

ON THE GREATEST CONGRUENCE OF RELATIONS

Marica D. Prešić

(Received February 19, 1979)

Introduction. Let L be a first order relational language and \mathcal{M} a model of L with the domain M . Further, let \sim be an equivalence on M and $\alpha \in L$ an n -ary relation¹⁾. We say that \sim is a congruence for α at i^{th} coordinate (or that \sim is compatible with α at i^{th} coordinate) where $i=1, 2, \dots, n$, iff the following condition holds

$$(1) (\forall x_1, \dots, x_n, x_i, x_i') (x_i \sim x_i' \Rightarrow (\alpha(x_1, \dots, x_i, \dots, x_n) \Leftrightarrow (x_1, \dots, x_i', \dots, x_n)))$$

The relation \sim is a congruence of α iff it is its congruence at each coordinate and \sim is a congruence for the model \mathcal{M} iff it is a congruence for each its relation. A congruence \sim (for α at i^{th} coordinate or for α or for \mathcal{M}) is said to be the greatest congruence if any other congruence \sim_1 of the same type is contained in \sim , i.e. iff the following condition holds

$$(\forall x, y) (x \sim_1 y \Rightarrow x \sim y)$$

In the paper [4] it has been given a formula describing all equivalences of the given nonempty set M . The formula reads:

$$(2) \quad x \sim y \Leftrightarrow (\forall z) (x \pi z \Leftrightarrow y \pi z)$$

where π is an arbitrary binary relation on M . It is not difficult to see that the relation \sim defined by means of (2) is a congruence for π at first coordinate (in such a case we say that \sim is a left congruence for π and if \sim is a congruence for a binary relation at its second coordinate we say that \sim is a right congruence). Our main purpose is to describe all congruences of a given relation or a given model. In that description the greatest congruences play the main role.

In the first part of the paper we prove that each relation as well as each model has the greatest congruence and we give a description of the greatest

¹⁾ For the relation of M corresponding to $\alpha \in L$ we shall not introduce a new symbol (as α_M or similar), since throughout the paper we deal only with one chosen model of L .

congruence in terms of the language L . In the case of the greatest congruence of one relation or a finite set of relations this description belongs to the first order predicate calculus. Further, using the notion of the greatest congruence we describe all congruences of the model \mathcal{M} . Similar to the previous case this description belongs to the first order calculus, if the language L is finite. In the second part of the paper we give some applications of the notion of greatest congruence to the decision problem.

We give now a review of some general notions concerning congruences. We have defined a congruence for the relation α as a relation \sim which is compatible with α at each coordinate. We recall that this definition is equivalent to the following:

An equivalence \sim is a congruence for α iff it has the following property

$$(3) \quad (\forall x_1, \dots, x_n, x'_1, \dots, x'_n) (x_1 \sim x'_1 \wedge \dots \wedge x_n \sim x'_n) \Rightarrow (\alpha(x_1, \dots, x_n) \Leftrightarrow \alpha(x'_1, \dots, x'_n))$$

Given equivalences \sim_1, \dots, \sim_n we shall prove that they are compatible with α at first, second, \dots , n^{th} coordinate respectively iff

$$(4) \quad (\forall x_1, \dots, x_n, x'_1, \dots, x'_n) (x_1 \sim_1 x'_1 \wedge \dots \wedge x_n \sim_n x'_n) \Rightarrow (\alpha(x_1, \dots, x_n) \Leftrightarrow \alpha(x'_1, \dots, x'_n))$$

Suppose that \sim_1, \dots, \sim_n are compatible with α at first, \dots , n^{th} coordinate, respectively and that the elements $x_1, \dots, x_n, x'_1, \dots, x'_n$ of M satisfy

$$(5) \quad x_1 \sim_1 x'_1, x_2 \sim_2 x'_2, \dots, x_n \sim_n x'_n$$

Using the fact that \sim_2, \dots, \sim_n are congruences for α at first, second, \dots , n^{th} coordinate from (3) we conclude

$$(6) \quad \begin{aligned} &\alpha(x_1, x_2, \dots, x_n) \Leftrightarrow \alpha(x'_1, x_2, \dots, x_n) \\ &\alpha(x'_1, x_2, \dots, x_n) \Leftrightarrow \alpha(x'_1, x'_2, x_3, \dots, x_n) \\ &\dots \\ &\alpha(x'_1, x'_2, \dots, x'_{n-1}, x_n) \Leftrightarrow \alpha(x'_1, x'_2, \dots, x'_{n-1}, x'_n) \end{aligned}$$

As logical equivalence \Leftrightarrow is transitive, from (6) we immediately obtain

$$(7) \quad \alpha(x_1, \dots, x_n) \Leftrightarrow \alpha(x'_1, \dots, x'_n)$$

what proves the formula (4). Conversely, suppose that \sim_1, \dots, \sim_n are equivalences having the property (4). Therefore for every $i = 1, 2, \dots, n$ we deduce

$$\begin{aligned} &(\forall x_1, \dots, x_n, x'_i) (x_1 \sim_1 x_1 \wedge \dots \wedge x_i \sim_i x'_i \wedge \dots \wedge x_n \sim_n x_n) \\ &\Rightarrow \alpha(x_1, \dots, x_i, \dots, x_n) \Leftrightarrow \alpha(x_1, \dots, x'_i, \dots, x_n) \end{aligned}$$

i.e. by reflexivity of the relations $\sim_1, \dots, \sim_{i-1}, \sim_{i+1}, \dots, \sim_n$

$$(\forall x_1, \dots, x_n, x'_i) (x_i \sim_i x'_i \Rightarrow (\alpha(x_1, \dots, x_i, \dots, x_n) \Leftrightarrow \alpha(x_1, \dots, x'_i, \dots, x_n)))$$

It means that \sim_i is congruence for α at i^{th} coordinate. As we have the similar proof for every $i=1, \dots, n$, we conclude that the relations \sim_1, \dots, \sim_n are congruences for α at first, second, \dots , n^{th} coordinate respectively.

Note that the relation \sim introduced as the intersection of \sim_1, \dots, \sim_n is a congruence for α if \sim_1, \dots, \sim_n are compatible with α at first, second, \dots , n^{th} coordinate respectively. That follows immediately from the fact that \sim is included in each relation \sim_i ($i=1, 2, \dots, n$), i.e. that

$$(\forall x, y) (x \sim y \Rightarrow x \sim_i y)$$

We conclude this preliminary discussion by mentioning one property of equivalences that we use in what follows.

