Reconstruction Codes for DNA Sequences with Uniform Tandem-Duplication Errors

Yonatan Yehezkeally, Student Member, IEEE, and Moshe Schwartz, Senior Member, IEEE

Abstract—DNA as a data storage medium has several advantages, including far greater data density compared to electronic media. We propose that schemes for data storage in the DNA of living organisms may benefit from studying the reconstruction problem, which is applicable whenever multiple reads of noisy data are available. This strategy is uniquely suited to the medium, which inherently replicates stored data in multiple distinct ways, caused by mutations. We consider noise introduced solely by uniform tandem-duplication, and utilize the relation to constant-weight integer codes in the Manhattan metric. By bounding the intersection of the cross-polytope with hyperplanes, we prove the existence of reconstruction codes with full rate, as well as suggest a construction for a family of reconstruction codes.

Index Terms—DNA storage, reconstruction, string-duplication systems, tandem-duplication errors

I. INTRODUCTION

DNA is attracting considerable attention in recent years as a medium for data storage, due to its high density and longevity [8]. Data storage in DNA may provide integral memory for synthetic-biology methods, where such is required, and offer a protected medium for long-period data storage [4], [42]. In particular, storage in the DNA of living organisms is now becoming feasible [40]; it has varied usages, including watermarking genetically modified organisms [3], [16], [35] or research material [21], [42], and even affords some concealment to sensitive information [9]. Naturally, therefore, data integrity in such media is of great interest.

Several recent works have studied the inherent constraints of storing and retrieving data from DNA. While desired sequences (over quaternary alphabet) may be synthesized (albeit, while suffering from substitution noise), generally data can only be read by observation of its subsequences, quite possibly an incomplete observation [22]. Moreover, the nature of DNA and current technology results in asymmetric errors which depend upon the dataset [14]. The medium itself also introduces other types of errors which are atypical in electronic storage, such as symbol/block-deletion and adjacent transpositions (possibly complemented) [15]. Finally, the purely combinatorial problem of recovering a sequence from the multiset of all its subsequences (including their numbers of incidence), was also studied, e.g., [1], [41], as well as coding schemes involving only these multisets (or their profile vectors – describing the incidence frequency of each subsequence) [38].

Other works were concerned with data storage in the DNA of a living organism. While this affords some level of protection to the data, and even propagation (through DNA replication), it is also exposed to specific noise mechanisms due to mutations. Examples of such noise include symbol insertions, deletion, substitutions (point-mutation), and duplication (including tandem- and interspersed-duplication). Therefore, schemes for data storage in live DNA must address data integrity and error-correction.

In an effort to better understand these typical noise mechanisms, their potential to generate the diversity observed in nature was studied. [12] classified the capacity and/or expressiveness of the systems of sequences over a finite alphabet generated by four distinct substring duplication rules: end-duplication, tandem-duplication, palindromic-duplication, and interspersed-duplication. [18] fully characterized the expressiveness of bounded tandem-duplication systems, proved bounds on their capacity (and, in some cases, even exact values). [20] later showed that when point-mutations act together with tandem-duplication as a sequence-generation process, they may actually increase the capacity of the generated system. [2] looked at the typical duplication distance of binary sequences; i.e., the number of tandem-duplications generating a binary sequence from its root. It was proven that for all but an exponentially small number of sequences that number is proportional to the sequence length. Further, when tandem-duplication is combined with point-mutations (here, only within the duplicated string), it was shown that the frequency of substitutions governs whether that distance becomes logarithmic.

The generative properties of interspersed-duplication were also studied from a probabilistic point of view. [11], [13] showed (under assumption of uniformity) that the frequencies of incidence for each subsequence converge to the same limit achieved by an i.i.d. source, thus reinforcing the notion that interspersed-duplication is—on its own—capable of generating diversity. [10] specifically looked at tandem- and end-duplication, and found exact capacities in the case of duplication length 1 by a generalization of the Pólya urn model that applies to strings. It also tightly bounded the capacity of complement tandem-duplication, a process where the duplicated symbol is complemented (using binary alphabet).

Finally, error-correcting codes for data affected by tandem-duplication have been studied in [19], which presented a...
construction of optimal-size codes for correcting any number of errors under uniform tandem-duplication (fixed duplication length), computing their (and thus, the optimal-) capacity. It also presented a framework for the construction of optimal codes for the correction of a fixed number of errors. Next, it studies bounded tandem-duplications, where a characterization of the capacity of error-correcting codes is made for small constants. In general, it characterized the cases where the process of tandem-duplication can be traced back uniquely. More recently, a flurry of activity in the subject includes works such as [27], [29], [30] which provide some implicit and explicit constructions for uniform tandem-duplication codes, as well as some bounds.

However, classical error-correction coding ignores some properties of the DNA storage channel; namely, stored information is expected to be replicated, even as it is mutated. This lends itself quite naturally to the reconstruction problem [34], which assumes that data is simultaneously transmitted over several noisy channels, and a decoder must therefore estimate that data based on several (distinct) noisy versions of it. Solutions to this problem have been studied in several contexts. It was solved in [34] for sequence reconstruction over finite alphabets, where several error models were considered, such as substitutions, transpositions and deletions. Moreover, a framework was presented for solving the reconstruction problem in general cases of interest in coding theory, utilizing a graph representation of the error model, which was further developed in [32], [33]. The problem was also studied in the context of permutation codes with transposition and reversal errors [23]–[25], and partially solved therein. Later, applications were found in storage technologies [6], [7], [43], [44], since modern application might preclude the retrieval of a single data point, in favor of multiple-point requests. However, the problem hasn’t been addressed yet for data storage in the DNA of living organisms, where it may be most applicable.

In this paper, we study the reconstruction problem over DNA sequences, with uniform tandem-duplication errors. The main contributions of the paper are the following: We show that reconstruction codes in this setting are necessarily error-correcting codes with appropriately chosen minimum distance, based on the uncertainty parameter. We also show that in two asymptotic regimes, we can always obtain higher size than error-correcting codes. These asymptotic regimes include what we believe is the most interesting one, where the uncertainty is sublinear, and the time (number of mutations) is bounded by a constant.

The paper is organized as follows: In Section II we present notations and definitions. In Section III we demonstrate that reconstruction codes partition into error-correcting codes and find the requisite minimal-distance of each part, as a function of the reconstruction parameters. We see that these parts can be isometrically embedded as constant-weight codes in the Manhattan metric. Finally, in Section IV we show that reconstruction codes exist with full capacity, and also suggest a construction for reconstruction codes; we also briefly review recent results, published after the submission of this paper. We conclude with closing remarks in Section V.

II. PRELIMINARIES

Throughout this paper, though DNA is composed of four nucleotide bases, we observe the more general case of sequences over a finite alphabet; since the alphabet elements are immaterial to our discussion, we denote it throughout as $\mathbb{Z}_q$.

We observe the set of finite sequences (also: words) over it $\mathbb{Z}_q^* \triangleq \bigcup_{n=0}^{\infty} \mathbb{Z}_q^n$. For any two words $u,v \in \mathbb{Z}_q^*$, we denote their concatenation $uv$. For each word $x \in \mathbb{Z}_q^n$, we denote its length $|x| = n$. We also take special note of the set of words with length higher than or equal to some $0 < k \in \mathbb{N}$, which we denote $\mathbb{Z}_q^{\geq k} \triangleq \{x \in \mathbb{Z}_q^* \mid |x| \geq k\}$. For ease of notation, we let $\mathbb{N}$ stand for the set of non-negative integers throughout the paper; when an integer is assumed to be strictly positive, we make special note of that fact.

For $0 < k \in \mathbb{N}$, $i \in \mathbb{N}$, we define a tandem-duplication of duplication-length $k$ by the mappings

$$\mathcal{T}_{k,i}(x) \triangleq \begin{cases} uuvw & x = uuv, \ |u| = i, |v| = k; \\ x & \text{otherwise.} \end{cases}$$

If $y = \mathcal{T}_{k,i}(x)$ and $y \neq x$ (which occurs whenever $|x| \geq i + k$), we say that $y$ is a descendant of $x$, and denote $x \Rightarrow_k y$. In what follows, we focus on the uniform tandem-duplication model (i.e., we fix $k$) because of its simplicity.

