Bounds on Single-Exclusion Numbers and Stopping Redundancy of MDS Codes

Junsheng Han Paul H. Siegel
University of California, San Diego
La Jolla, CA 92093-0401, USA
Email: {j9han, psiegel}@ucsd.edu

Ron M. Roth
Computer Science Department
Technion, Haifa 32000, Israel
Email: ronny@cs.technion.ac.il

***Abstract*— New bounds on *single-exclusion numbers* are obtained via probabilistic arguments, recurrent relations, as well as explicit constructions. The new bounds are used to better understand the *stopping redundancy* of MDS codes. In particular, it is shown that for any fixed k, the stopping redundancy of a linear $[n,k]$ MDS code is between $\frac{1}{k+1}\binom{n}{k}$ and $\big(1+o(1)\big)\frac{1}{k}\binom{n}{k}$.**

I. Introduction

We say a set A *covers* set B if $|B\setminus A|=1$, i.e. if A contains all except one element of B. An (n,r)-*single-exclusion (SE) system* [1], $n>r$, is a collection of r-subsets of an n-set, called *blocks*, such that all i-subsets of the n-set, $i=1,\ldots,r+1$, are covered by at least one block. The smallest number of blocks in an (n,r)-single-exclusion system is called the (n,r)-*single-exclusion (SE) number*, and is denoted by $S(n,r)$. An (n,r)-SE system with $S(n,r)$ blocks is said to be *minimal*. The *stopping redundancy* [2] of a linear code $\mathcal{C}$, denoted by $\rho(\mathcal{C})$, is the smallest number of rows in a parity-check matrix of $\mathcal{C}$ such that the smallest size of nonempty stopping sets [3] is equal to the minimum distance of $\mathcal{C}$.

The stopping redundancy of a code characterizes the minimum "complexity" (number of check nodes) required in a Tanner graph of the code, such that iterative erasure decoding achieves performance comparable to (up to a constant factor, asymptotically) maximum-likelihood (ML) decoding. In the case of maximum distance separable (MDS) codes, stopping redundancy has a highly combinatorial nature, and is closely related to SE numbers, defined above, and Turán numbers [4].

Briefly, an (n,s,t)-*Turán system*, $n\ge s\ge t$, is a collection of t-subsets of an n-set, called *blocks*, such that every s-subset of the n-set contains at least one block. The *Turán number*, $T(n,s,t)$, is the smallest number of blocks in an (n,s,t)-Turán system. An (n,s,t)-Turán system is *minimal* if it contains $T(n,s,t)$ blocks. A related concept is that of covering design [5]. An (n,s,t)-*covering design*, $n\ge s\ge t$, is a collection of s-subsets of an n-set, called *blocks*, such that every t-subset of the n-set is contained in at least one block. The *covering number*, $C(n,s,t)$, is the smallest number of blocks in an (n,s,t)-covering design. An (n,s,t)-covering design with $C(n,s,t)$ blocks is said to be *minimal*. Clearly, by definition,

$$T(n,s,t)=C(n,n-t,n-s).$$

It is also straightforward to see that an (n,r)-SE system is necessarily an $(n,r+1,r)$-Turán system. Noting further that each block (an r-subset in this case) is contained in $n-r$ $(r+1)$-subsets, we have

$$S(n,r)\ge T(n,r+1,r)\ge\frac{1}{n-r}\binom{n}{r+1}=\frac{1}{r+1}\binom{n}{r}.$$

In [2], the stopping redundancy of MDS codes was connected to covering numbers, and it was shown that for any linear $[n,k,d=n-k+1]$ MDS code $\mathcal{C}$ with $d\ge 3$,

$$\frac{1}{d-1}\binom{n}{d-2}<\rho(\mathcal{C})\le\frac{\max\{n-d+2,d-1\}}{n}\binom{n}{d-2}.$$

The connection was further studied using results on Turán numbers and through the definition of SE systems in [1], based on the observation that

$$T(n,d-1,d-2)\le\rho(\mathcal{C})\le S(n,d-2).$$

Hence, upper bounds on $\rho(\mathcal{C})$ can be obtained by studying upper bounds on SE numbers. Indeed, much improved upper bounds had been found this way in [1]. In this paper, we will further improve these results.

