On the efficiency of normal form systems of Boolean functions

Horizons of Logic, Computation and Definability
Lauri Hella's 60th birthday

Miguel Couceiro

Joint work with S. Foldes, E. Lehtonen, P. Mercuriali, R. Péchoux, A. Saffidine

LORIA

Outline

Part I. Clone theory and Normal form systems

Part II. Complexity issues: Median normal forms

Preliminaries

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

Examples: For a fixed arity n,

- Projections: $(a_1, \ldots, a_n) \mapsto a_i$ denoted by $x_1, \ldots, x_n$.
- Negated projections: $\neg x_1, \ldots, \neg x_n$
- Constants: 0-constant and 1-constant functions denoted by $\mathbf{0}$ and $\mathbf{1}$, resp.

Notation: $\Omega^{(n)} = \{0,1\}^{\{0,1\}^n}$ and $\Omega = \bigcup_{n \geq 1} \Omega^{(n)}$.

Example: $\Omega^{(1)}$ contains the unary proj.s, negated proj.s and constants

Convention: $\Omega^{(1)}$ contains proj.s, negated proj.s and constants of **any arity**

Preliminaries

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

Examples: For a fixed arity n,

- Projections: $(a_1, \ldots, a_n) \mapsto a_i$ denoted by $x_1, \ldots, x_n$.
- Negated projections: $\neg x_1, \ldots, \neg x_n$
- Constants: 0-constant and 1-constant functions denoted by **0** and **1**, resp.

Notation: $\Omega^{(n)} = \{0,1\}^{\{0,1\}^n}$ and $\Omega = \bigcup_{n \geq 1} \Omega^{(n)}$.

Example: $\Omega^{(1)}$ contains the unary proj.s, negated proj.s and constants

Convention: $\Omega^{(1)}$ contains proj.s, negated proj.s and constants of **any arity**

Clones

The composition of an n-ary f with m-ary $g_1, \ldots, g_n$ is 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 clone is a class $C \subseteq \Omega$ that contains all projections and satisfies $C \circ C = C$.

Known results about (Boolean) clones:

- Clones constitute an algebraic lattice (E. Post, 1941).
- Ω is the largest clone **while** I_c of all projections is the smallest
- Each clone C is finitely generated: $C = [K]$, for some finite $K \subseteq \Omega$
- Each C has a dual $C^d = \{f^d \colon f \in C\}$,
  $f^d(x_1, \ldots, x_n) = \neg f(\neg x_1, \ldots, \neg x_n)$

Clones

The composition of an n-ary f with m-ary $g_1, \ldots, g_n$ is 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

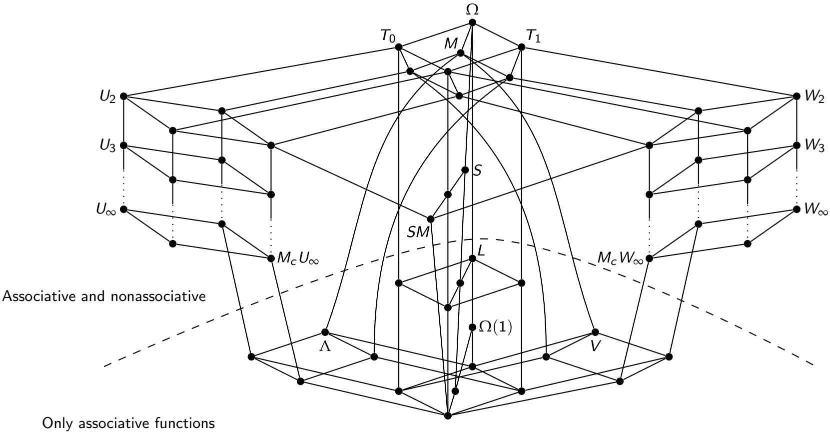
$$K \circ J = \{f(g_1, \ldots, g_n) \colon f \ n\text{-ary in } K,\ g_1, \ldots, g_n \ m\text{-ary in } J\}.$$

A clone is a class $C \subseteq \Omega$ that contains all projections and satisfies $C \circ C = C$.

