SAT Introslides

DM573

Rolf Fagerberg

Recap: Boolske funktioner

Nogle velkendte Boolske funktioner:

x	$\neg x$
0	1
1	0

x_1	x_2	$x_1 \wedge x_2$
0	0	0
0	1	0
1	0	0
1	1	1

x_1	x_2	$x_1 \vee x_2$
0	0	0
0	1	1
1	0	1
1	1	1

Boolske funktioner

Ny funktion (nyt navn for én af de 16 mulige Boolske funktioner med to input-variable):

x_1	x_2	$x_1 \Rightarrow x_2$
0	0	1
0	1	1
1	0	0
1	1	1

Boolske funktioner

Ny funktion (nyt navn for én af de 16 mulige Boolske funktioner med to input-variable):

x_1	x_2	$x_1 \Rightarrow x_2$
0	0	1
0	1	1
1	0	0
1	1	1

Bemærk:

x_1	x_2	$\neg x_1 \vee x_2$
0	0	1
0	1	1
1	0	0
1	1	1

Ækvivalens af Boolske funktioner

To Boolske udtryk siges at være **ækvivalente**, hvis de har samme tabel.

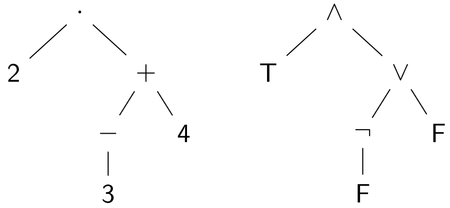
Så $x_1 \Rightarrow x_2$ og $\neg x_1 \vee x_2$ er ækvivalente, og kan erstatte hinanden.

x_1	x_2	$x_1 \Rightarrow x_2$
0	0	1
0	1	1
1	0	0
1	1	1

x_1	x_2	$\neg x_1 \vee x_2$
0	0	1
0	1	1
1	0	0
1	1	1

Udtrykstræer

Husk at Boolske udtryk (lige som for normale algebraiske udtryk), er udtrykstræer, hvor beregningen går nedefra og op.



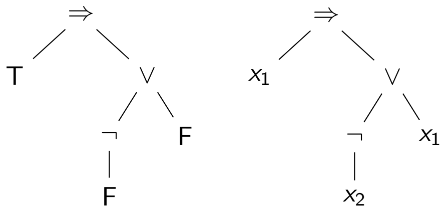
Input: tal	Input: Booleans
Output: tal	Output: Booleans

$2 \cdot ((-3) + 4) \qquad T \wedge ((\neg F) \vee F)$

Vi bruger parenteser til at lave en lineær beskrivelse af den hierarkiske struktur.

Udtrykstræer

Funktionen $\Rightarrow$ kan naturligvis også indgå i et udtryk(stræ):



$$T \Rightarrow ((\neg F) \vee F) \qquad x_1 \Rightarrow ((\neg x_2) \vee x_1)$$

Hvis bladene er Boolske variable, giver udtrykket en ny Boolsk funktion (en ny tabel).

Satisfiability

Et Boolsk udtryk med n variable $x_1, x_2, \ldots, x_n$, kaldes **satisfiable** hvis der findes et sæt værdier (f.eks. $x_1 = F, x_2 = S, \ldots, x_n = F$) som gør hele udtrykket sandt.

Dvs. hvis der findes en linje i udtrykkets tabel, hvor output er 1.

Satisfiability

Et Boolsk udtryk med n variable $x_1, x_2, \ldots, x_n$, kaldes **satisfiable** hvis der findes et sæt værdier (f.eks. $x_1 = F, x_2 = S, \ldots, x_n = F$) som gør hele udtrykket sandt.

Dvs. hvis der findes en linje i udtrykkets tabel, hvor output er 1.

SAT problemet: givet et Boolsk udtryk med n variable, afgør om det er satisfiable (og hvis ja, find et satisfying sæt værdier for $x_1, x_2, \ldots, x_n$).

Conjunctive Normal Form (CNF)

Et Boolsk udtryk er på **CNF form** hvis det er en konjunktion (ANDs) af disjunktioner (ORs) af literals (variable og negerede variable).

Eksempel:

$$(x_1 \vee \neg x_2 \vee x_4) \wedge (x_2 \vee x_3) \wedge (\neg x_1 \vee x_2 \vee \neg x_4 \vee \neg x_5) \wedge (\neg x_1 \vee x_3 \vee x_5)$$

Conjunctive Normal Form (CNF)

Et Boolsk udtryk er på **CNF form** hvis det er en konjunktion (ANDs) af disjunktioner (ORs) af literals (variable og negerede variable).

