Vereinfachungen von MERF

MERF (Wiederholung)

Instanz:

- Variablen $Y_1, \ldots, Y_n$ mit (endlichen) Wertebereichen $B_1, \ldots, B_n$
- Formel F, aufgebaut mit $\wedge$ und $\vee$ aus Termen der Form
  - $Y_i = a$
  - $Y_i \neq a$
  - $Y_i = Y_j$
  - $Y_i \neq Y_j$

Frage: Gibt es eine Variablenbelegung, die F wahr macht?

Vereinfachungen von MERF

MERF (Wiederholung)

Instanz:

- Variablen $Y_1, \ldots, Y_n$ mit (endlichen) Wertebereichen $B_1, \ldots, B_n$
- Formel F, aufgebaut mit $\wedge$ und $\vee$ aus Termen der Form
  - $Y_i = a$
  - $Y_i \neq a$
  - $Y_i = Y_j$
  - $Y_i \neq Y_j$

Frage: Gibt es eine Variablenbelegung, die F wahr macht?

Wird MERF leichter, wenn wir:

- Art der Terme beschränken?
- Wertebereiche der Variablen einschränken?
- nur spezielle Formeln erlauben?

SMERF - Simple Mehrwertige Erfüllbarkeit

SMERF

Instanz:

- Variablen $Y_1, \ldots, Y_n$ mit Wertebereichen $B_1, \ldots, B_n$
- Formel F, aufgebaut mit $\wedge$ und $\vee$ aus Termen der Form $Y_i = a$ (Terme der Form $Y_i \neq a$, $Y_i = Y_j$ und $Y_i \neq Y_j$ sind nicht erlaubt.)

Frage: Gibt es eine Variablenbelegung, die F wahr macht?

SMERF - Simple Mehrwertige Erfüllbarkeit

SMERF

Instanz:

- Variablen $Y_1, \ldots, Y_n$ mit Wertebereichen $B_1, \ldots, B_n$
- Formel F, aufgebaut mit $\wedge$ und $\vee$ aus Termen der Form $Y_i = a$ (Terme der Form $Y_i \neq a$, $Y_i = Y_j$ und $Y_i \neq Y_j$ sind nicht erlaubt.)

Frage: Gibt es eine Variablenbelegung, die F wahr macht?

Satz

SMERF *ist* NP-*vollständig.*

SMERF (Fortsetzung)

Beweis.

1. SMERF $\in$ NP: Rate nichtdet. Variablebelegung und verifiziere F.
2. MERF $\preccurlyeq_p$ SMERF
   - Brauchen: MERF Instanz $(Y_i, B_i, F) \mapsto$ SMERF Instanz (Y_i', B_i', F')

SMERF (Fortsetzung)

Beweis.

1. SMERF $\in$ NP: Rate nichtdet. Variablebelegung und verifiziere F.
2. MERF $\preccurlyeq_p$ SMERF
   - Brauchen: MERF Instanz $(Y_i, B_i, F) \mapsto$ SMERF Instanz (Y_i', B_i', F')

Beispiel

MERF Instanz:

- $Y_1 \in \{1, 2, 3\}, Y_2 \in \{3, 5, 7\}, Y_3 \in \{1, 2, 5\}, Y_4 \in \{1, 2, 3\}$
- $F = ((Y_1 = 2) \wedge (Y_3 = Y_4)) \vee ((Y_1 \neq 3) \wedge (Y_2 \neq Y_3))$

SMERF Instanz:

- $Y_1' \in \{1, 2, 3\}, Y_2' \in \{3, 5, 7\}, Y_3' \in \{1, 2, 5\}, Y_4' \in \{1, 2, 3\}$
- $F' = ((Y_1 = 2) \wedge ((Y_3 = 1 \wedge Y_4 = 1) \vee (Y_3 = 2 \wedge Y_4 = 2))) \vee$ $((Y_1 = 1 \vee Y_1 = 2) \wedge ((Y_2 = 3 \wedge Y_3 = 1) \vee (Y_2 = 3 \wedge Y_3 = 2) \vee \dots))$

SMERF (Fortsetzung)

Beweis.

1. SMERF $\in$ NP: Rate nichtdet. Variablebelegung und verifiziere F.
2. MERF $\preccurlyeq_p$ SMERF
   - Brauchen: MERF Instanz $(Y_i, B_i, F) \mapsto$ SMERF Instanz (Y_i', B_i', F')

SMERF (Fortsetzung)

Beweis.

