

# Introduction to Computational Complexity

Lance Fortnow  
Notes(15-2-2008) by Ramanathan Narayanan

Homework 4 Posted. Due on Friday, Feb 22, 2008

- Randomized Computation

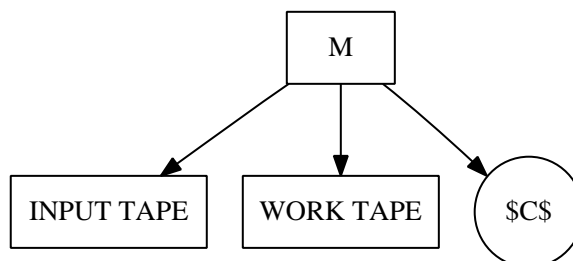


Figure 1. Randomized Turing Machine

- Fermat's Little Theorem: If  $p$  is prime and  $1 \leq a \leq p - 1$ ,  $a^p \equiv a \pmod{p}$
- $S_m = \{a \mid a^p \equiv a \pmod{m}\}$  is a sub group of  $Z_m^*$   
 $(ab)^p \pmod{m} = (a^p \pmod{m} b^p \pmod{m}) \pmod{m}$   
 $= (a \pmod{m} b \pmod{m}) \pmod{m}$   
 $= (ab) \pmod{m}$
- Algorithm:

```
Input m:  
i = 0  
while i ≤ N do  
  if  $a^m \equiv a \pmod{m}$  then  
    output composite  
  else  
    output likely-prime  
  end if  
end while
```

- In above algorithm, if  $m$  is prime, the algorithm always outputs 'likely-prime'  
 If  $m$  is composite, then  $P(\text{Algorithm outputs composite}) \geq 1 - 2^{-100}$   
 Carmichael numbers are composites such that  $a^m \equiv a \pmod{m}$  for all  $a$   
 So above algorithm will not work

- Miller-Rabin Test

```

Input  $m$ 
if  $m = 2$  then
    output prime;
else if  $m > 2$  and  $m$  is even then
    output composite;
else
    Let  $m - 1 = 2^S d$ , where  $d$  is odd
     $i = 0$ 
    while  $i < N$  do
        Pick random  $a$ 
        if  $a^m \equiv a \pmod{m}$  then
            output composite;
        end if
        if  $\forall 0 \leq i \leq S, a^{2^i d} \equiv -1 \pmod{m}$  then
            output composite;
        end if
    end while
end if

```

- Agrawal, Kayal, Saxena (2002) : "Primes in P"

```

Input:  $m > 2$ 
if  $m = a^b$  for  $b > 1, a > 0$  then
    output composite;
else
    Find smallest  $r$  such that  $O_r(m) > \log^2(m)$ 
    if  $\exists a \leq r, \gcd(a, m) \neq 1$  then
        output composite;
    else if  $m \leq r$  then
        output prime;
    end if
    flag = false
    for  $a = 1$  to  $\sqrt{\Phi(r)}$  do
        if  $(x + a)^m \not\equiv x^m + a \pmod{(x^r - 1, m)}$  then
            flag = true
            output composite;
        end if
    end for

```

```

if flag = false then
    output prime;
end if
end if

```

- Algebraic circuit: Function built up with +, -, \*  
 Problem: Find if algebraic circuit is “identically zero” eg.  $(x + y)^*z - x^*z - y^*z \equiv 0$ 
  - Pick Random inputs for variables
  - Evaluate circuit
  - If zero output “identically zero” else output “not zero”

- Schwartz-Zippel

$P(X_1, X_2, \dots, X_n)$  is a polynomial in  $n$  variables, degree  $d$  over some field  $F$ ,  $P \neq 0$   
 $S \subseteq F$

Claim:  $\Pr_{a_1, a_2, \dots, a_n \in S}(P(a_1, a_2, \dots, a_n) = 0) \leq \frac{d}{|S|}$

- Proof: Induction over  $n$

Base case: If  $n = 1$ ,  $\Pr_{a \in S}(P(a) \neq 0) \leq \frac{d}{|S|}$

Suppose it is true for  $n$

Then we need to find  $\Pr_{a_i \in S}(P(a_1, a_2, \dots, a_{n+1}) = 0)$  Let  $B$  be event that  $P(a_1, a_2, \dots, a_{n+1}) = 0$

$P(X_1, X_2, \dots, X_{n+1}) = \sum_{j=0}^d X_{n+1}^j P_j(X_1, X_2, \dots, X_n)$

Let  $k$  be the max degree such that  $P_k X_1, X_2, \dots, X_n \neq 0$

$A =$  event that  $P_k a_1, a_2, \dots, a_n = 0$

$\Pr(B) = \Pr(B/A) \Pr(A) + \Pr(B/\bar{A}) \Pr(\bar{A})$

$\leq \Pr(A) + \Pr(B/\bar{A})$

$\leq \frac{d-k}{|S|} + \frac{k}{|S|} = \frac{d}{|S|}$