Growth of Generating Sets of Direct Powers

Nik Ruskuc

nik@mcs.st-and.ac.uk

School of Mathematics and Statistics, University of St Andrews

Glasgow, 30 September 2009

University of St Andrews

James Wiegold (1934–2009)

Theorem. (E.F. Robertson, NR, J. Wiegold, 1998)
Let S and T be two infinite semigroups. The direct product $S \times T$ is finitely presented if and only if it is finitely generated and both S and T are stable.

A mini-quiz: $d(A_5)$, $d(S_5)$

Definition

The rank of an algebraic structure A 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)

The $\mathbf{d}$-sequence

Definition

The *d-sequence* of an algebraic structure A is

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

Some basic properties:

- $\mathbf{d}(A)$ is non-decreasing.
- $\mathbf{d}(A)$ is bounded above by $|A|^n$.
- Often $d(A \times B) \leq d(A) + d(B)$, in which case $\mathbf{d}(A)$ is bounded above by a linear function.

Pozzo and Vladimir Introduce Types of Growth

Very, very good	Constant
Good	Logarithmic
Middling	Linear
Poor	Exponential
Positively bad	∞

Examples

Examples

- Cyclic groups: $\mathbf{d}(C_n) = (1, 2, 3, 4, \ldots)$ (middling).
- Alternating groups: $\mathbf{d}(A_5) = (\underbrace{2, \ldots, 2}_{19}, \underbrace{3, \ldots, 3}_{1649}, 4, \ldots)$

  (Hall 1936, good).
- Zero semigroup: $\mathbf{d}(Z_2) = (1, 3, 7, 15, \ldots)$ (poor).
- Positive integers: $\mathbf{d}(\mathbb{N}) = (1, \infty, \infty, \ldots)$ (positively bad 🙂)

J Wiegold: **d**-sequences of groups

- J. Wiegold, Growth sequences of finite groups 1-5 (5 with D. Meier), J. Austral Math. Soc. 1974–1981.
- J. Wiegold and J.S. Wilson, Growth sequences of finitely generated groups, Arch. Math. (Basel) 1978.
- A.G.R. Stewart and J. Wiegold, Growth sequences of finitely generated groups II, Bull. Austral. Math. Soc. 1989.

J Wiegold: **d**-sequences of groups

For a non-trivial group G:

- $\mathbf{d}(G)$ is linear if G is non-perfect. (middling)
- $\mathbf{d}(G)$ is logarithmic if G is finite and perfect. (Good)
- $\mathbf{d}(G)$ is eventually constant if G is infinite simple.

  (very, very good )
- $\mathbf{d}(G)$ is bounded above by a logarithmic function if G is infinite and perfect.

$\mathbf{d}(G^n) \leq d(G) + 1$ (G infinite simple)

We begin with a technical lemma whose proof is easier to describe on a blackboard than it is to consign to print. (J Wiegold, 1978)

Functional completeness

Definition
An algebraic structure A is functionally complete if every function $A^n \to A$ can be expressed in terms of the basic operations and elements of A.

Example
The boolean algebra $\{0, 1\}$ is functionally complete.

Example
The cyclic group $\mathbb{Z}_2 = \{0, 1\}$ is not functionally complete.

Theorem (MR Quick, NR)
If A is finite functionally complete then $\mathbf{d}(A)$ is logarithmic.

Functionally complete classical structures

Definition

Classical structures: groups, rings, modules, algebras, Lie algebras.

Theorem (various authors)

Functionally complete finite classical structures are: non-abelian simple groups, simple rings with identity, simple algebras with identity, non-abelian simple Lie algebras.

Corollary

All of the above have logarithmic $\mathbf{d}$*-sequences.*

A dichotomy theorem from Universal Algebra

Definition

Polynomial equivalence: A, B are polynomially equivalent if and only if every operation of A can be expressed in terms of operations and elements of B, and vice versa.

Theorem (Werner; Herrmann; MR Quick, NR)

A finite simple algebraic structure A in a congruence permutable equational class is either:

- *functionally complete, in which case $\mathbf{d}(A)$ is logarithmic; or*
- *polynomially equivalent to a simple module over a finite ring with 1, and $\mathbf{d}(A)$ is linear.*

d-sequences of finite classical structures

Theorem (MR Quick, NR)

The **d***-sequence of a finite non-trivial classical structure grows either logarithmically or linearly. Those with logarithmic growth are:*

- *perfect groups,*
- *rings with* 1,
- *algebras with* 1,
- *perfect Lie algebras.*

Remark

Jump from simple to arbitrary requires more work, and a generalisation of a lovely old trick of Gaschütz, for lifting generating sets to pre-images.

Infinite classical structures

The perfect parallel with groups continues:

- Simple structures have eventually constant **d**-sequences. (Interpolation replaces functional completeness here.)
- Perfect groups and Lie algebras, rings and algebras with identity – logarithmic upper bound.
- At worst: linear.

Question

Is the identity element necessary for a good growth? Does there exist a finitely generated infinite simple ring without identity?

Wiegold on finite semigroups

J. Wiegold, Growth sequences of finite semigroups, J. Austral. Math. Soc. 1987.

Theorem

For a finite (non-group) semigroup S we have:

- $\mathbf{d}(S)$ *is linear if* S *is a monoid.*
- *otherwise* $\mathbf{d}(S)$ *is exponential.*

Polycyclic monoid

Definition

$$P_k = \langle b_i, c_i \ (i = 1, \ldots, k) \mid b_i c_i = 1, \ b_i c_j = 0 \ (i \neq j) \rangle$$

Fact

P_k ($k \geq 2$) is an infinite, congruence-free monoid.

