Maximality of Reversible Gate Sets

Tim Boykett[1,2,3](✉)

[1] Institute for Algebra, Johannes-Kepler University, Linz, Austria
tim.boykett@jku.at, tim@timesup.org
[2] Time's Up Research, Linz, Austria
[3] University for Applied Arts, Vienna, Austria

Abstract. We investigate collections of reversible gates closed under parallel and serial composition. In order to better understand the structure of these collections of reversible gates, we investigate the lattice of closed sets and the maximal members of this lattice, that is, collections that are not all gates, but the addition of a single new gate will allow us to construct all gates. We find the maximal closed sets over a finite alphabet.

We then extend to ancilla and borrow closure for reversible gates. Here we find some structural results, including some examples.

Keywords: Reversible gates · Maximal closed classes · Permutation groups

1 Introduction

For a given finite set A, we investigate the collections of reversible gates, or bijections of A^k for all k. The work derived from Tomasso Toffoli's work [14] and as such we call closed systems of bijections reversible Toffoli Algebras (RTAs). We also consider ancilla and borrow closure, where an extra input and output is allowed; an *ancilla* is provided and returned in a particular state, whereas a *borrowed* bit is provided and returned in an arbitrary state.

The work also relates to permutation group theory, as an RTA C is a $\mathbb{N}$-indexed collection of permutations groups, $C^{[i]} \leq Sym(A^i)$.

In previous papers, Aaronson, Grier and Schaeffer have determined all ancilla closed gates on a set of order 2 [1], and the author, together with Jarkko Kari and Ville Salo, has investigated generating sets [2,3] and other themes.

In this paper, we determine the possible maximal closed systems, relying strongly on Liebeck, Praeger and Saxl's work [11], and determine some properties of maximal borrow and ancilla closed RTAs.

We show that the maximal RTAs are defined by an index that defines the single arity at which the RTA is not the full set of bijections. We then show that for different indices and orders of A, only certain possibilities can arise. For

The research has been supported by Austrian Science Fund (FWF) research projects AR561 and P29931.

I. Lanese and M. Rawski (Eds.): RC 2020, LNCS 12227, pp. 206–217, 2020.
https://doi.org/10.1007/978-3-030-52482-1_12

ancilla and borrow closed RTAs we find that there is similarly an index below which the maximal RTAs are full symmetry groups and above which they are never full.

We start by introducing the background properties of RTAs and some permutation group theory. The next section is an investigation of maximality, with the main result, Theorem 4, taking up the main body of this section. We then investigate properties of borrow and ancilla closed RTAs.

2 Background

In this section we will introduce the necessary terminology.

Let A be a finite set. $Sym(A) = S_A$ is the set of permutations or bijections of A, $Alt(A)$ the set of permutations of even parity. If $A = \{1, \ldots, n\}$ we will write S_n and A_n. We write permutations in cycle notation and act from the right. We write the action of a permutation $g \in G \leq Sym(A)$ on an element $a \in A$ as a^g. A subgroup $G \leq S_A$ is *transitive* if for all $a, b \in A$ there is a $g \in G$ such that $a^g = b$. We also say that G acts *transitively* on A. If for all distinct $a_1, \ldots, a_n \in A$ and $b_1, \ldots, b_n \in A$ there is a $g \in G$ such that $a_i^g = b_i$ for all i, then we say G is n-transitive on A. A subgroup G of S_A acts *imprimitively* if there is a nontrivial equivalence relation ρ on A such that for all $a, b \in A$, for all $g \in G$, $a \rho b \Rightarrow a^g \rho b^g$. If there is no such equivalence relation, then G acts *primitively* on A.

Let G be a group of permutations of a set A. Let $n \in \mathbb{N}$. Then the *wreath product* $GwrS_n$ is a group of permutations acting on A^n. The elements of $GwrS_n$ are $\{(g_1, \ldots, g_n, \alpha) \mid g_i \in G, \alpha \in S_n\}$ with action defined as follows: for $(a_1, \ldots, a_n) \in A^n$, $(a_1, \ldots, a_n)^{(g_1, \ldots, g_n, \alpha)} = (a^{g_1}_{\alpha^{-1}1}, \ldots, a^{g_n}_{\alpha^{-1}n})$.

Let $B_n(A) = Sym(A^n)$ and $B(A) = \bigcup_{n \in \mathbb{N}} B_n(A)$. We call $B_n(A)$ the set of *n-ary reversible gates* on A, $B(A)$ the set of *reversible gates*. For $\alpha \in S_n$, let $\pi_\alpha \in B_n(A)$ be defined by $\pi_\alpha(x_1, \ldots, x_n) = (x_{\alpha^{-1}(1)}, \ldots, x_{\alpha^{-1}(n)})$. We call this a *wire permutation*. Let $\Pi = \{\pi_\alpha | \alpha \in S_n,\ n \in \mathbb{N}\}$. In the case that α is the identity, we write $i_n = \pi_\alpha$, the n-ary identity. Let $f \in B_n(A)$, $g \in B_m(A)$. Define the *parallel composition* as $f \oplus g \in B_{n+m}(A)$ with $(f \oplus g)(x_1, \ldots, x_{n+m}) = (f_1(x_1, \ldots, x_n), \ldots,\ f_n(x_1, \ldots, x_n),\ g_1(x_{n+1}, \ldots, x_{n+m}), \ldots,\ g_m(x_{n+1}, \ldots, x_{n+m}))$. For $f, g \in B_n(A)$ we can compose $f \bullet g$ in $Sym(A^n)$. If they have distinct arities we "pad" them with identity, for instance $f \in B_n(A)$ and $g \in B_m(A)$, $n < m$, then define $f \bullet g = (f \oplus i_{m-n}) \bullet g$ and we can thus serially compose all elements of $B(A)$.

