An incompleat history of the $(7, 3, 1)$ block design

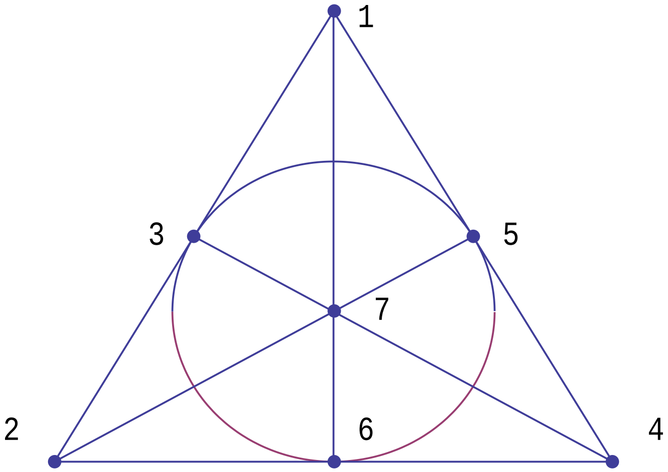
Ezra Brown
Virginia Tech

MD-DC-VA Fall Section Meeting
Johns Hopkins University
November 5, 2016

What to expect

- 1835: apparent beginnings
- 1844: octonions
- 1847: block designs
- 1891: map coloring and topology
- 1892: finite geometries
- 1933: difference sets
- 1947: codes
- Before 1835 . . . what?

The Design



A Beautiful Design

The birth of combinatorial designs

1835: Julius Plücker and cubics

- A general plane cubic curve has nine points of inflection.
- The points lie on four sets of three lines, with three points per line.
- Exactly one of these twelve lines must pass through any two inflection points.

1839: Julius Plücker and the nine-point affine plane

Designate the points as $1, 2, 3, 4, 5, 6, 7, 8$, and 9. Then the twelve lines are as follows:

$$\{1,2,3\},\{4,5,6\},\{7,8,9\}$$
$$\{1,4,7\},\{2,5,8\},\{3,6,9\}$$
$$\{1,5,9\},\{2,6,7\},\{3,4,8\}$$
$$\{1,6,8\},\{2,4,9\},\{3,5,7\}$$

This is the first block design to appear in print.

The birth of combinatorial designs

1835: Julius Plücker and cubics

- A general plane cubic curve has nine points of inflection.
- The points lie on four sets of three lines, with three points per line.
- Exactly one of these twelve lines must pass through any two inflection points.

1839: Julius Plücker and the nine-point affine plane

Designate the points as $1, 2, 3, 4, 5, 6, 7, 8$, and 9. Then the twelve lines are as follows:

$$\{1,2,3\},\{4,5,6\},\{7,8,9\}$$
$$\{1,4,7\},\{2,5,8\},\{3,6,9\}$$
$$\{1,5,9\},\{2,6,7\},\{3,4,8\}$$
$$\{1,6,8\},\{2,4,9\},\{3,5,7\}$$

This is the first block design to appear in print. Or is it?

Euler and Hamilton and the quaternions

1748: Euler's four-square identity

$$(a_1^2 + a_2^2 + a_3^2 + a_4^2)(b_1^2 + b_2^2 + b_3^2 + b_4^2) =$$
$$= (a_1 b_1 - a_2 b_2 - a_3 b_3 - a_4 b_4)^2 + (a_1 b_2 + a_2 b_1 + a_3 b_4 - a_4 b_3)^2$$
$$+ (a_1 b_3 - a_2 b_4 + a_3 b_1 + a_4 b_2)^2 + (a_1 b_4 + a_2 b_3 - a_3 b_2 + a_4 b_1)^2$$

1843: Hamilton's four-dimensional normed algebra – the quaternions

$$i^2 = j^2 = k^2 = ijk = -1$$

What happened next

October 18, 1843: Hamilton writes John Graves with the news.
November 1843: John writes back, "I'll see your four squares and raise you four more."