Let \sim_1, \sim_2 be equivalences of the set M having the following equivalence classes

$$A_1, A_2, \dots, A_k \quad (\text{for the relation } \sim_1)$$

$$B_1, B_2, \dots, B_l \quad (\text{for the relation } \sim_2)$$

where k, l , are natural numbers. The relation \sim defined as the intersection, of \sim_1, \sim_2 has as equivalence classes nonempty sets of the form

$$(8) \quad A_i \cap B_j$$

Namely, as by assumption

$$\sim_1 = \bigcup_{i=1}^k A_i^2 \quad \sim_2 = \bigcup_{j=1}^l B_j^2 \quad (\text{where } S^2 = S \times S)$$

it follows immediately

$$\sim_1 \cap \sim_2 = \left(\bigcup_i A_i^2 \right) \cap \left(\bigcup_j B_j^2 \right) = \bigcup_{i,j} (A_i^2 \cap B_j^2) = \bigcup_{i,j} (A_i \cap B_j)^2$$

that is

$$\sim_1 \cap \sim_2 = \bigcap_{i,j} (A_i \cap B_j)^2$$

whence we conclude that

$$\{A_i \cap B_j \mid \substack{i=1, \dots, k; \\ j=1, \dots, l; \\ A_i \cap B_j \neq \emptyset}\}$$

is the partition corresponding to $\sim_1 \cap \sim_2$.

Note that the relation \sim has at most $k \cdot l$ equivalence classes, for some of the sets (8) may be empty.

More generally, let \sim_1, \dots, \sim_k be equivalences having as equivalence classes the following sets

$$A_{11}, A_{12}, \dots, A_{1n_1} \quad (\text{for the relation } \sim_1)$$

$$A_{21}, A_{22}, \dots, A_{2n_2} \quad (\text{for the relation } \sim_2)$$

$$\dots \dots \dots \dots \dots \dots \dots$$

$$A_{k1}, A_{k2}, \dots, A_{kn_k} \quad (\text{for the relation } \sim_k)$$

Further, let \sim be the intersection of all preceding relations. Then the equivalence classes for \sim are nonempty sets of the form

$$A_{1i_1} \cap A_{2i_2} \cap \dots \cap A_{ki_k}$$

therefore the relation \sim has at most

$$n_1 \cdot n_2 \cdot \dots \cdot n_k$$

equivalence classes.

1. Let now $\alpha \in L$ be an arbitrary n -ary relation. Related to α we define the relations¹⁾ $\sim_{i\alpha}$, where $i=1, 2, \dots, n$, in the following way

$$(9) \quad x \sim_{i\alpha} y \stackrel{\text{def}}{\Leftrightarrow} (\forall x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n) (\alpha(x_1, \dots, x_{i-1}, x, x_{i+1}, \dots, x_n)) \\ \Leftrightarrow \alpha(x_1, \dots, x_{i-1}, y, x_{i+1}, \dots, x_n))$$

Further let \sim_α be the intersection of all the relations $\sim_{1\alpha}, \sim_{2\alpha}, \dots, \sim_{n\alpha}$, i.e. \sim_α is the relation defined by

$$(10) \quad x \sim_\alpha y \stackrel{\text{def}}{\Leftrightarrow} x \sim_{1\alpha} y \wedge x \sim_{2\alpha} y \wedge \dots \wedge x \sim_{n\alpha} y$$

Finally let \sim_M be the intersection of all the relations \sim_α , where α runs over L , i.e.

$$(11) \quad x \sim_M y \stackrel{\text{def}}{\Leftrightarrow} (\forall \alpha \in L) x \sim_\alpha y$$

We prove the following theorem.

Theorem 1. *The relation \sim_M defined by (11) is the greatest congruence for \mathcal{M} .*

Proof. Note that all definitions (9), (10), (11) are correct and therefore the relations $\sim_{i\alpha}$ ($i=1, \dots, n$), \sim_α , \sim_M exist.

First of all we shall prove that $\sim_{i\alpha}$ ($i=1, \dots, n$) is the greatest congruence for α at i^{th} coordinate. Namely, the following formulas are true on \mathcal{M}

$$(12) \quad (\forall x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n) (\alpha(x_1, \dots, x_{i-1}, x, x_{i+1}, \dots, x_n)) \\ \Leftrightarrow \alpha(x_1, \dots, x_{i-1}, x, x_{i+1}, \dots, x_n))$$

$$(13) \quad (\forall x_1, \dots, x_{i-1}, \dots, x_n) (\alpha(x_1, \dots, x_{i-1}, x, x_{i+1}, \dots, x_n)) \\ \Leftrightarrow \alpha(x_1, \dots, x_{i-1}, y, x_{i+1}, \dots, x_n))$$

$$\Rightarrow (\forall x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n) (\alpha(x_1, \dots, x_{i-1}, y, x_{i+1}, \dots, x_n)) \\ \Leftrightarrow \alpha(x_1, \dots, x_{i-1}, x, x_{i+1}, x_n))$$

¹⁾ The relations $\sim_{i\alpha}$ ($i=1, 2, \dots, n$) have been introduced by S. B. Prešić at the Seminar for mathematical logic taking place in the Mathematical Institute, Beograd.

$$\begin{aligned}
 & (\forall x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n) (\alpha(x_1, \dots, x_{i-1}, x, x_{i+1}, \dots, x_n) \\
 & \quad \Leftrightarrow \alpha(x_1, \dots, x_{i-1}, y, x_{i+1}, \dots, x_n)) \\
 (14) \quad & \wedge (\forall x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n) (\alpha(x_1, \dots, x_{i-1}, y, x_{i+1}, \dots, x_n) \\
 & \quad \Leftrightarrow \alpha(x_1, \dots, x_{i-1}, z, x_{i+1}, \dots, x_n))) \\
 & \Rightarrow (\forall x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n) (\alpha(x_1, \dots, x_{i-1}, x, x_{i+1}, \dots, x_n) \\
 & \quad \Leftrightarrow \alpha(x_1, \dots, x_{i-1}, z, x_{i+1}, \dots, x_n))
 \end{aligned}$$

what immediately follows from the tautologies

$$p \Leftrightarrow p, (p \Leftrightarrow q) \Rightarrow (q \Leftrightarrow p), (p \Leftrightarrow q) \wedge (q \Leftrightarrow r) \Rightarrow (p \Leftrightarrow r)$$

and from the valid formulæ

$$(\forall x)(A \Rightarrow B) \Rightarrow ((\forall x)A \Rightarrow (\forall x)B), (\forall x)(A \wedge B) \Leftrightarrow (\forall x)A \wedge (\forall x)B$$