Further, given a sequence $\{x_j\}_{j=0}^{t} \subseteq \mathbb{Z}_q^*$ such that for all $0 \leq j < t$, $x_j \Rightarrow_k x_{j+1}$, we say that $x_t$ is a $t$-descendant of $x_0$, and denote $x_0 \Rightarrow_k^t x_t$. For completeness, we also denote $x \Rightarrow_k^0 x$. Finally, if there exists some $t \in \mathbb{N}$ such that $x \Rightarrow_k^t y$, we also denote $x \Rightarrow_k^\ast y$.

We denote the set of $t$-descendants of $x \in \mathbb{Z}_q^*$ as $D_k(x) \triangleq \{y \in \mathbb{Z}_q^* \mid x \Rightarrow_k^t y\}$, for some $t \in \mathbb{N}$. We also denote the descendant cone of $x$ by $D_k(x) \triangleq \bigcup_{t=0}^{\infty} D_k(x)$.

We say that $x \in \mathbb{Z}_q^{\geq k}$ is irreducible if $x \notin D_k(x)$ implies $y = x$. We exclude from the definition shorter words, for which the condition vacuously holds. We denote by $\text{Irr}_k$ the set of all irreducible words, and $\text{Irr}_k(n) \triangleq \text{Irr}_k \cap \mathbb{Z}_q^n$.

It was shown in [20], [31] that for each word $x \in \mathbb{Z}_q^{\geq k}$, a unique irreducible word exists for which $x$ is a descendant.

We call it the root of $x$, and denote it by $R_k(x)$. This induces an equivalence relation by $x \sim_k y$ if $R_k(x) = R_k(y)$.

We also follow [20] in defining, for $x \in \mathbb{Z}_q^{\geq k}$, $\text{Pref}(x)$ as the length-$k$ prefix of $x$, and $\text{Suff}(x)$ as its suffix; i.e., if $x = xu'v$ where $|u| = |v| = k$, then $\text{Pref}(x) = u$ and $\text{Suff}(x) = v$. Using this notation, we define an embedding $\phi_k : \mathbb{Z}_q^{\geq k} \to \mathbb{Z}_q^k \times \mathbb{Z}_q^*$ by

$$\phi_k(x) \triangleq (\text{Pref}(x), \text{Suff}[x|-k](x) - \text{Pref}[x|-k](x)).$$

It is seen in [20] that this mapping is indeed injective. Further, it was shown that, defining $\zeta_{k,i} : \mathbb{Z}_q^k \times \mathbb{Z}_q^* \to \mathbb{Z}_q^k \times \mathbb{Z}_q^*$ by

$$\zeta_{k,i}(a,b) \triangleq \begin{cases} (a,b_10^kb_2) & b = b_1b_2, |b_1| = i; \\ (a,b) & \text{otherwise,} \end{cases}$$

is also presented a framework for the construction of optimal-size codes for correcting any number of errors under uniform tandem-duplication (fixed duplication length), computing their (and thus, the optimal-) capacity. It also presented a framework for the construction of optimal codes for the correction of a fixed number of errors. Next, it studies bounded tandem-duplications, where a characterization of the capacity of error-correcting codes is made for small constants. In general, it characterized the cases where the process of tandem-duplication can be traced back uniquely. More recently, a flurry of activity in the subject includes works such as [27], [29], [30] which provide some implicit and explicit constructions for uniform tandem-duplication codes, as well as some bounds.

However, classical error-correction coding ignores some properties of the DNA storage channel; namely, stored information is expected to be replicated, even as it is mutated. This lends itself quite naturally to the reconstruction problem [34], which assumes that data is simultaneously transmitted over several noisy channels, and a decoder must therefore estimate that data based on several (distinct) noisy versions of it. Solutions to this problem have been studied in several contexts. It was solved in [34] for sequence reconstruction over finite alphabets, where several error models were considered, such as substitutions, transpositions and deletions. Moreover, a framework was presented for solving the reconstruction problem in general cases of interest in coding theory, utilizing a graph representation of the error model, which was further developed in [32], [33]. The problem was also studied in the context of permutation codes with transposition and reversal errors [23]–[25], and partially solved therein. Later, applications were found in storage technologies [6], [7], [43], [44], since modern application might preclude the retrieval of a single data point, in favor of multiple-point requests. However, the problem hasn’t been addressed yet for data storage in the DNA of living organisms, where it may be most applicable.

In this paper, we study the reconstruction problem over DNA sequences, with uniform tandem-duplication errors. The main contributions of the paper are the following: We show that reconstruction codes in this setting are necessarily error-correcting codes with appropriately chosen minimum distance, based on the uncertainty parameter. We also show that in two asymptotic regimes, we can always obtain higher size than error-correcting codes. These asymptotic regimes include what we believe is the most interesting one, where the uncertainty is sublinear, and the time (number of mutations) is bounded by a constant.

The paper is organized as follows: In Section II we present notations and definitions. In Section III we demonstrate that reconstruction codes partition into error-correcting codes and find the requisite minimal-distance of each part, as a function of the reconstruction parameters. We see that these parts can be isometrically embedded as constant-weight codes in the Manhattan metric. Finally, in Section IV we show that reconstruction codes exist with full capacity, and also suggest a construction for reconstruction codes; we also briefly review recent results, published after the submission of this paper. We conclude with closing remarks in Section V.
where $0 < k \in \mathbb{N}$, $i \in \mathbb{N}$, we have
\[
\phi_k(T_{k,i}(x)) = \zeta_{k,i}(\phi_k(x)).
\]
The simplicity of $\zeta_{k,i}$ in comparison to $T_{k,i}$ motivates the analysis of tandem-duplications using the $\phi_k$ images of sequences.

If $b \in \mathbb{Z}_q^n$ is composed of the subsequences
\[
b = 0^{s_1}w_10^{s_2} \cdots w_m0^{s_{m+1}}; \quad w_1, \ldots, w_m \in \mathbb{Z}_q \setminus \{0\}
\]
we define
\[
\mu(b) \triangleq 0^{s_1} \bmod k \cdot w_10^{s_2} \bmod k \cdots w_m0^{s_{m+1}} \bmod k,
\]
\[
\sigma(b) \triangleq \left( \left\lfloor \frac{s_1}{k} \right\rfloor, \ldots, \left\lfloor \frac{s_{m+1}}{k} \right\rfloor \right).
\]
We may note that $\wt(b) = \wt(\mu(b)) = m$, where $\wt$ is the Hamming weight, and $\sigma(b) \in \mathbb{N}^{\wt(b)+1} = \mathbb{N}^{\wt(\mu(b))+1}$. We also observe that $b$ is recoverable from $\sigma(b), \mu(b)$. It was proven in [20, Cor. 10] that if $\phi_k(x) = (a, b)$, then
\[
\phi_k(R_k(x)) = (a, \mu(b)).
\]
Thus, if $x, y \in \mathbb{Z}_q^{2k}, \phi_k(x) = (a_1, b_1)$ and $\phi_k(y) = (a_2, b_2)$, then $x \sim y$ if and only if $a_1 = a_2$ and $\mu(b_1) = \mu(b_2)$. Moreover, $x \in \text{Irr}_k$ if and only if $\sigma(b_1) = (0, 0, \ldots, 0)$. Note that, equivalently, we may say that $b$ contains no zero-runs of length $k$; such sequences are called $(0, k-1)_q$-Run-Length-Limited, or $(0, k-1)_q$-RLL.

For $x \in \text{Irr}_k$, $\phi_k(x) = (a, b)$, we denote $m(x) \triangleq \wt(b)$ and define $\psi_x : D_k^*(x) \to \mathbb{N}^{m(x)+1}$ by $\psi_x(y) \triangleq \sigma((b))$, where $\phi_k(y) = (a, b)$.

