Syntaks og semantik

Lektion 8

6 marts 2008

Pumpelemmaet og dets anvendelser

Sætning 2.34: Hvis A er et kontekstfrit sprog, så findes der et (naturligt) tal p således at ethvert ord $s \in A$ der har længde mindst p kan opsplittes i fem stykker, $s = uvxyz$, med

- $|vy| > 0$ og $|vxy| \leq p$,
- og således at ordene $uv^ixy^iz \in A$ for alle $i \in \mathbb{N}_0$.

Bevis (oversigt):

1. Lad G være en CFG der genererer A, med $n = |V|$ variable.
2. Vælg p således at der gælder for enhver streng $s \in A$ med $|s| \geq p$, at ethvert parsetræ for s har højde mindst $n + 1$.
3. Tag en streng $s \in A$ med $|s| \geq p$, og tag et af dens laveste parsetræer. Dette træ indeholder en sti med mindst $n + 2$ punkter.
4. Der er $n + 1$ variable på den sti, så en af dem må forekomme to gange. En løkke.
5. Skriv $s = uvxyz$, hvor x deriveres af den sidste forekomst af den dobbelte variabel, og vxy af den næstsidste.
6. Erstat den dobbelte variabels del-parsetræer med hinanden (rekursivt) for at få parsetræer for alle uv^ixy^iz. Voilà.

Udsagnslogik beskæftiger sig med logiske udsagn som kan være enten sande eller falske.

- Månen er en grøn ost.
- Enhver CFG kan konverteres til en PDA.

Givet udsagn p, q, etc. kan vi danne kombinerede udsagn:

$\neg p$: Negationen af p. Sandt hvis p er falsk, falsk hvis p er sandt.

$p \wedge q$: Konjunktionen af p og q. Sandt hvis p og q begge er sande.

$p \vee q$: Alternativet mellem p og q. Sandt hvis p eller q (eller begge) er sandt.

$p \Rightarrow q$: Implikationen fra p til q. Sandt hvis p er falsk eller q er sandt.

Vigtige sætninger:

- $\neg(p \wedge q) = \neg p \vee \neg q \quad \neg(p \vee q) = \neg p \wedge \neg q$ (De Morgans love)
- $p \Rightarrow q = \neg p \vee q$ (direkte fra definitionen
- $p \Rightarrow q = \neg q \Rightarrow \neg p$ (Kontraposition)

Prædikatlogik beskæftiger sig med udsagn der er kvalificerede med kvantorer:

$\forall x : p(x)$: For alle x gælder udsagnet $p(x)$.
$\exists x : p(x)$: Der findes et x for hvilket udsagnet $p(x)$ er sandt.

Eksempler:

- $\forall x \in \mathbb{Z} : x^2 \geq 0$ For alle heltal x er $x^2 \geq 0$. Sandt.
- $\forall x \in \mathbb{Z} : \exists y \in \mathbb{Z} : x + y = 0$ For alle heltal x findes der et heltal y for hvilket $x + y = 0$. Sandt.
- $\forall x \in \mathbb{N} : \exists y \in \mathbb{N} : x + y = 0$ For alle naturlige tal x findes der et naturligt tal y for hvilket $x + y = 0$. Falsk.
- $\mathrm{PRIM}(p) = \forall i \in \mathbb{N} : \big((i > 1 \wedge i < p) \Rightarrow p \bmod i \neq 0\big)$
  p er et primtal.
- $\forall x \in \mathbb{N} : \exists p \in \mathbb{N} : \big(p > x \wedge \mathrm{PRIM}(p)\big)$
  Der findes uendeligt mange primtal. Sandt.

Negation af kvantorer:

- $\neg(\forall x : p(x)) = \exists x : \neg p(x)$
- $\neg(\exists x : p(x)) = \forall x : \neg p(x)$

Konstruktivt bevis: At vise en sætning ved at konstruere det der påstås.

- Der findes en algoritme der konverterer NFAs til DFAs
  Bevis ved at opskrive algoritmen
- Ethvert kontekstfrit sprog kan genkendes af en PDA
  Bevis ved at opskrive en algoritme der konverterer CFGs til PDAs

Direkte bevis: At vise konklusionen som en logisk konsekvens af forudsætningerne og generelle sandheder.

- Alle konstruktive beviser er direkte.
- De fleste direkte beviser er konstruktive.

Indirekte bevis: At vise en påstand ved at antage at den er forkert.