From (12), (13), (14) it follows that the relation $\sim_{i\alpha}$ has the properties

$$(R) x \sim_{i\alpha} x, (S) x \sim_{i\alpha} y \Rightarrow y \sim_{i\alpha} x, (T) x \sim_{i\alpha} y \wedge y \sim_{i\alpha} z \Rightarrow x \sim_{i\alpha} z$$

i. e. that it is an equivalence. That $\sim_{i\alpha}$ is compatible with α at i^{th} coordinate follows immediately from definition (9), for $\sim_{i\alpha}$ includes this compatibility in its definition.

We now prove that $\sim_{i\alpha}$ is the greatest congruence for α at i^{th} coordinate. For this take an arbitrary congruence \sim_i of the same type. Then we have the following implication chain

$$\begin{aligned}
 x \sim_i y & \Rightarrow (\forall x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n) (\alpha(x_1, \dots, x_{i-1}, x, x_{i+1}, \dots, x_n) \\
 & \quad \Leftrightarrow \alpha(x_1, \dots, x_{i-1}, y, x_{i+1}, \dots, x_n)).
 \end{aligned}$$

(For \sim_i is compatible with α at i^{th} coordinate)

$$\Rightarrow x \sim_{i\alpha} y.$$

(By the definition of $\sim_{i\alpha}$).

Consequently, for every $x, y \in M$ the following implication holds

$$x \sim_i y \Rightarrow x \sim_{i\alpha} y$$

This means that any congruence for α at i^{th} coordinate is included in $\sim_{i\alpha}$, i. e. that $\sim_{i\alpha}$ is the greatest congruence.

Further, we prove that \sim_α is the greatest congruence for α . As the relations

$$\sim_{1\alpha}, \sim_{2\alpha}, \dots, \sim_{n\alpha}$$

are congruences for α at the first, second, ..., n^{th} coordinate respectively, the relation \sim_α defined as the intersection of all above relations is a congruence for α . Let now \sim be a congruence for α .

By the definition of congruence \sim is compatible with α at each its coordinate. As $\sim_{i\alpha}$ is the greatest congruence for α at i^{th} coordinate, we conclude that \sim is included in $\sim_{i\alpha}$ for each $i=1, 2, \dots, n$, i. e. the following implications hold

$$x \sim y \Rightarrow x \sim_{1\alpha} y, x \sim y \Rightarrow x \sim_{2\alpha} y, \dots, x \sim y \Rightarrow x \sim_{n\alpha} y$$

From this it is easy to obtain

$$x \sim y \Rightarrow (x \sim_{1\alpha} y \wedge x \sim_{2\alpha} y \wedge \dots \wedge x \sim_{n\alpha} y)$$

or, in other words

$$x \sim y \Rightarrow x \sim_{\alpha} y.$$

Thus \sim_{α} is the greatest congruence for α .

Finally we prove that the relation \sim_M defined by (11) is the greatest congruence for \mathcal{M} . Namely, \sim_M being defined as the intersection of all equivalences \sim_{α} , where α runs over L , is also an equivalence. Further, \sim_M is a congruence for \mathcal{M} because for any $\alpha \in L$ we have:

$$\begin{aligned} x \sim_M y &\Rightarrow (\forall \alpha \in L) x \sim_{\alpha} y \\ &\Rightarrow x \sim_{\alpha} y. \\ &\quad (\text{Where } \alpha \text{ is the chosen relation of length } n) \\ &\Rightarrow (\forall x_1, \dots, x_{i-1}, \dots, x_n) (\alpha(x_1, \dots, x_i, x, x_{i+1}, \dots, x_n) \\ &\quad \Leftrightarrow \alpha(x_1, \dots, x_{i-1}, y, x_{i+1}, \dots, x_n)). \end{aligned}$$

(By the definition of \sim_{α}).

Thus \sim_M is a congruence for α at, i^{th} coordinate, where $i = 1, 2, \dots, n$, i. e. \sim_M is a congruence for each $\alpha \in L$.

We now prove that \sim_M is the greatest such a congruence. Let \sim be any congruence for \mathcal{M} . Then \sim is included in each of the relations \sim_{α} , where $\alpha \in L$, for \sim_{α} is the greatest congruence for α . Therefore \sim is included in the intersection of all the relation \sim_{α} , i. e. \sim is included in \sim_M , whence \sim_M is the greatest congruence for \mathcal{M} . The proof of Theorem 1 is complete.

We note that the definitions of the relations $\sim_{i\alpha}$ and \sim_{α} are the formulae of the first order predicate calculus. In the case L is finite so is the definition of \sim_M .

We give now an example. Let $L = \{\alpha, \beta\}$, where α, β are of length 1, 2, respectively. Further let $M = \{1, 2, 3, 4, 5, 6, 7\}$ and the relations α, β be defined by the tables¹⁾:

α	1	2	3	4	5	6	7	β	1	2	3	4	5	6	7
	T	⊥	T	⊥	T	⊥	T	1	⊥	T	⊥	T	⊥	T	T
								2	⊥	⊥	⊥	⊥	T	⊥	⊥
								3	⊥	T	⊥	T	⊥	T	T
								4	⊥	⊥	⊥	⊥	T	⊥	⊥
								5	T	⊥	T	⊥	T	⊥	⊥
								6	⊥	⊥	⊥	⊥	T	⊥	⊥
								7	⊥	⊥	⊥	⊥	T	⊥	⊥

In that example the definitions of $\sim_{\alpha}, \sim_{\beta}$ read:

$$\begin{aligned} x \sim_{\alpha} y &\stackrel{\text{def}}{\Leftrightarrow} (\alpha(x) \Leftrightarrow \alpha(y)), \\ x \sim_{\beta} y &\stackrel{\text{def}}{\Leftrightarrow} (\forall z) (\beta(x, z) \Leftrightarrow \beta(y, z)) \wedge (\forall z) (\beta(z, x) \Leftrightarrow \beta(z, y)). \end{aligned}$$

¹⁾ The symcols T, ⊥ correspond to the words true, false respectively.

