

Some interesting properties of direct products of groups, semigroups and other algebraic structures

Nik Ruskuc

`nik@mcs.st-and.ac.uk`

School of Mathematics and Statistics, University of St Andrews

Edinburgh 26 February 2008



University
of
St Andrews

Preview: $1 + 1 = 2$

... for I cannot satisfy myself that, when one is added to one, the one to which the addition is made becomes two, or that the two units added together make two by reason of the addition. I cannot understand how, when separated from the other, each of them was one and not two, and now, when they are brought together, the mere juxtaposition or meeting of them should be the cause of their becoming two: neither can I understand how the division of one is the way to make two; for then a different cause would produce the same effect,—as in the former instance the addition and juxtaposition of one to one was the cause of two, in this the separation and subtraction of one from the other would be the cause. Nor am I any longer satisfied that I understand the reason why one or anything else is either generated or destroyed or is at all, but I have in my mind some confused notion of a new method ... (Socrates in Plato's Phaedo)

Instead of an Introduction: $d(A_n)$, $d(S_n)$

Definition

The **rank** of an algebraic structure is the smallest number of generators needed to generate A ; it is denoted $d(A)$.

G	$d(G)$
S_5	2
A_5	2
$S_5 \times S_5$	2
$A_5 \times A_5$	2
$S_5 \times S_5 \times S_5$	3
$A_5 \times A_5 \times A_5$	2

Facts

$d(A_5^{19}) = 2$, $d(A_5^{20}) = 3$. (P. Hall in 1936)

$A, B, A \times B$

$$A \xleftarrow{\pi_A : (a,b) \mapsto a} A \times B \xrightarrow{\pi_B : (a,b) \mapsto b} B \xleftarrow{\pi_A : (a,b) \mapsto a} A$$

Nice, Boring Theorems

Theorem

Let G and H be two groups, and let \mathcal{P} be any of the following properties: being finite, abelian, soluble, nilpotent, periodic, finitely generated, finitely presented, locally finite, residually finite, ... Then $G \times H$ satisfies \mathcal{P} if and only if both G and H satisfy \mathcal{P} .

Proof (for finite generation)

(\Rightarrow) G and H are homomorphic images of $G \times H$.

(\Leftarrow) $G \times H$ is generated by the natural copies of G and H inside it.

Remark

This works for monoids.

Growth of Direct Powers

Corollary

For any monoids M, N we have

$$\max(d(M), d(N)) \leq d(M \times N) \leq d(M) + d(N).$$

Definition

$\mathbf{d}(A) = (d(A), d(A^2), d(A^3), \dots)$.

Corollary

For a monoid M we have

$$d(M) \leq d(M^n) \leq nd(M).$$

Growth Sequences: Finite Groups

J. Wiegold (with J.S. Wilson, D. Meier, A.G.R. Stewart, A. Efranian), 1974–1995.

Theorem

For a finite group G , the sequence $\mathbf{d}(G)$ is

- ▶ *logarithmic if G is perfect;*
- ▶ *eventually linear if G is non-perfect.*

Growth Sequences: Infinite Groups

Theorem

For an infinite group G , the sequence $\mathbf{d}(G)$ is

- ▶ eventually constant, if G is simple;
- ▶ either eventually constant or logarithmic if G is perfect and non-simple;
- ▶ eventually linear if G is non-perfect.

Question

Does there exist an infinite simple group G such that $d(G^n) = d(G) + 1$?

Question

If a perfect group G has no finite images, is $\mathbf{d}(G)$ necessarily eventually constant?

Growth Sequences: Finite Semigroups

Theorem

For a finite semigroup S , the sequence $\mathbf{d}(S)$ is

- ▶ *eventually linear if S is a monoid;*
- ▶ *asymptotically exponential if S is not a monoid.*

Question

In the non-monoid case, is $\mathbf{d}(S)$ eventually exponential?

Growth Sequences: Infinite Monoids

Does there exist a monoid with an eventually constant growth sequence?

Suppose we have a finitely generated monoid $M = \langle A \rangle$ such that for every $k \geq 1$ there exists a k -tuple $(a_1, \dots, a_k) \in M^k$ such that

$$\{(a_1 m, \dots, a_k m) : m \in M\} = M^k.$$

Let \overline{M} be the diagonal copy of M in M^k :

$$\overline{M} = \{(m, \dots, m) : m \in M\} \cong M.$$

Then $M^k = \{(a_1, \dots, a_k)\} \overline{M}$.

So: $d(M^k) \leq d(M) + 1$.

