The Ordered Dimension of a Boolean Function

Jean Vuillemin
ENS, Paris

- Dimension $d=\mathcal{D}(f)$
- Bound $d \leq |DD(f)|$ on all known bit-level DDs
- Minimal multi-linear diagram $d = |MLD(f)|$
- Incremental operations on MLDs

Regular Language Dimension

- MDA: minimal deterministic automaton $s = |\mathrm{mda}(\mathrm{R})|$

$$\mathrm{mda}(\mathrm{R}) = \left\langle R, \cdot 0^{-}, \cdot 1^{-} \right\rangle \qquad \mathrm{mda}(\mathrm{R}) = R \cup \mathrm{mda}(\mathrm{R} \cdot 0^{-}) \cup \mathrm{mda}(\mathrm{R} \cdot 1^{-})$$

- Dimension: $d = \dim(\mathrm{R}) = \log_2 \left| \left\langle \mathrm{mda}(\mathrm{R}), \oplus \right\rangle \right|$ $\qquad d < s \leq 2^d$
- NXA: non-deterministic XOR automata
- MXA: minimal NXA w.r.t. integer word ordering

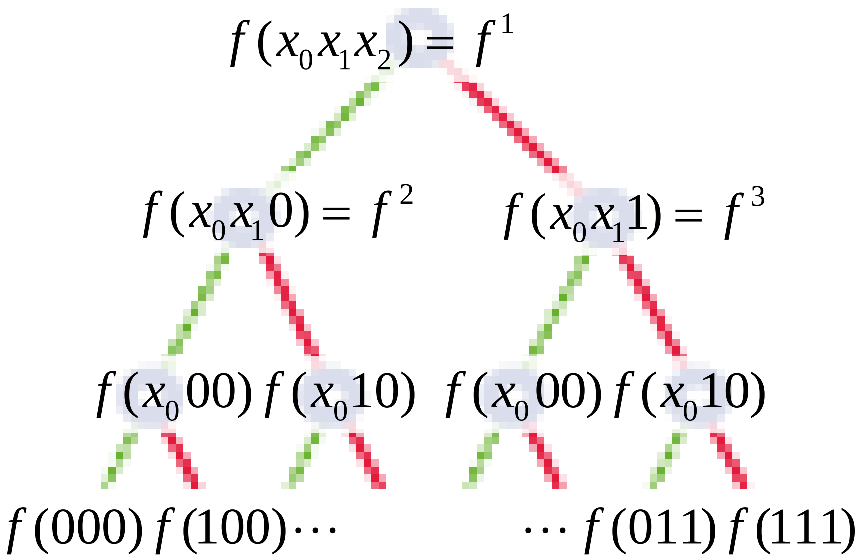
Theorem (Fliess 74)

- All NXA for *R* have size ≥*d*
- Reduced NXA of size *d* exist
- All reduced NXA are similar

Theorem (Ga.Vu. 09)

- Minimal NXA *d*=|*MXA(R)*|
- *(R=S)↔(MXA(R)=MXA(S))*
- Space n^2 + time n^3 minimization

Binary Decision Tree



$$f^1 = f \quad i = msi(f)$$

$$b \in \mathbb{B}: \quad f^{2n+b} = f^n[x_{i-|n|} = b]$$

$$f^n = x_{i-|n|}\, ?\, f^{2n+1} : f^{2n}$$

$$\mathrm{bdt}(\mathrm{f}) = \bigcup_{n>0} f^n$$

Example $m = x_2\, ?\, x_1 : x_0 \quad bdt(m) = \{0, 1, x_0, x_1, m\}$

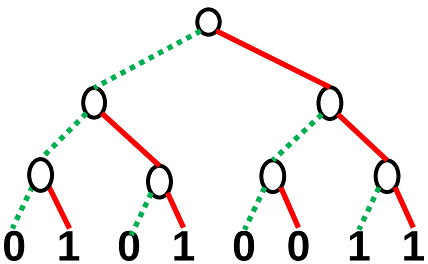
Definition $\mathfrak{D}(\mathrm{f}) = \log_2 |< \mathrm{bdt}(\mathrm{f}), \oplus >|$

$$\langle bdt(m), \oplus \rangle = \langle 1, x_0, x_1, m, \oplus \rangle \quad \mathfrak{D}(m) = 4$$

