Certifying the Restricted Isometry Property is Hard

Afonso S. Bandeira, Edgar Dobriban, Dustin G. Mixon, and 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.**

***Index Terms*—Compressed sensing, computational complexity, restricted isometry property.**

I. Introduction

It is now well known that compressed sensing offers a method of taking few measurements of high-dimensional sparse vectors, while at the same time enabling efficient and stable reconstruction [1]. In this field, the restricted isometry property (RIP) 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 Φ satisfies the (K,δ)-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 this paper, we prove this conjecture.

Problem 2: Given a matrix Φ, a positive integer K, and some $\delta \in (0,1)$, does Φ satisfy the (K,δ)-RIP?

Manuscript received November 18, 2012; revised February 17, 2013; accepted February 18, 2013. Date of publication March 12, 2013; date of current version May 15, 2013. A. S. Bandeira was supported by the National Science Foundation under Grant DMS-0914892. D. G. Mixon was supported by the A. B. Krongard Fellowship.

A. S. Bandeira is with the Program in Applied and Computational Mathematics, Princeton University, Princeton, NJ 08544 USA (e-mail: ajsb@math.princeton.edu).

E. Dobriban is with the Department of Statistics, Stanford University, Stanford, CA 94305 USA (e-mail: dobriban@stanford.edu).

D. G. Mixon is with the Department of Mathematics and Statistics, Air Force Institute of Technology, Wright-Patterson AFB, OH 45433 USA (e-mail: dustin.mixon@afit.edu).

W. F. Sawin is with the Department of Mathematics, Princeton University, Princeton, NJ 08544 USA (e-mail: wsawin@math.princeton.edu).

Communicated by M. Elad, Associate Editor for Signal Processing.

Digital Object Identifier 10.1109/TIT.2013.2248414

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 the work of Koiran and Zouzias, who report hardness results based on alternative complexity hypotheses, i.e., the complexity of dense subgraph problems [8] and the hidden clique problem [9]. We note that our result was independently proved by Tillmann and Pfetsch [10] using a nearly identical argument.

In Section II, we review the basic concepts we will use from computational complexity, and Section III contains our main result.

II. 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 that can be solved in polynomial time, while problems in EXP 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[11]. 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

obvious whether the problem is actually NP-hard. Indeed, by the definition of NP-hard, one must compare its complexity to the complexity of every problem in NP. To this end, notice that $A \leq B$ and $B \leq C$ together imply $A \leq C$, and so to demonstrate that a problem C is NP-hard, it suffices to show that $B \leq C$ for some NP-hard problem B.

In this paper, we demonstrate the hardness of certifying RIP by reducing from the following problem.

Problem 3: Given a matrix Ψ and some positive integer K, do there exist K columns of Ψ which are linearly dependent?

Problem 3 has a brief history in computational complexity. First, McCormick [12] demonstrated that the analogous problem of testing the girth of a transversal matroid is NP-complete, and so by invoking the randomized matroid representation of Marx [13], Problem 3 is hard for NP under randomized reductions [14]. Next, Khachiyan [15] showed that the problem is NP-hard by focusing on the case where K equals the number of rows of Ψ; using a particular matrix construction with Vandermonde components, he reduced the subset sum problem to this instance of the problem. Later, Erickson [16] and Chistov *et al.* [17] offered alternative proofs of this NP-hardness result, the latter reducing from a different NP-complete problem. Recently, Tillmann and Pfetsch [10] used ideas similar to McCormick's to reduce Problem 3 from the clique problem, thereby demonstrating strong NP-hardness. Each of these complexity results uses $M \times N$ matrices with integer entries whose binary representations take $\leq p(M,N)$ bits for some polynomial p; we will exploit this feature in our proof.

III. Main Result

Theorem 4: Problem 2 is NP-hard.

Proof: Reducing from Problem 3, suppose we are given a matrix Ψ with integer entries. Letting $\mathrm{Spark}(\Psi)$ denote the size of the smallest collection of linearly dependent columns of Ψ, we wish to determine whether $\mathrm{Spark}(\Psi) \leq K$. To this end, we take $P \leq 2^{p(M,N)}$ to be the size of the largest entry in Ψ, and define $C = 2^{\lceil \log_2 \sqrt{MN}P \rceil}$ and $\Phi = \frac{1}{C}\Psi$; note that we choose C to be of this form instead of $\sqrt{MN}P$ to ensure that the entries of Φ can be expressed in $\mathsf{poly}(M,N)$ bits without truncation. Of course, linear dependence between columns is not affected by scaling, and so testing Φ is equivalent to testing Ψ. In fact, since we plan to appeal to an RIP oracle, it is better to test Φ since the right-hand inequality of Definition 1 is already satisfied for every $\delta > 0$:

$$\|\Phi\|_2 \leq \sqrt{MN}\|\Phi\|_{\max} = \sqrt{MN}\frac{P}{C} \leq 1 \leq \sqrt{1+\delta}.$$

