BASICS OF CLONE THEORY
DRAFT

ERHARD AICHINGER

Abstract. Some well known facts on clones are collected (cf. [PK79, Sze86, Maš10]).

Contents

1. Definition of clones

Let A be a nonempty set. Then $\mathcal{O}(A) := \bigcup\{A^{A^n} \mid n \in \mathbb{N}\}$ is the set of finitary operations on A. For $\mathcal{C} \subseteq \mathcal{O}(A)$ and $m \in \mathbb{N}$, we let $\mathcal{C}^{[m]}$ be the functions in $\mathcal{C}$ with arity m. For $n \in \mathbb{N}$ and $j \in \{1, \ldots, n\}$, the function $\pi_j^{(n)} : A^n \to A$ is

Date: June 21, 2011.

Course material for the course “Universal Algebra”, JKU Linz, Summer term 2011.

defined by $\pi_j^{(n)}(x_1, \dots, x_n) := x_j$ for all $x_1, \dots, x_n \in A$. For $n \in \mathbb{N}$, a subset R of A^n is also called a *n-ary relation on A*, and for any set I, a subset of A^I is also called a *relation on A indexed by I*. Let $v \in A^I$. Then we will denote v also by $\langle v(i) \mid i \in I \rangle$. The expression $\langle v(i) \mid i \in I \rangle$ can also be seen as a shorthand for $\{(i, v(i)) \mid i \in I\}$. For $m, n \in \mathbb{N}$, $f \in \mathcal{O}(A)^{[n]}$, and $g_1, \dots, g_n \in \mathcal{O}(A)^{[m]}$, $f(g_1, \dots, g_n)$ denotes the function $\langle f(g_1(x), \dots, g_n(x)) \mid x \in A^m \rangle$.

Definition 1.1 (Clone)**.** Let A be a set, $J \neq \emptyset$, $\mathcal{C} \subseteq \mathcal{O}(A)$. $\mathcal{C}$ is a *clone on A* if

(1) for all $n, j \in \mathbb{N}$ with $j \leq n$, we have $\pi_j^{(n)} \in \mathcal{C}$;
(2) for all $n, m \in \mathbb{N}$, for all $f \in \mathcal{C}^{[n]}$ and for all $g_1, \dots, g_n \in \mathcal{C}^{[m]}$, we have $f(g_1, \dots, g_n) \in \mathcal{C}^{[m]}$.

Proposition 1.2. *Let A be a set, and let all $\mathcal{C}_j$ ($j \in J$) be clones on A. Then $\bigcap\{\mathcal{C}_j \mid j \in J\}$ is a clone on A.*

Proof: It can be seen from Definition 1.1 that the properties carry over to arbitrary intersections. □

2. Polymorphisms and invariant relations

Definition 2.1 (Preservation of a relation)**.** Let A and I be nonempty sets, let $f : A^n \to A$, and let $R \subseteq A^I$. We say that f *preserves* R if for all $v_1, \dots, v_n \in R$, we have $\langle f(v_1(i), \dots, v_n(i)) \mid i \in I \rangle \in R$. Then R *is invariant under* f, and we write $f \rhd R$. We also say that f *is a polymorphism of the relational structure* $(A; R)$ and that f *is compatible with* R.

Using the terminology of universal algebra, we see that an operation f preserves $R \subseteq A^I$ if and only if R is a subuniverse of $\langle A, f \rangle^I$. From a relation that is invariant under f, other invariant relations can be constructed in the following ways.

Definition 2.2. Let A, I, J be nonempty sets, let $R \subseteq A^J$, and let σ be a function from I to J. Then $R * \sigma$ is a subset of A^I defined by $R * \sigma := \{v \circ \sigma \mid v \in R\}$.

Definition 2.3. Let A be a nonempty set, let I, J be sets, let $S \subseteq A^J$, and let $\sigma : J \to I$. Then $(S : \sigma)_I$ is the subset of A^I defiuned by $(S : \sigma)_I := \{g \in A^I \mid g \circ \sigma \in S\}$.

Lemma 2.4. *Let A, I, J be nonempty sets, let $R \subseteq A^J$, let $\sigma : I \to J$ and $\tau : J \to I$. Let $f \in \mathcal{O}(A)$ be such that $f \rhd R$. Then $f \rhd R * \sigma$ and $f \rhd (R : \tau)_I$.*

Proof: Let n be the arity of f, and let $w_1, \ldots, w_n \in R * \sigma$. We have to show $\langle f(w_1(i), \ldots, w_n(i)) \mid i \in I \rangle \in R * \sigma$. Let $k \in \{1, \ldots, n\}$. Since $w_k \in R * \sigma$, there is $v_k \in R$ such that $w_k = v_k \circ \sigma$. Now we have to show

$$\langle f(v_1(\sigma(i)), \ldots, v_n(\sigma(i))) \mid i \in I \rangle \in R * \sigma. \tag{2.1}$$

Let $g := \langle f(v_1(j), \ldots, v_n(j)) \mid j \in J \rangle$. Since $v_1, \ldots, v_n \in R$, $f \rhd R$ implies that $g \in R$. Therefore, $g \circ \sigma \in R * \sigma$. We have

$$g \circ \sigma = \langle f(v_1(\sigma(i)), \ldots, v_n(\sigma(i))) \mid i \in I \rangle.$$

Thus, since $g \circ \sigma \in R * \sigma$, (2.1) holds, which completes the proof of $f \rhd R * \sigma$.

For proving $f \rhd (S : \tau)_I$, we let $g_1, \ldots, g_n \in (S : \tau)_I$. We have to show $\langle f(g_1(i), \ldots, g_n(i)) \mid i \in I \rangle \in (S : \tau)_I$. To this end, we show

$$\langle f(g_1(i), \ldots, g_n(i)) \mid i \in I \rangle \circ \tau \in S. \tag{2.2}$$

We have $\langle f(g_1(i), \ldots, g_n(i)) \mid i \in I \rangle \circ \tau = \langle f(g_1 \circ \tau(j), \ldots, g_n \circ \tau(j)) \mid j \in J \rangle$. Since $g_1 \circ \tau \in S, \ldots, g_n \circ \tau \in S$, the fact that $f \rhd S$ implies $\langle f(g_1 \circ \tau(j), \ldots, g_n \circ \tau(j)) \mid j \in J \rangle \in S$, which implies (2.2). ☐

If I is a finite set, a relation $R \subseteq A^I$ can therefore often be replaced with a relation R' on A^m, where $m := |I|$.