We call a subset $C \subseteq B(A)$ that includes Π and is closed under $\oplus$ and $\bullet$ a *reversible Toffoli algebra* (RTA) based upon Toffoli's original work [14]. These have also been investigated as *permutation clones* [8], with ideas from category theory [9] and as *memoryless computation* [6]. If we do not insist upon the inclusion of Π, then we have *reversible iterative algebras* [3] in reference to Malcev and Post's iterative algebras. For a set $F \subseteq B(A)$ we write $\langle F \rangle$ as the smallest RTA that includes F, the RTA *generated* by F.

Let C be an RTA. We write $C^{[n]} = C \cap B_n(A)$ for the elements of C of arity n. We will occasionally write $(a_1, \ldots, a_n) \in A^n$ as $a_1 a_2 \ldots a_n$ for clarity.

In any RTA C, the unary part $C^{[1]}$ is found as a wreath product in all other parts, $C^{[1]} wr S_n \leq C^{[n]}$ because the wire permutations give us the right hand factor while $f_1 \oplus \cdots \oplus f_n$ for $f_i \in C^{[1]}$ gives us the left hand side.

Let q be a prime power, $GF(q)$ the field of order q, $AGL_n(q)$ the collection of affine invertible maps of $GF(q)^n$ to itself. We note that for all $m \in \mathbb{N}$, $AGL_n(q^m) \leq AGL_{nm}(q)$. For a prime p, let $\mathrm{Aff}(p^m) = \bigcup_{n \in \mathbb{N}} AGL_{nm}(p)$ be the RTA of affine maps over $A = GF(p)^m$.

We say that an RTA $C \leq B(A)$ is *borrow closed* if for all $f \in B(A)$, $f \oplus i_1 \in C$ implies that $f \in C$. We say that an RTA $C \leq B(A)$ is *ancilla closed* if for all $f \in B_n(A)$, $g \in C^{[n+1]}$ with some $a \in A$ such that for all $x_1, \ldots, x_n \in A$, for all $i \in \{1, \ldots, n\}$, $f_i(x_1, \ldots, x_n) = g_i(x_1, \ldots, x_n, a)$ and $g_{n+1}(x_1, \ldots, x_n, a) = a$ implies that $f \in C$. If an RTA is ancilla closed then it is borrow closed. For any prime power q, $\mathrm{Aff}(q)$ is borrow and ancilla closed.

3 Maximality in Permutation Groups

In this section we introduce some results from permutation group theory that will be of use. The maximal subgroups of permutation groups have been determined.

Theorem 1 **([11]).** *Let $n \in \mathbb{N}$. Then the maximal subgroups of S_n are conjugate to one of the following G.*

1. *(alternating) $G = A_n$*
2. *(intransitive) $G = S_k \times S_m$ where $k + m = n$ and $k \neq m$*
3. *(imprimitive) $G = S_m wr S_k$ where $n = mk$, $m, k > 1$*
4. *(affine) $G = AGL_k(p)$ where $n = p^k$, p a prime*
5. *(diagonal) $G = T^k.(Out(T) \times S_k)$ where T is a nonabelian simple group, $k > 1$ and $n = |T|^{(k-1)}$*
6. *(wreath) $G = S_m wr S_k$ with $n = m^k$, $m \geq 5$, $k > 1$*
7. *(almost simple) $T \lhd G \leq Aut(T)$, $T \neq A_n$ a nonabelian simple group, G acting primitively on A*

Moreover, all subgroups of these types are maximal when they do not lie in A_n, except for a list of known exceptions.

It is worth noting that in the imprimitive case, A is a disjoint sum of k sets of order m, giving an equivalence relation with k equivalence classes of order m, the wreath product acts by reordering the equivalence classes as S_k, then acting as S_m on each equivalence class. In the wreath case, the set A is a direct product of k copies of a set of order m, the wreath product acts by permuting indices by S_k then acting as S_m on each index.

Lemma 1. *Let A be a set of even order and $n \geq 3$. Then $S_A wr S_n \leq Alt(A^n)$.*

Proof. $S_A wr S_n$ is generated by S_A acting on the first coordinate of A^n and S_n acting on coordinates.

The action of S_A on A^n is even because for each cycle in the first coordinate, the remaining $n-1$ coordinates are untouched. Every cycle occurs $|A|^{n-1}$ times, which is even, so the action of S_A lies in $Alt(A^n)$.

