Sparse Signal Recovery from Quadratic Measurements via Convex Programming

Xiaodong Li* and Vladislav Voroninski†

September 2012

Abstract

In this paper we consider a system of quadratic equations $|⟨z_j, x⟩|^2 = b_j$, $j = 1, ..., m$, where $x \in \mathbb{R}^n$ is unknown while normal random vectors $z_j \in \mathbb{R}^n$ and quadratic measurements $b_j \in \mathbb{R}$ are known. The system is assumed to be underdetermined, i.e., $m < n$. We prove that if there exists a sparse solution $x$ i.e., at most $k$ components of $x$ are non-zero, then by solving a convex optimization program, we can solve for $x$ up to a multiplicative constant with high probability, provided that $k \leq O(\sqrt{m \log n})$. On the other hand, we prove that $k \leq O(\log n \sqrt{m})$ is necessary for a class of naive convex relaxations to be exact.

Keywords. $\ell_1$-minimization, Trace minimization, Shor’s SDP-relaxation, Compressed Sensing, PhaseLift, KKT Condition, Approximate Dual Certificate, Golfing Scheme, Random Matrices with IID Rows.

1 Introduction

1.1 Introduction and the main results

Convex optimization methods have recently been proven to be very successful in solving some classes of linear or quadratic algebraic equations. One classical example is compressed sensing (CS), where a system of underdetermined linear equations can be solved exactly by using an $\ell_1$-convex relaxation, provided that the unknown vector is sparse. A typical result is as follows:

Compressed Sensing Suppose $A \in \mathbb{R}^{m \times n}$ has IID $\mathcal{N}(0, 1)$ entries and $x_0 \in \mathbb{R}^n$ satisfies $\|x_0\|_0 = k$ (only $k$ components of $x$ are not zeros). If we have linear measurements $b = Ax_0$, then we can recover $x$ exactly with high probability by solving

$$\begin{align*}
\text{minimize} & \quad \|x\|_1 \\
\text{subject to} & \quad b = Ax
\end{align*}$$

(1.1)
provided \( k \leq O(m/\log(n/m)) \).

Another example is a recently proposed semidefinite programming framework for phase retrieval, called PhaseLift \([5]\), by which a signal can be exactly recovered up to a multiplicative constant from quadratic measurements. The SDP is a combination of trace minimization and Shor’s SDP-relaxation for quadratic constraints. We review the results in \([4, 5]\) below:

**PhaseLift** Fix a signal \( x \in \mathbb{R}^n \). Let \( z_i \in \mathbb{R}^n \) be IID standard normal random vectors, and suppose \( b_j, j = 1, \ldots, m \) are defined as follows:

\[
    b_j = |\langle z_j, x \rangle|^2, \quad j = 1, \ldots, m, \tag{1.2}
\]

If we assume \( m \geq C_0 n \) for some numerical constant \( C_0 \), then with high probability, \( xx^T \) is the unique solution to the following convex optimization problem:

\[
\begin{align*}
    &\text{minimize} & & \text{Tr}(X) \\
    &\text{subject to} & & z_j^T X z_j = b_j, \quad j = 1, \ldots, m, \\
    & & & X \succeq 0. \tag{1.3}
\end{align*}
\]

Notice that \( xx^T \) is feasible since \( xx^T \succeq 0 \) and

\[
    z_j^T (xx^T) z_j = |\langle z_j, x \rangle|^2 = b_j, \quad j = 1, \ldots, m.
\]

There is an inherent ambiguity to the solution of (1.2), since multiplying by a phase factor \((\pm 1 \text{ in the real case})\) does not change measurements. From now on, we only consider solutions modulo phase.

In this paper, we consider model (1.2) in the case that \( m \ll n \). In this regime, (1.2) does not yield injective measurements. In fact, each equation in (1.2) is the union of two linear equations by assigning different signs, so generally we have \( 2^m \) solutions. However, if we assume that the unknown vector \( x \) is \( k \)-sparse, then under some mild conditions on the number of measurements, system (1.2) becomes well-posed:

**Theorem 1.1** Let \( x \in \mathbb{R}^n \) be a \( k \)-sparse real signal, \( a_i \in \mathbb{R}^n, i = 1, \ldots, m_1 \) be generic real measurement vectors and let \( y \in \mathbb{C}^n \) be a \( k \)-sparse complex signal and \( b_i \in \mathbb{C}^n, i = 1 \ldots m_2 \) be generic complex measurement vectors. Then \( m_1 \geq 4k - 1, m_2 \geq 8k - 2 \) quadratic measurements \( \{ \langle a_i, x \rangle^2 \}_{i=1}^{m_1}, \{ | \langle b_i, y \rangle |^2 \}_{i=1}^{m_2} \) are sufficient to recover \( x \) and \( y \) modulo phase.

By generic we mean an open dense subset of the set of all \( m \)-element frames in \( \mathbb{R}^n \) or \( \mathbb{C}^n \).

**Proof** We only prove the complex case, since the real case is similar. Assume that there is a \( k \)-sparse \( y' \in \mathbb{C}^n \) such that \( |\langle b_i, y' \rangle|^2 = |\langle b_i, y \rangle|^2, \quad i = 1, \ldots, m_2 \geq 8k - 2 \). Let \( T \) be the union of the supports of \( y \) and \( y' \). Clearly \( |T| \leq 2k \). Then

\[
    |\langle b_i, y \rangle|^2 = |\langle b_i, y' \rangle|^2, \quad i = 1, \ldots, m_2,
\]
which is equivalent to
\[ |\langle b_j, y_T \rangle|^2 = |\langle b_j, y'_T \rangle|^2, \quad i = 1, \ldots, m, \]
where \( y_T \) means the restriction of \( y \) on the support \( T \). The genericity of \( b_i, \ i = 1, \ldots, m, \) implies the genericity of \( b_jT, \ i = 1, \ldots, m. \) Then since \( m \geq 4(2k) - 2 = 8k - 2 \) we have \( y_T = e^{i\psi}y'_T \) for some real number \( \psi \) by Theorem 3.1 in [1]. Therefore \( y = e^{i\psi}y'. \) \( \blacksquare \)

Injectivity of the measurements of course doesn’t imply that efficient recovery is possible. Yet, inspired by the success of convex relaxations in compressed sensing and phase retrieval, it is natural to leverage the sparsity assumption to try to efficiently recover signals from fewer than \( n \) intensity measurements. A convex formulation in this direction, which, to the best of our knowledge, was first proposed in [8] to solve (1.2), is the following program:

\[
\begin{align*}
\text{minimize} \quad & \|X\|_1 + \lambda \text{Tr}(X) \\
\text{subject to} \quad & z_j^T X z_j = b_j, \quad j = 1, \ldots, m, \\
& X \succeq 0. \\
\end{align*}
\]

(1.4)

The next theorem shows that when \( z_j \) are IID standard normal random vectors, the solution to \( (1.4) \) for an appropriate choice of \( \lambda \), is exactly \( xx^T \), provided that \( k \leq O(\sqrt{\frac{m}{\log n}}) \).