Finally, for $n \geq k$ and $x, y \in \mathbb{Z}_q^n$ we define
\[
d_k(x, y) \triangleq \min \{ t \in \mathbb{N} \mid D_k^*(x) \cap D_k^*(y) \neq \emptyset \},
\]
or $d_k(x, y) = \infty$ if $\{ t \in \mathbb{N} \mid D_k^*(x) \cap D_k^*(y) \neq \emptyset \} = \emptyset$. It was shown in [20, Lem. 14] that $d_k(x, y) = \infty$ if and only if $x \not\sim y$, hence $d_k(\cdot, \cdot)$ is finite on $D_k^*(x)$, for any particular $x \in \mathbb{Z}_q^n$. Furthermore, [20, Lem. 19] shows that for any $x \sim y$ with $|x| = |y|$ it holds that
\[
d_k(x, y) = \frac{1}{2} \parallel \sigma(b_1) - \sigma(b_2) \parallel_1,
\]
thus $d_k(\cdot, \cdot)$ defines a metric on each equivalence class of $\sim_k$.

III. RECONSTRUCTION CODES

The reconstruction problem in the context of uniform tandem-duplication errors can be stated as follows: suppose data is encoded in $C \subseteq \mathbb{Z}_q^n$, and suppose we later are able to read distinct $x_0, x_1, \ldots, x_N \in D_k^*(c)$ for some specific $c \in C$ and $t \in \mathbb{N}$; can we uniquely identify $c$?

It is apparent (see [34]) that to allow successful reconstruction we require codes to satisfy the following.

Definition 1 Take $N, t, n > 0$. We say that $C \subseteq \mathbb{Z}_q^n$ is a uniform tandem-duplication reconstruction code, which we abbreviate as an $(N, t, k)_q$-UTR code, if
\[
\max \{ |D_k^*(c) \cap D_k^*(c')| \mid c, c' \in C, \ c \neq c' \} \leq N.
\]

The purpose of this section is to characterize reconstruction codes. By an evaluation of the size of intersection of descendant cones, we determine the achievable size of $(N, t, k)_q$-UTR codes. We shall state the solution to this problem in terms of error-correcting codes for the Manhattan metric, and devote the next section to an observation of such codes.

A. Structure of descendant cones

Throughout this section we fix some $x \in \text{Irr}_k$, and denote $\phi_k(x) = (a, b)$.

As noted above, for all $y \in D_k^*(x)$, we have $\phi_k(y) = (a, b')$, with $\mu(b') = b$ (hence, in particular, $\wt(b') = \wt(b)$). We therefore denote $m = m(x) = \wt(b)$ and make the following definition:

Definition 2 We let $\psi_x : D_k^*(x) \to \mathbb{N}^{m+1}$ be defined by $\psi_x(y) = \sigma(b')$, where $\phi_k(y) = (a, b')$.

It was noted in the previous section that $\psi_x$ is then distance-preserving from $(D_k^*(x), d_k)$ to $(\mathbb{N}^{m+1}, \frac{1}{2} \parallel \cdot \parallel_1)$ (the definition of $d_k$, made here specifically for sequences of equal-length, can be extended to $D_k^*(x)$ by considering the shortest path between any two sequences, but for simplicity in what follows, we shall implicitly only consider $d_k$ as a metric over $D_k^*(x)$ for any given $t \in \mathbb{N}$).

Definition 3 We define on $\mathbb{N}^{m+1}$ the partial order $b' \preceq b''$ if for every coordinate $i = 1, \ldots, m + 1$ it holds that $b'_i \leq b''_i$ ($\preceq$ is the well-known product order).

The poset $(\mathbb{N}^{m+1}, \preceq)$ has a simple structure. We shall therefore find it more convenient to consider $D_k^*(x)$ in these terms:

Lemma 4 $\psi_x$ is a poset isomorphism from $(D_k^*(x), \preceq)$ to $(\mathbb{N}^{m+1}, \preceq)$. In particular,
\begin{itemize}
  \item 1) For all $y, y' \in D_k^*(x)$ there exists $z \in D_k^*(x) \cap D_k^*(y')$ such that $D_k^*(y) \cap D_k^*(y') = D_k^*(z)$;
  \item 2) If in addition $|y| = |y'|$ then for all $t \in \mathbb{N}$
  \[
  |D_k^*(y) \cap D_k^*(y')| = \begin{cases} 0 & t < d_k(y, y'), \\ D_k^t - d_k(y, y')(x) & t \geq d_k(y, y'). \end{cases}
  \]
\end{itemize}

Proof: We note that $x \in \text{Irr}_k$, hence $\psi_x(x) = (0, 0, \ldots, 0) \in \mathbb{N}^{m+1}$. Further, we note that in the image of $\phi_k$, a tandem-duplication $\zeta_{k,i}$ corresponds to increasing by one a single coordinate of $\sigma(\cdot)$, i.e., an addition of a unit vector $e_j \in \mathbb{N}^{m+1}$ to $\psi_x(\cdot)$.

Hence, $\psi_x$ is indeed a poset isomorphism, and we see that $\rightarrow$ endows $D_k^*(x)$ with a lattice structure; We denote the join of $y, y' \in D_k^*(x)$ as $y \vee y'$, and their meet $y \wedge y'$. It follows that $z = y \vee y'$ satisfies item 1.

Finally, if $|y| = |y'|$ then by definition of $d \triangleq d_k(y, y')$ we have $z = y \vee y' \in D_k^*(y) \cap D_k^*(y')$, and item 2 is now straightforward to prove from the poset-isomorphism.

Given Lemma 4, we can now find the size of intersection of descendant cones for any $c, c' \in \mathbb{Z}_q^n$ $(n \geq k)$, keeping in mind that $D_k^*(c) \cap D_k^*(c') \neq \emptyset$ if and only if $c \sim_k c'$.

Lemma 5 For $x \in \text{Irr}_k$, $|D_k^*(x)| = \{t+m(x)\}$.

Proof: By Lemma 4 we know that
\[
D_k^*(x) = \{y \in D_k^*(x) \mid \parallel \psi_x(y) \parallel_1 = t\}.
\]
Since \( \psi_z : D_k^r(x) \rightarrow N^{m(x)+1} \) is bijective, \( |D_k^r(x)| \) equals the number of distinct integer solutions to \( \sum_{j=1}^{m+1} x_j = t \), where \( x_1, \ldots, x_{m+1} \geq 0 \) (equivalently, the number of distinct ways to distribute \( t \) identical balls into \( m(x)+1 \) bins).

### B. Size of reconstruction codes

In this section we aim to estimate the maximal size of \((N, t, k, q)\)- UTR codes.

**Definition 6** For \( m, r > 0 \) we denote the simplex of dimension \( m \) and weight \( r \), or \((m, r)\)-simplex

\[
\Delta^m_r \triangleq \left\{ (x_i)_{i=1}^{m+1} \in \mathbb{N}^{m+1} \mid \sum_{j=1}^{m+1} x_j = r \right\}.
\]

**Theorem 7** We take positive integers \( N, t \) and \( n > k \). For \( C \subseteq \mathbb{Z}_q^n \) and \( x \in \text{Irr}_k \) we partition \( C_x \triangleq C \cap D_k^*(x) \) and define \( r(x) \triangleq \frac{n-k}{k} \).

If \( x \neq \emptyset \) then \( r(x) \in \mathbb{N} \) and \( r(x) < \left\lfloor \frac{n}{k} \right\rfloor \). Moreover, \( C \) is an \((N, t, k, q)\)- UTR code if and only if for all \( x \in \text{Irr}_k \) such that \( C_x \neq \emptyset \), the image \( \psi_x(C_x) \subseteq \Delta^m(r(x)) \) satisfies

\[
\min \left\{ \frac{1}{2} ||c - c'||_1 \mid c \neq c' \in \psi_x(C_x) \right\} \geq d_{N,t}(m(x)),
\]

where we make the notation

\[
d_{N,t}(m) \triangleq \min \left\{ \delta \in \mathbb{N} \mid \frac{t - \delta + m}{m} \leq N \right\}.
\]

**Proof:** If \( C \cap D_k^*(x) \neq \emptyset \) then it follows from the definitions that for some \( r \in \mathbb{N} \) we have \( |x| + rk = n \); since \( |x| \geq k \), necessarily \( r = r(x) < \left\lfloor \frac{n}{k} \right\rfloor \). Furthermore, \( C \cap D_k^*(x) = C \cap D_k^*(x) \), hence we have seen in the proof of Lemma 4 that for all \( y \in D_k^*(x) \) we have \( \psi_x(y) = \sum_{y_j \in \psi_x(y)} y_j \in \Delta^m(r(x)) \).