Substituting for x, y the elements of M in all possible ways, it is easy to conclude that the tables of $\sim_\alpha \sim_\beta$, are:

\sim_α	1	2	3	4	5	6	7
1	T	T	T	T	⊥	⊥	⊥
3	T	T	T	T	⊥	⊥	⊥
5	T	T	T	T	⊥	⊥	⊥
7	T	T	T	T	⊥	⊥	⊥
2	⊥	⊥	⊥	⊥	T	T	T
4	⊥	⊥	⊥	⊥	T	T	T
6	⊥	⊥	⊥	⊥	T	T	T

\sim_β	1	3	2	4	6	7	5
1	T	T	⊥	⊥	⊥	⊥	⊥
3	T	T	⊥	⊥	⊥	⊥	⊥
2	⊥	⊥	T	T	T	T	⊥
4	⊥	⊥	T	T	T	T	⊥
6	⊥	⊥	T	T	T	T	⊥
7	⊥	⊥	T	T	T	T	⊥
5	⊥	⊥	⊥	⊥	⊥	⊥	T

The intersection of \sim_α, \sim_β , i. e. the relation \sim_M has the following table

\sim_M	1	3	2	4	6	5	7
1	T	T	⊥	⊥	⊥	⊥	⊥
3	T	T	⊥	⊥	⊥	⊥	⊥
2	⊥	⊥	T	T	T	⊥	⊥
4	⊥	⊥	T	T	T	⊥	⊥
6	⊥	⊥	T	T	T	⊥	⊥
5	⊥	⊥	⊥	⊥	⊥	T	⊥
7	⊥	⊥	⊥	⊥	⊥	⊥	T

We now return to the general case and go to the problem of describing of all congruences of a given relation α or a given model \mathcal{M} . We shall prove the following theorem.

Theorem 2. *Let $\alpha \in L$ be an n -ary relation. All congruences \sim for the relation α are determined by the following formula*

$$(15) \quad x \sim y \Leftrightarrow (x \sim_\alpha y \wedge x \rho y)$$

where \sim_α is defined by (10) and ρ is any equivalence of the set M .

Proof. We have to prove that the equivalence (15) determines a general solution for congruences of α . In other words we have to prove the following assertion.

The binary relation \sim is a congruence for α iff there is an equivalence ρ of M such that \sim is the intersection of \sim_α and ρ , i. e. that the equivalence (15) holds.

If-part: Suppose that (15) holds for some equivalence ρ . Then \sim being the intersection of two equivalences \sim_α and ρ is itself an equivalence. Further, \sim is a congruence for α at each coordinate because of:

$$x \sim y \Rightarrow (x \sim_{\alpha} y \wedge x \rho y)$$

(By assumption (15))

$$\Rightarrow x \sim_{\alpha} y$$

$$\Rightarrow (\alpha(x_1, \dots, x_{i-1}, x, x_{i+1}, \dots, x_n) \Leftrightarrow \alpha(x_1, \dots, x_{i-1}, y, x_{i+1}, \dots, x_n))$$

(Since \sim_{α} is a congruence for α).

Thus the relation \sim satisfying equivalence (15) is a congruence for α .

Only if-part: Assume that \sim is a congruence for α . We must prove that \sim can be obtained from (15) for some suitable equivalence relations ρ . Namely, for ρ it is enough to choose just the relation \sim , since the following equivalence holds

$$x \sim y \Leftrightarrow (x \sim_{\alpha} y \wedge x \sim y).$$

The implication

$$(x \sim_{\alpha} y \wedge x \sim y) \Rightarrow x \sim y$$

is obviously true by the tautology $p \wedge q \Rightarrow p$, and the converse implication

$$x \sim y \Rightarrow (x \sim_{\alpha} y \wedge x \sim y)$$

follows from the fact, that \sim_{α} is the greatest congruence for α . This completes the proof.

Combining the preceding theorem and the result [3] mentioned in the preliminary discussion we obtain a general solution for congruences of the relation α depending on the arbitrary binary relation, what is the usual form of general solution.

So, replacing the equivalence ρ in (15) with the relation determined by $(\forall z)(x \pi z \Leftrightarrow y \pi z)$ on the basis of general solution (2), it is easy to obtain the following corollary.

Corollary 1. *Let $\alpha \in L$ be an n -ary relation.*

All congruences \sim for α are determined by the following formula

$$(16) \quad x \sim y \Leftrightarrow (x \sim_{\alpha} y \wedge (\forall z)(x \pi z \Leftrightarrow y \pi z))$$

where \sim_{α} is defined by (10) and π is an arbitrary binary relation of M .

In a similar way it is possible to describe all congruences of a model \mathcal{M} . This is done in the following theorem.

Theorem 3. *All congruences \sim of a model \mathcal{M} are determined by the equivalence*

$$(17) \quad x \sim y \Leftrightarrow (x \sim_M y \wedge x \rho y)$$

where ρ is an arbitrary equivalence of M and \sim_M is defined by (11).

The proof is quite similar to the proof of the previous theorem and we omit it.

As in the case of one relation α , by the equivalence (2) we obtain the following corollary.

Corollary 2. All congruences of \mathcal{M} are determined by

$$(18) \quad x \sim y \Leftrightarrow (x \sim_M y \wedge (\forall z) (x \pi z \Leftrightarrow y \pi z))$$

where \sim_M is defined by (11) and π is an arbitrary binary relation of M .

Note that in the case the language L is finite, the equivalences (17) and (18) are formulae of the first order predicate calculus, since in that case the definition of \sim_M belongs to that calculus.

Let us state one more note concerning all general solutions (15), (16), (17), (18). Namely, they all are so called *reproductive general solutions*. This means that they yield just the relation \sim if the arbitrary equivalence ρ or arbitrary relation π is replaced by \sim itself. We recall that the notion of reproductive solution is due to E. Schröder and L. Löwenheim and that the general theory of reproductive solutions has been developed by S. B. Prešić and S. Rudeanu.

