Recovery of Binary Sparse Signals from Structured Biased Measurements

Sandra Keiper

Institut für Mathematik, Technische Universität Berlin

July 30, 2020

Abstract

In this paper we study the reconstruction of binary sparse signals from partial random circulant measurements. We show that the reconstruction via the least-squares strategy is as good as the reconstruction via the usually used program basis pursuit. We further show that we need as many measurements to recover an s-sparse signal $x_0 \in \mathbb{R}^N$ as we need to recover a dense signal, more-precisely an $N-s$-sparse signal $x_0 \in \mathbb{R}^N$. We further establish stability with respect to noisy measurements.

Keywords. Compressed Sensing, Sparse Recovery, Null Space Property, Finite Alphabet, Binary Signals, Dual Certificates, Partial Random Circulant Matrices, Partial Random Toeplitz Matrices
AMS classification. 15A12, 15A60, 15B52, 42A61, 60B20, 90C05, 94A12, 94A20

1 Introduction

A recent mathematical framework that ensures recovery of sparse vectors from incomplete information is *Compressed sensing*. In this context, incomplete information refers to the fact that linear systems of the form

$$Ax_0 = y$$

can only be solved uniquely for general $x_0 \in \mathbb{R}^N$ if $A \in \mathbb{R}^{M,N}$ is quadratic and invertible, i.e., if $M < N$ the information is incomplete. By imposing an a-priori structure on x_0, however, the ill-posed problem for $M < N$ can be turned into a well-posed one. An important structure of x_0 is that of *sparsity*, which means that only a few entries of x_0 are different from zero. Another relevant assumption on x_0 is that its entries stem from a finite alphabet. In this paper we study sparse signals whose entries stem from a binary alphabet, e.g., $x_0 \in \{0,1\}^N$. Such signals appear for example in wireless communications, where the transmitted signals are sequences of bits. Moreover, in certain types of communication networks it is appropriate to assume that only a few transmitters are active at a certain instance, which naturally induces sparsity.

Note that binary signals are in particular symmetric in the sense, that if x_0 is a dense signal, $\mathbb{1} - x_0$ is sparse. In the recent publication [5], we have proven that using shifted random matrices such signals can be recovered from a particularly small number of measurements and that this number reflects the mentioned symmetry of x_0. This means that we need the same number of measurements to recover an s-sparse signal as we need to recover an $(N-s)$-sparse signal.

The in [5], considered measurement matrices, however, are of somewhat limited use in applications. The reasons are diverse. Often the design of the measurement matrix is given by the applications with little or even no freedom to design it. Moreover, unstructured matrices, such as random or particularly Gaussian and Rademacher matrices, do not allow for a fast matrix multiplication, which may speed up recovery algorithms significantly. Beyond that storing a large unstructured matrix might be difficult. Hence, from a computational and application-technological point of view it would be desirable to use structured random matrices.

Up until now there are only few good recovery conditions for completely deterministic measurement matrices available. One, therefore, should allow for some randomness to come into play. In this work, we consider biased partial random circulant matrices for the measurement process. A precise definition of such matrices is given in

Subsection 1.4 (Equation (6)). A main difference is that those matrices depend on only one random vector and accordingly N random variables, whereas (sub-) Gaussians either depend on MN random variables (following the definition in [6]) or on M random row vectors (following the definition in [21]).

The concern of this work is to proof recovery guarantees for binary, sparse signals from biased random partial circulant and Toeplitz measurements.

Partial random circulant matrices (centered and not biased) have already been successfully applied to the classical compressed problem (see for example [15]) and in one-bit compressed sensing ([1, 2]). In [1], [2] and [4], the reconstruction of sparse signals from binary Gaussian circulant measurements was also considered. The main difference is that in those papers the measurements $y = \operatorname{sign}(Ax_0)$ are assumed to be binary whereas we assume that the signal x_0 itself is binary. Besides, the proof techniques are very different.

1.1 Preliminaries

To put our results in a precise setting we first aim to introduce some notation. We define $[N] := \{1, \dots, N\}$ and denote the standard unit vectors with e_i for $i \in [N]$, i.e., the vector which is zero everywhere except at the i-th entry it is equal to one. Further, we denote with $\mathbb{1}$ the matrix or vector, respectively, which is equal to one in each entry. For a subset $S \subset [N]$ and a vector $x = (x_1, \dots, x_N) = (x(1), \dots, x(N)) \in \mathbb{R}^N$ the notation x_S refers to the following vector

$$x_S(i) = \begin{cases} x_i, & \text{if} \quad i \in S \\ 0, & \text{else.} \end{cases}$$

Further $\|\cdot\|_0$ denotes the ℓ_0-norm and $\|\cdot\|_p$ the ℓ_p-norm for $p > 0$, i.e., for $x = [x_1, \dots, x_N] \in \mathbb{R}^N$

$$\|x\|_0 := |\{i : x_i \neq 0\}| \qquad \text{and} \qquad \|x\|_p^p := \sum_{i=1}^{N} |x_i|^p.$$

For a matrix $A \in \mathbb{R}^{M,N}$ the transposed matrix is denoted by A^*. The notation $\operatorname{supp}(x)$ refers to the support of a vector $x \in \mathbb{R}^N$, i.e., to the set of non-zero entries of x.

For two real numbers $a, b \in \mathbb{R}$ we write $a \gtrsim b$ if there exists a constant $c > 0$, which is independent from a and b, such that $a \geq cb$.

For $\Theta \subset [N]$ we define

$$i + \Theta := \{(i + k) (\operatorname{mod} N) : k \in \Theta\}.$$

Moreover, for a linear operator $L : \mathbb{R}^N \to \mathbb{R}^M$ with matrix representation $L = [L_{i,j}]_{i,j=1}^{M,N}$ the Hilbert-Schmidt norm of L is denoted by

$$\|L\|_{HS} := \sqrt{\operatorname{tr}(L^* L)} = \sqrt{\sum_{i=1}^{M} \sum_{j=1}^{N} L_{i,j}^2},$$

and

$$\|L\| := \sup_{\|w\|_2 \leq 1} \|Lw\|_2$$

is the operator norm of L. Note that the operator norm of $L : \mathbb{R}^N \to \mathbb{R}^N$ corresponds to the square root of largest eigenvalue of $L^* L$. Further note that for $A, B \in \mathbb{R}^{N,N}$ with $B = [b_1, \dots, b_N]$ it holds true that

$$\|AB\|_{\mathrm{HS}}^2 = \sum_{i=1}^{N} \|Ab_i\|_2^2 \leq \sum_{i=1}^{N} \|A\|^2 \|b_i\|_2^2 = \|A\| \|B\|_{\mathrm{HS}}^2, \tag{1}$$

where we used the consistency of the operator norm with the Euclidean norm $\|\cdot\|_2$.

For $A \in \mathbb{R}^{M,N}$ and $S \subset [N]$ we let A_S be either the matrix which consists of the rows of A corresponding to the indices in S, i.e., $A_S \in \mathbb{R}^{s,N}$, or the matrix whose rows corresponding to the indices in S equal those of A and all other columns are zero, i.e., $A_S \in \mathbb{R}^{M,N}$. We further let $A^S \in \mathbb{R}^{M,s}$ or $A^S \in \mathbb{R}^{M,N}$ be the matrix whose columns corresponding to S are deleted or substituted with zero-columns.

Finally, let us recall Gershgorin circle theorem, which is an important tool for our proofs.

Theorem 1.1 (Gershgorin circle theorem [8]) *Let $A = [a_{i,j}]_{i,j=1}^N \in \mathbb{C}^{N,N}$ and for $i \in [N]$ let $R_i = \sum_{j \neq i} |a_{ij}|$ be the sum of the absolute values of the non-diagonal entries in the i-th row. Further define $D(a_{ii}, R_i) \subseteq \mathbb{C}$ be a closed disc centered at a_{ii} with radius R_i. Every eigenvalue of A lies then within at least one of the* Gershgorin discs $D(a_{ii}, R_i)$.

1.2 Reconstruction of Binary Signals

There are several compressed sensing approaches for the reconstruction of nonnegative sparse signals from random measurements [3, 13, 18]. As binary vectors are particularly nonnegative, those approaches can readily be applied to binary vectors. Let us therefore shortly review one of the approaches for the recovery of nonnegative signals.