Known results about (Boolean) clones:

- Clones constitute an algebraic lattice (E. Post, 1941).
- Ω is the largest clone **while** I_c of all projections is the smallest
- Each clone C is finitely generated: $C = [K]$, for some finite $K \subseteq \Omega$
- Each C has a dual $C^d = \{f^d \colon f \in C\}$,
  $f^d(x_1, \ldots, x_n) = \neg f(\neg x_1, \ldots, \neg x_n)$

Classification of clones: Post's lattice



Examples: essentially unary and minimal clones

Essentially unary clones: clones contained in $\Omega^{(1)}$

- $I_c = [\,]$, $I_0 = [\mathbf{0}]$, $I_1 = [\mathbf{1}]$ and $I = [\mathbf{0}, \mathbf{1}]$
- $I^* = [\,\neg x\,]$ **and** $\Omega^{(1)} = [\mathbf{0}, \mathbf{1}, \neg x\,]$

Minimal clones: clones that cover the clone I_c of projections

- $\Lambda_c = [\wedge]$ of conjunctions and $V_c = [\vee]$ of disjunctions
- $L_c = [\oplus_3]$ of constant-preserving linear functions
- $SM = [\mathrm{m}]$ of self-dual ($f = f^d$) monotone functions

Composition of clones and normal forms

Known results about composition of clones:

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

Descending Irredundant Factorizations of Ω:

- **D**: $\Omega = V_c \circ \Lambda_c \circ I^*$ and **C**: $\Omega = \Lambda_c \circ V_c \circ I^*$
- **P**: $\Omega = L_c \circ \Lambda_c \circ I$ and $\mathbf{P}^d$: $\Omega = L_c \circ V_c \circ I$
- **M**: $\Omega = SM \circ \Omega^{(1)}$

NB: Each corresponds to a **normal form system** (**NFS**), i.e., a set of terms $T(\alpha_1 \cdots \alpha_n)$ over the connectives $\alpha_1, \ldots, \alpha_n$ taken in this order.

Example: $\mathbf{D} = T(\vee \wedge \neg)$ and $\mathbf{C} = T(\wedge \vee \neg)$

Composition of clones and normal forms

Known results about composition of clones:

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

Descending Irredundant Factorizations of Ω:

- **D**: $\Omega = V_c \circ \Lambda_c \circ I^*$ and **C**: $\Omega = \Lambda_c \circ V_c \circ I^*$
- **P**: $\Omega = L_c \circ \Lambda_c \circ I$ and $\mathbf{P}^d$: $\Omega = L_c \circ V_c \circ I$
- **M**: $\Omega = SM \circ \Omega^{(1)}$

NB: Each corresponds to a **normal form system** (**NFS**), i.e., a set of terms $T(\alpha_1 \cdots \alpha_n)$ over the connectives $\alpha_1, \ldots, \alpha_n$ taken in this order.

Example: $\mathbf{D} = T(\vee \wedge \neg)$ and $\mathbf{C} = T(\wedge \vee \neg)$

Complexity

Let **A** be an **NFS** and $T_{\mathbf{A}}$ the set of *terms* of **A**. The **A**-complexity of f is

$$C_{\mathbf{A}}(f) := \min\{|t| : \ t \text{ represents } f \text{ and } t \in T_{\mathbf{A}}\}$$

NB: Members of $\Omega^{(1)}$ are not counted in $|t|$

Example: **A**-terms and **A**-complexities of $\mathrm{m} = \mathrm{median}$

$\mathbf{M}$: $t = \mathrm{m}(x_1, x_2, x_3)$ and $C_{\mathbf{M}}(\mathrm{m}) = 1$

$\mathbf{D}$: $t = (x_1 \wedge x_2) \vee (x_1 \wedge x_3) \vee (x_2 \wedge x_3)$ and $C_{\mathbf{D}}(\mathrm{m}) = 5$

$\mathbf{C}$: $t = (x_1 \vee x_2) \wedge (x_1 \vee x_3) \wedge (x_2 \vee x_3)$ and $C_{\mathbf{C}}(\mathrm{m}) = 5$

$\mathbf{P}$: $t = \oplus_3(x_1 \wedge x_2, x_1 \wedge x_3, x_2 \wedge x_3)$ and $C_{\mathbf{P}}(\mathrm{m}) = 4$

$\mathbf{P}^{\mathrm{d}}$: $t = \oplus_3(x_1 \vee x_2, x_1 \vee x_3, x_2 \vee x_3)$ and $C_{\mathbf{P}^{\mathrm{d}}}(\mathrm{m}) = 4$

Complexity

Let **A** be an **NFS** and $T_{\mathbf{A}}$ the set of *terms* of **A**. The **A**-complexity of f is

$$C_{\mathbf{A}}(f) := \min\{|t| : \ t \text{ represents } f \text{ and } t \in T_{\mathbf{A}}\}$$

NB: Members of $\Omega^{(1)}$ are not counted in $|t|$

Example: **A**-terms and **A**-complexities of $\mathrm{m} = \mathrm{median}$

M : $t = \mathrm{m}(x_1, x_2, x_3)$ and $C_{\mathbf{M}}(\mathrm{m}) = 1$

D : $t = (x_1 \wedge x_2) \vee (x_1 \wedge x_3) \vee (x_2 \wedge x_3)$ and $C_{\mathbf{D}}(\mathrm{m}) = 5$

