PUBLICATIONS DE L'INSTITUT MATHÉMATIQUE
Nouvelle série tome 54 (68), 1993, 13–17

PSEUDO-GALOIS EXTENSIONS OF BOOLEAN ALGEBRAS

Žikica Perović

Abstract. We define pseudo-Galois extensions of Boolean algebras and reduce the problem of their characterization to some problems on permutations groups.

0. Introduction

In [**9**] was given a characterization of Galois extensions of Boolean algebras. Here we weaken the definition of Galois extensions and obtain an interesting characterization. Let us fix a few definitions first.

Let B be a Boolean algebra. $\operatorname{Ult} B$ denotes the Stone space of ultrafilters on B. Let C be a subalgebra of B. For $q \in \operatorname{Ult} C$, $\langle q\rangle^{fi}$ is the filter on B generated by q. We say that q splits in B if there are distinct $p, p' \in \operatorname{Ult} B$ which extend q i.e. such that $p \cap C = p' \cap C = q$. C is relatively complete (rc) subalgebra of B if for each $b \in B$ there exists the greatest element $c \in C$ such that $c \leq b$. We denote this element by $\operatorname{pr}_C(b)$. We also use notation $\operatorname{ind}_C(b)$ for $-(\operatorname{pr}(b) + \operatorname{pr}(-b))$. It is a clopen set in $\operatorname{Ult} C$ consisting of ultrafilters that have an extension to $\operatorname{Ult} B$ containg b and also an extension to $\operatorname{Ult} B$ containing $-b$.

B is a finite extension of C if there exist $u_1, \dots, u_n \in B$, such that $B = C(u_1, \dots, u_n)$. Let $B = C(u_1, \dots, u_n)$. Set of generators $F = \{u_1, \dots, u_n\}$ is reduced if they are partition of one, and for every $u \neq v \in F$, $u \notin \langle C \cup F \setminus \{u, v\}\rangle$. For $i \leq n$, $J_i^u = \{b \in B | b \cdot u_i = 0\}$ is an ideal in B. These ideals make an extender, meaning that their intersection contains just 0, and if $b \in B$ belongs to one of them, then $-b$ does not belong to any of them. It is easy to see that in the case when B is an rc-extension of C, these ideals are principal.

Definition. Let $B = C(u_1, \dots, u_n)$, where $\langle u_1, \dots, u_n\rangle$ is a reduced set of generators. For $p \in \operatorname{Ult} C$, $h(p)$ is the number of extensions of p in $\operatorname{Ult} B$.

PROPOSITION 0.1 *Let C and B be as in definition, $p \in \operatorname{Ult} C$ ultrafilter which splits in b and $M_p = \{i | i \leq n,\ p \in \operatorname{ind}(u_i)\}$; $h(p) = |M_p|$.*

Supported by the Science Fund of Serbia, grant number 0401A, through Math. Inst.

AMS Subject Classification (1991): Primary 03 E 05

Definition. Let $B = C(u_1, \ldots, u_n)$, and $k \leq n$; define $\mathcal{F}_k^B = \{p \in \mathrm{Ult}\, C | h(p) = k\}$.

PROPOSITION 0.2 *$\mathcal{F}_k^B$ is clopen in $\mathrm{Ult}\, C$ i.e. $\mathcal{F}_k^B \in C$, and $\bigvee\{\mathcal{F}_k^B | k \leq n\}$=1.*

Definition. Let B be a finite extension of C. The height sequence for B over C is $\{k \in N | \mathcal{F}_k^B \neq 0\}$ in the increasing order.

The following theorem is Theorem 2.2 from [**8**].

THEOREM 0.1. *Let B be a finite* rc*-extension of C, such that* $\max\{h(p) : p \in \mathrm{Ult} C\} = l$. *There exists a reduced set of generators $\langle v_1, \ldots, v_l \rangle$, such that $B = C(v_1, \ldots, v_l)$. B cannot be generated by a smaller reduced set over C. If M is a generating set for B over C, then $2^{|M|} \geq l$.*

From the proof of this theorem (presented in [**8**]), one can see that $\langle v_1, \ldots, v_l \rangle$ was constructed so that $\mathcal{F}_k^B = \bigwedge\{\mathrm{ind}(v_i) : i \leq k\}$, for $2 \leq k \leq l$, and $\mathcal{F}_1^B \leq v_1$. This means that for $2 \leq k \leq l$ and $p \in \mathcal{F}_k^B$, the atoms of $B/\langle p \rangle^{fi}$ are $v_1/\langle p \rangle^{fi}, \ldots, v_k/\langle p \rangle^{fi}$.

