Improved Upper Bounds on Stopping Redundancy

Junsheng Han and Paul H. Siegel, *Fellow, IEEE*

***Abstract*—For a linear block code with minimum distance d, its *stopping redundancy* is the minimum number of check nodes in a Tanner graph representation of the code, such that all nonempty stopping sets have size d or larger. We derive new upper bounds on stopping redundancy for all linear codes in general, and for maximum distance separable (MDS) codes specifically, and show how they improve upon previous results. For MDS codes, the new bounds are found by upper-bounding the stopping redundancy by a combinatorial quantity closely related to Turán numbers. (The *Turán number*, $T(v,k,t)$, is the smallest number of t-subsets of a v-set, such that every k-subset of the v-set contains at least one of the t-subsets.) Asymptotically, we show that the stopping redundancy of MDS codes with length n and minimum distance $d>1$ is $T(n,d-1,d-2)(1+O(n^{-1}))$ for fixed d, and is at most $T(n,d-1,d-2)(3+O(n^{-1}))$ for fixed code dimension $k=n-d+1$. For $d=3,4$, we prove that the stopping redundancy of MDS codes is equal to $T(n,d-1,d-2)$, for which exact formulas are known. For $d=5$, we show that the stopping redundancy of MDS codes is either $T(n,4,3)$ or $T(n,4,3)+1$.**

***Index Terms*—Erasure channel, iterative decoding, linear code, maximum distance separable (MDS) code, stopping set, Turán number.**

I. Introduction

It is well known [1] that the performance of a message-passing decoder on erasure channels is determined by certain combinatorial structures known as *stopping sets*. Unlike weight distribution, which is a property of the *code*, stopping sets are affected by the actual *representation* of the code. This brings up the problem of finding "good" and "efficient" representations of a code that are amenable to iterative decoding.

By "representations," we refer to Tanner graph representations [2], which directly correspond to parity-check matrices. (It should be noted that in our context, a parity-check matrix can have linearly dependent rows as long as the rows of the matrix span the dual code.) In a Tanner graph, a *stopping set* is a set of variable nodes all of whose neighbors are connected to the set at least twice. In the context of a parity-check matrix, a *stopping set* is a set of code coordinates such that the matrix formed by the corresponding columns of the parity-check matrix does not contain a row of weight one. We shall assume this latter definition throughout the rest of the paper. Given a parity-check matrix H, let the size of the smallest nonempty stopping set be termed the *stopping distance* [3] of the code with respect to H, denoted by $s(H)$. The importance of $s(H)$ has been widely recognized [1], [4]–[6]. The relationship of $s(H)$ to the performance of iterative erasure decoding is similar to that of minimum distance to the performance of maximum-likelihood (ML) decoding. For better performance, it is desired that $s(H)$ be maximized. Let $\mathcal{C}$ be a linear code and denote its minimum distance by $d(\mathcal{C})$. Since the support of any codeword is a stopping set, $s(H) \leq d(\mathcal{C})$ for all choices of H. It is known [3], [7] that by proper choice of H, $s(H)=d(\mathcal{C})$ can always be achieved. The *stopping redundancy* of $\mathcal{C}$, denoted by $\rho(\mathcal{C})$, is the minimum number of rows in a parity-check matrix H such that $s(H)=d(\mathcal{C})$.

Stopping redundancy was introduced by Schwartz and Vardy [3], [8], who derived general upper and lower bounds, as well as more specific bounds for Reed–Muller codes, Golay codes, and maximum distance separable (MDS) codes. The stopping redundancy of Reed–Muller and related codes was further studied by Etzion [9]. Effects of parity-check matrices on stopping set distribution were discussed by Weber and Abdel-Ghaffar [7], who found that by adding a small number of redundant parity checks, one can minimize the number of stopping sets of size 3 for a binary Hamming code. In related work, Hollmann and Tolhuizen [10], [11] consider collections of parity checks that correct all correctable erasure patterns up to a certain size for binary codes. There, emphasis was placed on (essentially) finding a *generic* r-column matrix with the least number of rows, having the property that when multiplied on the right by *any* matrix H with r independent rows, it produces a parity-check matrix that corrects all correctable erasure patterns up to size $m \leq r$ for the code defined by the null space of H.

In this paper, we obtain a number of new results on stopping redundancy. For all linear codes, we derive a new upper bound using probabilistic methods [12]. In the case of MDS codes, we show that their stopping redundancy is upper-bounded by a combinatorial quantity, by constructions of which new upper bounds are obtained. Our analysis reveals a strong coupling of the stopping redundancy of MDS codes and Turán numbers. The *Turán number*, $T(v,k,t)$, is the smallest number of t-subsets of a v-set, such that every k-subset of the v-set contains at least one of the t-subsets. It should be noted that the link between the stopping redundancy of MDS codes and *covering numbers*—the "dual" of Turán numbers, has been used in [3] to prove a number of lower bounds.

The rest of the paper is arranged as follows.

In Section II, we focus on general upper bounds. We start by giving an interesting variant of an upper bound from [3] for binary linear codes. We then derive a new upper bound using a probabilistic approach. We show that the new bound is tighter than other known bounds for many interesting cases. Particularly, we show that the bound based on probabilistic methods is asymptotically tighter for all "good" families of codes. The results are then extended to nonbinary codes.

Manuscript received November 14, 2005; revised July 6, 2006. The material in this paper was presented in part at the IEEE International Symposium on Information Theory, Seattle, WA, USA, July 2006.

The authors are with the Center for Magnetic Recording Research, University of California, San Diego, La Jolla, CA 92093-0401 USA (e-mail: han@cts.ucsd.edu; psiegel@ucsd.edu).

Communicated by R. J. McEliece, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2006.887513

Section III is devoted to MDS codes. First, we recall the observation made in [3] to show that for an MDS code $\mathcal{C}$ with length n and minimum distance d, $\rho(\mathcal{C}) \geq T(n, d-1, d-2)$. Next, by introducing a new combinatorial object, we convert the quest for upper bounds on $\rho(\mathcal{C})$ to a purely combinatorial problem. Proceeding in this way, we first discover that the lower bound of $T(n, d-1, d-2)$ is tight for small values of d. In particular, for $d = 3, 4$, we prove that $\rho(\mathcal{C}) = T(n, d-1, d-2)$, for which exact formulas are known, and, for $d = 5$, we show that $\rho(\mathcal{C})$ is no greater than $T(n, 4, 3) + 1$. We then generalize these results and show that for a fixed minimum distance d, the stopping redundancy of MDS codes is asymptotically equal to $T(n, d-1, d-2)$. Finally, we obtain tighter upper bounds through explicit constructions of the newly defined combinatorial object. One of the upper bounds further shows that for fixed code dimension $k = n-d+1$, the stopping redundancy of MDS codes is asymptotically at most $T(n, d-1, d-2)(3+O(n^{-1}))$.

Section IV concludes the paper.

II. General Bounds

A. Binary Linear Codes

Let $r(\mathcal{C})$ denote the *redundancy* of code $\mathcal{C}$, i.e., $r(\mathcal{C}) = \dim(\mathcal{C}^{\perp})$, where $\mathcal{C}^{\perp}$ is the dual code of $\mathcal{C}$. The following theorem is taken from [3].

Theorem 1: Let $\mathcal{C}$ be a binary linear code with $d(\mathcal{C}) \geq 3$. Then

$$\rho(\mathcal{C}) \leq \sum_{i=1}^{d(\mathcal{C})-2} \binom{r(\mathcal{C})}{i}. \tag{1}$$

□

Following the same idea, we derive the following bound, which is often better than (1).

Theorem 2: Let $\mathcal{C}$ be a binary linear code with $d(\mathcal{C}) \geq 2$. Then

$$\rho(\mathcal{C}) \leq \sum_{i=1}^{\lceil \frac{d(\mathcal{C})-1}{2} \rceil} \binom{r(\mathcal{C})}{2i-1}. \tag{2}$$

□

Proof: Take any basis of $\mathcal{C}^{\perp}$ to form a parity-check matrix H. If $\mathcal{C}$ is of length n, then H is an $r(\mathcal{C}) \times n$ matrix. Now, for every i rows of H, where i is odd and $1 \leq i \leq d(\mathcal{C}) - 1$, take their binary sum. Let a new matrix H' be formed consisting of all these binary sums as rows. Clearly, H' is a parity-check matrix for $\mathcal{C}$, and the number of rows in H' is exactly the quantity on the right-hand side of (2).

It suffices to show that $s(H') = d(\mathcal{C})$. For $t = 1, 2, \ldots, d(\mathcal{C})-1$, take an arbitrary set of t columns of H and form the matrix H_t. Take the corresponding t columns of H' and form the corresponding matrix H'_t. Since $t < d(\mathcal{C})$, the columns of H_t are linearly independent. Therefore, there exist t rows of H_t that form a basis for $\mathbb{F}_2^t$. Take t such rows of H_t and call this $t \times t$ matrix H_{tt}. Clearly, H_{tt} is full rank.

By construction, H'_t contains all sums of odd number of rows of H_{tt}. The proof is complete if we can show that at least one of these sums is of weight one. Think of summing rows of H_{tt} as multiplying H_{tt} by a binary row vector on the left. To find which rows of H_{tt} sum to a vector of weight one, one can simply solve for G in $GH_{tt} = I$, where I is the $t \times t$ identity matrix. Since the solution, $G = H_{tt}^{-1}$, is a full-rank binary matrix, it must contain at least one row of odd weight. ■

Remark: If $d(\mathcal{C})$ is odd, then the bound of (2) is always better than (1) as it sums a proper subset of the terms in (1), all of which are positive. If $d(\mathcal{C})$ is even, an improvement is not guaranteed since the bound in (2) includes the term $\binom{r(\mathcal{C})}{d(\mathcal{C})-1}$ while that in (1) does not. For the particular case where $r(\mathcal{C})$ grows with n while $d(\mathcal{C})$ remains fixed, (2) is asymptotically a looser bound. □

Remark: Bound (2) implies that $\rho(\mathcal{C}) \leq 2^{r(\mathcal{C})-1}$, an upper bound which cannot be deduced from (1). Note that $\rho(\mathcal{C}) \leq 2^{r(\mathcal{C})} - 1$ can be easily shown by considering a parity-check matrix that contains all nonzero codewords of $\mathcal{C}^{\perp}$. (See [3].) □

It was pointed out by one of the reviewers that a result in [10] actually implies both Theorems 1 and 2. That result, when applied to stopping redundancy, is summarized as follows.

Theorem 3: Let $\mathcal{C}$ be a binary linear code with $d(\mathcal{C}) \geq 3$. Then

$$\rho(\mathcal{C}) \leq \sum_{i=0}^{d(\mathcal{C})-2} \binom{r(\mathcal{C})-1}{i}. \qquad \square$$

The proof of Theorem 3 was based on very similar ideas, but was more careful in selecting the binary sums in the construction of the new parity-check matrix. It can be shown that Theorem 3 is the sam as Theorem 2 when $d(\mathcal{C})$ is odd, and is better than both Theorems 1 and 2 when $d(\mathcal{C})$ is even. In [13], Hollmann and Tolhuizen improve upon their constructions in [10] for the special case of even weight codes.

We now propose a new upper bound on $\rho(\mathcal{C})$ based on a probabilistic approach (cf. [12]).

Theorem 4: Let $\mathcal{C}$ be a binary linear code with length n. Then

$$\rho(\mathcal{C}) \leq \rho^*(n, d(\mathcal{C})) + r(\mathcal{C}) - d(\mathcal{C}) + 1 \tag{3}$$

where $\rho^*(n, d)$ is the smallest integer ρ^* that satisfies

$$\sum_{i=1}^{d-1} \binom{n}{i} \left(1 - \frac{i}{2^i}\right)^{\rho^*} < 1. \tag{4}$$

□

Proof: For any given number of rows ρ, consider a random ensemble of matrices $\mathcal{H}_\rho$, consisting of all $\rho \times n$ matrices whose rows are codewords of $\mathcal{C}^{\perp}$. Let the probability measure P on $\mathcal{H}_\rho$ be that which is induced when the rows of matrices in $\mathcal{H}_\rho$ are chosen uniformly and independently from $\mathcal{C}^{\perp}$.

Let $[n]^i$ denote the set of all i-element subsets of $\{1, 2, \ldots, n\}$. We refer to the elements of $[n]^i$ as *i-sets* and think of them as sets of vector coordinates. For a matrix H with n columns, we say that H *covers* $\iota \in [n]^i$ if the projection of rows of H onto ι contains a vector of weight one.

Clearly, $s(H) = d(\mathcal{C})$ if and only if H covers all i-sets for $i = 1, \ldots, d(\mathcal{C}) - 1$.

