This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIT.2019.2919632, IEEE Transactions on Information Theory

Online codes for analog signals

Leonard J. Schulman, Piyush Srivastava

***Abstract*—This paper revisits a classical scenario in communication theory: a waveform sampled at regular intervals is to be encoded so as to minimize distortion in its reconstruction, despite noise. This transformation must be online (causal), to enable real-time signaling; and should use no more power than the original signal. The noise model we consider is an "atomic norm" convex relaxation of the standard (discrete alphabet) Hamming-weight-bounded model: namely, adversarial ℓ_1-bounded. In the "block coding" (noncausal) setting, such encoding is possible due to the existence of large almost-Euclidean sections in ℓ_1 spaces, a notion first studied in the work of Dvoretzky in 1961. Our main result is that an analogous result is achievable even causally. Equivalently, our work may be seen as a "lower triangular" version of ℓ_1 Dvoretzky theorems. In terms of communication, the guarantees are expressed in terms of certain time-weighted norms: the time-weighted ℓ_2 norm imposed on the decoder forces increasingly accurate reconstruction of the distant past signal, while the time-weighted ℓ_1 norm on the noise ensures vanishing interference from distant past noise. Encoding is linear (hence easy to implement in analog hardware). Decoding is performed by an LP analogous to those used in compressed sensing.**

Keywords: ***Online coding, Dvoretzky theorems, Analog signals, Random matrices.***

I. Introduction

A. The problem

We study a fundamental scenario of communication theory. A source is generating a waveform which we sample at regular intervals. We wish to encode the signal in real time, and decode the noise-affected transmission in real time, all while minimizing distortion in the reconstruction.

We require that the power (the $\|\cdot\|_2$ norm) of the transmission $\mathcal{E}(x)$ not exceed a constant factor of the power of the signal x; for simplicity of operation, we also wish the encoding map $\mathcal{E}$ to be linear and deterministic. We operate in a worst-case model, namely, the adversary has advance knowledge of the signal and its encoding. Furthermore, at a minimum, we wish to have the following kind of decoding guarantee: for any signal $x : \mathbb{N} \to \mathbb{R}$, and any bounded-power adversary noise $y : \mathbb{N} \to \mathbb{R}$ (i.e., $\|y\|_2 < \infty$), the "limiting decoding" $\mathcal{D}(\mathcal{E}(x) + y)$ should equal x.

Actually, much of our effort will be devoted to stronger results quantifying the rate with which the decoder can eliminate noise. For this we must examine more closely the strength of the adversary. A conventional approach in analog communications would be to allow noise y such that $\|y\|_2$ is small compared with $\|x\|_2$. This is indeed the standard framework in analog communication in which one first source-codes the signal using vector quantization, then channel-codes the now discrete signal using a finite alphabet, which, in turn, is encoded with a waveform. We would like, however to allow noise of comparable power to the signal, $\|y\|_2 \leq O(\|x\|_2)$, and even beyond.

It is immediately apparent, however, is that this kind of $\|\cdot\|_2$-bounded adversary is too powerful for the problem we consider: the adversary can assign $y = -\mathcal{E}(x)$ and simply zero-out the transmission.

However, a power constraint is only one plausible assumption on the noise source. The goal of our work is to show that if instead of the power constraint on the adversary, we make a different but very familiar assumption, we can provide an entirely different approach to this communication problem.

In our setting, where the noise is generated by an adversary, an alternative modeling assumption for noise is one that has proven fruitful as a model for *signals* in the compressed sensing literature: it is that the signal is bounded in (a possibly weighted) $\|\cdot\|_1$ norm. An $\|\cdot\|_1$ norm bound (for a signal of given power) is a kind of sparsity assumption, and sparsity is a natural characteristic of many signal sources, which is in large part why this approach has succeeded in compressed sensing [1]. It is therefore natural to pose the problem of protecting our signal against interference by sparse signals generated by an adversary. Indeed, in the context of digital error-correcting codes, the most basic and prevalent model has long been of noise limited in Hamming norm, which is precisely a sparsity assumption. Relaxations of such

Leonard J. Schulman, California Institute of Technology. Email: schulman@caltech.edu.

Piyush Srivastava, Tata Institute of Fundamental Research. Email: piyush.srivastava@tifr.res.in.

Work supported in part by: United States NSF grants 1319745 and 1618795; a Ramanujan Fellowship for the second author from SERB, Indian Department of Science and Technology; and a residency for the first author at the Israel Institute for Advanced Studies, supported by a EURIAS Senior Fellowship co-funded by the Marie Skłodowska-Curie Actions under the 7th Framework Programme.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIT.2019.2919632, IEEE Transactions on Information Theory

combinatorial sparsity assumptions to convex norms such as $\|\cdot\|_1$ are also used to make them amenable to convex programming formulations [2].

Methodologically, the approach of considering adversaries bounded in the same norm as the signal has a fundamental limitation: no deterministic coding method can recover the signal to accuracy better than the signal-to-noise ratio. On the other hand, focusing on an adversary bounded in a different norm than the signal (here $\|\cdot\|_1$ rather than $\|\cdot\|_2$) opens the possibility of achieving in the limit noise-free decoding. That, as well as convergence rates to this limit, is the contribution of this paper: power-limited, real-time communications against an $\|\cdot\|_1$-bounded adversary.[1]

B. An easier problem: block coding

Undoubtedly, as for any error-correction problem, the most basic problem which one must consider here is that of *block coding* a signal. That is, the incoming signal is a vector $x \in \mathbb{R}^T$. We transmit at rate $1/\rho$, that is, we map x to $\mathcal{E}(x) \in \mathbb{R}^{\rho T}$. Our first constraint on the encoder is an *energy constraint*. If the encoder could amplify the signal by an arbitrarily large factor, then it could swamp out any interference by an adversary who is bounded in power or any other norm. Since this is an unrealistic (and uninteresting) model for the encoder, we stipulate that the total power of the transmission should be comparable to the total power of the original message itself. That is, we ask that

$$\left\|\mathcal{E}(x)_{[\rho t]}\right\|_2 \leq \left\|x_{[t]}\right\|_2, \text{ for all } t \in [T]. \qquad (*)$$

(Here $*_{[t]}$ denotes the prefix of a vector consisting of its first t co-ordinates.) The noise source adds a vector $y \in \mathbb{R}^{T\rho}$ onto $\mathcal{E}(x)$; the noise y may depend upon $\mathcal{E}(x)$. The receiver then applies a decoding map $\mathcal{D}(\mathcal{E}(x) + y)$. The question is then what can be achieved in terms of simultaneously

- Maximizing communication rate (minimizing ρ),
- Minimizing distortion relative to noise, i.e., minimizing the ratio $\frac{\|\mathcal{D}(\mathcal{E}(x)+y)-x\|_2}{\|y\|_1}$

As we discuss in more detail below, the answer to this question, although not posed in this language, was given long ago in the work of Milman [3], Kašin [4], and Figiel, Lindenstrauss and Milman [5], pursuing the study initiated by Dvoretzky [6] of Euclidean sections in Banach spaces. Further, the codes so achieved are *linear*: the encoding operation consists of multiplying the source vector by an appropriate $\rho T \times T$ matrix A, and the distortion ratio achieved is $O(T^{-1/2})$ (see discussion leading to eq. (8) below):

$$\|\mathcal{D}(\mathcal{E}(x) + y) - x\|_2 \leq O(T^{-1/2}) \|y\|_1 . \qquad (1)$$

In contrast, our object of study in this paper is the *real-time* or *causal* encoding and decoding of a source generated on the fly, as for instance an audio signal, or the signal from a remote sensor, in a distributed control setting. While the guarantees achieved in the offline (block coding) setting do serve as a guideline for framing what might be achievable in online coding, it will be clear from later discussions that not everything achievable offline can be achieved in the online setting.

We now proceed to formulate the appropriate requirements for the online setting. The *encoder* $\mathcal{E}$ is required to be such that the transmissions $1, \ldots, \rho t$ can depend only on the prefix $x_{[t]}$ of the message that is available to the source at time t: in other words, $\rho \geq 1$ symbols are sent for each symbol of the message, in a way such that these ρ symbols depend only on the prefix $x_{[t]}$ of the message available at time t. In particular this enforces that

$$\mathcal{E}(x)_{[\rho t]} = \mathcal{E}(x_{[t]}), \text{ for all } t \in [T]. \qquad (**)$$

The *decoder* is now a collection of maps from $\mathbb{R}^{\rho t}$ to $\mathbb{R}^t$ for each $t \in [T]$; the output of the decoder at time t is $\mathcal{D}\left(\mathcal{E}\left(x_{[t]}\right) + y\right)$, where $y \in \mathbb{R}^{\rho t}$ is the unknown error introduced by the adversary up to time t.

As in the offline setting, we would like our encoder to be linear. The requirement in eq. (**) then implies that the matrix A implementing the encoder needs to be lower triangular in the rate-adjusted sense that $A_{i,j} = 0$ if $i < j\rho$. (This is what we shall mean by "lower triangular" from here on.) However, none of the constructions arising from the work on Euclidean sections cited above provide a lower triangular A. This is to be expected since our decoding requirement in eq. (1) is itself unreasonable in the online setting: for example, an adversary who is silent for a while and then inserts a brief burst of noise can satisfy the $\|\cdot\|_1$ bound over the history of the communication, yet obliterate the last ρ transmissions, which are the only ones to carry information about the most recent portion of the signal.

The above objection guides us toward the right decoding requirement in the online setting. The idea is that the inaccuracy in the decoding of a prefix $(x_1, \ldots x_t)$, of the signal should decrease as time elapses after t, provided that the noise (even if adversarial) is subject to a possibly time-weighted $\|\cdot\|_1$-norm bound. Our aim is that for that portion of the signal that is in the remote

[1]As noted this cannot be achieved against *general* $\|\cdot\|_2$-bounded adversaries. However, if an $\|\cdot\|_2$-bounded adversary eventually stops inserting noise, i.e., if y has compact support, our decoding will be successful—reconstruction error will tend to 0—because in this case the two norms are comparable.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIT.2019.2919632, IEEE Transactions on Information Theory

past, our decoding guarantee is analogous to what can be achieved in the block coding setting. We now develop this idea quantitatively.

C. Two inadequate definitions

We start with two extreme formalizations, each of which captures one desirable feature; and then combine these. The first desideratum is that for any fixed i, as time t goes on, our decoding of x_i at time t become evermore accurate provided that the noise is below tolerable limits. (And in particular if the adversary stops injecting noise into the system.) This is analogous to the decoding guarantee given for discrete alphabets by tree codes.

We can formulate such a guarantee using a time-weighted norm for the decoding error. For a vector $x \in \mathbb{R}^T$, we define the $\|\cdot\|_\star$ "decoding norm", in which the error on inputs from the remote past is given higher weight than that on recent inputs:

$$\|x\|_\star := \|x\|_{\star(T)} := \sqrt{\frac{1}{T}\sum_{i=1}^{T}(T-i+1)x_i^2}, \qquad (2)$$

and we modify the block-code decoding requirement (eq. (1)) to the following:

$$\left\|\mathcal{D}(\mathcal{E}(x_{[t]})+y)-x_{[t]}\right\|_{\star(t)} \le \frac{\|y\|_1}{t^{1/2-\delta}},$$
$$\text{for all } t \in [T] \text{ and any given fixed } \delta \in (0,1/2). \qquad (3)$$

The flaw in this definition is that once the adversary has ever injected noise into the system, no decoding is ever possible of signals in the recent past (i.e., of x_{t-c} at time t for small c), even if say the adversary has ceased to inject any noise after a fixed time t_0. That is, requirement (3) fails a second desideratum: that the effects of any noise burst should dissipate over time.

This leads us to the other extreme: a decoding guarantee in which noise from the distant past is allowed to contribute only vanishingly to the decoding error. For this we define the time-weighted "noise norm" $\|\cdot\|_\dagger$:

$$\|y\|_\dagger := \|y\|_{\dagger(\rho T)} := \sum_{i=1}^{\rho T}|y_i|\left(\frac{\rho T-i+1}{\rho T}\right)^{-1/2}, \qquad (4)$$

and impose again the decoding requirement

$$\left\|\mathcal{D}(\mathcal{E}(x_{[t]})+y)-x_{[t]}\right\|_2 \le \frac{\|y\|_{\dagger(t)}}{t^{1/2-\delta}},$$
$$\text{for all } t \in [T] \text{ and any given fixed } \delta \in (0,1/2). \qquad (5)$$

The flaw in this second definition is that it does not provide gradually-improving decoding of each fixed input character (which was the motivation for the first definition). For any fixed level of noise, we have no better decoding guarantee on x_1 than on x_T at time T. (In particular, a bounded noise burst at time T is enough to ruin the decoding of x_1.)

D. The satisfactory definition and our main result

We achieve both desiderata with a definition which time-weights both the adversary's noise and the decoding error. Formally, for any $\mu \in [0,1]$, define

$$\|x\|_{\star_\mu} := \|x\|_{\star_\mu(T)} := \sqrt{\sum_{i=1}^{T}\left(\frac{T-i+1}{T}\right)^{\mu} x_i^2}$$
$$\|y\|_{\dagger_\mu} := \|y\|_{\dagger_\mu(\rho T)} := \sum_{i=1}^{\rho T}\left(\frac{\rho T-i+1}{\rho T}\right)^{-(1-\mu)/2}|y_i|\,. \qquad (6)$$

This subsumes the earlier cases we considered: eq. (2) is the case $\mu = 1$ while eq. (4) is the case $\mu = 0$.

Now, given any choice of $\mu \in (0,1]$ and $\delta \in (0,1/2)$, we demand the decoding guarantee (generalizing eqs. (3) and (5)):

$$\left\|\mathcal{D}(\mathcal{E}(x_{[t]})+y)-x_{[t]}\right\|_{\star_\mu(t)} \le \frac{\|y\|_{\dagger_\mu(\rho t)}}{t^{1/2-\delta}}, \text{for all } t \in [T]. \qquad (***)$$

Note that for any μ, the penalty imposed by the $\|\cdot\|_{\star_\mu}$-norm for errors made in decoding entries far away in the past (say at times $s < ct$) is the same (to within a constant factor $c' = c'(c)$) as that imposed by the $\|\cdot\|_2$-norm. Similarly, the weight assigned by the $\|\cdot\|_\dagger$ norm to the adversary's noise inserted at times $s < ct$ is within a constant factor to its unweighted $\|\cdot\|_1$ norm. However, when we are decoding entries x_s for s close to t, for which we do not yet have much information, these weighted norms allow us to make larger errors in decoding without much penalty. For $0 < \mu \le 1$, the requirement (***) on the decoder guarantees that as time progresses, so does our ability to attenuate the error introduced by the adversary. Further, in Theorem II.2, we show that our requirements enforce that the scaling of the attenuation factor in (***) cannot be $O(t^{-1/2})$ and must be of the form $\omega(t^{-1/2})$. In this the online coding problem differs from the block coding or $\|\cdot\|_1$-Dvoretzky problem.

Our main result is that for any fixed $\mu \in (0,1]$ and any $\delta \in \left(0,\frac{1}{2}\right)$, there is a constant-rate, constant-power code achieving requirement (***). Our code is linear, and decoding too is efficient: the decoder solves a linear program analogous to those appearing in the compressed sensing literature.

