

P. GORALČÍK

Z. HEDRLÍN

V. KOUBEK

J. RYŠUNKOVÁ

A game of composing binary relations

RAIRO. Informatique théorique, tome 16, n° 4 (1982), p. 365-369

http://www.numdam.org/item?id=ITA_1982__16_4_365_0

© AFCET, 1982, tous droits réservés.

L'accès aux archives de la revue « RAIRO. Informatique théorique » implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques

<http://www.numdam.org/>

A GAME OF COMPOSING BINARY RELATIONS (*)

by P. GORALČÍK, Z. HEDRLÍN,
V. KOUBEK et J. RYŠLÍKOVÁ (1)

Communicated by J. BERSTEL

Résumé. — Nous étudions la longueur du plus court produit de relations binaires, pris dans un ensemble fini et donnant un résultat prescrit. On montre que dans certains cas, cette longueur croît polynomialement en fonction de la taille des relations, et que dans d'autres cas, une telle majoration n'existe pas.

Abstract. — We study the length of the shortest product of binary relations taken in a finite set and giving a prescribed result. We show that in some cases this length grows polynomially with the size of the relations, and that in other cases, such an upper bound does not exist.

The game is for one player, who is given a family $\mathcal{R} = \{R_1, \dots, R_k\}$ of binary relations on a set X of size n and whose goal is to compose, as quickly as possible, a relation S of a specified form from those in \mathcal{R} . Of course, one must be sure that it can be done, i. e. that S belongs to the semigroup \mathcal{R}^+ generated by \mathcal{R} . Next, since the only thinkable point in playing this sort of patience is to kill time, it would be interesting to know how quickly — polynomially or not — the necessary time spent on it grows with the size n of the underlying set X . The necessary time can be measured by the length of the shortest sequence $w = (R_{i_1}, \dots, R_{i_s})$ in \mathcal{R} such that $R_{i_1} \dots R_{i_s} = S$ (where on the left is the right-hand composition of w defined by: $(x, z) \in R_{i_1} \dots R_{i_s}$ iff there exists a sequence y_0, y_1, \dots, y_s such that $y_0 = x$, $y_s = z$, and $(y_{k-1}, y_k) \in R_{i_k}$ for all $k = 1, \dots, s$).

It will be convenient to write $R_{i_1} \dots R_{i_s}$ instead of $(R_{i_1}, \dots, R_{i_s})$ when it is clear if a word in \mathcal{R} or the corresponding composition is meant.

Let us consider five types of possible resulting relation S : the identity $1_X = \{(x, x) \mid x \in X\}$, a constant (i. e. a transformation of X with one-point image), the universal relation X^2 , the empty relation \emptyset , a hyperconstant ($R \subseteq X^2$ is a hyperconstant iff $\exists y \forall x ((x, y) \in R)$). We shall show that no one of these can be composed in a polynomial time unless we confine the relations

(*) Received March 1981, revised September 1981.

(1) MFF KU, Sokolovska 83, 18600 Praha 8, Tchécoslovaquie.

occurring in \mathcal{R} to some more restricted class \mathcal{C} of relations, such as e.g. partial transformations, (full) transformations, or rich relations (defined as the relations with both projections equal to X).

Combining the classes \mathcal{C} of relations just mentioned with the above five possibilities for S we can formulate the following bunch of results :

$\mathcal{C} \backslash S$	1_X	Constant	X^2	\emptyset	Hyperconstant
General relations.	N	N	N	N	N
Partial transformations.	N	N		P	N
Transformations.	N	P			P
Rich relations.	N		P		P

THEOREM: *In the above Table the filled entries assign to the corresponding couples (\mathcal{C}, S) true statements P or $N = \text{non } P$, where $P =$ "there exists a polynomial $p(n)$ such that, for an arbitrary family $\mathcal{R} \subseteq \mathcal{C}$ of binary relations on an n -set X such that $S \in \mathcal{R}^+$, the shortest sequence $(R_{i_1}, \dots, R_{i_s})$ in \mathcal{R} with $R_{i_1} \dots R_{i_s} = S$ has length $s \leq p(n)$ ".*

The blank entries in the Table indicate that S cannot be generally composed from the relations in \mathcal{C} .

Proof: Thanks to the logical interconnections we soon discover between some of the entries we need not prove all of them but concentrate upon the key ones.

