TUM

INSTITUT FÜR INFORMATIK

Symmetric Quotients

Rudolf Berghammer, Gunther Schmidt, Hans Zierer

TUM-I8620
NOVEMBER 1986

TECHNISCHE UNIVERSITÄT MÜNCHEN

TUM -INFO-11-86-I20-300/1- FMI

Anforderungen an: Bibliothek der Fakultät
für Mathematik und Informatik
Technische Universität München
Arcisstr. 21 / Postfach 202420
D - 8000 München 2 Germany

Druck: Mathematisches Institut und
Institut für Informatik der
Technischen Universität München

Symmetric Quotients

Rudolf Berghammer, Gunther Schmidt, Hans Zierer

Technische Universität München
Institut für Informatik
Postfach 20 24 20
D–8000 München 2

ABSTRACT:

We introduce the symmetric quotient of two relations as a new construct in abstract relational algebra generalizing the notion of a "noyau" of Riguet (cf. [2]). After exhibiting the main properties of symmetric quotients we study several applications. In particular, connections to ordering relations and powerset constructions are investigated.

TUM – INFO – 8620
November 1986

Contents

1. Introduction

In a Boolean algebra $(X, \wedge, \vee, \bar{\ })$ the symmetric difference of $a, b \in X$ is defined by the expression $\overline{a \vee \bar{b}} \vee \overline{\bar{a} \vee b}$. In this paper we consider a related construct in relational algebra, viz. the symmetric quotient $\overline{A^T\bar{B}} \wedge \overline{\bar{A}^T B}$ of two relations A and B.

As the subsequent sections will be formulated in terms of abstract relational algebra, we present the main features of this calculus in Chapter 2.

In Chapter 3 we motivate the definition of the symmetric quotient and exhibit its main properties. In particular, we look for properties in connection with special relations, e.g. equivalence relations or mappings.

In Chapter 4 applications of the symmetric quotient are studied. First, we discuss the univalent and the properly ambiguous part of a relation. The univalent part can easily be defined in terms of symmetric quotients. Section 4.2 is devoted to ordering relations. For a given ordering relation on a set M and a subset N of M we consider special sets and elements, e.g. the set of majorants of N, using relational algebraic means. We show that these notions can also be described by symmetric quotients making formal manipulations easier.

Relations between a set M and its powerset $\mathcal{P}(M)$ are investigated in Section 4.3. Using the symmetric quotient we give a monomorphic characterization of the powerset $\mathcal{P}(M)$. Then we introduce the usual inclusion ordering on $\mathcal{P}(M)$ and prove that $\mathcal{P}(M)$ together with this ordering relation is a complete lattice. Some properties of the "is-element-of" relation between M and $\mathcal{P}(M)$ can also be described by symmetric quotients. Eventually, symmetric quotients are used to establish an isomorphism between the subsets of M and the elements of $\mathcal{P}(M)$. All proofs are given by relational algebraic means.

It seems worth mentioning that the technique explained in Section 4.3 can easily be extended to function domain constructions. Therefore, applications in theoretical computer science are also possible, see [7].

2. Relational Algebraic Preliminaries

This section deals with the fundamental concepts of an abstract relational algebra. We also define relations fulfilling certain properties. In the homogeneous case we investigate ordering relations, in the heterogeneous case we look for "quasifunctional" properties such as uniqueness, totality and so on. Finally, we introduce the concept of homomorphism and isomorphism.

2.1. Relational Algebra

For a comprehensive explanation of the basic concepts of a relational algebra we refer to [3, 4], where more details are presented.

The essence of a relational algebra R is easily communicated by saying that it is a category $(Obj(R), Mor(R))$:

- The objects of R are sets.
- For $X, Y \in Obj(R)$ the morphisms $Mor(X, Y)$ constitute a set, as well. In addition these sets are complete atomistic Boolean algebras $(Mor(X, Y), \wedge, \vee, \bar{\ }, \subset)$.
- There is a correspondence between $Mor(X, Y)$ and $Mor(Y, X)$, given by transposition $R \to R^T$, and between $Mor(X, Y)$, $Mor(Y, Z)$, and $Mor(X, Z)$, established by composition $(R,S) \to RS$. Furthermore, we postulate the **Dedekind rule**

  $$RS \wedge Q \subset (R \wedge QS^T)(S \wedge R^TQ)$$

  and the **Tarski rule**

  $$R \neq O_{XY} \implies L_{WX} R L_{YZ} = L_{WZ}.$$

Here O_{XY} and L_{XY} denote the null element and the universal element in the Boolean algebra $Mor(X, Y)$, respectively. Since the sets X and Y are usually understood, we denote O_{XY}, L_{XY} and the identity I_{XX} by O, L and I, for simplicity.

We call an element $R \in Mor(X, Y)$ a (heterogeneous) **relation**. In the case $X = Y$, R is called **homogeneous**.

All the well-known rules for composition of relations hold in a relational algebra. They may be deduced from the axioms.

We note:

$$\begin{array}{ll} (R^T)^T = R & R \subset S \implies R^T \subset S^T \\ R^T S^T = (SR)^T & \overline{R}^T = \overline{R^T} \\ R \subset S \implies QR \subset QS & R \subset S \implies RQ \subset SQ \\ R(S \wedge Q) \subset RS \wedge RQ & R(S \vee Q) = RS \vee RQ \\ (R \wedge S)^T = R^T \wedge S^T & (R \vee S)^T = R^T \vee S^T. \end{array}$$

In addition we have the so-called Schröder rule

$$RS \subset Q \iff R^T\overline{Q} \subset \overline{S} \iff \overline{Q}S^T \subset \overline{R}.$$

These two equivalences are equivalent to the Dedekind rule.

