Is an irng singly generated as an ideal?

OZAWA, Narutaka (小澤 登高)

RIMS at Kyoto University

京都大学・談話会 2012年2月

Research partially supported by JSPS & IHP

Apologies

Joint work with N. Monod and A. Thom, carried out while we were visiting at Institut Henri Poincaré in the spring 2011 for the Program "von Neumann algebras and ergodic theory of group actions."

References: arXiv:1112.1802
http://mathoverflow.net/questions/82365/

Disclaimer: Most of results are inconclusive.

The weight of a group

Throughout the talk, Γ is a countable discrete group.

We would like to estimate the *weight* (a.k.a. the killing number) of Γ,

$$w(\Gamma) := \min\{n : \Gamma \text{ is a normal closure of } n \text{ elements}\}.$$

It is notoriously difficult to find an estimate from below, except for

$$w(\Gamma) \geq w(\Gamma_{\mathrm{ab}}),$$

where $\Gamma_{\mathrm{ab}} = \Gamma/[\Gamma,\Gamma]$ is the abelianization of Γ.

Memo: If $\Gamma_{\mathrm{ab}} = \mathbb{Z}^m \oplus (\mathbb{Z}/k_1\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/k_l\mathbb{Z})$ with $k_1 \mid k_2 \mid \cdots \mid k_l$, then $w(\Gamma_{\mathrm{ab}}) = m + l$.

E.g., $(\mathbb{F}_n)_{\mathrm{ab}} = \mathbb{Z}^n$ and $w(\mathbb{F}_n) = n$.

It is also clear if $\Gamma_i \neq \mathbf{1}$ for all $i \in \mathbb{N}$, then

$$w(\Gamma_1 \times \Gamma_2 \times \cdots) = +\infty.$$

Scott–Wiegold conjecture

What can be said about the free product $\Gamma = \Gamma_1 * \Gamma_2$?

If $g_i \in \Gamma_i$ are finite order elements with $\mathrm{ord}(g_1)$ and $\mathrm{ord}(g_2)$ coprime, then one can kill both of g_1 and g_2 at once by killing $g = g_1 g_2 \in \Gamma$.

Indeed, $g_1 = g_2^{-1} = 1$ in $\Gamma/\langle\langle g \rangle\rangle$. In particular

$$w(\mathrm{PSL}_2(\mathbb{Z})) = w((\mathbb{Z}/2\mathbb{Z}) * (\mathbb{Z}/3\mathbb{Z})) = 1.$$

It seems there are no other tricks to reduce $w(\Gamma_1 * \Gamma_2)$.

Scott–Wiegold Conjecture (1976)

$$w((\mathbb{Z}/p\mathbb{Z}) * (\mathbb{Z}/q\mathbb{Z}) * (\mathbb{Z}/r\mathbb{Z})) > 1.$$

Confirmed by Howie (2002) by topological considerations on S^1, S^2 & S^3.

Generalized Scott–Wiegold Conjecture

$$w(\Gamma_1 * \Gamma_2 * \cdots * \Gamma_n) \geq n/2$$

for non-trivial (cyclic, finite, etc.) groups Γ_i.

Wiegold problem

Recall that Γ is *perfect* if $\Gamma_{\mathrm{ab}} = \mathbf{1}$.

Wiegold "Conjecture" ('70s)

Every f.g. perfect group has weight 1. Equivalently,

$$w(\Gamma_{\mathrm{ab}}) \leq w(\Gamma) \leq w(\Gamma_{\mathrm{ab}}) + 1.$$

Obviously, this is inconsistent with the previous conjecture that

$$w((\mathbb{Z}/p_1\mathbb{Z}) * \cdots * (\mathbb{Z}/p_5\mathbb{Z})) \geq 3.$$

It is also plausible that $w(\Gamma * \Gamma) > 1$ for any torsion-free (perfect) group Γ.

Still the Wiegold "conjecture" is verified for

- finite perfect groups (Wiegold),
- compactly generated locally compact perfect groups with no infinite discrete quotient (Monod–Eisenmann 2012).

Proof of Wiegold's theorem for finite perfect groups

Observation: If Γ_i perfect and $w(\Gamma_i) = 1$, then $w(\Gamma_1 \times \Gamma_2) = 1$.

