Error-correcting group testing matrices

1 Error-correcting separable and disjunct matrices

In many practical applications such as drug and DNA library screening [10–12, 15], the group tests are not perfect. Positive outomes may not turn out positive and vice versa. To model the situation, we introduce two new parameters: e_0 is the maximum number of 0-to-1 errors (false positives) in test outcomes, and e_1 is the maximum number of 1-to-0 errors (false negatives).

1.1 Error-correcting separable matrices

A binary matrix $\mathbf{M}$ is said to be (d, e_0, e_1)-*separable* iff from the test outcome vector $\mathbf{y}$ which can contain up to e_0 false positives and e_1 false negatives we are still able to unambiguously identify the (true) positive items. Note that we always assume there are at most d unknown positive items/columns. Since such matrices can correct errors we also call them *error-correcting* separable matrices.

The above definition is not very useful because it does not give us an obvious way to characterize an error-correcting separable matrix. When there was no error, the definition was: the unions of $\leq d$ columns are all distinct. What is the analog in this case? For any set $S \subset [N]$ of at most d columns, let $\mathbf{M}[S]$ denote the error-free outcome vector if the positives were S, i.e. $\mathbf{M}[S] = \bigcup_{j \in S} \mathbf{M}^j$. Recall that $\mathbf{M}^j$ denotes the jth column of the matrix $\mathbf{M}$. When S is the set of positives, the outcome vector $\mathbf{y}$ might be different from $\mathbf{M}[S]$. However if there were at most e_0 false positives and e_1 false negatives then $\mathbf{y}$ can only be (e_0, e_1)-*close* to $\mathbf{M}[S]$ which means we should be able to obtain $\mathbf{y}$ from $\mathbf{M}[S]$ by flipping at most e_0 bits of $\mathbf{M}[S]$ from 0 to 1 and at most e_1 bits from 1 to 0. In an error-correcting separable matrix, we want to be able to recover S from $\mathbf{y}$ no matter how such errors appeared. This observation leads to the following "official" definintion of error-correcting separable matrices.

Definition 1.1 (Error-correcting separable matrix)**.** A binary $t \times N$ matrix $\mathbf{M}$ is (d, e_0, e_1)-separable if for every vector $\mathbf{y} \in \{0,1\}^t$ there corresponds a subset $R_{\mathbf{y}} \subseteq [N]$ satisfying the following property. Let S be any subset of at most d columns. If $\mathbf{y}$ is (e_0, e_1)-close to $\mathbf{M}[S]$ then $R_{\mathbf{y}} = S$.

Three remarks are in order. First, if $\mathbf{y}$ is not (e_0, e_1)-close to any $\mathbf{M}[S]$ then $R_{\mathbf{y}}$ can be arbitrary. In that case we can simply set $R_{\mathbf{y}} = \emptyset$. If $\mathbf{y}$ is indeed (e_0, e_1)-close to any $\mathbf{M}[S]$ then $R_{\mathbf{y}}$ is unique because $R_{\mathbf{y}} = S$. Second, the definition does not tell us how to obtain $R_{\mathbf{y}}$ from $\mathbf{y}$, as long as the $R_{\mathbf{y}}$ exist we have an error-correcting separable matrix. Third, the definition also does not give us a method for verifying if a given matrix is error-correcting separable. It is possible to give another equivalent definition, summarized in the following proposition.

Proposition 1.2. *For any vector $\mathbf{z} \in \{0,1\}^t$, let $B(\mathbf{z}, e_0, e_1)$ denote the set of all vectors $\mathbf{y} \in \{0,1\}^t$ such that $\mathbf{y}$ is (e_0, e_1)-close to $\mathbf{z}$. A binary $t \times N$ matrix $\mathbf{M}$ is (d, e_0, e_1)-separable if and only if the sets $B(\mathbf{M}[S], e_0, e_1)$ are disjoint for all sets $S \subset [N]$ with $|S| \leq d$.*

Proof. Suppose $B(\mathbf{M}[S_1], e_0, e_1) \cap B(\mathbf{M}[S_2], e_0, e_1) \neq \emptyset$ for some $S_1 \neq S_2$. Consider any vector $\mathbf{y}$ in the intersection. If $\mathbf{M}$ was (d, e_0, e_1)-separable, then $R_{\mathbf{y}} = S_1$ and $R_{\mathbf{y}} = S_2$, a contradiction. □

The above proposition does give us a method for verifying if a given matrix is error-correcting separable. However, the straightforward way of verification will take time $O\left(\binom{N}{d}^2 \binom{t}{e_0+e_1}\right)$.

Open Problem 1.3. We should be able to prove that verifying if a matrix is ECLS is co-**NP** hard.

1.2 Error-correcting disjunct matrices

Next, we want to formalize the idea of a naive-decoding algorithm, from which we can define error-tolerant disjunct matrices. When there is no error, we eliminate any column (i.e. item) contained in a negative test and return the remaining columns. When there is one false negative, the fact that a column belongs to *one* negative test does not guarantee that it is a negative column because the test might have been in error. But, if there was only at most one false negative and a column belongs to at least *two* negative tests, then we can be sure that the column is indeed a negative. Generalizing the above idea, we define the *naive decoding algorithm* to be the algorithm which eliminates all columns which participated in at least $e_1 + 1$ negative tests.

Definition 1.4 (Error-correcting disjunct matrix)**.** A binary $t \times N$ matrix $\mathbf{M}$ is (d, e_0, e_1)-disjunct if the naive decoding algorithm always returns correctly the positives, as long as there are at most d positives, at most e_0 false positive tests, and at most e_1 false negative tests.

Just like in the error-free case, the definition does not give us any hint as to how to tell if a matrix is error-correcting disjunct. Is there a better characterization? We have to look a little closer at the algorithm. First, the algorithm certainly never eliminates a positive column. It was designed that way. But, a negative column $\mathbf{M}^j$ might still remain uneliminated. This happens if $\mathbf{M}^j$ does not participate in enough negative tests. What makes things worse is when $\mathbf{M}^j$ participated in enough negative tests but the e_0-errors turned some of the negative tests $\mathbf{M}^j$ participated into positives and in the end $\mathbf{M}^j$ does not have enough negative "certificates." Thus, if S was the set of positives, it must be the case that $|\mathbf{M}^j \setminus \mathbf{M}[S]| \geq e_0 + e_1 + 1$ for $\mathbf{M}^j$ to be surely eliminated by the naive decoding algortihm. The analysis leads to the following proposition.

Proposition 1.5. *A binary $t \times N$ matrix $\mathbf{M}$ is (d, e_0, e_1)-disjunct if and only if for any column $\mathbf{M}^j$ and any subset $S \subset [N]$ for size $|S| \leq d$, $j \notin S$, we have*

$$|\mathbf{M}^j \setminus \mathbf{M}[S]| \geq e_0 + e_1 + 1.$$

Proof. The above analysis shows that if $\mathbf{M}$ satisfies the stated property then $\mathbf{M}$ is (d, e_0, e_1)-disjunct. Conversely, suppose $\mathbf{M}$ is (d, e_0, e_1)-disjunct but $\mathbf{M}$ does not satisfy the stated property. Let j and S be such that $j \notin S$, $|S| \leq d$, and

$$|\mathbf{M}^j \setminus \mathbf{M}[S]| \leq e_0 + e_1.$$

Then, we claim that the naive decoding algorithm does not always return S when S is the set of positives. Suppose the tests come out positives whenever a member of S belongs to the tests. Also, e_0 of the tests that j belongs but S do not belong were false positives. Then, item j only belongs to at most e_1 negative tests and thus j is not eliminated. □

What is really nice about the above proposition is the following observation. Suppose $\mathbf{M}$ is (d, e_0, e_1)-disjunct. Let $e = e_0 + e_1$. Then, for any e_0', e_1' such that $e_0' + e_1' = e$ we know that $\mathbf{M}$ is also (d, e_0', e_1')-disjunct because we can check

$$|\mathbf{M}^j \setminus \mathbf{M}[S]| \geq e_0 + e_1 + 1 = e_0' + e_1' + 1.$$

Thus, the matrix can correct up to e errors overall, whether or not the errors were false positives or false negatives.

But then what is the naive decoding algorithm if the e_1 is shifting between 0 and e? Well, we need to know the specific value of e_1 to be able to run the naive decoding algorithm (which has e_1 as a parameter). But, it is still true that a (d, e_0, e_1)-disjunct matrix is (d, e_0', e_1')-disjunct. Their naive decoding algorithms are different though.

Open Problem 1.6. We should be able to prove that verifying if a matrix is ECLD is co-$\mathbf{NP}$ hard.

1.3 (Almost) Equivalence between error-correcting disjunct and separable matrices

A (d, e_0, e_1)-disjunct matrix is certainly (d, e_0, e_1)-separable because the naive decoding algorithm gives us $R_{\mathbf{y}}$ for a given test outcome $\mathbf{y}$.

