An algorithm for producing median formulas for Boolean functions

Reed-Muller Workshop 2011

Miguel Couceiro
Joint work with E. Lehtonen, J.-L. Marichal, T. Waldhauser

University of Luxembourg

May 2011

Preliminaries

A Boolean function is a map $f : \{0,1\}^n \to \{0,1\}$, for $n \geq 1$, called the arity of f.

Preliminaries

A Boolean function is a map $f : \{0,1\}^n \to \{0,1\}$, for $n \geq 1$, called the arity of f.

We use the notations $\Omega^{(n)} = \{0,1\}^{\{0,1\}^n}$ and $\Omega = \bigcup_{n \geq 1} \Omega^{(n)}$.

Preliminaries

A Boolean function is a map $f : \{0,1\}^n \to \{0,1\}$, for $n \geq 1$, called the arity of f.

We use the notations $\Omega^{(n)} = \{0,1\}^{\{0,1\}^n}$ and $\Omega = \bigcup_{n \geq 1} \Omega^{(n)}$.

For a fixed arity n, the n different projections (variables) $(a_1, \ldots, a_n) \mapsto a_i$ are denoted by $x_1, \ldots, x_n$.

For a fixed arity n, the n different negated projections are denoted by $\overline{x_1}, \ldots, \overline{x_n}$.

Preliminaries

A Boolean function is a map $f : \{0,1\}^n \to \{0,1\}$, for $n \geq 1$, called the arity of f.

We use the notations $\Omega^{(n)} = \{0,1\}^{\{0,1\}^n}$ and $\Omega = \bigcup_{n \geq 1} \Omega^{(n)}$.

For a fixed arity n, the n different projections (variables) $(a_1, \ldots, a_n) \mapsto a_i$ are denoted by $x_1, \ldots, x_n$.

For a fixed arity n, the n different negated projections are denoted by $\overline{x_1}, \ldots, \overline{x_n}$.

For each arity n, we denote by

- **0** the 0-constant functions.
- **1** the 1-constant functions.

The composition of an n-ary function f with m-ary functions $g_1, \ldots, g_n$ is the m-ary Boolean function $f(g_1, \ldots, g_n)$ given by

$$f(g_1, \ldots, g_n)(\mathbf{a}) = f(g_1(\mathbf{a}), \ldots, g_n(\mathbf{a})) \text{ for every } \mathbf{a} \in \{0, 1\}^m.$$

The composition of an n-ary function f with m-ary functions $g_1, \ldots, g_n$ is the m-ary Boolean function $f(g_1, \ldots, g_n)$ given by

$$f(g_1, \ldots, g_n)(\mathbf{a}) = f(g_1(\mathbf{a}), \ldots, g_n(\mathbf{a})) \text{ for every } \mathbf{a} \in \{0, 1\}^m.$$

For $K, J \subseteq \Omega$ the class composition of K with J, is defined by

$$K \circ J = \{f(g_1, \ldots, g_n) \colon \ f \ n\text{-ary in } K,\ g_1, \ldots, g_n \ m\text{-ary in } J\}.$$

The composition of an n-ary function f with m-ary functions $g_1, \ldots, g_n$ is the m-ary Boolean function $f(g_1, \ldots, g_n)$ given by

$$f(g_1, \ldots, g_n)(\mathbf{a}) = f(g_1(\mathbf{a}), \ldots, g_n(\mathbf{a})) \text{ for every } \mathbf{a} \in \{0, 1\}^m.$$

For $K, J \subseteq \Omega$ the class composition of K with J, is defined by

$$K \circ J = \{f(g_1, \ldots, g_n) \colon \ f \ n\text{-ary in } K,\ g_1, \ldots, g_n \ m\text{-ary in } J\}.$$

A (Boolean) clone is a class $C \subseteq \Omega$ containing all projections and satisfying $C \circ C = C$.

Known results about clones

- Clones constitute an algebraic lattice which was completely classified by Emil Post (1941).
- The class Ω of all Boolean functions is the largest clone.
- The class I_c of all projections is the smallest clone.

