Mathieu groups, the Golay code and Curtis’ Miracle Octad Generator

1 Coding theory

1.1 Coding Theory

The purpose of coding theory is to detect and correct errors in communication. This is achieved by assigning to the information to be transmitted a string of codewords that have been previously agreed upon by the sender and the receiver. The codewords are usually strings of letters of equal length from a set of characters e.g. {0, 1}, or the roman alphabet. The set is |S|, then the code is related to a binary code. Ideally the code should have as many words as possible and the words should be as short as possible to speed transmission.

If any errors (altered characters) occur in a word during the transmission then ideally the received word will not match any of the words in the code and the error can be detected. The error can also be corrected using the concept of hamming distance, which is the number of characters that are different between two words. Any words received that are not in the code are then replaced by the codeword that is closest to it i.e. differs in the least number of characters. If it is the maximum number of errors that a code can accurately correct then the code is related to a error correcting code. Ideally the code should be able to correct as many errors as possible.

The concept of hamming distance can also be used to define a ball around any word w in the set |W| of all possible words of a given length n is given using a set of characters Ω. If the distance between a word w and w' is less than r then it is said to be contained in the ball of radius r around w'. The balls considered have a fixed set of characters and therefore have the space of all possible words. If |W| is every possible word is a ball of radius r around some codeword, and none of these balls overlap, then the code is related to a perfect.

1.2 The Golay Code

The Golay code was first found in 1949 in the Proceedings of the I.R.E. (IEEE) in a paper titled “Notes on Digital Coding” [5]. The paper occupied less than a half a page in the correspondence section but E. R. Berlekamp has called it the “best single published paper” in coding theory. The 24 Golay code is a maximization of the 23 Golay code which is a perfect 3 error correcting code. The 24 Golay code consists of 8080 binary words of length 24 of which 7920 words have weight (i.e. no of ones and 16 zeros), 2760 are of weight 12 and 720 have weight 16 (and of one weight 0, and of weight 24). It also happens to be a quadratic residue code.

The Golay code also has connections to sphere packing since it can be used to construct the Leech lattice which is a set of equally spaced points in 24-dimensional space. When each ball (of radius r) are placed with their centers at the points of the Leech lattice each ball touches 196,560 neighbors and this is known to be the largest number of non-overlapping 24-dimensional unit balls which can simultaneously touch a single unit ball (compare with 6 in dimension 2, the maximum number of coins which can touch a central coin).

2 The MOG and the Hexacode

The Miracle Octad Generator (MOG) of R.T. Curtis [4] [5] is a computational tool projecting the 24 Golay code onto a [6,3,4] hexacode that makes it easy to perform calculations with these objects. Each of the characters 0, 1, or the roman alphabet. If the set is |S|, then the code is related to a binary code. Ideally the code should have as many words as possible and the words should be as short as possible to speed transmission.

The MOG can also be used to visualise partitions of the 24 points which is important as all maximal subgroups of the Mathieu groups have as many words as possible and the words should be as short as possible to speed transmission. The MOG is a computational tool projecting the 24 Golay code onto a [6,3,4] hexacode that makes it easy to perform calculations with these objects. Each of the characters 0, 1, or the roman alphabet. If the set is |S|, then the code is related to a binary code. Ideally the code should have as many words as possible and the words should be as short as possible to speed transmission.

The MOG can also be used to visualise partitions of the 24 points which is important as all maximal subgroups of the Mathieu groups, the Golay code and Curtis’ Miracle Octad Generator

3 Group Theory

Group Theory

3.1 Simple Groups

The concept of a group initially arose out of a set of permutations (ways of rearranging) of some objects. The set of permutations of some objects has three basic properties:

1. Identity - leaving the objects untouched is always a choice among them.
2. Inverse - if we can permute them in one way then there is a permutation in the set that will put them back the way they were before.
3. Associativity - if you have three permutations then doing the first two then and the last is the same as doing the first one and then the last two.

Permutations can also be “multiplied” to get another permutation in the set: the product of two permutations a and b is the permutation that results from applying a and then b. Most of the interesting properties of the group of permutations could be obtained from these simple assumptions and did not even require the assumption that the elements of the group were permutations, just that they could be multiplied to get other elements in the group and that the following three axioms were satisfied:

1. Identity - there is an element e in the group that satisfies e·a = a = a·e for every a in the group.
2. Inverse - every element a in the group has an inverse a⁻¹ in the group that satisfies a·a⁻¹ = a⁻¹·a = e.
3. Associativity - every three elements a, b, c in the group satisfy (a·b)·c = a·(b·c).

An important result in the study of groups that appeared in the early 20th century is that every finite group (group with a finite number of elements) can be constructed from finite groups with an additional property called simplicity. So the problem of classifying all finite groups is reduced to the problem of classifying all simple groups.

The classification of finite simple groups is a vast body of work, mostly published between around 1955 and 1983, which comprises 15,000 pages across 240 journal articles. The problem turns out that there are 26 finite simple groups of which there are an infinite number fall into three families except for 20 of them. For this reason the 26 remaining finite simple groups are known as sporadic.

The classification of finite simple groups is a vast body of work, mostly published between around 1955 and 1983, which comprises 15,000 pages across 240 journal articles. The problem turns out that there are 26 finite simple groups of which there are an infinite number fall into three families except for 20 of them. For this reason the 26 remaining finite simple groups are known as sporadic.

2.4 Finite Geometry

Finite Geometry

4.1 Finite Geometry

Finite Geometry is an extension of the methods of Euclid to sets with a finite number of points. Each axiom relies only on the concept of a point, a line, and a point lying on a line. A point lying on a line goes through a point. This idea can be extended into the notion of an incidence structure which consists of a set of points, a set of lines (the “lines”) and an incidence relation which defines which points lie on which lines.

A particularly useful incidence structure in a Steiner system which satisfies the additional condition that each block contains r points and every set of r points is contained in a unique block. A Steiner system is ordered (r, k, v) where r is the number of points in a block and v is the number of points in a block and k is the size of the set that defines a unique block. An example of a Steiner system is the finite projective plane PG(2,q) which has 2q+1 points, and each (block) line contains 2q points and every set of 2 points is contained in a unique block (line).

The automorphism group of a Steiner system is the group of permutations of the points in the system which maintain the block structure; i.e. if two points are on the same block before the permutation then they are also on the same block after the permutation although the block may be a different one.

4.2 The Steiner system (and relations to the Golay code)

An important Steiner system is the S(5, 8, 24) Steiner system. This system has 24 points, each block contains 8 points and every set of 5 points is contained in a unique block. This Steiner system has as its automorphism group the Mathieu group M24 and is also intimately related to the Golay code. If the points are used to index the coordinates of a 24,112 then each block defines a unique vector where the coordinates of points in the block are 1 and the coordinates of points that aren’t in the block are 0. The set of vectors that come from blocks of S(5, 8, 24) in this way are all the codewords of weight 8 in the Golay code. This process can be reversed and used to construct S(5, 8, 24) from the Golay code.

S(5, 8, 24) can also be constructed from the projective plane PG(2,q) by adding an additional 3 points. The blocks are then defined using various geometric objects such as lines, hyperovals, and Baer subplanes. The subplanes are defined roughly in the following manner (where the three additional points are labelled u, v, w):

1. A(u,v) for a line Δ
2. C(u,v,w) for a hyperoval O
3. B(u,v,w) for a Baer subplane Σ
4. The symmetric difference of Δ and Σ for two distinct lines Δ∩Σ

References
