On Levenshtein's Channel and List Size in Information Retrieval

Ville Junnila, Tero Laihonen and Tuomo Lehtilä

***Abstract*—The Levenshtein's channel model for substitution errors is relevant in information retrieval where information is received through many noisy channels. In each of the channels there can occur at most t errors and the decoder tries to recover the information with the aid of the channel outputs. Recently, Yaakobi and Bruck considered the problem where the decoder provides a list instead of a unique output. If the underlying code $C \subseteq \mathbb{F}_2^n$ has error-correcting capability e, we write $t = e + \ell$, ($\ell \geq 1$). In this paper, we provide new (constant) bounds on the size of the list. In particular, we give using the Sauer-Shelah lemma the upper bound $\ell + 1$ on the list size for large enough n provided that we have a sufficient number of channels. We also show that the bound $\ell + 1$ is the best possible. Most of our other new results rely on constant weight codes.**

***Index Terms*—Levenshtein's Channel, Information Retrieval, Substitution Errors, List Decoding, Sauer-Shelah Lemma.**

I. Introduction

In this paper, we consider the *Levenshtein's channel model* of substitution errors introduced in [2] for sequences reconstruction problems. The original motivation came from biology and chemistry where the usual redundancy method of error correction is not feasible. Recently, it was pointed out that this channel model is very relevant to information retrieval in advanced storage technologies where the stored information is either a single copy, which is read by many read heads, or the stored information has several copies [3], [4]. As mentioned in [3], this model is specifically applicable to DNA data storage systems, [5]–[8]. In those systems, DNA strands give us a large number of erroneous copies of the information and we try to recover the information with the aid of these strands. For various related sequences reconstruction problems (like the deletion and insertion errors) see, for example, [2], [9], [10].

Let us first introduce some notation. We denote the set $\{1, 2, \ldots, n\}$ by $[1, n]$. Let $\mathbb{F} = \mathbb{F}_2$ be a finite field of 2 elements, and denote the Hamming space by $\mathbb{F}^n$. The *support* of a word $\mathbf{x} = x_1 \ldots x_n \in \mathbb{F}^n$ is defined by $\text{supp}(\mathbf{x}) = \{i \mid x_i \neq 0\}$. We denote the all-zero word $\mathbf{0} = 00 \ldots 0 \in \mathbb{F}^n$ and $\mathbf{e}_i \in \mathbb{F}^n$ is a word with 1 in the ith coordinate and zeros elsewhere. The *Hamming weight* $w(\mathbf{x})$ of $\mathbf{x} \in \mathbb{F}^n$ equals $|\text{supp}(\mathbf{x})|$. The *Hamming distance* is defined as $d(\mathbf{x}, \mathbf{y}) = w(\mathbf{x} + \mathbf{y})$ for $\mathbf{x}, \mathbf{y} \in \mathbb{F}^n$. We denote the *Hamming ball* of radius t centered at $\mathbf{x} \in \mathbb{F}^n$ by $B_t(\mathbb{F}^n; \mathbf{x}) = B_t(\mathbf{x}) = \{\mathbf{y} \in \mathbb{F}^n \mid d(\mathbf{x}, \mathbf{y}) \leq t\}$ and the cardinality of the ball by $V(n, t) = \sum_{i=0}^{t} \binom{n}{i}$. A nonempty subset of $\mathbb{F}^n$ is called a *code* and its elements are called *codewords*. The *minimum distance* of a code $C \subseteq \mathbb{F}^n$ is defined as $d_{\min}(C) = \min_{\mathbf{c}_1, \mathbf{c}_2 \in C, \mathbf{c}_1 \neq \mathbf{c}_2} d(\mathbf{c}_1, \mathbf{c}_2)$. Thus, the code has the error-correcting capability $e = e(C) = \lfloor (d_{\min}(C) - 1)/2 \rfloor$.

Let us consider now the channel model in more detail. A codeword $\mathbf{x} \in C \subseteq \mathbb{F}_2^n$ is transmitted through N channels where at most t substitution errors can occur in each of them — in other words, we get N estimations of a stored information unit. The set of output words is denoted by Y. (In the model, it is assumed that all the outputs from the channels are different from each other.) This is illustrated in Fig. 1. It is also assumed that $t > e(C)$, that is, there can be more errors than the code C can cope with if it is considered only as an error-correcting code. We denote

$$t = e(C) + \ell = e + \ell$$

for $\ell \geq 1$. For a recent generalization of the problem, see [3].

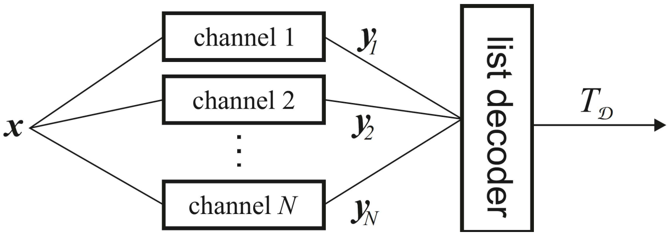

Fig. 1. The Levenshtein's channel model.

Based on the N different outputs $Y = \{\mathbf{y}_1, \ldots, \mathbf{y}_N\}$ of the channels, we should be able to recover $\mathbf{x}$. Clearly, if $t \leq e$, then only one channel is enough. In [11], [12], the authors consider the situation where instead of always recovering $\mathbf{x}$ uniquely, we obtain sometimes a short list of possibilities for $\mathbf{x}$. In other words, based on the different output words $\mathbf{y}_1, \ldots, \mathbf{y}_N$ and the code C, the list decoder $\mathcal{D}$ gives an estimation $T_\mathcal{D} = T_\mathcal{D}(Y) = \{\mathbf{x}_1, \ldots, \mathbf{x}_{|T_\mathcal{D}|}\}$ on the transmitted word $\mathbf{x}$. We denote by $\mathcal{L}_\mathcal{D}$ the maximum cardinality of the list $T_\mathcal{D}(Y)$ over all possible sets Y of output words. The decoder is *successful* if the transmitted word $\mathbf{x}$ belongs to $T_\mathcal{D}$. In this paper, we concentrate on the minimal value of $\mathcal{L}_\mathcal{D}$ over all successful decoders $\mathcal{D}$, that is, on the value $\mathcal{L} = \min_{\mathcal{D} \text{ is successful}} \{\mathcal{L}_\mathcal{D}\}$. We denote

$$T = T(Y) = C \cap (\bigcap_{\mathbf{y} \in Y} B_t(\mathbf{y})).$$

This paper was presented in part at 2019 IEEE International Symposium on Information Theory (ISIT2019) (see [1]).

T. Lehtilä was supported by the University of Turku Graduate School (UTUGS) and the Vilho, Yrjö and Kalle Väisälä Foundation.

The authors are with the Department of Mathematics and Statistics, University of Turku, Turku FI-20014, Finland (e-mail: viljun@utu.fi; terolai@utu.fi; tualeh@utu.fi)

Hence, we have

$$\mathcal{L} = \max\{|T(Y)| \mid Y \text{ is a set of } N \text{ output words}\}.$$

The value of $\mathcal{L}$ is studied for example, in [11]–[16]. Naturally, we would like to have as small an $\mathcal{L}$ as possible. Notice that $\mathcal{L}$ depends on e, ℓ, n, C and N where C is an e-error-correcting code. In this paper, we mainly fix e and ℓ and then consider the relation between N and $\mathcal{L}$ for various n. In particular, we bound N and see how large $\mathcal{L}$ can be for any e-error-correcting code C.

There is also another closely related problem of *information retrieval in associative memory* introduced by Yaakobi and Bruck [11], [12]. In their model, an associative memory is given as a (simple and undirected) graph $G = (V, E)$. A vertex in the graph corresponds to a stored information unit and if two information units are associated, then there is an edge between them. Moreover, two vertices are called *t-associated*, if the distance between them is at most t. An unknown information unit $x \in V$ is retrieved from the associative memory using *input clues* provided by an information seeker. The input clues are t-associated to x and also belong to a code $C \subseteq V$ serving as a reference set. The reference set should be such that given enough input clues, the sought information unit x can be found unambiguously (or with some small uncertainty). Naturally, we want the maximum number m of input clues, which are needed to retrieve any information unit from the memory, to be as small as possible. The two parameters $\mathcal{L}$ and m are closely related (see, for instance, [13]).

The structure of the paper is as follows. In Section II, we show some upper and lower bounds on $\mathcal{L}$ for an e-error-correcting code when $t = e + \ell$. We also show that there exist e-error-correcting codes such that $\mathcal{L}$ is not a constant (i.e., depends on n) if the number of channels $N \leq V(n, \ell - 1)$. In Section III, we give an upper bound $\mathcal{L} \leq \ell + 1$ for an e-error-correcting code when n is large enough and $N \geq V(n, \ell - 1) + 1$. Moreover, in Theorem 9, we show that there exist codes which attain this upper bound. Section IV considers a case with at least two distant output words in Y when $e \geq 2\ell - 1$. We show that having distant output words is a reasonable assumption and in that case $\mathcal{L}$ is rather small (we may even reach $|T| \leq 2$). Finally, in Section V, we consider the case with less than $V(n, \ell - 1) + 1$ channels. We especially show that if $V(n, \ell - a - 1) + 1 \leq N \leq V(n, \ell - a)$ where $0 \leq a \leq \ell - 1$ and if C is an e-error-correcting code such that $\mathcal{L}$ is maximal, then $\mathcal{L} = \Theta(n^a)$.

II. Some upper and lower bounds on $\mathcal{L}$

For the rest of the section, let C be an e-error-correcting code in $\mathbb{F}^n$ and $t = e + \ell$ be the maximum number of errors that might occur during the transmission. We will first consider upper bounds on $\mathcal{L}$ and then lower bounds. The basic idea on estimating the maximum length $\mathcal{L}$ of the decoded list is the following: given the output words of the channels, we analyse the number of codewords of C that locate in the intersection of Hamming balls of radius t centered at the output words. As expected, the length $\mathcal{L}$ of the decoded list in Levenshtein's channel model strongly depends on the number of channels. In particular, as N increases, $\mathcal{L}$ decreases and vice versa. We discuss more about the dependency between N and $\mathcal{L}$ in Section V.

We focus on the case with $N \geq V(n, \ell - 1) + 1$. In Theorem 10, we show that if the number of channels N is at most $V(n, \ell - 1)$, then the maximum length $\mathcal{L}$ of the decoded list depends on n for some e-error-correcting codes. On the other hand, in Theorem 7 we see that if we have $N \geq V(n, \ell - 1) + 1$ channels, then $\mathcal{L} \leq 2^\ell$. Hence, $V(n, \ell - 1) + 1$ is the exact number of channels necessary to have constant list size $\mathcal{L}$ on n. Previously, in [2] and [11], Levenshtein's channel model had been considered for $\mathcal{L} = 1$ and $\mathcal{L} = 2$, respectively. However, in both cases, the number of channels is larger than $N = V(n, \ell - 1) + 1$ which is the focus of this paper. In [2], Levenshtein has given the following lower bound for the number of channels in the case $\mathcal{L} = 1$. Originally, Levenshtein considered a case with a code of minimum distance d. For easier comparison, we assume that minimum distance $d = 2e + 1$.

Theorem 1. *[2] Let $C \subseteq \mathbb{F}^n$ be an e-error-correcting code with minimum distance $d = 2e + 1$ and $t = e + \ell$. If*

$$N \geq \sum_{i=0}^{\ell-1} \binom{n - 2e - 1}{i} \sum_{k=e+1+i-\ell}^{t-i} \binom{2e+1}{k} + 1,$$

then we have $\mathcal{L} = 1$.

Notice that if n is large enough, then the largest term of the sum is $2\binom{n-2e-1}{\ell-1}\binom{2e+1}{e+1}$ which is roughly $2\binom{n}{\ell-1}\binom{2e+1}{e+1}$ when $n \gg e$. Hence, the number of channels given by this theorem is notably larger than $V(n, \ell - 1) + 1$. The number of channels required to have $\mathcal{L} \leq 2$ presented in [11, Theorem 6] is between our $V(n, \ell - 1) + 1$ and Levenshtein's result. For example, when $n = 20$, $\ell = 3$, $e = 4$ and minimum distance $d = 2e + 1$, Levenshtein's result for $\mathcal{L} = 1$ requires that $N \geq 18972$, the result for $\mathcal{L} \leq 2$ given by Yaakobi and Bruck requires that $N \geq 2712$ and the bound $\mathcal{L} \leq 2^\ell = 8$ presented in Theorem 7 requires that $N \geq 212$. In particular, the number of channels required to have $\mathcal{L} = 1$ (Theorem 1) or $\mathcal{L} \leq 2$ ([11, Theorem 6]) depends on e. However, in most of our results $V(n, \ell - 1) + 1$ channels are enough and this bound does not depend on e. In [11, Theorem 12], Yaakobi and Bruck have shown that if n is large enough, then we need $N = \Theta(n^{\ell-1})$ channels to have constant list size $\mathcal{L}$. Clearly, $V(n, \ell - 1) \in \Theta(n^{\ell-1})$.

The results on the number of required channels in the cases $\mathcal{L} = 1$ and $\mathcal{L} = 2$ are obtained by analysing cardinalities of two and three intersecting Hamming balls centered at the codewords of C, respectively. However, contrary to the cases with two or three balls, if the intersection of four or more balls is considered, then the size of the intersection no longer depends on the distances of the centers of the balls (see [17, p. 36]). Thus, we rather try to cover $T(Y)$ with some k copies of e-radius balls. Since C is an e-error-correcting code, there can be at most one codeword in any e-radius ball and thus $|T(Y)| \leq k$. Hence, in this paper, we use the approach presented in Lemma 2.

Lemma 2. *Let $C \subseteq \mathbb{F}^n$ be an e-error-correcting code. If for any set of output words $Y = \{\mathbf{y}_1, \ldots, \mathbf{y}_N\}$ we have*

$$T(Y) = C \cap \left(\bigcap_{i=1}^{N} B_t(\mathbf{y}_i) \right) \subseteq \bigcup_{i=1}^{k} B_e(\beta_i)$$

for some words $\beta_i \in \mathbb{F}^n$ $(i = 1, \ldots, k)$, then $\mathcal{L} \leq k$.

Proof. Observe, that we have $d(\mathbf{c}_1, \mathbf{c}_2) \geq 2e + 1$ for any distinct codewords in C. Therefore, we may have at most one codeword in any e-radius ball. Thus, there can be at most k codewords in a union of k copies of e-radius balls. Moreover, since each word in $T(Y)$ is a codeword and $T(Y)$ is covered by k copies of some e-radius balls centered at words β_i, we have $|T(Y)| \leq k$ for each choice of Y and thus, $\mathcal{L} \leq k$. □

Notice that the previous lemma also gives a decoding algorithm if we know how to choose the words β_i. Indeed, if the words β_i are known, then each ball $B_e(\beta_i)$ contains at most one codeword and the decoding can be done by using decoding algorithm of code C on words β_i and then adding these codewords to the list T.

A. Upper bounds on $\mathcal{L}$

Now we are ready to examine the actual upper bounds on $\mathcal{L}$. The first upper bound is based on the following theorem by Kleitman [18].

Theorem 3. *If r is a positive integer, $n \geq 2r + 1$ and S is a subset of $\mathbb{F}^n$ such that $d(\mathbf{x}, \mathbf{y}) \leq 2r$ for any distinct $\mathbf{x}, \mathbf{y} \in S$, then $|S| \leq V(n, r)$.*

The following result is an immediate corollary of the previous theorem.

Corollary 4. *If $n \geq 2\ell - 1$ and the number of channels $N \geq V(n, \ell - 1) + 1$, then there exist two output words $\mathbf{y}_1$ and $\mathbf{y}_2$ such that $d(\mathbf{y}_1, \mathbf{y}_2) \geq 2\ell - 1$.*

In the following theorem, we show that the maximum length $\mathcal{L}$ of the decoded list is at most $\binom{2\ell}{\ell}$. This result and its proof can be seen as reformulations of a result by Yaakobi and Bruck [11, Algorithm 18]. Moreover, this theorem is weaker than Theorem 7. However, it illustrates the use of Lemma 2.

Theorem 5. *Let $n \geq 2\ell - 1$ and C be an e-error-correcting code in $\mathbb{F}^n$. If $t = e + \ell$ and $N \geq V(n, \ell - 1) + 1$, then we have*

$$\mathcal{L} \leq \binom{2\ell}{\ell}.$$

Proof. Assume that $N \geq V(n, \ell - 1) + 1$ and let $\mathbf{x} \in C$ be the input word. By Corollary 4, we have two outputs $\mathbf{y}_0, \mathbf{y} \in Y$ such that $d(\mathbf{y}_0, \mathbf{y}) \geq 2\ell - 1$. Trivially,

$$T(Y) = C \cap \left(\bigcap_{\mathbf{y}_i \in Y} B_t(\mathbf{y}_i) \right) \subseteq C \cap B_t(\mathbf{y}_0) \cap B_t(\mathbf{y}).$$

Now, our goal is to find a set of $k = \binom{2\ell}{\ell}$ such words β_i that we have $C \cap B_t(\mathbf{y}_0) \cap B_t(\mathbf{y}) \subseteq \bigcap_{i=1}^{k} B_e(\beta_i)$. If we find these words, then Lemma 2 states that $\mathcal{L} \leq k$.

$$\begin{array}{rl} \mathbf{x} = & 1\,0\,1\,0\,0\,1\,0\,1 \\ \beta_j = & 1\,0\,1\,0\,0\,1\,1\,0 \\ \mathbf{y} = & \underbrace{1\,1\,1\,1\,1}_{A}\,1\,1\,0 \\ \mathbf{y}_0 = & 0\,0\,0\,0\,0\,0\,0\,0 \end{array}$$

Fig. 2. Two output words $\mathbf{y}$ and $\mathbf{y}_0$ at distance $7 \geq 2\ell - 1$ when $\ell = 3$ and $e = 2$. We have $d(\beta_j, \mathbf{x}) = 2 \leq e$ where $j \in [\binom{2\ell-1}{\ell} + 1, 2\binom{2\ell-1}{\ell}]$.

Without loss of generality, we may assume that $\mathbf{y}_0 = \mathbf{0}$. Since $w(\mathbf{y}) \geq 2\ell - 1$, there exists a set $A \subsetneq \text{supp}(\mathbf{y})$ with $2\ell - 1$ elements. Moreover, let us denote each distinct word of weight ℓ with the support belonging to A by $\mathbf{b}_i \in \mathbb{F}^n$, for $i \in [1, \binom{2\ell-1}{\ell}]$. Furthermore, either $\mathbf{y}_0$ or $\mathbf{y}$ differs from the input word $\mathbf{x}$ in at least ℓ coordinates in A. Suppose first that this is the case with the word $\mathbf{y}_0$, i.e., $|A \cap \text{supp}(\mathbf{x})| \geq \ell$. Let us have $\beta_i = \mathbf{b}_i + \mathbf{y}_0 = \mathbf{b}_i$, for $1 \leq i \leq \binom{2\ell-1}{\ell}$. Since $|A \cap \text{supp}(\mathbf{x})| \geq \ell$, there exists such a word β_j, for some $j \in [1, \binom{2\ell-1}{\ell}]$, that $\text{supp}(\beta_j) \subseteq \text{supp}(\mathbf{x})$. Since $d(\mathbf{y}_0, \mathbf{x}) \leq t$, we have $d(\beta_j, \mathbf{x}) = d(\mathbf{y}_0, \mathbf{x}) - \ell \leq t - \ell = e$.

Let us then consider the case where $|A \cap \text{supp}(\mathbf{x})| \leq \ell - 1$. Hence, $\mathbf{x}$ differs from $\mathbf{y}$ in at least ℓ coordinates in A. We have illustrated this situation in Figure 2. Now, we consider the words $\beta_h = \mathbf{b}_i + \mathbf{y}$, where $i \in [1, \binom{2\ell-1}{\ell}]$ and $h = i + \binom{2\ell-1}{\ell}$. We have $|A \cap \text{supp}(\beta_h)| = \ell - 1$ and $\text{supp}(\beta_h) \setminus A = \text{supp}(\mathbf{y}) \setminus A$ for each $h \in [\binom{2\ell-1}{\ell} + 1, 2\binom{2\ell-1}{\ell}]$. Again, for some β_j, $j \in [\binom{2\ell-1}{\ell} + 1, 2\binom{2\ell-1}{\ell}]$, we have such a word that $\text{supp}(\mathbf{x}) \cap A \subseteq \text{supp}(\beta_j)$ and hence, $d(\beta_j, \mathbf{x}) = d(\mathbf{y}, \mathbf{x}) - \ell \leq e$. Therefore, by Lemma 2, we obtain $\mathcal{L} \leq \binom{2\ell-1}{\ell-1} + \binom{2\ell-1}{\ell} = \binom{2\ell}{\ell}$ and the claim follows. □

In order to improve the previous upper bound (to 2^ℓ), we present the well-known Sauer-Shelah lemma ([19], [20]). Let $\mathcal{F}$ be a family of subsets of $[1, n]$, where n is a positive integer. We say that a subset S of $[1, n]$ is *shattered* by $\mathcal{F}$ if for any subset $E \subseteq S$ there exists a set $F \in \mathcal{F}$ such that $F \cap S = E$. The Sauer-Shelah lemma states that if $|\mathcal{F}| > \sum_{i=0}^{k-1} \binom{n}{i}$, then $\mathcal{F}$ shatters a subset of size (at least) k. Since the subsets of $[1, n]$ can naturally be interpreted as words of $\mathbb{F}^n$, the Sauer-Shelah lemma can be reformulated as follows. Notice that $\sum_{i=0}^{k-1} \binom{n}{i} = V(n, k - 1)$.

Theorem 6 ([19], [20])**.** *If $Y \subseteq \mathbb{F}^n$ is a set containing at least $V(n, k - 1) + 1$ words, then there exists a set S of k coordinates such that for any word $\mathbf{w} \in \mathbb{F}^n$ with supp$(\mathbf{w}) \subseteq S$ there exists a word $\mathbf{s} \in Y$ satisfying supp$(\mathbf{w})$ = supp$(\mathbf{s}) \cap S$. Here we say that the set S of coordinates is* shattered *by Y.*

In the following theorem, we show that $\mathcal{L} \leq 2^\ell$.

