On residual finiteness of direct products of algebraic systems

R. Gray · N. Ruskuc

Abstract   It is well known that if two algebraic structures **A** and **B** are residually finite then so is their direct product. Here we discuss the converse of this statement. It is of course true if **A** and **B** contain idempotents, which covers the case of groups, rings, etc. We prove that the converse also holds for semigroups even though they need not have idempotents. We also exhibit three examples which show that the converse does not hold in general.

Keywords   Residual finiteness · Direct product · Semigroup · Unary algebra

Mathematics Subject Classification (2000)   08A30 · 20M10 · 08A60

An algebraic system **A** (which here means a set A with some operations defined on it) is said to be *residually finite* if for any two distinct $x, y \in A$ there is an epimorphism $f : \mathbf{A} \to \mathbf{B}$ onto a finite algebra **B** such that $f(x) \neq f(y)$. This is equivalent to the existence of a congruence θ (an equivalence relation respecting all operations) of finite index (i.e. with finitely many classes) on **A** such that $x/\theta \neq y/\theta$. (For more details on algebraic systems and congruences we refer the reader to [2]).

In this note we discuss residual finiteness of the direct product $\mathbf{A} \times \mathbf{B}$ of two algebras. In many classical cases (e.g. where **A**, **B** are groups or rings) $\mathbf{A} \times \mathbf{B}$ is residually finite

---

Communicated by D. Segal.

R. Gray
School of Mathematics, University of Leeds, Leeds LS2 9JT, UK
e-mail: robertg@maths.leeds.ac.uk

N. Ruskuc (✉)
School of Mathematics and Statistics, University of St Andrews, St Andrews KY16 9SS, UK
e-mail: nik@mcs.st-and.ac.uk

if and only if **A** and **B** are both residually finite, and this is regarded as folk-lore. In fact, in one direction this is always true.

Proposition 1 *If* **A** *and* **B** *are residually finite then* **A** × **B** *is residually finite.*

Proof Each of **A** and **B** is a natural homomorphic image of **A** × **B**. □

The proofs of the converse for groups and rings, etc. rely on the presence of idempotents. An element $e \in A$ is an *idempotent* if $f(e, e, \ldots, e) = e$ for every basic operation f of **A**.

Proposition 2 *Let* **A** *and* **B** *be algebras, and suppose that* **A** *contains an idempotent. If* **A** × **B** *is residually finite then* **B** *is residually finite.*

Proof If e is an idempotent in **A** then $\{e\} \times$ **B** is a subalgebra of **A** × **B** isomorphic to **B**, and every subalgebra of a residually finite algebra is itself residually finite. □

The best known class of algebraic structures which do not necessarily contain idempotents are semigroups. The easiest example of a semigroup without idempotents is **N** = $(\mathbb{N}, +)$ the additive semigroup of positive integers.

Theorem 1 *Let* **S** *be a semigroup. Then* **N** × **S** *is residually finite if and only if* **S** *is residually finite.*

Before proving the result we must make a few observations about congruences in semigroups (and, more generally, in algebras with a single binary operation).

Let $\mathbf{A} = (A, \cdot)$ be an algebra with a single binary operation. We say that an equivalence relation σ on A is *right compatible* (with the operation) if for all $c \in A$, $(a, b) \in \sigma$ implies $(ac, bc) \in \sigma$. Dually we define the notion of a *left compatible* equivalence relation. A right (resp. left) compatible equivalence relation on **A** is called a *right* (resp. *left*) *congruence*. It is then straightforward to verify that an equivalence relation on A is a congruence if and only if it is both a left and right congruence. In the particular case of semigroups, it follows from [3, Theorem 2.4] that any right congruence with finite index can be refined to give a congruence that also has finite index. Consequently in order to show that a semigroup is residually finite it is sufficient to show that any pair of distinct elements may be separated by a right congruence of finite index.

Proof of Theorem 1 (⇐) This is trivial as **N** is residually finite.

