Logische Complexiteit

XIII : Tijdcomplexiteitsklassen

Jeroen Goudsmit
Universiteit Utrecht
donderdag 22 maart 2012

Polynomiale Tijd

$$\mathrm{P} := \bigcup_{k \in \mathbb{N}} \mathrm{Time}\left(n^k\right)$$

Voorbeeld

$$\{ *^n \mid n \text{ is een fibonaccigetal } \}$$

Voorbeeld

$$\{ *^n \mid n \text{ is een fibonaccigetal } \}$$

M = "Op invoer w:

1. Vervang de eerste $*$ door een 1. Is er geen, verwerp.
2. Vervang de eerste $*$ door een 2. Is er geen, accepteer.
3. Test of nog $*$'en over zijn. Zo nee, accepteer.
4. Per 1 op de tape, vervang de eerste $*$ door een 3. Als er geen $*$ over is, verwerp.
5. Verander alle 2's in 1's.
6. Verander alle 3's in 2's.
7. Ga naar toestand 3.

Voorbeeld

$$\text{Path} := \left\{ \langle G, s, t \rangle \;\middle|\; \begin{array}{l} G \text{ is een gerichte graaf} \\ \text{met een pad van } s \text{ naar } t \end{array} \right\}$$

Voorbeeld

$$\text{Path} := \left\{ \langle G, s, t \rangle \;\middle|\; \begin{array}{l} G \text{ is een gerichte graaf} \\ \text{met een pad van } s \text{ naar } t \end{array} \right\}$$

M = "Op invoer $\langle$ G, s, t $\rangle$ met G een graaf en k, s knopen:

1. Markeer knoop s.
2. Voor elke pijl $\langle a, b \rangle$, als a gemarkeerd is, markeer b
3. Als er een nieuwe knoop gemarkeerd is, ga naar 2.
4. Als t gemarkeerd is, accepteer. Zo niet, verwerp."

Voorbeeld

$$\text{Path} := \left\{ \langle G, s, t \rangle \;\middle|\; \begin{array}{l} G \text{ is een gerichte graaf} \\ \text{met een pad van } s \text{ naar } t \end{array} \right\}$$

$\langle V, E \rangle$

M = "Op invoer $\langle$ G, s, t $\rangle$ met G een graaf en k, s knopen:

1. Markeer knoop s.
2. Voor elke pijl $\langle a, b \rangle$, als a gemarkeerd is, markeer b
3. Als er een nieuwe knoop gemarkeerd is, ga naar 2.
4. Als t gemarkeerd is, accepteer. Zo niet, verwerp."

Voorbeeld

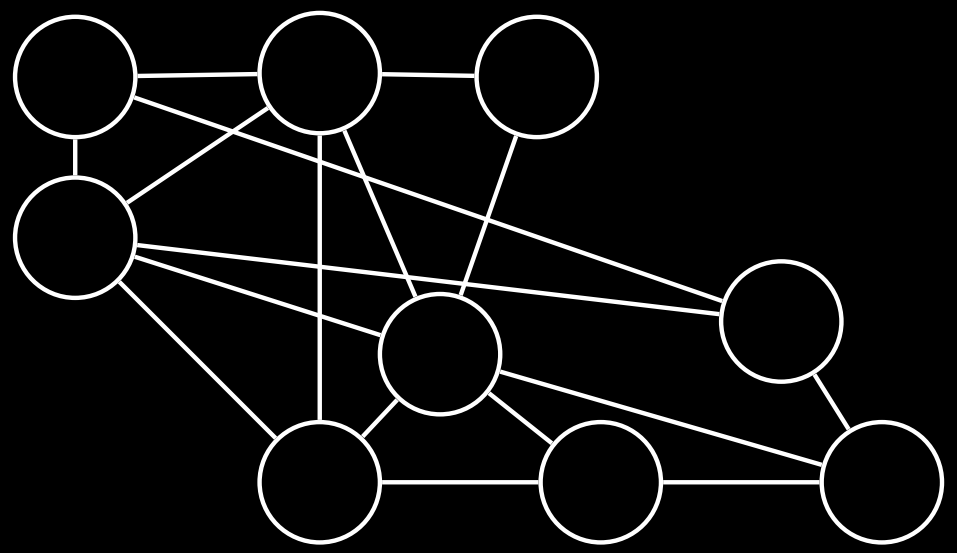
$$\text{Path} := \left\{ \langle G, s, t \rangle \;\middle|\; \begin{array}{l} G \text{ is een gerichte graaf} \\ \text{met een pad van } s \text{ naar } t \end{array} \right\}$$

