03684155: On the P vs. BPP problem. 22/1/2017 – Lecture 14b

Toda's theorem – Part II

Amnon Ta-Shma and Dean Doron

Last lecture we proved that $\mathsf{PH} \subseteq \mathsf{BPP}^{\oplus \mathsf{P}}$. Here we will prove that:

Lemma 1. $\mathsf{PP}^{\oplus \mathsf{P}} \subseteq \mathsf{P}^{\#\mathsf{P}}$.

As $\mathsf{BPP} \subseteq \mathsf{PP}$, both lemmas imply Toda's theorem, that $\mathsf{PH} \subseteq \mathsf{P}^{\#\mathsf{P}}$.

1 The class GapP

Definition 2. *The class* GapP *is the class of functions* f *such that for some* NP *machine* M, $f(x)$ *is the number of accepting paths minus the number of rejecting paths of* M *on* x.

GapP functions are closed under under exponential-size sums and polynomial-size products (we will see this in the exercise). Further:

Claim 3. $\#\mathsf{P} \subseteq \mathsf{GapP}$.

Proof. Given $f \in \#\mathsf{P}$ corresponding to an NP machine M, let N be the NP machine that on input x: Simulates $M(x)$. If it accepted, accept and otherwise branch to an accepting state and a rejecting one.

Let a and r be the number of accepting and rejecting paths of M on x. Thus, the number of accepting paths of N is $a+r$ and the number of rejecting paths of N is r. Thus, the GapP function corresponds to N is $(a+r)-r=a$, as desired. ☐

Claim 4. $\mathsf{FP}^{\mathsf{GapP}} = \mathsf{FP}^{\#\mathsf{P}}$.

Proof. (Sketch). The only direction left to prove is $\mathsf{FP}^{\mathsf{GapP}} \subseteq \mathsf{FP}^{\#\mathsf{P}}$. Let $L \in \mathsf{FP}^{\mathsf{GapP}}$ and assume it makes an oracle call to a function $f \in \mathsf{GapP}$. We will see in the exercise that every GapP function is a difference between a $\#\mathsf{P}$ function and an FP function. Thus, we can compute its output with an oracle to $\#\mathsf{P}$ and an FP computation. ☐

We have the following GapP characterization of $\oplus\mathsf{P}$:

Claim 5. *A language* L *is in* $\oplus\mathsf{P}$ *if and only if there is a* GapP *function* f *such that:*

- *If* $x \in L$ *then* $f(x) \equiv 1 \pmod 2$.
- *If* $x \notin L$ *then* $f(x) \equiv 0 \pmod 2$.

Proof. The left-to-right direction follows from Claim 3. For the other direction, consider such a GapP function with a corresponding NP machine M. Let N be the following NP machine: On input x, it branches twice, simulating $M(x)$ on one branch and $\overline{M}(x)$ on the other. Clearly,

$$\#acc_N(x) \;=\; acc_M(x) + rej_M(x) \;=\; (\#acc_M(x) - \#rej_M(x)) + 2 \cdot \#rej_M(x),$$

so if $x \in L$ then $\#acc_M(x) - \#rej_M(x)$ is odd and $acc_N(x)$ is odd as well, and if $x \notin L$ then $\#acc_M(x) - \#rej_M(x)$ is even and $acc_N(x)$ is even as well. Thus, $L \in \oplus\mathsf{P}$ due to the NP machine N. $\square$

2 Characterizing $\mathsf{PP}^{\oplus\mathsf{P}}$

We define PP^A using P^A predicates.

Claim 6. *A language L is in PP^A if and only if there is a language $B \in \mathsf{P}^A$ and a polynomial q such that:*

- *If $x \in L$ then*
$$\left|\left\{y \in \{0,1\}^{q(|x|)} : (x,y) \in B\right\}\right| \;\geq\; \left|\left\{y \in \{0,1\}^{q(|x|)} : (x,y) \notin B\right\}\right|$$
- *If $x \notin L$ then*
$$\left|\left\{y \in \{0,1\}^{q(|x|)} : (x,y) \in B\right\}\right| \;<\; \left|\left\{y \in \{0,1\}^{q(|x|)} : (x,y) \notin B\right\}\right|$$

Proof. The left-to-right direction follows immediately from the definition of PP. For the other direction, consider such a language B with a corresponding P^A machine $M(x,y)$. Let N be the NP^A machine that on input x, guesses $y \in \{0,1\}^{q(|x|)}$, simulates $M(x,y)$ and answers accordingly. The correctness easily follows. $\square$

Combining the above two claims, and the fact that $\mathsf{P}^{\oplus\mathsf{P}} = \oplus\mathsf{P}$ implied by what we did last lecture, we have:

