"Unification in finite MV-algebras with constants"

Ramaz Liparteliani

Tbilisi State University, Georgia

Tbilisi 2012

Outline

MV-algebras.

An *MV*-algebra is a structure $(A, \oplus, \otimes, ^*, 0, 1)$ with properties:

- $(A, \oplus, 0)$ is a commutative monoid
- $(x \otimes y) = (x^* \oplus y^*)^*$
- * is an involution: $(x^*)^* = x^*$
- $x \oplus 1 = 1$
- $0^* = 1$
- $(x^* \oplus y)^* \oplus y = (y^* \oplus x)^* \oplus x$, $(x \vee y = y \vee x)$

Axioms for *MV*-algebras.

- $x \oplus y = y \oplus x$
- $x \oplus (y \oplus z) = (x \oplus y) \oplus z$
- $x \oplus 1 = 1$
- $x \oplus 0 = x$
- $x \otimes y = (x^* \oplus y^*)^*$
- $x = (x^*)^*$
- $0^* = 1$
- $(x^* \oplus y)^* \oplus y = (x \oplus y^*) \oplus x$

Example:

$([0,1], \oplus, \otimes, ^*, 0, 1)$:

- $(x \oplus y) = min(1, x + y)$
- $(x \otimes y) = max(0, x + y - 1)$
- $x^* = 1 - x$

For MV_m-algebras we have following additional properties:

Axioms for MV_m-algebras

- $(m-1)x \oplus x = (m-1)x$
- $[(jx) \otimes (x^* \oplus [(j-1)x]^*)]^{m-1} = 0$
  for $m > 3$, $1 < j < m-1$ and j does not divide $m-1$

Example:

$$\left([0, \tfrac{1}{m-1}, ..., \tfrac{m-2}{m-1}, 1], \oplus, \otimes, ^{*}, 0, 1\right):$$

- $(x \oplus y) = min(1, x + y)$
- $(x \otimes y) = max(0, x + y - 1)$
- $x^{*} = 1 - x$

$$(A, \oplus, \otimes, ^*, 0 = C_0, C_1, ..., C_{n-2}, 1 = C_{n-1})$$

Axioms for MVS_n-algebras

- $iC_1 = C_i,\ i = (2, ..., n-1)$
- $C_1 = C^*_{n-2}$

Subalgebra:

- $C_i \oplus C_j = C_k$
- $C_i \otimes C_j = C_{k-n+1}$
- $C_i^* = C_{n-1-i}$.

Here $k = min(n-1, i+j)$.

Example:

$S = ([0,1], \oplus, \otimes, ^*, 0, C_1, ..., C_{n-2}, 1)$

$C_i(x) = \frac{i}{n-1}$

MV_mS_n algebras

- Defined for such m-s, that $n-1$ divides $m-1$
- MV_m-algebra axioms.
- Axioms for C_i operators.

From here on by MV_mS_n, we consider that $n-1$ divides $m-1$.

Proposition:

The only subdirectly irreducible algebras in variety $\mathbf{MV_m S_n}$:

$$S(k) = (\{0, \frac{1}{k-1}, \frac{2}{k-1}, ..., \frac{k-2}{k-1}, 1\}, \oplus, \otimes, ^*, 0, C_1, ..., C_{n-2}, 1),$$

where $n-1$ divides $k-1$ and $k-1$ divides $m-1$.

Corollary:

Every MV_mS_n-algebra A is isomorphic to the subdirect product of $S(k) = (\{0, \frac{1}{k-1}, \frac{2}{k-1}, ..., \frac{k-2}{k-1}, 1\}, \oplus, \otimes, ^*, 0, C_1, ..., C_{n-2}, 1)$ where $n-1$ divides $k-1$ and $k-1$ divides $m-1$.

$$A \hookrightarrow \prod_{k:n-1|k-1\&k-1|m-1} S(k)$$

Recall that every identity $P(x_1, ..., x_k) = Q(x_1, ..., x_k)$ is an identity of $\mathbf{MV_mS_n}$ iff the corresponding polynomials $P(x_1, ..., x_k)$ and $Q(x_1, ..., x_k)$ are equal to each other in the k-generated free algebra $F_{MV_mS_n}(k)$ on its free generators $P(g_1, ..., g_k) = Q(g_1, ..., g_k)$.