For a nonempty set A, we let $\mathcal{R}(A) := \bigcup_{n \in \mathbb{N}} \mathcal{P}(A^n)$ be the set of all finitary relations on A that are indexed by an initial section of the natural numbers. We will write $\underline{n}$ for the set $\{1, \ldots, n\}$. As is usual, the set A^n is understood to be the same set as $A^{\underline{n}}$. For $\mathcal{R} \subseteq \mathcal{R}(A)$, we let $\mathcal{R}^{[n]} := \{R \in \mathcal{R} \mid R \subseteq A^n\}$. We note that the $\mathcal{R}^{[n]}$ need not be disjoint, since each of them might contain $\emptyset$.

Definition 2.5. Let $m \in \mathbb{N}$, let A be a nonempty set, and let $\mathcal{F} \subseteq \mathcal{O}(A)$. We define $\mathsf{Inv}^{[m]}(\mathcal{F}) := \{R \subseteq A^m \mid \forall f \in \mathcal{F} : f \rhd R\}$, and $\mathsf{Inv}(\mathcal{F}) := \bigcup\{\mathsf{Inv}^{[m]}(\mathcal{F}) \mid m \in \mathbb{N}\}$.

Definition 2.6. Let $m \in \mathbb{N}$, let A, I be nonempty sets, and let $R \subseteq A^I$. Then $\mathsf{Pol}^{[m]}(\{R\}) := \{f : A^m \to A \mid f \rhd R\}$. If I_j ($j \in J$ with $j \neq \emptyset$) are sets, $R_j \subseteq A^{I_j}$ for $j \in J$, and $\mathcal{R} := \{R_j \mid j \in J\}$, then we define $\mathsf{Pol}^{[m]}(\mathcal{R}) := \bigcap\{\mathsf{Pol}^{[m]}(\{R\}) \mid R \in \mathcal{R}\}$. Furthermore, $\mathsf{Pol}(\mathcal{R}) := \bigcup\{\mathsf{Pol}^{[m]}(\mathcal{R}) \mid m \in \mathbb{N}\}$.

Theorem 2.7. *Let A be a set, let $\mathcal{R}, \mathcal{R}_1, \mathcal{R}_2$ be sets of finitary relations on A, and let $\mathcal{F}, \mathcal{F}_1, \mathcal{F}_2$ be sets of finitary operations on A. Then we have:*

(1) $\mathcal{R}_1 \subseteq \mathcal{R}_2 \Rightarrow \mathsf{Pol}(\mathcal{R}_2) \subseteq \mathsf{Pol}(\mathcal{R}_1)$.
(2) $\mathcal{F}_1 \subseteq \mathcal{F}_2 \Rightarrow \mathsf{Inv}(\mathcal{F}_2) \subseteq \mathsf{Inv}(\mathcal{F}_1)$.
(3) $\mathcal{F} \subseteq \mathsf{Pol}(\mathsf{Inv}(\mathcal{F}))$.
(4) $\mathcal{R} \subseteq \mathsf{Inv}(\mathsf{Pol}(\mathcal{R}))$.
(5) $\mathsf{Pol}(\mathsf{Inv}(\mathsf{Pol}(\mathcal{R}))) = \mathsf{Pol}(\mathcal{R})$.
(6) $\mathsf{Inv}(\mathsf{Pol}(\mathsf{Inv}(\mathcal{F}))) = \mathsf{Inv}(\mathcal{F})$.

Proof: (1) Let $f \in \mathsf{Pol}(\mathcal{R}_2)$, and let $R \in \mathcal{R}_1$. Then $R \in \mathcal{R}_2$, and since $f \in \mathsf{Pol}(\mathcal{R}_2)$, we have $f \rhd R$.

(2) Let $R \in \mathsf{Inv}(\mathcal{F}_2)$, and let $f \in \mathcal{F}_1$. Then $f \in \mathcal{F}_2$, and since $R \in \mathsf{Inv}(\mathcal{F}_2)$, we have $f \rhd R$.

(3) Let $f \in \mathcal{F}$. To prove that $f \in \mathsf{Pol}(\mathsf{Inv}(\mathcal{F}))$, we let $R \in \mathsf{Inv}(\mathcal{F})$. Then since $f \in \mathcal{F}$, we have $f \rhd R$. Hence we have $f \in \mathsf{Pol}(\mathsf{Inv}(\mathcal{F}))$.

(4) Let $R \in \mathcal{R}$. To prove that $R \in \mathsf{Inv}(\mathsf{Pol}(\mathcal{R}))$, we let $f \in \mathsf{Pol}(\mathcal{R})$. Since $R \in \mathcal{R}$, we have $f \rhd R$. Hence we have $R \in \mathsf{Inv}(\mathsf{Pol}(\mathcal{R}))$.

(5) By item (4), we have $\mathcal{R} \subseteq \mathsf{Inv}(\mathsf{Pol}(\mathcal{R}))$, and therefore by item (1) the inclusion $\mathsf{Pol}(\mathsf{Inv}(\mathsf{Pol}(\mathcal{R}))) \subseteq \mathsf{Pol}(\mathcal{R})$ holds. The other inclusion follows from (3) by setting $\mathcal{F} := \mathsf{Pol}(\mathcal{R})$.

(6) By item (3), we have $\mathcal{F} \subseteq \mathsf{Pol}(\mathsf{Inv}(\mathcal{F}))$, and therefore by item (2) the inclusion $\mathsf{Inv}(\mathsf{Pol}(\mathsf{Inv}(\mathcal{F}))) \subseteq \mathsf{Inv}(\mathcal{F})$ holds. The other inclusion follows from item (4) by setting $\mathcal{R} := \mathsf{Inv}(\mathcal{F})$. $\square$

3. The invariant relations encode the functions in a clone

Lemma 3.1. *Let $\mathcal{C}$ be a clone on the set A, let $m \in \mathbb{N}$, let $f \in \mathcal{C}^{[m]}$, and let R be the subset of A^{A^n} defined by $R := \mathcal{C}^{[n]}$. Then $f \rhd R$.*

Proof: Let $g_1, \ldots, g_m \in R$. Since $g_1, \ldots, g_m \in \mathcal{C}^{[n]}$ and $f \in \mathcal{C}^{[m]}$, we have $f(g_1, \ldots, g_m) \in \mathcal{C}^{[n]}$, and hence $f(g_1, \ldots, g_m) \in R$. Now $f(g_1, \ldots, g_m) = \langle f(g_1(i), \ldots, g_m(i)) \mid i \in A^n \rangle$. Therefore, the last expression lies in R, which completes the proof of $f \rhd R$. $\square$

Theorem 3.2. *Let $\mathcal{C}$ be a clone on the set A, let $n \in \mathbb{N}$, and let $f : A^n \to A$, and let R be the subset of A^{A^n} defined by $R := \mathcal{C}^{[n]}$. Then the following are equivalent:*

(1) $f \in \mathcal{C}$;
(2) $f \rhd R$;

If A is finite and $m := |A|^n$, then each of these properties is furthermore equivalent to

(3) $f \in \mathsf{Pol}(\mathsf{Inv}^{[m]}(\mathcal{C}))$.

