CDM
Group Actions and Counting

Klaus Sutner

Carnegie Mellon Universality

24-actions 2017/12/15 23:15

1. Some Counting Problems

- Actions
- Burnside's Lemma
- Some Applications

So far, we have talked at various levels of detail about:

- computability and decidability
- iteration of endofunctions
- finite state machines
- first-order logic and automaticity
- semigroups and groups

Next up: group actions, with an application to counting.

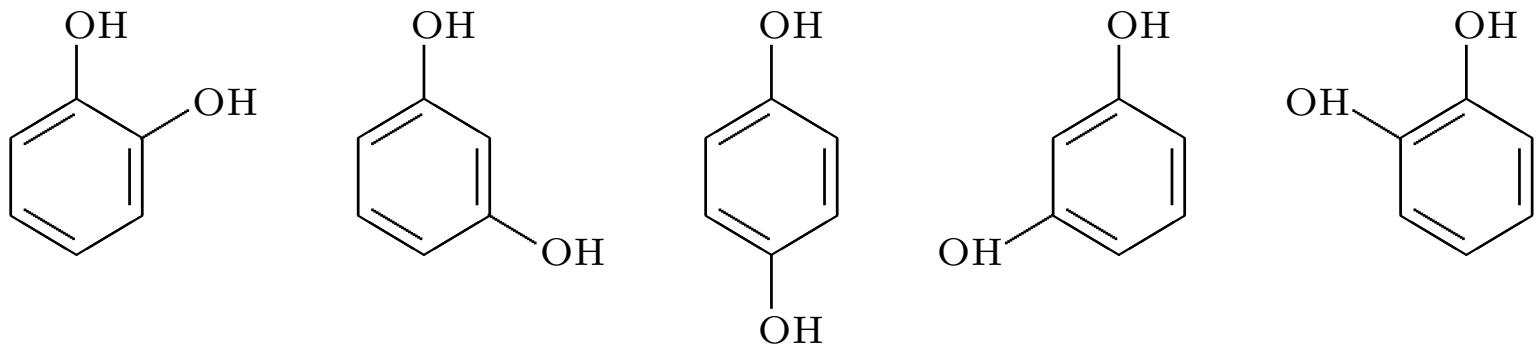
Here is the central problem:

> We have a finite set A and an equivalence relation $\approx$ on A. We want to count the number of equivalence classes of $\approx$ (also known as the index of the equivalence relation).

Think of an equivalence class as a pattern, so we want to count patterns.

Of course, A will be large. In fact, often we have a whole parametrized family A_n and we want an answer in terms of a function of n.

Suppose we want to enumerate carbocycles like benzene, where some H atoms have been replaced by OH groups.



Some counting: $\binom{6}{2} = 15$, $\binom{5}{1} = 5$ or, taking into account symmetry, 3.

Only the last answer makes chemical sense.

G. Pólya

Kombinatorische Anzahlbestimmungen für Gruppen, Graphen und chemische Verbindungen

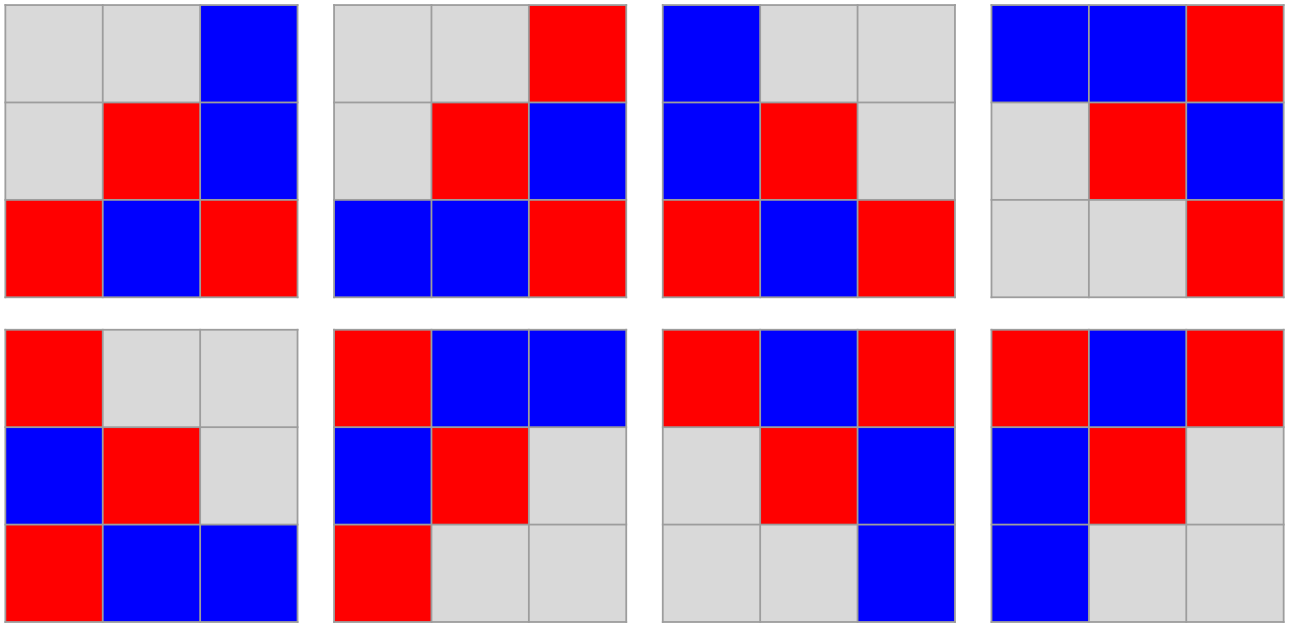
Acta Mathematica 68 (1937) 1: 145–254.

Actually, Pólya was scooped by J. H. Redfield in 1927, "The Theory of Group-Reduced Distributions."

How many different ways are there to place 3 crosses and 3 naughts on a (standard 3×3) Tic-Tac-Toe board?

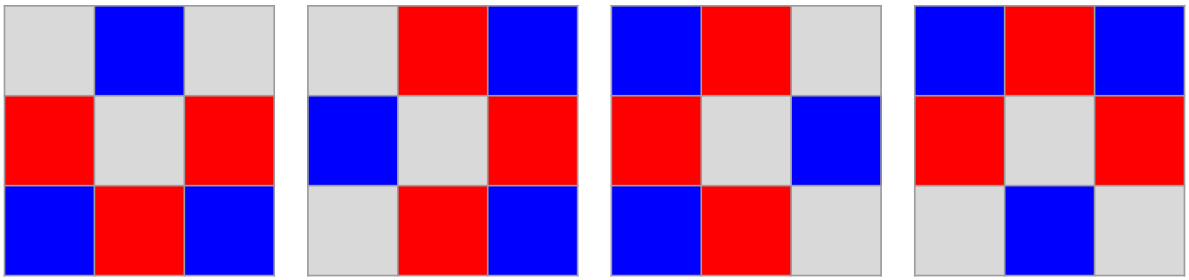
No problem: there are $\binom{9}{3,3,3} = 1680$ possible placements.

OK, but what if we identify boards that can be obtained from rotation, or looking through a mirror?



Clearly this involves the dihedral group D_4, and a single placement of marks can have as many as 8 variants.

So we should roughly expect $1680/8 = 210$ patterns.



