List Decodability at Small Radii

Yeow Meng Chee · Gennian Ge · Lijun Ji · San Ling · Jianxing Yin

Abstract $A'(n,d,e)$, the smallest ℓ for which every binary error-correcting code of length n and minimum distance d is decodable with a list of size ℓ up to radius e, is determined for all $d \geq 2e-3$. As a result, $A'(n,d,e)$ is determined for all $e \leq 4$, except for 42 values of n.

Keywords Bounded-weight codes · Constant-weight codes · Error-correcting codes · List decoding

1 Introduction

If more than $d/2$ errors occur when using a binary error-correcting code of minimum distance d, unambiguous decoding cannot always be guaranteed. Instead of simply letting the decoding algorithm report a failure in this case, *list decoding*, a notion introduced independently by Elias [9] and Wozencraft [23], demands that the decoding algorithm returns

The research of Y. M. Chee and S. Ling is supported in part by the National Research Foundation of Singapore under Research Grant NRF-CRP2-2007-03. The research of Y. M. Chee is also supported in part by the Nanyang Technological University under Research grant M58110040.
The research of G. Ge is supported in part by the National Outstanding Youth Science Foundation of China under Grant 10825103, National Natural Science Foundation of China under Grant 10771193, Specialized Research Fund for the Doctoral Program of Higher Education, Program for New Century Excellent Talents in University, and Zhejiang Provincial Natural Science Foundation of China under Grant D7080064.
The research of L. Ji is supported by NSFC under Grants 10701060, 10831002, and the Qing Lan Project of Jiangsu province.
The research of J. Yin is supported by NSFC under Grants 10831002 and 10671140.

Y. M. Chee · S. Ling
Division of Mathematical Sciences, School of Physical & Mathematical Sciences, Nanyang Technological University, Singapore 637371
E-mail: ymchee@ntu.edu.sg, lingsan@ntu.edu.sg

G. Ge
Department of Mathematics, Zhejiang University, Hangzhou 310027, Zhejiang, China
E-mail: gnge@zju.edu.cn

L. Ji · J. Yin
Department of Mathematics, Suzhou University, Suzhou 215006, Jiangsu, China
E-mail: jilijun@suda.edu.cn, jxyin@suda.edu.cn

a small list of codewords that contains the transmitted codeword, as a weak form of error recovery.

Early applications of list decoding include

(i) tighter analysis of error-probability and error-exponent of probabilistic channels [9, 11, 23],
(ii) derivation of the Elias-Bassalygo bound [2, 19, 20],
(iii) determination of channel capacities [1], and
(iv) error-correction under an adversarial model [3, 4, 10, 24].

Renewed interest in list decoding in theoretical computer science stemmed from the work of Goldreich and Levin [12], and is largely due to the breakthrough discovery by Sudan [22] of the first efficient algorithm for list decoding a nontrivial code. Sudan's work led to a multitude of new applications of list decoding in theoretical computer science and became a powerful tool in complexity theory.

In this paper, we study the list decodability of error-correcting codes. More specifically, we are interested in determining the smallest ℓ so that every error-correcting code of length n and minimum distance d can be list decoded with a list of size ℓ at a given radius e. This parameter, denoted by $A'(n,d,e)$, was investigated by Elias [10] and more recently by Guruswami and Sudan [14] as well as Cassuto and Bruck [8]. These works all focused on giving upper bounds on $A'(n,d,e)$. In contrast, our attention in this paper is on determining the exact value of $A'(n,d,e)$ for specified d and e. More specifically, we determine the exact value of $A'(n,d,e)$ for all $e \leq 4$, except for 42 values of n. A summary of the results obtained is provided in Table 1.

We review some coding-theoretic terminology and notations next.

1.1 Preliminaries

The set of integers $\{1,\ldots,n\}$ is denoted by $[n]$.

Let $\mathbb{F}_2^n$ be the vector space of all the binary n-tuples, endowed with the *Hamming metric*. Specifically, the *Hamming distance* $\Delta(\mathsf{u},\mathsf{v})$ between $\mathsf{u},\mathsf{v} \in \mathbb{F}_2^n$ is defined as the number of positions where u and v differ. The *Hamming weight* $\mathrm{wt}(\mathsf{u})$ of $\mathsf{u} \in \mathbb{F}_2^n$ is its distance from the origin, that is, $\mathrm{wt}(\mathsf{u}) = \Delta(\mathsf{u},0)$. For $\mathsf{u} \in \mathbb{F}_2^n$ and $i \in [n]$, u_i denotes the ith component of u. The *support* $\mathrm{supp}(\mathsf{u})$ of $\mathsf{u} \in \mathbb{F}_2^n$ is the set of positions of u with nonzero value, that is, $\mathrm{supp}(\mathsf{u}) = \{i \in [n] : \mathsf{u}_i = 1\}$.

A *binary code* of length n is a nonempty subset of $\mathbb{F}_2^n$ and its elements are called *codewords*. Since we are concerned with only binary codes in this paper, henceforth we omit the "binary" quantifier throughout. The number of codewords in a code is called its *size*. The *minimum distance* of a code $\mathcal{C}$, denoted $\mathrm{dist}(\mathcal{C})$, is the quantity $\min_{\mathsf{u},\mathsf{v}\in\mathcal{C},\mathsf{u}\neq\mathsf{v}}\{\Delta(\mathsf{u},\mathsf{v})\}$. A code of length n and minimum distance d is denoted an (n,d) code. Given a code $\mathcal{C} \subseteq \mathbb{F}_2^n$, the translate of $\mathcal{C}$ by $\mathsf{u} \in \mathbb{F}_2^n$ is the code $\mathcal{C}+\mathsf{u} = \{\mathsf{v}+\mathsf{u} : \mathsf{v} \in \mathcal{C}\}$, where vector addition is in $\mathbb{F}_2^n$.

