Submonoids of groups, and group-representability of restricted relation algebras

George M. Bergman

To the memory of Bjarni Jónsson

Abstract. Marek Kuczma asked in 1980 whether for every positive integer n, there exists a subsemigroup M of a group G, such that G is equal to the n-fold product $M\,M^{-1}M\,M^{-1}\dots M^{(-1)^{n-1}}$, but not to any proper initial subproduct of this product. We answer his question affirmatively, and prove a more general result on representing a certain sort of relation algebra by a family of subsets of a group. We also sketch several variants of the latter result.

1. Introduction

M. Kuczma [4, Problem P190, p. 304] raised the question quoted in the Abstract for general n, and for $n = 3$ in particular. The $n = 3$ case was answered affirmatively by an example of W. Benz [4, Remark P190S1, p. 305]. We sketch in Section 2 a construction that works for all n, then prove in Section 5 a general result, Theorem 4, from which, as we show in Section 6.1, the asserted behavior of that construction follows.

In Section 7 we look at some variants (and further possible variants) of Theorem 4. In particular, in Section 7.5 we note a class of operations on binary relations, described in B. Jónsson's survey paper [2], which that theorem can be extended to cover.

2010 *Mathematics Subject Classification*: Primary: 03G15; Secondary: 06A06, 20M20.

Key words and phrases: monoid, group, relation algebra, Hilbert's Hotel.

Work partly supported by NSF contract MCS 80-02317. (The author apologizes for the long delay in publishing this work, most of which was done in 1981.)

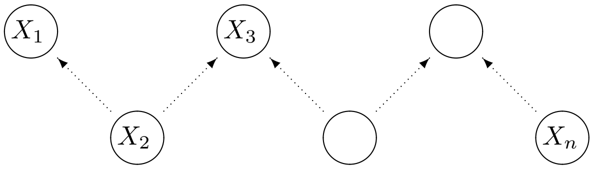
http://arxiv.org/abs/1702.06088 . After publication of this note, updates, errata, related references etc., if found, will be recorded at http://math.berkeley.edu/~gbergman/papers/ .

2. Sketch of the construction answering Kuczma's question

If G is a group of permutations of a set X, we shall write elements of G to the right of elements of X, and compose them accordingly.

Given a positive integer n, let $X_1, \dots, X_n$ be disjoint *infinite* sets, let $X = X_1 \cup \ldots \cup X_n$, and let G be the group of those permutations g of X such that for all but finitely many $x \in X$, the element xg lies in the same set X_i as does x. Note that given any *finite* set of elements of X, and any assignment of a destination-set X_i for each of them, one can construct a $g \in G$ which realizes these movements, and keeps all other elements in their original sets. (If the number of newcomers assigned to some X_i is not equal to the number of elements specified to leave X_i, then infinitely many elements can be moved within X_i, as in "Hilbert's Hotel" [1, p. 17], to accommodate these relocations.)

Now let $M \subseteq G$ be the submonoid consisting of those g which involve no movement of elements from one X_i to a different one, except for transitions from even-indexed sets X_{2i} to *adjacent* odd-indexed sets, X_{2i-1} and X_{2i+1}, as suggested by the picture (1) below. (For concreteness, n is there assumed even.) Dotted arrows show directed paths along which finitely many elements may move.



(1)

Clearly, M^{-1} is the submonoid of G corresponding to the same diagram with the dotted arrows reversed.

One finds that using n elements of M and M^{-1}, acting alternately, starting with an element of M, one can achieve the action of any element of G; but that one cannot in general represent such an element using a shorter product of this sort. The reader might think this through now, or wait for the details in Sections 4-6. In convincing oneself that n factors do suffice, it can be helpful to think of first finding a sequence of n elements, alternately from M and from M^{-1}, that together bring every element into the correct X_i, then modifying the last of these factors by a permutation which preserves each of the sets X_i, and simply rearranges elements within those sets.

One may ask why $n-1$ factors $MM^{-1}\ldots$ do not suffice, since there are only $n-1$ links in (1). The reason is that if an element of X_1 is to travel to X_n, it has to wait for the second factor, M^{-1}, to begin this journey, since the initial factor M does not move elements out of X_1. (If n is odd, the same also applies to elements traveling from X_n to X_1.)

Assuming the above handwaving filled in, as will be done below, this construction answers Kuczma's question.

3. Sketch of the motivation for a more general result

The definition of M above can be thought of as based on a partial ordering $\preccurlyeq$ on the index set $\{1,\dots,n\}$, under which the only comparability relations say that each even element is less than the two adjacent odd elements (cf. (1)). The monoid M embodies this partial ordering in allowing elements to move from X_i to X_j if $i \preccurlyeq j$. The monoid M^{-1} similarly embodies the reverse partial ordering.

What do sets such as $M\,M^{-1}$ look like? Application of an element gh^{-1} $(g,h\in M)$ allows elements to move from X_i to X_j if the pair (i,j) belongs to $\{(i,j) : (\exists\, k)\ i \preccurlyeq k \succcurlyeq j\}$, the *composite* of the binary relations $\preccurlyeq$ and $\succcurlyeq$ on X. So we can think of the construction of the preceding section as starting with a binary relation $\preccurlyeq$ on the set $I=\{i,\dots,n\}$, obtaining from it a subset M of G, and applying the operations of elementwise inversion of subsets of G, and multiplication of such subsets, to get subsets of G similarly determined by various composites of the binary relations $\preccurlyeq$ and $\succcurlyeq$. The maximal binary relation, $I\times I$, is reached as a certain n-fold composite of $\preccurlyeq$ and $\succcurlyeq$, but not as a proper initial subcomposite thereof, and this turns out to imply the corresponding condition on representation of G as the product of strings of M's and M^{-1}'s of those lengths.

