Generalized Unique Reconstruction From Substrings

Yonatan Yehezkeally, Member, IEEE, Daniella Bar-Lev, Student Member, IEEE, Sagi Marcovich, Student Member, IEEE, and Eitan Yaakobi, Senior Member, IEEE

Abstract—This paper introduces a new family of reconstruction codes which is motivated by applications in DNA data storage and sequencing. In such applications, DNA strands are sequenced by reading some subset of their substrings. While previous works considered two extreme cases in which all substrings of pre-defined lengths are read or substrings are read with no overlap for the single string case, this work studies two extensions of this paradigm. The first extension considers the setup in which consecutive substrings are read with some given minimum overlap. First, an upper bound is provided on the attainable rates of codes that guarantee unique reconstruction. Then, efficient constructions of codes that asymptotically meet that upper bound are presented. In the second extension, we study the setup where multiple strings are reconstructed together. Given the number of strings and their length, we first derive a lower bound on the read substrings’ length \( \ell \) that is necessary for the existence of multi-strand reconstruction codes with non-vanishing rates. We then present two constructions of such codes and show that their rates approach 1 for values of \( \ell \) that asymptotically behave like the lower bound.

Index Terms—Sequence reconstruction, DNA sequences, error correction codes, worst-case analysis.

I. INTRODUCTION

STRING reconstruction refers to a large class of problems where information about a string can only be obtained in the form of multiple, incomplete and/or noisy observations. Examples of such problems are the reconstruction problem by Levenshtein [20], the trace reconstruction problem [3], [6], and the k-deck problem [8], [9], [23], [32].

Notably, when observations are comprised of unordered consecutive substrings, two distinct models have received significant interest in the past decade due to applications in DNA- or polymer-based storage systems, resulting from contemporary sequencing technologies [4], [11], [15], [18], [24], [26], [27], [33], [35], [39] (including extensions for erroneous observations [5], [13], [24], [39]), which arise from an idealized assumption of full overlap (and uniform coverage) in read substrates; the second is the torn-paper problem [2], [28], [29], [36] (a problem closely related to the shuffling channel [16], [19], [34], [38]), which results from an assumption of no overlap. In applications, the distinction models the question of whether the complete information string may be replicated and uniformly segmented for sequencing, or if segmentation occurs adversarially in the medium prior to sequencing.

Motivated by these two paradigms, we study in this paper a generalized (or intermediate) setting where an information string is observed through an arbitrary collection of its substrings, where the minimum length of each retrieved substring, as well as the length of overlap between consecutive substrings, are bounded from below. A similar setting was recently studied in [30], where both substrings’ lengths and overlap were assumed to be random; we study the problem in the aforementioned worst-case regime.

Further, in both sequencing and tandem-mass-spectrometry technologies, used for DNA and polymer-based storage systems respectively, it is typical that not a single string is read alone, but multiple strings simultaneously [7], [14], [17], [22], [31]. We therefore study a setting where retrieved substrings are taken from a collection of information strings stored together, with no information on the string from which they originated. We remark that this extension was already studied by the authors for the torn-paper problem, in [2].

Our problem setting is therefore given as follows: a multiset of \( k \) length-\( n \) strings is transmitted, and substrings of all information strings are retrieved, such that the length of each substring is at least \( \ell_{\text{min}} \), and consecutive substrings of the same information string overlap in at least \( \ell_{\text{over}} \) positions. We are interested in the minimum value of \( \ell_{\text{min}} \), as a function of \( k \) and \( n \), for which there exist codes allowing for unique reconstruction in this channel with asymptotically non-vanishing rates, and then what is the asymptotically optimal obtainable rate given the value of \( \ell_{\text{over}} \). In these cases, we seek to develop efficient coding schemes which asymptotically attain optimal rates.
The rest of this paper is organized as follows. In Section II, we present notation and definitions which are used throughout the paper. In Section III, we overview and extend results in existing literature which already solve our problem setting in specific end-cases. In Sections IV and V, we present a solution to the aforementioned problem in the private case of a single string ($k = 1$), by respectively bounding from above the asymptotically attainable rate of codes for unique reconstruction as a function of $\ell_{\text{min}}, \ell_{\text{over}}$, and then developing efficient encoding and decoding algorithms for such codes, asymptotically meeting this bound. Then, in Section VI, we study solutions to the problem in a different private case, where $\ell_{\text{over}} = \ell_{\text{min}} - 1$ (i.e., a multi-strand extension of the reconstruction from substrings problem); we likewise present bounds and two efficient constructions of multiset-codes for this case, whose rates asymptotically approach 1 for values of $\ell_{\text{min}}$ asymptotically equivalent to the lower bound. We conclude in Section VII with a summary and closing remarks.

II. DEFINITIONS AND PRELIMINARIES

Let $\Sigma$ be a finite alphabet of size $q$. Where advantageous, we assume $\Sigma$ is equipped with a ring structure, and in particular identify elements $0, 1 \in \Sigma$. For a positive integer $n$, let $[n]$ denote the set $[n] \triangleq \{0, 1, \ldots, n - 1\}$. We denote a multiset by $S = \{(a, a, b, \ldots)\}$; i.e., elements are allowed to appear with multiplicity. For convenience we let $|S|$, for a multiset $S$, denote the number of unique elements in $S$.

For two non-negative functions $f, g$ of a common variable $n$, denoting $L \triangleq \limsup_{n \to \infty} \frac{f(n)}{g(n)}$ (in the wide sense) we say that $f = o(n)$ if $L = 0$, $f = \Omega(n)$ if $L > 0$, $f = O(n)$ if $L < \infty$, and $f = \omega(n)$ if $L = \infty$. We say that $f = \Theta(n)$ if $f = \Omega(n)$ and $f = O(n)$. If $f$ is not positive, we say $f = o(n)$ if $f = \omega(n)$. We denote a prefix (suffix) of $x$ is a substring which is not complete (since $x$ is observed only through a multiset of substrings of $x$). For a positive integer $\ell$, we denote their concatenation of $v$ and $w$, respectively, $v \circ w$. We denote a prefix of $x$ is a substring which is not complete. Where advantageous, we extend the definitions of traces. Our channel accepts $x$ is not complete (since $i_1 > 0$).

Let $\Sigma^n$ denote the set of all finite strings over $\Sigma$. The length of a string $x = (x_0, x_1, \ldots, x_{n-1}) \in \Sigma^n$ is denoted by $|x| = n$. For strings $x, y \in \Sigma^n$, we denote their concatenation by $x \circ y$. We say that $y$ is a substring of $x$ if there exist strings $u, w$ such that $x = u \circ y \circ w$. If $u$ (respectively, $w$) is empty, we say that $y$ is a prefix (suffix) of $x$. If the length of $y$ is $\ell$, we specifically say $y$ is an $\ell$-substring of $x$. For $I \subseteq [|x|]$, we let $x_I$ denote the subsequence of $x$ obtained by restriction to the coordinates of $I$ (i.e., when $x$ is considered as a function from $[|x|]$ into $\Sigma$); specifically, for $i \in [|x| - \ell + 1]$ we denote by $x_{i+\ell}[i]$ the $\ell$-substring of $x$ at location $i$ (we reserve the term index for a different use), where $i + \ell = \{i + j : j \in \ell\}$.

We define $X_{n,k} \triangleq \{S : \{(x_1, \ldots, x_k) : \forall i, x_i \in \Sigma^n\}\},$ and observe that $|X_{n,k}| = \binom{n+k-1}{k-1}$. We consider in this paper the problem of multi-string reconstruction from substrings with partial overlap. That is, we assume that a message $S \in X_{n,k}$ is observed only through a multiset of substrings of its elements, without order or information on the substring from which they originate, with the following restrictions: (i) all observed substrings are of length at least $\ell_{\text{min}}$, and (ii) succeeding substrings of the same $x \in S$ overlap with length at least $\ell_{\text{over}}$ (in particular, every symbol of $x$ is observed in some substring).

More formally, a substring-trace of $x \in \Sigma^n$ is a multiset $\{x_{i_j,[\ell_j]} : 1 \leq j \leq m\}$, for some $m \in \mathbb{N}$, such that $i_1 < i_2 < \cdots < i_m$ and $\ell_j \in [n - i_j + 1]$. A substring-trace is complete if $i_1 = 0$, $i_{j+1} < i_j + \ell_j$ for all $j < m$, and $i_m + \ell_m = n$. A complete substring-trace of $x \in \Sigma^n$ is called an $(\ell_{\text{min}}, \ell_{\text{over}})$-trace if $\ell_j \geq \ell_{\text{min}} \geq \ell_{\text{over}}$ for all $j$, and $i_j + \ell_j - i_{j+1} \geq \ell_{\text{over}}$ for all $j < m$. For example, for $x = 1110110101111111$,

- $\{1110111, 111010, 10111\}$ is a $(6, 2)$-trace of $x$;
- $\{1111011, 110101, 10111\}$ is a complete substring-trace of $x$ which is not a $(6, 2)$-trace; and
- $\{1110111, 110101, 10111\}$ is a substring-trace of $x$ which is not complete (since $i_1 > 0$).

See Figures 1 to 3 for an illustration if these substring-traces.

