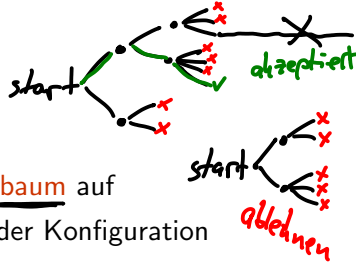
Gliederung

Co-Nichtdeterministische Turing-Maschinen

Definition (Nichtdeterministische Turing-Maschine)

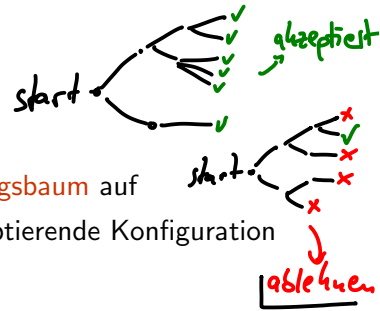


- $\delta \subseteq (Z \setminus E) \times \Gamma \times Z \times \Gamma \times \{L, R, N\}$
- "Folgekonfiguration"-Relation $\vdash_M^1$ von M spannt Berechnungsbaum auf
- NTM akzeptiert $\Leftrightarrow$ es gibt Berechnungspfad zu akzeptierender Konfiguration

Co-Nichtdeterministische Turing-Maschinen

Definition (Co-Nichtdeterministische Turing-Maschine)

- $\delta \subseteq (Z \setminus E) \times \Gamma \times Z \times \Gamma \times \{L, R, N\}$
- "Folgekonfiguration"-Relation $\vdash_M^1$ von M spannt Berechnungsbaum auf
- coNTM akzeptiert $\Leftrightarrow$ alle Berechnungspfade erreichen akzeptierende Konfiguration



Co-Nichtdeterministische Turing-Maschinen

Definition (Co-Nichtdeterministische Turing-Maschine)

- $\delta \subseteq (Z \setminus E) \times \Gamma \times Z \times \Gamma \times \{L, R, N\}$
- "Folgekonfiguration"-Relation $\vdash_M^1$ von M spannt Berechnungsbaum auf
- coNTM akzeptiert $\Leftrightarrow$ alle Berechnungspfade erreichen akzeptierende Konfiguration

time_{coN} und $\text{coNTIME}(f(n))$ analog zu time_N und $\text{NTIME}(f(n))$

Länge des längsten Berechnungspfades

Probleme die von coNTM in $f(n)$ Zeit entschieden werden können

Co-Nichtdeterministische Turing-Maschinen

Definition (Co-Nichtdeterministische Turing-Maschine)

- $\delta \subseteq (Z \setminus E) \times \Gamma \times Z \times \Gamma \times \{L, R, N\}$
- "Folgekonfiguration"-Relation $\vdash_M^1$ von M spannt Berechnungsbaum auf
- coNTM akzeptiert $\Leftrightarrow$ alle Berechnungspfade erreichen akzeptierende Konfiguration

time_{coN} und $\mathrm{coNTIME}(f(n))$ analog zu time_N und $\mathrm{NTIME}(f(n))$

Definition (coNP)

$\mathrm{coNP} := \bigcup_{k \geq 1} \mathrm{coNTIME}(n^k)$.

"**co-nicht**deterministisch, in Polynomzeit"

Co-Nichtdeterministische Turing-Maschinen

Definition (Co-Nichtdeterministische Turing-Maschine)

- $\delta \subseteq (Z \setminus E) \times \Gamma \times Z \times \Gamma \times \{L, R, N\}$
- "Folgekonfiguration"-Relation $\vdash_M^1$ von M spannt Berechnungsbaum auf
- coNTM akzeptiert $\Leftrightarrow$ alle Berechnungspfade erreichen akzeptierende Konfiguration

time_{coN} und $\mathrm{coNTIME}(f(n))$ analog zu time_N und $\mathrm{NTIME}(f(n))$

Definition (coNP)

$\mathrm{coNP} := \bigcup_{k \geq 1} \mathrm{coNTIME}(n^k)$. "**co-nicht**deterministisch, in Polynomzeit"

Theorem (Alternative Definition für NP („Guess and Check"))

