# Single-Exclusion Number and the Stopping Redundancy of MDS Codes

Junsheng Han, *Member, IEEE*, Paul H. Siegel, *Fellow, IEEE*, and Ron M. Roth, *Fellow, IEEE*

***Abstract*—For a linear block code $\mathcal{C}$, its *stopping redundancy* is defined as the smallest number of check nodes in a Tanner graph for $\mathcal{C}$, such that there exist no stopping sets of size smaller than the minimum distance of $\mathcal{C}$. Schwartz and Vardy conjectured that the stopping redundancy of a maximum-distance separable (MDS) code should only depend on its length and minimum distance.**

**We define the $(n,t)$-*single-exclusion number*, $S(n,t)$ as the smallest number of $t$-subsets of an $n$-set, such that for each $i$-subset of the $n$-set, $i=1,\ldots,t+1$, there exists a $t$-subset that contains all but one element of the $i$-subset. New upper bounds on the single-exclusion number are obtained via probabilistic methods, recurrent inequalities, 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 $[n,k=n-d+1,d]$ MDS codes, as $n\rightarrow\infty$, the stopping redundancy is asymptotic to $S(n,d-2)$, if $d=o(\sqrt{n})$, or if $k=o(\sqrt{n})$, $k\rightarrow\infty$, thus giving partial confirmation of the Schwartz–Vardy conjecture in the asymptotic sense.**

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

## I. Introduction

The stopping redundancy of a linear code characterizes the minimum "complexity" (number of check nodes) required in a Tanner graph for the code, such that iterative erasure decoding achieves performance comparable to (up to a constant factor, asymptotically) maximum-likelihood (ML) decoding. It can be viewed as a basic measure of the complexity–performance tradeoff in the use of redundant parity checks (RPCs) in an iterative decoder on the erasure channel.

Although this tradeoff is less straightforward to understand in non-erasure channels, there is empirical evidence that RPCs can improve performance in belief-propagation decoding on an additive white Gaussian noise (AWGN) channel [1], [2], and, recently, the concept of stopping redundancy has provided partial motivation for novel decoding algorithms that achieve near-ML performance for short, high-rate codes [3].

Formally, we define stopping redundancy as follows. Let $\mathcal{C}$ be an $[n,k,d]$ linear code, and let $H=(h_{ij})_{l\times n}$ be a parity-check matrix for $\mathcal{C}$. We shall assume that $\mathrm{rank}(H)=n-k$, but $l$ may be larger than $(n-k)$. The Tanner graph $\mathcal{G}(H)$ is a bipartite graph with $n$ variable nodes, each corresponding to one column of $H$, and $l$ check nodes, each corresponding to one row of $H$, such that variable node $j$ is adjacent to check node $i$ if and only if $h_{ij}\neq 0$. A *stopping set* in $\mathcal{G}(H)$ is a set of variable nodes such that all check nodes adjacent to the set are connected to the set at least twice. It is well known [4] that iterative erasure decoding is successful if and only if the set of erasure locations does not contain a stopping set. The size of a smallest nonempty stopping set, referred to as the *stopping distance* and denoted by $s(H)$, is therefore an important parameter governing the performance of the iterative decoder. It is clear that $s(H)\leq d$, and it is not difficult to see that equality can be achieved for any code, for example by choosing the rows of $H$ to be the nonzero codewords of the dual code $\mathcal{C}^{\perp}$. This leads to the following definition.

*Definition 1:* Let $\mathcal{C}$ be a linear code with minimum distance $d$. The *stopping redundancy* of $\mathcal{C}$, denoted by $\rho(\mathcal{C})$, is the smallest integer such that there exists a parity-check matrix $H$ for $\mathcal{C}$ with $\rho(\mathcal{C})$ rows, and $s(H)=d$.

Stopping redundancy was introduced by Schwartz and Vardy [5], [6], and was further studied in [7], [8]. The concept was later extended in a number of interesting ways [9]–[11]. Related concepts, such as *stopping set enumerator*, and *generic erasure-correcting sets*, were studied in [12], [13], and in [14], [15], respectively.

In this paper, we study the stopping redundancy of *maximum-distance separable (MDS)* codes. A code is MDS if it satisfies the Singleton bound [16] with equality. Hence, an $[n,k,d]$ linear code is MDS if $d=n-k+1$. MDS codes are interesting for their unique properties and their close relation to other problems in mathematics and engineering. They are also very widely used in practice, a prime example being the class of Reed–Solomon codes [17].

For the rest of the paper, unless otherwise noted, $\mathcal{C}$ denotes an $[n,k=n-d+1,d]$ linear MDS code. In [6], it was shown that for all $d\geq 3$

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

where

$$d^{\perp}=n-d+2$$

Manuscript received December 07, 2007. Current version published August 19, 2009. This work was supported in part by the Center for Magnetic Recording Research at the University of California, San Diego (UCSD), by the National Science Foundation (NSF) under Grant CCF-0829865, and by the United States–Israel Binational Science Foundation (BSF), Jerusalem, Israel, under Grant 2002197. The material in this paper was presented in part at the IEEE International Symposium on Information Theory, Nice, France, June 2007.

J. Han was with the Department of Electrical and Computer Engineering, University of California, San Diego, La Jolla, CA, USA. He is now with Qualcomm Inc., San Diego, CA 92121 USA (e-mail: junsheng@qualcomm.com).

P. H. Siegel is with the Department of Electrical and Computer Engineering, University of California, San Diego, La Jolla, CA 92093-0401 USA (e-mail: psiegel@ucsd.edu).

R. M. Roth is with the Computer Science Department, Technion–Israel Institute of Technology, Technion City, Haifa 32000, Israel (e-mail: ronny@cs.technion.ac.il).

Communicated by T. J. Richardson, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2009.2025578

is the minimum distance of $\mathcal{C}^{\perp}$, the dual code of $\mathcal{C}$. The authors of [6] then made an intriguing conjecture that $\rho(\mathcal{C})$ should in fact be a function of just $n$ and $d$.

Note that the upper bound in (1) is never better than

$$\frac{1}{2}\binom{n}{d-2}.$$

So the upper and lower bounds can differ by up to a factor of $n$. In [8], Han and Siegel observed that the upper bound can be improved by introducing a new combinatorial quantity, the single-exclusion number, which we describe below. Before doing so, we first review two related, well-studied combinatorial constructs. For positive integers $n \geq s \geq t$, and an $n$-set[1] $N$, an $(n,s,t)$-*Turán system* [18] is a collection of $t$-subsets of $N$, called *blocks*, such that each $s$-subset of the $n$-set contains at least one block. The $(n,s,t)$-*Turán number*, denoted hereafter by $T(n,s,t)$, is the smallest number of blocks in an $(n,s,t)$-Turán system. A concept "dual" to that of a Turán system is that of a covering design [19]. Specifically, for $n \geq s \geq t$ and an $n$-set $N$, an $(n,s,t)$-*covering design* is a collection of $s$-subsets of $N$, also called *blocks*, such that each $t$-subset of the $n$-set is contained in at least one block. The $(n,s,t)$-*covering number*, denoted by $C(n,s,t)$, is the smallest number of blocks in an $(n,s,t)$-covering design. Clearly, by definition

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

The stopping redundancy of an MDS code is closely related to covering/Turán numbers. In fact, the lower bound in (1) was shown by noting that to maximize $s(H)$, the supports of minimum-weight rows of $H$ must form an $(n,n-d+2,n-d+1)$-covering design (equivalently, the complements of supports form an $(n,d-1,d-2)$-Turán system). Hence

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

We now define the single-exclusion number, which was introduced in [20].

*Definition 2:* For an $n$-set $N$ and $t < n$, an $(n,t)$-*single-exclusion (SE) system* is a collection of $t$-subsets of $N$, called *blocks*, such that for each $i$-subset of $N$, $i = 1,\ldots,t+1$, there exists at least one block that contains all but one element from the $i$-subset. The $(n,t)$ *SE number*, $S(n,t)$, is the smallest number of blocks in an $(n,t)$-SE system.

Note that an $(n,t)$-SE system is a special kind of $(n,t+1,t)$-Turán system. Note also that if we require all rows in the parity-check matrix $H$ to be of minimum weight, then $s(H) = d$ is equivalent to the condition that the sets of column indices corresponding to the zeros in each row form an $(n,d-2)$-SE system. Hence

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

Therefore, any upper bound on $S(n,d-2)$ is an upper bound on $\rho(\mathcal{C})$.

In [8], a number of upper bounds on $S(n,t)$ were obtained using combinatorial constructions and were shown to be superior to the upper bound in (1). It was shown that $\rho(\mathcal{C}) = T(n,d-1,d-2)$ for $1 < d \leq 4$, $n \geq 6$, and $\rho(\mathcal{C}) \leq T(n,d-1,d-2)+1$ for $d = 5$. It was also shown that $\rho(\mathcal{C})$ is asymptotic to $T(n,d-1,d-2)$ (and to $S(n,d-2)$) as $n \longrightarrow \infty$ for any fixed $d$, and that it is asymptotically at most $3T(n,d-1,d-2)$ for any fixed $k = n-d+1$.