Notation. For a $\rho T \times T$ matrix A, we denote by A_t the $\rho t \times t$ matrix consisting of its top ρt rows and leftmost t columns.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIT.2019.2919632, IEEE Transactions on Information Theory

Theorem I.1 (**Informal, see Theorem II.1 for a formal statement**)**.** *For any $\mu \in (0,1]$ and $\delta \in (0, \frac{1}{2})$, there exists a rate parameter $\rho > 0$ for which there exists an encoder $\mathcal{E}$ and a decoder $\mathcal{D}$ satisfying the energy, error attenuation, and causal constraints in eqs.* (*), (**)*, and* (***).

In particular, the encoder $\mathcal{E}$ acts as left multiplication by a $\rho T \times T$ matrix C that is rate-adjusted lower triangular (i.e., $C_{ij} = 0$ when $i \le (j-1)\rho$), where T is the total time of transmission. At time $t \le T$, the decoder $\mathcal{D}$ acts by making an $\|\cdot\|_\dagger$-norm projection to $\mathbf{Range}(C_t)$ *and then applying C_t^{-1} (which is well defined on* $\mathbf{Range}(C)$*).*

A natural special case of the above is with $\mu = 1/2$. In this case the decoder and encoder guarantee

$$\sqrt{\sum_{i=1}^{T} \left(\frac{T-i+1}{T}\right)^{1/2} |\mathcal{D}(\mathcal{E}(x_{[t]}) + y)_i - x_i|^2} \le O(T^{\delta - 1/2}) \sum_{i=1}^{\rho T} \left(\frac{\rho T - i + 1}{\rho T}\right)^{-1/4} |y_i|$$

In particular, if both the waveform values x_i and the noise values y_i are $\Theta(1)$, then the error incurred by the decoder on a given entry of the signal, decreases to zero (at almost a $T^{-1/2}$ pace) as the communication continues in time. We also note that the quantity $(1-\mu)$ appearing in the exponent of the gain factor used in the $\|\cdot\|_{\dagger_\mu}$ norm cannot be replaced by any strictly smaller quantity; see the remark following Theorem II.1 for details.

E. Block coding and the Dvoretzky theorem

We now revisit the relation between Euclidean sections and block coding briefly alluded to above. Our goal in this paper may also be framed as showing the existence of a "lower triangular" analogue of a Euclidean section. This lower triangular constraint is the main source of technical difficulty in our work as compared to previous work; in particular, our method is quite different. The prior work does, however, show some limits on what can be achieved: specifically, it is enough to imply that the parameter δ in Theorem I.1 has to be non-negative. In recent years, the classic work on Euclidean sections has been re-interpreted explicitly in coding-theoretic language in a line of work that seeks to derandomize the original constructions [7]–[11]. We now sketch these connections.

Dvoretzky [6] initiated the study of the existence of large subspaces S of $\mathbb{R}^n$ equipped with an arbitrary norm which are "close" to being Euclidean. Our interest here is in the case where the norm is an $\|\cdot\|_p$-norm with $p = 1$, in which case the condition of S being close to Euclidean can be written as

$$\sup_{x \in S} \frac{\sqrt{n}\,\|x\|_2}{\|x\|_1} \le \Delta.$$

Here Δ is the distortion of the section, and one seeks to make it as close to 1 as possible. The problem of finding Euclidean sections of large dimension has also been extensively studied, starting with the work of Figiel, Lindenstrauss and Milman, and of Kašin [3]–[5], and in the special case $p = 1$ it is known that there exists a constant $c > 1$ (depending on Δ) such that $(\mathbb{R}^{cn}, \|\cdot\|_1)$ contains an Euclidean section of dimension n.

An equivalent view of Euclidean sections can be obtained in terms of a modified "condition number" of appropriate tall matrices (see, e.g., [5]). In particular, if there exists a real $cn \times n$ matrix A of rank n such that

$$\|A\|_{2\to 2} \cdot \left\|A^{-1}\right\|_{1\to 2} \le \frac{\Delta}{\sqrt{n}} \tag{7}$$

then $(\mathbb{R}^{cn}, \|\cdot\|_p)$ has a Euclidean section of dimension n (namely, $\mathbf{Range}(A)$) with distortion at most Δ (Here, and subsequently, A^{-1} denotes Moore-Penrose pseudo-inverse). It is also not hard to see that the existence of such a Euclidean section implies the existence of a rank n $cn \times n$ matrix A satisfying eq. (7).

This representation of an Euclidean section allows us to view it as a "block" version of the codes we seek in this paper. For, let A be a matrix satisfying the constraint in eq. (7), and assume without loss of generality that $\|A\|_{2\to 2} = 1$ (this can be ensured since the requirement in eq. (7) is invariant under scaling A by constants). Define the encoder $\mathcal{E}$ as left multiplication by A: $\mathcal{E}(x) = Ax$. The decoder $\mathcal{D}$ acts on an input y by first finding the point y' in $\mathbf{Range}(A)$ that is closest to y in the $\|\cdot\|_1$-norm (choosing one arbitrarily if there are several such points), and then returning $A^{-1}y'$. Since $\|A\|_{2\to 2} = 1$, the energy constraint (eq. (*)) is satisfied automatically. Using eq. (7) it can also be shown that

$$\|\mathcal{D}(\mathcal{E}(x) + y) - x\|_2 \le \frac{2\Delta}{\sqrt{n}} \|y\|_1 . \tag{8}$$

It is this guarantee for block decoding that we compare our result in Theorem I.1 against.

F. Related work

We are following here on two main lines of work in communications. One is the investigation begun by Sahai and Mitter of the "anytime capacity" of a communication channel, which they discovered to be essential to the feasibility of using that channel to control an unstable plant in real time [12]. Several types of channels and noise have been studied but the primary concern in that

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIT.2019.2919632, IEEE Transactions on Information Theory

literature is the role of channel noise in a feedback loop, and to our knowledge there is no result which resembles ours. The second concerns real-time communication of discrete signals over discrete channels; one of the results from that literature is that it is possible to causally encode a signal in such a manner that at all times T, if the noise has so far corrupted only cT characters ($c > 0$ sufficiently small), then the decoder can correctly determine the initial $(1 - O(c))T$ characters [13]. Our main result in this paper is intended as the appropriate analog of the latter statement for a physical signal and a physical channel, where "characters" are amplitudes of a waveform.

Our proof of existence of the code proceeds through an analysis of certain random matrices with independent but not identically distributed Gaussian entries. In this light, our requirements, especially when rephrased in terms similar to eq. (7), are connected to the long line of work on the condition number of almost square (and even square) random matrices (see, e.g, [14]–[17] and the references therein). Note, however, that we are concerned here with an analogue of a $\|\cdot\|_{1\to 2}$-norm of the pseudo-inverse of the encoding matrix, while in the work on condition number the emphasis is on the $\|\cdot\|_{2\to 2}$ norm of the inverse. Further, much of the work on the condition number has considered rectangular random matrices with identically distributed entries (see, however, the work of Cook [18] and Rudelson and Zeitouni [19] for recent progress on the lowest singular value of a class of structured matrices with non-i.i.d. entries) while we are in a very different regime—the main technical challenge of our work is to deal with the pseudo-inverse of random lower triangular matrices (whose non-zero entries are also not identically distributed). Nevertheless, we believe that the techniques developed in the work on the condition number may be relevant for further improvements of our result, especially on the question of achieving an optimal rate. We also note in passing that if one is concerned only with the norm of a matrix with independent but not necessarily i.i.d. entries (rather than the norm of its pseudo-inverse) then there are results in the literature providing good asymptotic bounds (see, e.g., [20]–[23]). Our analysis in fact uses one of these bounds from the work of Bandeira and van Handel [22].

A rather different notion of online coding underlies the long and celebrated line of work on fountain codes [24]. Recall that in our online coding setting, (1) the encoder does not receive the message symbols as a block but in an online fashion; (2) the adversary corrupts transmitted symbols rather than erasing them, so that the receiver does not know if a received symbol is corrupted or not; (3) both the original message and the transmission have real numbers as symbols. In fountain codes and continuing work such as LT codes [25] and Raptor codes [26] (see also [27]), the setting is different: (1) even at time $t = 0$, the encoder has access to the full block of n symbols comprising the message; (2) the message is to be sent over an erasure channel; (3) both the source and transmission symbols come from a discrete alphabet. The goal is for the code to be online in the sense that the encoder generates a potentially infinite number of symbols using a randomized algorithm, in such a way that the generated symbols are mutually independent random variables, but the receiver is able to decode the message with high probability as soon as it gets access to *any* $\Theta(n)$ of the encoder's generated symbols. Fountain codes and refinements such as LT and Raptor codes allow for very fast encoding and decoding while achieving the above goal.

G. Discussion

The most fundamental open question left open by our work is no doubt that of an explicit construction. On the positive side, the random matrices used in our constructions have with positive constant probability the properties we require. However, a more explicit construction that reduces the dependence on randomness, and more importantly enables efficient verification of the properties, is desirable. The ideas involved in the partial derandomizations of Euclidean sections [7]–[11] or in tree code constructions [28]–[31] may help toward this goal.

It is also likely that the tradeoff we provide between the rate $1/\rho$ of the code and the $\tilde{O}(t^\delta)$ overhead in Theorem I.1 can be improved; such optimization will be important toward practical implementation.

A third and fascinating question is whether the LPs to be solved in each decoding round, can be solved more quickly (at least in an amortized sense) thanks to the "warm start" from the only-slightly-different LP solved in the previous round.

II. Online codes and low distortion matrices

In this section, we provide a more quantitative discussion of the connection of our work to Euclidean sections of ℓ_1. We start with setting up some preliminary notation, and then state our main technical theorem (Theorem II.1), which establishes the existence of a lower triangular analogue of an Euclidean section. We then show that this implies the existence of the codes we seek. The rest of the paper is then devoted to proving Theorem II.1.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIT.2019.2919632, IEEE Transactions on Information Theory

A. Notation

Given a positive integer k a *k-lower triangular matrix* M with T columns is a $kT \times T$ matrix in which $M_{ij} = 0$ if $i \le (k-1)j$. For convenience, we also index the rows of such a matrix by ordered pairs (i, l) where $i \in [T]$ and $l \in [k]$, and the row indexed (i, l) is the $((k-1)i + l)$-th row from the top. The k-lower triangular condition can then be stipulated more succinctly as

$$M_{(i,l),j} = 0 \text{ when } i > j. \tag{9}$$

B. The main theorem and the code

Note that left multiplication of a message vector x by a k-lower triangular matrix M satisfies the "online" or "causal" constraint referred to in the introduction. The next theorem shows that there exists such a k-lower triangular matrix with properties which imply the other properties asked of the code in the introduction.

Theorem II.1 (The encoding matrix). *For any $\mu \in (0, 1]$ and $\delta \in (0, \frac{1}{2})$, there exist positive constants c_0, k_0 such that the following is true. Let $T \ge 3$ be any integer. For any rate parameter $k \ge k_0$ there exists a k-lower triangular $kT \times T$ matrix C satisfying the following conditions. (Recall that we denote by C_t the $kt \times t$ leading principal submatrix of C.)*

1) **Submatrices of C have small operator norm***: $\|C_t\|_{2\to 2} \le 1$ for $1 \le t \le T$.*
2) **Submatrices of C are robustly invertible***: for $1 \le t \le T$,*

$$\|C_t x\|_{\dagger_\mu(kt)} \ge c_0 t^{(1/2-\delta)} \|x\|_{\star_\mu(t)} \text{ for all } x \in \mathbb{R}^t.$$

The proof of this theorem will be through an analysis of certain k-lower triangular random matrices with independent but *not* identically distributed Gaussian entries. In the next section (Section III), we start with a simplified overview of the proof, before proceeding with the complete proof in Section IV. Here, we will show how the theorem immediately yields a code satisfying the conditions outlined in the introduction. But, first, we make a couple of remarks on the choice of the norms $\|\cdot\|_{\star_\mu}$ and $\|\cdot\|_{\dagger_\mu}$, and on the comparison between the respective robust invertibility guarantees that can be made in the online and block coding settings.

Remark II.1. We argue, by considering the action of the code on a unit pulse e_t at time t, $(1 \le t \le T)$, that the quantity $(1-\mu)$ appearing in the exponent of the gain factor used in the $\|\cdot\|_{\dagger_\mu}$ norm cannot be replaced by any strictly smaller quantity independent of δ. To see this, observe that when $x = e_t$, the right hand side of item 2 of the theorem is $\Theta(t^{(1-\mu)/2-\delta})$. On the other hand, due to the online encoding requirement (*), $C_t e_t$ must be a vector in $\mathbb{R}^{kt}$ in which only the last k entries may be non-zero. Further, the power constraint requirement (**) implies that these non-zero entries are $O(1)$. It follows that if the quantity $(1-\mu)$ in the definition of the $\|\cdot\|_{\dagger_\mu(kt)}$-norm is replaced by τ, the left hand side of item 2 is at most $O(t^{\tau/2})$. Thus for the inequality in item 2 to be possible for all $\delta > 0$, one requires that $\tau \ge (1-\mu)$.

Remark II.2. The robust invertibility guarantee obtained for the encoding matrices constructed in Theorem II.1 falls short of the guarantee obtainable in the block coding setting (eq. (7)), in the sense that we lose an extra $\Theta(t^\delta)$ factor in the online setting, albeit with the option to choose $\delta > 0$ as close to zero as we please at the cost of a deterioration in the rate of the code. A natural question therefore is whether it is possible to get rid of this loss and obtain a guarantee as strong as the block coding setting in the online setting as well. In the following theorem (proved in Section VI), we show that it is *not* possible to obtain the guarantee of (eq. (7)) in the online coding setting, and a loss of an $\omega_t(1)$ factor in the robust invertibility criterion must be incurred if the power constraint is to be satisfied.

Theorem II.2. *Fix $\mu \in (0, 1]$, $c_0 > 0$ and a positive integer k. There exists a constant $\tau = \tau(\mu, c_0, k)$ such that the following is true. If C is a $kT \times T$ k-lower triangular matrix such that for all $t \in [T]$ the submatrix C_t of C satisfies*

$$\|C_t x\|_{\dagger_\mu(kt)} \ge c_0 t^{1/2} \|x\|_{\star_\mu(t)} \text{ for all } x \in \mathbb{R}^t,$$

then there exists a non-zero $x \in \mathbb{R}^T$ for which

$$\|Cx\|_2^2 \ge \tau \sum_{i=1}^{T} \frac{1}{i} \ge (\tau \log T) \cdot \|x\|_2^2.$$

(An open question left by our work is to narrow the gap between our upper bound of $O(t^\delta)$ and our lower bound of $\Omega(\sqrt{\log t})$, on the norm loss due to the causal-coding restriction.)

We now show how Theorem II.1 immediately yields a code satisfying the conditions outlined in the introduction. Let T be the total time of transmission, and for $\delta \in (0, 1/2)$ let C be a k-lower triangular matrix with the rate parameter k as in the theorem. The encoder $\mathcal{E}$ is defined as left multiplication by the $kt \times t$ leading principal submatrix of C:

$$\mathcal{E}(x) = C_t x \text{ for all } x \in \mathbb{R}^t, 1 \le t \le T.$$

Thus, the encoder only needs to send k symbols at each time t.

