Multiple-Error-Correcting Codes for Analog Computing on Resistive Crossbars

Hengjia Wei and Ron M. Roth

***Abstract*—Error-correcting codes over the real field are studied which can locate outlying computational errors when performing approximate computing of real vector–matrix multiplication on resistive crossbars. Prior work has concentrated on locating a single outlying error and, in this work, several classes of codes are presented which can handle multiple errors. It is first shown that one of the known constructions, which is based on spherical codes, can in fact handle multiple outlying errors. A second family of codes is then presented with 0–1 parity-check matrices which are sparse and disjunct; such matrices have been used in other applications as well, especially in combinatorial group testing. In addition, a certain class of the codes that are obtained through this construction is shown to be efficiently decodable. As part of the study of sparse disjunct matrices, this work also contains improved lower and upper bounds on the maximum Hamming weight of the rows in such matrices.**

***Index Terms*—Fault-tolerant computing, linear codes over the real field, vector–matrix multiplication, sparse group testing, disjunct matrices with limited row weights**

I. Introduction

Vector–matrix multiplication is a computational task that is found in numerous applications, including machine learning (e.g., deep learning) and signal processing. Designing circuits for vector–matrix multiplication requires achieving high computational throughput while concurrently ensuring minimal energy consumption and a compact physical footprint. These criteria have prompted recent proposals to incorporate resistive memory technology into analog computing architectures.

Let $\boldsymbol{u}$ be a row ℓ-vector and A be an $\ell \times n$ matrix—both with (nonnegative) entries in $\mathbb{R}$ or $\mathbb{Z}$. In current implementations of vector–matrix multiplication [1],[9],[10],[14],[22], the matrix $A = (a_{i,j})$ is realized as a crossbar of ℓ row conductors and n column conductors with programmable nano-scale resistors at the junctions. The resistor at the junction (i, j) is set to have conductance that is proportional to the entry $a_{i,j}$ of A. Each entry u_i of $\boldsymbol{u}$ is converted into a voltage level that is proportional to u_i and fed to the corresponding row conductor. Then the product $\boldsymbol{c} = \boldsymbol{u}A$, carried out over the real field $\mathbb{R}$, can be computed by reading the currents at the column conductors. Negative entries in $\boldsymbol{u}$ or A can be accommodated by duplication of the circuit.

Recently, the second author proposed two classes of coding schemes to locate computational errors under two distinct scenarios: *exact* integer vector–matrix multiplication [18] and *approximate* real vector–matrix multiplication [19]. We next describe the second scenario, as it will be the subject of this work as well.

In the model described in [19], the ideal computation $\boldsymbol{c} = \boldsymbol{u}A \in \mathbb{R}^n$ may be distorted by two types of errors, which lead to a read vector

$$\boldsymbol{y} = \boldsymbol{c} + \boldsymbol{\varepsilon} + \boldsymbol{e} \in \mathbb{R}^n, \tag{1}$$

where $\boldsymbol{e}, \boldsymbol{\varepsilon} \in \mathbb{R}^n$. The entries of $\boldsymbol{\varepsilon}$ are all within the interval $[-\delta, \delta]$ for some prescribed threshold δ, representing small computational errors that are tolerable, while the entries of $\boldsymbol{e}$ represent outlying errors that may be caused by events such as stuck cells or short cells in the array (and may have large magnitudes). The goal is to design a coding scheme that allows to locate all the non-zero entries of $\boldsymbol{e}$ that are outside an interval $[-\Delta, \Delta]$, for the smallest Δ, provided that the number of outlying errors does not exceed a prescribed number τ. A more general setting includes the option of detecting σ additional errors and, as shown in [19], in this case the value $m = 2\tau + \sigma$ plays a role when analyzing the correction capability of a coding scheme.

The encoding scheme presented in [19] can be characterized by a linear $[n, k]$ code $\mathcal{C}$ over $\mathbb{R}$: we allocate $r = n-k$ columns of the matrix A for redundancy so that each row of A forms a codeword of $\mathcal{C}$. Then the result of the multiplication of any input real row vector $\boldsymbol{u}$ by the matrix A is also a codeword of $\mathcal{C}$.

In crude terms (with more details to be provided in Section II), the required condition from the linear code $\mathcal{C}$ is that it has a decoder that locates all the outlying errors of magnitude above Δ, whenever the Hamming weight of $\boldsymbol{e}$ does not exceed τ; moreover, if the decoder returns a set of locations (rather than just detects errors), then $\boldsymbol{e}$ should be nonzero at all these locations. Linear codes over $\mathbb{R}$ which satisfy this condition are referred to as *analog error-correcting codes*.

For the case $m = 2\tau + \sigma \leqslant 2$ (which includes the single error location/detection cases, i.e., $(\tau, \sigma) = (0, 1), (1, 0)$), code constructions were proposed in [19] for several trade-offs between the redundancy r and the smallest attainable ratio Δ/δ. One of the constructions for $m = 2$ has a sparse parity-check matrix over $\{-1, 0, 1\}$ and attains $\Delta/\delta \leqslant 2\lceil 2n/r \rceil$, for every even redundancy $r \geqslant \sqrt{n}$; another construction has a

Hengjia Wei is with the Peng Cheng Laboratory, Shenzhen 518055, China (e-mail: hjwei05@gmail.com). He is also with the School of Mathematics and Statistics, Xi'an Jiaotong University, Xi'an 710049, China, and the Pazhou Laboratory (Huangpu), Guangzhou 510555, China.

Ron M. Roth is with the Computer Science Department, Technion–Israel Institute of Technology, Haifa 3200003, Israel (e-mail: ronny@cs.technion.ac.il).

The work of H. Wei was supported in part by the major key project of Peng Cheng Laboratory under Grant PCL2024AS103 and Grant PCL2023AS1-2 and the National Natural Science Foundation of China under Grant 12371523. The work of R. M. Roth was supported in part by Grant No. 1713/20 from the Israel Science Foundation.

parity-check matrix that forms a spherical code and attains $\Delta/\delta = O(n/\sqrt{r})$ with $r = \Theta(\log n)$.

In this work, we present several classes of codes over $\mathbb{R}$ for a wide range of values m, and compute upper bounds on the attainable ratios Δ/δ, in terms of n, m, and r; see Table I. When $m = 2$, our bounds coincide with those presented in [19],[20]. One of the classes is actually the spherical code scheme of [19] when constructed with redundancy $r = \Theta(m^2 \log n)$: we show that these codes can still attain $\Delta/\delta = O(n/\sqrt{r})$ yet for a wide range of $m \geqslant 2$. In our analysis we make use of the *restricted isometry property* (and a variant thereof) of *matrices of low coherence*—a tool which is widely used in compressed sensing [2],[3].

A second class of codes to be presented is based on *disjunct matrices with limited row weights*—a notion that has been applied, *inter alia*, in combinatorial group testing [11]. Employing the known construction of disjunct matrices of [11], for any $n, \ell, m \in \mathbb{Z}^+$ such that $n^{1/(\ell+1)}$ is a prime power and $m \leqslant \lceil n^{1/(\ell+1)}/\ell \rceil$, our codes attain $\Delta/\delta \leqslant 2n^{\ell/(\ell+1)}$ with $r \leqslant \ell m n^{1/(\ell+1)}$.

Our study also includes a new family of disjunct matrices (which, in turn, can then be employed in our code construction mentioned above). Specifically, for any positive integer $\rho \leqslant \sqrt{n}$ such that n/ρ is a prime power, we construct optimal disjunct matrices with maximum row weight $\leqslant \rho$, achieving the lower bound on the number of rows as stated in [11]; formerly, such disjunct matrices were exclusively established for $\rho = \sqrt{n}$. Moreover, by deriving a new lower bound on the number of rows, we show that the construction in [11] of disjunct matrices with maximum row weight $\rho \geqslant \sqrt{n}$ is asymptotically optimal.

The paper is organized as follows. We begin, in Section II, by providing notation and known results used throughout the paper. This section also contains our new lower bound on the number of rows of a disjunct matrix with limited row weights.

In Section III, we analyze the spherical code construction and establish its performance for a wide range of values m.

In Section IV, we present the code construction that is based on disjunct matrices with limited row weights. Efficient decoding algorithms to locate the outlying errors are also presented.

In Section V, we present our new family of optimal disjunct matrices. Employing these matrices in our code construction, for any (fixed) rational number $\alpha \in [1/2, 1)$ they attain $r \leqslant mn^{\alpha}$ and $\Delta/\delta \leqslant 2mn/r$ for infinitely many values of n. Interestingly, these parameters align with those of the single-error-correcting codes in [19] (wherein r can be any even integer such that $r(r-1) \geqslant n$ and $\Delta/\delta \leqslant 2\lceil 2n/r \rceil$).

II. Preliminaries

For integers $\ell \leqslant n$, we denote by $[\ell : n]$ the integer subset $\{z \in \mathbb{Z} : \ell \leqslant z < n\}$. We will use the shorthand notation $[n]$ for $[0 : n]$, and we will typically use $[n]$ to index the entries of vectors in $\mathbb{R}^n$. Similarly, the entries of an $r \times n$ matrix $H = (H_{i,j})$ will be indexed by $(i, j) \in [r] \times [n]$, and H_i and $\boldsymbol{h}_j$ will denote, respectively, row i and column j in H. For a subset $\mathcal{J} \subseteq [n]$, the notation $(H)_{\mathcal{J}}$ stands for the $r \times |\mathcal{J}|$ submatrix of H that is formed by the columns that are indexed by $\mathcal{J}$.

Unless specified otherwise, all logarithms are taken to base 2.

A. Analog error-correcting codes

Given $\delta, \Delta \in \mathbb{R}^+$, let

$$\mathcal{Q}(n, \delta) \triangleq \{\boldsymbol{\varepsilon} = (\varepsilon_j) \in \mathbb{R}^n : \|\boldsymbol{\varepsilon}\|_\infty \leqslant \delta\}$$

be the set of all tolerable error vectors with threshold δ, where $\|\boldsymbol{\varepsilon}\|_\infty$ stands for the infinity norm $\max_{j\in[n]}|\varepsilon_j|$. For $\boldsymbol{e} = (e_j)_j \in \mathbb{R}^n$, define

$$\mathsf{Supp}_\Delta(\boldsymbol{e}) \triangleq \{j \in [n] : |e_j| > \Delta\}.$$

In particular, $\mathsf{Supp}_0(\boldsymbol{e})$ is the ordinary support of $\boldsymbol{e}$. We use $\mathsf{w}(\boldsymbol{e})$ to denote the Hamming weight of $\boldsymbol{e}$. The set of all vectors of Hamming weight at most w in $\mathbb{R}^n$ is denoted by $\mathcal{B}(n, w)$.

Let $\mathcal{C}$ be a linear $[n, k]$ code over $\mathbb{R}$. A decoder for $\mathcal{C}$ is a function $\mathcal{D} : \mathbb{R}^n \to 2^{[n]} \cup \{\text{“e”}\}$ which returns a set of locations of outlying errors or an indication “e” that errors have been detected. Given $\delta, \Delta \in \mathbb{R}^+$ and prescribed nonnegative integers τ and σ, we say that the decoder $\mathcal{D}$ corrects τ errors and detects σ additional errors with respect to the threshold pair (δ, Δ), or that $\mathcal{D}$ is a (τ, σ)-*decoder for* $(\mathcal{C}, \Delta : \delta)$, if the following conditions hold for every $\boldsymbol{y}$ as in (1), where $\boldsymbol{c} \in \mathcal{C}$, $\boldsymbol{\varepsilon} \in \mathcal{Q}(n, \delta)$, and $\boldsymbol{e} \in \mathcal{B}(n, \tau + \sigma)$.

(D1) If $\boldsymbol{e} \in \mathcal{B}(n, \tau)$ then “e” $\neq \mathcal{D}(\boldsymbol{y}) \subseteq \mathsf{Supp}_0(\boldsymbol{e})$.