Eine Sprache $L \subseteq \Sigma^*$ ist in NP, gdw. ein Polynom $p : \mathbb{N} \to \mathbb{N}$ und eine polynomiell zeitbeschränkte **D**TM M (d.h. $\mathrm{time}_M(n) \in O(n^c)$) existieren, sodass für jedes $x \in \Sigma^*$ gilt

$$x \in L \Leftrightarrow \exists_{u \in \Sigma^{p(|x|)}} \langle x, u \rangle \in T(M)$$

beziehungsweise

$$x \in L \Leftrightarrow \exists_{u \in \Sigma^{p(|x|)}} \langle x, u \rangle \in T(M).$$

Co-Nichtdeterministische Turing-Maschinen

Definition (Co-Nichtdeterministische Turing-Maschine)

- $\delta \subseteq (Z \setminus E) \times \Gamma \times Z \times \Gamma \times \{L, R, N\}$
- "Folgekonfiguration"-Relation $\vdash_M^1$ von M spannt Berechnungsbaum auf
- coNTM akzeptiert $\Leftrightarrow$ alle Berechnungspfade erreichen akzeptierende Konfiguration

time_{coN} und $\mathrm{coNTIME}(f(n))$ analog zu time_N und $\mathrm{NTIME}(f(n))$

Definition (coNP)

$\mathrm{coNP} := \bigcup_{k \geq 1} \mathrm{coNTIME}(n^k)$. "**co-nicht**deterministisch, in Polynomzeit"

Theorem (Alternative Definition für coNP („Guess and Check“))

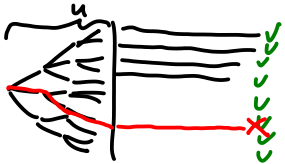
Eine Sprache $L \subseteq \Sigma^*$ ist in coNP, gdw. ein Polynom $p : \mathbb{N} \to \mathbb{N}$ und eine polynomiell zeitbeschränkte **D**TM M (d.h. $\mathrm{time}_M(n) \in O(n^c)$) existieren, sodass für jedes $x \in \Sigma^*$ gilt

$$x \in L \Leftrightarrow \forall_{u \in \Sigma^{p(|x|)}} \langle x, u \rangle \in T(M)$$

beziehungsweise

$$x \in L \Leftrightarrow \exists_{u \in \Sigma^{p(|x|)}} \langle x, u \rangle \in T(M).$$

Co-Nichtdeterministische Turing-Maschinen



Definition (Co-Nichtdeterministische Turing-Maschine)

- $\delta \subseteq (Z \setminus E) \times \Gamma \times Z \times \Gamma \times \{L, R, N\}$
- "Folgekonfiguration"-Relation $\vdash_M^1$ von M spannt Berechnungsbaum auf
- coNTM akzeptiert $\Leftrightarrow$ alle Berechnungspfade erreichen akzeptierende Konfiguration

time_{coN} und $\mathrm{coNTIME}(f(n))$ analog zu time_N und $\mathrm{NTIME}(f(n))$

Definition (coNP)

$\mathrm{coNP} := \bigcup_{k \geq 1} \mathrm{coNTIME}(n^k)$.

"**co-nicht**deterministisch, in Polynomzeit"

Theorem (Alternative Definition für coNP („Guess and Check“))

Eine Sprache $L \subseteq \Sigma^*$ ist in coNP, gdw. ein Polynom $p : \mathbb{N} \to \mathbb{N}$ und eine polynomiell zeitbeschränkte **D**TM M (d.h. $\mathrm{time}_M(n) \in O(n^c)$) existieren, sodass für jedes $x \in \Sigma^*$ gilt

beziehungsweise

$$x \in L \Leftrightarrow \forall_{u \in \Sigma^{p(|x|)}} \langle x, u \rangle \in T(M)$$

$$x \notin L \Leftrightarrow \exists_{u \in \Sigma^{p(|x|)}} \langle x, u \rangle \notin T(M).$$

zertifikat „Gegenbeispiel"

Co-Nichtdeterministische Turing-Maschinen

Definition (Co-Nichtdeterministische Turing-Maschine)

