CS760 Topics in Computational Complexity 13 August 2024

Lecture 4: PRIMES $\in$ NP; NTM definition of NP

Lecturer: Prof. Rohit Gurjar *Scribe: Arnav (210050018)*

1 Proof of Pratt's Theorem

1.1 Lucas' Primality Test

Theorem 1.1. *p is prime iff $\exists z$*

- $z^{p-1} \equiv 1 \pmod{p}$ *and*
- $\forall r < p-1 : z^r \not\equiv 1 \pmod{p}$

The latter condition is equivalent to

$$\text{for each prime factor } q \text{ of } p-1,\ z^{(p-1)/q} \not\equiv 1 \pmod{p}$$

(since if for some $r < p-1$ we have $z^r \equiv 1 \pmod{p}$ then $r|(p-1)$ and thus (since $r < (p-1)$) for some prime factor q of $p-1$, $r|\frac{p-1}{q}$ and hence $z^{(p-1)/q} \equiv 1 \pmod{p}$)

1.2 Proof of Lucas' Primality Test

Claim 1.2. *If p is prime then $\forall z \not\equiv 0 \pmod{p}$ we have $z^{p-1} \equiv 1 \pmod{p}$.*

Proof. We work in $\mathbb{Z}_p$. We first note that since $z \not\equiv 0$,

$$\{z \cdot i | i \in \mathbb{Z}_p\} = \mathbb{Z}_p$$

(If possible let $a \not\equiv b$ be st $za \equiv zb \implies z(a-b) \equiv 0 \implies a - b \equiv 0$ since $z \neq 0$, a contradiction!)

Now consider $y = z^{p-1} \cdot 1 \cdot 2 \cdot 3 \cdot (p-1)$. By the above result we must have

$$z^{p-1} \cdot 1 \cdot 2 \cdot 3 \cdot (p-1) \equiv 1 \cdot 2 \cdot 3 \cdot (p-1)$$

Since, $1 \cdot 2 \cdot 3 \cdot (p-1) \not\equiv 0$ and p is prime, hence it has a multiplicative inverse in $\mathbb{Z}_p^*$. Thus we conclude that

$$z^{p-1} \equiv 1$$

■

Claim 1.3. *If p is prime then $\forall z \not\equiv 0 \pmod{p}$ and $k \geq 1$, we have $z^{p^{k-1}(p-1)} \equiv 1 \pmod{p^k}$*

Proof. We proceed by induction.

Base case $k = 1$**:** Proven above

Inductive step $k \geq 2$**:** If possible let $k \geq 2$ be such that

$$z^{p^{k-2}(p-1)} \equiv 1 \pmod{p^{k-1}}$$

Then $z^{p^{k-2}(p-1)} = 1 + mq^{k-1}$ and

$$\begin{aligned} z^{p^{k-1}(p-1)} &= \left(1 + mp^{k-1}\right)^p \\ &= 1 + \sum_{i=1}^{q-1} \binom{p}{i} m^i p^{i(k-1)} + m^p p^{p(k-1)} \end{aligned}$$

Note that in each term of the sum, power of p is $\geq k$. Thus for some m'

$$z^{p^{k-1}(p-1)} = 1 + m'p^k$$

and we get $z^{p^{k-1}(p-1)} \equiv 1 \pmod{p^k}$.

Thus by principal of mathematical induction, the assertion holds for all $k \geq 1$. ■

Now we prove one direction of the statement.

Theorem 1.4. *If q is not prime then for all z there exists $r < q - 1$ such that*

$$z^r \equiv 1 \pmod{q}$$

Proof. Let q have a prime factorisation $p_1^{n_1} p_2^{n_2} \dots p_k^{n_k}$. Then we have for each z

$$\begin{aligned} z^{p_i - 1} &\equiv 1 \pmod{p_i} \\ \implies z^{p_i^{n_i - 1}(p_i - 1)} &\equiv 1 \pmod{p_i^{n_i}} \\ \implies z^{\prod_{i=1}^{k} p_i^{n_i - 1}(p_i - 1)} &\equiv 1 \pmod{p_i^{n_i}} \end{aligned}$$

and since all the $p_i^{n_i}$'s are coprime, we then get

$$z^{\prod_{i=1}^{k} p_i^{n_i - 1}(p_i - 1)} \equiv 1 \pmod{q}$$

Exponent on LHS is $< q - 1$ for composite q, so we are done. ■

Let $O_p(z)$ represent the smallest nonzero power (order) of z that is $\equiv 1 \pmod{p}$.

Claim 1.5. *For prime p, if we have z_1, z_2 st $r_1 = O_p(z_1), r_2 = O_p(z_2)$ with $\text{GCD}(r_1, r_2) = 1$ then $O_p(z_1 z_2) = r_1 r_2$.*

Proof. By definition of order we must have $(z_1 z_2)^{r_1 r_2} \equiv 1 \pmod{p}$.

If possible let $\exists r, 0 < r < r_1 r_2$ st $(z_1 z_2)^r \equiv 1 \pmod{p}$.

Let us write

$$r = m_1 r_1 + n_1 = m_2 r_2 + n_2$$

for some $0 \leq n_1 < r_1, 0 \leq n_2 < r_2$.

Now n_1 and n_2 can't both be zero since $\text{GCD}(r_1, r_2) = 1$. If $n_1 = 0$ then $1 \equiv (z_1 z_2)^r \equiv z_2^{n_2} \pmod{p}$, a contradiction since $n_2 < r_2$. So we must have $n_1 > 0, n_2 > 0$.

