NP

CSCI 338

NP

$\boldsymbol{P}$ is the set of languages that are decidable in polynomial time on a deterministic single-tape TM.

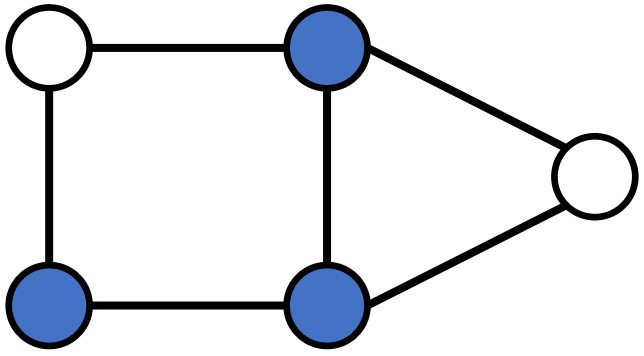
To show something is in P, build a polynomial time decider for it.

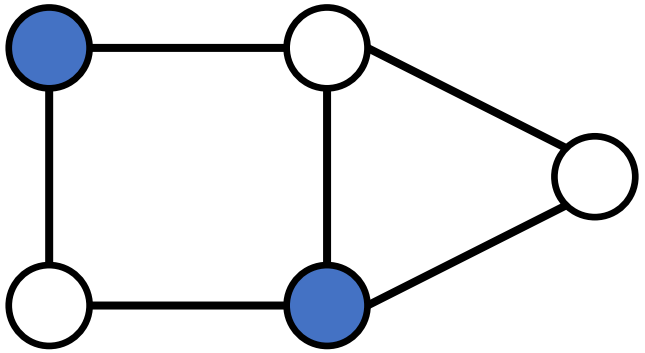
NP { Set of languages that have polynomial time verifiers.

Vertex Cover (VC)

Vertex Cover = $\{\langle G, k\rangle$: $G = (V, E)$ is a graph and k is an integer $\leq |V|$ such that there exists some $V' \subseteq V$ with $|V'| \leq k,$ such that each edge in E contains an end point in $V'\}$

Vertex Cover: Given graph $G = (V, E)$ and integer $k \leq |V|$, is there $V' \subseteq V$, with $|V'| \leq k$, such that each edge in E contains an end point in V'?





Vertex Cover (VC)

Vertex Cover: Given graph $G = (V, E)$ and integer $k \leq |V|$, is there $V' \subseteq V$, with $|V'| \leq k$, such that each edge in E contains an end point in V'?

Claim: VC $\in NP$

Proof:

Build a polynomial time verifier.

$|V| = n$.

M = on input $\langle \langle G, k \rangle, V' \rangle$, where V' is a subset of V.

$\boldsymbol{O(1)}$ ⟶ 1. Test if $|V'| \leq k$, reject if not.

$\boldsymbol{O(n^2)}$ ⟶ 2. For each edge $e = (a, b)$ in E,

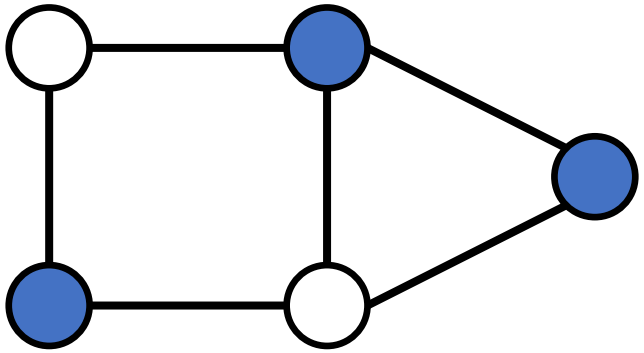
$\boldsymbol{O(n)}$ ⟶ 2.1 Test if $a \in V'$ or $b \in V'$, reject if neither.

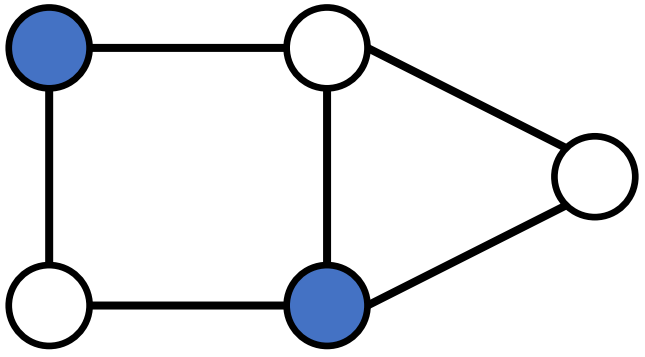
$\boldsymbol{O(1)}$ ⟶ 3. accept.

