Hadamard 2-Groups Redux

J. F. Dillon

National Security Agency
Fort George G. Meade, MD USA

Algebraic Combinatorics:
In Memory of Bob Liebler
Colorado State University
November 2011

"THE NEED FOR HAPPINESS"

"Perhaps it is sufficient to find representations with really simple value enumerator. Unfortunately, I have no really effective idea how to achieve this rather vague objective. For this reason I will call such a representation **happy**. *Perhaps you will then accept that I cannot tell you what happiness is but only that I seem to be able to recognize it when I find it. Happiness is highly basis dependent and therefore not spectral. Perhaps happiness is combinatorial."*

“THE NEED FOR HAPPINESS”

“Perhaps it is sufficient to find representations with really simple value enumerator. Unfortunately, I have no really effective idea how to achieve this rather vague objective. For this reason I will call such a representation ***happy****. Perhaps you will then accept that I cannot tell you what happiness is but only that I seem to be able to recognize it when I find it. Happiness is highly basis dependent and therefore not spectral. Perhaps happiness is combinatorial.”*

Robert A. Liebler,
NON-ABELIAN DIFFERENCE SETS, Proceedings NATO Advanced Study Institute on Difference Sets, Sequences and Their Correlation Properties, A. Pott et. al. Eds., Kluwer, 1998.

Terminology and notation

G a group of order v , D a k-subset of G

Terminology and notation

G a group of order v , D a k-subset of G
D is a (v, k, λ)-difference set in G if

Terminology and notation

G a group of order v , D a k-subset of G
D is a (v, k, λ)-difference set in G if in the group ring $\mathbb{Z}G$

Terminology and notation

G a group of order v , D a k-subset of G
D is a $(v,\ k,\ \lambda)$-difference set in G if in the group ring $\mathbb{Z}G$

$$DD^{(-1)} = n + \lambda G, n := k - \lambda.$$

Terminology and notation

G a group of order v , D a k-subset of G
D is a (v, k, λ)-difference set in G if in the group ring $\mathbb{Z}G$

$$DD^{(-1)} = n + \lambda G, n := k - \lambda.$$

$D^* := G - 2D \Rightarrow$

$$D^* D^{*(-1)} = 4n + (v - 4n)G$$

Terminology and notation

G a group of order v , D a k-subset of G
D is a $(v,\ k,\ \lambda)$-difference set in G if in the group ring $\mathbb{Z}G$

$$DD^{(-1)} = n + \lambda G, n := k - \lambda.$$

$D^* := G - 2D \Rightarrow$

$$D^* D^{*(-1)} = 4n + (v - 4n)G$$

$v = 1$ or $v = 4n \Rightarrow$

$$D^* D^{*(-1)} = |G|.$$

Terminology and notation

G a group of order v , D a k-subset of G
D is a $(v,\ k,\ \lambda)$-difference set in G if in the group ring $\mathbb{Z}G$

$$DD^{(-1)} = n + \lambda G, n := k - \lambda.$$

$D^* := G - 2D \Rightarrow$

$$D^* D^{*(-1)} = 4n + (v - 4n)G$$

$v = 1$ or $v = 4n \Rightarrow$

$$D^* D^{*(-1)} = |G|.$$

In this case the $v \times v$ matrix $\left[D^*(yx^{-1})\right]$ is Hadamard.

Terminology and notation

G a group of order v , D a k-subset of G
D is a (v, k, λ)-difference set in G if in the group ring $\mathbb{Z}G$

$$DD^{(-1)} = n + \lambda G, n := k - \lambda.$$

$D^* := G - 2D \Rightarrow$

$$D^* D^{*(-1)} = 4n + (v - 4n)G$$

$v = 1$ or $v = 4n \Rightarrow$

$$D^* D^{*(-1)} = |G|.$$

In this case the $v \times v$ matrix $\left[D^*(yx^{-1})\right]$ is Hadamard.
Let $\mathcal{H}$ denote the family of groups which have such a difference set.