Thus

$$z_1^{n_1} z_2^{n_2} \equiv 1 \pmod{p}$$

Raising to r_1, we get

$$\begin{aligned} & z_1^{n_1 r_1} z_2^{n_2 r_1} \equiv 1 \pmod{p} \\ \implies & z_2^{n_2 r_1} \equiv 1 \pmod{p} \end{aligned}$$

Thus we must have $r_2 | n_2 r_1$, and since r_1, r_2 are coprime,

$$r_2 | n_2$$

which is a contradiction since $0 < n_2 < r_2$. Hence $O_p(z_1 z_2) = r_1 r_2$. ■

Claim 1.6. *For prime p, let r be the maximum order among elements of $\mathbb{Z}_p^*$. Then*

$$\forall z,\ z^r \equiv 1 \pmod{p}$$

Proof. Let z be such that $O_p(z) = r$.

If possible let there be a z' with order $r' < r$ st $z^r \not\equiv 1 \pmod{p}$.

Let $w = \text{GCD}(r, r')$. Let $\tilde{r} = \frac{r'}{w}$ ($\tilde{r} > 1$ since $r' < r$). Then we must have $\text{GCD}(r, \tilde{r}) = 1$.

Consider $\tilde{z} = z'^w$. Then $O_p(z) = r, O_p(\tilde{z}) = \tilde{r}$. Thus using the preceding result,

$$O_p(z\tilde{z}) = r\tilde{r} > r,$$

a contradiction. Hence the assertion holds. ■

Now we prove the reverse direction.

Theorem 1.7. *If p is prime, $\exists\, z\, O_p(z) = p - 1$.*

Proof. Let r be the maximum order among elements of $\mathbb{Z}_p^*$. Then the polynomial $z^r - 1$ has at most $p - 1$ distinct roots. Hence $r \geq p - 1$. We also know that order $\leq p - 1$. Hence $r = p - 1$ and thus some element of $\mathbb{Z}_p^*$ has order $p - 1$. ■

1.3 Proof of size of certificate

For a prime p, the Pratt certificate lists the prime factors of $p-1$ and the witness z that satisfies Lucas' test for p. Adjoined to this are the certificates for the listed prime factors (2 is a special case and does not require a certificate).

Theorem 1.8. *The Pratt certificate for a prime p is of size $\mathcal{O}(\log_2(p))$.* [1]

2 Nondeterministic Turing Machines and NP

Definition 2.1. *A Nondeterministic Turing Machine is a tuple $N = \langle Q, \Gamma, b, \Sigma, \delta, q_0, F\rangle$ where*

- *Q is a finite non-empty set of states,*
- *Γ is a finite non-empty set of tape symbols,*
- *$b \in \Gamma$ is the blank symbol,*
- *$\Sigma \subseteq \Gamma \setminus b$ is the set of input symbols,*
- *$q_0 \in Q$ is the initial state,*
- *$F \subseteq Q$ is the set of accepting states, and*
- *$\delta : (Q \setminus F) \times \Gamma \to \mathcal{P}(Q \times \Gamma \times \{L, R\})$ is the transition function.*

Here the function δ takes the current state and the current tape symbol and outputs a set *of possible transitions. Each possible transition describes the new state, the new symbol written at the head, and the movement of the head. At any step, the non-deterministic TM can choose any transition from the set of transitions given by δ. That means for a given input an NTM has multiple possible computation paths (possibly exponential in the number of steps).*

A language $L \subseteq \Sigma^*$ is said to be accepted by an NTM N when

$$x \in L \iff \exists \text{ computation path in } N \text{ with input } x \text{ halting in } F$$

An NTM N is said to be polytime if $\exists$ polynomial $p : \mathbb{N} \to \mathbb{N}$ such that for all inputs x, N halts in at most $p(|x|)$ steps on all computation paths.

Theorem 2.2. *A language $L \subseteq \{0,1\}^*$ is in NP iff there exists a polytime NTM N accepting L.*

Proof. $\underline{L \in \mathsf{NP} \overset{?}{\implies} \exists\, N}$ Since $L \in \mathsf{NP}$, there exists verifier DTM V and a polynomial bound q on size of the certificate. We construct an NTM N that on input x does the following:

1. N first nondeterministically writes a size $q(|x|)$ certificate to the tape.

[1] Pratt, V. R. (1975) 'Every Prime Has A Succint Certificate', *SIAM Journal on Computing*, 4(3)

2. Then it runs V on the resulting tape.

The first step takes time $\mathcal{O}(q(|x|))$.

If $x \in L$, then for some $c \in \{0,1\}^{q(|x|)}$, V will halt and accept in polynomial time by definition. Thus N is a polytime NTM accepting L.

$\underline{\exists\, N \overset{?}{\implies} L \in \mathsf{NP}}$ Let p be the polynomial bounding the number of transitions taken by polytime NTM N for any accepted input.

For an input $x \in L$, consider the accepting run of N. This can be encoded as a sequence of choices made, one at each transition, by N. Let us encode this in $\{0,1\}^*$ as c; it will have size $p(|x|)$ with appropriate padding.

Now we construct a DTM V that takes an input x and a certificate c and simulates N on the input x until atmost $p(|x|)$ steps, taking a single transition at each step according to what is encoded in c (if encoding is invalid or N halts then V halts and rejects).

If $x \in L$ then using the certificate described before, V halts and accepts in polynomial time in $|x|$.

OTOH if $x \notin L$ then there cannot be an accepting run in N, so no certificate can cause V to halt and accept.

■