Binary Relations and Permutation Groups *

Hajnal Andréka†
Mathematical Institute
Academy of Sciences
Budapest 1363, Hungary
andreka@math-inst.hu

Ivo Düntsch‡
Faculty of Informatics
University of Ulster at Jordanstown
Newtonabbey, BT 37 0QB, N.Ireland
I.Duentsch@ulst.ac.uk

István Németi
Mathematical Institute
Academy of Sciences
Budapest 1363, Hungary
nemeti@math-inst.hu

Abstract

We discuss some new properties of the natural Galois connection among set relation algebras, permutation groups, and first order logic. In particular, we exhibit infinitely many permutational relation algebras without a Galois closed representation, and we also show that every relation algebra on a set with at most six elements is Galois closed and essentially unique. Thus, we obtain the surprising result that on such sets, logic with three variables is as powerful in expression as full first order logic.

Key words: Relation algebras, Galois closure, clones of operations

0 Introduction and summary of results

Logics with limited resources as well as questions of expressibility of relational properties- in particular on finite structures - have received considerable attention in areas like finite model theory, non - classical logics, and descriptive complexity. The interested reader is invited to consult [9], [11], [12], and [14] for more details. In this paper, we shall investigate problems relating to automorphisms (i.e. edge preserving permutations) of binary relations. Our approach will be algebraic using Tarski's relation algebras. Roughly speaking, a relation algebra is a description of how various relations must interact among each other. More concretely, given a set $\mathcal{R} = \{R_i : i < n\}$ of binary relations on a set U, we form the closure of this set under the Boolean operations, composition of relations, and converse, and add the identity as an extra constant; the result will be an algebra $\mathfrak{A}$ of binary relations (BRA). Since the operations used are first order definable, any automorphism of the first order structure $\langle U, \mathcal{R}\rangle$ will preserve all the relations in $\mathfrak{A}$ as well. Such an automorphism will be called a *base automorphism of the algebra* $\mathfrak{A}$ (We use the qualified term to distinguish them from the automorphisms of the algebra). A fundamental result by Tarski states that $\mathfrak{A}$ contains exactly those binary

*Mathematical Logic Quarterly 41 (1995), 197–216

†Andréka's and Németi's research sponsored by Hungarian National Foundation for Scientific Research Grants 1911 and T7255

‡Member of Institut für semantische Informationsverarbeitung, Universität Osnabrück, Germany

relations on U which are definable in $\langle U, \mathcal{R} \rangle$ by first order formulas having at most three variables. Thus, the equational logic of relation algebras corresponds roughly to the three variable fragment of full first order logic. Conversely, given a representation $\mathfrak{B}$ of an abstract simple relation algebra $\mathfrak{A}$ (i.e. $\mathfrak{B}$ is a BRA isomorphic to $\mathfrak{A}$), the algebraic structure of $\mathfrak{A}$ will tell us something about the properties of and the connections among the relations in $\mathfrak{B}$.

We exhibit connections between the structure of BRAs and their groups of base automorphisms. The notion of Galois closure will play a major role: A BRA on a finite set U is *Galois closed* iff its atoms are the orbits of the action of its group of base automorphisms on $U \times U$. The Galois closure of a BRA $\mathfrak{A}$ on U is the smallest Galois closed algebra containing $\mathfrak{A}$. It turns out that the nonempty subsets definable by formulas of first order logic in the model $\langle U, R \rangle_{R \in \mathfrak{A}}$ are exactly the domains of the unions of those atoms of the Galois closure of $\mathfrak{A}$ which are below the identity - equivalently, the unions of orbits of the group of base automorphisms of $\mathfrak{A}$. Furthermore, $\mathfrak{A}$ is shown to be Galois closed iff $\mathfrak{A}$ contains all relations definable in the model $\langle U, R \rangle_{R \in \mathfrak{A}}$, and that, whenever an edge $\langle a, b \rangle$ of an atom R of $\mathfrak{A}$ has a first order property, then all edges of R have this property. We also show that the property of a BRA to be Galois closed is a general first order property for finite models, and that its negation is not.

With regard to the question which properties of concrete relations can be prescribed by the structure of an abstract relation algebra, we exhibit a relation algebra $\mathfrak{A}$ which has a representation with a transitive group of base automorphisms, but no representation of $\mathfrak{A}$ is Galois closed. This seems a rather strong result: The algebraic structure of $\mathfrak{A}$ - which in general reflects only logic with three variables - tells us something about a property of all representations of $\mathfrak{A}$ which is not even general first order.

Finally, we show that every BRA on a set with at most six elements is Galois closed and essentially unique. Thus, we obtain the surprising result that on such sets, logic with three variables is as powerful in expression as full first order logic.

Computational results were obtained with the help of CAYLEY, ([7]), NAUTY ([18], and RELALG ([8]).

1 Definitions and notation

Unless otherwise indicated, we shall suppose throughout that all structures under consideration are finite, and that U is a non empty finite set. $|U|$ denotes the cardinality of U. We identify $\{0, \ldots, n-1\}$ with the ordinal n, and emphasize this by writing $\mathbf{n}$. If no confusion is likely to arise, algebras are referred to by their respective carrier set.

A relation algebra (RA)

$$\langle A, +, \cdot, -, 0, 1, \circ, ^{-1}, 1' \rangle$$

is a structure of type $\langle 2, 2, 1, 0, 0, 2, 1, 0 \rangle$ which satisfies

1. $\langle A, +, \cdot, -, 0, 1 \rangle$is a Boolean algebra.

2. $\langle A, \circ, ^{-1}, 1' \rangle$ is an involuted monoid.

3. For all $a, b, c \in A$ the following conditions are equivalent:

$$(a \circ b) \cdot c = 0, \ (a^{-1} \circ c) \cdot b = 0, \ (c \circ b^{-1}) \cdot a = 0.$$

The *full algebra of binary relations* $\langle Rel(U), \cup, \cap, -, \emptyset, {}^2U, \circ, ^{-1}, 1' \rangle$ is a relation algebra, where $Rel(U)$ is the set of all binary relations on U, $\cap, \cup, -$ are the usual set theoretic operations, and $\emptyset$, ${}^2U$ are, respectively, the empty and the universal relation, $\circ$ is relational composition, $^{-1}$ the relational inverse (i.e. $P^{-1} = \{\langle x,y \rangle : \langle y,x \rangle \in P\}$), and $1'$ is the identity relation on U. We shall usually use $P, Q, R, \ldots$ to denote binary relations on U. A subset A of $Rel(U)$ which is closed under the distinguished operations of $Rel(U)$ and contains the distinguished constants is called an *algebra of binary relations* (BRA) on U. It is a subalgebra of $Rel(U)$, a fact which we denote by $A \leq Rel(U)$. If $A \leq Rel(U)$, then $At(A)$ denotes the set of atoms of (the Boolean part of) A. A complete and atomic A is completely determined by the relation composition table of $At(A)$. When writing such a table, we usually omit column and row $1'$, if $1'$ is an atom of A. If $R_0, \ldots, R_k \in Rel(U)$, we denote the BRA generated by $R_0, \ldots, R_k$ by $\langle R_0, \ldots, R_k \rangle$.

A relation algebra A is called *representable* if it is isomorphic to a subalgebra of a product of full algebras of binary relations.

The following fundamental result is due to A. Tarski [20]:

Proposition 1.1. *If $R_0, \ldots, R_k \in Rel(U)$, then $\langle R_0, \ldots, R_k \rangle$ is the set of all binary relations on U which are definable in the relational structure $\langle U, R_0, \ldots, R_k \rangle$ by first order formulas using at most 3 variables.*

$A \leq Rel(U)$ is called *essentially unique* on U if for every $B \leq Rel(U)$ which is isomorphic to A and every RA - isomorphism $h : A \to B$ there is a permutation ϕ of U such that $h(R) = \phi^{-1} \circ R \circ \phi$ for all $R \in A$. Consequently, if A is essentially unique on U and $B \leq Rel(U)$ is isomorphic to A, then A and B are isomorphic as first order relational structures on U – usually a much stronger condition.

For $P, Q \in A \leq Rel(U)$ and $x, y, z \in U$ we usually write xPy if $\langle x, y \rangle \in P$, and $xPyQz$ means xPy and yQz. We also set

$$\begin{aligned}
dom(P) &= \{x \in U : \text{There is some } y \in U \text{ such that } xPy\}, \\
ran(P) &= \{x \in U : \text{There is some } y \in U \text{ such that } yPx\}, \\
dom_P(x) &= \{y \in U : yPx\}, \\
ran_P(x) &= \{y \in U : xPy\}.
\end{aligned}$$

The set $ran_P(x)$ is also called a *row of* P. If $|ran_P(y)| = |ran_P(x)|$ for all $x, y \in dom(P)$, then P is called *regular*.

