A Well-Characterized Approximation Problem

Johan Håstad
Royal Institute of Technology

Steven Phillips*
Stanford University

Shmuel Safra
Stanford University &
IBM Almaden

Abstract

We consider the following NP optimization problem: Given a set of polynomials $P_i(x)$, $i = 1 \ldots s$ of degree at most 2 over $GF[p]$ in n variables, find a root common to as many as possible of the polynomials $P_i(x)$. We prove that in the case when the polynomials do not contain any squares as monomials, it is always possible to approximate this problem within a factor of $\frac{p^2}{p-1}$ in polynomial time for fixed p. This follows from the stronger statement that one can, in polynomial time, find an assignment that satisfies at least $\frac{p-1}{p^2}$ of the nontrivial equations.

More interestingly, we prove that approximating the maximal number of polynomials with a common root to within a factor of $p - \epsilon$ is NP-hard. This implies that the ratio between the performance of the approximation algorithm and the impossibility result is essentially $\frac{p}{p-1}$ which can be made arbitrarily close to 1 by choosing p large.

We also prove that for any constant $\delta < 1$, it is NP-hard to approximate the solution of quadratic equations over the rational numbers, or over the reals, within n^δ.

*Partially supported by NSF Grant CCR-9010517 and grants from Mitsubishi and OTL.

1 Introduction

Recently, there has been substantial progress [9, 2, 4, 3, 13, 11, 6] in showing that the approximation of various NP optimization problems is NP-hard. At the heart of these results stands a new characterization of the class NP as all languages whose membership proofs can be verified probabilistically, reading only a few bits of the membership proof, and using a small number of random bits. The proof of that characterization uses quite powerful techniques and is rather complicated. As yet we do not know of a simple proof for that characterization, or of a different proof for the hardness of these approximation problems. Finding a simpler proof for that characterization would be meaningful progress, possibly yielding other results, such as closing the gap between the factors of approximation known to be tractable and those known to be NP-hard.

This note studies an optimization problem, related to problems studied in the above-mentioned work, whose approximability can be determined using fairly simple techniques. The problem is: given a set of degree 2 equations over a finite field of size p, where p is a small prime, determine the maximal number of equations that can be satisfied by a single setting of the variables. For the case where the polynomials contain no squares we first prove that this number can be approximated to within a factor $\frac{p^2}{p-1}$ in polynomial time. This is established by showing that for any set of nontrivial equations it is always possible to find in polynomial time an assignment that satisfies a fraction at least $\frac{1}{p} - \frac{1}{p^2}$ of the equations.

On the other hand, we show that approxi-

mating the maximal number of polynomials satisfiable concurrently to within a factor of $p-\epsilon$ is NP-hard. In fact we prove slightly more, namely that it is NP-hard to determine whether it is possible to satisfy all equations simultaneously or only a fraction $\frac{1}{p}+\epsilon$.

The bounds imply that the gap between the factor to which our problem can be approximated and the factor for which it is NP-hard to approximate is essentially $\frac{p}{p-1}$ which can be made as close to 1 as desired by choosing p large.

Nonapproximability results for sets of polynomial equations over the rational numbers have been obtained by Bellare and Petrank [12], and more general nonlinear optimization has been studied by Bellare and Rogaway [7]. However, in both these cases, the nonapproximability results use the complicated techniques originating from interactive proofs. We strengthen the results of Bellare and Petrank and show, without using any complicated techniques, that when the field in question is the rational numbers or the real numbers, then our problem cannot be approximated within n^{δ} in polynomial time, for any constant $\delta < 1$.

An outline of the paper is the following: In Section 2 we state our problem formally. We prove our positive results in Section 3 and the negative results in Sections 4 and 5, and end with some remarks.

2 The problem

Let p be a fixed prime. We consider the problem in which we are given a set of polynomial equations of degree at most 2 in n unknowns over $GF[p]$,

$$P_i(x) = 0, i = 1, 2 \ldots s.$$

We assume that none of the polynomials contains any monomial x_i^2 and that none of the polynomials is a constant. We want to find an assignment to the variables which satisfy as many as possible of the equations. Let us call the problem QS_p, where QS stands for quadratic solvability.

