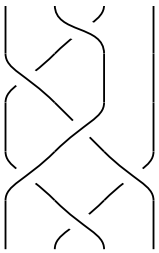
An Introduction to the Mathematics of Braids

SecureRF Corporation
100 Beard Sawmill Road
Suite 350
Shelton, CT 06484

203-227-3151
info@SecureRF.com
www.SecureRF.com

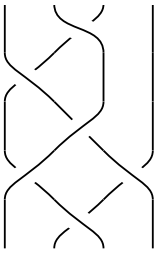
What are braids?

The study of braids, as abstract mathematical objects, dates back to the 1920's with the groundbreaking work of the Austrian mathematician Emil Artin. He considered geometric configurations of strands of the following form.



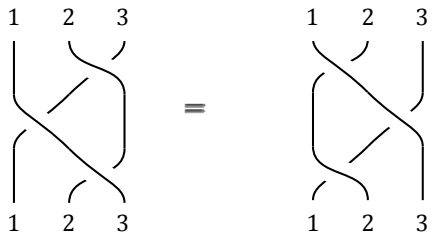
In the single crossing configuration below, the strand starting at the point labeled 1 is said to cross *over* the strand starting at the point labeled 2 and the strand starting at the point 2 crosses *under* the strand starting at the point 1.

A braid, for example,

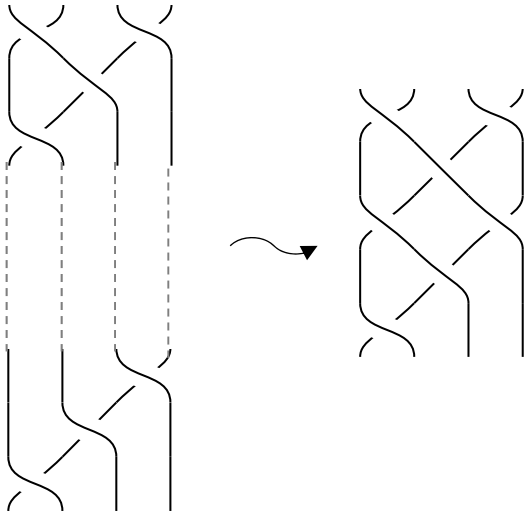


consists of a collection of crossed strands whose points of origin and whose endpoints are fixed and unmoving. The strands themselves can be maneuvered (by, for example, stretching, pulling and pushing, but never cutting) which allows one braids to be morphed into another.

The three stranded braids below are equal because the braid on the left can be transformed into the one on the right in the following manner: push the strand starting at the point 2 to the left (and over the strand starting at 3) and under the strand starting at 1.

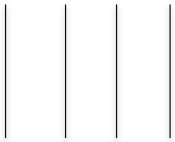


Two braids can be vertically attached to each other to produce a third braid. This process, depicted below in a four stranded example, is key to analyzing braids abstractly because this concatenation can be viewed as an analogue to the multiplication of numbers.

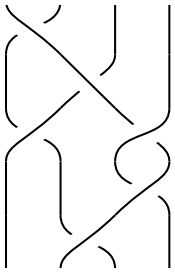


Working with braids.

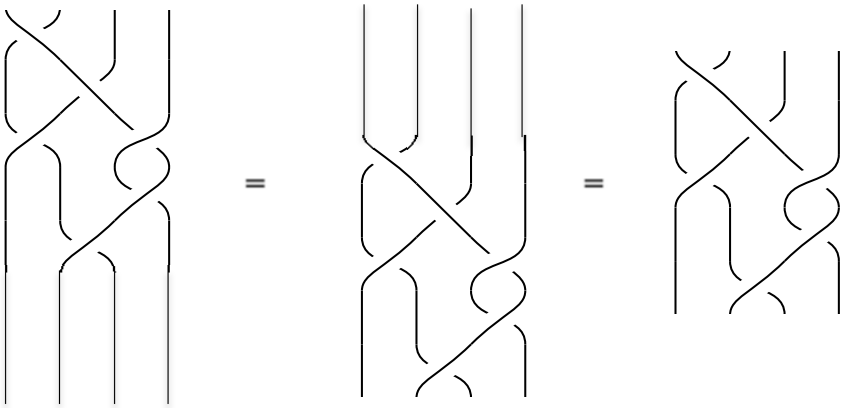
The above vertical concatenation process, which is called braid multiplication, behaves in many familiar ways. The number 1 has the property that, given any other number x, we always have the equality $1 \cdot x = x \cdot 1$. In the world of braids the analogue of the number 1 is call the trivial braid: in the case of four strands, the trivial braid is four parallel uncrossed strands.



To see why the trivial braid functions like the number 1, we multiply say

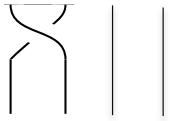
$\beta =$ 

by the trivial braid:



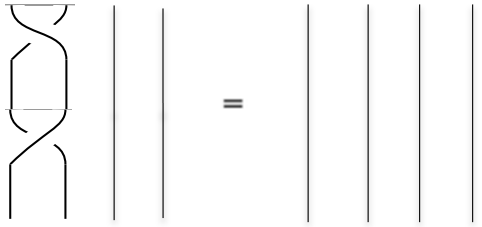
Another parallel between numbers and braids is the concept of the inverse. For any number x, $x \neq 0$, the number $\frac{1}{x}$ is it's multiplicative inverse: $x \cdot \frac{1}{x} = \frac{1}{x} \cdot x = 1$. In braids the process of finding an inverse works in the following way.

