

Jaroslav Ježek; Tomáš Kepka

Groupoids and the associative law XII. (Representable cardinal functions)

Acta Universitatis Carolinae. Mathematica et Physica, Vol. 37 (1996), No. 1, 41--62

Persistent URL: <http://dml.cz/dmlcz/142677>

Terms of use:

© Univerzita Karlova v Praze, 1996

Institute of Mathematics of the Academy of Sciences of the Czech Republic provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these *Terms of use*.



This paper has been digitized, optimized for electronic delivery and stamped with digital signature within the project *DML-CZ: The Czech Digital Mathematics Library* <http://project.dml.cz>

Groupoids and the Associative Law XII. (Representable Cardinal Functions)

JAROSLAV JEŽEK and TOMÁŠ KEPKA

Praha*)

Received 10. October 1995

In this paper we investigate under what conditions is a mapping f of a semigroup S into the class of cardinals representable by a groupoid G and a homomorphism g of G onto S such that $\ker(g)$ is the associativity congruence of G and $\text{Card}(g^{-1}(x)) = f(x)$ for every $x \in S$.

V tomto článku vyšetřujeme, za jakých podmínek lze zobrazení f pologrupy S do třídy všech kardinálních čísel reprezentovat grupoidem G a zobrazením $g: G \rightarrow S$ tak, že $f(G) = S$, $\ker(g)$ je kongruence asociativity grupoidu G a $\text{Card}(g^{-1}(x)) = f(x)$ pro všechna $x \in S$.

XII.1 Introduction

For a groupoid G , we denote by s_G the least congruence of G such that the corresponding factor of G is a semigroup. Clearly, s_G is just the congruence of G generated by the pairs $(xy \cdot z, x \cdot yz)$ with $x, y, z \in G$ arbitrary.

Let S be a semigroup. By a cardinal function on S we mean a mapping of S into the class of nonzero cardinal numbers. We say that a cardinal function f on S is representable (by a groupoid) if there exist a groupoid G and a homomorphism g of G onto S such that $\ker(g) = s_G$ and $\text{Card}(g^{-1}(x)) = f(x)$ for every $x \in S$. We also say that the pair (G, g) represents the pair (S, f) .

In this paper we are going to investigate under what conditions is a cardinal function on a semigroup representable by a groupoid. Let us start with some definitions, observations and remarks.

A groupoid G is said to be counterassociative if $s_G = G \times G$. Among counterassociative groupoids we find all non-associative simple groupoids. These form a very large class; in particular, every groupoid can be embedded into a counterassociative groupoid.

Let S be a semigroup. We put $S^2 = SS = \{xy: x, y \in S\}$ and $S^n = SS^{n-1}$ for $n \geq 3$. Also, put $S^1 = S$. Put

$$\text{Id}(S) = \{a \in S: a = a^2\},$$

*) MFF UK, Sokolovská 83, 186 00 Praha 8, Czech Republic

$$\begin{aligned} \text{Lu}(S) &= \{a \in S : a \in Sa\}, \\ \text{Ru}(S) &= \{a \in S : a \in aS\}, \\ \text{Li}(S) &= \{a \in S : a \in \text{Id}(S)a\}, \\ \text{Ri}(S) &= \{a \in S : a \in a\text{Id}(S)\}, \\ \text{K}(S) &= \bigcap_{i=1}^{\infty} S^i. \end{aligned}$$

A semigroup S is called nilpotent of class at most n if S contains an annihilating element 0 (usually also called zero element) and $S^n = \{0\}$.

1.1 Lemma. *Let S be a semigroup. Then:*

- (1) $\text{Lu}(S)$ is either empty or a right ideal of S ; $\text{Ru}(S)$ is either empty or a left ideal of S ;
- (2) $\text{Li}(S)$ is either empty or a right ideal of S ; $\text{Ri}(S)$ is either empty or a left ideal of S ;
- (3) $\text{K}(S)$ is either empty or an ideal of S ;
- (4) $\text{Id}(S) \subseteq \text{Li}(S) \subseteq \text{Lu}(S) \subseteq \text{K}(S)$ and $\text{Id}(S) \subseteq \text{Ri}(S) \subseteq \text{Ru}(S) \subseteq \text{K}(S)$.

Proof. It is obvious. \square

1.2 Lemma. *Let S be a finite semigroup. Then $\text{Id}(S)$ is non-empty, $\text{Li}(S) = \text{Lu}(S)$, $\text{Ri}(S) = \text{Ru}(S)$ and $\text{Lu}(S) \cup \text{Ru}(S) \subseteq \text{Ru}(S)\text{Lu}(S)$.*

Proof. It is easy. \square

1.3 Lemma. *Let S be a finite semigroup with $S = S^2$. then $S = \text{Ru}(S)\text{Lu}(S)$. In particular, $S = \text{Lu}(S)$, provided that S is commutative.*

Proof. Put $I = \text{Ru}(S)\text{Lu}(S)$ and define a relation r on S by $(a, b) \in r$ if and only if $a \in bS$. Clearly, I is an ideal of S , r is a transitive relation and $a \in \text{Ru}(S)$ if and only if $(a, a) \in r$.

Suppose that there exists an element $a \in S - I$. Since $S = S^2$, there exists an infinite sequence a_0, a_1, a_2, \dots of elements of S such that $a_0 = a$ and $a_i = a_{i+1}b_i$ for some $b_i \in S$, whenever $i \geq 0$. We have $(a_i, a_{i+1}) \in r$; by transitivity, $(a_i, a_j) \in r$ whenever $0 \leq i < j$. Since I is an ideal and $a_0 \notin I$, we conclude that none of the elements a_0, a_1, a_2, \dots belongs to I . Since S is finite, it follows that $a_i = a_j$ for some $0 \leq i < j$. Thus $(a_i, a_i) \in r$, $a_i \in \text{Ru}(S)$ and, since $\text{Ru}(S) \subseteq I$ by 1.2, we get $a_i \in I$, a contradiction. \square

1.4 Example. Let T be the five-element semigroup with the following multiplication table:

T	0	a	b	c	d
0	0	0	0	0	0
a	0	0	0	0	0
b	0	0	0	a	b
c	0	0	0	0	0
d	0	0	0	c	d

We have $T = T^2$ and $a \notin \text{Lu}(T) \cup \text{Ru}(T)$.

1.5 Lemma. *Let S be a semigroup with at most five elements, such that $S = S^2$ and $\text{Lu}(S) \cup \text{Ru}(S) \neq S$. Then S is isomorphic to the semigroup T from Example 1.4.*

Proof. Take an element $a \in S - (\text{Lu}(T) \cup \text{Ru}(T))$. By 1.3, we have $a = bc$ for some elements $b \in \text{Ru}(S)$ and $c \in \text{Lu}(S)$. Clearly, $b \notin \text{Lu}(S)$ and $c \notin \text{Ru}(S)$. Put $0 = a^2$. It is easy to see that the four elements $0, a, b, c$ are pairwise different. Since $b \in \text{Ru}(S)$, we have $b \in bd$ for some element d .

Let us prove that $d \notin \{0, a, b, c\}$. Clearly, $d \neq b$ and $d \neq c$. If either $d = a$ or $d = 0 = a^2$, then either $b = ba$ or $b = ba^2$; then it follows from $a = bc$ that for any $n \geq 1$ we can write $a = b^n x$ for some element x ; but b^n is an idempotent for some $n \geq 1$ and we get $a \in \text{Lu}(S)$, a contradiction.

Hence $\text{Card}(S) = 5$ and $S = \{0, a, b, c, d\}$.

Quite similarly, there is an element d' with $c = d'c$, and $d' \notin \{0, a, b, c\}$. Hence $d' = d$ and we get $dc = c$. Now we shall try to compute the rest of the multiplication table for S .

It is easy to see that $ab \neq a, b, c, d$, and hence $ab = 0$. We also have, by similar arguments, $bb = cc = ba = ac = ca = 0$.

Clearly, $ad \neq a$ and $ad \neq b$. If $ad = c$, then $a = bc = bad = b^2ad = \dots$, a contradiction. If $ad = d$, then $b = bd = bad$ and $a = bc = badc = b^2a(dc)^2 = \dots$, again a contradiction. Consequently, $ad = 0$ and, similarly, $da = 0$. Since $a \notin \text{Ru}(S) \cup \text{Lu}(S)$, $b \notin \text{Lu}(S)$ and $c \notin \text{Ru}(S)$, we have $cb = cd = db = 0$. Clearly, $a^3 \neq a, b, c$. If $a^3 = d$, then $a = bc = bdc = ba^3c$, which is not possible. Thus $a^3 = 0$ and it follows that $00 = b0 = 0b = c0 = 0c = d0 = 0d = 0$. Finally, $dd = d$, since $S = S^2$. \square

An element a of a semigroup S is said to be of height n if $a \in S^n$ but $a \notin S^{n+1}$; a is said to be of infinite height if $a \in K(S)$. Clearly, if S contains only elements of finite height, then S is infinite.

1.6 Proposition. *Let G be a division groupoid. Then G/s_G is a group and the blocks of s_G are all of the same cardinality.*

Proof. G/s_G is a division semigroup, and hence a group. Let A and B be two blocks of s_G ; take two elements $a \in A$ and $b \in B$. We have $ca = b$ for some $c \in G$ and $cA \subseteq B$. On the other hand, if $d \in B$, $e \in G$ and $ce = d$, then $(ca, ce) \in s_G$, $(a, e) \in s_G$, $e \in A$ and we see that $cA = B$. Consequently, $\text{Card}(A) \geq \text{Card}(B)$ and the rest is clear. \square

Let G be a division groupoid. We put $\sigma(G) = \text{Card}(A)$, where A is a block of s_G . By 1.6, $\sigma(G)$ does not depend on the choice of the block A .