In this paper, we build upon the work in [8] and investigate $S(n,t)$ through a number of different approaches. New upper bounds are obtained and analyzed. They are then used to show that as $n \longrightarrow \infty$, $\rho(\mathcal{C})$ is asymptotic to $S(n,d-2)$ if $d = o(\sqrt{n})$, or if $k = o(\sqrt{n}) \longrightarrow \infty$.[2] Hence, in an asymptotic sense, the Schwartz–Vardy conjecture is proved in these cases. For all $d \leq 5$, it is shown that $\rho(\mathcal{C}) = S(n,d-2)$. A lower bound on $S(n,t)$ is also derived.

The connection between SE systems and the stopping redundancy of MDS codes provides ample motivation to better understand their properties. In addition, they hold intrinsic appeal as well-defined mathematical objects with close relationships to other combinatorial constructs, such as covering designs and Turán systems, that have found wide use in discrete mathematics and its applications.

The rest of the paper is arranged as follows. Section II is devoted to upper bounds on $S(n,t)$. The bounds are obtained through three approaches: combinatorial construction, probabilistic methods, and recurrent inequalities. Certain asymptotic properties of our bounds are observed and discussed, some confirming the Schwartz–Vardy conjecture in an asymptotic sense. The upper bounds are also compared numerically with the best bounds found for $n$ up to 512. In Section III, we derive a lower bound on $S(n,t)$ and observe its implications. Section IV focuses on the Schwartz–Vardy conjecture. We prove the conjecture for all MDS codes with $1 < d \leq 5$, and comment on why $S(n,d-2)$ may be a reasonable estimate of $\rho(\mathcal{C})$. Section V concludes the paper.

## II. Upper Bounds on $S(n,t)$

We start with some preliminaries. For any set $A$, let $[A]^i$ denote the set of all $i$-subsets of $A$. We say that $A$ *covers* another set $B$ if $|B \setminus A| = 1$. Hence, if $N$ is an $n$-set, then $\mathcal{S} \subseteq [N]^t$ is an $(n,t)$-SE system if and only if for each $i = 1,\ldots,t+1$ and $X \in [N]^i$, there exists a block in $\mathcal{S}$ that covers $X$. A covering design/Turán system/SE system (with prescribed parameters) is said to be *minimal* if it contains the least number of blocks.

By definition, an $(n,t)$-SE system is also an $(n,t+1,t)$-Turán system. Hence, we have

$$S(n,t) \geq T(n,t+1,t) \geq \frac{1}{n-t}\binom{n}{t+1} = \frac{1}{t+1}\binom{n}{t} \quad (2)$$

where the second inequality [22] follows by noting that each block in the Turán system is contained in $(n-t)$ distinct $(t+1)$-subsets.

Let $\mathcal{C}$ be an $[n, k = n-d+1, d]$ linear MDS code. Recall that the stopping redundancy of $\mathcal{C}$ is related to SE and Turán numbers in the following way:

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

[1] An *n-set* is a set that contains $n$ elements. Similarly, if $A$ is any set, then a *t-subset* of $A$ is a subset of $A$ that contains $t$ elements.

[2] We adopt the standard "$O$-notation" and related asymptotic expressions [22, Ch. 9]. Functions $f(n)$ and $g(n)$ are said to be *asymptotic* to each other, denoted by $f(n) \sim g(n)$, if $\lim_{n \longrightarrow \infty} f(n)/g(n) = 1$, or equivalently, if $f(n) = (1+o(1))g(n)$, where $o(1)$ stands for any function that goes to zero as $n$ goes to infinity. More generally, we write $f(n) = o(g(n))$ if $\lim_{n \longrightarrow \infty} f(n)/g(n) = 0$.

or equivalently

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

We now focus on upper bounds on $S(n,t)$.

### *A. Probabilistic Bounds*

Probabilistic methods were used to obtain general upper bounds on stopping redundancy [8], [23]. For the case of SE number, we appeal to the same approach with a different argument.

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

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

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

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

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

*Theorem 1:* For all $0 \le p \le 1$,

$$S(n,t) \le p\binom{n}{t} + \sum_{i=1}^{t+1}\binom{n}{i}(1-p)^{i\binom{n-i}{t-i+1}}. \tag{3}$$

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

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

if the drawing is done with replacement, and equals

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

where $(x)^+ \overset{\text{def}}{=} \max\{x, 0\}$, if the drawing is done without replacement. The results are the following bounds.

*Theorem 2:* For all $l \in \mathbb{N}$

$$S(n,t) \le l + \sum_{i=1}^{t+1}\binom{n}{i}\left(1 - \frac{i\binom{n-i}{t-i+1}}{\binom{n}{t}}\right)^l. \tag{4}$$

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

$$S(n,t) \le l + \sum_{i=1}^{t+1}\binom{n}{i}\prod_{j=0}^{l-1}\left(1 - \frac{i\binom{n-i}{t-i+1}}{\binom{n}{t} - j}\right)^+. \tag{5}$$

Theorem 3 is clearly stronger than Theorem 2, and is closely related to Theorem 1. In fact, one can show that

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

So the upper bound (5), when minimized over $l$, is no greater than

$$\min_{\substack{l \in \mathbb{Z} \\ 0 \le l \le \binom{n}{t}}}\left\{l + \sum_{i=1}^{t+1}\binom{n}{i}\left(1 - \frac{l}{\binom{n}{t}}\right)^{\varphi(n,t,i)}\right\} + 1.$$

Note that we have strategically allowed $l$ to take the value $\binom{n}{t}$ in the above expression. On the other hand, letting $l = p\binom{n}{t}$ in (3), we see that the minimum value of the upper bound (3) is

$$\min_{\substack{l \in \mathbb{R} \\ 0 \le l \le \binom{n}{t}}}\left\{l + \sum_{i=1}^{t+1}\binom{n}{i}\left(1 - \frac{l}{\binom{n}{t}}\right)^{\varphi(n,t,i)}\right\}.$$

Now, suppose the minimum value of the above expression is $y$, achieved at $l = l^*$. Then its value at $l = \lceil l^* \rceil$ is less than $y+1$. Therefore, we conclude that the upper bound (5) (when minimized over $l$) is less than the upper bound (3) (when minimized over $p$) plus two. In practice, the difference between the two bounds is very small, while the upper bound in (3) is usually easier to compute.

The upper bound in (3) can be written as

$$\left(p + (1-p)^{t+1}\frac{n-t}{t+1}\right)\binom{n}{t} + \sum_{i=1}^{t}(1-p)^{\varphi(n,t,i)}\binom{n}{i}. \tag{6}$$

The first term in (6) is minimized when $p$ takes the value

$$p_{\min} = 1 - (n-t)^{-1/t}$$

in which case (6) becomes

$$\left(1 - (n-t)^{-1/t} + \eta(n,t)\right) \cdot \binom{n}{t} \tag{7}$$

where

$$\begin{aligned}\eta(n,t) &= \binom{n}{t}^{-1} \cdot \sum_{i=1}^{t+1}(1-p_{\min})^{\varphi(n,t,i)}\binom{n}{i} \\ &= \frac{n-t}{t+1} \cdot \sum_{i=1}^{t+1}\left((n-t)^{-i\binom{n-i}{n-t-1}}/t\right)\frac{\binom{t+1}{i}}{\binom{n-i}{n-t-1}}. \end{aligned} \tag{8}$$

As $n \to \infty$, it can be shown (see Appendix A) that if $t < n - \ln n$, then the term corresponding to $i = t+1$ prevails in the sum (8). Therefore

$$\eta(n,t) = \left(1 + o(1)\right) \cdot \frac{(n-t)^{-1/t}}{t+1}.$$

Plugging the above into (7), we conclude that as $n \to \infty$, the bound (7) is[3]

$$\begin{cases} \left(1+O(n^{-1/t})\right)\binom{n}{t}, & \text{if } t \prec \ln n \\ \left(1-e^{-1/c}+o(1)\right)\binom{n}{t}, & \text{if } t = \left(c+o(1)\right)\ln n \\ \left(1+O\left(\frac{\ln(n-t)}{t}\right)\right)\frac{\ln(n-t)}{t}\binom{n}{t}, & \text{if } \ln n \prec t < n-\ln n \end{cases}$$

where $c > 0$ is any constant. By the choice of $p_{\min}$, and the fact that for $p = p_{\min}$ the $(t+1)$st term prevails in (8), no other values of $p$ give asymptotically tighter bounds than the above.

For the case when $t \geq n - \ln n$, a different asymptotic analysis (see Appendix B) shows that the bound (3), when minimized over $p$, is $O\left(\binom{n}{t}(\ln n)/n\right)$ for all $t$ such that $2 < n-t = o\left((n \ln\ln n)/\ln n\right)$, and is, particularly, $\Theta\left(\binom{n}{t}(\ln n)/n\right)$ for all $t = n - \Theta(1)$.

### *B. Constructive Bounds*

Our first construction for SE systems is based on a Turán system construction due to Kim and Roush [24].

