

Fast and Robust Compressive Phase Retrieval with Sparse-Graph Codes

Dong Yin, Kangwook Lee, Ramtin Pedarsani, and Kannan Ramchandran

Department of Electrical Engineering and Computer Sciences

University of California, Berkeley

Email: {dongyin, kw1jjang, ramtin, kannan}@eecs.berkeley.edu

Abstract—In this paper, we tackle the compressive phase retrieval problem in the presence of noise. The noisy compressive phase retrieval problem is to recover a K -sparse complex signal $s \in \mathbb{C}^n$, from a set of m noisy quadratic measurements: $y_i = |\mathbf{a}_i^H \mathbf{s}|^2 + w_i$, where $\mathbf{a}_i^H \in \mathbb{C}^n$ is the i th row of the measurement matrix $\mathbf{A} \in \mathbb{C}^{m \times n}$, and w_i is the additive noise to the i th measurement. We consider the regime where $K = \beta n^\delta$, $\delta \in (0, 1)$. We use the architecture of *PhaseCode* algorithm [1], and robustify it using two schemes: the almost-linear scheme and the sublinear scheme. We prove that with high probability, the almost-linear scheme recovers s with sample complexity¹ $\Theta(K \log(n))$ and computational complexity $\Theta(n \log(n))$, and the sublinear scheme recovers s with sample complexity $\Theta(K \log^3(n))$ and computational complexity $\Theta(K \log^3(n))$. To the best of our knowledge, this is the first scheme that achieves sublinear computational complexity for compressive phase retrieval problem. Finally, we provide simulation results that support our theoretical contributions.

I. INTRODUCTION

A. Problem Formulation

In this paper, we consider the noisy compressive phase retrieval problem. The noisy compressive phase retrieval problem is to recover a sparse complex signal s , from a set of quadratic measurements

$$y_i = |\mathbf{a}_i^H \mathbf{s}|^2 + w_i, \quad i \in [m],$$

where $\mathbf{a}_i^H \in \mathbb{C}^n$ are rows of the measurement matrix $\mathbf{A} \in \mathbb{C}^{m \times n}$, w_i 's are noise, and $[m]$ denotes the set $\{1, 2, \dots, m\}$. We assume that w_i 's are independent, zero-mean, sub-exponential [2] random variables. This model is considered in many phase retrieval literatures [3]–[5]. As mentioned in [3], in many applications such as optics [6], one can measure squared-magnitudes rather than magnitudes. Our goal is to design \mathbf{A} and recover s up to a global phase from the y_i 's with small sample and computational complexity. Although the measurement matrix cannot be freely designed in some cases [7], considering the most general compressive phase retrieval problem can provide the insight to tackle more constrained problems. Moreover, there is no constraint on the design of \mathbf{A} in some applications such as quantum optics [8].

¹Here, we define the notations $\mathcal{O}(\cdot)$, $\Theta(\cdot)$, and $\Omega(\cdot)$. We have $f = \mathcal{O}(g)$ if and only if there exists a constant $C_1 > 0$ such that $|f/g| < C_1$; $f = \Theta(g)$ if and only if there exist two constants $C_1, C_2 > 0$ such that $C_1 < |f/g| < C_2$; and $f = \Omega(g)$ if and only if there exists a constant $C_1 > 0$ such that $|f/g| > C_1$.

We also assume that signal s is quantized, which means that the components of s lie in a finite set of complex numbers. More specifically, let L_m and L_p be the number of possible magnitudes and phases of the non-zero components, respectively, and each component of s is in the set

$$\mathbb{S} = \{u \varepsilon e^{i \frac{2\pi(v-1)}{L_p}} \mid u \in [L_m], v \in [L_p]\} \cup \{0\} \subset \mathbb{C},$$

where $\varepsilon > 0$ and i denotes the imaginary unit. Quantized signals can be good approximations of the real world signals and are natural for signal processing with computers [9], [10]. Additionally, we assume s is K -sparse², i.e., $|\text{supp}(s)| = K$. In this paper, we consider the regime where there exist two constants β and δ such that $K = \beta n^\delta$, $\delta \in (0, 1)$.

B. Main Contributions

In this paper, we propose two schemes: *almost-linear* and *sublinear* schemes for noisy compressive phase retrieval. These two schemes are robust versions of the PhaseCode algorithm [1], which is a fast and effective framework for the noiseless scenarios. The key idea of PhaseCode is the usage of sparse-graph codes, a powerful tool from coding theory. Sparse-graph codes have been widely applied in communications [11] and signal processing [12], [13]. The main advantage of our schemes is the small sample and computational complexity³, as shown in Table I.

TABLE I: Sample and computational complexity

	almost-linear	sublinear
sample complexity	$\Theta(K \log(n))$	$\Theta(K \log^3(n))$
computational complexity	$\Theta(n \log(n))$	$\Theta(K \log^3(n))$

The sublinear scheme uses slightly more samples than the almost-linear scheme but the computational complexity is much smaller. To the best of our knowledge, the sublinear scheme is the first proposed algorithm that achieves sublinear computational complexity in the signal dimension n for compressive phase retrieval problem.

II. RELATED WORK

A. Previous Works on Robust Phase Retrieval

The phase retrieval problem has been studied extensively over several decades. We do not attempt to provide a compre-

²We define the *support*, denoted by $\text{supp}(s)$, to be the set of the indices of the non-zero components of s .

³In this paper, we set $\log(n)$ to be \log base 2.

hensive literature review here; instead, we highlight only some of the pertinent and diverse approaches to this problem that we are aware of. There are two popular classes of approaches, one based on convex-optimization methods, and the other based on greedy methods such as gradient descent and alternation minimization. In the first class, the bulk of the literature on phase retrieval problems is dedicated to the non-sparse signal regime, where the signal has no sparsity-structure to be exploited. “Phaselift” [3] and “PhaseCut” [14] are seminal examples of this class, featuring the use of convex relaxation methods based on Semi-Definite Programming (SDP). While SDP-based algorithms can provide provable performance guarantees and are robust to noise, they typically suffer from prohibitively high computational and memory complexity. There are also interesting works on the use of SDP-based approaches to exploit signal sparsity in the compressive phase retrieval [5], [15]–[17]. The second class of methods, which are popular in practice, is based on greedy methods. In general, these algorithms have a reasonable computational complexity, and are therefore used in many practical applications [18]. However, with the exception of a few recent works [19], [20], this class of algorithms generally comes with little theoretical guarantees.

B. PhaseCode algorithm

As mentioned in Section I, our proposed schemes are based on the PhaseCode algorithm. Here we briefly review the basic ideas of PhaseCode⁴.

The PhaseCode algorithm iteratively recovers the non-zero components via a *ball coloring* algorithm based on a “divide-and-conquer” philosophy. The measurement matrix of PhaseCode algorithm $\mathbf{A} \in \mathbb{C}^{4M \times n}$ is designed to be a row tensor product of a trigonometric modulation matrix $\mathbf{A}_0 \in \mathbb{C}^{4 \times n}$ and a code matrix $\mathbf{H} \in \{0, 1\}^{M \times n}$, i.e., $\mathbf{A} = \mathbf{A}_0 \otimes \mathbf{H}$. This means we have $\mathbf{A} = [\mathbf{A}_1^H \ \mathbf{A}_2^H \ \dots \ \mathbf{A}_M^H]^H$, where $\mathbf{A}_i = \mathbf{A}_0 \text{diag}(\mathbf{h}_i) \in \mathbb{C}^{4 \times n}$ and \mathbf{h}_i is the i th row of \mathbf{H} . Here, $\text{diag}(\mathbf{h}_i)$ denotes a diagonal matrix whose diagonal entries are the entries of \mathbf{h}_i . Each of the \mathbf{A}_i 's gives us a set of 4 measurements. PhaseCode's measurement system can be equivalently represented using a balls-and-bins model, or a bipartite graph model. In this representation, there are n balls and M bins, and the balls and bins correspond to the components of \mathbf{s} and the sets of 4 measurements, respectively. Then, \mathbf{A}_i is the measurement matrix of the i th bin, and \mathbf{H} is the biadjacency matrix of the bipartite graph. To be specific, if $h_{ij} = 1$, the j th ball is put into the i th bin. For example, in Figure 1, the third bin has $\mathbf{h}_3 = [0 \ 0 \ 1 \ 1 \ 0 \ 1]$. If a ball corresponds to one of the K non-zero components of \mathbf{s} , it is called an *active ball*. And we simply choose the bipartite graph to be d -left regular, i.e., each ball is connected to d bins chosen from the M bins uniformly at random.

