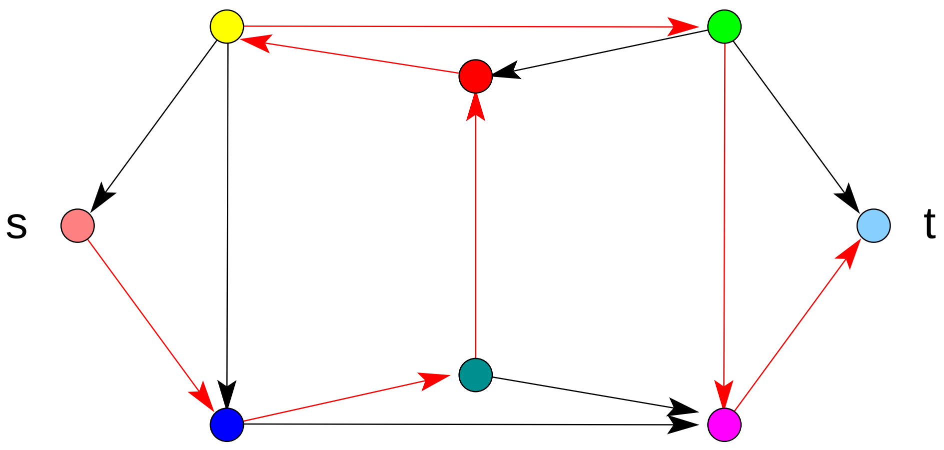
- HAMPATH

  $\{ \langle G, s, t \rangle \mid$ directed graph G has Hamilton path from s to t $\}$



- COMPOSITES $\{ n \in \mathbb{N} \mid \exists p, q > 1 : n = pq \}$

- length of input

```
for i=2 to n-1 do
  if i*(n/i)=n
    return true
  else
    return false
  fi
od
```

- language decided by NTM

  non-deterministic Turing-machine $N = (Q, \Sigma, \delta, q_0)$

  relation $\delta \subseteq (Q \times \Sigma) \times (Q \cup \{q_{\mathsf{yes}}, q_{\mathsf{no}}\} \times \Sigma \times \{\mathsf{L}, \mathsf{R}\})$

  decided language $\mathcal{L}(N) = \{\ x \in \Sigma^* \mid q_0 x \vdash^* y q_{\mathsf{yes}} z\ \}$

- language verified by DTM

  deterministic Turing-machine $D = (Q, \Sigma, \delta, q_0)$

  function $\delta\colon (Q \times \Sigma) \to (Q \cup \{q_{\mathsf{yes}}, q_{\mathsf{no}}\} \times \Sigma \times \{\mathsf{L}, \mathsf{R}\})$

  verified language $\mathcal{L}'(D) = \{\ x \in \Sigma^* \mid \exists c \in \Sigma^*\colon c q_0 x \vdash^* y q_{\mathsf{yes}} z\ \}$

- the class NP

  languages decided by a halting NTM in polynomial time

  languages verified by a halting DTM in polynomial time

- Theorem

polynomially verifying DTM $=$ polynomially deciding NTM

$[\Rightarrow]$ construct deciding NTM as follows:

guess certificate; run verifier

acceptance iff certificate exists

polynomial running time

$[\Leftarrow]$ construct verifying DTM as follows:

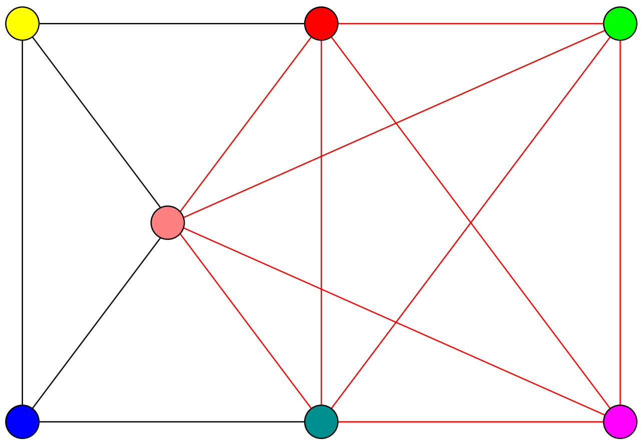
take scheduler for deciding NTM as candiate certificate

certificate exists iff NTM has accepting branch

polynomial running time

- CLIQUE

  $\{\ \langle G, k\rangle \mid$ undirected graph G has a k-clique $\}$



- SUBSET-SUM

  $\{\ \langle S, t\rangle \mid S \subseteq \mathbb{N}$ finite multiset, $\exists S' \subseteq S : \sum_{y \in S'} y = t\ \}$

