REDUCIBILITY, RANDOMNESS, AND INTRACTIBILITY

(Abstract)

Leonard Adleman[†]
Department of Mathematics
Massachusetts Institute of Technology
Cambridge, Massachusetts 02139

Kenneth Manders*
Group in Logic and Methodology of Science
University of California at Berkeley
Berkeley, California 94720

I. INTRODUCTION

Reducibility and Intractibility

The method of showing a problem NP-complete by polynomial reduction is one of the most elegant and productive in our theory ([1], [3]). It is a means of providing compelling evidence that a problem in NP is not in P. In this paper we will demonstrate new methods for showing this.

Our methods, based on a new notion of reducibility (gamma-reducibility) are apparently of more general applicability than that of polynomial reduction and are intended to be of practical value to researchers in the field.

[†]Supported in part by ONR N00014-67-0204-0063.

*Research Supported by National Science Foundation Grant DCR72-03725-A02

We use our methods to "demonstrate" (i.e., give compelling evidence) that some natural problems in NP *which are not known to be NP-complete* are, nonetheless, not in P. In particular, we show:

Theorem I: The following are equivalent:

(1) $NP \neq NP^C$ (= the complement of NP)

(2) (Linear Divisibility)

Let $A = \{\langle a,c\rangle \mid a,c \in \omega \text{ and } (\exists x \in \omega)[x \neq 0 \text{ and } ax+1 \text{ divides } c]\}$ then the membership problem for A is not in $NP \cap NP^C$ (and, therefore, not in P).

(3) (Binary-Quadratic Diophantine Equations)

The problem of deciding from inputs $a,b \in \omega$ whether there exists $x,y \in \mathbb{Z}^+$ such that $axy+y=b$ is not in $NP \cap NP^C$ (and, therefore, not in P).

(4) The problem of deciding from inputs $p,q_1,\ldots,q_z$ where p is a prime, $q_i (1 \leq i \leq z)$ are sparse polynomials whether there is a natural number n such that $\prod_{i=1}^{z} q_i(n) \neq 0 \bmod(p)$ is not in $NP \cap NP^C$ (and, therefore, not in P).

In Section II additional motivation, definitions and a proof of Theorem I are presented.

Reducibility and Randomness

Strassen [12], Miller [8], Rabin [11] and others have recently shown that primality can be "decided" with a fixed small ($< \frac{1}{1,000,000}$) probability of error on a random ("coin

---

†In [7] we proved that the problem of finding natural number solutions to binary quadratic diophantine equations was NP-complete; however, we were unable to extend that result to include the possibility of integer solutions.

flipping") machine running in polynomial time. More precisely, there is a deterministic Turing machine M with a random number generator which on any given input x

(1) halts with a "yes" or "no" output within $p(|x|)$ steps (for some polynomial p independent of x)

(2) when x is prime outputs "yes"

(3) when x is non-prime outputs "no" with probability $1 - 1/1{,}000{,}000$ (independent of x).

We call sets for which such machines exist randomly decidable[†]. We are curious about the power of randomness. Can every set in NP be randomly decided? We doubt this (a proof requires showing NP≠P); however, the notion is too new for any strong intuitions either way. It is clear that satisfiability (an NP-complete problem) is randomly decidable if and only if every set in NP is randomly decidable (i.e., polynomial reduction preserves randomness downwards). Using a different, broader notion of reducibility (which also preserves randomness downwards) we show (using extended Riemann hypothesis) that a problem which is *not* known to be NP-complete has the property that it is randomly decidable if and only if every set in NP is randomly decidable.

Theorem II: [Assuming Extended Riemann Hypothesis] Every set in NP is randomly decidable

$$\Leftrightarrow$$

$B = \{\langle k,b,L\rangle \mid k,b,L \in \omega \text{ and } (\exists xy \in \omega)[2^k xy + by = L]\}$ is randomly decidable.

This is either evidence that this problem is not randomly decidable (and a fortiori not in P), or grounds to focus on this problem to show that every set in NP is randomly decidable. In Section III a proof of Theorem II is outlined.

If every set in NP is randomly decidable (or if a significant subset of sets is), then we may be forced to reappraise our current thesis that "tractible" means decidable in deterministic polynomial time. In Section IV, we briefly consider this philosophical question and give an example of a set which is not known to be in P (is "more" than randomly decidable) and satisfies out intuitions about tractibility.