A *set system* is a pair $\mathcal{S} = (X,\mathcal{A})$, where X is a finite set of *points* and $\mathcal{A} \subseteq 2^X$. Elements of $\mathcal{A}$ are called *blocks*. The *order* of $\mathcal{S}$ is the number of points, $|X|$. The *size* of $\mathcal{S}$ is the number of blocks in $\mathcal{A}$. The natural bijection between $\mathbb{F}_2^n$ and $2^{[n]}$ (where a vector $\mathsf{u} \in \mathbb{F}_2^n$ corresponds to the set $\mathrm{supp}(\mathsf{u}) \in 2^{[n]}$) implies that a binary code $\mathcal{C}$ of length n can be represented by a set system $\mathcal{S}$ of order n, and vice versa:

$$\mathcal{C} \subseteq \mathbb{F}_2^n \longleftrightarrow ([n], \{\mathrm{supp}(\mathsf{u}) : \mathsf{u} \in \mathcal{C}\}).$$

Table 1 $A'(n,d,e)$, for $1 \le e \le 4$

d \ e	1	2	3	4
1	$\sum_{k=0}^{e}\binom{n}{k}$			
2	$\sum_{k=0}^{e}\binom{n-1}{k}$			
3	1	$\lfloor\frac{n+1}{2}\rfloor$	$\begin{cases}\lfloor\frac{n+1}{3}\lfloor\frac{n}{2}\rfloor\rfloor, & \text{if } n\not\equiv 4 \bmod 6,\ n\notin\{1,3\}\\ \lfloor\frac{(n+1)n}{6}\rfloor-1, & \text{if } n\equiv 4 \bmod 6\\ 2, & \text{if } n=3\\ 1, & \text{if } n=1\end{cases}$	$\begin{cases}\lfloor\frac{n+1}{4}\lfloor\frac{n}{3}\lfloor\frac{n-1}{2}\rfloor\rfloor\rfloor+1, & \text{if } n\not\equiv 5 \bmod 6\\ \lfloor\frac{n+1}{4}\left(\lfloor\frac{n}{3}\lfloor\frac{n-1}{2}\rfloor\rfloor-1\right)\rfloor+1, & \text{if } n\equiv 5 \bmod 6,\end{cases}$ except possibly for $n\in\{22, 34, 46, 58, 70, 82, 94, 118, 142, 154, 166, 178, 190, 202, 214, 274, 286, 454, 466, 478, 958\}$
4		$\lfloor\frac{n}{2}\rfloor$	$\begin{cases}\lfloor\frac{n}{3}\lfloor\frac{n-1}{2}\rfloor\rfloor, & \text{if } n\not\equiv 5 \bmod 6,\ n\notin\{1,2,4\}\\ \lfloor\frac{n(n-1)}{6}\rfloor-1, & \text{if } n\equiv 5 \bmod 6\\ 2, & \text{if } n=4\\ 1, & \text{if } n\in\{1,2\}\end{cases}$	$\begin{cases}\lfloor\frac{n}{4}\lfloor\frac{n-1}{3}\lfloor\frac{n-2}{2}\rfloor\rfloor\rfloor+1, & \text{if } n\not\equiv 0 \bmod 6\\ \lfloor\frac{n}{4}\left(\lfloor\frac{n-1}{3}\lfloor\frac{n-2}{2}\rfloor\rfloor-1\right)\rfloor+1, & \text{if } n\equiv 0 \bmod 6,\end{cases}$ except possibly for $n\in\{23, 35, 47, 59, 71, 83, 95, 119, 143, 155, 167, 179, 191, 203, 215, 275, 287, 455, 467, 479, 959\}$
5		1	$\lfloor\frac{n+1}{3}\rfloor$	$\begin{cases}\lfloor\frac{(n+1)n}{12}\rfloor-1, & \text{if } n\equiv 6,9 \bmod 12,\ n\notin\{9,18\}\\ \lfloor\frac{n+1}{4}\lfloor\frac{n}{3}\rfloor\rfloor, & \text{if } n\not\equiv 6,9 \bmod 12,\ n\notin\{7,8,10,16\}\\ 25, & \text{if } n=18\\ \lfloor\frac{n+1}{4}\lfloor\frac{n}{3}\rfloor\rfloor-1, & \text{if } n\in\{8,16\}\\ \lfloor\frac{n+1}{4}\lfloor\frac{n}{3}\rfloor\rfloor-2, & \text{if } n\in\{7,9,10\}\end{cases}$
6			$\lfloor\frac{n}{3}\rfloor$	$\begin{cases}\lfloor\frac{n(n-1)}{12}\rfloor-1, & \text{if } n\equiv 7,10 \bmod 12,\ n\notin\{10,19\}\\ \lfloor\frac{n}{4}\lfloor\frac{n-1}{3}\rfloor\rfloor, & \text{if } n\not\equiv 7,10 \bmod 12,\ n\notin\{8,9,11,17\}\\ 25, & \text{if } n=19\\ \lfloor\frac{n}{4}\lfloor\frac{n-1}{3}\rfloor\rfloor-1, & \text{if } n\in\{9,17\}\\ \lfloor\frac{n}{4}\lfloor\frac{n-1}{3}\rfloor\rfloor-2, & \text{if } n\in\{8,10,11\}\end{cases}$
7			1	$\lfloor\frac{n+1}{4}\rfloor$
8				$\lfloor\frac{n}{4}\rfloor$
9				1

Hence, we may speak of the set system of a binary code. When more natural, we deal with the set system of a binary code, rather than the binary code itself.

The *Hamming ball* of radius r around u is the set

$$B(\mathsf{u},r) = \{\mathsf{v} \in \mathbb{F}_2^n : \Delta(\mathsf{u},\mathsf{v}) \leq r\}.$$

For a code $\mathcal{C} \subseteq \mathbb{F}_2^n$, the quantity $e = \lfloor (\mathrm{dist}(\mathcal{C})-1)/2 \rfloor$ is referred to as the *error-correction bound* of $\mathcal{C}$ [22]. This terminology reflects that given any $\mathsf{u} \in \mathbb{F}_2^n$,

$$|B(\mathsf{u},e) \cap \mathcal{C}| \leq 1,$$

so that any transmitted codeword corrupted by at most e errors can be unambiguously decoded (to the nearest codeword) with maximum likelihood decoding. If the number of errors is beyond the error-correction bound, we may not always be able to decode to a unique codeword. However, it is desirable that in this case, the decoding algorithm outputs a list of candidate codewords, containing the transmitted codeword. This motivates the definition of list decodable codes.

For positive integers e and ℓ, a code $\mathcal{C} \subseteq \mathbb{F}_2^n$ is (e,ℓ)-*list decodable* if every ball of radius e contains at most ℓ codewords, that is,

$$|B(\mathsf{u},e) \cap \mathcal{C}| \leq \ell, \text{ for all } \mathsf{u} \in \mathbb{F}_2^n.$$

2 The Function $A'(n,d,e)$

The key function we study in this paper is $A'(n,d,e)$, defined to be the maximum size of a set $S \subseteq \mathbb{F}_2^n$ contained in a ball of radius e such that $\Delta(\mathsf{u},\mathsf{v}) \geq d$ for all distinct $\mathsf{u},\mathsf{v} \in S$. More formally,

$$A'(n,d,e) = \max\{|S| : S \text{ is an } (n,d) \text{ code, and } S \subseteq B(\mathsf{x},e) \text{ for some } \mathsf{x} \in \mathbb{F}_2^n\}. \qquad (1)$$

Notice that translating a code does not affect its distance properties. Hence we may assume that the maximum in (1) is attained when $\mathsf{x} = 0$. The definition of $A'(n,d,e)$ can then take the following equivalent form:

$$A'(n,d,e) = \max\{|S| : S \text{ is an } (n,d) \text{ code, and } \mathrm{wt}(\mathsf{u}) \leq e \text{ for all } \mathsf{u} \in S\}.$$

We call an (n,d) code having codewords of weight at most e an (n,d,e) *bounded-weight code*. Hence, determining $A'(n,d,e)$ is equivalent to determining the maximum size of an (n,d,e) bounded-weight code. An (n,d,e) bounded-weight code of size $A'(n,d,e)$ is said to be *optimal*.