Remark: Disallowing constant polynomials is just a matter of definition, while not allowing any square terms is a restriction.

3 The approximation algorithm

In this section we prove

Theorem 3.1 *Given an instance of QS_p with s equations we can in polynomial time find an x which satisfies at least $\frac{(p-1)s}{p^2}$ of the equations.*

Proof: We will assign the variables one by one. In the process we will keep a potential of the left hand side of the equations nondecreasing. The potential of a nonconstant polynomial of degree 2 is $(p-1)p^{-2}$, the potential of a nonconstant linear polynomial is p^{-1}, while the potential of the constant 0 is 1 and the potential of other constants is 0. This potential corresponds to a lower bound on the fraction of inputs that satisfy the equation. Our algorithm tries to find an assignment which satisfies as least the same number of equations as a random assignment does on the average. The potential is used to guide this search.

When assigning a variable x_i we evaluate the potential of the p possibilities (i.e. setting $x_i = a$ for $a \in \{0, 1, \ldots p-1\}$) and make the assignment which gives the largest potential. We need to check that the potential will never decrease using this procedure. We do this by proving that the average of the potential of the p possibilities is at least the potential before x_i is assigned a value.

The only way the potential of an equation can go down is when it transforms into a nonzero constant. Suppose the assignment $x_i = 0$ transforms P_j to the constant 1. There are two cases, either the original equation was of degree two or of degree one. The second case is easy since if P_j is nontrivial linear, some other assignment of x_i will give $P_j = 0$. This means that out of p assignments, one will give potential 1 (and all others will give 0) and thus the average potential remains the same.

If P_j was of degree two then it must be of the form $x_i L(x) + 1$. Here $L(x)$ is a nontrivial linear polynomial which does not contain x_i and hence any other assignment than $x_i = 0$ will give a nontrivial linear function. Thus in this case we get the potential p^{-1} in $p-1$ cases and thus also in the average potential remains the same.

Because the average potential of the p alternatives is at least the original potential, picking

the maximum will ensure that the potential is always greater than or equal to its initial value. The potential is initially at least $s(p-1)p^{-2}$ and hence the final assignment must satisfy at least $s(p-1)p^{-2}$ equations. ∎

Remark The problem with allowing square terms is clear in this proof since equations of the form $x_i^2 + c = 0$ might not allow any solutions.

4 Impossibility of good approximations

In this section we prove the following theorem:

Theorem 4.1 *If QS_p can be approximated within a factor of $p-\epsilon$ in polynomial time where ϵ is at least an inverse polynomial, then $P = NP$.*

We will first prove that it is NP-complete to determine if we can satisfy all equations.

Theorem 4.2 *Given an instance of QS_p it is NP-complete to determine whether it is possible to satisfy all equations simultaneously.*

Proof: This problem (for $GF[2]$) appears as AN9 on page 251 in Garey & Johnson [10]; the variant we consider here is attributed to Valiant as personal communication. For completeness, we give the proof. We reduce from SAT. Given an instance φ of SAT that contains the variables $x_1, x_2, \ldots x_n$. First we make a straight line program that computes $\varphi(x)$ leaving $x_1, x_2, \ldots x_n$ as free variables. We can assume that this program uses the variables $x_{n+1}, x_{n+2} \ldots x_m$ and that each instruction is of the form $x_i = x_j \wedge x_k$ with $i > j > k$ or $x_i = \neg x_j$ with $i > j$.

Now form a set of equations using $x_i - x_j x_k = 0$ in the first case and $x_i + x_j - 1 = 0$ in the second. Finally add the equation $x_m - 1 = 0$. If $p = 2$, to satisfy all these equations one must clearly find an instance that satisfies φ. When $p > 2$ there is the added problem that x_i might take values that are not 0 or 1. This is dealt with by making sure that $x_i(1 - x_i) = 0$. We do not want to add any equations not of the proper form and hence we add variables z_i and the equations $z_i = x_i$ and $x_i(1 - z_i) = 0$. Now clearly any assignment that satisfies this system of equations contains a subassignment that satisfies φ. ∎

The polynomials obtained are of a very special form. For instance no equation contains more than three variables. This does not, however, matter for the proof of Theorem 4.1. We will refer to the problem of satisfying all equations considered in Theorem 4.2 as the *exact* problem.

