Mathematical Institute
Slovak Academy of Sciences, Bratislava

Preprint 25/1996

Ivan Korec

Algebraical constructions of reversible generalized Pascal triangles and one–dimensional cellular automata

August 15, 1996

PREPRINT SERIES

Algebraical constructions of reversible generalized Pascal triangles and one-dimensional cellular automata

Ivan KOREC, Bratislava

Abstract

The notion of reversibility in algebras for generalized Pascal triangles and local rules of one-dimensional cellular automata is discussed. Several constructions of such algebras and rules are presented. Some constructions start from operations satisfying cancellation law and produce reversible operations, resp. local rules. Other constructions, permutation of values and permutation of arguments, (1) preserve reversibility and (2) give nontrivial examples from simpler ones. These constructions are very simple but nevertheless they can substantially increase the complexity of underlying generalized Pascal triangles (or computations of cellular automata).

1 Introduction

Generalized Pascal triangles (abbreviation: GPT) can be used to describe computations of one-dimensional cellular automata (abbreviation: 1D CA) from finite initial configurations. They were originally defined in [K85] to study the structure of (regular) real-time systolic trellis automata, see [CGS]. We shall give their definition, and also repeat the definition of 1D CA.

Definition 1.1 *For every algebra* $\mathcal{A} = \langle \mathbf{A}; *, \mathrm{o}\rangle$ *of signature* $(2, 0)$ *and every word* $w \in \mathbf{A}^+$ *the function* $G = \mathrm{GPT}(\mathcal{A}, w)$ *will be the mapping of a subset*

The work was supported by Grant 1224 of Slovak Academy of Sciences.

AMS 1991 Subject Classification: Primary 08A70, Secondary 68Q80.

Keywords and phrases: Reversible cellular automata, quasigroups, cancellation law.

of $\mathbb{N} \times \mathbb{N}$ *into* $\mathbf{A}$ *given by*

$$G(x,y) = \begin{cases} \text{undefined} & \text{if} \quad x+y < |w|-1, \\ w(x) & \text{if} \quad x+y = |w|-1, \\ \mathrm{o} * G(0, y-1) & \text{if} \quad x = 0, \ y \geq |w|, \\ G(x-1, 0) * \mathrm{o} & \text{if} \quad y = 0, \ x \geq |w|, \\ G(x-1, y) * G(x, y-1) & \text{if} \quad x+y \geq |w|, \ x > 0, \ y > 0. \end{cases}$$

The functions of the form $\mathrm{GPT}(\mathcal{A}, w)$ *for a finite algebra* $\mathcal{A}$ *and a word* $w \in \mathbf{A}^+$ *will be called generalized Pascal triangles.*

Definition 1.2 *A one-dimensional cellular automaton is an ordered quadruple* $C = (S, N, f, q)$*, where*

S *is a finite set of states;*

$N = (a_1, \ldots, a_n)$*, the neighbourhood vector, is a finite sequence of integers;*

$f : S^n \to S$ *is a local transition function;*

$q \in S$*, the quiescent state, satisfies* $f(q, \ldots, q) = q$.

A computation of one-dimensional CA C *is a function* $F : \mathbb{Z} \times \mathbb{N} \to S$ *such that*

$$F(z, t+1) = f(F(z+a_1, t), \ldots, F(z+a_n, t))$$

for all $z \in \mathbb{Z}$*,* $t \in \mathbb{N}$.

The restrictions of F *to sets* $\mathbb{Z} \times \{t\}$*,* $t \in \mathbb{N}$ *will be called configurations, for* $t = 0$ *the initial configuration. A configuration (at time* t*) is called finite if* $F(z,t) = q$ *for all but finitely* $z \in \mathbb{Z}$.

As we can see from the above, GPT are defined so that they immediately correspond to computations of one-sided 1D CA from finite initial configurations. (The mentioned automata have binary local transition functions (i.e., $n = 2$ above) and neighborhood types $(0,1)$ or $(-1,0)$. They were considered e.g. in [CGS].) In the relation to one-sided 1D CA the binary operation of the underlying algebra corresponds to the local transition rule and its constant to the quiescent state. The relationship to other one-dimensional CA also can be established, although it is not so immediate; every element of the algebra can correspond to a $k$tuple of states. The details were considered in [K85].

By Definition 1.1 GPT are constructed top-down, similarly as the classical Pascal triangle can be constructed. A GPT will be called reversible if it can be locally constructed also bottom-up, using a binary operation. An algebra will be called reversible if all its GPT are reversible. (The definitions will be repeated more formally later.) Several kinds of reversibility of algebras will be introduced; all of them lead to reversible one-sided 1D CA. (However, general reversibility of 1D CA will not be completely covered by them because it allows reverse local transition rules with more than two arguments.)

In Section 2 monoids of binary operations and various kinds of reversibility of binary operations (and algebras of signature $(2,0)$) are introduced. The relationship between reversibility and invertibility in the monoids of binary operations is established.

Section 3 deals with two constructions of binary operations from other binary operations: permutation of values and permutation of arguments. These constructions use a permutation of the base set $\mathbf{A}$; the base set itself is not changed. The construction is applied here mainly to algebras from Definition 1.1. We usually want to preserve the constant o, and therefore only permutations preserving o are usually used. Both permutation of arguments and permutation of values preserve reversibility. We shall deal with binary operations but the generalization to n-ary operations (or local transition rules), and also to higher dimensions, is straightforward.

Section 4 contains some constructions of reversible algebras from groupoids satisfying cancellation laws (both or one of them). Elements of the constructed algebra will usually belong to the cartesian square of the groupoid, and the constructed operation will be determined by a formula

$$\langle x_0, y_0\rangle * \langle x_1, y_1\rangle = \langle S, T\rangle,$$

where S, T are suitable terms composed from x_i, y_i, and the groupoid operation symbol.

The presented constructions usually require neither finiteness of the base sets nor existence of distinguished idempotent elements. Nevertheless, these conditions are obviously very important for GPT and cellular automata, and hence they will be fulfilled in all presented examples. The constructions are very simple from the algebraic point of view but nevertheless they can substantially increase the complexity of the corresponding GPT (and also corresponding computations of 1D CA). For example, we can obtain an algebra with GPT containing all words from $\mathbf{A}^+$ in its rows from a semilinear algebra $\mathcal{A} = \langle \mathbf{A}; *, \mathrm{o}\rangle$ of degree 1. (We say that $\mathcal{A} = \langle \mathbf{A}; *, \mathrm{o}\rangle$ is a semilinear algebra of degree 1 if the set of rows of every of its GPT is a regular language.) Such an example is presented in Section 3.