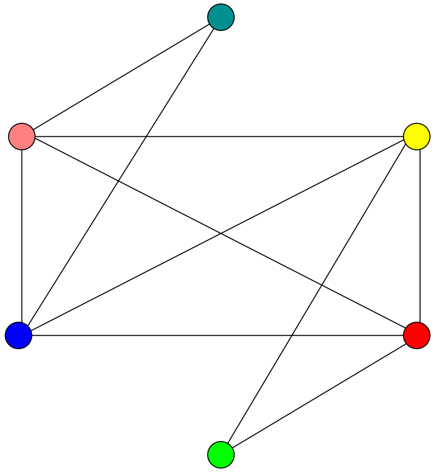
- SAT $\{\ \phi \mid \phi$ satisfiable propositional formula $\}$

- 3SAT $\{\ \phi \mid \phi$ satisfiable 3cnf-formula $\}$

  $(x_1 \vee \bar{x}_2 \vee \bar{x}_3) \wedge (x_3 \vee \bar{x}_5 \vee x_6) \wedge (x_3 \vee \bar{x}_6 \vee x_4) \wedge (x_4 \vee x_5 \vee x_6)$

- VERTEX-COVER

  $\{\ \langle G, k \rangle \mid$ undirected graph G has a k-cover $\}$



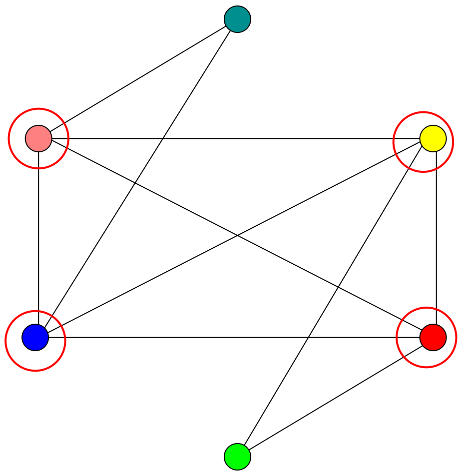
- SAT $\{ \phi \mid \phi$ satisfiable propositional formula $\}$

- 3SAT $\{ \phi \mid \phi$ satisfiable 3cnf-formula $\}$

$(x_1 \vee \bar{x}_2 \vee \bar{x}_3) \wedge (x_3 \vee \bar{x}_5 \vee x_6) \wedge (x_3 \vee \bar{x}_6 \vee x_4) \wedge (x_4 \vee x_5 \vee x_6)$

- VERTEX-COVER

$\{ \langle G, k \rangle \mid$ undirected graph G has a k-cover $\}$

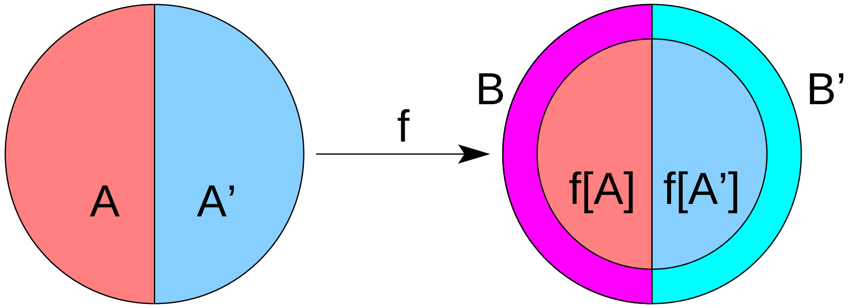


- $A \leq_P B$

  language A polynomial reduces to language B:

  $$\forall w \in \Sigma^*\colon w \in A \iff f(w) \in B$$

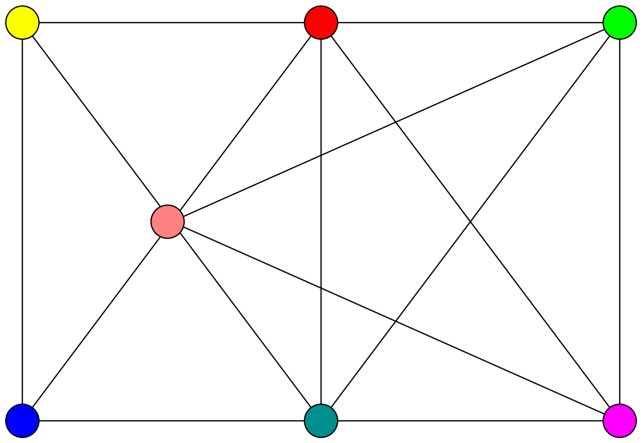
  for some polynomial $f\colon \Sigma^* \to \Sigma^*$