The $(\ell_{\text{min}}, \ell_{\text{over}})$-trace spectrum of $x \in \Sigma^n$, denoted $T_{\ell_{\text{min}}}(x)$, is the set of all $(\ell_{\text{min}}, \ell_{\text{over}})$-traces of $x$. We extend the definition to $S \subseteq X_{n,k}$ by $T_{\ell_{\text{min}}}(S) \triangleq \bigcup_{x \in S} T_{\ell_{\text{min}}}(x)$, where the union respects multiplicity (i.e., multiset union), and similarly extend the definitions of traces. Our channel accepts $S \subseteq X_{n,k}$ and outputs a single arbitrary $(\ell_{\text{min}}, \ell_{\text{over}})$-trace of $S$.

For all $C \subseteq X_{n,k}$, we denote the rate, redundancy of $C$ by $R(C) \triangleq \frac{\log |C|}{\log |X_{n,k}|}$, resd($C) \triangleq \log |X_{n,k}| - \log |C|$, respectively. Throughout the paper, we use the base-$q$ logarithms. Motivated by the above channel definition, a code $C \subseteq \Sigma^n$ is called an $(\ell_{\text{min}}, \ell_{\text{over}})$-code if for all $c_1 \neq c_2 \in C$, $T_{\ell_{\text{min}}}(c_1) \cap T_{\ell_{\text{min}}}(c_2) = \emptyset$. We likewise define a multi-strand $(\ell_{\text{min}}, \ell_{\text{over}})$-code $C \subseteq X_{n,k}$. The main goal of this work is to find, for $(\ell_{\text{min}}, \ell_{\text{over}})$ as functions of $n, k$, the maximum asymptotic rate of (multi-strand) $(\ell_{\text{min}}, \ell_{\text{over}})$-code. We will also be interested in efficient constructions of codes with rate asymptotically approaching that value.

For convenience of analysis we denote by $\ell_{\text{min}}(x) = T_{\ell_{\text{min}}}(x)$, for $x \in \Sigma^n$, the $(\ell_{\text{min}}, \ell_{\text{over}})$-trace of $x$ containing specifically its $\ell_{\text{min}}$-prefix, and subsequent $\ell_{\text{min}}$-substrings overlapping in precisely $\ell_{\text{over}}$ coordinates. For example, if...
\[ x = 11101110101111 \]

\[ L_1^\ell(x) = \{ \{1110, 1011, 1110, 1010, 1011, 1111\} \}. \]

(Here, if \( \ell_{\min} - \ell_{\overline{\text{over}}} \) does not divide \( n - \ell_{\min} \), we allow the \( \ell_{\min}\)-suffix to contain a longer overlap with its preceding \( \ell_{\min}\)-substring.) We likewise let \( L_{\ell_{\text{in}}}^\ell(S) = \bigcup_{x \in S} L_{\ell_{\text{in}}}^\ell(x) \).

### III. Repeat-Free Strings

In this this section, we discuss the special case of \((\ell, \ell-1)\)-trace codes, which has been studied in literature in the context of reconstruction from substring compositions. To that end, we introduce the pertinent notion of repeat-free strings [11], which we denote herein for all \( \ell \leq n \) by

\[ RF_\ell(n) \triangleq \{ x \in \Sigma^n : |L_{\ell-1}(x)| = n - \ell + 1 \}, \]

That is, the set of all length-\( n \) strings whose \( \ell \)-substrings are all distinct. It was observed in [37] that if \( x \in RF_\ell(n) \), then \( L_{\ell+i}(x) \neq L_{\ell+i}(y) \) for all \( y \in \Sigma^n \) and \( y \neq x \). A straightforward generalization of the arguments therein demonstrates the following lemma.

**Lemma 1:** Given \( \ell_{\min} > \ell_{\overline{\text{over}}} \), for all \( x \in RF_{\ell_\overline{\text{over}}}(n) \), there exists an efficient algorithm reconstructing \( x \) from any \((\ell_{\min}, \ell_{\overline{\text{over}}})\)-trace of \( x \).

**Proof:** Let \( T \) be any \((\ell_{\min}, \ell_{\overline{\text{over}}})\)-trace of \( x \). For any \( u \in T \), suppose by negation that there exist \( v_1, v_2 \in T \), \( v_1 \neq v_2 \), such that the \( \ell_i\)-suffix of \( v_i \) equals the \( \ell_i\)-prefix of \( u \), where \( \ell_i \geq \ell_{\overline{\text{over}}} \). Since \( v_1 \neq v_2 \), they occur in distinct locations in \( x \), and in particular their \( \min\) \((\ell_1, \ell_2)\)-suffix occurs in distinct locations; this in contradiction to \( x \in RF_{\ell_{\overline{\text{over}}}}(n) \). The same argument proves that there do not exist \( v_1, v_2 \in T \), \( v_1 \neq v_2 \), such that the \( \ell_i\)-prefix of \( v_i \) equals the \( \ell_i\)-suffix of \( u \), where again \( \ell_i \geq \ell_{\overline{\text{over}}} \), for \( i \in \{1, 2\} \).

Hence, matching prefix to suffix, of lengths at least \( \ell_{\overline{\text{over}}} \), one reconstructs \( x \) from \( T \). Equivalently, for each \( u \in T \), finding the unique \( v \in T \) that contains the \( \ell_{\overline{\text{over}}}\)-prefix of \( u \) as a substring (which exists unless \( u \) is itself a prefix of \( x \)) results with complete reconstruction. A naive implementation requires \( O(n^2 \ell_{\overline{\text{over}}}) \) run-time.

We also denote multi-strand \( \ell \)-repeat-free strings

\[ RF_\ell(n, k) \triangleq \{ S \in X_n^k : |L_{\ell-1}^\ell(S)| = k(n - \ell + 1) \}, \]

and observe the following corollary of Lemma 1.

**Corollary 2:** For all \( S \in RF_{\ell_{\overline{\text{over}}}}(n, k) \) there exists an efficient algorithm reconstructing \( S \) from any \((\ell_{\min}, \ell_{\overline{\text{over}}})\)-trace of \( S \).

**Proof:** Observe that \( S \) is a set, \( S \subseteq RF_{\ell_{\overline{\text{over}}}}(n, k) \), and that \( \{ L_{\ell_{\overline{\text{over}}}}^{-1}(x) : x \in S \} \) are pairwise-disjoint, hence the reconstruction algorithm of Lemma 1 may operate on all elements of \( S \) in parallel without interference.

As a consequence of Corollary 2, \( RF_{\ell_{\overline{\text{over}}}}(n, k) \) forms a multi-strand \((\ell_{\min}, \ell_{\overline{\text{over}}})\)-trace code in \( X_n^k \) (likewise, \( RF_{\ell_{\overline{\text{over}}}}(n) \) in \( \Sigma^n \)).

Further, we note for \( k = 1 \) that if \( \lim \inf \ell_{\overline{\text{over}}}/\log(n) > 1 \), then [11] showed that \( RF_{\ell_{\overline{\text{over}}}}(n) \) forms a rate \( 1 - o_{\min}(1) \) code in \( \Sigma^n \) with an efficient encoder/decoder pair. Before summarizing their results, we will require the following notation: let

\[ RLL_s(n) \triangleq \{ u \in \Sigma^n : u \text{ has no length-s run of zeros} \}. \]

This is the well-understood run-length-limited constraint (see, e.g., [25, Sec. 1.2]).

Then, from [11] we have the following lemma.

**Lemma 3:** 1) [11, Sec. IV] There exists an efficient encoder/decoder pair into \( RF_2[\log(n)+2](n) \), requiring a single redundant symbol.

2) [11, Sec. V] There exists an efficient encoder/decoder pair into \( RF_s'(n) \cap RLL_s'(n) \), where

\[ s' \triangleq \log(n) + 10|\log \log(n)| + 10; \]

\[ s'' \triangleq 4|\log \log(n)| + 2. \]

The required redundancy is

\[ s'' + 1 + \text{red}(RLL_2[\log(n)](n - s'' - 1)). \]

Analysis of the asymptotic rate achieved by the encoder of Lemma 3, part 2 is given in the following lemma.

**Lemma 4:** There exist efficient encoders into \( RLL_s(n) \) requiring \( 2[2n/2^s] \) redundant symbols for \( q = 2 [21, \text{Sec. III}] \), or \( \lfloor \frac{q-2}{q}n/q \rfloor \) for \( q > 2 \).

**Proof:** The claim for \( q = 2 \) is proven in [21, Sec. III]. Hence, we need only extend it when \( q > 2 \), and to do so we rely on the concept of the encoder in [21, Alg. 1]. First, the information string \( x \in \Sigma^m \) is divided into blocks of length \( N \) (where the last block is permitted to be shorter), to be determined later. Then, in each block:

1) Append a 1 to the block.

2) From left to right, search for zero-runs of length \( s \); if one is encountered, remove it, and append the index of its incidence to the block using \( s \) symbols, such that the last symbol is restricted not to be either \( \{0, 1\} \).

3) Continue, until no further zero-runs of length \( s \) exist.

Note that this process concludes in finite time (since in each iteration of part 2 it advances by at least \( s \) locations of the original block, and appended symbols contain no zero-run of length \( s \)). Further, with the given restriction, \( s \) symbols may index a total of \( q^{s-1}(q-2) \) locations for the beginning of the zero-\( s \)-substring. It is therefore required to set \( N \triangleq q^{s-1}(q-2)+s-1 \).

