Bounds on Unique-Neighbor Codes

Nati Linial* Idan Orzech†

Abstract

Let A be an $m \times n$ parity check matrix of a binary code of length n, rate R, and distance δn. This means that for every $\delta n > k > 0$, every $m \times k$ submatrix of A has a row of odd weight. *Message-passing* decoding algorithms require the stronger *unique neighbor* property. Namely, that every such submatrix has a row *of weight* 1. It is well known that if $\delta \geq \frac{1}{2}$, then $R = o_n(1)$ whereas for every $\frac{1}{2} > \delta$ there exist linear codes of length $n \to \infty$ and distance $> \delta n$ with R bounded away from zero. We believe that the unique neighbor property entails sharper upper bounds on the rate. Concretely, we conjecture that for a proper choice of $f(n) = o(n)$ and some constant $\epsilon_0 > 0$, every $n \times (n + f(n))$ binary matrix has an $n \times k$ submatrix with $(\frac{1}{2} - \epsilon_0)n \geq k > 0$ where no row weighs 1. We make several contributions to the study of this conjecture.

1 Introduction

We consider here only binary codes $\mathcal{C} \subseteq \{0,1\}^n$ of length 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 $\text{dist}(\mathcal{C}) = \min_{x \neq y, x, y \in \mathcal{C}} d_H(x,y)$, where d_H stands for the 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*

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

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, $\mathcal{C} = \{x \mid Ax = 0\}$.

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. We refer to the number of 1-entries in a binary vector as its *weight* or *sum*.

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 $u(m,n)$.*

With this, the question analogous to Problem 1.1 for linear codes suggests itself:

*School of Computer Science and Engineering, Hebrew University, Jerusalem 91904, Israel. e-mail: nati@cs.huji.ac.il. Supported in part by a NSF-BSF research grant "Global Geometry of Graphs".

†School of Computer Science and Engineering, Hebrew University, Jerusalem 91904, Israel. e-mail: idan.orzach@mail.huji.ac.il. Based on the second author's undergraduate honors project.

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

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

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 $\mathcal{C} = \{x \mid Ax = 0\}$. In the analysis of such algorithms, A is viewed as the bipartite adjacency matrix of the code's *factor graph*. This is a bipartite graph $(L, R; E)$, where L is the set of A's columns and R its set of rows, and edges correspond to 1-entries in A. 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 appropriate 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 has cardinality bigger than B. For codes that satisfy such conditions, a decoding algorithm due to Sipser and Spielman [9] can correctly decode incoming messages in linear time with not too large error patterns. In this case $(L, R; E)$ is a highly expanding bipartite graph. A full account of this subject is to be found in [1].

In this view we ask:

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

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

in other words, $R_U(\delta)$ 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 all these three functions 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 $\delta \geq \frac{1}{2}$.

We believe 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 positive 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 a 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?*

We often use the fact that u and ε are invariant under row and column permutations. The matrices that we consider have size $m \times n$ or $n \times (n + k)$ in different parts of the paper.

1.1 Some Further Background

The literature on unique-neighbor codes is fascinating and yet we still know very little. In particular, quantitative results in this area are few and far between. It is this lacuna that motivates our work. Alon and Capalbo [7] found explicit constructions of unique-neighbor bipartite expander graphs $(L, R; E)$ with an even stronger property. Namely, every subset $S \subseteq L$ of cardinality $|S| \leq \epsilon|L|$ has at least $\alpha|S|$ unique-neighbors in R, where $\epsilon, \alpha > 0$ are some absolute constants. This parameter α is sometimes referred to as the graph's unique-neighbor expansion. More recently Becker [8] showed how to construct such graphs that are also *Cayley graphs*.

Let A be a parity check matrix of $\mathcal{C} := \{x \in \mathbb{F}_2^n \mid Ax = 0\}$. If A has bounded row and column weights we say that $\mathcal{C}$ is an LDPC code. Equivalently, the above bipartite graph $(L, R; E)$ has bounded vertex degrees. As Sipser and Spielman [9] showed, if the expansion of this graph is high enough, then $\mathcal{C}$ has a linear-time decoding algorithm, as long as the error rate is not too large. The correctness of this algorithm crucially relies on the fact that these graphs also have a high unique-neighbor expansion. The work of Sipser and Spielman has been subsequently improved several times. Viderman [10] proved that the same conclusions hold as well for graphs with lower expansion rate, resp. unique-neighbor expansion rate. Dowling and Gao [11] generalized the results to Tanner codes. They determined a range of parameters for which linear-time decoding is possible. Namely, the (unique) expansion rate of the inner graph of Tanner's code, the distance of the inner code and the error rate.