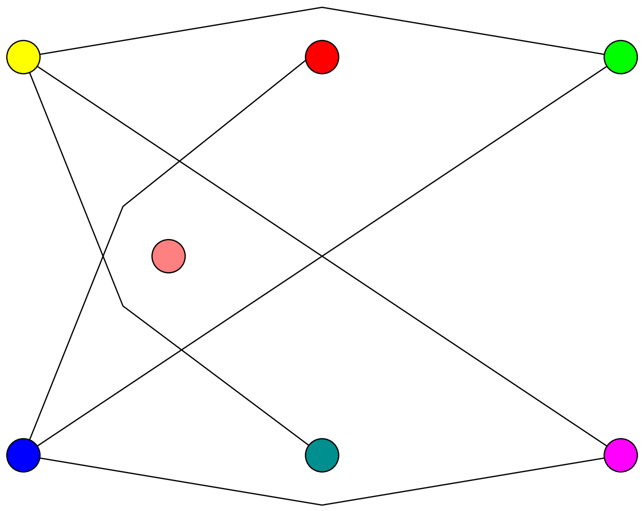
- CLIQUE $\leq_P$ VERTEX-COVER

  $f\colon \langle G, k\rangle \mapsto \langle G^c, n-k\rangle$

  G^c complementary graph, n number of nodes



graph G

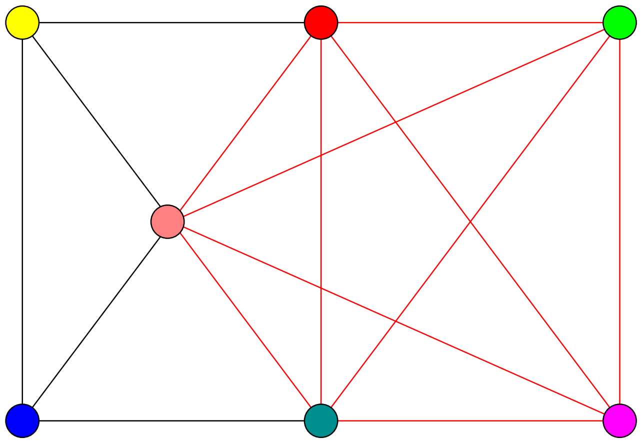


complementary graph G^c

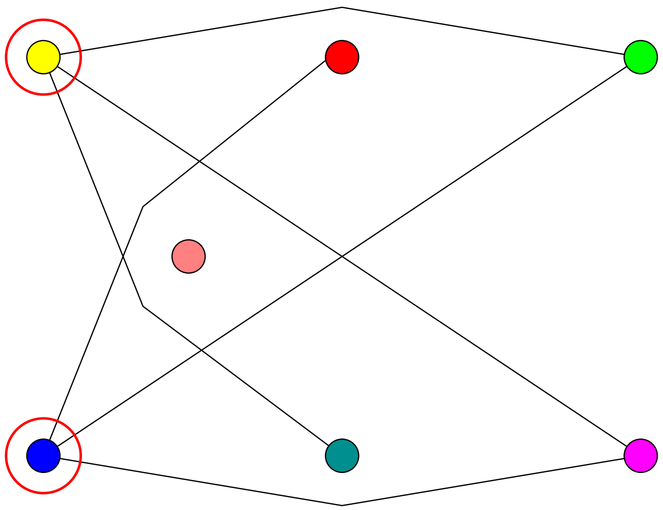
- CLIQUE $\leq_P$ VERTEX-COVER

  $f\colon \langle G, k\rangle \mapsto \langle G^c, n-k\rangle$

  G^c complementary graph, n number of nodes



graph G



complementary graph G^c

- DOUBLE-SAT

  $\{ \phi \mid \phi$ has a least two satisfying assignments $\}$

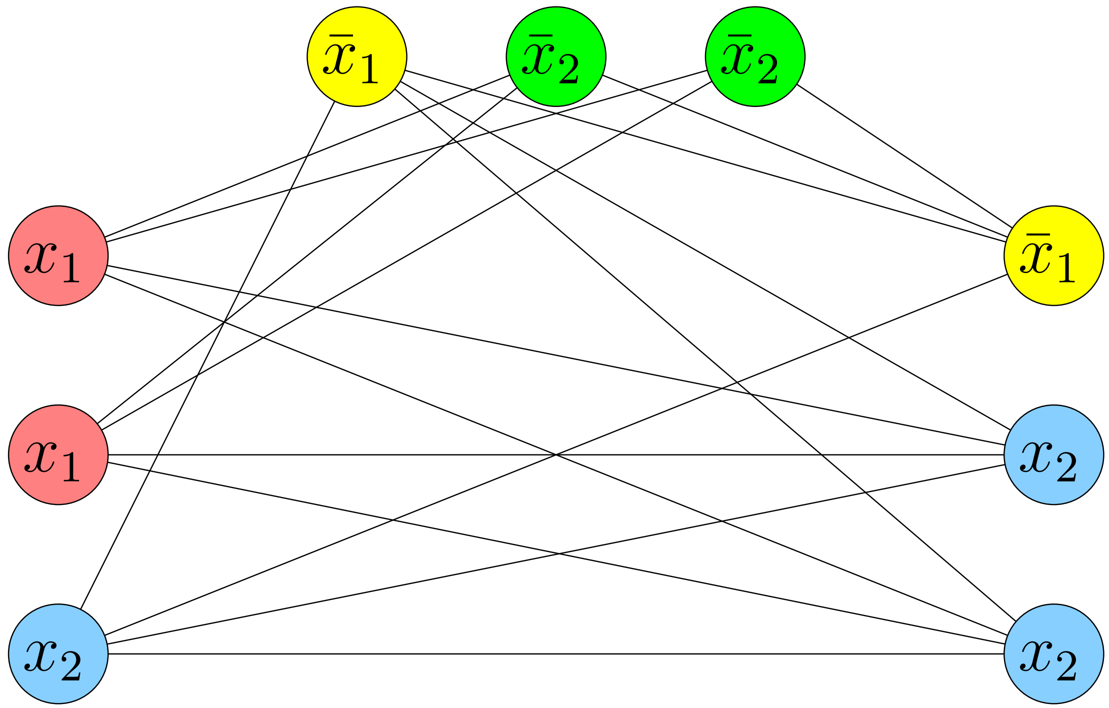
- SAT $\leq_P$ DOUBLE-SAT

- HALF-CLIQUE

  $\{ G \mid$ graph G with n nodes has a $n/2$-clique $\}$

- CLIQUE $\leq_P$ HALF-CLIQUE

- 3SAT $\leq_P$ CLIQUE



graph for $(x_1 \vee x_1 \vee x_2) \wedge (\bar{x}_1 \vee \bar{x}_2 \vee \bar{x}_2) \wedge (\bar{x}_1 \vee x_2 \vee x_2)$

- SUBSET-SUM

  $\{ \langle S, t\rangle \mid S \subseteq \mathbb{N}$ finite multiset, $\exists S' \subseteq S : \sum_{y\in S'} y = t \}$

- PARTITIONING

  $\{ S \mid S \subseteq \mathbb{N}$ finite multiset,

  $\exists S_1, S_2 \subseteq S\colon S_1 \cup S_2 = S \wedge S_1 \cap S_2 = \emptyset \wedge$