In contrast, an (n,d,e) *constant-weight code* is an (n,d) code whose codewords are all of weight e. The maximum size of an (n,d,e) constant-weight code is denoted $A(n,d,e)$. The determination of $A(n,d,e)$ has been a central problem in coding theory, with a rich literature (see, for example, [7]). The importance of the function $A'(n,d,e)$ is only realized relatively recently [13], due to the following observation.

Proposition 1

(i) If $\ell \geq A'(n,d,e)$, then every (n,d) code is (e,ℓ)-list decodable.
(ii) If $\ell < A'(n,d,e)$, then there exists an (n,d) code that is not (e,ℓ)-list decodable.

Proof Suppose $\mathcal{C}$ is an (n,d) code. Then $|B(\mathsf{u},e)\cap\mathcal{C}|\leq A'(n,d,e)$ for all $\mathsf{u}\in\mathbb{F}_2^n$. It follows that if $\ell\geq A'(n,d,e)$, then $\mathcal{C}$ is (e,ℓ)-list decodable. If $\ell<A'(n,d,e)$, then an (n,d,e) bounded-weight code of size $A'(n,d,e)$ is an (n,d) code that is not (e,ℓ)-list decodable. □

Consequently, the problem of determining $A'(n,d,e)$ has attracted some direct attention [8,10,13,14]. The determination of the exact value of $A'(n,d,e)$ is no doubt a difficult problem, so most work has gone to establishing upper bounds on $A'(n,d,e)$. Proposition 1(i) can be applied when an upper bound of $A'(n,d,e)$ is known. However, this is not true for Proposition 1(ii). So we do not get as strong a conclusion as if we know the exact value of $A'(n,d,e)$. A useful result proven by Elias [10] is the following:

Proposition 2 (Elias [10, Proposition 10(c)]) *If d is odd, then $A'(n,d,e)=A'(n+1,d+1,e)$.*

In subsequent sections, we determine the value of $A'(n,d,e)$ for several parameter sets. We end this section with some easy exact values.

Proposition 3

(i) *If $d\geq 2e+1$, then $A'(n,d,e)=1$.*
(ii) *If $d=2e$, then $A'(n,d,e)=\lfloor n/e\rfloor$.*
(iii) *If $d=2e-1$, then $A'(n,d,e)=\lfloor (n+1)/e\rfloor$.*
(iv) *If $d=2$, then $A'(n,d,e)=\sum_{k=0}^{e}\binom{n-1}{k}$.*
(v) *If $d=1$, then $A'(n,d,e)=\sum_{k=0}^{e}\binom{n}{k}$.*

Proof (i) Since $\Delta(\mathsf{u},\mathsf{v})\leq \mathrm{wt}(\mathsf{u})+\mathrm{wt}(\mathsf{v})\leq 2e$, there can be at most one codeword in the code.
(ii) Follows from the observation that all the codewords must have weight e and have disjoint supports.
(iii) Follows from part (ii) and Proposition 2.
(iv) Follows from part (v) and Proposition 2.
(v) Taking all binary n-tuples of weight e or less gives the required code of distance one.
□

Proposition 3 can be used to completely determine the exact value of $A'(n,d,1)$.

Corollary 1

$$A'(n,d,1)=\begin{cases}1, & \text{if } d\geq 3\\ n, & \text{if } d=2\\ n+1, & \text{if } d=1.\end{cases}$$

3 Determining $A'(n,2e-2,e)$ and $A'(n,2e-3,e)$

By Proposition 2, we have $A'(n,2e-2,e)=A'(n-1,2e-3,e)$, so it suffices to focus on the case $d=2e-2$ in this section. When $d=2e-2$, $A'(n,d,e)$ can be expressed in terms of $A(n,d,e)$.

Proposition 4 *When $d=2e-2$,*

$$A'(n,d,e)=\max_{\substack{\alpha\in\{0,1\}\\ 0\leq\beta\leq\frac{n}{e-1}\\ \alpha\beta=0}}\{\alpha+\beta+A(n-\alpha(e-2)-\beta(e-1),d,e)\}.$$

Proof By considering the distance between codewords, we see that an $(n, 2e-2, e)$ bounded-weight code $\mathcal{C}$ must satisfy:

(i) $\mathrm{wt}(\mathsf{u}) \geq e-2$ for all $\mathsf{u} \in \mathcal{C}$;
(ii) there exists at most one $\mathsf{u} \in \mathcal{C}$ such that $\mathrm{wt}(\mathsf{u}) = e-2$;
(iii) if there exists $\mathsf{u} \in \mathcal{C}$ such that $\mathrm{wt}(\mathsf{u}) = e-2$, then there do not exist any $\mathsf{v} \in \mathcal{C}$ such that $\mathrm{wt}(\mathsf{v}) = e-1$.

Let $\alpha \in \{0,1\}$ be the number of codewords in $\mathcal{C}$ of weight $e-2$, and let $0 \leq \beta \leq n/(e-1)$ be the number of codewords in $\mathcal{C}$ of weight $e-1$. Note that $\alpha\beta = 0$ by property (iii) above. The supports of these $\alpha+\beta$ codewords of weight $e-2$ and $e-1$ are pairwise disjoint, and are also pairwise disjoint from those of codewords of weight e. Hence, if we shorten $\mathcal{C}$ at the positions containing nonzero values among these $\alpha+\beta$ codewords, we end up with an $(n-\alpha(e-2)-\beta(e-1), 2e-2, e)$ constant-weight code. It follows that

$$A'(n,2e-2,e) = \max_{\substack{\alpha\in\{0,1\} \\ 0\leq\beta\leq\frac{n}{e-1} \\ \alpha\beta=0}} \{\alpha+\beta+A(n-\alpha(e-2)-\beta(e-1),2e-2,e)\}.$$

□

Hence, for any fixed e, we can determine $A'(n,2e-2,e)$ whenever the exact value of $A(n,2e-2,e)$ is known for all n. The following are classical results from the theory of constant-weight codes.

