

# CS21 Decidability and Tractability

Lecture 22  
February 29, 2008

February 29, 2008

CS21 Lecture 22

1

## Outline

- the class coNP
- the class  $NP \cap coNP$ 
  - factoring in  $NP \cap coNP$

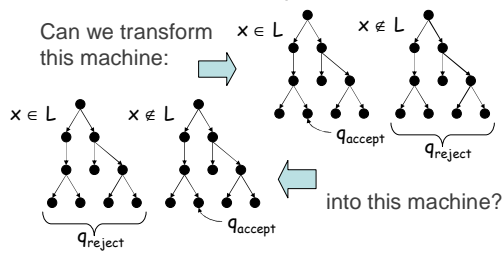
February 29, 2008

CS21 Lecture 22

2

## coNP

- Is NP closed under complement?



February 29, 2008

CS21 Lecture 22

3

## coNP

- language  $L$  is in coNP iff its complement ( $co-L$ ) is in NP
- it is believed that  $NP \neq coNP$
- note:  $P = NP$  implies  $NP = coNP$ 
  - proving  $NP \neq coNP$  would prove  $P \neq NP$
  - another major open problem...

February 29, 2008

CS21 Lecture 22

4

## coNP

- canonical coNP-complete language:  
 $UNSAT = \{\varphi : \varphi \text{ is an unsatisfiable 3-CNF formula}\}$ 
  - proof?

February 29, 2008

CS21 Lecture 22

5

## coNP

Disjunctive Normal Form  
= OR of ANDs

- another example  
 $3\text{-DNF-TAUTOLOGY} = \{\varphi : \varphi \text{ is a 3-DNF formula and for all } x, \varphi(x) = 1\}$ 
  - proof?
- another example:  
 $EQUIV\text{-CIRCUIT} = \{(C_1, C_2) : C_1 \text{ and } C_2 \text{ are Boolean circuits and for all } x, C_1(x) = C_2(x)\}$ 
  - proof?

February 29, 2008

CS21 Lecture 22

6

## Quantifier characterization of coNP

- recall that a language L is in NP if and only if it is expressible as:

$$L = \{ x \mid \exists y, |y| \leq |x|^k, (x, y) \in R \}$$

where R is a language in P.

- Theorem:** language L is in coNP if and only if it is expressible as:

$$L = \{ x \mid \forall y, |y| \leq |x|^k, (x, y) \in R \}$$

where R is a language in P.

February 29, 2008

CS21 Lecture 22

7

## Proof interpretation of coNP

- What is a proof?
- Good formalization comes from NP:  
 $L = \{ x \mid \exists y, |y| \leq |x|^k, (x, y) \in R \}$ , and  $R \in P$   
 "proof" "short" proof "proof verifier"
- NP languages have short proofs of membership
- co-NP languages have short proofs of non-membership
- coNP-complete languages are least likely to have short proofs of membership

February 29, 2008

CS21 Lecture 22

8

## coNP

- what complexity class do the following languages belong in?
  - COMPOSITES = {x : integer x is a composite}
  - PRIMES = {x : integer x is a prime number}
  - GRAPH-NONISOMORPHISM = {(G, H) : G and H are graphs that are not isomorphic}
  - EXPANSION = {(G = (V, E),  $\alpha > 0$ ): every subset  $S \subset V$  of size at least  $|V|/2$  has at least  $\alpha|S|$  neighbors}

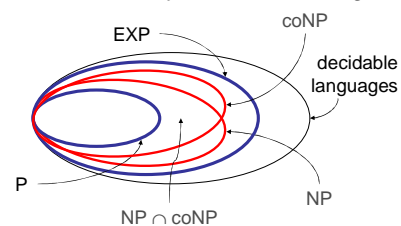
February 29, 2008

CS21 Lecture 22

9

## coNP

- Picture of the way we believe things are:



February 29, 2008

CS21 Lecture 22

10

## $NP \cap coNP$

- Might guess  $NP \cap coNP = P$  by analogy with RE (since  $RE \cap coRE = DECIDABLE$ )
- Not believed to be true.
- A problem in  $NP \cap coNP$  not believed to be in P:  
 $L = \{(x, k) : \text{integer } x \text{ has a prime factor } p < k\}$   
 (decision version of factoring)

February 29, 2008

CS21 Lecture 22

11

## $NP \cap coNP$

- Theorem:** This language is in  $NP \cap coNP$ :  
 $L = \{(x, k) : \text{integer } x \text{ has a prime factor } p < k\}$
- Proof:
- In NP (why?)
  - In coNP (what certificate demonstrates that x has no small prime factor?)
  - Use this claim: PRIMES is in NP:  
 $PRIMES = \{x : \forall 1 < y < x, y \text{ does not divide } x\}$