Known results about clones

- Clones constitute an algebraic lattice which was completely classified by Emil Post (1941).
- The class Ω of all Boolean functions is the largest clone.
- The class I_c of all projections is the smallest clone.
- Each clone C is finitely generated:

$$C = [K], \text{ for some finite } K \subseteq \Omega.$$

Known results about clones

- Clones constitute an algebraic lattice which was completely classified by Emil Post (1941).
- The class Ω of all Boolean functions is the largest clone.
- The class I_c of all projections is the smallest clone.
- Each clone C is finitely generated:

$$C = [K], \text{ for some finite } K \subseteq \Omega.$$

- Each clone C has a dual clone $C^d = \{f^d \colon f \in C\}$, where

$$f^d(x_1, \ldots, x_n) = \overline{f(\overline{x_1}, \ldots, \overline{x_n})}.$$

Examples: Essentially Unary Clones

- $I_c = [\,]$: Clone of projections.
- $I_0 = [\mathbf{0}]$: Clone of projections and 0-constant functions.
- $I_1 = [\mathbf{1}]$: Clone of projections and 1-constant functions.
- $I = [\mathbf{0}, \mathbf{1}]$: Clone of projections and constant functions.
- $I^* = [\,\overline{x}\,]$: Clone of projections and negated projections.
- $\Omega^{(1)} = [\mathbf{0}, \mathbf{1}, \overline{x}\,]$: Clone of essentially unary functions.

Examples: Minimal Clones

We say that C is a minimal clone if it covers I_c.

- $\Lambda = [\wedge]$: Clone of conjunctions.
- $V = [\vee]$: Clone of disjunctions.
- $L_c = [\oplus_3]$: Clone of constant-preserving linear functions, where $\oplus_3 = x_1 + x_2 + x_3$.
- $SM = [\text{median}]$: Clone of self-dual monotone functions:

$$f = f^d \quad \text{and} \quad f(\mathbf{a}) \leq f(\mathbf{b}) \quad \text{whenever} \quad \mathbf{a} \leq \mathbf{b}.$$

Known results about composition of clones

- The composition of clones is associative.
- The composition $C_1 \circ C_2$ of clones is not always a clone, e.g., $I^* \circ \Lambda$ is not a clone.
- The composition of clones was completely described by C., Foldes, Lehtonen (2006).
- Ω can be factorized into a composition of minimal clones.

Descending Irredundant Factorizations of Ω

- **D**: $\Omega = V \circ \Lambda \circ I^*$.
- **C**: $\Omega = \Lambda \circ V \circ I^*$.
- **P**: $\Omega = L_c \circ \Lambda \circ I$.
- **P**$^{\mathrm{d}}$: $\Omega = L_c \circ V \circ I$.
- **M**: $\Omega = SM \circ \Omega^{(1)}$.

Normal form systems

A normal form system (NFS) is a pair $(\{C_i\}_{1\leq i\leq k}, \{\gamma_j\}_{1\leq j\leq k-1})$ satisfying the following conditions:

- $\Omega = C_1 \circ \cdots \circ C_{k-1} \circ C_k$, where $C_k \subseteq \Omega^{(1)}$,
- C_i is generated by $\gamma_i \notin C_k$ for $1 \leq i \leq k-1$,
- $\gamma_i \neq \gamma_j$ for $i \neq j$.

Formulas

An *n-ary formula* of a NFS $(\{C_i\}_{1\leq i\leq k}, \{\gamma_j\}_{1\leq j\leq k-1})$ is a string over $\mathcal{C}_k^{(n)} \cup \{\gamma_j\}_{1\leq j\leq k-1}$ given by the recursion:

1. The elements of $\mathcal{C}_k^{(n)}$ are n-ary formulas.
2. If γ_i is m-ary and $a_1, \ldots, a_m$ are n-ary formulas without γ_j for $i > j$, then $\gamma_i a_1 \cdots a_m$ is an n-ary formula.

A *formula* of a NFS is an n-ary formula Φ for some n, and its *length* $|\Phi|$ is the number of symbols occurring in it.

