Decision Procedures

An Algorithmic Point of View

Decision Procedures for Propositional Logic

D. Kroening O. Strichman

ETH/Technion

Version 1.0, 2007

Part I

Decision Procedures for Propositional Logic

Outline

SAT Example: Equivalence Checking if-then-else Chains

Optimization of if-then-else chains

original C code		**optimized C code**

`if(!a && !b) h();`
`else if(!a) g();`
`else f();`
		`if(a) f();`
		`else if(b) g();`
		`else h();`

$\Downarrow$		$\Uparrow$

`if(!a) {`
`  if(!b) h();`
`  else g();`
`} else f();`
	$\Rightarrow$	`if(a) f();`
		`else {`
		`  if(!b) h();`
		`  else g(); }`

SAT Example II

1. Represent procedures as *independent* Boolean variables

$$\begin{array}{ll} \textit{original} := & \textit{optimized} := \\ \quad \textbf{if } \neg a \wedge \neg b \textbf{ then } h & \quad \textbf{if } a \textbf{ then } f \\ \quad \textbf{else if } \neg a \textbf{ then } g & \quad \textbf{else if } b \textbf{ then } g \\ \quad \textbf{else } f & \quad \textbf{else } h \end{array}$$

2. Compile if-then-else chains into Boolean formulae

$$\text{compile}(\textbf{if } x \textbf{ then } y \textbf{ else } z) \quad \equiv \quad (x \wedge y) \vee (\neg x \wedge z)$$

3. Check equivalence of Boolean formulae

$$\boxed{\text{compile}(\textit{original}) \quad \Leftrightarrow \quad \text{compile}(\textit{optimized})}$$

"Compilation"

$$\begin{aligned} \textit{original} &\equiv \textbf{if } \neg a \wedge \neg b \textbf{ then } h \textbf{ else if } \neg a \textbf{ then } g \textbf{ else } h \\ &\equiv (\neg a \wedge \neg b) \wedge h \vee \neg(\neg a \wedge \neg b) \wedge \textbf{ if } \neg a \textbf{ then } g \textbf{ else } f \\ &\equiv (\neg a \wedge \neg b) \wedge h \vee \neg(\neg a \wedge \neg b) \wedge (\neg a \wedge g \vee a \wedge f) \end{aligned}$$

$$\begin{aligned} \textit{optimized} &\equiv \textbf{if } a \textbf{ then } f \textbf{ else if } b \textbf{ then } g \textbf{ else } h \\ &\equiv a \wedge f \vee \neg a \wedge \textbf{ if } b \textbf{ then } g \textbf{ else } h \\ &\equiv a \wedge f \vee \neg a \wedge (b \wedge g \vee \neg b \wedge h) \end{aligned}$$

$$(\neg a \wedge \neg b) \wedge h \vee \neg(\neg a \wedge \neg b) \wedge (\neg a \wedge g \vee a \wedge f) \quad \Leftrightarrow \quad a \wedge f \vee \neg a \wedge (b \wedge g \vee \neg b \wedge h)$$

How to Check (In)Equivalence?

Reformulate it as a satisfiability (SAT) problem:

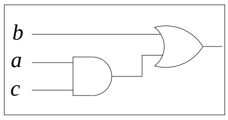
> Is there an assignment to a, b, f, g, h, which results in different evaluations of *original* and *optimized*?

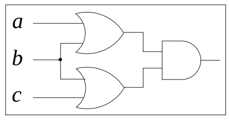
or equivalently:

> Is the boolean formula $\text{compile}(\mathit{original}) \not\leftrightarrow \text{compile}(\mathit{optimized})$ satisfiable?

Such an assignment provides an easy to understand counterexample

SAT Example: Circuit Equivalence Checking





$b \lor a \land c$ $\qquad$ $(a \lor b) \land (b \lor c)$

equivalent?

$$b \lor a \land c \quad \Leftrightarrow \quad (a \lor b) \land (b \lor c)$$

SAT

SAT (Satisfiability) the classical NP-complete problem:
Given a propositional formula f over n propositional variables $V = \{x, y, \ldots\}$.

> Is there are an assignment $\sigma : V \rightarrow \{0, 1\}$ with $\sigma(f) = 1$?

SAT

- **SAT belongs to NP**
  There is a *non-deterministic* Touring-machine deciding SAT in polynomial time:
  guess the assignment σ (linear in n), calculate $\sigma(f)$ (linear in $|f|$)
  Note: on a *real* (deterministic) computer this still requires 2^n time
- **SAT is complete for NP** (see complexity / theory class)

Implications for us: general SAT algorithms are probably exponential in time (unless NP = P)

Conjunctive Normal Form

Definition (Conjunctive Normal Form)

A formula in *Conjunctive Normal Form* (CNF) is a conjunction of clauses

$$C_1 \land C_2 \land \ldots \land C_n$$

each clause C is a disjunction of literals

$$C = L_1 \lor \ldots \lor L_m$$

and each literal is either a plain variable x or a negated variable $\overline{x}$.