At time $t \le T$, the decoder $\mathcal{D}$ acts as follows. Given a received message $z \in \mathbb{R}^{kt}$, it outputs the solution $x_0 \in \mathbb{R}^t$ of the following linear program:

$$\|z - C_t x_0\|_{\dagger_\mu(kt)} \le \min_{z' \in \mathbf{Range}(C_t)} \|z - z'\|_{\dagger_\mu(kt)} . \qquad (10)$$

We now show that the code C satisfies the conditions (*)-(***). The online encoding condition, eq. (**), holds by construction since C and its submatrices C_t are k-lower triangular. The power constraint, eq. (*), is satisfied since for each $1 \le t \le T$ and any $x \in \mathbb{R}^t$, applying Theorem II.1(1),

$$\|\mathcal{E}x\|_2 \le \|C_t\|_{2\to 2} \cdot \|x\|_2 \le \|x\|_2 .$$

We now show that the condition in eq. (***) is satisfied as well. Let x be the original message and y the noise added by the adversary, so that the received vector is $z = C_t x + y$. Let x_0 be the output of the decoder on input z computed according to eq. (10). We then have

$$\begin{aligned} \|C_t(x - x_0)\|_{\dagger_\mu(kt)} &\le \|y\|_{\dagger_\mu(kt)} + \|z - C_t x_0\|_{\dagger_\mu(kt)} \\ &\le 2\,\|y\|_{\dagger_\mu(kt)} , \end{aligned} \qquad (11)$$

where the second inequality follows from eq. (10) since $C_t x$ is in $\mathbf{Range}(C_t)$. Applying Theorem II.1(2), we now see that there exists a constant c_0 such that

$$\|x - x_0\|_{\star_\mu(t)} \le c_0 t^{-(1/2-\delta)} \|y\|_{\dagger_\mu(kt)} ,$$

so that the condition in eq. (***) also holds.

III. Overview

This section is devoted to a high-level description of the main ideas of our construction and its analysis. All main ideas needed for the proof of Theorem II.1 are discussed here, and a roadmap with forward references to the full arguments is provided. The details, being more complicated, have been consigned to Sections IV and V.

Our starting point is the connection to Euclidean sections of $(\mathbb{R}^{cT}, \|\cdot\|_1)$ alluded to in the introduction. Specifically, we recall the discussion there of rectangular matrices A whose range is a Euclidean section, or equivalently, which satisfy eq. (7). One standard construction of such a matrix is to choose a $cT \times T$ random matrix whose entries are i.i.d. Gaussian variables. In order to ensure that $\|A\|_{2\to 2} = O(1)$, it suffices to choose the standard deviation of the entries to be $\Theta(1/\sqrt{T})$. For the purposes of the informal discussion in this section, we will refer to such a random matrix, whose entries are independent Gaussians with variances within a constant factor of each other, as a *Dvoretzky matrix*. The discussion in the introduction showed that a Dvoretzky matrix suffices if we were interested only in block coding with a block length of T and did not enforce the online encoding constraint.

The first step to adapting this standard construction to our online setting is to zero out the entries above the diagonal (in the indexing of rows and columns introduced in Section II-A, this corresponds to enforcing eq. (9)). However, this is not sufficient since the entries close to the diagonal are still of order $O(1/\sqrt{T})$ where T is the total time of transmission. To see what the problem is, consider the operation of the encoder and the decoder at a time $t \ll T$. In this setting, messages sent by the encoder up to time t are all attenuated by a factor that is $O(1/\sqrt{T})$, and this allows the adversary to swamp out the signal with noise of small $\|\cdot\|_1$-norm. Such a situation will not allow us to achieve a decoding guarantee similar to eq. (3) where the guarantee provided at time $t \ll T$ keeps monotonically improving as the total time T for which the transmission lasts increases (in fact, in this scenario, the decoding at time $t \ll T$ becomes progressively worse with increasing T). We therefore cannot attenuate all entries of the matrix by a factor of the form $O(1/\sqrt{T})$; indeed we want entries close to the diagonal of the matrix to be of order $\tilde{\Omega}(1)$ (so that immediate decoding is accurate unless there is a noise burst). On the other hand, we do want the variances of the matrix entries to have properties similar to those of Dvoretzky matrices, in the sense that

1) the sum of variances across a row or column of the matrix is at most a constant: intuitively, this is a prerequisite for enforcing that the $2 \to 2$-norm of the matrix is a constant, and
2) the sum of their square roots (i.e., standard deviations) across a row or column is roughly $\tilde{\Omega}(\sqrt{t})$: intuitively, this is a prerequisite for making sure that all vectors in the image of the unit $\|\cdot\|_2$-ball under the matrix have $\|\cdot\|_1$-norm about $\tilde{\Omega}(\sqrt{t})$.

To satisfy the above two conditions with the lower triangular constraint, we consider random matrices whose entries are Gaussians with progressively attenuated variances. The construction we actually use in the proof of Theorem II.1 appears in Section IV, but for the purposes of this informal discussion, we use a slightly simplified version. Let k be a fixed constant rate parameter. We then define the distribution $\mathcal{A}'_{T,k}$ on k-lower triangular matrices such that a $kT \times T$ matrix $M \sim \mathcal{A}'_{T,k}$ is sampled as follows:

$$M((i,l), j) = \frac{1}{k} \cdot \begin{cases} 0, & i < j, \\ g(i-j)\xi_{(i,l),j}, & i \ge j, \end{cases} \qquad (12)$$

where that $\xi_{(i,l),j}$ are independent standard normal random

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIT.2019.2919632, IEEE Transactions on Information Theory

variables, and

$$g(i) := \frac{1}{\sqrt{i+1}\log(i+2)}.$$

Note that $\sum_{i\geq 0} g(i)^2$ converges, while $\sum_{i\in[t]} g(i) = \tilde{\Omega}(\sqrt{t})$. A lower bound on the probability that M as sampled above has small $\|\cdot\|_{2\to 2}$-norm is established by adapting known results in the literature: see Lemma IV.4. The main technical problem, however, is to show that $\|Mx\|_{\dagger_\mu(kT)}$ is large compared to $\|x\|_{\star_\mu(T)}$ for all $x \in \mathbb{R}^T$. Again, we emphasize that to prove Theorem II.1, we actually need to establish this condition at all times $t \leq T$: however, for now we focus on the case $t = T$.

We now introduce some notation that will be useful both in our proofs and in the discussion here (see Figure 1 for a pictorial illustration of the notation introduced here). For any positive integer n, we define $\mathbf{lg}(n) := \lceil \lg(n+1)\rceil$ so that $\mathbf{lg}(\mathrm{n})$ is the length of the canonical binary representation of n. For a vector $x \in \mathbb{R}^T$, we denote by $\mathbf{bl}(x,i)$ the sub-vector of x of length 2^{i-1} consisting of the entries $(x_{T+2-2^i}, \cdots, x_{T+1-2^{i-1}})$. We similarly define the sub-vector $\mathbf{cl}(x, j_1, j_2)$ to be the concatenation of the sub-vectors $\mathbf{bl}(x,i)$ for $j_2 \leq i \leq j_1$. When $j_2 = 1$, we write $\mathbf{cl}(x, j_1, 1)$ as $\mathbf{cl}(x, j_1)$.

Our analysis of M will need to consider the action of appropriate sub-matrices of M on such sub-vectors; we now introduce notation for these sub-matrices. For any matrix A with T columns, let $\mathbf{Bl}(A, j)$ denote the matrix consisting of the 2^{j-1} columns of A with indices in the interval $[T+2-2^j, T+1-2^{j-1}]$. We thus have for any such A (in particular for M) that

$$Ax = \sum_{j=1}^{\mathbf{lg}(T)} \mathbf{Bl}(A,j)\mathbf{bl}(x,j).$$

Similarly, we define $\mathbf{Cl}(A, j)$ to be the sub-matrix of A consisting of its last $2^j - 1$ columns. In particular, $\mathbf{Cl}(A, j)$ acts on $\mathbf{cl}(x, j)$ and we have

$$\mathbf{Cl}(A,j)\mathbf{cl}(x,j) = \mathbf{Bl}(A,j)\mathbf{bl}(x,j) + \mathbf{Cl}(A,j-1)\mathbf{cl}(x,j-1).$$

We will also need to consider suffixes of the output of these matrices at several places in the proofs and also in this discussion. Formally, given an integer k and any matrix A, we define $\overline{\mathbf{ll}}(A, j)$ to be the sub-matrix of A consisting of its last $k \cdot 2^{j-1}$ rows. We also extend this notion to vectors in the co-domain of A: for such a vector y, $\overline{\mathbf{ll}}(y, j)$ denotes the sub-vector consisting of the last $k \cdot 2^{j-1}$ entries of y.

In our proofs, it is easier to work in terms of a matrix B obtained by rescaling the entries of M in such a way that

$$\inf_{y\neq 0} \frac{\|My\|_{\dagger_\mu(kT)}}{\|y\|_{\star_\mu(T)}} = \sqrt{T}\cdot \inf_{\|x\|_2=1} \|Bx\|_1 .$$

Such a k-lower triangular matrix B is obtained by setting

$$B_{(i,l),j} = \frac{M_{(i,l),j}}{\left[(T-i+1)^{1-\mu}(T-j+1)^{\mu}\right]^{1/2}}$$

for $i \geq j$ and $B_{(i,l),j} = 0$ otherwise. Theorem IV.5 and Lemma IV.6 then show that for each j, $\overline{\mathbf{ll}}(\mathbf{Bl}(B,j), j-1)$ behaves roughly like a Dvoretzky matrix, in the sense that $\sup \frac{\left\|\overline{\mathbf{ll}}(\mathbf{Bl}(B,j),j-1)x\right\|_1}{\|x\|_2}$ is within a factor $\Theta(1)$ of $\inf \frac{\left\|\overline{\mathbf{ll}}(\mathbf{Bl}(B,j),j-1)x\right\|_1}{\|x\|_2}$, with probability at least $1 - \exp(-\Omega(k\cdot 2^j))$. Corollary IV.7 strengthens this to show that with the same probability, the infimum above is not decreased substantially even if the output of $\overline{\mathbf{ll}}(\mathbf{Bl}(B,j), j-1)$ is perturbed with a vector drawn from a small dimensional subspace (namely, the range of $\mathbf{Cl}(B, j-1)$).

Lemma IV.8 then shows that the $\|\cdot\|_1$ norm of this perturbation itself is also preserved in the output of $\overline{\mathbf{ll}}(\mathbf{Bl}(B,j), j-1)$. Together, these results lead to Lemma IV.9 which shows, roughly speaking, that with probability $1 - \exp(-\Omega(k\cdot 2^j))$,

$$\begin{aligned}
&\left\|\overline{\mathbf{ll}}(\mathbf{Cl}(B,j)\mathbf{cl}(x,j), j-1)\right\|_1 \\
&\quad\geq \max\left\{\left\|\overline{\mathbf{ll}}(\mathbf{Bl}(B,j)\mathbf{bl}(x,j), j-1)\right\|_1,\right. \\
&\quad\left.(1-\epsilon)\left\|\overline{\mathbf{ll}}(\mathbf{Cl}(B,j-1)\mathbf{cl}(x,j-1), j-1)\right\|_1\right\},
\end{aligned}$$

for some small constant $\epsilon > 0$. Informally, this says that the output of each trailing principal sub-matrix $\mathbf{Cl}(B, j)$ preserves both the output of its left most block $\mathbf{Bl}(B, j)$, as well as the output of the remaining trailing principal sub-matrix $\mathbf{Cl}(B, j-1)$. Underlying these results is a sequence of ϵ-net arguments, which use concentration bounds on the ℓ_1 norms of Gaussian vectors with independent entries of non-identical means and variances, provided in Theorems A.4 and A.7.

Finally, Theorem IV.10 and Corollary IV.11 use Lemma IV.9 in an induction to show that with probability at least $1 - \exp(-\Omega(k))$,

$$\|Mx\|_{\dagger_\mu(kT)} \geq \tilde{\Omega}(T^{1/2-\delta})\,\|x\|_{\star_\mu(T)} \tag{13}$$

Equation (13) establishes that M has the requisite properties at time T, but recall that our code requires online decoding at all times $t \leq T$. Unfortunately, we cannot take an union bound over all t using eq. (13) unless we choose $k = \Omega(\log T)$, which would lead to a very low communication rate of $1/k = O(1/\log T)$ (recall that what we actually want, and achieve, is k a constant).

However, there is a simple remedy if we would be willing to carry information only about a sufficiently delayed prefix of x. In particular, Theorem IV.10

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIT.2019.2919632, IEEE Transactions on Information Theory

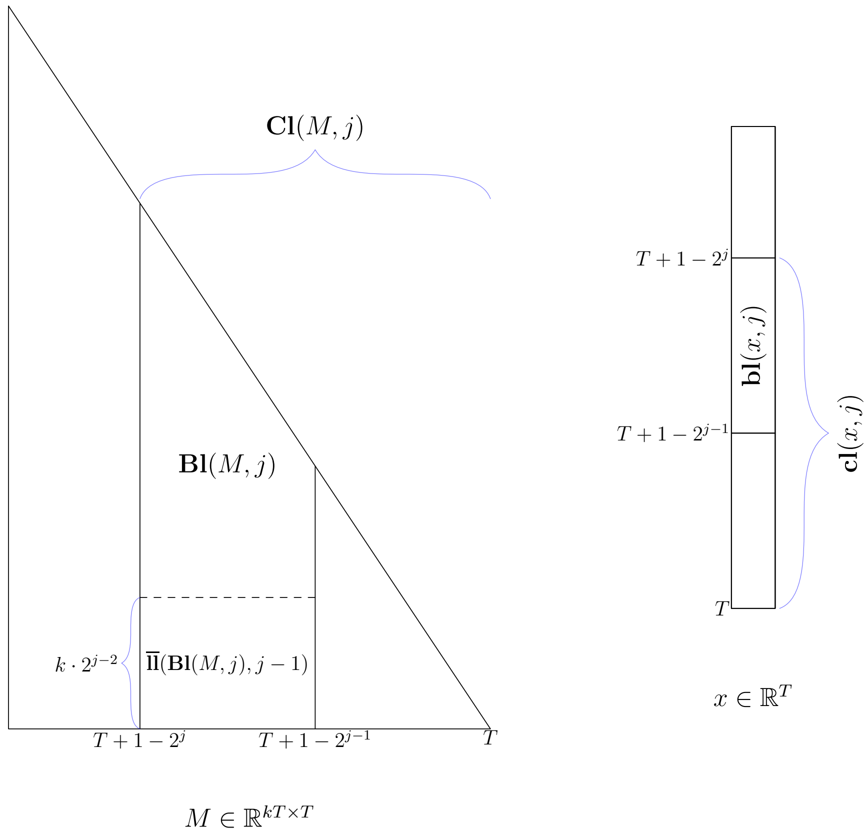

Figure 1. Notation for submatrices and sub-vectors

and Corollary IV.11 also show that if j_0 is chosen so that $j_0 = \Omega(\log\log T)$, then M carries enough information about $\mathbf{cl}(x, \tau_0, j_0)$ (recall that this is the prefix of x which ignores its last $2^{j_0-1} - 1 = \mathrm{poly}(\log T)$ entries) so that with probability at least $1 - O(1/T^2)$:

$$\|Mx\|_{\dagger_\mu(kT)} \geq O(T^{1/2-\delta}) \|\mathbf{cl}(x, \tau_0, j_0)\|_{\star_\mu(T)} .$$

We can now indeed take a union bound over all $t \leq T$ to see that the above is true at all times $t \leq T$ with probability at least $1 - O(1/T)$. However, the price we pay for this is that we cannot say anything about the most recent $\mathrm{poly}(\log T)$ characters of the message. This can be fixed by making the code systematic: the details are in Section V.