It has become evident that basis pursuit restricted to the positive orthant

$$\mathbb{R}^N_+ := \left\{x = (x_i)_{i=1}^N \in \mathbb{R}^N : x_i \geq 0, i \in [N]\right\}$$

has a strong performance at recovering nonnegative-valued sparse signals x_0 from the measurements $y = Ax_0$. This is the following program:

$$\min \|x\|_1 \quad \text{subject to} \quad Ax = y \quad \text{and} \quad x \in \mathbb{R}^N_+, \tag{2}$$

Even so the mentioned approach is applicable to binary signals, it is already known that there are methods which yield even stronger recovery guarantees for binary signals. The canonical approach is to use the following adaptation of basis pursuit, to which we typically refer to as *box-constrained basis pursuit*:

$$\min \|x\|_1 \quad \text{subject to} \quad Ax = y \quad \text{and} \quad x \in [0,1]^N. \tag{3}$$

In [12, 19], the following equivalent condition for the success of (3) has been shown. The vector $\mathbb{1}_S$, $S \subset [N]$, is the unique solution of (3) if and only if

$$\ker(A) \cap N^+ \cap H_S = \{0\},$$

where $\ker(A)$ denotes the nullspace of A,

$$N^+ := \left\{ w \in \mathbb{R}^N : \sum_{i=1}^N w_i \leq 0 \right\} \quad \text{and} \quad H_S := \left\{ w \in \mathbb{R}^N : w_i \leq 0 \text{ for } i \in S \text{ and } w_i \geq 0 \text{ for } i \notin S \right\}.$$

Least-squares on the other hand is a strategy which is usually not well-applicable to sparse vectors since the ℓ_2-norm does not promote sparsity. In [5], however, it has been shown that least-squares with box-constraints works comparably well for binary-valued sparse signals, when reconstructing from biased sub-Gaussian measurements, even, if the measurements are contaminated with noise. *Least-squares with box-constraints* is the following program

$$\min \|Ax - y\|_2 \quad \text{subject to} \quad x \in [0,1]^N. \tag{4}$$

Note, that this fact has some practical impact. On the one hand least-squares is less complex and on the other hand it ensures a priori robustness in case of noisy measurements.

1.3 Biased Random Matrices

In compressed sensing the measurement matrix is often assumed to be (sub-) Gaussian, meaning that each entry of the measurement matrix $A \in \mathbb{R}^{M,N}$ is an independent copy of some (sub-) Gaussian. More precisely, we call $A \in \mathbb{R}^{M,N}$ *Gaussian*, if its entries are independently drawn from a renormalized normal distribution, i.e.,

$$A = \frac{1}{\sqrt{M}} [a_{i,j}]_{i,j=1}^{M,N} \qquad \text{with} \qquad a_{i,j} \sim \mathcal{N}(0,1).$$

A more general type of measurement matrices are sub-Gaussians, whose entries follow a sub-Gaussian distribution:

Definition 1.2 Let $(\Omega, \Sigma, \mathbb{P})$ be a probability space. Further let $X : \Omega \to \mathbb{R}$ be a random variable. The *sub-Gaussian* or *Orclitz-2*-norm of X is given by

$$\|X\|_{\Psi_2} = \sup_{p \geq 1} p^{-\frac{1}{2}} \mathbb{E}\left(|X|^p\right)^{\frac{1}{p}}.$$

We call X *sub-Gaussian* if $\|X\|_{\Psi_2} < \infty$. We call a matrix $A \in \mathbb{R}^{m,N}$ *sub-Gaussian matrix* if its entries are independent sub-Gaussian variables with expected value 0.

A particular example for a sub-Gaussian matrix is a Rademacher matrix. $A \in \mathbb{R}^{M,N}$ is called *Rademacher matrix*, if its entries follow a Rademacher distribution, i.e., are chosen to be -1 or 1 with equal probability:

$$A = \frac{1}{\sqrt{M}} [a_{i,j}]_{i,j=1}^{M,N} \qquad \text{with} \qquad \mathbb{P}(a_{i,j} = 1) = \mathbb{P}(a_{i,j} = -1) = \frac{1}{2}.$$

Rademacher variables X are indeed sub-Gaussians with norm $\|X\|_{\Psi_2} = 1$, because $|X| = 1$. Further, note that sub-Gaussians are sometimes also defined by assuming that the rows are independent random vectors, which fulfill some specific properties such as sub-Gaussian marginals (cf. [21]). This basically is some generalization of the definition used in the underlying paper.

Sub-Gaussian matrices, whose entries have mean zero, are often considered to model the measurement process. However, it was shown in a recent work [5] that non-centered matrices have some advantage for the recovery of binary signals. Moreover, in [13], a similar phenomenon was observed for the recovery of non-negative signals by (2). To be more precise the following *biased random matrices* have been considered in [5]:

$$A = \mu \mathbb{1} + D, \tag{5}$$

where $\mu \geq 0$ is a freely chosen parameter that controls the expected value of the entries, $\mathbb{1} \in \mathbb{R}^{M,N}$ is the matrix having only entries equal to one, and $D \in \mathbb{R}^{M,N}$ is assumed to have sub-Gaussian entries whose expected value is 0.

Roughly speaking the following was proven for the recovery of binary, sparse signals from biased random measurements:

Theorem 1.3 (Simplified Version of Theorem III.2 and III.8 of [5]) *Let $x_0 \in \{0,1\}^N$ be a binary vector, and $A \in \mathbb{R}^{M,N}$ be a biased random matrix of the form (5) with $\mu > 0$, and $x_0 \in \{0,1\}^N$ a s-sparse binary vector.*

i) If M is slightly larger than $N/2$, x_0 is the unique solution of (3) with high probability.

ii) Under the assumption

$$M \gtrsim \max\left(\frac{R^2}{\mu^2}, \min(s, N-s)\right) \log(N),$$

the solution x_* of (4) for $y = Ax_0 + n$ with $n \in \mathbb{R}^M$ and $\|n\|_2 \leq \eta$ obeys with high probability

$$\|x_0 - x_*\|_2 \leq \sqrt{\frac{\left(\frac{\sigma^2}{\mu^2} + 32\min(s, N-s)\right)}{m\sigma^2}} \cdot \eta,$$

where σ is the variance of the entries of A. Particularly, in the case of noiseless measurements, i.e., $\eta = 0$, x_0 is the unique solution of (3) and of (4) with high probability.

1.4 Main Result

As above-mentioned there are several applications where we do not have full freedom to design the measurement matrix. It is therefore of some importance to study structured random matrices. In applications such as radar or wireless communications the measurement process can be represented using partial random circulant matrices and partial random Toeplitz matrices (cf. [11],[16]). In those applications binary sparse signals appear also in a natural way. The main goal of this work is therefore to prove comparable results as in [5] (see Theorem 1.3), for such matrices. Before stating our main results, let us introduce the considered matrices.

For $b = (b_0, b_1, \ldots, b_{N-1}) \in \mathbb{R}^N$ we define the associated *circulant matrix* $\Phi = \Phi(b) \in \mathbb{R}^{N,N}$ by setting

$$\Phi_{k,j} = b_{(j-k) (\mathrm{mod}\, N)} \qquad k, j \in [N].$$

Similarly, for a vector $c = (c_{-N+1}, c_{-N+2}, \ldots, c_{N-1}) \in \mathbb{R}^{2N-1}$ the associated *Toeplitz matrix* $T = T(c) \in \mathbb{R}^{N,N}$ has entries

$$T_{k,j} = c_{j-k} \qquad k, j \in [N].$$

For an arbitrary subset $\Theta \subset [N]$ of cardinality $M < N$, we let the *partial circulant matrix* $\Phi_\Theta = \Phi_\Theta(b) \in \mathbb{R}^{M,N}$, and the *partial Toeplitz matrix* T_Θ, respectively, be the submatrix of Φ, and T respectively, consisting of the rows indexed by Θ. In [15], one can find a comprehensive overview of compressed sensing with structured random matrices. It is particularly shown that partial circulant matrices with Rademacher input vector b work comparable well for the classical compressed sensing task as completely random sub-Gaussian matrices.

For our purpose we choose the vectors b and c to be sub-Gaussian and centered sequences. Hence, the matrices Φ_Θ and T_Θ are centered. Similarly to the results in [5], we consider biased partial random matrices given by

$$A = A(b) = \mu \mathbb{1} + \Phi_\Theta(b), \tag{6}$$

or

$$A = A(c) = \mu \mathbb{1} + T_\Theta(c). \tag{7}$$

Here, the parameter $\mu \geq 0$ controls the expected value of the entries of A and $\mathbb{1} \in \mathbb{R}^{M,N}$ is the matrix having all entries equal to one.

The main purpose of this paper is to prove the symmetric phase transition observed in [5], for biased partial random matrices given by Equation (6). This means we show that we need as many measurements to recover sparse signals as we need to recover dense signals. The main result of this paper is the following theorem:

Theorem 1.4 *Let $\mu > 0$ and fix some tolerance $\varepsilon > 0$. Let $A \in \mathbb{R}^{M,N}$ be a biased measurement matrix*

i) of the form (6), where $b = [b_i]_{i=1}^N \in \mathbb{R}^N$ is a sub-Gaussian vector with $\mathbb{E}(b_i) = 0$, $\mathbb{E}(b_i^2) = \sigma^2$, for $i \in [N]$, and sub-Gaussian norm R. Or

ii) of the form (7), where $c = [c_i]_{i=-N+1}^{N-1} \in \mathbb{R}^{2N-1}$ is a sub-Gaussian vector with $\mathbb{E}(c_i) = 0$, $\mathbb{E}(c_i^2) = \sigma^2$, for $i \in \{-N+1, \dots, N-1\}$, and sub-Gaussian norm R.