Conversely, we will show that a (d, e_0, e_1)-separable matrix $\mathbf{M}$ is $(d-1, e_0, e_1)$-disjunct. Assume the contrary that $\mathbf{M}$ is not $(d-1, e_0, e_1)$-disjunct. Then, there exists a column j and a set $S \subset [N]$ of size $|S| \leq d-1$ such that

$$|\mathbf{M}^j \setminus \mathbf{M}[S]| \leq e_0 + e_1.$$

Let $S' = S \cup \{j\}$. We claim that $B(\mathbf{M}[S], e_0, e_1) \cap B(\mathbf{M}[S'], e_0, e_1) \neq \emptyset$, which then by Proposition 1.2 leads to a contradiction. Consider vector $\mathbf{z} \in \mathbf{M}[S]$. Then, $\mathbf{M}[S']$ has at most $e_0 + e_1$ ones not in common with $\mathbf{z}$. Hence, if we turn e_1 bits 1 of $\mathbf{M}[S']$ not in common with $\mathbf{z}$ from 1 to 0, we obtain a vector $\mathbf{y}$ which has at most e_0 ones not in common with $\mathbf{z}$. From $\mathbf{z}$, we can turn at most e_0 zeros from 0 to 1 to get to $\mathbf{y}$. Consequently, $\mathbf{y} \in B(\mathbf{M}[S], e_0, e_1) \cap B(\mathbf{M}[S'], e_0, e_1)$.

1.4 Lower bounds

Since (d, e_0, e_1)-disjunct matrices are (d, e_0', e_1')-disjunct matrices as long as $e_0 + e_1 = e_0' + e_1'$, we define a matrix $\mathbf{M}$ to be d^r-disjunct if for any column j and any set $S \subset [N]$ of at most d columns we have

$$|\mathbf{M}^j \setminus \mathbf{M}[S]| \geq r.$$

Think of $r = e_0 + e_1 + 1$. Let $t(d, r, N)$ denote the minimum number of rows of a d^r-disjunct matrix with N columns. Note that a d-disjunct matrix is exactly a d^1-disjunct matrix.

1.4.1 Known bounds

Dyachkov-Rykov-Rashad [7] gave the first known results on d^r-list-disjunct matrices, which were called *super-imposed distance codes* in their paper. Their results are summarized below.

We first define the *rate* of a d^r-list-disjunct matrix. Let ρ be the relative distance of the corresponding superimposed code, namely $\rho = r/t$. Let $\bar{N}(d, t, r)$ denote the maximum number of columns of a d^r-disjunct matrix with t rows. Also, let $H(\rho)$ denote the binary entropy function

$$H(\rho) := -\rho \log_2 \rho - (1-\rho) \log_2 (1-\rho). \tag{1}$$

And, define

$$\rho_d := \frac{d^d}{(d+1)^{d+1}}. \tag{2}$$

$$R_d(\rho) = \overline{\lim_{t\to\infty}} \frac{\log_2 \bar{N}(d,t,\rho t)}{t}. \tag{3}$$

Theorem 1.7 (Dyachkov-Rykov-Rashad, 1989)**.** *The rate of a d^r-disjunct matrix is bounded by*

$$R_d(\rho) \le U_d(\rho), \tag{4}$$

where, $U_d(\rho) = 0$ for $\rho \ge \rho_d$, and $U_d(\rho)$ is defined recursively for $0 < \rho < \rho_d$ as follows.

(i) If $d = 1$, then

$$U_1(\rho) := \begin{cases} H\left(\frac{1}{2}\left[1 - \sqrt{8\rho(1-2\rho)}\right]\right) & \text{if } 0 < \rho < 1/4 \\ 0, & \text{if } \rho \ge 1/4. \end{cases}$$

(ii) If $d \ge 2$, then

$$U_d(\rho) = \min\left\{1 - \rho/\rho_d, U_1(\rho)/d, \hat{U}_d(\rho)\right\}$$

where $\hat{U}_d(\rho)$ is the unique solution to the equation

$$\hat{U}_d(\rho) = \max_{(5)} \left\{ H\left(\frac{x}{d}\right) - (x+\rho) H\left(\frac{x}{(x+\rho)d}\right)\right\}$$

$$0 \le x \le 1 - \frac{\hat{U}_d(\rho)}{U_{d-1}(\rho)} - \rho. \tag{5}$$

Remark 1.8. The above theorem is not very useful if we need the case when d, N and r are given as parameters to our problem. It can be used in the $d = 1$ case as the bound is explicit. When $d \ge 2$, Dyachkov-Rykov-Rashad derived the asymptotic behaviors of the function $U_d(\rho)$ for fixed d in the following corollary.

Corollary 1.9. *(a) For any fixed $d \ge 1$, if $\rho \to \rho_d - 0$, then*

$$R_d(\rho) \le U_1(\rho) = 1 - \rho/\rho_d,$$

(b) If $d \to \infty$ and $\rho d \to 0$, then

$$R_d(\rho) \le U_d(\rho) = \hat{U}_d(\rho) = \frac{(2-\rho d)\log_2 d}{d^2}(1 + o(1)).$$

Dyachkov-Rykov-Rashad also gave a lower bound for the rate, summarized in the following theorem. Define the Kullback distance for any $0 < \alpha, \beta < 1$:

$$K(\alpha,\beta) = \alpha \log_2\left(\frac{\alpha}{\beta}\right) + (1-\alpha)\log_2\left(\frac{1-\alpha}{1-\beta}\right). \tag{6}$$

Theorem 1.10 (Dyachkov-Rykov-Rashad, 1989)**.** *We have the following lower bound for $R_d(\rho)$:*

$$R_d(\rho) \geq L_d(\rho) := \frac{\max\left\{A_d(\rho, x) \mid \rho \leq (1-x)x^d, 0 < x < 1\right\}}{d}, \tag{7}$$

where

$$A_d(\rho, x) := \max_{0<y<1} \left\{(1-x)K(\rho/(1-x), y^d) - dK(x, y)\right\}.$$

Note that $(1-x)x^d \leq \rho_d$, and equality is reached when $x = \frac{d}{d+1}$. Furthermore, at $\rho = (1-x)x^d$ we have $A_d(\rho, x) = 0$. When $0 < \rho < (1-x)x^d$ the function $A_d(\rho, x) > 0$ decreases as ρ increases and

$$A_d(\rho, x) > K(\rho, (1-x)x^d).$$

In particular, we have the following corollary.

Corollary 1.11. *We have $L_d(\rho_d) = 0$, and $L_d(\rho) > 0$ for $0 < \rho < \rho_d$. Moreover, $L_d(\rho)$ is a decreasing function satisfying*

$$L_d(\rho) > \frac{K(\rho, \rho_d)}{d}. \tag{8}$$

In the $d = 1$ case, a more precise bound is known.

Theorem 1.12 (Theorem 1 of Balding-Torney [1])**.** *If $\mathbf{M}$ is a $t \times N$ 1^r-disjunct matrix, then*

$$N \leq \frac{1}{K_{r-1}} \binom{t}{\lfloor t/2 \rfloor},$$

where $K_0 = 1$ (this is precisely Sperner's lemma for maximum antichain!) and, for r even,

$$K_r = \sum_{s=0}^{r/2} \binom{\lfloor t/2 \rfloor}{s} \binom{\lceil t/2 \rceil}{s},$$

while for r odd,

$$K_r = K_{r-1} + \frac{1}{T} \binom{\lfloor t/2 \rfloor}{(r+1)/2} \binom{\lceil t/2 \rceil}{(r+1)/2},$$

where $T = \lfloor 2\lfloor t/2 \rfloor/(r+1) \rfloor$.

1.4.2 Our bounds

The following 1975 result was attributed to Bassalygo by Dyachkov and Rykov [6]. We proved it in one of the earlier lectures.

Proposition 1.13 (Bassalygo – 1975)**.** *For the d-disjunct matrices, we have the following bound*

$$t(d, 1, N) \geq \min\left\{\binom{d+2}{2}, n\right\}.$$

We will attempt to derive an error-correcting analog of Bassalygo's bound. It is tempting to try to show that

$$t(d, r, N) \geq \min\left\{\binom{d+r+1}{2}, rN\right\},$$

which would require the following base case

$$t(1, r, N) \geq \min\left\{\binom{r+2}{2}, rN\right\},$$

However, both of the above are too strong. We shall show later that $t(d, r, N) = O(d^2 \log N + dr)$. For $d = 1$ and $r \approx \sqrt{N}$, for instance, the upper bound $O(\sqrt{N})$ would contradict the conjectured lower bound of $\Omega(N)$. Thus, we shall show a different analog of Bassalygo's bound.

Let us first define some more terminologies which will be used throughout. For any $t \times N$ binary matrix $\mathbf{M}$, recall that we can think of any column $\mathbf{M}^j$ as the subset of rows $\{i \mid m_{ij} = 1\}$. A subset $W \subseteq [t]$ is called a *private subset* of column $\mathbf{M}^j$ if no other column of $\mathbf{M}$ contains W. An element $i \in [t]$ is a *private element* of column $\mathbf{M}^j$ if no other column contains i. Define the *weight* $w(\mathbf{M}^j)$ of a column $\mathbf{M}^j$ to be the number of 1's in it. Let $N(w)$ be the number of columns with weight w. And, let $w_{\max}$ be the maximum column weight.

