in the form $\Theta(\Phi(x))$, then we can first find a basis $\{\varepsilon_k\}_{k\in\mathcal{Y}_{2,2}}$ of the root space of $\Theta(x)$ and then solve the nonhomogeneous equations $\Phi(\beta_k) = \varepsilon_k$ for $\{\beta_k\}_{k\in\mathcal{Y}_{2,2}}$.)

At this point, the set of equations (27) has become linear in the remaining unknown variables $\{\beta_k\}_{k\in\mathcal{Y}_{2,1}}$ and $\{\delta_k\}_{k\in\mathcal{Y}_{1,2}\cup\mathcal{Y}_{2,2}}$, and so those variables can be solved for in a straightforward manner.

Following is a summary of Step 6 of the outlined decoding algorithm. We assume that the decoder already knows the entries $\{\beta_k\}_{k\in\mathcal{Y}_{1,1}\cup\mathcal{Y}_{1,2}}$ in the vector $\boldsymbol{\beta} = \boldsymbol{\alpha}U^*$, as well as the entries $\{\delta_k\}_{k\in\mathcal{Y}_{1,1}\cup\mathcal{Y}_{2,1}}$ in $\boldsymbol{\delta} = D^*\boldsymbol{\omega}$.

Step 6.1 Compute the syndrome vector $\mathbf{s}$ by (24) and the modified syndrome vector $\tilde{\mathbf{s}}$ by (26).

Step 6.2 Compute the coefficients of $\Phi(x)$ and $\Psi(x)$ by solving (28) and (29).

Step 6.3 Compute the matrix $R_\gamma S Q^T$ using (30), (31), and (35).

Step 6.4 Compute the coefficients of $\Theta(x)$ by solving (36).

Step 6.5 Find a set $\{\beta_k\}_{\mathcal{Y}_{2,2}}$ that extends $\{\beta_k\}_{k\in\mathcal{Y}_{1,2}}$ to a basis of the root space of $\Lambda(x) = \Theta(\Phi(x))$.

Step 6.6 Find the remaining unknown entries of $\boldsymbol{\beta}$ and $\boldsymbol{\delta}$ by solving the set of (already linear) equations (27).

Step 6.7 $E = U^* D^*$, where $\boldsymbol{\beta} = \boldsymbol{\alpha} U^*$ and $\boldsymbol{\delta} = D^* \boldsymbol{\omega}$.

The overall complexity of Step 6 is $O(tn + t^3)$ arithmetic operations over F_{q^n}.

Appendix A

We present here an example that exhibits the savings in redundancy that can be obtained by the use of $\mathsf{C}_q(n, t, \mathsf{p})$ for specific channel parameters.

Example 3 Suppose that $q = 2^8$, $n = 200$, $\mathsf{p} = 10^{-15}$, and $t = 6$. (Such a value of t corresponds, for example, to the case where each row or column gets corrupted with probability $\pi = 10^{-4}$, independently of the other rows or columns, and we want to guarantee that the probability of having more than t crisscross errors is less than 10^{-15}.) If we assume that decoding failure introduces t new crisscross errors in addition to up to $t+1$ existing ones, then the chosen value of p corresponds to an average 'byte error rate' of $((2t+1)/n) \cdot \mathsf{p} = 0.65 \times 10^{-16}$ after decoding.

Plugging our parameters into (4) yields $d = 18$. For the given q and n, we can take H_1 and H_2 to be parity-check matrices of shortened Reed-Solomon codes, in which case $r = 17$. Hence, by Proposition 1, the overall redundancy of $\mathsf{C}_{2^8}(200, 6, 10^{-15})$ is at most 1404 bytes. This is more than 40% savings compared to the $2tn = 2400$ redundancy bytes that we would need if we insisted on decoding correctly any pattern of up to t crisscross errors. □

Appendix B

We show here how matrices (U_1, D_1) that satisfy requirements (a)–(c) in Proposition 9 can be found by a search over subsets $T \subseteq [n]$ of size $|T| \leq \lfloor \frac{t-\rho}{2} \rfloor + 1 \leq \lceil \frac{t}{4} \rceil$. To this end, we will assume that H_1 and H_2 are parity-check matrices of conventional linear codes for which there exists an efficient syndrome-based algorithm to decode up to t errors. This means that we need d to be at least $2t+1$, but this is typically the case in (4).

The modified decoding algorithm reads as follows (Steps 1–2 and 4–6 remain unchanged):

Steps 1–2 Compute $\hat{E}$ as in Section 4.

Step 3.0 Let $\rho = \mathsf{rank}(\hat{E})$ and $w = 0$.