We emphasize here that although the above discussion often refers to the total time of communication T, our actual construction does not assume a knowledge of T. In particular, the rate and error guarantees in Theorem II.1 are achieved also at times t that might be much smaller than the eventual total time T.

The rest of the paper is devoted to the details of the proof.

IV. Progressively attenuated Gaussian matrices

Our proof of Theorem II.1 will proceed through an analysis of a specific distribution over random k-lower triangular matrices. We start by recalling some results from the literature that will be used in our proofs.

A. Technical preliminaries

1) Operator norm of Gaussian matrices: We will use the following result on the operator norm of matrices with independent Gaussian entries.

Theorem IV.1 (Bandeira and van Handel [22, Theorem 3.1]). *Let A be a $n \times m$ random matrix with independent mean zero Gaussian entries such that $A_{ij} \sim \mathcal{N}(0, a_{ij}^2)$. Then*

$$\mathbb{E}\left[\|A\|_{2\to 2}\right] \leq \frac{3}{2}\left(\sigma_1 + \sigma_2 + 10\sigma_0\sqrt{\log\min(n,m)}\right),$$

where

$$\sigma_1^2 := \max_{i\in[n]} \sum_{j=1}^m a_{ij}^2;\ \sigma_2^2 := \max_{j\in[m]} \sum_{i=1}^n a_{ij}^2;\ \sigma_0 := \max_{\substack{i\in[n]\\ j\in[m]}} |a_{ij}| .$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIT.2019.2919632, IEEE Transactions on Information Theory

2) ϵ-nets: We will use the following standard facts about ϵ-nets for subspaces of $(\mathbb{R}^n, \|\cdot\|_p)$ for $p \geq 1$ (see, e. g., [5]).

Fact IV.2. *Let U be a subspace of $(\mathbb{R}^n, \|\cdot\|_p)$ of dimension at most d. Then, for $\epsilon \leq r$ the $\|\cdot\|_p$-ball (respectively, the $\|\cdot\|_p$-sphere) of radius r in U has an ϵ-net in $\|\cdot\|_p$ of size at most $(3r/\epsilon)^d$.*

Fact IV.3. *Let $p, q \geq 1$, and let M be a $m \times n$ real matrix. If $\|Mx\|_q \leq c$ for all x in a $\|\cdot\|_p$ (1/2)-net of the $\|\cdot\|_p$ sphere in $\mathbb{R}^n$, then $\|M\|_{p\to q} \leq 2c$.*

B. The distribution $\mathcal{A}_{T,k}$

We now describe the distribution on random k-lower triangular matrices that will be used in the proof of Theorem II.1.

Let T be a positive integer, and set $\tau = \mathbf{lg}(T)$, where

$$\mathbf{lg}(T) := \lceil \lg(T+1) \rceil$$

is the number of bits in the canonical binary representation of T . Given a rate parameter k, $\mathcal{A}_{T,k}$ is a distribution on $kT \times T$ k-lower triangular matrices, such that a matrix $M \sim \mathcal{A}_{T,k}$ is sampled as follows:

$$M((i,l), j) = \frac{1}{k \cdot \mathbf{lg}(i)^4} \cdot \begin{cases} 0, & i < j, \\ \frac{1}{\sqrt{i-j+1}} \cdot \xi_{(i,l),j}, & i \geq j. \end{cases} \tag{14}$$

where $i, j \in [T], l \in [k]$, and the $\xi_{(i,l),j}$ are independent standard normal random variables. Note that we divide the rows of M into T *segments*, where the ith segment is of size k, and index the rows by a pair (i, l) where $i \in [T]$ denotes the segment, and $l \in [k]$ determines the offset in the segment.

Remark IV.1. Note that the distribution $\mathcal{A}_{T,k}$ is "time-invariant" in the sense that for any $1 \leq t \leq T$, the $kt \times t$ leading principal submatrix of M sampled from $\mathcal{A}_{T,k}$ is also a faithful sample from $\mathcal{A}_{t,k}$.

C. The distribution of $\|M\|_{2\to 2}$

We begin with a short discussion of the operator norm of M sampled according to $\mathcal{A}$; much of our technical work would be devoted to the study of M^{-1}. For the operator norm, however, the following corollary of Theorem IV.1 of Bandeira and van Handel will be sufficient for our purposes.

Lemma IV.4. *For any $\gamma \in (0, 1)$ there exists a positive integer c_0 such that if $k > c_0$ then $M \sim \mathcal{A}_{T,k}$ satisfies $\|M\|_{2\to 2} \leq 1$ with probability at least $1 - \gamma$.*

Proof: For $1 \leq i \leq \mathbf{lg}(T)$, let $M(i)$ denote the submatrix of M consisting of the consecutive rows from $(2^{i-1}, 1)$ to $(\min(2^i - 1, T), k)$. Here, we are using the indexing scheme for rows of M that was defined in eq. (14). Note that the number of non-zero columns of $M(i)$ is at most $2^i - 1$. We now apply Theorem IV.1 to each $M(i)$. In the notation of that theorem, we have for $M(i)$

$$\sigma_1 \leq \frac{1}{k \cdot i^3}, \; \sigma_2 \leq \frac{1}{\sqrt{k} \cdot i^3} \text{ and } \sigma_0 \leq \frac{2}{k \cdot i^4},$$

where we use the estimate

$$\sum_{x=1}^{n} \frac{1}{x} \leq \sum_{x=1}^{2^{\mathbf{lg}(n)}-1} \frac{1}{x} \leq \sum_{j=1}^{\mathbf{lg}(n)} \sum_{x:\mathbf{lg}(x)=j} \frac{1}{2^{j-1}} = \mathbf{lg}(n).$$

The theorem then implies that when $k \geq c$ for $c = c(\gamma)$ large enough, we have $\mathbb{E}[\|M(i)\|_{2\to 2}] \leq \frac{\gamma}{4i^3}$ for all $1 \leq i \leq \mathbf{lg}(T)$. Thus, for $1 \leq i \leq \mathbf{lg}(T)$,

$$\mathbb{P}\left[\|M(i)\|_{2\to 2} > \frac{1}{i\sqrt{2}}\right] \leq \frac{\gamma}{2i^2}.$$

By a union bound (and using $\sum_{i\geq 1}(1/i^2) < 2$), we get that with probability at least $1 - \gamma$

$$\|M(i)\|_{2\to 2} \leq \frac{1}{i\sqrt{2}} \text{ for all } 1 \leq i \leq \mathbf{lg}(T). \tag{15}$$

When the event in eq. (15) occurs, we have $\|M\|_{2\to 2} \leq 1$, since for any $x \in \mathbb{R}^T$ (here $x_{[l]}$ denotes the prefix of x consisting of its first l co-ordinates)

$$\begin{aligned} \|Mx\|_2^2 &= \sum_{i=1}^{\mathbf{lg}(T)} \left\|M(i) x_{[2^i-1]}\right\|_2^2 \\ &\leq \sum_{i=1}^{\mathbf{lg}(T)} \|M(i)\|_{2\to 2}^2 \left\|x_{[2^i-1]}\right\|_2^2 \leq \sum_{i=1}^{\mathbf{lg}(T)} \frac{1}{2i^2} \left\|x_{[2^i-1]}\right\|_2^2 \\ &\leq \sum_{j=1}^{T} x_j^2 \sum_{i=\tau(j)}^{\mathbf{lg}(T)} \frac{1}{2i^2} \leq \|x\|_2^2, \end{aligned}$$

where the last inequality uses $\sum_{i\geq 1}(1/i^2) < 2$. ■

D. Invertibility of M

To ease notation, we fix a $\mu \in (0, 1]$ in the rest of this section, and proceed to study the robust invertibility of a matrix M sampled from $\mathcal{A}_{T,k}$ with respect to the $\|\cdot\|_{\dagger_\mu(kT)}$ and $\|\cdot\|_{\star_\mu(T)}$ norms by analyzing the quantity $\inf_{y\neq 0} \frac{\|My\|_{\dagger_\mu(kT)}}{\|y\|_{\star_\mu(T)}}$. The constants appearing in the statements of the theorems appearing below therefore carry an implicit dependence upon this fixed value of μ.

Our first step is to pass to standard unweighted norms via a simple reduction. Let L be a $kT \times kT$ diagonal matrix with $L_{i,i} = (kT)^{(1-\mu)/2} \cdot (kT - i + 1)^{-(1-\mu)/2}$, and let R be

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIT.2019.2919632, IEEE Transactions on Information Theory

a $T \times T$ diagonal matrix with $R_{i,i} = T^{\mu/2} \cdot (T-i+1)^{-\mu/2}$. We then have

$$\inf_{y\neq 0} \frac{\|My\|_{\dagger_\mu(kT)}}{\|y\|_{\star_\mu(T)}} = \inf_{x\neq 0} \frac{\|LMRx\|_1}{\|x\|_2} \geq \sqrt{T} \cdot \inf_{\|x\|_2=1} \|Bx\|_1 , \tag{16}$$

where the matrix B is defined in terms of M as follows:

$$B_{(i,l),j} = \frac{M_{(i,l),j}}{\left[(T-i+1)^{1-\mu}(T-j+1)^{\mu}\right]^{1/2}}. \tag{17}$$

Denote the distribution of B obtained from $M \sim \mathcal{A}_{T,k}$ as $\mathcal{B}_{T,k}$. We will now study the properties of the blocks $\mathbf{Bl}(B,j)$ for B sampled from this distribution in detail. We start with an investigation of their $2 \to 1$ norm.

Theorem IV.5. *Let k be a rate parameter such that $k \geq 1 + \log 6$, and let $B \sim \mathcal{B}(T,k)$ for some positive integer T. Then for each $2 \leq j \leq \mathbf{lg}(T)$,*

$$\mathbb{P}\left[\left\|\overline{\mathbf{ll}}(\mathbf{Bl}(B,j), j-1)\right\|_{2\to 1} > \frac{256}{\sqrt{\mu}\,\mathbf{lg}(T)^4}\right] \leq \exp\left(-(k-\log 6)2^{j-1}\right).$$

Proof: Fix $2 \leq j \leq \mathbf{lg}(T)$, and let S be any $1/2$-net for the unit sphere in $(R^{2^{j-1}}, \|\cdot\|_2)$. Note that we can choose S so that $|S| \leq \exp\left(2^{j-1}\log 6\right)$. For ease of notation, we index the co-ordinates of any $x \in S$ from 2^{j-1} to $2^j - 1$. Now, for any such $x \in S$, we have

$$\left\|\overline{\mathbf{ll}}(\mathbf{Bl}(B,j)x, j-1)\right\|_1 = \sum_{i=1}^{2^{j-2}} \sum_{l=1}^{k} \left|X_{i,l}\right|, \tag{18}$$

where $X_{i,l}$ are independent mean zero normal variables with variances

$$\sigma_{i,l}^2 = \frac{1}{k^2 \cdot \mathbf{lg}(T-i+1)^8} \sum_{s=2^{j-1}}^{2^j-1} \frac{x_s^2}{s^{\mu} \cdot i^{1-\mu} \cdot (s-i+1)}. \tag{19}$$

Note that since $j \leq \mathbf{lg}(T)$, we have $T \geq 2^{j-1}$. For $1 \leq i \leq 2^{j-2}$, this implies that $\mathbf{lg}(T-i+1) \geq \max(1, \mathbf{lg}(T)-1) \geq \mathbf{lg}(T)/2$, so that we have

$$\begin{aligned}\sum_{i=1}^{2^{j-2}} \sum_{l=1}^{k} \sigma_{i,l}^2 &\leq \frac{2^8}{k\,\mathbf{lg}(T)^8} \sum_{i=1}^{2^{j-2}} \sum_{s=2^{j-1}}^{2^j-1} \frac{x_s^2}{s^{\mu} \cdot i^{1-\mu} \cdot (s-i+1)} \\ &\leq \frac{2^{11} \cdot 2^{-(1+\mu)j} \cdot \|x\|_2^2}{k\,\mathbf{lg}(T)^8} \cdot \sum_{i=1}^{2^{j-2}} \frac{1}{i^{1-\mu}} \\ &\leq \frac{2^{11} \cdot 2^{-j}}{\mu k\,\mathbf{lg}(T)^8} \|x\|_2^2 ,\end{aligned} \tag{20}$$

where in the first inequality we use $0 < \mu \leq 1, s \geq 2^{j-1}$ and $s-i+1 \geq 2^{j-2}$, and in the second inequality the fact that $\sum_{i=1}^N i^{\mu-1} \leq N^{\mu}/\mu$.

We now apply Corollary A.2 to the sum in eq. (18). The number of terms n is $k \cdot 2^{j-2}$, and we set the parameter α in Corollary A.2 to $\alpha = \frac{2^7}{\sqrt{\mu}\,\mathbf{lg}(T)^4\sqrt{n}} \|x\|_2$ to get

$$\mathbb{P}\left[\left\|\overline{\mathbf{ll}}(\mathbf{Bl}(B,j)x, j-1)\right\|_1 > 2^7/(\sqrt{\mu}\,\mathbf{lg}(T)^4)\,\|x\|_2\right] \leq \exp\left(-k \cdot 2^j\right). \tag{21}$$

A union bound over all $x \in S$ now yields

$$\mathbb{P}\left[\exists x \in S, \left\|\overline{\mathbf{ll}}(\mathbf{Bl}(B,j)x, j-1)\right\|_1 > 2^7/(\sqrt{\mu}\,\mathbf{lg}(T)^4)\,\|x\|_2\right] \leq \exp\left(-(k-\log 6) \cdot 2^j\right). \tag{22}$$

Since S is a $1/2$-net, Fact IV.3 implies that $\left\|\overline{\mathbf{ll}}(\mathbf{Bl}(B,j), j-1)\right\|_{2\to 1} \leq 2^8/(\sqrt{\mu}\,\mathbf{lg}(T)^4)$ with probability at least $1 - \exp\left(-(k-\log 6) \cdot 2^{j-1}\right)$. ∎

The next lemma shows that the $\|\cdot\|_1$ norm of the output of $\mathbf{Bl}(B,j)$ cannot be very small.

Lemma IV.6. *There exist positive constants $c_1, c_2 > 0$ such that the following is true. For any integer $j \geq 2$, any $k \geq c_1$, and any vector y,*

$$\mathbb{P}\left[\exists x, \|x\|_2 = 1 \text{ and } \left\|\overline{\mathbf{ll}}(\mathbf{Bl}(B,j)x + y, j-1)\right\|_1 < c_2/(\mathbf{lg}(T)^4)\right] \leq \exp\left(-c_2 k \cdot 2^j\right).$$

Proof: Let S be an ϵ-net for the unit sphere in $\left(\mathbb{R}^{2^{j-1}}, \|\cdot\|_2\right)$, for an ϵ to be determined later. As in eq. (18) in the proof of Theorem IV.5, for any $x \in S$, we have

$$\left\|\overline{\mathbf{ll}}(\mathbf{Bl}(B,j)x + y, j-1)\right\|_1 = \sum_{i=1}^{2^{j-2}} \sum_{l=1}^{k} \left|X_{i,l} + y_{i,l}\right| \tag{23}$$

where $X_{i,l}$ are independent mean zero normal variables with variances $\sigma_{i,l}$ as defined in eq. (19). Recall also that $\mathbf{lg}(T) - 1 \leq \mathbf{lg}(T-i+1) \leq \mathbf{lg}(T)$ since $i \leq 2^{j-2}$.