Let G be a groupoid. One can define a binary hyperoperation \circ on G by $x \circ y = \{z \in G : (xy, z) \in s_G\}$. It is easy to check that $G(\circ)$ is then a semihypergroup (called the associativity semihypergroup of the groupoid G). This semihypergroup

is complete and it is a hypergroup if and only if G/s_G is a group. In particular, $G(\circ)$ is a hypergroup, provided G is a division groupoid.

XII.2 A necessary condition

2.1 Lemma. *Let f be a representable cardinal function on a semigroup S . Then $f(a) = 1$ for every $a \in S - S^3$.*

Proof. Let (G, g) be a pair representing the pair (S, f) . Let $a \in S - S^3$ and suppose $f(a) \geq 2$. Then the set $A = g^{-1}(a)$ is the disjoint union of two non-empty subsets, say $A = B \cup C$, and the relation $r = (s_G - (A \times A)) \cup (B \times B) \cup (C \times C)$ is an equivalence on G properly contained in s_G .

If x, y, z are three elements of G , then the elements $x \cdot yz$ and $xy \cdot z$ do not belong to A and $(x \cdot yz, xy \cdot z) \in s_G$; hence $(x \cdot yz, xy \cdot z) \in r$. Now, to get a contradiction, it suffices to show that r is a congruence of G . This is clear if $a \notin S^2$. So, let $a \in S^2$. We shall prove, for example, that $(x, y) \in r$ implies $(zx, zy) \in r$. Of course, we have $(zx, zy) \in s_G$. If $zx \notin A$, then $(zx, zy) \in r$ follows. If $zx \in A$, then $a = g(zx) = g(z)g(x)$, $g(x) = g(y) \in S - S^2$ and therefore $x = y$ (we have $f(g(x)) = 1$); then $zx = zy$ and $(zx, zy) \in r$. \square

2.2 Lemma. *Let I be a non-empty set and \mathcal{K} be a non-empty system of pairwise disjoint non-empty sets. The following two conditions are equivalent:*

- (1) *There exists a mapping h of $\bigcup \mathcal{K}$ onto I such that $I \times I$ is the only equivalence on I containing all the relations $h(K) \times h(K)$ with $K \in \mathcal{K}$.*
- (2) $\text{Card}(I) \leq 1 + \sum_{K \in \mathcal{K}} (\text{Card } K - 1)$.

Proof. Let us start with the direct implication. Let us construct, by transfinite induction, for an ordinal number i an element K_i of \mathcal{K} and an element $a_i \in K_i$ as follows. K_0 is any element of \mathcal{K} , and a_0 is any element of K_0 . Now let i be an ordinal number such that K_j and a_j have been defined for all $j < i$. Put $\mathcal{K}' = \{K_j : j < i\}$. If $\mathcal{K}' = \mathcal{K}$, we stop the construction, so that i is the first ordinal number for which K_i is not defined. Otherwise, it follows easily from (1) that there is a set $K \in \mathcal{K} - \mathcal{K}'$ such that $h(K)$ has a non-empty intersection with $h(K_j)$ for some $j < i$. Put $K_i = K$ let a_i be an element of K_i with $h(a_i) = h(b)$ for some $b \in K_j$. It is easy to see that h maps the set $\{a_0\} \cup \sum_i (K_i - \{a_i\})$ onto I . Consequently, $\text{Card}(I)$ cannot be bigger than the cardinality of the set, which is just the right side of the inequality (2).

It remains to prove the converse. For every $K \in \mathcal{K}$ take an element $a_K \in K$ arbitrarily. Moreover, take an element $b \in I$. It follows from (2) that there exists a mapping h_0 of $\bigcup_{K \in \mathcal{K}} (K - \{a_K\})$ onto $I - \{b\}$. Let h be the extension of h_0 with $h(a_K) = b$ for all $K \in \mathcal{K}$. It is easy to see that h has the desired property. \square

Let S be a semigroup and a be an element of S . We denote $M_a = \{(b, c) \in S \times S : bc = a\}$. Further, we denote by E_a the equivalence on M_a generated by the pairs $((bc, c), (b, cd))$ where $b, c, d \in S$ are such that $bcd = a$. Put $e_a = \text{Card}(M_a/E_a)$, so that e_a is the number of blocks of E_a .

Let f be a cardinal function on a semigroup S . We introduce the following condition:

$$(R) \quad f(a) \leq 1 + \sum_{B \in M_a/E_a} \left(\left(\sum_{(b, c) \in B} f(b)f(c) \right) - 1 \right) \quad \text{for every } a \in S.$$

2.3 Theorem. *Let f be a cardinal function on a semigroup S . If f is representable, then the condition (R) is satisfied.*

Proof. Let G be a groupoid and g be a homomorphism of G onto S such that (G, g) represents (S, f) . For an element $a \in S$ such that $f(a) = 1$, the inequality in (R) is trivially true; with respect to 2.1, we can assume that $a \in S^3$ and $f(a) \geq 2$. Put $I = g^{-1}(a)$, so that $\text{Card}(I) \geq 2$.

Define a binary relation s on G by $(u, v) \in s$ if and only if $(u, v) \in \ker(g) = s_G$ and if $u, v \in I$, then either $u = v$ or $u, v \in GG$. One can easily see that s is a congruence of G , $s \subseteq \ker(g)$ and G/s is a semigroup. Consequently, $s = \ker(g) = s_G$ and we have proved that $I \subseteq GG$ (use the fact that $\text{Card}(I) \geq 2$).

Further, define a binary relation r on G as follows: $(u, v) \in r$ if and only if $u, v \in \ker(g)$ and if $u, v \in I$ then there exists a finite sequence u_0, \dots, u_k , $k \geq 0$, elements of I such that $u_0 = u$, $u_k = v$ and such that for each $i = 1, \dots, k$ there exist elements $x, y, z, t \in G$ with $u_{i-1} = xy$, $u_i = zt$ and $((g(x), g(y)), (g(z), g(t))) \in E_a$. Again, it is easy to see that r is an equivalence on G . It is a congruence, as well, since if $(u, v) \in r$ and $w \in G$, then in the case $uw, vw \in I$ we can put $k = 1$, $u_0 = uw$, $u_1 = vw$, $x = u$, $y = w$, $z = v$ and $t = w$ to get $(uw, vw) \in r$ (we have $(g(x), g(y)) = (g(z), g(t))$); similarly, $(wu, wv) \in r$. In order to be able to assert that G/r is a semigroup, we have to prove $(uv \cdot w, u \cdot vw) \in r$ for all $u, v, w \in G$. We have, of course, $(uv \cdot w, u \cdot vw) \in \ker(g)$. Let both $uv \cdot w$ and $u \cdot vw$ belong to I . Then we can put $k = 1$, $u_0 = uv \cdot w$, $u_1 = u \cdot vw$, $x = uv$, $y = w$, $z = u$, $t = vw$ to get $(uv \cdot w, u \cdot vw) \in r$. We have proved that G/r is a semigroup, and therefore $r = \ker(g) = s_G$. This means that for any two elements u, v in I , there exists a finite sequence u_0, \dots, u_k as above.

For every block B of E_a , let K_B denote the set of the elements $x \in I$ such that $x = yz$ for some $y, z \in G$ with $(g(y), g(z)) \in B$. From what we have proved it follows that the system \mathcal{K} of the sets K_B , $B \in M_a/E_a$, has the following properties: $\bigcup \mathcal{K} = I$, and $I \times I$ is the only equivalence on I containing all the relations $K_B \times K_B$. The system \mathcal{K} need not be, in general, a system of pairwise disjoint sets, but in such a case we can take a system \mathcal{K}' of pairwise disjoint copies of the sets K_B instead, and the natural projection $h: \bigcup \mathcal{K}' \rightarrow I$. By 2.2, we get

$$\text{Card}(I) \leq 1 + \sum_{B \in M_a/E_a} (\text{Card}(K_B) - 1).$$

However, $\text{Card}(I) = f(a)$ and, as it is easy to see,

$$\text{Card}(K_B) \leq \sum_{(b,c) \in B} f(b)f(c). \quad \square$$

2.4 Corollary. *Let f be a cardinal function on a semigroup S . If f is representable, then*

$$f(a) \leq \sum_{(b,c) \in M_a} f(b)f(c)$$

for every $a \in S^2$. \square

2.5 Theorem. *Let S be a semigroup (which may but need not contain a zero) in which every nonzero element is of finite height. A cardinal function f on S is representable if and only if the condition (R) is satisfied.*

Proof. The necessity of (R) was proved in Theorem 2.3. Let (R) be satisfied.

For every element $a \in S$ take a set A_a of cardinality $f(a)$ and denote by G the disjoint union of the sets A_a , $a \in S$. Define a mapping g of G onto S by $g(x) = a$ for all $a \in S$ and $x \in A_a$. We are going to define a binary operation (multiplication) on G .