For $|V| = n$, M runs in $O(n^3)$ time, therefore $VC \in NP$.

Independent Set (IS)

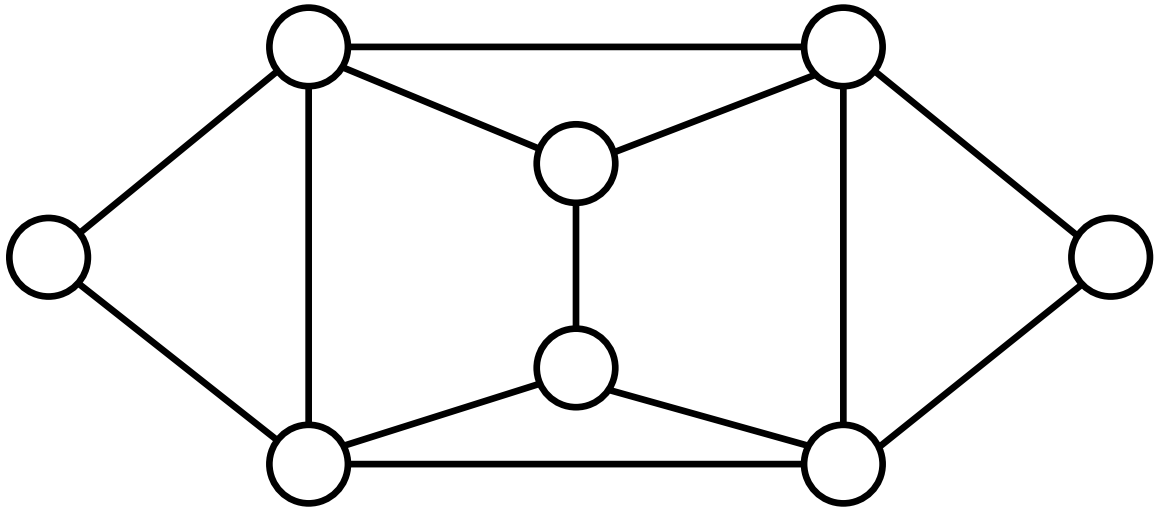
Independent Set: Given a graph $G = (V, E)$ and integer $k \leq |V|$, is there a subset V' of size $\geq k$, such that no two vertices $\in V'$ are adjacent?





Independent Set (IS)

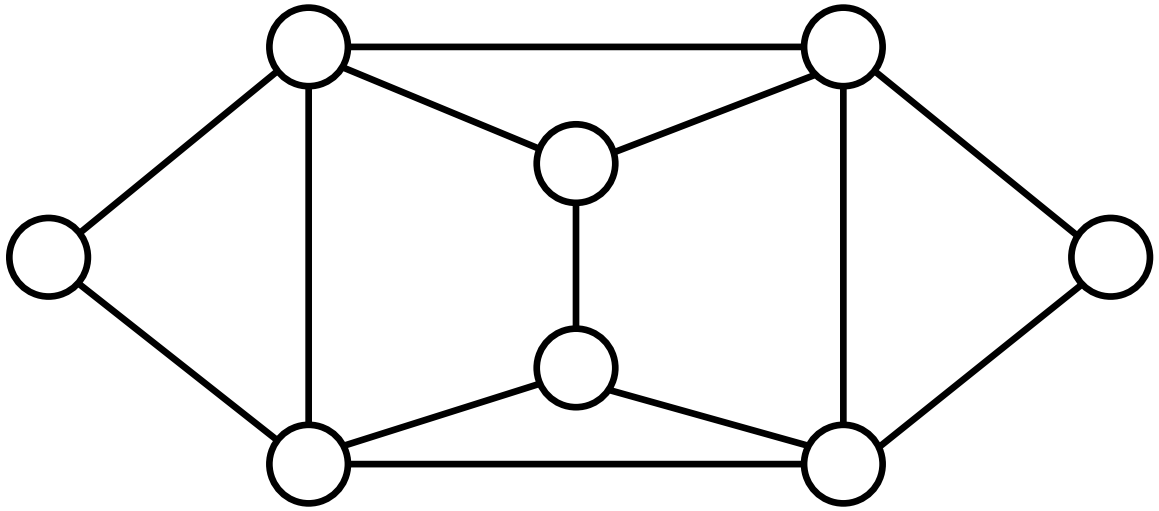
Independent Set: Given a graph $G = (V, E)$ and integer $k \leq |V|$, is there a subset V' of size $\geq k$, such that no two vertices $\in V'$ are adjacent?



