CS6840: Advanced Complexity Theory Feb 14, 2012

Lecture 21 : Interactive protocol for permanent

Lecturer: Jayalal Sarma M.N. *Scribe: T Devanathan*

In the previous lecture, we introduced the following theorem

Theorem 1. $\mathsf{P}^{\#\mathsf{P}} \subseteq \mathsf{IP}$

To prove this theorem, we attempted come up with an IP for perm.
We take the discussion from the previous lecture further and try to come up with an Interactive Protocol for permanent of a matrix.

1 Interactive Protocol for Permanent

Let $A \in \{0,1\}^{n\times n}$ be a matrix. In the previous lecture, we discussed a basic IP where the prover first sends a claim q as $\mathsf{perm}(A)$ and subclaims $q_1, q_2, \ldots, q_n$ as the permanent of the minors of the first row of the matrix to the verifier. The verifier then does a basic consistency check of whether $q = \sum_{j=1}^{n} A_{ij} q_j$.
If the check fails, the verifier directly rejects.
If the check succeeds, it recursively gets claims for minors of each of the q_i.
The above IP failed as the verifier will take exponential time to run in this case. We also discussed a second possibility where the verifier randomly chooses a q_i and verifies it. But since the prover has to cheat in only one q_i to convince the verifier, it is with very low probability that the verifier will actually catch the q_i with the wrong value.

In this lecture, we try to come up with a better IP for permanent of matrix. We first consider a simpler case to get a better understanding.
Assume $n = 2$. The prover gives a claim q as $\mathsf{perm}(A)$ and subclaims q_1 and q_2 as $\mathsf{perm}(Z_1)$ and $\mathsf{perm}(Z_2)$ where Z_1 and Z_2 are minors of the two elements in the first row. Instead of verifying each of the matrices individually, we try and come up with a new matrix whose verification, with high probability, implies that both the sub-claims are correct. Consider the matrix
$D(x) = xZ_1 + (1-x)Z_2$.
We observe that each entry of $D(x)$ is a funciton of x. Also, $D(0) = Z_2$ and $D(1) = Z_1$.
Let $f(x) = \mathsf{perm}(D(x))$. $f(x)$ is a polynomial in x with a degree atmost n as the matrix $D(x)$ is $n \times n$.
The verifier asks the prover for $f(x)$. This is alright as the prover just has to give $n+1$ coefficients. If the prover cheats, it has to give a polynomial $f'(x)$ that has to satisfy the basic consistency check of $f'(0) = q_2$ and $f'(1) = q_1$.

Consider the polynomial $(f - f')(x)$. This is also a polynomial with a degree atmost n. Hence, it can atmost have n roots. In other words, $f(x)$ and $f'(x)$ can agree on only atmost n values. Since we are dealing with polynimials, we have work on a field. If S is the set on which we are working on, if we choose a $r \in_R S$, then
$\mathcal{P}(f'(r) = f(r)) \leq \frac{n}{|S|}$
Probability that prover is caught if prover cheats $\geq (1 - \frac{n}{|S|})$
By the above process, we have reduced two verifications to one with an additional error probability of only $\frac{n}{|S|}$.

We now try to reduce n claims using the above method to come up with a single matrix whose verification will, with high probability, verify the n individual claims.
Say we have $Z_1, Z_2, \ldots, Z_k$ as the k minors and $q_1, q_2, \ldots, q_n$ as their corresponding minors. We consider Z_1 and Z_2 and come up with a new matrix Z_{12} with a corresponding q_{12} upon whose verification, with high probability, we can consider Z_1 and Z_2 correct. We then consider Z_{12} and Z_3 to come up with Z_{123} and so on till we end up with just one matrix. In the whole of the above process, we encounter an error $\frac{(k-1)n}{|S|} \leq \frac{n^2}{|S|}$.
Now, we formally give the protocol for permanent of a matrix.
At stage k,

a) Prover sends the claim $q' = \mathsf{perm}(C)$ and subclaims $\{q_1, q_2, \ldots, q_n\}$ as the permanent of the minor of each element of the first row of C.

b) Verifier verifies if $q' = \sum_{j=1}^{n-k} C_{ij} q_j$.

c) If the minors Z_1, Z_2 are of the first two elements and l_1 and l_2 are the corresponding claims, prover sends a claim for
$\mathsf{perm}(xZ_1 + (1-x)Z_2)$.
Verifier checks consistency by checking if

   (a) $f(0) = l_2$
   (b) $f(1) = l_1$
   (c) Choose $r \in_R S$ and check if $C' = D(r)$ has $f(r)$ as its permanent.

$\vdots$

$n - k$ levels.

After $(n-k)$ levels, we will encounter an error of atmost $\frac{(n-k)n^2}{|S|}$.
$\Rightarrow$ The probability that the prover can convince the verifier of a wrong answer $\leq \frac{n^3}{|S|}$.
The error probability is not high as we can control the size of S. The above is an IP for permanent. Also note that in the above analysis, the minors $Z_1, Z_2, \ldots$ in stage k are not the minors of the original matrix itself.

2 Interactive Protocol for #SAT- A brief introduction

Consider a boolean equation ϕ and a claim q as the number of satisfying assignments. We arithmatize the boolean equation ϕ to an arithmetic expression $\tilde{\phi}$ using the following rules.

- $x_i \wedge x_j \rightarrow x_i x_j$
- $\sim x_i \rightarrow (1 - x_i)$
- By De-Morgan's law, $x_i \vee x_j = (1 - (1 - x_i)(1 - x_j))$

Following the above rules, we obtain the arithmetic expression $\tilde{\phi}$ where,

$$\#\phi = \sum_{x_n \in \{0,1\}} \sum_{x_{n-1} \in \{0,1\}} \cdots \sum_{x_1 \in \{0,1\}} (\tilde{\phi}) = q$$

Using the above construction, we come up with an Interactive Proof for #SAT.
The IP will be discussed in detail in the next lecture.