The Word Problem in Group Theory

CSC 707-001: Final Project

William J. Cook
wjcook@math.ncsu.edu

Wednesday, April 28, 2004

1 Introduction and History

It would be hard to describe all of the areas in which group theory plays a major role. Group Theory has important applications to most areas of mathematics and science. In Algebra almost every object is built on top of a group of some kind. For instance, vector spaces are built on top of Abelian (commutative) groups. Many important questions in Topology can be reduced to questions about a group (i.e. fundamental groups and homology groups). The group of integers modulo n (defined later) is fundamentally important to the study of Number Theory. Cryptography elegantly displays the interplay between Number Theory and Algebra. Felix Klein initiated the study of Geometry through groups of symmetries. Much of modern Physics is built around the study of certain groups of symmetries. In Chemistry, symmetries of molecules are often used to study chemical properties.

Seeing that Group Theory touches so much of modern science and mathematics, it is obviously important to know what can and cannot be computed in relation to groups. One of the most basic questions we can ask is, "Do two given representations of elements of a group represent the same element?" Or in other words, "Given a group G and $a, b \in G$, is it true that $a = b$?" In the following section I will state this problem (first posed by Max Dehn in 1910) formally in terms of finitely presented groups. A related question asking, "Can we always decide if two finitely presented groups are isomorphic?" was posed by H. Tietze two years earlier in 1908 [S].

The word problem for semigroups was shown to be unsolvable by E. Post and independently by A.A. Markov in 1947. However, the word problem for groups remained open until 1955 when Pyotr S. Novikov showed that groups also have an unsolvable word problem. In 1957 William W. Boone and in 1958 J.L. Britton both independently proved the same. Although Novikov was first to conquer this problem, the argument I will present shortly is adapted from a proof by Britton. The group with an unsolvable word problem presented in the following is essentially Boone's group. The related isomorphism problem for groups was solved shortly after these developments by Adian in 1957 and independently by Rabin in 1958. In fact, Adian and Rabin proved that many group properties could not be decided in general.

2 Some Definitions

Let us start by reviewing some basic definitions.

Definition 2.1. *Let S be a (non-empty) set. A **binary operation** on S is a mapping from $S \times S$ into S. We write $(a, b) \mapsto ab$ for each $(a, b) \in S \times S$.*

Definition 2.2. *We say that a binary operation on S is **associative** if for each $a, b, c \in S$ we have: $(ab)c = a(bc)$. A set S with an associative binary operation is called a **semigroup**.*

Definition 2.3. *Let M be a semigroup. Suppose that there is some element $1 \in M$ such that for each $a \in M$ we have $1a = a1 = a$. Then 1 is called the **identity**, and M is a **monoid**.*

Note that the identity is unique. Because if a monoid M has two identities 1 and $1'$ then $1 = 11'$ because $1'$ is an identity and $1' = 11'$ because 1 is an identity. Thus $1 = 1'$ so identities are unique.

Example 2.4. *Let Σ be a set, and Σ^* the set of all words over Σ. Give Σ^* the operation of concatenation. Then Σ^* is a monoid and the empty word ε is an identity. Σ^* is called the **free monoid** or sometimes the **free semigroup** generated by Σ.*

Proof: Let $a = \sigma_1 ... \sigma_k, b = \tau_1 ... \tau_l, c = \gamma_1 ... \gamma_m$ be words in Σ^*. Then we get that $(ab)c = (\sigma_1 ... \sigma_k \tau_1 ... \tau_l)\gamma_1 ... \gamma_m = \sigma_1 ... \sigma_k \tau_1 ... \tau_l \gamma_1 ... \gamma_m = \sigma_1 ... \sigma_k(\tau_1 ... \tau_l \gamma_1 ... \gamma_m) = a(bc)$ hence concatenation is associative. Also notice that $\varepsilon a = \varepsilon\sigma_1 ... \sigma_k = \sigma_1 ... \sigma_k = a = \sigma_1 ... \sigma_k \varepsilon = a\varepsilon$ so that ε is an identity. ■

Definition 2.5. *Let G be a monoid with identity 1. Suppose that for each $a \in G$ there is some $b \in G$ such that $ab = ba = 1$. Then b is an **inverse** for a and G is a **group**.*

Also note that inverses are unique. Suppose that a has two inverses b and c. Then $b = b1 = b(ac) = (ba)c = 1c = c$ thus $b = c$ so inverses are unique. If multiplicative notation is used we denote the inverse of a by a^{-1}. If additive notation is used we denote the inverse of a by $-a$.

Example 2.6. *Consider a regular n-gon (where $n \geq 3$) in the real plane $\mathbb{R}^2$. Any map which leaves the n-gon unchanged is called a symmetry of the n-gon. The group of symmetries of a regular n-gon is called the Dihedral group D_n (the group operation is function composition). When $n = 3$, D_3 is the group of symmetries of an equilateral triangle. When $n = 4$, D_4 gives the group of symmetries of a square. $D_3 = \{\mathrm{R}_0, \mathrm{R}_{120}, \mathrm{R}_{240}, \mathrm{V}, \mathrm{D}, \mathrm{D}'\}$ where R_θ is a counterclockwise rotation of θ degrees and $\mathrm{V}, \mathrm{D}, \mathrm{D}'$ are reflections as shown below.*

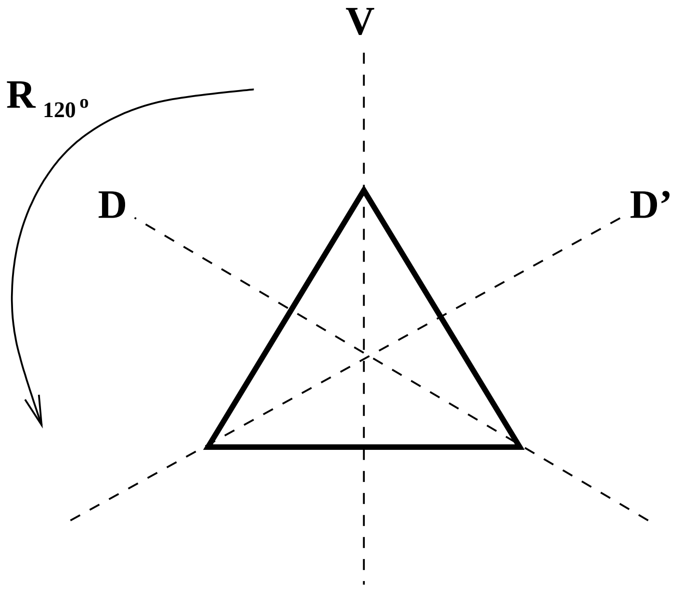

Figure: Symmetries of an equilateral triangle.

D_3	R_0	R_{120}	R_{240}	V	D	D'
R_0	R_0	R_{120}	R_{240}	V	D	D'
R_0	R_0	R_{120}	R_{240}	V	D	D'
R_{120}	R_{120}	R_{240}	R_0	D	D'	V
R_{240}	R_{240}	R_0	R_{120}	D'	V	D
V	V	D'	D	R_0	R_{240}	R_{120}
D	D	V	D'	R_{120}	R_0	R_{240}
D'	D'	D	V	R_{240}	R_{120}	R_0

Figure: The Dihedral group, D_3, and its Cayley (multiplication) table.

As an example let's multiply DVD together. Looking at the table, $VD = R_{240}$ thus $DVD = DR_{240}$ which again looking at the table is D'. Thus $DVD = D'$. Notice that $VD^2 = V$ $(\neq D')$.

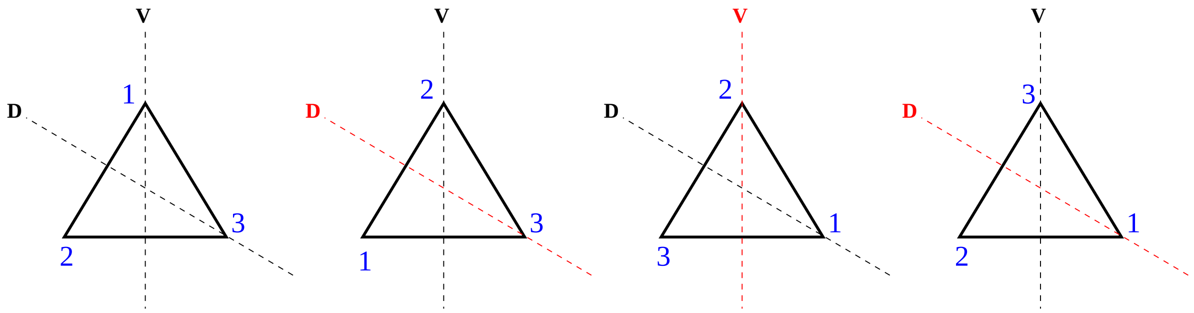

Figure: Calculating $DVD = D'$.