Is there an IS $\leq k$ for $k = 1$?

Independent Set (IS)

Independent Set: Given a graph $G = (V, E)$ and integer $k \leq |V|$, is there a subset V' of size $\geq k$, such that no two vertices $\in V'$ are adjacent?

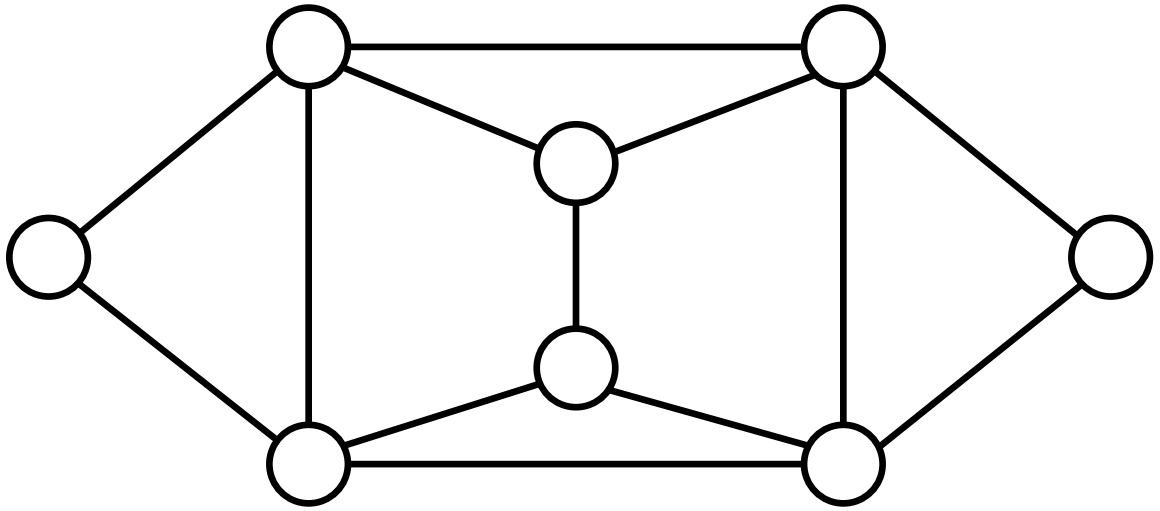


Is there an IS $\leq k$ for $k = 1$?

Yes! Any vertex by itself is an IS!

Independent Set (IS)

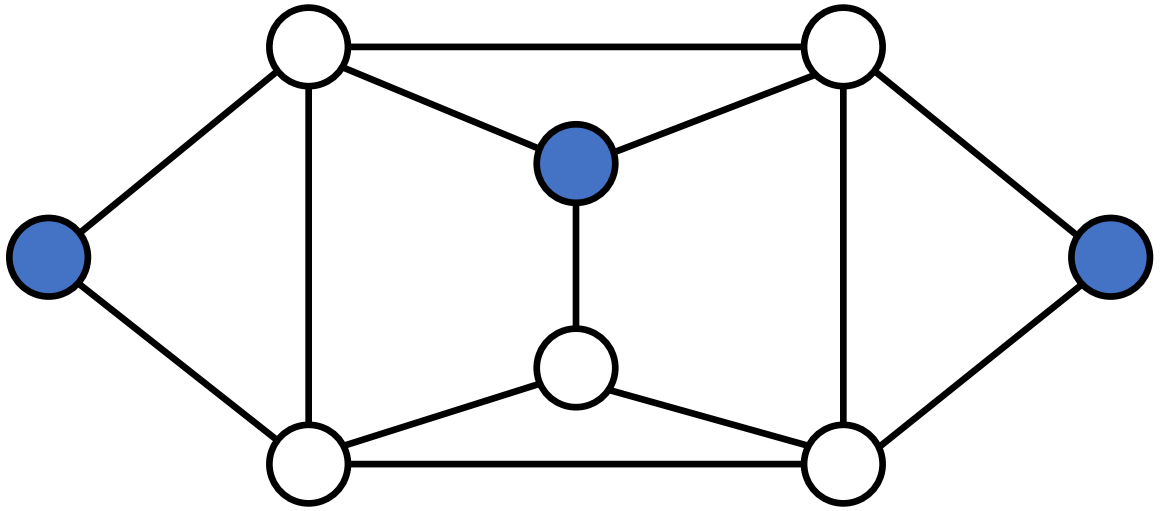
Independent Set: Given a graph $G = (V, E)$ and integer $k \leq |V|$, is there a subset V' of size $\geq k$, such that no two vertices $\in V'$ are adjacent?



