Mathematical Institute
Slovak Academy of Sciences, Bratislava

Preprint 9/1996

Ivan Korec

Reversibility in generalized Pascal triangles and binary reversibility in one-dimensional cellular automata

May 21, 1996

PREPRINT SERIES

REVERSIBILITY IN GENERALIZED PASCAL TRIANGLES AND BINARY REVERSIBILITY IN ONE-DIMENSIONAL CELLULAR AUTOMATA

IVAN KOREC

ABSTRACT. Generalized Pascal triangles (GPT) are constructed top-down from finite algebras $\mathcal{A} = \langle \mathbf{A}; *, \circ \rangle$ and words $w \in \mathbf{A}^+$ similarly as the classical Pascal triangle is constructed from $\langle \mathbb{N}; +, 0 \rangle$ and the constant 1. A GPT will be called reversible if it also can be locally constructed bottom-up, using a binary operation. An algebra will be called reversible if all its GPT are reversible. Several kinds of reversibility are introduced and some constructions of reversible algebras are presented. Reversible algebras are constructed from algebras satisfying cancellation laws, or from other reversible algebras. A relationship to reversibility of cellular automata is briefly discussed.

1. INTRODUCTION AND NOTATION

Computations of cellular automata (CA) are constructed in the direction of time: the configuration in time $t+1$ is computed from the configuration in time t. (Definitions for one-dimensional CA are presented in the next section.) It is interesting and important to know whether they can be constructed also in the opposite directions, whether they are *reversible.* This question was studied for a long time, see e.g. [Ri], [Ka]. There are only few methods how to construct reversible CA.

In the present paper the reversibility is studied for generalized Pascal triangles (GPT; defined below) which correspond to computations of one-dimensional CA with 2-element neighbourhood from finite initial configurations. The case of CA with 2-element neighborhood is the simplest non-trivial one, and general neighborhood can be reduced to 2-element ones (in some sense). A special case is studied when the reverse computations also use a binary local transition function; therefore we spoke about binary reversibility in the title. (For one-dimensional CA in general, the number of arguments of reverse transition rule can be greater, and for two- and more-dimensional CA it even cannot be recursively estimated because the reversibility problem is undecidable.) Reversibility of algebras generating GPT is investigated from algebraical point of view, for example identities for direct and reverse local transition functions are presented. However, for GPT the CA terminology is not used; we shall speak about finite algebras of signature $(2,0)$. Several

---

1991 *Mathematics Subject Classification.* Primary 68Q80, Secondary 08A70.
Key words and phrases. Cellular automata, reversibility, cancellation law.
This work was supported by Grant 2/1224/94 of Slovak Academy of Sciences.

algebraical constructions of (in a sense nontrivial) reversible algebras for GPT are given; they can be immediately transformed to constructions of one-dimensional reversible CA. The constructions will usually start with algebras satisfying cancellation laws. Notice that the cancellation laws can be checked very easily from Cayley tables, while reversibility is not so easy to recognize.

2. Generalized Pascal triangles and cellular automata

If $\mathbf{A}$ is an alphabet (i. e., a finite nonempty set) then $\mathbf{A}^+$ will denote the set of all nonempty words in the alphabet $\mathbf{A}$. The length of a word w will be denoted $|w|$. The i-th symbol of w will be denoted by $w(i)$; the starting symbol is $w(0)$ and hence the last symbol is $w(|w|-1)$. $\mathbb{Z}$ will denote the set of integers and $\mathbb{N}$ the set of nonnegative integers. For every $n \in \mathbb{N}$ we denote

$$\mathbb{D}_n = \{(x,y) \in \mathbb{N} \times \mathbb{N} |\ x+y \geq n-1\}.$$

By an algebra we shall always understand a finite algebra, $\mathcal{A} = \langle \mathbf{A}; *, \mathrm{o} \rangle$ of signature $(2,0)$ and satisfying the identity $\mathrm{o} * \mathrm{o} = \mathrm{o}$.

Definition 2.1. *To 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 $G : \mathbb{D}_{|w|} \to \mathbf{A}$ defined by*

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

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 (abbreviation: GPT).

An example of GPT can be found in Figure 1. It arises from the algebra on the left; the role of the algebra on the right will be explained later. It is also clear from this figure what are rows and columns of GPT, and how the coordinate axes x, y are oriented (x right downwards and y left downwards). Any value $G(x,y)$ is written into the unit square with the top vertex (x,y) (and the bottom vertex $(x+1, y+1)$).

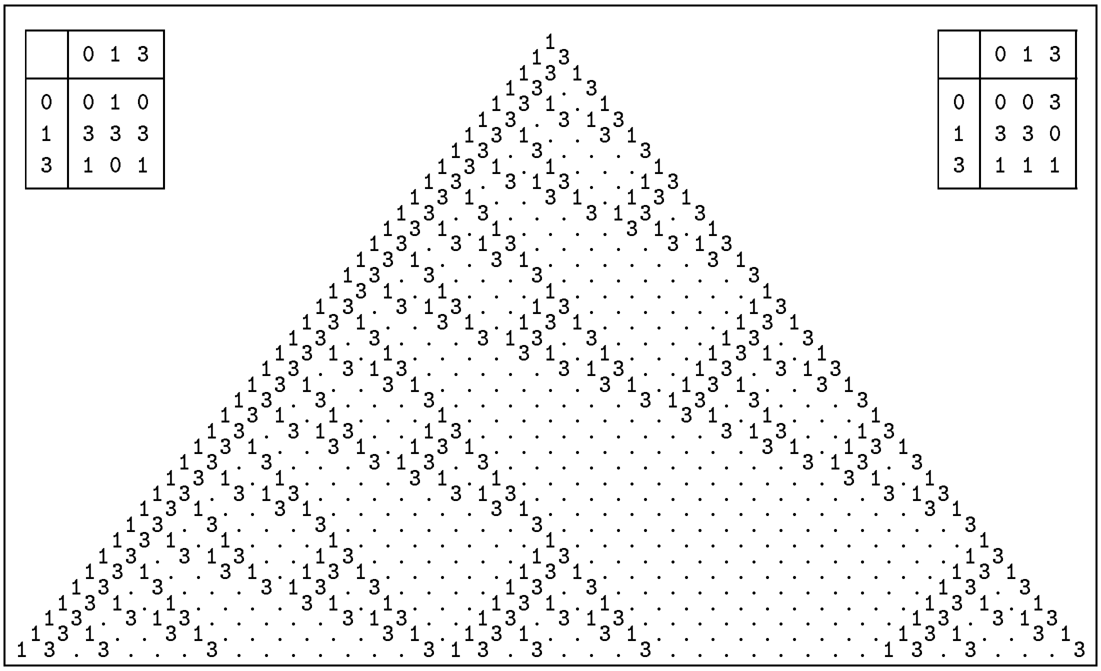
GPT were originally defined in [K1] by study of the structure of real-time systolic trellis automata, see [CGS]. However, GPT also can be used to describe computations of one-dimensional cellular automata (abbreviation:CA) from finite initial configurations. To explain that, we shall briefly repeat the notion of one-dimensional CA at first.

Definition 2.2. *A one-dimensional CA is an ordered quadruple*

$$C = (S, N, f, q), \tag{2.2.1}$$

where S is a finite set of states;

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



	0	1	3
0	0	1	0
1	3	3	3
3	1	0	1

	0	1	3
0	0	0	3
1	3	3	0
3	1	1	1

Figure 1.

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

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

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

$$F(z, t+1) = f(F(z+a_1, t), \dots, F(z+a_n, t)) \tag{2.2.2}$$

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 $z \in \mathbb{Z}$.

By displaying computations of one-dimensional CA we usually use the coordinate system with "space" axis z horizontal and "time" axis t vertical, oriented downwards. (Then we have $z = x - y$ and $t = x + y$, where x, y are coordinates used to display GPT.) For CA with neighbourhood vector $(-1, 1)$ the computations from finite initial configurations look like GPT. (More precisely, every such computation consists of two overlapping GPT which do not influence each other.) However, also for another neighborhood vectors there is a relationship between computations of one-dimensional CA and GPT. To establish it we sometimes must use affine transformations of coordinate systems, and consider ordered $k$tuples of states of CA as elements of algebras generating GPT (k depends on the neighborhood vector). Details can be found e.g. in [K3].

Remark. The idempotent constant o in the considered algebras is not important for reversibility. We leave it here because it is related to the quiescent state of one-dimensional CA. It also is not substantial for reversibility of CA but can be important from other reasons.

3. THE MONOID OF BINARY OPERATIONS

Definition 3.1. *The set of all binary operations on* $\mathbf{A}$ *will be denoted* $\mathrm{Op}_2(\mathbf{A})$.

For every $f, g \in \mathrm{Op}_2(\mathbf{A})$ *we define*

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

this operation $\circ$ *will be called binary composition (on* $\mathrm{Op}_2(\mathbf{A})$*).*

Further, we denote $\mathrm{I}_{\mathbf{A}}$ *and* $\mathrm{J}_{\mathbf{A}}$ *the first and the second projection on* $\mathbf{A}$*, i.e. for all* $x, y \in \mathbf{A}$

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

Powers of an operation $f \in \mathrm{Op}_2(\mathbf{A})$ *will be defined by* $f^0 = \mathrm{I}_{\mathbf{A}}$ *and* $f^{n+1} = f^n \circ f$ *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 delete 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.