2.2. Special Heterogeneous Relations

A relation R is called **unique**, if $R^TR \subset I$ or, equivalently, if $R\overline{I} \subset \overline{R}$. If one of the three equivalent conditions $I \subset RR^T$, $L = RL$ and $\overline{R} \subset R\overline{I}$ is fulfilled, R will be called **total**. Thus, **mappings** (or **functions**), i.e. total and unique relations, are characterized by $R\overline{I} = \overline{R}$.

If R is unique, then $R(S \wedge Q) = RS \wedge RQ$ and $R\overline{S} \subset \overline{RS}$; if R is total, then $\overline{RS} \subset R\overline{S}$. Therefore, for a function R we have $R\overline{S} = \overline{RS}$ for every relation S.

A relation R is **injective**, if R^T is unique; R is called **surjective**, if R^T is total. Note that these properties are defined for arbitrary relations, not only, as usually, for functions.

If a surjective relation R is contained within an injective relation S, then R and S are equal. This can easily be proved using the Dedekind rule:

$$S = L \wedge S = LR \wedge S \subset (L \wedge SR^T)(R \wedge LS) \subset SR^TR \subset SS^TR \subset R$$

2.3. Special Homogeneous Relations

If R is a homogeneous relation, then R^2 is defined. This leads to the notion of an ordering relation. A **reflexive** (i.e. $I \subset R$) and **transitive** (i.e. $R^2 \subset R$) relation is called a (reflexive) **quasi-ordering relation**. If in addition R is **antisymmetric** (i.e. $R \wedge R^T \subset I$), then R is called a (reflexive) **ordering relation**.

By $R \wedge \overline{I}$ we denote the **irreflexive part** of a reflexive ordering relation R, which is also transitive and antisymmetric.

Equivalence relations are also interesting homogeneous relations. A relation R is an **equivalence relation**, if it is reflexive, transitive and **symmetric** (i.e. $R \subset R^T$).

2.4. Sets and Points

A relation r with $r = rL$ is called **row constant** and always denoted by lower case letters. If we consider a (concrete) relation r as a Boolean matrix $r \in \mathbb{B}^{X \times Y}$, this condition means: Whatever set Z and universal relation $L \in \mathbb{B}^{Y \times Z}$ we choose, an element $x \in X$ is either in relation rL to none of the elements $z \in Z$ or to all elements $z \in Z$.

Relations of this kind may be considered as **subsets** of X, **predicates** on X, or **vectors**. An injective vector $r = rL \neq O$ therefore corresponds to an element of X and is called a **point**.

2.5. Homomorphisms

Let A and B be (heterogeneous) relations. A pair (Ψ, Φ) of relations is called a **homomorphism** from A to B if Ψ and Φ are functions (in the sense of Section 2.2) and $A \subset \Psi B \Phi^T$ holds. An equivalent version of this postulate, which is used in Section 4.3, is $A\Phi \subset \Psi B$. This in turn is equivalent to $\Psi^T A \Phi \subset B$ and to $\Psi^T A \subset B \Phi^T$.

If in addition (Ψ^T, Φ^T) is a homomorphism from B to A, then (Ψ, Φ) is called an **isomorphism**. Therefore, an isomorphism between two relations A and B is characterized by two bijective functions Ψ and Φ, fulfilling $A = \Psi B \Phi^T$ or equivalently $A\Phi = \Psi B$. Clearly, the composition $(\Psi_1\Psi_2, \Phi_1\Phi_2)$ of two homomorphisms (isomorphisms) (Ψ_1, Φ_1) and (Ψ_2, Φ_2) also is a homomorphism (isomorphism).

If A and B are homogeneous relations, we briefly call Φ a homomorphism (isomorphism) if (Φ, Φ) is a homomorphism (isomorphism) from A to B.

3. Symmetric Quotients

In this section we introduce the notion of the symmetric quotient of two relations and exhibit its basic properties.

3.1. Motivating the Definition

Assume M to be a set and $y \subseteq \mathcal{P}(M)$ to be a subset of its powerset. If we define the set $x \in \mathcal{P}(M)$ to be the union of the members of y, then we may describe this property of x by the expression

$$(1) \quad \bigwedge_{z \in M} (z \in x \iff \bigvee_{w \in y} z \in w).$$

Analogously, we define x to be the intersection of all members of y by

$$(2) \quad \bigwedge_{z \in M} (z \in x \iff \bigwedge_{w \in y} z \in w).$$

As another example, we consider an ordering relation $\leqq$ on a set M. If y is a subset of M, then the element $x \in M$ is the greatest element of y, if and only if

$$(3) \quad \bigwedge_{z \in M} (z \leqq x \iff \bigvee_{w \in y} z \leqq w)$$

holds. Analogously, we can describe the least element of y.

We give a third example: If M is a set, then the equality of two subsets x and y of M is given by the expression

$$(4) \quad \bigwedge_{z \in M} (z \in x \iff z \in y).$$

Now let us compare the expressions given in (1) through (4). Obviously all of them may be described by the scheme

$$(5) \quad \bigwedge_{z \in M} (A(z, x) \iff B(z, y))$$

where $A \in \mathbb{B}^{M \times X}$ and $B \in \mathbb{B}^{M \times Y}$ are (concrete) relations, the variable x ranges over X and the variable y over Y.