Recursive Sequence:

- $p_n(n, k) = n^k$
- $p_n(i, k) = i^k - \sum_{\substack{j-1 | i-1 \\ n \leq j < i}} p_n(j, k)$

Example:

- $p_4(4, k) = 4^k$
- $p_4(7, k) = 7^k - 4^k$
- $p_4(13, k) = 13^k - (7^k - 4^k) - 5^k - 4^k = 13^k - 7^k - 5^k$

Theorem

k-generated free MV_mS_n-algebra over the variety $\mathbf{MV_mS_n}$:

$$F_{MV_mS_n}(k) = \prod_{j \geq n}^{j-1|m-1} S_j^{p_n(j,k)}$$

Example:

$$F_{MV_{13}S_4}(k) = S_4^{4^k} \times S_5^{5^k} \times S_7^{7^k - 4^k} \times S_{13}^{13^k - 7^k - 4^k}$$

Another Recursive Set:

$$J = \{j_i | i = 1, 2, ...\}$$

- $j_1 = n$
- $(j_i - 1)$ divides $(j_{i+1} - 1)$

Example:

$$J = \{n, 2n-1, 4n-3, 8n-7, ..., 2^i n - 2^i + 1, ...\}$$

Theorem:

Let $g_1^{(j_i)}, ..., g_k^{(j_i)}$ be free generators of the k-generated free algebras $F_{MV_{j_i}S_n}(k)$ and $s_m = (g_m^{(j_1)}, g_m^{(j_2)}, ...)$. The subalgebra $F_{MVS_n}(k)$ of the direct limit $\prod\limits_{j_i \in J} F_{MV_{j_i}S_n}(k)$ generated by $s_m \in \prod\limits_{j_i \in J} F_{MV_{j_i}S_n}(k)$ $(m = 1, ..., k)$ is a free MVS_n-algebra.

Direct Limit:

$$F_{MV_{j_1}S_n}(k) \mapsto \ldots F_{MV_{j_i}S_n}(k) \mapsto \ldots \mapsto \prod_{j_i \in J} F_{MV_{j_i}S_n}(k) \hookleftarrow F_{MVS_n}(k)$$

Generators:

$$\begin{array}{cccccccccccc}
s_1 & = & (& g_1^{(j_1)} & , & g_1^{(j_2)} & , & \ldots & g_1^{(j_i)} & , & \ldots &) \\
s_2 & = & (& g_2^{(j_1)} & , & g_2^{(j_2)} & , & \ldots & g_2^{(j_i)} & , & \ldots &) \\
. & . & . & . & . & . & . & . & . & . & . & . \\
s_k & = & (& g_k^{(j_1)} & , & g_k^{(j_2)} & , & \ldots & g_k^{(j_i)} & , & \ldots &)
\end{array}$$

Proposition:

In the algebra S_n we can construct the cyclic operator by means of the MV_mS_n-algebra operations:

$$f(x) = ((n-1)x)^* \vee (x \otimes C_{n-2}).$$

Theorem

Algebra S_n is functionally equivalent to n-valued Post algebra.

Logic $L_m C_n$:

The language consists of:
1) propositional variables p,q,r and with indices;
2) connectives: $\rightarrow, \neg, C_0, C_1, ..., C_{n-2}, C_{n-1}$.

Formulas are built in usual way. Denote set of all formulae by Φ.

The axioms of the logic:

- Lukasiewicz logic axioms
- axioms translating the ones for operators $C_i (i = 0, ...n-1)$.

Inference rule: $\alpha, \alpha \rightarrow \beta / \beta$ (Modus Ponens)

Definition:

Lindenbaum algebra L is constructed in usual way. Define the equivalence relation $\equiv$: $\alpha \equiv \beta$ iff $\vdash \alpha \to \beta$ and $\vdash \beta \to \alpha$. It is clear that $[\alpha/\equiv] = [\beta/\equiv]$ iff $\vdash \alpha \leftrightarrow \beta$.

