REPORTS ON MATHEMATICAL LOGIC
30 (1996), 3–11

Manuel ABAD, Alicia FERNANDEZ and Nelli MESKE

FREE BOOLEAN CORRELATION LATTICES

A b s t r a c t. In this paper we study some algebraic properties of the variety of Boolean correlation lattices. We give a characterization of congruences and simple algebras of the variety and we describe the algebra with a finite set of free generators.

1. Introduction

A *correlation lattice* is an algebra $(B, \wedge, \vee, \sigma, 0, 1)$ where $(B, \wedge, \vee, 0, 1)$ is a bounded lattice and σ is a dual endomorphism on B which has the property $\sigma^{2n}(x) = x$ for a fixed number n, $n \in 2N + 1$ ([3], [4]). This notion generalizes orthomodular lattices, and in the distributive case, Boolean algebras, De Morgan algebras and some classes of Ockham algebras. Moreover, in [4], D. Schweigert and M. Szymanska proved that correlation lattices can be used as switching algebras for multivalued logic functions.

The aim of this paper is to study some properties of the variety of Boolean correlation lattices. We give a characterization of congruences and simple algebras of the variety in a different way from that given in

Received

[4]. Finally, we determine the finitely-generated, free Boolean correlation lattice.

We would like to thank the referee for his/her thoughtful comments and suggestions. We found them very helpful and felt that they led to a much improved presentation.

2. Involutive Filters and Congruences

Let $\mathcal{A}_n$ be the class of algebras $(B, \wedge, \vee, \sigma, 0, 1)$ of type $(2, 2, 1, 0, 0)$, n fixed, $n \in 2N+1$, such that:

1. $(B, \wedge, \vee, 0, 1)$ is a distributive lattice with 0 and 1.
2. $\sigma(x \wedge y) = \sigma(x) \vee \sigma(y)$, $\sigma(x \vee y) = \sigma(x) \wedge \sigma(y)$.
3. $\sigma^n(x) \wedge x = 0$, $\sigma^n(x) \vee x = 1$.
4. $\sigma^{2n}(x) = x$.

It is clear that σ is order reversing, $\sigma(0) = 1$ and $\sigma(1) = 0$.

If $B \in \mathcal{A}_n$, we say that B is a *Boolean correlation lattice* [3], [4]. The Boolean complementation is given by $\alpha = \sigma^n$, and the mapping $\tau = \sigma \circ \alpha$ is a Boolean automorphism.

Let $B \in \mathcal{A}_n$. An element $b \in B$ is called an *involutive element* of B if $\sigma^2(b) = b$.

If b is an involutive element, then $\sigma(b) \vee b = 1$ (and consequently, $b \wedge \sigma(b) = 0$). Indeed, if $\sigma^2(b) = b$, then $1 = \sigma(0) = \sigma(\sigma^n(b) \wedge b) = \sigma^{n+1}(b) \vee \sigma(b) = b \vee \sigma(b)$, since $n+1$ is even, and hence $\sigma^{n+1}(b) = b$. Moreover, if $\sigma(b) \vee b = 1$, then b is an involutive element, as is easy to verify.

Thus, b is an involutive element of B if and only if $\sigma(b)$ is the Boolean complement of b. 0 and 1 are involutive elements of B.

The set of all involutive elements in B will be denoted I.

Proposition 2.1. *I is a Boolean algebra.*

A filter F of an algebra B is said to be an *involutive filter* of B if $\sigma^2(x) \in F$, whenever $x \in F$.

Theorem 2.2. *A principal filter $F = F(b)$ of B is an involutive filter if and only if b is an involutive element of B.*

Proof. Let $F = F(b)$ be an involutive filter of B. Since $\sigma^2(b) \in F(b)$ we get $b \leq \sigma^2(b)$. Since σ^2 is order preserving, $\sigma^2(b) \leq \sigma^4(b)$, $\sigma^4(b) \leq \sigma^6(b)$, $\ldots$, $\sigma^{2n-2}(b) \leq \sigma^{2n}(b)$. Hence $b \leq \sigma^2(b) \leq \ldots \leq \sigma^{2n}(b) = b$, which proves $b = \sigma^2(b)$. Thus b is an involutive element of B. For the converse, if $x \in F$, then $b \leq x$, so $b \wedge x = b$ and then $b = \sigma^2(b) = \sigma^2(b) \wedge \sigma^2(x) = b \wedge \sigma^2(x)$. Therefore $b \leq \sigma^2(x)$. So $\sigma^2(x) \in F$.