1844: John Graves' news

The eight-squares identity

$$
\begin{aligned}
&\left(a_0{}^2 + a_1{}^2 + a_2{}^2 + a_3{}^2 + a_4{}^2 + a_5{}^2 + a_6{}^2 + a_7{}^2\right) \\
&\times\left(b_0{}^2 + b_1{}^2 + b_2{}^2 + b_3{}^2 + b_4{}^2 + b_5{}^2 + b_6{}^2 + b_7{}^2\right) \\
&= (a_0b_0 - a_1b_1 - a_2b_2 - a_3b_3 - a_4b_4 - a_5b_5 - a_6b_6 - a_7b_7)^2 \\
&+(a_0b_1 + a_1b_0 + a_2b_3 - a_3b_2 + a_4b_5 - a_5b_4 - a_6b_7 + a_7b_6)^2 \\
&+(a_0b_2 - a_1b_3 + a_2b_0 + a_3b_1 + a_4b_6 + a_5b_7 - a_6b_4 - a_7b_5)^2 \\
&+(a_0b_3 + a_1b_2 - a_2b_1 + a_3b_0 + a_4b_7 - a_5b_6 + a_6b_5 - a_7b_4)^2 \\
&+(a_0b_4 - a_1b_5 - a_2b_6 - a_3b_7 + a_4b_0 + a_5b_1 + a_6b_2 + a_7b_3)^2 \\
&+(a_0b_5 + a_1b_4 - a_2b_7 + a_3b_6 - a_4b_1 + a_5b_0 - a_6b_3 + a_7b_2)^2 \\
&+(a_0b_6 + a_1b_7 + a_2b_4 - a_3b_5 - a_4b_2 + a_5b_3 + a_6b_0 - a_7b_1)^2 \\
&+(a_0b_7 - a_1b_6 + a_2b_5 + a_3b_4 - a_4b_3 - a_5b_2 + a_6b_1 + a_7b_0)^2.
\end{aligned}
$$

The octaves

Graves' letter describes a way to multiply *octaves*, or eight-dimensional real vectors. We now call them octonions.

Meanwhile, in another part of the forest:

1844-46: Wesley Woolhouse

"How many triads can be made out of n symbols, so that no pair of symbols shall be comprised more than once amongst the triads?"

1847: Thomas Kirkman

"On a problem of combinations": monumental paper that begins serious study of combinatorial designs, gives birth to its central objects, and exhibits the $(7, 3, 1)$ block design.

Block Designs

A *balanced incomplete block design* with parameters (v, k, λ) is a collection of k-subsets of a v-element set V such that every pair of distinct elements of V occurs together in exactly λ of the k-subsets.

1847: Kirkman describes the $(7, 3, 1)$ block design

1	2	3	A
1	4	5	B
1	6	7	C
2	4	6	D
2	5	7	E
3	4	7	F
3	5	6	G

- The objects $V = \{1, 2, 3, 4, 5, 6, 7\}$ are called *varieties*, *treatments*, or *points*
- The 3-element subsets $\{A, B, C, D, E, F, G\}$ of V are called *blocks*, *plots*, or *lines*.

The octonions and the $(7, 3, 1)$ block design

1845: Graves' and Cayley's multiplication of octonion units

$$
\begin{aligned}
{i_1}^2 = {i_2}^2 = {i_3}^2 = {i_4}^2 = {i_5}^2 = {i_6}^2 = {i_7}^2 = -1 \\
i_1 = i_2 i_3 = i_4 i_5 = i_7 i_6 = -i_3 i_2 = -i_5 i_4 = -i_6 i_7 \\
i_2 = i_3 i_1 = i_4 i_6 = i_5 i_7 = -i_1 i_3 = -i_6 i_4 = -i_7 i_5 \\
i_3 = i_1 i_2 = i_4 i_7 = i_6 i_5 = -i_2 i_1 = -i_7 i_4 = -i_5 i_6 \\
i_4 = i_5 i_1 = i_6 i_2 = i_7 i_3 = -i_1 i_5 = -i_2 i_6 = -i_3 i_7 \\
i_5 = i_1 i_4 = i_7 i_2 = i_3 i_6 = -i_4 i_1 = -i_2 i_7 = -i_6 i_3 \\
i_6 = i_2 i_4 = i_1 i_7 = i_5 i_3 = -i_4 i_2 = -i_7 i_1 = -i_3 i_5 \\
i_7 = i_6 i_1 = i_2 i_5 = i_3 i_4 = -i_1 i_6 = -i_5 i_2 = -i_4 i_3
\end{aligned}
$$

1848: Kirkman and the octonions

Shows that the $(7, 3, 1)$ design plays a central role in Graves and Cayley's multiplication of octonion units.

Incidence matrices and $(7, 3, 1)$

The incidence matrix M of a design

- Given a (v, k, λ) design with b blocks.
- $M = [m_{ij}]$ is a $b \times v$ matrix with $m_{ij} = 1$ or 0 if the ith block does or does not contain the jth variety, respectively.