*Construction A:* Let $N$ be an $n$-set, and $t < n-2$ be a positive integer. For a prescribed positive integer $l$, 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 $\lfloor n/l \rfloor \leq |N_i| \leq \lceil n/l \rceil$ for all $i$. We will call each $N_i$ a *bin*. Define

$$w(X) = \sum_{i=0}^{l-1} i|X \cap N_i|, \quad \forall X \subseteq N.$$

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

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

where

$$\begin{aligned} \tilde{B}_j &= \left\{X \in [N]^t : w(X) \equiv j \pmod{l}\right\} \\ Z &= \left\{X \in [N]^t : \exists m, X \cap N_m = \emptyset, N_{m-1} \not\subseteq X\right\}. \end{aligned}$$

Note that in the above definition of $Z$, the subscript $m-1$ is to be interpreted as $(m-1) \bmod l$, and we shall stick to this convention where applicable.

*Proposition 1:* For all $j$ and all $l \geq n/(n-t-2)$, $B_j$ as given in Construction A is an $(n,t)$-SE system.

*Proof:* We show that any $X \in [N]^i$, $i = 1, \ldots, t+1$, is covered by a block in $B_j$. If $X \cap N_m = \emptyset$ for some $m$, let $Y \in [N \setminus N_m]^{t+1}$ be selected such that $X \subseteq Y$ and $|Y \cap N_{m-1}|$ is minimized. Such $Y$ exists since $l \geq n/(n-t-2)$, which implies that $|N \setminus N_m| \geq t+2$. Now let $x \in X$ be chosen such that if $N_{m-1} \subseteq X$ then $x \in N_{m-1}$. Note that $Y \setminus \{x\}$ covers $X$. Note also that $(Y \setminus \{x\}) \cap N_m = \emptyset$, and that the choice of $Y$ and $x$ ensures $N_{m-1} \subseteq (Y \setminus \{x\})$. Hence, $Y \setminus \{x\} \in Z$.

On the other hand, if $X \cap N_m \neq \emptyset$ for all $m$, select one element in each such intersection, say $x_m \in X \cap N_m$. Now, choose $Y \in [N]^{t+1}$ such that $X \subseteq Y$, and consider $Y \setminus \{x_m\}$, $m = 0, \ldots, l-1$. All these sets cover $X$, and since $w(Y \setminus \{x_m\}) = w(Y) - m$, the set $\left\{w(Y \setminus \{x_m\})\right\}_{m=0}^{l-1}$ contains $l$ consecutive integers, one of which must be congruent to $j$ modulo $l$. Hence, for all $j$, there exists $m$ such that $X$ is covered by $Y \setminus \{x_m\} \in \tilde{B}_j$. □

*Theorem 4:* For all integers $l \geq n/(n-t-2)$

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

*Proof:* From Proposition 1, for all $l \geq n/(n-t-2)$

$$S(n,t) \leq \min_j |B_j|.$$

Noting that

$$Z = \bigcup_{m=0}^{l-1} (Z_m \setminus Z'_m)$$

where

$$\begin{aligned} Z_m &= \left\{X \in [N]^t : X \cap N_m = \emptyset\right\} \\ Z'_m &= \left\{X \in [N]^t : X \cap N_m = \emptyset, N_{m-1} \subseteq X\right\} \end{aligned}$$

and that $\{\tilde{B}_j\}_{j=0}^{l-1}$ is a partition of $[N]^t$, we have

$$\begin{aligned} \min_j |B_j| &\leq |Z| + \min_j |\tilde{B}_j| \\ &\leq \sum_{m=0}^{l-1}\left[\binom{n - |N_m|}{t} - \binom{n - |N_m| - |N_{m-1}|}{t - |N_{m-1}|}\right] + \min_j |\tilde{B}_j| \\ &\leq l\left[\binom{n - \lfloor \frac{n}{l} \rfloor}{t} - \binom{n - \lfloor \frac{n}{l} \rfloor - \lceil \frac{n}{l} \rceil}{t - \lceil \frac{n}{l} \rceil}\right] + \frac{1}{l}\binom{n}{t}. \end{aligned}$$ □

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

*Theorem 5:* For all integers $l \geq n/(n-t-2)$

$$S(n,t) \leq \frac{1}{l}\binom{n}{t} + l\left\lceil \frac{n}{l} \right\rceil \binom{n - \lfloor \frac{n}{l} \rfloor - 1}{t}. \tag{9}$$

*Proof:* Note that

$$Z = \bigcup_{m=0}^{l-1} \bigcup_{\alpha \in N_{m-1}} \left[N \setminus \left(N_m \cup \{\alpha\}\right)\right]^t.$$

The rest of the proof is similar to that of Theorem 4. □

*Corollary 1:* For all 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:* Theorem 5 applies provided that $l \geq n/(k-1)$. If $k \geq 4$, let $l = \lfloor n/2 \rfloor$. From (9), we have

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

[3] We write $f(n) \prec g(n)$, if $f(n) = o(g(n))$, and similarly, $f(n) \succ g(n)$, if $g(n) = o(f(n))$, as $n \to \infty$.

For $k=3$, let $l=\lceil n/2\rceil$. If $n$ is even, the above derivation is still valid. If $n$ is odd, then there is one bin that contains a single element, while the remaining $(n-1)/2$ bins each contain two elements. From the proof of Theorem 5, we have

$$\begin{aligned}|Z| &\le \sum_{m=0}^{\lceil n/2\rceil-1} |N_{m-1}|\cdot\binom{n-|N_m|-1}{n-4}\\ &=(n-2)\cdot\binom{n-3}{n-4}+2\cdot\binom{n-2}{n-4}\\ &=O\big(n^2\big).\end{aligned}$$

Hence

$$\begin{aligned}S(n,n-4) &\le \frac{2}{n+1}\binom{n}{n-4}+O(n^2)\\ &=\frac{1}{2}\binom{n}{3}+O\big(n^2\big).\end{aligned}$$

For $k<3$, the result has already been shown in [8]. □

Since

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

Corollary 1 also implies that for any fixed $k$

$$S(n,n-k-1)\le\big(2+O(n^{-1})\big)T(n,n-k,n-k-1)$$

confirming a conjecture made in [8]. Note that the asymptotic factor of 2 in the above inequality 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 $k>1$, stronger results can be obtained using recurrent inequalities, as shall be discussed in the next section.

Construction A is also a construction for Turán systems. Indeed, it can be viewed as an improved version (i.e., one with fewer blocks) of the Turán system construction in [24].

*Proposition 2:* For all $j$ and all $l$, $B_j$ as given in Construction 1 is an $(n,t+1,t)$-Turán system.

*Proof:* The proof is similar to that of Proposition 1. □

Our second construction for SE systems is inspired by a construction for Turán systems due to Frankl and Rödl [25].

*Construction B:* Let $N$ be an $n$-set, and $t<n$ be a positive integer. Let $N_i$, $i=0,\dots,l-1$, and $w(X)$, $\forall X\subseteq N$, be defined as in Construction A. For $j=0,1,\dots,l-1$, let

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

where

$$w_j(X)=(w(X)+j) \bmod l$$

and

$$\begin{aligned}e(X)&=|\{i : X\cap N_i=\emptyset\}|\\ f(X)&=|\{i : N_i\subseteq X\}|\end{aligned}$$

are the number of "empty" and "full" bins for $X$, respectively.

For $j=0,1,\dots,l-1$, the constructed subset of $[N]^t$ is

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

where $F$ is constructed as follows. Fix an arbitrary total order on $N$. Let $I\subseteq\{0,\dots,l-1\}$ be an index set that satisfies $\sum_{m\in I}|N_m|>t$, and is *minimal* in the sense that all proper subsets of $I$ violate this condition. For each such $I$ and $i,j\in I$, $i\ne j$, let $F$ contain the $t$-set that consists of all elements from bins $N_m, m\in I\setminus\{i,j\}$, the smallest $|N_i|-1$ elements of $N_i$, and the smallest $\big(t+1-\sum_{m\in I,m\ne j}|N_m|\big)$ elements of $N_j$.

*Proposition 3:* For all $j$ and all $l$, $B_j$ as given in Construction B is an $(n,t)$-SE system.

*Proof:* We show that any $X\in[N]^i$, $i=1,\dots,t+1$, is covered by a block in $B_j$. If $i=t+1$, note that all $t$-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 $\{0,\dots,l-1\}$ are greater than $e(X)$, there exists $x\in X$ such that $w_j(X\setminus\{x\})\le e(X)\le e(X\setminus\{x\})$, hence $X\setminus\{x\}\in\tilde{B}_j$, and it covers $X$.

If $i\le t$, consider two cases. First, let us assume that there exists $m$, such that $X\cap N_m\ne\emptyset$ and $N_m\nsubseteq X$. In this case, remove from $X$ an arbitrary element in $X\cap N_m$, add in $t-i$ other elements from $N$ using as few elements from $N_m$ as possible, and call the resulting $(t-1)$-set $\tilde{X}$. That is, $\tilde{X}=(X\setminus\{x\})\cup Y$, for some $x\in X\cap N_m$ and some $Y\in[N\setminus X]^{t-i}$ that has a minimal number of elements from $N_m$. 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 $z\notin\tilde{X}$, $z\ne x$, 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 $\{0,\dots,l-1\}$ are greater than $f(\tilde{X})$, there exists $z$ such that $w_j(\tilde{X}\cup\{z\})\le f(\tilde{X})\le f(\tilde{X}\cup\{z\})$, hence $\tilde{X}\cup\{z\}\in\tilde{B}_j$, and it covers $X$.