II. REDUCIBILITY AND INTRACTIBILITY

The following is a well known theorem in complexity theory.

[†]Many other researchers have considered such machines including Gill [2], Miller [8], Strassen [12], Solovay [12], and Rabin [10].

Theorem (Cook, Karp) For all A

$$(\forall B \in NP)\ [B \leq_p A] \Longrightarrow [NP \neq P \Longrightarrow A \notin P].$$

It states that if a set can be shown to have a certain property ($(\forall B \in NP[B \leq_p A])$ then there is evidence ($NP \neq P$) that the membership problem for that set is intractible ($A \notin P$). It has been estimated that since 1970 over 2000 problems have been demonstrated† to be intractible by this method. However, some problems (most notably graph isomorphism) which appear to be intractible have resisted such a demonstration. Possibly such problems simply require greater ingenuity in applying this method and will eventually yield. Another possibility is captured in the following theorem:

Theorem (Ladner [4]) Assuming $NP \neq P$ then

$$(\exists A \in NP)[A \notin P \text{ and } \neg\ (\forall B \in NP)[B \leq_p A]\ .$$

So ($NP \neq P$ implies) there are sets which are intractible but which cannot be demonstrated to be by showing that every set in NP is polynomial reducible to them. Our goal is to find new, useful methods of showing the intractibility of such sets. Our approach has been to start with a weaker (though still compelling) choice of evidence ($NP \neq NP^C$) and to find a new method for applying this evidence in demonstrating the intractibility of problems. Because our notion of evidence is weaker we expect our methods to be more generally applicable. Our basic theorem is:

Theorem III For all sets A

$$(\forall B \in NP)[B \leq_\gamma A] \Longrightarrow [NP \neq NP^C \Longrightarrow A \notin P]$$

where intuitively $B \leq_\gamma A$ is the same as $B \leq_p A$ except that the reducing machine is nondeterministic and, therefore, is allowed to guess. Below $\leq_\gamma$ is defined precisely.

Def A nondeterministic Turing Machine M runs in polynomial time iff there is a polynomial p such that for all x: any computation path of M on input x which halts, does so within $p(|x|)$ steps.

We allow nondeterministic Turing machines which produce outputs when they halt.

Def For any nondeterministic Turing machine M which runs in polynomial time

$R_M = \{\langle x,y\rangle |$ Some computation path of M on input x halts with the output y$\}$.

---

†We will say that a problem has been "shown to be intractible" or "demonstrated to be intractible" to mean some compelling evidence (e.g., $NP \neq P$) for its intractibility has been proved -- not that its intractibility has been proved.

Def For any sets A and B: A is γ-reducible to B ($A \leq_\gamma B$) iff there is a non-deterministic Turing machine M which runs in polynomial time such that:

(1) $(\forall x)\ (\exists y)\ [\langle x,y\rangle \in R_M]$
(at least one path halts),

(2) $(\forall x)\ (\forall y)\ [\langle x,y\rangle \in R_M \rightarrow [x \in A \Leftrightarrow y \in B]]$
(all outputs are valid reductions of A to B).

Below are some basic facts about γ-reducibility:

Theorem IV $A \leq_p B \Rightarrow A \leq_\gamma B$

So every polynomial reduction is a special case of a γ-reduction.

Def A set A is γ-complete iff

(1) $A \in NP$,

(2) $(\forall B \in NP)[B \leq_\gamma A]$.

Theorem V If A is γ-complete then

$$A \in NP \cap NP^C \Leftrightarrow NP = NP^C .$$

Pf. It is easily seen that the nondeterministic machine which γ-reduces SAT to A together with a non-deterministic acceptor of $\overline{A}$ can be combined into a non-deterministic acceptor of the complement of SAT. The theorem follows easily.

Cor If A is γ-complete then

$$NP \neq NP^C \Rightarrow A \notin P.$$

Before proving Theorem I we motivate the linear divisibility problem. Consider the following set

$$B = \{\langle a,c\rangle \mid a,c \in \omega \text{ and } (\exists x \in \omega)[x \neq 0 \text{ and } ax+0 \text{ divides } c]\} .$$

What is the complexity of this set? It is easily seen that $\langle a,c\rangle \in B \Leftrightarrow a$ divides c, so its complexity is less than n^2. It is, therefore, surprising that replacing $ax+0$ by $ax+1$ in the definition yields an intractible problem.

