Mathematica Slovaca

Ivan Korec

Disjoint covering systems and product-invariant relations

Mathematica Slovaca, Vol. 35 (1985), No. 3, 233--237

Persistent URL: http://dml.cz/dmlcz/136394

Math. Slovaca 35, 1985, No. 3, 233—237

DISJOINT COVERING SYSTEMS AND PRODUCT-INVARIANT RELATIONS

IVAN KOREC

I. Introduction and notation

A system of residue classes of the additive group $(Z, +)$ of integers

$$a_i \pmod{n_i}, \quad i=1, \ldots, k \quad (k \geqq 2) \tag{1}$$

is said to be a disjoint covering system (DCS) if every integer belongs to exactly one of the residue classes (1). Every finite system of pairwise disjoint residue classes (with moduli greater than 1) can be completed to a DCS. Among other problems concerning DCS, conditions on the moduli

$$n_1, \ldots, n_k \tag{2}$$

were studied. For example, for every DCS (1) the following conditions hold (see [1]):

$$\sum_{i=1}^{k} \frac{1}{n_i} = 1. \tag{A}$$

$$D(n_i, n_j) > 1 \quad \text{for every} \quad i, j = 1, \ldots, k. \tag{B}$$

Here $D(x, y)$ denotes the greatest common divisor of x, y; the symbols (x, y) and $(x_1, \ldots, x_k)$ are reserved for the ordered pair and the ordered k-tuple, respectively. The condition (B) contains also the formulas with $i = j$; we shall need them only to exclude $n_i = 0$ when (B) is considered separately, i.e. without (A).

The property (B) (for fixed i, j) is expressible by a formula in the first order language of the multiplicative semigroup $(N, \cdot)$ of nonnegative integers. (The symbol $>$ can be excluded from (B).) We shall show that (B) is the strongest condition of this kind which holds for the moduli of every DCS. The restriction to the first order language could be weakened but the restriction to the only non-logical symbol $\cdot$ is substantial.

Since we use only the usual notation we need not repeat it in details. We only notice that $\bigwedge$ is used for the conjunction of several formulas, and not as a quantifier. The non-logical symbols $\cdot$, $+$, 0, 1, etc., are used in their usual (hence fixed) meaning, so that we need not explicitly specify the semantics of the formulas.

II.

Definition 1. *An s-ary relation R on the set N of nonnegative integers will be called product-invariant if for every automorphism f of the semigroup $(N, \cdot)$ and for every $x_1, \ldots, x_s \in N$*

$$(x_1, \ldots, x_s) \in R \leftrightarrow (f(x_1), \ldots, f(x_s)) \in R.$$

There is a one-to-one correspondence between the set of automorphisms of $(N, \cdot)$ and the set of all permutations of the set P of primes. Indeed, if π is a permutation of P, then the corresponding automorphism f is given by

$$f(x)=0 \quad \text{if} \quad x=0 \quad \text{and}$$
$$f(x)=\pi(p_1)^{a_1} \cdot \ldots \cdot \pi(p_n)^{a_n}, \text{ where } x=p_1^{a_1} \cdot \ldots \cdot p_n^{a_n}$$

is the standard form of x if $x \neq 0$.
Conversely, since the set P is first-order definable in $(N, \cdot)$ the restriction of any automorphism f of $(N, \cdot)$ to the set P is a permutation of P.

Every relation R which is (first or higher order) definable in the semigroup $(N, \cdot)$ is obviously product-invariant; the converse need not hold. The symbols 0, 1, $|$, D can be defined by the formulas

$$x=0 \leftrightarrow \forall y(x \cdot y=x), \qquad x=1 \leftrightarrow \forall y(x \cdot y=y), \qquad x|y \leftrightarrow \exists z\,(x \cdot z=y)$$

and

$$z=\mathrm{D}(x, y) \leftrightarrow z|x \wedge z|y \wedge \forall w(w|x \wedge w|y \rightarrow w|z).$$

The symbols $>$, $+$, 2, 3, etc., are not definable because the corresponding relations (e.g., the unary relation $\{2\}$ for the symbol 2) are not product-invariant. However, $\mathrm{D}(x, y)>1$ can be replaced by $\mathrm{D}(x, y) \neq 0 \wedge \mathrm{D}(x, y) \neq 1$.