The following bound implies Bassalygo's.

Proposition 1.14 (Error-correction analog of Bassalygo's bound)**.** *We have*

$$t(d, r, N) \geq \min\left\{(d+1)(\frac{d}{2} + r) + r - 1, rN\right\}. \tag{9}$$

Proof. We first prove the base case of (9) that

$$t(1, r, N) \geq \min\{3r, rN\} \tag{10}$$

Consider a 1^r-disjunct matrix $\mathbf{M}$ with t rows and N columns. Let R be the set of ordered triples (i, j_1, j_2) for which $i \in [t], j_1 \neq j_2 \in [N]$, and $i \in \mathbf{M}^{j_1} \setminus \mathbf{M}^{j_2}$. For a fixed pair (j_1, j_2), there must be at least r different i for which $(i, j_1, j_2) \in R$. Hence,

$$|R| \geq rN(N-1).$$

For a fixed $i \in [t]$, let N_i be the number of columns j for which $i \in \mathbf{M}^j$. Then, there are precisely $N_i(N - N_i)$ pairs (j_1, j_2) for which $(i, j_1, j_2) \in R$. From $N_i(N - N_i) \leq \lfloor N/2 \rfloor \lceil N/2 \rceil$, we conclude that

$$|R| \leq t\lfloor N/2 \rfloor \lceil N/2 \rceil.$$

Consequently,

$$t \geq \frac{rN(N-1)}{\lfloor N/2 \rfloor \lceil N/2 \rceil}. \tag{11}$$

When $N = 2, 3$, (11) implies $t \geq rN$. When $N \geq 4$, we have

$$t \geq \frac{4r(N-1)}{N} \geq 3r.$$

Thus, (10) follows and (9) holds for $d = 1$.

When $d > 1$, consider a d^r-disjunct matrix $\mathbf{M}$ with t rows and N columns. If column $\mathbf{M}^j$ has weight at most $d + r - 1$, then it must have at least r private elements. The total number of private elements of all columns is at most t; hence,

$$\sum_{1 \le w \le d+r-1} N(w) \le t/r.$$

Consequently, if $w_{\max} \le d + r - 1$ then $N = \sum_w N(w) \le t/r$, or $t \ge rN$. Now, suppose $w_{\max} \ge d + r$ and consider a column $\mathbf{M}^j$ with weight equal to $w_{\max}$. If we remove column $\mathbf{M}^j$ and all rows i for which $m_{ij} = 1$, we are left with a $(d-1)^r$-disjunct matrix with $t - w_{\max}$ rows and $N - 1$ columns. Thus,

$$t \ge d + r + t(d - 1, r, N - 1).$$

The induction hypothesis concludes the proof. □

Remark 1.15. In any inductive proof, the base case deals with the $d = 1$, $r \ge 1$ case, for which there was a nice known bound from [1] (Theorem 1.12 below). The question is, can we use this result to show a better base case than that in (10)?

A 1^r-disjunct matrix with N columns and rN rows is trivial to construct (by stacking up r copies of the identity matrix of order N). If $d \ge \sqrt{2rN}$ then

$$(d + 1)(\frac{d}{2} + r) + r - 1 > rN$$

in which case $t(d, r, N) = rN$. Hence, we only need to consider $d < \sqrt{2rN}$.

In order to prepare for a more general bound, we need to slightly extend Lemma 9.1 from Erdős-Frankl-Füredi [8].

Proposition 1.16. *Let $\mathbf{M}$ be a $t \times N$ d^r-disjunct matrix. Fix a positive integer $w \le t$. Let $\mathcal{C}$ denote the set of all columns of $\mathbf{M}$. Let $\mathcal{C}_w$ denote the set of columns $\mathbf{M}^j$ of $\mathbf{M}$ each of which has a private w-subset. Then, for any column $C \in \mathcal{C} - \mathcal{C}_w$ and any $k \ge 0$ other columns $C_1, \cdots, C_k \in \mathcal{C}$, we have*

$$\left| C \setminus \bigcup_{j=1}^{k} C_j \right| \ge (d - k)w + r. \tag{12}$$

In particular, if $\mathbf{M}$ has at least $d + 1$ columns $C_1, \ldots, C_{d+1}$ none of which have any private w-subset, then

$$\left| \bigcup_{j=1}^{d+1} C_j \right| \ge \frac{1}{2}(d + 1)(dw + 2r). \tag{13}$$

Proof. Inequality (12) is straightforward. To see (13), we apply (12) as follows.

$$\begin{aligned} \left| \bigcup_{j=1}^{d+1} C_j \right| &= |C_1| + |C_2 \setminus C_1| + \cdots + |C_{d+1} \setminus C_1 \cup \cdots \cup C_d| \\ &\ge (dw + r) + ((d - 1)w + r) + \cdots + (w + r) + r \\ &= \frac{1}{2}(d + 1)(dw + 2r). \end{aligned}$$

□

Now, let $\mathcal{C}_w$ be the sub-collection of columns of $\mathbf{M}$ each of which has a private w-subset, and $\mathcal{C}_{<w}$ be the sub-collection of columns of $\mathbf{M}$ each of which has weight $< w$. Then, it is not hard (see [9]) to show that, for any $w \leq t/2$, $|\mathcal{C}_w| + |\mathcal{C}_{<w}| \leq \binom{t}{w}$. Now, if there were at least $d+1$ columns **not** in $\mathcal{C}_w \cup \mathcal{C}_{<w}$, then by Proposition 1.16 the union of columns not in $\mathcal{C}_w \cup \mathcal{C}_{<w}$ is at least $\frac{1}{2}(d+1)(dw+2r)$. Suppose we choose w such that

$$\frac{1}{2}(d+1)(dw+2r) \geq t+1, \tag{14}$$

then we reach a contradiction and thus we can conclude that $N \leq d + \binom{t}{w}$. The minimum w for which (14) holds is $w = \left\lceil \frac{t+1-r(d+1)}{\binom{d+1}{2}} \right\rceil$, which is at most $t/2$ when $d \geq 2$. Hence, we just proved the following theorem

Theorem 1.17. *For $N \geq d \geq 2$, and a positive integer r. For any d^r-disjunct matrix with t rows and N columns we have*

$$N \leq d + \binom{t}{\left\lceil \frac{t+1-r(d+1)}{\binom{d+1}{2}} \right\rceil}.$$

From the error-tolerant version of Bassalygo's bound, we only need to consider the case when $t \geq (d+1)(d/2+r)+r = \binom{d+1}{2} + (d+2)r$, which means

$$\begin{aligned}
\frac{t}{t+1-r(d+1)} &\leq \frac{\binom{d+1}{2} + (d+2)r}{\binom{d+1}{2} + (d+2)r + 1 - r(d+1)} \\
&= \frac{\binom{d+1}{2} + (d+2)r}{\binom{d+1}{2} + 1 + r} \\
&< \frac{\binom{d+1}{2} + r + 1 + (d+1)r}{\binom{d+1}{2} + 1 + r} \\
&= 1 + \frac{(d+1)r}{\binom{d+1}{2} + 1 + r} \\
&< 1 + \frac{(d+1)r}{r} \\
&= d+2.
\end{aligned}$$

Now, from the above theorem we get

$$\begin{aligned}
\log(N-d) &\leq \left\lceil \frac{t+1-r(d+1)}{\binom{d+1}{2}} \right\rceil \log\left(\frac{te}{\left\lceil \frac{t+1-r(d+1)}{\binom{d+1}{2}} \right\rceil} \right) \\
&\leq \left\lceil \frac{t+1-r(d+1)}{\binom{d+1}{2}} \right\rceil \log\left(\frac{te\binom{d+2}{2}}{t+1-r(d+1)} \right) \\
&\leq \left\lceil \frac{t+1-r(d+1)}{\binom{d+1}{2}} \right\rceil \log\left((d+2)^3 \right).
\end{aligned}$$

Thus, for large N we get a lower bound of about

$$t = \Omega\left(\frac{d^2}{\log d} \log(N-d) + rd \right).$$

1.5 Probabilistic upper bounds

We use the concatenation of a random outer code and the identity inner code to show the existence of a good d^r-disjunct matrix. Recall that a d^r-disjunct matrix is (d, e_0, e_1)-disjunct for any e_0, e_1 such that $e_0 + e_1 = r - 1$.

Theorem 1.18. *For the d^r-disjunct matrices, we have $t(d, r, N) = O\left(d^2 \log \frac{N}{d} + rd\right)$.*

Proof. Let C_{out} be a code of length n over an alphabet Σ of size q constructed randomly be selecting each codeword from Σ^n uniformly at random. This is equivalent to setting each position of a random codeword to be one of q symbols from Σ. Let $C_{\text{in}} = \text{ID}_q$. We will choose $q > d$.