Proof: (1)⇒(2): This follows from Lemma 3.1.

(2)⇒(1): We know that $\pi_1^{(n)} \in R, \ldots, \pi_n^{(n)} \in R$. Since $f \rhd R$, we have $\langle f(\pi_1^{(n)}(i), \ldots, \pi_n^{(n)}(i)) \mid i \in A^n\rangle \in R$, and hence $f(\pi_1^{(n)}, \ldots, \pi_n^{(n)}) \in R$. Therefore $f \in R$, which means $f \in \mathcal{C}^{[n]}$.

(1)⇒(3): By Theorem 2.7 (3), we have $\mathcal{C} \subseteq \mathsf{Pol}(\mathsf{Inv}(\mathcal{C}))$. Since $\mathsf{Inv}^{[m]}(\mathcal{C}) \subseteq \mathsf{Inv}\,(\mathcal{C})$, item (1) of Theorem 2.7 yields $\mathsf{Pol}(\mathsf{Inv}(\mathcal{C})) \subseteq \mathsf{Pol}(\mathsf{Inv}^{[m]}(\mathcal{C}))$.

(3)⇒(2): From Lemma 3.1, we know that for all functions $c \in \mathcal{C}$, we have $c \rhd R$. Now let π be a bijective map from $\{1, \ldots, m\}$ to A^n, and let $R' := R * \pi = \{r \circ \pi \mid r \in R\}$. The relation R' is a subset of A^m. By Lemma 2.4, we have $c \rhd R'$ for all $c \in \mathcal{C}$. Therefore, $R' \in \mathsf{Inv}^{[m]}(\mathcal{C})$. Since $f \in \mathsf{Pol}(\mathsf{Inv}^{[m]}(\mathcal{C})$, we have $f \rhd R'$. Now $R = \{f \circ \pi^{-1} \mid f \in R'\}$, and thus Lemma 2.4 yields that $f \rhd R$. □

4. The clones of the form $\mathsf{Pol}(\mathcal{R})$

Proposition 4.1. *Let A, I be sets, and let $R \subseteq A^I$. Then $\mathsf{Pol}(\{R\})$ is a clone on A.*

Proof: Let $n, j \in \mathbb{N}$ be such that $i \leq n$. We first show that $\pi_j^{(n)}$ lies in $\mathsf{Pol}(\{R\})$. To this end, let $v_1, \ldots, v_n \in R$. We have to show

$$\langle \pi_j^{(n)}(v_1(i), \ldots, v_n(i)) \mid i \in I\rangle \in R. \tag{4.1}$$

We have $\langle \pi_j^{(n)}(v_1(i), \ldots, v_n(i)) \mid i \in I\rangle = \langle v_j\,(i) \mid i \in I\rangle = v_j$. Since $v_j \in R$, (4.1) is proved.

Now let $n, m \in \mathbb{N}$, and let $g_1, \ldots, g_n \in A^{A^m}, f \in A^{A^n}$ such that all functions $g_1, \ldots, g_m, f$ preserve R. Now let $v_1, \ldots, v_m \in R$. For each $j \in \{1, \ldots, n\}$, we have $g_j \rhd R$, and therefore

$$w_j := \langle g_j\big(v_1(i), \ldots, v_m(i)\big) \mid i \in I\rangle \in R.$$

Since $f \rhd R$, we have $\langle f(w_1(i), \ldots, w_n(i)) \mid i \in I\rangle \in R$, and hence $\langle f\big(g_1(v_1(i), \ldots, v_m(i)), \ldots, g_n(v_1(i), \ldots, v_m(i))\big) \mid i \in I\rangle \in R$. Hence

$$\langle f(g_1, \ldots, g_n)\,\big(v_1(i), \ldots, v_m(i)\big) \mid i \in I\rangle \in R,$$

and thus $\mathsf{Pol}(\{R\})$ is closed under composition. □

Theorem 4.2. *Let A be a finite set, and let $\mathcal{C}$ be a clone on A. Then $\mathcal{C} = \mathsf{Pol}(\mathsf{Inv}(\mathcal{C}))$.*

Proof: The inclusion $\subseteq$ is a consequence of Theorem 2.7. For the other inclusion, let $f \in \mathsf{Pol}(\mathsf{Inv}(\mathcal{C}))$. Let n be the arity of f, and let $m := |A|^n$. Then $\mathsf{Inv}^{[m]}(\mathcal{C}) \subseteq \mathsf{Inv}(\mathcal{C})$, and thus by Theorem 2.7 (1), we have $f \in \mathsf{Pol}(\mathsf{Inv}^{[m]}(\mathcal{C})$. Now from Theorem 3.2, we obtain $f \in \mathcal{C}$. □

Corollary 4.3. *Let A be a finite set, and let $\mathcal{F}$ be a subset of $\mathcal{O}(A)$. Then $\mathsf{Pol}(\mathsf{Inv}(\mathcal{F}))$ is a clone, and for every clone $\mathcal{D}$ with $\mathcal{F} \subseteq \mathcal{D}$, we have $\mathsf{Pol}(\mathsf{Inv}(\mathcal{F})) \subseteq \mathcal{D}$.*

Proof: From Propositions 4.1 and 1.2, we obtain that $\mathsf{Pol}(\mathsf{Inv}(\mathcal{F}))$ is a clone. Now let $\mathcal{D}$ be a clone containing all functions from $\mathcal{F}$. Then from items (1) and (2) of Theorem 2.7, we obtain $\mathsf{Pol}(\mathsf{Inv}(\mathcal{F})) \subseteq \mathsf{Pol}(\mathsf{Inv}(\mathcal{D}))$. By Theorem 4.2, we have $\mathsf{Pol}(\mathsf{Inv}(\mathcal{D})) = \mathcal{D}$, hence $\mathsf{Pol}(\mathsf{Inv}(\mathcal{F})) \subseteq \mathcal{D}$. □