JFD MH talk (1990):Hadamard Groups of order 64

1

A SURVEY OF
DIFFERENCE SETS
IN 2-GROUPS

(Subtitle: HADAMARD GROUPS OF ORDER 64)

J.F. Dillon
National Security Agency

Marshall Hall Conf.
U. Vermont
Sept. 1990

JFD MH talk (1990):Hadamard Groups of order 64

STATUS REPORT

AMONG ? 5 $\mathbb{Z}_{16}\times\mathbb{Z}_4$ transfers

HADAMARD	NONHADAMARD	?
258	8	1

$$M_{64} = \langle x, y : x^{32} = 1 = y^2, yxy = x^{17} \rangle$$

JFD MH talk (1990):Hadamard Groups of order 64

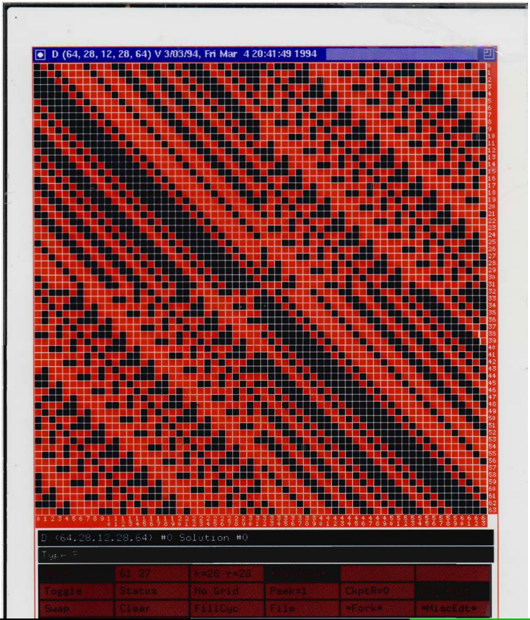
Theorem. Of the 267 groups of order 64 there are exactly 8 ~~9~~ which do not have nontrivial difference sets.

These non-Hadamard groups are:

Exponent	Cayley #	group
64	1	$\mathbb{Z}_{64}$
32	50	$\mathbb{Z}_{32} \times \mathbb{Z}_2$
	51	$M_{64} = \langle x,y : x^{32} = 1 = y^2, yxy = x^{17} \rangle$
	52	D_{64}
	53	SD_{64}
	54	Q_{64}
16	38	$\langle x,y,z : x^{16} = 1 = y^2, xy = yx, z^4 = 1, z^2 = y, zxz^{-1} = x^{-1}y \rangle$
	47	$\langle x,y : x^{16} = 1 = y^4, yxy^{-1} = x^{-1} \rangle$
	186	$D_{32} \times \mathbb{Z}_2$

difference set constructed by KWSmith 26 March 1991

M64 Hadamard matrix



Hadamard Groups of order 256 ???

28

```
SUN/UNIX CAYLEY      V3.7.3        Mon Sep 10 1990 20:00:38  STORAGE 200000

library gps256;
Library module found as /usr/local/src/cayley/caylibs/gps256/gps256

 A CAYLEY library for the groups of order 256

 Version 1.0          Date of release May 1989

 E.A. O'Brien
 Department of Mathematics
 Marquette University
 Milwaukee, WI 53233
 USA

 This library contains descriptions for the groups of order 256. The
 stored description for each group can be used to calculate a standard
 power-commutator presentation for the group.
 The organisation of this library is similar to that of the library TWOGPS.
 To obtain a listing of the library contents type CONTENTS;
 To list the topics for which on-line help is available type TOPICS;
 These commands and all other help commands may be used at any stage.
 The library was initially developed at the Department of Mathematics,
 Institute of Advanced Studies, Australian National University.

contents;
    The library contains files storing compact descriptions for the groups
    of order 256. For each d in {2, 6, 7}, there is a file storing the
    descriptions for the groups of order 256 having generator number d.
    These files are called GPSDd. For each d in {3, 4, 5}, there are files
    containing the d-generator groups having exponent-p class c; c runs
    from 2 to at most 6. These files are called GPSDdCc.

    A procedure, GENRAT, is also supplied with the library.
quit;

     END OF RUN.
   0.420 SECONDS
```