What is the optimal (i.e., largest) independent set?

Independent Set (IS)

Independent Set: Given a graph $G = (V, E)$ and integer $k \leq |V|$, is there a subset V' of size $\geq k$, such that no two vertices $\in V'$ are adjacent?



What is the optimal (i.e., largest) independent set?

Independent Set (IS)

Independent Set: Given a graph $G = (V, E)$ and integer $k \leq |V|$, is there $V' \subseteq V$, with $|V'| \geq k$, such that no two vertices $\in V'$ are adjacent?

Claim: IS $\in NP$

Proof:

Independent Set (IS)

Independent Set: Given a graph $G = (V, E)$ and integer $k \leq |V|$, is there $V' \subseteq V$, with $|V'| \geq k$, such that no two vertices $\in V'$ are adjacent?

Claim: IS $\in NP$

Proof:

Build a polynomial time verifier.

M = on input $\langle \langle G, k \rangle, ?? \rangle$

Independent Set (IS)

Independent Set: Given a graph $G = (V, E)$ and integer $k \leq |V|$, is there $V' \subseteq V$, with $|V'| \geq k$, such that no two vertices $\in V'$ are adjacent?

Claim: IS $\in NP$

Proof:

Build a polynomial time verifier.

M = on input $\langle \langle G, k \rangle, V' \rangle$, where V' is a subset of V.

Independent Set (IS)

Independent Set: Given a graph $G = (V, E)$ and integer $k \leq |V|$, is there $V' \subseteq V$, with $|V'| \geq k$, such that no two vertices $\in V'$ are adjacent?

Claim: IS $\in NP$

Proof:

Build a polynomial time verifier.

M = on input $\langle \langle G, k \rangle, V' \rangle$, where V' is a subset of V.

1. ???

Independent Set (IS)

Independent Set: Given a graph $G = (V, E)$ and integer $k \leq |V|$, is there $V' \subseteq V$, with $|V'| \geq k$, such that no two vertices $\in V'$ are adjacent?

Claim: IS $\in NP$

Proof:

Build a polynomial time verifier.

M = on input $\langle \langle G, k \rangle, V' \rangle$, where V' is a subset of V.

1. Test if $|V'| \geq k$, reject if not.
2. ???

Independent Set (IS)

Independent Set: Given a graph $G = (V, E)$ and integer $k \leq |V|$, is there $V' \subseteq V$, with $|V'| \geq k$, such that no two vertices $\in V'$ are adjacent?

Claim: IS $\in NP$

Proof:

Build a polynomial time verifier.

M = on input $\langle \langle G, k \rangle, V' \rangle$, where V' is a subset of V.

1. Test if $|V'| \geq k$, reject if not.
2. For each pair of vertices v_1, v_2 in V',
   2.1 ???

Independent Set (IS)

Independent Set: Given a graph $G = (V, E)$ and integer $k \leq |V|$, is there $V' \subseteq V$, with $|V'| \geq k$, such that no two vertices $\in V'$ are adjacent?

Claim: IS $\in NP$

Proof:

Build a polynomial time verifier.

M = on input $\langle \langle G, k \rangle, V' \rangle$, where V' is a subset of V.

1. Test if $|V'| \geq k$, reject if not.
2. For each pair of vertices v_1, v_2 in V',
   2.1 Test if $(v_1, v_2) \in E$ and reject if it is.
3. ???

Independent Set (IS)

Independent Set: Given a graph $G = (V, E)$ and integer $k \leq |V|$, is there $V' \subseteq V$, with $|V'| \geq k$, such that no two vertices $\in V'$ are adjacent?

Claim: IS $\in NP$

Proof:

Build a polynomial time verifier.

M = on input $\langle \langle G, k \rangle, V' \rangle$, where V' is a subset of V.