1. Pseudo-Galois extensions

Definition. Let B be a finite extension of a Boolean algebra C. Automorphisms $f, g \in \mathrm{Aut}_C B$ are relatively-strongly distinct if for every nonzero $c \in C$, there is an $s \in B$ such that $f(s) \cdot c \neq g(s) \cdot c$.

Definition. Let $C < B$. b is a pseudo-Galois extension of C, if B is a finite extension of C and there exists a finite subgroup G of relatively-strongly distinct members of $\mathrm{Aut}_C B$ such that $\mathrm{Fix} G = C$.

Pseudo-Galois extensions are relatively complete (Theorem 3.6 in [**6**]). Henceforth we can suppose that the generating set for B over C has been chosen according to the note following Theorem 0.1. Let $G < \mathrm{Aut}_C B$. For $g \in G$ and $p \in \mathcal{F}_k^B \subset \mathrm{Ult}\, C$, let $\hat{g} : B/\langle p \rangle^{fi} \to B/\langle p \rangle^{fi}$ be the automorfism induced by g. Let also $\rho_g^p : At(B/\langle p \rangle^{fi}) \to B/\langle p \rangle^{fi}$ be the correspondence among the atoms of factor algebras. ρ_g^p ia actually a permutation of the set $\{u_1/\langle p \rangle^{fi}, \ldots, u_k/\langle p \rangle^{fi}\}$. Finally, we define a mapping $\sigma_p : G \to S_k$, by $\rho_g^p(u_i/\langle p \rangle^{fi}) = u_{\sigma_p(g)\,(i)}/\langle p \rangle^{fi}$.

The following two propositions are from [**9**]:

PROPOSITION 1.1. *Let $a, b \in B$. Then $a = b$ iff for every $p \in \mathrm{Ult}\, C$, $a/\langle p \rangle^{fi} = b/\langle p \rangle^{fi}$.*

PROPOSITION 1.2. *Let $p \in \mathcal{F}_k^B \subset \mathrm{Ult}\, C$. There exists $c \subset \mathcal{F}_k^B$, such that for all $q \in c$, $\sigma_q = \sigma_p$. For c we also have that for every $i \leq k$ and every $g \in G$, $g(cu_i) = cu_{\sigma(i)}$.*

PROPOSITION 1.3. *Let $B = C(v_1, \ldots, v_n)$ be a pseudo-Galois extension of C and $G < \mathrm{Aut}_C B$ a group of relatively-strongly distinct automorphisms, such that $\mathrm{Fix} G = C$. Then, for $k \leq m$ and $p \in \mathcal{F}_k^B$, $\sigma_p(G)$ is a transitive subgroup of S_k.*

Proof. Let $\langle u_1, \dots, u_n\rangle$, $n \le m$, be the generating set for B over C, constructed in the proof of Theorem 0.1 i.e. having the properties from the note following the theorem. Let also, $a_k = \mathcal{F}_k^B$, $k \le n$, and let G be a finite subgroup of $\mathrm{Aut}_C B$, consisting of relatively-strongly distinct automorphisms. If $a_1 = 1$, then $B = C$ and $h(p) = 1$. Otherwise, there exists k, $2 \le k \le n$, such that $a_k \ne 0$. Let us prove $a_1 = 0$ first. Since $a_1 \le u_1$, $\forall g, h \in G\ \forall x \in B\ g(x)a_1 = h(x)a_1$. Really, if $x = \sum_{i \le n} c_i u_i$, then for every $g \in G$, $g(x)a_1 = g(xa_1) = g(c_1a_1) = c_1a_1$. The result does not depend on g, i.e. it is a constant. Since the automorphisms from G are relatively-strongly distinct, $a_1 = 0$. Let $c \subset a_k$ be the set from Proposition 1.2. The mapping $\sigma_p : G \to S_k$ is an embedding. It is a homomorphism, since $\rho_g^p \circ \rho_h^p = \rho_{gh}^p$. Let us check that it is 1–1. Let $g \ne h$ and $\sigma_p(g) = \sigma_p(h)$. Then $\rho_g^p = \rho_h^p$. Let $x \in B$, $x = \sum_{i \le n} c_i u_i$. We have:

$$g(c)x = g(cx) = g(\sum_{i\le k} cc_iu_i) = \sum_{i\le k} c_i g(cu_i) = \sum_{i\le k} cc_iu_{\sigma(g)(i)}$$
$$= \sum_{i\le k} cc_iu_{\sigma(h)(i)} = h(cx) = h(c)x.$$

Since x was arbitrary, and $c \in C$, g and h are not relatively-strongly distinct. Contradiction.