2. In this part of the paper we give some applications of the greatest congruences. Let L be a relational language without equality symbol and let \mathcal{M} be a model of L . If \sim is a congruence for \mathcal{M} then \mathcal{M} and \mathcal{M}/\sim are elementary equivalent. It is an immediate consequence of the following assertion:

Let \mathcal{M}, \mathcal{N} be models of L and $f: M \rightarrow N$ maps M onto N . If for any relation symbol $\rho \in L$ of length n the equivalence

$$M \models \rho(a_1, \dots, a_n) \leftrightarrow N \models \rho(fa_1, \dots, fa_n) \quad (a_1, \dots, a_n \in M)$$

holds, then for any sentence F in the language L the following equivalence

$$M \models F \leftrightarrow N \models F$$

hold.

Proof of that assertion is by induction on the number of logical symbols in F .

In the case \mathcal{N} is \mathcal{M}/\sim , where \sim is a congruence of \mathcal{M} , the assumption of the previous assertion is true (f is the mapping $x \rightarrow C_x$, where C_x is the equivalence class for x), and therefore for any sentence F in L the equivalence

$$\mathcal{M} \models F \leftrightarrow \mathcal{M}/\sim \models F$$

holds. Thus the models \mathcal{M} and \mathcal{M}/\sim are elementary equivalent. By virtue of that equivalence the problem of examination whether a formula F is true on \mathcal{M} may be replaced by the problem whether F is true on \mathcal{M}/\sim . Therefore, if the congruence \sim has a finite number of equivalence classes the problem

$$(19) \quad \mathcal{M} \models F$$

is decidable. The important role in such a consideration is played by the greatest congruences, since they have the least number of equivalence classes. For example, one way of proving decidability for the theory in the language L consisting of unary relation symbols and having no axioms is based on the fact that in such a case the greatest congruence of any formula F (i. e. of its relations) has always a finite number of equivalence classes. To prove that

suppose that $\alpha_1, \alpha_2, \dots, \alpha_k$ are all relation symbols appearing in F , i. e. F is in the language $L(F) = \{\alpha_1, \alpha_2, \dots, \alpha_k\}$. Where $\alpha_1, \alpha_2, \dots, \alpha_k$ are unary relation symbols and \mathcal{M} is a model of $L(F)$. Then each of the relations

$$(20) \quad \sim_{\alpha_1}, \sim_{\alpha_2}, \dots, \sim_{\alpha_k}$$

defined by (10) has at most two equivalence classes: first containing those elements of M which are in the relation α_i (if any), where $i \in \{1, \dots, k\}$, and second containing those elements of M which are not in that relation (if any). We designate those two classes with A_i, B_i ($i = 1, 2, \dots, k$) respectively. Thus

$$(21) \quad A_i \stackrel{\text{def}}{=} \{x \in M \mid \alpha_i(x)\}, \quad B_i = \{x \in M \mid \neg \alpha_i(x)\}$$

Two cases are possible: 1° The sets A_i, B_i are both nonempty, 2° One of these sets is empty (i. e. α_i is either empty or full relation).

Relation $\sim_{L(F)}$ being the intersection of the relation (20) has as equivalence classes nonempty sets of the form

$$X_1 \cap X_2 \cap \dots \cap X_k$$

where X_i may be either A_i or B_i . In other words the equivalence classes are nonempty sets of the form

$$(22) \quad \{x \in M \mid \alpha_1^{a_1}(x) \alpha_2^{a_2}(x) \dots \alpha_k^{a_k}(x)\} \quad (a_1, a_2, \dots, a_k \in \{\top, \perp\})$$

where we used the following denotation

F^\top stands for F , F^\perp stands for $\neg F$

$F_1 F_2 \dots F_k$ stands for $(\dots((F_1 \wedge F_2) \wedge F_3) \wedge \dots \wedge F_k)$

(F, F_1, F_2, \dots, F_k are any predicate formulae).

Since there are at most 2^k nonempty sets of the form (22), we conclude that \sim_M has at most 2^k — thus finite number — equivalence classes. Therefore the problem of the form (19) is decidable for any model \mathcal{M} of the language $L(F)$. Moreover that problem is decidable for any model \mathcal{M} of the language L .

In the case the language L contains relation symbols of greater lengths the problem (19) need not to be decidable. In what follows our main purpose is to give some examples of decidable theories having also relation symbols of length greater than 1.

(i) Let L be a relational language containing relation symbols of length 1 or 2. The theory T of L has the following property:

For each binary relation symbol $\rho \in L$ there exist unary relation symbols

$$\alpha_1, \alpha_2, \dots, \alpha_k, \beta_1, \beta_2, \dots, \beta_l$$

say, such that the following formulae

$$(\forall x, y) (\alpha_1^\top(x) \alpha_2^\top(x) \dots \alpha_k^\top(x) \beta_1^\top(y) \beta_2^\top(y) \dots \beta_l^\top(y) \Rightarrow \rho^{a_1}(x, y))$$

$$(23) \quad (\forall x, y) (\alpha_1^\top(x) \alpha_2^\top(x) \dots \alpha_k^\top(x) \beta_1^\top(y) \beta_2^\top(y) \dots \beta_l^\top(y) \Rightarrow \rho^{a_2}(x, y))$$

$$(\forall x, y) (\alpha_1^\perp(x) \alpha_2^\perp(x) \dots \alpha_k^\perp(x) \beta_1^\perp(y) \beta_2^\perp(y) \dots \beta_l^\perp(y) \Rightarrow \rho^{a_2^{k+l}}(x, y))$$

are axioms of T .

In other words, all the formulae of the form

$$(24) \quad (\forall x, y) (\alpha_1^{b_1}(x) \beta_2^{c_2}(x) \cdots \alpha_k^{b_k}(x) \beta_1^{c_1}(y) \beta_2^{c_2}(y) \cdots \beta_l^{c_l}(y) \Rightarrow \rho^{a_i}(x, y))$$

are axioms of T , where $(b_1, b_2, \dots, b_k), (c_1, c_2, \dots, c_l)$ run over $\{\top, \perp\}^k, \{\top, \perp\}^l$ respectively, and with each k -tuple (b_1, b_2, \dots, b_k) and each l -tuple (c_1, c_2, \dots, c_l) exactly one element a_i of $\{\top, \perp\}$ is associated.