$\langle V, E \rangle$

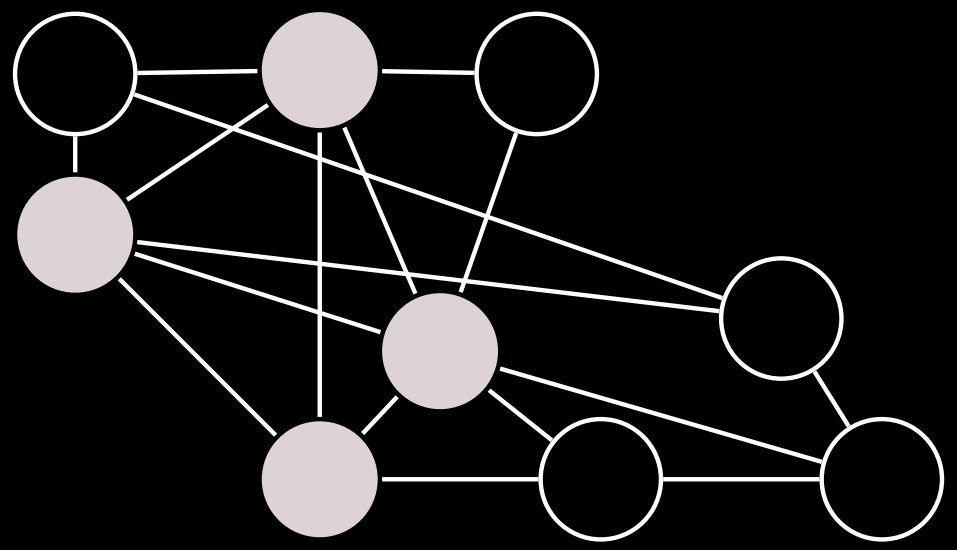
M = "Op invoer $\langle$ G, s, t $\rangle$ met G een graaf en k, s knopen:

1. Markeer knoop s. $O(1)$
2. Voor elke pijl $\langle a, b \rangle$, als a gemarkeerd is, markeer b $O(|E|)$
3. Als er een nieuwe knoop gemarkeerd is, ga naar 2. $O(1)$
4. Als t gemarkeerd is, accepteer. Zo niet, verwerp." $O(1)$

Moeilijk Probleem



Moeilijk Probleem



Clique

R. Duncan Luce

National Science Foundation

Clique

$$\text{Clique} := \left\{ \langle G, k \rangle \;\middle|\; \begin{array}{c} G \text{ een ongerichte} \\ \text{graaf met } k\text{-kliek} \end{array} \right\}$$

Clique

$$\text{Clique} := \left\{ \langle G, k \rangle \;\middle|\; \begin{array}{l} G \text{ een ongerichte} \\ \text{graaf met } k\text{-kliek} \end{array} \right\}$$

M = "Op invoer $\langle \langle G, k \rangle, W \rangle$ met G een graaf en $k \in \mathbb{N}$:

1. Test of W een lijstje knopen is uit G.
2. Per paar knopen in W, kijk test of een pijl in G ze verbind.
3. Als alle tests succesvol verliepen, accepteer. Zo niet, verwerp."

Getuigen

Definitie

Een beslisser M heet een controleur voor $\mathcal{L}$ wanneer:

$$w \in \mathcal{L} \quad \text{precies als} \langle w, c \rangle \in \mathcal{L}(M) \text{ voor een getuige } c$$

Getuigen

Definitie
Een beslisser M heet een controleur voor $\mathcal{L}$ wanneer:

$$w \in \mathcal{L} \quad \text{precies als} \langle w, c \rangle \in \mathcal{L}(M) \text{ voor een getuige } c$$

Zeg dat ze in polynomiale tijd werkt als de tijdscomplexiteit polynomiaal is in de grootte van w.