Completeness:

The function $\nu : \Phi \to S_n$ is called a value function if:

i) the function is defined for every formula $\alpha \in \Phi$.

ii) for every propositional variable p $\nu(p) \in S_n$.

iii) if α and β are formulas, then

$\nu(\alpha \to \beta) = \nu(\alpha) \to \nu(\beta) = \nu(\alpha)^* \oplus \nu(\beta)$; $\nu(\neg\alpha) = \nu(\alpha)^*$;

$\nu(\alpha \vee \beta) = \nu(\alpha) \vee \nu(\beta) = (\nu(\alpha) \otimes \nu(\beta)^*) \oplus \nu(\beta)$;

$\nu(\alpha \wedge \beta) = \nu(\alpha) \wedge \nu(\beta) = (\nu(\alpha) \oplus \nu(\beta)^*) \otimes \nu(\beta)$;

$\nu(C_i) = C_i \quad i = 0, ..., n-1$

A formula α is called tautology if $\nu(\alpha) = 1$ for every value function ν.

Completeness:

A formula α is a theorem of logic if and only if α is a tautology.

Some Definitions:

$\Psi_k = \{p_1, ..., p_k\}$
$\Phi_k = \{\alpha : \alpha$ is a formula with variables in $\Psi_k\}$

Theorem:

$F_{MV_m S_n}(k) \cong \Phi_k / \equiv$.

Definition:

An algebra $A \in \mathbf{K}$ is called projective, if for any $B, C \in \mathbf{K}$, any epimorphism (onto homomorphism) $\beta : B \to C$ and any homomorphism $\gamma : A \to C$, there exists a homomorphism $\alpha : A \to B$ such that $\beta\alpha = \gamma$

Definition:

A subalgebra A of free algebra $F_V(k)$ is called a projective subalgebra of $F_V(k)$ if there exists an endomorphism $h : F_V(k) \to F_V(k)$ such that $h(F_V(k)) = A$ and $h(x) = x$ for every $x \in A$.

Theorem

Algebra A is projective in the variety $\mathbf{MV_m S_n}$ if it is isomorphic to the algebra $S_n \times A^{'}$ where $A^{'}$ is some $MV_m S_n$-algebra.

$$A \equiv S_n \times A^{'}$$

Theorem:

Every subalgebra of the free k-generated algebra $F_{MV_m S_n}(k)$ is projective.

Theorem:

Every endomorphic image of the free k-generated algebra $F_{MV_m S_n}(k)$ is projective.

Definition:

A formula $\alpha \in \Phi_k$ is called projective if there exists a substitution $\sigma : \Psi_k \to \Phi_k$ such that $\vdash \sigma(\alpha)$ and $\alpha \vdash \beta \leftrightarrow \sigma(\beta)$, for all $\beta \in \Phi_k$.

Theorem:

For every k-generated projective MV_mS_n-algebra, there exists a projective formula α of k-variables, such that A is isomorphic to $\Phi_k/[\alpha)$, where $[\alpha)$ is the principal filter generated by $\alpha \in \Phi_k$.

Theorem:

For every projective formula α of k-variables, $\Phi_k/[\alpha)$ is a projective algebra.

Corollary:

There exists a one-to-one correspondence between projective formulas with k-variables and k-generated projective subalgebras of Φ_k.

E-Unification:

Given a pair of terms s,$t \in T_n$ we call the *substitution* $\sigma : T_n \Rightarrow T_\omega$ an *E-unifier* of s, t if

$$E \models \sigma(s) \approx \sigma(t).$$

less/more general unifications:

Given substitutions $\sigma, \sigma' : T_n \Rightarrow T_\omega$ we say σ is *less general* (Mod E) than σ' and write $\sigma \preceq \sigma'$ if there exists a substitution $\tau : T_\omega \Rightarrow T_\omega$ such that

$$E \models \sigma(x_i) \approx \tau \circ \sigma'(x_i)(1 \leq i \leq n).$$

E-equivalent substitutions:

$\sigma \sim_E \sigma'$ iff $\sigma \preceq \sigma'$ and $\sigma' \preceq \sigma$

most general unifiers:

We call unifier σ a *most general unifier* (E-unifier) (*mgu* for short) if for any unification τ,

$$\sigma \preceq \tau \text{ implies } \sigma \sim_E \tau$$

Unificators:

Suppose we have to find unifiers for $f(x_1, ..., x_k)$.