Theorem 7. *Let $n \geq \ell$ and C be an e-error-correcting code in $\mathbb{F}^n$. If $t = e + \ell$ and $N \geq V(n, \ell - 1) + 1$, then we have*

$$\mathcal{L} \leq 2^\ell.$$

Proof. Let Y be the set of output words and $\mathbf{x}$ be the input word. Assume that $N \geq V(n, \ell - 1) + 1$. Now, by Theorem 6, there exists a set S of ℓ coordinates which is shattered by Y. Let $\mathbf{s}$ be the word such that $\mathrm{supp}(\mathbf{s}) = S$ and $Y' = \{\mathbf{y}_1, \dots, \mathbf{y}_{2^\ell}\}$ be a subset of Y such that Y' shatters S. Define then $\beta_i = \mathbf{s} + \mathbf{y}_i \in \mathbb{F}^n$ for $1 \leq i \leq 2^\ell$. By the choice of Y', there exists a word $\mathbf{y}_i \in Y'$ such that $\mathrm{supp}(\mathbf{y}_i) \cap S = \mathrm{supp}(\mathbf{x} + \mathbf{s}) \cap S$, i.e., $\mathbf{y}_i$ and $\mathbf{x}$ differ in ℓ coordinate places of S. Hence, we obtain $d(\beta_i, \mathbf{x}) \leq e$ for $\beta_i = \mathbf{s} + \mathbf{y}_i$. Therefore, by Lemma 2, we have $\mathcal{L} \leq 2^\ell$ and the claim follows. □

Observe that when $\ell = 1$ and $N \geq 2$ or $\ell = 2$ and $N \geq n+2$, we have $\mathcal{L} \leq 2$ or $\mathcal{L} \leq 4$, respectively. Later, in Theorem 9, we show that the first upper bound is tight and then, in Remark 21, we show that we can in some circumstances attain the upper bound $\mathcal{L} \leq 4$.

B. Lower bounds on $\mathcal{L}$

In the following, we concentrate on the lower bounds on $\mathcal{L}$. Here the main idea of the proofs is to find a (bad) set of output words Y to maximize the possible input words that could have been transmitted. In the following theorem, we give a lower bound on the list size when the number of channels is bounded from above.

Let $\mathbf{x} \in \mathbb{F}^n$ and $A \subseteq \mathbb{F}^n$. We call the set

$$\mathbf{x} + A = \{\mathbf{x} + \mathbf{a} \mid \mathbf{a} \in A\}$$

a *translate* of A.

Theorem 8. *For an e-error-correcting code $C \subseteq \mathbb{F}^n$ and radius $t = e + \ell$, we have*

$$\mathcal{L} \geq \frac{|C|(V(n, t-a+1) - \binom{n-a}{t-a+1})}{2^n}$$

if there exist at most $N \leq V(n, a-1)+1$ channels, $1 \leq a \leq \ell$ and $n \geq t+1$.

Proof. Let us first consider the words of $B_{a-1}(\mathbf{0})$. The intersection of the balls with radius t centered at these words gives

$$\bigcap_{\mathbf{b} \in B_{a-1}(\mathbf{0})} B_t(\mathbf{b}) = B_{t-a+1}(\mathbf{0}). \tag{1}$$

Denote by $\mathbf{s}$ the word with $\mathrm{supp}(\mathbf{s}) = [1, a]$. Let Z denote the set $B_{a-1}(\mathbf{0}) \cup \{\mathbf{s}\}$. Our set of (bad) output words Y will be a suitable translate of Z if $N = V(n, a-1)+1$ and a subset of size N of the translate if $N < V(n, a-1)+1$. Let P denote the intersection of balls of radius t centered at the words of Z. By (1), we get $P = B_t(\mathbf{s}) \cap B_{t-a+1}(\mathbf{0})$. It is easy to verify that

$$|P| = V(n, t-a+1) - \binom{n-a}{t-a+1}. \tag{2}$$

Next we show that there exist $\mathbf{u} \in \mathbb{F}^n$ such that the translate $\mathbf{u} + P$ contains at least $|C||P|/2^n$ codewords of C. By double counting the number M of pairs $(\mathbf{u}, \mathbf{c})$ such that $\mathbf{u} \in \mathbb{F}^n$, $\mathbf{c} \in C$ and $\mathbf{c} \in \mathbf{u} + P$, we obtain

$$\sum_{\mathbf{u} \in \mathbb{F}^n} |(\mathbf{u} + P) \cap C| = M = |C||P|.$$

Therefore, considering the average, there exists $\mathbf{u} \in \mathbb{F}^n$ such that $|(\mathbf{u} + P) \cap C| \geq |C||P|/2^n$. Notice that the set $\mathbf{u} + P$ is the set of intersection of the balls of radius t centered at the words of the corresponding translate $\mathbf{u} + Z$ of Z. Clearly, $\mathbf{u} + Z = B_{a-1}(\mathbf{u}) \cup \{\mathbf{u} + \mathbf{s}\}$.

Let $\mathbf{c} \in C$ be a codeword in $\mathbf{u} + P$. If we transmit $\mathbf{c}$ through the N channels with at most t errors occurring in each one, then we can receive the set of output words $Y = \mathbf{u} + Z = B_{a-1}(\mathbf{u}) \cup \{\mathbf{s} + \mathbf{u}\}$ if $N = V(n, a-1)+1$ or a subset Y of size N of the translate $\mathbf{u} + Z$ if $N < V(n, a-1)+1$. In both cases, the codewords of $(\mathbf{u} + P) \cap C$ are a subset of the possible input words that could have been transmitted. Therefore, we get $\mathcal{L} \geq |C||P|/2^n$. The claim follows by (2). □

Next we give a lower bound on the list size when the number of channels $N \leq V(n, \ell-1)+1$. In other words, we show that there exists an e-error-correcting code for which $\mathcal{L} \geq \ell + 1$. Later, in Section III, it is shown that the lower bound can be attained for any e-error-correcting code if $N = V(n, \ell-1)+1$ and n is large enough.

Theorem 9. *Let $t = e + \ell$. There exists an e-error-correcting code $C \subseteq \mathbb{F}^n$ such that $\mathcal{L} \geq \ell + 1$ if $n \geq \ell + \ell e + e$ and the number of channels satisfies $N \leq V(n, \ell - 1) + 1$.*

Proof. Let us consider a code C_1 which consists of the codewords $\mathbf{c}_i$ ($i = 1, \dots, \ell$) satisfying

$$\mathrm{supp}(\mathbf{c}_i) = \{i, \ell + e(i-1) + 1, \dots, \ell + e(i-1) + e\}$$

together with the word $\mathbf{c}_{\ell+1}$ where $\mathrm{supp}(\mathbf{c}_{\ell+1}) = [n-e+1, n]$. Observe that $w(\mathbf{c}_1) = \cdots = w(\mathbf{c}_\ell) = e + 1$ and $w(\mathbf{c}_{\ell+1}) = e$. Since the supports of these $\ell + 1$ codewords are disjoint, they form a code with minimum distance $2e + 1$.

Let $\mathbf{s} \in \mathbb{F}^n$ be the word such that $\mathrm{supp}(\mathbf{s}) = [1, \ell]$. Assume that the set Y of the N received output words from the channels is a subset of $B_{\ell-1}(\mathbf{0}) \cup \{\mathbf{s}\}$. It is easy to see that the codewords of C_1 are included in $B_t(\mathbf{s})$. Moreover, all the codewords of C_1 also belong to the intersection of the balls of radius t centered at the output words of $B_{\ell-1}(\mathbf{0})$. Indeed, by (1) (where now $a = \ell$), we have

$$B_{e+1}(\mathbf{0}) = B_{t-\ell+1}(\mathbf{0}) = \bigcap_{\mathbf{b} \in B_{\ell-1}(\mathbf{0})} B_t(\mathbf{b}) \tag{3}$$

and the weights of the codewords are at most $e + 1$. Consequently, for the code C_1, we obtain $\mathcal{L} \geq \ell + 1$ (actually, we even have $\mathcal{L} = \ell + 1$). □

Notice that Theorem 9 is not just an example suitable for small codes. In fact, if n is large enough, we may take any e-error-correcting code $C \subseteq \mathbb{F}^n$, remove every codeword in some $(3e+1)$-radius ball and insert the code $C_1 \subseteq \mathbb{F}^n$ inside it in such a way that the all-zero word in the proof of previous theorem corresponds to the central word $\mathbf{w}$ of the $(3e+1)$-radius ball. Indeed, let $C' = (C \setminus B_{3e+1}(\mathbf{w})) \cup (\mathbf{w} + C_1)$ where $\mathbf{w} \in \mathbb{F}^n$. Let us next show that C' is still e-error-correcting. Consider a pair $(\mathbf{c}_1, \mathbf{c}_2)$ of distinct codewords of C'. If $\mathbf{c}_1, \mathbf{c}_2 \in \mathbf{w} + C_1$ or $\mathbf{c}_1, \mathbf{c}_2 \in C \setminus B_{3e+1}(\mathbf{w})$, we immediately have $d(\mathbf{c}_1, \mathbf{c}_2) \geq 2e + 1$. Let then $\mathbf{c}_1 \in \mathbf{w} + C_1$ and $\mathbf{c}_2 \in C \setminus B_{3e+1}(\mathbf{w})$. We can write $\mathbf{c}_1 = \mathbf{w} + \mathbf{a}$ where $e \leq w(\mathbf{a}) \leq e + 1$ and $\mathbf{c}_2 = \mathbf{w} + \mathbf{b}$, where $w(\mathbf{b}) \geq 3e + 2$. Now $d(\mathbf{c}_1, \mathbf{c}_2) = d(\mathbf{w}+\mathbf{a}, \mathbf{w}+\mathbf{b}) = d(\mathbf{a}, \mathbf{b}) = w(\mathbf{a}) + w(\mathbf{b}) - 2|\mathrm{supp}(\mathbf{a}) \cap \mathrm{supp}(\mathbf{b})| \geq w(\mathbf{b}) - w(\mathbf{a}) \geq 3e + 2 - (e + 1) =$

$2e+1$. Therefore, C' is e-error-correcting. Now it is easy to see that with set of output words corresponding to the one in the proof of Theorem 9, that is, $Y = B_{\ell-1}(\mathbf{w}) \cup \{\mathbf{s}+\mathbf{w}\}$, we get $\mathcal{L} \geq \ell+1$ for the code C'.

Next we show that the list size $\mathcal{L}$ can depend on n if the number of channels is at most $V(n,\ell-1)$. Let C be an e-error-correcting code in $\mathbb{F}^n$. Assume that the number of channels $N \leq V(n,\ell-1)$ and that all the output words are located inside $B_{\ell-1}(\mathbf{0})$. By (3), all the words of weight $e+1$ belong to the intersection. Moreover, by [21, p. 525], there exists a code with constant weight $e+1$ and minimum distance $2e+2$ with $\lfloor n/(e+1) \rfloor$ words. This implies that $\mathcal{L} \geq \lfloor n/(e+1) \rfloor$ and, hence, the list size depends on n when e is constant. Consequently, we obtain the following result.

Theorem 10. *If $N \leq V(n,\ell-1)$, then there exists an e-error-correcting code such that $\mathcal{L} \geq \lfloor n/(e+1) \rfloor$.*

III. Optimal upper bound $\mathcal{L} \leq \ell+1$ for large enough n

In this section, our goal is to show that $\mathcal{L} \leq \ell+1$ when $N \geq V(n,\ell-1)+1$ and n is large enough. In Theorem 17, we give the bound $\mathcal{L} \leq \ell+1$ where n depends exponentially on e and ℓ. Later, in Theorem 20, we improve on this result by proving that the bound already holds when n is only of polynomial size with respect to e and ℓ. Although Theorem 20 can be viewed as an improvement of Theorem 17, we have decided also to include the simpler result to the paper as the proof of the other main theorem is highly complicated and technical. The main ideas of the proof are more evident in the simpler result. Moreover, observe that for some (sporadic) small values of e and ℓ the requirement of Theorem 17 for n can be smaller than the one of Theorem 20. In what follows, we present a few lemmas in order to prove the main results of the section.

The following lemma is a critical part in showing that $\mathcal{L} \leq \ell+1$ when n is large enough. In particular, we show that if there exists a word $\mathbf{w}$ close to every codeword in $T = T(Y)$, then the cardinality of T is rather small. Moreover, in Theorems 17 and 20 we verify the existence of such a word $\mathbf{w}$.

Lemma 11. *Let the set of outputs Y consist of $N \geq V(n,\ell-1)+1$ words and C be an e-error-correcting code. Further let h be an integer and $\mathbf{w} \in \mathbb{F}^n$ be a word such that $0 \leq h \leq \ell$ and $d(\mathbf{w},\mathbf{c}) \leq e+h$ for each $\mathbf{c} \in T(Y)$. Then we have*

$$|T(Y)| \leq \sum_{i=0}^{h} \binom{\ell}{i}.$$

Proof. Let $\mathbf{x}$ be the transmitted codeword. Assume that $\mathbf{w} \in \mathbb{F}^n$ is a word satisfying $d(\mathbf{w},\mathbf{c}) \leq e+h$ for every $\mathbf{c} \in T(Y)$; in particular, $d(\mathbf{w},\mathbf{x}) \leq e+h$. Without loss of generality, we may assume that $\mathbf{w} = \mathbf{0}$. Since $N \geq V(n,\ell-1)+1$, by Theorem 6, there exists a set $S \subseteq [1,n]$ of ℓ coordinates which are shattered by a subset $Y' = \{\mathbf{y}_1, \ldots, \mathbf{y}_{2^\ell}\} \subseteq Y$. Let $\mathbf{s}$ denote the word such that $\mathrm{supp}(\mathbf{s}) = S$. The proof now divides into two cases based on the number of different coordinates between $\mathbf{x}$ and $\mathbf{w}$ in S, that is, $|\mathrm{supp}(\mathbf{x}) \cap S|$.

Assume first that $|\mathrm{supp}(\mathbf{x}) \cap S| \leq h-1$. Define $\overline{Y} = \{\overline{\mathbf{y}} \in Y' \mid |\mathrm{supp}(\overline{\mathbf{y}}) \cap S| \geq \ell-(h-1)\} \subseteq Y'$ and $\mathcal{B}_1 = \{\beta = \overline{\mathbf{y}}+\mathbf{s} \mid \overline{\mathbf{y}} \in \overline{Y}\}$. Notice that $|\overline{Y}| = |\mathcal{B}_1| = \sum_{i=\ell-(h-1)}^{\ell} \binom{\ell}{i} = \sum_{i=0}^{h-1} \binom{\ell}{i}$. Since $|\mathrm{supp}(\mathbf{x}) \cap S| \leq h-1$, there exists a word $\overline{\mathbf{y}} \in \overline{Y}$ such that $\mathrm{supp}(\overline{\mathbf{y}}+\mathbf{x}) \cap S = S$, that is, $\mathbf{x}$ and $\overline{\mathbf{y}}$ differ in every coordinate of S. Then $\beta = \overline{\mathbf{y}}+\mathbf{s} \in \mathcal{B}_1$. Therefore, we have $d(\mathbf{x},\beta) = d(\mathbf{x},\overline{\mathbf{y}}+\mathbf{s}) = d(\mathbf{x},\overline{\mathbf{y}}) - \ell \leq t-\ell = e$.

Let us then assume that $|\mathrm{supp}(\mathbf{x}) \cap S| \geq h$. Define $\mathcal{B}_2 = \{\beta \in \mathbb{F}^n \mid w(\beta) = h \text{ and } \mathrm{supp}(\beta) \subseteq S\}$. Notice that $|\mathcal{B}_2| = \binom{\ell}{h}$. Now there exists a word $\beta \in \mathcal{B}_2$ such that $\mathrm{supp}(\beta) \subseteq \mathrm{supp}(\mathbf{x})$. Hence, we have $d(\mathbf{x},\beta) = |\mathrm{supp}(\mathbf{x})| - h \leq (e+h) - h = e$. Therefore, we obtain that

$$\mathbf{x} \in \bigcup_{\beta \in \mathcal{B}_1 \cup \mathcal{B}_2} B_e(\beta)$$

and the claim follows by Lemma 2 since $|\mathcal{B}_1 \cup \mathcal{B}_2| = |\mathcal{B}_1| + |\mathcal{B}_2| = \sum_{i=0}^{h} \binom{\ell}{i}$. □

The following corollary is immediately obtained by choosing $h=1$ in the previous lemma.

Corollary 12. *Let the set of output words Y consist of $N \geq V(n,\ell-1)+1$ words, C be an e-error-correcting code and let there exist a word $\mathbf{w} \in \mathbb{F}^n$ such that $d(\mathbf{w},\mathbf{c}) \leq e+1$ for each $\mathbf{c} \in T(Y)$. Then we have*

$$|T(Y)| \leq \ell+1.$$

In Theorems 9 and 20 the aim is to show that a word $\mathbf{w}$ occurring in the previous corollary indeed exists. For this purpose, we first begin with the following lemma which shows that if n is large enough and $N \geq V(n,\ell-1)+1$, then there exists an output word $\mathbf{y} \in Y$ such that $\mathbf{y}$ differs from the transmitted codeword $\mathbf{x}$ in at least $\ell-1$ coordinate places outside a small set of restricted coordinates (the set $\overline{D}$ in the lemma). Observe that $\mathrm{supp}(\mathbf{a}+\mathbf{b})$ denotes the set of coordinates in which the words $\mathbf{a}$ and $\mathbf{b}$ differ. Moreover, we have $d(\mathbf{a},\mathbf{b}) = |\mathrm{supp}(\mathbf{a}+\mathbf{b})|$.

Lemma 13. *Assume that $Y \subseteq \mathbb{F}^n$, $|Y| = N \geq V(n,\ell-1)+1$, C is an e-error-correcting code and b is a positive integer. If $n \geq \ell-2+(\ell-1)^2 2^b$, then for any codeword $\mathbf{c} \in T(Y)$ and for any set $\overline{D} \subseteq [1,n]$ with $|\overline{D}| = b$, there exists a word $\mathbf{y} \in Y$ such that*

$$|\mathit{supp}(\mathbf{c}+\mathbf{y}) \setminus \overline{D}| \geq \ell-1.$$

Proof. Let $\overline{D} \subseteq [1,n]$ and $|\overline{D}| = b$ for some fixed b. Without loss of generality, we may assume that $\mathbf{c} = \mathbf{0}$. Suppose to the contrary that there does not exist a word $\mathbf{y} \in Y$ such that $|\mathrm{supp}(\mathbf{c}+\mathbf{y}) \setminus \overline{D}| = |\mathrm{supp}(\mathbf{y}) \setminus \overline{D}| \geq \ell-1$, i.e., $|\mathrm{supp}(\mathbf{y}) \setminus \overline{D}| < \ell-1$ for all $\mathbf{y} \in Y$. This implies that the number of words in

Y is at most

$$\begin{aligned}&\sum_{j=0}^{\ell-2}\sum_{i=0}^{\min\{b,t-j\}}\binom{b}{i}\binom{n-b}{j}\\ \le&\sum_{j=0}^{\ell-2}\sum_{i=0}^{b}\binom{b}{i}\binom{n-b}{j}\\ =&2^b\sum_{j=0}^{\ell-2}\binom{n-b}{j}\\ \le&(\ell-1)2^b\binom{n}{\ell-2}\\ =&(\ell-1)\binom{n}{\ell-1}\frac{\ell-1}{n-\ell+2}2^b\\ \le&\binom{n}{\ell-1},\end{aligned}$$

when $n \geq \ell-2+(\ell-1)^2 2^b$. This contradicts with the assumption that $N = |Y| \geq V(n,\ell-1)+1$. Thus, the claim follows. □

In the following lemma, we show that if n is large enough and $N \geq V(n,\ell-1)+1$, then the pairwise distances of codewords in T are rather small.

Lemma 14. *Let $n \geq \ell-2+(\ell-1)^2 2^{2t}$, C be an e-error-correcting code and $|Y| = N \geq V(n,\ell-1)+1$. Then we have $d(\mathbf{c}_1,\mathbf{c}_2) \leq 2e+2$ for any two $\mathbf{c}_1,\mathbf{c}_2 \in T(Y)$.*

Proof. Let $\mathbf{c}_1$ and $\mathbf{c}_2$ be codewords in $T(Y)$. Without loss of generality, we may assume that $\mathbf{c}_1 = \mathbf{0}$. In order to show that $d(\mathbf{c}_1,\mathbf{c}_2) \leq 2e+2$, we suppose to the contrary that $d(\mathbf{c}_1,\mathbf{c}_2) \geq 2e+3$, i.e., $w(\mathbf{c}_2) \geq 2e+3$. Since $\mathbf{c}_1,\mathbf{c}_2 \in T(Y)$, we have $w(\mathbf{c}_2) = d(\mathbf{c}_1,\mathbf{c}_2) \leq 2t$. Hence, there exists a set $\overline{D} \subseteq [1,n]$ such that $|\overline{D}| = 2t$ and $\mathrm{supp}(\mathbf{c}_2) \subseteq \overline{D}$.

Since $n \geq \ell-2+(\ell-1)^2 2^{2t}$, by Lemma 13, there exists an output $\mathbf{y} \in Y$ such that $|\mathrm{supp}(\mathbf{y}) \setminus \mathrm{supp}(\mathbf{c}_2)| \geq \ell-1$. Since $w(\mathbf{y}) = d(\mathbf{y},\mathbf{c}_1) \leq t$, we have $|\mathrm{supp}(\mathbf{c}_2) \cap \mathrm{supp}(\mathbf{y})| \leq e+1$; indeed, if $|\mathrm{supp}(\mathbf{c}_2) \cap \mathrm{supp}(\mathbf{y})| \geq e+2$, then $w(\mathbf{y}) = |\mathrm{supp}(\mathbf{c}_2) \cap \mathrm{supp}(\mathbf{y})| + |\mathrm{supp}(\mathbf{y}) \setminus \mathrm{supp}(\mathbf{c}_2)| \geq (e+2)+(\ell-1) = t+1$ (a contradiction). This further implies that

$$\begin{aligned}d(\mathbf{c}_2,\mathbf{y}) &\geq (w(\mathbf{c}_2) - |\mathrm{supp}(\mathbf{c}_2) \cap \mathrm{supp}(\mathbf{y})|) + \ell - 1\\ &\geq (2e+3-(e+1)) + \ell - 1 = t+1.\end{aligned}$$

This leads to a contradiction, and the claim follows. □

Recall that if C is an e-error-correcting code, then the pairwise distance of any codewords of C is at least $2e+1$. By the previous lemma, we also know that for any two codewords in $T(Y)$ the distance is at most $2e+2$ when $|Y| = N \geq V(n,\ell-1)+1$ and n is large enough. In the following lemma, we discuss a couple of useful properties for such codewords. For the lemma, notice that the word $\mathbf{w}$ in (i) can also be viewed as obtained by majority voting on the coordinates of the codewords $\mathbf{c}_0$, $\mathbf{c}_1$ and $\mathbf{c}_2$.