Step 3.1 Find an $n \times \sigma$ matrix U_1 over F_q whose columns form a maximal set of linearly-independent elements in $\{\, \mathbf{u} \mid \mathbf{u} \in \mathcal{S}_q(n, w) \text{ and } H_1\mathbf{u} \in \mathsf{span}_{\mathrm{c}}(\hat{E}) \,\}$ (such a matrix U_1 can be found using a search over all subsets of $[n]$ of size w).

If $\sigma + t \geq 2\rho$, then let $\tau = 0$ and go to Step 4.

Step 3.2 Find a matrix Υ whose rows form a basis of the left null space of H_1U_1, i.e., $\{\, \mathbf{y} \in \mathsf{F}_q^r \mid \mathbf{y}H_1U_1 = \mathbf{0} \,\}$. If $\sigma = 0$ then let $\Upsilon = I_r$.

Step 3.3 Find a $\tau \times r$ matrix V whose rows form a basis of the rows of $\Upsilon\hat{E}$.

Step 3.4 For each row in V, attempt to decode an 'error vector' in $\mathcal{S}_q(n, t)$ whose syndrome with respect to H_2^T equals that row.

If all decoding attempts are successful, write the resulting decoded vectors as rows in a $\tau \times n$ array D_1 and go to Step 4. Otherwise, go to Step 7.

Steps 4–6 Compute E as in Section 4.

Step 7 If Steps 3.4 and 6 were successful and $\mathsf{rank}(E) = \rho$ and $\mathsf{w}_{\mathrm{cov}}(E) \leq t$ then stop.

Otherwise (failure so far), return to Step 3.1 while switching the roles of rows and columns of the received array Y. If that fails, increase w and return to Step 3.1 as long as $w \leq \frac{t-\rho}{2}+1$.

The cover weight in Step 7 is easy to find: this problem can be formulated as finding the smallest vertex cover in a bipartite graph whose vertices are the rows and columns of E, and an edge connects row i to column j if and only if the (i, j)th entry in E is nonzero. Now, it is known that the size of the smallest vertex cover in a bipartite graph is equal to the size of a maximum matching in that graph [22, p. 207], and the latter can be found by an efficient algorithm [2, Section 10.5].

Steps 2, 6, and 7 guarantee that the decoded error array will satisfy conditions 1–4 of Theorem 10. Hence, it suffices to show that D_1 decodes successfully in Step 3.4 for at least one of the iterations of Steps 3.1–3.4 and that the resulting pair (U_1, D_1) satisfies requirements (a)–(c) in Proposition 9.

We first observe that the columns of U_1 which are found in every iteration of Step 3.1 belong to the set $\{\, \mathbf{u} \mid \mathbf{u} \in \mathcal{S}_q(n, \lceil t/4 \rceil) \text{ and } H_1\mathbf{u} \in \mathsf{span}_{\mathrm{c}}(\hat{E}) \,\}$ and, so, the event $\{\, \mathsf{span}_{\mathrm{c}}(U_1) \not\subseteq \mathsf{span}_{\mathrm{c}}(E) \,\}$ is contained in the 'bad event' $\mathcal{B}_{\mathrm{c}}$ in the proof of Proposition 3. The probability of the latter event is less than p and so we assume from now on that $\mathsf{span}_{\mathrm{c}}(U_1) \subseteq \mathsf{span}_{\mathrm{c}}(E)$.

Next we show that if the decoding in Step 3.4 is successful, then $\mathsf{rank}(D_1) = \tau$ and $\sigma + \tau = \rho \geq 2\rho - t$. Since $\mathsf{span}_{\mathrm{c}}(U_1) \subseteq \mathsf{span}_{\mathrm{c}}(E)$, we can extend U_1 to form an $n \times \rho$ matrix

$U = [\, U_1 \; U_2 \,]$ whose columns are a basis of $\mathsf{span}_{\mathrm{c}}(E)$. Decompose E by

$$E \;=\; UD \;=\; \Big[U_1 \; U_2 \Big] \left[\begin{array}{c} D' \\ D'' \end{array} \right] \;=\; U_1 D' + U_2 D'' \;, \tag{37}$$

where $\mathsf{rank}(D') = \sigma$ and $\mathsf{rank}(D'') = \rho{-}\sigma$. Since $\langle U, I_\rho, D \rangle$ is a decomposition of E, then, by Lemma 8(a), $\langle H_1 U, I_\rho, D H_2^T \rangle$ is a decomposition of $\hat{E}$ and, so, $\mathsf{rank}(H_1 U_1) = \mathsf{rank}(D' H_2^T) = \sigma$ and $\mathsf{rank}(H_1 U_2) = \mathsf{rank}(D'' H_2^T) = \rho{-}\sigma$.