Let us now proceed to establish Theorem 4.1. Suppose we have an instance of the exact problem given by Q_i, $i = 1, 2 \ldots s$. Now suppose we have a set A of vectors in $GF[p]^s$ which have the property that for any nonzero vector t in $GF[p]^s$ the number of vectors a in A such that $\sum_{i=1}^{s} a_i t_i = 0$ is at most $(\frac{1}{p} + \frac{\epsilon}{p^2})|A|$. The construction of such a set A has been considered in the case $p = 2$ by [14, 1] and the more general case has been studied in [1, 5, 8]. Using these constructions it is possible to choose an explicit and easy to construct such set A of size $O(p^4 s^2 \epsilon^{-2})$. Suppose this set contains the vectors $a^{(i)}$, $i = 1, 2 \ldots r$. Consider the system of equations

$$\sum_{j=1}^{s} a_j^{(i)} Q_j(x) = 0 \qquad i = 1, 2 \ldots r$$

where the summation is in $GF[p]$. If the original system was satisfiable, it is possible to satisfy all r equations using the same assignment. On the other hand if the system was not satisfiable, by the above property for the set A, no assignment will satisfy more than $(\frac{1}{p} + \frac{\epsilon}{p^2})r$ equations. This implies that if there is an approximation algorithm satisfying the assumption of Theorem 4.1, then this can be used to solve an NP-complete problem in polynomial time and thus the proof is complete.

5 Approximating quadratic equations over the rationals and reals

In this section we generalize the negative results of Section 4 to the real field $\mathcal{R}$ and the rational field $\mathcal{Q}$.

For a field $\mathcal{F}$, let us denote by $QS_{\mathcal{F}}$ the following problem: given a set of polynomial equations of degree 2 over $\mathcal{F}$, determine the maximum number of equations that can be simultaneously satisfied. Below we use n to denote the total number of nonzero coefficients in all the equations.

Theorem 5.1 *Let $\mathcal{F} = \mathcal{R}$ or $\mathcal{F} = \mathcal{Q}$. Then, for any constant $\delta < 1$, it is NP-hard to approximate $QS_{\mathcal{F}}$ within a factor of n^{δ}.*

Proof: We first note that the proof of Theorem 4.2 shows that the exact problem is NP-hard, regardless of the field. Starting from the system of quadratic equations over $\mathcal{F}$ used in Theorem 4.2, we construct a new quadratic system by taking many linear combinations of the original quadratic equations. We could derive nonapproximability within n^{δ} for $\delta < 1/2$ by determining the coefficients of the linear combinations as in Theorem 4.1. (Indeed, nonapproximability within any constant factor smaller than 2 can be derived using the field $GF(2)$). However, we obtain the stronger result by defining the coefficients as follows.

Let S be the set of equations used in the proof of Theorem 4.2, and let $s = |S|$. We start by selecting a prime p so that $p/s \approx (ps)^{\delta}$. Let B be the $p \times s$ matrix over $GF[p]$ whose (i,j)'th entry $b_{i,j}$ satisfies $b_{i,j} = i^j \pmod p$. B defines a set of equations, where equation i is obtained by multiplying each equation j from S by $i^j \pmod p$, and summing. Note that for this set of equations, we have $n = O(ps)$.

Any assignment that does not satisfy all equations in S can only satisfy at most s of the new equations, since for equation i to be satisfied, i needs to satisfy a nontrivial equation mod p of degree at most s.

To complete the proof and show hardness of approximating within $p/s = \Omega(n^{\delta})$, we need to show that for any non-zero real or rational vector $y \in \mathcal{R}^s$, representing the value of the quadratic system under some assignment to the variable vector x, the vector By has at most s zero entries.