For example, in (4) the relation A and the relation B both are defined as the "is-element-of"-relation $\in$ between the set M and the powerset $\mathcal{P}(M)$. The other examples are a little bit more complicated, because B is a product of relations.

For convenience, we now convert (5) into a more algebraic form. Using the definition of composition, transposition, and negation of concrete relations, cf. [1, 2, 5], we get

$$(6) \quad \overline{\bigvee_{z \in M} A^T(x,z) \wedge \overline{B}(z,y)} \wedge \overline{\bigvee_{z \in M} \overline{A^T}(x,z) \vee B(z,y)}\,.$$

As x and y range over X and Y respectively, this expression defines a new relation in $\mathbb{B}^{X\times Y}$ depending on A and B. This new relation associates an element $x \in X$ with an element $y \in Y$, if and only if the two sets $M_x := \{z \in M : A(z,x)\}$ and $M_y := \{z \in M : B(z,y)\}$ coincide.

We now forget the notation with components and present (6) in terms of abstract relational algebra. This leads to the following

3.1.1 Definition. Let A and B be relations. If the following products exist, we call $\mathrm{syq}(A, B) := \overline{A^T\overline{B}} \wedge \overline{\overline{A}^T B}$ the **symmetric quotient** of A and B.

We denote syq(A, A) by noy(A) resembling the french notion of a noyau that can already be found in [2].

3.2. Basic Properties

As we have defined the symmetric quotient in terms of abstract relational algebra, the proofs are also given in this fashion.

Some particular useful properties are summarized in a first statement. The proofs are obvious.

$$(7)\qquad \mathrm{syq}(\overline{A}, \overline{B}) = \mathrm{syq}(A, B) \quad\text{and}\quad \mathrm{syq}(B, A) = \mathrm{syq}(A, B)^T$$

Note that in general syq(A, B) is not symmetric in the sense of Section 2.3.

If R and S are two relations, then $RS \subset RS$ by Schröder's rule is equivalent to $R^T\overline{RS} \subset \overline{S}$ and to $\overline{RS}^T R \subset \overline{S}^T$. This shows that the symmetric quotient is expanded by arbitrary left factors, i.e.

$$(8)\qquad \mathrm{syq}(A, B) \subset \mathrm{syq}(CA, CB) \quad \text{for every } C.$$

As a partial justification of the wording "symmetric quotient", we prove the

3.2.1 Theorem. If A and B are relations, then we have

$$A\,\mathrm{syq}(A, B) = B \wedge L\,\mathrm{syq}(A, B) \subset B.$$

In particular, the equality $A\,\mathrm{syq}(A, B) = B$ holds, if syq(A, B) is surjective.

Proof: By Schröder's rule we get $A\overline{A^T\overline{B}} \subset B$ from $A^T\overline{B} \subset A^T\overline{B}$. This shows the inclusion "$\subset$". Using (7), $A\,\mathrm{syq}(A, B) \subset B$ leads to $\overline{A}\,\mathrm{syq}(A, B) \subset \overline{B}$. Finally,

$$\begin{aligned} B \wedge L\,\mathrm{syq}(A, B) &= B \wedge (\overline{A}\,\mathrm{syq}(A, B) \vee A\,\mathrm{syq}(A, B)) \\ &\subset (B \wedge \overline{B}) \vee A\,\mathrm{syq}(A, B) \\ &= A\,\mathrm{syq}(A, B) \end{aligned}$$

shows the opposite inclusion. Surjectivity $L = L\,\mathrm{syq}(A, B)$ immediately implies the second assertion. □

If A and B are chosen to be equal in this theorem, we get for all A

$$(9)\qquad A\,\mathrm{syq}(A, A) = A\,\mathrm{noy}(A) = A,$$

since by Schröder's rule $AI \subset A$ is equivalent to $A^T\overline{A} \subset \overline{I}$, so that $I \subset \mathrm{syq}(A, A)$.

Theorem 3.2.1 shows that the symmetric quotient is a solution of the inequality $AR \subset B$. But syq(A, B) is not an arbitrary solution. In fact, it is the greatest relation solving $AR \subset B$ as well as $RB^T \subset A^T$. This property leads to a descriptive characterization of the symmetric quotient without the use of negation.

Defining the set $M_{A,B}$ of relations by

$$M_{A,B} = \{R \mid AR \subset B \text{ and } RB^T \subset A^T\},$$

we obtain $\mathrm{syq}(A, B) \in M_{A,B}$ by Theorem 3.2.1. Now let R be an arbitrary element of $M_{A,B}$. Then Schröder's rule yields $R \subset \mathrm{syq}(A, B)$ as

$$AR \subset B \iff A^T\overline{B} \subset \overline{R} \iff R \subset \overline{A^T\overline{B}} \quad\text{and}$$

$$RB^T \subset A^T \iff \overline{A}^T B \subset \overline{R} \iff R \subset \overline{\overline{A}^T B}\,.$$

Therefore, syq(A, B) is the greatest element of $M_{A,B}$.

