

# Finite generating sets for reversible gate sets under general conservation laws<sup>☆,☆☆</sup>

Tim Boykett<sup>a</sup>, Jarkko Kari<sup>b</sup>, Ville Salo<sup>b</sup>

<sup>a</sup> Institute for Algebra, Johannes Kepler University Linz, Austria and Time's Up Research, Linz, Austria.

<sup>b</sup> Department of Mathematics and Statistics, University of Turku, Finland.

## Abstract

It is well-known that the Toffoli gate and the negation gate together yield a universal gate set, in the sense that every permutation of  $\{0, 1\}^n$  can be implemented as a composition of these gates. Since every bit operation that does not use all of the bits performs an even permutation, we need to use at least one auxiliary bit to perform every permutation, and it is known that one bit is indeed enough. Without auxiliary bits, all even permutations can be implemented. We generalize these results to non-binary logic: For any finite set  $A$ , a finite gate set can generate all even permutations of  $A^n$  for all  $n$ , without any auxiliary symbols. This directly implies the previously published result that a finite gate set can generate all permutations of  $A^n$  when the cardinality of  $A$  is odd, and that one auxiliary symbol is necessary and sufficient to obtain all permutations when the cardinality of  $A$  is even. We also consider the conservative case, that is, those permutations of  $A^n$  that preserve the weight of the input word. The weight is the vector that records how many times each symbol occurs in the word or, more generally, the image of the word under a fixed monoid homomorphism from  $A^*$  to a commutative monoid. It turns out that no finite conservative gate set can, for all  $n$ , implement all conservative even permutations of  $A^n$  without auxiliary bits. But we provide a finite gate set that can implement all those

<sup>☆</sup>The authors would like to acknowledge the contribution of the COST Action IC1405. This work was partially funded by SFB Project F5004 of the Austrian Science Foundation, FWF, by the Academy of Finland grant 296018, and by FONDECYT research grant 3150552.

<sup>☆☆</sup>A preliminary version of this work was presented at the 8th International Conference on Reversible Computation, RC 2016 [3].

conservative permutations that are even within each weight class of  $A^n$ .

*Keywords:* reversible gates, reversible circuits, universal gates, conservative gates, reversible clones

---

## 1. Introduction

The study of reversible and conservative binary gates was pioneered in the 1970s and 1980s by Toffoli and Fredkin [4, 10]. Recently, Aaronson, Greier and Schaeffer [1] described all binary gate sets closed under the use of auxiliary bits, as a prelude to their eventual goal of classifying these gate sets in the quantum case. It has been noted that ternary gates have similar, yet distinct properties [12].

In this article, we consider the problem of finitely-generatedness of various families of reversible logic gates without using auxiliary bits. In the case of a binary alphabet, it is known that the whole set of reversible gates is not finitely generated in this strong sense, but the family of gates that perform an even permutation of  $\{0, 1\}^n$  is [1, 6, 11]. In [12], it is shown that for the ternary alphabet, the whole set of reversible gates is finitely generated. In [5] the result is announced for all odd alphabets, with a proof attributed to personal communication, which has recently been published as [8]. Another proof of this fact can be found in [2]. In this paper, we look at gate sets with arbitrary finite alphabets, and prove the natural generalization: the whole set of reversible gates is finitely generated if and only if the alphabet is odd, and in the case of an even alphabet, the even permutations are finitely generated.

In [11], it is proved that in the binary case the conservative gates, reversible gates that preserve the numbers of symbols in the input (that is, its weight), are not finitely generated, even with the use of ‘borrowed bits’, bits that may have any initial value but must return to their original value in the end. On the other hand, it is shown that with bits whose initial value is known (and suitably chosen), all permutations can be performed. We prove for all alphabets that the gates that perform an even permutation in every weight class are finitely generated, but the whole class of conservative permutations is far from being finitely generated (which implies in particular the result of [11]).

We also consider more general conservation laws for gates. Assign to each letter of the alphabet as its weight an element of an arbitrary commutative

monoid. We say that a reversible gate conserves this assignment if the sum in the monoid of the weights of the input symbols always equals the sum of the weights of the output symbols. This concept generalizes both the conservative gates and the unrestricted reversible gates. We prove that the generalized conservative gates that perform an even permutation in each weight class are finitely generated. In contrast, the whole conservative class without the evenness requirement is not finitely generated, provided there are sufficiently many non-trivial weight classes available. This general result implies the special cases above.

Our methods are rather general, and the proofs in all cases follow the same structure. The negative aspect of these methods is that our universal gates are not the usual ones, and for example in the conservative case, one needs a bit of work (or computer time) to construct our universal gate family from the Fredkin gate.

We start by introducing our terminology, taking advantage of the concepts of clone theory [9] applied to bijections as developed in [2], leading to what we call *reversible clones* or *revclones*, and *reversible iterative algebras* or *revitals*. We note in passing that one can also use category-theoretic terminology to discuss the same concepts, and this is the approach taken in [5, 6]. In this terminology, what we call revitals are strict symmetric monoidal groupoids in the category where objects are sets of the form  $A^n$  and the horizontal composition rule is given by Cartesian product. A formal difference is that unlike morphism composition in a category, our composition operation is total.

We generalize the idea of the Toffoli gate and Fredkin gate to what we call *controlled permutations* and prove a general induction lemma showing that if we can add a single new control wire to a controlled permutation, we can add any number of control wires. We then show two combinatorial results about permutation groups that allow us to simplify arguments about revitals. This allows us to describe generating sets for various revclones and revitals of interest, with the indication that these results will be useful for more general revital analysis, as undertaken for instance in [1]. While theoretical considerations show that finite generating sets do not exist in some cases, in other cases explicit computational searches are able to provide small generating sets.

## 2. Background

Let  $A$  be a finite set. We write  $S_A$  or  $\text{Sym}(A)$  for the group of permutations or bijections of  $A$ ,  $S_n$  for  $\text{Sym}(\{1, \dots, n\})$  and  $\text{Alt}(A)$  for the group of even permutations of  $A$ ,  $A_n = \text{Alt}(\{1, \dots, n\})$ . Let  $B_n(A) = \{f : A^n \rightarrow A^n \mid f \text{ a bijection}\} = \text{Sym}(A^n)$  be the group of  $n$ -ary bijections on  $A^n$ , and let  $B(A) = \cup_{n \in \mathbb{N}} B_n(A)$  be the collection of all bijections on powers of  $A$ . We call them *gates*. For  $f \in B_n(A)$ , we denote by  $f_i : A^n \rightarrow A$  the  $i$ 'th component of gate  $f$ , so that  $f(x_1, \dots, x_n) = (f_1(x_1, \dots, x_n), \dots, f_n(x_1, \dots, x_n))$ .

We denote by  $\langle X \rangle$  the group generated by  $X \subseteq B_n(A)$ , a subgroup of  $B_n(A)$ . As  $B_n(A)$  is a finite group,  $\langle X \rangle$  is also the monoid generated by  $X$ , that is, it consists of all compositions of functions in  $X$ . All our compositions are from right to left, so that  $f \circ g : x \mapsto f(g(x))$ . For consistency, elements of permutation groups are then multiplied from right to left as well.

Each  $\alpha \in S_n$  defines a *wire permutation*  $\pi_\alpha \in B_n(A)$  that permutes the coordinates of its input according to  $\alpha$ :

$$\pi_\alpha(x_1, \dots, x_n) = (x_{\alpha^{-1}(1)}, \dots, x_{\alpha^{-1}(n)}).$$

The wire permutation  $id_n = \pi_{()}$  corresponding to the identity permutation  $() \in S_n$  is the  $n$ -ary identity map. Conjugating  $f \in B_n(A)$  with a wire permutation  $\pi_\alpha \in B_n(A)$  gives  $\pi_\alpha \circ f \circ \pi_\alpha^{-1}$ , which we call a *rewiring* of  $f$ . Rewirings of  $f$  correspond to applying  $f$  on arbitrarily ordered input wires, that is, the rewiring  $g = \pi_\alpha \circ f \circ \pi_\alpha^{-1}$  satisfies  $(g_{\alpha(1)}(x), \dots, g_{\alpha(n)}(x)) = f(x_{\alpha(1)}, \dots, x_{\alpha(n)})$  for all  $x = (x_1, \dots, x_n)$ .

Any  $f \in B_\ell(A)$  can be extended to  $A^n$  for  $n > \ell$  by applying it on any selected  $\ell$  coordinates while leaving the other  $n - \ell$  coordinates unchanged. Using the clone theory derived terminology in [2] we first define, for any  $f \in B_n(A)$  and  $g \in B_m(A)$ , the parallel application  $f \oplus g \in B_{n+m}(A)$  by

$$(f \oplus g)(x_1, \dots, x_{n+m}) = (f_1(x_1, \dots, x_n), \dots, f_n(x_1, \dots, x_n), \\ g_1(x_{n+1}, \dots, x_{n+m}), \dots, g_m(x_{n+1}, \dots, x_{n+m})).$$

Then the *extensions* of  $f \in B_\ell(A)$  on  $A^n$  are the rewirings of  $f \oplus id_{n-\ell}$ .