(D2) If $\mathcal{D}(\boldsymbol{y}) \neq$ “e” then $\mathsf{Supp}_\Delta(\boldsymbol{e}) \subseteq \mathcal{D}(\boldsymbol{y})$.

Let $\boldsymbol{x} = (x_j)_{j\in[n]}$ be a nonzero vector in $\mathbb{R}^n$ and let π be a permutation on $[n]$ such that

$$|x_{\pi(0)}| \geqslant |x_{\pi(1)}| \geqslant \cdots \geqslant |x_{\pi(n-1)}|.$$

Given an integer $m \in [n]$, the m-*height* of $\boldsymbol{x}$, denoted by $\mathsf{h}_m(\boldsymbol{x})$, is defined as

$$\mathsf{h}_m(\boldsymbol{x}) \triangleq \left|\frac{x_{\pi(0)}}{x_{\pi(m)}}\right|,$$

and we formally define $\mathsf{h}_n(\boldsymbol{x}) \triangleq \infty$. For a linear code $\mathcal{C} \neq \{\boldsymbol{0}\}$ over $\mathbb{R}$, its m-height, denoted by $\mathsf{h}_m(\mathcal{C})$, is defined by

$$\mathsf{h}_m(\mathcal{C}) \triangleq \max_{\boldsymbol{c}\in\mathcal{C}\setminus\{\boldsymbol{0}\}} \mathsf{h}_m(\boldsymbol{c}).$$

The minimum Hamming distance of $\mathcal{C}$, denoted by $\mathsf{d}(\mathcal{C})$, can be related to $(\mathsf{h}_m(\mathcal{C}))_m$ by

$$\mathsf{d}(\mathcal{C}) = \min\{m \in [n+1] : \mathsf{h}_m(\mathcal{C}) = \infty\}. \tag{2}$$

Theorem 1 ([19],[21])**.** *Let $\mathcal{C}$ be a linear $[n, k]$ code over $\mathbb{R}$. There is a (τ, σ)-decoder for $(\mathcal{C}, \Delta : \delta)$, if and only if*

$$\Delta/\delta \geqslant 2\,\mathsf{h}_{2\tau+\sigma}(\mathcal{C}) + 2.$$

Recalling our definition of a decoder, the decoding capability studied in this paper is specified by the number of correctable or detectable outlying errors (determined by the parameters τ and σ) as well as by (the ratio between) Δ and δ. Theorem 1 then provides a necessary and sufficient condition for given τ, σ, and Δ/δ to be attainable by a linear code $\mathcal{C}$, in terms of the m-heights of $\mathcal{C}$. In particular, by Eq. (2) it

TABLE I
SUMMARY OF THE $[n, k\geqslant n-r]$ CODES $\mathcal{C}$ OVER $\mathbb{R}$

m	r	Attainable Δ/δ	Comments	Reference
2	$\Theta(\log n)$	$O\left(\frac{n}{\sqrt{r}}\right)$		Prop. 5 in [20]
$O\left(\sqrt{\frac{n}{\log n}}\right)$	$\Theta(m^2 \log n)$	$O\left(\frac{n}{\sqrt{r}}\right)$		Cor. 14
2	$r \leqslant n \leqslant r(r-1)$	$2\left\lceil\frac{2n}{r}\right\rceil$		Prop. 6 in [19]
$m \leqslant \rho$	$\frac{mn}{\rho}$	$\frac{2mn}{r}$	$\rho \in \mathbb{Z}^+$, $\rho \leqslant \sqrt{n}$, $\frac{n}{\rho}$ is a prime power	Cor. 25
$m \leqslant \min\{\rho, p_1^{e_1}, p_2^{e_2}, \ldots\}$	$\frac{mn}{\rho}$	$\frac{2mn}{r}$	$\rho \in \mathbb{Z}^+$, $\rho \leqslant \sqrt{n}$, $\frac{n}{\rho} = p_1^{e_1} p_2^{e_2} \cdots$	Thm. 27
$m \leqslant \lceil q/\ell \rceil$	$(\ell m - \ell + 1)q$	$\frac{2(\ell m - \ell + 1)n}{r}$	$\ell \in \mathbb{Z}^+$, q is a prime power, $n = q^{\ell+1}$	Cor. 16

follows that the inequality $\mathsf{d}(\mathcal{C}) > 2\tau + \sigma$ is a necessary and sufficient condition for having a (τ, σ)-decoder for $(\mathcal{C}, \Delta : \delta)$, for some (sufficiently large yet) finite ratio Δ/δ.

Theorem 1 motivated in [19] to define for every $m \in [n+1]$ the expression

$$\Gamma_m(\mathcal{C}) \triangleq 2\,\mathsf{h}_m(\mathcal{C}) + 2, \tag{3}$$

so that $\Gamma_{2\tau+\sigma}(\mathcal{C})$ is the smallest ratio Δ/δ for which there is a (τ, σ)-decoder for $(\mathcal{C}, \Delta : \delta)$. Equivalently, $\Gamma_{2\tau+\sigma}$ is the smallest Δ such that there is a (τ, σ)-decoder for $(\mathcal{C}, \Delta : 1)$. Thus, given n and m, our aim is to construct linear codes $\mathcal{C}$ over $\mathbb{R}$ with both $\Gamma_m(\mathcal{C})$ and redundancy r as small as possible.

For the case $m = 2\tau + \sigma \leqslant 2$, a characterization of $\Gamma_1(\mathcal{C})$ and $\Gamma_2(\mathcal{C})$ was presented in [19] in terms of the parity-check matrix of $\mathcal{C}$. In the next proposition, we present a generalization of that characterization to any $m \in [1 : \mathsf{d}(\mathcal{C})]$, which will be used to analyze the value of $\Gamma_m(\mathcal{C})$ for the codes proposed in Section III and Section IV. Given a parity-check matrix H of $\mathcal{C}$ over $\mathbb{R}$, let

$$\mathcal{S} = \mathcal{S}(H) \triangleq \left\{H\boldsymbol{\varepsilon}^\top : \boldsymbol{\varepsilon} \in \mathcal{Q}(n, 1)\right\} \tag{4}$$

and

$$\begin{aligned} 2\mathcal{S} \triangleq \mathcal{S} + \mathcal{S} &= \left\{H(\boldsymbol{\varepsilon} + \boldsymbol{\varepsilon}')^\top : \boldsymbol{\varepsilon}, \boldsymbol{\varepsilon}' \in \mathcal{Q}(n, 1)\right\} \\ &= \left\{H\boldsymbol{\varepsilon}^\top : \boldsymbol{\varepsilon} \in \mathcal{Q}(n, 2)\right\}. \end{aligned} \tag{5}$$

Note that $\mathcal{S}$ is the set of all the syndrome vectors (with respect to H) that can be obtained when there are no outlying errors, assuming that $\delta = 1$. Also, for $\Delta \in \mathbb{R}^+$ let

$$\mathcal{B}_\Delta(n, m) \triangleq \{\boldsymbol{e} \in \mathcal{B}(n, m) : \|\boldsymbol{e}\|_\infty > \Delta\}, \tag{6}$$

i.e., $\mathcal{B}_\Delta(n, m)$ consists of all the vectors $\boldsymbol{e} \in \mathbb{R}^n$ such that both $\mathsf{w}(\boldsymbol{e}) \leqslant m$ and $\mathsf{Supp}_\Delta(\boldsymbol{e}) \neq \varnothing$.

Proposition 2. *Given a linear $[n, k>0]$ code $\mathcal{C}$ over $\mathbb{R}$, let H be a parity-check matrix of $\mathcal{C}$ and let $m \in [1 : \mathsf{d}(\mathcal{C})]$. Then*

$$\Gamma_m(\mathcal{C}) = \min\left\{\Delta \in \mathbb{R}^+ : H\boldsymbol{e}^\top \notin 2\mathcal{S} \text{ for all } \boldsymbol{e} \in \mathcal{B}_\Delta(n, m)\right\}. \tag{7}$$

Proof: We first show that $\Delta^* \triangleq \Gamma_m(\mathcal{C})$ is contained in the minimand set in (7). Assume to the contrary that there is a vector $\boldsymbol{e} \in \mathcal{B}_{\Delta^*}(n, m)$ such that $H\boldsymbol{e}^\top \in 2\mathcal{S}$, namely, $H\boldsymbol{e}^\top = H\boldsymbol{\varepsilon}^\top$ for some $\boldsymbol{\varepsilon} \in \mathcal{Q}(n, 2)$. Then $\boldsymbol{e} - \boldsymbol{\varepsilon} \in \mathcal{C}$ and, so,

$$\mathsf{h}_m(\mathcal{C}) \geqslant \mathsf{h}_m(\boldsymbol{e} - \boldsymbol{\varepsilon}) \geqslant \frac{\|\boldsymbol{e}\|_\infty - 2}{2} > \frac{\Delta^* - 2}{2}.$$

This, in turn, implies

$$\Gamma_m(\mathcal{C}) \overset{(3)}{=} 2\,\mathsf{h}_m(\mathcal{C}) + 2 > \Delta^*,$$

which is a contradiction.

We next show that $\Gamma_m(\mathcal{C})$ is indeed the minimum of the set in (7). Assuming to the contrary that this set contains some $\Delta < \Gamma_m(\mathcal{C})$, there is a nonzero codeword $\boldsymbol{c} \in \mathcal{C}$ such that

$$\mathsf{h}_m(\boldsymbol{c}) > \frac{\Delta - 2}{2}.$$

Without loss of generality we can assume that

$$c_0 \geqslant |c_1| \geqslant |c_2| \geqslant \cdots \geqslant |c_{n-1}|,$$

where $|c_m| = 2$ and (thus) $c_0 > \Delta - 2$. Define the vectors $\boldsymbol{e}, \boldsymbol{\varepsilon} \in \mathbb{R}^n$ as follows:

$$\begin{aligned} \boldsymbol{e} &= (c_0{+}2 \;\; c_1 \;\; c_2 \;\; \ldots \;\; c_{m-1} \;\; 0 \;\; 0 \;\; \ldots \;\; 0), \\ \boldsymbol{\varepsilon} &= (-2 \;\; 0 \;\; 0 \;\; \ldots \;\; 0 \;\; c_m \;\; c_{m+1} \;\; \ldots \;\; c_{n-1}). \end{aligned}$$

Then $\boldsymbol{c} = \boldsymbol{e} + \boldsymbol{\varepsilon}$ and $\boldsymbol{\varepsilon} \in \mathcal{Q}(n, 2)$, namely, $H\boldsymbol{e}^\top = -H\boldsymbol{\varepsilon}^\top \in 2\mathcal{S}$. On the other hand $\boldsymbol{e} \in \mathcal{B}_\Delta(n, m)$, which means that Δ is *not* in the minimand in (7), thereby reaching a contradiction. ■

Propositions 9 and 8 in [19] are special cases of Proposition 2 for $m = 1$ and $m = 2$, respectively. Proposition 2 holds (vacuously) also when $m \geqslant \mathsf{d}(\mathcal{C})$: in this case the minimand in (7) is empty (since $\mathcal{C}$ contains nonzero codewords in $\mathcal{B}(n, m)$ with arbitrary infinity norms), while $\Gamma_m(\mathcal{C}) = \infty$ (from (2)).

We end this subsection by mentioning two of the constructions for $m = 2$ that were presented in [19].

Theorem 3 ([19, Proposition 6])**.** *Let H be an $r \times n$ matrix over $\{-1, 0, 1\}$ which satisfies the following three conditions:*

1) *all columns of H are distinct,*

2) *each column in H contains exactly two nonzero entries, the first of which being a* 1*, and*
3) *each row has Hamming weight $\lfloor 2n/r \rfloor$ or $\lceil 2n/r \rceil$.*

(In particular, these conditions require that $n \leqslant r(r-1)$.) The linear $[n, k \geqslant n-r]$ code $\mathcal{C}$ over $\mathbb{R}$ with a parity-check matrix H satisfies $\Gamma_2(\mathcal{C}) \leqslant 2 \cdot \lceil 2n/r \rceil$.