Since we are interested in upper bounding the probability that the above sum is small, it follows from Corollary A.6 that the worst case is $y = 0$. In preparation to apply Theorem A.4 to the above sum with $y = 0$, we also note that since the $\sigma_{i,l}^2$ are positive linear functions of the x_s^2 and $\|x\|_2 = 1$, $GM\left(\left(\sigma_{i,l}\right)_{\substack{i\in[2^{j-2}]\\ l\in[k]}}\right)$ is minimized when $x = e_s$ for some $s \in [2^{j-1}, 2^j - 1]$. We thus have

$$\begin{aligned} &GM\left(\left(\sigma_{i,l}\right)_{\substack{i\in[2^{j-2}]\\ l\in[k]}}\right) \\ &\geq \frac{1}{k\,\mathbf{lg}(T)^4}\cdot\frac{1}{\sqrt{GM\left(\left(i^{1-\mu}\right)_{i\in[2^{j-2}]}\right)}} \\ &\quad\cdot \min_{s\in[2^{j-1},2^j-1]} \frac{1}{\sqrt{s^{\mu} GM\left(\left(s-i+1\right)_{i\in[2^{j-2}]}\right)}} \\ &\geq \frac{2^{-j/2}}{k\,\mathbf{lg}(T)^4} \min_{s\in[2^{j-1},2^j-1]} \frac{1}{\sqrt{s}}. \end{aligned}$$

Applying Theorem A.4, and noting that the number of terms in the sum in eq. (23) for which the geometric mean was taken above is $k \cdot 2^{j-2}$, we now find a positive constant $c > 0$ such that the following holds for all $\tau \in (0, 1)$:

$$\mathbb{P}\left[\left\|\overline{\mathbf{ll}}(\mathbf{Bl}(B,j)x + y, j-1)\right\|_1 < \frac{c\tau}{\mathbf{lg}(T)^4}\right] \leq \tau^{k\cdot 2^{j-2}}.$$

Taking a union bound over all x in the ϵ-net S, and then using the bound on $\left\|\overline{\mathbf{ll}}(\mathbf{Bl}(B,j), j-1)\right\|_{2\to 1}$ derived in the proof of Theorem IV.5, we then have

$$\begin{aligned} &\mathbb{P}\Big[\exists x, \|x\|_2 = 1, \text{ and} \\ &\left\|\overline{\mathbf{ll}}(\mathbf{Bl}(B,j)x + y, j-1)\right\|_1 < (c\tau - 256\mu^{-1/2}\epsilon)/\mathbf{lg}(T)^4\Big] \\ &\quad\leq \exp\left(-2^{j-1}\cdot[(k/2)\log(1/\tau) - \log(3/\epsilon)]\right) \\ &\qquad + \exp\left(-2^{j-1}\cdot(k-\log 6)\right). \quad (24) \end{aligned}$$

Since $k \geq c_1$ for a large enough c_1, the claim now follows after choosing ϵ and τ to be appropriate constants. ■

We now consider small dimensional perturbations to the output of $\mathbf{Bl}(B, j)$ for $j \geq 2$, and start with a corollary of Lemma IV.6.

Corollary IV.7. *There exist positive constants $C, C_1, C_2 > 0$ such that the following is true. For any $j \geq 2$, $k \geq C_1$, and V an arbitrary subspace of dimension at most $2(2^j - 1)$,*

$$\mathbb{P}\left[\exists x \in \mathbb{R}^{2^{j-1}}, y \in V \text{ s. t. } \left\|\overline{\mathbf{ll}}(\mathbf{Bl}(B,j)x + y, j-1)\right\|_1 < C\|x\|_2/(\mathbf{lg}(T)^4)\right] \leq \exp\left(-C_2 k\cdot 2^j\right).$$

Proof: Let U be the vector space $\left\{\overline{\mathbf{ll}}(y, j-1) \mid y \in V\right\}$. Note that we can replace V by U in the statement of the corollary (i.e., if the result holds for U, then it also holds for V). We therefore restrict our attention to U. Note that the dimension of U is no more than the dimension of V.

Let c_2 be as in Lemma IV.6 and define $C = c_2/2$. From Theorem IV.5 we know that $\left\|\overline{\mathbf{ll}}(\mathbf{Bl}(B,j), j-1)\right\|_{2\to 1} \leq 256/(\sqrt{\mu}\,\mathbf{lg}(T)^4)$ with probability at least $1 - \exp\left(-\Theta(k\cdot 2^j)\right)$. Under this event we also have

$$\left\|\overline{\mathbf{ll}}(\mathbf{Bl}(B,j)x + y, j-1)\right\|_1 \geq C/\mathbf{lg}(T)^4$$

whenever $\|x\|_2 = 1$ and $\|y\|_1 > (C + 256\mu^{-1/2})/\mathbf{lg}(T)^4$.

Therefore, let N be a $\left(C/\mathbf{lg}(T)^4\right)$-net in ℓ_1 for the ℓ_1 ball of radius $(C+256\mu^{-1/2})/\mathbf{lg}(T)^4$ in U. We have $|N| \leq \exp\left(c' 2^j\right)$ for some $c' > 0$. Thus, applying Lemma IV.6 to each element in N and then taking a union bound, we have

$$\begin{aligned} &\mathbb{P}\Big[\exists x \in \mathbb{R}^{2^{j-1}}, y \in N \text{ s. t. } \|x\|_2 = 1 \text{ and} \\ &\quad\left\|\overline{\mathbf{ll}}(\mathbf{Bl}(B,j)x + y, j-1)\right\|_1 < 2C/\mathbf{lg}(T)^4\Big] \\ &\qquad\leq \exp\left(-c'' k\cdot 2^j\right), \end{aligned}$$

for some positive constant c'' whenever $k \geq c_1$ for some other positive constant c_1. Using the fact that N is a $(C/\mathbf{lg}(T)^4)$-net in ℓ_1 we get the claimed result. ■

We now show that adding the output of $\mathbf{Bl}(B, j)$ does not shrink the size of the perturbation either, as long as the perturbations comes from a small dimensional space.

Lemma IV.8. *For any $\gamma \in (0, 1)$ there exist positive constants $c_1 = c_1(\gamma), c_2 = c_2(\gamma)$ such that for any integers $j \geq 2$ and any $k > c_1$, the following is true. Let V be an arbitrary subspace of dimension at most $2(2^j - 1)$. Then,*

$$\begin{aligned} &\mathbb{P}\Big[\exists x \in \mathbb{R}^{2^{j-1}}, y \in V \text{ s. t.} \\ &\quad\left\|\overline{\mathbf{ll}}(\mathbf{Bl}(B,j)x + y, j-1)\right\|_1 < \gamma\left\|\overline{\mathbf{ll}}(y, j-1)\right\|_1\Big] \\ &\qquad\leq \exp\left(-c_2 k\cdot 2^j\right). \end{aligned}$$

Proof: From Theorem IV.5 and Corollary IV.7 we have that for some constant $c > 0$, the following events occur with probability at least $1 - \exp\left(-\Theta(k\cdot 2^j)\right)$ for all large enough constant k:

1) $\frac{\left\|\overline{\mathbf{ll}}(\mathbf{Bl}(B,j)x, j-1)\right\|_1}{\|x\|_2} \leq 256\mu^{-1/2}/\mathbf{lg}(T)^4$, for all $x \neq 0$, and
2) $\left\|\overline{\mathbf{ll}}(\mathbf{Bl}(B,j)x + y, j-1)\right\|_1 \geq c\|x\|_2/\mathbf{lg}(T)^4$ for all $x \in \mathbb{R}^{2^{j-1}}, y \in V$.

We assume henceforth that both the above events occur.

In particular, we have

$$\left\|\overline{\mathbf{ll}}(y, j-1)\right\|_1 = 1, \quad \|x\|_2 \geq \frac{\gamma}{c} \cdot \mathbf{lg}(T)^4 \implies \left\|\overline{\mathbf{ll}}(\mathbf{Bl}(B, j)x + y, j-1)\right\|_1 \geq \gamma \left\|\overline{\mathbf{ll}}(y, j-1)\right\|_1. \tag{25}$$

Let U be the vector space $\left\{\overline{\mathbf{ll}}(z, j-1) \mid z \in V\right\}$. Now, let N_z be an ϵ-net in ℓ_1 for the set $\left\{z \in U \mid \|z\|_1 = 1\right\}$ for $\epsilon = (1-\gamma)/(1+257\mu^{-1/2})$, and N_x and ϵ_1-net in ℓ_2 for the ℓ_2-ball of radius $\frac{\gamma}{c} \cdot \mathbf{lg}(T)^4$ in $\mathbb{R}^{2^{j-1}-1}$ for $\epsilon_1 = \epsilon \cdot \mathbf{lg}(T)^4$. N_z and N_x can be chosen so that $|N_z| \cdot |N_x| \leq \exp\left(c' \cdot 2^j\right)$ where $c' = c'(\gamma) > 0$. Let $\gamma' = \gamma + (1 + 256\mu^{-1/2})\epsilon < 1$. We now have, for any $z \in N_z$ and $x \in N_x$,

$$\left\|\overline{\mathbf{ll}}(\mathbf{Bl}(B, j)x + z, j-1)\right\|_1 = \sum_{i=1}^{2^{j-2}} \sum_{l=1}^{k} \left|X_{i,l} + z_{i,l}\right|, \tag{26}$$

where, as before, $X_{i,l}$ are independent mean zero normal variables with variances $\sigma_{i,l}$ as in eq. (19). In preparation to apply Theorem A.7, we now estimate

$$\begin{aligned}
\sum_{i=1}^{2^{j-2}} \sum_{\ell=1}^{k} \sigma_{i,l} &\geq \frac{1}{\mathbf{lg}(T)^4} \sum_{i=1}^{2^{j-2}} \sqrt{\sum_{s=2^{j-1}}^{2^j-1} \frac{x_s^2}{s^\mu i^{1-\mu}(s-i+1)}} \\
&\geq \frac{1}{\|x\|_2 \, \mathbf{lg}(T)^4} \sum_{s=2^{j-1}}^{2^j-1} \frac{x_s^2}{s^{\mu/2}} \sum_{i=1}^{2^{j-2}} \frac{1}{i^{(1-\mu)/2}\sqrt{s-i+1}} \\
&\geq \frac{\|x\|_2}{\mathbf{lg}(T)^4} 2^{-j(1+\mu)/2} \sum_{i=1}^{2^{j-2}} \frac{1}{i^{(1-\mu)/2}} \\
&\geq c_0 \text{ for some fixed constant } c_0(\gamma, \mu).
\end{aligned}$$

Here, the second inequality uses the concavity of the square root function, the last that $x \in N_x$ so that $\|x\|_2 = \gamma\,\mathbf{lg}(T)^4/c$, and the rest are elementary estimates. Now, using the upper bound on $\sum \sigma_{i,l}^2$ obtained in eq. (20) (while remembering that the vector x in that calculation needs to be scaled to have length $\gamma\,\mathbf{lg}(T)^4/c$ instead of 1), we can apply Theorem A.7 to get that for some constant $c'' = c''(\gamma) > 0$,

$$\mathbb{P}\left[\left\|\overline{\mathbf{ll}}(\mathbf{Bl}(B, j)x, j-1) + z\right\|_1 < \gamma' \|z\|_1\right] \leq \exp\left(-c'' k \cdot 2^j\right).$$

Taking a union bound over the product $N_z \times N_x$ of the two nets, using eq. (25) and recalling that $\gamma' = \gamma + (1 + 256\mu^{-1/2})\epsilon$ and that N_z and N_x are ϵ and $\epsilon \cdot \mathbf{lg}(T)^4$ nets respectively, we deduce that for some constant $D = D(\gamma) > 0$

$$\mathbb{P}\left[\exists x \in R^{2^{j-1}}, z \in U \text{ s.t. } \|z\|_1 = 1 \text{ and } \left\|\overline{\mathbf{ll}}(\mathbf{Bl}(B, j)x, j-1) + z\right\|_1 < \gamma\right] \leq \exp\left(-Dk \cdot 2^j\right)$$

when $k \geq c_1$ for c_1 large enough. The result now follows. ■

Combining the results of Corollary IV.7 and Lemma IV.8, we get

Lemma IV.9. *There exists a positive constant C such that for any $\gamma \in (0, 1)$ there exist positive constants $c_1 = c_1(\gamma), c_2 = c_2(\gamma)$ such that for any integers $j \geq 2$ and any $k \geq c_1$, the following is true. Let V be an arbitrary subspace of dimension at most $2^{j-1} - 1$. Then,*

$$\mathbb{P}\left[\exists x \in \mathbb{R}^{2^{j-1}}, y \in V \text{ s. t. } \left\|\overline{\mathbf{ll}}(\mathbf{Bl}(B, j)x + y, j-1)\right\|_1 < \max\left\{C \|x\|_2 / \mathbf{lg}(T)^4, \gamma \left\|\overline{\mathbf{ll}}(y, j-1)\right\|_1\right\}\right] \leq \exp\left(-c_2 k \cdot 2^j\right).$$

We are now ready to prove the main theorem of this section.