Let  $P \subseteq B(A)$ . We denote by  $[P] \subseteq B(A)$  the set of gates that can be obtained from the identity  $id_1$  and the elements of  $P$  by compositions of gates of equal arity and by extensions of gates of arities  $\ell$  on  $A^n$ , for  $n \geq \ell$ . Clearly  $P \mapsto [P]$  is a closure operator. Sets  $C \subseteq B(A)$  such that  $C = [C]$  are called *reversible iterative algebras*, or *revitals*, for short. We say that gate set  $P$

*generates* revitai  $C$  if  $C = \lceil P \rceil$ . We say that revitai  $C$  is *finitely generated* if there exists a finite set  $P$  that generates it.

For example, the revitai  $\lceil \pi_{(1\ 2)} \rceil$  generated by a single wire swap  $\pi_{(1\ 2)}$  is exactly the set of all wire permutations. Note that a revitai is not required to contain wire permutations; revitais that contain all wire permutations are known as *reversible clones* or *revclones* in clone theory [2].

We sometimes refer to general elements of  $B_n(A)$  as *word permutations* to distinguish them from the wire permutations. In particular, by a wire swap we mean a function  $f : A^2 \rightarrow A^2$  with  $f(a, b) = (b, a)$  for all  $a, b \in A$  (or an extension of such a function), while a word swap refers to a permutation  $(u\ v) \in B_n(A)$  that swaps two individual words of the same length. Of course, a wire swap is a composition of word swaps, but the converse is not true. Similarly, and more generally, we talk about *wire and word rotations*. A *symbol permutation* is a permutation of  $A$ .

We are interested in finding out if some naturally arising revitais are finitely generated. First of all, we have the *full revitai*  $B(A)$  and the *alternating revitai*  $\text{Even}(A) = \bigcup_n \text{Alt}(A^n)$  that contains all even permutations.

We also consider permutations that conserve the letters in their inputs. For any  $n \in \mathbb{N}$ , define  $w_n : A^n \rightarrow \mathbb{N}^A$ , such that for all  $x \in A^n$ ,  $a \in A$ ,  $w_n(x)(a)$  the number of occurrences of  $a$  in  $x$ . We say  $w_n(u)$  is the *weight* of the word  $u$ . A mapping  $f \in B_n(A)$  is *conservative* if for all  $x \in A^n$ ,  $w_n(f(x)) = w_n(x)$ , we let  $\text{Cons}_n(A) \subseteq B_n(A)$  be the set of conservative maps of arity  $n$ . Then  $\text{Cons}(A) = \bigcup_{n \in \mathbb{N}} \text{Cons}_n(A)$  is the *conservative revitai*. We also consider the set of conservative permutations that perform an even permutation on each weight class, denoted by  $E\text{Cons}(A)$ , called the *alternating conservative revitai*.

We also investigate a more general concept of conservation. Let  $M$  be a commutative monoid and let  $\phi : A^* \rightarrow M$  be a monoid homomorphism. *Weight classes* under  $\phi$  consist of words of equal length having the same value under  $\phi$ . Without loss of generality we may assume that  $\phi$  also records the length of the input word in the sense that  $|x| \neq |y| \Rightarrow \phi(x) \neq \phi(y)$ . Indeed, if needed we can replace  $\phi$  with the length-recording homomorphism  $x \mapsto (\phi(x), |x|)$  from  $A^*$  to  $M \times \mathbb{N}$  that has the same weight classes as  $\phi$ .

A mapping  $f \in B_n(A)$  is  $\phi$ -*conservative* if  $\phi(f(x)) = \phi(x)$  holds for all  $x \in A^n$ . Such  $f$  performs a permutation on each weight class. We let  $\text{Cons}_n^\phi(A) \subseteq B_n(A)$  be the set of  $\phi$ -conservative maps of arity  $n$ . Then  $\text{Cons}^\phi(A) = \bigcup_{n \in \mathbb{N}} \text{Cons}_n^\phi(A)$  is the  $\phi$ -*conservative revitai*. We also consider  $\phi$ -conservative permutations that perform an even permutation on each weight

class. We denote the set of such alternating  $\phi$ -conservative permutations by  $ECons^\phi(A)$ , and call it the *alternating  $\phi$ -conservative revival*.

Note that  $Cons(A) = Cons^\phi(A)$  and  $ECons(A) = ECons^\phi(A)$  for the homomorphism  $\phi : A^* \rightarrow \mathbb{N}^A$  that counts the numbers of occurrences of letters in a word, that is,  $\phi|_{A^n} = w_n$  for all  $n \in \mathbb{N}$ . Also note that  $B(A) = Cons^\phi(A)$  and  $Even(A) = ECons^\phi(A)$  for the length homomorphism  $\phi : x \mapsto |x|$  from  $A^*$  to  $\mathbb{N}$ . The weight classes of this homomorphism are namely the full sets  $A^n$ . This also means that some of the results concerning the full, the alternating, the conservative and the alternating conservative revivals follow from our more general results for arbitrary  $\phi$ -conservative revivals. However, we include the proofs for these special cases as gentle preludes to the general case.

Using the terminology in [11], we say that gate  $f \oplus id_k \in B_{n+k}(A)$  computes  $f \in B_n(A)$  using  $k$  *borrowed* bits. The borrowed bits are auxiliary symbols in the computation of  $f$  that can have arbitrary initial values, and at the end these values must be restored unaltered. Regardless of the initial values of the borrowed bits, the permutation  $f$  is computed on the other  $n$  inputs. We have cases where borrowed bits help (Corollary 22) and cases where they don't (Theorem 27).

### 3. Induction Lemma

In this section, we introduce the concept of controlled gate, a generalisation of the Toffoli and Fredkin gates. With this definition, we are able to formulate a useful induction lemma. This lemma formalizes the following idea. If we can build an  $(n+1)$ -ary controlled gate in a certain class from gates of arity  $n$ , then by replacing each  $n$ -ary gate with its  $(n+1)$ -ary extension, we have a “spare” control line from each  $n+1$  gate, which can then be attached to an extra control input to get an  $(n+2)$ -ary gate.

**Definition 1.** Let  $k \in \mathbb{N}$  and  $P \subseteq B_\ell(A)$ . For  $w \in A^k$  and  $p \in P$ , define the function  $f_{w,p} : A^{k+\ell} \rightarrow A^{k+\ell}$  by

$$f_{w,p}(uv) = \begin{cases} uv & \text{if } u \neq w \\ up(v) & \text{if } u = w \end{cases}$$

where  $u \in A^k$ ,  $v \in A^\ell$ . The functions  $f_{w,p}$ , and more generally their rewirings  $\pi_\alpha \circ f_{w,p} \circ \pi_\alpha^{-1}$  for  $\alpha \in S_{k+\ell}$ , are called *k-controlled P-permutations*, and we denote this set of functions by  $CP(k, P) \subseteq B_{k+\ell}(A)$ . We refer to  $CP(P) = \bigcup_k CP(k, P)$  as *controlled P-permutations*.

When  $P$  is a named family of permutations, such as the family of all swaps in  $S_A$ , we usually talk about ‘ $k$ -controlled swaps’ instead of ‘controlled swap permutations’. These are word swaps rather than wire swaps. The Toffoli gate is a (particular) 2-controlled symbol permutation, while the Fredkin gate is a (particular) 1-controlled wire swap. Note that the ‘ $k$ ’ in ‘ $k$ -controlled’ refers to the fact that the number of controlling wires is  $k$ . Of course, sometimes we want to talk about also the particular word  $w$  in  $f_{w,p}(uv)$ . To avoid ambiguity, we say such  $f_{w,p}(uv)$  is *w-word controlled permutation*. In particular, the Toffoli gate is the 11-word controlled symbol permutation, while the Fredkin gate is a 1-word controlled wire swap.

The following lemma formalizes the idea of adding new common control wires to all gates in a circuit.