**Theorem 1.2** Fix a signal \( x \in \mathbb{R}^n \) with \( \|x\|_2 = 1 \) and \( \|x\|_0 = k \), i.e., only \( k \) components of \( x \) are non-zero. Let \( z_i \in \mathbb{R}^n \) be IID standard normal random vectors, and suppose \( b_j, \ j = 1, \ldots, m, \) are defined as in (1.2). Then the solution to the convex program (1.4) is exact with probability at least

\[ 1 - (2 \log n + 3)(4e^{-\frac{m}{3\log(n)+3}} + \frac{1}{n}) - (5 + 2n^2)e^{-\gamma n}, \]

provided \( \lambda > \sqrt{k}\|x\|_1 + 1 \), \( \lambda < \frac{n^2}{4} \) and \( m > C_0\lambda^2 \log n \). Here \( C_0 \) and \( \gamma \) are numerical constants.

Remark 1: By choosing \( \lambda = \sqrt{\frac{m}{3C_0 \log n}} \), we have exact recovery with probability at least

\[ 1 - (2 \log n + 3)(4e^{-\frac{m}{3\log(n)+3}} + \frac{1}{n}) - (5 + 2n^2)e^{-\gamma n}, \]

if the number of measurements obeys

\[ m \geq O(\frac{\|x\|_2^2k \log n}{k}). \]

Moreover, by choosing \( x \) to be a \( k \)-sparse vector with components \( x_i = \pm \frac{1}{\sqrt{k}} \), this reads

\[ m \geq O(k^2 \log n). \]

Remark 2: In [8], the authors operate under an assumption that the sampling operator satisfies a generalization of the Restricted Isometric Property and mutual coherence, while in Theorem 1.2 of our paper we assume the \( z_j \)'s are IID standard Normal vectors. In our setting the mutual coherence of the sampling operator defined in [8] will be on the order of \( O(1) \), since the diagonal entries of \( \langle z_j, z_j^T \rangle \) are always \( \chi^2 \) random variables. Applying the result in [8] we get \( k = O(1) \) in our setting, which is a much smaller range of sparsity than considered in the result of the above theorem.

The conclusion of Theorem 1.2 is far more restrictive than that of Theorem 1.1, so one may ponder whether 1.2 is optimal. The following result shows that indeed there is a substantial gap between solving 1.2 and 1.4.

**Theorem 1.3** Under the setting of Theorem 1.2, assuming \( 4 \leq k \leq m \leq \frac{n}{40 \log n} \), then there is an event \( E \) with probability at least

\[ 1 - \frac{m}{n} - me^{-0.09m + 0.09k + 0.79m}, \]

such that the following property
holds: If there exists a $\lambda \in \mathbb{R}$ such that $xx^T$ is a minimizer of (1.4), then we have

$$m \geq \min \left( \left( \frac{k}{4} - 1 \right)^2, \frac{\max(\|x\|_1^2 - k/2, 0)^2}{500 \log^2 n} \right).$$

Remark: Taking $x$ to be a k-sparse vector with components $x_i = \pm \frac{1}{\sqrt{k}}$, this reads $m \geq O(k^2 / \log^2 n)$.

This theorem obtains sharp theoretical results on the performance of (1.4) in the Gaussian quadratic measurement setting, which may be surprising since it implies that there is a substantial gap between the sufficient number of measurements for injectivity and the necessary number of measurements for recovery via a class of natural convex relaxations.

1.2 Definitions and notations

In this section we introduce some useful definitions and notations, which will be used in the proofs of Theorems 1.2 and 1.3. In this paper vectors and matrices are boldfaced while scalars are not.

For any positive integer $n_0$, denote $[n_0] = \{1, \ldots, n_0\}$. Let $G = \{i \in [n] : x_i \neq 0\}$ be the support of $x$ and $B$ be the complement $G = \{i \in [n] : x_i = 0\}$. Without loss of generality, we assume $G = \{1, \ldots, k\}$. Define the subspaces of symmetric matrices $\{X_{ij} = 0, i > k \text{ or } j > k, X = X^T\}$, $\Gamma = \{X|X_{ij} = 0, i \leq k \text{ or } j \leq k, X = X^T\}$ and $T = \{x x_0^T + x_0 x_0^T, x_0 \in \mathbb{R}^n\}$. In the space of symmetric matrices, we define the inner product $\langle X, Y \rangle = \text{Tr}(X Y)$. Then for any subspace of symmetric matrices $R$, we denote by $R^\perp$ its orthogonal complement under such an inner product.

For the given random vectors $z_j, j = 1, \ldots, m$, let $A : \mathbb{R}^{n \times n} \to \mathbb{R}^m$ be the linear operator $A(X) = \{\text{Tr}(z_i z_i^T X)\}_{i \in [m]}$ for any symmetric matrix $(X)$. Hence its adjoint is $A^*(y) = \sum_{i \in [m]} y_i z_i z_i^T$.

For a symmetric matrix $X$, we put $X_T$ for the orthogonal projection of $X$ onto $T$ and similar to $X_{T^\perp}$, $X_\Omega$, $X_{\Omega^\perp}$, $X_{\Omega^\perp T}$ and so on. For a vector $v \in \mathbb{R}^n$, we define $v_G = \langle v, e_1 \rangle e_1 + \ldots + \langle v, e_k \rangle e_k$ and $v_B = v - v_G$. Here $(e_1, \ldots, e_n)$ is the standard basis of $\mathbb{R}^n$.

Denote $\|y\|_p$ as the $\ell_p$ norm of a vector $y$, where $p$ could be 0, 1 or 2. Let $\|X\|$ and $\|X\|_F$ be the spectral and Frobenius norms of a matrix $X$, respectively. Moreover, let $\|X\|_\infty$ and $\|X\|_1$ be the maximum and the summation of absolute values of all entries of $X$ respectively, i.e., they represent the $\ell_\infty$ and $\ell_1$ norms of the vectorizations of matrices.