Lemma 7. *A language L is in $\mathsf{PP}^{\oplus\mathsf{P}}$ if and only if there is a GapP function f and a polynomial q such that:*

- *If $x \in L$ then*
$$\left|\left\{y \in \{0,1\}^{q(|x|)} : f(x,y) \equiv 1 \pmod 2\right\}\right| \;\geq\; \left|\left\{y \in \{0,1\}^{q(|x|)} : f(x,y) \equiv 0 \pmod 2\right\}\right|$$
- *If $x \notin L$ then*
$$\left|\left\{y \in \{0,1\}^{q(|x|)} : f(x,y) \equiv 1 \pmod 2\right\}\right| \;<\; \left|\left\{y \in \{0,1\}^{q(|x|)} : f(x,y) \equiv 0 \pmod 2\right\}\right|$$

3 Proving $\mathsf{PP}^{\oplus\mathsf{P}} \subseteq \mathsf{P}^{\#\mathsf{P}}$

Our plan is to give a $\mathsf{FP}^{\mathsf{GapP}}$ algorithm to compute
$$\left|\left\{y \in \{0,1\}^{q(|x|)} : f(x,y) \equiv 1 \pmod 2\right\}\right|$$
and
$$\left|\left\{y \in \{0,1\}^{q(|x|)} : f(x,y) \equiv 0 \pmod 2\right\}\right|.$$
With that algorithm, we can prove $\mathsf{PP}^{\oplus\mathsf{P}} \subseteq \mathsf{P}^{\#\mathsf{P}}$.

Proof. Let $L \in \mathsf{PP}^{\oplus\mathsf{P}}$. By Lemma 7, there exists a GapP function f and a polynomial q such that:

- If $x \in L$ then
$$\left|\left\{y \in \{0,1\}^{q(|x|)} : f(x,y) \equiv 1 \pmod 2\right\}\right| \;\geq\; \left|\left\{y \in \{0,1\}^{q(|x|)} : f(x,y) \equiv 0 \pmod 2\right\}\right|$$
- If $x \notin L$ then
$$\left|\left\{y \in \{0,1\}^{q(|x|)} : f(x,y) \equiv 1 \pmod 2\right\}\right| \;<\; \left|\left\{y \in \{0,1\}^{q(|x|)} : f(x,y) \equiv 0 \pmod 2\right\}\right|$$

We compute in $\mathsf{FP}^{\mathsf{GapP}}$ the above two quantities, and decide accordingly. As $\mathsf{FP}^{\mathsf{GapP}} = \mathsf{FP}^{\#\mathsf{P}}$, $L \in \mathsf{P}^{\#\mathsf{P}}$. $\square$

So, fix a GapP function $f(x,y)$. Consider the polynomial $g(m) = 3m^2 - 2m^3$. One can verify that indeed:

Lemma 8. *For all m,*

1. *If $m \equiv 0 \pmod{2^j}$ then $g(m) \equiv 0 \pmod{2^{2j}}$.*
2. *If $m \equiv 1 \pmod{2^j}$ then $g(m) \equiv 1 \pmod{2^{2j}}$.*
3. *If $m \equiv 0 \pmod 2$ then $g^{(k)}(m) \equiv 0 \pmod{2^{2^k}}$.*
4. *If $m \equiv 1 \pmod 2$ then $g^{(k)}(m) \equiv 1 \pmod{2^{2^k}}$.*

Now, let $h(x,y) = g^{(1+\log q(|x|))}(f(x,y))$. As f is a GapP function, and GapP functions are closed under exponential-size sums and polynomial-size products, $h(x,y)$ is itself a GapP function. By the above lemma,

- If $f(x,y) \equiv 1 \pmod 2$ then $h(x,y) \equiv 1 \pmod{2^{q(|x|)+1}}$.
- If $f(x,y) \equiv 0 \pmod 2$ then $h(x,y) \equiv 0 \pmod{2^{q(|x|)+1}}$.

Define $r(x)$ as
$$r(x) \;=\; \sum_{y \in \{0,1\}^{q(|x|)}} h(x,y),$$
which is also a GapP function. We then have:
$$r(x) \bmod 2^{q(|x|)+1} \;=\; \left|\left\{y \in \{0,1\}^{q(|x|)} : f(x,y) \equiv 1 \pmod 2\right\}\right|$$
and
$$2^{q(|x|)} - \left(r(x) \bmod 2^{q(|x|)+1}\right) \;=\; \left|\left\{y \in \{0,1\}^{q(|x|)} : f(x,y) \equiv 0 \pmod 2\right\}\right|.$$
The above two computations can be done in $\mathsf{FP}^{\mathsf{GapP}}$, so we are done.