Notice also that similar problems were considered also in [Bo96]; of course, the short abstract could not contain all results which T. Boykett presented in his talk.

2 Monoids of binary operations and reversibility among binary operations

Definition 2.1 *The set of binary operations on* $\mathbf{A}$ *will be denoted by* $\mathrm{Op}_2(\mathbf{A})$. *For every* $f, g \in \mathrm{Op}_2(\mathbf{A})$ *we define*

$$h = f \circ g \iff (\forall x, y \in \mathbf{A})(h(x,y) = f(g(x,y), g(y,x))); \tag{2.1}$$

the operation $\circ$ *will be called binary composition (on* $\mathrm{Op}_2(\mathbf{A})$*). Further, we denote by* $\mathrm{I}_{\mathbf{A}}$ *and* $\mathrm{J}_{\mathbf{A}}$ *the first and the second projection on* $\mathbf{A}$*, respectively, i.e. the operations such that for all* $x, y \in \mathbf{A}$

$$\mathrm{I}_{\mathbf{A}}(x,y) = x, \qquad\qquad \mathrm{J}_{\mathbf{A}}(x,y) = y.$$

Powers of an operation $f \in \mathrm{Op}_2(\mathbf{A})$ *will be defined by*

$$f^0 = \mathrm{I}_{\mathbf{A}} \quad \textit{and} \quad f^{n+1} = f^n \circ f \quad \textit{for all } n \in \mathbb{N}.$$

If there is (unique) g *such that* $g \circ f = f \circ g = \mathrm{I}_{\mathbf{A}}$ *we shall write* $g = f^{-1}$.

Since $\mathbf{A}$ will be usually fixed we shall often omit the subscript $\mathbf{A}$. In most important cases $\mathbf{A}$ will be a finite set of cardinality at least two, but these assumptions will be repeated in all theorems where it is necessary. The following two theorems were proved in [K95].

Theorem 2.2 *For every set* $\mathbf{A}$ *the structure* $\langle \mathrm{Op}_2(\mathbf{A}); \circ, \mathrm{I}_{\mathbf{A}} \rangle$ *is a monoid. Its centre (i. e., the set of elements which commute with every element of* $\mathrm{Op}_2(\mathbf{A})$*) consists of* $\mathrm{I}_{\mathbf{A}}$ *and* $\mathrm{J}_{\mathbf{A}}$.

To every $f \in \mathrm{Op}_2(\mathbf{A})$ a mapping $\overline{f} : \mathbf{A}^2 \to \mathbf{A}^2$ can be naturally assigned by the formula $\overline{f}(\langle x, y \rangle) = \langle f(x,y), f(y,x) \rangle$ for all $x, y \in \mathbf{A}$. The mapping $f \mapsto \overline{f}$ is an injective homomorphism of $\langle \mathrm{Op}_2(\mathbf{A}); \circ, \mathrm{I}_{\mathbf{A}} \rangle$ into the monoid of all mappings of $\mathbf{A}^2$ into $\mathbf{A}^2$. Its range consists of all $F : \mathbf{A}^2 \to \mathbf{A}^2$ which satisfy

$$(\forall x, y, u, v \in \mathbf{A})\Big(F(\langle x, y \rangle) = \langle u, v \rangle \iff F(\langle y, x \rangle) = \langle v, u \rangle\Big).$$

Theorem 2.3 *If* $\mathbf{A}$ *is a finite set and* $f, g \in \mathrm{Op}_2(\mathbf{A})$ *then:*

1. $g \circ f = \mathrm{I}_{\mathbf{A}}$ *if and only if* $f \circ g = \mathrm{I}_{\mathbf{A}}$;
2. $g \circ f = \mathrm{J}_{\mathbf{A}}$ *if and only if* $f \circ g = \mathrm{J}_{\mathbf{A}}$;
3. *if* f^{-1} *exists then it is a term operation in the algebra* $\langle \mathbf{A}; f \rangle$;

4. *if* $f \circ g = \mathrm{J}_{\mathbf{A}}$ *then* g *is a term operation in the algebra* $\langle \mathbf{A}; f \rangle$.

Definition 2.4 *Let* $f \in \mathrm{Op}_2(\mathbf{A})$ *and* $a, b \in \mathbb{Z}$. *For a both-side infinite sequence* $\mathbf{x} = (\,\ldots, x_{-1}, x_0, x_1, \,\ldots\,) \in \mathbf{A}^{\mathbb{Z}}$ *we denote by* $\mathrm{Next}_{a,b}(f, \mathbf{x})$ *the both-side infinite sequence* $\mathbf{y} = (\,\ldots, y_{-1}, y_0, y_1, \,\ldots\,) \in \mathbf{A}^{\mathbb{Z}}$ *such that*

$$y_i = f(x_{i+a}, x_{i+b}) \quad \text{for all } i \in \mathbb{Z}. \tag{2.2}$$

A usual interpretation of the above definition is that $\mathbf{x}$, $\mathbf{y}$ are two consecutive configurations of a one-sided 1D CA or two consecutive rows of a GPT.

Definition 2.5 *Let* $f, g \in \mathrm{Op}_2(\mathbf{A})$ *and* $a, b \in \mathbb{Z}$.

1. *We say that* g *is an* (a, b)*-reverse of* f *if for all* $\mathbf{x} \in \mathbf{A}^{\mathbb{Z}}$

$$\mathrm{Next}_{a,b}(g,\ \mathrm{Next}_{0,1}(f, \mathbf{x})) = \mathbf{x}. \tag{2.3}$$

2. *We say that* f *is* (a, b)*-reversible if there is an* (a, b)*-reverse of* f.
3. *We say that* f *is reversible if* f *is* (a, b)*-reversible for some* $a, b \in \mathbb{Z}$.
4. *We shall write L-reverse, C-reverse, R-reverse instead of* $(0, 1)$*-reverse,* $(-1, 0)$*-reverse,* $(-2, -1)$*-reverse, respectively. Analogously for the word "reversible".*

The letters L, C, R abbreviate the words left, central, right, respectively. (Notice that [Bo96] deals with C-reversibility.) To explain the ideas of definitions, let us consider two consecutive rows $\mathbf{x}$, $\mathbf{y}$ of a GPT (completed to both-sides sequences by the quiescent element, i.e. the constant o of $\mathcal{A}$). They can be displayed as follows (the role of the head row will be clear later).

$$\begin{array}{ccccccccccccc}
 & & & & \mathrm{L} & & \mathrm{C} & & \mathrm{R} & & & & \\
\ldots & & x_{i-1} & & x_i & & x_{i+1} & & x_{i+2} & & x_{i+3} & & \ldots \\
 & \ldots & & y_{i-1} & & y_i & & y_{i+1} & & y_{i+2} & & \ldots &
\end{array}$$

If f is the binary operation of the corresponding algebra then $y_i = f(x_i, x_{i+1})$ for all i, and hence $\mathbf{y} = \mathrm{Next}_{0,1}(f, \mathbf{x})$. A reverse g of f computes locally $\mathbf{x}$ from $\mathbf{y}$, but it is not clear which y_j are necessary to obtain x_i; they are specified by the pair (a, b). More concretely, three consecutive elements x_i, x_{i+1}, x_{i+2} of the row $\mathbf{x}$ suffice to determine two elements y_i, y_{i+1} of the row $\mathbf{y}$. The elements y_i, y_{i+1} can be backwise used to determine an element of the row $\mathbf{x}$. Unless some trivial situations they can determine only one of the elements x_i, x_{i+1}, x_{i+2}, which leads to the three kinds of reversibility introduced above.