We can classify bins according to the number of active balls in them. A *zeroton* is a bin with no active balls; a *singleton* is a bin with one active ball, which is called a *singleton ball*;

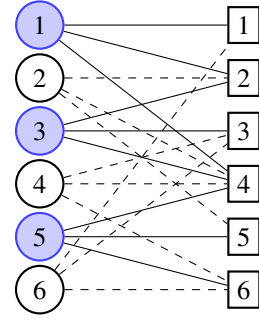


Fig. 1: An example of PhaseCode. Bins 1, 3, 5, 6 are singletons with singleton balls 1, 3, 5, 6, which can be found in the first iteration of PhaseCode algorithm. Then, the algorithm finds a strong doubleton: bin 2, and the relative phases between balls 1 and 3. In the next iteration, the algorithm finds a resolvable multiton bin 4 and colors ball 5. After that, no more balls can be colored. The algorithm stops and successfully finds all the non-zero components.

a *doubleton* is a bin with two active balls; a *multiton* is a bin with more than one active balls.⁵ We also define *strong doubletons*, which are doubletons consisting of two singleton balls. For a multiton, if we know the indices, magnitudes and relative phases of all of the active balls except one, we call it a *resolvable multiton*.

In the noiseless case, the 4 measurements in each bin are carefully designed so that the decoding algorithm can detect singletons, resolve strong doubletons and resolvable multitons. To be specific, the decoding algorithm can detect whether a bin is a singleton, and if it is, the decoder can find the location index and magnitude of the active ball; if magnitudes of the two active balls in a doubleton is known, the decoder can find their relative phase; for a resolvable multiton, the decoder can calculate the index and magnitude of the unknown ball, and the relative phase between this ball and others.

The decoding algorithm of PhaseCode is an iterative process. In the first iteration, it resolves all the singletons. In the second iteration, it resolves all the strong doubletons consisting of the singleton balls found in the previous iteration and gets the relative phases between the two singleton balls in them. Then, the algorithm finds the largest set of singleton balls whose relative phases are known and call these balls *colored*. In the following iterations, the algorithm iteratively checks whether the bins are resolvable multitons and colors the remaining balls. In [1], it is shown that in order to guarantee successful recovery with high probability, we need to use $M = \Theta(K)$ bins. It is proved that PhaseCode algorithm can recover a fraction $1 - p$, for arbitrarily small p , of the non-zero elements with probability $1 - \mathcal{O}(1/K)$, with $m = \Theta(K)$ measurements⁶ and the computational complexity of the algorithm is $\Theta(K)$. The PhaseCode algorithm is illustrated by a simple example in Figure 1.

In practice, the measurements are corrupted by noise, and in this case, we can not use only 4 measurements in each bin

⁵This implies that a doubleton is also a multiton.

⁶To be more specific, the authors characterized the exact number of measurements and the corresponding fraction of recoverable balls: $14K$ measurements with $p = 10^{-7}$.

⁴Here, we only consider the Unicolor PhaseCode algorithm.

for the decoding algorithm. However, we can robustify the algorithm by redesigning the measurement pattern \mathbf{A}_0 while keeping the code matrix \mathbf{H} and the ball coloring algorithm the same as the noiseless case.

III. MAIN RESULTS

We propose two schemes to robustify PhaseCode in the presence of noise: almost-linear scheme and sublinear scheme. The main results of this paper are the following theorems.

Theorem 1. *The almost-linear scheme can recover a fraction $1-p$, for arbitrarily small p , of the non-zero elements of \mathbf{s} with probability $1-\mathcal{O}(1/K)$, with $\Theta(K \log(n))$ measurements. The computational complexity of the algorithm is $\Theta(n \log(n))$.*

Theorem 2. *The sublinear scheme can recover a fraction $1-p$, for arbitrarily small p , of the non-zero elements of \mathbf{s} with probability $1-\mathcal{O}(1/K)$, with $\Theta(K \log^3(n))$ measurements. The computational complexity of the algorithm is $\Theta(K \log^3(n))$.*

See the proofs of Theorems 1 and 2 in Appendix B and E. Details of the measurement design and the decoding algorithm are shown in the following sections.

IV. ALMOST-LINEAR SCHEME

The idea of the almost-linear scheme is to encode the columns as different patterns. With the number of measurements in each bin being $\Theta(\log(n))$, the patterns are guaranteed to be different enough, so that we can successfully resolve singletons or uncolored balls in resolvable multitons.

A. Design of Measurements

Instead of using the 4-by- n trigonometric modulation matrix, we use a new random matrix $\mathbf{A}_0 = \{a_{ij}\}_{P \times n}$ whose entries are i.i.d. with the following distribution:

$$a_{ij} = \begin{cases} 0, & \text{with probability } 1/2 \\ e^{i\theta_{ij}}, & \text{with probability } 1/2, \end{cases} \quad (1)$$

where θ_{ij} 's are i.i.d. and uniformly distributed in $[0, 2\pi)$. We call \mathbf{A}_0 the *test matrix*, and we can show that we need $P = \Theta(\log(n))$ for each bin to achieve successful recovery.

For the almost-linear algorithm, the measurement matrix of the l th bin is $\mathbf{A}_l = \mathbf{A}_0 \text{diag}(\mathbf{h}_l)$. Without loss of generality, we omit bin index l , and simply use \mathbf{h} to denote the coding pattern of any bin. Then the measurements of this bin would be

$$y_i = |\mathbf{a}_i^H \text{diag}(\mathbf{h}) \mathbf{s}|^2 + w_i, \quad i \in [P], \quad (2)$$

where \mathbf{a}_i^H is the i th row of \mathbf{A}_0 , and the noise $w_i \in \mathbb{R}$, $i \in [n]$ satisfies the properties given in Section I. To simplify notation, we define a linear map \mathcal{A} from $\mathbb{C}^{n \times n}$ to \mathbb{R}^P :

$$\mathcal{A}: \mathbf{X} \mapsto \{\mathbf{a}_i^H \mathbf{X} \mathbf{a}_i\}_{i \in [P]}. \quad (3)$$

Now according to (2), by defining $\mathbf{x} = \text{diag}(\mathbf{h}) \mathbf{s}$, we have $\mathbf{y} = \mathcal{A}(\mathbf{x} \mathbf{x}^H) + \mathbf{w}$, where $\mathbf{y} = \{y_i\}_{i \in [P]}$ and $\mathbf{w} = \{w_i\}_{i \in [P]}$ are the measurement vector and noise vector, respectively. We call \mathbf{x} the *true signal* corresponding to this bin.

B. Decoding Algorithm

As mentioned in Section II, PhaseCode algorithm requires the measurements in each bin to handle three operations, i.e., detecting singletons, resolving strong doubletons, and detecting resolvable multitons and coloring the uncolored ball in it. Using our new measurement system, these operations can be done reliably by a simple guess-and-check method: we guess all possible indices, magnitudes, and relative phases, and use an energy test to decide whether our guess is correct. For any of the three operations, we make hypothesis on the unknown index, magnitude, and phase of the true signal \mathbf{x} and construct the corresponding hypothesis signal $\hat{\mathbf{x}}$. For example, when we do singleton detecting, if our hypothesis is that the bin is a singleton, and that the location index of the active ball is 5 with the magnitude being 3ε , we construct $\hat{\mathbf{x}} = 3\varepsilon \mathbf{e}_5$, where \mathbf{e}_i denotes the i th vector of the canonical basis. Similarly, we can resolve strong doubletons. For instance, suppose that we know a bin has two singleton balls, which are located at 2 and 5, respectively, and we also know the magnitudes of the two balls are 2ε and 3ε , respectively. Then, if we can make a hypothesis that the relative phase is $\frac{\pi}{4}$, we can construct $\hat{\mathbf{x}} = 2\varepsilon \mathbf{e}_2 + 3\varepsilon e^{i\frac{\pi}{4}} \mathbf{e}_5$. Then, we need to check whether our hypothesis is correct. To do this, we perform an ℓ_1 norm energy test shown in (4):

$$\begin{aligned} \hat{\mathbf{x}} \sim \mathbf{x}, & \text{ if } \frac{1}{P} \left\| \mathbf{y} - \mathcal{A}(\hat{\mathbf{x}} \hat{\mathbf{x}}^H) \right\|_1 < t_0, \\ \hat{\mathbf{x}} \not\sim \mathbf{x}, & \text{ otherwise,} \end{aligned} \quad (4)$$

where $\hat{\mathbf{x}} \sim \mathbf{x}$ means $\hat{\mathbf{x}}$ and \mathbf{x} are equal up to a global phase, and t_0 is the threshold. The intuitive reason why we do this test is that when $\hat{\mathbf{x}} \sim \mathbf{x}$, $\mathcal{A}(\hat{\mathbf{x}} \hat{\mathbf{x}}^H) = \mathcal{A}(\mathbf{x} \mathbf{x}^H)$, then $\mathbf{y} - \mathcal{A}(\hat{\mathbf{x}} \hat{\mathbf{x}}^H) = \mathbf{w}$, whose energy should be small. Conversely, when $\hat{\mathbf{x}} \not\sim \mathbf{x}$, the energy of $\mathbf{y} - \mathcal{A}(\hat{\mathbf{x}} \hat{\mathbf{x}}^H)$ should be large. Here, we give a result on the error probability of the energy test.