Starting with the first column, realize that 1_X can be composed only from permutations on X . However, even in case \mathcal{R} consists of a single permutation f we have no polynomial bound on the least positive integer r with $f^r = 1_X$ (the order $\text{Ord}(f)$). Indeed, taking $n = \sum_{i=1}^k p_i$, the sum of the first k primes, and a permutation f with exactly one p_i -cycle for each $i = 1, \dots, k$, we have, using the well-known Tchebyscheff's estimate [2], $p_i \leq p_k \leq k^2$ for $i = 1, \dots, k$, whence $n = \sum_{i=1}^k p_i \leq k p_k \leq k^3$, therefore $\text{Ord}(f) = \prod_{i=1}^k p_i \geq k! \geq [\sqrt[3]{n}]!$, which establishes all the entries in the first column of the table.

We use the fact that there is no polynomial bound on the orders of permutations for establishing all the other cases of non-polynomiality; all of

them will involve a fixed permutation f of maximal order r on X and a fixed transformation g taking each cycle of f constantly into itself (see fig. 1).

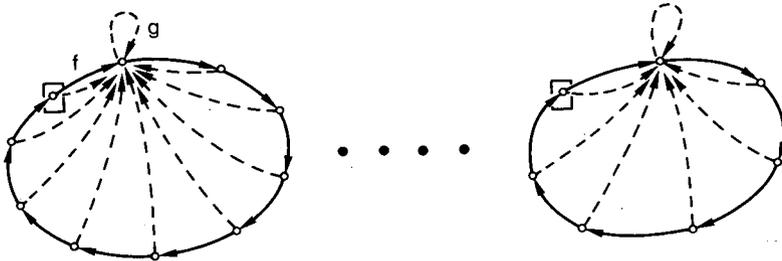


Fig. 1

The set $Y = Xgf^{-1} = \{y \in X \mid yf \in \text{Im}(g) = Xg\}$, consisting of points marked by little squares in figure 1, enters into description of the following relations:

$R = Y \times X$, the arrows go only from each point $y \in Y$ to all points of X ;

$\bar{R} = X^2 - R$, the complement of R ;

ψ , a partial transformations of X with domain Y , taking Y as a constant into itself.

(a) Let $\mathcal{R} = \{f, g, R\}$. Then we have $X^2 = gf^{-1}R \in \mathcal{R}^+$. The shortest word in \mathcal{R} giving X^2 cannot start with R , for $xR = \emptyset$ if $x \notin Y$. The first occurrence of R must be preceded by a subword gf^k with $\text{Im}(gf^k) \subseteq Y$ which is only possible with $f^k = f^{-1}$. Thus the shortest word giving X^2 is unique and equal to $gf^{r-1}R$, where $r = \text{Ord}(f)$. This proves that X^2 cannot be polynomially composed from general relations.

(b) Let $\mathcal{R} = \{f, g, \bar{R}\}$. Then $\emptyset = gf^{-1}\bar{R} \in \mathcal{R}^+$. The shortest word in \mathcal{R} giving \emptyset must be ended by \bar{R} . Throwing the last letter \bar{R} away we must get a relation with the image (second projection) contained in Y , which is possible only if the last occurrence of \bar{R} is preceded by gf^{r-1} . For any $w \in \mathcal{R}^+$, either $w\bar{R} = \emptyset$ or the second projection of $w\bar{R}$ is X . Again, the shortest word in \mathcal{R} giving \emptyset is unique and equal to $gf^{r-1}\bar{R}$, which proves that \emptyset cannot be polynomially composed from general relations.

(c) Let $\mathcal{R} = \{f, g, \psi\}$. Then $gf^{-1}\psi$ is a constant contained in \mathcal{R}^+ . In the shortest word in \mathcal{R} giving a constant, ψ cannot be the first letter. Moreover, the first occurrence of ψ must be preceded by the shortest word in $\{f, g\}$ giving a transformation with image contained in Y , which is gf^{r-1} . Thus $gf^{r-1}\psi$ is

the shortest word giving a constant, which proves that neither a constant nor a hyperconstant can be polynomially composed from partial transformations, and thus neither from general relations.

(d) Let \mathcal{R} be a family of partial transformations such that $\Phi \in \mathcal{R}^+$. Then the subset $Z \subseteq X$ of all points z such that some $\varphi \in \mathcal{R}$ is not defined in z is non-void and for every $x \in X$ there exists a word w in \mathcal{R} such that $xw \in Z$, thus $xw\varphi = \Phi$ for a suitable $\varphi \in \mathcal{R}$. Let $w = a_1 \dots a_k$. If the sequence $xa_1, xa_1 a_2, \dots, xa_1 a_2 \dots a_k$ is not one-one then we clearly can find a shorter word w' with $xw' = xw$, thus we can assume that w is of length $k \leq n-1$. Let $X = \{x_1, \dots, x_n\}$. We can recursively define a sequence of words w_1, \dots, w_n in \mathcal{R} , each of length $\leq n$, such that:

$$x_1 w_1 = \Phi, x_2 w_1 w_2 = \Phi, \dots, x_n w_1 \dots w_n = \Phi.$$

Then $w = w_1 \dots w_n$ is a word of length $\leq n^2$ giving Φ .

