

coNP

Guan-Shieng Huang

Nov. 22, 2006

coNP

- A problem is in coNP iff its complement is in NP.
- The complement of a decision problem is to interchange the “yes” / “no” answer for each instance with respect to the membership problem.
- Let A be a problem in NP. Then any positive instance of A has a succinct certificate.
- Let B be a coNP problem. Then any negative instance of B has a succinct disqualification.

Validity

Given a Boolean formula represented in conjunctive-normal form, is it true for all truth assignments?

This problem is coNP-complete.

That is, any coNP problem can reduce to Validity.

- F is valid iff $\neg F$ is unsatisfiable.
- The complement of “ $\neg F$ is unsatisfiable” is “ $\neg F$ is satisfiable.”
It is indeed the SAT problem.
- Since SAT is NP-complete, any coNP problem can reduce to coSAT.

Proposition 10.1

If L is NP-complete, then its complement $\bar{L} = \Sigma^* - L$ is coNP-complete.

Proof.

We have to show that any problem L' in coNP can reduce to \bar{L} .

- \bar{L}' is in NP.
- \bar{L}' can reduce to L . That is, $x \in \bar{L}'$ iff $R(x) \in L$.
- The complement of \bar{L}' can reduce to \bar{L} since $x \notin \bar{L}'$ iff $R(x) \in \bar{L}$.
- That is, \bar{L}' can reduce to \bar{L} by the same reduction from \bar{L}' to L .

Open Question

$NP=coNP?$

If $P=NP$, then $NP=coNP$. ($NP=P=coP=coNP$)

However, it is also possible that $NP=coNP$, even $P \neq NP$.

Proposition 10.2

If a coNP-complete problem is in NP, then $\text{NP}=\text{coNP}$.

Proof.

Let L be the coNP-complete problem that is in NP.

1. $\text{coNP} \subseteq \text{NP}$:

Since any $L' \in \text{coNP}$ can reduce to L and L is in NP, we have L' is in NP.

2. $\text{NP} \subseteq \text{coNP}$:

For any $L'' \in \text{NP}$, asking “whether $x \notin L''$ ” is in coNP. This problem can reduce to L since L is coNP-complete. Thus, asking whether $x \in L''$ can reduce to the complement of L , which is in coNP.

Example 10.2

PRIMES: Determines whether an integer N given in binary is a prime number.

It is easy to see that PRIMES is in coNP since COMPOSITE is in NP.

Notations

- $x|y$ if there is a whole number z with $y = xz$.
- $x \nmid y$ iff it is not the case for $x|y$.
- $a \equiv b \pmod{n}$ iff $n|(a - b)$.
(9 \equiv 14 (mod 5))
- $a \equiv a \pmod{n}$. (reflexive)
- $a \equiv b \pmod{n}$ implies $b \equiv a \pmod{n}$ (symmetric)
- $a \equiv b$ and $b \equiv c$ implies $a \equiv c \pmod{n}$ (transitive)
- If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then
 1. $a + c \equiv b + d \pmod{n}$
 2. $a - c \equiv b - d \pmod{n}$
 3. $a \cdot c \equiv b \cdot d \pmod{n}$
- If $a \equiv b \pmod{n}$, then $ac \equiv bc \pmod{n}$ for any c .

- If $ac \equiv bc \pmod{n}$ and c and n are relatively prime, then we can conclude that $a \equiv b \pmod{n}$. (cancellation rule)

Historic Events

- Euclid: There are infinite primes.
- (1974) Pratt: $\text{PRIMES} \in \text{NP}$
 $\Rightarrow \text{PRIMES} \in \text{NP} \cap \text{coNP}$
- (1975) Miller: deterministic polynomial time based on Extended Riemann's Hypothesis
(ERH: The first quadratic nonresidue mod p of a number is always less than $3(\ln p)^2/2$, from MathWorld.)
- (1977) Solovay, Strassen
(1980) Rabin: Monte Carlo test for compositeness
 $\Rightarrow \text{PRIMES} \in \text{coRP}$