Not every binary relation on I determines a nonempty subset of G, since members of G by definition leave most (hence, some) elements of each X_i in X_i; so let us restrict the relations on I which we look at as defining such subsets to be reflexive, i.e., to contain the diagonal relation $\{(i,i) : i\in I\}$. Not all of the resulting subsets will be submonoids: the fact that the M discussed above is closed under multiplication is a consequence of the fact that the relation $\preccurlyeq$, a partial ordering, is transitive; but, for example, $M\,M^{-1}$, corresponding to the relation $\preccurlyeq\circ\succcurlyeq$, is not in general a submonoid.

The next two sections develop in detail the result suggested by these observations: that the system of all reflexive binary relations on any set I is mirrored in a system of subsets of a corresponding group G, in a way that respects certain operations on these two families. In Section 6.1 we verify that this implies the asserted properties of the example we started with.

4. Down to business: definitions

In the remainder of this note, we shall distinguish between an algebra A (in the sense of universal algebra) and its underlying set, which we denote $|A|$. We continue to write permutations to the right of the elements they are applied to, and to compose them accordingly. We shall similarly compose binary relations like functions written to the right of their arguments.

For I a set, logicians regard the set $|R(I)|$ of all binary relations on I, that is, all subsets $\rho\subseteq I\times I$, as the underlying set of an algebra $R(I)$ with three binary operations, two unary operations, and three zeroary operations (constants) [3] [5]. (Jónsson [2] calls the clone of operations that these generate the "classical clone", and discusses further operations; more on that in Section 7.5.) The three binary operations are setwise intersection and union, which we shall write $\cap$ and $\cup$ (also so denoted in [2], but written $\cdot$ and $+$ in [3], and $\wedge$ and $\vee$ in [5]), and composition, which we shall write $\circ$:

$$\rho\circ\sigma \;=\; \{(i,k)\in I\times I : (\exists\, j\in I)\;\; (i,j)\in\rho,\;\, (j,k)\in\sigma\,\}. \tag{2}$$

(This is written $\rho\,|\,\sigma$ in [2] and [3], and $\rho\cdot\sigma$ in [5].) The two unary operations are complementation, which we may write ${}^{c}\rho$ (but which will not come into our results; it is denoted "$\overline{\rho}$" in [2] and [3] and "ρ^{-}" in [5]), and the *converse* operation,

$$\rho^{-1} \;=\; \{(i,j)\in I\times I : (j,i)\in\rho\,\} \tag{3}$$

(denoted $\rho^{\smile}$ in [2], [3] and [5]). The three zeroary operations are the empty relation 0 (set-theoretically, $\emptyset$), the total relation 1 (set-theoretically, $I\times I$), and the *diagonal* or *identity* relation,

$$\Delta \;=\; \{(i,i) : i\in I\} \tag{4}$$

(denoted E in [2], I in [3], $\mathbf{I}$ in [5]).

Note that $\cap$, $\cup$, ^{c}, 0, and 1 are the Boolean operations on subsets of $I\times I$; so $R(I)$ is a Boolean algebra with three additional operations, $\circ$, ${}^{-1}$, and Δ.

As indicated in the preceding section, we are only interested here in *reflexive* binary relations, i.e., relations containing Δ, so the operations 0 and ^{c} will not concern us. Moreover, the construction we are interested in does not respect unions of relations: given sets X_i $(i\in I)$, the set of permutations of $X=\bigcup_{i\in I} X_i$ that allow movement of (finitely many) elements from X_i to X_j whenever $(i,j)\in\rho\cup\sigma$ may be larger than the union of the set that allows such movement only when $(i,j)\in\rho$, and the set that allows such movement only when $(i,j)\in\sigma$. Nor does our construction respect the diagonal relation Δ on I, since Δ induces, not the trivial ("identity") subgroup of G, but the subgroup of those permutations that carry each X_i into itself.

Hence we will work with the following more restricted structures.

Definition 1. For I a set, the *restricted* relation algebra on I will mean the algebra

$$r(I) \;=\; (|r(I)|,\ \cap,\ \circ,\ {}^{-1},\ 1), \tag{5}$$

where $|r(I)|$ is the set of all reflexive binary relations on I, and the four operations are defined as in the above discussion of the full relation algebra $R(I)$.

We now turn to groups. For G a group, the set of all subsets of $|G|$, furnished with certain operations, is called in [3] the *complex algebra* of G, apparently based on terminology in which a subset of a group was called a complex. Nowadays, the concepts of chain and cochain complex are the immediate associations of that word in algebra, so it seems best to introduce a different terminology. We again use the word "restricted" to signal the limitation in the sets and operations we allow.

Definition 2. For G a group (with identity element written e), the *restricted subset algebra* of G will mean the algebra

$$p(G) \ = \ \{\,|p(G)|,\ \cap,\ \cdot,\ {}^{-1},\ |G|\,\}, \tag{6}$$

where

$$|p(G)| \ = \ \{S \subseteq |G| : e \in X\}, \tag{7}$$

and where for S, $T \in |p(G)|$ we define

$$S \cdot T \ = \ \{gh : g \in S,\ h \in T\}, \tag{8}$$

and

$$S^{-1} \ = \ \{g^{-1} : g \in S\}, \tag{9}$$

while letting $\cap$ and $|G|$ in (6) have their obvious meanings (intersection of subsets, and the improper subset of $|G|$).

We can now formulate precisely the general construction sketched in the preceding section.

Definition 3. Let $(X_i)_{i\in I}$ be a family of pairwise disjoint infinite sets, with union $X = \bigcup_I X_i$, and for each $x \in X$, let $\iota(x) \in I$ be the index such that $x \in X_{\iota(x)}$. We shall denote by $G_{(X_i)}$ the group of those permutations g of X having the property that $\iota(xg) = \iota(x)$ for all but finitely many $x \in X$.