  $\sum_{x\in S_1} x = \sum_{y\in S_2} y \}$

- SUBSETSUM $\leq_P$ PARTITIONING

  special elements of weight $2s - t$ and $s + t$

$\neq$-SAT $= \{\ \phi \in$ 3CNF $\mid \phi$ has a $\neq$-assignment $\}$

in each clause both a true and a false literal

- 3SAT $\leq_P$ $\neq$-SAT

replace $a_i \vee b_i \vee c_i$ by $(a_i \vee b_i \vee y_i) \wedge (\bar{y}_i \vee c_i \vee z)$

where y_i and z are fresh and z shared among all clauses

$(x_1 \vee x_1 \vee x_2) \wedge (\bar{x}_1 \vee \bar{x}_2 \vee \bar{x}_2) \wedge (\bar{x}_1 \vee x_2 \vee x_2)$

translates into
$(x_1 \vee x_1 \vee y_1) \wedge (\bar{y}_1 \vee x_2 \vee z) \wedge (\bar{x}_1 \vee \bar{x}_2 \vee y_2) \wedge (\bar{y}_2 \vee \bar{x}_2 \vee z) \wedge (\bar{x}_1 \vee x_2 \vee y_3) \wedge (\bar{y}_3 \vee x_2 \vee z)$

if α is a $\neq$-assigment, then so is its conjugate $\bar{\alpha}$

- SET-SPLITTING

  $\{ \langle S, C \rangle \mid S$ finite set,

  $C = \{ C_1, \ldots, C_k \}$ collection subsets of S,

  $\exists \gamma \colon S \to \{ \mathtt{red}, \mathtt{blue} \}$:

  $\forall i, 1 \leq i \leq k \, \exists x, y \in C_i$:

  $\gamma(x) = \mathtt{red} \land \gamma(y) = \mathtt{blue} \}$

- $\neq$-SAT $\leq_P$ SET-SPLITTING