Let Υ and V be the matrices computed in Steps 3.2 and 3.3. We have $\mathsf{rank}(\Upsilon) = r - \mathsf{rank}(H_1 U_1) = r{-}\sigma$ and so $\tau = \mathsf{rank}(V) \geq \rho{-}\sigma$. On the other hand,

$$V \;=\; \Upsilon H_1 E H_2^T \;=\; \Upsilon H_1 U_1 D' H_2^T + \Upsilon H_1 U_2 D'' H_2^T \;=\; \Upsilon H_1 U_2 D'' H_2^T \tag{38}$$

and, therefore, $\mathsf{rank}(V) \leq \mathsf{rank}(H_1 U_2) = \rho{-}\sigma$. Hence, $\tau = \rho{-}\sigma$. Now, linearly-independent rows in V necessarily decode in Step 3.4 into linearly-independent rows in D_1. We thus have $\mathsf{rank}(D_1) = \tau = \rho{-}\sigma$.

At this point, we have established requirements (a) and (c) in Proposition 9 (with probability greater than $1{-}\mathsf{p}$). We next show that D_1 decodes successfully in Step 3.4 and $\mathsf{span}_{\mathrm{r}}(D_1) \subseteq \mathsf{span}_{\mathrm{r}}(E)$ when w equals $\lfloor \frac{t-\rho}{2} \rfloor{+}1$, possibly by using the transposition in Step 7. To this end, we turn to the proof of Lemma 7 with $B = E$ and observe that (16) implies that at least one of the spaces therein, $\mathcal{L}_{\mathrm{c}}$ or $\mathcal{L}_{\mathrm{r}}$, has a basis in which each element has Hamming weight $\leq \lfloor \frac{t-\rho}{2} \rfloor{+}1$. Without loss of generality, we assume that $\mathcal{L}_{\mathrm{c}}$ has such a basis (the transposition in Step 7 takes care of the remaining possibility). Recalling that $\mathsf{span}_{\mathrm{c}}(H_1 E) = \mathsf{span}_{\mathrm{c}}(H_1 E H_2^T)$, we have,

$$\begin{aligned} \mathcal{L}_{\mathrm{c}} \;&\subseteq\; \mathsf{span}_{\mathrm{c}} \Big(\mathcal{S}_q(n, \lfloor \tfrac{t-\rho}{2} \rfloor{+}1) \cap \mathsf{span}_{\mathrm{c}}(E) \Big) \\ &\subseteq\; \mathsf{span}_{\mathrm{c}} \Big\{ \mathbf{u} \mid \mathbf{u} \in \mathcal{S}_q(n, \lfloor \tfrac{t-\rho}{2} \rfloor{+}1) \text{ and } H_1 \mathbf{u} \in \mathsf{span}_{\mathrm{c}}(\hat{E}) \Big\} \\ &=\; \mathsf{span}_{\mathrm{c}}(U_1) \;, \end{aligned}$$

where U_1 is the matrix computed in Step 3.1 for $w = \lfloor \frac{t-\rho}{2} \rfloor{+}1$. In particular, U_1 spans all the columns of E_{c}^- since the latter are contained in $\mathcal{L}_{\mathrm{c}}$. Returning to the decomposition (37), D'' will thus have nonzero entries only at columns which are indexed by $\mathcal{X}_{\mathrm{c}}$. Now, by (38) we have that the ith row in V equals $\mathbf{v}_i D'' H_2^T$ for some $\mathbf{v}_i \in \mathsf{F}_q^\tau$. Since the support of $\mathbf{v}_i D''$ is contained in $\mathcal{X}_{\mathrm{c}}$, the decoding of the ith row of V in Step 3.4 will be successful, making the ith row of D_1 equal to $\mathbf{v}_i D''$. Furthermore, we have $\mathsf{span}_{\mathrm{r}}(D_1) = \mathsf{span}_{\mathrm{r}}(D'') \subseteq \mathsf{span}_{\mathrm{r}}(E)$.

Finally, in the next lemma we bound from below the probability of having $\mathsf{rank}(E_{\mathrm{c}}^-) = x_{\mathrm{r}}$. In such a case, the space $\mathcal{L}_{\mathrm{c}}$ in the proof of Lemma 7 has dimension x_{r} (see (14)), and so it has a basis which consists of unit vectors. Hence, in this case, the error array will be found when $w = 1$, thus requiring a search in Step 3.1 which is linear in n.