The notions from the above definition will be used also for groupoids and algebras of signature $(2,0)$ in the obvious way: they will concern the binary operations of the algebras. (The base sets and the constants will be preserved.) They enable us also to define reversibility of GPT (and some 1D CA) in its usual sense as follows.

Definition 2.6 *A GPT G will be called reversible if there is a reversible algebra $\mathcal{A}$ and a word w such that $G = \mathrm{GPT}(\mathcal{A}, w)$. Analogously for (a,b)-reversibility, and also for L-, C- and R-reversibility.*

Theorem 2.7 *Let $f, g \in \mathrm{Op}_2(\mathbf{A})$. Then:*

1. *If f is reversible then f is (a,b)-reversible for some pair*
$$(a,b) \in \{(0,1), (-1,0), (-2,-1)\}. \tag{2.4}$$
(In other words, f is L-, C-, or R-reversible.)
2. *g is an L-reverse of f if and only if for all $x, y, z \in \mathbf{A}$*
$$g(f(x,y), f(y,z)) = x. \tag{2.5}$$
3. *g is a C-reverse of f if and only if for all $x, y, z \in \mathbf{A}$*
$$g(f(x,y), f(y,z)) = y. \tag{2.6}$$
4. *g is an R-reverse of f if and only if for all $x, y, z \in \mathbf{A}$*
$$g(f(x,y), f(y,z)) = z. \tag{2.7}$$

Proof. To prove the first part, let us assume that f is (a,b)-reversible; let g be the function from (2.3). The condition (2.3) can be rewritten as
$$g(f(x_{i+a}, x_{i+a+1}), f(x_{i+b}, x_{i+b+1})) = x_i. \tag{2.8}$$
Since (2.3) holds for all $\mathbf{x} \in \mathbf{A}^{\mathbb{Z}}$ we may consider the latest formula as an identity with variables $x_{i+a}, \ldots, x_i$. (Then i could be fixed, e.g. replaced by zero.) The subscripts ought to be evaluated, hence e.g. if $a = 0$, $b = 1$ then the variables x_{i+a+1}, x_{i+b} are identical. We may assume $a \le b$; otherwise we can exchange a, b, and replace g by $g \circ \mathrm{J}$.

If $\{a,b\} \cap \{-1,0\} = \emptyset$ then x_i does not occur on the left-hand side of (2.8), and hence (2.8) implies the identity $x = y$. Then $\mathrm{card}(\mathbf{A}) = 1$, and there is only one binary operation on $\mathbf{A}$. In this trivial case f is (a,b) reversible for all pairs $(a,b) \in \mathbb{Z}^2$. Hence we may assume $\{a,b\} \cap \{-1,0\} \neq \emptyset$ in what follows.

If $b \geq a+2$ then four distinct variables occur in the left-hand side of (2.8). Three of them are distinct from x_i, hence they can be replaced by any other variables. By suitable substitution we obtain a necessary identity for L-, C- or R-reversibility. (For example, if $b = 0$ we have to replace x_{i+a}, x_{i+a+1} by x_{i-1}, x_i, respectively.) So we may assume $b \leq a + 1$ in what follows.

Now there are only five remaining cases, three from (2.4) and two with $a = b$. The last two must be transformed.

If $a = b = -1$ we may replace the operation g by the operation $g_1(x, y) = g(x, x)$. Then we have

$$g_1(f(x_{i-1}, x_i), f(x_i, x_{i+1})) = g(f(x_{i-1}, x_i), f(x_{i-1}, x_i)) = x_i;$$

hence f is C-reversible. For $a = b = 0$ we can similarly use the function $g_2(x, y) = g(y, y)$, and the proof of of the first part is completed.

The identities (2.5)–(2.7) almost immediately correspond to the definition of L-, C-, and R-reverse. □

Generally speaking, (a, b)-reverse of a function is not uniquely determined. We can see it from examples with an infinite set $\mathbf{A}$; such examples are constructed in [K95]. The situation is quite similar to that with (left) inverses of mappings of $\mathbf{A}$ into $\mathbf{A}$, and also examples can be constructed similarly. However, notice that we have not introduced all analogons of the terms "left inverse", "right inverse", "inverse". If we would do that then we have to add the adjective "left" to our three above notions (and so obtain e.g. "left R-reverse"), and define six new notions, three with the adjective "right", and three "both-side" ones. It seems unnecessary for finite sets $\mathbf{A}$, as the following theorem shows.

We shall say that $f \in \mathrm{Op}_2(\mathbf{A})$ *substantially depends* on both its arguments if there are $x, y, z, u, v, w \in \mathbf{A}$ such that $f(x, z) \neq f(y, z)$ and $f(u, v) \neq f(u, w)$.

Theorem 2.8 *Let* $\mathbf{A}$ *be a finite set and* $f, g \in \mathrm{Op}_2(\mathbf{A})$. *Then:*

1. *If* g *is a C-reverse of* f *then* $g = f^{-1} \circ \mathrm{J}_{\mathbf{A}}$.
2. *If* g *is a L-reverse or an R-reverse of* f *then* $g = f^{-1}$.
3. *For every* $(a, b) \in \mathbb{Z}^2$, $a \neq b$ *there is at most one* (a, b)*-reverse of* f.
4. *If* f *substantially depends on both its arguments then there is at most one pair* $(a, b) \in \mathbb{Z}$ *such that* $a \leq b$ *and* f *is* (a, b)*-reversible.*

Remark. Instead of $\circ$ we could also define the operation $\bullet$ on $\mathrm{Op}_2(\mathbf{A})$ by the formula

$$[f \bullet g](x, y) = f(g(y, x), g(x, y)).$$

Notice that $f \bullet g = f \circ \mathrm{J} \circ g$. We can obtain similar theorems for $\bullet$ instead of $\circ$, only the roles of I, J will be interchanged. This statement can be considered as a duality principle.