We are now ready to state the remainder of our reduction: For some value of δ (which we will determine later), ask the oracle if Φ is (K,δ)-RIP; then

$$\begin{array}{lrcl} \text{(i)} & \Phi \text{ is } (K,\delta)\text{-RIP} & \Longrightarrow & \mathrm{Spark}(\Psi) > K, \\ \text{(ii)} & \Phi \text{ is not } (K,\delta)\text{-RIP} & \Longrightarrow & \mathrm{Spark}(\Psi) \leq K. \end{array}$$

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

Note that (i) immediately holds for all choices of $\delta \in (0,1)$ by the contrapositive. Indeed, $\mathrm{Spark}(\Psi) \leq K$ implies the existence of a nonzero vector x in the nullspace of Φ with $\leq K$ nonzero entries, and $\|\Phi x\|^2 = 0 < (1-\delta)\|x\|^2$ violates the left-hand inequality of Definition 1. For (ii), we also consider the contrapositive. When $\mathrm{Spark}(\Psi) > K$, we have that every size-K subcollection of Ψ's columns is linearly independent. Letting $\Psi_{\mathcal{K}}$ denote the submatrix of columns indexed by a size-K subset $\mathcal{K} \subseteq \{1,\dots,N\}$, this implies that $\lambda_{\min}(\Psi_{\mathcal{K}}^*\Psi_{\mathcal{K}}) > 0$, and so $\det(\Psi_{\mathcal{K}}^*\Psi_{\mathcal{K}}) > 0$. Since the entries of Ψ lie in $\{-P,\dots,P\}$, we know the entries of $\Psi_{\mathcal{K}}^*\Psi_{\mathcal{K}}$ lie in $\{-MP^2,\dots,MP^2\}$, and since $\Psi_{\mathcal{K}}^*\Psi_{\mathcal{K}}$ is integral with positive determinant, we must have $\det(\Psi_{\mathcal{K}}^*\Psi_{\mathcal{K}}) \geq 1$. In fact

$$\begin{aligned} 1 &\leq \det(\Psi_{\mathcal{K}}^*\Psi_{\mathcal{K}}) \\ &= \prod_{k=1}^{K} \lambda_k(\Psi_{\mathcal{K}}^*\Psi_{\mathcal{K}}) \\ &\leq \lambda_{\min}(\Psi_{\mathcal{K}}^*\Psi_{\mathcal{K}}) \cdot \lambda_{\max}(\Psi_{\mathcal{K}}^*\Psi_{\mathcal{K}})^{K-1} \\ &\leq \lambda_{\min}(\Psi_{\mathcal{K}}^*\Psi_{\mathcal{K}}) \cdot \left(K\|\Psi_{\mathcal{K}}^*\Psi_{\mathcal{K}}\|_{\max}\right)^{K-1} \end{aligned}$$

and so we can rearrange to get

$$\lambda_{\min}(\Phi_{\mathcal{K}}^*\Phi_{\mathcal{K}}) = \frac{1}{C^2}\lambda_{\min}(\Psi_{\mathcal{K}}^*\Psi_{\mathcal{K}}) \geq \frac{1}{C^2(KMP^2)^{K-1}}.$$

From here, we apply the definition of C to get $C^2 \leq 2^{4\log_2\sqrt{MN}P} = (MNP^2)^2$. Since $K \leq M \leq N$, the denominator above is then bounded by

$$C^2(KMP^2)^{K-1} \leq (MNP^2)^{M+1} \leq 2^{(M+1)(2p(M,N)+MN)}$$

where the last inequality follows from the assumption $P \leq 2^{p(M,N)}$ and $\log_2(MN) \leq MN$. Therefore, if we pick $\delta := 1 - 2^{-(M+1)(2p(M,N)+MN)}$, then since our choice for $\mathcal{K}$ was arbitrary, we conclude that Φ is (K,δ)-RIP whenever $\mathrm{Spark}(\Psi) > K$, as desired. Moreover, since δ can be expressed in the standard representation using $\mathsf{poly}(M,N)$ bits, we can ask the oracle our question in polynomial time. ∎

It is important to note that Theorem 4 is a statement about testing for RIP in the worst case; this result does not rule out the existence of matrices for which RIP is easily verified (e.g., using coherence in conjunction with the Gershgorin circle theorem for small values of K[5]). Furthermore, our choice of δ in the above proof is rather close to 1, and so Theorem 4 should be viewed as a first step toward understanding the computational complexity of certifying RIP. Indeed, the complexity for smaller values of δ is still open, as is the hardness of approximating the smallest δ for which a matrix is (K,δ)-RIP, though both of these are addressed by Koiran and Zouzias in [8] and [9].

