NP-Completeness (cont)

VC (VERTEX-COVER)

Instance: A graph $G = (V, E)$ and an integer $m$.

Question: Does $G$ have a vertex cover of size $m$ or less?

($V'$ is a vertex cover for $G = (V, E)$ if for every edge $e=(u,v)$ either $u \in V'$ or $v \in V'$ or both.)

$$m=3 \quad \text{YES} \quad G_1$$

$$m=2 \quad \text{NO} \quad G_2$$

NP-Completeness (cont)

CLIQUE $\leq_p$ VC

Step 1: Construct $f : \{(G,k)_{\text{CLIQUE}} \} \rightarrow \{(G',m)_{\text{VC}} \}$

Given $G = (V, E)$ and $k$, let $G' = \overline{G}$ and $m = |V| - k$.

$\overline{G} = (V, \overline{E})$ where $\overline{E} = \{(u,v) \mid u, v \in V \text{ and } (u,v) \notin E \}$.

Example:

$\begin{array}{c}
(G,4)_{\text{CLIQUE}} \\
(G_1)_{\text{VC}} \quad \overset{k=4}{\longrightarrow} \quad (G',2)_{\text{VC}} \\
\end{array}$

$\begin{array}{c}
m = 6 - 4 = 2 \\
\end{array}$

NP-Completeness (cont)

CLIQUE $\leq_p$ VC

Step 2: Show that $(G,k) \in L_{\text{CLIQUE}} \iff f(G,k) \in L_{\text{VC}}$

$G$ has a clique of size $\geq k \iff \overline{G}$ has a vertex cover of size $\leq |V| - k$

Proof: Suppose $V'$ is a clique of size at least $k$ in $G$.

Pick any two vertices $u$ and $v$ in $V$.

If the edge $(u,v)$ is in $\overline{E}$, then it is not in $E$.

So $u$ and $v$ cannot both be in $V'$ (a clique of $G$).

Either $u$ or $v$ is in $V'' = V - V'$.

$V''$ is a vertex cover for $\overline{G}$ of size at most $|V| - k$.

Proof: (cont) Now suppose $V''$ is a vertex cover of size at most $|V| - k$ in $\overline{G}$.

Pick any two vertices $u$ and $v$ in $V' = V - V''$.

Then both $u$ and $v$ are not in $V''$ (a vertex cover for $\overline{G}$).

So the edge $(u,v)$ is not in $\overline{E}$, and hence is in $E$.

$V'$ is a clique in $G$ of size at least $|V| - (|V| - k) = k$.

QED
NP-Completeness (cont)

**CLIQUE \( \leq_p \) VC**

Step 3: Show that \( f \) is computable in polynomial time.

If \( G \) has \( a \) vertices and \( b \) edges then \( f(G,k) \) has \( a \) vertices and \( O(a^2) \) edges.

Whether an edge exists or not in \( \overline{G} \) can be determined by inspection of \( G \).

\( f \) is computable in polynomial time.

Finished **CLIQUE \( \leq_p \) VC**

---

**NP-Completeness (cont)**

**VC \( \leq_p \) SUBSET-SUM**

Step 1: Construct \( f : \{(G,m)_{\text{VC}}\} \rightarrow \{(S,t)_{\text{SUBSET-SUM}}\} \)

Given \( G = (V,E) \) and \( m \) where \( E = \{e_1,e_2,\ldots,e_{|E|}\} \) create for each \( v_i \in V \) the integer

\[ s_i = 4^{|E|} + \sum_{j=1}^{|E|} 4^{|E|-1} \cdot b_{ij} \]

where \( b_{ij} = \begin{cases} 1 & \text{if } v_i \text{ is an endpoint of } e_j \\ 0 & \text{otherwise} \end{cases} \)

create for each \( e_j \in E \) the integer \( s_j = 4^{|E|-1} \).

and let \( t = m4^{|E|} + \sum_{j=0}^{|E|-1} 2 \cdot 4^j \).

