Cryptocomplexity II

Kryptokomplexität II

Sommersemester 2024

Chapter 9: Boolean Hierarchy over NP

Dozent: Prof. Dr. J. Rothe

HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

Outline of this Chapter

- Problems in DP
- Structure and Properties of the Boolean Hierarchy over NP
- Exact Graph Colorability

Reminder: Directed Hamilton Circuit

Definition

DIRECTED HAMILTON CIRCUIT (DHC):

Given: A directed graph $G = (V(G), E(G))$.

Question: Does there exist a *Hamilton cycle* in G, i.e., a sequence $(v_1, v_2, \ldots, v_n)$, $v_i \in V(G)$, $n = \|V(G)\|$, such that $(v_n, v_1) \in E(G)$ and $(v_i, v_{i+1}) \in E(G)$ for $1 \leq i < n$?

Theorem

DHC *is* NP-*complete.*

Proof: Has been presented in Kryptokomplexität I. ❑

Reminder: Hamilton Circuit

Definition

HAMILTON CIRCUIT (HC):

Given: An undirected graph $G = (V(G), E(G))$.

Question: Does there exist a *Hamilton cycle* in G, i.e., a sequence $(v_1, v_2, \ldots, v_n)$, $v_i \in V(G)$, $n = \|V(G)\|$, such that $\{v_n, v_1\} \in E(G)$ and $\{v_i, v_{i+1}\} \in E(G)$ for $1 \leq i < n$?

Theorem

HC *is* NP*-complete.*

Proof: (Kryptokomplexität I.) Hint: Reduction from DHC. ❑

Reminder: Traveling Salesperson Problem

Definition

TRAVELING SALESPERSON PROBLEM (TSP):

Given: A complete undirected graph $K_n = (V, E)$, a cost function $c : E \to \mathbb{N}$, and $k \in \mathbb{N}$.

Question: Does there exist a Hamilton cycle in K_n such that the sum of the edge costs is at most k?

Theorem

TSP *is* NP*-complete.*

Proof: TSP $\in$ NP is easy to see.

Reminder: TSP is NP-complete

TSP is NP-hard: We show $\mathrm{HC} \leq_{\mathrm{m}}^{\mathrm{p}} \mathrm{TSP}$.

Given an undirected graph $G = (V(G), E(G))$ with $V(G) = \{v_1, v_2, \ldots, v_n\}$, define

$$f(G) = (K_n, c, n),$$

where $K_n = (V, E)$, $V = \{1, 2, \ldots, n\}$, and for each edge $e = \{i, j\}$ of K_n:

$$c(\{i,j\}) = \begin{cases} 1 & \text{if } \{v_i, v_j\} \in E(G) \\ 2 & \text{otherwise.} \end{cases}$$

Clearly, $G \in \mathrm{HC}$ if and only if $f(G) \in \mathrm{TSP}$. ❑

Optimization and Search Variants of TSP

Definition

- MinTSP:

  Given: A complete undirected graph $K_n = (V, E)$ and a cost function $c : E \to \mathbb{N}$.

  Output: The minimum cost of a Hamilton cycle in K_n with respect to c.

- SearchTSP:

  Given: A complete undirected graph $K_n = (V, E)$ and a cost function $c : E \to \mathbb{N}$.

  Output: A Hamilton cycle in K_n having minimum cost with respect to c.

Exact Variant of the Traveling Salesperson Problem

Definition

EXACT TRAVELING SALESPERSON PROBLEM (EXACT-TSP):

Given: A complete undirected graph $K_n = (V, E)$, a cost function $c : E \to \mathbb{N}$, and $k \in \mathbb{N}$.

Question: Is it true that $tsp(K_n, c) = k$, where $tsp(K_n, c)$ denotes the length of an optimal tour in (K_n, c)?

Exact Variant of the Traveling Salesperson Problem

Fact

EXACT-TSP *is* NP-*hard.*

Proof: $\mathrm{HC} \leq_{\mathrm{m}}^{\mathrm{p}} \text{Exact-TSP}$ can be shown with the same reduction $f(G) = (K_n, c, n)$, where $K_n = (V, E)$ and $V = \{1, 2, \dots, n\}$, as in the previous proof:

$$G \in \mathrm{HC} \text{ if and only if } tsp(K_n, c) = n,$$

which proves the fact. ❑

Question: Is it true that EXACT-TSP $\in$ NP?

Exact Variant of the Traveling Salesperson Problem

Observation: $\textsc{Exact-TSP}$ can be written as:

$$
\begin{aligned}
\textsc{Exact-TSP} &= \{(K_n, c, k) \mid \cdots \text{ and } tsp(K_n, c) = k\} \\
&= \{(K_n, c, k) \mid \cdots \text{ and } tsp(K_n, c) \leq k\} \cap \\
&\quad\; \{(K_n, c, k) \mid \cdots \text{ and } tsp(K_n, c) \geq k\}
\end{aligned}
$$

Note that:

- $\{(K_n, c, k) \mid \cdots \text{ and } tsp(K_n, c) \leq k\}$ is in NP and
- $\{(K_n, c, k) \mid \cdots \text{ and } tsp(K_n, c) \geq k\}$ is in coNP.

DP: "Difference NP"

Definition

$$\begin{aligned} \mathrm{DP} &= \{L \mid L = A \cap B \text{ and } A \in \mathrm{NP} \text{ and } B \in \mathrm{coNP}\} \\ &= \{L \mid L = A - B \text{ and } A, B \in \mathrm{NP}\}. \end{aligned}$$

Lemma

$$\mathrm{DP} = \{L \mid L = L_1 - L_2 \textit{ and } L_1, L_2 \in \mathrm{NP} \textit{ and } L_2 \subseteq L_1\}.$$

Proof: The inclusion "$\supseteq$" is trivially true.