Theorem 1 (Schönheim [18], Spencer[21], Brouwer [6])

(i)

$$A(n,4,3) = \begin{cases} \left\lfloor \frac{n}{3} \left\lfloor \frac{n-1}{2} \right\rfloor \right\rfloor - 1, & \text{if } n \equiv 5 \bmod 6 \\ \left\lfloor \frac{n}{3} \left\lfloor \frac{n-1}{2} \right\rfloor \right\rfloor, & \text{otherwise.} \end{cases}$$

(ii)

$$A(n,6,4) = \begin{cases} \left\lfloor \frac{n}{4} \left\lfloor \frac{n-1}{3} \right\rfloor \right\rfloor - 1, & \text{if } n \equiv 7,10 \bmod 12 \text{ and } n \notin \{10,19\} \\ \left\lfloor \frac{n}{4} \left\lfloor \frac{n-1}{3} \right\rfloor \right\rfloor - 1, & \text{if } n \in \{9,17\} \\ \left\lfloor \frac{n}{4} \left\lfloor \frac{n-1}{3} \right\rfloor \right\rfloor - 2, & \text{if } n \in \{8,10,11\} \\ \left\lfloor \frac{n}{4} \left\lfloor \frac{n-1}{3} \right\rfloor \right\rfloor - 3, & \text{if } n = 19 \\ \left\lfloor \frac{n}{4} \left\lfloor \frac{n-1}{3} \right\rfloor \right\rfloor, & \text{otherwise.} \end{cases}$$

Note that $A(n,d-1,e) = A(n,d,e)$ when d is even, so results on $A(n,d,e)$ are normally stated only for even d.

Corollary 2 *For n a positive integer, $A'(n,4,3) = A(n,4,3)$, except when $n \in \{1,2,4\}$, in which case, we have $A'(1,4,3) = A'(2,4,3) = 1$ and $A'(4,4,3) = 2$.*

Proof The values of $A'(n,4,3)$ are trivial to obtain when $n \leq 4$, so we assume henceforth that $n \geq 5$. From Proposition 4 and Theorem 1(ii), we have

$$\begin{aligned} A'(n,4,3) &= \max_{\substack{\alpha\in\{0,1\} \\ 0\leq\beta\leq n/2 \\ \alpha\beta=0}} \{\alpha+\beta+A(n-\alpha-2\beta,4,3)\} \\ &= \max_{0\leq\beta\leq n/2} \{\beta+A(n-2\beta,4,3), 1+A(n-1,4,3)\}. \end{aligned}$$

First, note that since $n \geq 5$, we have $1 + A(n-1,4,3) \leq A(n,4,3)$.

Now, take any $(n,4,3)$ bounded-weight code $\mathcal{C}$ attaining the bound $\beta + A(n-2\beta,4,3)$, that is, $\mathcal{C}$ contains β codewords of weight two and then outside the supports of these codewords of weight two, $\mathcal{C}$ contains the remaining codewords of weight three. Without loss of generality, assume that the last coordinate position does not belong to any of the supports of the codewords of weight two. We consider two cases:

$2\beta \neq n$: Change the last coordinate (from zero to one) in every codeword of weight two in $\mathcal{C}$ to obtain a new code $\mathcal{C}'$. Clearly, the distances between the codewords in $\mathcal{C}'$ obtained from those of weight two in $\mathcal{C}$ are unaffected, and remain at least four. The distances between codewords of weight two and codewords of weight three in $\mathcal{C}$ are all five, so the distances between codewords in $\mathcal{C}'$ obtained from codewords of weight two in $\mathcal{C}$ and the other codewords in $\mathcal{C}$ are all at least four. Therefore, $\mathcal{C}'$ is an $(n,4,3)$ constant-weight code, and hence its size can never exceed $A(n,4,3)$. Since $|\mathcal{C}| = |\mathcal{C}'|$, we also have $|\mathcal{C}| \leq A(n,4,3)$. Furthermore, equality holds when $\beta = 0$.

$2\beta = n$: In this case, $\beta + A(n-2\beta,4,3) = n/2 + A(0,4,3) \leq A(n,4,3)$ when $n \geq 6$.

It follows that $A'(n,4,3) = A(n,4,3)$ when $n \geq 5$. □

We skip the proof for Corollary 3 below as it is similar to that for Corollary 2.

Corollary 3 *$A'(n,6,4) = A(n,6,4)$ for all positive integers n, except when $n \in \{1,2,3,6\}$, in which case, we have $A'(n,6,4) = 1$ for $n \in \{1,2,3\}$ and $A'(6,6,4) = 2$.*

We end this section by giving the exact value of $A'(n,d,2)$ and $A'(n,d,3)$.

Theorem 2

$$A'(n,d,2) = \begin{cases} 1, & \text{if } d \geq 5 \\ \lfloor n/2 \rfloor, & \text{if } d = 4 \\ \lfloor (n+1)/2 \rfloor, & \text{if } d = 3 \\ \binom{n}{2} + 1, & \text{if } d = 2 \\ \binom{n}{2} + n + 1, & \text{if } d \leq 1. \end{cases}$$

Proof The value of $A'(n,d,2)$ follows from Proposition 3. □

Theorem 3 *When $(n,d) \notin \{(1,3), (1,4), (2,4), (3,3), (4,4)\}$, we have*

$$A'(n,d,3) = \begin{cases} 1, & \text{if } d \geq 7 \\ \lfloor n/3 \rfloor, & \text{if } d = 6 \\ \lfloor (n+1)/3 \rfloor, & \text{if } d = 5 \\ \left\lfloor \frac{n}{3} \left\lfloor \frac{n-1}{2} \right\rfloor \right\rfloor, & \text{if } d = 4,\ n \not\equiv 5 \bmod 6,\ n \notin \{1,2,4\} \\ \left\lfloor \frac{n(n-1)}{6} \right\rfloor - 1, & \text{if } d = 4,\ n \equiv 5 \bmod 6 \\ \left\lfloor \frac{n+1}{3} \left\lfloor \frac{n}{2} \right\rfloor \right\rfloor, & \text{if } d = 3,\ n \not\equiv 4 \bmod 6,\ n \notin \{1,3\} \\ \left\lfloor \frac{(n+1)n}{6} \right\rfloor - 1, & \text{if } d = 3,\ n \equiv 4 \bmod 6 \\ \sum_{k=0}^{3} \binom{n-1}{k}, & \text{if } d = 2 \\ \sum_{k=0}^{3} \binom{n}{k}, & \text{if } d \leq 1. \end{cases}$$

The remaining values are given by

$$A'(1,3,3) = A'(1,4,3) = A'(2,4,3) = 1,$$
$$A'(3,3,3) = A'(4,4,3) = 2.$$

Table 2 Elements of $\mathcal{N}$, the possible exceptions to $A(n,4,4) = J(n,4,4)$

23	35	47	59	71	83	95	119	143	155	167
179	191	203	215	275	287	455	467	479	959	

Proof The value of $A'(n,d,3)$ for $d \geq 5$ and $d \leq 2$ follows from Proposition 3, and for $d = 4$ follows from Corollary 2. The remaining required value of $A'(n,3,3)$ follows by applying Proposition 2 to Corollary 2. □

4 Determining $A'(n,4,4)$

We consider the case $e = 4$ and $d = 4$ in this section, since $A'(n,d,e)$ has already been determined for all $e \leq 3$ in Corollary 1, Theorem 2 and Theorem 3, and for $e = 4$ and $d = 6$ (and hence also $d = 5$) in Corollary 3. The main result in this section is that $A'(n,4,4) = A(n,4,4) + 1$ for all sufficiently large n.