It was conjectured in [2] that the stopping redundancy of MDS codes should only depend on the code parameters n and k, rather than on the code itself. In [1], this was shown to be true in the asymptotic sense for any fixed d, and in the exact sense in some special cases (where d is small). It was also conjectured that $\rho(\mathcal{C})$ should equal $S(n,d-2)$.

Our primary motivation for the further study of SE systems is their evident relevance to an improved understanding of iterative erasure decoding, especially the MDS stopping redundancy conjectures outlined above. The results of this paper take us one step closer to resolving them, particularly for the asymptotic case with k fixed.

In addition, we believe that SE systems warrant further attention because of their intrinsic mathematical appeal. They are natural combinatorial objects, intimately connected to covering designs and Turán systems, and it is not hard to imagine that they might become useful in other applications. Indeed, certain properties of SE numbers are rather surprising. For example, we shall see that for any fixed k,

$$\frac{S(n,n-k-1)}{T(n,n-k,n-k-1)}\le\big(1+o(1)\big)\left(1+\frac{1}{k}\right).$$

1-4244-1429-6/07/$25.00 ©2007 IEEE

Thus, despite the stricter requirements imposed upon the SE system in comparison to the Turan system, the increase in the total number of blocks is very small, for example, only up to two percent when $k = 50$.

As shown in the remainder of this paper, expanding our knowledge about SE systems can shed further light upon properties of both MDS codes and combinatorial constructs to which they are closely related.

II. Probabilistic Bounds

For any set A, let $[A]^i$ denote the set of all i-subsets of A.

Let N be an n-set. Consider the following random experiment in which we build an (n,r)-SE system, $\mathcal{S} \subseteq [N]^r$. In the first step, for a prescribed real value $p \in (0,1)$, insert into $\mathcal{S}$ each element of $[N]^r$ with probability p. The expected size of $\mathcal{S}$ at this point is $p\binom{n}{r}$, but some i-subsets, $i = 1, \ldots, r+1$, may not be covered. The probability that a given i-subset is not covered equals $(1-p)^{\varphi(n,r,i)}$, where

$$\varphi(n,r,i) = i\binom{n-i}{r-i+1} = i\binom{n-i}{n-r-1}.$$

So, as a second step, for each $X \in [N]^i$, $i = 1, \ldots, r+1$, that is not yet covered, insert into $\mathcal{S}$ some element of $[N]^r$ that covers X. The expected size of $\mathcal{S}$ is then bounded from above by

$$p\binom{n}{r} + \sum_{i=1}^{r+1} \binom{n}{i}(1-p)^{\varphi(n,r,i)}.$$

This implies the following upper bound on $S(n,r)$.

Theorem 1: For all $0 < p < 1$,

$$S(n,r) \le p\binom{n}{r} + \sum_{i=1}^{r+1} \binom{n}{i}(1-p)^{i\binom{n-i}{r-i+1}}. \qquad (1)$$

Alternatively, in the first step of the random experiment, we may instead make t random drawings from $[N]^r$. At the end of the first step, the probability that a given i-subset is not covered equals

$$\left(1 - \frac{\varphi(n,r,i)}{\binom{n}{r}}\right)^t$$

if the drawing is done with replacement, and equals

$$\prod_{j=0}^{t-1}\left(1 - \frac{\varphi(n,r,i)}{\binom{n}{r}-j}\right)$$

if the drawing is done without replacement. The results are the following bounds.