Does such a monoid exist?

Diagonal Acts

Example

Consider the full transformation monoid $T_{\mathbb{N}}$. Define $a_i : \mathbb{N} \rightarrow \mathbb{N}$, $i = 1, \dots, k$ by

$$xa_i = xk + i \quad (x \in \mathbb{N}).$$

Let $t_1, \dots, t_k \in T_{\mathbb{N}}$ be arbitrary. Define $m : \mathbb{N} \rightarrow \mathbb{N}$:

$$(qk + r)m = qt_r \quad (1 \leq r \leq k).$$

Clearly: $(a_1 m, \dots, a_k m) = (t_1, \dots, t_k)$.

Difficulty: $T_{\mathbb{N}}$ is not finitely generated :-)

Example

The monoid of all recursive functions $\mathbb{N} \rightarrow \mathbb{N}$ is finitely generated, and also has the above property.

Finite Generation: Semigroups

Theorem

Let M, N be monoids. $M \times N$ is finitely generated if and only if M and N are finitely generated.

Example

Consider the additive semigroup $\mathbb{N} \times \mathbb{N}$ ($0 \notin \mathbb{N}$). Note:

$(1, n) \neq (a, b) + (c, d)$. We say that $(1, n)$ is **indecomposable**. So, $\{(1, n) : n \in \mathbb{N}\}$ is contained in every generating set.

Finite Generation: Semigroups

Theorem (EF Robertson, NR, J. Wiegold)

Let S, T be infinite semigroups. $S \times T$ is finitely generated if and only if

- (i) S and T are finitely generated; and*
- (ii) neither S nor T have indecomposable elements.*

Theorem

Let S, T be semigroups, with S infinite, T finite. $S \times T$ is finitely generated if and only if

- (i) S is finitely generated; and*
- (ii) T has no indecomposable elements.*

Finite Presentability

Theorem

Let M, N be monoids. $M \times N$ is finitely presented if and only if M and N are finitely presented.

Example

\mathbb{N} is finitely presented (in fact free), but $\mathbb{N} \times \mathbb{N}$ is not finitely presented.

Question

Will $S \times T$ be finitely presented provided S and T are finitely presented and $S \times T$ is finitely generated?

Critical Pairs and Stability

S – a semigroup; $\langle A|R \rangle$ a finite presentation for it.

Fact

*Two words u, v over A are equal in S if and only if there is a sequence of applications of relations from R (a **deduction**) which transforms u into v .*

Definition

A pair (u, v) of words is **critical** if every deduction from u to v contains a word of length smaller than $\min(|u|, |v|)$.

Definition

S is said to be **stable** if it has no critical pairs.

Remark

The above definition of stability is not constructive.

Stability and Finite Presentability

Theorem (EF Robertson, NR, J Wiegold)

Let S, T be two infinite semigroups. $S \times T$ is finitely presented if and only if

- (i) S and T are (finitely presented) and stable; and*
- (ii) neither S nor T contain indecomposable elements.*

Theorem (EF Robertson, NR, J Wiegold)

Let S be an infinite semigroup, and let T be a finite semigroup. $S \times T$ is finitely presented if and only if

- (i) S is finitely presented; and*
- (ii) T is stable and contains no indecomposable elements.*

Finite Presentability: 'Good Classes'

Corollary

Suppose that S and T belong to any of the following classes: monoids (including groups), regular semigroups (including inverse semigroups), surjective commutative semigroups (...). Then $S \times T$ is finitely presented if and only if S and T are finitely presented.

Some Non-Finitely-Presented Examples

Theorem (I Araujo, NR)

There is an (effective) algorithm which decides whether a finite semigroup is stable.

Example

The four element semigroup

S	a	b	c	0
a	a	a	c	0
b	b	b	c	0
c	0	0	0	0
0	0	0	0	0

is a non-stable semigroup of minimal size. Hence, for example, $S \times \mathbb{Z}$ is finitely generated but not finitely presented.

A Digression: A Strange Union

S		a	b	c	0
a		a	a	c	0
b		b	b	c	0
0		0	0	0	0
0		0	0	0	0

Example (Araujo, Branco, Fernandes, Gomes, NR)

Note that $S = U \cup V$, where $U = \{a\} \leq S$, $V = \{b, c, 0\} \leq S$.

Both U and V are stable. So:

- ▶ $U \times \mathbb{Z}$ and $V \times \mathbb{Z}$ are finitely presented.
- ▶ $S \times \mathbb{Z} = (U \times \mathbb{Z}) \cup (V \times \mathbb{Z})$.
- ▶ $S \times \mathbb{Z}$ is not finitely presented.