It is well known [14, p. 139] that the matrix of all codewords of $\mathcal{C}^\perp$ is an orthogonal array of strength $d(\mathcal{C}) - 1$. This implies that on any i-set, $i = 1, \ldots, d(\mathcal{C}) - 1$, all i-tuples appear, and they appear the same number of times. Since there are i weight-one vectors among a total of 2^i possible i-tuples, the probability that any given i-set is covered by a randomly chosen codeword of $\mathcal{C}^\perp$ is $i/2^i$. Hence, for $i = 1, \ldots, d(\mathcal{C}) - 1$, the probability that a given i-set is not covered by rows in a matrix in the random ensemble $\mathcal{H}_\rho$ is $(1 - i/2^i)^\rho$. We have

$$\begin{aligned}
&P\big(\{\text{all } i\text{-sets are covered, } i = 1, \ldots, d(\mathcal{C}) - 1\}\big) \\
&\quad = 1 - P\Big(\big\{\text{at least one } i\text{-set is not covered} \\
&\qquad\qquad \text{for some } i \in \{1, \ldots, d(\mathcal{C}) - 1\}\big\}\Big) \\
&\quad = 1 - P\left(\bigcup_{i=1}^{d(\mathcal{C})-1} \bigcup_{\iota \in [n]^i} \{\iota \text{ is not covered}\}\right) \\
&\quad \geq 1 - \sum_{i=1}^{d(\mathcal{C})-1} \sum_{\iota \in [n]^i} \left(1 - \frac{i}{2^i}\right)^\rho \\
&\quad = 1 - \sum_{i=1}^{d(\mathcal{C})-1} \binom{n}{i} \left(1 - \frac{i}{2^i}\right)^\rho.
\end{aligned}$$

If

$$\sum_{i=1}^{d(\mathcal{C})-1} \binom{n}{i} (1 - i/2^i)^\rho < 1$$

then $P(\{\text{all } i\text{-sets are covered, } i = 1, \ldots, d(\mathcal{C}) - 1\}) > 0$, which implies that there exists $H \in \mathcal{H}_\rho$ that covers all i-sets, $i = 1, \ldots, d(\mathcal{C}) - 1$. Note that the fact that H covers all i-sets up to $i = d(\mathcal{C}) - 1$ implies that $\operatorname{rank}(H) \geq d(\mathcal{C}) - 1$. Therefore, by adding at most $r(\mathcal{C}) - d(\mathcal{C}) + 1$ appropriate codewords from $\mathcal{C}^\perp$ as additional rows to H, we have found a parity-check matrix for $\mathcal{C}$ that covers all i-sets, $i = 1, \ldots, d(\mathcal{C}) - 1$. ∎

Note that Hollmann and Tolhuizen [15], [11] also use probabilistic methods in their analysis of generic erasure correcting sets.

The upper bound given in Theorem 4 involves solving an inequality. A closed-form expression would be desirable. This is addressed in the following corollaries.

Corollary 5: Let $\mathcal{C}$ be a binary linear code with length n and minimum distance $1 < d(\mathcal{C}) < n/2$. Then

$$\rho(\mathcal{C}) \leq \frac{nh(\delta) + \frac{1}{2}\log\frac{\delta}{2\pi n(1-\delta)(1-2\delta)^2}}{-\log\left(1 - \frac{d(\mathcal{C})-1}{2^{d(\mathcal{C})-1}}\right)} + r(\mathcal{C}) - d(\mathcal{C}) + 1$$

where $\delta = d(\mathcal{C})/n$, and $h(\delta) = -\delta\log\delta - (1-\delta)\log(1-\delta)$. □

Proof: First, note that $(1 - i/2^i)$ is nondecreasing for $i \in \mathbb{N}$, so that

$$\sum_{i=1}^{d-1} \binom{n}{i} \left(1 - \frac{i}{2^i}\right)^\rho \leq \left(1 - \frac{d-1}{2^{d-1}}\right)^\rho \sum_{i=1}^{d-1} \binom{n}{i}. \quad (5)$$

Next, for $0 < \delta = d(\mathcal{C})/n < 1/2$, it can be shown that

$$\sum_{i=1}^{d(\mathcal{C})-1} \binom{n}{i} < \frac{\delta}{1-2\delta} \binom{n}{\delta n}. \quad (6)$$

Further, by Stirling's approximation it is known that [16]

$$\binom{n}{\delta n} \leq \frac{1}{\sqrt{2\pi n\delta(1-\delta)}} 2^{nh(\delta)}. \quad (7)$$

Now, by putting together (5), (6), and (7), and referring to (4), we see that a positive solution to the equation

$$\frac{\delta}{1-2\delta} \frac{1}{\sqrt{2\pi n\delta(1-\delta)}} 2^{nh(\delta)} \left(1 - \frac{d(\mathcal{C})-1}{2^{d(\mathcal{C})-1}}\right)^\rho = 1$$

must be an upper bound on $\rho^*(n, d(\mathcal{C}))$. We thus obtain

$$\rho^*(n, d(\mathcal{C})) \leq \frac{nh(\delta) + \frac{1}{2}\log\frac{\delta}{2\pi n(1-\delta)(1-2\delta)^2}}{-\log\left(1 - \frac{d(\mathcal{C})-1}{2^{d(\mathcal{C})-1}}\right)}. \quad (8)$$

Plugging (8) in (3) we get the desired bound. ∎

If we do not require $d(\mathcal{C}) < n/2$, we have to weaken the upper bound, but the resulting bound has a simpler form.

Corollary 6: Let $\mathcal{C}$ be a binary linear code with length n and minimum distance $d(\mathcal{C}) > 1$. Then

$$\rho(\mathcal{C}) \leq \frac{n}{-\log\left(1 - \frac{d(\mathcal{C})-1}{2^{d(\mathcal{C})-1}}\right)} + r(\mathcal{C}) - d(\mathcal{C}) + 1. \quad (9)$$

□

Proof: The argument is almost identical to the proof of Corollary 5, except that we instead bound $\sum_{i=1}^{d(\mathcal{C})-1} \binom{n}{i}$ by

$$\sum_{i=1}^{d(\mathcal{C})-1} \binom{n}{i} < 2^n.$$ ∎

Remark: While the bounds in Theorems 1, 2, and 3 are roughly on the same order, the upper bound in Theorem 4 often appears to be tighter. We demonstrate this for a specific example—the extended binary Golay code—and for two asymptotic scenarios ($d(\mathcal{C})$ and $r(\mathcal{C})$ both linear in n, and $d(\mathcal{C})$ fixed).

Example 1: Let $\mathcal{G}_{24}$ denote the extended binary Golay $(24, 12, 8)$ code. In [3], it was shown by explicit construction that $\rho(\mathcal{G}_{24}) \leq 35$. This was later improved to $\rho(\mathcal{G}_{24}) \leq 34$ [8].

Applying the upper bounds obtained in this section to $\mathcal{G}_{24}$, we see that Theorem 1 gives $\rho(\mathcal{G}_{24}) \leq 2509$, Theorem 2 gives $\rho(\mathcal{G}_{24}) \leq 1816$, Theorem 3 gives $\rho(\mathcal{G}_{24}) \leq 1486$, and Theorem 4 gives $\rho(\mathcal{G}_{24}) \leq 232$. Also, the relaxed bounds in Corollaries 5 and 6 give $\rho(\mathcal{G}_{24}) \leq 245$ and $\rho(\mathcal{G}_{24}) \leq 300$, respectively. We see that in this example, bounds based on Theorem 4 have a clear advantage. □

Remark: A 34-row parity-check matrix for $\mathcal{G}_{24}$ that achieves maximum stopping distance is given in Appendix I. Compared

to the one reported in [8], this parity-check matrix is able to correct more low-weight erasure patterns. □

Example 2: The bound of Theorem 4 is a function of n, $d(\mathcal{C})$, and $r(\mathcal{C})$. Similarly, the bounds of Theorems 1, 2, and 3 are functions of $d(\mathcal{C})$ and $r(\mathcal{C})$. In this example, we consider the asymptotic behavior of these bounds as $n \to \infty$. Detailed derivations can be found in Appendix II.

We discuss two different assumptions about $d(\mathcal{C})$ and $r(\mathcal{C})$. The first case corresponds to "good" codes, i.e., codes whose rate is bounded away from zero and whose minimum distance is nondiminishing relative to the code length. The second case concerns codes with fixed minimum distance, an example of which is the family of extended binary Hamming codes.

Case 1: $d(\mathcal{C}) = \delta n$, $r(\mathcal{C}) = \gamma n$, where $0 < \delta < 1/2$, $0 < \gamma < 1$ are constants.

It can be shown that the bound in Theorem 4 is $\Theta(2^{\delta n})$.[1] In comparison, the bounds of Theorems 1, 2, and 3 are all $\Omega\left(2^{2\delta n}/\sqrt{n}\right)$. Clearly, the bound given by Theorem 4 is tighter.

Case 2: $d(\mathcal{C}) = d$ is a constant.

With the expression in Corollary 5, it is not hard to see that the bound of Theorem 4 is $\Theta(\log n + r(\mathcal{C}))$. On the other hand, the bound given by Theorem 1 is clearly $\Theta(r(\mathcal{C})^{d-2})$; the bound given by Theorem 2 is $\Theta(r(\mathcal{C})^{d-2})$ if d is odd, and $\Theta(r(\mathcal{C})^{d-1})$ if d is even; and the bound of Theorem 3 is $\Theta((r(\mathcal{C})-1)^{d-2})$.

By the Hamming bound, $r(\mathcal{C}) > \log n$ for $d \geq 3$. Therefore, as long as $d > 3$, the bound of Theorem 4 is asymptotically tighter. Since it is known for all binary linear codes [3] that if $d(\mathcal{C}) \leq 3$, then $\rho(\mathcal{C}) = r(\mathcal{C})$, Theorem 4 gives a better bound asymptotically for all nontrivial values of d. □

B. Linear Codes Over $\mathbb{F}_q$

The bounds in Theorems 1, 2, and 3 can all be viewed as improved versions of the more intuitive bound

$$\rho(\mathcal{C}) \leq \sum_{i=1}^{d(\mathcal{C})-1} \binom{r(\mathcal{C})}{i}$$

which extends in a straightforward manner to nonbinary codes (although, unfortunately, none of the improvements made in these theorems can be directly carried over).

Theorem 7: Let $\mathcal{C}$ be a linear code over $\mathbb{F}_q$. Then

$$\rho(\mathcal{C}) \leq \sum_{i=1}^{d(\mathcal{C})-1} \binom{r(\mathcal{C})}{i}(q-1)^{i-1}. \qquad \square$$

Proof: The proof is similar to that of Theorem 2. Here we take a basis of $\mathcal{C}^{\perp}$ and construct H by taking linear combinations of i basis vectors, $i = 1, \ldots, d(\mathcal{C}) - 1$, with nonzero coefficients. Note that for each set of i basis vectors, we may fix one of the linear coefficients at 1. ■

[1]We use the standard "big O" and related asymptotic notations, the definitions of which can be found in, for example, [17, Ch. 9].

For $\mathcal{C}$ a linear code over $\mathbb{F}_q$, the codewords of $\mathcal{C}^{\perp}$ are known to form an orthogonal array of strength $d(\mathcal{C}) - 1$ with q levels [18, Ch. 4]. Therefore, the argument we used to prove Theorem 4 extends directly to nonbinary codes.

Theorem 8: Let $\mathcal{C}$ be a linear code over $\mathbb{F}_q$ with length n. Then

$$\rho(\mathcal{C}) \leq \rho^*(n, d(\mathcal{C}), q) + r(\mathcal{C}) - d(\mathcal{C}) + 1$$

where $\rho^*(n, d, q)$ is the smallest integer ρ^* that satisfies

$$\sum_{i=1}^{d-1} \binom{n}{i} \left(1 - \frac{(q-1)i}{q^i}\right)^{\rho^*} < 1. \qquad \square$$

Corollary 9: Let $\mathcal{C}$ be a linear code over $\mathbb{F}_q$ with length n and minimum distance $1 < d(\mathcal{C}) < n/2$. Then

$$\rho(\mathcal{C}) \leq \frac{nh(\delta) + \frac{1}{2}\log\frac{\delta}{2\pi n(1-\delta)(1-2\delta)^2}}{-\log\left(1 - \frac{(q-1)(d(\mathcal{C})-1)}{q^{d(\mathcal{C})}-1}\right)} + r(\mathcal{C}) - d(\mathcal{C}) + 1$$

where $\delta = d(\mathcal{C})/n$, and $h(\delta) = -\delta\log\delta - (1-\delta)\log(1-\delta)$. □

Corollary 10: Let $\mathcal{C}$ be a linear code over $\mathbb{F}_q$ with length n and minimum distance $d(\mathcal{C}) > 1$. Then

$$\rho(\mathcal{C}) \leq \frac{n}{-\log\left(1 - \frac{(q-1)(d(\mathcal{C})-1)}{q^{d(\mathcal{C})}-1}\right)} + r(\mathcal{C}) - d(\mathcal{C}) + 1. \qquad \square$$

Example 3: Let $\mathcal{G}_{12}$ denote the extended ternary $(12, 6, 6)$ Golay code. The bound of Theorem 7 gives $\rho(\mathcal{G}_{12}) \leq 332$, while the bound of Theorem 8 gives $\rho(\mathcal{G}_{12}) \leq 160$. The best known result (by construction, see [3]) is $\rho(\mathcal{G}_{12}) \leq 22$. □

Example 4: Similar to Example 2 for the case of binary codes, we compare the bounds of Theorems 7 and 8 as $n \to \infty$. Here, we will only treat the case of "good" codes.