1. SMERF $\in$ NP: Rate nichtdet. Variablebelegung und verifiziere F.
2. MERF $\preccurlyeq_p$ SMERF
   - Brauchen: MERF Instanz $(Y_i, B_i, F) \mapsto$ SMERF Instanz (Y_i', B_i', F')
   - Konstruktion. $\forall 1 \leq i, j \leq n$:
     - $Y_i' = Y_i,\ B_i' = B_i$,
     - $Y_i = Y_j$ wird ersetzt durch $F_{ij} = \bigvee_{a \in B_i \cap B_j} ((Y_i = a) \wedge (Y_j = a))$
     - $Y_i \neq a$ wird ersetzt durch $F_{ia} = \bigvee_{a' \neq a} (Y_i = a')$
     - $Y_i \neq Y_j$ wird ersetzt durch $D_{ij} = \bigvee_{(a,a') \in B_i \times B_j, a \neq a'} ((Y_i = a) \wedge (Y_j = a'))$
   - Es gilt: F erfüllbar $\Leftrightarrow$ F' erfüllbar

SMERF (Fortsetzung)

Beweis.

1. SMERF $\in$ NP: Rate nichtdet. Variablebelegung und verifiziere F.
2. MERF $\preccurlyeq_p$ SMERF
   - Brauchen: MERF Instanz $(Y_i, B_i, F) \mapsto$ SMERF Instanz (Y_i', B_i', F')
   - Konstruktion. $\forall 1 \leq i, j \leq n$:
     - $Y_i' = Y_i,\ B_i' = B_i,$
     - $Y_i = Y_j$ wird ersetzt durch $F_{ij} = \bigvee_{a \in B_i \cap B_j} ((Y_i = a) \wedge (Y_j = a))$
     - $Y_i \neq a$ wird ersetzt durch $F_{ia} = \bigvee_{a' \neq a} (Y_i = a')$
     - $Y_i \neq Y_j$ wird ersetzt durch $D_{ij} = \bigvee_{(a,a') \in B_i \times B_j, a \neq a'} ((Y_i = a) \wedge (Y_j = a'))$
   - Es gilt: F erfüllbar $\Leftrightarrow$ F' erfüllbar
   - Laufzeit: (Größe der MERF-Instanz sei g)
     - proportional zur Länge von F'
     - $|F_{ij}| \in \mathcal{O}(|B_i| + |B_j|) \in \mathcal{O}(g)$
     - $|F_{ia}| \in \mathcal{O}(|B_i|) \in \mathcal{O}(g)$
     - $|D_{ij}| \in \mathcal{O}(|B_i| \cdot |B_j|) \in \mathcal{O}(g^2)$
     - $\Rightarrow |F'| \in \mathcal{O}(|F| \cdot g^2) \in \mathcal{O}(g^3)$, polynomiell in g

$\square$

SAT - Boole'sche Erfüllbarkeit

SAT

Instanz: Boole'sche Formel F in Boole'schen Variablen
Beispiel: $(x_1 \wedge \neg x_2) \vee \neg(x_2 \vee x_3)$

Frage: Ist F erfüllbar, d.h. gibt es eine Wahrheitsbelegungen der Variablen, so dass F wahr ist?

SAT - Boole'sche Erfüllbarkeit

SAT

Instanz: Boole'sche Formel F in Boole'schen Variablen
Beispiel: $(x_1 \wedge \neg x_2) \vee \neg(x_2 \vee x_3)$

Frage: Ist F erfüllbar, d.h. gibt es eine Wahrheitsbelegungen der Variablen, so dass F wahr ist?

Satz

SAT *ist* NP-*vollständig.*

SAT(Fortsetzung)

Beweis.

1. SAT $\in$ NP: Rate nichtdet. Wahrheitsbelegungen und verifiziere F.
2. SMERF $\preccurlyeq_p$ SAT:
   - Wollen: $\mathrm{cod}(Y_1)\cdots\mathrm{cod}(Y_n)\$\,\mathrm{cod}(B_1)\cdots\mathrm{cod}(B_n)\$\,\mathrm{cod}(F') \mapsto \mathrm{cod}(F)$

SAT(Fortsetzung)

Beweis.

