Bounds on Unique Neighbor Codes

Nati Linial and Edan Orzech

1 Introduction

By default, codes $\mathcal{C}$ that we consider here have length n and are binary, $\mathcal{C} \subseteq \{0,1\}^n$. As usual, we denote the *rate* of $\mathcal{C}$ by $R = R(\mathcal{C}) = \frac{1}{n}\log_2|\mathcal{C}|$ and its distance by $\mathrm{dist}(\mathcal{C}) = \min_{x\neq y, x,y\in\mathcal{C}} d_H(x,y)$, where d_H stands for Hamming distance. A fundamental open problem in coding theory seeks the best possible tradeoff between R and $1 \geq \delta \geq 0$. We refer to this as

Problem 1.1. *Determine, or estimate the real function*

$$R(\delta) = \limsup_{n\to\infty}\{R(\mathcal{C})|\mathcal{C} \subseteq \{0,1\}^n \ , \ \mathit{dist}(\mathcal{C}) \geq \delta n\}$$

A *linear code* is a linear subspace of the vector space $\mathbb{F}_2^n$, which we identify with $\{0,1\}^n$. Such a code is defined in terms of its *parity check matrix* A which is a $\lceil(1-R)n\rceil \times n$ binary matrix. Namely, $\mathcal{C} = \{x|Ax = 0\}$.

Let S be a nonempty set of columns in a binary matrix and let z be the sum over the integers of the columns in S. We say that the set S is 1-*free* if no entry of z equals 1, and we call S *even*, if all entries of z are even integers.

Definition 1.2. *Let A be a binary matrix.*

- *We let $\varepsilon(A)$ be the smallest cardinality of a nonempty even set of columns in A.*
- *We let $u(A)$ be the smallest cardinality of a nonempty 1-free set of columns in A.*
- *The maximum value of $\varepsilon(A)$ over all binary $m \times n$ matrices is denoted $\varepsilon(m,n)$.*
- *The maximum value of $u(A)$ over all binary $m \times n$ matrices is denoted $u(m,n)$.*

Regarding linear codes, the question analogous to Problem 1.1 is

Problem 1.3. *Determine, or estimate the real function*

$$R_L(\delta) := \limsup_{n\to\infty}\{R|\ \textit{there exists a } \lceil(1-R)n\rceil \times n \textit{ binary matrix with } \varepsilon(A) \geq \lfloor\delta n\rfloor\}$$

in other words, $R_L(\delta)$ is the smallest real R such that

For any $\rho > R$ and large enough n, every $\lceil(1-\rho)n\rceil \times n$ binary matrix has an even set of $\leq \delta n$ columns

Message-passing algorithms offer a powerful approach to the *decoding* problem of linear codes $\mathcal{C} = \{x|Ax = 0\}$. In the analysis of such algorithms, A is viewed as the bipartite adjacency matrix of the code's *factor graph*, a bipartite graph $(L, R; E)$, where L is the set of A's columns and R its set of rows. Upon receiving a message $y \notin \mathcal{C}$ the receiver calculates $Ay \neq 0$ and seeks to change y minimally so as to arrive at a word in $\mathcal{C}$. We refer the reader to [1, 2] for detailed discussion of such algorithms and only mention that the *unique neighbor property* plays a key role in the analysis. Namely, the property that for some appropriately set bound B, for every subset $S \subset L$ of cardinality $|S| \leq B$ there is a vertex $v \in R$ that has exactly one neighbor in S. Equivalently, every 1-free set of columns in A must have cardinality bigger than B.

In this context we ask:

Problem 1.4. *Determine, or estimate the real function*

$$R_U(\delta) := \limsup_{n\to\infty}\{R|\ \textit{there exists a } \lceil(1-R)n\rceil \times n \textit{ binary matrix with } u(A) \geq \lfloor \delta n \rfloor\}$$

in other words, $R_L(\delta)$ is the smallest real R such that

For any $\rho > R$ and large enough n, every $\lceil(1-\rho)n\rceil \times n$ binary matrix has a 1-free set of $\leq \delta n$ columns

Clearly,

$$R(\delta) \geq R_L(\delta) \geq R_U(\delta) \text{ for all } \delta \geq 0$$

At present, we cannot even rule out the possibility that R and R_L are, in fact, identical. It is easily verified that (i) All three are nonincreasing functions of $\delta > 0$, and (ii) $R(0) = R_L(0) = R_U(0) = 1$.

It is also well known that $R(\delta), R_L(\delta) > 0$ for $\frac{1}{2} > \delta$ and $R(\delta), R_L(\delta) = 0$ for $\delta \geq \frac{1}{2}$.

Our main objective is to prove that the strict inequality $R_L(\delta) > R_U(\delta)$ holds for at least some of the range $\frac{1}{2} > \delta > 0$. More specifically that R_U vanishes already at some $\frac{1}{2} > \delta_0$. Concretely, we state

Conjecture 1.5. *There is some function $f = f(n) = o(n)$ and some $\epsilon_0 > 0$ such that every $n \times (n + f(n))$ binary matrix has a 1-free set of $\leq (\frac{1}{2} - \epsilon_0)n$ columns.*

Let A be the parity check matrix of a linear code $\mathcal{C} \subseteq \{0,1\}^n$. Of course $\mathcal{C}$ remains invariant under elementary row operations on A. Also distances among vectors in $\mathcal{C}$ remain unchanged as A's columns get permuted. Consequently, in the study of $R_L(\delta)$ as in Problem 1.3, there is no loss of generality in assuming that A is in *standard form*, i.e., its first n columns form an order-n identity matrix. We pose:

Problem 1.6. *Let n, K be positive integers, and let A be a binary $n \times (n + K)$ matrix A whose first n columns form the order-n identity matrix. How large can $u(A)$ be?*

Remark 1.7. *The* weight *or* sum *of a row is the number of its* 1*-entries.*

2 Our New Results

Our work addresses Problems 1.4 and 1.6. Problems 1.1 and 1.3 are mentioned here for context only.

