Cryptographic Protocols

Spring 2021

Part 2

Polynomial, Negligible, Noticeable

Function $f : \mathbb{N} \to \mathbb{R}$

- f is polynomial $\Leftrightarrow$ $\exists c\ \exists n_0 \forall n \geq n_0 :\ f(n) \leq n^c$
- f is negligible $\Leftrightarrow$ $\forall c\ \exists n_0 \forall n \geq n_0 :\ f(n) \leq \frac{1}{n^c}$
- f is noticeable $\Leftrightarrow$ $\exists c\ \exists n_0 \forall n \geq n_0 :\ f(n) \geq \frac{1}{n^c}$
- f is overwhelming $\Leftrightarrow$ $1-f$ is negligible

Implications

- poly $\times$ poly = poly; poly(poly) = poly
- poly $\times$ negligible $\subseteq$ negligible
- (poly $\times$ noticeable) $\cap$ overwhelming $\neq$ $\{\}$

P, NP, PSPACE, etc.

Running Time of a Turing machine (TM, aka algorithm)

- for input z: number of steps $s(z)$
- for n-bit input: $t(n) :=$ max$\{s(z) : |z| \leq n\}$ (worst-case)
- TM is poly-time iff $t(n)$ is a polynomial function

Complexity Classes

- P $= \{L : \exists$ poly-time TM that decides $L\}$
- NP $= \{L : \exists$ poly p $\exists$ poly comp. $\varphi : \{0,1\}^* \times \{0,1\}^* \to \{0,1\}$
  s.t. $z \in L \Leftrightarrow \exists x\ (\varphi(z,x) = 1\ \wedge\ |x| \leq p(|z|))\ \}$
  (also: NP $= \{L : \exists$ non-det. poly-time TM that accepts $L\}$)
- NP-hard $= \{L : \forall L' \in$ NP: accepting L' can be poly reduced to $L\}$
- NP-Complete $=$ NP $\cap$ NP-hard
- PSPACE $= \{L : \exists$ TM that accepts L with poly memory (in any time)$\}$

Interactive Proofs of Statements

Def: An interactive proof for language L is a pair (P,V) of int. programs s.t.

i) running time of V is polynomial in $|z|$
ii) $\forall z \in L$: Pr((P(z) $\Leftrightarrow$ V(z)) $\to$ "accept") $\geq 3/4$ $[p = 3/4]$
iii) $\forall z \notin L, \forall$P' : Pr((P'($z$) $\Leftrightarrow$ V(z)) $\to$ "accept") $\leq 1/2$ $[q = 1/2]$

Examples: Sudoku, GI, GNI, Fiat-Shamir.

Remarks

- Constants p, q are arbitrary, could be $p = 1-2^{-|z|}$ and $q = 2^{-|z|}$
- However: only NP-languages have proofs with $q = 0$
- If iii) holds only for poly-time P': interactive argument (not a proof)
- Probabilistic P are not more powerful than deterministic P

Def: IP = set of L which have an interactive proof.

Theorem: IP $=$ PSPACE.