In addition, by Lemma 4 and Lemma 5, for all \( x \in \text{Irr}_k \) and \( y \neq y' \in C_x \) the size of intersection \( D_k^*(y) \cap D_k^*(y') \) is \( (t - d_k(y, y') + m(x)) \). It follows that \( C_x \) is an \((N, t, k, q)\)- UTR code if and only if that size is no greater than \( N \) for all such \( y, y' \in C_x \).

Recalling that \( \psi_x \) is bijective and distance-preserving, i.e., that \( d_k(y, y') = \frac{1}{2} \| \psi_x(y) - \psi_x(y') \|_1 \), the claim follows for \( C_x \).

To conclude the proof, we recall that for \( x, x' \in \text{Irr}_k \) we have \( D_k^*(x) \cap D_k^*(x') \neq \emptyset \), hence \( C \) is an \((N, t, k, q)\)- UTR if and only if the same is true for \( C_x \), for all \( x \in \text{Irr}_k \).

In other words, Theorem 7 states that the intersection of a uniform-tandem-duplication reconstruction code \( C \) with the descendant cone of any irreducible word \( D_k^*(x) \) can be viewed as an error-correcting code with a suitable minimal distance. Further, we see that these error-correcting codes are equivalent to codes in the Manhattan metric over a simplex \( \Delta^m(r(x)) \). We note here, however, that this does not hold for \( C \) in general: not only is each code’s minimal distance dependent on \( x \), but the dimension and weight of the simplex in which that code exists do, as well.

We therefore see that constructions and bounds on the size of error-correcting codes for uniform tandem-duplication depend on doing the same for error-correcting codes in the Manhattan metric over \( \Delta^m \). We start by noting the maximal size of such codes:

**Definition 8** For \( m, r > 0 \) and \( d \geq 0 \) we define

\[
M(m, r, d) \triangleq \max \left\{ |C| \mid C \subseteq \Delta^m, \min_{c \neq c' \in C} ||c - c'||_1 \geq d \right\}.
\]

We now reiterate that if \( C \subseteq \mathbb{Z}_q^n \), \( x, x' \in \text{Irr}_k(n - rk) \) (i.e., \( r(x) = r(x') = r \)) and \( m(x) = m(x') \), then \( D_k^{n-rk}(x) \cong D_k^{n-rk}(x') \) (through, e.g., \( \psi_x^{-1} \circ \psi_{x'} \)). It is therefore practical to assume \( |C_x| = |C_x'| = M(m, r, d_{N,t}(m)) \) for all such \( x, x' \). This results in the following corollary, which concludes this section:

**Corollary 9** If \( C \subseteq \mathbb{Z}_q^n \) is an \((N, t, k, q)\)- UTR code, and for all \( x \in \text{Irr}_k \) it holds that \( |C_x| = M(m, r, d_{N,t}(m)) \), then

\[
|C| = \sum_{r=0}^{\lfloor n/k \rfloor - 1} \sum_m M(m, r, d_{N,t}(m)) \cdot \left| \{x \in \text{Irr}_k(n - rk) \mid m(x) = m \} \right| = \sum_{r=0}^{\lfloor n/k \rfloor - 1} M(m, r, d_{N,t}(m)) \cdot q^k.
\]

**Proof:** First, trivially, \( |C| = \sum_{x \in \text{Irr}_k} |C_x| \).

Observe that \( x \in \text{Irr}_k \) satisfies \( C_x \neq \emptyset \), \( r(x) = r \) and \( m(x) = m \), if and only if \( \phi_x(x) = (a, b) \), \( b \in (0, k-1)_q \) and \( \text{wt}_b(m) = m \). The rest now follows from Theorem 7.

Corollary 9 motivates us to estimate the optimal size of error-correcting codes in the Manhattan metric over \((m, r)\)-simplex. This topic was examined in some depth in [28], where a construction based on Sidon sets (of particular interest for our application, see [26], and references therein) was proposed, leading to lower bounds tighter than the Gilbert-Varshamov bound. For our purposes, we cite an asymptotic result (we slightly rephrase):

**Lemma 10** [28, Eq. 36] Take \( \mu \in (0, 1) \), \( \rho > 0 \) and integer sequences \((m_n)_{n \geq 0}, (r_n)_{n \geq 0} \) such that \( \lim_{n \to \infty} m_n^{-1} = \mu \) and \( \lim_{n \to \infty} r_n^{-1} = \rho \). Also take a fixed \( d > 0 \). Then

\[
\lim_{n \to \infty} \frac{1}{n} \log_2 M(m_n, r_n, d) = (\mu + \rho) H \left( \frac{1}{1 + \frac{\rho}{\mu}} \right).
\]

**C. Minimal distance of reconstruction codes**

Next, before we can ascertain the sizes of error-correcting codes over simplices, we bound their requisite minimal distance. That is, given \( N, t > 0 \) and \( m > 0 \), we establish bounds on

\[
d_{N,t}(m) \triangleq \min \left\{ \delta \in \mathbb{N} \mid \frac{t - \delta + m}{m} \leq N \right\}
\]

seen in Theorem 7.
Lemma 11 If \( N \leq m \) then \( d_{N,t}(m) = t \).

Proof: We may verify by substitution that \( \delta = t \) satisfies 
\((t-\delta+m)leq N\), while \( \delta = t-1 \) does not. Using the strict 
monotonicity of \( s \mapsto (s+m \over m) \), we are done.

In order to find a practical bound for \( d_{N,t}(m) \) when \( N > m \), 
we first require the following three lemmas:

Lemma 12 1) [36, Ch.10, Sec.11, Lem.7] For integers \( 0 < k < n \) it holds that 
\[
\sqrt{\frac{n}{8k(n-k)}} 2^{H(p)} \leq \left( \frac{k}{n} \right)^n \leq \sqrt{\frac{n}{2\pi k(n-k)}} 2^{nH(\phi)}
\]
where \( H \) is the binary entropy function, defined by 
\( H(p) = -p \log_2 p - (1-p) \log_2 (1-p) \).

Proof: For item 1, we see that if \( 0 < k < n \) we have 
\( n-1 \leq k(n-k) \leq \frac{n^2}{4} \), hence 
\[
\frac{n}{2\pi k(n-k)} \leq \frac{1}{1 + \frac{1}{n-1}} \leq \frac{1}{\pi} < 1,
\]
which completes the proof.

Lemma 13 For \( N > m > 0 \) and \( t > 0 \) it holds that 
\[
d_{N,t}(m) \leq \min \left\{ \delta \in \mathbb{N} \mid H(1 + \frac{t-\delta}{m}) \leq \log_2 N \right\}.
\]

Proof: Under the assumption, \( \delta = t-1 \) satisfies the 
inequality \((t-\delta+m)leq N\). Therefore we may restrict the minimum to \( \delta < t \), giving \( 0 < m < (t-\delta)+m \). Now, 
Lemma 12 implies 
\[
\log_2 \left( \frac{t-\delta+m}{m} \right) \leq m \left( 1 + \frac{t-\delta}{m} \right) H \left( \frac{1}{1 + \frac{1}{\pi}} \right),
\]
which completes the proof.

Lemma 14 For \( x \geq 1 \) it holds that 
\( \mathcal{H}(x) \leq 2 \sqrt{x - 1} \).

Proof: The claim can be restated by the substitution 
\( p = \frac{1}{2} \) as the known inequality 
\( H(p)^2 \leq 4p(1-p) \) (its proof 
follows elementary calculus, and is omitted here).

Finally, 

Theorem 15 Take \( N > m > 0 \). Then 
\[
d_{N,t}(m) \leq \max \left\{ 1, t - \left( \frac{\log_2 N}{4m} \right)^2 \right\}.
\]

Proof: Using Lemma 14 we may bound 
\( \mathcal{H}(1 + \frac{t-\delta}{m}) \leq 2 \sqrt{\frac{t-\delta}{m}} \). Lemma 13 therefore implies that it suffices to require 
\( \sqrt{\frac{t-\delta}{m}} \leq \frac{\log_2 N}{4m} \), and reordering the inequality we get \( \delta \geq t - \left( \frac{\log_2 N}{4m} \right)^2 \), yielding the claim.