Corollary 2.3. *If B is a finite algebra, then an involutive filter F of B is maximal if and only if $F = F(b)$ and b is an atom of the Boolean algebra I.*

Lemma 2.4. *If $B \in \mathcal{A}_n$ and b is an involutive element of B, then $x \wedge b = y \wedge b$ if and only if $x \vee \sigma(b) = y \vee \sigma(b)$.*

Proof. It follows immediately, since $\sigma(b)$ is the Boolean complement of b.

Theorem 2.5. *For b an involutive element of B, $b \neq 0, 1$, the relation θ_b defined by $(x, y) \in \theta_b$ if and only if $x \wedge b = y \wedge b$, is a non trivial congruence on B.*

Proof. It follows easily from the previous Lemma.

Theorem 2.6. *If θ is a congruence on a finite Boolean correlation lattice B, then there exists an involutive element b of B, such that $\theta = \theta_b$, that is $(x, y) \in \theta$ if and only if $x \wedge b = y \wedge b$.*

Proof. Consider $F = \{x \in B : (x, 1) \in \theta\}$. Then, F is a filter.

If $x \in F$, then $b_x = x \wedge \sigma^2(x) \wedge \ldots \wedge \sigma^{2n-2}(x) \in F$ and b_x is an involutive element of B.

Then $b = \bigwedge_{x \in F} b_x$ is an involutive element and $F = F(b)$.

Now we must prove that $(x, y) \in \theta$ if and only if $x \wedge b = y \wedge b$.

Let $x' = \alpha x$, $y' = \alpha y$ Boolean complements of $x, y \in B$.

Then $(x, y) \in \theta$ if and only if $x \vee y' \in F$ and $x' \vee y \in F$, and this is equivalent to $(x \vee y') \wedge b = (x' \vee y) \wedge b = b$.

From $(x \vee y') \wedge b = b$, it follows $(x \vee y') \wedge b \wedge y = b \wedge y$, that is, $(x \wedge y) \wedge b = b \wedge y$. Similarly, from $(x' \vee y) \wedge b = b$ it follows $(x \wedge y) \wedge b = b \wedge x$. Thus, $x \wedge b = y \wedge b$.

Conversely, if $x \wedge b = y \wedge b$, then

$$(x \vee y') \wedge b = (x \wedge b) \vee (y' \wedge b) = (y \wedge b) \vee (y' \wedge b) = (y \vee y') \wedge b = b.$$

Similarly, $(x' \vee y) \wedge b = b$. So $(x \vee y') \wedge b = (x' \vee y) \wedge b$.

So $(x \vee y') \wedge b = (x' \vee y) \wedge b$ if and only if $x \wedge b = y \wedge b$.

If b_1 and b_2 are involutive elements of B, and $\theta_{b_1} = \theta_{b_2}$, then $F(b_1) = F(b_2)$ and hence $b_1 = b_2$. Then, there is a one-to-one correspondence between the family of congruences defined on a finite Boolean correlation lattice B and the set of involutive elements of B.

Corollary 2.7. *An algebra B is simple if and only if* 0 *and* 1 *are the only involutive elements of B.*

Corollary 2.8 [4]**.** *A finite algebra B in $\mathcal{A}_n$ is simple if and only if σ^2 is a Boolean automorphism of B that acts transitively on the atoms of B.*

As a consequence, if A_k is a simple Boolean correlation lattice with k atoms, then $(\sigma^2)^k(x) = x$ for all $x \in A_k$, and k is the least positive integer with this property. Thus $k|n$, as is easy to verify. Conversely, suppose that $k|n$ and let A_k be a Boolean algebra with k atoms. Consider the automorphism τ on A_k induced by a cyclic permutation on the atoms. If $\{a_1, a_2, \ldots, a_k\}$ is the set of atoms of A_k, we can assume, with no loss in generality, that τ is induced by the permutation $(a_1 a_2 \ldots a_k)$. Then, the operation $\sigma(x) = \tau(\alpha(x))$ is such that (A_k, σ) is a simple member of the variety $\mathcal{A}_n$. So, for each $k|n$, there exists a uniquely determined simple Boolean correlation lattice A_k. The algebras $\{A_k\}$ generate $\mathcal{A}_n$ [4].

If $b_1, b_2, \ldots, b_s$ are the atoms of I, then the algebras $B/F(b_i)$, $1 \leq i \leq s$ are simple, and we know that B is isomorphic to a subalgebra of $\prod_{i=1}^{s} B/F(b_i)$, where the isomorphism is given by $\phi(x) = (\phi_\gamma(x))_{1\leq\gamma\leq s}$, $\phi_\gamma : B \to B/F(b_\gamma)$ being the natural homomorphism.