3 Permutations of values and arguments

For arbitrary (i.e., possibly infinite) set $\mathbf{A}$ we shall use the term *permutation* of $\mathbf{A}$ for a bijective mapping of $\mathbf{A}$ onto $\mathbf{A}$.

Definition 3.1 *Let $f, g \in \mathrm{Op}_2(\mathbf{A})$ and let p be a permutation of the set $\mathbf{A}$.*

1. *We shall say that g arises from f, p by permutation of values if*

$$g(x,y) = p(f(x,y)) \qquad \text{for all } x, y \in \mathbf{A}. \tag{3.1}$$

2. *We shall say that g arises from f, p by permutation of arguments if*

$$g(x,y) = f(p(x), p(y)) \qquad \text{for all } x, y \in \mathbf{A}. \tag{3.2}$$

Remark 3.2 If we denote $\overline{p}(x,y) = p(x)$ then (3.1), (3.2) can be rewritten as $g = \overline{p} \circ f$ and $g = f \circ \overline{p}$, respectively.

Permutation of values and permutation of arguments preserve reversibility in the following sense:

Theorem 3.3 *Let $f, g \in \mathrm{Op}_2(\mathbf{A})$ let p be a permutation of the set $\mathbf{A}$ and let $X \in \{L, C, R\}$. Further, let g arise from f, p either by permutation of values or by permutation of arguments. Then g is X-reversible if and only if f is X-reversible.*

Proof. Let q be the permutation inverse to p. Let, for example, f be C-reversible and let f_1 be its C-reverse. Then we have $f_1 \circ f = \mathrm{J}_{\mathbf{A}}$. We shall use Remark 3.2. If g arises from f, p by permutation of arguments then we have $g = \overline{p} \circ f$. For $g_1 = f_1 \circ \overline{q}$ we have

$$g_1 \circ g = (f_1 \circ \overline{q}) \circ (\overline{p} \circ f) = f_1 \circ (\overline{q} \circ \overline{p}) \circ f_1 = f_1 \circ \mathrm{I}_{\mathbf{A}} \circ f = f_1 \circ f = \mathrm{J}_{\mathbf{A}}.$$

If g arises from f, p by permutation of values then we have $g = f \circ \overline{p}$. For $g_1 = \overline{q} \circ f_1$ we have

$$g_1 \circ g = (\overline{q} \circ f_1) \circ (f \circ \overline{p}) = \overline{q} \circ (f_1 \circ f) \circ \overline{p} = \overline{q} \circ \mathrm{J}_{\mathbf{A}} \circ \overline{p} = \overline{q} \circ \overline{p} \circ \mathrm{J}_{\mathbf{A}} = \mathrm{J}_{\mathbf{A}}.$$

(We used that $\mathrm{J}_{\mathbf{A}}$ commutes with every element.) The proofs for $X = L$ and $X = R$ are similar (even a little simpler because $\mathrm{J}_{\mathbf{A}}$ does not occur in them).
$\square$

We have seen that permutation of values in an operation corresponds to permutation of arguments in its reverse. Both operations are very simple. Nevertheless, we can give examples that they can substantially change the structure of the corresponding GPT.

Example 3.4 In the upper part of Figure 1 we can see an L-reversible algebra; it is a special case of J. Kari's example from [Ka92]. Its GPT looks trivially: Every of them is empty (i. e., contains the quiescent states only) but the right margin of a fixed width. However, after a permutation of values (which interchanges 1, 2) we can obtain GPT with "fractal" structure. We can see one of them in the bottom part of the figure.

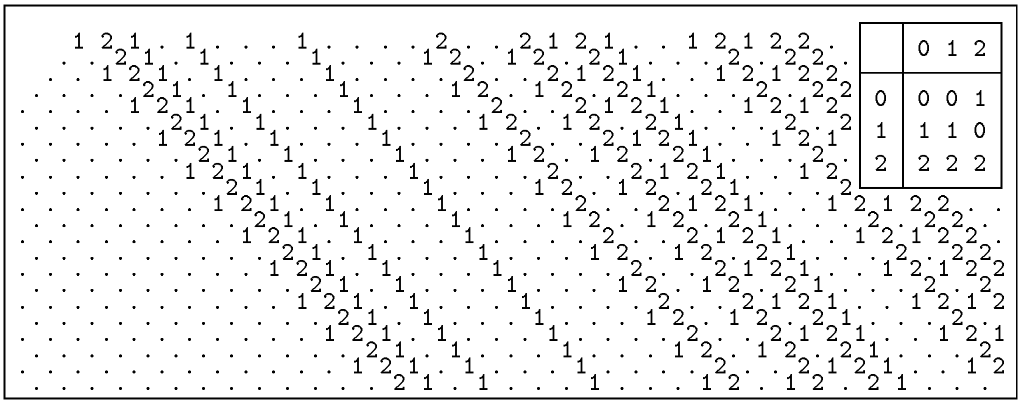
Example 3.5 Let us consider the algebras $\mathcal{A}_1 = \langle\{0,1,2\}; \mathrm{I}_{\{0,1,2\}}, 0\rangle$ and $\mathcal{A}_2 = \langle\{0,3\}; \mathrm{J}_{\{0,3\}}, 0\rangle$. Then elements 1, 2 in any GPT of $\mathcal{A}_1$ represents particles which run to the right with maximal possible speed. Analogously 3's in any GPT of $\mathcal{A}_2$ run to the left with maximal speed. Let us form the direct product $\mathcal{A}$ of $\mathcal{A}_1$ and $\mathcal{A}_2$ (instead of forming ordered pairs (x, y) we can simply use sums $x + y$). Since $\mathcal{A}_1$ and $\mathcal{A}_2$ are C-reversible the algebra $\mathcal{A}$ is C-reversible, too. In any GPT of $\mathcal{A}$ there are (at most) three kinds of particles which run with maximal speeds, either to the right (the elements 1, 2), or to the left (the element 3). By their crossing elements 4 and 5 arise; there are only finitely many such crossings. Hence all GPT of $\mathcal{A}$ have very simple structure. Every of them is empty (i. e., full of 0's) up to margins of a fixed width. However, if we apply permutation of values (with a suitable permutation) to $\mathcal{A}$ we can obtain the algebra which we denote $M(2,6)$. As we can see from the bottom part of Figure 2, its GPT can be nontrivial. An exact sense of this non-triviality is formulated in the following theorem.