Example $\quad (a \lor b \lor c) \land (\overline{a} \lor \overline{b}) \land (\overline{a} \lor \overline{c})$

CNF for Parity Function is Exponential

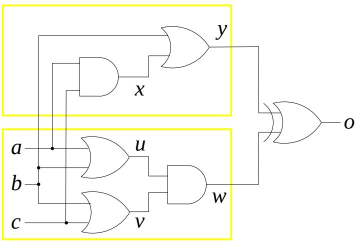
		b	b		
	0	1	0	1	
a	1	0	1	0	
a	0	1	0	1	c
	1	0	1	0	c
			d	d	

$a \oplus b \oplus c \oplus d$

- no merging in the Karnaugh map
- all clauses contain all variables
- CNF for parity with n variables has 2^{n-1} clauses

Better ideas?

Example of Tseitin Transformation: Circuit to CNF



$$
\begin{aligned}
& o \wedge \\
(x & \leftrightarrow a \wedge c) \wedge \\
(y & \leftrightarrow b \vee x) \wedge \\
(u & \leftrightarrow a \vee b) \wedge \\
(v & \leftrightarrow b \vee c) \wedge \\
(w & \leftrightarrow u \wedge v) \wedge \\
(o & \leftrightarrow y \oplus w)
\end{aligned}
$$

$$o \wedge (x \rightarrow a) \wedge (x \rightarrow c) \wedge (x \leftarrow a \wedge c) \wedge \ \ldots$$

$$o \wedge (\overline{x} \vee a) \wedge (\overline{x} \vee c) \wedge (x \vee \overline{a} \vee \overline{c}) \wedge \ \ldots$$

Algorithmic Description of Tseitin Transformation

Tseitin Transformation

1. For each non input circuit signal s generate a new variable x_s
2. For each gate produce complete input / output constraints as clauses
3. Collect all constraints in a big conjunction

- The transformation is satisfiability equivalent: the result is satisfiable iff and only the original formula is satisfiable
- Not equivalent in the classical sense to original formula: it has new variables
- You an get a satisfying assignment for original formula by projecting the satisfying assignment onto the original variables

Tseitin Transformation: Input / Output Constraints

$$
\begin{aligned}
\text{Negation:} \quad & x \leftrightarrow \overline{y} \Leftrightarrow (x \rightarrow \overline{y}) \wedge (\overline{y} \rightarrow x) \\
& \Leftrightarrow (\overline{x} \vee \overline{y}) \wedge (y \vee x) \\
\text{Disjunction:} \quad & x \leftrightarrow (y \vee z) \Leftrightarrow (y \rightarrow x) \wedge (z \rightarrow x) \wedge (x \rightarrow (y \vee z)) \\
& \Leftrightarrow (\overline{y} \vee x) \wedge (\overline{z} \vee x) \wedge (\overline{x} \vee y \vee z) \\
\text{Conjunction:} \quad & x \leftrightarrow (y \wedge z) \Leftrightarrow (x \rightarrow y) \wedge (x \rightarrow z) \wedge ((y \wedge z) \rightarrow x) \\
& \Leftrightarrow (\overline{x} \vee y) \wedge (\overline{x} \vee z) \wedge (\overline{(y \wedge z)} \vee x) \\
& \Leftrightarrow (\overline{x} \vee y) \wedge (\overline{x} \vee z) \wedge (\overline{y} \vee \overline{z} \vee x) \\
\text{Equivalence:} \quad & x \leftrightarrow (y \leftrightarrow z) \Leftrightarrow (x \rightarrow (y \leftrightarrow z)) \wedge ((y \leftrightarrow z) \rightarrow x) \\
& \Leftrightarrow (x \rightarrow ((y \rightarrow z) \wedge (z \rightarrow y)) \wedge ((y \leftrightarrow z) \rightarrow x) \\
& \Leftrightarrow (x \rightarrow (y \rightarrow z)) \wedge (x \rightarrow (z \rightarrow y)) \wedge ((y \leftrightarrow z) \rightarrow x) \\
& \Leftrightarrow (\overline{x} \vee \overline{y} \vee z) \wedge (\overline{x} \vee \overline{z} \vee y) \wedge ((y \leftrightarrow z) \rightarrow x) \\
& \Leftrightarrow (\overline{x} \vee \overline{y} \vee z) \wedge (\overline{x} \vee \overline{z} \vee y) \wedge (((y \wedge z) \vee (\overline{y} \wedge \overline{z})) \rightarrow x) \\
& \Leftrightarrow (\overline{x} \vee \overline{y} \vee z) \wedge (\overline{x} \vee \overline{z} \vee y) \wedge ((y \wedge z) \rightarrow x) \wedge ((\overline{y} \wedge \overline{z}) \rightarrow x) \\
& \Leftrightarrow (\overline{x} \vee \overline{y} \vee z) \wedge (\overline{x} \vee \overline{z} \vee y) \wedge (\overline{y} \vee \overline{z} \vee x) \wedge (y \vee z \vee x)
\end{aligned}
$$