2 The proof of Theorem 1.2

In this section we will prove Theorem 1.2. First we will cite and prove some supporting lemmas. Then we prove that it suffices to construct an approximate dual certificate matrix to the primal convex optimization problem. Finally we use a modification of the golfing scheme to construct such an approximate dual certificate with high probability. Both the idea of the approximate dual certificate and the golfing scheme are originally due to David Gross’ work [7] in Matrix completion.
2.1 Preliminaries

In this section we establish some useful properties of $A$.

Lemma 2.1 (\[5\]) There is an event $E$ of probability at least $1 - 5e^{-\gamma_0 m}$ such that on $E$, any positive symmetric matrix obeys

\[
(1 - 1/8) \text{Tr}(X^\Omega) \leq m^{-1} \|A(X^\Omega)\|_1 \leq (1 + 1/8) \text{Tr}(X^\Omega),
\]

and any symmetric rank-2 matrix obeys

\[
m^{-1}\|A(X^\Omega)\|_1 \geq 0.94(1 - 1/8) \|X^\Omega\|.
\]

(2.1)

Proof By direct calculation, we have

\[
\frac{1}{m}\|A(X)\|_1 = \frac{1}{m}\sum_{j=1}^{m} |\langle X, z_jz_j^T \rangle| \leq \frac{1}{m}\sum_{j=1}^{m} \sum_{a,b} |X_{ab}z_ja z_jb| \leq \max_{a,b} \frac{1}{m}(\sum_{j=1}^{m} |z_ja z_jb|)\|X\|_1.
\]

Since $|z_ja z_jb|$, $j = 1..., m$ are IID sub-exponential variables with expectation 1 or $2\pi$ and have finite $\psi_1$-norm. By Proposition 5.16 of \[9\], we have

\[
\max_{a,b} \frac{1}{m}(\sum_{j=1}^{m} |z_ja z_jb|) \leq 9/8
\]

with probability at least $1 - 2n^2 e^{-\gamma_0 m}$. On this event we have $m^{-1}\|A(X)\|_1 \leq \frac{9}{8}\|X\|_1$. \(\blacksquare\)

2.2 Exact recovery by the existence of an approximate dual certificate.

In the classical theory of semidefinite programming, the existence of an exact dual certificate can be used to prove that a specific point is the solution to the primal problem. By using an idea in \[7\], in order to prove Theorem \[1.2\] it suffices to prove the existence of an approximate dual certificate.

Lemma 2.3 Denote $X_0 = \lambda xx^T + P_T(\text{sgn}(x) \text{sgn}(x)^T)$. Suppose there exists $Y = v_1 z_1 z_1^T + ... + v_m z_m z_m^T$ for some real numbers $v_1, ..., v_m$ satisfying \[
\|Y_{T:} - X_0\|_F \leq \frac{\|X_0\|_F}{6n^2}, \|Y_{T^+}\|_F \leq \frac{\|X_0\|_F}{6}
\]

and \[
\|Y_{\Omega^\perp}\|_\infty \leq \frac{C\sqrt{\log n}}{\sqrt{m}}\|X_0\|_F, \text{ with some numerical constant } C.
\]

Then assuming that $A$ satisfies properties (2.1), (2.2) and (2.3), we have that $xx^T$ is the unique solution to the convex program (1.4), provided that $\lambda > \sqrt{k}\|x\|_1 + 1$, $\lambda < \frac{n^2}{T}$ and $m > 64C^2\lambda^2\log n$. 

5
Proof Let $\hat{X}$ be the solution to the convex program \eqref{convex_program} and let $H = \hat{X} - xx^T$. Then by the feasibility condition of the convex program \eqref{convex_program}, we have
\[ A(H) = 0, \tag{2.4} \]
and
\[ xx^T + H \succeq 0. \tag{2.5} \]
By inequality \eqref{2.5}, we have
\[ H_T \cap \Omega \succeq 0, \quad H_B \succeq 0 \quad \text{and} \quad H_T \perp \succeq 0. \tag{2.6} \]
By equality \eqref{2.4}, we have
\[ A(H_T \cap \Omega) = A(H_T \perp \cup \Omega \perp). \]
Then by \eqref{2.1}, \eqref{2.2}, \eqref{2.3} and \eqref{2.6}, we have
\[ \|H_T \cap \Omega\|_1 \leq 10 \times (7/8)m \left(\frac{1}{0.94} \right) \|A(H_T \cap \Omega)\|_1 \leq \frac{1.3}{m} \|A(H_T \perp \cup \Omega \perp)\|_1 \leq \frac{1.3}{m} \left(\|A(H_T \perp \cap \Omega)\|_1 + \|A(H_\Omega \perp)\|_1\right) \leq 1.3 \times (9/8) (\text{Tr}(H_T \cap \Omega) + \|H_\Omega \perp\|_1). \tag{2.7} \]
Since rank$(H_T \cap \Omega) \leq 2$, we have
\[ \|H_T \cap \Omega\|_F \leq \sqrt{2}\|H_T \cap \Omega\| \leq 2.5 (\text{Tr}(H_T \cap \Omega) + \|H_\Omega \perp\|_1). \]
Now let’s see what inequalities about $H$ we can get from the objective function. Since both $\hat{X}$ and $xx^T$ are feasible and $\hat{X}$ is the minimizer, we have
\[ \|\hat{X}\|_1 + \lambda \text{Tr}(\hat{X}) \leq \|xx^T\|_1 + \lambda \text{Tr}(xx^T). \]
Also, since
\[ \|\hat{X}\|_1 + \lambda \text{Tr}(\hat{X}) = \|xx^T + H\|_1 + \lambda \text{Tr}(xx^T + H) \geq \|xx^T\|_1 + \langle \text{sgn}(x) \text{sgn}(x)^T, H \rangle + \|H_\Omega \perp\|_1 + \lambda \text{Tr}(xx^T) + \lambda \text{Tr}(H), \]
we have
\[ \langle \text{sgn}(x) \text{sgn}(x)^T, H \rangle + \|H_\Omega \perp\|_1 + \lambda \text{Tr}(H) \leq 0. \]
This implies
\[ \langle \mathcal{P}_T(\text{sgn}(x) \text{sgn}(x)^T) + \lambda xx^T, H_T \rangle + \langle \mathcal{P}_T(\text{sgn}(x) \text{sgn}(x)^T), H_T \perp \rangle + \|H_\Omega \perp\|_1 + \lambda \text{Tr}(H_T \perp) \leq 0. \]
It is easy to see that $\mathcal{P}_T(\text{sgn}(x) \text{sgn}(x)^T)$ is positive semidefinite and combining with \eqref{2.6}, we get
\[ \langle \mathcal{P}_T(\text{sgn}(x) \text{sgn}(x)^T), H_T \perp \rangle \geq 0, \]
which implies
\[ \langle X_0, H_T \cap \Omega \rangle + \|H_\Omega \perp\|_1 + \lambda \text{Tr}(H_T \perp) \leq 0. \]
By the assumed properties of $Y$, we know $Y = A^*(v)$, which implies
$$\langle H, Y \rangle = \langle A(H), v \rangle = 0.$$ 
Then we have
$$\langle H_{T \cap \Omega}, Y_{T \cap \Omega} - X_0 \rangle + \langle H_{T \cap \Omega}, X_0 \rangle + \langle H_{T^\perp \cap \Omega}, Y_{T^\perp \cap \Omega} \rangle + \langle H_{\Omega^\perp}, Y_{\Omega^\perp} \rangle = 0.$$ 