Also observe that a possible decoder can use the last symbol to indicate whether a zero-run of length \( s \) was removed and indexed (which it can then inject in the correct place, discarding the index), or if the process is concluded (in which case the suffix ‘1’ should also be discarded).

Next, since every encoded block ends with a nonzero symbol, these blocks can be concatenated without violating the constraint. Observe, then, that a single redundant symbol is added per block, hence the claimed overall redundancy.

Finally, note that both encoder and decoder operate in polynomial time in the input length.

**Lemma 4** provides efficient encoders/decoders into \( RLL_s(n) \); to complete the picture, we observe that their redundancy has asymptotically optimal order of magnitude; indeed, by [21, Lem. 3] we have that \( \text{red}(RLL_s(n)) \geq \log(c)(1 - 1/q)^2n - 2\log(c)n \).

Next, although the encoder of part 2 of Lemma 3 asymptotically achieves rate 1, it is of interest to encode into \( RF_\ell(n) \) using less redundancy, for any \( \ell < 2\log(n) \). We will show...
that the approach of [11, Sec. V] can be generalized to this end.

**Theorem 5:** For integers $\ell(n), t$ satisfying

$$\left\lfloor \log \log(n) \right\rfloor + 4 \leq t \leq \left\lfloor (\ell(n) - \log(n)) / 3 \right\rfloor$$

(for $q = 2$, require $\left\lfloor \log \log(n) \right\rfloor + 5 \leq t \leq \left\lfloor (\ell(n) - \log(n)) / 3 \right\rfloor$) there exists an efficient encoder/decoder pair into $RF_{\ell(n)} \cap RLL_t(n)$, requiring at most $t + 1 + \left\lceil q^s n/q^t \right\rceil$ redundant symbols (for $q = 2$, this is $t + 1 + 2 \lceil 16n/2^t \rceil$, i.e., rate $1 - O(n (\frac{1}{n} + q^{-t})$.

**Proof:** The proof follows the steps of [11, Sec. V], with some amendments; where their arguments hold without change, we shall clearly cite the relevant proposition while reproducing its proof (when possible, we prioritize intuition over formality in our proof, without sacrificing rigour). The rest of the proof is organized in stages, to improve readability.

1) In the first stage, an information string $x \in \Sigma^m$ is encoded into $y \in RLL_{t-3}(n - t - 1)$, where $m$ is determined by, e.g., Lemma 4.

2) Next, we wish to eliminate from $y$ repeated substrings of length $s \triangleq \left\lfloor \log(n) \right\rfloor + t + 2$. The elimination stage requires an indexing function $h: [n] \rightarrow RLL_{t-3}(n)$ (i.e., an integer $N$ satisfying $\left| RLL_{t-3}(n) \right| \geq n$). By Lemma 4 an explicit function exists if $\left\lceil \frac{q^{s+1}}{2} N / q^{t-3} \right\rceil \leq N - \log(n)$ (for $q = 2$ that is $2 \left\lceil 2N / 2^{t-3} \right\rceil \leq N - \log(n)$), or equivalently $(1 - q^{-t}) N \geq \left\lfloor \log(n) \right\rfloor$. With the assumed lower bound on $t$, this requirement is satisfied by $N \triangleq \left\lceil \log(n) \right\rceil + 1$, for sufficiently large $n$.

3) In the elimination stage (based on [11, Alg. 3]), $y$ is processed from left to right; whenever $j > i$ are found such that $y_{j+i} = y_{j+i}$ (and again, $j$ is minimal satisfying this requirement), the segment $y_{j+i}$ is deleted and replaced with

$$1 0^{t-3} 1 \circ h(i) \circ 1,$$

where we consider $10^{t-3} 1$ to be a marker, indicating the replaced segment (based on the first step, this marker does not appear elsewhere in $y$). Based on the fact that any elimination reduces the string length by 1, this stage is concluded in $O(n^2)$ steps. We denote the resulting string by $w$, of length $n'$ (for some $n' \leq n - t - 1$, depending on how many eliminations were performed).

Trivially, the only instances of $0^{t-3}$ in $w$ are the markers used in replaced substrings (and $w \in RLL_{t-2}(n')$). By following the same approach as in [11, Lem. 19] (which in turn was based on [13, Cla. 10]) one observes that $w \in RF_{n'}(n')$ and that the process can be reversed; the former is trivial since the process only terminates when no repeated sequences remain. The latter is done by decoding from right to left, where replaced substrings are identified by the presence of markers, and the eliminated substrings are restored based on $h(i)$. To prove this is possible, one needs only show that after any iteration of the process, the right-most instance of a marker is the one injected in that iteration. Indeed, since the process scans for $j$ from left to right, if $j$ is the location identified (i.e., $y_{j+i}$ was replaced) in the last iteration, and $j'$ in the iteration before that, then by necessity $j \geq j' - s + 1$; clearly, then, if $j < j'$ then the marker injected at location $j'$ was overwritten in the last iteration. I.e., the marker injected at any iteration either overwrites the last injected marker, or appears in the replaced string to its right.

4) The process is concluded in an expansion stage, meant to output strings of length $n$ from which $w$ (hence also $x$) can be decoded. For that purpose, an arbitrary string $v \in RF_{n}(n') \cap RLL_{t-3}(n)$ is generated in a fashion to be described below, and interleaved with $0^{t-2}$ markers-segments after every $s$ positions; i.e., if $v = v_0 \circ v_1 \circ \cdots \circ v_{[n/s]-1}$, where $|v_i| = s$ for all $i \in ([n/s])$ and $[v_{[n/s]}-1] \leq s$, then

$$w' \triangleq v_0 \circ 0^{t-2} 1 \circ v_1 \circ 0^{t-2} 1 \circ \cdots \circ v_{[n/s]-1}.$$

Clearly, $w' \in RF_{s+t}(n'') \cap RLL_{t-3}(n'')$, where $n'' \triangleq |w'| \geq n$. It is straightforward that the only instances of $0^{t-2}$ in $w'$ are the markers interleaved into it. Based on these observations, it is proven similarly to [11, Lem. 23] that

$$\hat{w} \triangleq w \circ 0^{t-1} 1 \circ w'$$

is $(s + 2t - 2) = (\left\lceil \log(n) \right\rceil + 3t)$-repeat-free and $t$-run-length-limited; this is done by observing that any substring of this length of $\hat{w}$ contains markers (potentially unless it is a substring of $w$, in which case the absence of markers indicates that fact), their length $(l - i)$ for $i \in (1, 2, 3, \ldots)$ indicates which portion of $\hat{w}$ it is taken from, and if it does not cover the unique instance of $0^{t-1}$ in $\hat{w}$ then it contains $s$ consecutive symbols of either $w$ or $v$, hence is unique.

Observe that by the upper bound on $t$, $\hat{w}$ is $\ell(n)$-repeat-free. Also, the $n$-prefix of $\hat{w}$ contains $w \in 0^{t-1} 1$, hence $\hat{w}$ can uniquely be extracted from it. That prefix is therefore output as the encoded information.

5) Finally, it remains to describe how any arbitrary $v \in RF_{n}(n') \cap RLL_{t-2}(n')$ might be generated (a single example suffices). To achieve this, any total order on $\Sigma$ is chosen where 0 is the minimum, and 1 the maximum. For a string $u \in \Sigma^s$, let its necklace be the lexicographic least cyclic rotation of $u$, and its periodic-reduction be the minimum period of $u$. It was shown in [12] that concatenating in lexicographic order periodic-reductions of necklaces of length $s$ produces a de Bruijn sequence $b \in \Sigma^s$ (in fact, this is the lexicographically least de Bruijn sequence of that length).

The last instance of 0$^t$ in $b$ is in the necklace $0^t 1^{s-t}$ (since only the “0” necklace ends with 0, and the longest zero-run in any necklace appears at its beginning). Hence, letting $i \in [q^t]$ be the unique location such that $b_{i+[n]} = 0^t 1^{s-t}$, we let $v \triangleq b_{q^s-n+[n]}$ and to conclude we need only show that $q^s - n > i$.

This was done in [11, Lem. 20] in case that $s$ is prime, and we generalize for all $s$; we do so by counting $\{b_{j+[n]} : i < j \leq q^s - s \} = q^s - s - i$. By the proof of [12, Th. 4] every $u \in \Sigma^s$ appears in $b$ in a location...
intersecting the appearance of the periodic-reduction of its necklace, potentially unless \( u_{q+1} = 1 \).

Observe that it is sufficient that \( u \in \mathcal{RLC}_{s}(s) \) satisfies \( u_{s-1} \neq 0 \) for its necklace to be greater than \( 0^{s-1}; \) therefore for all \( u \in \mathcal{RLC}_{s}(s-2) \) and \( u', u'' \in \Sigma \) satisfying \( u' \neq 1, u'' \neq 0 \) there exists \( j > i \) such that \( b_{j+i} = u' \odot u \odot u'' \). It follows that

\[
q^a - s - i = |\{b_{j+i} : i < j \leq q^a - s\}| \\
\geq (q-1)^2|\mathcal{RLC}_{s}(s-2)| \\
\geq (q-1)^2q^{s-2}(1-2q^{-1}) \\
\geq (q-1)^2n(1+t/\log(n))(1-2q^{-t}),
\]

where \((*)\) is justified by [21, Lemma, 3] for sufficiently large \( t \). Since \( t > \lceil \log(\log(n)) \rceil \), for sufficiently large \( n \) we have \((1+t/\log(n))(1-2q^{-t}) > 1\), as required.

