# A finite alternation result for reversible boolean circuits

Peter Selinger

Dalhousie University

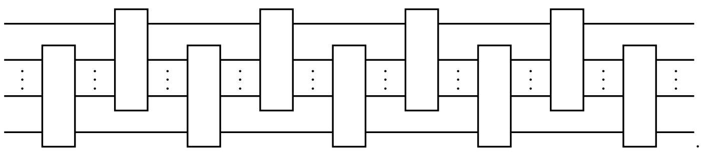
**Abstract**

We say that a reversible boolean function on $n$ bits has *alternation depth $d$* if it can be written as the sequential composition of $d$ reversible boolean functions, each of which acts only on the top $n-1$ bits or on the bottom $n-1$ bits. Moreover, if the functions on $n-1$ bits are even, we speak of *even alternation depth*. We show that every even reversible boolean function of $n \geqslant 4$ bits has alternation depth at most 9 and even alternation depth at most 13.

## 1 Introduction

A reversible boolean function on $n$ bits is a permutation of $\{0,1\}^n$. It is well-known that the NOT, controlled NOT, and Toffoli gates form a universal gate set for reversible boolean functions [5, 2, 1]. More precisely, these gates generate (via the operations of composition and cartesian product, and together with the identity functions) all reversible boolean functions on $n$ bits, when $n \leqslant 3$, and all even reversible boolean functions on $n$ bits, when $n \geqslant 4$. A particular representation of a reversible boolean function in terms of these generators is called a *reversible circuit*. The problem of finding a (preferably short) circuit to implement a given reversible function is called the *synthesis problem* [3].

When working with reversible boolean functions and circuits, it is not typically possible to reason inductively; we cannot usually reduce a problem about circuits on $n$ bits to a problem about circuits on $n-1$ bits. In this paper, we prove a theorem that may, in some cases, make such inductive reasoning possible: we prove that when $n \geqslant 4$, every even reversible function on $n$ bits can be decomposed into at most 9 reversible functions on $n-1$ bits:



(1)

If, moreover, each of the functions on $n-1$ bits is also required to be even, we prove that a decomposition into 13 such functions is possible. It is of course not remarkable that $n$-bit circuits can be decomposed into $(n-1)$-bit circuits: after all, we already know that they can be decomposed into 3-bit circuits, namely gates. What is perhaps remarkable is that the bound 9 (respectively, 13) on the depth is independent of $n$.

There are some potential applications of such a result — although admittedly, they may not be very practical. As a first application, one may obtain an alternative proof of universality, by turning any universal gate set on $n$ bits into a universal gate set on $n+1$ bits, provided that $n \geqslant 3$. This also yields a new method for circuit synthesis: given a good procedure for synthesizing even $n$-bit circuits, we obtain a procedure for synthesizing even $(n+1)$-bit circuits that is at most 13 times worse. By applying this idea recursively, we obtain circuits of size $O(13^n)$ for any reversible function on $n$ bits. This is worse than what can be obtained by other methods. However, it may be possible to improve this procedure further, for example by noting that the 13 subcircuits need not be completely general; they can be chosen to be of particular forms, which may be easier to synthesize recursively.

Another potential application is the presentation of (even) reversible boolean functions by generators and relations. While the NOT, CNOT, and Toffoli gates are a well-known set of generators, to the author's knowledge, no complete set of relations for these generators is known. For any given $n$, the group of $n$-bit reversible functions is a finite group, so finding a complete set of relations for any fixed $n$ is a finite (although very large) problem. However, it is not trivial to find a set of relations that works for all $n$; at present, it is not even known whether the theory is finitely axiomatizable. If we had a procedure for rewriting every circuit into one of the form (1), then we could obtain a complete set of relations for $n$-bit circuits by considering (a) a complete set of relations for $(n-1)$-bit circuits, (b) the relations required to do the rewriting, and (c) any relations required to prove equalities between circuits of the form (1). In particular, if it could be shown that a finite set of relations is sufficient for (b) and (c), a finite equational presentation of reversible boolean functions could be derived.

Finally, the task of realizing a given permutation with low alternation depth can also make for an entertaining puzzle. Such a puzzle has been implemented and is available from [4].

## 2 Statement of the main result

We write $S(X)$ for the group of permutations of a finite set $X$. For $f \in S(X)$ and $g \in S(Y)$, let $f \times g \in S(X \times Y)$ be the permutation defined componentwise by $(f \times g)(x, y) = (f(x), g(y))$. We also write $\mathrm{id}_X \in S(X)$ for the identity permutation on $X$. Recall that a permutation is *even* if it can be written as a product of an even number of 2-cycles.

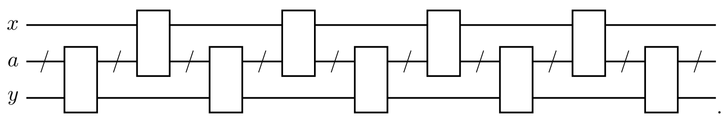
Let $2 = \{0, 1\}$ be the set of booleans, which we identify with the binary digits 0 and 1. By abuse of notation, we also write $2 = \mathrm{id}_2$ for the identity permutation on the set 2.

**Definition.** Let $A$ be a finite set, and let $\sigma \in S(2 \times A \times 2)$ be a permutation. We say that $\sigma$ has *alternation depth $d$* if it can be written as a product of $d$ factors $\sigma = \sigma_1\sigma_2 \cdots \sigma_d$, where each factor $\sigma_i$ is either of the form $f \times 2$ for some $f \in S(2 \times A)$ or of the form $2 \times g$ for some $g \in S(A \times 2)$.

The purpose of this paper is to prove the following theorem:

**Theorem 2.1.** *Let $A$ be a finite set of 3 or more elements. Then every even permutation $\sigma \in S(2 \times A \times 2)$ has alternation depth 9.*

In circuit notation, Theorem 2.1 can be understood as stating that every reversible boolean function on the set $2 \times A \times 2$ can be expressed as a circuit in the following form:




(2)

Here, the lines labelled $x$ and $y$ each represent a bit, and the line labelled $a$ represents an element of the set $A$. The case of boolean circuits arises as the special case where the cardinality of $A$ is a power of 2.

**Remark 2.2.** The evenness of $\sigma$ is a necessary condition for Theorem 2.1, because all permutations of the forms $f \times 2$ and $2 \times g$ are even, and therefore only even permutations can have an alternation depth.

**Remark 2.3.** Our definition of alternation depth does not require that the permutations $f \in S(2 \times A)$ and $g \in S(A \times 2)$ are themselves even. However, if Theorem 2.1 is to be applied recursively (as required, for example, by the potential applications mentioned in the introduction), we need each $f$ and $g$ to be even. Since the proof of Theorem 2.1 is already complicated enough without this restriction, we do not consider the case of even $f$ and $g$ until Section 6, where we prove that the alternation depth is at most 13 in that case.

Our proof of Theorem 2.1 is in two parts. In Section 3, we will show that every even permutation of a certain form $g + h$ has alternation depth 5. In Section 4, we will show that every even permutation can be decomposed into a permutation of alternation depth 4 and a permutation of the form $g + h$. Together, these results imply Theorem 2.1.

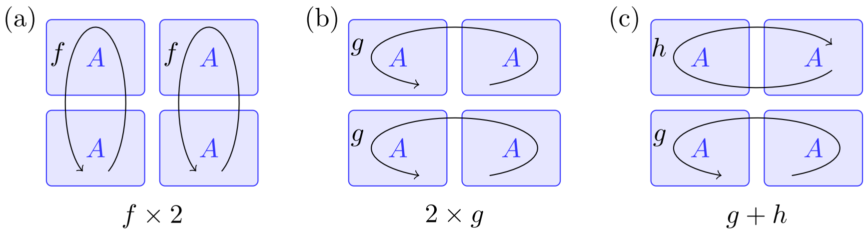



Figure 1: Visualizing permutations of $2 \times A \times 2$

# 3 First construction: balanced permutations

## 3.1 Preliminaries

We fix some terminology. The *support* of a permutation $\sigma \in S(X)$ is the set $\operatorname{supp} \sigma = \{x \in X \mid \sigma(x) \neq x\}$. Two permutations $\sigma, \tau \in S(X)$ are *disjoint* if $\operatorname{supp} \sigma \cap \operatorname{supp} \tau = \emptyset$. In this case, $\sigma$ and $\tau$ commute: $\sigma\tau = \tau\sigma$. We also call $\sigma\tau$ a *disjoint product* in this case. Recall the cycle notation for permutations: for $k > 1$, we write $(a_1\ a_2\ \ldots\ a_k)$, or sometimes $(a_1, a_2, \ldots, a_k)$, for the permutation with support $\{a_1, \ldots, a_k\}$ defined by $a_1 \mapsto a_2$, $a_2 \mapsto a_3$, $\ldots$, $a_{k-1} \mapsto a_k$ and $a_k \mapsto a_1$. Such a permutation is also called a *$k$-cycle*. Every permutation can be uniquely decomposed (up to the order of the factors) into a product of disjoint cycles. A $k$-cycle is even if and only if $k$ is odd.

Two permutations $\sigma, \sigma' \in S(X)$ are *similar*, in symbols $\sigma \sim \sigma'$, if there exists $\tau$ such that $\sigma' = \tau^{-1}\sigma\tau$. It is easy to see that $\sigma, \sigma'$ are similar if and only if their cycle decompositions contain an equal number of $k$-cycles for every $k$.

If $g, h \in S(X)$ are permutations on some finite set $X$, we define their *disjoint sum* $g + h \in S(2 \times X)$ by

$$(g + h)(0, x) = (0, g(x)) \quad \text{and} \quad (g + h)(1, x) = (1, h(x)).$$

We note the following properties:

$$\begin{aligned} g + g &= 2 \times g, && (3) \\ (g + h) \times 2 &= g \times 2 + h \times 2, && (4) \\ (g + h)(g' + h') &= gg' + hh'. && (5) \end{aligned}$$

Property (3) also helps explain our choice of writing "2" for the identity permutation in $S(2)$.

Although it will not be strictly necessary for the proofs that follow (which are combinatorial), it may sometimes be helpful to visualize sets of the form $2 \times A \times 2$, and permutations thereon, as follows. We visualize the set $2 \times A$ as two copies of $A$ stacked vertically, with elements of the form $(0, a)$ and $(1, a)$ belonging to the lower and upper copy, respectively. Similarly, we visualize the set $A \times 2$ as two copies of $A$ side by side, with elements of the form $(a, 0)$ and $(a, 1)$ belonging to the left and right copy, respectively. In the same vein, we visualize the set $2 \times A \times 2$ as four copies of $A$ arranged in two rows and columns. The effect of a permutations of the form $f \times 2$ is to apply $f$ separately to the left and right column, as shown in Figure 1(a). Similarly, the effect of $2 \times g$ is to apply $g$ separately to the top and bottom rows, and the effect of $g + h$ is to apply $g$ to the bottom row and $h$ to the top row, as shown in Figure 1(b) and (c).

## 3.2 Decomposition into balanced permutations

**Definition.** A permutation $\sigma$ is *balanced* if the number of $k$-cycles in its cycle decomposition is even for all $k \geqslant 2$. Moreover, $\sigma$ is *nearly balanced* if the number of $k$-cycles in its cycle decomposition is even for all $k \geqslant 3$.