Definition 2. *For every integer $k \geq 1$ denote by E_k the set of all k-tuples $(n_1, \ldots, n_k) \in N^k$ for which there are $a_1, \ldots, a_k \in N$ such that* (1) *is a DCS. Further, for every $s \geqq 1$ denote by H_s the set of all s-tuples $(n_1, \ldots, n_s)$ for which there are $k \geqq s$ and $n_{s+1}, \ldots, n_k$ such that*

$$(n_1, \ldots, n_s, n_{s+1}, \ldots, n_k) \in E_k,$$

and by U_s the smallest product-invariant set which contains H_s.

The existence of U_s follows from the fact that the intersection of any set of s-ary product-invariant relations is a product-invariant relation. For $s=1$ we have $E_1=\emptyset$ because of the condition $k \geqq 2$ in the definition of DCS, and $H_1=U_1=N-\{0, 1\}$. Notice also that the relations E_s, H_s, U_s are symmetric in the following sense.

Definition 3. *An s-ary relation R is said to be symmetric if for every permutation π of the set $\{1, \ldots, s\}$ and every $x_1, \ldots, x_s$*

$$(x_1, \ldots, x_s) \in R \leftrightarrow (x_{\pi(1)}, \ldots, x_{\pi(s)}) \in R.$$

Theorem 1. *For every integer $s \geqq 1$*

$$U_s = \left\{(x_1, \ldots, x_s) \in N^s;\ \bigwedge_{i,j=1}^{s} (\mathrm{D}(x_i, x_j) > 1)\right\}. \tag{3}$$

Proof. Denote by V_s the right-hand side of (3). Since the set V_s is first-order definable in $(N, \cdot)$ (elimination of ">1" was explained above) it is also product-invariant. Further, since every DCS satisfies (B) the set V_s contains H_s, and hence $U_s \subseteq V_s$. To prove the converse, consider arbitrary $(x_1, \ldots, x_s) \in V_s$. Choose an automorphism f of $(N, \cdot)$ which maps every prime divisor of the product $x_1 \cdot \ldots \cdot x_s$ onto a prime greater or equal s, and denote

$$(y_1, \ldots, y_s) = (f(x_1), \ldots, f(x_s)).$$

If we show $(y_1, \ldots, y_s) \in H_s$, then $(y_1, \ldots, y_s) \in U_s$, and since U_s is product-invariant $(x_1, \ldots, x_s) \in U_s$. This will complete the proof.

To prove $(y_1, \ldots, y_s) \in H_s$ it suffices to show that the congruence classes

$$1 \pmod{y_1},\ 2 \pmod{y_2}, \ldots, s \pmod{y_s}$$

are pairwise disjoint. If they are not, then there are z, t, i, j, $1 \leqq i < j \leqq s$ such that $i + z \cdot y_i = j + t \cdot y_j$. Let p be a common prime divisor of x_i, x_j. Then $f(p)$ is a common prime divisor of y_i, y_j, and hence $f(p) | j - i$, which contradicts $0 < j - i < s$ and $f(p) \geqq s$.

As an immediate consequuence we obtain the following statement which is formulated in the metalanguage.

Corollary. *Let φ be a first order formula with s free variables and the only non-logical symbol "$\cdot$". Let for every DCS* (1) *the following condition hold:*

(C) $\varphi(n_{i_1}, \ldots, n_{i_s})$ *for all s-tuples* $(i_1, \ldots, i_s)$ *of pairwise different* $i_1, \ldots, i_s \in \{1, \ldots, k\}$.

Then (B) *implies* (C).

In other words: (B) is the strongest among all conditions of the form (C) which are necessary for (1) to be a DCS. Notice that (B) is not exactly of the form (C) because $i = j$ is considered in (B). However, we can obtain a condition equivalent to (B) if we take $\mathrm{D}(x, y) \neq 1 \wedge x \neq 0 \wedge y \neq 0$ for φ in (C).