Theorem 2: For all $t \in \mathbb{N}$,

$$S(n,r) \le t + \sum_{i=1}^{r+1} \binom{n}{i}\left(1 - \frac{i\binom{n-i}{r-i+1}}{\binom{n}{r}}\right)^t. \qquad (2)$$

Theorem 3: For all $t \in \mathbb{N}$, $t \le \binom{n}{r}$,

$$S(n,r) \le t + \sum_{i=1}^{r+1} \binom{n}{i}\prod_{j=0}^{t-1}\left(1 - \frac{i\binom{n-i}{r-i+1}}{\binom{n}{r}-j}\right). \qquad (3)$$

The bound of Theorem 3 is clearly tighter than that of Theorem 2, and is closely related to the bound of Theorem 1. In fact, one can show that

$$\prod_{j=0}^{t-1}\left(1 - \frac{i\binom{n-i}{r-i+1}}{\binom{n}{r}-j}\right) \le \left(1 - \frac{t-1}{\binom{n}{r}}\right)^{i\binom{n-i}{r-i+1}}.$$

On the other hand, if we let $p = t/\binom{n}{r}$, then (1) can be written as

$$S(n,r) \le t + \sum_{i=1}^{r+1} \binom{n}{i}\left(1 - \frac{t}{\binom{n}{r}}\right)^{i\binom{n-i}{r-i+1}}.$$

Hence, excluding integer effects, the bound of Theorem 3 is at most that of Theorem 1 plus one. In practice, the difference between the two will be small, while the bound of Theorem 1 is usually easier to compute.

Asymptotically, as $n \to \infty$, it can be shown that (details omitted) if $n = \mathrm{Poly}(r)$, then the upper bound in (1) (minimized over p) is $O\left(\frac{\ln r}{r}\binom{n}{r}\right)$. In particular, if $n - r$ is a constant, then the upper bound is $O\left(\frac{\ln n}{n}\binom{n}{r}\right)$, while it can also be shown that in this case the bound must grow faster than $\frac{c}{n}\binom{n}{r}$, for any constant c. We shall see in later sections that other bounds provide much stronger results in this case. In the other extreme, if r is a constant, then the bound in (1) is asymptotic to $\binom{n}{r}$, the trivial upper bound.

III. Constructive Bounds

Construction A: Let N be an n-set, and let r be a prescribed positive integer such that $r < n-2$. Partition N into l subsets, N_i, $i = 0, \ldots, l-1$, as equally as possible. Thus, $N = \bigcup_{i=0}^{l-1} N_i$, such that $\lfloor n/l \rfloor \le |N_i| \le \lceil n/l \rceil$ for all i. For all $X \subseteq N$, define the *weight* of X as $w(X) = \sum_{i=0}^{l-1} i|X \cap N_i|$. For all $j \in \{0, \ldots, l-1\}$, a subset of $[N]^r$ is constructed as follows:

$$B_j = Z \cup \tilde{B}_j,$$

where

$$Z = \{X \in [N]^r : \exists k, X \cap N_k = \emptyset, N_{k-1} \nsubseteq X\},$$

and

$$\tilde{B}_j = \{X \in [N]^r : w(X) \equiv j \mod l\}.$$

Note that in the above definition of Z, the subscript $k-1$ is interpreted as $(k-1 \mod l)$. We shall stick to this convention wherever applicable.

Theorem 4: For all j and all $l \ge n/(n-r-2)$, B_j as given in Construction A is an (n,r)-SE system.

Proof: We show that any $X \in [N]^i$, $i = 1, \ldots, r+1$, is covered by a block in B_j. If $X \cap N_k = \emptyset$ for some k, let $Y \in [N \setminus N_k]^{r+1}$ be selected such that $X \subseteq Y$ and $|Y \cap N_{k-1}|$ is as small as possible. Since $l \ge n/(n-r-2)$, we have $n - |N_k| \ge r+2$, which ensures that Y exists and that if $N_{k-1} \nsubseteq X$ then $N_{k-1} \nsubseteq Y$. Now, choose $x \in X$ such that if $N_{k-1} \subseteq X$ then $x \in N_{k-1}$, otherwise arbitrarily. Note that X is covered by $Y \setminus \{x\}$. But we also have $(Y \setminus \{x\}) \cap N_k = \emptyset$, and $N_{k-1} \nsubseteq (Y \setminus \{x\})$. Therefore, $Y \setminus \{x\} \in Z$.

