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

Shane Kelly - AMSI/ICE-EM Vacation Scholarship

1 Coding theory

1.1 Coding Theory

The purpose of coding theory is to detect and correct errors in communication. This is achieved by converting all of the information to be transmitted into a string of codewords that have been previously agreed upon by the sender and the reciever. The codewords are usually strings of letters of equal length from a set of characters e.g. $\{0, 1\}$, $\mathbb{Z}$ or the roman alphabet. If the set is $\{0, 1\}$ then the code is refered to as 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.

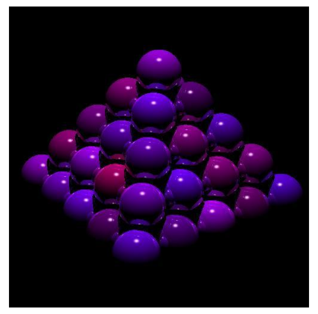
If any errors (altered characters) occur to a word during the transmission then (ideally) the received word will not match any of the words in the code and the error can be detected. The error can also be corrected using the concept of Hamming distance, which is the number of characters that are different between any 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 e is the maximum number of errors that a code can accurately correct then the code is refered to as a e error correcting code. Ideally the code should be able to correct as many errors as possile.

The concept of Hamming distance can also be used to define a ball around any word w in the set Ω^n of all possible words of a given length n using a given set of characters Ω. If the distance between a word and w is less than r then it is said to be contained in the ball of radius r around w. Now the ideals of having lots of short words and also being able to correct many errors are at odds with each other. One way of achieving a good balance between the two is to spread the codewords evenly around the space of all possible words. If for some number r, every possible word is in a ball of radius r around some codeword, and none of these balls overlap, then the code is refered to as perfect.

1.2 The Golay Code

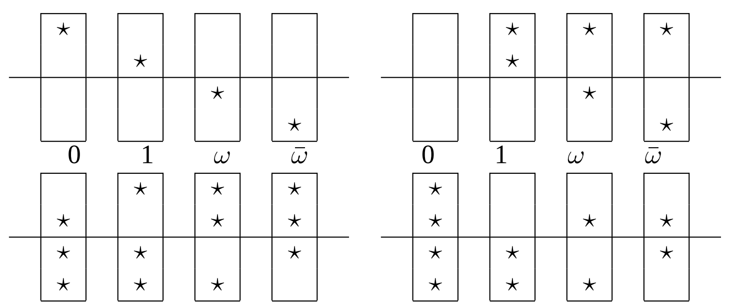
The Golay code first appeared in June 1949 in the Proceedings of the I.R.E. (I.E.E.E.) in a paper titled "Notes on Digital Coding" [8]. The paper occupied a little more that half a page in the Correspondence section but E. R. Berkekamp has called it the "best single published paper" in coding theory. The 24 Golay code is an extension of the 23 Golay code which is a perfect 3 error correcting code. The 24 Golay code consists of 4096 binary words of length 24 of which 759 words have weight 8 (8 ones and 16 zeros), 2576 are of weight 12 and 759 have weight 16 (and of course one of weight 0, and one 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 regularly spaced points in 24 dimensional space. When unit balls (balls of radius one) are placed with their centers at the points of the Leech lattice each ball touches 196,560 neighbours 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, as 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 $\{0, 1, \omega, \bar{\omega}\}$ is assigned two odd interpretations and two even interpretations as follows (blank and non-blank symbols are used instead of 0 and 1):

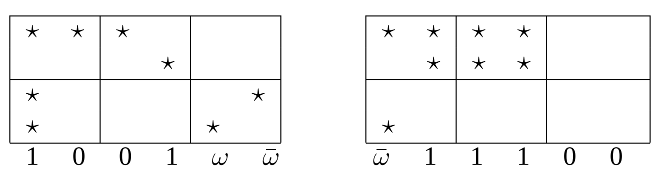


The hexacode can then be used to obtain all Golay codewords and incomplete codewords can be completed easily. The MOG can also be used to visualise partitions of the 24 points which is important as all maximal subgroups of M_{24} with the exception of $L_2(23)$ can be characterized by non-trivial partitions.