Let a be a nonzero element of SS . For every $B \in M_a/E_a$ let $K_B = \bigcup_{(b,c) \in B} (A_b \times A_c)$. From (R) we get that condition (2) of 2.2 is satisfied for the system \mathcal{K} of the sets K_B , $B \in M_a/E_a$. Consequently, by Lemma 2.2, there exists a mapping h_a of $\bigcup_{(b,c) \in M_a} (A_b \times A_c)$ onto A_a such that $A_a \times A_a$ is the only equivalence on A_a containing the relation $\bigcup_{(b,c) \in B} h_a(A_b \times A_c)$ for any block B of E_a . Now, if $(b, c) \in M_a$, $x \in A_b$ and $y \in A_c$, and we put $xy = h_a(x, y)$.

So far, we have defined the product xy for all $x, y \in G$ such that $x \in A_b$ and $y \in A_c$, where $bc \neq 0$. If S has no zero, the multiplication on G is well defined. In the opposite case, we need to complete the definition by considering the pairs $x \in A_b$, $y \in A_c$, where $bc = 0$. Then, take a fixed element $o \in A_0$ and put $xo = x$ if $x \in A_0$ and $xy = o$ in the remaining cases. Now, we have obtained a groupoid G .

Clearly, g is homomorphism of G onto S and it remains to show that $\ker(g) = s_G$. For, let r be a congruence of G such that G/r is a semigroup. We have to prove that $A_a \times A_a \subseteq r$ for any element $a \in S$. If S contains a zero, then $A_0 \times A_0 \subseteq r$ is easily seen: for any element $x \in A_0 - \{o\}$ we have $xo \cdot x = x$, so that $(o, x) \in r$.

Now, we have to show that $A_a \times A_a \subseteq r$ for every $0 \neq a \in S$. This will be done by induction on the height of a . If the height is at most 2, then $f(a) = 1$ and everything is clear. Let $a \in S^3$. By induction we can suppose that $A_b \times A_b \subseteq r$ whenever b has smaller height than a .

According to the construction of h_a , it is enough to prove that if B is a block of E_a and if (b, c) and (d, e) are two elements of B , then $(xy, zu) \in r$ for all $x \in A_b$,

$y \in A_c$, $z \in A_d$, and $u \in A_e$. In other words, to prove that the equivalence E_a is contained in the binary relation E on M_a defined as follows: E is the set of the ordered pairs $((b, c), (d, e)) \in M_a \times M_a$ such that $(xy, zu) \in r$ for all $x \in A_b$, $y \in A_c$, $z \in A_d$ and $u \in A_e$.

By the definition of E_a , it suffices to show that E is an equivalence relation containing all the pairs $((bc, d), (b, cd))$ where $b, c, d \in S$ are such that $bcd = a$. The reflexivity of E can be verified easily: if $(b, c) \in M_a$ and $x \in A_b$, $y \in A_c$, $z \in A_b$, $u \in A_c$, then $(x, z) \in r$ and $(y, u) \in r$ (since both b and c have smaller height than a), so that $(xy, zu) \in r$, which yields $((b, c), (b, c)) \in E$. The symmetry and the transitivity of E are easily seen, as well. Now, let $b, c, d \in S$ and $bcd = a$. Take $x \in A_{bc}$, $y \in A_d$, $z \in A_b$, $u \in A_{cd}$, and $v \in A_c$. Since the elements bc and cd are of smaller height than a , we have $(zv, x) \in r$ and $(vy, u) \in r$. Further, $(zv \cdot y, z \cdot vy) \in r$ by the definition of r , and hence, since r is a congruence, $(xy, zy) \in r$. From this, $((bc, d), (b, cd)) \in r$, which concludes the proof. \square

2.6 Corollary. *Let S be a nilpotent semigroup. A cardinal function f on S is representable if and only if the condition (R) is satisfied.* \square

$$(R') \quad f(a) = 1 \quad \text{for every } a \in S - S^3 \quad \text{and} \\ f(a) + e_a \leq 1 + \sum_{(b,c) \in M_a} f(b)f(c) \quad \text{for every } a \in S^3.$$

2.7 Proposition. *Let S be a semigroup and let f be a cardinal function on S . then:*

- (1) (R) implies (R'). (In particular, (R) implies that $f(a) = 1$ whenever $a \in S - S^3$.)
- (2) If M_a is finite for every $a \in S$ (in particular, if S is finite), then also (R') implies (R).

Proof. It is easy. \square

2.8 Theorem. *Let S be a free semigroup (or, more generally, a subsemigroup of a free semigroup) and let f be a cardinal function on S . Then f is representable if and only if it satisfied the condition (R').*

Proof. It follows from theorems 2.3, 2.5 and 2.7(2). \square

2.9 Example. Let S be a semigroup nilpotent of class at most 3. According to 2.6, a cardinal function f on S is representable if and only if $f(a) = 1$ for every $a \in S - \{0\}$.

2.10 Example. Let $S = \{0, 1, \dots\} \cup (\{2, 3, \dots\} \times \{2, 3, \dots\})$. Define a binary operation $*$ on S as follows: for $i, j, k \geq 2$, $i * j = (i, j)$ and $(i, j) * k = k * (i, j) = 1$; all the remaining products are 0. It is easy to check that $S(*)$ is a semigroup nilpotent of class 4. By 2.6, a cardinal function f on this semigroup is representable if and only if $f(i) = f(i, j) = 1$ for all $i, j \geq 2$ and $f(1) \leq \aleph_0$.

2.11 Example. Let $S = \{0, 1, 2, 3, \dots\}$. Define a binary operation $*$ on S as follows: $3 * 3 = 2$, $2 * 3 = 3 * 2 = 1$, $i * j = 1$ for all $i, j \geq 4$; and all the remaining products are 0. By 2.6, a cardinal function on this semigroup is representable if and only if $f(i) = 1$ for all $i \geq 2$ and $f(1) \in \{1, 2\}$.

This example shows that condition (R') is not strong enough (even for semigroups nilpotent of class 4) to characterize the representable cardinal functions: here, (R') is satisfied if $f(i) = 1$ for all $i \geq 2$ and $f(1) \leq \aleph_0$.

2.12 Example. Let $S = \{0, a, b, c, d, e, f, g, h, i, z_1, z_2, \dots\}$ and let a multiplication on S be given as follows: $bc = di = hf = a$, $dz_k = b$, $ef = c$, $z_k e = g$, $be = dg = h$, $gf = z_k c = i$, and the remaining products are all equal to 0. It needs just a tedious checking to show that S is a semigroup nilpotent of class 4, $S^2 = \{0, a, b, c, g, h, i\}$, $S^3 = \{0, a, h, i\}$, and $e_a = e_h = e_i = 1$. By Theorem 2.5, a cardinal function F on S is representable if and only if $F(b) = F(c) = F(d) = F(e) = F(f) = F(g) = F(z_k) = 1$, $F(h) \leq 2$, $F(i) \leq \aleph_0$ and $F(a) \leq 3 + F(i)$. Hence, if $F(i) = \aleph_0$, we can take $F(a) = \aleph_0$, as well.

XII.3 Catalan numbers and representability of cardinal functions on free semigroups

Let $0! = 1$ and $n! = 1 \cdot 2 \dots (n - 1) \cdot n$ for every positive integer n .

In the following, we shall make use of the numbers $\binom{n}{m}$, n and m being arbitrary integers. These are defined as follows: $\binom{n}{m} = 0$ if $n < 0$; $\binom{0}{0} = 1$ and $\binom{0}{m} = 0$ for every $m \neq 0$; if $n > 0$, then $\binom{n}{m}$ are defined by induction on n , namely, $\binom{n}{m} = \binom{n-1}{m-1} + \binom{n-1}{m}$. For any integers n and m , the following are clearly true:

- (1) $\binom{n}{m}$ is a nonnegative integer and $\binom{n}{m} = 0$ if and only if either $n < 0$ or $m < 0$ or $n < m$.
- (2) If $n < 0$, then $\binom{n}{0} = \binom{n}{n} = 1$.
- (3) If $0 \leq m \leq n$, then $\binom{n}{m} = n! / m!(n - m)!$
- (4) If $n \geq 0$, then $\binom{n}{m}$ is just the number of the m -element subsets of an n -element set and $2^n = \sum_{m=0}^n \binom{n}{m}$.

For any rational number q and any nonnegative integer n , define $q^{(n)}$ as follows: $q^{(0)} = 1$; $q^{(n+1)} = q^{(n)} \cdot (q - n)$. Obviously, $q^{(n)} = q(q - 1) \dots (q - n + 1)$ for $n > 0$ and $1^{(n)} = 0$ for $n \geq 2$.

3.1 Lemma. *We have*

$$(r + s)^{(n)} = \sum_{m=0}^n \binom{n}{m} r^{(m)} s^{(n-m)}$$

for all rational numbers r, s and nonnegative integers n .