Let $\mathbf{M} = C_{\text{out}} \circ C_{\text{in}}$. Fix $d + 1$ columns (i.e. codewords) of $\mathbf{M}$: $\mathbf{M}^{j_0}, \mathbf{M}^{j_1}, \ldots, \mathbf{M}^{j_d}$. For a fixed position $i \in [n]$, and a column j, let $\mathbf{M}^j[i] \in \Sigma$ denote the symbol in position i of the jth codeword. Then,

$$\text{Prob}[\mathbf{M}^{j_0}[i] \in \{\mathbf{M}^{j_k}[i] \mid k \in [d]\}] \leq (d/q).$$

Let X_i be the binary random variable indicating the event that $\mathbf{M}^{j_0}[i] \in \{\mathbf{M}^{j_k}[i] \mid k \in [d]\}$. And, let $X = \sum_{i=1}^{n} X_i$. Then, by linearity of expectation

$$\text{E}[X] = \sum_{i=1}^{n} \text{E}[X_i] \leq nd/q.$$

Thus, by Hoeffding's inequality

$$\begin{aligned}
\text{Prob}\left[|\mathbf{M}^{j_0} \setminus \bigcup_{k=1}^{d} \mathbf{M}^{j_k}| < r\right] &= \text{Prob}[X > n - r] \\
&= \text{Prob}[X - \text{E}[X] > n - r - \text{E}[X]] \\
&\leq \text{Prob}[X - \text{E}[X] > n(1 - d/q) - r] \\
&< e^{-2(n(1-d/q)-r)^2/n}.
\end{aligned}$$

By the union bound,

$$\begin{aligned}
\text{Prob}[\mathbf{M} \text{ is not } d^r\text{-disjunct}] &\leq (d+1)\binom{N}{d+1} \text{Prob}\left[|\mathbf{M}^{j_0} \setminus \bigcup_{k=1}^{d} \mathbf{M}^{j_k}| < r\right] \\
&\leq (d+1)\left(\frac{Ne}{d+1}\right)^{d+1} e^{-2(n(1-d/q)-r)^2/n}.
\end{aligned}$$

Thus, we need to pick parameters q and n such that the right-hand-side above is smaller than 1. To simplify things a little, recall by (the analog of) Bassalygo's bound that we can assume $d + 1 \leq \sqrt{rN}$ (otherwise $t \geq rN$ and the problem is trivial). Also, assume $e \leq N/(d+1)$. Thus,

$$(d+1)\left(\frac{Ne}{d+1}\right)^{d+1} \leq r(N/(d+1))^{2d+3}.$$

Thus, we want to set q and n such that

$$\frac{2(n(1-d/q)-r)^2}{n} \geq (2d+3)\ln(N/(d+1)) + \ln r.$$

Now, pick

$$\begin{aligned} q &= 2d \\ n &= 6(2d+3)\ln(N/(d+1)) + 6r \end{aligned}$$

we have

$$\begin{aligned} \frac{2(n(1-d/q)-r)^2}{n} &= \frac{[3(2d+3)\ln(N/(d+1)) + 2r]^2}{3(2d+3)\ln(N/(d+1)) + 3r} \\ &> \frac{[3(2d+3)\ln(N/(d+1)) + 3r] \cdot [(2d+3)\ln(N/(d+1)) + r]}{3(2d+3)\ln(N/(d+1)) + 3r} \\ &= (2d+3)\ln(N/(d+1)) + r \\ &> (2d+3)\ln(N/(d+1)) + \ln r. \end{aligned}$$

Overall, the matrix has $t = nq = 12d(2d+3)\ln(N/(d+1)) + 12dr$ rows. □

2 Error-correcting list-separable and list-disjunct matrices

We next develop the notions of error-correcting list-separable and list-disjunct matrices using the same line of reasoning.

2.1 Error-correcting list-separable matrices

Definition 2.1 (Error-correcting list-separable matrix)**.** A binary $t \times N$ matrix $\mathbf{M}$ is said to be (d, ℓ, e_0, e_1)-*list-separable* if for every $\mathbf{y} \in \{0,1\}^t$ there exists a set $R_{\mathbf{y}} \subseteq [N]$ such that the following holds. Let $S \subseteq [N]$ be any subset of columns where $|S| \leq d$. If $\mathbf{y}$ is (e_0, e_1)-close to $\mathbf{M}[S]$ then $S \subseteq R_{\mathbf{y}}$ and $|R_{\mathbf{y}}| < |S| + \ell$.

We remark that if $\mathbf{y}$ is not (e_0, e_1)-close to any $\mathbf{M}[S]$, then we can simply set $R_{\mathbf{y}} = \emptyset$. Also, when the matrix $\mathbf{M}$ is equipped with a decoding algorithm which returns $R_{\mathbf{y}}$ given $\mathbf{y}$, then it is automatically error-correcting list-separable. We next derive a combinatorial condition to verify if a matrix is error-correcting list-separable.

Proposition 2.2. *A $t \times N$ binary matrix $\mathbf{M}$ is (d, ℓ, e_0, e_1)-list-separable if and only if, for any $\mathbf{y} \in \{0,1\}^t$ the following condition holds. Define $S(\mathbf{y}, e_0, e_1)$ to be the collection of all S of size at most d such that $\mathbf{y}$ can be an (erroneous) outcome vector when S is the set of positives; specifically,*

$$\mathcal{S}(\mathbf{y}, e_0, e_1) = \{S \subseteq [N] \mid |S| \leq d, \mathbf{y} \text{ is } (e_0, e_1)\text{-close to } \mathbf{M}[S].\}$$

Then,

$$\left| \bigcup_{S \in \mathcal{S}(\mathbf{y}, e_0, e_1)} S \right| < \ell + \min_{S \in \mathcal{S}(\mathbf{y}, e_0, e_1)} |S|.$$

Proof. For necessity, note that $S \subseteq R_{\mathbf{y}}$ for every $S \in \mathcal{S}(\mathbf{y}, e_0, e_1)$; and thus $\bigcup_{S \in \mathcal{S}(\mathbf{y}, e_0, e_1)} S \subseteq R_{\mathbf{y}}$. Hence,

$$\left| \bigcup_{S \in \mathcal{S}(\mathbf{y}, e_0, e_1)} S| \leq |R_{\mathbf{y}} \right| < \ell + \min_{S \in \mathcal{S}(\mathbf{y}, e_0, e_1)} |S|.$$

For sufficiency, we can simply set $R_{\mathbf{y}} = \bigcup_{S \in \mathcal{S}(\mathbf{y}, e_0, e_1)} S$. □

2.2 Error-correcting list-disjunct matrices

The definition of error-correcting list-separable matrix does not tell us how to obtain $R_{\mathbf{y}}$ given $\mathbf{y}$. We next develop the notion of error-correcting list-disjuct matrix for which the naive decoding algorithm returns a set $R_{\mathbf{y}}$ which contains all the positive columns plus less than ℓ spurious columns. Since we can not eliminate a positive column, the only natural choice is to eliminate all columns which participated in at least $e_1 + 1$ negative tests because those are the columns we know for sure are negative. We call this strategy the *naive decoding algorithm* (Algorithm 2.2).

Algorithm 1 Naive decoding for (d, ℓ, e_0, e_1)-list-disjunct matrices

Input: The test outcome vector $\mathbf{y} \in \{0,1\}^t$

for $j = 1$ to N **do**
  if $|\{i \in [t] \mid i \in \mathbf{M}^j, y_i = 0\}| \geq e_1 + 1$ **then** // *item j belongs to at least $e_1 + 1$ negative tests*
    mark j as a *negative* item
  end if
end for
return $R_{\mathbf{y}}$, the set of unmarked items

Definition 2.3 (Error-correcting list-disjunct matrix)**.** A matrix $\mathbf{M}$ is called (d, ℓ, e_0, e_1)-list-disjunct if the following property holds for all $S \subseteq [N]$, $|S| \leq d$. Let $\mathbf{y} \in \{0,1\}^t$ be any vector which is (e_0, e_1)-close to $\mathbf{M}[S]$. The naive decoding algorithm on $\mathbf{y}$ returns a set $R_{\mathbf{y}} \subseteq [N]$ such that $S \subseteq R_{\mathbf{y}}$ and $|R_{\mathbf{y}}| < |S| + \ell$. In other words, the naive decoding algorithm always works (in the list sense), even if there are up to e_0 false positives and e_1 false negatives in test outcomes.

Which properties must $\mathbf{M}$ satisfy so that the naive decoder returns the desired $R_{\mathbf{y}}$? Suppose $S \subseteq [N]$, $|S| \leq d$, is some set of positives. Let $\mathbf{y}$ be a vector which is (e_0, e_1)-close to $\mathbf{M}[S]$, which means $\mathbf{y}$ can potentially be the outcome vector when S is the set of positives. Let T be an arbitrary set of ℓ columns not in S. We want at least one column of T to be eliminated, which means there must be at least one column j of T which is contained in $e_1 + 1$ negative tests even when all the e_0 and e_1 errors went "against" it. Specifically, let $X \subseteq \mathbf{M}[T] \setminus \mathbf{M}[S]$ be any set of up to e_0 tests. The tests in X should contribute to certifying the "innocence" of members of T. But, due to the false positive test errors, all of X might return positive. We want to say that, no matter where X lies, there still exists a column in T which is contained in $e_1 + 1$ tests which are neither in X nor in $\mathbf{M}[S]$. This intuition turns out to be necessary and sufficient.