Getuigen

Definitie
Een beslisser M heet een controleur voor $\mathcal{L}$ wanneer:

$$w \in \mathcal{L} \quad \text{precies als} \langle w, c \rangle \in \mathcal{L}(M) \text{ voor een getuige } c$$

Zeg dat ze in polynomiale tijd werkt als de tijdscomplexiteit polynomiaal is in de grootte van w.

Noem $\mathcal{L}$ dan polynomiaal controleerbaar.

Nondetermistisch Polynomiale Tijd

$$\mathrm{NP} := \left\{ \begin{array}{c} \text{polynomiaal} \\ \text{controleerbare} \\ \text{talen} \end{array} \right\}$$

Alternatieve formulering

$\mathcal{L}$ zit in NP precies als $\mathcal{L}$ in polynomiale tijd besloten wordt door een nondeterministische TM.

Vervulbaarheid

$$\mathrm{Sat} := \left\{ \langle \phi \rangle \;\middle|\; \begin{array}{l} \phi \text{ is een vervulbare} \\ \text{propositionele formule} \end{array} \right\}$$

Vervulbaarheid Beperkt

$$\mathrm{3Sat} := \left\{ \langle \phi \rangle \;\middle|\; \begin{array}{l} \phi \text{ is een vervulbare} \\ \text{propositionele formule} \\ \text{in 3-CNV} \end{array} \right\}$$

Vervulbaarheid Beperkt

$$\mathrm{3Sat} := \left\{ \langle \phi \rangle \;\middle|\; \begin{array}{l} \phi \text{ is een vervulbare} \\ \text{propositionele formule} \\ \text{in 3-CNV} \end{array} \right\}$$

conjunctieve normaalvorm met precies drie atomen per clausule

3Sat Oplossen

Lemma

3Sat *reduceert tot* Clique.

3Sat Oplossen

Lemma

3Sat *reduceert tot* Clique.

Bewijs.

Gegeven een formule $\phi = \phi_1 \wedge \phi_2 \wedge \ldots \wedge \phi_n$ maken we een ongerichte graaf $G = \langle V, E \rangle$.

3Sat Oplossen

Lemma

3Sat *reduceert tot* Clique.

Bewijs.

Gegeven een formule $\phi = \phi_1 \wedge \phi_2 \wedge \ldots \wedge \phi_n$ maken we een ongerichte graaf $G = \langle V, E \rangle$. Definieer de knopen als volgt

$$V \quad := \quad \{ \langle a, i \rangle \mid \text{het atoom } a \text{ komt voor in } \phi_i \} \ .$$

Trek een pijl tussen $\langle a, i \rangle$ en $\langle b, j \rangle$ als $a \wedge b$ vervulbaar is en $i \neq j$.

3Sat Oplossen

Lemma

3Sat *reduceert tot* Clique.

Bewijs.

Gegeven een formule $\phi = \phi_1 \wedge \phi_2 \wedge \ldots \wedge \phi_n$ maken we een ongerichte graaf $G = \langle V, E \rangle$. Definieer de knopen als volgt

$$V \quad := \quad \{ \langle a, i \rangle \mid \text{het atoom } a \text{ komt voor in } \phi_i \} \ .$$

Trek een pijl tussen $\langle a, i \rangle$ en $\langle b, j \rangle$ als $a \wedge b$ vervulbaar is en $i \neq j$.

Stel G heeft een n-kliek, zeg
W.

3Sat Oplossen

Lemma
3Sat *reduceert tot* Clique.

Bewijs.
Gegeven een formule $\phi = \phi_1 \wedge \phi_2 \wedge \ldots \wedge \phi_n$ maken we een ongerichte graaf $G = \langle V, E \rangle$. Definieer de knopen als volgt

$$V \quad := \quad \{ \langle a, i \rangle \mid \text{het atoom } a \text{ komt voor in } \phi_i \} \ .$$

Trek een pijl tussen $\langle a, i \rangle$ en $\langle b, j \rangle$ als $a \wedge b$ vervulbaar is en $i \neq j$.