**Lemma 1.** *Let  $k, h, \ell \in \mathbb{N}$ ,  $P \subseteq B_\ell(A)$  and  $Q \subseteq B_n(A)$ . If  $CP(h, Q) \subseteq [CP(k, P)]$ , then  $CP(h+m, Q) \subseteq [CP(k+m, P)]$  for all  $m \in \mathbb{N}$ .*

PROOF. Consider an arbitrary  $f \in CP(h+m, Q)$ . Let  $uv \in A^{h+m}$  be its control word where  $u \in A^m$  and  $v \in A^h$ , and let  $p \in Q$  be its permutation. By the hypothesis,  $f_{v,p}$  can be implemented by maps in  $CP(k, P)$ . In all their control words, add the additional input  $u$ . This implements  $f$  as a composition of maps in  $CP(k+m, P)$ , as required.  $\square$

The main importance of the lemma comes from the following corollary:

**Lemma 2 (Induction Lemma).** *Let  $P \subseteq B_\ell(A)$  be such that  $CP(k+1, P) \subseteq [CP(k, P)]$  for some  $k \in \mathbb{N}$ . Then  $[CP(m, P)] \subseteq [CP(n, P)]$  for all  $m \geq n \geq k$ .*

PROOF. We apply Lemma 1, setting  $Q = P$  and  $h = k+1$ . We obtain that  $CP(k+m+1, P) \subseteq [CP(k+m, P)]$  for all  $m \in \mathbb{N}$ . As  $[\cdot]$  is a closure operator we have that  $[CP(k+m+1, P)] \subseteq [CP(k+m, P)]$  for all  $m \in \mathbb{N}$ . Hence

$$[CP(k, P)] \supseteq [CP(k+1, P)] \supseteq [CP(k+2, P)] \supseteq \dots$$

which clearly implies the claimed result.  $\square$

By the previous lemma, in order to show that a revital  $C$  is finitely generated, it is sufficient to find some  $P \subseteq B_\ell(A)$  such that

- (i)  $\langle CP(m, P) \rangle = C \cap B_{m+\ell}(A)$  for all large enough  $m$ , and
- (ii)  $CP(k+1, P) \subseteq [CP(k, P)]$  for some  $k$ .

Indeed, if  $n \geq k$  is such that (i) holds for all  $m \geq n$  then,

$$C \cap B_{m+\ell}(A) = \langle CP(m, P) \rangle \subseteq [CP(m, P)] \subseteq [CP(n, P)],$$

where the last inclusion follows from (ii) and the Induction lemma. Note that by (i) we also have  $CP(n, P) \subseteq C$ . So the finite subset  $CP(n, P)$  of  $C$  generates all but finitely many elements of  $C$ .

Condition (i) motivates the following definition.

**Definition 2.** Let  $C$  be a revital. We say that a set of permutations  $P \subseteq B_\ell(A)$  is *n-control-universal* for  $C$  if  $\langle CP(n - \ell, P) \rangle = C \cap B_n(A)$ . More generally, a set  $P \subseteq B(A)$  that may contain gates of different arities, is *n-control-universal* for  $C$  if

$$\left\langle \bigcup_{\ell} \bigcup_{f \in B_\ell(A) \cap P} CP(n - \ell, P) \right\rangle = C \cap B_n(A).$$

If  $P$  is *n-control-universal* for all large enough  $n$ , we say it is *control-universal* for  $C$ .

In the next two sections we find gate sets that are control-universal for revitals of interest.

#### 4. Some combinatorial group theory

In this section, we prove some basic results that the symmetric group is generated by any ‘connected’ family of swaps, and the alternating group by any ‘connected’ family of 3-cycles. Similar results are folklore in combinatorial group theory, but we include full proofs for completeness’ sake.

A *hypergraph* is a set  $V$  of vertices and a set  $E$  of edges,  $E \subseteq \mathcal{P}(V)$ . A  $k$ -hypergraph is a hypergraph where every edge has the same size,  $k$ . A 2-hypergraph is a standard (undirected) graph. A *path* is a series of vertices  $(v_1, \dots, v_n)$  such that for each pair  $(v_i, v_{i+1})$  there is an edge  $e_i \in E$  such that  $\{v_i, v_{i+1}\} \subseteq e_i$ . Two vertices  $a, b \in V$  are *connected* if there is a path  $(v_1, \dots, v_n)$  with  $v_1 = a$  and  $v_n = b$ . The relation of being connected is an equivalence relation and induces a partition of the vertices into *connected components*.

If  $H$  is a 3-hypergraph, write  $\text{Graph}(H)$  for the underlying graph of  $H$ :  $V(\text{Graph}(H)) = V(H)$  and  $\{a, b\} \in E(\text{Graph}(H)) \iff \exists c : \{a, b, c\} \in E(H)$ . Note that by our definition, the connected components of a 3-hypergraph  $H$  are precisely the connected components of  $\text{Graph}(H)$ .

**Swap group.** Let  $H$  be a graph with nodes  $V(H)$  and edges  $E(H)$ . The *swap group*  $SG(H)$  is the group  $G \leq \text{Sym}(V(H))$  generated by swaps  $(a\ b)$  with  $\{a, b\} \in E(H)$ .

**Lemma 3.** *Let  $H$  be a graph with connected components  $H_1, \dots, H_k$ . Then*

$$SG(H) = \text{Sym}(V(H_1)) \times \cdots \times \text{Sym}(V(H_k))$$

PROOF. All of the swaps act in one of the components and there are no relations between them. Thus, the swap group is the direct product of some permutation groups of the connected components. We only need to show that in each connected component  $H_i$ , we can realize any permutation of vertices. Since swaps generate the symmetric group, it is enough to show that if  $a, b \in V(H_i)$  then the swap  $(a\ b)$  is in  $SG(H)$ . For this, let  $a = a_1, a_2, \dots, a_\ell = b$  be a path from  $a$  to  $b$ . Then

$$(a, b) = (a_1\ a_2)(a_2\ a_3) \cdots (a_{\ell-2}\ a_{\ell-1})(a_\ell\ a_{\ell-1})(a_{\ell-1}\ a_{\ell-2}) \cdots (a_3\ a_2)(a_2\ a_1).$$

□

**Cycling group.** Let  $H$  be a 3-hypergraph with nodes  $V(H)$  and hyperedges  $E(H)$ . The *cycling group*  $CG(H)$  of  $H$  is the group  $G \leq \text{Sym}(V(H))$  generated by cycles  $(a\ b\ c)$  where  $\{a, b, c\} \in E(H)$ .

The following observation allows us to take any element of the alternating group given two 3-hyperedges that intersect in one or two places.

**Lemma 4.**

$$\begin{aligned} A_4 &= \langle (1\ 2\ 3), (2\ 3\ 4) \rangle, \\ A_5 &= \langle (1\ 2\ 3), (3\ 4\ 5) \rangle. \end{aligned}$$

**Lemma 5.** *Let  $H$  be a hypergraph, and let the connected components of  $H$  be  $H_1, \dots, H_k$ . Then*

$$CG(H) = \text{Alt}(V(H_1)) \times \text{Alt}(V(H_2)) \times \cdots \times \text{Alt}(V(H_k)).$$

PROOF. We prove the claim by induction on the number of hyperedges. If there are no hyperedges, then  $CG(H) = \{\text{id}(V(H))\}$ , as required. Now, suppose that the claim holds for a hypergraph  $H'$  and  $H$  is obtained from  $H'$  by adding a new hyperedge  $\{a, b, c\}$ . If none of  $a, b, c$  are part of a hyperedge of  $H'$  or are fully contained in a connected component of  $\text{Graph}(H')$ , then the claim is trivial, as either we add a new connected component and by definition add its alternating group  $\text{Alt}_3 \cong \langle (a \ b \ c) \rangle$  to  $CG(H)$ , or we do not modify the connected components at all.

Every permutation on the right side of the equality we want to prove decomposes into even permutations in the components. We thus only have to show that a pair of swaps  $(x \ y)(u \ v)$  can be implemented for any vertices  $x, y, u, v$  that are in the same component in  $H$ . In components that do not intersect  $\{a, b, c\}$ , we can implement this permutation by assumption. If  $x, y, u, v \in \{a, b, c\}$ , the permutation is in  $CG(H)$  by definition. Since  $(x \ y)(u \ v) = (x \ y)(a \ b)^2 (u \ v)$  it is enough to implement the permutation  $(a \ b)(u \ v)$ .

Now, we have two cases (up to reordering variables). Either  $u \in \{a, b, c\}$  and  $v \notin \{a, b, c\}$  or  $\{u, v\} \cap \{a, b, c\} = \emptyset$ . By analysing cases, the claim reduces to the  $\text{Alt}_5$  or the  $\text{Alt}_4$  situation of the previous Lemma.  $\square$

## 5. Control-universality

Recall control-universality from Definition 2: a set of permutations  $P$  is control-universal for revitil  $C$  if, for all sufficiently large  $n$ , the  $n$ -ary gates in  $C$  are precisely the compositions of  $n$ -ary controlled  $P$ -permutations. As corollaries of the previous section, we will now find control-universal families of gates for our revitils of interest: the full revitil  $B(A) = \bigcup_n \text{Sym}(A^n)$ , the conservative revitil  $Cons(A)$  and the more general  $\phi$ -conservative revitil  $Cons^\phi(A)$ , the alternating revitil  $Even(A) = \bigcup_n \text{Alt}(A^n)$  and the alternating conservative revitil  $ECons(A)$  and its generalization alternating  $\phi$ -conservative revitil  $ECons^\phi(A)$ . Corollaries 7, 9, 11, 13, 15 and 17 below provide control-universal gate sets for these revitils. In each case the result is obtained by first constructing an appropriate graph (or 3-hypergraph) whose edges (hyperedges) correspond to controlled swaps (controlled 3-cycles) using  $P$ . With the help of Lemma 3 (or Lemma 5, respectively) one can then conclude that all permutations (even permutations, respectively) in appropriate sets can be generated.