C : $t = (x_1 \vee x_2) \wedge (x_1 \vee x_3) \wedge (x_2 \vee x_3)$ and $C_{\mathbf{C}}(\mathrm{m}) = 5$

P : $t = \oplus_3(x_1 \wedge x_2, x_1 \wedge x_3, x_2 \wedge x_3)$ and $C_{\mathbf{P}}(\mathrm{m}) = 4$

$\mathbf{P}^{\mathrm{d}}$: $t = \oplus_3(x_1 \vee x_2, x_1 \vee x_3, x_2 \vee x_3)$ and $C_{\mathbf{P}^{\mathrm{d}}}(\mathrm{m}) = 4$

Comparison of **NFS**'s

An **NFS A** is polynomially as efficient as **B**, denoted $\mathbf{A} \preceq \mathbf{B}$, if there is a polynomial p with integer coefficients such that

$$C_{\mathbf{A}}(f) \leq p(C_{\mathbf{B}}(f)) \quad \text{for all } f \in \Omega$$

NB: $\preceq$ is a *quasi-ordering* of **NFS**s'

If A $\not\preceq$ **B** and **B** $\not\preceq$ **A** holds, **then A** and **B** are incomparable

If A $\preceq$ **B** but **B** $\not\preceq$ **A**, **then A** is polynomially more efficient than **B**

If A $\preceq$ **B** and **B** $\preceq$ **A**, **then A** and **B** are equivalently efficient ($\mathbf{A} \sim \mathbf{B}$)

Comparison of **NFS**'s

An **NFS** **A** is polynomially as efficient as **B**, denoted $\mathbf{A} \preceq \mathbf{B}$, if there is a polynomial p with integer coefficients such that

$$C_{\mathbf{A}}(f) \leq p(C_{\mathbf{B}}(f)) \quad \text{for all } f \in \Omega$$

NB: $\preceq$ is a *quasi-ordering* of **NFS**s'

If $\mathbf{A} \not\preceq \mathbf{B}$ and $\mathbf{B} \not\preceq \mathbf{A}$ holds, **then** **A** and **B** are incomparable

If $\mathbf{A} \preceq \mathbf{B}$ but $\mathbf{B} \not\preceq \mathbf{A}$, **then** **A** is polynomially more efficient than **B**

If $\mathbf{A} \preceq \mathbf{B}$ and $\mathbf{B} \preceq \mathbf{A}$, **then** **A** and **B** are equivalently efficient ($\mathbf{A} \sim \mathbf{B}$)

Motivation

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**, $\mathbf{P}^{\mathrm{d}}$

Problem 1. Other **NFS**'s? **E.g.:** based on other connectives (generators)

Problem 2. Classification of **NFS**'s in terms of efficiency

Problem 3. Does the choice of generators within **NFS**s impact efficiency?
E.g.: m_3 vs m_5?

Problem 4. How to obtain optimal (minimal) representations in efficient **NFS**?
E.g.: optimal median normal forms?

Motivation

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**, $\mathbf{P}^{\mathrm{d}}$

Problem 1. Other **NFS**'s? **E.g.:** based on other connectives (generators)

Problem 2. Classification of **NFS**'s in terms of efficiency

Problem 3. Does the choice of generators within **NFS**s impact efficiency?
E.g.: m_3 vs m_5?

Problem 4. How to obtain optimal (minimal) representations in efficient **NFS**?
E.g.: optimal median normal forms?

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**, $\mathbf{P}^{\mathrm{d}}$

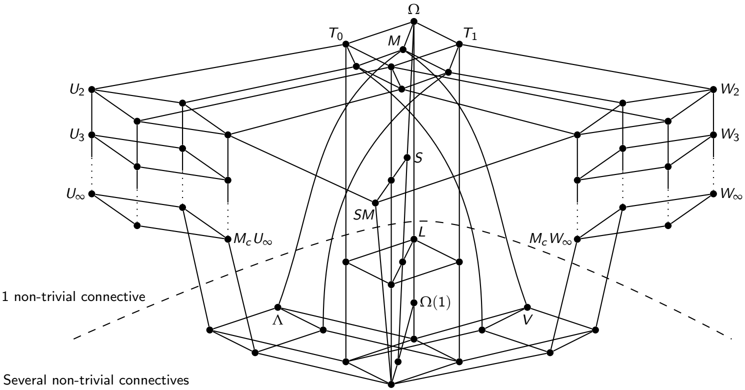
Problem 1. Other **NFS**'s? **E.g.:** based on other connectives (generators)

