Runlength-Limited Sequences and Shift-Correcting Codes: Asymptotic Analysis

Mladen Kovačević

Abstract—This work is motivated by the problem of error correction in bit-shift channels with the so-called \((d, k)\) input constraints (where successive 1’s are required to be separated by at least \(d\) and at most \(k\) zeros, \(0 \leq d < k \leq \infty\)). Bounds on the size of optimal \((d, k)\)-constrained codes correcting a fixed number of bit-shifts are derived, with a focus on their asymptotic behavior in the large block-length limit. The upper bound is obtained by a packing argument, while the lower bound follows from a construction based on a family of integer lattices. Several properties of \((d, k)\)-constrained sequences that may be of independent interest are established as well; in particular, the exponential growth-rate of the number of \((d, k)\)-constrained constant-weight sequences is characterized. The results are relevant for magnetic and optical information storage systems, reader-to-tag RFID channels, and other communication models where bit-shift errors are dominant and where \((d, k)\)-constrained sequences are used for modulation.

Index Terms—Runlength-limited sequence, constrained code, constant-weight code, bit-shift channel, peak shift, timing error, integer composition, Manhattan metric, asymmetric distance.

I. INTRODUCTION

SHIFT AND TIMING errors are a dominant type of noise in several communication and information storage scenarios, examples of which include magnetic and optical recording devices [13], [38], inductively coupled channels such as the reader-to-tag RFID channel [35], parallel asynchronous communications [9], various types of timing channels [2], [22], [53], etc. Designing codes that are able to correct these types of errors and studying their fundamental limits is important for all these applications, in addition to being an interesting theoretical challenge. The problem is further complicated by the fact that, in many of the mentioned applications, particularly magnetic, optical, and emerging DNA storage systems, the codewords are required to satisfy modulation constraints that are introduced to alleviate inter-symbol interference and other impairing effects [14]–[17], [39], [40]. Perhaps the best-known example of such constraints are runlength constraints where a minimum and a maximum number of zero symbols between two consecutive non-zero symbols is specified. Motivated by these communication settings, we study the error correction problem for channels with shift and timing errors, and with runlength input constraints. The precise channel model we have in mind and our contributions are described in the following two subsections.

Date: March 13, 2019.

The author was with the Department of Electrical & Computer Engineering, National University of Singapore, Singapore 117583. He is now with the BioSense Institute, University of Novi Sad, 21000 Novi Sad, Serbia (email: kmladen@uns.ac.rs).

This work was supported by the Singapore Ministry of Education (grant no. R-263-000-B61-112) and by the European Commission (H2020 Antares project, ref. no. 739570).

A. The Channel Model

Fix \(d, k \in \mathbb{Z} \cup \{\infty\}\) with \(0 \leq d < k \leq \infty\). We assume that the channel inputs are binary strings of length \(n\) that are composed of blocks from the set \(\{0^d1, \ldots, 0^k1\}\), where \(0^j\) is a string of \(j\) zeros. In other words, the set of inputs is

\[
S_{d,k}(n) := \{0,1\}^n \cap \{0^d1, \ldots, 0^k1\}^*.
\]

(1)

(Here \(A^*\) is the usual notation for the set \(\bigcup_{i=0}^{\infty} A^i\).) For a string \(x = x_1 \cdots x_n \in \{0,1\}^n\), denote by \(\text{wt}(x) = \sum_{i=1}^{n} x_i\) its Hamming weight. The set of all channel inputs of weight \(W\) is denoted by:

\[
S_{d,k}(n,W) := \{x \in S_{d,k}(n) : \text{wt}(x) = W\}.
\]

(2)

In other words, \(S_{d,k}(n,W)\) contains all strings of length \(n\) that are composed of exactly \(W\) blocks from the set \(\{0^d1, \ldots, 0^k1\}\).

The definition (1) ensures that (a) consecutive 1’s in any input string are separated by at least \(d\) and at most \(k\) zeros, and (b) every input string starts with a string of zeros of length \(j\), \(d \leq j \leq k\), and ends with a 1. The property (a) is the defining property of the so-called \((d, k)\)-constrained sequences. However, the boundary conditions (b) are not universally adopted in the literature [14]. We shall nevertheless find it convenient to work under definition (1), as in, e.g., [27]; it will be evident later on that different boundary conditions would not affect the analysis in any significant way.

For a given input string \(x \in S_{d,k}(n,W)\), the channel outputs another binary string \(y\) of length \(n\) and weight \(W\). We think of 1’s in \(x\) as being “shifted” in the channel, each for a number of positions to the left or to the right of its original position, thus producing \(y\) at the output. We say that \(t\) bit-shifts have occurred in the channel if \(\sum_{i=1}^{W} |\bar{x}_i - \bar{y}_i| = t\), where \(\bar{x}_i\) (resp. \(\bar{y}_i\)) is the position of the \(i\)'th 1 in \(x\) (resp. \(y\)).

1 \(\leq i \leq W\); see Example 1 for an illustration.

Example 1. Consider an input string \(x \in S_{2,4}(15, 4)\) and the corresponding output string \(y\):

\[
x = 0 0 1 0 0 0 0 1 0 0 1 0 0 0 1
\]

\[
y = 0 1 0 0 0 1 0 0 0 0 0 0 0 0 1 0 0 0 1
\]

(3)

We think of \(y\) as obtained from \(x\) by shifting the first 1 in \(x\) one position to the left, the second 1 two positions to the left, and the third 1 one position to the right. We then say that the total number of bit-shifts that occurred in the channel is \(t = 1 + 2 + 1 = 4\).

Note that the output string \(y\) may in general violate the \((d, k)\)-constraints.
B. Main Results

Our main object of study in the present paper are error-correcting codes for the above-described channel model. In particular, we shall derive explicit bounds on the cardinality of optimal \((d, k)\)-constrained codes correcting \(t\) shifts, with a focus on their asymptotic form in the regime of growing block-length \((n \to \infty)\). Despite a sizable body of literature on the bit-shift channel and related model, such bounds, to the best of our knowledge, have not been obtained before, even for a single bit-shift \((t = 1)\).

We consider two scenarios. The first one, analyzed in Section III, corresponds to the situation where shifts to the right (right-shifts) and shifts to the left (left-shifts) are treated independently, and separate requirements on their correctability are imposed. More precisely, codes are in this case required to have the capability of correcting \(t_+\) right-shifts and \(t_-\) left-shifts, for given \(t_+\) and \(t_-\). The second scenario, analyzed in Section IV, corresponds to the situation where right-shifts and left-shifts are treated in a symmetric way, i.e., where codes are required to have the capability of correcting \(t\) shifts, regardless of the direction of each individual shift. In both cases, a metric appropriate for characterizing the error-correcting capability of a code is given.

In Section III we state several properties of the code space \(S_{d, k}(n)\) that are needed to derive the bounds in Sections III and IV but are also of independent interest. In particular, we determine the capacity of the noiseless channel with \((d, k)\)-constrained constant-weight inputs, i.e., the exponential growth-rate of \(|S_{d, k}(n, w_n)|\) as \(n \to \infty\).

C. Notation

\(\log\) denotes the base-2 logarithm.

If we write \(\sum_i s_i\), it is understood that \(i\) ranges over all possible values, which will be clear from the context.

We adopt the following asymptotic notation: for any two non-negative real sequences \((a_n)\) and \((b_n)\),

- \(a_n \sim b_n\) means \(\lim_{n \to \infty} \frac{a_n}{b_n} = 1\);
- \(a_n \geq b_n\) means \(\liminf_{n \to \infty} \frac{a_n}{b_n} \geq 1\);
- \(a_n \sim b_n\) means \(\log a_n \sim \log b_n\) (i.e., the exponents of \(a_n\) and \(b_n\) have the same asymptotic behavior);
- \(a_n = O(b_n)\) means \(\sup_{n \to \infty} \frac{a_n}{b_n} < \infty\);
- \(a_n = o(b_n)\) means \(\lim_{n \to \infty} \frac{a_n}{b_n} = 0\).

