Today

- Arithmetic games on # accepting paths.
- Amplifying $\mathrm{BP} \cdot \bigoplus \cdot$P.
- $bp \cdot \bigoplus \cdot \mathsf{P} \subseteq \mathsf{P}^{\#\mathsf{P}}$.

Arithmetic games

- If non-deterministic machine M_1 on input w_1 has n_1 accepting paths, and M_2 on input w_2 has n_2 accepting paths, then can create machines + inputs that have n_1+n_2, or $n_1 \times n_2$ accepting paths.
- W.l.o.g. consider circuits. Have circuits C_1, C_2 ($C_i(\cdot) = M_i(w_i, \cdot)$) taking n-bit inputs and accepting n_1 and n_2 inputs respectively.
- Then, circuit C_3 given by $C_3(x, y) = C_1(x) \wedge C_2(x)$ accepts $n_1 n_2$ inputs.
- And, C_4 given by $C_4(x, b) = (b \wedge C_1(x)) \vee (\bar{b} \wedge C_2(x))$ has $n_1 + n_2$ accepting inputs.

More arithmetic

- Can also construction circuits with any fixed number of accepting inputs.
- So given any polynomial p with positive coefficients, and circuit C with N accepting inputs, can construct C' with $p(N)$ accepting inputs. Furthermore size of $C' = O(|p| \cdot |C|)$.
- If p is a constant degree polynomial with constant coefficients, can apply this process $O(\log n)$ times.

Will use the last parts later, but first show how to amplify.

Amplifying error

- For simplicity assume error is one-sided (this is essentially all we need to consider).
- Simple case: have a circuit $C(x, y)$. We are interested in $\mathrm{BP}_y\{\bigoplus_x\{C(x, y)\}\}$.
- Either for every y, $\bigoplus_x\{C(x, y)\} = 1$
  Or for $1/\mathrm{poly}(n)$ y's, $\bigoplus_x\{C(x, y)\} = 0$.
- New BP algorithm: Pick $y_1, \ldots, y_m$.
  Accept if $\wedge_{i=1}^m \left(\bigoplus_{x_i}\{C(x_i, y_i)\}\right)$.
  Eq'vly, if $\prod_{i=1} \left(\#_{x_i}\{C(x_i, y_i)\}\right)$ is odd.
- Good case: still accept w.p. 1.
  Bad case: accept w.p. $\leq (1-1/\mathrm{poly}(n))^m$.

Amplifying error (contd.)

- Slightly harder case:
- For $1/\text{poly}(n)$ y's, $\bigoplus_x \{C(x,y)\} = 1$.
  Or for every y, $\bigoplus_x \{C(x,y)\} = 0$
- Idea: Complement parities, take product, complement result.
- New algorithm: Pick $y_1, \ldots, y_m$. Accept if $1 + \prod_i (1 + \#_{x_i}\{C(x_i, y_i)\})$ is odd.
- Can construct $C'(x_1, \ldots, y_1, \ldots)$ accepting $1 + \prod_i (1 + \#_{x_i}\{C(x_i, y_i)\})$ inputs.
- Good case: accept w.p. $(1 - \text{poly}(n))^m$.
  Bad case: accept w.p. 0.

Amplification: final thoughts

- Strictly speaking, need to consider case where error is "almost one-sided" (e.g., accept w.p. $1 - exp(-n)$ vs. $1 - 1/\text{poly}(n)$.) But almost nothing changes.
- On the other extreme, one can do much more complex operations on $\bigoplus \cdot$P and stay within (and not just $\wedge$).

  Exercise: Show $\mathsf{P}^{\bigoplus \cdot \mathsf{P}} \subseteq \bigoplus \cdot$P.

Where are we?

- Showed yesterday $\Sigma_i^P \subseteq \text{BP} \cdot \bigoplus \cdot$P.
- By induction, $\Sigma_i^P \subseteq (\text{BP} \cdot \bigoplus)^i \cdot$ P.
- Also showed yesterday
  $\text{BP} \cdot \bigoplus \cdot \text{BP} \cdot \bigoplus \cdot$P $\subseteq \text{BP} \cdot \bigoplus \cdot$P.
- Another induction,
  $(\text{BP} \cdot \bigoplus)^i \cdot$ P $\subseteq \text{BP} \cdot \bigoplus \cdot$P.

Conclude: $\text{PH} \subseteq \text{BP} \cdot \bigoplus \cdot$P.

Next

Will show: $\text{BP} \cdot \bigoplus \cdot$P $\subseteq \mathsf{P}^{\#\mathsf{P}}$.

More clearly:

- Have circuit $C(x,y)$.
- Want circuit $C'(z)$ such that $\#_z(C'(z))$ allows us to compute $\text{BP}_y \{\bigoplus_x C(x,y)\}$.
- Assume BP_y gives right answer w.p. $\frac{3}{4}$.
- Will construct C' such that for every y:
  - $\#_x C'(x,y) = 0 \mod 2^{m+2}$ if $\#_x C(x,y) = 0 \mod 2$.
  - $\#_x C'(x,y) = -1 \mod 2^{m+2}$ if $\#_x C(x,y) = -1 \mod 2$.

- $\#_{x,y}C'(x,y) = ?$
  - $\in [-2^m, -\frac{3}{4}2^m]$ if $\mathrm{BP}_y\{\bigoplus_x C(x,y)\} = 1$.
  - $\in [-\frac{1}{4}2^m, 0]$ if $\mathrm{BP}_y\{\bigoplus_x C(x,y)\} = 0$.

Done, modulo construction of C'.

"Boosting" modular counts

- Suppose $a = b (\bmod\ 2^{2^c})$ for $b \in \{0, -1\}$.
- Then for $h(a) = 3a^4 + 4a^3$ have $h(a) = b (\bmod\ 2^{2^{c+1}})$.
- Let $h^{(i)}(a) = h(h^{(i-1)}(a))$, where $h^{(0)}(a) = a$.
- Let $t = O(\log m)$. Let C' be the circuit with $h^{(t)}(\#_x C(x,y))$ accepting inputs. (Can construct such C' in polynomial time.).
- C' is what we need.

QED. (Done with Toda's theorem.)

Polynomial magic=?

How would we come up with the polynomial h?

- Requirements:
  - $h(a) = b(\mod 2^{2^{c+1}})$ for $b \in \{0, -1\}$.
  - Coefficients of h non-negative.
- First condition says $a^2 | h(a)$ and $(a+1)^2 | h(a) + 1$. Natural choice (to make coeff. of a^1 disappear), $h_1(a) + 1 = (a+1)^2(a-1)^2 = a^4 - 2a^2 + 1$. Now have $h_2(a) = a^4 - 2a^2$. Satisfies first condition, but violates second.
- To make coefficients positive, add a (large multiple of) polynomial with +ve

coefficients that is 0 on a^2 and $(a+1)^2$. Simple choice $= a^2(a+1)^2$.

- New candidate $h_2(a) = h_1(a) + 2 \cdot a^2(a+1)^2 = 3a^4 + 4a^3$.