

NP $\hat{=}$ Menge aller Entscheidungsprobleme, die durch NTM in Polynomialzeit $\cup_{k \in \mathbb{N}} O(n^k)$ entschieden werden können

$\hat{=}$ Menge aller Entscheidungsprobleme mit in Polynomialzeit überprüfbarer Zertifikate (=Zeuge)

Rate
„Zeuge“



$\text{poly}_2(|x|)$

Überprüfe
„Zeuge“



$\text{poly}_2(|x|)$

Die Mutter aller NP-Probleme SAT

Gegeben: Aussagenlogische Formel F

$$F ::= V \mid \neg F \mid (F \vee F) \mid (F \wedge F)$$

$$V ::= A \mid V' \quad \text{mit } A_0 := A, A_1 := A', A_2 := A'', \dots \\ \text{oder } x := A, y := A', z := A'', \dots$$

Frage: Ist F erfüllbar?

Zeuge: erfüllende Belegung σ von maximal $|F|$ Bits
 \rightarrow polynomial in $|F|$

Überprüfen: Einsetzen und Auswerten

no bottom-up Syntaxbaum
auswerten

as in $\mathcal{O}(|F|)$



$$\sigma(A_0) = 0, \sigma(A_1) = 0, \sigma(A_2) = 1$$

Syntaxbaum
mittels \rightarrow
CYK in PTIME

6.3 NP-Vollständigkeit

- 1 Polynomielle Reduzierbarkeit \leq_p
- 2 NP-vollständige Probleme = härteste Probleme in NP, alle anderen Probleme in NP darauf polynomiell reduzierbar
- 3 Satz: SAT ist NP-vollständig

Definition 6.10

Sei $A \subseteq \Sigma^*$ und $B \subseteq \Gamma^*$.

Dann heißt A **polynomiell reduzierbar** auf B , $A \leq_p B$,
gdw es eine totale und von einer DTM in polynomieller Zeit
berechenbare Funktion $f : \Sigma^* \rightarrow \Gamma^*$ gibt, so dass für alle $w \in \Sigma^*$

$$w \in A \iff f(w) \in B$$

Da $q(p(n))$ ein Polynom ist falls p und q Polynome sind:

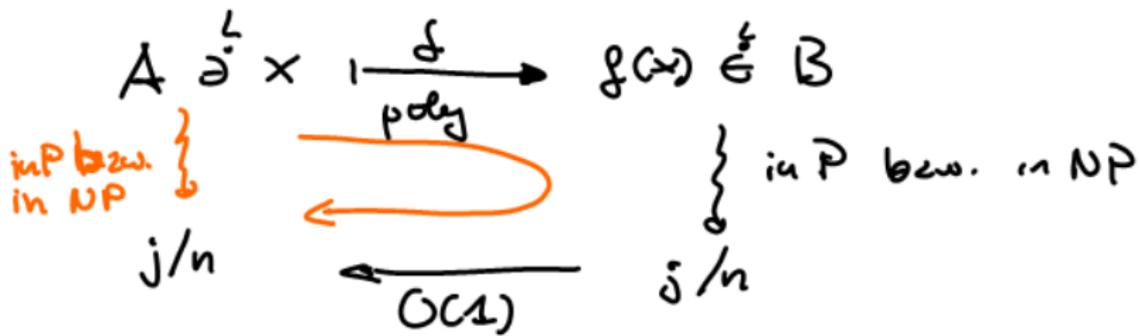
Lemma 6.11

Die Relation \leq_p ist transitiv.

Lemma 6.12

Die Klassen P und NP sind unter polynomieller Reduzierbarkeit nach unten abgeschlossen:

$$A \leq_p B \in P/NP \implies A \in P/NP$$



da: $A \ni x$ gdw. $f(x) \in B$

Lemma 6.12

Die Klassen P und NP sind unter polynomieller Reduzierbarkeit nach unten abgeschlossen:

$$A \leq_p B \in P/NP \implies A \in P/NP$$

Beweis:

- Sei $A \leq_p B$ mittels f , die von DTM M_f berechnet wird. Polynom p begrenzt Rechenzeit von M_f .
- Sei $B \in P$ mittels DTM M . Polynom q begrenzt Rechenzeit von M .

Damit ist $M_f; M$ polynomiell zeitbeschränkt in $|w|$:

- $M_f[w]$ macht $\leq p(|w|)$ Schritte.
- Ausgabe $f(w)$ von M_f hat Länge $\leq |w| + p(|w|)$.
- M macht $\leq q(|f(w)|) \leq q(|w| + p(|w|))$ Schritte (q monoton)

Daher macht $(M_f; M)[w]$ maximal $p(|w|) + q(|w| + p(|w|))$ Schritte, ein Polynom in $|w|$.

Analog: $A \leq_p B \in NP \implies A \in NP$



Englisch: NP-hard
Deutsch: NP-schwer

Ein Problem ist NP-hart,
wenn es mindestens so hart wie alles in NP ist:

Definition 6.13

Eine Sprache L heißt NP-hart gdw $A \leq_p L$ für alle $A \in \text{NP}$.

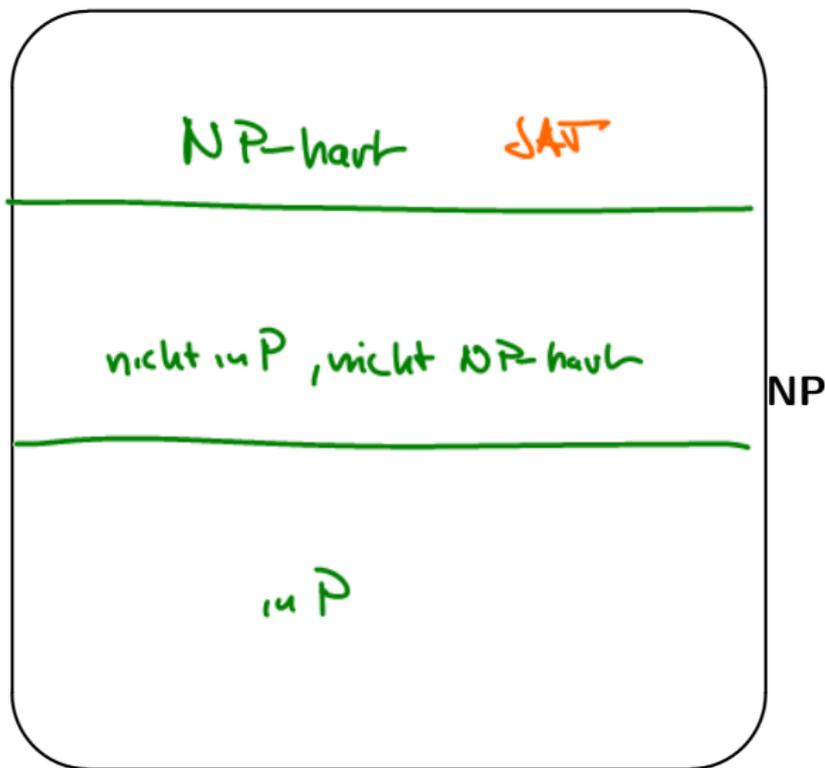
Definition 6.14

Eine Sprache L heißt NP-vollständig gdw
 L NP-hart ist und $L \in \text{NP}$.