When r is even, the inequality $n \leqslant r(r-1)$ is also sufficient for having a matrix H that satisfies the conditions of the theorem [12].

A second construction is presented in [19] that is based on spherical codes. The construction will be recapped in Section III, and the next theorem summarizes its properties.

Theorem 4 ([20, Proposition 5])**.** *There exists a linear $[n, k=n-r]$ code $\mathcal{C}$ over $\mathbb{R}$ with $\Gamma_2(\mathcal{C}) = O(n/\sqrt{r})$, whenever $r/\log n$ is bounded away from (above)* 1*.*

B. Disjunct matrices

Let $n, r \in \mathbb{Z}^+$ and let $D \in [n]$. An $r \times n$ matrix $H = (H_{i,j})$ over $\{0, 1\}$ is called *D-disjunct* if the union of the supports of any D columns of H does not contain the support of any other column. In other words, for any column index $j \in [n]$ and a subset $\mathcal{J} \subseteq [n] \setminus \{j\}$ of D additional column indexes there is a row index $i \in [r]$ such that $H_{i,j} = 1$ while $H_{i,j'} = 0$ for all $j' \in \mathcal{J}$. (Equivalently, every $r \times (D+1)$ submatrix of H contains $D+1$ rows that form the identity matrix.)

A *(D, ρ)-disjunct* matrix is a D-disjunct matrix whose rows all have weights bounded from above by $\rho \in \mathbb{Z}^+$.

Disjunct matrices play a crucial role in the area of group testing, which studies how to identify a set of at most D positive items from a batch of n total items. The basic strategy of group testing is to group the items into several tests, i.e., some subsets of items. In each test, a positive outcome indicates that at least one of the items included in this test is positive and a negative outcome indicates that all items included are negative. A disjunct matrix H describes a nonadaptive group testing scheme: we use the tests to index the rows and use items to index the columns. Then the ith test contains the jth item if and only if $H_{i,j} = 1$. It is not very difficult to see that the D-disjunct property ensures that this testing scheme can identify all the positive items as long as their number is at most D.

The first explicit construction of disjunct matrices was proposed by Kautz and Singleton [13]. Their construction uses a Reed–Solomon (RS) outer code concatenated with binary unit vectors and requires $r = O(D^2 \log_D^2 n)$ tests, which matches the best known lower bound, $\Omega(D^2 \log_D n)$, in [7],[8] when $D = \Theta(n^\alpha)$ for some fixed $\alpha \in (0, 1)$. Subsequently, Porat and Rothschild [17] proposed another explicit construction, which is similar to the Kautz–Singleton construction but uses a code meeting the Gilbert–Varshamov (G–V) bound as the outer code. Their construction achieves $r = O(D^2 \log n)$ and outperforms the Kautz–Singleton construction in the regime where $D = O(\mathrm{poly}(\log n))$.

More recently, motivated by practical applications in group testing and wireless communication, Inan *et al.* investigated disjunct matrices with constraints on either the maximal row weight (i.e, (D, ρ)-disjunct matrices) or the maximal column weight [11]. In the context of this paper, we focus on (D, ρ)-disjunct matrices and demonstrate in Section IV that (D, ρ)-disjunct matrices can be used to construct analog error-correcting codes.

Inan *et al.* first examined the Kautz–Singleton construction and the Porat–Rothschild construction and computed the maximum row weight ρ of the corresponding disjunct matrices.

Theorem 5 ([11, Theorems 2 and 3])**.** *The Kautz–Singleton construction yields a (D, ρ)-disjunct $r \times n$ matrix with constant row weight $\rho = n/\sqrt{r}$ and*

$$r = O\left(\left(\frac{D \log n}{\log(D \log n)}\right)^2\right).$$

The Porat–Rothschild construction yields a (D, ρ)-disjunct $r \times n$ matrix where $\rho = \Omega(n/D)$ and $r = O(D^2 \log n)$.

In the Porat–Rothschild construction, the number of rows, $r = O(D^2 \log n)$, meets the lower bound $\Omega(D^2 \log_D n)$ when D is fixed. The following result shows that in a (D, ρ)-disjunct matrix with $r = O(\log n)$ rows one must have $\rho = \Theta(n)$; so, in a regime where D is fixed, both r and ρ in the Porat–Rothschild construction meet their respective lower bounds.

Lemma 6. *Let H be a (D, ρ)-disjunct $r \times n$ matrix, where $r \leqslant a \log n$ for some fixed a. Then $\rho = \Theta(n)$.*

Proof: Since H is D-disjunct, it cannot contain two identical columns and, so, $a \geqslant 1$. Let $\alpha \in (0, 1/2)$ be such that $h(\alpha) = 1/(2a)$, where $h(\cdot)$ is the binary entropy function. Then

$$\sum_{i=0}^{\lfloor \alpha r \rfloor} \binom{r}{i} \leqslant 2^{r h(\alpha)} \leqslant \sqrt{n}.$$

Hence, there are at least $n - \sqrt{n}$ columns in H each of which has weight at least αr. By counting the number of 1s in H, we get that

$$r\rho \geqslant (n - \sqrt{n})(\alpha r),$$

which implies that $\rho \geqslant (n - \sqrt{n})\alpha$. ∎

Inan *et al.* proved the following generic lower bound on the number of rows of a (D, ρ)-disjunct matrix.

Theorem 7 ([11, Theorem 8])**.** *A (D, ρ)-disjunct $r \times n$ matrix must satisfy*

$$r \geqslant \begin{cases} \dfrac{(D+1)n}{\rho}, & \text{if } \rho > D+1, \\ n, & \text{if } \rho \leqslant D+1. \end{cases}$$

They also modified the Kautz–Singleton construction by changing the dimension of the outer RS code and obtained the following result.

Theorem 8 ([11, Theorem 8])**.** *Let $\ell \in \mathbb{Z}^+$, let q be a prime power, and set*

$$n = q^{\ell+1} \quad \text{and} \quad \rho = q^\ell = n^{\ell/(\ell+1)}.$$

Also, let $D \in \mathbb{Z}^+$ be such that $\ell D + 1 \leqslant q$. The Kautz–Singleton construction yields a (D, ρ)-disjunct $r \times n$ matrix with constant row weight ρ and

$$r = (\ell D + 1) \cdot q = \frac{(\ell D + 1)n}{\rho}.$$

Substituting $\ell = 1$ in Theorem 8 yields a construction for $\rho = \sqrt{n}$ with $r = (D+1)n/\rho$, which, in view of Theorem 7, is optimal with respect to r. In Section V, for any $\rho \leqslant \sqrt{n}$ such that n/ρ is a prime power, we construct optimal (D, ρ)-disjunct matrices with number of rows $r = (D+1)n/\rho$.

We end this section with a new lower bound on the number of rows of (D, ρ)-disjunct matrices; this bound, in turn, will imply that for any (fixed) $\ell \geqslant 2$, the matrices in Theorem 8 are asymptotically optimal when $D = o\big(n^{1/(\ell(\ell+1))}\big)$. We use the following terms (as defined in the proof of Theorem 4 in [11]). In an $r \times n$ binary matrix $H = (\boldsymbol{h}_j)_{j \in [n]}$, a row $i \in [r]$ is said to be *private* for a column $j \in [n]$ if row i contains a 1 only at column j. Similarly, a *private set* for column j is defined as a subset $\mathcal{R} \subseteq \mathsf{Supp}_0(\boldsymbol{h}_j)$ such that $\mathcal{R} \not\subseteq \mathsf{Supp}_0(\boldsymbol{h}_{j'})$ for any $j' \in [n] \setminus \{j\}$.

Theorem 9. *Let $n, \ell, D, \rho \in \mathbb{Z}^+$ be such that $\rho \geqslant \ell D + 1$. Any (D, ρ)-disjunct $r \times n$ matrix must satisfy*

$$r \geqslant \frac{\ell D + 1}{\rho} \left(n - \max\left\{ \binom{r}{\ell}, \binom{2\ell}{\ell} \right\} \right).$$

In particular, if $\max\{\binom{r}{\ell}, \binom{2\ell}{\ell}\} = o(n)$, then

$$r \geqslant \frac{(\ell D + 1)n}{\rho} \cdot (1 - o(1)).$$

Proof: Let H be a (D, ρ)-disjunct $r \times n$ matrix where $\rho \geqslant \ell D + 1$. Consider the columns that have weight $\leqslant D$ and denote their number by n_1. Since H is D-disjunct, each of these columns must have a private row; hence, $n_1 \leqslant r$. Remove these columns along with the corresponding private rows and let H' be the resulting $(r - n_1) \times (n - n_1)$ matrix. Clearly, H' is (D, ρ)-disjunct and each column in H' has weight $\geqslant D + 1 \geqslant \ell$.

Next, consider the columns of H' that have weight $\leqslant \ell D$ and denote their number by n_2. Since H' is D-disjunct, each of these columns must have a private set of size at most ℓ. Note that these private sets cannot be nested. If $2\ell \leq r - n_1$, it follows from the LubellYamamotoMeshalkin inequality (see [15]) that $n_2 \leqslant \binom{r-n_1}{\ell} \leqslant \binom{r}{\ell}$; if $2\ell > r - n_1$, it follows from Sperner's theorem that $n_2 \leqslant \binom{r-n_1}{\lfloor (r-n_1)/2 \rfloor} \leqslant \binom{2\ell}{\ell}$. Hence, $n_2 \leq \max\{\binom{r}{\ell}, \binom{2\ell}{\ell}\}$. We remove these n_2 columns from H' and count the number of 1s in the resulting matrix in two ways; doing so, we get

$$(n - n_1 - n_2)(\ell D + 1) \leqslant (r - n_1)\rho,$$

which implies that

$$\begin{aligned} r\rho &\geqslant (n - n_2)(\ell D + 1) + n_1(\rho - (\ell D + 1)) \\ &\geqslant (n - n_2)(\ell D + 1) \\ &\geqslant \left(n - \max\left\{ \binom{r}{\ell}, \binom{2\ell}{\ell} \right\} \right)(\ell D + 1). \end{aligned}$$

■

Taking ℓ fixed and $D = o\big(n^{1/(\ell(\ell+1))}\big)$, we get $r^\ell = (\ell D + 1)^\ell n^{\ell/(\ell+1)} = o(n)$. Hence, for this parameter range, the construction in Theorem 8 asymptotically attains the lower bound in Theorem 9.

III. The Spherical-Code Construction: Locating Multiple Errors

When $m = 2$, the spherical code construction of [19] yields a linear $[n, n - r]$ code $\mathcal{C}$ over $\mathbb{R}$ with redundancy $r = \Theta(\log n)$ and with $\Gamma_2(\mathcal{C}) = O(n/\sqrt{r})$. In this section, we use Proposition 2 to analyze the multiple-error-correcting capability of $\mathcal{C}$. In particular, we show that for any fixed $m > 2$, we still have $\Gamma_m(\mathcal{C}) = O(n/\sqrt{r})$.

We first recap the construction. Let B be a linear $[r, \kappa, d]$ code over $\mathbb{F}_2$ which satisfies the following two properties:

(B1) B contains the all-one codeword, and—

(B2) $\mathsf{d}(B^\perp) > 2$.

Let $n = 2^{\kappa - 1}$ and let B_0 be the set of the n codewords of B whose first entry is a 0. Let $H = H(B)$ be the $r \times n$ matrix over $\mathbb{R}$ whose columns are obtained from the codewords in B_0 by replacing the 0–1 entries by $\pm 1/\sqrt{r}$. The code $\mathcal{C}(B)$ is defined as the $[n, k \geqslant n - r]$ code over $\mathbb{R}$ with the parity-check matrix H.