Ben-Sasson and Viderman [6] used unique-neighbor expanders to construct *robustly-testable* codes by taking their tensor products with another code with good distance and rate. They stress that unique-neighbor expansion is a minimal requirement in order to argue that an expander code has a good distance. A linear code with parity check matrix A is called *smooth* if its distance remains large also after a few rows and columns are removed from A. It is called *weakly-smooth* if the above holds provided the removed rows combined have a small number of nonzero entries. It is not known if unique-neighbor expander codes are smooth. However, Ben-Sasson and Viderman showed that they are weakly-smooth, and can therefore be used to form robustly-testable codes.

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 under the assumption of a lower bound on the weight of each row in A (Theorem 3.1). In that case the statement holds in fact with $f(n) = 0$.
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 4.1).
4. Clearly $\varepsilon(m, n) \geq u(m, n)$ for all m and n. We find the smallest $n > m$ for which the inequality is strict (Theorem 7.1, Item 1).

3 The Effect of Large Row Weights

As we show next, matrices of sufficiently large row weights satisfy Conjecture 1.5. In contrast, finding small 1-free sets in sparse matrices seems harder, and in Theorem 6.1 we use matrices with row sums 3 to derive a lower bound on $f = f(n)$ without which the conclusion of Conjecture 1.5 fails to hold.

Theorem 3.1. *1. If A is a binary $n \times n$ matrix in which every row weighs at least 9, then it has an $n \times m$ submatrix with $m \leq 0.49n$ with all row sums at least 2.*

2. On the other hand, there exist binary $n \times n$ matrices where every row has weight 4, such that every $n \times m$ submatrix with no row of weight 1 must satisfy $m \geq n/2$.

Proof. Let c be the smallest Hamming weight of the rows in such a matrix. 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 in the resulting submatrix of weight zero, resp. one. Next we correct every row of weight zero/one by adding two/one columns 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 $c = 9, \rho = 0.4$.

For the second part, let A be the $n \times n$ binary matrix whose rows are comprised of all n cyclic rotations of the vector $1^4 0^{n-4}$. Given a vector $x \in \{0,1\}^n \setminus \{\mathbf{0}\}$, let the vector Ax be defined by real arithmetic. Clearly, $Ax \in \{0,1,2,3,4\}^n$. Multiply on the left by the all-1 vector to conclude that $\|Ax\|_1 = 4\|x\|_1$. Note next that if $(Ax)_i = 0$, then $(Ax)_{i+1 \bmod n}$ is either 0 or 1. Therefore, if Ax has no 1 coordinates, then all its coordinates are ≥ 2, so that $4\|x\|_1 = \|Ax\|_1 \geq 2n$ and $\|x\|_1 \geq n/2$, as claimed. □

Part 2 of Theorem 3.1 reflects on the validity of Conjecture 1.5. It shows that to guarantee the existence of small 1-free sets of columns, we must consider matrices with more columns than rows. This statement is made quantitative in Theorem 6.1.

We suspect that part 1 of 3.1 remains valid even when all row weights are ≥ 5. However, this seems to require a substantial new idea.

4 Matrices in Standard Form

We denote by $u_I(m,n)$ the maximum of $u(A)$ for a binary $m \times n$ matrix in standard form $A = [I_m|B]$. Answering Problem 1.6, we give an upper bound on $u_I(m,n)$ that is tight in infinitely many cases.

Theorem 4.1. *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 $\langle u, v \rangle$ the inner product of the two real vectors u and v. It is easy to describe all 1-free sets of columns in A: Start with a submatrix of B with column set $S \subset [k]$ and observe the weight-1 rows in this submatrix. Then add all the corresponding columns in I_n to make the set 1-free. So, given a matrix B, we can express the least size of a 1-free set of columns in A as the optimum of an integer linear program. 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, and $\sum_{u \in \{0,1\}^k} x_u = n$.