First what we are going to prove is that the set of formulae of the form (23) is consistent. Let \mathcal{M} be a model of the language $\{\alpha_1, \alpha_2, \dots, \alpha_k, \beta_1, \beta_2, \dots, \beta_l\}$ and let $\sim_{\alpha_1}, \sim_{\alpha_2}, \dots, \sim_{\alpha_k}, \sim_{\beta_1}, \sim_{\beta_2}, \dots, \sim_{\beta_l}$ be the greatest congruences, related to the relations $\alpha_1, \alpha_2, \dots, \alpha_k, \beta_1, \beta_2, \dots, \beta_l$ respectively. Further, let \sim_1, \sim_2 be the intersection of $\sim_{\alpha_1}, \sim_{\alpha_2}, \dots, \sim_{\alpha_k}$, and $\sim_{\beta_1}, \sim_{\beta_2}, \dots, \sim_{\beta_l}$ respectively. The equivalence classes of \sim_1, \sim_2 are nonempty sets of the form

$$(25) \quad \{x \in M \mid \alpha_1^{b_1}(x) \alpha_2^{b_2}(x) \cdots \alpha_k^{b_k}(x)\}, \quad \{x \in M \mid \beta_1^{c_1}(x) \beta_2^{c_2}(x) \cdots \beta_l^{c_l}(x)\}$$

respectively. By means of conditions (23) we define the relation ρ , i. e. we realise the conditions (23) as implicit definition of ρ . Thus, the definition of ρ reads:

$$(26) \quad \text{If } \alpha_1^{b_1}(x) \alpha_2^{b_2}(x) \cdots \alpha_k^{b_k}(x)$$

and

$$\beta_1^{c_1}(y) \beta_2^{c_2}(y) \cdots \beta_l^{c_l}(y),$$

then

$$\tau\rho(x, y) = a_i$$

where, a_i is the element of $\{\top, \perp\}$ corresponding to $(b_1, b_2, \dots, b_k), (c_1, c_2, \dots, c_l)$. As by assumption a_i is unique, the preceding definition is correct in the case x, y satisfy the conditions

$$(27) \quad \alpha_1^{b_1}(x) \alpha_2^{b_2}(x) \cdots \alpha_k^{b_k}(x), \quad \beta_1^{c_1}(x) \beta_2^{c_2}(y) \cdots \beta_l^{c_l}(y)$$

Further, as the relations \sim_1, \sim_2 are equivalences having as equivalence classes nonempty sets of the form (25), for each ordered pair $(x, y) \in M^2$ there exist nonempty sets of the form (25) such that x belongs to the first of them and y to the second. Therefore the value $\tau\rho(x, y)$ is defined for every pairs $(x, y) \in M^2$. In the case some of the condition (27) is inconsistent, i.e. the corresponding set (25) is empty, the formula (24) becomes \top , we do not have any new information about ρ .

Thus the definition (26) is correct.

Note that it is generally true the following:

If \sim_1, \sim_2 are equivalences of the set M having as equivalence classes

$$(28) \quad A_i (i \in I), \quad B_j (j \in J)$$

respectively, then the following definition of the relation ρ

$$\text{If } x \in A_i, y \in B_j, \text{ then } \tau(x, y) = a_{ij}$$

is correct, where we suppose that a_{ij} is an element of $\{\top, \perp\}$ choosing in the way that to each pair $(i, j) \in I \times J$ there corresponds, exactly one a_{ij} . For example, let $M = \{1, 2, 3, 4, 5\}$ and let the relations \sim_1, \sim_2 be determined by the tables:

\sim_1	1	2	3	4	5
1	\top	\top	\top	\perp	\perp
2	\top	\top	\top	\perp	\perp
3	\top	\top	\top	\perp	\perp
4	\perp	\perp	\perp	\top	\top
5	\perp	\perp	\perp	\top	\top

\sim_2	1	2	3	4	5
1	\top	\top	\perp	\perp	\perp
2	\top	\top	\perp	\perp	\perp
3	\perp	\perp	\top	\top	\perp
4	\perp	\perp	\top	\top	\perp
5	\perp	\perp	\perp	\perp	\top

Equivalence classes for the first relations are

$$A_1 = \{1, 2, 3\}, \quad A_2 = \{4, 5\}$$

and for the second

$$B_1 = \{1, 3\}, \quad B_2 = \{2, 4\}, \quad B_3 = \{5\}$$

the relation ρ determined by

$$x \in A_1 \wedge y \in B_1 \Rightarrow \top \rho(x, y), \quad x \in A_1 \wedge y \in B_2 \Rightarrow \rho(x, y) \quad x \in A_1 \wedge y \in B_3 \Rightarrow \top \rho(x, y),$$

$$x \in A_2 \wedge y \in B_1 \Rightarrow \rho(x, y), \quad x \in A_2 \wedge y \in B_2 \Rightarrow \top \rho(x, y) \quad x \in A_2 \wedge y \in B_3 \Rightarrow \top \rho(x, y)$$

has the following table

ρ	1	2	3	4	5
1	\perp	\perp	\top	\top	\perp
2	\perp	\perp	\top	\top	\perp
3	\perp	\perp	\top	\top	\perp
4	\top	\top	\perp	\perp	\perp
5	\top	\top	\perp	\perp	\perp

or

ρ	1	2	3	4	5
1	\perp	\top	\perp	\top	\perp
2	\perp	\top	\perp	\top	\perp
3	\perp	\top	\perp	\top	\perp
4	\top	\perp	\top	\perp	\perp
5	\top	\perp	\top	\perp	\perp

We return again to the general consideration. We have just concluded that the definition (26) of the relation ρ is correct. Further, let \mathcal{M}' be the expansion of \mathcal{M} obtained by interpreting ρ as the relation defined by (26). \mathcal{M}' is obviously a model for the formulae (23). Thus that set is consistent.

We now prove the following theorem.

