Electronic Colloquium on Computational Complexity, Report No. 93 (2008)

A simple constant-probability RP reduction from NP to $\oplus$P

Cristopher Moore
moore@cs.unm.edu
Department of Computer Science
University of New Mexico
and the Santa Fe Institute

Alexander Russell
acr@cse.uconn.edu
Department of Computer Science and Engineering
University of Connecticut

October 6, 2008

Abstract

The proof of Toda's celebrated theorem that the polynomial hierarchy is contained in $\mathrm{P}^{\#\mathrm{P}}$ relies on the fact that, under mild technical conditions on the complexity class $\mathcal{C}$, we have $\exists\mathcal{C} \subset \mathrm{BP}\cdot\oplus\mathcal{C}$. More concretely, there is a randomized reduction which transforms nonempty sets and the empty set, respectively, into sets of odd or even size. The customary method is to invoke Valiant's and Vazirani's randomized reduction from NP to UP, followed by amplification of the resulting success probability from $1/\mathrm{poly}(n)$ to a constant by combining the parities of $\mathrm{poly}(n)$ trials. Here we give a direct algebraic reduction which achieves constant success probability without the need for amplification. Our reduction is very simple, and its analysis relies on well-known properties of the Legendre symbol in finite fields.

Valiant and Vazirani [VV86] gave a clever randomized reduction from NP to UP, the class of promise problems which have either a unique solution or no solution at all. Their reduction works as follows. Given, say, a 3-SAT formula ϕ on n variables, we begin choose an integer k uniformly from $\{1,\ldots,n\}$. We then add the additional constraint that a hash function h takes the value zero, where h is chosen from a pairwise independent family of hash functions, and where a given truth assignment $\mathbf{x}$ obeys $h(\mathbf{x})=0$ with probability 2^{-k}. If ϕ is satisfiable, then with probability $\Omega(1/n)$ this additional constraint makes the solution unique.

So long as the complexity class $\mathcal{C}$ is expressive enough to compute the hash function h and is closed under intersection, this reduction asserts that:

$$\exists\mathcal{C} \subseteq \mathrm{RP}_{\mathrm{poly}}\cdot\exists!\mathcal{C}\,,$$

where $\mathrm{RP}_{\mathrm{poly}}$ denotes one-sided error with a $1/\mathrm{poly}(n)$ probability of success and where $\exists!$ denotes unique existence. Since 1 is odd, we can also write

$$\exists\mathcal{C} \subseteq \mathrm{RP}_{\mathrm{poly}}\cdot\oplus\mathcal{C}\,,$$

where, for instance, $\oplus$P is the class of decision problems which ask whether the number of witnesses for a problem in NP is odd.

For the case of $\oplus$P, we can amplify the probability of success as follows: if we perform $m=\Omega(n)$ independent trials of this reduction, then with probability $\Omega(1)$ at least one trial will yield a formula ϕ' with a unique solution (assuming ϕ is satisfiable). Since the expression

$$a = 1+\prod_{i=1}^{m}(a_i+1)$$

is odd if and only if at least one of the a_i is odd, and it is easy to implement such expressions within $\oplus$P by constructing m-tuples of witnesses, we conclude

$$\exists\,\mathrm{P} \subseteq \mathrm{RP}\cdot\oplus\,\mathrm{P}$$

ISSN 1433-8092

where now the reduction works with probability $\Omega(1)$. (Of course, by taking, say, $m = n^2$, we can make the probability of success exponentially close to 1.) By showing that the operators BP and $\oplus$ can be commuted, we obtain Toda's result [Tod91] that

$$\mathrm{PH} \subseteq \mathrm{BP} \cdot \oplus \mathrm{P} \subseteq \mathrm{P}^{\#\mathrm{P}} .$$

The purpose of this note is to give an alternate reduction from NP to $\mathrm{RP}^{\oplus\mathrm{P}}$ which works with constant probability without the need for amplification. Our reduction is quite simple, and may be of independent interest. First, let p be a prime, let $\mathbb{F}_p$ denote the field of order p, and for $a \in \mathbb{F}_p$ let $\chi(a)$ denote the Legendre symbol

$$\chi(a) = \begin{cases} 0 & \text{if } a = 0 \\ +1 & \text{if } a = b^2 \text{ for some } b \neq 0 \\ -1 & \text{otherwise} . \end{cases}$$

If p has $\mathrm{poly}(n)$ digits, then $\chi(a)$ can be computed in polynomial time as follows. Using modular exponentiation, calculate

$$t = a^{(p-1)/2} \bmod p .$$

Then $\chi(a) = +1$ or -1 if $t = 1$ or $p - 1 \equiv -1$ respectively.