Theorem 3.6 *Let* $M(2,6) = \langle\{0,1,2,3,4,5\}; *, 0\rangle$ *where the operation* $*$ *is defined by*

$$x * y = (2x)\ \mathrm{MOD}\ 6 + (2y)\ \mathrm{DIV}\ 6 \qquad \text{for all } x, y \in \{0,1,2,3,4,5\}$$

and let $w \in \{0,1,2,3,4,5\}^+ \setminus 0^+$*. Then for every word* $u \in \{0,1,2,3,4,5\}^+$ *there is a row of GPT* Aw *which contains* u *(as a contigous block).*

Proof. Every GPT G of $M(2,6)$ has the following property: If we read its rows as numbers in the system with base 6 then forming of the next row corresponds to multiplying by 2. If its initial row w corresponds to the integer z then the nth row corresponds to $2^n \cdot z$. This property can be easily derived from the definition of $*$. By the assumption $w \notin 0^+$ we have $z > 0$;



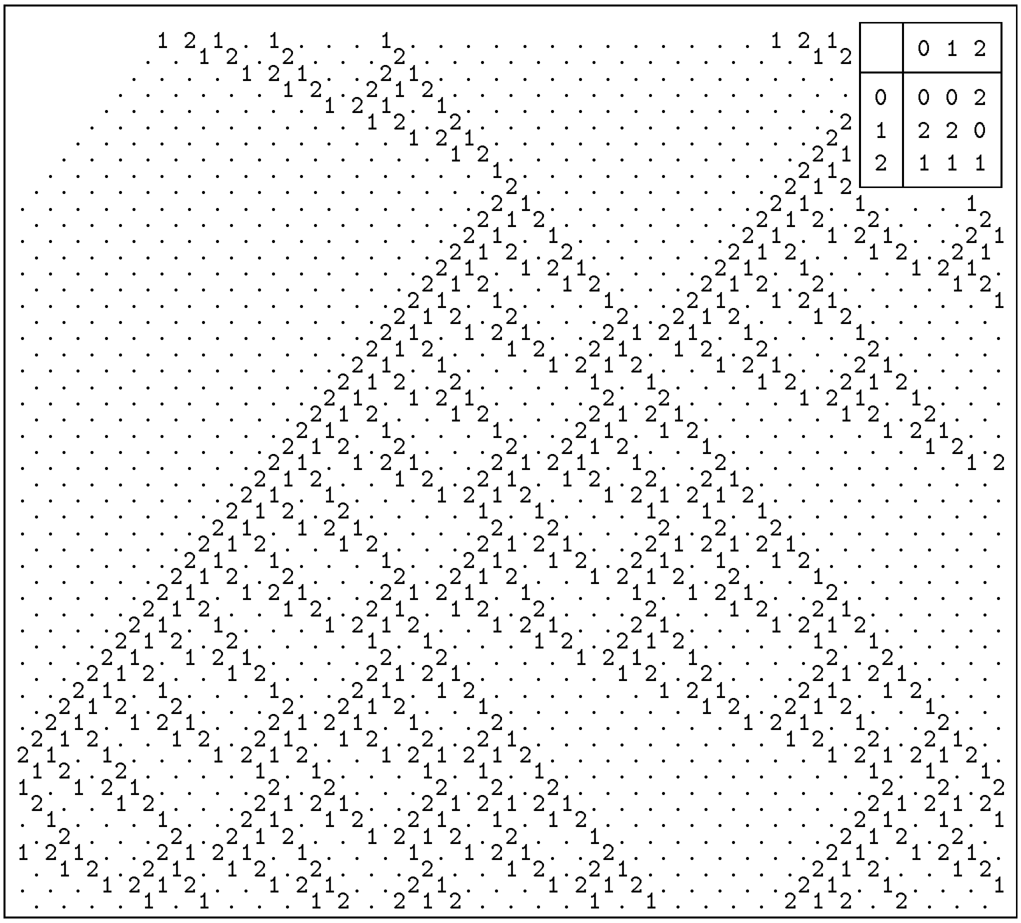


Figure 1.

hence $\log_6 z$ is defined. Since $\log_6 2$ is irrational by [KN74] the sequence of reals $(\log_6 z + n \cdot \log_6 2;\ n = 0, 1, 2, \ldots)$ is uniformly distributed modulo 1. (It suffices for our purposes that the sequence of fractional parts is dense in the interval $(0, 1)$.) Therefore the numbers $2^n \cdot z$ written in base 6 system have arbitrary initial digits (we add leading zeros if necessary). Hence every word $u \in \{0, 1, 2, 3, 4, 5\}^+$ occurs in a row of any such GPT. □

The latest example can be generalized for any two multiplicatively independent integers $p, q \geq 2$. Then GPT of the algebra $\mathcal{A}$ will contain $p - 1$ particles running to the left and $q - 1$ particles running to the right. By a suitable permutation of values we could obtain the algebra $M(p, pq)$ which corresponds to multiplication by p in the pq-ary system.

4 Application of cancellation laws

We shall deal preferably with the right cancellation law, i. e. with the property $\forall \ldots (xz = yz \Rightarrow x = y)$. Of course, similar theorems can be obtained for left cancellation law. The constructions given below can be combined with those of the previous section; in this way more interesting examples can be obtained.

Theorem 4.1 *Let $\langle B, .\rangle$ be a groupoid with right cancellation law, let j, k, $i_1, \ldots, i_s \in \{0, 1\}$ and let the operation $*$ on $\mathbf{A} = B \times B$ be defined by*

$$\langle x_0, y_0\rangle * \langle x_1, y_1\rangle = \langle x_j, y_k.x_{i_1}.\cdots.x_{i_s}\rangle \quad \textit{for all } x_0, y_0, x_1, y_1 \in B;$$