But that is not quite right: some placements have less that 8 variants, so we are under-counting the number of patterns.

Here is a similar but somewhat less frivolous problem. Suppose we want to implement Boolean functions $f : \mathbb{B}^n \to \mathbb{B}$ as circuits.

There are 2^{2^n} such functions, but we don't need as many circuits. For example, we may have $f(x, y, z) = g(y, z, x)$ so it suffices to implement either f or g.

In general, we can permute the variables arbitrarily: two functions f and g are equivalent if

$$f(\boldsymbol{x}) = g(\pi(\boldsymbol{x}))$$

for some permutation π.

How many Boolean functions are there modulo input permutations?

Permuting the inputs is an obvious modification of a circuit, but there are other possibilities.

For example, it is straightforward to negate input bits and/or the output bit. Thus, there is another equivalence

$$f(\boldsymbol{x}) = g(\boldsymbol{x} \oplus \boldsymbol{c}) \oplus d$$

where $\boldsymbol{c} \in \mathbf{2}^n, d \in \mathbf{2}$ and $\oplus$ denotes exclusive or.

And, of course, we can combine permutations and negations.

So how many functions $\mathbb{B}^n \to \mathbb{B}$ are there in all these cases?

- Some Counting Problems

2. Actions

- Burnside's Lemma

- Some Applications

Observe that I write functions on the right and functional composition from left to right. This is undoubtedly the Wave of the Future. It makes functional diagrams easier to read and corresponds to the natural order of doing things on a pocket calculator.

This is from a 1976 paper "Some Applications of the Wreath Product Construction" by the category theorist Charles Wells. Obviously, Wells was the proud owner of an HP calculator.

Alas, he missed the boat on this one. By about a lightyear.

We will realize half of Wells' dream: composition is diagrammatic, but we chicken out and write function application on the left. Yes, I know . . .

Let's go back to the Tic-Tac-Toe problem from above: we want to count patterns, where two boards are equivalent if one can be moved to the other by rotations and/or reflections.

Clearly, we have to consider the interaction between Tic-Tac-Toe boards and the elements of the dihedral group D_4.

As we have seen, we can safely assume that the group in question is always a subgroup of a symmetric group, so we are dealing with a class of permutations (but see below for some twists).

What is needed is some glue that connects the permutations with the objects we are interested in (such as the boards, or carbocycles, or circuits, . . .)

We are dealing with

- a collection X of objects (configurations),
- a collection S of operations on the carrier set X.

A priori, X is just a flat set with no particular structure. We can think of S as a collection of atomic actions that can be performed on on X.

It is entirely natural to consider composite operations that are obtained by applying a whole sequence of operations from S. This can be modeled naturally by the free monoid $S^\star$, so we are dealing with monoid actions.

Proviso: This time we are interested in reversible operations. In this case, it is natural to consider the group generated by S rather than the monoid.

The main idea is that s^{-1} should undo the effect of s.

As before with monoids, 1 should have no effect whatsoever and things need to be compatible in the right way.

We already have seen these ideas in the context of semigroups and FSMs, but without reversibility. Here is an axiomatization for groups.

Definition

Let G be a group and X a set. A left action of G on X is a function φ such that

$$\varphi : G \times X \to X$$
$$\varphi(a * b, x) = \varphi(a, \varphi(b, x))$$
$$\varphi(1, x) = x$$

X is also called a G-set.

Notation:
It is customary to write $a \cdot x$ or even $a\,x$ instead of $\varphi(a, x)$. Hence

$$(a * b) \cdot x = a \cdot (b \cdot x)$$
$$1 \cdot x = x$$

This is much better notation, albeit slightly dangerous.

One can also think of having an endofunction $\widehat{a} : X \to X$ associated with every group element a such that

$$\widehat{1} = I$$
$$\widehat{ab} = \widehat{a}\,\widehat{b} \qquad \text{standard composition}$$

Definition

An action is faithful if $\widehat{a} = \widehat{b}$ implies $a = b$.

If an action fails to be faithful, consider the normal subgroup

$$H = \{\, a \in G \mid \widehat{a} = I \,\}$$

Then the quotient G/H acts faithfully in the natural manner.

Recall that $\mathfrak{S}(X)$ denotes the group of all permutations of X under composition.

Definition

A permutation group over X is a subgroup G of $\mathfrak{S}(X)$. The order of G is its cardinality and the degree of G is the cardinality of X.

By Cayley's Theorem every group G is isomorphic to a permutation group: we can think of the carrier set as being G. Note that in general the degree of G may be much smaller than the order of G, though.

Again: we use diagrammatic composition for $\mathfrak{S}(X)$.

An element of a permutation group can naturally be used to "rearrange" objects.

Consider a list of n objects:

$$\boldsymbol{x} = (x_1, x_2, \ldots, x_n)$$

We can use any permutation f in $\mathfrak{S}_n$ to rearrange the elements of $\boldsymbol{x}$:

$$\boldsymbol{x}' = (x_{f(1)}, x_{f(2)}, \ldots, x_{f(n)})$$

More generally, a permutation group of degree n can operate on n-vectors.

If we have some natural group G, say, some geometric group of rations and/or reflections, we can translate it into a permutation group.

We connect G to a symmetry group by a homomorphism $\Phi : G \to \mathfrak{S}(X)$. Particularly interesting to us is the case where Φ is a monomorphism, but the idea works in general.

Then

$$\varphi(a, x) = \Phi(a^{-1})(x)$$

is a left action of G on X, and all left actions arise in this way.

You may find the a^{-1} a bit peculiar and probably expected a plain a instead. The reason we need the inverse is that we want a left action and we use diagrammatic composition.

$$\begin{aligned}
\varphi(a * b, x) &= \Phi((a * b)^{-1})(x) \\
&= \Phi(b^{-1} * a^{-1})(x) \\
&= (\Phi(b^{-1}) \circ \Phi(a^{-1}))(x) \\
&= \Phi(a^{-1})\big(\Phi(b^{-1})(x)\big) \\
&= \varphi(a, \varphi(b, x))
\end{aligned}$$

Exercise

What if we had failed Wells and used the wrong definition of composition?

Consider a permutation group $G \subseteq \mathfrak{S}_n$ (of degree n and order at most $n!$).

One very useful space of objects here is

$$X = A^n$$

the set of n-vectors over A, an arbitrary set (later A will often have additional structure, but for the time being it's a naked set).

Claim

G acts on X on the left via

$$f \cdot \boldsymbol{x} = (x_{f(1)}, x_{f(2)}, \ldots, x_{f(n)})$$

It is clear that $1 \cdot \boldsymbol{x} = \boldsymbol{x}$.

Consider

$$(f \circ g) \cdot \boldsymbol{x} = \boldsymbol{y}$$

versus

$$f \cdot (g \cdot \boldsymbol{x}) = \boldsymbol{z}.$$

We need to show that $\boldsymbol{y} = \boldsymbol{z}$.

Recall that we compose functions from left to right, so that $\boldsymbol{y} = (x_{g(f(1))}, \ldots, x_{g(f(n))})$.

But then $\boldsymbol{z} = f \cdot (x_{g(1)}, \ldots, x_{g(n)}) = \boldsymbol{y}$.

□

Right?

Think carefully – this looks absolutely wrong, but it's right. Take a good look at the following.