---

**NP-Completeness (cont)**

**SUBSET-SUM**

**Instance:** A set of positive integers \( S = \{s_1,s_2,\ldots,s_k\} \) and an integer \( t \).

**Question:** Does \( S \) have a subset \( S' \) which totals exactly to \( t \)?

**Examples:** \( S = \{2,9,3,5,11,24\} \) and \( t = 23 \)

YES: \( 11+9+3=23 \)

\( S = \{2,9,3,5,11,24\} \) and \( t = 15 \)

NO

---

**NP-Completeness (cont)**

**VC \( \leq_p \) SUBSET-SUM**

**Example:**

\((G,3)_{\text{VC}}\)

\[(S,t)_{\text{SUBSET-SUM}}\]

Radix 4 representation of \( S \)

\[
\begin{array}{|c|c|c|c|c|c|c|c|c|c|}
\hline
V & E & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \\
\hline
a & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\
\hline
b & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\
\hline
c & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\
\hline
d & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\
\hline
e & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\
\hline
f & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\
\hline
\end{array}
\]

**Example:**

\[
\begin{array}{|c|c|c|c|c|c|c|c|c|c|}
\hline
E & 3 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \\
\hline
\end{array}
\]

Radix 4 representation of \( S \)
NP-Completeness (cont)

**VC \leq_p SUBSET - SUM**

Step 2: Show that \((G, m) \in I_{VC} \iff f(G, m) \in I_{\text{SUBSET-SUM}}\)

- \(G\) has a vertex cover of size \(\leq m\) \(\iff\)
- \(S\) has a subset \(S'\) that totals to \(t\)

**Proof:** Suppose \(V'\) is a vertex cover of size \(m\) in \(G\).

(If \(G\) has a vertex cover of size \(\leq m\), then it has one of size \(m\).)

Construct a subset \(S' \subseteq S\) as follows:

- for each \(v_j \in V'\), add \(s_j\) to \(S'\)
- for each \(e_j\) with only one endpoint in \(V'\), add \(s_{j + |V|} \) to \(S'\)

---

NP-Completeness (cont)

**VC \leq_p SUBSET - SUM**

**Proof:** Represent each of the integers in \(S'\) in radix 4.

By construction each digit position from 0 to \(|E| - 1\) has exactly two 1’s among all the integers in \(S'\) since each edge has either one or two endpoints in \(V'\).

Since \(V'\) has size exactly \(m\), there are exactly \(m\) integers in \(S'\) which are \(\geq 4^{\lfloor |E| \rfloor}\).

The integers in \(S'\) total to \(m4^{\lfloor |E| \rfloor} + \sum_{j=0}^{\lfloor |E| \rfloor - 1} 2 \cdot 4'^j = t\).

Now suppose \(S\) has a subset \(S'\) totals to \(t\).

---

NP-Completeness (cont)

**VC \leq_p SUBSET - SUM**

**Proof:** Construct a subset of vertices \(V'\):

- for each \(s_i \in S'\) with \(1 \leq i \leq |V|\), add \(v_i\) to \(V'\)

Since the integers in \(S'\) total \(t\) and there are no carries possible among the least significant \(|E|\) digit positions, for each of these digit positions there must be exactly two integers in \(S'\) with 1’s in that position.

One of these 1’s must be from an \(s_i \in S'\) with \(1 \leq i \leq |V|\).

For each edge \(e_j = (v_a, v_b)\) either \(s_a\) or \(s_b\) \(\in S'\).

For each edge \(e_j = (v_a, v_b)\) either \(v_a\) or \(v_b\) \(\in V'\).

---

NP-Completeness (cont)

**VC \leq_p SUBSET - SUM**

**Proof:** \(V'\) is a vertex cover for \(G\).

Since the integers in \(S'\) total to \(t\) and there are no carries possible among the least significant \(|E|\) digit positions, there must be exactly \(m\) integers in \(S' \geq 4^{\lfloor |E| \rfloor}\).

All \(s_i \in S\) with \(s_i \geq 4^{\lfloor |E| \rfloor}\) have \(1 \leq i \leq |V|\).

\(V'\) is a vertex cover for \(G\) of size \(m\).

QED
**NP-Completeness (cont)**

**VC ≤ₚ SUBSET - SUM**

Step 3: Show that \( f \) is computable in polynomial time.

If \( G \) has \( a \) vertices and \( b \) edges then \( f(G,k)=(S,t) \) and \( S \) has \( a+b \) integers and each of these integers has \( 2b+2 \) bits.

The integer \( t \) can be encoded in less than \( 2b+\lg a \) bits.

The integers can be constructed in \( O(ab) \) time by first building the incidence matrix for \( G \).

\( f \) is computable in polynomial time.