Note that, as discussed at the end of this section, the results concerning the generalized conservative gates, presented as items (b $^\phi$ ) and (d $^\phi$ ) below, imply the results on the unrestricted and on the standard conservative gates, presented as items (a), (b), (c) and (d). These weaker results are included as an introduction to our method.

**(a) The full revital  $B(A)$ .** Define the graph  $G_{A,n}^{(1)}$  that has nodes  $A^n$  and edges  $\{u, v\}$  where the Hamming distance between  $u$  and  $v$  is one. The following is obvious:

**Lemma 6.** *The graph  $G_{A,n}^{(1)}$  is connected.*

Let  $P_1 = \{(a b) \mid a, b \in A\} \subseteq B_1(A)$ , the set of symbol swaps. The swap group of  $G_{A,n}^{(1)}$  is then contained in  $\langle CP(n-1, P_1) \rangle \subseteq \text{Sym}(A^n)$ . By Lemmas 3 and 6 the swap group is  $\text{Sym}(A^n)$ , so  $\langle CP(n-1, P_1) \rangle = \text{Sym}(A^n)$ . We have the following:

**Corollary 7.** *For all  $n$ ,  $P_1$  is  $n$ -control-universal for the revital  $B(A)$ .*

**(b) The conservative revital  $Cons(A)$ .** Define the graph  $G_{A,n}^{(2)}$  that has nodes  $A^n$  and edges  $\{uabv, ubav\}$  for all  $a, b \in A$  and words  $u, v$  with  $|u| + |v| = n - 2$ . Because any two words with the same weight are obtained from each other by permuting the positions of letters, and because swaps of adjacent letters generate such permutations, we have the following lemma.

**Lemma 8.** *The connected components of  $G_{A,n}^{(2)}$  are the weight classes.*

Let  $P_2 = \{(ab ba) \mid a, b \in A\} \subseteq B_2(A)$ . For  $n \geq 2$ , the swap group of  $G_{A,n}^{(2)}$  is contained in  $\langle CP(n-2, P_2) \rangle \subseteq Cons(A) \cap B_n(A)$ . By Lemmas 3 and 8 the swap group is  $Cons(A) \cap B_n(A)$ , so we have the following:

**Corollary 9.** *For all  $n$ ,  $P_2$  is  $n$ -control-universal for the conservative revital  $Cons(A)$ .*

The classical Fredkin gate that operates on  $\{0, 1\}^3$  is a 1-controlled  $P_2$ -permutation. However, note that in the case of a larger alphabet the controlled  $P_2$ -permutations only swap a specific pair of symbols, not just the arbitrary contents of two cells.

**(b $^\phi$ ) The  $\phi$ -conservative revital  $Cons^\phi(A)$ .** Let  $\phi : A^* \rightarrow M$  be a homomorphism to a commutative monoid  $M$ , and let  $m \in \mathbb{N}$ . For  $n \geq m$ , define the graph  $G_{A,n}^{(2),\phi,m}$  that has nodes  $A^n$  and edges  $\{uxv, u\phi(y)v\}$  for all  $x, y \in A^m$  such that  $\phi(x) = \phi(y)$ , and all words  $u, v$  with  $|u| + |v| = n - m$ .

**Lemma 10.** *For any sufficiently large  $m$ , and any  $n \geq m$ , the connected components of  $G_{A,n}^{(2),\phi,m}$  are the weight classes of  $A^n$  under  $\phi$ .*

PROOF. Each edge connects two vertices in the same weight class, so it only remains to show that the weight classes are connected. Recall from Section 2 that we may assume that  $\phi$  separates words of different length:  $|x| \neq |y| \Rightarrow \phi(x) \neq \phi(y)$ .

Because  $\phi(A^*)$  is a finitely generated commutative monoid, it is finitely presented [7, Chapter 5]. Let  $m$  be the length of the longest word involved in a finite presentation of  $\phi(A^*)$  under the generator set  $\phi(A)$ . Note that both sides of any relation  $x = y$  in the presentation are words of equal length  $\leq m$  over alphabet  $\phi(A)$ . Let  $n \geq m$ , and let  $s, t \in A^n$  be arbitrary vertices in the same weight class, that is, they satisfy  $\phi(s) = \phi(t)$ . It follows from the definition of monoid presentations that there is a sequence  $s = w_1, w_2, \dots, w_k = t$  of words  $w_i \in A^n$  where consecutive words are connected by a relation of the monoid presentation, that is, for all  $i$  there are words  $u, v, x, y$  such that  $w_i = uxv$  and  $w_{i+1} = uyyv$ , and we have  $\phi(x) = \phi(y)$  and  $|x| = |y| \leq m$ . We can assume  $|x| = |y| = m$  by appending symbols from  $u$  or  $v$  to  $x$  and  $y$  if needed, so in fact all  $\{w_i, w_{i+1}\}$  are edges in the graph.  $\square$

Let  $P_2^{\phi,m} = \{(x y) \mid x, y \in A^m \text{ and } \phi(x) = \phi(y)\} \subseteq B_m(A)$ . For  $n \geq m$ , the swap group of  $G_{A,n}^{(2),\phi,m}$  is contained in  $\langle CP(n-m, P_2^{\phi,m}) \rangle \subseteq \text{Cons}^\phi(A) \cap B_n(A)$ . By Lemmas 3 and 10, when  $m$  is large enough the swap group is  $\text{Cons}^\phi(A) \cap B_n(A)$ .

**Corollary 11.** *For sufficiently large  $m$ , set  $P_2^{\phi,m}$  is  $n$ -control-universal for the  $\phi$ -conservative revital  $\text{Cons}^\phi(A)$ , for all  $n \geq m$ .*

**(c) The alternating revital  $\text{Even}(A)$ .** Define the 3-hypergraph  $G_{A,n}^{(3)}$  that has nodes  $A^n$  and hyperedges  $\{uabv, uacv, udbv\}$  where  $a, b, c, d \in A$ ,  $a \neq d$  and  $b \neq c$ , that is, all triples of words of which two are at Hamming distance 2 and others at distance 1, and the symbol differences are in consecutive positions. When  $n \geq 2$ , any pair of words  $u, v \in A^n$  of Hamming distance one are in a common hyperedge, so by Lemma 6 we have the following:

**Lemma 12.** *If  $n \geq 2$ , then  $G_{A,n}^{(3)}$  is connected.*

Let  $P_3 = \{(ab\ ac\ db) \mid a, b, c, d \in A\} \subseteq B_2(A)$  so that the cycling group of  $G_{A,n}^{(3)}$  is contained in  $\langle CP(n-2, P_3) \rangle \subseteq \text{Alt}(A^n)$ . By Lemmas 5 and 12 the cycling group contains all even permutations of  $A^n$  so we have the following:

**Corollary 13.** *For all  $n \geq 2$ ,  $P_3$  is  $n$ -control-universal for the alternating revival Even( $A$ ).*

(d) **The alternating conservative revival  $ECons(A)$ .** Let  $n \geq 3$ . Define the 3-hypergraph  $G_{A,n}^{(4)}$  that has nodes  $A^n$  and hyperedges  $\{uxv, u y v, u z v\}$  for all distinct  $x, y, z \in A^3$  with equal weights, and all  $u, v$  whose lengths satisfy  $|u| + |v| = n - 3$ . Then, for all distinct  $a, b \in A$  and words  $u, v \in A^*$  such that  $|u| + |v| = n - 2$ , the words  $u a b v$  and  $u b a v$  are in a common hyperedge. Indeed, any word of length three that contains at least two different letters has at least three different letter permutations. We obtain from Lemma 8 the following:

**Lemma 14.** *If  $n \geq 3$ , then the connected components of  $G_{A,n}^{(4)}$  are the weight classes.*

Let  $P_4 = \{(x\ y\ z) \mid x, y, z \in A^3 \text{ and } x, y, z \text{ have equal weights}\} \subseteq B_3(A)$  consist of all 3-cycles inside weight classes in  $A^3$ . The cycling group of  $G_{A,n}^{(4)}$  is contained in  $\langle CP(n-3, P_4) \rangle \subseteq ECons(A) \cap B_n(A)$ . But by Lemmas 5 and 14 the cycling group is  $ECons(A) \cap B_n(A)$ .