Write $u_i = x_{g(i)}$.

$$\begin{aligned} g \cdot \boldsymbol{x} &= (x_{g(1)}, x_{g(2)}, \ldots, x_{g(n)}) \\ &= (u_1, u_2, \ldots, u_n) \end{aligned}$$

$$\begin{aligned} f \cdot \boldsymbol{u} &= (u_{f(1)}, u_{f(2)}, \ldots, u_{f(n)}) \\ &= (x_{g(f(1))}, x_{g(f(2))}, \ldots, x_{g(f(n))}) \end{aligned}$$

Exercise

Make sure you really understand the proof.
What would happen if we did composition the other way around?

As before with monoids: where there's a left, there must be a right ...

Definition

Let G be a group and X a set. A right action of G on X is a function φ such that

$$\begin{aligned}\varphi &: X \times G \to X \\ \varphi(x, a * b) &= \varphi(\varphi(x, a), b) \\ \varphi(x, 1) &= x\end{aligned}$$

Needless to say, this is often written $x \cdot a$ and $x\,a$.

To maintain a semblance of sanity, we always write a, b, c, ... for group elements and x, y, z, ... for the elements of X.

As before for left actions, we can use group homomorphisms $\Phi : G \to \mathfrak{S}(X)$ to obtain right actions.

This time we define

$$\varphi(x, a) = \Phi(a)(x)$$

to get a right action of G on X, and vice versa.

Recall that for a left action we had to use a^{-1}, now the definition is perhaps a bit more natural.

Exercise

Verify that this definition really produces a right action.

Again, here is our primary example of a group action: some permutation f from the symmetric group $\mathfrak{S}_n$ rearranging the elements of $\boldsymbol{x} = (x_1, x_2, \ldots, x_n)$.

Let $f(i) = j$.

type	intuitively	result
left	x_i is replaced by x_j	$(x_{f(1)}, \ldots, x_{f(n)})$
right	x_i moves to x_j	$(x_{f^{-1}(1)}, \ldots, x_{f^{-1}(n)})$

Having two versions to deal with might seem plain annoying, but there are occasions when left actions are more convenient to work with, and there are occasions when right actions are more convenient. Grin and bear it.

For group actions, we can interchange left and right in the following sense.

Proposition

Consider two maps $\varphi : G \times X \to X$ *and* $\psi : X \times G \to X$ *such that*

$$\psi(x, a) = \varphi(a^{-1}, x).$$

Then φ *is a left action if, and only if,* ψ *is a right action.*

Proof. Suppose φ is a left action.

$$\begin{aligned}
\psi(x, a * b) &= \varphi((a * b)^{-1}, x) \\
&= \varphi(b^{-1} * a^{-1}, x) \\
&= \varphi(b^{-1}, \varphi(a^{-1}, x)) \\
&= \psi(\psi(x, a), b)
\end{aligned}$$

The other direction is entirely similar. □

Another way to establish a connection between left and right actions is to reverse the multiplication. Given a group $\mathcal{G} = \langle G, \cdot \rangle$ define a new group

$$\mathcal{G}^{\mathsf{op}} = \langle G, * \rangle \qquad a * b = b \cdot a.$$

It is not hard to check that $\mathcal{G}^{\mathsf{op}}$ is in fact a group.

Now any left action φ over $\mathcal{G}$ translates into a right action ψ over $\mathcal{G}^{\mathsf{op}}$ by

$$\psi(x, a) = \varphi(a, x)$$

Exercise

Give a detailed proof of this claim.

From a sufficiently abstract perspective, left and right actions are the same: it doesn't matter much if we replace each group element by its inverse or change the order of multiplication. In fact, there are older texts that just speak about "a group acting on a set". The following is a classic, highly recommended.

N.G. de Bruijn

Pólya's Theory of Counting

E.F. Beckenbach (ed.): Applied Combinatorial Mathematics, Wiley (1964).

That's fine, but when it comes to actual implementation one has to be more careful, the code for both versions is different. More importantly, you must never mix the two versions within the same algorithm.

An action is

- transitive if $\forall\, x, y \,\exists\, a\, (ax = y)$.
- free if $\exists\, x\, (ax = bx)$ implies $a = b$.
- regular if it is transitive and free.

Free means that $ax = x$ implies $a = 1$; free implies faithful.

A standard example of a regular action is a group acting on itself.

Define three word maps $\alpha, \beta, \gamma : \mathbf{2}^\star \to \mathbf{2}^\star$ by $\alpha(\varepsilon) = \beta(\varepsilon) = \gamma(\varepsilon) = \varepsilon$ and

$$\begin{aligned}
\alpha(0x) &= 1\,\gamma(x) \\
\alpha(1x) &= 0\,\beta(x) \\
\beta(sx) &= s\,\alpha(x) \\
\gamma(sx) &= s\,\beta(x)
\end{aligned}$$

Claim

The maps α, β and γ are bijections.

Hence we can define an action of F_3, the free group of rank 3, on $\mathbf{2}^\star$.

Alas, this action is not faithful: the word maps commute and there is another somewhat unexptected identity:

$$\alpha^2\beta^2\gamma = I$$

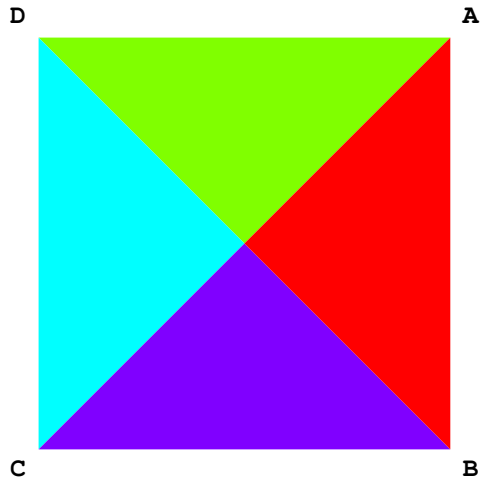
Hence we get a faithful action of $\mathbb{Z}^3$ on $\mathbf{2}^\star$:

$$(a, b, c)x = \alpha^a\beta^b\gamma^c(x)$$

Exercise

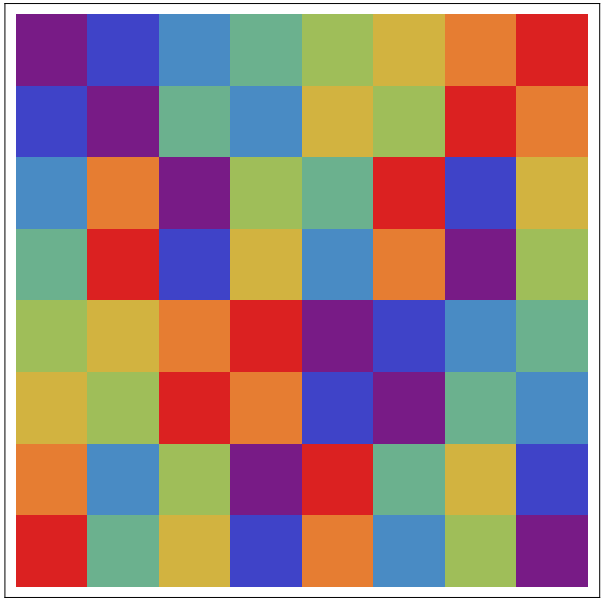
Prove all these claims.