Lemma 15. *Let C be a code and $\mathbf{c}_0$, $\mathbf{c}_1$ and $\mathbf{c}_2$ be codewords of C such that $2e+1 \leq d(\mathbf{c}_i,\mathbf{c}_j) \leq 2e+2$ for any distinct $i,j \in \{0,1,2\}$.*

(i) If the word $\mathbf{w} \in \mathbb{F}^n$ is such that supp$(\mathbf{w}+\mathbf{c}_0) =$ supp$(\mathbf{c}_0+\mathbf{c}_1) \cap$ supp$(\mathbf{c}_0+\mathbf{c}_2)$, then $|$supp$(\mathbf{w}+\mathbf{c}_i)| = d(\mathbf{w},\mathbf{c}_i) \leq e+1$ for any $i \in \{0,1,2\}$.

(ii) If there exists a word $\mathbf{y} \in \mathbb{F}^n$ such that $\mathbf{c}_0,\mathbf{c}_1,\mathbf{c}_2 \in B_t(\mathbf{y})$ and $|$supp$(\mathbf{y}+\mathbf{c}_0) \setminus ($supp$(\mathbf{c}_0+\mathbf{c}_1) \cup$ supp$(\mathbf{c}_0+\mathbf{c}_2))| \geq \ell-1$, then supp$(\mathbf{y}+\mathbf{c}_0) \cap$ supp$(\mathbf{c}_0+\mathbf{c}_1) =$ supp$(\mathbf{y}+\mathbf{c}_0) \cap$ supp$(\mathbf{c}_0+\mathbf{c}_2) =$ supp$(\mathbf{c}_0+\mathbf{c}_1) \cap$ supp$(\mathbf{c}_0+\mathbf{c}_2)$.

Proof. Recall first that for any $\mathbf{z} \in \mathbb{F}^n$ the support $\mathrm{supp}(\mathbf{c}_0+\mathbf{z})$ consists of the coordinate places in which $\mathbf{c}_0$ and $\mathbf{z}$ differ. Therefore, we may without loss of generality assume that $\mathbf{c}_0 = \mathbf{0}$ (as the whole Hamming space can be translated by $\mathbf{c}_0$). Denote now $A = \mathrm{supp}(\mathbf{c}_0+\mathbf{c}_1) \cap \mathrm{supp}(\mathbf{c}_0+\mathbf{c}_2) = \mathrm{supp}(\mathbf{c}_1) \cap \mathrm{supp}(\mathbf{c}_2)$, and let $\mathbf{w} \in \mathbb{F}^n$ be the word such that $\mathrm{supp}(\mathbf{w}) = A$. Let $\mathbf{y} \in \mathbb{F}^n$ be a word such that $|\mathrm{supp}(\mathbf{y}) \setminus (\mathrm{supp}(\mathbf{c}_0+\mathbf{c}_1) \cup \mathrm{supp}(\mathbf{c}_0+\mathbf{c}_2))| \geq \ell-1$. This implies that

$$\begin{aligned}&|\mathrm{supp}(\mathbf{y}) \cap \mathrm{supp}(\mathbf{c}_i)|\\ \leq&|\mathrm{supp}(\mathbf{y}) \cap (\mathrm{supp}(\mathbf{c}_1) \cup \mathrm{supp}(\mathbf{c}_2))| \qquad (4)\\ \leq&e+1 \text{ for } i \in \{1,2\}\end{aligned}$$

since otherwise $w(\mathbf{y}) \geq |\mathrm{supp}(\mathbf{y}) \cap (\mathrm{supp}(\mathbf{c}_1) \cup \mathrm{supp}(\mathbf{c}_2))| + |\mathrm{supp}(\mathbf{y}) \setminus (\mathrm{supp}(\mathbf{c}_1) \cup \mathrm{supp}(\mathbf{c}_2))| \geq (e+2)+(\ell-1) = t+1$ contradicting with the assumption $w(\mathbf{y}) = d(\mathbf{y},\mathbf{c}_0) \leq t$. Observe further that the sum of the distances

$$\begin{aligned}&d(\mathbf{c}_0,\mathbf{c}_1)+d(\mathbf{c}_1,\mathbf{c}_2)+d(\mathbf{c}_2,\mathbf{c}_0)\\ =&2\sum_{i=0}^{2} w(\mathbf{c}_i) - 2|\mathrm{supp}(\mathbf{c}_0) \cap \mathrm{supp}(\mathbf{c}_1)| \qquad (5)\\ &-2|\mathrm{supp}(\mathbf{c}_1) \cap \mathrm{supp}(\mathbf{c}_2)| - 2|\mathrm{supp}(\mathbf{c}_2) \cap \mathrm{supp}(\mathbf{c}_0)|\end{aligned}$$

is even. Hence, we have two possibilities for the distances among the three codewords: either each of them equals $2e+2$ or exactly one of them equals $2e+2$.

Consider first the latter case. We have illustrated that case in Figure 3 for $e=2$, $\ell=3$ and $d(\mathbf{c}_1,\mathbf{c}_2) = 2e+2$. The proof now further divides into the following two cases:

- Assume first that $d(\mathbf{c}_1,\mathbf{c}_2) = 2e+2$. Then we have $d(\mathbf{c}_0,\mathbf{c}_1) = d(\mathbf{c}_0,\mathbf{c}_2) = 2e+1$, i.e., $w(\mathbf{c}_1) = w(\mathbf{c}_2) = 2e+1$. It is now immediate that $|A| = e$ and $|\mathrm{supp}(\mathbf{c}_i) \setminus A| = e+1$ for each $i \in \{1,2\}$. Hence, we clearly have

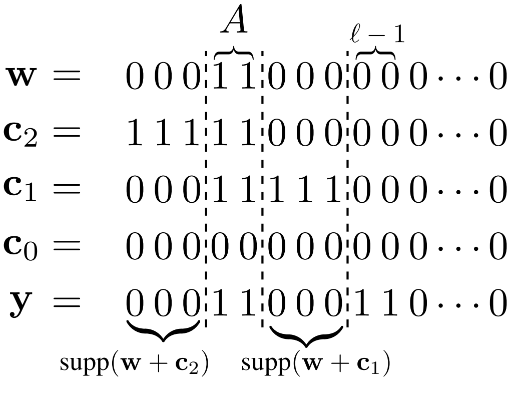
A
$\ell-1$
$\mathbf{w} =$ 0 0 0 1 1 0 0 0 0 0 0 ⋯ 0
$\mathbf{c}_2 =$ 1 1 1 1 1 0 0 0 0 0 0 ⋯ 0
$\mathbf{c}_1 =$ 0 0 0 1 1 1 1 1 0 0 0 ⋯ 0
$\mathbf{c}_0 =$ 0 0 0 0 0 0 0 0 0 0 0 ⋯ 0
$\mathbf{y} =$ 0 0 0 1 1 0 0 0 1 1 0 ⋯ 0
supp$(\mathbf{w}+\mathbf{c}_2)$
supp$(\mathbf{w}+\mathbf{c}_1)$

Fig. 3. Three codewords $\mathbf{c}_0$, $\mathbf{c}_1$ and $\mathbf{c}_2$ with $e=2$ and $\ell=3$. We have $d(\mathbf{w},\mathbf{c}_i) \leq e+1$ for $0 \leq i \leq 2$ and $A = \mathrm{supp}(\mathbf{c}_0+\mathbf{c}_1) \cap \mathrm{supp}(\mathbf{c}_0+\mathbf{c}_2)$.

$|\text{supp}(\mathbf{w}+\mathbf{c}_i)| = d(\mathbf{w},\mathbf{c}_i) \le e+1$ for $i \in \{0,1,2\}$, and the claim (i) follows.

Notice then that $|\text{supp}(\mathbf{y}) \cap \text{supp}(\mathbf{c}_i)| \ge e$ for $i \in \{1,2\}$ since otherwise $d(\mathbf{y},\mathbf{c}_i) \ge |\text{supp}(\mathbf{c}_i)\setminus\text{supp}(\mathbf{y})|+(\ell-1) \ge 2e+1-(e-1)+(\ell-1) = t+1$ (a contradiction). Therefore, by (4), we have $e \le |\text{supp}(\mathbf{y}) \cap \text{supp}(\mathbf{c}_i)| \le e+1$ for $i \in \{1,2\}$. Moreover, if $|\text{supp}(\mathbf{y}) \cap \text{supp}(\mathbf{c}_1)| = e+1$, then $d(\mathbf{y},\mathbf{c}_2) = |\text{supp}(\mathbf{y}) \setminus \text{supp}(\mathbf{c}_2)| + |\text{supp}(\mathbf{c}_2) \setminus \text{supp}(\mathbf{y})| \ge ((\ell-1)+1)+e+1 > t$ (a contradiction). Hence, using analogous arguments to $\mathbf{c}_2$, we obtain that

$$|\text{supp}(\mathbf{y}) \cap \text{supp}(\mathbf{c}_1)| = |\text{supp}(\mathbf{y}) \cap \text{supp}(\mathbf{c}_2)| = e.$$

Now it can be shown that $A = \text{supp}(\mathbf{y}+\mathbf{c}_0) \cap \text{supp}(\mathbf{c}_0+\mathbf{c}_1) = \text{supp}(\mathbf{y}) \cap \text{supp}(\mathbf{c}_1)$ and $A = \text{supp}(\mathbf{y}+\mathbf{c}_0) \cap \text{supp}(\mathbf{c}_0+\mathbf{c}_2) = \text{supp}(\mathbf{y}) \cap \text{supp}(\mathbf{c}_2)$. Indeed, suppose to the contrary that $\text{supp}(\mathbf{c}_1) \cap (\text{supp}(\mathbf{y}) \setminus A) \neq \emptyset$ or $\text{supp}(\mathbf{c}_2) \cap (\text{supp}(\mathbf{y}) \setminus A) \neq \emptyset$. Now a contradiction follows since $d(\mathbf{y},\mathbf{c}_2) = |\text{supp}(\mathbf{y}) \setminus \text{supp}(\mathbf{c}_2)| + |\text{supp}(\mathbf{c}_2) \setminus \text{supp}(\mathbf{y})| \ge (1+(\ell-1)) + |\text{supp}(\mathbf{c}_2) \setminus \text{supp}(\mathbf{y})| \ge \ell+(2e+1-e) = t+1$ or $d(\mathbf{y},\mathbf{c}_1) \ge t+1$, respectively. Thus, the claim (ii) follows.

- Assume then that $d(\mathbf{c}_0,\mathbf{c}_1) = w(\mathbf{c}_1) = 2e+2$. (The case with $d(\mathbf{c}_0,\mathbf{c}_2) = 2e+2$ is analogous.) Then we have $d(\mathbf{c}_0,\mathbf{c}_2) = w(\mathbf{c}_2) = 2e+1$ and $d(\mathbf{c}_1,\mathbf{c}_2) = 2e+1$. It is now immediate that $|A| = e+1$, $|\text{supp}(\mathbf{c}_1) \setminus A| = e+1$ and $|\text{supp}(\mathbf{c}_2) \setminus A| = e$. Hence, we obviously have $|\text{supp}(\mathbf{w}+\mathbf{c}_i)| = d(\mathbf{w},\mathbf{c}_i) \le e+1$ for $i \in \{0,1,2\}$, and the claim (i) follows.

  Notice then that $|\text{supp}(\mathbf{y}) \cap \text{supp}(\mathbf{c}_1)| \ge e+1$ and $|\text{supp}(\mathbf{y}) \cap \text{supp}(\mathbf{c}_2)| \ge e$, since otherwise $d(\mathbf{y},\mathbf{c}_1) \ge |\text{supp}(\mathbf{c}_1)\setminus\text{supp}(\mathbf{y})|+(\ell-1) \ge 2e+2-e+(\ell-1) = t+1$ and $d(\mathbf{y},\mathbf{c}_2) \ge |\text{supp}(\mathbf{c}_2)\setminus\text{supp}(\mathbf{y})|+(\ell-1) \ge 2e+1-(e-1)+(\ell-1) = t+1$, respectively (a contradiction). Together with (4), this implies that $|\text{supp}(\mathbf{y})\cap\text{supp}(\mathbf{c}_1)| = e+1$ and $e \le |\text{supp}(\mathbf{y}) \cap \text{supp}(\mathbf{c}_2)| \le e+1$. Now it can be shown that $A = \text{supp}(\mathbf{y}+\mathbf{c}_0) \cap \text{supp}(\mathbf{c}_0+\mathbf{c}_1) = \text{supp}(\mathbf{y}) \cap \text{supp}(\mathbf{c}_1)$. Indeed, suppose to the contrary that $\text{supp}(\mathbf{c}_1)\cap(\text{supp}(\mathbf{y})\setminus A) \neq \emptyset$. This implies that $|\text{supp}(\mathbf{y})\cap \text{supp}(\mathbf{c}_2)| = e$ (by (4)). Hence, a contradiction follows since $d(\mathbf{y},\mathbf{c}_2) = |\text{supp}(\mathbf{y}) \setminus \text{supp}(\mathbf{c}_2)| + |\text{supp}(\mathbf{c}_2) \setminus \text{supp}(\mathbf{y})| \ge (1+(\ell-1))+(2e+1-e) = t+1$. Therefore, we have $A = \text{supp}(\mathbf{y}) \cap \text{supp}(\mathbf{c}_1)$. Hence, we have $|\text{supp}(\mathbf{y})\cap\text{supp}(\mathbf{c}_2)| = e+1$ and $A = \text{supp}(\mathbf{y})\cap\text{supp}(\mathbf{c}_2)$. Thus, the claim (ii) follows.

Consider then the former case with $d(\mathbf{c}_0,\mathbf{c}_1) = d(\mathbf{c}_0,\mathbf{c}_2) = d(\mathbf{c}_1,\mathbf{c}_2) = 2e+2$; in particular, $w(\mathbf{c}_1) = w(\mathbf{c}_2) = 2e+2$. It is now immediate that $|A| = e+1$ and $|\text{supp}(\mathbf{c}_i) \setminus A| = e+1$ for each $i \in \{1,2\}$. Hence, we clearly have $|\text{supp}(\mathbf{w}+\mathbf{c}_i)| = d(\mathbf{w},\mathbf{c}_i) = e+1$ for $i \in \{0,1,2\}$, and the claim (i) follows.

Notice then that $|\text{supp}(\mathbf{y})\cap\text{supp}(\mathbf{c}_i)| \ge e+1$ for $i \in \{1,2\}$ since otherwise $d(\mathbf{y},\mathbf{c}_i) \ge |\text{supp}(\mathbf{c}_i) \setminus \text{supp}(\mathbf{y})| + (\ell-1) \ge 2e+2-e+(\ell-1) = t+1$ (a contradiction). Therefore, by (4), we have

$$\begin{aligned}&|\text{supp}(\mathbf{y}) \cap \text{supp}(\mathbf{c}_1)|\\ =&|\text{supp}(\mathbf{y}) \cap \text{supp}(\mathbf{c}_2)|\\ =&|\text{supp}(\mathbf{y}) \cap (\text{supp}(\mathbf{c}_1) \cup \text{supp}(\mathbf{c}_2))| = e+1.\end{aligned}$$

This immediately implies that $\text{supp}(\mathbf{y})\cap\text{supp}(\mathbf{c}_1) = \text{supp}(\mathbf{y})\cap(\text{supp}(\mathbf{c}_1) \cup \text{supp}(\mathbf{c}_2)) = \text{supp}(\mathbf{y}) \cap \text{supp}(\mathbf{c}_2)$. Therefore, as $|A| = |\text{supp}(\mathbf{c}_1) \cap \text{supp}(\mathbf{c}_2)| = |\text{supp}(\mathbf{y}) \cap \text{supp}(\mathbf{c}_1)| = |\text{supp}(\mathbf{y}) \cap \text{supp}(\mathbf{c}_2)| = e+1$, we have $A = \text{supp}(\mathbf{y}) \cap \text{supp}(\mathbf{c}_1) = \text{supp}(\mathbf{y}) \cap \text{supp}(\mathbf{c}_2)$. Thus, the claim (ii) follows. □

Before the proof of the (simpler) main theorem, we still need one auxiliary lemma which concerns the maximum size of union of supports of words relatively close to each other.

Lemma 16. *Let k be a positive integer. If $\mathbf{z}_0$, $\mathbf{z}_1$ and $\mathbf{z}_2$ are words of $\mathbb{F}^n$ such that $d(\mathbf{z}_i,\mathbf{z}_j) \le 2k$ for any distinct $i,j \in \{0,1,2\}$, then $|supp(\mathbf{z}_0+\mathbf{z}_1) \cup supp(\mathbf{z}_0+\mathbf{z}_2)| \le 3k$.*

Proof. Let $\mathbf{z}_0$, $\mathbf{z}_1$ and $\mathbf{z}_2$ be words of $\mathbb{F}^n$ such that $d(\mathbf{z}_i,\mathbf{z}_j) \le 2k$ for any distinct $i,j \in \{0,1,2\}$. Without loss of generality, we may assume that $\mathbf{z}_0 = \mathbf{0}$ since for $i \in \{1,2\}$ the support $\text{supp}(\mathbf{z}_0+\mathbf{z}_i)$ consists of the coordinate places in which $\mathbf{z}_0$ and $\mathbf{z}_i$ differ. The proof divides into two parts depending on the size of $\text{supp}(\mathbf{z}_1) \cap \text{supp}(\mathbf{z}_2)$:

- If $|\text{supp}(\mathbf{z}_1)\cap\text{supp}(\mathbf{z}_2)| \ge k+m$, where $m \in \{1,\dots,k\}$, then $|\text{supp}(\mathbf{z}_0+\mathbf{z}_1) \cup \text{supp}(\mathbf{z}_0+\mathbf{z}_2)| = |\text{supp}(\mathbf{z}_1) \cup \text{supp}(\mathbf{z}_2)| = |\text{supp}(\mathbf{z}_1)\setminus\text{supp}(\mathbf{z}_2)| + |\text{supp}(\mathbf{z}_2)\setminus\text{supp}(\mathbf{z}_1)| + |\text{supp}(\mathbf{z}_1)\cap\text{supp}(\mathbf{z}_2)| \le 2(k-m)+(k+m) = 3k-m$ (as $w(\mathbf{z}_1) \le 2k$ and $w(\mathbf{z}_2) \le 2k$) and the claim follows.
- If $|\text{supp}(\mathbf{z}_1)\cap\text{supp}(\mathbf{z}_2)| \le k$, then $|\text{supp}(\mathbf{z}_1)\cup\text{supp}(\mathbf{z}_2)| = (|\text{supp}(\mathbf{z}_1) \setminus \text{supp}(\mathbf{z}_2)| + |\text{supp}(\mathbf{z}_2) \setminus \text{supp}(\mathbf{z}_1)|) + |\text{supp}(\mathbf{z}_1) \cap \text{supp}(\mathbf{z}_2)| \le d(\mathbf{z}_1,\mathbf{z}_2) + k \le 2k+k = 3k$ and the claim follows.

□

In Corollary 12, we have shown that if there exists a word $\mathbf{w}$ such that it is close to every codeword in T, then $|T|$ is small. Furthermore, in Lemma 14, we have shown that every codeword in T is pairwise close to each other. Therefore, it seems that such a word $\mathbf{w}$ should indeed exist. The proof of the following theorem is based on this idea.

Theorem 17. *Let $n \ge \ell-2+(\ell-1)^2 2^b$, $b = \max\{2t, 4e+4\}$, $|Y| = N \ge V(n,\ell-1)+1$ and C be an e-error-correcting code. Then we have*

$$\mathcal{L} \le \ell+1.$$

Proof. Observe first that the cases $\ell = 0$ and $\ell = 1$ follow from Theorem 7 since $2^0 = 0+1$ and $2^1 = 1+1$. Therefore, we may assume that $\ell \ge 2$. Hence, there exist codewords $\mathbf{c}_0,\mathbf{c}_1,\mathbf{c}_2 \in T(Y)$ (as we are immediately done if $|T(Y)| \le 2$). Since C is an e-error-correcting code and $\mathbf{c}_0,\mathbf{c}_1,\mathbf{c}_2 \in C$, the distance $d(\mathbf{c}_i,\mathbf{c}_j) \ge 2e+1$ for any distinct $i,j \in \{0,1,2\}$. Therefore, as the conditions of Lemma 14 are satisfied due the choice of $b \ge 2t$ and n, we have

$$2e+1 \le d(\mathbf{c}_i,\mathbf{c}_j) \le 2e+2 \text{ for any distinct } i,j \in \{0,1,2\}. \tag{6}$$

Without loss of generality, we may assume that $\mathbf{c}_0 = \mathbf{0}$. Thus, we have $w(\mathbf{c}_1) = d(\mathbf{c}_0,\mathbf{c}_1)$ and $w(\mathbf{c}_2) = d(\mathbf{c}_0,\mathbf{c}_2)$. Let $\mathbf{w} \in \mathbb{F}^n$ be the word such that $\text{supp}(\mathbf{w}) = \text{supp}(\mathbf{c}_1)\cap\text{supp}(\mathbf{c}_2)$. By Lemma 15, we have $d(\mathbf{w},\mathbf{c}_i) \le e+1$ for any $i \in \{0,1,2\}$. Let $\mathbf{c}$ be an arbitrary codeword in $T(Y)$ different from $\mathbf{c}_i$, $i = 0,1,2$. In what follows, we show that also for $\mathbf{c}$ we have

$d(\mathbf{w}, \mathbf{c}) \leq e+1$. Thus, the word $\mathbf{w}$ can act as the one of Corollary 12.