Now we prove that $\sigma_p(G)$ is a transitive subgroup of S_k. Suppose contrary. Then none of the orbits is the whole set $\{1, \dots, k\}$. Consider an orbit F. Then for $x = \sum_{i\in F} cu_i$ and arbitrary $g \in G$, we have:

$$g(x) = \left(\sum_{i\in F} cu_i\right) = c\sum_{i\in F} g(u_i) = c\sum_{i\in F} u_{\rho(g)(i)} = c\sum_{i\in F} u_i = x$$

Henceforth, $x \in \mathrm{Fix}G$. On the other hand, for $p \in \mathrm{Ult}\, C$, $x/\langle p\rangle^{fi} = \sum_{i\in F} u_i/\langle p\rangle^{fi}$ is neither 0 nor 1 (in B_p), since F is neither empty nor the whole set $\{1, \dots, k\}$. Henceforth, $x \in B \setminus C$. Contradiction.

THEOREM 1.4. *Let B be a relatively complete extension of Boolean algebra C, with the height sequence $(n_1, \dots, n_k)$. The following are equivalent:*

(i) *B is a pseudo-Galois extension of C.*

(ii) *There exists a group G which transitively embedes into permutation groups $S_{n_1}, \dots, S_{n_k}$.*

(iii) *There exist irreducible polynomials of powers $n_1, \dots, n_k$, with the same Galois group.*

Proof. The equivalence between (ii) and (iii), follows from the well known correspondence in Galois theory, between irreducible polynomials and transitive subgroups of permutation groups (Theorem. 4.14 in [**3**]). We will prove that (i) and (ii) are equivalent.

(i) $\Rightarrow$ (ii) is just Proposition 1.3, so we are left with the proof of (ii) $\Rightarrow$ (i). Suppose that G is a group having properties from (ii). Let also, for $i \in \{n_1, \dots, n_k\}$,

$\rho_i : G \to S_i$ be transitive embedings. For $g \in G$, let us define $\varphi = h(g) \in \mathrm{Aut}_C B$ in the following way: we will define $\varphi(x)$, for $x \leq a_i$, $i \in \{n_1, \dots, n_k\}$ first. If $x = \sum_{j \leq n} c_j \cdot u_j = \sum_{j \leq i} c_j \cdot u_j$ ($a_i \cdot u_j = 0$ for $j > i$), then $\varphi(x) = \sum_{j \leq i} c_j \cdot u_{\rho_i(g)\,(j)}$. Actually, it is the automorphism that maps $C|(a_i)$ indenticly onto itself, and $u_j \cdot a_i$ to $u_{\rho_i(g)\,(j)} \cdot a_i$, for $j \leq i$. This automorphism exists by the Sikorsky exstension criterion. Let x be arbitrary element of B. If $x = \sum_{i \in S} d_i \cdot a_i$, then for $S = \{n_1, \dots, n_k\}$ we define $\varphi(x) = \sum_{i \in S} \varphi(d_i \cdot a_i)$. We will prove that $H = \{h(g) | g \in G\}$ is a subgroup of $\mathrm{Aut}_C B$ such that $\mathrm{Fix} H = C$ and that the memebers of H are relatively-strongly distinct.

$H < \mathrm{Aut}_C B$ since it is isomorphic to G. Really, h is a homomorphism since $h(g \cdot k)(u_j \cdot a_i) = u_{\rho_i(g \cdot k)\,(j)} \cdot a_i = u_{(\rho_i(g) \circ \rho_i(k))\,(j)} \cdot a_i = (h(g) \circ h(k))\,(u_j \cdot a_i)$. Since they also agree on C, we have $h(g \cdot k) = h(g) \circ h(k)$. It is also easy to see that h is a bijection.

We now prove that $\mathrm{Fix} H = C$. First $C \subset \mathrm{Fix} H$ by definition. On the other hand, let $x \in \mathrm{Fix} H \setminus C$. Since $x \neq 0$, $x \cdot a_i \neq 0$, for some $i \in \{n_1, \dots, n_k\}$, and $x \cdot a_i \in \mathrm{Fix} H$. Therefore we can assume, without loss of generality, that $x \leq a_i$ for some $i \in S$. Let $x = \sum_{j \leq i} c_j \cdot u_j$. Let us note first, that nonzero elements among $\{c_1, \dots, c_i\}$ are equal. Suppose not. Then for some $k, l \leq i$, $d = c_k \cdot -c_l$. Let $g \in G$ be an element such that $\rho_i(g)\,(l) = k$. Then, $d \cdot u_k \leq x$, but $d \cdot u_k \cdot h(g)\,(x) = d \cdot u_k \cdot \sum_{j \leq i} c_j \cdot u_{\rho_i(g)\,(j)} = d \cdot u_k \cdot c_l \cdot u_k = 0$, contradicting the assumption $h(g)\,(x) = x$. Therefore, we have $x = \sum_{j \in T} c \cdot u_j$, for some $T \subset \{1, \dots, i\}$, $c \leq a_i$. If T was the whole set $\{1, \dots, i\}$, we would have $x / \langle p \rangle^{fi} = 1$, for every $p \in C$, and further $x = c \in C$, contrary to our assumption. Henceforth, we conclude that $C \neq \{1, \dots, i\}$. But now we have for every $g \in G$, that $h(g)\,(x) = \sum_{j \in T} c \cdot u_{\rho_i(g)\,(j)} = \sum_{j \in \rho_i(g)\,[T]} c \cdot u_j = x$. This means that $\tau[T] = T$, for every $\tau \in \rho_i[G]$, i.e. T is an orbit of $\rho_i[G]$ different from the whole set $\{1, \dots, i\}$, contradicting the fact that $\rho_i[G]$ is a transitive subgroup of S_i. This contradiction proves that $\mathrm{Fix} H = C$.