Let $d(\mathcal{C}) = \delta n$, $r(\mathcal{C}) = \gamma n$, where $0 < \delta < (q-1)/q$ and $0 < \gamma < 1$ are constants. It is not hard to show that the bound of Theorem 8 is $\Theta(q^{\delta n})$. On the other hand, it can be shown (details provided in Appendix II) that the bound of Theorem 7 is $\Omega\left(q^{\delta n q/(q-1)}/\sqrt{n}\right)$. We see that the bound given by Theorem 8 is tighter. □

III. MDS Codes

Being MDS imposes a lot of structure on a code. We will take advantage of the special properties of MDS codes to show that their stopping redundancy is of a highly combinatorial nature and is closely related to Turán numbers. New, tighter upper bounds will be obtained through constructions.

First, a few notes (reminders) on notation. Let n, k be integers and A, B be sets. Then

- $|A|$:= Number of elements of A;
- $A \setminus B := \{x \in A : x \notin B\}$;
- $[n] := \{1, 2, \ldots, n\}$;
- $[A]^k := \{X \subseteq A : |X| = k\}$ is the set of k-*subsets* of A;
- $[n]^k := [[n]]^k$.

Also, a k-*set* is generally any set that has k elements. Particular to our discussions, a k-set usually refers to a set of k codeword coordinates, i.e., a k-subset of $[n]$, if n is the length of the code.

A *Turán* (v,k,t)-*system* is a set of t-subsets of a v-set, called *blocks*, such that each k-subset of the v-set contains at least one of the blocks. The smallest number of blocks in a Turán (v,k,t)-system is known as the *Turán number*, and is correspondingly denoted by $T(v,k,t)$. For more information on Turán numbers, the reader is referred to [19], and references therein.

Consider an MDS code $\mathcal{C}$ of length n and minimum distance $d>1$. Then its dual code, $\mathcal{C}^{\perp}$, is an MDS code with minimum distance $d^{\perp}=n-d+2$. Also, note that for all MDS codes with minimum distance d, any set of d coordinates is the support of at least one codeword. These properties (and many more) can be found in MacWilliams and Sloane [14].

The authors of [3] noted the following.[2]

Theorem 11: Let $\mathcal{C}$ be a MDS code with length n and minimum distance $d>1$. Then

$$\rho(\mathcal{C}) \geq T(n,d-1,d-2). \qquad \square$$

Proof: Suppose H is a parity-check matrix for $\mathcal{C}$ and $s(H)=d$. Note that each row of H is a codeword in $\mathcal{C}^{\perp}$, and therefore has at most $n-d^{\perp}=d-2$ zeros. Now, if ι is any $(d-1)$-set, then since ι is not a stopping set, there exists a row of H with $d-2$ zeros whose positions are contained in ι. Since no $(d-1)$-sets are stopping sets, the complements of the supports of minimum-weight rows of H form a Turán $(n,d-1,d-2)$-system. ∎

This link between stopping redundancy and Turán numbers immediately gives rise to a number of lower bounds on $\rho(\mathcal{C})$ for MDS codes. For example, it is simple to note $T(v,k,t) \geq \binom{v}{k}/\binom{v-t}{k-t} = \binom{v}{t}/\binom{k}{t}$. So we immediately obtain

$$\rho(\mathcal{C}) \geq T(n,d-1,d-2) \geq \frac{1}{d-1}\binom{n}{d-2}$$

(cf. [3]). Better bounds can be obtained by utilizing a stronger lower bound on $T(v,k,t)$.

Now, let $\mathcal{C}$ be an MDS code with length n and minimum distance $d>1$, and consider the minimum number of rows in a parity-check matrix for $\mathcal{C}$ all of whose rows are minimum-weight codewords of $\mathcal{C}^{\perp}$ and that achieves the maximum stopping distance d. This number only depends on n and d, because

1) as far as covering i-sets is concerned, only the *supports* of rows of a parity-check matrix matter;
2) for any $d^{\perp}$-set as support, we can find at least one codeword in $\mathcal{C}^{\perp}$;
3) if such a parity-check matrix has a minimum number of rows, then all rows must have distinct supports.

[2]In [3], the observation was made with respect to covering numbers rather than Turán numbers. A (v,k,t) *covering design* is a set of k-subsets of a v-set, such that each t-subset of the v-set is contained in at least one of the k-subsets. The smallest size of a covering design is known as the *covering number*, and is correspondingly denoted by $C(v,k,t)$. It is simple to note that a (v,k,t) covering design is a Turán $(v,v-t,v-k)$-system and *vice versa*. Hence, $C(v,k,t)=T(v,v-t,v-k)$. For more information on covering designs and covering numbers, the reader is referred to [20].

Let us denote this number by $\Gamma'(n,d)$. Clearly, $\Gamma'(n,d)$ is an upper bound of $\rho(\mathcal{C})$. Note that $\Gamma'(n,d)$ always exists since a matrix consisting of one codeword from $\mathcal{C}^{\perp}$ for each $d^{\perp}$-set as support achieves stopping distance equal to d (cf. [3]).

We shall see that $\Gamma'(n,d)$ is in fact a combinatorial quantity with a formulation similar to that of Turán numbers, without any explicit reference to codes at all.

Definition 1: A *single-exclusion* (v,r)-*system* is a collection of r-subsets of a v-set, called *blocks*, such that for all i, $i=1,\ldots,r+1$, each i-subset of the v-set is covered by at least one of the blocks. Here, an i-subset ι is *covered* by block β if

$$|\iota \setminus \beta| = 1. \tag{10}$$

The smallest number of blocks in a single-exclusion (v,r)-system is called the *single-exclusion number*, and is denoted by $\Gamma(v,r)$. □

Remark: Clearly, condition (10) is equivalent to

$$|\iota \cap \beta| = i-1. \qquad \square$$

Remark: The definition of single-exclusion (v,r)-system requires that $r \leq v-1$. For $r=v-1$, it is easy to see that $\Gamma(v,v-1)=v$. For the sake of discussion, unless otherwise noted, we shall always make the assumption that $r \leq v-2$. In relation to $\rho(\mathcal{C})$, we are mostly interested in $\Gamma(n,d-2)$, where n is the length of $\mathcal{C}$ and d is the minimum distance. Clearly, $d-2 \leq n-2$ is always satisfied. □

Remark: A single-exclusion (v,r)-system is always a Turán $(v,r+1,r)$-system. It is interesting that the definition of single-exclusion systems may actually be interpreted meaningfully in design theory terms. One can analogously define k-exclusion (v,r)-systems. □

Let H be a parity-check matrix for $\mathcal{C}$ that achieves stopping distance d and whose rows all have weight $d^{\perp}$. Then the positions of zeros in the rows of H form a single-exclusion $(n,d-2)$-system. On the other hand, let S be a single-exclusion $(n,d-2)$-system. For each $\beta \in S$, we can find $c \in \mathcal{C}^{\perp}$ such that the support of c is $[n]\setminus\beta$. If we use these codewords as rows to form matrix H, then $s(H)=d$. Note that $s(H)=d$ implies that H has a $(d-1)\times(d-1)$ upper triangular submatrix (up to column permutations) and hence, $\operatorname{rank}(H) \geq d-1 = r(\mathcal{C}^{\perp})$. Therefore, H is indeed a parity-check matrix. In summary, an l-block single-exclusion $(n,d-2)$-system exists if and only if an l-row parity-check matrix consisting solely of minimum-weight codewords of $\mathcal{C}^{\perp}$ can be found that achieves maximum stopping distance. Relating to the earlier definition, it is clear that $\Gamma'(n,d)=\Gamma(n,d-2)$.

The following comes straight from the discussion above.

Theorem 12: If $\mathcal{C}$ is an MDS code with length n and minimum distance $d>1$, then

$$\rho(\mathcal{C}) \leq \Gamma(n,d-2). \qquad \square$$

We conjecture that equality holds always.

Conjecture 13: If $\mathcal{C}$ is an MDS code with length n and minimum distance $d > 1$, then

$$\rho(\mathcal{C}) = \Gamma(n, d-2). \qquad \square$$

Up to now we have bounded $\rho(\mathcal{C})$ between two well-defined combinatorial quantities, $T(n, d-1, d-2)$ and $\Gamma(n, d-2)$. Clearly, any lower bound on $T(n, d-1, d-2)$ is a lower bound on $\rho(\mathcal{C})$ and any upper bound on $\Gamma(n, d-2)$ is an upper bound on $\rho(\mathcal{C})$. We will actually proceed in this way—in fact, we will be focusing solely on the upper bound, and all results we shall show for $\rho(\mathcal{C})$ hold for $\Gamma(n, d-2)$ as well, although it may not be made explicit.

We start by looking at how things work for $d = 2, 3, 4, 5$, where much stronger results can be derived.

If $d = 2$, then $\rho(\mathcal{C}) = T(n, 1, 0) = \Gamma(n, 0) = 1$.

The case where $d = 3$ is also quite trivial, and the result is actually implied by the best upper and lower bounds on $\rho(\mathcal{C})$ given in [3].

Theorem 14: Let $\mathcal{C}$ be an MDS code with length n and minimum distance $d = 3$. Then

$$\rho(\mathcal{C}) = T(n, 2, 1) = n - 1. \qquad \square$$

Proof: It suffices to show that $n - 1 \leq T(n, 2, 1) \leq \Gamma(n, 1) \leq n - 1$. On one hand, it is easy to verify that any $(n-1)$-subset of $[n]^1$ is a single-exclusion $(n, 1)$-system. On the other hand, a Turán $(n, 2, 1)$-system cannot have $(n-2)$ or fewer blocks, or there would exist $i, j \in [n]$, such that $\{i, j\}$ does not contain any of the blocks. ∎

The case for $d = 4$ needs a bit more work.

Lemma 15: For all $n \geq 3$

$$T(n, 3, 2) \leq \binom{n-3}{2} + 3. \qquad \square$$

Proof: The proof is by construction. Let $L = \{1, 2, 3\}$, $R = [n] \setminus L$, and $T = [L]^2 \cup [R]^2$. It is easy to verify that T is a Turán $(n, 3, 2)$-system, and it has $\binom{n-3}{2} + 3$ blocks. ∎

Theorem 16: Let $\mathcal{C}$ be an MDS code with length $n \geq 6$ and minimum distance $d = 4$. Then

$$\rho(\mathcal{C}) = T(n, 3, 2) = \left\lfloor \frac{n}{2} \right\rfloor \left(\left\lceil \frac{n}{2} \right\rceil - 1 \right). \qquad \square$$

Proof: The formula for $T(n, 3, 2)$ is a known result first discovered by Mantel [21] in 1907. Later, Turán [22], [23] solved the more general case of $T(n, k, 2)$.

It suffices to show that $\Gamma(n, 2) \leq T(n, 3, 2)$. Let T be a Turán $(n, 3, 2)$-system with smallest size. We show that T must also be a single-exclusion $(n, 2)$-system. By definition of T, all 3-sets are covered. We show that all 1- and 2-sets are covered as well.

Suppose there is a 1-set, say $\{i\}$, that is not covered. Then i is contained in all blocks of T. But this implies that all 3-subsets of $[n] \setminus \{i\}$ are not covered, contradicting the fact that T is a Turán $(n, 3, 2)$-system.

Suppose there is a 2-set, say $\{i, j\}$, that is not covered. This implies that a block of T either is $\{i, j\}$, or is disjoint from $\{i, j\}$. Note that $\{i, j\}$ must be a block of T, or 3-sets like $\{i, j, k\}$ would not be covered. Also, all 2-sets disjoint from $\{i, j\}$ must be blocks of T; otherwise, if $\{k, l\} \subseteq [n] \setminus \{i, j\}$ is not a block, then 3-set $\{i, k, l\}$ would not be covered by T. This shows that $T(n, 3, 2) = |T| = \binom{n-2}{2} + 1$. But $\binom{n-2}{2} + 1 > \binom{n-3}{2} + 3$ for $n \geq 6$, which contradicts Lemma 15. ∎

Remark: Since the formula for $T(n, 3, 2)$ is known, Lemma 15 may seem unnecessary. But we find its simple construction to be appealing, and the bound it gives, though loose, is enough to show $\Gamma(n, 2) = T(n, 3, 2)$ without further knowledge about $T(n, 3, 2)$. $\square$

Remark: The proof of Theorem 16 needs $n \geq 6$ to go through. It turns out that the only two cases for $n < 6$ are indeed "anomalies" for which $\rho(\mathcal{C})$ is strictly greater than $T(n, 3, 2)$.

