Braid Group Cryptography - Liam Hardiman

Background

A **finitely presented group** is specified by the following data.

1. **Generators** $x_1, x_2, \ldots, x_n$. Just a set of symbols.
2. **Relators** $r_1 = e$, $r_2 = e$, $\ldots$, $r_m = e$. More on these in a moment.

For each generator x_i there is a corresponding inverse, x_i^{-1}. A **word** is just a finite string made of the symbols x_i and x_i^{-1}. The empty string e is a word and will be the identity element in G. The relators are words.

G consists of all *equivalence classes* of words, where two words u and v are equivalent if u can be transformed into v by a finite sequence of cancellations or eliminating/introducing relators.

Equivalently, G is a quotient of the free group on the generators modulo the normal closure of the relators.

The Word Problem

The **word problem** is the decision problem that asks whether two words u and v are equivalent in G. In some finitely presented groups this is straight up **undecidable** – it is provably impossible to give an algorithm that always outputs a correct answer.

The Conjugacy Problem

The **conjugacy problem** is the decision problem that asks whether two words u and v are **conjugate** in G. In other words, it asks whether there exists a word w such that $u = wvw^{-1}$.