A binary signal $x_0 \in \{0,1\}^N$ with $\|x_0\|_0 = s$ is the unique solution of (3) and (4) for $y = Ax_0$ with probability larger than $1 - \varepsilon$, provided

$$M \gtrsim \max\left(\frac{R^2}{\mu^2}, \min(s, N-s)\frac{2R^4}{\sigma^4}\right) \ln^2\left(\frac{N}{\varepsilon}\right), \tag{8}$$

with a constant depending only on σ and μ^{-1}.

iii) Under the additional assumption $M \gtrsim \left(\frac{R}{\sigma}\right)^{4/3} \ln(\varepsilon^{-1})$ the solution x_* of (4) for $y = Ax_0 + n$ with $\|n\|_2 \leq \eta$ for some $\eta > 0$ obeys

$$\|x_0 - x_*\|_2 \leq \sqrt{\frac{2\left(\frac{4\sigma^2}{\mu^2} + 32\min(s, N-s)\right)}{M\sigma^2}} \cdot \eta.$$

2 Proof of Theorem 1.4

We prove Theorem 1.4 by deriving a so-called *dual certificate* [7, 10, 20], that is a vector $\nu \in \mathbb{R}^M$ having a small ℓ_2-norm and fulfilling $A^*\nu \in H_S^t$, for some $t \geq 0$, where

$$H_S^t := \left\{w \in \mathbb{R}^N : w_i \leq -t \text{ for } i \notin S \text{ and } w_i \geq t \text{ for } i \in S\right\}.$$

To justify that this helps to prove the theorem, let us recall some results from [5].

Proposition 2.1 (Propositions II.3 and III.1 of [5]) *Let $A \in \mathbb{R}^{M,N}$, $S \subset [N]$ and $\mathbb{1}_S \in \mathbb{R}^N$ be the binary signal supported on S. Then the following statements are equivalent:*

i) $\mathbb{1}_S$ and $\mathbb{1} - \mathbb{1}_S = \mathbb{1}_{S^C}$ are the unique solutions of (3) with $y = A\mathbb{1}_S$ and $y = A\mathbb{1}_{S^C}$, respectively.

ii) $\ker(A) \cap H_S^0 = \{0\}$.

iii) $\{x \in [0,1]^N : Ax = A\mathbb{1}_S\} = \mathbb{1}_S$.

iv) *There is* $\nu \in \mathbb{R}^M$ *such that* $A^*\nu \in H_S^t$ *for some* $t > 0$.

Hence, finding a dual certificate indeed ensures, that $\mathbb{1}_S$ is the unique solution of (3). However, the third equivalence even yields that there is no other solution of $Ax = A\mathbb{1}_S$ other than $\mathbb{1}_S$ in the box $[0,1]^N$. Thus, the ℓ_1-minimization in (3) is not crucial and we can, at least in the noiseless case, run the box-constrained least-squares (4) instead.

The proof for the noisy case in Part *iii)* of Theorem 1.4 makes use of the following result from [5].

Proposition 2.2 *[Proposition III.4 of [5]] Let* $r, t, \eta > 0$, $S \subset [N]$ *and* $A \in \mathbb{R}^{M,N}$. *Suppose that there exists a dual certificate* $\nu \in \mathbb{R}^M$ *such that* $A^*\nu \in H_S^t$ *and* $\|\nu\|_2 \leq r$.

Let $x_0 = \mathbb{1}_S \in \mathbb{R}^N$ *be the binary signal supported on* S, *and* $y = Ax_0 + n$ *with* $\|n\|_2 \leq \eta$. *Then the solution* x_* *of the program* (4) *obeys*

$$\|x_* - x_0\|_2 \leq \frac{2r}{t}\eta.$$

Before constructing the dual certificate explicitly, let us recall the general Hoeffding's inequality as well as the Hanson-Wright inequality, which will be important probabilistic tools for the proof of Theorem 1.4.

Theorem 2.3 (Proposition 2.6.2 of [22] and Theorem 1.1 of [17])

i) *There exists a universal constant* $C > 0$ *with the following property: If* $X_1, \dots, X_M$ *are independent, mean zero, sub-Gaussian random variables, then, for every* $t \geq 0$ *we have*

$$\mathbb{P}\left(\left|\sum_{i=1}^M X_i\right| \geq t\right) \leq 2 \cdot \exp\left(-\frac{Ct^2}{\gamma^2}\right),$$

with $\gamma = \sum_{i=1}^M \|X_i\|_{\psi_2}^2$.

ii) *There exists a universal constant* $C > 0$ *with the following property: Suppose that* $X = (X_1, \dots, X_q) \in \mathbb{R}^q$ *is a random vector with independent, mean zero, sub-Gaussian entries. Let further* L *be a fixed linear map from* $\mathbb{R}^q$ *to* $\mathbb{R}^q$. *Then we have*

$$\mathbb{P}\left(|\langle X, LX\rangle - \mathbb{E}\left(\langle X, LX\rangle\right)| > t\right) \leq 2\exp\left(-C\min\left(\frac{t^2}{R^4\|L\|_{HS}^2}, \frac{t}{R^2\|L\|}\right)\right)$$

with $R = \max_{\ell=1,\dots q} \|X_\ell\|_{\psi_2}$.

Now we are prepared to prove Theorem 1.4. Note that we will use the same dual certificate as for the proof of the main theorem of [5] and that the probabilistic tool will also be the Hanson-Wright inequality. However, the proof is considerably more sophisticated.

Proof of Theorem 1.4. We first prove **Part *i)*** of Theorem 1.4, hence, we assume that the measurement matrix A is a biased partial random circulant matrix. To make notations easier we enlarge A by inserting zero-rows for indices not in Θ. Hence, we define

$$A = \mu\,\mathbb{1} + \Phi_\Theta(b),$$

where

$$(\Phi_\Theta)_{k,j} = \begin{cases} b_{(j-k)(\mathrm{mod}\,N)} & \text{if} \quad k \in \Theta \\ 0 & \text{else} \end{cases} \qquad \text{and} \qquad \mathbb{1}_{k,j} = \begin{cases} 1 & \text{if} \quad k \in \Theta \\ 0 & \text{else} \end{cases},$$

and $b \in \mathbb{R}^N$ is the given sub-Gaussian vector. This matches the aforementioned measurement process; the vector Ax_0 is only enlarged by some zeros. Further we define β_0 to be the sparser of the two vectors x_0 and $\mathbb{1} - x_0$, i.e.,

$$\beta_0 = \begin{cases} x_0 & \text{if } \|x_0\|_0 \leq \|\mathbb{1} - x_0\|_0, \\ \mathbb{1} - x_0 & \text{else.} \end{cases}$$

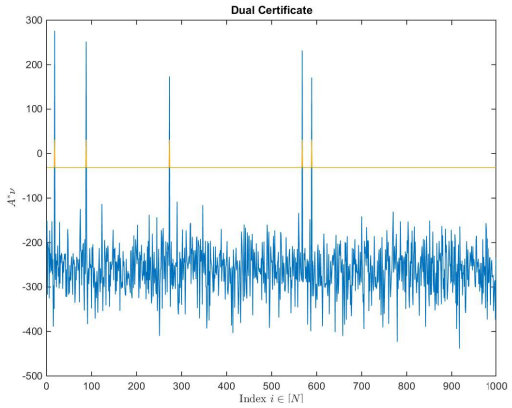

Figure 1: Values of $(A^*\nu)_i$ for $i \in [N]$, for ν defined in Equation (9) (blue).
We choose the ambient dimension $N = 1000$, the number of measurements $M = 500$ and the size of the support $s = 5$. We draw a biased Gaussian circulant matrix $A \in \mathbb{R}^{M,N}$ and the support S of the binary vector the same way as for the experiments described in Section 3. The blue plot illustrates the value of $A^*\nu$ and the yellow plot the value for $-t = -\frac{M}{16}$ on S^C and $t = \frac{M}{16}$ on S. We see that it indeed holds true that $A^*\nu \in H_S^t$. This observation holds true with high probability.

Similarly, as in [5] we define the dual certificate to be

$$\nu = \rho\,\mathbb{1} + \Phi_\Theta\beta_0 - M^{-1}\langle \Phi_\Theta\beta_0, \mathbb{1}\rangle\,\mathbb{1}, \qquad \text{where} \quad \rho = -\frac{\sigma^2}{2\mu}, \tag{9}$$

and prove that $A^*\nu \in H_S^t$, where $S = \operatorname{supp}\beta_0$ and $t = \frac{M\sigma^2}{16}$. This means that we prove that we have with high probability

$$\langle \nu, Ae_i\rangle = \langle A^*\nu, e_i\rangle = (A^*\nu)_i \begin{cases} \leq -t & \text{if } i \in [N]\setminus S \\ \geq t & \text{if } i \in S. \end{cases} \tag{10}$$

In Figure 1, we validated numerically that the defined dual certificate indeed fulfills this required property.