III. Concluding remarks

1. The condition (A) implies: For every $(n_1, \ldots, n_s) \in H_s$

$$\text{(A}'\text{)} \qquad \sum_{i=1}^{s} \frac{1}{n_i} \leqq 1.$$

The condition (A′) is not equivalent to any condition (C), and it is not a consequence of (B). Hence (A′)∧(B) is a stronger necessary condition for the members of H_s. However, it is not a sufficient one. Moreover, we shall show that for every positive ε there is $(n_1, n_2, n_3) \in U_3 - H_3$ such that $n_1^{-1} + n_2^{-1} + n_3^{-1} < \varepsilon$. It suffices to put $(n_1, n_2, n_3) = (2p, 2q, 2r)$ where p, q, r are sufficiently large pairwise different primes. Obviously $(3p, 3q, 3r) \in H_3$, and hence $(2p, 2q, 2r) \in U_3$. However, $(2p, 2q, 2r) \notin H_3$ because the congruence classes

$$a \pmod{2p}, \quad b \pmod{2q}, \quad c\,(\text{mos } 2r)$$

could be pairwise disjoint only if the parities of a, b, c are distinct, which is impossible. Analogical examples can be found for every $s \geqq 3$.

2. It can be shown that the sets E_s, H_s are primitive recursive. Hence they are first order definable by formulas with the two non-logical symbols + and ·, i.e. in the structure $(N, +, \cdot)$. We submit the conjecture that every set H_s is first order definable by a formula with the non-logical symbol · and constants. (For the sets E_s it is obvious because they are finite.)

3. The conditions (A′), (B) for the members of H_s (or (A), (B) for the members of E_s) can be readily checked. Roughly speaking, they can be verified within polynomial many arithmetical operations for any given sequence (2) (with respect to the length of the usual code of (2)). From this point of view, they are more advantageous than conditions which consider arbitrary subsequences or partitions of $\{1, \ldots, k\}$. A straightforward verifying of such a condition needs at least exponential time. (Condition of this type can be found, e.g., in [4].) A question arises whether the sets

$$\bigcup_{s=1}^{\infty} H_s, \qquad \bigcup_{s=1}^{\infty} E_s$$

can be recognized in the polynomial time.

REFERENCES

[1] ERDÖS, P.: Egy kongruenciarendszerekről szóló problémáról. Matematikai Lapok, 4, 1952, 122—128.
[2] KOREC, I.—ZNÁM, Š.: On disjoint covering of groups by their cosets. Mathematica Slovaca 27, 1, 1977, 3—7.
[3] PORUBSKÝ, Š.: Results and problem on covering systems of residue classes. Mitt. Math. Semin. Giessen, Heft 150, 1981, 1—85.
[4] ZNÁM, Š.: A survey on covering systems of congruences. Acta Mathematica Univ. Comen., 40—41, 1982, 59—79.

Received February 14, 1983

Katedra algebry a teórie čísel
Matematicko-fyzikálna fakulta Univerzity Komenského
Mlynská dolina
842 15 Bratislava

ТОЧНО НАКРЫВАЮЩИЕ СИСТЕМЫ И ОТНОШЕНИЯ, ИНВАРИАНТНЫЕ ОТНОСИТЕЛЬНО УМНОЖЕНИЯ

Ivan Korec

Резюме

Конечная система (1) смежных классов аддитивной группы целых чисел называется точно накрывающей системой, если всякое целое число принадлежит одному и только одному из классов (1). Хорошо известно, что для всякой т.н.с. (1) выполняются условия (A) и (B). Условие (B) формулируемо в элементарной теории мультипликативной полугруппы $(N, \cdot)$ натуральных чисел. Точнее, (B) эквивалентно условию (C) для подходящей формулы φ этой теории T. Доказывается следующий результат:

Пусть φ — формула теории T такая, что (C) выполняется для всякой т.н.с. (1); тогда (C) является следствием (B).

Итак, (B) является самым сильным среди условий типа (C) необходимых для того, чтобы (1) была т.н.с. В доказательствие используется, что всякое отношение, определимое в теории T, инвариантно относительно всех автоморфизмов полугруппы $(N, \cdot)$. Такие отношения были в статье названы инвариантными относительно умножения.