# On the Stopping Redundancy of MDS Codes

Junsheng Han
Department of Electrical and Computer Eng.
University of California, San Diego
La Jolla, CA 92093-0409, USA
Email: han@cts.ucsd.edu

Paul H. Siegel
Department of Electrical and Computer Eng.
University of California, San Diego
La Jolla, CA 92093-0407, USA
Email: psiegel@ucsd.edu

***Abstract*— The *stopping redundancy* of a linear code is defined as the minimum number of rows in its parity-check matrix such that the smallest stopping sets have size equal to the minimum distance of the code. We derive new upper bounds on the stopping redundancy of maximum distance separable (MDS) codes, and show how they improve upon previously known results. 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 $d=2,3,4$, we prove that the stopping redundancy is equal to $T(n,d-1,d-2)$. For $d=5$, we show that the stopping redundancy is either $T(n,4,3)$ or $T(n,4,3)+1$.**

## I. Introduction

In a Tanner graph, a *stopping set* [1] 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. Given a parity-check matrix $H$, let the size of the smallest nonempty stopping set be termed the *stopping distance* [2] of the code with respect to $H$, denoted by $s(H)$. 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. Let $\mathcal{C}$ be a linear code with minimum distance $d$. Since the support of any codeword is a stopping set, $s(H)\le d$ for all choices of $H$. It is known [2], [3] that by proper choice of $H$, $s(H)=d$ 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 $s(H)=d$.

Stopping redundancy was introduced by Schwartz and Vardy [2], [4], 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 [5]. Weber and Abdel-Ghaffar [3] studied the number of redundant parity checks required to minimize the number of size-three stopping sets for binary Hamming codes. Hollmann and Tolhuizen considered a similar concept, termed *generic $(r,m)$-correcting sets* [6].

In this paper, we study the stopping redundancy of MDS codes. In [2], Schwartz and Vardy pointed out a link between the stopping redundancy of MDS codes and covering numbers. This led to a number of lower bounds on $\rho(\mathcal{C})$. We show that the stopping redundancy of MDS codes is upper bounded by another combinatorial quantity, which we shall define as the *single-exclusion number*. Further results, both asymptotic and for codes with specific (small) minimum distance, reveal a strong connection between the stopping redundancy of MDS codes and Turán numbers – combinatorial quantities closely related to covering numbers to be defined later. We also obtain new upper bounds on the stopping redundancy through combinatorial constructions of *single-exclusion systems*, and compare them to the upper bounds of [2].

In the discussion that follows, most of the proofs are omitted due to limited space. The interested reader is referred to [7] for details.

## II. Stopping Redundancy of MDS codes

First, a few notes 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 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 [8], 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 [9].

The authors of [2] noted the following.[1]

**Theorem 1** *Let $\mathcal{C}$ be an 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 $\iota$ is any $(d-1)$-set, then since $\iota$ is not a stopping set, there exists a row of $H$ with $d-2$ zeros whose positions are contained in $\iota$. 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. [2]). Better bounds can be obtained by utilizing a stronger lower bound on $T(v,k,t)$.

Now, let us make the following definition and see how it leads to an upper bound on the stopping redundancy of MDS codes.

**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 $\iota$ is *covered* by block $\beta$ if

$$|\iota \setminus \beta| = 1.$$

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* It is easy to see that $[v]^r$ is a single-exclusion $(v,r)$-system, so $\Gamma(v,r)$ is well-defined. □

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 a parity-check matrix. In summary, for every $l$-block single-exclusion $(n, d-2)$-system, there exists an $l$-row parity-check matrix for $\mathcal{C}$ that achieves maximum stopping distance. Hence, we have the following result.

**Theorem 2** *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 3** *If $\mathcal{C}$ is an MDS code with length $n$ and minimum distance $d > 1$, then*

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

We now have bounded $\rho(\mathcal{C})$ between two well-defined combinatorial quantities, $T(n, d-1, d-2)$ and $\Gamma(n, d-2)$. To upper bound $\rho(\mathcal{C})$, it suffices to upper bound $\Gamma(n, d-2)$. We will actually proceed in this way – in the rest of the paper, 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 $d \leq 5$. If $d = 2$, then $\rho(\mathcal{C}) = T(n, 1, 0) = \Gamma(n, 0) = 1$. The results for $d = 3, 4, 5$ are summarized in Theorems 4, 5, 6, and Corollary 7. Note that the case for $d = 3$ is quite trivial, and the result is actually implied by the best upper and lower bounds on $\rho(\mathcal{C})$ given in [2].

**Theorem 4** *Let $\mathcal{C}$ be an MDS code with length $n$ and minimum distance $d = 3$. Then*

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

**Theorem 5** *Let $\mathcal{C}$ be an MDS code with length $n \geq 6$ and minimum distance $d = 4$. Then*

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

**Theorem 6** *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,*

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

**Corollary 7** *Let $\mathcal{C}$ be an MDS code with length $n$ and minimum distance $d = 5$. Then*

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

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 8** *For fixed $d$, $d > 1$, as $n \to \infty$,*

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

*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.