Problem 2. Classification of **NFS**'s in terms of efficiency

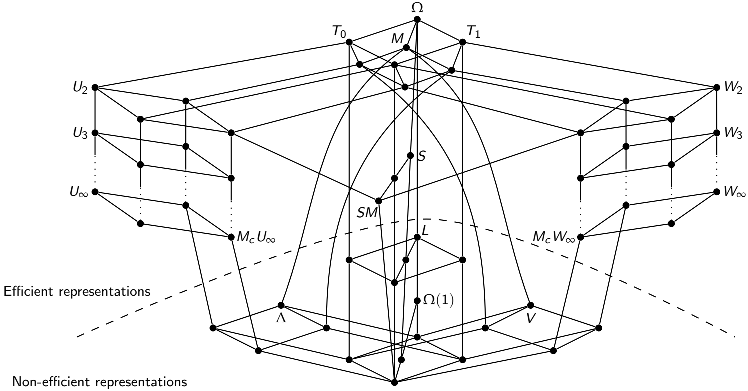
Problem 3. Does the choice of generators within **NFS**s impact efficiency?
E.g.: m_3 vs m_5?

Problem 4. How to obtain optimal (minimal) representations in efficient **NFS**?
E.g.: optimal median normal forms?

Single vs several connectives



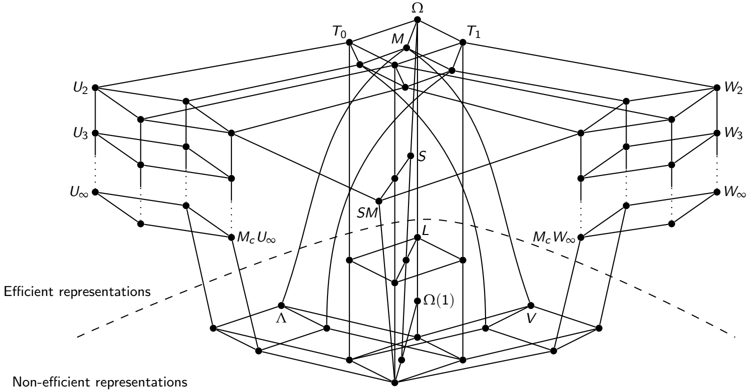
Locating efficient **NFS**s...



Result: NFS based on a single nontrivial connective are more efficient

Examples: NFS based on $\Omega = [x \uparrow y]$ and $M_c U_\infty = [x \wedge (y \vee z)]$

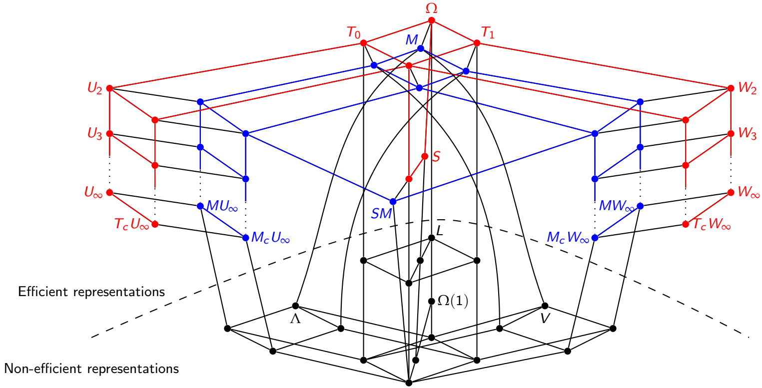
Locating efficient **NFS**s...



Result: NFS based on a single nontrivial connective are more efficient

Examples: NFS based on $\Omega = [x \uparrow y]$ and $M_c U_\infty = [x \wedge (y \vee z)]$

Towards a finer classification of **NFS**s



Result I: Black $\prec$ **Blue** $\preceq$ **Red**

Result II: Efficient monotone **NFS**s are all equivalent to **M**

Result III: The choice of monotone connectives does not impact efficiency

Main tools: **NFS** reductions

Consider **NFSs** $\mathbf{A} = T(\alpha\neg)$ (or $T(\alpha)$) and $\mathbf{B} = T(\beta\neg)$ (or $T(\beta)$). We say that