Proof. It is easy by induction on n . \square

3.2 Lemma. $(1/2)^{(n)} = (-1)^{n-1} \cdot (1/2)^n \cdot (2n-3)! / (2^{n-2} \cdot (n-2)!)$ for every $n \geq 2$.

Proof. It follows easily from

$$1 \cdot 3 \cdot 5 \dots (2m+1) = (2m+1)! / (2^m \cdot m!),$$

which is easy to prove for any $m \geq 0$. \square

The Catalan numbers c_n , $n \geq 1$, are defined by $c_1 = 1$ and $c_n = c_1 c_{n-1} + c_2 c_{n-2} + \dots + c_{n-2} c_2 + c_{n-1} c_1$ for $n \geq 2$. Clearly,

$$c_n = \begin{cases} 2c_1 c_{n-1} + \dots + 2c_{(n-1)/2} c_{(n+1)/2} & \text{for } n \geq 3 \text{ odd,} \\ 2c_1 c_{n-1} + \dots + 2c_{(n-2)/2} c_{(n+2)/2} + c_{n/2}^2 & \text{for } n \geq 2 \text{ even.} \end{cases}$$

In particular, we have

$$c_1 = 1, c_2 = 1, c_3 = 2, c_4 = 5, c_5 = 14, c_6 = 42, c_7 = 132, c_8 = 429,$$

$$c_9 = 1430, c_{10} = 4862.$$

For any nonnegative integer n , let $v_n = (1/2)^{(n)}/n!$. By 3.2,

$$v_0 = 1, v_1 = 1/2, \text{ and } v_n = (-1)^{n-1} (2n-3)! / 2^{2n-2} \cdot (n-2)! \cdot n! \text{ for } n \geq 2.$$

Let $Q\{x\}$ denote the integral domain of formal power series in one indeterminate x over Q . Put $f = \sum_{k=0}^{\infty} v_k x^k \in Q\{x\}$ and let $f^2 = \sum_{k=0}^{\infty} u_k x^k$. Then, for every $n \geq 0$,

$$\begin{aligned} u_n &= \sum_{m=0}^n v_m v_{n-m} = \sum_{m=0}^n (1/2)^{(m)} \cdot (1/2)^{(n-m)}/m! \cdot (n-m)! \\ &= (1/n!) \sum_{m=0}^n \binom{n}{m} (1/2)^{(m)} (1/2)^{(n-m)} = (1/n!) \cdot 1^{(n)} \end{aligned}$$

by Lemma 3.1. Thus $u_0 = 1$, $u_1 = 1$ and $u_n = 0$ for $n \geq 2$. We have proved that $f^2 = 1 + x$.

Now, put $g = \sum_{k=0}^{\infty} c_k x^k \in Q\{x\}$, where $c_0 = 0$ and the other coefficients are Catalan numbers. Let $g^2 = \sum_{k=0}^{\infty} d_k x^k$. Then $d_0 = c_0^2 = 0 = c_0$, $d_1 = 2c_0 c_1 = 0$ and $d_n = c_0 c_n + c_1 c_{n-1} + \dots + c_{n-1} c_1 + c_n c_0 = c_n$ for each $n \geq 2$. Hence $g^2 = g - x$ and $g^2 - g + x = 0$ in $Q\{x\}$. On the other hand, it follows from what was proved above that $h^2 = 1 - 4x$, where $h = \sum_{k=0}^{\infty} v_k (-4x)^k \in Q\{x\}$. Hence $(g - 1/2)^2 = h^2/4$. From this, either $g = (h + 1)/2$ or $g = (1 - h)/2$. The first case is not possible, since $c_0 = 0$ and $v_0 = 1$. Consequently, $g = (1 - h)/2$. We get $c_k = (-1)^{k+1} 2^{2k-1} v_k = (2k-2)! / (k-1)! \cdot k!$ for $k \geq 2$. The result is also true for $k = 1$. So, we have proved the following

3.3 Proposition. $c_n = (2n-2)! / n!(n-1)!$ for every $n \geq 1$. \square

3.4 Remark. From 3.3 it follows that $c_n/c_{n-1} = (4n-6)/n$ for every $n \geq 2$ and $c_n - c_{n-1} = 3(2n-4)! / n!(n-3)!$. Since $n! = n^{(n)}$ and $\binom{n}{m} = n^{(m)}/m^{(m)}$ for all $0 \leq m \leq n$, we have $c_n = (2n-2)^{(n-1)}/n^{(n)}$.

3.5 Theorem. A cardinal function f on the additive semigroup of positive integers is representable if and only if $f(1) = f(2) = 1$ and $f(n) \leq \sum_{i=1}^{n-1} f(i) f(n-i)$ for all $n \geq 3$.

Proof. The semigroup is a free semigroup with one generator. By Theorem 2.8, f is representable if and only if (R') is satisfied. Now, (R') is equivalent to the above condition, since evidently $e_n = 1$ for every $n \geq 3$. \square

Let us call an infinite sequence a_1, a_2, \dots representable, if the cardinal function f , where $f(n) = a_n$, is representable on the additive semigroup of positive integers. It follows from Theorem 3.5 and Proposition 3.3 that if a_1, a_2, \dots is representable, then $a_n \leq c_n = (2n-2)!/n!(n-1)!$ for every positive integer n . On the other hand, the sequence c_1, c_2, \dots is representable by Theorem 3.5. Consequently, the sequence of Catalan numbers is the best upper bound for representable sequences of positive integers.

3.6 Example. It follows easily from Theorem 3.5 that any sequence a_1, a_2, \dots of positive integers, such that $a_1 = 1$ and $a_n \leq n(n-1)/2$ for all $n \geq 2$, is representable. In particular, there are uncountably many representable sequences of positive integers.

3.7 Theorem. Let S be a free semigroup with free generating set X . A cardinal function f on S is representable if and only if $f(x) = 1$ for all $x \in X$ and $f(x_1 \dots x_n) \leq \sum_{i=1}^{n-1} f(x_1 \dots x_i) f(x_{i+1} \dots x_n)$ for all $n \geq 2$ and $x_1, \dots, x_n \in X$. If f is representable, then $f(u) \leq c_{\lambda(u)}$ for every $u \in S$, where $\lambda(u)$ denotes the length of u .

Proof. It follows from Theorem 2.8; note that $e_u = 1$ for all elements $u \in S$ of length ≥ 2 . \square

3.8 Example. Let S be a free semigroup with free generating set X . The cardinal function f on S , defined by $f(u) = c_{\lambda(u)}$, is representable. In fact, if G is the absolutely free groupoid over X and $g: G \rightarrow S$ is the natural projection, then $\ker(g) = s_G$ and $\text{Card}(g^{-1}(u)) = c_{\lambda(u)}$ for every $u \in S$.

XII.4 A representation criterion

Let f be a cardinal function on a semigroup S . For every $a \in S$ we define a cardinal function f_a on S by $f_a(a) = f(a)$ and $f_a(b) = 1$ for every $b \in S, b \neq a$.

4.1 Theorem. Let f be a cardinal function on a semigroup S . If f_a is representable for any $a \in S$, then f is also representable.

Proof. There exist pairwise disjoint groupoids $G_a (a \in S)$ and projective homomorphism $g_a: G_a \rightarrow S$ such that $\ker(g_a) = s_{G_a}$ and $\text{Card}(g_a^{-1}(a)) = f(a)$ and $\text{Card}(g_a^{-1}(b)) = 1$ for $b \neq a$. The operations of the groupoids G_a will be denoted

by $*$. We put $H_a = g_a^{-1}(a)$ and $G = \bigcup_{a \in S} H_a$. We shall make G a groupoid by defining its operation in the following way.

- (1) If $x, y \in H_a$ and $a = aa$, then $xy = x * y \in H_a$.
- (2) If $x \in H_a, y \in H_b$ and $ab = c$, where $a \neq c \neq b$, then $xy = g_c^{-1}(a) * g_c^{-1}(b) \in H_c$.
- (3) If $x \in H_a, y \in H_b, a \neq b$ and $ab = a$, then $xy = x * g_a^{-1}(b) \in H_a$.
- (4) If $x \in H_a, y \in H_b, a \neq b$ and $ab = b$, then $xy = g_b^{-1}(a) * y \in H_b$.

It is obvious that the mapping $g: G \rightarrow S$, defined by $g(H_a) = a$ for all $a \in S$, is a homomorphism of G onto S . We still have to show that $s_G = \ker(g)$. Clearly, $s_G \subseteq \ker(g)$. For every $a \in S$ define an equivalence t_a on G by

$$t_a = (\ker(g) - (H_a \times H_a)) \cup (s_G \cap (H_a \times H_a))$$

and an equivalence r_a on G_a by

$$r_a = \{(x, x) : x \in G_a\} \cup (s_G \cap (H_a \times H_a)).$$

We are going to show that t_a is a congruence of G and r_a is a congruence of G_a .

In order to prove that $(x, y) \in t_a$ implies $(zx, zy) \in t_a$ for any elements $x, y, z \in G$, we will distinguish two cases.

Case 1: $x, y \in H_b$ for some $b \neq a$. Then $(zx, zy) \in \ker(g)$ and $(zx, zy) \in t_a$, if $zx \notin H_a$. If $zx \in H_a$, then $zy \in H_a$, too, and there is an element $c \in S$ such that $z \in H_c$ and $a = cb$. If $a \neq c$, then $zx = g_a^{-1}(c) * g_a^{-1}(b) = zy$, and hence $(zx, zy) \in t_a$. If $a = c$, then $zx = z * g_a^{-1}(b) = zy$ and again $(zx, zy) \in t_a$.

Case 2: $x, y \in H_a$ and $(x, y) \in s_G$. If $zx \notin H_a$ and $zy \notin H_a$, then $(zx, zy) \in \ker(g)$ and $(zx, zy) \in t_a$. If $zx, zy \in H_a$, then $(zx, zy) \in s_G \cap (H_a \times H_a)$, and hence $(zx, zy) \in t_a$.

One can prove similarly that $(x, y) \in t_a$ implies $(xz, yz) \in t_a$. We conclude that t_a is a congruence of G .

Now let x, y, z be three elements of G_a with $(x, y) \in r_a$. We have to take into account the following three cases.

Case 1: $x \notin H_a$. Then $y \notin H_a, x = y$ and $(z * x, z * y) \in r_a$.