S_n is generated by S_{n-1} and the involution $(n-1\, n)$. By the same argument, each cycle of the action occurs an even number of times, so the action of S_{n-1} and the involution $((n-1)\, n)$ on A^n lies in $Alt(A^n)$ so we are done. □

We have a similar inclusion for affineness.

Lemma 2. *For $n \geq 3$, $AGL_n(2) \leq Alt(2^n)$.*

Proof. $AGL_n(2)$ is generated by the permutation matrices $\{\pi_{(1,i)} \mid i = 2, \ldots, n\}$ and the matrix $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \oplus i_{n-2}$. These bijections are even parity because they only act on two entries, thus have parity divisible by 2^{n-2} modulo 2 which is 0. □

Lemma 3. *Let A be even order. Then $S_A wr S_2 \leq Alt(A^2)$ iff 4 divides $|A|$.*

Proof. The same argument as above applies for S_A. The action of S_2 swaps $\frac{|A|(|A|-1)}{2}$ pairs. This is even iff 4 divides $|A|$. □

4 Maximality in RTAs

In this section, we will determine the maximal RTAs on a finite set A.

We have some generation results from other papers that will be useful.

Theorem 2 **([2] Theorem 5.9]).** *Let A be odd. If $B_1(A), B_2(A) \subseteq C \subseteq B(A)$, then $C = B(A)$.*

Theorem 3 **([3] Theorem 20]).** *If $Alt(A^4) \subseteq C \subseteq B(A)$ then $Alt(A^k) \subseteq C$ for all $k \geq 5$.*

Lemma 4. *Let $|A| \geq 3$, then $\langle B_1(A), B_2(A) \rangle$ is 3-transitive on A^3.*

Proof. Let $A = \{1, 2, 3, \ldots\}$. Let $a, b, c \in A^3$ be distinct. We show that we can map these to $111, 112, 113 \in A^3$. There are three cases. See Fig. 1.

Case 1: Suppose a_3, b_3, c_3 all distinct. Let $\alpha = (a_1a_3 \;\; 1a_3)(b_1b_3 \;\; 1b_3)(c_1c_3 \;\; 1c_3) \in B_2(A)$. Let $\beta = (a_2a_3 \;\; 11)(b_2b_3 \;\; 12)(c_2c_3 \;\; 13) \in B_2(A)$. Then $\gamma = (\pi_{(23)} \bullet (\alpha \oplus i_1) \bullet \pi_{(23)}) \bullet (i_1 \oplus \beta)$ satisfies the requirements.

Case 2: Suppose a_3, b_3, c_3 contains two values, wlog suppose $a_3 = b_3$. Let $d \in A - \{a_3, c_3\}$. Let $\delta = (a_1a_3 \;\; a_1d) \in B_2(A)$. Let $\lambda = \pi_{(23)} \bullet (\delta \oplus i_1) \bullet \pi_{(23)}$. Then λ will map a, b, c to the situation in the first case.

Case 3: Suppose $a_3 = b_3 = c_3$. Then one of a_1, b_1, c_1 or a_2, b_2, c_2 must contain at least two values, wlog let a_1, b_1, c_1 be so. Then $\pi_{(13)}$ will give us the Case 1 if a_1, b_1, c_1 contains three values, Case 2 if a_1, b_1, c_1 contains two values. □

The two following results are only relevant for even A.

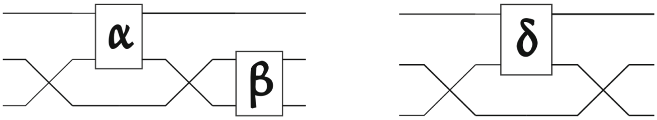

Fig. 1. Cases 1 and 2 in Lemma 4

Lemma 5. *Let $|A| \geq 4$, $B_1(A), B_2(A) \subset C \leq B(A)$. Then $Alt(A^3) \subseteq C^{[3]}$.*

Proof. For $|A| = 4$, the result is shown by calculation in GAP [7] that $\langle B_1(A) \oplus i_2 \cup B_2(A) \oplus i_1 \cup \Pi^{[3]} \rangle$ as a subgroup of $B_3(A)$ is $Alt(A^3)$.

For $|A| = 5$ the result follows from Theorem 2.

Suppose $|A| \geq 6$ Since $B_2(A) \subseteq C$, we have all 1-controlled permutations of A in C. By [3] Lemma 18, with $P \subset Alt(A)$ the set of all 3-cycles, we have all 2-controlled 3-cycles in C. Thus $(111\ 112\ 113) \in C$. $B_1(A) \cup B_2(A)$ is 3-transitive on A^3 by Lemma 4, so we have all 3-cycles in C, so $Alt(A^3) \subseteq C$. □

We know that this is not true for A of order 2, where $B_2(A)$ generates a group of order 1344 in $B_3(A)$, which is of index 15 in $Alt(A^3)$ and is included in no other subgroup of $B_3(A)$. However we find the following.