IV. CAPACITY OF RECONSTRUCTION CODES

Definition 16 We define the rate of a code \( C \subseteq \mathbb{Z}_q^n \) as 
\[
R(C) = \frac{1}{n} \log_q |C|,
\]
and the capacity of a system \( C \subseteq \mathbb{Z}_q^n \) as 
\[
cap(C) = \limsup_{n \to \infty} \frac{1}{n} \log_q |C \cap \mathbb{Z}_q^n|.
\]

We are interested in \( \sup \{ \cap(C) \} \), where \( C \) is any family of 
reconstruction codes (i.e., \( C \cap \mathbb{Z}_q^n \) is an \( (N,n,t_n,k) \)-code for all \( n \)).

The purpose of this section is to determine that optimal 
capacity in two asymptotic regimes:

Regime I When \( N_n = o(n) \) and \( t_n = t \) is fixed.

Regime II When \( N_n = 2^{\alpha n} \) and \( t_n = \beta n \) for constants 
\( \alpha, \beta > 0 \) (such that \( N_n, t_n \in \mathbb{N} \) for some, hence infinitely 
many, indices).

In practical applications, Regime I is likely to apply, since 
we may indeed expect the number of duplications \( t \), which is 
dependent on the period of time before data is read, 
to be fixed w.r.t. \( n \). The allowed uncertainty \( N_n \) will also 
likely be bounded. Regime II requires Theorem 15 (and some 
restrictions over the values of \( \alpha, \beta \)), but allows us to calculate 
capacity in much the same way, which we do after presenting 
the first.

Note, since [19] showed that \( \text{Irr}_k(n) \) can correct any number of 
tandem-duplication errors, they are trivially \( (N, t, k, q) \)-codes 
for all \( N, t \) (more precisely, they are \( (0, t, k) \)-codes for all \( t \)). In comparison, in the setting we consider only \( t \) tandem-
duplications are assumed to have occurred, therefore the codes 
we seek are less restrictive. Nevertheless, at the time of this 
paper’s submission no bounds on the size of error-correcting 
codes for a fixed number of tandem-duplications were known; 
It is our purpose, then, to demonstrate that reconstruction 
codes exist which have strictly higher capacity than \( \text{Irr}_k \), 
and suggest constructions for families of such codes.

First, we denote for any \( n, r \in \mathbb{N} \) such that \( n \geq k \) and 
\( r < \left\lfloor \frac{n}{k} \right\rfloor \), and any \( N, t \in \mathbb{N} \)
\[
\mathcal{M}_{N,t}(n, r) = \sum_{m=0}^{n} M(m, r, d_{N,t}(m)).
\]

We recall for all \( n \), if \( r_n = \arg\max_r \mathcal{M}_{N,t}(n, r) \), that by 
Corollary 9 we have an \( (N, t, k, q) \)-code \( C \subseteq \mathbb{Z}_q^n \) with \( |C| \geq q^k \mathcal{M}_{N,t}(n, r_n) \). Corollary 9 also implies that for all \( C \subseteq \mathbb{Z}_q^n \) it holds that \( |C| \leq q^k \mathcal{M}_{N,t}(n, r_n) \). We therefore focus on maximizing \( \limsup_{n \to \infty} \frac{1}{n} \log_q \mathcal{M}_{N,t}(n, r_n) \) by choice of \( r_n \).

In what follows, we take \( \gamma \in (0, 1) \) and set \( r_n = \frac{1-\gamma}{k} n - 1 \) 
for any \( n \in \mathbb{N} \) for which \( r_n \in \mathbb{N} \); we shall assume that such \( n \) exist (hence, infinitely many exist), and refer only to such 
indices.

For all \( x \in \text{Irr}_k(n - r_n k) = \text{Irr}_k(k + \gamma n) \), recall that we 
denoted \( \phi_k(x) = (a, b) \) with \( b \in \mathbb{Z}_q^{n-2} \) in \((0, k-1)\)-RLL. We
shall build a reconstruction code in the descendant cones of only such $x$, which we denote $C_\gamma$.

**Lemma 17** There exists a system $S \subseteq (0, k - 1)_q$-RLL and $\theta \in (\frac{1}{2}, 1)$ such that

$$\text{cap}(S) = \lim_{l \to \infty} \frac{1}{l} \log_q |S \cap \mathbb{Z}_q^l| = \text{cap}((0, k - 1)_q$-RLL)

and for all $b \in S$ it holds that $\text{wt}_H(b) \geq \theta |b|$.

**Proof:** Let $G_q(k - 1)$ be the strongly connected deterministic digraph representing the $(0, k - 1)_q$-RLL system, seen in Figure 1, whose adjacency matrix is

$$T_q(k - 1) = \begin{pmatrix} q - 1 & 1 & 0 & \cdots & 0 \\ q - 1 & 0 & 1 & \vdots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ q - 1 & 0 & \cdots & 0 & 1 \\ q - 1 & 0 & \cdots & 0 & 0 \end{pmatrix}.$$

As is well known for the case of $q = 2$ (see, e.g., [17], [45]), its characteristic polynomial is

$$\rho_q(k - 1)(x) = x^k - (q - 1) \sum_{j=0}^{k-1} x^j = \frac{x^{k+1} - qx^k + (q - 1)}{x - 1},$$

hence the Perron eigenvalue $\lambda$ of $T_q(k - 1)$ is the unique positive root of $\rho_q(k - 1)(x) = x^{k+1} - qx^k + (q - 1)$ greater than 1 (in fact, $\lambda \in (q - 1, q)$, which can readily be computed either using elementary calculus or by information-theoretic methods, since $(\mathbb{Z}_q \setminus \{0\})^* \subseteq (0, k - 1)_q$-RLL $\subseteq \mathbb{Z}_q^*$).

Further, $T_q(k - 1)$ has positive right- and left-eigenvectors associated with $\lambda$, which we denote $\vec{v}, \vec{w}$ respectively; specifically,

$$\vec{v} = \left( \begin{array}{c} 1 \\ 1, \lambda - (q - 1), \ldots, \lambda^{j-1} - (q - 1) \sum_{i=0}^{j-2} \lambda^i, \\ \ldots \\ \lambda^{k-1} - (q - 1) \sum_{i=0}^{k-2} \lambda^i \end{array} \right),$$

$$\vec{w} = \left( \begin{array}{c} \lambda^{-1} \\ \lambda^{-2} \\ \ldots \\ \lambda^{-k_j} \ldots, 1 \end{array} \right),$$

and we may verify that

$$v_k = \lambda^{k-1} - (q - 1) \sum_{i=0}^{k-2} \lambda^i = \frac{1}{\lambda} \left[ \lambda^{k-1} - (q - 1) \sum_{i=1}^{k-1} \lambda^i \right]$$

$$= \frac{q - 1}{\lambda} > 0$$

and $v_j = \frac{v_{j+1} + v_{j+q-1}}{\lambda}$, hence every entry of $\vec{v}$ is indeed positive.

Denoting $q_{i,j} = (T_q(k - 1))_{i,j} \cdot \frac{v_{j+q-1}}{\lambda}$, it follows (see, e.g., [37][Sec. 3.5]) that $Q = (q_{i,j})_{1 \leq i,j \leq k}$ is stochastic, and represents a transition matrix of a stationary Markov chain $\mathcal{P}$ on $G_q(k - 1)$ (a probability measure on its edges set $E_q(k - 1)$) satisfying $H(\mathcal{P}) = \log_q \lambda = \text{cap}((0, k - 1)_q$-RLL). Further, the stationary distribution of the Markov chain, i.e., a positive $\vec{\pi} = (\pi_1, \ldots, \pi_k)$ such that $\sum_{j=1}^{k} \pi_j = 1$ and $\vec{\pi}^T Q = \vec{\pi}^T$, is given by $\pi_j = \frac{\vec{v}_j}{\sum_{i=1}^{k} \vec{v}_i}$, where $\vec{\pi}$ is defined by $\vec{\pi}_j = w_j v_j$. It holds for all $j$ that $\bar{\pi}_j$ is the sum of probabilities $\sum \mathcal{P}(e)$ of edges terminating at the $j$th node.