Proposition 2.4. *Given positive integers $d, \ell > 0$ such that $d + \ell \leq N$; and, given non-negative integers e_0, e_1. A binary $t \times N$ matrix $\mathbf{M}$ is (d, ℓ, e_0, e_1)-list-disjunct if and only if, for any disjoint sets $S, T \subseteq [N]$ with $|S| = d$ and $|T| = \ell$ the following holds. Let X be an arbitrary subset of $\mathbf{M}[T] \setminus \mathbf{M}[S]$ of size at most e_0. Then, there exists a column $\bar{j} \in T$ such that $|\mathbf{M}^{\bar{j}} \setminus (X \cup \mathbf{M}[S])| \geq e_1 + 1$.*

Proof. The fact that the condition is sufficient follows from the analysis above. We show that it is also necessary. Suppose for the contrary that there exists S, T, X satisfying the stated criteria but for every $j \in T$ we have $|\mathbf{M}^j \setminus (X \cup \mathbf{M}[S])| \leq e_1$. Then, suppose the tests in X are all false positives. Then, no element in T will be eliminated, which means the returned set of items contains $|S| + \ell$ elements; thus, $\mathbf{M}$ is not (d, ℓ, d_0, d_1)-list-disjunct. □

From the proposition, the following result follows straightforwardly.

Proposition 2.5. *If $e_0 > 0$, then a $(d, \ell, e_0 - 1, e_1 + 1)$-list-disjunct matrix is a a (d, ℓ, e_0, e_1)-list-disjunct matrix. In particular, for every non-negative e_0, e_1, a $(d, \ell, 0, e_0+e_1)$-list-disjunct matrix is a a (d, ℓ, e_0, e_1)-list-disjunct matrix.*

2.3 (Almost) Equivalence between error-correcting list-disjunct and list-separable matrices

Our development so far has been relatively natural, following the reasoning line from the none-error, none-list classic results of group testing. We know that a matrix is d-separable if it is d-disjunct, and it is $(d-1)$-disjunct if it is d-separable. It turns out that the exact same result holds for the list- and error-case.

Proposition 2.6. *A (d, ℓ, e_0, e_1)-list-disjunct matrix is (d, ℓ, e_0, e_1)-list-separable, and a (d, ℓ, e_0, e_1)-list-separable matrix is $(d-1, \ell, e_0, e_1)$-list-disjunct.*

Proof. The first statement is trivial. To show the second statement, consider a (d, ℓ, e_0, e_1)-list-separable matrix $\mathbf{M}$ with t rows and N columns. Suppose it is not $(d-1, \ell, e_0, e_1)$-list-disjunct which means there is a column set T of size ℓ, a disjoint column set S of size at most $d-1$, and $X \subseteq \mathbf{M}[T] \setminus \mathbf{M}[S]$ of size $|X| \leq e_0$ such that, for any $j \in T$ we have $|\mathbf{M}^j \setminus (X \cup \mathbf{M}[S])| \leq e_1$. We will show that $\mathbf{M}$ is not (d, ℓ, e_0, e_1)-list-separable to reach a contradiction.

For each $j \in T$, let $S^j = S \cup \{j\}$. Let $\mathbf{y} = \mathbf{M}[S] \cup X$. Then, $\mathbf{y}$ is (e_0, e_1)-close to $\mathbf{M}[S^j]$ because we can turn $\mathbf{M}[S^j]$ into $\mathbf{y}$ by turning at most e_1 bits in positions $\mathbf{M}^j \setminus (X \cup \mathbf{M}[S])$ from 1 to 0, and at most e_0 bits in positions $X \setminus \mathbf{M}^j$ from 0 to 1. Also, trivially $\mathbf{y}$ is (e_0, e_1)-close to $\mathbf{M}[S]$. Consequently, S and the S^j, $j \in T$, are all in $\mathcal{S}(\mathbf{y}, e_0, e_1)$. Hence,

$$\left| \bigcup_{S' \in \mathcal{S}(\mathbf{y}, e_0, e_1)} S' \right| \geq |S| + |T| = |S| + \ell \geq \ell + \min_{S' \in \mathcal{S}(\mathbf{y}, e_0, e_1)} |S'|$$

contradicting Proposition 2.2. □

Remark 2.7. It is not hard to find an example of a matrix which is (d, ℓ, e_0, e_1)-list-separable but not (d, ℓ, e_0, e_1)-list-disjunct.

2.4 Lower bounds

2.4.1 Known bounds

Cheraghchi [3] has defined a slightly more general notion of list-separable matrix, where $R_{\mathbf{y}}$ does not necessarily have to contain the positive set. In particular, he studied the following notion. A $t \times N$ binary matrix $\mathbf{M}$ is called (e_0, e_1, e_0', e_1')-*correcting for d-sparse vectors* if, for every vector $\mathbf{y} \in \{0,1\}^t$, there exists a (valid decoding) vector $\mathbf{z} \in \{0,1\}^N$ such that for every $\mathbf{x} \in \{0,1\}^N$ for which $(\mathbf{x}, \mathbf{z})$ is (e_0', e_1')-far from, we have $\mathbf{y}$ is (e_0, e_1)-far from $\mathbf{M}[\mathbf{x}]$. Here, $\mathbf{x}$ can be understood as a subset of $[N]$ in the usual sense.

If we use $\mathbf{M}$ to do group testing, then given at most e_0 false positive test outcomes and at most e_1 false negative test outcomes, we can recover an "approximation" $\mathbf{z}$ of the original positive set $\mathbf{x}$ such that we identified at most e_0' false positive items and at most e_1' false negative items. In particular, *every $(e_0, e_1, e_0', 0)$-correcting matrix for d-sparse vectors is $(d, e_0'+1, e_0, e_1)$-list-separable, and vice versa.*

Lemma 2.8 (Lemma 2 from [3])**.** *For any $t \times N$ matrix $\mathbf{M}$ that is (e_0, e_1, e_0', e_1')-correcting for d-sparse vectors,*

$$\frac{\max\{e_0, e_1\} + 1}{e_0' + e_1' + 1} \leq \frac{t}{d}.$$

Lemma 2.9 (Lemma 3 from [3]). *For any $t \times N$ matrix $\mathbf{M}$ that is (e_0, e_1, e_0', e_1')-correcting for d-sparse vectors, and every $\epsilon > 0$, either $e_1 < \frac{(e_1'+1)t}{\epsilon d}$ or $e_0' \geq \frac{(1-\epsilon)(N-d+1)}{(e_1'+1)^2}$.*

Lemma 2.10 (Lemma 4 from [3]). *For any $t \times N$ matrix $\mathbf{M}$ that is $(0, 0, e_0', e_1')$-correcting for d-sparse vectors,*

$$t \geq d \log(N/d) - d - e_0' - O(e_1' \log((N - d - e_0')/e_1')),$$

where the last term is defined to be 0 when $e_1' = 0$.

Since a (d, ℓ, e_0, e_1)-list-disjunct matrix is a $(e_0, e_1, \ell - 1, 0)$-correcting matrix for d-sparse vectors, all bounds in the above three lemmas apply to (d, ℓ, e_0, e_1)-list-disjunct matrices. We summarize the known bounds in the following corollary.

Corollary 2.11. *For any $t \times N$ matrix $\mathbf{M}$ that is (d, ℓ, e_0, e_1)-list-disjunct, all the following hold:*

$$d(\max\{e_0, e_1\} + 1) \leq t\ell, \tag{15}$$

$$\textit{for any } \epsilon > 0, \textit{ either } e_1 < \frac{t}{\epsilon d} \textit{ or } \ell - 1 \geq (1 - \epsilon)(N - d + 1), \tag{16}$$

and

$$t > d \log(N/d) - d - \ell \textit{ when } e_0 = e_1 = 0. \tag{17}$$

Let $t(d, \ell, e_0, e_1, N)$ denote the minimum number of rows of a (d, ℓ, e_0, e_1)-list-disjunct matrix with N columns. Dýachkov-Rykov [5, 6], Rashad [14], and De Bonis-Gąsieniec-Vaccaro [4] studied upper and lower bounds for the rates of (d, ℓ)-list-disjunct matrices. We quote their relevant results here. The upper bounds in [14] are (slightly) better than those in [5, 6]. Dýachkov-Rykov [5, 6] and De Bonis-Gąsieniec-Vaccaro [4] proved different types of lower bounds: the former is better when certain parameters tend to infinity, while the latter is more specific and holds for given finite parameters.

The first lower bound from Dýachkov-Rykov is a simple information theoretic bound.

Proposition 2.12 (Proposition 2 in [6]). *Given positive integers $N \geq d + \ell$, we have*

$$t(d, \ell, 0, 0, N) \geq \log \binom{N}{d} - \log \binom{d + \ell - 1}{d}.$$

Dýachkov-Rykov [5] used a recursive inequality to prove another lowerbound on $t(d, \ell, 0, 0, N)$, which can be summarized as follows. $H(\cdot)$ denotes the binary entropy function.