For $n = 4$, $T(4, 3, 2) = 2$, while it is simple to see that $\rho(\mathcal{C}) = 3$. For $n = 5$, $T(5, 3, 2) = 4$. But it can be shown that $\rho(\mathcal{C}) = 5$. $\square$

For $d = 5$, we first note a couple of bounds on $T(n, 4, 3)$.

Lemma 17:

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

where equality holds for $n \leq 13$. $\square$

Proof: The upper bound comes from a construction of Turán $(n, 4, 3)$-systems due to Ringel [24], which has been verified to be optimal for $n \leq 13$ [20]. ∎

Lemma 18: For $n \geq 13$

$$T(n, 4, 3) \geq \frac{56}{143} \binom{n}{3}. \qquad \square$$

Proof: It is known [25] that $T(n, k, r) / \binom{n}{r}$ is nondecreasing in n, hence

$$T(n, k, r) \geq \frac{T(n_0, k, r)}{\binom{n_0}{r}} \binom{n}{r}, \qquad \text{for } n \geq n_0.$$

Since $T(13, 4, 3) = 112$ by Lemma 17, the result follows. ∎

Theorem 19: Let $\mathcal{C}$ be an MDS code with length n and minimum distance $d = 5$. Then

$$T(n, 4, 3) \leq \rho(\mathcal{C}) \leq T(n, 4, 3) + 1.$$

Further

$$\rho(\mathcal{C}) = T(n, 4, 3), \qquad \text{for } n = 6, \ldots, 53. \qquad \square$$

Proof: It suffices to show that $\Gamma(n, 3) \leq T(n, 4, 3) + 1$ and $\Gamma(n, 3) = T(n, 4, 3)$ for $n = 6, \ldots, 53$.

For $n = 5$, it is known that $T(5, 4, 3) = 3$, while it can be easily verified that $\Gamma(5, 3) = 4$. So the claimed inequality holds for $n = 5$.

In the following, assume $n \geq 6$. Let T be a Turán $(n, 4, 3)$-system of smallest size. If T is a single-exclusion $(n, 3)$-system then we are done. Otherwise, let ι be a *smallest* i-set that is not covered. Then $|\iota| = 1, 2$, or 3. (All 4-sets are covered since T is a Turán $(n, 4, 3)$-system.)

First, suppose $|\iota| = 1$. Since ι is not covered, it is contained in all blocks of T. Then a 4-subset of $[n] \setminus \iota$ is not covered. This is a contradiction.

Next, suppose $|\iota| = 2$, say $\iota = \{i, j\}$. Then any block of T either contains ι or is disjoint from ι. Out of the $(n-2)$ 3-sets that contain ι, at least $(n-3)$ must be in T. Otherwise, we could find $a, b \in [n] \setminus \iota$ such that $\{i, j, a\}, \{i, j, b\} \notin T$. But then the 4-set $\{i, j, a, b\}$ would not be covered. On the other hand, all of the $\binom{n-2}{3}$ 3-sets that are disjoint from ι must be blocks of T. Otherwise, if $\{a, b, c\} \subseteq [n] \setminus \iota$ is not a block, then $\{i, a, b, c\}$ would not be covered. In summary, T must have at least $\binom{n-2}{3} + n - 3$ blocks. Since

$$\binom{n-2}{3} + n - 3 > \left\lfloor \frac{n}{3} \right\rfloor \left\lfloor \frac{n-1}{3} \right\rfloor \left(2 \left\lfloor \frac{n-2}{3} \right\rfloor + 1 \right)$$

for $n \geq 6$, this contradicts Lemma 17.

Finally, suppose $|\iota| = 3$, say $\iota = \{i, j, k\}$. Then for all $\beta \in T$, $|\beta \cap \iota| \neq 2$. Note the following facts.

Fact 1: ι itself must be a block of T, otherwise 4-sets like $\{i, j, k, a\}$ would not be covered.

Fact 2: For each 2-set $\{a, b\} \subseteq [n] \setminus \iota$, at least two of $\{a, b, i\}$, $\{a, b, j\}$, and $\{a, b, k\}$ must be blocks of T. This is true because if, say, $\{a, b, i\}$ and $\{a, b, j\}$ both were not blocks of T, then $\{a, b, i, j\}$ would not be covered.

Fact 3: All blocks that are disjoint from ι form a Turán $(n-3, 4, 3)$-system.

Together, these imply that

$$T(n, 4, 3) = |T| \geq 1 + 2\binom{n-3}{2} + T(n-3, 4, 3)$$

which contradicts Lemmas 17 and 18 for $n = 6, \ldots, 53$.

For $n \geq 54$, we do not have an immediate contradiction. However, note that a 3-set that contains zero or one element of ι is covered due to Fact 2, and one that contains two elements of ι is covered due to Fact 1. So, in this case ι must be the only 3-set that is not covered. Since ι is also the smallest uncovered i-set, by adding one more block to T to cover ι, we have found a single-exclusion $(n, 3)$-system that has $T(n, 4, 3) + 1$ blocks. ■

Corollary 20: Let $\mathcal{C}$ be an MDS code with length n and minimum distance $d = 5$. Then

$$\rho(\mathcal{C}) = \left\lfloor \frac{n}{3} \right\rfloor \left\lfloor \frac{n-1}{3} \right\rfloor \left(2 \left\lfloor \frac{n-2}{3} \right\rfloor + 1 \right), \quad \text{for } n = 6, \ldots, 13.$$

□

We have seen that $\Gamma(n, d-2)$ (and hence $\rho(\mathcal{C})$ of an MDS code with the corresponding parameters) is almost the same as $T(n, d-1, d-2)$ for small values of d. We now show that these results can be generalized in an asymptotic sense when d is fixed.

Theorem 21: For fixed d, $d > 1$, as $n \to \infty$

$$\Gamma(n, d-2) = T(n, d-1, d-2)(1 + O(n^{-1})).$$ □

Proof: We show that we can always add $O(n^{d-3})$ blocks to a Turán $(n, d-1, d-2)$-system to make it a single-exclusion $(n, d-2)$-system.

Let $L = \{1, \ldots, d-2\}$ and $R = [n] \setminus L$. Let $T' = \{\beta \in [n]^{d-2} : \beta \cap L \neq \emptyset\}$. Clearly

$$|T'| = \sum_{m=0}^{d-3} \binom{d-2}{d-2-m} \binom{n-d+2}{m} = O(n^{d-3}).$$

We show that blocks of T' cover all i-sets, $i = 1, 2, \ldots, d-2$. Let ι be an i-set and $a \in \iota$ be an arbitrary element. Take $\iota \setminus \{a\}$, adjoin to it the $(d-i-1)$ smallest elements of $[n] \setminus \iota$ and call the resulting set β. It is easy to verify that $\beta \in T'$ and $|\iota \setminus \beta| = 1$.

Now, let T be a Turán $(n, d-1, d-2)$-system of smallest size. Let $S = T \cup T'$. Then S is a single-exclusion $(n, d-2)$-system with $T(n, d-1, d-2) + O(n^{d-3})$ blocks.

Finally, note that $T(n, d-1, d-2) = \Theta(n^{d-2})$, since

$$\frac{1}{d-1}\binom{n}{d-2} \leq T(n, d-1, d-2) \leq \binom{n}{d-2}$$

and the result follows. ■

With Theorems 11, 12, and 21, the following result is immediate.

Theorem 22: Let $\{\mathcal{C}_i\}_{i=1}^{\infty}$ be a sequence of MDS codes with strictly increasing code length $\{n_i\}_{i=1}^{\infty}$. If $d(\mathcal{C}_i) = d > 1$ for all i, then as $i \to \infty$,

$$\rho(\mathcal{C}_i) = T(n, d-1, d-2)(1 + O(n^{-1}))$$

where $n = n_i$. □

Katona, Nemetz, and Simonovits [25] showed that $T(n, k, r)/\binom{n}{r}$ is nondecreasing in n and hence there exists the limit

$$t(k, r) = \lim_{n \to \infty} \frac{T(n, k, r)}{\binom{n}{r}}.$$

Theorems 21 and 22 essentially tell us that for fixed d, $T(n, d-1, d-2)$, $\rho(\mathcal{C}_i)$, and $\Gamma(n, d-2)$ are all asymptotic to $t(d-1, d-2)\binom{n}{d-2}$.[3]

Corollary 23: Let $\{\mathcal{C}_i\}_{i=1}^{\infty}$ be a sequence of MDS codes with strictly increasing code length $\{n_i\}_{i=1}^{\infty}$. If $d(\mathcal{C}_i) = d > 1$ for all i, then

$$\lim_{i \to \infty} \frac{\rho(\mathcal{C}_i)}{\binom{n_i}{d-2}} = \lim_{n \to \infty} \frac{\Gamma(n, d-2)}{\binom{n}{d-2}} = t(d-1, d-2).$$ □

The value of $t(r+1, r)$, although unknown for $r > 2$, is well studied. In fact, the determination of $t(k, r)$ for $k > r > 2$ has been one of the most challenging open problems in combinatorial theory (for the solution of which Erdös offered a $1000

[3]Functions $f(x)$ and $g(x)$ are said to be asymptotic to each other as $x \to x_0$ if $\lim_{x \to x_0} \frac{f(x)}{g(x)} = 1$, and is denoted by $f(x) \sim g(x)$. In this paper we usually talk about integer functions of n and the condition $n \to \infty$ is sometimes omitted where there is no confusion.

TABLE I
SOME KNOWN BOUNDS ON $t(r+1,r)$

r	Lower Bound	Upper Bound
2	$\frac{1}{2}$	$\frac{1}{2}$
3	$\frac{9-\sqrt{17}}{12}$	$\frac{4}{9}$
4	$\frac{37}{143}$	$\frac{5}{16}$
5	$\frac{37-\sqrt{345}}{80}$	$\frac{5}{16}$
6	$\frac{1}{6}$	$\frac{17}{64}$
asymp.	$\frac{1}{r}$	$\left(\frac{1}{2}+o(1)\right)\frac{\ln r}{r}$

award; see [26]). Some of the known bounds on $t(r+1,r)$ are summarized in Table I (cf. [22], [23], [19], [27]–[31]).

In contrast, the bounds on $\rho(\mathcal{C})$ for MDS codes given in [3] are

$$\frac{1}{d-1} \le \frac{\rho(\mathcal{C})}{\binom{n}{d-2}} \le \frac{\max\{d^\perp, d-1\}}{n}. \tag{11}$$

Compared to what is promised by Corollary 23 and Table I, here the lower bound is already close to our best knowledge of $t(r+1,r)$. On the other hand, since $d^\perp + d - 1 = n+1$, $\max\{d^\perp, d-1\}/n > 1/2$. This suggests room for improvement in the upper bound.

We will derive new upper bounds on the stopping redundancy of MDS codes through constructions of single-exclusion systems. First, consider the following construction of a Turán $(n, r+1, r)$-system due to Kim and Roush [32].

Construction 1: Partition $[n]$ into l disjoint sets, $N_0, \ldots, N_{l-1}$, with sizes as equal as possible. (For example, let $N_i := \{k \in [n] : k \equiv i \mod l\}$.) For any $X \subseteq [n]$, define

$$w(X) := \sum_{i=0}^{l-1} i|X \cap N_i|.$$

For $j = 0, 1, \ldots, l-1$, let

$$\mathcal{B}_j := \{B \in [n]^r : \exists k, B \cap N_k = \emptyset\} \cup \{B \in [n]^r : w(B) \equiv j \mod l\}. \tag{12}$$

□

Theorem 24 ([32]): For all l and all j, $\mathcal{B}_j$ as defined in Construction 1 is a Turán $(n, r+1, r)$-system. □

Proof: Let $C \in [n]^{r+1}$ be any $(r+1)$-set. If there exists k such that $C \cap N_k = \emptyset$, then any $B \in [C]^r$ satisfies $B \cap N_k = \emptyset$ and hence is a member of $\mathcal{B}_j$. Otherwise, we can find $c_k \in C \cap N_k$ for all k. Let $B_k := C \setminus \{c_k\}$. Then $B_k \in [C]^r$. Note that $w(B_k) = w(C) - k$, $k = 0, \ldots, l-1$. So by choosing k we can realize any value of $(w(B_k) \mod l)$. Therefore, for any j, there exists k such that $B_k \in \mathcal{B}_j$. ■

Theorem 25: For all j, $\mathcal{B}_j$ as defined in Construction 1 is a single-exclusion (n, r)-system if $l \ge n/(n-r-1)$. □

Proof: Given Theorem 24, it suffices to show that for any $C \in [n]^i$, $i = 1, \ldots, r$, there exists $B \in \mathcal{B}_j$ such that $|C \setminus B| = 1$.

If there exists k such that $C \cap N_k = \emptyset$, pick $D \in [[n] \setminus N_k]^{r+1}$ such that $C \subseteq D$. The availability of such a choice is guaranteed if $n - \lceil n/l \rceil \ge r+1$, which is implied by $l \ge n/(n-r-1)$. Let $B = D \setminus \{c\}$ where c is an arbitrary element of C. Then $B \in \mathcal{B}_j$ since $B \cap N_k = \emptyset$. Also, $|C \setminus B| = |\{c\}| = 1$.