1. We prove Conjecture 1.5, and even with $f(n) = 0$ when all (integer) row sums in A are bounded from below (Theorem 3.1).
2. We show (Theorem 6.1) that Conjecture 1.5 cannot hold unless $f(n) > \log_2(n)$.
3. We answer Problem 1.6 in full (Theorem 4.2).
4. Clearly $\varepsilon(m,n) \geq u(m,n)$ for all m and n, and there exist $n > m$ for which the inequality is strict.

Remark 2.1. *Assuming that Conjecture 1.5 is valid, it is not clear which proof technique can establish it. As Theorem 6.1 shows, methods that work for square matrices and matrices with only a few more columns than rows as in Theorem 3.1 are not likely to deliver a full answer.*

3 The Effect of Lower Bounds on the Row Weights

As the following theorem demonstrates, row weights in A are very significant in our problem. It seems harder to find small 1-free sets in sparse matrices. Thus the proof of Theorem 6.1 uses matrices in which all row sums equal 3.

Theorem 3.1. *Let A be a binary $n \times n$ matrix in which every row weighs at least $c = 9$. Then there is a set of $\leq 0.49n$ columns in A in whose sum over the integers all entries are at least 2. However, the analogous statement is invalid for $c \leq 4$.*

Proof. Let us sample a random set of columns by picking every column independently with probability ρ. We denote by X_0, X_1 be the (random) sets of rows of weight zero, resp. one. Next we correct every row of weight zero/one by adding two/one column to make its weight ≥ 2. This yields a set of columns as described in the proposition of cardinality $\leq (\rho + 2\mathbb{E}(X_0) + \mathbb{E}(X_1))n$. Note that

$$\mathbb{E}(X_0) \leq n(1-\rho)^c + o(n) \; ; \quad \mathbb{E}(X_1) \leq nc\rho(1-\rho)^{c-1} + o(n)$$

The first part now follows by observing that this expression is $< 0.481n$ for $\rho = 0.4$.

For the second part, consider the $n \times n$ binary matrix whose rows are comprised of all n cyclic rotations of the vector $1^4 0^{n-4}$. □

The second part of the claim tells us that if Conjecture 1.5 is true, then the extra $f(n)$ columns play a critical role in the existence of small 1-free sets of columns. Theorem 6.1 further asserts that corollary.

We can generalize the above by defining a the (upper bound on the) expectation of number of columns that will be picked as a function of c, ρ. Define $h_1 : \mathbb{R} \times [0,1] \to \mathbb{R}$ by

$$h_1(c,\rho) = \rho + (1-\rho)^c + c\rho(1-\rho)^{c-1} \tag{1}$$

such that the expression from before matches $h_1(c,\rho) \cdot n$. We can do this with a 2-stage strategy as well: first pick every column with probability ρ, then pick each of the remaining columns with probability θ, and then correct the induced rows that weigh 0 and 1. We then define 4 variables to indicate rows that weigh 0/1: X_0, X_1 are rows that weigh 0/1 in the first round of column-picking, and Y_0, Y_1 are those that weigh 0/1 in the second round, *excluding* the first round. We get a function $h_2 : \mathbb{R} \times [0,1]^2 \to \mathbb{R}$ defined by

$$h_2(c,\rho,\theta) = \rho + (1-\rho)\theta + 2\left((1-\rho)(1-\theta)\right)^c + (1-\rho)^c c\theta(1-\theta)^{c-1} + c\rho(1-\rho)^{c-1}(1-\theta)^{c-1} \tag{2}$$

Namely $h_2(c,\rho,\theta)$ upper-bounds $\rho + (1-\rho)\theta + 2\mathbb{E}(X_0Y_0) + \mathbb{E}(X_1Y_0 + X_0Y_1)$. However, after regrouping we actually get that $h_2(c,\rho,\theta) = h_1(c, \rho + \theta - \rho\theta)$. It is well-defined since $\rho + \theta - \rho\theta \in [0,1]$ in the domain $[0,1]^2$.

We can generalize this even further: define $h_m(c,\rho_1,...,\rho_m)$ to be the corresponding upper bound for the analogous m-stage procedure. It can be shown with a similar argument that for every m we have $h_m(c,\rho_1,...,\rho_m) = h_1\left(c, 1 - \prod_{i=1}^m (1-\rho_i)\right)$.

4 Matrices in Standard Form

Here we address Problem 1.6, and provide an upper bound on u for matrices in standard form for every m, n, which is also tight for infinitely many values of m, n. First we define a function:

Definition 4.1. *The maximum value of $u(A)$ over all binary $m \times n$ matrices A in standard form is denoted $u_I(m,n)$.*

A binary linear code is defined as $C = \{x | Ax = 0\}$. We refer to the binary matrix A as a *parity check matrix* of C. It is an easy and standard fact that by applying elementary row operations A can be made to take the form $A = [I_n | B]$. This prompts our next result.

Theorem 4.2. *For every positive integer k and $n \to \infty$, every binary $n \times (n+k)$ matrix of the form $A = [I_n|B]$ has a 1-free set of at most $\frac{n}{H_k} + O(k)$ columns where $H_k = \sum_{\ell=1}^k \frac{1}{\ell}$ is the k-th harmonic sum. The bound is tight, that is $u_I(n, n+k) = \frac{n}{H_k} + O(k)$.*

Proof. We denote by $\langle u, v \rangle = \sum u_i v_i = 1$ the integer inner product of the vectors u and v, and $|u| := \langle u, u \rangle = ||u||_1$. To extend a given set $S \subset [k]$ of columns in B to a 1-free set of columns in A, we observe which coordinates in the integer sum of these columns equals 1. We then must add all the corresponding columns in I_n to make the set 1-free. For a binary vector $u \in \{0,1\}^k$, let x_u be the number of rows in B that equal u. Clearly, x_u is a nonnegative integer, but we only require that $x_u \geq 0$ and $\sum_{u \in \{0,1\}^k} x_u = n$.

