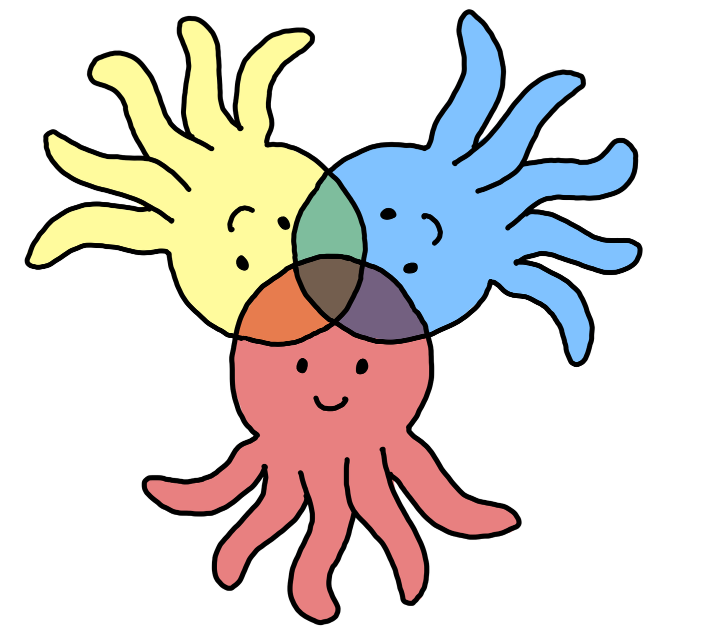
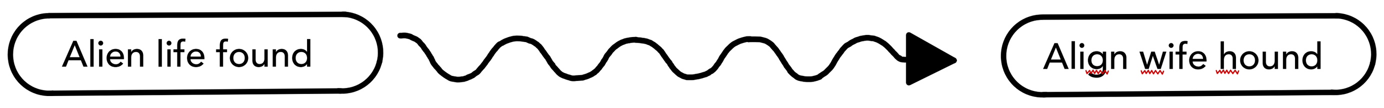
Veronica Kelsey
veronica.kelsey@manchester.ac.uk
Joint work with P.J. Rowley

Octad Triples



1 Problem

Sending messages through a noisy channel, for example in deep space communication, can result in errors



To communicate effectively through these noisy channels we need to model the noise and understand the errors that can occur

Prof Nigel Boston and his PhD student needed an answer to the following question as part of their study of noisy channels

Question

"I'm investigating the Golay Code. Is there a nice way to describe the orbits of Octads triples under the automorphism group?"

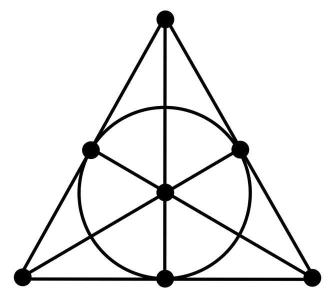
See §4 — See §2 — See §3

2 Octads

To define octads we first need to introduce Steiner systems. These are best exhibited through the following example

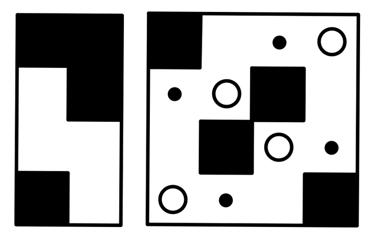
The Steiner system S(2,3,7) has
- 7 points
- lines that contain 3 points
- the magic property that any 2 points lie on a unique line

There are 7 lines which can be represented in the Fano pane


The Fano plane

The Steiner system S(5,8,24) has
- 24 points
- octads that contain 8 points
- the magic property that any 5 points lie in a unique octad