Observe first that (as in (6)) we $2e+1 \leq d(\mathbf{c}, \mathbf{c}_i) \leq 2e+2$ for any $i \in \{0,1,2\}$. Moreover, if $|\text{supp}(\mathbf{c}) \setminus (\text{supp}(\mathbf{c}_1) \cup \text{supp}(\mathbf{c}_2))| \geq e+2$, then $|\text{supp}(\mathbf{c}_1) \setminus \text{supp}(\mathbf{c})| \geq e+1$ (as $|\text{supp}(\mathbf{c}_1) \cap \text{supp}(\mathbf{c})| \leq e$) and a contradiction follows as $d(\mathbf{c}_1, \mathbf{c}) \geq 2e+3$. Hence, we have $|\text{supp}(\mathbf{c}) \setminus (\text{supp}(\mathbf{c}_1) \cup \text{supp}(\mathbf{c}_2))| \leq e+1$. Furthermore, by Lemma 16, we have $|\text{supp}(\mathbf{c}_1) \cup \text{supp}(\mathbf{c}_2)| \leq 3e+3$. Thus, denoting $\overline{D} = \text{supp}(\mathbf{c}_1) \cup \text{supp}(\mathbf{c}_2) \cup \text{supp}(\mathbf{c})$, we have $|\overline{D}| \leq 4e+4$.

By Lemma 13 (as $b \geq 4e+4$), there exists an output word $\mathbf{y} \in Y$ such that $|\text{supp}(\mathbf{y}) \setminus \overline{D}| \geq \ell - 1$. (Observe that $\mathbf{y}$ depends on the choice of $\mathbf{c}$.) The word $\mathbf{y}$ satisfies the conditions of Lemma 15(ii) for the codewords $\mathbf{c}_0$, $\mathbf{c}_1$ and $\mathbf{c}_2$. Therefore, we have $\text{supp}(\mathbf{w}) = \text{supp}(\mathbf{c}_1) \cap \text{supp}(\mathbf{c}_2) = \text{supp}(\mathbf{y}) \cap \text{supp}(\mathbf{c}_1) = \text{supp}(\mathbf{y}) \cap \text{supp}(\mathbf{c}_2)$. Similarly, the word $\mathbf{y}$ satisfies the conditions of Lemma 15(ii) for the codewords $\mathbf{c}_0$, $\mathbf{c}_1$ and $\mathbf{c}$. Hence, we have $\text{supp}(\mathbf{c}_1) \cap \text{supp}(\mathbf{c}) = \text{supp}(\mathbf{y}) \cap \text{supp}(\mathbf{c}_1) = \text{supp}(\mathbf{y}) \cap \text{supp}(\mathbf{c})$. These two observations together imply that $\text{supp}(\mathbf{w}) = \text{supp}(\mathbf{c}_1) \cap \text{supp}(\mathbf{c})$. Thus, by Lemma 15(i), we have $d(\mathbf{w}, \mathbf{c}) \leq e+1$ concluding the proof. □

In the previous theorem, we have shown that $\mathcal{L} \leq \ell + 1$ when n depends exponentially on e and ℓ. The proof utilizes Lemma 13, in which we use rather rough estimations. In what follows, we significantly improve the previous theorem by showing that it is enough to require n to depend only polynomially on e and ℓ. We first present an improved version of Lemma 13. The proof of the improved lemma is rather technical and, therefore, it is postponed to Appendix.

Lemma 18. *Let $b \geq 3t$ be an integer with $t = e + \ell$ and C_1 be an e-error-correcting code. Assume that $n \geq (\ell-1)^2(b - e + (e+1)(b - 3e - 2e^2 + eb + \binom{b-2e-1}{2})) + \ell - 2$, $|Y| = N \geq V(n, \ell-1) + 1$, $|T(Y)| \geq 3$ and $\mathbf{c}_0, \mathbf{c}_1, \mathbf{c}_2 \in T(Y)$. If now $\overline{D} \subseteq [1,n]$ is a set such that $|\overline{D}| = b$ and*

$$\textit{supp}(\mathbf{c}_0 + \mathbf{c}_1) \cup \textit{supp}(\mathbf{c}_0 + \mathbf{c}_2) \cup \textit{supp}(\mathbf{c}_1 + \mathbf{c}_2) \subseteq \overline{D},$$

then for any word $\mathbf{w} \in \mathbb{F}^n$ we have $\textit{supp}(\mathbf{w} + \mathbf{c}_0) \setminus \overline{D} = \textit{supp}(\mathbf{w} + \mathbf{c}_1) \setminus \overline{D} = \textit{supp}(\mathbf{w} + \mathbf{c}_2) \setminus \overline{D}$ and there exists an output word $\mathbf{y} \in Y$ such that

$$|\textit{supp}(\mathbf{y} + \mathbf{c}_0) \setminus \overline{D}| \geq \ell - 1.$$

Proof. See Appendix. □

Using the previous lemma, we show a result similar to Lemma 14.

Lemma 19. *Let $n \geq (\ell-1)^2(2t + \ell + (e+1)(3\ell - 2e^2 + 3et + \binom{t+2\ell-1}{2})) + \ell - 2$, $|Y| = N \geq V(n, \ell-1) + 1$, C be an e-error-correcting code and $|T(Y)| \geq 3$. Then we have $d(\mathbf{c}_1, \mathbf{c}_2) \leq 2e+2$ for any two $\mathbf{c}_1, \mathbf{c}_2 \in T(Y)$.*

Proof. The proof is similar to the one of Lemma 14. Let $\mathbf{c}_1$ and $\mathbf{c}_2$ be distinct codewords in $T(Y)$ ($|T(Y)| \geq 3$). Without loss of generality, we may assume that $\mathbf{c}_1 = \mathbf{0}$. In order to show that $d(\mathbf{c}_1, \mathbf{c}_2) \leq 2e+2$, we suppose to the contrary that $d(\mathbf{c}_1, \mathbf{c}_2) \geq 2e+3$, i.e., $w(\mathbf{c}_2) \geq 2e+3$. Since $|T(Y)| \geq 3$, there exists another codeword $\mathbf{c}_3 \in T(Y)$. Recall that $d(\mathbf{c}_i, \mathbf{c}_j) \leq 2t$ for any distinct $i, j \in \{1,2,3\}$. Therefore, by Lemma 16, we have $|\text{supp}(\mathbf{c}_1 + \mathbf{c}_2) \cup \text{supp}(\mathbf{c}_1 + \mathbf{c}_3) \cup \text{supp}(\mathbf{c}_2 + \mathbf{c}_3)| = |\text{supp}(\mathbf{c}_2) \cup \text{supp}(\mathbf{c}_3) \cup \text{supp}(\mathbf{c}_2 + \mathbf{c}_3)| = |\text{supp}(\mathbf{c}_2) \cup \text{supp}(\mathbf{c}_3)| \leq 3t$. Hence, there exists a set $\overline{D} \subseteq [1,n]$ such that $|\overline{D}| = b = 3t$ and $\text{supp}(\mathbf{c}_2) \subseteq \text{supp}(\mathbf{c}_1 + \mathbf{c}_2) \cup \text{supp}(\mathbf{c}_1 + \mathbf{c}_3) \cup \text{supp}(\mathbf{c}_2 + \mathbf{c}_3) \subseteq \overline{D}$.

Since $n \geq (\ell-1)^2(2t + \ell + (e+1)(3\ell - 2e^2 + 3et + \binom{t+2\ell-1}{2})) + \ell - 2 = (\ell-1)^2(b - e + (e+1)(b - 3e - 2e^2 + eb + \binom{b-2e-1}{2})) + \ell - 2$, by Lemma 18, there exists an output word $\mathbf{y} \in Y$ such that $|\text{supp}(\mathbf{y}) \setminus \text{supp}(\mathbf{c}_2)| \geq |\text{supp}(\mathbf{y}) \setminus \overline{D}| \geq \ell - 1$. Since $w(\mathbf{y}) = d(\mathbf{y}, \mathbf{c}_1) \leq t$, we have $|\text{supp}(\mathbf{c}_2) \cap \text{supp}(\mathbf{y})| \leq e+1$ as otherwise $w(\mathbf{y}) = |\text{supp}(\mathbf{y}) \setminus \text{supp}(\mathbf{c}_2)| + |\text{supp}(\mathbf{c}_2) \cap \text{supp}(\mathbf{y})| \geq (\ell - 1) + (e+2) = t+1$ (a contradiction). This further implies that

$$\begin{aligned} d(\mathbf{c}_2, \mathbf{y}) &\geq (w(\mathbf{c}_2) - |\text{supp}(\mathbf{c}_2) \cap \text{supp}(\mathbf{y})|) + \ell - 1 \\ &\geq (2e + 3 - (e+1)) + \ell - 1 \geq t + 1. \end{aligned}$$

This leads to a contradiction, and the claim follows. □

The following theorem is an improved version of Theorem 17; a version in which n is only required to depend polynomially on e and ℓ. Notice that in some (sporadic) cases Theorem 17 is better than Theorem 20.

Theorem 20. *Let $n \geq (\ell-1)^2(b - e + (e+1)(b - 3e - 2e^2 + eb + \binom{b-2e-1}{2})) + \ell - 2$, $b = \max\{3t, 4e+4\}$, $|Y| = N \geq V(n, \ell-1) + 1$ and C be an e-error-correcting code. Then we have*

$$\mathcal{L} \leq \ell + 1.$$

Proof. As in the proof of Theorem 17, we may assume that $\ell \geq 2$ and that there exist codewords $\mathbf{c}_0, \mathbf{c}_1, \mathbf{c}_2 \in T(Y)$. Since C is an e-error-correcting code and $\mathbf{c}_0, \mathbf{c}_1, \mathbf{c}_2 \in C$, the distance $d(\mathbf{c}_i, \mathbf{c}_j) \geq 2e+1$ for any distinct $i, j \in \{0,1,2\}$. Together with Lemma 19 (due to the choice of $b \geq 3t$ and n), this implies that

$$2e + 1 \leq d(\mathbf{c}_i, \mathbf{c}_j) \leq 2e+2 \text{ for any distinct } i, j \in \{0,1,2\}. \tag{7}$$

Without loss of generality, we may assume that $\mathbf{c}_0 = \mathbf{0}$. Thus, we have $w(\mathbf{c}_1) = d(\mathbf{c}_0, \mathbf{c}_1)$ and $w(\mathbf{c}_2) = d(\mathbf{c}_0, \mathbf{c}_2)$. Let $\mathbf{w} \in \mathbb{F}^n$ be a word such that $\text{supp}(\mathbf{w}) = \text{supp}(\mathbf{c}_1) \cap \text{supp}(\mathbf{c}_2)$. By Lemma 15, we have $d(\mathbf{w}, \mathbf{c}_i) \leq e+1$ for any $i \in \{0,1,2\}$. Let $\mathbf{c}$ be an arbitrary codeword in $T(Y)$. Next, we show that also for $\mathbf{c}$ we have $d(\mathbf{w}, \mathbf{c}) \leq e+1$. Therefore, the word $\mathbf{w}$ for Corollary 12 is found.

Clearly, (as in (7)) we have $2e+1 \leq d(\mathbf{c}, \mathbf{c}_i) \leq 2e+2$ for any $i \in \{0,1,2\}$. Furthermore, if $|\text{supp}(\mathbf{c}) \setminus (\text{supp}(\mathbf{c}_1) \cup \text{supp}(\mathbf{c}_2))| \geq e+2$, then $|\text{supp}(\mathbf{c}_1) \setminus \text{supp}(\mathbf{c})| \geq e+1$ and a contradiction follows as $d(\mathbf{c}_1, \mathbf{c}) \geq 2e+3$. Thus, we have $|\text{supp}(\mathbf{c}) \setminus (\text{supp}(\mathbf{c}_1) \cup \text{supp}(\mathbf{c}_2))| \leq e+1$. Moreover, by Lemma 16, we have $|\text{supp}(\mathbf{c}_1) \cup \text{supp}(\mathbf{c}_2)| \leq 3e+3$. Hence, denoting $\overline{D} = \text{supp}(\mathbf{c}_1) \cup \text{supp}(\mathbf{c}_2) \cup \text{supp}(\mathbf{c})$, we have $|\overline{D}| \leq 4e+4$.

The requirements for b and n as well as the additional requirement $\text{supp}(\mathbf{c}_0 + \mathbf{c}_1) \cup \text{supp}(\mathbf{c}_0 + \mathbf{c}_2) \cup \text{supp}(\mathbf{c}_1 + \mathbf{c}_2) \subseteq \overline{D} = \text{supp}(\mathbf{c}_0) \cup \text{supp}(\mathbf{c}_1) \cup \text{supp}(\mathbf{c}_2)$ of Lemma 18 are clearly satisfied. Thus, there exists an output word $\mathbf{y} \in Y$ such that $|\text{supp}(\mathbf{y}) \setminus \overline{D}| \geq \ell - 1$. The word $\mathbf{y}$ satisfies the conditions of Lemma 15(ii) for the codewords $\mathbf{c}_0$, $\mathbf{c}_1$ and

$\mathbf{c}_2$. Hence, we have $\mathrm{supp}(\mathbf{w}) = \mathrm{supp}(\mathbf{c}_1) \cap \mathrm{supp}(\mathbf{c}_2) = \mathrm{supp}(\mathbf{y}) \cap \mathrm{supp}(\mathbf{c}_1) = \mathrm{supp}(\mathbf{y}) \cap \mathrm{supp}(\mathbf{c}_2)$. Similarly, the word $\mathbf{y}$ satisfies the conditions of Lemma 15(ii) for the codewords $\mathbf{c}_0$, $\mathbf{c}_1$ and $\mathbf{c}$. Therefore, we have $\mathrm{supp}(\mathbf{c}_1) \cap \mathrm{supp}(\mathbf{c}) = \mathrm{supp}(\mathbf{y}) \cap \mathrm{supp}(\mathbf{c}_1) = \mathrm{supp}(\mathbf{y}) \cap \mathrm{supp}(\mathbf{c})$. Together these two observations imply that $\mathrm{supp}(\mathbf{w}) = \mathrm{supp}(\mathbf{c}_1) \cap \mathrm{supp}(\mathbf{c})$. Hence, by Lemma 15(i), we have $d(\mathbf{w}, \mathbf{c}) \leq e + 1$ giving the assertion. □

Notice that Theorem 7 gives similar results as Theorem 17 and Theorem 20 in the case $\ell = 1$. In the following remark, we show that in order to have $\mathcal{L} \leq \ell + 1$ when C is an e-error-correcting and $N = V(n, \ell - 1) + 1$ some restrictions are needed on the values n, ℓ and e.

TABLE I
A POSSIBLE SET OF EIGHT OUTPUT WORDS WITH LIST SIZE $|T| = 2^\ell$.

		$d(\mathbf{c}_1, *)$	$d(\mathbf{c}_2, *)$	$d(\mathbf{c}_3, *)$	$d(\mathbf{c}_0, *)$
$\mathbf{c}_1$	011100	0	4	4	3
$\mathbf{c}_2$	101010	4	0	4	3
$\mathbf{c}_3$	110001	4	4	0	3
$\mathbf{c}_0$	000000	3	3	3	0
$\mathbf{y}_0$	000000	3	3	3	0
$\mathbf{y}_1$	111000	2	2	2	3
$\mathbf{y}_2$	011000	1	3	3	2
$\mathbf{y}_3$	101000	3	1	3	2
$\mathbf{y}_4$	110000	3	3	1	2
$\mathbf{y}_5$	100100	3	3	3	2
$\mathbf{y}_6$	010010	3	3	3	2
$\mathbf{y}_7$	001001	3	3	3	2

Remark 21. In what follows, we give a couple of examples of e-error-correcting codes such that $\mathcal{L} > \ell + 1$ when the number of channels $N \leq V(n, \ell - 1) + 1$. Consider first a code $C = \{\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \mathbf{c}_0\} \subseteq \mathbb{F}^6$ and a set of outputs $Y = \{\mathbf{y}_0, \dots, \mathbf{y}_7\} \subseteq \mathbb{F}^6$ given in Table I. By the table, we observe that C is a code with minimum distance 3 and, hence, it is a 1-error-correcting code. Assume $\mathbf{x} = \mathbf{c}_0 = \mathbf{0}$ is the transmitted word. Then notice by the table that $Y \subseteq B_3(\mathbf{x})$. Thus, with $e = 1$, $\ell = 2$ and $t = 3$, the set Y is a possible set of output words for $\mathbf{x}$. Therefore, as $\{\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \mathbf{c}_0\} \subseteq \bigcap_{j=0}^{7} B_3(\mathbf{y}_j)$, we have $|T| = 4 > \ell + 1 = 3$ with $|Y| = V(n, \ell - 1) + 1 = 8$. Hence, $\mathcal{L} > \ell + 1$.

Another example is the extreme situation with $e = 0$, $C = \mathbb{F}^n$, $\ell = n$ and $N = V(n, \ell - 1) + 1 = 2^n$. In this case, we have $B_t(\mathbf{y}) = \mathbb{F}^n$ for every $\mathbf{y} \in Y$. Therefore, we obtain that $\bigcap_{\mathbf{y} \in Y} B_t(\mathbf{y}) = \mathbb{F}^n = C$. Thus, $\mathcal{L} = 2^\ell > \ell + 1$ with $N = V(n, \ell - 1) + 1$.

Notice also that the previous examples attain the upper bound $\mathcal{L} \leq 2^\ell$ of Theorem 7.

IV. SMALL LIST SIZE WITH DISTANT OUTPUT WORDS

Throughout the section, we assume that the errors occurring in the transmission are uniformly and (almost) randomly distributed with the exception that no two output words are identical. We have previously assumed that we have at least $V(n, \ell - 1) + 1$ channels. However, as we will see in this section, it is very likely that such a large number of channels is unnecessary to get a small list size if n is large and e is sufficiently large compared to ℓ. Indeed, it is very likely that we have two words among the outputs such that they give a small list. In other words, although $\mathcal{L}$ might be large, $|T(Y)|$ is very likely small.

First in Subsection IV-A, we show that we are very likely to either have two distant output words or to have $|T| = 1$. After that, in Subsection IV-B, we use this observation together with bounds on constant weight codes to derive bounds for $|T|$. In Corollary 28, we show that if $e \geq 4\ell - 2$, then distant output words give $|T| \leq 2$. Similarly, we derive bounds for $|T|$ in Corollaries 29 and 30 for cases with $e \geq 3\ell - 2$ and $e \geq 2\ell - 1$, respectively. Notice that these results are improvements on the results in the conference version of this paper [1].

A. Likelihood of distant output words

Let C be an e-error-correcting code and $\mathbf{x} \in C$ be the transmitted word. In the following theorem, we see that if we have an output word $\mathbf{y}$ in the vicinity of $\mathbf{x}$, then there cannot be any other codewords in $B_t(\mathbf{y})$, thus, giving us exact knowledge about the transmitted word.

Theorem 22. *Let C be an e-error-correcting code in $\mathbb{F}^n$ and $\mathbf{x} \in C$. If $t = e + \ell$ and $d(\mathbf{x}, \mathbf{y}) \leq e - \ell$ for some output word $\mathbf{y} \in Y$, then we have $B_t(\mathbf{y}) \cap C = \{\mathbf{x}\}$ and $\mathbf{x}$ is the transmitted word.*

Proof. Let $\mathbf{x} \in C$ and $d(\mathbf{x}, \mathbf{y}) \leq e - \ell$ for some $\mathbf{y} \in Y$. Furthermore, we have $d(\mathbf{x}, \mathbf{c}) \geq 2e + 1$ for every codeword $\mathbf{c} \in C$, $\mathbf{c} \neq \mathbf{x}$. Hence, if we have $d(\mathbf{x}, \mathbf{y}) \leq e - \ell$, then the triangular inequality gives us

$$2e + 1 \leq d(\mathbf{x}, \mathbf{c}) \leq d(\mathbf{x}, \mathbf{y}) + d(\mathbf{y}, \mathbf{c}) \leq e - \ell + d(\mathbf{y}, \mathbf{c}).$$

Thus, we have $d(\mathbf{y}, \mathbf{c}) \geq t + 1$ for each $\mathbf{c} \in C$, $\mathbf{c} \neq \mathbf{x}$. Therefore, $B_t(\mathbf{y}) \cap C = \{\mathbf{x}\}$. Moreover, at most t errors occur in each channel and hence, the transmitted word is in $B_t(\mathbf{y}) \cap C$. Thus, $\mathbf{x}$ is the transmitted word and the claim follows. □

Now we are going to show that if n is large, then we very likely have two pairwise distant output words.