If B is finite, ϕ is also surjective. Indeed, if $y = (y_\gamma)_{1\leq\gamma\leq s}$ belongs to $\prod_{i=1}^{s} B/F(b_i)$, for each γ, let $x_\gamma \in B$ be such that $\phi_\gamma(x_\gamma) = y_\gamma$. Then $x = \bigvee_{\gamma=1}^{s}(x_\gamma \wedge b_\gamma)$ is such that $\phi_\gamma(x) = y_\gamma$, hence $\phi(x) = y$.

Then we have the following theorem:

Theorem 2.9. *Any finite Boolean correlation lattice (with more than one element) is isomorphic to the direct product* $\prod_{\gamma=1}^{s} B/F(b_\gamma)$*, where* $\{b_1, b_2, \ldots, b_s\}$ *is the set of all atoms of the Boolean algebra* I*.*

In the next section, we will need the subalgebras of a simple algebra A_k, $k|n$.

As before, let $\{a_1, \sigma^2(a_1), \ldots, \sigma^{2k-1}(a_1)\}$ denote the set of atoms of A_k. Let d be a divisor of k, $k = t \cdot d$, t a positive integer. Then there exists a unique subalgebra S_d of A_k verifying: $(\sigma^2)^d(x) = x$ for all $x \in S_d$ and d is the least positive integer with that property. Indeed, Consider the element $b = a_1 \vee \sigma^{2d}(a_1) \vee \ldots \vee \sigma^{2(t-1)d}(a_1)$ and let S_d be the subalgebra generated by b. It is not difficult to see that S_d verifies the required property. Now, suppose that S is a subalgebra of A_k such that $(\sigma^2)^d(x) = x$ for all $x \in S$ and d is the least positive integer with that property. Let c be an atom of S. Then, since σ^2 acts transitively on the atoms of A_k, the elements c, $\sigma^2(c)$, $\ldots$, $\sigma^{2(d-1)}(c)$ are all distinct atoms of S. Suppose, with no loss in generality, that $a_1 \leq c$. Then $\sigma^{2d}(a_1) \leq c$, $\ldots$, $\sigma^{2(t-1)d}(a_1) \leq c$. For cardinality reasons, it follows that $a_1, \sigma^{2d}(a_1), \ldots, \sigma^{2(t-1)d}(a_1)$ are all the atoms of A_k preceding c (so $c = b$) and that $S = S_d$.

Summarizing, the mapping $d \to S_d$ is a one-to-one correspondence between the set of divisors of k and the set of subalgebras of A_k, so identifying isomorphic algebras we can say that the subalgebras of A_k are the algebras A_d, with $d|k$. It is not dificult to see that if A_d and $A_{d'}$ are subalgebras of A_k, then $A_d \cap A_{d'} = A_m$, where m is the greatest common divisor of d and d'.

3. Free Algebras

The aim of this section is to describe the free algebra $L_r(n)$ of the variety $\mathcal{A}_n$ over a finite set G with r generators, r being a positive cardinal number. It is known that $L_r(n)$ exists, and from [1], Th. 3, it is finite.

So

$$L_r(n) = \prod_{M \in \mathcal{M}} L_r(n)/M,$$

where $\mathcal{M}$ is the family of all maximal involutive filters of $L_r(n)$.

We know that $L_r(n)/M$ is isomorphic to A_k for some k, $k|n$. Then if we put $\mathcal{M}_k = \{M \in \mathcal{M} : L_r(n)/M \text{ is isomorphic to } A_k\}$, we have that $\mathcal{M} = \bigcup \mathcal{M}_k$, $\mathcal{M}_i \bigcap \mathcal{M}_j = \emptyset$ if $i \neq j$, and

$$L_r(n) = \prod_{k|n} \prod_{M \in \mathcal{M}_k} L_r(n)/M \cong \prod_{k|n} A_k^{\alpha_k},$$

where $\alpha_k = |\mathcal{M}_k|$.

So we must calculate α_k.

Lemma 3.1. *A lattice automorphism f of a Boolean correlation lattice B is a correlation automorphism if and only if $f \circ \tau = \tau \circ f$.*

Proof. Observe that f commutes with α, being that α is the Boolean complementation. Then $f(\sigma(x)) = f((\tau \circ \alpha)(x)) = \alpha f(\tau(x))$, and $\sigma(f(x)) = (\tau \circ \alpha)(f(x)) = \alpha\tau(f(x))$.

If $\mathrm{Aut}(A_k)$ denotes the set of all automorphisms of A_k, then we have the following:

Theorem 3.2. $\mathrm{Aut}(A_k) = \{\tau^t : 0 \leq t \leq k-1\}$.