February 29, 2008

CS21 Lecture 22

12

## PRIMES in NP

**Theorem:** PRIMES is in NP.

$\text{PRIMES} = \{x : \forall 1 < y < x, y \text{ does not divide } x\}$

- **Proof outline:**
  - Step 1: give “ $\exists$ ” characterization of PRIMES
  - Step 2: show this leads to a short certificate of primality
  - Step 3: show that this certificate can be checked in polynomial time

February 29, 2008

CS21 Lecture 22

13

## PRIMES in NP: Step 1

**Lemma:**  $x$  is a prime iff  $\exists r$  such that

- $1 < r < x$
- $r^{x-1} = 1 \pmod{x}$
- $r^{(x-1)/q} \neq 1 \pmod{x}$ , for all prime divisors  $q$  of  $x-1$

Needed for proof:

– Definition:

$$\Phi(x) = \{y : 1 \leq y < x, \gcd(x,y) = 1\}$$

e.g.  $\Phi(10) = \{1,3,7,9\}$      $\Phi(7) = \{1,2,3,4,5,6\}$

February 29, 2008

CS21 Lecture 22

14

## PRIMES in NP: Step 1

$$\Phi(x) = \{y : 1 \leq y < x, \gcd(x,y) = 1\}$$

– Claim: for all  $r \in \Phi(x)$ ,  $r^{|\Phi(x)|} = 1 \pmod{x}$ .

- $r \cdot \Phi(x) = \Phi(x) \pmod{x}$ 
  - if not,  $ry = rz \pmod{x}$  with  $y, z \in \Phi(x)$ ,  $y > z \Rightarrow r(y-z) = 0 \pmod{x}$ , but  $1 \leq (y-z) < x$
- $r^{|\Phi(x)|} \prod_{y \in \Phi(x)} y = \prod_{y \in \Phi(x)} y \pmod{x}$
- $(r^{|\Phi(x)|} - 1) \prod_{y \in \Phi(x)} y = 0 \pmod{x}$
- $x$  must divide  $(r^{|\Phi(x)|} - 1)$
- $x$  must divide  $(r^{|\Phi(x)|} - 1) \Rightarrow r^{|\Phi(x)|} = 1 \pmod{x}$ .

February 29, 2008

CS21 Lecture 22

15

## PRIMES in NP: Step 1

– definition: the exponent of  $r \pmod{x}$  is the smallest positive integer  $k$  s.t.  $r^k = 1 \pmod{x}$

- exponent of 3 mod 8 is 2
- exponent of 2 mod 5 is 4
- exponent of 2 mod 8 does not exist

– Claim: exponent  $k$  of  $r \pmod{x}$  divides  $|\Phi(x)|$

- the only powers of  $r$  equal to 1 mod  $x$  are multiples of  $k$
- we saw that  $r^{|\Phi(x)|} = 1 \pmod{x}$

February 29, 2008

CS21 Lecture 22

16

## PRIMES in NP: Step 1

**Lemma:**  $x$  is a prime iff  $\exists r$  such that

- $1 < r < x$
- $r^{x-1} = 1 \pmod{x}$
- $r^{(x-1)/q} \neq 1 \pmod{x}$ , for all prime divisors  $q$  of  $x-1$

( $\Rightarrow$ ) assume  $x$  is prime

- we have:  $\Phi(x) = \{1,2,3,\dots,x-1\}$
- we saw: for all  $r \in \Phi(x)$ ,  $r^{|\Phi(x)|} = 1 \pmod{x}$
- Fact (without proof): for some  $r \in \Phi(x)$ , exponent of  $r \pmod{x}$  is  $|\Phi(x)| = x-1$ .

February 29, 2008

CS21 Lecture 22

17

## PRIMES in NP: Step 1

**Lemma:**  $x$  is a prime iff  $\exists r$  such that

- $1 < r < x$
- $r^{x-1} = 1 \pmod{x}$
- $r^{(x-1)/q} \neq 1 \pmod{x}$ , for all prime divisors  $q$  of  $x-1$

( $\Leftarrow$ ) assume  $x$  is not prime (so  $|\Phi(x)| < x-1$ )

- suppose  $r^{x-1} = 1 \pmod{x}$
- $r$  has an exponent  $k$ ,  $k$  divides  $x-1$
- we saw:  $k$  divides  $|\Phi(x)| < x-1$
- must exist  $q$  (dividing  $(x-1)/k$ ) such that  $r^{(x-1)/q} = 1 \pmod{x}$

February 29, 2008

CS21 Lecture 22

18

## PRIMES in NP: Step 2

**Lemma:**  $x$  is a prime iff  $\exists r$  such that

- $-1 < r < x$
- $-r^{x-1} = 1 \pmod{x}$
- $-r^{(x-1)/q} \neq 1 \pmod{x}$ , for all prime divisors  $q$  of  $x-1$