Finally, we show that the automorphisms from H are strongly distinct. So let $\varphi, \psi \in H$, $\varphi \neq \psi$, $\varphi = h(g)$, $\psi = h(k)$, for some $h, k \in G$. Let also $c \in C$, $c \neq 0$. Since $c \cdot a_i \neq 0$, for some $i \in \{n_1, \dots, n_k\}$, without loss of generality, we can assume that $c \leq a_i$, for some $i \in \{n_1, \dots, n_k\}$. Let $j \leq i$ be a number such that $\rho_i(g)\,(j) \neq \rho_i(k)\,(j)$. Then, $\varphi(c \cdot a_i \cdot u_j) = a_i \cdot u_{\rho_i(g)\,(j)} \neq a_i \cdot u_{\rho_i(k)\,(j)} = \psi(c \cdot a_i \cdot u_j)$, hence $c \cdot \varphi(a_i \cdot u_j) \neq c \cdot \psi(a_i \cdot u_j)$. This proves that φ and ψ are relatively-strongly distinct. This ends the proof of our theorem. ■

Unfortunately, we are not able to simplify this characterization, and we pose this as a question.

Question 1. What is a necessary and sufficient condition,given an increasing sequence $(n_1, \dots, n_k)$, for the existence of a group G which transitively embeds into $S_{n_1}, \dots, S_{n_k}$.

Even the simplest case of the above question seems unclear to us. We pose it as a separate question.

Question 2. Let $m < n \in N$. When S_m transitively embedes into S_n?

Relevant to this question could be the following known facts.

PROPOSITION 1.5. (i) *Let $G < S_n$, so that $n < |G|$. Then G is transitive iff the subgroup $G_1 = \{f \in G : f(1) = 1\}$ (the stabilizer of 1), is of index n in G.*

(ii) *If S_m contains a subgroup H of index n, then there exists a transitive embedding of S_m into S_n so that H is the stabilizer of 1.*

(iii) *Let $\{p_i | i \in I\}$ be a family of integers, $\sum \rho_i = m$ and x the set of partitions $\langle F_i \rangle_{i \in I}$ such that $|F_i| = p_i$. Then S_m acts transitively on X, and $|X| = m!/\prod_{i \in I} p_i$.*

From the first two facts we see that our question is equivalent to the question of existence of a subgroup of S_m of a given index n. A necessary condition is $n|m!$. (iii) gives a sufficient condition. We could give some partial answers to this question, like giving examples showing that for the pairs $(3,6)$, $(4,6)$, $(5,10)$, $(m, m!/2m)$ for $m > 4$, such embedings do exist, but we cannot answer the question completely.

REFERENCES

[1] N. Bourbaki, *Algebra*, Addison Wesley, Reading Massachusets, 1974

[2] N. Božović and Ž. Mijajlović, *Uvod u teoriju grupa*, Naučna knjiga, Beograd, 1982

[3] N. Jacobson, *Basic Algebra I*, Freeman, San Francisko, 1982

[4] S. Koppelberg, *On Boolean algebras with distinguished subalgebras*, Enseign. Math **28** (1982), 233–252

[5] S. Koppelberg, *Projective Boolean algebras*, in: D. Monk, ed., *Handbook of Boolean algebras, vol. 3*, North Holand, Amsterdam, 1989, pp. 741–775

[6] D. Monk, *Automorphism groups*, in: D. Monk, ed., *Handbook of Boolean Algebras, vol. 2*, North Holand, Amsterdam, 1989, pp. 517–546

[7] Ž. Perović, *Relatively complete 2-extensions of Boolean algebras*, Mathematica Balkanica **6**(2), (1992), 125–128.

[8] Ž. Perović, *Relatively complete finite extensions of Boolean algebras*, Zbornik radova Fil.fak. u Nišu **5** (1992) 169–174.

[9] Ž. Perović, *Galois extensions of Boolean algebras*, (to appear)

Filozofski fakultet
18000 Niš
Jugoslavija

(Received 26 09 1992)