Finally, redundancy of this construction is \( t+1 \), plus the redundancy of encoding into \( \mathcal{RLC}_{t-3}(n-t-1) \); Lemma 4 now concludes the proof.

In summary, we have the following corollary:

**Corollary 6:** By Lemma 1, \( \mathcal{RF}_{\ell_{\text{over}}}(n) \) forms an \((\ell_{\text{min}}, \ell_{\text{over}})\)-trace code in \( \Sigma^n \), which by Theorem 5 has \( 1-o_n(1) \) rate whenever \( \ell_{\text{over}} \geq \lceil \log(n) \rceil + 3|\log(\log(n))| + 12 \).

In the sequel, we focus on the complexity, unsolved case of \( \lim \sup \ell_{\text{over}}/\log(n) \leq 1 \).

**IV. Bounds**

In this section we demonstrate an upper bound on the achievable asymptotic rate of \((\ell_{\text{min}}, \ell_{\text{over}})\)-trace codes.

**Lemma 7:** Any multi-strand \((\ell_{\text{min}}, \ell_{\text{over}})\)-trace code \( C \subset \mathcal{X}_{n,k} \) satisfies

\[
|C| \leq \left( k^{\left( \frac{n-\ell_{\text{over}}}{\ell_{\text{min}}-\ell_{\text{over}}} \right)} + q^{\ell_{\text{min}}} \right).
\]

**Proof:** Since \( \mathcal{L}_{\ell_{\text{min}}}^\ell_{\text{over}}(x) \subset \mathcal{F}_{\ell_{\text{min}}}^\ell_{\text{over}}(x) \) for all \( x \in \Sigma^n \), we have

\[
|C| \leq \left| \left\{ \mathcal{L}_{\ell_{\text{min}}}^{\ell_{\text{over}}}(S) : S \subset \mathcal{X}_{n,k} \right\} \right|.
\]

Similarly to the argument used in [5], we count the incidences of each possible \( u \in \Sigma_{\ell_{\text{min}}}^{\ell_{\text{over}}}(S) \), resulting in \( f_{S}: \Sigma_{\ell_{\text{min}}}^{\ell_{\text{over}}} \rightarrow \mathbb{N} \) (dubbed a profile-vector in [5]). Observe that \( \sum_{u \in \Sigma_{\ell_{\text{min}}}^{\ell_{\text{over}}}} f_{S}(u) = k \left( 1 + \frac{n-\ell_{\text{over}}}{\ell_{\text{min}}-\ell_{\text{over}}} \right) = k \ell_{\text{min}}^{\ell_{\text{min}}-\ell_{\text{over}}} \); thus, we have an embedding of \( \left\{ \mathcal{L}_{\ell_{\text{min}}}^{\ell_{\text{over}}}(S) : S \subset \mathcal{X}_{n,k} \right\} \) into

\[
\left\{ f \in \mathbb{N}_{\ell_{\text{min}}}: \sum_{i \in [q^{\ell_{\text{min}}}]^{t}} f_{i} = k \left( \frac{n-\ell_{\text{over}}}{\ell_{\text{min}}-\ell_{\text{over}}} \right) \right\},
\]

and therefore

\[
|C| \leq \left( k^{\left( \frac{n-\ell_{\text{over}}}{\ell_{\text{min}}-\ell_{\text{over}}} \right)} + q^{\ell_{\text{min}}-1} \right),
\]

which concludes the proof.

**Lemma 8:** For \( k = 1 \), if \( \ell_{\text{min}} = a \log(n) + O_{n}(1) \) and \( \ell_{\text{over}} = \gamma \ell_{\text{min}} + O_{n}(1) \), for some \( a > 1 \) and \( 0 \leq \gamma \leq \frac{1}{a} \), then any \((\ell_{\text{min}}, \ell_{\text{over}})\)-trace code \( C \subset \Sigma^n \) satisfies

\[
R(C) \leq \frac{1-1/a}{1-\gamma} + O\left( \frac{\log \log(n)}{\log(n)} \right).
\]

(Note that \( \gamma \) is a linear scaling of the required overlap between consecutive segments, in proportion to their required minimum length. We scale that minimum length linearly with \( \log(n) \) (where the constant \( a \) indicates the ratio), a decision informed by the statement of this lemma, and the succeeding corollary. Finally, observe that in this notation, \( \frac{1-1/a}{1-\gamma} \leq 1 \) if and only if \( \lim \ell_{\text{over}}/\log(n) = \gamma a \leq 1 \).)

**Proof:** From the known bound \( u > (u/e)^u \) we observe for all \( v > u > 0 \) that

\[
\log \left( \frac{u + v}{u} \right) \leq \frac{u + v}{u} - \log \left( \frac{u + v}{u} \right) = u \frac{2 \log \left( \frac{u + v}{u} \right)}{u} + 1 - \frac{u}{u}.
\]

We divide the last inequality into \( u \nabla 1 \leq 2 < e \).

Letting \( v \triangleq q^{\ell_{\text{min}}-1} \) and \( u \triangleq \left\lceil \frac{n-\ell_{\text{over}}}{\ell_{\text{min}}-\ell_{\text{over}}} \right\rceil < v \), we observe that \( \log \left( \frac{u}{v} \right) = O(\log(n)) \) and \( \log(u) \geq \log(n - \ell_{\text{over}} - \log(n) - O(1)) \); observing

\[
\log(n - \ell_{\text{over}}) = \log(n) - \log(1 - \ell_{\text{over}}) - \log(n - \ell_{\text{over}} - \log(n) - O(1))
\]

Next, by Lemma 7 \(|C| \leq \left( u^{\gamma} \right) \), hence we have

\[
\log |C| \leq \left( \frac{n - \ell_{\text{over}}}{\ell_{\text{min}} - \ell_{\text{over}}} \right) + \log \left( \frac{u}{v} \right) + 2 \log(e) + O(\log \left( \frac{u}{v} \right))
\]

\[
= n \left( \frac{\log \left( \frac{u}{v} \right)}{\ell_{\text{min}} - \ell_{\text{over}}} + 2 \log(e) \right) + O(\log \left( \frac{u}{v} \right))
\]

\[
= n \left( \frac{\log(v) - \log(u)}{n - \ell_{\text{over}}} + O \left( \frac{n}{\log(n)} \right) \right) + O(\log(n))
\]

\[
= n \left( \frac{\log(v) - \log(u)}{n - \ell_{\text{over}}} + O \left( \frac{1}{\log(n)} \right) \right)
\]

\[
\leq n \left( \frac{\ell_{\text{min}} - \ell_{\text{over}}}{\ell_{\text{min}} - \ell_{\text{over}}} + O \left( \log \left( \frac{n}{\log(n)} \right) \right) \right)
\]

\[
= n \left( \frac{1}{1 - \gamma} + O \left( \frac{\log \log(n)}{\log(n)} \right) \right).
\]

In particular, Lemma 8 implies the following lower bound on \( \ell_{\text{min}} \) for the existence of codes with asymptotically non-vanishing rates.

**Corollary 9:** Take \( (\ell_{\text{min}})^n, (\ell_{\text{over}})^n \) and let \( C^n \) be \((\ell_{\text{min}}^{(n)}, \ell_{\text{over}}^{(n)})\)-trace codes. If \( \lim \sup \ell_{\text{min}}/\log(n) \leq 1 \), then \( R(C^n) = o_n(1) \).

**Proof:** Since \( C^n \) are also \((\ell_{\text{min}}^{(n)}, 0)\)-trace codes for \( \ell_{\text{min}}^{(n)} \geq \ell_{\text{min}}^{(n)} \), it follows from Lemma 8 that \( R(C^n) \leq \frac{1-1/a}{1-\gamma} + o(1) \) for all \( a > 1 \), hence the claim follows.
V. A CONSTRUCTION OF TRACE CODES

In this section we present an efficient encoder for \((\ell_{\min}, \ell_{\overline{\text{over}}})\)-trace codes (i.e., in the case \(k = 1\)), achieving asymptotically optimal rate, for the case \(\limsup \ell_{\overline{\text{over}}} / \log(n) \leq 1\) (completing the results of Section II). Throughout the section, we let

\[
\ell_{\min} \triangleq \lceil a \log(n) \rceil; \\
\ell_{\overline{\text{over}}} \triangleq \lceil \gamma \ell_{\min} \rceil, 
\]

for some \(a > 1\) and \(0 < \gamma \leq 1/a\). Further, we let \(f\) be any integer function satisfying \(f(n) = o(\log(n))\) and \(f(n) \geq \log(\log(n)) + 4\), and finally

\[
I \triangleq \left\lceil \frac{1 - \gamma a}{1 - \gamma} \log(n) + (\log(n))^{0.5 + \epsilon} \right\rceil, 
\]

for some small \(\epsilon > 0\). In our construction, \(I\) is the number of symbols dedicated to (unencoded)-indices, which are then partitioned into length-\(f(n)\) fragments, as described below. When analyzing the redundancy of our construction, we shall optimize it by a proper choice of \(f(n)\), in Theorem 15.