If s is the indicator vector of S, then we must add at least $\sum\{x_u|\langle u,s\rangle=1\}$ columns from I_n to reach a 1-free set of columns. We get a lower bound on $u_I(n,n+k)$ from the following linear program. This is only a lower bound, since the x_u are not required to be integers. It can however, be easily verified that optimum for integers and for real x_u hardly differ. Let M be the $2^k\times 2^k$ matrix whose rows and columns are indexed by $\{0,1\}^k$. For $u,v\in\{0,1\}^k$ we let $M[u,v]=1$ iff $\langle u,v\rangle=\sum u_iv_i=1$ (integer addition).

$$\begin{aligned} u_I(n,n+k)-O(k) = &\max y\\ \text{subject to}\quad &M\mathbf{x}\geq \mathbf{1}\cdot y,\\ &\langle \mathbf{x},1\rangle = n \text{ and } \mathbf{x}\geq 0\end{aligned}$$

We pass to the dual and find the 2^k-dimensional vector w with

$$w_{\mathbf{0}}=0 \text{ and } w_u=\frac{1}{\binom{k-1}{|u|-1}} \text{ for every } u\neq\mathbf{0} \text{ in } \{0,1\}^k$$

It follows that if $v\in\{0,1\}^k$ with $|v|=j$ for some $k\geq j\geq 1$ then

$$(wM)_v=\sum_{i\geq 1}\frac{1}{\binom{k-1}{i-1}}j\binom{k-j}{i-1}=\frac{j!(k-j)!}{(k-1)!}\sum_{i\geq 1}\binom{k-i}{j-1}=\frac{j!(k-j)!}{(k-1)!}\binom{k}{j}=k.$$

And $(wM)_{\mathbf{0}}=0$. In other words, $wM=k(\mathbf{1}-e_{\mathbf{0}})$, and hence $k\geq wM\mathbf{x}$. The first equality follows from the definition. The second only involves reorganizing terms. The third one uses the standard and easy fact that for all positive integers $s\leq N$ there holds

$$\sum_{r\leq N}\binom{r}{s}=\binom{N+1}{s+1}$$

Also

$$\langle w,\mathbf{1}\rangle=\sum_{i=1}^{k}\frac{\binom{k}{i}}{\binom{k-1}{i-1}}=kH_k.$$

It follows that

$$\frac{n}{H_k}\geq u_I(n,n+k)-O(k).$$

The reverse inequality follows by letting

$$\mathbf{x}\coloneqq n\frac{w}{kH_k}$$

and observing that with similar calculations we get $M\mathbf{x}\geq y$ and $\langle\mathbf{x},\mathbf{1}\rangle=n$. □

5 How Far Do ε and u Coincide?

In this section we investigate the question its title suggests. We refer to the dimensions of the matrices here as $n,n+k$. We start from the case of $k=1$, prove that $\varepsilon(n,n+1)=u(n,n+1)=n+1$, and prove a characterization all matrices that achieve this bound. We then proceed to the more general case of $k\leq\log n$, by proving Theorem 6.1. Afterward, we return to small values of k and provide a more detailed analysis of ε,u.

The following proposition will be used throughout this section:

Proposition 5.1. *Every $n\times(n+k)$ binary matrix A has a set of at most $(1+\frac{1}{2^k-1})\frac{n+k}{2}$ columns that sum to zero* mod 2.

Note that rows of weight 1 in A can be eliminated. If $a_{ij} = 1$ while $a_{ik} = 0$ for all $k \neq j$, then column j does not belong to any 1-free set of columns. Therefore both ε and u remain unchanged if we remove row i and column j from A. Such a step is called an *elementary collapse* (the terminology comes from topology), and repeat this step until no more elementary collapses are possible. Note that the resulting matrix does not depend on the order at which we carry out the collapses. All-zero rows can also with no change to be eliminated with no change to ε and u. Therefore, we can and will henceforth assume that

$$\text{Every row of } A \text{ has weight } \geq 2. \tag{3}$$

Let us make the following easy observation:

Proposition 5.2. *If $k \geq 2$, then every $n \times (n+k)$ binary matrix A has at least two distinct 1-free sets of columns.*

This is obvious since the right kernel of A over $\mathbb{F}_2$ has dimension $\geq k \geq 2$.

This conclusion is no longer valid for $k = 1$. Let $A = A_T$ be the edges vs. vertices incidence matrix of a tree T on $n+1$ vertices. Since every row of A weighs 2, the full set of A's columns is 1-free. Also, since T is connected, no proper subset of the columns is 1-free. It turns out that up to collapsing no other such matrices exist.

Proposition 5.3. *Let A be an $n \times (n+1)$ binary matrix. If $u(A) = n+1$, then $A = A_T$ for some tree T on $n+1$ vertices.*

Proof. Let $G = (V, E)$ be the hypergraph whose edges vs. vertices incidence matrix is A. An edge in E of size 2 (resp. ≥ 3) is considered *light* (resp. *heavy*). Let L be the graph with vertex set V and all light edged in E. Our claim is that $L = G$. For then G is a connected graph on $n+1$ vertices with n edges, namely it is a tree, as claimed.

Note that at least *some* edges in E are light, for otherwise every row in A weighs at least 3, and every set of n columns of A is 1-free, contrary to our assumption. If $L \neq G$, so that G has some heavy edges, then L has $n+1$ vertices and at most $n-1$ edges, and is, therefore, disconnected. Let $V_1, ..., V_k$ (with $k \geq 2$) be the vertex sets of L's connected components. Note that for every $1 \leq i \leq k$, every 1-free set of columns is either disjoint from V_i or contains it. In other words, each V_i is an *atom* which every 1-free set either avoids or uses whole.