Note, then, that

$$\sum_{i=1}^{k} \bar{\pi}_i = \lambda^{k-1} + \sum_{i=2}^{k} \left[ \lambda^{k-1} - (q - 1) \frac{\lambda^{k-1} - \lambda^{k-1}}{\lambda - 1} \right]$$

$$= \lambda^{k-1} + \left[ 1 + (k - 1) \left( 1 - \frac{q - 1}{\lambda - 1} \right) \right] + \frac{q - 1}{\lambda - 1} \sum_{i=2}^{k-2} \lambda^{k-i}$$

$$= \lambda^{k-1} \left[ k - (k - 1) \frac{q - 1}{\lambda - 1} \right] + \frac{q - 1}{\lambda - 1} \sum_{j=0}^{k-2} \lambda^j$$

$$= \lambda^{k-1} \left[ k - (k - 1) \frac{q - 1}{\lambda - 1} \right] + \frac{\lambda^k - (q - 1)\lambda^{k-1}}{\lambda - 1}$$

and in particular $\pi_1 = \frac{\lambda^{-1} - 1}{\lambda^{-1} - q}$.

(Incidentally, it follows from $\pi_1 \in (0, 1)$ that $1 < q(k - q) < \lambda$, that is, $q - \frac{q}{k-1} < \lambda < \frac{1}{k-1}$.)

Next, recall that for a given $\epsilon > 0$, a $(\mathcal{P}, \epsilon)$-strongly-typical path in $G$ is a path $\gamma = (e_1, e_2, \ldots, e_l)$ (denoted by its edges $\{e_1, e_2, \ldots, e_l\} \subseteq E_q(k - 1)$) such that each $e \in E_q(k - 1)$ appears in the path $l \cdot \tau$ times, for some $\tau$ satisfying $|\tau - \mathcal{P}(e)| \leq \epsilon$. If we let $S_\epsilon \subseteq \mathbb{Z}_q^*$ be the system induced by $(\mathcal{P}, \frac{\epsilon}{k(q - 1)})$-strongly-typical, paths, then it is also known that $\text{cap}(S_\epsilon) = \text{cap}((0, k - 1)_q$-RLL). Note, for $b \in S_\epsilon$ of length $|b| = l$, which is generated by the path $\gamma = (e_1, \ldots, e_l)$, $\text{wt}_H(b)$ is precisely the number of edges which terminate at the first node; since $\gamma$ is $(\mathcal{P}, \frac{\epsilon}{k(q - 1)})$-strongly-typical,

$$\text{wt}_H(b) \geq \sum_{e \text{ terminates at first node}} l \cdot \frac{\epsilon}{k(q - 1)} = l(\pi_1 - \epsilon)$$

To conclude the proof, note

$$\lambda + k(q - \lambda) = q + (k - 1)(q - \lambda) > q \geq 2$$

$$\implies \lambda > 2 - k(q - \lambda)$$

$$\implies 2(\lambda - 1) > \lambda - k(q - \lambda) \implies \pi_1 > \frac{1}{2}$$

Hence we can take any $0 < \epsilon < \pi_1 - \frac{1}{2}$, and observe that $S = S_\epsilon$, $\theta = \pi_1 - \epsilon$ satisfy the proposition.

**Lemma 17** implies that there exists a subset $S_k \subseteq \mathbb{I}_q(k)$ such that $\text{cap}(S_k) = \text{cap}(\mathbb{I}_q(k))$, and for every $x \in S_k$ of length $|x| = k + \gamma n$ we have $m(x) \geq \lfloor \theta \cdot n \rfloor$. For the rest of this section we only build codes $C^n_\gamma$ in the descendant cones of roots in $S_k$. Note, then, that if we denote $m_n = \lfloor \theta \cdot n \rfloor$ and $C_\gamma \triangleq \bigcup C^n_\gamma$, then

$$\text{cap}(C_\gamma) \geq \lim sup \frac{1}{n} \log_q \left[ \mathbb{I}_q(k + \gamma n) \cdot M(m_n, r_n, d_{N, \epsilon}(m_n)) \right]$$

$$= \gamma \cdot \text{cap}(\mathbb{I}_q(k)) +$$

$$+ \lim sup \frac{1}{n} \log_q M(m_n, r_n, d_{N, \epsilon}(m_n))$$

We evaluate the second addend in the following theorem:
Figure 1. The graph $G_q(k-1)$ generating the $(0, k-1)_q$ RLL system.

**Theorem 18** As before, we denote $r_n = \frac{1-\alpha}{k} n - 1$ and $m_n = [\theta \cdot \gamma n]$. Then

$$\lim_{n \to \infty} \frac{1}{n} \log_q M(m_n, r_n, d_{N_n, t_n}(m_n)) = \frac{\theta \gamma}{\log_q q} \cdot \mathcal{H} \left( 1 + \frac{1 - \gamma}{k \theta \gamma} \right)$$

in both of the aforementioned two regimes:

1) Regime I: when $N_n = o(n)$ and $t_n = t$ is fixed.
2) Regime II: when $N_n = 2^\alpha n$ and $t_n = \beta n$, if we additionally require $\frac{\alpha^2}{\beta^2} > 4\theta \gamma$.

**Proof:**

1) Note, for sufficiently large $n$, that $N_n < \theta \cdot \gamma n \leq m_n$, resulting by Lemma 11 in $d_{N_n, t_n}(m_n) = t$. We note that $\lim_{n \to \infty} \frac{m_n}{n} = \frac{1 - \gamma}{\theta \gamma}$ and $\lim_{n \to \infty} \frac{m_n}{n} = \theta \gamma$, hence by Lemma 10 the claim is proven when $t$ is fixed.

2) By Theorem 15:

$$d_{N_n, t_n}(m_n) \leq \max\left\{1, \beta n - \left\lfloor \frac{\alpha^2 n}{4 [\theta \cdot \gamma n]} \right\rfloor \right\} = \max\left\{1, \left\lfloor \beta n - \frac{\alpha^2 n}{4 [\theta \cdot \gamma n]} \right\rfloor \right\}.$$  

If $\frac{\alpha^2}{\beta^2} > 4\theta \gamma$ then for sufficiently large $n$ we have $\beta < \frac{\alpha^2 n}{4 [\theta \cdot \gamma n]}$, hence $d_{N_n, t_n}(m_n) = 1$. Since it is fixed, we may now apply the same argument used in the previous part.

Going forward, we shall view the lower bound to $\text{cap}(C_\gamma)$,

$$R(\gamma) \triangleq \gamma \text{cap}(\text{Irr}_k) + \frac{\theta \gamma}{\log_q q} \cdot \mathcal{H} \left( 1 + \frac{1 - \gamma}{k \theta \gamma} \right),$$

as a function of $\gamma$. Before moving on to show that it may be made to exceed $\text{cap}(\text{Irr}_k)$ by a careful choice of $\gamma$, we look at the following example.

**Example 19** Set $q = k = 2$. Then the Perron eigenvalue of $T_2(1)$ is $\lambda = \frac{1 + \sqrt{5}}{2}$, and

$$\text{cap}(\text{Irr}_2) = \log_2(\lambda) = \log_2 \left( \frac{1 + \sqrt{5}}{2} \right) \approx 0.6942.$$  

In addition, any $\theta$ which is less than $\pi_1 = \frac{1}{2} \left( 1 + \frac{1}{\sqrt{5}} \right) \approx 0.7326$ satisfies Lemma 17.

Alternatively, we may set $q = 4$ (for the special case of DNA) and duplication-length $k = 2$. Now the Perron eigenvalue of $T_4(1)$ is given by $\lambda = \frac{3 + \sqrt{21}}{2}$, hence

$$\text{cap}(\text{Irr}_4) = \log_4(\lambda) = \log_4 \left( \frac{3 + \sqrt{21}}{2} \right) \approx 0.9613.$$  

Further, we may choose any $\theta$ which is less than $\pi_1 = \frac{1}{2} \left( 1 + \frac{1}{\sqrt{7}} \right) \approx 0.8273$. The value at $\gamma = 1$ equals $\text{cap}(\text{Irr}_k)$.