- ved kontraposition: At bevise $p \Rightarrow q$ ved at give et bevis for $\neg q \Rightarrow \neg p$.
- ved modstrid: At bevise p ved at antage at p er forkert og komme frem til en logisk modstrid.
- at bevise $p \Rightarrow q$ ved modstrid:
  - Antag $\neg(p \Rightarrow q)$.
  - Bemærk at $\neg(p \Rightarrow q) = \neg(\neg p \vee q) = p \wedge \neg q$.
  - Dvs. vi antager at forudsætningen p holder, men at konklusionen q er falsk. Specielt kan p indgå som argument i beviset.

- Det kan være svært at kende forskel på kontrapositions- og modstridsbeviser.
- Alle indirekte beviser er ikke-konstruktive.

Sætning: $\sqrt{2}$ er et irrationelt tal.

Bevis:

1. *Antag* at $\sqrt{2}$ er et *rationelt* tal.
2. Så må det kunne skrives som en brøk: $\sqrt{2} = \frac{a}{b}$, for to positive heltal a og b.
3. Lad brøken være *reduceret*, dvs. specielt er ikke både a og b lige tal.
4. $\frac{a}{b} = \sqrt{2}$ medfører at $2b^2 = a^2$.
5. Hvis a er ulige, er a^2 også ulige, modstrid til (4).
6. Dvs. a må være et lige tal, og med (3) må b så være ulige.
7. Skriv $a = 2c$. Så er $2b^2 = a^2 = 4c^2$, dvs. $b^2 = 2c^2$.
8. Men b er ulige, så det er b^2 også, modstrid til (7).
9. Antagelsen om at $\sqrt{2}$ var et rationelt tal ledte frem til et modstrid, så den må være forkert. Konklusion: $\sqrt{2}$ er et irrationelt tal.

Sætning: Der findes uendeligt mange primtal.

Bevis:

1. *Antag* at der kun findes endeligt mange primtal. Kald dem $p_1, p_2, \ldots, p_k$.
2. Lad $N = p_1 p_2 \ldots p_k + 1$.
3. N er større end ethvert af primtallene, så det kan ikke være et primtal selv.
4. Dvs. der er et primtal der går op i N. Kald det p_i.
5. Men $N - 1 = p_1 p_2 \ldots p_k$, så p_i går også op i $N - 1$.
6. Derfor går p_i op i $N - (N - 1) = 1$, modstrid.
7. Antagelsen om at der kun findes endeligt mange primtal ledte frem til et modstrid, så den må være forkert. Konklusion: Der findes uendeligt mange primtal.

Sætning: Der findes ikke nogen generel algoritme der kan afgøre om et program går i uendelig løkke.

Præcisering: Følgende algoritme HALT findes ikke:

1. HALT (algoritme P, streng s) :
2. hvis algoritmen P, givet s som input, standser, output "FINT"
3. ellers (hvis P med input s går i uendelig løkke) output "HOVSA"

Med andre ord: Standseproblemet er uafgørbart.

Flere andre ord: Generel softwareverifikation er umulig.

Og en masse andre dårlige nyheder som konsekvens.

(Meget mere om det på næste semester!)

Sætning: Følgende algoritme HALT findes ikke:

1. HALT (algoritme P, streng s) :
2. hvis algoritmen P, givet s som input, standser, output "FINT"
3. ellers (hvis P med input s går i uendelig løkke) output "HOVSA"

Bevis:

1. Antag at HALT findes.
2. Definér følgende nye algoritme:
   1. HEST (algoritme P) :
   2. hvis HALT (P, P) = "HOVSA!", output SANDT
   3. ellers gå i uendelig løkke
3. Hvis HEST (HEST) går i uendelig løkke, må HALT (HEST, HEST) være "FINT", dvs. HEST standser givet input HEST. Modstrid!
4. Hvis HEST (HEST) standser, må HALT (HEST, HEST) være "HOVSA", dvs. HEST går i uendelig løkke givet input HEST. Modstrid!

Pumpelemma: Hvis A er et kontekstfrit sprog, så findes der et (naturligt) tal p således at ethvert ord $s \in A$ der har længde mindst p kan opsplittes i fem stykker, $s = uvxyz$, med

- $|vy| > 0$ og $|vxy| \leq p$,
- og således at ordene $uv^ixy^iz \in A$ for alle $i \in \mathbb{N}_0$.