Lemma 3.2. *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 commutes with every element of* $\mathrm{Op}_2(\mathbf{A})$*) consists of* $\mathrm{I}_{\mathbf{A}}$ *and* $\mathrm{J}_{\mathbf{A}}$.

Proof. To prove associativity of $\circ$, let us consider arbitrary $f, g, h \in \mathrm{Op}_2(\mathbf{A})$. For all $x, y \in \mathbf{A}$ we have

$$\begin{aligned}[(f \circ g) \circ h](x,y) &= [f \circ g]\big(h(x,y), h(y,x)\big) = \\ &= f\Big(g\big(h(x,y), h(y,x)\big), g\big(h(y,x), h(x,y)\big)\Big) = \\ &= f\big([g \circ h](x,y), [g \circ h](y,x)\big) = [f \circ (g \circ h)](x,y),\end{aligned}$$

and hence $(f \circ g) \circ h = f \circ (g \circ h)$. Similarly we have e.g.

$$[f \circ \mathrm{I}](x,y) = f\big(\mathrm{I}(x,y), \mathrm{I}(y,x)\big) = f(x,y) = \mathrm{I}(f(x,y), f(y,x)) = [\mathrm{I} \circ f](x,y),$$
$$[f \circ \mathrm{J}](x,y) = f\big(\mathrm{J}(x,y), \mathrm{J}(y,x)\big) = f(y,x) = \mathrm{J}\big(f(x,y), f(y,x)\big) = [\mathrm{J} \circ f](x,y),$$

hence I is the unit element and J belong to the center.

Now assume that h belongs to the center of $\mathrm{Op}_2(\mathbf{A})$. For every $f \in \mathrm{Op}_2(\mathbf{A})$ and $x, y \in \mathbf{A}$ we have $[f \circ h](x,y) = [h \circ f](x,y)$, i.e.

$$f(h(x,y), h(y,x)) = h(f(x,y), f(y,x)) \tag{3.2.1}$$

If for some x, y we have $\{h(x,y), h(y,x)\} \neq \{x, y\}$ then we can choose the values of f on the (two or three) ordered pairs $\langle h(x,y), h(y,x)\rangle$, $\langle x, y\rangle$, $\langle y, x\rangle$ so that (3.2.1) will not hold. Therefore we have $\{h(x,y), h(y,x)\} = \{x, y\}$ for all $x, y \in \mathbf{A}$ (we also can express that by the formula $h \circ h = \mathrm{I}$). In particular, $h(x,x) = x$ for all $x \in \mathbf{A}$.

If $h \neq \mathrm{I}$ and $h \neq \mathrm{J}$ then there are $u, v, w, z \in \mathbf{A}$ such that

$$h(u,v) = u \neq v = h(v,u) \quad \text{and} \quad h(w,z) = z \neq w = h(z,w).$$

By (3.2.1) we have $f(u,v) = h(f(u,v), f(v,u))$ for all f; we may choose $f(u,v) = w$, $f(v,u) = z$, and we obtain $w = h(w,z)$, what is a contradiction. $\square$

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 $\big\langle\, \mathrm{Op}_2(\mathbf{A}); \circ, \mathrm{I}_{\mathbf{A}} \big\rangle$ into the monoid of all mappings of $\mathbf{A}^2$ into $\mathbf{A}^2$. The range of the homomorphism consists of all $F : \mathbf{A}^2 \to \mathbf{A}^2$ which satisfy $F(\langle x,y\rangle) = \langle u,v\rangle \iff F(\langle y,x\rangle) = \langle v,u\rangle$ for all $x,y,u,v \in \mathbf{A}$.

Lemma 3.3. *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* $\big\langle \mathbf{A}; f \big\rangle$*;*
(4) *if* $f \circ g = \mathrm{J}_{\mathbf{A}}$ *then* g *is a term operation in the algebra* $\big\langle \mathbf{A}; f \big\rangle$.

Proof. We can use the homomorphism $f \mapsto \overline{f}$ mentioned above, and properties of mappings of a finite set into itself. For example, if $f \circ g = \mathrm{I}$ then $\overline{f}\overline{g} = 1$ (where 1 denotes the identical mapping on $\mathbf{A}^2$), hence both $\overline{f}$, $\overline{g}$ are bijections and $\overline{g}\overline{f} = 1$; then we have $g \circ f = \mathrm{I}$. For (3) we can use that if f^{-1} exists then $f^n = \mathrm{I}$ for some positive integer n; then $f^{-1} = f^{n-1}$. For (4) we can transform $f \circ g = \mathrm{J}_{\mathbf{A}}$ into $f \circ (g \circ \mathrm{J}) = \mathrm{I}$ which gives $g \circ \mathrm{J} = f^{n-1}$ for some positive n. Then we have $g = f^{n-1} \circ \mathrm{J}$, which immediately gives a term for g.

Remark. We could also define an operation $\bullet$ on $\mathrm{Op}_2(\mathbf{A})$ by the formula

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

Notice that $f \bullet g = f \circ \mathrm{J} \circ g$. We can obtain similar statements for $\bullet$ instead of $\circ$, only the roles of I, J will be interchanged. This statement can be considered as a duality principle; we shall neither develop nor use it.

4. REVERSIBILITY AND RELATED IDENTITIES

Definition 4.1. *Let* $f, g \in \mathrm{Op}_2(\mathbf{A})$ *and* $a, b \in \mathbb{Z}$.

(1) *For a both-side infinite sequence* $\mathrm{x} = (\dots x_{-1}, x_0, x_1, \dots) \in \mathbf{A}^{\mathbb{Z}}$ *we denote by* $\mathrm{Next}_{a,b}(f, \mathrm{x})$ *the both-side infinite sequence* $\mathrm{y} = (\dots y_{-1}, y_0, y_1, \dots) \in \mathbf{A}^{\mathbb{Z}}$ *such that* $y_i = f(x_{i+a}, x_{i+b})$ *for all* $i \in \mathbb{Z}$.
(2) *We say that* g *is an* (a,b)*-reverse of* f *if for all* $\mathrm{x} \in \mathbf{A}^{\mathbb{Z}}$

$$\mathrm{Next}_{a,b}\left(g, \mathrm{Next}_{0,1}(f, \mathrm{x})\right) = \mathrm{x}. \tag{4.1.1}$$

(3) *We say that* f *is* (a,b)*-reversible if there is an* (a,b)*-reverse of* f.
(4) *We say that* f *is reversible if* f *is* (a,b)*-reversible for some* $a, b \in \mathbb{Z}$.
(5) *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 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.) The letters L, C, R abbreviate the words left, central, right, respectively.

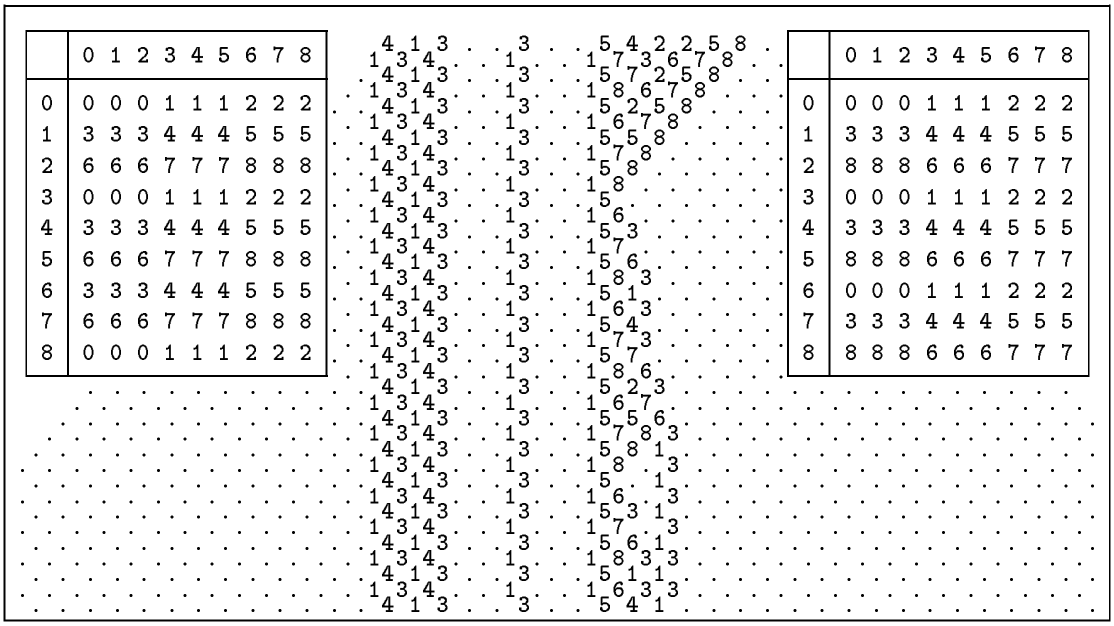
Definition 4.2. *A GPT G will be called reversible if there is a reversible algebra $\mathcal{A}$ and a word w such that $G = \mathrm{GPT}(\mathcal{A}, w)$. Analogously for (a,b)-reversibility, and also for L-, C- and R-reversibility.*

To explain the definitions, let us consider two consecutive rows x, y of a GPT (completed on both sides by the quiescent element, i.e. the constant o of $\mathcal{A}$):

$$\begin{array}{ccccccccccccc} \dots & x_{i-2} & & x_{i-1} & & x_i & & x_{i+1} & & x_{i+2} & & \dots & \\ & \dots & y_{i-2} & & y_{i-1} & & y_i & & y_{i+1} & & y_{i+2} & & \dots \end{array} \tag{4.2.2}$$

If f is the binary operation of the corresponding algebra then $y_i = f(x_i, x_{i+1})$ for all i, and hence $\mathrm{y} = \mathrm{Next}_{0,1}(f, \mathrm{x})$. A reverse g of f computes locally x from y, but it is not clear which y_j are necessary to obtain x_i; they are specified by the pair (a, b).