Definition 2.7. *G is an* **Abelian** *(or commutative) group if for each $a, b \in G$ we have $ab = ba$.*

Notice that D_3 is not Abelian. An Abelian group's Cayley table must be symmetric across the main diagonal. Looking at D_3's Cayley table, we see that: $\mathrm{R}_{120}V = D$ but $V\mathrm{R}_{120} = D'$. In fact all of the Dihedral groups are non-Abelian.

Definition 2.8. *Let G_1 and G_2 be groups. Let $f : G_1 \to G_2$ be a bijective map. If f is* **operation preserving** *which means $\forall a, b \in G_1$ $f(ab) = f(a)f(b)$ (ab of the LHS is given by the operation in G_1 and $f(a)f(b)$ on the RHS is given by the operation in G_2), then f is called an* **isomorphism**. *If there exists an isomorphism between two groups, we say that those groups are* **isomorphic**.

If two groups are isomorphic, then it is not too hard to show given a group property, either both groups have it or both groups lack it.

Definition 2.9. *Let "$\equiv$" be an equivalence relation on a semigroup S. If for every $a, b, a', b' \in S$ such that $a \equiv a'$ and $b \equiv b'$ we have $ab \equiv a'b'$, then $\equiv$ is called a* ***congruence*** *on S. Denote the equivalence class of a by $[a]$, and the set of equivalence classes by $S/\equiv$.*

Proposition 2.10. *Let $\equiv$ be a congruence on a semigroup S. The set of equivalence classes $S/\equiv$ with the induced operation $[a][b] = [ab]$ is a semigroup. Moreover, if S is a monoid with identity 1, then $S/\equiv$ is a monoid with identity $[1]$. Finally, if S is a group, then $S/\equiv$ is a group too.*

Proof: Given $a, b, a', b' \in S$, where $[a] = [a']$ and $[b] = [b']$ then $[ab] = [a'b']$ (because $\equiv$ is a congruence). Therefore, the induced operation is well-defined. Suppose that $a, b, c \in S$ then $([a][b])[c] = [ab][c] = [(ab)c] = [a(bc)] = [a][bc] = [a]([b][c])$. Therefore the induced operation is associative so that $S/\equiv$ is a semigroup.

Suppose that S is also monoid. Then $[a][1] = [a1] = [a] = [1a] = [1][a]$ for all $a \in S$. Hence $S/\equiv$ is a monoid with identity $[1]$.

Suppose that S is a group. Let $a \in S$ there exists $b \in S$ such that $ab = ba = 1$. Therefore, $[a][b] = [ab] = [1]$ and $[b][a] = [ba] = [1]$. Hence $S/\equiv$ has inverses for each element. Thus $S/\equiv$ is a group. ■

Lemma 2.11. *Let S be a semigroup and $R \subset S \times S$. The intersection of all congruences containing R is a congruence. We call this the congruence* ***generated*** *by R.*

Proof: It is well known that the arbitrary intersection of equivalence relations is still an equivalence relation. Let $\equiv$ be the equivalence relation obtained by intersecting all congruences which contain R. Suppose that $a, b, a', b' \in S$ are elements such that $[a] = [a']$ and $[b] = [b']$. This means that a is equivalent to a' and b is equivalent to b' in each of the congruences containing R, hence ab is equivalent to $a'b'$ in each of the congruences containing R (because they are congruences). Therefore, $[ab] = [a'b']$ and thus $\equiv$ is also a congruence. ■

Lemma 2.12. *Let S be a monoid with identity 1 and $R \subset S \times S$. The congruence generated by R is exactly the set of all $(x, y) \in S \times S$ such that there exists $n \geq 1$ and $x_i, y_i, a_i, b_i \in S$ $1 \leq i \leq n$ where $x = a_1x_1b_1$, $y = a_ny_nb_n$, $a_iy_ib_i = a_{i+1}x_{i+1}b_{i+1}$ for $1 \leq i \leq n-1$, and either $(x_i, y_i) \in R$ or $(y_i, x_i) \in R$ or $x_i = y_i$ for every $1 \leq i \leq n$.*

Proof: Call the set of all such pairs $\hat{R}$. Using $n = 1$, $a_1 = b_1 = 1$, and $(x_1, y_1) \in R$ we get that $(x_1, y_1) \in \hat{R}$. Thus $R \subset \hat{R}$.

Note that for any congruence containing R we need $[axb] = [ayb]$ whenever $(x, y) \in R$ and $a, b \in S$ because if $[x] = [y]$ then $[a][x][b] = [a][y][b]$ thus $[axb] = [ayb]$. Transitivity demands that all finite sequences of such relations must be included. Symmetry requires that we allow for both $(x_i, y_i) \in R$ and $(y_i, x_i) \in R$. To be reflexive we also need to include $x_i = y_i$. Thus the every congruence containing R must include at least the elements of $\hat{R}$. Therefore, $\hat{R}$ is contained in the congruence generated by R.

The relation is reflexive because $(x, x) \in \hat{R}$ for each $x \in S$ (use $n = 1$, $a_1 = b_1 = 1$, $x_1 = y_1 = x$). This relation is also obviously symmetric and transitive (we have rigged it to be so).

Let $c, d \in S$. Suppose that $(x, y) \in \hat{R}$ then there is some $n \geq 1$ and $x_i, y_i, a_i, b_i \in S$ $1 \leq i \leq n$ where $x = a_1x_1b_1$, $y = a_ny_nb_n$, $a_iy_ib_i = a_{i+1}x_{i+1}b_{i+1}$ for $1 \leq i \leq n-1$, and either $(x_i, y_i) \in R$ or $(y_i, x_i) \in R$ or $x_i = y_i$ for every $1 \leq i \leq n$. Use ca_i and b_id instead of a_i and b_i. Then we get that $cxd = ca_1x_1b_1d$, $cyd = ca_ny_nb_nd$, $ca_iy_ib_id = ca_{i+1}x_{i+1}b_{i+1}d$ for $1 \leq i \leq n-1$. Thus we have $(cxd, cyd) \in \hat{R}$. If $[a] = [a']$ and $[b] = [b']$ then we have $(a, a') \in \hat{R}$ thus $(1ab, 1a'b) = (ab, a'b) \in \hat{R}$ and $(b, b') \in \hat{R}$ thus $(a'b1, a'b'1) = (a'b, a'b') \in \hat{R}$. Then using transitivity we have $(ab, a'b), (a'b, a'b') \in \hat{R}$ implies that $(ab, a'b') \in \hat{R}$. Therefore, $[ab] = [a'b']$ thus $\hat{R}$ is a congruence.

Finally, since $\hat{R}$ is in the intersection of all congruences containing R, $R \subset \hat{R}$, and $\hat{R}$ is itself a congruence. We conclude that the intersection of all congruences containing R is equal to $\hat{R}$. ■

Definition 2.13. *Let X be a finite set and $R \subseteq X^* \times X^*$ a finite set of relations where $(u_i, v_i) \in R$ means $[u_i] = [v_i]$. Then the semigroup $\langle X \mid R \rangle_S$ is a **finitely presented** semigroup. Furthermore, $(X \mid R)_S$ is its **finite presentation**. Any semigroup with a finite presentation is a finitely presented semigroup.*

Definition 2.14. *A finitely presented semigroup $\langle X \mid R \rangle_S$ has a **solvable word problem** if for every $w_0 \in X^*$ we have that $\{w \in X^* \mid [w] = [w_0]\}$ is a recursive set.*

Therefore, the finitely presented semigroup $\langle X \mid R \rangle_S$ has a solvable word problem if for each $w_0 \in X^*$ there is a Turing machine $\mathcal{M}$ that decides membership in $\{w \in X^* \mid [w] = [w_0]\}$. That is given $w \in X^*$ as input $\mathcal{M}$ will either accept or reject w depending on whether w is equivalent to w_0.