Remark 1. Properties (B1)–(B2) imply that B has a generator matrix with an all-one row and with columns that are all distinct. This, in turn, requires that $\kappa \geqslant 1 + \log r$. We will in fact assume that the latter inequality is strict (in order to have $r < n$), in which case $d < r/2$. ■

Remark 2. In what follows, we will also use codes B which—in addition to satisfying properties (B1)–(B2)—attain the G–V bound, i.e.,

$$\frac{\kappa}{r} \geqslant 1 - h(d/r),$$

where $h(\cdot)$ is the binary entropy function. E.g., when r is a power of 2, the construction of a generator matrix of such a code B can start with the $1 + \log r$ rows of the generator matrix of the first-order binary Reed–Muller code (thereby guaranteeing properties (B1)–(B2)), followed by iterations of adding rows that are within distance $\geqslant d$ from the linear span of the already-selected rows. (As shown in [17], this process can be carried out by a deterministic algorithm in time $O(2^\kappa r) = O(nr)$.) ■

The property of $\mathsf{d}(B^\perp) > 2$ guarantees that any two rows of H are orthogonal which, in turn, implies that

$$\|H\boldsymbol{\varepsilon}^\top\|_2 \leqslant \frac{n}{\sqrt{r}}, \quad \text{for every } \boldsymbol{\varepsilon} \in \mathcal{Q}(n, 1).$$

Equivalently,

$$\|\boldsymbol{s}\|_2 \leqslant \frac{4n^2}{r}, \quad \text{for every } \boldsymbol{s} \in 2\mathcal{S}, \tag{8}$$

where $\mathcal{S} = \mathcal{S}(H)$ and $2\mathcal{S}$ are as defined in (4)–(5). The minimum Hamming distance of B and property (B1) jointly imply that for any two distinct columns $\boldsymbol{h}_i$ and $\boldsymbol{h}_j$ in H,

$$|\boldsymbol{h}_i^\top \cdot \boldsymbol{h}_j| = \cos(\phi_{i,j}) \leqslant 1 - \frac{2d}{r}, \tag{9}$$

where $\phi_{i,j}$ is the angle between $\boldsymbol{h}_i$ and $\boldsymbol{h}_j$. Then, using geometric arguments, it is shown in [19] that

$$\Gamma_2(\mathcal{C}(B)) \leqslant \frac{n/\sqrt{r}}{\min_{i\neq j}\sin(\phi_{i,j})} \leqslant \frac{n}{\sqrt{d(1-d/r)}}.$$

As argued in [19], we can now select B to be a linear $[r,\kappa,d]$ code over $\mathbb{F}_2$ that satisfies properties (B1)–(B2) with both κ/r and d/r bounded away from 0, in which case the code $\mathcal{C}(B)$ has $r=\Theta(\log n)$ and $\Gamma_2(\mathcal{C}(B))=O(n/\sqrt{r})$.

Turning now to $m>2$, we make use of of the following concepts used in the theory of compressed sensing [2],[3],[4],[6]. Let $H=(\boldsymbol{h}_j)_{j\in[n]}$ be an $r\times n$ matrix over $\mathbb{R}$ and let $m\in[1:n{+}1]$ and $\gamma\in\mathbb{R}^+$. We say that H satisfies *the restricted isometry property (RIP)* of order m with constant γ, if for every $\boldsymbol{e}\in\mathcal{B}(n,m)$,

$$(1-\gamma)\|\boldsymbol{e}\|_2^2 \leqslant \|H\boldsymbol{e}^\top\|_2^2 \leqslant (1+\gamma)\|\boldsymbol{e}\|_2^2.$$

In what follows we concentrate on matrices whose columns are unit vectors, i.e., $\|\boldsymbol{h}_j\|_2=1$ for all $j\in[n]$. For such matrices, we define the *coherence* by

$$\mu(H)\triangleq\max_{i\neq j}|\boldsymbol{h}_i^\top\cdot\boldsymbol{h}_j|.$$

Proposition 10 ([2, Proposition 1])**.** *Let H be an $r\times n$ matrix over $\mathbb{R}$ with columns that are unit vectors and with coherence $\mu=\mu(H)$, and let $m\in\mathbb{Z}^+$ be such that $m\leqslant n$. Then H satisfies the RIP of order m with constant $(m-1)\mu$.*

Under the conditions of Proposition 10, the RIP implies that for every $\boldsymbol{e}\in\mathcal{B}(n,m)$ we have

$$\|H\boldsymbol{e}^\top\|_2^2 \geqslant (1-(m-1)\mu)\|\boldsymbol{e}\|_2^2. \tag{10}$$

Theorem 11. *Let B be a linear $[r,\kappa,d{<}r/2]$ code over $\mathbb{F}_2$ that satisfies properties (B1)–(B2). Denote*

$$\vartheta\triangleq 1-\frac{2d}{r}, \tag{11}$$

and let $m\in\mathbb{Z}^+$ be such that $m\leqslant\lceil 1/\vartheta\rceil$. Then

$$\Gamma_m(\mathcal{C}(B)) \leqslant \frac{2n}{\sqrt{r(1-(m-1)\vartheta)}}.$$

In particular, if B attains the G–V bound, then

$$\Gamma_m(\mathcal{C}(B)) \leqslant \frac{2n}{\sqrt{r-(m-1)\sqrt{2\cdot r\cdot\ln(2n)}}},$$

for every $m\in\mathbb{Z}^+$ for which the denominator under the outer square root is positive.

Proof: Let $H=H(B)$ be the $r\times n$ parity-check matrix that was used to define $\mathcal{C}(B)$ and let $\mu=\mu(H)$. Each column in H is a unit vector and, so, from (9) we get

$$\mu\leqslant 1-\frac{2d}{r}\overset{(11)}{=}\vartheta. \tag{12}$$

Let

$$\Delta\triangleq\frac{2n}{\sqrt{r(1-(m-1)\vartheta)}}, \tag{13}$$

where the condition $m\leqslant\lceil 1/\vartheta\rceil$ guarantees that $(m{-}1)\vartheta<1$. Also, let $\boldsymbol{e}$ be an arbitrary vector in $\mathcal{B}_\Delta(n,m)$ (see (6)). For such a vector,

$$\|\boldsymbol{e}\|_2\geqslant\|\boldsymbol{e}\|_\infty>\Delta \tag{14}$$

and, so,

$$\begin{aligned}\left\|H\boldsymbol{e}^\top\right\|_2^2 &\overset{(10)}{\geqslant} (1-(m-1)\mu)\|\boldsymbol{e}\|_2^2\\ &\overset{(12)+(14)}{>} (1-(m-1)\vartheta)\Delta^2\overset{(13)}{=}\frac{4n^2}{r}.\end{aligned} \tag{15}$$

It therefore follows from (8) that

$$H\boldsymbol{e}^\top\notin 2\mathcal{S},$$

and by Proposition 2 we thus conclude that $\Gamma_m(\mathcal{C}(B))\leqslant\Delta$.

If B attains the G–V bound, then

$$\frac{\kappa}{r}\geqslant 1-h(d/r)=1-h(1/2-(\vartheta/2))>\vartheta^2/c, \tag{16}$$

where $c=2\ln 2$. From $n=2^{\kappa-1}$ we then get

$$\log(2n)=\kappa>r\cdot\vartheta^2/c,$$

or

$$\vartheta<\sqrt{\frac{c\cdot\log(2n)}{r}}=\sqrt{\frac{2\cdot\ln(2n)}{r}}\,.$$

Hence, in this case,

$$\begin{aligned}\Gamma_m(\mathcal{C}(B))\leqslant\Delta &= \frac{2n}{\sqrt{r(1-(m-1)\vartheta)}}\\ &< \frac{2n}{\sqrt{r-(m-1)\sqrt{2\cdot r\cdot\ln(2n)}}}\,.\end{aligned}$$

■

The next lemma presents an alternative to the bound (10) that leads to some improvement on Theorem 11. For $\vartheta\in(0,1)$ and a positive integer $m\leqslant\lceil 1/\vartheta\rceil$, we introduce the notation

$$\eta_m(\vartheta)\triangleq\frac{1}{1/\vartheta+2-m}.$$

Remark 3. In the range $1\leqslant m\leqslant\lceil 1/\vartheta\rceil$ we have $\eta_m(\vartheta)<1$. Also, it is easy to verify by differentiation that in that range of ϑ (when m is assumed to be fixed), the mapping $\vartheta\mapsto(1+\vartheta)(1-\eta_m(\vartheta))$ is non-increasing. ■

Lemma 12. *Let H be an $r\times n$ matrix over $\mathbb{R}$ with columns that are unit vectors and with coherence $\mu=\mu(H)$, and let $m\in\mathbb{Z}^+$ be such that $m\leqslant\min\{\lceil 1/\mu\rceil,n\}$. Then for every $\boldsymbol{e}\in\mathcal{B}(n,m)$,*

$$\|H\boldsymbol{e}^\top\|_2^2\geqslant(1+\mu)(1-\eta_m(\mu))\|\boldsymbol{e}\|_\infty^2.$$

Proof: We first observe that the entries along the main diagonal of $H^\top H$ are all 1 and that the absolute value of each off-diagonal entry is at most μ. Hence,

$$\begin{aligned}\|H\boldsymbol{e}^\top\|_2^2 &= \boldsymbol{e}H^\top H\boldsymbol{e}^\top\\ &\geqslant \|\boldsymbol{e}\|_2^2-\mu\sum_{0\leqslant i\neq j<n}|e_ie_j|\\ &= (1+\mu)\|\boldsymbol{e}\|_2^2-\mu\sum_{i\in[n]}|e_i|\sum_{j\in[n]}|e_j|\\ &= (1+\mu)\|\boldsymbol{e}\|_2^2-\mu\|\boldsymbol{e}\|_1^2.\end{aligned} \tag{17}$$

We next minimize the expression (17) over $\boldsymbol{e}$ under the constraint that $\boldsymbol{e} \in \mathcal{B}(n,m)$ and $\|\boldsymbol{e}\|_\infty$ is given. Assuming without loss of generality that $e_0 = \|\boldsymbol{e}\|_\infty$ and that $e_j = 0$ for all $j \in [m:n]$, we claim that the minimum is attained when $|e_1| = |e_2| = \ldots = |e_{m-1}|$. Otherwise, if $|e_i| \neq |e_j|$ for some $1 \leqslant i < j < m$ then replacing both e_i and e_j by $(|e_i|+|e_j|)/2$ would reduce the term $\|\boldsymbol{e}\|_2^2$ while keeping $\|\boldsymbol{e}\|_1^2$ unchanged.

Substituting $|e_i| \leftarrow x$ for all $i \in [1:m]$ in (17) yields the following quadratic expression in x:

$$(1+\mu)(e_0^2 + (m-1)x^2) - \mu(e_0 + (m-1)x)^2. \tag{18}$$

The coefficient of x^2 is $(1-(m-2)\mu)(m-1)$, which is positive under our assumption $m \leqslant \lceil 1/\mu \rceil$; hence, (18) attains a global minimum at $x_{\min} = e_0 \cdot \eta_m(\mu)$. Plugging this value into (18) yields the result. ∎

The lower bound in Lemma 12 can be written more explicitly as

$$\|H\boldsymbol{e}^\top\|_2^2 \geqslant \frac{1+\mu}{1-(m-2)\mu} \cdot (1-(m-1)\mu) \cdot \|\boldsymbol{e}\|_\infty^2.$$

Comparing with (10), the bound in Lemma 12 is expressed in terms of $\|\boldsymbol{e}\|_\infty$ rather than $\|\boldsymbol{e}\|_2$, yet the multiplying constant therein is larger when $\mu > 0$ and $m > 1$.