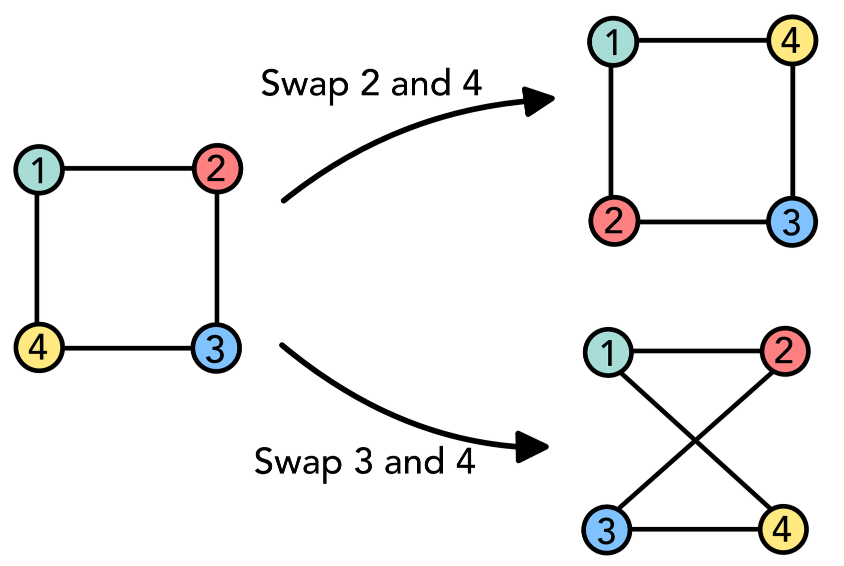
There are 759 Octads, which are all represented in the MOG (Miracle Octad Generator).


A section of the MOG

Fun fact - There exist Steiner systems S(t,k,n) with t > 6 but we don't know a single example of one!

3 Automorphisms

An automorphism is a map from an object to itself which preserves the object's structure



This map is an automorphism because our object is still a square :)

This map isn't an automorphism because our object is no longer a square :(

Were interested in the following automorphism group

$$\text{Aut}(\,S(5,8,24)\,) = M_{24}$$

The set of all maps on the 24 points which preserve the set of Octads = The Mathieu group M_{24} is a sporadic simple groups. These are the building blocks of all finite groups. It was the first of its type to be discovered and has many fascinating properties

4 Golay Code

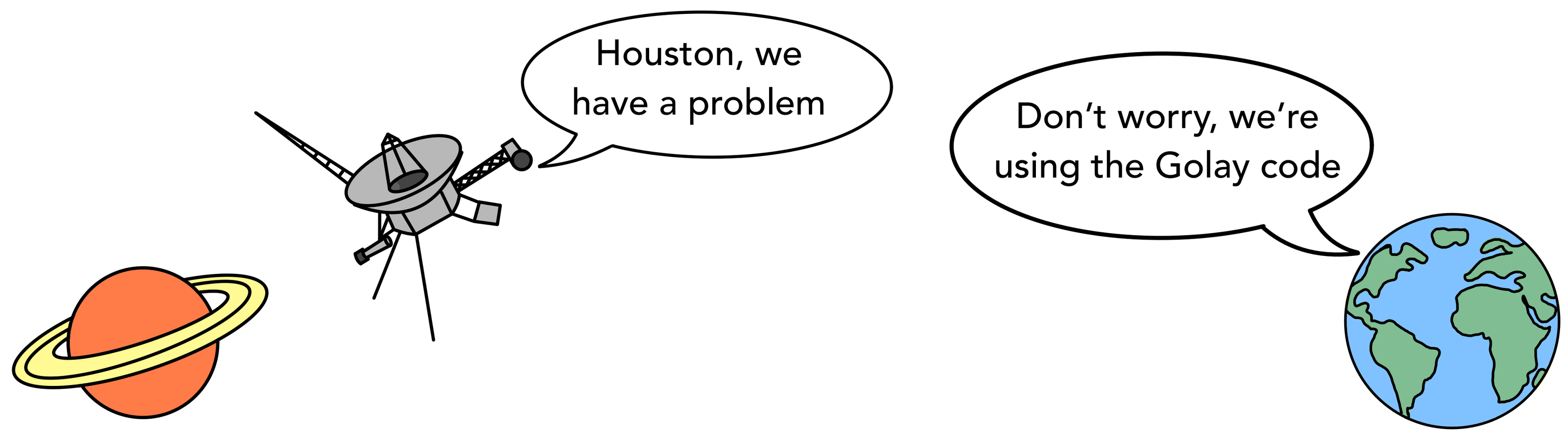
The Golay code was described as "the best single published page" in coding theory

The Golay code is perfect, meaning it is as efficient as possible. It can correct an optimal number of errors. Errors naturally occur during the transmission of messages and so being able to spot errors and correct them without needing the message to be resent is very useful