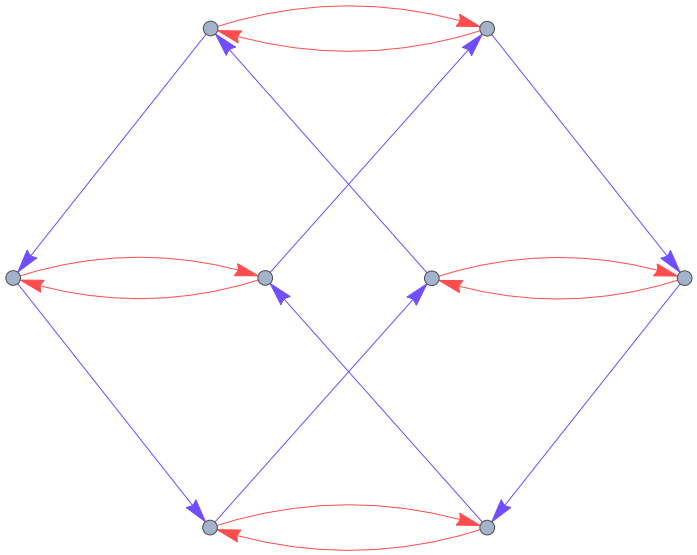
Let's come back to the dihedral group D_4 which we can think of as the symmetries of a square.



Abstractly, D_4 has the presentation

$$\langle \alpha, \beta \mid \alpha^4 = 1, \beta^2 = 1, \alpha\beta = \beta\alpha^3 \rangle$$





The Cayley table and Cayley graph for D_4.

The natural degree of D_4 is 4, and we can identify this group with a subgroup G of $\mathfrak{S}_4$ (the permutations that preserve adjacency):

$$G = \{\, T(1,2,3,4), T(2,3,4,1), T(3,4,1,2), T(4,1,2,3),$$
$$T(2,1,4,3), T(1,4,3,2), T(4,3,2,1), T(3,2,1,4) \,\}$$

It is this subgroup G that induces a regular action on the square.

For simplicity, one might express this by casually omitting G and saying something like "D_4 acts on the square."

We can now formally describe patterns by having the whole group act on an element in X.

Definition

Let $\varphi : G \times X \to X$ be a left action. The orbit of $x \in X$ under G is defined to be

$$G\,x := \{\, a\,x \mid a \in G \,\}.$$

One says that the elements in an orbit are G-equivalent.

So a pattern is simply an orbit under G.

Note that our venerable old notion of orbit obtained by iterating an endofunction $f : A \to A$ is entirely analogous: it's just the special case where we have the additive monoid $\mathbb{N}$ rather than a group.

Proposition

Let G be a group. Then the orbits $G\,x$ form a partition of X.

Proof. $z \in G\,x \cap G\,y$ implies $a\,x = z = b\,y$ for some $a, b \in G$. But G is a group, so $x = (a^{-1}b)\,y \in G\,y$. □

So, our terminology makes sense: the blocks of this partition are exactly the patterns we are interested in.

Note, though, that we really need G to be a group, the argument fails for monoids. Over a monoid, all we have is a basin of attraction.

- Some Counting Problems
- Actions

3. Burnside's Lemma

- Some Applications

Now comes the important idea: using subgroups and fixed points to count. Let $\varphi : G \times X \to X$ be a left group action.

Definition

The stabilizer of G at $x \in X$ is

$$G_x := \{\, a \in G \mid a\,x = x \,\}$$

The invariant subset of X at $a \in G$ is

$$X_a := \{\, x \in X \mid a\,x = x \,\}$$

So both definitions involve fixed points of the action, once from the perspective of the group, and once from the perspective of the G-set.

The idea is this: we want to determine the size of the orbit Gx.

A trivial upper bound is $|G|$, but usually this bound is not tight. The problem is that we may well have $ax = bx$ for $a \neq b$. But then

$$a\,x = b\,x \iff a^{-1}b\,x = x \iff a^{-1}b \in G_x \iff b \in aG_x$$

Note that the algebraic manipulations are all justified by the definition of action.

Exercise

Check that this is really true.

Proposition

The stabilizers G_x are subgroups of G.

Proof.

Let $a, b \in G_x$.

Then

$$(a^{-1}b)\,x = a^{-1}\,(b\,x) = a^{-1}\,(x) = a^{-1}\,(a\,x) = x$$

Hence $a^{-1}b \in G_x$ and we are done. □

Proposition

The index $[G : G_x]$ is the size of the orbit of x.

Proof. As already pointed out

$$a\,x = b\,x \iff b \in aG_x$$

Hence $|G_x|$ many elements in G produce the same element in the orbit.
So $|Gx| = [G : G_x]$. □

Recall that by Lagrange's theorem, $[G : H] = |G|/|H|$ is integral for finite groups.

So we can write the partition of G into blocks as

$$G/G_x = \{g_1 G_x, g_2 G_x, \ldots, g_r G_x\}$$

where $r = [G : G_x]$ then the orbit has the form

$$G\,x = \{g_1\,x, g_2\,x, \ldots, g_r\,x\}$$

Hence, if we know representatives for the cosets, then we can enumerate the orbit of x directly without repetitions.

The bad news: We can always choose $g_1 = 1$, but other than that it may not be so easy to get at the g_i (the problem of finding a complete set of representatives).

Double counting is a very simple but sometimes surprisingly powerful idea.

Suppose R (for rows) and C (for columns) are two finite sets and M is an R by C matrix with 0/1 entries.

Let row(r) be the number of 1's in row $r \in R$, and let col(c) be the number of 1's in columns $c \in C$.

Then

$$\sum_{r \in R} \text{row}(r) = \sum_{c \in C} \text{col}(c).$$

Yes, yes, that's trivial. But ...

Lemma

$$\sum_{a \in G} |X_a| = \sum_{x \in X} |G_x|.$$

Proof.