If s is the indicator vector of S, then we must add at least $\sum\{x_u \mid \langle u, s \rangle = 1\}$ columns from I_n to reach a 1-free set of columns. So, let M be the $2^k \times 2^k$ binary matrix that is indexed by $\{0,1\}^k$. The (u,v) entry of M equals 1 iff $\langle u, v \rangle = 1$ (integer arithmetic), and conclude that

$$m + k \geq u_I(n, n+k) \geq m$$

where

$$\begin{aligned} m = &\max y \\ \text{subject to} \quad &M\mathbf{x} \geq \mathbf{1} \cdot y, \\ &\langle \mathbf{x}, 1 \rangle = n \text{ and } \mathbf{x} \geq 0 \text{ is a vector of integers} \end{aligned}$$

The $\pm k$ uncertainty in our bound on $u_I(n, n+k)$ has to do with the size of $S \subset [k]$ mentioned above. We turn to solve the rational relaxation of the above ILP.

$$\begin{aligned} &\max y \\ \text{subject to} \quad &M\mathbf{x} \geq \mathbf{1} \cdot y, \\ &\langle \mathbf{x}, 1 \rangle = n \text{ and } \mathbf{x} \geq 0 \end{aligned}$$

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 $(wM)_{\mathbf{0}} = 0$, and if $v \in \{0,1\}^k$ with $|v| = j$ for some $k \geq j \geq 1$ then

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

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

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

In other words, $wM = k(\mathbf{1} - e_{\mathbf{0}})$, and hence $nk \geq wM\mathbf{x} \geq w \cdot \mathbf{1}y = \langle w, \mathbf{1} \rangle \cdot y$.

Also

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

It follows that

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

since an upper bound on the LP applies as well to the corresponding ILP, both of which seek to maximize the same objective function.

The reverse inequality follows by letting

$$\mathbf{x} := n \frac{w}{kH_k}$$

and observing that with similar calculations we get $\langle \mathbf{x}, \mathbf{1} \rangle = n$, therefore $M\mathbf{x} = \mathbf{1}\frac{n}{H_k} \geq \mathbf{1}y$, hence u_I of an $n \times (n+k)$ matrix with rows corresponding to such $\mathbf{x}$ is $\frac{n}{H_k} + O(k)$.

To get the lower? bound on the ILP, let $H_k := \frac{a_k}{b_k}$ written as a reduced rational. If n is divisible by a_k, say $n = pa_k$, then $u_I(n, n+k) = pb_k + O(k)$, because in this case the optimal solutions to our LP and the ILP coincide. More generally, if $n = pa_k + q$ then $u_I(n, n+k) \geq \lfloor \frac{n}{a_k} \rfloor b_k + O(k) \geq \frac{n}{H_k} + O(k) - 1$. $\square$

5 Some Useful Constructions

In this section we introduce a $(2^k - 1 - k) \times (2^k - 1)$ binary matrix U_k for $k = 2, 3, \ldots$ to be used below. We define U_k both recursively and directly. It is easy to verify by a simple inductive argument that the two definitions coincide. Here is the recursive one:

$$U_2 = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix} \tag{1}$$

$$U_{k+1} = \begin{pmatrix} I_{2^k-1} & \mathbf{1}_{2^k-1 \times 1} & I_{2^k-1} \\ \mathbf{0} & \mathbf{0} & U_k \end{pmatrix} \tag{2}$$

In the direct definition of U_k we index its columns by all integers $2^k - 1, 2^k - 2, \ldots, 1$, in this order. The rows are indexed by the subsequence of the above excluding the powers of 2. Each row of U_k has weight 3. If the integer $m \in \{1, \ldots, 2^k - 1\}$ is not a power of 2, say $2^{t+1} > m > 2^t$, then the three 1 entries in row m appear in columns $m, m - 2^t$ and 2^t.

For example,

$$U_3 = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

with rows called $7, 6, 5, 3$ in this order and columns called $7, \ldots, 1$.

We note that U_k is a generator matrix of the generalized $[2^k-1, 2^k-1-k, 3]_2$ Hamming code. Clearly every such triplet belongs to the relevant generalized Hamming code. Also, U_k has a full row rank since it contains an upper-triangular square submatrix called T_k which is attained by erasing those columns of U_k that correspond to a power of two. The remaining submatrix is called R_k.

An interesting aspect of this construction is that it exploits the duality between Hamming Codes and shortened Hadamard Codes. Since the former are generated by a matrix with row weights 3, it is relatively easy to derive a lower bound on u. On the other hand, due to the fact that all vectors in an order-N Hadamard Codes have weight $N/2$ it yields a upper bound on ε. Since these bounds coincide they are both tight. Indeed, in the next section we show that these matrices attain the bounds $u(n, n+k), \varepsilon(n, n+k)$ (for the corresponding n, k) and are, in fact, equal.