Lemma 1. *When $P = \Theta(\log(n))$ and ε is appropriately large, with proper threshold t_0 , the error probability of the energy test shown in (4) is $\mathcal{O}(1/n^2)$.*

The proof of this lemma follows the similar idea which appears in Lemma 14 in [21]. We can also show that we need to perform $\Theta(n)$ energy tests before the algorithm stops. Then, using Lemma 1 and some basic principles in probability theory, we can show that the failure probability of almost-linear scheme is $\mathcal{O}(1/K)$. As for the sample and computational complexity, since we have $\Theta(\log(n))$ measurements in each bin and $\Theta(K)$ bins, the sample complexity of almost-linear scheme would be $\Theta(K \log(n))$; and since the computational cost of each test is $\Theta(\log(n))$ and there are $\Theta(n)$ tests, the computational complexity of almost-linear scheme is $\Theta(n \log(n))$.

V. SUBLINEAR SCHEME

Although the $\mathcal{O}(n \log(n))$ computational complexity of almost-linear scheme is compelling, we can further improve the computational complexity. Recall that in the noiseless scenario, we get the location index of the singletons and the

uncolored balls in resolvable multitons by only looking at the measurements. Based on this idea, we propose the sublinear scheme for the noisy scenario, which can achieve much lower computational cost compared to the almost-linear scheme, at the cost of slightly larger sample complexity.

A. Design of Measurements

In the sublinear scheme, the measurement matrix in each bin is designed to be a concatenation of the test matrix \mathbf{A}_0 defined in the almost-linear scheme and R index matrices $\mathbf{F}_1, \dots, \mathbf{F}_R$. The test matrix \mathbf{A}_0 is still used to perform the energy tests and the index matrices are used to find the location indices.

Now we show how to design the index matrices. The main idea is to encode each column as a binary code such that we can directly decode the column index from the measurements. The similar idea is also used in the Chaining Pursuit method [22]. First, we define a deterministic matrix $\mathbf{B} = \{b_{ij}\} \in \{0, 1\}^{R \times n}$, where $R = \lceil \log n \rceil$, and the i th column of \mathbf{B} is the binary representation of the integer $i - 1$. For example, when $n = 4$, we have,

$$\mathbf{B} = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix}.$$

We use b_i and \mathbf{B}_j to denote the i th row and j th column of \mathbf{B} , respectively. Let $\mathbf{F}_0 \in \mathbb{C}^{Q \times n}$ be a random matrix whose elements are i.i.d. and uniformly distributed on the unit circle, and $\mathbf{F} = \mathbf{F}_0 \otimes \mathbf{B} \in \mathbb{C}^{RQ \times n}$. This means we have $\mathbf{F} = [\mathbf{F}_1^H \ \mathbf{F}_2^H \ \dots \ \mathbf{F}_R^H]^H$, where $\mathbf{F}_i = \mathbf{F}_0 \text{diag}(\mathbf{b}_i) \in \mathbb{C}^{Q \times n}$. By concatenating with the test matrix, the measurement matrix of the l th bin is $\mathbf{A}_l = [\mathbf{A}_0^H \ \mathbf{F}^H]^H \text{diag}(\mathbf{h}_l) \in \mathbb{C}^{(P+QR) \times n}$. Here, we give a simple example of \mathbf{A}_l . Let $n = 4$ and thus $R = 2$. We have

$$\mathbf{A}_l = \begin{bmatrix} \mathbf{A}_{0,1} & \mathbf{A}_{0,2} & \mathbf{A}_{0,3} & \mathbf{A}_{0,4} \\ \mathbf{0} & \mathbf{0} & \mathbf{F}_{0,3} & \mathbf{F}_{0,4} \\ \mathbf{0} & \mathbf{F}_{0,2} & \mathbf{0} & \mathbf{F}_{0,4} \end{bmatrix} \text{diag}(\mathbf{h}_l), \quad (5)$$

where $\mathbf{A}_{0,i}$'s and $\mathbf{F}_{0,i}$'s are the columns of \mathbf{A}_0 and \mathbf{F}_0 . We can show that we need $Q = \Theta(\log^2(n))$ to reliably find the correct location index and we also need $P = \Theta(\log(n))$ to perform energy tests.

Consequently, there are $R + 1$ sets of measurements. The first set $\mathbf{y}_0 = \{y_{0,i}\}_{i \in [P]}$ is the same as the measurements in almost-linear scheme and is called the *test measurements*:

$$y_{0,i} = |\mathbf{a}_i^H \mathbf{x}|^2 + w_{0,i}, \quad i \in [P],$$

where $\mathbf{x} = \text{diag}(\mathbf{h})\mathbf{s}$ and is still called the true signal. The other R sets $\mathbf{y}_j = \{y_{j,i}\}_{i \in [Q]}$, $j \in [R]$ correspond to the index matrices and are called the *index measurements*. Each set is composed of Q measurements:

$$y_{j,i} = |\mathbf{f}_{j,i}^H \mathbf{x}|^2 + w_{j,i}, \quad i \in [Q], \quad j \in [R],$$

where $\mathbf{f}_{j,i}^H$ is the i th row of \mathbf{F}_j . We also let \mathbf{w}_j 's be the noise vectors, $j \in \{0\} \cup [R]$.

B. Decoding Algorithm

The sublinear scheme can find the location index by only looking at the measurements. For example, assume that the bin with measurement matrix in (5) is a singleton whose non-zero component is at position 2. Then, the decoder can see that the elements of the first set of index measurements \mathbf{y}_1 have small absolute value since these measurements only contain noise. Now the decoder knows that the non-zero element should be in the first half of the signal. Then it sees that the elements in \mathbf{y}_2 have large energy. The decoder knows that if it is indeed a singleton, the only possible index of the non-zero component would be 2. Actually this procedure is a binary search on all the n indices of the signal. After this indexing process, the decoder can use the same way as the almost-linear scheme to construct a signal $\hat{\mathbf{x}}$ as the hypothesis of the true signal of this bin, and then use the testing measurements to perform the same energy test.

Now we formally show the details of the fast index search. Assume that $|\text{supp}(\mathbf{x})| = T$, and there are T_s uncolored balls in this bin. More specifically, $\mathbf{x} = \mathbf{x}_c + \mathbf{x}_s$, $|\text{supp}(\mathbf{x}_s)| = T_s$, $\text{supp}(\mathbf{x}_c) \cap \text{supp}(\mathbf{x}_s) = \emptyset$, and we know a vector $\hat{\mathbf{x}}_c \sim \mathbf{x}_c$. Note that when $T = T_s = 1$, we have $\hat{\mathbf{x}}_c = \mathbf{x}_c = 0$. Our goal is to find the index l_s of the non-zero element in \mathbf{x}_s when $T_s = 1$ and $\text{supp}(\mathbf{x}_s) = \{l_s\}$. When $T = 1$ and $T > 1$, we are looking for singleton balls and uncolored balls in resolvable multitons, respectively. We perform the following index tests for $j \in [R]$ with threshold $t_1 > 0$ to get l_s :

$$\tilde{b}_j = 0, \quad \text{if } \left| \frac{1}{Q} \sum_{i=1}^Q \tilde{y}_{j,i} \right| < t_1, \quad (6)$$

$$\tilde{b}_j = 1, \quad \text{otherwise.}$$

The index tests output a binary string $\tilde{\mathbf{b}} = \{\tilde{b}_j\}_{j \in [R]}$. We should also notice that if $T_s > 1$, we can still get an output after the index tests, but the energy test with the test measurements prevents us from making mistakes. Lemma 2 tells us that with high probability $\tilde{b}_j = b_{j,l_s}$.

Lemma 2. *When $Q = \Theta(\log^2(n))$, with proper threshold t_1 , if $\text{supp}(\mathbf{x}_s) = \{l_s\}$, then $\mathbb{P}\{\tilde{b}_j \neq b_{j,l_s}\} = \mathcal{O}(1/K^3)$.*

Similar to the almost-linear scheme, using Lemma 2, we can prove that the failure probability of sublinear scheme is $\mathcal{O}(1/K)$. Since the total number of measurements in each bin is $P + RQ = \Theta(\log^3(n))$, the sample complexity of sublinear scheme is $\Theta(K \log^3(n))$. In terms of the computational complexity, since there are $\Theta(K)$ bins and a constant number of iterations, the computational complexity of sublinear algorithm is $\Theta(K \log^3(n))$.