For example, the permutation (1 2)(3 4)(5 6 7)(8 9 10) is balanced, the permutation (1 2)(3 4 5)(6 7 8) is nearly balanced, and (1 2)(3 4)(5 6 7) is neither balanced nor nearly balanced.

**Remark 3.1.** The disjoint product of any number of (nearly) balanced permutations is (nearly) balanced. Moreover, a nearly balanced permutation is balanced if and only if it is even.

The purpose of this subsection is to prove that every even permutation on a set of 5 or more elements can be decomposed into a product of two balanced permutations. This will be Proposition 3.8 below. The proof requires a sequence of lemmas.

**Lemma 3.2.** *Let $\sigma$ be a $k$-cycle, where $k \geqslant 2$ and $k \neq 3$. Then there exists a balanced permutation $\rho$ and a nearly balanced permutation $\tau$ such that $\sigma = \tau\rho$. Moreover,* $\operatorname{supp}\tau \cup \operatorname{supp}\rho \subseteq \operatorname{supp}\sigma$.

*Proof.* Let $\sigma = (a_1\ a_2\ \dots\ a_k)$. If $k = 2t$ is even, let

$$\begin{aligned} \rho &= (a_1\ a_2\ \dots\ a_t)(a_{t+1}\ a_{t+2}\ \dots\ a_{2t}), \\ \tau &= (a_1\ a_{t+1}). \end{aligned}$$

If $k = 2t+1$ is odd (and therefore, by assumption, $t \geqslant 2$), let

$$\begin{aligned} \rho &= (a_1\ a_2\ \dots\ a_t)(a_{t+1}\ a_{t+3}\ a_{t+4}\ \dots\ a_{2t+1}), \\ \tau &= (a_1\ a_{t+1})(a_{t+2}\ a_{t+3}). \end{aligned}$$

In both cases, the conclusion of the lemma is satisfied. □

**Lemma 3.3.** *Let $\sigma$ be the disjoint product of a 3-cycle and a $k$-cycle, where $k \geqslant 2$. Then there exists a balanced permutation $\rho$ and a nearly balanced permutation $\tau$ such that $\sigma = \tau\rho$. Moreover,* $\operatorname{supp}\tau \cup \operatorname{supp}\rho \subseteq \operatorname{supp}\sigma$.

*Proof.* Let $\sigma = (b_1\ b_2\ b_3)(a_1\ a_2\ \dots\ a_k)$. If $k = 2$, let

$$\begin{aligned} \rho &= (b_1\ b_2)(a_1\ a_2), \\ \tau &= (b_1\ b_3). \end{aligned}$$

If $k = 3$, let

$$\begin{aligned} \rho &= (b_1\ b_2)(a_1\ a_2), \\ \tau &= (b_1\ b_3)(a_1\ a_3), \end{aligned}$$

If $k = 4$, let

$$\begin{aligned} \rho &= (b_1\ b_2\ b_3)(a_1\ a_2\ a_3), \\ \tau &= (a_1\ a_4). \end{aligned}$$

If $k = 2t+1$ is odd, with $t \geqslant 2$, let

$$\begin{aligned} \rho &= (b_1\ b_2\ b_3)(a_t\ a_{t+1}\ a_{2t+1}), \\ \tau &= (a_1\ a_2\ \dots\ a_t)(a_{t+2}\ a_{t+3}\ \dots\ a_{2t+1}). \end{aligned}$$

If $k = 2t$ is even, with $t \geqslant 3$, let

$$\begin{aligned} \rho &= (a_3\ a_4\ \dots\ a_t\ a_{2t})(a_{t+1}\ a_{t+2}\ \dots\ a_{2t-1}), \\ \tau &= (b_1\ b_2\ b_3)(a_1\ a_2\ a_3)(a_{t+1}\ a_{2t}). \end{aligned}$$

In all cases, the conclusion of the lemma is satisfied. □

**Lemma 3.4.** *Let $\sigma$ be a disjoint product of two or more 3-cycles. Then there exist balanced permutations $\rho, \tau$ such that $\sigma = \tau\rho$. Moreover,* $\operatorname{supp}\tau \cup \operatorname{supp}\rho \subseteq \operatorname{supp}\sigma$.

*Proof.* By assumption, $\sigma$ can be factored as $\sigma = \gamma_1\gamma_2\cdots\gamma_\ell$, where $\gamma_1,\ldots,\gamma_\ell$ are pairwise disjoint 3-cycles and $\ell \geqslant 2$. Note that $\gamma_i^2$ is also a 3-cycle, and $\gamma_i^4 = \gamma_i$, for all $i$.

If $\ell$ is even, let $\rho = \tau = \gamma_1^2\gamma_2^2\cdots\gamma_\ell^2$. If $\ell$ is odd, let $\rho = \gamma_1\gamma_2^2\gamma_3^2\cdots\gamma_{\ell-1}^2$ and $\tau = \gamma_2^2\gamma_3^2\cdots\gamma_{\ell-1}^2\gamma_\ell$. In both cases, the conclusion of the lemma is satisfied. □

**Lemma 3.5.** *Let $\sigma$ be an even permutation, other than a 3-cycle. Then $\sigma$ can be written as $\sigma = \tau\rho$, where $\rho, \tau$ are balanced.*

*Proof.* By considering the cycle decomposition of $\sigma$, it is easy to see that $\sigma$ can be factored into disjoint factors such that each factor satisfies the premise of one of Lemmas 3.2, 3.3, or 3.4. Let $\sigma = \sigma_1\cdots\sigma_\ell$ be such a factorization. Using the lemmas, each $\sigma_i$ can be written as $\sigma_i = \tau_i\rho_i$, where $\rho_i$ is balanced and $\tau_i$ is nearly balanced. Moreover, since the support of each $\rho_i$ and $\tau_i$ is contained in that of $\sigma_i$, the $\rho_i$ are pairwise disjoint, the $\tau_i$ are pairwise disjoint, and $\rho_i\tau_j = \tau_j\rho_i$ whenever $i \neq j$. Let $\rho = \rho_1\cdots\rho_\ell$ and $\tau = \tau_1\cdots\tau_\ell$. Then we have $\sigma = \tau\rho$. Moreover, by Remark 3.1, $\rho$ is balanced and $\tau$ is nearly balanced. Finally, since $\sigma$ and $\rho$ are even permutations, so is $\tau$, and it follows, again by Remark 3.1, that $\tau$ is balanced. □

**Lemma 3.6.** *Let $\sigma$ be a 3-cycle in $S(X)$, where $|X| \geqslant 5$. Then there exist balanced permutations $\rho, \tau$ such that $\sigma = \tau\rho$.*

*Proof.* Let $\sigma = (a_1\ a_2\ a_3)$. Since $|X| \geqslant 5$, there exist elements $a_4, a_5$ of $X$ that are different from each other and from $a_1,\ldots,a_3$. Let

$$\begin{aligned} \rho &= (a_1\ a_2)(a_4\ a_5), \\ \tau &= (a_1\ a_3)(a_4\ a_5). \end{aligned}$$

Then the conclusion of the lemma is satisfied. □

**Remark 3.7.** Unlike the situation in Lemmas 3.2–3.5, it is not possible to choose $\rho$ and $\tau$ in Lemma 3.6 so that their support is contained in that of $\sigma$. An easy case distinction shows that Lemma 3.6 is false when $|X| \leqslant 4$.

**Proposition 3.8.** *Let $\sigma$ be an even permutation in $S(X)$, where $|X| \geqslant 5$. Then there exist balanced permutations $\rho, \tau$ such that $\sigma = \tau\rho$.*

*Proof.* By Lemma 3.6 if $\sigma$ is a 3-cycle, and by Lemma 3.5 otherwise. □

### 3.3 Alternation depth of permutations of the form $\mathrm{id} + \tau$

Using balanced permutations, we prove that every even permutation of the form $\mathrm{id}+\tau$ has alternation depth 5.

**Proposition 3.9.** *Let $A$ be a finite set of 3 or more elements, and let $\tau \in S(A\times 2)$ be an even permutation. Let $\sigma = \mathrm{id}_{A\times 2} + \tau \in S(2\times A\times 2)$. Then $\sigma$ has an alternating decomposition of depth 5, starting and ending with a factor of the form $2\times g$.*

The proof requires two lemmas.

**Lemma 3.10.** *Let $\tau \in S(A\times 2)$ be a balanced permutation. Then there exist permutations $g \in S(A\times 2)$ and $h \in S(A)$ such that*

$$\tau = g^{-1}(h\times 2)g.$$

*Proof.* For all $k \geqslant 2$, let $y_k$ be the number of $k$-cycles in the cycle decomposition of $\tau$. Since the cycles are disjoint, we have $\sum_k ky_k \leqslant 2|A|$. Since $\tau$ is balanced, all $y_k$ are even. We can therefore find a permutation $h \in S(A)$ whose number of $k$-cycles is exactly $y_k/2$, for all $k$. Since $h\times 2$ and $\tau$ have, by construction, the same number of $k$-cycles for all $k$, we have $h\times 2 \sim \tau$. By definition of similarity, it follows that there exists some $g$ with $\tau = g^{-1}(h\times 2)g$, as claimed. □

**Lemma 3.11.** *Let $\tau \in S(A \times 2)$ be a balanced permutation, and let $\sigma = \mathrm{id}_{A\times 2} + \tau \in S(2 \times A \times 2)$. Then there exist permutations $g \in S(A \times 2)$ and $f \in S(2 \times A)$ such that*

$$\sigma = (2 \times g^{-1})(f \times 2)(2 \times g).$$

*Proof.* By Lemma 3.10, we can find $g \in S(A\times 2)$ and $h \in S(A)$ such that $\tau = g^{-1}(h\times 2)g$. Let $f = \mathrm{id}_A + h \in S(2 \times A)$. Then

$$\begin{array}{rl} & (2 \times g^{-1})(f \times 2)(2 \times g) \\ = & (2 \times g^{-1})((\mathrm{id}_A + h) \times 2)(2 \times g) \\ = & (g^{-1} + g^{-1})(\mathrm{id}_A \times 2 + h \times 2)(g + g) \\ = & (g^{-1}\,\mathrm{id}_{A\times 2}\, g) + (g^{-1}(h \times 2)g) \\ = & \mathrm{id}_{A\times 2} + \tau \\ = & \sigma. \end{array}$$

Here, in addition to the defining properties of $f$, $g$, $h$, and $\sigma$, we have also used (3) and (4) in the second step and (5) in the third step. □

*Proof of Proposition 3.9.* By assumption, $\tau \in S(A \times 2)$ is even. By Proposition 3.8, there exist balanced permutations $\tau_1, \tau_2 \in S(A \times 2)$ such that $\tau = \tau_2\tau_1$. By Lemma 3.11, there exist $g_1, g_2 \in S(A \times 2)$ and $f_1, f_2 \in S(2 \times A)$ such that $\mathrm{id} + \tau_i = (2 \times g_i^{-1})(f_i \times 2)(2 \times g_i)$, for $i = 1, 2$. Then we have:

$$\begin{array}{rcl} \mathrm{id} + \tau & = & (\mathrm{id} + \tau_2)(\mathrm{id} + \tau_1) \\ & = & (2 \times g_2^{-1})(f_2 \times 2)(2 \times g_2)(2 \times g_1^{-1})(f_1 \times 2)(2 \times g_1) \\ & = & (2 \times g_2^{-1})(f_2 \times 2)(2 \times g_2 g_1^{-1})(f_1 \times 2)(2 \times g_1), \end{array}$$

which is the desired decomposition of alternation depth 5. □

### 3.4 Alternation depth of permutations of the form $g + h$

We now come to the main result of Section 3, which is that every even permutation of the form $g + h$ has alternation depth 5.