- $\delta \subseteq (Z \setminus E) \times \Gamma \times Z \times \Gamma \times \{L, R, N\}$
- "Folgekonfiguration"-Relation $\vdash_M^1$ von M spannt Berechnungsbaum auf
- coNTM akzeptiert $\Leftrightarrow$ alle Berechnungspfade erreichen akzeptierende Konfiguration

time_{coN} und $\mathrm{coNTIME}(f(n))$ analog zu time_N und $\mathrm{NTIME}(f(n))$

Definition (coNP)

$\mathrm{coNP} := \bigcup_{k \geq 1} \mathrm{coNTIME}(n^k)$. "**co-nicht**deterministisch, in Polynomzeit"

Theorem (Alternative Definition für coNP („Guess and Check“))

Eine Sprache $L \subseteq \Sigma^*$ ist in coNP, gdw. ein Polynom $p : \mathbb{N} \to \mathbb{N}$ und eine polynomiell zeitbeschränkte **D**TM M (d.h. $\mathrm{time}_M(n) \in O(n^c)$) existieren, sodass für jedes $x \in \Sigma^*$ gilt

$$x \in L \Leftrightarrow \forall_{u \in \Sigma^{p(|x|)}} \langle x, u \rangle \in T(M)$$

beziehungsweise

$$x \notin L \Leftrightarrow \exists_{u \in \Sigma^{p(|x|)}} \langle x, u \rangle \notin T(M).$$

Beachte: zentraler Unterschied zu NP: „$\forall$“ statt „$\exists$“

Die Komplexitätsklasse coNP I

Erinnerung: Sei $L \subseteq \Sigma^*$, dann ist $\bar{L} := \Sigma^* \setminus L$ das Komplement von L.

Theorem

$\text{coNP} = \{L \subseteq \Sigma^* \mid \bar{L} \in \text{NP}\}$.

Die Komplexitätsklasse coNP I

Erinnerung: Sei $L \subseteq \Sigma^*$, dann ist $\bar{L} := \Sigma^* \setminus L$ das Komplement von L.

Theorem

$\text{coNP} = \{L \subseteq \Sigma^* \mid \bar{L} \in \text{NP}\}$.

Beweis

Sei $L \subseteq \Sigma^*$.

Die Komplexitätsklasse coNP I

Erinnerung: Sei $L \subseteq \Sigma^*$, dann ist $\bar{L} := \Sigma^* \setminus L$ das Komplement von L.

Theorem

$\text{coNP} = \{L \subseteq \Sigma^* \mid \bar{L} \in \text{NP}\}$.

Beweis

Sei $L \subseteq \Sigma^*$. "Guess and Check" $\rightsquigarrow \bar{L} \in \text{NP}$ genau dann wenn es eine polynomiell zeitbeschränkte DTM M gibt mit

$$x \in \bar{L} \Leftrightarrow \exists_{u \in \Sigma^{p(|x|)}} \langle x, u \rangle \in T(M).$$

Die Komplexitätsklasse coNP I

Erinnerung: Sei $L \subseteq \Sigma^*$, dann ist $\bar{L} := \Sigma^* \setminus L$ das Komplement von L.

Theorem

$\text{coNP} = \{L \subseteq \Sigma^* \mid \bar{L} \in \text{NP}\}$.

Beweis

Sei $L \subseteq \Sigma^*$. "Guess and Check" $\rightsquigarrow \bar{L} \in \text{NP}$ genau dann wenn es eine polynomiell zeitbeschränkte DTM M gibt mit

$$x \in \bar{L} \Leftrightarrow \exists_{u \in \Sigma^{p(|x|)}} \langle x, u \rangle \in T(M).$$

Eine solche DTM M gibt es genau dann, wenn es auch eine polynomiell zeitbeschränkte DTM M' gibt, die genau dann ablehnt, wenn M akzeptiert.

Die Komplexitätsklasse coNP I

Erinnerung: Sei $L \subseteq \Sigma^*$, dann ist $\bar{L} := \Sigma^* \setminus L$ das Komplement von L.

Theorem

$\text{coNP} = \{L \subseteq \Sigma^* \mid \bar{L} \in \text{NP}\}$.