Definition 2.15. *Let Σ^* be the free monoid generated by Σ. Let $R = \{w_i = u_i \,|\, i \in I\}$ be a family of equations where $w_i, u_i \in \Sigma^*$ for each $i \in I$. Let $\equiv$ be the congruence generated by R. $\langle \Sigma \,|\, w_i = u_i \; i \in I \rangle_S = \Sigma^* / \equiv$ is again a monoid with identity $[\varepsilon]$. We call this the monoid* ***generated*** *by Σ with* ***relations*** *R. $(\Sigma \,|\, w_i = u_i \; i \in I)_S$ is called a* ***presentation*** *of $\Sigma^*/ \equiv$.*

Proposition 2.16. *Let $\Sigma^{-1} = \{\sigma^{-1} \,|\, \sigma \in \Sigma\}$ and $X = \Sigma \cup \Sigma^{-1}$. Also let $R_{grp} = \{\sigma^{-1}\sigma = \varepsilon, \sigma\sigma^{-1} = \varepsilon \,|\, \sigma \in \Sigma\}$ and let $R = \{w_i = \varepsilon \,|\, i \in I\}$, $w_i \in X^*$ for all $i \in I$, be some other relations (possibly empty). Set $R' = R_{grp} \cup R$. Then $\langle \Sigma \,|\, R \rangle = \langle X \,|\, R' \rangle_S$ is a group.*

Proof: By a previous proposition we know that $\langle X \,|\, R' \rangle_S$ is a monoid with identity $[\varepsilon]$. Let $[a] \in \langle X \,|\, R' \rangle$ then $a = \sigma_1 ... \sigma_k \in X^*$. If $\sigma_i = \tau^{-1} \in \Sigma^{-1}$, then let $\sigma_i^{-1} = \tau$ (this just means that $(\tau^{-1})^{-1} = \tau$). Consider, $[a]^{-1} = [\sigma_k^{-1} ... \sigma_1^{-1}]$. $[a][a]^{-1} = [\sigma_1 ... \sigma_k][\sigma_k^{-1} ... \sigma_1^{-1}] = [\sigma_1 ... \sigma_k \sigma_k^{-1} ... \sigma_1^{-1}] = [\sigma_1 ... \sigma_{k-1}][\sigma_k \sigma_k^{-1}][\sigma_{k-1}^{-1} ... \sigma_1^{-1}]$. But σ is of the form τ or τ^{-1} for some $\tau \in \Sigma$. Therefore, $\sigma_k \sigma_k^{-1}$ is either $\tau\tau^{-1}$ or $\tau^{-1}\tau$. But both of these are equivalent to ε (by our relations $R_{grp} \subset R'$), thus $[\sigma_k \sigma_k^{-1}] = [\varepsilon]$. Therefore, $[\sigma_1 ... \sigma_k][\sigma_k^{-1} ... \sigma_1^{-1}] = [\sigma_1 ... \sigma_{k-1}][\varepsilon][\sigma_{k-1}^{-1} ... \sigma_1^{-1}] = [\sigma_1 ... \sigma_{k-1} \sigma_{k-1}^{-1} ... \sigma_1^{-1}]$ using induction we find that $[\sigma_1 ... \sigma_k][\sigma_k^{-1} ... \sigma_1^{-1}] = [\varepsilon]$. So we get that $[a][a]^{-1} = [\varepsilon]$ and likewise $[a]^{-1}[a] = [\varepsilon]$. Therefore, $[a]^{-1}$ is an inverse for $[a]$. Thus, every element of $\langle \Sigma \,|\, R \rangle$ has an inverse. Therefore, $\langle \Sigma \,|\, R \rangle$ is a group. ■

Remark 2.17. *If R is empty, we call $\langle \Sigma \rangle$ the* ***free group*** *generated by Σ. $(\Sigma \,|\, R)$ is called a* ***presentation*** *of the group $\langle \Sigma \,|\, R \rangle$.*

Definition 2.18. *Let X be a finite set and $R \subseteq (X \cup X^{-1})^*$ (identify R with $R \times \{\varepsilon\}$) a finite set of relations where $u_i \in R$ means $[u_i] = [\varepsilon]$. Then the group $\langle X \,|\, R \rangle$ is a* ***finitely presented*** *group. Furthermore, $(X \,|\, R)$ is its* ***finite presentation****. Any group with a finite presentation is a finitely presented group.*

It may seem that we are being overly restrictive on the types of relations allowed in a group. Consider the relation $[u_i] = [v_i]$. In a group, we can use the fact that v_i has an inverse and get an equivalent equation $[v_i^{-1} u_i] = [\varepsilon]$. Thus, even when we force the right hand side of the relations to be the identity, we have no fewer choices for relations.

Example 2.19. *Consider the example of D_3 from before. We can use each element as a generator and each entry of the Cayley table as a relation to get a finite (although hardly compact) presentation of the group. That is $D_3 \cong \langle X \,|\, R \rangle$ where $X = \{\mathrm{R}_0, \mathrm{R}_{120}, \mathrm{R}_{240}, V, D, D'\}$ and $R = \{\mathrm{R}_0\mathrm{R}_0 = \mathrm{R}_0, \mathrm{R}_0\mathrm{R}_{120} = \mathrm{R}_{120}, ..., D'D' = \mathrm{R}_0\}$ (36 relations in all – one for each of the 36 entries in the Cayley table).*

Example 2.20. *A much more compact presentation of the Dihedral groups ($n \geq 3$) is given by $D_n \cong \langle x, y \,|\, x^2 = y^2 = (xy)^n = 1\rangle$. Think of the generators "x" and "y" as two reflections which reflect across lines which meet in the center of the n-gon. We need the relations $x^2 = 1$ and $y^2 = 1$ because reflections are their own inverses. Also, x and y reflect across lines which have a $360/2n$ degree angle between them. So, xy (one reflection followed by the other) will rotate the n-gon about its center (because the lines of reflection meet there). Since the angle between x and y is $360/2n$, xy is a $2 \times 360/2n = 360/n$ degree rotation. Thus the relation: $(xy)^n = 1$.*

Definition 2.21. *A finitely presented group $\langle X \,|\, R\rangle$ has a **solvable word problem** if $\{w \in (X \cup X^{-1})^* \,|\, [w] = [\varepsilon]\}$ is a recursive set.*

Stated in another way, the finitely presented group $\langle X \mid R\rangle$ has a solvable word problem if there is a Turing machine $\mathcal{M}$ that decides membership in $\{w \in (X \cup X^{-1})^* \,|\, [w] = [\varepsilon]\}$. That is given $w \in (X \cup X^{-1})^*$ as input $\mathcal{M}$ will either accept or reject w depending on whether w is equivalent to the identity.

We can view a finitely presented group $\langle X \,|\, R\rangle$ as a finitely presented semigroup $\langle X \cup X^{-1} \,|\, R_{grp} \cup R\rangle_S$. If $\langle X \mid R\rangle$ has a solvable word problem, then so does $\langle X \cup X^{-1} \,|\, R_{grp} \cup R\rangle_S$. because given $\mathcal{M}$ which solves the group's word problem we could build $\mathcal{M}'$ which takes two words $u, v \in (X \cup X^{-1})^*$, computes v^{-1} (we have already discussed how to do this), concatenate u and v^{-1}, and then use $\mathcal{M}$ to decide if uv^{-1} is equivalent to the identity. So $\mathcal{M}'$ could decide if $[uv^{-1}] = [\varepsilon]$ that is if $[u] = [v]$. Also if $\langle X \cup X^{-1} \,|\, R_{grp} \cup R\rangle_S$ has a solvable word problem, then use $w_0 = \varepsilon$ and get that $\{w \in (X \cup X^{-1})^* \,|\, [w] = [\varepsilon]\}$ is a recursive set. Hence, $\langle X \,|\, R\rangle$ has a solvable word problem too. So for any group, its group word problem is solvable if and only if its semigroup word problem is solvable.

Proposition 2.22. *If G has a solvable word problem with respect to one finite presentation, then G has a solvable word problem with respect to every finite presentation.*

Proof: Suppose that $(X \,|\, R)$ and $(X' \,|\, R')$ are finite presentations of the same group G. Therefore, if they both indeed present the same group then $\langle X \,|\, R\rangle \cong \langle X' \,|\, R'\rangle$. Hence there is an isomorphism $\psi : \langle X \,|\, R\rangle \to \langle X' \,|\, R'\rangle$. X is finite say $X = \{x_1, x_2, ..., x_k\}$. Let $w_i = \psi(x_i)$ ($\in (X' \cup X'^{-1})^*$) and also, $v_i = \psi(x_i^{-1})$ for $1 \leq i \leq k$.