For the inclusion "$\subseteq$", let $L \in \mathrm{DP}$, i.e., $L = A - B$ for $A, B \in \mathrm{NP}$.

Define $L_1 = A$ and $L_2 = A \cap B$. Then L_1 and L_2 are in NP (because NP is $\cap$-closed), $L_2 \subseteq L_1$, and $L = A - B = A - (A \cap B) = L_1 - L_2$. ❑

Exact Variants of Other NP-complete Problems

Analogously to EXACT-TSP, exact variants can be defined for many NP-complete problems:

- EXACT VERTEX COVER,
- EXACT INDEPENDENT SET,
- EXACT CLIQUE,
- EXACT DOMINATING SET,
- EXACT-k-COLOR,
- ...

Exact Independent Set

Definition

EXACT INDEPENDENT SET (XIS):

Given: An undirected graph $G = (V, E)$ and $k \in \mathbb{N}$.

Question: Is it true that $mis(G) = k$, where $mis(G)$ denotes the size of a maximum independent set in G?

Theorem

EXACT-TSP, EXACT INDEPENDENT SET, *and the other exact variants of* NP*-complete problems are* DP*-complete.* **without proof**

The proof for EXACT-k-COLOR will be sketched later on.

SAT-UNSAT

Definition

$\mathrm{SAT\text{-}UNSAT}$:

Given: A pair (φ, φ') of boolean formulas in 3-CNF.

Question: Is it true that $\varphi \in \mathrm{SAT}$ and $\varphi' \notin \mathrm{SAT}$?

Theorem

$\mathrm{SAT\text{-}UNSAT}$ *is* DP*-complete.*

Proof:

1. $\mathrm{SAT\text{-}UNSAT}$ is in DP because $\mathrm{SAT\text{-}UNSAT} = A \cap B$ with

$$\begin{aligned} A &= \{(\varphi, \varphi') \mid \varphi \in \mathrm{SAT}\} \quad \text{is in NP and} \\ B &= \{(\varphi, \varphi') \mid \varphi' \notin \mathrm{SAT}\} \quad \text{is in coNP.} \end{aligned}$$

SAT-UNSAT

2. SAT-UNSAT is DP-hard: Let L be an arbitrary set in DP.

   Then there are sets $A \in \mathrm{NP}$ and $B \in \mathrm{coNP}$ such that

$$L = A \cap B.$$

   Since SAT is NP-complete, there are reductions

$$A \leq_{\mathrm{m}}^{\mathrm{p}} \mathrm{SAT} \qquad \text{via } f \in \mathrm{FP} \text{ and}$$
$$\overline{B} \leq_{\mathrm{m}}^{\mathrm{p}} \mathrm{SAT} \qquad \text{via } g \in \mathrm{FP}.$$

   Then $L \leq_{\mathrm{m}}^{\mathrm{p}} \mathrm{SAT\text{-}UNSAT}$ via $h(x) = (f(x), g(x))$, since:

$$\begin{aligned} x \in L &\iff x \in A \text{ and } x \in B \\ &\iff f(x) \in \mathrm{SAT} \text{ and } g(x) \notin \mathrm{SAT} \\ &\iff h(x) \in \mathrm{SAT\text{-}UNSAT}. \quad ❑ \end{aligned}$$

Critical Problems in DP

- Minimal-3-UNSAT:

  Given: A boolean formula φ in 3-CNF.

  Question: Is it true that φ is unsatisfiable, yet removing any clause from φ makes it satisfiable?

- Minimal-3-Uncolorability:

  Given: An undirected graph G.

  Question: Is it true that G is not 3-colorable, yet removing any one of its vertices makes it 3-colorable?

- Maximal Non-Hamilton Circuit:

  Given: An undirected graph G.

  Question: Is it true that G has no Hamilton cycle, yet adding any one edge to G creates one?

Critical Problems in DP

Papadimitriou & Yannakakis (JCSS 1984) introduced DP to capture the complexity of problems that are

- known to be NP-hard or coNP-hard,
- but not known to be in NP or coNP.

Critical problems tend to be extremely elusive and very hard to tackle.

Papadimitriou & Yannakakis (JCSS 1984) write:

> *"This difficulty seems to reflect the extremely delicate and deep structure of critical problems—too delicate to sustain any of the known reduction methods. One way to understand this is that critical graphs is usually the object of hard theorems."*

Critical Problems in DP

Theorem (Papadimitriou & Wolfe (JCSS 1988))

MINIMAL-3-UNSAT *is* DP*-complete.* **without proof**

Theorem (Cai & Meyer (SICOMP 1987))

MINIMAL-3-UNCOLORABILITY *is* DP*-complete.* **without proof**

Theorem (Papadimitriou & Wolfe (JCSS 1988))

MAXIMAL NON-HAMILTON CIRCUIT *is* DP*-complete.* **without proof**

Unique Solution Problems in DP

Definition

UNIQUE SAT:

Given: A boolean formula φ.

Question: Does there exist a unique satisfying assignment for φ?

Theorem

UNIQUE SAT *is* coNP*-hard and in* DP*.*

Proof: Excercise. ❑

Remark: It is still open whether UNIQUE SAT is DP-complete.

