# Boolean Functions

## Motivations

- Properties of Digital System ⇘ Boolean Expressions
- Can keep similar sizes

## Computer representations

- Circuits: smallest known representations
- Normal Forms CNF/BDD/…
- Lazy normalizations BED/SAT

## Exponential risk

- Cook's theorem: NP-complete
- Real world systems: polynomial normal form?

## Applications

- Circuit/System/Software Verification
- Circuit/Software Synthesis
- Non Boolean applications

| $b_3b_2b_1b_0$ | {i : 1=$b_i$} | b(z) | $\sum_{k<4} b_k 2^k$ | $\sum_{k<3} b_k 2^k - 8b_3$ | f(x,y) = $b_{x+2y}$ |
|---|---|---|---|---|---|
| 0000 | | 0 | 0 | 0 | 0 |
| 0001 | 0 | 1 | 1 | 1 | ¬x & ¬y |
| 0010 | 1 | z | 2 | 2 | x & ¬y |
| 0011 | 0,1 | 1+z | 3 | 3 | ¬y |
| 0100 | 2 | $z^2$ | 4 | 4 | ¬x & y |
| 0101 | 0,2 | $1+z^2$ | 5 | 5 | ¬x |
| 0110 | 1,2 | $z+z^2$ | 6 | 6 | x ^ y |
| 0111 | 0,1,2 | $1+z+z^2$ | 7 | 7 | ¬x \| ¬y |
| 1000 | 3 | $z^3$ | 8 | -8 | x & y |
| 1001 | 0,3 | $1+z^3$ | 9 | -7 | ¬x ^ y |
| 1010 | 1,3 | $z+z^3$ | 10 | -6 | x |
| 1011 | 0,1,3 | $1+z+z^3$ | 11 | -5 | x \| ¬y |
| 1100 | 2,3 | $z^2+z^3$ | 12 | -4 | y |
| 1101 | 0,2,3 | $1+z^2+z^3$ | 13 | -3 | ¬x \| y |
| 1110 | 1,2,3 | $z+z^2+z^3$ | 14 | -2 | x \| y |

# Net-list

## Expression

$$\mathcal{E}_i = 0 \mid 1 \mid x_1 \mid \quad \mid x_i \mid$$

$$? e \mid e ? \ e' \mid e ? \ e' \mid e ? \ e' \mid mux( e, e', e')$$

$$e, e', e'' ? \ \mathcal{E}_i$$

## Boolean function

$$e ? \ ^{i} \quad \mid \ ^{i} ? \quad \models 2^{2^i}$$

$$f ? \ ^{i} \quad ^{j} \quad \mid \ ^{i} ? \quad ^{j} \models 2^{j2^i}$$

## Circuit net-list

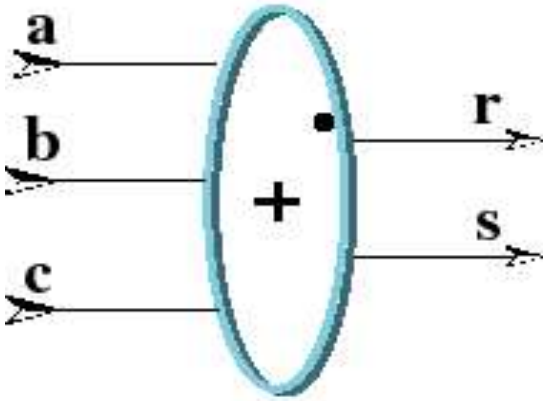
$$f(x_1 \quad x_i) = (x_{o1} \quad x_{oj})$$

$$[\, x_{i+1} = e_1 \quad x_{i+n} = e_n \,]$$

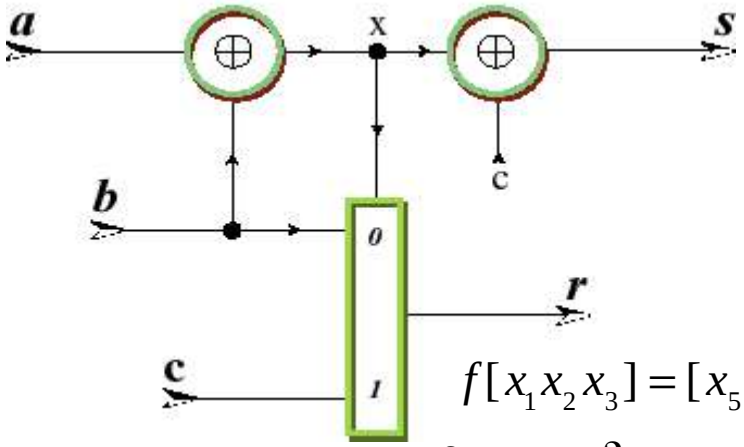
$$e_k \mid \mathcal{E}_{i+k} \text{ ok} \downarrow \{i \models 1 \quad i+n\}$$