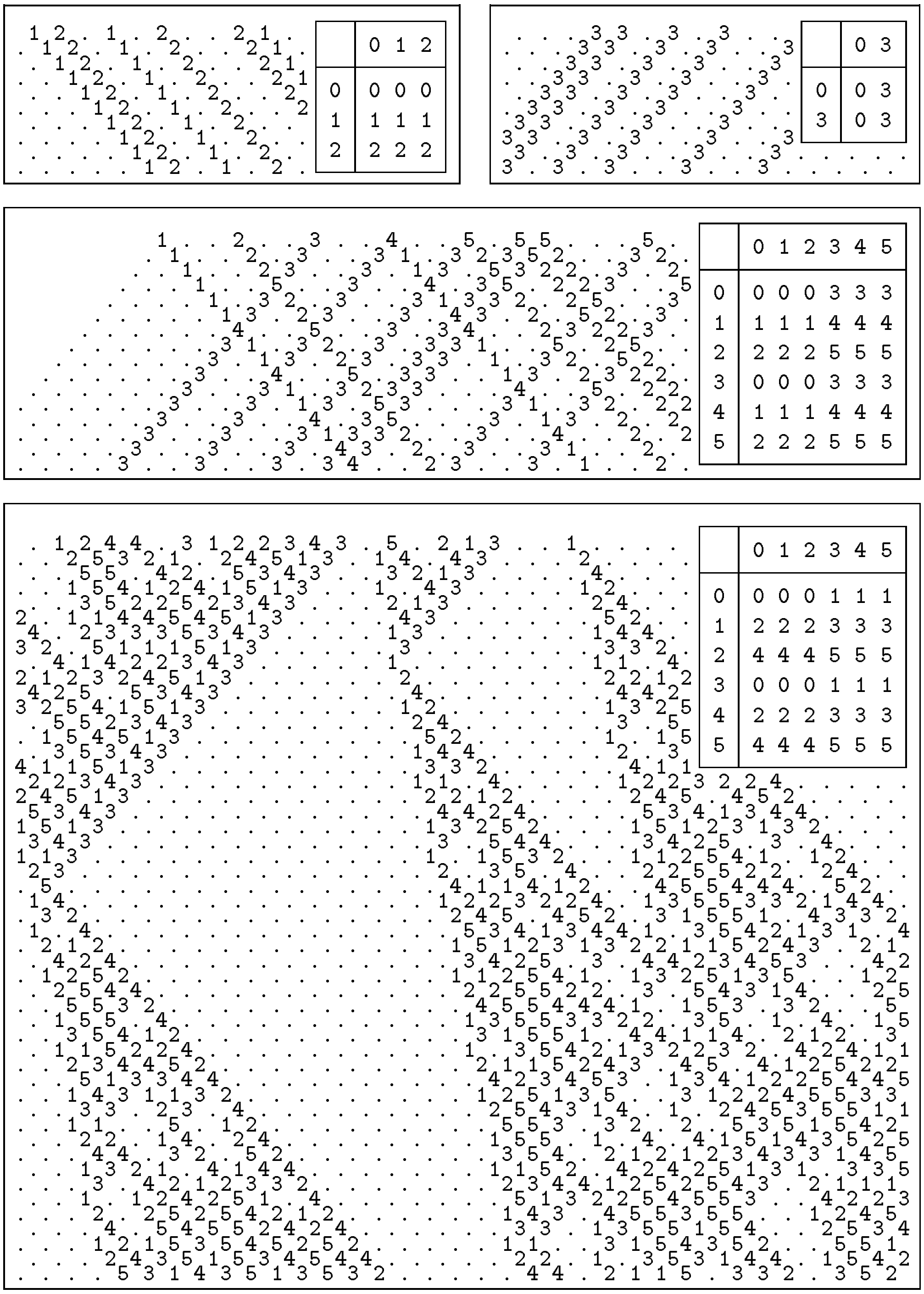
parentheses in the term $y_k.x_{i_1}.\cdots.x_{i_s}$ can be displaced in any (admissible) fixed way. Then the operation $*$ is L-reversible, C-reversible or R-reversible provided that $j + k = 0$, $j + k = 1$ or $j + k = 2$, respectively.

Proof. Let us consider arbitrary $\langle x_0, y_0\rangle, \langle x_1, y_1\rangle, \langle x_2, y_2\rangle \in \mathbf{A}$, and let us form

$$\langle u_0, v_0\rangle = \langle x_0, y_0\rangle * \langle x_1, y_1\rangle, \qquad \langle u_1, v_1\rangle = \langle x_1, y_1\rangle * \langle x_2, y_2\rangle.$$

We have to reconstruct one of $\langle x_i, y_i\rangle$, $0 \leq i \leq 2$ from $\langle u_0, v_0\rangle$, $\langle u_1, v_1\rangle$. Since $u_i = x_{j+i}$ we can immediately reconstruct x_0, x_1 if $j = 0$ or x_1, x_2 if $j = 1$. Let us continue with v_j. We already know all factors of $y_{k+j}.x_{i_1+j}.\cdots.x_{i_s+j}$ except y_{k+j}, and we know the whole "product" v_j. By repeated use of right cancellation law we can determine y_{j+k} (some details below; remember that the operation '.' need not be associative). We already know x_{j+k}, and hence the whole pair $\langle x_{j+k}, y_{j+k}\rangle$. The described reconstruction determines a binary operation $\oplus$ on $\mathbf{A}$, and we have

$$\forall \ldots \Big((\langle x_0, y_0\rangle * \langle x_1, y_1\rangle) \oplus (\langle x_1, y_1\rangle * \langle x_2, y_2\rangle) = \langle x_{j+k}, y_{j+k}\rangle \Big).$$



	0	1	2
0	0	0	0
1	1	1	1
2	2	2	2

	0	3
0	0	3
3	0	3

	0	1	2	3	4	5
0	0	0	0	3	3	3
1	1	1	1	4	4	4
2	2	2	2	5	5	5
3	0	0	0	3	3	3
4	1	1	1	4	4	4
5	2	2	2	5	5	5

	0	1	2	3	4	5
0	0	0	0	1	1	1
1	2	2	2	3	3	3
2	4	4	4	5	5	5
3	0	0	0	1	1	1
4	2	2	2	3	3	3
5	4	4	4	5	5	5

Figure 2.

The latest formula corresponds to L-, C-, or R-reversibility of $*$ provided that $j+k=0$, $j+k=1$ or $j+k=2$, respectively.

We give some details to the reconstruction of y_{k+j}. Since $*$ satisfies right cancellation law there is an operation $/$ which satisfies the identity $(x*y)/y = x$. If v_j is y_{k+j} we need do nothing. Otherwise v_j has the form $S.T$ and we can write $S = v_j/T$. Now we can recursively continue with S instead of v_j until y_{j+k} alone is obtained. Hence y_{j+k} can be expressed as a term built from the variables u_0, u_1, v_j (i.e. v_0 or v_1, not a composed term!) and functional symbols $*$, $/$. $\Box$

Definition 4.2 *Let $\langle S, T\rangle$ be an ordered pair of terms composed from the variables x_0, y_0, x_1, y_1 and the binary functional symbol '.' (dot). We shall say that $\langle S, T\rangle$ is admissible for reversibility from right cancellation law (or shortly "admissible") if the following condition holds: For every groupoid $\langle B, .\rangle$ with right cancellation law, the operation $*$ on $\mathbf{A} = B \times B$ defined by*

$$\langle x_0, y_0\rangle * \langle x_1, y_1\rangle = \langle S, T\rangle \quad \textit{for all } x_0, y_0, x_1, y_1 \in B$$

is L-reversible, C-reversible or R-reversible.