Next, if no $m$ exists such that $X\cap N_m\ne\emptyset$ and $N_m\nsubseteq X$, this means that for all $m$ such that $X\cap N_m\ne\emptyset$, we have $N_m\subseteq X$. Figuratively, it means that $X$ consists of a number of full bins. Let $N_m$ be any bin that $X$ intersects. Let $x\in N_m$ 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 the smallest to the largest within each bin, until $X\setminus\{x\}$ is augmented to contain $t$ elements. By construction, the $t$-subset thus obtained is contained in $F$. □

*Theorem 6:* For all positive integers $l$

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

where

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

*Proof:* From Proposition 3, for any prescribed $l$

$$S(n,t)\le\min_j|B_j|\le|F|+\min_j|\tilde{B}_j|.$$

To further bound $\min_j|\tilde{B}_j|$, first note that

$$\begin{aligned}\sum_{X\in[N]^t} f(X)&=\sum_{X\in[N]^t}\sum_i[N_i\subseteq X]\\ &=\sum_i\left(\sum_{X\in[N]^t}[N_i\subseteq X]\right)\end{aligned}$$

$$\leq l\binom{n-\lfloor\frac{n}{l}\rfloor}{t-\lfloor\frac{n}{l}\rfloor}$$

where $[N_i \subseteq X] = 1$ if $N_i \subseteq X$, and 0 otherwise. Similarly

$$\sum_{X\in[N]^t} e(X) \leq l\binom{n-\lfloor\frac{n}{l}\rfloor}{t}.$$

Now, since each $X \in [N]^t$ is contained in precisely $1 + \max\{e(X), f(X)\}$ $\tilde{B}_j$'s, we have

$$\begin{aligned}\sum_j |\tilde{B}_j| &= \sum_{X\in[N]^t}\big(1+\max\{e(X),f(X)\}\big)\\ &\leq \binom{n}{t} + \sum_{X\in[N]^t}\big(e(X)+f(X)\big)\\ &\leq \binom{n}{t} + l\binom{n-\lfloor\frac{n}{l}\rfloor}{t} + l\binom{n-\lfloor\frac{n}{l}\rfloor}{t-\lfloor\frac{n}{l}\rfloor}.\end{aligned}$$

Hence

$$\min_j |\tilde{B}_j| \leq \frac{1}{l}\binom{n}{t} + \binom{n-\lfloor\frac{n}{l}\rfloor}{t} + \binom{n-\lfloor\frac{n}{l}\rfloor}{t-\lfloor\frac{n}{l}\rfloor}.$$

Finally, note that $F$ contains $|I|(|I|-1)$ $t$-subsets for each valid $I$, which must satisfy $|I|\lceil n/l\rceil \geq t+1$ and $(|I|-1)\lfloor n/l\rfloor < t+1$. Therefore, $|F| \leq g(n,t,l)$. □

### C. Recurrent Bounds

We observe that an $(n,t)$-SE system can be constructed from an $(n-1,t-1)$-SE system and an $(n-1,t+1,t)$-Turán system, as shown in the following lemma.

*Lemma 1:* For all $0 < t < n-1$

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

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 $\mathcal{S} \subseteq [N\setminus\{a\}]^{t-1}$ be a minimal $(n-1,t-1)$-SE system, and $\mathcal{T} \subseteq [N\setminus\{a\}]^t$ be a minimal $(n-1,t+1,t)$-Turán system. Define $\mathcal{S}' = \{s\cup\{a\} : s\in\mathcal{S}\}$. Then $\mathcal{S}'\cup\mathcal{T}$ is an $(n,t)$-SE system. Indeed, for all $X\in[N]^i$, $i=1,\dots,t+1$, if $1 \leq |X\setminus\{a\}| \leq t$, 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 $X\in[N\setminus\{a\}]^{t+1}$. In either case, $X$ is covered by a block in $\mathcal{T}$. □

*Theorem 7:* For all $0 < t < n-1$

$$S(n,t) \leq \sum_{i=0}^{t} T(n-t+i-1,i+1,i) \tag{10}$$

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

$$S(n,n-k-1) \leq \sum_{i=k}^{n-1} C(i,k,k-1). \tag{11}$$

*Proof:* Recursively apply Lemma 1. □

Interesting results follow. When $k=1$, (11) implies that $S(n,n-2) \leq n-1$, which is sharp. When $k=2$, since $C(i,2,1) = \lceil i/2\rceil$, (11) gives

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

which is asymptotically tighter than Corollary 1.

Generally, since exact values of most Turán/covering numbers are not known, the upper bounds in Theorem 7 often cannot be directly evaluated. To get a computable upper bound, one can simply replace each Turán/covering number in the sum by an explicit upper bound. We show several ways to do this. The first one is based on a result by Erdös and Spencer [26].

*Theorem 8:* For all $0 < k < n-1$

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

*Proof:* In [26], it was shown that for all $n \geq s \geq t$

$$C(n,s,t) \leq \left(1+\ln\binom{s}{t}\right)\frac{\binom{n}{t}}{\binom{s}{t}}. \tag{12}$$

Plugging (12) into (11), we obtain the claimed result after some algebraic manipulations. □

The second computable upper bound is based on an upper bound on Turán numbers due to Sidorenko [18, Construction 4].

*Theorem 9:* For all $0 < t < n-1$ and positive integers $l_0, l_1, \dots, l_t$

$$S(n,t) \leq \sum_{i=0}^{t} f_{n,t}(i,l_i)$$

where

$$f_{n,t}(i,l_i) = \left[\frac{1}{2l_i} + \frac{1}{2}\left(3 + \frac{i}{l_i - 1 - \frac{l_i(i-1)}{m+i}}\right)\left(1-\frac{1}{l_i}\right)^i\right]\cdot\binom{m+i}{i}$$

and $m = n-t-1$.

*Proof:* Omitted. □

A third way to obtain an explicit upper bound from Theorem 7 is based on a construction of an $(n,k,k-1)$-covering design due to Kuzjurin [27], although we count blocks in a slightly different manner.

*Lemma 2:* For all positive integers $n \geq k$

$$C(n,k,k-1) \leq \frac{1}{k}\binom{n}{k-1} + \frac{k-1}{k}\binom{n-1}{k-2}.$$

*Proof:* Let $N$ be an $n$-set. Without loss of generality, let $N = \{1,2,\dots,n\}$. Let

$$Q_i = \left\{X\in[N]^k : \sum_{x\in X} x \equiv i \pmod{n}\right\}$$

and

$$C_i = \{X\in[N]^{k-1} : \nexists Y\in Q_i, \text{s.t. } X\subset Y\},\quad i=0,1,\dots,n-1.$$

For each $X \in C_i$, we can add one block $Y \in [N]^k$ to $Q_i$, such that $X \subset Y$. Hence, by adding no more than $|C_i|$ blocks to $Q_i$, we construct an $(n, k, k-1)$-covering design. Therefore, for all $i$

$$C(n,k,k-1) \leq |Q_i| + |C_i|.$$

Now note that for all $Y, Z \in Q_i, Y \neq Z$, we have $|Y \cap Z| \leq k-2$. Therefore, for all $X \in [N]^{k-1}$ there is at most one block $Y$ in $Q_i$ such that $X \subset Y$; on the other hand, for every $Y \in [N]^k$ there are $k$ elements $X \in [N]^{k-1}$ such that $X \subset Y$. Hence

$$|C_i| = \binom{n}{k-1} - k|Q_i|.$$

We have

$$\begin{aligned}\sum_{i=0}^{n-1}\big(|Q_i| + |C_i|\big) &= \sum_{i=0}^{n-1}\left(\binom{n}{k-1} - (k-1)|Q_i|\right)\\ &= n\binom{n}{k-1} - (k-1)\binom{n}{k}.\end{aligned}$$

Therefore, there exists $i$, such that

$$\begin{aligned}|Q_i| + |C_i| &\leq \binom{n}{k-1} - \frac{k-1}{n}\binom{n}{k}\\ &= \frac{1}{k}\binom{n}{k-1} + \frac{k-1}{k}\binom{n-1}{k-2}. \qquad \square\end{aligned}$$

Plugging the bound in the preceding lemma into (11), we obtain the following theorem.

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

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

*Proof:* Omitted. □

*Corollary 2:* For all $0 < k < n-1$

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

In particular, as $n \longrightarrow \infty$, if $k = o(\sqrt{n})$ and $k \longrightarrow \infty$, then

$$S(n, n-k-1) \sim T(n, n-k, n-k-1).$$

*Proof:* Omitted. □

Interestingly, a similar asymptotic result can be shown for $S(n,t)$ when $t$ is relatively small. First, we note the following theorem relating SE and Turán numbers.

*Theorem 11:* For all $0 < t < n-1$

$$S(n,t) \leq \left(1 - \frac{t}{n}\right) T(n, t+1, t) + \binom{n-1}{t-1}.$$

*Proof:* We will use the fact [28] that

$$T(n,s,t) \geq \frac{n}{n-t}\ T(n-1, s, t).$$

From Theorem 7, we have

$$\begin{aligned}S(n,t) &\leq T(n-1, t+1, t) + \sum_{i=0}^{t-1} T(n-t+i-1, i+1, i)\\ &\leq \left(1 - \frac{t}{n}\right) T(n, t+1, t) + \sum_{i=0}^{t-1}\binom{n-t+i-1}{i}\\ &= \left(1 - \frac{t}{n}\right) T(n, t+1, t) + \sum_{i=n-t-1}^{n-2}\binom{i}{n-t-1}\\ &= \left(1 - \frac{t}{n}\right) T(n, t+1, t) + \binom{n-1}{t-1}. \qquad \square\end{aligned}$$

In [8, Theorem 21], it was shown that $S(n,t)$ is asymptotic to $T(n, t+1, t)$ for any fixed $t$ as $n \longrightarrow \infty$. Theorem 11 enables us to extend this result to all $t = o(\sqrt{n})$.