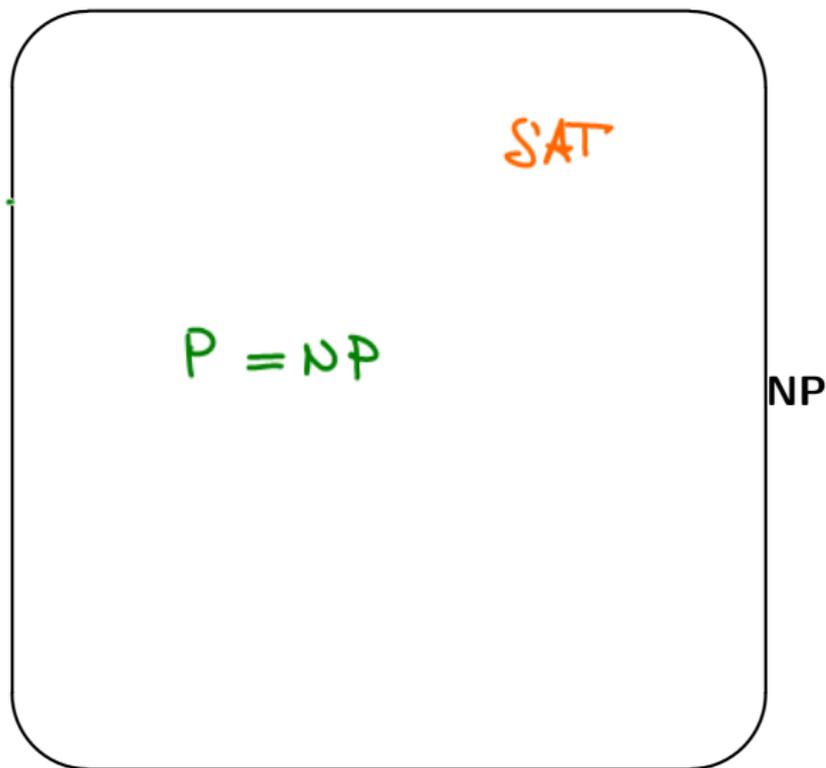
Intuition: NP-vollständige Probleme sind die schwierigsten
Probleme in NP:

alle Probleme in NP sind polynomiell auf sie reduzierbar.

Mögliche Szenarien für $P \subseteq NP \subseteq NP$ -vollständig



Mögliche Szenarien für $P \subseteq NP \subseteq NP$ -vollständig



NICHT möglich \leadsto siehe z.B. Papadimitriou

NP-hart

SAT

$P =$ alle nicht NP-harten
Probleme in NP

NP

Wie man $P \stackrel{?}{=} NP$ lösen kann:

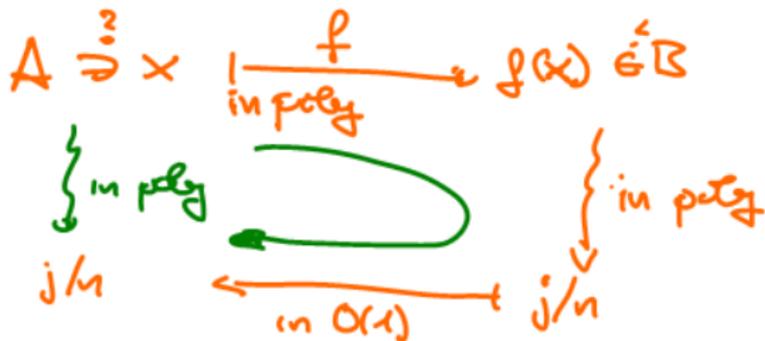
Lemma 6.15

Es gilt $P=NP$ gdw ein NP-vollständiges Problem in P liegt.

richt: NP-hart

\Leftarrow $A \in NP, \quad B \in P \text{ mit } \forall C \in NP: C \leq_p B$

also



\Rightarrow trivial

Wie man $P \stackrel{?}{=} NP$ lösen kann:

Lemma 6.15

Es gilt $P=NP$ gdw ein NP-vollständiges Problem in P liegt.

Beweis:

„ \Rightarrow “: Falls $P=NP$, so liegt jedes NP-vollständige Problem in P .

„ \Leftarrow “: Sei L ein NP-vollständiges Problem in P . Dann gilt $P \supseteq NP$:
Ist $A \in NP$, so gilt $A \leq_p L$ (da L NP-hart) und nach Lemma 6.12
 $A \in P$ (da $L \in P$). □

Starke Vermutung:

- $P \neq NP$
- dh kein NP-vollständiges Problem ist in P .

Aber gibt es überhaupt NP-vollständige Probleme?

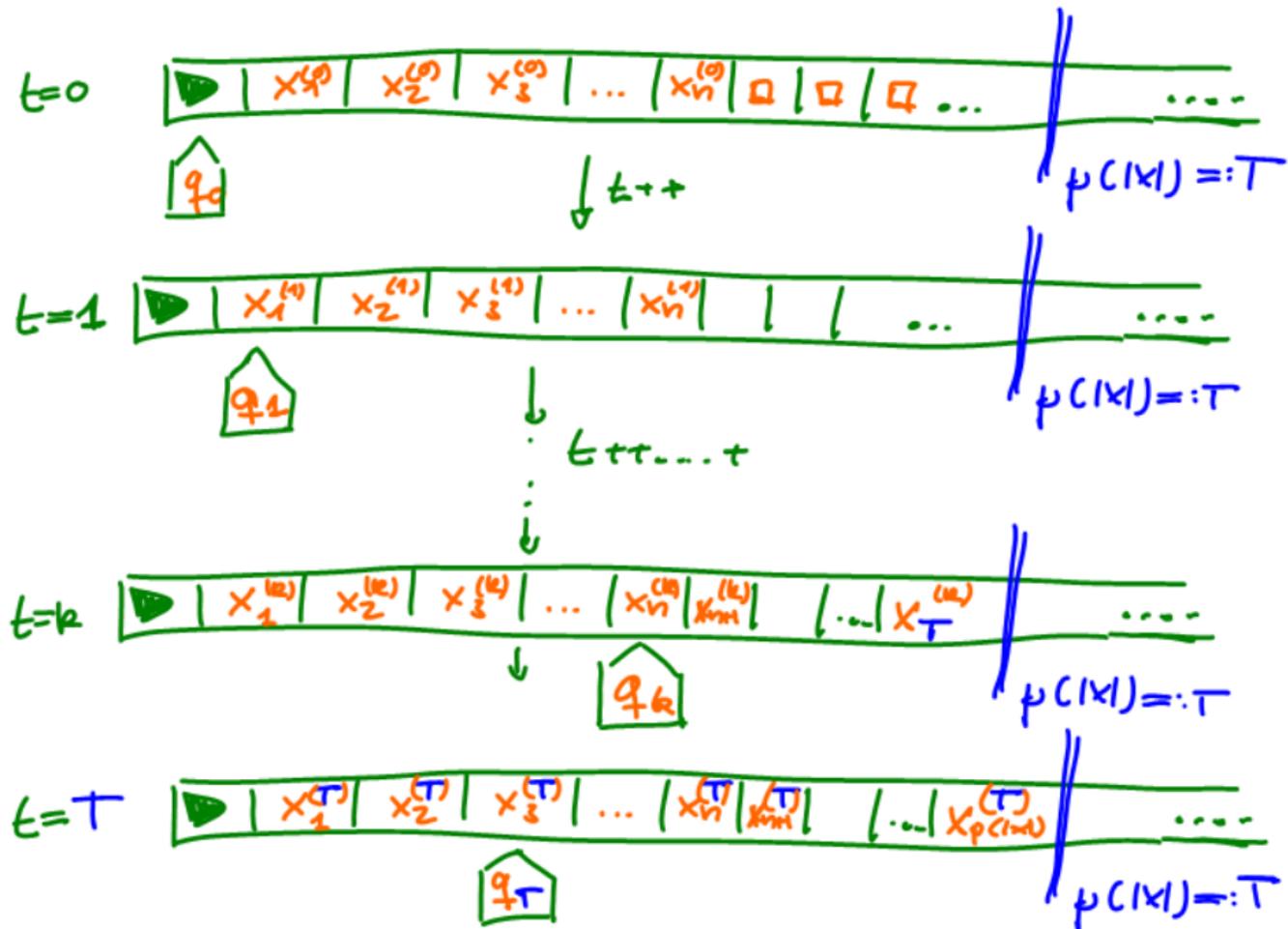
Satz 6.17 (Cook 1971)
 SAT ist NP-vollständig.