Fractions or quotients can be reduced. Symmetric quotients have a similar property:

3.2.2 Theorem If A, B, and C are relations, then

$$\mathrm{syq}(A, B)\,\mathrm{syq}(B, C) = \mathrm{syq}(A, C) \wedge \mathrm{syq}(A, B)\,L \subset \mathrm{syq}(A, C)\,,$$

$$\mathrm{syq}(A, B)\,\mathrm{syq}(B, C) = \mathrm{syq}(A, C) \wedge L\,\mathrm{syq}(B, C) \subset \mathrm{syq}(A, C)\,.$$

In particular,

$$\mathrm{syq}(A, A)\,\mathrm{syq}(A, B) = \mathrm{syq}(A, B) \quad\text{and}\quad \mathrm{syq}(A, B)\,\mathrm{syq}(B, A) \subset \mathrm{syq}(A, A)\,.$$

Proof: From (7) and Theorem 3.2.1 we obtain

$$\begin{aligned} \overline{\mathrm{syq}(A, C)}\,\mathrm{syq}(B, C)^T &= \overline{\mathrm{syq}(A, C)}\,\mathrm{syq}(C, B) \\ &= A^T\overline{C}\ \mathrm{syq}(\overline{C}, \overline{B}) \vee \overline{A}^T C\ \mathrm{syq}(C, B) \\ &\subset A^T\overline{B} \vee \overline{A}^T B = \overline{\mathrm{syq}(A, B)}\,. \end{aligned}$$

Now Schröder's rule shows the inclusion "$\subset$".

We use this result, (7) and the Dedekind rule to prove "$\supset$". Without loss of generality we only consider the first equation.

$$\begin{aligned} syq(A, C) \wedge syq(A, B)L &\subset (syq(A, B) \wedge L\,syq(A, C))(L \wedge syq(A, B)^T syq(A, C)) \\ &\subset syq(A, B)\,syq(B, A)\,syq(A, C) \\ &\subset syq(A, B)\,syq(B, C)\ . \end{aligned}$$

As a special case one obtains the inclusion $syq(A, A)\,syq(A, B) \subset syq(A, B)$ which actually is an equation due to $syq(A, A) \supset I$. □

Next we look for properties of symmetric quotients in connection with special relations. First, we consider symmetric quotients and equivalence relations.

Clearly, $syq(A, A) = noy(A)$ always is an equivalence relation. Reflexivity is trivial, (7) shows symmetry, and (7) in connection with Theorem 3.2.2 implies transitivity.

Now we characterize equivalence relations in terms of symmetric quotients. We get, cf. [2], the

3.2.3 Theorem. A relation A is an equivalence relation if and only if $A = syq(A, A)$.

Proof: "⟹" If A is an equivalence relation, then $I \subset A$ yields $syq(A, A) \subset A\,syq(A, A) \subset A$. The reverse inclusion follows from transitivity and symmetry since

$$A \subset \overline{A^T\overline{A}} \iff A^T\overline{A} \subset \overline{A} \iff AA \subset A \quad \text{and} \quad A \subset \overline{\overline{A}^T A} \iff A = A^T \subset \overline{A^T\overline{A}}\ .$$

"⟸" is trivial since $syq(A, A)$ is an equivalence relation. □

As a second special kind of relations we consider relations which we characterized in Section 2.2.

The first interesting formula is

(10) A surjective and unique $\implies$ $syq(A, A) = I$.

For the proof we use that $L = A^TL = A^T\overline{A} \vee A^TA$ since A is surjective. Therefore, $syq(A, A) \subset A^TA \subset I$ as A is unique. Reflexivity of the symmetric quotient finally implies equality.

The next theorem shows properties of $syq(A, B)$, if A and B are injective relations.

3.2.4 Theorem If A and B are injective relations, then the symmetric quotient fulfills:

i) $A^TB \subset syq(A, B)$

ii) $A\,syq(A, B) = AL \wedge B$

iii) $B \subset syq(A^T, syq(A, B))$

Proof: i) Since $O = A^T(B \wedge \overline{B}) = A^TB \wedge A^T\overline{B}$ by distributivity, we get $A^TB \subset \overline{A^T\overline{B}}$ and $A^TB \subset \overline{\overline{A}^TB}$ analogously.

ii) The inclusion "⊂" is trivial; "⊃" may be deduced from i) by Dedekind's rule as follows:

$$AL \wedge B \subset (A \wedge BL)(L \wedge A^TB) \subset AA^TB \subset A\,syq(A, B)$$

iii) From i) we obtain $A\,\overline{syq(A, B)} \subset \overline{B}$, from (7) and Theorem 3.2.1 we get

$$B \subset \overline{A\,\overline{syq(A, B)}} \wedge \overline{\overline{A}\,syq(A, B)} = syq(A^T, syq(A, B))\ .$$ □

If R is an injective and surjective relation, then $\overline{S}R = \overline{SR}$ holds for every relation S (cf. 2.2). From this equation the following property is easily derived.

(11) R injective and surjective $\implies$ $\left\{\begin{array}{l} syq(A, B)R = syq(A, BR) \\ \text{for all relations } A \text{ and } B. \end{array}\right.$

Finally, we look for properties of symmetric quotients concerning the universal relation L.

Since $syq(L, L) = L$, we obtain by Theorem 3.2.2 $syq(L, A) = syq(L, L)\,syq(L, A) = L\,syq(L, A)$. Now we use (7) in order to show that $syq(A, L)$ is a vector:

$$syq(A, L)\,L = syq(L, A)^T L^T = syq(L, A)^T = syq(A, L).$$

The last theorem of this section gives a condition on two relations A and B for $syq(A, B)$ to be a universal relation.

3.2.5 Theorem If A and B are relations, then

$$syq(A, B) = L \iff A \text{ and } B \text{ are vectors and } AL = BL.$$

Proof: "⟹" By Schröder's rule we conclude

$$L \subset syq(A, B) \implies A^T\overline{B} \subset O \iff AL \subset B$$

and

$$L \subset syq(A, B) \implies \overline{A}^TB \subset O \iff LB^T \subset A^T \iff BL \subset A.$$

Therefore, $AL \subset B \subset BL$ and $BL \subset A \cdot \subset AL$. As $LL = L$ (due to the Tarski rule), this yields $AL = BL$. The vector-properties $A = AL$ and $B = BL$ are now obvious.