Let

$$J(n,4,4) = \begin{cases} \left\lfloor \frac{n}{4} \left\lfloor \frac{n-1}{3} \left\lfloor \frac{n-2}{2} \right\rfloor \right\rfloor \right\rfloor, & \text{if } n \not\equiv 0 \bmod 6 \\ \left\lfloor \frac{n}{4} \left(\left\lfloor \frac{n-1}{3} \left\lfloor \frac{n-2}{2} \right\rfloor \right\rfloor - 1 \right) \right\rfloor, & \text{if } n \equiv 0 \bmod 6. \end{cases}$$

The following bound was obtained by Johnson [17]:

$$A(n,4,4) \leq J(n,4,4). \tag{2}$$

With recent advances, the value of $A(n,4,4)$ is now known for all but the values of $n \in \mathcal{N}$, where $\mathcal{N}$ is the set of 21 numbers in Table 2.

Theorem 4 (Hanani [15], Brouwer [5], Ji [16]) *$A(n,4,4) = J(n,4,4)$ for all positive integers n, except possibly for $n \in \mathcal{N}$.*

Throughout this section, $\mathcal{C}$ is an $(n,4,4)$ bounded-weight code and $\mathcal{S} = ([n],\mathcal{A})$ is the set system of $\mathcal{C}$. Note that taking an optimal $(n,4,4)$ constant-weight code together with the zero-weight codeword yields an $(n,4,4)$ bounded-weight code of size $A(n,4,4)+1$. Therefore,

$$A'(n,4,4) \geq A(n,4,4) + 1 = J(n,4,4) + 1. \tag{3}$$

To establish that the inequality in (3) is indeed an equality, we show below that $A'(n,4,4) \leq J(n,4,4)+1$. We do this by case analysis on the number of codewords of weight k in $\mathcal{C}$, and counting.

Let m_k, $k \in \{0,1,2,3,4\}$, denote the number of blocks of size k in $\mathcal{A}$. If $\mathcal{A}$ contains the empty set as a block, then all other blocks of $\mathcal{A}$ must have size four, and hence the size of $\mathcal{S}$ in this case is at most $A(n,4,4)+1$. Henceforth, assume $m_0 = 0$.

Clearly, $m_1 \in \{0,1\}$, since $\mathcal{C}$ has minimum distance four. If $m_1 = 1$ and $A = \{x\}$ is a block in $\mathcal{A}$, then x cannot be contained in any other block of $\mathcal{A}$, and moreover all other blocks of $\mathcal{A}$ must have size three or four. Hence, it follows that the size of $\mathcal{S}$ in this case is at most one more than the largest size of an $(n-1,4,4)$ bounded-weight code with only codewords of size three and four. We can therefore restrict our attention to the case when $m_1 = 0$.

For $T \subseteq [n]$ and $k \in \{2,3,4\}$, let $f_k(T)$ denote the number of blocks of size k in $\mathcal{A}$ that contain T. For succinctness of notation, we suppress braces in the argument of f_k so that, for example, we write $f_k(x)$ for $f_k(\{x\})$ and $f_k(x,y)$ for $f_k(\{x,y\})$. Define, for $k \in \{2,3\}$,

$$D_k = \{x \in [n] : f_k(x) > 0\}.$$

Then $D_2 \cap D_3 = \emptyset$, since $\mathrm{dist}(\mathcal{C}) = 4$. Let $D_4 = [n] \setminus (D_2 \cup D_3)$.

The following equations are obtained by counting points in the blocks of $\mathcal{A}$:

$$\sum_{x \in D_2} f_2(x) = 2m_2, \tag{4}$$

$$\sum_{x \in D_3} f_3(x) = 3m_3, \tag{5}$$

$$\sum_{x \in [n]} f_4(x) = 4m_4. \tag{6}$$

We also have the inequality

$$f_2(x,y) + f_3(x,y) \leq 1,$$

for $\{x,y\} \subseteq [n]$. If $f_2(x,y) + f_3(x,y) = 1$, then $f_4(x,y) = 0$. Otherwise, we have the following.

Lemma 1 *Let $\{x,y\} \subseteq [n]$. If $f_2(x,y) + f_3(x,y) = 0$, then*

$$f_4(x,y) \leq \begin{cases} \left\lfloor \frac{n-4}{2} \right\rfloor, & \text{if } x \in D_2 \text{ and } y \in D_2 \\ \left\lfloor \frac{n-3-2f_3(y)}{2} \right\rfloor, & \text{if } x \in D_2 \text{ and } y \in D_3 \\ \left\lfloor \frac{n-3}{2} \right\rfloor, & \text{if } x \in D_2 \text{ and } y \in D_4 \\ \left\lfloor \frac{n-2-2f_3(x)-2f_3(y)}{2} \right\rfloor, & \text{if } x \in D_3 \text{ and } y \in D_3 \\ \left\lfloor \frac{n-2-2f_3(x)}{2} \right\rfloor, & \text{if } x \in D_3 \text{ and } y \in D_4 \\ \left\lfloor \frac{n-2}{2} \right\rfloor, & \text{if } x \in D_4 \text{ and } y \in D_4. \end{cases}$$

Proof First note that the blocks of size four containing $\{x,y\}$ have pairwise intersection exactly $\{x,y\}$, so that the number of such blocks is at most $\lfloor (n-2-|E|)/2 \rfloor$, where $E \subseteq [n] \setminus \{x,y\}$ is a set of points that must be excluded in any blocks of size four containing $\{x,y\}$.

(i) When $x \in D_2$ and $y \in D_2$, suppose that the two blocks of size two containing x and y, respectively, are $\{x,a\}$ and $\{y,b\}$. Then taking $E = \{a,b\}$ gives $f_4(x,y) \leq \lfloor (n-4)/2 \rfloor$.