**Corollary 15.** *Set  $P_4$  is  $n$ -control-universal for the alternating conservative revival  $ECons(A)$ , for all  $n \geq 3$ .*

(d $\phi$ ) **The alternating  $\phi$ -conservative revival  $ECons^\phi(A)$ .** Let  $\phi : A^* \rightarrow M$  be a homomorphism to a commutative monoid  $M$ , and let  $m \in \mathbb{N}$ . For  $n \geq m$ , define the 3-hypergraph  $G_{A,n}^{(4),\phi,m}$  that has nodes  $A^n$  and hyperedges  $\{uxv, u y v, u z v\}$  for all distinct  $x, y, z \in A^m$  such that  $\phi(x) = \phi(y) = \phi(z)$ , and all words  $u, v$  with  $|u| + |v| = n - m$ .

**Lemma 16.** *For all sufficiently large  $m$ , and all  $n \geq m$ , the connected components of  $G_{A,n}^{(4),\phi,m}$  are the weight classes of  $A^n$  under  $\phi$ .*

PROOF. If  $x, y \in A^{m-1}$  are such that  $\phi(x) = \phi(y)$  then for all  $a \in A$  holds  $\phi(xa) = \phi(ya) = \phi(ay) = \phi(ax)$ . If, moreover,  $x \neq y$  then there are at least three distinct elements among  $ax$ ,  $ay$ ,  $xa$  and  $ya$  and, in addition,  $ax \neq ay$  and  $xa \neq ya$ . It follows that if  $wxw', wyw' \in A^n$  where  $n \geq m$  and  $x, y \in A^{m-1}$  are distinct and such that  $\phi(x) = \phi(y)$ , then there are three distinct words  $s, t, u \in A^m$  such that  $\phi(s) = \phi(t) = \phi(u)$ , and  $wxw', wyw' \in \{zsz', ztz', zuz'\}$  for some words  $z, z'$ . This means that for  $n \geq m$  any vertices connected by an edge in the graph  $G_{A,n}^{(2),\phi,m-1}$  belong to a hyperedge in the 3-hypergraph  $G_{A,n}^{(4),\phi,m}$ , and hence the connected components of the first one are subsets of the connected components of the latter one. By Lemma 10, if  $m$  is sufficiently large the connected components of  $G_{A,n}^{(2),\phi,m-1}$  are the weight classes. Since the hyperedges of  $G_{A,n}^{(4),\phi,m}$  only connect vertices of the same weight class, we conclude that for sufficiently large  $m$  and all  $n \geq m$ , the connected components of the hypergraph  $G_{A,n}^{(4),\phi,m}$  are precisely the weight classes.  $\square$

Let  $P_4^{\phi,m} = \{(x y z) \mid x, y, z \in A^m \text{ and } \phi(x) = \phi(y) = \phi(z)\} \subseteq B_m(A)$ . The cycling group of  $G_{A,n}^{(4),\phi,m}$  is contained in  $\langle CP(n-m, P_4^{\phi,m}) \rangle \subseteq ECons^\phi(A) \cap B_n(A)$ . By Lemmas 5 and 16 the cycling group is  $ECons^\phi(A) \cap B_n(A)$  when  $m$  is sufficiently large.

**Corollary 17.** *For sufficiently large  $m$  and all  $n \geq m$ , set  $P_4^{\phi,m}$  is  $n$ -control-universal for the alternating  $\phi$ -conservative revital  $ECons^\phi(A)$ .*

Note that Corollaries 13 and 15 are special cases of Corollary 17, in the same way as Corollaries 7 and 9 are special cases of Corollary 11. From the proof we can see that a bound on  $m$  in Corollary 11 is given by the maximum length of the words occurring in the relations in the presentation of  $\phi(A^*)$ , and the corresponding bound for  $m$  in Corollary 17 is one greater. If  $\phi : A^* \rightarrow \mathbb{N}^A$  is the homomorphism that counts the numbers of occurrences of letters, the image  $\phi(A^*) = \mathbb{N}^A$  has a presentation using words of length two (that defines the commutation of symbols); hence the values 2 and 3 for  $m$  in Corollaries 9 and 15, respectively. If  $\phi : A^* \rightarrow \mathbb{N}$  is the homomorphism  $x \mapsto |x|$  then words of length one are used in the presentation stating that  $\phi(a) = \phi(b)$  for all  $a, b \in A$ ; hence the values 1 and 2 for  $m$  in Corollaries 7 and 13, respectively.

## 6. Finite generating sets of gates

In order to apply the Induction Lemma we first observe that 2-controlled 3-word-cycles in any five element set can be obtained from 1-controlled 3-word-cycles.

**Lemma 18.** *Let  $X \subseteq A^n$  contain at least five elements, and let*

$$P = \{(x y z) \mid x, y, z \in X \text{ all distinct}\} \subseteq B_n(A)$$

*consist of all 3-word-cycles in  $X$ . Then  $CP(2, P) \subseteq [CP(1, P)]$ .*

PROOF. Let  $x, y, z \in X$  be pairwise different, and pick  $s, t \in X$  so that  $x, y, z, s, t$  are five distinct elements of  $X$ . Let  $p_1 = (s t)(x y)$  and  $p_2 = (s t)(y z)$ . Then  $p_1$  and  $p_2$  consist of two disjoint word swaps, so they are both involutions. Moreover,  $(x y z) = p_2 p_1 p_2 p_1$ . Further, we have that

$$\begin{aligned} p_1 &= (x s y)(s t x), \text{ and} \\ p_2 &= (y s z)(s t y). \end{aligned}$$

It is important to recall that we compose permutations from right to left.

Let  $a, b \in A$  be arbitrary and consider the 2-controlled  $P$ -permutation  $f = f_{ab, (x y z)} \in B_{2+n}(A)$  determined by the control word  $ab$  and the 3-word-cycle  $(x y z)$ . Then  $f = g \circ g$  where

$$g = f_{*, p_2} \circ f_{a*, p_1} = f_{*, b, (y s z)} \circ f_{*, b, (s t y)} \circ f_{a*, (x s y)} \circ f_{a*, (s t x)}$$

is a composition of four 1-controlled  $P$ -permutations, where the star symbol indicates the control symbol not used by the gate. See Figure 1 for an illustration. In the picture the inputs arrive from the left, so the gates are composed in the reverse order compared to the text.

To verify that indeed  $f = g \circ g$ , consider an input  $w = a'b'u$  where  $a', b' \in A$  and  $u \in A^n$ . If  $a' \neq a$  then  $g(w) = f_{*, b, p_2}(w)$ , so that  $g \circ g(w) = w = f(w)$  since  $p_2$  is an involution. Analogously, if  $b' \neq b$  then  $g \circ g(w) = w = f(w)$ , because  $p_1$  is an involution. Suppose then that  $a' = a$  and  $b' = b$ . We have  $g \circ g(w) = ab(p_2 p_1 p_2 p_1(u)) = f(w)$ . We conclude that  $f \in [CP(1, P)]$ , and because  $f$  was an arbitrary element of  $CP(2, P)$ , up to reordering the input and output symbols, the claim  $CP(2, P) \subseteq [CP(1, P)]$  follows.  $\square$

**Corollary 19.** *Let  $X \subseteq A^n$ ,  $P \subseteq B_n(A)$  be as in Lemma 18. Then we have  $[CP(m, P)] \subseteq [CP(1, P)]$  for all  $m \geq 1$ .*

PROOF. Apply Lemma 2 with  $k = 1$ .  $\square$

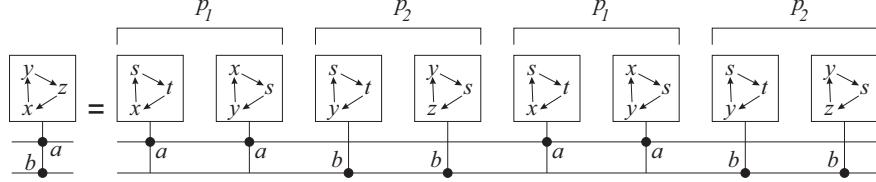


Figure 1: A decomposition of the  $ab$ -controlled 3-word-cycle  $(x y z)$  into a composition of eight 1-controlled 3-word-cycles. Note that in our illustrations the input-output direction of gates is from left to right. This means that the gates appear in the opposite order as in the main text where all compositions are written from right to left.

### 6.1. The alternating and full revivals

Assuming that  $|A| > 1$ , the set  $X = A^3$  contains at least five elements. For  $P = \{(x y z) \mid x, y, z \in A^3 \text{ all distinct}\} \subseteq B_3(A)$  we then have, by Corollary 19, that  $[CP(m, P)] \subseteq [CP(1, P)]$  for all  $m \geq 1$ .

Recall that  $P_3 = \{(ab ac db) \mid a, b, c, d \in A\} \subseteq B_2(A)$  is  $n$ -control-universal for the alternating revival  $\text{Even}(A)$ , for  $n \geq 2$  (Corollary 13). Clearly  $CP(1, P_3) \subseteq P \subseteq [CP(0, P)]$ , so by Lemma 1, for any  $m \geq 1$ ,

$$CP(m + 1, P_3) \subseteq [CP(m, P)] \subseteq [CP(1, P)].$$

Hence  $\text{Even}(A) \cap B_{m+3}(A) = \langle CP(m + 1, P_3) \rangle \subseteq [CP(1, P)]$ . We conclude that  $[CP(1, P)]$  contains all permutations of  $\text{Even}(A)$  except the ones in  $B_1(A)$ ,  $B_2(A)$  and  $B_3(A)$ . We have proved the following theorem.