1. SAT $\in$ NP: Rate nichtdet. Wahrheitsbelegungen und verifiziere F.
2. SMERF $\preccurlyeq_p$ SAT:
   - Wollen: $\text{cod}(Y_1)\cdots\text{cod}(Y_n)\$\,\text{cod}(B_1)\cdots\text{cod}(B_n)\$\,\text{cod}(F') \mapsto \text{cod}(F)$
   - Konstruktion:
     - Variablen $X_{ib}, 1 \leq i \leq n, b \in B_i$ (X_{ib} kodiert $Y_i = b$)
     - F_1 entstehe aus F' indem wir Terme $Y_i = b$ durch X_{ib} ersetzen
     - Müssen $\forall i$ sicherstellen: genau eine der $X_{ib_1}, X_{ib_2}, \ldots, X_{ib_m}$ ist wahr
     - Dazu neue Variablen $D_i = \bigvee_{b \in B_i}(X_{ib} \wedge \bigwedge_{b' \in B_i, b' \neq b} \neg X_{ib'})$
     - Setze $F_2 = \bigwedge_{1 \leq i \leq n} D_i$
     - Dann $F = F_1 \wedge F_2$
   - Es gilt: F' erfüllbar $\Leftrightarrow$ F erfüllbar

SAT(Fortsetzung)

Beweis.

1. SAT $\in$ NP: Rate nichtdet. Wahrheitsbelegungen und verifiziere F.
2. SMERF $\preccurlyeq_p$ SAT:
   - Wollen: $\mathrm{cod}(Y_1)\cdots\mathrm{cod}(Y_n)\$\,\mathrm{cod}(B_1)\cdots\mathrm{cod}(B_n)\$\,\mathrm{cod}(F') \mapsto \mathrm{cod}(F)$
   - Konstruktion:
     - Variablen $X_{ib}, 1 \leq i \leq n, b \in B_i$ (X_{ib} kodiert $Y_i = b$)
     - F_1 entstehe aus F' indem wir Terme $Y_i = b$ durch X_{ib} ersetzen
     - Müssen $\forall i$ sicherstellen: genau eine der $X_{ib_1}, X_{ib_2}, \ldots, X_{ib_m}$ ist wahr
     - Dazu neue Variablen $D_i = \bigvee_{b \in B_i}(X_{ib} \wedge \bigwedge_{b' \in B_i, b' \neq b} \neg X_{ib'})$
     - Setze $F_2 = \bigwedge_{1 \leq i \leq n} D_i$
     - Dann $F = F_1 \wedge F_2$
   - Es gilt: F' erfüllbar $\Leftrightarrow$ F erfüllbar
   - Laufzeit: (Größe der SMERF-Instanz sei g)
     - proportional zur Länge von F
     - $|F_1| \in \mathcal{O}(|F'|) \in \mathcal{O}(g)$
     - $|D_i| \leq |B_i|^2 \in \mathcal{O}(g^2) \Rightarrow |F_2| \in \mathcal{O}(g^3)$
     - $\Rightarrow |F| \in \mathcal{O}(g^3)$, polynomiell in g

$\square$

3-SAT

3-SAT

Instanz: Boole'sche Formel F in KNF (konjuktiver Normalform) mit ≤ 3 Literalen pro Klausel, d.h.

- $F = K_1 \wedge \cdots \wedge K_i \wedge \cdots \wedge K_m$
- $K_i = (L_{i1} \vee \cdots \vee L_{ij} \vee \cdots \vee L_{it}), \forall 1 \leq i \leq m$
- Jedes Literal L_{ij} ist eine Variable X_k oder deren Negation $\overline{X_k}$

Beispiel: $(X_1 \vee \overline{X_2}) \wedge (X_2 \vee \overline{X_3} \vee X_4)$

Frage: Ist F erfüllbar, d.h. gibt es eine Wahrheitsbelegungen der Variablen, so dass F wahr ist?

3-SAT

3-SAT

Instanz: Boole'sche Formel F in KNF (konjuktiver Normalform) mit ≤ 3 Literalen pro Klausel, d.h.

- $F = K_1 \wedge \cdots \wedge K_i \wedge \cdots \wedge K_m$
- $K_i = (L_{i1} \vee \cdots \vee L_{ij} \vee \cdots \vee L_{it}), \forall 1 \leq i \leq m$
- Jedes Literal L_{ij} ist eine Variable X_k oder deren Negation $\overline{X_k}$

Beispiel: $(X_1 \vee \overline{X_2}) \wedge (X_2 \vee \overline{X_3} \vee X_4)$

Frage: Ist F erfüllbar, d.h. gibt es eine Wahrheitsbelegungen der Variablen, so dass F wahr ist?

Satz

3-SAT *ist* NP-*vollständig.*

3-SAT (Fortsetzung)

Beweis.

1. 3-SAT $\in$ NP: Rate nichtdet. Wahrheitsbelegungen und verifiziere F.
2. SAT $\preccurlyeq_p$ 3-SAT. Brauchen: SAT Formel $F \mapsto$ 3-SAT Formel F'

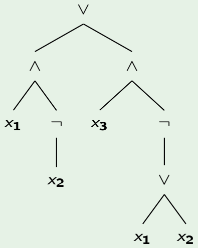
3-SAT (Fortsetzung)

Beweis.