Examples of L-reversible algebras (and also an L-reversible GPT) can be found in Figure 1; each of two algebras there is L-reverse of the other. Examples of C-reversible algebras (and GPT) can be found in Figure 2.



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

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

Figure 2.

Theorem 4.3. *Let $f, g \in \mathrm{Op}_2(\mathbf{A})$. Then:*

(1) *If f is reversible then f is (a,b)-reversible for some pair*

$$(a,b) \in \{(0,1), (-1,0), (-2,-1)\}. \tag{4.3.1}$$

(In other words, f is L-, C-, or R-reversible.)

(2) *g is an L-reverse of f if and only if for all $x, y, z \in \mathbf{A}$*

$$g(f(x,y), f(y,z)) = x. \tag{4.3.2}$$

(3) *g is a C-reverse of f if and only if for all $x, y, z \in \mathbf{A}$*

$$g(f(x,y), f(y,z)) = y. \tag{4.3.3}$$

(4) *g is an R-reverse of f if and only if for all $x, y, z \in \mathbf{A}$*

$$g(f(x,y), f(y,z)) = z. \tag{4.3.4}$$

Proof. To prove (1), let us assume that f is (a,b)-reversible; let g be the function from (4.1.1). The condition (4.1.1) can be rewritten as

$$g(f(x_{i+a}, x_{i+a+1}), f(x_{i+b}, x_{i+b+1})) = x_i. \tag{4.3.5}$$

Since (4.1.1) holds for all 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 cold 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 $a \leq b$; 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 (4.3.5), and hence (4.3.5) implies the identity $x = y$. Then $\mathrm{card}(\mathbf{A}) \leq 1$, 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 (4.3.5). 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 (4.3.1) 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 (3) is completed.

The identities in (2)–(4) almost immediately correspond to the definition of L-, C-, and R-reverse. $\square$

Generally speaking, (a,b)-reverse of a function is not uniquely determined, as we can see from the following example.

Example 4.4. Let $\mathbf{A} = \mathbb{N}$ and let C, L, R be the pairing functions (i.e., $C(x,y) = \frac{(x+y)(x+y+1)}{2} + x$ and $C(L(x), R(x)) = x$ for all $x, y \in \mathbb{N}$). Then the function C is L-reversible, C-reversible, and also R-reversible. Its L-reverse is $L_1(x,y) = L(x)$ and its R-reverse is $R_1(x,y) = R(y)$. There are infinitely many C-reverses are of C; the simplest ones are $L_2(x,y) = L(y)$ and $R_1(x,y) = R(x)$, one of more complicated is $g(x,y) = C\left(L(R(x)), R(L(y))\right)$. The function $f(x,y) = C(C(x,y), C(x,y))$ has infinitely many X-reverses for all three X $\in \{\mathrm{L}, \mathrm{C}, \mathrm{R}\}$.

If we assume that $\mathbf{A}$ is finite, the situation is simpler, as we can see from the following theorem. Roughly speaking, the situation is similar to that with inverting of mappings of a set into itself. Notice that the notion "X-reverse" corresponds to a one-sided inverse of a mapping. Hence the term "left X-reverse" would be more adequate (then also "right X-reverse" ought to be introduced). However, since we are interested mostly in operations on finite sets this more complicated term seems to be unnecessary in the present paper.

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 4.5. *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* $g = f^{-1} \circ \mathrm{J}$.
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.*

Proof. For (1) and (2) let us substitute $z := x$ into the identities (4.3.2), (4.3.3), (4.3.4); the obtained identities correspond to the equation $g \circ f = \mathrm{J}_{\mathbf{A}}$ in the second case ((1) in the theorem), and to $g \circ f = \mathrm{I}_{\mathbf{A}}$ in the other cases. From these equations g can be (uniquely) computed.

To prove (3), let us denote $f_1(z) = f(z, z)$, $g_1(z) = g(z, z)$ for all $z \in \mathbf{A}$. The identity (4.3.5) implies $g_1(f_1(z)) = z$, hence f_1 g_1 are permutations of $\mathbf{A}$. Notice that g_1 is uniquely determined by f (and also by f_1, of course).

From similar reasons as in the previous theorem we may assume $a < b$. If $0 \notin \{a, a+1, b, b+1\}$ then x_i does not occur in the left-hand side of (4.3.5), and hence $\mathrm{card}(\mathbf{A}) \leq 1$. Then (3) trivially holds because there is exactly one binary operation on $\mathbf{A}$. Let $0 \in \{a, a+1, b, b+1\}$ in what follows.

For $b > a + 1$ let us distinguish four cases:

$$a = -1, \qquad a = 0, \qquad b = -1, \qquad b = 0. \tag{4.5.1}$$

In the first case (4.3.5) implies the identity $g(f(y, x), f(z, z)) = x$. Since f_1 is a permutation of $\mathbf{A}$ we can replace $f(z, z)$ by (any variable, e.g.) z, and we obtain the identity $g(f(y, x), z) = x$. The last identity implies that g depends only on its first argument, and f only on its second argument, i.e.

$$g(u, z) = g_1(u), \qquad f(y, x) = f_1(x)$$

for all $u, z, x, y \in \mathbf{A}$. Since g_1 is uniquely determined by f the operation g is uniquely determined, too. (The statement about f will be used later.) For the remaining three cases in (4.5.1) we can similarly consider the identities

$$g(f(x, y), z) = x, \qquad g(z, f(y, x)) = x, \qquad g(z, f(x, y)) = x.$$

Now only three cases $b = a + 1$, $-2 \leq a \leq 0$ remain. But in these cases explicit formulas for g were given in (1) and (2).

To prove (4) notice that if f is (a, b)-reversible then (4.3.1) holds. (This is not an immediate consequence of Theorem 4.3, (1), but can be proved similarly.) Further, if two of identities (4.3.2)–(4.3.4) hold then we can obtain an identity of the form $x = y$. Then card ≤ 1, and f cannot depend on both arguments, which is a contradiction. □

Theorem 4.6. *Let* $\mathbf{A}$ *be a finite set,* $f, g \in \mathrm{Op}_2(\mathbf{A})$ *and* $X \in \{L, C, R\}$. *Then* f *is an* X*-reverse of* g *if and only if* g *is an* X*-reverse of* f.

Proof. Let us consider X=C, and let us write $*$ instead of f and $\oplus$ instead of g. We have to prove that the identity

$$(x * y) \oplus (y * z) = y \tag{4.6.1}$$

implies the identity

$$(x \oplus y) * (y \oplus z) = y. \tag{4.6.2}$$

Then by the symmetry also the later identity implies the former.

Let us consider the mapping F of $\mathbf{A}^3$ into $\mathbf{A}^3$ defined by

$$F\langle x, y, z\rangle = \langle x * y, y * z, z * x\rangle.$$

The mapping F is bijective; to show that, we prove that F is injective (and use that $\mathbf{A}^3$ is finite). If $F\langle x_1, y_1, z_1\rangle = F\langle x_2, y_2, z_2\rangle$ then by the definition of F we have

$$x_1 * y_1 = x_2 * y_2, \qquad y_1 * z_1 = y_2 * z_2, \qquad z_1 * x_1 = z_2 * x_2.$$

By the first two equalities and (4.6.1) we have

$$y_1 = (x_1 * y_1) \oplus (y_1 * z_1) = (x_2 * y_2) \oplus (y_2 * z_2) = y_2.$$

Similarly we can obtain $x_1 = x_2$ and $z_1 = z_2$. Hence F is injective, and then also bijective. Now let us define

$$G\langle u, v, w\rangle = \langle w \oplus u, u \oplus v, v \oplus w\rangle$$

for all $\langle u, v, w\rangle \in \mathbf{A}^3$. Let us take arbitrary $x, y, z \in \mathbf{A}$. The third and the first component of $F\langle x, y, z\rangle$ are $z * x$ and $x * y$, respectively. Hence the first component of $G(F\langle x, y, z\rangle)$ is equal to $(z * x) \oplus (x * y)$, which is equal to x by the identity (4.6.1). Similarly the second and the third component are y and z. Therefore GF is the identical mapping on $\mathbf{A}^3$. Since F is bijective we have $G = F^{-1}$, and hence

$$F(G\langle x, y, z\rangle) = \langle x, y, z\rangle$$

for all $x, y, z \in \mathbf{A}$. By the definitions of F, G the first component of the left-hand side is $(z \oplus x) * (x \oplus y)$, and hence (4.6.2) holds.