Indeed, suppose $\Gamma_i = \langle g_i \rangle^{\Gamma_i}$ and let $g = (g_1, g_2) \in \Gamma_1 \times \Gamma_2$.
Then, $\forall x \in \Gamma_1\ \exists k$ such that $(x, g_2^k) \in \langle g \rangle^{\Gamma_1 \times \mathbf{1}}$.
It follows $\Gamma_1 \times \mathbf{1} = [\Gamma_1, \Gamma_1] \times \mathbf{1} \subset \langle g \rangle^{\Gamma_1 \times \mathbf{1}}$; and $\Gamma_1 \times \Gamma_2 = \langle g \rangle^{\Gamma_1 \times \Gamma_2}$.

Theorem (Wiegold)

If Γ is a finite perfect group, then $w(\Gamma) = 1$.

Proof.

By induction on $|\Gamma|$. If Γ is simple, we are done.
Otherwise, take a minimal normal subgroup $\mathbf{1} \neq N \triangleleft \Gamma$.
By the induction hypothesis, $w(\Gamma/N) = 1$ and $\exists g \in \Gamma$ s.t. $\Gamma = \langle g \rangle^{\Gamma} N$.
If $N \subset \langle g \rangle^{\Gamma}$, then $\Gamma = \langle g \rangle^{\Gamma}$; else $N \cap \langle g \rangle^{\Gamma} = \mathbf{1}$ and $\Gamma = N \times \langle g \rangle^{\Gamma}$. $\square$

From a Group Problem to a Ring Problem

Let $n \geq 3$ be fixed and R be a **rng** (i.e., a possibly non-unital ring).
$\mathrm{E}_n(R)$ is the group generated by the elementary matrices

$$e_{ij}(r) = \begin{pmatrix} 1 & & & \\ & 1 & r & \\ & & \ddots & \\ & & & 1 \end{pmatrix}, \quad r \in R \text{ and } i \neq j.$$

Steinberg relations:

- $e_{ij}(r)e_{ij}(s) = e_{ij}(r+s)$,
- $[e_{ij}(r), e_{jk}(s)] = e_{ik}(rs)$ if $i \neq k$,
- $[e_{ij}(r), e_{kl}(s)] = 1$ if $i \neq l$ and $j \neq k$.

Corollary

For every f.g. idempotent rng R (i.e., $R = \mathrm{span}(R^2)$) and $n \geq 3$, the group $E_n(R)$ is finitely generated and perfect.

idempotent rng = irng

Counterexample to Wiegold Conjecture?

Proposition (MOT)

For an irng R and $n \geq 3$, one has

$$\frac{1}{n^2} w(R) \leq w(\mathrm{E}_n(R)) \leq \left\lceil \frac{2}{n^2 - n - 2} w(R) \right\rceil.$$

Here $w(R)$ is the *weight* of R:

$$w(R) := \min\{n : R \text{ is generated by } n \text{ elements as an ideal}\}.$$

Memo:

- $w(R) \geq w(R/\operatorname{span}(R^2))$.
- If R is an irng s.t. $R = \langle\langle Z \rangle\rangle$, then $R = \operatorname{span}(RZR)$.

Proof of the first inequality.

Suppose $\mathrm{E}_n(R) = \langle\langle A_1, \ldots, A_k \rangle\rangle$, and let Z be the set of entries of $A_i - I$. Then, the canonical homomorphism $\mathrm{E}_n(R) \to \mathrm{E}_n(R/\langle\langle Z \rangle\rangle)$ kills all A_i's. It follows $R = \langle\langle Z \rangle\rangle$. □

iRng Problem

iRng Problem

Find a f.g. irng R with $w(R) > 9$ (or just $w(R) > 1$).

Theorem (Kaplansky)

R commutative f.g. irng $\Rightarrow$ R is unital and hence $w(R) = 1$.

Proof.

Suppose $R = \langle x_1, \ldots, x_n \rangle$, and let $\mathbf{x} = (x_1, \ldots, x_n)^T$.
Then, $\exists A \in \mathbb{M}_n(R)$ such that $A\mathbf{x} = \mathbf{x}$.
Let $d = \det(I - A)$ (computed in the unitization of R).

By Cramer's formula, $d\mathbf{x} = \widetilde{(I - A)}\,(I - A)\mathbf{x} = \mathbf{0}$.

This means $dx_i = 0$ for all i, and $1 - d \in R$ is a unit for R. □

Examples of irngs with weight 1

How about the free rng on n idempotents: $\langle x_1, \ldots, x_n : x_i^2 = x_i \rangle$?