Finished \( \text{VC} \leq_p \text{SUBSET - SUM} \)

---

**CIRCUIT-SAT**

**Instance:** A boolean combinational circuit with one output, composed of AND, OR, and NOT gates.

**Question:** Is there an input that causes the circuit to output 1?

**Examples:**

- **YES**
- **NO**

---

**SUBSET - SUM ≤ₚ CIRCUIT - SAT**

Step 1: Construct \( f : \{(S,t)\} \rightarrow \{C\} \)

Given \( (S,t) \) where \( S = \{s_1,s_2,\ldots,s_k\} \) and \( m \) is the maximum number of bits in any \( s_i \) in \( S \) and \( t \),

Create a circuit for adding together \( k \) \( m \)-bit integers.

Size \( \theta(k(m+k)) \)

---

**SUBSET - SUM ≤ₚ CIRCUIT - SAT**

For each \( s_i \in S \), create a new boolean variable (input) \( x_i \) and a circuit which outputs

\[
\begin{align*}
0 & \quad \text{when } x_i = 0 \\
1 & \quad \text{when } x_i = 1
\end{align*}
\]

Each has size \( \theta(m) \)

Total size \( \theta(mk) \)
Create a circuit which compares an $m+k-1$ bit integer with $t$ and outputs 1 only when they are equal

Size $\theta(m+k)$

Combine circuits as follows:

Size $\theta(k(m+k))$

Step 2: Show that $(S,t) \in L_{\text{SUBSET-SUM}}$ if and only if $S$ has a subset $S'$ that totals to $t$. There are inputs for $C$ that make its output 1.

Proof (sketch): Suppose $S' \subseteq S$ that totals to $t$. Set the value of $C$’s inputs as follows:

\[ x_i = \begin{cases} 1 & \text{if } s_i \in S' \\ 0 & \text{if } s_i \notin S' \end{cases} \]

Since $S'$ totals to $t$ the output of $C$ will be 1.

Proof (sketch cont): Now suppose $\bar{X}$ is an input for $C$ which makes its output 1.

Construct $S'$ as follows: Let $S' = \{ s_i | x_i = 1 \text{ in } \bar{X} \}$

Then $S'$ totals to $t$ since the output of $C$ is only 1 when $\sum_{s_i \in S'} s_i = t$

Step 3: $f$ is computable in polynomial time since the size of $C$ is $O(m(k+m))$ and it can be constructed in time $O(m(k+m))$.

Finished $\text{SUBSET-SUM} \leq_p \text{CIRCUIT-SAT}$
**NP-Completeness (cont)**

**CIRCUIT - SAT \( \leq_p \) 3SAT**

Step 1: Construct \( f : \{C\} \rightarrow \{\phi\} \)

Given a circuit \( C \), first break any \( n \)-input gates for \( n > 2 \) into 2-input gates.

Create a clause for each gate as follows:

\[
\begin{align*}
(x \lor y \lor \bar{z})(x \lor \bar{y} \lor \bar{z})(\bar{x} \lor y \lor \bar{z})(\bar{x} \lor \bar{y} \lor z)
\end{align*}
\]

\[
\begin{align*}
(x \lor z)(\bar{x} \lor z)
\end{align*}
\]

\[
\begin{align*}
(x \lor y \lor \bar{z})(x \lor \bar{y} \lor \bar{z})(\bar{x} \lor y \lor z)(\bar{x} \lor \bar{y} \lor z)
\end{align*}
\]

Each clause will be \( 0 \) for an inconsistent set of values on the gate inputs and output.
3SAT $\leq_p$ 3SAT

The final $\phi$ in 3-CNF form is satisfiable $\Leftrightarrow C$ is satisfiable.

The size of the final $\phi$ is $O(|C|)$.

All the steps used to construct $\phi$ are $O(|C|)$, so $f$ is polynomial time computable.

Finished $\text{Circuit-SAT} \leq_p 3\text{SAT}$

NP-Completeness (cont)

Summary

$3\text{SAT} \leq_p \text{Clique}$

$\text{Clique} \leq_p \text{VC}$

$\text{VC} \leq_p \text{Subset-Sum}$

$\text{Subset-Sum} \leq_p \text{Circuit-SAT}$

$\text{Circuit-SAT} \leq_p \text{3SAT}$

If anyone of these problems is in $P$, then they all are.