Now, suppose that G has a solvable word problem with respect to the presentation $\langle X' \,|\, R'\rangle$. Let $u = \sigma_1...\sigma_l \in (X \cup X^{-1})^*$ where $\sigma_1 \in (X \cup X^{-1})$. Thus $\psi(u) = \psi(\sigma_1)\psi(\sigma_2)...\psi(\sigma_l) = \tau_1\tau_2...\tau_l$ where each τ_i is either w_i or v_i. Thus $\psi(u)$ is a word in $(X' \cup X'^{-1})^*$ and since we have that G has a solvable word problem in this presentation, we can decide if $[\psi(u)] = [\varepsilon]$. Since ψ is an isomorphism it is one-to-one and maps identity to identity. Therefore, this also decides if $[u] = [\varepsilon]$ in $\langle X \,|\, R\rangle$. ■

An easy consequence of this proposition is that if a group has a unsolvable word problem with respect to one presentation, then it must have an unsolvable word problem with respect to every presentation. Therefore, it makes sense to talk about a *group* having an unsolvable word problem (instead of a presentation of a group having an unsolvable word problem).

3 Some Groups with Solvable Word Problems

We get a finite presentation (for any given finite group) by encoding the whole Cayley table into the set of relations (as done with D_3 above). With this presentation the word problem is easy to solve.

Proposition 3.1. ***Finite Groups*** *have solvable word problems.*

Proof: Let $G = \{g_1, ..., g_n\}$ be a finite group. Then since the group operation is closed we have that for each $1 \leq i, j \leq n$, there exists a $1 \leq k_{i,j} \leq n$ such that $g_i g_j = g_{k_{i,j}}$ thus $1 = g_j^{-1} g_i^{-1} g_{k_{i,j}}$. It is easy to see that $G \cong \langle g_1, ..., g_n \,|\, g_j^{-1} g_i^{-1} g_{k_{i,j}}$ where $1 \leq i, j \leq n \rangle$. We are just encoding the whole Cayley (multiplication) table into the group's presentation. Now given $w \in G^*$ say $w = w' g_i g_j$ (w is of length 2 or greater). We have that $[w] = [w' g_i g_j g_j^{-1} g_i^{-1} g_{k_{i,j}}] = [w' g_i g_i^{-1} g_{k_{i,j}}] = [w' g_{k_{i,j}}]$ The new word $w' g_{k_{i,j}}$ is equivalent to w but is strictly shorter than w. Thus in a finite number of steps we can find an equivalent word of length 1 or 0. If length 0, then $[w]$ is equal to the identity. If length 1, then $[w] = [g_i]$. If g_i is the identity then $[w]$ is equal to the identity. Otherwise $[w]$ is not equal to the identity.

Thus we have sketched a way to solve the word problem for any finite group (with this rather large presentation). By an earlier proposition, we are guaranteed that G has a solvable word problem given any finite presentation. ■

Example 3.2. *Let $n \geq 3$, then D_n has exactly $2n$ elements (it is finite). Thus all the Dihedral groups have solvable word problems.*

Example 3.3. ***Integers Modulo*** n***:*** *Let $G = \langle a \,|\, a^n \rangle$. $\mathbb{Z}_n = \{0, 1, ..., n-1\}$ define addition by $k + l \bmod n$ for each $k, l \in \mathbb{Z}_n$. It is easy to check that $\phi : \mathbb{Z}_n \to G$ defined by $\phi(k) = [a^k]$ is an isomorphism. Hence $G \cong \mathbb{Z}_n$. Since this is a finite group we already know that it has a solvable word problem.*

Automatic groups form an interesting class of groups with solvable word problems.

Definition 3.4. *Let $\langle X \,|\, R \rangle$ be a finitely presented group. If the set $[\varepsilon]$ is a regular language (i.e. can be recognized by a finite automata), then we say that $\langle X \,|\, R \rangle$ is an* ***automatic group****.*

Thus the set $[\varepsilon]$ is not just recursive, it is regular. It is not hard to see that if G is automatic with respect to one presentation, then it is automatic with respect to every presentation. The proof is analogous to that of groups with solvable word problems. Given two isomorphic presentations, we just "rewire" the automata using the isomorphism between the two presentations.

For example, consider $\langle A, B, C, ... \,|\, R \rangle \cong \langle a, b, c, ... \,|\, r \rangle$. Suppose that second presentation is automatic. If A maps to abc we look at each node, if node i goes to i_a via a and then i_a goes to i_b via b and i_b goes to i_c via c, then we make a new automata with node

i connected to node i_c via A. Since automatic groups are not my main focus, I will skip the details of this proof.

Also, notice that all finite groups are automatic groups. We can use the same presentation from the proof that groups have solvable word problems, but instead of multiplying elements on the tape of the Turing machine, we can "hardwire" the Cayley table relations into the finite automata. Again, I will skip the details.

Example 3.5. ***An Infinite Group*** *with a solvable word problem.* $\langle a \,|\, \rangle = \langle a \rangle$ *is called the free Abelian group of rank 1. Consider the mapping* $\phi : \mathbb{Z} \to \langle a \rangle$ *defined by* $\phi(m) = [a^m]$*. Then it is easy to check that* ϕ *is bijective. In addition,* $\phi(m+n) = [a^{m+n}] = [a^m][a^n] = \phi(m)\phi(n)$*. Thus* ϕ *is an isomorphism. Hence the integers (under addition) are isomorphic to the free Abelian group of rank 1.*

Moreover, given $a^{m_1}a^{m_2}...a^{m_k}$ *it is easy to reduce this to* a^M *where* $M = \sum_{i=1}^{k} m_i$ *and then* $[a^{m_1}a^{m_2}...a^{m_k}] = [a^M] = [\varepsilon]$ *if and only if* $M = 0$ *(we have no relations to use). Therefore, the free Abelian group of rank 1 (and hence the integers under addition) has a solvable word problem.*

Definition 3.6. *Let* G_i*,* $1 \leq i \leq m$*, be groups. The* **external direct product** *of* G_1*,...,*G_m *is the group* $G_1 \oplus G_2 \oplus ... \oplus G_m$*. Elements of this group are just m-tuples:* $(g_1, ..., g_m)$ *where* $g_i \in G_i$*. Multiplication is defined by* $(g_1, ..., g_m)(h_1, ..., h_m) = (g_1h_1, ..., g_mh_m)$ *where* g_ih_i *is given by the operation in* G_i*. It is easy to verify that* $G_1 \oplus G_2 \oplus ... \oplus G_m$ *is in fact a group.*

Proposition 3.7. *If* G_i*,* $1 \leq i \leq m$*, are finitely presented groups with solvable word problems, then* $G_1 \oplus G_2 \oplus ... \oplus G_m$ *is a finitely presented group with solvable word problem.*

Proof: Let $(X_1 \,|\, R_1)$,...,$(X_m \,|\, R_m)$ be finite presentations of the G_i. Then it is clear that $(X_1 \times ... \times X_m \,|\, R_1 \times ... \times R_m)$ is a finite presentation of $G_1 \oplus G_2 \oplus ... \oplus G_m$. Moreover, if G_i has a solvable word problem, then there exists a Turing machine $\mathcal{M}_i$ which recognizes words equivalent to the identity in G_i. Take any word over $X_1 \times ... \times X_m$ and run $\mathcal{M}_i$ on the i^{th} coordinate. If each $\mathcal{M}_i$ accepts each coordinate, then the word is equivalent to the identity otherwise, it is not. Thus $G_1 \oplus G_2 \oplus ... \oplus G_m$ has a solvable word problem. ■

Theorem 3.8. The Fundamental Theorem of Finitely Generated Abelian Groups *Let G be a finitely generated Abelian group. That is G has a presentation* $(X \,|\, R)$ *where X is finite. Then there exists a finite list of prime powers* $p_1^{m_1}, ..., p_k^{m_k}$ *such that G is isomorphic to* $\mathbb{Z} \oplus ... \oplus \mathbb{Z} \oplus \mathbb{Z}_{p_1^{m_1}} \oplus ... \oplus \mathbb{Z}_{p_k^{m_k}}$ *where the number of copies of* $\mathbb{Z}$ *is finite.*

Proof: See Michael Artin's book *Algebra* [A]. Chapter 12, page 472, Theorem 6.4. ■

Putting these two theorems together with the preceding examples we get the following result.