Theorem 4.3 *The following pairs of terms are admissible for reversibility from right cancellation law:*

(1) $\langle x_j, y_k.x_{i_1}.\cdots.x_{i_s}\rangle$ *and*

(2) $\langle y_j, x_k.y_{i_1}.\cdots.y_{i_s}\rangle$ *for arbitrary $j, k, i_1, \ldots, i_s \in \{0,1\}$ (also $s=0$ allowed) and parentheses displaced arbitrarily;*

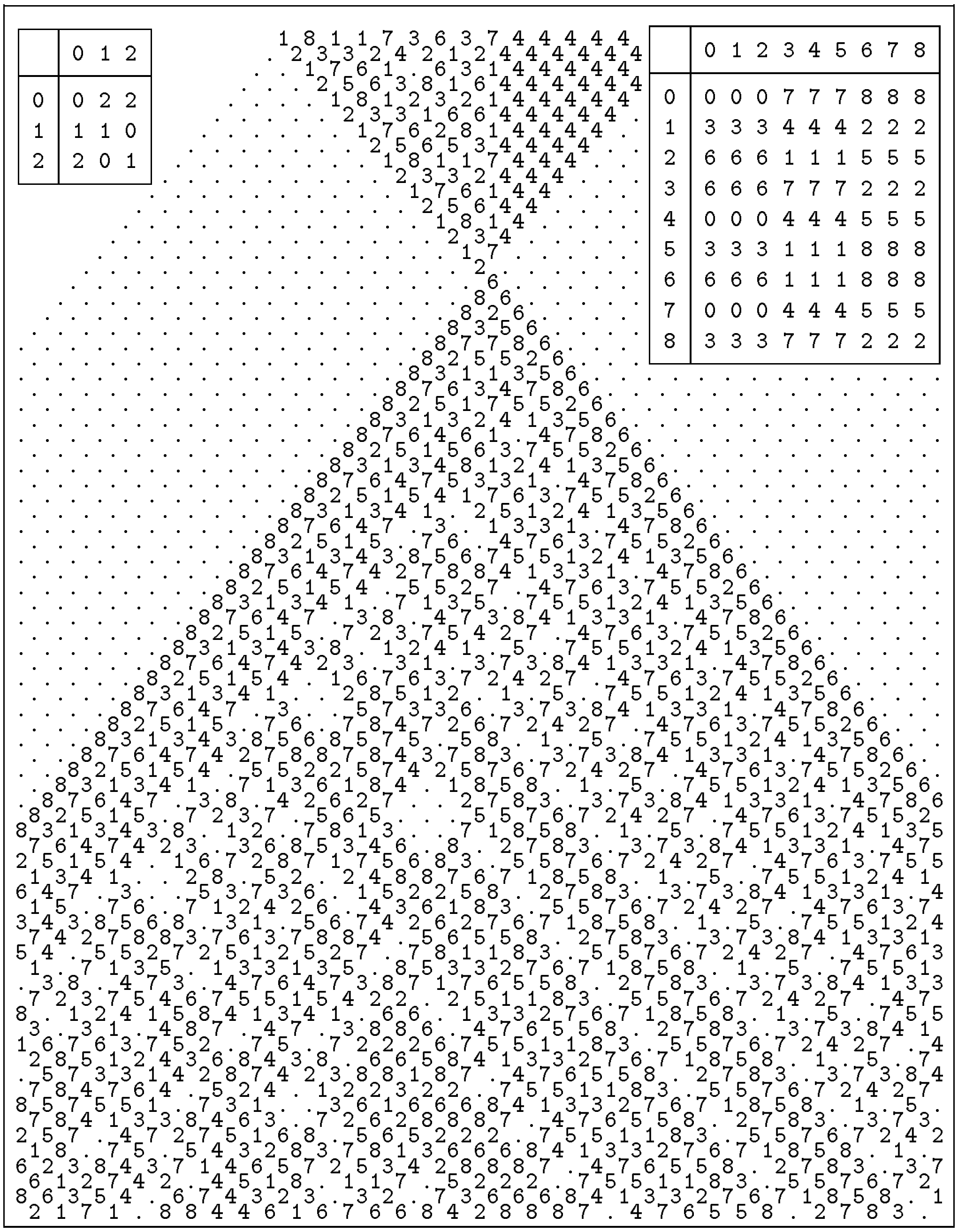
(3) $\langle T, S\rangle$ *provided that $\langle S, T\rangle$ is admissible;*

(4) $\langle S, T.S\rangle$ *provided that $\langle S, T\rangle$ is admissible.*

Proof. We shall use results of the previous section (Theorem 3.3). Notice that (1) correspond to Theorem 4.1 and (2) can be obtained from (1) by permutation of arguments; the corresponding permutation of $B \times B$ interchanges components. The rule (3) corresponds to the permutation of values for the same permutation. Finally, (4) corresponds to the permutation of values induced by the permutation $\langle x, y\rangle \mapsto \langle x, y.x\rangle$ for all $x, y \in B$. $\Box$

Example 4.4 An application of Theorem 4.3 is in Figure 3. The used groupoid is in the left upper corner and the used pair is $\langle y_0.(x_1.x_0), x_1\rangle$. The obtained algebra is C-reversible.

Conjecture 4.5 *All pairs of terms admissible for reversibility from right cancellation law can be obtained by the rules (1)–(4) from Theorem 4.3.*



	0	1	2
0	0	2	2
1	1	1	0
2	2	0	1

	0	1	2	3	4	5	6	7	8
0	0	0	0	7	7	7	8	8	8
1	3	3	3	4	4	4	2	2	2
2	6	6	6	1	1	1	5	5	5
3	6	6	6	7	7	7	2	2	2
4	0	0	0	4	4	4	5	5	5
5	3	3	3	1	1	1	8	8	8
6	6	6	6	1	1	1	8	8	8
7	0	0	0	4	4	4	5	5	5
8	3	3	3	7	7	7	2	2	2

Figure 3.