Define a hypergraph $G' = (V', E')$, where $V' = \{v_1, ..., v_k\}$ and E' has one edge per every heavy edge $e \in E$. Namely, $\{v_i | V_i \cap e \neq \emptyset\}$. In words, G' is the hypergraph that results from G by shrinking each V_i to a single new vertex v_i. Let A' be the edges vs. vertices matrix of G'. Every 1-free set of columns S in A' yields a 1-free set in A by "inflating" each $v_i \in S$ to V_i. By assumption, A has only one 1-free set, and distinct 1-free sets in A' give rise to distinct 1-free sets in A. Consequently, A' has exactly one 1-free set that is comprised of all its columns. By Proposition 5.2 A' must have at least $k-1$ rows. Since L has $n+1$ vertices and k connected components, it has at least $n+1-k$ edges, and consequently A' has at most $k-1$ rows.

We conclude that A' is a $(k-1) \times k$ binary matrix whose one and only 1-free set is the set of all its columns. This suggests that we finish the proof by induction, except that A' may have rows of weight 1. Previously, we dealt with such rows by an elementary collapse and the fact that a set of columns that is 1-free in the reduced matrix is also 1-free in the original matrix. The row in A' of the heavy edge $e \in E$ has weight 1 iff $e \subseteq V_i$ for some i. Let us remove this row and consider a 1-free set S in the resulting matrix. We claim that S is 1-free in A' as well. Indeed, if $v_i \notin S$, then in the submatrix of A' that corresponds to S the row of e is all zeros, and if $v_i \in S$ then the sum of this row is $|e| \geq 3$.

It follows by induction that A' has no row of weight 1, and since heavy edges have weight ≥ 3, and again by induction A' is empty, proving the claim. $\square$

6 The Logarithmic Lower Bound

6.1 Overview of the Proof

We prove next that $u(n - \log_2 n - 1, n - 1) = \varepsilon(n - \log_2 n - 1, n - 1) = \frac{n}{2}$ for infinitely many values of n. Concretely,

Theorem 6.1. *For every integer $k \geq 2$ there holds*

$$u(2^k - 1 - k, 2^k - 1) = \varepsilon(2^k - 1 - k, 2^k - 1) = 2^{k-1},$$

Moreover,

$$u((2^k - 1)m - k, (2^k - 1)m) = \varepsilon((2^k - 1)m - k, (2^k - 1)m) = 2^{k-1}m$$

holds for every two integers $k \geq 2$ and $m \geq 1$.

We prove in full only the case of $m = 1$. The $m > 1$ case does not add much insight beyond the $m = 1$ case, so we only sketch its proof. The proof follows by an inductive construction of binary $2^k - 1 - k \times 2^k - 1$ matrices A_k such that $u(A_k) = \varepsilon(A_k) = 2^{k-1}$. The matrix A_k has the following form:

$$A_k = \left(\begin{array}{c|c|c|c} P_{k-2} & \mathbf{0} & Q_{k-2} & R_{k-2} \\ \hline \mathbf{0} & \multicolumn{2}{c|}{A_{k-1}} & \mathbf{0} \end{array}\right) \tag{4}$$

The sizes of these matrices are as follows:

- P_{k-2} is a $2^{k-1} - 1 \times 2^{k-1} - 1$ matrix.
- Q_{k-2} is a $2^{k-1} - 1 \times k - 1$ matrix.
- R_{k-2} is a $2^{k-1} - 1 \times 1$ matrix.
- A_{k-1} is a $2^{k-1} - k \times 2^{k-1} - 1$ matrix.

We denote by $\mathrm{col}(X)$ the set of X's columns. Let S be a 1-free set in A_k. We consider two cases.

1. If $S \cap \mathrm{col}(A_{k-1}) \neq \emptyset$, then by induction, $|S \cap \mathrm{col}(A_{k-1})| \geq 2^{k-2}$. By considering the top part of the matrix we conclude that $|S \setminus \mathrm{col}(A_{k-1})| \geq 2^{k-2}$ as well, so that $|S| \geq 2^{k-1}$, as claimed.
2. Otherwise, S and $\mathrm{col}(A_{k-1})$ are disjoint and we prove that $|S| \geq 2^{k-1}$ by considering the upper part of A_k, namely $\mathrm{col}(P_{k-2}) \cup \mathrm{col}(R_{k-2})$.

The question is how to construct $P_{k-2}, Q_{k-2}, R_{k-2}$. For that we define a hypergraph G_k for every k, with $2^{k+1} - 1$ vertices whose hyperedges are the columns in P_k, Q_k, R_k (where a column j has 1 in coordinate i iff $v_i \in e_j$).

An important remark is that A_k has a special structure: it is a generator matrix of the generalized $[2^k - 1, 2^k - 1 - k, 3]_2$ Hamming code, which is also a parity check for the shortened Hadamard code. Furthermore, it contains only rows of Hamming weight 3 (but not all of them, according to [3]), which the minimal nonzero weight possible for those codes. Moreover, it can be achieved from the known generator matrix

$$\left(\begin{array}{c|c} I_{2^k-1-k} & C \end{array}\right) \tag{5}$$

(where C contains all length-k rows of weight ≥ 2) using a greedy algorithm. It is nice to notice that, because Hamming codes have the (almost) smallest minimum distance possible, while Hadamard codes have the largest minimum distance possible for linear codes. In some sense, using that every row in A_k weighs exactly 3, the small minimum distance of the (generalized) Hamming code, allows the unique-neighbor property and linear dependence (over $\mathbb{F}_2$) to coincide. The large minimum distance of the Hadamard code then allows the properties' values to reach their upper bound, and as a result we are able to show that $u(n - \log_2 n, n) = \frac{n}{2}$ for infinitely many n's.

Further note that from Proposition 5.1, the constructions above are the "hardest" matrices to find either an even or a 1-free set of columns in them. Moreover, the weights of the rows are almost minimal. If every row weighs 2, then the matrix is an edge-vertex adjacency matrix of a simple graph, where only 2 extra vertices are sufficient to find a small 1-free set (in this case a small connected component). This provides the observation that the "hardest" matrices are sparse once again. Investigating this special set of matrices seems as a promising direction where there is more literature, and progress can be made.

We remark that for every $k, m = 1$, one cannot achieve a 1-free set of A_k using only columns from the part of P_{k-2}, since we can construct A_k to be an upper triangular matrix (up to the last k columns), and it is straightforward to see that other columns would be needed as well. We use that fact (which will be proved) to simplify further the proof.

