

# Research Report

Tayden White

May 26, 2025

We started with an introduction to the project: An algorithm for fusion of permutation defects. My specific focus will be to determine the runtime of this algorithm, as well as implement it programmatically in the language GAP. Defects are particle-like, point-like objects that are hosted in a  $(2 + 1)$ -D topological phase of matter. Their notation is as follows:  $X_a^\sigma$ , where the subscript is a multilayer anyon, think of  $n$  spatially separate patches of 2-dimensional space. Each of these hosting a monolayer anyon, all of these monolayer anyons are represented with the vector in the subscript. The superscript is a permutation, an element of the symmetric group of  $n$  letters.

A permutation is a bijection from a set  $\Omega$ ,  $\Omega = \{1, 2, 3 \dots n\}$  onto itself. It can be represented like a function  $f$ , for it to be a bijection it needs to be both injective (one-to-one), and surjective (onto). Being injective means that there is no two distinct elements in the source set that get mapped to the same one element in the target set:  $f(x) = f(y) \rightarrow x = y$ . Being surjective means that for all elements in the target set, there exists an element in the source set that maps to it:  $\forall y \in \Omega, \exists x \in \Omega$  s.t.  $f(x) = y$ .

There are three notations for representing permutations, the most important of which is cycle notation, which denotes the cycles in the permutation and is the most compact way of storing the permutation. In an  $\Omega$  of size 5, given the mapping  $\{1 \rightarrow 5, 2 \rightarrow 3, 3 \rightarrow 4, 4 \rightarrow 2, 5 \rightarrow 1\}$ , the cycle decomposition would be  $(15)(234)$ . Permutations can also be multiplied, this entails applying the permutations sequentially from right to left, and seeing what the final mapping is from the initial state of  $\Omega$  to its final state.

After the introduction to the project we turned towards group theory, and how the permutations described on the set  $\Omega$  represent transformations in a symmetry group. A group is defined by a set  $G$  and a binary operation  $\bullet : G \times G \rightarrow G$  s.t  $(g, h) \rightarrow g \bullet h$ .

The following axioms must hold:

1. There exists an element  $e$ , or  $id \in G$  that represents the identity element of the group.  
 $e \cdot g = g = g \cdot e \quad \forall g \in G$ .
2. There exists an inverse for all elements in  $G$ :  $\forall g \in E \exists h \in G$  s.t.  $g \cdot h = e$ . It can be an inverse on both sides.
3. The binary operation is associative:  $(g \cdot h) \cdot k = g \cdot (h \cdot k)$

Groups can be infinite or finite, depending on if the set contains an infinite amount of elements. An example of an infinite group is the set of all integers and the operator  $+$ . An example of a finite group is the set of hours on the clock (modulus) and the operator  $+$ . A group  $(G, \bullet)$  is called abelian if  $g \cdot h = h \cdot g$ , i.e. the operation is commutative with the given elements.

An extension of groups are rings. A ring, denoted by  $(R, +, \bullet)$ , is a set together with **two** binary operators, one called addition  $(+ : R \times R = R)$  the other multiplication  $(\bullet : R \times R = R)$ .

The following axioms must hold:

1.  $(R, +)$  is an abelian group. This means that it follows the axioms of a group: having inverses, an identity element, and being associative. Additionally, the operation is commutative.
2. The  $\bullet$  operation is associative:  $(r \cdot s) \cdot t = r \cdot (s \cdot t) \forall r, s, t \in R$ .
3. The distributive property works between the addition and multiplication, this would look like this:  $r \cdot (s + t) = r \cdot s + r \cdot t$  and  $(r + s) \cdot t = r \cdot t + s \cdot t \forall r, s, t \in R$ .

There are also a few optional properties that can be used to describe special kinds of rings.

1. A ring has an identity if  $\exists 1 \in R$  s.t.  $1 \cdot r = r \cdot 1 \forall r \in R$
2. A ring is commutative (not called abelian for rings) if the multiplicative operator is commutative:  $r \cdot s = s \cdot r \forall r, s \in R$ .
3. A ring with an identity element has multiplicative inverses if  $\forall r \in R \exists s \in R$  s.t.  $r \cdot s = s \cdot r = 1$ . This is called a division ring. Furthermore, a commutative division ring is called a field.

Lastly, we combined the idea of permutations in a symmetry group with the representation of defects and their fusion. By ignoring the multilayer anyon (making the defects we are working with be called bare defects, with the subscript anyone being called the "vacuum anyon" or  $\vec{1}$ ), we can represent the fusion of defects by just multiplying the permutations defined in the two defect superscripts.

For example:  $X^{(12)} \cdot X^{(23)} = X^{(123)}$  and  $X^{(12)} \cdot X^{(34)} = X^{(12)(34)}$

A crucial part of the algorithm for the fusion of defects is the fact that a transposition (a permutation that only switches two elements) is the inverse of itself. This means that two defects can be simplified by the factoring out of similar transpositions from their respective permutations, then having them "annihilate" each other.

Example:  $X^{(123)} \cdot X^{(234)} \rightarrow X^{(12)} \cdot X^{(23)} \cdot X^{(23)} \cdot X^{(34)} \rightarrow X^{(12)} \cdot [] \cdot X^{34}$

The amount of times this simplification can occur in the algorithm is bounded by the overlap between the sets describing the permutation for each defect. As long as there are two elements that exist in both permutations, they can be factored out (using the inverse property of groups) and placed at the inner part of the multiplication, causing them to annihilate each other.