# Full Adder

$$a_N + b_N + c_N = s_N + 2r_N$$

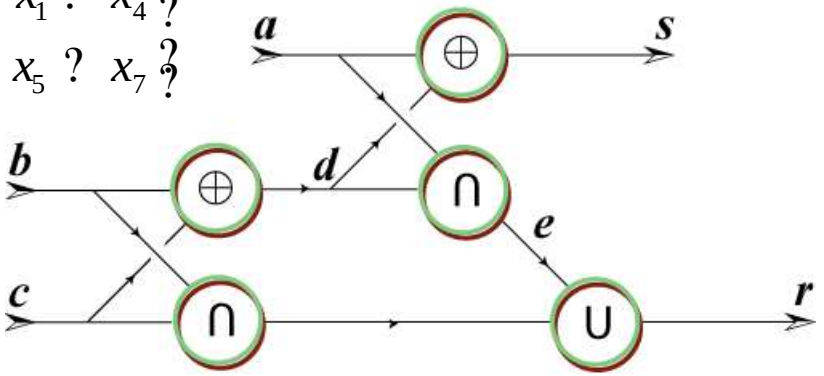



$$s_N = (a_N + b_N + c_N) \mid 2 = a_N \oplus b_N \oplus c_N$$
$$r_N = (a_N + b_N + c_N) \oplus 2 = a_N b_N \oplus b_N c_N \oplus c_N a_N$$




$$f[x_1 x_2 x_3] = [x_5 x_6]$$
$$x_4 = x_1 \oplus x_2$$
$$x_5 = x_3 \oplus x_4$$
$$x_6 = mux(x_4\, x_2\, x_3)$$

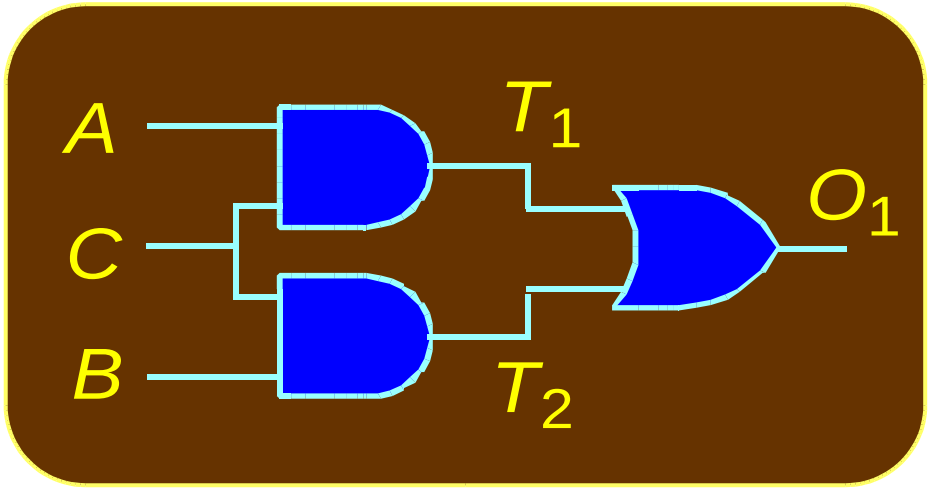
$$g[x_1 x_2 x_3] = [x_5 x_8]$$
$$x_4 = x_2 \oplus x_3$$
$$x_5 = x_2 \oplus x_3$$
$$x_6 = x_1 \oplus x_4$$
$$x_7 = x_1 \oplus x_4$$
$$x_8 = x_5 \oplus x_7$$

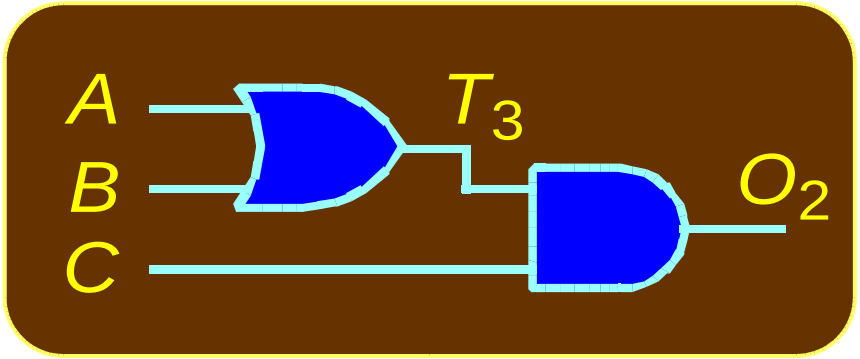


# Example Analysis Task

## Logic Circuit Comparison

- ***Do circuits compute identical function?***
  - Basic task of formal hardware verification
  - Compare new design to “known good” design