Theorem 23. *Let C be an e-error-correcting code in $\mathbb{F}^n$ and $\mathbf{x} \in C$ be the transmitted word. If $t = e + \ell$ and $\mathbf{y}_1, \mathbf{y}_2 \in Y$ are output words such that $d(\mathbf{y}_i, \mathbf{x}) \geq e - \ell + 1$ for $i = 1, 2$, then the probability that $d(\mathbf{y}_1, \mathbf{y}_2) \geq 2e - 2\ell + 2$ tends to 1 as n tends to infinity.*

Proof. Let us assume, without loss of generality, that $\mathbf{x} = \mathbf{0}$, $w(\mathbf{y}_1) = e - \ell + a_1$ and $w(\mathbf{y}_2) = e - \ell + a_2$ where $1 \leq a_2 \leq a_1 \leq 2\ell$. We encourage the reader to assume that $\mathrm{supp}(\mathbf{y}_1) = [1, e - \ell + a_1]$ in order to better visualize the proof. Observe that if $|\mathrm{supp}(\mathbf{y}_1) \cap \mathrm{supp}(\mathbf{y}_2)| \leq \frac{a_1 + a_2}{2} - 1$, then we have $d(\mathbf{y}_1, \mathbf{y}_2) = w(\mathbf{y}_1) + w(\mathbf{y}_2) - 2|\mathrm{supp}(\mathbf{y}_1) \cap \mathrm{supp}(\mathbf{y}_2)| \geq w(\mathbf{y}_1) + w(\mathbf{y}_2) - (a_1 + a_2 - 2) = 2e - 2\ell + 2$. Notice that $\frac{a_1 + a_2}{2} - 1 \geq 0$ since $a_1 \geq a_2 \geq 1$. Let us denote by

$P_n(a_1, a_2)$ the probability that $d(\mathbf{y}_1, \mathbf{y}_2) \geq 2e - 2\ell + 2$, i.e., $|\text{supp}(\mathbf{y}_1) \cap \text{supp}(\mathbf{y}_2)| \leq (a_1 + a_2)/2 - 1$. Now, we have

$$\begin{aligned}
P_n(a_1, a_2) &\geq \sum_{i=0}^{\lfloor \frac{a_1+a_2}{2} - 1 \rfloor} \frac{\binom{e-\ell+a_1}{i}\binom{n-e+\ell-a_1}{e-\ell+a_2-i}}{\binom{n}{e-\ell+a_2}} \\
&\geq \frac{\binom{n-e+\ell-a_1}{e-\ell+a_2}}{\binom{n}{e-\ell+a_2}} \\
&= \prod_{i=0}^{e-\ell+a_2-1} \frac{n - e + \ell - a_1 - i}{n - i} \overset{n\to\infty}{\longrightarrow} 1.
\end{aligned}$$

Since $P_n(a_1, a_2) \overset{n\to\infty}{\longrightarrow} 1$ for each possible value of a_1 and a_2, the claim follows. □

Now, based on Theorems 22 and 23, we obtain that if n is large, $e \geq \ell$ and we have at least two output words in Y, then we either have $|T(Y)| = 1$ or we are very likely to have two output words which are far away from each other. Furthermore, we only consider two output words in this section. However, if we have more output words, say m, and none of them is close to the transmitted word $\mathbf{x}$, then the likelihood that at least two of them are distant is naturally greater than we would have with only two output words. More precisely, the probability is greater than $1 - \prod_{i=2}^{m}(1 - P_n(a_1, a_i))$.

Note that quite modest n is enough for this approach to work; especially, if we have multiple channels. For example, assuming $n = 250$, $e = 10$ and $\ell = 3$, we have $P(a_1, a_2) \geq 0.768$ if $a_1 = a_2 = 1$ and $N = 2$. However, if we have $a_1 = a_2 = 4$ and $N = 2$, then $P(a_1, a_2) \geq 0.999$ or if $a_i = 1$ for $i \in [1, N]$, then $1 - \prod_{i=2}^{N}(1 - P_n(a_1, a_i)) \geq 1 - 0.232^{N-1}$.

B. List size with distant output words

We have discussed about the likelihood of having distant output words in IV-A. In this section, we use the assumption that there are two distant output words to give small list sizes. In what follows, we use known results for codes with a given minimum distance to obtain upper bounds on the outputted list of codewords. As usual, we denote by $A(n, d)$ the maximal cardinality among all codes in $\mathbb{F}^n$ with minimum distance at least d. Similarly, we denote by $A(n, d, w)$ the maximal cardinality among all *constant weight codes* in $\mathbb{F}^n$, in which each codeword has weight w and of which minimum distance is d. The maximum cardinalities $A(n, d)$ and $A(n, d, w)$ have been widely studied. In what follows, we first present some useful results regarding them. In the following theorem, the well-known Plotkin bound on $A(n, d)$ is given.

Theorem 24 (Plotkin bound [22]). *If $n < 2d + 1$ and d is odd, then*

$$A(n, d) \leq 2 \left\lfloor \frac{d + 1}{2d + 1 - n} \right\rfloor .$$

In the following theorem, we give some useful bounds on $A(n, d, w)$ from [23]. Inequality (i) immediately follows from the definitions of $A(n, d)$ and $A(n, d, w)$. Inequalities (ii), (iii) and (iv) have been shown in [23, Theorem 8], [23, Corollary 5] and [23, Theorem 12], respectively.

Theorem 25 ([23]). *We have*

(i) $A(n, d, w) \leq A(n, d)$,

(ii) $A(n, 2\delta - 1, w) = A(n, 2\delta, w)$,

(iii) $A(n, 2\delta, w) \leq \left\lfloor \frac{\delta}{b} \right\rfloor$, *if* $b \geq \frac{\delta}{n}$ *where* $b = \delta - \frac{w(n-w)}{n}$ *and*

(iv) $A(n, 2\delta, w) \leq \frac{\binom{n}{k}}{\binom{w}{k}}$ *where* $k = w - \delta + 1$.

$$\begin{array}{rl}
\mathbf{c} = & \overbrace{1\,1}^{S_{\mathbf{c}}}\,0\,0\,0\,0\,\overbrace{1\,1}^{A_{\mathbf{c}}}\,0\cdots 0 \\
\mathbf{y} = & 1\,1\,1\,1\,1\,1\,0\,0\,0\cdots 0 \\
\mathbf{y_c} = & 1\,1\,\underbrace{0}_{V_{\mathbf{c}}}\,0\,0\,0\,0\,0\,0\cdots 0 \\
\mathbf{y}_0 = & 0\,0\,0\,0\,0\,0\,0\,0\,0\cdots 0
\end{array}$$

Fig. 4. Two output words at distance 6 when $e = 4$, $\ell = 2$ and $a = 0$. Notice that $d(\mathbf{y}, \mathbf{y_c}) = 4 = w(\mathbf{y})/2 + V_{\mathbf{c}}$ and $d(\mathbf{y}_0, \mathbf{y_c}) = 2 = w(\mathbf{y})/2 - V_{\mathbf{c}}$. Moreover, it is easy to observe that $A_{\mathbf{c}}$ is maximal since $d(\mathbf{y}, \mathbf{c}) \leq t = 6$.

In the following theorem, we establish an upper bound for $|T(Y)|$ using $A(n, d)$ and $A(n, d, w)$ when we have two remote output words. After that we get bounds for $\mathcal{L}$ as easy corollaries of Theorems 24, 25 and 26.

Theorem 26. *Let $C \subseteq \mathbb{F}^n$ be an e-error-correcting code in $\mathbb{F}^n$ and $\mathbf{y}_0$ and $\mathbf{y}$ be words of Y such that $d(\mathbf{y}_0, \mathbf{y}) = 2e - 2\ell + 2 + a$ and $0 \leq a \leq 4\ell - 2$. If $t = e + \ell \geq 3\ell - 1$, then we have*

$$|T| \leq A\left(2e - 2\ell + 2 + a, 2e - 4\ell + 3 + 2\left\lceil \frac{a}{2} \right\rceil\right)$$

and

$$\begin{aligned}
|T| \leq A\,\Big(&2e - 2\ell + 2 + a, \\
&2e - 4\ell + 3 + a, e - \ell + 1 + \left\lfloor \frac{a}{2} \right\rfloor\Big) .
\end{aligned}$$

Proof. Without loss of generality, we may assume that $\mathbf{y}_0 = \mathbf{0}$, and $w(\mathbf{y}) = 2e - 2\ell + 2 + a$. Moreover, we encourage the reader to assume that $\text{supp}(\mathbf{y}) = [1, w(\mathbf{y})]$ in order to better visualize the proof. Our first goal is to show that each pair of codewords in $T(Y)$ differs in at least $d = 2e - 4\ell + 3 + 2\lceil a/2 \rceil$ coordinates in $\text{supp}(\mathbf{y})$. Hence, $|T(Y)| \leq A(w(\mathbf{y}), d)$. After that we show that we can modify the codewords to have a constant weight of $\lfloor w(\mathbf{y})/2 \rfloor$ and then we can get the second bound by considering cardinality of maximal constant weight codes in $\mathbb{F}^{w(\mathbf{y})}$.

Notice that since the all-zero word is received as an output word, we may restrict our investigation to codewords with weight at most t. For a codeword $\mathbf{c} \in C \cap B_t(\mathbf{y}_0) \cap B_t(\mathbf{y})$, we use the following notation: $S_{\mathbf{c}} = \text{supp}(\mathbf{c}) \cap \text{supp}(\mathbf{y})$, $A_{\mathbf{c}} = \text{supp}(\mathbf{c}) \setminus \text{supp}(\mathbf{y})$ and $\mathbf{y_c}$ is the word such that $\text{supp}(\mathbf{y_c}) = S_{\mathbf{c}}$. Moreover, we denote $V_{\mathbf{c}} = \left\lfloor |w(\mathbf{y_c}) - \frac{w(\mathbf{y})}{2}| \right\rfloor$. In other words, if $w(\mathbf{y})$ is even, then $V_{\mathbf{c}}$ gives the difference of $w(\mathbf{y_c})$ and $w(\mathbf{y})/2$, and if $w(\mathbf{y})$ is odd, then it gives the difference of $w(\mathbf{y_c})$ and $\lfloor w(\mathbf{y})/2 \rfloor$ or $\lceil w(\mathbf{y})/2 \rceil$ whichever is closer. We illustrate these notations in Figure 4.

In order to show that $\max\{d(\mathbf{y}_0, \mathbf{y_c}), d(\mathbf{y}, \mathbf{y_c})\} = \max\{w(\mathbf{y_c}), w(\mathbf{y}) - w(\mathbf{y_c})\} = \left\lceil \frac{w(\mathbf{y})}{2} \right\rceil + V_{\mathbf{c}}$, we need to study the following two cases:

- If $w(\mathbf{y_c}) \geq w(\mathbf{y})/2$, then $w(\mathbf{y}) - w(\mathbf{y_c}) \leq w(\mathbf{y}) - w(\mathbf{y})/2 \leq w(\mathbf{y_c})$ and
$$\max\{w(\mathbf{y_c}), w(\mathbf{y}) - w(\mathbf{y_c})\} = w(\mathbf{y_c}) = \lceil w(\mathbf{y})/2 \rceil + V_{\mathbf{c}}.$$
- If $w(\mathbf{y_c}) < w(\mathbf{y})/2$, then $w(\mathbf{y}) - w(\mathbf{y_c}) > w(\mathbf{y}) - w(\mathbf{y})/2 > w(\mathbf{y_c})$ and
$$\begin{aligned} &\max\{w(\mathbf{y_c}), w(\mathbf{y}) - w(\mathbf{y_c})\}\\ &= w(\mathbf{y}) - w(\mathbf{y_c})\\ &= w(\mathbf{y}) - (\lfloor w(\mathbf{y})/2 \rfloor - V_{\mathbf{c}})\\ &= \lceil w(\mathbf{y})/2 \rceil + V_{\mathbf{c}}. \end{aligned}$$

Moreover, we have $d(\mathbf{y}_0, \mathbf{c}) = |A_{\mathbf{c}}| + d(\mathbf{y}_0, \mathbf{y_c})$ and $d(\mathbf{y}, \mathbf{c}) = |A_{\mathbf{c}}| + d(\mathbf{y}, \mathbf{y_c})$. Furthermore, since $\max\{d(\mathbf{y}_0, \mathbf{c}), d(\mathbf{y}, \mathbf{c})\} \leq t$, we have $|A_{\mathbf{c}}| \leq t - d(\mathbf{y}_0, \mathbf{y_c})$ and $|A_{\mathbf{c}}| \leq t - d(\mathbf{y}, \mathbf{y_c})$. Since both of these upper bounds hold simultaneously, we have $|A_{\mathbf{c}}| \leq t - \max\{d(\mathbf{y}_0, \mathbf{y_c}), d(\mathbf{y}, \mathbf{y_c})\}$. Thus, we have

$$|A_{\mathbf{c}}| \leq t - \left\lceil \frac{w(\mathbf{y})}{2} \right\rceil - V_c. \tag{8}$$

Assume then that $\mathbf{c}_1, \mathbf{c}_2 \in C \cap B_t(\mathbf{y}_0) \cap B_t(\mathbf{y})$ and $\mathbf{c}_1 \neq \mathbf{c}_2$. We may trivially approximate the distance of $\mathbf{c}_1$ and $\mathbf{c}_2$ in following way:

$$d(\mathbf{c}_1, \mathbf{c}_2) \leq |A_{\mathbf{c}_1}| + |A_{\mathbf{c}_2}| + d(\mathbf{y}_{\mathbf{c}_1}, \mathbf{y}_{\mathbf{c}_2}). \tag{9}$$

Now, by estimating the right side of Inequality (9) with Inequality (8) and the left side of Inequality (9) by recalling $d(\mathbf{c}_1, \mathbf{c}_2) \geq 2e + 1$, we get the following lower bound for $d(\mathbf{y}_{\mathbf{c}_1}, \mathbf{y}_{\mathbf{c}_2})$ (as $w(\mathbf{y}) = 2e - 2\ell + 2 + a$):

$$\begin{aligned} d(\mathbf{y}_{\mathbf{c}_1}, \mathbf{y}_{\mathbf{c}_2}) &\geq 2 \left\lceil \frac{w(\mathbf{y})}{2} \right\rceil + 1 - 2\ell + V_{\mathbf{c}_1} + V_{\mathbf{c}_2} \\ &= 2e - 4\ell + 3 + 2\lceil a/2 \rceil + V_{\mathbf{c}_1} + V_{\mathbf{c}_2}. \end{aligned} \tag{10}$$

Observe that when $e \geq 2\ell - 1$ this lower bound is positive and $\mathbf{y}_{\mathbf{c}_1}$ and $\mathbf{y}_{\mathbf{c}_2}$ are distinct.

By Inequality (10), each pair of codewords in $B_t(\mathbf{y}_0) \cap B_t(\mathbf{y})$ differ in at least $2e - 4\ell + 3 + 2\left\lceil \frac{a}{2} \right\rceil$ coordinate positions of supp$(\mathbf{y})$ (as $V_{\mathbf{c}_1}, V_{\mathbf{c}_2} \geq 0$). Thus, the words $\mathbf{y_c}$ form a code with minimum distance $2e - 4\ell + 3 + 2\left\lceil \frac{a}{2} \right\rceil$ in $\mathbb{F}^{w(\mathbf{y})}$. Hence, we have $|T| \leq A\left(w(\mathbf{y}), 2e - 4\ell + 3 + 2\left\lceil \frac{a}{2} \right\rceil\right)$. This gives the first bound of the theorem. However, the bound does not take into account the values $V_{\mathbf{c}_1}$ and $V_{\mathbf{c}_2}$ in Inequality (10). In what follows, we try to improve the previous bound by making use of $V_{\mathbf{c}_1}$ and $V_{\mathbf{c}_2}$.

$$\begin{aligned} \mathbf{y}_0 &= \; 0\,0\,0\,0\,0\,0\,0\,0\,0\,0 \cdots 0 \\ \mathbf{y} &= \; 1\,1\,1\,1\,1\,1\,0\,0\,0\,0 \cdots 0 \\ \mathbf{c}'_1 &= \; 1\,1\,0\,0\,0\,0\,1\,1\,0\,0 \cdots 0 \\ \mathbf{c}_1 &= \; 1\,1\,0\,0\,0\,0 \\ \mathbf{c}'_2 &= \; 0\,0\,1\,1\,1\,1\,0\,0\,1\,0 \cdots 0 \\ \mathbf{c}_2 &= \; 0\,0\,1\,1\,1\,1 \end{aligned}$$

Fig. 5. Two output words $\mathbf{y}_0$ and $\mathbf{y}$ at distance 6 when $e = 4$, $\ell = 2$ and $a = 0$. Codewords $\mathbf{c}_1 \in \mathbb{F}^{w(\mathbf{y})}$ and $\mathbf{c}_2 \in \mathbb{F}^{w(\mathbf{y})}$ are formed from $\mathbf{c}'_1$ and $\mathbf{c}'_2$ as in the code C' defined in (11).

Let us define

$$C' = \{\mathbf{c} \in \mathbb{F}^{w(\mathbf{y})} \mid \mathbf{c}' \in C \cap B_t(\mathbf{y}_0) \cap B_t(\mathbf{y}), \text{supp}(\mathbf{c}) = S_{\mathbf{c}'}\}, \tag{11}$$

that is, the code $C' \subseteq \mathbb{F}^{w(\mathbf{y})}$ is formed by taking each codeword in $B_t(\mathbf{y}_0) \cap B_t(\mathbf{y})$ and then restricting their support to supp$(\mathbf{y})$. In Figure 5, we have presented how codewords of the code C' are formed. Therefore, as $d(\mathbf{y}_{\mathbf{c}_1}, \mathbf{y}_{\mathbf{c}_2}) > 0$ by Inequality (10), we have $|C'| = |C \cap B_t(\mathbf{y}_0) \cap B_t(\mathbf{y})|$. The proof now divides into two cases depending on the parity of $w(\mathbf{y})$.

Suppose first that $w(\mathbf{y})$ is even, that is, a is even. Based on C', form a new code D as follows:

- If $\mathbf{c} \in C'$ and $w(\mathbf{c}) = w(\mathbf{y})/2$, then add $\mathbf{c}$ to D.
- If $\mathbf{c} \in C'$ and $w(\mathbf{c}) > w(\mathbf{y})/2$, then delete $V_{\mathbf{c}}$ elements from the support supp$(\mathbf{c})$ and add the resulting word of weight $w(\mathbf{y})/2$ to D.
- If $\mathbf{c} \in C'$ and $w(\mathbf{c}) < w(\mathbf{y})/2$, then add $V_{\mathbf{c}}$ elements to the support supp$(\mathbf{c})$ and add the resulting word of weight $w(\mathbf{y})/2$ to D.

Assume that $\mathbf{c}'_1$ and $\mathbf{c}'_2$ are codewords of D and that they have been respectively formed from the codewords $\mathbf{c}_1$ and $\mathbf{c}_2$ of C'. By Inequality (10), we obtain that $d(\mathbf{c}'_1, \mathbf{c}'_2) \geq d(\mathbf{c}_1, \mathbf{c}_2) - V_{\mathbf{c}_1} - V_{\mathbf{c}_2} \geq 2e - 4\ell + 3 + a > 0$ when $e \geq 2\ell - 1$. Thus, D is a code with minimum distance (at least) $w(\mathbf{y}) + 1 - 2\ell$ and $|C'| = |D|$. Therefore, we have $|T| \leq |C'| = |D| \leq A\left(w(\mathbf{y}), 2e - 4\ell + 3 + a, \frac{w(\mathbf{y})}{2}\right) = A\left(w(\mathbf{y}), 2e - 4\ell + 3 + a, e - \ell + 1 + \left\lfloor \frac{a}{2} \right\rfloor\right)$.

Suppose then that $w(\mathbf{y})$ is odd, that is, a is odd. As in the previous case, form a code D based on C' as follows:

- If $\mathbf{c} \in C'$ and $w(\mathbf{c}) \geq \lceil w(\mathbf{y})/2 \rceil$, then delete $V_{\mathbf{c}} + 1$ elements from the support supp$(\mathbf{c})$ and add the resulting word of weight $\lfloor w(\mathbf{y})/2 \rfloor$ to D.
- If $\mathbf{c} \in C'$ and $w(\mathbf{c}) \leq \lfloor w(\mathbf{y})/2 \rfloor$, then delete $V_{\mathbf{c}}$ elements from the support supp$(\mathbf{c})$ and add the resulting word of weight $\lfloor w(\mathbf{y})/2 \rfloor$ to D.

Thus, the resulting code D contains words of weight $\lfloor w(\mathbf{y})/2 \rfloor$. Assume that $\mathbf{c}'_1$ and $\mathbf{c}'_2$ are codewords of D and that they have been respectively formed from the codewords $\mathbf{c}_1$ and $\mathbf{c}_2$ of C'. By Inequality (10) and recalling the additional element deleted in the former case of the construction of D, we obtain that $d(\mathbf{c}'_1, \mathbf{c}'_2) \geq d(\mathbf{c}_1, \mathbf{c}_2) - V_{\mathbf{c}_1} - V_{\mathbf{c}_2} - 2 \geq 2e - 4\ell + 2 + a > 0$ when $e \geq 2\ell - 1$. Thus, D is a code with minimum distance (at least) $2e - 4\ell + 2 + a$ and $|C'| = |D|$. Therefore, we have $|T| \leq |C'| = |D| \leq A\left(w(\mathbf{y}), 2e - 4\ell + 2 + a, \lfloor \frac{w(\mathbf{y})}{2} \rfloor\right) = A\left(w(\mathbf{y}), 2e - 4\ell + 3 + a, e - \ell + 1 + \left\lfloor \frac{a}{2} \right\rfloor\right)$ (where the last equality is due to Theorem 25(ii)). □

Notice that in the proof of the previous theorem, in the case of odd a, we actually have a *two-weight code*, that is, a code where every codeword has either weight w_1 or w_2. Then, in order to obtain a constant weight code, the two-weight code is slightly modified. Hence, it might be possible to gain a slight improvement on the bound by investigating two-weight codes. Observe that in the proof of Theorem 5 we have actually considered a two-weight code (the set of words β_i).

In what follows, we give a few corollaries of the previous theorem. For this purpose, we first make the following simple observation: if k, k' and m are nonnegative integers such that $k \geq k'$, then

$$\frac{k}{k'} = \frac{k + m(k/k')}{k' + m} \geq \frac{k+m}{k'+m}. \tag{12}$$

Now we are ready to present the first corollary.

Corollary 27. *If $e \geq 3\ell - 2$, $C \subseteq \mathbb{F}^n$ is an e-error-correcting code and $d(\mathbf{y}_0, \mathbf{y}) \geq 2e - 2\ell + 2$ with $\mathbf{y}, \mathbf{y}_0 \in Y$, then we have*

$$|T| \leq 2 \left\lfloor \frac{2e - 4\ell + 4}{2e - 6\ell + 5} \right\rfloor .$$

Proof. Let a be an integer such that $d(\mathbf{y}_0, \mathbf{y}) = 2e - 2\ell + 2 + a$ and $0 \leq a \leq 4\ell - 2$. By Theorem 26, we have $|T| \leq A(2e - 2\ell + 2 + a, 2e - 4\ell + 3 + 2\lceil a/2 \rceil)$. Since $e \geq 3\ell - 2$, it can be straightforwardly verified that the requirement $n < 2d + 1$ of the Plotkin bound is satisfied. Now the proof divides into the following two cases depending on the parity of a:

- Suppose that a is even. By the Plotkin bound and Observation (12), we obtain that

$$\begin{aligned}|T| &\leq A(2e - 2\ell + 2 + a, 2e - 4\ell + 3 + a) \\ &\leq 2 \left\lfloor \frac{2e - 4\ell + 4 + a}{2e - 6\ell + 5 + a} \right\rfloor \leq 2 \left\lfloor \frac{2e - 4\ell + 4}{2e - 6\ell + 5} \right\rfloor .\end{aligned}$$

- Suppose that a is odd. By the Plotkin bound and Observation (12), we obtain that

$$\begin{aligned}|T| &\leq A(2e - 2\ell + 2 + a, 2e - 4\ell + 4 + a) \\ &\leq 2 \left\lfloor \frac{2e - 4\ell + 5 + a}{2e - 6\ell + 7 + a} \right\rfloor \leq 2 \left\lfloor \frac{2e - 4\ell + 4}{2e - 6\ell + 5} \right\rfloor .\end{aligned}$$

Thus, the claim follows. □

When $e \geq 4\ell - 2$, the previous corollary implies the following result.