Main Theorem (MOT)

If $R = \langle\langle x_1, \ldots, x_n \rangle\rangle$ and $\exists u_i \in \langle\langle x_1, \ldots, x_i \rangle\rangle$ s.t. $x_i = u_i x_i$, then $w(R) = 1$. In particular, free rngs on finitely many idempotents have weight 1.

Proof.

$$z_0 := 1 - (1 - u_n) \cdots (1 - u_3)(1 - u_2)(1 - u_1) \in R.$$

Then, $x_1 = z_0 x_1 \in \langle\langle z_0 \rangle\rangle$ and $u_1 \in \langle\langle x_1 \rangle\rangle \subset \langle\langle z_0 \rangle\rangle$. It follows

$$z_1 := 1 - (1 - u_n) \cdots (1 - u_3)(1 - u_2) \in \langle\langle z_0 \rangle\rangle$$

and $x_2 = z_1 x_2 \in \langle\langle z_0 \rangle\rangle$ and $u_2 \in \langle\langle x_1, x_2 \rangle\rangle \subset \langle\langle z_0 \rangle\rangle$. Now let

$$z_2 := 1 - (1 - u_n) \cdots (1 - u_3) \in \langle\langle z_0 \rangle\rangle$$

and repeat. □

More examples of irngs with weight 1

Theorem (MOT)

If $R = \langle\!\langle x_1, \ldots, x_n \rangle\!\rangle$ and $\exists u_i \in \langle\!\langle x_1, \ldots, x_i \rangle\!\rangle$ s.t. $x_i = u_i x_i$, then $w(R) = 1$.

Corollary

R finite irng $\Rightarrow w(R) = 1$.

$\because$ Every finite irng is generated by idempotents as an ideal.

Theorem (A. Smoktunowicz and G. M. Bergman)

Let S be a f.g. idempotent semigroup. Then S is generated as an ideal by a finite subset X_0 such that every $x \in X_0$ satisfies $x \in SxSx$.
In particular, $w(kS) = 1$ for any unital commutative ring k.

Final remarks

Recall that the *augmentation ideal* of a group Γ is

$$I_\Gamma := \ker(\varepsilon\colon \mathbb{Z}\Gamma \to \mathbb{Z}).$$

Denoting $t_g := g - 1 \in I_\Gamma$, one sees

$$t_g t_h = gh - g - h + 1 = t_{gh} - t_g - t_h.$$

It follows that I_Γ is a f.g. irng iff Γ is a f.g. perfect group.

Moreover, $\langle\!\langle t_g : g \in S \rangle\!\rangle = \ker(I_\Gamma \to I_{\Gamma/\langle\!\langle S \rangle\!\rangle})$ and hence $w(I_\Gamma) \le w(\Gamma)$.

Theorem (MOT)

To generate I_Γ as a left ideal, it needs at least $\lceil b_1^{(2)}(\Gamma) + 1 \rceil$ elements.

One line proof.

$$b_1^{(2)}(\Gamma) + 1 = \dim_\Gamma Z^1(\Gamma, \ell_2\Gamma) = \dim_\Gamma \mathrm{Hom}_{\mathbb{Z}\Gamma}(I_\Gamma, \ell_2\Gamma).$$ □

Conclusion

Wiegold Problem

Find a (f.g.) perfect group Γ such that

$$1 < w(\Gamma) < +\infty.$$

iRng Problem

Find a (f.g.) irng R such that

$$1 < w(R) < +\infty.$$

Thank you for your attention!

"RNGS" (RINGS WITHOUT UNIT)

Nathan Jacobson, **Basic Algebra I.** *W. H. Freeman & Co.*, 1974. p. 149.

2.17 "RNGS" (RINGS WITHOUT UNIT)

In most algebra books a ring is defined to be non-vacuous set R equipped with two binary compositions $+$ and $\cdot$ and an element 0 such that $(R, +, 0)$ is an abelian group, $(R, \cdot)$ is a semigroup (p. 28), and the distributive laws hold. In other words, the existence of a unit for multiplication is not assumed. We shall consider these systems briefly, and so as not to conflict with our old terminology we adopt a different term: *rngs*[6] for the structures which are not assumed to have units. We remark first that the elementary properties of rings which we noted in section 2.1 (generalized associativity, generalized distributivity, rules for multiples, etc.) carry over to rngs. The verification of this is left to the reader. We shall now show that any rng can be imbedded in a ring. This fact permits the reduction of most questions on rngs to the case of rings.

---

[6] Suggested pronunciation: rŭng. This term was suggested to me by Louis Rowen.