Lemma 6. *Let $|A|$ be even, $B_1(A), B_2(A), B_3(A) \subset C \leq B(A)$. Then $Alt(A^4) \subseteq C^{[4]}$.*

Proof. For A of order 4 or more, we use the same techniques as in Lemma 5.

For A of order 2, we calculate. We look at $C^{[4]}$ as a subgroup of S_{16}. The wire permutations $\Pi^{[4]}$ are generated by $(2,9,5,3)(4,10,13,7)(6,11)(8,12,14,15)$ and $(5,9)(6,10)(7,11)(8,12)$. Then $i_1 \oplus B_3(A)$ is a subgroup of $B_4(A)$ acting on the indices $\{2,3,4\}$, generated by $(1,2,3,4,5,6,7,8)(9,10,11,12,13,14,15,16)$ and $(1,2)(9,10)$. It is a simple calculation to determine that this group is the entire alternating group A_{16}, so $Alt(A^4) \subseteq C^{[4]}$. □

We can now state our main theorem.

Theorem 4. *Let A be a finite set. Let M be a maximal sub RTA of $B(A)$. Then $M^{[i]} \neq B_i(A)$ for exactly one i and M belongs to the following classes:*

1. *$i = 1$ and $M^{[1]}$ is one of the classes in Theorem 1.*
2. *$i = 2$, $|A| = 3$, and $M^{[2]} = AGL_2(3)$ (up to conjugacy)*
3. *$i = 2$, $|A| \geq 5$ is odd and $M^{[2]} = S_A wr S_2$*
4. *$i = 2$, $|A| \equiv 2 \mod 4$ and $M^{[2]} = S_A wr S_2$*
5. *$i = 2$, $|A| \equiv 0 \mod 4$ and $M^{[2]} = Alt(A^2)$*
6. *$i = 2$, $|A| \equiv 0 \mod 4$ and $M^{[2]} = T^{(3)}.(Out(T) \times S_3)$ where T is a finite nonabelian simple group, with $|A| = |T|$ (up to conjugacy)*
7. *$i = 2$, $|A| \equiv 0 \mod 4$ and $M^{[2]}$ is an almost simple group (up to conjugacy)*
8. *$i \geq 3$, $|A|$ is even and $M^{[i]} = Alt(A^i)$*

Proof. Suppose $M < B(A)$ with $i \neq j$ natural numbers such that $M^{[i]} \neq B_i(A)$ and $M^{[j]} \neq B_j(A)$. Wlog, $i < j$, let $N = \langle M \cup B_j(A)\rangle$. Remember that compositions of mappings of arity at least j will also be of arity at least j, so $N^{[k]} = M^{[k]}$ for all $k < j$. Then $M < N$ because N contains all of $B_j(A)$ and $N < B(A)$ because $N^{[i]} = M^{[i]} \neq B_i(A)$. Thus M was not maximal, proving our first claim.

For the rest of the proof, take M maximal with $M^{[i]} \neq B_i(A)$. Then $M^{[i]}$ is a maximal subgroup of $B_i(A)$.

Suppose $i = 1$. Then $B_1(A) = S_A$ and we are interested in the maximal subgroups of S_A. From Theorem 1 we know that these are in one of the 7 classes.

Suppose $i \geq 2$. Then $S_A^i \leq M^{[i]}$ so $M^{[i]}$ is transitive on A^i. As $\Pi^{[i]} \leq M^{[i]}$ we also know that $S_A wr S_i \leq M^{[i]}$. Assume $M^{[i]}$ acts imprimitively on A^i with equivalence relation ρ. Let $a, b \in A^i$, $a\rho b$ with $a_i \neq b_i$. By the action of S_A acting on the ith coordinate we obtain $a'\rho b'$ with $a_j = a'_j$ and $b_j = b'_j$ for all $j \neq i$. By the action of S_i on coordinates we can move this inequality to any index. Thus by transitivity we can show that $\rho = (A^n)^2$ and is thus trivial, so our action cannot be imprimitive.

We now consider the cases of A odd and even separately.

Suppose $i \geq 2$ and $|A|$ is odd. If $i \geq 3$ then $M^{[1]} = B_1(A)$ and $M^{[2]} = B_2(A)$, so by Theorem 2 we have all of $B(A)$ and thus M is not maximal, a contradiction. Thus we have $i = 2$. $M^{[1]} = B_1(A) = S_A$ and $\pi_{(1\,2)} \in M$ so M contains $S_A wr S_2$. If $|A| \geq 5$ then by Theorem 1 this is maximal in $Sym(A^2)$ so $M^{[2]}$ must be precisely this. So the case of A order 3 is left. We want to know which maximal subgroups of $Sym(A^2)$ contain $S_A wr S_2$. There are 7 classes of maximal subgroups, we deal with them in turn.