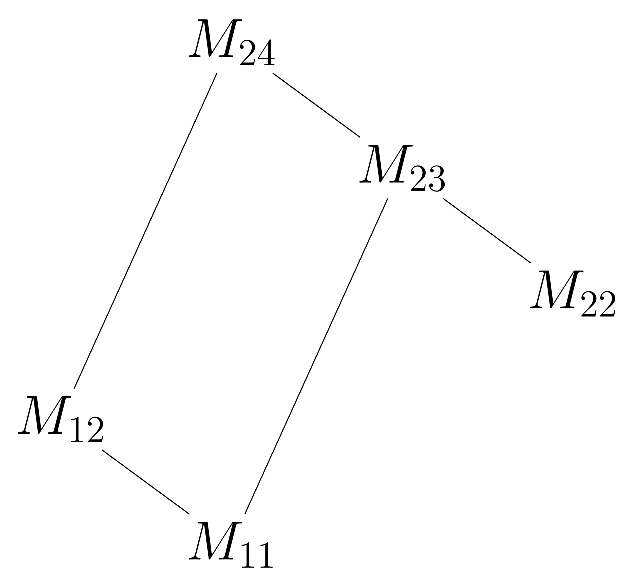
The points in the Steiner system as a projective plane $PG_2(4)$ with an extra 3 points:

∞	∞_0	00	10	$\omega 0$	$\bar{\omega}0$
a	∞_1	01	11	$\omega 1$	$\bar{\omega}1$
b	∞_ω	0ω	1ω	$\omega\omega$	$\bar{\omega}\omega$
c	$\infty_{\bar{\omega}}$	$0\bar{\omega}$	$1\bar{\omega}$	$\omega\bar{\omega}$	$\bar{\omega}\bar{\omega}$

Left: An octad constructed from the hyperoval extending the conic $X^2 + YZ = 0$.
Right: An octad constructed from a Baer subplane.



3 Group Theory



Group	Order	Subgroup of $Aut(S(5,8,24))$	Transitivity
M_{24}	$244823040 = 2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23$	$Aut(S(5,8,24))$	5
M_{23}	$10200960 = 2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 23$	Stabilizer of a point.	4
M_{22}	$443520 = 2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$	Stabilizer of two points.	3
M_{12}	$95040 = 2^6 \cdot 3^3 \cdot 5 \cdot 11$	Stabilizer of a dodecad.	5
M_{11}	$7920 = 2^4 \cdot 3^2 \cdot 5 \cdot 11$	Stabilizer of a dodecad and a point.	4

Maximal subgroups of M_{24} [1]		
Group structure	Partition	Name
M_{23}	1, 23	monad group
$M_{22}:2$	2, 22	duad group
$P\Gamma L_3(4)$	3, 21	triad group
$2^6 : 3 \cdot S_6$	4^6	sextet group
$2^4 : A_8$	8, 16	octad group
$M_{12}:2$	12^2	dodecad group
$2^6 : S_3 \times L_2(7)$	8^3	trio group
$L_2(23)$	24	projective group
$L_2(7)$	3^8	octern group

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 of rearanging them.
2. Inverse - if you can permute them one way then there is a permutation in the set that will put them back the way there were before.
3. Associativity - if you have three permutations then doing the first two and then 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 where the product of two permutations a and b is the permutation that results from doing 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 that satisfies $e \cdot a = a = a \cdot e$ for every a in the group.
2. Inverse - every element a in the group has an inverse a^{-1} in the group that satisfies $a \cdot a^{-1} = e = a^{-1} \cdot a$
3. Associativity - every three elements in the group satisfy $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

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 "atoms" of finite group theory from which all other finite groups are made.

The classification of finite simple groups is a vast body of work, mostly published between around 1955 and 1983, which comprises 10,000 - 15,000 pages in 500 journal articles by some 100 authors. It turns out that all finite simple groups (of which there are an infinite number) fall into three families except for 26 of them. For this reason the 26 remaining finite simple groups are known as sporadic.

3.2 Mathieu Groups

The Mathieu groups were first described in papers of Emile Mathieu (1861, 1873) [6] [7] and were the only sporadic groups known to exist until 1965. They are all subgroups of M_{24} and also multiply transitive. $M_{24}, M_{23}, M_{12}, M_{11}$ are the only finite simple groups which are not alternating or symmetric and are more than 3-transitive. If a group is k-transitive it means that when considered as a permutation group of some points, any k points can be sent to any k other points.