Optimizations for the Tseitin Transformation

- Goal is smaller CNF (less variables, less clauses)
- Extract multi argument operands (removes variables for intermediate nodes)
- NNF: half of AND, OR node constraints may be removed due to monotonicity
- use *sharing*

DIMACS CNF

- DIMACS CNF format = standard format for CNF
- Used by most SAT solvers
- Plain text file with following structure:
  `p cnf` <# variables> <# clauses>
  <clause> 0
  <clause> 0
  ...
- One or more lines per clause

DIMACS CNF

- Every clause is a list of numbers, separated by spaces
- A clause ends with 0
- Every number $1, 2, \ldots$ corresponds to a variable

→ variable names (e.g., a, b, $\ldots$) have to be mapped to numbers

- A negative number corresponds to negation

→ Let a have number 5. Then $\overline{a}$ is -5.

DIMACS CNF: Example

$$(x_1 \vee x_2 \vee \overline{x_3}) \wedge (x_2 \vee \overline{x_1}) \wedge (x_4 \vee \overline{x_2} \vee \overline{x_1})$$

- 4 variables, 3 clauses
- CNF file:

```
p cnf 4 3
1 2 -3 0
2 -1 0
4 -2 -1 0
```


Example SAT: Circuit Equivalence

formula:

$$\begin{array}{l} o \wedge \\ (x \leftrightarrow a \wedge c) \wedge \\ (y \leftrightarrow b \vee x) \wedge \\ (u \leftrightarrow a \vee b) \wedge \\ (v \leftrightarrow b \vee c) \wedge \\ (w \leftrightarrow u \wedge v) \wedge \\ (o \leftrightarrow y \oplus w) \end{array}$$

number assignment:

variable	number
o	1
a	2
c	3
x	4
b	5
y	6
u	7
v	8
w	9

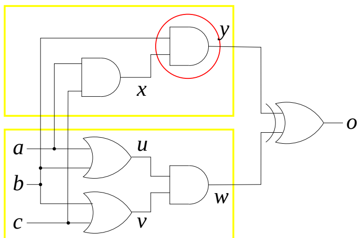
Simply in order of occurrence.

Example SAT: Circuit Equivalence

formula	clauses	DIMACS
o	o	1 0
$x \leftrightarrow a \wedge c$	$a \vee \overline{x}$	2 -4 0
	$c \vee \overline{x}$	3 -4 0
	$\overline{a} \vee \overline{c} \vee x$	-2 -3 4 0
$y \leftrightarrow b \vee x$	$\overline{x} \vee y$	-4 6 0
	$\overline{b} \vee y$	-5 6 0
	$x \vee b \vee \overline{y}$	4 5 -6 0
$u \leftrightarrow a \vee b$	$\overline{a} \vee u$	-2 7 0
	$\overline{b} \vee u$	-5 7 0
	$a \vee b \vee \overline{u}$	2 5 -7 0
$v \leftrightarrow b \vee c$	$\overline{b} \vee v$	-5 8 0
	$\overline{c} \vee v$	-3 8 0
	$b \vee c \vee \overline{v}$	5 3 -8 0
$w \leftrightarrow u \wedge v$	$u \vee \overline{w}$	7 -9 0
	$v \vee \overline{w}$	8 -9 0
	$\overline{u} \vee \overline{v} \vee w$	-7 -8 9 0
$o \leftrightarrow y \oplus w$	$\overline{y} \vee \overline{w} \vee \overline{o}$	-6 -9 -1 0
	$y \vee w \vee \overline{o}$	6 9 -1 0
	$\overline{y} \vee w \vee o$	-6 9 1 0

Example SAT: Circuit Equivalence

Let's change the circuit!



$$\begin{array}{l} o \wedge \\ (x \leftrightarrow a \wedge c) \wedge \\ (y \leftrightarrow b \wedge x) \wedge \\ (u \leftrightarrow a \vee b) \wedge \\ (v \leftrightarrow b \vee c) \wedge \\ (w \leftrightarrow u \wedge v) \wedge \\ (o \leftrightarrow y \oplus w) \end{array}$$

Is the CNF satisfiable?

Example SAT: Circuit Equivalence

- Output of the SAT solver:

```
SATISFIABLE
1 2 3 4 -5 -6 7 8 9
```

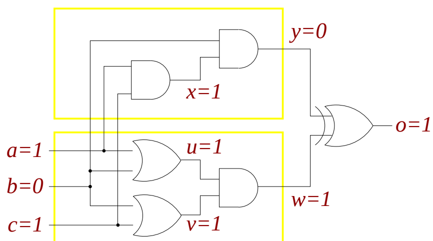
- Values of the variables:

variable	number	value
o	1	1
a	2	1
c	3	1
x	4	1
b	5	0
y	6	0
u	7	1
v	8	1
w	9	1

- Caveat: there is more than one solution

Example SAT: Circuit Equivalence

Satisfying assignment mapped to the circuit:



variable	value
o	1
a	1
c	1
x	1
b	0
y	0
u	1
v	1
w	1