If A is any RA, then $x \in A$ is called a *functional element* if $x^{-1} \circ x \leq 1'$. A is called *integral* if, for all $x, y \in A$, $x \circ y = 0$ implies $x = 0$ or $y = 0$. A well known characterization of integral RAs [17] is given by

Lemma 1.2. *Let A be a relation algebra. Then, the following statements are equivalent:*

1. *A is integral.*
2. *$1'$ is an atom of A.*
3. *$x \circ 1 = 1$ for any non zero $x \in A$.*
4. *Every functional non zero $x \in A$ is an atom of A.*
5. *If A is a BRA on a finite set U, then $dom(R) = ran(R) = U$ for some atom R of A.*

If $M \in A \leq Rel(U)$ is an equivalence relation, the set $B = \{R \in A : R \subseteq M\}$ becomes a relation algebra under the operations $\cup, \cap, \emptyset, \circ, ^{-1}$ inherited from A, with greatest element M, identity element $\{\langle x,x\rangle : x \in dom(M)\}$, and complementation being relative to M. This algebra is called the *relative algebra of A with respect to M*. Unless $M = {}^2U$, B is not a subalgebra of A.

Suppose that the BRA A on U is not integral; then, there are atoms $E_i, i < k$, of A such that $E_i \subsetneq 1'$. For $i, j < k$, set $U_i = dom(E_i)$ and $U_{ij} = U_i \times U_j$. We observe that $U_{ij} = E_i \circ {}^2U \circ E_j$, so that $U_{ij} \in A$. Since each U_{ii} is an equivalence relation contained in A, we can consider the relative algebra of A with respect to U_{ii}, which we denote by A_i. If $R \in A_i$, then R is an atom of A_i if and only if R is an atom of A. Consequently, each A_i is an integral relation algebra, and, in loose analogy to permutation groups, we call the algebra A_i an *integral constituent* of A and U_i its *constituent set*. The following technical lemma will be useful in the sequel:

Lemma 1.3. *Let A have the integral constituents $A_i, i < k$.*

1. *If $P \in At(A)$ and $|ran_P(x)| = 1$ for some $x \in U$, then this holds for all $x \in dom(P)$.*
2. *If $P \in At(A),\ P \subseteq U_{ij}$, then $dom(P) = U_i,\ ran(P) = U_j$.*
3. *Suppose that $i, j < k,\ |U_i| \leq 3,\ |U_i| < |U_j|,\ |U_j|$ is not a multiple of $|Ui|$, and that every $R \in At(A_j)$ is regular. Then, $U_{ij} \in At(A)$.*

Proof. 1. Suppose that $ran_P(x) = \{a\}$, and assume that $|ran_P(y)| \geq 2$ for some $y \in U$. Let $\phi(x)$ be the formula

$$(\exists y)(\forall z)[xPy \wedge (xPz \Rightarrow y = z)].$$

The truth set M of ϕ in the model $\langle U,P\rangle$ is the set of all those elements of $dom(P)$ whose P - range consists of exactly one element. By our assumption we have $\emptyset \subsetneq M \subsetneq dom(P)$, and by 1.1 the relation $1' \cap {}^2M$ is an element of $\langle P\rangle \subseteq A$, since ϕ contains only three variables. This contradicts the fact that P is an atom of A.

2. Assume that $y \in U_i \setminus dom(P)$; then, $\langle y,y\rangle \notin (P \circ P^{-1}) \cap E_i$, contradicting that E_i is an atom of A. The other part is shown analogously.

3. Assume that for some $i \neq j$ there is some $P \in At(A)$ such that $P \subsetneq U_{ij}$, and set $Q = U_{ij} \setminus P$. Let $y \in U_j$; if there is exactly one $x \in U_i$ with xPy, then P^{-1} is a function by the fact that it is an atom

and 1. above. Thus, the P-ranges of elements of U_i partition U_j, and from the condition on A_j and 1.2 it follows that the classes of this partition have the same number of elements. This, however, contradicts that $|U_j|$ is not a multiple of $|U_i|$. Therefore, each $y \in U_j$ appears in at least two rows of P, and the same arguments apply to Q. Hence, for each $y \in U_j$ we have $2 \leq |dom_P(y)| \leq |U_i| - 2$, which contradicts $|U_i| \leq 3$. □

We now turn to permutation groups. The symmetric group on U is denoted by $Sym(U)$. If G is a subgroup of $Sym(U)$ - a fact which we describe by $G \leq Sym(U)$ - , and if $M \subseteq U$, we denote by M^G the set $\{\phi(x) : x \in M,\ \phi \in G\}$; for $\phi \in Sym(U)$, M^ϕ is the set $\{\phi(x) : x \in M\}$. A *fixed block of* G is a non empty subset M of U such that $M = M^G$; a minimal fixed block is called an *orbit of* G. If G has only one orbit, it is called *transitive*. $M \subseteq U$ is a *set of imprimitivity*, if $M^G = M$ or $M^G \cap M = \emptyset$. The empty set, the singletons and U itself are called *trivial sets of imprimitivity*. A transitive G is called *primitive* if it has no non trivial sets of imprimitivity.

G is called *semiregular* if the identity is the only element of G that fixes a point, or, equivalently, if for all $\phi, \psi \in G$ the fact that $\phi(x) = \psi(x)$ for some $x \in U$ implies that $\phi = \psi$. If G is semiregular and transitive it is called *regular*.

If $\phi \in Sym(U)$ and $x, y \in U$, then we set $\phi(\langle x,y\rangle) = \langle \phi(x), \phi(y)\rangle$, and $R^\phi = \{\phi(\langle x,y\rangle) : \langle x,y\rangle \in R\}$; note that $R^\phi = \phi^{-1} \circ R \circ \phi$. If $R^\phi = R$, then ϕ is called a *base automorphism of* R. For $A \leq Rel(U)$ we set

$$A^\rho = \{\phi \in Sym(U) : R^\phi = R \text{ for all } R \in A\}.$$

It is not hard to see that A^ρ is a subgroup of $Sym(U)$, called the *group of base automorphisms of* A, and that $\phi \in A^\rho$ if and only if ϕ commutes with every atom of A.

Conversely, if G is a subgroup of $Sym(U)$ and $x, y \in U$, we set

$$G_{x,y} = \{\phi(\langle x,y\rangle) : \phi \in G\},$$

and let G^σ be the BRA on U generated by $\{G_{x,y} : x, y \in U\}$. Observe that the sets $G_{x,y}$ are just the orbits of the action of G on ${}^2U$, and hence a partition of ${}^2U$. Indeed, each $G_{x,y}$ is an atom of G^σ, and every atom of G^σ has this form. The assignments ρ and σ form a Galois connection, and $A \leq Rel(U)$ is called *Galois closed* if $A^{\rho\sigma} = A$; similarly, $H \leq Sym(U)$ is Galois closed if $H^{\sigma\rho} = H$ (see [15]).

2 Groups and relation algebras

It has been of some interest to investigate which properties of some $G \leq Sym(U)$ carry over in which form to the relation algebra G^σ and vice versa. As an example, we cite a result from [15]:

Proposition 2.1. *If $A \leq Rel(U)$, and every atom of A is functional, then A is Galois closed and A^ρ is semiregular. Conversely, if $G \leq Sym(U)$ is semiregular, then G is Galois closed and every atom of G^σ is functional.*

The following connection has been known for some time:

Proposition 2.2. *1. If G is transitive, then G^{σ} is integral.*

2. If G is primitive, then G^{σ} does not contain a non trivial proper equivalence relation.

Proof. The proof of 1. is straightforward, and a proof of 2. can be found in [21]. □

The corresponding statements for relation algebras are not true:

Proposition 2.3. *1. There is an integral $A \leq Rel(\mathbf{7})$ such that A^{ρ} is not transitive.*

2. There is an integral $A \leq Rel(\mathbf{8})$ which does not contain a non trivial proper equivalence relation, and for which A is not primitive.

Proof. 1. Let $S = {}^2\mathbf{3} \cup {}^2(\mathbf{7} \setminus \mathbf{3})$. S is the disjoint union of a K_3 and a K_4, and generates an integral relation algebra A on $U = \mathbf{7}$ with atoms $S, T, 1'$ and the following composition table:

$\circ$	S	T
S	$-T$	T
T	T	$-T$

Since 0 is an even node, and 1 is an odd node, A^{ρ} is not transitive. It will follow from a subsequent result that this example is the smallest possible for this situation.