1. Test if $|V'| \geq k$, reject if not.
2. For each pair of vertices v_1, v_2 in V',
   2.1 Test if $(v_1, v_2) \in E$ and reject if it is.
3. accept.

Independent Set (IS)

Independent Set: Given a graph $G = (V, E)$ and integer $k \leq |V|$, is there $V' \subseteq V$, with $|V'| \geq k$, such that no two vertices $\in V'$ are adjacent?

Claim: IS $\in NP$

Proof:

Build a polynomial time verifier.

$|V| = n$.

M = on input $\langle \langle G, k \rangle, V' \rangle$, where V' is a subset of V.

$\boldsymbol{O}(?)$ ⟶ 1. Test if $|V'| \geq k$, reject if not.

2. For each pair of vertices v_1, v_2 in V',

2.1 Test if $(v_1, v_2) \in E$ and reject if it is.

3. accept.

Independent Set (IS)

Independent Set: Given a graph $G = (V, E)$ and integer $k \leq |V|$, is there $V' \subseteq V$, with $|V'| \geq k$, such that no two vertices $\in V'$ are adjacent?

Claim: IS $\in NP$

Proof:

Build a polynomial time verifier.

$|V| = n$.

M = on input $\langle \langle G, k \rangle, V' \rangle$, where V' is a subset of V.

$\boldsymbol{O(1)}$ ⟶ 1. Test if $|V'| \geq k$, reject if not.

2. For each pair of vertices v_1, v_2 in V',

   2.1 Test if $(v_1, v_2) \in E$ and reject if it is.

3. accept.

Independent Set (IS)

Independent Set: Given a graph $G = (V, E)$ and integer $k \leq |V|$, is there $V' \subseteq V$, with $|V'| \geq k$, such that no two vertices $\in V'$ are adjacent?

Claim: IS $\in NP$

Proof:

Build a polynomial time verifier.

$|V| = n$.

M = on input $\langle \langle G, k \rangle, V' \rangle$, where V' is a subset of V.

$\boldsymbol{O(1)}$ ⟶ 1. Test if $|V'| \geq k$, reject if not.

$\boldsymbol{O(?)}$ ⟶ 2. For each pair of vertices v_1, v_2 in V',

2.1 Test if $(v_1, v_2) \in E$ and reject if it is.

3. accept.

Independent Set (IS)

Independent Set: Given a graph $G = (V, E)$ and integer $k \leq |V|$, is there $V' \subseteq V$, with $|V'| \geq k$, such that no two vertices $\in V'$ are adjacent?

Claim: IS $\in NP$

Proof:

Build a polynomial time verifier.

$|V| = n$.

M = on input $\langle \langle G, k \rangle, V' \rangle$, where V' is a subset of V.

$\boldsymbol{O(1)}$ ⟶ 1. Test if $|V'| \geq k$, reject if not.

$\boldsymbol{O(n^2)}$ ⟶ 2. For each pair of vertices v_1, v_2 in V',

2.1 Test if $(v_1, v_2) \in E$ and reject if it is.

3. accept.

Independent Set (IS)

Independent Set: Given a graph $G = (V, E)$ and integer $k \leq |V|$, is there $V' \subseteq V$, with $|V'| \geq k$, such that no two vertices $\in V'$ are adjacent?

Claim: IS $\in NP$

Proof:

Build a polynomial time verifier.

$|V| = n$.

M = on input $\langle \langle G, k \rangle, V' \rangle$, where V' is a subset of V.

$\boldsymbol{O(1)}$ ⟶ 1. Test if $|V'| \geq k$, reject if not.

$\boldsymbol{O(n^2)}$ ⟶ 2. For each pair of vertices v_1, v_2 in V',

$\boldsymbol{O(?)}$ ⟶ 2.1 Test if $(v_1, v_2) \in E$ and reject if it is.

3. accept.

Independent Set (IS)

Independent Set: Given a graph $G = (V, E)$ and integer $k \leq |V|$, is there $V' \subseteq V$, with $|V'| \geq k$, such that no two vertices $\in V'$ are adjacent?

Claim: IS $\in NP$

Proof:

Build a polynomial time verifier.

$|V| = n$.

M = on input $\langle \langle G, k \rangle, V' \rangle$, where V' is a subset of V.

$\boldsymbol{O(1)}$ ⟶ 1. Test if $|V'| \geq k$, reject if not.