By the assumed properties of $Y$, we have
$$\frac{\|X_0\|_F}{6n^2} \|H_{T \cap \Omega}\|_F + \langle H_{T \cap \Omega}, X_0 \rangle + \frac{\|X_0\|_F}{5} \text{Tr}(H_{T^\perp \cap \Omega}) + \frac{C\sqrt{\log n}}{m} \|X_0\|_F \|H_{\Omega^\perp}\|_1 \geq 0.$$ 

By (2.8), we have
$$\frac{\|X_0\|_F}{6n^2} \|H_{T \cap \Omega}\|_F \geq (\lambda - \frac{\|X_0\|_F}{5}) \text{Tr}(H_{T^\perp \cap \Omega}) + (1 - \frac{C\sqrt{\log n}}{m} \|X_0\|_F) \|H_{\Omega^\perp}\|_1.$$ 

Since
$$\mathcal{P}_T(\text{sgn}(x) \text{sgn}(x)^T) = \|xx^T\|_1 (x \text{sgn}(x)^T + \text{sgn}(x)x^T) - \|xx^T\|_1,$$
we have
$$\|X_0\|_F = \|\lambda xx^T + \mathcal{P}_T(\text{sgn}(x) \text{sgn}(x)^T)\|_F \leq \lambda + \|x\|_1^2 + 2\sqrt{\lambda} \|x\|_1.$$ 
Then together with the assumptions of $\lambda > \sqrt{\lambda} \|x\|_1 + 1$, $\lambda < \frac{n^2}{1}$ and $m > 64C^2\lambda^2 \log n$, we have
$$\frac{\|X_0\|_F}{6n^2} \leq 3(\lambda - \frac{\|X_0\|_F}{5}) \text{ and } \frac{\|X_0\|_F}{6n^2} \leq 3(1 - \frac{C\sqrt{\log n}}{m} \|X_0\|_F),$$
by direct calculation. Therefore, by (2.9)
$$\|H_{T \cap \Omega}\|_F \geq 3 \left( \text{Tr}(H_{T^\perp \cap \Omega}) + \|H_{\Omega^\perp}\|_1 \right).$$
Equations (2.7) and (2.10) give $H_{T \cap \Omega} = 0$, and then by (2.10), we have $H_{T^\perp \cap \Omega} = 0$ and $H_{\Omega^\perp} = 0$. Hence $H = 0$, which implies $xx^T$ is the unique minimizer of the convex program (1.4).

### 2.3 Key lemma

The following lemma will be essential for the construction of a desirable dual certificate:

**Lemma 2.4** For any fixed $X \in T \cap \Omega$, we have $\text{rank}(X) \leq 2$. Consider an eigenvalue decomposition $X = \lambda_1 u_1 u_1^T + \lambda_2 u_2 u_2^T$, where $\|u_1\| = \|u_2\| = 1$, $u_1^T u_2 = 0$ and both $u_1$ and $u_2$ are supported on $G$. Define
$$Y = f(\lambda_1, \lambda_2, u_1, u_2) = \frac{1}{m(\beta_1 - \beta_2)} \sum_{j=1}^m (\lambda_1(|z_j^T u_1|^2 1_{|z_j^T u_1| \leq 3} - \beta_2) + \lambda_2(|z_j^T u_2|^2 1_{|z_j^T u_2| \leq 3} - \beta_2)) z_j z_j^T.$$
Here we define $\beta_2 = \mathbb{E} z^2 1_{\{|z| \leq 3\}} \approx 0.9707$, $\beta_4 = \mathbb{E} z^4 1_{\{|z| \leq 3\}} \approx 2.6728$, where assuming $z$ a standard normal variable. Then with probability at least $1 - 4e^{-\gamma m} - 1/n^3$,

$$\|Y_{T\cap\Omega} - X\|_F \leq \frac{1}{5}\|X\|_F, \quad \|Y_{T\perp\cap\Omega}\| \leq \frac{1}{10}\|X\|_F$$

and $\|Y_{\Omega\perp}\| \leq \frac{C_0\sqrt{\log n}}{\sqrt{m}}\|X\|_F$.

provided $m \geq C_1 k$. Here $\gamma$, $C_0$ and $C_1$ are numerical constants.

Before proving Lemma 2.4, we need to prove the following supporting lemma:

**Lemma 2.5** Suppose $z_j \in \mathbb{R}^n$, $j = 1, \ldots, m$ are IID $N(0, I_{n \times n})$ random vectors, and $u$ is any fixed vector with unit 2-norm, i.e., $\|u\|_2 = 1$. Then for any fixed $\epsilon > 0$, there exists a constant $\gamma(\epsilon)$ and $C_0(\epsilon)$ satisfying

$$\left\| \frac{1}{m} \sum_{j=1}^m (|z_j^T u|^2 1_{\{|z_j^T u| \leq 3\}}) z_j z_j^T - ((\beta_4 - \beta_2) uu^T + \beta_2 I) \right\| \leq \epsilon$$

with probability at least $1 - 2e^{-\gamma m}$ provided $m \geq C_0 n$.