Acknowledgment

The authors thank Boris Alexeev for reading this manuscript and providing thoughtful comments and suggestions. The views expressed in this article are those of the authors and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the U.S. Government.

References

[1] E. J. Candès and T. Tao, "Decoding by linear programming," *IEEE Trans. Inf. Theory*, vol. 51, no. 12, pp. 4203–4215, Dec. 2005.

[2] E. J. Candès, "The restricted isometry property and its implications for compressed sensing," *C. R. Acad. Sci. Paris, Ser. I*, vol. 346, pp. 589–592, 2008.
[3] D. Needell and J. A. Tropp, "CoSaMP: Iterative signal recovery from incomplete and inaccurate samples," *Appl. Comput. Harmon. Anal.*, vol. 26, pp. 301–321, 2009.
[4] T. Blumensath and M. E. Davies, "Iterative hard thresholding for compressed sensing," *Appl. Comput. Harmon. Anal.*, vol. 27, pp. 265–274, 2009.
[5] A. S. Bandeira, M. Fickus, D. G. Mixon, and P. Wong, The road to deterministic matrices with the restricted isometry property [Online]. Available: arXiv:1202.1234
[6] R. DeVore, "Deterministic constructions of compressed sensing matrices," *J. Complex.*, vol. 23, pp. 918–925, 2007.
[7] T. Tao, Open Question: Deterministic UUP Matrices [Online]. Available: http://terrytao.wordpress.com/2007/07/02/open-question-deterministic-uup-matrices
[8] P. Koiran and A. Zouzias, On the certification of the restricted isometry property [Online]. Available: arXiv: 1103.4984
[9] P. Koiran and A. Zouzias, Hidden cliques and the certification of the restricted isometry property [Online]. Available: arXiv:1211.0665
[10] A. M. Tillmann and M. E. Pfetsch, The computational complexity of the restricted isometry property, the nullspace property, and related concepts in compressed sensing [Online]. Available: arXiv:1205.2081
[11] S. Cook, The P Versus NP Problem [Online]. Available: http://www.claymath.org/millennium/P_vs_NP/pvsnp.pdf
[12] S. T. McCormick, "A combinatorial approach to some sparse matrix problems," Ph.D. dissertation, Stanford Univ., Stanford, CA, USA, 1983.
[13] D. Marx, "A parameterized view on matroid optimization problems," *Theor. Comput. Sci.*, vol. 410, pp. 4471–4479, 2009.
[14] B. Alexeev, J. Cahill, and D. G. Mixon, "Full spark frames," *J. Fourier Anal. Appl.*, vol. 18, pp. 1167–1194, 2012.
[15] L. Khachiyan, "On the complexity of approximating extremal determinants in matrices," *J. Complex.*, vol. 11, pp. 128–153, 1995.
[16] J. Erickson, "New lower bounds for convex hull problems in odd dimensions," *SIAM J. Comput.*, vol. 28, pp. 1198–1214, 1999.
[17] A. Chistov, H. Fournier, L. Gurvits, and P. Koiran, "Vandermonde matrices, NP-completeness, and transversal subspaces," *Found. Comput. Math*, vol. 3, pp. 421–427, 2003.

Afonso S. Bandeira received both the B.S. degree in mathematics in 2009 and the M.S. degree in applied analysis and computational mathematics in 2010, both from the University of Coimbra, Coimbra, Portugal. Since 2010, he has been a graduate student at Princeton University, Princeton, NJ, pursuing the Ph.D. in applied and computational mathematics. His research interests include spectral graph theory, applied harmonic and functional analysis, and approximate algorithms to solve problems motivated by the mathematical analysis of massive data sets.

Edgar Dobriban received the B.A. degree in mathematics from Princeton University, Princeton, NJ, in 2012. As of 2013, he is a Ph.D. student in the Department of Statistics at Stanford University, Stanford, CA. His research interests include the statistical and computational methods needed for high-dimensional data sets, and applications to computational biology.

Dustin G. Mixon received the B.S. degree in mathematics from Central Washington University, Ellensburg, WA, in 2004, the M.S. degree in applied mathematics from the Air Force Institute of Technology, Wright-Patterson AFB, OH, in 2006, and the Ph.D. degree in applied and computational mathematics from Princeton University, Princeton, NJ, in 2012.

From 2006 to 2009, he was an applied mathematical analyst at the Air Force Research Laboratory, Brooks City-Base, TX. He is presently an Assistant Professor of Mathematics in the Department of Mathematics and Statistics at the Air Force Institute of Technology. His research interests include frame theory, signal processing, and compressed sensing.

William F. Sawin received the B.S. degree in mathematics and economics from Yale University, New Haven, CT, in 2011. Since 2011, he has been a graduate student at Princeton University, Princeton, NJ, pursuing the Ph.D. in mathematics. His research interests include algebraic geometry and number theory.