- $\mathbf{A}$ is linear reducible to $\mathbf{B}$, denoted $\mathbf{A} \sqsupseteq \mathbf{B}$, if:
  $\exists t \in T(\beta)$ **s.t.** $\alpha(x_1, \ldots, x_{\mathrm{ar}(\alpha)}) \equiv t$ **and** $\forall j \in \{1, \ldots, \mathrm{ar}(\alpha)\}$, $|t|_{x_j} = 1$
- $\mathbf{A}$ is universally reducible to $\mathbf{B}$, denoted $\mathbf{A} \sqsupseteq_\forall \mathbf{B}$, if:
  $\forall j \in \{1, \ldots, \mathrm{ar}(\alpha)\}, \exists t_j \in T(\beta)$ **s.t.** $\alpha(x_1, \ldots, x_{\mathrm{ar}(\alpha)}) \equiv t_j$ **and** $|t_j|_{x_j} = 1$;
- $\mathbf{A}$ is existentially reducible to $\mathbf{B}$, denoted $\mathbf{A} \sqsupseteq_\exists \mathbf{B}$, if:
  $\exists t \in T(\beta)$ **s.t.** $\alpha(x_1, \ldots, x_{\mathrm{ar}(\alpha)}) \equiv t$ **and** $\exists j \in \{1, \ldots, \mathrm{ar}(\alpha)\}$, $|t|_{x_j} = 1$.

Result I: $\sqsupseteq \subset \sqsupseteq_\forall \subset \sqsupseteq_\exists$. **Moreover** $\sqsupseteq \subset \sqsupseteq_\forall \subseteq \succeq$

Result II: Suppose $\mathbf{A} = T(\alpha\neg) \sqsupseteq_\exists \mathbf{B}$. If $[\alpha]$ is symmetric, then $\mathbf{A} \succeq \mathbf{B}$.

Main tools: **NFS** reductions

Consider **NFSs** $\mathbf{A} = T(\alpha\neg)$ (or $T(\alpha)$) and $\mathbf{B} = T(\beta\neg)$ (or $T(\beta)$). We say that

- $\mathbf{A}$ is linear reducible to $\mathbf{B}$, denoted $\mathbf{A} \sqsupseteq \mathbf{B}$, if:
  $\exists t \in T(\beta)$ **s.t.** $\alpha(x_1, \ldots, x_{\mathrm{ar}(\alpha)}) \equiv t$ **and** $\forall j \in \{1, \ldots, \mathrm{ar}(\alpha)\}$, $|t|_{x_j} = 1$
- $\mathbf{A}$ is universally reducible to $\mathbf{B}$, denoted $\mathbf{A} \sqsupseteq_\forall \mathbf{B}$, if:
  $\forall j \in \{1, \ldots, \mathrm{ar}(\alpha)\}, \exists t_j \in T(\beta)$ **s.t.** $\alpha(x_1, \ldots, x_{\mathrm{ar}(\alpha)}) \equiv t_j$ **and** $|t_j|_{x_j} = 1$;
- $\mathbf{A}$ is existentially reducible to $\mathbf{B}$, denoted $\mathbf{A} \sqsupseteq_\exists \mathbf{B}$, if:
  $\exists t \in T(\beta)$ **s.t.** $\alpha(x_1, \ldots, x_{\mathrm{ar}(\alpha)}) \equiv t$ **and** $\exists j \in \{1, \ldots, \mathrm{ar}(\alpha)\}$, $|t|_{x_j} = 1$.

Result I: $\sqsupseteq \subset \sqsupseteq_\forall \subset \sqsupseteq_\exists$. **Moreover** $\sqsupseteq \subset \sqsupseteq_\forall \subseteq \succeq$

Result II: Suppose $\mathbf{A} = T(\alpha\neg) \sqsupseteq_\exists \mathbf{B}$. If $[\alpha]$ is symmetric, then $\mathbf{A} \succeq \mathbf{B}$.

Examples I

Recall: If $\mathbf{A} = T(\alpha\neg) \sqsupseteq_{\exists} \mathbf{B}$ and $[\alpha]$ is symmetric, then $\mathbf{A} \succeq \mathbf{B}$.

Let $\mathbf{U} = T(u\neg)$ be the **NFS** based on the generator $u = x \wedge (y \vee z)$ of $M_c U_\infty$

NB: $u(x,y,z) \equiv \mathrm{m}(\mathrm{m}(x,1,y),0,z)$ and $\mathrm{m}(x,y,z) \equiv u(u(x,0,y),u(x,y,z),1)$

Hence: $\mathbf{U} \sqsupseteq \mathbf{M}$ and $\mathbf{M} \sqsupseteq_{\exists} \mathbf{U}$ (with m sym.) and thus $\mathbf{M} \sim \mathbf{U}$

Let $\mathbf{S} = T(x \uparrow y)$ be the **NFS** based on the *Sheffer function* $x \uparrow y = \neg(x \wedge y)$

NB: $x \uparrow y \equiv \mathrm{m}(\neg x, 1, \neg y)$ and $\mathrm{m}(x,y,z) \equiv (y \uparrow z) \uparrow (x \uparrow ((y \uparrow 1) \uparrow (z \uparrow 1)))$

Hence: $\mathbf{S} \sqsupseteq \mathbf{M}$ and $\mathbf{M} \sqsupseteq_{\exists} \mathbf{S}$ (with m sym.) and thus $\mathbf{M} \sim \mathbf{S}$

Examples I

Recall: If $\mathbf{A} = T(\alpha\neg) \sqsupseteq_{\exists} \mathbf{B}$ and $[\alpha]$ is symmetric, then $\mathbf{A} \succeq \mathbf{B}$.