$R(\gamma)$ is shown for both cases in Figure 2, under the assumptions of asymptotic regime made in Theorem 18. The figure demonstrates that the capacity of reconstruction codes (bounded from below by the maximum of the curve) is greater than $\text{cap}(\text{Irr}_k)$.

We now attempt to maximize $R(\gamma)$ by a proper choice of $\gamma \in (0, 1)$. Analysis of $R(\gamma)$ is simpler using the following change of variable:

**Definition 20** Define $x : (0, 1) \to (0, \infty)$ by $x(\gamma) \triangleq \frac{1 - \gamma}{\gamma}$.

We observe that $x(\gamma)$ is a decreasing diffeomorphism, and $\gamma = \frac{1}{1 + x(\gamma)}$. 

Figure 2. Rate $R(\gamma)$ in the cases (a) $q = k = 2, \theta = 0.7236$, and (b) $q = 4, k = 2, \theta = 0.8273$. The value at $\gamma = 1$ equals $\text{cap}(\text{Irr}_k)$. 

Going forward, we shall view the lower bound to $\text{cap}(C_\gamma)$,
**Lemma 21** One has

\[ R(\gamma) = \gamma \text{cap}(\text{Irr}_k) + \theta \gamma \left[ (1 + \frac{x(\gamma)}{k\theta}) \log_q \left( 1 + \frac{x(\gamma)}{k\theta} \right) - \frac{x(\gamma)}{k\theta} \log_q \frac{x(\gamma)}{k\theta} \right] \]

Proof: We observe that for all \( x > 0 \), \( \log \left( x + 1 \right) = \log(x) \log(1 + \frac{1}{x}) = \log(x) - \log x \); in particular

\[ \log_q \left( 1 + \frac{k\theta}{1 - \gamma} \right) = \log_q \left( 1 + \frac{1 - \gamma}{k\theta} \right) - \log_q \frac{1 - \gamma}{k\theta} \gamma \]

Hence,

\[ R(\gamma) = \gamma \text{cap}(\text{Irr}_k) + \theta \gamma \log_q \left( 1 + \frac{1 - \gamma}{k\theta} \right) + \frac{1 - \gamma}{k} \log_q \left( 1 + \frac{k\theta}{1 - \gamma} \right) \]

\[ = \gamma \text{cap}(\text{Irr}_k) + \theta \gamma \log_q \left( 1 + \frac{1 - \gamma}{k\theta} \right) - \frac{1 - \gamma}{k} \log_q \frac{1 - \gamma}{k\theta} \gamma \]

Thus, the main result of this paper is established. In what remains of this section we show that we can bound \( \gamma_0 \) which maximizes \( R(\gamma) \), in practice, to any desired level of accuracy. We begin by establishing bounds in the following lemma.

**Lemma 23** Let \( \gamma_0 \in (0, 1) \) be the unique maximum of \( R(\gamma) \), and denote \( x_0 = x(\gamma_0) \). Then

\[ x_0 \geq \frac{k\theta}{(q^\theta \text{cap}(\text{Irr}_k))^k - 1} \]

and

\[ x_0 \leq \frac{1}{2} \left[ \sqrt{\left( 1 - q^{-\text{cap}(\text{Irr}_k)k} \right)^2 + k\theta q^{-\text{cap}(\text{Irr}_k)k}} - \left( 1 - q^{-\text{cap}(\text{Irr}_k)k} \right) \right] \]

Proof: For fixed \( x \in [0, \infty) \) define \( g_x : (0, \infty) \to \mathbb{R} \) by

\[ g_x(y) = y \ln \left( 1 + \frac{x}{y} \right) \]

Then

\[ g_x'(y) = \ln \left( 1 + \frac{x}{y} \right) + \frac{y}{1 + \frac{x}{y}} \cdot \frac{x - y}{y^2} = \ln \left( 1 + \frac{x}{y} \right) - \frac{x}{y + x} \]

\[ = - \frac{x}{y + x} - \frac{x}{y + x} \geq 0 \]

Therefore, \( f_x(y) = e^{g_x(y)} = \left( 1 + \frac{x}{y} \right)^y \) satisfies \( 1 + x = f_x(1) \leq f_x(y) = \left( 1 + \frac{x}{y} \right)^y \) for all \( y \geq 1 \). In our case \( k\theta > 1 \) and \( x_0 \) satisfies Eq. (4), hence

\[ q^{-\text{cap}(\text{Irr}_k)k} = 1 + \frac{x_0}{k\theta} \]

which we simplify to \( x_0 \geq x_0^2 + (1 - q^{-\text{cap}(\text{Irr}_k)k}) x_0 - k\theta q^{-\text{cap}(\text{Irr}_k)k} \). Thus, the first upper bound is proven. For the second, we require only that for \( a, b > 0 \) it holds that \( \sqrt{a + b^2} - b \leq \frac{a}{2} \), which is readily shown by differentiation.

On the other hand, Eq. (4) implies that \( x_0 \leq k\theta \). Therefore

\[ q^{-\text{cap}(\text{Irr}_k)k} = 1 + \frac{x_0}{k\theta} \leq \frac{2k\theta}{1 + \frac{x_0}{k\theta}} \cdot \frac{x_0}{k\theta} = x_0 + x_0^2 \]

which proves the lower bound.

Next, we show that we may tighten the bounds we derived in the previous lemma.

**Lemma 24** Let \( x_0 > 0 \) be the unique solution to Eq. (4), and denote \( z_0 = \frac{x_0}{k\theta} \). If \( \bar{z} \leq z_0 \leq \gamma \) then \( F(z) \leq z_0 \leq F(\gamma) \), where

\[ F(z) \triangleq \frac{q^{-\text{cap}(\text{Irr}_k)k}}{1 + (z + 1)^{k\theta - 1}} \]

Proof: By assumption we have \( q^{-\text{cap}(\text{Irr}_k)k} \geq (1 + z_0) \gamma^{k\theta - 1} \cdot z_0 \), hence \( q^{-\text{cap}(\text{Irr}_k)k} \leq (1 + \gamma)^{k\theta - 1} \cdot z_0 \), and
\[
R'(\gamma) = \text{cap}(\text{Irr}_k) + \frac{dz}{d\gamma} \frac{dx}{dx} \left[ \frac{\theta}{1 + \frac{m(x)}{k\theta}} \log_4 \left( 1 + \frac{m(x)}{k\theta} \right) - \frac{m(x)}{k\theta} \log_4 \left( \frac{x}{k\theta} \right) \right] = \text{cap}(\text{Irr}_k) - \frac{1}{\gamma} \frac{dx}{dx} \left[ \frac{\theta}{1 + x^2} \log_4 \left( 1 + \frac{x}{k\theta} \right) - \frac{x}{k\theta} \log_4 \left( \frac{x}{k\theta} \right) \right] + \frac{\theta}{1 + x^2} \cdot \left[ \frac{1}{k\theta} \log_4 \left( 1 + \frac{x}{k\theta} \right) - \frac{1}{k\theta} \log_4 \left( \frac{x}{k\theta} \right) \right]
\]

implies that \( z_0 \geq G(\gamma) \) where \( G(z) = \frac{2^{-2\text{cap}(\text{Irr}_k)}}{1 + z^2} \). Similarly, \( z_0 \leq G(z) \). The proposition now trivially follows for \( F(z) = G(G(z)) \).

Finally, we can show that \( x_0 \) may be found by the following limiting process:

**Theorem 25** The unique solution to Eq. (4) is given by \( x_0 = k\theta \lim_{n \to \infty} F^n(z_1) \), for all \( z_1 \in [0, 1] \).

**Proof:** As before, we denote the unique solution \( x_0 > 0 \), and take \( z_0 = \frac{x_0}{k\theta} \).

Note that Lemma 24 implies that \( z_0 = F(z_0) \). We will prove that \( F : [0, 1] \to [0, 1] \) is a contraction; that is, for all \( z_1, z_2 \in [0, 1] \) we have \( |F(z_1) - F(z_2)| \leq c|z_1 - z_2| \) for some \( c < 1 \). Indeed, recalling \( k\theta > 1 \) we find

\[
F(z) = \frac{2^{-2\text{cap}(\text{Irr}_k)}(k\theta - 1)^2}{1 + z^2} \leq \frac{(k\theta - 1)^2}{2^2\text{cap}(\text{Irr}_k)} \leq \frac{(k - 1)^2}{2^2} < \frac{9}{16} < 1,
\]

where the next to last inequality may be directly verified for all small \( k \).