**Proposition 3.12.** *Let $A$ be a finite set of 3 or more elements, and let $g, h \in S(A \times 2)$ be permutations such that $\sigma = g + h$ is even. Then $\sigma$ has alternation depth 5.*

*Proof.* This is an easy corollary of Proposition 3.9. Let $\tau = hg^{-1} \in S(A \times 2)$, and note that $\tau$ is even. By Proposition 3.9, $\mathrm{id}_{A\times 2} + \tau$ can be written in the form $\mathrm{id} + \tau = (2 \times g_5)(f_4 \times 2)(2 \times g_3)(f_2 \times 2)(2 \times g_1)$. We then have

$$\begin{array}{rcl} \sigma & = & g + h \\ & = & (\mathrm{id} + \tau)(g + g) \\ & = & (\mathrm{id} + \tau)(2 \times g) \\ & = & (2 \times g_5)(f_4 \times 2)(2 \times g_3)(f_2 \times 2)(2 \times g_1 g), \end{array}$$

which proves that $\sigma$ has alternation depth 5. □

# 4 Second construction: colorings

## 4.1 Colorings

As before, let $2 = \{0, 1\}$. If $X$ is any finite set, a *coloring* of $X$ is a map $c : X \to 2$. Here, we think of the binary digits 0 and 1 as *colors*, i.e., $x \in X$ has color $c(x)$. We say that the coloring $c$ is *fair* if there is an equal number of elements of each color, i.e., $|c^{-1}\{0\}| = |c^{-1}\{1\}|$.

The group $S(X)$ acts in a natural way on the colorings of $X$ as follows: we define $\sigma \bullet c = c'$, where $c'(x) = c(\sigma^{-1}(x))$. Note that $(\sigma\tau) \bullet c = \sigma \bullet (\tau \bullet c)$. Also, $\sigma \bullet c$ is fair if and only if $c$ is fair.

On a set of the form $2 \times X$, the *standard coloring* is the one given by $c_{\mathrm{st}}(0, x) = 0$ and $c_{\mathrm{st}}(1, x) = 1$, for all $x$.

(a)

| $p$ | $q$ | $r$ | $p$ | $q$ | $r$ |
|---|---|---|---|---|---|
| 0 | 1 | 1 | 1 | 1 | 1 |
| 0 | 0 | 0 | 1 | 0 | 0 |

(b)

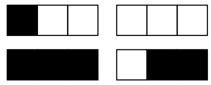


Figure 2: Visualizing colorings of $2 \times A \times 2$

**Remark 4.1.** The standard coloring is fair. Conversely, if $c$ is a fair coloring of $2 \times X$, there exists a permutation $f \in S(2 \times X)$ such that $f \bullet c = c_{\text{st}}$.

The following lemma relates colorings to permutations of the form $g + h$ considered in the previous section.

**Lemma 4.2.** *A permutation $\sigma \in S(2 \times X)$ is of the form $\sigma = g + h$, for some $g, h \in S(X)$, if and only if $\sigma \bullet c_{\text{st}} = c_{\text{st}}$.*

*Proof.* This is elementary. We have $\sigma \bullet c_{\text{st}} = c_{\text{st}}$ if and only if for all $x$, $\sigma(0, x)$ is of the form $(0, y)$, and $\sigma(1, x)$ is of the form $(1, z)$. By setting $g(x) = y$ and $h(x) = z$, this is equivalent to $\sigma$ being of the form $g + h$. □

We are now ready to state the main result of Section 4, which is that every fair coloring of $2 \times A \times 2$ can be converted to the standard coloring by the action of a permutation of alternation depth 4.

**Proposition 4.3.** *Let $A$ be a finite set of 3 or more elements, and let $c$ be a fair coloring of $2 \times A \times 2$. Then there exists a permutation $\sigma \in S(2 \times A \times 2)$ such that $\sigma \bullet c = c_{\text{st}}$ and $\sigma$ has alternation depth 4.*

The proof of Proposition 4.3 will take up the remainder of Section 4.

## 4.2 Visualizing colorings

Colorings on $2 \times A \times 2$ can be visualized in the same row-and-column format we used in Figure 1. An example of a coloring, where $A = \{p, q, r\}$, is shown in Figure 2(a). The figure indicates, for example, that $c(1, p, 0) = 0$, $c(1, q, 0) = 1$, and so on. When the names of the elements of $A$ are not important, we omit them. Additionally, we sometimes represent the colors 0 and 1 by black and white squares, respectively, as in Figure 2(b).

## 4.3 Color pairs

We begin by characterizing when two colorings $c, c'$ of $2 \times X$ are related by the action of a permutation of the form $2 \times g$ for $g \in S(X)$. This is the case if and only if $c$ and $c'$ have the same *color pair distribution.*

**Definition.** Let $X$ be a set, and consider a coloring $c$ of $2 \times X$. We define a function $c^* : X \to 2 \times 2$ by $c^*(x) = (c(0, x), c(1, x))$. We call $c^*(x)$ the *color pair* of $x$.

Informally, a color pair corresponds to a single column of digits in Figure 2(a). We note that the action of permutations $g \in S(X)$ respects color pairs in the following sense: let $c' = (2 \times g) \bullet c$. Then

$$c'^*(g(x)) = (c'(0, g(x)), c'(1, g(x))) = (c(0, x), c(1, x)) = c^*(x). \tag{6}$$

In particular, the action of $2 \times g$ on colorings does not change the *number* of elements of $X$ with each color pair. Conversely, whenever two colorings $c, c'$ have this property, then they are related by the action of $2 \times g$, for some $g$. The following definition helps us state this more precisely.

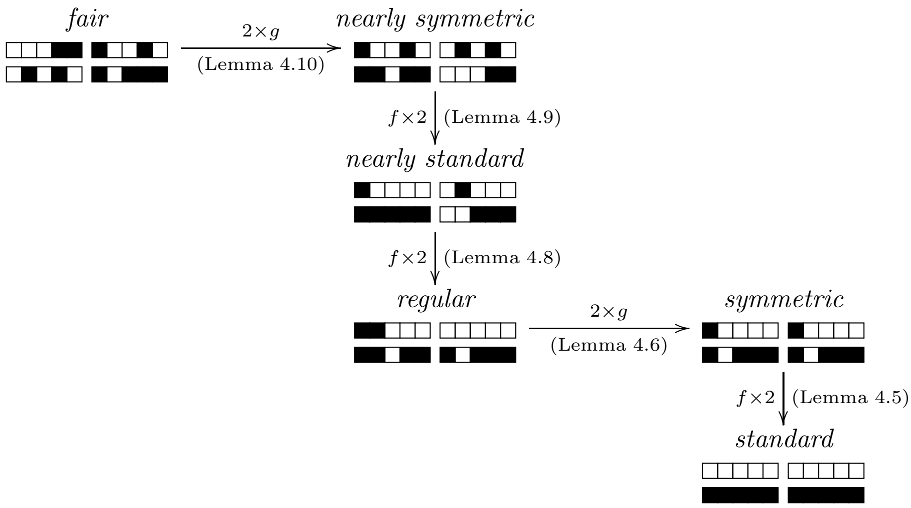



Figure 3: Standardizing a fair permutation

**Definition.** Let $X$ be a set, and $c$ a coloring of $2 \times X$. For any $i, j \in 2$, define $N_c(i,j) \subseteq X$ to be the set of elements with color pair $(i,j)$, i.e.,

$$N_c(i,j) = \{x \in X \mid c^*(x) = (i,j)\}.$$

Note that $X$ is the disjoint union of the $N_c(i,j)$, for $i, j \in 2$. Let $n_c(i,j) = |N_c(i,j)|$ be the number of elements with color pair $(i,j)$. Then the *color pair distribution* of $c$ is the 4-tuple

$$(n_c(0,0), n_c(0,1), n_c(1,0), n_c(1,1)).$$

For example, the coloring from Figure 2 has color pair distribution $(1,4,0,1)$, because the color pair $(0,0)$ occurs once, the color pair $(0,1)$ occurs four times, and so on. The following lemma is then obvious.

**Lemma 4.4.** *Let $c, c'$ be colorings of $2 \times X$. Then $c, c'$ have the same color pair distribution if and only if there exists a permutation $g \in S(X)$ such that $c' = (2 \times g) \bullet c$.* $\square$

## 4.4 Color standardization

**Definition.** Let $A$ be a set, and let $c$ be a coloring of $2 \times A \times 2$. We say that $c$ is

- *standard* if $c = c_{\mathrm{st}}$, i.e., if $c^*(a,0) = c^*(a,1) = (0,1)$ for all $a \in A$;
- *symmetric* if $c^*(a,0) = c^*(a,1)$ for all $a \in A$;
- *regular* if each color pair occurs an even number of times, i.e., if $n_c(0,0)$, $n_c(0,1)$, $n_c(1,0)$, and $n_c(1,1)$ are even;
- *nearly standard* if $c^*(a,0) = c^*(a,1) = (0,1)$ for almost all $a \in A$, except that there is at most one $a_1 \in A$ such that $c^*(a_1,0) = (0,0)$ and $c^*(a_1,1) = (1,1)$, and at most one $a_2 \in A$ such that $c^*(a_2,0) = (0,1)$ and $c^*(a_2,1) = (1,0)$;
- *nearly symmetric* if $c^*(a,0) = c^*(a,1)$ for almost all $a \in A$, except that there is at most one $a_1 \in A$ such that $c^*(a_1,0) = (0,0)$ and $c^*(a_1,1) = (1,1)$, and at most one $a_2 \in A$ such that $c^*(a_2,0) = (0,1)$ and $c^*(a_2,1) = (1,0)$.

An example of each of these properties is shown in Figure 3. Our strategy for proving Proposition 4.3 is to use the action of permutations of the forms $2 \times g$ and $f \times 2$ to successively improve the properties of a coloring until it is standard. This procedure is also outlined in Figure 3, along with the number of the lemma that will be used in each step. The remainder of this section is devoted to the statements and proofs of these lemmas, culminating in the proof of Proposition 4.3 in Section 4.5.