"$\Leftarrow$" We have $AL L = BL$, so that $(AL)^T\overline{BL} \subset O$ and $L \subset \overline{(AL)^T\overline{BL}}$. Similarly, we get $L \subset \overline{(BL)^T\overline{AL}}$. This gives

$$\mathrm{syq}(A, B) = \mathrm{syq}(AL, BL) = \overline{(AL)^T\overline{BL}} \wedge \overline{(BL)^T\overline{AL}}^T \supset L . \qquad \square$$

As a special case of Theorem 3.2.5 we obtain a characterization of vectors. A relation A is a vector if and only if $\mathrm{syq}(A, A) = L$.

4. Applications

We will now investigate some applications of symmetric quotients. First, we consider the univalent part of a relation. Then, we look for connections between ordering relations and symmetric quotients. In the third part of this chapter, we use the symmetric quotient in order to give a monomorphic characterization of the powerset of a set.

4.1. The Univalent Part of a Relation

Using matrix terminology, the univalent part of a relation A extracts that part which behaves like a partial function. Therefore, we only associate x to y if and only if

$$\bigwedge_z (A(x, z) \iff z = y).$$

If we compare this expression with (5) in Section 3.1, we get the following

4.1.1 Definition. If A is a relation, then $\mathrm{up}(A) := \mathrm{syq}(A^T, I) = A \wedge \overline{A\overline{I}}$ is called the **univalent part** of A.

Clearly, $\mathrm{up}(O) = O$, $\mathrm{up}(I) = I$ and $\mathrm{up}(L) = \overline{L\overline{I}} = O$ if $I \neq L$, i.e. if we are concerned with relations on a set with more than one element.

$\mathrm{up}(A)$ is unique indeed, since

$$\mathrm{up}(A)^T\mathrm{up}(A) = \mathrm{syq}(A^T, I)^T\,\mathrm{syq}(A^T, I) = \mathrm{syq}(I, A^T)\,\mathrm{syq}(A^T, I) \subset \mathrm{syq}(I, I) = I$$

by (7) and Theorem 3.2.2. Furthermore, taking the univalent part of a relation is an idempotent operation, i.e.

(12) $\quad \mathrm{up}(\mathrm{up}(A)) = \mathrm{up}(A).$

This equation is proved by $\mathrm{up}(\mathrm{up}(A)) = \overline{\mathrm{up}(A)\overline{I}} \wedge \overline{\overline{\mathrm{up}(A)}\,I} = \mathrm{up}(A)$, since $\mathrm{up}(A)$ is unique and thus $\overline{\mathrm{up}(A)\overline{I}} \supset \mathrm{up}(A)$.

The next theorem shows that up is a monotonic descending functional as long as the domain of the relation is not extended.

4.1.2 Theorem Let A and B be relations, then $A \subset B$ and $AL = BL$ imply $\mathrm{up}(B) \subset \mathrm{up}(A)$.

Proof: First we have $\mathrm{up}(B) \subset \overline{B\overline{I}} \subset \overline{A\overline{I}}$. Therefore, $\mathrm{up}(B) \wedge A\overline{I} \subset O$, and we may proceed

$$\mathrm{up}(B) = \mathrm{up}(B) \wedge BL = \mathrm{up}(B) \wedge AL = (\mathrm{up}(B) \wedge AI) \vee (\mathrm{up}(B) \wedge A\overline{I}) \subset A \vee O = A. \quad \square$$

We call the relative complement $A \wedge \overline{up(A)}$ of the univalent part of A the **properly ambiguous part** $pap(A)$ of A. It can be described by $pap(A) = A \wedge A\overline{I}$. Therefore, every relation can be decomposed into

$$A = up(A) \vee pap(A) \qquad \text{where} \qquad up(A) \wedge pap(A) = O\,.$$

Further properties of up and pap can be found in [5].

The following theorem gives some sort of an orthogonality between $up(A)$ and $pap(A)$.

4.1.3 Theorem If A is an arbitrary relation, then

$$pap(A)^T up(A) = O \qquad \text{and} \qquad A^T up(A) = up(A)^T up(A).$$

Proof: We have

$$\begin{aligned}(A \wedge \overline{up(A)})^T up(A) &\subset A^T up(A) \wedge \overline{up(A)}^T up(A) \\ &\subset A^T syq(A^T, I) \wedge \overline{I} && \text{by Schröder's rule} \\ &\subset I \wedge \overline{I} = O && \text{by Theorem 3.2.1}\,.\end{aligned}$$

This shows the first equation. The second one is proved by

$$A^T up(A) = (up(A) \vee pap(A))^T up(A) = up(A)^T up(A)\,. \qquad \square$$

An obvious relationship between up and functions is given without proof:

(13) $\quad A$ is a function $\iff up(A)L = L$.

4.2. Symmetric Quotients and Ordering Relations

Let $\leqq$ be a reflexive ordering relation on a set M. If x is a subset of M, then $y \in M$ is a majorant of x if

(14) $$\bigwedge_{z \in M} z \in x \implies z \leqq y.$$

From (14) we derive a purely relational characterization of the set of majorants. For a reflexive ordering relation E and a vector r we call $\overline{\overline{E}^T r}$ the vector of the majorants of r with respect to E. This relational approach has already been introduced in [2].