(e) This is well-known (*cf.* [1]). A simple argument is as follows: If \mathcal{R} is a set of transformations on X such that \mathcal{R}^+ contains a constant then any pair of points of X can be merged by a word in \mathcal{R} of length $\leq \binom{n}{2} - 1$ and we must merge at most $n-1$ couples to get a constant, which yields the estimate $(n^3/2) - n^2 - (n/2) + 1$.

(f) Let \mathcal{R} be a set of rich relations on X such that \mathcal{R}^+ contains a hyperconstant. Define a set of transformations \mathcal{T} by $f \in \mathcal{T}$ iff there exists $R \in \mathcal{R}$ such that $f \subseteq R$. Then we prove that \mathcal{T}^+ contains a constant: Let $X \times \{c\} \subseteq R_1 \dots R_k$, where R_j are rich for all $j=1, \dots, k$. Then we have a matrix $(x_{i,j})$, $i=1, \dots, n, j=0, \dots, k$, such that $\{x_{1,0}, \dots, x_{n,0}\} = X$, $x_{1,k} = \dots = x_{n,k} = c$, and $(x_{i,j-1}, x_{i,j}) \in R_j$ for all $i=1, \dots, n, j=1, \dots, k$. We form recursively a new matrix $(y_{i,j})$ of the same type as follows: we put $y_{1,j} = x_{1,j}$ for all $j=0, \dots, k$; to each $i=2, \dots, n$ we find the smallest $j(i)$ such that $x_{i,j(i)} = y_{s,j(i)}$ for some $s < i$ (there must be such, since $x_{i,k} = x_{s,k}$ for any i, s) and put:

$$\begin{aligned} y_{i,j} &= x_{i,j} & \text{for all } i=2, \dots, n & \quad \text{and} & \quad j \leq j(i), \\ y_{i,j} &= y_{s,j} & \text{for all } i=2, \dots, n & \quad \text{and} & \quad j > j(i), \end{aligned}$$

where s is such that $s < i$ and $x_{i,j(i)} = x_{s,j(i)}$. Then:

$$\varphi_j = \{(y_{i,j-1}, y_{i,j}) \mid i=1, \dots, n\}$$

is a partial transformation of X , $\varphi_j \subseteq R_j$ for every $j=1, \dots, k$. Since R_j is rich, we can easily extend φ_j to a full transformation f_j so that $\varphi_j \subseteq f_j \subseteq R_j$, for every

$j=1, \dots, k$. Clearly, $f_1 \dots f_k = X \times \{c\}$. By (e), this constant can be composed from \mathcal{F} polynomially. Replacing in this composition each transformation by a relation from \mathcal{R} containing it, we get a polynomial composition of a hyperconstant from the relations in \mathcal{R} .

(g) Let $X^2 \in \mathcal{R}^+$ for a set \mathcal{R} of rich relations on X . Since X^2 is a hyperconstant, we have a word w_1 in \mathcal{R} of length $\leq n^3$ which contains a constant, say on $c_1 \in X$. Noting that converses of rich relations are again rich and the converse of X^2 is X^2 , we can, for the same reason, polynomially compose a hyperconstant w_2^{-1} , say on $c_2 \in X$, from the converses of the relations in \mathcal{R} . Then $w_2 \in \mathcal{R}^+$. There must exist a word u in \mathcal{R} not longer than $n-1$ such that $c_1 u = c_2$. Then $w_1 u w_2 = X^2$ polynomially.

The theorem is proved.

J.-E. PIN [1] asked about the length of a shortest word composing X^2 from a family of binary relations. Our result shows it is not polynomial. Likewise, a full constant cannot be polynomially composed from partial functions (while Pin shows that a partial constant can be so). Hence it makes difference if we conceive synchronization in the incompletely specified automata as by a word acting on the states as a full or only as a partial constant.

REFERENCES

1. J.-E. PIN, *Le problème de la synchronisation et la conjecture de Černý*, in A. DELUCA, Ed., *Non Commutative Structures in Algebra and Geometric Combinatorics*, C.N.R., 1978, pp. 46-58.
2. W. SCHWARZ, *Einführung in Methoden und Ergebnisse der Primzahltheorie*, BI-Hochschultaschenbuch, 278/278a, Mannheim, 1969.