II. THE SPACE OF \((d, k)\)-CONSTRAINED SEQUENCES

In this section we demonstrate some properties of the set \(S_{d, k}(n)\) that will be used in the derivations to follow but are also of potential interest in other applications. We also describe another representation of this space that is equivalent to the one given in (1)-(2) but that may be preferable to it, depending on the problem being analyzed.

A. Equivalent Representation

Another representation of the set of all channel inputs that is useful for analyzing bit-shift errors is based on specifying the positions of \(1\)'s in the input string [1].

For \(x \in S_{d, k}(n, W)\), we denote by \(\bar{x} = (\bar{x}_1, \ldots, \bar{x}_W)\) the vector indicating the positions of \(1\)'s in the string \(x\), meaning that \(\bar{x}_i\) is the position of the \(i\)th 1 in \(x\). For example, for \(x = 0100101 \in S_{1, 3}(7, 3)\) we have \(\bar{x} = (2, 5, 7)\). The mapping \(x \mapsto \bar{x}\) is clearly one-to-one. With this correspondence in mind, we define

\[
\bar{S}_{d, k}(n, W) := \{ \bar{x} \in \mathbb{Z}^W : 0 < \bar{x}_1 < \cdots < \bar{x}_W = n, \\
d + 1 \leq \bar{x}_i - \bar{x}_{i-1} \leq k + 1 \text{ for } i = 1, \ldots, W \},
\]

where it is understood that \(\bar{x}_0 = 0\). Hence, \(\bar{S}_{d, k}(n, W)\) is just a different representation of the set of all channel inputs of length \(n\) and weight \(W\), namely \(S_{d, k}(n, W)\), and \(\bar{S}_{d, k}(n) := \bigcup_W \bar{S}_{d, k}(n, W)\) is the corresponding representation of the set of all channel inputs of length \(n\), namely \(S_{d, k}(n)\). Note that \(\bar{S}_{d, k}(n, W)\) is a \((W - 1)\)-dimensional subset of \(\mathbb{Z}^W\) because the position of the last 1 in every input string is fixed to \(n\) by our convention [1], i.e.,

\[
\bar{S}_{d, k}(n, W) \subset \mathbb{Z}^{W-1} \times \{n\}.
\]

The space \(\bar{S}_{d, k}(n, W)\), or \(\bar{S}_{d, k}(n, W)\) in the constant-weight case, seems to be more convenient for describing constructions of codes for the bit-shift channel.

B. Combinatorial Description and Asymptotics

Define

\[
S_{d, k}(n) := |S_{d, k}(n)| = |\bar{S}_{d, k}(n)|, \\
S_{d, k}(n, W) := |S_{d, k}(n, W)| = |\bar{S}_{d, k}(n, W)|,
\]

and note that

\[
S_{d, k}(n, W) = \sum_{W=0}^{n} S_{d, k}(n, W). \tag{7}
\]

We see from the definition of the code space (1) that \(\bar{S}_{d, k}(n)\) is in fact the number of composition [1] of the integer \(n\) with parts restricted to the set \(\{d + 1, \ldots, k + 1\}\). This number can be expressed in the recursive form:

\[
S_{d, k}(n) = \sum_{i=d+1}^{k+1} S_{d, k}(n-i) \tag{8}
\]

with initial conditions \(S_{d, k}(0) = 1\) and \(S_{d, k}(n) = 0\) for \(n < 0\). As is well-known [43], this implies that \(S_{d, k}(n) \sim c\rho^{-n}\), where \(\rho\) is the unique positive solution [4] to the characteristic polynomial of an integer \(n\) is a tuple of positive integers (called parts) summing to \(n\) [42]. For a study of compositions with parts restricted to a subset of \(\mathbb{N}\) see, e.g., [13].

\[A\] A composition of an integer \(n\) is a tuple of positive integers (called parts) summing to \(n\) [42].
equation $\sum_{i=d+1}^{k+1} x^i = 1$, and the constant $c$ can be obtained from the recurrence (3) and its initial conditions.

Similarly, $S_{d,k}(n,W)$ is the number of compositions of the integer $n$ having exactly $W$ parts, each part belonging to the set $\{d+1, d+2, \ldots \}$. This quantity can be expressed in the recursive form [12]:

$$S_{d,k}(n,W) = \sum_{i=d+1}^{k+1} S_{d,k}(n-i,W-1)$$

with initial conditions $S_{d,k}(0,0) = 1$, $S_{d,k}(n,0) = 0$ for $n \neq 0$, and $S_{d,k}(n,W) = 0$ for $n < 0$. For $k = \infty$ one can obtain an explicit solution to (9) by directly counting the compositions of $n$ with parts in $\{d+1, d+2, \ldots \}$:

$$S_{d,\infty}(n,W) = \binom{n-1-Wd}{W-1}.$$  

In particular, $S_{0,\infty}(n,W) = \binom{n-1}{W-1}$ and $S_{0,\infty}(n) = 2^{n-1}$ (recall that the last bit of every sequence is fixed to 1 by our convention (1)). In the following lemma we characterize the asymptotic behavior of $S_{d,k}(n,W)$ as $n \to \infty$ and $W = wn$, for fixed $w \in (\frac{1}{k+1}, \frac{1}{d+1}]$. For simplicity, we write $wn$ instead of, e.g., $|wn|$, ignoring the fact that the former is not necessarily an integer.

For $w \in (\frac{1}{k+1}, \frac{1}{d+1}]$ define the function

$$\sigma_{d,k}(w) := w \log \sum_{i=d+1}^{k+1} \rho_w^i \frac{i}{w},$$

where $\rho_w$ is the unique positive solution to $\sum_{i=d+1}^{k+1} \left(1 - \frac{1}{w} \right)x^i = 0$. Additionally, let $\sigma_{d,k}(\frac{1}{k+1}) = \sigma_{d,k}(\frac{1}{d+1}) = 0$.

**Lemma 1.** (a) For any fixed $w \in (\frac{1}{k+1}, \frac{1}{d+1}]$, 

$$\lim_{n \to \infty} \frac{1}{n} \log S_{d,k}(n,wn) = \sigma_{d,k}(w).$$  

(b) The exponent $\sigma_{d,k}(w)$ is a continuous, strictly concave function of $w$. It attains its maximal value at

$$w^* = \left( \sum_{i=d+1}^{k+1} \rho_w^i \right)^{-1}$$

and this value is $\sigma_{d,k}(w^*) = - \log \rho$, where $\rho$ is the unique positive solution to $\sum_{i=d+1}^{k+1} x^i = 1$.

**Proof:** Part (a) of the claim, referring to the asymptotics of $S_{d,k}(n,wn)$ as $n \to \infty$, follows from the known results in analytic combinatorics [35]. Namely, the generating function of the bivariate sequence $(S_{d,k}(n,W))_{n,W}$ is obtained from (3) as:

$$F_{d,k}(x,y) := \sum_{n=0}^{\infty} \sum_{W=0}^{\infty} S_{d,k}(n,W)x^n y^W=$$

$$= \frac{1}{1 - y(x^{d+1} + \ldots + x^{k+1})}.$$  

wherefrom one verifies that this sequence is a Riordan array and satisfies the conditions of [35 Thm 12.2.2]. We then conclude from [35 Thm 12.2.2] that

$$S_{d,k}(n,wn) \sim v(\rho_w)^w \rho_w^{-n} = \left( \sum_{i=d+1}^{k+1} \rho_w^i \right)^{-n},$$  

where $v(x) := \sum_{i=d+1}^{k+1} x^i$ is the polynomial appearing in the denominator of the generating function (14), and $\rho_w$ is the unique positive solution to $\frac{\partial}{\partial w} v(\rho_w) = \frac{1}{w}$. This proves (12).

