APPLICATIONS

1 Counting via group actions

Theorem 1.1 (Burnside’s Formula). Let $G$ be a finite group acting on $X$. Then, if $r$ = the number of orbits of $G$ in $X$, then

$$r = \frac{1}{|G|} \sum_{g \in G} |X_g|.$$ 

What does this mean? Let’s do an example.

Example 1.2. How many different ways are there to paint the edges of a triangle using four colors of paint?

Let $X$ be the set of all colorings of the triangle. Note there are $64 = 4^3$ possible colorings, but many of these are the same triangle (it’s just been rotated or flipped). We know $S_3$ acts on $X$, and two triangles have the same painting if they are in the same orbit of $S_3$. So, we need to compute the number of distinct orbits (these are just the colorings of the triangle up to symmetries, so they are the physically indistinguishable colorings).

We can use Burnside’s Formula! We just compute $|X_g|$ for each $g \in G$.

$|X_e| = 64$ because every coloring is fixed by $e$

$|X_r| = 4$ because the only colorings fixed by a rotation must have all the same colored edges

$|X_{r^2}| = 4$ by the same reason

$|X_f| = 16$ : the switched edges must be the same color, and the other can be any color

$|X_{fr}| = 16$ by the same reason

$|X_{fr^2}| = 16$ by the same reason

So, using Burnside’s formula, the number of triangles = number of orbits is

$$= \frac{1}{6} (64 + 4 + 4 + 16 + 16 + 16) = 20.$$ 

You can count many things this way!

2 RSA Encryption

Alice wants to send a message to Bob securely. How does she do this? In RSA encryption, imagine Bob has a large supply of locks (that only he has the key to!). The lock will be his public key, meaning anyone has access to it, and the key will be his private key, meaning only he has access to it. Alice wants to message Bob, so she gets him to send her an unlocked lock, then places her message in a box, and locks it with his lock. She then can send the locked message securely to Bob, and he has the key, so he can unlock it when it arrives!

How do we turn this into a cryptosystem? Today we will explore RSA (Rivest-Shamir-Adleman) Encryption.
Example 2.1. For any number $n$, recall that $\phi(n) =$ the number of numbers in $\mathbb{Z}_n$ such that $\gcd(a,n) = 1$. Show that, if $n = pq$, where $p$ and $q$ are distinct primes, then $\phi(n) = (p-1)(q-1)$. (Note: you did this already, in Homework 2, Problem 10!)

Example 2.2. If $n = pq$ where $p$ and $q$ are prime numbers, let $\phi(n) = (p-1)(q-1)$. Pick a number $2 < e < \phi(n)$ such that $\gcd(e,\phi(n)) = 1$ and compute its multiplicative inverse $d$, so $ed \equiv 1 \mod \phi(n)$. Show that

$$m \equiv m^{ed} \mod n.$$  

Answer: by Lagrange’s Theorem and its corollaries (Fermat’s little theorem!), we know, if $\gcd(m,n) = 1$, then $m^{\phi(n)} = 1 \mod n$. Because $ed = 1 \mod \phi(n)$, this means $ed = 1 + k\phi(n)$ for some integer $k$. Note: if $\gcd(m,n) = 1$, then because $n = pq$, $\gcd(m^k,n) = 1$, so $m^{ed} = m^{1+k\phi(n)} = m(m^k)^{\phi(n)} = m \mod n$. If $\gcd(m,n) \neq 1$, then $\gcd(m,n) = p, q, \text{ or } pq$. Treating these cases carefully, we can get the same result, although it requires a bit more work.

Once we have this, this is how it works:

1. Choose two large primes $p$ and $q$ of approximately equal size and compute $n = pq$.
2. Compute $\phi(n) = (p-1)(q-1)$.
3. Choose an integer $e > 1$ such that $\gcd(e,\phi(n)) = 1$ and compute its inverse $d \mod \phi(n)$. (This means: pick $e$ and compute $d$ such that $de \equiv 1 \mod \phi(n)$.)
4. Your **public key** is $(n,e)$. Everyone knows this
5. Your **private key** is $(n,d)$. You don’t tell this to anyone.
6. Convert a message to a number $m$.
7. Choose someone to send your message to. Look up their **public key** and compute $c = m^e \mod n$.
8. To decrypt a message sent to you, use **your** private key to compute $m = c^d \mod n$. This works because we know

$$c^d \mod n = (m^e)^d \mod n = m^{ed} \mod n$$

and, by the previous example,

$$m = m^{ed} \mod n.$$  

If you pick small primes, this is not a particularly good cryptosystem. For example, if you know how to factor $n$ as $n = pq$, then it is easy to compute private keys (which are supposed to be secret!).