5. How the functions in a clone encode the invariant relations

Theorem 5.1. *Let A be a nonempty set, let $\mathcal{C}$ be a clone on A, let $n, t \in \mathbb{N}$, and let S be a subset of A^t with $S \in \mathsf{Inv}^{[t]}(\mathcal{C}^{[n]})$. We assume that S is n-generated as a subuniverse of $\langle A, \mathcal{C}^{[n]}\rangle^t$. Then there exists $\sigma : \{1, \ldots, t\} \to A^n$ such that $S = \mathcal{C}^{[n]} * \sigma$. Furthermore, we then have $S \in \mathsf{Inv}(\mathcal{C})$.*

Proof: Let $s_1, \ldots, s_n \in S$ such that the subuniverse of $\langle A, \mathcal{C}^{[n]}\rangle^t$ that is generated by $\{s_1, \ldots, s_n\}$ is equal to S. We define $\sigma : \{1, \ldots, t\} \to A^n$ by

$$\sigma(r)\,(i) := s_i(r)$$

for $r \in \{1, \ldots, t\}$, $i \in \{1, \ldots, n\}$. We will now prove

$$S = \mathcal{C}^{[n]} * \sigma. \tag{5.1}$$

For $\subseteq$, we first show that all s_i are elements of $\mathcal{C}^{[n]} * \sigma$. To this end, let $i \in \{1, \ldots, n\}$. Let us now compute $\pi_i^{(n)} \circ \sigma$. This is a function from $\{1, \ldots, t\}$ to A, and for $r \in \{1, \ldots, t\}$, we have $\pi_i^{(n)}(\sigma(r)) = \pi_i^{(n)}(\sigma(r)(1), \ldots, \sigma(r)(n)) = \sigma(r)\,(i) = s_i(r)$. Hence $\pi_i^{(n)} \circ \sigma = s_i$. Thus s_i lies in $\mathcal{C}^{[n]} * \sigma$. By Lemma 2.4, $\mathcal{C}^{[n]} * \sigma$ is a subuniverse of $\langle A, \mathcal{C} \rangle$. Therefore, it is also a subuniverse of the reduct $\langle A, \mathcal{C}^{[n]} \rangle$ of $\langle A, \mathcal{C} \rangle$. Thus we have $S \subseteq \mathcal{C}^{[n]} * \sigma$.

To prove $\supseteq$ of (5.1), we let $f \in \mathcal{C}^{[n]}$ and consider

$$\begin{aligned} g := f \circ \sigma &= \langle f \circ \sigma(r) \mid r \in \{1, \ldots, t\} \rangle \\ &= \langle f(\sigma(r)) \mid r \in \{1, \ldots, t\} \rangle \\ &= \langle f(\sigma(r)\,(1), \ldots, \sigma(r)\,(n)) \mid r \in \{1, \ldots, t\} \rangle \\ &= \langle f(s_1(r), \ldots, s_n(r)) \mid r \in \{1, \ldots, t\} \rangle. \end{aligned} \tag{5.2}$$

We know that $s_1, \ldots, s_n \in S$. Since $f \in \mathcal{C}^{[n]}$ and $S \in \mathsf{Inv}(\mathcal{C}^{[n]})$, we have that $f \rhd S$. Hence the last expression of (5.2) is an element S. Therefore $f \circ \sigma \in S$, which completes the proof of (5.1).

By Lemma 3.1, we know that $\mathcal{C}^{[n]}$ is invariant under all operations in $\mathcal{C}$. Hence by Lemma 2.4, $S = \mathcal{C}^{[n]} * \sigma$ is invariant under all operations in $\mathcal{C}$. Thus $S \in \mathsf{Inv}(\mathcal{C})$. ☐

Corollary 5.2. *Let A be a nonempty set, let $\mathcal{C}$ be a clone on A, let $t \in \mathbb{N}$, let S be a finite subset of A^t, and let $n := |S|$. Then the following are equivalent:*

(1) $S \in \mathsf{Inv}(\mathcal{C}^{[n]})$.
(2) *There exists $\sigma : \{1, \ldots, t\} \to A^n$ such that $S = \mathcal{C}^{[n]} * \sigma$.*
(3) $S \in \mathsf{Inv}(\mathcal{C})$.

Proof: (1)⇒(2): Since $|S| = n$, S is n-generated as a subuniverse of $\langle A, \mathcal{C}^{[n]} \rangle^t$. Hence by Theorem 5.1, there is a $\sigma : \{1, \ldots, t\} \to A^n$ such that $S = \mathcal{C}^{[n]} * \sigma$. (2)⇒(3): By Lemma 3.1, we know that $\mathcal{C}^{[n]}$ is invariant under all operations in $\mathcal{C}$. Hence by Lemma 2.4, $S = \mathcal{C}^{[n]} * \sigma$ is invariant under all operations in $\mathcal{C}$. Thus $S \in \mathsf{Inv}(\mathcal{C})$. (3)⇒(1): This follows from Theorem 2.7 (2). ☐

Corollary 5.3. *Let A be a nonempty set, let $\mathcal{C}$ be a clone, and let $m, n, t \in \mathbb{N}$. We assume that $m \le n$, $S \in \mathsf{Inv}(\mathcal{C}^{[n]})$, and that S is n-generated as a subuniverse of $\langle A, \mathcal{C}^{[m]} \rangle^t$. Then $S \in \mathsf{Inv}(\mathcal{C})$.*

Proof: Since S is n-generated as a subuniverse of $\langle A, \mathcal{C}^{[m]} \rangle^t$ and $m \le n$, S is also n-generated as a subuniverse of $\langle A, \mathcal{C}^{[n]} \rangle^t$. Thus by Theorem 5.1, there is a $\sigma : \{1, \ldots, t\} \to A^n$ such that $S = \mathcal{C}^{[n]} * \sigma$. Now by Lemma 3.1 and Lemma 2.4, every $f \in \mathcal{C}$ preserves S. □

6. Properties of the lattice of all clones

Definition 6.1. Let A be a nonempty set, and let $\mathcal{F}$ be a subset of $\mathcal{O}(A)$. Then $\mathsf{Clone}(\mathcal{F})$ denotes the smallest clone $\mathcal{C}$ on A with $\mathcal{F} \subseteq \mathcal{C}$.

By Corollary 4.3, for a finite set A, we have $\mathsf{Clone}(\mathcal{F}) = \mathsf{Pol}(\mathsf{Inv}(\mathcal{F}))$.