VI. SIMULATION RESULTS

In this section, we show the simulation results to support our theory. The simulations are conducted in Python. Since the sublinear scheme has much lower computational complexity than the almost-linear scheme, we only conduct simulations on the sublinear scheme here. We define the signal-to-noise

ratio (SNR):

$$\text{SNR} = 10 \log_{10} \frac{\sum_{j=0}^R \|\mathbf{y}_j - \mathbf{w}_j\|_2^2}{\sum_{j=0}^R \|\mathbf{w}_j\|_2^2},$$

and use Gaussian noise. Since the fraction of unrecovered balls p can be arbitrarily small, in the simulations, we simply define a successful recovery as the cases when all non-zero components are correctly found up to a global phase. In all the simulations, we set $P = 5 \log(n)$, $d = 15$, $M = 8K$, $L_m = 3$, $L_p = 6$, and $\varepsilon = 1$.

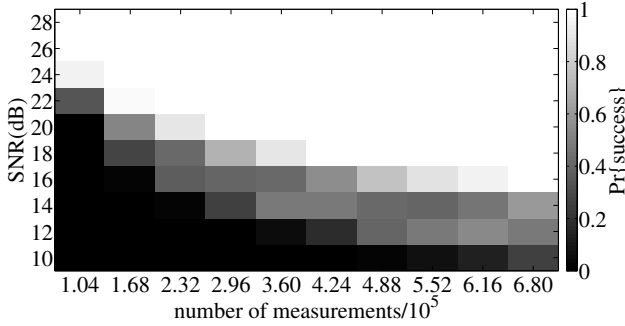


Fig. 2: Probability of successful recovery. We choose $n = 2^{20}$ and $K = 50$. Different values of Q and SNR are tested, and for each set of parameters, 1000 experiments are conducted.

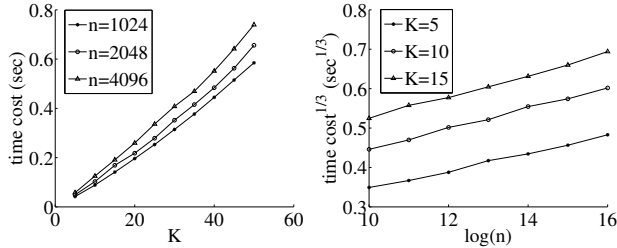


Fig. 3: Time cost. We choose $Q = 2 \log^2(n)$ and $\text{SNR} = 20\text{dB}$. Different values of n and K are tested, and for each set of parameters, 100 experiments are conducted and the average time cost is shown.

In Figure 2, we show the results of simulations on the probability of successful recovery as a function of the number of measurements and the SNR. Since the total number of measurements is dominated by Q . The sample complexity is mainly determined by Q . Therefore, we fixed P , i.e., the size of the test matrix, and tried different values of Q . From the results, we can see that the sublinear scheme can successfully recover the signal at relatively low SNR, such as 16dB, when $Q = 2 \log^2(n)$ and the number of measurements is 6.8×10^5 .

In Figure 3, we show the results of simulations on the time cost of the sublinear scheme⁷. It can be seen that the time cost of sublinear scheme is indeed low and linear in K and $\Theta(\log^3(n))$.

ACKNOWLEDGMENT

The authors would like to thank Yudong Chen and Xiao Li for helpful discussions.

⁷The simulations are conducted on a laptop with 2.8 GHz Intel Core i7 CPU and 16 GB memory.

REFERENCES

- [1] R. Pedarsani, K. Lee, and K. Ramchandran, "Phasecode: Fast and efficient compressive phase retrieval based on sparse-graph-codes," *arXiv preprint arXiv:1408.0034*, 2014.
- [2] R. Vershynin, "Introduction to the non-asymptotic analysis of random matrices," *arXiv preprint arXiv:1011.3027*, 2010.
- [3] E. J. Candes, T. Strohmer, and V. Voroninski, "Phaselift: Exact and stable signal recovery from magnitude measurements via convex programming," *Communications on Pure and Applied Mathematics*, vol. 66, no. 8, pp. 1241–1274, 2013.
- [4] B. Alexeev, A. S. Bandeira, M. Fickus, and D. G. Mixon, "Phase retrieval with polarization," *SIAM Journal on Imaging Sciences*, vol. 7, no. 1, pp. 35–66, 2014.
- [5] H. Ohlsson, A. Y. Yang, R. Dong, and S. S. Sastry, "Compressive phase retrieval from squared output measurements via semidefinite programming," *arXiv preprint arxiv.org/abs/1111.6323*, 2011.
- [6] O. Bunk, A. Diaz, F. Pfeiffer, C. David, B. Schmitt, D. K. Satapathy, and J. F. van der Veen, "Diffractive imaging for periodic samples: retrieving one-dimensional concentration profiles across microfluidic channels," *Acta Crystallographica Section A: Foundations of Crystallography*, vol. 63, no. 4, pp. 306–314, 2007.
- [7] E. G. Loewen and E. Popov, *Diffraction gratings and applications*. CRC Press, 1997.
- [8] M. Mirhosseini, O. S. Magaña-Loaiza, S. M. H. Rafsanjani, and R. W. Boyd, "Compressive direct measurement of the quantum wavefunction," *arXiv preprint arXiv:1404.2680*, 2014.
- [9] D. J. Love, R. W. Heath, W. Santipach, and M. L. Honig, "What is the value of limited feedback for mimo channels?" *Communications Magazine, IEEE*, vol. 42, no. 10, pp. 54–59, 2004.
- [10] J. C. Candy, "A use of limit cycle oscillations to obtain robust analog-to-digital converters," *Communications, IEEE Transactions on*, vol. 22, no. 3, pp. 298–305, 1974.
- [11] T. Richardson and R. Urbanke, *Modern coding theory*. Cambridge University Press, 2008.
- [12] X. Li, S. Pawar, and K. Ramchandran, "Sub-linear time support recovery for compressed sensing using sparse-graph codes," *arXiv preprint arXiv:1412.7646*, 2014.
- [13] S. Pawar and K. Ramchandran, "Computing a k-sparse n-length discrete fourier transform using at most 4k samples and $\mathcal{O}(k \log k)$ complexity," *arXiv preprint arXiv:1305.0870*, 2013.
- [14] I. Waldspurger, A. d'Aspremont, and S. Mallat, "Phase recovery, maxcut and complex semidefinite programming," *Mathematical Programming*, pp. 1–35, 2013.
- [15] X. Li and V. Voroninski, "Sparse signal recovery from quadratic measurements via convex programming," *arXiv preprints arXiv:1209.4785*, 2012.
- [16] K. Jaganathan, S. Oymak, and B. Hassibi, "Sparse phase retrieval: Convex algorithms and limitations," pp. 1022–1026, 2013.
- [17] —, "Phase retrieval for sparse signals using rank minimization," in *Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing*, 2012, pp. 3449–3452.
- [18] R. Gerchberg and W. Saxton, "Phase determination for image and diffraction plane pictures in the electron microscope," *Optik*, vol. 34, pp. 275–284, 1971.
- [19] P. Netrapalli, P. Jain, and S. Sanghavi, "Phase retrieval using alternating minimization," *arXiv preprints arXiv:1306.0160*, 2013.
- [20] E. Candes, X. Li, and M. Soltanolkotabi, "Phase retrieval via wirtinger flow: Theory and algorithms," *arXiv preprint arXiv:1407.1065*, 2014.
- [21] Y. Chen, X. Yi, and C. Caramanis, "A convex formulation for mixed regression with two components: Minimax optimal rates," in *Proceedings of The 27th Conference on Learning Theory*, 2014, pp. 560–604.
- [22] A. C. Gilbert, M. J. Strauss, J. A. Tropp, and R. Vershynin, "Algorithmic linear dimension reduction in the ℓ_1 norm for sparse vectors," *arXiv preprint cs/0608079*, 2006.
- [23] S. Pawar, "Pulse: Peeling-based ultra-low complexity algorithms for sparse signal estimation," Ph.D. dissertation, PhD Dissertation, 2013.
- [24] M. Rudelson and R. Vershynin, "Hanson-wright inequality and sub-gaussian concentration," *arXiv preprint arXiv:1306.2872*, 2013.

A. Notations

We introduce some useful notations for the proofs. Here, $\|\cdot\|_F$ denotes the Frobenius norm of a matrix, $\|\cdot\|$ denotes the operator norm of a matrix. For a sub-exponential random variable, $\|\cdot\|_{\psi_1}$ denotes the sub-exponential norm of it; for a sub-gaussian random variable, $\|\cdot\|_{\psi_2}$ denotes the sub-gaussian norm of it [2]. The notations c , c_i , C , and C_i represent absolute constants with positive value.

In our model, we also assume that the noise w_i satisfies $\mathbb{E}[w_i] = \mu$, $\mathbb{E}[w_i^2] = \sigma^2$, and $\|w_i\|_{\psi_1} = \nu$. Since the entries in \mathbf{A}_0 and \mathbf{F}_0 are bounded and thus sub-gaussian, we let $\eta = \|a_{ij}\|_{\psi_2}$ and $\eta_0 = \|f_{0,ij}\|_{\psi_2}$, where a_{ij} and $f_{0,ij}$ are entries of \mathbf{A}_0 and \mathbf{F}_0 .