It is well known that the 1st order theory of the natural numbers with plus and times, $Th(\langle \omega,+,\cdot\rangle)$, is undecidable. It is no surprise then that $Th(\langle \omega,+,|\rangle)$ (where $|$ is the "divides" relation) is also undecidable. Restriction of $Th(\langle \omega,+,\cdot\rangle)$ to just existentially quantified sentences (in prenex form) is also undecidable (this is Hilbert's 10th problem) it is surprising then that Lipschitz [6] has shown that the existential part

of $Th(<\omega,+,|>)$ is NP-complete. In a subsequent paper Lipschitz [5] has shown that restriction of this existential theory to sentences with fewer than eight clauses is still NP-complete. When the theory is restricted to single clauses of the simpliest type (e.g., $(\exists x)[5x+7|120]$ then the theory is not known to be NP-complete but this is the linear divisibility problem which we now show is γ-complete.

Proof of Theorem I Since $X \leq_p Y \Rightarrow X \leq_\gamma Y$ it suffices to show that an NP-complete problem is γ-reducible to A.

FACT: The problem of accepting those inputs

$$<a_1,a_2,\ldots,a_n,b> \quad (a_i,b\varepsilon\omega, 0<a_i<b, 1\leq i\leq n)$$

such that

$$(\exists S\subseteq\{1,2,\ldots,n\})(\exists m\varepsilon\omega)[S\neq\phi \text{ and } \sum_{i\varepsilon S} a_i=mb] \text{ is NP-complete.}$$

We call this variant of the knapsack problem [3] the multisack problem. It is easily shown to be NP-complete. Consider the following nondeterministic Turing machine which runs in polynomial time and γ-reduces the multisack problem to the linear divisibility problem

"on input $<a_1,\ldots,a_n,b>$ nondeterministically guess $<p,F_{p-1},pf_p,g',g,p_1,\ldots,p_n,$ $pf_1,\ldots,pf_n,\alpha_1,\ldots,\alpha_n>$ of length at most $|\sum_{i=1}^{n} a_i+b|^4$ and confirm the following:

(1) pf_p is a proof of the primality of p (e.g., a path through Pratts' algorithm [10]).

(2) p is in the arithmetic progression $\{b+1,2b+1,\ldots\}$.

(3) F_{p-1} is the prime factorization of p-1 (so guessing F_{p-1} actually involves guessing several primes and proofs of primality).

(4) g' is a generator of the (cyclic) group $\mathbb{Z}_p$ and $g'\leq p$. (We have the prime factorization of p-1 which allows for a fast confirmation of this.)

(5) $g \equiv (g')^{\frac{p-1}{b}} \bmod(p)$ and $g\leq p$ (by (2) $b|p-1$)

(6) $\alpha_i \equiv g^{a_i} \bmod(p)$ and $\alpha_i\leq p (1\leq i\leq n)$.

(7) pf_i proves p_i is prime, $1\leq i\leq n$.

(8) p_i is in the arithmetic progression $\{p+\alpha_i,2p+\alpha_i,\ldots\}$.

If any of these conditions fail to be confirmed then diverge. Otherwise, compute

$C = \prod_{i=1}^{n} p_i$ and output $<p,C>$."

That for any input at least one set of numbers exist which satisfy (1) - (8), has size no worse than quartic in the size of the input, and can be confirmed in polynomial time follows from elementary number theory, Pratt's results on primes [10], and the following deep result due to Linnik.

Theorem (Linnik (1940)) There exists a constant $c>0$ such that for all a,b relatively prime with $b<a$, there exists an $x \leq a^c$ such that $ax+b$ is prime. (Later results show that $c < 5000$).

Thus condition (1) of a γ-reduction holds.