Now consider the following theorem.

Theorem 1. *Let S be a nonempty subset of $\mathbb{F}_p$ of size $|S| = o(p^{1/2})$. If b is chosen uniformly at random from $\mathbb{F}_p$, then the set*

$$S' = \{x \in S \mid \chi(x + b) = -1\}$$

is of odd size with probability $1/2 - o(1)$.

Proof. First note that, with probability $1 - |S|/p = 1 - o(n^{-1/2})$, we have $x + b \neq 0$ for all $x \in S$. Henceforth we will assume that this is the case.

Then note that S' is of odd size if and only if

$$\prod_{x \in S} \chi(x + b) = -1 .$$

Since χ is a *multiplicative character*, i.e., since $\chi(ab) = \chi(a)\chi(b)$, we can write this as

$$\chi\left(\prod_{x \in S} (x + b)\right) = -1 .$$

Then

$$\Pr\left[|S'| \text{ is odd}\right] = \frac{1 - T}{2} \quad \text{where} \quad T = \mathbb{E}_b\, \chi\left(\prod_{x \in S} (x + b)\right) .$$

Now note that $\prod_{x \in S}(x + b)$ is a polynomial function of b. The expectation of a multiplicative character on the image of a polynomial on $\mathbb{F}_q$ is bounded by the following theorem, proved by A. Weil:

Theorem 2 ([Wei48])**.** *Let χ be a multiplicative character of $\mathbb{F}_p$ of order $m > 1$ (that is, m is the least integer for which $\chi(a)^m = 1$ for any a). Let $f(b) \in \mathbb{F}_p[x]$ be a polynomial that is not the mth power of a polynomial, and let d be the number of distinct roots of f in its splitting field over $\mathbb{F}_q$. Then*

$$\left| \sum_{b \in \mathbb{F}_p} \chi(f(b)) \right| \leq (d - 1)\, p^{1/2} .$$

In our case, $m = 2$ and $f(b) = \prod_{x \in S}(x + b)$. Since this product gives a complete factorization of $f(b)$ into distinct linear terms, $f(b)$ is certainly not the square of a polynomial. Moreover, it has degree $|S|$, so $d \leq |S| = o(p^{1/2})$. Therefore,

$$T = \frac{1}{p} \sum_{b \in \mathbb{F}_p} \chi(f(b)) = o(1)$$

and $|S'|$ is odd with probability $(1 - T)/2 = 1/2 - o(1)$. □

See also [LN97, §5] for further discussion.

Our reduction works as follows. For concreteness, suppose we have a 3-SAT formula ϕ on n variables. Choose a prime $p > 2^{cn}$ for some $c > 2$, so that $2^n = o(p^{1/2})$. Interpret each truth assignment $\mathbf{x}$ as an n-bit integer x, choose b uniformly from $\mathbb{F}_p$, and add the constraint that $\chi(x + b) = -1$. Then by Theorem 1, if ϕ is satisfiable, the resulting formula ϕ' will have an odd number of satisfying assignments with probability $1/2 - o(1)$.

References

[LN97] Rudolf Lidl and Harald Niederreiter. *Finite Fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, 1997.

[Tod91] Seinosuke Toda. PP is as hard as the polynomial-time hierarchy. *SIAM Journal of Computing*, 20(5):865–877, 1991.

[VV86] Leslie G. Valiant and Vijay V. Vazirani. NP is as easy as detecting unique solutions. *Theoretical Computer Science*, 47(3):85–93, 1986.

[Wei48] André Weil. On some exponential sums. *Proc. Nat. Acad. Sci.*, 34:204–207, 1948.

ECCC ISSN 1433-8092

http://eccc.hpi-web.de/