Examples

Observe that...

Every n-ary formula represents an n-ary function, and every n-ary function is represented by an n-ary formula.

Formulas representing the negation $\overline{x}$:

$$\mathbf{M}, \mathbf{D}, \mathbf{C}: \ \overline{x},$$
$$\mathbf{P}, \mathbf{P}^{\mathrm{d}}: \ \oplus_3 \, x\mathbf{0}\mathbf{1}.$$

Complexity

Let A be a NFS and denote by F_A the set of formulas of A.

The A-complexity of f is defined by $C_A(f)$, as

$$C_A(f) := \min\{|\Phi| : \Phi \in F_A, \Phi \text{ represents } f\}.$$

A-complexities of the negation $\overline{x}$:

$$C_{\mathbf{M}}(\overline{x}) = C_{\mathbf{D}}(\overline{x}) = C_{\mathbf{C}}(\overline{x}) = 1,$$
$$C_{\mathbf{P}}(\overline{x}) = C_{\mathbf{P}^{\mathrm{d}}}(\overline{x}) = 4.$$

Representations and A-complexities of median

Formulas representing median:

$$
\begin{aligned}
\mathbf{M}&: \ \mathrm{median}\, x_1 x_2 x_3, \\
\mathbf{D}&: \ \vee\vee\wedge x_1 x_2 \wedge x_1 x_3 \wedge x_2 x_3, \\
\mathbf{C}&: \ \wedge\wedge\vee x_1 x_2 \vee x_1 x_3 \vee x_2 x_3, \\
\mathbf{P}&: \ \oplus_3 \wedge x_1 x_2 \wedge x_1 x_3 \wedge x_2 x_3, \\
\mathbf{P}^{\mathrm{d}}&: \ \oplus_3 \oplus_3 \vee x_1 x_2 \vee x_1 x_3 \vee x_2 x_3 \mathbf{0}\mathbf{1}.
\end{aligned}
$$

Representations and A-complexities of median

Formulas representing median:

$$\begin{aligned}
\mathbf{M}&:\ \mathrm{median} x_1 x_2 x_3,\\
\mathbf{D}&:\ \vee\vee\wedge x_1 x_2 \wedge x_1 x_3 \wedge x_2 x_3,\\
\mathbf{C}&:\ \wedge\wedge\vee x_1 x_2 \vee x_1 x_3 \vee x_2 x_3,\\
\mathbf{P}&:\ \oplus_3 \wedge x_1 x_2 \wedge x_1 x_3 \wedge x_2 x_3,\\
\mathbf{P}^{\mathrm{d}}&:\ \oplus_3 \oplus_3 \vee x_1 x_2 \vee x_1 x_3 \vee x_2 x_3 \mathbf{0}\mathbf{1}.
\end{aligned}$$

A-complexities of median:

$$C_{\mathbf{M}}(\mathrm{median}) = 4, \quad C_{\mathbf{D}}(\mathrm{median}) = C_{\mathbf{C}}(\mathrm{median}) = 11,$$
$$C_{\mathbf{P}}(\mathrm{median}) = 10, \quad C_{\mathbf{P}^{\mathrm{d}}}(\mathrm{median}) = 13.$$

Comparison of NFSs'

We say that A is polynomially as efficient as B, denoted $A \preceq B$, if there is a polynomial p with integer coefficients such that

$$C_A(f) \leq p(C_B(f)) \quad \text{for all } f \in \Omega.$$

Comparison of NFSs'

We say that A is polynomially as efficient as B, denoted $A \preceq B$, if there is a polynomial p with integer coefficients such that

$$C_A(f) \leq p(C_B(f)) \quad \text{for all } f \in \Omega.$$

Fact

The relation $\preceq$ is a quasi-order on any set of NFSs'.

Comparison of NFSs'

We say that A is polynomially as efficient as B, denoted $A \preceq B$, if there is a polynomial p with integer coefficients such that

$$C_A(f) \leq p(C_B(f)) \quad \text{for all } f \in \Omega.$$

Fact

The relation $\preceq$ is a quasi-order on any set of NFSs'.