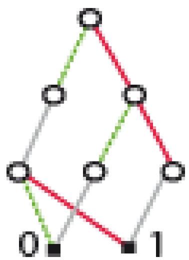
Reduced Ordered Decision Diagrams

Example: $m = \begin{array}{c} x_2 x_1 + x_2' x_0 \\ x_2 \,?\, x_1 : x_0 \\ x_0 \oplus x_0 x_2 \oplus x_1 x_2 \end{array}$

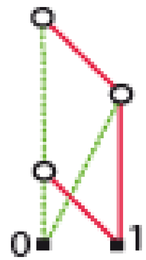
BDT



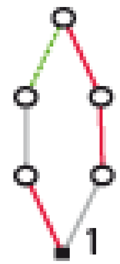
MDA



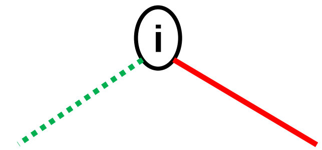
BDD



MXA



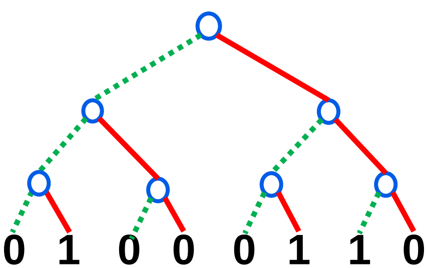
$$f = (1 - x_i) f^0 + x_i f^1$$



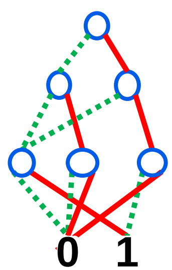
$$f^0 = f[x_i = 0] \quad f^1 = f[x_i = 1]$$

Shannon

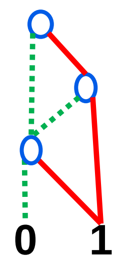
BMT



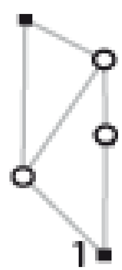
MMA



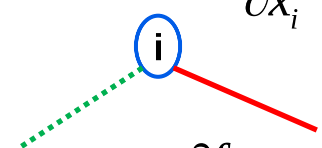
BMD



MLD



$$f = f^0 + x_i \frac{\partial f}{\partial x_i}$$



$$f^0 \qquad \frac{\partial f}{\partial x_i} = f^0 \oplus f^1$$

Reed-Muller

Invariant: $\langle \mathrm{bdt}(f), \oplus \rangle = \langle \mathrm{mda}(f), \oplus \rangle = \langle \mathrm{bdd}(f), \oplus \rangle = \langle \mathrm{mxa}(f), \oplus \rangle = \langle \mathrm{bmt}(f), \oplus \rangle = \langle \mathrm{mma}(f), \oplus \rangle = \langle \mathrm{bmd}(f), \oplus \rangle = \langle \mathrm{mld}(f), \oplus \rangle$ ☺

Examples

2^k ways mux	$mx(k) = x_a \quad a = \sum_{j<k} x_{j+2^k} 2^j$	$\text{msi} = k + 2^k - 1$
Hidden weight	$hw(k) = x_{w \dot{-} 1} \quad w = \sum_{j<k} x_j$	$\text{msi} = k$
Scalar XOR product	$spx(k) = \bigoplus_{i<k} x_i x_{2k-i-1}$	$\text{msi} = 2k - 1$
Scalar OR product	$spo(k) = \bigcup_{i<k} x_i x_{2k-i-1}$	$\text{msi} = 2k - 1$
Carry-free product	$cfp(k)(z) = \sum_{i<k} x_i z^i \times \sum_{i<k} x_{i+k} z^i \pmod 2$	$\text{msi} = 2k - 1$

f	mx	mx˜	hw	spx	Ő spx	cfp	spo
BDD	☺	☠	☠	☠	☺	☠	☠
BMD	☺	☺	☠	☺	☠	☠	☠
MLD	☺	☺	☺	☺	☺	☺	☠