- (1983) Adleman, Pomerance, Rumely: $(\lg n)^{O(\lg \lg \lg n)}$ deterministic algorithm
- (1987) Adleman, Huang: Monte Carlo test for PRIMES
 $\Rightarrow \text{PRIMES} \in \text{RP} \cap \text{coRP} = \text{ZPP}$
- (2002) Agrawal, Kayal, Saxena: $O^\sim(\lg^{7.5} n)$ algorithm
(Note: $O^\sim(t(n))$ is $O(t(n)) \cdot \text{poly}(\log t(n))$)

Theorem 10.1

A number $p > 2$ is prime if and only if there is a number $1 < r < p$ such that $r^{p-1} \equiv 1 \pmod{p}$, and $r^{\frac{p-1}{q}} \not\equiv 1 \pmod{p}$ for all prime divisors q of $p - 1$.

In fact, we can claim that $p > 2$ is prime iff there is a number $1 < r < p$ such that $r^{p-1} \equiv 1 \pmod{p}$, and $r^{\frac{p-1}{m}} \not\equiv 1 \pmod{p}$ for all proper **divisors** m of $p - 1$.

Pratt's Theorem

PRIMES is in $NP \cap coNP$.

1. We know that PRIMES is in coNP.

2. We will show that PRIMES is in NP.

- 13 is prime: by setting $r = 2$

$$2^{12} = (2^4)^3 = 16^3 \equiv 3^3 = 27 \equiv 1 \pmod{13}.$$

$13 - 1 = 12 \Rightarrow$ The prime factors are 2 and 3.

$$2^{\frac{13-1}{2}} = 2^6 = 64 \equiv -1 \not\equiv 1 \pmod{13}.$$

$$2^{\frac{13-1}{3}} = 2^4 = 16 \equiv 3 \not\equiv 1 \pmod{13}.$$

\therefore 13 is prime.

Our certificate for 13 being prime is $(2; 2, 3)$.

- 17 is prime: by setting $r = 3$

$$3^{16} = (3^4)^4 = 81^4 \equiv (-4)^4 = 16^2 \equiv 1 \pmod{17}.$$

$17 - 1 = 16 \Rightarrow$ The prime factor is only 2.

$$3^{\frac{17-1}{2}} = 3^8 \equiv 16 \not\equiv 1 \pmod{17}.$$

\therefore 17 is prime.

Our certificate for 13 being prime is $(3; 2)$.

- 91 is **not** prime:

However, by setting $r = 10$ we have

$$10^{90} = 100^{45} \equiv 9^{45} = (9^3)^{15} \equiv 1 \pmod{91};$$

$$91 - 1 = 90 \Rightarrow 2, 45;$$

$$10^{\frac{91-1}{2}} = 10^{45} = 1000^{15} \equiv (-1)^{15} \equiv -1 \pmod{91};$$

$$10^{\frac{91-1}{45}} = 10^2 \equiv 9 \pmod{91}.$$

However, 91 is not prime.

$$91 - 1 = 90 \Rightarrow 2, 3, 5$$

$$10^{\frac{91-1}{3}} = 10^{30} \equiv 1 \pmod{91}!$$

3. How to test whether $a^n \equiv 1 \pmod{p}$?

By the Horner's rule.

$$90 = 64 + 16 + 8 + 2 = (1011010)_2$$

Hence if we can compute $a^0, a^1, a^2, a^4, a^8, \dots, a^{64}$, we can compute $a^{90} \pmod{p}$.

We can compute $a \cdot b \pmod{p}$ in time $O(\ell^2)$ where ℓ is the length of p in binary number.

Hence, we can test whether $a^n \equiv 1 \pmod{p}$ in time $O(\ell^3)$.

4. The certificate for p being prime is of the form:

$$C(p) = (r; q_1, C(q_1), \dots, q_k, C(q_k)).$$

For example,

$$C(67) = (2; 2, (1), 3, (2; 2, (1)), 11, (8; 2, (1), 5, (3; 2, (1))))).$$

We need to test

- (a) $r^{p-1} \equiv 1 \pmod{p}$
- (b) q_1, q_2, \dots, q_k are the only prime divisors of $p - 1$.
- (c) $r^{\frac{p-1}{q_i}} \not\equiv 1 \pmod{p}$ for all possible i .
- (d) q_i 's are prime.

In fact, we can show that $C(p)$ is in polynomial length with respect to the length of the binary representation of p .