Theorem 13. *Under the conditions of Theorem 11,*

$$\Gamma_m(\mathcal{C}(B)) \leqslant \frac{2n}{\sqrt{r \cdot (1+\vartheta)(1-\eta_m(\vartheta))}}\,.$$

Proof: Let

$$\Delta \triangleq \frac{2n}{\sqrt{r \cdot (1+\vartheta)(1-\eta_m(\vartheta))}}\,. \tag{19}$$

Referring to the proof of Theorem 11, by applying Lemma 12 we can replace (15) by

$$\begin{aligned}\left\|H\boldsymbol{e}^\top\right\|_2^2 &\geqslant (1+\mu)\,(1-\eta_m(\mu))\,\|\boldsymbol{e}\|_\infty^2 \\ &\overset{(12)+(14)+\text{Remark 3}}{>} (1+\vartheta)\,(1-\eta_m(\vartheta))\,\Delta^2 \overset{(19)}{=} \frac{4n^2}{r}.\end{aligned}$$

And as in that proof, we then conclude that $\Gamma_m(\mathcal{C}(B)) \leqslant \Delta$. ∎

When $1 < m < 1 + 1/\vartheta$, we have

$$1 - \vartheta(m-1) < (1+\vartheta)(1-\eta_m(\vartheta))$$

and so, Theorem 13 is stronger than Theorem 11. The improvement of Theorem 13 is seen best when m is close to $\lceil 1/\vartheta \rceil$.[1] For example, when $m = 1/\vartheta$, Theorem 11 yields the upper bound

$$\Gamma_m(\mathcal{C}(B)) \leqslant \sqrt{m} \cdot \frac{2n}{\sqrt{r}},$$

while from Theorem 13 we get:

$$\Gamma_m(\mathcal{C}(B)) \leqslant \sqrt{\frac{2m}{m+1}} \cdot \frac{2n}{\sqrt{r}} < \sqrt{8} \cdot \frac{n}{\sqrt{r}}. \tag{20}$$

[1]This means that given n and r, we select m to be close to the largest possible and analyze which values of $\Gamma_m(\mathcal{C}(B))$ can then be attained.

In fact, (20) is the bound we get in Theorem 11 when we reduce m (by almost half) to $1/(2\vartheta)+1$ while, for this m, Theorem 13 yields

$$\Gamma_m(\mathcal{C}(B)) \leqslant \sqrt{\frac{2m}{2m-1}} \cdot \frac{2n}{\sqrt{r}}.$$

When $m \ll 1/\vartheta$, the upper bounds in both theorems approach $2n/\sqrt{r}$.

Corollary 14. *For any $n, m \in \mathbb{Z}^+$ there exists a linear $[n, k \geqslant n-r]$ code $\mathcal{C}$ over $\mathbb{R}$ with*

$$r = 2m^2\lceil \ln(2n) \rceil$$

and

$$\Gamma_m(\mathcal{C}) < \sqrt{8} \cdot \frac{n}{\sqrt{r}} \leqslant \frac{2n}{m\sqrt{\ln(2n)}}.$$

Proof: Write $\vartheta = 1/m$ and let B be a linear $[r, \kappa, d]$ code over $\mathbb{F}_2$ that satisfies properties (B1)–(B2) with parameters

$$r = 2m^2\lceil \ln(2n) \rceil \quad \text{and} \quad d = m(m-1)\lceil \ln(2n) \rceil,$$

in which case

$$\vartheta \triangleq 1 - \frac{2d}{r} = \frac{1}{m}.$$

Indeed, by the G–V bound (16), such a code exists with dimension

$$\kappa > \frac{r \cdot \vartheta^2}{2\ln 2} \geqslant \log(2n)$$

and, so, the respective code $\mathcal{C}(B)$ has length $2^{\kappa-1} > n$ and can be shortened to form a linear $[n, k \geqslant n-r]$ code $\mathcal{C}$ over $\mathbb{R}$. Finally, since $m = 1/\vartheta$, we get from (20) that $\Gamma_m(\mathcal{C}) \leqslant \Gamma_m(\mathcal{C}(B)) < \sqrt{8} \cdot n/\sqrt{r}$. ∎

Remark 4. The last corollary is non-vacuous when $m = O\big(\sqrt{n/\log n}\big)$ (otherwise we have $r > n$). When $m = 2$, the corollary coincides with Theorem 4. ∎

Remark 5. In Corollary 14, we can make r grow more slowly with m at the expense of a faster growth with $\log n$, while keeping the same upper bound $\Gamma_m(\mathcal{C}) \leqslant \sqrt{8} \cdot n/\sqrt{r}$. Specifically, in the proof, we take B to be the dual of an extended binary BCH primitive code [16, p. 280], or as a concatenation of a RS outer code with the first-order binary Reed–Muller code. In both cases we have, for a parameter $t \in \mathbb{Z}^+$,

$$\vartheta = 1 - \frac{2d}{r} = O\left(\frac{t}{\sqrt{r}}\right) \quad \text{and} \quad \kappa = \Theta(t \log r),$$

i.e.,

$$\vartheta = O\left(\frac{\kappa}{\sqrt{r} \cdot \log r}\right).$$

Substituting $\kappa = \lceil \log(2n) \rceil$ and $\vartheta = 1/m$ then yields

$$r \log^2 r = O\left(m^2 \log^2 n\right),$$

which is non-vacuous when $m = O(\sqrt{n})$. ∎

IV. Code Construction Based on Disjunct Matrices

In this section, we study the relationship between analog error-correcting codes and disjunct matrices. Specifically, we consider linear codes over $\mathbb{R}$ with parity-check matrices that are (D,ρ)-disjunct: we first study their properties (Theorem 15) and then propose decoding algorithms for these codes.

Theorem 15. *Let H be an $(m-1,\rho)$-disjunct $r\times n$ matrix, for some $m,\rho\in[1:n+1]$, and let $\mathcal{C}$ be the linear $[n,k\geqslant n-r]$ code over $\mathbb{R}$ that has H as a parity-check matrix. Then*

$$\Gamma_m(\mathcal{C})\leqslant 2\rho.$$

Proof: We show that $\Delta=2\rho$ is contained in the minimand set in (7); the result will then follow from Proposition 2. Given any vector $\boldsymbol{e}=(e_j)_{j\in[n]}\in\mathcal{B}_\Delta(n,m)$, write $\mathcal{J}=\mathsf{Supp}_0(\boldsymbol{e})$ and let $t\in\mathcal{J}$ be a position at which $|e_t|>\Delta$. Since H is $(m-1)$-disjunct and $|\mathcal{J}|\leqslant m$, there is a row index $i\in[r]$ such that $(H_i)_{\mathcal{J}}$ contains a 1 only at position t. Therefore,

$$\left|H_i\boldsymbol{e}^\top\right|=|e_t|>\Delta=2\rho. \tag{21}$$

On the other hand, since $\mathsf{w}(H_i)\leqslant\rho$, for every $\boldsymbol{\varepsilon}\in\mathcal{Q}(n,2)$ we have $|H_i\boldsymbol{\varepsilon}^\top|\leqslant 2\rho$, namely,

$$|s_i|\leqslant 2\rho,\quad \text{for every } \boldsymbol{s}=(s_v)_{v\in[r]}\in 2\mathcal{S}. \tag{22}$$

By (21) and (22) we get that $H\boldsymbol{e}^\top\notin 2\mathcal{S}$, thus establishing that $\Delta=2\rho$ is contained in the minimand in (7). ∎

Combining Theorem 15 with Theorem 8, we obtain the following result.

Corollary 16. *Let $\ell\in\mathbb{Z}^+$, let q be a prime power, and set $n=q^{\ell+1}$. Then for any positive integer $m\leqslant\lceil q/\ell\rceil$ there is an explicit construction of a linear $[n,k\geqslant n-r]$ code $\mathcal{C}$ over $\mathbb{R}$ such that*

$$r=(\ell m-\ell+1)q$$

and

$$\Gamma_m(\mathcal{C})\leqslant 2q^\ell=\frac{2(\ell m-\ell+1)n}{r}.$$

In particular, by taking $\ell=1$, for any $m\leqslant\sqrt{n}$ one can obtain a linear code $\mathcal{C}$ with

$$r=m\sqrt{n}\quad\textit{and}\quad\Gamma_m(\mathcal{C})\leqslant 2\sqrt{n}=\frac{2mn}{r}.$$

It is worth noting that when $m=2$, the bound $\Gamma_2(\mathcal{C})\leqslant 4n/r$ coincides with the one in Theorem 3 (although r in that theorem can take multiple values, including values that are smaller than $2\sqrt{n}$). We also note that in Corollary 16, we have $r=\Theta(mn^\alpha)$ and $\Gamma_m(\mathcal{C})=O(mn/r)$, for certain (fixed) $\alpha\in(0,1/2]$ and infinitely many values of n. In Section V, we present a construction of disjunct matrices which produce codes with similar dependence of r and $\Gamma_m(\cdot)$ on n and m, yet for $\alpha\in[1/2,1)$.

Next, we compare the construction of Corollary 14 with the case $\ell=1$ in Corollary 16 (as this case yields the slowest growth of r with n). For the former we have $\Gamma_m(\mathcal{C})\leqslant\sqrt{8}\cdot n/\sqrt{r}$, while for the latter $\Gamma_m(\mathcal{C})=\sqrt{n}$, which is smaller since $r<n$. Yet the construction of Corollary 16 requires $r=m\sqrt{n}$, which can match the redundancy, $2m^2\lceil\ln(2n)\rceil$, in Corollary 14 only when

$$m=\Omega\left(\sqrt{n}/\log n\right)$$

(still, by Remark 4, this range partially overlaps with the range of m for which the codes in Corollary 14 are realizable).

Remark 6. The construction of Theorem 15, when applied with the Porat–Rothschild disjunct matrices in Theorem 5, yields $r=O(m^2\log n)$ (i.e., a similar guarantee to that in Corollary 14) yet with $\Gamma_m(\mathcal{C})=\Omega(n/m)$, which is $\Omega(\sqrt{\log n})$ times larger than the respective value in Corollary 14. ∎

In the remainder of this section, we present decoders for linear codes with parity-check matrices that are $(m-1,\rho)$-disjunct. In Subsection IV-A we present a decoder for the generic case, yet its complexity is $O(rmn^m)$, i.e., polynomial only when m is fixed. A much more efficient algorithm is presented in Subsection IV-B, yet under the additional assumption that the column weights in the parity-check matrix are also constrained.

A. Decoder for the generic disjunct construction

Our first decoder, denoted by $\overline{\mathcal{D}}$, is presented in Algorithm 1.

Algorithm 1 Decoder $\overline{\mathcal{D}}$ for codes from disjunct matrices

▷ $H=(H_{i,j})$ is an $(m-1,\rho)$-disjunct $r\times n$ matrix
▷ $\tau,\sigma\in\mathbb{Z}_{\geqslant 0}$ are such that $2\tau+\sigma=m$
Input: vector $\boldsymbol{y}\in\mathbb{R}^n$
Output: subset $\overline{\mathcal{D}}(\boldsymbol{y})\subseteq[n]$

Set $\Lambda=\{(\mathcal{T},\mathcal{J}):\varnothing\neq\mathcal{T}\subseteq\mathcal{J}\subseteq[n]\text{ and }|\mathcal{J}|\leqslant\tau+\sigma\}$
For each $(\mathcal{T},\mathcal{J})\in\Lambda$, let

$$\mathcal{R}(\mathcal{T},\mathcal{J})=\{i\in[r]:\mathsf{w}((H_i)_{\mathcal{T}})=\mathsf{w}((H_i)_{\mathcal{J}})=1\}$$

$\overline{\mathcal{D}}(\boldsymbol{y})\leftarrow\varnothing$
$\boldsymbol{s}=(s_i)_{i\in[r]}\leftarrow H\boldsymbol{y}^\top$
while $\exists(\mathcal{T},\mathcal{J})\in\Lambda$ s.t. $|s_i|>\rho$ for all $i\in\mathcal{R}(\mathcal{T},\mathcal{J})$ **do**
  $\overline{\mathcal{D}}(\boldsymbol{y})\leftarrow\overline{\mathcal{D}}(\boldsymbol{y})\cup\mathcal{T}$
  $\Lambda\leftarrow\Lambda\setminus\{(\mathcal{T},\mathcal{J})\}$
end while
return $\overline{\mathcal{D}}(\boldsymbol{y})$

Theorem 17. *Let $\mathcal{C}$ be a code as in Theorem 15. Then the mapping $\overline{\mathcal{D}}:\mathbb{R}^n\to 2^{[n]}$ that is defined by Algorithm 1 is a (τ,σ)-decoder for $(\mathcal{C},2\rho:1)$.*

Proof: Assume a received (read) vector

$$\boldsymbol{y}=\boldsymbol{c}+\boldsymbol{e}+\boldsymbol{\varepsilon},$$

where $\boldsymbol{c}\in\mathcal{C}$, $\boldsymbol{\varepsilon}\in\mathcal{Q}(n,1)$, and $\boldsymbol{e}\in\mathcal{B}(n,\tau+\sigma)$.