On the other hand, if for all k, $C \cap N_k \ne \emptyset$, we can find $c_k \in C \cap N_k$ for all k. Pick $D \in [n]^{r+1}$ such that $C \subseteq D$. Let $B_k := D \setminus \{c_k\}$. Similarly to the proof of Theorem 24, we can show that for any j, there exists k such that $B_k \in \mathcal{B}_j$. Also, by construction, $|C \setminus B_k| = |\{c_k\}| = 1$. ■

Now, we wish to estimate the smallest number of blocks in $\mathcal{B}_j$. Note

$$\begin{aligned}
\min_{0 \le j \le l-1} |\mathcal{B}_j| &\le \min_{0 \le j \le l-1} \left(|\{B \in [n]^r : \exists k, B \cap N_k = \emptyset\}| \right. \\
&\quad \left. + |\{B \in [n]^r : w(B) \equiv j \mod l\}| \right) \\
&= \left| \bigcup_{k=0}^{l-1} \{B \in [n]^r : B \cap N_k = \emptyset\} \right| \\
&\quad + \min_{0 \le j \le l-1} |\{B \in [n]^r : w(B) \equiv j \mod l\}| \\
&\le \sum_{k=0}^{l-1} |\{B \in [n]^r : B \cap N_k = \emptyset\}| + \frac{1}{l}\binom{n}{r} \\
&\le l\binom{n - \lfloor \frac{n}{l} \rfloor}{r} + \frac{1}{l}\binom{n}{r}.
\end{aligned} \tag{13}$$

Therefore, we arrive at the following upper bound on $\Gamma(n, r)$.

Theorem 26: For all integers $l \ge n/(n-r-1)$

$$\Gamma(n,r) \le l\binom{n - \lfloor \frac{n}{l} \rfloor}{r} + \frac{1}{l}\binom{n}{r}.$$ □

This immediately leads to an upper bound on $\rho(\mathcal{C})$.

Theorem 27: Let $\mathcal{C}$ be an MDS code with length n and minimum distance $d > 1$. For all integers $l \ge R^{-1}$, where $R = (n-d+1)/n$ is the code rate of $\mathcal{C}$,

$$\rho(\mathcal{C}) \le l\binom{n - \lfloor \frac{n}{l} \rfloor}{d-2} + \frac{1}{l}\binom{n}{d-2}.$$ □

Let us interpret this upper bound asymptotically as $n \to \infty$. Consider the following cases.

1) d is fixed:
   Assume $d > 3$. By choosing $l = \lceil (d-2)/(2\ln(d-2)) \rceil$, one can show that the upper bound of Theorem 27 is asymptotically better than $\frac{1+2\ln(d-2)}{d-2}\binom{n}{d-2}$, while the best upper bound from [3] (as given in (11)) is asymptotic to $\binom{n}{d-2}$. This shows that for all $d > 5$, the bound of Theorem 27 is asymptotically tighter. Note that for this particular case we already knew more—Corollary 23 gives a better understanding of the asymptotic behavior of $\rho(\mathcal{C})$, and a tighter bound on $t(d-1, d-2)$ could have been used. The upper bound in Theorem 27 is valuable in that it is exact—it holds for all n, rather than only asymptotically in n.
2) $d/n = \delta < 1$ is fixed:
   Choosing $l = \lceil (d-2)/(2\ln(d-2)) \rceil$, we see that the upper bound of Theorem 27 is $O\left(\frac{\ln n}{n}\binom{n}{d-2}\right)$, which is better than $\Theta\left(\binom{n}{d-2}\right)$, given by (11). Note that from (11), $\rho(\mathcal{C})$ is at least $\Theta\left(\frac{1}{n}\binom{n}{d-2}\right)$.

3) $k = n - d + 1$, the dimension of $\mathcal{C}$, is fixed:
Theorem 27 requires that $l \geq n/k$. If $k \geq 4$, we can choose l such that $l \in (n/3-1, n/3]$. Then the bound of Theorem 27 becomes, asymptotically,

$$\begin{aligned}\rho(\mathcal{C}) &\leq l\binom{n-\left\lfloor \frac{n}{l} \right\rfloor}{d-2} + \frac{1}{l}\binom{n}{d-2} \\ &\leq l\binom{n-3}{n-k-1} + \frac{1}{l}\binom{n}{n-k-1} \\ &= O(n^{k-1}) + \frac{3}{n}\left(1 + O\left(\frac{1}{n}\right)\right)\binom{n}{k+1} \\ &= O(n^{k-1}) + \frac{3}{k+1}\binom{n}{k}.\end{aligned}$$

The bound above is asymptotic to $\frac{3}{k+1}\binom{n}{k}$. For comparison, (11) implies an upper bound that is asymptotic to $\binom{n}{k+1}$, and a lower bound of $\frac{1}{k+1}\binom{n}{k}$.

The last case of the discussion above is interesting in its own right and we summarize it in the following theorems. Note that what we have talked about applies to $\Gamma(n, d-2) = \Gamma(n, n-k-1)$ as well as $\rho(\mathcal{C})$.

Theorem 28: For fixed k, as $n \to \infty$,

$$\frac{1}{k+1} \leq \frac{\Gamma(n, n-k-1)}{\binom{n}{k}} \leq \frac{3}{k+1} + O\left(n^{-1}\right). \qquad \square$$

Proof: The lower bound is trivial since

$$T(n, n-k, n-k-1) \geq \frac{1}{k+1}\binom{n}{k}.$$

Also, we have seen that the claimed upper bound is true for $k \geq 4$.

For $k = 3$, note that if we had been a bit more careful in writing (13), we could have shown that

$$\begin{aligned}\Gamma(n, r) \leq (l - (n \mod l))&\binom{n-\left\lfloor \frac{n}{l} \right\rfloor}{r} \\ &+ (n \mod l)\binom{n-\left\lfloor \frac{n}{l} \right\rfloor - 1}{r} + \frac{1}{l}\binom{n}{r}. \quad (14)\end{aligned}$$

Choosing l such that $l \in [n/3, n/3+1)$ and noting $l - (n \mod l) < 3$ if $3 \nmid n$ gives the desired result.

For $k = 2$, we show that we can construct a single-exclusion $(n, n-3)$-system using less than $\frac{2}{3}\binom{n}{2}$ blocks. Let $n = 3t + r$, $r = 0, 1, 2$. Consider the n-set

$$N := ([t] \times \{0, 1, 2\}) \cup (\{t+1\} \times \{0, \ldots, r-1\}).$$

Choose as blocks the complements of the following triples (if they exist in N) to construct S:

1) $\{(x, 0), (x, 1), (x, 2)\}$, for $x = 1, \ldots, t$;
2) $\{(x, i), (y, i), (y, i+1)\}$ and $\{(x, i), (x, i+1), (y, i)\}$, for $x, y \in [t+1]$, $x < y$, $i = 0, 1, 2$;
3) $\{(x, 0), (x, 2), (t+1, 0)\}$, for $x = 1, \ldots, t$, if $r > 0$.

(In the above, $i+1$ is modulo 3.) We claim that S is a single-exclusion $(n, n-3)$-system. Let ι be an i-set. We show that ι is covered in that there exists $\beta \in S$ such that $|\iota \setminus \beta| = 1$, i.e., such that $|\iota^c \cap \beta^c| = 2$. Let us call the set of points in N that share a common first coordinate a *bin*. It is not hard to verify that if ι^c intersects some bin at exactly two points, then ι is covered. Also, if ι^c intersects some two bins each at just one point, then ι is also covered. Now, excluding the two cases already discussed above, we may assume that ι^c intersects no bins at two points, and intersects at most one bin at one point. But since $|\iota^c| \geq 2$, ι^c must intersect some bin at three points. This fact, however, also implies that ι is covered. Finally, it is simple algebra to verify that $|S| < \frac{2}{3}\binom{n}{2}$.

For $k = 1$, it is not hard to see that $\Gamma(n, n-2) = n - 1$. (Note in this case $T(n, n-1, n-2) = \lceil n/2 \rceil$.) ■

The following is an immediate consequence of Theorem 28.

Theorem 29: Let $\{\mathcal{C}_i\}_{i=1}^{\infty}$ be a sequence of MDS codes with strictly increasing code length $\{n_i\}_{i=1}^{\infty}$. If the dimension of $\mathcal{C}_i$ is k for all i, then, as $i \to \infty$,

$$\frac{1}{k+1} \leq \frac{\rho(\mathcal{C}_i)}{\binom{n}{k}} \leq \frac{3}{k+1} + O\left(n^{-1}\right),$$

where $n = n_i$. $\square$

Previously we have seen a close connection between $\Gamma(n, d-2)$ and $T(n, d-1, d-2)$. Let us see what the results of Theorems 28 and 29 tell us in those terms.

Theorem 30: For fixed k, as $n \to \infty$,

$$\Gamma(n, n-k-1) \leq T(n, n-k, n-k-1)(3 + O(n^{-1})). \ \square$$

Proof: It suffices to note that $T(n, n-k, n-k-1) \geq \frac{1}{k+1}\binom{n}{k}$, and the result follows directly from Theorem 28. It should be noted that for fixed a and b, $T(v, v-b, v-a)$ is asymptotic to $\binom{v}{b}/\binom{a}{b}$ (cf. [33], [34]). Therefore, if k is fixed, then $T(n, n-k, n-k-1) \sim \frac{1}{k+1}\binom{n}{k}$ and the claimed result is indeed the best that one can get out of Theorem 28. ■

Theorem 31: Let $\{\mathcal{C}_i\}_{i=1}^{\infty}$ be a sequence of MDS codes with strictly increasing code length $\{n_i\}_{i=1}^{\infty}$. If the dimension of $\mathcal{C}_i$ is k for all i, then, as $i \to \infty$,

$$\rho(\mathcal{C}_i) \leq T(n, d-1, d-2)(3 + O(n^{-1})),$$

where $n = n_i$, $d = d(\mathcal{C}_i) = n_i - k + 1$. $\square$

Remark: The proof of Theorem 28 shows that for $k = 1, 2$,

$$\Gamma(n, n-k-1) \leq T(n, n-k, n-k-1)(2 + O(n^{-1})).$$

Empirical data suggest that this may be true for all k, so that it may be possible for the constant factor of 3 to be improved. $\square$

Next, consider the following construction of a Turán $(n, r+1, r)$-system, due to Frankl and Rödl [35].

Construction 2: Partition $[n]$ into l disjoint sets, $N_0, \ldots, N_{l-1}$, with sizes as equal as possible. For all $X \subseteq [n]$, define $S(X) := \{i : X \cap N_i \neq \emptyset\}$ and $s(X) := |S(X)|$. So $s(X)$ is the number of partitions that X intersects. Also, define

$$w(X) := \sum_{i=0}^{l-1} i|X \cap N_i|.$$

Now, for $j \in \{0,\ldots,l-1\}$, let

$$\mathcal{B}_j := \{B \in [n]^r : (w(B)+j) \mod l \in \{0,1,\ldots,l-s(B)\}\}. \quad (15)$$

□

Theorem 32 ([35]): For all l and all j, $\mathcal{B}_j$ constructed according to Construction 2 is a Turán $(n, r+1, r)$-system. □

Proof: Note that in general, if $x \in X \cap N_i$, then $w(X \setminus \{x\}) = w(X) - i$. Let X be an $(r+1)$-set. Since X intersects $s(X)$ partitions, $\{(w(Y)+j) \mod l : Y \in [X]^r\}$ contains $s(X)$ distinct values. Hence, there exists $Y \in [X]^r$, such that $(w(Y)+j) \mod l \in \{0,1,\ldots,l-s(X)\}$. Now, note that $s(Y) \le s(X)$ since $Y \subseteq X$. Therefore, $(w(Y)+j) \mod l \in \{0,1,\ldots,l-s(Y)\}$, which implies that $Y \in \mathcal{B}_j$. ■

Theorem 33: If $n \ge l(r+1)$, then for all j, $\mathcal{B}_j$ constructed according to Construction 2 is a single-exclusion (n,r)-system. □

Proof: Given Theorem 32, it suffices to show that all i-sets are covered by $\mathcal{B}_j$, $i = 1,\ldots,r$.