**Theorem 20.** *The alternating revival  $\text{Even}(A)$  is finitely generated. Even permutations of  $A^4$  generate all even permutations of  $A^n$  for all  $n \geq 4$ .*

**Corollary 21 ([8, 2]).** *Let  $|A|$  be odd. Then the full revival  $B(A)$  is finitely generated. The permutations of  $A^4$  generate all permutations of  $A^n$  for all  $n \geq 4$ .*

**PROOF.** Let  $|A| > 1$  be odd. Let  $P$  be the set of all permutations of  $A^4$ , and let  $n \geq 4$ . By Theorem 20, the closure  $[P]$  contains all even permutations of  $A^n$ . The set  $P$  also contains an odd permutation  $f$ , say the word swap (0000 1000). Consider  $\pi = f \oplus id_{n-4} \in B_n(A)$  that applies the swap  $f$  on the first four input symbols and keeps the others unchanged. This  $\pi$  is an odd permutation because it consists of  $|A|^{m-4}$  disjoint swaps and  $|A|$  is odd. Because  $[P] \cap B_n(A)$  contains all even permutations of  $A^n$  and an odd one, it contains all permutations.  $\square$

Recall that if a circuit implements the permutation  $f \oplus id_k \in B_{n+k}(A)$ , we say it implements  $f \in B_n(A)$  using  $k$  borrowed bits.

**Corollary 22.** *The revital  $B(A)$  is finitely generated using at most one borrowed bit.*

PROOF. For  $|A|$  odd the claim follows from Corollary 21. When  $A$  is even then the permutations  $f \oplus id$  with one borrowed bit are all even, so the claim follows from Theorem 20.  $\square$

### 6.2. The alternating conservative revital

Every non-trivial weight class of  $A^5$  contains at least five elements. (The trivial weight-classes are the singletons  $\{a^5\}$  for  $a \in A$ .) For every non-trivial weight class  $X$  we set  $P_X = \{(x y z) \mid x, y, z \in X\} \subseteq B_5(A)$  for the 3-word-cycles in  $X$ . By Corollary 19 we know that  $[CP(m, P_X)] \subseteq [CP(1, P_X)]$  for all  $m \geq 1$ . Let  $P$  be the union of  $P_X$  over all non-trivial weight classes  $X$ . Then, because  $[\cdot]$  is a closure operator, also  $[CP(m, P)] \subseteq [CP(1, P)]$  for all  $m \geq 1$ .

By Corollary 15, the set  $P_4 \subseteq B_3(A)$  of 3-cycles within weight classes is  $n$ -control-universal for the alternating conservative revital  $ECons(A)$ , for all  $n \geq 3$ . Let  $m \geq 1$ . Because  $CP(2, P_4) \subseteq P \subseteq [CP(0, P)]$ , by Lemma 1 we have

$$CP(m+2, P_4) \subseteq [CP(m, P)] \subseteq [CP(1, P)].$$

Hence  $ECons(A) \cap B_{m+5}(A) = \langle CP(m+2, P_4) \rangle \subseteq [CP(1, P)]$ . We conclude that  $[CP(1, P)]$  contains all permutations of  $ECons(A)$  except possibly the ones in  $B_\ell(A)$  for  $\ell \leq 5$ .

**Theorem 23.** *The alternating conservative revital  $ECons(A)$  is finitely generated. A gate set generates the whole  $ECons(A)$  if it generates, for all  $n \leq 6$ , the conservative permutations of  $A^n$  that are even on all weight classes.*  $\square$

### 6.3. The generalized alternating conservative case

Let  $\phi : A^* \rightarrow M$  be a homomorphism to a commutative monoid  $M$ . Analogously to the standard alternating conservative case, we have the following:

**Theorem 24.** *The alternating  $\phi$ -conservative revital  $ECons^\phi(A)$  is finitely generated.*

PROOF. Fix  $m$  to be sufficiently large so that the conclusions of Lemma 16 and Corollary 17 hold, and let  $n = \max(5, m + 1)$ .

Consider a non-trivial weight class  $X \subseteq A^n$  under  $\phi$ . Let us prove that  $X$  contains at least five elements. By Lemma 16 weight class  $X$  contains the vertices of some hyperedge of  $G_{A,n}^{(4),\phi,m}$ . These hyperedges have form  $\{uxv, u y v, u z v\}$  for distinct  $x, y, z \in A^m$ . Because  $n \geq m + 1$ , either  $u$  or  $v$  is a non-empty word. It follows that  $X$  contains a word with at least two distinct letters. Any letter permutation of such a word is also in  $X$ , and because  $n \geq 5$  there are at least five distinct such permutations, proving  $|X| \geq 5$ .

Next we apply Corollary 19 as in Section 6.2 above. Let

$$P = \{(x \ y \ z) \mid x, y, z \in A^n \text{ and } \phi(x) = \phi(y) = \phi(z)\} \subseteq B_n(A)$$

be the set of 3-word cycles inside the weight classes of  $A^n$ . Because all non-trivial weight classes contain at least five elements we get from Corollary 19 that  $[CP(k, P)] \subseteq [CP(1, P)]$  for all  $k \geq 1$ .

Consider  $P_4^{\phi,m} \subseteq B_m(A)$ , the set of 3-word cycles within the weight classes of  $A^m$ . Because  $CP(n - m, P_4^{\phi,m}) \subseteq P \subseteq [CP(0, P)]$ , we get from Lemma 1 that for all  $k \geq 1$

$$CP(n - m + k, P_4^{\phi,m}) \subseteq [CP(k, P)] \subseteq [CP(1, P)].$$

By Corollary 17 the set  $P_4^{\phi,m}$  is  $n + k$ -control-universal for  $ECons^\phi(A)$ . Hence  $ECons^\phi(A) \cap B_{n+k}(A) = \langle CP(n - m + k, P_4^{\phi,m}) \rangle \subseteq [CP(1, P)]$ . We conclude that  $[CP(1, P)]$  contains all permutations of  $ECons^\phi(A)$  except possibly the ones in  $B_\ell(A)$  for  $\ell \leq n$ .

□

## 7. Non-finitely generated revitals

It is well known that the full revival is not finitely generated over even alphabets. The reason is that any permutation  $f \in B_n(A)$  can only compute even permutations on  $A^m$  for  $m > n$ .

**Theorem 25 ([10]).** *For even  $|A|$ , the full revival  $B(A)$  is not finitely generated.*

By another parity argument we can also show that the conservative revital  $Cons(A)$  is not finitely generated on any non-trivial alphabet, not even if infinitely many borrowed bits are available. This generalizes a result in [11] on binary alphabets. Our proof is based on the same parity sequences as the one in [11], where these sequences are computed concretely for generalized Fredkin gates. However, our observation only relies on the (necessarily) low rank of a finitely-generated group of such parity sequences, and the particular conserved quantity is not as important.

Let  $n \in \mathbb{N}$ , and let  $\mathcal{W}$  be the family of the weight classes of  $A^n$ . For any  $f \in Cons(A) \cap B_n(A)$  and any weight class  $X \in \mathcal{W}$ , the restriction  $f|_X$  of  $f$  on the weight class  $X$  is a permutation of  $X$ . Let  $\psi(f)_X \in \mathbb{Z}_2$  be its parity. Clearly,  $\psi(f \circ g)_X = \psi(f)_X + \psi(g)_X$  modulo two, so  $\psi$  defines a group homomorphism from  $Cons(A) \cap B_n(A)$  to the additive abelian group  $(\mathbb{Z}_2)^{\mathcal{W}}$ . The image  $\psi(f)$  that records all  $\psi(f)_X$  for all  $X \in \mathcal{W}$  is the *parity sequence* of  $f$ . Because each element of the commutative group  $(\mathbb{Z}_2)^{\mathcal{W}}$  is an involution, it follows that the subgroup generated by any  $k$  elements has cardinality at most  $2^k$ .

Consider then a function  $f \in Cons(A) \cap B_\ell(A)$  for  $\ell \leq n$ . Its application  $f_n = f \oplus id_{n-\ell} \in B_n(A)$  on length  $n$  inputs is conservative, so it has the associated parity sequence  $\psi(f')$ , which we denote by  $\psi_n(f)$ . Note that any conjugate  $\pi_\alpha \circ f \circ \pi_\alpha^{-1}$  of  $f$  by a wire permutation  $\pi_\alpha$  has the same parity sequence, so the parity sequence does not depend on which input wires we apply  $f$  on.