Case 2: $x \in H_a$ and $z * x \in H_a$. We have $y \in H_a, (x, y) \in \ker(g_a), (z * x, z * y) \in \ker(g_a)$ and thus $z * x = z * y$, which implies $(z * x, z * y) \in r_a$.

Case 3: $x \in H_a$ and $z * x \in H_a$. Then $y \in H_a, z * y \in H_a$ and, naturally, $(x, y) \in s_G$. Put $b = g_a(z)$, so that $a = ba$. If $b \neq a$ (this means $z \notin H_a$), then, for any $u \in H_b, (ux, uy) \in s_G$ and, moreover, $ux = z * x$ and $uy = z * y$; consequently $(z * x, z * y) \in r_a$. If $b = a$ (then $z \in H_a$), we have $(zx, zy) \in s_G, zx = z * x$ and $zy = z * y$; once again, $(z * x, z * y) \in r_a$.

Since $(x * z, y * z) \in r_a$ could be proved similarly, we see that r_a is a congruence of G_a .

Since $s_G \subseteq t_a \subseteq \ker(g)$, there exist natural projections $p: G \rightarrow G/s_G, q: G/s_G \rightarrow G/t_a$ and a homomorphism $k: G/t_a \rightarrow S$ such that $g = kqp$. Since $r_a \subseteq \ker(g_a)$, we also have the natural projection $w: G_a \rightarrow G_a/r_a$ and a homomorphism $v: G_a/r_a \rightarrow S$ such

that $g_a = vw$. Finally, define a mapping $h: G \rightarrow G_a$ by $h(x) = x$ for $x \in H_a$ and $h(x) = g_a^{-1}(b)$ for $x \in H_b$ with $b \neq a$. This mapping h is a homomorphism of G onto G_a and we have the following commutative diagram:

$$\begin{array}{ccccc} G/s_G & \xrightarrow{q} & G/t_a & \xrightarrow{k} & S \\ \uparrow p & & & & \uparrow v \\ G & \xrightarrow{h} & G_a & \xrightarrow{w} & G_a/r_a \end{array}$$

It is easy to verify that $\ker(wh) = t_a = \ker(qp)$, from which it follows that the groupoids G/t_a and G_a/r_a are isomorphic. Since G/t_a is a homomorphic image of G/s_G , it is a semigroup and it implies that G_a/r_a is a semigroup, too. Moreover, we get $r_a = s_{G_a} = \ker(g_a)$ and then $s_G \cap (H_a \times H_a) = H_a \times H_a$. This yields $H_a \times H_a \subseteq s_G$ for every $a \in S$ and therefore $s_G = \ker(g)$, completing the proof. \square

XII.5 Semigroups with local units

5.1 Lemma. *Let M be a non-empty set. Then there exists a mapping t of M onto M such that for all $x, y \in M$ there are positive integers m, n with $t^m(x) = t^n(y)$.*

Proof. If M is finite, we can take a full cycle on M . Now let M be infinite. Denote by B the set of the mappings f of M into the set of positive integers, such that $f(x) = 1$ for all but finitely many elements $x \in M$. Define a mapping $t: B \rightarrow B$ by $t(f)(x) = 1$ if $f(x) = 1$ and $t(f)(x) = f(x) - 1$ if $f(x) \geq 2$. Clearly, t has the desired property with respect to the set B , which has the same cardinality as M . \square

5.2 Lemma. *Let S be a semigroup, $a \in \text{Lu}(S)$ and let f be a cardinal function on S such that $f(b) = 1$ for every $b \in S - \{a\}$. Then f is representable.*

Proof. Let M be a set with $\text{Card}(M) = f(a)$ and $S \cap M = \emptyset$; let t be a mapping of M onto M as given in 5.1. Put $R = S - \{a\}$ and $G = R \cup M$. Define a mapping g of G onto S by $g(x) = x$ for $x \in R$ and $g(x) = a$ for $x \in M$.

Consider first the case $aa \neq a$. Since $a \in \text{Lu}(S)$, we have $a = ea$ for some $e \in S$. Define a binary operation $*$ on G as follows.

- (1) $e * x = (ee) * x = t(x)$ for every $x \in M$;
- (2) $b * c = bc$ for all $b, c \in R$ with $bc \neq a$;
- (3) $b * c$ is any element of M if $b, c \in R$ and $bc = a$;
- (4) $b * x = ba$ if $b \in R, x \in M$ and $ba \neq a$;
- (5) $b * x$ is any element of M if $b \in R, x \in M, b \notin \{e, ee\}$ and $ba = a$;
- (6) $x * b = ab$ if $b \in R, x \in M$ and $ab \neq a$;
- (7) $x * b$ is any element of M if $b \in R, x \in M$ and $ab = a$;
- (8) $x * y = aa \in R$ for any $x, y \in M$.

This makes G a groupoid. Evidently, g is a homomorphism of G onto S . It remains to show that $\ker(g) = s_G$. Put $s = s_G \cap (M \times M)$. If $(x, y) \in s$, then $(t(x), t(y)) = (e * x, e * y) \in s$, which means that s is a congruence of the algebra (M, t) with one unary operation t . If $x \in M$ then, by the definition of s_G , $(e * (e * x), (e * e) * x) \in s_G$. But $e * (e * x) = t^2(x)$ and $(e * e) * x = t(x)$, hence $(t^2(x), t(x)) \in s$. In fact, $(t^n(x), t(x)) \in s$ for any positive integer n . Let $(u, v) \in M \times M$. There exist $w, z \in M$ such that $u = t(w)$ and $v = t(z)$. By 5.1, there also exist positive integers m, n with $t^m(w) = t^n(z)$. On the other hand, $(t^m(w), t(w)) \in s$ and $(t^n(z), t(z)) \in s$. Consequently, $(t(w), t(z)) = (u, v) \in s$. We have proved that $s = M \times M$ and then $M \times M \subseteq s_G$ and $s_g = \ker(g)$.

Now consider the case $aa = a$. Choose an element $w \in M$ and define a binary operation $*$ on G as follows.

- (1) $x * y = w$ for all $x, y \in M$ with $y \neq w$;
- (2) $x * w = x$ for every $x \in M$;
- (3) $b * c = bc$ for all $b, c \in R$ with $bc \neq a$;
- (4) $b * c = w$ for all $b, c \in R$ with $bc = a$;
- (5) $b * x = ba$ for all $b \in R$ and $x \in M$ with $ba \neq a$;
- (6) $b * x = w$ for all $b \in R$ and $x \in M$ with $ba = a$;
- (7) $x * b = ab$ for all $b \in R$ and $x \in M$ with $ab \neq a$;
- (8) $x * b = w$ for all $b \in R$ and $x \in M$ with $ab = a$.

This makes G a groupoid. Evidently, g is a homomorphism of G onto S . Let $(x, y) \in M \times M$. Then $(x * (w * x), (x * w) * x) \in s_G$, i.e., $(x, w) \in s_G$. Similarly, $(y, w) \in s_G$ and hence $(x, y) \in s_G$. We have proved $\ker(g) = s_G$ also in this case, completing thus the proof. \square

5.3 Theorem. *Let S be a semigroup. The following two conditions are equivalent:*

- (1) *Every cardinal function on S is representable.*
- (2) $S = \text{Lu}(S) \cup \text{Ru}(S)$.

Proof. Suppose that (1) is satisfied but there exists an element $a \in S - (\text{Lu}(S) \cup \text{Ru}(S))$. By 2.1, $S = S^2$. Put $\kappa = \text{Card}(M_a)$ and take a cardinal function f on S such that $f(a) > \kappa$ and $f(b) = 1$ for every $b \in S - \{a\}$. By 2.4, we have $\kappa < f(a) \leq \sum_{(b, c) \in M_a} f(b)f(c) = \sum_{M_a} 1$, a contradiction.

For the converse implication, just combine Theorem 4.1 with Lemma 5.2 and its dual. \square

5.4 Remark. The following semigroups belong to the class of semigroups S satisfying $S = \text{Lu}(S) \cup \text{Ru}(S)$:

- (1) semigroups with a left (or right) neutral element;
- (2) groups;
- (3) regular semigroups;

- (4) idempotent semigroups;
- (5) finite commutative semigroups S with $S = S^2$ (see 1.3);
- (6) at most four-element semigroups S with $S = S^2$ (see 1.5).

XII.6 An example

6.1 Example. Consider the five-element semigroup T with elements $0, a, b, c, d$ from Example 1.4. We will see that a cardinal function f on T is representable if and only if (R) is satisfied, i.e., if and only if $f(a) \leq f(b)f(c)$.

The necessity is settled by 2.6. Let $f(a) \leq f(b)f(c)$. Put $G = P \cup A \cup B \cup C \cup D$ where P, A, B, C, D are five pairwise disjoint sets with $\text{Card}(P) = f(0)$, $\text{Card}(A) = f(a)$, $\text{Card}(B) = f(b)$, $\text{Card}(C) = f(c)$ and $\text{Card}(D) = f(d)$. By 5.1, there exist a mapping p of B onto B and a mapping q of C onto C such that for all $x, y \in B$ there are positive integers m, n with $p^m(x) = p^n(y)$ and for all $x, y \in C$ there are positive integers m, n with $q^m(x) = q^n(y)$. From $f(a) \leq f(b)$ it follows that there exists a mapping h of $B \times C$ onto A . Take two elements $z \in P$ and $w \in D$ arbitrarily. Define a multiplication on G as follows.