On the other hand, if $X \cap N_k \neq \emptyset$ for all k, select one element in each such intersection, say $x_k \in X \cap N_k$. Now, choose $Y \in [N]^{r+1}$ such that $X \subseteq Y$, and consider $Y \setminus \{x_k\}$, $k = 0, \ldots, l-1$. All these sets cover X, and since $w(Y \setminus \{x_k\}) = w(Y) - k$, they have distinct weights that span l consecutive integers, one of which must be congruent to j modulo l. Hence, for all j, there exists k such that $Y \setminus \{x_k\} \in \tilde{B}_j$. ∎

Corollary 1: For all integers $l \geq n/(n-r-2)$,

$$S(n,r) \leq l\left[\binom{n-\lfloor \frac{n}{l} \rfloor}{r} - \binom{n-\lfloor \frac{n}{l} \rfloor - \lceil \frac{n}{l} \rceil}{r-\lceil \frac{n}{l} \rceil}\right] + \frac{1}{l}\binom{n}{r}.$$

Proof: Omitted. ∎

An alternative (slightly looser) form of the upper bound is given in the following corollary.

Corollary 2: For all integers $l \geq n/(n-r-2)$,

$$S(n,r) \leq l\left\lceil \frac{n}{l} \right\rceil \binom{n-\lfloor \frac{n}{l} \rfloor - 1}{r} + \frac{1}{l}\binom{n}{r}.$$

Proof: Omitted. ∎

Corollary 3: For fixed k, as $n \to \infty$,

$$S(n, n-k-1) \leq \left(\frac{2}{k+1} + O(n^{-1})\right)\binom{n}{k}.$$

Proof: Corollary 2 applies provided that $l \geq n/(k-1)$. If $k \geq 4$, let $l = \lfloor n/2 \rfloor$. We have

$$\begin{aligned} &S(n, n-k-1) \\ &\leq \frac{3n}{2}\binom{n-3}{n-k-1} + \frac{2}{n}\left(1 + O\left(\frac{1}{n}\right)\right)\binom{n}{n-k-1} \\ &= \frac{2}{k+1}\binom{n}{k} + O(n^{k-1}). \end{aligned}$$

For $k < 4$, the result has already been shown in [1]. ∎

Corollary 4: For all fixed k,

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

Hence, for all $[n,k]$ MDS codes $\mathcal{C}$ with a fixed dimension k,

$$1 \leq \frac{\rho(\mathcal{C})}{T(n, n-k, n-k-1)} \leq 2 + O(n^{-1}).$$

Proof: Simply note $T(n, n-k, n-k-1) \geq \frac{1}{k+1}\binom{n}{k}$. ∎

That $S(n, n-k-1)$ is asymptotically at most $2T(n, n-k, n-k-1)$ has been conjectured in [1]. This bound is sharp for $k = 1$, in which case $S(n, n-2) = n-1$, while $T(n, n-1, n-2) = \lceil n/2 \rceil$. For all $k > 1$, the result can be further improved using recurrent inequalities to be discussed in the next section.

Construction A can also be used to construct Turán systems. In that sense, it can be viewed as an improved version (i.e. one with fewer blocks) of a Turán system construction due to Kim and Roush [6].

Theorem 5: For all j and all l, B_j as given in Construction A is a Turán $(n, r+1, r)$-system.

Proof: Omitted, similar to the proof of Theorem 4. ∎

Next, we consider another construction for SE systems, inspired by a construction for Turán systems due to Frankl and Rödl [7].

Construction B: Let N be an n-set, and let r be a prescribed positive integer such that $r < n$. Let N_i, $i = 0, \ldots, l-1$, and $w(X)$, for all $X \subseteq N$, be defined as in Construction A. We will call the N_i's *bins*. For all $j \in \{0, \ldots, l-1\}$, let

$$\tilde{B}_j = \{X \in [N]^r : w_j(X) \leq \max\{e(X), f(X)\}\},$$

where

$$w_j(X) = (w(X) + j) \mod l,$$

and

$$e(X) = |\{i : X \cap N_i = \emptyset\}|,$$

$$f(X) = |\{i : N_i \subseteq X\}|$$

are the number of "empty" and "full" bins for X, respectively. The constructed collection of r-subsets of N is

$$B_j = F \cup \tilde{B}_j,$$

where F is constructed as follows.

