A Note On Enumerative Counting

Jin-yi Cai[1]
Lane A. Hemachandra[2]

February, 1990
Keywords: Computational Complexity, Theory of Computation

In this note we show the following theorem:

Theorem 1.1 *For any k, and an n^k-enumerator E (given a Boolean formula f, E prints out a list of n^k many numbers one of which is $\#f$), one can find $\#f$ in deterministic polynomial time relative to E. In particular, if an n^k-enumerator E exists in P, then $P = P^{\#P}$.*

The idea of enumerative counting was introduced in [CH89], where the above theorem was conjectured but left open. Instead, a weaker result was proved, namely if an $n^{1-\epsilon}$-enumerator exists in P, then $P = P^{\#P}$. This result has been extended by Amir, Beigel and Gasarch [ABG89]. They showed that if an n^k-enumerator exists then $BPP = P^{\#P}$. The above result will settle our original conjecture in [CH89].[3]

The proof is based on the newly developed idea of using polynomial interpolation for tree pruning, with which Lund, Fortnow, Karloff, and Nisan [LFKN89] and Shamir [Sha89] proved that the polynomial hierarchy and indeed even PSPACE have interactive proofs, and with which Babai, Fortnow, and Lund [BFL90] have shown that $\cup_{k>0}\mathrm{NTIME}[2^{n^k}]$ has two-prover interactive protocols, and Cai [Cai89] has shown that the polynomial hierarchy has two-prover one-round interactive protocols.

Our proof works as follows: Since the permanent function is hard for $\#P$, without loss of generality we assume that our n^k-enumerator E is given for the permanent; thus, for any integer matrix A of n bits, E gives a list of n^k-numbers one of which is $perA$, where k is some fixed integer. As the enumerator E gives some n^k possible values for $perA$, the task is to determine which value is the right one. Suppose our matrix A is $m \times m$. For some fixed constant d (independent of n), we will produce an $(m-1) \times (m-1)$ matrix, for which E gives up to n^d possible values and each of which, if it is correct, certifies exactly one of the claimed values for $perA$ is correct. Then by induction, the correct value of $perA$ will be computed.

We now proceed to the formal proof. Let us be given an $m \times m$ integer matrix $A = (a_{ij})$ of n bits, where perforce $|a_{ij}| \leq 2^n$, and $m^2 \leq n$. Clearly $perA$ is bounded by $n!(2^n)^n$, hence by Chinese Remainder Theorem and Prime Number Theorem, for any $c \geq 2$, the values $perA \bmod p$ for all the primes $n^c < p < n^{c+1}$ uniquely determine $perA$. (The exact value of c will be chosen later.) As there are at most a polynomial number of such primes and they are of $O(\log n)$ bits each, we have no problem checking the primality of all of them; thus we will just concentrate on getting $perA \bmod p$ for any fixed prime $n^c < p < n^{c+1}$ in polynomial time. (The reason for introducing primes and Chinese Remaindering is to make sure we don't have a blow-up in the size of the entries; this will become clear later on.)

Assume $m > 1$, and let $A[1|k]$ be the $(m-1) \times (m-1)$ submatrices obtained from A by striking out row 1 and column $k, 1 \leq k \leq m$. Now we view each matrix as a matrix over $\mathbf{Z}/p\mathbf{Z}$, i.e., we take a reduction modulo p. Let $A(x) = \sum_{k=1}^{m} e_k(x)A[1|k] \in M_{m-1}(\mathbf{Z}/p\mathbf{Z})[x]$ be a matrix polynomial, where

[1] Department of Computer Science, Princeton University, Princeton, NJ 08544.

[2] Department of Computer Science, University of Rochester, Rochester, NY 14627. Supported in part by the National Science Foundation under research grant CCR-8996198 and a Presidential Young Investigator Award.

[3] Seinosuke Toda has, independently, shown Theorem 1.1 as an extension of the work of Amir, Beigel, and Gasarch [Tod90].

$e_k(x) \in \mathbf{Z}/p\mathbf{Z}[x]$ are polynomials of degree at most $m-1$, such that $e_k(\ell) = \delta_{k\ell}$, for $1 \leq k, \ell \leq m$. Hence, $A(k) = A[1|k]$, and $per(A(k))$ is the kth permanental minor of A. Thus, $perA = \sum_{k=1}^{m} a_{1k} per(A(k))$. $p > m$, so polynomials $e_k(x)$ as described above can be chosen.