Let  $f^{(1)}, f^{(2)}, \dots, f^{(m)} \in Cons(A)$  be a finite generator set, and let us denote by  $C \subseteq Cons(A)$  the revital they generate. Let  $n \geq 2$  be larger than the arity of any  $f^{(i)}$ . Then  $C \cap B_n(A)$  is the group generated by the applications  $f_n^{(1)}, f_n^{(2)}, \dots, f_n^{(m)}$  of the generators on length  $n$  inputs, up to conjugation by wire permutations. We conclude that there are at most  $2^m$  different parity sequences on  $C \cap B_n(A)$ , for all sufficiently large  $n$ . We have proved the following lemma.

**Lemma 26.** *Let  $C$  be a finitely generated subrevital of  $Cons(A)$ . Then there exists a constant  $N$  such that, for all  $n$ , the elements of  $C \cap B_n(A)$  have at most  $N$  different parity sequences.*

Now we can prove the following negative result. Not only does it state that no finite gate set generates the conservative revital, but even that there necessarily remain conservative permutations that cannot be obtained using any number of borrowed bits.

**Theorem 27.** Let  $|A| > 1$ . The conservative revital  $\text{Cons}(A)$  is not finitely generated. In fact, if  $C \subseteq \text{Cons}(A)$  is finitely generated then there exists  $f \in \text{Cons}(A)$  such that  $f \oplus id_k \notin C$  for all  $k = 0, 1, 2, \dots$ .

PROOF. Let  $0, 1 \in A$  be distinct. Let  $C$  be a finitely generated subrevital of  $\text{Cons}(A)$ , and let  $N$  be the constant from Lemma 26 for  $C$ . Let us fix  $n \geq N + 2$ . For each  $i = 1, 2, \dots, N + 1$ , consider the non-trivial weight classes  $X_i$  containing the words of  $A^n$  with  $i$  letters 1 and  $n - i$  letters 0. For each  $i$ , let  $f_i \in \text{Cons}(A) \cap B_n(A)$  be a permutation that swaps two elements of  $X_i$ , keeping all other elements of  $A^n$  unchanged. This  $f_i$  is odd on  $X_i$  and even on all other weight classes, so all  $f_i$  have different parity sequences. We conclude that some  $f_i$  is not in  $C$ .

For the second, stronger claim, we continue by considering an arbitrary  $k \in \mathbb{N}$ . For  $i = 1, 2, \dots, N + 1$ , let  $X_i^{(k)}$  be the parity class of  $A^{n+k}$  containing the words with  $i$  letters 1 and  $n + k - i$  letters 0. Note that  $f_i^{(k)} = f_i \oplus id_k$  is a single word swap on  $X_i^{(k)}$  and the identity map on all  $X_j^{(k)}$  with  $j < i$ . This means that the parity sequences of  $f_1^{(k)}, f_2^{(k)}, \dots, f_{N+1}^{(k)}$  are all different, hence some  $f_i^{(k)}$  is not in  $C$ . But then, for some  $i \in \{1, 2, \dots, N + 1\}$ , there are infinitely many  $k \in \mathbb{N}$  with the property that  $f_i^{(k)} = f_i \oplus id_k$  is not in  $C$ . This means that  $f_i \oplus id_k \notin C$  for any  $k \in \mathbb{N}$  as  $f_i \oplus id_k \in C$  implies that  $f_i \oplus id_\ell \in C$  for all  $\ell > k$ . The permutation  $f = f_i$  has the claimed property.  $\square$

Let us consider next the more general case of the  $\phi$ -conservative revital  $\text{Cons}^\phi(A)$ . The following example shows that the second, stronger statement in Theorem 27 concerning borrowed bits does not hold for all choices of  $\phi$ .

**Example.** Let  $A = \{0, 1, 2, 3\}$  and consider the morphism  $\phi : A^* \rightarrow \mathbb{N}^2$  defined by  $\phi(0) = \phi(2) = (1, 0)$  and  $\phi(1) = \phi(3) = (0, 1)$ . Now  $\phi(x) = \phi(y)$  if and only if  $x$  and  $y$  contain equally many even letters, and equally many odd letters. Let  $C = E\text{Cons}^\phi(A)$ , a sub-revital of  $\text{Cons}^\phi(A)$  that is finitely generated by Theorem 24.

Let  $f \in \text{Cons}^\phi(A)$  be arbitrary. Then  $f \oplus id$  is even on every  $\phi$ -weight class:  $x0$  and  $x2$  are in the same weight class, as are  $x1$  and  $x3$ . In each case  $f \oplus id$  only changes the word  $x$  independent of the last symbol, so  $f \oplus id$  performs in each weight class two copies of the same permutation. We conclude that  $f \oplus id \in C$ . This means that  $\text{Cons}^\phi(A)$  is finitely generated using one borrowed bit.  $\triangle$

However, we can prove that  $\text{Cons}^\phi(A)$  itself – without borrowed bits – is not finitely generated if there are enough non-trivial weight classes. Let us call  $\phi : A^* \rightarrow M$  *infinite-dimensional* if for all  $m \in \mathbb{N}$  there exists  $n \in \mathbb{N}$  such that there are at least  $m$  weight classes with more than one word in  $A^n$ . The homomorphism in the previous example is infinite dimensional. In contrast, if  $M$  is finite then  $\phi$  can not be infinite-dimensional.

**Theorem 28.** *Let homomorphism  $\phi : A^* \rightarrow M$  be infinite-dimensional. Then  $\text{revital } \text{Cons}^\phi(A)$  is not finitely generated.*

The theorem shows, for example, that the revital of functions in  $B(\{0, 1, 2\})$  that preserve the number of zeroes, and preserve the number of ones modulo  $k$ , is not finitely generated.

**PROOF.** Suppose  $\text{Cons}^\phi(A)$  is finitely generated. We define the parity sequence of  $f \in \text{Cons}^\phi(A) \cap B_n(A)$  analogously to the case of  $\text{Cons}(A)$ : it records the parities of  $f$  restricted to  $\phi$ -weight classes of  $A^n$ . Lemma 26 holds with an analogous proof: there exists a constant  $N$  such that, for all  $n$ , the elements of  $\text{Cons}^\phi(A) \cap B_n(A)$  have at most  $N$  different parity sequences. Because  $\phi$  is infinite-dimensional, for some  $n$  there are at least  $N + 1$  non-trivial weight classes  $X_1, X_2, \dots, X_{N+1}$  in  $A^n$ . For  $i \in \{1, 2, \dots, N + 1\}$ , let  $f_i \in B_n(A)$  swap two elements of class  $X_i$  and keep all other words unchanged. This  $f_i$  is in  $\text{Cons}^\phi(A)$ , and it is odd on  $X_i$  and even on all other weight classes. Thus there are  $N + 1$  functions  $f_1, f_2, \dots, f_{N+1}$  in  $\text{Cons}^\phi(A) \cap B_n(A)$  with different parity sequences, a contradiction.  $\square$

Note that the theorem is not valid without the infinite-dimensionality condition: For example the full revital  $B(A)$  is  $\text{Cons}^\phi(A)$  for the length homomorphism  $\phi : x \mapsto |x|$ , but it is finitely generated when  $|A|$  is odd (Corollary 21).

## 8. Concrete generating families

We have found finite generating sets for revitals in the general and the conservative cases. Our generating sets are of the form ‘all controlled 3-word cycles that are in the family’, and the reader may wonder whether there are more natural gate families that generate these classes. Of course, by our results, there is an algorithm for checking whether a particular set of gates is a set of generators, and in this section we give some examples.

First, we observe that  $CP(2, P_1)$  (that is, 2-controlled symbol swaps) generate all permutations of  $A^3$  and all even permutations of  $A^n$  for all  $n \geq 4$ . Indeed, by Corollary 7 they generate  $B_3(A)$ , and by Figure 2 they generate  $CP(2, P_3)$  (the 2-controlled 3-cycles of length-two words). These in turn, by Corollary 13, generate all even permutations of  $A^4$  which is enough by Theorem 20 to get all even permutations on  $A^n$  for  $n \geq 4$ .

It is easy to see that  $CP(2, P_1)$  in turn is generated by all symbol swaps and the  $w$ -word-controlled symbol swaps for a single  $w \in A^2$ . In particular in the case of binary alphabets, we obtain that the alternating revival is generated by the Toffoli gate and the negation gate, which was also proved in [11].

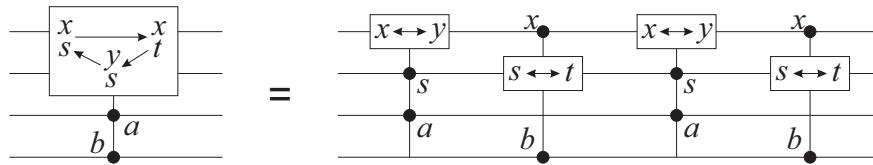


Figure 2: A decomposition of the  $ab$ -controlled 3-cycle  $(xs\ xt\ ys)$  into a composition of four 2-controlled swaps.