A simple calculation yields

$$\begin{aligned} \langle \nu, Ae_i\rangle &= \rho\mu M + \rho\,\langle \mathbb{1}, \Phi_\Theta e_i\rangle + \langle \Phi_\Theta\beta_0, \Phi_\Theta e_i\rangle - M^{-1}\langle \Phi_\Theta\beta_0, \mathbb{1}\rangle\langle \mathbb{1}, \Phi_\Theta e_i\rangle \\ &=: \rho\mu M + \rho X_1(i) + X_2(i) - M^{-1}X_3(i). \end{aligned}$$

We now estimate the quantities $X_1(i), X_2(i), X_3(i)$ for each $i \in S$ and $i \notin S$ separately.

Estimation of X_1:
We start with X_1. For every $i \in [N]$,

$$X_1(i) = \langle \mathbb{1}, \Phi_\Theta e_i\rangle = \sum_{l\in\Theta}(\Phi_\Theta)_{l,i} = \sum_{l\in\Theta} b_{(i-l)(\mathrm{mod}\,N)}$$

is a sum of M independent, centered, sub-Gaussian variables with sub-Gaussian norm R. Thus, it follows from Part i) of Theorem 2.3 that

$$\Pr(|X_1(i)| \geq \theta_1) \leq 2\exp\left(-\frac{C\theta_1^2}{MR^2}\right),$$

for every $i \in [N]$. The estimations of X_2 and X_3 are a slightly more involved. Let us start with X_2.

Estimation of X_2:
For every $i \in [N]$ it holds true that

$$X_2(i) = \langle \Phi_\Theta \beta_0, \Phi_\Theta e_i \rangle = \sum_{j=1}^{N} \sum_{k \in S} (\Phi_\Theta)_{j,k} (\Phi_\Theta)_{j,i} = \sum_{k \in S} \sum_{j \in \Theta} b_{(k-j)(\mathrm{mod}\, N)} b_{(i-j)(\mathrm{mod}\, N)},$$

and therefore

$$\mathbb{E}(X_2(i)) = \sum_{k \in S} \sum_{j \in \Theta} \sigma^2 \delta_{(k-j)(\mathrm{mod}\, N),(i-j)(\mathrm{mod}\, N)},$$

where for $j, k \in [N]$ the number $\delta_{j,k}$ is equal to one for $j = k$ and to zero otherwise. Now it holds true that $(k-j)(\mathrm{mod}\, N) = (i-j)(\mathrm{mod}\, N)$ if and only if $k = i$ and therefore

$$\mathbb{E}(X_2(i)) = \begin{cases} \sum_{j \in \Theta} \sigma^2 \delta_{i-j,i-j} & \text{if } i \in S \\ 0 & \text{if } i \notin S \end{cases} = \begin{cases} M\sigma^2 & \text{if } i \in S \\ 0 & \text{if } i \notin S. \end{cases}$$

To estimate the deviation from this expected value we want to use the Hanson-Wright inequality. Thus, we want to define the maps $L(i) : \mathbb{R}^N \to \mathbb{R}^N$ such that $\langle b, L(i)b \rangle = X_2(i)$ for all $i \in [N]$. We therefore define the map $L(i) : \mathbb{R}^N \to \mathbb{R}^N$, $(v_1, \dots, v_N) \mapsto (w_1, \dots, w_N)$ by

$$w_j = \begin{cases} \sum_{k \in S} v_{(k-i+j)(\mathrm{mod}\, N)} & \text{if } j \in \Theta_i \\ 0 & \text{else,} \end{cases}$$

where $\Theta_i := i - \Theta = (i - \Theta)(\mathrm{mod}\, N)$. Then it indeed holds true that

$$\langle b, L(i)b \rangle = \sum_{j=1}^{N} b_j (L(i)b)_j = \sum_{j \in \Theta_i} b_j \sum_{k \in S} b_{(k-i+j)(\mathrm{mod}\, N)} = \sum_{j \in \Theta} b_{(i-j)(\mathrm{mod}\, N)} \sum_{k \in S} b_{(k-j)(\mathrm{mod}\, N)} = X_2(i).$$

Thus, to apply the Hanson-Wright inequality we just need to estimate the Hilbert-Schmidt norm $\|L(i)\|_{HS}$ and the operator norm $\|L(i)\|$. Note that $L(i)$ is a linear map and the corresponding matrix, which we also call $L(i) = (L_{j,l})_{j,l=1}^N$ is given by

$$L(i)_{j,l} = \begin{cases} 1 & \text{if } j \in \Theta_i \text{ and } l \in S_{j-i} \\ 0 & \text{else,} \end{cases}$$

where $S_{j-i} = j - i + S$. Thus, we can easily verify that $\|L(i)\|_{HS}^2 = M|S| = Ms$. To estimate $\|L(i)\|$ we use the Gershgorin circle Theorem 1.1 to estimate the largest eigenvalue of $L(i)^* L(i)$. The row sum for the l-th row of $L(i)^* L(i)$ is given by

$$\sum_{j \in [N]} (L(i)^* L(i))_{l,j} = \sum_{j \in [N]} \sum_{k \in [N]} L(i)_{k,l} L(i)_{k,j} = \sum_{k \in \Theta_i} L_{k,l} \sum_{j \in [N]} L(i)_{k,j} = s \sum_{k \in \Theta_i} L(i)_{k,l} = Ms,$$

where we used in the second to last step that in the l-th row, $l \in \Theta_i$, of $L(i)$ exactly s entries are equal to 1 and all others are equal to zero. Thus, the Gershgorin disk $D((L(i)^* L(i))_{ll}, R_l)$, where R_l is the sum of the non-diagonal row elements, is contained in the disk $D(0, Ms)$, because all elements of $L(i)^* L(i)$ are positive. By the Gershgorin circle theorem this yields that all eigenvalues of $L^*(i)L(i)$ lie in the circle $D(0, Ms)$ and the operator norm of $L(i)$ can be estimated by $\|L(i)\| \leq \sqrt{Ms}$. The Hanson-Wright inequality therefore implies that there is a universal constant $C > 0$ such that for $i \notin S$

$$\mathbb{P}\left(|X_2(i)| > \theta_2\right) \leq 2 \exp\left(-C \min\left(\frac{\theta_2^2}{R^4 Ms}, \frac{\theta_2}{R^2 \sqrt{Ms}}\right)\right),$$

and for $i \in S$

$$\mathbb{P}\left(|X_2(i) - M\sigma^2| > \theta_2\right) \leq 2 \exp\left(-C \min\left(\frac{\theta_2^2}{R^4 Ms}, \frac{\theta_2}{R^2 \sqrt{Ms}}\right)\right).$$

Estimation of X_3:
The estimation of $X_3(i)$ is even more involved. We can simplify

$$X_3(i) = \langle \Phi_\Theta \beta_0, \mathbb{1} \rangle \langle \mathbb{1}, \Phi_\Theta e_i \rangle = \beta_0^* \Phi_\Theta^* \mathbb{1}\,\mathbb{1}^*\,\Phi_\Theta e_i = \sum_{k\in S} \sum_{m\in\Theta} \sum_{l\in\Theta} b_{(k-m)(\mathrm{mod}\,N)} b_{(i-l)(\mathrm{mod}\,N)},$$

because $(\Phi_\Theta^* \mathbb{1}\,\mathbb{1}^*\,\Phi_\Theta)_{k,n} = \sum_{m\in\Theta}\sum_{l\in\Theta} b_{(k-m)(\mathrm{mod}\,N)} b_{(n-l)(\mathrm{mod}\,N)}$. We start by estimating the expected value of $X_3(i)$:

$$\begin{aligned} E_{k,n} :&= \mathbb{E}(\Phi_\Theta^* \mathbb{1}\,\mathbb{1}^*\,\Phi_\Theta)_{k,n} = \sum_{m\in\Theta}\sum_{l\in\Theta} \mathbb{E}\big(b_{(k-m)(\mathrm{mod}\,N)} b_{(n-l)(\mathrm{mod}\,N)}\big) \\ &= \sum_{m\in\Theta}\sum_{l\in\Theta} \begin{cases} \sigma^2 & \text{if } (k-m)(\mathrm{mod}\,N) = (n-l)(\mathrm{mod}\,N) \\ 0 & \text{else} \end{cases}. \end{aligned} \tag{11}$$

Note that $(k-m)(\mathrm{mod}\,N) = (n-l)(\mathrm{mod}\,N)$ if and only if $(k-m-n+l)(\mathrm{mod}\,N) = 0$. That is, if and only if $k-m-n+l \in \{-N, 0, N\}$, because $k-m-n+l \in (-2N, 2N)$. Let us identify when this is the case:

First, suppose that $k < n$, then we have $k-n-m < 0$, or more precisely either $k-n-m \in [-N,-1]$ or $k-n-m \in [-2N, -N-1]$. If the first case is true, l can only be chosen such that $k-n-m+l = 0$, because $l \in [N]$ there is no possibility that $k-n-m+l \in \{-N, N\}$. Analogously, if the second case is true, the only possibility to choose l such that $k-n-m+l \in \{-N, 0, N\}$ is $l = m+n-k-N$. In other words, for fixed $k < n$ and $m \in [N]$ there is exactly one $l \in [N]$ such that $(k-m)(\mathrm{mod}\,N) = (n-l)(\mathrm{mod}\,N)$. Similarly, we can show that the same is true for $k \geq n$.