OBdA: 1 Band,
 nur nach
 rechts offen

• Gegeben $A \in NP$ zeige NTM M , Polynom p
 so dass $x \in A$ gdw. $M[x] = 1$ und
 alle Abläufe zu $M[x]$
 bestehen aus genau $p(|x|)$ Schritten

• also kann sich Kopf von M um maximal
 $p(|x|)$ Positionen bewegen

• Idee Beschreibe alle möglichen Abläufe $M[x]$
 mittels aussagenlogischer Formel, der Länge
 $\text{poly}(p(|x|))$



Variablen

- $Z_{t,q}$:= "Zustand zum Zeitpunkt t ist q "
- $P_{t,i}$:= "Position von Kopf zum Zeitp. t ist i "
- $B_{t,j,a}$:= "Bandinhalt zum Zeitp. t an Position j ist a "
 $i, j, t \in \{0, \dots, p(|x|)\}, q \in Q, a \in T$

Beschreibung

- ① Anfangskonfiguration : F_A
- ② akzeptierende Endkonfiguration : F_E
- ③ korrekten Übergang von t nach $t+1$: F_U
- ④ Rand bedingung; Immer genau eine Möglichkeit F_R
z.B. $\neg (P_{0,0} \wedge P_{0,1})$ muss erfüllt sein

Variablen

- $Z_{t,q} :=$ "Zustand zum Zeitpunkt t ist q "
- $P_{t,i} :=$ "Position von Kopf zum Zeitp. t ist i "
- $B_{t,j,a} :=$ "Bandinhalt zum Zeitp. t an Position j ist a "
 $i, j, t \in \{0, \dots, p(|X|)\}, q \in Q, a \in T$

Hauptsformel: $G(X) :=$ "genau eine Variable aus X mit \perp belegt"

$$G(X) = \left(\bigvee_{x \in X} x \right) \wedge \bigwedge_{\substack{x, y \in X \\ x \neq y}} \neg(x \wedge y)$$

$$|G(X)| \in O(|X| + |X|^2) \\ = O(|X|^2)$$

↑
mindestens
eine Variable wahr

↑
nie zwei Variablen
wahr

Variablen

- $Z_{t,q} :=$ "Zustand zum Zeitpunkt t ist q "
- $P_{t,i} :=$ "Position von Kopf zum Zeitp. t ist i "
- $B_{t,j,a} :=$ "Bandinhalt zum Zeitp. t an Position j ist a "
 $i, j, t \in \{0, \dots, p(x)\}, q \in Q, a \in T$

⑥ Randbedingung Zu jedem Zeitpunkt genau ein Zustand,
genau eine Position, genau ein Zeichen je
Position

$$F_R = \bigwedge_{t=0}^{p(x)} \left(\begin{aligned} &G(\{Z_{t,q} \mid q \in Q\}) \wedge G(\{P_{t,i} \mid i=0 \dots p(x)\}) \\ &\wedge \bigwedge_{j=0}^{p(x)} G(\{B_{t,j,a} \mid a \in T\}) \end{aligned} \right) \quad | F_R \in OC \quad p(x) = (|Q|^2 + p(x)^2 + |T|^2)$$

Variablen

- $Z_{t,q} :=$ "Zustand zum Zeitpunkt t ist q "
- $P_{t,i} :=$ "Position von Kopf zum Zeitp. t ist i "
- $B_{t,j,a} :=$ "Bandinhalt zum Zeitp. t an Position j ist a "
 $i, j, t \in \{0, \dots, p(|x|)\}, q \in Q, a \in T$

① Anfangskonfiguration $\triangleright |x_1| x_2 | \dots | x_n | \square | \square | \dots$

$$F_A = Z_{0, q_0} \wedge P_{0,0} \wedge B_{0,0, \triangleright}$$

$$(t=0) \quad \wedge_{i=1}^{|x|} B_{0,i, x_i} \quad |F_A| = \mathcal{O}(p(|x|))$$
$$\wedge_{i=|x|+1}^{p(|x|)} B_{0,i, \square}$$

Variablen

- $Z_{t,q}$:= "Zustand zum Zeitpunkt t ist q "
- $P_{t,i}$:= "Position von Kopf zum Zeitp. t ist i "
- $B_{t,j,a}$:= "Bandinhalt zum Zeitp. t an Position j ist a "
 $i, j, t \in \{0, \dots, p(|x|)\}, q \in Q, a \in T$

② akzeptierende Endkonfiguration

$$F_E = \bigvee_{q \in Q_F} Z_{p(|x|), q}$$

Variablen

- $Z_{t,q}$:= "Zustand zum Zeitpunkt t ist q "
- $P_{t,i}$:= "Position von Kopf zum Zeitp. t ist i "
- $B_{t,j,a}$:= "Bandinhalt zum Zeitp. t an Position j ist a "
 $i, j, t \in \{0, \dots, p(|x|)\}, q \in Q, a \in \Gamma$

③ korrekter Übergang:

$$F_u = \bigwedge_{\substack{t, q, i, a \\ t < p(|x|) \\ q \in Q \\ i = 0 \\ a \in \Gamma}} (Z_{t,q} \wedge P_{t,i} \wedge B_{t,i,a})$$

$$\wedge \bigwedge_{t, j} (\neg P_{t,0} \rightarrow \bigwedge_{a \in \Gamma} (B_{t,j,a} \rightarrow B_{t+1,j,a}))$$

switch (.-) {
case: ... break;
}

Von der Lösbarkeit zur Lösung

Die Berechnung einer erfüllenden Belegung kann auf SAT "reduziert" werden

von Entscheidungsproblem : F erfüllbar? (SAT)
zu Berechnungsproblem : Bestimme erfüllende Belegung

↳ Idee SAT als "Orakel", ob erfüllende Belegung im Fall $x=0$ bzw. $x=1$ existiert.

- Falls $F[x_i=0]$ erfüllbar, setze $\sigma(x_i)=0$ und berechne erfüllende Belegung zu $F[x_i=0]$, ansonsten $\sigma(x_i)=1$ und analog für $F[x_i=1]$

("Selbstreduktion von SAT")

#Var
 $\leq |F|$
also
 $O(|F|)$
SAT-
Aufrufe ↓

Von der Lösbarkeit zur Lösung

Die Berechnung einer erfüllenden Belegung kann auf SAT "reduziert" werden

Sei F eine Formel mit den Variablen x_1, \dots, x_k :

if $F \notin \text{SAT}$ **then** output("nicht lösbar")

else

for $i := 1$ **to** k **do**

if $F[x_i := 0] \in \text{SAT}$ **then** $b := 0$ **else** $b := 1$

 output(x_i "=" b)

$F := F[x_i := b]$

wobei $F[x := b] = F$ mit x ersetzt durch b .

Entscheidung von SAT in Zeit $O(f(n))$

\implies Berechnung einer erf. Bel. in Zeit $O(n \cdot (f(n) + n))$

(falls es eine gibt.)

$f(n)$ polynomiell $\implies n \cdot (f(n) + n)$ polynomiell

$f(n)$ exponentiell $\implies n \cdot (f(n) + n)$ exponentiell

Von NP-hart zu „NP-leicht“

- Bis vor ca. 15 Jahren:

NP-vollständig = Todesurteil

- In den letzten 15 Jahren:

Spektakuläre Fortschritte bei *Implementierung* von

SAT-Lösern (*SAT-solver*): <http://satcompetition.org>

Stand der Kunst: Erfüllbar: bis 10^5 Variablen

Unerfüllbar: bis 10^3 Variablen

- Jetzt:

NP-vollständig = Hoffnung durch SAT

- Paradigma:

SAT (Logik!) als universelle Sprache
zur Kodierung kombinatorischer Probleme

Reduktion auf SAT manchmal schneller als problemspezifische
Löser! Und fast immer einfacher.

Beispiel: Reduktion von 3-Färbbarkeit (3COL) auf SAT.

3COL

Gegeben: Ein ungerichteter Graph

Problem: Gibt es eine Färbung der Knoten, so dass keine benachbarten Knoten gleich gefärbt sind?

