Problem definition: Vertex Cover

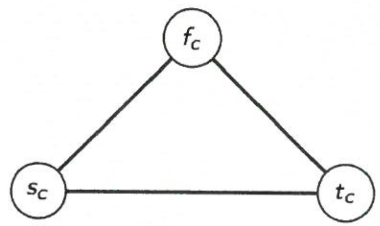
Given a graph $G = (N, E)$ and an integer k, does there exist a subset S of at most k vertices in N such that each edge in E is touched by at least one vertex in S?

- No polynomial-time algorithm is known
- Is in NP (short and verifiable solution):
  - If a graph is "k-coverable", there exists k-subset $S \subseteq N$ such that each edge is touched by at least one of its vertices
  - Length of S encoding is polynomial in length of G encoding
  - There exists a polynomial-time algorithm that verifies whether S is a valid k-cover
    - Verify that $|S| \leq k$
    - Verify that, for any $(u, v) \in E$, either $u \in S$ or $v \in S$

NP-completeness

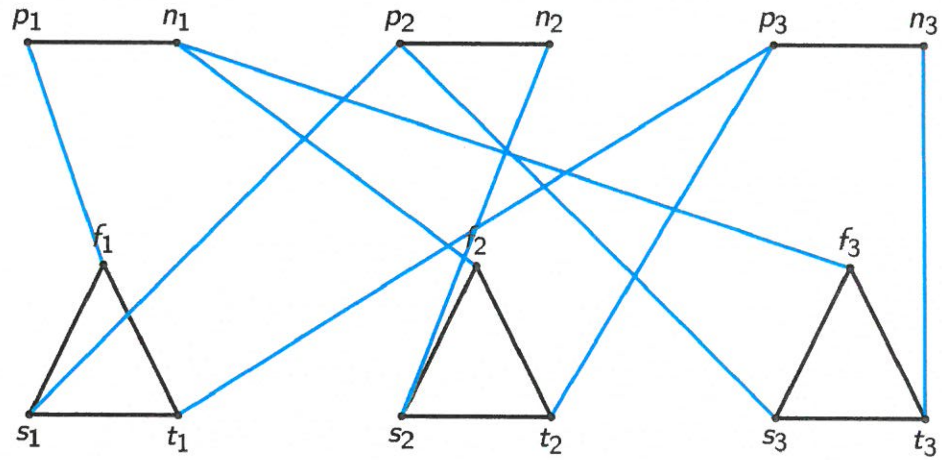
- Reduction of 3–Sat to Vertex Cover:
- Technique: component design
  - For each variable a gadget (that is, a sub-graph) representing its truth value
  - For each clause a gadget representing the fact that one of its literals is true
  - Edges connecting the two kinds of gadget
- Gadget for variable u:

  - One vertex is sufficient and necessary to cover the edge
- Gadget for clause c:



  - Two vertices are sufficient and necessary to cover the three edges
- $k = n + 2m$, where n is number of variables and m is number of clauses

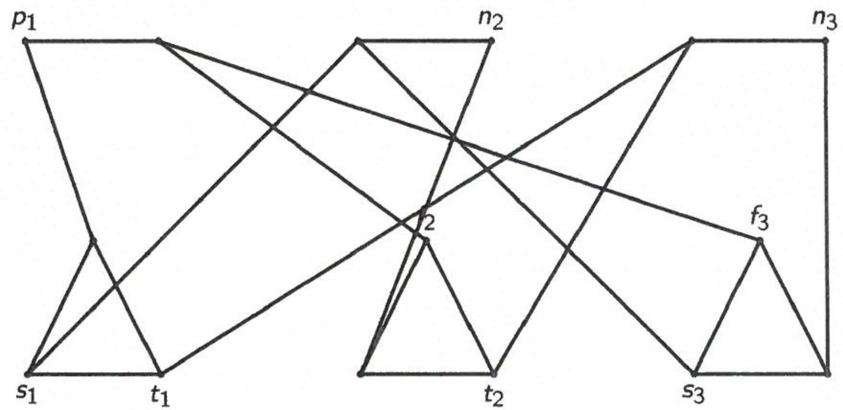
- Connections between variable and clause gadgets
  - First (second, third) vertex of clause gadget connected to vertex corresponding to first (second, third) literal of clause
  - Example: $(x_1 \vee x_2 \vee x_3) \wedge (\overline{x_1} \vee \overline{x_2} \vee x_3) \wedge (\overline{x_1} \vee x_2 \vee \overline{x_3})$



  - Idea: if first (second, third) literal of clause is true (taken), then first (second, third) vertex of clause gadget has not to be taken in order to cover the edges between the gadgets

Proof of correctness

- Show that Formula satisfiable ⇒ Vertex cover exists:
  - Include in S all vertices corresponding to true literals
  - For each clause, include in S all vertices of its gadget but the one corresponding to its first true literal
  - Example
    - $(x_1 \vee x_2 \vee x_3) \wedge (\overline{x_1} \vee \overline{x_2} \vee x_3) \wedge (\overline{x_1} \vee x_2 \vee \overline{x_3})$
    - x_1 true, x_2 and x_3 false



- Show that Vertex cover exists ⇒ Formula satisfiable:
  - Assign value true to variables whose p-vertices are in S
  - Since $k = n + 2m$, for each clause at least one edge connecting its gadget to the variable gadgets is covered by a variable vertex
    - Clause is satisfied

Problem definition: Subset Sum

Given a (multi)set A of integer numbers and an integer number s, does there exist a subset of A such that the sum of its elements is equal to s?