Theorem 2.13 (Corollary 1 and Theorem 4 in [6]). *When $N \to \infty$ and d, ℓ stay constant, we have*

$$t(d, \ell, 0, 0, N) \geq \max\{d, F(\lfloor d/\ell \rfloor)\} \cdot \log N(1 + o(1)),$$

where the sequence $F(1) = 1, F(2), F(3), \ldots,$ is defined recursively: $F(x), x \geq 2$ is the unique solution to the equation

$$F(x) = \frac{1}{\max\left\{H(v/x) - vH(1/x) \mid 0 < v \leq \frac{F(x)-F(x-1)}{F(x)}\right\}}$$

It is hard if not impossible to guess the asymptotic behavior of $F(x)$ directly from its definition. Fortunately, they can be shown to satisfy the following properties

$$F(x) \geq \frac{x^2}{2\log[e(x+1)/2]}, \quad x \geq 2.$$
$$F(x) \geq \frac{x^2}{2\log x(1+o(1))}, \quad x \to \infty.$$

De Bonis-Gąsieniec-Vaccaro [4] proved a more accessible lowerbound, though probably not as good asymptotically as that of Dýachkov-Rykov. They also proved an upper bound via upperbounding their (k, m, N)-selectors. The following theorem summarize their results.

Theorem 2.14 (De Bonis-Gąsieniec-Vaccaro [4], 2005)**.** *For any positive integers N, d, ℓ with $N > d^2/(4\ell)$, we have*

$$t(d,\ell,0,0,N) > \quad d\log\left(\tfrac{N}{e(d+\ell-1)}\right) \quad \text{if } d < 2\ell \tag{18}$$
$$t(d,\ell,0,0,N) > \quad \tfrac{\ell(\lfloor d/(2\ell)\rfloor^2)}{\log\left(\frac{ed^2}{4\ell}\right)}\log\left(\tfrac{4(N-2(\ell-1)-d/2)}{ed^2}\right) \quad \text{if } d \geq 2\ell \tag{19}$$

For any positive integers N, d, ℓ with $N \geq d + \ell$, we have

$$t(d,\ell,0,0,N) < \frac{(d+\ell)^2}{\ell}\ln\frac{N}{d+\ell} + \frac{2e(d+\ell)^2}{\ell} \tag{20}$$

In terms of upper bounds, Rashad [14] gave a random coding bound for $t(d, \ell, 0, 0, N)$ which uses the code (or matrix) generation method of [13]. The results are stated in the same manner as that of Theorem 1.7, which makes it difficult if not impossible to interpret the asymptotic behavior of the function. Then, two corollaries were derived in the same sense as Corollaries 1.9 and 1.11 were derived from Theorem 1.7. We summarize these corollaries by Rashad as follows.

Theorem 2.15 (Rashad, 1990)**.** *When ℓ is a constant and $N, d \to \infty$, we have*

$$t(d,\ell,0,0,N) \leq \frac{d^2\log e}{\ell}\log N(1+o(1)).$$

On the other hand, when d is a constant and $N, \ell \to \infty$, we have

$$t(d,\ell,0,0,N) \leq \frac{ed}{\log e}\log N(1+o(1)) \approx \frac{d}{0.5307}\log N(1+o(1)).$$

2.4.2 Our bounds

We first prove a lower bound for the error free case. Our bounds are asymptotically the same as those in Theorem 2.14, with slight better constants and a better pre-condition (Theorem 2.14 requires $N > d^2/(4\ell)$ while ours does not).

Lemma 2.16. *For any positive integers N, d, ℓ with $N \geq d + \ell - 1$, we have*

$$t(d, \ell, 0, 0, N) \geq d \log \left(\frac{N}{d + \ell - 1} \right). \tag{21}$$

When $d \geq \min\{2\ell, \ell + 2\}$, the following bound holds

$$t(d, \ell, 0, 0, N) \geq \frac{\lfloor d/\ell \rfloor (d + 2 - \ell)}{2 \log \left(e \lfloor d/\ell \rfloor (d + 2 - \ell)/2 \right)} \log \left(\frac{N - d - 2\ell + 2}{\ell} \right) \tag{22}$$

Proof. Proposition 2.12 easily yields (21)

$$\begin{aligned} t(d, \ell, e_0, e_1, N) &\geq t(d, \ell, 0, 0, N) \\ &\geq \log \left(\frac{\binom{N}{d}}{\binom{d+\ell-1}{d}} \right) \\ &= \log \frac{N \cdots (N - d + 1)}{(d + \ell - 1) \cdots \ell} \\ &\geq \log \left(\frac{N}{d + \ell - 1} \right)^d \\ &= d \log \frac{N}{d + \ell - 1}. \end{aligned}$$

Next, consider the case when $d \geq \min\{2\ell, \ell+2\}$. Let $\mathbf{M}$ be a $t \times N$ (d, ℓ)-list-disjunct matrix. The columns of $\mathbf{M}$, again, will simultaneously be treated as a set family on $[t]$ and as a collection of N binary vectors of length t. Then, $\mathbf{M}$ as a set family satisfies the property that the union of any ℓ columns of $\mathbf{M}$ is not covered by the union of any other d columns. In particular, let S and T be two disjoint sets of columns of $\mathbf{M}$ with $|S| \leq d$ and $|T| \geq \ell$, then $\mathbf{M}[T] \not\subseteq \mathbf{M}[S]$.

For any $j \in [N]$, a subset $X \subseteq \mathbf{M}^j$ is called a *private subset* of $\mathbf{M}^j$ if X is not a subset of any other $\mathbf{M}^{j'}$ for $j' \neq j$. Fix a positive integer $w \leq t$ to be determined later. Partition the columnns $[N]$ into three sub-sets

$$[N] = C^{\mathrm{p}}_{\geq w} \cup C^{\mathrm{np}}_{\geq w} \cup C_{<w}$$

defined as follows.

$$\begin{aligned} C^{\mathrm{p}}_{\geq w} &:= \left\{ j \in [N] \ : \ |\mathbf{M}^j| \geq w \text{ and } \mathbf{M}^j \text{ has a private } w\text{-subset} \right\} \\ C^{\mathrm{np}}_{\geq w} &:= \left\{ j \in [N] \ : \ |\mathbf{M}^j| \geq w \text{ and } \mathbf{M}^j \text{ has no private } w\text{-subset} \right\} \\ C_{<w} &:= \left\{ j \in [N] \ : \ |\mathbf{M}^j| < w \right\}. \end{aligned}$$

We make two claims regarding these subsets. (Note that $t \geq d + 1$, which is not hard to see.)

Claim 1. If $w \leq t/2$ then $|C^{\mathrm{p}}_{\geq w}| + \left\lfloor \frac{|C_{<w}|}{\ell} \right\rfloor \leq \binom{t}{w}$.

Claim 2. If $w \geq \frac{2(t-\lfloor d/\ell \rfloor)}{\lfloor d/\ell \rfloor (d+2-\ell)}$, then $|C^{\mathrm{np}}_{\geq w}| \leq d+\ell-1$.

Let us complete the proof of the lemma before proving the claims. Define

$$\begin{aligned} w &= \left\lceil \frac{2(t-\lfloor d/\ell \rfloor)}{\lfloor d/\ell \rfloor (d+2-\ell)} \right\rceil \\ \bar{w} &= \frac{2t}{\lfloor d/\ell \rfloor (d+2-\ell)}. \end{aligned}$$

Because $d \geq \min\{\ell+2, 2\ell\}$, we have $w < \bar{w} \leq \frac{t}{2}$. Noting that the function $(te/w)^w$ is increasing in w when $w \in [0, \bar{w}]$, from Claims 1 and 2 we obtain

$$\begin{aligned} N &= \left(|C^{\mathrm{p}}_{\geq w}| + |C_{<w}|\right) + |C^{\mathrm{np}}_{\geq w}| \\ &\leq \left(\ell\left(|C^{\mathrm{p}}_{\geq w}| + \left\lfloor \frac{|C_{<w}|}{\ell} \right\rfloor\right) + (\ell-1)\right) + d + \ell - 1 \\ &\leq \ell\binom{t}{w} + d + 2\ell - 2 \\ &\leq \ell(te/w)^w + d + 2\ell - 2 \\ &\leq \ell(te/\bar{w})^{\bar{w}} + d + 2\ell - 2. \end{aligned}$$

Inequality (22) follows.