We next construct for every $k \geq 2, m \geq 1$ a $((2^k-1)m-k) \times ((2^k-1)m)$ binary matrix as follows.

$$U_{k,m} = \left(\begin{array}{ccc|c} T_k & & & R_k \\ & \ddots & & \vdots \\ & & T_k & R_k \\ \hline & & & I_k \\ & & I_{(m-1)k} & \vdots \\ & & & I_k \end{array}\right) \tag{3}$$

where the empty blocks are all-zero.

6 Conjecture 1.5 Can Hold Only If f is at Least Logarithmic

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 integers n. Concretely,

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

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

Proof. The proof proceeds by showing that

$$\varepsilon(2^k - 1 - k, 2^k - 1) \leq 2^{k-1} \quad \text{and} \quad u(U_k) \geq 2^{k-1}.$$

We recall the following well-known fact:

Proposition 6.2. *Every $n \times (n+k)$ binary matrix A has an even set of at most $\left(1 + \frac{1}{2^k-1}\right) \frac{n+k}{2}$ columns.*

This yields $2^{k-1} \geq \varepsilon(U_k)$.

We turn to prove that $u(U_k) \geq 2^{k-1}$ by induction on $k \geq 2$. For $k = 2$ the claim clearly holds. For the induction step we use the recursive description of U_{k+1} in Section 5. Consider a 1-free column set of U_{k+1}. If it contains column 2^k, then it must include at least $2^k - 1$ additional columns (from either side of the column), for a total of $\geq 2^k$ columns, as claimed.

Thus it suffices to consider a 1-free set of columns of the form $L \sqcup R$, where R, L is the subset of columns from the $2^k - 1$ rightmost, leftmost ones (respectively). By the induction hypothesis $|R| \geq 2^{k-1}$.

For every $r \in R$, one of its first (upper) $2^k - 1$ coordinates contains a 1. Since column 2^k is absent from $L \sqcup R$, the (unique) matching column from the $2^k - 1$ leftmost columns should be picked, in order for $L \sqcup R$ to be 1-free. It follows that $|L \sqcup R| \geq 2^k$, completing the proof. □

Theorem 6.1 and the weak monotonicity of u, ε (see Proposition 7.2 below) yield

Corollary 6.3. *For every k, n it holds that $u(n, n+k) \geq \varepsilon(n, n+k) - 2^{k-1} - 1$.*

Further cases where ε and u coincide are provided by the following extension of Theorem 6.1:

Theorem 6.4. *For every integers $k \geq 2$ and $m \geq 1$ there holds*

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

Proof. Again we bound u from below and ε from above. The bound on u uses the matrices $U_{k,m}$ from Section 5 and the bound on ε follows from Proposition 6.2. To show that $u(U_{k,m}) \geq 2^{k-1}m$, we consider 1-free sets of columns in $U_{k,m}$. The matrix $U_{k,m}$ with its last k columns removed has no nonempty 1-free sets, since it is an upper-triangular, full-rank matrix. So consider a 1-free set that includes $t > 0$ columns among the last k columns of $U_{k,m}$. By Theorem 6.1 at least $(2^{k-1} - t)m$ additional columns are needed, namely at least $2^{k-1} - t$ from every T_k in the direct sum. The lower part of $U_{k,m}$ necessitates exactly $(m-1)t$ columns from the columns that contain the block $I_{(m-1)k}$. In total the cardinality of the 1-free set at hand is at least $t + (2^{k-1} - t)m + (m-1)t = 2^{k-1}m$, as claimed. □

7 Between u and ε When $n - m$ is Bounded

In this section we compare between $u(m,n), \varepsilon(m,n)$ when $n - m \geq 1$ is bounded. Here is our main result:

Theorem 7.1.

1. *$u(4,8) = 3$ whereas $\varepsilon(4,8) = 4$. This is the first case where $\varepsilon > u$.*
2. *$u(n, n+1) = \varepsilon(n, n+1) = n+1$. The case of equality is fully characterized.*
3. *$u(n, n+2) = \varepsilon(n, n+2) = \lfloor \frac{2n+4}{3} \rfloor$.*
4. *If $n \not\equiv -1 \bmod 7$, then $u(n, n+3) = \varepsilon(n, n+3) = \lfloor \frac{4n+12}{7} \rfloor$. Also, $u(7m-1, 7m+2) = 4m$ for every positive integer m.*

Proof. We start with several simple observations:

Proposition 7.2.

