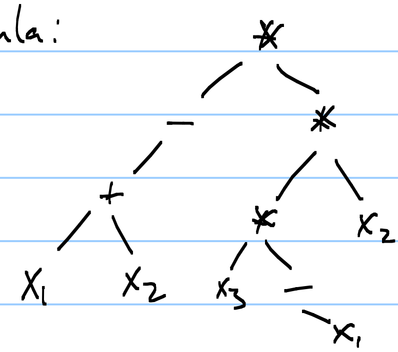
Randomness

Note Title 4/23/2013

We'll start our discussion about randomness and complexity with a couple of examples illustrating the use of randomness.

Polynomial Identity Testing:

Given a polynomial over a field as an arithmetic formula:
leaves are labeled w/ variables
internal nodes: $\underbrace{*}_{\deg 2}, +, \underbrace{-}_{\deg 1}$.



Is $p \equiv 0$?
is $p(\vec{x}) = 0 \quad \forall \; \vec{x} \in \mathbb{F}^n$ Assume $|F| >$ degree.

This is the same as polynomial identity testing
$$p = q \iff (p-q) \equiv 0.$$

One could try all $|F|^n$ inputs.
Or multiply it out symbolically to check that all the coefficients are 0 $\rightarrow$ (potentially an exponential # terms).
Randomness will help!

Lemma: (Schwartz-Zippel)
Let $p(x_1, \ldots, x_n)$ be a polynomial of degree d over field F.
$S \subseteq F$. Then if $p \neq 0$ then
$$\Pr_{r_1 \ldots r_n \in S}\left[p(r_1, \ldots, r_n) = 0\right] \leq d/|S|$$

Before we prove the theorem we'll show how to use it:
pick $S \subseteq F$ $|S| = 2d$.
pick $(r_1, \ldots, r_n) \in S^n$ at random

if $p(r_1, \dots, r_n) = 0 \Rightarrow$ output "yes"
if $p(r_1, \dots, r_n) \neq 0 \Rightarrow$ output "no".

if $p \equiv 0 \rightarrow$ always correct
if $p \neq 0 \rightarrow$ correct w.p. $\geq 1/2$

Pf of lemma: By induction on the # of variables

- $n = 1$: polynomial $p(x)$ of degree d has $\leq d$ roots.
  If we pick $S \subseteq F$ $|S| = 2d$.
  $$\Pr_r[p(r) = 0] \leq d/|S|$$

- Write $p(x_1, \dots, x_n) = \sum_i (x_1)^i \, \underbrace{p_i(x_2, \dots, x_n)}_{\text{degree} \leq d-i}$

  let $k = \max i$ s.t. $p_i(x_2, \dots, x_n) \neq 0$.
  $$\Pr[p_k(r_2, \dots, r_n) = 0] \leq \frac{d-k}{|S|}. \quad \text{(by induction)}$$

  If $p_k(r_2, \dots, r_n) \neq 0$ $p(x, r_1, \dots, r_n)$ is a univariate polynomial of degree k.
  $$\Pr[p(r_1, \dots, r_n) = 0 \mid p_k(r_2 \cdots r_n) \neq 0] \leq k/|S|.$$

$$\Pr[p(r_1, \dots, r_n) = 0] \leq \Pr[p_k(r_2, \dots, r_n) = 0] + \Pr[p(r_1, \dots, r_n) \mid p_k(r_2, \dots, r_n) \neq 0]$$
$$= \frac{d-k}{|S|} + \frac{k}{|S|}$$

$$\Pr[E] = \Pr[E \mid \cancel{E'}] \cdot \Pr[E'] + \Pr[E \mid \neg E'] \cdot \Pr[\cancel{\neg E'}]$$
$$\leq \Pr[E'] + \Pr[E \mid \neg E'].$$

Another example of the use of randomness.

A positive instance of SAT may have many solutions.
Does the difficulty arise from not knowing which one to work on?
Suppose we know that the # of satisfying assignments is 1 or 0. Can we determine which?
OR
Given an algorithm that can distinguish between one or 0 satisfying assignments, can we solve general instances efficiently?
→ Yes, but the only way we know how to do this is with a randomized reduction.