We now prove Claim 1. For each set $\mathbf{M}^j$, $j \in C^{\mathrm{p}}_{\geq w}$, collect exactly one private w-subset of $\mathbf{M}^j$ and put it in the collection $\mathcal{P}_1$; hence, $|\mathcal{P}_1| = |C^{\mathrm{p}}_{\geq w}|$. Let T be an arbitrary ℓ-subset of $C_{<w}$. Then, there must exist $j \in T$ such that $\mathbf{M}^j$ is **not** a subset of any set in $\mathcal{P}_1 \cup \left\{\mathbf{M}^j \mid j \in C_{<w} \setminus T\right\}$. Otherwise, because $\ell < d$, $\mathbf{M}[T]$ will be covered by $\mathbf{M}[S]$ for some $S \subseteq [N]$ with $|S| \leq d$. We refer to such j as a *representative* of T. For each T, pick an arbitrary representative of T and call it *the* representative of T. Partition $C_{<w}$ into $\left\lfloor \frac{|C_{<w}|}{\ell} \right\rfloor$ ℓ-subsets plus possibly one extra sub-set whose size is less than ℓ. Let $\mathcal{P}_2$ be the collection of all $\mathbf{M}^j$ where j are the representatives of the first $\left\lfloor \frac{|C_{<w}|}{\ell} \right\rfloor$ subsets. Then, $\mathcal{P}_1 \cup \mathcal{P}_2$ is a Sperner family, each of whose members is of cardinality at most w. For $w \leq t/2$, it is well-known (see, e.g., [2]) that $|\mathcal{P}_1 \cup \mathcal{P}_2| \leq \binom{t}{w}$. Because $|\mathcal{P}_2| = \left\lfloor \frac{|C_{<w}|}{\ell} \right\rfloor$ and $|\mathcal{P}_1| = |C^{\mathrm{p}}_{\geq w}|$, Claim 1 follows.

To prove Claim 2, we need a technical result stated in Claim 3 below.

Claim 3. Let $T = \{j_1, \cdots, j_\ell\}$ be an arbitrary set of ℓ different members of $C^{\mathrm{np}}_{\geq w}$. For any non-negative integer $k \leq d/\ell - 1$ and any column set $D \subseteq [N] - T$ such that $|D| = k\ell$, we have

$$|\mathbf{M}[T] \setminus \mathbf{M}[D]| \geq (d - (k+1)\ell + 1)w + 1.$$

To prove the claim, assume to the contrary that

$$|\mathbf{M}[T] \setminus \mathbf{M}[D]| \leq (d - (k+1)\ell + 1)w$$

for some set D and integer k satisfying the conditions in the claim. For every $i \in [\ell]$, define

$$\begin{aligned} C_i &:= \mathbf{M}^{j_i} \setminus (\mathbf{M}[D] \cup \mathbf{M}[\{j_1, \ldots, j_{i-1}\}]). \\ x_i &:= \left\lfloor \frac{|C_i|}{w} \right\rfloor \\ y_i &:= |C_i| \bmod w. \end{aligned}$$

Then,

$$\begin{aligned}(d-(k+1)\ell+1)w &\geq |\mathbf{M}[T]\setminus\mathbf{M}[D]|\\ &= \sum_{i=1}^{\ell}|C_i|\\ &= \sum_{i=1}^{\ell}(x_i w+y_i)\\ &= w\left(\sum_{i=1}^{\ell}x_i\right)+\sum_{i=1}^{\ell}y_i.\end{aligned}$$

Partition C_i into x_i parts of size w each and one part of size $y_i \leq w-1$. First, consider the case when $\sum_{i=1}^{\ell} y_i > 0$; then, $\sum_{i=1}^{\ell} x_i \leq d-(k+1)\ell$. Because $\mathbf{M}^{j_i}$ has no private w-subset (and thus no private y_i-subset), the set C_i can be covered by at most x_i+1 columns of $\mathbf{M}$; the union $\bigcup_{i\in[\ell]} C_i$ can thus be covered by at most $\sum_{i=1}^{\ell} x_i+\ell \leq d-k\ell$ columns of $\mathbf{M}$. Those $d-k\ell$ columns covering the C_i along with $k\ell$ columns $\mathbf{M}^j$, $j\in D$ cover $\mathbf{M}[T]$ completely, which is a contradiction. Second, when $\sum_{i=1}^{\ell} y_i = 0$ we only need at most $\sum_{i=1}^{\ell} x_i \leq d-(k+1)\ell+1 \leq d-k\ell$ columns to cover the C_i. The same contradiciton is reached.

Finally we are now ready to prove Claim 2. Suppose $|C^{\mathrm{np}}_{\geq w}| \geq d+\ell$. Consider $d+\ell$ columns $j_1,\ldots,j_{d+\ell}$ in $C^{\mathrm{np}}_{\geq w}$. For $k=0,1,\cdots,\lfloor d/\ell\rfloor-1$, define $D_k=\{j_1,\cdots,j_{k\ell}\}$ and $T_k=\{j_{k\ell+1},\cdots,j_{(k+1)\ell}\}$. ($D_0=\emptyset$.) Then, noting Claim 3, we have

$$\begin{aligned}t &\geq \mathbf{M}[\{j_1,\ldots,j_{d+\ell}\}]\\ &\geq \sum_{k=0}^{\lfloor d/\ell\rfloor-1}|\mathbf{M}[T_k]\setminus\mathbf{M}[D_k]|+|\mathbf{M}[\{j_{d+1},\cdots,j_{d+\ell}\}]\setminus\mathbf{M}[\{j_1,\ldots,j_d\}]|\\ &\geq \sum_{k=0}^{\lfloor d/\ell\rfloor-1}\left[\big(d-(k+1)\ell+1\big)w+1\right]+1\\ &= w\lfloor d/\ell\rfloor\left[d+1-\ell(\lfloor d/\ell\rfloor+1)/2\right]+\lfloor d/\ell\rfloor+1\\ &\geq \frac{1}{2}w\lfloor d/\ell\rfloor(d+2-\ell)+\lfloor d/\ell\rfloor+1,\end{aligned}$$

which contradicts the assumption that $w \geq \frac{2(t-\lfloor d/\ell\rfloor)}{\lfloor d/\ell\rfloor(d+2-\ell)}$. □

Theorem 2.17. *For any non-negative integers d,ℓ,e_0,e_1,N where $N\geq d+\ell$, we have*

$$t(d,\ell,e_0,e_1,N)=\Omega\left(d\log\frac{N}{d+\ell-1}+e_0+de_1\right). \tag{23}$$

In particular, when $\ell=\Theta(d)$ we have

$$t(d,\Theta(d),e_0,e_1,N)=\Omega\left(d\log(N/d)+e_0+de_1\right). \tag{24}$$

Furthermore, when $d\geq\min\{\ell+2,2\ell\}$ the following holds

$$t(d,\ell,e_0,e_1,N)=\Omega\left(\frac{d^2/\ell}{\log(d/\ell)}\log\frac{N-d}{\ell}+e_0+de_1\right). \tag{25}$$

Proof. In light of inequalities (21) and (22) from Lemma 2.16, to prove (23) and (25) we only need to show that $t(d, \ell, e_0, e_1, N) = \Omega(e_0 + de_1)$. Consider a (d, ℓ, e_0, e_1)-list-disjunct matrix $\mathbf{M}$ with t rows and N columns. Consider two disjoint subsets of columns $S, T \subseteq [N]$ with $|S| = d$ and $|T| = \ell$. There must be a column $\mathbf{M}^j$ in T with at least $e_1 + 1$ ones in rows where all columns in S contain zeros. Now, swap j with some column in S which has not been swapped before, and repeat the reasoning. In the end, we get at least $d + 1$ columns, each of which has at least $e_1 + 1$ ones in some rows for which all the other d columns have zeros. Further more, after d columns have been swapped into S, the $d+1$st column we found in T has e_1+1 ones none of S has *after* removing up to e_0 rows with all zeros in S. Thus, $t \geq (d + 1)(e_1 + 1) + e_0$. □

2.5 Probabilistic upper bounds

We apply the usual trick: concatenate a random code of length n over an alphabet of size q with the identity code ID_q, where each of the N codewords is chosen randomly by selecting a uniformly random symbol at each position. Let $\mathbf{M}$ be the resulting binary matrix. We bound the probability that $\mathbf{M}$ is not (d, ℓ, e_0, e_1)-list-disjunct.