Residual Finiteness: Definition

Definition

An algebraic structure A is **residually finite** if for any two $a, b \in A$ ($a \neq b$) there is a homomorphism $f : A \rightarrow B$, B finite, such that $f(a) \neq f(b)$. Equivalently, A is **residually finite** if for any two $a, b \in A$ ($a \neq b$) there exists a congruence ρ with finitely many classes such that $(a, b) \notin \rho$.

Residual Finiteness: General, Nice, Boring Theorem?

Proposition

If A and B are residually finite then $A \times B$ is residually finite.

Proof

Take $(a, b) \neq (c, d)$. Wlog suppose $a \neq c$. Map:

$$A \times B \xrightarrow{\pi_A} A \xrightarrow{f} C, \quad C \text{ finite, } f(a) \neq f(c).$$

Proposition

If both A and B contain idempotents and $A \times B$ is residually finite then A and B are residually finite.

Proof

If $e \in A$ is an idempotent, then $B \cong \{e\} \times B \leq A \times B$.

Residual Finiteness: Semigroups

R. Gray, NR

Lemma

Let S be a semigroup. If $\mathbb{N} \times S$ is residually finite then S is residually finite.

Proof

Let $a, b \in S$, $a \neq b$.

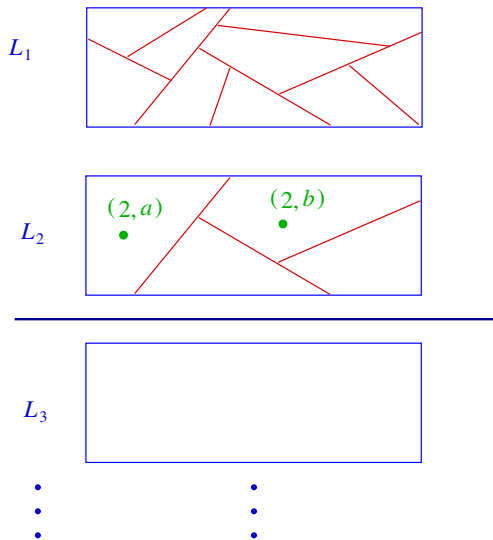
Let ρ be a congruence on $\mathbb{N} \times S$ with finitely many classes that separates $(2, a)$ and $(2, b)$.

$\mathbb{N} \times S$ naturally splits into levels: $L_i = \{i\} \times S$.

The equivalence relation λ with classes $L_1, L_2, L_3 \cup L_4 \cup \dots$ is a congruence with finitely many classes.

Intersect ρ and λ to obtain a congruence $\sigma = \rho \cap \lambda$ which has finitely many classes, respects levels 1 and 2, and separates $(2, a)$ and $(2, b)$.

Residual Finiteness: Levels of $\mathbb{N} \times S$



Residual Finiteness: Semigroups

Lemma

Let S be a semigroup. If $\mathbb{N} \times S$ is residually finite then S is residually finite.

Proof (contd.)

γ – the equivalence on S corresponding to the partition of level 1.

δ – the equivalence on S corresponding to the partition of level 2.

τ – the right congruence generated by γ .

Claim: $\gamma \subseteq \tau \subseteq \delta$.

Proof: τ is obtained by taking pairs (xu, yu) , $(x, y) \in \gamma$, $u \in S^1$, and closing transitively. But

$$\begin{aligned}(x, y) \in \gamma &\Rightarrow ((1, x), (1, y)) \in \sigma \Rightarrow ((1, x)(1, u), (1, y)(1, u)) \in \sigma \\ &\Rightarrow ((2, x), (2, y)) \in \sigma \Rightarrow (x, y) \in \delta.\end{aligned}$$

Hence: τ has finitely many classes, and separates a and b .

A technicality to pass to a congruence.

Residual Finiteness: A Nice, (Not Boring?) Theorem

Lemma

Let S be a semigroup. If $\mathbb{N} \times S$ is residually finite then S is residually finite.

Theorem (Gray, NR)

Let S and T be semigroups. $S \times T$ is residually finite if and only if S and T are residually finite.

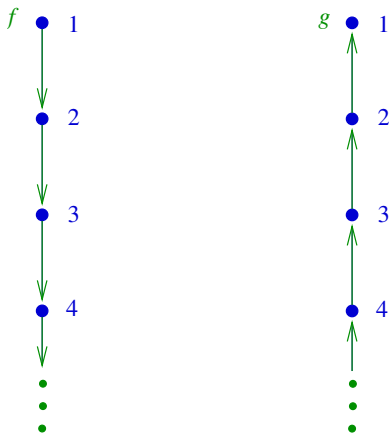
Proof

A semigroup either contains an idempotent or a copy of \mathbb{N} .