Boolean Hierarchy over NP

Definition (Boolean Hierarchy over NP)

- For classes $\mathscr{C}$ and $\mathscr{D}$ of sets, define:

$$\begin{aligned} \mathscr{C} \wedge \mathscr{D} &= \{A \cap B \,|\, A \in \mathscr{C} \text{ and } B \in \mathscr{D}\}; \\ \mathscr{C} \vee \mathscr{D} &= \{A \cup B \,|\, A \in \mathscr{C} \text{ and } B \in \mathscr{D}\}. \end{aligned}$$

- The *boolean hierarchy over* NP is inductively defined by:

$$\begin{aligned} \mathrm{BH}_0(\mathrm{NP}) &= \mathrm{P}, \\ \mathrm{BH}_1(\mathrm{NP}) &= \mathrm{NP}, \\ \mathrm{BH}_2(\mathrm{NP}) &= \mathrm{NP} \wedge \mathrm{coNP} = \mathrm{DP}, \\ \mathrm{BH}_k(\mathrm{NP}) &= \mathrm{BH}_{k-2}(\mathrm{NP}) \vee \mathrm{BH}_2(\mathrm{NP}) \quad \text{for each } k \geq 3, \text{ and} \\ \mathrm{BH}(\mathrm{NP}) &= \bigcup_{k \geq 0} \mathrm{BH}_k(\mathrm{NP}). \end{aligned}$$

Boolean Hierarchy over NP

Theorem (Cai et al. (SICOMP 1988))

For each $k \geq 1$,

$$\mathrm{BH}_k(\mathrm{NP}) = \left\{ A_1 - A_2 - \cdots - A_k \;\middle|\; \begin{array}{l} A_1, A_2, \ldots, A_k \in \mathrm{NP} \textit{ and} \\ A_k \subseteq A_{k-1} \subseteq \cdots \subseteq A_1 \end{array} \right\},$$

where we agree by convention that parentheses may be omitted in such set differences:

$$A_1 - A_2 - \cdots - A_{k-1} - A_k = A_1 - (A_2 - (\cdots - (A_{k-1} - A_k) \cdots)).$$

without proof

Boolean Hierarchy over NP: Inclusion Structure

Theorem (Cai et al. (SICOMP 1988))

For each $k \geq 0$,

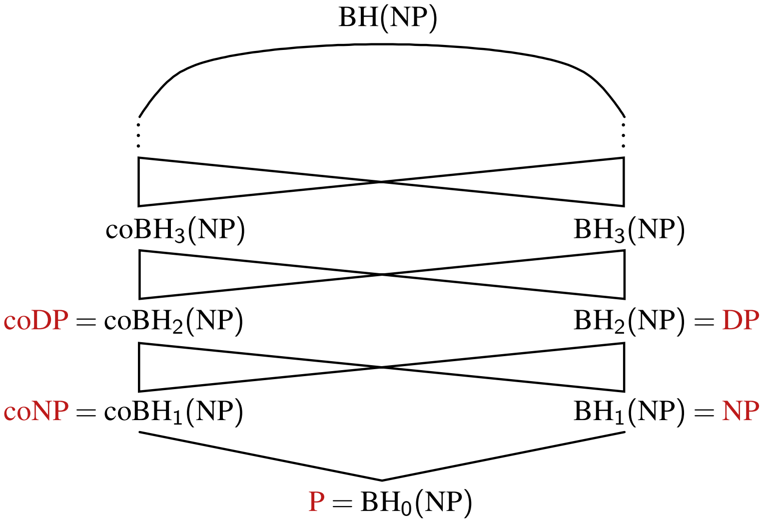
$$\mathrm{BH}_k(\mathrm{NP}) \subseteq \mathrm{BH}_{k+1}(\mathrm{NP}) \quad \textit{and} \quad \mathrm{coBH}_k(\mathrm{NP}) \subseteq \mathrm{coBH}_{k+1}(\mathrm{NP})$$

and, hence,

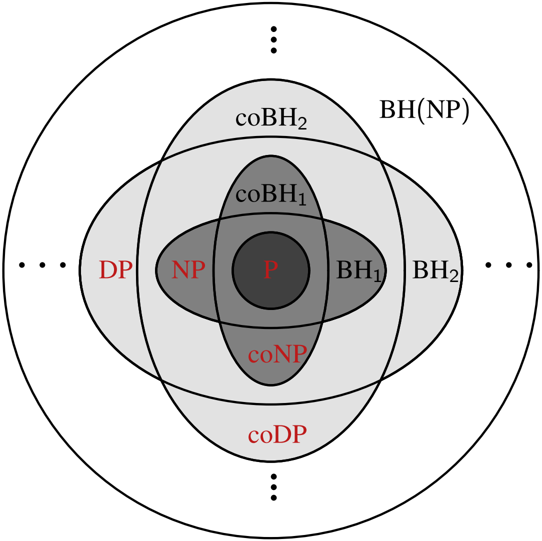
$$\mathrm{BH}_k(\mathrm{NP}) \cup \mathrm{coBH}_k(\mathrm{NP}) \subseteq \mathrm{BH}_{k+1}(\mathrm{NP}).$$

Proof: Follows immediately from the definitions. ❑

Boolean Hierarchy over NP (Hasse Diagram)



Boolean Hierarchy over NP (Venn Diagram)



Boolean Hierarchy over NP: Upward Collapse

Theorem (Cai et al. (SICOMP 1988))

1. *For each* $k \geq 0$, *if* $\mathrm{BH}_k(\mathrm{NP}) = \mathrm{BH}_{k+1}(\mathrm{NP})$, *then*

$$\mathrm{BH}_k(\mathrm{NP}) = \mathrm{coBH}_k(\mathrm{NP}) = \mathrm{BH}_{k+1}(\mathrm{NP}) = \mathrm{coBH}_{k+1}(\mathrm{NP}) = \cdots = \mathrm{BH}(\mathrm{NP}).$$

2. *For each* $k \geq 1$, *if* $\mathrm{BH}_k(\mathrm{NP}) = \mathrm{coBH}_k(\mathrm{NP})$, *then*

$$\mathrm{BH}_k(\mathrm{NP}) = \mathrm{coBH}_k(\mathrm{NP}) = \mathrm{BH}_{k+1}(\mathrm{NP}) = \mathrm{coBH}_{k+1}(\mathrm{NP}) = \cdots = \mathrm{BH}(\mathrm{NP}).$$

Boolean Hierarchy over NP: Upward Collapse

Proof:

1. Suppose that $\mathrm{BH}_k(\mathrm{NP}) = \mathrm{BH}_{k+1}(\mathrm{NP})$ is true for some fixed $k \geq 0$.

   We prove by induction on n:

   $$(\forall n \geq k)\,[\mathrm{BH}_n(\mathrm{NP}) = \mathrm{coBH}_n(\mathrm{NP}) = \mathrm{BH}_{n+1}(\mathrm{NP})]. \qquad (1)$$

   The induction base, $n = k$, follows immediately from the previous theorem and the hypothesis $\mathrm{BH}_k(\mathrm{NP}) = \mathrm{BH}_{k+1}(\mathrm{NP})$:

   $$\mathrm{coBH}_k(\mathrm{NP}) \subseteq \mathrm{BH}_{k+1}(\mathrm{NP}) = \mathrm{BH}_k(\mathrm{NP}),$$

   which immediately implies $\mathrm{coBH}_k(\mathrm{NP}) = \mathrm{BH}_k(\mathrm{NP})$.

   The induction hypothesis says that (1) is true for some $n \geq k$.

   We have to show that $\mathrm{BH}_{n+1}(\mathrm{NP}) = \mathrm{BH}_{n+2}(\mathrm{NP})$. By an argument as in the induction base, this also implies $\mathrm{BH}_{n+1}(\mathrm{NP}) = \mathrm{coBH}_{n+1}(\mathrm{NP})$.

Boolean Hierarchy over NP: Upward Collapse

Let X be any set in $\mathrm{BH}_{n+2}(\mathrm{NP})$.

Thus, there exist sets $A_1, A_2, \ldots, A_{n+2}$ in NP such that

$$A_{n+2} \subseteq A_{n+1} \subseteq \cdots \subseteq A_1 \quad \text{and} \quad X = A_1 - A_2 - \cdots - A_{n+2}.$$

Let $Y = A_2 - A_3 - \cdots - A_{n+2}$. Thus, $Y \in \mathrm{BH}_{n+1}(\mathrm{NP})$.

By induction hypothesis, Y is contained in $\mathrm{BH}_n(\mathrm{NP}) = \mathrm{BH}_{n+1}(\mathrm{NP})$.

Hence, $Y = B_1 - B_2 - \cdots - B_n$, for suitable NP sets $B_1, B_2, \ldots, B_n$ satisfying $B_n \subseteq B_{n-1} \subseteq \cdots \subseteq B_1$.

By our choice of the sets A_i, we have $Y \subseteq A_1$, which implies $Y \cap A_1 = Y$.

It follows that

$$Y \quad = \quad (B_1 \cap A_1) - (B_2 \cap A_1) - \cdots - (B_n \cap A_1).$$

Boolean Hierarchy over NP: Upward Collapse

Each of the sets $B_i \cap A_1$ is in NP, since NP is closed under intersection.

Consequently,

$$X \;=\; A_1 - Y = A_1 - (B_1 \cap A_1) - (B_2 \cap A_1) - \cdots - (B_n \cap A_1),$$

is a set in $\mathrm{BH}_{n+1}(\mathrm{NP})$, where

$$(B_n \cap A_1) \subseteq (B_{n-1} \cap A_1) \subseteq \cdots \subseteq (B_1 \cap A_1) \subseteq A_1,$$

which concludes the induction and proves (1).

Boolean Hierarchy over NP: Upward Collapse

2. Suppose that $\mathrm{BH}_k(\mathrm{NP}) = \mathrm{coBH}_k(\mathrm{NP})$ is true for some fixed $k \geq 1$.

   We show that this supposition implies $\mathrm{BH}_{k+1}(\mathrm{NP}) = \mathrm{BH}_k(\mathrm{NP})$, thus reducing the second statement to the first statement of the theorem.

   Let $X = A_1 - A_2 - \cdots - A_{k+1}$ be a set in $\mathrm{BH}_{k+1}(\mathrm{NP})$, where $A_1, A_2, \ldots, A_{k+1}$ are sets in NP satisfying that $A_{k+1} \subseteq A_k \subseteq \cdots \subseteq A_1$.

   Hence, $Y = A_2 - A_3 - \cdots - A_{k+1}$ is a set in $\mathrm{BH}_k(\mathrm{NP})$.

   By our supposition, Y is in $\mathrm{coBH}_k(\mathrm{NP}) = \mathrm{BH}_k(\mathrm{NP})$.

   Thus, $\overline{Y}$ is a set in $\mathrm{BH}_k(\mathrm{NP})$.

   Let $B_1, B_2, \ldots, B_k$ be sets in NP such that

$$\overline{Y} = B_1 - B_2 - \cdots - B_k \quad \text{and} \quad B_k \subseteq B_{k-1} \subseteq \cdots \subseteq B_1.$$

Boolean Hierarchy over NP: Upward Collapse

Again, since NP is closed under intersection, each of the sets $A_1 \cap B_i$, $1 \leq i \leq k$, is in NP.

Furthermore, $A_1 \cap B_k \subseteq A_1 \cap B_{k-1} \subseteq \cdots \subseteq A_1 \cap B_1$.

Hence,

$$X = A_1 - Y = A_1 \cap \overline{Y} = (A_1 \cap B_1) - (A_1 \cap B_2) - \cdots - (A_1 \cap B_k)$$

is a set in $\mathrm{BH}_k(\mathrm{NP})$, which proves that

$$\mathrm{BH}_{k+1}(\mathrm{NP}) = \mathrm{BH}_k(\mathrm{NP}),$$

and the argument given in the proof of the first statement of the theorem applies to prove the collapse $\mathrm{BH}_k(\mathrm{NP}) = \mathrm{BH}(\mathrm{NP})$. ❑

Boolean Hierarchy over NP: Complete Problems

Definition

D_k-SAT:

Given: A tuple $(H_1, H_2, \ldots, H_k)$ of boolean formulas in CNF.