We would like to know the polynomial $p(x) = perA(x) \in \mathbf{Z}/p\mathbf{Z}[x]$, which is of degree at most $(m-1)^2$. Clearly the values of $p(x)$ at any $(m-1)^2+1$ points uniquely determine the polynomial itself. However, if we query E directly, we will get some n^k values for each point we query, and together they make up an exponential number of polynomials by interpolation.

We get around this problem by suitably combining the queries, and in effect, force the enumerator E to sort itself out consistently. Thus we consider the matrices $A(i) \in M_{m-1}(\mathbf{Z}/p\mathbf{Z})$, for $0 \leq i \leq (m-1)^2$. As $p > n^c \geq m^2$, these i are all distinct points in $\mathbf{Z}/p\mathbf{Z}$. Now we lift them back to the integers $\mathbf{Z}$, and form a single NP machine N, such that the number of accepting computation of N on 1^n is $\sum_{i=0}^{(m-1)^2} 2^{i \cdot n^2} \cdot perA(i)$. We note first that by lifting back to the integers, we can assume all the entries of $A(i)$ are nonnegative and bounded by $p < n^{c+1}$. Thus each permanent $perA(i)$ over $\mathbf{Z}$ is nonnegative and bounded by $(m-1)! \cdot (n^{c+1})^n < 2^{n^2}$, hence the values of these permanents can be read off easily from the number of accepting computation of N on 1^n. The construction of N can be easily carried out in polynomial time as follows: For each matrix, first guess a permutation, then multiply the entries on the "diagonal" given by the permutation, and generate the appropriate number of accepting paths. Finally the computation subtrees corresponding to each permanental matrices are combined to form the computation of N on 1^n.

To the machine N we apply Valiant's reduction from $\#P$ to the permanent function, and we get an integer matrix of n^ℓ bits, for some constant ℓ, and whose permanental value can be easily decoded to obtain the number of accepting computation of N on 1^n, which in turn, upon reduction modulo p, gives a tuple of values $p(i) = perA(i) \in \mathbf{Z}/p\mathbf{Z}$, for $0 \leq i \leq (m-1)^2$, which uniquely determines a polynomial $p(x) \in \mathbf{Z}/p\mathbf{Z}[x]$. Of course, we will query E, and we get instead a list of up to $n^{k\ell}$ polynomials in $\mathbf{Z}/p\mathbf{Z}[x]$, one of which is the right one $perA(x)$. Note that these polynomials are of degree at most $(m-1)^2 < n$, thus any two distinct polynomials can agree on at most n points. Now choose $c > 2k\ell+1$; then $n \cdot \binom{n^{k\ell}}{2} < n^c < p$, thus there exists a point $r \in \mathbf{Z}/p\mathbf{Z}$, such that no two of the $n^{k\ell}$ polynomials agree at r. This point can be found by exhaustive search in P. We note crucially that each value claimed by E for $perA(r)$ labels a unique polynomial $p(x)$ which certifies a unique value for the permanent of A: $perA = \sum_{i=1}^{m} a_{1i} p(i)$. If a particular value $p_0(r)$ is found to be the right value for $perA(r)$, this implies that all the other polynomials we obtained by interpolation are incorrect. Since E must be right on one of its answers to any query, the tuple that interpolates to $p_0(x)$ must be all correct, and thus $p_0(x)$ is the correct polynomial, and therefore the value $perA = \sum_{i=1}^{m} a_{1i} p_0(i)$ it certifies must be correct.

Now replace A by $A(r)$. The proof is completed by induction. We only need to note that each entry of $A(r)$ is bounded by p, without any blow-up in size.

References

[ABG89] A. Amir, R. Beigel, and W. Gasarch. Cheatable, P-terse, and P-superterse sets. Manuscript, December 1989.

[BFL90] L. Babai, L. Fortnow, and C. Lund. Non-deterministic exponential time has two-prover interactive protocols. Manuscript, January 1990.

[Cai89] J. Cai. The polynomial hierarchy is provable by two provers in one round. Manuscript, December 1989.

[CH89] J. Cai and L. Hemachandra. Enumerative counting is hard. *Information and Computation*, 82(1):34–44, July 1989.

[LFKN89] C. Lund, L. Fortnow, H. Karloff, and N. Nisan. The polynomial time hierarchy has interactive proofs (Note). Manuscript, 1989.

[Sha89] A. Shamir. IP=PSPACE. Manuscript, December 1989.

[Tod90] S. Toda, February 1990. Personal Communication.