Beweis

Sei $L \subseteq \Sigma^*$. "Guess and Check" $\rightsquigarrow \bar{L} \in \text{NP}$ genau dann wenn es eine polynomiell zeitbeschränkte DTM M gibt mit

$$(*) \quad x \in \bar{L} \Leftrightarrow \exists_{u \in \Sigma^{p(|x|)}} \langle x, u \rangle \in T(M).$$

Eine solche DTM M gibt es genau dann, wenn es auch eine polynomiell zeitbeschränkte DTM M' gibt, die genau dann ablehnt, wenn M akzeptiert. Also gilt

$$\begin{aligned} x \in L \Leftrightarrow x \notin \bar{L} &\Leftrightarrow \neg \left(\exists_{u \in \Sigma^{p(|x|)}} \langle x, u \rangle \in T(M)\right) \\ &\Leftrightarrow \forall_{u \in \Sigma^{p(|x|)}} \langle x, u \rangle \notin T(M) \\ &\Leftrightarrow \forall_{u \in \Sigma^{p(|x|)}} \langle x, u \rangle \in T(M') \end{aligned}$$

Die Komplexitätsklasse coNP II

Erinnerung: Sei $L \subseteq \Sigma^*$, dann ist $\bar{L} := \Sigma^* \setminus L$ das Komplement von L.

Theorem

$\text{coNP} = \{L \subseteq \Sigma^* \mid \bar{L} \in \text{NP}\}$.

Bemerkungen:

- coNP ist nicht das Komplement von NP (z.B. $H \notin \text{NP}$ und $H \notin \text{coNP}$)

Die Komplexitätsklasse coNP II

Erinnerung: Sei $L \subseteq \Sigma^*$, dann ist $\bar{L} := \Sigma^* \setminus L$ das Komplement von L.

Theorem

$\text{coNP} = \{L \subseteq \Sigma^* \mid \bar{L} \in \text{NP}\}$. (*)

Bemerkungen:

- coNP ist nicht das Komplement von NP (z.B. $H \notin \text{NP}$ und $H \notin \text{coNP}$)
- $\text{P} \subseteq \text{NP} \cap \text{coNP}$ (da $L \in \text{P} \Leftrightarrow \bar{L} \in \text{P}$)

$$\begin{aligned} P = P \cap NP = P \cap coNP &= \{L \mid \bar{L} \in NP \wedge L \in P\} \\ &= \{L \mid \bar{L} \in NP \wedge \bar{L} \in P\} \\ &= \{L \mid \bar{L} \in P\} = \{L \mid L \in P\} = P \end{aligned}$$

Die Komplexitätsklasse coNP II

Erinnerung: Sei $L \subseteq \Sigma^*$, dann ist $\bar{L} := \Sigma^* \setminus L$ das Komplement von L.

Theorem

$\text{coNP} = \{L \subseteq \Sigma^* \mid \bar{L} \in \text{NP}\}$.

Bemerkungen:

- coNP ist nicht das Komplement von NP (z.B. $H \notin \text{NP}$ und $H \notin \text{coNP}$)
- $\text{P} \subseteq \text{NP} \cap \text{coNP}$ (da $L \in \text{P} \Leftrightarrow \bar{L} \in \text{P}$)
- coNP-Vollständigkeit analog zu NP-Vollständigkeit:
  $A \subseteq \Sigma^*$ ist coNP-vollständig $\Leftrightarrow \forall_{L \in \text{coNP}}\ L \leq_m^p A$ und $A \in \text{coNP}$

A coNP-schwer

Die Komplexitätsklasse coNP II

Erinnerung: Sei $L \subseteq \Sigma^*$, dann ist $\bar{L} := \Sigma^* \setminus L$ das Komplement von L.

Theorem

$\text{coNP} = \{L \subseteq \Sigma^* \mid \bar{L} \in \text{NP}\}$. (*)

Bemerkungen:

- coNP ist nicht das Komplement von NP (z.B. $H \notin \text{NP}$ und $H \notin \text{coNP}$)
- $\text{P} \subseteq \text{NP} \cap \text{coNP}$ (da $L \in \text{P} \Leftrightarrow \bar{L} \in \text{P}$)
- coNP-Vollständigkeit analog zu NP-Vollständigkeit:
  $A \subseteq \Sigma^*$ ist coNP-vollständig $\Leftrightarrow \forall_{L \in \text{coNP}}\ L \leq_m^p A$ und $A \in \text{coNP}$
- $\overline{\text{SAT}} := \{\langle\varphi\rangle \mid \varphi \text{ ist unerfüllbar}\} \in \text{coNP}$ (sogar coNP-vollständig)

Die Komplexitätsklasse coNP II

Erinnerung: Sei $L \subseteq \Sigma^*$, dann ist $\bar{L} := \Sigma^* \setminus L$ das Komplement von L.