Consider the action matrix: a G by X matrix M defined by

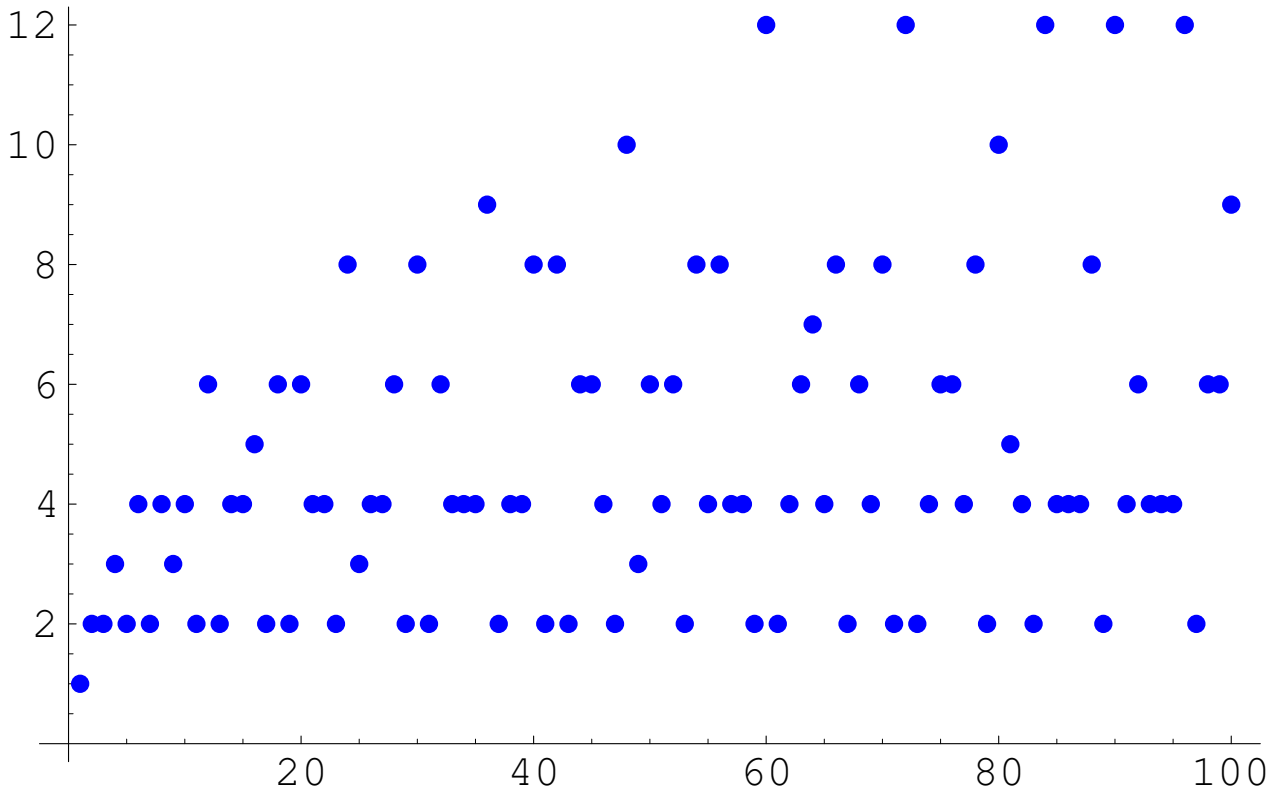
$$M(a, x) = \begin{cases} 1 & \text{if } a\,x = x, \\ 0 & \text{otherwise.} \end{cases}$$

The rows are bitvectors for the invariant sets, and the columns are bitvectors for the stabilizers.

□

For a positive integer n let $d(n)$ be the number of divisors of n.

$d(n)$ is fairly complicated.

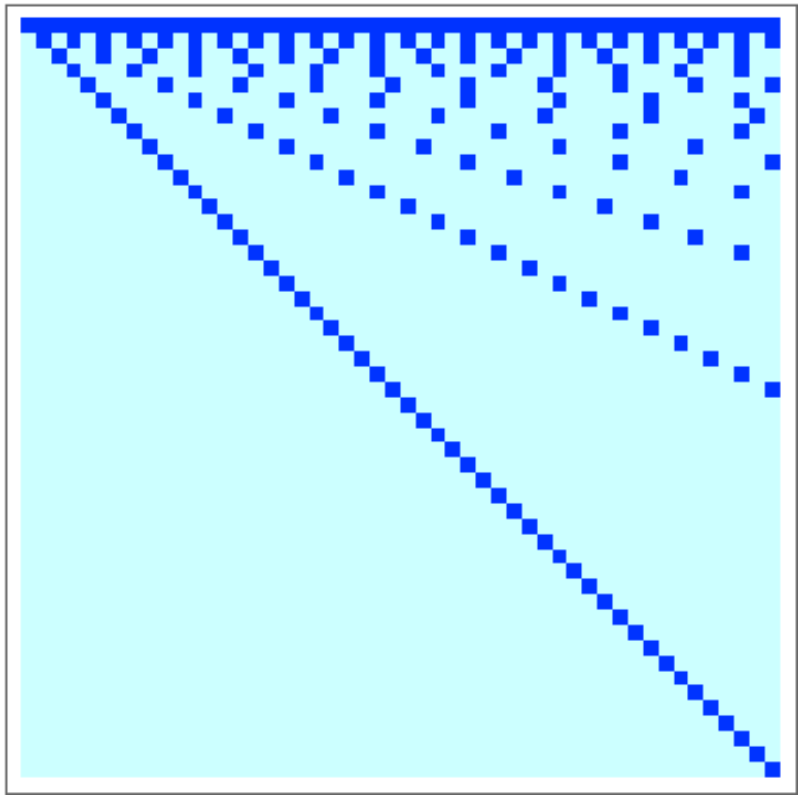


How about the average

$$\widehat{d}(n) := 1/n \sum_{x \leq n} d(x).$$

Just as hopeless? Even more hopeless?

Let M be the n by n binary matrix with 1 in position (x, y) iff x divides y.



The number of 1's in column y is just $d(y)$, and difficult.

But the number of 1's in row x is simply $\lfloor n/x \rfloor$.

So the total number of 1's is

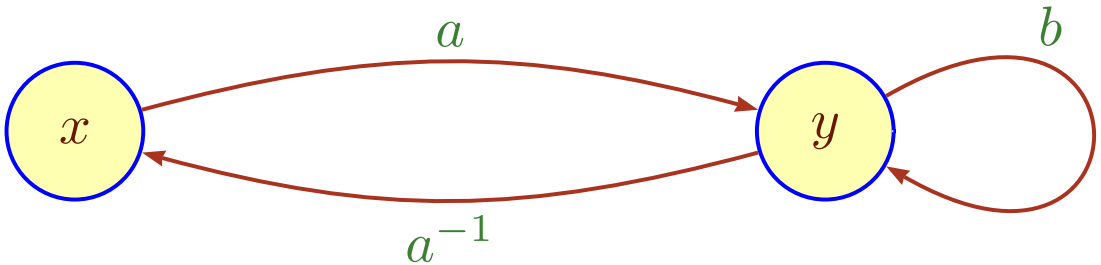
$$\sum_{x \le n} \mathsf{row}(x) = \sum_{x \le n} \lfloor n/x \rfloor \le \sum_{x \le n} n/x = n \cdot H_n.$$

and the error is at most n.

Hence $\widehat{d}(n)$ is about $\log n$.

What is the relationship between the stabilizers of elements of the same orbit?

Say, $a\,x = y$. Then $b\,y = y$ iff $a^{-1}ba\,x = x$.



Thus, G_x and G_y are conjugate subgroups: $G_y = a\,G_x\,a^{-1}$.

In particular if the group G is commutative, all the stabilizers along a single orbit are the same.

Theorem

Let N be the number of distinct orbits of G acting on X. Then

$$N = \frac{1}{|G|} \sum_{a \in G} |X_a|.$$

Proof.

$$\frac{1}{|G|} \sum_{a \in G} |X_a| = \frac{1}{|G|} \sum_{x \in X} |G_x| = \sum_{x \in X} \frac{1}{[G : G_x]} = \sum_{x \in X} \frac{1}{|G\,x|} = N.$$

□

So the number of orbits is the average of the number of fixed points.

Burnside published this lemma in 1900.

Unfortunately, Frobenius already published the same result in 1887: *Über die Congruenz nach einem aus zwei endlichen Gruppen gebildeten Doppelmodul.*

And Frobenius was scooped by Cauchy in 1835: *Mémoire sur diverses propriétés remarquables des substitutions régulières ou irrégulières, et des systémes de substitutiones conjugées.*

Note how papers used to have long, descriptive names.