The cases X=L and X=R can be proved similarly. We have to define $G\langle u, v, w\rangle = \langle u \oplus v, \dots\rangle$ and $G\langle u, v, w\rangle = \langle v \oplus w, \dots\rangle$, respectively. □

Remark. We could use any $\mathbf{A}^n$, $n \geq 3$ instead of $\mathbf{A}^3$ in the proof above. However, $\mathbf{A}^2$ would not suffice. On the other hand, considerations with $\mathbf{A}^2$ suffice to construct X-reverse of F provided we know that it exists (compare (1), (2) of Theorem 4.5).

5. REVERSIBLE ALGEBRAS CONSTRUCTED FROM QUASIGROUPS

Remember that a *quasigroup* can be defined as a structure $\langle \mathbf{B}; *, \backslash, / \rangle$ with three binary operations which satisfies the identities

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

The last two identities are superfluous because they follow from the previous ones; we have $x = (y/x)\backslash\big((y/x) * x\big) = (y/x)\backslash y$ and $x = \big(x * (x\backslash y)\big)/(x\backslash y) = y/(x\backslash y)$. However, we shall mainly use these identities.

We shall explain the idea used below. Let us take any GPT of a quasigroup, let us complete it by the element o on both sides, and let us divide it into squares so that every square contains two elements of the GPT. The sides of squares will be horizontal and vertical, and their length will be $\sqrt{2}$ (or, equivalently: the diagonals of the squares will be parallel with the coordinate axes, and their length will be 2). Let us call these squares shortly 2-squares. An illustrating example is in Figure 3, where Pascal triangle modulo 2 is displayed; to obtain a more transparent figure, all o = 0 are replaced by dots.

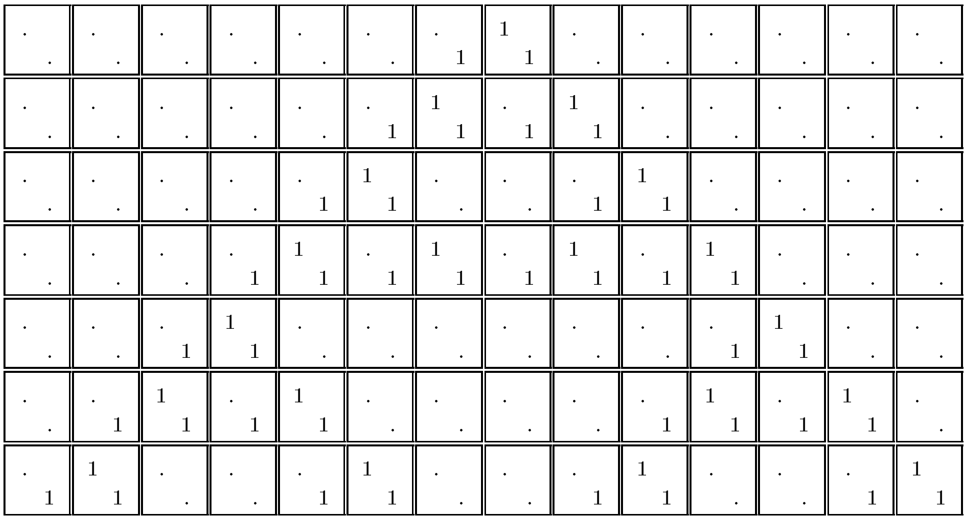


Figure 3.

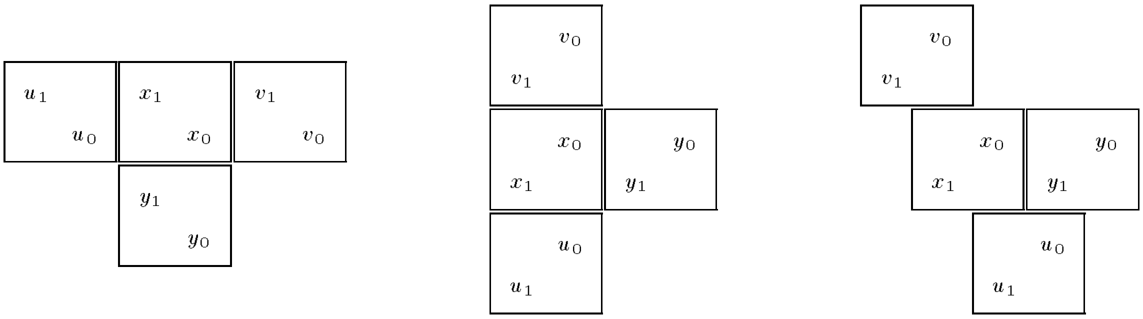


Figure 4.

If we know the (contents of the) 2-squares in one column then we can construct 2-squares of both neighbour columns. More precisely, two consecutive 2-squares of a column uniquely determine both the left and the right neighbour of the upper 2-square. In the left part of Figure 4, $u = \langle u_1, u_0\rangle$ and $v = \langle v_1, v_0\rangle$ are determined by $x = \langle x_1, x_0\rangle$ and $y = \langle y_1, y_0\rangle$. Let us turn the GPT 90° counterclockwise, and let us shift the new rows as it is displayed in the central and the right part of Figure 4. Then every 2-square is (uniquely) determined by the two 2-squares over it (u is determined by x, y); the corresponding rule enables us to form a new GPT from 2-squares. (The figure obtained by turning the original GPT need not be a GPT, and need not contain any new GPT. However, it contains arbirarily large pieces of new GPT.) Since also v is determined by x, y the obtained GPT is L-reversible. This is the idea behind the following lemma.

Lemma 5.1. *Let* $\langle \mathbf{B}; *, \backslash, /\rangle$ *be a quasigroup and let the operations* $\oplus, \otimes$ *on* $\mathbf{A} = \mathbf{B}^2$ *be defined by*

$$\langle x_1, x_0\rangle \oplus \langle y_1, y_0\rangle = \langle (y_1/x_0)/x_1, y_1/x_0\rangle. \tag{5.1.1}$$

$$\langle x_1, x_0\rangle \otimes \langle y_1, y_0\rangle = \langle x_1\backslash x_0, x_0\backslash(y_1\backslash y_0)\rangle, \tag{5.1.2}$$

for all $\langle x_1, x_0\rangle, \langle y_1, y_0\rangle \in \mathbf{A}$. *Then the following identities hold:*

$$(x \oplus y) \otimes (y \oplus z) = x, \tag{5.1.3}$$

$$(x \otimes y) \oplus (y \otimes z) = x. \tag{5.1.4}$$

Proof. Let $x = \langle x_1, x_0\rangle$ and similarly for the other letters. To prove the first identity, let us denote $u = x \oplus y$, $v = y \oplus z$, and $w = u \otimes v$. Then we have

$$\begin{aligned}
\langle u_1, u_0\rangle = \langle (y_1/x_0)/x_1, y_1/x_0\rangle, \qquad & \langle v_1, v_0\rangle = \langle (z_1/y_0)/y_1, z_1/y_0\rangle,\\
w_1 = u_1\backslash u_0 &= ((y_1/x_0)/x_1)\backslash(y_1/x_0) = x_1,\\
w_0 = u_0\backslash(v_1\backslash v_0) &= u_0\backslash((v_0/y_1)\backslash v_0) = u_0\backslash y_1 = (y_1/x_0)\backslash y_1 = x_0,
\end{aligned}$$

and therefore $w = x$. The second identity can be proved similarly. (For $\mathbf{B}$ finite it also directly follows from the first one.) Let $x, y, z \in \mathbf{A}$ and $u = x \otimes y$, $v = y \otimes z$, $w = u \oplus v$. We have