If $A \npreceq B$ and $B \npreceq A$ holds, then A and B are incomparable.

If $A \preceq B$ but $B \npreceq A$, then A is polynomially more efficient than B.

Comparison of NFSs' (cont.)

Theorem (C., Foldes, Lehtonen)

1. **D**, **C**, **P**, and $\mathbf{P}^{\mathrm{d}}$ are incomparable.
2. **M** is polynomially more efficient than **D**, **C**, **P**, $\mathbf{P}^{\mathrm{d}}$.

Median representations of monotone Boolean functions

A function $f\colon \{0,1\}^n \to \{0,1\}$ is median decomposable if for every $i \in \{1,\ldots,n\}$,

$$f(\mathbf{x}) = \mathrm{median}(\, f(\mathbf{x}_i^0)\,,\, x_i\,,\, f(\mathbf{x}_i^1)\,),$$

where $\mathbf{x}_i^c = (x_1,\ldots,x_{i-1},c,x_{i+1},\ldots,x_n)$.

Theorem (Tohma, C., Marichal,...)

A Boolean function $f\colon \{0,1\}^n \to \{0,1\}$ is monotone iff f is median decomposable.

Algorithm MMNF – Median normal form for monotone Boolean functions

Require: a monotone Boolean function $f\colon \{0,1\}^n \to \{0,1\}$

Ensure: a median normal form representation of f

if $n \geq 2$ **then**
  $\alpha \leftarrow \mathrm{MMNF}(f(x_1, \ldots, x_{n-1}, 0))$
  $\beta \leftarrow \mathrm{MMNF}(f(x_1, \ldots, x_{n-1}, 1))$
  return $\operatorname{median} \alpha x_n \beta$
else if $f = \mathbf{0}$ **then**
  return 0
else if $f = \mathbf{1}$ **then**
  return 1
else
  return x_1
end if

Median representations of arbitrary Boolean functions

Given $f\colon \{0,1\}^n \to \{0,1\}$, define $g_f\colon \{0,1\}^{2n} \to \{0,1\}$ as: for all $\mathbf{b}, \mathbf{c} \in \{0,1\}^n$, let

$$g_f(\mathbf{bc}) := \begin{cases} 0 & \text{if } \mathrm{weight}(\mathbf{bc}) < n, \\ 1 & \text{if } \mathrm{weight}(\mathbf{bc}) > n, \\ f(\mathbf{b}) & \text{if } \mathbf{b} = \overline{\mathbf{c}}, \\ 0 & \text{otherwise.} \end{cases}$$

Median representations of arbitrary Boolean functions

Given $f\colon \{0,1\}^n \to \{0,1\}$, define $g_f\colon \{0,1\}^{2n} \to \{0,1\}$ as: for all $\mathbf{b}, \mathbf{c} \in \{0,1\}^n$, let

$$g_f(\mathbf{bc}) := \begin{cases} 0 & \text{if } \mathrm{weight}(\mathbf{bc}) < n, \\ 1 & \text{if } \mathrm{weight}(\mathbf{bc}) > n, \\ f(\mathbf{b}) & \text{if } \mathbf{b} = \overline{\mathbf{c}}, \\ 0 & \text{otherwise.} \end{cases}$$

Facts:

For any Boolean function $f\colon \{0,1\}^n \to \{0,1\}$,

1. g_f is monotone;
2. $f(x_1, \ldots, x_n) = g_f(x_1, \ldots, x_n, \overline{x_1}, \ldots, \overline{x_n})$.

Algorithm GenMNF – Median normal form for Boolean functions

Require: a Boolean function $f\colon \{0,1\}^n \to \{0,1\}$
Ensure: a median normal form representation of f

if f is monotone **then**
    return $\mathrm{MMNF}(f)$
else
    Construct g_f as shown.
    $w \leftarrow \mathrm{MMNF}(g_f)$
    for $i = 1$ to n **do**
        Replace each occurrence of x_{n+i} in w by $\overline{x_i}$.
    end for
    return w
end if

Thank you for your attention!