Hadamard Groups of order 256 ???

```
28

SUN/UNIX CAYLEY      V3.7.3        Mon Sep 10 1990 20:00:38  STORAGE 200000

library gps256;
Library module found as /usr/local/src/cayley/caylibs/gps256/gps256

 A CAYLEY library for the groups of order 256

 Version 1.0          Date of release May 1989

 E.A. O'Brien
 Department of Mathematics
 Marquette University
 Milwaukee, WI 53233
 USA

 This library contains descriptions for the groups of order 256. The
 stored description for each group can be used to calculate a standard
 power-commutator presentation for the group.
 The organisation of this library is similar to that of the library TWOGPS.
 To obtain a listing of the library contents type CONTENTS;
 To list the topics for which on-line help is available type TOPICS;
 These commands and all other help commands may be used at any stage.
 The library was initially developed at the Department of Mathematics,
 Institute of Advanced Studies, Australian National University.

contents;
    The library contains files storing compact descriptions for the groups
    of order 256. For each d in {2, 6, 7}, there is a file storing the
    descriptions for the groups of order 256 having generator number d.
    These files are called GPSDd. For each d in {3, 4, 5}, there are files
    containing the d-generator groups having exponent-p class c; c runs
    from 2 to at most 6. These files are called GPSDdCc.

    A procedure, GENRAT, is also supplied with the library.
quit;

     END OF RUN.
   0.420 SECONDS
```

56092 groups

Hadamard Groups of order 256 ???

28

```
SUN/UNIX CAYLEY      V3.7.3        Mon Sep 10 1990 20:00:38  STORAGE 200000

library gps256;
Library module found as /usr/local/src/cayley/caylibs/gps256/gps256

 A CAYLEY library for the groups of order 256

 Version 1.0          Date of release May 1989

 E.A. O'Brien
 Department of Mathematics
 Marquette University
 Milwaukee, WI 53233
 USA

 This library contains descriptions for the groups of order 256. The
 stored description for each group can be used to calculate a standard
 power-commutator presentation for the group.
 The organisation of this library is similar to that of the library TWOGPS.
 To obtain a listing of the library contents type CONTENTS;
 To list the topics for which on-line help is available type TOPICS;
 These commands and all other help commands may be used at any stage.
 The library was initially developed at the Department of Mathematics,
 Institute of Advanced Studies, Australian National University.

contents;
    The library contains files storing compact descriptions for the groups
    of order 256. For each d in {2, 6, 7}, there is a file storing the
    descriptions for the groups of order 256 having generator number d.
    These files are called GPSDd. For each d in {3, 4, 5}, there are files
    containing the d-generator groups having exponent-p class c; c runs
    from 2 to at most 6. These files are called GPSDdCc,

    A procedure, GENRAT, is also supplied with the library.
quit;

     END OF RUN.
   0.420 SECONDS
```

56092 groups

Al Schwartz started this project but world-changing events intervened! :(

Hadamard Groups of order 256 ???

28

```
SUN/UNIX CAYLEY      V3.7.3        Mon Sep 10 1990 20:00:38  STORAGE 200000

library gps256;
Library module found as /usr/local/src/cayley/caylibs/gps256/gps256

 A CAYLEY library for the groups of order 256

 Version 1.0          Date of release May 1989

 E.A. O'Brien
 Department of Mathematics
 Marquette University
 Milwaukee, WI 53233
 USA

 This library contains descriptions for the groups of order 256. The
 stored description for each group can be used to calculate a standard
 power-commutator presentation for the group.
 The organisation of this library is similar to that of the library TWOGPS.
 To obtain a listing of the library contents type CONTENTS;
 To list the topics for which on-line help is available type TOPICS;
 These commands and all other help commands may be used at any stage.
 The library was initially developed at the Department of Mathematics,
 Institute of Advanced Studies, Australian National University.

contents;
    The library contains files storing compact descriptions for the groups
    of order 256. For each d in {2, 6, 7}, there is a file storing the
    descriptions for the groups of order 256 having generator number d.
    These files are called GPSDd. For each d in {3, 4, 5}, there are files
    containing the d-generator groups having exponent-p class c; c runs
    from 2 to at most 6. These files are called GPSDdCc.

    A procedure, GENRAT, is also supplied with the library.
quit;

     END OF RUN.
   0.420 SECONDS
```