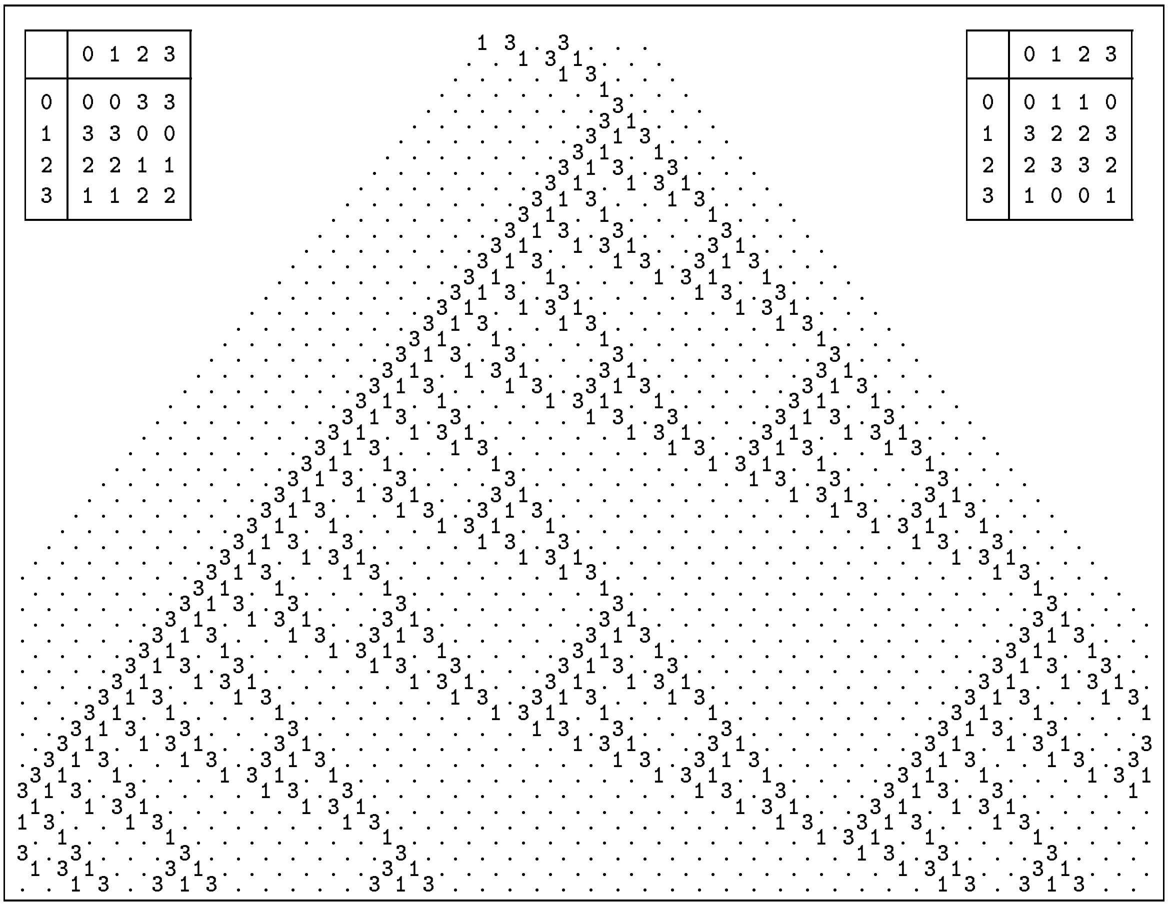
$$\langle u_1, u_0\rangle = \langle x_1\backslash x_0, x_0\backslash(y_1\backslash y_0)\rangle, \qquad \langle v_1, v_0\rangle = \langle y_1\backslash y_0, y_0\backslash(z_1\backslash z_0)\rangle.$$

Since $\langle w_1, w_0\rangle = \langle (v_1/u_0)/u_1, v_1/u_0\rangle$ we have

$$w_0 = v_1/u_0 = (y_1\backslash y_0)/(x_0\backslash(y_1\backslash y_0)) = x_0, \qquad w_1 = w_0/u_1 = x_0/(x_1\backslash x_0) = x_1$$

and therefore again $w = x$. □

An illustrating example to Lemma 5.1 is in Figure 5. The starting algebra is the additive group modulo 2; the pairs $\langle i, j\rangle$ in the constructed algebras are replaced by the digits $2i + j$ (e. g. $\langle 1, 1\rangle$ by 3). The presented GPT corresponds to the algebra on the left; to obtain a nicer figure, zeros is replaced by dots in the GPT.



	0	1	2	3
0	0	0	3	3
1	3	3	0	0
2	2	2	1	1
3	1	1	2	2

	0	1	2	3
0	0	1	1	0
1	3	2	2	3
2	2	3	3	2
3	1	0	0	1

Figure 5.

The L-reverse algebra is displayed on the right. Notice that the same GPT can be obtained also from an (L-reversible) algebra of cardinality 3. (See Figure 1. The L-reverse GPT is displayed there, and therefore the right algebra in Figure 1 corresponds to the left algebra in Figure 5. The former is not a subalgebra of the later. However, this situation would take place if we replace both algebras by partial ones, defined only on places necessary for the presented GPT.)

The operations $\oplus$, $\otimes$ constructed in Lemma 1 are L-reversible. Nicer, C-reversible operations (on a bigger set) can be constructed from them by the following lemma.

Lemma 5.2. *Let the operations* $\oplus, \otimes$ *on* $\mathbf{A}$ *satisfy the identities* (5.1.3), (5.1.4). *Let the operations* $\boxplus, \boxtimes$ *on the set* $\mathbf{C} = \mathbf{A}^2$ *be defined by*

$$\langle x_1, x_0\rangle \boxplus \langle y_1, y_0\rangle = \langle x_0 \oplus y_1, y_1 \oplus y_0\rangle, \tag{5.2.1}$$

$$\langle x_1, x_0\rangle \boxtimes \langle y_1, y_0\rangle = \langle x_0 \otimes y_1, y_1 \otimes y_0\rangle \tag{5.2.2}$$

for all $\langle x_1, x_0\rangle, \langle y_1, y_0\rangle \in \mathbf{C}$. *Then the following identities hold:*

$$(x \boxplus y) \boxtimes (y \boxplus z) = y, \tag{5.2.3}$$

$$(x \boxtimes y) \boxplus (y \boxtimes z) = y. \tag{5.2.4}$$

Proof. By the symmetry, it suffices to prove the first identity. If we denote $x = \langle x_1, x_0 \rangle$, and similarly for other letters, we have for arbitrary $x, y, z \in \mathbf{C}$:

$$\begin{aligned}(x \boxplus y) \boxtimes (y \boxplus z) &= \langle x_0 \oplus y_1, y_1 \oplus y_0 \rangle \boxtimes \langle y_0 \oplus z_1, z_1 \oplus z_0 \rangle = \\ &= \langle (y_1 \oplus y_0) \otimes (y_0 \oplus z_1), (y_0 \oplus z_1) \otimes (z_1 \oplus z_0) \rangle = \langle y_1, y_0 \rangle = y.\end{aligned}$$

(We did not use (5.1.1), (5.1.2). Hence Lemma 5.2 can be applied also for $\oplus$, $\otimes$ which do not arise from a quasigroup by Lemma 5.1.) $\square$

Lemmas 5.1 and 5.2 can be reformulated as follows:

Theorem 5.3. (1) *If $\langle \mathbf{B}; *, \backslash, / \rangle$ is a quasigroup then the operations $\oplus$, $\otimes$ defined by* (5.1.1) *and* (5.1.2) *are L-reversible; each of them is L-reverse of the other.*

(2) *If every of operations $\oplus$, $\otimes$ on a set $\mathbf{A}$ is L-reverse of the other then the operations $\boxplus$, $\boxtimes$ defined by* (5.2.1) *and* (5.2.2) *are C-reversible; each of them is a C-reverse of the other.*

Corollary 5.4. *Let $\langle \mathbf{B}; *, \backslash, / \rangle$ be a quasigroup and let the operations $\boxplus, \boxtimes$ on $\mathbf{A} = \mathbf{B}^4$ be defined by*

$$\langle x_3, x_2, x_1, x_0 \rangle \boxplus \langle y_3, y_2, y_1, y_0 \rangle = \langle (y_3/x_2)/x_3, y_3/x_2, (y_1/x_0)/x_1, y_1/x_0 \rangle. \tag{5.4.1}$$

$$\langle x_3, x_2, x_1, x_0 \rangle \boxtimes \langle y_3, y_2, y_1, y_0 \rangle = \langle x_3 \backslash x_2, x_2 \backslash (y_3 \backslash y_2), x_1 \backslash x_0, x_0 \backslash (y_1 \backslash y_0) \rangle \tag{5.4.2}$$

for all $\langle x_3, x_2, x_1, x_0 \rangle, \langle y_3, y_2, y_1, y_0 \rangle \in \mathbf{A}$. Then the operations $\oplus$, $\otimes$ are C-reversible; each of them is the C-reverse of the other. (I.e., the identities (5.2.3), (5.2.4) *hold.)*

To prove that we can simply apply Lemma 5.2 and Lemma 5.3. The formulas (5.4.1), (5.4.2) can be also written directly from Figure 5; the original GPT is divided into rectangles, each of which consists of two 2-squares, and then it is turned 90° counterclockwise (however, no shift of new rows is necessary).

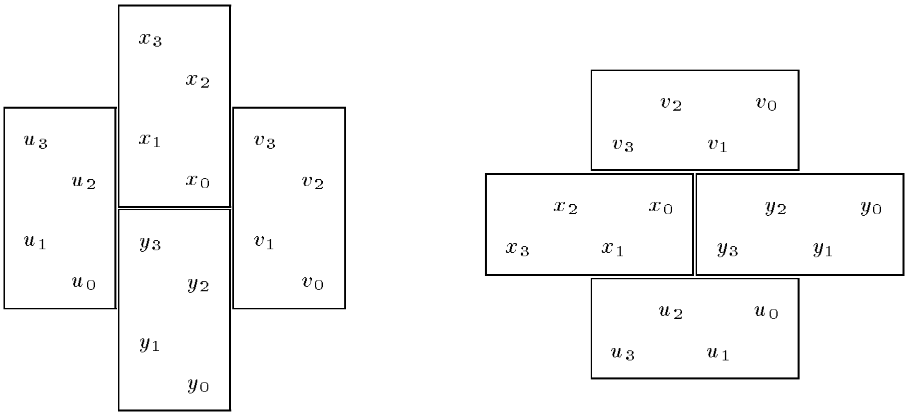


Figure 6.