Eksempel:

$$(x_1 \vee \neg x_2 \vee x_4) \wedge (x_2 \vee x_3) \wedge (\neg x_1 \vee x_2 \vee \neg x_4 \vee \neg x_5) \wedge (\neg x_1 \vee x_3 \vee x_5)$$

Om notation: Bemærk, at $a \vee (b \vee c)$ er ækvivalent med $(a \vee b) \vee c$, dvs. har samme tabel. Parenteser mellem $\vee$ kan derfor udelades, og vi skriver blot $a \vee b \vee c$. Tilsvarende er $a \wedge (b \wedge c)$ ækvivalent med $(a \wedge b) \wedge c$, og vi skriver blot $a \wedge b \wedge c$. Vi lader $\neg$ binde stærkere end de andre Boolske operatorer, således at vi blot skriver $\neg a$ i stedet for $(\neg a)$.

Conjunctive Normal Form (CNF)

Et Boolsk udtryk er på **CNF form** hvis det er en konjunktion (ANDs) af disjunktioner (ORs) af literals (variable og negerede variable).

Eksempel:

$$(x_1 \vee \neg x_2 \vee x_4) \wedge (x_2 \vee x_3) \wedge (\neg x_1 \vee x_2 \vee \neg x_4 \vee \neg x_5) \wedge (\neg x_1 \vee x_3 \vee x_5)$$

Om notation: Bemærk, at $a \vee (b \vee c)$ er ækvivalent med $(a \vee b) \vee c$, dvs. har samme tabel. Parenteser mellem $\vee$ kan derfor udelades, og vi skriver blot $a \vee b \vee c$. Tilsvarende er $a \wedge (b \wedge c)$ ækvivalent med $(a \wedge b) \wedge c$, og vi skriver blot $a \wedge b \wedge c$. Vi lader $\neg$ binde stærkere end de andre Boolske operatorer, således at vi blot skriver $\neg a$ i stedet for $(\neg a)$.

En disjunktion af literals, f.eks. $(x_1 \vee \neg x_2 \vee x_4)$, kaldes en **clause**.

CNF som udtrykstræ

Eksempel (gentaget):

$$(x_1 \vee \neg x_2 \vee x_4) \wedge (x_2 \vee x_3) \wedge (\neg x_1 \vee x_2 \vee \neg x_4 \vee \neg x_5) \wedge (\neg x_1 \vee x_3 \vee x_5)$$

Set som udtrykstræ er et Boolsk udtryk i CNF, hvis det set fra oven består af: først et lag af $\wedge$-knuder, dernæst et lag af $\vee$-knuder, dernæst et lag (af max tykkelse én) af $\neg$-knuder, og dernæst et lag (tykkelse præcis én) af variabel-knuder (blade). Se næste side for illustration.

CNF som udtrykstræ

Eksempel (gentaget):

$$(x_1 \vee \neg x_2 \vee x_4) \wedge (x_2 \vee x_3) \wedge (\neg x_1 \vee x_2 \vee \neg x_4 \vee \neg x_5) \wedge (\neg x_1 \vee x_3 \vee x_5)$$

Set som udtrykstræ er et Boolsk udtryk i CNF, hvis det set fra oven består af: først et lag af $\wedge$-knuder, dernæst et lag af $\vee$-knuder, dernæst et lag (af max tykkelse én) af $\neg$-knuder, og dernæst et lag (tykkelse præcis én) af variabel-knuder (blade). Se næste side for illustration.

Sagt på en anden måde, enhver sti fra roden til et blad indeholder:

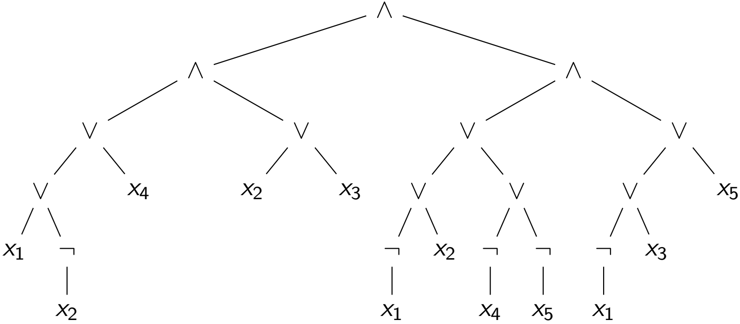
- Nul eller flere $\wedge$-knuder
- Nul eller flere $\vee$-knuder
- Nul eller én $\neg$-knude
- Én variabel-knude (blad)

Specielt er der ingen $\Rightarrow$-knuder i træet.