1. *$u(m,n) \leq \varepsilon(m,n) \leq m$.*
2. *Both $u(m,n)$ and $\varepsilon(m,n)$ weakly increase with m and decrease with n.*
3. *$u(m+1, n+1) \geq u(m,n)$, $\varepsilon(m+1, n+1) \geq \varepsilon(m,n)$.*
4. *If a binary matrix A has a row of weight 1, then $u(B) = u(A), \varepsilon(B) = \varepsilon(A)$ where B is attained by from A* elementary collapse*, i.e., by deleting the corresponding row and column of A.*

7.1 Proof of Item 1: $u(4,8) = 3 < 4 = \varepsilon(4,8)$.

Proof. Proposition 6.2 implies that $\varepsilon(4,8) \leq 4$. On the other hand $\varepsilon(A) = 4$ for

$$A = \left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{array}\right) \tag{4}$$

We now show that $u(4,8)=3$. The following matrix yields $u(4,8)\geq 3$

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} \tag{5}$$

Next we show that $u(A)\leq 3$ for every binary 4×8 matrix A. We reduce to the case that every column of A weighs at least 2. If A has a zero column, then clearly $u(A)=1$. If some column of A weighs 1, say $a_{1,1}=1$ and $a_{i,1}=0$ for $i=2,3,4$, consider the submatrix B of A that is obtained by erasing its first row and column. If B has an all-zero column, then $u(A)\leq 2$, and if B has two equal columns, then $u(A)\leq 3$. The only remaining case is when

$$B=\begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \tag{6}$$

up to permutations of the rows and columns. Consider the weight $w=\sum a_{1,j}$ of row 1 in A. If $w=1$, then $a_{1,j}=0$ for all $j\geq 2$. Consequently, $u(A)=u(B)=3$, since every set of columns that is 1-free in B is also 1-free in A. If $w\geq 3$ there are at least two indices $\alpha>\beta>1$ such that $a_{1,\alpha}=a_{1,\beta}=1$. If columns α,β of B are the vectors u resp. v, then some column γ corresponds to $u\oplus v$ (mod 2 sum). Columns α,β,γ form a 1-free set in A. Finally, if $w=2$, there is exactly one index $\delta>1$ such that $a_{1,\delta}=1$. But then we can find a triplet of columns of the form $u,v,u\oplus v$ in B none of which is column δ.

We can now assume that every column of A has weight $2,3$ or 4. Also A has no repeated columns, or else $u(A)=2$. Also A can have at most two columns of weight ≥ 3, for any three such distinct vectors form a 1-free set. Consequently A has exactly two columns of weight ≥ 3 and each of the six columns of weigh 2. But the latter 6-tuple contains a 1-free set of three columns. □

Note that $4,8$ are the *minimal* m,n for which $u(m,n)<\varepsilon(m,n)$: The other parts of the present theorem show that equality holds when $n-m\leq 3$. For $(m,n)=(1,5),(2,6)$ equality trivially holds (with values of 2 for both cases). Also $u(3,7)=\varepsilon(3,7)=3$ since both are ≤ 3, with equality for the canonica parity-check matrix of the $[7,4,3]_2$ Hamming code.

7.2 Proof of Item 2

It is clear that $u(n,n+1)=\varepsilon(n,n+1)=n+1$. Also $\varepsilon(A)=n+1$ for an $n\times(n+1)$ matrix A iff it has a full $\mathbb{F}_2$-rank and all its row weights are even. Let $A=A_T$ be the edges vs. vertices incidence matrix of an $(n+1)$-vertex tree T. It is easily seen that $u(A)=n+1$. As we show, no other examples exist.

Proposition 7.3. *If $u(A)=n+1$ for some $n\times(n+1)$ binary matrix A, then $A=A_T$ for some $(n+1)$-vertex tree T.*

Proof. A cannot have a zero row, or else $u(A)\leq\varepsilon(A)\leq\frac{2(n+1)}{3}$, by Proposition 6.2. As in Proposition 7.2, Item 4, any row of weight 1 in A can be collapsed, without changing ε and u. So w.l.o.g. every row of A weighs at least 2. Let us view A as the edges vs. vertices incidence matrix of a hypergraph $G=(V,E)$. An edge in E of size 2 (resp. ≥ 3) is called *light* (resp. *heavy*). Let $L\subseteq E$ be the set of light edges. If all edges in E are heavy, we can omit a single column of A and obtain a matrix in which all rows weigh at least 2, contrary to our assumption that $u(A)=n+1$.