Now let R be an arbitrary relation. Then in matrix terminology the columns of R are vectors. Therefore, the columns of $\overline{\overline{E}^T R}$ correspond to the majorants of these vectors.

Analogously, one can treat the minorants. This leads to a generalization of the corresponding definitions in [2].

4.2.1 Definition Let E and R be relations. If E is a reflexive ordering relation, then we define $ma_E(R) := \overline{\overline{E}^T R}$ to be the **set of majorants** of R w.r.t. E and $mi_E(R) := \overline{\overline{E}R}$ to be the **set of minorants** of R w.r.t. E.

If one has majorants and minorants, it is easy to define greatest and least elements, least upper and greatest lower bounds. We note:

(15)
$$\begin{aligned} gr_E(R) &:= R \wedge ma_E(R) && \text{greatest element} \\ le_E(R) &:= R \wedge mi_E(R) && \text{least element} \\ lub_E(R) &:= le_E(ma_E(R)) && \text{least upper bound} \\ glb_E(R) &:= gr_E(mi_E(R)) && \text{greatest lower bound} \end{aligned}$$

The name "greatest element" is justified by proving the injectivity of $gr_E(R)$ (using Schröder's rule and the antisymmetry of E):

$$gr_E(R)\, gr_E(R)^T \subset R\, \overline{R^T \overline{E}} \wedge \overline{\overline{E}^T R}\, R^T \subset E \wedge E^T \subset I$$

Therefore, $gr_E(r)$ is a point if $r = rL$ is a vector and if $gr_E(r)$ exists ($gr_E(r) \neq O$). Analogously, $le_E(R)\, le_E(R)^T \subset I$ holds. Of course, $lub_E(R)$ and $glb_E(R)$ are also injective. This property will be used in the proof of 4.3.4.i.

In the following we will demonstrate that the notions introduced in Definition 4.2.1 and (15) are closely related to symmetric quotients. For a reflexive ordering relation E we will need the equations (cf. [2])

(16) $$\overline{E}^T = \overline{E}^T E \qquad \text{and} \qquad E^T \overline{ER} = \overline{ER} \quad \text{for an arbitrary relation } R,$$

which follow directly from reflexivity and transitivity with the help of Schröder's rule.

4.2.2 Theorem Let E and R be relations, where E is a reflexive ordering relation. Then we have:

$$gr_E(R) = syq(E, ER) \qquad \text{and} \qquad lub_E(E) = syq(E, E)$$

Proof: From (16) we obtain $ma_E(R) = \overline{\overline{E}^T R} = \overline{\overline{E}^T E R} = ma_E(ER)$. Using this equation we now prove

(17) $$gr_E(R) = gr_E(ER).$$

"$\subset$" $gr_E(R) = IR \wedge ma_E(R) \subset ER \wedge ma_E(ER) = gr_E(ER)$ since E is reflexive.

"$\supset$" As E is antisymmetric, we have $E \subset \overline{E}^T \vee I$. This implies $ER \subset \overline{E}^T R \vee R$ and the equivalent inclusion $ER \wedge ma_E(R) \subset R$. So we obtain $gr_E(ER) = ER \wedge ma_E(ER) \subset R$. Finally, from $gr_E(ER) \subset ma_E(ER) = ma_E(R)$ we get (17).

Using the second equation of (16) leads to

$$gr_E(R) = gr_E(ER) = ER \wedge \overline{\overline{E}^T E R} = \overline{E^T \overline{ER}} \wedge \overline{\overline{E}^T E R} = syq(E, ER).$$

This is the first equation. Let us now prove the second equation. Again we use (16) and obtain

$$lub_E(E) = \overline{\overline{E}^T E} \wedge \overline{\overline{E}\,\overline{\overline{E}^T E}} = \overline{\overline{E}^T E} \wedge \overline{\overline{E} E^T} = \overline{\overline{E}^T E} \wedge \overline{E^T \overline{E}} = syq(E, E)$$

as $\overline{E} E^T = \overline{E} = E^T \overline{E}$. These equations can be proved by transitivity of E and Schröder's rule. □

One should remark that such equations can also be proved for the least element and the greatest lower bound.

4.3. Powersets

We want to characterize the powerset $P(M)$ of a set M by the "is-element-of" relation $\epsilon \subseteq M \times P(M)$. Of course, two elements of the powerset should be considered equal if they consist of the same elements. We express this property by the algebraic version of (4) in 3.1. With the second postulate we demand that for every subset $N \subseteq M$ there exists an element in $P(M)$.

4.3.1 Definition Let ϵ be a relation. We call ϵ a **direct power** if and only if

i) $syq(\epsilon, \epsilon) \subset I$

ii) $L = L\,syq(\epsilon, R)$ for every relation R.

Equivalently, we could have defined a direct power by:

$syq(\epsilon, R)$ is bijective for every relation R.

Property ii) of Definition 4.3.1 is surjectivity of $syq(\epsilon, R)$, and $syq(\epsilon, R)\,syq(\epsilon, R)^T \subset syq(\epsilon, \epsilon) \subset I$ implies injectivity. Conversely, from the injectivity of $syq(\epsilon, R)$ and from $syq(\epsilon, \epsilon) \supset I$ we derive $syq(\epsilon, \epsilon) \subset syq(\epsilon, \epsilon)\,syq(\epsilon, \epsilon)^T \subset I$ by choosing $R := \epsilon$.

In a given relational algebra a direct power may not exist. But if it does exist, it uniquely determines (up to isomorphism) the powerset $P(M)$ of a set M. We prove this property by purely relational algebraic means.