Truth Tables for $f \in \mathbb{B}^* \to \mathbb{B}$

Exclusive Truth-Table

$$x = \mathrm{xtt}(f) = \sum_{k \in f} 2^k \quad = \sum_{k \in x} \prod_{j \in k} \mathrm{x}(j) \quad 2^k = 2^{\sum k_j 2^j} = \prod_{j \in k} \mathrm{x}(j)$$

$$f = \mathrm{xnf}(x) = \bigoplus_{k \in x} \mathrm{mon}(k) \quad = \bigoplus_{k \in x} \prod_{j \in k} \mathrm{x}_j \quad \mathrm{mon}(k) = \prod_{j \in k} x_j \quad \mathrm{xtt}(x_j) = x(j) = 2^{2^{2^j}}$$

Binary Moebius Transform

$$g(n) = \bigoplus_{n \subseteq d} f(d) \qquad BDT(g) = BMT(f)$$

$$g = \overset{oo}{\mathrm{O}} f \quad f = \overset{oo}{\mathrm{O}} g \qquad BDT(f) = BMT(g)$$

Disjunctive Truth-Table

$$d = \mathrm{dtt}(f) = \sum f(n) 2^n \qquad \mathrm{lip}(k) = \mathrm{mon}(k)\mathrm{neg}(k)$$

$$f = \mathrm{dnf}(d) = \sum_{k \in d} \mathrm{lip}(k) \qquad \mathrm{neg}(k) = \prod_{j \notin k} x_j' \qquad \mathrm{dtt}(x_i) = {}_2(0^{2^i} 1^{2^i}) = \frac{x(i+1) - x(i)}{1 - x(i+1)}$$

$$f = 0 \Leftrightarrow d = x = 0 \quad f = f' \Leftrightarrow d = d' \Leftrightarrow x = x'$$

$$x < x' \Leftrightarrow f < f'$$

$$1 \quad x_0 \quad x_0' \quad x_1 \quad x_1' \quad x_0 \oplus x_1 \quad x_0 \oplus x_1' \quad x_0 x_1 \quad \cdots$$

XNF $\quad x_0 \oplus x_0 x_2 \oplus x_1 x_2 \qquad x(0) + x(0)x(2) + x(1)x(2) = 98$

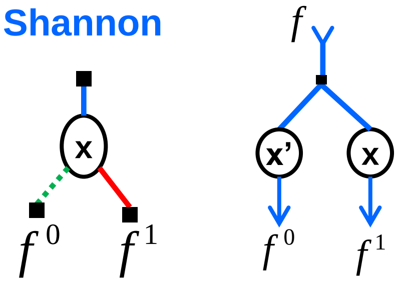
$$m = \begin{matrix} x_2 \,?\, x_1 : x_0 \\ x_2 x_1 + x_2' x_0 \end{matrix} \qquad \mathrm{xtt}(m) = {}_2 0100011 = 98$$

DNF $\quad x_0 x_1' x_2' + x_0 x_1 x_2' + x_0' x_1 x_2 + x_0 x_1 x_2 \qquad \mathrm{dtt}(m) = {}_2(01010011) = \dfrac{202}{1 - 2^8}$

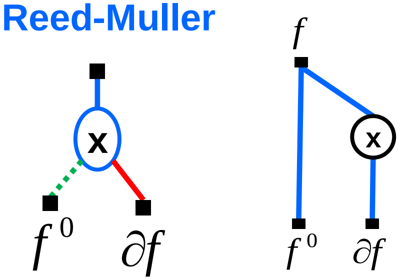
Multi-Linear Diagram

$$f = x' f^0 + x f^1 \qquad f = f^0 + x\partial f \qquad \partial f = f^0 \oplus f^1 \qquad f = f^1 + x'\partial f$$