Part (b) of the claim is obtained by carefully analyzing the involved functions. The root $\rho_w$ is a function of the relative weight $w$ and is implicitly defined by $\sum_{i=d+1}^{k+1}(\frac{1}{w} - 1)\rho_w^i = 0$, $\rho_w > 0$. Differentiating this equation w.r.t. $w$ we find that $\frac{\partial}{\partial w} \rho_w < 0$. Also, we have $\frac{\partial}{\partial w} \sigma_{d,k}(w) = \log c \cdot \frac{\partial}{\partial w} \rho_w < 0$, implying that $\sigma_{d,k}(w)$ is concave. The weight $w^*$ that maximizes the exponent $\sigma_{d,k}(w)$ is the one for which $\frac{\partial}{\partial w} \sigma_{d,k}(w) = 0$, i.e., $v(\rho_w) = \sum_{i=d+1}^{k+1} \rho_w^i = 1$.

It is illustrative to specialize Lemma 1 to $k = \infty$ because this case admits an explicit solution. After a simple calculation we get $\rho_w = \frac{1-w(d+1)}{1-wd}$ and

$$\sigma_{d,\infty}(w) = (1-wd)H\left( \frac{w}{1-wd} \right),$$

where $H(\cdot)$ is the binary entropy function, which can also be found directly from (10) by using Stirling’s approximation.

The exponent (16) is maximized at $w^* = \frac{1}{1+1/p^d}$, where $p$ is the unique positive solution to $1 - x - x^{d+1} = 0$. Further specializing to $d = 0$, we recover the well-known fact that $\sigma_{0,\infty}(w) = H(w)$, in which case $p = 1/2$ and $w^* = 1/2$.

The quantity $\sigma_{d,k}(w)$ defined in (11) is the maximal information rate (i.e., the capacity) that can be achieved in the noiseless channel with $(d,k)$-constrained inputs of relative weight $w$. This is a refinement of the well-known result that states that the capacity of the noiseless channel with $(d,k)$-constrained inputs (but with no weight constraints) is $\lim_{n \to \infty} \frac{1}{n} \log S_{d,k}(n)$, $= - \log \rho$ [44]. Namely, it follows from (7) and the fact that the exponential growth-rate of $S_{d,k}(n,wn)$ is maximized for $w = w^*$ (Lemma 1) that $S_{d,k}(n) \sim S_{d,k}(n,w^n) \sim 2^{\sigma_{d,k}(w^n)} = 2^{n \log \rho}$. The following claim strengthens this result; it asserts that the input strings of weight (approximately) equal to $w^n$ account for most of the space $S_{d,k}(n)$. Informally, we say that the “typical” $(d,k)$-constrained strings have relative weight $w^*$.

**Lemma 2.** There exists a sublinear function $f(n) = o(n)$ such that, as $n \to \infty$,

$$\sum_{W:|W-w^n|<f(n)} S_{d,k}(n,W) \lesssim \frac{S_{d,k}(n)}{n^{\log n}}.$$  

Bivariate sequences with generating functions of the form $\frac{\phi(x)}{1-y^\rho x}$ are called (generalized) Riordan arrays [4].

4Lemmas 3 and 4 can also be expressed in the probabilistic language. Such a formulation is close in spirit to the statements about high-probability sets and typical sequences in information theory [8].

8The function $f$ may depend on the parameters $d,k$ as well; this is suppressed for notational simplicity.
Proof: Recall that (a) $S_{d,k}(n)$ grows exponentially with exponent $-\log \rho$, (b) $S_{d,k}(n,W)$ grows exponentially with exponent $\sigma_{d,k}(W)$ that is uniquely maximized at $w^*$, and (c) there are only linearly (in $n$) many possible weights $W$ (see (2)). These facts together imply that, for any given $\epsilon > 0$, the number of $(d,k)$-constrained strings of weight satisfying $|W - w^*n| > \epsilon n$ is exponential with an exponent strictly smaller than $-\log \rho$. More precisely, for every $\epsilon > 0$ there exists a (sufficiently small) $\gamma(\epsilon) > 0$ such that, as $n \to \infty$,

$$\sum_{W: |W - w^*n| > \epsilon n} S_{d,k}(n,W) \lesssim \frac{S_{d,k}(n)}{2^{\gamma(\epsilon)n}}. \quad (18)$$

This further implies that, for every $\epsilon > 0$ and large enough $n$,

$$\sum_{W: |W - w^*n| > \epsilon n} S_{d,k}(n,W) \lesssim \frac{S_{d,k}(n)}{n^{\log n}}. \quad (19)$$

Let $n_0(\epsilon)$ be the smallest positive integer such that (19) holds for all $n \geq n_0(\epsilon)$. Take an arbitrary sequence $(\epsilon_i)$ satisfying $1 = \epsilon_0 > \epsilon_1 > \epsilon_2 > \ldots$ and $\lim_{i\to\infty} \epsilon_i = 0$, and define the function:

$$f(n) := \epsilon_in, \quad n_0(\epsilon_i) \leq n < n_0(\epsilon_{i+1}). \quad (20)$$

It is now easy to verify that (19) and (20) imply (17). ■

The function $n^{\log n}$ in the statement of Lemma 2 can be replaced with an arbitrary sub-exponential function, but this choice is sufficient for our purposes. In particular, since $\frac{1}{\log n} = o\left(\frac{\epsilon}{n}^{\gamma(\epsilon)}\right)$ for any fixed $t$, Lemma 2 implies that one can, without loss of generality, disregard the non-typical input strings in the asymptotic analysis of optimal codes correcting $t$ shifts.

In the sequel, we shall also need an estimate of the number of blocks $0^1$, for fixed $j \in \{d, \ldots, k\}$, in typical input strings. For the purpose of formally stating this result, denote by $S_{d,j}^{(1)}(n,W,\ell)$ the number of input strings consisting of $W$ blocks from $\{0^1, \ldots, 0^k1\}$, exactly $\ell$ of which are $0^1$. Equivalently, $S_{d,j}^{(1)}(n,W,\ell)$ is the number of compositions of the integer $n$ having $W$ parts, each part taking value in $\{d+1, \ldots, k+1\}$, and exactly $\ell$ of the parts having value $j+1$. We then have $S_{d,j}(n,W) = \sum_{\ell=0}^{W} S_{d,j}^{(1)}(n,W,\ell)$, for every $j \in \{d, \ldots, k\}$.

Lemma 3. Fix $j \in \{d, \ldots, k\}$ and denote $\lambda^*_j := \rho^{j+1} w^* = \rho^{j+1} \left(\sum_{i=d+1}^{k} i \rho^i\right)^{-1}$, where $\rho$ is the unique positive solution to $\sum_{i=d+1}^{k} x^i = 1$. Then, for every $j \in \{d, \ldots, k\}$, as $n \to \infty$ we have

$$S_{d,j}(n) \sim S_{d,j}^{(1)}(n,w^*n,\lambda^*_j n). \quad (21)$$

Moreover, there exists a sublinear function $f(n) = o(n)$ such that, for every $j \in \{d, \ldots, k\}$, as $n \to \infty$ we have

$$S_{d,j}(n) - \sum_{W,\ell: |W - w^*n| \leq f(n)} S_{d,j}^{(1)}(n,W,\ell) \lesssim \frac{S_{d,k}(n)}{n^{\log n}}. \quad (22)$$

Proof: Let us consider $j = d$ and denote $\lambda := \lambda_d$ for simplicity; the proof for general $j$ is analogous. The following relation is valid:

$$S_{d,k}(n,W,\ell) = \left(\frac{W}{\ell}\right) S_{d+1,k}(n - \ell(d + 1), W - \ell) \quad (23)$$

for $\ell \geq 2$ and $\rho$ parts of value $d + 1$ can be distributed among the $W$ parts in $W^\ell$ ways, and the remaining $W - \ell$ parts, which are all from $\{d+2, \ldots, k+1\}$, form a composition of the number $n - \ell(d + 1)$, and therefore

$$S_{d,k}(n) = \sum_{W} \sum_{\ell} \left(\frac{W}{\ell}\right) S_{d+1,k}(n - \ell(d + 1), W - \ell). \quad (24)$$