We first show that

$$\mathsf{Supp}_{2\rho}(\boldsymbol{e})\subseteq\overline{\mathcal{D}}(\boldsymbol{y}). \tag{23}$$

Take $\mathcal{T}=\mathsf{Supp}_{2\rho}(\boldsymbol{e})$ and $\mathcal{J}=\mathsf{Supp}_0(\boldsymbol{e})$. Then for every $i\in\mathcal{R}(\mathcal{T},\mathcal{J})$, since $\mathsf{w}((H_i)_{\mathcal{T}})=1$ and $(H_i)_{\mathcal{J}\setminus\mathcal{T}}=\mathbf{0}$, we have

$$|s_i|=|H_i\boldsymbol{e}^\top+H_i\boldsymbol{\varepsilon}^\top|\geqslant\underbrace{|H_i\boldsymbol{e}^\top|}_{>2\rho}-\underbrace{|H_i\boldsymbol{\varepsilon}^\top|}_{\leqslant\rho}>2\rho-\rho=\rho. \tag{24}$$

Hence, $(\mathcal{T},\mathcal{J})$ passes the check in the while loop and, so, the set $\mathcal{T}$ is joined into $\overline{\mathcal{D}}(\boldsymbol{y})$, thereby establishing (23).

Next, we assume that $\mathsf{w}(\boldsymbol{e}) \leqslant \tau$ and show that

$$\overline{\mathcal{D}}(\boldsymbol{y}) \subseteq \mathsf{Supp}_0(\boldsymbol{e}). \tag{25}$$

Write $\mathcal{K} = \mathsf{Supp}_0(\boldsymbol{e})$; then $|\mathcal{K}| \leqslant \tau$. Let $(\mathcal{T},\mathcal{J})$ be a pair in Λ that passes the check in the while loop, i.e., $|s_i| > \rho$ for all $i \in \mathcal{R}(\mathcal{T},\mathcal{J})$. We claim that $\mathcal{T} \subseteq \mathcal{K}$. Otherwise, take a $t \in \mathcal{T} \setminus \mathcal{K}$. Since H is $(m-1)$-disjunct and

$$|\mathcal{J} \cup \mathcal{K}| \leqslant |\mathcal{J}| + |\mathcal{K}| \leqslant (\tau+\sigma) + \tau = m,$$

there is a row index $i \in [r]$ such that $H_{i,t} = 1$ and $H_{i,j} = 0$ for all $j \in (\mathcal{J} \cup \mathcal{K}) \setminus \{t\}$. Then $\mathsf{w}((H_i)_{\mathcal{T}}) = \mathsf{w}((H_i)_{\mathcal{J}}) = 1$ and, so, $i \in \mathcal{R}(\mathcal{T},\mathcal{J})$. On the other hand, we also have $(H_i)_{\mathcal{K}} = \mathbf{0}$, from which we get

$$|s_i| = |\underbrace{H_i \boldsymbol{e}^\top}_{0} + H_i \boldsymbol{\varepsilon}^\top| \leqslant \rho.$$

Yet this means that the pair $(\mathcal{T},\mathcal{J})$ does *not* pass the check in the while loop, thereby reaching a contradiction. We conclude that when $\mathsf{w}(\boldsymbol{e}) \leqslant \tau$, any set $\mathcal{T}$ that is joined into $\overline{\mathcal{D}}(\boldsymbol{y})$ in the while loop is a subset of $\mathcal{K} = \mathsf{Supp}_0(\boldsymbol{e})$, thus establishing (25).

Eqs. (23) and (25), in turn, imply that the function $\overline{\mathcal{D}}$ in Algorithm 1 satisfies conditions (D2) and (D1), respectively, in the definition of a (τ,σ)-decoder for $(\mathcal{C}, 2\rho : 1)$. ∎

We note that

$$|\Lambda| = \sum_{j=1}^{\tau+\sigma} \binom{n}{j} (2^j - 1) = O(n^{\tau+\sigma}) = O(n^m).$$

Given a pair $(\mathcal{T},\mathcal{J}) \in \Lambda$, checking the conditions in the while loop of Algorithm 1 can be done in $O(rm)$ time.

B. Decoder when columns in H are also weight-constrained

Let $\mathcal{C}$ be a code as in Theorem 15 and w be a positive integer. We next present a more efficient (τ,σ)-decoder for $(\mathcal{C}, 2\rho : 1)$ under the following two additional conditions on H:

(H1) Every row of H has weight at least 2.

(H2) Every column of H has weight at most w.

Condition (H1) is not really limiting: the case where H contains rows of weight 1 is degenerate, as then there are positions on which all the codewords in $\mathcal{C}$ are identically 0 (and, thus, these coordinates can be ignored, thereby reducing the decoding to a shorter code). In Section V, we present constructions of (D,ρ)-disjunct matrices that satisfy conditions (H1)–(H2).

We will use the following lemma.

Lemma 18. *Let H be an $(m-1)$-disjunct $r \times n$ matrix that satisfies condition (H1). Given any nonempty subset $\mathcal{J} \subseteq [n]$ of size $|\mathcal{J}| \leqslant m$, for every column index $j \in \mathcal{J}$ there exist at least $m + 1 - |\mathcal{J}|$ nonzero rows in the submatrix $(H)_{\mathcal{J}}$ that contain a 1 only at column j.*

Proof: The proof is by backward induction on $|\mathcal{J}|$, with the induction base, $|\mathcal{J}| = m$, following from the definition of a $(m-1)$-disjunct matrix.

Turning to the induction step, suppose that $0 < |\mathcal{J}| \leqslant m-1$ and let j be any column index in $\mathcal{J}$. By the disjunct property, there exists a row index $i \in [r]$ such that $(H_i)_{\mathcal{J}}$ contains a 1 only at position j. By condition (H1), there is at least one index $j' \in [n] \setminus \mathcal{J}$ for which $H_{i,j'} = 1$. Letting $\mathcal{J}' = \mathcal{J} \cup \{j'\}$, by the induction hypothesis there are at least $m + 1 - |\mathcal{J}'| = m - |\mathcal{J}|$ nonzero rows in $(H)_{\mathcal{J}'}$ that contain a 1 only at column j; clearly, none of these rows is indexed by i since $(H_i)_{\mathcal{J}'}$ contains two 1s. Altogether there are at least $m+1-|\mathcal{J}|$ nonzero rows in $(H)_{\mathcal{J}}$ that contain a 1 only at column j. ∎

Remark 7. Applying Lemma 18 with $|\mathcal{J}| = 1$ implies that the weight of every column in H must be at least m (recall that we have used this fact in the proof of Theorem 9). Hence, $(m-1)$-disjunct matrices can satisfy conditions (H1) and (H2) only when $w \geqslant m$. ∎

Given $\rho \in \mathbb{R}^+$ and a vector $\boldsymbol{s} = (s_i)_{i\in[r]} \in \mathbb{R}^r$ (such as a syndrome that is computed with respect to H), we let $\boldsymbol{\chi}_\rho(\boldsymbol{s})$ be the real row vector $(\chi_i)_{i\in[r]} \in \{0,1\}^r$ whose entries are given by

$$\chi_i = \begin{cases} 0, & \text{if } |s_i| \leqslant \rho, \\ 1, & \text{otherwise.} \end{cases}$$

Theorem 19. *Let $\mathcal{C}$ be a code as in Theorem 15 and suppose that H also satisfies conditions (H1)–(H2). For nonnegative integers τ and σ such that*

$$2\tau + \sigma \leqslant 2m - w \ (\leqslant m), \tag{26}$$

let $\widetilde{\mathcal{D}} : \mathbb{R}^n \to 2^{[n]}$ be defined for every $\boldsymbol{y} \in \mathbb{R}^n$ by

$$\widetilde{\mathcal{D}}(\boldsymbol{y}) \triangleq \mathsf{Supp}_{m-\tau-\sigma}\left(\boldsymbol{\chi}_\rho(\boldsymbol{s})H\right), \tag{27}$$

where $\boldsymbol{s} = H\boldsymbol{y}^\top$. Then $\widetilde{\mathcal{D}}$ is a (τ,σ)-decoder for $(\mathcal{C}, 2\rho : 1)$.

Proof: Assume a received (read) vector

$$\boldsymbol{y} = \boldsymbol{c} + \boldsymbol{e} + \boldsymbol{\varepsilon},$$

where $\boldsymbol{c} \in \mathcal{C}$, $\boldsymbol{\varepsilon} \in \mathcal{Q}(n,1)$, and $\boldsymbol{e} \in \mathcal{B}(n,\tau+\sigma)$.

We first show that

$$\mathsf{Supp}_{2\rho}(\boldsymbol{e}) \subseteq \widetilde{\mathcal{D}}(\boldsymbol{y}). \tag{28}$$

Take $\mathcal{J} = \mathsf{Supp}_0(\boldsymbol{e})$ and let $j \in \mathsf{Supp}_{2\rho}(\boldsymbol{e})$ $(\subseteq \mathcal{J})$. By Lemma 18 we get that the submatrix $(H)_{\mathcal{J}}$ contains at least

$$m + 1 - |\mathcal{J}| \geqslant m + 1 - \tau - \sigma \tag{29}$$

rows with a 1 only at column j. Denoting by $\mathcal{R}$ the set of indexes of these rows, for every $i \in \mathcal{R}$, the respective entry s_i in the syndrome $\boldsymbol{s}$ satisfies:

$$|s_i| = |H_i\boldsymbol{e}^\top + H_i\boldsymbol{\varepsilon}^\top| \geqslant |H_i\boldsymbol{e}^\top| - |H_i\boldsymbol{\varepsilon}^\top| > \rho$$

(similarly to (24)). It follows that the respective entry, χ_i, in $\boldsymbol{\chi}_\rho(\boldsymbol{s})$ equals 1 and, so, the supports of $\boldsymbol{\chi}_\rho(\boldsymbol{s})$ and the column $\boldsymbol{h}_j$ in H overlap on at least $|\mathcal{R}|$ positions. Hence,

$$\boldsymbol{\chi}_\rho(\boldsymbol{s}) \cdot \boldsymbol{h}_j \geqslant |\mathcal{R}| \overset{(29)}{\geqslant} m + 1 - \tau - \sigma,$$

i.e., $j \in \mathsf{Supp}_{m-\tau-\sigma}\left(\boldsymbol{\chi}_\rho(\boldsymbol{s})H\right) \triangleq \widetilde{\mathcal{D}}(\boldsymbol{y})$. We conclude that

$$j \in \mathsf{Supp}_{2\rho}(\boldsymbol{e}) \implies j \in \widetilde{\mathcal{D}}(\boldsymbol{y}),$$

thereby establishing (28).