- No polynomial-time algorithm is known
- Is in NP (short and verifiable certificates):
  - If a set is "good", there exists subset $B \subseteq A$ such that the sum of the elements in B is equal to s
  - Length of B encoding is polynomial in length of A encoding
  - There exists a polynomial-time algorithm that verifies whether B is a set of numbers whose sum is s:
    - Verify that $\sum_{a \in B} a = s$

NP-completeness

- Reduction of 3–Sat to Subset Sum:
  - n variables x_i and m clauses c_j
- For each variable x_i, construct numbers t_i and f_i of $n+m$ digits:
  - The i-th digit of t_i and f_i is equal to 1
  - For $n+1 \leq j \leq n+m$, the j-th digit of t_i is equal to 1 if x_i is in clause c_{j-n}
  - For $n+1 \leq j \leq n+m$, the j-th digit of f_i is equal to 1 if $\overline{x_i}$ is in clause c_{j-n}
  - All other digits of t_i and f_i are 0
- Example:
  $(x_1 \vee x_2 \vee x_3) \wedge (\overline{x_1} \vee \overline{x_2} \vee x_3) \wedge (\overline{x_1} \vee x_2 \vee \overline{x_3}) \wedge (x_1 \vee \overline{x_2} \vee x_3)$

	i			j			
Number	1	2	3	1	2	3	4
t_1	1	0	0	1	0	0	1
f_1	1	0	0	0	1	1	0
t_2	0	1	0	1	0	1	0
f_2	0	1	0	0	1	0	1
t_3	0	0	1	1	1	0	1
f_3	0	0	1	0	0	1	0

- For each clause c_j, construct numbers x_j and y_j of $n+m$ digits:
  - The $(n+j)$-th digit of x_j and y_j is equal to 1
  - All other digits of x_i and y_j are 0
- Example:
  $(x_1 \vee x_2 \vee x_3) \wedge (\overline{x_1} \vee \overline{x_2} \vee x_3) \wedge (\overline{x_1} \vee x_2 \vee \overline{x_3}) \wedge (x_1 \vee \overline{x_2} \vee x_3)$

	i			j			
Number	1	2	3	1	2	3	4
x_1	0	0	0	1	0	0	0
y_1	0	0	0	1	0	0	0
x_2	0	0	0	0	1	0	0
y_2	0	0	0	0	1	0	0
x_3	0	0	0	0	0	1	0
y_3	0	0	0	0	0	1	0
x_4	0	0	0	0	0	0	1
y_4	0	0	0	0	0	0	1

- Finally, construct a sum number s of $n+m$ digits:
  - For $1 \leq j \leq n$, the j-th digit of s is equal to 1
  - For $n+1 \leq j \leq n+m$, the j-th digit of s is equal to 3

Proof of correctness

- Show that Formula satisfiable ⇒ Subset exists:
  - Take t_i if x_i is true
  - Take f_i if x_i is false
  - Take x_j if number of true literals in c_j is at most 2
  - Take y_j if number of true literals in c_j is 1
  - Example
    - $(x_1 \vee x_2 \vee x_3) \wedge (\overline{x_1} \vee \overline{x_2} \vee x_3) \wedge (\overline{x_1} \vee x_2 \vee \overline{x_3}) \wedge (x_1 \vee \overline{x_2} \vee x_3)$
    - All variables true

	i			j			
Number	1	2	3	1	2	3	4
t_1	1	0	0	1	0	0	1
t_2	0	1	0	1	0	1	0
t_3	0	0	1	1	1	0	1
x_2	0	0	0	0	1	0	0
y_2	0	0	0	0	1	0	0
x_3	0	0	0	0	0	1	0
y_3	0	0	0	0	0	1	0
x_4	0	0	0	0	0	0	1
s	1	1	1	3	3	3	3

- Show that Subset exists $\Rightarrow$ Formula satisfiable:
  - Assign value true to x_i if t_i is in subset
  - Assign value false to x_i if f_i is in subset
  - Exactly one number per variable must be in the subset
    - Otherwise one of first n digits of the sum is greater than 1
  - Assignment is consistent
  - At least one variable number corresponding to a literal in a clause must be in the subset
    - Otherwise one of next m digits of the sum is smaller than 3
  - Each clause is satisfied