2. Let $\phi \in Sym(\mathbf{8})$ be the cycle $(0...7)$, and let $S = \phi \cup \phi^4 \cup \phi^{-1}$. S generates an algebra $A \leq Rel(\mathbf{8})$ with the atoms $S, T, 1'$ and the following composition table:

$\circ$	S	T
S	$-S$	$-1'$
T	$-1'$	${}^2U$

A^{ρ} is generated by the permutations $(17)(26)(35)$ and $(01)(27)(36)(45)$, and it has 16 elements. It is transitive and not primitive; a system of imprimitivity is given by $\{0,4\},\{1,5\},\{2,6\},\{3,7\}$. □

The situation is described by

Proposition 2.4. *Let $A \leq Rel(U)$. Then,*

1. A^{ρ} is transitive if and only if $A^{\rho\sigma}$ is integral.

2. Suppose that A^{ρ} is transitive. Then, A^{ρ} is primitive if and only if $A^{\rho\sigma}$ does not contain a non trivial proper equivalence relation.

Proof. 1. "⇒" is just 2.2.1. Thus, set $G = A^{\rho}$, and suppose that G^{σ} is integral. If $x, y \in U$, then, by the integrality of G^{σ}, the atom $G_{x,y}$ of G^{σ} has all of U as its domain. Thus, there is some $z \in U$ such that $\langle y, z \rangle \in G_{x,y}$; by the definition of $G_{x,y}$ there is some $\phi \in G$ with $\phi(x) = y$, and hence G is transitive.

2. "⇒" is 2.2.2. Thus, let $G = A^{\rho}$, and suppose that G^{σ} does not contain a non trivial equivalence relation. Assume that there is a subset M of U such that $1 < |M| < |U|$, and that M is minimal with respect to the property that for all $\phi \in G$, either $M^{\phi} = M$ or $M \cap M^{\phi} = \emptyset$. Define a relation P on U by xPy if and only if $x, y \in M^{\phi}$ for some $\phi \in G$. Since the family $\{M^{\phi} : \phi \in G\}$ is a partition of U, P is an

equivalence relation, and by our assumption on M, P is not trivial. Let xPy; then, $G_{x,y} \cap P \neq \emptyset$, and we can assume without loss of generality that $x,y \in M$. If $\langle u,v\rangle \in G_{x,y}$ with $\phi \in G$ exhibiting this fact, then $u = \phi(x) \in M^{\phi}$, $v = \phi(y) \in M$, and thus uPv. It follows that $G_{x,y} \subseteq P$. Since U is finite, P is a union of atoms of $A^{\rho\sigma}$, and therefore $P \in A^{\rho\sigma}$. This contradicts our hypothesis. □

Call an integral $A \leq Rel(U)$ *c - permutational* if A^{ρ} is transitive, i.e. for all $u,v \in U$ there is a base automorphism of A taking u to v. An integral abstract relation algebra is called *permutational*, if it has a c - permutational representation. Proposition 2.3.1 above gives an example of an integral BRA on **7** which is not c - permutational. A representation of A which is c - permutational is available on a six element set: Just let S be the disjoint union of two K_3's. In [2] we have exhibited an integral representable relation algebra which does not have a c - permutational representation. The algebra of Proposition 2.3.2 is an example of a permutational BRA A which is not Galois closed. However, this A, regarded as an abstract relation algebra, has a Galois closed representation on a ten element set: If G is the action of $Sym(\mathbf{5})$ on the set of unordered pairs of **5**, then G is the BRA generated by the Petersen graph ([6]) which is isomorphic to A. The remaining question whether there is a permutational relation algebra without a Galois closed representation is answered below.

Proposition 2.5. *There is a permutational relation algebra which does not have a Galois closed representation.*

Proof. Let $S,G \in Sym(\mathbf{4})$ be defined by

$$\begin{aligned} S &= (01)(23), \\ G &= (02)(13), \end{aligned}$$

and $R,B \in Rel(\mathbf{4})$ by

$$\begin{aligned} ran_R(0) &= ran_R(1) = \{0,2\}, & ran_R(2) &= ran_R(3) = \{1,3\} \\ ran_B(0) &= ran_B(2) = \{0,3\}, & ran_B(1) &= ran_R(3) = \{1,2\} \end{aligned}$$

For any positive natural number n we set $U_n = \mathbf{n} \times \mathbf{4}$, and define

$$\begin{aligned} s &= \{\langle\langle i,j\rangle,\langle i,S(j)\rangle\rangle : i < n,\ j < 4\} \\ g &= \{\langle\langle i,j\rangle,\langle i,G(j)\rangle\rangle : i < n,\ j < 4\} \\ r &= \{\langle\langle i,j\rangle,\langle i+1,k\rangle\rangle : i < n,\ \langle j,k\rangle \in R\} \\ b &= \{\langle\langle i,j\rangle,\langle i+2,k\rangle\rangle : i < n,\ \langle j,k\rangle \in B\} \end{aligned}$$

Here, as throughout this proof, addition is modulo n. Let A_n be the BRA generated by s,g,r and b. To facilitate notation, we denote $x \circ y$ by xy for $x,y \in A_n$.

1. *If $n < 7$, then A_n is not integral*:

This is easy to check, e.g. if $n = 6$, then $dom(rb \cap (rb)^{-1}) \neq U$, and if $n = 5$, then $dom(rb \cap b^{-1}) \neq U$.

2. *If $n \geq 7$, then A_n is integral with the following $n+9$ atoms*:

$$s, g, sg, 1', r, rs, b, bs, rb, rbs, r^{-1}, sr^{-1}, b-1, sb^{-1}, b^{-1}r^{-1}, sb^{-1}r^{-1}, r^4, r^5, \ldots, r^{n-4}.$$

The proof is straightforward, if somewhat computational, and is left to the reader.

3. *If* $n \geq 8$, *then* A_n *has no Galois closed representation*:

We first show that, though A_n is not essentially unique on U, all its representations are on some $n \cdot 4$ element set, and that all representations are very much alike. Thus, let U' be a set, $A' \in Rel(U')$, and $rep : A_n \to A'$ be an RA - isomorphism; furthermore, set $e = s + g + sg + 1'$.

From $ss = gg = 1'$ and $sg = gs$ we obtain that $rep(e)$ is an equivalence relation on U' with each block containing exactly four elements. So we may suppose that $U' = \mathbf{n}' \times \mathbf{4}$ for some n', and that

$$\begin{aligned} rep(s) &= \{\langle\langle i,j\rangle,\langle i,S(j)\rangle\rangle : i < n',\ j < 4\} \\ rep(g) &= \{\langle\langle i,j\rangle,\langle i,G(j)\rangle\rangle : i < n',\ j < 4\} \end{aligned}$$

Let $f = r + rs$ and set

$$L_i = \{\langle\langle i,j\rangle,\langle i+1,k\rangle\rangle : j,k < 4\}$$

for $i < n$. By $f = ef = fe,\ ff^{-1} = e$ and $f^n = 1',\ f^k \neq 1'$ for $k < n$, we have $n = n'$ and also

$$\begin{aligned} rep(f) &= \{\langle\langle i,j\rangle,\langle i+1,k\rangle\rangle : i < n,\ j,k < 4\}, \\ rep(s) &= s,\ rep(g) = g. \end{aligned}$$

Furthermore, from $r = sr = rg,\ r \cap rs = r \cap gr = \emptyset$, and the same for r replaced by rs, we obtain

$$rep(r) \cap L_i = r \cap L_i \text{ or } rep(r) \cap L_i = rs \cap L_i$$

for all $i < n$. By $rep(s) = s$ we now have

$$(*)\ \{rep(r) \cap L_i, rep(rs) \cap L_i\} = \{r \cap L_i, rs \cap L_i\}.$$

Using a completely analogous argument, we similarly obtain

$$(**)\ \{rep(b) \cap L_i, rep(bs) \cap L_i\} = \{b \cap L_i, bs \cap L_i\}.$$

Thus, A' is very similar to A_n.

Assume that A' is Galois closed. Since $n \geq 8$, r^4 is an atom of A'; hence, for each $j < 4$ there is a base automorphism taking $\langle\langle 0,0\rangle,\langle 4,0\rangle\rangle$ to $\langle\langle 0,0\rangle,\langle 4,j\rangle\rangle$. It follows that there are at least four base automorphisms which fix $\langle 0,0\rangle$. However, we shall show that there are at most two such base automorphisms, and consequently, A' cannot be Galois closed.