And, a searchable web really is a blessing (of course, this assumes proper semantic markup, currently a pipedream).

In practice, this means that one has to

- Determine the group of actions G.
- Compute the (sizes of the) invariant sets X_a for all group elements a.

Usually G is clear from the given atomic actions, but sometimes even this step requires a bit of work.

Counting fixed points can be problematic when the group is large, or when the action is very complicated. In the 21st century, one can use computer algebra to take care of the more painful computations.

- Some Counting Problems
- Actions
- Burnside's Lemma

4. Some Applications

Here is a trivial counting problem, but it provides on opportunity to use the new machinery.

We consider binary lists of length n.

We want to identify two lists when one is obtained from the other by flipping all bits.

To apply Burnside let

$$X = \mathbf{2}^n$$
$$G = \{1, s\}$$

where s means flip all bits. Hence $s^2 = 1$ and G really is a group.

In fact, G is isomorphic to $\mathbb{Z}_2$ but let's use the multiplicative notation.

We need to calculate the invariant sets, which is easy in this case.

$$X_1 = X$$
$$X_s = \emptyset$$

Hence

$$N = \frac{1}{2}(2^n + 0) = 2^{n-1}$$

So each orbit has the form $\{x, s\,x\}$ and has size 2.

Not very exciting, but at least it's correct.

In the context of cellular automata one encounters the following problem: we have binary lists of length $n = 2^k$ encoding the local functions.

Two lists L and K are equivalent if K can be obtained from L by any combination of reversing the list, or flipping all bits.

To apply Burnside let

$$X = \mathbf{2}^n$$
$$G = \left\langle r, s \;\middle|\; r^2 = s^2 = 1, rs = sr \right\rangle = \{1, r, s, rs\}$$

where r means reversal, s means flip all bits. Note that G is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$, the Kleinsche Vierergruppe.

Since n is even we have

$$X_1 = X$$

$$X_r = \{\, uu^{\mathsf{op}} \mid u \in \mathbf{2}^{n/2} \,\}$$

$$X_s = \emptyset$$

$$X_{rs} = \{\, u\,\overline{u}^{\mathsf{op}} \mid u \in \mathbf{2}^{n/2} \,\}$$

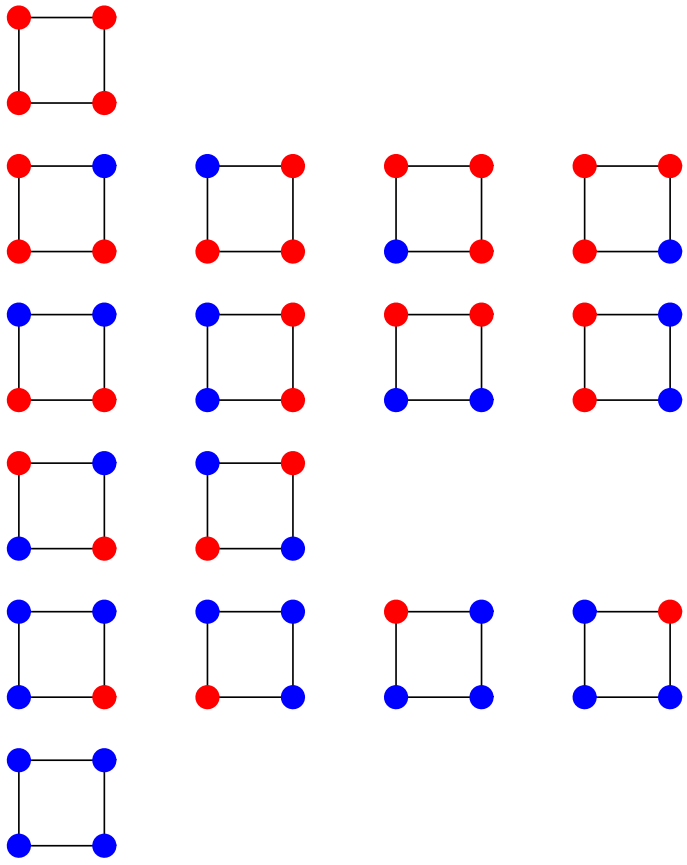
Hence

$$N = \frac{1}{4}(2^n + 2^{n/2} + 0 + 2^{n/2}) = 2^{n-2} + 2^{n/2-1}$$

Color the corners of a square red and blue. Obviously there are 2^4 colorings (our configurations).

Now suppose we do not wish to distinguish between colorings that can be obtained from each other by rotations and reflections (our patterns).

For 2 colors and 4 vertices we can easily compute this to death, but think about the analogous problem with c colors and n vertices.



So there are 6 patterns.

Let X be the set of all colorings. It is convenient to think of X as $\mathbf{2}^4$ (read off the colors in clockwise order).

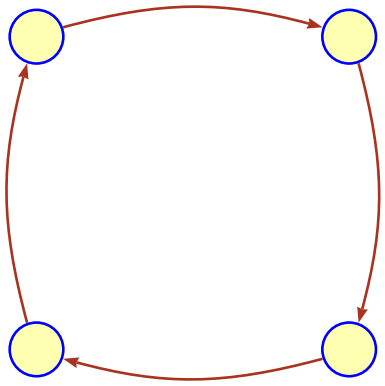
The patterns are exactly the orbits of $x \in X$ under D_4.

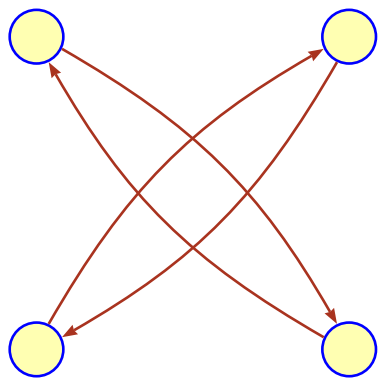
Hence

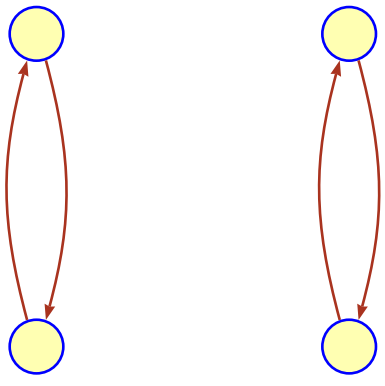
$$N = \frac{1}{8} \sum_{a \in D_4} |X_a|.$$

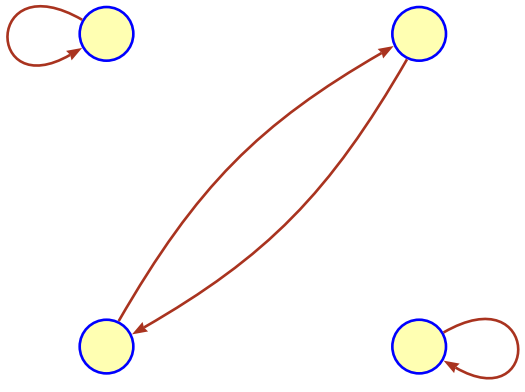
So what are the invariant sets?