**Proof** By rotational invariance, we can assume $u = e_1$. Define a matrix $D = \text{diag}(\frac{1}{\sqrt{\beta_4}}, \frac{1}{\sqrt{2}}, \ldots, \frac{1}{\sqrt{m}})$. Define $w_j = D|z_j| 1_{\{|z_j| \leq 3\}} z_j$. It is immediate to check that the $w_j$'s are IID copies of a zero-mean, isotropic and sub-Gaussian random vector $w$. Standard results about random matrices with sub-gaussian rows—e.g. Theorem 5.39 in [9]—give

$$\left\| \frac{1}{m} \sum_{j=1}^m w_j w_j^T - I \right\| \leq \epsilon/3,$$

which implies

$$\left\| \left( \frac{1}{m} \sum_{j=1}^m (|z_j^T u|^2 1_{\{|z_j^T u| \leq 3\}}) z_j z_j^T - ((\beta_4 - \beta_2) e_1 e_1^T + \beta_2 I) \right) \right\|$$

$$= \left\| D^{-1} \left( \frac{1}{m} \sum_{j=1}^m (w_j w_j^T - I) \right) D^{-1} \right\| \leq \|D^{-1}\| (\epsilon/3) \|D^{-1}\| \leq \epsilon.$$

with probability at least $1 - 2e^{-\gamma(\epsilon)m}$ provided that $m \geq C_0(\epsilon)n$, where $C_0$ is sufficiently large. 

**Proof** of Lemma 2.4. It suffices to prove

$$\|Y_{\Omega} - X\| \leq \frac{\sqrt{2}}{20}\|X\|_F, \quad \|Y_{\Omega}\|_\infty \leq \frac{C_0\sqrt{\log n}}{\sqrt{m}}\|X\|_F.$$

since

$$\|Y_{T\cap\Omega} - X\|_F \leq \sqrt{2}\|Y_{T\cap}\Omega} - X\| \leq 2\sqrt{2}\|Y_{\Omega} - X\| \leq \frac{1}{5}\|X\|_F,$$

and

$$\|Y_{T\perp\Omega}\| \leq \frac{1}{10}\|X\|_F.$$
1. \( \| Y_\Omega - X \| \leq \frac{\sqrt{2}}{20} \| X \|_F \). By Lemma 2.5, we have

\[
\left\| \frac{1}{m} \sum_{j=1}^{m} (|z_{jG}^T u_a| t_{1(|z_{jG}^T u_a| \leq 3}) z_{jG} z_{jG}^T - ((\beta_4 - \beta_2) u_a u_a^T + \beta_2 I)) \right\| \leq \epsilon, \quad a = 1, 2.
\]

with probability at least \( 1 - 2e^{-\gamma m} \) provided \( m \geq C_1 n \). Similarly, since \( \frac{1}{m} \sum_{j=1}^{m} z_{jG} z_{jG}^T \) is Wishart when restricted on \( \Omega \), standard results in random matrix theory—e.g. Corollary 5.35 in [9]—assert that

\[
\left\| \frac{1}{m} \sum_{j=1}^{m} z_{jG} z_{jG}^T - I \right\| \leq \epsilon
\]

with probability at least \( 1 - 2e^{-\gamma m} \) provided \( m \geq C_1 n \). Then Denote

\[
W_a = \frac{1}{m(\beta_4 - \beta_2)} \sum_{j=1}^{m} (|z_{jG}^T u_a| t_{1(|z_{jG}^T u_a| \leq 3}) - \beta_2) z_{jG} z_{jG}^T - u_a u_a^T, \quad a = 1, 2.
\]

We have with probability at least \( 1 - 4e^{\gamma m} \), \( \| W_a \| \leq \frac{1}{20} \) provided \( m \geq C_1 k \). This actually gives us the conclusion by noticing that

\[
Y_\Omega - X = \lambda_1 W_1 + \lambda_2 W_2.
\]

2. \( \| Y_\Omega \|_\infty \leq \frac{C_0 \sqrt{\log n}}{\sqrt{m}} \| X \|_F \).

For any fixed \( a, b \in [n], \ a > k \) or \( b > k \), we know \( Y_{ab} = e_a^T Y e_b \) is the arithmetic mean of \( m \) IID centered sub-exponential random variables, whose \( \psi_1 \)-norm is bounded by \( K(|\lambda_1| + |\lambda_2|) \) with a numerical constant \( K \). Then by Proposition 5.16 in [9], we have

\[
|Y_{ab}|_\infty \leq \frac{C_0 \sqrt{\log n}}{\sqrt{m}} \| X \|_F,
\]

with probability at least \( 1 - 1/n^5 \), which implies our claim.

2.4 Adaptation of the golfing scheme

In this section we will construct the dual certificate satisfying all the properties in Lemma 2.3 by using the golfing scheme.

**Proof** of Theorem 1.2 It suffices to construct \( Y \) satisfying all the properties in Lemma 2.3 with high probability. We divide the group of IID random vectors \( \{ z_1, ..., z_m \} \) into \( l := \lfloor 2 \log(n) \rfloor + 3 \) groups

\[
\{ z_1^{(1)}, ..., z_1^{(l)} \}, ..., \{ z_m^{(1)}, ..., z_m^{(l)} \}.
\]

This implies that \( m_1 + ... + m_l = m \). We use the same definition of \( X_0 \) in Lemma 2.3. For \( i=1, ..., l \), as in Lemma 2.4 we define the eigenvalue decomposition

\[
X_{i-1} = \lambda_{1i-1} u_{1i-1} u_{1i-1}^T + \lambda_{2i-1} u_{2i-1} u_{2i-1}^T.
\]
\[ Y_i = f(\lambda_{i-1}, \lambda_{2i-1}, \mathbf{u}_{1i-1}, \mathbf{u}_{2i-1}) \]