**Lemma 4.5.** *Let $c$ be a symmetric fair coloring of $2 \times A \times 2$. Then there exists $f \in S(2 \times A)$ such that $(f \times 2) \bullet c$ is standard.*

*Proof.* Since $c$ is symmetric, we have $c(i, a, 0) = c(i, a, 1)$ for all $(i, a) \in 2 \times A$; write $p(i, a) = c(i, a, 0)$. Since $c$ is fair, $p : 2 \times A \to 2$ is also fair. By Remark 4.1, there exists a permutation $f \in S(2 \times A)$ such that $f \bullet p$ is the standard coloring of $2 \times A$. It follows that $(f \times 2) \bullet c$ is the standard coloring of $2 \times A \times 2$. $\square$

**Lemma 4.6.** *Let $c$ be a regular coloring of $2 \times A \times 2$. Then there exists $g \in S(A \times 2)$ such that $(2 \times g) \bullet c$ is symmetric.*

*Proof.* Since $c$ is regular, we can find integers $p, q, r, s$ such that $n_c(0, 0) = 2p$, $n_c(1, 1) = 2q$, $n_c(0, 1) = 2r$, and $n_c(1, 0) = 2s$. Note that $n_c(0, 0) + n_c(0, 1) + n_c(1, 0) + n_c(1, 1) = 2|A|$, and therefore $p + q + r + s = |A|$. Write $A$ as a disjoint union of sets $P \cup Q \cup R \cup S$, where $|P| = p$, $|Q| = q$, $|R| = r$, and $|S| = s$. Define a coloring $c'$ by

$$\begin{aligned} c'^*(a, 0) = c'^*(a, 1) &= (0, 0), \quad \text{if } a \in P, \\ c'^*(a, 0) = c'^*(a, 1) &= (1, 1), \quad \text{if } a \in Q, \\ c'^*(a, 0) = c'^*(a, 1) &= (0, 1), \quad \text{if } a \in R, \\ c'^*(a, 0) = c'^*(a, 1) &= (1, 0), \quad \text{if } a \in S. \end{aligned}$$

Then by construction, $c'$ is symmetric and has the same color pair distribution as $c$. Hence by Lemma 4.4, there exists $g \in S(A \times 2)$ such that $c' = (2 \times g) \bullet c$, which was to be shown. $\square$

**Lemma 4.7.** *Suppose $|A| = 3$ and $c$ is a nearly standard coloring of $2 \times A \times 2$. Then there exists $f \in S(2 \times A)$ such that $(f \times 2) \bullet c$ is regular.*

*Proof.* Write $A$ as the disjoint union $A_1 \cup A_2 \cup A_3$, where $c^*(a_1, 0) = (0, 0)$ and $c^*(a_1, 1) = (1, 1)$ for all $a_1 \in A_1$, $c^*(a_2, 0) = (0, 1)$ and $c^*(a_2, 1) = (1, 0)$ for all $a_2 \in A_2$, and $c^*(a, 0) = c^*(a, 1) = (0, 1)$ for all $a \in A_3$. By the definition of nearly standard, we know that $A_1$ and $A_2$ have at most one element each. Since we assumed $|A| = 3$, this leaves us with four cases.

- Case 1. Assume $|A_1| = |A_2| = 0$. Say $A_3 = \{p, q, r\}$. Since $c^*(a, 0) = c^*(a, 1) = (0, 1)$ for all $a \in A$, $c$ is the following coloring (using the notation of Section 4.2):

$$\begin{array}{ccc|ccc} p & q & r & p & q & r \\ \hline 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0. \end{array}$$

  Since $c$ is already regular (in fact, standard), we can take $f$ to be the identity permutation.

- Case 2. Assume $|A_1| = 1$ and $|A_2| = 0$. Say $A_1 = \{a_1\}$ and $A_3 = \{p, q\}$. Then $c$ is the coloring

$$\begin{array}{ccc|ccc} a_1 & p & q & a_1 & p & q \\ \hline 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0. \end{array}$$

  Define $f : 2 \times A \to 2 \times A$ by $f(0, a_1) = (1, p)$, $f(1, p) = (0, q)$, $f(0, q) = (0, a_1)$, and the identity elsewhere. Then $(f \times 2) \bullet c$ is the coloring

$$\begin{array}{ccc|ccc} a_1 & p & q & a_1 & p & q \\ \hline 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1. \end{array}$$

- Case 3. Assume $|A_1| = 0$ and $|A_2| = 1$. Say $A_2 = \{a_2\}$ and $A_3 = \{p, q\}$. Then $c$ is the coloring

$$\begin{array}{ccc|ccc} a_2 & p & q & a_2 & p & q \\ \hline 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0. \end{array}$$

  Define $f : 2 \times A \to 2 \times A$ by $f(0, a_2) = (1, p)$, $f(1, p) = (0, q)$, $f(0, q) = (0, a_2)$, and the identity elsewhere. Then $(f \times 2) \bullet c$ is the coloring

$$\begin{array}{ccc|ccc} a_2 & p & q & a_2 & p & q \\ \hline 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1. \end{array}$$

- Case 4. Assume $|A_1| = |A_2| = 1$. Say $A_1 = \{a_1\}$, $A_2 = \{a_2\}$, and $A_3 = \{p\}$. Then $c$ is the coloring

$$\begin{array}{ccc|ccc} a_1 & a_2 & p & a_1 & a_2 & p \\ \hline 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0. \end{array}$$

  Define $f : 2 \times A \to 2 \times A$ by $f(0, a_1) = (1, a_2)$, $f(1, a_2) = (0, p)$, $f(0, p) = (0, a_1)$, and the identity elsewhere. Then $(f \times 2) \bullet c$ is the coloring

$$\begin{array}{ccc|ccc} a_1 & a_2 & p & a_1 & a_2 & p \\ \hline 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0. \end{array}$$

In all four cases, $(f \times 2) \bullet c$ is regular, as desired. $\square$

**Lemma 4.8.** *Suppose $|A| \geqslant 3$ and $c$ is a nearly standard coloring of $2 \times A \times 2$. Then there exists $f \in S(2 \times A)$ such that $(f \times 2) \bullet c$ is regular.*

*Proof.* The only difference to Lemma 4.7 is that $A$ may have more than 3 elements. However, by the definition of nearly standard, $c$ is already standard (hence regular) on the excess elements. Therefore, we can ignore all but 3 elements of $A$ and proceed as in Lemma 4.7. $\square$

**Lemma 4.9.** *Let $c$ be a nearly symmetric fair coloring of $2 \times A \times 2$. Then there exists $f \in S(2 \times A)$ such that $(f \times 2) \bullet c$ is nearly standard.*

*Proof.* Let $A' = \{a \in A \mid c^*(a, 0) = c^*(a, 1)\}$, and let $c'$ be the coloring of $2 \times A' \times 2$ obtained by restricting $c$ to the domain $2 \times A' \times 2$. Then $c'$ is symmetric. By definition of "nearly symmetric", there exists at most two elements $a_1, a_2 \in A \setminus A'$; moreover, the element $a_1$, if any, satisfies $c^*(a_1, 0) = (0, 0)$ and $c^*(a_1, 1) = (1, 1)$ and the element $a_2$, if any, satisfies $c^*(a_2, 0) = (0, 1)$ and $c^*(a_2, 1) = (1, 0)$. By assumption, $c$ is fair. Since $c$ restricted to $2 \times (A \setminus A') \times 2$ is evidently fair as well, it follows that $c'$ is also fair. We will choose the permutation $f$ so that its support does not touch the elements $a_1$ and $a_2$; it therefore suffices to find some permutation $f' \in S(2 \times A')$ such that $(f' \times 2) \bullet c'$ is standard. But such an $f'$ exists by Lemma 4.5. $\square$

**Lemma 4.10.** *Let $c$ be a fair coloring of $2 \times A \times 2$. Then there exists $g \in S(A \times 2)$ such that $(2 \times g) \bullet c$ is nearly symmetric.*

*Proof.* The proof is very similar to that of Lemma 4.6. Start by considering the color pair distribution $(n_c(0, 0), n_c(0, 1), n_c(1, 0), n_c(1, 1))$ of the given coloring $c$, and note that

$$n_c(0, 0) + n_c(0, 1) + n_c(1, 0) + n_c(1, 1) = 2|A|. \tag{7}$$

Because $c$ is fair, we must have $n_c(0,0) = n_c(1,1)$, and in particular, $n_c(0,0)$ and $n_c(1,1)$ have the same parity (even or odd). From (7), it follows that $n_c(0,1)$ and $n_c(1,0)$ have the same parity. Therefore, there exist natural numbers $p,q,r,s,t,u$, with $t,u \in \{0,1\}$, such that

$$n_c(0,0) = 2p + t, \quad n_c(1,1) = 2q + t, \quad n_c(0,1) = 2r + u, \quad n_c(1,0) = 2s + u.$$

(As a matter of fact, $p = q$, but we will not make further use of this fact). From (7), we have that $p + q + r + s + t + u = |A|$. Write $A$ as a disjoint union $P \cup Q \cup R \cup S \cup T \cup U$, where $|P| = p$, $|Q| = q$, $|R| = r$, $|S| = s$, $|T| = t$, and $|U| = u$. Define a coloring $c'$ by

$$\begin{array}{rl}
c'^*(a,0) = c'^*(a,1) = (0,0), & \text{if } a \in P, \\
c'^*(a,0) = c'^*(a,1) = (1,1), & \text{if } a \in Q, \\
c'^*(a,0) = c'^*(a,1) = (0,1), & \text{if } a \in R, \\
c'^*(a,0) = c'^*(a,1) = (1,0), & \text{if } a \in S, \\
c'^*(a,0) = (0,0) \quad \text{and} \quad c'^*(a,1) = (1,1), & \text{if } a \in T, \\
c'^*(a,0) = (0,1) \quad \text{and} \quad c'^*(a,1) = (1,0), & \text{if } a \in U.
\end{array}$$

By construction, $c'$ has the same color pair distribution as $c$. Hence by Lemma 4.4, there exists $g \in S(A \times 2)$ such that $c' = (2 \times g) \bullet c$. On the other hand, by construction, $c'$ is nearly symmetric (with $a_1$ being the unique element of $T$, if any, and $a_2$ being the unique element of $U$, if any). □

### 4.5 Proof of Proposition 4.3

Proposition 4.3 is now an easy consequence of Lemmas 4.5–4.10. Figure 3 contains a proof "without words". For readers who prefer a proof "with words", we give it here:

Assume $|A| \geqslant 3$ and let $c$ be a fair coloring of $2 \times A \times 2$. By Lemma 4.10, there exists $g_1 \in S(A \times 2)$ such that $c_1 = (2 \times g_1) \bullet c$ is nearly symmetric. By Lemma 4.9, there exists $f_2 \in S(2 \times A)$ such that $c_2 = (f_2 \times 2) \bullet c_1$ is nearly standard. By Lemma 4.8, there exists $g_3 \in S(A \times 2)$ such that $c_3 = (2 \times g_3) \bullet c_2$ is regular. By Lemma 4.6, there exists $g_4 \in S(A \times 2)$ such that $c_4 = (2 \times g_4) \bullet c_3$ is symmetric. By Lemma 4.5, there exists $f_5 \in S(2 \times A)$ such that $c_5 = (f_5 \times 2) \bullet c_4$ is standard. Let

$$\begin{array}{rcl}
\sigma & = & (f_5 \times 2)(2 \times g_4)(2 \times g_3)(f_2 \times 2)(2 \times g_1) \\
& = & (f_5 \times 2)(2 \times g_4 g_3)(f_2 \times 2)(2 \times g_1).
\end{array}$$

Then $\sigma \bullet c = c_{\mathrm{st}}$, and $\sigma$ has alternation depth 4, as claimed. □

## 5 Proof of the main theorem

Our main result, Theorem 2.1, follows from Propositions 3.12 and 4.3. Specifically, let $\sigma \in S(2 \times A \times 2)$ be an even permutation, and let $c = \sigma^{-1} \bullet c_{\mathrm{st}}$. By Proposition 4.3, we can find $\tau \in S(2 \times A \times 2)$ of alternation depth 4 such that $\tau \bullet c = c_{\mathrm{st}}$. Note that $\tau$ is even by Remark 2.2. Let $\rho = \sigma\tau^{-1}$. Then $\rho$ is also even, and $\rho \bullet c_{\mathrm{st}} = \sigma \bullet (\tau^{-1} \bullet c_{\mathrm{st}}) = \sigma \bullet c = c_{\mathrm{st}}$. Therefore, by Lemma 4.2, $\rho$ is of the form $g + h$, for $g, h \in S(A \times 2)$. By Proposition 3.12, $\rho$ has alternation depth 5, and it follows that $\sigma = \rho\tau$ has alternation depth 9, as claimed. □

## 6 Even alternation depth

As promised in Remark 2.3, we now refine Theorem 2.1 to the case where in each factor of the form $f \times 2$ and $2 \times g$, the permutations $f$ and $g$ are required to be even.