5. We also have to bound the time complexity for verifying the certificate.

As a result, one can bound the time in $O(\ell^5)$ where $\ell = \lfloor \lg p \rfloor$.

Hence PRIMES is in NP.

In order to prove Theorem 10.1, we need more knowledge on the number theory.

Theorem 10.1 A number $p > 2$ is prime if and only if there is a number $1 < r < p$ such that $r^{p-1} \equiv 1 \pmod{p}$, and $r^{\frac{p-1}{q}} \not\equiv 1 \pmod{p}$ for all prime divisors q of $p - 1$.

Notations

1. p , a prime
2. m divides n if $n = mk$. ($m|n$)
3. (m, n) , the greatest common divisor of m and n
4. $\mathbb{Z}_n = \{0, 1, 2, \dots, n - 1\}$, the residues modulo n
5. $\Phi(n) = \{m : 1 \leq m \leq n, (m, n) = 1\}$
6. $\phi(n) = |\Phi(n)|$ (Euler's totient function)
7. $\mathbb{Z}_n^* = \{m : 1 \leq m < n, (m, n) = 1\} \cup \{0\}$, the reduced residues modulo n

Example $\Phi(12) = \{1, 5, 7, 11\}$, $\Phi(11) = \{1, 2, 3, 4, \dots, 10\}$.
 $\phi(1) = 1$.

Lemma 10.1 $\phi(n) = n \prod_{p|n} (1 - \frac{1}{p})$.

Corollary If $(m, n) = 1$, then $\phi(m \cdot n) = \phi(m) \cdot \phi(n)$.
(multiplicative)

Example If $n = pq$ where p and q are primes. Then

$$\phi(n) = n - p - q + 1 = n(1 - \frac{1}{p})(1 - \frac{1}{q}).$$

Proof.

By the inclusive-exclusive principle.

Let A_p be the set of numbers between $1, \dots, n$ that are divisible by prime p . ($A_p = \{x : 1 \leq x \leq n \& p|x\}$)

Then $\Phi(n) = \bar{A}_{p_1} \cap \bar{A}_{p_2} \cap \dots \cap \bar{A}_{p_\ell} = \square - (A_{p_1} \cup A_{p_2} \cup \dots \cup A_{p_\ell})$.

$\#(A_{p_1} \cup A_{p_2} \cup \dots \cup A_{p_\ell}) = \dots$

The Chinese Remainder Theorem

Let $n = p_1 \cdots p_k$.

$\phi(n) = (p_1 - 1)(p_2 - 1) \cdots (p_k - 1)$ reveals a more important fact.

There is a one-one correspondence between r and (r_1, \dots, r_k) where $r \in \Phi(n)$ and $r_i \in \Phi(p_i)$ for all i .

In fact, $r_i \equiv r \pmod{p_i}$ and $r \in \Phi(n) \rightarrow r_i \in \Phi(p_i)$, a bijection.

Lemma 10.2 $\sum_{m|n} \phi(m) = n.$

Take $n = 12$ for illustration: $m = 1, 2, 3, 4, 6, 12.$

$$\phi(1) + \phi(2) + \phi(3) + \phi(4) + \phi(6) + \phi(12) = 12.$$

Proof.

For the case when $n = 12.$

$$\frac{1}{12}, \frac{2}{12}, \frac{3}{12}, \frac{4}{12}, \frac{5}{12}, \frac{6}{12}, \frac{7}{12}, \frac{8}{12}, \frac{9}{12}, \frac{10}{12}, \frac{11}{12}, \frac{12}{12}$$

Fermat's Theorem

Lemma 10.3 $a^{p-1} \equiv 1 \pmod{p}$ for $p \nmid a$.

$a^{\phi(n)} \equiv 1 \pmod{n}$ if $(a, n) = 1$ (Euler's Theorem)

Proof.

$1, 2, 3, \dots, p-1$

$\{a, 2a, 3a, \dots, a(p-1)\} = \{1, 2, 3, \dots, p-1\}$ since $ax \equiv ay$ implies $x \equiv y \pmod{p}$.

$(p-1)! \equiv a^{p-1} \cdot (p-1)!$

$\therefore a^{p-1} \equiv 1 \pmod{p}$.