Theorem

$\text{coNP} = \{L \subseteq \Sigma^* \mid \bar{L} \in \text{NP}\}$.

Bemerkungen:

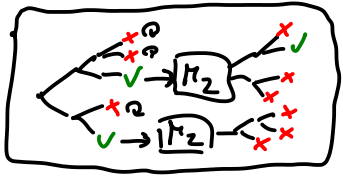
- coNP ist nicht das Komplement von NP (z.B. $H \notin \text{NP}$ und $H \notin \text{coNP}$)
- $\text{P} \subseteq \text{NP} \cap \text{coNP}$ (da $L \in \text{P} \Leftrightarrow \bar{L} \in \text{P}$)
- coNP-Vollständigkeit analog zu NP-Vollständigkeit:
  $A \subseteq \Sigma^*$ ist coNP-vollständig $\Leftrightarrow \forall_{L \in \text{coNP}}\ L \leq_m^p A$ und $A \in \text{coNP}$
- $\overline{\text{SAT}} := \{\varphi \mid \varphi \text{ ist unerfüllbar}\} \in \text{coNP}$ (sogar coNP-vollständig)
- $(\text{P} = \text{NP}) \Rightarrow (\text{NP} = \text{coNP} = \text{P})$
  für alle $L \in \text{coNP}$ gilt: $\bar{L} \in \text{NP} \Rightarrow \bar{L} \in \text{P} \Rightarrow L \in \text{P}$ und somit $L \in \text{NP}$

Die Komplexitätsklasse coNP II

Erinnerung: Sei $L \subseteq \Sigma^*$, dann ist $\bar{L} := \Sigma^* \setminus L$ das Komplement von L.

Theorem

$\text{coNP} = \{L \subseteq \Sigma^* \mid \bar{L} \in \text{NP}\}$.



Bemerkungen:

- coNP ist nicht das Komplement von NP (z.B. $H \notin \text{NP}$ und $H \notin \text{coNP}$)
- $\text{P} \subseteq \text{NP} \cap \text{coNP}$ (da $L \in \text{P} \Leftrightarrow \bar{L} \in \text{P}$)
- coNP-Vollständigkeit analog zu NP-Vollständigkeit:
  $A \subseteq \Sigma^*$ ist coNP-vollständig $\Leftrightarrow \forall_{L \in \text{coNP}}\ L \leq_m^p A$ und $A \in \text{coNP}$
- $\overline{\text{SAT}} := \{\varphi \mid \varphi \text{ ist unerfüllbar}\} \in \text{coNP}$ (sogar coNP-vollständig)
- $(\text{P} = \text{NP}) \Rightarrow (\text{NP} = \text{coNP} = \text{P})$
  für alle $L \in \text{coNP}$ gilt: $\bar{L} \in \text{NP} \Rightarrow \bar{L} \in \text{P} \Rightarrow L \in \text{P}$ und somit $L \in \text{NP}$
- **Offen:** $(\text{NP} = \text{coNP}) \Rightarrow (\text{P} = \text{NP})$?
- Vorsicht: können nicht ohne Weiteres NTM & coNTM „zusammenstecken"

Ein coNP-vollständiges Problem

$(x \vee \overline{x})$

TAUT

Eingabe: aussagenlogische Formel F

Frage: Ist F eine **Tautologie**, d.h. wird F für **alle** $\{0,1\}$-wertigen Belegungen der in F verwendeten Booleschen Variablen zu wahr (d.h. 1) ausgewertet?

F ist Tautologie
$\Leftrightarrow$
$\neg F$ unerfüllbar

$F \in TAUT$
$\Leftrightarrow$
$\neg F \notin SAT$

Ein coNP-vollständiges Problem

TAUT

Eingabe: aussagenlogische Formel F

Frage: Ist F eine **Tautologie**, d.h. wird F für **alle** $\{0,1\}$-wertigen Belegungen der in F verwendeten Booleschen Variablen zu wahr (d.h. 1) ausgewertet?