[1] In [2], 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 [10].

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 $\iota$ 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 $\beta$. 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 Theorem 1, Theorem 2 and Theorem 8, the following result is immediate.

**Theorem 9** *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 [11] showed that $T(n,k,r)/\binom{n}{r}$ is non-decreasing in $n$ and hence there exists the limit

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

Theorem 8 and Theorem 9 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 $t(d-1, d-2)\binom{n}{d-2}$.

The value of $t(r+1, r)$, although unknown for $r > 2$, is well-studied. The best known upper bound is $t(r+1, r) \leq (1/2 + o(1)) \ln r / r$, due to Sidorenko ([8]). In contrast, the bounds for MDS codes given in [2] are

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

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 [12].

**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

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

□

**Theorem 10** *For all $j$, $\mathcal{B}_j$ as defined in Construction 1 is a single-exclusion $(n, r)$-system if $l \geq n/(n-r-1)$.* □

It is not hard to show that (cf. [12])

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

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

**Theorem 11** *For all integers $l \geq n/(n-r-1)$,*

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

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

**Theorem 12** *Let $\mathcal{C}$ be an MDS code with length $n$ and minimum distance $d > 1$. For all integers $l \geq R^{-1}$, where $R = (n-d+1)/n$ is the code rate of $\mathcal{C}$,*

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

Let's consider the upper bound of Theorem 11 and Theorem 12 as $n \to \infty$, and compare it to (1).

1) *$d$ is fixed:*
   By choosing $l = \lceil (d-2)/(2 \ln(d-2)) \rceil$ (assume $d > 3$), one can show that the upper bound of Theorem 12 is asymptotically better than $\frac{1 + 2\ln(d-2)}{d-2}\binom{n}{d-2}$, while the upper bound of (1) is asymptotic to $\binom{n}{d-2}$.
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 12 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 (1).
3) *$k = n - d + 1$, the dimension of $\mathcal{C}$, is fixed:*
   Theorem 12 requires that $l \geq n/k$. If $k \geq 4$, we can choose $l$ such that $l \in (\frac{n}{3} - 1, \frac{n}{3}]$. Then the bound of Theorem 12 becomes, asymptotically,

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

   The bound above is asymptotic to $\frac{3}{k+1}\binom{n}{k}$. For comparison, (1) 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 is interesting in its own right and it turns out that the upper bound holds for $k = 1, 2, 3$ as well.

We summarize it as follows. (Note that the discussion above applies to $\Gamma(n, d-2) = \Gamma(n, n-k-1)$ as well as $\rho(\mathcal{C})$.)

**Theorem 13** *For fixed $k$, as $n \to \infty$,*

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

**Theorem 14** *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 $i \to \infty$,*

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

*where $n = n_i$.* □

Previously, we have seen a close connection between $\Gamma(n, d-2)$ and $T(n, d-1, d-2)$ for fixed $d$. Theorem 13 and Theorem 14 lead to a similar result for fixed $k$.

**Theorem 15** *For fixed $k$, as $n \to \infty$,*

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

**Theorem 16** *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 $i \to \infty$,*

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

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

Next, consider the following construction of a Turán $(n, r+1, r)$-system, due to Frankl and Rödl [13].

**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 $S(X) := \{i : X \cap N_i \ne \emptyset\}$ 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

$$\begin{aligned}\mathcal{B}_j := \{&B \in [n]^r : (w(B) + j) \mod l \\ &\in \{0, 1, \ldots, l - s(B)\}\}. \qquad \square\end{aligned}$$

**Theorem 17** *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.* □

It can be shown that ([8])

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

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 18** *For all positive integers $l \le n/(r+1)$,*

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

**Theorem 19** *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 $\mathcal{C}$,*

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

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 a $\frac{n}{l} \times l$ 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 $t = 0, \ldots, \frac{n}{l} - 1$, let

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

Finally, for all $j$, $t$, let

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

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

**Theorem 20** *For all $l$, $j$, and $t$, $\mathcal{B}_{j,t}$ as defined in Construction 3 is a single-exclusion $(n, r)$-system.* □

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 in the proof remains valid.

Clearly,

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

Hence,

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

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

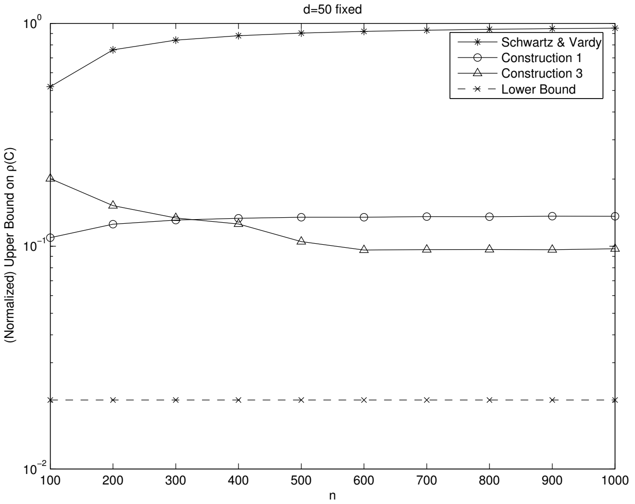

Fig. 1. Bounds on $\rho(\mathcal{C})$ for $(n, k, d)$ MDS codes. $d = 50$ is fixed. Bounds are normalized relative to $\binom{n}{d-2}$.