For the simplest nontrivial application of the corollary we again take the additive group modulo 2. Figure 7 shows an inner part of Pascal's triangle modulo 2, divided into rectangles as explained above, and then rotated 90° counterclockwise. Zeros are again replaced by dots. Figure 8 shows the 16-element algebra obtained by

Corollary 5.4, one of its GPT, the suitable 4-element subalgebra and its C-reverse. Rectangles from Figure 6 are replaced by hexadecimal digits in the obvious way (a rectangle containing $\langle x_3, x_2, x_1, x_0\rangle$ is replaced by $8x_3 + 4x_2 + 2x_1 + x_0$), and dots are displayed instead of zeros. The rectangle in GPT corresponds to Figure 7.

We can generalize the constructions presented above so that we shall not start from GPT, but from more general objects which are constructed similarly as GPT, but instead of one binary operation $*$ two binary operations $*$, $\odot$ are used. The operation $*$ will be used in odd steps, and $\odot$ in even steps. (The parity of a step can be understand as the parity of $x+y$ when $G(x,y)$ is computed; see Definition 2.1.) In the left part of Figure 4 it means that

(1) $*$ is used when the lower elements of 2-squares are computed, and
(2) $\odot$ is used when the upper elements of the 2-squares (in the next row) are computed.

So we can generalize Lemma 5.1 as follows.

Lemma 5.6. *Let* $\langle \mathbf{A}; *, \backslash_o\ , /_o\ \rangle$, $\langle \mathbf{A}; \odot, \backslash_e\ , /_e\ \rangle$ *be two quasigroups (with the same base set) and let the operations* $\oplus$, $\otimes$ *on* $\mathbf{A}^2$ *be defined by*

$$\langle x_1, x_0\rangle \oplus \langle y_1, y_0\rangle = \langle (y_1 /_e x_0) /_o x_1,\ y_1 /_e x_0\rangle. \tag{5.6.1}$$

$$\langle x_1, x_0\rangle \otimes \langle y_1, y_0\rangle = \langle x_1 \backslash_o x_0,\ x_0 \backslash_e (y_1 \backslash_o y_0)\rangle, \tag{5.6.2}$$

for all $\langle x_1, x_0\rangle, \langle y_1, y_0\rangle \in \mathbf{A}^2$. *Then each of* $\oplus$, $\otimes$ *is an L-reverse of the other. (I.e., the identities* (5.1.3), (5.1.4) *hold.)*

The similar generalization of the formulas from Corollary 5.4 is straightforward. Now we show a modification of Lemma 5.1 based on another division of GPT into 2-squares. Now every 2-square will contain the elements of GPT in the lower left corner and in the upper right corner. The rotation and the shift will not be changed. Then we can prove:

Lemma 5.7. *Let* $\langle \mathbf{B}; *, \backslash, /\rangle$ *be a quasigroup and let the operations* $\oplus, \otimes$ *on* $\mathbf{A} = \mathbf{B}^2$ *be defined by*

$$\langle x_1, x_0\rangle \oplus \langle y_1, y_0\rangle = \langle (y_1/y_0)/x_1, x_1/x_0\rangle. \tag{5.7.1}$$

$$\langle x_1, x_0\rangle \otimes \langle y_1, y_0\rangle = \langle x_1\backslash y_0, x_0\backslash(x_1\backslash y_0)\rangle, \tag{5.7.2}$$

for all $\langle x_1, x_0\rangle, \langle y_1, y_0\rangle \in \mathbf{A}$. *Then each of the operations* $\oplus$, $\otimes$ *is L-reverse of the other.*

If we want to obtain similar formulas for R-reversibility we have to join the symmetry with respect to vertical axis. (Equivalently, we can replace the rotation 90° counterclockwise by the symmetry with respect to the axis y; remember that it is oriented left downwards.)

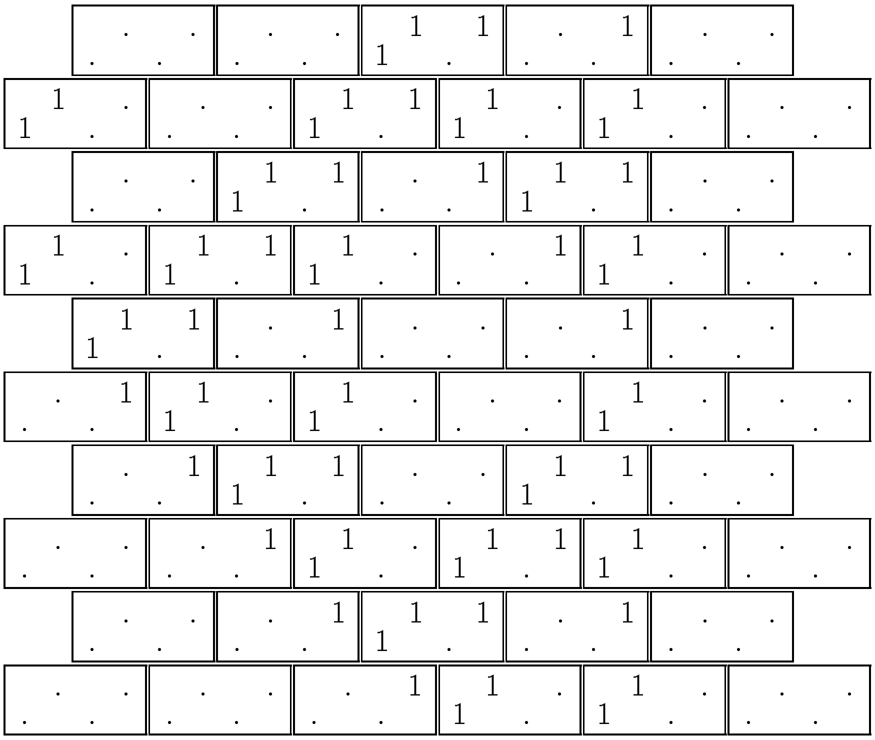
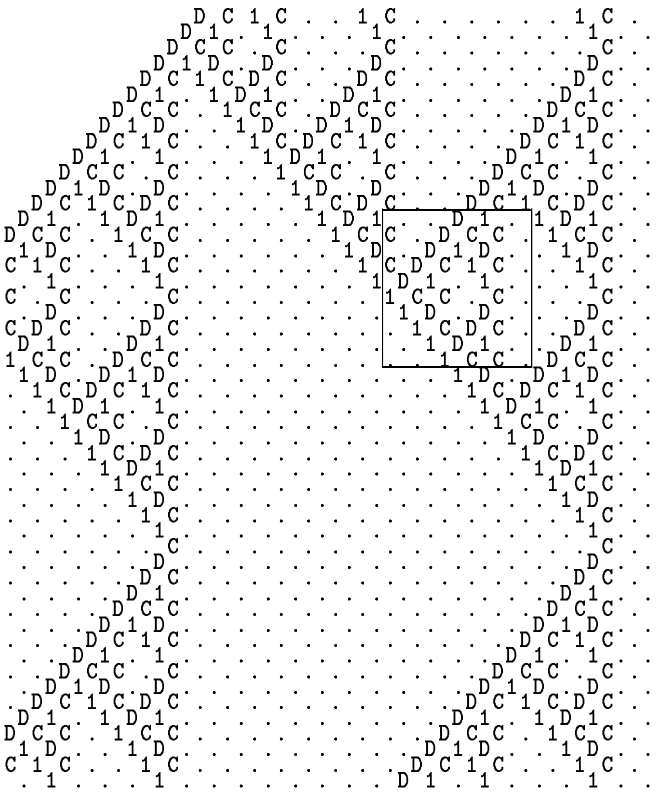


Figure 7.



	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	0	3	3	3	3	0	0	E	E	D	D	D	D	E	E
1	C	C	F	F	F	F	C	C	2	2	1	1	1	1	2	2
2	8	8	B	B	B	B	8	8	6	6	5	5	5	5	6	6
3	4	4	7	7	7	7	4	4	A	A	9	9	9	9	A	A
4	0	0	3	3	3	3	0	0	E	E	D	D	D	D	E	E
5	C	C	F	F	F	F	C	C	2	2	1	1	1	1	2	2
6	8	8	B	B	B	B	8	8	6	6	5	5	5	5	6	6
7	4	4	7	7	7	7	4	4	A	A	9	9	9	9	A	A
8	0	0	3	3	3	3	0	0	E	E	D	D	D	D	E	E
9	C	C	F	F	F	F	C	C	2	2	1	1	1	1	2	2
A	8	8	B	B	B	B	8	8	6	6	5	5	5	5	6	6
B	4	4	7	7	7	7	4	4	A	A	9	9	9	9	A	A
C	0	0	3	3	3	3	0	0	E	E	D	D	D	D	E	E
D	C	C	F	F	F	F	C	C	2	2	1	1	1	1	2	2
E	8	8	B	B	B	B	8	8	6	6	5	5	5	5	6	6
F	4	4	7	7	7	7	4	4	A	A	9	9	9	9	A	A

	0	1	C	D
0	0	0	D	D
1	C	C	1	1
C	0	0	D	D
D	C	C	1	1

	0	1	C	D
0	0	1	1	0
1	C	D	D	C
C	0	1	1	0
D	C	D	D	C

Figure 8.

