Agenda

• Two weeks ago
  - The Class P
• Last week
  - The Class NP
• This week
  - More on the class NP
Announcement

- **Quiz tomorrow**
  - Big-O and small-o notation
  - Machine dependent complexity
  - Proving a problem is in P
  - NP definitions
Solving vs. verifying

• What if we can’t solve the problem in $O(n^k)$ time?
• Given a problem and a potential solution, can we verify the solution is correct?
Example

• The vertex cover problem
  - Given a graph $G = \langle V, E \rangle$ and a number $k$ in $\mathbb{N}$, does there exist a subset $V'$ of $V$ such that
  - $|V'| = k$
  - For every $(u, v) \in E$, either $u \in V'$ or $v \in V'$
Vertex cover
The vertex cover problem

• There is no known polynomial solution to the vertex cover problem

• What if we have a potential solution
  - Can we verify it in $O(n^k)$ time?
Verifier

\( M = \text{"On input } <V,E,V'>\)

1. For each vertex \( v \) in \( V' \)
2. For each edge \( (u,w) \) in \( E \)
3. If \( u = v \) or \( w=v \), mark \( (u,w) \)
4. For each edge \( (u,w) \) in \( E \)
5. If \( (u,w) \) is not marked, reject
6. Accept"

- \( M \) accepts \( <V,E,V'> \) if and only if every edge in \( E \) has at least one endpoint in \( V' \)
- **Computational complexity?**
  - \( O(|V'| \times |E|) \)
The class NP

Definition: A verifier for a language $A$ is an algorithm $V$, where
$A = \{ w | V \text{ accepts } <w,c> \text{ for some string } c \}$
The string $c$ is called a certificate of membership in $A$.

Definition: NP is the class of languages that have polynomial-time verifiers.
Why NP?

- The N in NP stands for non-deterministic
- Any language in NP can be non-deterministically solved in polynomial time using the verifier
  - Guess the certificate
  - Verify
Is NP closed under complementation?

• For example, can we verify in polynomial time that a graph cannot be 3-colored?
  - Not obviously
  - It seems we need to check many 3-colorings before we can conclude that none exist

• The 3-coloring problem is in coNP
What we know

NP  P  coNP
What we don’t know

Are there any problems here?

NP

P

coNP