Fix $S, T \subseteq [N]$ with $|S| = d$, $|T| = \ell$, and $S \cap T = \emptyset$. We call the pair (S, T) "bad" if there exists a set $X \subseteq \mathbf{M}[T] \setminus \mathbf{M}[S]$ of size $|X| \leq e_0$ such that for *all* $j \in T$, $|\mathbf{M}^j \setminus (X \cup \mathbf{M}[S])| \leq e_1$. We will choose parameters so that

$$n(q - d) - e_0 \geq 2qe_1. \tag{26}$$

This way, if (S, T) is bad then there exists a set X of e_0 members of $[t]$ such that $|\mathbf{M}^j \setminus (X \cup \mathbf{M}[S])| \leq e_1$ for all $j \in T$. Fix a set X of e_0 members of $[t]$. Let x_i be the number of members of X coming from position i of the outter code. Then, $e_0 = x_1 + \cdots + x_n$. For any $j \in T$, conditioned on the codewords in S, we have

$$\mathrm{E}[|\mathbf{M}^j \setminus (X \cup \mathbf{M}[S])|] \geq \sum_{i=1}^{n} \frac{(q - d) - x_i}{q} = \frac{n(q - d) - e_0}{q}.$$

By Chernoff inequality,

$$\begin{aligned} \text{Prob}\left[|\mathbf{M}^j \setminus (X \cup \mathbf{M}[S])| \leq e_1\right] &\leq \exp\left(-\frac{1}{2}\left(1 - \frac{e_1 q}{n(q - d) - e_0}\right)^2 \frac{n(q - d) - e_0}{q}\right) \\ &\leq \exp\left(-\frac{n(q - d) - e_0}{8q}\right). \end{aligned}$$

Since the codewords in T were chosen indepenently, by the union bound we have

$$\text{Prob}[(S, T) \text{ is bad}] \leq \binom{nq}{e_0} \exp\left(-\frac{n(q - d) - e_0)\ell}{8q}\right),$$

and hence

$$\text{Prob}[\mathbf{M} \text{ is not } (d, \ell, e_0, e_1)\text{-list-disjunct}] \leq \binom{N}{d + \ell}\binom{d + \ell}{d}\binom{nq}{e_0} \exp\left(-\frac{n(q - d) - e_0)\ell}{8q}\right).$$

To simplify the above expression, we pick

$$q = 2d \tag{27}$$

and choose n such that $n(q - d) - e_0 = nd - e_0 \geq nd/2$, which is the same as

$$nd \geq 2e_0. \tag{28}$$

With these choices, $\exp\left(-\frac{n(q-d)-e_0)\ell}{8q}\right) \le \exp\left(-n\ell/32\right)$ and thus

$$\text{Prob}[\mathbf{M} \text{ is not } (d,\ell,e_0,e_1)\text{-list-disjunct}] \le \binom{N}{d+\ell}\binom{d+\ell}{d}\binom{2nd}{e_0}\exp\left(-n\ell/32\right).$$

We bound the binomial product as follows.

$$\begin{aligned}\binom{N}{d+\ell}\binom{d+\ell}{d}\binom{2nd}{e_0} &< \exp\left((d+\ell)\log\frac{Ne}{d+\ell} + d\log\frac{(d+\ell)e}{d} + e_0\log\frac{2nde}{e_0}\right)\\ &= \exp\left(d\log\frac{Ne^2}{d} + \ell\log\frac{Ne}{d+\ell} + e_0\log\frac{2end}{e_0}\right).\end{aligned}$$

In summary, we just proved the following lemma

Lemma 2.18. *Let e_0, e_1, d, ℓ, N be given. If n is a positive integer such that*

$$nd \ge 2e_0 + 4de_1$$

and that

$$d\log\frac{Ne^2}{d} + \ell\log\frac{Ne}{d+\ell} + e_0\log\frac{2end}{e_0} \le n\ell/32$$

then there exists a $2dn \times N$ matrix which is (d,ℓ,e_0,e_1)-list-disjunct.

The following theorem follows easily.

Theorem 2.19. *Let d, ℓ, e_0, e_1, N be given parameters.*

(a) If $\ell = \Omega(d)$, then there exists a $t \times N$ matrix $\mathbf{M}$ which is (d,ℓ,e_0,e_1)-list-disjunct where

$$t = O\left(d\log(N/d) + e_0 + de_1\right).$$

(b) If $\ell \le d$, then there exists a $t \times N$ matrix $\mathbf{M}$ which is (d,ℓ,e_0,e_1)-list-disjunct where

$$t = O\left((d^2/\ell)\log(N/d) + \min\{d, (d/\ell)\cdot\log(d/\ell)\cdot\log\log(d/\ell)\}\cdot e_0 + de_1\right)$$

Proof. The plan is to pick n such that the following three inequalities hold

$$n \ge 2e_0/d + 4e_1 \tag{29}$$

$$n\ell/64 \ge d\log\frac{Ne^2}{d} + \ell\log\frac{Ne}{d+\ell} \tag{30}$$

$$n\ell/64 \ge e_0\log\frac{2end}{e_0} \tag{31}$$

(a) Suppose $\ell \ge Cd$ for some fixed constant C. Inequality (30) holds if

$$n \ge \frac{64}{C}\log\frac{Ne^2}{d} + 64\log\frac{Ne}{d+Cd} = 64\frac{C+1}{C}\log\frac{N}{d} + 64(2/C + 1 - \log(1+C)).$$

Inequality (31) holds when $\frac{2end/e_0}{\log\frac{2end}{e_0}} \ge 128e/C$. Since the function $x/\log x$ is increasing for $x > 1$, the inequality holds when nd/e_0 is sufficiently large. Overall, it is clear that

$$n = \Omega\left(\log\frac{N}{d} + e_0/d + e_1\right)$$

is sufficient, which proves part (a) of the theorem.

(b) To satisfy inequality 30, we set

$$n = \Omega\left((d/\ell)\log(N/d)\right).$$

The tedious part comes from satisfying inequality (31).

On the one hand, because every $(d, \ell, 0, e_0 + e_1)$-list-disjunct matrix is a (d, ℓ, e_0, e_1)-list-disjunct matrix (Proposition 2.5), we could have set $e_1 = e_0 + e_1$ and $e_0 = 0$ so that inequality (31) does not have to be satisfied. If we set the parameters this way then

$$n = \Omega\left((d/\ell)\log(N/d) + e_0 + e_1\right)$$

is sufficient, which implies $t = O\left((d^2/\ell)\log(N/d) + d(e_0 + e_1)\right)$.

On the other hand, if e_0 is large then the above bound is not good. In this case we need to pick n to satisfy (31), which is equivalent to

$$\frac{2end/e_0}{\log(2end/e_0)} \geq 128ed/\ell.$$

Let $D = 128ed/\ell$, we want the minimum x for which $x/\log x \geq D$. Setting $x = \Omega(D \cdot \log(D) \cdot \log\log(D))$ is sufficient. Hence, in this case

$$n = \Omega\left((d/\ell)\log(N/d) + (1/\ell) \cdot \log(d/\ell) \cdot \log\log(d/\ell)\} \cdot e_0 + e_1\right)$$

and the conclusion follows.

□

Corollary 2.20. *For the d^r-list-disjunct matrices, we have $t(d, r, N) = O(d^2 \log(N/d) + rd)$.*

References

[1] D. J. BALDING AND D. C. TORNEY, *Optimal pooling designs with error detection*, J. Combin. Theory Ser. A, 74 (1996), pp. 131–140.

[2] B. BOLLOBÁS, *Combinatorics*, Cambridge University Press, Cambridge, 1986. Set systems, hypergraphs, families of vectors and combinatorial probability.

[3] M. CHERAGHCHI, *Noise-resilient group testing: Limitations and constructions*, in FCT, 2009, pp. 62–73.

[4] A. DE BONIS, L. GĄSIENIEC, AND U. VACCARO, *Optimal two-stage algorithms for group testing problems*, SIAM J. Comput., 34 (2005), pp. 1253–1270 (electronic).

[5] A. G. D′YACHKOV AND V. V. RYKOV, *Bounds on the length of disjunctive codes*, Problemy Peredachi Informatsii, 18 (1982), pp. 7–13.

[6] ———, *A survey of superimposed code theory*, Problems Control Inform. Theory/Problemy Upravlen. Teor. Inform., 12 (1983), pp. 229–242.

[7] A. G. D′YACHKOV, V. V. RYKOV, AND A. M. RASHAD, *Superimposed distance codes*, Problems Control Inform. Theory/Problemy Upravlen. Teor. Inform., 18 (1989), pp. 237–250.

[8] P. ERDŐS, P. FRANKL, AND Z. FÜREDI, *Families of finite sets in which no set is covered by the union of r others*, Israel J. Math., 51 (1985), pp. 79–89.

[9] Z. FÜREDI, *On r-cover-free families*, J. Combin. Theory Ser. A, 73 (1996), pp. 172–173.

[10] KAINKARYAM, *Pooling in high-throughput drug screening*, Current Opinion in Drug Discovery & Development, 12 (2009), pp. 339–350.

[11] R. KAINKARYAM AND P. WOOLF, *poolhits: A shifted transversal design based pooling strategy for high-throughput drug screening*, BMC Bioinformatics, 9 (2008).

[12] H. Q. NGO AND D.-Z. DU, *A survey on combinatorial group testing algorithms with applications to DNA library screening*, in Discrete mathematical problems with medical applications (New Brunswick, NJ, 1999), vol. 55 of DIMACS Ser. Discrete Math. Theoret. Comput. Sci., Amer. Math. Soc., Providence, RI, 2000, pp. 171–182.

[13] A. Q. NGUYEN AND T. ZEISEL, *Bounds on constant weight binary superimposed codes*, Problems Control Inform. Theory/Problemy Upravlen. Teor. Inform., 17 (1988), pp. 223–230.

[14] A. M. RASHAD, *Random coding bounds on the rate for list-decoding superimposed codes*, Problems Control Inform. Theory/Problemy Upravlen. Teor. Inform., 19 (1990), pp. 141–149.

[15] X. XIN, J.-F. F. RUAL, T. HIROZANE-KISHIKAWA, D. E. HILL, M. VIDAL, C. BOONE, AND N. THIERRY-MIEG, *Shifted transversal design smart-pooling for high coverage interactome mapping.*, Genome research, 19 (2009), pp. 1262–1269.