(ii) When $x \in D_2$ and $y \in D_3$, suppose that the block of size two containing x is $\{x,a\}$, and the blocks of size three containing y are $\{y,b_i,c_i\}$, $i = 1,\ldots,f_3(y)$. Then taking $E = \{a,b_i,c_i : i = 1,\ldots,f_3(y)\}$ gives

$$f_4(x,y) \leq \lfloor (n-3-2f_3(y))/2 \rfloor.$$

(iii) When $x \in D_2$ and $y \in D_4$, suppose that the block of size two containing x is $\{x,a\}$. Then taking $E = \{a\}$ gives $f_4(x,y) \leq \lfloor (n-3)/2 \rfloor$.

(iv) When $x \in D_3$ and $y \in D_3$, suppose that the blocks of size three containing x and the blocks of size three containing y are $\{x,a_i,b_i\}$, $i = 1,\ldots,f_3(x)$, and $\{y,c_i,d_i\}$, $i = 1,\ldots,f_3(y)$, respectively. Then taking $E = \{a_i,b_i : i = 1,\ldots,f_3(x)\} \cup \{c_i,d_i : i = 1,\ldots,f_3(y)\}$ gives

$$f_4(x,y) \leq \lfloor (n-2-2f_3(x)-2f_3(y))/2 \rfloor.$$

(v) When $x \in D_3$ and $y \in D_4$, suppose that the blocks of size three containing x are $\{x, a_i, b_i\}$, $i = 1, \ldots, f_3(x)$. Then taking $E = \{a_i, b_i : i = 1, \ldots, f_3(x)\}$ gives $f_4(x,y) \leq \lfloor (n-2-2f_3(x))/2 \rfloor$.

(vi) When $x \in D_4$ and $y \in D_4$, taking $E = \emptyset$ gives $f_4(x,y) \leq \lfloor (n-2)/2 \rfloor$. □

Counting in two ways the number of 2-subsets $T \subseteq [n]$ containing the point x such that T is contained in a block of size four gives

$$3f_4(x) = \sum_{y \in [n] \setminus \{x\}} f_4(x,y), \tag{7}$$

since each block of size four contains three 2-subsets, each of which contains x.

Applying the inequality on $f_4(x,y)$ in Lemma 1 to (7), and recalling that if $f_2(x,y) + f_3(x,y) = 1$ then $f_4(x,y) = 0$, gives the inequality

$$3f_4(x) \leq \begin{cases} (|D_2|-2)\left\lfloor \frac{n-4}{2} \right\rfloor + |D_3|\left\lfloor \frac{n-5}{2} \right\rfloor + (n-|D_2|-|D_3|)\left\lfloor \frac{n-3}{2} \right\rfloor, & \text{if } x \in D_2 \\ |D_2|\left\lfloor \frac{n-5}{2} \right\rfloor + (|D_3|-1-2f_3(x))\left\lfloor \frac{n-6}{2} \right\rfloor + (n-|D_2|-|D_3|)\left\lfloor \frac{n-4}{2} \right\rfloor, & \text{if } x \in D_3 \\ |D_2|\left\lfloor \frac{n-3}{2} \right\rfloor + |D_3|\left\lfloor \frac{n-4}{2} \right\rfloor + (n-1-|D_2|-|D_3|)\left\lfloor \frac{n-2}{2} \right\rfloor, & \text{if } x \in D_4. \end{cases} \tag{8}$$

We are now ready to establish upper bounds on the size of $\mathcal{S}$ when $m_0 = m_1 = 0$. By (4)–(6),

$$\begin{aligned} |\mathcal{A}| &= m_2 + m_3 + m_4 \\ &= \frac{1}{2}\sum_{x \in D_2} f_2(x) + \frac{1}{3}\sum_{x \in D_3} f_3(x) + \frac{1}{4}\sum_{x \in [n]} f_4(x) \\ &= \frac{1}{2}\sum_{x \in D_2} f_2(x) + \frac{1}{3}\sum_{x \in D_3} f_3(x) + \frac{1}{4}\left(\sum_{x \in D_2} f_4(x) + \sum_{x \in D_3} f_4(x) + \sum_{x \in D_4} f_4(x)\right) \\ &= \frac{1}{4}\left(\sum_{x \in D_2} (2f_2(x) + f_4(x)) + \sum_{x \in D_3}\left(\frac{4}{3}f_3(x) + f_4(x)\right) + \sum_{x \in D_4} f_4(x)\right). \end{aligned}$$

Let

$$\begin{aligned} F_2(x) &= 2f_2(x) + f_4(x), \\ F_3(x) &= \frac{4}{3}f_3(x) + f_4(x), \\ F_4(x) &= f_4(x), \end{aligned}$$

so that

$$|\mathcal{A}| = \frac{1}{4}\left(\sum_{x \in D_2} F_2(x) + \sum_{x \in D_3} F_3(x) + \sum_{x \in D_4} F_4(x)\right). \tag{9}$$

4.1 $n \equiv 1 \bmod 2$

In this subsection, we consider the case when n is odd.

An upper bound on $F_2(x) = 2f_2(x) + f_4(x)$ can be obtained by observing that there can be at most one block of size two containing x (and hence $f_2(x) \leq 1$), and applying (8) to upper bound $f_4(x)$. More specifically, when $x \in D_2$, we have

$$\begin{aligned}
F_2(x) &= 2f_2(x) + f_4(x) \\
&\leq 2 + \frac{1}{3}\left((|D_2|-2)\left\lfloor \frac{n-4}{2} \right\rfloor + |D_3|\left\lfloor \frac{n-5}{2} \right\rfloor + (n-|D_2|-|D_3|)\left\lfloor \frac{n-3}{2} \right\rfloor \right) \\
&= 2 + \frac{1}{3}\left((|D_2|-2)\cdot\frac{n-5}{2} + |D_3|\cdot\frac{n-5}{2} + (n-|D_2|-|D_3|)\cdot\frac{n-3}{2} \right) \\
&= \frac{n^2-5n-2D_2-2D_3-22}{6} \\
&= \frac{n-1}{3}\cdot\frac{n-3}{2} - \frac{n+2|D_2|+2|D_3|-19}{6}.
\end{aligned}$$

Since $F_2(x)$ is an integer, we have

$$F_2(x) \leq \left\lfloor \frac{n-1}{3}\cdot\frac{n-3}{2} - \frac{n+2|D_2|+2|D_3|-19}{6} \right\rfloor, \quad \text{when } x \in D_2.$$

We can similarly derive

$$\begin{aligned}
F_3(x) &\leq \left\lfloor \frac{n-1}{3}\cdot\frac{n-3}{2} - \frac{n+|D_3|-2+(n-11)f_3(x)}{3} \right\rfloor, \quad \text{when } x \in D_3, \\
F_4(x) &\leq \left\lfloor \frac{n-1}{3}\cdot\frac{n-3}{2} - \frac{|D_3|}{3} \right\rfloor, \quad \text{when } x \in D_4.
\end{aligned}$$

If $|D_2| \neq 0$ (that is $|D_2| \geq 2$), then $\frac{n+2|D_2|+2|D_3|-19}{6} \geq -2/3$ when $n \geq 11$, so that $F_2(x) \leq \left\lfloor \frac{n-1}{3}\cdot\frac{n-3}{2} \right\rfloor$ for $n \geq 11$.