Corollary 3.9. *Let G be a finitely presented Abelian group. G has a solvable word problem.*

Example 3.10. *An* **infinite non-Abelian** *group with a solvable word problem.*

We have seen already that $D_n \cong \langle x, y \,|\, x^2 = y^2 = (xy)^n = 1\rangle$. It's natural to consider what happens as n tends toward infinity. Consider $(xy)^\infty = 1$ as an empty relation. We get the infinite dihedral group:

$$D_\infty \cong \langle x, y \,|\, x^2 = y^2 = 1\rangle$$

First notice that $xy, (xy)^2, \ldots$ are all distinct (since we have no relation that allows us to interchange x's and y's). Thus, D_∞ is in fact an infinite group. It is also easy to see that D_∞ is non-Abelian (since $xy \neq yx$). Consider the following "basic moves" which could easily be performed by a Turing machine. $y^{-1} \to y^{-1}yy \to y$. Likewise, $x^{-1} \to x^{-1}xx \to x$. Thus given a word over $\{x, y, x^{-1}, y^{-1}\}$ we could build a Turing machine which first changes all y^{-1} to y, and changes all x^{-1} to x. Scan through the resulting word and delete any pair xx or yy. If something was deleted, then scan again. If a scan did not delete any pairs xx or yy, then the remaining word must be either empty (in this case it is the identity), or an alternating list of x's and y's. In this case, the input is not the identity (we cannot interchange x's and y's, so no more simplifying can be done). Thus this Turing machine solves the word problem for D_∞.

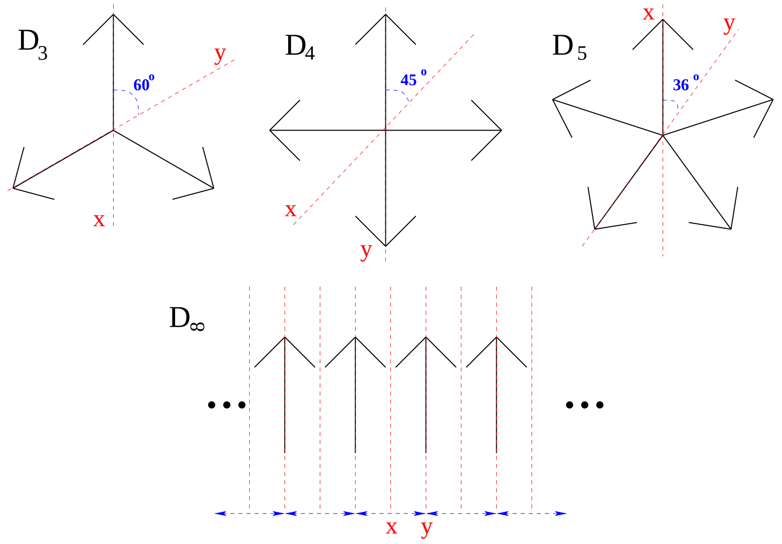

Figure: Some objects with Dihedral symmetries.

Notice that as n increases, the angle between the lines of reflect becomes smaller and smaller. In some sense, these lines are becoming parallel. The generators of D_∞ represent reflections across lines parallel to each other. Now, xy is a translation instead of a rotation.

It is interesting to note that D_∞ is not an automatic group (although it has a solvable word problem). This follows from the following lemma.

Lemma 3.11. $[\varepsilon]$ *is not regular.*

Proof: First, notice that $(xy)^1 y(xy)^0 x = (xy)y1x = xyyx = xx = 1$, thus $(xy)yx \in [\varepsilon]$. Also, $(xy)^{k+1}y(xy)^k x = (xy)^k xyyxy(xy)^{k-1}x = (xy)^k xxy(xy)^{k-1}x = (xy)^k y(xy)^{k-1}x$ thus by induction we find that $(xy)^{k+1}y(xy)^k x \in [\varepsilon]$ for each $k \geq 0$.

Now, suppose that $[\varepsilon]$ is regular and that N is the constant provided by the pumping lemma. We know that given any word of length greater than N can be written in the form uvw with $|uv| = N$ and $|v| = l \geq 1$. Consider the following cases.

Case 1: $|v| = l$ is odd. We know that in order for a word to be equal to the identity is must be of even length. This comes from the fact that all of our relations reduce word length by two: $xx^{-1} = 1$, $xx = 1$, etc. Thus if $uvw = 1$ then $|uvw|$ is of even length, but uv^2w has length $|uvw| + l$ which is odd. Therefore, $uv^2w \neq 1$. Hence, $|v|$ must be even.

Case 2: Suppose that $|v|$ is even and $N = 2k$ (N is even). We know $(xy)^{k+1}y(xy)^k x = 1$, this word breaks up into $uv = (xy)^k$ and $w = (xy)y(xy)^k x$. $v = (xy)^m$ (since $|v|$ is even). Thus $(xy)^{k+m+1}y(xy)^k x = (xy)^m(xy)^{k+1}y(xy)^k x = (xy)^m = 1$ which is a contradiction since xy is of infinite order (we cannot interchange x and y). Thus we must have that $|v|$ is even and N is odd.

Case 3: Suppose that $|v|$ is even and $N = 2k{+}1$ (N is odd). We know $(xy)^{k+1}y(xy)^k x = 1$, this word breaks up into $uv = (xy)^k x$ and $w = yy(xy)^k x$. $v = y(xy)^m x$ (since $|v|$ is even). Thus $(xy)^k xy(xy)^m xy(xy)^k x = (xy)^{k+1}(xy)^{m+1}(xy)^k x = (xy)^{2k+m+2}x = 1$ which again cannot be true. Hence we have reached yet another contradiction.

Therefore, we are forced to conclude that $[\varepsilon]$ is not regular. ■

4 A Group with an Unsolvable Word Problem

The group we are about to construct is essentially Boone's group [B]. I will follow the proof laid out in [R2], this is essentially due to Britton.

The proof has three big steps. The first is to construct a Turing machine which halts on a set of inputs which is a non-recursive set (yet recursively enumerable).

The second step is to show that there exists a semigroup with an unsolvable word problem. This basically involves encoding the steps of a Turing machine T into a semigroup $\Gamma(T)$. Then we notice that if we can tell when two elements are equal, we can also solve the halting problem (which is impossible).

The final step involves building a group $\mathcal{B}(T)$ which has a solvable word problem only if the semigroup $\Gamma(T)$ has a solvable word problem.

4.1 The Turing Machine

The proof that there exists a finitely presented group with an unsolvable word problem uses the existence of a semigroup with an unsolvable word problem. To construct this semigroup I need to set up some notation involving Turing machines.

Let $\bar{Q} = \{q_0, q_1, ...\}$ be a countable set of states. Let $\bar{\Sigma} = \{s_0, s_1, ...\}$ be a countable alphabet. Then a Turing machine, T, is characterized by its set of states: $Q(T) = \{q_0, ..., q_M\}$, alphabet: $\Sigma(T) = \{s_0, ..., s_N\}$, and transition function: $\delta_T : \Sigma(T) \times Q(T) \to \Sigma(T) \times Q(T) \times \{R, L\}$. By convention let s_0 be the **blank** character, q_0 the **halting state**, and q_1 the **start state**.

The first thing to notice is that the transition function can be described by a finite set of words of length 5 over the alphabet $\Sigma(T) \cup Q(T) \cup \{L, R\}$. If $\delta_T(s_i, q_j) = (s_k, q_l, X)$, then use $s_i q_j s_k q_l X$ to describe this transition. There is exactly one word for each element in the domain of δ_T. Thus there are only $|\Sigma(T) \times Q(T)| = MN$ such words. So let $p_1, ..., p_{5MN}$ be the first $5MN$ primes. Assign $R \to 0$, $L \to 1$, $q_i \to 2i + 2$, and $s_j \to 2j + 3$. Concatenate the words formed from the transition function in any order (use a lexicographic ordering on $\Sigma(T) \times Q(T)$). Then let e_i be the integer assigned to the i^{th} character in that word. Thus the Turing machine can be encoded by a single natural number as follows: $G(T) = \prod_{i=1}^{5MN} p_i^{e_i}$ (the Gödel number of T). The *Fundamental Theorem of Arithmetic* assures us that each Turing machine has a different Gödel number. Finally, we order the Turing machines by their Gödel numbers and get an enumeration of Turing machines: $\{T_0, T_1, ...\}$.