6.2 The Proof

In this section we use some notations of set theory. $\mathbb{N}$ includes 0, and every $n \in \mathbb{N}$ is defined to be $n = \{0, ..., n-1\}$ (and $0 = \emptyset$). For a set of sets S, $\bigcup S := \bigcup_{s \in S} s$. Let $\mathcal{P}(X)$ denote the powerset of a set X. In addition, we use the terms "edge" and "hyperedge" interchangeably here. Also let $\deg_G v$ denote the degree of v in the hypergraph G.

Definition 6.2. *For every $k \in \mathbb{N}$, define $G_k = (V_k, E_k)$ in the following way:*

- $V_k = \mathcal{P}(k+1) \setminus \{\emptyset\}$.
- $E_k = P_k \sqcup Q_k \sqcup R_k$ *is a disjoint union of 3 types of edges, where*
  - $P_k = \left\{\bigcup_{i \in k} \{v \cup \{i\}\} \mid v \in V_k\right\}$. *Those will be also called type-p edges.*
  - $Q_k = \{e_i \mid i \in k+1\}$, *such that* $e_i = \{v \in V_k \mid \min v = i\}$. *Those will be also called type-q edges.*
  - $R_k = \{e_r\}$, *where* $e_r = \{v \in V_k \mid |v| = 1\}$ *(here $|v|$ is the cardinality of v as a set). That will be also called a type-r edge.*

Basic properties of G_k can be deduced. $|V_k| = 2^{k+1} - 1$ by definition. We can also view G_k as 2 instances of G_{k-1}, where the first instance has the vertices $V'_{k-1} := \{v \in V_k \mid |v| > 1,\ \max v = k\}$, and the second instance has the vertices $V''_{k-1} := (V_k \setminus V'_{k-1}) \setminus \{\{k\}\}$. Also note that $\deg_G v = 3$ for every $v \in V_k$: v is a vertex in some edge in P_k, some edge in Q_k, and either an additional edge in P_k or the edge e_r. Moreover, $|P_k| = |V_k|$, as the function $v \mapsto \bigcup_{i \in k} \{v \cup \{i\}\}$ is bijective. We will use those notations in the following proof.

Proposition 6.3. *For every $k \geq 1$, for every subgraph $G' = (V_k, E')$ of G_k with $V(G') = V_k$ such that no vertex in G' has degree 1 has $|E' \setminus Q_k| \geq 2^k$. Furthermore, if $E' \cap P_k = \emptyset$, then $|E'| \geq 2^{k+1}$.*

Proof. We prove this by induction on $k \geq 1$. For $k = 1$ the correctness is clear. Suppose the claim is true for every $k' < k$, and we show that it is true for k. For the first part of the claim (namely $E' \cap P_k \neq \emptyset$), we split into cases:

1. $e_k, e_r \notin E'$: then by the definition of G_k, $\deg_{G'}\{k\} = 0$, so we can decompose V_k into V'_{k-1} and V''_{k-1}. The edges Q_k are shared among those vertices. R_k is not shared with V'_{k-1}, but the latter is compensated with the edge $\bigcup_{i \in k}\{\{k, i\}\}$. The edges P_k are straightforward divided between V'_{k-1}, V''_{k-1} as each $e \in P_k$ is a subset of only one of the 2 vertex subsets. Thus, G' defines 2 instances of subgraphs of G_{k-1} which both satisfy the premises of the claim. For those instances, Q_k constitutes their type-q edges (as in Definition 6.2). We have that the problem for the parameter k is reduced to 2 problems for the parameter $k-1$, and the uncounted edges are all in Q_k. Thus, by the induction hypothesis we have $|E' \setminus Q_k| \geq 2 \cdot 2^{k-1} = 2^k$.

2. $e_k \in E'$, $e_r \notin E'$: then the same argument of (1) holds, with the additional following observation. Since e_k was chosen, the only way to increase the degree of $\{k\} \in V_k$ from 1 to 2 (3 is not possible as $\deg_G\{k\} = 3$) is by having the edge $\bigcup_{i \in k}\{\{k, i\}\}$ in E' as well. Now, when looking at the 2

instances of subgraphs of G_{k-1} (as described in case 1), the edge $\bigcup_{i\in k}\{\{k,i\}\}$ corresponds to the choice of the type-r edge of the first instance. This edge will be counted in both the original problem and in that reduction $k-1$ as the parameter. Therefore, by the induction hypothesis we get here as well that $|E' \setminus Q_k| \geq 2^k$.

3. $e_k \notin E'$, $e_r \in E'$: then $\bigcup_{i\in k}\{\{k,i\}\} \in E'$, so similarly to cases 1,2, the problem is now reduced into 2 instances of the problem for the parameter $k-1$, where $\bigcup_{i\in k}\{\{k,i\}\}$ and e_r correspond to the type-r edge of the first and second instances (respectively). Thus by the induction hypothesis, $|E' \setminus Q_k| \geq 2 \cdot 2^{k-1} = 2^k$.

4. $e_k, e_r \in E'$: then we can assume that $\bigcup_{i\in k}\{\{k,i\}\} \notin E'$ (for otherwise we return to case 3, as e_k contains only $\{k\}$). Then, if $E' \cap Q_k = \{e_k\}$, we have only the second of the two instances described earlier, but with no type-q edges chosen, so from it we have $|E'| \geq 2^k$ immediately. Otherwise, $e_i \in E'$ for some $i < k$, so we again have two instances as in the previous cases, which again yield $|E'| \geq 2 \cdot 2^{k-1} = 2^k$, as required.

And this proves the first part of the proposition.