Lemma 14 *Let the probability measure on an $n \times n$ array E over F_q be defined according to conditions (P1)–(P3), and further suppose that the channel marks in (P2) at least η entries in each one of the rows that were selected in (P1). Then,*

$$\mathsf{Prob}\Big\{\, \mathsf{rank}(E_{\rm c}^{-}) = x_{\rm r} \,\Big\} \;>\; 1 - q^{t-\eta} \;.$$

Proof. For $i = 1, 2, \ldots, x_{\rm r}$ we denote by M_i the $i \times (n - x_{\rm c})$ submatrix of $E_{\rm c}^{-}$ whose rows are the portions within $E_{\rm c}^{-}$ of the first i selected rows in (P1). Defining $\mathsf{rank}(M_0) = 0$, we show by induction on $i = 1, 2, \ldots, x_{\rm r}$ that $\mathsf{rank}(M_i) > \mathsf{rank}(M_{i-1})$ with probability $\geq 1 - q^{(i-1)+x_{\rm c}-\eta}$.

The first row selected in (P1) contains at least $\eta - x_{\rm c}$ marked entries within $E_{\rm c}^{-}$. Therefore, M_1 is nonzero with probability $\geq 1 - q^{x_{\rm c}-\eta}$.

As for the induction step, suppose without loss of generality that the last $i-1$ columns of M_{i-1} contain a basis of $\mathsf{span}_{\rm c}(M_{i-1})$. Per our assumption, there are at least $\eta - x_{\rm c} - (i-1)$ entries that were marked in (P3) within the first $n - x_{\rm c} - (i-1)$ coordinates of the ith row of M_i. Let $\mathbf{v}$ denote a column of M_i that contains one of those marked entries as its ith coordinate. The probability that $\mathbf{v}$ belongs to the linear span of the last $i-1$ columns of M_i is at most $1/q$. Therefore, $\mathsf{rank}(M_i) = \mathsf{rank}(M_{i-1})$ with probability $\leq q^{(i-1)+x_{\rm c}-\eta}$.

Hence,

$$\begin{aligned}
\mathsf{Prob}\Big\{\, \mathsf{rank}(E_{\rm c}^{-}) = x_{\rm r} \,\Big\} \;&=\; \mathsf{Prob}\Big\{\, \mathsf{rank}(M_{x_{\rm r}}) = x_{\rm r} \,\Big\} \\
&=\; \mathsf{Prob}\Big\{ \bigcap_{i=1}^{x_{\rm r}} \{\, \mathsf{rank}(M_i) > \mathsf{rank}(M_{i-1}) \,\} \Big\} \\
&\geq\; 1 - \sum_{i=1}^{x_{\rm r}} \mathsf{Prob}\Big\{\, \mathsf{rank}(M_i) = \mathsf{rank}(M_{i-1}) \,\Big\} \\
&\geq\; 1 - \sum_{i=1}^{x_{\rm r}} q^{(i-1)+x_{\rm c}-\eta} \;>\; 1 - q^{t-\eta} \;,
\end{aligned}$$

as claimed. □

References

[1] E.R. Berlekamp, H. Rumsey, G. Solomon, *On the solution of algebraic equations over finite fields, Inform. Control,* 10 (1967), 553–564.

[2] N.L. Biggs, *Discrete Mathematics,* Oxford University Press, Oxford, 1985.

[3] M. Blaum, R.J. McEliece, *Coding protection for magnetic tapes: a generalization of the Patel-Hong code, IEEE Trans. Inform. Theory,* IT-31 (1985), 690–693.

[4] Ph. Delsarte, *Bilinear forms over a finite field, with applications to coding theory, J. Comb. Th. A,* 25 (1978), 226–241.

[5] S.A. Elkind, D.P. Siewiorek, *Reliability and performance of error-correcting memory and register codes, IEEE Trans. Computers,* C-29 (1980), 920–927.

[6] P.G. Farrell, *A survey of array error control codes, Europe. Trans. Telecomm. Rel. Technol.,* 3 (1992) 441–454.

[7] G.D. Forney, *Concatenated Codes,* MIT Press, Cambridge, Massachusetts, 1966.

[8] E.M. Gabidulin, *Theory of codes with maximum rank distance, Probl. Peredach. Inform.,* 21 (1985), 3–16 (in Russian; pp. 1–12 in the English translation).

[9] E.M. Gabidulin, *Optimal array error-correcting codes, Probl. Peredach. Inform.,* 21 (1985), 102–106 (in Russian).