Definition 6.2. Let A be a nonempty set, and let $\mathcal{C}$ be a clone on A. The clone $\mathcal{C}$ is *finitely generated* if there is a finite subset $\mathcal{F}$ of $\mathcal{C}$ with $\mathsf{Clone}(\mathcal{F}) = \mathcal{C}$. the clone $\mathcal{C}$ is *finitely related* if there is a finite set $\mathcal{R} \subseteq \mathcal{R}(A)$ such that $\mathcal{C} = \mathsf{Pol}(\mathcal{R})$.

For a nonempty set A, let $\mathbf{C}(A)$ be the set of clones on A. For $\mathcal{C}, \mathcal{D} \in \mathbf{C}(A)$, we write $\mathcal{C} \le \mathcal{D}$ if $\mathcal{C} \subseteq \mathcal{D}$, $\mathcal{C} < \mathcal{D}$ if $\mathcal{C} \le \mathcal{D}$ and $\mathcal{C} \ne \mathcal{D}$, and $\mathcal{C} \prec \mathcal{D}$ if $\mathcal{C} < \mathcal{D}$ and there is no clone $\mathcal{E}$ with $\mathcal{C} < \mathcal{E} < \mathcal{D}$.

Theorem 6.3. *Let A be a finite nonempty set, and let $\mathcal{C}$ be a finitely generated clone on A. Let $N \in \mathbb{N}$ be such that $\mathcal{C} = \mathsf{Clone}(\mathcal{C}^{[N]})$. Then we have:*

1. *$S(\mathcal{C}) := \{\mathcal{D} \in \mathbf{C}(A) \mid \mathcal{D} \prec \mathcal{C}\}$ is finite (and has at most $2^{|A|^{|A|^N}}$ elements).*
2. *For all $\mathcal{E} \in \mathbf{C}(A)$ with $\mathcal{E} < \mathcal{C}$ there is a $\mathcal{D} \in S(\mathcal{C})$ such that $\mathcal{E} \le \mathcal{D}$.*

Proof: Let $S_0(\mathcal{C}) := \{\mathcal{C} \cap \mathsf{Pol}(\{\rho\}) \mid \rho \subseteq A^{(|A|^N)}, \rho \notin \mathsf{Inv}(\mathcal{C})\}$.

Let $\mathcal{E} \in \mathbf{C}(A)$ with $\mathcal{E} < \mathcal{C}$. Suppose first that $\mathsf{Inv}^{[|A|^N]}(\mathcal{E}) \subseteq \mathsf{Inv}^{[|A|^N]}(\mathcal{C})$. We show that then we have $\mathcal{C}^{[N]} \subseteq \mathcal{E}$. To this end, let $f \in \mathcal{C}^{[N]}$. Then $f \in \mathsf{Pol}(\mathsf{Inv}(\mathcal{C})) \subseteq \mathsf{Pol}(\mathsf{Inv}^{[|A|^N]}(\mathcal{C})) = \mathsf{Pol}(\mathsf{Inv}^{[|A|^N]}(\mathcal{E}))$. Hence by Theorem 3.2, we have $f \in \mathcal{E}$. This completes the proof of $\mathcal{C}^{[N]} \subseteq \mathcal{E}$. Hence $\mathcal{C} \subseteq \mathcal{E}$, contradicting $\mathcal{E} < \mathcal{C}$. This contradiction shows that there exists $\rho \in \mathsf{Inv}^{[|A|^N]}(\mathcal{E})$ with $\rho \notin \mathsf{Inv}(\mathcal{C})$. Now we have $\mathcal{E} \subseteq \mathsf{Pol}(\{\rho\})$, and therefore $\mathcal{E} \le \mathsf{Pol}(\{\rho\}) \cap \mathcal{C}$. Hence we have that every

$\mathcal{E} \in \mathbf{C}(A)$ with $\mathcal{E} < \mathcal{C}$ is contained in an element of $S_0(\mathcal{C})$. Thus, the set $S(\mathcal{C})$ is a subset of $S_0(\mathcal{C})$, and therefore finite.

We now show that every $\mathcal{E} \in \mathbf{C}(A)$ with $\mathcal{E} < \mathcal{C}$ is contained in some $\mathcal{D}$ with $\mathcal{E} \leq \mathcal{D} \prec \mathcal{C}$. To this end, let $\mathcal{D}$ be maximal in $S_0(\mathcal{C})$ with $\mathcal{E} \leq \mathcal{D}$. To show $\mathcal{D} \prec \mathcal{C}$, let $\mathcal{D}_1$ be such that $\mathcal{D} < \mathcal{D}_1 < \mathcal{C}$. Then there is $\mathcal{D}_2 \in S_0(\mathcal{C})$ such that $\mathcal{D}_1 \leq \mathcal{D}_2$. This $\mathcal{D}_2$ contradicts the maximality of $\mathcal{D}$. □

Lemma 6.4. *Let A be a finite nonempty set, and let $\mathcal{C} \in \mathbf{C}(A)$. Then the following are equivalent:*

(1) *$\mathcal{C}$ is not finitely generated.*
(2) *There is a strictly increasing sequence $(\mathcal{C}_i)_{i\in\mathbb{N}}$ of clones with $\bigcup_{i\in\mathbb{N}} \mathcal{C}_i = \mathcal{C}$.*

Proof: (1)⇒(2): Let $f_1, f_2, \ldots$ be an enumeration of all functions in $\mathcal{O}(A)$. Let $\mathcal{C}_1$ be the clone on A consisting only of projections, and let $\sigma(1)$ be such that $f_{\sigma(1)}$ is the unary identity operation. For $i \geq 2$, let $\sigma(i)$ be minimal such that $f_{\sigma(i)} \in \mathcal{C} \setminus \mathsf{Clone}(\{f_{\sigma(j)} \mid j < i\})$. Set $\mathcal{C}_i := \mathsf{Clone}(\{f_{\sigma(j)} \mid j \leq i\})$. 2⇒1: If $\mathcal{C}$ is finitely generated by $f_1, \ldots, f_m$, then each of these generators is contained in some $\mathcal{C}_i$. Hence there is a $j \in \mathbb{N}$ such that $\mathcal{C}_j$ contains $f_1, \ldots, f_m$, and therefore $\mathcal{C}_j = \mathcal{C}$. This contradicts the fact that $(\mathcal{C}_i)_i \in \mathbb{N}$ is strictly increasing. □

Theorem 6.5. *Let A be a finite nonempty set, and let $\mathcal{C}$ be a finitely related clone on A. Let $\mathcal{R}$ be a finite subset of $\mathcal{R}(A)$ such that $\mathcal{C} = \mathsf{Pol}(\mathcal{R})$, and let $N \in \mathbb{N}$ be such that for all $\rho \in \mathcal{R}$ we have $|\rho| \leq N$. Then we have:*

(1) *$T(\mathcal{C}) := \{\mathcal{D} \in \mathbf{C}(A) \mid \mathcal{C} \prec \mathcal{D}\}$ is finite (and has at most $|A|^{|A|^N}$ elements).*
(2) *For all $\mathcal{E} \in \mathbf{C}(A)$ with $\mathcal{C} < \mathcal{E}$ there is a $\mathcal{D} \in T(\mathcal{C})$ such that $\mathcal{D} \leq \mathcal{E}$.*

Proof: Let $T_0(\mathcal{C}) := \{\mathsf{Clone}(\mathcal{C} \cup \{f\}) \mid f : A^N \to A, f \notin \mathcal{C}\}$.