Next, we assume that $\mathsf{w}(\boldsymbol{e}) \leqslant \tau$ and show that

$$\widetilde{\mathcal{D}}(\boldsymbol{y}) \subseteq \mathsf{Supp}_0(\boldsymbol{e}). \tag{30}$$

Write $\mathcal{K} = \mathsf{Supp}_0(\boldsymbol{e})$ and let $j \in [n] \setminus \mathcal{K}$. Lemma 18, now applied with $\mathcal{J} = \mathcal{K} \cup \{j\}$, implies that the submatrix $(H)_{\mathcal{J}}$ contains at least

$$m + 1 - |\mathcal{J}| \geqslant m - \tau \tag{31}$$

rows with a 1 only at column j. Letting $\mathcal{R}$ be the set of indexes of these rows, for every $i \in \mathcal{R}$ we then have $(H_i)_{\mathcal{K}} = \mathbf{0}$ and, so, the respective entry in the syndrome $\boldsymbol{s}$ satisfies:

$$|s_i| = |\underbrace{H_i \boldsymbol{e}^\top}_{0} + H_i \boldsymbol{\varepsilon}^\top| \leqslant \rho,$$

namely, $\chi_i = 0$. Hence, the number of positions on which the supports of $\boldsymbol{\chi}_\rho(\boldsymbol{s})$ and $\boldsymbol{h}_j$ overlap is at most

$$\mathsf{w}(\boldsymbol{h}_j) - |\mathcal{R}| \overset{\text{(H2)+(31)}}{\leqslant} w - (m - \tau) \overset{(26)}{\leqslant} m - \tau - \sigma$$

and, so,

$$(0 \leqslant)\ \boldsymbol{\chi}_\rho(\boldsymbol{s}) \cdot \boldsymbol{h}_j \leqslant m - \tau - \sigma,$$

i.e., $j \notin \mathsf{Supp}_{m-\tau-\sigma}\left(\boldsymbol{\chi}_\rho(\boldsymbol{s}) H\right) \triangleq \widetilde{\mathcal{D}}(\boldsymbol{y})$. We conclude that when $\mathsf{w}(\boldsymbol{e}) \leqslant \tau$,

$$j \notin \mathsf{Supp}_0(\boldsymbol{e}) \implies j \notin \widetilde{\mathcal{D}}(\boldsymbol{y}),$$

thereby establishing (30).

Eqs. (28) and (30), in turn, imply that the function $\boldsymbol{y} \mapsto \widetilde{\mathcal{D}}(\boldsymbol{y})$ defined in (27) is a (τ, σ)-decoder for $(\mathcal{C}, 2\rho : 1)$. ∎

The decoder (27) is easy to compute: it consists of a multiplication of H to the right by $\boldsymbol{y}$ to obtain the syndrome $\boldsymbol{s}$, and then to the left by a binary vector which is a quantized copy of $\boldsymbol{s}$. Since H is a 0–1 matrix whose rows and columns have limited weights (at most ρ and w, respectively), the decoding requires less than $2\min\{r\rho, wn\}$ real additions.

We note that the condition (26) (which was used in our analysis), is generally stricter than the condition $2\tau + \sigma \leqslant m$ which, by Theorems 15 and 17, is sufficient for having a (τ, σ)-decoder for $(\mathcal{C}, 2\rho : 1)$. These two conditions coincide when $w = m$, and this case is characterized in the next lemma.

Lemma 20. *Let $H = (\boldsymbol{h}_j)_{j \in [n]}$ be an $(m-1)$-disjunct $r \times n$ matrix that satisfies conditions (H1)–(H2) with $w = m$. Then the following holds.*

- M1) *Every column of H has weight (exactly) m.*
- M2) *The supports of every two distinct columns of H intersect on at most one coordinate.*

Equivalently, for every $j \neq j'$ in $[n]$:

$$\|\boldsymbol{h}_j\|_2 = \sqrt{m} \quad \textit{and} \quad |\boldsymbol{h}_j^\top \cdot \boldsymbol{h}_{j'}| \leqslant 1$$

(and, thus, the columns of H constitute a spherical code).

Proof: Condition (M1) follows from Lemma 18 when applied with $|\mathcal{J}| = 1$ (see Remark 7), and condition (M2) follows from applying the lemma with $|\mathcal{J}| = 2$. ∎

We end this section by presenting a simple decoder for the detection-only case, i.e., $\tau = 0$. In this case, we actually do not need conditions (H1)–(H2), and we can handle any $\sigma \leqslant m$.

Theorem 21. *Let $\mathcal{C}$ be a code as in Theorem 15 and let $\widehat{\mathcal{D}} : \mathbb{R}^n \to \{\varnothing, \text{“e”}\}$ be defined by*

$$\widehat{\mathcal{D}}(\boldsymbol{y}) = \begin{cases} \varnothing, & \textit{if } \boldsymbol{\chi}_\rho(\boldsymbol{s}) = \mathbf{0}, \\ \text{“e”}, & \textit{otherwise}, \end{cases}$$

where $\boldsymbol{s} = H\boldsymbol{y}^\top$. Then $\widehat{\mathcal{D}}$ is a $(0, m)$-decoder for $(\mathcal{C}, 2\rho : 1)$.

Proof: Condition (D1) pertains only to the error vector $\boldsymbol{e} = \mathbf{0}$, in which case

$$\|\boldsymbol{s}\|_\infty = \|\underbrace{H\boldsymbol{e}^\top}_{\mathbf{0}} + H\boldsymbol{\varepsilon}^\top\|_\infty \leqslant \rho.$$

Consequently, $\boldsymbol{\chi}_\rho(\boldsymbol{s}) = \mathbf{0}$ and we have $\widehat{\mathcal{D}}(\boldsymbol{y}) = \varnothing$, as required.

As for condition (D2), we have $\widehat{\mathcal{D}}(\boldsymbol{y}) \neq$ “e” only when $\boldsymbol{\chi}_\rho(\boldsymbol{s}) = \mathbf{0}$. Now, in the proof of Theorem 19, we have established (28) without using conditions (H1)–(H2); hence, we can apply (28) to conclude that

$$\mathsf{Supp}_{2\rho}(\boldsymbol{e}) \subseteq \mathsf{Supp}_{m-\tau-\sigma}\left(\boldsymbol{\chi}_\rho(\boldsymbol{s}) H\right) \big|_{\tau=0, \sigma=m} = \varnothing = \widehat{\mathcal{D}}(\boldsymbol{y}),$$

as required. ∎

V. Constructions of Disjunct Matrices with Weight-Constrained Rows and Columns

In this section, we present several constructions for (D, ρ) disjunct matrices which satisfy conditions (H1)–(H2) with $w = D + 1$. Our constructions are based on combinatorial designs. We start by recalling several definitions.

Let $t, r, s \in \mathbb{Z}^+$ be such that $r \geqslant s \geqslant t$. A t-$(r, s, 1)$ *packing design* is a pair $(X, \mathfrak{B})$, where X is a set of r elements (called *points*) and $\mathfrak{B}$ is a collection of s-subsets (called *blocks*) of X, such that every t-subset of X is contained in at most one block. Furthermore, a packing design is called *resolvable* if its blocks can be partitioned into sets (*parallel classes*) $\mathcal{P}_0, \mathcal{P}_1, \ldots, \mathcal{P}_{\rho-1}$ such that each point is contained in exactly one block in each $\mathcal{P}_i$.

The *incidence matrix* of packing design $(X, \mathfrak{B})$ is an $|X| \times |\mathfrak{B}|$ binary matrix $H = (H_{x,\beta})$ whose rows and columns are indexed by the elements of X and $\mathfrak{B}$, respectively, and for each $x \in X$ and $\beta \in \mathfrak{B}$,

$$H_{x,\beta} = \begin{cases} 1, & \text{if } x \in \beta, \\ 0, & \text{if } x \notin \beta. \end{cases}$$

Proposition 22. *Let $(X, \mathfrak{B})$ be a resolvable t-$(r, s, 1)$ packing design with ρ parallel classes. Then its incidence matrix H is a D-disjunct matrix with constant row weight ρ, where $D = \lfloor (s-1)/(t-1) \rfloor$.*

Proof: Write $H = (\boldsymbol{h}_\beta)_{\beta \in \mathfrak{B}}$ and let $\beta_0, \beta_1, \ldots, \beta_D$ be arbitrary $D + 1$ blocks in $\mathfrak{B}$. Since $(X, \mathfrak{B})$ is a t-$(r, s, 1)$ packing design, every two blocks of $\mathfrak{B}$ have at most $t - 1$ common points. Then $|\beta_0 \cap \beta_j| \leqslant t - 1$ for all $1 \leqslant j \leqslant D$ and, so,

$$\left|\beta_0 \cap \left(\cup_{j=1}^D \beta_j\right)\right| \leqslant \sum_{j=1}^D |\beta_0 \cap \beta_j| \leqslant D(t-1) < s = |\beta_0|,$$

where the third inequality follows from $D = \lfloor (s-1)/(t-1) \rfloor$. It follows that

$$\beta_0 \setminus \left(\cup_{j=1}^D \beta_j\right) \neq \varnothing,$$

namely, there is a point $x \in X$ such that $H_{x,\beta_0} = 1$ whereas $H_{x,\beta_j} = 0$ for all $1 \leqslant j \leqslant D$. Hence, H is D-disjunct.

Next, we consider the row weight, $\mathsf{w}(H_x)$, where x is any point in X: this weight equals the number of blocks in $\mathfrak{B}$ which contain x. Since x is contained in exactly one block in each parallel class and there are in total ρ parallel classes, we get $\mathsf{w}(H_x) = \rho$. ∎

A *transversal design* $\mathrm{TD}(s, g)$ is a triple $(X, \mathfrak{G}, \mathfrak{B})$, where X is a set of sg points, $\mathfrak{G}$ is a partition of X into s partition elements (*groups*), each of size g, and $\mathfrak{B}$ is a collection of s-subsets (*blocks*) of X such that every 2-subset of X is contained either in one group or in one block, but not both. A $\mathrm{TD}(s, g)$ is called *resolvable* if its blocks can be partitioned into parallel classes.

It is easy to see that in a $\mathrm{TD}(s, g)$, each block intersects with each group at exactly one point. A direct calculation shows that there are g^2 blocks and each point is contained in g blocks. So, if it is resolvable, then the blocks should be partitioned into g parallel classes.

It is known that the existence of a resolvable $\mathrm{TD}(s, g)$ is equivalent to the existence of $s - 1$ mutually orthogonal latin squares of side g, while the latter can be constructed by using linear polynomials (e.g., see Theorem 3.18 and Construction 3.29 in [5, Section III.3]). In the following example, we use linear polynomials to construct resolvable TDs directly.

Example 1. Let q be a prime power. We can construct a resolvable $\mathrm{TD}(q, q)$ as follows. Take $X = \mathbb{F}_q \times \mathbb{F}_q$, $\mathfrak{G} = \{\{y\} \times \mathbb{F}_q\}_{y \in \mathbb{F}_q}$, and $\mathfrak{B} = \{\beta_{a,b}\}_{(a,b) \in \mathbb{F}_q \times \mathbb{F}_q}$, where

$$\beta_{a,b} = \{(y, ay + b) \,:\, y \in \mathbb{F}_q\}.$$

For each $a \in \mathbb{F}_q$, let $\mathcal{P}_a = \{\beta_{a,b}\}_{b \in \mathbb{F}_q}$; clearly, $\{\mathcal{P}_a\}_{a \in \mathbb{F}_q}$ is a partition of $\mathfrak{B}$.