1. 3-SAT $\in$ NP: Rate nichtdet. Wahrheitsbelegungen und verifiziere F.
2. SAT $\preccurlyeq_p$ 3-SAT. Brauchen: SAT Formel $F \mapsto$ 3-SAT Formel F'

Beispiel

- $F = (x_1 \wedge \neg x_2) \vee (x_3 \wedge \neg(x_1 \vee x_2))$



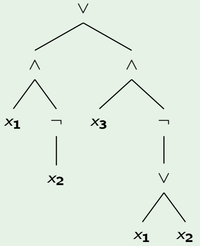
3-SAT (Fortsetzung)

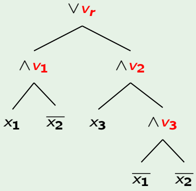
Beweis.

1. 3-SAT $\in$ NP: Rate nichtdet. Wahrheitsbelegungen und verifiziere F.
2. SAT $\preccurlyeq_p$ 3-SAT. Brauchen: SAT Formel $F \mapsto$ 3-SAT Formel F'

Beispiel

- $F = (x_1 \wedge \neg x_2) \vee (x_3 \wedge \neg(x_1 \vee x_2))$





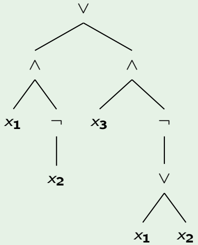
3-SAT (Fortsetzung)

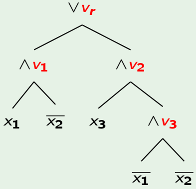
Beweis.

1. 3-SAT $\in$ NP: Rate nichtdet. Wahrheitsbelegungen und verifiziere F.
2. SAT $\preccurlyeq_p$ 3-SAT. Brauchen: SAT Formel $F \mapsto$ 3-SAT Formel F'

Beispiel

- $F = (x_1 \wedge \neg x_2) \vee (x_3 \wedge \neg(x_1 \vee x_2))$





- $v_r \wedge (v_r \Leftrightarrow v_1 \vee v_2) \wedge (v_1 \Leftrightarrow x_1 \vee \overline{x_2}) \wedge (v_2 \Leftrightarrow x_3 \vee v_3) \wedge (v_3 \Leftrightarrow \overline{x_1} \vee \overline{x_2})$
- in KNF bringen: z.B. $(A \Leftrightarrow P \vee Q) \equiv (\overline{A} \vee P \vee Q) \wedge (\overline{P} \vee A) \wedge (\overline{Q} \vee A))$

CLIQUE

CLIQUE

Instanz: $G = (V, E)$ ein ungerichter Graph, $k \in \mathbb{N}$

Frage: Besitzt G eine Clique der Größe k?, d.h: $\exists W \in \binom{V}{k} : \binom{W}{2} \subset E$?

CLIQUE

CLIQUE

Instanz: $G = (V, E)$ ein ungerichter Graph, $k \in \mathbb{N}$

Frage: Besitzt G eine Clique der Größe k?, d.h: $\exists W \in \binom{V}{k} : \binom{W}{2} \subset E$?

Satz

CLIQUE *ist* NP-*vollständig.*

CLIQUE

CLIQUE

Instanz: $G = (V, E)$ ein ungerichter Graph, $k \in \mathbb{N}$

Frage: Besitzt G eine Clique der Größe k?, d.h: $\exists W \in \binom{V}{k} : \binom{W}{2} \subset E$?

Satz

CLIQUE *ist* NP-*vollständig.*

Beweis.

1. CLIQUE $\in$ NP:
   - rate eine Lösung $W \in \binom{V}{k}$
   - verifiziere: $\forall u, v \in W,\ (u, v) \in E$ (Laufzeit $\mathcal{O}(|V|^2)$)

CLIQUE

CLIQUE

Instanz: $G = (V, E)$ ein ungerichter Graph, $k \in \mathbb{N}$

Frage: Besitzt G eine Clique der Größe k?, d.h: $\exists W \in \binom{V}{k} : \binom{W}{2} \subset E$?

Satz

CLIQUE *ist* NP-*vollständig.*

Beweis.

1. CLIQUE $\in$ NP:
   - rate eine Lösung $W \in \binom{V}{k}$
   - verifiziere: $\forall u, v \in W,\ (u, v) \in E$ (Laufzeit $\mathcal{O}(|V|^2)$)
2. CLIQUE $\preccurlyeq_p$ 3-SAT
   - Brauchen: 3-SAT Formel $F \mapsto$ CLIQUE Instanz (G_F, k_F)

CLIQUE (Fortsetzung)

Beweis.