Theorem 4. *Let \mathcal{M} be a model of formulae (23), \sim_1 the intersection of the relation $\sim_{\alpha_1}, \sim_{\alpha_2}, \dots, \sim_{\alpha_k}$, \sim_2 the intersection of $\sim_{\beta_1}, \sim_{\beta_2}, \dots, \sim_{\beta_l}$. Then \sim_1 is a left congruence for ρ , \sim_2 is a right congruence and their intersection denoted by \sim , say, is a congruence for ρ .*

Proof. The relations \sim_1, \sim_2 are equivalences, what follows by the proof of theorem 1. In order to prove that \sim_1 is a left congruence and \sim_2 a right congruence for ρ , by the preliminary consideration it suffices to prove the following

$$(29) \quad (\forall x, y, x', y') (x \sim_1 x' \wedge y \sim_2 y' \Rightarrow (\rho(x, y) \Leftrightarrow \rho(x', y')))$$

Let us suppose that some $u, v, u', v' \in M$ satisfy

$$(30) \quad u \sim_1 u', \quad v \sim_2 v'$$

in other words

$$u \sim_{\alpha_1} u', u \sim_{\alpha_2} u', \dots, u \sim_{\alpha_k} u'$$

$$v \sim_{\beta_1} v', v \sim_{\beta_2} v', \dots, v \sim_{\beta_l} v'$$

By definition (9) it means that the following equivalences

$$\alpha_1(u) \Leftrightarrow \alpha_1(u'), \quad \alpha_2(u) \Leftrightarrow \alpha_2(u'), \dots, \alpha_k(u) \Leftrightarrow \alpha_k(u')$$

$$\beta_1(v) \Leftrightarrow \beta_1(v'), \quad \beta_2(v) \Leftrightarrow \beta_2(v'), \dots, \beta_l(v) \Leftrightarrow \beta_l(v')$$

are satisfied

Using the tautologies

$$(p \Leftrightarrow q) \wedge (r \Leftrightarrow s) \Rightarrow (p \wedge r \Leftrightarrow q \wedge s), \quad (p \Leftrightarrow q) \Rightarrow (\neg p \Leftrightarrow \neg q)$$

from the previous equivalences we conclude

$$(31) \quad \alpha_1^{b_1}(u) \alpha_2^{b_2}(u) \dots \alpha_k^{b_k}(u) \beta_1^{c_1}(v) \beta_2^{c_2}(v) \dots \beta_l^{c_l}(v)$$

$$\Leftrightarrow \alpha_1^{b_1}(u') \alpha_2^{b_2}(u') \dots \alpha_k^{b_k}(u') \beta_1^{c_1}(v') \beta_2^{c_2}(v') \dots \beta_l^{c_l}(v')$$

for any k -tuple (b_1, b_2, \dots, b_k) and l -tuple (c_1, c_2, \dots, c_l) .

Let further $a_i \in \{\top, \perp\}$ be the element corresponding to (b_1, b_2, \dots, b_k) , (c_1, c_2, \dots, c_l) such that the formula of the form (24) is an axiom of the theory T . Replacing x, y first with u, v and then with u', v' respectively we obtain

$$(32) \quad \alpha_1^{b_1}(u) \alpha_2^{b_2}(u) \dots \alpha_k^{b_k}(u) \beta_1^{c_1}(v) \beta_2^{c_2}(v) \dots \beta_l^{c_l}(v) \Rightarrow \rho^{a_i}(u, v)$$

$$\alpha_1^{b_1}(u') \alpha_2^{b_2}(u') \dots \alpha_k^{b_k}(u') \beta_1^{c_1}(v') \beta_2^{c_2}(v') \dots \beta_l^{c_l}(v') \Rightarrow \rho^{a_i}(u', v')$$

Using equivalence (31) from (32) it follows immediately

$$(33) \quad \alpha_1^{b_1}(u) \alpha_2^{b_2}(u) \dots \alpha_k^{b_k}(u) \beta_1^{c_1}(v) \beta_2^{c_2}(v) \dots \beta_l^{c_l}(v) \Rightarrow \rho^{a_i}(u, v)$$

$$\alpha_1^{b_1}(u) \alpha_2^{b_2}(u) \dots \alpha_k^{b_k}(u) \beta_1^{c_1}(v) \beta_2^{c_2}(v) \dots \beta_l^{c_l}(v) \Rightarrow \rho^{a_i}(u', v')$$

Therefore it is easy to obtain

$$(34) \quad \alpha_1^{b_1}(u) \alpha_2^{b_2}(u) \dots \alpha_k^{b_k}(u) \beta_1^{c_1}(v) \beta_2^{c_2}(v) \dots \beta_l^{c_l}(v) \Rightarrow \rho^{a_i}(u, v) \rho^{a_i}(u', v')$$

Finally by the tautology $(p \wedge q) \Rightarrow (p \Leftrightarrow q)$ from (33) we have

$$(35) \quad \alpha_1^{b_1}(u) \alpha_2^{b_2}(u) \dots \alpha_k^{b_k}(u) \beta_1^{c_1}(v) \beta_2^{c_2}(v) \dots \beta_l^{c_l}(v) \Rightarrow (\rho^{a_i}(u, v) \Leftrightarrow \rho^{a_i}(u', v'))$$

i.e. by tautology $(\neg p \Leftrightarrow \neg q) \Rightarrow (p \Leftrightarrow q)$

$$(36) \quad \alpha_1^{b_1}(u) \alpha_2^{b_2}(u) \dots \alpha_k^{b_k}(u) \beta_1^{c_1}(v) \beta_2^{c_2}(v) \dots \beta_l^{c_l}(v) \Rightarrow (\rho(u, v) \Leftrightarrow \rho(u', v'))$$

As k -tuple (b_1, b_2, \dots, b_k) and l -tuple (c_1, c_2, \dots, c_l) were arbitrary, from (35) we conclude

$$(37) \quad (\forall b_1, \dots, b_k, c_1, \dots, c_l \in \{\top, \perp\}) \\ (\alpha_1^{b_1}(u) \alpha_2^{b_2}(u) \dots \alpha_k^{b_k}(u) \beta_1^{c_1}(v) \beta_2^{c_2}(v) \dots \beta_l^{c_l}(v)) \Rightarrow (\rho(u, v) \Leftrightarrow \rho(u', v'))$$