**Definition.** We say that $\sigma \in S(2 \times A \times 2)$ has *even alternation depth* $d$ if it can be written as a product of $d$ factors of the forms $f \times 2$ or $2 \times g$, where each such $f \in S(2 \times A)$ and $g \in S(A \times 2)$ is an even permutation.

We have the following analogue of Theorem 2.1 for even alternation depth:

**Theorem 6.1.** *Let $A$ be a finite set of 3 or more elements. Then every even permutation $\sigma \in S(2 \times A \times 2)$ has even alternation depth 13.*

We prove Theorem 6.1 by appropriately modifying the proof of Theorem 2.1. We first prove that the permutation $\sigma$ in Proposition 4.3 can be chosen to be of even alternation depth 4, and then that the permutation $g + h$ in Proposition 3.12 has even alternation depth 9.

**Lemma 6.2.** *Let $|A| \geqslant 3$, and let $c$ be any coloring of $2 \times A \times 2$. Then there exists an odd permutation $g \in S(A \times 2)$ such that $(2 \times g) \bullet c = c$. Similarly, there exists an odd permutation $f \in S(2 \times A)$ such that $(f \times 2) \bullet c = c$.*

*Proof.* Recall from Section 4.3 that we can associate to each element $x \in A \times 2$ a color pair $c^*(x) \in 2 \times 2$. Since there are more elements in $A \times 2$ than in $2 \times 2$, there must exist two elements $x, y \in A \times 2$ with the same color pair. Let $g$ be the permutation that exchanges $x$ and $y$. Then clearly $g$ is odd and $g \bullet c = c$. The second claim is proved symmetrically. $\square$

**Proposition 6.3.** *The permutation $\sigma$ in Proposition 4.3 can be chosen to be of even alternation depth 4.*

*Proof.* Using Lemma 6.2, each of the permutations $f$ or $g$ constructed in Lemmas 4.5–4.10 can be chosen to be even without affecting the coloring. Hence, all relevant permutations in the proof of Proposition 4.3 can be chosen to be even. $\square$

We now turn to generalizing the results of Section 3 to the evenly alternating case.

**Definition.** A permutation $\sigma$ is *evenly balanced* if it can be written as the disjoint product of two even permutations $\tau$ and $\tau'$, such that $\tau$ and $\tau'$ are similar.

We note that every evenly balanced permutation is balanced, but not vice versa. For example, the permutation $(1\ 2)(3\ 4)$ is balanced, but not evenly balanced. The permutation $(1\ 2\ 3)(4\ 5\ 6)$ is evenly balanced. A permutation is evenly balanced if and only if it is balanced and the total number of odd cycles in its cycle decomposition is divisible by 4.

We have the following generalization of Proposition 3.8:

**Lemma 6.4.** *Let $\sigma$ be an even permutation in $S(X)$, where $|X| \geqslant 6$. Then one of the following two conditions holds:*

*(a) $|X| = 6$ and $\sigma$ is the disjoint product of a 2-cycle and a 4-cycle; or*

*(b) there exist evenly balanced permutations $\rho, \tau$ such that $\sigma = \tau\rho$.*

The proof of Lemma 6.4 is a long and tedious case distinction, and in the interest of readability, we give it separately in Section 7 below.

**Lemma 6.5.** *Let $|X| \geqslant 2$. Every balanced permutation on $X$ commutes with some odd permutation.*

*Proof.* Let $\sigma \in S(X)$ be a balanced permutation. If $\sigma$ is the identity, it commutes with everything, and therefore, since $|X| \geqslant 2$, with some odd permutation. Otherwise, by definition of being balanced, the cycle decomposition of $\sigma$ contains two $k$-cycles $\gamma_1 = (a_1\ a_2\ \ldots\ a_k)$ and $\gamma_2 = (b_1\ b_2\ \ldots\ b_k)$, for some $k \geqslant 2$. If $k$ is even, let $\tau = \gamma_1$. If $k$ is odd, let $\tau = (a_1\ b_1)(a_2\ b_2) \cdots (a_k\ b_k)$. In either case, $\tau$ is an odd permutation and commutes with $\sigma$. $\square$

The next two lemmas generalize Lemmas 3.10 and 3.11, respectively.

**Lemma 6.6.** *Let $\tau \in S(A \times 2)$ be an evenly balanced permutation. Then there exist even permutations $g \in S(A \times 2)$ and $h \in S(A)$ such that $\tau = g^{-1}(h \times 2)g$.*

*Proof.* By Lemma 3.10, we can find $g' \in S(A \times 2)$ and $h \in S(A)$ such that $\tau = g'^{-1}(h \times 2)g'$. Since $\tau$ is evenly balanced, so is $h \times 2$, and it follows that $h$ is even. If $g'$ is even, let $g = g'$, and we are done. If $g'$ is odd, let $g''$ be some odd permutation that commutes with $h \times 2$; such a $g''$ exists by Lemma 6.5. Letting $g = g''g'$, we have $g^{-1}(h \times 2)g = g'^{-1}g''^{-1}(h \times 2)g''g' = g'^{-1}(h \times 2)g' = \tau$. □

**Lemma 6.7.** *Let $\tau \in S(A \times 2)$ be an evenly balanced permutation, and let $\sigma = \mathrm{id}_{A\times 2} + \tau \in S(2 \times A \times 2)$. Then there exist even permutations $g \in S(A \times 2)$ and $f \in S(2 \times A)$ such that*

$$\sigma = (2 \times g^{-1})(f \times 2)(2 \times g).$$

*Proof.* Exactly like the proof of Lemma 3.11, except using Lemma 6.6 instead of Lemma 3.10. □

Next, we deal with two special cases.

**Lemma 6.8.** *Let $|A| \geqslant 3$ and let $\tau \in S(A \times 2)$ be the disjoint product of a 2-cycle and a 4-cycle. Then* $\mathrm{id} + \tau \in S(2 \times A \times 2)$ *has even alternation depth 5, starting and ending with a factor of the form $2 \times g$.*

*Proof.* Let $a, b, c$ be three distinct elements of $A$. First consider the permutation $\tau' \in S(A \times 2)$ that is given, in cycle notation, by

$$\tau' = \big((a, 0), (a, 1)\big)\ \big((b, 0), (c, 0), (c, 1), (b, 1)\big).$$

Let

$$\begin{array}{rcll} g_1 & = & \big((b, 1), (c, 0), (c, 1)\big) & \in \ S(A \times 2), \\ f_2 & = & \big((0, c), (1, c), (1, b)\big) & \in \ S(2 \times A), \\ g_3 & = & \big((a, 0), (a, 1), (b, 1)\big) & \in \ S(A \times 2), \\ f_4 & = & \big((0, b), (0, c), (1, b), (1, a), (1, c)\big) & \in \ S(2 \times A), \\ g_5 & = & \big((a, 0), (b, 1), (c, 1)\big) & \in \ S(A \times 2), \end{array}$$

all of which are even. By a direct calculation, one can verify that

$$\mathrm{id} + \tau' = (2 \times g_5)(f_4 \times 2)(2 \times g_3)(f_2 \times 2)(2 \times g_1), \tag{8}$$

and therefore $\mathrm{id}+\tau'$ has been written in the desired form. Now consider some arbitrary $\tau \in S(A\times 2)$ that is the disjoint product of a 2-cycle and a 4-cycle. Since $\tau$ is similar to $\tau'$, there is some $g \in S(A \times 2)$ such that $\tau = g^{-1}\tau' g$. Without loss of generality, we can assume that $g$ is even, because if it is not, we can replace $g$ by $\big((a, 0), (a, 1)\big)\, g$, noting that $\big((a, 0), (a, 1)\big)$ is odd and commutes with $\tau'$. Then $\mathrm{id}+\tau = (2\times g^{-1})(\mathrm{id}+\tau')(2\times g)$. When combined with (8), this shows that $\mathrm{id} + \tau$ is of the required form. □

**Lemma 6.9.** *Let $|A| \geqslant 2$. There exist permutations $g_1, g_3, g_5 \in S(A\times 2)$ and $f_2, f_4, f_6 \in S(2\times A)$ such that $g_1$ is odd, $f_2, g_3, f_4, g_5, f_6$ are even, and such that*

$$\mathrm{id}_{2\times A\times 2} = (f_6 \times 2)(2 \times g_5)(f_4 \times 2)(2 \times g_3)(f_2 \times 2)(2 \times g_1).$$

*Proof.* Let $a, b$ be distinct elements of $A$. The following permutations, given in cycle notation, satisfy the conclusion of the lemma:

$$\begin{array}{rcll} g_1 & = & \big((a, 0), (b, 1)\big) & \in \ S(A \times 2), \\ f_2 & = & \big((1, b), (0, a), (1, a)\big) & \in \ S(2 \times A), \\ g_3 & = & \big((b, 0), (a, 0), (b, 1)\big) & \in \ S(A \times 2), \\ f_4 & = & \big((1, b), (1, a), (0, a)\big) & \in \ S(2 \times A), \\ g_5 & = & \big((b, 0), (a, 0), (b, 1)\big) & \in \ S(A \times 2), \\ f_6 & = & \big((0, b), (1, b), (1, a)\big) & \in \ S(2 \times A). \end{array}$$

□

The following two propositions generalize Proposition 3.9 and 3.12, respectively, to the evenly alternating case.