Now let $\mathcal{E} \in \mathbf{C}(A)$ be such that $\mathcal{C} < \mathcal{E}$. Suppose first that $\mathcal{E}^{[N]} \subseteq \mathcal{C}^{[N]}$. We show that then we have $\mathcal{E} \subseteq \mathcal{C}$. To this end, let $\rho \in \mathcal{R}$. Then $\rho \in \mathsf{Inv}(\mathcal{C}^{[N]}) \subseteq \mathsf{Inv}(\mathcal{E}^{[N]})$ Then since $|\rho| \leq N$, Corollary 5.2 yields $\rho \in \mathsf{Inv}(\mathcal{E})$. Hence $\mathcal{E}$ preserves every relation $\rho \in \mathcal{R}$. Thus $\mathcal{E} \subseteq \mathsf{Pol}(\mathcal{R}) = \mathcal{C}$. This contradicts the assumption $\mathcal{C} < \mathcal{E}$, and establishes the existence of an N-ary function $f \in \mathcal{E}$ with $f \notin \mathcal{C}$. Thus $\mathsf{Clone}(\mathcal{C} \cup \{f\}) \subseteq \mathcal{E}$. Altogether, every clone $\mathcal{D}$ with $\mathcal{C} < \mathcal{D}$ contains an element of $T_0(\mathcal{C})$ as a subclone. Hence $T(\mathcal{C}) \subseteq T_0(\mathcal{C})$.

Now let $\mathcal{E}$ be a clone with $\mathcal{C} < \mathcal{E}$. Let $\mathcal{D}$ minimal in $T_0(\mathcal{C})$ with $\mathcal{D} \leq \mathcal{E}$. Suppose $\mathcal{C} \prec \mathcal{D}$ fails. Then there is $\mathcal{D}_1 \in \mathbf{C}(A)$ with $\mathcal{C} < \mathcal{D}_1 < \mathcal{D}$. Now there is a clone

$\mathcal{D}_2 \in T_0(\mathcal{C})$ with $\mathcal{D}_2 \leq \mathcal{D}_1$, contradicting the minimality of $\mathcal{D}$. Hence we have $\mathcal{C} \prec \mathcal{D}$. □

Lemma 6.6. *Let A be a finite nonempty set, and let $\mathcal{C} \in \mathbf{C}(A)$. Then the following are equivalent:*

(1) *$\mathcal{C}$ is not finitely related.*
(2) *There is a strictly decreasing sequence $(\mathcal{C}_i)_{i\in\mathbb{N}}$ of clones with $\bigcap_{i\in\mathbb{N}_0} \mathcal{C}_i = \mathcal{C}$.*

Proof: (1)⇒(2): Let $\rho_1, \rho_2, \ldots$ be an enumeration of all relations in $\mathcal{R}(A)$. Let $s(1)$ be such that $\rho_{s(1)}$ is the unary relation A^1, and $\mathcal{C}_1 := \mathsf{Pol}(\rho_1) = \mathcal{O}(A)$. For $i \geq 2$, let $s(i)$ be minimal such that $\rho_{s(i)} \in \mathsf{Inv}(\mathcal{C})$ and $\rho_{s(i)} \notin \mathsf{Inv}(\mathcal{C}_{i-1})$, and let $\mathcal{C}_i := \mathsf{Pol}(\{\rho_{s(j)} \mid j \leq i\}$. (2)⇒(1): Suppose $\mathcal{C} = \mathsf{Pol}(\{\rho_1, \ldots, \rho_m\})$, and let $N := \max\{|\rho_j| : j \in \{1, \ldots, m\}\}$. Let r be such that $\mathcal{C}_r^{[N]} = \mathcal{C}^{[N]}$. Then $\mathcal{D} := \mathcal{C}_r$ preserves all relations in $\{\rho_1, \ldots, \rho_m\}$. Therefore $\mathcal{C}_r \leq \mathsf{Pol}(\{\rho_1, \ldots, \rho_m\}) = \mathcal{C}$, contradicting the fact that $(\mathcal{C}_i)_{i\in\mathbb{N}}$ is strictly decreasing. □

7. The definition of relational clones

Definition 7.1. Let A be a nonempty set, and let $\mathcal{R} \subseteq \mathcal{R}(A)$. Then $\mathcal{R}$ is a *relational clone* if and only if

(1) For all $m, n \in \mathbb{N}$, for all $R \in \mathcal{R}^{[m]}$, and for all $\sigma : \underline{n} \to \underline{m}$, we have $R * \sigma \in \mathcal{R}^{[n]}$.
(2) For all $m, n \in \mathbb{N}$, for all $R \in \mathcal{R}^{[n]}$, and for all $\sigma : \underline{n} \to \underline{m}$, we have $(R : \sigma)_{\underline{m}} \in \mathcal{R}^{[m]}$.
(3) For all $n \in \mathbb{N}$ and $R, S \in \mathcal{R}^{[n]}$, we have $R \cap S \in \mathcal{R}^{[n]}$.

We note that $(R : \sigma)_{\underline{m}} = \{(a_1, \ldots, a_m) \in A^m \mid (a_{\sigma 1}, \ldots, a_{\sigma n}) \in R\}$.

8. The relational clones of the form $\mathsf{Inv}(\mathcal{F})$

Proposition 8.1. *Let A be a nonempty set, and let $\mathcal{F} \subset \mathcal{O}(A)$. Then $\mathsf{Inv}(\mathcal{F})$ is a relational clone.*

Proof: The first two properties in the definition of relational clones followw from Lemma 2.4. For the third property, let $n \in \mathbb{N}$, and let $R, S \in \mathsf{Inv}^{[n]}(\mathcal{F})$. We have to show that $R \cap S \in \mathsf{Inv}^{[n]}(\mathcal{F})$. To this end, let $m \in \mathbb{N}$ and $f \in \mathcal{F}^{[m]}$, and let

$v_1, \dots, v_m \in R \cap S$. Then $\langle f(v_1(i), \dots, v_m(i) \mid i \in \underline{n}\rangle$ lies in R because of $f \rhd R$ and in S because of $f \rhd S$. □

The next lemma will be needed in proving that every relational clone on a finite set is of the form $\mathsf{Inv}(\mathcal{F})$.