Let X be an i-set. Choose $Z \in [n]^{(r+1)}$, such that $X \subseteq Z$ and $S(Z) = S(X)$. This is possible as

$$\left|\bigcup_{k\in S(X)} N_k\right| \ge s(X)(r+1) \ge r+1.$$

Consider the class of r-sets, $\mathcal{Y} := \{Z \setminus \{x\} : x \in X\}$. Note that $\{(w(Y)+j) \mod l : Y \in \mathcal{Y}\}$ contains $s(X)$ distinct values. Hence, there exists $Y \in \mathcal{Y}$, such that

$$(w(Y)+j) \mod l \in \{0,1,\ldots,l-s(X)\}.$$

Now, note that $Y \subseteq Z$ implies that $s(Y) \le s(Z) = s(X)$. Therefore, $(w(Y)+j) \mod l \in \{0,1,\ldots,l-s(Y)\}$, which implies that $Y \in \mathcal{B}_j$. Finally, it is clear that $|X \setminus Y| = 1$. ■

Now we wish to estimate $\min_j |\mathcal{B}_j|$. It can be shown that [19]

$$\sum_{j=0}^{l-1} |\mathcal{B}_j| = \binom{n}{r} + l\binom{n-\lfloor \frac{n}{l} \rfloor}{r}.$$

Therefore

$$\min_j |\mathcal{B}_j| \le \frac{1}{l}\sum_{j=0}^{l-1} |\mathcal{B}_j| = \frac{1}{l}\binom{n}{r} + \binom{n-\lfloor \frac{n}{l} \rfloor}{r}.$$

Thus, we have the following theorems.

Theorem 34: For all positive integers $l \le n/(r+1)$,

$$\Gamma(n,r) \le \frac{1}{l}\binom{n}{r} + \binom{n-\lfloor \frac{n}{l} \rfloor}{r}. \quad \square$$

Theorem 35: Let $\mathcal{C}$ be an MDS code with length n and minimum distance $d > 1$. Then for all positive integers $l \le (1-R)^{-1}$, where $R = (n-d+1)/n$ is the code rate of $\mathcal{C}$,

$$\rho(\mathcal{C}) \le \frac{1}{l}\binom{n}{d-2} + \binom{n-\lfloor \frac{n}{l} \rfloor}{d-2}. \quad \square$$

The requirement that l be no greater than $(1-R)^{-1}$ turns out to be too restrictive for most cases and makes the upper bound less useful when R is not close to 1. To mitigate the problem, we can get rid of this requirement by adding some more blocks to $\mathcal{B}_j$. For clarity, we first assume $l \mid n$.

Construction 3: Arrange elements of $[n]$ into an $(n/l) \times l$ matrix (in an arbitrary way). The columns of this matrix partition $[n]$ into l disjoint sets with equal size which we denote by $N_0,\ldots,N_{l-1}$. With $N_0,\ldots,N_{l-1}$, let $\mathcal{B}_j$ be defined the same way as described in Construction 2. Now, the rows of this matrix also partition $[n]$. We denote them by $M_0,\ldots,M_{\frac{n}{l}-1}$. For all $X \subseteq [n]$, define

$$w'(X) := \sum_{i=0}^{\frac{n}{l}-1} i|X \cap M_i|.$$

For $t = 0,\ldots,n/l-1$, let

$$\mathcal{M}_t := \left\{B \in [n]^r : w'(B) \equiv t \mod \frac{n}{l}\right\}.$$

Finally, for all j, t, let

$$\mathcal{B}_{j,t} := \mathcal{B}_j \cup \mathcal{M}_t. \quad \square$$

We show that $\mathcal{B}_{j,t}$ as defined in Construction 3 is a single-exclusion (n,r)-system for all l.

Lemma 36: Let $l \ge 2$ be an integer. Let $L = \{0,1,\ldots,l-1\}$. For all $X \subseteq L$, define

$$\|X\| := \sum_{i\in X} i.$$

Then, for all k, $k = 1,\ldots,l-1$,

$$\{\|\kappa\| \mod l : \kappa \in [L]^k\} = L. \quad \square$$

Proof: First, it is easy to see that the claim is true for $k = 1$ and 2. The case $k = 1$ is quite trivial. For $k = 2$, it suffices to note that $i = \|\{0,i\}\|$ for $i = 1,\ldots,l-1$ and $l = \|\{1,l-1\}\|$.

In general, if the claim is true for $k = m$, then it is also true for $k = l-m$, since

$$\{\|\kappa\| \mod l : \kappa \in [L]^{l-m}\} = \{\|L\| - \|\kappa\| \mod l : \kappa \in [L]^m\}. \quad (16)$$

So, the claim is also true for $k = l-1$ and $k = l-2$.

Now, for the general case, let us assume $k \le l-3$. The idea is to consider pairs of elements in L that sum to 0 modulo l. First, suppose l is even. Then L can be partitioned in the following way:

$$L = \{0\} \cup \{l/2\} \cup \bigcup_{i=1}^{l/2-1} \{i, l-i\} = \{0\} \cup \{l/2\} \cup \bigcup_{i=1}^{l/2-1} Z_i$$

where $Z_i := \{i, l-i\}$, $i = 1,\ldots,l/2-1$. We show that for all $j \in L$, we can find a k-set β such that $\|\beta\| \equiv j \mod l$. If k is even, then we get the following.

- If $j \in Z_m$ for some m, let β be the union of $\{0,j\}$ and $(k/2-1)$ Z_i 's other than Z_m.
- If $j = l/2$, let β be the union of $\{0,j\}$ and $(k/2-1)$ Z_i 's.

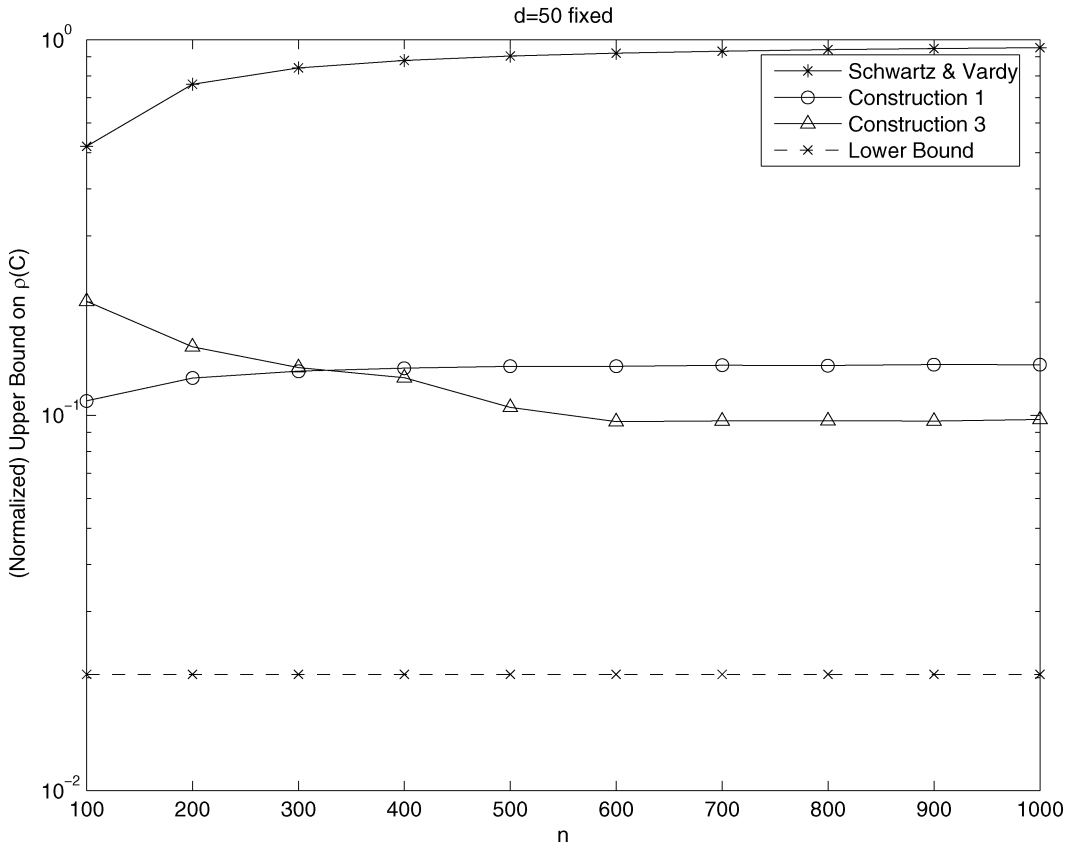

Fig. 1. Bounds on $\rho(\mathcal{C})$ for (n,k,d) MDS codes. $d=50$ is fixed. Bounds are normalized relative to $\binom{n}{d-2}$.

- If $j=0$, let β be the union of $k/2$ Z_i 's.

Similarly, if k is odd, then we get the following.

- If $j \in Z_m$ for some m, let β be the union of $\{j\}$ and $(k-1)/2$ Z_i 's other than Z_m.
- If $j=l/2$, let β be the union of $\{j\}$ and $(k-1)/2$ Z_i 's.
- If $j=0$, let β be the union of $\{0\}$ and $(k-1)/2$ Z_i 's.

For odd l, the proof is very similar and we will not elaborate here. ■

Theorem 37: For all l, j, and t, $\mathcal{B}_{j,t}$ as defined in Construction 3 is a single-exclusion (n,r)-system. □

Proof: Let X be an i-set, $i=1,\ldots,r$, and $x \in X$ be an arbitrary element. First, suppose that for all k, $N_k \nsubseteq X$. If $r \leq n-l$, then we can find an r-set $Z \supseteq X$ such that $N_k \nsubseteq Z$ for all k. Now, choose $y_k \in N_k \setminus Z$ for all k and consider r-sets of the form $Y_k := (Z \setminus \{x\}) \cup \{y_k\}$. For all j, we can choose k such that $w(Y_k)+j \equiv 0 \mod l$, and hence, $Y_k \in \mathcal{B}_j$. Clearly, $|X \setminus Y_k| = 1$. On the other hand, if $r > n-l$, then we can find an $(n-l)$-set $Z \supseteq X$ such that $N_k \nsubseteq Z$ for all k. Clearly, $[n] \setminus Z$ intersects each N_k at exactly one element. Consider r-sets that consist of the union of $Z \setminus \{x\}$ and an $(r-n+l+1)$-subset of $[n] \setminus Z$. By Lemma 36, for all j, there exists $W \in [[n] \setminus Z]^{r-n+l+1}$ such that if $Y = (Z \setminus \{x\}) \cup W$ then $w(Y)+j \equiv 0 \mod l$. Therefore, $Y \in \mathcal{B}_j$ and clearly $|X \setminus Y| = 1$.

Otherwise, suppose $N_k \subseteq X$. By construction, N_k contains elements from each M_m. Let $Z \supseteq X$ be an $(r+1)$-set; then, by choosing $Y \in \mathcal{Y} := \{Z \setminus \{x\} : x \in X\}$, we can realize any value of $w'(Y)$. Hence, for any t, there exists an r-set $Y \in \mathcal{M}_t$ such that $|X \setminus Y| = 1$. ■

If $l \nmid n$, we can define $M_0,\ldots,M_{\lfloor \frac{n}{l} \rfloor - 1}$ by applying Construction 3 to the first $\lfloor n/l \rfloor l$ elements of $[n]$ and letting $M_{\lfloor \frac{n}{l} \rfloor - 1}$ include the extra $(n \mod l)$ elements. All reasoning is still valid.

Clearly

$$\sum_{t=0}^{\lfloor \frac{n}{l} \rfloor - 1} |\mathcal{M}_t| = \binom{n}{r}.$$

Hence

$$\min_t |\mathcal{M}_t| \leq \frac{1}{\lfloor n/l \rfloor}\binom{n}{r}.$$

By the union bound, $|\mathcal{B}_{j,t}| \leq |\mathcal{B}_j| + |\mathcal{M}_t|$, hence, we arrive at the following bounds.

