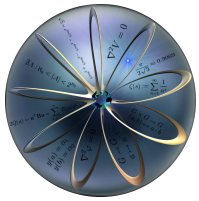

planetmath.org

Math for the people, by the people.

miracle octad generator

Canonical name	MiracleOctadGenerator
Date of creation	2013-03-22 18:43:14
Last modified on	2013-03-22 18:43:14
Owner	monster (22721)
Last modified by	monster (22721)
Numerical id	8
Author	monster (22721)
Entry type	Derivation
Classification	msc 20B25
Classification	msc 20B20
Classification	msc 51E10
Classification	msc 94B05
Synonym	MOG
Related topic	hexacode
Related topic	LeechLattice
Related topic	Hexacode
Defines	miracle octad generator
Defines	MOG
Defines	octad
Defines	dodecad

The Miracle Octad Generator (MOG) is a construction of the [24,12,8] extended binary Golay code $\mathcal{G}_{24}$. It makes use of the hexacode. The notation [24,12,8] indicates that this linear code has http://planetmath.org/LinearCodelength 24, http://planetmath.org/LinearCodedimension 12, and http://planetmath.org/MinimumDis weight 8.

The construction is originally due to R. T. Curtis ([?], [?]). The description of the MOG below is taken from [?], Chapter 11. A proof that the construction gives a [24,12,8] code is given below. A proof of the uniqueness of the binary Golay code (up to permutation of the coordinates) can be found in [?], Chapter 5.

1 Construction

The MOG consists of a rectangular array of 4 rows and 6 columns. The rows of the MOG are labelled with elements of $\mathbb{F}_4$ (the field of 4 elements). The labels are $0, 1, \omega, \overline{\omega}$ from top to bottom, where ω is a cube root of unity. The code $\mathcal{G}_{24}$ consists of subsets S of the 24 squares of the array which satisfy the following conditions:

- the parities of the number of elements in S in each of the 6 columns, and in the top row, are the same
- the sums of the row labels for elements of S in each column form an element of the hexacode.

For example:

0		$*$			$*$	
1		$*$				$*$
ω				$*$	$*$	$*$
$\overline{\omega}$				$*$		
	0	1	0	1	ω	$\overline{\omega}$

In a MOG diagram, asterisks indicate a subset of the 24 squares. On the left side, we have written the row labels, and at the bottom we have written the column sums for our subset. For the subset above, each of the columns, as well as the top row, contains 2 elements, and the column sums 01 01 $\omega\overline{\omega}$ form an element of the hexacode. Hence, this subset of the MOG is an element of $\mathcal{G}_{24}$.

Notation: For S any subset of the MOG, let us write $\Sigma(S)$ for the element of $\mathbb{F}_4^6$ corresponding to the column sums. Hence, the second condition above says that $\Sigma(S)$ is in the hexacode for any $S \in \mathcal{G}_{24}$.

When we say that a column is "even" or "odd", we are referring to the of the number of elements of S in the column. When we speak of the "sum" of a column, we are referring to the sum of the row labels of S for that column, i.e., the component of $\Sigma(S)$ for that column.

2 Proof that the construction gives a [24,12,8] code

Let us note a few facts about $\mathcal{G}_{24}$ and the MOG.

Fact 1 *$\mathcal{G}_{24}$ is an* `http://planetmath.org/EvenCode`*even linear code of 24 over $\mathbb{F}_2$, and is closed under complementation.*

This follows from the linearity of the two conditions above (which in turn follows from the linearity of the hexacode), and the fact that the and column sums do not change under complementation.

Fact 2 *If an even column has sum 0, then it contains 0 or 4 elements. If an odd column has sum 0, then the top row entry is in the column iff the column consists of exactly 1 element (and otherwise it consists of exactly 3 elements).*

Fact 3 *If an even column has nonzero sum, then it consists of 2 elements. If an odd column has nonzero sum, then the top row entry is in the column iff the column consists of exactly 3 elements (and otherwise it consists of exactly 1 element).*

From these facts, we can show that $\mathcal{G}_{24}$ is a doubly even code (the weight of any element is divisible by 4). Let S be an element of $\mathcal{G}_{24}$. If the columns of S are even, then it is clear that $|S|$ is divisible by 4. Suppose the columns of S are odd. Let t_1 (resp., t_3) denote the number of columns consisting of 1 (resp., 3) elements, for which the top row is filled. Let u_1 (resp., u_3) denote the number of columns consisting of 1 (resp., 3) elements, for which the top row is empty. The defining conditions of $\mathcal{G}_{24}$ imply that $t_1 + t_3$ is odd. By

Fact 2, the number of 0's in $\Sigma(S)$ is equal to $t_1 + u_3$, which is therefore even by a property of the hexacode. So $t_3 + u_3$ is odd. Since there are 6 columns, we have $t_1 + t_3 + u_1 + u_3 = 6$. Hence

$$\begin{aligned} |S| &= 3t_3 + 3u_3 + t_1 + u_1 \\ &= 3t_3 + 3u_3 + t_1 + (6 - t_1 - t_3 - u_3) \\ &= 2(t_3 + u_3) + 6 \\ &\equiv 0 \pmod 4. \end{aligned}$$

Furthermore, it is not difficult to see that an element of weight 4 is impossible, hence the minimum weight of $\mathcal{G}_{24}$ is 8. So the only possible weights of elements of $\mathcal{G}_{24}$ are 0, 8, 12, 16, and 24.

To calculate the of $\mathcal{G}_{24}$, we need to count the number of elements of each weight. Weights 0 and 24 are obvious, and the counts for weight 8 and weight 16 are the same. So we need only count weights 8 and 12. This is not difficult using the defining conditions above, and knowledge of the hexacode; the final result is that the number of elements of weights 0,8,12,16,and 24 are 1, 759, 2576, 759, and 1, respectively, for a total of $4096 = 2^{12}$. Hence $\mathcal{G}_{24}$ has 12, so it is a [24,12,8] code.

3 Further facts about the binary Golay code

Elements of $\mathcal{G}_{24}$ of weight 8 are called *octads*. Elements of $\mathcal{G}_{24}$ of weight 12 are called *dodecads*.

The octads of $\mathcal{G}_{24}$ form a (5,8,24) Steiner system. In other words, given any 5 squares in the MOG, there is a unique way to add 3 squares to form an octad. To complete an octad, it is necessary to solve `http://planetmath.org/hexacode`3-problems or `http://planetmath.org/hexacode`5-problems for the hexacode. For a detailed procedure, see ([**?**], 11.6).

The automorphism group of $\mathcal{G}_{24}$ is the largest Mathieu group M_{24}, one of the sporadic simple groups.

The code $\mathcal{G}_{24}$ is used in the construction of the Leech `http://planetmath.org/LatticeInMathb` whose automorphism group is the largest Conway group Co_0 (sometimes written $\cdot 0$). The quotient of Co_0 by its center, called Co_1, is a sporadic simple group. The group Co_1 plays an important role in the construction of the monster group, the largest sporadic simple group of all.

References

[1] J. H. Conway and N. J. A. Sloane. Sphere Packings, Lattices, and Groups. Springer-Verlag, 1999.

[2] Robert L. Griess, Jr. Twelve Sporadic Groups. Springer-Verlag, 1998.

[3] R. T. Curtis. On subgroups of $\cdot 0$, I: lattice stabilizers. Journal of Algebra, 27 (1973), 549-573.

[4] R. T. Curtis. A new combinatorial approach to M_{24}. Proceedings of the Cambridge Philosophical Society 79 (1976), 25-42.