- Since $\pi_{(1\,2)} \in M$ is odd on A^2, $M^{[2]} \not\subseteq Alt(A^2)$.
- From the discussion above we know that $M^{[2]}$ is transitive and primitive on A^2, so the second and third cases do not apply.
- The permutations in S_3 can be written as affine maps in $\mathbb{Z}_3$ and $\pi_{(1\,2)}$ can be written as $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, the off diagonal 2×2 matrix over $\mathbb{Z}_3$, so $S_3 wr S_2$ embeds in the affine general linear group. Thus $M^{[2]} = AGL_2(3)$ is one possibility.
- The diagonal case requires $|T|^{k-1} = 9$ for some nonabelian finite simple group T, a contradiction.
- The wreath case requires $9 \geq 5^2$, a contradiction.
- By [4] all G acting primitively on A^2 with subgroups that are nonabelian finite simple groups are subgroups of $Alt(A^2)$, and we have odd elements in M, so this is a contradiction.

Thus the only maximal subgroup is $M^{[2]} = AGL_2(3)$.

Suppose $i \geq 2$ and $|A|$ is even. We know from Theorem 3 that for $i > 4$ we can get all of $Alt(A^i)$ from $\cup_{1 \leq j < i} B_j(A)$. $Alt(A^i)$ is maximal in $Sym(A^i)$ so we are done.

Thus we are left with 3 cases, $i = 2, 3, 4$.

From Lemma 6 we know that for $i = 4$, $M^{[4]} = Alt(A^4)$ is the only possibility.

From Lemma 5 we know that for $i = 3$ and $|A| \neq 2$, $M^{[3]} = Alt(A^3)$ is the only possibility. For $|A| = 2$ we find that $B_2(A)$ generates a subgroup of $B_3(A)$ that is only included in $Alt(A^3)$, so again $M^{[3]} = Alt(A^3)$ is the only possibility.

Thus we are left with the case $i = 2$. From the above we know that the intransitive and imperfect cases cannot arise. Thus we need to consider the wreath, affine, diagonal and almost simple cases.

- $|A| = 2$: $S_A wr S_2$ has order 8, $B_2(2)$ has order 24, so $M^{[2]} = S_A wr S_2$ is maximal and we are done.
- Case $6 \leq |A| \equiv 2 \mod 4$: Lemma 3 above says that $S_A wr S_2 \not\leq Alt(A^2)$ so it is maximal by Theorem 1.
- Case $|A| = 4$: Alternating is possible by inclusion. The affine case $AGL_4(2)$ lies in A_{16} by Lemma 2. Diagonal not possible by order. Almost simple not possible because all primitive groups of degree 16 lie in the alternating group A_{16} [4] .
- Case $8 \leq |A| \equiv 0 \mod 4$: Alternating is always possible. If $A = 2^m$ for some m, then $AGL_m(2)$ might be possible, but lies in $Alt(A^2)$ by Lemma 2. Diagonal, almost simple might be possible, if $S_A wr S_2 \leq M^{[2]}$.

□

4.1 The Existence of Maximal RTAs

It is not immediately clear that all the classes of maximal RTAs can actually exist. So let us investigate a few small examples.

Let us take A of order 2. For $i = 1$ we find no nontrivial subgroups, so the maximal is $M^{[1]}$ of order 1. For $i = 2$ case 4 gives us $S_2 wr S_2$ of order 8 as a maximal subgroup. We note that $B_2(A) = AGL_2(2)$, i.e. all binary bijections are affine maps. For $i \geq 3$ we have $M^{[i]}$ alternating as the only example, as we know from Toffoli [14] and others that the alternating bijections of arity i are generated by the collection of all permutations of arity less than i.

Taking A of order 3, we obtain a few more examples. For $i = 1$ we write $A = \{1, 2, 3\}$ and we know that S_3 has maximal subgroups A_3 as well as $\langle(1\,2)\rangle$, $\langle(1\,3)\rangle$, $\langle(2\,3)\rangle$. These correspond in Theorem 1 to the alternating case and intransitive cases. For $i = 2$ we write $A = Z_3$ and note that the unary maps are all affine, that is, the set of affine maps $\{x \mapsto ax + b | a, b \in \mathbb{Z}_3,\ a \neq 0\}$ is identical to the permutations $S_3 = B_1(A)$. The binary affine maps $AGL_2(3)$ include all sums of unary affine maps and the wire permutation $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$. With the inclusion of the linear map $(x, y) \mapsto (x + y, y) = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ we obtain all affine maps. From Theorem 1 above we know this is maximal as a subgroup of $B_2(A)$. For $i \geq 3$ we know that $B_1(A), B_2(A)$ generate all of $B(A)$ so we are done.

For A of order 4 things get a touch more complex. For $i = 1$ we get a number of maximal subgroups. A_4 is maximal. By fixing one element we obtain 4 maximal subgroups isomorphic to S_3 as intransitive subgroups. By imposing an equivalance relation with two classes of two elements each ($1, 2 \mid 3, 4$ or $1, 3 \mid 2, 4$ or $1, 3 \mid 2, 3$) we obtain subgroups isomorphic to $S_2 wr S_2$ that act imprimitively on A. $AGL_2(2)$ is of order 24, same as S_4, we see that the affine maps are precisely the permutations, not maximal. There is no nonabelian simple group to allow a diagonal maximal subgroup. The wreath product also fails by order, and no nonabelian simple group of order less than 24 exists, so the almost simple case cannot arise. For $i \geq 2$ we find $M^{[2]} = Alt(A^2)$ a maximal subgroup. For $i = 2$ we see that there are no nonabelian finite simple groups of order 16, so case 6 cannot arise. It can be shown by investigation of [4] that $M^{[2]}$ cannot be an almost simple group.