Let the elements in each bin be ordered in some arbitrary, but fixed way. Let $I \subseteq \{0, \ldots, l-1\}$ be a *minimal* index set satisfying $\sum_{k \in I} |N_k| > r$, in the sense that all proper subsets of I violate this condition. For each minimal I and index pair $i, j \in I$, $i \neq j$, let F include the r-set that contains all elements from bins $N_k, k \in I \setminus \{i,j\}$, the smallest $|N_i| - 1$ elements of N_i, and the smallest $r + 1 - \sum_{k \in I, k \neq j} |N_k|$ elements of N_j.

Theorem 6: For all j and all l, B_j as given in Construction B is an (n,r)-SE system.

Proof: We show that any $X \in [N]^i$, $i = 1, \ldots, r+1$, is covered by a block in B_j. If $i = r+1$, note that all r-subsets of X can be written as $X \setminus \{x\}$, for some $x \in X$. Since $w(X \setminus \{x\}) = w(X) - w(\{x\})$ for all $x \in X$, by choosing x from different bins that X intersects, we can make $w(X \setminus \{x\})$ take on $l - e(X)$ different values. Since no two of these values differ by more than $l-1$, this also means that we can realize $l - e(X)$ different values for $w_j(X \setminus \{x\})$. Since only $l - e(X) - 1$ numbers in $\{0, \ldots, l-1\}$ are greater than $e(X)$, there exists $x \in X$ such that $w_j(X \setminus \{x\}) \leq e(X) \leq e(X \setminus \{x\})$, hence $X \setminus \{x\} \in \tilde{B}_j$, and it covers X.

If $i \leq r$, consider two cases. First, let us assume that there exists k, such that $X \cap N_k \neq \emptyset$ and $N_k \not\subseteq X$. In this case, remove from X an arbitrary element in $X \cap N_k$, add in $r - i$ other elements from N using as few elements from N_k as possible, and call the resulting $(r-1)$-set $\tilde{X}$. That is, $\tilde{X} = (X \setminus \{x\}) \cup Y$, for some $x \in X \cap N_k$ and some $Y \in [N \setminus X]^{r-i}$ that has a minimal number of elements from N_k. Note that the choice of $\tilde{X}$ ensures that $f(\tilde{X} \cup \{x\}) = f(\tilde{X})$. Since $w(\tilde{X} \cup \{z\}) = w(\tilde{X}) + w(\{z\})$ for all $z \notin \tilde{X}$, by choosing $z \notin \tilde{X}$, $z \neq x$, from different bins where possible, we can make $w(\tilde{X} \cup \{z\})$ take on $l - f(\tilde{X} \cup \{x\}) = l - f(\tilde{X})$ different values. This also means that we can realize $l - f(\tilde{X})$ different values for $w_j(\tilde{X} \cup \{z\})$. Since only $l - f(\tilde{X}) - 1$ numbers in $\{0, \ldots, l-1\}$ are greater than $f(\tilde{X})$, there exists z such that $w_j(\tilde{X} \cup \{z\}) \leq f(\tilde{X}) \leq f(\tilde{X} \cup \{z\})$, hence $\tilde{X} \cup \{z\} \in \tilde{B}_j$, and it covers X.