Theorem IV.10. *For any $\kappa \in (0, 1)$ there exist positive constant c_0, c_1 and c_2 such that the following is true. Let T be any positive integer and set $\tau := \mathbf{lg}(T)$. For any rate parameter $k \geq c_1$ and $j_0 \in [1, \tau]$,*

$$\mathbb{P}_{B\sim\mathcal{B}(T,k)}\left[\exists x \in \mathbb{R}^T \text{ s. t. } \left\|\overline{\mathbf{ll}}(Bx, \tau)\right\|_1 < c_0 \kappa^{\tau - j_0} \|\mathbf{cl}(x, \tau, j_0)\|_2 / \tau^4\right] \leq \exp\left(-c_2 k \cdot 2^{j_0 - 1}\right).$$

Proof of Theorem IV.10: Let $c_0(\kappa)$ be a fixed constant to be determined later. For $j_0 \leq j \leq \tau$, let $\mathcal{E}_j$ be the event that

$$\left\|\overline{\mathbf{ll}}(\mathbf{Cl}(B, j)x, j)\right\|_1 \geq c_0 \kappa^{j - j_0} \|\mathbf{cl}(x, j, j_0)\|_2 / \tau^4 \quad \forall x \in \mathbb{R}^{2^j - 1}.$$

Corollary IV.7 (or, in the case $j_0 = 1$, a direct calculation identical to that in Lemma IV.6) shows that if c_0 is a small enough positive constant, there exist positive constants c', c'' (independent of j_0) such that $\mathbb{P}\left[\neg\mathcal{E}_{j_0}\right] \leq \exp\left(-c' k 2^{j_0 - 1}\right)$ for all large enough constant k (to show this, one chooses the vector space V in the statement of Corollary IV.7 to be $\mathbf{Range}(\mathbf{Cl}(B, j-1))$). Now, let

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIT.2019.2919632, IEEE Transactions on Information Theory

$C > 0$ be as in Lemma IV.9. We choose c_0 to be small enough so that there exists $\gamma \in (0,1)$ satisfying

$$\kappa = \frac{\gamma}{\sqrt{1+(c_0/C)^2}}. \tag{27}$$

The claim of the theorem then follows if there exist positive constants c_1, c_2 such that for $k \geq c_1$, $\mathbb{P}[\neg\mathcal{E}_\tau] \leq \exp\left(-c_2 k 2^{j_0-1}\right)$. We have already established this above for $j = j_0$. We will show now that there exists a constant $c_2 > 0$ such that for large enough constant k and $j \geq 2$,

$$\mathbb{P}\left[\neg\mathcal{E}_j | \mathcal{E}_{j-1}\right] \leq \exp\left(-c_2 k \cdot 2^{j-1}\right). \tag{28}$$

This will establish the claim if c_1 is chosen large enough that $\exp(-c_2 c_1) \leq \frac{1}{2}$, since in that case $k \geq c_1$ implies

$$\mathbb{P}[\neg\mathcal{E}_\tau] \leq \mathbb{P}\left[\neg\mathcal{E}_{j_0}\right] + \sum_{j=j_0+1}^{\tau} \mathbb{P}\left[\neg\mathcal{E}_j|\mathcal{E}_{j-1}\right]$$
$$\leq \sum_{j=j_0}^{\tau} \exp\left(-c_2 k \cdot 2^{j-1}\right) \leq 2\exp\left(-c_2 k 2^{j_0-1}\right).$$

We now establish eq. (28). Fix $j \geq j_0 + 1$, and assume $\mathcal{E}_{j-1}$ occurs. Note that

$$\mathbf{Cl}(B,j)x = \mathbf{Bl}(B,j)\mathbf{bl}(x,j) + \mathbf{Cl}(B,j-1)\mathbf{cl}(x,j-1),$$

so that we can apply Lemma IV.9 with $V = \mathbf{Range}(\mathbf{Cl}(B,j-1))$ and γ as chosen above to find $c_1, c_2 > 0$ (not depending upon j) such that when $k \geq c_1$, it holds with probability at least $1-\exp\left(-c_2 k \cdot 2^{j-1}\right)$ that

$$\frac{\left\|\overline{\mathbf{ll}}(\mathbf{Cl}(B,j)x,j)\right\|_1^2}{\|\mathbf{cl}(x,j,j_0)\|_2^2} \geq \frac{1}{\tau^8}\max\left\{C^2\frac{\|\mathbf{bl}(x,j)\|_2^2}{\|\mathbf{cl}(x,j,j_0)\|_2^2}, \frac{c_0^2\gamma^2\kappa^{2(j-j_0)}}{\kappa^2}\frac{\|\mathbf{cl}(x,j-1,j_0)\|_2^2}{\|\mathbf{cl}(x,j,j_0)\|_2^2}\right\} \quad \forall x \neq 0 \in \mathbb{R}^{2^j-1}. \tag{29}$$

Since

$$\min_{0\leq\eta\leq1}\max\{a\eta, b(1-\eta)\} = \frac{ab}{a+b}, \text{ for all } a,b > 0,$$

the guarantee in eq. (29) implies that for all $x \neq 0$ in $\mathbb{R}^{2^j-1}$:

$$\frac{\left\|\overline{\mathbf{ll}}(\mathbf{Cl}(B,j)x,j)\right\|_1}{\|\mathbf{cl}(x,j,j_0)\|_2} \geq \frac{c_0\kappa^{j-1-j_0}}{\tau^4}\cdot\frac{\gamma}{\sqrt{1+(\gamma c_0\kappa^{j-j_0-1}/C)^2}} \geq \frac{c_0\kappa^{j-j_0}}{\tau^4},$$

where the last inequality uses eq. (27) and the fact that $\gamma, \kappa \leq 1$. We thus have $\mathbb{P}\left[\mathcal{E}_j|\mathcal{E}_{j-1}\right] \geq 1 - \exp\left(-c_2 k \cdot 2^{j-1}\right)$, as required. ■

We now use the information about B derived above to show that M comes very close to satisfying the conditions asked of an encoding matrix in Theorem II.1. In particular, Corollary IV.11 implies that M satisfies these constraints at any given fixed time T. Corollary IV.12 then shows that encoding using M actually satisfies, at *each* time t up to the total time T for which communication lasts, a slightly weaker set of conditions which allow for the decoding of all but a poly $(\log t)$ sized suffix of the signal. Finally, we obtain the full statement of Theorem II.1 in Section V by slightly modifying M to handle the suffix differently.

Corollary IV.11 (Invertibility of M). *For any $\delta \in (0, \frac{1}{2})$, there exist constants c_0, c_1, c_2 such that the following is true. Let T be a fixed integer, and let $\tau = \mathbf{lg}(T)$. Let $k \geq c_1$ be a rate parameter. Then, for M sampled according to $\mathcal{A}_{T,k}$, we have*

$$\mathbb{P}\left[\exists x \in \mathbb{R}^T \text{ s.t. } \|Mx\|_{\dagger_\mu(kT)} < c_0 2^{\delta j_0} 2^{\tau(1/2-\delta)}\|\mathbf{cl}(x,\tau,j_0)\|_{\star_\mu(T)}/\tau^4\right] \leq \exp\left(-c_2 k \cdot 2^{j_0-1}\right)$$

for all $1 \leq j_0 \leq \tau$. Here, for the purposes of computing the $\|\cdot\|_{\star_\mu(T)}$-norm, $\mathbf{cl}(x,\tau,j_0)$ is seen as a vector in $\mathbb{R}^T$ whose last $2^{j_0-1}-1$ coordinates are 0.

Proof: Using the same calculation as in eq. (16), we see that if $M \sim \mathcal{A}_{T,k}$, and B is constructed from M as defined in eq. (17), then $B \sim \mathcal{B}_{T,k}$ and

$$\inf\frac{\|Mx\|_{\dagger_\mu(kT)}}{\|\mathbf{cl}(x,\tau,j_0)\|_{\star_\mu(T)}} \geq 2^{\tau/2-1}\inf\frac{\|By\|_1}{\|\mathbf{cl}(y,\tau,j_0)\|_2}. \tag{30}$$

Given $\delta \in \left(0, \frac{1}{2}\right)$, we choose $\kappa = 2^{-\delta}$. After applying Theorem IV.10 with this value of κ and using eq. (30), we then find positive constants c_0, c_1, c_2 (depending upon κ) such that when $k \geq c_1$, the matrix M satisfies

$$\|Mx\|_{\dagger_\mu(kT)} \geq c_0 2^{\delta j_0+\tau(1/2-\delta)}\|\mathbf{cl}(x,t,j_0)\|_{\star_\mu(T)}/\tau^4 \;\forall x$$

with probability at least $1 - \exp\left(-c_2 k \cdot 2^{j_0-1}\right)$. ■

Corollary IV.12 (Invertibility of principal submatrices of M). *For any $\delta \in (0, \frac{1}{2})$, there exist constants c_0, c_1 such that the following is true. Let T be a positive integer, and set $\tau := \mathbf{lg}(T)$, $j_0(n) := \left\lceil\frac{4\,\mathbf{lg}(\mathbf{lg}(n))}{\delta}\right\rceil = \Theta(\log\log n)$. Then, for any rate parameter $k \geq c_1$, there exists a k-lower triangular matrix M satisfying the following conditions. (Here, for $1 \leq n \leq T$ and a k-lower triangular matrix A, A_n denotes the k-lower triangular matrix* *obtained by taking the first n columns of A and the first kn rows).*

1) **Submatrices of M have small operator norm***:* $\|M_n\|_{2\to 2} \le 1$ *for* $1 \le n \le T$.
2) **Submatrices of M are robustly invertible with respect to the past***: for* $1 \le n \le T$,

$$\|M_n x\|_{\dagger_\mu(kn)} \ge c_0 n^{(1/2-\delta)} \|\mathbf{cl}(x, \mathbf{lg}(n), j_0(n))\|_{\star_\mu(n)} .$$

for all $x \in \mathbb{R}^n$.

Proof: Let $M \sim \mathcal{A}_{T,k}$. We will show that when $k \ge c_1$ for c_1 large enough, then M satisfies both the above conditions with positive probability. We start by noting that Lemma IV.4 implies that item 1 is satisfied with probability at least $\frac{1}{2}$, as long as c_1 is large enough. We now turn to item 2.

Each sub-matrix M_n of M is a sample from $\mathcal{A}_{n,k}$. From Corollary IV.11, we therefore find constants c_0, c_1' and c_2' such that as long as $k \ge c_1'$, we have

$$\begin{aligned}\mathbb{P}\Big[\exists x \in \mathbb{R}^n, &\|M_n x\|_{\dagger_\mu(kn)} \\ &< \frac{c_0 2^{\delta j_0(n)} 2^{\mathbf{lg}(n)(1/2-\delta)}}{\mathbf{lg}(n)^4} \|\mathbf{cl}(x, \mathbf{lg}(n), j_0(n))\|_{\star_\mu(n)}\Big] \\ &\le e^{-c_2' k 2^{j_0(n)}} \le e^{-c_2' k \,\mathbf{lg}(n)^8}, \quad (31)\end{aligned}$$

where the last inequality uses the value of j_0. (Note that, strictly speaking, we can only apply Corollary IV.11 when $j_0(n) \le \mathbf{lg}(n)$. However, when $j_0(n) > \mathbf{lg}(n)$, eq. (31) is vacuously satisfied since in that case, $\mathbf{cl}(x, \mathbf{lg}(n), j_0(n))$ is an empty vector for all $x \in \mathbb{R}^n$.) Now, when $k \ge c_1$ where c_1 is chosen to be large enough that $c_2' c_1 \ge 10$ and $c_1 \ge c_1'$, we can substitute the value of $j_0(n)$ in eq. (31) to find that for all $1 \le n \le T$

$$\begin{aligned}\mathbb{P}\Big[\exists x \in \mathbb{R}^n, &\|M_n x\|_{\dagger_\mu(kn)} \\ &< c_0 2^{\mathbf{lg}(n)(1/2-\delta)} \|\mathbf{cl}(x, \mathbf{lg}(n), j_0(n))\|_{\star_\mu(n)}\Big] \\ &\le e^{-10\,\mathbf{lg}(n)^8} \le \frac{1}{10n^2}.\end{aligned}$$

Taking a union bound over $1 \le n \le T$ and using $\sum_{n\ge 1}(1/n^2) < 2$, we now see that M satisfies both conditions with probability at least $\frac{1}{2} - \frac{1}{5} = \frac{3}{10}$. ∎

V. The encoding matrix

Corollary IV.12 already contains most of the information necessary for the construction of our encoding matrix. Indeed, the matrix M guaranteed there can already decode all but the last poly$(\log t)$ entries at any time t with the required guarantee. To get the final guarantee, we only need to make our encoding systematic by including a copy of the input symbols. More precisely, given a k-lower triangular matrix of the form guaranteed by Corollary IV.12, we construct a $(k+1)$-lower triangular matrix C which at time t produces the k symbols that would have been output by M, followed by the current input x_t. In symbols, this means that entries of C can be written as follows (we use again the block notation for row indices of k-lower triangular matrices introduced in Section II):

$$C_{(i,l),j} = \begin{cases} M_{(i.l),j} & \text{when } 1 \le l \le k, \\ 1 & \text{when } l = k+1, \text{ and} \\ 0 & \text{otherwise} \end{cases} \quad (32)$$

We note the following simple consequences of this definition:

1) Let $y = Mx$ for $x \in \mathbb{R}^T$. Then

$$\begin{aligned}&\|Cx\|_{\dagger_\mu((k+1)T)} \\ &= \sum_{\substack{1\le i\le T\\ 1\le l\le k}} |y_{(i,l)}| \left(\frac{(k+1)T}{(k+1)(T-i+1)-l+1}\right)^{(1-\mu)/2} \\ &\qquad + \sum_{i=1}^{T} |x_i| \left(\frac{(k+1)T}{(k+1)(T-i+1)-k}\right)^{(1-\mu)/2} \\ &\ge \frac{\|y\|_{\dagger_\mu(kT)}}{3} + \sum_{i=1}^{T} |x_i| \left(\frac{T}{T-i+1}\right)^{(1-\mu)/2} . \quad (33)\end{aligned}$$

2) For every $x \in \mathbb{R}^T$,

$$\|Cx\|_2^2 = \|Mx\|_2^2 + \|x\|_2^2. \quad (34)$$

We can now prove Theorem II.1 which we restate here for easy reference.

Theorem (The encoding matrix, restatement of Theorem II.1). *For any $\mu \in (0,1]$ and $\delta \in (0, \frac{1}{2})$, there exist constants c, c_1 such that the following is true. Let $T \ge 3$ be any integer. For a rate parameter k satisfying $k \ge c_1$, there exists a matrix C satisfying the following conditions. (Here, for $1 \le n \le T$ and a k-lower triangular matrix A, A_n denotes the leading principal sub-matrix of A consisting of its first n columns and kn rows).*

1) **Submatrices of C have small operator norm***:* $\|C_n\|_{2\to 2} \le 1$ *for* $1 \le n \le T$.
2) **Submatrices of C_n are robustly invertible***: for* $1 \le n \le T$,

$$\|C_n x\|_{\dagger_\mu(kn)} \ge c n^{(1/2-\delta)} \|x\|_{\star_\mu(n)} \text{ for all } x \in \mathbb{R}^n.$$

Proof: Applying Corollary IV.12 with μ and δ, we obtain c_0, c_1, j_0 and a k-lower triangular matrix M (for a $k \ge c_1$) as in the corollary. We define the $k+1$-lower triangular matrix C using M as done in eq. (32) above, and set $C = \frac{1}{\sqrt{2}}C$. Item 1 now follows from item 1 and eq. (34).

For item 2, we use eq. (33) followed by item 2 of Corollary IV.12 to get (with $c' := c_0/3$)

$$\begin{aligned}\sqrt{2}\,\|C_n x\|_{\dagger_\mu(kn)} &\geq c' n^{(1/2-\delta)}\,\|\mathbf{cl}(x, \mathbf{lg}(n), j_0(n))\|_{\star_\mu(n)} \\ &\quad + \sum_{i=1}^{n}\left(\frac{n}{n-i+1}\right)^{(1-\mu)/2}|x_i|, \\ &\qquad \text{for all } x \in \mathbb{R}^n, \end{aligned} \tag{35}$$

where $\mathbf{lg}(n) := \lceil \lg(n+1) \rceil$, and j_0 is as in Corollary IV.12 and satisfies $j_0(n) = O(\log\log n)$. We now estimate the second term as follows:

$$\begin{aligned}&\sum_{i=1}^{n}\left(\frac{n}{n-i+1}\right)^{(1-\mu)/2}|x_i| \\ &\geq \sum_{i=n-2^{j_0(n)}+2}^{n}\frac{\sqrt{n}}{\sqrt{n-i+1}}\cdot\left(\frac{n-i+1}{n}\right)^{\mu/2}|x_i| \\ &\geq \frac{\sqrt{n}}{O(\mathrm{poly}\,(\log n))}\sqrt{\sum_{i=n-2^{j_0(n)}+2}^{n}\left(\frac{n-i+1}{n}\right)^{\mu}|x_i|^2} \\ &\geq c'' n^{(1/2-\delta)}\,\|\mathbf{cl}(x, j_0(n)-1)\|_{\star_\mu(n)},\end{aligned}$$

for some fixed positive constant $c'' = c''(\delta)$. Item 2 now follows by substituting this into eq. (35) and using the fact that

$$\begin{aligned}&\|\mathbf{cl}(x, j_0(n)-1)\|_{\star_\mu(n)} + \|\mathbf{cl}(x, \mathbf{lg}(n), j_0(n))\|_{\star_\mu(n)} \\ &\geq \sqrt{\|\mathbf{cl}(x, j_0(n)-1)\|^2_{\star_\mu(n)} + \|\mathbf{cl}(x, \mathbf{lg}(n), j_0(n))\|^2_{\star_\mu(n)}} \\ &= \|x\|_{\star_\mu(n)}.\end{aligned}$$

■

VI. Comparing the online and block settings: A lower bound

As noted in the introduction, when compared with the block coding setting, we lose an extra $\Theta(t^\delta)$ factor in the robust invertibility guarantee in the online setting. A natural question therefore is whether it is possible to get rid of this loss and obtain a guarantee as strong as the block coding setting (eq. (7)) in the online setting as well. We now prove Theorem II.2, which was stated in the introduction as a partial answer to this question. We restate the theorem here for ease of reference.