Stel G heeft een n-kliek, zeg W. Definieer bedeling die p waar maakt als $\langle p, i \rangle \in W$ of $\langle \neg p, j \rangle \notin W$ voor een i.

3Sat Oplossen

Lemma
3Sat *reduceert tot* Clique.

Bewijs.
Gegeven een formule $\phi = \phi_1 \wedge \phi_2 \wedge \ldots \wedge \phi_n$ maken we een ongerichte graaf $G = \langle V, E \rangle$. Definieer de knopen als volgt

$$V \quad := \quad \{ \langle a, i \rangle \mid \text{het atoom } a \text{ komt voor in } \phi_i \} \ .$$

Trek een pijl tussen $\langle a, i \rangle$ en $\langle b, j \rangle$ als $a \wedge b$ vervulbaar is en $i \neq j$.

Stel G heeft een n-kliek, zeg W. Definieer bedeling die p waar maakt als $\langle p, i \rangle \in W$ of $\langle \neg p, j \rangle \notin W$ voor een i. Deze bedeling maakt ϕ waar.

3Sat Oplossen

Lemma

3Sat *reduceert tot* Clique.

Bewijs.

Gegeven een formule $\phi = \phi_1 \wedge \phi_2 \wedge \ldots \wedge \phi_n$ maken we een ongerichte graaf $G = \langle V, E \rangle$. Definieer de knopen als volgt

$$V \quad := \quad \{ \langle a, i \rangle \mid \text{het atoom } a \text{ komt voor in } \phi_i \} \ .$$

Trek een pijl tussen $\langle a, i \rangle$ en $\langle b, j \rangle$ als $a \wedge b$ vervulbaar is en $i \neq j$.

Stel G heeft een n-kliek, zeg W. Definieer bedeling die p waar maakt als $\langle p, i \rangle \in W$ of $\langle \neg p, j \rangle \notin W$ voor een i. Deze bedeling maakt ϕ waar.

Stel ϕ heeft een vervullende bedeling, zeg σ.

3Sat Oplossen

Lemma

3Sat *reduceert tot* Clique.

Bewijs.

Gegeven een formule $\phi = \phi_1 \wedge \phi_2 \wedge \ldots \wedge \phi_n$ maken we een ongerichte graaf $G = \langle V, E \rangle$. Definieer de knopen als volgt

$$V \quad := \quad \{ \langle a, i \rangle \mid \text{het atoom } a \text{ komt voor in } \phi_i \} \ .$$

Trek een pijl tussen $\langle a, i \rangle$ en $\langle b, j \rangle$ als $a \wedge b$ vervulbaar is en $i \neq j$.

Stel G heeft een n-kliek, zeg W. Definieer bedeling die p waar maakt als $\langle p, i \rangle \in W$ of $\langle \neg p, j \rangle \notin W$ voor een i. Deze bedeling maakt ϕ waar.

Stel ϕ heeft een vervullende bedeling, zeg σ. Kies per $0 \leq i \leq n$ een atoom a zodat $\sigma(a)$ waar is. Dit geeft een n-kiek.

$\blacksquare$

Reductie

Definitie
Een functie $f : \Sigma^* \to \Sigma^*$ is in polynomiale tijd berekenbaar als:

1. er is een TM M die f berekent;
2. M werkt in polynomiale tijd.

Reductie

Definitie
Een functie $f : \Sigma^* \to \Sigma^*$ is in polynomiale tijd berekenbaar als:

1. er is een TM M die f berekent;
2. M werkt in polynomiale tijd.

Definitie
A is in polynomiale tijd te reduceren tot B wanneer er een in polynomiale tijd berekenbare functie f bestaat zó dat:

$$w \in A \quad \text{precies als} \quad f(w) \in B$$

Reductie

Definitie
Een functie $f : \Sigma^* \to \Sigma^*$ is in polynomiale tijd berekenbaar als:

1. er is een TM M die f berekent;
2. M werkt in polynomiale tijd.

Definitie
A is in polynomiale tijd te reduceren tot B wanneer er een in polynomiale tijd berekenbare functie f bestaat zó dat:

$$w \in A \quad \text{precies als} \quad f(w) \in B$$

Schrijf $A \leq_{\mathrm{P}} B$.