Lemma 8.2. *Let A be a nonempty finite set, let K be a set, and for each $k \in K$, let $R_k \subseteq A^{I_k}$ be a finitary relation on A. Let $\mathcal{R} := \{R_k \mid k \in K\}$. Let $n \in \mathbb{N}$. Then for each $k \in K$, there are: $m_k \in \mathbb{N}_0$ and $\sigma_{k,1} : I_k \to A^n, \dots, \sigma_{k,m_k} : I_k \to A^n$ such that*

$$\mathsf{Pol}^{[n]}(\mathcal{R}) = \bigcap_{k \in K} \bigcap_{m \in \{1,\dots,m_k\}} (R_k : \sigma_{k,m})_{A^n}.$$

Proof: Let $k \in K$, let $m_k := |R_k|^n$, and let $r_1, \dots, r_{m_k} \in (A^{I_k})^n$ be the elements of $(R_k)^n$. Then for $m \in \{1, \dots, m_k\}$, we define $\sigma_{k,m} : I_k \to A^n$, $\sigma_{k,m}(i) = (r_m(1)\,(i), \dots, r_m(n)\,(i))$.

Now we prove $\subseteq$. Let $f \in \mathsf{Pol}^{[n]}(\mathcal{R})$, let $k \in K$, and let $m \in \{1, \dots, m_k\}$. We have to prove $f \circ \sigma_{k,m} \in R$. We have $f \circ \sigma_{k,m} = \langle f(\sigma_{k,m}(i)) \mid i \in I_k\rangle = \langle f(r_m(1)(i) \dots, r_m(n)(i)) \mid i \in I_k\rangle$. Since $(r_m(1), \dots, r_m(n))$ is an element of $(R_k)^n$, we have $r_m(j) \in R_k$ for all $j \in \{1, \dots, n\}$. Now since $f \rhd R_k$, we have $\langle f(r_m(1)(i) \dots, r_m(n)(i)) \mid i \in I_k\rangle \in R_k$.

For $\supseteq$, let f be in the right hand side, and let $k \in K$. We show $f \rhd R_k$. To this end, let $v_1, \dots, v_n \in R_k$. There is $m \in \{1, \dots, m_k\}$ such that $r_m = (v_1, \dots, v_n)$. We know that $f \circ \sigma_{k,m} \in R_k$. We have $f \circ \sigma_{k,m} = \langle f(\sigma_{k,m}(i)) \mid i \in I\rangle = \langle f(r_m(1)(i), \dots, r_m(n)(i)) \mid i \in I\rangle = \langle f(v_1(i), \dots, v_n(i)) \mid i \in I\rangle$. The fact that the last expression lies in R_k completes the proof that f preserves R_k. □

Lemma 8.3. *Let I, J, K, L be nonempty sets, let $R \in A^I$, let $\sigma : I \to J$, for each $l \in L$ let $S_l \in A^J$, and let $\tau : K \to J$. Then we have:*

(1) *If τ is bijective, we have $(R : \sigma)_J * \tau = (R : \tau^{-1} \circ \sigma)_K$.*
(2) *If τ is surjective onto J, we have $(\bigcap_{l \in L} S_l) * \tau = \bigcap_{l \in L}(S_l * \tau)$.*

Proof: (1) For proving $\supseteq$, we assume that $f \in A^K$ lies in $(R : \tau^{-1} \circ \sigma)_K$. Then $f \circ \tau^{-1} \circ \sigma \in R$. This implies $f \circ \tau^{-1} \in (R : \sigma)_J$, and therefore $(f \circ \tau^{-1}) \circ \tau \in (R : \sigma)_J * \tau$.

For the inclusion $\subseteq$, let $g \in (R : \sigma)_J$. We show $g \circ \tau \in (R : \tau^{-1} \circ \sigma)_K$. To this end, we have to show $g \circ \tau \circ \tau^{-1} \circ \sigma \in R$. Since $g \circ \tau \circ \tau^{-1} \circ \sigma = g \circ \sigma$ and $g \in (R : \sigma)_J$, we have $g \circ \sigma \in R$, which implies the result.

(2) $\subseteq$: Let $r \in \bigcap_{l \in L} S_l$. Then for each $l \in L$, we have $r * \tau \in S_l * \tau$. $\supseteq$: Let $r \in \bigcap_{l \in L} (S_l * \tau)$. We choose $l_0 \in L$. Since $r \in S_{l_0} * \tau$, we have $s_0 \in S_{l_0}$ such that $r = s_0 \circ \tau$. Now let $l \in L$. Then we have $s \in S_l$ such that $r = s \circ \tau$. Therefore the functions s_0 and s agree on the image of τ. By the surjectivity of τ, we have $s_0 = s$. Hence $s_0 \in S_l$. Thus $s_0 \in \bigcap_{l \in L} S_l$, which implies $r \in (\bigcap_{l \in L} S_l) * \tau$. $\square$

Theorem 8.4. *Let $\mathcal{R}$ be a relational clone on the finite set A. Then $\mathcal{R} = \mathsf{Inv}(\mathsf{Pol}(\mathcal{R}))$.*

Proof: Let $S \in \mathsf{Inv}(\mathsf{Pol}(\mathcal{R}))$, and let $t \in \mathbb{N}$ be such that $S \subseteq A^t$. Let n be such that S is n-generated as a subuniverse of $\langle A, \mathsf{Pol}^{[n]}(\mathcal{R}) \rangle^t$; this will for example always be accomplished by setting $n := |S|$. Then by Theorem 5.1, there is $\sigma : \{1, \ldots, t\} \to A^n$ such that $S = \mathsf{Pol}^{[n]}(\mathcal{R}) * \sigma$.

From Lemma 8.2, we have a set K, and for each $k \in K$ an $r_k \in \mathbb{N}_0$ and $\sigma_{k,1} : A^n \to \underline{i_k}, \ldots, \sigma_{k,r_k} : A^n \to \underline{i_k}$ such that

$$\mathsf{Pol}^{[n]}(\mathcal{R}) = \bigcap_{k \in K} \bigcap_{r \in \{1,\ldots,r_k\}} (R_k : \sigma_{k,r})_{A^n}.$$

Since $A^{(A^n)}$ is a finite set, $\mathsf{Pol}^{[n]}(\mathcal{R})$ is an intersection of at most $|A|^{|A|^n}$ of the sets appearing on the right hand side; thus there is a finite $K_0 \subseteq K$ (with at most $|A|^{|A|^n}$ elements) such that $\mathsf{Pol}^{[n]}(\mathcal{R}) = \bigcap_{k \in K_0} \bigcap_{r \in \{1,\ldots,r_k\}} (R_k : \sigma_{k,r})_{A^n}$.