However, the sum in (11) is not over $m, l \in [N]$ but over the smaller subset $m, l \in \Theta$. Thus, the number matching the criterion $(k-m)(\mathrm{mod}\,N) = (n-l)(\mathrm{mod}\,N)$ is smaller than $M = |\Theta|$, more precisely:

$$E_{k,n} = \begin{cases} |\Theta \cap ((k-n+\Theta) \cup (N+k-n+\Theta))|\sigma^2 & \text{if } k < n, \\ M\sigma^2 & \text{if } k = n, \\ |\Theta \cap ((k-n+\Theta) \cup (-N+k-n+\Theta))|\sigma^2 & \text{if } k > n. \end{cases} = |\Theta \cap (k-n+\Theta)|\sigma^2$$

It holds true that for $i \notin S$

$$\mathbb{E}(X_3(i)) = \big\langle \beta_0, (E_{k,i})_{k=1}^N \big\rangle = \sum_{k\in S} E_{k,i} = \sum_{k\in S} |\Theta \cap (k-i+\Theta)|\sigma^2 \in [0, sM\sigma^2] \tag{12}$$

and for $i \in S$ that

$$\mathbb{E}(X_3(i)) \in [M\sigma^2, sM\sigma^2]. \tag{13}$$

Now we can compute the probability that $X_3(i)$ deviates from its expected value. We again aim to apply the Hanson-Wright inequality. For this we define $L^3(i) : \mathbb{R}^N \to \mathbb{R}^N$, $(v_1, \dots, v_N) \mapsto (w_1, \dots, w_N)$ by

$$w_l = \begin{cases} \sum_{m\in\Theta}\sum_{k\in S} v_{(k-m)(\mathrm{mod}\,N)} & \text{if } l \in i - \Theta, \\ 0 & \text{else.} \end{cases}$$

This yields $X_3(i) = \big\langle b, L^3(i) b \big\rangle$. To compute the Hilbert-Schmidt norm and operator norm of $L_3(i)$, we further define the matrices $(K^1(i)_{n,m})_{n,m=1}^N$ and $(K^2(i)_{k,l})_{k,l=1}^N$ by

$$K^1(i)_{n,m} = \begin{cases} 1 & \text{if } n \in i-\Theta, m \in \Theta \\ 0 & \text{else,} \end{cases} \quad \text{and} \quad K^2(i)_{k,l} = \begin{cases} 1 & \text{if } k \in \Theta, l \in -k+S \\ 0 & \text{else.} \end{cases}$$

It is then easy to verify, that $K^1(i)K^2(i)v = L_3(i)(v)$. Now the Hilbert-Schmidt norm of $K^1(i)$ is given by $\|K^1(i)\|_{\mathrm{HS}}^2 = M^2$ and of $K^2(i)$ by $\|K^2(i)\|_{\mathrm{HS}}^2 = Ms$. Thus,

$$\|L_3(i)\|_{\mathrm{HS}}^2 = \|K^1(i)K^2(i)\|_{\mathrm{HS}}^2 \leq \|K^1(i)\|_{\mathrm{HS}}^2 \|K^2(i)\|_{\mathrm{HS}}^2 = M^3 s.$$

On the other hand, it holds true that

$$(K^1(i)K^2(i))_{m,n} = \begin{cases} \sum_{l\in\Theta\cap(S-n)} 1 & \text{if } m \in i-\Theta \\ 0 & \text{else.} \end{cases}$$

To use the Gershgorin circle theorem to estimate the operator norm of $L_3(i)$ we estimate the row sum of $L_3^*(i)L_3(i)$:

$$\sum_{j\in[N]} (L_3(i)^* L_3(i))_{l,j} = \sum_{j\in[N]} \sum_{k\in[N]} (L_3(i))_{k,l}(L_3(i))_{k,j} = \sum_{j\in[N]} \sum_{k\in i-\Theta} |\Theta\cap S-l||\Theta\cap S-j| \leq Ms \sum_{j\in[N]} |\Theta\cap S-j|,$$

where we used that $|i-\Theta| = M$ and $|\Theta\cap S-l| \leq |S-l| = s$. To estimate $\sum_{j\in[N]}|\Theta\cap S-j|$ note that each $n\in\Theta$ is exactly contained in s sets of the form $S-j$, in other words there are exactly s pairwise different $j_1,\dots,j_s\in[N]$ such that $n\in S-j_l$ for $l\in[s]$. Thus, it holds true that

$$\sum_{j\in[N]} |\Theta\cap S-j| = \sum_{j\in[N]} |\cup_{n\in\Theta}\{n\}\cap S-j| \leq \sum_{j\in[N]}\sum_{n\in\Theta} |\{n\}\cap S-j| = \sum_{n\in\Theta}\sum_{j\in[N]} |\{n\}\cap S-j| = \sum_{n\in\Theta} s = Ms.$$

We can conclude by the Gershgorin circle theorem that the largest eigenvalue of $L_3^*(i)L_3(i)$ is smaller than M^2s^2, which yields to

$$\|L_3(i)\| \leq Ms.$$

By the Hanson-Wright inequality it follows

$$\mathbb{P}\left(|X_3(i)-\mathbb{E}(X_3(i))| > \theta_3\right) \leq 2\exp\left(-C\min\left(\frac{\theta_3^2}{R^4M^3s}, \frac{\theta_3}{R^2Ms}\right)\right).$$

In particular, it follows for $i\notin S$

$$\begin{aligned}\mathbb{P}\left(X_3(i) < -\theta_3\right) &\leq \mathbb{P}\left(X_3(i) < \mathbb{E}(X_3(i)) - \theta_3\right) \leq \mathbb{P}\left(X_3(i)-\mathbb{E}(X_3(i)) < -\theta_3\right) \leq \mathbb{P}\left(|X_3(i)-\mathbb{E}(X_3(i))| > \theta_3\right) \\ &\leq 2\exp\left(-C\min\left(\frac{\theta_3^2}{R^4M^3s}, \frac{\theta_3}{R^2Ms}\right)\right),\end{aligned}$$

where we used (12) in the first step. For $i\in S$ it follows

$$\begin{aligned}\mathbb{P}\left(X_3(i) > \theta_3 + Ms\sigma^2\right) &\leq \mathbb{P}\left(X_3(i) > \theta_3 + \mathbb{E}(X_3(i))\right) \leq \mathbb{P}\left(X_3(i)-\mathbb{E}(X_3(i)) > \theta_3\right) \\ &\leq \mathbb{P}\left(|X_3(i)-\mathbb{E}(X_3(i))| > \theta_3\right) \leq 2\exp\left(-C\min\left(\frac{\theta_3^2}{R^4M^3s}, \frac{\theta_3}{R^2Ms}\right)\right),\end{aligned}$$

where we used (13).

Finally, we are able to estimate the probability that Equation (10) is true for $t = \frac{M\sigma^2}{16}$. To this end remember that $\rho = -\frac{\sigma^2}{2\mu}$ and choose

$$\theta_1 = \frac{\mu M}{8}, \qquad \theta_2 = \frac{|\rho|\mu M}{8}, \qquad \theta_3 = \frac{|\rho|\mu M^2}{8}.$$

Using that by Equation (8) we have in particular $M > 4s$ we derive for $i\in S$

$$\begin{aligned}\langle \nu, Ae_i\rangle &= \rho\mu M - |\rho|X_1(i) + X_2(i) - M^{-1}X_3(i) \geq \rho\mu M - |\rho|\theta_1 + M\sigma^2 - \theta_2 - s\sigma^2 - M^{-1}\theta_3 \\ &= \frac{11\rho\mu M}{8} + (M-s)\sigma^2 \geq \frac{11\rho\mu M}{8} + \frac{3M}{4}\sigma^2 = -\frac{11}{16}M\sigma^2 + \frac{3}{4}M\sigma^2 = \frac{M\sigma^2}{16}\end{aligned}$$

with a failure probability no larger than

$$s\left(2\exp\left(-\frac{C\mu M}{64R^2}\right) + 2\exp\left(-C\min\left(\frac{\rho^2\mu^2M}{64R^4s}, \frac{|\rho|\mu M}{8R^2\sqrt{Ms}}\right)\right) + 2\exp\left(-C\min\left(\frac{\rho^2\mu^2M}{64R^4s}, \frac{\rho\mu M}{8R^2s}\right)\right)\right).$$

On the other hand, we can estimate for $i \notin S$

$$\langle \nu, Ae_i \rangle \leq \rho\mu M + |\rho|\theta_1 + \theta_2 + M^{-1}\theta_3 = \frac{5\rho\mu M}{8} \leq -\frac{M\sigma^2}{16}$$

with a failure probability no larger than

$$(N-s)\left(2\exp\left(-\frac{C\mu M}{64R^2}\right) + 2\exp\left(-C\min\left(\frac{\rho^2\mu^2 M}{64R^4 s}, \frac{|\rho|\mu M}{8R^2\sqrt{Ms}}\right)\right) + 2\exp\left(-C\min\left(\frac{\rho^2\mu^2 M}{64R^4 s}, \frac{\rho\mu M}{8R^2 s}\right)\right)\right).$$

This finishes the proof of Part *i)* of Theorem 1.4.