6. FURTHER CONSTRUCTIONS OF REVERSIBLE ALGEBRAS

Here we shall present several simple constructions of reversible algebras from finite algebras satisfying left cancellation law

$$\forall \ldots \bigl(x * y = x * z \implies y = z\bigr),$$

or right cancellation law (given by similar formula, with x on the right side of $*$). If the left or the right division with respect to $*$ exists we shall denote it by $\backslash$ or $/$, respectively. Further, we shall show how to obtain a new reversible algebras from a given one and a permutation of its base set. We shall also investigate some properties of the corresponding GPT. We start by an easy general theorem:

Theorem 6.1. (1) *For every $X \in \{L, C, R\}$ the class of X-reversible algebras is closed under subalgebras, homomorphic images and direct products.*

(2) *If an algebra $\bigl\langle \mathbf{A}; f, \circ \bigr\rangle$ is L-, C- or R-reversible then the algebra $\bigl\langle \mathbf{A}; \mathrm{J}_{\mathbf{A}} \circ f, \circ \bigr\rangle$ ie R-, C- or L-reversible, respectively.*

Proof. For (1) we can use that every X-reversibility was characterized by an identity (see Theorem 4.3). Notice that for direct products we may not replace "X-reversible" by "reversible". (In CA terminology, we obtain a reversible local rule, but its reverse need not be binary.) For (2) we can use the same characterization, but now the concrete form of identities is substantial; notice that if g is an X-reverse of f then $g \circ \mathrm{J}$ is an X-reverse of $\mathrm{J} \circ f$. $\square$

Let $\mathcal{A} = \bigl\langle \mathbf{A}; *, \circ \bigr\rangle$ be an algebra which satisfies left or right cancellation law. We shall consider operations $\odot$ on $\mathbf{A}^2$ defined by formulas of the form

$$\langle x_1, x_0 \rangle \odot \langle y_1, y_0 \rangle = \langle \alpha_i * \beta_j, \gamma_k \rangle,$$

where $\alpha, \beta, \gamma \in \{x, y\}$ and $i, j, k \in \{0, 1\}$. This seems to be the simplest possible formula which really uses the operation $*$. (If we replace the right-hand side by $\langle \gamma_k, \alpha_i * \beta_j \rangle$ we obtain a formula as simple as the original one. However, it can be reduced to the original one by interchanging the components in all three ordered pairs in the formula.) There are 64 such rules but

(a) some of them can be reduced to others;
(b) some seems to give only trivial algebras, and
(c) for some there is no hope to obtain reversible algebras.

So we can substantially reduce the number of considered rules. (Notice that the form of the theorem below will be similar to that of Lemma 5.1.) By (a) we can restrict our considerations to $\alpha = x$. Left /right/ cancellation law can be applied probably only if $k = i$ or $k = j$, respectively. Therefore by (c) we shall assume $k \in \{i, j\}$. Further, if $i = j = k$ then the components x_n, y_n ($n = 1 - i$) play no role in the construction; therefore we shall consider only the case $i \neq j$. If $\gamma_k \in \{\alpha_i, \beta_j\}$ then we can use (left or right) division in each of $x \odot y$, $y \odot z$ separately. So we could use Theorem 6.3 below, and use a permutation instead of $*$. Therefore by (b) we shall exclude this case. (The above considerations are not rigorous. However, they serve only to choose the variants of $\odot$ into the following theorem. They are not used in its proof.)

Theorem 6.2. *Let $*$ be a binary operations on a finite set* $\mathbf{A}$ *and let the operations* $\odot_n$ *be defined for all* $x = \langle x_1, x_0\rangle \in \mathbf{A}^2$, $y = \langle y_1, y_0\rangle \in \mathbf{A}^2$*) as follows:*

$$\begin{aligned}
x \odot_1 y &= \langle x_1 * x_0, y_1\rangle, & x \odot_5 y &= \langle x_0 * x_1, y_1\rangle,\\
x \odot_2 y &= \langle x_1 * x_0, y_0\rangle, & x \odot_6 y &= \langle x_0 * x_1, y_0\rangle,\\
x \odot_3 y &= \langle x_1 * y_0, x_0\rangle, & x \odot_7 y &= \langle x_0 * y_1, x_1\rangle,\\
x \odot_4 y &= \langle x_1 * y_0, y_1\rangle, & x \odot_8 y &= \langle x_0 * y_1, y_0\rangle.
\end{aligned}$$

(1) If $*$ satisfies left cancellation law then the operations $\odot_1$, $\odot_6$ are C-reversible and the operations $\odot_4$, $\odot_8$ are R-reversible.

(2) If $*$ satisfies right cancellation law then the operations $\odot_2$, $\odot_5$ are C-reversible and the operations $\odot_3$, $\odot_7$ are L-reversible.

Proof. For each $\odot_n$ we can proceed as follows. Let $x = \langle x_1, x_0\rangle$, and analogously for the other letters. Let us (formally) compute $u = x * y$, $v = y * z$. We want to reconstruct both components of one of x, y, z from u, v. Two of six components are given immediately, and a further one can be obtained by $/$ or $\backslash$ applied to suitable components of u, v. In every case we obtain both components of one variable x, y, or z. So we could write a formula for reverse operation. Its verification is then very easy.

As an example consider $\odot_1$. Then $u = \langle x_1 * x_0, y_1\rangle$, $v = \langle y_1 * y_0, z_1\rangle$. We immediately know $y_1 = u_0$, $z_1 = v_0$, and we can compute $y_0 = u_0\backslash v_1$. Therefore the C-reverse of $\odot_1$ is

$$\langle u_1, u_0\rangle \otimes_1 \langle v_1, v_0\rangle = \langle u_0\backslash v_1,\ u_0\rangle.$$

Similarly we can obtain e.g. the C-reverse of $\odot_6$:

$$\langle u_1, u_0\rangle \otimes_6 \langle v_1, v_0\rangle = \langle u_0\backslash v_1,\ u_0\rangle,$$

and also the requested reverses of all remaining operations. □

Remark. Some of the operations from Theorem 6.2 give GPT of very simple structure only. E.g., these GPT considered as ternary relations on $\mathbb{N}$ are definable in Presburger arithmetics (the elementary theory of $\langle \mathbb{N}; +\rangle$). We do not prove that in the present paper. However, $\odot_n$ for $n = 1, 4, 5, 7$ can give GPT of rather complex structure. For example, the operation $*$ on $\{0, 1, 2\}$ defined by

$$x * y = y \ \text{ if } x \neq 2, \qquad 2 * 0 = 1, \qquad 2 * 1 = 2, \qquad 2 * 2 = 0.$$

can be use to define the binary operation of the left algebra in Figure 2 as $\odot_1$.

Theorem 6.3. *Let $*$ be an X-reversible ($X \in \{L, R, C\}$) operation on a finite set* $\mathbf{A}$ *and let ϕ be a permutation of the set* $\mathbf{A}$*. Then the operations $\oplus$, $\otimes$ defined (for all $x, y \in$* $\mathbf{A}$*) by*

(6.3.1) $$x \oplus y = \phi(x * y),$$

(6.3.2) $$x \otimes y = \phi(x) * \phi(y)$$

are X-reversible.

Proof. Let $\odot$ be an X-reverse of $*$ and $\psi = \phi^{-1}$. Then the operation

$$x \ominus y = \psi(x) \odot \psi(y)$$

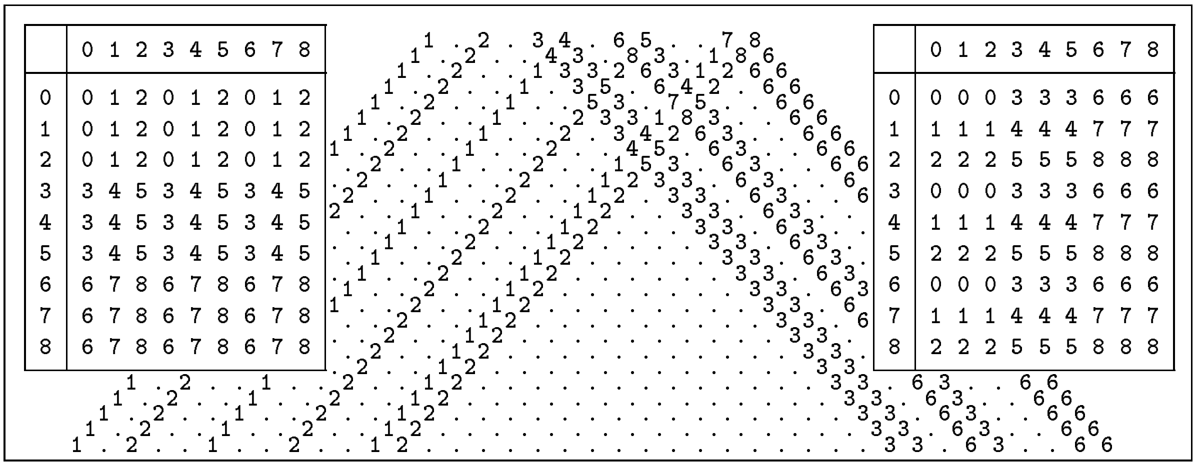
is an X-reverse of $\oplus$. Indeed, we have

$$(x \oplus y) \ominus (y \oplus z) = \psi(\phi(x * y)) \odot \psi(\phi(y * z)) = (x * y) \odot (y * z),$$

what is equal to x, y or z (depending on X). Up to now finiteness of $\mathbf{A}$ was not used. For $\otimes$ we can use Theorem 4.6. If $\mathbf{A}$ is finite then $\ominus$ is X-reversible, and the definitions of $\otimes$ and $\ominus$ have the same form in essential. ☐