- (1) $xy = yx = z$ for all $x \in P$ and $y \in A \cup B \cup C \cup D$;
- (2) $xy = z$ for all $x, y \in A \cup B$;
- (3) $xy = yx = z$ for all $x \in A$ and $y \in C \cup D$;
- (4) $xy = z$ for all $x \in C$ and $y \in B \cup C \cup D$;
- (5) $xy = z$ for all $x \in D$ and $y \in B$;
- (6) $xy = z$ for all $x, y \in P$ with $y \neq z$;
- (7) $xz = x$ for all $x \in P$;
- (8) $xy = w$ for all $x, y \in D$ with $y \neq w$;
- (9) $xw = x$ for all $x \in D$;
- (10) $xy = p(x)$ for all $x \in B$ and $y \in D$;
- (11) $xy = q(y)$ for all $x \in D$ and $y \in C$;
- (12) $xy = h(x, y)$ for all $x \in B$ and $y \in C$.

Define a mapping $g: G \rightarrow T$ by $g(P) = 0$, $g(A) = a$, $g(B) = b$, $g(C) = c$ and $g(D) = d$. It is easy to check that g is a homomorphism. Now, we have to show that $\ker(g) = s_G$.

We have $(x \cdot xx, xx \cdot x) \in s_G$ for any $x \in P$, so that $x \cdot xx = xz = x$ and $xx \cdot x = zx = z$ yield $(x, z) \in s_G$; we get $P \times P \subseteq s_G$. The inclusion $D \times D \subseteq s_G$ can be proved in the same way. The inclusions $B \times B \subseteq s_G$ and $C \times C \subseteq s_G$ can be proved as in 5.2, with p and q , respectively, playing the role of t . Finally, if $(x, y) \in B \times B$ and $(u, v) \in C \times C$, then $(x, y) \in s_G$ and $(u, v) \in s_G$, so that $(h(x, u), h(y, v)) = (xu, yv) \in s_G$; we see that $A \times A \subseteq s_G$. We conclude that $\ker(g) = s_G$.

XII.7 Representability of “small” cardinal functions

7.1 Proposition. *Let S be a semigroup, a be an element of S and f be the cardinal function on S with $f(a) = 2$ and $f(b) = 1$ for every $b \in S - \{a\}$. Then f is representable if and only if at least one of the following two conditions is satisfied:*

- (1) $a \in \text{Lu}(S) \cup \text{Ru}(S)$;
- (2) *there exist elements $x, y, z \in S$ such that $xyz = a$ and either $xy \neq x$ or $yz \neq z$.*

Proof. If (1) is satisfied, the result follows from 5.2 and its dual. Let $a \notin \text{Lu}(S) \cup \text{Ru}(S)$ and $a = xyz$, where $xy \neq x$. Take an element $e \notin S$, put $G = S \cup \{e\}$ and define a binary operation $*$ on G in the following way.

- (i) $u * v = uv$ for all $u, v \in S$ with $uv \neq a$;
- (ii) $u * v = a$ for all $u, v \in S$ with $uv = a$ and either $u \neq x$ or $v \neq yz$;
- (iii) $x * (yz) = e$;
- (iv) $e * u = a * u$ and $u * e = u * a$ for every $u \in S$;
- (v) $e * e = a * a$.

Clearly, the mapping $g: G \rightarrow S$, defined by $g(e) = a$ and $g(x) = x$ for every $x \in S$, is a homomorphism of G onto S and $\ker(g) = s_G$. We can proceed similarly if $a = xyz$ and $xy \neq x$.

Now, we are going to prove the converse. Suppose that neither (1) nor (2) is satisfied, but there exists a groupoid G and a homomorphism g of G onto S such that $\ker(g) = s_G$, $\text{Card}(g^{-1}(a)) = 2$ and $\text{Card}(g^{-1}(b)) = 1$ for every $b \neq a$. Let $u, v, w \in G$; put $x = uv$ and $y = vw$. If $g(uy) \neq a$, then also $g(xw) \neq a$, and hence $uy = xw$. Let $g(uy) = a$. Then $g(xw) = a$ and we have $a = g(u)g(v)g(w)$. Since (2) is not satisfied, $g(u) = g(u)g(v) = g(x)$ and $g(w) = g(v)g(w) = g(y)$. Since (1) is not satisfied, $g(u) \neq a \neq g(w)$, yielding $u = x$ and $w = y$. But then $u \cdot vw = uy = uw = xw = uv \cdot w$. We see that G is a semigroup, a contradiction. \square

7.2 Proposition. *Let S be a semigroup such that for every element $a \in S^3 - (\text{Lu}(S) \cup \text{Ru}(S))$ there exist elements $x, y, z \in S$ with $a = xyz$ and $(x, yz) \neq (xy, z)$. (In the notation introduced in Section 2, this can be expressed by saying that the equivalence E_a on M_a is not identical.) If f is a cardinal function on S such that $f(a) \leq 2$ for all $a \in S$, then f is representable if and only if $f(b) = 1$ for every $b \in S - S^3$.*

Proof. Just combine 2.1, 4.1 and 7.1. \square

7.3 Corollary. *Let S be a commutative semigroup and f be a cardinal function on S such that $f(a) \leq 2$ for all $a \in S$. Then f is representable if and only if $f(a) = 1$ for every $a \in S - S^3$. \square*

XII.8 Some constructions of quasigroups and loops

Let G be a group, H be an abelian group and g a mapping of $G \times G$ into H . Then $Q(G, H, g)$ denotes the groupoid $Q(*)$ with the underlying set $Q = G \times H$ and the operation $*$ defined by $(x, a) * (y, b) = (xy, a + b + g(x, y))$ for all $x, y \in G$ and $a, b \in H$. Further, define a relation t on Q by $((x, a), (y, b)) \in t$ if and only if $x = y$. For a subset L of H , define a relation t_L on Q by $((x, a), (y, b)) \in t_L$ if and only if $x = y$ and $a - b \in L$. Denote by K the subgroup of H generated by all the elements $g(y, z) + g(x, yz) - g(x, y) - g(xy, z)$, for $x, y, z \in G$.

8.1 Lemma.

- (1) $Q(*)$ is a quasigroup, t is a congruence of $Q(*)$, the factor $Q(*)/t$ is isomorphic to G and every block of t has the same cardinality, equal to $\text{Card}(H)$.
- (2) The quasigroup $Q(*)$ is commutative if and only if G is commutative and $g(x, y) = g(y, x)$ for all $x, y \in G$.
- (3) $Q(*)$ is a loop if and only if $g(1, x) = g(y, 1)$ for all $x, y \in G$.
- (4) $Q(*)$ is a group if and only if $g(x, y) + g(xy, z) = g(y, z) + g(x, yz)$ for all $x, y, z \in G$.
- (5) t_L is an equivalence if and only if L is a subgroup of H . In that case, t_L is a cancellative congruence of $Q(*)$.
- (6) If L is a subgroup of H , then $Q(*)/t_L$ is a group if and only if $K \subseteq L$.
- (7) If r is a congruence of $Q(*)$ with $r \subseteq t$, then $r = t_L$ for a subgroup L of H .
- (8) $t = s_{Q(*)}$ if and only if $K = H$. In that case, $\sigma(Q*) = \text{Card}(H)$.
- (9) If G contains at least three elements and H is cyclic, then the mapping g can be chosen in such a way that $K = H$ and $g(x, y) = g(y, x)$ and $g(1, x) = g(y, 1)$ for all $x, y \in G$.

Proof. (1) through (6) are easy. (7) Let $((x, a), (x, b)) \in r$, $y \in G$, $c, d \in H$, $c - d = a - b$. Then $(yx^{-1}, g(yx^{-1}, x)) * (x, a) = (y, b)$ and $(yx^{-1}, g(yx^{-1}, x)) * (x, b) = (y, c)$, so that $((y, a), (y, b)) \in r$. Further, $(1, c - a - g(1, x)) * (x, a) = (x, c)$ and $(1, c - a - g(1, x)) * (x, b) = (x, d)$, so that $((x, c), (x, d)) \in r$ and then also $((y, c), (y, d)) \in r$. From this we see that $r = t_L$, where $L = \{a - b : ((x, a), (x, b)) \in r\}$. By (5), L is a subgroup of H .

(8) This follows easily from (6) and (7).

(9) Let $u, v \in G$ be such that the elements $1, u, v$ are pairwise different and let a be a generator of H . It is easy to see that we can define g in such a way that $g(x, x) = g(y, x)$, $g(1, x) = g(y, 1)$, $g(u, v) = a$, $g(u, uv) = g(u^2, v)$ and $g(u, u) = 0$. Then $g(u, v) + g(u, uv) - g(u, u) - g(u^2, v) = a$, and so $K = H$. \square

8.2 Proposition. Let G be a group containing at least three elements and let $1 \leq \kappa \leq \aleph_0$ be a cardinal number. Then there exists a loop Q such that $\sigma(Q) = \kappa$ and Q/s_Q is isomorphic to G . Moreover, Q can be chosen commutative, provided that G is commutative.