Now we aim to prove **Part *iii)***. Applying Proposition 2.2, we particularly need to prove the boundedness of the dual certificate ν, i.e., $\|\nu\|_2 \leq r$, for some $r > 0$. First, note that

$$\|\nu\|_2^2 \leq M\rho^2 + \langle \Phi_\Theta \beta_0, \Phi_\Theta \beta_0 \rangle .$$

Thus, we in particular need to bound $\langle \Phi_\Theta \beta_0, \Phi_\Theta \beta_0 \rangle$. It is easy to verify that

$$\langle \Phi_\Theta \beta_0, \Phi_\Theta \beta_0 \rangle = \sum_{n\in\Theta} \sum_{k\in S} \sum_{l\in S} b_{(k-n)(\mathrm{mod}\, N)} b_{(l-n)(\mathrm{mod}\, N)}.$$

Because $(k-n)(\mathrm{mod}\, N) = (l-n)(\mathrm{mod}\, N)$ if and only if $k = l$ we obtain

$$\mathbb{E}(\langle \Phi_\Theta \beta_0, \Phi_\Theta \beta_0 \rangle) = \sum_{n\in\Theta} \sum_{k\in S} \sum_{l\in S} \mathbb{E}(b_{(k-n)(\mathrm{mod}\, N)} b_{(l-n)(\mathrm{mod}\, N)}) = \sum_{n\in\Theta} \sum_{k\in S} \mathbb{E}(b_{(k-n)(\mathrm{mod}\, N)} b_{(k-n)(\mathrm{mod}\, N)}) = Ms\sigma^2.$$

To estimate the deviation of $\langle \Phi_\Theta \beta_0, \Phi_\Theta \beta_0 \rangle$ from its expected value we define $L : \mathbb{R}^N \to \mathbb{R}^N$, $(v_1, \dots v_N) \mapsto (w_1, \dots, w_N)$ by

$$w_i = \begin{cases} \sum_{k\in S} v_{(k-i)(\mathrm{mod}\, N)} & \text{if } i \in \Theta \\ 0 & \text{else.} \end{cases}$$

Then it holds true that $\langle \Phi_\Theta \beta_0, \Phi_\Theta \beta_0 \rangle = \langle Lb, Lb \rangle := \langle b, Kb \rangle$, with $K := L^*L$. To again apply the Hanson-Wright inequality we need to estimate the Hilbert-Schmidt norm $\|K\|_{\mathrm{HS}}$ as well as the operator norm $\|K\|$ of K. Note that L can be represented by the matrix $[L_{i,j}]_{i,j=1}^N$, where

$$L_{i,j} = \begin{cases} 1 & \text{if } i \in \Theta \text{ and } j \in S - i \\ 0 & \text{else} \end{cases} = \begin{cases} 1 & \text{if } i \in \Theta \cap S - j \\ 0 & \text{else} \end{cases}.$$

Further K can be represented by the matrix $[K_{k,l}]_{k,l=1}^N$ with

$$K_{k,l} = \sum_{i=1}^N L_{k,i}^* L_{i,l} = \sum_{i\in\Theta\cap(S-k)\cap(S-l)} 1 = |\Theta \cap (S-k) \cap (S-l)|.$$

By the Gershgorin circle theorem all eigenvalues of K lie in the circle $D(0, \sum_{k\in[N]} K_{kl})$ for all $l \in [N]$ and

$$\sum_{k\in[N]} K_{k,l} = \sum_{k\in[N]} |\Theta \cap (S-k) \cap (S-l)| \leq \sum_{k\in[N]} |(S-k) \cap (S-l)| \leq s^2,$$

where the last step follows from the following fact: Let $l \in [N]$ and $S - k = \{k_1, \dots, k_s\}$ then for $i \in [s]$ it holds true that $k_i \in S - (k_j - k_i)$ for each $j \in [s]$. Thus, each $k_i \in S - k$ is contained in exactly s sets of the form $S - r$. Therefore, we can conclude $\|K\| \leq s^2$ and $\|L\| = \sqrt{\lambda_{\max}(L^*L)} = \sqrt{\lambda_{\max}(K)} = s$, where $\lambda_{\max}$ denotes the largest eigenvalue. Further, it is easy to verify by the matrix representation that $\|L\|_{\mathrm{HS}} = \sqrt{Ms}$ and therefore by (1)

$$\|K\|_{\mathrm{HS}}^2 = \|L^*L\|_{\mathrm{HS}}^2 \leq \|L^*\|^2 \|L\|_{\mathrm{HS}}^2 \leq Ms^3.$$

By the Hanson-Wright inequality it now follows

$$\mathbb{P}\left(|\langle \Phi_\Theta \beta_0, \Phi_\Theta \beta_0\rangle - Ms\sigma^2| \geq Ms\sigma^2\right) \leq 2\exp\left(-c\min\left(\frac{M\sigma^4}{sR^4}, \frac{M\sigma^2}{R^2 s}\right)\right).$$

Thus $\langle \Phi_\Theta \beta_0, \Phi_\Theta \beta_0\rangle \leq 2Ms\sigma^2$ with high probability. And more precisely we derive for the dual certificate that $\|\nu\|_2^2 \leq M\sigma^2\left(\frac{\sigma^2}{4\mu^2} + 2s\right)$ with probability $1-\varepsilon$ if $M \gtrsim \max\left(\frac{R^4}{\sigma^4}, \frac{R^2}{\sigma^2}\right)\ln\left(\frac{2}{\varepsilon}\right) s$ for some $\varepsilon > 0$.

It remains to prove **Part *ii)***. For this purpose, it is enough to argue that the previous proof also applies to Toeplitz matrices of the form (6). To see this, note that Toeplitz matrices are submatrices of circulant matrices. More precisely, let $T = T(c_{-N+1}, c_{-N+2}, \ldots, c_{N-1}) \in \mathbb{R}^{N,N}$ then T is the submatrix of $\Phi([c_0, \ldots, c_{N-1}, c_{-N+1}, \ldots, c_{-1}]) \in \mathbb{R}^{2N-1,2N-1}$ consisting of the first N columns and rows of Φ, i.e., $T_{i,j} = C_{i,j}$ for $i, j \in [N]$.

Define $A = \mu\,\mathbb{1} + T_\Theta$ and $B = \mu\,\mathbb{1} + \Phi_\Theta$. For the dual certificate ν and $i \in [N]$ it then holds true that $\langle \nu, Ae_i\rangle = \langle \nu, B\tilde{e}_i\rangle$, where $\tilde{e}_i$ denotes the i-th canonical vector in $\mathbb{R}^{2N-1}$. Further note that $Ax = B[x \quad \vec{0}]$ for $x \in \mathbb{R}^N$, where $\vec{0} \in \mathbb{R}^{N-1}$.

Thus, the former proof shows that $B^*\nu \in \tilde{H}_S^t := \left\{w \in \mathbb{R}^{2N-1} : w_i \leq -t \text{ for } i \in S \text{ and } w_i \geq t \text{ for } i \in [N] \setminus S\right\}$ for some $t > 0$. Note that for $w \in \tilde{H}_S^t$, the last $N-1$ entries of w can be arbitrary. Moreover, it is easy to prove similarly as in [5] (cf. Proposition 2.3 in [5]) that this is equivalent to

$$\left\{x \in [0,1]^{2N-1} : Bx = B\,\mathbb{1}_S\right\} \cap \left\{x \in [0,1]^{2N-1} : x_i = 0, i = N+1, \ldots, 2N-1\right\} = \mathbb{1}_S \in \mathbb{R}^{2N-1}.$$

Hence, $\left\{x \in [0,1]^N : Ax = A\,\mathbb{1}_S\right\} = \mathbb{1}_S \in \mathbb{R}^N$, under same assumption of Theorem 1.4. □

Remark 2.4 *Note that the (implicit) constant in Equation (8) is doubled in comparison to the result in [5] for non-structured matrices. The main reason is the pessimistic estimation of the expected value of $X_3(i)$ in Equation (13). Particularly, $\mathbb{E}X_3(i) = sM\sigma^2$ can only be true for very specific choices of Θ and S. Suppose $\Theta = \{m, m+k, m+2k, \ldots, m+(M-1)k\}$ such that $Mk = N$ and $S_i = \{0, k, 2k, 3k, (s-1)k\}$ then $\mathbb{E}X_3(i) = sM\sigma^2$. However, if there is no $k \in S$ such that $\Theta = \{m, m+k, m+2k, \ldots, m+(M-1)k\}$ then $|\Theta \cap (k+\Theta)| \leq (M-1)$. Moreover, if $S_i \neq \{0, k, 2k, 3k, (s-1)k\}$ for some k, then for $l \in S_i, l \neq k$, it holds true that $|\Theta \cap (l+\Theta)| \leq (M-1)$.*

One possibility to ensure that $\mathbb{E}(X_3(i)) \leq \frac{Ms}{2}$, which gives the same constant as in [5], is to choose $\Theta = \{m_1 > m_2 > \ldots m_M\}$ such that every possible distance between m_i and m_{i+1} arises at most $M/2$-times. This might be possible because we may assume that $M \leq \frac{N}{2}$ by what the numerics indicate (see Section 3).