Corollary 6.4. *Every X-reversible ($X \in \{L, C, R\}$) operation $\odot$ on a finite set $\mathbf{A}$ can be obtained from an idempotent X-reversible operation $*$ and a permutation ϕ by formula* (6.3.1) *(and by formula* (6.3.2) *as well).*

Proof. If $\odot$ is X-reversible then the unary operation $h(x) = x \odot x$ is a permutation of $\mathbf{A}$. For any idempotent operation $*$ the identity (6.3.1) would imply $x = \phi(h(x))$; hence $\phi = h^{-1}$. If we know ϕ (and $\oplus$) we can use (6.3.1) to define the operation $*$. Verification of required properties is straightforward. The proof for (6.3.2) is similar. ☐



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

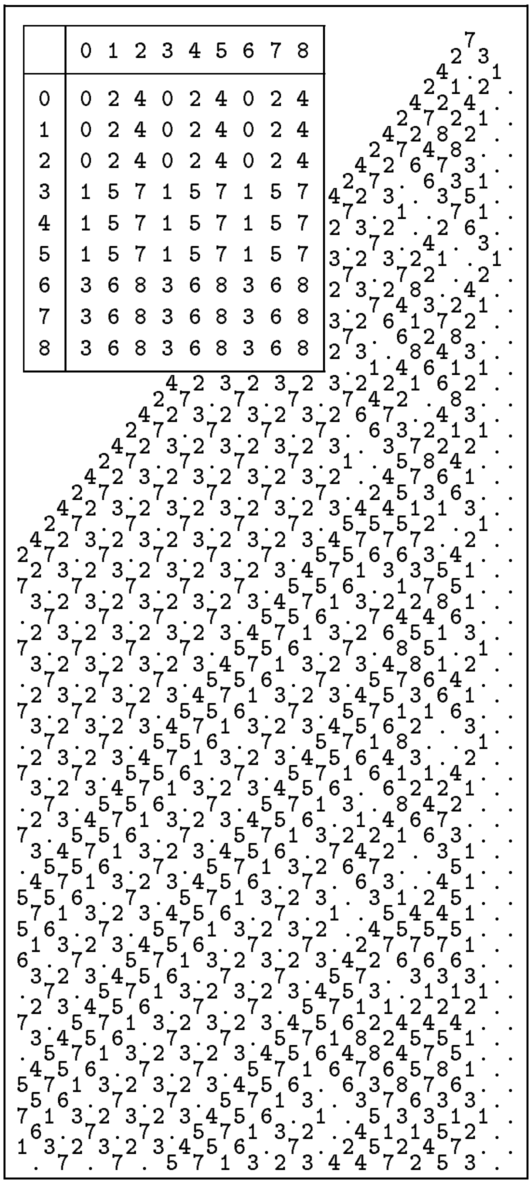
	0	1	2	3	4	5	6	7	8
0	0	0	0	3	3	3	6	6	6
1	1	1	1	4	4	4	7	7	7
2	2	2	2	5	5	5	8	8	8
3	0	0	0	3	3	3	6	6	6
4	1	1	1	4	4	4	7	7	7
5	2	2	2	5	5	5	8	8	8
6	0	0	0	3	3	3	6	6	6
7	1	1	1	4	4	4	7	7	7
8	2	2	2	5	5	5	8	8	8

Figure 9.

Example 6.5. We shall apply Corollary 6.4 to the idempotent C-reversible operation

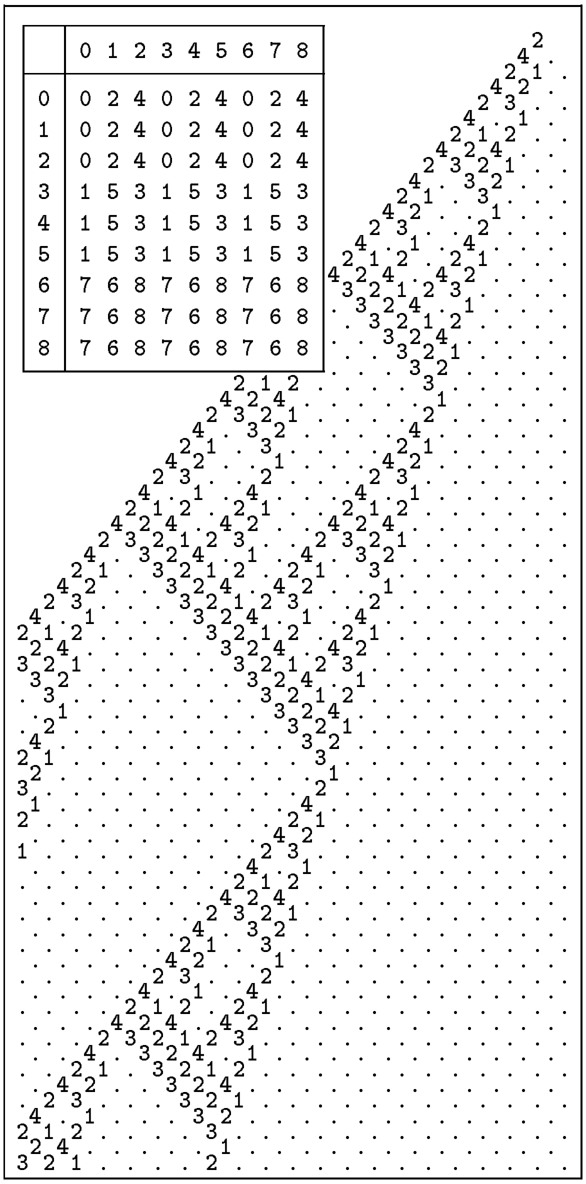
$$\langle x_1, x_0 \rangle \odot_0 \langle y_1, y_0 \rangle = \langle x_1, y_0 \rangle$$

on the set $\mathbf{A}^2$ where $\mathbf{A} = \{0, 1, 2\}$. Any element $\langle i, j \rangle \in \mathbf{A}^2$ will be replaced by the digit $3i + j$; this method was already used above for $\mathbf{A} = \{0, 1\}$. (The main reason why we use a bigger set here is to obtain substantially different examples of GPT.) Notice that the definition of $\odot_0$ is still simpler than the definitions in Theorem 6.2, and that all GPT of the algebra $\langle \mathbf{A}; \odot_0, 0 \rangle$ are trivial: they contain nonzero elements only on the margins of width depending on the initial word. A typical example is in Figure 9 (where the C-reverse algebra is on the right). Two next figures contain GPT of algebras obtained from $\langle \mathbf{A}; \odot_0, 0 \rangle$ by the formula (6.3.1).



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

Figure 10.



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

Figure 11.

REFERENCES

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

[Br] 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*, Intern. Journal Computer Math. **15 and 16** (1984), 195-212 and 3-22.

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

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

[K1] I. Korec, *Generalized Pascal triangles. Decidability results*, Acta Math. Univ. Comen. **46-47** (1985), 93-130.

[K2] I. Korec, *Generalized Pascal triangles*, K. Halkowska and S. Stawski, ed.: Proceedings of the V Universal Algebra Symposium, Turawa, Poland, May 1988, World Scientific, Singapore, 1989, pp. 198-218.

[K3] I. Korec, *Generalized Pascal triangles, their relation to cellular automata and their elementary theories*, K. Dassow and A. Kelemenová, ed.: Proceedings of 7th IMYCS Smolenice, November 16-20, 1992, Gordon and Breach Science Publishers, Yverdon (Switzerland), 1994, pp. 59-70.

[Ri] D. Richardson, *Tesselation with local transformations*, J. Cumput. System Sci. **6** (1972), 373-388.

MATHEMATICAL INSTITUTE, SLOVAK ACADEMY OF SCIENCES,
ŠTEFÁNIKOVA 49, 81473 BRATISLAVA, SLOVAKIA

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:

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

4/1996 *Ján Haluška*: Equal temperament and Pythagorean tuning: a geometrical interpretation in the plane

3/1996 *Winfried Just, Peter Vojtáš*: On matrix rapid filters

2/1996 *Anatolij Dvurečenskij*: Fuzzy set representations of some quantum structures

1/1996 *Miloslav Duchoň, Beloslav Riečan*: On the product of semigroup valued measures

(continued on inside back cover)