B. Proof of Theorem 1

In order to prove Theorem 1, we need to prove Lemma 1 first. Here we restate Lemma 1 with more details.

Lemma 1. *There exists $\zeta > 0$, determined by η , ν , and σ , such that when $\phi > \mu/\zeta$, for any $t_0 \in (\mu, \zeta\phi)$,*

$$\mathbb{P}\left\{\frac{1}{P}\|\mathbf{w}\|_1 \geq t_0\right\} = \mathcal{O}(1/n^2), \quad (7)$$

and

$$\mathbb{P}\left\{\frac{1}{P}\left\|\mathbf{y} - \mathcal{A}(\hat{\mathbf{x}}\hat{\mathbf{x}}^H)\right\|_1 < t_0\right\} = \mathcal{O}(1/n^2), \quad (8)$$

when $\hat{\mathbf{x}} \approx \mathbf{x}$.

See the proof of Lemma 1 in Appendix C. Now we can analyze the failure probability of the almost-linear scheme. Since the bipartite graph is d -left regular, there are dn balls in all the bins. In the first iteration, we need to search all the balls. For each ball, we need to check $\Theta(1)$ possible magnitudes. Therefore, we need to do $\Theta(n)$ tests in the first iteration (d is also a constant). Similarly, in the later iterations, we need to do at most $\Theta(n)$ tests. Since it is proved in [1] that the number of iterations is a constant, we need to do $N_t = \Theta(n)$ tests. Lemma 1 tells us that, for any energy test, if the tests before it are all correct, and thus we have the correct colored balls, then, the error probability of this test is $\mathcal{O}(1/n^2)$. More specifically, let E_i be the event that there is an error in the i th test, while the tests $1, \dots, i-1$ are all correct. The event E_{test} that there is error in all the energy tests can be decomposed as

$$E_{\text{test}} = \bigcup_{i=1}^{N_t} E_i.$$

By union bound, we have

$$\mathbb{P}\{E_{\text{test}}\} \leq N_t \sum_{i=1}^{N_t} \mathbb{P}\{E_i\} = \Theta(n)\mathcal{O}(1/n^2) = \mathcal{O}(1/n).$$

Another possibility of making an error lies in the ball coloring algorithm itself. When there is no error in energy tests, this probability is $\mathcal{O}(1/K)$ as analyzed in the noiseless case.

Therefore the failure probability of the almost-linear scheme is

$$\begin{aligned} \mathbb{P}\{E_a\} &= \mathbb{P}\{E_a|E_{\text{test}}\}\mathbb{P}\{E_{\text{test}}\} + \mathbb{P}\{E_a|E_{\text{test}}^c\}\mathbb{P}\{E_{\text{test}}^c\} \\ &\leq \mathbb{P}\{E_{\text{test}}\} + \mathbb{P}\{E_a|E_{\text{test}}^c\} \\ &= \mathbb{P}\{E_{\text{test}}\} + \mathbb{P}\{E_{\text{coloring}}\} \\ &= \mathcal{O}(1/n) + \mathcal{O}(1/K) \\ &= \mathcal{O}(1/K) \end{aligned}$$

The sample and computational complexity are already analyzed in Section IV. Now we complete the proof.

C. Proof of Lemma 1

To prove equation (7), we simply use the Bernstein's inequality in [2]. For any $t > 0$,

$$\begin{aligned} &\mathbb{P}\left\{\frac{1}{P}\sum_{i=1}^P(|w_i| - \mathbb{E}[|w_i|]) > t\right\} \\ &\leq \exp\left[-C_1 P \min\left\{\frac{t^2}{\nu^2}, \frac{t}{\nu}\right\}\right]. \end{aligned}$$

Therefore, by choosing $t_0 > \mathbb{E}[|w_i|] = \mu$ and $t = t_0 - \mu$, we have

$$\mathbb{P}\left\{\frac{1}{P}\|\mathbf{w}\|_1 \geq t_0\right\} \leq \exp[-\delta_1 P].$$

Since δ_1 is a constant and $P = \Theta(\log(n))$, equation (7) is proved.

Now we prove equation (8). Before getting into the details of the proof, we give the definition of a new notation ϕ . For two vectors $\mathbf{p}, \mathbf{q} \in \mathbb{S}^n$, it is easy to see that $\mathbf{p} \approx \mathbf{q} \Leftrightarrow \mathbf{p}\mathbf{p}^H - \mathbf{q}\mathbf{q}^H \neq 0$. Since the entries of \mathbf{p} and \mathbf{q} lie in the quantized set \mathbb{S} , we know that there exists $\phi > 0$, such that $\|\mathbf{p}\mathbf{p}^H - \mathbf{q}\mathbf{q}^H\|_F > \phi$, when $\mathbf{p} \approx \mathbf{q}$, where ϕ depends on ε , L_m , and L_p . Then, we need the following lemma.

Lemma 3. *Given two vectors $\mathbf{x}_1, \mathbf{x}_2 \in \mathbb{C}^N$, let $\mathbf{X} = \mathbf{x}_1\mathbf{x}_1^H - \mathbf{x}_2\mathbf{x}_2^H \neq 0$. \mathcal{A} is the linear function defined in (3), and \mathbf{w} is the noise. Then, for any $s > 0$, we have,*

$$\begin{aligned} &\mathbb{P}\left\{\frac{1}{P}\|\mathcal{A}(\mathbf{X}) + \mathbf{w}\|_1 < (\zeta - s\eta_d)\|\mathbf{X}\|_F - 2s\nu\right\} \\ &\leq \exp[-C_0 P \min\{s^2, s\}], \end{aligned}$$

where $\zeta > 0$ depends on η , σ , and ν , $\eta_d > 0$ only depends on η .

See the proof of Lemma 3 in Appendix D. Note that $\mathbf{y} - \mathcal{A}(\hat{\mathbf{x}}\hat{\mathbf{x}}^H) = \mathcal{A}(\mathbf{x}\mathbf{x}^H - \hat{\mathbf{x}}\hat{\mathbf{x}}^H) + \mathbf{w}$, and that $\|\mathbf{x}\mathbf{x}^H - \hat{\mathbf{x}}\hat{\mathbf{x}}^H\|_F > \phi$. Now using Lemma 3, conditioning on \mathbf{h} , we have for any $s > 0$,

$$\begin{aligned} &\mathbb{P}\left\{\frac{1}{P}\left\|\mathbf{y} - \mathcal{A}(\hat{\mathbf{x}}\hat{\mathbf{x}}^H)\right\|_1 < \zeta\phi - (\eta_d\phi + 2\nu)s \mid \mathbf{h}\right\} \\ &\leq \exp[-C_0 P \min\{s^2, s\}]. \end{aligned} \quad (9)$$

Since (9) holds for any \mathbf{h} , we know that it also holds without conditioning on \mathbf{h} . If $\zeta\phi > t_0$, we can choose $s = \frac{\zeta\phi - t_0}{\eta_d\phi + 2\nu}$, then

$$\mathbb{P}\left\{\frac{1}{P}\left\|\mathbf{y} - \mathcal{A}(\hat{\mathbf{x}}\hat{\mathbf{x}}^H)\right\|_1 < t_0\right\} \leq \exp[-\delta_2 P].$$

Since δ_2 is a constant and $P = \Theta(\log(n))$, equation (8) is proved.

Then, we can conclude that there exists ζ , determined by the statistics of noise, such that when $\phi > \mu/\zeta$, for any threshold $t_0 \in (\mu, \zeta\phi)$, the energy test fails with probability $\mathcal{O}(1/n^2)$. This completes the proof of Lemma 1.