Recall $D_4 = \{1, \alpha, \alpha^2, \alpha^3, \beta, \alpha\beta, \alpha^2\beta, \alpha^3\beta\}$







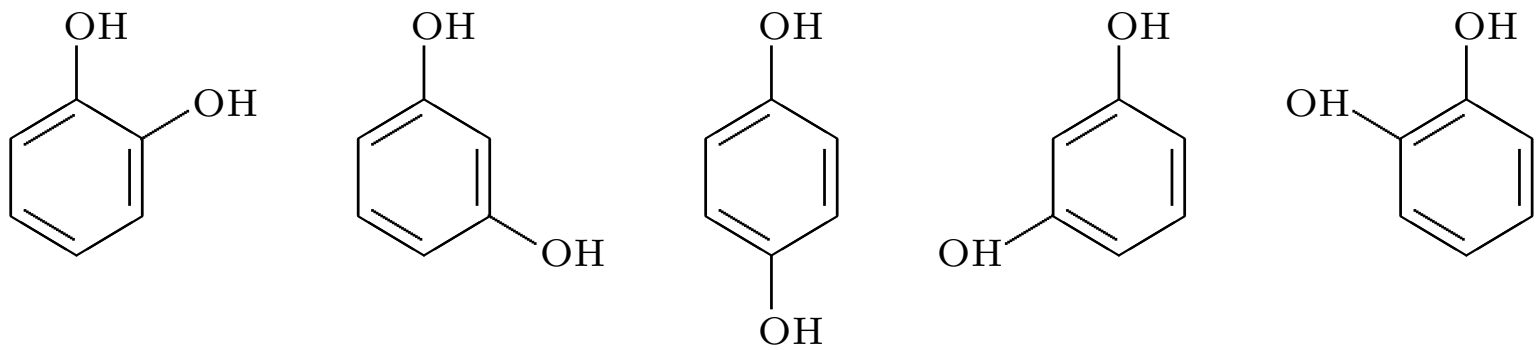


$$
\begin{aligned}
X_1 &= X \\
X_\alpha &= X_{\alpha^3} = \{0000, 1111\} \\
X_{\alpha^2} &= \{0000, 0101, 1010, 1111\} \\
X_\beta &= \{0000, 0011, 1100, 1111\} \\
X_{\alpha\beta} &= \{\, ijik \mid i, j, k \in \mathbf{2} \,\} \\
X_{\alpha^2\beta} &= \{0000, 0101, 1010, 1111\} \\
X_{\alpha^3\beta} &= \{\, jiki \mid i, j, k \in \mathbf{2} \,\}
\end{aligned}
$$

Hence

$$N = \frac{1}{8}(16 + 2 + 4 + 2 + 4 + 8 + 4 + 8) = 6$$

Let's return to the historical root: counting chemical compounds. For example, suppose we want to enumerate carbocycles like benzene, where 2 H atoms have been replaced by OH groups.



Clearly we can model this again using something like a dihedral group.

A k-ary bracelet is a circular string of beads in k different colors: do not distinguish between variants obtained by rotation or reflection.

It is customary to represent each equivalence class by its lexicographically first element.

Example: all 21 ternary bracelets of length 4.

$$
\begin{array}{llll}
(1,1,1,1) & (1,1,1,2) & (1,1,1,3) & (1,1,2,2) \\
(1,1,2,3) & (1,1,3,3) & (1,2,1,2) & (1,2,1,3) \\
(1,2,2,2) & (1,2,2,3) & (1,2,3,2) & (1,2,3,3) \\
(1,3,1,3) & (1,3,2,3) & (1,3,3,3) & (2,2,2,2) \\
(2,2,2,3) & (2,2,3,3) & (2,3,2,3) & (2,3,3,3) \\
(3,3,3,3) & & &
\end{array}
$$

To apply Burnside note that the group acting on X is the same as for a regular n-gon, so we can use

$$X = [k]^n$$
$$G = D_n$$

What are the invariant sets?

We need the cardinality of

$$X_{\alpha^p} = \{\, x \in X \mid \alpha^p\, x = x \,\}$$
$$X_{\alpha^p \beta} = \{\, x \in X \mid \alpha^p \beta\, x = x \,\}$$

For the rotations this means $x_0 = x_p = x_{2p} = \ldots$ and things wrap around modulo n.

Remember the function

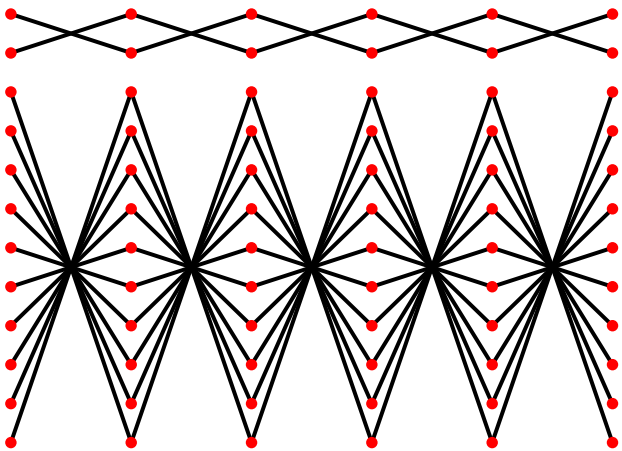
$$\begin{array}{rccc} f_p: & \mathbb{Z}_n & \longrightarrow & \mathbb{Z}_n \\ & z & \longmapsto & z + p \bmod n \end{array}$$

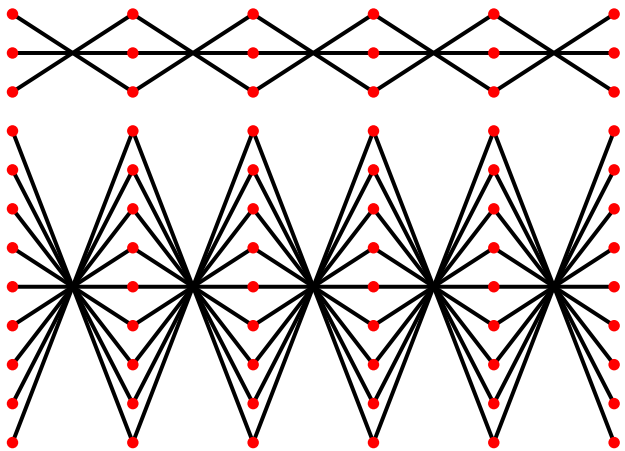
f_p has $\gcd(n,p)$ distinct orbits, each of length $n/\gcd(n,p)$.

$\alpha^p\, x = x$ means that the list elements on each orbit of f_p are the same.

Hence there are $k^{\gcd(n,p)}$ invariant lists for the rotation α^p.

How about the reflections $\alpha^k\beta$? A few pictures help a lot in this case.





The pictures are for $n = 12$ and $k = 2, 3$.

It looks like there 2-cyles and possibly fixed points, nothing else.

Remember that the motions in D_n are either rotations or reflections with respect to a properly chosen axis, nothing else can happen.

As a consequence, for even n, there are either $n/2$ many 2-cyles or $(n/2-1)$ many 2-cycles and two fixed points: depending on whether the axis of the reflection passes through vertices or the center of the sides of the n-gon.

For odd n, there are always $(n-1)/2$ many 2-cyles plus one fixed point: the reflection axis always has to pass through a vertex and the center of one side.

Exercise

Draw pictures to confirm these assertions.