Now let $m := |A|^n$, and let $\tau : \underline{m} \to A^n$ be a bijection. Then by Lemma 8.3, we have

$$\begin{aligned}
\mathsf{Pol}^{[n]}(\mathcal{R}) &= \bigcap_{k \in K_0} \bigcap_{r \in \{1,\ldots,r_k\}} ((R_k : \sigma_{k,r})_{A^n} * \tau * \tau^{-1}) \\
&= \Big(\bigcap_{k \in K_0} \bigcap_{r \in \{1,\ldots,r_k\}} ((R_k : \sigma_{k,r})_{A^n} * \tau) \Big) * \tau^{-1} \\
&= \Big(\bigcap_{k \in K_0} \bigcap_{r \in \{1,\ldots,r_k\}} (R_k : \tau^{-1} \circ \sigma_{k,r})_{\underline{m}} \Big) * \tau^{-1}.
\end{aligned}$$

Hence

$$S = \Big(\bigcap_{k \in K_0} \bigcap_{r \in \{1,\dots,r_k\}} (R_k : \tau^{-1} \circ \sigma_{k,r})_{\underline{m}} \Big) * \tau^{-1} * \sigma$$
$$= \Big(\bigcap_{k \in K_0} \bigcap_{r \in \{1,\dots,r_k\}} (R_k : \tau^{-1} \circ \sigma_{k,r})_{\underline{m}} \Big) * (\tau^{-1} \circ \sigma).$$

□

9. A Theorem on Groups

Theorem 9.1. *Let G be a finite group. Then there exist $k \in \mathbb{N}$ and a subgroup H of G^k with the following property:*

> *For each $n \in \mathbb{N}$ there are $l \in \mathbb{N}$ and $m \in \mathbb{N}_0$ with $l \leq |G|^{\max(2, \lfloor n \cdot \log_2(|G|) \rfloor)}$ and $m \leq l \cdot \log_2(|G|)$, and there is a mapping $\sigma : \underline{m} \times \underline{k} \to \underline{l}$ such that for every subgroup S of G^n there is a mapping $\tau : \underline{n} \to \underline{l}$ with $S = \{(g_1, \dots, g_n) \in G^n \mid \exists a_1, \dots, a_l \in G : \big(\bigwedge_{i \in \underline{m}} (a_{\sigma(i,1)}, \dots, a_{\sigma(i,k)}) \in H\big) \wedge g_1 = a_{\tau(1)} \wedge \dots \wedge g_n = a_{\tau(n)}\}$.*

Proof: By [AMM11], we know that there is a a finite subgroup of H of G^k such that the clone $\mathcal{C}$ of term operations on G consists exactly of those functions that preserve H. Now let $n \in \mathbb{N}$, let $e := \max(2, \lfloor n \log_2(|G|) \rfloor)$, $l := |G|^e$, and let $m := \lfloor l \cdot \log_2(|G|) \rfloor$.

Then from Lemma 8.2, we know that there is an $m_1 \in \mathbb{N}$ and $\alpha_1, \dots, \alpha_{m_1} : \underline{k} \to G^e$ such that $\mathcal{C}^{[e]} = \bigcap (H : \alpha_i)_{G^e}$. Let ρ be a bijection from $\{1, \dots, l\}$ to G^e. Then by Lema 8.3, $\mathcal{C}^{[e]} * \rho = \bigcap_{i \in \underline{m_1}} (H : \rho^{-1} \circ \alpha_i)_{\underline{l}}$. Since $\mathcal{C}^{[e]} * \rho$ is a subgroup of G^l, we can choose m subgroups such that the intersection of these m subgroups is equal to the intersection of the m_1 given subgroups of G^l, where $m \leq \lfloor \log_2(|G|^l) \rfloor = \lfloor l \cdot \log_2(|G|) \rfloor$.

As a subgroup of G^n, S has a set of generators with at most $\log_2(|G|^n)$ elements. Since $e \geq 2$, S is e-generated as a subuniverse of $\langle S, \mathcal{C}^{[e]} \rangle^n$. Hence from Theorem 5.1, we have a mapping $\tau_1 : \underline{n} \to \underline{l}$ such that $S = \mathcal{C}^{[e]} * \tau_1 = \mathcal{C}^{[e]} * \rho * \rho^{-1} * \tau_1$. Now let $\tau := \rho^{-1} \circ \tau_1$. Then $S = \mathcal{C}^{[e]} * \rho * \tau$. We have $(a_1, \dots, a_l) \in \mathcal{C}^{[e]} * \rho$ if and only if for all $i \in \underline{m} : (a_{\rho^{-1}(\alpha_i(1))}, \dots, a_{\rho^{-1}(\alpha_i(k))}) \in H$. We define $\sigma(i,j) := \rho^{-1}(\alpha_i(j))$.

Now we know that $(b_1, \dots, b_n) \in \mathcal{C}^{[e]} * \rho * \tau$ if and only if there is $(a_1, \dots, a_l) \in \mathcal{C}^{[e]} * \rho$ such that $b_j = a_{\tau(j)}$ for all $j \in \underline{n}$. □

References

[AMM11] E. Aichinger, P. Mayr, and R. McKenzie, *On the number of finite algebraic structures*, submitted; available on arXiv:1103.2265v1 [math.RA].

[Maš10] D. Mašulović, *Introduction to discrete mathematics*, Lecture notes for a course at JKU Linz, Austria, 2010; available at `http://www.algebra.uni-linz.ac.at/Students/DiskreteMathematik/ws10/`, 2010.

[PK79] R. Pöschel and L. A. Kalužnin, *Funktionen- und Relationenalgebren*, Mathematische Monographien [Mathematical Monographs], vol. 15, VEB Deutscher Verlag der Wissenschaften, Berlin, 1979, Ein Kapitel der diskreten Mathematik. [A chapter in discrete mathematics].

[Sze86] Á. Szendrei, *Clones in universal algebra*, Séminaire de Mathématiques Supérieures [Seminar on Higher Mathematics], vol. 99, Presses de l'Université de Montréal, Montreal, QC, 1986.