Theorem: Valiant-Vazirani
There is a randomized polynomial procedure that given a 3-CNF formula $\phi(x_1, x_2, \ldots, x_n)$, outputs a 3-CNF formula ϕ' such that
- if ϕ is not satisfiable then ϕ' is not satisfiable
- if ϕ is satisfiable then w.p. $\geq \frac{1}{8n}$, ϕ' has exactly one satisfying assignment.

Proof: Given $S \subseteq \{1, \ldots, n\}$ $\exists$ 3-CNF formula θ_S on $\{x_i \mid i \in S\}$ and possibly some additional variables such that
- θ_S is satisfiable iff an even # of variables in $\{x_i\}_{i \in S}$ are true
- For each such assignment of the x_i variables there is a unique satisfying assignment (i.e. setting of the auxiliary variables is determined).

Also $|\theta_S|$ is $O(n)$

$$S = x_{i_1} \cdots x_{i_k}$$

Here's a sketch of how you would construct θ_S:

$y_j = 1$ if # of 1's in $x_{i_1} \dots x_{i_j}$ is even

$y_0 = 1$

$$\begin{aligned} &(y_0) \\ \wedge \; &(x_{i_{j+1}} \to y_j \neq y_{j+1}) \\ \wedge \; &(\neg x_{i_{j+1}} \to y_j = y_{j+1}) \\ &\vdots \\ &(y_k) \end{aligned}$$

Here's the overall construction:

$\phi_0 = \phi \leftarrow$ the original formula:

for $i = 1, \dots, n$

pick a random subset S_i of $\{1, \dots, n\}$

$\phi_i = \phi_{i-1} \wedge \theta_{S_i}$

Output random ϕ_k $k \in \{1, \dots, n\}$

Claim if $|T| > 0$ then

$$\Pr_{k \in \{0, \dots, n-1\}} [2^k \leq |T| < 2^{k+1}] \geq 1/n.$$

probability we pick the correct ϕ_k

Claim if $2^k \leq |T| \leq 2^{k+1}$ then the probability that ϕ_{k+2} has exactly one satisfying assignment is $\geq 1/8$.

prob of success given the correct ϕ_k is chosen.

$\hookrightarrow$ prob of success: $1/8n$.

Fix t & $t' \in T$

$$\Pr[t \text{ and } t' \text{ agree on } \theta_{S_i}] = 1/2$$

Consider a string where position i is 0 iff t & t' agree on x_i and is 1 otherwise.

t & t' agree on θ_{S_i} iff S_i contains an even # 1's

$$\Pr[t \text{ satisfies } \theta_{S_i}] = 1/2$$

Note: we need to assume that $x_i = 0 \; \forall i$ does not satisfy ϕ. This can be checked before the reduction.

Also these two events are independent.

Note that we only have and only need pairwise independence.

$$\Pr\left[t \text{ satisfies } \Theta_{S_i} \wedge t' \text{ satisfies } \Theta_{S_i} \right] = 1/4$$

Consider a location ℓ where t + t' differ.
Say $t_\ell = 0$ + $t'_\ell = 1$.
There also has to be a location k where $t_k = 1$. We have:

	ℓ	k
t	0	1
t'	1	0/1

Regardless of whether $t'_k = 0$ or 1, When we consider the 4 possibilities whether $\ell, k \in S_i$.

This generates all four possible cases for whether t and or t' satisfy Θ_{S_i}

Since the S_i are independent from each other, we have

$$\text{Prob}\left[t \text{ and } t' \text{ both satisfy } \phi_{k+2} \right] = \left(\frac{1}{4}\right)^{k+2}$$

$$\text{Prob}\left[t \text{ uniquely satisfies } \phi_{k+2} \right] =$$

$$\text{Prob}\left[t \text{ satisfies } \phi_{k+2} \right] - \left(|T|-1\right) \text{Prob}\left[t + t' \text{ both satisfy } \phi_{k+2} \right]$$

$$\geq \left(1/2\right)^{k+2} - \frac{2^{k+1}}{4^{k+2}} = \left(\frac{1}{2}\right)^{k+2}\left(1 - 1/2\right) = \frac{1}{2^{k+3}}$$

$$\text{Prob}\left[\exists\, t \text{ which uniquely satisfies } \phi_{k+2} \right] \geq \frac{2^k}{2^{k+3}} = \frac{1}{8}.$$