Moreover, we define \( \mathbf{X}_i = \mathbf{X}_{i-1} - P_{T \cap \Omega}(\mathbf{Y}_i) \), and \( \mathbf{Y} = \sum_{i=1}^l \mathbf{Y}_i \). By definition we have \( \mathbf{X}_i \)'s are in \( T \cap \Omega \), so \( \mathbf{Y}_i \) is well-defined. By Lemma (2.4), with probability at least \( 1 - l(4e^{-\gamma m} + 1/n^3) \), we have for \( i = 1, \ldots, l \)

\[
\| \mathbf{X}_i \|_F \leq \frac{1}{5} \| \mathbf{X}_{i-1} \|_F, \quad \| \mathbf{Y}_i \|_F \leq \frac{1}{10} \| \mathbf{X}_i \|_F, \quad \text{and} \quad \| \mathbf{Y}_{i\Omega}^+ \|_\infty \leq \frac{C_0 \sqrt{\log n}}{\sqrt{m}} \| \mathbf{X}_i \|_F,
\]

provided \( m_1 \geq C_1 k, \ldots, m_l \geq C_1 k \). Therefore, \( \mathbf{Y} = v_1 z_1^T + \ldots + v_m z_m z_m^T \) and

\[
\| \mathbf{Y}_T \|_F - \| \mathbf{X}_0 \|_F = \| \mathbf{X}_l \|_F \leq \left( \frac{1}{5} \right)^l \| \mathbf{X}_0 \|_F < \frac{\| \mathbf{X}_0 \|_F}{6n^2}, \quad \text{(by } l > 2 \log n + 2)\]

\[
\| \mathbf{Y}_{T \cap \Omega} \| \leq \sum_{i=1}^l \| \mathbf{Y}_{i \cap \Omega} \| \leq \sum_{i=1}^l \| \mathbf{X}_{i-1} \|_F \frac{10}{10} \leq \sum_{i=1}^l \| \mathbf{X}_0 \|_F \frac{1}{5}(l-1) \leq \frac{\| \mathbf{X}_0 \|_F}{8},
\]

and

\[
\| \mathbf{Y}_{\Omega}^+ \|_\infty \leq \sum_{i=1}^l \| \mathbf{Y}_{i\Omega}^+ \| \leq \sum_{i=1}^l \frac{C_0 \sqrt{\log n} \| \mathbf{X}_{i-1} \|_F}{\sqrt{m}} \leq \frac{5 C_0 \sqrt{\log n}}{4 \sqrt{m}} \| \mathbf{X}_0 \|_F.
\]

When \( m \geq (2 \log n + 3)C_1 k \), we can always make such a division of \( \{ z_1, \ldots, z_m \} \), so the proof is complete.

\section{The proof of Theorem 1.3}

We first prove a useful lemma:

\textbf{Lemma 3.1} Suppose \( \mathbf{a}_j, j = 1, \ldots, m_1 \) and \( \mathbf{b}_j, j = 1, \ldots, m_2 \) are IID \( \mathcal{N}(0, \mathbf{I}_{N \times N}) \) random vectors in \( \mathbb{R}^N \), where \( m_1 \geq 0, m_2 \geq 0 \) and \( m_1 + m_2 < N \). Then there is an event

\[ \tilde{E} = \tilde{E}(\mathbf{a}_1, \ldots, \mathbf{a}_{m_1}, \mathbf{b}_1, \ldots, \mathbf{b}_{m_2}) \]

\[ \text{with probability at least } 1 - m_2 e^{-0.00(N-m_1)}, \]

such that on \( \tilde{E} \) we have the following property:

Any \( \alpha_j < 0, j = 1, \ldots, m_1, \beta_j \geq 0, j = 1, \ldots, m_2, \lambda \in \mathbb{R}, S \leq 0 \) and \( \mathbf{L} \in \mathbb{R}^{n \times n} \) symmetric satisfying

\[
\sum_{j=1}^{m_1} \alpha_j \mathbf{a}_j \mathbf{a}_j^T + \sum_{j=1}^{m_2} \beta_j \mathbf{b}_j \mathbf{b}_j^T = \mathbf{L} + \mathbf{S} + \lambda \mathbf{I},
\]

must also satisfy

\[
\frac{N-m_1}{2} \left( \sum_{j=1}^{m_2} \beta_j \right) \leq \lambda m_2 + \sqrt{m_2} \| \mathbf{L} \|_F.
\]
Proof With probability 1 we have $a_1, ..., a_{m_1}, b_1, ..., b_{m_2}$ are linearly independent. Suppose 
\{v_1, ..., v_{m_1}, v_{m_1+1}, ..., v_{m_1+m_2}, ..., v_N\} is an orthonormal basis of $\mathbb{R}^N$ satisfying
\[
\text{span}(a_1, ..., a_{m_1}) = \text{span}(v_1, ..., v_{m_1}),
\]
and
\[
\text{span}(a_1, ..., a_{m_1}, b_1, ..., b_{m_2}) = \text{span}(v_1, ..., v_{m_1+m_2}).
\]
Then we can further assume $(v_1, ..., v_{m_1})$ only depend on $(a_1, ..., a_{m_1})$ and are independent of $(b_1, ..., b_{m_2})$. Then we have
\[
\left\langle \sum_{j=m_1+1}^{m_1+m_2} v_j v_j^T, L + S + \lambda I \right\rangle = \left\langle \sum_{j=m_1+1}^{m_1+m_2} v_j v_j^T, \sum_{j=1}^{m_1} \alpha_j a_j a_j^T + \sum_{j=1}^{m_2} \beta_j b_j b_j^T \right\rangle = \left\langle \sum_{j=m_1+1}^{m_1+m_2} v_j v_j^T, \sum_{j=1}^{m_1} \beta_j b_j b_j^T \right\rangle
\]
\[
= \left\langle \sum_{j=m_1+1}^{m_1+m_2} v_j v_j^T, \sum_{j=1}^{m_2} \beta_j b_j b_j^T \right\rangle = \left\langle I - \sum_{j=1}^{m_1} v_j v_j^T, \sum_{j=1}^{m_2} \beta_j b_j b_j^T \right\rangle
\]
\[
= \sum_{j=1}^{m_2} \beta_j \left( \|b_j\|^2 - \sum_{k=1}^{m_1} |v_k^T b_j|^2 \right).
\]
Since $b_j$ are IID $\mathcal{N}(0, I)$ random vectors, and are independent from the orthonormal vectors $v_1, ..., v_{m_1}$, we have
\[
\|b_j\|^2 - \sum_{k=1}^{m_1} |v_k^T b_j|^2 \sim \chi^2(N - m_1).
\]
By the Chernoff upper bound for the $\chi^2$ distribution, we have
\[
\mathbb{P} \left( \|b_j\|^2 - \sum_{k=1}^{m_1} |v_k^T b_j|^2 \geq \frac{N - m_1}{2} \right) \leq \left( \frac{1}{e^{1/2}} \right)^{(N - m_1)/2} \leq e^{-0.09(N-m_1)}.
\]
Then we have
\[
\left\langle \sum_{j=m_1+1}^{m_1+m_2} v_j v_j^T, L + S + \lambda I \right\rangle \geq \sum_{j=1}^{m_2} \beta_j \left( \frac{N - m_1}{2} \right)
\]
with probability $1 - m_2 e^{-0.09(N-m_1)}$.