If $|D_3| \neq 0$ and $x \in D_3$, then $|D_3| \geq 2f_3(x)+1$ since in each block of size three, x appears with two other points, and these points are all distinct. In this case, $n+|D_3|-2+(n-11)f_3(x) \geq 0$ when $n \geq 9$, so that $F_3(x) \leq \left\lfloor \frac{n-1}{3}\cdot\frac{n-3}{2} \right\rfloor$ for $n \geq 9$.

Hence, when $|D_2| \neq 0$ or $|D_3| \neq 0$, each of $F_2(x)$, $F_3(x)$, and $F_4(x)$ is at most $\left\lfloor \frac{n-1}{3}\cdot\frac{n-3}{2} \right\rfloor$ for $n \geq 11$. It follows from (9) that

$$\begin{aligned}
|\mathcal{A}| &\leq \frac{1}{4}\sum_{x\in[n]} \left\lfloor \frac{n-1}{3}\cdot\frac{n-3}{2} \right\rfloor \\
&= \left\lfloor \frac{n}{4}\left\lfloor \frac{n-1}{3}\left\lfloor \frac{n-2}{2} \right\rfloor \right\rfloor \right\rfloor = J(n,4,4).
\end{aligned}$$

We summarize the results in this section as:

Proposition 5 *When $n \equiv 1 \bmod 2$, $n \geq 11$, an optimal $(n,4,4)$ bounded-weight code $\mathcal{C}$ has $|D_2| = |D_3| = 0$, that is, $\mathcal{C}$ contains no codewords of weight two and weight three, except possibly for $n \in \{23, 35, 47, 59, 71, 83, 95, 119, 143, 155, 167, 179, 191, 203, 215, 275, 287, 455, 467, 479, 959\}$.*

4.2 $n \equiv 2$ or 4 mod 6

In this subsection, we consider the case when $n \equiv 2$ or 4 mod 6.

Using (8) and simplifying gives, when $x \in D_2$:

$$F_2(x) \leq \left\lfloor \frac{n-1}{3} \cdot \frac{n-2}{2} - \frac{3n+2|D_3|-18}{6} \right\rfloor,$$

when $x \in D_3$:

$$F_3(x) \leq \left\lfloor \frac{n-1}{3} \cdot \frac{n-2}{2} - \frac{n+|D_2|+|D_3|-2+(n-10)f_3(x)}{3} \right\rfloor,$$

and when $x \in D_4$:

$$F_4(x) \leq \left\lfloor \frac{n-1}{3} \cdot \frac{n-2}{2} - \frac{|D_2|+|D_3|}{3} \right\rfloor.$$

If $|D_2| \neq 0$, then since $3n+2|D_3|-18 \geq 0$ when $n \geq 6$, we have $F_2(x) \leq \lfloor \frac{n-1}{3} \cdot \frac{n-2}{2} \rfloor$ for $n \geq 6$.

If $|D_3| \neq 0$, then $|D_3| \geq 2f_3(x)+1$, giving $n+|D_2|+|D_3|-2+(n-10)f_3(x) \geq 0$ when $n \geq 8$, so that $F_3(x) \leq \lfloor \frac{n-1}{3} \cdot \frac{n-2}{2} \rfloor$ for $n \geq 8$.

As in subsection 4.1, we deduce the following:

Proposition 6 *When $n \equiv 2$ or 4 mod 6, $n \geq 8$, an optimal $(n,4,4)$ bounded-weight code $\mathcal{C}$ has $|D_2| = |D_3| = 0$, that is, $\mathcal{C}$ contains no codewords of weight two and weight three.*

4.3 $n \equiv 0$ mod 6

Here, the remaining case of $n \equiv 0$ mod 6 is addressed. First note that

$$\left\lfloor \frac{n-1}{3} \left\lfloor \frac{n-2}{2} \right\rfloor \right\rfloor - 1 = \frac{n^2-3n-6}{6}.$$

Using (8) and simplifying gives, when $x \in D_2$:

$$F_2(x) \leq \left\lfloor \frac{n^2-3n-6}{6} - \frac{3n+2|D_3|-26}{6} \right\rfloor,$$

when $x \in D_3$:

$$F_3(x) \leq \left\lfloor \frac{n^2-3n-6}{6} - \frac{n+|D_2|+|D_3|-6+(n-10)f_3(x)}{3} \right\rfloor,$$

and when $x \in D_4$:

$$F_4(x) \leq \left\lfloor \frac{n^2-3n-6}{6} - \frac{|D_2|+|D_3|-4}{3} \right\rfloor.$$

If $|D_2| \neq 0$, then since $3n+2|D_3|-26 \geq 0$ when $n \geq 9$, we have $F_2(x) \leq \frac{n^2-3n-6}{6}$ for $n \geq 9$.

If $|D_3| \neq 0$, then $|D_3| \geq 2f_3(x)+1$, giving $n+|D_2|+|D_3|-6+(n-10)f_3(x) \geq 0$ when $n \geq 8$, so that $F_3(x) \leq \frac{n^2-3n-6}{6}$ for $n \geq 8$.

If $|D_2 \cup D_3| \neq 0$, then $|D_2 \cup D_3| \geq 2$, and hence $F_4(x) \leq \left\lfloor \frac{n^2-3n-6}{6} - \frac{|D_2|+|D_3|-4}{3} \right\rfloor \leq \frac{n^2-3n-6}{6}$.

We therefore have:

Table 3 Some Optimal $(n,4,4)$ Bounded-Weight Codes

n	Codewords
6	111000 100101 010110 001011
7	0000000 1110010 1101001 1010101 1001110 0111100 0100111 0011011
9	000000000 111010000 110100100 110001001 101100001 101000110 100101010 100011100 100010011 011100010 011001100 010110001 010011010 010000111 001111000 001010101 001001011 000110110 000101101

Proposition 7 *When $n \equiv 0 \bmod 6$, $n \geq 12$, an optimal $(n,4,4)$ bounded-weight code $\mathcal{C}$ has $|D_2| = |D_3| = 0$, that is, $\mathcal{C}$ contains no codewords of weight two and weight three.*

4.4 Optimal $(n,4,4)$ Bounded-Weight Codes of Small Lengths

The values of $A'(n,4,4)$ for several small values of n are provided below.