For orders 5 and above, we know that the maximal RTAs for $i = 1$ can be obtained by permutation group analysis directly. For A of odd order we have the wreath case $S_A wr S_2$ maximal in $B_2(A)$ and none others. For A even we have the alternating and wreath cases easily constructible. We are left with the question whether, for A of order a multiple of 4, the diagonal or almost simple cases can actually arise.

The possibilities for the diagonal case with A of order equal to the order of a finite simple nonabelian group start with A of order 60. The other possibility is that $|A|^2 = |T|$ for some finite simple nonabelian group T. The only known result in this direction is in [13] where they show that symplectic groups $Sp(4, p)$ where p is a certain type of prime, now known as NSW primes, have square order. The first of these groups is of order $(2^4 \cdot 3 \cdot 5 \cdot 7^2)^2$ corresponding to A of order $(2^4 \cdot 3 \cdot 5 \cdot 7^2) = 11760$. We note that the sporadic simple groups have order that always contains a prime to the power one, so they are not of square order. We know that the Alternating group can never have order that is a square, as the highest prime less than n will occur exactly once in the order of the group. It might be possible that there are other finite simple groups of square order. As far as we are aware, there have been no further results in this direction.

Each of these possibilities is far beyond the expected useful arities for computational processes.

The other case is to look at almost simple groups. Let A be of order $4k$, then we are looking for an almost simple action of degree $16k^2$. In [4] we saw that all primitive actions of degree 16 are alternating, that is, they are subgroups of A_{16}. In order to find an example, we can hope to use results about primitive permutation groups of prime power [5] and product of two prime power [10] degrees, so we would be able to investigate A of order $4k$ for $k \leq 14$. Once again this would include all examples of arities expected to be useful for computational processes.

5 Maximality with Borrow and Ancilla Closure

The strength of Theorem 4 is partially due to the fact that there is no effect of the existence of mappings of a certain arity in a given RTA on the size of the lower arity part, as there are no operators to lower the arity of a mapping. This does not apply with ancilla and borrow closure. In this section we collect some results about maximal ancilla and borrow closed RTAs. The following result reflects the first part of Theorem 4.

Lemma 7. *Let $M \leq B(A)$ be a maximal borrow or ancilla closed RTA. Then there exists some $k \in \mathbb{N}$ such that for all $i < k$, $M^{[i]} = B_i(A)$ and for all $i \geq k$, $M^{[i]} \neq B_i(A)$.*

Proof. Suppose $M^{[k]} = B_k(A)$. Then for all $f \in B_m(A)$, $m < k$, $f \oplus i_{k-m} \in M$ so by borrow closure $f \in M$, so $M^{[m]} = B_m(A)$ for all $m \leq k$. As M is maximal, there must be a largest k for which $M^{[k]} = B_k(A)$, since otherwise $M = B(A)$. □

We will call k the *index* of the maximal ancilla closed or borrow closed RTA. From Theorem 2 we then note the following.

Lemma 8. *Let $|A|$ be odd. Then M maximal with index $k = 1, 2$ are the only options.*

In this case, we can say a bit more for index 2. If A is of order 3, then by the argument in Theorem 4 above, we find that $M = \mathrm{Aff}(A)$, the affine maps over a field of order 3. Otherwise A is at least 5 and $B_1(A)$ is no longer affine. See Lemma 11 below.

Similarly, we obtain the following, but see Corollary 1 below for a stronger result.

Lemma 9. *Let $|A| \geq 4$ be even. Then M maximal with index $k = 1, 2, 3$ are the only options and for $i > k$, $M^{[i]} \neq Alt(A^i)$.*

Proof. We start by noting that for even $|A|$, for all $f \in B_i(A)$, $f \oplus i_1 \in Alt(A^{i+1})$. Thus if $M^{[i]} = Alt(A^i)$ for some $i > k$, then $M^{[i-1]} = B_{i-1}(A)$ which is a contradiction, which shows the second part of the result.

Suppose $k \geq 4$, so $B_1(A), B_2(A), B_3(A) \subseteq M$. Then by Lemma 6 $Alt(A^4) \subseteq M$, so by Theorem 3 $Alt(A^j) \subseteq M$ for all $j \geq 5$. But we know that by borrow closure, this implies that $B_{j-1}(A) \subseteq M$ so M is in fact $B(A)$. This is a contradiction, so $k < 4$. □

Using similar arguments, we obtain the following.

Lemma 10. *Let $|A| = 2$. Then M maximal with index $k = 1, 2, 3$ are the only options and for $i > k$, $M^{[i]} \neq Alt(A^i)$.*

Proof. Suppose M is maximal with $k \geq 5$. Then by Theorem 3 we obtain $M^{[i]} = Alt(A^i)$ for all $i \geq 5$, which by the first argument in the previous Lemma, implies that M is not maximal.