3 Numerical Validation

To support our theory, we aim to conclude by showing the results of the following numerical experiments. Basically, we run the boxed-constrained basis pursuit (3) and the box-constrained least squares (4) for biased circulant matrices $\Phi(b)$ and Toeplitz matrices $T(b)$ for either Gaussian or Rademacher input vectors. For all experiments we choose the ambient dimension to be $N = 500$. For each $s, M \in \{5i : i \in [100]\}$ we choose a random binary vector $x_0 \in \mathbb{R}^N$ with s-non-zero elements. These s-non-zero positions of x_0 are chosen uniformly randomly from 1 to 500 without repetition (Matlab method *randperm*). Then we constructed the different structured measurement matrices and run boxed constrained linear least squares (Matlab method *lsqlin*) as well as the linear program *linprog* with box constraints to obtain reconstructions x_{LS} and x_{PBin} of x_0. Finally we computed the ℓ_2-error $\|x_{\text{LS}} - x_0\|_2$ and $\|x_{\text{PBin}} - x_0\|_2$ and repeated the computation for each combination of s and M 100-times.

The measurement matrices were constructed as follows. For the Rademacher Toeplitz matrix we choose $c = [c_1, \ldots, c_N] \in \mathbb{R}^N$ and $r = [r_1, \ldots, r_{N-1}] \in \mathbb{R}^{N-1}$ such that c_i, r_j are either 0 or 1 with equal probability for $i \in [N]$, $j \in [N-1]$. Then we define $A = \text{toeplitz}(c, [c_1\ r])$, thus c is the first column of A and $[c_1\ r]$ the first row. Finally we choose a random subset $\Theta \subset [N]$ of size $|\Theta| = M$ by randomly permutating $[N]$ and choosing the first M numbers (matlab method *randperm*(N, M)). The measurement matrix Φ then consist of the columns A which correspond to the subset Θ.

The Gaussian Toeplitz matrix is constructed analogously but with $c \in \mathbb{R}^N$ and $r \in \mathbb{R}^{N-1}$ shifted Gaussian random vectors, i.e., $c = g_c + \mathbb{1}$ and $r = g_r + \mathbb{1}$, where $g_c \in \mathbb{R}^N$ and $g_r \in \mathbb{R}^{N-1}$ are Gaussian vectors.

To construct the partial circulant matrices we choose $c \in \mathbb{R}^N$ as in the Toeplitz case either as shifted Rademacher or Gaussian vector. Then we flipped c and shifted it circularly by one position to obtain the row vector $r \in \mathbb{R}^N$ ($r = circshift(fliplr(c),1,2)$). Then we define $A = \text{toeplitz}(c, r)$ and the measurement matrix Φ as in the Toeplitz case.

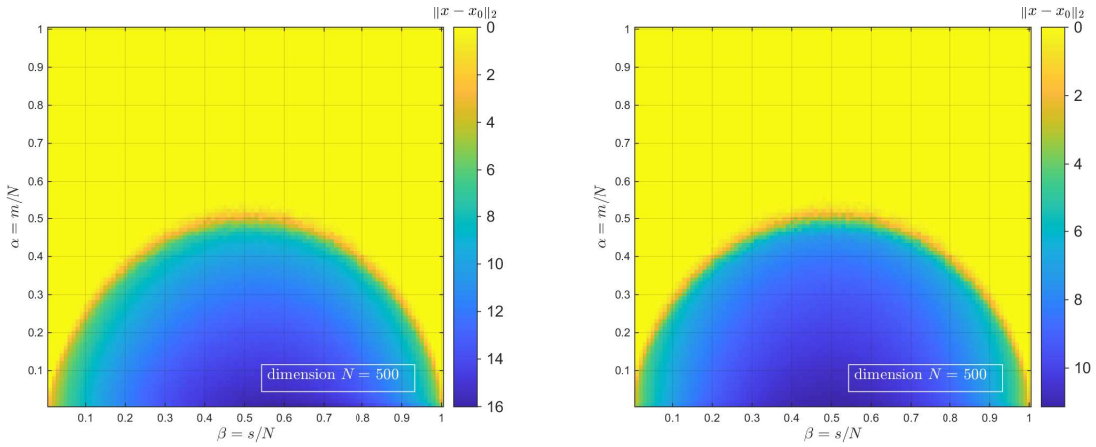

Figure 2: Reconstruction from biased Rademacher Toeplitz measurements via (3) (left) and (4) (right). The experiment yielding this figure is explained above.

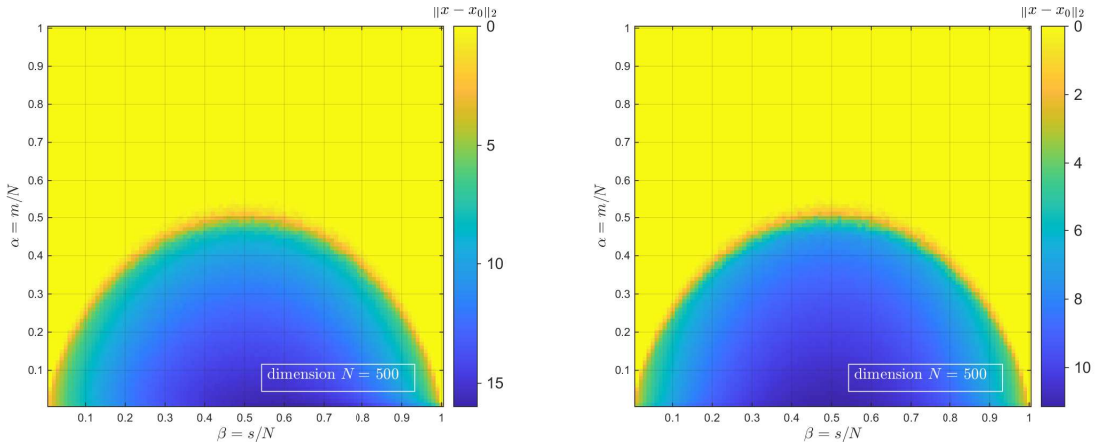

Figure 3: Reconstruction from biased Gaussian Toeplitz measurements via (3) (left) and (4) (right). The experiment yielding this figure is explained above.

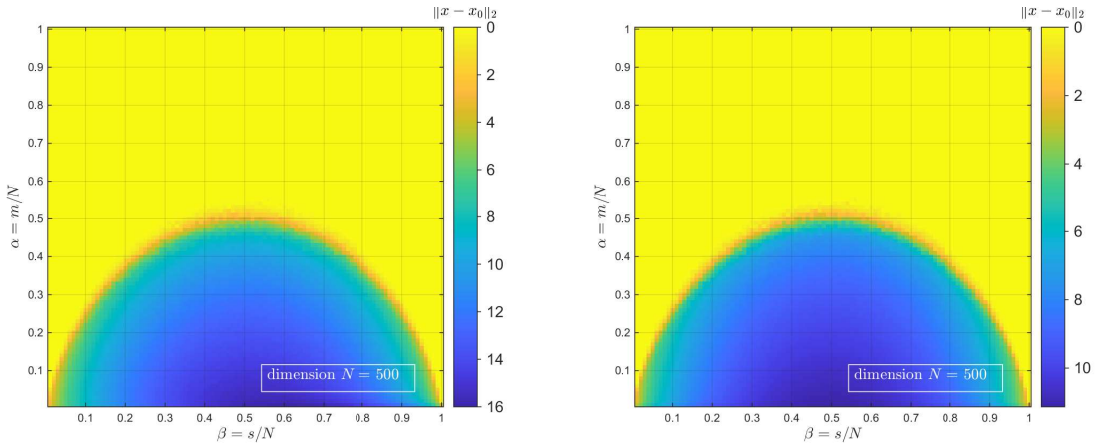

Figure 4: Reconstruction from biased Rademacher circulant measurements via (3) (left) and (4) (right). The experiment yielding this figure is explained above.