Let $\mathbf{U} = T(u\neg)$ be the **NFS** based on the generator $u = x \wedge (y \vee z)$ of $M_c U_\infty$

NB: $u(x, y, z) \equiv \mathrm{m}(\mathrm{m}(x, 1, y), 0, z)$ and $\mathrm{m}(x, y, z) \equiv u(u(x, 0, y), u(x, y, z), 1)$

Hence: $\mathbf{U} \sqsupseteq \mathbf{M}$ and $\mathbf{M} \sqsupseteq_{\exists} \mathbf{U}$ (with m sym.) and thus $\mathbf{M} \sim \mathbf{U}$

Let $\mathbf{S} = T(x \uparrow y)$ be the **NFS** based on the *Sheffer function* $x \uparrow y = \neg(x \wedge y)$

NB: $x \uparrow y \equiv \mathrm{m}(\neg x, 1, \neg y)$ and $\mathrm{m}(x, y, z) \equiv (y \uparrow z) \uparrow (x \uparrow ((y \uparrow 1) \uparrow (z \uparrow 1)))$

Hence: $\mathbf{S} \sqsupseteq \mathbf{M}$ and $\mathbf{M} \sqsupseteq_{\exists} \mathbf{S}$ (with m sym.) and thus $\mathbf{M} \sim \mathbf{S}$

Example II

Median decomposition scheme (MD): $f : \{0,1\}^n \to \{0,1\}$ is monotone **iff**

$$(*) \quad f(\mathbf{x}) = \mathrm{m}(\, f(\mathbf{x}_i^0)\,,\, x_i\,,\, f(\mathbf{x}_i^1)\,), \quad \text{for every } i \in \{1, \ldots, n\}$$

Result: If $\mathbf{A} = T(\alpha\neg)$ with α monotone, **then** $\mathbf{A} \succeq \mathbf{M}$. In fact, $\mathbf{M} \sim \mathbf{A}$

Example: Let $\mathbf{M}_{2n+1} = T(\mathrm{m}_{2n+1}\neg)$, $n \geq 1$. **Then** $\mathbf{M}_{2n+1} \sim \mathbf{M}$.

Indeed: $\mathrm{m}(x, y, z) = \mathrm{m}_{2n+1}(x, y^n, z^n)$

Example II

Median decomposition scheme (MD): $f : \{0,1\}^n \to \{0,1\}$ is monotone **iff**

$$(*) \quad f(\mathbf{x}) = \mathrm{m}(\, f(\mathbf{x}_i^0)\,,\, x_i\,,\, f(\mathbf{x}_i^1)\,), \quad \text{for every } i \in \{1,\ldots,n\}$$

Result: If $\mathbf{A} = T(\alpha\neg)$ with α monotone, **then** $\mathbf{A} \succeq \mathbf{M}$. In fact, $\mathbf{M} \sim \mathbf{A}$

Example: Let $\mathbf{M}_{2n+1} = T(\mathrm{m}_{2n+1}\neg)$, $n \geq 1$. **Then** $\mathbf{M}_{2n+1} \sim \mathbf{M}$.

Indeed: $\mathrm{m}(x,y,z) = \mathrm{m}_{2n+1}(x, y^n, z^n)$

Example II

Median decomposition scheme (MD): $f : \{0,1\}^n \to \{0,1\}$ is monotone **iff**

$$(*) \quad f(\mathbf{x}) = \mathrm{m}(\, f(\mathbf{x}_i^0)\,,\, x_i\,,\, f(\mathbf{x}_i^1)\,), \quad \text{for every } i \in \{1, \ldots, n\}$$

Result: If $\mathbf{A} = T(\alpha\neg)$ with α monotone, **then** $\mathbf{A} \succeq \mathbf{M}$. In fact, $\mathbf{M} \sim \mathbf{A}$

Example: Let $\mathbf{M}_{2n+1} = T(\mathrm{m}_{2n+1}\,\neg)$, $n \geq 1$. **Then** $\mathbf{M}_{2n+1} \sim \mathbf{M}$.

Indeed: $\mathrm{m}(x, y, z) = \mathrm{m}_{2n+1}(x, y^n, z^n)$

Part II. Complexity issues: Median normal forms

Median **NFS**

How to obtain median representations?