*Corollary 3:* For all $0 < t < n-1$

$$S(n,t) \leq \left(1 + \frac{t^2}{n}\right) T(n, t+1, t).$$

In particular, as $n \longrightarrow \infty$, if $t = o(\sqrt{n})$, then

$$S(n,t) \sim T(n, t+1, t).$$

*Proof:* Note that

$$\frac{\binom{n-1}{t-1}}{T(n,t+1,t)} \leq \frac{\binom{n-1}{t-1}}{\frac{1}{t+1}\binom{n}{t}} = \frac{t^2+t}{n}.$$

The result then follows immediately from Theorem 11. □

### *D. Comparison of Upper Bounds*

We numerically computed several of the upper bounds on $S(n, d-2)$, and hence on $\rho(\mathcal{C})$, for all $5 < d \leq n \leq 512$. For each $(n,d)$ pair, the tightest bound is identified, and the results are shown in Fig. 1. Other bounds in the comparison that do not appear in Fig. 1 are those of Theorem 8, [1, Theorem 27], [1, Theorem 39], and the upper bound in (1), which is due to Schwartz and Vardy [6]. Note that $d \leq 5$ is not considered, since in this case $S(n, d-2)$ (and $\rho(\mathcal{C})$) is known to be at most $T(n, d-1, d-2) + 1$, for which either precise formulas are known, or tighter special upper bounds exist [8].

We observe that Theorem 9 appears to be the best upper bound except when the code rate is low, in which case Theorems 1, 4, and 10 give better results. Theorem 6 yields the tightest bound for just a few occasions with small values of $n$ and $d$.

Some examples of the upper bounds are given in Table I. The tightest are highlighted in boldface. For comparison, a lower bound on $T(n, d-1, d-2)$ (hence on $S(n, d-2)$ and $\rho(\mathcal{C})$ as well) has been included, based on (13) (see Section III). Compared to upper bounds previously known, significant improvements are observed. As a side note, we caution that while Theorem 10 is an excellent bound when $d$ is very close to $n$, it becomes loose quickly as $d$ gets smaller, and should be avoided if the code rate is greater than $1/2$.

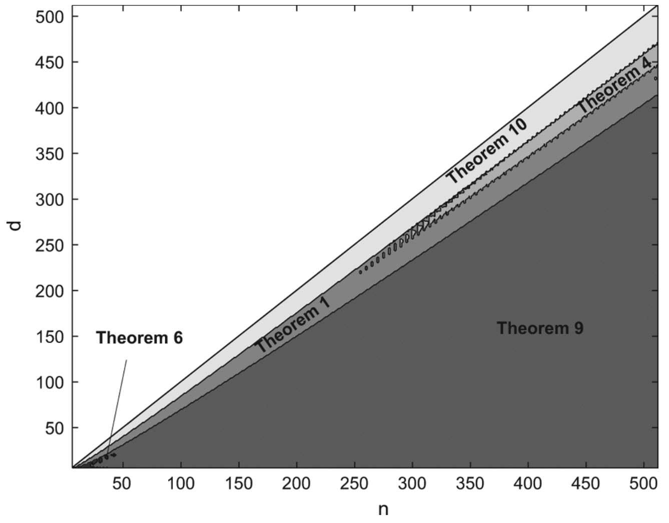

Fig. 1. Best upper bounds on $S(n, d{-}2)$ (hence on $\rho(\mathcal{C})$), for $5 < d \leq n \leq 512$.

TABLE I
UPPER BOUNDS ON $S(n, d-2)$ AND $\rho(\mathcal{C})$

| $(n, d) =$ | $(31, 7)$ | $(31, 23)$ | $(31, 27)$ |
|---|---|---|---|
| Theorem 1 | 96,112 | **6,412,596** | 77,298 |
| Theorem 4 | 93,691 | 7,693,683 | 86,148 |
| Theorem 6 | 76,986 | 12,151,903 | 299,697 |
| Theorem 8 | 124,250 | 7,161,809 | 88,673 |
| Theorem 9 | **71,891** | 9,665,343 | 520,847 |
| Theorem 10 | 599,474 | 7,442,607 | **55,905** |
| Han-Siegel [8, Theorem 27] | 93,691 | 7,786,707 | 106,388 |
| Han-Siegel [8, Theorem 39] | 76,986 | 16,275,110 | 269,970 |
| Schwartz-Vardy (1) [6] | 142,506 | 31,475,730 | 617,526 |
| Lower Bound (13) | 33,981 | 2,103,660 | 29,450 |

## III. LOWER BOUNDS ON $S(n, t)$

A few other lower bounds on Turán/covering numbers are known, besides the simple lower bound in (2). For example, Schönheim [28] showed that

$$T(n, t+1, t) \geq \left\lceil \frac{n}{n-t} \left\lceil \frac{n-1}{n-t-1} \left\lceil \cdots \left\lceil \frac{t+2}{2} \right\rceil \cdots \right\rceil \right\rceil \right\rceil. \tag{13}$$

Another useful bound is due to de Caen [29]

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

Note that a lower bound on $T(n, d-1, d-2)$ is in turn a lower bound on $\rho(\mathcal{C})$ and on $S(n, d-2)$.

In this section, we study a lower bound result on $S(n, t)$ (which is not a lower bound on $T(n, t+1, t)$ in general). Note that a lower bound (just) on $S(n, d{-}2)$ is not necessarily a lower bound on $\rho(\mathcal{C})$.

*Theorem 12:* For all $0 < t < n-1$

$$\left(1 + \frac{n-t}{n\left(n-t-\frac{1}{2}\right)}\right) S(n, t) \geq T(n-1, t+1, t) + \frac{1}{n-t-\frac{1}{2}} \binom{n-1}{t}.$$

*Proof:* Let $N$ be an $n$-set, and $\mathcal{S} \subseteq [N]^t$ be a minimal $(n, t)$-SE system. For each $j \in N$, $\mathcal{S}$ can be partitioned into blocks that contain $j$ and those that do not, namely

$$\mathcal{S} = \mathcal{A}_j \cup \mathcal{B}_j$$

where $\mathcal{A}_j = \{X \in \mathcal{S} : j \in X\}$ and $\mathcal{B}_j = \{X \in \mathcal{S} : j \notin X\}$. Note that for all $j$, $\mathcal{B}_j$ is an $(n{-}1, t{+}1, t)$-Turán system. Further, if we let $\mathcal{A}'_j = \{A \setminus \{j\} : A \in \mathcal{A}_j\}$, then each member of $[N \setminus \{j\}]^t \setminus \mathcal{B}_j$ includes an element of $\mathcal{A}'_j$ as a subset. To see this, suppose $X \in [N \setminus \{j\}]^t \setminus \mathcal{B}_j$. Then $X \cup \{j\}$ is a $(t{+}1)$-set and so there exists $Y \in \mathcal{S}$ such that $Y \subset \big(X \cup \{j\}\big)$. Since $X \notin \mathcal{S}$, we must have $j \in Y$. Hence, $(Y \setminus \{j\}) \in \mathcal{A}'_j$ and $(Y \setminus \{j\}) \subset X$.

On the other hand, since each element of $\mathcal{A}'_j$ is contained in

$$(n-1) - (t-1) = n - t$$

$t$-subsets of $N \setminus \{j\}$, it is contained in at most $(n-t)$ distinct $t$-sets in $[N \setminus \{j\}]^t \setminus \mathcal{B}_j$. Therefore

$$|\mathcal{A}_j| = |\mathcal{A}'_j| \geq \frac{1}{n-t} \left( \binom{n-1}{t} - |\mathcal{B}_j| \right).$$

This lower estimate can be improved by a more careful argument as follows. Let

$$\begin{aligned}
\mathcal{A}'_{j1} &= \{A \in \mathcal{A}'_j : \exists B \in \mathcal{B}_j, A \subset B\},\\
\mathcal{A}'_{j2} &= \{A \in \mathcal{A}'_j \setminus \mathcal{A}'_{j1} : \exists A' \in \mathcal{A}'_{j1}, |A \setminus A'| = 1\},\\
\mathcal{A}'_{j3} &= \{A \in \mathcal{A}'_j \setminus (\mathcal{A}'_{j1} \cup \mathcal{A}'_{j2}) : \exists A' \in \mathcal{A}'_{j2}, |A \setminus A'| = 1\},\\
&\vdots\\
\mathcal{A}'_{ji} &= \left\{A \in \mathcal{A}'_j \setminus \bigcup_{l=1}^{i-1} \mathcal{A}'_{jl} : \exists A' \in \mathcal{A}'_{j(i-1)}, |A \setminus A'| = 1\right\},\\
&\vdots
\end{aligned}$$