Suppose M is maximal with $k = 4$. We know that $M^{[3]} = B_3(A)$. Then by Lemma 6 we find that $M^{[4]} = Alt(A^4)$, by Theorem 3 we obtain all of $Alt(A^5)$ so by borrow closure all of $B_4(A)$ and thus M is not maximal. □

We obtain some examples of maximal borrow and ancilla closed RTA. The expression *degenerate* to describe maps where each output index depends only upon one input comes from [1].

Lemma 11. *For $|A| \geq 5$, the degenerate RTA $Deg(A)$ generated by $B_1(A)$ is a maximal borrow closed RTA and maximal ancilla closed RTA.*

Proof. Let $Deg(A)$ be generated by $B_1(A) = S_A$. Then $Deg(A)^{[i]} = S_A wr S_i$ for all $i \geq 2$ which is maximal in $B_i(A)$ by Theorem 1. Thus any RTA N properly containing $Deg(A)$ will have $N^{[i]} = B_i(A)$ for some $i \geq 2$ and thus $N^{[2]} = B_2(A)$ by Lemma 7. Let $f \in N^{[2]} - Deg(A)^{[2]}$, then $f \oplus f \in N[4] - Deg(A)^{[4]}$ so $N^{[4]} = B_4(A)$ and by Lemmas 8 and 9, $N = B(A)$, so $Deg(A)$ is maximal. □

For $|A| < 5$, $B_1(A)$ consists of affine maps, so $Deg(A) < \mathrm{Aff}(A)$ and thus cannot be maximal.

Corollary 1. *Let $|A| \geq 4$ be even. Then M maximal with index $k = 1, 2$ are the only options.*

Proof. From Lemma 9 we know $k = 1, 2, 3$ are possible. Suppose M is maximal in B(A) with $k = 3$.

Suppose $|A| = 4$. $B_2(A)$ can be embedded in $B_4(A)$ represented on S_{256} with the tuples in A^4 represented by the integers $1, \ldots, 256$, generated by the permutations

$$\begin{aligned}&(1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16)\\ &\quad(17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32)\ldots\\ &\quad\ldots(241,242,243,244,245,246,247,248,249,250,251,252,253,254,255,256)\end{aligned}$$

and $(1,2)(17,18)\ldots(241,242)$. With the wire permutations we obtain a subgroup of S_{256} that is the alternating group, so $M^{[4]} = Alt(A^4)$ and by Theorem 3 we then get $M^{[5]} = Alt(A^5)$ and thus M is not maximal.

Suppose A is even with more than 6 elements. The degenerate RTA $Deg(A) \leq M$ because $M^{[1]} = B_1(A)$, but because $Deg(A)$ is maximal and $M^{[2]}$ is a supergroup of $Deg(A)^{[2]}$, M is all of $B(A)$ and is not maximal. □

Lemma 12. *Let A be of prime power order. Then* $\mathrm{Aff}(A)$ *is a maximal borrow closed RTA and a maximal ancilla closed RTA.*

Proof. Let $M = \mathrm{Aff}(A)$. Suppose M is not maximal, so $M < N < B(A)$.

Let A be of odd order. For every i, except $i = 1$ with A of order 3, $M^{[i]}$ is maximal in $B_i(A)$ by Theorem 1. Let $f \in B_n(A)$, $f \in N - M$. Then $N^{[n]} = B_n(A)$ by subgroup maximality, so for all $i < n$, $N^{[i]} = B_i(A)$. For all $j \in \mathbb{N}$, $f \oplus i_j \in (N - M)^{[n+j]}$ so similarly $N^{[n+j]} = B_{n+j}(A)$ so $N = B(A)$ and M is maximal.

Let A be of even order, so a power of 2. Let $f \in B_n(A)$, $f \in N - M$. We know from Lemma 2 above that $M^{[n]} \leq Alt(A^n)$ is not maximal, so the odd order argument above does not hold. By [12] we know that $N^{[n]} = B_n(A)$ or $N^{[n]} = Alt(A^n)$. For all $j \in \mathbb{N}$, $f \oplus i_j \in (N - M)^{[n+j]}$ so $N^{[n+j]} = B_{n+j}(A)$ or $N^{[n+j]} = Alt(A^{n+j})$. In both cases this means that $N^{[n+j-1]} = B_{n+j-1}(A)$, as for all $g \in B_{n+j-1}(A)$ $g \oplus i_1 \in Alt(A^{n+j})f$, so $N = B(A)$ and M was maximal.

Because Aff(A) is ancilla closed and maximal as borrow closed, there can be no ancilla closed RTA between Aff(A) and $B(A)$ so Aff(A) is a maximal ancilla closed RTA. □

We look at a few concrete examples.

By [1] we know that for A of order 2, we have the following maximal ancilla closed RTAs.

- The affine mappings,
- The parity respecting mappings, which either preserve the number of 1s mod 2, or invert it,
- The odd prime-conservative mappings, that preserve the number of 1s mod p, an odd prime.