Proof. Some of the assertions in Lemma 8.1 may turn out to be useful. \square

8.3 Remark. Let P be a loop such that $\sigma(P) = 2$. Put $G = P/s_P$ and, for every $x \in G$, choose an element $w_x \in x$; the choice should be such that $w_1 = 1$. Let $\{1, a\}$ be the block of s_P containing the unit of P . Then, clearly, $G = \{\{w_x, aw_x\} : x \in G\}$; the element a belongs to the center of P and $a^2 = 1$. Further, define a mapping g of $G \times G$ into the two-element cyclic group $\mathbf{Z}_2 = \{0, 1\}$ by $g(x, y) = 0$ if $w_x w_y = w_{xy}$ and $g(x, y) = 1$ otherwise. Then $g(x, 1) = g(1, y)$ for all $x, y \in G$. Moreover, if P is commutative, then $g(x, y) = g(y, x)$ for all $x, y \in G$. Finally, define a mapping $f : P \rightarrow Q(G, \mathbf{Z}_2, g)$ by $f(w_x) = (x, 0)$ and $f(aw_x) = (x, 1)$ for every $x \in G$. It is easy to check that f is an isomorphism of P onto $Q(G, \mathbf{Z}_2, g)$.

8.4 Remark. There exists no loop P with $\sigma(P) = 2$ and $\text{Card}(P/s_P) = 2$. Indeed, every four-element loop is a group. On the other hand, consider the four-element commutative quasigroup Q with the following multiplication table:

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

One can easily check that $\sigma(Q) = 2$ and Q/s_Q is isomorphic to \mathbf{Z}_2 .

8.5 Lemma. Let $G(+)$ be an abelian group of order $n \geq 5$ such that the transformations $x \mapsto 2x$ and $x \mapsto 3x$ are permutations of G (i.e., G is uniquely 2- and 3-divisible). Take an element $e \notin G$, put $P = G \cup \{e\}$ and define multiplication on P by

$$xy = \begin{cases} (x + y)/2 & \text{for } x, y \in G, x \neq y, \\ e & \text{for } x = y, \\ x & \text{for } y = e, \\ y & \text{or } x = e. \end{cases}$$

Then P is a simple, commutative and nonassociative loop of order $n + 1$.

Proof. It is easy to check that P is a commutative loop of order $n + 1$; it is nonassociative, because $n \geq 5$. Let r be a congruence of P and put $K = \{x \in P : (x, e) \in r\}$. If $K = \{e\}$, then $r = \text{id}_P$. Assume $K \neq \{e\}$ and take an element $a \in K - \{e\}$. Then for every element $b \in G - \{a\}$ we have $((a + b)/2, b) \in r$ and $((a + 3b)/4, e) \in r$, so that $(a + 3b)/4 \in K$. From this it is easy to see that $K = P$ and $r = P \times P$. \square

8.6 Lemma. For every cardinal number $\kappa \geq 1$, $\kappa \neq 4$, there exists a simple commutative loop P of order κ . If $\kappa \geq 6$, then P can be chosen nonassociative.

Proof. It follows from Griffin [8] and Lemma 8.5. \square

8.7 Proposition. *Let G be a group and $\kappa \geq 6$ be a cardinal number. Then there exists a loop Q such that $\sigma(Q) = \kappa$ and Q/s_Q is isomorphic to G . Moreover, if G is abelian, then Q can be chosen commutative.*

Proof. By 8.6, there is a simple commutative and nonassociative loop P of order κ . It suffices to put $Q = G \times P$. \square

XII.9 Quasigroups with subquasigroups of index 2

Let P be a non-empty set and $*$, \circ , Δ , ∇ be four quasigroup operations on P . Put $Q = P \times \{0, 1\}$ and define multiplication on Q as follows:

$$\begin{aligned}(x, 0)(y, 0) &= (x * y, 0); \\ (x, 1)(y, 1) &= (x \circ y, 0); \\ (x, 0)(y, 1) &= (x \Delta y, 1); \\ (x, 1)(y, 0) &= (x \nabla y, 1)\end{aligned}$$

for all $x, y \in P$. The groupoid just obtained will be denoted by $Q(P, *, \circ, \Delta, \nabla)$. Put $R = \{(x, 0) : x \in P\}$.

9.1 Lemma.

- (1) Q is a quasigroup, R is a normal subquasigroup of Q , R is isomorphic to $P(*)$ and Q/R is a two-element group.
- (2) Q is commutative if and only if the operations $*$ and \circ are commutative and $x \Delta y = y \nabla x$ for all $x, y \in P$.
- (3) Let $e \in P$ and $a \in \{0, 1\}$. Then (e, a) is a unit of Q if and only if $a = 0$, e is a unit of $P(*)$, e is a left unit of $P(\Delta)$ and e is a right unit of $P(\nabla)$.
- (4) Q is a group if and only if $P(*)$ is a group and $x \Delta (y \Delta z) = (x * y) \Delta z$, $x \Delta (y \nabla z) = (x \Delta y) \nabla z$, $x \nabla (y * z) = (x \nabla y) \nabla z$, $x * (y \circ z) = (x \Delta y) \circ z$, $x \circ (y \nabla z) = (x \circ y) * z$, $x \circ (y \Delta z) = (x \nabla y) \circ z$ and $x \nabla (y \circ z) = (x \circ y) \Delta z$ for all $x, y, z \in P$.

Proof. It is easy. \square

Define a relation t on Q by $((x, a), (y, b)) \in t$ if and only if $a = b$. Then t is a normal congruence of Q and Q/t is isomorphic to \mathbf{Z}_2 .

Let r, s be two equivalences defined on P . Then we define a relation $t(r, s)$ on Q by $((x, a), (y, b)) \in t(r, s)$ if and only if either $a = b = 0$ and $(x, y) \in r$ or else $a = b = 1$ and $(x, y) \in s$. Consider the following two conditions:

- (P1) If $x, y, z \in P$ and $(x, y) \in r$, then $(z \nabla x, z \nabla y) \in s$ and $(x \Delta z, y \Delta z) \in s$;
- (P2) If $x, y, z \in P$ and $(x, y) \in s$, then $(z \circ x, z \circ y) \in r$, $(x \circ z, y \circ z) \in r$, $(z \Delta x, z \Delta y) \in s$ and $(x \nabla z, y \nabla z) \in s$.

9.2 Lemma.

- (1) $t(r, s)$ is an equivalence contained in t and $t(r, s)$ is a congruence of Q if and only if r is a congruence of $P(*)$ and the conditions (P1) and (P2) are satisfied.
- (2) Suppose that (P1) is satisfied and either $P(\Delta)$ (resp. $P(\nabla)$) possesses a right (resp. left) unit or s is a right (resp. left) cancellative relation on $P(\Delta)$ (resp. $P(\nabla)$). Then $r \subseteq s$.
- (3) Suppose that (P2) is satisfied and that r is a left or a right cancellative relation on $P(\circ)$. Then $s \subseteq r$.
- (4) Suppose that (P2) is satisfied and $r \subseteq s$. Then both r and s are congruences of $P(\circ)$.
- (5) Suppose that (P2) is satisfied and $P(\Delta)$ (resp. $P(\nabla)$) is commutative. Then s is a congruence of $P(\Delta)$ (resp. $P(\nabla)$).

Proof. It is easy. \square

9.3 Lemma. Suppose that $t(r, s)$ is a congruence of Q . Then the corresponding factor of Q is a group if and only if $P(*)/r$ is a group and $((x * y) \Delta z, x \Delta (y \Delta z)) \in s$, $((x \Delta y) \nabla z, x \Delta (y \nabla z)) \in s$, $((x \nabla y) \nabla z, x \nabla (y * z)) \in s$, $((x \circ y) \Delta z, x \nabla (y \circ z)) \in s$, $((x \nabla y) \circ z, x \circ (y \Delta z)) \in r$, $((x \Delta y) \circ z, x * (y \circ z)) \in r$, $((x \circ y) * z, x \circ (y \nabla z)) \in r$ for all $x, y, z \in P$.

Proof. It is easy. \square

9.4 Lemma. Suppose that $t(r, s)$ is a congruence of Q and the corresponding factor is a group. Let $e \in P$.

- (1) If e is a right unit of $P(\Delta)$, then $(x * x, x \Delta y) \in s$ for all $x, y \in P$.
- (2) If e is a left unit of $P(\nabla)$, then $(x * y, x \nabla y) \in s$ for all $x, y \in P$.
- (3) If e is a right unit of both $P(*)$ and $P(\Delta)$ and a left unit of $P(\nabla)$, and if $e \circ e = e$, then $(x * y, x \circ y) \in r$ for all $x, y \in P$.

Proof. Use 9.3. \square

9.5 Lemma. Suppose that $t(r, r)$ is a congruence of Q , the corresponding factor is a group and $P(*)$, $P(\Delta)$, $P(\nabla)$ are commutative loops with the same unit $e = e \circ e$. Then $r = s$ is a cancellative congruence of all the four quasigroups $P(*)$, $P(\circ)$, $P(\Delta)$ and $P(\nabla)$ and $(x * y, x \circ y) \in r$ and $(x \Delta y, x \nabla y) \in r$ for all $x, y \in P$.

Proof. Apply the preceding lemmas. \square

9.6 Lemma. Let p be a congruence of Q with $p \subseteq t$. Then there exist a congruence r of $P(*)$ and an equivalence s on P such that the conditions (P1) and (P2) are satisfied and $p = t(r, s)$.