Having done so, we utilize Banach’s fixed-point theorem to deduce that \( F \) has a unique fixed point (necessarily \( z_0 \)), and for all \( z \in [0, 1] \), defining \( z_{n+1} = F(z_n) \) we get \( \lim_{n \to \infty} z_n = z_0 \).

We can now suggest a construction for \((N, t, k, q)\)-UTR codes achieving better capacity than the error-correcting codes \( \text{Irr}_k(n) \) suggested in [19] (provided that one is willing to consider reconstruction codes over unambiguous decoding of any single output).

**Construction A** We set the alphabet size \( q \), duplication length \( k \). In the case that our application falls within Regime I, we also set a fixed decoding delay \( t \), and restrict the ambiguity \( N_n \) to be sub-linear in \( n \). (With the necessary adjustments, this construction also applies for Regime II.)

- Start by finding the Perron eigenvalue \( \lambda \) of \( T(k - 1) \), and \( \pi_1 = \frac{k - 1}{k(q - 1)} \), as in the proof of Lemma 17. Set some \( \theta < \pi_1 \).
- The upper and lower bounds on \( x_0 \) from Lemma 23 can be made tighter by a repetitive application of \( F(\cdot) \) from Lemma 24; Theorem 25 guarantees that the bounds--hence the acceptable error--can be made as tight as desired for our application.
- With \( \gamma_0 = \frac{1}{1 + x_0} \), we may find \( r_n = \frac{1 - \gamma_0}{x_0} - 1 \), and we note that a capacity-achieving subset of \( \text{Irr}_k(n - r_n) \) has weight \( m(x) \geq m_n = [\theta \cdot \gamma_0 \cdot \gamma_n] \).

- Within \( D^c_{m_n}(x) \) of just such irreducible sequences \( x \) we may utilize any construction of codes for the Manhattan metric over \( \Delta_{m_n}^c \) with minimal distance \( t \), if it produces codes of size sufficiently close to \( M(m_n, r_n, t) \). For practical applications, [28, Sec. IV -A] showed that if \( m_n \) is a prime power, then by [5] there exist such codes of size \( |\Delta_{m_n}^c| / m_n^t - 1 \) (which improves on the Gilbert-Varshamov bound, and is sufficiently tight to achieve the same result as in Theorem 18).

Note that we do not establish that Construction A produces a system of codes of capacity 1, rather only greater than \( \text{cap}(\text{Irr}_k) \). To conclude this section, we also present a non-constructive argument proving the existence of a system of reconstruction codes with capacity 1 by an application of the Gilbert-Varshamov bound.

Recall that in the proof of Theorem 18 we have shown that the minimal distance, \( d_{N_n, t}^c(m_n) \) was bounded. In particular, in the case of interest Regime I, we used the fact that \( m_n = \Theta(n) \); This does not, in general, hold for \( m(R_k(y)) \) for all \( y \in \mathbb{Z}_q^n \).

However, if we show that to be the case for a sufficiently large subset \( S_n \subseteq \mathbb{Z}_q^n \), then we may note the following: by [28, Lem. 1] the size of ball in the \( d_k(\cdot, \cdot) \) metric of radius \( d \) in the descendant cone of \( x \in \text{Irr}_k \), where \( m(x) \geq d \), is

\[
\sum_{j=0}^d \binom{m(x)}{j} \binom{d}{d-j} \binom{d+m(x)-j}{d} \leq (d+1) \cdot \binom{m(x)}{d} \binom{d}{d/2} \binom{d+m(x)}{d} = O(m(x)^d) = O(d^d)
\]

It would follow that a code of size \( |S_n| / (m(x)^d) \) exists (and, again, the capacity of these codes will be \( \text{cap}(S_n) \)).

It now suffices to show that except for a vanishingly small portion of \( y \in \mathbb{Z}_q^n \), it holds that \( m(R_k(y)) = \Theta(n) \). Indeed, recall that \( m(R_k(y)) = \text{wt}_H(\mu(b)) = \text{wt}_H(b) \), where \( \phi_k(y) = (a, b) \), \( b \in \mathbb{Z}_q^{-k} \). Then, for any real \( 0 < \xi < 1 - \frac{1}{q} \),

\[
\left\{ b \in \mathbb{Z}_q^{-k} \mid \text{wt}_H(b) \leq q^{n-k} \right\} \leq q^{(n-k)(H_q(\xi) - 1)},
\]

where \( H_q(\cdot) \) is the \( q \)-ary entropy function.

\[
H_q(\xi) \triangleq -\xi \log_q \xi - (1 - \xi) \log_q(1 - \xi) + \xi \log_q(q - 1),
\]

and where we used a standard bounding of the size on the Hamming ball, e.g., see [39, Lemma 4.7].
A. Comparison to recent results

Before we finish, we note here that the last argument also shows via the GV bound that error-correcting codes for a fixed number of tandem-duplications achieve capacity 1. Indeed, after the submission of this manuscript [27], [29] were made available, wherein bounds on the optimal size of such error-correcting codes were presented; these bounds show that the redundancy required to correct a fixed number of tandem-duplications is logarithmic in \( n \).

More specifically, both works showed (see [27, Thm. 4], [29, Lem. 6]) that there exist codes \( C^n \subseteq \mathbb{Z}_q^n \) that correct up to \( t \) tandem-duplications, for a fixed \( t \in \mathbb{N} \), satisfying
\[
\frac{q^n}{n^t} \left( \frac{q}{q-1} \right)^t \lesssim |C^n|
\]
(where we say that \( a_n \lesssim b_n \) if \( \limsup \frac{a_n}{b_n} \leq 1 \)). They also showed that the optimal size was \( \Theta \left( \frac{n^t}{q} \right) \). Finally, [27, Lem. 3] demonstrated that \( C^n \) can be assumed w.l.o.g. to only contain sequences which roots satisfy \( m(x) = \Theta(n) \).

We note that error-correcting codes for \( t \) tandem-duplications have minimal \( d_{\text{L, \cdot}}(\cdot, \cdot) \) distance \( t+1 \); In comparison, then, we have showed that \( (N, t, k)_q \)-UTR codes, where \( t \) is fixed and \( N = o(n) \), have minimal distance \( t \) (when restricted to descendant cones of irreducible words with \( m(x) = \Theta(n) \)). The observations above imply that codes designed in the aforementioned works for correcting \( t-1 \) tandem-duplications, of size \( \gtrsim \frac{q^n}{n^{t-1}} \left( \frac{q}{q-1} \right)^{t-1} \), are \( (N, t, k)_q \)-UTR codes. Importantly, this validates the hypothesis that reconstruction codes for data storage in the DNA of living organisms offer greater data-density than error-correcting codes. Namely, in comparison to the \( t \log(n)+O(1) \) redundancy achieved by optimal error-correcting codes in [27], [29], \( (N, t, k)_q \)-UTR codes achieve redundancy \( (t-1) \log(n)+O(1) \).

Finally, we also note for completeness that our results in Regime II, albeit less applicable in practice, are unique to this work.

V. Conclusion

We have proposed that reconstruction codes can be applied to data-storage in the DNA of living organisms, due to the channel’s inherent property of data replication.

We have showed, under the assumption of uniform tandem-duplication noise, that any reconstruction code is partitioned into error-correcting codes for the Manhattan metric over a simplex, with minimal distances dependent on the reconstruction parameters. We then proved the existence of reconstruction codes with rate 1, and suggested a construction of a family of codes, which relies on constructions of codes for the simplex. Via Theorem 25, we showed that we can bound the parameters required for code-design in any real application, to any degree of accuracy.

We believe that further research should examine explicit code constructions on the simplex; specifically, encoding and decoding algorithms for sufficiently large codes haven’t yet been developed; in addition, only specific asymptotic regimes have been explored, and a gap still exists between lower an upper bounds on the size of non-linear codes. It is also desirable to examine the problem under broader noise models, such as bounded tandem-duplication, interspersed-duplication (perhaps complemented), as well as combinations of multiple error models.

ACKNOWLEDGMENTS

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

REFERENCES