For the second part, suppose that $E' \cap Q_k = \emptyset$. Since $E' \neq \emptyset$, it follows using a standard induction on k that $\deg_{G'}\{k\} = 2$, therefore $e_r \in E'$ by the construction of G_k. When removing Q_k from G_k, $\deg_G v = 2$ for every $v \in V_k$, so again using a standard induction yields that $E' = P_k \cup R_k$, since $E' \neq \emptyset$. By the construction of E_k,

$$|E'| = |P_k| \cup |R_k| = |V_k| + 1 = 2^{k+1}$$

This concludes the second part of the claim, hence it is true for every $k \geq 1$. □

We are now ready to construct the matrix that achieves the bound stated in Theorem 6.1. For simplicity, we will abuse the notation of P_k, Q_k, R_k from Definition 6.2.

Definition 6.4. *For every $k \geq 2$, we define recursively A_k to be the following block matrix:*

- $A_2 = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}$.
- *Given $A_{k-1} \in \mathbb{F}_2^{2^{k-1}-k\times 2^{k-1}-1}$, take G_{k-2}, order $V_{k-2} = \{v_1, ..., v_{2^{k-1}-1}\}$ lexicographically in a descending order (as sorted arrays) and define*

$$A_k = \left(\begin{array}{c|c|c|c} P_{k-2} & \mathbf{0} & Q_{k-2} & R_{k-2} \\ \hline \mathbf{0} & \multicolumn{2}{c|}{A_{k-1}} & \mathbf{0} \end{array}\right) \in \mathbb{F}_2^{2^k-1-k\times 2^k-1}$$

  The sizes of these matrices are as follows:

  - *P_{k-2} is a $2^{k-1}-1 \times 2^{k-1}-1$ matrix, Q_{k-2} is a $2^{k-1}-1 \times k-1$ matrix and R_{k-2} is a $2^{k-1}-1 \times 1$ matrix. Their rows are indexed by the vertices in G_{k-2}, and their columns are the edges in $P_{k-2}, Q_{k-2}, R_{k-2}$ (namely $P_{k-1}[i,j] = 1$ iff v_i is in the j'th edge of P_{k-2} after fixing an ordering of the edges, and similarly for Q_{k-2}, R_{k-2}).*
    In other words, their rows are indexed by all nonzero vectors in $\{0,1\}^{k-2}$. For P_{k-2}, its columns are also indexed by those vectors, and $P_{k-2}[u,v] = 1$ iff u results from v by flipping at most one 0 entry to 1. For Q_{k-2}, its columns are indexed with the numbers in $[k-1]$, and $Q_{k-2}[u,j] = 1$ iff $\min\{j' \mid u_{j'} = 1\} = j$. For R_{k-2}, the only column in it holds that $R_{k-2}[u,1] = 1$ iff $||u||_1 = 1$.
  - *A_{k-1} is a $2^{k-1}-k \times 2^{k-1}-1$ matrix.*
  - *The sizes of each of the $\mathbf{0}$ blocks are deduced from the other blocks.*

It is fairly straightforward to see that finding a 1-free column set of the matrix $\begin{pmatrix} P_{k-2} & Q_{k-2} & R_{k-2} \end{pmatrix}$ is equivalent to finding a subset of E_{k-2} that satisfies the requirements in Proposition 6.3. We use this in Theorem 6.1's proof.

Proof of Theorem 6.1. First, by Proposition 5.1 and the $u \leq \varepsilon$ inequality we have $u(2^k - 1 - k2^k - 1) \leq \varepsilon(2^k - 1 - k, 2^k - 1) \leq 2^{k-1}$. We show that $u(A_k) = 2^{k-1}$ by induction on k. For $k = 1, 2$ the claim follows trivially. Suppose the claim is true for $k-1$, and we now prove it for k. Denote A_k in the block-formation as in Definition 6.4, and we refer to the 2 horizontal block-layers of A_k as the upper half and the lower half. To construct a 1-free column set for A_k, we start with J a subset of the last k columns, denoted as $c_1, ..., c_k$ respectively (they are the columns that fall into the Q_{k-2}, R_{k-2} parts of the matrix). From Proposition 6.3, we know that $J \neq \emptyset$ by considering only the upper half (which correspond to the vertices of G_{k-2}). If $J = \{c_k\}$, then the coordinates of c_k in the lower half are all 0, meaning that we only need to take care of the upper half, in order to achieve a 1-free set of columns. Since column c_k corresponds to the type-r edge e_r of G_{k-2}, by Proposition 6.3 we would need at least $2^{k-1} - 1$ more edges, for a total of 2^{k-1} edges. This implies a total of at least 2^{k-1} columns that constitute a 1-free set in A_k.

Otherwise, J contains some (nonempty choice) of $c_1, ..., c_{k-1}$. Denote $J = J' \sqcup J''$, where J'' is either empty or contains c_k. Now by the induction hypothesis, we would need at least $2^{k-2} - |J'|$ more columns to take care of the bottom half of A_k, and by Proposition 6.3 additional $2^{k-2} - |J''|$ columns for the upper half. This yields a total of $|J| + 2^{k-2} - |J'| + 2^{k-2} - |J''| = 2^{k-1}$ columns in order to achieve a 1-free set of columns of A_k, which proves the first part of the theorem for every k. □

Corollary 6.5. *For every k, n it holds that $u(n, n+k) \geq \varepsilon(n, n+k) - 2^{k-1} - 1$.*

Proof. The inequality follows from Theorem 6.1 and by the weak monotonicity of u, ε. □