# Combinatorial Search

## Satisfiability Formulation

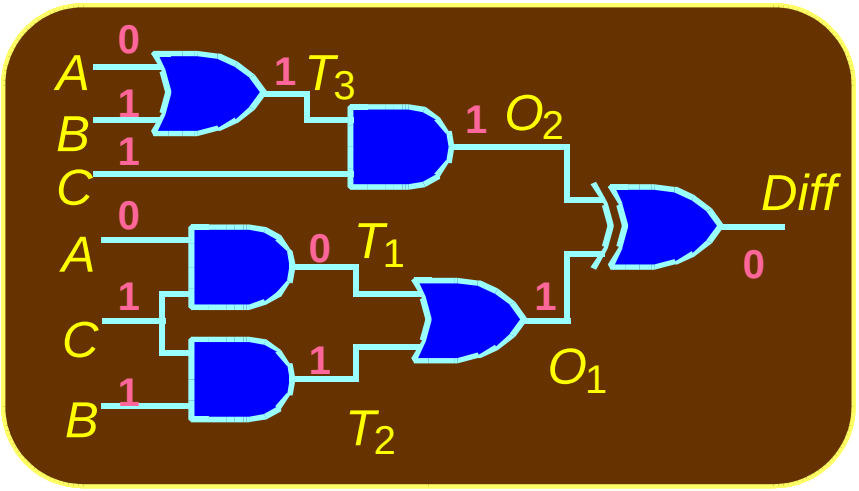
- Search for input assignment giving different outputs

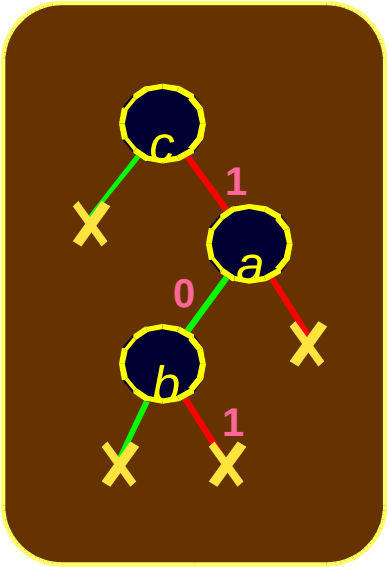
## Branch & Bound

- Assign input(s)
- Propagate forced values
- Backtrack when cannot succeed

## Challenge

- Must prove all assignments fail
  - Co-NP complete problem
- Typically explore significant fraction of inputs
- Exponential time complexity