Note that $\mathcal{A}'_{ji} \cap \mathcal{A}'_{jl} = \emptyset$ for all $i \neq l$. Since $\mathcal{A}'_j$ is finite, there exists $i$ such that $\mathcal{A}'_{jl} = \emptyset$ for all $l > i$. Regardless, define

$$\tilde{\mathcal{A}}'_j = \bigcup_{l=1}^{\infty} \mathcal{A}'_{jl}.$$

We claim that on average, an element in $\tilde{\mathcal{A}}'_j$ is contained in at most $(n-t-1)$ $t$-sets in $[N \setminus \{j\}]^t \setminus \mathcal{B}_j$. To see this, consider a process in which we enumerate elements of $\mathcal{A}'_j$, and for each element, "mark" the $t$-sets in $[N \setminus \{j\}]^t \setminus \mathcal{B}_j$ that contain it. We start with elements in $\mathcal{A}'_{j1}$ and proceed to $\mathcal{A}'_{j2}, \mathcal{A}'_{j3}$, and so on. Each element in $\mathcal{A}'_{j1}$ is contained in $(n-t)$ $t$-sets in $[N \setminus \{j\}]^t$, at least one of which lies in $\mathcal{B}_j$. Therefore, for each element in $\mathcal{A}'_{j1}$, at most $(n-t-1)$ $t$-sets are marked. Now, for any $X \in \mathcal{A}'_{j2}$, by definition, there exists $Y \in \mathcal{A}'_{j1}$, such that $|X \setminus Y| = 1$. Hence, among the $(n-t)$ $t$-sets that contain $X$, at least one of them, namely, $X \cup Y$, is already marked. Therefore, processing any $X \in \mathcal{A}'_{j2}$ marks at most $(n-t-1)$ additional $t$-sets in $[N \setminus \{j\}]^t \setminus \mathcal{B}_j$. A similar argument shows that among the $(n-t)$ $t$-sets that contain an element of $\mathcal{A}'_{ji}$, at least one of them is already marked after elements of $\mathcal{A}'_{j(i-1)}$ have been processed.

For $\mathcal{A}'_j \setminus \tilde{\mathcal{A}}'_j$, we show that on average, each element marks at most $(n-t-1/2)$ $t$-sets in $[N\setminus\{j\}]^t \setminus \mathcal{B}_j$. Let $X \in \mathcal{A}'_j \setminus \tilde{\mathcal{A}}'_j$. As $X \cup \{j\} \in [N]^t$, there exists $Y \in \mathcal{S}$ such that $|(X\cup\{j\}) \setminus Y| = 1$. Since $X \notin \mathcal{A}'_{j1}$, we have $j \in Y$ and, hence, $Y \setminus \{j\} \in \mathcal{A}'_j$. In fact, $Y \setminus \{j\} \in \mathcal{A}'_j \setminus \tilde{\mathcal{A}}'_j$, since otherwise it would imply that $X \in \tilde{\mathcal{A}}'_j$. Now, let $Z = X \cup Y \setminus \{j\}$, and denote by $l$ the number of elements of $\mathcal{A}'_j \setminus \tilde{\mathcal{A}}'_j$ that are contained in $Z$. Note that $l \geq 2$, since $Z$ contains both $X$ and $Y \setminus \{j\}$. Therefore, of the $l$ elements that are contained in $Z$, each on average marks

$$n - t - \frac{l-1}{l} \leq n - t - \frac{1}{2}$$

$t$-sets in $[N \setminus \{j\}]^t \setminus \mathcal{B}_j$. For other elements in $\mathcal{A}'_j \setminus \tilde{\mathcal{A}}'_j$, the above argument can be repeated until all elements have been considered.

Based on the preceding discussions, we conclude that on average, each block in $\mathcal{A}'_j$ is contained in no more than $(n-t-1/2)$ $t$-sets in $[N \setminus \{j\}]^t \setminus \mathcal{B}_j$. Hence

$$\begin{aligned}|\mathcal{S}| &= |\mathcal{A}'_j| + |\mathcal{B}_j| \\ &\geq \frac{1}{n-t-\frac{1}{2}}\left(\binom{n-1}{t} - |\mathcal{B}_j|\right) + T(n-1,t+1,t). \quad (14)\end{aligned}$$

Since each block of $\mathcal{S}$ appears in $n-t$ of the $\mathcal{B}_j$'s, we have

$$\sum_{j\in N} |\mathcal{B}_j| = (n-t)|\mathcal{S}|.$$

Summing (14) over all $j$, dividing both sides by $n$, and noting that $|\mathcal{S}| = S(n,t)$ (since $\mathcal{S}$ was chosen to be minimal) gives the desired inequality. □

*Corollary 4:* For all $0 < t < n-1$, we have

$$S(n,t) \geq \frac{1}{n-t-\frac{t}{n}+\frac{1}{2}}\binom{n}{t+1}.$$

*Proof:* Simply use the facts that

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

and

$$\binom{n}{t+1} = \binom{n-1}{t+1} + \binom{n-1}{t}. \qquad \square$$

Equivalently, letting $k = n-t-1$, we have that for all $0 < k < n-1$

$$S(n,n-k-1) \geq \frac{1}{k+\frac{k+1}{n}+\frac{1}{2}}\binom{n}{k}$$

hence the following corollary.

*Corollary 5:* For all $k > 0$, as $n \longrightarrow \infty$

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

*Proof:* Trivial. □

For fixed $k$, the value $T(n,n-k,n-k-1)$ is asymptotic to $\binom{n}{k}/(k+1)$ (cf. [30]). So the above corollary shows that for *any* fixed $k$, the ratio $S(n,n-k-1)\,/\,T(n,n-k,n-k-1)$ is bounded away from 1 as $n \longrightarrow \infty$.

## IV. On the Schwartz–Vardy Conjecture

Schwartz and Vardy [6] conjectured that the stopping redundancy of an MDS code only depends on its length and minimum distance. Han and Siegel [8] showed that for $1 < d \leq 5$, the upper and lower bounds on $\rho(\mathcal{C})$ for any $[n, n-d+1, d]$ MDS code $\mathcal{C}$ differ by at most 1. Using Theorem 7, we can now close the gap completely and prove the Schwartz–Vardy conjecture for all MDS codes with $1 < d \leq 5$.

*Theorem 13:* For all $n \geq 6$

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

*Proof:* Let $\mathcal{T}$ be a minimal $(n,4,3)$-Turán system, $n \geq 6$. We show that $\mathcal{T}$ must also be an $(n,3)$-SE system. Since $\mathcal{T}$ is an $(n,4,3)$-Turán system, all 4-sets are covered. In [8], it was shown that all 1-sets and 2-sets are covered too. It remains to show that all 3-sets are covered. Suppose, to the contrary, that some 3-set, $X$, is not covered. It was shown in [8] that at least $1+2\binom{n-3}{2}$ blocks in $\mathcal{T}$ contain elements from $X$, and those that do not form an $(n-3,4,3)$-Turán system. Hence

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

However, from Theorem 7

$$S(n,3) \leq T(n-1,4,3) + T(n-2,3,2) + T(n-3,2,1) + 1.$$

And since (cf. [18])

$$T(n,s,t) \leq T(n-1,s,t) + T(n-1,s-1,t-1)$$

we have

$$T(n-1,4,3) \leq T(n-3,4,3) + T(n-3,3,2) + T(n-2,3,2).$$

Together, these imply that

$$\begin{aligned}S(n,3) \leq T(n-3,4,3) &+ 2T(n-2,3,2) \\ &+ T(n-3,3,2) + n - 3.\end{aligned}$$

Putting the upper and lower bounds on $S(n,3)$ together, we have

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

However, since it is known (cf. [31], [32]) that $T(n,3,2) = \lfloor n/2 \rfloor (\lceil n/2 \rceil - 1)$, the above inequality results in a contradiction for all $n \geq 9$. For $n = 6, 7, 8$, the theorem can be verified directly, and was also proved in [8] (for $6 \leq n \leq 53$) using a different argument. □

Summarizing Theorem 13 and results in [8], we reach the following conclusion.

*Proposition 4:* If $\mathcal{C}$ is an $[n, n-d+1, d]$ MDS code, and $1 < d \leq 5$, then

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

*Proof:* For $(n,d) \in \{(4,4),(5,4),(5,5)\}$, it is easy to find that $S(4,2) = 3$, $S(5,2) = 5$, $S(5,3) = 4$, and verify that

$\rho(\mathcal{C}) = S(n, d-2)$ in all three cases. Otherwise, since $T(n, d-1, d-2) \leq \rho(\mathcal{C}) \leq S(n, d-2)$, it follows immediately from Theorem 13 and [8, Theorems 14 and 16] that

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

in all other cases. □

In addition, from Corollaries 2 and 3, we see that as $n \longrightarrow \infty$, if $d = o(\sqrt{n})$, or if $k = o(\sqrt{n})$ and $k \longrightarrow \infty$, then

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

So in these cases we may say that the Schwartz–Vardy conjecture holds in the asymptotic sense.

Our approach regarding the conjecture has been so far to show that in some cases the upper and lower bounds on stopping redundancy (SE and Turán numbers, respectively) converge, either exactly or asymptotically. However, we have seen that in other cases the corresponding SE and Turán numbers can be provably different, even in the asymptotic sense (for example, see the discussion following Corollary 5), which shows the limitation of the current approach in fully resolving the conjecture.