Question: Does there exist an i such that $H_1, \ldots, H_{2i-1} \in \mathrm{SAT}$ and $H_{2i}, \ldots, H_k \notin \mathrm{SAT}$?

Remark: Special cases:

- $k = 1$: D_1-$\mathrm{SAT} = \mathrm{SAT}$ is NP-complete.
- $k = 2$: D_2-$\mathrm{SAT} = \mathrm{SAT}$-$\mathrm{UNSAT}$ is DP-complete.

Theorem

For each $k \geq 1$, D_k-SAT is $\mathrm{BH}_k(\mathrm{NP})$-complete. **without proof**

Boolean Hierarchy over NP: Complete Problems

Definition D_k-INDEPENDENT SET (D_k-IS):

Given: An undirected graph $G = (V, E)$ and a tuple $(m_1, m_2, \ldots, m_k)$ of positive integers.

Question: Is it true that:

- if k is even then $0 < m_1 \leq m_2 < m_3 \leq m_4 < \cdots < m_{k-1} \leq m_k < \|V\|$ and

$$mis(G) \in [m_1, m_2] \cup [m_3, m_4] \cup \cdots \cup [m_{k-1}, m_k]?$$

- if k is odd then $0 < m_1 \leq m_2 < m_3 \leq m_4 < \cdots \leq m_{k-1} < m_k \leq \|V\|$ and

$$mis(G) \in [m_1, m_2] \cup [m_3, m_4] \cup \cdots \cup [m_k, \|V\|]?$$

Boolean Hierarchy over NP: Complete Problems

Remark: Special cases:

- $k = 1$: $\mathrm{D}_1\text{-}\mathrm{IS} = \mathrm{IS}$ is NP-complete.
- $k = 2$ and $m_1 = m_2$: $\mathrm{D}_2\text{-}\mathrm{IS} = \mathrm{XIS}$ is DP-complete.

Theorem

For each $k \geq 1$, $\mathrm{D}_k\text{-}\mathrm{IS}$ is $\mathrm{BH}_k(\mathrm{NP})$-complete. **without proof**

Wagner's Tool for Proving DP-Hardness

Lemma (Wagner, TCS 1987)

Let A be some NP*-complete problem and let B be an arbitrary problem. If there exists a polynomial-time computable function f such that, for all input strings x_1 and x_2 for which $x_2 \in A$ implies $x_1 \in A$, we have that*

$$(x_1 \in A \wedge x_2 \notin A) \iff f(x_1, x_2) \in B,$$

then B is DP*-hard.*

- Has been applied to prove DP-completeness of, e.g.,
  - XIS, EXACT-7-COLOR, etc. (Wagner, TCS 1987),
  - EXACT-4-COLOR (Rothe, IPL 2006).
- Analogues for all levels of the boolean hierarchy and $\mathrm{P}_{||}^{\mathrm{NP}}$, e.g.,
  - DODGSON WINNER is $\mathrm{P}_{||}^{\mathrm{NP}}$-complete (Hemaspaandra et al., J.ACM 1997)

Wagner's Tool for Proving $\mathrm{BH}_{2k}(\mathrm{NP})$-Hardness

Lemma (Wagner, TCS 1987)

Let A be some NP-complete problem, B be an arbitrary problem, and $k \geq 1$ a fixed integer. If there exists a polynomial-time computable function f such that, for all input strings $x_1, x_2, \ldots, x_{2k}$ for which

$$(\forall j : 1 \leq j < 2k)\ [x_{j+1} \in A \Rightarrow x_j \in A],$$

we have that

$$\|\{i \mid x_i \in A\}\| \text{ is odd} \iff f(x_1, x_2, \ldots, x_{2k}) \in B, \tag{2}$$

then B is $\mathrm{BH}_{2k}(\mathrm{NP})$-hard.

Proof: Relatively easy to show and thus omitted. ❑

Wagner's Tool for Proving $\mathrm{BH}_{2k-1}(\mathrm{NP})/\mathrm{coBH}_{2k}(\mathrm{NP})/\mathrm{coBH}_{2k-1}(\mathrm{NP})$-Hardness

Remark:

- Replacing "$2k$" by "$2k-1$" in the lemma above yields an analogous criterium for $\mathrm{BH}_{2k-1}(\mathrm{NP})$-Hardness.
- Replacing "odd" by "even" yields an analogous criterium for $\mathrm{coBH}_{2k}(\mathrm{NP})$- and $\mathrm{coBH}_{2k-1}(\mathrm{NP})$-Hardness, respectively.

Reminder: Graph Colorability

Definition

Let $G = (V(G), E(G))$ be an undirected graph.

- A *k-coloring of G* is a mapping $V(G) \to \{1, 2, \ldots, k\}$.
- A k-coloring ψ of G is called *legal* if for any two vertices x and y in $V(G)$, if $\{x, y\} \in E(G)$ then $\psi(x) \neq \psi(y)$.
- The *chromatic number of G*, denoted by $\chi(G)$, is the smallest number k such that G is legally k-colorable.