Since the sum in (24) has polynomially many terms, we know that it grows exponentially with the same exponent as one of its summands $W = wn$, $\ell = \lambda n$, for some $w \in \left(\frac{1}{k+1}, \frac{1}{2}\right)$ and $\lambda \in (0, w)$. By using Stirling’s approximation and the previous result, this exponent can be expressed in the form

$$\lim_{n \to \infty} \frac{1}{\log n} \log \left[\left(\frac{wn}{\lambda n}\right) S_{d+1,k}(n - \lambda n(d + 1), (w - \lambda)n)\right] = w H(\frac{\lambda}{w}) + (w - \lambda) \log \sum_{i=d+2}^{k+1} \rho_i^{-1},$$

where $H(\cdot)$ is the binary entropy function and $\rho_{w,\lambda} > 0$ is a function implicitly defined by

$$\sum_{i=d+2}^{k+1} \left(1 - \frac{1 - \lambda(d + 1)}{w - \lambda}\right) \rho_i^i = 0. \quad (25b)$$

By calculating the derivatives of the exponent (the function on the right-hand side of (25a)) with respect to $w$ and $\lambda$, one finds that it is uniquely maximized for $\lambda^* = \rho^{k+1} w^* + (\sum_{i=d+1}^{k+1} i \rho^i)^{-1}$, where $\sum_{i=d+1}^{k+1} i \rho^i = 1$. This implies that

$$S_{d,k}(n) \sim S_{d,k}^{(1)}(n,w^*n,\lambda^* n). \quad (26)$$

and proves (21). It also implies that, for every $\epsilon > 0$, the part of the sum in (24) where $W \leq (w^* - \epsilon)n$ or $W \geq (w^* + \epsilon)n$ or $\ell \leq (\lambda^* - \epsilon)n$ or $\ell \geq (\lambda^* + \epsilon)n$ is exponentially smaller than the remaining part, from which we infer (22) by a reasoning identical to that in the proof of Lemma 2 (see (18)-(20)). ■

In words, $(d,k)$-constrained strings of length $n$ typically contain $\sim \lambda^*_j n$ blocks $0^1$, i.e., runs of zeros of length $j$, and all the non-typical strings can be safely ignored in the asymptotic analysis. Notice that, since $\sum_{i=d+1}^{k+1} i \rho^i = 1$, we have $\sum_{j=d}^{k} \lambda^*_j = w^*$, which is expected as $w^*$ is the total (typical) number of blocks in the input strings of length $n$.

For example, in the unconstrained case ($d = 0, k = \infty$) we have $\rho = 1/2$, $w^* = 1/2$, and $\lambda^*_j = 2^{-j+2}$ for $j \geq 0$. As a further illustration, numerical values of the quantities discussed in Lemmas 2 and 3 are listed in Table I for several archetypal $(d,k)$-constraints; see, e.g., [14, 15, 40] for applications of these and other $(d,k)$-constrained codes.

A run of zeros is a block of contiguous zeros of maximal length, i.e., such that it is delimited on both sides either by a 1, or by the end of the string.
We now turn to the analysis of the bit-shift channel with $(d,k)$-shifts and $t_-$ left-shifts if no two different codewords $\bar{x}, \bar{y} \in \mathcal{C}$ can produce the same output after being impaired with arbitrary patterns of $t_-$ or fewer right-shifts and $t_-$ or fewer left-shifts. In symbols, for every $\bar{x}, \bar{y} \in \mathcal{C}, \bar{x} \neq \bar{y}$, \(\text{wt}(\bar{x}) = \text{wt}(\bar{y}) = W\), and all noise vectors $\mathbf{f}, \mathbf{g} \in \mathbb{Z}^W$ with $\sum_i f_i^+ \leq t_-, \sum_i f_i^- \leq t_-, \sum_i g_i^+ \leq t_-, \sum_i g_i^- \leq t_-$, we have $\bar{x} + \mathbf{f} \neq \bar{y} + \mathbf{g}$. Such a code $\mathcal{C}$ is said to be optimal if there is no code $\mathcal{C}' \subseteq \mathcal{S}_{d,k}(n)$ which corrects $t_-$ right-shifts and $t_-$ left-shifts and satisfies $|\mathcal{C}'| > |\mathcal{C}|$.

Consider the following metric on $\mathcal{S}_{d,k}(n)$:

$$d_a(\bar{x}, \bar{y}) := \max\left\{ \sum_{i=1}^W (\bar{x}_i - \bar{y}_i)^+, \sum_{i=1}^W (\bar{x}_i - \bar{y}_i)^- \right\}.$$  \hspace{1cm} (27)

This distance is of importance in the theory of codes for asymmetric channels [18] (hence the subscript ‘a’). For vectors of different dimensions (corresponding to strings of different weights), $\bar{x} \in \mathcal{S}_{d,k}(n, W_1)$, $\bar{y} \in \mathcal{S}_{d,k}(n, W_2)$, $W_1 \neq W_2$, we define $d_a(\bar{x}, \bar{y}) = \infty$. The minimum distance of a code $\mathcal{C} \subseteq \mathcal{S}_{d,k}(n)$ with respect to the metric $d_a$ is denoted $d_a(\mathcal{C})$.

The following proposition gives a metric characterization of shift-correcting codes in the asymmetric setting.

**Proposition 5.** A code $\mathcal{C} \subseteq \mathcal{S}_{d,k}(n)$ can correct $t_-$ right-shifts and $t_-$ left-shifts if and only if $d_a(\mathcal{C}) > t_- + t_-$.

**Proof:** Suppose that $\mathcal{C}$ cannot correct $t_-$ right-shifts and $t_-$ left-shifts, i.e., that there exist two distinct codewords $\bar{x}$, $\bar{y}$ and two noise vectors $\mathbf{f}, \mathbf{g}$ with $\sum_i f_i^+ \leq t_-, \sum_i f_i^- \leq t_-, \sum_i g_i^+ \leq t_-, \sum_i g_i^- \leq t_-$, such that $\bar{x} + \mathbf{f} = \bar{y} + \mathbf{g}$, or equivalently, $\bar{x} + \mathbf{f}^+ + \mathbf{g}^- = \bar{y} + \mathbf{g}^+ + \mathbf{f}^-$. This implies that $d_a(\bar{x}, \bar{y}) \leq \max\{\sum_{i=1}^W (f_i^+ + g_i^-), \sum_{i=1}^W (g_i^+ + f_i^-)\} \leq t_- + t_-$, and so $d_a(\mathcal{C}) \leq t_- + t_-.$

The other direction is similar. Suppose that $d_a(\bar{x}, \bar{y}) \leq t_- + t_-$. For two distinct codewords $\bar{x}, \bar{y} \in \mathcal{C}$, and define $f = (\bar{y} - \bar{x})^+ = \max\{\bar{y} - \bar{x}, 0\}$ and $g = (\bar{x} - \bar{y})^+ = \max\{\bar{x} - \bar{y}, 0\}$. Then $\bar{x} + \mathbf{f} = \bar{y} + \mathbf{g}$ and $f_i, g_i \geq 0$, $\sum_{i=1}^W f_i \leq t_- + t_-$, $\sum_{i=1}^W g_i \leq t_- + t_-$. (the last two inequalities together are equivalent to our assumption that $d_a(\bar{x}, \bar{y}) \leq t_- + t_-$.)

We can then find non-negative vectors $\mathbf{f}', \mathbf{f}'', \mathbf{g}', \mathbf{g}''$ satisfying $\mathbf{f} = \mathbf{f}' + \mathbf{f}'', \mathbf{g} = \mathbf{g}' + \mathbf{g}''$, $\sum_i f_i^+ \leq t_-$, $\sum_i f_i^- \leq t_-$, $\sum_i g_i^+ \leq t_-$, $\sum_i g_i^- \leq t_-$, and write $\bar{x} + \mathbf{f}'' - \mathbf{f}' = \bar{y} + \mathbf{g}'' - \mathbf{g}'$. This means that $\mathcal{C}$ cannot correct $t_-$ right-shifts and $t_-$ left-shifts.