The main idea of the construction presented below of an \((\ell_{\min}, \ell_{\overline{\text{over}}})\)-trace code \(C_A(n)\) is to encode an information string \(x\) into \((z_i)_{i \in [q^I]}\) so that the following two properties are satisfied: (i) the index \(i\) can be decoded from any \(\ell_{\min}\)-substring of \(z_i\); and (ii) the string \(z_i\) can be uniquely reconstructed from an \((\ell_{\min}, \ell_{\overline{\text{over}}})\)-trace of \(z_i\). This is performed by interleaving segments of indices in appropriate locations in the encoded strings. Then, we let

\[
\text{Enc}_{A}(x) \triangleq z = z_0 \circ \cdots \circ z_{q^I - 1} \in C_A(n).
\]

Before presenting the construction, we describe the method of index-generation.

**Definition 10:** Let \((c_i)_{i \in [q^I]}, c_i \in \Sigma^f\) be indices in ascending lexicographic order. We encode each \(c_i\) independently as follows (see Figure 4). Denoting \(F \triangleq \lceil I/f(n) \rceil\), we partition \(c_i\) into \(F\) non-overlapping segments of equal lengths \(\{c_i^{(h)}\}_{h \in [F]}\); here and in the sequel, we say a string is partitioned into non-overlapping segments of equal lengths if \(c_i^{(0)} \circ c_i^{(1)} \circ \cdots \circ c_i^{(F - 1)} = c_i\), and

\[
|c_i^{(h)}| = \begin{cases} \lceil I/F \rceil, & h < I \mod F; \\ \lfloor I/F \rfloor, & \text{otherwise}. \end{cases}
\]

Observe that \(|c_i^{(h)}| \leq f(n)\) for all \(h \in [F]\). We then denote \(c_i^{(h)} \equiv h \circ c_i^{(h)} \circ 1\). We refer to \(c_i\) (or simply \(i\)) as an index in the construction, and to \(\{c_i^{(h)}\}_{h \in [F]}\) as segments of an encoded index.

Further, for \(N \leq n\) to be defined later, and \(I > \lceil \log(N) \rceil + 3\, f(n)\), we denote the encoder of Theorem 5

\[
E_{N,F}^{RF} : \Sigma^m(N) \to \mathcal{RF}_I(E) \cap \mathcal{RF}_F(n), \quad n < 1 + f(n)
\]

for any \(n \leq n\), we denote the encoder of Theorem 5

\[
E_{N,F}^{RF} : \Sigma^m(N) \to \mathcal{RF}_I(E) \cap \mathcal{RF}_F(n), \quad n < 1 + f(n)
\]

Here,

\[
m(N) \triangleq N - \text{red}(E_{N,F}^{RF}) \\
\geq N \left(1 - \frac{f(n) + 2}{N} - \frac{q^3}{2} - f(n)\right).
\]

(For \(q = 2, m(N) \geq N \left(1 - \frac{f(n) + 4}{N} - 2^{i+1}\right)\).

**Construction A:** The encoding into \(z_i\), for all \(i \in [q^I]\), is performed as follows (see Figure 5). We denote

\[
r \triangleq I + 2F + f(n) + 4 \\
= I + \frac{2f(n)}{f(n)} + f(n) + O(1),
\]

then define

\[
\ell \triangleq \left\lceil \frac{\ell_{\overline{\text{over}}} - f(n) - 6}{1 + (f(n) + 2)/\lceil \ell_{\min} \rceil} \right\rceil,
\]

(see Lemmas 11 and 12, respectively, for the reason for these definitions). Also, for all \(i \in [q^I]\)

\[
N_i \triangleq \left\{ \left[q^{-I} / \ell \right] - \left[n / (q^I \ell_{\min})\right] r, \quad i < n \mod q^I \middle| \\
\left[q^{-I} n \right] - \left[n / (q^I \ell_{\min})\right] r, \quad \text{otherwise}. \right.
\]

Now, for all \(i \in [q^I]\) define \(y_i \triangleq E_{N,F}^{RF}(x_i) \in \Sigma^N_i\), where \(x_i \in \Sigma^m(N_i)\) and

\[
x = x_0 \circ x_1 \circ \cdots \circ x_{q^I - 1}
\]

is an arbitrary information string (see the proof of Theorem 5 for a choice of \(f(n)\) satisfying the conditions of Theorem 5, hence assuring the existence of \(E_{N,F}^{RF}\)).

Next, for all \(i \in [q^I]\)

1) Partition \(y_i\) into \(\left[n / (q^I \ell_{\min})\right]\) non-overlapping segments of equal length

\[
y_i = y_i^{(0)} \circ y_i^{(1)} \circ \cdots \circ y_i^{\left[n / (q^I \ell_{\min})\right] - 1}.
\]

2) For all \(j \in \left[\left[n / (q^I \ell_{\min})\right]\right]\):

a) Partition each \(y_{i,j}\) into \(F\) non-overlapping segments of equal lengths

\[
y_{i,j} = y_{i,j}^{(0)} \circ y_{i,j}^{(1)} \circ \cdots \circ y_{i,j}^{\left[F - 1\right]}.
\]

b) Combine \(\{y_{i,j}^{(h)} : h \in [F]\}\) with segments of the encoded index \(i\), as follows. Define for all \(h \in [F]\)

\[
z_{i,j}^{(h)} \triangleq y_{i,j}^{(h)} \circ c_i^{(h)}
\]

then

\[
z_{i,j} \triangleq \begin{cases} 1 \circ \left( f(n) + 1 \right) \circ \cdots \circ \left( f(n) + 1 \right), & j = 0; \\
1 \circ \left( f(n) + 1 \right) \circ \cdots \circ \left( f(n) + 1 \right), & j > 0
\end{cases}
\]
(we refer to the substrings $10^{f(n)+1}11, 10^{f(n)+1}01$ as synchronization markers).

3) Concatenate

$$z_i = z_{i,0} \circ \cdots \circ z_{i,\lceil n/(q' \ell_{\min}) \rceil - 1}$$

First, we prove the correctness of Construction A. We begin with two technical lemmas which are key to the proof of correctness in Theorem 13.

**Lemma 11:** Every $\ell_{\min}$-substring $u$ of $z \in C_A(n)$ contains as subsequences at least an $(I - \mu)$-suffix of an index $c_i$ (see Definition 10), and an $\mu$-prefix of either $c_i$ or $c_{i+1}$, for some $i \in \lbrack q' \rbrack$ and $\mu \in \lbrack I \rbrack$, in identifiable locations.

**Proof:** Note that

$$\ell_{\min} - q'\ell_{\min}/n \leq \frac{\ell_{\min} - 1}{1 + q'/\ell_{\min}} = \frac{n/q'}{n/q'} + 1 \leq \frac{n/q'}{n/q'} + 1 \leq \ell_{\min}$$

Observe from Eq. (2) that $q'\ell_{\min} = o(n)$, and by subtracting $r$ from the above inequality, it holds from Eq. (6) for sufficiently large $n$ and all $i \in \lbrack q' \rbrack$ that $\ell_{\min} - r - 1 \leq \ell_{\min}$. Hence also for all $j \in \lbrack n/(q'\ell_{\min}) \rbrack$ it holds that

$$\ell_{\min} - r - 1 \leq \lvert y_{i,j} \rvert \leq \ell_{\min} - r.$$  

(7)

By part 2 of Construction A it follows that $\lvert z_{i,j} \rvert = \lvert y_{i,j} \rvert + r \in \{\ell_{\min}, \ell_{\min} - 1\}$.

Next, observe that instances of synchronization markers only appear in $z$ at the beginning of $\{z_{i,j} \}_{i,j}$. From the last paragraph, either $u$ contains a complete synchronization marker as substring, or it contains a suffix-prefix pair whose concatenation is an instance of a synchronization marker; in both cases, the exact locations in which symbols of the indices $\{c_{i(h)}\}$ appear can be determined. Extracting $\{c_{i(h)}\}$, these contain a suffix of $c_i$ and a prefix of either $c_i$ or $c_{i+1}$ (depending on whether $u$ is a substring of $z_i$, for some $i$) whose combined lengths is $I$, again since for all $i, j, \lvert z_{i,j} \rvert \leq \ell_{\min}$ and $z_{i,j}$ contains all symbols of $c_i$. Taking $\mu \in \lbrack I \rbrack$ to be the length of the prefix ($\mu = 0$ indicates the possibility that all symbols of the same index appear in $u$) concludes the proof.

**Lemma 12:** Every $\ell_{\overline{r}}$-substring $v$ of $z \in C_A(n)$ contains at least $\ell$ consecutive symbols of $y = y_0 \cdot \cdots \cdot y_{h-1}$ (see Eq. (5)).