– short certificate  $C(x)$  of primality:

- $C(2) = 2$
  - $C(x) = x, r, C(q_1), C(q_2), \dots, C(q_m)$
- where  $r$  is the integer guaranteed by the lemma and  $q_1, q_2, \dots, q_m$  are the prime factors of  $x-1$

February 29, 2008

CS21 Lecture 22

19

## PRIMES in NP: Step 2

- $C(2) = 2$
  - $C(x) = x, r, C(q_1), C(q_2), \dots, C(q_m)$
- where  $r$  is the integer guaranteed by the lemma and  $q_1, q_2, \dots, q_m$  are the prime factors of  $x-1$

**Claim:**  $S(x) = |C(x)|$  is at most  $5\log^2 x$

- $S(2) \leq 5\log^2 2$
- $S(x) \leq 5\log x + \sum_{q|(x-1)} S(q) \leq 5\log x + \sum_{q|(x-1)} 5\log^2 q$   
 $\leq 5\log x + 5(\log x/2)(\log x)$   
 $\leq 5\log x + 5(\log x - 1)(\log x) = 5(\log^2 x)$

February 29, 2008

CS21 Lecture 22

20

## PRIMES in NP: Step 3

**Lemma:**  $x$  is a prime iff  $\exists r$  such that

- $-1 < r < x$
- $-r^{x-1} = 1 \pmod{x}$
- $-r^{(x-1)/q} \neq 1 \pmod{x}, \forall q|x-1$

short certificate  $C(x)$ :

- $C(2) = 2$
- $C(x) = x, r,$   
 $C(q_1), C(q_2), \dots, C(q_m)$   
 $(q_1, \dots, q_m \text{ prime factors of } x-1)$

– efficient verification:

- check that  $r^{x-1} = 1 \pmod{x}$
- check that  $r^{(x-1)/q_i} \neq 1 \pmod{x}$
- check that  $\prod_i q_i = x-1$
- recursively check that  $q_i$  is prime for all  $i$

February 29, 2008

CS21 Lecture 22

21

## PRIMES in NP: Step 3

– efficient verification:

- check that  $r^{x-1} = 1 \pmod{x}$
- check that  $r^{(x-1)/q_i} \neq 1 \pmod{x}$
- check that  $\prod_i q_i = x-1$
- recursively check that  $q_i$  is prime for all  $i$

– efficient exponentiation:

- compute  $r^j$  for  $j = 0, 1, 2, 4, 8, 16, 32, \dots, \log_2 x$  by repeated squaring (mod  $x$ )
- to compute  $r^a$  write  $a$  in binary  $a = \sum_i a_i 2^i$

$$r^a = r^{\sum_i a_i 2^i} = \prod_{i: a_i=1} r^{2^i}$$

February 29, 2008

CS21 Lecture 22

22

## PRIMES in NP: Step 3

– efficient verification:

- check that  $r^{x-1} = 1 \pmod{x}$
- check that  $r^{(x-1)/q_i} \neq 1 \pmod{x}$
- check that  $\prod_i q_i = x-1$
- recursively check that  $q_i$  is prime for all  $i$

**Claim:**  $T(x) =$  time to check  $C(x)$  is  $\leq \text{clog}^4 x$

–  $T(2) \leq \text{clog}^4 2$

- $T(x) \leq \text{clog}^3 x + \sum_{q|(x-1)} T(q) \leq \text{clog}^3 x + \sum_{q|(x-1)} \text{clog}^4 q$   
 $\leq \text{clog}^3 x + c(\log x/2)^3 (\log x)$   
 $< \text{clog}^3 x + c(\log x - 1)(\log x)^3 = \text{clog}^4 x$

February 29, 2008

CS21 Lecture 22

23

## PRIMES in NP

- we have shown PRIMES is in NP
  - Step 1: give “ $\exists$ ” characterization of PRIMES
  - Step 2: short certificate of primality
  - Step 3: certificate can be checked in poly time

- 2002: M. Agrawal, N. Kayal, N. Saxena, prove PRIMES is in P (!)

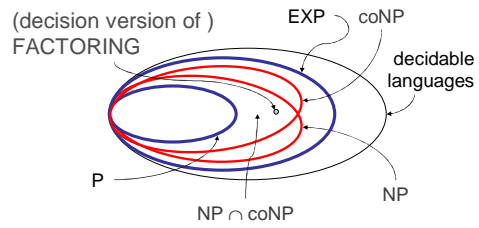
February 29, 2008

CS21 Lecture 22

24

## Summary

- Picture of the way we believe things are:



February 29, 2008

CS21 Lecture 22

25