Therefore, the error-correcting capability of a code $\mathcal{C}$ depends on the parameters $t_-$ and $t_-$ only through their sum. In particular, $\mathcal{C}$ can correct $t_-$ right-shifts and $t_-$ left-shifts if and only if it can correct $t_- + t_-$ right-shifts (and 0 left-shifts).

Note that the metric space $(\mathcal{S}_{d,k}(n, W), d_a)$ is not uniform in the sense that balls in this space have varying sizes, i.e., the size of a ball of radius $r$ depends on its center. For that reason, when studying properties of codes in $(\mathcal{S}_{d,k}(n, W), d_a)$, it is sometimes more convenient to consider the unrestricted metric space $(\mathbb{Z}^W)^\forall, d_a)$ (see (5)) where this effect does not

| $(d,k)$ | $(0,2)$ | $(1,3)$ | $(1,7)$ | $(2,7)$ | $(2,10)$ |
|--------|--------|--------|--------|--------|--------|
| $\rho$  | 0.544  | 0.682  | 0.624  | 0.699  | 0.687  |
| $-\log \rho$ | 0.879  | 0.551  | 0.679  | 0.517  | 0.542  |
| $w^*$  | 0.618  | 0.363  | 0.295  | 0.221  | 0.205  |
| $\lambda_5^*$  | 0.336  | -      | -      | -      | -      |
| $\lambda_6^*$  | 0.183  | 0.169  | 0.115  | -      | -      |
| $\lambda_7^*$ | 0.099  | 0.115  | 0.072  | 0.075  | 0.066  |
| $\lambda_8^*$ | 0.078  | 0.045  | 0.053  | 0.046  | -      |
| $\lambda_9^*$ | 0.028  | 0.037  | 0.031  | -      | -      |
| $\lambda_{10}^*$ | -      | 0.017  | 0.026  | 0.022  | -      |
| $\lambda_{11}^*$ | -      | 0.011  | 0.018  | 0.015  | -      |
| $\lambda_{12}^*$ | -      | 0.007  | 0.013  | 0.010  | -      |
| $\lambda_{13}^*$ | -      | -      | -      | -      | 0.007  |
| $\lambda_{14}^*$ | -      | -      | -      | -      | -      |
| $\lambda_{15}^*$ | -      | -      | -      | -      | 0.005  |
| $\lambda_{16}^*$ | -      | -      | -      | -      | 0.003  |

**Table I:** The exponential growth-rate of the number of $(d,k)$-constrained strings ($-\log \rho$), and the typical values of the relative Hamming weight ($w^*$) and the relative numbers of runs of zeros of length $j$ ($\lambda_j^*$) in $(d,k)$-constrained strings of length $n \to \infty$ (rounded to three decimal places).
formally, so we give it here for completeness. A few definitions

The lower bound on $M_{d,k}(n,t)$ given in Theorem 7 below is obtained by constructing a family of codes in $(\tilde{S}_{d,k}(n,W),d_a)$, which in turn is done by using “good” codes in $(Z^{W-1},d_a)$, translating them to $(Z^{W-1} \times \{n\},d_a)$, and then restricting to $\tilde{S}_{d,k}(n,W)$. For that reason, a lower bound for codes in $(Z^{W-1},d_a)$ is given first (Lemma 6). This bound was essentially obtained in [23] but was not stated there formally, so we give it here for completeness. A few definitions are needed to state it precisely.

We say that $L \subseteq Z^m$ is a sublattice of $Z^m$ if $(L,+)$ is a subgroup of $(Z^m,+)$, the density of $L$ in $Z^m$ is defined as $\mu(L) := |Z^m/L|^{-1}$, where $Z^m/L$ is the quotient group of $L$, and represents the average number of lattice points from $(L)$ per one point of the ambient space $(Z^m)$. The quantity of interest to us in the present context is the maximum density a lattice $L \subseteq Z^m$ can have when its minimum distance is required to satisfy $d_a(L) > t$, namely

$$\mu_a(m,t) = \max \{ \mu(L) : L \subseteq Z^m, d_a(L) > t \} .$$

Lemma 6. For every $t \geq 1$, as $m \to \infty$ we have

$$\mu_a(m,1) \sim \frac{1}{m}, \quad \mu_a(m,2) \sim \frac{1}{m^2} .$$

Proof: It was shown in [23] Thm 7 that every sublattice $L \subseteq Z^m$ with $d_a(L) > t$ corresponds to a Sidon set of order $t$ and cardinality $m+1$ in an Abelian group, and vice versa. Consequently, the largest possible density of such a sublattice can be expressed as $\mu_a(m,t) = \frac{1}{\phi(m,t)}$, where $\phi(m,t)$ denotes the size of the smallest Abelian group containing a Sidon set of order $t$ and cardinality $m+1$. The relation (30) then follows from the Bose–Chowla construction of Sidon sets [4] which asserts that $\phi(m,t) \leq m^t + m^{t-1} + \cdots + 1$ when $m$ is a prime power.

For $t = 2$ and $m$ a prime power, the Bose–Chowla construction (obtained earlier by Singer [41]) is known to be optimal, meaning that $\phi(m,2) = m^2 + m + 1$. This, together with the obvious fact that $\phi(m,1) = m + 1$ for every $m$, implies (31).

Theorem 7. For every $t \geq 1$ and $d,k$ with $0 \leq d < k \leq \infty$, as $n \to \infty$ we have

$$M_{d,k}^2(n,t) \sim \frac{S_{d,k}(n)}{n^t} \left( \sum_{i=d+1}^{k+1} i \rho^i \right)^t ,$$

$$M_{d,k}^2(n,t) \sim \frac{S_{d,k}(n)}{n^t} \left( \sum_{i=d+1}^{k+1} i \rho^i \right)^t \frac{[t/2]! [t/2]!}{((1-\rho^{d+1})(1-\rho^{k+1}))^t} .$$

where $\rho$ is the unique positive solution to $\sum_{i=d+1}^{k+1} i \rho^i = 1$.

Proof: We first derive the lower bound (32a). Consider a class of codes in $\tilde{S}_{d,k}(n,W)$ obtained in the following way: Take a lattice $L \subseteq Z^{W-1}$ of minimum distance $d_a(L) = t+1$, and let $C_u := \{(u + L) \times \{n\}\}$ for an arbitrary $u \in Z^{W-1}$ (here $u + L = \{u + x : x \in L\}$). Clearly, the code $C_u$ has minimum distance $d_a(C_u) > t$. To give a lower bound on its cardinality notice that there are $|Z^{W-1}/L| = \mu(L)$ different translates $u + L$ that are disjoint and whose union is all of $Z^{W-1}$, so there exists at least one $u$ for which $|C_u| = 10$.
To see this, first count the number of strings that can be obtained by shifting \([t/2]\) 1’s one position to the right. In other words, pick \([t/2]\) out of \(W\) 1’s, and shift each of them one position to the right. Notice that not all such choices will result in a string that belongs to the code space \(S_{d,k}(n)\). Namely, right-shifting a 1 that (a) is preceded by exactly \(k\) zeros, or (b) is followed by exactly \(d\) zeros, or (c) is the last symbol in the string, would result in either a string that violates the \((d,k)\)-constraints, or is of length \(n+1\). Excluding the 1’s satisfying (a)-(c) leaves us with at least \(n\choose d\Lambda_{d,k} - 1\) 1’s to choose from, which gives the left-hand term in (38). The right-hand term is obtained in an analogous way by counting the number of strings that can be obtained after picking \([t/2]\) out of \(\Lambda_{d,k} - 1\)’s and shifting each of them one position to the left. The difference here is that, after choosing \([t/2]\) 1’s for the right-shifts in the first step, we exclude additional \(3[t/2]\) 1’s in the second step. Namely, if the \(i\)’th 1 has been chosen for the right-shift in the first step, then the \((i-1)\)’th, the \(i\)’th, and the \((i+1)\)’th 1 are excluded in the second step. 

\[
M_{d,k}^2(n,t) = \sum_{W} M_{d,k}^2(n,W,t) \geq \mu_{d,k} \cdot S_{d,k}(n,W) \geq \mu_{d,k} \cdot S_{d,k}(n,w^n(t)) \geq \frac{S_{d,k}(n,w^n(t))}{w^n(t)},
\]

where \(w^n\) is the optimizing weight given in Lemma 1, and \(f(n)\) is the sublinear function from Lemma 2. Here (35) follows from our code construction, (36) follows from Lemma 6 and (37) follows from Lemma 2 and the fact that \(f(n) = o(n)\).