NP-volledigheid

Definitie

$\mathcal{L}$ heet NP-volledig als $\mathcal{L}$ in NP zit, en voor alle $A \in \mathrm{NP}$ geldt $A \leq_{\mathrm{P}} \mathcal{L}$.

NP-volledigheid

Definitie
$\mathcal{L}$ heet NP-volledig als $\mathcal{L}$ in NP zit, en voor alle $A \in \mathrm{NP}$ geldt $A \leq_{\mathrm{P}} \mathcal{L}$.

Lemma
De relatie $\leq_{\mathrm{P}}$ is transitief.

NP-volledigheid

Definitie

$\mathcal{L}$ heet NP-volledig als $\mathcal{L}$ in NP zit, en voor alle $A \in \mathrm{NP}$ geldt $A \leq_{\mathrm{P}} \mathcal{L}$.

Lemma

De relatie $\leq_{\mathrm{P}}$ is transitief.

Gevolg

Als een NP-volledig probleem reduceert tot $\mathcal{L}$, dan is $\mathcal{L}$ NP-volledig als ze in NP zit.

$$\text{wil dat} \quad \forall A \in \mathrm{NP}.\ A \leq_{\mathrm{P}} \mathcal{L}$$

NP-volledigheid

Definitie

$\mathcal{L}$ heet NP-volledig als $\mathcal{L}$ in NP zit, en voor alle $A \in \mathrm{NP}$ geldt $A \leq_{\mathrm{P}} \mathcal{L}$.

Lemma

De relatie $\leq_{\mathrm{P}}$ is transitief.

Gevolg

Als een NP-volledig probleem reduceert tot $\mathcal{L}$, dan is $\mathcal{L}$ NP-volledig als ze in NP zit.

$$\begin{aligned} \text{wil dat} \quad & \forall A \in \mathrm{NP}.\ A \leq_{\mathrm{P}} \mathcal{L} \\ \text{weet} \quad & \forall A \in \mathrm{NP}.\ A \leq_{\mathrm{P}} B \leq_{\mathrm{P}} \mathcal{L} \end{aligned}$$

NP-volledigheid

Definitie

$\mathcal{L}$ heet NP-volledig als $\mathcal{L}$ in NP zit, en voor alle $A \in \mathrm{NP}$ geldt $A \leq_{\mathrm{P}} \mathcal{L}$.

Lemma

De relatie $\leq_{\mathrm{P}}$ is transitief.

Gevolg

Als een NP-volledig probleem reduceert tot $\mathcal{L}$, dan is $\mathcal{L}$ NP-volledig als ze in NP zit.

$$\begin{aligned} \text{wil dat} \quad & \forall A \in \mathrm{NP}.\ A \leq_{\mathrm{P}} \mathcal{L} \\ \text{weet} \quad & \forall A \in \mathrm{NP}.\ A \qquad \leq_{\mathrm{P}} \mathcal{L} \end{aligned}$$

Stephen Cook
Jiří Janíček

Leonid Levin

Cook–Levin Stelling

$$\mathrm{Sat} \in \mathrm{P} \quad \text{precies als} \quad \mathrm{P} = \mathrm{NP}$$

Cook–Levin Stelling

Sat is NP-volledig

Cook–Levin Stelling

$$\forall A \in \mathrm{NP}.\ A \leq_{\mathrm{P}} \mathrm{Sat}$$

Gezien

Tijdscomplexiteit

Gezien

Tijdscomplexiteit

P

Praktisch
berekenbaar

Gezien

Tijdscomplexiteit

P

Praktisch berekenbaar

NP

Sat, 3Sat, Clique

Gezien

Tijdscomplexiteit

P

Praktisch berekenbaar

Reducties

Als voorheen, maar met tijdscomplexiteit.

NP

Sat, 3Sat, Clique

Gezien

Tijdscomplexiteit

P

Praktisch berekenbaar

Reducties

Als voorheen, maar met tijdscomplexiteit.

NP

Sat, 3Sat, Clique

NP-volledige problemen