Next, define the set: $K = \{n \in \mathbb{N} \,|\, T_n \text{ halts on input } s_1^{n+1}\}$. Consider, T_i. Initially, T_i is in the start state q_1 with input s_1^{i+1}. Let $\alpha_{i,j}$ be the state and tape contents of T_i after j steps of the Turing machine. If the machine halts after k steps then let $\alpha_{i,j} = \alpha_{i,k}$ for all $j \geq k$. If we dovetail through the steps of the Turing machines (see the following figure), we will reach the halting state for any Turing machine T_n that halts on the input s_1^{n+1}. See the figure below:

$$\begin{tikzcd}
T_0 & T_1 & T_2 & T_3 & T_4 & T_5 \\
\alpha_{0,0} \arrow[d] & \alpha_{1,0} \arrow[r] & \alpha_{2,0} \arrow[dl] & \alpha_{3,0} \arrow[r] & \alpha_{4,0} \arrow[dl] & \alpha_{5,0} \\
\alpha_{0,1} \arrow[ur] & \alpha_{1,1} \arrow[dl] & \alpha_{2,1} \arrow[ur] & \alpha_{3,1} \arrow[dl] & \alpha_{4,1} \arrow[ur] & \\
\alpha_{0,2} \arrow[d] & \alpha_{1,2} \arrow[ur] & \alpha_{2,2} \arrow[dl] & \alpha_{3,2} \arrow[ur] & & \\
\alpha_{0,3} \arrow[ur] & \alpha_{1,3} \arrow[dl] & \alpha_{2,3} \arrow[ur] & & & \\
\alpha_{0,4} \arrow[d] & \alpha_{1,4} \arrow[ur] & & & & \\
\alpha_{0,5} \arrow[ur] & & & & &
\end{tikzcd}$$

Figure: Dovetailing through all of the Turing machines

Hence we can build a Turing machine which preforms this dovetailing. That is, we can build a Turing machine T^* such that given the input s_1^{n+1}, T^* halts only if T_n halts on the input s_1^{n+1}. Thus K is a recursively enumerable set.

Proposition 4.1. *K is not recursive*

Proof: Suppose that K is recursive, then its complement $\bar{K} = \{n \in \mathbb{N} \,|\, T_n \text{ does not halt on } s_1^{n+1}\}$ must be recursively enumerable. Let T' be the machine that enumerates $\bar{K}$. That is T' halts on the input s_1^{n+1} if and only if T_n does not halt on that same input.

Since we have enumerated all of the Turing machines, we must have that $T' = T_m$ for some natural number m.

Suppose that $m \in \bar{K}$. This means that $T' = T_m$ will halt on s_1^{m+1}, but then this implies that $m \in K$ which is a contradiction.

On the other hand, if $m \notin \bar{K}$ then $m \in K$ so that T_m $(= T')$ halts on s_1^{m+1} hence $m \in \bar{K}$.

Therefore, no such m can exist. Thus there cannot be a Turing machine which enumerates $\bar{K}$. Therefore, $\bar{K}$ is not r.e. and hence K is not recursive. ■

Notice that we can describe a Turing machine at any point in its computation with a word over the alphabet $Q(T) \cup \Sigma(T)$. Let $\sigma, \tau \in \Sigma(T)^*$, $q_i \in Q(T)$, and $s_j \in \Sigma(T)$ then if the Turing machine's tape content is $\sigma s_j \tau$ (only a finite amount of tape can be used at any given point) and if the machine is currently in the state q_i and is scanning s_j then we describe the state of the machine by the following word: $\sigma q_i s_j \tau$.

Definition 4.2. *Such a word $\sigma q_i s_j \tau$ is called an **instantaneous description** of the Turing machine.*

Note: "□" is used to denote the ends of the used part of a Turing machine's tape.

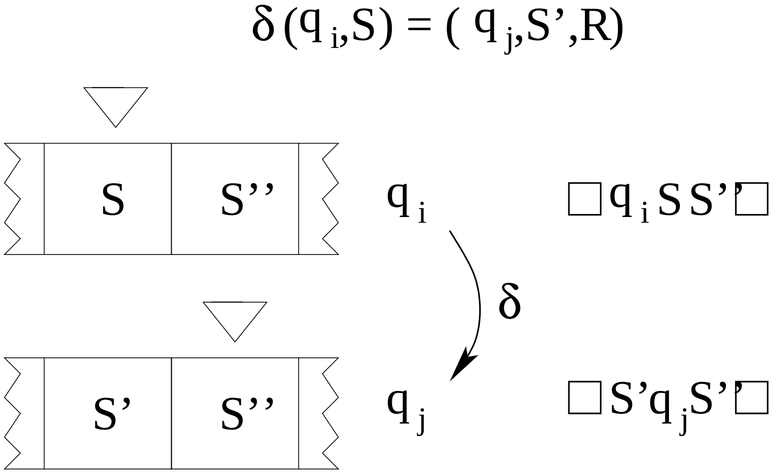

Figure: Transitioning from one instantaneous description to another.

Definition 4.3. *Let $q_i \in Q(T)$, $s_j \in \Sigma(T)$, and $w = \sigma q_i s_j \tau, w' \in (\{\Box, q\} \cup Q(T) \cup \Sigma(T))^*$ then $w \to w'$ is a* ***basic move****...*

- If $\delta_T(s_i, q_j) = (s_k, q_l, R)$ and w' is of the form $\sigma s_k q_l \tau'$ where $\tau' = \tau$ if τ is non-empty and $\tau' = s_0$ otherwise.
- If $\delta_T(s_i, q_j) = (s_k, q_l, L)$ and w' is of the form $\sigma' q_l s_m s_k \tau$ where we define σ' and s_m by $\sigma = \sigma' s_m$ if σ is non-empty and $\sigma' = \varepsilon$, $s_m = s_0$ (a blank) otherwise.

4.2 The Semigroup

Let $\Gamma(T)$ be the semigroup generated by $\{\Box, q\} \cup Q(T) \cup \Sigma(T)$ with the following relations:

1. $q_i s_j s_m = s_k q_l s_m$ where $\delta_T(s_j, q_i) = (s_k, q_l, R)$.
2. $q_i s_j \Box = s_k q_l s_0 \Box$ where $\delta_T(s_j, q_i) = (s_k, q_l, R)$.
3. $s_m q_i s_j = q_l s_m s_k$ where $\delta_T(s_j, q_i) = (s_k, q_l, L)$.
4. $\Box q_i s_j = \Box q_l s_0 s_k$ where $\delta_T(s_j, q_i) = (s_k, q_l, L)$.
5. $q_0 s_i = q_0$
6. $s_i q_0 \Box = q_0 \Box$
7. $\Box q_0 \Box = q$

The semigroup $\Gamma(T)$ is called the semigroup **associated with** T.

Definition 4.4. *$w \in \Gamma(T)$ is* ***$\Box$-special*** *if $w = \Box \alpha \Box$ where α is an instantaneous description of T.*

Now notice that in $\Gamma(T)$ relations 1-4 correspond the effects of basic moves in T on a $\Box$-special element. The second and fourth relations handle the cases when the head reaches a point on the tape that it hasn't reached before (if we are at the "end of the tape", we simply add an extra s_0 – blank).

In $\Gamma(T)$ relations 3-7 guarantee that T halts on input $w \in \Sigma(T)^+$ if and only if $[\Box q_1 w \Box] = [q]$. To see this notice that if T does not halt on w then T will never enter the state q_0 so we can never use relation 7 to destroy the "$\Box$"s. On the other hand if T does halt on w then after a finite number of basic moves we get $[\Box q_1 w \Box] = [\Box \sigma q_0 \tau \Box]$ for some $\sigma, \tau \in \Sigma(T)^*$. Then using relation 5 we get $[\Box \sigma q_0 \tau \Box] = [\Box \sigma q_0 \Box]$ then relations 6 and 7 get $[\Box \sigma q_0 \Box] = [\Box q_0 \Box] = [q]$.

Next note that in any monoid $\langle X \mid R \rangle$ if $[w] = [w']$, then by the lemma which describes the contents of the congruence generated by R we know that there is a finite sequence $w = w_1 \to w_2 \to ... \to w_t = w'$ where for each $1 \leq i < t$ there are $a_i, b_i, x_i, y_i \in X^*$ such that $w_i = a_i x_i b_i$, $w_{i+1} = a_i y_i b_i$, and either (x_i, y_i) or (x_i, y_i) is in R. We call each step $w_i \to w_{i+1}$ an **elementary operation**.