The affine mappings have index 3, the parity respecting index 2 and the odd prime-conservative mappings have index 1.

It remains an open problem whether these are the borrow closed maximal RTAs over A of order 2.

For A of order 3, we know that the affine maps Aff(3) is an index 2 maximal borrow closed RTA and a maximal ancilla closed RTA.

For A of order 4, we can say the following about index 2 maximals. There are the following inclusions, $S_4 wr S_2 < ASp < AGL_4(2) < Alt(4^2)$ where ASp is a group of order 11520 that consists of the affine maps where the linear part is a symplectic linear map in $Sp(4,2)$. If $M^{[2]} = Alt(4^2)$ then M includes the affine maps properly. We know that the affine maps are maximal, a contradiction. $M^{[2]} = AGL_4(2)$ for the affine maps that we know form a maximal borrow and ancilla closed RTA. It is possible that $M^{[2]} = S_4 wr S_2$ or $M^{[2]} = ASp$ for some maximal M.

For A of order 5 or more, we know that index 2 arises only for the degenerate RTA $Deg(A)$.

6 Conclusion and Further Work

We have determined the maximal RTAs, using results from permutation group theory and some generation results.

As we have not been able to construct explicitly an example of a maximal RTA with $i = 2$ and $M^{[i]}$ of diagonal or almost simple type, the conjecture remains that these are not, in fact, possible. We note however that if such examples exist, they will arise for A of order 8 or more, so will probably not be relevant for any practical reversible computation implementation.

In future work we aim to determine the weight functions as described by [8] for maximal RTAs, in order to determine whether they hold some interesting insights.

The results for borrow and ancilla closed RTAs are not as comprehensive. We hope to determine these in the foreseeable future. We note interestingly that for a state set of order 5 or more, Lemma 11 indicates that if we can implement all permutations of the state set, we need only have one non-degenerate gate in order to implement all gates under borrow or ancilla closure. Similarly we see that once we can implement all affine maps on a state set of prime power order, then only one nonaffine gate is needed to implement all gates. For the ancilla case, many of the techniques of [1] will prove useful. In the ancilla case, we know all maximal RTA with index 2 except for A of order 4.

Acknowledgements. Michael Guidici has helped extensively with understanding primitive permutations groups, for which I thank him greatly.

References

1. Aaronson, S., Grier, D., Schaeffer, L.: The classification of reversible bit operations. Electron. Colloquium Comput. Complexity (66) (2015). https://eccc.weizmann.ac.il//report/2015/066/
2. Boykett, T.: Closed systems of invertible maps. J. Multiple-Valued Logic Soft Comput. **32**(5–6), 565–605 (2019)
3. Boykett, T., Kari, J., Salo, V.: Finite generating sets for reversible gate sets under general conservation laws. Theor. Comput. Sci. **701**(C), 27–39 (2017). https://doi.org/10.1016/j.tcs.2016.12.032
4. Buekenhout, F., Leemans, D.: On the list of finite primitive permutation groups of degree $\leq$ 50. J. Symb. Comput. **22**(2), 215–225 (1996). https://doi.org/10.1006/jsco.1996.0049
5. Cai, Q., Zhang, H.: A note on primitive permutation groups of prime power degree. J. Discrete Math. **2**, 191–192 (2015)
6. Gadouleau, M., Riis, S.: Memoryless computation: new results, constructions, and extensions. Theoret. Comput. Sci. **562**, 129–145 (2015). https://doi.org/10.1016/j.tcs.2014.09.040
7. The GAP Group: GAP - Groups, Algorithms, and Programming, Version 4.10.2 (2019). https://www.gap-system.org
8. Jeřábek, E.: Galois connection for multiple-output operations. Algebra Universalis **79**(2), 1–37 (2018). https://doi.org/10.1007/s00012-018-0499-7
9. LaFont, Y.: Towards an algebraic theory of Boolean circuits. J. Pure Appl. Algebra **184**, 257–310 (2003)
10. Li, C.H., Li, X.: On permutation groups of degree a product of two prime-powers. Commun. Algebra **42**(11), 4722–4743 (2014). https://doi.org/10.1080/00927872.2013.823500
11. Liebeck, M.W., Praeger, C.E., Saxl, J.: A classification of the maximal subgroups of the finite alternating and symmetric groups. J. Algebra **111**(2), 365–383 (1987). https://doi.org/10.1016/0021-8693(87)90223-7
12. Mortimer, B.: Permutation groups containing affine groups of the same degree. J. Lond. Math. Soc. **2**(3), 445–455 (1977). https://doi.org/10.1112/jlms/s2-15.3.445
13. Newman, M., Shanks, D., Williams, H.C.: Simple groups of square order and an interesting sequence of primes. Acta Arith. **38**(2), 129–140 (1980)
14. Toffoli, T.: Reversible computing. In: de Bakker, J., van Leeuwen, J. (eds.) ICALP 1980. LNCS, vol. 85, pp. 632–644. Springer, Heidelberg (1980). https://doi.org/10.1007/3-540-10003-2_104