Reminder: Graph Colorability

Definition

For fixed $k \geq 1$, define

$$k\text{-}\textsc{Color} = \{G \mid G \text{ is a graph with } \chi(G) \leq k\}.$$

Example:

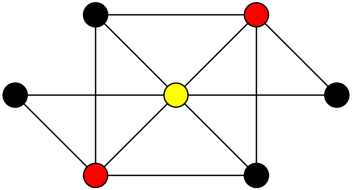


Figure: A 3-colorable graph

Exact Graph Colorability

Definition

For fixed $k \geq 1$, define

$$\textsc{Exact-}k\textsc{-Color} = \{ G \mid G \text{ is a graph with } \chi(G) = k \}.$$

Example:

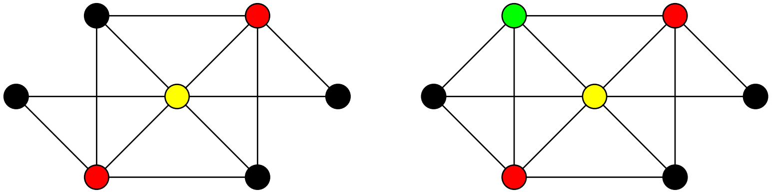


Figure: A graph in $\textsc{Exact-3-Color}$ (left) and in $\textsc{Exact-4-Color}$ (right)

Generalized Exact Graph Colorability

Definition

For fixed $j \geq 1$, let $M_j \subseteq \mathbb{N}$ be a given set of j non-consecutive integers and define

$$\text{EXACT-}M_j\text{-COLOR} = \{G \mid G \text{ is a graph with } \chi(G) \in M_j\}.$$

Remark: For $j = 1$ with $M_1 = \{k\}$, we write EXACT-k-COLOR instead of EXACT-M_1-COLOR $=$ EXACT-$\{k\}$-COLOR.

Theorem (Wagner, TCS 1987)

For fixed $k \geq 1$, let $M_k = \{6k+1, 6k+3, \ldots, 8k-1\}$. EXACT-$M_k$-COLOR is $\mathrm{BH}_{2k}(\mathrm{NP})$-complete. In particular, for $k = 1$ (i.e., $M_1 = \{7\}$), EXACT-7-COLOR is DP-complete. **without proof**

Generalized Exact Graph Colorability

Lemma

There exists a polynomial-time computable function σ that $\leq_{m}^{p}$-reduces $\mathrm{3\text{-}SAT}$ to 3-Color and satisfies the following two properties:

$$\varphi \in \mathrm{3\text{-}SAT} \quad \Rightarrow \quad \chi(\sigma(\varphi)) = 3; \tag{3}$$

$$\varphi \notin \mathrm{3\text{-}SAT} \quad \Rightarrow \quad \chi(\sigma(\varphi)) = 4. \tag{4}$$

Proof: Use standard reduction $\mathrm{3\text{-}SAT} \leq_{m}^{p}$ 3-Color (next slides). ❑

Lemma (Guruswami and Khanna, CCC-2000)

There exists a polynomial-time computable function ρ that $\leq_{m}^{p}$-reduces $\mathrm{3\text{-}SAT}$ to 3-Color and satisfies the following two properties:

$$\varphi \in \mathrm{3\text{-}SAT} \quad \Rightarrow \quad \chi(\rho(\varphi)) = 3; \tag{5}$$

$$\varphi \notin \mathrm{3\text{-}SAT} \quad \Rightarrow \quad \chi(\rho(\varphi)) = 5. \tag{6}$$

Reminder: 3-$\textsc{Color}$ is NP-complete

Fact

2-$\textsc{Color}$ *is in* P. **without proof**

Theorem

3-$\textsc{Color}$ *is* NP*-complete.*

Proof:

1. 3-$\textsc{Color} \in \mathrm{NP}$ is easy to see.
2. 3-$\textsc{Color}$ is NP-hard: We show $3\text{-}\mathrm{SAT} \leq_{\mathrm{m}}^{\mathrm{p}} 3\text{-}\textsc{Color}$. Let

$$\varphi(x_1, x_2, \ldots, x_n) = C_1 \wedge C_2 \wedge \cdots \wedge C_m$$

be a given $3\text{-}\mathrm{SAT}$ instance with exactly three literals per clause.

Reminder: 3-Color is NP-complete

Define a reduction f mapping φ to the graph G constructed as follows. The vertex set of G is defined by

$$\begin{aligned} V(G) &= \{v_1, v_2, v_3\} \cup \{x_i, \neg x_i \mid 1 \leq i \leq n\} \\ &\cup \{y_{j,k} \mid 1 \leq j \leq m \text{ and } 1 \leq k \leq 6\}, \end{aligned}$$

where the x_i and $\neg x_i$ are vertices representing the literals x_i and their negations $\neg x_i$, respectively.

Reminder: 3-Color is NP-complete

The edge set of G is defined by

$$
\begin{aligned}
E(G) \;=\; & \{\{v_1,v_2\},\{v_2,v_3\},\{v_1,v_3\}\} \cup \{\{x_i,\neg x_i\} \mid 1 \le i \le n\} \\
& \cup \{\{v_3,x_i\},\{v_3,\neg x_i\} \mid 1 \le i \le n\} \\
& \cup \{\{a_j,y_{j,1}\},\{b_j,y_{j,2}\},\{c_j,y_{j,3}\} \mid 1 \le j \le m\} \\
& \cup \{\{v_2,y_{j,6}\},\{v_3,y_{j,6}\} \mid 1 \le j \le m\} \\
& \cup \{\{y_{j,1},y_{j,2}\},\{y_{j,1},y_{j,4}\},\{y_{j,2},y_{j,4}\} \mid 1 \le j \le m\} \\
& \cup \{\{y_{j,3},y_{j,5}\},\{y_{j,3},y_{j,6}\},\{y_{j,5},y_{j,6}\} \mid 1 \le j \le m\} \\
& \cup \{\{y_{j,4},y_{j,5}\} \mid 1 \le j \le m\},
\end{aligned}
$$

where $a_j, b_j, c_j \in \bigcup_{1 \le i \le n}\{x_i, \neg x_i\}$ are vertices representing the literals occurring in clause $C_j = (a_j \vee b_j \vee c_j)$.