Theorem VI.1. *Fix $\mu \in (0,1]$, $c_0 > 0$ and a positive integer k. There exists a constant $\tau = \tau(\mu, c_0, k)$ such that the following is true. If C is a $kT \times T$ k-lower triangular matrix such that for all $t \in [T]$ the submatrix C_t of C satisfies*

$$\|C_t x\|_{\dagger_\mu(kt)} \geq c_0 t^{1/2}\,\|x\|_{\star_\mu(t)} \text{ for all } x \in \mathbb{R}^t, \tag{36}$$

then there exists a non-zero $x \in \mathbb{R}^T$ for which

$$\|Cx\|_2^2 \geq \tau\,\|x\|_2^2\sum_{i=1}^{T}\frac{1}{i} \geq (\tau\log T)\cdot\|x\|_2^2.$$

In particular, x can be taken to be the unit pulse at time 1.

Proof: When $x = e_1$ is the unit pulse at time 1, we have $\left\|x_{[t]}\right\|_{\star_\mu(t)} = 1$ for all $\mu \in (0,1]$ and $1 \leq t \leq T$. Let $z \in \mathbb{R}^{kT}$ be the vector such that $z_i := \left|C_{i,1}\right|$. Then, for $x = e_1$, we have

$$\begin{aligned}\|Cx\|_2 &= \|z\|_2, \text{ and} \\ \left\|C_t x_{[t]}\right\|_{\dagger_\mu(kt)} &= \sum_{i=1}^{kt} z_i\cdot\left(\frac{kt}{kt-i+1}\right)^{(1-\mu)/2}.\end{aligned}$$

It therefore follows that when the guarantees of eq. (36) are enforced, the objective value of the following convex program is a lower bound on $\|Ce_1\|_2$:

$$\begin{aligned}\text{min} \quad & \|z\|_2^2 \\ \text{subject to} \quad & \sum_{i=1}^{kt} z_i f_{it} \geq \gamma_t, \quad 1 \leq t \leq T \\ & z_i \geq 0, \quad 1 \leq i \leq kT.\end{aligned} \tag{37}$$

Here

$$\gamma_t := \frac{c_0 t^{\mu/2}}{k^{(1-\mu)/2}}, \text{ and } f_{it} := \frac{1}{(kt-i+1)^{(1-\mu)/2}}.$$

We will lower bound the objective value of this program by providing a feasible solution to its dual program.[2] The dual program is given as

$$\begin{aligned}\text{sup} \quad & g(\lambda, \nu) \\ \text{subject to} \quad & \lambda_i \geq 0, \quad 1 \leq i \leq T \\ & \nu_i \geq 0, \quad 1 \leq i \leq kT\end{aligned} \tag{38}$$

where

$$g(\lambda, \nu) := \inf_{z \in \mathbb{R}^{kT}} \|z\|_2^2 - \sum_{t=1}^{T}\lambda_t\left(\sum_{i=1}^{kt} z_i f_{it} - \gamma_t\right) - \sum_{i=1}^{kT}\nu_i z_i.$$

[2]Note that since the primal objective function is convex in z and the since the primal constraints admit a feasible point where all constraints are satisfied with a strict inequality, Slater's constraint qualifications are satisfied. Thus, strong duality also holds, though it is not required for our purposes.

The expression to be minimized in the definition of g is a convex function of z, and hence we can perform the minimization by equating the gradient to 0. This yields

$$g(\lambda,\nu) = \sum_{t=1}^{T} \lambda_t \gamma_t - \frac{1}{4}\sum_{t=1}^{kT} \Lambda_i^2 - \frac{1}{4}\sum_{i=1}^{kT} \nu_i^2 - \frac{1}{2}\sum_{t=1}^{kT} \Lambda_t \nu_t, \tag{39}$$

where, for $1 \le i \le kT$,

$$\Lambda_i := \sum_{t=\lceil i/k\rceil}^{T} \lambda_t f_{it} = \sum_{t=\lceil i/k\rceil}^{T} \frac{\lambda_t}{(kt-i+1)^{(1-\mu)/2}}.$$

Note that when λ and ν are non-negative, g is non-increasing in the ν_i, and hence we can set $\nu_i = 0$ (for $1 \le i \le kT$) without changing the optimal value of the program in (38). We now consider the following dual feasible solution:

$$\begin{aligned} \lambda_t &= \frac{a_0}{t^{1+\mu/2}} && \text{for } 1 \le t \le T, \text{ and} \\ \nu_i &= 0 && \text{for } 1 \le i \le kT, \end{aligned} \tag{40}$$

where a_0 is a positive constant to be chosen later. To lower bound the dual objective value, we now upper bound the Λ_i given this choice of the λ_t. For positive integers i and j such that $1 \le j \le T$ and $k(j-1)+1 \le i \le kj$, we have

$$\begin{aligned} \Lambda_i &= a_0 \sum_{t=j}^{T} \frac{1}{t^{1+\mu/2}(kt-i+1)^{(1-\mu)/2}} \\ &\le a_0 \sum_{t=j}^{T} \frac{1}{t^{1+\mu/2}\cdot(kt-kj+1)^{(1-\mu)/2}} \\ &\le \frac{a_0}{j^{1+\mu/2}} + \frac{a_0}{k^{(1-\mu)/2}} \sum_{t=1}^{T-j} \frac{1}{(t+j)^{1+\mu/2}\cdot t^{(1-\mu)/2}}. \end{aligned} \tag{41}$$

The last term above can also be shown to be $O(\sqrt{j})$, as follows:

$$\begin{aligned} &\sum_{t=1}^{T-j} \frac{1}{(t+j)^{1+\mu/2}\cdot t^{(1-\mu)/2}} \\ &\le \sum_{t=1}^{\infty} \frac{1}{(t+j)^{1+\mu/2}\cdot t^{(1-\mu)/2}} \\ &= \sum_{l=1}^{\infty} \sum_{t=(l-1)j+1}^{lj} \frac{1}{(t+j)^{1+\mu/2}\cdot t^{(1-\mu)/2}} \\ &\le \sum_{l=1}^{\infty} \frac{1}{(lj)^{1+\mu/2}} \sum_{t=(l-1)j+1}^{lj} \frac{1}{t^{(1-\mu)/2}} \\ &\le \frac{2}{1+\mu} \sum_{l=1}^{\infty} \frac{j^{(1+\mu)/2}}{(lj)^{1+\mu/2}} \cdot \left(l^{(1+\mu)/2} - (l-1)^{(1+\mu)/2}\right) \\ &\le \frac{2}{1+\mu}\cdot\frac{1}{\sqrt{j}} \sum_{l=1}^{\infty} \frac{1}{l^{1+\mu/2}} \le \frac{2(2+\mu)}{\mu(1+\mu)}\cdot\frac{1}{\sqrt{j}}. \end{aligned}$$

Here, the third and the last inequalities use Fact VI.2 (note that $\mu > 0$, so only the case $\alpha \ne 1$ of Fact VI.2 is used), and the fourth uses the fact that when $\beta \in (0,1]$ and n is a non-negative integer, $(n+1)^\beta - n^\beta \le 1$. Plugging the above estimate into eq. (41), we get that when j is a positive integer such that $k(j-1)+1 \le i \le kj$,

$$\Lambda_i \le \frac{a_0 c'}{\sqrt{j}},$$

where $c' = c'(\mu,k) := 1 + \frac{2(2+\mu)}{\mu(1+\mu)\cdot k^{(1-\mu)/2}}$. Thus, at the feasible solution in eq. (40), the dual objective value is

$$\begin{aligned} g(\lambda,\mathbf{0}) &= \sum_{t=1}^{T} \lambda_t \gamma_t - \frac{1}{4}\sum_{i=1}^{kT} \Lambda_i^2 \\ &= \frac{a_0 c_0}{k^{(1-\mu)/2}} \sum_{t=1}^{T} \frac{1}{t} - \frac{1}{4}\sum_{i=1}^{kT} \Lambda_i^2 \\ &\ge a_0 \left(\frac{c_0}{k^{(1-\mu)/2}} - \frac{k a_0 c'^2}{4}\right) \sum_{t=1}^{T} \frac{1}{t}, \end{aligned}$$

where the last inequality uses the above estimate on Λ_i. Thus, by choosing $a_0 = a_0(\mu, c_0, k)$ to be $\frac{2c_0}{k^{(3-\mu)/2} c'^2}$, we find that there exists a positive constant $\tau = \tau(\mu, c_0, k)$ such that the dual objective value is at least $\tau \sum_{t=1}^{T} \frac{1}{t}$. By weak duality, this is also a lower bound on the objective value of the primal program in (37). By the discussion preceding (37), this completes the proof. ■

The proof of Theorem VI.1 uses the following elementary estimate.

Fact VI.2. *Let $a < b$ be positive integers and α a positive real number. Then,*

$$\sum_{i=a+1}^{b} i^{-\alpha} \le \int_a^b x^{-\alpha} dx = \begin{cases} \frac{b^{1-\alpha} - a^{1-\alpha}}{1-\alpha} & \text{when } \alpha \ne 1, \\ \log(b/a) & \text{when } \alpha = 1. \end{cases}$$

Appendix

In this section we collect concentration bounds for the $\|\cdot\|_1$-norms of Gaussian vectors with independent but not identically distributed entries. The bounds here are adaptations of standard arguments and results in the literature on Gaussian concentration to our setting.

We begin with the following elementary fact and a consequence, and then proceed to bounds for the lower tail of the $\|\cdot\|_1$ norm of Gaussian vectors with independent but not identically distributed entries (in Theorems A.4 and A.7).

Fact A.1 (Gaussian tail). *If $X \sim \mathcal{N}(0, \sigma^2)$, then for*

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIT.2019.2919632, IEEE Transactions on Information Theory

$t > 0$,

$$\mathbb{P}[X \geq t] = \frac{1}{\sqrt{2\pi\sigma^2}} \int_t^\infty \exp\left(-x^2/(2\sigma^2)\right) dx < \frac{\sigma}{t \cdot \sqrt{2\pi}} \exp\left(-\frac{t^2}{2\sigma^2}\right).$$

Corollary A.2 (Upper tail of the $\|\cdot\|_1$-norm). *Let $X \sim \mathcal{N}\left(0, \operatorname{diag}\left((\sigma_i^2)_{i=1}^n\right)\right)$. Then, for any $t > 0$ and $c > 0$, we have*

$$\mathbb{P}[\|X\|_1 > t] \leq \exp\left(-ct + n\log 2 + \frac{c^2}{2}\sum_{i=1}^n \sigma_i^2\right).$$

In particular, choosing $c = \frac{t}{\sum_{i=1}^n \sigma_i^2}$ and then $t = \alpha\sqrt{n}$, we have

$$\mathbb{P}\left[\|X\|_1 > \alpha\sqrt{n}\right] \leq \exp\left(-n\left(\frac{\alpha^2}{2\sum_{i=1}^n \sigma_i^2} - \log 2\right)\right).$$

Proof: For $Y \sim \mathcal{N}(0, \sigma^2)$, we have, for any $c > 0$, $\mathbb{E}[\exp(c|Y|)] \leq 2\exp(c^2\sigma^2/2)$. Thus we have, for any $c > 0$,

$$\begin{aligned}\mathbb{P}[\|X\|_1 > t] &= \mathbb{P}[\exp(c\|X\|_1) > \exp(ct)] \\ &\leq \exp(-ct)\prod_{i=1}^n \mathbb{E}[\exp(c|X_i|)] \\ &\leq \exp\left(-ct + n\log 2 + \frac{c^2}{2}\sum_{i=1}^n \sigma_i^2\right).\end{aligned}$$

■

A. The lower tail of the $\|\cdot\|_1$-norm

We now state two concentration results for the lower tail of the ℓ_1 norm of Gaussian vectors with independent but not identically distributed entries. The first (Theorem A.4) deals with the lower tail for mean 0 vectors (in other words, this is an upper bound on small-ball probability), while the second (Theorem A.7) considers the concentration around the ℓ_1 norm of the mean for vectors with non-zero mean.

Lemma A.3. *Let $X \sim \mathcal{N}\left(0, \operatorname{diag}\left((\sigma_i^2)_{i=1}^n\right)\right)$. Then, for any $t > 0$ and $c > 0$, we have*

$$\mathbb{P}[\|X\|_1 < t] \leq \exp(ct + \sum_{i=1}^n \nu(c^2\sigma_i^2)),$$

where for $x \geq 0$,

$$\nu(x) := \frac{x}{2} - \frac{1}{2}\log\frac{\pi}{2} + \log\int_{\sqrt{x}}^\infty \exp(-t^2/2)dt \leq \frac{1}{2}\min\left\{0, -\log\frac{\pi x}{2}\right\}.$$

Proof: Let $X = (X_1, X_2, \ldots, X_n)$ where $X_i \sim \mathcal{N}(0, \sigma_i^2)$. For any $c > 0$, we have

$$\begin{aligned}\mathbb{P}[\|X\|_1 < t] &= \mathbb{P}[\exp(-c\|X\|_1) > \exp(-ct)] \\ &\leq \exp(ct) \cdot \prod_{i=1}^n \mathbb{E}[\exp(-c|X_i|)].\end{aligned} \tag{42}$$

The first claim now follows since for $Y \sim \mathcal{N}(0, \sigma^2)$, we have

$$\begin{aligned}\mathbb{E}[\exp(-c|Y|)] &= \sqrt{\frac{2}{\pi\sigma^2}}\int_0^\infty \exp\left(-cy - \frac{y^2}{2\sigma^2}\right) dy \\ &= \sqrt{\frac{2}{\pi}}\exp(c^2\sigma^2/2) \\ &\quad \cdot \int_0^\infty \exp\left(-(z + c\sigma)^2/2\right) dz \\ &= \sqrt{\frac{2}{\pi}}\exp(c^2\sigma^2/2)\int_{c\sigma}^\infty \exp\left(-z^2/2\right) dz \\ &= \exp\left(\nu(c^2\sigma^2)\right).\end{aligned}$$

The definition of ν implies that $\nu(x) \leq 0$ for all positive x. Now, using Fact A.1, we have

$$\begin{aligned}\nu(x) &\leq -\frac{1}{2}\log\left(\frac{\pi}{2}\right) + \frac{x}{2} + \log\left(\frac{1}{\sqrt{x}}\exp(-x/2)\right) \\ &= -\frac{1}{2}\log\left(\frac{\pi x}{2}\right), \text{ for all } x \geq 0.\end{aligned}$$

Thus, we obtain $\nu(x) \leq \frac{1}{2}\min\left\{0, -\log\frac{\pi x}{2}\right\}$. ■

Theorem A.4 (Lower tail of the $\|\cdot\|_1$-norm). *There exists a positive constant γ such that the following is true. Let $X \sim \mathcal{N}\left(0, \operatorname{diag}\left((\sigma_i^2)_{i=1}^n\right)\right)$, S an arbitrary subset of $[n]$. Define $G := GM\left((\sigma_i)_{i\in S}\right)$ to be the geometric mean of the σ_i for $i \in S$. Then, for all $\tau \geq 0$ and*

$$t \leq \tau\gamma G|S|$$

we have

$$\mathbb{P}[\|X\|_1 < t] \leq (\tau)^{|S|}.$$

In particular, given α, if there exists a set S for which $G \geq \alpha/|S|$, then for all $\tau \geq 0$,

$$\mathbb{P}[\|X\|_1 < \tau\gamma \cdot \alpha] \leq \tau^{|S|}.$$

Proof: Set $\gamma = \sqrt{\pi/2}/e$. We now use Lemma A.3 and the upper bound on the function ν defined there, after exercising our choice for c by setting $c = |S|/t$. We then have

$$\begin{aligned}\mathbb{P}\left[\|X\|_1 < t\right] &\leq \exp\left(ct + |S|\log(\sqrt{2/\pi})\right.\\ &\qquad\left. - |S|\log c - |S|\log G\right)\\ &= \exp\left(|S|\left(-\log\gamma - \log|S| + \log t - \log|G|\right)\right)\\ &= \left(\frac{t}{\gamma G|S|}\right)^{|S|}.\end{aligned}$$

Substituting $t = \tau\gamma|G|S$, we get the claimed result. ∎

The standard fact below shows that it is sufficient to consider mean 0 vectors in the setting of Theorem A.4. We include a proof for completeness.