D. Proof of Lemma 3

The proof of Lemma 3 is based on similar ideas appeared in [21]. Let $\boldsymbol{\xi} = \mathcal{A}(\mathbf{X}) + \mathbf{w}$, then $\xi_i = \mathbf{a}_i^H \mathbf{X} \mathbf{a}_i + w_i$. According to the definition of the matrix \mathbf{A} , we know that the Hanson-Wright inequality for complex random variables in Appendix G holds for $\mathbf{a}_i^H \mathbf{X} \mathbf{a}_i$ and we have for every $t > 0$,

$$\begin{aligned} & \mathbb{P} \left\{ \left| \mathbf{a}_i^H \mathbf{X} \mathbf{a}_i - \mathbb{E} [\mathbf{a}_i^H \mathbf{X} \mathbf{a}_i] \right| > t \right\} \\ & \leq 6 \exp \left[-c \min \left\{ \frac{t^2}{\eta^4 \|\mathbf{X}\|_F^2}, \frac{t}{\eta^2 \|\mathbf{X}\|} \right\} \right] \\ & \leq 6 \exp \left[-c \min \left\{ \frac{t}{\eta^2 \|\mathbf{X}\|_F} - \frac{1}{4}, \frac{t}{\eta^2 \|\mathbf{X}\|_F} \right\} \right] \\ & \leq 6 \exp \left[c \left(\frac{1}{4} - \frac{t}{\eta^2 \|\mathbf{X}\|_F} \right) \right], \end{aligned}$$

where the second inequality is due to the fact that $(a-1/2)^2 \geq 0$ and $\|\mathbf{X}\| \leq \|\mathbf{X}\|_F$. From [2], we know that $\mathbf{a}_i^H \mathbf{X} \mathbf{a}_i - \mathbb{E} [\mathbf{a}_i^H \mathbf{X} \mathbf{a}_i]$ is a sub-exponential random variable with sub-exponential norm

$$\|\mathbf{a}_i^H \mathbf{X} \mathbf{a}_i - \mathbb{E} [\mathbf{a}_i^H \mathbf{X} \mathbf{a}_i]\|_{\psi_1} \leq C\eta^2 \|\mathbf{X}\|_F. \quad (10)$$

On the other hand,

$$\|\mathbb{E} [\mathbf{a}_i^H \mathbf{X} \mathbf{a}_i]\| = \frac{1}{2} \left| \|\mathbf{x}_1\|_2^2 - \|\mathbf{x}_2\|_2^2 \right| \leq \frac{1}{2} \|\mathbf{X}\|_F.$$

Thus, it gives us

$$\begin{aligned} \|\xi_i\|_{\psi_1} &= \|\mathbf{a}_i^H \mathbf{X} \mathbf{a}_i - \mathbb{E} [\mathbf{a}_i^H \mathbf{X} \mathbf{a}_i] + \mathbb{E} [\mathbf{a}_i^H \mathbf{X} \mathbf{a}_i] + w_i\|_{\psi_1} \\ &\leq \|\mathbf{a}_i^H \mathbf{X} \mathbf{a}_i - \mathbb{E} [\mathbf{a}_i^H \mathbf{X} \mathbf{a}_i]\|_{\psi_1} + |\mathbb{E} [\mathbf{a}_i^H \mathbf{X} \mathbf{a}_i]| + \nu \\ &\leq (C\eta^2 + 1/2) \|\mathbf{X}\|_F + \nu, \end{aligned} \quad (11)$$

where the first inequality is due to the fact that $\mathbb{E} [\mathbf{a}_i^H \mathbf{X} \mathbf{a}_i]$ is a constant, $\|\mathbb{E} [\mathbf{a}_i^H \mathbf{X} \mathbf{a}_i]\|_{\psi_1} = |\mathbb{E} [\mathbf{a}_i^H \mathbf{X} \mathbf{a}_i]|$, and that $\|w_i\|_{\psi_1} = \nu$. Then

$$\|\xi_i - \mathbb{E} [\xi_i]\|_{\psi_1} \leq 2 \|\xi_i\|_{\psi_1} \leq \eta_d \|\mathbf{X}\|_F + 2\nu, \quad (12)$$

where $\eta_d = 2C\eta^2 + 1$. Now according to Bernstein's inequality in [2], we have for every $t > 0$,

$$\begin{aligned} & \mathbb{P} \left\{ \frac{1}{P} \sum_{i=1}^P (|\xi_i| - \mathbb{E} [|\xi_i|]) < -t \right\} \\ & \leq \exp \left[-C_0 P \min \left\{ \frac{t^2}{(\eta_d \|\mathbf{X}\|_F + 2\nu)^2}, \frac{t}{\eta_d \|\mathbf{X}\|_F + 2\nu} \right\} \right]. \end{aligned}$$

Let $t = s(\eta_d \|\mathbf{X}\|_F + 2\nu)$. For any $s > 0$,

$$\begin{aligned} & \mathbb{P} \left\{ \frac{1}{P} \sum_{i=1}^P (|\xi_i| - \mathbb{E} [|\xi_i|]) < -s(\eta_d \|\mathbf{X}\|_F + 2\nu) \right\} \\ & \leq \exp [-C_0 P \min \{s^2, s\}]. \end{aligned} \quad (13)$$

By Cauchy-Schwartz inequality, for any $i \in [P]$, we have

$$(\mathbb{E} [\xi_i^2])^2 \leq \mathbb{E} [|\xi_i|] \mathbb{E} [|\xi_i|^3] \leq \mathbb{E} [|\xi_i|] \sqrt{\mathbb{E} [\xi_i^2] \mathbb{E} [\xi_i^4]},$$

which implies

$$\mathbb{E} [|\xi_i|] \geq \sqrt{\frac{(\mathbb{E} [\xi_i^2])^3}{\mathbb{E} [\xi_i^4]}}. \quad (14)$$

According to the definition of sub-exponential norm and the fact that $\eta_d > 1$, we have

$$\begin{aligned} \mathbb{E} [\xi_i^4] &\leq (4 \|\xi_i\|_{\psi_1})^4 \leq (2\eta_d \|\mathbf{X}\|_F + 4\nu)^4 \\ &\leq (8\eta_d^2 \|\mathbf{X}\|_F^2 + 32\nu^2)^2. \end{aligned} \quad (15)$$

On the other hand, we have

$$\begin{aligned} \mathbb{E} [\xi_i^2] &= \mathbb{E} [(\mathbf{a}_i^H \mathbf{X} \mathbf{a}_i)^2] + \mathbb{E} [w_i^2] \\ &= \mathbb{E} [(\mathbf{a}_i^H \mathbf{X} \mathbf{a}_i) \text{tr} (\mathbf{a}_i \mathbf{a}_i^H \mathbf{X})] + \sigma^2 \\ &= \mathbb{E} [\text{tr} ((\mathbf{a}_i^H \mathbf{X} \mathbf{a}_i) \mathbf{a}_i \mathbf{a}_i^H \mathbf{X})] + \sigma^2 \\ &= \text{tr} (\mathbb{E} [(\mathbf{a}_i^H \mathbf{X} \mathbf{a}_i) \mathbf{a}_i \mathbf{a}_i^H] \mathbf{X}) + \sigma^2 \\ &= \frac{1}{4} \text{tr} ((\mathbf{X} + \text{tr}(\mathbf{X}) \mathbf{I}) \mathbf{X}) + \sigma^2 \\ &\geq \frac{1}{4} \|\mathbf{X}\|_F^2 + \sigma^2. \end{aligned} \quad (16)$$

Here we give an explanation of equation (16). Let $\mathbf{Y} = (\mathbf{a}_i^H \mathbf{X} \mathbf{a}_i) \mathbf{a}_i \mathbf{a}_i^H$. Then,

$$\begin{aligned} & \mathbb{E} [Y_{jk}] \\ &= \mathbb{E} \left[\sum_{1 \leq g, h \leq n} a_{ig}^* X_{gh} a_{ih} a_{ij} a_{ik}^* \right] \\ &= \sum_{g=1}^n \mathbb{E} [a_{ig}^* X_{gg} a_{ig} a_{ij} a_{ik}^*] + \sum_{g \neq h} \mathbb{E} [a_{ig}^* X_{gh} a_{ih} a_{ij} a_{ik}^*]. \end{aligned}$$

If $j = k$, we have

$$\begin{aligned} \mathbb{E} [Y_{jj}] &= \sum_{g=1}^n X_{gg} \mathbb{E} [|a_{ig}|^2 |a_{ij}|^2] + \sum_{g \neq h} X_{gh} \mathbb{E} [a_{ig}^* a_{ih} |a_{ij}|^2] \\ &= \frac{1}{4} (\text{tr}(\mathbf{X}) + X_{jj}). \end{aligned}$$

If $j \neq k$, we have

$$\begin{aligned} \mathbb{E} [Y_{jk}] &= \sum_{g=1}^n X_{gg} \mathbb{E} [|a_{ig}|^2 a_{ij} a_{ik}^*] + \sum_{g \neq h} X_{gh} \mathbb{E} [a_{ig}^* a_{ih} a_{ij} a_{ik}^*] \\ &= X_{jk} \mathbb{E} [|a_{ij}|^2 |a_{ik}|^2] \\ &= \frac{1}{4} X_{jk}. \end{aligned}$$

Therefore, $\mathbb{E} [\mathbf{Y}] = \frac{1}{4} (\mathbf{X} + \text{tr}(\mathbf{X}) \mathbf{I})$.