Theorem 38: For all integers l, $1 \leq l \leq n$,

$$\Gamma(n,r) \leq \begin{cases} \binom{n-\lfloor n/l \rfloor}{r} + \frac{1}{l}\binom{n}{r}, & \text{if } l \leq \frac{n}{r+1} \\ \binom{n-\lfloor n/l \rfloor}{r} + \left(\frac{1}{l} + \frac{1}{\lfloor n/l \rfloor}\right)\binom{n}{r}, & \text{if } l > \frac{n}{r+1}. \end{cases}$$ □

Theorem 39: Let $\mathcal{C}$ be an MDS code with length n and minimum distance $d > 1$. Then for all integers l, $1 \leq l \leq n$,

$$\rho(\mathcal{C}) \leq \begin{cases} \binom{n-\lfloor n/l \rfloor}{d-2} + \frac{1}{l}\binom{n}{d-2}, & \text{if } l \leq (1-R)^{-1} \\ \binom{n-\lfloor n/l \rfloor}{d-2} + \left(\frac{1}{l} + \frac{1}{\lfloor n/l \rfloor}\right)\binom{n}{d-2}, & \text{if } l > (1-R)^{-1} \end{cases}$$

where $R = (n-d+1)/n$ is the code rate of $\mathcal{C}$. □

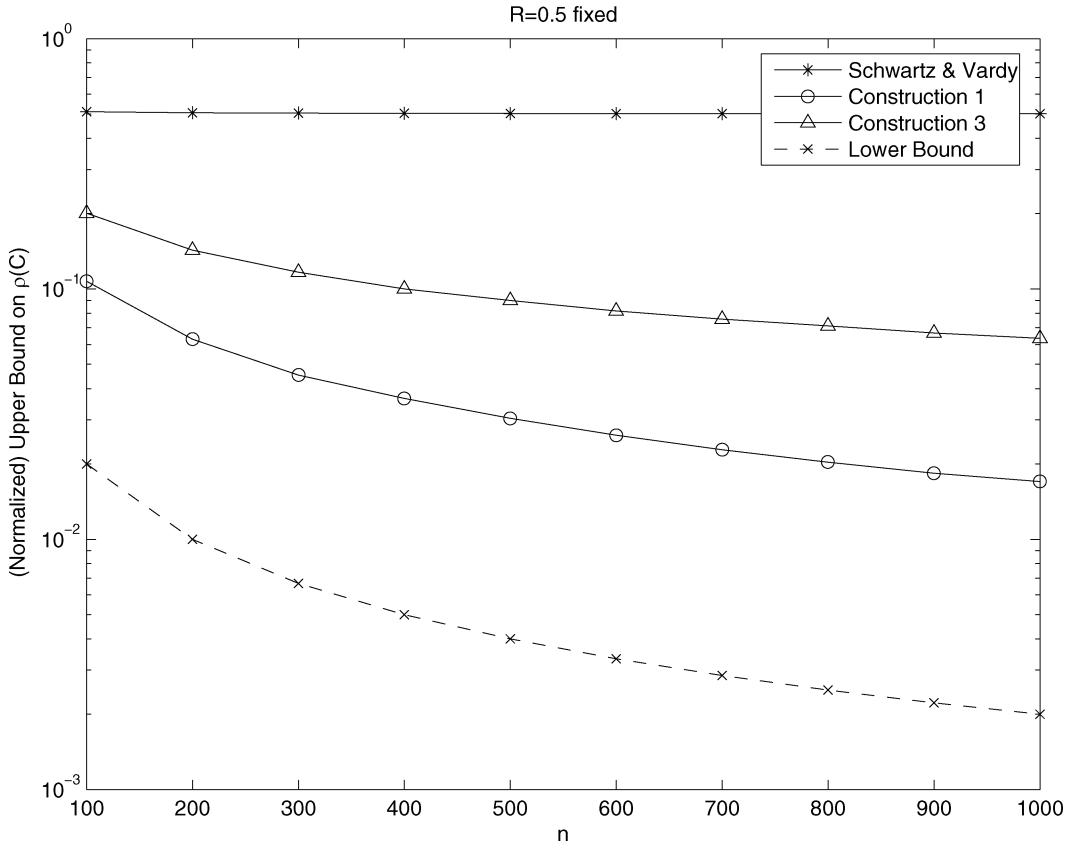

Fig. 2. Bounds on $\rho(\mathcal{C})$ for (n, k, d) MDS codes. $R = 0.5$ is fixed. Bounds are normalized relative to $\binom{n}{d-2}$.

Note that when we choose l in the region $l > (1-R)^{-1}$, the upper bound is never better than $\frac{2}{\sqrt{n}}\binom{n}{d-2}$. So the strength of the bound above still lies in the regime of high rate codes.

Figs. 1 –3 compare the upper bounds we have obtained so far, i.e., those of Theorems 27 and 39 (minimized over l), to the previously known bounds as given in (11). In the plots, all bounds are normalized with respect to $\binom{n}{d-2}$. We see that the new upper bounds are both tighter than (11) in a variety of situations, with the one based on Construction 1 outperforming the one based on Construction 3 for all but very high code rate scenarios.

IV. Conclusion

We have obtained new upper bounds on the stopping redundancy of linear codes. Compared to the bounds from [3] and [10], our bound based on probabilistic methods gives better results for a number of interesting cases, including for all "good" codes, i.e., those whose minimum distance is asymptotically nontrivial relative to code length.

Though tighter, the new upper bounds for the case of "good" codes are still exponential in the length of the code. It remains an open question whether there exist "good" codes whose stopping redundancy is polynomial in the code length.

Improving the lower bound on stopping redundancy seems to be difficult. Applying the probabilistic method only yields the same bound as given in [3].

For MDS codes, the interesting relationship between stopping redundancy and Turán numbers has been explored. We have defined a new combinatorial quantity, the single-exclusion number $\Gamma(v, r)$, and related it to the Turán number and the stopping redundancy of MDS codes. By studying $\Gamma(v, r)$, we have obtained new upper bounds on the stopping redundancy of MDS codes, which have been shown to be tighter than the best previously known bounds for various situations. We have also proved that for MDS codes with length n and minimum distance d, $\rho(\mathcal{C})$ is asymptotic to $T(n, d-1, d-2)$ for fixed d, and is asymptotic to $T(n, d-1, d-2)$ up to a constant factor of at most 3 for fixed $k = n - d + 1$. We conjecture that in the latter case the constant factor can be improved to 2. We also conjecture that $\rho(\mathcal{C}) = \Gamma(n, d-2)$ for all MDS codes. For one thing, the two are asymptotic to each other if d is fixed. Further, for $d = 3, 4$, both $\rho(\mathcal{C})$ and $\Gamma(n, d-2)$ are equal to $T(n, d-1, d-2)$. For $d = 5$, we have shown that neither can differ from $T(n, d-1, d-2)$ by more than 1.

Appendix I
The Binary Golay Code

We present here a parity-check matrix with 34 rows that achieves maximum stopping distance and corrects more low-weight erasure patterns than the parity-check matrix given in [8]. The details of our parity-check matrix, denoted by H, are given in Table II. It was found by a greedy computer search. The idea is to start with a random selection of codewords from $\mathcal{G}_{24}$ (note that $\mathcal{G}_{24}$ is self-dual), and in each iteration, replace one codeword in the selection so that as many more i-sets ($1 \leq i \leq 7$) as possible are covered. When no such improvements can be made, an additional codeword is added to the selection and the iteration continues. The process is stopped

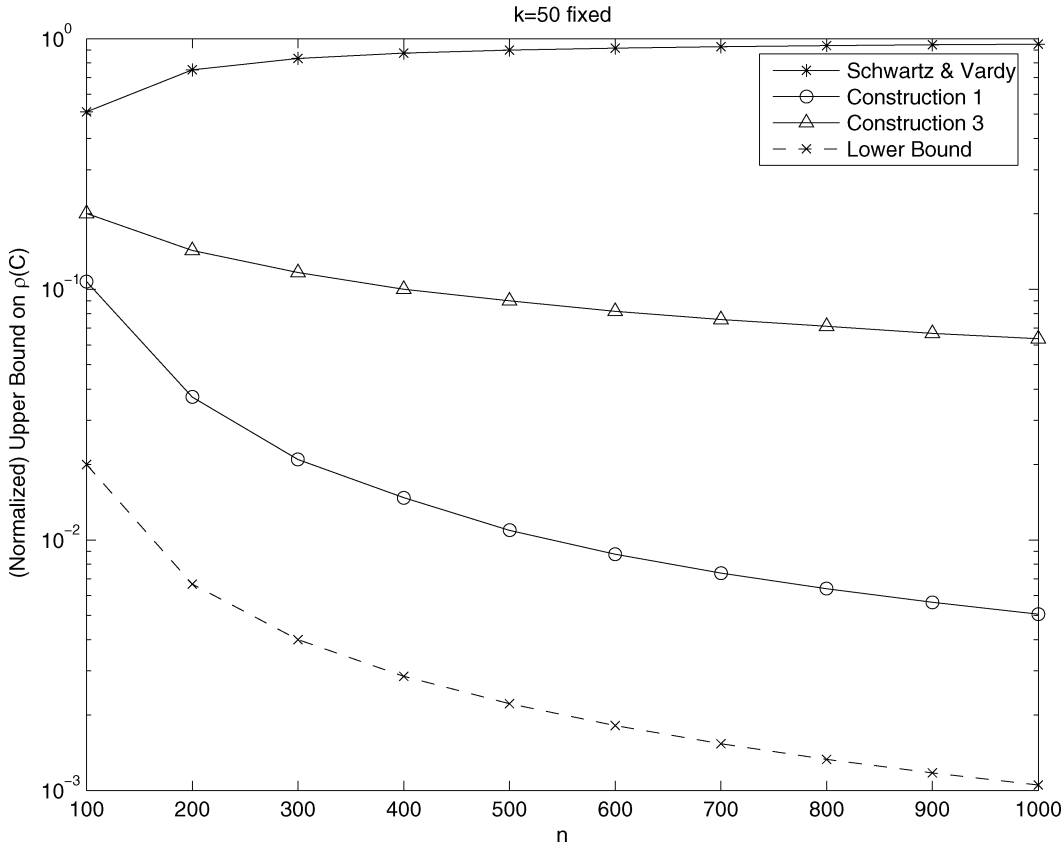

Fig. 3. Bounds on $\rho(\mathcal{C})$ for (n, k, d) MDS codes. $k = 50$ is fixed. Bounds are normalized relative to $\binom{n}{d-2}$.

TABLE II
PARITY-CHECK MATRIX WITH 34 ROWS FOR $\mathcal{G}_{24}$ THAT ACHIEVES STOPPING DISTANCE 8

$$H = \begin{pmatrix}
0\,0\,0\,0\,0\,0\,0\,1\,1\,0\,1\,1\,0\,1\,0\,0\,0\,0\,0\,1\,1\,1\,0\,0\,0\\
0\,0\,0\,0\,0\,0\,1\,0\,0\,1\,0\,0\,0\,1\,1\,1\,1\,0\,1\,0\,0\,0\,0\,1\\
0\,0\,0\,0\,0\,0\,1\,1\,1\,0\,1\,0\,0\,0\,0\,1\,0\,1\,0\,0\,1\,0\,1\,0\\
1\,0\,0\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,1\,0\,0\,0\,0\,1\,1\,0\\
0\,0\,0\,0\,0\,1\,0\,0\,1\,1\,1\,0\,1\,1\,0\,0\,0\,0\,1\,0\,0\,0\,0\,1\\
0\,0\,0\,0\,0\,1\,1\,0\,0\,0\,0\,0\,0\,1\,1\,1\,0\,0\,0\,1\,0\,0\,1\,1\,0\\
0\,0\,0\,0\,0\,1\,1\,1\,0\,0\,1\,0\,0\,1\,1\,0\,0\,0\,0\,0\,1\,0\,0\,1\\
1\,0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,1\,1\,0\,1\,1\,1\,0\,0\\
1\,0\,0\,0\,1\,0\,0\,1\,0\,1\,1\,1\,1\,1\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\\
0\,0\,0\,0\,1\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,1\,1\,0\,1\,0\,1\,1\\
1\,0\,0\,0\,1\,1\,1\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,0\,0\,0\,0\,0\,1\,0\,1\\
0\,0\,0\,1\,0\,0\,0\,1\,0\,0\,1\,1\,1\,1\,0\,0\,0\,0\,1\,0\,1\,0\,0\,1\,0\\
1\,0\,0\,1\,0\,0\,1\,0\,0\,0\,0\,1\,0\,0\,0\,0\,1\,1\,0\,0\,1\,0\,1\,0\\
0\,0\,0\,1\,0\,1\,0\,1\,0\,0\,0\,1\,0\,1\,0\,1\,0\,1\,0\,0\,1\,0\,0\,0\\
1\,0\,0\,1\,1\,0\,0\,1\,1\,1\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,1\,0\,0\\
0\,0\,1\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,1\,0\,1\,0\,1\,0\,1\,1\,1\,0\,0\\
0\,0\,1\,0\,0\,0\,1\,1\,1\,0\,1\,1\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\\
0\,0\,1\,0\,0\,1\,1\,0\,0\,1\,0\,0\,1\,0\,1\,0\,0\,1\,0\,0\,0\,0\,0\,1\\
0\,0\,1\,0\,1\,1\,0\,0\,0\,0\,0\,1\,0\,1\,0\,1\,0\,0\,0\,0\,0\,1\,1\,0\\
0\,0\,1\,1\,0\,0\,0\,0\,1\,0\,1\,0\,1\,1\,0\,0\,1\,0\,0\,1\,0\,0\,0\,0\\
0\,0\,1\,1\,1\,0\,0\,0\,0\,0\,1\,0\,1\,0\,0\,0\,0\,1\,1\,0\,0\,0\,0\,1\\
0\,1\,0\,0\,0\,0\,0\,0\,1\,1\,0\,1\,0\,0\,1\,0\,0\,0\,0\,1\,1\,1\,0\,0\\
1\,1\,0\,0\,0\,0\,1\,0\,0\,1\,0\,0\,0\,0\,0\,1\,0\,1\,0\,0\,0\,0\,1\,1\\
0\,1\,0\,0\,0\,1\,0\,0\,0\,1\,1\,0\,0\,0\,1\,1\,0\,0\,0\,1\,0\,0\,0\,1\\
0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,0\,1\,0\,1\,0\,1\,1\,0\,1\,0\,0\,0\,0\,0\\
0\,1\,0\,0\,1\,1\,0\,0\,0\,0\,0\,1\,0\,0\,0\,1\,0\,0\,1\,0\,1\,0\,1\,1\\
1\,1\,0\,1\,0\,0\,1\,1\,0\,1\,0\,0\,0\,0\,0\,0\,1\,0\,1\,0\,0\,0\,0\,0\\
0\,1\,0\,1\,0\,1\,0\,1\,0\,0\,0\,0\,1\,0\,0\,1\,1\,0\,0\,1\,0\,0\,0\,0\\
0\,1\,0\,1\,1\,0\,0\,1\,0\,0\,0\,0\,1\,0\,1\,0\,0\,0\,1\,0\,0\,0\,1\,0\\
1\,1\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,1\,0\,1\,0\,1\,1\,0\\
1\,1\,1\,0\,0\,0\,1\,0\,1\,0\,1\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,1\,0\\
1\,1\,1\,0\,1\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,1\,1\,0\,1\,1\,0\,0\,0\,0\\
1\,1\,1\,1\,0\,0\,0\,0\,1\,1\,0\,0\,0\,0\,0\,1\,0\,0\,0\,1\,0\,0\,0\,0\,0\\
0\,1\,1\,1\,1\,0\,0\,0\,0\,0\,0\,0\,1\,1\,0\,1\,0\,0\,0\,0\,1\,0\,0\,0
\end{pmatrix}$$