Lineare Reduktion von Graph $G = (V, E)$ auf SAT:

- Variablen = $V \times \{1, 2, 3\}$. Notation: x_{vi}
- Interpretation: $x_{vi} = 1$ gdw Knoten v hat Farbe i

Formel: *genau ein Farbe pro Knoten*

$$\bigwedge_{v \in V} G(x_{v1}, x_{v2}, x_{v3}) \wedge \bigwedge_{(u,v) \in E} \neg(x_{u1} \wedge x_{v1} \vee x_{u2} \wedge x_{v2} \vee x_{u3} \wedge x_{v3})$$

*benachbarte Knoten haben
verschiedene Farben*

Bemerkungen

- Zeigt $3COL \leq_p SAT$ und damit $3COL \in NP$.
- **Zeigt nicht, dass 3COL NP-vollständig ist.**

SAT auf 3COL mittels 3SAT.

3SAT kurz für 3-KNF-SAT

kurz für: entscheide, ob Formel in 3-KNF erfüllbar

3-KNF:
$$F = \bigwedge_{i=1}^n \underbrace{(L_{i,1} \vee L_{i,2} \vee L_{i,3})}_{\text{Klausel}}$$

mit $L_{i,j} \in \{A_1, \neg A_1 \mid A \text{ Variable}\}$ Literal

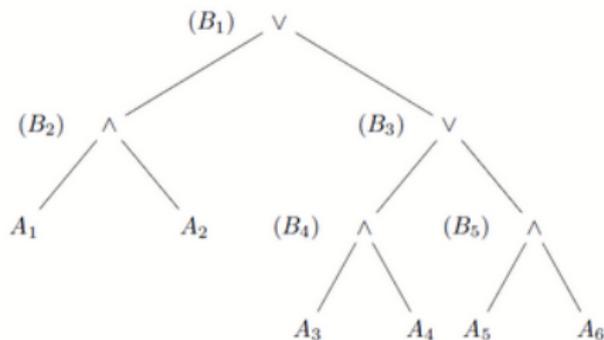
Erinnerung: bel. Formel \sim 3-KNF

$$F = \begin{array}{c} \text{op} \\ \swarrow \quad \searrow \\ G \quad H \end{array} \equiv_e \begin{array}{l} (B_F \leftrightarrow (B_G \text{ op } B_H)) \\ \wedge (B_G \leftrightarrow G) \\ \wedge (B_H \leftrightarrow H) \end{array}$$

\sim B_F Hilfsvariable, speichert Wert von Teilformel F

DS
und
nächstes
Mal

siehe DS TA 5.2 (2015)



Für F_3 erhält man so:

$$G_3 = B_1 \wedge (B_1 \leftrightarrow (B_2 \vee B_3)) \wedge (B_2 \leftrightarrow (A_1 \wedge A_2)) \wedge (B_3 \leftrightarrow (B_4 \vee B_5)) \wedge (B_4 \leftrightarrow (A_3 \wedge A_4)) \wedge (B_5 \leftrightarrow (A_5 \wedge A_6))$$

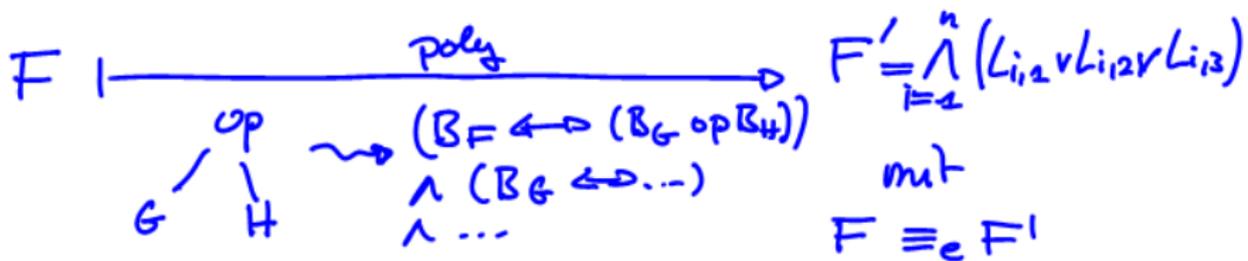
Es lässt sich zeigen, dass F_3 genau dann erfüllbar ist, wenn G_3 erfüllbar ist (kurz: F und G sind **erfüllbarkeitsäquivalent**):

- Ist β eine minimale, F_3 erfüllende Belegung, so kann man β zu einer G_3 erfüllenden Belegung erweitern.
- Gilt $[G_3](\beta) = 1$, dann auch gilt auch $[F_3](\beta) = 1$.

(b) Zeigen Sie für beliebige aussagenlogische Formeln F, G, H :

- $(F \leftrightarrow (G \wedge H)) \equiv (F \vee \neg G \vee \neg H) \wedge (\neg F \vee G) \wedge (\neg F \vee H)$
- $(F \leftrightarrow (G \vee H)) \equiv (\neg F \vee G \vee H) \wedge (F \vee \neg G) \wedge (F \vee \neg H)$

$SAT \leq_p 3SAT$



\leadsto $3SAT$ bereits NP-vollständig
($2SAT$ aber in P)

$3SAT \leq_p 3COL$

$F' = \bigwedge_{i=1}^n (L_{i,1} \vee L_{i,2} \vee L_{i,3}) \longmapsto ? \text{ Graph?}$

\exists SAT \leq_p \exists CCL

Literale \mapsto Knoten

Beziehungen zw Literalen \mapsto Kanten

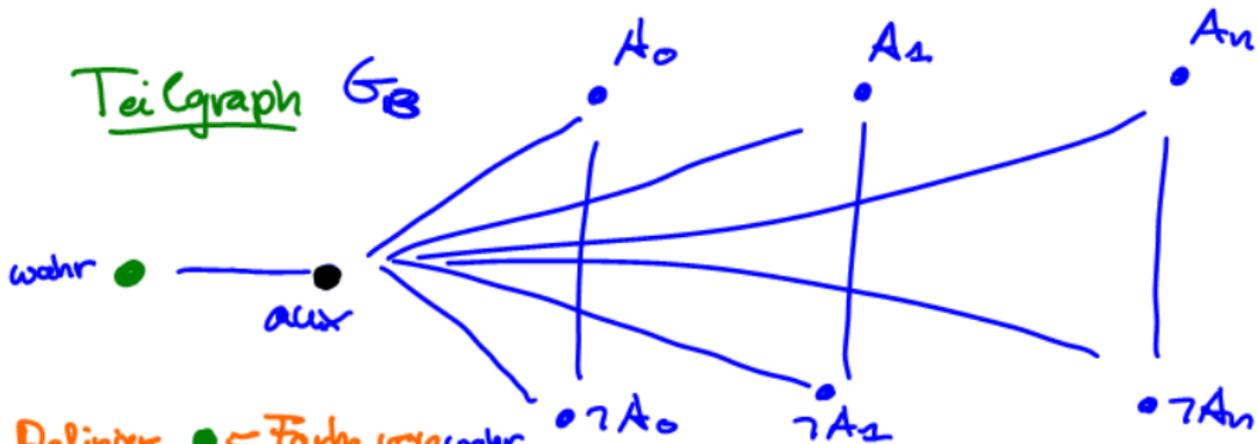
+ Hilfsknoten & -kanten

Belegung \longleftrightarrow Färbung

1. Ziel: Korrekte Färbung muss Belegung codieren

3SAT \leq_p 3COL

\leadsto 1. Ziel Korrekte Färbung muss A und $\neg A$ verschieden färben
und immer dieselben Farben für \perp und \circ



Definiere

- \bullet = Farbe von wahr
- \bullet = Farbe von aus
- \circ = vorbeibende Farbe (jedoch)

3SAT

 \leq_p

SCC

2. Ziel $\mathcal{C} \subseteq \mathcal{K}$ Klausur 

$$\mathcal{C} = L_1 \vee L_2 \vee L_3$$

Idee Falls Färbung von G_B
 eine erfüllende Belegung von \mathcal{C}
 codiert, dann und nur dann
 soll G_C korrekt gefärbt
 werden können.