4 Finite Geometry

4.1 Finite Geometry

Finite Geometry is an extension of the methods of Euclid to sets with a finite number of points. Euclid's axioms rely only on the concept of a point, a line, and incidence. i.e. when a point is contained in a line, or 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 blocks (the "lines") and an incidence relation which defines which points are contained in which blocks.

A particularly useful incidence structure is a Steiner system which satisfies the additional criterion that each block contains k points and every set of t points is contained in a unique block. A Steiner system is notated $S(t, k, v)$ where v is the number of points, k is the number of points in a block and t is the size of the set that defines a unique block. An example of a Steiner system is the finite projective plane $PG_2(4)$ which has 21 points, each block (line) contains 5 points and every set of 2 points is contained in a unique block (line).

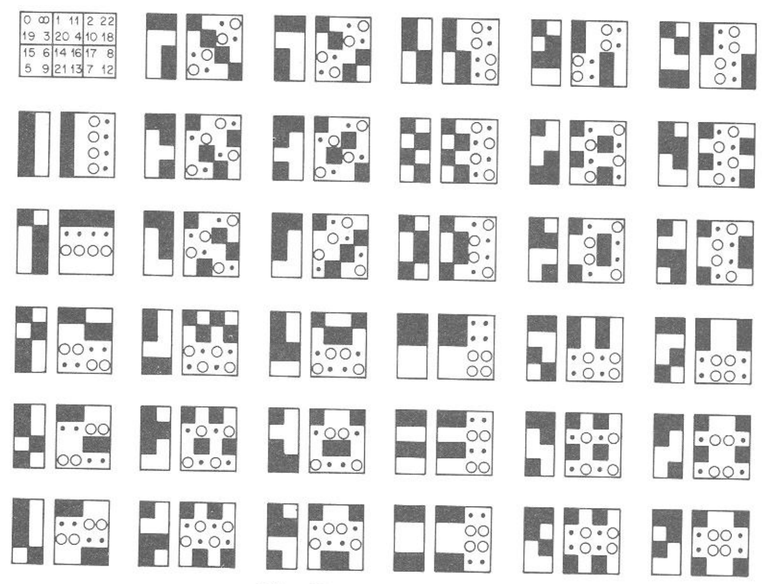
The automorphism group of a Steiner system is the group of permutations of the points in the system which maintain the block structure. i.e. if two points are in the same block before the permutation then they are in the same block after the permutation although the block may be a different one.

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 M_{24} and it is also intimately related to the Golay code. If the points are used to index the coordinates of $\{0, 1\}^{24}$ 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 $PG_2(4)$ by adding an additional 3 points. The blocks are then defined using various geometric objects such as lines, hyperovals, and Baer subplanes. The blocks are defined roughly in the following manner (where the three additional points are labelled a, b, c):

1. $\Lambda \cup \{a, b, c\}$ for a line Λ
2. $\mathcal{O} \cup \{a, b\}, \mathcal{O} \cup \{a, c\}, \mathcal{O} \cup \{b, c\}$ for a hyperoval $\mathcal{O}$
3. $\Pi \cup \{a\}, \Pi \cup \{b\}, \Pi \cup \{c\}$ for a Baer subplane Π
4. The symmetric difference of Λ_1 and Λ_2 for two distinct lines Λ_1, Λ_2



The 35 standard sextets of the MOG.

References

[1] J.H. Conway, N.J.A. Sloane, Sphere packings, Lattices and Groups, Springer-Verlag, New York, 1988

[2] John D. Dixon, Brian Mortimer, Permutation Groups, Springer-Verlag, New York, 1996

[3] Peter Dembowski, Finite Geometries, Springer-Verlag, Berlin, 1968

[4] R. T. Curtis, On subgroups of ·0, I: lattice stabilizers, J. Alg. 27 (1973), 549-573

[5] R. T. Curtis, A new combinatorial approach to M24, Math. Proc. Camb. Phil. Soc., 79 (1976), 25-42.

[6] E. Mathieu. Mémoire sur l'étude des functions des plusieurs quantités, sur le maniére de les former st sur les substitutions qui les laissent invariables. J. Math. Pures Appl. (Liouville) (2) 6 (1961), 241-323.

[7] E. Mathieu. Sur la function cing fois transitive de 24 quantités. J. Math. Pures Appl. (Liouville) (2) 18 (1873), 25-46.

[8] M. J. E. Golay, Notes on Digital Coding, Proc. I. R. E. 37 (1949) p 657.