**Proposition 6.10.** *Let $A$ be a finite set of 3 or more elements, and let $\tau \in S(A\times 2)$ be an even permutation. Then $\mathrm{id}_{A\times 2}+\tau \in S(2\times A\times 2)$ has an evenly alternating decomposition of depth 5, starting and ending with a factor of the form $2\times g$.*

*Proof.* If $\tau$ is the disjoint product of a 2-cycle and a 4-cycle, the claim follows by Lemma 6.8. Otherwise, by Lemma 6.4, there exist evenly balanced permutations $\tau_1, \tau_2 \in S(A\times 2)$ such that $\tau = \tau_2\tau_1$. By Lemma 6.7, there exist even $g_1, g_2 \in S(A\times 2)$ and $f_1, f_2 \in S(2\times A)$ such that $\mathrm{id}+\tau_i = (2\times g_i^{-1})(f_i\times 2)(2\times g_i)$, for $i = 1, 2$. Therefore

$$\mathrm{id}+\tau = (2\times g_2^{-1})(f_2\times 2)(2\times g_2 g_1^{-1})(f_1\times 2)(2\times g_1),$$

proving the claim. □

**Proposition 6.11.** *Let $A$ be a finite set of 3 or more elements, and let $g, h \in S(A\times 2)$ be permutations such that $\sigma = g+h$ is even. Then $\sigma$ has even alternation depth 9.*

*Proof.* Let $\tau = hg^{-1} \in S(A\times 2)$, and note that $\tau$ is even. By Proposition 6.10, $\mathrm{id}+\tau$ can be written in the form $(2\times g_5)(f_4\times 2)(2\times g_3)(f_2\times 2)(2\times g_1)$, where all the $f_i$ and $g_j$ are even. As in the proof of Proposition 3.12, we have

$$\sigma = g+h = (2\times g_5)(f_4\times 2)(2\times g_3)(f_2\times 2)(2\times g_1 g). \tag{9}$$

If $g$ is even, we are done; in fact, in this case, $\sigma$ has even alternation depth 5. So assume $g$ is odd. By Lemma 6.9, there exists an odd permutation $g_6 \in S(A\times 2)$ and even permutations $f_7, f_9, f_{11} \in S(2\times A)$ and $g_8, g_{10} \in S(A\times 2)$ such that

$$\mathrm{id} = (f_{11}\times 2)(2\times g_{10})(f_9\times 2)(2\times g_8)(f_7\times 2)(2\times g_6). \tag{10}$$

Combining (9) and (10), we have

$$\sigma = (2\times g_5)(f_4\times 2)(2\times g_3)(f_2 f_{11}\times 2)(2\times g_{10})(f_9\times 2)(2\times g_8)(f_7\times 2)(2\times g_6 g_1 g),$$

and since $g_6 g_1 g$ is even, this demonstrates that $\sigma$ has even alternation depth 9. □

Finally, Theorem 6.1 follows from Propositions 6.3 and 6.11 in exactly the same way as Theorem 2.1 was shown to follow from Propositions 4.3 and 3.12 in Section 5.

# 7 Proof of Lemma 6.4

Recall that a cycle of length $k$ is an even permutation if and only if $k$ is odd. We denote a conjugacy class of permutations by $k_1 \cup \ldots \cup k_n$, where $k_1, \ldots, k_n$ are the lengths of the cycles in its cycle decomposition. We further schematically write $k^+$ for any cycle of length $k+4i$, where $i \in \{0, 1, 2, \ldots\}$.

We say that an even non-identity permutation is *atomic* if it cannot be factored into disjoint smaller even non-identity permutations. Clearly every even permutation can be factored into disjoint atoms. The atomic permutations are exactly: (a) odd-length cycles, and (b) disjoint products of two even-length cycles. Using the above notations, we can further divide the atomic permutations into 14 cases:

$$\underline{3},\ \underline{5},\ 7^+,\ 9^+,\ \underline{2\cup 2},\ \underline{2\cup 4},\ 2\cup 6^+,\ 2\cup 8^+,\ 4\cup 4,\ 4\cup 6^+,\ 4\cup 8^+,\ 6^+\cup 6^+,\ 6^+\cup 8^+,\ 8^+\cup 8^+. \tag{11}$$

An atom is called *special* if it has been underlined in (11). Therefore, the four special atoms are $\underline{3}$, $\underline{5}$, $\underline{2\cup 2}$, and $\underline{2\cup 4}$. An even permutation is *decomposable* if it can be written as a product of two evenly balanced permutations.

**Proposition 7.1.** *Every even permutation, other than a special atom, is decomposable. Moreover, if the size of the domain is* 6 *or greater, the special atoms $\underline{3}$, $\underline{5}$, $\underline{2\cup 2}$ are decomposable. Moreover, if the size of the domain is* 7 *or greater, the special atom $\underline{2\cup 4}$ is decomposable.*

*Proof.* Let us schematically write $A$ for a non-special atom and $\underline{A}$ for a special atom. To prove the first claim of Proposition 7.1, it is sufficient to show that the following are decomposable:

$$(1)\ A, \quad (2)\ \underline{A} \cup \underline{A}, \quad (3)\ \underline{A} \cup A, \quad (4)\ \underline{A} \cup \underline{A} \cup \underline{A}.$$

This is because every even permutation (except special atoms) can be decomposed into disjoint factors of the forms (1)–(4). (This follows by an easy induction on the number of special atoms). To prove the second and third claims of Proposition 7.1, we must moreover show that the following is decomposable when the size of the domain is large enough:

$$(0)\ \underline{A}.$$

Since each atom is of one of the fourteen types shown in (11), each claim (0)–(4) amounts to a finite case distinction. We exhibit a particular decomposition into evenly balanced permutations for each of the cases.

For greater brevity, we use the following convention in the cycle notation for permutations. Let $i, j \in \{0, 1, 2, \ldots\}$. We write $n^\bullet$ as a shorthand for a list of $2i+1$ elements $n_1, \ldots, n_{2i+1}$, and we similarly write $m^\circ$ as a shorthand for a list of $2j+1$ elements $m_1, \ldots, m_{2j+1}$. Thus, $(1^\bullet, 2, 3)$ denotes the $(2i+3)$-cycle $(1_1, \ldots, 1_{2i+1}, 2, 3)$, and $(1^\bullet, 2^\circ, 3)$ denotes the $(2i+2j+3)$-cycle $(1_1, \ldots, 1_{2i+1}, 2_1, \ldots, 2_{2j+1}, 3)$. Here, it is understood that multiple $n^\bullet$ notations appearing in the same equation share the same value of $i$, and multiple $m^\circ$ notations share the same value of $j$.

(0) **Decomposition of $\underline{A}$ (4 cases)**

- $\underline{3}$, where $|X| \geqslant 6$: $(1,2,3) = (1,3,2)(4,5,6) \circ (1,3,2)(4,6,5)$.
- $\underline{5}$, where $|X| \geqslant 6$: $(1,2,3,4,5) = (1,4,3)(2,6,5) \circ (1,5,3)(2,4,6)$.
- $\underline{2 \cup 2}$, where $|X| \geqslant 6$: $(1,2)(3,4) = (1,3,5)(2,4,6) \circ (1,6,4)(2,5,3)$.
- $\underline{2 \cup 4}$, where $|X| \geqslant 7$: $(1,2)(3,4,5,6) = (2,4,3)(5,6,7) \circ (1,3,2)(4,7,6)$.

(1) **Decomposition of $A$ (10 cases)**

- $7^+$: $(1^\bullet,2,3,4^\bullet,5,6,7) = (1,6,5)(2,3,7) \circ (1^\bullet,7,5)(4^\bullet,6,3)$.
- $9^+$: $(1^\bullet,2,3,4^\bullet,5,6,7,8,9) = (2,3,8)(5,6,7) \circ (1^\bullet,8,9)(4^\bullet,7,3)$.
- $2 \cup 6^+$: $(1,2)(3^\bullet,4^\bullet,5,6,7,8) = (3,1,4)(5,6,7) \circ (3^\bullet,1,2)(4^\bullet,7,8)$.
- $2 \cup 8^+$: $(1,2)(3^\bullet,4,5,6^\bullet,7,8,9,10) = (3,2,6)(7,9,8) \circ (3^\bullet,4,5,2,1)(6^\bullet,8,7,9,10)$.
- $4 \cup 4$: $(1,2,3,4)(5,6,7,8) = (1,2,4)(3,6,5) \circ (2,5,3)(6,7,8)$.
- $4 \cup 6^+$: $(1,2,3,4)(5^\bullet,6^\bullet,7,8,9,10) = (2,6,5)(7,9,8) \circ (1,5^\bullet,2,3,4)(6^\bullet,8,7,9,10)$.
- $4 \cup 8^+$: $(1,2,3,4)(5^\bullet,6^\bullet,7,8,9,10,11,12)$
  $= (2,6,5)(8,9,10) \circ (1,5^\bullet,2,3,4)(6^\bullet,7,10,11,12)$.
- $6^+ \cup 6^+$: $(1^\bullet,2^\bullet,3,4,5,6)(7^\circ,8,9,10^\circ,11,12)$
  $= (2,5)(7,10)(8,11)(9,12) \circ (1^\bullet,5,6)(2^\bullet,3,4)(7^\circ,11,9)(10^\circ,8,12)$.
- $6^+ \cup 8^+$: $(1^\bullet,2^\bullet,3,4,5,6)(7,8^\circ,9^\circ,10,11,12,13,14)$
  $= (2,5)(7,8)(9,13)(10,11) \circ (1^\bullet,5,6)(2^\bullet,3,4)(8^\circ,13,14)(9^\circ,11,12)$.
- $8^+ \cup 8^+$: $(1,2,3,4,5,6,7^\bullet,8^\bullet)(9,10^\circ,11^\circ,12,13,14,15,16)$
  $= (1,2)(3,7,4)(5,6,8)(9,10)(11,15)(12,13)$
  $\circ\, (2,4,8^\bullet)(3,7^\bullet,6)(10^\circ,15,16)(11^\circ,13,14)$.

(2) **Decomposition of $\underline{A} \cup \underline{A}$ (10 cases)**

- $\underline{3} \cup \underline{3}$: $(1,2,3)(4,5,6) = \mathrm{id} \circ (1,2,3)(4,5,6)$.
- $\underline{3} \cup \underline{5}$: $(1,2,3)(4,5,6,7,8) = (1,3,2)(6,7,8) \circ (1,3,2)(4,5,8)$.

- $\underline{3} \cup (\underline{2 \cup 2})$: $(1,2,3)(4,5)(6,7) = (1,3,2)(4,7,6) \circ (1,3,2)(4,5,6)$.
- $\underline{3} \cup (\underline{2 \cup 4})$: $(1,2,3)(4,5)(6,7,8,9) = (1,2,3)(4,7,6) \circ (4,5,6)(7,8,9)$.
- $\underline{5} \cup \underline{5}$: $(1,2,3,4,5)(6,7,8,9,10) = \mathrm{id} \circ (1,2,3,4,5)(6,7,8,9,10)$.
- $\underline{5} \cup (\underline{2 \cup 2})$: $(1,2,3,4,5)(6,7)(8,9) = (2,3,4)(6,8,9) \circ (1,4,5)(6,7,9)$.
- $\underline{5} \cup (\underline{2 \cup 4})$: $(1,2,3,4,5)(6,7)(8,9,10,11)$
  $= (2,5)(3,4)(8,11)(9,10) \circ (1,5)(2,4)(6,7)(8,10)$.
- $(\underline{2 \cup 2}) \cup (\underline{2 \cup 2})$: $(1,2)(3,4)(5,6)(7,8) = \mathrm{id} \circ (1,2)(3,4)(5,6)(7,8)$.
- $(\underline{2 \cup 2}) \cup (\underline{2 \cup 4})$: $(1,2)(3,4)(5,6)(7,8,9,10)$
  $= (1,4)(2,3)(7,10)(8,9) \circ (1,3)(2,4)(5,6)(7,9)$.
- $(\underline{2 \cup 4}) \cup (\underline{2 \cup 4})$: $(1,2)(3,4,5,6)(7,8)(9,10,11,12)$
  $= \mathrm{id} \circ (1,2)(3,4,5,6)(7,8)(9,10,11,12)$.