Next, if no k exists such that $X \cap N_k \neq \emptyset$ and $N_k \nsubseteq X$, this means that for all k such that $X \cap N_k \neq \emptyset$, we have $N_k \subseteq X$. Figuratively, it means that X consists of a number of full bins. Let N_i be any bin that X intersects. Let $x \in N_i$ be its largest element. Take $X \setminus \{x\}$, and add to it elements from bins that X does not intersect, one bin after another, from smallest to the largest within each bin, until $X \setminus \{x\}$ is augmented to contain r elements. By construction, the r-subset thus obtained is contained in F. ∎

Corollary 5: For all positive integers l,

$$S(n,r) \leq \frac{1}{l}\binom{n}{r} + \binom{n - \lfloor \frac{n}{l} \rfloor}{r} + \binom{n - \lfloor \frac{n}{l} \rfloor}{r - \lfloor \frac{n}{l} \rfloor} + g(n,r,l),$$

where

$$g(n,r,l) = \sum_{\frac{r+1}{\lceil n/l \rceil} \leq i \leq \lceil \frac{r+1}{\lfloor n/l \rfloor} \rceil} \binom{l}{i} i(i-1).$$

Proof: Omitted. ∎

IV. Recurrent Bounds

Lemma 1: For all $0 < r < n-1$,

$$S(n,r) \leq S(n-1,r-1) + T(n-1,r+1,r),$$

or equivalently, for all $0 < k < n-1$,

$$S(n,n-k-1) \leq S(n-1,n-k-2) + C(n-1,k,k-1).$$

Proof: Let N be an n-set and $a \in N$ be an arbitrary element. Let $\mathcal{S} \subseteq [N \setminus \{a\}]^{r-1}$ be a minimal $(n-1,r-1)$-SE system, and $\mathcal{T} \subseteq [N \setminus \{a\}]^r$ be a minimal Turán $(n-1,r+1,r)$-system. Define $\mathcal{S}' = \{s \cup \{a\} : s \in \mathcal{S}\}$. Then $\mathcal{S}' \cup \mathcal{T}$ is an (n,r)-SE system. Indeed, for all $X \in [N]^i$, $i = 1,\ldots,r+1$, if $1 \leq |X \setminus \{a\}| \leq r$, then there exists $s \in \mathcal{S}$ such that $|(X \setminus \{a\}) \setminus s| = 1$, which implies that $|X \setminus (s \cup \{a\})| = 1$, i.e. X is covered by a block in $\mathcal{S}'$. The only cases left are when $X = \{a\}$, and when $X \in [N \setminus \{a\}]^{r+1}$. In either case, X is covered by a block in $\mathcal{T}$. ∎

Theorem 7: For all $0 < r < n-1$,

$$S(n,r) \leq \sum_{i=0}^{r} T(n-r+i-1, i+1, i), \tag{4}$$

or equivalently, for all $0 < k < n-1$,

$$S(n,n-k-1) \leq \sum_{i=k}^{n-1} C(i,k,k-1). \tag{5}$$

Proof: Recursively apply Lemma 1. ∎

Interesting results follow. When $k = 1$, (5) implies that $S(n,n-2) \leq n-1$, which is sharp. When $k = 2$, since $C(i,2,1) = \lceil i/2 \rceil$, (5) gives

$$S(n,n-3) \leq \left\lceil \frac{n}{2} \right\rceil \left\lfloor \frac{n}{2} \right\rfloor - 1,$$

which is better than Corollary 3. In general, we have the following theorem.

Theorem 8: For all fixed k, $k > 0$, as $n \to \infty$,

$$\frac{1}{k+1}\binom{n}{k} \leq S(n,n-k-1) \leq \big(1+o(1)\big)\frac{1}{k}\binom{n}{k}$$

Proof: Since (cf. [8]) for fixed k, t, as $n \to \infty$, $C(n,s,t) = \big(1+o(1)\big)\binom{n}{t}/\binom{s}{t}$, we have

$$\begin{aligned}
&S(n,n-k-1) \\
&\leq \sum_{i \leq \ln n} C(i,k,k-1) + \sum_{\ln n < i < n} C(i,k,k-1) \\
&\leq \ln n \cdot \binom{\ln n}{k} + \sum_{\ln n < i < n} \big(1+o(1)\big)\frac{1}{k}\binom{i}{k-1} \\
&\leq o(n) + \big(1+o(1)\big)\frac{1}{k}\sum_{i=0}^{n-1}\binom{i}{k-1} \\
&= \big(1+o(1)\big)\frac{1}{k}\binom{n}{k}.
\end{aligned}$$

∎

Corollary 6: For all fixed k, $k > 0$, as $n \to \infty$,

$$1 \leq \frac{S(n,n-k-1)}{T(n,n-k,n-k-1)} \leq \frac{k+1}{k}\big(1+o(1)\big).$$

In [1], it was shown that $S(n,3) = T(n,4,3)$ for $6 \leq n \leq 53$. Theorem 7 now allows us to show that the result holds for all $n \geq 6$.