**Proof:** At worst, $v$ either begins or ends with a complete instance of a synchronization marker; hence the remaining $\ell_{\overline{r}} - f(n) - 4$ symbols are sampled from $\{y_{i,j}\}$, and again, at worst end with a complete segment of an encoded index. Since from Definition 10 $|c_{i(h)}| \leq f(n) + 2$ and by Eq. (7) $|y_{i,j}| \geq \lceil \frac{\ell_{\min} - r}{f(n)} \rceil$ for all $i, j, v$ contains at least

$$\ell_{\overline{r}} - 2f(n) - 6 \leq \frac{1 + (f(n) + 2)/\ell_{\min}}{f(n)} = \ell$$

consecutive symbols of $y$.

Combining both lemmas, we have the following theorem.

**Theorem 13:** For all admissible values of $n$, the code $C_A(n)$ is an $(\ell_{\min}, \ell_{\overline{r}})$-trace code.

**Proof:** Take $z \in C_A(n)$ and let $T = T_{\ell_{\overline{r}}}(z)$, i.e., any $(\ell_{\min}, \ell_{\overline{r}})$-trace of $z$.

For $u \in T$, we extract the $(I - \mu)$-suffix of $c_i$, and an $\mu$-prefix of either $c_i$ or $c_{i+1}$, for some $i \in \lbrack q' \rbrack$ and $\mu \in \lbrack I \rbrack$, guaranteed by Lemma 11. Observe that if this prefix belongs to $c_{i+1}$, then $u$ also contains a complete synchronization marker $10^{f(n)+1}$ (the instance appearing as prefix of $z_{i+1}$), hence these two cases may be distinguished. Further, note that the $\mu$-prefix of $c_{i+1}$ equals the $\mu$-prefix of $c_i$, unless every symbol of the $(I - \mu)$-suffix of $c_i$ is $(q - 1)$, in which case it is the $q$-arity expansion of the successor natural number to that prefix. In both cases, one can correctly deduce that the location of $u$ in $z$ begins in the segment $z_i$. It is therefore possible to partition $T$ into $n$ by index $i$ (corresponding to the starting location of each sub-string).

For each substring $u$ of index $i$, intersecting both $y_i, y_{i+1}$, $u$ must contain a complete synchronization marker $10^{f(n)+1}$ (the instance appearing as prefix of $z_{i+1}$); hence its location in $u$ implies the exact location of $u$ in $z$. For all other substrings of index $i$, it holds by Lemma 12, and since each $y_i$ is $\ell$-repeat-free, that there exist a unique way to concatenate these substrings (excluding overlap) as shown in Lemma 1.

Finally, once $z$ is reconstructed we may extract $\{y_{i,j}\}_{i \in \lbrack q' \rbrack}$, then decode $\{x_{i,j}\}_{i \in \lbrack q' \rbrack}$ with the decoder of $E^\ell_{\overline{r}}$.

Next, we analyze $\overline{R}(C_A(n))$. First, we require a simplified (asymptotic) expression for $\ell$, used in Construction A for repeat-free encoding, which we derive in the next lemma.

**Lemma 14:** Denoting $\lambda = l - 1$, we have

$$\ell = \lambda \ell_{\overline{r}} + O\left(\frac{\log(n)}{f(n)}\right).$$

**Proof:** Recall the definition $\ell = \left\lfloor \frac{\ell_{\overline{r}} - 2f(n) - 6}{1 + (f(n) + 2)/\ell_{\min}} \right\rfloor$ in Eq. (5), where $F = \lceil I/f(n) \rceil$ and $r$ is defined in Eq. (4). We begin by observing

$$\ell_{\overline{r}} - 2f(n) - 6 \leq \frac{1 + (f(n) + 2)/\ell_{\min}}{f(n)} = \frac{I + O(f(n))}{\ell_{\min} - I + O(f(n) + \frac{\log(n)}{f(n)})}$$

Authorized licensed use limited to: Eitan Yaakobi. Downloaded on December 04,2023 at 04:02:14 UTC from IEEE Xplore. Restrictions apply.
where the second to last equality is justified by \( \frac{1}{1-x} = 1 + x + \frac{x^2}{2} \) for \( x \neq 1 \), and since from Equations (1) and (2)

\[
\ell_{\text{min}} - I = \frac{I}{\ell_{\text{min}}} + O\left(\frac{f(n)}{\log(n)}\right)
\]

\[
= \frac{I}{\ell_{\text{min}}} + O\left(\frac{f(n)}{\log(n)}\right)
\]

\[
= \frac{I}{\ell_{\text{min}}} + O\left(\frac{f(n)}{\log(n)}\right)
\]

\[
= \frac{I}{\ell_{\text{min}}} + O\left(\frac{f(n)}{\log(n)}\right)
\]

\[
= \frac{I}{\ell_{\text{min}}} + O\left(\frac{f(n)}{\log(n)}\right)
\]

hence

\[
\log(N_i) \geq (a-1)\gamma \log(n) - \frac{(a-1)\gamma}{1-\gamma} O(1)
\]

In particular for sufficiently large \( n \) we have

\[
f(n) \geq \lceil \log(N_i) \rceil + 3 f(n) \quad \text{(8)}
\]

Next, by Lemma 14,

\[
\ell = \left(\frac{1}{\ell_{\text{min}}} + \ell_{\text{over}}\right) - O\left(\frac{f(n)}{\log(n)}\right)
\]

\[
= \frac{1}{\ell_{\text{min}}} - \frac{O(f(n))}{\log(n)}
\]

\[
= \frac{1}{\ell_{\text{min}}} - \frac{O(f(n))}{\log(n)}
\]

\[
= \frac{1}{\ell_{\text{min}}} - \frac{O(f(n))}{\log(n)}
\]

Hence

\[
\ell - \lceil \log(N_n, \ell(m)) \rceil = (1 - \gamma)(\log(n))^{0.5 + \epsilon} - O\left(\sqrt{\log(n)}\right)
\]

\[
> 3 f(n)
\]

for sufficiently large \( n \). Together, Equations (8) and (9) satisfy the conditions of Theorem 5, allowing us to efficiently encode \( y_i = E_{N_i, \ell(x_i)} \in R_{\ell}(N_i) \) (and vice versa, decode \( x_i \)) while attaining from Eq. (3) \( m(N_i) \geq 1 - \frac{f(n) + f(n)}{\log(n)} - \frac{a^2}{q^2} q^{-f(n)} = 1 - O(q^{-f(n)}) \), where the coefficient of the asymptotic notation does not depend on \( i \). Hence,

\[
\sum_{i \in [q]} m(N_i) \geq \left(1 - O(q^{-f(n)})\right) \sum_{i \in [q]} N_i
\]

\[
\geq \left(1 - O(q^{-f(n)})\right) \left(1 - \frac{r}{\ell_{\text{min}}} - \frac{q^r \rho}{\ell_{\text{min}}}\right)
\]

where the equality on the second line follows from Eq. (6), which concludes the proof.}

\[\text{VI. MULTI-STRAND RECONSTRUCTION FROM SUBSTRING-COMPOSITIONS}\]

In this section, we study an extension of the reconstruction from substring-compositions problem, i.e., \( (\ell, \ell - 1) \)-trace codes, to multisets of strings, i.e., to codes over \( \mathcal{X}_{nk} \) for \( k > 1 \). For a string \( x \in \Sigma^n \) we denote for brevity an \( (\ell, \ell - 1) \)-trace of \( x \), \( \mathcal{T}_i \) by \( \mathcal{T}_i(x) \) and \( \mathcal{L}_i^{\ell - 1}(x) \) by an \( \ell \)-trace, \( \mathcal{T}_i(x) \) and \( \mathcal{L}_i(x) \), respectively. We say \( \mathcal{L}_i(x) \) in particular is the \( \ell \)-profile of \( x \), the multiset of all of its \( \ell \)-substrings.

We shall assume throughout in asymptotic analysis that as \( n \) grows, \( \limsup \frac{\log(k)}{n} < 1 \), which is most relevant in applications (see, e.g., [10] for an overview of typical string-lengths in applications); the complement case is of independent theoretical interest, and is left for future work. Hence, we have the following lemma.
Lemma 16: \( \log |\mathcal{X}_{n,k}| = k(n - \log(k/e)) + o(k) = \Theta(nk) \).

Proof: From Stirling’s approximation we have \( (k/e)^k \leq k! \leq e^{\sqrt{k(k/e)}} \), implying
\[
\frac{1}{e^{\sqrt{k/k/e}}} \leq \frac{q^n}{k!} \leq |\mathcal{X}_{n,k}| < \left( \frac{q^n + k}{k!} \right)^k \leq \left( \frac{q^n(1 + k/q^n)}{k/e} \right)^k.
\]

For a multi-string \( \ell \)-trace code \( \mathcal{C} \) we have from Lemma 7 that \( |\mathcal{C}| \leq (nk+q^k)^n \). A corollary of Lemma 8 is therefore stated:

Corollary 17: Assume \( \limsup \frac{\log(n)}{n} < 1 \). If \( \log(nk) - \ell = \omega_{nk}(1) \) then for any multi-string \( \ell \)-trace code \( \mathcal{C} \subseteq \mathcal{X}_{n,k} \) it holds that
\[
R(\mathcal{C}) = o_{nk}(1).
\]

Proof: By the observation in the proof of Lemma 8
\[
R(\mathcal{C}) \leq \frac{1}{|\mathcal{X}_{n,k}|} \log \left( \frac{nk + q^k}{q^\ell} \right) = O \left( \frac{q^n}{nk} (2 \log(e) + \log(nk) - \ell) \right),
\]
where the equality follows from Lemma 16.