Let $y \in \mathcal{F}^s$, $y \neq 0$. Consider the following linear system in variables $z_1, \ldots, z_s$:

$$\sum_{j=1}^{s} a_j^i z_j = 0 \qquad \text{for } i \text{ where } \textstyle\sum_{j=1}^{s} a_j^i y_j = 0$$

$$\sum_{j=1}^{s} a_j^i z_j > 0 \qquad \text{for } i \text{ where } \textstyle\sum_{j=1}^{s} a_j^i y_j > 0$$

$$\sum_{j=1}^{s} a_j^i z_j < 0 \qquad \text{for } i \text{ where } \textstyle\sum_{j=1}^{s} a_j^i y_j < 0$$

Clearly, in case $\mathcal{F} = \mathcal{Q}$ this system has a rational solution, but this holds also for $\mathcal{F} = \mathcal{R}$ (since a solution in reals, to a linear system, implies one in rationals). Let us denote the rational solution by w. Let l be the lcm of the integers appearing as denominators in w. Let $w' = lw$, so w' is an integer vector which also satisfies the above linear system. Let g be the gcd of the integers appearing in w', and set $w'' = w'/g$. Then, w'' is an integer vector that is not divisible by p. Lastly reduce each entry of w'' modulo p, to get a non-zero vector $w''' \in GF[p]^s$, for which Bw''' (where operations are over $GF[p]$) has at least as many zeroes as By, and hence By has at most s zero entries. ∎

6 Conclusions

We have studied a fairly natural approximation problem and without any sophisticated techniques we have proved that this problem can be approximated within a factor of $\frac{p^2}{p-1}$ but not within a factor significantly smaller than p.

It is not clear to us how this ties in with existing results. The problem does not seem to be in MAXSNP. One might hope that the technique used for the lower bound might be useful in obtaining strong results for more central problems.

7 Acknowledgements

We would like to thank Oded Goldreich for many helpful comments and suggestions.

References

[1] N. Alon, O. Goldreich, J. Håstad and R. Peralta. Simple constructions of almost

k-wise independent random variables. *Random Structures and Algorithms*, 3(3):289-304, 1992.

[2] S. Arora and S. Safra. Probabilistic Checking of Proofs; a New Characterization of NP. *Proc. 33rd IEEE Sym. on Foundation of Computer Science*, October 1992, pp. 1-13.

[3] S. Arora, C. Lund, R. Motwani, M. Sudan and M. Szegedy. Proof verification and intractability of approximation problems. *Proc. 33rd IEEE Sym. on Foundation of Computer Science*, October 1992, pp. 14-23.

[4] S. Arora, R. Motwani, S. Safra, M. Sudan and M. Szegedy. PCP and the hardness of approximation problems. Unpublished note, February 1992.

[5] Y. Azar, R. Motwani and J. Naor. Approximating Arbitrary Probability Distributions Using Small Sample Spaces. To appear, 1993.

[6] M. Bellare, S. Goldwasser, C. Lund and A. Russell. Efficient Probabilistically Checkable Proofs; Applications to Approximation. *25th ACM Sym. on Theory of Computation*, May 1993, pp 294-304.

[7] M. Bellare and P. Rogaway. The complexity of approximating a nonlinear program. IBM Technical report, RC 17831 (# 78493).

[8] G. Even. Construction of Small Probability Spaces for Deterministic Simulation. M. Sc. Thesis (in Computer Science), Technion, Haifa, Israel, August 1991, (in Hebrew, abstract in English).

[9] U. Feige, S. Goldwasser, L. Lovász, S. Safra and M. Szegedy. Approximating clique is almost NP-complete. *Proc. 32nd IEEE Sym. on Foundations of Computer Science*, October 1991, pp. 2-12.

[10] M.R. Garey and D. S. Johnson. *Computers and Intractability: A Guide to the Theory of NP-Completeness.* W. H. Freeman, 1979.

[11] C. Lund and M. Yannakakis. On the Hardness of Approximating Minimization Problems. *25th ACM Sym. on Theory of Computation*, May 1993, pp 286-293.

[12] E. Petrank. The Hardness of Approximation: Gap Location. To appear at *2nd Israel Symposium on Theory of Computing and Systems*, 1993.

[13] S. Phillips and S. Safra. PCP and tighter bounds for approximating MAX-SNP. Manuscript, April 1992.

[14] J. Naor and M. Naor. Small-bias probability spaces: Efficient constructions and applications. *Proc. 22nd ACM Sym. on Theory of Computing*, May 1990, pp. 213-223.