Theorem 9: For all $n \geq 6$,

$$S(n,3) = T(n,4,3).$$

Proof: Omitted. ∎

Since the exact values of most Turán / covering numbers are not known, in most cases, the upper bounds in Theorem 7 cannot be directly evaluated. To get a computable upper bound, one way is to replace each Turán / covering number in the sum by an explicit upper bound. Erdős and Spencer [9] showed that for all $n \geq s \geq t$,

$$C(n,s,t) \leq \left(1 + \ln\binom{s}{t}\right)\frac{\binom{n}{t}}{\binom{s}{t}}. \tag{6}$$

Plugging the above into (5), we obtain the following result.

Theorem 10: For all $0 < k < n-1$,

$$S(n,n-k-1) \leq \frac{1+\ln k}{k}\binom{n}{k}.$$

If instead we bound each term in the sum of (4) or (5) using a different technique, we end up with a different bound. For example, one could apply to (4) the constructive bound on Turán numbers due to Sidorenko [4].

V. Concluding Remarks

Figs. 1–3 show how some of the bounds obtained in this paper compare with other known bounds, when applied to stopping redundancy of MDS codes. (Hence, for an $[n,k,d{=}n{-}k{+}1]$ MDS code, bounds on $S(n,d-2)$ are used.) For "probabilistic" and "Construction A", the bounds of Theorem 1 and Corollary 1 have been used, respectively. For bounds based on recurrent inequalities, "Recurrent A" refers to Theorem 10, and "Recurrent B" refers to (4), with each term in the sum replaced by an upper bound from [4]. All bounds are minimized over their respective auxiliary variables (e.g. p, l), if any, and are normalized relative to the trivial upper bound, $\binom{n}{d-2}$.

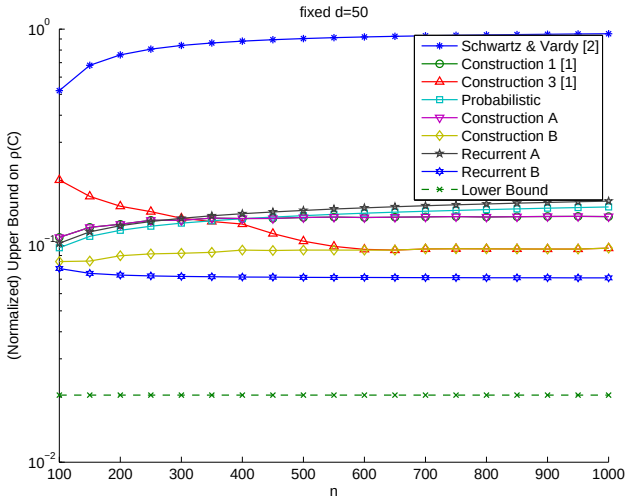

Fig. 1. Bounds on the stopping redundancy of an $(n, n-49, 50)$ MDS code. All bounds normalized relative to $\binom{n}{48}$.