Theorem (St Andrews Summer School 2008)

$\mathbf{d}(P_k) = (2k - 1, 3k - 1, 4k - 1, \ldots)$.

Infinite semigroups: how bad can they get?

Theorem (EF Robertson, NR, J Wiegold)

Let S, T be two infinite semigroups. $S \times T$ is finitely generated if and only if S and T are finitely generated and neither has indecomposable elements, in which case

$$d(S \times T) \leq 4d(S)d(T).$$

Corollary

If $d(S^2) < \infty$ then all S^n are finitely generated, and $\mathbf{d}(S)$ grows exponentially at worst.

Cyclic diagonal acts

Definition

A semigroup S is said to have cyclic diagonal bi-acts if for every $n \geq 1$ there exist $a_1, \ldots, a_n \in S$ such that

$$\{(sa_1t, \ldots, sa_nt) \; : \; s, t \in S^1\} = S^n.$$

Theorem

If S has cyclic diagonal bi-acts then

$$d(S^n) \leq d(S) + 1,$$

and so $\mathbf{d}(S)$ is eventually constant.

Theorem (St Andrews Summer School 2008)

For the monoid $R_{\mathbb{N}}$ of all partially recursive functions in one variable we have

$$\mathbf{d}(R_{\mathbb{N}}) = (2, 2, 2, \ldots).$$

A semigroup without identity (after Byleen 1990)

$A = \{a_1, a_2, \dots\}$, $B = \{b_1, b_2, \dots\}$ – two infinite alphabets.

Let $P = (p_{ab})_{A\times B}$ be a matrix over $A \cup B \cup \{0\}$ such that:

- Every collection of rows or columns contains every possible tuple infinitely often.
- $p_{a_i,b_i} = b_{i+1}$, $p_{a_i,b_{i+1}} = a_{i+1}$.

Define

$$S = \langle A, B \mid ab = p_{a,b} \rangle.$$

A semigroup without identity

$S = \langle A, B \mid ab = p_{a,b} \rangle.$

Theorem (MR Quick, NR)

S has the following properties:

- *it is a congruence free semigroup with 0 but with no identity;*
- *it is finitely generated;*
- *it has cyclic diagonal bi-acts.*

Corollary

There exists an infinite semigroup S without identity for which $\mathbf{d}(S)$ is eventually constant.

Corollary

There exists an infinite semigroup S without identity for which $\mathbf{d}(S)$ is (a) logarithmic; (b) linear.

A ring without identity

$S = \langle A, B \mid ab = p_{a,b} \rangle.$

$R = \mathbb{Z}_2 S / \{0, 1 \cdot 0\}.$

Theorem (MR Quick, NR)

R is a finitely generated infinite simple ring without identity, and $\mathbf{d}(R)$ is eventually constant.

Two-element structures

Post (1941) described all 2-element algebraic structures:

- 14 algebras with basic operations of arity ≤ 2.
- 9 algebras with basic operations of arity ≤ 3, with at least one ternary operation.
- Four countably infinite, 1-parameter, families of structures involving higher arities.

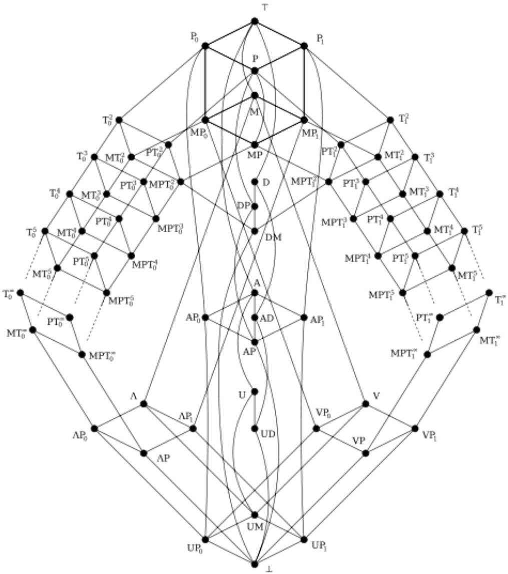
Theorem (St Andrews Summer School 2009)

If A is a two-element algebraic structure then $\mathbf{d}(A)$ is either logarithmic or linear or exponential.

Remark (Agoston et al. 1986)

There are uncountably many inequivalent algebraic structures on a 3-element set.

Post's Lattice



A selection of problems

- Does there exist an infinite simple group G and $n > 1$ such that $d(G^n) \neq d(G)$. (*One wonders whether or not these results reflect a general truth about infinite simple groups.*, J Wiegold 1978)
- If G is an infinite perfect group without finite non-trivial images, is it always the case that $\mathbf{d}(G)$ is eventually constant? (*The most important and apparently quite unattackable problem...*, J Wiegold, 1989)
- The analogous questions for rings, algebras and Lie algebras.
- Is it true that for every finite structure A, the **d**-sequence is either logarithmic, linear or exponential?
- Does there exist a semigroup S for which the growth of $\mathbf{d}(S)$ is strictly between (a) constant and logarithmic? (b) logarithmic and linear? (c) linear and exponential?

Future Directions

- Other structures: lattices, tournaments, Steiner triple systems (A Geddes, MR Quick, NR).
- Other constructions: wreath products (M Neunhöffer, MR Quick, NR).
- Number of relations; higher homological invariants.