**Theorem 21** *For all integers $l$, $1 \leq l \leq n$,*

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

**Theorem 22** *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 $\mathcal{C}$.* □

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

In Fig. 1 through Fig. 3, the upper bounds of Theorem 12 and Theorem 22 (minimized over $l$) are compared to the previously known bounds of (1). All bounds are normalized with respect to $\binom{n}{d-2}$. We see that both proposed upper bounds are tighter than (1) 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.

## References

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

[2] M. Schwartz and A. Vardy, "On the stopping distance and the stopping redundancy of codes," *IEEE Trans. Inform. Theory*, submitted March 16, 2005. [Online]. Available: http://arxiv.org/abs/cs.IT/0503058

[3] 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./Sept. 2005, pp. 244–247.

[4] M. Schwartz and A. Vardy, "On the stopping distance and stopping redundancy of codes," in *Proc. IEEE International Symposium on Information Theory (ISIT'05)*, Adelaide, Australia, Sept. 2005, pp. 975–979.

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

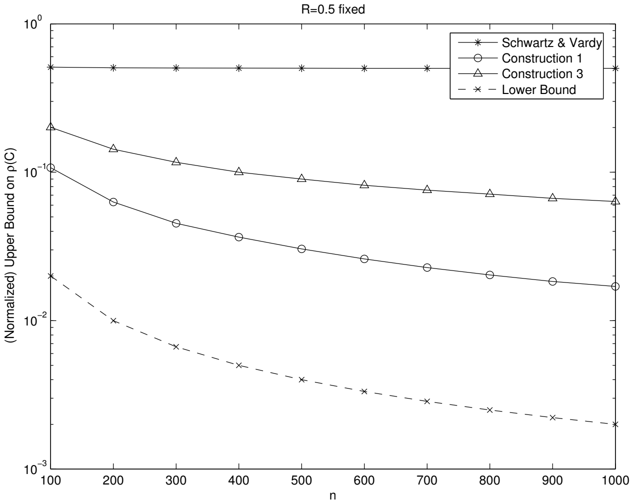

Fig. 2. Bounds on $\rho(\mathcal{C})$ for $(n, k, d)$ MDS codes. $R = 0.5$ is fixed. Bounds are normalized relative to $\binom{n}{d-2}$.

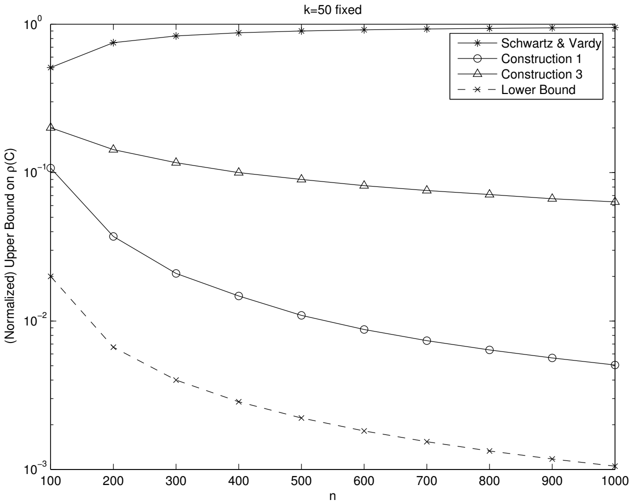

Fig. 3. Bounds on $\rho(\mathcal{C})$ for $(n, k, d)$ MDS codes. $k = 50$ is fixed. Bounds are normalized relative to $\binom{n}{d-2}$.

[6] H. D. Hollmannn and L. M. Tolhuizen, "On parity check collections for iterative erasure decoding that correct all correctable erasure patterns of a give size," *IEEE Trans. Inform. Theory*, submitted July 28, 2005. [Online]. Available: http://arxiv.org/abs/cs.IT/0507068

[7] J. Han and P. H. Siegel, "Improved upper bounds on stopping redundancy," *IEEE Trans. Inform. Theory*, submitted November 14, 2005. [Online]. Available: http://arxiv.org/abs/cs.IT/0511056

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

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

[10] 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.

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

[12] 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: Birkhäuser Verlag, 1983, pp. 423–425.

[13] P. Frankl and V. Rödl, "Lower bounds for Turán's problem," *Graphs Combin.*, vol. 1, pp. 213–216, 1985.