$\boldsymbol{O(n^2)}$ ⟶ 2. For each pair of vertices v_1, v_2 in V',

$\boldsymbol{O(n^2)}$ ⟶ 2.1 Test if $(v_1, v_2) \in E$ and reject if it is.

3. accept.

Independent Set (IS)

Independent Set: Given a graph $G = (V, E)$ and integer $k \leq |V|$, is there $V' \subseteq V$, with $|V'| \geq k$, such that no two vertices $\in V'$ are adjacent?

Claim: IS $\in NP$

Proof:

Build a polynomial time verifier.

$|V| = n$.

M = on input $\langle \langle G, k \rangle, V' \rangle$, where V' is a subset of V.

$\boldsymbol{O(1)}$ ⟶ 1. Test if $|V'| \geq k$, reject if not.

$\boldsymbol{O(n^2)}$ ⟶ 2. For each pair of vertices v_1, v_2 in V',

$\boldsymbol{O(n^2)}$ ⟶ 2.1 Test if $(v_1, v_2) \in E$ and reject if it is.

$\boldsymbol{O(?)}$ ⟶ 3. accept.

Independent Set (IS)

Independent Set: Given a graph $G = (V, E)$ and integer $k \leq |V|$, is there $V' \subseteq V$, with $|V'| \geq k$, such that no two vertices $\in V'$ are adjacent?

Claim: IS $\in NP$

Proof:

Build a polynomial time verifier.

$|V| = n$.

M = on input $\langle \langle G, k \rangle, V' \rangle$, where V' is a subset of V.

$\boldsymbol{O(1)}$ ⟶ 1. Test if $|V'| \geq k$, reject if not.

$\boldsymbol{O(n^2)}$ ⟶ 2. For each pair of vertices v_1, v_2 in V',

$\boldsymbol{O(n^2)}$ ⟶ 2.1 Test if $(v_1, v_2) \in E$ and reject if it is.

$\boldsymbol{O(1)}$ ⟶ 3. accept.

Independent Set (IS)

Independent Set: Given a graph $G = (V, E)$ and integer $k \leq |V|$, is there $V' \subseteq V$, with $|V'| \geq k$, such that no two vertices $\in V'$ are adjacent?

Claim: IS $\in NP$

Proof:

Build a polynomial time verifier.

$|V| = n$.

M = on input $\langle \langle G, k \rangle, V' \rangle$, where V' is a subset of V.

$\boldsymbol{O(1)}$ ⟶ 1. Test if $|V'| \geq k$, reject if not.

$\boldsymbol{O(n^2)}$ ⟶ 2. For each pair of vertices v_1, v_2 in V',

$\boldsymbol{O(n^2)}$ ⟶ 2.1 Test if $(v_1, v_2) \in E$ and reject if it is.

$\boldsymbol{O(1)}$ ⟶ 3. accept.

For $|V| = n$, M runs in $O(n^4)$ time, therefore IS $\in NP$.

NP

$\boldsymbol{P}$ is the set of languages that are decidable in polynomial time on a deterministic single-tape TM.

To show something is in P, build a polynomial time decider for it.

NP { Set of languages that have polynomial time verifiers.

NP

$\boldsymbol{P}$ is the set of languages that are decidable in polynomial time on a deterministic single-tape TM.

To show something is in P, build a polynomial time decider for it.

NP {
- Set of languages that have polynomial time verifiers.
- Set of languages that are decidable by nondeterministic polynomial time TMs.

NP

$\boldsymbol{P}$ is the set of languages that are decidable in polynomial time on a deterministic single-tape TM.

To show something is in P, build a polynomial time decider for it.

NP {
- Set of languages that have polynomial time verifiers.
- Set of languages that are decidable by nondeterministic polynomial time TMs.

Nondeterministic polynomial time decider:

1. Pick a potential solution.
2. Verify its correctness.

Vertex Cover (VC)

Vertex Cover: Given graph $G = (V, E)$ and integer $k \leq |V|$, is there $V' \subseteq V$, with $|V'| \leq k$, such that each edge in E contains an end point in V'?

Claim: VC $\in NP$

Proof:

M = on input $\langle \langle G, k \rangle, V' \rangle$, where V' is a subset of V.

1. Test if $|V'| \leq k$, reject if not.
2. For each edge $e = (a, b)$ in E,
   2.1 Test if $a \in V'$ or $b \in V'$,
   reject if neither.
3. accept.