Proof. Define r and s as follows: $(x, y) \in r$ if and only if $((x, 0), (y, 0)) \in p$ and $(x, y) \in s$ if and only if $((x, 1), (y, 1)) \in p$. \square

9.7 Lemma. *Suppose that Q is not associative and that the quasigroup $P(*)$ is simple. Then $t = s_Q$ and $\sigma(Q) = \text{Card}(P)$.*

Proof. We have $p = s_Q \subseteq t$ and $p = t(r, s)$ by 9.6. If $r = P \times P$, then $s = P \times P$ by (P1), and therefore $p = t$. If $r = \text{id}_P$, then $s = \text{id}_P$ by (P2) and Q is a group, a contradiction. \square

9.8 Lemma. *Let P be a finite set with $n \geq 4$ elements and let $0 \in P$. Then there exist two cyclic groups $P(*)$ and $P(\circ)$ such that 0 is the neutral element of both $P(*)$ and $P(\circ)$ and $x * y \neq x \circ y$ for some $x, y \in P$. Moreover, 0 and P are the only common subgroups of $P(*)$ and $P(\circ)$.*

Proof. Let $n = p_1^{k_1} \dots p_m^{k_m}$ where $m, k_1, \dots, k_m \geq 1$ and $p_1 < p_2 < \dots < p_m$ are primes. Further, let $P(*)$ be an arbitrary cyclic group such that 0 is its zero element. If n is a prime, then the result is clear. Suppose that n is composed and let $a_1, \dots, a_m \in P(*)$ be some elements of orders p_1, \dots, p_m , respectively. It is easy to construct a cyclic group $P(\circ)$ such that 0 is its zero and each of the elements a_1, \dots, a_m is a generator of $P(\circ)$. Now, if R is a nonzero subgroup of both $P(*)$ and $P(\circ)$, then $a_i \in R$ for at least one $1 \leq i \leq m$, and hence $R = P$. Finally, $P(*)$ contains a nonzero proper subgroup, and so $P(*) \neq P(\circ)$. \square

9.9 Remark. Let $Q(*)$ be a quasigroup containing a normal subquasigroup $P(*)$ of index 2. Let $a \in Q, a \notin P$. Then Q is formed by the elements x and $x * x$, with x running over P , and we can define three binary operations \circ, \triangle and ∇ on P as follows:

$$\begin{aligned} x \circ y &= (a * x) * (a * y); \\ x \triangle y &= z, \text{ where } x * (a * y) = a * z; \\ x \nabla y &= z, \text{ where } (a * x) * y = a * z \end{aligned}$$

for all $x, y \in P$. It is easy to see that $P(\circ), P(\triangle)$ and $P(\nabla)$ are quasigroups and that $Q(*)$ is isomorphic to $Q(P, *, \circ, \triangle, \nabla)$ (define $f: Q(P, *, \circ, \triangle, \nabla) \rightarrow Q(*)$ by $f(x, 0) = x$ and $f(x, 1) = a * x$).

9.10 Proposition. *Let $\kappa \geq 1, \kappa \neq 2$ be a cardinal number. Then there exists a commutative loop Q such that $\sigma(Q) = \kappa$ and Q/s_Q is isomorphic to \mathbf{Z}_2 .*

Proof. Let $4 \leq \kappa < \aleph_0$. By 9.8, there exist two different cyclic group $P(*)$ and $P(\circ)$ with the same underlying set P , $\text{Card}(P) = \kappa$, with the same zero element 0 and without nontrivial common subgroups. Consider the quasigroup $Q = Q(P, *, \circ, *, *)$. By 9.1, Q is a commutative loop. Put $s = s_Q$. We have $s \subseteq t$ and $s = t(r, r)$ for a congruence r of both $P(\circ)$ and $P(*)$ (see 9.5 and 9.6) such that $(x * y, x \circ y) \in r$ for all $x, y \in P$. Put $K = \{x \in P : (x, 0) \in r\}$. Then K is a subgroup of both $P(*)$ and $P(\circ)$. If $K = P$, then $r = P \times P$ and $s = t$. If $K = \{0\}$, then $r = \text{id}_P$ and $x * y = x \circ y$ for all $x, y \in P$, a contradiction.

Let $\kappa \neq 2, 4$ and let $P(*)$ be an abelian group of order κ and with a zero element 0. It is easy to see that there exists a simple commutative quasigroup $P(\circ)$ such that $0 \circ 0 = 0$ and either $\kappa = 1$ or $P(\circ)$ is not associative. Now, put $Q = Q(P, *, \circ, *, *)$ and $s = s_Q$. Then $s = t(r, r)$ for a congruence r of both $P(*)$ and $P(\circ)$ such that $(x * y, x \circ y) \in r$ for all $x, y \in P$. If $r = P \times P$, then $s = t$. If $r \neq P \times P$, then $\kappa \geq 3$, $r = \text{id}_P$ and $P(*) = P(\circ)$, a contradiction. \square

XII.10 Representations of cardinal functions on groups by quasigroups and loops

10.1 Proposition. *Let G be a group of order β and let $\alpha \geq 1$ be a cardinal number. Then, except for the cases listed below, there exists a loop Q such that $\sigma(Q) = \alpha$ and Q/s_Q is isomorphic to G . The exceptional cases for (α, β) are $(2, 1)$, $(2, 2)$, $(3, 1)$ and $(4, 1)$.*

Proof. If $\alpha \geq 6$, then the result is settled by 8.7. If $\alpha \neq 2$ and $\beta = 2$, then 9.10 applies. If $\alpha \leq \aleph_0$ and $\beta \geq 3$, then 8.2 takes place. The five-element loop Q with the multiplication table

Q	1	2	3	4	5
1	1	2	3	4	5
2	2	3	4	5	1
3	3	5	1	2	4
4	4	1	5	3	2
5	5	4	2	1	3

is simple and nonassociative, solving the question for $(\alpha, \beta) = (5, 1)$. The four cases for (α, β) are excluded by the fact that every at most four-element loop is associative. \square

10.2 Proposition. *Let G be an abelian group of order β and let $\alpha \geq 1$ be a cardinal number. Then, except for the cases listed below, there exists a commutative loop Q such that $\sigma(Q) = \alpha$ and Q/s_Q is isomorphic to G . The exceptional cases for (α, β) are $(2, 1)$, $(2, 2)$, $(3, 1)$, $(4, 1)$ and $(5, 1)$.*

Proof. Similar to that of 10.1. (Every commutative loop of order 5 is a group.) \square

10.3 Proposition. *Let G be a (commutative) group of order β and $\alpha \geq 1$ be a cardinal number. Then, in all cases except for $(\alpha, \beta) = (2, 1)$, there exists a (commutative) quasigroup Q such that $\sigma(Q) = \alpha$ and Q/s_Q is isomorphic to G .*

Proof. Similar to that of 10.1. (See 8.4; it is easy to construct simple nonassociative and commutative quasigroups of orders 3, 4 and 5.) \square

XII.11 Comments and open problems

The investigation of representability of cardinal-valued functions on semigroups by groupoids was initiated by P. Corsini in [3] (see also [5] and [6]). His results were generalized and completed in [7], [9] and [14]. The case of cardinal functions on groups was studied in [12].

According to Theorem 2.3, the condition (R) is necessary for a cardinal function f on a given semigroup S to be representable. We have seen that for some classes of semigroups, the condition is also sufficient. However, we do not know if this is true in general. The idea to Section 2 came from [9], where condition (R') was formulated. Section 2 is a correction to [9].

References

- [1] CORSINI P. *Hypergroupes d'associativité des quasigroupes mediaux*, Atti del Convegno su "Sistemi Binari e loro Applicazioni," Taormina 1978.
- [2] CORSINI P., ROMEO G. *Hypergroupes completes et τ -groupoïdes*, Atti del Convegno su "Sistemi Binari e loro Applicazioni," Taormina 1978.
- [3] CORSINI P. *Sur les semi-hypergroupes*, Atti Soc. Pelor. Sci. M. F. N. (1979).
- [4] CORSINI P. *Sur les semi-hypergroupes completes et les τ -groupoïdes*, Atti Soc. Pelor. Sci. M.F.N. (1980).
- [5] CORSINI P. *Prolegomeni alla teoria degli ipergruppi*, Quaderni dell'istituto di matematica, informatica e sistematica, Università di Udine, Udine 1986.
- [6] CORSINI P. *Prolegomena of hypergroup theory*, Aviani, Udine 1984.
- [7] DRBOHLAV K., KEPKA T., NĚMEC P. *Associativity semihypergroups and related problems*, Atti del Convegno su "Ipergruppi, altre strutture multivoche e loro applicazioni," Udine (1985), 75–86.
- [8] GRIFFIN H. *The abelian quasigroups*, Amer. J. Math. **62** (1940), 725–737.
- [9] JEŽEK J. *On representable mappings of semigroups into cardinals*, Rivista di Matematica Pura ed Applicata **6** (1990), 99–103.
- [10] KEPKA T. *Distributive τ -groupoids*, Atti Soc. Pelor. Sci. F.M.N. **27** (1981), 19–25.
- [11] KEPKA T. *A note on τ -groupoids*, Atti Soc. Pelor. Sci. F.M.N. **27** (1981), 27–34.
- [12] KEPKA T. *A note on the associativity hypergroups of quasigroups and loops*, Atti Soc. Pelor. Sci. F.M.N. **27** (1981), 35–46.
- [13] KEPKA T. *A note on representable mappings*, Rivista di Matem. Pura ed Appl. **9** (1991), 135–136.
- [14] KEPKA T., NĚMEC P., NIEMENMAA, M. *On representable pairs*, Annales Acad. Sci. Fennicae, Ser. A.I. Mathem. **13** (1988), 71–88.
- [15] KOSKAS M. *Groupoïdes, demi-hypergroupes et hypergroupes*, J. Math. pures et appl. **49** (1970), 155–192.