CNF som udtrykstræ, illustration

Eksempel (gentaget):

$$(x_1 \vee \neg x_2 \vee x_4) \wedge (x_2 \vee x_3) \wedge (\neg x_1 \vee x_2 \vee \neg x_4 \vee \neg x_5) \wedge (\neg x_1 \vee x_3 \vee x_5)$$



Konvertering til CNF

Man kan nemt checke, at i hver linje i følgende tabel er de to Boolske udtryk ækvivalente:

1)	$a \Rightarrow b$	$\neg a \vee b$
2)	$\neg(a \wedge b)$	$\neg a \vee \neg b$
3)	$\neg(a \vee b)$	$\neg a \wedge \neg b$
4)	$\neg(\neg a)$	a
5)	$a \vee (b \wedge c)$	$(a \vee b) \wedge (a \vee c)$

Dette giver en **algoritme til at omforme** et generelt Boolsk udtryk (med $\Rightarrow$, $\wedge$, $\vee$, og $\neg$-knuder) **til** et ækvivalent udtryk på **CNF**:

Fjern først alle $\Rightarrow$-knuder vha. 1). Flyt derefter alle $\neg$-knuder nedad mod bladene vha. 2), 3) og 4). Gentag: hvis der findes en $\vee$-knude med en $\wedge$-knude under sig, brug 5) på en sådan $\vee$-knude af størst afstand fra roden.

Eksempel på konvertering til CNF

Opgave: Konverter $(x_1 \vee \neg x_2) \Rightarrow (x_3 \Rightarrow x_4)$ til CNF.

Eksempel på konvertering til CNF

Opgave: Konverter $(x_1 \vee \neg x_2) \Rightarrow (x_3 \Rightarrow x_4)$ til CNF.

Løsning:

$$
\begin{array}{rlr}
 & & \textit{Regel} \\
 & (x_1 \vee \neg x_2) \Rightarrow (x_3 \Rightarrow x_4) & \\
 = & \neg(x_1 \vee \neg x_2) \vee (x_3 \Rightarrow x_4) & 1) \\
 = & \neg(x_1 \vee \neg x_2) \vee (\neg x_3 \vee x_4) & 1) \\
 = & (\neg x_1 \wedge \neg(\neg x_2)) \vee (\neg x_3 \vee x_4) & 3) \\
 = & (\neg x_1 \wedge x_2) \vee (\neg x_3 \vee x_4) & 4) \\
 = & (\neg x_1 \vee (\neg x_3 \vee x_4)) \wedge (x_2 \vee (\neg x_3 \vee x_4)) & 5) \\
 = & (\neg x_1 \vee \neg x_3 \vee x_4) \wedge (x_2 \vee \neg x_3 \vee x_4) &
\end{array}
$$

Et eksempel mere på konvertering til CNF

Opgave: Konverter $((x_1 \wedge \neg x_2) \vee (x_2 \vee \neg x_4)) \Rightarrow (x_1 \vee \neg x_3)$ til CNF.

Et eksempel mere på konvertering til CNF

Opgave: Konverter $((x_1 \wedge \neg x_2) \vee (x_2 \vee \neg x_4)) \Rightarrow (x_1 \vee \neg x_3)$ til CNF.

Løsning:

$$
\begin{aligned}
& ((x_1 \wedge \neg x_2) \vee (x_2 \vee \neg x_4)) \Rightarrow (x_1 \vee \neg x_3) && \textit{Regel} \\
&= \neg((x_1 \wedge \neg x_2) \vee (x_2 \vee \neg x_4)) \vee (x_1 \vee \neg x_3) && 1) \\
&= (\neg(x_1 \wedge \neg x_2) \wedge \neg(x_2 \vee \neg x_4)) \vee (x_1 \vee \neg x_3) && 3) \\
&= ((\neg x_1 \vee x_2) \wedge \neg(x_2 \vee \neg x_4)) \vee (x_1 \vee \neg x_3) && 2) + 4) \\
&= ((\neg x_1 \vee x_2) \wedge (\neg x_2 \wedge x_4)) \vee (x_1 \vee \neg x_3) && 3) + 4) \\
&= ((\neg x_1 \vee x_2) \vee (x_1 \vee \neg x_3)) \wedge ((\neg x_2 \wedge x_4) \vee (x_1 \vee \neg x_3)) && 5) \\
&= ((\neg x_1 \vee x_2) \vee (x_1 \vee \neg x_3)) \\
&\qquad \wedge ((\neg x_2 \vee (x_1 \vee \neg x_3)) \wedge (x_4 \vee (x_1 \vee \neg x_3))) && 5) \\
&= (\neg x_1 \vee x_2 \vee x_1 \vee \neg x_3) \wedge (\neg x_2 \vee x_1 \vee \neg x_3) \wedge (x_4 \vee x_1 \vee \neg x_3)
\end{aligned}
$$

[Første clause er altid sand, da enten x_1 eller $\neg x_1$ altid gælder, og kan derfor fjernes (det resulterende udtryk er ækvivalent).]

Uses of SAT modeling and solving

Probably unbeknownst to you, you are using products of SAT solvers for your daily life: CPUs are verified using SAT solver-based techniques, airplane software is formally verified using SAT solvers, FPGA and CPU layouts are optimized using them, and if you are lucky, your car's safety-critical systems are also verified using formal techniques, which basically means SAT solvers. Also train schedules and public transport schedules can be created using SAT solvers — many trains in Europe are scheduled using these techniques.

All these can be done using the very simple problem description, the CNF.

Mate Soos, maintainer of the SAT solver CryptoMiniSat.