56092 groups

Al Schwartz started this project but world-changing events intervened! :(

Fewer than 5000 groups left after analogous tests! :)

Chronology of Hadamard groups

prehistory James Singer formally defined difference sets in 1938;

Chronology of Hadamard groups

prehistory James Singer formally defined difference sets in 1938; but Rev. Thomas Kirkman constructed many around 1857.

Chronology of Hadamard groups

prehistory James Singer formally defined difference sets in 1938; but Rev. Thomas Kirkman constructed many around 1857. These were all cyclic difference sets.

Chronology of Hadamard groups

1955 R. H. Bruck: first paper on difference sets in general groups

1955 R. H. Bruck: first paper on difference sets in general groups gave example in $G := \mathbb{Z}_2^4$:

Example 6. Let G be the multiplicative abelian group of order $v = 2^4$, type (2, 2, 2, 2), with generators a, b, c, d, and let D consist of the k = 6 elements a, b, c, d, ab, cd. Then (G, D) is a (16, 6, 2) difference set. Note that the multiplier group is isomorphic to the group of permutations 1, (ab)(cd), (ac)(bd), (ad)(be).

$$D := \{a, b, c, d, ab, cd\}$$

Chronology of Hadamard groups

1955 R. H. Bruck: first paper on difference sets in general groups gave example in $G := \mathbb{Z}_2^4$:

Example 6. Let G be the multiplicative abelian group of order $v = 2^4$, type (2, 2, 2, 2), with generators a, b, c, d, and let D consist of the k = 6 elements a, b, c, d, ab, cd. Then (G, D) is a (16, 6, 2) difference set. Note that the multiplier group is isomorphic to the group of permutations 1, (ab)(cd), (ac)(bd), (ad)(be).

$$D := \{a, b, c, d, ab, cd\}$$

Equivalent to {0000,1000,0100,0010,0001,1111 } in E_{16}

Chronology of Hadamard groups

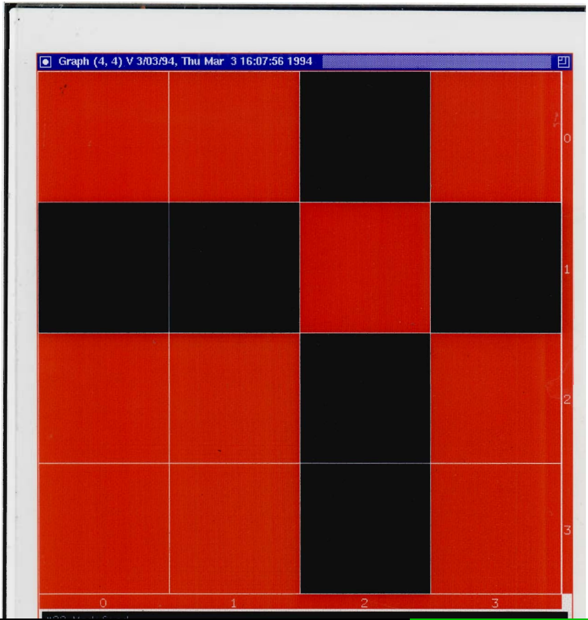
1955 R. H. Bruck: first paper on difference sets in general groups gave example in $G := \mathbb{Z}_2^4$:

