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?
A Beautiful Design

Brown  History of (7, 3, 1)
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:

\[
\begin{align*}
\{1, 2, 3\}, \{4, 5, 6\}, \{7, 8, 9\} \\
\{1, 4, 7\}, \{2, 5, 8\}, \{3, 6, 9\} \\
\{1, 5, 9\}, \{2, 6, 7\}, \{3, 4, 8\} \\
\{1, 6, 8\}, \{2, 4, 9\}, \{3, 5, 7\}
\end{align*}
\]

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:

\[
\begin{align*}
\{1, 2, 3\}, \{4, 5, 6\}, \{7, 8, 9\} \\
\{1, 4, 7\}, \{2, 5, 8\}, \{3, 6, 9\} \\
\{1, 5, 9\}, \{2, 6, 7\}, \{3, 4, 8\} \\
\{1, 6, 8\}, \{2, 4, 9\}, \{3, 5, 7\}
\end{align*}
\]

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.”
The eight-squares identity

\[
(a_0^2 + a_1^2 + a_2^2 + a_3^2 + a_4^2 + a_5^2 + a_6^2 + a_7^2) \times (b_0^2 + b_1^2 + b_2^2 + b_3^2 + b_4^2 + b_5^2 + b_6^2 + b_7^2)
\]

\[
= (a_0 b_0 - a_1 b_1 - a_2 b_2 - a_3 b_3 - a_4 b_4 - a_5 b_5 - a_6 b_6 - a_7 b_7)^2
\]

\[+ (a_0 b_1 + a_1 b_0 + a_2 b_3 - a_3 b_2 + a_4 b_5 - a_5 b_4 - a_6 b_7 + a_7 b_6)^2\]

\[+ (a_0 b_2 - a_1 b_3 + a_2 b_0 + a_3 b_1 + a_4 b_6 + a_5 b_7 - a_6 b_4 - a_7 b_5)^2\]

\[+ (a_0 b_3 + a_1 b_2 - a_2 b_1 + a_3 b_0 + a_4 b_7 - a_5 b_6 + a_6 b_5 - a_7 b_4)^2\]

\[+ (a_0 b_4 - a_1 b_5 - a_2 b_6 - a_3 b_7 + a_4 b_0 + a_5 b_1 + a_6 b_2 + a_7 b_3)^2\]

\[+ (a_0 b_5 + a_1 b_4 - a_2 b_7 + a_3 b_6 - a_4 b_1 + a_5 b_0 - a_6 b_3 + a_7 b_2)^2\]

\[+ (a_0 b_6 + a_1 b_7 + a_2 b_4 - a_3 b_5 - a_4 b_2 + a_5 b_3 + a_6 b_0 - a_7 b_1)^2\]

\[+ (a_0 b_7 - a_1 b_6 + a_2 b_5 + a_3 b_4 - a_4 b_3 - a_5 b_2 + a_6 b_1 + a_7 b_0)^2.\]

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 \((v, k, \lambda)\) 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 \(\lambda\) of the \(k\)-subsets.
1847: Kirkman describes the \((7, 3, 1)\) block design

\[
\begin{array}{ccc}
1 & 2 & 3 & A \\
1 & 4 & 5 & B \\
1 & 6 & 7 & C \\
2 & 4 & 6 & D \\
2 & 5 & 7 & E \\
3 & 4 & 7 & F \\
3 & 5 & 6 & G \\
\end{array}
\]

- 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

\[
\begin{align*}
i_1^2 &= i_2^2 = i_3^2 = i_4^2 = i_5^2 = i_6^2 = i_7^2 = -1 \\
i_1 &= i_2 i_3 = i_4 i_5 = i_7 i_6 = -i_3 i_2 = -i_5 i_4 = -i_6 i_7 \\
i_2 &= i_3 i_1 = i_4 i_6 = i_5 i_7 = -i_1 i_3 = -i_6 i_4 = -i_7 i_5 \\
i_3 &= i_1 i_2 = i_4 i_7 = i_6 i_5 = -i_2 i_1 = -i_7 i_4 = -i_5 i_6 \\
i_4 &= i_5 i_1 = i_6 i_2 = i_7 i_3 = -i_1 i_5 = -i_2 i_6 = -i_3 i_7 \\
i_5 &= i_1 i_4 = i_7 i_2 = i_3 i_6 = -i_4 i_1 = -i_2 i_7 = -i_6 i_3 \\
i_6 &= i_2 i_4 = i_1 i_7 = i_5 i_3 = -i_4 i_2 = -i_7 i_1 = -i_3 i_5 \\
i_7 &= i_6 i_1 = i_2 i_5 = i_3 i_4 = -i_1 i_6 = -i_5 i_2 = -i_4 i_3
\end{align*}
\]

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.
The incidence matrix $M$ of a design

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

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

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>$A$</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$B$</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$C$</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$D$</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>$E$</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>$F$</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>$G$</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>
The block-point graph $BP(D)$ of a $(v, k, \lambda)$ 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:
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 $\lceil (7 + \sqrt{1 + 48g})/2 \rceil$, and this bound is sharp.

This number is 7 for the 1-holed torus.
Seven mutually adjacent hexagons on a torus:
a toroidal imbedding of the block-point graph of (7, 3, 1)
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 \((v, k, \lambda)\) difference set is a \(k\)-element subset \(D\) of \(V = \mathbb{Z} \mod v\) such that every nonzero element of \(V\) can be expressed as a difference \(a - b\) of elements \(a, b \in D\) in exactly \(\lambda\) 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 difference set

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

- $2 - 1 \equiv 1$
- $1 - 4 \equiv 4$
- $4 - 2 \equiv 2$
- $2 - 4 \equiv 5$
- $4 - 1 \equiv 3$
- $1 - 2 \equiv 6$

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 $(v, k, \lambda)$ difference set: the translates $\{D + k \mod v : 1 \leq k \leq v\}$ of $D$ mod $v$ form a $(v, k, \lambda)$ 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.
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:

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

When a block of seven is received, $\alpha, \beta$ and $\gamma$ 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 $(7, 3, 1)$

<p>| | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

$D$ 0 1 0 1 0 1 0 0 \{2, 4, 6\}

$C$ 1 0 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\}

$A$ 1 1 1 0 0 0 0 \{1, 2, 3\}

$F$ 0 0 1 1 0 0 1 \{3, 4, 7\}

$G$ 0 0 1 0 1 1 0 \{3, 5, 6\}

1's in weight-3 codewords

0 0 0 1 1 1 1 1
The magic square of order 3 (ancient times):

\[
\begin{array}{ccc}
8 & 1 & 6 \\
3 & 5 & 7 \\
4 & 9 & 2 \\
\end{array}
\]

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:
4th Century BCE: Euclid’s figure

That Beautiful Design
THANK YOU!