Each block $\beta_{a,b}$ has size q, which equals the number of groups, and every 2-subset of the form $\{(y, z), (y, z')\}$ (which is contained in one group) cannot be contained in any block. For a 2-subset $\{(y, z), (y', z')\}$ with $y \neq y'$, the system of equations

$$\begin{cases} ay + b = z \\ ay' + b = z' \end{cases}$$

has a unique solution for (a, b); hence, there is a unique block in $\mathfrak{B}$ which contains that 2-subset. Therefore, $(X, \mathfrak{G}, \mathfrak{B})$ is a transversal design. Moreover, for each $a \in \mathbb{F}_q$ and each point $(y, z) \in X$, there is a unique $b \in \mathbb{F}_q$ such that $ay + b = z$. Hence, each $\mathcal{P}_a$ is a parallel class. ∎

Lemma 23. *If there is a resolvable* $\mathrm{TD}(s, g)$*, then for every* $2 \leqslant s' \leqslant s$ *and* $1 \leqslant g' \leqslant g$*, there is a* $2\text{-}(s'g, s', 1)$ *packing design with* g' *parallel classes.*

Proof: From a resolvable $\mathrm{TD}(s, g)$ we can form a resolvable $\mathrm{TD}(s', g)$ by deleting $s - s'$ groups. This resolvable design consists of g parallel classes. We can take g' of them to form a $2\text{-}(s'g, s', 1)$ packing design. ∎

Theorem 24. *Let* $n, \rho, D \in \mathbb{Z}^+$ *be such that* n/ρ *is a prime power and* $D+1 \leqslant \rho \leqslant \sqrt{n}$*. There is an explicit construction of a* (D, ρ)*-disjunct* $r \times n$ *matrix with constant row weight* ρ*, constant column weight* $D+1$*, and (therefore) number of rows*

$$r = \frac{(D+1)n}{\rho},$$

thereby attaining the bound in Theorem 7.

Proof: Since n/ρ is a prime power, we can take a resolvable $\mathrm{TD}(n/\rho, n/\rho)$ from Example 1. Then, according to Lemma 23, for any D, ρ such that $D + 1 \leqslant \rho \leqslant n/\rho$, we can construct a $2\text{-}((D+1)n/\rho, D+1, 1)$ packing with ρ parallel classes. Since each parallel class consists of n/ρ blocks, the total number of blocks is n. So, the incidence matrix H of this packing is of order $r \times n$, where $r = (D+1)n/\rho$, and constant row weight ρ. Moreover, according to Proposition 22, H is D-disjunct. ∎

Combining Theorem 24 with Theorem 15 yields the following result.

Corollary 25. *Let* $n, \rho, m \in \mathbb{Z}^+$ *be such that* n/ρ *is a prime power and* $m \leqslant \rho \leqslant \sqrt{n}$*. There is an explicit construction of a linear* $[n, k \geqslant n-r]$ *code* $\mathcal{C}$ *over* $\mathbb{R}$ *with*

$$r = \frac{mn}{\rho} \quad \textit{and} \quad \Gamma_m(\mathcal{C}) \leqslant 2\rho = \frac{2mn}{r}.$$

We note that the $\mathrm{TD}(q, q)$ in Example 1 is equivalent to a $[q, 2]$ (extended) RS code over $\mathbb{F}_q$: each block $\beta_{a,b}$ in the TD corresponds to a codeword whose positions are indexed by the elements of $y \in \mathbb{F}_q$. An element (y, z) contained in the block indicates that in the corresponding codeword there should be a symbol z at the position which is indexed by y.

In the Kautz–Singleton construction, the columns of the disjunct matrix are the codewords of the binary code that is obtained by concatenating a RS outer code over $\mathbb{F}_q$ with the binary code which consists of the words in $\{0, 1\}^q$ of Hamming weight 1. In light of this, it is not difficult to see that the incidence matrix of the TD in Example 1 is actually the disjunct matrix from the Kautz–Singleton construction with an RS outer code of dimension 2. Hence, the disjunct matrices in Theorem 24 can also be obtained by carefully choosing the columns of the Kautz–Singleton disjunct matrix which correspond to the selected parallel classes.

We have the following product construction of TD's, which yields more disjunct matrices. The proof of this construction is straightforward and is therefore omitted.

Proposition 26. *Let* $(X, \mathfrak{G}, \mathfrak{B})$ *be a resolvable* $\mathrm{TD}(s, g)$ *with a group partition* $\mathfrak{G} = \{\gamma_i\}_{i \in [s]}$ *and with parallel classes* $\mathcal{P}_j$*,* $j \in [g]$*, and let* $(X', \mathfrak{G}', \mathfrak{B}')$ *be a resolvable* $\mathrm{TD}(s, g')$ *with a group partition* $\mathfrak{G}' = \{\gamma'_i\}_{i \in [s]}$ *and with parallel classes* $\mathcal{P}'_j$*,* $j \in [g']$*. For any two blocks* $\beta \in \mathfrak{B}$ *and* $\beta' \in \mathfrak{B}'$*, denote*

$$\beta \otimes \beta' \triangleq \{(x_i, x'_i) \,:\, i \in [s]\},$$

where x_i *(respectively,* x'_i*) is the unique element in* $\beta \cap \gamma_i$ *(respectively,* $\beta' \cap \gamma'_i$*),* $i \in [s]$*. Then the set of points*

$$\bigcup_{i \in [s]} (\gamma_i \times \gamma'_i),$$

the group partition $\{\gamma_i \times \gamma'_i \,:\, i \in [s]\}$*, and the set of blocks*

$$\{\beta \otimes \beta' \,:\, (\beta, \beta') \in \mathfrak{B} \times \mathfrak{B}'\},$$

form a resolvable $\mathrm{TD}(s, gg')$ *with* gg' *parallel classes*

$$\mathcal{P}_{j,j} \triangleq \{\beta \otimes \beta' : (\beta, \beta') \in \mathcal{P}_j \times \mathcal{P}'_{j'}\}, \quad j, j' \in [g] \times [g'].$$

Theorem 27. *Let* n, ρ *be positive integers such that* $\rho \leqslant \sqrt{n}$ *and* ρ *divides* n*, and let* $p_1^{e_1} p_2^{e_2} \cdots$ *be the prime factorization of* n/ρ*. Let* $p^e = \min_i\{p_i^{e_i}\}$*.*

(i) For any positive integer $D < \min\{p^e, \rho\}$*, there is an explicit construction of a* D*-disjunct* $r \times n$ *matrix with constant row weight* ρ *and constant column weight* $D+1$*, where* $r = (D+1)n/\rho$ *(thereby attaining the bound of Theorem 7).*

(ii) For any positive integer m *such that* $m \leqslant \min\{p^e, \rho\}$*, there is a linear* $[n, k \geqslant n-r]$ *code* $\mathcal{C}$ *over* $\mathbb{R}$ *with*

$$r = \frac{mn}{\rho} \quad \textit{and} \quad \Gamma_m(\mathcal{C}) \leqslant 2\rho = \frac{2mn}{r}.$$

Proof: Since $p^e = \min_i\{p_i^{e_i}\}$, there is a resolvable $\mathrm{TD}(p^e, p_i^{e_i})$ for each i. Using the product construction recursively, we obtain a resolvable $\mathrm{TD}(p^e, n/\rho)$. Then, according to Lemma 23, for any D, ρ such that $D < \min\{\rho, p^e\}$ and $\rho \leqslant n/\rho$, we can construct a 2-$((D+1)n/\rho, D+1, 1)$ packing with ρ parallel classes. Parts (i) and (ii) then follow from Proposition 22 and Theorem 15, respectively. ∎

REFERENCES

[1] B. E. Boser, E. Sackinger, J. Bromley, Y. L. Cun, and L. D. Jackel, "An analog neural network processor with programmable topology," *IEEE J. Solid-State Circuits*, vol. 26, no. 12, pp. 2017–2025, Dec. 1991.

[2] J. Bourgain, S. J. Dilworth, K. Ford, S. Konyagin, and D. Kutzarova, "Explicit constructions of RIP matrices and related problems," *Duke Math. J.*, vol. 159, no. 1, pp. 145–185, 2011.

[3] E. Candès, "The restricted isometry property and its implications for compressed sensing," *C.R. Acad. Sci. Paris, Ser. I*, vol. 346, pp. 589–592, 2008.

[4] E. Candès, J. Romberg, and T. Tao, "Robust uncertainty principles: Exact signal reconstruction from highly incomplete frequency information," *IEEE Trans. Inf. Theory*, vol. 52, no. 2, pp. 489–509, Feb. 2006.

[5] C. Colbourn and J. Dinitz, *Handbook of combinatorial designs, second edition*. CRC press Boca Raton, FL, 2007.

[6] D. Donoho, "Compressed sensing," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1289–1306, Apr. 2006.

[7] A. G. D'yachkov and V. V. Rykov, "Bounds on the length of disjunctive codes," *Probl. Peredachi Inf.*, vol. 18, no. 3, pp. 7–13, 1982.

[8] Z. Füredi, "On r-cover-free families," *J. Combin. Theory Ser. A*, vol. 73, no. 1, pp. 172–173, 1996.

[9] M. Hu, C. E. Graves, C. Li, Y. Li, N. Ge, E. Montgomery, N. Davila, H. Jiang, R. S. Williams, J. J. Yang, Q. Xia, and J. P. Strachan, "Memristor-based analog computation and neural network classification with a dot product engine," in *Adv. Mater.*, vol. 30, Mar. 2018, paper no. 1705914.

[10] M. Hu, J. P. Strachan, Z. Li, E. M. Grafals, N. Davila, C. Graves, S. Lam, N. Ge, J. Yang, and R. S. Williams, "Dot-product engine for neuromorphic computing: Programming 1T1M crossbar to accelerate matrix-vector multiplication," in *Proc. 53rd ACM/EDAC/IEEE Design Automat. Conf. (DAC)*, Austin, TX, 2016, paper no. 19.

[11] H. A. Inan, P. Kairouz, and A. Özgür, "Sparse combinatorial group testing," *IEEE Trans. Inf. Theory*, vol. 66, no. 5, pp. 2729–2742, May 2020.

[12] G. Katona and A. Seress, "Greedy construction of nearly regular graphs," *European J. of Combin.*, vol. 14, pp. 213–229, 1993.

[13] W. Kautz and R. Singleton, "Nonrandom binary superimposed codes," *IEEE Trans. Inf. Theory*, vol. 10, no. 4, pp. 363–377, Oct. 1964.

[14] F. J. Kub, K. K. Moon, I. A. Mack, and F. M. Long, "Programmable analog vector-matrix multipliers," *IEEE J. Solid-State Circuits*, vol. 25, no. 1, pp. 207–214, Feb. 1990.

[15] D. Lubell, "A short proof of Sperner's lemma," *J. Combin. Theory Ser. A*, vol. 1, no. 2, p. 299, 1966.

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

[17] E. Porat and A. Rothschild, "Explicit non-adaptive combinatorial group testing schemes," *IEEE Trans. Inf. Theory*, vol. 57, no. 12, pp. 7982–7989, Dec. 2011.

[18] R. M. Roth, "Fault-tolerant dot-product engines," *IEEE Trans. Inf. Theory*, vol. 65, no. 4, pp. 2046–2057, Apr. 2019.

[19] ——, "Analog error-correcting codes," *IEEE Trans. Inf. Theory*, vol. 66, no. 7, pp. 4075–4088, Jul. 2020.

[20] ——, "Fault-tolerant neuromorphic computing on nanoscale crossbar architectures," in *Proc. 2020 IEEE Inf. Theory Workshop (ITW)*, Mumbai, India, 2022, pp. 202–207.

[21] ——, "Correction to "analog error-correcting codes"," *IEEE Trans. Inf. Theory*, vol. 69, no. 6, pp. 3793–3794, Jan. 2023.

[22] A. Shafiee, A. Nag, N. Muralimanohar, R. Balasubramonian, J. P. Strachan, M. Hu, R. S. Williams, and V. Srikumar, "ISAAC: A convolutional neural network accelerator with in-situ analog arithmetic in crossbars," in *Proc. ACM/IEEE 43rd Annu. Int. Symp. Comput. Archit. (ISCA)*, Seoul, Korea, Jun. 2016, pp. 14–26.