Assume that h, h', h'' are base automorphisms of A' fixing $\langle 0,0\rangle$, i.e.

$$h(\langle 0,0\rangle) = h'(\langle 0,0\rangle) = h''(\langle 0,0\rangle) = \langle 0,0\rangle.$$

Since base automorphisms preserve the elements of A', $h(e) = e$ implies that $h(\langle 1,0\rangle) = \langle 1,j\rangle$ for some $j < 4$; furthermore, $h(r) = r,\ h(rs) = rs$ show that $j \in \{0,2\}$. As the same hold for h' and h'', we infer that two of h, h', h'' agree on $\langle 1,0\rangle$ as well. Thus, let w.l.o.g. $h(\langle 1,0\rangle) = h'(\langle 1,0\rangle)$.

Next, we show that if two base automorphisms of A' agree on $\langle 0,0\rangle$ and $\langle 1,0\rangle$, then they are equal: Define two equivalence relations on **4** by

$$\begin{aligned}\gamma &= {}^2\{0,2\} \cup {}^2\{1,3\},\\ \chi &= {}^2\{0,3\} \cup {}^2\{1,2\},\end{aligned}$$

and suppose that

$$\begin{aligned}h(\langle 1,0\rangle) &= h'(\langle 1,0\rangle) = \langle i,j\rangle,\\ h(\langle 2,0\rangle) &= \langle 2,k\rangle.\end{aligned}$$

Then,

$$\langle\langle 1,0\rangle,\langle 2,0\rangle\rangle \in rep(r) \cap rep(rs)$$

together with (*) and the fact that h preserves r and rs, imply that k is in the same γ - class as j. Similarily,

$$\langle\langle 0,0\rangle,\langle 2,0\rangle\rangle \in rep(b) \cap rep(bs)$$

together with (**), and the fact that h preserves b and bs, imply that k is in the same χ - class as 0.

Let $h'(\langle 2,0\rangle) = \langle 2,k'\rangle$. By the same argument, k' is in the same γ - class as j and in the same χ - class as 0. It follows that k and k' are in the same γ - class and in the same χ - class. Now, it can be easily checked that the intersection of any γ - class with any χ - class contains exactly one element, and therefore $k = k'$. A completely analogous argument establishes that in fact $h(\langle i,0\rangle) = h'(\langle i,0\rangle)$ for each $i < n$. Again using that h, h' are base automorphisms – in particular that they preserve s and g – we obtain $h = h'$ (Full details of this argument along with some combinatorial background can be found in [2]). This establishes that A' is not Galois closed.

4. *If n is a multiple of* 7, *then* A_n *is permutational*:

This follows from the fact that the "period" of the function we implicitly construct in the preceding paragraph is 7; more on this can be found in [2]. If e.g. $n = 14$, then one can check by hand (or by CAYLEY) that the group H of base automorphisms of A_{14} has 112 elements and is transitive. Consequently, A is permutational. If we translate $\langle i,j\rangle \in U_{14}$ into $i \cdot 4 + j$, then H is generated by the permutations

$$\begin{aligned}\phi = \; & (4\ 6)(5\ 7)(8\ 11)(9\ 10)(12\ 15)(13\ 14)(16\ 17)(18\ 19)\\ & (20\ 22)(21\ 23)(24\ 25)(26\ 27)(32\ 34)(36\ 39)(37\ 38)\\ & (40\ 43)(41\ 42)(44\ 45)(46\ 47)(49\ 51)(52\ 53)(54\ 55),\end{aligned}$$

$$\begin{aligned}\psi = \; & (0\ 52\ 48\ 44\ 40\ 36\ 32\ 28\ 24\ 20\ 16\ 12\ 8\ 4)\\ & (1\ 53\ 49\ 45\ 41\ 37\ 33\ 29\ 25\ 21\ 17\ 13\ 9\ 5)\\ & (2\ 54\ 50\ 46\ 42\ 38\ 34\ 30\ 26\ 22\ 18\ 14\ 10\ 6)\\ & (3\ 55\ 51\ 47\ 43\ 39\ 35\ 31\ 27\ 23\ 19\ 15\ 11\ 7).\end{aligned}$$

This completes the proof. □

Thus, A_{14} is the smallest example of a permutational BRA without Galois closed representation which can be obtained by this construction. It is unknown to us whether any smaller examples exist. It also may be interesting to note that A_{14} is not group representable in the sense of [19], since H does not contain a regular subgroup. A similar statement holds for all representations of A.

Even though in the proof above we exhibited infinitely many permutational RAs without Galois closed representation, these algebras cannot be used to show that having a Galois closed representation cannot be expressed with one first order formula relative to the class of permutational RA's. The reason for this is that any ultraproduct of these algebras is also permutational and does not have a Galois closed representation; this can be seen using the same arguments as in the proof of Proposition 2.5. However, by using the same kind of argument in a more sophisticated way, one can construct a sequence $A_n,\ n < \omega$, of BRAs where each A_n is permutational without Galois closed representation, so that an ultraproduct of these remains permutational, but has a Galois closed representation: In the construction of 2.5, replace 4 by a prime p, s and g by suitable functions, and choose n_p large enough so that A_{n_p} has a "big" atom and n_p is divisible by the period of R and B.

Essential uniqueness has the following not totally unexpected consequence:

Proposition 2.6. *If $A \leq Rel(U)$ is essentially unique, and if $B \leq Rel(U)$ with $A \cong B$, then A^ρ is conjugate to B^ρ*

Proof. Let $h : A \to B$ be an isomorphism, $G = A^\rho,\ H = B^\rho$, and $\phi \in Sym(U)$ with $h(R) = R^\phi$ for each $R \in A$. Furthermore, let $\psi \in G$ and $P \in B$. Then, $P = h(R) = R^\phi$ for some $R \in A$. Now,

$$\begin{aligned}(\phi^{-1}\circ\psi^{-1}\circ\phi)\circ P\circ(\phi^{-1}\circ\psi^{-1}\circ\phi)^{-1} &= (\phi^{-1}\circ\psi^{-1}\circ\phi)\circ\phi^{-1}\circ R\circ\phi\circ(\phi^{-1}\circ\psi^{-1}\circ\phi)^{-1}\\ &= \phi^{-1}\circ\psi^{-1}\circ R\circ\psi\circ\phi\\ &= \phi^{-1}\circ P\circ\phi\\ &= R,\end{aligned}$$

and hence $\phi^{-1}\circ G\circ\phi \leq H$.

Conversely, if $\psi \in H$, then $\phi\circ\psi\circ\phi^{-1} \in G$, and thus $\psi \in \phi^{-1}\circ G\circ\phi$. ☐

The converse is not necessarily true: There are two BRAs A, B on an 11 element set such that $A \cong B$, $A^\rho = B^\rho = \{1'\}$, and A (and hence B) is not essentially unique. We have, however, a partial converse which will be used later:

Proposition 2.7. *Suppose that $A, B \in Rel(U)$ are Galois closed, and that A^ρ and B^ρ are conjugate. Then, $A \cong B$ and for every isomorphism $h : A \to B$ there is some $\phi \in Sym(U)$ such that $h(R) = R^\phi$ for any $R \in A$.*

Proof. Let $G = A^\rho,\ H = B^\rho$, and $H = \psi^{-1}\circ G\circ\psi$ for some $\psi \in Sym(U)$. Recall that for each $\phi \in Sym(U)$, the assignment $R \to \phi^{-1}\circ R\circ\phi$ is an automorphism of $Rel(U)$. Now, set

$$h(G_{x,y}) = \psi^{-1}\circ G_{x,y}\circ\psi.$$

Since $B = H^\sigma$, and $H = \psi^{-1}\circ G\circ\psi$, it is clear that the image of h is B, and that $h(R) = R^\psi$ for any $R \in A$. ☐

Corollary 2.8. *Suppose that all subalgebras of $Rel(U)$ are Galois closed, and that for all Galois closed $G,H \leq Sym(U)$, $G^\sigma \cong H^\sigma$ implies that G and H are conjugate. Then every subalgebra of $Rel(U)$ is essentially unique.* $\square$

We close this section with some observations regarding non integral BRAs:

Proposition 2.9. *Let $A \leq Rel(U)$ have the integral constituents $A_i, i < k$, and set $G = A^\rho$. Then,*

1. *Each U_i is a fixed block of G.*
2. *If M is a union of constituent sets, B is the relative algebra of A with respect to ${}^2M$, and $\phi \in G$, then the restriction ψ of ϕ to M is a base automorphism of B.*
3. *Suppose that*
   (a) *$M = U \setminus U_i$, B is the relative algebra of A with respect to ${}^2M$,*
   (b) *U_{ij} is an atom of A for all $j < k,\ j \neq i$,*
   (c) *$\phi \in A_i^\rho,\ \psi \in B^\rho$.*

   Then, $\phi \cup \psi \in G$.
4. *If each A_i is Galois closed and U_{ij} is an atom of A for all $i, j < k,\ j \neq i$, then A is Galois closed.*

Proof. 1. Suppose w.l.o.g. that $k > 1$, and assume that there are $i, j < k,\ i \neq j,\ x \in U_i,\ y \in U_j$, and some $\phi \in G$ such that $\phi(x) = y$. Then, $\langle x, x\rangle \in E_i$, but $\langle x, x\rangle \notin \phi \circ E_i \circ \phi^{-1}$, contradicting that ϕ is a base automorphism of A.