That for any output <p,C>

$$(\exists x)[x\neq 0 \text{ and } px+1 \text{ divides } c]$$

$$\Leftrightarrow$$

$$(\exists S\subseteq\{1,2,\ldots,n\})(\exists m)[S\neq\phi \text{ and } \sum_{i\in S} a_i = mb]$$

follows from:

$$(\exists x)[x\neq 0 \text{ and } px+1 \mid c]$$

$$\Leftrightarrow$$

$$(\exists x)(\exists S\subseteq\{1,2,\ldots,n\})[S\neq\phi \text{ and } \prod_{i\in S} p_i = px+1]$$

$$\Leftrightarrow$$

$$(\exists S\subseteq\{1,2,\ldots,n\})[S\neq\phi \text{ and } \prod_{i\in S} p_i \equiv 1 \bmod(p)]$$

$$\Leftrightarrow$$

$$(\exists S\subseteq\{1,2,\ldots,n\})[S\neq\phi \text{ and } \prod_{i\in S} \alpha_i \equiv 1 \bmod(p)]$$

(by our selection of p_i, $p_i \equiv \alpha_i \bmod(p)$)

$$\Leftrightarrow$$

$$(\exists S\subseteq\{1,2,\ldots,n\})[S\neq\phi \text{ and } \prod_{i\in S} g^{a_i} \equiv 1 \bmod(p)]$$

$$\Leftrightarrow$$

$$(\exists S\subseteq\{1,2,\ldots,n\})[S\neq\phi \text{ and } \sum_{i\in S} a_i \text{ is a multiply of the order of } g \text{ in } \mathbb{Z}_p]$$

$$\Leftrightarrow$$

$$(\exists S \subseteq \{1,2,\ldots,n\})(\exists m)[S \neq \phi \text{ and } \sum_{i \in S} a_i = mb]$$

(since g was selected to have order b in $\mathbf{Z}_p$).

Thus condition (2) of a γ-reduction holds and multisack $\leq_\gamma$ linear divisibility.

Notice that there is probably no way to find the numbers used in this algorithm in deterministic polynomial time (as a polynomial reduction along these lines would demand). There is no reason to believe that we can factor numbers or find primes in arithmetic progressions in polynomial time. Further, without using the extended Riemann hypothesis (which we do not) there are no known polynomial time methods for determining if a number is prime or finding a generator in $\mathbf{Z}_p$.

That the binary quadratic diophantine equations problem is γ-complete follows from a slight modification of the proof above. The problem given in (4) of Theorem I has been studied by Plaisted [9]. Starting with his results its γ-completeness is easily proved.

III REDUCIBILITY AND RANDOMNESS

We are investigating the power of randomness. Are all sets in NP randomly decidable? To begin we give a more precise characterization of the randomly decidable sets due to Miller [8].

Def A set A is randomly decidable iff there is a non-deterministic Turing machine M and a polynomial p such that

$x \notin A \Rightarrow$ no computation path of machine M on input x halt

$x \in A \Rightarrow 1/2^{\dagger}$ of the computation paths of length $p(|x|)$ of machine M on input x halt.

Let R denote the class of randomly decidable sets. Clearly $P \subseteq R \subseteq NP$.

Theorem VI If A is NP-complete

$$R = NP \Leftrightarrow A \in R$$

Theorem VI follows because if $B \leq_p A$ and $A \in R$ then the deterministic machine which reduces B to A can be combined with the non-deterministic machine which randomly accepts A to yield a non-deterministic machine which randomly accepts B. However,

---

†If $1/2$ is replaced by any fixed fraction or any function of the form $\frac{1}{|x|^c}$ then the class defined remains the same.

the same argument can be made if B is γ-reducible to A, as long as the non-deterministic machine doing the reducing produces enough outputs -- call such a reduction a random-reduction (R-reduction). Then if for all $B \in NP$, $B \leq_R A$ it follows that $R = NP \Leftrightarrow A \in R$. *But notice A need not have been shown NP-complete.* Below we make this precise and outline a proof of theorem II.

For any sets A and B:

Def A is R-reducible to B ($A \leq_R B$) iff there is a non-deterministic Turing machine M which runs in polynomial time (in particular $p(|x|)$ time) such that:

(1) $(\forall x)$ [at least 1/2 of the computation paths of length $p(|x|)$ of machine M on input x halt (with outputs)].

(2) $(\forall x)(\forall y)[\langle x,y\rangle \in R_m \Rightarrow [x \in A \Leftrightarrow y \in B]]$.

Theorem VII $A \leq_p B \Rightarrow A \leq_R B \Rightarrow A \leq_\gamma B$

Def A set A is R-complete (random complete) iff

(1) $A \in NP$

(2) $(\forall B \in NP)[B \leq_R A]$.