Theorem

TAUT ist coNP-vollständig.

(1) TAUT $\in$ coNP $\leftarrow$
(2) TAUT coNP-schwer $L \in \text{coNP} \leq_m^p \text{TAUT}$

Ein coNP-vollständiges Problem

TAUT

Eingabe: aussagenlogische Formel F

Frage: Ist F eine **Tautologie**, d.h. wird F für **alle** $\{0,1\}$-wertigen Belegungen der in F verwendeten Booleschen Variablen zu wahr (d.h. 1) ausgewertet?

Theorem

TAUT ist coNP-vollständig.

Beweis

1. $\mathrm{TAUT} \in$ coNP via "Guess and Check" (nicht-erfüllende Belegung zertifiziert $F \notin \mathrm{TAUT}$)

Ein coNP-vollständiges Problem

TAUT

Eingabe: aussagenlogische Formel F

Frage: Ist F eine **Tautologie**, d.h. wird F für **alle** $\{0,1\}$-wertigen Belegungen der in F verwendeten Booleschen Variablen zu wahr (d.h. 1) ausgewertet?

Theorem

TAUT ist coNP-vollständig.

Beweis

1. $\mathrm{TAUT} \in \mathrm{coNP}$ via "Guess and Check" (nicht-erfüllende Belegung zertifiziert $F \notin \mathrm{TAUT}$)
2. TAUT ist coNP-schwer (d.h. $\forall_{L \in \mathrm{coNP}}\ L \leq_m^p \mathrm{TAUT}$):
Da $\bar{L} \in \mathrm{NP}$, gilt $\bar{L} \leq_m^p \mathrm{SAT}$ vermöge einer Polynomzeitreduktion $f : x \mapsto F_x$. Also

Ein coNP-vollständiges Problem

TAUT

Eingabe: aussagenlogische Formel F

Frage: Ist F eine **Tautologie**, d.h. wird F für **alle** $\{0,1\}$-wertigen Belegungen der in F verwendeten Booleschen Variablen zu wahr (d.h. 1) ausgewertet?

Theorem

TAUT ist coNP-vollständig.

Beweis

1. $\mathrm{TAUT} \in \mathrm{coNP}$ via "Guess and Check" (nicht-erfüllende Belegung zertifiziert $F \notin \mathrm{TAUT}$)
2. TAUT ist coNP-schwer (d.h. $\forall_{L \in \mathrm{coNP}}\ L \leq_m^p \mathrm{TAUT}$):
Da $\bar{L} \in \mathrm{NP}$, gilt $\bar{L} \leq_m^p \mathrm{SAT}$ vermöge einer Polynomzeitreduktion $f : x \mapsto F_x$. Also

$$x \in L \Leftrightarrow x \notin \bar{L} \Leftrightarrow F_x \notin \mathrm{SAT} \Leftrightarrow \neg F_x \in \mathrm{TAUT}.$$

Reduktionseigenschaft v. f

Ein coNP-vollständiges Problem

TAUT

Eingabe: aussagenlogische Formel F

Frage: Ist F eine **Tautologie**, d.h. wird F für **alle** $\{0,1\}$-wertigen Belegungen der in F verwendeten Booleschen Variablen zu wahr (d.h. 1) ausgewertet?

Theorem

TAUT ist coNP-vollständig.

Beweis

1. $\mathrm{TAUT} \in \mathrm{coNP}$ via "Guess and Check" (nicht-erfüllende Belegung zertifiziert $F \notin \mathrm{TAUT}$)

2. TAUT ist coNP-schwer (d.h. $\forall_{L \in \mathrm{coNP}}\ L \leq_m^p \mathrm{TAUT}$):
Da $\bar{L} \in \mathrm{NP}$, gilt $\bar{L} \leq_m^p \mathrm{SAT}$ vermöge einer Polynomzeitreduktion $f : x \mapsto F_x$. Also

$$x \in L \Leftrightarrow x \notin \bar{L} \Leftrightarrow F_x \notin \mathrm{SAT} \Leftrightarrow \neg F_x \in \mathrm{TAUT}.$$

Also ist $g : x \mapsto \neg F_x$ eine Polynomzeitreduktion von L auf TAUT.