1. CLIQUE $\in$ NP
2. 3-SAT $\preccurlyeq_p$ CLIQUE
   - Brauchen: 3-SAT Formel $F \mapsto$ CLIQUE Instanz (G_F, k_F)

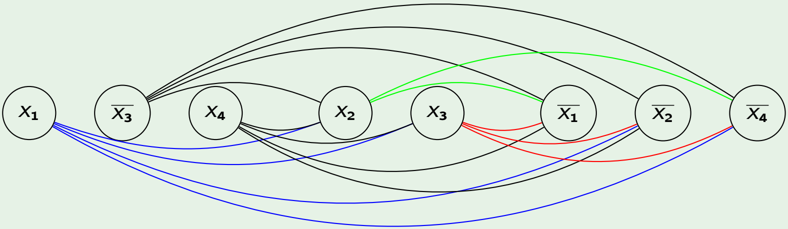
CLIQUE (Fortsetzung)

Beweis.

1. CLIQUE $\in$ NP
2. 3-SAT $\preccurlyeq_p$ CLIQUE
   - Brauchen: 3-SAT Formel $F \mapsto$ CLIQUE Instanz (G_F, k_F)

Beispiel

- $F = (X_1 \vee \overline{X_3} \vee X_4) \wedge (X_2 \vee X_3) \wedge (\overline{X_1} \vee \overline{X_2} \vee \overline{X_4})$
- F erfüllbar $\Leftrightarrow$ G_F hat Clique der Größe $m = 3$. G_F :



CLIQUE (Fortsetzung)

Beweis.

1. CLIQUE $\in$ NP
2. 3SAT $\preccurlyeq_p$ CLIQUE
    - Brauchen: 3-SAT Formel $F \mapsto$ CLIQUE Instanz (G_F, k_F)
    - Konstruktion.

CLIQUE (Fortsetzung)

Beweis.

1. CLIQUE $\in$ NP
2. 3SAT $\preccurlyeq_p$ CLIQUE
   - Brauchen: 3-SAT Formel $F \mapsto$ CLIQUE Instanz (G_F, k_F)
   - Konstruktion.
     - $k_F = m$, $G_F = (V, E)$ und
     - $V = \{v_{ij} \mid L_{ij} \text{ Literal in } F\}$
     - $E = \{(v_{i_1 j_1}, v_{i_2 j_2}) \mid i_1 \neq i_2 \wedge (L_{i_1 j_1}, L_{i_2 j_2}) \neq \{X_k, \overline{X_k}\}, \forall k\}$
   - Laufzeit: $\mathcal{O}(g)$ (Größe der 3-SAT Instanz sei g)

CLIQUE (Fortsetzung)

Beweis.

1. CLIQUE $\in$ NP
2. 3SAT $\preccurlyeq_p$ CLIQUE
   - Brauchen: 3-SAT Formel $F \mapsto$ CLIQUE Instanz (G_F, k_F)
   - Konstruktion.
     - $k_F = m$, $G_F = (V, E)$ und
     - $V = \{v_{ij} \mid L_{ij} \text{ Literal in } F\}$
     - $E = \{(v_{i_1 j_1}, v_{i_2 j_2}) \mid i_1 \neq i_2 \wedge (L_{i_1 j_1}, L_{i_2 j_2}) \neq \{X_k, \overline{X_k}\}, \forall k\}$
   - Laufzeit: $\mathcal{O}(g)$ (Größe der 3-SAT Instanz sei g)
   - Es gilt: F erfüllbar $\Leftrightarrow$ G_F besitzt eine k_F-Clique:
     - “ $\Rightarrow$ ” F erfüllbar. Dann es gibt eine Wahrheitsbelungung $L_{ij_i} = wahr, \forall 1 \leq i \leq m$, so dass F wahr ist.$\Rightarrow \{v_{ij_i} \mid \forall 1 \leq i \leq m\}$ bilden eine m-Clique in G_F
     - “ $\Leftarrow$ ”G_F besitzt eine k_F-Clique $C = \{v_{i_k j_k} \mid 1 \leq k \leq k_F\}$. $\Rightarrow C = \{v_{ij_i} \mid 1 \leq i \leq k_F\}$. $(v_{i_1 j_{i_1}}, v_{i_2 j_{i_2}}) \in E \Rightarrow$ die Wahrheitsbelungung $L_{ij_i} = wahr$ macht F wahr.

$\square$