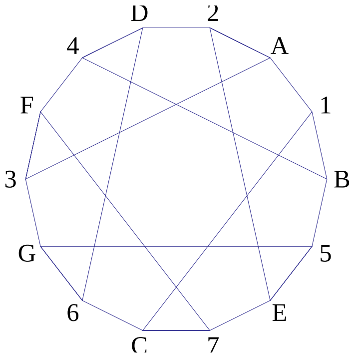
The incidence matrix of $(7, 3, 1)$

	1	2	3	4	5	6	7
A	**1**	**1**	**1**	0	0	0	0
B	**1**	0	0	**1**	**1**	0	0
C	**1**	0	0	0	0	**1**	**1**
D	0	**1**	0	**1**	0	**1**	0
E	0	**1**	0	0	**1**	0	**1**
F	0	0	**1**	**1**	0	0	**1**
G	0	0	**1**	0	**1**	**1**	0

The *block-point graph* BP(D)of a (v, k, λ) design D

Blocks and points are vertices, and there is an edge between a point p and a block X if and only if $p \in X$. The block-point graph of a design with v varieties and b k-element blocks contains $b + v$ vertices and bk edges.

The block-point graph of $(7, 3, 1)$ is called the Heawood graph:



1891: P. J. Heawood and map-coloring

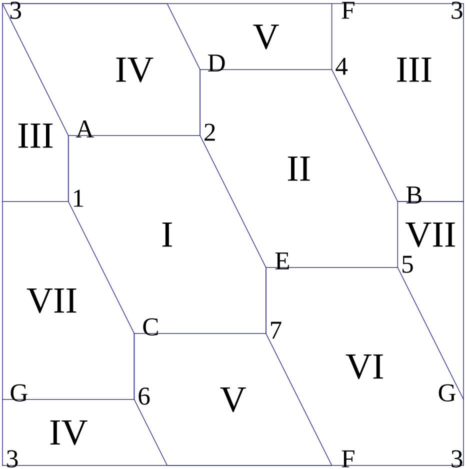
- *Proper coloring of a map M*: an assignment of colors to the regions of a map so that adjacent regions have distinct colors.

- *Chromatic number of M*: the smallest number of colors needed in a proper coloring of M

- *Heawood's Conjecture* (1891, proved in 1968): For $g > 0$, the chromatic number of every map drawn on the surface of a g-holed torus is at most $\lfloor (7 + \sqrt{1 + 48g})/2 \rfloor$, and this bound is sharp.

- This number is 7 for the 1-holed torus.

1891: The Heawood Graph on the Torus

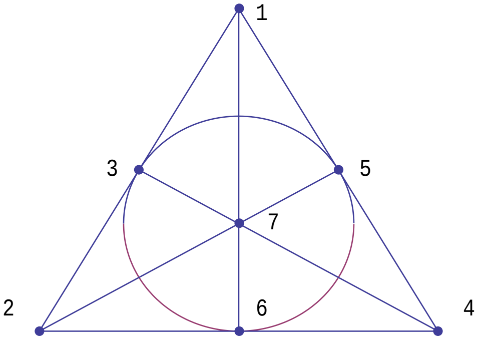


Seven mutually adjacent hexagons on a torus:
a toroidal imbedding of the block-point graph of $(7, 3, 1)$

Finite Geometries

1892: Gino Fano

- Publishes major work on the foundations of projective geometry.
- Pioneers ideas about finite geometry that Kirkman anticipated in the 1850s before Fano was born.



The Fano plane: vertices and sides are the points and blocks of $(7, 3, 1)$

1933: Paley constructs difference sets

- A (v, k, λ) *difference set* is a k-element subset D of $V = \mathbb{Z} \bmod v$ such that every nonzero element of V can be expressed as a difference $a - b$ of elements $a, b \in D$ in exactly λ ways.

- In 1933, R. E. A. C. Paley proves that if $p = 4n + 3$ is a prime, then the nonzero squares mod p form a $(4n + 3, 2n + 1, n)$ difference set.

- These are the so-called Paley-Hadamard difference sets.

The $(7, 3, 1)$ difference set – and a bonus

The difference set

Let $D = \{1, 2, 4\}$ be the nonzero squares mod $p = 7$. Look at the differences of elements of D mod 7 :

$$\begin{array}{ll} 2 - 1 \equiv \mathbf{1} & 1 - 4 \equiv \mathbf{4} \\ 4 - 2 \equiv \mathbf{2} & 2 - 4 \equiv \mathbf{5} \\ 4 - 1 \equiv \mathbf{3} & 1 - 2 \equiv \mathbf{6} \end{array}$$

The numbers $\{1, 2, 3, 4, 5, 6\}$ are each expressible as a difference of elements of D in exactly 1 way. Hence, $D = \{1, 2, 4\}$ is a $(7, 3, 1)$ Paley-Hadamard difference set.

The bonus

D a (v, k, λ) difference set: the translates $\{D + k \bmod v : 1 \leq k \leq v\}$ of D mod v form a (v, k, λ) block design.Thus the sets $\{1, 2, 4\}, \{2, 3, 5\}, \{3, 4, 6\}, \{4, 5, 7\}, \{5, 6, 1\}, \{6, 7, 2\}, \{7, 1, 3\}$ form a $(7, 3, 1)$ block design.