On the other hand, recall from Corollary 2 that \( \mathcal{R} \mathcal{F}_\ell(n, k) \subseteq \mathcal{X}_{n,k} \) is a multi-string \((\ell + 1)\)-trace code. Next, we show in contrast to Corollary 17 that if \( \ell - \log(nk) = \omega_{nk}(1) \), then \( R(\mathcal{R} \mathcal{F}_\ell(n, k)) = 1 - o_{nk}(1) \). We shall do so by presenting two explicit constructions of multi-string \( \ell \)-repeat-free codes with efficient encoders and decoders. For convenience, we assume all integers to have integer values; a straightforward adjustment of the described methods applies for all values.

A. Index-Based Construction

Construction B: Denote \( n' \triangleq (n - \log(k))k \), and take \( m \) such that \( E : \Sigma^m \rightarrow \mathcal{R} \mathcal{F}_\ell(n') \) is any repeat-free encoder, for a given \( \ell' \). Let \( x \in \Sigma^m \) be an arbitrary information string, and encode it into \( y \triangleq E(x) \). Take \( y_0, \ldots, y_{k-1} \in \Sigma^{n \log(k)} \) such that \( y = y_0 \circ y_1 \circ \cdots \circ y_{k-1} \). Let \( c_i \in \Sigma^{\log(k)} \) be a \( q \)-ary expansion of \( i \in [k] \). Denote \( \hat{y}_i \triangleq c_i \circ y_i \); then,
\[
\text{Enc}_B(x) = \{(\hat{y}_i : i \in [k]) \in \mathcal{X}_{n,k} \}.
\]

We denote \( \mathcal{C}_B(n, k) \triangleq \text{Enc}_B(\Sigma^m) \). The decoding success of Construction B follows from the next lemma.

Lemma 18: \( \mathcal{C}_B(n, k) \subseteq \mathcal{R} \mathcal{F}_\ell(n, k) \), where \( \ell = \ell' + \log(k) \).

Proof: For \( x \in \Sigma^m \), note that \( y \triangleq \text{Enc}_B(x) = y_0 \circ y_1 \circ \cdots \circ y_{k-1} \in \mathcal{R} \mathcal{F}_\ell(n') \) and thus \( \|E' (y)\| = n' - \ell' + 1 \). It follows that \( \|E(v) (\{y_i : i \in [k]\})\| = (n' - \ell' + 1) - (k - 1)(\ell' - 1) = (k - 1)(k - n - \ell + 1) \).

Now, let \( u, v \) be \( \ell \)-substrings of \( y_i, y_j \), respectively; note that the \( \ell \)-suffices of \( u, v \) are \( \ell \)-substrings of \( y_i, y_j \), respectively, and hence if \( u = v \) then \( i = j \) and their locations in \( y_i \) agree. It follows that the locations of \( u, v \) in \( y_i \) agree as well, and the claim follows.

Recall, then, that given \( \mathcal{L}_{\ell+1}(\text{Enc}_B(x)) \), an efficient algorithm produces the set of strings \( \{\hat{y}_i : i \in [k]\} \). Then, by ordering and subsequent removal of the length-log(k) indices from these strings, one obtains the string \( y = E(x) \), and consequently, \( x \). Note that the role of the indices in this construction is crucial to deduce \( y \) from its \( \ell \)-profile; without the indices the order of these \( k \) substrings could not have been derived, hence one would only obtain \( y \) up to a permutation of its non-overlapping \((n/k')\)-substrings. The next theorem analyzes the parameters of codes that can be constructed using Construction B based upon Lemma 3 and Theorem 5.

Theorem 19: Given \( \ell(n, k) \), denote \( f(n, k) \triangleq \ell(n, k) - \log(nk) - \log(k) \). Further, let \( \ell' \triangleq \ell(n, k) - \log(k) \). Here, we assume Construction B is operated with \( n, k, \ell' \). Observe
\[
\ell' - \log(n') = f(n, k) - \log\left(1 - \frac{\log(k)}{n}\right) \geq f(n, k).
\]

1) If \( f(n, k) \geq 3 \log \log(nk) + 2 \) then utilizing Theorem 5 in Construction B we obtain
\[
R(\mathcal{C}_B(n, k)) \geq 1 - \left( \frac{q^4 - |f(n, k)/3|}{q - 2} - \log(e) \right) - o(\frac{1}{n}).
\]

(For \( q = 2 \) that is \( R(\mathcal{C}_B(n, k)) \geq 1 - 2^{-\log(nk)} - 2^{-\log(k)} - o(\frac{1}{n}) \).

2) If \( f(n, k) \geq \log(nk) + 2 + 2 \log\left(1 - \frac{\log(k)}{n}\right) \) then utilizing Lemma 3 in Construction B we have
\[
R(\mathcal{C}_B(n, k)) \geq 1 - \frac{\log(e)}{n - \log(k)} - o(\frac{1}{n}).
\]

Proof:

1) Note that by the assumption, Theorem 5 may be applied for some choice of \( t \). Since Construction B does not require \( y \) to be run-length constrained, we let \( t \triangleq \left(\log(n')/3\right) \) and observe
\[
m \geq n' - t - 1 - \left[ \frac{q^t}{q - 2} n'/q \right] = n' - \left[ \frac{q^t}{q - 2} n'/q (\ell' - \log(n')/3) \right] \geq \left(1 - \frac{q^t}{q - 2} |f(n, k)/3| \right) k(n - \log(k)) - 1.
\]

(For \( q = 2 \), that is \( m \geq (1 - 2^{-\log(nk)/3}) k(n - \log(k)) - 3 \).)

It then follows from Lemma 16 that
\[
R(\mathcal{C}_B(n, k)) = \left( \frac{m}{\log |\mathcal{X}_{n,k}|} \right) \geq \frac{1}{k} k(n - \log(k/e)) + o(k) = \frac{q^4 - |f(n, k)/3|}{q - 2} - \frac{1}{n - \log(k)} k(n - \log(k)) + o(k)
\]
\[
= 1 - \frac{q^4 - |f(n, k)/3|}{q - 2} - \frac{1}{n - \log(k)} - o(\frac{1}{n}).
\]

where again the last equality follows from \( \frac{1}{1-x} = 1 + x + x^2 + \cdots \), and from the observation \( n - \log(k) = \Theta(n) \). (Similarly for \( q = 2 \).)

2) Equivalently, \( \ell' \geq 2 \log(n') + 2 \), hence by Lemma 3 we have \( m = n' - 1 \). Following the same steps as
in the last part,\[ R(C_B(n,k)) = \frac{m}{\log|X_{n,k}|} \geq 1 - \frac{\log(e)}{n - \log(k)} - o\left(\frac{1}{n}\right). \]

**B. Overlap-Based Construction**

While in Construction B we added indices in order to overcome the lack of ordering when the string \( y = E(x) \) is partitioned into \( k \) substrings, in Construction C we tackle this constraint differently. To wit, we again partition \( y \), but include overlapping segments between consecutive substrings. The overlapping segments will guarantee in decoding that, given the set of \( k \) substrings, there will be a unique way to concatenate them into one long string. As opposed to Construction B, this approach eliminates the need to decrease the length used for repeat-free encoders with respect to that of the read substrings, i.e., \( \ell \).

**Construction C:** For a given \( \ell \), denote \( n' = nk - (k - 1)\ell \), and take \( m \) such that \( E : \Sigma^m \to RF_\ell(n') \) is any repeat-free encoder. Let \( x \in \Sigma^m \) be an arbitrary information string, and encode it into \( y \equiv E(x) \). Define \( k \)-length-\( n \) strings \( y_0, \ldots, y_{k-1} \in \Sigma^m \) by segmenting \( y \) with an overlap of \( \ell \) symbols between consecutive segments; more precisely, let \( y_i \equiv (y_{i,1}, \ldots, y_{i,n}) \) for \( i \in [k] \), where\[ y_{i,j} \equiv y_{i(n-\ell)+j}; \quad j \in [n]. \]

Then,\[ \text{Enc}_C(x) \equiv \{y_i : i \in [k]\} \in X_{n,k}. \] We denote \( C_C(n,k) \equiv \text{Enc}_C(\Sigma^m) \). The decoding success of Construction C follows from the following simple observation.

**Lemma 20:** For all \( x \in \Sigma^m \) it holds that \( \mathcal{L}_{\ell+1}(y) = \mathcal{L}_{\ell+1}(\text{Enc}_C(x)) \).

**Proof:** Since \( y_i \) is a substring of \( y \) for all \( i \), it follows that \( \mathcal{L}_{\ell+1}(\text{Enc}_C(x)) \subseteq \mathcal{L}_{\ell+1}(y) \). For the other direction, note that \( y_i, y_{i+1} \) are overlapping substrings of \( y \) for all \( 1 \leq i < k \), with a common substring of length \( \ell \); thus all \( (\ell+1) \)-substrings of \( y \) are also substrings of some \( y_i \).

Lemma 20 immediately implies the next corollary.