On the other hand, we have
\[
\left\langle \sum_{j=m_1+1}^{m_1+m_2} v_j v_j^T, L + S + \lambda I \right\rangle \leq \left\langle \sum_{j=m_1+1}^{m_1+m_2} v_j v_j^T, L + \lambda I \right\rangle \leq \lambda m_2 + \|L\|_F \sqrt{m_2},
\]
which implies our claim.
The proof of Theorem 1.3:

We start by defining the event $E = E(z_1, ..., z_m)$. First, we define an event

$$ E_0 = \{ |\langle x, z_jG \rangle |^2 \leq 10 \log n, j = 1, ..., m \}. $$

By the assumption that $\|x\|_2 = 1$ and $z_jG \sim N(0, I_{k \times k})$, we have

$$ |\langle x, z_jG \rangle |^2 \sim \chi^2(1), $$

which implies that $\mathbb{P}(E_0) \geq 1 - \frac{m}{n^5}$. Next, for any partition of $\{1, ..., m\} = \{j_1, ..., j_{m_1}\} \cup \{k_1, ..., k_{m_2}\}$, where $j_1 < ... < j_{m_1}$, $k_1 < ... < k_{m_2}$, $m_1 \geq 0$, $m_2 \geq 0$ and $m_1 + m_2 = m$, define

$$ E_{\{j_1, ..., j_{m_1}\} \cup \{k_1, ..., k_{m_2}\}} = \tilde{E}(z_{j_1B}, ..., z_{j_{m_1}B}, z_{k_1B}, ..., z_{k_{m_2}B}). $$

Then by Lemma 3.1 we have

$$ \mathbb{P}(E_{\{j_1, ..., j_{m_1}\} \cup \{k_1, ..., k_{m_2}\}}) \geq 1 - m_2e^{-0.09(n-k-m)} \geq 1 - me^{-0.09(n-k-m)}. $$

Now we define the event $E$ by

$$ E = E_0 \cap \left( \bigcap \text{all partitions of } [m] \right). $$

Then

$$ \mathbb{P}(E) \geq 1 - \frac{m}{n^5} - 2^m me^{-0.09(n-k-m)} \geq 1 - \frac{m}{n^5} - me^{-0.09n+0.09k+0.79m}. $$

Hereafter all our discussions will be on the event $E$.

We now come back to derive the necessary condition for $xx^T$ to be an optimal point of (1.4). By section 5.9.2 of [2], the condition is

$$ 0 \in \partial (\|X\|_1 + \lambda \text{Tr}(X))|_{xx^T} + S + A^*(v), \quad S \preceq 0, \quad \langle S, xx^T \rangle = 0 $$

which, using the definition of the subgradient, is equivalent to

$$ 0 \in \text{sgn}(xx^T) + L_{\Omega^\perp} + \lambda I + S + A^*(v), \quad S \preceq 0, \quad \langle S, xx^T \rangle = 0, \quad \|L_{\Omega^\perp}\|_\infty \leq 1 $$

One can verify that $S \preceq 0$ and $\langle S, xx^T \rangle = 0$ is equivalent to $S \preceq 0$ and $P_T(S) = 0$. Thus the necessary condition for $xx^T$ to be a minimizer of this program is the existence of a dual certificate $Y$ with the following properties:

$$ Y = \sum_{j=1}^m c_j z_jz_j^T = \text{sgn}(x) \text{sgn}(x)^T + L_{\Omega^\perp} + \lambda I + S_T^\perp, \quad (3.1) $$

$$ \|L_{\Omega^\perp}\|_\infty \leq 1, \quad (3.2) $$

$$ S_T^\perp \preceq 0. \quad (3.3) $$
Project both sides of (3.1) on $\Gamma$, we have

$$Y_{\Gamma} = \sum_{j=1}^{m} c_j z_j B z_j^T = L_{\Gamma} + \lambda I_{\Gamma} + S_{\Gamma}. \quad (3.4)$$

Since $\Gamma \in T^\perp$, we have

$$S_{\Gamma} \preceq 0. \quad (3.5)$$

It is also obvious that $\|L_{\Gamma}\|_{\infty} \leq \|L_{\Omega^\perp}\|_{\infty} \leq 1$, which implies

$$\|L_{\Gamma}\|_F \leq (n-k)\|L_{\Gamma}\|_\infty \leq n-k, \text{ and } \text{Tr}(L_{\Gamma}) \leq n-k. \quad (3.6)$$

On the other hand, project both sides of (3.1) on $T$, we have

$$Y_T = \|x\|_1 (\text{sgn}(x)x^T + x \text{sgn}(x)^T) - \|x\|_1^2 xx^T + L_{T \cap \Omega^\perp} + \lambda xx^T,$$

and

$$Y_{T \cap \Omega} = \|x\|_1 (\text{sgn}(x)x^T + x \text{sgn}(x)^T) - \|x\|_1^2 xx^T + \lambda xx^T,$$

which implies

$$x^T Y_{T \cap \Omega} x = \sum_{j=1}^{m} c_j \left|\langle x, z_j G \rangle\right|^2 = \|x\|_1^2 + \lambda \|x\|_2^2 = \|x\|_1^2 + \lambda. \quad (3.7)$$

Case 1: $\lambda < -\frac{k}{2}$.