Naive approach: Based on median decomposition scheme

$$(*) \quad f(\mathbf{x}) = \mathrm{m}(\, f(\mathbf{x}_i^0)\,,\, x_i\,,\, f(\mathbf{x}_i^1)\,), \quad \text{for every } i \in \{1, \ldots, n\}$$

NB: In the case of monotone functions...

Problem 1: The expressions thus obtained are not be optimal!

Example: m_5 would need 1+2+4+8+16= 31 ms but 4 suffice:

$$\mathrm{m}_5 \equiv \mathrm{m}(x_1, \mathrm{m}(x_2, x_3, x_4), \mathrm{m}(x_2, x_5, \mathrm{m}(x_3, x_4, x_5)))$$

Problem 2: There are equivalent median terms with = "size" but $\neq$ depth

Depth of t, denoted $d(t)$, is defined recursively by

- if $t = x$ or c, then $d(t) = 0$
- if $t = \mathrm{m}(t_1, t_2, t_3)$, then $d(t) = d(t_1) + d(t_2) + d(t_3) + 1$

Median NFS

How to obtain median representations?

Naive approach: Based on median decomposition scheme

$$(*) \quad f(\mathbf{x}) = \mathrm{m}(\, f(\mathbf{x}_i^0)\,,\, x_i\,,\, f(\mathbf{x}_i^1)\,), \quad \text{for every } i \in \{1, \ldots, n\}$$

NB: In the case of monotone functions...

Problem 1: The expressions thus obtained are not be optimal!

Example: m_5 would need 1+2+4+8+16= 31 ms but 4 suffice:

$$\mathrm{m}_5 \equiv \mathrm{m}(x_1, \mathrm{m}(x_2, x_3, x_4), \mathrm{m}(x_2, x_5, \mathrm{m}(x_3, x_4, x_5)))$$

Problem 2: There are equivalent median terms with = "size" but ≠ depth

Depth of t, denoted $d(t)$, is defined recursively by

- if $t = x$ or c, then $d(t) = 0$
- if $t = \mathrm{m}(t_1, t_2, t_3)$, then $d(t) = d(t_1) + d(t_2) + d(t_3) + 1$

Median **NFS**

How to obtain median representations?

Naive approach: Based on median decomposition scheme

$$(*) \quad f(\mathbf{x}) = \mathrm{m}(\, f(\mathbf{x}_i^0)\,,\, x_i\,,\, f(\mathbf{x}_i^1)\,), \quad \text{for every } i \in \{1, \ldots, n\}$$

NB: In the case of monotone functions...

Problem 1: The expressions thus obtained are not be optimal!

Example: m_5 would need 1+2+4+8+16= 31 ms but 4 suffice:

$$\mathrm{m}_5 \equiv \mathrm{m}(x_1, \mathrm{m}(x_2, x_3, x_4), \mathrm{m}(x_2, x_5, \mathrm{m}(x_3, x_4, x_5)))$$

Problem 2: There are equivalent median terms with = "size" but ≠ depth

Depth of t, denoted $d(t)$, is defined recursively by

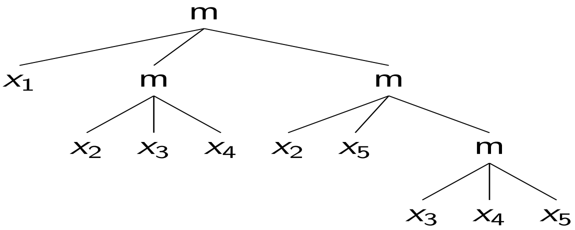
- if $t = x$ or c, then $d(t) = 0$
- if $t = \mathrm{m}(t_1, t_2, t_3)$, then $d(t) = d(t_1) + d(t_2) + d(t_3) + 1$

Structural representation of median forms

Structural representation of a median term t of depth d is $S_t = (n_d, \ldots, n_0)$ where n_i is the number of medians at depth $\leq i$

NB: S_t is a decreasing sequence and $n_d = |t|$

Ex: $t = \mathrm{m}(x_1, \mathrm{m}(x_2, x_3, x_4), \mathrm{m}(x_2, x_5, \mathrm{m}(x_3, x_4, x_5)))$?



