Symmetry of a Pastry: An Investigation into the Braid Group

Ethan Partida, McNair Scholar & Prof. Vic Reiner, School of Mathematics
University of Minnesota Twin-Cities

Braids

We define a braid as the set of strings which connect one set of objects to a duplicate set of those objects. We are allowed to bend and stretch the strings, but not uncross them or change what objects they are connected to. Figure 1 gives an example of a braid in this group and an action we can take on the braid without changing it.

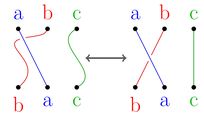

Fig. 1: An example of a braid, we can bend this braid without changing it

The braid group is the mathematical formalization of physical braids. This formalization allows us to create and apply general rules to even the most complicated of braids. The braid group appears in a variety of places, such as knot theory, particle physics, cryptography, or even molecular biology. Some interesting properties and general rules of the braid group are:

- We can compose braids by adding one directly after the other. This allows for us to have a sense of "multiplying" braids.
- Let σ_i be the braid which crosses the ith string underneath the string to its right, see Figure 2. One can observe that each braid consists of a sequence of adjacent crossings. This allows for us to write any braid as a product of σ_i's, Figure 3 illustrates this process.

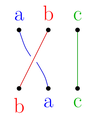

Fig. 2: σ_1 acting on a braid of three strings

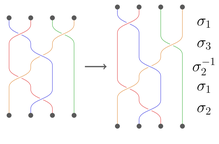

Fig. 3: The process of writing any braid as a product of σ_is

- It's clear that σ_i has an inverse, just pass the ith string over the top of the string to its right. Figure 4 visually describes this. Thus, since every braid is a product of σ_is, every braid has an inverse.

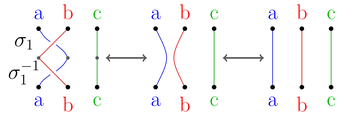

Fig. 4: Since one string simply passes underneath the other, we can undue the crossings

Knot Theory

Knot Theory is quite simply, the mathematical study of knots. One can think of a knot as a string with its ends connected to each other. For an example, see Figure 5. Much like braids, we are able to bend and stretch this string as long as we don't break any physical laws.

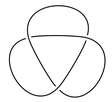

Fig. 5: An example of a knot, the trefoil!

A central goal of knot theory is to characterize every possible knot. Obviously, there are infinitely many different knots so we will try to start with *uncomplicated* knots.
Before we can do this, we must first determine what it means to be *uncomplicated*. One way of classifying knots is to count how many crossings they have. Figure 5 has three crossings. We will determine a knots complexity by this number.
It turns out there is a unique amount of knots for each specific number of crossings. In Figure 6, we classify the first few of these into a knot table.

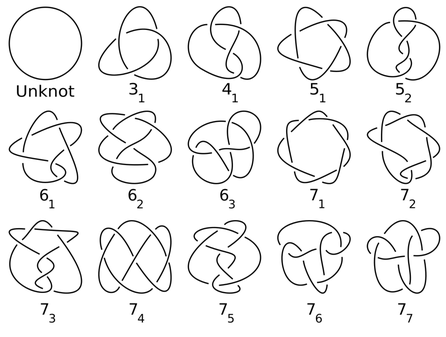

Fig. 6: A knot table classifying all knots with 0-7 crossings

An interesting theorem states that every knot is just a closed up braid. This "closed up" braid is formed by taking the ends of the braid and connecting to them each other just like Figure 7.

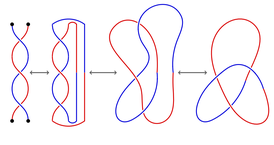

Fig. 7: The process of converting a braid into a knot

This theorem allows us to increase the ways in which we can understand knots. If something is true for braids, then an analog of it is true for knots!

Cryptography

Cryptography is the science of encrypting information. Much like the secret codes created in elementary school, cryptologists seek to create codes where the sender and receiver understand their messages while they appear like gibberish to an outsider.
To do this, they create a key which gives the solution to an incredibly difficult math problem. They then use this to encode the information so that it only makes sense if one has the solution to this problem. Figure 8 illustrates this procedure. Since both the sender and receiver have the solution, the message makes perfect sense to them. But because this solution is incredibly hard to find naturally, no outsider can make sense of the message.

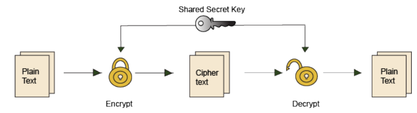

Fig. 8: An overview of a typical cryptology

Many of the typical cryptologies use math problems are based on factoring integers into their prime factors. An example of this would be:

$$28 = 2 \cdot 14 = 2 \cdot 2 \cdot 7.$$

When the numbers are much larger than 28, this is a very difficult thing to do. In fact it would take a traditional super computer more time than the universe has existed to break a code with these encryptions.
Quantum computing's impending arrival poses a big threat to the difficulty of these problems. Because of their *quantumness*, quantum computers will be able to solve the factorization problem with relative ease. This means that almost all of our secure data will no longer be secure. Braid groups might be an answer to this problem.
The key quality which makes factorization easily solvable by quantum computers is the fact they are commutative, order of addition does not matter i.e. $2 + 3 = 6 = 3 + 2$. Luckily braid groups are not commutative, since

$$\sigma_1\sigma_2 \neq \sigma_2\sigma_1$$

. Thus basing a cryptology on a hard to solve problem in the braid group might make a quantom-proof encryption!

Acknowledgments

Figure 6: https://en.wikipedia.org/wiki/File:Knot_table.svg
Figure 8: https://www.icao.int/Security/FAL/PKD/BVRT/Pages/Basics.aspx
Cryptography: https://arxiv.org/pdf/1910.04346.pdf

School of Mathematics · University of Minnesota Driven to Discover · TRIO Ronald E. McNair Post-Baccalaureate Achievement Program