The Golay code was used by NASA in the Voyager 1 and 2 missions to Jupiter and Saturn

The codewords of the extended binary code can be built from the octads. Take subsets S of the 24 points of S(5,8,24) that are octads or the symmetric difference of octads. The corresponding codeword is the vector

$$\underline{c} = (c_1, c_2, \ldots, c_{24}) \text{ where } c_i = 1 \text{ if } i \in S \text{ and } c_i = 0 \text{ otherwise}$$

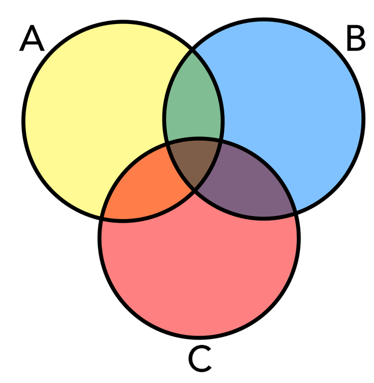


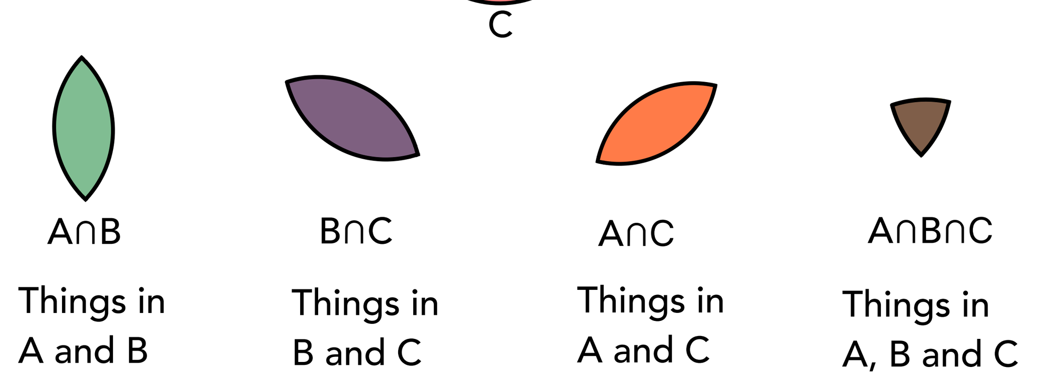
5 Solution

Notation

For a set A, we use |A| to denote the size of (number of elements in) the set

For sets A,B,C the following illustrates the intersection between them





Theorem

We were able to answer Prof Boston's question. The answer was a surprisingly elegant one.

We have since published this theorem as part of a peer reviewed paper in the Springer journal of Graphs and Cominatorics

Springer

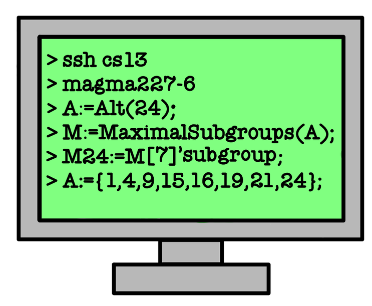
Answer

Theorem - Let { A, B, C } and { X, Y, Z } be two sets of three octads. They are in the same orbit under M_{24} if and only if

$$\{\, |A\cap B|, |A\cap C|, |B\cap C|, |A\cap B\cap C| \,\}$$
$$= \{\, |X\cap Y|, |X\cap Z|, |Y\cap Z|, |X\cap Y\cap Z| \,\}$$

Method

We wanted to do some coding in Magma, which is a computer algebra system



There are 72,586,459 octad triples! Too many to directly input into the computer. We first needed to develop some theory to help break the problem into manageable chunks that could be fed into the computer

During this process we got a feel for the problem and what we suspected the answer might be. We were able to confirm this suspicion with the computer

A computer can say that something *is* true but doesn't shed much light on *why* it's true. This is why we were motivated to find a computer-free proof

The proof uses information known about the various actions of M_{24} as well as classical results from finite group theory

My funders
Heilbronn Institute for Mathematical Research

My employers
MANCHESTER 1824
The University of Manchester

The grant providers
LONDON MATHEMATICAL SOCIETY
EST. 1865

Not bored yet?