Theorem VIII If A is R-complete then

$A \in R \Leftrightarrow NP = R$.

Cor If A is R-complete then $NP \neq R \Rightarrow A \notin P$.

Proof of Theorem II (Outline)

The γ-reducing machine in the proof of Theorem I is modified to reduce the knapsack problem to the set B and to guarantee that at least half of the paths converge. The following facts are essential:

Fact I: $(\forall K>2)$ [5 has order 2^{k-2} mod 2^k]

Fact II: There exists a rational $c>0$ such that for all $a,b \in \omega$, relatively prime with $b<a$, the proportion of primes in the set $\{a+b, 2a+b, \ldots, a^{50001}+b\}$ is at least $\frac{c}{\log(a)}$ †.

† Notice that the well-known asymptotic result for the distribution of primes in arithmetic progressions will not suffice in our proofs since our algorithms only guess primes in a fixed initial segment of arithmetic progressions. The fact stated here is not in any publication to our knowledge; however, its truth and provability have been attested to by knowledgable number theorist.

Fact III: (Miller [8]) extended Riemann hypothesis implies that primality is in P.

The following machine M, R-reduces knapsack to B (several details have been omitted for the sake of clarity):

"On input $\langle a_1, a_2, \ldots, a_n, b\rangle$

deterministically compute:

(1) the least $k \in \omega$ such that $2^{k-2} > \sum_{i=1} a_i + b$

(2) $\ell = \frac{kn}{c}$ (where c is as in Fact II)

(3) $\alpha_i = 5^{a_i} \pmod{2^k}$ and $\alpha_i < 2^k$ for $1 \leq i \leq n$

(4) $\beta = 5^b \pmod{2^k}$ and $\beta < 2^k$

non-deterministically guess:

$$\langle X_{11}, X_{12}, \ldots, X_{1,\ell}, X_{2,1}, X_{2,2}, \ldots, X_{2,\ell}, \ldots, X_{n,1}, X_{n,2}, \ldots, X_{n,\ell}\rangle$$

of length at most $\frac{k^4 n}{c}$ (where c is as in Fact II).

Deterministically compute:

$$p_{ij} = 2^k x_{i,j} + \alpha_i \quad 1 \leq i \leq n, \ 1 \leq j \leq \ell$$

deterministically confirm:

(a) For each i, $1 \leq i \leq n$ there is a $j, 1 \leq j \leq \ell$ such that p_{ij} is prime denote the 1st such prime p_i (use Fact III).

If (a) is not confirmed diverge. Otherwise, compute $L = \prod_{i=1}^{n} p_i$ and output $\langle K, \beta, L\rangle$."

The proof that M satisfies condition (2) in the definition of R-reducibility is along the same line as that used in Theorem I. That condition (1) holds is because Fact II and the selection of ℓ assure that the odds that condition (a) in the algorithm are not confirmed are less than 1/2. Put another way, there are so many primes in the progression $2^k x + \alpha_i$ and we have guessed so many candidates that we have probably hit one and in fact probably hit one for each i.

IV. TRACTIBILITY

Do randomly decidable sets conform to our intuitions about tractibility? One reason to think so is because the probability of hardware failure causing an incorrect answer from a "randomly computing" machine is far greater than the probability of it "lying".

One reason for doubt stems from mathematical considerations. Should a number theorist accept the assertion that a number is prime because the odds against the assertion being wrong are a million to one? On the other hand what if we had a deterministic Turing machine M with a random number generator which on any given input x

(1) halts within $p(|x|)$ steps (for some polynomial p independent of x),

(2) outputs "no" only when x is non-prime,

(3) outputs "yes" only when x is prime,

(4) outputs "?" with probability 1/1,000,000 (independent of x).

Then this machine's assertions would not be probabilistic, but certain. The sets A for which such machines exist are exactly those with $A \in R$ and $\overline{A} \in R$. We call such sets Δ-random and denote the class Δ^R. The Δ-random sets conform to our intuitions about tractibility; yet, it seems likely they form a proper super set of P. An example of a Δ-random set is given in the next theorem. It could well be that this set is in P but without extended Riemann hypothesis we have not been able to show it.