By the valid formula

$$(\forall x) (A(x) \Rightarrow B) \Leftrightarrow ((\exists x) A(x) \Rightarrow B) \quad (x \text{ is not free in } B)$$

it follows that (37) is equivalent to

$$(38) \quad (\exists b_1, \dots, b_k, c_1, \dots, c_l \in \{\top, \perp\}) \\ \alpha_1^{b_1}(u) \alpha_2^{b_2}(u) \dots \alpha_k^{b_k}(u) \beta_1^{c_1}(v) \beta_2^{c_2}(v) \dots \beta_l^{c_l}(v) \Rightarrow (\rho(u, v) \Leftrightarrow \rho(u', v'))$$

As the formula

$$(\exists b_1, \dots, b_k, c_1, \dots, c_l \in \{\top, \perp\}) \alpha_1^{b_1}(u) \alpha_2^{b_2}(u) \dots \alpha_k^{b_k}(u) \beta_1^{c_1}(v) \beta_2^{c_2}(v) \dots \beta_l^{c_l}(v)$$

is a tautology, implication (38) becomes

$$(39) \quad \rho(u, v) \Leftrightarrow \rho(u', v')$$

Thus from assumption (30) it follows conclusion (39) what means that formula (29) is true. Therefore we conclude that \sim_1 is a left and \sim_2 a right congruence for ρ . Their intersection \sim is then congruence for ρ what completes the proof of the theorem.

Since \sim is the greatest congruence for the set of relations

$$\{\alpha_1, \alpha_2, \dots, \alpha_k, \beta_1, \beta_2, \dots, \beta_l\}$$

and a congruence for ρ , \sim is the greatest congruence for the set

$$\{\alpha_1, \alpha_2, \dots, \alpha_k, \beta_1, \beta_2, \dots, \beta_l, \rho\}$$

Now, let F be a formula in the language L . Of course, F contains only a finite number of relation symbols. Further, we have a set of axioms of the form (23), related to each binary relation symbol and a relation \sim satisfying the conditions of theorem 4. Each such a relation \sim has a finite number of equivalence classes. The same is true for the greatest congruences of unary relations of the formula F . The greatest congruence \sim_F for F (i.e. for relations corresponding to the relation symbols of F) is the intersection of all the greatest congruences corresponding to the relation symbols of F . Therefore \sim_F has also a finite number of equivalence classes whence we conclude that the problem (19) is decidable.

(ii) In the similar way it can be proved the decidability of the theory T in the language L having in addition relational symbols of length greater than two and satisfying the following condition:

For each $\rho \in L$ of length n ($n \geq 2$) there exist in L unary relation symbols

$$\begin{aligned} &\alpha_{11}, \alpha_{12}, \dots, \alpha_{1k_1} \\ &\alpha_{21}, \alpha_{22}, \dots, \alpha_{2k_2} \\ &\dots \dots \dots \dots \dots \dots \\ &\alpha_{n1}, \alpha_{n2}, \dots, \alpha_{nk_n} \end{aligned}$$

such that the formulae of the form

$$(40) \quad (\forall x_1, x_2, \dots, x_n) \left[\begin{array}{l} \alpha_{11}^{b_{11}}(x_1) \alpha_{12}^{b_{12}}(x_1) \dots \alpha_{1k_1}^{b_{1k_1}}(x_1) \\ \alpha_{21}^{b_{21}}(x_2) \alpha_{22}^{b_{22}}(x_2) \dots \alpha_{2k_2}^{b_{2k_2}}(x_2) \Rightarrow \rho^{a_i}(x_1, x_2, \dots, x_n) \\ \alpha_{n1}^{b_{n1}}(x_n) \alpha_{n2}^{b_{n2}}(x_n) \dots \alpha_{nk_n}^{b_{nk_n}}(x_n) \end{array} \right]$$

are axioms of T , where $(b_{11}, b_{12}, \dots, b_{1k_1}), (b_{21}, b_{22}, \dots, b_{2k_2}), \dots, (b_{n1}, b_{n2}, \dots, b_{nk_n})$ run over the sets $\{\top, \perp\}^{k_1}, \{\top, \perp\}^{k_2}, \dots, \{\top, \perp\}^{k_n}$ respectively, $a_i \in \{\top, \perp\}$ and for each n given tuples of previous form there corresponds exactly one a_i .

The proof has only technical differences from the proof in the example (i). Namely, at first it can be proved that the relations $\sim_1, \sim_2, \dots, \sim_n$ defined as the intersections of k_1, k_2, \dots, k_n relations:

$$\begin{aligned} &\sim_{\alpha_{11}}, \sim_{\alpha_{12}}, \dots, \sim_{\alpha_{1k_1}} \\ &\sim_{\alpha_{21}}, \sim_{\alpha_{22}}, \dots, \sim_{\alpha_{2k_2}} \\ &\sim_{\alpha_{n1}}, \sim_{\alpha_{n2}}, \dots, \sim_{\alpha_{nk_n}} \end{aligned}$$

respectively is a congruence for ρ at first, second, \dots , n^{th} coordinate, and that their intersection \sim is a congruence for ρ .

Further, relate to the arbitrary formula F all the greatest congruences of its relations. There is a finite number of these congruences and each of them has a finite number of equivalence classes, whence it follows that the greatest congruence for F has also a finite number of equivalence classes. Thus, the problem (19) is decidable.

REFERENCES

- [1] Bernays, P. and Schönfinkel, M., *Zum Entscheidungsproblem der mathematischen Logik*, Math. Ann t. 99 (1928), pp. 348—372.
- [2] Löwenheim, L., *Über die Auflösungen von Gleichungen im logischen Gebietskalkul*, Math. Ann. t. 68 (1919), pp. 169—207
- [3] Quine, W. V., *O Sentido da Nova Lógica*, São Paulo, Brazil, 1944
- [4] Prešić, M. D., *On certain formulas for equivalence and order relations*, Mat. vesnik Beograd, 7 (22), 1970, pp. 143—148
- [5] Prešić, S. B., *Une classe d'équations matricielles et l'équation $f^2 = f$* , Publ. Inst. Math. Beograd, t. 8 (22), 1968, pp. 143—148
- [6] Prešić, S. B., *Ein Satz über reproduktive Lösungen*, Publ. Inst. Math. Beograd, t. 14 (28), 1972, pp. 133—136
- [7] Rudeanu, S., *Boolean Functions and Equations*, Amsterdam, London, New York, 1974
- [8] Schröder, E., *Der Operationskreis des Logikkalkuls*, Leipzig, 1877