Residual Finiteness: Unary Algebras

Example

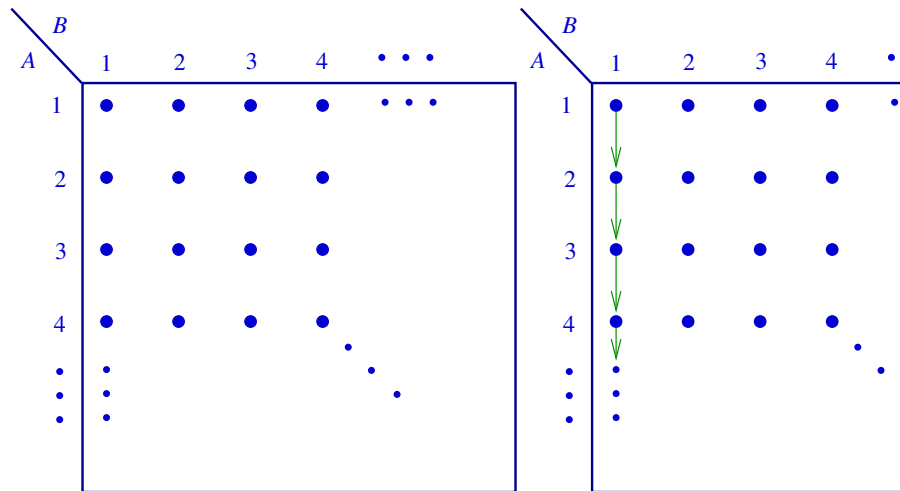
Consider two unary operations on \mathbb{N} :



Let $A = (\mathbb{N}, f)$, $B = (\mathbb{N}, g)$.

Residual Finiteness: Unary Algebras

Form the direct product $A \times B$:



Residual Finiteness: Unary Algebras

Lemma

B is not residually finite.

Proof

Suppose ρ is a congruence with finitely many classes separating 1 and 2.

Let $(m, n) \in \rho$, $m > n$.

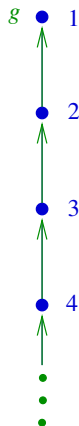
We have

$$\begin{aligned}(m, n) \in \rho &\Rightarrow (m-1, n-1) = (g(m), g(n)) \in \rho \\ &\Rightarrow \dots \Rightarrow (2, 1) \in \rho,\end{aligned}$$

a contradiction.

Lemma

A is residually finite.

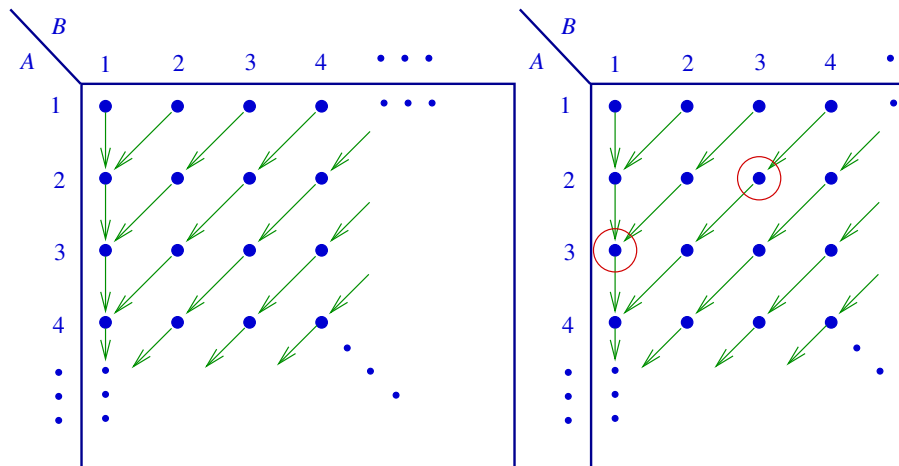


Residual Finiteness: Unary Algebras

Lemma

$A \times B$ is residually finite.

Proof



What Next?

A famous open problem: Is it true that $G \times H$ (G, H groups) is automatic if and only if G and H are automatic?

If not true, a counter-example might be easier to find for monoids/semigroups first.

Other products: wreath product, work in progress with M Quick, M Neunhöffer.