3SAT

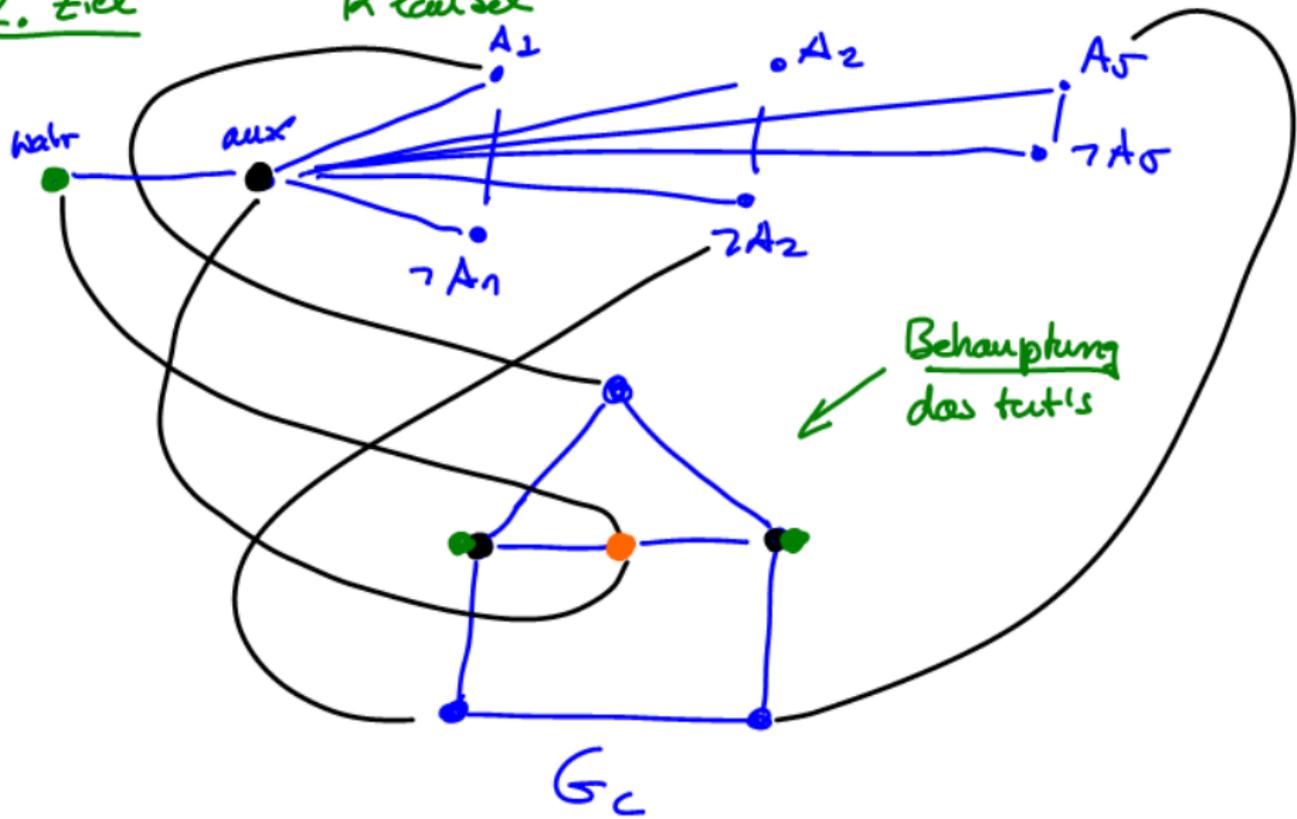
\leq_p

SCCL

2. Ziel

Klausur

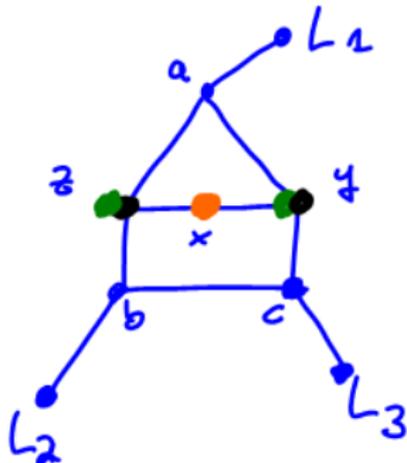
$$C = A_1 \vee \neg A_2 \vee A_5$$



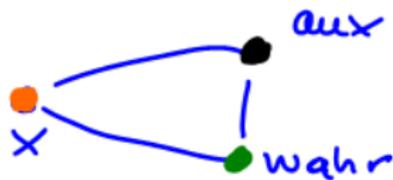
Intuition zu G_C mit $C = L_1 \vee L_2 \vee L_3$

Fallunterscheidung nach L_1 :

- Falls L_1 grün, dann Farben von L_2 und L_3 egal
- sonst mindestens L_2 oder L_3 grün,
- ansonsten keine Färbung möglich sein.