1947: Hamming constructs error-correcting codes

The Hamming Code According To Shannon

"Let a block of seven [binary] symbols be $X_1, X_2, \ldots, X_7$. Of these X_3, X_5, X_6 and X_7 are message symbols and chosen arbitrarily by the source. The other three are redundant and calculated as follows:

$$X_4 \text{ is chosen to make } \alpha = X_4 + X_5 + X_6 + X_7 \text{ even}$$
$$X_2 \text{ is chosen to make } \beta = X_2 + X_3 + X_6 + X_7 \text{ even}$$
$$X_1 \text{ is chosen to make } \gamma = X_1 + X_3 + X_5 + X_7 \text{ even}$$

When a block of seven is received, α, β and γ are calculated and if even called zero, if odd called one. The binary number $\alpha\beta\gamma$ then gives the subscript of the X_i that is incorrect (if 0 there was no error)."

The $(7, 4)$ Hamming Code

1	2	**3**	4	**5**	**6**	**7**
0	0	**0**	0	**0**	**0**	**0**
1	1	**0**	1	**0**	**0**	**1**
0	1	**0**	1	**0**	**1**	**0**
1	0	**0**	0	**0**	**1**	**1**
1	0	**0**	1	**1**	**0**	**0**
0	1	**0**	0	**1**	**0**	**1**
1	1	**0**	0	**1**	**1**	**0**
0	0	**0**	1	**1**	**1**	**1**
1	1	**1**	0	**0**	**0**	**0**
0	0	**1**	1	**0**	**0**	**1**
1	0	**1**	1	**0**	**1**	**0**
0	1	**1**	0	**0**	**1**	**1**
0	1	**1**	1	**1**	**0**	**0**
1	0	**1**	0	**1**	**0**	**1**
0	0	**1**	0	**1**	**1**	**0**
1	1	**1**	1	**1**	**1**	**1**

The $(7, 4)$ Hamming Code and $(7, 3, 1)$

	1	2	3	4	5	6	7	1's in weight-3 codewords
	0	0	0	0	0	0	0	
	1	1	0	1	0	0	1	
D	0	**1**	0	**1**	0	**1**	0	$\{2, 4, 6\}$
C	**1**	0	0	0	0	**1**	**1**	$\{1, 6, 7\}$
B	**1**	0	0	**1**	**1**	0	0	$\{1, 4, 5\}$
E	0	**1**	0	0	**1**	0	**1**	$\{2, 5, 7\}$
	1	1	0	0	1	1	0	
	0	0	0	1	1	1	1	
A	**1**	**1**	**1**	0	0	0	0	$\{1, 2, 3\}$
F	0	0	**1**	**1**	0	0	**1**	$\{3, 4, 7\}$
	1	0	1	1	0	1	0	
	0	1	1	0	0	1	1	
	0	1	1	1	1	0	0	
	1	0	1	0	1	0	1	
G	0	0	**1**	0	**1**	**1**	0	$\{3, 5, 6\}$
	1	1	1	1	1	1	1	

Block designs before 1835

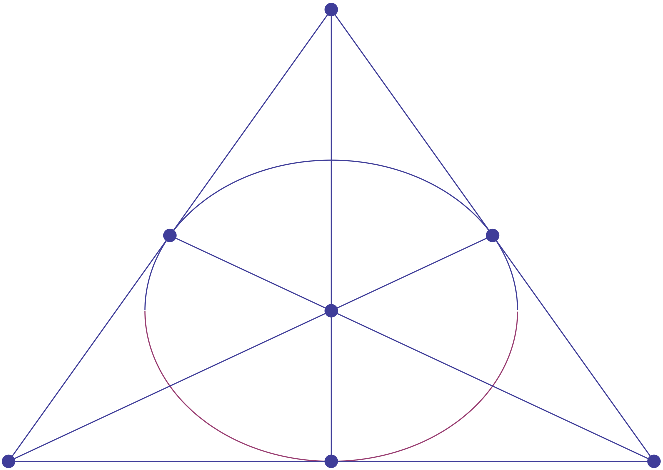
The magic square of order 3 (ancient times):

8	1	6
3	5	7
4	9	2

The three rows, three columns, and six extended diagonals form a $(9, 3, 1)$ block design:

$$\{1,2,3\}, \{4,5,6\}, \{7,8,9\}$$
$$\{1,4,7\}, \{2,5,8\}, \{3,6,9\}$$
$$\{1,5,9\}, \{2,6,7\}, \{3,4,8\}$$
$$\{1,6,8\}, \{2,4,9\}, \{3,5,7\}$$

Finally, it is safe to assume that Euclid (early 4th century BCE) would have drawn the following figure some time during his life:



That Beautiful Design

THANK YOU!