It was conjectured in [20] that for an $[n, n-d+1, d]$ MDS code $\mathcal{C}$

$$\rho(\mathcal{C}) = S(n, d-2), \tag{15}$$

the proof of which would in turn prove the Schwartz–Vardy conjecture. We have shown that (15) is true for $1 < d \leq 5$ and that it is true in an asymptotic sense for $d = o(\sqrt{n})$, and for $k = o(\sqrt{n})$, $k \longrightarrow \infty$. A reasonable question to ask is: what if both $d$ and $k$ are larger than $o(\sqrt{n})$? For example, what if $k/n$ approaches a constant? The current approach only bounds $\rho(\mathcal{C})$ to within a factor of up to $\ln n$. For example, using the result of Theorem 8, we have

$$\rho(\mathcal{C}) \leq \frac{n-d+2}{n-d+1} \cdot \frac{1 + \ln(n-d+1)}{d-1} \cdot \binom{n}{d-2}$$

while, for the lower bound, we saw that

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

Alternatively, let us make the following observation. Suppose we are given one optimal parity-check matrix, i.e., one with $\rho(\mathcal{C})$ rows that maximizes stopping distance. It is not apparent that all rows should have minimum weight, but suppose $T'$ rows are of minimum weight and the rest are not. We can replace each row that is not of minimum weight (and whose weight is, of course, at most $n$) with no more than $\lceil n/(n-d+2) \rceil$ minimum-weight rows, such that the union of supports of these rows is precisely the support of the row they replaced. It is simple to verify that the replacement procedure does not decrease the stopping distance, which also implies that the rank of the matrix is not reduced. After all rows that are not of minimum weight have been replaced, we obtain a parity-check matrix with at most

$$T' + \left\lceil \frac{n}{n-d+2} \right\rceil \left( \rho(\mathcal{C}) - T' \right)$$

rows, all having minimum weight, that achieves maximum stopping distance. Therefore

$$T' + \left\lceil \frac{n}{n-d+2} \right\rceil \left( \rho(\mathcal{C}) - T' \right) \geq S(n, d-2).$$

Now note that

$$T' \geq T(n, d-1, d-2)$$

so we have

$$\rho(\mathcal{C}) \geq \frac{S(n, d-2)}{\left\lceil \frac{n}{n-d+2} \right\rceil} + \frac{\left\lceil \frac{n}{n-d+2} \right\rceil - 1}{\left\lceil \frac{n}{n-d+2} \right\rceil} \cdot T(n, d-1, d-2).$$

Without knowing better how $T(n, d-1, d-2)$ compares with $S(n, d-2)$, if we just ignore the second term, we obtain

$$\frac{S(n, d-2)}{\left\lceil \frac{n}{n-d+2} \right\rceil} \leq \rho(\mathcal{C}) \leq S(n, d-2).$$

This shows that in many cases, $S(n, d-2)$ is a good estimate of $\rho(\mathcal{C})$. For example, if the code rate $R = (n-d+1)/n \geq 1/2$, then

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

And, clearly, for any constant code rate, $\rho(\mathcal{C})$ is within a constant factor of $S(n, d-2)$.

## V. Concluding Remarks

While we have obtained a fairly good understanding of the SE number, and in some cases come close to uncovering the true value of the stopping redundancy of MDS codes along the way, many interesting questions remain unanswered. For example, what is the asymptotic value of $S(n, n-k-1)$ for a fixed $k$? And how does $S(n, t)$ compare with $T(n, t+1, t)$ in general? (Do they differ by at most a constant factor?) Finally, is it true that the stopping redundancy of an $[n, n-d+1, d]$ MDS code equals $S(n, d-2)$?

## Appendix A
## Asymptotics of (8) for $t < n - \ln n$

Rewrite (8) as

$$\eta(n, t) = \frac{n-t}{t+1} \cdot \sum_{i=1}^{t+1} f(i) \tag{16}$$

where

$$f(i) = \frac{\binom{t+1}{i}}{\binom{n-i}{n-t-1}} \cdot (n-t)^{-i \binom{n-i}{n-t-1}/t}.$$

Assuming

$$n - t > \ln n$$

we show that the $(t+1)$st term

$$f(t+1) = (n-t)^{-(t+1)/t}$$

prevails in the sum of (16).

It suffices to show that each of the other $t$ terms is an $o(1/t)$ fraction of $f(t+1)$. For $i = t$, it is easy to verify that

$$f(t) = \frac{t+1}{n-t} \cdot (n-t)^{-(n-t)} = o\left(\frac{1}{t}\right) f(t+1).$$

In general, we have

$$\frac{f(i)}{f(t+1)} = \frac{\binom{t+1}{i}}{\binom{n-i}{n-t-1}} \cdot (n-t)^{-i\binom{n-i}{n-t-1}/t+(t+1)/t}. \qquad (17)$$

For $i = 1, \ldots, t-1$, consider two cases. For $i \leq 2n/\ln n = o(n)$, we have

$$\binom{n-i}{n-t-1} \geq \binom{n\left(1-\frac{2}{\ln n}\right)}{2} = \Omega(n^2).$$

In this case, (17) decreases super-exponentially with $n$, and is certainly $o(1/t)$. On the other hand, for $2n/\ln n < i \leq t-1$, we show that $f(i) < f(t) = o(1/t)f(t+1)$, by showing that $f(i)$ is monotonically increasing for $2n/\ln n < i \leq t$. Indeed, for $2n/\ln n < i \leq t-1$, we have

$$\begin{aligned} \frac{f(i+1)}{f(i)} &= \frac{n-i}{i+1} \cdot (n-t)^{-(i+1)\binom{n-i-1}{n-t-1)}/t+i\binom{n-i}{n-t-1}/t} \\ &= \frac{n-i}{i+1} \cdot (n-t)^{(i-(t-i+1)/(n-t-1)\binom{n-i-1}{n-t-2})/t} \\ &> \frac{\ln n}{n} \cdot (\ln n)^{(2n/\ln n - n/\ln n)\binom{\ln n}{2}/t} \\ &> \left(\frac{\sqrt{\ln n}}{e}\right)^{\ln n} > 1. \end{aligned}$$

## Appendix B
### Asymptotics of the Bound (3) for $t \geq n - \ln n$

Let $k = n-t-1$, and $j = t+1-i$. The right-hand side of (3) becomes

$$p\binom{n}{k+1} + \sum_{j=0}^{t} \binom{n}{k+j}(1-p)^{(n-k-j)\binom{k+j}{k}}. \qquad (18)$$

Let $p = (\ln n)/n$. Assume that

$$1 < k = o\left(\frac{n \ln\ln n}{\ln n}\right)$$

($n - \ln n \leq t < n-2$ being a special case). We show that the first term in (18) prevails. Note that

$$\begin{aligned} \left(1 - \frac{\ln n}{n}\right)^{(n-k-j)\binom{k+j}{k}} &\leq e^{-(n-k-j)\binom{k+j}{k}(\ln n)/n} \\ &= n^{-(n-k-j)\binom{k+j}{k}/n}. \end{aligned}$$

For $1 \leq j \leq n\sqrt{2/\ln n}$, we have

$$\frac{n-k-j}{n}\binom{k+j}{k} \geq \left(1-o(1)\right)\binom{j+2}{2} > j+1.$$

For $j > n\sqrt{2/\ln n}$, we have

$$\frac{\ln n}{n} \cdot (n-k-j)\binom{k+j}{k} \geq \frac{\ln n}{n}\binom{j+2}{2} > n.$$

Noting further that for $j \geq 1$

$$\binom{n}{k+j} \leq \binom{n}{k+1} \cdot n^{j-1}$$

we see that the second term in (18) is at most

$$\begin{aligned} &\binom{n}{k} \cdot n^{-(n-k)/n} + \sum_{j=1}^{\lfloor n\sqrt{2/\ln n}\rfloor} \binom{n}{k+1} \cdot n^{j-1} \\ &\quad \cdot n^{-(n-k-j)\binom{k+j}{k}/n} + \sum_{j=\lfloor n\sqrt{2/\ln n}\rfloor+1}^{r} \binom{n}{k+j} \\ &\quad \cdot e^{-(n-k-j)\binom{k+j}{k}(\ln n)/n} \\ &\leq \binom{n}{k+1} \cdot n^{-1+k/n} + \binom{n}{k+1} \sum_{j=1}^{\lfloor n\sqrt{2/\ln n}\rfloor} n^{-2} \\ &\quad + e^{-n} \sum_{j=\lfloor n\sqrt{2/\ln n}\rfloor+1}^{r} \binom{n}{k+j} \\ &\leq \frac{1}{n}\binom{n}{k+1}\left(e^{(k\ln n)/n} + \sqrt{\frac{2}{\ln n}}\right) + 2^n \cdot e^{-n} \\ &= \frac{1}{n}\binom{n}{k+1}\Big(o(\ln n) + o(1)\Big) + o(1) \\ &= o\left(\frac{\ln n}{n}\binom{n}{k+1}\right). \end{aligned}$$

Hence, at $p = (\ln n)/n$, the upper bound (3) is asymptotic to $\binom{n}{t}(\ln n)/n$ for all $t$ such that $2 < n-t = o\big((n\ln\ln n)/\ln n\big)$, which implies that for $2 < n-t = o\big((n\ln\ln n)/\ln n\big)$, the upper bound (3), when minimized over $p$, is $O\big(\binom{n}{t}(\ln n)/n\big)$.

