Theoretical Computer Science ••• (••••) •••–•••

Contents lists available at ScienceDirect

Theoretical Computer Science

www.elsevier.com/locate/tcs

Finite generating sets for reversible gate sets under general conservation laws ☆, ☆☆

Tim Boykett [a,b], Jarkko Kari [c,*], Ville Salo [c]

[a] Institute for Algebra, Johannes Kepler University Linz, Austria
[b] Time's Up Research, Linz, Austria
[c] Department of Mathematics and Statistics, University of Turku, Finland

ARTICLE INFO

Article history:
Received 3 November 2016
Accepted 20 December 2016
Available online xxxx

Keywords:
Reversible gates
Reversible circuits
Universal gates
Conservative gates
Reversible clones

ABSTRACT

It is well-known that the Toffoli gate and the negation gate together yield a universal gate set, in the sense that every even permutation of $\{0,1\}^n$ can be implemented as a composition of these gates. An analogous result holds also on non-binary logic: For any finite set A, a finite set of reversible gates can generate all even permutations of A^n for all n. This means that a finite gate set can generate all permutations of A^n when the cardinality of A is odd, and that one auxiliary "borrowed" symbol is necessary and sufficient to obtain all permutations when the cardinality of A is even. We 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 borrowed symbols. But we provide a finite gate set that can implement all those conservative permutations that are even within each weight class of A^n.

1. Introduction

The study of reversible and conservative binary gates was pioneered in the 1970s and 1980s by Toffoli and Fredkin [2,3]. Recently, Aaronson, Greier and Schaeffer [4] 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 [5].

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 [4,6,7]. In [5], it is shown that for the ternary alphabet, the whole set of reversible gates is finitely generated. In [8] the result is announced for all odd alphabets, with a proof attributed to personal communication, which has recently been published as [9]. Another

☆ 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.
☆☆ A preliminary version of this work was presented at the 8th International Conference on Reversible Computation, RC 2016 [1].
* Corresponding author.
E-mail address: jkari@utu.fi (J. Kari).

http://dx.doi.org/10.1016/j.tcs.2016.12.032
0304-3975/

proof of this fact can be found in [10]. 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 [7], 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 [7]).

We also consider more general conservation laws for gates, extending the results we reported in [1]. 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 [11] applied to bijections as developed in [10], 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 [8,6]. 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 [4]. 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 $\mathrm{Sym}(A)$ for the group of permutations or bijections of A, S_n for $Sym(\{1,\dots,n\})$ and $\mathrm{Alt}(A)$ for the group of even permutations of A, $A_n = Alt(\{1,\dots,n\})$. Let $B_n(A) = \{f : A^n \to A^n \mid f \text{ a bijection}\} = \mathrm{Sym}(A^n)$ 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 $f_i : A^n \to A$ 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 α:

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

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 ℓ coordinates while leaving the other $n-\ell$ coordinates unchanged. Using the clone theory derived terminology in [10] 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 $\lceil P\rceil \subseteq B(A)$ 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 ℓ on A^n, for $n \geq \ell$. Clearly $P \mapsto \lceil P\rceil$ is a closure operator. Sets $C \subseteq B(A)$ such that $C = \lceil C\rceil$ are called *reversible iterative algebras*, or *revitals*, for short. We say

Please cite this article in press as: T. Boykett et al., Finite generating sets for reversible gate sets under general conservation laws, Theoret. Comput. Sci. (2017), http://dx.doi.org/10.1016/j.tcs.2016.12.032