Consider the braid with one crossing,

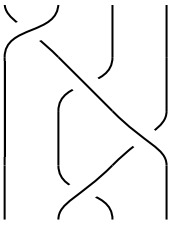


and the braid with the opposite crossing,

When these two braids are multiplied

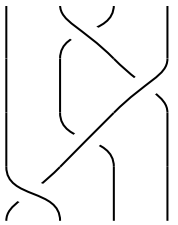


the trivial braid emerges: pull the first strand directly to the left and the second strand directly to the right. Given a more complex braid, say

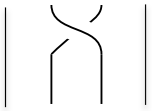
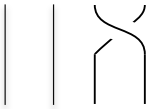
$\beta =$ 

the inverse is obtained by finding the inverse of the final crossing and multiplying it by the inverse of the previous crossing and continuing in this way until the inverse of the first crossing is reached.

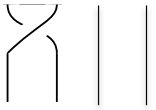
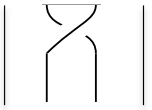
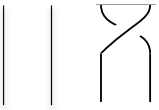
In the case of β above, the inverse is given by the braid β^{-1} below.

$\beta^{-1} =$ 

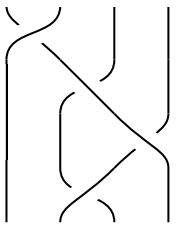
Every braid β on N strands can be viewed as a product of a sequence of braids with a single crossing (where one strand crosses over its neighbor to the right) and their inverses. For example, when $N = 4$ we have

$b_1 =$  $b_2 =$  $b_3 =$ 

whose inverses are given as follows.

$b_1^{-1} =$  $b_2^{-1} =$  $b_3^{-1} =$ 

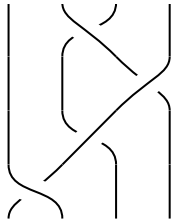
Then the braid β

$\beta =$ 

is the product

$$\beta = b_1^{-1}\, b_2\, b_3\, b_2^{-1},$$

The inverse of β, β^{-1} is given by

$\beta^{-1} =$ 

and is the product

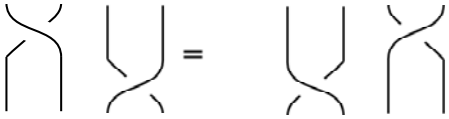
$$\beta^{-1} = b_2\, b_3^{-1} b_2^{-1} b_1.$$

The braid group B_N is defined to be the collection of all the braids on N strands, and the single crossing braids $\{b_1, b_2, \dots\}$ are called the Artin generators. Viewing braids as products of generators is a powerful analytic approach to understanding braids. The identity

when expressed as an equality of products of generators, becomes

$$b_2\, b_1\, b_2 = b_1\, b_2\, b_1.$$

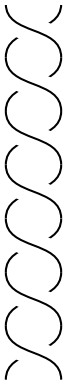
Another identity that emerges when the number of strands is at least 4: since the crossings can be pushed both up and down the 4 strand braids below are equal.



This equality is expressed in generator form as

$$b_1\, b_3 = b_3\, b_1.$$

The braid group is an infinite set. To see this look at the product of a single generator, say b_1, repeated with itself over and over: every time an extra twist is added a new braid is created. Since this process doesn't stop, there is an infinite collection of braids.

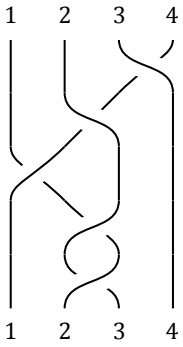


Connections to Permutations.

A permutation of a set of points, say {1,2,3, … } is the technical term for a shuffle of the points. Focusing on the set {1,2,3,4} an example of a permutation, σ, is

$$1 \to 2, \quad 2 \to 3, \quad 3 \to 4, \quad 4 \to 1.$$

The connection between braids is both intuitive and important. Consider the braid β whose points of origin and whose endpoints are labeled {1,2,3,4}.



The strand starting at the point 1 travels through the braid β at ends at the point 2. Following the strand starting at 2, we land a 3, following 3 we land at 4, and finally 4 travels back to 1. Standing back for a moment, we see that β has actually

produced a permutation of the set {1,2,3,4}: in fact it produces is precisely the permutation σ that we started with.
Two permutations can be multiplied (by applying the first and then the second, resulting in a third permutation), and when braids are turned into permutations (as above) the multiplication of braids becomes multiplication of permutations.

This connection between the braid group, which is infinite, and the collections of permutations, which is finite, facilitates the development of cryptographic applications of the braid group. The Algebraic Eraser™ is a function which facilitates a range of cryptographic applications, including a Public Key Agreement protocol, and is in part braid based. For an introduction to this the reader is referred to the SecureRF white paper, *Colored Burau Matrices, E-multiplication, and Algebraic Eraser™ Key Agreement Protocol*.

About SecureRF

SecureRF Corporation – Securing the Internet of Things® – provides security solutions for embedded systems and wireless sensor technologies used in non traditional payment systems, secure supply chain management, cold chain management, and anti counterfeiting applications in the pharmaceutical, fashion, spirits, defense, and homeland security sectors. The company's technology is based on a breakthrough in public key cryptography that is computationally efficient, yet highly secure and available as a software development kit, Verilog/VHDL, or as a core for FPGAs and ASICs. SecureRF also offers the LIME Tag™ - a range of highly secure NFC, UHF and Bluetooth LE sensor tags along with its anticounterfeiting solution – Veridify™.

For more information on anti-counterfeiting, cybersecurity or securing the Internet of Things, please contact us at info@SecureRF.com. More information about SecureRF can be found on its Web site at http://www.SecureRF.com. SecureRF's insights on security can be found on its blog at http://www.SecureRF.com/blog. Follow us on Twitter: https://twitter.com/SecureRF.