Indfør pumpe-egenskaben $\mathrm{PE}(s, A)$:

$$\mathrm{PE}(s, A) := \exists u, v, x, y, z : (s = uvxyz \wedge |vy| > 0 \wedge |vxy| \leq p \wedge \forall i \in \mathbb{N}_0 : uv^ixy^iz \in A)$$

Så er pumpelemmaet:

$$A \in \mathrm{CFL} \Rightarrow (\exists p \in \mathbb{N} : \forall s \in A : (|s| \geq p \Rightarrow PE(s, A))$$

Pumpe-egenskaben PE(s, A) : der findes en opsplitning $s = uvxyz$ således at

- $|vy| > 0$ og $|vxy| \leq p$,
- og således at ordene $uv^ixy^iz \in A$ for alle $i \in \mathbb{N}_0$.

$$\mathrm{PE}(s, A) = \exists u, v, x, y, z : (s = uvxyz \wedge |vy| > 0 \wedge |vxy| \leq p \wedge \forall i \in \mathbb{N}_0 : uv^ixy^iz \in A)$$

Pumpelemmaet: Hvis A er et kontekstfrit sprog, så findes der et (naturligt) tal p således at ethvert ord $s \in A$ der har længde mindst p opfylder PE(s, A).

At anvende pumpelemmaet:

1. Givet et konkret sprog A, vis at A ikke er kontekstfrit:
2. Antag at A er kontekstfrit, så holder pumpelemmaet for A.
3. Dvs. vi har en (ukonkret) pumpelængde p således at $\forall s \in A : (|s| \geq p \Rightarrow PE(s, A))$.
4. Demonstrér ved eksempel at der findes et $s \in A$ med $|s| \geq p$ og $\neg PE(s, A)$. Modstrid til (3)!

$$\mathrm{PE}(s, A) = \exists u, v, x, y, z : (s = uvxyz \land |vy| > 0 \land |vxy| \leq p \land \forall i \in \mathbb{N}_0 : uv^i xy^i z \in A)$$

1. Givet et konkret sprog A, vis at A ikke er kontekstfrit:
2. Antag at A er kontekstfrit, så holder pumpelemmaet for A.
3. Dvs. vi har en (ukonkret) pumpelængde p således at $\forall s \in A : (|s| \geq p \Rightarrow PE(s, A))$.
4. Demonstrér ved eksempel at der findes et $s \in A$ med $|s| \geq p$ og $\neg PE(s, A)$. Modstrid til (3)!

$$\neg\mathrm{PE}(s, A) = \forall u, v, x, y, z : ((s = uvxyz \land |vy| > 0 \land |vxy| \leq p) \Rightarrow \exists i \in \mathbb{N}_0 : uv^i xy^i z \notin A)$$

Eksempel 2.36: Sproget $B = \{a^n b^n c^n \mid n \in \mathbb{N}_0\}$ er ikke kontekstfrit:

Bevis:

1. Antag at B er kontekstfrit, og lad p være dets pumpelængde.
2. Lad $s = a^p b^p c^p$. *(Et smart valg!)* Vi har $|s| \geq p$.
3. Lad $s = uvxyz$ være den opsplitning af s som pumpelemmaet garanterer. *(Vi ved den findes. Vi ved ikke hvordan den ser ud!)*
4. Hvis v og y hver kun indeholder én slags af symbolerne a, b og c, er der et af symbolerne der ikke er med i v eller y. Strengen uv^2xy^2z indeholder så for få symboler af denne slags og er derfor ikke indeholdt i B, modstrid!
5. Hvis v eller y indeholder mere end én slags symboler, optræder de i uv^2xy^2z i forkert rækkefølge $\Rightarrow$ $uv^2xy^2z \notin B$, modstrid!
6. Ligegyldigt hvad får vi en modstrid. $\Rightarrow$ antagelsen forkert $\Rightarrow$ B er ikke kontekstfrit.

Eksempel 2.38: Sproget $D = \{ww \mid w \in \{0,1\}^*\}$ er ikke kontekstfrit:

Bevis:

1. Antag at D er kontekstfrit, og lad p være dets pumpelængde.
2. Lad $s = 0^p1^p0^p1^p$. Vi har $|s| \geq p$. Lad $s = uvxyz$ være den opsplitning af s som pumpelemmaet garanterer.
3. Hvis strengen vxy er en del af det første 0^p1^p i s, starter anden halvdel af uv^2xy^2z med et 1. Men første halvdel starter stadig med 0, så $uv^2xy^2z \notin D$, modstrid!
4. Hvis strengen vxy er en del af det andet 0^p1^p i s, slutter første halvdel af uv^2xy^2z med et 0, men anden halvdel slutter med 1, så $uv^2xy^2z \notin D$, modstrid!
5. Så strengen vxy må indeholde midten af s, dvs. vxy er en del af det midterste 1^p0^p. Men $|vy| > 0$, så $|x| < |vxy|$, dvs. $uv^0xy^0z = 0^p1^i0^j1^p$ med $i < p$ eller $j < p$, så $uv^0xy^0z \notin D$, modstrid!