Vertex Cover (VC)

Vertex Cover: Given graph $G = (V, E)$ and integer $k \leq |V|$, is there $V' \subseteq V$, with $|V'| \leq k$, such that each edge in E contains an end point in V'?

Claim: VC $\in NP$

Proof:

M = on input $\langle \langle G, k \rangle, V' \rangle$, where V' is a subset of V.

1. Test if $|V'| \leq k$, reject if not.
2. For each edge $e = (a, b)$ in E,
   2.1 Test if $a \in V'$ or $b \in V'$, reject if neither.
3. accept.

M = on input $\langle G, k \rangle$.

1. Nondeterministically select a subset V' of V of size k.
2. For each edge $e = (a, b)$ in E,
   2.1 Test if $a \in V'$ or $b \in V'$, reject if neither.
3. accept.

P versus NP

$\boldsymbol{P}$ is the set of languages that are decidable in polynomial time on a deterministic single-tape TM.

To show something is in P, build a polynomial time decider for it.

NP {

- Set of languages that have polynomial time verifiers.
- Set of languages that are decidable by nondeterministic polynomial time TMs.

To show something is in NP, build a polynomial time verifier (or nondeterministic decider) for it.

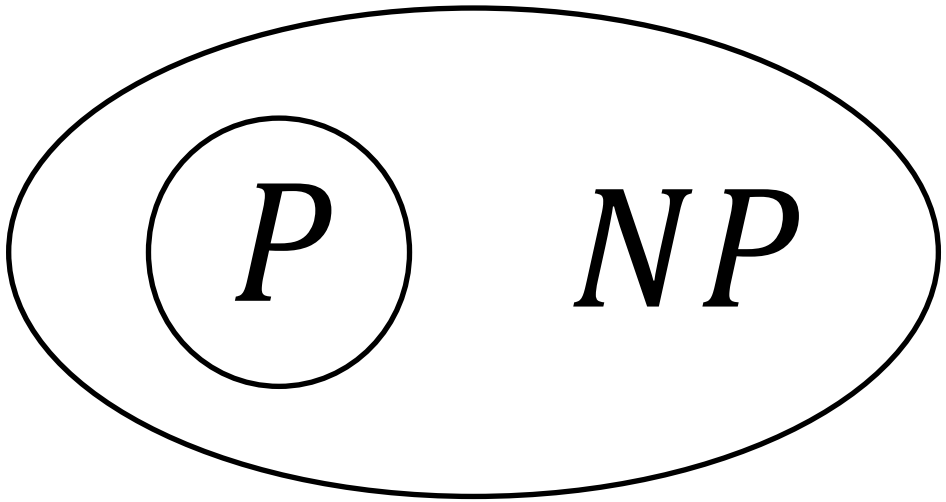
P versus NP

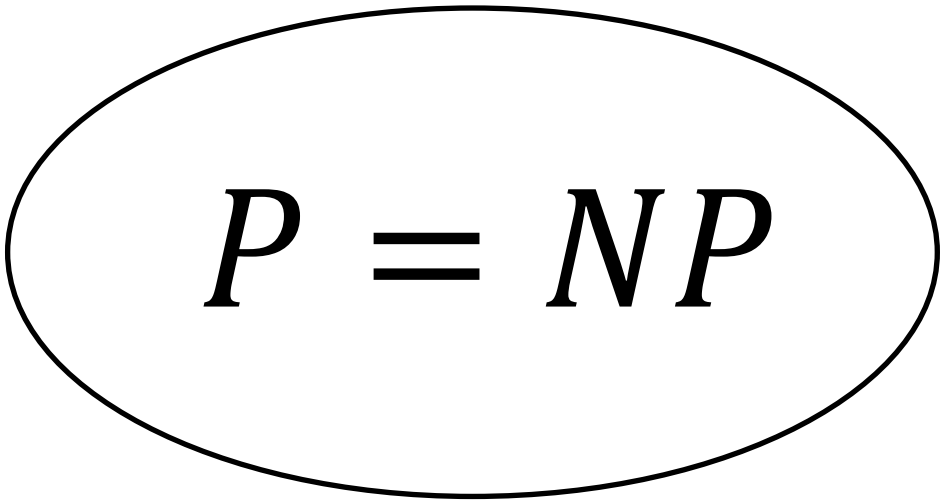
$$P \overset{?}{=} NP$$

Solvable in polynomial time

Verifiable in polynomial time

P versus NP





Can all problems that are verifiable in polynomial time be solved in polynomial time?