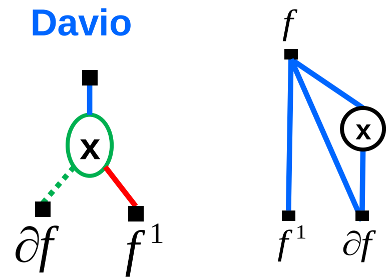
Shannon

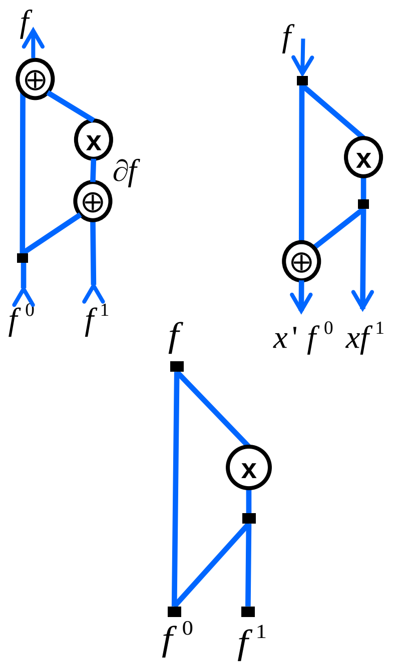


Reed-Muller



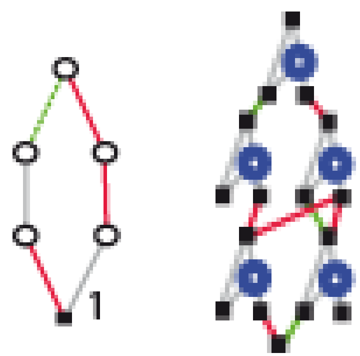
Davio



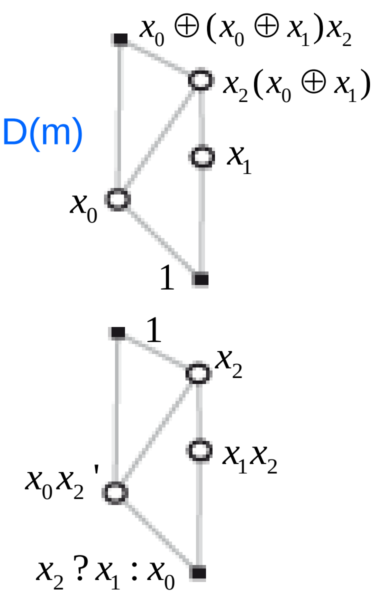


$$m = \begin{array}{c} x_2 x_1 + x_2' x_0 \\ x_2 \,?\, x_1 : x_0 \\ x_0 \oplus x_0 x_2 \oplus x_1 x_2 \end{array}$$

MXA(m)



MLD(m)



Dimension Properties

$\mathfrak{DD} = \{\text{BDD BMD FDD KDD HDD IDD} \cdots\}$ deterministic

$\cup\{\text{MXA } \oplus\text{BDD } \mathit{MLD} \cdots\}$ non-deterministic

Theorem Let $f \in B^i \to B$ have dimension $d=\mathcal{D}(f) \in N$

1. $\forall DD \in \mathcal{DD}$: $d \leq |DD(f)|$ linear decomposition
2. $d = \mathcal{D}(f^{\sim})$ mirror
3. $d=|MLD(f)|$ minimal base
4. $f=g \leftrightarrow MLD(f)=MLD(g)$ strong normal form
5. $d = \mathcal{D}(f') \leftrightarrow \delta f \neq 0$ not
6. $\mathcal{D}(f \oplus g) \leq \mathcal{D}(f,g) < \mathcal{D}(f) + \mathcal{D}(g)$ xor
7. $\mathcal{D}(f \cap g) < \mathcal{D}(f) \times \mathcal{D}(g)$ and
8. $\forall f$: $\mathcal{D}(f) < 2^{i/2+1}$ worst/average dim

   $\forall f$: $|\mathcal{BDD}(f)| < 2^{i+1}/i$ worst/average BDD

Minimal Base

$[b_1 \dots b_d]$ is a Reduced Basis for f if $d=\mathcal{D}(f)$ and bdt(f) $\subset \langle b_1 \dots b_d \oplus \rangle$.

All RB are linearly similar.

Theorem: Unique minimal basis B=base(f)=LC$[b_1 \dots b_d]$:
All RB $A=[a_1 \dots a_d]$ a.s.t. $\forall k$: $b_k \le a_k$ and $\exists k$: $b_k < a_k$ iff $B \ne A$.