Corollary 28. *If $e \geq 4\ell - 2$, $C \subseteq \mathbb{F}^n$ is an e-error-correcting code and $d(\mathbf{y}_0, \mathbf{y}) \geq 2e - 2\ell + 2$ with $\mathbf{y}_0, \mathbf{y} \in Y$, then we have*

$$|T| \leq 2.$$

Proof. Since $e \geq 4\ell - 2$, we obtain by the previous corollary and Observation (12) that

$$\begin{aligned}|T| &\leq 2 \left\lfloor \frac{2e - 4\ell + 4}{2e - 6\ell + 5} \right\rfloor \\ &\leq 2 \left\lfloor \frac{2(4\ell - 2) - 4\ell + 4}{2(4\ell - 2) - 6\ell + 5} \right\rfloor = 2 \left\lfloor \frac{4\ell}{2\ell + 1} \right\rfloor = 2.\end{aligned}$$

Hence, the claim follows. □

The previous corollaries have been obtained by applying the Plotkin bound to Theorem 26. In some cases, this can be improved by considering constant weight codes and Theorem 25(iii).

Corollary 29. *If $e \geq 3\ell - 2$, $C \subseteq \mathbb{F}^n$ is an e-error-correcting code and $d(\mathbf{y}_0, \mathbf{y}) \geq 2e - 2\ell + 2$ with $\mathbf{y}, \mathbf{y}_0 \in Y$, then we have*

$$|T| \leq 2 \left\lfloor \frac{\ell + 1}{2} \right\rfloor$$

if a is odd and

$$|T| \leq 2\ell$$

if a is even.

Proof. Let a be an integer such that $d(\mathbf{y}_0, \mathbf{y}) = 2e - 2\ell + 2 + a$ and $0 \leq a \leq 4\ell - 2$. Based on the parity of a, the proof divides into the following cases:

- Suppose that a is odd. By Theorem 26, we have

$$\begin{aligned}|T| &\leq A(2e - 2\ell + 2 + a, 2e - 4\ell + 3 + 2\lceil a/2 \rceil) \\ &= A(2e - 2\ell + 2 + a, 2e - 4\ell + 4 + a).\end{aligned}$$

Further, by the Plotkin bound and Observation (12), we obtain that

$$\begin{aligned}|T| &\leq 2 \left\lfloor \frac{2e - 4\ell + 5 + a}{2e - 6\ell + 7 + a} \right\rfloor \\ &\leq 2 \left\lfloor \frac{2(3\ell - 2) - 4\ell + 5 + a}{2(3\ell - 2) - 6\ell + 7 + a} \right\rfloor \\ &\leq 2 \left\lfloor \frac{2\ell + 2}{4} \right\rfloor = 2 \left\lfloor \frac{\ell + 1}{2} \right\rfloor .\end{aligned}$$

- Suppose that a is even. By Theorems 26 and 25(ii), we have

$$\begin{aligned}&|T| \\ &\leq A(2e - 2\ell + 2 + a, 2e - 4\ell + 3 + a, e - \ell + 1 + a/2) \\ &= A(2e - 2\ell + 2 + a, 2e - 4\ell + 4 + a, e - \ell + 1 + a/2) \\ &= A(n, 2\delta, w),\end{aligned}$$

where $n = 2w$, $w = e - \ell + 1 + a/2$ and $\delta = e - 2\ell + 2 + a/2$. In order to apply Theorem 25(iii), we observe that

$$\begin{aligned}b &= \delta - \frac{w(n-w)}{n} \\ &= \delta - \frac{w}{2} \\ &= \frac{2e - 6\ell + 6 + a}{4} \\ &\geq \frac{2(3\ell - 2) - 6\ell + 6 + a}{4} \geq \frac{1}{2}\end{aligned}$$

and

$$\frac{\delta}{n} = \frac{1}{2} - \frac{\ell - 1}{n} \leq \frac{1}{2}.$$

Therefore, as $b \geq \delta/n$, we obtain by Theorem 25(iii) and Observation (12) that

$$\begin{aligned}|T| &\leq A(n, 2\delta, w) \\ &= \left\lfloor \frac{\delta}{b} \right\rfloor \\ &= 1 + \left\lfloor \frac{e - \ell + 1 + a/2}{e - 3\ell + 3 + a/2} \right\rfloor \\ &\leq 1 + \left\lfloor \frac{(3\ell - 2) - \ell + 1}{(3\ell - 2) - 3\ell + 3} \right\rfloor = 2\ell.\end{aligned}$$

Thus, the claim follows. □

In the three corollaries above, we have considered the cases with $e \geq 3\ell - 2$. However, Theorem 26 already holds for $e \geq 2\ell - 1$. In the following corollary, we complete this gap.

Corollary 30. *If $e \geq 2\ell - 1$, $C \subseteq \mathbb{F}^n$ is an e-error-correcting code and $d(\mathbf{y}_0, \mathbf{y}) = 2e - 2\ell + 2 + a$ with $\mathbf{y}, \mathbf{y}_0 \in Y$ and $0 \leq a \leq 4\ell - 2$, then we have*

$$|T| \leq \frac{\binom{2e-2\ell+2+a}{\ell}}{\binom{e-\ell+1+\lfloor \frac{a}{2} \rfloor}{\ell}}.$$

Proof. Let a be an integer such that $d(\mathbf{y}_0, \mathbf{y}) = 2e - 2\ell + 2 + a$ and $0 \leq a \leq 4\ell - 2$. Theorem 26 gives $|T| \leq A\left(2e - 2\ell + 2 + a,\ 2e - 4\ell + 3 + a,\ e - \ell + 1 + \lfloor a/2 \rfloor\right)$. The proof now divides into the following two cases depending on the parity of a:

- Suppose that a is even. By Theorem 25(ii), we have $|T| \leq A(2e-2\ell+2+a, 2e-4\ell+4+a, e-\ell+1+a/2) = A(n, 2\delta, w)$, where $n = 2e-2\ell+2+a$, $\delta = e-2\ell+2+a/2$ and $w = e - \ell + 1 + a/2$. Now $k = w - \delta + 1 = \ell$. Hence, by Theorem 25$(iv)$, we obtain that
$$|T| \leq \frac{\binom{2e-2\ell+2+a}{\ell}}{\binom{e-\ell+1+\lfloor a/2 \rfloor}{\ell}}.$$
- Suppose that a is odd. Now we have $|T| \leq A(2e - 2\ell + 2 + a, 2e - 4\ell + 3 + a, e - \ell + 1 + (a-1)/2) = A(n, 2\delta, w)$, where $n = 2e - 2\ell + 2 + a$, $\delta = e - 2\ell + 2 + (a-1)/2$ and $w = e - \ell + 1 + (a-1)/2$. Now $k = w - \delta + 1 = \ell$. Hence, by Theorem 25$(iv)$, we obtain that
$$|T| \leq \frac{\binom{2e-2\ell+2+a}{\ell}}{\binom{e-\ell+1+\lfloor a/2 \rfloor}{\ell}}.$$

Thus, the claim follows. □

Notice that if $e = 2\ell - 1$, then we are very likely to have two output words with distance at least 2ℓ by Theorem 23 (or we have $|T| = 1$). Earlier, in Corollary 4, we have shown that if $N \geq V(n, \ell - 1) + 1$, then we have two output words with distance at least $2\ell - 1$. In Theorem 5, this is applied to give the upper bound $|T| \leq \binom{2\ell}{\ell}$. Observe that Corollary 30 also gives upper bound $\binom{2\ell}{\ell}$ when $e = 2\ell - 1$ and $a = 0$.

V. Less than $V(n, \ell - 1) + 1$ channels

In this section, we investigate some cases with $N \leq V(n, \ell - 1)$. In the following, we consider the asymptotic behaviour of $\mathcal{L}$ for different values of N when e and ℓ are constants and $C \subseteq \mathbb{F}^n$ is such an e-error-correcting code that $\mathcal{L}$ is maximal. First we give an upper bound on $\mathcal{L}$ and then a lower bound.

Lemma 31. *Let $N \geq V(n, \ell - a - 1) + 1$ where $0 \leq a \leq \ell - 1$. Then for any e-error-correcting code $C \subseteq \mathbb{F}^n$, we have*

$$\mathcal{L} \leq 2^{\ell - a} V(n - e - \ell + a, a).$$

Proof. Let $\mathbf{x}$ be the input word and Y be the set of output words. We will use the Sauer-Shelah lemma to find a word at distance $e + a$ from $\mathbf{x}$. Then we correct the a errors by going through each possible word containing those errors. Finally, the upper bound follows from Lemma 2.

By Theorem 6 there exists a set $S \subseteq [1, n]$ of size $\ell - a$ which is shattered by some set $Y' \subseteq Y$ such that $|Y'| = 2^{\ell - a}$. Without loss of generality, we may assume that $S = [1, \ell - a]$. Moreover, let $\mathbf{s}$ be such a word that $\mathrm{supp}(\mathbf{s}) = S$. Furthermore, as in the proof of Theorem 7, for each $\mathbf{y}_i \in Y'$, $1 \leq i \leq 2^{\ell - a}$, we denote $\beta_i = \mathbf{y}_i + \mathbf{s}$.

Let β_j, $j \in [1, 2^{\ell - a}]$, be such a word that $\mathrm{supp}(\mathbf{x}) \cap S = \mathrm{supp}(\beta_j) \cap S$. This word β_j exists because the set of coordinates S is shattered by the set of words Y'. Since $d(\mathbf{x}, \mathbf{y}_j) \leq e + \ell$, we have $d(\mathbf{x}, \beta_j) \leq e + \ell - (\ell - a) = e + a$. Hence, let $d(\mathbf{x}, \beta_j) = e + a' \leq e + a$. Now, $\mathbf{x}$ and β_j differ in $e + a'$ coordinates in the set $[\ell - a + 1, n]$. Thus, for $0 \leq h \leq V(n - e - \ell + a, a)$, we may consider words $\beta_j + \mathbf{w}_h$, where $\mathrm{supp}(\mathbf{w}_h) \in [\ell - a + 1, n - e]$ and $0 \leq w(\mathbf{w}_h) \leq a$. Since $d(\mathbf{x}, \beta_j) = e + a' \leq e + a$ one of the words $\mathbf{w}_h$, say $\mathbf{w}_{h'}$, corresponds to a' differences between $\mathbf{x}$ and β_j (or to 0 differences if a' is negative), i.e., $\mathrm{supp}(\mathbf{w}_{h'}) \subseteq \mathrm{supp}(\mathbf{x} + \beta_j)$ and $w(\mathbf{w}_{h'}) = a'$. Hence, we have $d(\mathbf{x}, \beta_j + \mathbf{w}_{h'}) \leq e$. Therefore, the upper bound for $\mathcal{L}$ follows from applying Lemma 2 with e-balls centered at words $\beta_j + \mathbf{w}_h$ where $j \in [1, 2^{\ell - a}]$ and $h \in [1, V(n - e - \ell + a, a)]$. □

Lemma 32. *Let $N \leq V(n, \ell - a)$ where $0 \leq a \leq \ell$ and $n \geq 2e + a$. Then there exists such an e-error-correcting code $C \subseteq \mathbb{F}^n$ that*

$$\mathcal{L} \geq \frac{\binom{n}{e+a}}{\sum_{i=0}^{e} \binom{e+a}{i}\binom{n-e-a}{i}} \geq \frac{n^a}{(e+a)^a \sum_{i=0}^{e} \binom{e+a}{i}}.$$

Proof. Let $S = \{\mathbf{w} \in \mathbb{F}^n \mid w(\mathbf{w}) \leq \ell - a\}$ and $Y \subseteq S$. We immediately notice that if $w(\mathbf{c}) \leq e + a$, then $\mathbf{c} \in \bigcap_{\mathbf{y} \in Y} B_t(\mathbf{y})$. Let us now consider a maximal e-error-correcting code C with constant weight $e + a$. By [24, Theorem 7] (Gilbert bound for constant weight codes) and Theorem 25(ii), we have $\mathcal{L} \geq |C| = A(n, 2e + 1, e + a) = A(n, 2e + 2, e + a) \geq \frac{\binom{n}{e+a}}{\sum_{i=0}^{e} \binom{e+a}{i}\binom{n-e-a}{i}}$. Furthermore, we may give lower bound

$$\begin{aligned}
&\frac{\binom{n}{e+a}}{\sum_{i=0}^{e} \binom{e+a}{i}\binom{n-e-a}{i}} \\
\geq &\frac{\binom{n}{e+a}}{\binom{n-a}{e} \sum_{i=0}^{e} \binom{e+a}{i}} \\
= &\frac{n!e!(n-e-a)!}{(n-a)!(e+a)!(n-e-a)! \sum_{i=0}^{e} \binom{e+a}{i}} \\
\geq &\frac{n^a}{(e+a)^a \sum_{i=0}^{e} \binom{e+a}{i}}.
\end{aligned}$$

The last inequality is due to Observation (12). □

In the following theorem, we give an asymptotic estimate for $\mathcal{L}$ with exact dependency on N.

Theorem 33. *Let $V(n, \ell - a - 1) + 1 \leq N \leq V(n, \ell - a)$ where $0 \leq a \leq \ell - 1$. Moreover, let $C \subseteq \mathbb{F}^n$ be such an e-error-correcting code that $\mathcal{L}$ is maximal. Then we have*

$$\mathcal{L} = \Theta(n^a).$$

Proof. Let $V(n, \ell - a - 1) + 1 \leq N \leq V(n, \ell - a)$. By Lemma 31 we have $\mathcal{L} \leq 2^{\ell - a} \sum_{i=0}^{a} \binom{n-e-\ell+a}{i} \leq 2^{\ell - a}(a + 1)\binom{n}{a} \leq 2^{\ell - a}(a + 1)\frac{n^a}{a!}$ (for $n \geq 2a$). Since e, ℓ and a are constants, the claim follows by Lemma 32. □

We have mostly considered situations where the e-error-correcting code C gives us as large $\mathcal{L}$ as possible, that is, in situations where C is as "bad" as possible. This is a reasonable approach to give some general bounds for $\mathcal{L}$. However, we can construct large e-error-correcting codes such that $\mathcal{L}$ is much smaller. Previously in Theorem 10, we have shown that there exist such e-error-correcting codes that $\mathcal{L}$ can be rather large (depends on n) when we have less than $V(n, \ell-1)+1$ channels. In the following, we construct such rather large e-error-correcting codes that $\mathcal{L}$ is constant on n when $N \geq V(n, \ell-k)+1$ where $k=2$.

Theorem 34. *For any $t = e+\ell$, there exist e-error-correcting codes $C \subseteq \mathbb{F}_2^n$ of length $n = 2^m - 1$, where $m > \log_2(e+1)! + 3$, and of size at least $2^{2^m-(e+1)m}$ with*

$$\mathcal{L} \leq 2^\ell$$

for

$$N \geq V(n, \ell-2)+1.$$

Proof. Let us first consider a primitive narrow-sense BCH code C with designed distance $2(e+1)+1$, that is, error-correcting capability at least $e+1$ [21, p. 203]. Let α be a primitive element of the finite field $\mathbb{F}_{2^m}$. It is also a primitive nth root of unity of the field. The BCH code is defined by

$$C = \{c(x) \in R \mid c(\alpha) = c(\alpha^3) = \cdots = c(\alpha^{2e+1}) = 0\}$$

where the ring $R = \mathbb{F}_2[x]/\langle x^n - 1\rangle$. Hence, $C = \{\mathbf{x} \in \mathbb{F}_2^n \mid H\mathbf{x}^T = 0\}$ where

$$H = \begin{pmatrix} 1 & \alpha & \dots & \alpha^{n-1} \\ 1 & \alpha^3 & \dots & \alpha^{3(n-1)} \\ \vdots & & & \vdots \\ 1 & \alpha^{2e+1} & \dots & \alpha^{(2e+1)(n-1)} \end{pmatrix}.$$

Let now $\{\gamma_1, \dots, \gamma_m\}$ be a basis of the field extension $\mathbb{F}_{2^m}$ over $\mathbb{F}_2$. Thus, we can write the elements α^i in H with the aid of the basis as column vectors. Consequently, we obtain an $(e+1)m \times n$-matrix H_2 with entries in $\mathbb{F}_2$ such that $C = \{\mathbf{x} \in \mathbb{F}_2^n \mid H_2\mathbf{x}^T = 0\}$.

Let us write $t = (e+1)+(\ell-1)$. Due to Theorem 7, we know that for any set of at least $V(n, \ell-2)+1$ outputs $Y = \{\mathbf{y}_1, \dots, \mathbf{y}_N\}$ we have

$$|\bigcap_{\mathbf{y} \in Y} B_t(\mathbf{y}) \cap C| \leq 2^{\ell-1} \tag{13}$$

for radius t. Notice that the error-correcting capability of C can be better than $e+1$, but in that case we get a code with even better parameters by writing $t = (e+i)+(\ell-i)$.

Since $m > 2\log_2(2e+1)$, the rows of H_2 are linearly independent [21, p. 263]. Let us delete suitable linearly independent rows among the rows in the matrix H_2 which correspond to the row

$$R = (1, \alpha^{2e+1}, \dots, \alpha^{(2e+1)(n-1)})$$

of the matrix H. We delete the smallest number of rows, say p rows ($p \leq m$), in such a way that the obtained matrix H' gives us a code $C' = \{\mathbf{x} \in \mathbb{F}_2^n \mid H'\mathbf{x}^T = 0\}$ with error-correcting capability exactly e. Notice that the error-correcting capability of C' is at least e. Indeed, since $m > \log_2(e+1)! + 1$, we know [21, p. 259] that the code corresponding to H without the row R has error-correcting capability exactly e and the corresponding rows in H' remain intact. Let C_2 be the code which is obtained just before C', that is, using the matrix where we have deleted only $p-1$ rows from H_2. Now the error-correcting capability of C_2 is at least $e+1$, so it has a list size at most $2^{\ell-1}$ according to (13). Due to the fact that the code C' consists of C_2 and one of its cosets, the code C' has list size at most $2 \cdot 2^{\ell-1} = 2^\ell$. For the cardinality we have [21, p. 203]

$$|C'| \geq 2^{2^m - m(e+1)}.$$

□

We may improve the previous theorem for suitable values of e and ℓ by using Theorem 20.

Theorem 35. *For any $t = e+\ell$ such that $e \geq \ell$ and $e \geq 7$, there exist e-error-correcting codes $C \subseteq \mathbb{F}_2^n$ of length $n = 2^m - 1$, where $m > \log_2(e+1)! + 3$, and of size at least $2^{2^m-(e+1)m}$ with*

$$\mathcal{L} \leq 2\ell$$

for

$$N \geq V(n, \ell-2)+1.$$

Proof. Consider the $(e+1)$-error-correcting code and Inequality (13) in the proof of the previous theorem together with Theorem 20 instead of Theorem 7. Since $e \geq 7$ and $e \geq \ell$, we have $3t \leq 6e$ and $4(e+1)+4 \leq 6e$. Therefore, we may choose $b = 6e$ in Theorem 20. Together with the notation $t = (e+1)+(\ell-1)$, we get

$$(\ell-2)^2(5e-1+(e+2)(12e^2-9e+1))+\ell-2$$

for the lower bound of n in Theorem 20. Moreover, since $e \geq 7$, we have

$$\begin{aligned} n &> 2^{\log_2(e+1)!+3} - 1 \\ &= 8 \cdot (e+1)! - 1 \\ &\geq 8(e+1)e(e-1)(e-2)(e-3)(e-4) - 1 \\ &\overset{(*)}{\geq} 12e^5 - 33e^4 - 24e^3 + 109e^2 - 51e + 2 \\ &= (e-2)^2(5e-1+(e+2)(12e^2-9e+1))+e-2 \\ &\geq (\ell-2)^2(5e-1+(e+2)(12e^2-9e+1))+\ell-2. \end{aligned}$$

Step $(*)$ is straightforward to verify as $e \geq 7$. Hence, n satisfies the requirements in Theorem 20 and we may modify Inequality (13) to

$$|\bigcap_{\mathbf{y} \in Y} B_t(\mathbf{y}) \cap C| \leq \ell$$

and thus, the code C' in the proof of Theorem 34 has list size at most $2 \cdot \ell$ instead of $2 \cdot 2^{\ell-1}$. □

Naturally, we can get corresponding results for shorter lengths than $n = 2^m - 1$ by applying the shortening method [21, p. 29] to the code C' in the proof above provided that the minimum distance of the code does not increase.

Example 36. Consider first a 2-error-correcting primitive and narrow-sense BCH code C_1 of length $n = 15$. By Theorem 7, we know that for $t = 4$ (so $\ell = 2$) using at least $N = 17$ channels C provides us a code with list size $\mathcal{L} \leq 4$. With the method of Theorem 34 we get a code C' with $\mathcal{L} \leq 4$ for $t = 4$ when we have only $N = 2$ channels! Notice that although here m does not satisfy $m > \log_2(2+1)! + 3$, we have one linearly independent row to delete from H_2 to get C'. The price we pay for this is that C_1 has 128 codewords and C' has 64.

VI. Conclusion

This paper studied a problem where we send a codeword $\mathbf{x} \in C \subseteq \mathbb{F}^n$ belonging to an e-error-correcting code through multiple identical channels in which at most $t = e + \ell$ errors occur. Based on multiple output words we give a list of codewords which were possibly transmitted. We have shown in Theorem 7 that if we have at least $N \geq V(n, \ell - 1) + 1$ channels, then the list size $\mathcal{L}$ is constant on n for any e-error-correcting code. Furthermore, if we have at most $N \leq V(n, \ell - 1)$ channels, then there exist such e-error-correcting codes that $\mathcal{L}$ depends on n as we have seen in Theorem 10. Moreover, the list size $\mathcal{L}$ is shown to be at most $\ell + 1$ when $N \geq V(n, \ell - 1) + 1$ and n is large enough in Theorems 17 and 20, and we have given a code which can achieve this bound in Theorem 9. Notably, the number of channels does not depend on e in these cases unlike in the previous results by Levenshtein (Theorem 1) and Yaakobi and Bruck ([11, Theorem 6]).