We describe how one may prove the second part of Theorem 6.1, namely the $m > 1$ case. The proof here also proceeds inductively on k. The idea here is similar to how each A_k is defined, but with scaling the construction by a factor of m. For every k we define matrices M_k such that $u(M_k) = 2^{k-1}m$. Similarly to A_k, A_{k-1}, M_k contains M_{k-1} as a submatrix, but when adding $P_{k-2}, Q_{k-2}, R_{k-2}$, we add m copies of them in a diagonal fashion, so as to create independence between their columns. However, if we stop here, there would be $m-1$ columns and rows missing, and the minimal 1-free set would be smaller than $2^{k-1}m$. In order to fix that we simply insert an identity matrix of size $m-1$ to M_k (in the same diagonal fashion), and an all-ones column of length $m-1$. That extra step takes care of both problems. The matrix M_k would have the following form:

$$M_k = \left(\begin{array}{c|c|cc|c} \multirow{3}{*}{$\mathrm{diag}(P_{k-2}, ..., P_{k-2})$} & \multirow{3}{*}{$\mathbf{0}$} & \mathbf{0} & Q_{k-2} & R_{k-2} \\ & & \multicolumn{2}{c|}{\vdots} & \vdots \\ & & \mathbf{0} & Q_{k-2} & R_{k-2} \\ \hline \mathbf{0} & I_{m-1} & \multicolumn{2}{c|}{\mathbf{0}} & \mathbf{1} \\ \hline \mathbf{0} & \mathbf{0} & \multicolumn{2}{c|}{M_{k-1}} & \mathbf{1} \end{array}\right) \tag{6}$$

From here, $u(M_k) = 2^{k-1}m$ can be concluded using induction and similar calculations to those in the proof of Theorem 6.1.

7 Where ε Strictly Exceeds u

The result above seems to hint that $u = \varepsilon$. However, we show that it is not the case, and present the minimal values of m, n where there is inequality.

For the case of $k = 1$, since $\varepsilon(n, n+1) = n+1$ and the bound is achieved exactly by the trees on $n+1$ vertices (Proposition 5.3), we also have that $u(n, n+1) = n+1$. For the case of $k = 2$, by Theorem 6.1 we know that $u(3m-2, 3m) = \varepsilon(3m-2, 3m) = 2m$. For $n = 3m-1$ we use Proposition 5.1 to deduce that u, ε do not change. Lastly, for $n = 3m$ we take the matrix $A : [X | c_1\ c_2]$ that achieves the bound of $u(3m-2, 3m)$ and construct the matrix

$$A' := \left(\begin{array}{cc|cc} X & \mathbf{0} & c_1 & c_2 \\ \mathbf{0} & I_2 & \multicolumn{2}{c}{I_2} \end{array}\right)$$

It is straightforward to see that $u(A') = \varepsilon(A') = 2m+1$, and this also the upper bound on $u(3m, 3m+2), \varepsilon(3m, 3m+2)$ by Proposition 5.1. Hence $u(n, n+2) = \varepsilon(n, n+2)$. Similarly, we show that that is the case for $k = 3$ as well. Recall the Griesmer bound, which was presented in [4]:

Proposition 7.1. *For a $[n, k, d]_2$ linear code, $n \geq \sum_{i=0}^{k-1} \lceil \frac{d}{2^i} \rceil$.*

Proposition 7.2. *For every n, $u(n, n+3) = \varepsilon(n, n+3)$.*

Proof. By Theorem 6.1 we know that $u(7m-3, 7m) = \varepsilon(7m-3, 7m)$ for every m. Therefore, it's left to show this equality for 6 more cases, and 3 edge cases. For simplicity we mention now that every case uses the upper bound on ε of Proposition 5.1, the inequality $u(n, n+3) \leq \varepsilon(n, n+3)$ and u, ε being increasing integer functions.

Overview: cases 1, 5 follow from cases 0, 4; cases 3, 4, 6 follow from explicit extension of case 0 (i.e. Proposition Theorem 6.1) and looking at the new parity-check matrix; case 2 follows from the Griesmer Bound.

1. $u(7m-2, 7m+1) = \varepsilon(7m-2, 7m+1) = 4m$: the equality follows since $\varepsilon(7m-2, 7m+1) = 4m$ by the above.

2. $u(7m-1, 7m+2) = \varepsilon(7m-1, 7m+2) = 4m$: we know that $\varepsilon(7m-1, 7m+2) \in \{4m, 4m+1\}$. From the Griesmer Bound, it can't be the case that $\varepsilon(7m-1, 7m+2) = 4m+1$, for otherwise

$$7m+2 \geq \sum_{i=0}^{2} \left\lceil \frac{4m+1}{2^i} \right\rceil = 7m+3$$

   which is a contradiction. Therefore, $u(7m-1, 7m+2) = \varepsilon(7m-1, 7m+2) = 4m$.

3. $u(7m, 7m+3) = \varepsilon(7m, 7m+3) = 4m+1$: given the matrix A_k with $k = 3$ from Definition 6.4, we append 3 additional rows to the bottom of A_3 of the form $0^{6m-3}100100$, $0^{6m-3}010010$ and $0^{6m-3}001001$. Using similar reasoning to Theorem 6.1 it follows that both u, ε have increased from $4m$ by at least 1. Since $\varepsilon(7m, 7m+3) \leq 4m+1$, the equality follows.

4. $u(7m+1, 7m+4) = \varepsilon(7m+1, 7m+4) = 4m+2$: same as the previous case, but now we add the 4 rows $0^{6m-3}1000100$, $0^{6m-3}0100110$, $0^{6m-3}0010011$ and $0^{6m-3}0001001$.

5. $u(7m+2, 7m+5) = \varepsilon(7m+2, 7m+5) = 4m+2$: follows from the previous case, along with the inequality $\varepsilon(7m+2, 7m+5) \leq 4m+2$.

6. $u(7m+3, 7m+6) = \varepsilon(7m+3, 7m+6) = 4m+3$: same as case 4, but now we add the 6 rows $0^{6m-3}100000110$, $0^{6m-3}010000101$, $0^{6m-3}001000011$, $0^{6m-3}000100100$, $0^{6m-3}000010010$ and $0^{6m-3}000001001$.