We now turn to the derivation of the upper bound (32b).

Our approach is essentially a packing argument; however, due to the structure of the code space and the fact that balls in it do not have uniform sizes, some care is needed in making the argument work. Let \(C \subseteq S_{d,k}(n)\) be an optimal code correcting \([t/2]\) right-shifts and \([t/2]\) left-shifts, \(|C| = M_{d,k}^2(n,t)\) (see Proposition 3). Consider a codeword \(x \in C\) of weight \(W\), and let \(\Lambda_j\) (resp. \(\Lambda_{j,X}\)) denote the number of 1’s in \(x\) that are followed (resp. preceded) by exactly \(j\) zeros, and \(\Lambda_{X,j}\) (resp. \(\Lambda_{X,j,X}\)) the number of 1’s in \(x\) that are followed (resp. preceded) by a run of zeros whose length is not \(j\). Also, let \(\Lambda_{0,j}\) denote the number of 1’s in \(x\) that are preceded by exactly \(i\) zeros and followed by exactly \(j\) zeros; \(i \neq j\) the number of 1’s in \(x\) that are preceded by exactly \(i\) zeros and followed by a run of zeros whose length is not \(j\); and similarly for \(i \neq j\) and \(i \neq X\). We next show that the number of strings in \(S_{d,k}(n)\) that can be obtained after \(x\) is impaired by \([t/2]\) right-shifts and \([t/2]\) left-shifts is at least

\[
\left(\frac{n \Lambda_{X,0} - 1}{[t/2]} \right) \left(\frac{n \Lambda_{0,X} - 2t}{[t/2]} \right).
\]

This proves our claim that the expression in (38) is a lower bound on the number of strings in \(S_{d,k}(n)\) that \(x\) can produce after being impaired by \([t/2]\) right-shifts and \([t/2]\) left-shifts.

We next give the asymptotic form of (38), for fixed \(t\) and \(n \to \infty\), that will be needed to conclude the proof.

We know from Lemma 3 that, for the “typical” strings in \(S_{d,k}(n)\), \(W \sim w^n\) and \(\Lambda_j \sim \Lambda_{X,j} \sim \rho^{j+1} w^n, d \leq j \leq k\). This implies that a given block \(0^j\) is preceded by a block \(0^k\) with probability \(\sim \frac{w^n}{\rho^{j+1}}\), or in other words, of the \(\Lambda_j\) blocks \(0^j\), a fraction of \(\sim \rho^{j+1}\) is preceded by a block \(0^k\). It follows that, for the typical strings in \(S_{d,k}(n)\), \(\Lambda_{X,k} \sim w^n(1-\rho^{d+1})(1-\rho^{k+1})n\), and therefore the expression (38) has the following asymptotic form:

\[
\left(\frac{n \Lambda_{X,0} - 1}{[t/2]} \right) \left(\frac{n \Lambda_{0,X} - 2t}{[t/2]} \right) \sim \left(\frac{n \Lambda_{X,0} - 1}{[t/2]} \right) \left(\frac{n \Lambda_{0,X} - 2t}{[t/2]} \right) \sim \left(\frac{n \Lambda_{X,0} - 1}{[t/2]} \right) \left(\frac{n \Lambda_{0,X} - 2t}{[t/2]} \right),
\]

where we have used the fact that \(\frac{w^n}{\rho^{j+1}} \sim \frac{n \Lambda_{X,j} - m}{w^n}\) for fixed \(m\) and \(n \to \infty\).

Finally, due to our assumption that \(C\) corrects \([t/2]\) right-shifts and \([t/2]\) left-shifts, the sets of outputs that can be obtained in the above-described way from any two different codewords \(x, y \in C\) have to be disjoint. This implies that

\[
M_{d,k}^2(n,t) \cdot \left(\frac{n \Lambda_{X,0} - 1}{[t/2]} \right) \left(\frac{n \Lambda_{0,X} - 2t}{[t/2]} \right) \leq M_{d,k}^2(n,\rho\Lambda) \leq S_{d,k}(n) \quad \text{for fixed } m\text{ and } n \to \infty.
\]

\[
M_{d,k}^2(n,t) \sim \left(\frac{n \Lambda_{X,0} - 1}{[t/2]} \right) \left(\frac{n \Lambda_{0,X} - 2t}{[t/2]} \right) \sim \left(\frac{n \Lambda_{X,j} - m}{[t/2]} \right) \left(\frac{n \Lambda_{X,j,X} - 2t}{[t/2]} \right)
\]

proves the upper bound in (32b). We have used in (40) the fact that in the asymptotic analysis we can safely ignore the non-typical inputs (see Lemma 3), as we did in the derivation of the lower bound as well.

**Corollary 8.** For every \(t \geq 1\) and \(d, k\) with \(0 \leq d < k \leq \infty\), as \(n \to \infty\) we have

\[
\log M_{d,k}^2(n,t) = -\log \rho - t \log n + \mathcal{O}(1),
\]

where \(\rho\) is the unique positive solution to \(\sum_{i=d+1}^{k+1} \rho^i = 1\).

**Proof:** The statement follows from Theorem 2 and the fact that \(S_{d,k}(n) \sim cn^{-\rho^{-n}},\) for a constant \(c\).

For example, in the unconstrained case \((d = 0, k = \infty)\) we have \(S_{0,\infty}(n) = \binom{n}{2^{n-1}}, \rho = 1/2\), and the bounds (32) reduce to:

\[
\frac{2^{n-1}}{n^2} \leq M_{0,\infty}^2(n,t) \leq \frac{2^{n-1}}{n^2} 4^{[t/2]![t/2]}.
\]

To conclude this section, we note that the bounds (32) would continue to hold if we had adopted different boundary
conditions in the definition of \((d,k)\)-sequences \([1]\), because these conditions do not affect the typical values \(w^*\) and \(\lambda^*_j\) (see Remark 4). Of course, in that case, \(S_{d,k}(n)\) in \([32]\) would represent the cardinality of the corresponding code space, not the cardinality of the code space considered in this paper (see \([8]\)). For example, if we do not require the last bit to be 1, the bounds for the unconstrained case would be the same as those in \([42]\), with \(2^{n−1}\) replaced by \(2^n\).

More generally, our construction and method of deriving the bounds can be used for the bit-shift channel with other types of input constraints—a code would be constructed by intersecting the code space with a translated lattice having the desired minimum distance, and the upper bound would be derived by an analogous packing argument. Note that, to state the resulting bounds explicitly, the typical values \(w^*\) and \(\lambda^*_j\) would first have to be determined for the constraint in question. Still more generally, the same approach can be used in some other weight-preserving channels as well, such as the channel with insertions and deletions of blocks of zeros \([26]\), \([31]\).

### IV. Codes Correcting Symmetric Shifts

In this section we discuss a slightly different scenario—the one which is usually considered in the literature on bit-shift channels—where left-shifts and right-shifts are treated in a symmetric way. Our object of study are codes that enable the receiver to reconstruct the transmitted string whenever the total shift of its 1’s does not exceed a specified threshold, regardless of the direction of each individual shift.

#### A. Geometric Characterization

Suppose that \(\bar{x} \in \bar{S}_{d,k}(n)\) is the transmitted codeword, and \(z\) the corresponding received vector. If the 1’s in \(\bar{x}\) have been shifted by \(t\) positions in total, then \(\sum_{i=1}^W |z_i - \bar{x}_i| = t\).