For each $\rho \in |r(I)|$ (see Definition 1), we shall write

$$S_\rho \ = \ \{g \in |G_{(X_i)}| : (\forall\, x \in X)\ (\iota(x), \iota(xg)) \in \rho\}, \tag{10}$$

in other words, the set of those permutations of X that change the home set X_i of only finitely many elements of X, and that can only move an element from X_i to X_j if $(i, j) \in \rho$.

5. Embeddings

The first part of the next theorem is the generalization of the properties of our example answering Kuczma's question; we shall recover that case from it in the next section. The second part of the theorem is a case of a known result in the opposite direction.

Theorem 4. *Let I be a set. Then there exists a group G and an embedding of the restricted relation algebra $r(I)$ in the restricted subset algebra $p(G)$. Namely, starting with any I-tuple of pairwise disjoint infinite sets $(X_i)_{i\in I}$, if we take for G the group $G_{(X_i)}$ of Definition 3, then the map $|r(I)| \to |p(G)|$ defined by*

$$\rho \ \mapsto \ S_\rho \ \subseteq \ |G| \quad (\textit{see } (10)) \tag{11}$$

is such an embedding.

Inversely, given any group G, there exists a set I and an embedding of $p(G)$ in $r(I)$. Namely, for $I = |G|$, such an embedding is given by

$$S \ \mapsto \ \{(g, gs) : g \in |G|,\ s \in S\}, \tag{12}$$

equivalently, $\{(g, h) \in |G| \times |G| : g^{-1}h \in S\}$.

Thus, if A is any algebra with four operations, two binary, one unary and one zeroary, then A is embeddable in the restricted relation algebra $r(I)$ of some set I if and only if it is embeddable in the restricted subset algebra $p(G)$ of some group G.

Proof. It is immediate from the definition (10) that the map (11) respects intersections, takes converse relations to inverse subsets, and takes the improper relation on I to the whole group $G_{(X_i)}$; so what we need to verify is that it respects composition and is one-to-one. It is straightforward that $S_\rho \cdot S_\sigma \subseteq S_{\rho\circ\sigma}$. Indeed, writing an element of $S_\rho \cdot S_\sigma$ as gh with $g \in S_\rho$ and $h \in S_\sigma$, consider any $x \in X$. By (10) $(\iota(x), \iota(xg)) \in \rho$ and $(\iota(xg), \iota(xgh)) \in \sigma$; hence $(\iota(x), \iota(xgh)) \in \rho \circ \sigma$. Since this holds for all $x \in X$, we have $gh \in S_{\rho\circ\sigma}$.

To get the reverse inclusion, consider any $f \in S_{\rho\circ\sigma}$, and let us try to write it as the product of a member of S_ρ and a member of S_σ. To this end, let $x_1, \dots, x_n$ be the finitely many elements $x \in X$ such that $\iota(xf) \neq \iota(x)$ (see Definition 3). Since $f \in S_{\rho\circ\sigma}$, each pair $(\iota(x_m),\, \iota(x_m f))$ lies in $\rho \circ \sigma$, so we can find $j_1, \dots, j_n \in I$ such that

$$(\iota(x_m),\, j_m) \in \rho, \quad (j_m,\, \iota(x_m f)) \in \sigma \quad (m = 1, \dots, n). \tag{13}$$

For $m = 1, \dots, n$, let us choose elements $y_m \in X_{j_m}$ so that $y_1, \dots, y_n$ are distinct (which is possible because the X_i are all infinite). Let us now choose any $g \in |G|$ such that

$$\begin{array}{l} x_m\, g \ = \ y_m \text{ for } m = 1, \dots, n, \text{ while } g \text{ moves no other elements} \\ \text{out of the sets } X_i \text{ in which they started.} \end{array} \tag{14}$$

This is again possible because the X_i are infinite, so that if the number of elements to be moved into and out of a given X_i are different, we can absorb the disparity by moving infinitely many elements within X_i. By (14) and the first relation of (13), $g \in S_\rho$. Letting $h = g^{-1}f$, we see that no element not among the y_m is moved by h from one X_i to another, while each y_m is moved from X_{j_m} to $X_{\iota(x_m f)}$; so by the second condition of (13), $h \in S_\sigma$. Since $f = gh$, this shows that the element $f \in S_{\rho\circ\sigma}$ indeed lies in $S_\rho \cdot S_\sigma$, completing the proof that (11) respects composition.

To show that (11) is one-to-one, suppose ρ and σ are distinct elements of $|r(I)|$. Assume without loss of generality that (i, j) belongs to ρ but not to σ. Then $i \neq j$, and we can construct a permutation g of X which moves one element of X_i into X_j, and keeps all other elements of X in their home sets. Thus g belongs to S_ρ but not to S_σ, showing that these are distinct, and completing the proof of the first assertion of the theorem.

That the construction (12) has the properties stated in the second assertion of the theorem is immediate, as is the final consequence of this pair of assertions. □

Remarks: The homomorphism (12) is a standard way of embedding the (unrestricted) "complex algebra" of a group in a relation algebra (also in the unrestricted sense). But the behavior of the construction (11) proved above is quite different from the situation for unrestricted relation algebras: R. McKenzie [3] shows, roughly, that the class of subalgebras of unrestricted relation algebras on sets which are embeddable (via *any* map) in subset algebras of groups is not determined by any finite set of first-order axioms.

The fact that the homomorphisms (11) and (12) are one-to-one and respect intersections shows that they are embeddings of posets. It also is not hard to see that, in addition to the finitary operations of Theorem 4, they respect unions and intersections of arbitrary chains.

6. Applications

6.1. Back to where we began. Let us recover from Theorem 4 the properties asserted in Section 2 for the group and monoid described there. We need the following observation.