By combining (14), (15), and (17), we have

$$\begin{aligned} \mathbb{E} [|\xi_i|] &\geq \sqrt{\left(\frac{\frac{1}{4} \|\mathbf{X}\|_F^2 + \sigma^2}{8\eta_d^2 \|\mathbf{X}\|_F^2 + 32\nu^2} \right)^2 \left(\frac{1}{4} \|\mathbf{X}\|_F^2 + \sigma^2 \right)} \\ &\geq \zeta \|\mathbf{X}\|_F, \end{aligned}$$

where $\zeta = \frac{1}{2} \min \left\{ \frac{1}{32\eta_d^2}, \frac{\sigma^2}{32\nu^2} \right\}$ is a constant determined by the distribution of a_{ij} and w_i . Then according to (13), we have

$$\begin{aligned} & \mathbb{P} \left\{ \frac{1}{P} \sum_{i=1}^P |\xi_i| < \zeta \|\mathbf{X}\|_F - s(\eta_d \|\mathbf{X}\|_F + 2\nu) \right\} \\ & \leq \exp \left[-C_0 P \min \{s^2, s\} \right], \end{aligned}$$

which completes the proof.

E. Proof of Theorem 2

To prove Theorem 2, we need to use Lemma 2. Here, we restate Lemma 2, providing more details.

Lemma 2. *If $T_s = 1$, $\text{supp}(\mathbf{x}_s) = \{l_s\}$, and threshold $t_1 \in (0, \varepsilon^2/2)$, then for any $j \in [R]$,*

$$\mathbb{P} \left\{ \tilde{b}_j \neq b_{jl_s} \right\} = \mathcal{O}(1/K^3).$$

See the proof of Lemma 2 in Appendix F. Then, by union bound, we know that $\mathbb{P}\{\tilde{\mathbf{b}} \neq \mathbf{B}_{l_s}\} = \mathcal{O}(R/K^3) \leq \mathcal{O}(1/K^2)$, since $K = \beta n^\delta$. Now we can see that we can reliably find l_s from the measurements with probability $1 - \mathcal{O}(1/K^2)$. For a bin with $T_s = 1$, the probabilities of error in index tests and energy test are $\mathcal{O}(1/K^2)$ and $\mathcal{O}(1/n^2)$, respectively. Therefore, the error probability of the tests for this bin is $\mathcal{O}(1/K^2)$. For a bin with $T_s > 1$, only the energy test should be considered and its error probability is $\mathcal{O}(1/n^2)$. Then, we know the probability of making mistakes in the index and energy tests is $\mathcal{O}(1/K^2)$. Since there are $\Theta(K)$ bins and a constant number of iterations, using the same decomposition method as in the proof of Theorem 1, we know that the error probability of all the tests is $\mathcal{O}(1/K)$. Similar to the almost-linear scheme, considering the $\mathcal{O}(1/K)$ probability of incomplete recovery in the ball coloring algorithm when there is no error in the index and energy tests, the failure probability of sublinear scheme is $\mathbb{P}\{E_s\} = \mathcal{O}(1/K)$. Since the sample and computational complexity are already analyzed in Section V, the proof of Theorem 2 is now complete.

F. Proof of Lemma 2

First, we define an event E_h such that there are more than $C_3 \log K$ active balls in a bin. As mentioned in [23], we have $\mathbb{P}\{E_h\} = \mathcal{O}(1/K^3)$. Now we condition on the coding pattern \mathbf{h} such that E_h^c happens, and thus $|\text{supp}(\mathbf{x})| = T \leq C_3 \log K$. Similar to the almost-linear algorithm, we define $R+1$ linear mappings, $\mathcal{A}_0, \mathcal{A}_1, \dots, \mathcal{A}_R$, where

$$\mathcal{A}_0 : \mathbf{X} \mapsto \{\mathbf{a}_i^H \mathbf{X} \mathbf{a}_i\}_{i \in [P]},$$

$$\mathcal{A}_j : \mathbf{X} \mapsto \{\mathbf{f}_{j,i}^H \mathbf{X} \mathbf{f}_{j,i}\}_{i \in [Q]}, \text{ for } j \in [R].$$

Then, We have $\mathbf{y}_j = \mathcal{A}_j(\mathbf{x}\mathbf{x}^H) + \mathbf{w}_j$, $j \in \{0\} \cup [R]$.

Define the matrix $\tilde{\mathbf{X}} = \{\tilde{X}_{ij}\}_{N \times N} := \mathbf{x}\mathbf{x}^H - \tilde{\mathbf{x}}_c \tilde{\mathbf{x}}_c^H = \mathbf{x}\mathbf{x}^H - \mathbf{x}_c \mathbf{x}_c^H$. Then $\tilde{\mathbf{y}}_j = \mathcal{A}_j(\tilde{\mathbf{X}}) + \mathbf{w}_j$. There is $\tilde{y}_{j,i} = \mathbf{f}_{j,i}^H \tilde{\mathbf{X}} \mathbf{f}_{j,i} + w_{j,i}$. Let $f_{j,i,m}$ be the m th element of $\mathbf{f}_{j,i}$. Since for a fixed j , $f_{j,i,m}$'s are independent, using the similar argument in Appendix D, we know that

$$\left\| \mathbf{f}_{j,i}^H \tilde{\mathbf{X}} \mathbf{f}_{j,i} - \mathbb{E} \left[\mathbf{f}_{j,i}^H \tilde{\mathbf{X}} \mathbf{f}_{j,i} \right] \right\|_{\psi_1} \leq C_2 \eta_0^2 \left\| \tilde{\mathbf{X}} \right\|_F.$$

Then we have $\|\tilde{y}_{j,i} - \mathbb{E}[\tilde{y}_{j,i}]\|_{\psi_1} \leq C_2 \eta_0^2 \|\tilde{\mathbf{X}}\|_F + \nu$. Since there are $2T-1$ nonzero entries in $\tilde{\mathbf{X}}$, we have $\|\tilde{\mathbf{X}}\|_F \leq \sqrt{2T-1} L_m \varepsilon$. We also have $T \leq C_3 \log K$, therefore we have $\|\tilde{y}_{j,i} - \mathbb{E}[\tilde{y}_{j,i}]\|_{\psi_1} \leq C_4 \eta_0^2 L_m \varepsilon \sqrt{\log K} + \nu \leq \zeta_0 \sqrt{\log K}$, where ζ_0 is determined by η_0, L_m, ε , and ν .

On the other hand, since $T_s = 1$ and $\text{supp}(\mathbf{x}_s) = \{l_s\}$, $\tilde{\mathbf{X}}$ only has one nonzero element on the diagonal, i.e., $\tilde{X}_{l_s l_s} = |x_{l_s}|^2$. We have $\mathbb{E}[\tilde{y}_{j,i}] = \mathbb{E}[|f_{j,i,l_s}|^2] |x_{l_s}|^2 = b_{jl_s} |x_{l_s}|^2$. According to Bernstein's inequality, for every $t \geq 0$, we have

$$\begin{aligned} & \mathbb{P} \left\{ \left| \frac{1}{Q} \sum_{i=1}^Q (\tilde{y}_{j,i} - b_{jl_s} |x_{l_s}|^2) \right| > t \mid \mathbf{h} \right\} \\ & \leq 2 \exp \left[-C_5 Q \min \left\{ \frac{t^2}{\zeta_0^2 \log K}, \frac{t}{\zeta_0 \sqrt{\log K}} \right\} \right] \\ & \leq 2 \exp \left[-\frac{C_5}{\zeta_0^2} \sqrt{Q} \min \{t^2, t\} \right], \end{aligned}$$

where the last inequality comes from the fact that $Q = \Theta(\log^2 N)$. Now choose $t_1 = t < \varepsilon^2/2$. When $b_{jl_s} = 0$, we know that

$$\begin{aligned} & \mathbb{P} \left\{ \left| \frac{1}{Q} \sum_{i=1}^Q \tilde{y}_{j,i} \right| > t_1 \mid \mathbf{h} \right\} \\ & \leq 2 \exp \left[-\frac{C_5}{\zeta_0^2} \sqrt{Q} \min \{t_1^2, t_1\} \right], \end{aligned} \quad (18)$$

and when $b_{jl_s} = 1$, we have

$$\begin{aligned} & \mathbb{P} \left\{ \left| \frac{1}{Q} \sum_{i=1}^Q \tilde{y}_{j,i} \right| < t_1 \mid \mathbf{h} \right\} \\ & \leq \mathbb{P} \left\{ \frac{1}{Q} \sum_{i=1}^Q \tilde{y}_{j,i} < t_1 \mid \mathbf{h} \right\} \\ & \leq \mathbb{P} \left\{ \frac{1}{Q} \sum_{i=1}^Q \tilde{y}_{j,i} < |x_{l_s}|^2 - t_1 \mid \mathbf{h} \right\} \\ & \leq \mathbb{P} \left\{ \left| \frac{1}{Q} \sum_{i=1}^Q \tilde{y}_{j,i} - |x_{l_s}|^2 \right| > t_1 \mid \mathbf{h} \right\} \\ & \leq 2 \exp \left[-\frac{C_5}{\zeta_0^2} \sqrt{Q} \min \{t_1^2, t_1\} \right], \end{aligned} \quad (19)$$