Note that the $O\big(\binom{n}{t}(\ln n)/n\big)$ estimate is not always tight. For example, when $t \approx n - \ln n$, we have shown using a different analysis that the upper bound (3), when minimized over $p$, is in fact $O\big(\ln\ln n)/n\binom{n}{t}\big)$. However, note that by keeping just the $i = t$ term in the sum, the upper bound (3) is at least

$$\begin{aligned} &\left(p + (1-p)^{t(n-t)}\right)\binom{n}{t} \\ &\geq \left(1 - \left(1 - \frac{1}{a}\right) \cdot a^{-1/(a-1)}\right)\binom{n}{t} \\ &= \left[\frac{\ln a}{a} + O\left(\frac{1}{a}\right)\right]\binom{n}{t} \end{aligned}$$

where $a = t(n-t)$. In particular, this shows that the $O\big(\binom{n}{t}(\ln n)/n\big)$ estimate is tight if $n-t$ is $\Theta(1)$. That is, the bound (3) is $\Theta\big(\binom{n}{t}(\ln n)/n\big)$ when minimized over $p$, for all $t = n - \Theta(1)$.

## Acknowledgment

The authors wish to thank Tuvi Etzion for helpful discussions.

## References

[1] Y. Kou, S. Lin, and M. P. C. Fossorier, "Low-density parity-check codes based on finite geometries: A rediscovery and new results," *IEEE Trans. Inf. Theory*, vol. 47, no. 7, pp. 2711–2736, Nov. 2001.

[2] C. Kelley and D. Sridhara, "Pseudocodewords of Tanner graphs," *IEEE Trans. Inf. Theory*, vol. 53, no. 11, pp. 4013–4038, Nov. 2007.

[3] T. Hehn, J. B. Huber, S. Laendner, and O. Milenkovic, "Multiple-bases belief-propagation for decoding of short block codes," in *Proc. IEEE Int. Symp. Information Theory*, Nice, France, Jun. 2007, pp. 311–315.

[4] 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.

[5] 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.

[6] 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.

[7] T. Etzion, "On the stopping redundancy of Reed–Muller codes," *IEEE Trans. Inf. Theory*, vol. 52, no. 11, pp. 4867–4879, Nov. 2006.

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

[9] O. Milenkovic, E. Soljanin, and P. Whiting, "Stopping and trapping sets in generalized covering arrays," in *Proc. 40th Annu. Conf. Information Sciences and Systems (CISS)*, Princeton, NJ, Mar. 2006, pp. 259–264.

[10] T. Hehn, S. Laendner, O. Milenkovic, and J. B. Huber, "The stopping redundancy hierarchy of cyclic codes," in *Proc. 44th Annu. Allerton Conf. Communication, Control and Computing*, Monticello, IL, Sep. 2006, pp. 1271–1280.

[11] K. A. Abdel-Ghaffar and J. H. Weber, "Generalized iterative decoding for linear block codes on the binary erasure channel," in *Proc. IEEE Int. Symp. Information Theory*, Nice, France, Jun. 2007, pp. 66–70.

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

[13] J. H. Weber and K. A. S. Abdel-Ghaffar, "Results on parity-check matrices with optimal stopping and or dead-end set enumerators," *IEEE Trans. Inf. Theory*, vol. 54, no. 3, pp. 1368–1374, Mar. 2008.

[14] H. D. L. Hollmann and L. M. G. M. Tolhuizen, "Generic erasure-correcting sets: Bounds and constructions," *J. Combin. Theory Ser. A*, vol. 113, pp. 1746–1759, Nov. 2006.

[15] 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 given size," *IEEE Trans. Inf. Theory*, vol. 53, no. 2, pp. 823–828, Feb. 2007.

[16] R. C. Singleton, "Maximum distance $q$-nary codes," *IEEE Trans. Inf. Theory*, vol. IT-10, no. 2, pp. 116–118, Apr. 1964.

[17] I. S. Reed and G. Solomon, "Polynomial codes over certain finite fields," *SIAM J. Appl. Math.*, vol. 8, no. 2, pp. 300–304, Jun. 1960.

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

[19] 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.

[20] J. Han and P. H. Siegel, "On the stopping redundancy of MDS codes," in *Proc. IEEE Int. Symp. Information Theory*, Seattle, WA, Jul. 2006, pp. 2491–2495.

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

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

[23] J. Han, P. H. Siegel, and A. Vardy, "Improved probabilistic bounds on stopping redundancy," *IEEE Trans. Inf. Theory*, vol. 54, no. 4, pp. 1749–1753, Apr. 2008.

[24] K. H. Kim and F. W. Roush, "On a problem of Turán," in *Studies in Pure Mathematics: To the Memory of Paul Turán*, P. Erdös, Ed. Basel, Switzerland: Birkhäuser-Verlag, 1983, pp. 423–425.

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

[26] P. Erdös and J. H. Spencer*, Probabilistic Methods in Combinatorics*. New York: Academic, 1974.

[27] N. N. Kuzjurin, "Minimal coverings and maximal coverings of $(k-1)$-subsets by $k$-subsets," *Matematicheskije Zametki*, vol. 21, no. 4, pp. 565–571, Apr. 1977.

[28] J. Schönheim, "On coverings," *Pacific J. Math.*, vol. 14, pp. 1405–1411, 1964.

[29] D. de Caen, "Extension of a theorem of Moon and Moser on complete subgraphs," *Ars Combin.*, vol. 16, pp. 5–10, 1983.

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

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

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

**Junsheng Han** (M'08) received the B.Eng. degree in automation from Tsinghua University, Beijing, China, in 1998, the M.S. degree in electrical engineering from the Ohio State University, Columbus, OH, in 2001, and the Ph.D. degree in electrical engineering from University of California, San Diego, La Jolla, CA, in 2008.

He was with Ericsson Wireless Communications, San Diego, CA, from 2001 to 2003. Since 2008, he has been with Qualcomm Inc., San Diego, where he is currently a Senior Engineer at Corporate R & D. His research interests include coding theory and communications.

**Paul H. Siegel** (M'82–SM'90–F'97) received the S.B. and Ph.D. degrees in mathematics from the Massachusetts Institute of Technology (MIT), Cambridge, in 1975 and 1979, respectively.

He held a Chaim Weizmann Postdoctoral Fellowship at the Courant Institute, New York University. He was with the IBM Research Division in San Jose, CA, from 1980 to 1995. He joined the faculty of the School of Engineering at the University of California, San Diego, in July 1995, where he is currently Professor of Electrical and Computer Engineering. He is affiliated with the California Institute of Telecommunications and Information Technology, the Center for Wireless Communications, and the Center for Magnetic Recording Research, where he holds an endowed chair and currently serves as Director. His primary research interests lie in the areas of information theory and communications, particularly coding and modulation techniques, with applications to digital data storage and transmission.

Prof. Siegel was a member of the Board of Governors of the IEEE Information Theory Society from 1991 to 1996 and was re-elected for a three-year term in 2009. He served as Co-Guest Editor of the May 1991 Special Issue on "Coding for Storage Devices" of the IEEE TRANSACTIONS ON INFORMATION THEORY. He served the same TRANSACTIONS as Associate Editor for Coding Techniques from 1992 to 1995, and as Editor-in-Chief from July 2001 to July 2004. He was also Co-Guest Editor of the May/September 2001 two-part issue on "The Turbo Principle: From Theory to Practice" of the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS. He was corecipient, with R. Karabed, of the 1992 IEEE Information Theory Society Paper Award and shared the 1993 IEEE Communications Society Leonard G. Abraham Prize Paper Award with B. Marcus and J. K. Wolf. With J. B. Soriaga and H. D. Pfister, he received the 2007 Best Paper Award in Signal Processing and Coding for Data Storage from the Data Storage Technical Committee of the IEEE Communications Society. He holds several patents in the area of coding and detection, and was named a Master Inventor at IBM Research in 1994. He is a member of Phi Beta Kappa and the National Academy of Engineering.

**Ron M. Roth** (M'88–SM'97–F'03) was born in Ramat-Gan, Israel, in 1958. He received the B.Sc. degree in computer engineering, the M.Sc. in electrical engineering, and the D.Sc. degree in computer science from Technion–Israel Institute of Technology, Haifa, Israel, in 1980, 1984, and 1988, respectively.

Since 1988, he has been with the Computer Science Department at Technion, where he now holds the General Yaakov Dori Chair in Engineering. During the academic years 1989–1991, he was a Visiting Scientist at IBM Research Division, Almaden Research Center, San Jose, CA, and during 1996–1997 and 2004–2005, he was on sabbatical leave at Hewlett-Packard Laboratories, Palo Alto, CA. He is the author of the book *Introduction to Coding Theory*, published by Cambridge University Press in 2006. His research interests include coding theory, information theory, and their application to the theory of complexity.

Prof. Roth was an Associate Editor for Coding Theory for IEEE TRANSACTIONS ON INFORMATION THEORY from 1998 to 2001, and he is now serving as an Associate Editor for *SIAM Journal on Discrete Mathematics*.