2. First, note that by 1., M is a fixed block of G, so that $\psi \in Sym(M)$. If $R \in At(B)$, then $R \in At(A)$, and the conclusion follows from $\phi \in A^\rho$.

3. Set $\chi = \phi \cup \psi$, and suppose that $R \in At(A)$. If $R \in B$ or $R \in A_i$, the conclusion follows at once from $\phi \in A_i^\rho$ and $\psi \in B^\rho$.

   Thus, let $R = U_{ij}$ for some $j < k,\ j \neq i$. Then, $\phi \circ R = R$ (since $\phi[U_i] = U_i$ by 1.), and $ran_R(x) = U_j$ for all $x \in U_i$; similarly, $R \circ \psi = R$. So, we have

$$\chi \circ R = \phi \circ R = R = R \circ \phi = R \circ \chi.$$

4. Suppose that $A_i^\rho = H_i$ and $H_i^\sigma = A_i$ for $i < k$. Since each A_i is Galois closed and integral, each H_i is transitive. Let $H \in Sym(U)$ be defined by $\phi \in H \iff \phi_i \in H_i$, P be an atom of A, and $\langle x, y\rangle \in P$.
   (a) $x, y \in U_i$: Since P is an atom of A, we have $dom(P) = ran(P) = U_i$, and P is in fact an atom of A_i. Since $H \restriction U_i = G_i$, we have $H_{x,y} = H_{i_{x,y}} = P$.
   (b) $x \in U_i,\ y \in U_j,\ i \neq j$: Then, $P = U_i \times U_j$ by the hypothesis. Let $\langle u, v\rangle \in P$. Since H_i and H_j are transitive, there are $\phi \in H_i,\ \psi \in H_j$ with $\phi(x) = u$ and $\psi(x) = v$. Set $\chi = \phi \cup \psi$; then, $\chi \in H$ and $\langle x, y\rangle = \langle u, v\rangle$, and it follows that $P \subseteq H_{x,y}$. The converse follows from $P = U_i \times U_j$.

It now follows from (a) and (b) that $H^\sigma = A$.
This finishes the proof. $\square$

3 Logic of Galois closed relation algebras

Throughout this section let A be a finite simple complete and atomic relation algebra with atoms $a_i, i < k$, and $a_j \leq 1'$ for $j < m < k$. The representation language L_A of A is a first order language with equality and the binary relation symbols $R_i,\ i < k$; we sometimes omit the subscript if the context is clear. For any language L, we denote the set of all L - formulas with just one free variable by L^x; the set of all L^x - formulas which contain at most n variables altogether is denoted by L^x_n. The sets $L^{x,y}$ and $L^{x,y}_n$ are defined analogously. The *truth set* def $\phi(x,y)$ of $\phi \in L^{x,y}$ in the model $\langle U, A\rangle$ is the relation

$$\{\langle a,b\rangle \in {}^2U : \langle U,A\rangle \models \phi(a,b)\}.$$

Similarly, we define def $\phi(x)$ for $\phi \in L^x$.

We start with an observation on definable sets:

Proposition 3.1. *Let $A \leq Rel(U)$ and $M \subseteq U$ be not empty. Then, M is definable in $\langle U,A\rangle$ if and only if M is a union of orbits of A^ρ.*

Proof. "$\Rightarrow$: Suppose that $\phi(x)$ is a first order formula in the language of A with one free variable which defines M in the model $\langle U,A\rangle$, and that ψ is a base automorphism of A. Then, $A \models \phi(a)$ implies that $A \models \phi(\psi(a))$, and hence M contains the orbit of each of its elements.

"$\Leftarrow$": Suppose that $G = A^\rho$, M is an orbit of G, $a \in M,\ b \in U$. It is shown in [1], 4.(i) together with 1.4.2. of [16] that each element of $A^{\rho\sigma}$ is definable by a formula $\psi(x,y)$ in the language of A. Now, $G_{a,b}$ is an atom of $A^{\rho\sigma}$ with domain M, and hence, M is definable. $\square$

Let us recall a few facts from [3]: Suppose that B is a representation of A on U with representation language L.

1. A is integral if and only if for any $\phi \in L^x_3$, the sentence $(\exists x)\phi(x) \Rightarrow (\forall x)\phi(x)$ holds in $\langle U,B\rangle$. In other words, no proper and non empty subset of U is definable in the model $\langle U,B\rangle$ by a formula with at most three variables.

2. B is c - permutational if and only if $\langle U,B\rangle \models (\exists x)\phi(x) \Rightarrow (\forall x)\phi(x)$ for any $\phi \in L^x$. In this case, no proper and non empty subset of U is definable, and all $x \in U$ have the same first order properties with respect to the model $\langle U,B\rangle$.

Every integral Galois closed relation algebra is permutational, and we have shown above that the converse is not true. Hence, being Galois closed is stronger than permutational; below, we show the logical background of this phenomenon.

The representation theory of A, denoted by $Th(A)$, is the collection of the following L_A-sentences:

1. $(\forall x)(\forall y)(xR_0y \vee \ldots \vee xR_{k-1}y)$
2. $(\forall x)(\forall y)(xR_iy \Rightarrow \neg\, xR_jy)$ for $i, j < k$ and $i \neq j$
3. For all $i, j, m_0, \ldots, m_{r-1} < k$ and $a_i \circ a_j = a_{m_0} + \ldots + a_{m_{r-1}}$,

$$(\forall x)(\forall y)[(\exists z)(xR_iz \wedge zR_jy) \iff (xR_{m_0}y \vee \ldots \vee xR_{m_{r-1}}y)]$$

A is representable if and only if $Th(A)$ has a model. It was remarked in [4] that a representation of A is essentially unique on U if $Th(A)$ is categorical on $|U|$.

If $\psi \in L^{x,y}$ and $i < k$, then ψ_i denotes the sentence

$$(\exists x)(\exists y)(xR_iy \wedge \psi(x,y)) \Rightarrow (\forall x)(\forall y)(xR_iy \Rightarrow \psi(x,y)).$$

Intuitively, ψ_i says that if ψ can be satisfied on some edge of the atom S_i, then it can be satisfied on all edges of S_i; in other words, all edges of S_i have the same first order properties.

Proposition 3.2. *If A has a Galois closed representation on a finite set, then* $Th(A) \cup \{\psi_i : \psi \in L^{x,y}$ *and* $i < k\}$ *is consistent. Conversely, if* $\langle U, B\rangle$ *is a model of* $Th(A) \cup \{\psi_i : \psi \in L^{x,y}$ *and* $i < k\}$ *and* U *is finite, then* B *is Galois closed.*

Proof. "$\Rightarrow$": Let B be a Galois closed representation of A on the finite set U; then, $\langle U, B\rangle$ is a model of $Th(A)$; furthermore, suppose that R_i is interpreted by the atom S_i of B, and let $G^\sigma = B$. We first observe that for all $u, v \in U$, $\psi(x,y) \in L^{x,y}$, and all base automorphisms ϕ of B,

$$\langle U, B\rangle \models \psi(u, v) \text{ if and only if } \langle U, B\rangle \models \psi(\phi(u), \phi(v)).$$

Suppose that $i < k$ and $u, v \in U$ such that $\langle U, B\rangle \models uS_iv \wedge \psi(u, v)$. Since S_i is an atom of B, we have $S_i = G_{u,v}$. Now, if $\langle u', v'\rangle \in G_{u,v}$, then there is some $\phi \in G$ such that $\phi(u) = u'$ and $\phi(v) = v'$. Since $\langle U, B\rangle \models \psi(u, v)$, we also have $\langle U, B\rangle \models \psi(u', v')$ by the observation above. Hence, $\langle U, B\rangle \models \psi_i$.

