coNP

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

- another example
  \[ \text{3-DNF-TAUTOL} = \{ \phi : \phi \text{ is a 3-DNF formula and for all } x, \varphi(x) = 1 \} \]
  - proof?

- another example:
  \[ \text{EQUIV-CIRCUIT} = \{ (C_1, C_2) : C_1 \text{ and } C_2 \text{ are Boolean circuits and for all } x, C_1(x) = C_2(x) \} \]
  - proof?

Quantifier characterization of coNP

- recall that a language \( L \) is in NP if and only if it is expressible as:
  \[ L = \{ x \mid \exists y, |y| \leq |x|^a, (x, y) \in R \} \]
  where \( R \) is a language in P.

**Theorem:** language \( L \) is in coNP if and only if it is expressible as:
\[ L = \{ x \mid \forall y, |y| \leq |x|^a, (x, y) \in R \} \]
where \( R \) is a language in P.

Proof interpretation of coNP

- What is a proof?
- Good formalization comes from NP:
  \[ L = \{ x \mid \exists y, |y| \leq |x|^a, (x, y) \in R \}, \text{ and } R \in \text{P} \]
  "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
coNP

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

\[
\begin{align*}
\text{NP} \cap \text{coNP} & \\
\text{PRIMES in NP} & \\
\text{Summary} & \\
\end{align*}
\]

NP \cap \text{coNP}

- Might guess \(\text{NP} \cap \text{coNP} = \text{P}\) by analogy with \(\text{RE}\) (since \(\text{RE} \cap \text{coRE} = \text{DECIDABLE}\))

- Not believed to be true.
- A problem in \(\text{NP} \cap \text{coNP}\) not believed to be in \(\text{P}\):
  \[
  L = \{(x, k) : \text{integer } x \text{ has a prime factor } p < k\}
  \]
  (decision version of factoring)

\[
\begin{align*}
\text{PRIMES in NP} & \\
\text{Summary} & \\
\end{align*}
\]

\textbf{Theorem}: (Pratt 1975) PRIMES is in \(\text{NP}\).
\[
\text{PRIMES} = \{x : \forall 1 < y < x, y \text{ does not divide } x\}
\]

- Proof outline:
  - Step 1: give “3” characterization of \(\text{PRIMES}\)
  - Step 2: this \(\implies\) short certificate of primality
  - Step 3: certificate checkable in poly time
    (we will skip, because…)

\textbf{Theorem}: (M. Agrawal, N. Kayal, N. Saxena 2002)

\[
\text{PRIMES is in } \text{P}.
\]

\[
\begin{align*}
\text{Summary} & \\
\end{align*}
\]
Space complexity

**Definition:** the space complexity of a TM $M$ is a function

$$f: \mathbb{N} \rightarrow \mathbb{N}$$

where $f(n)$ is the maximum number of tape cells $M$ scans on any input of length $n$.

- "$M$ uses space $f(n)$," "$M$ is a $f(n)$ space TM"

---

PSPACE

- A PSPACE-complete problem:
  - Quantified Satisfiability:
    - $\text{QSAT} = \{ \varphi : \varphi$ is a 3-CNF, and
      \[ \exists x_1 \forall x_2 \exists x_3 \forall x_4 \exists x_5 \ldots \forall x_n \varphi(x_1, x_2, x_3, \ldots, x_n) \}$
    - example: $\varphi = (x_1 \lor \neg x_2 \lor \neg x_3) \land (\neg x_2 \lor \neg x_3)$
      
      YES: $x_1 = T;~ x_2 = T;~ x_3 = F$; if $x_2 = T$...
  
- \(\text{PSPACE} \subseteq \text{EXP}\) (proof?)
- containments believed to be proper

---

QSAT is PSPACE-complete

**Theorem:** QSAT is PSPACE-complete.

**Proof:**

- in PSPACE: $\exists x_1 \forall x_2 \exists x_3 \ldots \exists x_n \varphi(x_1, x_2, \ldots, x_n)$?
  - "$\exists x_1$": for both $x_1 = 0$, $x_1 = 1$, recursively solve $\forall x_2 \exists x_3 \ldots \exists x_n \varphi(x_1, x_2, \ldots, x_n)$?
    - if at least one "yes", return "yes"; else return "no"
  - "$\forall x_2$": for both $x_2 = 0$, $x_2 = 1$, recursively solve $\exists x_3 \ldots \exists x_n \varphi(x_1, x_2, \ldots, x_n)$?
    - if at least one "no", return "no"; else return "yes"
  - base case: evaluating a 3-CNF expression
    - poly(n) recursion depth
    - poly(n) bits of state at each level
QSAT is **PSPACE**-complete

- given TM $M$ deciding $L \in \text{PSPACE}$; input $x$
- $2^n$ possible configurations
- single START configuration
- assume single ACCEPT configuration

- define:
  
  \[ \text{REACH}(X, Y, i) \iff \text{configuration } Y \text{ reachable from configuration } X \text{ in at most } 2^i \text{ steps.} \]

---

Goal: produce 3-CNF $\phi(w_1, w_2, w_3, \ldots, w_m)$ such that

\[ \exists w_1 \forall w_2 \ldots \exists w_m \phi(w_1, \ldots, w_m) \iff \text{REACH}(\text{START, ACCEPT, } n^k) \]

---

for $i = 0, 1, \ldots, n^k$ produce quantified Boolean expressions $\psi_i(A, B, W)$ such that $\forall A, B$:

\[ \exists w_1 \forall w_2 \ldots \psi_i(A, B, W) \iff \text{REACH}(A, B, i) \]

- convert $\psi_{n^k}$ to 3-CNF $\phi$
  - add variables $V$
- hardwire $A = \text{START}, B = \text{ACCEPT}$
  
  \[ \exists w_1 \forall w_2 \ldots \exists V \phi(W, V) \iff x \in L \]