(3) **Decomposition of $\underline{A} \cup A$ (40 cases)**

- $\underline{3} \cup 7^+$: $(1,2,3)(4^\bullet,5,6,7^\bullet,8,9,10) = (1,2,3)(5,6,9) \circ (4^\bullet,9,10)(6,7^\bullet,8)$.
- $\underline{3} \cup 9^+$: $(1,2,3)(4,5^\bullet,6,7,8,9,10^\bullet,11,12)$
  $= (2,6,4)(8,9,10) \circ (1,4,5^\bullet,2,3)(6,7,10^\bullet,11,12)$.
- $\underline{3} \cup (2 \cup 6^+)$: $(1,2,3)(4,5)(6^\bullet,7,8,9^\bullet,10,11)$
  $= (1,2)(4,5)(7,11)(8,10) \circ (2,3)(6^\bullet,11)(7,10)(8,9^\bullet)$.
- $\underline{3} \cup (2 \cup 8^+)$: $(1,2,3)(4,5)(6^\bullet,7,8,9^\bullet,10,11,12,13)$
  $= (1,2,3)(4,5,6)(7,8,13)(10,11,12) \circ (5,6^\bullet,13)(8,9^\bullet,12)$.
- $\underline{3} \cup (4 \cup 4)$: $(1,2,3)(4,5,6,7)(8,9,10,11)$
  $= (1,2)(4,5)(6,7)(9,11) \circ (2,3)(5,7)(8,11)(9,10)$.
- $\underline{3} \cup (4 \cup 6^+)$: $(1,2,3)(4,5,6,7)(8^\bullet,9,10^\bullet,11,12,13)$
  $= (1,2,3)(4,9,8) \circ (4,5,6,7,8^\bullet)(9,10^\bullet,11,12,13)$.
- $\underline{3} \cup (4 \cup 8^+)$: $(1,2,3)(4,5,6,7)(8^\bullet,9,10^\bullet,11,12,13,14,15)$
  $= (1,2)(4,5)(6,7)(10,14) \circ (2,3)(5,7)(8^\bullet,9,14,15)(10^\bullet,11,12,13)$.
- $\underline{3} \cup (6^+ \cup 6^+)$: $(1,2,3)(4,5,6^\bullet,7^\bullet,8,9)(10^\circ,11^\circ,12,13,14,15)$
  $= (1,2,3)(4,5,6)(7,9)(12,13)(11,14)(10,15) \circ (6^\bullet,9)(7^\bullet,8)(10^\circ,14)(11^\circ,13)$.
- $\underline{3} \cup (6^+ \cup 8^+)$: $(1,2,3)(4^\bullet,5^\bullet,6,7,8,9)(10,11^\circ,12^\circ,13,14,15,16,17)$
  $= (1,2,3)(6,9,8)(5,7)(10,11)(12,16)(13,14)$
  $\circ\, (4^\bullet,7,9)(5^\bullet,8,6)(11^\circ,16,17)(12^\circ,14,15)$.
- $\underline{3} \cup (8^+ \cup 8^+)$: $(1,2,3)(4,5^\bullet,6^\bullet,7,8,9,10,11)(12^\circ,13^\circ,14,15,16,17,18,19)$
  $= (1,2)(4,5)(6,11)(7,10)(8,9)(13,19)(14,18)(15,17)$
  $\circ\, (2,3)(5^\bullet,11)(6^\bullet,10)(7,9)(12^\circ,19)(13^\circ,18)(14,17)(15,16)$.
- $\underline{5} \cup 7^+$: $(1,2,3,4,5)(6,7,8,9,10,11^\bullet,12^\bullet)$
  $= (3,5,4)(6,11,12) \circ (1,2,4,3,5)(6,7,8,9,10)(11^\bullet)(12^\bullet)$.
- $\underline{5} \cup 9^+$: $(1,2,3,4,5)(6^\bullet,7,8,9^\bullet,10,11,12,13,14)$
  $= (1,2,3,4,5)(7,8,11,12,13) \circ (6^\bullet,13,14)(8,9^\bullet,10)$.
- $\underline{5} \cup (2 \cup 6^+)$: $(1,2,3,4,5)(6,7)(8,9,10^\bullet,11^\bullet,12,13)$
  $= (2,6,7,3,5)(9,10,11,12,13) \circ (1,5)(2,7)(3,4)(8,13)(10^\bullet)(11^\bullet)$.
- $\underline{5} \cup (2 \cup 8^+)$: $(1,2,3,4,5)(6,7)(8,9,10^\bullet,11,12^\bullet,13,14,15)$
  $= (2,5)(3,4)(6,7)(8,12) \circ (1,5)(2,4)(8,9,10^\bullet,11)(12^\bullet,13,14,15)$.
- $\underline{5} \cup (4 \cup 4)$: $(1,2,3,4,5)(6,7,8,9)(10,11,12,13)$
  $= (2,3,5)(11,13,12) \circ (1,5)(3,4)(6,7,8,9)(10,12,11,13)$.

- $\underline{5} \cup (4 \cup 6^+)$: $(1,2,3,4,5)(6,7,8,9)(10,11^\bullet,12,13,14^\bullet,15)$
$= (2,5)(3,4)(7,9)(10,13) \circ (1,5)(2,4)(6,9)(7,8)(10,11^\bullet,12)(13,14^\bullet,15)$.
- $\underline{5} \cup (4 \cup 8^+)$: $(1,2,3,4,5)(6,7,8,9)(10,11^\bullet,12,13,14,15^\bullet,16,17)$
$= (1,2)(4,5)(6,7,9,8)(10,13,14,17) \circ (2,3,5)(7,9,8)(10,11^\bullet,12)(14,15^\bullet,16)$.
- $\underline{5} \cup (6^+ \cup 6^+)$: $(1,2,3,4,5)(6^\bullet,7^\bullet,8,9,10,11)(12^\circ,13^\circ,14,15,16,17)$
$= (2,3,5)(6,7,8)(15,17,16)(12,13,14)$
$\circ\, (1,5)(3,4)(8,9,10,11)(6^\bullet)(7^\bullet)(14,16,15,17)(12^\circ)(13^\circ)$.
- $\underline{5} \cup (6^+ \cup 8^+)$: $(1,2,3,4,5)(6,7^\bullet,8,9,10^\bullet,11)(12^\circ,13,14,15,16^\circ,17,18,19)$
$= (2,5)(3,4)(6,9)(12,16)$
$\circ\, (1,5)(2,4)(6,7^\bullet,8)(9,10^\bullet,11)(12^\circ,13,14,15)(16^\circ,17,18,19)$.
- $\underline{5} \cup (8^+ \cup 8^+)$: $(1,2,3,4,5)(6^\bullet,7,8,9,10^\bullet,11,12,13)(14^\circ,15,16,17^\circ,18,19,20,21)$
$= (1,2)(4,5)(7,9,10,12,8,13)(15,16,17,19,20,21)$
$\circ\, (2,3,5)(6^\bullet,13)(7,12,8)(10^\bullet,11)(14^\circ,21)(17^\circ,18)$.
- $(\underline{2 \cup 2}) \cup 7^+$: $(1,2)(3,4)(5,6^\bullet,7^\bullet,8,9,10,11)$
$= (1,2)(3,4)(5,6)(7,10) \circ (6^\bullet,10,11)(7^\bullet,8,9)$.
- $(\underline{2 \cup 2}) \cup 9^+$: $(1,2)(3,4)(5^\bullet,6,7,8^\bullet,9,10,11,12,13)$
$= (1,4,3)(5,8,11) \circ (1,2,3)(5^\bullet,6,7)(8^\bullet,9,10)(11,12,13)$.
- $(\underline{2 \cup 2}) \cup (2 \cup 6^+)$: $(1,2)(3,4)(5,6)(7^\bullet,8,9,10^\bullet,11,12)$
$= (1,2)(3,4)(5,6)(7,10) \circ (7^\bullet,8,9)(10^\bullet,11,12)$.
- $(\underline{2 \cup 2}) \cup (2 \cup 8^+)$: $(1,2)(3,4)(5,6)(7^\bullet,8,9,10,11^\bullet,12,13,14)$
$= (1,4)(2,3)(7,10)(11,14) \circ (1,3)(2,4)(5,6)(7^\bullet,8,9)(10,14)(11^\bullet,12,13)$.
- $(\underline{2 \cup 2}) \cup (4 \cup 4)$: same as $(\underline{2 \cup 4}) \cup (\underline{2 \cup 4})$.
- $(\underline{2 \cup 2}) \cup (4 \cup 6^+)$: $(1,2)(3,4)(5,6,7,8)(9^\bullet,10,11,12^\bullet,13,14)$
$= (1,3)(2,4)(6,8)(9,12) \circ (1,4)(2,3)(5,8)(6,7)(9^\bullet,10,11)(12^\bullet,13,14)$.
- $(\underline{2 \cup 2}) \cup (4 \cup 8^+)$: $(1,2)(3,4)(5,6,7,8)(9^\bullet,10,11,12,13^\bullet,14,15,16)$
$= (1,2)(3,4)(5,6,7,8)(9,12,13,16) \circ (9^\bullet,10,11)(13^\bullet,14,15)$.
- $(\underline{2 \cup 2}) \cup (6^+ \cup 6^+)$: $(1,2)(3,4)(5^\bullet,6,7,8^\bullet,9,10)(11^\circ,12,13,14^\circ,15,16)$
$= (1,2)(3,4)(5,8)(11,14) \circ (5^\bullet,6,7)(8^\bullet,9,10)(11^\circ,12,13)(14^\circ,15,16)$.
- $(\underline{2 \cup 2}) \cup (6^+ \cup 8^+)$: $(1,2)(3,4)(5^\bullet,6,7,8^\bullet,9,10)(11,12,13^\circ,14^\circ,15,16,17,18)$
$= (1,4)(2,3)(5,8)(11,12,13)(14,18)(15,16,17)$
$\circ\, (1,3)(2,4)(5^\bullet,6,7)(8^\bullet,9,10)(13^\circ,18)(14^\circ,17)$.
- $(\underline{2 \cup 2}) \cup (8^+ \cup 8^+)$: $(1,2)(3,4)(5^\bullet,6,7,8,9^\bullet,10,11,12)(13^\circ,14,15,16,17^\circ,18,19,20)$
$= (1,2)(3,4)(5,8,9,12)(13,16,17,20)$
$\circ\, (5^\bullet,6,7)(9^\bullet,10,11)(13^\circ,14,15)(17^\circ,18,19)$.
- $(\underline{2 \cup 4}) \cup 7^+$: $(1,2)(3,4,5,6)(7^\bullet,8,9,10,11^\bullet,12,13)$
$= (2,3,6)(7,10,11) \circ (1,6,2)(3,4,5)(7^\bullet,8,9)(11^\bullet,12,13)$.
- $(\underline{2 \cup 4}) \cup 9^+$: $(1,2)(3,4,5,6)(7,8^\bullet,9,10,11^\bullet,12,13,14,15)$
$= (3,4)(5,6)(7,8)(11,15) \circ (1,2)(4,6)(8^\bullet,9,10,15)(11^\bullet,12,13,14)$.
- $(\underline{2 \cup 4}) \cup (2 \cup 6^+)$: same as $(\underline{2 \cup 2}) \cup (4 \cup 6^+)$.
- $(\underline{2 \cup 4}) \cup (2 \cup 8^+)$: same as $(\underline{2 \cup 2}) \cup (4 \cup 8^+)$.
- $(\underline{2 \cup 4}) \cup (4 \cup 4)$: $(1,2)(3,4,5,6)(7,8,9,10)(11,12,13,14)$
$= (3,6,5)(7,8,9) \circ (1,2)(3,4,6,5)(9,10)(11,12,13,14)$.
- $(\underline{2 \cup 4}) \cup (4 \cup 6^+)$: $(1,2)(3,4,5,6)(7,8,9,10)(11^\bullet,12,13,14^\bullet,15,16)$
$= (1,2)(3,4,5,6)(7,8,9,10)(11,14) \circ (11^\bullet,12,13)(14^\bullet,15,16)$.