Number of Roots for Polynomials

Lemma 10.4 Any polynomial of degree k that is not identically zero has at most k distinct roots modulo p .

Proof.

Let $p(x)$ be a polynomial of degree k . If x_k is a root for $p(x)$, then there is $q(x)$ of degree $k - 1$ such that

$$p(x) \equiv (x - x_k)q(x) \pmod{p}.$$

Any x that is not a root for $q(x)$ cannot make $q(x) \equiv 0$. Therefore there are at most $(k - 1) + 1 = k$ roots for $p(x)$ by the induction.

Exponent for a Number m

It is the smallest k such that $m^k \equiv 1 \pmod{p}$.

- Such k always exists as long as $(p, m) = 1$ since $a^{p-1} \equiv 1 \pmod{p}$.
- $k | (p - 1)$.
- If $m^{k_1} \equiv 1 \pmod{p}$ and $m^{k_2} \equiv 1 \pmod{p}$, then $m | k_1$ and $m | k_2$.

The Primitive Roots for \mathbb{Z}_p

A number r such that r^1, r^2, \dots, r^{p-1} generates $1, 2, \dots, p-1$.

There always exists a primitive root for any prime.

Let us fix a p .

Define $R(k)$ to be the set of elements in \mathbb{Z}_p with exponents exactly equal to k .

Lemma $|R(k)| \leq \phi(k)$.

Proof.

if $R(k) \neq \emptyset$, there exists s such that

$$s^1, \dots, s^{k-1} \not\equiv 1 \text{ and } s^k \equiv 1 \pmod{p}.$$

These are all k distinct roots for $x^k \equiv 1 \pmod{p}$.

And $s^t \in R(k)$ iff $(t, k) = 1$, since otherwise $(s^t)^{k/d} \equiv 1$ for some $d|(k, t)$. There are exactly $\phi(k)$ such t .

If $R(k) = \emptyset$, the inequality certainly holds.

Lemma

$$|R(k)| = \phi(k) \text{ if } k|(p-1).$$

Proof.

1. Since $a^{p-1} \equiv 1 \pmod{p}$, each $a \in \Phi(p)$ must belong to some $R(k)$ for some $k|(p-1)$.
2. Thus, $\sum_{k|(p-1)} R(k) = p-1$.
3. $\sum_{k|(p-1)} R(k) \leq \sum_{k|(p-1)} \phi(k) = p-1$.
4. Hence, all inequalities are in fact equalities.

Lemma There is an r such that r is a primitive root for \mathbb{Z}_p .

$(r^1, r^2, \dots, r^{p-1})$ generates $1, 2, \dots, p-1$

Proof.

1. There is an r such that $r \in R(p-1)$.
2. $r^1, r^2, \dots, r^{p-2} \not\equiv 1$ and $r^{p-1} \equiv 1 \pmod{p}$.
3. r^1, r^2, \dots, r^{p-1} are all distinct.
4. r is a primitive root.

Theorem 10.1 A number $p > 2$ is prime if and only if there is a number $1 < r < p$ such that $r^{p-1} \equiv 1 \pmod{p}$, and $r^{\frac{p-1}{q}} \not\equiv 1 \pmod{p}$ for all prime divisors q of $p - 1$.

Proof.

If $p > 2$ is a prime, let r be its primitive root and all conditions on the only-if part are satisfied.

Conversely, assume p is not a prime.

1. Any r satisfies $r^{\phi(p)} \equiv 1 \pmod{p}$. (Euler's Theorem)
2. If $r^{p-1} \equiv 1 \pmod{p}$, then the exponent of r must divide $\phi(p)$ and $p - 1$, and $\phi(p) \neq p - 1$.
3. There exists $q > 1$ such that $\frac{p-1}{q}$ is the exponent of r .
4. Thus, $r^{\frac{p-1}{q}} \equiv 1 \pmod{p}$ for some $q > 1$. (Contradiction)

The Primitive Roots for \mathbb{Z}_m

We can extend the idea of primitive roots to general m (which may not be a prime). It is a number r such that $r^1, r^2, \dots, r^{\phi(m)}$ (mod m) generates $\Phi(m)$.

Theorem There is a primitive root for m if and only if $m = 2, 4, p^\ell, 2p^\ell$ where p is an odd prime.