We have also given tight asymptotic bounds for list size when we have less than $V(n, \ell - 1) + 1$ channels in Lemmas 31 and 32 and in Theorem 33. Besides studying e-error-correcting codes which give maximal decoded list size, we have also constructed large codes giving smaller list sizes in Section V. Moreover, we have shown in Section IV that the list $T(Y)$ is very likely (even when N is small) constant size when e is sufficiently large compared to ℓ and n is large enough. In this case, we get a small constant list with little work when we have suitable words among the set of output words Y.

Acknowledgement

The authors would like to thank the referees for many comments which helped to improve significantly the readability of the paper.

References

[1] V. Junnila, T. Laihonen, and T. Lehtilä, "The Levenshtein's channel and the list size in information retrieval," in *Proceedings of 2019 IEEE International Symposium on Information Theory*, 2019, pp. 295–299.

[2] V. I. Levenshtein, "Efficient reconstruction of sequences," *IEEE Trans. Inform. Theory*, vol. 47, no. 1, pp. 2–22, 2001.

[3] M. Horovitz and E. Yaakobi, "Reconstruction of sequences over non-identical channels," *IEEE Trans. Inform. Theory*, vol. 65, no. 2, pp. 1267–1286, 2018.

[4] E. Yaakobi, J. Bruck, and P. H. Siegel, "Constructions and decoding of cyclic codes over b-symbol read channels," *IEEE Trans. Inform. Theory*, vol. 62, no. 4, pp. 1541–1551, 2016.

[5] J. Bornholt, R. Lopez, D. M. Carmean, L. Ceze, G. Seelig, and K. Strauss, "A DNA-based archival storage system," *ACM SIGARCH Computer Architecture News*, vol. 44, no. 2, pp. 637–649, 2016.

[6] G. M. Church, Y. Gao, and S. Kosuri, "Next-generation digital information storage in DNA," *Science*, vol. 337, no. 6102, pp. 1628–1628, 2012.

[7] R. N. Grass, R. Heckel, M. Puddu, D. Paunescu, and W. J. Stark, "Robust chemical preservation of digital information on DNA in silica with error-correcting codes," *Angewandte Chemie International Edition*, vol. 54, no. 8, pp. 2552–2555, 2015.

[8] S. H. T. Yazdi, H. M. Kiah, E. Garcia-Ruiz, J. Ma, H. Zhao, and O. Milenkovic, "DNA-based storage: Trends and methods," *IEEE Transactions on Molecular, Biological and Multi-Scale Communications*, vol. 1, no. 3, pp. 230–248, 2015.

[9] V. Levenshtein, E. Konstantinova, E. Konstantinov, and S. Molodtsov, "Reconstruction of a graph from 2-vicinities of its vertices," *Discrete Applied Mathematics*, vol. 156, pp. 1399–1406, 2008.

[10] R. Gabrys and E. Yaakobi, "Sequence reconstruction over the deletion channel," *IEEE Trans. Inform. Theory*, vol. 64, no. 4, pp. 2924–2931, 2018.

[11] E. Yaakobi and J. Bruck, "On the uncertainty of information retrieval in associative memories," *IEEE Trans. Inform. Theory*, vol. 65, no. 4, pp. 2155–2165, 2018.

[12] ——, "On the uncertainty of information retrieval in associative memories," in *Proceedings of 2012 IEEE International Symposium on Information Theory*, 2012, pp. 106–110.

[13] V. Junnila and T. Laihonen, "Information retrieval with varying number of input clues," *IEEE Trans. Inform. Theory*, vol. 62, no. 2, pp. 625–638, 2016.

[14] ——, "Codes for information retrieval with small uncertainty," *IEEE Trans. Inform. Theory*, vol. 60, no. 2, pp. 976–985, 2014.

[15] T. Laihonen and T. Lehtilä, "Improved codes for list decoding in the Levenshtein's channel and information retrieval," in *Proceedings of 2017 IEEE International Symposium on Information Theory*, 2017, pp. 2643–2647.

[16] T. Laihonen, "On t-revealing codes in binary Hamming spaces," *Information and Computation*, vol. 268, 2019.

[17] G. Cohen, I. Honkala, S. Litsyn, and A. Lobstein, *Covering codes*, ser. North-Holland Mathematical Library. Amsterdam: North-Holland Publishing Co., 1997, vol. 54.

[18] D. J. Kleitman, "On a combinatorial conjecture of Erdös," *Journal of Combinatorial Theory*, vol. 1, no. 2, pp. 209–214, 1966.

[19] N. Sauer, "On the density of families of sets," *Journal of Combinatorial Theory, Series A*, vol. 13, no. 1, pp. 145–147, 1972.

[20] S. Shelah, "A combinatorial problem; stability and order for models and theories in infinitary languages," *Pacific Journal of Mathematics*, vol. 41, no. 1, pp. 247–261, 1972.

[21] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes*, ser. North-Holland Mathematical Library. Amsterdam: North-Holland Publishing Co., 1977, vol. 16.

[22] M. Plotkin, "Binary codes with specified minimum distance," *IRE Trans. Inform. Theory*, vol. 6, no. 4, pp. 445–450, 1960.

[23] E. Agrell, A. Vardy, and K. Zeger, "Upper bounds for constant-weight codes," *IEEE Trans. Inform. Theory*, vol. 46, no. 7, pp. 2373–2395, 2000.

[24] R. Graham and N. Sloane, "Lower bounds for constant weight codes," *IEEE Trans. Inform. Theory*, vol. 26, no. 1, pp. 37–43, 1980.

Appendix
Proof of Lemma 18

In the appendix, we give the rather technical proof of Lemma 18. For the proof, we first present an auxiliary result. In [17, Theorem 2.4.10], it has been shown that the size of an intersection of three Hamming balls in $\mathbb{F}^n$ increases (or, more precisely, does not decrease) as the pairwise distances of the centers of the balls decrease. In the following lemma, we show that an analogous result holds even though certain restrictions are given to the words in the intersection. Recall that $B_t(\mathbb{F}^n; \mathbf{x}) = \{\mathbf{w} \in \mathbb{F}^n \mid d(\mathbf{w}, \mathbf{x}) \leq t\}$ and that $\mathrm{supp}(\mathbf{a} + \mathbf{b})$ denotes the set of coordinates in which the words $\mathbf{a}$ and $\mathbf{b}$ differ. Moreover, we have $d(\mathbf{a}, \mathbf{b}) = |\mathrm{supp}(\mathbf{a} + \mathbf{b})|$.

Lemma 37. *Let $b \leq n$ be a positive integer, $\mathbf{c}_0$, $\mathbf{c}_1$ and $\mathbf{c}_2$ be words of $\mathbb{F}^n$ and set $\overline{D} \subseteq [1, n]$, $|\overline{D}| = b$, be such that* *supp*$(\mathbf{c}_i+\mathbf{c}_j) \subseteq \overline{D}$ *for any distinct* $i, j \in \{0,1,2\}$*. Further, let* $\mathbf{c}_0'$*,* $\mathbf{c}_1'$*,* $\mathbf{c}_2'$ *be three such words in* $\mathbb{F}^n$ *that* $d(\mathbf{c}_i, \mathbf{c}_j) \geq d(\mathbf{c}_i', \mathbf{c}_j')$ *and supp*$(\mathbf{c}_i' + \mathbf{c}_j') \subseteq \overline{D}$ *for all* i *and* j*. Denote*

$$S = \{\mathbf{w} \in \mathbb{F}^n \mid \mathbf{w} \in \bigcap_{i=0}^{2} B_t(\mathbf{c}_i) \textit{ and } \\ |\textit{supp}(\mathbf{w}+\mathbf{c}_0) \setminus \overline{D}| < \ell - 1\}$$

and

$$S' = \{\mathbf{w} \in \mathbb{F}^n \mid \mathbf{w} \in \bigcap_{i=0}^{2} B_t(\mathbf{c}_i') \textit{ and } \\ |\textit{supp}(\mathbf{w}+\mathbf{c}_0') \setminus \overline{D}| < \ell - 1\}.$$

Then, we have $|S| \leq |S'|$*.*

Proof. Observe first that $\mathbf{c}_0$ and $\mathbf{c}_0'$ could be replaced in the definitions of S and S' by $\mathbf{c}_i$ and $\mathbf{c}_i'$ with $i \in \{1, 2\}$, respectively. Indeed, notice that we have

$$\text{supp}(\mathbf{w}+\mathbf{c}_0)\setminus\overline{D} = \text{supp}(\mathbf{w}+\mathbf{c}_1)\setminus\overline{D} = \text{supp}(\mathbf{w}+\mathbf{c}_2)\setminus\overline{D} \quad (14)$$

and $\text{supp}(\mathbf{w}+\mathbf{c}_0')\setminus\overline{D} = \text{supp}(\mathbf{w}+\mathbf{c}_1')\setminus\overline{D} = \text{supp}(\mathbf{w}+\mathbf{c}_2')\setminus\overline{D}$ for any $\mathbf{w} \in \mathbb{F}^n$ since $\text{supp}(\mathbf{c}_i + \mathbf{c}_j) \subseteq \overline{D}$ and $\text{supp}(\mathbf{c}_i' + \mathbf{c}_j') \subseteq \overline{D}$ for any $i, j \in \{0, 1, 2\}$. Hence, the codewords $\mathbf{c}_0$, $\mathbf{c}_1$ and $\mathbf{c}_2$ differ only inside the set $\overline{D}$ and the same is true for the words $\mathbf{c}_0'$, $\mathbf{c}_1'$ and $\mathbf{c}_2'$. In other words, the codewords $\mathbf{c}_0$, $\mathbf{c}_1$ and $\mathbf{c}_2$ ($\mathbf{c}_0'$, $\mathbf{c}_1'$ and $\mathbf{c}_2'$) do not differ outside the set $\overline{D}$. Therefore, all the codewords $\mathbf{c}_i$ and $\mathbf{c}_i'$ have symmetrical roles (albeit at first sight it might seem that $\mathbf{c}_0$ and $\mathbf{c}_0'$ have a special role). Thus, we may without loss of generality assume that $\mathbf{c}_0 = \mathbf{c}_0' = \mathbf{0}$ and $\overline{D} = [1, b]$ since only the cardinalities of S and S' are considered and the distances between $\mathbf{c}_i$'s and the distances between $\mathbf{c}_i'$'s do not depend on each other. Observe that $\text{supp}(\mathbf{c}_i) \setminus \overline{D} = \text{supp}(\mathbf{c}_i') \setminus \overline{D} = \emptyset$ for each i.

Consider first the intersections among the coordinates in $\overline{D}$. For this purpose, let $\mathbf{c}_{Di}$ and $\mathbf{c}_{Di}'$ be words of $\mathbb{F}^b$ such that $\text{supp}(\mathbf{c}_{Di}) = \text{supp}(\mathbf{c}_i)$ and $\text{supp}(\mathbf{c}_{Di}') = \text{supp}(\mathbf{c}_i')$ for $i \in \{0, 1, 2\}$. Notice that $\mathbf{c}_{Di}$ and $\mathbf{c}_{Di}'$ preserve the distances, that is, $d(\mathbf{c}_{Di}, \mathbf{c}_{Dj}) = d(\mathbf{c}_i, \mathbf{c}_j)$ and $d(\mathbf{c}_{Di}', \mathbf{c}_{Dj}') = d(\mathbf{c}_i', \mathbf{c}_j')$. Then denote $S_h^b = B_h(\mathbb{F}^b; \mathbf{c}_{D0}) \cap B_h(\mathbb{F}^b; \mathbf{c}_{D1}) \cap B_h(\mathbb{F}^b; \mathbf{c}_{D2})$ and $S_h'^b = B_h(\mathbb{F}^b; \mathbf{c}_{D0}') \cap B_h(\mathbb{F}^b; \mathbf{c}_{D1}') \cap B_h(\mathbb{F}^b; \mathbf{c}_{D2}')$. Now we have $|S_h'^{\,b}| \geq |S_h{}^b|$ by [17, Theorem 2.4.10].

Now, we are ready to determine $|S|$ and $|S'|$. Notice that $|S_{t-i}^b|$ is equal to the number of words $\mathbf{y} \in S$ such that $\text{supp}(\mathbf{y})\setminus\overline{D}$ is fixed and contains $i \leq \ell-2$ elements. Therefore, we obtain that $|S| = \sum_{i=0}^{\ell-2} \binom{n-b}{i} |S_{t-i}^b|$. Similarly, we get $|S'| = \sum_{i=0}^{\ell-2} \binom{n-b}{i} |S_{t-i}'^b|$. Thus, as $|S_h{}^b| \leq |S_h'^{\,b}|$, we have $|S| \leq |S'|$. □

Now we are ready to present the proof of Lemma 18.

Lemma 18. *Let* $b \geq 3t$ *be an integer with* $t = e + \ell$ *and* C_1 *be an e-error-correcting code. Assume that* $n \geq (\ell-1)^2(b - e + (e+1)(b - 3e - 2e^2 + eb + \binom{b-2e-1}{2}))) + \ell - 2$*,* $|Y| = N \geq V(n, \ell-1) + 1$*,* $|T(Y)| \geq 3$ *and* $\mathbf{c}_0, \mathbf{c}_1, \mathbf{c}_2 \in T(Y)$*. If now* $\overline{D} \subseteq [1, n]$ *is a set such that* $|\overline{D}| = b$ *and*

$$\textit{supp}(\mathbf{c}_0 + \mathbf{c}_1) \cup \textit{supp}(\mathbf{c}_0 + \mathbf{c}_2) \cup \textit{supp}(\mathbf{c}_1 + \mathbf{c}_2) \subseteq \overline{D},$$

then for any word $\mathbf{w} \in \mathbb{F}^n$ *we have supp*$(\mathbf{w} + \mathbf{c}_0) \setminus \overline{D} =$ *supp*$(\mathbf{w} + \mathbf{c}_1) \setminus \overline{D} =$ *supp*$(\mathbf{w} + \mathbf{c}_2) \setminus \overline{D}$ *and there exists an output word* $\mathbf{y} \in Y$ *such that*

$$|\textit{supp}(\mathbf{y} + \mathbf{c}_0) \setminus \overline{D}| \geq \ell - 1.$$

Proof. Let $\mathbf{c}_0$, $\mathbf{c}_1$ and $\mathbf{c}_2$ be codewords of $T(Y)$ (with respect to C_1). Indeed, such codewords exist as $|T(Y)| \geq 3$. Observe that $\ell \geq 2$ by Theorem 7 as $\mathcal{L} \geq |T(Y)| \geq 3$. Let $\overline{D}$ be a subset of $[1, n]$ such that $|\overline{D}| = b$ and $\text{supp}(\mathbf{c}_0+\mathbf{c}_1) \cup \text{supp}(\mathbf{c}_0+\mathbf{c}_2) \cup \text{supp}(\mathbf{c}_1+\mathbf{c}_2) \subseteq \overline{D}$. In other words, all differences between codewords $\mathbf{c}_0$, $\mathbf{c}_1$ and $\mathbf{c}_2$ are contained in the set $\overline{D}$. Without loss of generality, we may assume that $\overline{D} = [1, b]$ (by rearranging the coordinate positions if needed). Further, denote $D = [1, n] \setminus \overline{D} = [b+1, n]$.

In order to show that there exists an output word $\mathbf{y}$ such that $|\text{supp}(\mathbf{y} + \mathbf{c}_0) \setminus \overline{D}| \geq \ell - 1$, we prove that

$$N > |S|, \quad (15)$$

where

$$S = \{\mathbf{w} \in \mathbb{F}^n \mid \mathbf{w} \in \bigcap_{i=0}^{2} B_t(\mathbf{c}_i) \text{ and } \\ |\text{supp}(\mathbf{w}+\mathbf{c}_0) \setminus \overline{D}| < \ell - 1\}$$

(when n is large enough). Moreover, if such $\mathbf{y}$ exists, then by Equation (14) we have $\text{supp}(\mathbf{y} + \mathbf{c}_0) \setminus \overline{D} = \text{supp}(\mathbf{y} + \mathbf{c}_1) \setminus \overline{D} = \text{supp}(\mathbf{y} + \mathbf{c}_2) \setminus \overline{D}$. Therefore, all the codewords $\mathbf{c}_i$ have symmetrical roles (albeit at first sight it might seem that $\mathbf{c}_0$ has a special role). By Lemma 37, $|S|$ obtains its maximum value when the codewords $\mathbf{c}_0$, $\mathbf{c}_1$ and $\mathbf{c}_2$ are as close to each other as possible. Recalling that $d(\mathbf{c}_i, \mathbf{c}_j) \geq 2e + 1$ for any distinct $i, j \in \{0, 1, 2\}$ and the parity of all the distances cannot be odd (see Equation (5)), we may without loss of generality assume (by the symmetry of $\mathbf{c}_0$, $\mathbf{c}_1$ and $\mathbf{c}_2$) that $d(\mathbf{c}_1, \mathbf{c}_2) = 2e + 2$ and $d(\mathbf{c}_0, \mathbf{c}_1) = d(\mathbf{c}_0, \mathbf{c}_2) = 2e + 1$. Furthermore, we may without loss of generality assume that $\mathbf{c}_0 = \mathbf{0}$ (as the whole Hamming space can be translated by $\mathbf{c}_0$).

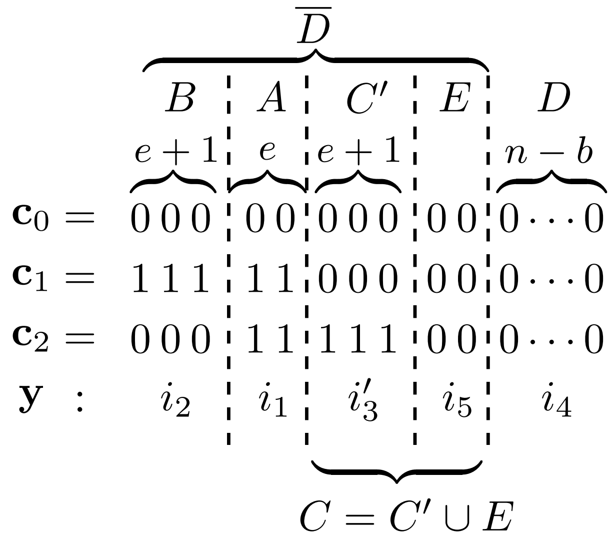
$\overline{D}$
B
A
C'
E
D
$e+1$
e
$e+1$
$n-b$
$\mathbf{c}_0 =$ 0 0 0 0 0 0 0 0 0 0 $0 \cdots 0$
$\mathbf{c}_1 =$ 1 1 1 1 1 0 0 0 0 0 $0 \cdots 0$
$\mathbf{c}_2 =$ 0 0 0 1 1 1 1 1 0 0 $0 \cdots 0$
$\mathbf{y}$: i_2 i_1 i_3' i_5 i_4
$C = C' \cup E$

Fig. 6. An illustration of the proof of Lemma 18 when $e = 2$.

Denote then $A = \text{supp}(\mathbf{c}_1) \cap \text{supp}(\mathbf{c}_2)$, $B = \text{supp}(\mathbf{c}_1) \setminus \text{supp}(\mathbf{c}_2)$, $C' = \text{supp}(\mathbf{c}_2) \setminus \text{supp}(\mathbf{c}_1)$ and $E = \overline{D} \setminus (\text{supp}(\mathbf{c}_1) \cup \text{supp}(\mathbf{c}_2))$ (see Figure 6 for illustration of these sets). Notice that $A \cup B \cup C'$ contains every coordinate in which the words $\mathbf{c}_0$, $\mathbf{c}_1$ and $\mathbf{c}_2$ differ. Straightforwardly, we obtain that

$$\begin{aligned} &|A| = e, \\ &|B| = |C'| = e+1, \\ &|E| = b - |A| - |B| - |C'| \text{ and} \\ &|D| = n - b. \end{aligned} \tag{16}$$

For a word $\mathbf{y} \in S$, we further denote $|\text{supp}(\mathbf{y}) \cap A| = i_1$, $|\text{supp}(\mathbf{y}) \cap B| = i_2$, $|\text{supp}(\mathbf{y}) \cap C'| = i'_3$, $|\text{supp}(\mathbf{y}) \cap D| = i_4$ and $|\text{supp}(\mathbf{y}) \cap E| = i_5$. In what follows, we prove our goal (15), that is,

$$|S| < V(n, \ell - 1) + 1 \leq N.$$

For this purpose, we first present some bounds on the values i_1, i_2, i'_3, i_4 and i_5.