The reason this is used is because, if $n$ is very large, it is very hard for computers to factor it quickly. This is a fundamental problem in math and computer science.

In the real world, computers choose two large numbers $p$ and $q$ with high probability that they are prime (we talked a bit about this with Fermat’s Little Theorem) each with 150 - 600 digits, and then compute everything else. They usually choose $e = 2^{16} + 1 = 65537$ for technical reasons. You can read a lot more about this and other cryptosystems on the internet.
3 Chemistry

Group theory has many applications to chemistry. Most of them require understanding something we have not discussed, called representation theory. If you’re interested, the internet is an *excellent* learning resource.\(^1\)

There are many applications to spectroscopy and crystallography coming from representation theory, but there is at least one application we can grapple with today.

**Question 3.1.** How do atoms bond to form molecules?

Some of you may know that atoms consist of a small, dense, positive center (the nucleus) surrounded by swirling probability clouds of very light, very fast electrons. Bonding happens when one atom shares an electron with another. But what happens to the electrons? Why can only certain bonds appear?

Because of the wave-particle duality of electrons, we cannot precisely know their position so we compute a probability function of where it will be. With about 95 percent certainty, we can say each electron will be in an atomic orbital. The orbitals are determined by how many electrons surround an atom. Here’s a picture of the energy clouds and a (very small) periodic table. The atomic number tells you how many electrons there are.

---

\(^1\) Spoiler: representations are essentially just homomorphisms from \(G\) to the group of \(n \times n\) matrices.
Only the orbitals with the highest quantum state can participate in molecular bonding. (The quantum state is the integer $n$ in front of the orbital type.) So, for the oxygen atom, only the $2s$, $2p_x$, $2p_y$, and $2p_z$ orbitals can contribute to bonding.

Once we know where the electrons live near a single atom, we can talk about molecular bonding. The molecular orbitals are the probability clouds that electrons occupy when atoms bond together and they are best approximated by linear combinations of atomic orbitals.

Generally, to solve for the shape of the probability clouds, you have to take eigenfunctions of the wave functions of the electrons and integrate those functions over all space, with some complicated formula abbreviated as

$$S_{ij} = \int \phi_i^* \phi_j d\tau$$

but, if we use symmetry, we can make this a whole lot simpler! If atomic orbitals are involved in forming a molecular orbital, they must be invariant under the same symmetry operations. Let’s look at a very friendly molecule as an example: water.

**Example 3.2.** Water has molecular formula $H_2O$. Hydrogen has one electron and oxygen has 8, so we know the hydrogen atoms’ electrons each occupy a $1s$ orbital and the oxygen atom’s bonding electrons occupy four different orbitals: $2s$, $2p_x$, $2p_y$, and $2p_z$.

```plaintext
Water (H₂O)

Bonding orbitals:
- Hydrogen: 1s
- Oxygen: 2s, 2pₓ, 2pᵧ, 2pᵦ

If the 1s orbitals are the same sign, they are unchanged by every symmetry operation.
So, they can only bond with an orbital on the oxygen atom if it is also unchanged by every symmetry operation!
```

```plaintext
Water (H₂O)

The 1s orbitals on the H atoms can either be the same sign or opposite sign:

The only such orbitals are the 2s and the 2pᵦ:
```

```plaintext
Water (H₂O)

The 1s orbitals on the H atoms can either be the same sign or opposite sign:

The only such orbitals are the 2s and the 2pᵦ:
```
Water (H₂O)

If the 1s orbitals are of opposite signs, they:
- switch signs under rotation
- switch signs under reflection in the plane bisecting the oxygen atom
- remain unchanged under reflection through the plane of the molecule

So, in summary, there are many potential ways the atomic orbitals could come together to bond. But, using symmetry and without integrating anything, we see that there are only three molecular orbitals involved in bonding.

Water (H₂O)
The only orbital on the oxygen atom that transforms the same way is the 2pₓ orbital:

The 2pₓ orbital on the oxygen atom does not form a molecular orbital, but the others do.

There is a lot of detail missing here and a lot more that can be said, but I wanted to at least give an indication of how group theory can be used in some hard sciences!