Skeletal Structure of the Graph in $3\text{-SAT} \leq_m^p 3\text{-Color}$

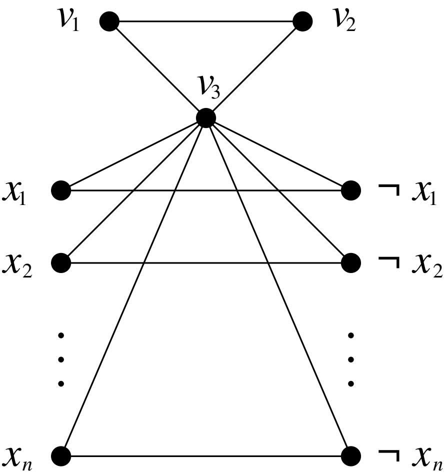


Figure: Skeletal Structure of the graph in $3\text{-SAT} \leq_m^p 3\text{-Color}$

Clause Graph in 3-SAT $\leq_m^p$ 3-COLOR

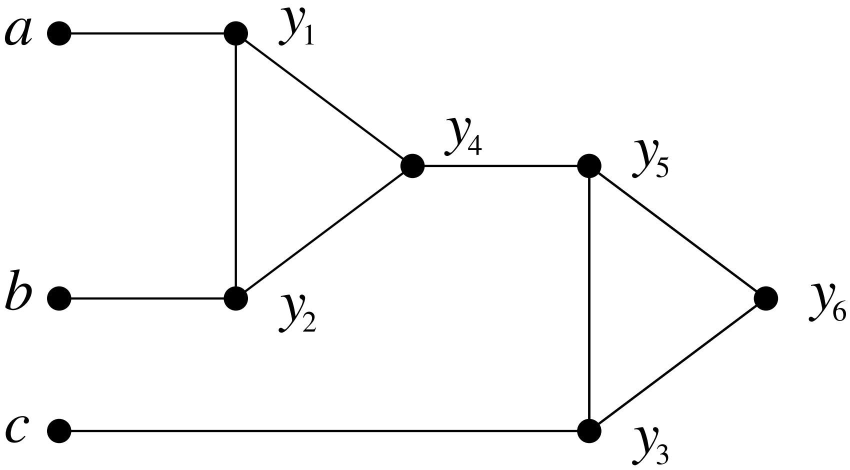


Figure: Graph H for clause $C = (a \vee b \vee c)$ in 3-SAT $\leq_m^p$ 3-COLOR

Properties of Clause Graph H in $\text{3-SAT} \leq_{\mathrm{m}}^{\mathrm{p}} \text{3-COLOR}$

1. Vertices x_i and $\neg x_i$ corresponding to the literals x_i and $\neg x_i$ are legally colored 1 ("true") or 2 ("false").

2. Any coloring of the vertices a, b, and c that assigns color 1 to one of a, b, and c can be extended to a legal 3-coloring of H that assigns color 1 to y_6. Thus, if $\varphi \in \text{3-SAT}$ then $G \in \text{3-COLOR}$.

3. If ψ is a legal 3-coloring of H with $\psi(a) = \psi(b) = \psi(c) = i$, then $\psi(y_6) = i$. Thus, if $\varphi \notin \text{3-SAT}$ then $G \notin \text{3-COLOR}$ because $\chi(\sigma(\varphi)) = \chi(G) = 4$.

It follows that

$$\varphi \in \text{3-SAT} \Longleftrightarrow f(\varphi) = G \in \text{3-COLOR}$$