"$\Leftarrow$": Conversely, suppose that $\langle U, B\rangle$ is a model of $Th(A) \cup \{\psi_i : \psi \in L^{x,y}$ and $i < k\}$ on the finite set U. Let $\psi(x,y) \in L^{x,y}$, and set $Q = \text{def } \psi(x,y)$ in the model $\langle U, B\rangle$. Suppose that $S_i \cap Q \neq \emptyset$, i. e. that there are $a, b \in U$ such that aS_ib and $\psi(a, b)$ is true in $\langle U, B\rangle$. Since $\langle U, B\rangle \models \psi_i$, we have $S_i \subseteq Q$. Therefore, Q is a union of atoms of B, and thus, B contains every binary relation definable over $\langle U, B\rangle$. Since U is finite, B is Galois closed by [1] 4.(i). □

This implies that being Galois closed is a general first order property for finite models, while one can use techniques similar to those mentioned after 2.5 to show that its negation is not.

4 Clones of operations

In this section we always suppose that the operations under consideration are finitary. Furthermore, if e.g. $\underline{R} = \langle R_0, \ldots, R_{n-1}\rangle \in {}^nRel(U)$, and h is a function on $Rel(U)$, then we assume that $h(\underline{R})$ is defined componentwise; a similar convention holds for permutations. Furthermore, we shall usually write $\phi\langle x, y\rangle$ instead of $\phi(\langle x, y\rangle)$.

A set $\mathcal{C}$ of operations on a set M is called a *clone on M* if

1. $\mathcal{C}$ contains all projections, i.e. all operations $p_i^n : {}^nM \to M$ with

$$p_i^n(m_0, \dots, m_{n-1}) = m_i,$$

for all $n \in \omega$ and $i < n$.

2. $\mathcal{C}$ is closed under composition, i.e. if $f \in \mathcal{C}$ is an n-ary operation and $g_0, \dots, g_{n-1}$ are m-ary operations, then the m-ary operation h with

$$h(a_0, \dots, a_{m-1}) = f(g_0(a_0, \dots, a_{m-1}), \dots, g_{n-1}(a_0, \dots, a_{m-1}))$$

is an element of $\mathcal{C}$.

If O is a set of operations on M, then we say that O *generates the clone* $\mathcal{C}$, if

$$\mathcal{C} = \bigcap\{\mathcal{F} : \mathcal{F} \text{ is a clone on } M \text{ and } O \subseteq \mathcal{F}\}.$$

The *classical clone* $\mathcal{C}_c$ is the clone generated by the basic operations and constants of $Rel(U)$.

Let L be a first order language with equality whose predicate symbols are binary. If $\psi \in L^{x,y}$ contains exactly the predicate variables $P_0, \dots, P_{n-1}$, then ψ defines an n-ary operation f_ψ on $Rel(U)$ by

$$f_\psi(R_0, \dots, R_{n-1}) = \text{def } \psi$$

in the model $\langle U, R_0, \dots, R_{n-1}\rangle$, where P_i is interpreted by R_i for $i < n$. The set of all the operations of this form is also a clone on $Rel(U)$ which we shall call the *logical clone*, and denote it by $\mathcal{C}_l$.

An n-ary operation f on $Rel(U)$ is called *invariant* if for all $\phi \in Sym(U)$ and all $R_0, \dots, R_{n-1} \in Rel(U)$

$$f(R_0^\phi, \dots, R_{n-1}^\phi) = f(R_0, \dots, R_{n-1})^\phi.$$

The set of all invariant operations on $Rel(U)$ is also a clone, denoted by $\mathcal{L}_i$.

Let $\underline{R} \in {}^nU$, and $a, b \in U$. Define an n-ary operation $F_{\underline{R},a,b}$ on $Rel(U)$ by

$$F_{\underline{R},a,b}(\underline{S}) = \{\langle x,y\rangle \in {}^2U : \langle U, \underline{R}, a, b\rangle \cong \langle U, \underline{S}, x, y\rangle\}.$$

In other words, $F_{\underline{R},a,b}(S) = \{\phi\langle a,b\rangle : \phi \in Sym(U) \text{ and } \underline{R} = \underline{S}^\phi\}$.

The following basic result on these clones can be found in [16]; there, U is not necessarily a finite set:

Proposition 4.1. *1. If U is not empty, then $\mathcal{C}_c \subseteq \mathcal{C}_l \subseteq \mathcal{C}_i$. If U is finite, then $\mathcal{C}_l = \mathcal{C}_i$.*

2. *$F_{\underline{R},a,b} = F_{\underline{S},c,d}$ iff $\langle U, \underline{R}, a, b\rangle \cong \langle U, \underline{S}, c, d\rangle$, otherwise, $F_{\underline{R},a,b} \cap F_{\underline{S},c,d} = \emptyset$.*

3. *The n-ary operations in $\mathcal{C}_i$ form a complete and atomic Boolean algebra with atom set $\{F_{\underline{R},a,b} : \underline{R} \in {}^nRel(U),\ a, b \in U\}$.* □

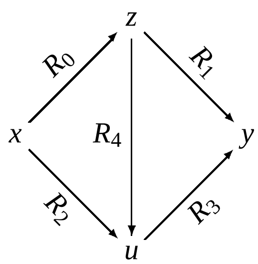
It is well known that $\mathcal{C}_l \neq \mathcal{C}_i$ if U is infinite: Transitive closure is an example of an invariant operation which is not first order definable on an infinite set; consequently, there is no global definition of transitive closure in first order logic in the sense that there is no formula ψ of $L^{x,y}$ such that for any binary relation R on a finite set the transitive closure of R is def ψ, see for instance [16] for a proof. It is of considerable interest to find a logic not involving linear order in which exactly the polynomial time computable invariant operations are expressible, or to show that there is no such logic (see [11] and [13] for further discussion and references).

Given a clone $\mathcal{C}$ on $Rel(U)$, the notation $A \leq \langle Rel(U), \mathcal{C}\rangle$ means that A is a subalgebra of $Rel(U)$ with respect to the operations in $\mathcal{C}$. If $\mathcal{C}_c \subseteq \mathcal{C}$, then A is a relation algebra, and thus the concepts of base automorphism and Galois closure as defined above apply.

We also consider the quinary operation Q on $Rel(U)$ which is defined by

$$xQ(R_0,\ldots,R_4)y \iff (\exists z)(\exists u)(xR_0zR_1y \wedge xR_2uR_3y \wedge zR_4u).$$

The situation that $\langle x,y\rangle \in Q(R_0,\ldots,R_4)$ is pictured below [1]:



It is shown in [16] that $Q \notin \mathcal{C}_c$ if $|U| \geq 25$, and it was asked in the draft version of [16] for which $|U|$ the operation Q is a member of the classical clone on U. To answer this question was, indeed, the starting point of this paper from which it has developed through numerous revisions (and several years) to its present form.

Proposition 4.2. *$Q \in \mathcal{C}_c$ if and only if $|U| \leq 6$.*

Proof. "⇒": Consider the algebra $A \leq Rel(\mathbf{7})$ introduced in 2.3.1 There,

$$Q(S,S,S,S,S) = 1' \cup {}^2\{3,4,5,6\},$$

which is not an element of A. More generally, for $n \geq 7$, set $M_0 = \{0,1,2\}$, $M_1 = \{3,4,\ldots,n-1\}$ and let A be generated by $S = {}^2M_0 \cup {}^2M_1$. Then, $Q(S,S,S,S,S) = 1' \cup {}^2M_1 \notin A$.

"⇐": This will follow from the next two results. □

The rest of the paper will characterize those sets U, for which $\mathcal{C}_c = \mathcal{C}_i$; it will turn out that the magic number is 6. The proof will be done in two stages: We first give a condition for a clone $\mathcal{C}$ which contains $\mathcal{C}_c$ to be equal to $\mathcal{C}_i$, and then we shall show that $\mathcal{C}_c$ fulfills this condition if and only if $|U| \leq 6$.

[1] The diagram was drawn using Paul Taylor's *Commutative Diagrams in TEX* macro package.

As a preparation for the first part, we need one more concept: For a set D, the *ternary discriminator* is an operation τ on D which satisfies

$$\tau(a,b,c) = \begin{cases} c, & \text{if } a = b \\ a, & \text{otherwise} \end{cases}$$

The classical clone contains the ternary discriminator via

$$\tau(P,Q,R) = [({}^2U \circ (P \oplus Q) \circ {}^2U) \cap P] \cup [-({}^2U \circ (P \oplus Q) \circ {}^2U) \cap R],$$

where $\oplus$ denotes symmetric difference.