Erzwingt, dass
x stets ● mittels



3SAT

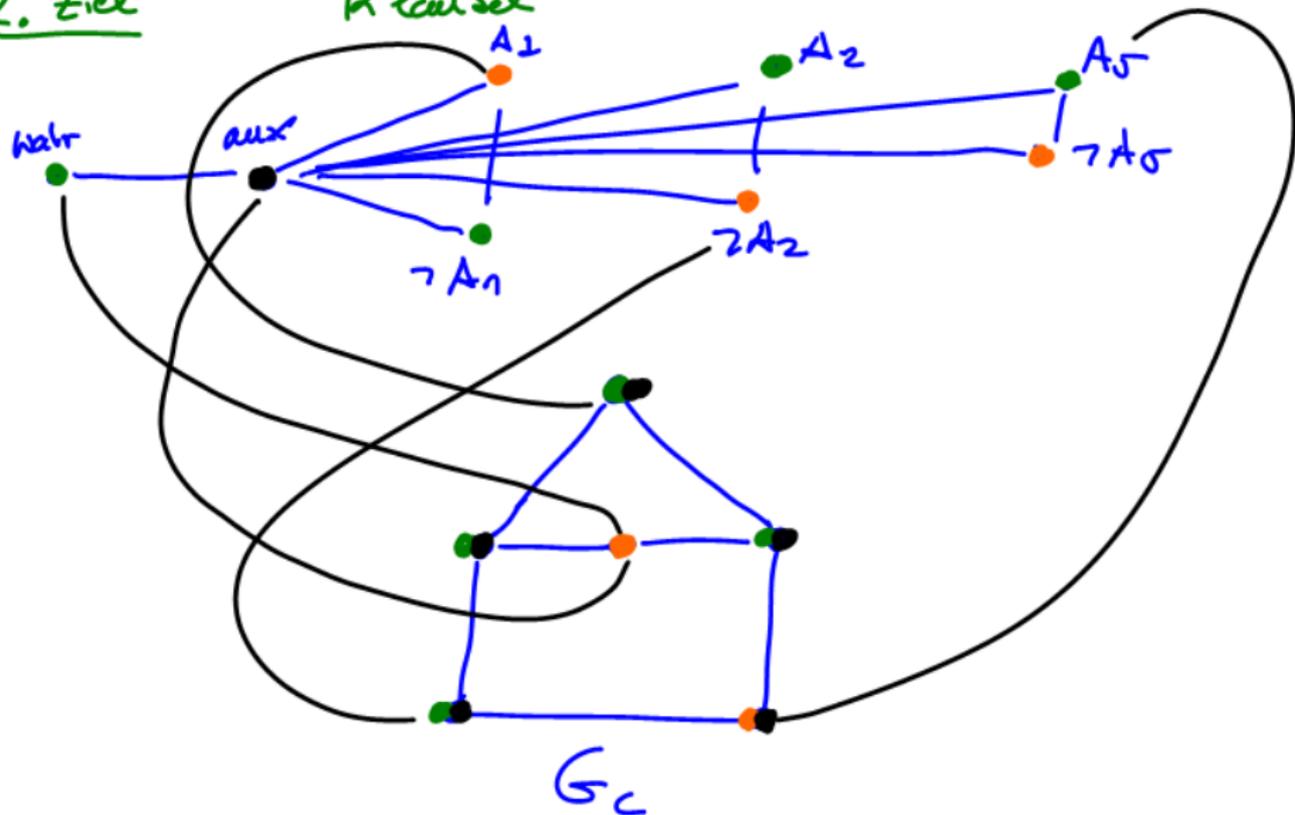
\leq_p

SCCL

2. Ziel

Klausur

$$C = A_1 \vee \neg A_2 \vee A_5$$



3SAT

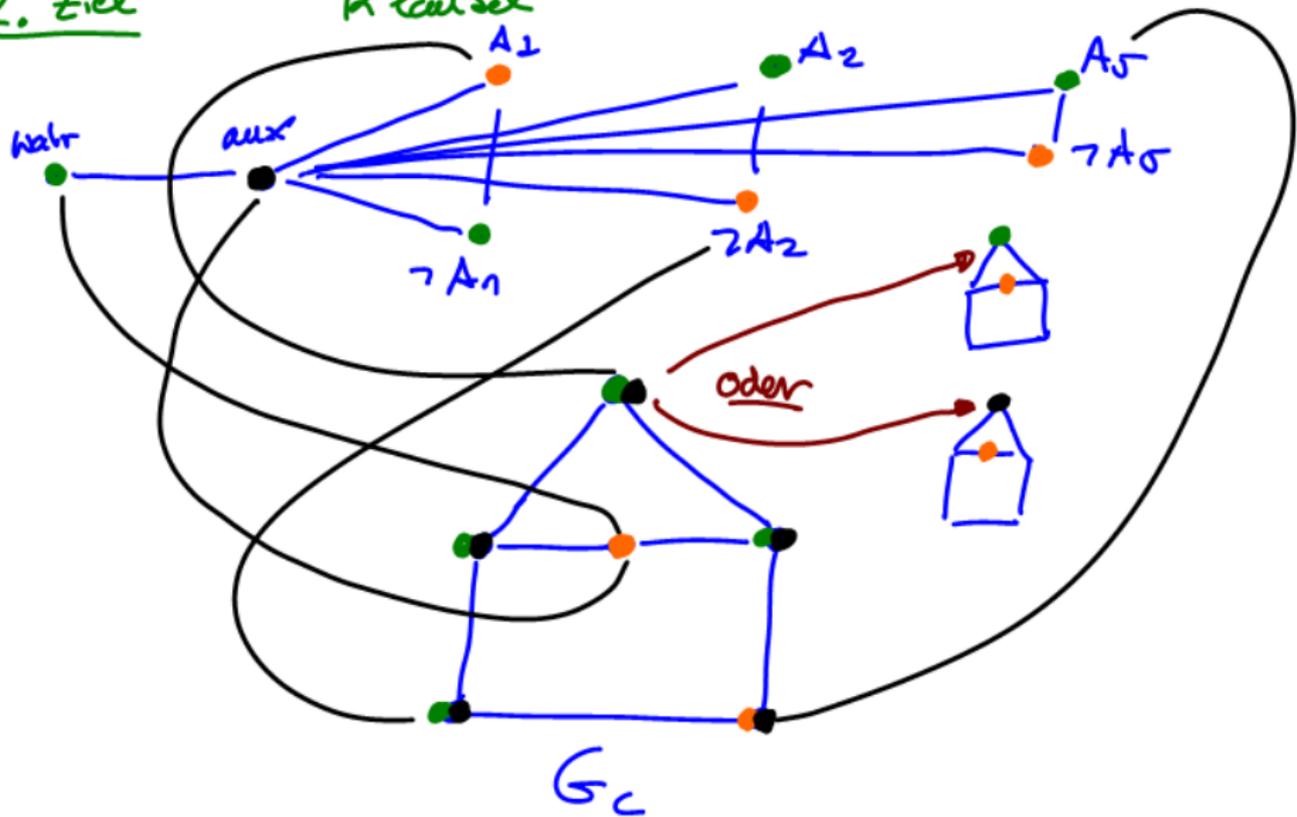
\leq_p

SCCL

2. Ziel

Klausur

$$C = A_1 \vee \neg A_2 \vee A_5$$



3SAT

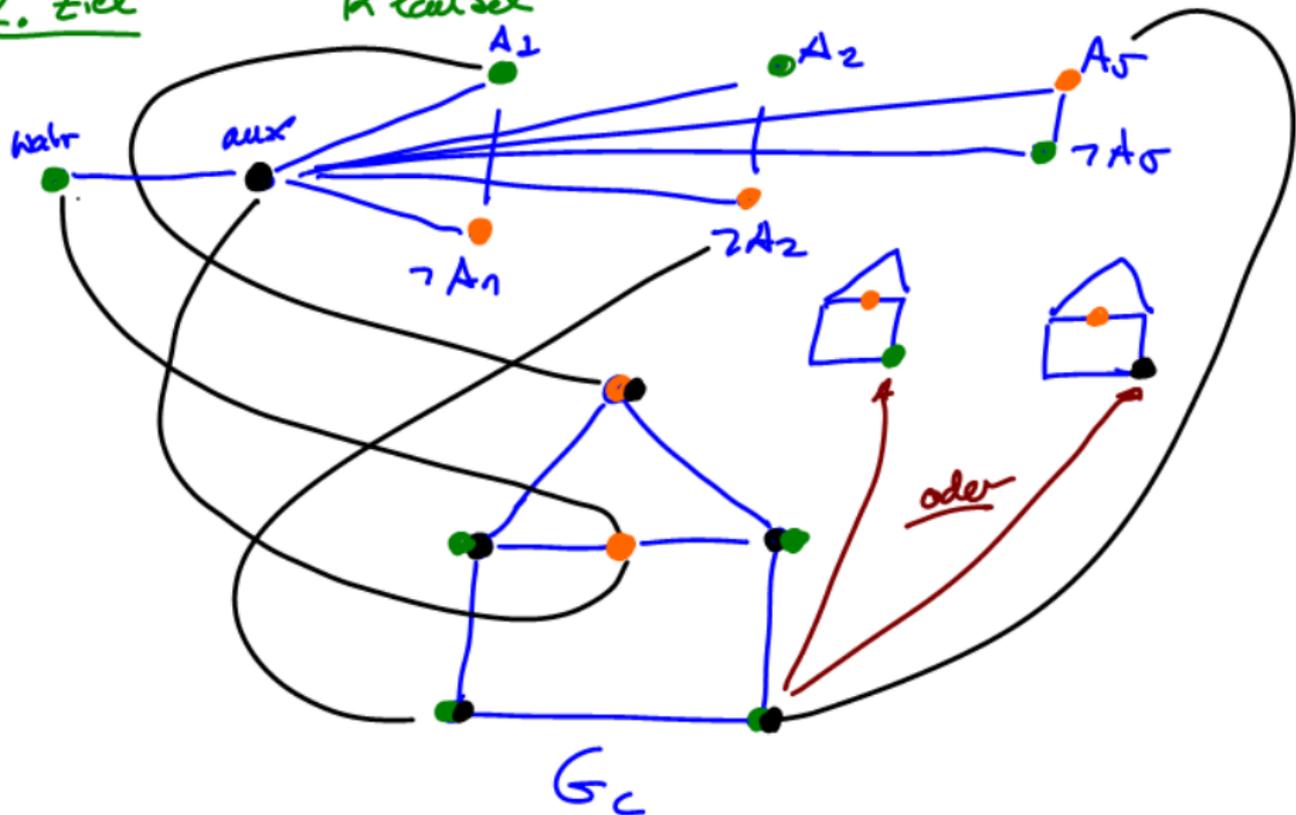
\leq_p

SCCL

2. Ziel

Klausur

$$C = A_1 \vee \neg A_2 \vee A_5$$



3SAT

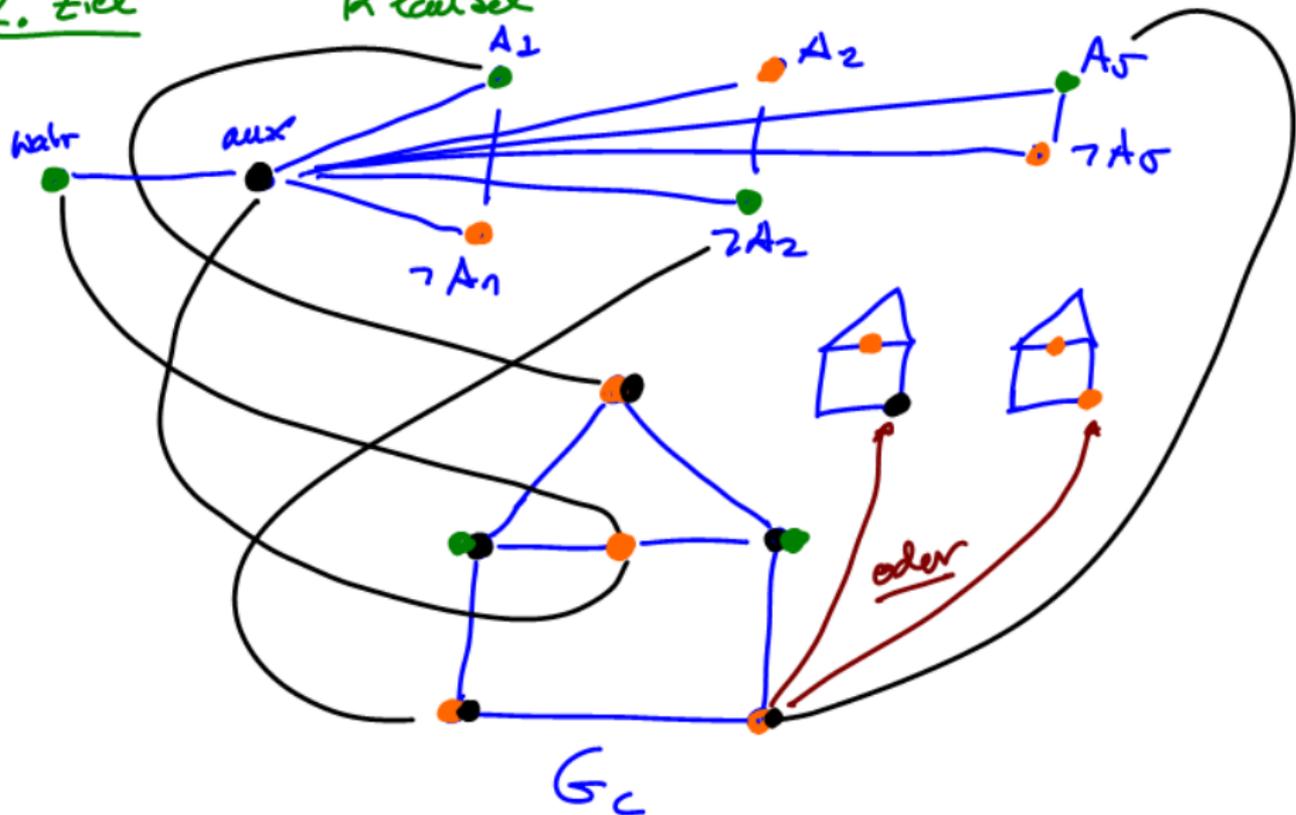
\leq_p

SCCL

2. Ziel

Klausur

$$C = A_1 \vee \neg A_2 \vee A_5$$



3SAT

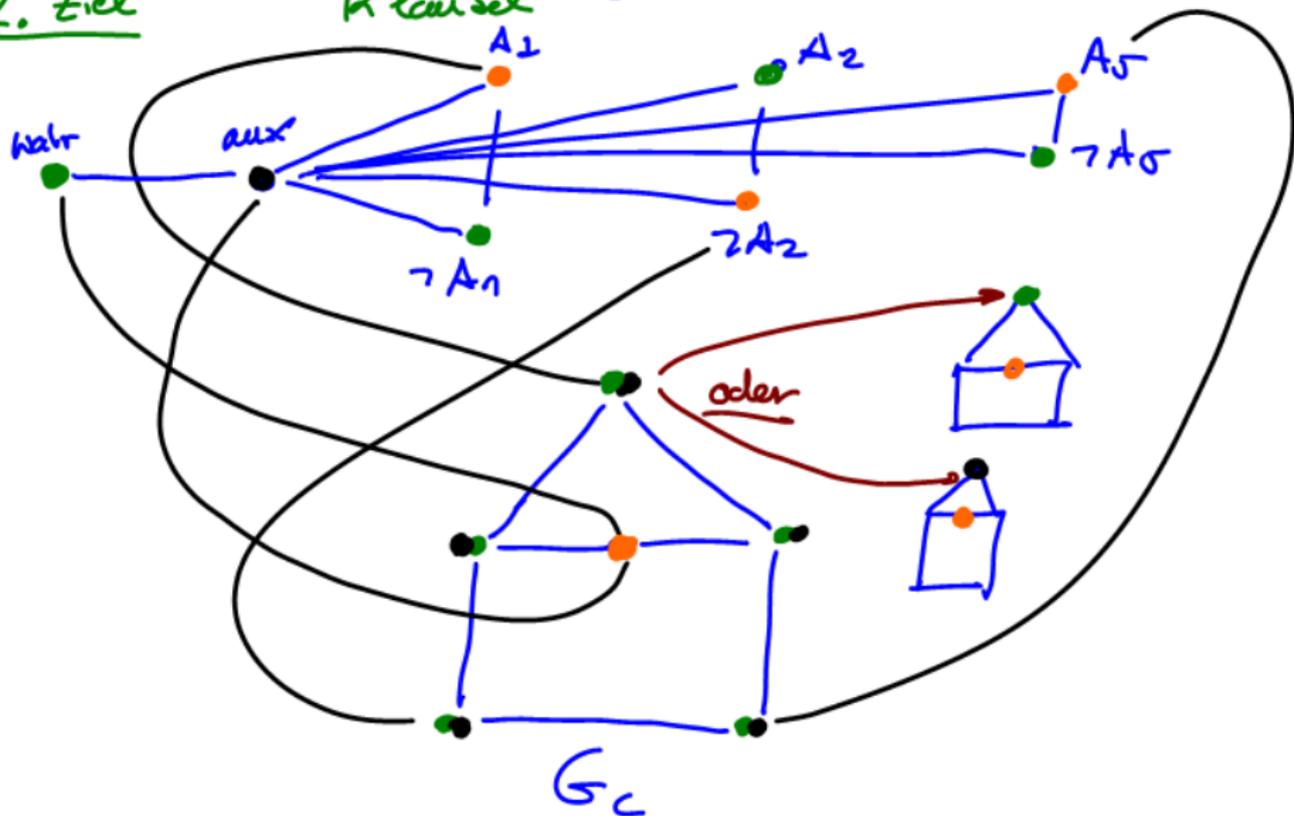
\leq_p

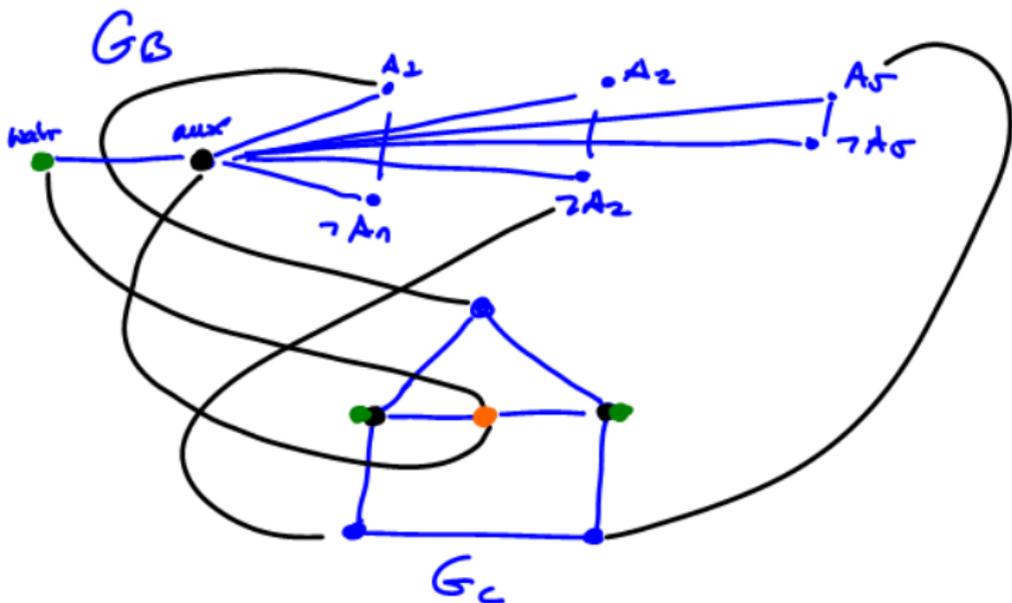
SCCL

2. Ziel

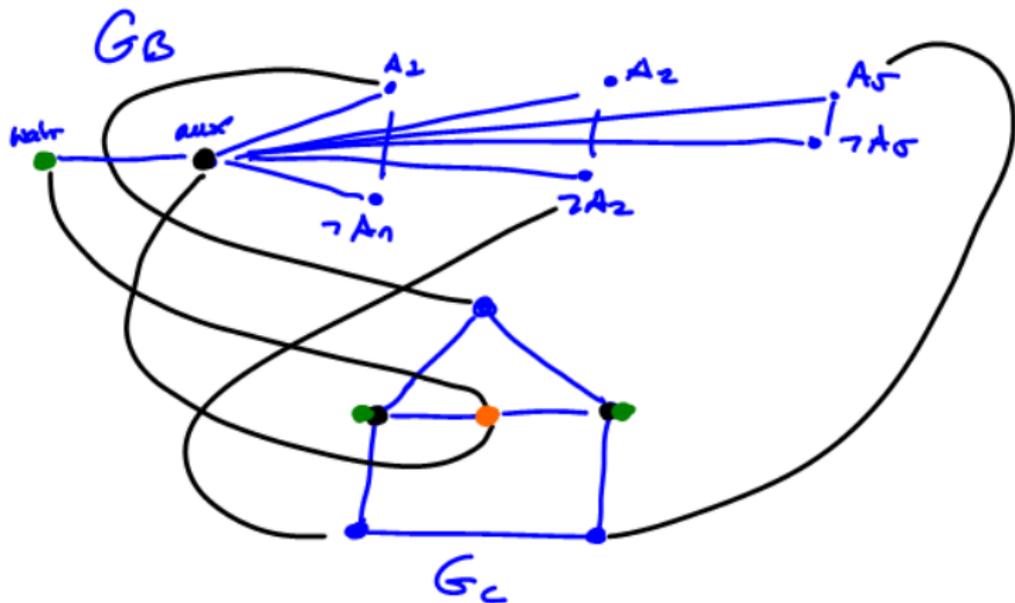
Klausur

$$C = A_1 \vee \neg A_2 \vee A_5$$





- Codiert Färbung von G_B eine erfüllende Belegung von C , dann kann G_C korrekt gefärbt werden (auf 2 Arten)
- Codiert Färbung von G_B eine passende nicht erfüllende Bel., dann kann G_C nicht korrekt gefärbt werden.



$$F = \bigwedge_{i=1}^n (L_{i1} \vee L_{i2} \vee L_{i3}) \xleftrightarrow{\text{poly}} G_F = 2n+2$$

mit $|G_F| = |G_B| + n \cdot (|G_C| + 4)$

$\underset{=}{=} 13$

Was wäre, wenn 3SAT in PTIME auf 2COL reduzierbar?

Industrielle Anwendungen von SAT

1. Äquivalenztest von Schaltkreisen.

Schaltung	→	Boole'sche Formel
Eingabe	→	Belegung
Eingabe mit 1-Ergebnis	→	Erfüllende Belegung
Funktionale Äquivalenz	→	Logische Äquivalenz

NICHTÄQUIVALENZ