By the assumption $k \leq m \leq \frac{n}{40 \log n}$, we can assume the eigenvalue decomposition

$$\sum_{j=1}^{m} c_j z_j B z_j^T = \mu_1 u_1 u_1^T + ... + \mu_m u_m u_m^T + 0 \cdot u_{m+1} u_{m+1}^T + ... + 0 \cdot u_{n-k} u_{n-k}^T,$$

where $\{u_1, ..., u_{n-k}\}$ is an orthogonal basis of span$(e_{k+1}, ..., e_n)$. Then by (3.3), we have

$$u_j^T (L_{\Gamma} + \lambda I_{\Gamma} + S_{\Gamma}) u_j = u_j^T \left( \sum_{j=1}^{m} c_j z_j B z_j^T \right) u_j = 0,$$

for $j = m+1, ..., n-k$. By (3.3), we have

$$u_j^T L_{\Gamma} u_j \geq \frac{\|x\|_1^2}{2} = -u_j^T (\lambda I_{\Gamma} + S_{\Gamma}) u_j \geq -\lambda \geq \frac{k}{2} \quad (3.8)$$

Since $\{u_1, ..., u_{n-k}\}$ is an orthogonal basis of span$(e_{k+1}, ..., e_n)$, we have

$$\sum_{j=1}^{n-k} u_j^T L_{\Gamma} u_j = \left\langle L_{\Gamma}, \sum_{j=1}^{n-k} u_j u_j^T \right\rangle = \text{Tr}(L_{\Gamma}) \leq n-k.$$
By (3.8) and the assumption $4 \leq k \leq m \leq n$, we have
\[
\sum_{j=1}^{m} u_j^T L \Gamma u_j u_m \leq n - k - (n - k - m) \frac{k}{2} < 0. \tag{3.9}
\]
On the other hand
\[
\left| \sum_{j=1}^{m} u_j^T L \Gamma u_j u_m \right| = \left| \langle L \Gamma, \sum_{j=1}^{m} u_j u_j^T \rangle \right| \leq \|L \Gamma\|_F \sum_{j=1}^{m} u_j u_j^T \| \leq (n - k) \sqrt{m}. \tag{3.10}
\]
By (3.9) and (3.10), we have
\[
(n - k) \sqrt{m} \geq (n - k - m) \frac{k}{2} - (n - k) \text{ which implies } m \geq \left( \frac{k}{4} - 1 \right)^2.
\]

Case 2: $\lambda \geq -\frac{k}{2}$.
Let $I_+ = \{ k \in \{1, 2, \ldots, m \}; c_k \geq 0 \}$ and $I_- = \{ k \in \{1, 2, \ldots, m \}; c_k < 0 \}$. By (3.7) and the definition of $E \subset E_0$, we have
\[
\|x\|_2^2 + \lambda \leq 10 \log(n) \sum_{j \in I_+} c_j. \tag{3.11}
\]
By (3.7),
\[
Y = \sum_{j \in I_-} c_j z_j B z_j^T + \sum_{j \in I_+} c_j z_j B z_j^T = L \Gamma + \lambda I \Gamma + S \Gamma.
\]
By the definition of $E$ and Lemma 3.1, we have
\[
\frac{n - k - |I_-|}{2} \sum_{j \in I_+} c_j \leq \lambda |I_+| + \sqrt{|I_+|} \|L \Gamma\|_F. \tag{3.12}
\]
Notice that $\|L \Gamma\|_F \leq (n - k) \|L \Gamma\|_\infty \leq n - k$. By (3.11) and (3.12),
\[
\frac{(n - k - m)\|x\|_2^2}{20 \log n} + \lambda \left( \frac{n - k - m}{20 \log n} - m \right) \leq \sqrt{m}(n - k).
\]
By the assumption that $k \leq m \leq \frac{n}{40 \log n}$ and $\lambda \geq -\frac{k}{2}$, we have
\[
\frac{(n - k - m)(\|x\|_2^2 - k/2)}{20 \log n} \leq \sqrt{m}(n - k),
\]
which implies
\[
m \geq \max(\|x\|_2^2 - k/2, 0)^2 \quad \text{and} \quad \frac{500 \log^2 n}{500 \log^2 n}.
\]
Therefore, by putting Case 1 and Case 2 together, we have
\[
m \geq \min \left( \left( \frac{k}{4} - 1 \right)^2, \frac{\max(\|x\|_2^2 - k/2, 0)^2}{500 \log^2 n} \right).
\]
4 Discussion

We provide theoretical guarantees on the recovery of a sparse signal from quadratic Gaussian measurements via convex programming and show that our results are sharp for a class of recently proposed convex relaxations. For this model, unlike classical compressed sensing, compressive phase retrieval imposes a stricter limitation on the number of measurements needed for recovery via naive convex relaxation than is needed for well-posedness. This leads to a natural open question: can we narrow the gap by using other convex programs besides (1.4)?

Theorem 1.3 shows the limitations of (1.4) in the sense of exact recovery, since we only need to recover the support of the unknown vector to recover $x$ by using the PhaseLift algorithm [4, 5] to solve the resulting overdetermined system of quadratic equations. Mathematically, recovering the support is at least as easy as exact recovery. Can we do better than (1.4) by formulating the right support recovery problem? We leave these considerations for future research.

5 Acknowledgements

We are thankful for fruitful discussion with Emmanuel Candès and also Mahdi Soltanolkotabi, who generously provided us with the results of his numerical experiments on sparse recovery.

References

[1] R. Balan, P.G. Casazza, and D. Edidin. On signal reconstruction without noisy phase. *Appl. Comp. Harm. Anal.*, 20:345–356, 2006.

[2] S. Boyd and L. Vandenberghe. *Convex Optimization*. Cambridge University Press, 2004.

[3] E. Candès, J. Romberg, and T. Tao. Robust uncertainty principles: exact signal reconstruction from highly incomplete frequency information. *IEEE Trans. Inform. Theory*, 52(2):489–509, 2006.

[4] E. J. Candès and X. Li. Solving quadratic equations via phaselift when there are about as many equations as unknowns. *ArXiv e-prints*, August 2012.

[5] E. J. Candès, T. Strohmer, and V. Voroninski. Phaselift: Exact and stable signal recovery from magnitude measurements via convex programming. To appear in *Comm. Pure Appl. Math.*, 2011.

[6] D. Donoho. Compressed sensing. *IEEE Trans. Inform. Theory*, 52(4):1289 – 1306, 2006.

[7] D. Gross. Recovering low-rank matrices from few coefficients in any basis. *IEEE Trans. on Information Theory*, 57(3):1548–1566, 2011.

[8] H. Ohlsson, A. Y. Yang, R. Dong, and S. S. Sastry. Compressive phase retrieval from squared output measurements via semidefinite programming. *ArXiv e-prints*, Mar 2012.

[9] R. Vershynin. Introduction to the non-asymptotic analysis of random matrices. In Y. C. Eldar and G. Kutyniok, editors, *Compressed Sensing: Theory and Applications*, pages 210–268. Cambridge University Press, 2012.