- $(\underline{2\cup 4})\cup(4\cup 8^+)$: $(1,2)(3,4,5,6)(7,8,9,10)(11^\bullet,12,13,14,15^\bullet,16,17,18)$
$= (1,2)(3,5,6,4)(7,8)(11,14,15,18)$
$\circ\ (3,6,4)(8,9,10)(11^\bullet,12,13)(15^\bullet,16,17)$.
- $(\underline{2\cup 4})\cup(6^+\cup 6^+)$: $(1,2)(3,4,5,6)(7,8,9,10,11^\bullet,12^\bullet)(13^\circ,14,15,16^\circ,17,18)$
$= (1,2)(3,5,6,4)(7,10,11,12)(13,16)$
$\circ\ (3,6,4)(7,8,9)(11^\bullet)(12^\bullet)(13^\circ,14,15)(16^\circ,17,18)$.
- $(\underline{2\cup 4})\cup(6^+\cup 8^+)$: $(1,2)(3,4,5,6)(7^\bullet,8,9,10^\bullet,11,12)(13^\circ,14,15,16,17^\circ,18,19,20)$
$= (1,2)(3,4,5,6)(7,10)(13,16,17,20)$
$\circ\ (7^\bullet,8,9)(10^\bullet,11,12)(13^\circ,14,15)(17^\circ,18,19)$.
- $(\underline{2\cup 4})\cup(8^+\cup 8^+)$: $(1,2)(3,4,5,6)(7,8,9^\bullet,10,11,12^\bullet,13,14)(15^\circ,16,17,18,19^\circ,20,21,22)$
$= (1,2)(3,5,6,4)(7,8)(9^\bullet,10,11)(12^\bullet,13,14)(15,18,19,22)$
$\circ\ (3,6,4)(8,11,14)(15^\circ,16,17)(19^\circ,20,21)$.

(4) **Decomposition of $\underline{A}\cup\underline{A}\cup\underline{A}$ (20 cases)**

- $\underline{3}\cup\underline{3}\cup\underline{3}$: $(1,2,3)(4,5,6)(7,8,9) = (1,3,2)(4,5,6)\circ(1,3,2)(7,8,9)$.
- $\underline{3}\cup\underline{3}\cup\underline{5}$: $(1,2,3)(4,5,6)(7,8,9,10,11) = (1,2,3)(7,8,9)\circ(4,5,6)(9,10,11)$.
- $\underline{3}\cup\underline{3}\cup(\underline{2\cup 2})$: $(1,2,3)(4,5,6)(7,8)(9,10)$
$= (1,2)(4,5)(7,10)(8,9)\circ(2,3)(5,6)(7,9)(8,10)$.
- $\underline{3}\cup\underline{3}\cup(\underline{2\cup 4})$: $(1,2,3)(4,5,6)(7,8)(9,10,11,12)$
$= (1,2)(4,5)(7,8)(9,11)\circ(2,3)(5,6)(9,10)(11,12)$.
- $\underline{3}\cup\underline{5}\cup\underline{5}$: $(1,2,3)(4,5,6,7,8)(9,10,11,12,13)$
$= (4,5,6,8,7)(9,10,11,12,13)\circ(1,2,3)(6,8,7)$.
- $\underline{3}\cup\underline{5}\cup(\underline{2\cup 2})$: $(1,2,3)(4,5,6,7,8)(9,10)(11,12)$
$= (1,2)(4,5)(6,8)(9,10)\circ(2,3)(5,8)(6,7)(11,12)$.
- $\underline{3}\cup\underline{5}\cup(\underline{2\cup 4})$: $(1,2,3)(4,5,6,7,8)(9,10)(11,12,13,14)$
$= (1,5,4)(11,12,13)\circ(1,2,3,4)(5,6,7,8)(9,10)(13,14)$.
- $\underline{3}\cup(\underline{2\cup 2})\cup(\underline{2\cup 2})$: $(1,2,3)(4,5)(6,7)(8,9)(10,11)$
$= (1,2)(4,5)(8,10)(9,11)\circ(2,3)(6,7)(8,11)(9,10)$.
- $\underline{3}\cup(\underline{2\cup 2})\cup(\underline{2\cup 4})$: $(1,2,3)(4,5)(6,7)(8,9)(10,11,12,13)$
$= (1,2)(4,5)(8,9)(10,12)\circ(2,3)(6,7)(10,11)(12,13)$.
- $\underline{3}\cup(\underline{2\cup 4})\cup(\underline{2\cup 4})$: $(1,2,3)(4,5)(6,7,8,9)(10,11)(12,13,14,15)$
$= (1,2,3)(4,10)(5,11)(6,7)(8,9)(12,13,14)\circ(4,11)(5,10)(7,9)(14,15)$.
- $\underline{5}\cup\underline{5}\cup\underline{5}$: $(1,2,3,4,5)(6,7,8,9,10)(11,12,13,14,15)$
$= (1,4,2,5,3)(6,7,8,9,10)\circ(1,4,2,5,3)(11,12,13,14,15)$.
- $\underline{5}\cup\underline{5}\cup(\underline{2\cup 2})$: $(1,2,3,4,5)(6,7,8,9,10)(11,12)(13,14)$
$= (1,2,3,4)(6,7,8,9)(11,13)(12,14)\circ(4,5)(9,10)(11,14)(12,13)$.
- $\underline{5}\cup\underline{5}\cup(\underline{2\cup 4})$: $(1,2,3,4,5)(6,7,8,9,10)(11,12)(13,14,15,16)$
$= (1,2,3,4)(6,7,8,9)(11,12)(13,15)\circ(4,5)(9,10)(13,14)(15,16)$.
- $\underline{5}\cup(\underline{2\cup 2})\cup(\underline{2\cup 2})$: $(1,2,3,4,5)(6,7)(8,9)(10,11)(12,13)$
$= (1,2)(3,5)(6,7)(10,11)\circ(2,5)(3,4)(8,9)(12,13)$.
- $\underline{5}\cup(\underline{2\cup 2})\cup(\underline{2\cup 4})$: $(1,2,3,4,5)(6,7)(8,9)(10,11)(12,13,14,15)$
$= (1,3,5)(11,12,15)\circ(1,2)(3,4)(6,7)(8,9)(10,15,11)(12,13,14)$.
- $\underline{5}\cup(\underline{2\cup 4})\cup(\underline{2\cup 4})$: $(1,2,3,4,5)(6,7)(8,9,10,11)(12,13)(14,15,16,17)$
$= (1,2)(3,5)(8,9,10,11)(14,15,16,17)\circ(2,5)(3,4)(6,7)(12,13)$.

- $(\underline{2 \cup 2}) \cup (\underline{2 \cup 2}) \cup (\underline{2 \cup 2})$: $(1,2)(3,4)(5,6)(7,8)(9,10)(11,12)$
  $= (1,3)(2,4)(5,6)(7,8) \circ (1,4)(2,3)(9,10)(11,12)$.
- $(\underline{2 \cup 2}) \cup (\underline{2 \cup 2}) \cup (\underline{2 \cup 4})$: $(1,2)(3,4)(5,6)(7,8)(9,10)(11,12,13,14)$
  $= (1,2)(3,4)(5,6)(11,13) \circ (7,8)(9,10)(11,12)(13,14)$.
- $(\underline{2 \cup 2}) \cup (\underline{2 \cup 4}) \cup (\underline{2 \cup 4})$: $(1,2)(3,4)(5,6)(7,8,9,10)(11,12)(13,14,15,16)$
  $= (1,3)(2,4)(5,6)(7,8)(9,10)(11,12)(13,14)(15,16)$
  $\circ\ (1,4)(2,3)(8,10)(14,16)$.
- $(\underline{2 \cup 4}) \cup (\underline{2 \cup 4}) \cup (\underline{2 \cup 4})$: $(1,2)(3,4,5,6)(7,8)(9,10,11,12)(13,14)(15,16,17,18)$
  $= (3,4,5,6)(9,10,11,12)(15,16)(17,18)$
  $\circ\ (1,2)(7,8)(13,14)(16,18)$.

□

*Proof of Lemma 6.4.* Proposition 7.1 implies that every even permutation on a set of 7 or more elements can be written as a product of two evenly balanced permutations; moreover, on a set of 6 elements, the only exception is the special atom $\underline{2 \cup 4}$. This is exactly the content of Lemma 6.4. □

# 8 Conclusion and further work

We have shown that every even permutation of $2 \times A \times 2$ has alternation depth 9 and even alternation depth 13. The bounds of 9 and 13 are probably not tight. The constructions of Sections 3 and 4 have many degrees of freedom, making it plausible that a tighter bound on alternation depth can be found. The best lower bound for alternation depth known to the author is 5. An exhaustive search shows that for $A = \{a, b, c\}$, a 3-cycle with support $\{0\} \times A \times \{0\}$ cannot be written with alternation depth 4. Of course, this particular permutation can be realized with alternation depth 5 by Proposition 3.12 (and in fact, its even alternation depth is also 5).

It is reasonable to conjecture that there is nothing special about the number 2 in Theorems 2.1 and 6.1. Specifically, if $N$ and $M$ are finite sets, one may conjecture that there exists a finite bound on the alternation depth of all permutations $\sigma \in S(N \times A \times M)$ (or all even permutations, when $N$ and $M$ are even), for large enough $A$, independently of the size of $A$.

# 9 Acknowledgments

This work was supported by the Natural Sciences and Engineering Research Council of Canada (NSERC) and by the Air Force Office of Scientific Research, Air Force Material Command, USAF under Award No. FA9550-15-1-0331. This work was done in part while the author was visiting the Simons Institute for the Theory of Computing.

# References

[1] A. De Vos, B. Raa, and L. Storme. Generating the group of reversible logic gates. *Journal of Physics A*, 35(33):7063, 2002.

[2] J. Musset. Générateurs et relations pour les circuits booléens réversibles. Technical Report 97-32, Institut de Mathématiques de Luminy, 1997. Available from `http://iml.univ-mrs.fr/editions/`.

[3] M. Saeedi and I. L. Markov. Synthesis and optimization of reversible circuits — a survey. *ACM Computing Surveys*, 45(2):34 pages, 2013. Also available from `arXiv:1110.2574`.

[4] P. Selinger. Permutation game. Software implemenation, available from `http://www.mathstat.dal.ca/~selinger/pgame/`, 2016.

[5] T. Toffoli. Reversible computing. In *Proceedings of the 7th Colloquium on Automata, Languages and Programming*, pages 632–644. Springer, 1980. Abridged version of Technical Memo MIT/LCS/TM-151, MIT Lab. for Comput. Sci., 1980.