Another generalization of Theorem 4.1 can be obtained if we replace groupoids by algebras with several binary operations each of which satisfies right cancellation law. Then we could replace dots '.' by symbols of these operations. If only some of the operations satisfy the right cancellation law we have to add special condition to parentheses. We could also find (sufficient) conditions for the case when some of the operations satisfy left cancellation laws. Instead of general statements we give an important special case. Remember that a quasigroup is an algebra $\langle B; *, /, \backslash\rangle$ of signature $(2,2,2)$ which satisfies the identities

$$\begin{array}{rclrclrcl} (x*y)/y &=& x, & y/(x\backslash y) &=& x, & (x/y)*y &=& x, \\ x\backslash(x*y) &=& y, & x*(x\backslash y) &=& y, & (x/y)\backslash x &=& y. \end{array}$$

Theorem 4.6 *Let $\langle B, ., /, \backslash\rangle$ be a quasigroup, let $j, k \in \{0,1\}$ and let the operation $*$ on $\mathbf{A} = B \times B$ be defined by*

$$\langle x_0, y_0\rangle * \langle x_1, y_1\rangle = \langle x_j, T\rangle \textit{ for all } x_0, y_0, x_1, y_1 \in B,$$

where T is a term composed from variables x_0, x_1, y_k and functional symbols $., /, \backslash$. Further, let y_k occur in T exactly once. Then the operation $*$ is L-reversible, C-reversible or R-reversible provided that $j+k=0$, $j+k=1$ or $j+k=2$, respectively.

Proof. We can continue similarly as in Theorem 4.1. Notice that we have both cancellation laws for every of three operations. Hence the positon of y_k in T is not important. □

References

[Bo90] B. A. Bondarenko, *Generalized Pascal triangles and pyramids, their fractals, graphs and applications* (in Russian), "Fan" Tashkent, 1990.

[Bo96] T. Boykett, *Algebraic aspects of one-dimensional cellular automata* In: M. Kutrib, T. Worsch (Eds.): Cellular automata Workshop 1996 Schloss Rauischholzhausen, March 25-27, 1996, Preproceedings, Universität Giessen and Universität Karlsruhe, pp. 10-11.

[Br58] R. H. Bruck, *A survey of binary systems*, Springer Verlag Berlin – Gottingen – Heidelberg, 1958.

[CGS] K. Culik II — J. Gruska — A. Salomaa, *Systolic trellis automata*, International Journal Computer Math. 15 and 16, 1984,1985, pp. 195-212 and 3-22.

[CHY] K. Culik II — L. P. Hurd — S. Yu, *Computation theoretic aspects of cellular automata*, Physica D 45, No. 1-3, 1990, pp. 357-378.

[Ka92] J. Kari, *On the inverse neighborhood of reversible cellular automata*, In G. Rosenberg, A. Salomaa (Eds.): Lindenmayer Systems, Inpact in Theoretical Computer Science, Computer Graphics and Developmental Biology, Springer Verlag Berlin — Heidelberg, 1992, pp. 477-495.

[K85] I. Korec, *Generalized Pascal triangles. Decidability results*, Acta Math. Univ. Comen. 46-47, 1985, pp. 93-130.

[K88] I. Korec, *Generalized Pascal triangles*, In K. Halkowska and S. Stawski, ed.: Proceedings of the V Universal Algebra Symposium, Turawa, Poland, May 1988, World Scientific Singapore, 1989, pp. 198-218.

[K94] I. Korec, *Generalized Pascal triangles, their relation to cellular automata and their elementary theories*, K. Dassow and A. Kelemenová (Eds.): Proceedings of 7th IMYCS Smolenice, November 16-20, 1992, Gordon and Breach Science Publishers Yverdon (Switzerland) 1994 pp 59-70.

[K95] I. Korec, *Reversibility in generalized Pascal triangles and binary reversibility in one-dimensional cellular automata*, Mathematica Slovaca (to appear)

[KN74] L. Kuipers — H. Niederreiter, *Uniform distribution of sequences*, J. Wiley and Sons, New York, 1974.

[Ri72] D. Richardson, *Tesselation with local transformations*, J. Comput. System Sci. 6, 1972, pp. 373-388.

Address of Author:
Mathematical Institute, Slovak Academy of Sciences,
Štefánikova 49,
814 73 Bratislava,
Slovakia

E-mail address: korec@savba.sk

This preprint series was founded in 1996. Its purpose is to present manuscripts of submitted or unpublished papers and reports of fellows of the Mathematical Institute of the Slovak Academy of Sciences in Bratislava and its Košice branch. The authors are fully responsible for the content of the preprints. Postal addresses:

Mathematical Institute
Slovak Academy of Sciences
Štefánikova 49
SK–814 73 Bratislava
SLOVAKIA

Tel./Fax (+421 7) 5249 7316

Mathematical Institute
Slovak Academy of Sciences
Grešákova 6
SK–040 01 Košice
SLOVAKIA

Tel./Fax (+421 95) 6228291

PostScript files of preprints are available at WWW address:
`http://www.mat.savba.sk/preprints`

Latest preprints of the series:

25/1996 *Ivan Korec*: Algebraical constructions of reversible generalized Pascal triangles and one–dimensional cellular automata

24/1996 *Peter Vojtáš*: Uncertain reasoning with floating connectives

23/1996 *Ivan Korec*: Definability of addition from multiplication and neighbourhood relation and some related results

22/1996 *Ivan Korec*: Open problems more or less related to generalized Pascal triangles

21/1996 *Sylvia Pulmannová*: On connections among some orthomodular structures

20/1996 *Pekka Lahti, Sylvia Pulmannová*: Coexistent observables and effects in quantum mechanics

19/1996 *Ivan Korec*: Definability of arithmetical operations from Pascal's triangle modulo n and arithmetical functions

18/1996 *Ivan Korec*: Undecidability and uniform definability in classes of structures related to Pascal's triangles modulo n

17/1996 *Beloslav Riečan*: Probability theory on some ordered structures

16/1996 *Beloslav Riečan*: Weak observables in MV algebras

15/1996 *Anatolij Dvurečenskij, Hee Sik Kim*: On connections between BCK-algebras and difference posets

14/1996 *Anatolij Dvurečenskij, Karl Svozil*: Product of partition logics, orthoalgebras and automata

13/1996 *Robin L. Hudson, Sylvia Pulmannová*: Chaotic expansion of elements of the universal enveloping algebra of a Lie algebra associated with a quantum stochastic calculus

12/1996 *Sylvia Pulmannová*: Congruences in partial abelian semigroups

11/1996 *Karol Nemoga, Štefan Schwarz*: An explicit description of the set of all normal bases generators of a finite field

10/1996 *Ján Jakubík*: Subdirect product decompositions of MV-algebras

9/1996 *Ivan Korec*: Reversibility in generalized Pascal triangles and binary reversibility in one-dimensional cellular automata

8/1996 *Jozef Bobok, Milan Kuchta*: X-minimal patterns and generalization of Sharkovskiĭ's theorem

7/1996 *Jarmila Hedlíková, Sylvia Pulmannová*: Generalized difference posets and orthoalgebras

6/1996 *Ján Borsík, Roman Frič*: Pointwise convergence fails to be strict

5/1996 *Miroslav Ploščica*: Affine completions of distributive lattices

(continued on inside back cover)