Gegeben: Zwei aussagenlogische Formeln F_1, F_2 über Variablenmengen X_1, X_2 .

Problem: Gibt es eine Belegung σ von $X_1 \cup X_2$ mit $\sigma(F_1) \wedge \neg \sigma(F_2)$?

Lemma 6.18

NICHTÄQUIVALENZ \leq_p SAT und SAT \leq_p NICHTÄQUIVALENZ.

$$F_1 \not\equiv F_2 \text{ gdw. } F_1 \leftrightarrow F_2 \equiv \text{false}$$
$$\text{gdw. } \neg(F_1 \leftrightarrow F_2) \equiv \text{true}$$

$$\begin{array}{ccc} \text{NICHT ÄQ} & \longrightarrow & \text{SAT} \\ (F_1, F_2) & \longmapsto & \neg(F_1 \leftrightarrow F_2) \\ & & \equiv (\neg F_2 \wedge F_1) \vee (F_2 \wedge \neg F_1) \end{array}$$

$$\begin{array}{ccc} (F, \text{false}) & \longleftarrow & F \\ \parallel & & \\ X \wedge \neg X & & \end{array}$$

2. *Bounded Model Checking*

Hardware Entscheide, ob eine Schaltung mit Zustand für **alle** Eingaben innerhalb von 10 Zyklen ein bestimmtes Verhalten (nicht) hat.

2. *Bounded Model Checking*

Hardware Entscheide, ob eine Schaltung mit Zustand für **alle** Eingaben innerhalb von 10 Zyklen ein bestimmtes Verhalten (nicht) hat.

Software Entscheide, ob ein Programm für **alle** Eingaben innerhalb von 10 Schritten ein bestimmtes Verhalten (nicht) hat.
Variablen müssen auf sehr kleine Wertebereiche eingeschränkt werden!

Aufgabe 4.3

Notation: $\mathbb{Z}_n := \{0, 1, 2, \dots, n-1\}$ ist Menge der möglichen Reste bei Division durch n ($n \in \mathbb{N}$).