Immediately, by the definition of S, we obtain that

$$0 \leq i_4 \leq \ell - 2. \tag{17}$$

Furthermore, as $d(\mathbf{y}, \mathbf{c}_i) \leq t$ for $i \in \{1, 2\}$, we have

$$\begin{aligned} &i_4 + i_5 + (|A| - i_1) + (|B| - i_2) + i'_3 \leq t \\ &\text{and} \\ &i_4 + i_5 + (|A| - i_1) + (|C'| - i'_3) + i_2 \leq t. \end{aligned} \tag{18}$$

Now, by adding these two inequalities, and recalling (16) and $t = e + \ell$, we get

$$e + 1 + i_4 + i_5 - \ell \leq i_1 \leq |A| = e. \tag{19}$$

This further implies that

$$0 \leq i_5 \leq \ell - 1 - i_4. \tag{20}$$

By (18), the value $|i_2 - i'_3|$ can be bounded from above as follows: by combining the inequalities, we obtain $i_4 + i_5 + (|A| - i_1) + (e+1) + |i_2 - i'_3| \leq t$ implying $|i_2 - i'_3| \leq \ell - i_4 - i_5 - (|A| - i_1) - 1$. It is straightforward to verify that $i_2 - |i_2 - i'_3| \leq i'_3 \leq i_2 + |i_2 - i'_3|$. Hence, combining this inequality with the previous one for $|i_2 - i'_3|$ and recalling $|A| = e$, we obtain that

$$\begin{aligned} &i_2 + i_4 + i_5 + e + 1 - \ell - i_1 \\ =&i_2 - (\ell - i_4 - i_5 - (|A| - i_1) - 1) \\ \leq&i'_3 \\ \leq&i_2 + (\ell - i_4 - i_5 - (|A| - i_1) - 1) \\ =&i_1 + i_2 + \ell - e - 1 - i_4 - i_5. \end{aligned} \tag{21}$$

Finally, as $d(\mathbf{y}, \mathbf{c}_0) \leq t$, we have $i_1 + i_2 + i'_3 + i_4 + i_5 \leq t$. Therefore, as $i'_3 \geq i_2 - |i_2 - i'_3|$, we obtain that $t - i_1 - i_4 - i_5 \geq i_2 + i'_3 \geq 2i_2 - |i_2 - i'_3| \geq 2i_2 + i_4 + i_5 + e + 1 - \ell - i_1$. Hence, we get

$$0 \leq i_2 \leq \ell - 1 - i_4 - i_5. \tag{22}$$

In the following sums, we agree that $\binom{p}{q} = 0$ when $q < 0$. The size of S can now be approximated based on the bounds (17), (19), (20), (21) and (22).

$$\begin{aligned} |S| \leq& \\ &\sum_{i_4=0}^{\ell-2} \sum_{i_5=0}^{\ell-1-i_4} \sum_{i_1=i_4+i_5+e+1-\ell}^{e} \sum_{i_2=0}^{\ell-1-i_4-i_5} \sum_{i'_3=i_2+i_4+i_5+e+1-\ell-i_1}^{i_1+i_2+\ell-e-1-i_4-i_5} \\ &\binom{|D|}{i_4}\binom{|E|}{i_5}\binom{|A|}{i_1}\binom{|B|}{i_2}\binom{|C'|}{i'_3} \\ \overset{(i)}{\leq}& \sum_{i_4=0}^{\ell-2} \sum_{i_1=i_4+e+1-\ell}^{e} \sum_{i_2=0}^{\ell-1-i_4} \sum_{i_5=0}^{\ell-1-i_4} \sum_{i'_3=i_2+i_4+i_5+e+1-\ell-i_1}^{i_1+i_2+\ell-e-1-i_4-i_5} \\ &\binom{|D|}{i_4}\binom{|A|}{i_1}\binom{|B|}{i_2}\binom{|E|}{i_5}\binom{|C'|}{i'_3} \\ \overset{(ii)}{\leq}& \sum_{i_4=0}^{\ell-2} \sum_{i_1=i_4+e+1-\ell}^{e} \sum_{i_2=0}^{\ell-1-i_4} \sum_{i_3=i_2+i_4+e+1-\ell-i_1}^{i_1+i_2+\ell-e-1-i_4} \\ &\binom{|D|}{i_4}\binom{|A|}{i_1}\binom{|B|}{i_2}\binom{|C|}{i_3}. \end{aligned}$$

In Step (i), we first relax the restrictions set by i_5 for i_1 and i_2. Furthermore, in Step (ii), we denote $C = C' \cup E$ and combine the binomial sums considering i'_3 and i_5. Indeed, this can be done since on the left-hand side i_5 elements are chosen from E and i'_3 elements from C' while on the right-hand side $i'_3 + i_5$ elements are chosen from $C' \cup E$. In order to further estimate the binomial sum on the right-hand side of the previous inequality (after Step (ii)), we partition it into smaller pieces using the following notations:

$$\begin{aligned} G(i_4) = &\sum_{i_1=i_4+e+1-\ell}^{e} \sum_{i_2=0}^{\ell-1-i_4} \sum_{i_3=i_2+i_4+e+1-\ell-i_1}^{i_1+i_2+\ell-e-1-i_4} \\ &\binom{|A|}{i_1}\binom{|B|}{i_2}\binom{|C|}{i_3} \end{aligned} \tag{23}$$

and

$$g(i_4) = \binom{|D|}{i_4} G(i_4). \tag{24}$$

Thus, we have

$$|S| \leq \sum_{i_4=0}^{\ell-2} g(i_4) = \sum_{i_4=0}^{\ell-2} \binom{|D|}{i_4} G(i_4). \tag{25}$$

Recall the assumption

$$\begin{aligned} n \geq (\ell-1)^2 \big(b - e + (e+1)\big(b - 3e - 2e^2 + eb \\ + \binom{b-2e-1}{2}\big)\big) + \ell - 2 \end{aligned} \tag{26}$$

(which is needed for n to be large enough). Now we outline the rest of the proof:

Part (a) We first show that

$$\begin{aligned} G(i_4 - 1) \leq \bigg(1 + \frac{e(|B||C| + 4)}{8} + |C| \\ + \frac{|B|(|C|+1)^2}{12}\bigg) G(i_4). \end{aligned} \tag{27}$$

Part (b) Then, based on this approximation, we prove that $g(i_4 - 1) \leq g(i_4)$ for any $i_4 = 1, \ldots, \ell - 2$. Therefore, for any $j \in [0, \ell-2]$, we have $g(j) \leq g(\ell-2)$.

Part (c) Thus, we have $|S| \leq (\ell-1)\binom{|D|}{\ell-2}G(\ell-2)$. Finally, it can be shown that $|S| \leq (\ell-1)\binom{|D|}{\ell-2}G(\ell-2) < N$, so our goal (15) follows. Therefore, there exists an output word $\mathbf{y} \in Y$ such that $|\mathrm{supp}(\mathbf{y}+\mathbf{c}_0) \setminus \overline{D}| \geq \ell - 1$.

Part (a): By comparing the sums $G(i_4)$ and $G(i_4-1)$, we first notice that the sum $G(i_4-1)$ contains every term in $G(i_4)$. The sum $G(i_4-1)$ may contain only three different types of additional terms: (I) the ones with $i_1 = (i_4-1)+e+1-\ell = i_4+e-\ell$, (II) the ones with $i_1 \in [i_4+e+1-\ell, e]$ and $i_2 = \ell-1-(i_4-1) = \ell-i_4$ and (III) the ones where $i_1 \in [i_4+e+1-\ell, e]$, $i_2 \in [0, \ell-1-i_4]$ and i_3 is either equal to $i_2+(i_4-1)+e+1-\ell-i_1 = i_2+i_4+e-\ell-i_1$ or $i_1+i_2+\ell-e-1-(i_4-1) = i_1+i_2+\ell-e-i_4$. For the additional terms (I), (II) and (III), we respectively use the notations $f(i_4)$, $s(i_4)$ and $h(i_4)$:

$$f(i_4) = \binom{|A|}{i_4+e-\ell}\sum_{i_2=0}^{\ell-i_4}\binom{|B|}{i_2}\binom{|C|}{i_2},$$

$$s(i_4) = \binom{|B|}{\ell-i_4}\sum_{i_1=i_4+e+1-\ell}^{e}\binom{|A|}{i_1}\sum_{i_3=e-i_1}^{i_1+2\ell-e-2i_4}\binom{|C|}{i_3}$$

and

$$h(i_4) = \sum_{i_1=i_4+e+1-\ell}^{e}\binom{|A|}{i_1}\sum_{i_2=0}^{\ell-1-i_4}\binom{|B|}{i_2} \cdot \left(\binom{|C|}{i_1+i_2+\ell-e-i_4} + \binom{|C|}{i_2+i_4+e-\ell-i_1}\right).$$

Thus, we have

$$G(i_4-1) \leq G(i_4) + f(i_4) + h(i_4) + s(i_4). \tag{28}$$

In order to prove Inequality (27), we first present upper bounds for $f(i_4)$, $h(i_4)$ and $s(i_4)$ with the aid of $G(i_4)$. For this purpose, we first present the following auxiliary result:

$$\binom{n}{a+1} = \frac{n-a}{a+1}\binom{n}{a} \iff \binom{n}{a} = \frac{a+1}{n-a}\binom{n}{a+1}. \tag{29}$$

Now an upper bound for the $f(i_4)$ can be obtained as follows:

$$\begin{aligned}
f(i_4) &= \binom{|A|}{i_4+e-\ell}\sum_{i_2=0}^{\ell-i_4}\binom{|B|}{i_2}\binom{|C|}{i_2} \\
&\overset{(29)}{=} \frac{i_4+e+1-\ell}{\ell-i_4}\binom{|A|}{i_4+e+1-\ell} \\
&\quad \cdot \left(\sum_{i_2=0}^{\ell-i_4-1}\binom{|B|}{i_2}\binom{|C|}{i_2} + \frac{i_4+|B|+1-\ell}{\ell-i_4}\right. \\
&\quad \left. \cdot \frac{i_4+|C|+1-\ell}{\ell-i_4}\binom{|B|}{\ell-i_4-1}\binom{|C|}{\ell-i_4-1}\right) \\
&\overset{(iii)}{\leq} \frac{i_4+e+1-\ell}{\ell-i_4} \\
&\quad \cdot \left(1 + \frac{i_4+|B|+1-\ell}{\ell-i_4} \cdot \frac{i_4+|C|+1-\ell}{\ell-i_4}\right) \\
&\quad \cdot \binom{|A|}{i_4+e+1-\ell}\sum_{i_2=0}^{\ell-1-i_4}\binom{|B|}{i_2}\binom{|C|}{i_2} \\
&\overset{(iv)}{\leq} \frac{i_4+e+1-\ell}{\ell-i_4} \\
&\quad \cdot \left(1 + \frac{i_4+|B|+1-\ell}{\ell-i_4} \cdot \frac{i_4+|C|+1-\ell}{\ell-i_4}\right) G(i_4) \\
&\overset{(v)}{\leq} \frac{e(|B||C|+4)}{8}G(i_4).
\end{aligned}$$

Here, in Step (iii), we estimate $\binom{|B|}{\ell-i_4-1}\binom{|C|}{\ell-i_4-1} \leq \sum_{i_2=0}^{\ell-i_4-1}\binom{|B|}{i_2}\binom{|C|}{i_2}$. Then, in Step (iv), we observe that the terms of

$$\binom{|A|}{i_4+e+1-\ell}\sum_{i_2=0}^{\ell-1-i_4}\binom{|B|}{i_2}\binom{|C|}{i_2}$$

appear in $G(i_4)$ when $i_1 = i_4+e+1-\ell$. Finally, in Step (v), we approximate $i_4 \leq \ell-2$ (i.e. $\ell \geq i_4+2$) and disregard some small negative constants.

The value $h(i_4)$ can be approximated as follows:

$$\begin{aligned}
h(i_4) &\overset{(29)}{=} \sum_{i_1=i_4+e+1-\ell}^{e}\binom{|A|}{i_1}\sum_{i_2=0}^{\ell-1-i_4}\binom{|B|}{i_2} \\
&\quad \cdot \Bigg(\frac{|C|+i_4+e+1-\ell-i_1-i_2}{i_1+i_2+\ell-e-i_4} \\
&\quad \cdot \binom{|C|}{i_1+i_2+\ell-e-1-i_4} \\
&\quad + \frac{i_2+i_4+e+1-\ell-i_1}{|C|+i_1+\ell-e-i_2-i_4}\binom{|C|}{i_2+i_4+e+1-\ell-i_1}\Bigg) \\
&\overset{(vi)}{\leq} |C|\sum_{i_1=i_4+e+1-\ell}^{e}\binom{|A|}{i_1}\sum_{i_2=0}^{\ell-1-i_4}\binom{|B|}{i_2} \\
&\quad \cdot \Bigg(\binom{|C|}{i_1+i_2+\ell-e-1-i_4} \\
&\quad + \binom{|C|}{i_2+i_4+e+1-\ell-i_1}\Bigg) \\
&\overset{(vii)}{\leq} |C|G(i_4).
\end{aligned}$$

For Inequality (vi), we first observe that $|C| - i_2 = b - 2e - 1 - i_2 \geq t + \ell > i_2$ since $b \geq 3t$ and $\ell - 1 \geq i_2$ by (22). Therefore, as $i_2 \geq 0$ and $i_1 \geq i_4 + e + 1 - \ell$, we obtain that

$$\begin{aligned} &\frac{i_2+i_4+e+1-\ell-i_1}{|C|+i_1+\ell-e-i_2-i_4} \\ <&\frac{|C|+i_4+e+1-\ell-i_1-i_2}{i_1+i_2+\ell-e-i_4}\\ \leq&\frac{|C|+i_4+e+1-\ell-i_1}{i_1+\ell-e-i_4}\\ \leq&|C|.\end{aligned}$$

Then, in Step (vii), we observe that the terms of

$$\begin{aligned} &\sum_{i_1=i_4+e+1-\ell}^{e}\binom{|A|}{i_1}\sum_{i_2=0}^{\ell-1-i_4}\binom{|B|}{i_2}\\ &\cdot\left(\binom{|C|}{i_1+i_2+\ell-e-1-i_4}\right.\\ &\left.+\binom{|C|}{i_2+i_4+e+1-\ell-i_1}\right)\end{aligned}$$

appear in $G(i_4)$ when either $i_3 = i_1 + i_2 + \ell - e - 1 - i_4$ or $i_3 = i_2 + i_4 + e + 1 - \ell - i_1$.

Finally, we derive the following upper bound for $s(i_4)$:

$$\begin{aligned} s(i_4)\overset{(29)}{=}&\frac{|B|+i_4+1-\ell}{\ell-i_4}\binom{|B|}{\ell-i_4-1}\\ &\cdot\sum_{i_1=i_4+e+1-\ell}^{e}\binom{|A|}{i_1}\sum_{i_3=e-i_1}^{i_1+2\ell-e-2i_4}\binom{|C|}{i_3}\\ =&\frac{|B|+i_4+1-\ell}{\ell-i_4}\binom{|B|}{\ell-i_4-1}\\ &\cdot\sum_{i_1=i_4+e+1-\ell}^{e}\binom{|A|}{i_1}\left(\sum_{i_3=e-i_1}^{i_1+2\ell-e-2-2i_4}\binom{|C|}{i_3}\right.\\ &+\frac{|C|+2i_4+e+2-2\ell-i_1}{i_1+2\ell-e-1-2i_4}\\ &\cdot\left(\frac{|C|+2i_4+e+1-2\ell-i_1}{i_1+2\ell-e-2i_4}+1\right)\\ &\left.\cdot\binom{|C|}{i_1+2\ell-e-2-2i_4}\right)\\ \overset{(viii)}{\leq}&\frac{|B|-1}{2}\left(1+\frac{|C|-1}{2}\left(1+\frac{|C|-2}{3}\right)\right)\\ &\cdot\binom{|B|}{\ell-1-i_4}\sum_{i_1=i_4+e+1-\ell}^{e}\binom{|A|}{i_1}\sum_{i_3=e-i_1}^{i_1+2\ell-e-2-2i_4}\binom{|C|}{i_3}\\ \overset{(ix)}{\leq}&\frac{|B|-1}{2}\left(1+\frac{|C|-1}{2}\left(1+\frac{|C|-2}{3}\right)\right)G(i_4)\\ <&\frac{|B|(|C|+1)^2}{12}G(i_4).\end{aligned}$$

Here, in Step $(viii)$, we bound from above the fractional multipliers by first estimating $i_1 \geq i_4+e+1-\ell$ (see (19)) and then approximating $i_4 \leq \ell-2$ (see (17)). Then, in Step (ix), we observe that the terms of

$$\binom{|B|}{\ell-1-i_4}\sum_{i_1=i_4+e+1-\ell}^{e}\binom{|A|}{i_1}\sum_{i_3=e-i_1}^{i_1+2\ell-e-2-2i_4}\binom{|C|}{i_3}$$

appear in $G(i_4)$ when $i_2 = \ell - 1 - i_4$.

Thus, in conclusion, Inequality 27 is obtained by combining (28) and the previous estimations for $f(i_4)$, $h(i_4)$ and $s(i_4)$:

$$\begin{aligned} &G(i_4-1)\\ \leq&G(i_4)+f(i_4)+h(i_4)+s(i_4)\\ \leq&\left(1+\frac{e(|B||C|+4)}{8}+|C|+\frac{|B|(|C|+1)^2}{12}\right)G(i_4).\end{aligned}$$

Part (b): By (24), (27) and (29), we now obtain that

$$\begin{aligned} &g(i_4-1)\\ =&G(i_4-1)\binom{|D|}{i_4-1}\\ \leq&\left(1+\frac{e(|B||C|+4)}{8}+|C|+\frac{|B|(|C|+1)^2}{12}\right)\\ &\cdot G(i_4)\binom{|D|}{i_4}\frac{i_4}{|D|-i_4+1}\\ =&\left(1+\frac{e(|B||C|+4)}{8}+|C|+\frac{|B|(|C|+1)^2}{12}\right)\\ &\cdot\frac{i_4}{|D|-i_4+1}g(i_4).\end{aligned}$$

Thus, we have $g(i_4-1) \leq g(i_4)$ if

$$\begin{aligned} &|D|-i_4+1\\ \geq&i_4\cdot\left(1+\frac{e(|B||C|+4)}{8}+|C|+\frac{|B|(|C|+1)^2}{12}\right),\\ &\text{i.e.}\\ n\geq&i_4\cdot\left(1+\frac{e(|B||C|+4)}{8}+|C|+\frac{|B|(|C|+1)^2}{12}\right)\\ &+i_4+b-1.\end{aligned}$$

Therefore, we have $g(j) \leq g(\ell-2)$ for any $j \in [0, \ell-3]$ if

$$\begin{aligned} &n\\ \geq&\left(1+\frac{e(|B||C|+4)}{8}+|C|+\frac{|B|(|C|+1)^2}{12}\right)\\ &\cdot(\ell-2)+(\ell-2)-1+b.\end{aligned}\tag{30}$$

In order to show that n satisfies this condition, we obtain by recalling the assumption (26) for n and Equation (16) that

$$\begin{aligned}
n \geq{} & (\ell-1)^2 \left(b-e+(e+1)\right. \\
& \left.\cdot \left(b-3e-2e^2+eb+\binom{b-2e-1}{2}\right)\right)+\ell-2 \\
={} & (\ell-1)^2 \left(|C|+|B|\left(2+|C|+e|C|+\binom{|C|}{2}\right)\right)+\ell-2 \\
\geq{} & (\ell-2)\left(|C|+|B|\left(2+|C|+e|C|+\binom{|C|}{2}\right)\right) \\
& +\ell-3+b \\
={} & \left(2|B|+\frac{4e|B||C|+4e|B||C|}{8}+|C|+6|B|\frac{|C|^2+|C|}{12}\right) \\
& \cdot(\ell-2)+\ell-3+b \\
\overset{(x)}{>} & \left(1+\frac{e(|B||C|+4)}{8}+|C|+\frac{|B|(|C|+1)^2}{12}\right) \\
& \cdot(\ell-2)+\ell-3+b.
\end{aligned} \tag{31}$$

Here, in Step (x), we use the following estimations: $2|B|>1$, $(4e|B||C|+4e|B||C|)/8>e(|B||C|+4)/8$ and $6|B|(|C|^2+|C|)/12=3|B|(2|C|^2+2|C|)/12>|B|(|C|^2+2|C|+1)/12$. Thus, we have $g(j)\leq g(\ell-2)$ for any $j\in[0,\ell-3]$. This concludes Part (b).

Part (c): Substituting $i_4=\ell-2$ to $G(i_4)$ in Equation (23) gives: $G(\ell-2)=|C|+|B|(1+|C|+e|C|+\binom{|C|}{2})+e+1=|C|+|B|(2+|C|+e|C|+\binom{|C|}{2})$ (recall here that $|B|=e+1$). Therefore, as $g(i_4)\leq g(\ell-2)$ for any $i_4\in[0,\ell-3]$ when n is large enough, we may estimate $|S|$ using Inequality (25):

$$\begin{aligned}
|S|\leq{} & \sum_{i_4=0}^{\ell-2} g(i_4)\leq(\ell-1)g(\ell-2) \\
={} & (\ell-1)\binom{|D|}{\ell-2}G(\ell-2) \\
<{} & (\ell-1)\binom{n}{\ell-2}G(\ell-2) \\
={} & \frac{(\ell-1)^2}{n-\ell+2}\binom{n}{\ell-1} \\
& \cdot\left(|C|+|B|\left(2+|C|+e|C|+\binom{|C|}{2}\right)\right).
\end{aligned}$$

Therefore, (recall our goal (15)), $|S|<\binom{n}{\ell-1}<N$ since the assumption $n\geq(\ell-1)^2\cdot\left(|C|+|B|\left(2+|C|+e|C|+\binom{|C|}{2}\right)\right)+\ell-2\overset{(31)}{=}(\ell-1)^2\cdot(b-e+(e+1)(b-3e-2e^2+eb+\binom{b-2e-1}{2})))+\ell-2$ implies $n-\ell+2\geq(\ell-1)^2\left(|C|+|B|\left(2+|C|+e|C|+\binom{|C|}{2}\right)\right)$. Thus, in conclusion, there exists an output word $\mathbf{y}\in Y$ such that $\mathbf{y}\notin S$ since $|S|<N$. □

Ville Junnila received the M.Sc. and Ph.D. degrees in mathematics from the University of Turku, Finland, in 2007 and 2011, respectively. He was a Postdoctoral Researcher on a grant in 2011–2014. Then, in 2014, he joined the faculty of the Department of Mathematics and Statistics at the University of Turku, where he is currently a University Lecturer. His research interests include combinatorial coding and graph theory as well as related areas of discrete mathematics.

Tero Laihonen received the M.Sc. and Ph.D. degrees in mathematics from the University of Turku, Turku, Finland, in 1995 and 1998, respectively. He was a Postdoctoral Researcher in 1999-2002 and an Academy Research Fellow in 2003-2008 at the Academy of Finland. He joined the faculty of the Department of Mathematics and Statistics at the University of Turku in 2008 where he is currently a Full Professor in discrete mathematics and theoretical computer science. His research interests include coding theory, graph theory and related areas of discrete mathematics.

Tuomo Lehtilä received the M.Sc. degree in mathematics from the University of Turku, Turku, Finland, in 2016. He is currently pursuing the Ph.D. degree in mathematics with University of Turku. His current research interests include coding theory, graph theory and related areas of discrete mathematics.