The graph (V,L) has no isolated vertices, for if $v\in V$ is incident with no light edge, then $V\setminus\{v\}$ is a 1-free set, contrary to our assumption. If $L=E$, then the vertex set of any connected component of G is a 1-free set. Therefore G is a connected graph with $n+1$ and n edges, i.e., a tree, as claimed. On the other hand, if $L\neq E$, the graph (V,L) must be disconnected, since it has $n+1$ vertices and at most $n-1$ edges. Let $(V_1,L_1),\ldots,(V_k,L_k)$ be the connected components of (V,L). By the above $\sum|V_i|=n+1$, $|L_i|\geq|V_i|-1$, so that $|L|=\sum|L_i|\geq n+1-k$, with equality iff (V,L) is a forest with no isolated vertices. Consequently, at most $k-1$ edges in E are heavy.

Let B be the edges vs. vertices matrix of the hypergraph that results from G by shrinking each V_i to a single new vertex v_i. Since $L \neq \emptyset$ this actually reduces the size of the matrix and we can induct. Every 1-free set S of B yields a 1-free set in A by inflating each $v_i \in S$ to V_i. In particular $u(B) < k$ would imply $u(A) \leq n$. Consequently, B is a $(k-1) \times k$ matrix with $u(B) = k$. By induction it is the edge-vertex matrix of K, a tree with vertex set $\{v_1, \ldots, v_k\}$. Say that v_1 is a leaf of K, and let e be the single edge of K that is incident with v_1. We claim that either V_1 or $V \setminus V_1$ comprise a 1-free set of A. Indeed, only the row corresponding to e may have weight 1 in the submatrix of A corresponding to either V_1 or $V \setminus V_1$. But it is impossible that both cases occur, for that would mean that the edge e has size 2 contrary to the fact that e is a heavy edge. Since both $V_1, V \setminus V_1$ are nonempty, this contradicts our assumption that $u(A) = n + 1$. This establishes case 2 of the theorem. □

7.3 Proof of Items 3, 4

The proof for $k = 2$ splits to cases according to the value of $n \bmod 3$. When $n \equiv 1 \bmod 3$ we have $u(3m-2, 3m) = \varepsilon(3m-2, 3m) = 2m$ by Theorem 6.4. By Proposition 6.2, u, ε do not change as we move to $n = 3m - 1$. Finally, for $n = 3m$ we introduce the matrix

$$A := \begin{pmatrix} U_{2,m} & \mathbf{0} \\ \mathbf{0} \quad I_2 & I_2 \end{pmatrix}$$

with $U_{2,m}$ as defined in Section 5. It is easy to see that $u(A) = \varepsilon(A) = 2m+1$. By Proposition 6.2 this is also the upper bound on $u(3m, 3m+2), \varepsilon(3m, 3m+2)$. We conclude that $u(n, n+2) = \varepsilon(n, n+2) = \left\lfloor \frac{2n+4}{3} \right\rfloor$ as claimed.

The analysis when $k = 3$ is somewhat more involved and proceeds according to the value of $n \bmod 7$. We start with the upper bound: By Proposition 6.2, $\varepsilon(n, n+3) \leq \lfloor \frac{4n+12}{7} \rfloor$. This bound is tight, except if $n \equiv -1 \bmod 7$, when it can be reduced by 1 due to Griesmer's bound [4]:

Proposition 7.4. *Every k-dimensional binary linear code of distance d has length at least $\sum_{i=0}^{k-1} \lceil \frac{d}{2^i} \rceil$.*

Indeed, our general upper bound is $\varepsilon(7m-1, 7m+2) \leq \lfloor \frac{28m+8}{7} \rfloor = 4m+1$, but by Griesmer's bound if the code's distance is $4m+1$, then its length, is at least $4m + 1 + \lceil \frac{4m+1}{2} \rceil + \lceil \frac{4m+1}{4} \rceil = 7m + 3$.

We proceed to deal with the lower bounds. The case $k = 3$ of Theorem 6.4 gives $u(7m-3, 7m) = \varepsilon(7m-3, 7m) = 4m$. Namely, $u = \varepsilon$ when $n \equiv 4 \bmod 7$.