- (a) Beschreiben Sie folgende Funktionen entsprechend TA3.3 durch aussagenlogische Formeln $\varphi_f, \varphi_g, \varphi_h$:

$$f: \mathbb{Z}_4 \rightarrow \mathbb{Z}_4: x \mapsto (x-1) \bmod 4 \quad g: \mathbb{Z}_4 \rightarrow \mathbb{Z}_4: x \mapsto (x^2) \bmod 4 \quad h: \mathbb{Z}_4 \rightarrow \mathbb{Z}_4: x \mapsto (3 \cdot x) \bmod 4$$

- (b) Beschreiben Sie folgendes Programm als aussagenlogische Formel φ . Verwenden Sie die Formeln aus (a) und Variablenbenennung (vgl. Tutorübungen).

```
x = (x - 1) % 4 # (x-1) mod 4
if x == 3:
    x = (x * x) % 4 # (x^2) mod 4
else:
    x = (3*x) % 4 # (3 * x) mod 4
return x
```

Der initiale Werte der Programmvariablen x soll durch die aussagenlogischen Variablen x_0, x_1 beschrieben werden.

3. Programmoptimierung. Beispiel: Registerverteilung

Kann man in einem Programmstück n Variablen so auf k Register verteilen, dass jede Variable so lange in einem Register bleibt, wie sie *lebendig* ist?

Variable ist an einem Punkt *lebendig*

gdw sie später noch gelesen wird, ohne vorher überschrieben worden zu sein.

Reduktion auf k -Färbbarkeit (und damit auf SAT):

Knoten = Variable

u und v verbunden = $u \neq v$ und es gibt einen Programmpunkt, an dem u und v lebendig sind

Farbe = Register

k -Färbung = Zuordnung eines Registers zu jeder Variablen

Sowohl k -Färbbarkeit als auch Registerverteilung ist für $k \geq 3$ NP-vollständig.

Mehr Information: Vorlesung *Programmoptimierung*

DS 2013
TA 13.1