Proposition 8

$$A'(n,4,4) = \begin{cases} 1, & \text{if } n \leq 3 \\ 2, & \text{if } n \in \{4,5\} \\ 4, & \text{if } n = 6 \\ 8, & \text{if } n = 7 \\ 19, & \text{if } n = 9. \end{cases}$$

Proof The value of $A'(n,4,4)$ is easily obtained for $n \leq 5$. The optimal $(n,4,4)$ bounded-weight codes for $n \in \{6,7,9\}$ are given in Table 3. The codes are obtained via exhaustive search. □

Proposition 8 shows that $A'(n,4,4) = A(n,4,4)+1$ for $n \in \{3,4,5,6,7,9\}$.

4.5 Piecing Together

Let $n \notin \mathcal{N} \cup \{1,2,3,4,5,6,7,9\}$, and let $\mathcal{C}$ be an $(n,4,4)$ bounded-weight code.

Propositions 5, 6, and 7 imply that $\mathcal{C}$ has size at most $J(n,4,4)$ if $\mathcal{C}$ contains codewords of weight two and/or three. Since (3) with Theorem 4 gives $A'(n,4,4) \geq J(n,4,4)+1$, $\mathcal{C}$ cannot be optimal. Therefore, if $\mathcal{C}$ is optimal, $\mathcal{C}$ can contain only codewords of weight zero, one, or four.

Suppose $\mathcal{C}$ contains only codewords of weight zero and four. Then obviously, $|\mathcal{C}| \leq A(n,4,4)+1 = J(n,4,4)+1$. If $\mathcal{C}$ contains a codeword of weight one, we have seen earlier that $\mathcal{C}$ has size at most one more than the size of the largest $(n-1,4,4)$ bounded weight code containing only codewords of weight three and four. As shown above, such a code has size at most $J(n-1,4,4)$. Since $J(n-1,4,4)+1 \leq J(n,4,4)+1$, we may assume that if $\mathcal{C}$ is optimal, then $\mathcal{C}$ has no codewords of weight one. With the results in subsection 4.4, we now have:

Theorem 5 *For all positive integers n,*

$$A'(n,4,4) = J(n,4,4)+1,$$

except possibly for $n \in \mathcal{N}$.

5 Conclusion

In this paper, we continue the investigation of the function $A'(n,d,e)$, which gives the smallest possible ℓ so that every (n,d) code is list decodable with a list of length ℓ up to radius e. Exact values of $A'(n,d,e)$ were determined for $d \geq 2e-5$ and $d \leq 3$. As a result, the exact value of $A'(n,d,e)$ is now known for all but 42 values of n, when $e \leq 4$. Our approach in this paper is purely combinatorial, and we have not attempted to address the existence of codes admitting efficient list decoding algorithms capable of meeting the bounds established here.

Acknowledgements We thank the anonymous reviewer for helpful comments.

References

1. Ahlswede, R.: Channel capacities for list codes. J. Appl. Probability **10**(4), 824–836 (1973)
2. Bassalygo, L.A.: New upper bounds for error-correcting codes. Problemy Peredači Informacii **1**(vyp. 4), 41–44 (1965)
3. Blinovsky, V.: Bounds for codes in the case of list decoding of finite volume. Problems of Information Transmission **22**(1), 7–19 (1986)
4. Blinovsky, V.: Asymptotic Combinatorial Coding Theory. The Kluwer International Series in Engineering and Computer Science, 415. Kluwer Academic Publishers, Boston (1997)
5. Brouwer, A.E.: On the packing of quadruples without common triples. Ars Combin. **5**, 3–6 (1978)
6. Brouwer, A.E.: Optimal packings of K_4's into a K_n. J. Combin. Theory Ser. A **26**(3), 278–297 (1979)
7. Brouwer, A.E., Shearer, J.B., Sloane, N.J.A., Smith, W.D.: A new table of constant weight codes. IEEE Trans. Inform. Theory **36**(6), 1334–1380 (1990)
8. Cassuto, Y., Bruck, J.: A combinatorial bound on the list size (2004). Technical Report, California Institute of Technology, Pasedna, CA (2004).
9. Elias, P.: List decoding for noisy channels. Tech. Rep. 335, Research Laboratory of Electronics, Massachusetts Institute of Technology (1957)
10. Elias, P.: Error-correcting codes for list decoding. IEEE Trans. Inform. Theory **37**(1), 5–12 (1991)
11. Forney, G.D.: Exponential error bounds for erasure, list and decision feedback schemes. IEEE Trans. Inform. Theory **14**, 549–557 (1968)
12. Goldreich, O., Levin, L.A.: A hard-core predicate for all one-way functions. In: STOC 1989: Proceedings of the 21st Annual ACM Symposium on Theory of Computing, 15-17 May 1989, Seattle, Washington, USA, pp. 25–32. ACM Press (1989)
13. Guruswami, V.: List Decoding of Error-Correcting Codes, *Lecture Notes in Computer Science*, vol. 3282. Springer-Verlag, Berlin (2004)
14. Guruswami, V., Sudan, M.: Extensions to the Johnson bound (2001). Unpublished manuscript
15. Hanani, H.: On quadruple systems. Canad. J. Math. **12**, 145–157 (1960)
16. Ji, L.: Asymptotic determination of the last packing number of quadruples. Des. Codes Cryptogr. **38**(1), 83–95 (2006)
17. Johnson, S.M.: Upper bounds for constant weight error-correcting codes. Discrete Math. **3**, 109–124 (1972)
18. Schönheim, J.: On maximal systems of k-tuples. Studia Sci. Math. Hungar **1**, 363–368 (1966)
19. Shannon, C.E., Gallager, R.G., Berlekamp, E.R.: Lower bounds to error probability for coding on discrete memoryless channels. I. Information and Control **10**, 65–103 (1967)
20. Shannon, C.E., Gallager, R.G., Berlekamp, E.R.: Lower bounds to error probability for coding on discrete memoryless channels. II. Information and Control **10**, 522–552 (1967)
21. Spencer, J.: Maximal consistent families of triples. J. Combin. Theory **5**, 1–8 (1968)
22. Sudan, M.: Decoding of Reed Solomon codes beyond the error-correction bound. J. Complexity **13**(1), 180–193 (1997)
23. Wozencraft, J.M.: List decoding. Research Laboratory of Electronics, Massachusetts Institute of Technology, Progress Report 48, 1958, pp. 90–95
24. Zyablov, V.V., Pinsker, M.S.: List cascade decoding. Problems of Information Transmission **17**(4), 236–240 (1982)