Proof. Let $g \in \mathrm{Aut}(A_k)$. Consider an atom a_i in A_k. Then $g(a_i) = a_j$ is an atom of A_k. We can suppose, without loss in generality, that $i < j$. Since the orbit of a_i under τ is $\{a_1, a_2, \ldots, a_k\}$, then there exists t such that $g(a_i) = \tau^t(a_i) = a_j$. Now, for arbitrary s, $1 \leq s \leq k$, there exists r such that $a_s = \tau^r(a_i)$. Then

$$g(a_s) = g(\tau^r(a_i)) = \tau^r g(a_i) = \tau^r \tau^t(a_i) = \tau^t \tau^r(a_i) = \tau^t(a_s).$$

So $g = \tau^t$ on the set of atoms of A_k. Thus $g = \tau^t$.

Corollary 3.3. $|\mathrm{Aut}(A_k)| = k$.

Let $\mathrm{Epi}(B, A)$ be the set of all epimorphisms from B onto A.

Theorem 3.4. $\alpha_k = |\mathcal{M}_k| = \dfrac{|\mathrm{Epi}(L_r(n), A_k)|}{|\mathrm{Aut}(A_k)|}$.

Proof. The map $h \to s(h) = \mathrm{Ker}\ h$ carrying each $h \in \mathrm{Epi}(L_r(n), A_k)$ into its kernel in $\mathcal{M}_k$ is clearly surjective. In addition, if $M = \mathrm{Ker}\ h \in \mathcal{M}_k$, then $s^{-1}(M) = \{g \circ h : g \in \mathrm{Aut}(A_k)\}$. Consequently, $|s^{-1}(M)| = |\mathrm{Aut} A_k|$ and then the result follows.

Proposition 3.5. *If $k \neq 1$, $|\mathrm{Epi}(L_r(n), A_k)| = |F^*(G, A_k)|$, where $F^*(G, A_k)$ is the set of all functions from G into A_k such that $f(G) \not\subseteq A_d$ for any maximal proper subalgebra A_d of A_k. If $k = 1$, $|\mathrm{Epi}(L_r(n), A_k)| = 2^r$.*

Proof. The case $k = 1$ is clear. For $k \neq 1$, it suffices to consider the map $h \to h_{|G}$ carrying each $h \in \mathrm{Epi}(L_r(n), A_k)$ into its restriction to G. The result follows since the subalgebra generated by $f(G)$ in A_k is A_k if and only if $f(G) \not\subseteq A_d$ for any maximal proper subalgebra A_d of A_k.

If we denote $D(k)$ the set of all maximal proper divisors of k, then $F^*(G, A_k) = F(G, A_k) \setminus \bigcup_{d \in D(k)} F(G, A_d)$, where $F(G, A_d)$ is the set of all functions from G into A_d. So

$$|F^*(G, A_k)| = |F(G, A_k)| \; - | \bigcup_{d \in D(k)} F(G, A_d)|$$

$$= |F(G, A_k)| - \sum_{X \subseteq D(k),\, X \neq \emptyset} (-1)^{|X|-1} |\bigcap_{d \in X} F(G, A_d)|.$$

But

$$\bigcap_{d \in X} F(G, A_d) = \{f \in F(G, A_k) : f(G) \subseteq \bigcap_{d \in X} A_d\}$$
$$= \{f \in F(G, A_k) : f(G) \subseteq A_{m(X)}\},$$

where $m(X)$ is the greatest common divisor of the elements of X.

Then

$$|\bigcap_{d \in X} F(G, A_d)| = 2^{r \cdot m(X)},$$

and then

$$|f^*(G, A_k)| = 2^{r \cdot k} - \sum_{X \subseteq D(k),\, X \neq \emptyset} (-1)^{|X|-1} \cdot 2^{r \cdot m(X)}$$

$$= \sum_{X \subseteq D(k)} (-1)^{|X|} \cdot 2^{r \cdot m(X)} = a(r, k),$$

if we put $m(\emptyset) = k$.

Therefore,

Corollary 3.6. $\alpha_k = \dfrac{a(r, k)}{k}.$

This formula has been obtained by A. Monteiro in [2] by using cyclic Boolean algebras.

References

[1] J. Berman, *Distributive lattices with an additional unary operation*, Aequationes Math. 16(1977), 165–171.

[2] A. Monteiro, *Algèbres de Boole Cycliques*, Rev. Roum. Math. Pures et Appl., Tome XXIII, No. 1(1978), 71–76.

[3] D. Schweigert and M. Szymanska, *On distributive correlation lattices*, Coll. Math. Soc. Janos Bolyai 33(1980), 697–721.

[4] D. Schweigert and M. Szymanska, *A completeness theorem for correlation lattices*, Zeitschr. f. math. Logik und Grundlagen d. Math. 29(1983), 427–434.

Departamento de Matemática
Universidad Nacional del Sur
8000 Bahía Blanca
Argentina

Departamento de Matemática
Fac. de Economía
Universidad Nacional del Comahue
8300 Neuquén
Argentina