4.3.2 Theorem The characterization of a direct power in 4.3.1 is monomorphic.

Proof: Assume that two direct powers ϵ and ϵ' exist. Then $\Phi := syq(\epsilon, \epsilon')$ is injective and unique by 3.2.2 and 4.3.1.i. Surjectivity and totality follow directly from 4.3.1.ii. Finally 3.2.1 and surjectivity imply $\epsilon \Phi = \epsilon'$. Therefore, (I, Φ) is an isomorphism between ϵ and ϵ'. □

Two interesting relations in connection with powersets are the ordering relation Ω on $P(M)$ and the embedding function $\iota : M \rightarrow P(M)$, mapping elements to their corresponding singleton sets. We define them by

$$\Omega := \overline{\epsilon^T \overline{\epsilon}}, \qquad \iota := syq(I, \epsilon)$$

and prove some of their properties in the following

4.3.3 Theorem.

i) Ω is an ordering relation.

ii) ι is an injective function.

iii) $\epsilon \iota^T = I$

iv) $\iota \Omega = \epsilon = \epsilon \Omega$

Proof: i) Applying Schröder's rule on $\epsilon I \subset \epsilon$ we get $\epsilon^T \overline{\epsilon} \subset \overline{I}$ and thus $I \subset \Omega$. Again we use Schröder's rule and derive transitivity by

$$\overline{\epsilon}^T \epsilon \subset \overline{\epsilon}^T \epsilon \iff \overline{\overline{\epsilon}^T \epsilon}\, \epsilon^T \subset \epsilon^T \implies \overline{\overline{\epsilon}^T \epsilon}\, \epsilon^T \overline{\epsilon} \subset \epsilon^T \overline{\epsilon} \iff \Omega^2 \subset \Omega.$$

Antisymmetry is established by 4.3.1.i.

ii) ι is total because of 4.3.1.ii. Uniqueness is implied by 3.2.2 and 4.3.1.i. Injectivity is obtained by $\iota = up(\epsilon^T)^T$ (cf. 4.1.1).

iii) follows from 3.2.1.

iv) From ii) and iii) we obtain $\iota \Omega = \overline{\iota \epsilon^T \overline{\epsilon}} = \epsilon$. Reflexivity of Ω implies $\epsilon \subset \epsilon \Omega$, and with Schröder's rule we get $\epsilon^T \overline{\epsilon} \subset \overline{\Omega} \iff \epsilon \Omega \subset \epsilon$. □

The isomorphism (I, Φ) from 4.3.2 is also an isomorphism between ι and $\iota' := syq(I, \epsilon')$ as $\iota \Phi = \iota'$ can easily be proved. In addition, the bijective relation Φ (or more exactly the pair (Φ, Φ)) is an isomorphism between Ω and $\Omega' := \overline{\epsilon'^T \overline{\epsilon'}}$. This follows immediately from the proof of Theorem 4.3.2.

Now we recall two of our introductory examples in 3.1 and use symmetric quotients to describe union and intersection. Moreover, we prove with algebraic means that $P(M)$ together with the ordering relation Ω is a complete lattice, i.e. $\mathrm{lub}_\Omega(R)$ is surjective for arbitrary relations R. The last two equations of 4.3.4 express another connection between symmetric quotients and least upper bounds: If the subset $N \subseteq M$ is represented by the vector v, then the symmetric quotient of the direct power ϵ and v is the least upper bound of all the singleton sets corresponding to elements of N. This symmetric quotient is also the least upper bound of those elements of the powerset $P(M)$ that correspond to subsets of N.

4.3.4 Theorem Let ϵ be a direct power and R a relation so that ϵR exists.

i) $\mathrm{syq}(\epsilon, \epsilon R) = \mathrm{lub}_\Omega(R)$

ii) $\mathrm{syq}(\epsilon, \overline{\epsilon R}) = \mathrm{glb}_\Omega(R)$

iii) $\mathrm{syq}(\epsilon, R) = \mathrm{lub}_\Omega(\iota^T R)$

iv) $\mathrm{syq}(\epsilon, R) = \mathrm{lub}_\Omega(\overline{\epsilon^T \overline{R}})$.

Proof: i) By Schröder's rule from $\overline{\epsilon}^T \epsilon R \subset \overline{\epsilon}^T \epsilon R$ we obtain $\epsilon\, \overline{\overline{\epsilon}^T \epsilon R} \subset \overline{\epsilon R}$. Therefore,

$$\mathrm{syq}(\epsilon, \epsilon R) = \overline{\overline{\epsilon}^T \epsilon R} \wedge \overline{\epsilon^T \overline{\epsilon R}} \subset \overline{\overline{\epsilon}^T \epsilon R} \wedge \overline{\epsilon^T \overline{\epsilon}\, \overline{\overline{\epsilon}^T \epsilon R}} = \mathrm{lub}_\Omega(R) .$$

As $\mathrm{syq}(\epsilon, \epsilon R)$ is surjective and $\mathrm{lub}_\Omega(R)$ is injective, equality holds (cf. 2.2). In particular, $\mathrm{lub}_\Omega(R)$ is surjective for arbitrary relations R.

ii) is proved similarly.

iii) Using i) and 4.3.3.iii we get $\mathrm{lub}_\Omega(\iota^T R) = \mathrm{syq}(\epsilon, \epsilon \iota^T R) = \mathrm{syq}(\epsilon, R)$.