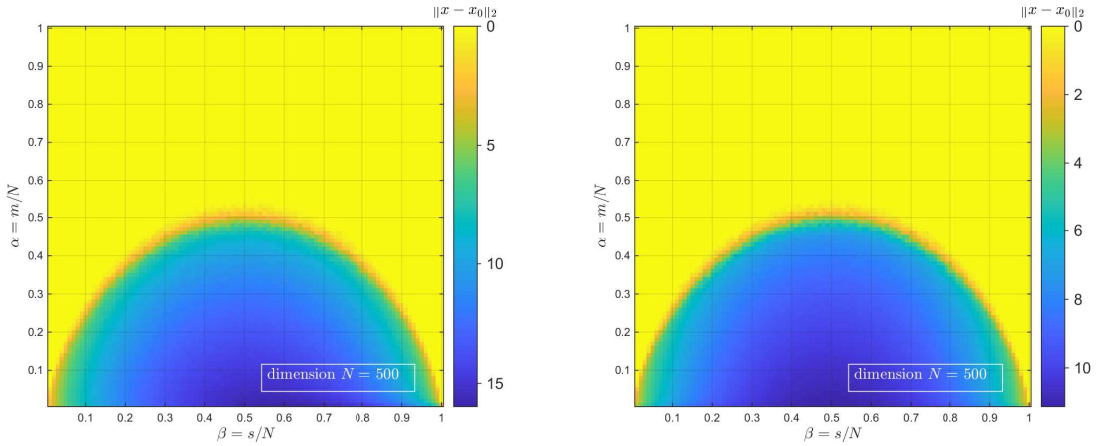

Figure 5: Reconstruction from biased Gaussian circulant measurements via (3) (left) and (4) (right). The experiment yielding this figure is explained above.

4 Outlook and Future Work

In this paper we have studied the reconstruction of a binary, sparse signal $x_0 \in \{0,1\}^N$ from biased partial random circulant and Toeplitz measurements $y = Ax_0 + n$, where n is some small noise vector and $A = \Phi(b) + \mu \mathbb{1}$. Here, $\Phi(b)$ a partial random circulant or Toeplitz matrix and b is a sub-Gaussian vector. In particular, we have studied the reconstruction via basis pursuit with box constraints and linear least squares with box constraints. Surprisingly, we could prove that the least squares strategy, which usually does not promote sparsity, works comparably well. We further showed that we need as many measurements to recover an s-sparse signal as we need to recover an $(N - s)$-sparse signal and that this number is about $\min\{s, N - s\} \log N$. Finally, we substantiated our theory by some numerical simulations.

The numerical simulations further indicate that, as for non-structured sub-Gaussian measurements, the number of necessary measurements M to ensure unique recovery (independently of the sparsity) is not larger than $M = N/2$. In the following we would like to explain some thoughts on this phenomenon and a possible proof of it.

In order to prove the mentioned phenomenon, we would need to show that the measurement matrix Φ_Θ is in general position and orthant symmetric; see the proof of Theorem III.2 in [5], for comparison.

Note, that Φ_Θ is in general position if for every subset $B \subset [N]$ of cardinality $|B| = M$ the eigenvalues of the matrix $(\Phi_\Theta^B)^* \Phi_\Theta^B$ are positive, i.e., if $\lambda(\Phi_\Theta^B)^* \Phi_\Theta^B) > 0$ or $s_N(\Phi_\Theta^B) \geq 0$, respectively, where $s_N(A)$ denotes the smallest singular value of a matrix $A \in \mathbb{R}^{N,N}$. Note that there exists a lot of work in the literature calculating the probability of $\lambda(\Phi^*\Phi) > 0$ ([9, 14]), but an analogous calculation for $\lambda((\Phi^B)^*\Phi^B)$ is much more difficult. The main reason is that the eigenvalues of Φ itself can be computed very easily, which is not the case for a submatrix. In particular it has been shown in [14], for Rademacher sequences $(b_0, \dots, b_{N-1})$ (among others) that for all $\varepsilon > 0$ and large N

$$\mathbb{P}\left(s_N(\Phi(b)) \geq \varepsilon N^{-1}\right) \geq 1 - C\varepsilon, \tag{14}$$

where $C > 0$ is a constant only depending on b. Since Φ_Θ^B seems to be more unstructured than Φ itself one might hope that the probability of $\lambda((\Phi_\Theta^B)^*\Phi_\Theta^B) > 0$ is even higher.

However, the proof of Theorem III.2 in [5], is also based upon the fact that the random part Φ of the measurement matrix $A = \mu \mathbb{1} + \Phi$ has an orthant symmetric kernel. This means, if for each diagonal matrix $S \in \mathbb{R}^{N,N}$ with diagonal in $\{-1, 1\}^N$ and every measurable set $\Omega \in \mathbb{R}^{M,N}$, it holds $\mathbb{P}(BS \in \Omega) = \mathbb{P}(B \in \Omega)$, where B is a matrix whose rows span the kernel of Φ.

From our point of view, it seems to be very unlikely that this is true for partial circulant matrices. The reason is the following. Suppose the kernel of Φ_Θ is spanned by $v_1, \dots, v_m$, for some $m \in [N]$, and let $B \in \mathbb{R}^{m,N}$ the matrix with rows $v_1', \dots, v_m'$, then the rows of BS span the kernel of TS. But TS is in general no circulant marix.

So for future work it is interesting to check if the kernel of a partial circulant matrix is indeed not or perhaps is orthant symmetric. Independently of the answer to this question it might be of own interest to prove an inequality in the spirit of (14) for partial circulant matrices. And, if the answer to the first question is negative, to find an alternative way to proof the upper bound on the necessary number of measurements in the order of $M \lesssim N/2$.

Acknowledgements

Sandra Keiper acknowledges support by the DFG Collaborative Research Center TRR 109 "Discretization in Geometry and Dynamics" and support by the Berlin Mathematical School.

References

[1] S. Dirksen, H. Jung, and H. Rauhut, *One-bit compressed sensing with partial gaussian circulant matrices*, Inf. Inference (2019).

[2] S. Dirksen and A. Stollenwerk, *Fast binary embeddings with gaussian circulant matrices: Improved bounds*, Discrete Comput. Geom. **60** (2018), 599–626.

[3] D. L. Donoho and J. Tanner, *Counting faces of randomly-projected polytopes when the projection radically lowers dimension*, J. Amer. Math. Soc **22** (2009), no. 1, 1–53.

[4] J.-M. Feng, F. Krahmer, and Saab R., *Quantized compressed sensing for partial random circulant matrices*, Comput. Harmon. Anal. **47** (2019), no. 3, 1014–1032.

[5] A. Flinth and S. Keiper, *Recovery of binary sparse signals with biased measurement matrices*, IEEE Trans. Inf. Theory **65** (2019), no. 12, 8084–8094.

[6] S. Foucart and H. Rauhut, *A mathematical introduction to compressive sensing*, Applied and Numerical Harmonic Analysis. Birkhäuser Basel, 2013.

[7] J. J. Fuchs, *On sparse representations in arbitrary redundant bases*, IEEE Trans. Inf. Theory **50** (2004), no. 6, 1341–1344.

[8] S. Gerschgorin, *Über die abgrenzung der eigenwerte einer matrix*, Izv. Akad. Nauk. USSR Otd. Fiz.-Mat. Nauk **7** (1931), 749–754.

[9] Robert M. Gray, *Toeplitz and circulant matrices: a review*, Found. Trends Commun. Inf. Theory **2** (2006), no. 3, 155–239.

[10] D. Gross, *Recovering low-rank matrices from few coefficients in any basis*, IEEE Trans. Inf. Theory **57** (2011), no. 3, 1548–1566.

[11] J. Haupt, W. U. Bajwa, G. Raz, and R. Nowak, *Toeplitz compressed sensing matrices with applications to sparse channel estimation*, IEEE Trans. Inf. Theory **56** (2010), no. 11, 5862–5875.

[12] S. Keiper, G. Kutyniok, D. G. Lee, and G. Pfander, *Compressed sensing for finite-valued signals*, Linear Algebra Appl. **532** (2017), 570–613.

[13] R. Kueng and P. Jung, *Robust nonnegative sparse recovery and the nullspace property of 0/1 measurements*, IEEE Trans. Inf. Theory **64** (2018), no. 2, 689–703.

[14] Paulo Cesar Manrique Miron, *Contributionson non–asymptotic singularity of random matrices and on backbend percolation*, Ph.D. thesis, Centro de Investigacion en Matematicas, A.C., 2017.

[15] H. Rauhut, *Compressive sensing and structured random matrices*, Theoretical Foundations and Numerical Methods for Sparse Recovery (M. Fornasier, ed.), deGruyter, 2010, p. 1–92.

[16] J. Romberg, *Compressive sensing by random convolution*, SIAM J. Imaging Sci. **2** (2009), no. 4, 1098–1128.

[17] Mark Rudelson and Roman Vershynin, *Hanson-wright inequality and sub-gaussian concentration*, Electron. Commun. Probab. **18** (2013), 9 pp.

[18] M. Stojnic, *A simple performance analysis of ℓ_1 optimization in compressed sensing*, IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP), 2009, pp. 3021–3024.

[19] ———, *Recovery thresholds for ℓ_1 optimization in binary compressed sensing*, IEEE International Symposium on Information Theory (ISIT), 2010, pp. 1593–1597.

[20] J. A. Tropp, *Recovery of short, complex linear combinations via ℓ_1 minimization*, IEEE Trans. Inf. Theory **51** (2005), no. 4, 1568–1570.

[21] J. A. Tropp, *Convex recovery of a structured signal from independent random linear measurements*, Sampling Theory, a Renaissance: Compressive sampling and other developments, Birkhäuser, Basel, 2015.

[22] R. Vershynin, *High-dimensional probability: An introduction with applications in data science*, Cambridge University Press, 2018.