TABLE III
NUMBER OF UNDECODABLE ERASURE PATTERNS BY WEIGHT w FOR DIFFERENT ITERATIVE DECODERS FOR $\mathcal{G}_{24}$

w	$\Psi_H(w)$	$\Psi_{H'_{24}}(w)$	$\Psi_{\mathrm{ML}}(w)$
≤ 7	0	0	0
8	3284	3598	759
9	78218	82138	12144
10	580166	585157	91080
11	1734967	1717082	425040
12	2569618	2556402	1313116
≥ 13	$\binom{24}{w}$	$\binom{24}{w}$	$\binom{24}{w}$

when the desired stopping distance is achieved. We find that it is enough to only consider covering 7-sets, and verify in the end that the matrix obtained indeed covers all smaller i-sets and has the proper rank.

Table III compares the number of undecodable erasure patterns by weight w (number of erased bits) for iterative decoders based on H, H'_{24} (the 34-row parity-check matrix reported in [8]), and the ML decoder. We see that the iterative decoder based on H corrects considerably more lower weight erasure patterns than does the one based on H'_{24}, which implies that it will perform better when the erasure probability is small. For a binary erasure channel with erasure probability p, a detailed comparsion shows that for all $p < 0.349$, the iterative decoder based on H has a smaller probability of decoding failure.

APPENDIX II
DERIVATIONS IN THE ASYMPTOTIC COMPARISON OF BOUNDS

Binary Linear Codes (Example 2, Case 1): Noting that $-\log(1-x) \sim x/\ln 2$ as $x \to 0$, we see the upper bound in (9) is $O(2^{\delta n})$, hence so is the bound in Theorem 4. On the other hand, note that

$$\sum_{i=1}^{d(\mathcal{C})-1} \binom{n}{i} \left(1-\frac{i}{2^i}\right)^{\rho} \geq \binom{n}{d(\mathcal{C})-1} \left(1-\frac{d(\mathcal{C})-1}{2^{d(\mathcal{C})-1}}\right)^{\rho}.$$

Setting

$$\binom{n}{d(\mathcal{C})-1} \left(1-\frac{d(\mathcal{C})-1}{2^{d(\mathcal{C})-1}}\right)^{\rho} = 1,$$

and solving for ρ, one can readily show that $\rho^*(n, d(\mathcal{C}))$ is also $\Omega(2^{\delta n})$. Therefore, the bound given by Theorem 4 is indeed $\Theta(2^{\delta n})$.

In comparison, consider the bound in Theorem 1. For $0 < \delta < 1/2$, the asymptotic Plotkin bound implies that $\delta/\gamma \leq 1/2$. Noting that $h(p) \geq 2p$ for $p \leq 1/2$, we have

$$\begin{aligned}
\sum_{i=1}^{d(\mathcal{C})-2} \binom{r(\mathcal{C})}{i} &= \Omega\left(\binom{r(\mathcal{C})}{d(\mathcal{C})-2}\right) \\
&= \Omega\left(\binom{\gamma n}{\delta n - 2}\right) \\
&= \Omega\left(\binom{\gamma n}{\delta n}\right) \\
&= \Omega\left(\frac{1}{\sqrt{n}} 2^{\gamma h(\frac{\delta}{\gamma}) n}\right) \\
&= \Omega\left(\frac{2^{2\delta n}}{\sqrt{n}}\right).
\end{aligned}$$

The analysis for the bounds of Theorems 2 and 3 is similar, and one can show that the same asymptotic result applies.

Linear Codes Over $\mathbb{F}_q$ (Example 4): Showing that the bound in Theorem 8 is $\Theta(q^{\delta n})$ is very similar to the binary case, and we will not elaborate here.

Now, consider the bound of Theorem 7. Let $\theta = (q-1)/q$. For $0 < \delta < \theta$, we see that $0 < \delta/\gamma \leq \theta$ by the asymptotic Plotkin bound. Noting that $h(p) \geq (h(\theta)/\theta)p$ for all $0 < p \leq \theta$, $0 < \theta < 1$, we have

$$\begin{aligned}
&\sum_{i=1}^{d(\mathcal{C})-1} \binom{r(\mathcal{C})}{i} (q-1)^{i-1} \\
&\quad = \Omega\left(\binom{r(\mathcal{C})}{d(\mathcal{C})-1} (q-1)^{d(\mathcal{C})-2}\right) \\
&\quad = \Omega\left(\frac{1}{\sqrt{n}} 2^{\gamma h(\frac{\delta}{\gamma}) n} (q-1)^{\delta n}\right) \\
&\quad = \Omega\left(\frac{1}{\sqrt{n}} 2^{\gamma \frac{h(\theta)}{\theta} \frac{\delta}{\gamma} n} (q-1)^{\delta n}\right) \\
&\quad = \Omega\left(\frac{1}{\sqrt{n}} \left(\frac{1}{\theta}\right)^{\delta n} \left(\frac{1}{1-\theta}\right)^{\frac{1-\theta}{\theta}\delta n} (q-1)^{\delta n}\right) \\
&\quad = \Omega\left(\frac{1}{\sqrt{n}} q^{\frac{q}{q-1}\delta n}\right).
\end{aligned}$$

ACKNOWLEDGMENT

The authors would like to thank Moshe Schwartz for helpful discussions.

REFERENCES

[1] C. Di, D. Proletti, I. Telatar, T. Richardson, and R. Urbanke, "Finite length analysis of low-density parity-check codes," *IEEE Trans. Inf. Theory*, vol. 48, no. 6, pp. 1570–1579, Jun. 2002.

[2] R. M. Tanner, "A recursive approach to low complexity codes," *IEEE Trans. Inf. Theory*, vol. IT-27, no. 5, pp. 533–547, Sep. 1981.

[3] M. Schwartz and A. Vardy, "On the stopping distance and the stopping redundancy of codes," *IEEE Trans. Inf. Theory*, vol. 52, no. 3, pp. 922–932, Mar. 2006.

[4] A. Orlitsky, R. Urbanke, K. Viswanathan, and J. Zhang, "Stopping sets and the girth of Tanner graphs," in *Proc. IEEE Int. Symp. Information Theory*, Lausanne, Switzerland, Jun./Jul. 2002, p. 2.

[5] N. Kashyap and A. Vardy, "Stopping sets in codes from designs," in *Proc. IEEE Int. Symp. Information Theory* , Yokohama, Japan, Jun./Jul. 2003, p. 122.

[6] A. Orlitsky, K. Viswanathan, and J. Zhang, "Stopping set distribution of LDPC code ensembles," *IEEE Trans. Inf. Theory*, vol. 51, no. 3, pp. 929–953, Mar. 2005.

[7] J. H. Weber and K. A. Abdel-Ghaffar, "Stopping set analysis for Hamming codes," in *Proc. IEEE ISOC Information Theory Workshop on Coding and Complexity*, Rotorua, New Zealand, Aug./Sep. 2005, pp. 244–247.

[8] M. Schwartz and A. Vardy, "On the stopping distance and stopping redundancy of codes," in *Proc. IEEE Int. Symp. Information Theory*, Adelaide, Australia, Sep. 2005, pp. 975–979.

[9] T. Etzion, "On the stopping redundancy of Reed-Muller codes," 2005, preprint.

[10] H. D. L. Hollmann and L. M. G. M. Tolhuizen, "On parity check collections for iterative erasure decoding that correct all correctable erasure patterns of a give size," *IEEE Trans. Inf. Theory*, submitted for publication.

[11] ——, "Generating parity check equations for bounded-distance iterative erasure decoding," in *Proc. IEEE Int. Symp. Information Theory*, Seattle, WA, Jul. 2006, pp. 514–517.

[12] N. Alon and J. H. Spencer, *The Probabilistic Method*. New York: Wiley, 1991.

[13] H. D. L. Hollmann and L. M. G. M. Tolhuizen, "Generating parity check equations for bounded-distance iterative erasure decoding of even weight codes," in *Proc. 27th Symp. Information Theory in the Benelux*, Noordwijk, The Netherlands, Jun. 2006, pp. 17–24.

[14] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1978.

[15] H. D. L. Hollmann and L. M. G. M. Tolhuizen, "Generic erasure correcting sets: Bounds and constructions," *J. Combin. Theory Ser. A*, vol. 113, no. 8, pp. 1746–1759, Nov. 2006.

[16] R. G. Gallager, *Low-Density Parity-Check Codes*. Cambridge, MA: MIT Press, 1963.

[17] R. L. Graham, D. E. Knuth, and O. Patashnik, *Concrete Mathematics*, 2nd ed. Reading, MA: Addison-Wesley, 1994.

[18] A. S. Hedayat, N. J. A. Sloane, and J. Stufken, *Orthogonal Arrays*. New York: Springer-Verlag, 1999.

[19] A. Sidorenko, "Upper bounds for Turán numbers," *J. Combin. Theory Ser. A*, vol. 77, pp. 134–147, 1997.

[20] W. H. Mills and R. C. Mullin, "Coverings and packings," in *Contemporary Design Theory*, J. H. Dinitz and D. R. Stinson, Eds. New York: Wiley, 1992, ch. 9, pp. 371–399.

[21] W. Mantel, "Vraagstuk XXVIII," *Wiskundige Opgaven met de Oplossingen*, vol. 10, pp. 60–61, 1907.

[22] P. Turán, "Egy gráfelméleti szélsőértékfeladatról," (in Hungarian) *Mat. Fiz. Lapok*, vol. 48, pp. 436–452, 1941.

[23] ——, "An extremal problem in graph theory," in *Collected Papers of Paul Turán,* P. Erdős, Ed. Budapest, Hungary: Akadémiai Kiadó, 1990, pp. 231–256.

[24] G. Ringel, "Extremal problems in the theory of graphs," in *Theory of Graphs and Their Applications*, M. Fiedler, Ed. Prague: Czechoslovak Acad. Sci., 1964.

[25] G. Katona, T. Nemetz, and M. Simonovits, "On a graph problem of Turán," (in Hungarian) *Mat. Lapok*, vol. 15, pp. 228–238, 1964.

[26] F. Chung and R. Graham, *Erdős on Graphs—His Legacy of Unsolved Problems*. Wellesley, MA: A K Peters, 1998.

[27] F. Chung and L. Lu, "An upper bound for the Turán number $t_3(n,4)$," *J. Combin. Theory Ser. A*, vol. 87, pp. 381–389, 1999.
[28] D. de Caen, D. L. Kreher, and J. Wiseman, "On constructive upper bounds for the Turán numbers $T(n,2r+1,2r)$," *Congr. Numer.*, vol. 65, pp. 277–280, 1988.
[29] A. F. Sidorenko, "Systems of sets that have the T-property," *Moscow Univ. Math. Bull.*, vol. 36, no. 5, pp. 22–26, 1981.
[30] ——, "The method of quadratic forms and Turán's combinatorial problem," *Moscow Univ. Math. Bull.*, vol. 37, no. 1, pp. 1–5, 1982.
[31] D. Applegate, E. M. Rains, and N. J. A. Sloane, "On asymmetric coverings and covering numbers," *J. Combin. Des.*, vol. 11, pp. 218–228, 2003.
[32] K. H. Kim and F. W. Roush, "On a problem of Turán," in *Studies in Pure Mathematics: To the Memory of Paul Turán*, P. Erdős, Ed. Basel, Switzerland: Birkhäuser, 1983, pp. 423–425.
[33] V. Rödl, "On a packing and covering problem," *Europ. J. Combin.*, vol. 5, pp. 69–78, 1985.
[34] P. Erdős and H. Hanani, "On a limit theorem in combinatorial analysis," *Publ. Math. Debrecen*, vol. 10, pp. 10–13, 1963.
[35] P. Frankl and V. Rödl, "Lower bounds for Turán's problem," *Graphs Combin.*, vol. 1, pp. 213–216, 1985.