**Corollary 21:** \( C_C(n,k) \subseteq RF_\ell(n') \).

**Proof:** By Lemma 20 and since \( y \in RF_\ell(n') \).

We are now ready to analyze the code parameters that Construction C can achieve, again based on Lemma 3 and Theorem 5.

**Theorem 22:** Given \( \ell(n,k) \), denote \( f(n,k) \equiv \ell(n,k) - \log(nk) \).

1) If \( f(n,k) \geq 3 \log(nk) + 12 \) then utilizing Theorem 5 in Construction C we obtain\[ R(C_C(n,k)) \geq 1 - \frac{g^{k/[f(n,k)/3]} - 1}{q - 2} - (1 + o(1)) \frac{\log(n) + f(n,k)}{n - \log(k)}. \]

(for \( q = 2 \), that is \( R(C_C(n,k)) \geq 1 - 2^{5[f(n,k)/3]} - (1 + o(1)) \frac{\log(n) + f(n,k)}{n - \log(k)} \).\]

2) If \( f(n,k) \geq \log(nk) + 2 + 2 \log\left(1 - \left(1 - \frac{1}{k}\right)\frac{\ell(n,k)}{n}\right) \) then utilizing Lemma 3 in Construction C we have\[ R(C_C(n,k)) \geq 1 - (1 + o(1)) \frac{\log(n) + f(n,k)}{n - \log(k)}. \]

**Proof:** Recalling from Construction C that \( n' = nk - (k - 1)\ell(n,k) \), we begin by observing\[ \frac{n'}{nk} = 1 - \left(1 - \frac{1}{k}\right)\frac{\ell(n,k)}{n} = 1 - \frac{\log(k)}{n} - (1 + o(1)) \frac{\log(n) + f(n,k)}{n}, \]

hence \( \ell(n,k) - \log(n') = \ell(n,k) - \log(nk) + O(1) = f(n,k) + O(1) \). Also, by multiplying the above equality with \( \frac{n}{n - \log(k)} \) we have\[ \frac{n'}{(n - \log(k))k} = 1 - (1 + o(1)) \frac{\log(n) + f(n,k)}{n - \log(k)}. \]

Next,\[ 1) \text{As in the proof of Theorem 19,} \]

\[ m \geq \left(1 - \frac{q^4}{q^2} q^{-[f(n,k)/3]}\right)n' - 1, \]

and following the same steps\[ R(C_C(n,k)) \geq \frac{m}{\log|X_{n,k}|} \geq 1 - \frac{g^{k/[f(n,k)/3]} - 1}{q - 2} - (1 + o(1)) \frac{\log(n) + f(n,k)}{n - \log(k)}. \]

2) Again, we have \( \ell(n,k) \geq 2 \log(n') + 2 \), hence \( m = n' - 1 \). It follows that\[ R(C_C(n,k)) = 1 - (1 + o(1)) \frac{\log(n) + f(n,k)}{n - \log(k)}. \]

We note that inherent to Construction C is that the last step might introduce more redundancy than is required for repeat-free encoding. Indeed, for \( f(n,k) \geq 3 \log(n) \) the latter term in Theorem 22 becomes significant, and the construction’s rate is then correspondingly decreasing in \( f(n,k) \); this is an oddity since \( RF_\ell_1(n,k) \subseteq RF_\ell_2(n,k) \) for all \( \ell_1 \leq \ell_2 \).

**C. Constructions’ Rates**

In this section we study the performance of the two proposed constructions. We first seek to give a converse to Corollary 17 and establish the result on the minimum value of \( \ell \) which guarantees that the asymptotic rate of multi-strand \( \ell \)-reconstruction codes (in fact, \( RF_\ell_1(n,k) \)) is 1. This result is established in the next corollary using Construction C.

**Corollary 23:** For \( n, k \) satisfying \( \limsup \frac{\log(k)}{n} < 1 \) and for \( \ell \geq \log(nk) + 3 \log\log(nk) + 12 \), it holds that \( R(RF_\ell_1(n,k)) = 1 - o_n(1) \).

Note that if one aims to achieve rate \( 1 - o(1) \) using Construction B, then the minimum value of \( \ell(n,k) \) should be \( \log(nk^2) + 3 \log\log(nk) + 12 \), i.e., there exists a gap of \( \log(k) \) with respect to the result in Corollary 23. However, for comparable values of \( \ell(n,k) \), Construction B may offer better code rate; a comparison of the rates of both constructions,
Fig. 6. Trade-off of window-length to constructions’ rates.

based on Theorems 19 and 22, for applicable values of \( \ell(n,k) \) is illustrated in Figure 6, in context of the lower bound of Corollary 17. The following observation follows from these results.

**Lemma 24:** \( R(C_B(n)) > R(C_C(n)) \) for sufficiently large \( n \) if 1) \( \ell(n,k) \geq \log(n^2k^3) + 2 + 2\log\left(1 - \frac{\log(k)}{n}\right) \); or 2) if \( k = \Omega(n^2) \), for \( \ell - \log(n^4k^2) + 3\log\log(n^4k) = \omega(1) \); or 3) if \( k = \omega(\sqrt{n}) \), for \( \ell \geq \log(n^2k^3) + 3\log\log(nk) + 12 \).

**Proof:** Clearly the claim holds if \( \ell(n,k) \geq \log(n^2k^3) + 2 + 2\log\left(1 - \frac{\log(k)}{n}\right) \) by part 2 of Theorem 19, satisfying part 1.

For lower values of \( \ell = \ell(n,k) \), suffice that \( \ell - \log(n^4k^2) + 3\log\log(n^4k) = \omega(1) \) (10).

For part 2, observe that
\[
\ell - \log(n^4k^2) + 3\log\log(n^4k) = \omega(1).
\]

For part 3 is justified by
\[
\begin{align*}
\log(n^2k^3) + 2 + 2\log\left(1 - \frac{\log(k)}{n}\right) \\
- \log(n^4k^2) + 3\log\log(n^4k)
\end{align*}
\]

VI. C CONCLUSION

In this work, we generalized both the reconstruction from substring-composition problem, and the torn-paper problem, by studying an intermediate setting of partial overlap between read substrings. Our analysis is done in worst-case (i.e., adversarial) regime, as opposed to the probabilistic treatment of this problem in [30]. For the case of a single string \( (k = 1) \), we proved an upper bound on achievable code rates (implying in particular a lower bound on the length of read substrings, required for asymptotically non-vanishing codes’ rates), and developed an efficient construction asymptotically achieving optimal rate. Pleasingly, at the two extreme points, Construction A essentially degenerates to known constructions for either the torn-paper channel [2] (for \( \gamma = 0 \)) or for reconstruction from substring-composition [11] (for \( \gamma \rightarrow 1/\alpha \)). Finally, we demonstrate that like in the torn-paper extreme, one may also extend solutions to the reconstruction from substring-composition problem to multiset-codes. It is left for future work to extend the intermediate setting in this fashion.

Before concluding, we suggest that one might consider a slightly different channel definition to that of Section VI, where the \( k \) strands are required to be distinct from one another, i.e., when information is stored in the space
\[
X^* = \{S \subseteq \Sigma^n : |S| = k\}.
\]

A priori, it seems feasible that the added restriction might allow for lower redundancy (when measured in \( X^* \)). However, we note that \( |X^*| = \binom{n}{k} \), thus a similar development to Lemma 16 yields
\[
\frac{(q^n - k)^k}{k!} \leq |X^*| = q^{nk/k!}.
\]

It follows that \( \log|X^*| = k(n - \log(k/e)) + o(k) \) as well. A careful examination reveals that Constructions B and C actually encode into \( X^* \) and \( R(x,k) \), and hence the results of this work also hold for that setup of the problem.

ACKNOWLEDGMENT

The authors gratefully acknowledge the two anonymous reviewers, and associate editor, whose insight and suggestions helped shape this paper and greatly improve its presentation.

**References**


Yonatan Yehezkeally (Member, IEEE) received the B.Sc. degree (cum laude) in mathematics and the M.Sc. (summa cum laude) and Ph.D. degrees in electrical and computer engineering from Ben-Gurion University of the Negev, Beer-Sheva, Israel, in 2013, 2017, and 2020 respectively. Since 2020, he is currently a Carl Friedrich von Siemens Post-Doctoral Research Fellow of the Alexander von Humboldt Foundation, working in the Associate Professorship of coding and cryptography (Prof. Wachter-Zeh), School of Computation, Information and Technology, Technical University of Munich. His research interests include coding for novel storage media, with a focus on DNA-based storage and nascent sequencing technologies, as well as combinatorial structures and finite group theory.

Daniella Bar-Lev (Student Member, IEEE) received the B.Sc. degree in computer science and mathematics and the M.Sc. degree in computer science from the Technion—Israel Institute of Technology, Haifa, Israel, in 2019 and 2021, respectively, where she is currently pursuing the Ph.D. degree with the Computer Science Department. Her research interests include algorithms, discrete mathematics, coding theory, and DNA storage.

Sagi Marcovich (Student Member, IEEE) received the B.Sc. degree in software engineering and the M.Sc. degree in computer science from the Technion—Israel Institute of Technology, Haifa, Israel, in 2016 and 2021, respectively, where he is currently pursuing the Ph.D. degree with the Computer Science Department. His research interests include algorithms, information theory, and coding theory with applications to DNA based storage.