Lemma 5. *For $(X_i)_{i\in I}$ as in Definition 3, and any $\rho \in |r(I)|$, the set S_ρ is a submonoid of $G_{(X_i)}$ if and only if ρ is a preorder, while it is a subgroup if and only if ρ is an equivalence relation.*

Proof. Since any $\rho \in |r(I)|$ is reflexive, ρ will be a preorder if and only if it is transitive, i.e., satisfies $\rho \circ \rho \subseteq \rho$, which by Theorem 4 is equivalent to the condition that $S_\rho \cdot S_\rho \subseteq S_\rho$. (Recall the remark at the end of the preceding section, that the constructions of that theorem are embeddings of posets, i.e., respect "$\subseteq$".) Since S_ρ contains the identity element of $G_{(X_i)}$, the above is precisely the condition for S_ρ to be a submonoid thereof.

A preorder on a set is an equivalence relation if and only it is symmetric, i.e., if and only if $\rho = \rho^{-1}$, which by Theorem 4 is equivalent to $S_\rho = S_\rho^{-1}$, which says that the monoid S_ρ is a subgroup of $G_{(X_i)}$. □

In particular, for $I = \{1, \ldots, n\}$ with the partial ordering $\preccurlyeq$ described at the start of Section 3, $S_\preccurlyeq$ is a submonoid M of $G = G_{(X_i)}$. If we form composites $\preccurlyeq \circ \preccurlyeq^{-1} \circ \preccurlyeq \circ \ldots$, it is easy to verify that the length-n composite is the indiscrete relation $I \times I$, but that no initial subcomposite is. (Specifically, one sees by induction that in building up that composite, we do not get the pair $(1, m)$ until we have m factors; so in particular, we don't get $(1, n)$ till we have all n factors.) Hence, as claimed, the n-fold product $M \cdot M^{-1} \cdot \ldots$ equals G, but no initial subproduct does.

6.2. Does the left hand know what the right hand is doing? Suppose we start with an arbitrary finite partially ordered set $(I, \preccurlyeq)$ and a family $(X_i)_{i\in I}$ of pairwise disjoint infinite sets. Because I is finite, the increasing chain of binary relations on I,

$$\preccurlyeq, \quad \preccurlyeq \circ \preccurlyeq^{-1}, \quad \preccurlyeq \circ \preccurlyeq^{-1} \circ \preccurlyeq, \quad \dots \tag{15}$$

will stabilize after finitely many steps; hence so will the chain of subsets $S_{\preccurlyeq} \cdot S_{\preccurlyeq}^{-1} \cdot \dots$ of $G = G_{(X_i)}$. Clearly, the eventual value of the latter chain will be the subgroup generated by $S_{\preccurlyeq}$ (corresponding to the equivalence relation on I generated by $\preccurlyeq$).

What if, instead of starting our products with $S_{\preccurlyeq}$, we begin with $S_{\preccurlyeq}^{-1}$? The chain of subsets $S_{\preccurlyeq}^{-1} \cdot S_{\preccurlyeq} \cdot \dots$ that we get will necessarily stabilize to the same group; but will the two chains achieve grouphood after the same numbers of steps?

If one of them achieves grouphood with an odd number of factors, then the other will do so at or before the same step; for the odd-length products have the forms $S_{\preccurlyeq} \cdot S_{\preccurlyeq}^{-1} \cdot \ \dots \ \cdot S_{\preccurlyeq}$ and $S_{\preccurlyeq}^{-1} \cdot S_{\preccurlyeq} \cdot \ \dots \ \cdot S_{\preccurlyeq}^{-1}$, which are inverses to one another; so if one is a group, the other is the same group. However, it is possible for one of the products, $S_{\preccurlyeq} \cdot S_{\preccurlyeq}^{-1} \cdot \ \dots$ or $S_{\preccurlyeq}^{-1} \cdot S_{\preccurlyeq} \cdot \ \dots$, to achieve grouphood at an even length $2m$, while the other does not do so till it reaches length $2m+1$ (at which stage it indeed gives the same group, since its *last* $2m$ factors form the product we have assumed is a group). In fact, for the poset of (1) with $n = 2m+1$, we find that the $n-1$-fold product beginning with $S_{\preccurlyeq}^{-1}$ equals G, though we have seen that the product starting with $S_{\preccurlyeq}$ needs n steps to get to G.

There are also partially ordered sets for which the two sorts of composites, $S_{\preccurlyeq} \cdot S_{\preccurlyeq}^{-1} \cdot \dots$ and $S_{\preccurlyeq}^{-1} \cdot S_{\preccurlyeq} \cdot \dots$, reach grouphood at the same even or odd step. For even n, this is true of the construction of Section 2, as may be deduced from the fact that in that case, $(I, \preccurlyeq)$ and $(I, \preccurlyeq^{-1})$ are isomorphic posets. For odd n, we can take $(I, \preccurlyeq)$ to be the union of a copy of the n-element poset constructed as in Section 2, and a copy of its opposite, with the elements of one copy incomparable with those of the other. A construction that works uniformly for even and odd n takes $I = |\mathbb{Z}/2(n-1)\mathbb{Z}|$, again letting $\preccurlyeq$ be the partial order under which each even element of I is $\preccurlyeq$ the two adjacent odd elements. (Thus, $(I, \preccurlyeq)$ is a "crown" with $2(n-1)$ vertices.)

6.3. Another group-from-monoids example. Let $I = \{1,2,3,4,5,6\}$, and consider the following three partial orderings on I.

$\preccurlyeq_1$, under which $1 \preccurlyeq_1 2 \preccurlyeq_1 3 \preccurlyeq_1 4 \preccurlyeq_1 5$, while 6 is incomparable with all of these,

$\preccurlyeq_3$, under which $3 \preccurlyeq_3 4 \preccurlyeq_3 5 \preccurlyeq_3 6 \preccurlyeq_3 1$, while 2 is incomparable with all of these, (16)

$\preccurlyeq_5$, under which $5 \preccurlyeq_5 6 \preccurlyeq_5 1 \preccurlyeq_5 2 \preccurlyeq_5 3$, while 4 is incomparable with all of these.

