Universal CA groups with few generators

Ville Salo
vosalo@utu.fi

February 28, 2020

Abstract

There exist f.g.-universal cellular automata groups which are quotients of $\mathbb{Z} * \mathbb{Z}_2$ or $\mathbb{Z}_2 * \mathbb{Z}_2 * \mathbb{Z}_2$, as previously conjectured by the author.

The following was stated in [3]: "We conjecture that three involutions can generate an f.g.-universal group of RCA." We confirm this, and also minimize the size of generating sets for f.g.-universal cellular automata groups.

The group $\mathrm{RCA}(m)$ is the group of self-homeomorphisms f of $\{0,1,..,m-1\}^{\mathbb{Z}}$ satisfying $f \circ \sigma = \sigma \circ f$, where $\sigma(x)_i = x_{i+1}$ is the left shift.

Theorem 1. *Let $G' \in \{\mathbb{Z}*\mathbb{Z}_2, \mathbb{Z}_2*\mathbb{Z}_2*\mathbb{Z}_2\}$ and let $m, n \geq 2$ be arbitary. There is a homomorphism $\phi : G' \to \mathrm{RCA}(m)$ such that $\phi(G')$ contains an embedded copy of every finitely-generated group of $\mathrm{RCA}(n)$.*

Proof. First consider $G' = \mathbb{Z} * \mathbb{Z}_2$. To show this for all $m, n \geq 2$, it suffices to show it for some $m, n \geq 2$, by [1]. We let B with $|B| \geq 2$ be arbitrary and $C = \{0, 1\}$ and use the alphabet $A = B \times C$, with $B^{\mathbb{Z}}$ the "top track" and $C^{\mathbb{Z}}$ the "bottom track". By [3], there exists a finitely-generated group H of cellular automata containing a copy of every finitely-generated group of cellular automata. By Lemma 7 in [3] (more precisely, its proof), for any large enough ℓ and unbordered word $|w| = \ell$, if a group $G \leq \mathrm{RCA}(B \times C)$ contains

$$\pi|_{[w]_i} \text{ and } \pi|_{[ww]_i}$$

for all $\pi \in \mathrm{Alt}(\{0,1\}^\ell)$ and all $i \in \mathbb{Z}$, then G contains a copy of H. The notation $\pi|_{[u]_i}$ is as in Definition 2 of [3], and means that we apply π on the second track if and only if u appears on the first track, with offset i.

Now, let $w \in B^\ell$ be unbordered where ℓ is as above, and very large. We construct a 2-generated group G containing the maps $\pi|_{[w]_i}$ and $\pi|_{[ww]_i}$, such that one of our generators is an involution.

Let $F : \{0,1\}^n \to \{0,1\}^n$ be a function such that $F^2 = \mathrm{id}|_{\{0,1\}^n}$ and defining $f : \{0,1\}^{\mathbb{Z}} \to \{0,1\}^{\mathbb{Z}}$ by $f(x.wy) = x.F(w)y$, the maps $\sigma^i \circ f \circ \sigma^{-i}$ generate the group of all self-homeomorphisms g of $\{0,1\}^{\mathbb{Z}}$ for which there exists m such that

$$\forall x \in \{0,1\}^{\mathbb{Z}} : \forall |i| \geq m : g(x)_i = x_i$$

holds. Such F exists [2].

Our generators are the partial shift on the first track, i.e. $\sigma_1(x, y) = (\sigma(x), y)$, and the map $f_0 = F|_{[w]_0}$. Let

$$G = \langle \sigma_1, F|_{[w]_0} \rangle.$$

Note that $f_i = F|_{[u]_{-i}} = f_0^{\sigma_1^i} \in G$.

Let F' be any finite set of even permutations of sets of the form $\{0,1\}^k$ such that every even permutation of $\{0,1\}^m$ for any large enough m can be decomposed into application of permutations in F' in contiguous subsequences $\{i, i+1, ..., i+k-1\}$ of the indices $\{0, 1, ..., m-1\}$. It is well-known that there exist such universal reversible gate sets. Note that $\{F\}$ need not be such a set: we may need to use more than m coordinates to build permutations of $\{0,1\}^m$ using translates of F.

For any i, since w is unbordered and of length ℓ, the maps $f_i, f_{i+1}, ..., f_{i+\ell-n}$ compose in the natural way, just like translates of F inside $\{0,1\}^\ell$. By universality of F, as long as ℓ is large enough, the maps $f'|_{[w]_i}$, $f' \in F'$, are generated. By the universality property of F', we have $\pi|_{[w]_i} \in G$ for all $\pi \in \mathrm{Alt}(\{0,1\}^\ell)$.

Now, we need to show that also $\pi|_{[ww]_i} \in G$. For this, pick a large *mutually unbordered* set $U \subset \{0,1\}^\ell$, i.e. any set such that $u_1, u_2 \in U$ have no nontrivial overlaps. For example we can pick $U = 0^{\ell-k-2}1\{0,1\}^k 1$ for any k such that $k < \frac{\ell-4}{2}$. By the above, we can perform any even permutation of U under occurrences of w. For two permutations $\pi_1, \pi_2 \in \mathrm{Alt}(\{0,1\}^\ell)$, with supports contained in U, a direct computation shows

$$[\pi_1|_{[w]_i}, \pi_2|_{[w]_{i+\ell}}] = [\pi_1, \pi_2]|_{[ww]_i},$$

so for $|U| \geq 5$ (ℓ has to be large enough for this) we have $\pi|_{[ww]_i} \in G$ for all $\pi \in \mathrm{Alt}(\{0,1\}^\ell)$ with support contained in U.

For two permutations $\pi_1, \pi_2 \in \mathrm{Alt}(\{0,1\}^\ell)$, a direct computation shows

$$(\pi_1|_{[ww]_i})^{\pi_2|_{[w]_i}} = (\pi_1^{\pi_2})|_{[ww]_i}$$

so, since $\mathrm{Alt}(\{0,1\}^\ell)$ is simple (supposing $\ell \geq 3$), G in fact contains $\pi|_{[ww]_i} \in G$ for all $\pi \in \{0,1\}^\ell$. This concludes the proof since G is clearly a quotient of $G' = \mathbb{Z} * \mathbb{Z}_2$, as it was generated by an RCA of infinite order and an involution.

Let us then show the claim for $G' = \mathbb{Z}_2 * \mathbb{Z}_2 * \mathbb{Z}_2$. For this, pick $B = \{0,1\}$ and add a third component $B' = \{0,1\}$ on top, so the alphabet becomes $A = B' \times B \times C$, $m = 8$. Thinking of $x \in (B' \times B \times C)^\mathbb{Z}$ as having three binary tracks, and writing σ_0 and σ_1 for the shifts on the first two tracks, it is easy to see that $\sigma_0^{-1} \times \sigma_1$ is the composition of two involutions, say $\sigma_0^{-1} \times \sigma_1 = a \circ b$.

In the proof of universality in [3], the shift on the first (B-)track is only used to construct the generators of an arbitrary f.g. group, but total sum of shifts is 0 in the elements giving the embedding. Thus, $G = \langle a, b, f_0 \rangle$, where f_0 is as above but ignores the B'-track, is clearly f.g.-universal, and a quotient of G'. □

References

[1] K. H. Kim and F. W. Roush. On the automorphism groups of subshifts. *Pure Mathematics and Applications*, 1(4):203–230, 1990.

[2] V. Salo. Universal gates with wires in a row. *ArXiv e-prints*, September 2018.

[3] V. Salo. Universal groups of cellular automata. *ArXiv e-prints*, August 2018. Available at `https://arxiv.org/abs/1808.08697`.