Certifying the Restricted Isometry Property is Hard

Afonso S. Bandeira, Edgar Dobriban, Dustin G. Mixon, William F. Sawin

Abstract—This paper is concerned with an important matrix condition in compressed sensing known as the restricted isometry property (RIP). We demonstrate that testing whether a matrix satisfies RIP is NP-hard. As a consequence of our result, it is impossible to efficiently test for RIP provided $P \neq NP$.

I. INTRODUCTION

It is now well known that compressed sensing offers a method of taking few sensing measurements of high-dimensional sparse vectors, while at the same time enabling efficient and stable reconstruction [1]. In this field, the restricted isometry property is arguably the most popular condition to impose on the sensing matrix in order to acquire state-of-the-art reconstruction guarantees:

Definition 1. We say a matrix $\Phi$ satisfies the $(K, \delta)$-restricted isometry property (RIP) if

$$(1 - \delta)\|x\|^2 \leq \|\Phi x\|^2 \leq (1 + \delta)\|x\|^2$$

for every vector $x$ with at most $K$ nonzero entries.

To date, RIP-based reconstruction guarantees exist for Basis Pursuit [2], CoSaMP [3] and Iterative Hard Thresholding [4], and the ubiquitous utility of RIP has made the construction of RIP matrices a subject of active research [5]–[7]. Here, random matrices have found much more success than deterministic constructions [5], but this success is with high probability, meaning there is some (small) chance of failure in the construction. Furthermore, RIP is a statement about the conditioning of all $\binom{N}{K}$ submatrices of an $M \times N$ sensing matrix, and so it seems computationally intractable to check whether a given instance of a random matrix fails to satisfy RIP; it is widely conjectured that certifying RIP for an arbitrary matrix is NP-hard. In the present paper, we prove this conjecture.

Problem 2. Given a matrix $\Phi$, a positive integer $K$, and some $\delta \in (0, 1)$, does $\Phi$ satisfy the $(K, \delta)$-restricted isometry property?

In short, we show that any efficient method of solving Problem 2 can be called in an algorithm that efficiently solves the NP-complete subset sum problem. As a consequence of our result, there is no method by which one can efficiently test for RIP provided $P \neq NP$. This contrasts with previous work [8], in which the reported hardness results are based on less-established assumptions on the complexity of dense subgraph problems.

In the next section, we review the basic concepts we will use from computational complexity, and Section 3 contains our main result.

II. A BRIEF REVIEW OF COMPUTATIONAL COMPLEXITY

In complexity theory, problems are categorized into complexity classes according to the amount of resources required to solve them. For example, the complexity class $P$ contains all problems which can be solved in polynomial time, while problems in $NP$ may require as much as exponential time. Problems in $NP$ have the defining quality that solutions can be verified in polynomial time given a certificate for the answer. As an example, the graph isomorphism problem is in $NP$ because, given an isomorphism between graphs (a certificate), one can verify that the isomorphism is legitimate in polynomial time. Clearly, $P \subseteq NP$, since we can ignore the certificate and still solve the problem in polynomial time.

While problem categories provide one way to describe complexity, another important tool is the polynomial-time reduction, which allows one to show that a given problem is “more complex” than another. To be precise, a polynomial-time reduction from problem $A$ to problem $B$ is a polynomial-time algorithm that solves problem $A$ by exploiting an oracle which solves problem $B$; the reduction indicates that solving problem $A$ is no harder than solving problem $B$ (up to polynomial factors in time), and we say “$A$ reduces to $B$,” or $A \leq B$. Such reductions lead to some of the most popular definitions in complexity theory: We say a problem $B$ is called NP-hard if every problem $A$ in $NP$ reduces to $B$, and a problem is called NP-complete if it is both NP-hard and in $NP$. In plain speak, NP-hard problems are harder than every problem in $NP$, while NP-complete problems are the hardest of problems in $NP$.

Contrary to popular intuition, NP-hard problems are not merely problems that seem to require a lot of computation to solve. Of course, NP-hard problems have this quality, as an NP-hard problem can be solved in polynomial time only if $P = NP$; this is an open problem, but it is widely believed that $P \neq NP$ [9]. However, there are other problems which seem hard but are not known to be NP-hard (e.g., the graph isomorphism problem). As such, while testing for RIP in the general case seems to be computationally intensive, it is not
Theorem 4. Problem 3 is NP-hard.

Proof: Reducing from Problem 2, suppose we are given a matrix $A$ with integer entries. Letting $\Psi$ be the matrix with integer entries whose binary representations take the entries of $A$ as coefficients, we can ask the oracle question using coherence in conjunction with the Gershgorin circle theorem for small values of $K$. 

We are now ready to state the remainder of our reduction: 

The remainder of this proof will demonstrate (i) and (ii).

By the contrapositive. Indeed, $\text{Spark}(\Psi) = 2$ implies that $\Psi$ is not $K$-RIP, and so testing $\text{Spark}(\Psi) < 2$ is equivalent to testing $\Psi$ is not $K$-RIP.

In fact, since we plan to appeal to an RLP oracle, it is better to test $\Psi$ since the right-hand inequality of Definition 1 is already satisfied for every $\delta > 0$.

For some value of $\delta$ (which we will determine later), ask the oracle if $\Psi$ is $(K, \delta)$-RIP, then

\[ |\lambda| \leq \sqrt{M/N} \max_{\lambda \in \mathbb{R}^N, \|\lambda\|_1 \leq 1} \|\Psi \lambda\|_2 \leq \sqrt{M + 4}. \]

If $\Psi$ is not $(K, \delta)$-RIP, then $\lambda = 0$.

(i) $K \not\subseteq \Psi K$, implying the existence of a nonzero vector $x$ in the nullspace of $\Psi$ with cardinality $K$.

Problem 3 has a brief history in computational complexity. 

For (ii), let $x$ be a positive determinant, we must have $\lambda = 0$.

(ii) $K \not\subseteq \Psi K$, implying the existence of a nonzero vector $x$ in the nullspace of $\Psi$ with cardinality $K$.

Problem 3 has a brief history in computational complexity. 

We are now ready to state the remainder of our reduction: 

Next, Khachiyan [13] showed that Problem 3 is hard for $\text{co-NP}$. Next, Khachiyan [13] showed that Problem 3 is hard for $\text{co-NP}$.

We are now ready to state the remainder of our reduction: 

Next, Khachiyan [13] showed that Problem 3 is hard for $\text{co-NP}$.

We are now ready to state the remainder of our reduction: 

Next, Khachiyan [13] showed that Problem 3 is hard for $\text{co-NP}$.
[13] L. Khachiyan, On the complexity of approximating extremal determinants in matrices, J. Complexity 11 (1995) 128–153.

[14] A.M. Tillmann, M.E. Pfetsch, The computational complexity of the restricted isometry property, the nullspace property, and related concepts in compressed sensing, Available online: arXiv:1205.2081