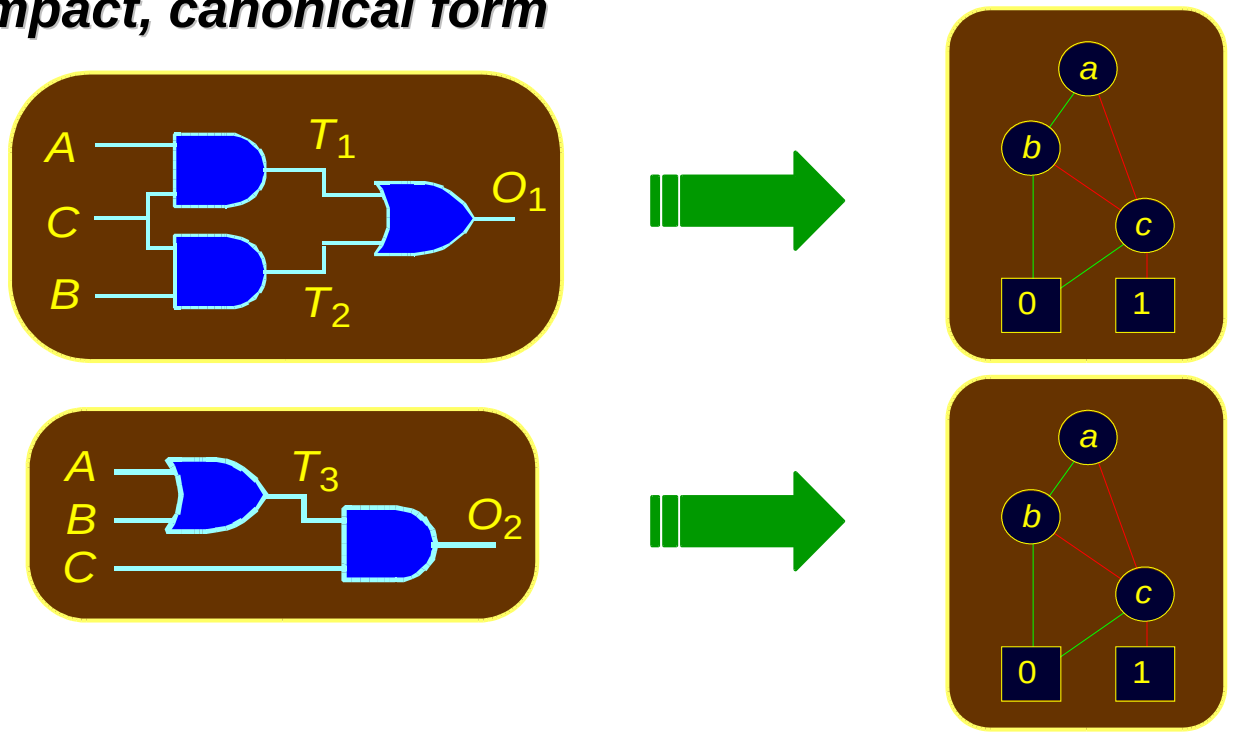


# Alternate Approach

## Generate Complete Representation of Circuit Function

- Compact, canonical form




- Functions equal if and only if representations identical
- Never enumerate explicit function values
- Exploit structure & regularity of circuit functions

# Truth Table Language

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| $x_1$ | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 |
| $x_2$ | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 |
| $x_3$ | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 |
| e | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 |

$$\text{truth } e = 2^3 + 2^5 + 2^7 = 168$$

$$\text{lang } e = \{011, 101, 111\} = \{3, 5, 7\}$$

$$\text{truth } f = \text{truth } g \;?\quad \text{lang } f = \text{lang } g \;?\quad f = g$$

$$\text{truth } f \;?\; [0, 2^{2^i} - 1] \qquad \text{truth } f = \left| \; f(b_0 \quad b_{i-1}) 2^n : n = \sum b_k 2^k \right.$$

$$\text{lang } f \;?\; 2^{\,i} \qquad \text{lang } f = \{w \;?\; B^i : f(w_1 \quad w_i) = 1\}$$

# Normal Forms

| $x_1$ | $x_2$ | $x_3$ | $f$ |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 0 | 0 | 1 | 0 |
| 0 | 1 | 0 | 0 |
| 0 | 1 | 1 | 1 |
| 1 | 0 | 0 | 0 |
| 1 | 0 | 1 | 1 |
| 1 | 1 | 0 | 0 |
| 1 | 1 | 1 | 1 |

## DNF (OR-AND)

$f = x_1'x_2x_3 + x_1x_2'x_3 + x_1x_2x_3$

$= x_1'x_2x_3 + x_1x_3$

## CNF (AND-OR)

$f = (x_1+x_2+x_3)(x_1+x_2+x_3')$

$(x_1+x_2'+x_3)(x_1'+x_2+x_3)(x_1'+x_2'+x_3)$

## ENF (XOR-AND)

$f = x_1x_3 + x_2x_3 + x_1x_2x_3$

# Cook's Theorem

$$\exists x_1 \quad x_i \quad s_k \qquad (i=1,\ldots,n;\ k=1,\ldots,m)$$

**SAT-CNF** $s_k = l_{k_1} \mid l_{k_2} \mid l_{k_3}$ **is NP-complete**

$l_{k_m} \mid \{0, x_k, \neg x_k\}$ **Satisfiability**

**SAT-DNF and TAUT-CNF in polynomial time**

$$\forall x_1 \quad x_i \quad p_k \qquad (i=1,\ldots,n;\ k=1,\ldots,m)$$

**TAUT-DNF** $p_k = l_{k_1} l_{k_2} l_{k_3}$ **is coNP-complete**

$l_{k_m} \mid \{1, x_k, \neg x_k\}$ **Tautology**

# Plan

- Binary Decision Diagrams BDD
- Integer Dichotomy ID
- Word Level Decision Diagrams *BMD
- Symbolic Diagrams TED