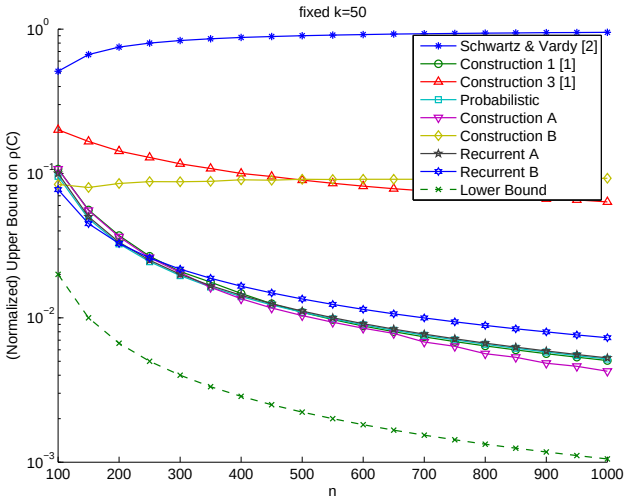

Fig. 2. Bounds on the stopping redundancy of an $(n, 50, n-49)$ MDS code. All bounds normalized relative to $\binom{n}{51}$.

Constructions A and B are closely related to Constructions 1 and 3 in [1], respectively. From the plots, we see that Construction A performs very similarly to Construction 1 in most cases, but shows noticeable improvement when the code rate is low, as supported by our asymptotic analysis. Like Construction 3, Construction B performs poorly when the code rate is low, while it works very well in all other cases, and the improvement over Construction 3 is often significant. The probabilistic bound gives good results in all cases considered. (Although it is asymptotically weak for fixed k or fixed d, the effect is insignificant in practice.) Moreover, its performance is very similar to that of "Recurrent A" (Theorem 10). This is not a coincidence, as (6) was derived based on similar probabilistic arguments. Except for very low code rates, "Recurrent B" gives the best results among all bounds considered. Its relatively weak performance for low code rates is only attributed to the ineffectiveness of the bound from [4] on $T(n, r+1, r)$ for r close to n.

Our study has brought up interesting questions that remain to be answered. For example, is $S(n, n-k-1)$ in fact asymptotic to $(1+1/k)T(n, n-k, n-k-1)$ for all fixed k? Is it true that $S(n, r) \leq 2T(n, r+1, r)$ for all n and r? Finally, does the stopping redundancy of a linear $[n, k, d]$ MDS code equal $S(n, d-2)$ (as conjectured in [1])?

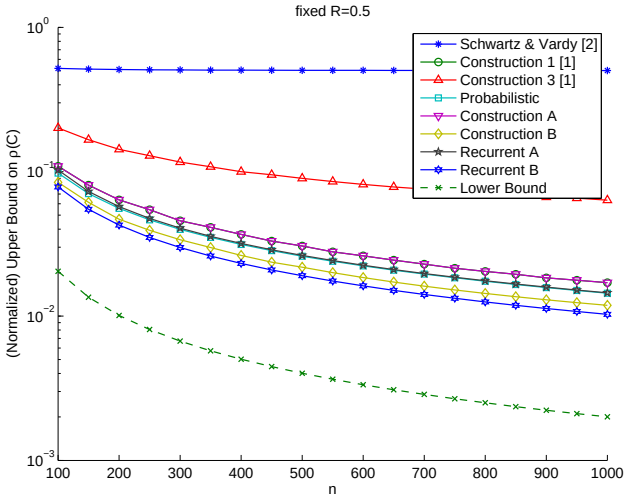

Fig. 3. Bounds on the stopping redundancy of an $(n, n/2, n/2+1)$ MDS code. All bounds normalized relative to $\binom{n}{n/2-1}$.

Acknowledgment

This work was supported in part by the Center for Magnetic Recording Research at UCSD, and by grant No. 2002197 from the United States–Israel Binational Science Foundation (BSF), Jerusalem, Israel. The authors wish to thank Tuvi Etzion for helpful discussions.

References

[1] J. Han and P. H. Siegel, "Improved upper bounds on stopping redundancy," *IEEE Trans. Inform. Theory*, vol. 53, no. 1, pp. 90–104, Jan. 2007.

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

[3] 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.

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

[5] 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.

[6] 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.

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

[8] V. Rödl, "On a packing and covering problem," *European J. Combin.*, vol. 5, pp. 69–78, 1985.

[9] P. Erdős and J. H. Spencer, *Probabilistic Methods in Combinatorics*. Academic Press, 1974.