I claim that

$$\begin{array}{l}(\preccurlyeq_5 \circ \preccurlyeq_3 \circ \preccurlyeq_1) \ = \ (\preccurlyeq_3 \circ \preccurlyeq_1 \circ \preccurlyeq_5) \ = \ (\preccurlyeq_1 \circ \preccurlyeq_5 \circ \preccurlyeq_3) \ = \ 1, \\ \text{but none of } (\preccurlyeq_1 \circ \preccurlyeq_3 \circ \preccurlyeq_5),\ (\preccurlyeq_5 \circ \preccurlyeq_1 \circ \preccurlyeq_3), \text{ or } (\preccurlyeq_3 \circ \preccurlyeq_5 \circ \preccurlyeq_1) \\ \text{equals } 1.\end{array} \tag{17}$$

(Above and in the next paragraph, parentheses are put around relation-symbols when set-theoretic relation symbols are applied to them.) From this, it will follow by Theorem 4 that the submonoids $A = S_{\preccurlyeq_5}$, $B = S_{\preccurlyeq_3}$ and $C = S_{\preccurlyeq_1}$ of G satisfy

$$\begin{array}{l}A \cdot B \cdot C \ = \ B \cdot C \cdot A \ = \ C \cdot A \cdot B \ = \ G, \\ \text{but none of } A \cdot C \cdot B \text{ or } B \cdot A \cdot C \text{ or } C \cdot B \cdot A \text{ equals } G.\end{array} \tag{18}$$

To establish (17), let us first verify that $(\preccurlyeq_5 \circ \preccurlyeq_3 \circ \preccurlyeq_1) = 1$. Given any $i \in I$, we must show that $(i, j) \in (\preccurlyeq_5 \circ \preccurlyeq_3 \circ \preccurlyeq_1)$ for all $j \in I$. We see from the last line of (16) that if $i \neq 4$, then $(i, 3) \in (\preccurlyeq_5)$, while if $i = 4$ we trivially have $(i, 4) \in (\preccurlyeq_5)$. From these two relations and the second line of (16), we can see that whatever i is, $\preccurlyeq_5 \circ \preccurlyeq_3$ contains $(i, 4)$, $(i, 5)$, $(i, 6)$, $(i, 1)$. Composing with $\preccurlyeq_1$, and using the fact that we have already gotten $(i, 1)$, we see from the first line of (16) that we get $(i, 2)$ and $(i, 3)$ as well. So $\preccurlyeq_5 \circ \preccurlyeq_3 \circ \preccurlyeq_1$ indeed contains all pairs (i, j) $(i, j \in I)$. The same is true of the other two composites listed in (17), by symmetry, i.e., by the fact that the 2-step cyclic permutation of the elements of I cyclically permutes the preorders (16). Thus we have established the first line of (17).

On the other hand, it is not hard to check that $\preccurlyeq_1 \circ \preccurlyeq_3 \circ \preccurlyeq_5$ does not contain $(5, 4)$, $(6, 4)$ or $(6, 5)$, hence is not the relation 1; and again, by symmetry, this implies the other cases of the second line of (17).

As noted, these results give (18).

7. Some variant constructions

7.1. Generalizing the finite/infinite contrast. There are some easy variants of Definitions 1-3 for which Theorem 4 goes over without difficulty.

On the one hand, for any fixed infinite cardinal κ one can everywhere replace "finite" and "infinite" by "of cardinality $< \kappa$" and "of cardinality $\geq \kappa$" in that theorem and the definitions which precede it.

If I is infinite, one can also weaken the condition that only finitely many (or in the above generalization, fewer than κ) elements of X move from one X_i to another, to merely say that each X_i receives only finitely many (respectively, fewer than κ) elements from outside itself, and sends only finitely many (respectively, fewer than κ) out of itself.

One can also replace infinite sets X_i, their finite subsets, and set maps among them by, say, measure spaces of positive measure, their subsets of measure zero, and measure-preserving permutations of X, if one uses measure spaces for which one has an appropriate measure-theoretic version of

Hilbert's Hotel. In particular, the standard measure on the real unit interval $[0,1]$ has the property that for every $Z \subseteq [0,1]$ of measure zero, there is a measure-preserving bijection between $[0,1] - Z$ and $[0,1]$ (Charles Pugh, personal communication). From this it easily follows that $X = \bigcup X_i$ has the desired properties if each X_i is a copy of $[0,1]$, and G consists of the measure-preserving permutations of X under which the set of points that move between the sets X_i has measure zero.

7.2. A finitely generated example. Dawid Kielak (personal communication) has asked whether one can get a G and an M answering Kuczma's original question, such that M is finitely generated as a monoid. I outline below how to modify the construction of §2 to get such an example.

Given a finite poset $(I, \preccurlyeq)$, let $X = \bigcup_{i \in I} X_i$, where each X_i consists of elements $x_{i,k}$ $(k \in \mathbb{Z})$, and elements with distinct subscript-pairs are understood to be distinct. Let M be the monoid of permutations of X generated by the following elements:

a_i, defined for each $i \in I$, which acts by $x_{i,k}\, a_i = x_{i,k+1}$, and fixes all $x_{i',k}$ with $i' \neq i$, (19)

a_i^{-1}, defined for each $i \in I$, which, of course, acts by $x_{i,k}\, a_i^{-1} = x_{i,k-1}$, and again fixes all $x_{i',k}$ with $i' \neq i$, (20)

b_i, defined for each $i \in I$, which interchanges $x_{i,0}$ and $x_{i,1}$, and fixes all other elements of X, (21)

$c_{i,i'}$ defined for all $i \neq i'$ such that $i \preccurlyeq i'$, which acts by

$$\begin{aligned} x_{i,0}\ c_{i,i'} &= x_{i',0}, \\ x_{i,k}\ c_{i,i'} &= x_{i,k-1}, \text{ for } k > 0, \\ x_{i',k}\ c_{i,i'} &= x_{i',k+1}, \text{ for } k \geq 0, \end{aligned} \tag{22}$$

and which fixes all elements of X other than those listed above (including elements $x_{i,k}$ and $x_{i',k}$ with $k < 0$).