where the inequality (19) is due to the fact that $t_1 < \varepsilon^2/2$ and $|x_{l_s}|^2 \geq \varepsilon^2$. Define the error events $E_{\text{index}} = \{|\frac{1}{Q} \sum_{i=1}^Q \tilde{y}_{j,i}| > t_1\}$, when $b_{jl_s} = 0$, and $E_{\text{index}} = \{|\frac{1}{Q} \sum_{i=1}^Q \tilde{y}_{j,i}| < t_1\}$, when $b_{jl_s} = 1$. Then, since $Q = \Theta(\log^2(n))$ and inequalities (18) and (20) hold for any $\mathbf{h} \in E_h^c$, we have,

$$\mathbb{P}\{E_{\text{index}} | E_h^c\} = \mathcal{O}(1/K^3).$$

Now we know that

$$\begin{aligned} \mathbb{P}\{E_{\text{index}}\} &= \mathbb{P}\{E_{\text{index}} | E_h^c\} \mathbb{P}\{E_h^c\} + \mathbb{P}\{E_{\text{index}} | E_h\} \mathbb{P}\{E_h\} \\ &\leq \mathbb{P}\{E_{\text{index}} | E_h^c\} + \mathbb{P}\{E_h\} \\ &= \mathcal{O}(1/K^3) + \mathcal{O}(1/K^3) \\ &= \mathcal{O}(1/K^3), \end{aligned}$$

which completes the proof.

G. Hanson-Wright Inequality for Complex Random Variables

Theorem 3. Let $\boldsymbol{\gamma} = \{\gamma_i\}_{i \in [n]} \in \mathbb{C}^n$ be a random vector with independent entries γ_i , satisfying $\mathbb{E}[\gamma_i] = 0$, and $|\gamma_i|$ is sub-gaussian with $\|\gamma_i\|_{\psi_2} \leq \eta$ for all $i \in [n]$. Let $\mathbf{U} \in \mathbb{C}^{n \times n}$ be a Hermitian matrix. Then, for every $t \geq 0$,

$$\begin{aligned} & \mathbb{P} \left\{ \left| \boldsymbol{\gamma}^H \mathbf{U} \boldsymbol{\gamma} - \mathbb{E} [\boldsymbol{\gamma}^H \mathbf{U} \boldsymbol{\gamma}] \right| > t \right\} \\ & \leq 6 \exp \left[-c_0 \min \left\{ \frac{t^2}{\eta^4 \|\mathbf{U}\|_F^2}, \frac{t}{\eta^2 \|\mathbf{U}\|} \right\} \right]. \end{aligned}$$

Proof. Let $\boldsymbol{\alpha} = \{\alpha_i\}_{i \in [n]}$ and $\boldsymbol{\beta} = \{\beta_i\}_{i \in [n]}$ be the real and imaginary parts of $\boldsymbol{\gamma}$. Then, we know that α_i 's and β_i 's are sub-gaussian random variables with $\|\alpha_i\|_{\psi_2} \leq \eta$ and $\|\beta_i\|_{\psi_2} \leq \eta$ for all $i \in [n]$. Note that here, although γ_i 's are independent, the real and imaginary parts of γ_i are not necessarily independent for a certain i . In other words, for any i , α_i and β_i may not be independent.

Let \mathbf{V} and \mathbf{W} be the real and imaginary parts of \mathbf{U} . Since \mathbf{U} is a Hermitian matrix, we have $\mathbf{V} = \mathbf{V}^T$ and $\mathbf{W} = -\mathbf{W}^T$. We also know that $\boldsymbol{\gamma}^H \mathbf{U} \boldsymbol{\gamma}$ is a real number. Then, we have

$$\boldsymbol{\gamma}^H \mathbf{U} \boldsymbol{\gamma} = \boldsymbol{\alpha}^T \mathbf{V} \boldsymbol{\alpha} - 2\boldsymbol{\alpha}^T \mathbf{W} \boldsymbol{\beta} + \boldsymbol{\beta}^T \mathbf{V} \boldsymbol{\beta}.$$

Therefore, $\mathbb{P} \left\{ \left| \boldsymbol{\gamma}^H \mathbf{U} \boldsymbol{\gamma} - \mathbb{E} [\boldsymbol{\gamma}^H \mathbf{U} \boldsymbol{\gamma}] \right| > t \right\}$ is upper bounded by three terms,

$$\begin{aligned} & \mathbb{P} \left\{ \left| \boldsymbol{\gamma}^H \mathbf{U} \boldsymbol{\gamma} - \mathbb{E} [\boldsymbol{\gamma}^H \mathbf{U} \boldsymbol{\gamma}] \right| > t \right\} \\ & \leq \mathbb{P} \left\{ \left| \boldsymbol{\alpha}^T \mathbf{V} \boldsymbol{\alpha} - \mathbb{E} [\boldsymbol{\alpha}^T \mathbf{V} \boldsymbol{\alpha}] \right| > t/4 \right\} \\ & \quad + \mathbb{P} \left\{ \left| \boldsymbol{\alpha}^T \mathbf{W} \boldsymbol{\beta} - \mathbb{E} [\boldsymbol{\alpha}^T \mathbf{W} \boldsymbol{\beta}] \right| > t/4 \right\} \\ & \quad + \mathbb{P} \left\{ \left| \boldsymbol{\beta}^T \mathbf{V} \boldsymbol{\beta} - \mathbb{E} [\boldsymbol{\beta}^T \mathbf{V} \boldsymbol{\beta}] \right| > t/4 \right\}. \end{aligned} \quad (21)$$

Since α_i 's are independent and $\mathbb{E}[\alpha_i] = 0$, according to the Hanson-Wright inequality for real numbers [24], we have

$$\begin{aligned} & \mathbb{P} \left\{ \left| \boldsymbol{\alpha}^T \mathbf{V} \boldsymbol{\alpha} - \mathbb{E} [\boldsymbol{\alpha}^T \mathbf{V} \boldsymbol{\alpha}] \right| > t/4 \right\} \\ & \leq 2 \exp \left[-c_1 \min \left\{ \frac{t^2}{\eta^4 \|\mathbf{V}\|_F^2}, \frac{t}{\eta^2 \|\mathbf{V}\|} \right\} \right]. \end{aligned}$$

We also have $\|\mathbf{V}\|_F \leq \|\mathbf{U}\|_F$, $\|\mathbf{V}\| \leq \|\mathbf{U}\|$. Therefore,

$$\begin{aligned} & \mathbb{P} \left\{ \left| \boldsymbol{\alpha}^T \mathbf{V} \boldsymbol{\alpha} - \mathbb{E} [\boldsymbol{\alpha}^T \mathbf{V} \boldsymbol{\alpha}] \right| > t/4 \right\} \\ & \leq 2 \exp \left[-c_1 \min \left\{ \frac{t^2}{\eta^4 \|\mathbf{U}\|_F^2}, \frac{t}{\eta^2 \|\mathbf{U}\|} \right\} \right]. \end{aligned} \quad (22)$$

And similarly,

$$\begin{aligned} & \mathbb{P} \left\{ \left| \boldsymbol{\beta}^T \mathbf{V} \boldsymbol{\beta} - \mathbb{E} [\boldsymbol{\beta}^T \mathbf{V} \boldsymbol{\beta}] \right| > t/4 \right\} \\ & \leq 2 \exp \left[-c_2 \min \left\{ \frac{t^2}{\eta^4 \|\mathbf{U}\|_F^2}, \frac{t}{\eta^2 \|\mathbf{U}\|} \right\} \right]. \end{aligned} \quad (23)$$

Now consider the cross term. Let W_{ij} be the entries of \mathbf{W} . Since $\mathbf{W} = -\mathbf{W}^T$, $W_{ii} = 0$ for all $i \in [n]$. Then we have $\boldsymbol{\alpha}^T \mathbf{W} \boldsymbol{\beta} = \sum_{i \neq j} W_{ij} \alpha_i \beta_j$, and $\mathbb{E} [\boldsymbol{\alpha}^T \mathbf{W} \boldsymbol{\beta}] = 0$. Then, we

can bound $\mathbb{P} \left\{ \left| \boldsymbol{\alpha}^T \mathbf{W} \boldsymbol{\beta} \right| > t/4 \right\}$ in the same way as in [24]. We have

$$\begin{aligned} & \mathbb{P} \left\{ \left| \boldsymbol{\alpha}^T \mathbf{W} \boldsymbol{\beta} \right| > t/4 \right\} \\ & \leq 2 \exp \left[-c_3 \min \left\{ \frac{t^2}{\eta^4 \|\mathbf{U}\|_F^2}, \frac{t}{\eta^2 \|\mathbf{U}\|} \right\} \right]. \end{aligned} \quad (24)$$

By combining (22), (23), and (24), Theorem 3 is proved. \square