Proposition 4.3. *Let U be a finite set, and $\mathcal{C}$ be a clone on $Rel(U)$ such that $\mathcal{C}_c \subseteq \mathcal{C} \subseteq \mathcal{C}_i$. If every subalgebra of $\langle Rel(U), \mathcal{C}\rangle$ is Galois closed and essentially unique, then $\mathcal{C} = \mathcal{C}_i$.*

Proof. By 4.1 it suffices to show that $\mathcal{C}$ contains the operations $F_{\underline{R},a,b}$ for each $n \geq 1$, and all $\underline{R} \in {}^nRel(U)$, $a,b \in U$. Since $\mathcal{C}_c \subseteq \mathcal{C}$, and $\mathcal{C}_c$ contains the ternary discriminator, so does $\mathcal{C}$. In other words, $\mathcal{C}$ is quasi - primal in the terminology of [10], p. 403, and by the characterization of these clones given in [10], we need to prove that

1. Each $F_{\underline{R},a,b}$ preserves subalgebras, i.e. whenever $\underline{S} \in {}^nRel(U)$, then $F_{\underline{R},a,b}(\underline{S})$ is contained in the subalgebra of $\langle Rel(U), \mathcal{C}\rangle$ generated by $\{S_0, \ldots, S_{n-1}\}$.

2. Each $F_{\underline{R},a,b}$ preserves internal isomorphisms, i.e. whenever $A, B \leq \langle Rel(U), \mathcal{C}\rangle$ and $h : A \to B$ is a $\mathcal{C}$-isomorphism, then, for all $\underline{S} \in {}^nA$,

$$F_{\underline{R},a,b}(h(S_0), \ldots, h(S_{n-1})) = h(F_{\underline{R},a,b}(\underline{S})).$$

1. If $\langle U, \underline{R}\rangle$ and $\langle U, \underline{S}\rangle$ are not isomorphic as first order structures, then $F_{\underline{R},a,b}(\underline{S}) = \emptyset$, and 1. is trivially fulfilled. If, on the other hand, $\langle U, \underline{R}\rangle \cong \langle U, \underline{S}\rangle$, then there is some $\phi \in Sym(U)$ such that $\underline{R}^\phi = \underline{S}$, and by 4.1.2 we have

$$F_{\underline{R},a,b}(S) = F_{\underline{S},\phi(a),\phi(b)}(\underline{S}) = \{\langle \pi(\phi(a)), \pi\phi(b)\rangle : \pi \in \langle \underline{S}\rangle^\sigma\}$$

which is the atom of the Galois closure of $\langle \underline{S}\rangle$ which contains $\langle \phi(a), \phi(b)\rangle$. Since $\langle \underline{S}\rangle$ is Galois closed by the hypothesis it contains $F_{\underline{R},a,b}(\underline{S})$.

2. Let $A, B \leq \langle Rel(U), \mathcal{C}\rangle$, and $h : A \to B$ be a $\mathcal{C}$-isomorphism. Since A is essentially unique, there is some $\psi \in Sym(U)$ such that

$$h(T) = T^\psi = \psi^{-1} \circ T \circ \psi$$

for all $T \in A$. Let $\underline{S} \in {}^nA$. Now,

$$\begin{aligned} F_{\underline{R},a,b}(h(\underline{S})) &= F_{\underline{R},a,b}(\underline{S}^\psi) \\ &= \{\pi\langle a,b\rangle : \pi \in Sym(U),\ \underline{R}^\pi = \underline{S}^\psi\} \\ &= \{\psi\psi^{-1}\pi\langle a,b\rangle : \pi \in Sym(U),\ \underline{R}^{\pi\psi^{-1}} = \underline{S}\} \\ &= \{\psi\delta\langle a,b\rangle : \delta \in Sym(U),\ \underline{R}^\delta = \underline{S}\} \\ &= (F_{\underline{R},a,b}(\underline{S}))^\psi \\ &= h(F_{\underline{R},a,b}(\underline{S})). \end{aligned}$$

This completes the proof of 4.3. ☐

We can now prove the main result of this section:

Proposition 4.4. *$\mathcal{C}_c = \mathcal{C}_i$ if and only if $|U| \leq 6$.*

Remark: Before we embark on the long and sometimes tedious proof we comment on the logical consequences of this result. Let L be a first order language with equality and binary predicate symbols $P_0, \dots, P_{n-1}$, and let $\langle U, R_0, \dots, R_{n-1} \rangle$ be a model of L. Because of 1.1 above, a binary relation S is in the image of an operator $F \in \mathcal{C}_c$ with arguments among the R_i if and only if S is definable by a formula of $L^{x,y}$ with at most three variables. On the other hand if we choose $F \in \mathcal{C}_i = \mathcal{C}_l$, then the results will be the relations definable by any finite number of variables, and the resulting relations will, in fact, form the Galois closure of $\langle R_0, \dots, R_{n-1} \rangle$. Thus, the proposition implies the surprising fact that on a set U with at most six elements, relation algebra logic (i.e. logic with three variables) is as powerful as first order logic. It would be interesting to know, whether this result carries over in some form to larger n, e.g. whether $n-3$ or even $\lfloor \log_2(n) \rfloor + 1$ variables suffice on an n-element set.

Proof. "$\Rightarrow$": This follows from (the already proven part of) 4.2, since Q is first order definable.

"$\Leftarrow$": By 4.3 it suffices to show that for $|U| \leq 6$, every subalgebra of $Rel(U)$ is Galois closed and essentially unique. For $|U| \leq 5$ this was already obtained in [16]. Thus, let $U = \{0, \dots, 5\}$.

The lattice of subgroups of $Sym(U)$ has 56 conjugacy classes, and we have checked that whenever Galois closed $G, H \leq Sym(U)$ are not conjugate, then G^σ is not isomorphic to H^σ. Thus, if all subalgebras of $Rel(U)$ are Galois closed, then they will be essentially unique by 2.8.

First, let $A \leq Rel(U)$ be integral. There are several cases and subcases:

1. *A has six atoms*: Then, each $R \in At(A)$ is a permutation by 1.3, and hence A is Galois closed by 2.1.

2. *A cannot have exactly five atoms*: If A had five atoms, three of these would be semiregular permutations because A is integral. Any three semiregular permutations of U, however, generate an algebra with six atoms.

3. *A has exactly four atoms*: Let $At(A) = \{1', R, S, T\}$; at least one of these is a semiregular permutation, say, R.

3.1. *R has order three*: Then, R consists of two cycles, say, $R = (024)(135)$. We see that R generates A, and A has the following relative composition table:

$\circ$	R	S	T
R	S	$1'$	T
S	$1'$	R	T
T	T	T	$-T$

If $G \leq Sym(U)$ is generated by the permutations (042), (153), and $(03)(12)(45)$, then $G^\sigma = A$.

3.2. *R has order two*: Then, by 1.3.1 and the argument used in 2. above, we have $|ran_S(x)| = |ran_T(x)| = 2$ for all $x \in U$, and the same holds for the domains. Furthermore, for $P \in \{S,T\}$,

$$(R \circ P) \cap P = (R \circ P) \cap R = (P \circ R) \cap R = \emptyset,$$

since $R = R^{-1}$. It follows that $S \circ R = S$ or $S \circ R = T$.

3.2.1. $S \circ R = S$: Then, $(S \circ R) \cap T = \emptyset$, and hence $(T \circ R) \cap S = \emptyset$. It follows that $T \circ R = T$. Therefore, the range of each $x \in U$ in S or T is a cycle of R.

Suppose that the cycles of R are D, E, F, and that $x \in D$ with $ran_s(x) = E$. Assume that $S = S^{-1}$, and let $y \in E$. Then, ySx, and therefore $ran_S(y) = D$. Hence, if $z \in F$ and zRu, then $u \in F$, contradicting that $R \cap S = \emptyset$. Thus, $S^{-1} = T$, and the S-ranges of cycles of R are a cyclic permutation of these cycles.

Let w.l.o.g. $R = (01)(23)(45)$, and S be defined by

$$\begin{array}{ccc} 0,1 & \to & 2,4 \\ 2,3 & \to & 4,5 \\ 4,5 & \to & 0,1 \end{array}$$

The algebra A generated by R and S has the relative composition table

$\circ$	R	S	T
R	$1'$	S	T
S	S	T	$1' \cup R$
T	T	$1' \cup R$	S

If $G \in Sym(U)$ is generated by $(025)(134)$ and $(034)(125)$, then $G^\sigma = A$.

3.2.2. $S \circ R = T$: Then, for any $x \in U$ the S-range of x intersects those two cycles of R which do not contain x, each in exactly one element. Let w.l.o.g. $R = (03)(12)(45)$, and $ran_S(0) = \{1,5\}$; then, $ran_S(3) = \{2,4\}$.