Note that the generators in the first three sets, (19)-(21), all have inverses in M, so the monoid they generate is a group H. Clearly, members of H carry each X_i into itself; it is not hard to verify that H *includes* all permutations with this property which move only finitely many elements of X (these form the subgroup generated by the conjugates of the b_i by powers of the a_i), and that the general element of H acts on each X_i as such a permutation, followed by a translation $a_i^{t_i}$ $(t_i \in \mathbb{Z})$.

It is also not hard to verify that when we bring in the $c_{i,i'}$, the effect is that whenever $i \prec i'$, an element $f \in M$ can move any finite family of elements of X_i to arbitrary positions in $X_{i'}$. (The idea is to move the elements of X_i that are to be transferred to $X_{i'}$ one by one to the position $x_{i,0}$, then apply $c_{i,i'}$, and, finally, move their images, $x_{i',0}$, to the desired positions in $X_{i'}$.) The actions of f on "most" elements of each X_i will still be by translations of the second subscript; but a consequence of the difference between the behavior the $c_{i,i'}$ on elements with positive and with negative second subscripts is that for each i, there will, in general, be two different translations, one affecting elements $x_{i,k}$ with k large (above some constant), the other affecting such elements with k small (below some constant). Precisely,

> A permutation f of X will belong to M if and only if (i) for all $i, i' \in I$, f carries no elements of X_i into $X_{i'}$ unless $i \preccurlyeq i'$, and (ii) for each $i \in I$, there exist an integer s_i such that for all sufficiently large k, $x_{i,k}f = x_{i,k+s_i}$, and an integer t_i such that for all sufficiently small k, $x_{i,k}f = x_{i,k+t_i}$. (23)

Here $s_i - t_i$ will be the number of elements that f moves into X_i, minus the number it moves out of X_i. It is not hard to deduce from (23), by the same method used in the proof of Theorem 4 to show that $S_\rho\, S_\sigma = S_{\rho\circ\sigma}$, that membership in a product $M\,M^{-1}M\ \dots\ M^{(-1)^{m-1}}$ is described by the condition like (23), except that in (i), the relation $\preccurlyeq$ is replaced by the relation $\preccurlyeq \circ \preccurlyeq^{-1} \circ \preccurlyeq \circ \cdots \circ \preccurlyeq^{(-1)^{m-1}}$. In particular, letting I be the poset of (1), we see that a product $M\,M^{-1}M \dots M^{(-1)^{m-1}}$ will be the group G of *all* permutations that satisfy (ii) if and only if $m \geq n$; from which it follows that M has the property asked for by Kuczma.

We remark that if I is any finite set, and for each $\rho \in |r(I)|$ we let S_ρ be the set of permutations f of X satisfying the analog of (23) with ρ in place of $\preccurlyeq$, then this gives us an embedding of $r(I)$ in $p(G)$, as in Theorem 4. But if ρ is not a preorder, I do not see any property of S_ρ generalizing the striking fact that when it is a preorder, M is finitely generated as a monoid. (The closest I can see is the observation that for all $\rho \in |r(I)|$, the submonoid of G generated by S_ρ is finitely generated.)

7.3. Dropping the finiteness restriction. We might enlarge, rather than restricting, the class of the permutations we consider. Given a finite set I and a family of disjoint infinite sets X_i, say, for simplicity, all countable, suppose we let G be the group of *all* permutations of $X = \bigcup X_i$, without the finiteness restriction on elements moving among the X_i. Let us again associate to each binary relation ρ on I the subset of those elements of G that don't move elements from X_i to X_j unless $(i,j) \in \rho$, and call this S_ρ.

Again, if $\preccurlyeq$ is a preorder, then $S_\preccurlyeq$ is a monoid; and we can again get examples where G can be expressed as a finite product of $S_\preccurlyeq$ and $S_\preccurlyeq^{-1}$, but where the smallest such product is arbitrarily long. But the monoid M determined by a given pair $(I, \preccurlyeq)$ under this version of our construction may in fact require longer products $M \cdot M^{-1} \cdot \dots$ to get this group G than the monoid of Sections 4-5 took to generate the G of that construction. For instance, if $I = \{1, 2\}$ with $1 \preccurlyeq 2$, I claim that a composite of $S_\preccurlyeq$ and $S_\preccurlyeq^{-1}$ which contains a permutation that *interchanges* the contents of the two sets X_1 and X_2 must have length at least 3. To see that no such permutation belongs to $S_\preccurlyeq \cdot S_\preccurlyeq^{-1}$, note that any member of $S_\preccurlyeq$ must leave in X_1 infinitely many of the elements that were originally there, and that none of these is moved out by any member of $S_{\preccurlyeq}^{-1}$. But we do get permutations interchanging X_1 and X_2 in $S_{\preccurlyeq} \cdot S_{\preccurlyeq}^{-1} \cdot S_{\preccurlyeq}$: think (roughly speaking) of first moving half the elements of X_1 up into X_2 (as in the versions of Hilbert's Hotel with infinitely many arriving or departing guests), then moving all the elements that were originally in X_2 down into X_1, and finally moving those that stayed in X_1 at the first step up into X_2.

In this situation, the class of sets $S_\rho \subseteq G$ ($\rho \in |r(I)|$) is not closed under composition; e.g., it is not hard to see that in the situation just described, $S_{\preccurlyeq} \cdot S_{\preccurlyeq}^{-1} = S_{\preccurlyeq} \cdot S_{\preccurlyeq^{-1}}$ does not have the form S_ρ for any $\rho \in |R(I)|$. I have not examined for general I the algebra of subsets of $|G|$ generated by the sets S_ρ ($\rho \in |R(I)|$) under the operations of $p(G)$.