Item 3 of Proposition 7.2 and Proposition 6.2 yield

$$u(n-1, n+2) \leq u(n, n+3) \leq \varepsilon(n, n+3) \leq \left\lfloor \frac{4}{7}(n+3) \right\rfloor.$$

When $u(n-1, n+2) = \left\lfloor \frac{4}{7}(n+3) \right\rfloor$, this trivially allows to derive the case $n \equiv r+1 \bmod 7$ from the case $n \equiv r \bmod 7$. This works verbatim for $r \equiv \pm 2 \bmod 7$. When $n \equiv 0, 1, 3 \bmod 7$, an additional argument is needed. To this end, we extend $U_{3,m}$ from Section 5 to an $n \times (n+3)$ matrix for the appropriate n. This resembles the construction of $U_{k,m}$ from U_k, and the case $k = 2$. In all three cases, these matrices show that $u(n, n+3)$ attains the upper bound on $\varepsilon(n, n+3)$, namely $\left\lfloor \frac{4}{7}(n+3) \right\rfloor$. Hence we get in each case a matrix U such that $\varepsilon(n, n+3) = u(U) \leq u(n, n+3)$. For illustration, when $n = 7m$, we use the matrix $U_{3,m}$ to construct

$$U := \begin{pmatrix} U_{3,m} & \mathbf{0} \\ \mathbf{0} \quad I_3 & I_3 \end{pmatrix}$$

Note that $4m + 1 = u(U) \leq u(7m, 7m+3)$ and $\varepsilon(7m, 7m+3) \leq 4m+1$ from Proposition 6.2, so in total $u(7m, 7m+3) = \varepsilon(7m, 7m+3) = 4m+1$.

We note that Item 4 holds as well when $n = 1, 2, 3$, but we skip this verification.

This concludes the proof of Theorem 7.1. □

8 Open Problems

Problem 8.1. *The most obvious question is Conjecture 1.5 which remains open.*

Problem 8.2. *What is the smallest c for which the conclusion of Theorem 3.1 holds? Is it 5?*

Problem 8.3. *Let $u_3(m,n)$ denote $\max u(A)$ of an $m \times n$ binary matrix A where every row weighs 3. Proposition 7.3 implies that $u_3(n,n+1) < u(n,n+1)$, but perhaps $u_3(m,n) = u(m,n)$ when $n > m+1$. Some supportive evidence for this is that $u_3(4,8) = u(4,8)$, $u_3(2^k-1-k, 2^k-1) = u(2^k-1-k, 2^k-1)$. We note that more generally, $u_3((2^k-1)m-1, (2^k-1)m) = u((2^k-1)m-1, (2^k-1)m)$ holds, because the matrices $U_{k,m}$ can be modified so all rows weigh 3 without changing u, ε.*

Problem 8.4. *The proof of Theorem 3.1 suggests a more general setup. We seek a 1-free set of columns in a binary matrix A. Having committed to some subset of columns, the rows of A are split into: $I_0 \sqcup I_1 \sqcup I_*$, those of weight $0, 1$ and ≥ 2, respectively. To extend our initially chosen set into a 1-free set, we need an additional set of columns J, the weight of whose I_0 and I_1 rows differ from $1, 0$ respectively. Under what conditions is it possible to pre-specify which row sums we wish to be $\neq 0$ and which $\neq 1$?*

Remark 8.5. *Assuming that Conjecture 1.5 is valid, it is not clear how it can be established. 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.*

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.

[6] Ben-Sasson, E. and Viderman, M., 2009. Tensor products of weakly smooth codes are robust. Theory of Computing, 5(1), pp.239-255.

[7] Alon, N. and Capalbo, M., 2002, November. Explicit unique-neighbor expanders. In The 43rd Annual IEEE Symposium on Foundations of Computer Science, 2002. Proceedings. (pp. 73-79). IEEE.

[8] Becker, O., 2016. Symmetric unique neighbor expanders and good LDPC codes. Discrete Applied Mathematics, 211, pp.211-216.

[9] Sipser, M. and Spielman, D.A., 1996. Expander codes. IEEE transactions on Information Theory, 42(6), pp.1710-1722.

[10] Viderman, M., 2013. Linear-time decoding of regular expander codes. ACM Transactions on Computation Theory (TOCT), 5(3), pp.1-25.

[11] Dowling, M. and Gao, S., 2017. Fast Decoding of Expander Codes. IEEE Transactions on Information Theory, 64(2), pp.972-978.