It is left to show the equality for $n = 1, 2, 3$. For $n = 1$ it is clear. For $n = 2$ it holds that $u(2, 5) = \varepsilon(2, 5) = 2$ by Proposition 5.1 and the lower bound imposed by the all-ones matrix $\mathbf{1}_{2\times 5}$. For $n = 3$, by Proposition 5.1 and the $n = 2$ case it holds that $2 \leq u(3, 6) \leq \varepsilon(3, 6) \leq 3$. The equality is obtained via the lower bound of 3 imposed by the matrix

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

Hence, $u(n, n+3) = \varepsilon(n, n+3)$. □

To summarize, $u(n, n+k) = \varepsilon(n, n+k)$ whenever $k \leq 3$. As we show in the following claim, this equivalence no longer holds for $k \geq 4$. This strongly reminds the result of Theorem 4.2, as the corollary from there is also that for $k \geq 4$, $u_I(n, n+k) \leq 0.49n + O(k)$ (which is $(1/2 - \epsilon)n$ for a constant $\epsilon > 0$ when $k := f(n) = o(n)$). In the next proposition we use a linear code presented in [5].

Proposition 7.3. $u(4,8) = 3 < 4 = \varepsilon(4,8)$.

Proof. First, $\varepsilon(4,8) \leq 4$ by Proposition 5.1. Equality holds for the following matrix[1]:

$$\left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{array}\right) \tag{7}$$

We now show that $u(4,8) = 3$. $u(4,8) \geq 3$ follows from the matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} \tag{8}$$

For the upper bound, let $A \in \mathbb{F}_2^{4\times 8}$. Suppose that A contains a column that weighs 1, namely column j of A has 1 only in its i'th coordinate. Consider now the length-3 columns of the minor $A[i|j] \in \mathbb{F}_2^{3\times 7}$. If the minor contains the all-zero column, then $u(A) \leq 2$. If the minor contains two instances of the same column, then $u(A) \leq 3$. Otherwise, $A[i|j]$ contains 7 different, nonzero columns. Namely,

$$A[i|j] = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \tag{9}$$

up to permutations of the columns. Now consider 1-free sets of $A[i|j]$ of size 3 in the scope of A. If by contradiction those sets are not 1-free in A, then we have the following constraints:

$$\begin{aligned} &w(A_{i,(1,2,3)}) = 1,\ w(A_{i,(3,5,6)}) = 1,\ w(A_{i,(1,6,7)}) = 1,\ w(A_{i,(2,5,7)}) = 1, \\ &w(A_{i,(3,4,7)}) = 1,\ w(A_{i,(2,4,6)}) = 1,\ w(A_{i,(1,4,5)}) = 1 \end{aligned}$$

Summing them, over $\mathbb{Z}$ we have $3w(A_i) = 7$ – contradiction to $w(A_i) \in \mathbb{Z}$. Thus one of the above sets is also 1-free in A, hence $u(A) \leq 3$.

Now suppose no column of A weighs 1. Clearly we can assume that no column weighs 0, for otherwise $u(A) = 1$. This leaves us with columns of weight $2, 3, 4$. Since

$$u\left(\begin{pmatrix} 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \end{pmatrix}\right) = 3 \tag{10}$$

then we can assume that only 2 of the columns above appear in A. This leaves 6 columns of weight 2 in A, and assuming no column repeats in A (otherwise $u(A) \leq 3$ trivially), then wlog

$$A = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & * & 1 \end{pmatrix} \tag{11}$$

where $* \in \{0,1\}$. In any case $u(A) \leq 3$ using columns $6, 7, 8$. We exhausted all cases, hence $u(A) \leq 3$, and $u(4,8) = 3$. □

[1] Up to coordinates permutations, this is a parity-check matrix for the Plotkin sum of the dual code to the repetition $[4,1,4]_2$ code with the repetition $[4,1,4]_2$ code (from [5]).

Note that similarly to Theorem 6.1, the bound $u(4,8) = 3$ is achieved with a matrix where all rows weigh exactly 3. Can $u(m,n)$ always be achieved using matrices where every row weighs exactly 3?

It is worth mentioning that $4, 8$ are the *minimal* m, n for which $u(m,n) < \varepsilon(m,n)$. Since equality holds when $n - m \leq 3$, the minimal case is when $n - m \geq 4$. For $(m,n) = (1,5), (2,6)$ trivially there is equality (with values of 2 for both cases), and for $(m,n) = (3,7)$ it holds that $u(3,7) = \varepsilon(3,7) = 3$ since both are upper-bounded by 3, and equality is achieved for the matrix that contains all nonzero 7 binary strings of length 3 as columns.

8 Open Problems

Problem 8.1. *What is the smallest c for which the conclusion of Theorem 3.1 holds?*

Problem 8.2. *Let $u_3(m,n)$ denote the maximal value of $u(A)$ over all binary matrices $A \in \mathbb{F}_2^{m \times n}$ such that every row weighs 3. From Proposition 5.3 we know that $u_3(n, n+1) < u(n, n+1)$. On the other hand, for a larger difference we have seen on several occasions that u_3 reaches u (e.g. $u_3(4,8) = u(4,8)$, $u_3(2^k - 1 - k, 2^k - 1) = u(2^k - 1 - k, 2^k - 1)$). Therefore, does $u_3(m,n) = u(m,n)$ hold for every $n > m + 1$?*

Problem 8.3. *Recall the proof technique of Theorem 3.1. We can generalize this as follows: we are given a set of columns, where some coordinates I_0 sum to 0 and some I_1 to 1 (over $\mathbb{Z}$). We then want to add columns J such that their I_0 and I_1 rows will have non- 0 and 1 Hamming weights (resp.). Under what conditions is it possible to pre-specify which row sums we wish to be $\neq 0$ and which $\neq 1$?*

References

[1] Guruswami, Venkatesan. Notes 8: Expander Codes and their decoding. Available at http://www.cs.cmu.edu/ venkatg/teaching/codingtheory/notes/notes8.pdf, 2010.

[2] Richardson, Tom, and Ruediger Urbanke. Modern coding theory. Cambridge university press, 2008.

[3] Kim, Dae San. "Weight distributions of Hamming codes." arXiv preprint arXiv:0710.1467 (2007).

[4] Griesmer, James H. "A bound for error-correcting codes." IBM Journal of Research and Development 4.5 (1960): 532-542.

[5] Grassl, Markus. "Bounds on the minimum distance of linear codes and quantum codes." Online available at http://www.codetables.de. Accessed on 2021-11-24.