7.4. A two-group construction. In the discussion preceding Definitions 1-3, we noted that the construction we were leading up to would not respect "identity elements", i.e., would not send $\Delta \in |r(I)|$ to $\{e\} \in |p(G)|$; so we left the zeroary operations Δ and $\{e\}$ out of the structures we defined. However, with a bit of added complication, we can bring Δ back in. Note that in the context of Definition 3, S_Δ is the subgroup $H \subseteq G$ of permutations of X that carry each X_i to itself; and that every subset S_ρ is left and right H-invariant (closed under left and right multiplication by elements of H). Building on this observation, suppose that for any group G and subgroup H, we let

$$|p'(G,H)| \;=\; \{S \subseteq |G| : e \in S,\ S = HSH\}. \tag{24}$$

This family of sets is closed under the four operations in our definition of $p(G)$, and has $|H|$ as least element. We find that if we now define algebras with five operations,

$$p'(G,H) \;=\; (|p'(G,H)|,\ \cap,\ \cdot,\ ^{-1},\ |H|,\ |G|), \tag{25}$$

$$r'(I) \;=\; (|r(I)|,\ \cap,\ \circ,\ \ ^{-1},\ \Delta,\ 1), \tag{26}$$

and for any family of disjoint infinite sets $(X_i)_{i\in I}$, we supplement Definition 3 with

$$H_{(X_i)} \;= \text{the subgroup of } G_{(X_i)} \text{ with underlying set } S_\Delta, \tag{27}$$

then the map (11), i.e., $\rho \mapsto S_\rho$, gives an embedding of $r'(I)$ in $p'(G_{(X_i)},\, H_{(X_i)})$ carrying the constant Δ to the constant $|H|$, as well as respecting the other four operations. Inversely, given a group G and a subgroup H, if we let $I = G/H$, the set of left cosets of H in G, and take as our analog of (12) the map $|p'(G,H)| \to |r'(I)|$ given by

$$S \;\mapsto\; \{(gH,\, gsH) : g \in |G|,\ s \in S\}, \tag{28}$$

then together these constructions satisfy the analog of Theorem 4.

(In a preprint version of this note, I claimed incorrectly that we could get such a construction using for I the set $H\backslash G/H$ of double cosets of H in G. The analog of (28) would have been

$$S \;\mapsto\; \{(HgH,\, HgsH) : g \in |G|,\, s \in S\}. \tag{29}$$

However, this map does not respect intersections. For instance, if G is the free group on $\{x, y, z\}$ and H its subgroup generated by x, consider the elements $S = H \cup HyH$ and $T = H \cup Hz^{-1}xzyH$ of $|p'(G, H)|$. I claim that the images in $I \times I$ under (29) of both S and T contain the pair $(HzH,\ HzyH)$. That the image of S does is clear; that the image of T also does can be seen by writing $(HzH,\ HzyH)$ as $(HzH,\ Hz \cdot z^{-1}xzyH)$. However, the image under (29) of $S \cap T = H$ clearly does not contain $(HzH,\ HzyH)$.)

7.5. Still more operations. In [2, Section 1.1] B. Jónsson notes that there are many more natural operations on the binary relations on a set I than those in the "classical clone", the clone generated by the operations here denoted $\cap$, $\cup$, $\circ$, ^{c}, ${}^{-1}$, 0, Δ and 1.

For example, given $\rho,\ \sigma \in |R(I)|$, he defines the left and right *residuals* of ρ with respect to σ:

$$\begin{aligned} \rho/\sigma \ &= \ \{(i,j) : (\forall\ k \in I)\ (j,k) \in \sigma \implies (i,k) \in \rho\}, \\ \sigma\backslash\, \rho \ &= \ \{(i,j) : (\forall\ k \in I)\ (k,i) \in \sigma \implies (k,j) \in \rho\}. \end{aligned} \tag{30}$$

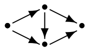
These are the largest relations τ_1 and τ_2 such that $\tau_1 \circ \sigma \subseteq \rho$ and $\sigma \circ \tau_2 \subseteq \rho$. Unfortunately, these two operations cannot be fitted into our restricted relation algebras, because they do not, in general, take reflexive relations to reflexive relations. Indeed, if ρ/σ, respectively, $\sigma\backslash\rho$, is reflexive, this implies, by the characterization of those operations just mentioned, that $\Delta \circ \sigma \subseteq \rho$, respectively $\sigma \circ \Delta \subseteq \rho$, which is not the case for all reflexive ρ and σ, since $\Delta \circ \sigma = \sigma = \sigma \circ \Delta$. Conceivably, it might be useful to bring in / and \ as *partial* operations, defined on those pairs (ρ, σ) such that $\sigma \subseteq \rho$; or, roughly equivalently, to look at the operations $\rho/(\sigma \cap \rho)$ and $(\sigma \cap \rho)\backslash\rho$.

However, another (infinite) family of operations discussed in [2, Section 1.1] can be incorporated nicely into our restricted relation algebras. These are typified by the 5-ary operation Q defined by

$$\begin{aligned} Q(\rho_1,\, \sigma_1,\, \rho_2,\, \sigma_2,\, \tau)\ &= \{(i,j) \in I \times I : (\exists\ k,\ \ell \in I) \\ &\quad (i,k) \in \rho_1,\ (k,j) \in \sigma_1,\ (i,\ell) \in \rho_2,\ (\ell,j) \in \sigma_2,\ (k,\ell) \in \tau\} \end{aligned} \tag{31}$$

[2, p. 247]. One finds that this corresponds as in Theorem 4 to the 5-ary operation on subsets of a group G,

$$\begin{aligned} Q(R_1,\, S_1,\, R_2,\, S_2,\, T)\ &=\ \{f \in |G| : (\exists\ g, h \in |G|) \\ &\quad g \in R_1,\ g^{-1}f \in S_1,\ h \in R_2,\ h^{-1}f \in S_2,\ g^{-1}h \in T\}\,. \end{aligned} \tag{32}$$