iv) We have $\iota^T R \subset \overline{\epsilon^T \overline{R}}$ by $\iota \epsilon^T \subset I$ and Schröder's rule. Using Schröder's rule again we obtain

$$\overline{\Omega}^T \overline{\epsilon^T \overline{R}} = \overline{\epsilon}^T \epsilon\, \overline{\epsilon^T \overline{R}} \subset \overline{\epsilon}^T R = \overline{\epsilon}^T \epsilon\, \iota^T R = \overline{\Omega}^T \iota^T R \subset \overline{\Omega}^T \overline{\epsilon^T \overline{R}} .$$

Therefore, $\mathrm{ma}_\Omega(\overline{\epsilon^T \overline{R}}) = \mathrm{ma}_\Omega(\iota^T R)$ and $\mathrm{lub}_\Omega(\overline{\epsilon^T \overline{R}}) = \mathrm{lub}_\Omega(\iota^T R) = \mathrm{syq}(\epsilon, R)$ by iii). □

An immediate consequence of Theorem 4.3.4 is

$$\mathrm{lub}_\Omega(R) = \mathrm{syq}(\epsilon, \epsilon R) = \mathrm{lub}_\Omega(\iota^T \epsilon R) = \mathrm{lub}_\Omega(\overline{\epsilon^T \overline{\epsilon R}}) .$$

Already in the preceding theorem it became apparent, how subsets of M (vectors) correspond to elements of $P(M)$ (points). We describe this correspondence with two functionals τ and σ which map vectors to points and points to vectors, respectively.

If v is a vector and e an element, we define

$$\tau[v] := \mathrm{syq}(\epsilon, v) \qquad \sigma[e] := \epsilon e .$$

Obviously, $\tau[v]$ and $\sigma[e]$ are also vectors. $\tau[v]$ is surjective because of 4.3.1.ii. Theorem 3.2.2 and 4.3.1.i imply injectivity. Therefore, $\tau[v]$ is a point. In the following theorem we prove that τ and σ establish some kind of an isomorphism between subsets of M and elements of $P(M)$.

4.3.5 Theorem Let v_1, v_2 be vectors and e_1, e_2 be points. Then

i) $\sigma[\tau[v_1]] = v_1$

ii) $\tau[\sigma[e_1]] = e_1$

iii) $e_1 \subset \Omega e_2 \implies \sigma[e_1] \subset \sigma[e_2]$

iv) $v_1 \subset v_2 \implies \tau[v_1] \subset \Omega\, \tau[v_2]$

Proof: i) follows directly from Theorem 3.2.1.

ii) $\tau[\sigma[e_1]] = \mathrm{syq}(\epsilon, \epsilon e_1) = \mathrm{syq}(\epsilon, \epsilon) e_1 = e_1$ because of (11) in 3.2 and 4.3.1.i.

iii) From 4.3.3.iv we obtain $\sigma[e_1] = \epsilon e_1 \subset \epsilon \Omega e_2 = \epsilon e_2 = \sigma[e_2]$.

iv) We use 4.3.4.iii and get

$$\tau[v_1]\,\tau[v_2]^T = \mathrm{syq}(\epsilon, v_1)\,\mathrm{syq}(\epsilon, v_2)^T = \mathrm{lub}_\Omega(\iota^T v_1)\,\mathrm{lub}_\Omega(\iota^T v_2)^T$$
$$\subset \mathrm{mi}_\Omega(\mathrm{ma}_\Omega(\iota^T v_1))\,\mathrm{ma}_\Omega(\iota^T v_2)^T \subset \mathrm{mi}_\Omega(\mathrm{ma}_\Omega(\iota^T v_1))\,\mathrm{ma}_\Omega(\iota^T v_1)^T \subset \Omega$$

With Schröder's rule and bijectivity of $\tau[v_2]$ we obtain $\overline{\Omega\, \tau[v_2]} = \overline{\Omega}\, \tau[v_2] \subset \overline{\tau[v_1]}$. □

In this last section we were concerned with the application of symmetric quotients to powerset construction. Having introduced direct products, we could extend this technique to define the sets of partial, total and monotonic functions monomorphically (cf. [6], see also [7]). Applications to function domain constructions for the semantics of recursive program schemes are also possible.

Acknowledgement: We gratefully acknowledge valuable discussions with T. Ströhlein. We thank H. Ehler for carefully reading a draft version of the manuscript.

References:

[1] Chin L.H., Tarski A.: Distributive and modular laws in the arithmetic of relation algebras. Univ. California Publ. Math. **1**, 341–384 (1951)

[2] Riguet J.: Relations binaires, fermetures, correspondances de Galois. Bull. Soc. Math. France **76**, 114–155 (1948)

[3] Schmidt G.: Programs as partial graphs I: Flow equivalence and correctness. Theoret. Comput. Sci. **15**, 1–25 (1981)

[4] Schmidt G., Ströhlein T.: Relation algebras – concept of points and representability. Discrete Mathematics **54**, 83–92 (1985)

[5] Schmidt G., Ströhlein T.: Diskrete Mathematik – Relationen, Graphen und Programme. Internal Report, Techn. Univ. München (1985)

[6] Zierer H.: Relationale Semantik. Techn. Univ. München, Institut für Informatik, Diplomarbeit (1983)

[7] Zierer H., Schmidt G., Berghammer R.: An Interactive Graphical Manipulation System for Higher Objects Based on Relational Algebra. In: Tinhofer G., Schmidt G. (Hrsg.): *12th International Workshop on Graphtheoretical Concepts in Computer Science. 17.–19. Juni 1986, Bernried/Starnberger See.* Lecture Notes in Computer Science **250**, Springer (1986), to appear