Fact A.5 (**Stochastic domination of absolute values of Gaussians**)**.** *Let $X \sim \mathcal{N}(0, \sigma^2)$. Then the random variable $|a + X|$ stochastically dominates the random variable $|b + X|$ whenever $|a| > |b|$.*

Proof: Without loss of generality, we assume $\sigma = 1$ and $a > b > 0$. Now for any fixed $y \geq 0$ and $x \in [b, a]$, we have

$$\mathbb{P}\left[|x + X| \geq y\right] = f(x) := G(y + x) + G(y - x),$$

where $G(x) := \frac{1}{\sqrt{2\pi}}\int_x^\infty \exp\left(-t^2/2\right) dt$ is the Gaussian tail. The claim now follows from the calculation that

$$f'(x) = \sqrt{\frac{2}{\pi}}\exp\left(-(x^2 + y^2)/2\right)\sinh(xy) \geq 0$$

for $x, y \geq 0$. ∎

A standard coupling argument gives the following corollary.

Corollary A.6. *Let $X \sim \mathcal{N}\left(0, \operatorname{diag}\left((\sigma_i^2)_{i=1}^n\right)\right)$, and $v \in \mathbb{R}^n$. For any $t \geq 0$, we have*

$$\mathbb{P}\left[\|v + X\|_1 < t\right] \leq \mathbb{P}\left[\|X\|_1 < t\right].$$

Theorem A.7 (**Lower tail of the $\|\cdot\|_1$-norm with non-zero means**)**.** *For any $\gamma \in (0, 1)$, there exists a positive constant $c = c(\gamma)$ such that the following is true. Let $X \sim \mathcal{N}(0, (\sigma_i)_{i=1}^n)$ be a Gaussian random vector with mean 0 and independent co-ordinates with non-zero variance, and let $a \in \mathbb{R}^n$ be an arbitrary vector.*

$$\mathbb{P}\left[\|X + a\|_1 < \gamma\|a\|_1\right] \leq \exp\left(-c\frac{(\sum_i \sigma_i)^2}{\sum_i \sigma_i^2}\right).$$

Proof: A direct calculation (or the fact that the map $X \mapsto |X + a|$ is 1-Lipschitz and the Cirel'son-Ibragimov-Sudakov inequality ([32], as stated in [33, Theorem 3.2.2]) implies that each $|X_i + a_i|$ is a sub-gaussian random variable with mean $\mu_i = \mathbb{E}\left[|X_i + a_i|\right]$ and sub-gaussian parameter σ_i. Further, note that $\mu_i \geq |a_i|$ (due to Jensen's inequality) and $\mu_i \geq \mathbb{E}\left[|X_i|\right] = \sigma_i\sqrt{2/\pi}$ (by Fact A.5).

Since the X_i are independent, this implies that $Z := \|X + a\|_1 = \sum_i |X_i + a_i|$ is also a sub-gaussian random variable with mean $\sum_i \mu_i$ and sub-Gaussian parameter $\sqrt{\sum_i \sigma_i^2}$. Further, since $\mu_i \geq |a_i|$, we have $\mathbb{E}[Z] \geq \|a\|_1$, so that

$$\begin{aligned}\mathbb{P}\left[Z \leq \gamma\|a\|_1\right] &\leq \mathbb{P}\left[Z \leq \gamma E[Z]\right]\\ &\leq \exp\left(-c'(1-\gamma)^2\mathbb{E}[Z]^2 \Big/ \left(\sum_i \sigma_i^2\right)\right),\end{aligned}$$

where the second inequality uses the fact that Z is sub-gaussian with sub-gaussian parameter $\sqrt{\sum_i \sigma_i^2}$. The claim now follows once we recall that $\mu_i \geq \sigma_i\sqrt{2/\pi}$ so that $\mathbb{E}[Z] \geq \sqrt{2/\pi}\sum_i \sigma_i$. ∎

Acknowledgments

We thank anonymous reviewers for several helpful comments and suggestions.

References

[1] D. L. Donoho, "Compressed sensing," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1289–1306, Apr. 2006. [Online]. Available: https://doi.org/10.1109/TIT.2006.871582

[2] V. Chandrasekaran, B. Recht, P. A. Parrilo, and A. S. Willsky, "The convex geometry of linear inverse problems," *Found. Comput. Math.*, vol. 12, no. 6, pp. 805–849, 2012. [Online]. Available: https://doi.org/10.1007/s10208-012-9135-7

[3] V. D. Mil'man, "New proof of the theorem of A. Dvoretzky on intersections of convex bodies," *Funct. Anal. Appl.*, vol. 5, no. 4, pp. 288–295, Oct. 1971. [Online]. Available: https://doi.org/10.1007/BF01086740

[4] B. S. Kašin, "Diameters of some finite-dimensional sets and classes of smooth functions," *Math. USSR-Izvestiya*, vol. 11, no. 2, p. 317, 1977. [Online]. Available: https://doi.org/10.1070/IM1977v011n02ABEH001719

[5] T. Figiel, J. Lindenstrauss, and V. D. Milman, "The dimension of almost spherical sections of convex bodies," *Acta Math.*, vol. 139, no. 1, pp. 53–94, Dec. 1977. [Online]. Available: https://doi.org/10.1007/BF02392234

[6] A. Dvoretzky, "Some results on convex bodies and Banach spaces," in *Proc. Int. Symp. Linear Spaces*. Jerusalem: Academic Press, 1961, pp. 123–160.

[7] S. Artstein-Avidan and V. D. Milman, "Logarithmic reduction of the level of randomness in some probabilistic geometric constructions," *J. Funct. Anal.*, vol. 235, no. 1, pp. 297–329, Jun. 2006. [Online]. Available: https://doi.org/10.1016/j.jfa.2005.11.003

[8] S. Lovett and S. Sodin, "Almost Euclidean sections of the N-dimensional cross-polytope using $O(N)$ random bits," *Comm. Contemp. Math.*, vol. 10, no. 04, pp. 477–489, Aug. 2008. [Online]. Available: https://doi.org/10.1142/S0219199708002879

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIT.2019.2919632, IEEE Transactions on Information Theory

[9] V. Guruswami, J. R. Lee, and A. Wigderson, "Euclidean sections of ℓ_1^N with sublinear randomness and error-correction over the reals," in *Approximation, Randomization and Combinatorial Optimization. Algorithms and Techniques. Proc. 11th APPROX and 12th RANDOM*, ser. Lecture Notes in Computer Science, A. Goel, K. Jansen, J. D. P. Rolim, and R. Rubinfeld, Eds. Springer, 2008, pp. 444–454. [Online]. Available: https://doi.org/10.1007/978-3-540-85363-3_35

[10] V. Guruswami, J. R. Lee, and A. Razborov, "Almost Euclidean subspaces of ℓ_1^N via expander codes," *Combinatorica*, vol. 30, no. 1, pp. 47–68, Sep. 2010. [Online]. Available: https://doi.org/10.1007/s00493-010-2463-9

[11] P. Indyk and S. Szarek, "Almost-Euclidean subspaces of ℓ_1^N via tensor products: A simple approach to randomness reduction," in *Approximation, Randomization and Combinatorial Optimization. Algorithms and Techniques. Proc. 13th APPROX and 14th RANDOM*, ser. Lecture Notes in Computer Science, M. Serna, R. Shaltiel, K. Jansen, and J. Rolim, Eds. Springer, 2010, pp. 632–641. [Online]. Available: https://doi.org/10.1007/978-3-642-15369-3_47

[12] A. Sahai and S. K. Mitter, "The necessity and sufficiency of anytime capacity for stabilization of a linear system over a noisy communication link – Part I: Scalar systems," *IEEE Trans. Inf. Theory*, vol. 52, no. 8, pp. 3369–3395, 2006. [Online]. Available: https://doi.org/10.1109/TIT.2006.878169

[13] L. J. Schulman, "Coding for interactive communication," *IEEE Trans. Inf. Theory*, vol. 42, no. 6, pp. 1745–1756, 1996. [Online]. Available: https://doi.org/10.1109/18.556671

[14] A. Edelman and B. Sutton, "Tails of condition number distributions," *SIAM J. Matrix Anal. Appl.*, vol. 27, no. 2, pp. 547–560, Jan. 2005. [Online]. Available: https://doi.org/10.1137/040614256

[15] M. Rudelson, "Invertibility of random matrices: norm of the inverse," *Ann. Math.*, vol. 168, no. 2, pp. 575–600, Sep. 2008. [Online]. Available: https://doi.org/10.4007/annals.2008.168.575

[16] M. Rudelson and R. Vershynin, "Smallest singular value of a random rectangular matrix," *Comm. Pure Appl. Math.*, vol. 62, no. 12, pp. 1707–1739, Dec. 2009. [Online]. Available: https://doi.org/10.1002/cpa.20294

[17] T. Tao and V. H. Vu, "Inverse Littlewood-Offord theorems and the condition number of random discrete matrices," *Ann. Math.*, vol. 169, no. 2, pp. 595–632, 2009. [Online]. Available: https://doi.org/10.4007/annals.2009.169.595

[18] N. Cook, "Lower bounds for the smallest singular value of structured random matrices," *Ann. Probab.*, vol. 46, no. 6, pp. 3442–3500, Nov. 2018. [Online]. Available: https://doi.org/10.1214/17-AOP1251

[19] M. Rudelson and O. Zeitouni, "Singular values of Gaussian matrices and permanent estimators," *Random Struct. Algor.*, vol. 48, no. 1, pp. 183–212, Jan. 2016. [Online]. Available: https://doi.org/10.1002/rsa.20564

[20] R. Latała, "Some estimates of norms of random matrices," *Proc. Amer. Math. Soc.*, vol. 133, no. 5, pp. 1273–1282, 2005. [Online]. Available: https://doi.org/10.1090/S0002-9939-04-07800-1

[21] C. Schütt and S. Riemer, "On the expectation of the norm of random matrices with non-identically distributed entries," *Electron. J. Probab.*, vol. 18, pp. 1–13, Feb. 2013. [Online]. Available: https://doi.org/10.1214/EJP.v18-2103

[22] A. S. Bandeira and R. van Handel, "Sharp nonasymptotic bounds on the norm of random matrices with independent entries," *Ann. Probab.*, vol. 44, no. 4, pp. 2479–2506, Jul. 2016. [Online]. Available: https://doi.org/10.1214/15-AOP1025

[23] R. Latała, R. van Handel, and P. Youssef, "The dimension-free structure of nonhomogeneous random matrices," *Invent. Math.*, vol. 214, no. 3, pp. 1031–1080, Dec. 2018. [Online]. Available: https://doi.org/10.1007/s00222-018-0817-x

[24] J. W. Byers, M. Luby, M. Mitzenmacher, and A. Rege, "A digital fountain approach to reliable distribution of bulk data," in *Proc. ACM SIGCOMM*. New York, NY, USA: ACM, 1998, pp. 56–67. [Online]. Available: https://doi.org/10.1145/285237.285258

[25] M. Luby, "LT codes," in *Proc. 43rd IEEE Symp. Found. Comput. Sci. (FOCS)*, 2002, pp. 271–280. [Online]. Available: https://doi.org/10.1109/SFCS.2002.1181950

[26] A. Shokrollahi, "Raptor codes," *IEEE Trans. Inf. Theory*, vol. 52, no. 6, pp. 2551–2567, Jun. 2006. [Online]. Available: https://doi.org/10.1109/TIT.2006.874390

[27] P. Maymounkov, "Online codes," New York University technical report, Nov. 2002. [Online]. Available: http://cs.nyu.edu/media/publications/TR2002-833.pdf

[28] W. Evans, M. Klugerman, and L. J. Schulman, "Postscript to 'Coding for interactive communication'," 1994, unpublished work, http://users.cms.caltech.edu/~schulman/Papers/intercodingpostscript.txt.

[29] M. Braverman, "Towards deterministic tree code constructions," in *Proc. 3rd Innovations Theoret. Comput. Sci. Conf. (ITCS)*, 2012, pp. 161–167. [Online]. Available: https://doi.org/10.1145/2090236.2090250

[30] C. Moore and L. J. Schulman, "Tree codes and a conjecture on exponential sums," in *Proc. 5th Innovations Theoret. Comput. Sci. Conf. (ITCS)*, 2014, pp. 145–154. [Online]. Available: https://doi.org/10.1145/2554797.2554813

[31] G. Cohen, B. Haeupler, and L. J. Schulman, "Explicit binary tree codes with polylogarithmic size alphabet," in *Proc. 50th ACM Symp. Theory Comput. (STOC)*, 2018, pp. 535–544. [Online]. Available: https://doi.org/10.1145/3188745.3188928

[32] B. S. Cirel'son, I. A. Ibragimov, and V. N. Sudakov, "Norm of Gaussian sample function," in *Proc. 3rd Japan-USSR Symp. Probab. Theory*, ser. Lecture notes in Mathematics, vol. 550. Springer, 1976, pp. 20–41. [Online]. Available: https://doi.org/10.1007/BFb0077482

[33] M. Raginsky and I. Sason, "Concentration of Measure Inequalities in Information Theory, Communications, and Coding," *Found. Trends Commun. Inf. Theory*, vol. 10, no. 1-2, pp. 1–246, Oct. 2013. [Online]. Available: https://doi.org/10.1561/0100000064

PLACE PHOTO HERE

Leonard J. Schulman is at the Division of Engineering and Applied Science at the California Institute of Technology, in Pasadena, California.

PLACE PHOTO HERE

Piyush Srivastava is at the School of Technology and Computer Science at the Tata Institute of Fundamental Research in Mumbai, India.