In the conservative binary case, the Fredkin gate is known to be universal (in the sense of auxiliary bits, see [11]). The Fredkin gate is, due to the binary alphabet, both the unique 1-word-controlled wire swap and the unique nontrivial conservative 1-word-controlled word swap. The natural generalizations would be to show that in general the 1-controlled wire swaps or conservative word swaps generate the alternating conservative revival. We do not prove this, but do show how the universality of the Fredkin gate follows from our results and a bit of computer search.

The following shows that the 00-word-controlled rotation and the 01-word-controlled are generated by the 0-word-controlled rotation. These implementations were found by computer search, and both are optimal in the number of gates.

**Lemma 29.** *The 00-word-controlled (resp. 01-word-controlled) three-wire rotation can be implemented with nine (resp. eight) 0-word-controlled three-wire rotations.*

PROOF. See Figure 3 for the diagrams of these implementations. We give the implementation of the 00-word-controlled rotation also in symbols: Let

$A = \{0, 1\}$  and  $R \in B_3(A)$  be the rotation  $R = \pi_{(123)}$ . Write  $\rho_{a,b,c,d}(f)$  for  $f$  applied to cells  $a, b, c, d$  in that order.

$$\begin{aligned} f_{00,R} &= \rho_{1,0,2,3}(f_{0,R}) \circ \rho_{3,1,4,2}(f_{0,R}) \circ \rho_{1,0,2,4}(f_{0,R}) \circ \\ &\quad \rho_{3,0,1,2}(f_{0,R}) \circ \rho_{0,1,3,4}(f_{0,R}) \circ \rho_{1,2,3,4}(f_{0,R}) \circ \\ &\quad \rho_{0,1,4,3}(f_{0,R}) \circ \rho_{1,0,2,3}(f_{0,R}) \circ \rho_{3,0,2,4}(f_{0,R}) \end{aligned}$$

□

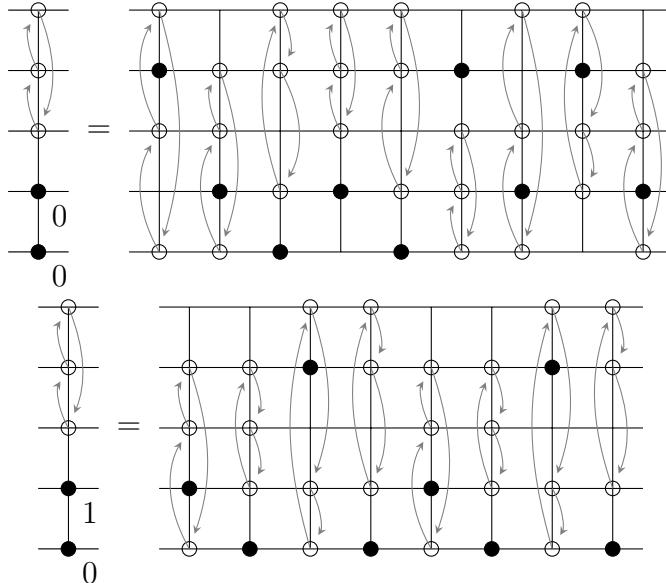


Figure 3: 00-controlled and 01-controlled rotations built from 0-controlled rotations. These are controlled by the two bottommost wires, the rotation rotates the wires in order  $2 \rightarrow 3 \rightarrow 4 \rightarrow 2$ , where the bottommost wire is the 0th. The diagram is read from left to right, and in each column we perform a 0-controlled rotation. A black circle indicates a control wire, and white circles are the rotated wires, and the arrows indicate the direction of rotation.

A similar brute force search also shows the following (again six is optimal).

**Lemma 30.** *The word cycle  $(0001 \ 0010 \ 0100)$  can be built from six 0-word-controlled three-wire rotations. The same is true for  $(0011 \ 0110 \ 0101)$ .*

Let  $\pi_1 = (001\ 010\ 100)$  and  $\pi_2 = (011\ 110\ 101)$ . Note that  $\pi_1 \circ \pi_2$  is the three-wire rotation. Then, by Lemma 29 and Lemma 2, 1-control  $(\pi_1 \circ \pi_2)$ -permutations generate  $k$ -controlled  $(\pi_1 \circ \pi_2)$ -permutations for all  $k$ . By Lemma 30, 1-controlled  $(\pi_1 \circ \pi_2)$ -permutations generate 1-controlled  $\{\pi_1, \pi_2\}$ -permutations, and then by Lemma 1,  $k$ -controlled  $(\pi_1 \circ \pi_2)$ -permutations generate  $k$ -controlled  $\{\pi_1, \pi_2\}$ -permutations. Putting these together and combining with Corollary 15, we have:

**Theorem 31.** *Let  $A = \{0, 1\}$ . Then the alternating conservative revital  $ECons(A)$  is generated by the controlled wire rotation*

$$f(a, b, c, d) = \begin{cases} (a, c, d, b) & \text{if } a = 0 \\ (a, b, c, d) & \text{otherwise} \end{cases}$$

and the even conservative permutations of  $A^3$ .

Clearly  $f(a, b, c, d)$  is generated by 1-controlled wire swaps. It follows that the Fredkin gate together with the (unconditional) wire swap generates all even conservative permutations of  $\{0, 1\}^n$  for  $n \geq 4$ .

## 9. Conclusion

We have precisely determined the revital generated by a finite set of generators on an even order alphabet and show that on an odd alphabet, a finite collection of mappings generates the whole revital. The first result confirms a conjecture in [2] and the second gives a simpler proof of the same result from that paper. Moreover, we have shown that the alternating conservative revital is finitely generated on all alphabets, but the conservative revital is never finitely generated.

The methods are rather general: We have developed an induction result (Lemma 2) for finding generating sets for revitals of controlled permutations, allowing us to determine finite generating sets for some revitals with uniform methods. We also prove the nonexistence of a finite generating family for conserved gates with a general method in Theorem 28, when borrowed bits are not used. We only need particular properties of the weight function in the proof of Theorem 27, where it is shown that the (usual) conservative revital is not finitely generated even when borrowed bits are allowed.

While this paper develops strong techniques for showing finitely generatedness and non-finitely generatedness of revitals, our generating sets are also

somewhat abstract, not corresponding very well to known generating sets. It would be of value to replace the constructions found in section 8 by more understandable constructions, in order to find more concrete generating sets in the case of general alphabets for conservative gates.

## References

- [1] Aaronson, S., Grier, D., Schaeffer, L.: The classification of reversible bit operations. *Electronic Colloquium on Computational Complexity* (66) (2015)
- [2] Boykett, T.: Closed systems of invertible maps (2015), <http://arxiv.org/abs/1512.06813>, submitted
- [3] Boykett, T., Kari, J., Salo, V.: Strongly universal reversible gate sets. In: Devitt, S.J., Lanese, I. (eds.) *Reversible Computation - 8th International Conference, RC 2016, Bologna, Italy, July 7-8, 2016, Proceedings*. Lecture Notes in Computer Science, vol. 9720, pp. 239–254. Springer (2016), [http://dx.doi.org/10.1007/978-3-319-40578-0\\_18](http://dx.doi.org/10.1007/978-3-319-40578-0_18)
- [4] Fredkin, E., Toffoli, T.: Conservative logic. *International Journal of Theoretical Physics* 21(3), 219–253 (1982), <http://dx.doi.org/10.1007/BF01857727>
- [5] LaFont, Y.: Towards an algebraic theory of boolean circuits. *Journal of Pure and Applied Algebra* 184, 257–310 (2003)
- [6] Musset, J.: Générateurs et relations pour les circuits booléens réversibles. Tech. Rep. 97-32, Institut de Mathématiques de Luminy (1997), <http://iml.univ-mrs.fr/editions/>
- [7] Rosales, J., García-Sánchez, P.: Finitely Generated Commutative Monoids. Nova Science Publishers (1999), <https://books.google.fi/books?id=LQsH6m-x8ysC>
- [8] Selinger, P.: Reversible k-ary logic circuits are finitely generated for odd k (April 2016), arXiv
- [9] Szendrei, Á.: Clones in universal algebra, Séminaire de Mathématiques Supérieures [Seminar on Higher Mathematics], vol. 99. Presses de l’Université de Montréal, Montreal, QC (1986)

- [10] Toffoli, T.: Reversible computing. Tech. Rep. MIT/LCS/TM-151, MIT (1980)
- [11] Xu, S.: Reversible Logic Synthesis with Minimal Usage of Ancilla Bits. Master's thesis, MIT (June 2015), <http://arxiv.org/pdf/1506.03777.pdf>
- [12] Yang, G., Song, X., Perkowski, M., Wu, J.: Realizing ternary quantum switching networks without ancilla bits. *J. Phys. A* 38(44), 9689–9697 (2005), <http://dx.doi.org/10.1088/0305-4470/38/44/006>