We say that a code \(\bar{C} \subseteq \bar{S}_{d,k}(n)\) can correct \(t\) shifts if no two different codewords \(\bar{x}, \bar{y} \in \bar{C}\) can produce the same output after being impaired with arbitrary patterns of \(t\) or fewer shifts. In symbols, for every \(\bar{x}, \bar{y} \in \bar{C}\), \(\bar{x} \neq \bar{y}\), \(\text{wt}(x) = \text{wt}(y) = W\), and all noise vectors \(f, g \in \mathbb{Z}^W\) with \(\sum_{i=1}^W |f_i| \leq t\), \(\sum_{i=1}^W |g_i| \leq t\), we have \(\bar{x} + f \neq \bar{y} + g\).

Such a code \(\bar{C}\) is said to be optimal if there is no other code \(\bar{C}' \subseteq \bar{S}_{d,k}(n)\) correcting \(t\) shifts and such that \(|\bar{C}'| > |\bar{C}|\).

Let \(d_\alpha\) denote the Manhattan distance on \(\bar{S}_{d,k}(n,W)\):

\[
d_\alpha(\bar{x}, \bar{y}) := \sum_{i=1}^W |\bar{x}_i - \bar{y}_i|.\]

For vectors of different dimensions (corresponding to strings of different weights), \(\bar{x} \in \bar{S}_{d,k}(n,W_1)\), \(\bar{y} \in \bar{S}_{d,k}(n,W_2)\), \(W_1 \neq W_2\), we set \(d_\alpha(\bar{x}, \bar{y}) = \infty\). The minimum distance of a code \(\bar{C} \subseteq \bar{S}_{d,k}(n)\) with respect to the metric \(d_\alpha\) is denoted \(d_\alpha(\bar{C})\). The metric space \((\bar{S}_{d,k}(n,W), d_\alpha)\) and a code in this space are illustrated in Figure 2 for specific values of the parameters \(d, k, n, W\).

The following proposition gives a metric characterization of shift-correcting codes in the symmetric setting. It was first stated in \([20]\) Thm 1 (in a more general form) but is also implicit in some of the earlier works, e.g., \([1]\).

**Proposition 9.** A code \(\bar{C} \subseteq \bar{S}_{d,k}(n)\) can correct \(t\) shifts if and only if \(d_\alpha(\bar{C}) > 2t\).

Again, the space \((\bar{S}_{d,k}(n,W), d_\alpha)\) is not uniform in the sense that ball sizes depend on the locations of their centers. In the unrestricted space \((\mathbb{Z}^{W−1}, d_\alpha)\) this effect does not occur and we have the following expression for the cardinality of a ball of radius \(r\) in \((\mathbb{Z}^m, d_\alpha)\) \([11]\):

\[
B_\alpha(m, r) = \sum_i 2^i \binom{m}{i} \binom{r}{i}. \tag{44}
\]

The cardinality of an arbitrary ball of radius \(r\) in \((\bar{S}_{d,k}(n,W), d_\alpha)\) is upper bounded by \(B_\alpha(W−1, r)\).

#### B. Construction and Bounds

Let \(M_{d,k}(n; t)\) (resp. \(M_{d,k}(n,W; t)\)) denote the cardinality of an optimal code in \(\bar{S}_{d,k}(n)\) (resp. \(\bar{S}_{d,k}(n,W)\)) correcting \(t\) shifts, or equivalently, having minimum distance larger than \(2t\) with respect to the metric \(d_\alpha\). Since the channel does not affect the weight of the transmitted string, we have \(M_{d,k}(n; t) = \sum_w M_{d,k}(n,W; t)\).

In analogy with \([29]\) we define the maximum density a lattice \(\mathcal{L} \subseteq \mathbb{Z}^m\) with \(d_\alpha(\mathcal{L}) > 2t\) can have as

\[
\mu_\alpha(m, t) := \max \left\{ \mu(\mathcal{L}) : \mathcal{L} \subseteq \mathbb{Z}^m \text{ a lattice, } d_\alpha(\mathcal{L}) > 2t \right\}. \tag{45}
\]

**Lemma 10.** For every \(t \geq 1\), as \(m \to \infty\) we have

\[
\mu_\alpha(m, t) \gtrsim \frac{c(t)}{m^t}, \tag{46}
\]
where
\[ c(t) := \begin{cases} \frac{1}{2t}, & t \leq 2 \\ \frac{1}{2t+1}, & t \geq 3 \end{cases}. \] (47)

For \( t = 1 \) this lower bound is tight, i.e.,
\[ \mu_s(m,1) \geq \frac{1}{2m} \] (48)

Proof: Consider the so-called \( A_{m-1} \) lattice defined by \( A_{m-1} := \{ (u_1, \ldots, u_m) \in \mathbb{Z}^m : \sum_{i=1}^m u_i = 0 \} \), and let \( L_0 \) be the densest sublattice of \( A_{m-1} \) satisfying \( d_s(L_0) > 2t \). By [23] Thm 4, the metric space \( (A_{m-1}, d_s) \) is isometric to \( (\mathbb{Z}^m, 2d_s) \), so the density of \( L_0 \) in \( A_{m-1} \) can be expressed as \( \mu(L_0) = |A_{m-1}/L_0| = \mu_s(m-1,t) \), which, together with Lemma 6, implies that \( \mu_s(m,t) \geq 1 - \frac{2}{2m}m^{-t} \).

The lower bound just given can be improved for \( t = 1, 2 \) to \( \mu_s(m,t) \geq \frac{1}{m} \). In fact, for \( t \) the optimal density is known exactly for every \( m \); \( \mu_s(m,1) = \frac{1}{2m+1} \). This follows from the existence of perfect codes of radius 1 in \( (\mathbb{Z}^m, d_s) \) [11]. For \( t = 2 \) (or, indeed, for any \( t \)), one can construct codes in \( (\mathbb{Z}^m, d_s) \) by periodically extending codes in the torus \( \mathbb{Z}_n^m \) correcting \( t \) errors in the Lee metric [7] (here \( \mathbb{Z}_n^m := \mathbb{Z}/(n\mathbb{Z}) \)). Such a periodic extension of Berlekamp’s codes for the Lee metric [3, Ch. 9] gives \( \mu_s(m,2) \geq \frac{1}{4}m^{-2} \). ■

Theorem 11. For every \( t \geq 1 \) and \( d, k \) with \( 0 \leq d < k \leq \infty \), as \( n \to \infty \) we have
\[ M_{d,k}(n; t) \geq \sup_{n=t+1}^{k+1} \left( \frac{k}{2n+1} \right)^t c(t), \] (49a)
\[ M_{d,k}(n; t) \leq \sup_{n=t+1}^{k+1} \left( \frac{k}{2n+1} \right)^t \left( \frac{t!}{(1-\rho^{d+1})(1-\rho^{k+1})} \right)^t, \] (49b)
where \( c(t) \) is defined in (47) and \( \rho \) is the unique positive solution to \( \sum_{i=1}^{k+1} x_i^t = 1 \).

Proof: The proof is analogous to the proof of Theorem 7 for the asymmetric case; the only difference in proving the lower bound (49a) is that we need to use the metric instead of \( d_s \) (see Proposition 9). Following the same steps as in (35)–(37) we get \( M_{d,k}(n; t) \geq \mu_s(w^n, n, t) \cdot S_d,k(n) \), and then the result follows by applying Lemma 10.