Each of the operations in the family exemplified by Q is determined by a finite directed graph with two distinguished vertices, and edges labeled by the arguments of the operation. E.g., Q corresponds to the graph , where the distinguished vertices are those at the left and right ends, and where ρ_1 and σ_1 label the top two edges, ρ_2 and σ_2 the bottom two, and τ the vertical edge [2, p. 248]. (To see the relation between this labeled diagram and (31), label the left and right vertices with the index-symbols i and j, and the top and bottom vertices with k and ℓ.) The operations $\cap$, $\circ$, ${}^{-1}$, Δ and 1 also correspond in this way to graphs, namely $\bullet\rightrightarrows\bullet$, $\bullet\!\rightarrow\!\bullet\!\rightarrow\!\bullet$, $\bullet\!\leftarrow\!\bullet$, $\bullet$, and $\bullet\ \bullet$, in each case with the leftmost and rightmost vertices distinguished, and with appropriate labeling of the edges by the arguments of the operation. On the other hand, the operations $\cup$, ^{c}, and 0 do not belong to this family, nor do the two operations of (30).

For each such labeled graph, we likewise get an operation on subsets of groups which relates to the operation on binary relations as in Theorem 4.

7.6. Some thoughts and questions. I do not know whether the variants sketched in Sections 7.1-7.5 of the main construction of this paper are likely to prove "useful", either in answering group-theoretic questions not answered by Theorem 4, or in other ways (e.g., whether the measure-theoretic variant of our construction might give some information on the structure of measurable maps among measure spaces).

The referee has raised the question of which finite relation algebras can be embedded in the restricted subset algebras $p(G)$ of *finite* groups G. One property that a relation algebra which can be so embedded must have is that every $\circ$-*idempotent* element is ${}^{-1}$-invariant, since in $p(G)$, every element idempotent with respect to "$\cdot$" is a nonempty subset of G closed under multiplication, hence, if G is finite, a subgroup. I don't know whether there are additional restrictions.

The referee has also asked whether Theorem 4 can be generalized to non-reflexive relations. Since our "Hilbert's Hotel" trick is based on keeping "most" members of each X_i within X_i, it has no obvious extension to the non-reflexive case; so this interesting question would require a different approach.

7.7. A family resemblance. We end with an observation of a different sort.

I claim that every case of a group G, a submonoid M of G, and a positive integer n such that

$$\begin{array}{l}\text{the } n\text{-fold product } M\,M^{-1}M\,M^{-1}\ldots\,M^{(-1)^{n-1}} \text{ equals } G,\\ \text{but the product of the first } n-1 \text{ of these factors does not,}\end{array}\tag{33}$$

closely resembles, in a way, the example of Section 2. To see this, let $X = G$, on which we let G act by right translation, and let $X_1 = M$, $X_2 = M\,M^{-1} - M$ (relative complement), $X_3 = M\,M^{-1}M - M\,M^{-1}$, and so on. By (33), $X_n \neq \emptyset$ but $X_{n+1} = \emptyset$, from which it is easy to deduce that X_i is nonempty for $1 \leq i \leq n$, and empty for all $i > n$.

I claim that

$$X_i\,M \ \subseteq\ X_i \quad \text{if } i \text{ is odd,}\tag{34}$$

while

$$X_i\,M \ \subseteq\ X_{i-1} \cup X_i \cup X_{i+1} \quad \text{if } i \text{ is even.}\tag{35}$$

To see (34), let i be odd and consider any element $x = g_1\,g_2^{-1}\ldots\,g_i \in X_i$ $(g_1, g_2, \ldots, g_i \in M)$, and any $h \in M$. Clearly, xh still belongs to the

i-fold product $M\,M^{-1}\dots M$ so we need only show that we cannot write $xh = g'_1\,{g'_2}^{-1}\dots {g'_{i-1}}^{-1}$ with all $g'_j \in M$. And indeed, if we could, we would have $x = g'_1\,{g'_2}^{-1}\dots (h\,g'_{i-1})^{-1}$, an expression as a length-$i{-}1$ product, contradicting our assumption that $x \in X_i$. The assertion (35) is verified similarly: the product of an element $x \in X_i$ and an element $h \in M$ can be written as an $i{+}1$-fold alternating product of members of M and M^{-1}, and if we could write it as a product of the same sort having fewer than $i-1$ terms, this would lead to a representation of x having fewer than i terms, again contradicting the condition $x \in X_i$.

Clearly, (34) and (35) have the same form as the restrictions pictured in (1).

Of course, this similarity does not extend to the assertion that elements of G move only finitely many members of X from one X_i to another.

8. Acknowledgements

I am indebted to Ralph McKenzie for a fruitful correspondence on the 1981 draft of this note, to Charles Pugh for the measure-theoretic result quoted in Section 7.1, to Dawid Kielak for the question answered in §7.2, and to the referee for several helpful comments.

References

[1] Gamow, G.: One, two, three . . . infinity. Viking Press (1947).

[2] Jónsson, B.: The theory of binary relations. In: Algebraic logic (Budapest, 1988). Colloq. Math. Soc. János Bolyai, vol. 54, pp. 245–292. North-Holland, Amsterdam (1991). MR1153429

[3] McKenzie, R.: Representations of integral relation algebras. Michigan Math. J. **17** 279–287 (1970). MR0286735

[4] Siebzehnte internationale Tagung über Funktionalgleichungen in Oberwolfach vom 17.6. bis 23.6.1979, Aequationes Mathematicae **20** 286–315 (1980). MR1553872

[5] Wikipedia: Relation algebra, `https://en.wikipedia.org/wiki/Relation_algebra`.

George M. Bergman
Department of Mathematics, University of California, Berkeley, CA 94720-3840, USA
e-mail: gbergman@math.berkeley.edu
URL: https://math.berkeley.edu/~gbergman