Clearly, reduction f is polynomial-time computable. ❑

Guruswami–Khanna Reduction: Sketch

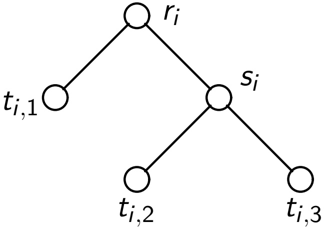


Figure: Tree-like structure S_i in the Guruswami–Khanna reduction

Guruswami–Khanna Reduction: Sketch

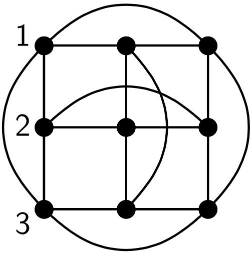


Figure: Basic template in the Guruswami–Khanna reduction

Guruswami–Khanna Reduction: Sketch

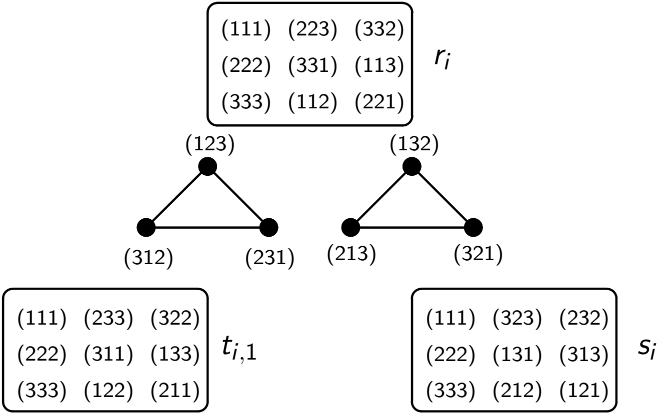


Figure: Connection pattern between the templates of a tree-like structure

Guruswami–Khanna Reduction: Sketch

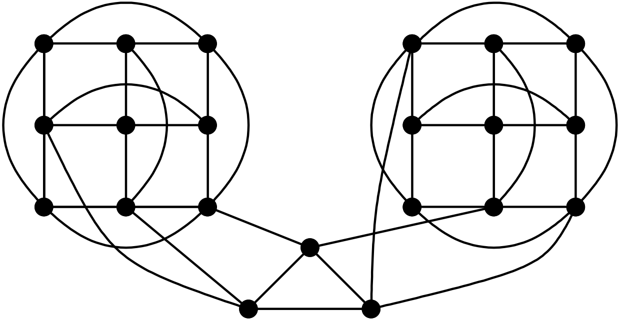


Figure: Gadget connecting two “leaves” of the “same row” kind

Guruswami–Khanna Reduction: Sketch

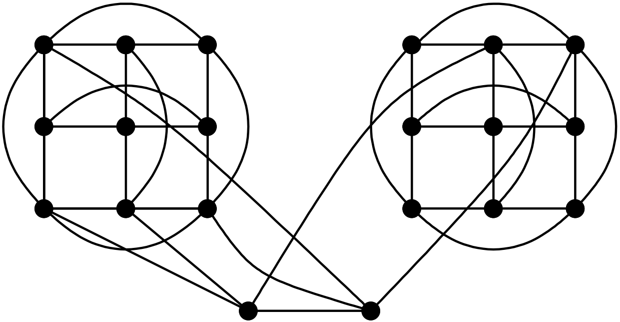


Figure: Gadget connecting two “leaves” of the “different rows” kind

Exact-4-Color is DP-complete

Theorem (Rothe, IPL 2001)

For fixed $k \geq 1$, let $M_k = \{3k+1, 3k+3, \ldots, 5k-1\}$.

- Exact-M_k-Color *is* $\mathrm{BH}_{2k}(\mathrm{NP})$*-complete.*
- *In particular, for $k = 1$ (i.e., $M_1 = \{4\}$),* Exact-4-Color *is* DP*-complete.*

Proof: Fix $k \geq 1$. Apply Wagner's Lemma with

- A being the NP-complete problem 3-SAT and
- B being the problem Exact-M_k-Color, where $M_k = \{3k+1, 3k+3, \ldots, 5k-1\}$.

Exact-4-Color is DP-complete

Let

- σ be the standard reduction from 3-SAT to 3-Color according to our previous lemma, and
- let ρ be the Guruswami–Khanna reduction from 3-SAT to 3-Color according to their lemma.

The *join operation on graphs*, denoted by $\bowtie$, is defined as follows: Given two disjoint graphs A and B, their join $A \bowtie B$ is the graph whose vertex and edge set, respectively, are:

$$\begin{aligned} V(A \bowtie B) &= V(A) \cup V(B); \\ E(A \bowtie B) &= E(A) \cup E(B) \cup \{\{a,b\} \mid a \in V(A) \text{ and } b \in V(B)\}. \end{aligned}$$

Note that $\chi(A \bowtie B) = \chi(A) + \chi(B)$ and $\bowtie$ is an associative operation.

Exact-4-Color is DP-complete

Let $\varphi_1, \varphi_2, \ldots, \varphi_{2k-1}, \varphi_{2k}$ be $2k$ given boolean formulas satisfying that $\varphi_{j+1} \in \mathrm{3\text{-}SAT}$ implies $\varphi_j \in \mathrm{3\text{-}SAT}$ for each j with $1 \leq j < 2k$.

Define $2k$ graphs $H_1, H_2, \ldots, H_{2k-1}, H_{2k}$ as follows.

For each i with $1 \leq i \leq k$, define

$$H_{2i-1} = \rho(\varphi_{2i-1}) \quad \text{and} \quad H_{2i} = \sigma(\varphi_{2i}).$$

By (3), (4), (5), and (6) from our previous two lemmas, it follows that

$$\chi(H_j) = \begin{cases} 3 & \text{if } 1 \leq j \leq 2k \text{ and } \varphi_j \in \mathrm{3\text{-}SAT} \\ 4 & \text{if } j = 2i \text{ for some } i \in \{1, 2, \ldots, k\} \text{ and } \varphi_j \notin \mathrm{3\text{-}SAT} \\ 5 & \text{if } j = 2i-1 \text{ for some } i \in \{1, 2, \ldots, k\} \text{ and } \varphi_j \notin \mathrm{3\text{-}SAT}. \end{cases} \tag{7}$$

EXACT-4-COLOR is DP-complete

For each i with $1 \leq i \leq k$, define the graph G_i to be the disjoint union of the graphs H_{2i-1} and H_{2i}.

Thus, $\chi(G_i) = \max\{\chi(H_{2i-1}), \chi(H_{2i})\}$, for each i, $1 \leq i \leq k$.

The construction of our reduction f is completed by defining

$$f(\langle \varphi_1, \varphi_2, \ldots, \varphi_{2k-1}, \varphi_{2k} \rangle) = G,$$

where the graph G is the join of the graphs $G_1, G_2, \ldots, G_k$.

Thus,

$$\chi(G) = \sum_{i=1}^{k} \chi(G_i) = \sum_{i=1}^{k} \max\{\chi(H_{2i-1}), \chi(H_{2i})\}. \tag{8}$$

Exact-4-Color is DP-complete

It follows from our construction that:

$$\|\{i \mid \varphi_i \in \text{3-SAT}\}\| \text{ is odd}$$

$$\iff (\exists i : 1 \leq i \leq k)[\varphi_1, \ldots, \varphi_{2i-1} \in \text{3-SAT and } \varphi_{2i}, \ldots, \varphi_{2k} \notin \text{3-SAT}]$$

$$\overset{(7),(8)}{\iff} (\exists i : 1 \leq i \leq k)\left[\begin{array}{rcl} \sum_{j=1}^{k} \chi(G_j) & = & 3(i-1)+4+5(k-i) \\ & = & 5k-2i+1 \end{array}\right]$$

$$\overset{(8)}{\iff} \chi(G) \in M_k = \{3k+1, 3k+3, \ldots, 5k-1\}$$

$$\iff f(\langle \varphi_1, \varphi_2, \ldots, \varphi_{2k-1}, \varphi_{2k} \rangle) = G \in \text{Exact-}M_k\text{-Color}.$$

Hence, the equivalence in Wagner's lemma is satisfied.

By Wagner's lemma, Exact-M_k-Color is $\text{BH}_{2k}(\text{NP})$-complete. ❑