Now for the upper bound (49b). Let \( C \subseteq S_{d,k}(n) \) be an optimal code correcting \( t \) shifts. \( |C| = M_{d,k}(n; t) \), and consider a codeword \( x \in C \). Every pattern of \( t \) shifts that can impair \( x \) in the channel consists of \( r \) right-shifts and \( t-r \) left-shifts, for some \( r \in \{0, 1, \ldots, t\} \). By a reasoning identical to that used in the proof of Theorem 7 we then conclude that the number of strings in \( S_{d,k}(n) \) that can be produced after \( x \) is impaired by \( t \) shifts is at least
\[ \sum_{r=0}^{t} {\binom{t}{r}} (\#d \Lambda_{d,k} - r - 1) \] (50)
(see equation (38) and the paragraph following it). Recalling that \( \#d \Lambda_{d,k} \approx \#d \Lambda_{d,k} \approx w^*(1 - \rho^{d+1})(1 - \rho^{k+1})n \) as \( n \to \infty \), we find the asymptotics of the expression (50) in the form:
\[ \approx \sum_{r=0}^{t} \frac{t!}{r!} (\#d \Lambda_{d,k} - r - 1) \] (51)
\[ \approx \frac{t!}{t!} (w^*(1 - \rho^{d+1})(1 - \rho^{k+1}))^t. \]
Since \( C \) corrects \( t \) shifts by assumption, we must have
\[ M_{d,k}(n; t) \geq \sup_{n=t+1}^{k+1} \left( \frac{k}{2n+1} \right)^t (w^*(1 - \rho^{d+1})(1 - \rho^{k+1}))^t n^t \leq S_{d,k}(n), \] (52)
which is equivalent to (49b). ■

Corollary 12. For every \( t \geq 1 \) and \( d, k \) with \( 0 \leq d < k \leq \infty \), as \( n \to \infty \) we have
\[ \log M_{d,k}(n; t) = -n \log \rho - t \log n + O(1), \] (53)
where \( \rho \) is the unique positive solution to \( \sum_{i=1}^{k+1} x_i^t = 1 \). ■

In the unconstrained case \( (d = 0, k = \infty) \) we have \( S_{0,\infty}(n) = 2n-1 \), \( \rho = 1/2 \), and the bounds (49) reduce to:
\[ \frac{2n-1}{n^t} 2^t c(t) \leq \log M_{0,\infty}(n; t) \leq \frac{2n-1}{n^t} 2^t t!. \] (54)
Similarly as in the asymmetric case, the bounds (49) would continue to hold if we had adopted different boundary conditions in the definition of \( (d, k) \)-sequences (1), because these conditions do not affect the typical values \( w^* \) and \( \lambda_i^* \) (see Remark 3). For example, if one does not fix the value of the last bit, the bounds for the unconstrained case would be the same as those in (54), with \( 2n-1 \) replaced by \( 2^n \).

V. CONCLUDING REMARKS
We conclude the paper with a few remarks on error models related to those we have studied here.

In some applications it is reasonable to assume that the shifts are limited in the sense that each \( 1 \) in an input string \( x \) can be shifted by at most \( s \) positions [11, 27, 31]. More precisely, if \( \tilde{x} \) is the transmitted vector and \( x \) the received vector, the assumption here is that \( |z_i - \tilde{x}_i| \leq s, 1 \leq i \leq n \). For such models, the lower bound on the cardinality of optimal shift-correcting codes can possibly be improved by using the known constructions of codes for limited-magnitude errors; see, e.g., [6]. For example, in the asymmetric case with \( t_+ + t_- = 2 \), \( s = 1 \), the lower bound in (32a) can be improved by a factor of 2 by using a construction of codes correcting 2 asymmetric 1-limited-magnitude errors [6] Sec. IV.C). Note that we have implicitly used the assumption that \( s = 1 \) in our derivation of the upper bounds (32b) and (39b). Therefore, the upper

---

11To the best of our knowledge, no known construction of codes in the Lee metric gives a lower bound on the density \( \mu_s(m,t) \) better than the one stated in (49a) except for \( t = 1, 2 \). For example, Berlekamp’s construction [3, Ch. 9] (see also [7]) gives \( \mu_s(m,t) \geq 2^{-\frac{m}{2}}-m^{-t} \), and the BCH-like construction of Roth and Siegel [27] gives \( \mu_s(m,t) \geq p_{2t+3} \), where \( p_{2t+3} \) is the smallest prime greater than or equal to \( 2t + 3 \).
bounds are not likely to be improved in limited-shift models by using the approach we have used.

In this context one may also be interested in codes correcting all possible patterns of shifts such that each shift is bounded by $s$. Such (zero-error) codes have been studied in several related settings: bit-shift channels, timing channels, skew-tolerant parallel asynchronous communications, etc. In many cases, the optimal codes have been found and the zero-error capacity of the corresponding channel determined.

ACKNOWLEDGMENT

The author would like to thank Vincent Y. F. Tan (NUS), for his detailed reading and helpful comments on a preliminary version of this work; Mehul Motani (NUS), for several discussions on a model related to the one studied in this paper; Anshoo Tandon (NUS), for the many helpful discussions on constrained codes and related notions; and the three anonymous referees, whose detailed comments and corrections have substantially improved the manuscript.

REFERENCES

[1] K. A. S. Abdel-Ghaffar and J. H. Weber, “Bounds and Constructions for Run-length-Limited Error-Control Block Codes,” IEEE Trans. Inform. Theory, vol. 37, no. 3, pp. 789–800, 1991.

[2] V. Anantharam and S. Verdú, “Bits Through Queues,” IEEE Trans. Inform. Theory, vol. 42, no. 1, pp. 4–18, 1996.

[3] E. R. Berlekamp, Algebraic Coding Theory, revised edition, World Scientific, Singapore, 2015.

[4] R. C. Bose and S. Chowla, “Theorems in the Additive Theory of Numbers,” Comment. Math. Helv., vol. 37, no. 1, pp. 141–147, 1962.

[5] P. A. H. Bours, “Construction of Fixed-Length Insertion/Deletion Correcting Run-length-Limited Codes,” IEEE Trans. Inform. Theory, vol. 40, no. 6, pp. 1841–1856, 1994.

[6] Y. Cassuto, M. Schwartz, V. Bohossian, and J. Bruck, “Codes for Asymmetric Limited-Magnitude Errors With Application to Multilevel Flash Memories,” IEEE Trans. Inform. Theory, vol. 56, no. 4, pp. 1582–1595, 2010.

[7] J. C. Chiang and J. K. Wolf, “On Channels and Codes for the Lee Metric,” Inform. and Control, vol. 19, no. 2, pp. 159–173, 1971.

[8] T. M. Cover and J. A. Thomas, Elements of Information Theory, 2nd ed., John Wiley & Sons, Inc., Hoboken, New Jersey, 2006.

[9] S. Engelberg and O. Keren, “Reliable Communications Across Parallel Asynchronous Channels With Arbitrary Skews,” IEEE Trans. Inform. Theory, vol. 63, no. 2, pp. 1120–1129, 2017.

[10] H. C. Ferreira and S. Lin, “Error and Erasure Control (d, k) Block Codes,” IEEE Trans. Inform. Theory, vol. 37, no. 5, pp. 1399–1408, 1991.

[11] S. W. Golomb and L. R. Welch, “Perfect Codes in the Lee Metric and the Packing of Polyominos,” SIAM J. Appl. Math., vol. 18, no. 2, pp. 302–317, 1970.

[12] S. Heubach and T. Mansour, “Compositions of $n$ with Parts in a Set,” Congr. Numer., vol. 168, pp. 127–143, 2004.

[13] H. M. Hilden, D. G. Howe, and E. J. Weldon, Jr., “Shift Error Correcting Modulation Codes,” IEEE Trans. Magn., vol. 27, no. 6, pp. 4600–4605, 1991.

[14] K. A. S. Immink, “Run-length-Limited Sequences,” Proc. IEEE, vol. 78, no. 11, pp. 1745–1759, 1990.

[15] K. A. S. Immink, P. H. Siegel, and J. K. Wolf, “Codes for Digital Recorders,” IEEE Trans. Inform. Theory, vol. 44, no. 6, pp. 2260–2299, 1998.

[16] K. A. S. Immink, Codes for Mass Data Storage Systems, 2nd ed., Shannon Foundation Publishers, Eindhoven, The Netherlands, 2004.

[17] K. A. S. Immink and K. Cai, “Design of Capacity-Approaching Constrained Codes for DNA-Based Storage Systems,” IEEE Commun. Lett., vol. 22, no. 2, pp. 224–227, 2018.

[18] T. Kløve, “Error Correcting Codes for the Asymmetric Channel,” Technical Report, Dept. of Informatics, University of Bergen, 1981. (Updated in 1995.)