(⇒) Let $s, t \in S$ with $s \neq t$. Let ρ be a right congruence of finite index on **N** × **S** which separates $(2, s)$ from $(2, t)$. Let λ be the equivalence relation on $\mathbb{N} \times S$ with classes $1 \times S$, $2 \times S$, $\{3, 4, \ldots\} \times S$. It is easy to check that λ is a congruence. The right congruence $\sigma = \rho \cap \lambda$ has finite index, separates $(2, s)$ from $(2, t)$, and $1 \times S$ and $2 \times S$ are unions of σ-classes, say:

$$1 \times S = \bigcup_{i=1}^{m} 1 \times C_i, \quad 2 \times S = \bigcup_{j=1}^{n} 1 \times D_j.$$

Let γ be the equivalence relation on S the equivalence classes of which are the non-empty sets of the form $C_i \cap D_j$ ($1 \le i \le m, 1 \le j \le n$). Also let δ be the equivalence

relation on S with classes D_j $(1 \leq j \leq n)$. Let τ be the right congruence on $\mathbf{S}$ generated by γ.

Claim 1 $\gamma \subseteq \tau \subseteq \delta$.

Proof of claim It is obvious that $\gamma \subseteq \tau$. Now we show that $\tau \subseteq \delta$. Let $(a, b) \in \tau$. This means (see [1, Section 1.5] for example) that there is a sequence

$$a = z_1, z_2, \ldots, z_p = b,$$

where, for all $i = 1, \ldots, p - 1$, $z_i = c'_i u_i$, $z_{i+1} = c''_i u_i$, $(c'_i, c''_i) \in \gamma$, and $u_i \in S$ or is empty. Now for all $i = 1, \ldots, p - 1$ we have:

$$(c'_i, c''_i) \in \gamma \Rightarrow ((1, c'_i), (1, c''_i)) \in \sigma \Rightarrow ((1, c'_i)(1, u_i), (1, c''_i)(1, u_i)) \in \sigma$$

$$\Rightarrow ((2, c'_i u_i), (2, c''_i u_i)) \in \sigma \Rightarrow ((2, z_i), (2, z_{i+1})) \in \sigma$$

$$\Rightarrow (z_i, z_{i+1}) \in \delta,$$

provided $u_i \in S$, while, if u_i is empty, we have immediately from definition of γ that

$$(z_i, z_{i+1}) \in \gamma \Rightarrow (z_i, z_{i+1}) \in \delta.$$

In either case we conclude that $(a, b) \in \delta$, as required.   □

The inclusion $\gamma \subseteq \tau$ tells us that τ has finite index, and $\tau \subseteq \delta$ implies that τ separates s from t.   □

As a consequence we can now prove the converse of Proposition 1 for semigroups.

Theorem 2 *The direct product* $\mathbf{S} \times \mathbf{T}$ *of two semigroups is residually finite if and only if* $\mathbf{S}$ *and* $\mathbf{T}$ *are both residually finite.*

Proof Suppose that $\mathbf{S} \times \mathbf{T}$ is residually finite. It is a well known elementary fact that any semigroup either contains an idempotent or else it contains a subsemigroup isomorphic to $\mathbf{N} = (\mathbb{N}, +)$. If $\mathbf{S}$ contains an idempotent then $\mathbf{T}$ is residually finite by Proposition 2. Otherwise $\mathbf{S}$ contains a copy of $\mathbf{N}$ and so $\mathbf{S} \times \mathbf{T}$ contains $\mathbf{N} \times \mathbf{T}$ which by Theorem 1 implies that $\mathbf{T}$ is residually finite. A dual argument shows that $\mathbf{S}$ must be residually finite.   □

But, is it not the case that $\mathbf{A} \times \mathbf{B}$ being residually finite always implies that $\mathbf{A}$ and $\mathbf{B}$ are residually finite? In what follows we present three surprisingly simple examples which show that the answer is no. In the first example the algebras have only a single unary operation.

Example 1 Consider the following two operations on $\mathbb{N}$:

$$f(x) = x + 1, \quad g(x) = \begin{cases} x - 1 & \text{if } x > 1 \\ 1 & \text{if } x = 1; \end{cases} \tag{1}$$

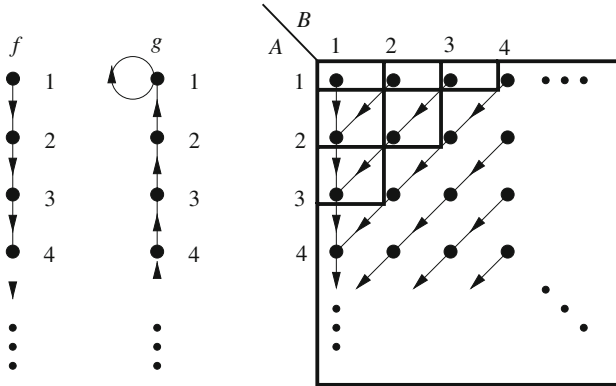see Fig. 1. Let $A = B = \mathbb{N}$. $\mathbf{A} = (A, f)$ and $\mathbf{B} = (B, g)$.