Lemma 4.5. *Let $w, w' \in (\{\Box, q\} \cup Q(T) \cup \Sigma(T))^*$. Let $w \to w'$ be an elementary operation (thus $[w] = [w']$). Also assume that $[w] = [w'] \neq [q]$. Then w is $\Box$-special if and only if w' is $\Box$-special.*

Proof: Suppose that u is $\Box$-special, then u describes T in the middle of a computation. If $[u] \neq [q]$, then T must not halt after getting to u's state. Hence, u cannot involve q_0. Thus if either $[w]$ or $[w']$ is $\Box$-special, the elementary operation $w \to w'$ must come from relations 1-4. But these relations are just basic moves of the Turing machine from a instantaneous description α to another instantaneous description β. We must have either $w = \Box\alpha\Box$ and $w' = \Box\beta\Box$ or $w = \Box\beta\Box$ and $w' = \Box\alpha\Box$. ■

Lemma 4.6. *Let $w, w' \in (\{\Box, q\} \cup Q(T) \cup \Sigma(T))^*$. If $w = \Box\alpha\Box$ is $\Box$-special, $[w'] \neq [q]$, and $w \to w'$ is an elementary operation from relations 1-4, then $w' = \Box\beta\Box$ where either $\alpha \to \beta$ or $\beta \to \alpha$ is a basic move of T.*

Proof: $w \to w'$ is an elementary operation thus $[w] = [w'] \neq [q]$. Therefore, by the previous lemma we know that w' is also $\Box$-special, say $w' = \Box\beta\Box$. Since the elementary operation came from relations 1-4, the instantaneous descriptions α and β must be related by a basic move of the Turing machine T. ■

Lemma 4.7. *Let $E_T = \{w \in \Sigma^+ \,|\, T \text{ halts on } w\}$. Then for each $w \in (\{\Box, q\} \cup Q(T) \cup \Sigma(T))^*$ we have that: $w \in E_T$ if and only if $[\Box q_1 w \Box] = [q]$.*

Proof: If $w \in E$ then we have already discussed why we must have that $[\Box q_1 w \Box] = [q]$. The other direction of the proof is a bit more difficult.

Suppose that $[\Box q_1 w \Box] = [q]$. We know then that $\Box q_1 w \Box$ and q are related by a finite number of elementary moves. But at some point they must involve q_0 (so eventually relation 7 can be used to destroy the "$\Box$"s). Therefore, we know that there exists a finite number of elementary moves of type 1-4 such that $\Box q_1 w \Box = \Box\alpha_1\Box \to \Box\alpha_2\Box$, $\Box\alpha_2\Box \to \Box\alpha_3\Box$, ..., $\Box\alpha_{t-1}\Box \to \Box\alpha_t\Box = \Box\sigma q_0 s_k \tau\Box$ where $\sigma, \tau \in \Sigma^*$ and $s_k \in \Sigma$. Each $\Box\alpha_i\Box \to \Box\alpha_{i+1}\Box$ then corresponds to a basic move of T. Either T moves from i to $i+1$ or from $i+1$ to i (the semigroup relations are symmetric although the Turing machines moves are not).

Now consider the case where $t = 2$ the machine cannot make a basic move from the halting state hence $\Box q_1 w \Box = \Box\alpha_1\Box$ to $\Box\alpha_2\Box = \Box\sigma q_0 s_k \tau\Box$ must be a basic move hence the arrows follow the moves of the Turing machine in order.

Assume, by induction, that given a list of length less than t, we can find a sublist in which each elementary move corresponds to a basic move of T and all the arrows go in the right direction.

Consider the list of length t above. By the $t = 2$ case, we know that that $\Box\alpha_{t-1}\Box \to \Box\alpha_t\Box = \Box\sigma q_0 s_k \tau\Box$ must move in the correct order. Let $i+1$ be the last index where T moves backward from $i+1$ to i. Hence $i + 1 \leq t - 1$ and thus T moves from $i+1$ to $i+2$. Therefore T moves from $i+1$ to both i and $i+2$, but T has well defined deterministic moves hence $\Box\alpha_i\Box = \Box\alpha_{i+2}\Box$ and thus we can delete $\Box\alpha_{i+1}\Box$ and $\Box\alpha_{i+2}\Box$ from the list. Therefore, by induction we can find a sublist in which the arrows all go in the right direction.

Therefore, if $[\Box q_1 w\Box] = [q]$ there must be a sequence of basic moves of T that get T into the state q_0. Thus T halts on w. ■

Theorem 4.8. ***(Markov-Post, 1947)*** *$\Gamma(T^*)$ is a finitely presented semigroup with an unsolvable word problem*

Proof: Let $\Gamma(T)$ be the semigroup associated with the Turing machine T. Define $\hat{\Omega} = (\{\Box, q\} \cup Q(T) \cup \Sigma(T))^*$ and $\Omega = \Sigma(T)^* \subset \hat{\Omega}$. Let E $(= E_T)$ be the set of all inputs on which T halts (note $E \subset \Omega$). Define $\hat{E} = \{\hat{w} \in \hat{\Omega} \,|\, [\hat{w}] = [q]\}$. Define $\phi : \Omega \to \hat{\Omega}$ by $w \mapsto \Box q_1 w \Box$, and identify Ω with its image $\Omega_1 \subset \hat{\Omega}$. Also, identify E with its image $E_1 = \{\Box q_1 w\Box \,|\, w \in E\}$. Then E is a recursive subset of Ω if and only if E_1 is a recursive subset of Ω_1. Note that Ω_1 is obviously a recursive subset of $\hat{\Omega}$. The previous lemma tells us that $E_1 = \hat{E} \cap \Omega_1$.

Consider the Turing machine T^* (the machine we obtained by dovetailing through all Turing machines). Then $E = K$ is recursively enumerable but not recursive. Thus E_1 is r.e. but not recursive. But the intersection recursive subsets of $\hat{\Omega}$ is still recursive. So we must conclude that $\hat{E}$ is not recursive. Thus, $\Gamma(T^*)$ has an unsolvable word problem. ■

4.3 The Group

I already constructed a Turing machine T^* and associated semigroup $\Gamma(T^*)$. The Markov-Post theorem showed that $\Gamma(T^*)$ has an unsolvable word problem. Consider the following restatement of the Markov-Post theorem.

Corollary 4.9. *There is a finitely presented semigroup:*

$$\Gamma = (q, q_0, ..., q_N, s_0, ..., s_M \,|\, F_i q_i' G_i = H_i q_i'' K_i,\ i \in I)$$

with an unsolvable word problem, where $F_i, G_i, H_i, K_i \in \{s_0, ..., s_M\}^*$ and $q_i', q_i'' \in \{q_0, ..., q_N\}$. Moreover, there is no way to decide if $[Xq'Y] = [q]$ for arbitrary $X, Y \in \{s_0, ..., s_M\}^*$ and $q' \in \{q_0, ..., q_N\}$.

Proof: Consider $\Gamma(T^*)$. Relabel $\Box$ as the last s_M and call this semigroup Γ. Thus, the relations in Γ have the desired form. The corollary follows from the Markov-Post theorem. ■

Definition 4.10. *If $X = \sigma_1^{e_1}\sigma_2^{e_2}...\sigma_k^{e_k}$ (e_j may be negative or positive) and $\sigma_i \in \{s_0, ..., s_M\}$, then let $X^\# = \sigma_1^{-e_1}\sigma_2^{-e_2}...\sigma_k^{-e_k}$. Note that this is not the inverse of X unless the σ's commute. Also, notice that $(X^\#)^\# = X$ and $(XY)^\# = X^\# Y^\#$.*

Definition 4.11. *Let $X, Y \in \{s_0, s_0^{-1}, ..., s_M, s_M^{-1}\}$ and $q_j \in \{q_0, ..., q_N\}$. Then let $(Xq_jY)^* = X^{\#}q_jY$.*

Definition 4.12. *A word W is* ***special*** *if $W = X^{\#}q_jY$, where $X, Y \in \{s_0, ..., s_M\}$ and $q_j \in \{q_0, ..., q_N\}$. Notice that if W is special (ie $W = X^{\#}q_jY$), then $W^* = (X^{\#})^{\#}q_jY = Xq_jY$ is a word over the generators of Γ (the semigroup).*

Let $\mathcal{B}(T)$ be the group generated by $q, q_0, ..., q_N, s_0, ..., s_M, r_i, i \in I, x, t, k$ with the following relations:

1. - $xs_\beta = s_\beta x^2$
2. - $r_i s_\beta = s_\beta x r_i x$
   - $r_1^{-1} F_i^{\#} q_{i_1} G_i r_i = H_i^{\#} q_{i_2} K_i$
3. - $tr_i = r_i t$
   - $tx = xt$
4. - $kr_i = r_i k$
   - $kx = xk$
   - $k(q^{-1}tq) = (q^{-1}tq)k$

where $i \in I$ and $\beta = 0, ..., M$.