For simplicity, assume n is odd. Then the number of k-ary necklaces of length n is

$$\frac{1}{2n}\left(\sum_{p<n}|X_{\alpha^p}|+\sum_{p<n}|X_{\alpha^p\beta}|\right)=$$

$$\frac{1}{2n}\left(\sum_{p<n}k^{\gcd(n,p)}+\sum_{p<n}k^{(n+1)/2}\right)=$$

$$\frac{1}{2n}\sum_{d|n}\varphi(n/d)\,k^d+k^{(n+1)/2}/2$$

where φ is Euler's totient function: $\varphi(m)=|\mathbb{Z}_m^*|$.

For even n the counting result is very similar.

$$\frac{1}{2n}\sum_{d|n}\varphi(n/d)\,k^d + (k+1)k^{(n+1)/2}/4$$

Not too pretty, but no nice simple closed form is known. Enough, though, to compute some values. $k = 2, \ldots, 6$ and $n = 1, \ldots, 8$:

2	3	4	6	8	13	18	30
3	6	10	21	39	92	198	498
4	10	20	55	136	430	1300	4435
5	15	35	120	377	1505	5895	25395
6	21	56	231	888	4291	20646	107331

For our original problem, there are 13 possible molecules obtained from substituting some H atoms by OH groups.

Let's check.

$$
\begin{array}{lll}
(1,1,1,1,1,1) & & \\
(1,1,1,1,1,2) & & \\
(1,1,1,1,2,2) & (1,1,1,2,1,2) & (1,1,2,1,1,2) \\
(1,1,1,2,2,2) & (1,1,2,1,2,2) & (1,2,1,2,1,2) \\
(1,1,2,2,2,2) & (1,2,1,2,2,2) & (1,2,2,1,2,2) \\
(1,2,2,2,2,2) & & \\
(2,2,2,2,2,2) & &
\end{array}
$$

Can we answer the old Tic-Tac-Toe question at this point? We need to count the number of patterns of type $(3, 3, 3)$.

So we have

- configuration space X consisting of all $(3, 3, 3)$ placements,
- dihedral group D_4 acting on X.

More formally, $X \subseteq \{0, 1, 2\}^{3,3}$ is determined by the condition that the number of 0's, 1's and 2's in a matrix is exactly 3 each.

Warning: We need to deal with a subgroup of $\mathfrak{S}_9$ that is isomorphic to D_4: the board has 9 squares. We need to boost D_4 to a group of degree 9.

Let us number the squares in row-major order:

1	2	3
4	5	6
7	8	9

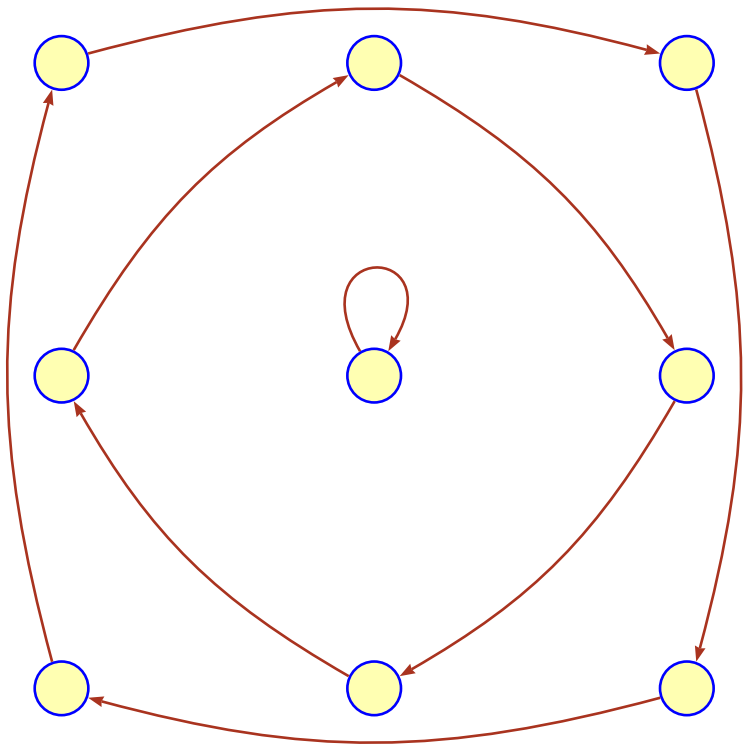
Then clockwise rotation and reflection along the horizontal axis correspond to

$$((1,3,9,7),(2,6,8,4))$$
$$((1,7),(2,8),(3,9))$$

They duly generate a subgroup of $\mathfrak{S}_9$ isomorphic to D_4.

Next we need to determine the cardinalities of the invariant sets X_a for all 8 group elements.

For rotations other than the identity all invariant sets are empty. We only consider rotation by 90 degrees, the other cases are entirely similar.



To see that $X_\alpha = \emptyset$ note that since we only have 3 marks of each kind no 4-cycle can be invariant.

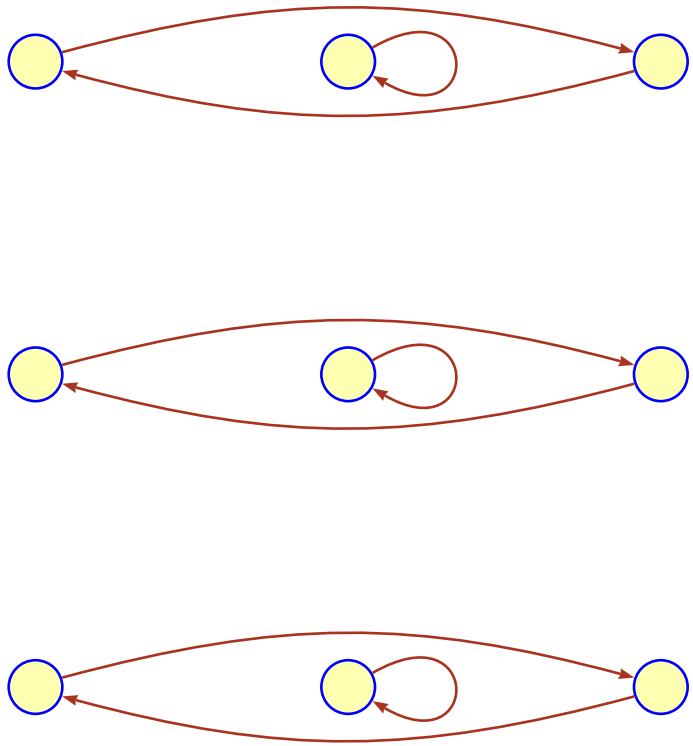
Note that this argument is a bit frail: if we were to look at different kinds of configurations we would need to start all over again – more on this later.

Exercise

Carry out the same argument for the invariant subset associated with rotation α^2.

Also argue that $X_{\alpha^2} = \emptyset$ *implies that* $X_\alpha = \emptyset$.

For reflections things are more interesting. We only consider reflection along the vertical axis, the other cases are entirely similar: the invariant set has size $6 \times 6 = 36$.



Hence the number of Tic-Tac-Toe configurations with 3 crosses and 3 naughts is

$$1/8\,(1680 + 36 + 36 + 36 + 36) = 228$$

Not bad, but as already mentioned, this method becomes tedious if we ask about other types of boards. E.g., we have no idea how many patterns there are for 2 crosses and 2 naughts. It would be nice to have a global tool to handle all possible cases.

Exercise

Determine the largest invariant set (other than X_1 of course) for all possible configurations.