Assume that $S^{-1} = T$. Then, we have the following partial matrix for S:

$$\begin{array}{ccl} 0 & \to & 1,5 \\ 1 & \to & 3, \text{ one of } 4,5 \\ 2 & \to & 0, \text{ one of } 4,5 \\ 3 & \to & 2,4 \\ 4 & \to & 0, \text{ one of } 1,2 \\ 5 & \to & 3, \text{ one of } 1,2. \end{array}$$

It is routine to check that none of these possibilities generates an algebra with exactly four atoms.

Thus, S and T are symmetric. We then have the following partial matrix for S:

$$\begin{array}{lll} 0 & \to & 1,5 \\ 1 & \to & 0, \text{ one of } 4,5 \\ 2 & \to & 3, \text{ one of } 4,5 \\ 3 & \to & 2,4 \\ 4 & \to & 3, \text{ one of } 1,2 \\ 5 & \to & 0, \text{ one of } 1,2. \end{array}$$

Depending on whether $1S4$ or $1S5$, we obtain the two isomorphic algebras A_1 and A_2, whose tables of relative multiplication are given by Table 1 and Table 2, respectively. If $G \leq Sym(U)$ is generated

Table 1: A_1, $\langle 1,4\rangle \in S$

$\circ$	R	S	T
R	$1'$	T	S
S	T	$1' \cup T$	$S \cup R$
T	S	$S \cup R$	$1' \cup T$

Table 2: A_2, $\langle 1,5\rangle \in S$

$\circ$	R	S	T
R	$1'$	T	S
S	T	$1' \cup S$	$T \cup R$
T	S	$T \cup R$	$1' \cup S$

by $(042)(135)$, $(02)(13)$, and $(01)(23)(45)$, then, $G^\sigma = A_1$. If $H \leq Sym(U)$ is generated by $(01)(23)$ and $(03)(14)(25)$, then $H^\sigma = A_2$. Observe that G and H are conjugate via $(014)(253)$.

4. *A has exactly three atoms*: There are two possible types, both of which are essentially unique (see [4]). Let $\phi = (012345)$.

4.1. If A is generated by $\phi \cup \phi^3 \cup \phi^5$, then $A = G^\sigma$, where G is generated by ϕ and (02).

4.2. If A is generated by ϕ^3, then $A = G^\sigma$, where G is generated by ϕ and $(01)(34)$.

This covers the case of the integral subalgebras of $Rel(U)$.

Now, suppose that $A \leq Rel(U)$ is not integral with constituent sets $U_i, i < k$. By 2.9 we can suppose that each constituent set of A has more than one element, and that some $U_{ij}, i \neq j$ is not an atom of A.

1. *A has three constituent sets*: Then, each constituent set has exactly two elements. Suppose that $U_0 = \{0,1\}$, $U_1 = \{2,3\}$, $U_2 = \{4,5\}$. If each atom of A is functional, then A is Galois closed by 2.1. Otherwise, let w.l.o.g. $\{\langle 0,2\rangle, \langle 1,3\rangle\}$, $U_{02} \in At(A)$. Then, $A = G^\sigma$, where G is generated by $(01)(23)$ and (45).

2. *A has two constituent sets*: There are two possibilities.

2.1. $|U_0| = |U_1| = 3$, $U_0 = \{0,2,4\}$, $U_1 = \{1,3,5\}$: If A_1 or A_2 has three atoms, then – keeping in mind that U_{01} is not an atom by our hypothesis – all atoms of A are functional, and A is Galois closed by 2.1.

Otherwise, both A_0 and A_1 have two atoms, and A is generated by a bijection $U_0 \to U_1$, say, $R = \{\langle 0,3\rangle, \langle 2,1\rangle, \langle 4,5\rangle\}$. Then, $A = G^\sigma$, where G is generated by $(01)(23)$ and (45).

2.2. $|U_0| = 4$, $|U_1| = 2$, $U_0 = \{0,1,2,3\}$, $U_1 = \{4,5\}$: Since U_{01} is split, A_0 cannot have exactly two atoms; furthermore, U_{01} is split into exactly two atoms P and Q, each of which is functional. There are three possibilities for A_0, and each of them determines of U_{01} is split:

2.2.1. *A_0 is generated by a cycle*: Let w.l.o.g. (0123) generate A_0. Then, we must have $ran_p(0) = ran_P(1)$, and we find that $A = G^\sigma$, where G is generated by $(0213)(45)$.

2.2.2. *A_0 is generated by two permutations of order two*: Suppose w.l.o.g. that $(02)(13)$ and $(01)(23)$ generate A_0. Again, $ran_P(0) = ran_P(1)$, and $A = G^\sigma$, where G is generated by $(01)(23)$ and $(03)(12)(45)$.

2.2.3. *A_0 is generated by one permutation of order two*: If A_0 is generated by $(01)(23)$, then $ran_P(0) = ran_P(1)$, and $A = G^\sigma$, where G is generated by $(0213)(45)$ and (23).

This concludes the proof of 4.4. □

We should like to close with the observation that two Galois closed algebras which are isomorphic as relation algebras on the same base set, need not be essentially unique: Consider $|U| = n \cdot m$, where $3 \leq n,m$, and $n \neq m$. Let S be a disjoint union of n K_m's, and T be the disjoint union of m K_n's. S and T generate isomorphic and Galois closed subalgebras A and B of $Rel(U)$, but they are clearly not isomorphic as first order structures; adding invariant operations to $\mathcal{C}_c$ will eventually destroy the isomorphism. It would be of interest to know whether there is a clone $\mathcal{C}$ with $\mathcal{C}_c \subseteq \mathcal{C} \subsetneq \mathcal{C}_i$ such that all subalgebras of $\langle U, \mathcal{C}\rangle$ are Galois closed and A is $\mathcal{C}$-isomorphic to B.

References

[1] H Andréka and I Németi, *On Jónsson's clones of operations on binary relations*, In Andréka et al. [5], pp. 431–442.

[2] Hajnal Andréka, Ivo Düntsch, and István Németi, *A non permutational integral relation algebra*, Michigan Math. J. **39** (1992), 371–384.

[3] ———, *Expressibility of properties of relations*, Journal of Symbolic Logic **60** (1995), no. 3, 970–991.

[4] Hajnal Andréka and Roger Maddux, *Representations for small relation algebras*, Notre Dame Journal of Formal Logic **35** (1994), no. 4, 550–562.

[5] Hajnal Andréka, J. Donald Monk, and István Németi (eds.), *Algebraic logic*, Colloquia Mathematica Societatis János Bolyai, vol. 54, North Holland, Amsterdam, 1991.

[6] N. L. Biggs and A. T. White, *Permutation groups and combinatorial structures*, LMS Lecture Note Series **33** (1979).

[7] John Cannon, *A language for group theory*, Tech. report, University of Sidney, 1987.

[8] Ivo Düntsch, *A microcomputer based system for small relation algebras*, J. Symb. Comput. **18** (1994), 83–86.

[9] Ron Fagin, *Finite model theory - a personal perspective*, Springer Lecture Notes in Computer Science **470** (1987), 3–24.

[10] George Grätzer, *Universal algebra*, 2 ed., Springer, Berlin, 1979.

[11] Y. Gurevich, *Toward a logic tailored for computational complexity*, Computation and Proof Theory, Lecture Notes in Mathematics 1104 (M. M. Richter, ed.), Springer-Verlag, 1984, pp. 175–216.

[12] Neil Immerman, *Upper and lower bounds for first order expressibility*, Journal of Computer and System Sciences **25** (1982), 76–98.

[13] ______, *Languages that capture complexity classes*, SIAM Journal of Computing **16** (1987), 760–778.

[14] Neil Immerman and Dexter Kozen, *Definability with a bounded number of variables*, Information and Computation **83** (1989), 121–139.

[15] Bjarni Jónsson, *Maximal algebras of binary relations*, Contemporary Mathematics **33** (1984), 299–307.

[16] ______, *The theory of binary relations*, In Andréka et al. [5], pp. 245–292.

[17] Bjarni Jónsson and Alfred Tarski, *Boolean algebras with operators II*, Amer. J. Math. **74** (1952), 127–162.

[18] Brendan McKay, *Nauty user guide*, Tech. Report TR-CS-90-02, Australian National University, 1990.

[19] Ralph McKenzie, *Representations of integral relation algebras*, Michigan Mathematical Journal **17** (1970), 279–287.

[20] Alfred Tarski and Steven Givant, *A formalization of set theory without variables*, Colloquium Publications, vol. 41, Amer. Math. Soc., Providence, 1987.

[21] H. Wielandt, *Finite permutation groups*, Academic Press, 1964.