Lemma 4.13. ***(Boone's Lemma)*** *Let T be a Turing machine with stopping state q_0 and associated semigroup $\Gamma = \Gamma(T)$ (rewritten as in the corollary). If W is a special word, then $[k(W^{-1}tW)] = [(W^{-1}tW)k]$ in $\mathcal{B} = \mathcal{B}(T)$ if and only if $[W^*] = [q]$ in $\Gamma(T)$.*

Proof: The proof of Boone's Lemma is rather long and involves some more advanced ideas from group theory. Since I have been following the group theory text by Rotman, I will refer the reader to [R2] for the proof of Boone's Lemma. The original proof by Boone is a bit longer and more involved. You can find it in [B]. $\blacksquare$

Theorem 4.14. ***(Novikov-Boone-Britton)*** *There exists a finitely presented group $\mathcal{B}$ with an unsolvable word problem.*

Proof: Let T^* be the Turing machine from the Markov-Post theorem. Let Γ be the corresponding semigroup and $\mathcal{B}$ be the corresponding group (as defined above). Suppose that the word problem for $\mathcal{B}$ is solvable. Then given an arbitrary special word W, we could decide if $[kW^{-1}tWk^{-1}W^{-1}t^{-1}W] = [\varepsilon]$ (where ε is the identity). But this would tell us whether $[k(W^{-1}tW)] = [(W^{-1}tW)k]$, and by Boone's lemma we would then be able to decide if $[W^*] = [q]$ in Γ. But by the corollary to the Markov Post theorem, we cannot decide if $[W^*] = [q]$ in Γ for an arbitrary W^*. Therefore, we have reached a contradiction. Thus we must conclude that $\mathcal{B}$ has an unsolvable word problem. $\blacksquare$

5 Markov Properties

In 1958, Adian and Rabin extended an idea of Markov from semigroups to groups. Originally, Markov showed that if a property of a semigroup was of a certain form, then no decision process could recognize whether a finite presented semigroup had this property or not. These properties are called Markov properties of semigroups. Such properties are quite abundant. In the following section, we will look at the analogue for groups.

Definition 5.1. *Let $\mathcal{M}$ be a group property such that*

- *If two groups are isomorphic, either both share property $\mathcal{M}$ or both lack it.*
- *There is at least one finitely presented group with this property.*
- *There is also a finitely presented group which cannot be embedded in (shown to be isomorphic to a subgroup of) some group with this property.*

Then $\mathcal{M}$ is a **Markov property***.*

Many familiar (and important) properties of groups are Markov properties. I will list just a few.

Proposition 5.2. *The following are Markov properties:*

1. *G is the trivial group (G has only 1 element – the identity).*
2. *G is a finite group.*
3. *G is Abelian.*
4. *G is a free group (has a presentation with no relations).*
5. *G has a solvable word problem.*

Proof:

1. Isomorphisms are bijective, so they preserve the "size" (or order) of a group. $(x \mid x = 1)$ is a finite presentation of the trivial group. And any non-trivial group cannot be embedded inside the trivial group!
2. Again, isomorphisms are bijective, so they preserve the order of a group. We have already given a finite presentation for an arbitrary finite group (see the proof that all finite groups have solvable word problems). Finally, D_∞ is a finitely presented group which obviously cannot be embedded in any finite group (it's too big!).
3. Suppose that two groups are isomorphic, then we have an isomorphism f. $ab = ba$ implies that $f(ab) = f(ba)$ thus $f(a)f(b) = f(b)f(a)$ hence if one group is Abelian, then so is the other. $\langle x|\rangle$ is a finitely presented Abelian group (isomorphic to the integers under addition). D_∞ cannot be embedded in any Abelian group since it is non-Abelian (subgroups of Abelian groups are Abelian themselves).

4. G is free if it is isomorphic to a group presented with no relations. Thus freeness is by definition invariant under isomorphisms. $\langle x \mid \rangle$ is a finitely presented free group. Free groups have no relations on their generators, so no element can be of finite order (this would be a relation on an element). Since finite groups consists entirely of elements of finite order, it is impossible to embed finite groups in free groups.

5. We have already shown that if G has an solvable word problem with respect to one finite presentation, then it will have an solvable word problem with respect to every presentation. Any finite group is finitely presented and has a solvable word problem. Finally, we have already constructed a group with an unsolvable word problem. This group obviously cannot be embedded in a group with a solvable word problem (else we could use the decision process of the larger group to solve the word problem of the subgroup). ■

Theorem 5.3. (Adian-Rabin, 1958) *Given a Markov property $\mathcal{M}$, there does not exist a Turing machine which when given finite presentation can tell if the finitely presented group has the property $\mathcal{M}$.*

Proof: This theorem was first proved (for semigroups) by Markov in 1950. See [R2] page 469 for a proof. ■

Thus we cannot decide if an arbitrary finitely presented group has a given Markov property or not.

Corollary 5.4. *Given an arbitrary finite presentation $(X \mid R)$, there is no way to decide if $\langle X \mid R\rangle$...*

1. *is the trivial group (G has only 1 element – the identity).*

2. *is not the trivial group.*

3. *is a finite group.*

4. *is an infinite group.*

5. *is Abelian.*

6. *is non-Abelian.*

7. *is a free group (has a presentation with no relations).*

8. *is not free.*

9. *has a solvable word problem.*

10. *has an unsolvable word problem.*

Proof: Obviously, if we could decide the complement of a Markov property, then we could just switch our "yes" answers and our "no" answers and thus decide the Markov property too. Hence complements of Markov properties are also undecidable. Now notice that each of these is either a Markov property or the complement of a Markov property. ■

Recall that the word problem for finite groups and (finitely generated) Abelian groups is solvable. So such groups have fairly nice structure. However, by the previous corollary, given an arbitrary finite presentation, there is no way to tell if it is in fact a presentation of a finite or Abelian group.

Seeing that it is (in general) impossible to figure out group properties from a finite presentation, the following corollary should not be too surprising.

Corollary 5.5. (The Isomorphism Problem for Groups) *There is no way to decide if two arbitrary finite presentations, present the same group.*

Proof: If we could decide whether two arbitrary finite presentations present the same group, then we could decide if an arbitrary group was isomorphic to $\langle x \,|\, x = 1 \rangle$. That is would could decide if the group was trivial. ■

References

[A] Michael Artin, *Algebra*, Prentice-Hall, Upper Saddle River, New Jersey, 1991.

[B] William W. Boone, *The Word Problem*, Annals of Mathematics, Vol. 70, No. 2, Sept. 1959, 207-265.

[E] D. Epstein, J.W. Cannon, D.F. Holt, S.V.F. Levy, M.S. Paterson, and W.P. Thurston, *Word Processing in Groups*, Jones and Bartlett Publishers, Boston, 1992.

[G] Joseph A. Gallian, *Contemporary Abstract Algebra*, Fifth Edition, Houghton Mifflin, Boston, 2002.

[LP] R. Lidl and G. Pilz, *Applied Abstract Algebra*, Second Edition, Undergraduate Texts in Math., Springer, New York, 1998.

[M] Bernard M. Moret, *The Theory of Computation*, Addison-Wesley, Reading, 1998.

[R1] Joseph J. Rotman, *The Theory of Groups: An Introduction*, Allyn and Bacon, Boston, 1965.

[R2] Joseph J. Rotman, *An Introduction to the Theory of Groups*, Fourth Edition, Graduate Texts in Math., Vol. 148, Springer-Verlag, New York, 1995.

[S] John Stillwell, *The Word Problem and the Isomorphism Problem for Groups*, Bulletin of the AMS, Vol. 6, Number 1, Jan. 1982, 33-56.