1. We evaluate the formula on the elements of the k-generated free algebra: $f(a_1, ..., a_k)$
2. For all evaluations that are equal to 1, we take the polynomials: $a_i = P(g_1, g_2, ..., g_k)$
3. Needed Unifications: $x_i \mapsto P(y_1, y_2, ..., y_k)$

Theorem:

Unification type in considered cases are unitary.

Proposition:

All the algebras considered here are symmetric (DeMorgan duality), so solving the unification problem for $f(X) = 1$ is equivalent to solving the problem for $f(X) = 0$

Definition:

Define n different functions $\dagger_i : S_n \to S_n$:

$$\dagger_i(x) = \begin{cases} 1, & \text{if } x = C_i \\ 0, & \text{if } x \neq C_i \end{cases}$$

Example:

In case of $n = 2$, S_n coinsides with the Boolean algebra:

- $\dagger_1(x) = x$
- $\dagger_0(x) = \bar{x}$
- $f(x) = \bar{x}f(0) \vee xf(1)$

CDNF:

Let f be a k-ary function on S_n. $f : S_n^k \to S_n$:

$$f(x_1, ..., x_k) = \bigvee_{i_1,...,i_k \in S_n} (\bigwedge_{j=1}^{k} \dagger_{i_j} x_j \wedge f(i_1, ..., i_k))$$

Example:

$(x \oplus y) \otimes z \otimes z \otimes x^*$

Example:

$f(x, y, z) = (\dagger_0 x \wedge \dagger_1 y \wedge \dagger_2 z \wedge C_1) \vee (\dagger_0 x \wedge \dagger_2 y \wedge \dagger_1 z \wedge C_2) \vee (\dagger_1 x \wedge \dagger_1 y \wedge \dagger_2 z \wedge C_1) \vee (\dagger_1 x \wedge \dagger_0 y \wedge \dagger_0 z \wedge C_1) \vee (\dagger_2 x \wedge \dagger_2 y \wedge \dagger_2 z \wedge C_1)$

Definition:

Cofactor of f w.r.t. to literal $\dagger_i x$ is obtained by substitution:

- $\dagger_i x$ by 1.
- $\dagger_j x$ by 0, for $j \neq i$.

Denote cofactor by $f_{\dagger_i x}$

Our example:

$$f_{\dagger_0 x} = (\dagger_1 y \wedge \dagger_2 z \wedge C_1) \vee (\dagger_2 y \wedge \dagger_1 z)$$
$$f_{\dagger_1 x} = (\dagger_1 y \wedge \dagger_2 z \wedge C_1) \vee (\dagger_0 y \wedge \dagger_0 z \wedge C_1)$$
$$f_{\dagger_2 x} = \dagger_2 y \wedge \dagger_2 z \wedge C_1$$

Variable Conjunctive Eliminant:

- $VCE(f, 0) = f$.
- $VCE(f, \{x\}) = f_{\dagger_0 x} \wedge f_{\dagger_1 x} \wedge ... \wedge f_{\dagger_{n-1} x}$.
- $VCE(f, A \cup B) = VCE(VCE(f, A), B)$.

Overview of Method:

X-Inputs; G-Parametric functions; P-Parameters:

Equation: $f(X) = 0$

Solution:

$$\begin{cases} g_0 = 0 \\ X = G(P) \end{cases}$$

With following conditions:

$$\begin{cases} g_0 = VCE(f, X) \\ f(G(P)) = VCE(f, X), \forall P \in S_n^k \\ f(A) = VCE(f, X) \implies \exists P \in S_n^k, G(P) = A \end{cases}$$

Work in Progress:

- Complete efficient Algorithm for the n-valued case;
- Complexity of the above algorithms.