Fig. 1 Operations f and g, the algebra $\mathbf{A} \times \mathbf{B}$ and the congruence $\rho(4)$

Claim 1 The algebra $\mathbf{A}$ is residually finite.

Proof Let $m, n \in \mathbb{N}$ $(m > n)$. Then the relation

$$\rho = \{(i, i) : i \in \mathbb{N}\} \cup \{(i, j) : i, j > n\}$$

is a congruence of finite index separating m and n.   □

Claim 2 The algebra $\mathbf{B}$ is not residually finite.

Proof We prove that 1 and 2 cannot be separated by a proper congruence ρ. Suppose $(m, n) \in \rho$ $(m > n)$. Then $(2, 1) = (g^{m-2}(m), g^{m-2}(n)) \in \rho$.   □

Claim 3 The algebra $\mathbf{A} \times \mathbf{B}$ is residually finite.

Proof For an arbitrary set X, let $\Delta(X)$ denote the *diagonal relation* $\Delta(X) = \{(x, x) : x \in X\}$, and let $\Phi(X)$ denote the *full relation* $\Phi(X) = \{(x, y) : x, y \in X\}$ on X. For $r \geq 2$ define

$$I(r) = \{(a, b) \in A \times B : a + b \geq r\}.$$

Let $(a, b), (c, d) \in \mathbf{A} \times \mathbf{B}$ with $(a, b) \neq (c, d)$. Let $\rho = \rho(N)$ be the equivalence relation

$$\rho = \Delta(A \times B) \cup \Phi(I),$$

where $N = \max(a+b, c+d)$ and $I = I(N+1)$; see Fig. 1. Clearly ρ is an equivalence relation of finite index and it separates (a, b) from (c, d). Moreover for all $x \in A$ and $y \in B$ we have

$$(x, y) \in I \Rightarrow f(x) + g(y) \geq (x + 1) + (y - 1) = x + y \geq N + 1$$

$$\Rightarrow (f(x), g(y)) \in I$$

and it follows that ρ is a congruence.   □

In our second example the algebras each have one binary operation, and the first of them is the additive semigroup of positive integers.

Example 2 Let $C = D = \mathbb{N}$, $\mathbf{C} = (C, +)$ and $\mathbf{D} = (D, *)$ with $x * y = g(x)$ where $g(x)$ is defined in (1). Clearly $\mathbf{C}$ is residually finite. Note that every congruence on $\mathbf{D}$ would also be a congruence on the algebra $\mathbf{B}$ from Example 1; hence $\mathbf{D}$ is not residually finite.

We claim that $\mathbf{C} \times \mathbf{D}$ is residually finite. Let (k, m), $(l, n) \in C \times D$ with $(k, m) \neq (l, n)$. If $k \neq l$ we can separate (k, m) from (l, n) by projecting onto $\mathbf{C}$ and then using the fact that $\mathbf{C}$ is residually finite. So suppose $k = l$ and $m > n$. Consider the sets:

$$R_{k,m,i} = \{i\} \times \{j : j \geq m + k + 1 - i\} \quad (i = 1, \ldots, k), \tag{2}$$

$$J_k = \{j : j > k\} \times \mathbb{N}. \tag{3}$$

Let $\rho = \rho_{k,m}$ be the equivalence relation

$$\rho = \rho_{k,m} = \Delta(C \times D) \cup \left(\bigcup_{i=1}^{k} \Phi(R_{k,m,i}) \right) \cup \Phi(J_k);$$

for an illustration see Fig. 2. We claim that the relation ρ is a congruence on $\mathbf{C} \times \mathbf{D}$. Since we are dealing with algebras with a single binary operation it is sufficient to prove that ρ is both a left and a right congruence. This is a consequence of the following:

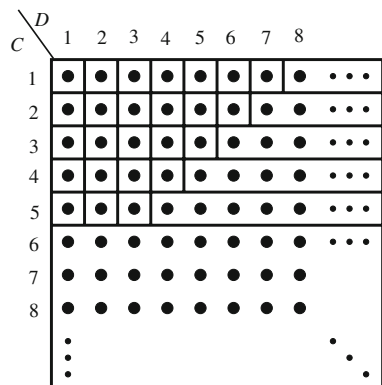$$R_{k,m,i}(a, b) \subseteq R_{k,m,i+a} \quad (\text{if } i + a \leq k), \tag{4}$$

$$R_{k,m,i}(a, b) \subseteq J_k \qquad (\text{if } i + a > k), \tag{5}$$

$$J_k(a, b) \subseteq J_k, \tag{6}$$

$$(a, b) R_{k,m,i} = \{(a + i, g(b))\}, \tag{7}$$

$$(a, b) J_k \subseteq J_k. \tag{8}$$

Fig. 2 The congruence $\rho_{5,3}$

Inclusions (5)–(8) are immediate consequences of (2), (3). Inclusion (4) follows from

$$
\begin{aligned}
(i, j) \in R_{k,m,i} &\Rightarrow j \geq m + k + 1 - i \\
&\Rightarrow g(j) \geq j - 1 \geq m + k + 1 - i - 1 \\
&\geq m + k + 1 - i - a \\
&\Rightarrow (i + a, g(j)) \in R_{k,m,i+a} \Rightarrow (i, j)(a, b) \in R_{k,m,i+a}.
\end{aligned}
$$

This demonstrates that $\mathbf{C} \times \mathbf{D}$ is residually finite because ρ separates (k, m) and (k, n).

In our final example we give two algebras neither of which is residually finite but whose direct product is residually finite.

Example 3 Let f and g be defined as in (1), let $E = F = \mathbb{N}$, and let $E = (E, f, g)$ and $F = (F, g, f)$; see Fig. 3. Neither of the algebras $\mathbf{E}$ nor $\mathbf{F}$ is residually finite since the algebra $\mathbf{B}$ in Example 1 is not residually finite. We are going to prove that $\mathbf{E} \times \mathbf{F}$ is residually finite. Let $(a, b), (c, d) \in E \times F$ with $(a, b) \neq (c, d)$. As in Example 1 let ρ be the equivalence relation

$$
\rho = \Delta(E \times F) \cup \Phi(I),
$$

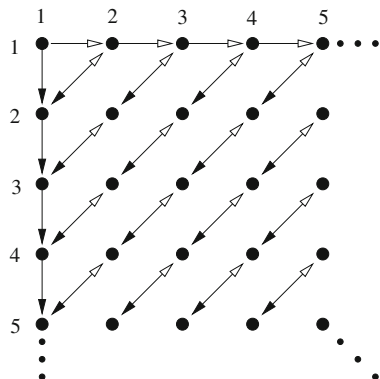where $N = \max(a + b, c + d)$ and $I = I(N + 1)$. Then for all $x \in E$ and $y \in F$

$$
(x, y) \in I \Rightarrow x + y \geq N + 1 \Rightarrow f(x) + g(y) \geq N + 1 \Rightarrow (f(x), g(y)) \in I
$$

and

$$
(x, y) \in I \Rightarrow x + y \geq N + 1 \Rightarrow g(x) + f(y) \geq N + 1 \Rightarrow (g(x), f(y)) \in I.
$$

Therefore ρ is a congruence of finite index and it separates (a, b) from (c, d).

Fig. 3 The algebra $\mathbf{E} \times \mathbf{F}$; different types of arrow correspond to the two basic operations

References

1. Howie, J.M.: Fundamentals of Semigroup Theory. Academic Press [Harcourt Brace Jovanovich Publishers], London (1995). L.M.S. Monographs, No. 7
2. McKenzie, R.N., McNulty, G.F., Taylor, W.F.: Algebras, Lattices, Varieties, vol. I. The Wadsworth & Brooks/Cole Mathematics Series. Wadsworth & Brooks/Cole Advanced Books & Software, Monterey (1987)
3. Ruškuc, N., Thomas, R.M.: Syntactic and Rees indices of subsemigroups. J. Algebra **205**(2), 435–450 (1998)