Theorem IX

$$C = \{x \mid x \in \omega \text{ and } x \text{ is prime and } (\exists y,z \in \omega)[x = y^z + 1 \text{ and } y < |x|]\} \in \Delta^R .$$

Proof

Fact I: It is easily seen that $\{x \mid x \in \omega$ and $(\exists y,z \in \omega)$ $[x = y^z + 1$ and $y < |x|]\} \in P$ and further in polynomial time y and z can be computed.

Fact II: Composites $\in R$.

Fact III: $\{\langle x,y,z,g\rangle \mid x = y^z + 1$ and $y < |x|$ and g is a generator of $\mathbb{Z}_x\} \in P$ this is because y is sufficiently small that it can be factored nievely.

From Facts I and II it follows that $\overline{C} \in R$. From Facts I and III, well known facts about primes, and a simple argument showing that if x is prime then $\mathbb{Z}_x$ has many generators it follows that $C \in R$.

In closing we point out that the proof of Theorem II supports the following (where B is as in Theorem II):

Theorem X [Assuming extended Riemann hypothesis]

$$B \in \Delta^R \Leftrightarrow \Delta^R = NP.$$

V. OPEN PROBLEMS

1. Show graph isomorphism is γ-complete.

2. Assuming NP≠P (and stronger assumptions if necessary) prove $X \leq_\gamma Y \not\Rightarrow Y \leq_p X$.

3. Are primes in Δ^R?

4. It is well known that the 0-degree of Turing reducibility is $RE \cap RE^C$ (i.e., the recursive sets). Post's problem was to prove the existence of a recursively enumerable set which was not recursive and not Turing complete. Such a set was exhibited in 1956 by Friedberg and Munchnik. However, there is no candidate for a "natural" set with these properties.

   On the other hand the 0-degree of polynomial reducibility is P but there are many candidates for sets in NP which are not in P and not NP-complete (e.g., linear programming, factoring).

   The 0-degree of γ-reducibility is $NP \cap NP^C$. However, we know of no candidates for a "natural" set which is in NP but which is not in $NP \cap NP^C$ and not γ-complete.

5. Analysze the degree structure of γ-reducibility (e.g., density, comparability,...) see Ladner [4].

6. Analyze the structure of γ-complete problems (e.g., with respect to polynomial isomorphism) see Hartmanis and Berman.

7. 5 and 6 for R-reducibility.

8. Remove the need for extended Riemann hypothesis in Theorem II.

ACKNOWLEDGMENT

The authors wish to thank Leonard Lipschitz for bringing the linear divisibility problem to their attention. Also Ron Rivest for several helpful ideas used in the proof of Theorem I.

REFERENCES

[1] Cook, S.A., "The Complexity of Theorem Proving Procedures", *Conf. Rec. 3rd ACM Symposium on Theory of Computing* (1971), 151-158.

[2] Gill, J., Computational Complexity of Probabilistic Turing Machines, *Conf. Records 6th ACM Symposium on Theory of Computing* (1974), pg. 91-95.

[3] Karp, R.M., "Reducibility Among Combinatorial Problems", *Complexity of Computer Computations*, eds. R.N. Miller and J.W. Thatcher, Plenum Press, 1972, pp.85-104.

[4] Ladner, R., "On the Structure of Polynomial Time Reducibility", *JACM* 22, 1 (Jan. 1975).

[5] Lipschitz, L., "A Remark on the Diophantine Problem for Addition and Division"

to appear.

[6] Lipschitz, L. private communications.

[7] Manders, K. and Adleman, L., "NP-Complete Decision Problems for Quadratic Polynomials", *Proceedings 8th Annual ACM Symposium on Theory of Computing* (1976), pp. 23-29.

[8] Miller, G.L., Riemann's Hypothesis and Tests for Primality, Ph.D. Thesis, Berkeley (1975).

[9] Plaisted, D.A., "Some Polynomial and Integer Divisibility Problems are NP-hard", Presentation at 17th Annual Symposium on the Foundations of Computer Science, pp. 264-267.

[10] Pratt, V. "Every Prime has a Succinct Certificate", *SIAM J. Comput. 4*, 3, pp. 214-220 (Sept. 1975).

[11] Rabin, M.O., "Probabilistic Algorithms" Algorithms and Complexity, New Directions and Recent Results, Edited by J. Traub, Academic Press.

[12] Strassen, V. and Solovay, R., "Fast Monte Carlo Tests For Primality" *SIAM J. on Computing*, to appear.