[10] G.L. Katsman, M.A. Tsfasman, S.G. Vladuţ, *Spectra of linear codes and error probability of decoding,* in *Proc. Int'l Workshop on Coding Theory and Algebraic Geometry,* Luminy, France (June 1991), 82–98, H. Stichtenoth, M.A. Tsfasman (eds.), Lecture Notes in Math., Vol. 1518, Springer, Berlin, 1992.

[11] L. Levine, W. Meyers, *Semiconductor memory reliability with error detecting and correcting codes, Computer,* 9 (Oct. 1976), 43–50.

[12] R. Lidl, H. Niederreiter, *Introduction to Finite Fields and their Applications,* Revised Edition, Cambridge University Press, Cambridge, 1994.

[13] S. Lin, D.J. Costello, Jr., *Error Control Coding, Fundamentals and Applications,* Prentice-Hall, Englewood Cliffs, New Jersey, 1983.

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

[15] R.J. McEliece, *The Theory of Information and Coding,* Addison-Wesley, Reading, Massachusetts, 1977.

[16] W.F. Mikhail, R.W. Bartoldus, R.A. Rutledge, *The reliability of memory with single-error correction, IEEE Trans. Computers,* C-31 (1983), 560–564.

[17] A.M. Patel, S.J. Hong, *Optimal rectangular code for high density magnetic tapes, IBM J. Res. Dev.,* 18 (1974), 579–588.

[18] P. Prunsinkiewicz, S. Budkowski, *A double track error-correction code for magnetic tape, IEEE Trans. Computers,* C-25 (1976), 642–645.

[19] R.M. Roth, *Maximum-rank array codes and their application to crisscross error correction, IEEE Trans. Inform. Theory,* IT-37 (1991), 328–336.

[20] R.M. Roth, *Tensor codes for the rank metric, IEEE Trans. Inform. Theory,* to appear.

[21] R.M. Roth, G. Seroussi, *Reduced-redundancy product codes, Proc. IEEE International Workshop on Information Theory,* Haifa, Israel (June 1996), p. 78.

[22] S.G. Williamson, *Combinatorics for Computer Science,* Computer Science Press, Rockville, Maryland, 1985.

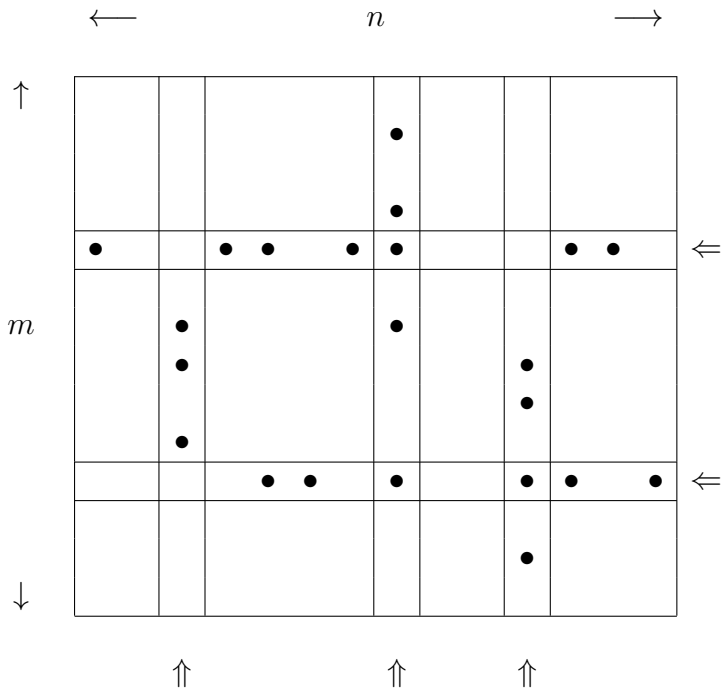

Figure 1: Typical crisscross error pattern.

Captions:

Figure 1: Typical crisscross error pattern.

RON M. ROTH (M'89) was born in Ramat Gan, Israel, in 1958. He received the B.Sc. degree in computer engineering, the M.Sc. in electrical engineering and the D.Sc. in computer science from Technion — Israel Institute of Technology, Haifa, Israel, in 1980, 1984 and 1988, respectively. Since 1988 he has been with the Computer Science Department at the Technion. During the academic years 1989–91 he was a Visiting Scientist at IBM Research Division, Almaden Research Center, San Jose, California, and, since 1994, he has been a consultant for Hewlett-Packard Company — Israel Science Center, Haifa, Israel. He is currently on a sabbatical leave from Technion, visiting Hewlett-Packard Laboratories, Palo Alto, California.

His research interests include coding theory, information theory, and their application to the theory of complexity.