Equally defined by:

- Xor Sorted $\forall i<j$: $b_i < b_j < b_i \oplus b_j$
- Reduced Echelon Form $\forall i \ne j$: $0 = b_i \cap 2^{l(b_j)}$

m

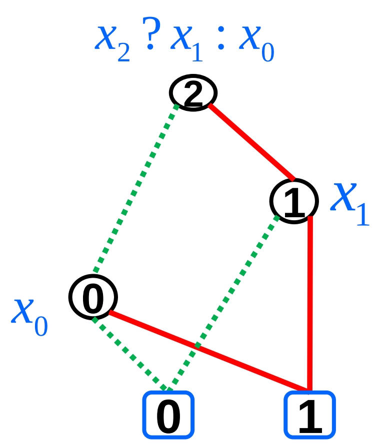
$$\text{xnf} = x_0 \oplus x_0 x_2 \oplus x_1 x_2$$

$$\text{xtt} = {}_2 0100011 = 98$$

$$\text{idd} = \{0100011, 01, 011, 0, 1\} = \{0, 1, 2, 6, 98\}$$

$$\text{base} = \{1, 01, 001, 0000011\} = \{1, 2, 8, 96\}$$

Minimal Multi-linear Diagram

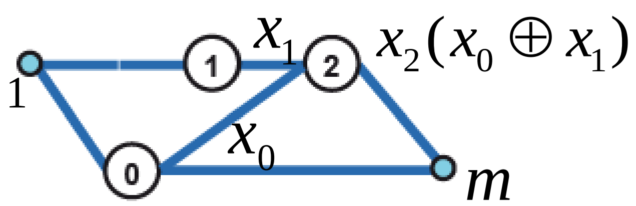


BDD

$$\mathfrak{D}(m = x_2 ? x_1 : x_0) = 4$$

$$\text{base}(m) = \langle 1 \quad x_0 \quad x_1 \quad x_2(x_0 + x_1) \rangle$$

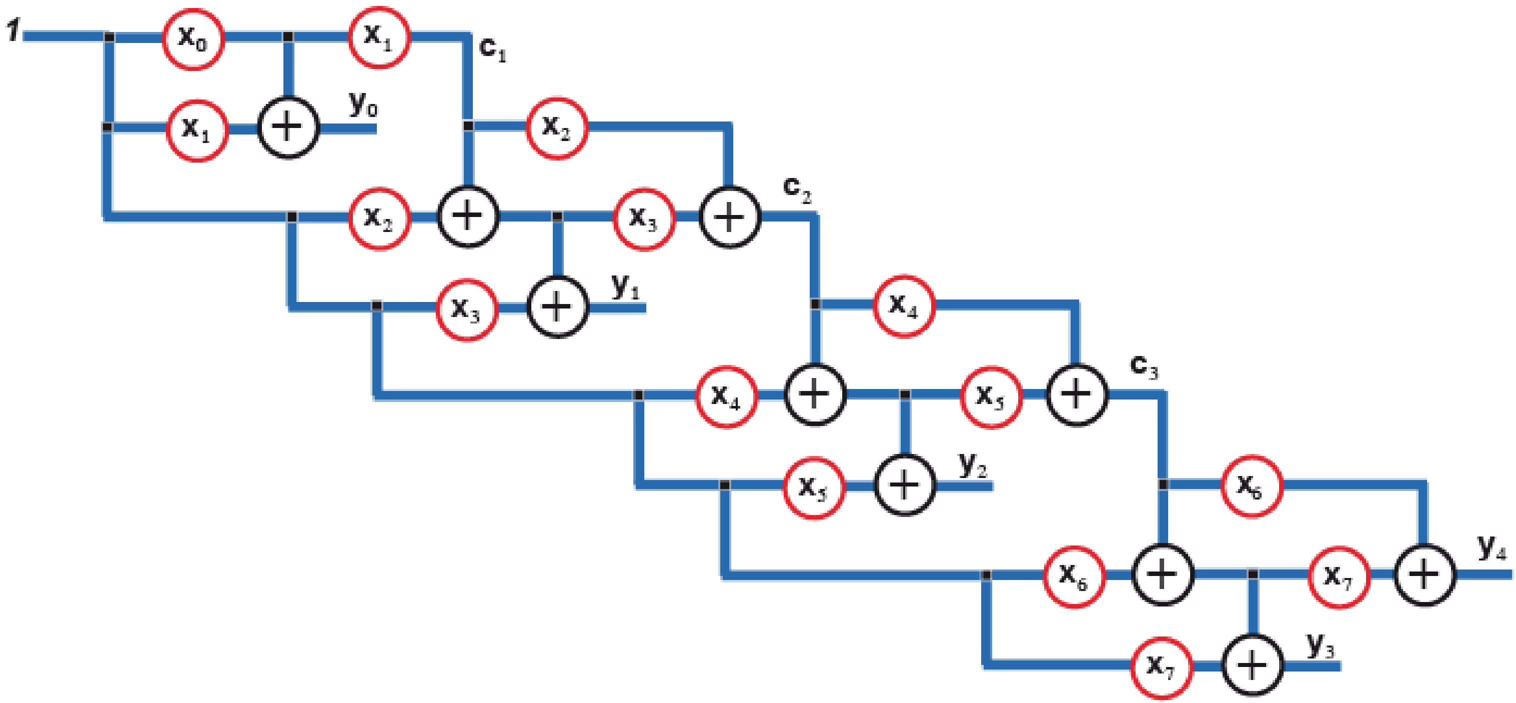
