19 The chessboard challenge

There is a famous trick used by computer scientists to illustrate the power of binary notation to encode data, but as we will see here you can view it through the lens of group theory.

You can find a nice account of this online at https://datagenetics.com/blog/december12014/index.html

A mathemagician and their apprentice set up an ordinary chessboard on the stage with a sack of 64 identical silver coins next to the board. A volunteer from the audience is selected and they are asked to blindfold the magician and then to place the 64 coins on the board as they please, choosing heads or tails in each square. They can do this at random or using any rule they want, but the mathemagician must not know how this has been done and must not be able to see the board.

Having covered the board in coins the volunteer chooses one of the chess squares and writes it down in the standard notation, showing it to the apprentice before sealing it in an envelope and returning to their seat, without revealing the choice to the mathemagician.

The apprentice is then allowed to choose and flip exactly one of the coins on the board from head to tail or tail to head. They have a free choice but must not tell the mathemagician which coin has been flipped.

Figure 19.1: Laying out the coins on the board

The mathemagician then removes their blindfold, inspects the board and immediately writes down a square on a board. The audience member opens their envelope and shows everyone that the mathemagician has correctly identified the chosen square.

At first the trick seems impossible. The apprentice can flip only one coin in a random sea of them and as the mathemagician removes their blindfold they are apparently presented with a random array of coins. Since they do not know what the layout of the coins was before the flip, there does not appear to be enough information for them to conclude anything, but of course this is itself an illusion.

The random layout of heads and tails can be regarded as an element of the abelian group $\mathbb{Z}_2^{64}$, where the 64 direct factors correspond to the squares on the board and heads and tails correspond to $0, 1$ respectively. There are 2^{64} elements in the group and 2^{64} possible layouts of the coins.

On the other hand the 64 squares of the board correspond to the group $\mathbb{Z}_2^6$ which we can also think of as $(\mathbb{Z}_2^3) \times (\mathbb{Z}_2^3)$, identifying the pairs (a, b) in this direct product decomposition with the chess board coordinates.

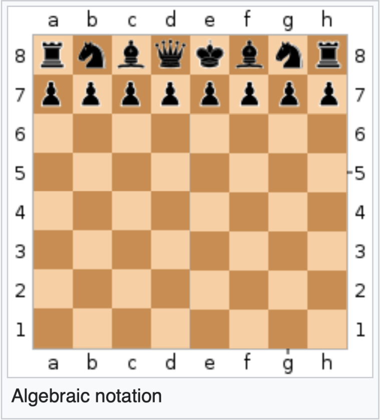

Figure 19.2: The coordinates on the chess board

The group $\mathbb{Z}_2^{64}$ is much larger than the group $\mathbb{Z}_2^6$. In fact it is 2^{58} times as big, i.e., a factor of over $2 * 10^{17}$ larger, and it is this fact that gives us the wiggle room to solve the puzzle of how the trick works. The large number of coin configurations means that each square of the board can be associated with a large number of configurations making it at least plausible that the apprentice could convert a random configuration into one denoting the chosen square by making a minimal change to the layout.

To formalise this and to understand how the trick works we use our notions of homomorphism and generators. We start by writing down 64 elements of the group $\mathbb{Z}_2^{64} = \mathbb{Z}_2 \times \mathbb{Z}_2 \times ... \times \mathbb{Z}_2$ which, together, generate it. These elements are of the form $g_i = (0, \ldots, 0, 1, 0, \ldots, 0)$, where the 1 appears in the i-th coordinatee.

We will show that there is a surjective homomorphism ϕ from the group $\mathbb{Z}_2^{64}$ to the group $\mathbb{Z}_2^6$ which has the property that for any two elements $\phi(h), \phi(k)$ in the image we can find one of the elements g_i such that $\phi(g_i + h) = \phi(k)$.

Think what this means in terms of the trick. The homomorphism associate a unique square on the chessboard to each configuration of coins, so providing that the mathemagician and the apprentice both know the formula for the homomorphism the apprentice can communicate the chosen square by ensuring that their master sees a configuration corresponding to that square when they remove the blindfold. In other words, the apprentice must make a change to the layout so that the resulting element k of the group $\mathbb{Z}_2^{64}$ maps to the element of $\mathbb{Z}_2^6$ corresponding to the selected position.

The constraint on the apprentice is that the audience member has, at random, selected an element h of the group $\mathbb{Z}_2^{64}$ by laying out the coins on the board, and the apprentice can only adjust this by flipping one of the coordinates, either from 0 to 1, or from 1 to 0. But this move corresponds to adding one of the generators g_i and we know that our homomorphism has the property that they can select some generator g_i such that $\phi(h + g_i) = \phi(k)$ which represents the chosen square.

It remains for the two entertainers to choose a homomorphism $\phi : \mathbb{Z}_2^{64} \to \mathbb{Z}_2^6$ with the required properties. Ideally this homomorphism will be easy to remember or work with so that the trick proceeds smoothly and quickly.

Recall that they need the property: for any two elements $\phi(h), \phi(k)$ there is a generator $g_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ such that $\phi(g_i + h) = \phi(k)$.

By the homomorphism law this is the same as saying that $\phi(g_i) + \phi(h) = \phi(k)$.

We now propose a recipe for the homomorphism. Since we have 64 chess board squares and 64 special elements $g_i \in \mathbb{Z}_2^{64}$ we can choose a matching between them. But the squares on the chess board are also matched with the elements of $\mathbb{Z}_2^3 \times \mathbb{Z}_2^3$, thought of as chess board coordinates. So we just define $\phi(g_i)$ to respect the two matchings.

To define ϕ on an arbitrary element $g \in \mathbb{Z}_2^{64}$ we note that any element of this group can be written uniquely as a sum of the generators. The generators required are just those corresponding to the coordinates of g which take the value 1. We then set $\phi(g)$ to be the sum of those terms $\phi(g_i)$. This is well defined, and it is easy to check that it satisfies the homomorphism law.

Having agreed this recipe the mathemagical team are ready to perform. Once the audience member has laid out the coins the apprentice immediately computes the element of $h \in \mathbb{Z}_2^{64}$ corresponding to the array and applies the homomorphism to check which element $\overline{h} := \phi(h) \in \mathbb{Z}_2^6$ this corresponds to. When the volunteer has selected a square the apprentice notes that element $\mathbb{Z}_2^6$ as well and we will denote it as $\overline{k}$. Since ϕ is surjective, this corresponds to an element $k \in \mathbb{Z}_2^{64}$ such that $\overline{k} = \phi(k)$. The apprentice then computes the difference $\overline{k} - \overline{h} \in \mathbb{Z}_2^6$ and finds the generator $g_i \in \mathbb{Z}_2^{64}$ such that $\phi(g_i) = \overline{k} - \overline{h}$. The element $\phi(g_i)$ tells them which square to flip:

$$\overline{h} + \phi(g_i) = \overline{h} + (\overline{k} - \overline{h}) = \overline{k}.$$

Removing the blindfold the mathemagician sees an array corresponding to the element $k \in \mathbb{Z}_2^{64}$. They apply the homomorphism to read off the element $\overline{k} \in \mathbb{Z}_2^6$ and announce the corresponding square on the board. The trick is complete, the audience go wild. Another win for mathematics.

The trick is even easier to pull off than this description sounds and if you would like to look further into this puzzle there is a really nice account by Oliver Nash which explores some alternative mathematical points of view on the solution. You can find it at http://olivernash.org/2009/10/31/yet-another-prisoner-puzzle/index.html. The purpose of the description above is to emphasise the fact that the solution depends crucially on two key ideas in group theory: the notions of generators and homomorphisms.