Define: $t_1 \leq_{Str} t_2$ if $S_{t_1} \leq_{lex} S_{t_2}$

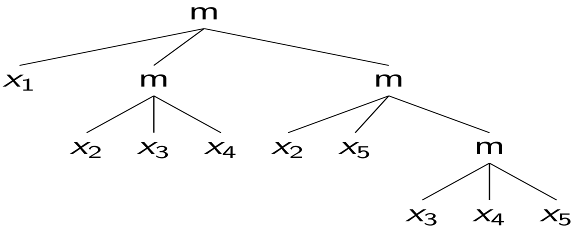
NB: $\leq_{Str}$ prioritizes the size over depth, and "shallowness" over "deepness"

Structural representation of median forms

Structural representation of a median term t of depth d is $S_t = (n_d, \ldots, n_0)$ where n_i is the number of medians at depth $\leq i$

NB: S_t is a decreasing sequence and $n_d = |t|$

Ex: $t = \mathrm{m}(x_1, \mathrm{m}(x_2, x_3, x_4), \mathrm{m}(x_2, x_5, \mathrm{m}(x_3, x_4, x_5)))$?



Define: $t_1 \leq_{Str} t_2$ if $S_{t_1} \leq_{lex} S_{t_2}$

NB: $\leq_{Str}$ prioritizes the size over depth, and "shallowness" over "deepness"

Complexity issues

MNF: t is a median normal form (MNF) if it is *minimal* w.r.t. $\leq_{Str}$

Problem: How difficult is it to find MNF's?

Still eludes us but probably intractable...

SMALLMED:

Input: a median representation t and a decreasing sequence S

Output: SUCCESS if there is an equiv. t' **s.t.** $S_{t'} < S$, FAIL if not

Result: SMALLMED is in the class Σ_2^P

Recall: Σ_2^P class of decision prob.s whose accepting instances are of the form $\{x : \exists c_1 \forall c_2 F(x, c_1, c_2)\}$ **where** c_1 and c_2 are certificates whose lengths are polynomial in $|x|$ **and** F is computable in polynomial time

Few words: Complexity of variant problems and restrictions...

Complexity issues

MNF: t is a median normal form (MNF) if it is *minimal* w.r.t. $\leq_{Str}$

Problem: How difficult is it to find MNF's?

Still eludes us but probably intractable...

SMALLMED:

Input: a median representation t and a decreasing sequence S

Output: SUCCESS if there is an equiv. t' **s.t.** $S_{t'} < S$, FAIL if not

Result: SMALLMED is in the class Σ_2^P

Recall: Σ_2^P class of decision prob.s whose accepting instances are of the form $\{x : \exists c_1 \forall c_2 F(x, c_1, c_2)\}$ **where** c_1 and c_2 are certificates whose lengths are polynomial in $|x|$ **and** F is computable in polynomial time

Few words: Complexity of variant problems and restrictions...

Complexity issues

MNF: t is a median normal form (MNF) if it is *minimal* w.r.t. $\leq_{Str}$

Problem: How difficult is it to find MNF's?

Still eludes us but probably intractable...

SMALLMED:

Input: a median representation t and a decreasing sequence S

Output: SUCCESS if there is an equiv. t' **s.t.** $S_{t'} < S$, FAIL if not

Result: SMALLMED is in the class Σ_2^{P}

Recall: Σ_2^{P} class of decision prob.s whose accepting instances are of the form $\{x : \exists c_1 \forall c_2 F(x, c_1, c_2)\}$ **where** c_1 and c_2 are certificates whose lengths are polynomial in $|x|$ **and** F is computable in polynomial time

Few words: Complexity of variant problems and restrictions...

Complexity issues

MNF: t is a median normal form (MNF) if it is *minimal* w.r.t. $\leq_{Str}$

Problem: How difficult is it to find MNF's?

Still eludes us but probably intractable...

SMALLMED:

Input: a median representation t and a decreasing sequence S

Output: SUCCESS if there is an equiv. t' **s.t.** $S_{t'} < S$, FAIL if not

Result: SMALLMED is in the class Σ_2^{P}

Recall: Σ_2^{P} class of decision prob.s whose accepting instances are of the form $\{x : \exists c_1 \forall c_2 F(x, c_1, c_2)\}$ **where** c_1 and c_2 are certificates whose lengths are polynomial in $|x|$ **and** F is computable in polynomial time

Few words: Complexity of variant problems and restrictions...

Open problems and ongoing work

Part II:

1. Better upper bound? Completeness?
2. Variant decision problems and resp. complexity classes

Part I:

1. Refinement of **NFS** classification
2. Analogous results stratified circuits (variable sharing)

Open problems and ongoing work

Part II:

1. Better upper bound? Completeness?
2. Variant decision problems and resp. complexity classes

Part I:

1. Refinement of **NFS** classification
2. Analogous results stratified circuits (variable sharing)

Kiitos mielenkiinnostanne!

Obrigado pela vossa atenção!

Thank you for your attention!

...and...

Happy Birthday!

...and thank you, Lauri, for all that remains unsaid!