$$m = x_0 \oplus x_2(x_0 \oplus x_1)$$

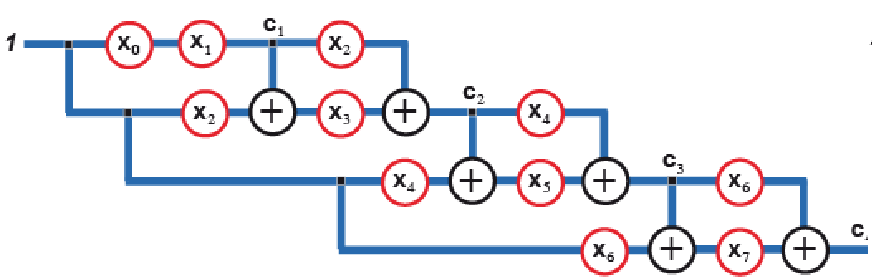


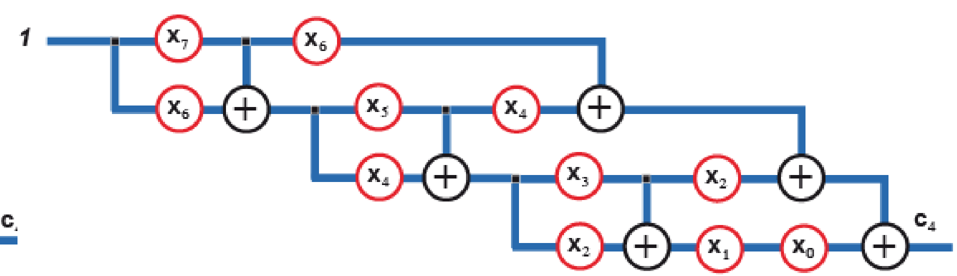
MLD

$b_1 = x_0$	$t_1 = x(0)$	2
$b_2 = x_1$	$t_2 = x(1)$	4
$b_3 = x_2(b_1 \oplus b_2)$	$t_3 = x(2)(t_1 + t_2)$	96
$m = b_1 \oplus b_3$	$x = t_1 + t_3$	98

MLD Adder


1
x_0 x_1 c_1
x_1 y_0 x_2
x_2 x_3 c_2
x_3 y_1 x_4
x_4 x_5 c_3
x_5 y_2 x_6
x_6 x_7 y_4
x_7 y_3


1
x_0 x_1 c_1 x_2
x_2 x_3 c_2 x_4
x_4 x_5 c_3 x_6
x_6 x_7


1
x_7 x_6
x_6 x_5 x_4
x_4 x_3 x_2
x_2 x_1 x_0 c_4

Incremental Operations on MLDs

Broad Word Computer 1 bwc= d bops

Minimize(f)	n^2	bwc	dn^2	bop
Mirror(f)	$l_2(d)$	bwc	$dl_2(d)$	bop
Xor(f,g)	1	bwc	d	bop
And(f,g)	d^2	bwc	d^3	bop