Example 6. Let G be the multiplicative abelian group of order $v = 2^4$, type (2, 2, 2, 2), with generators a, b, c, d, and let D consist of the k = 6 elements a, b, c, d, ab, cd. Then (G, D) is a (16, 6, 2) difference set. Note that the multiplier group is isomorphic to the group of permutations 1, (ab)(cd), (ac)(bd), (ad)(be).

$$D := \{a, b, c, d, ab, cd\}$$

Equivalent to {0000,1000,0100,0010,0001,1111 } in E_{16}
but $Dev(D)$ is the $(16, 6, 2)$-design studied by Jordan around 1869

Jordan 4 x 4 Difference Set



Chronology of Hadamard groups

1956 Marshall Hall, Jr.: A Survey of Difference Sets

Chronology of Hadamard groups

1956 Marshall Hall, Jr.: A Survey of Difference Sets
A survey of (v, k, λ) cyclic difference sets, $k \leq 50$

1956 Marshall Hall, Jr.: A Survey of Difference Sets
A survey of (v, k, λ) cyclic difference sets, $k \leq 50$
12 undecided cases included:

Chronology of Hadamard groups

1956 Marshall Hall, Jr.: A Survey of Difference Sets
A survey of (v, k, λ) cyclic difference sets, $k \leq 50$
12 undecided cases included:

$$(36, 15, 6), (64, 28, 12), (100, 45, 20)$$

Chronology of Hadamard groups

1956 Marshall Hall, Jr.: A Survey of Difference Sets
A survey of (v, k, λ) cyclic difference sets, $k \leq 50$
12 undecided cases included:

$$(36, 15, 6), (64, 28, 12), (100, 45, 20)$$

Note: $v = 4n$

Chronology of Hadamard groups

1956 Marshall Hall, Jr.: A Survey of Difference Sets
A survey of (v, k, λ) cyclic difference sets, $k \leq 50$
12 undecided cases included:

$$(36, 15, 6), (64, 28, 12), (100, 45, 20)$$

Note: $v = 4n$ These would give circulant Hadamard matrices! :)

Chronology of Hadamard groups

1960-62 P. Kesava Menon:

Chronology of Hadamard groups

1960-62 P. Kesava Menon:
1960

- Formally introduced characters to prove Multiplier Theorem for abelian groups.

Chronology of Hadamard groups

1960-62 P. Kesava Menon:
1960

- Formally introduced characters to prove Multiplier Theorem for abelian groups.
- General construction for ds in $G = \mathbb{Z}_2^{2s+2}$

Chronology of Hadamard groups

1960-62 P. Kesava Menon:
1960

- Formally introduced characters to prove Multiplier Theorem for abelian groups.
- General construction for ds in $G = \mathbb{Z}_2^{2s+2} := E_{2^{s+2}}$:

1960-62 P. Kesava Menon:
1960

- Formally introduced characters to prove Multiplier Theorem for abelian groups.
- General construction for ds in $G = \mathbb{Z}_2^{2s+2} := E_{2^{s+2}}$:
- $D := \{v \in G | wt(v) = 0, 1 \pmod 4\}$

Chronology of Hadamard groups

1960-62 P. Kesava Menon:
1960

- Formally introduced characters to prove Multiplier Theorem for abelian groups.
- General construction for ds in $G = \mathbb{Z}_2^{2s+2} := E_{2^{s+2}}$:
- $D := \{v \in G | wt(v) = 0, 1 \pmod 4\}$

1962 Formally studied ds with $v = 4n$ and proved:

Chronology of Hadamard groups

1960-62 P. Kesava Menon:
1960

- Formally introduced characters to prove Multiplier Theorem for abelian groups.
- General construction for ds in $G = \mathbb{Z}_2^{2s+2} := E_{2^{s+2}}$:
- $D := \{v \in G | wt(v) = 0, 1 \pmod 4)\}$

1962 Formally studied ds with $v = 4n$ and proved:

- $(v, k, \lambda) = (4N^2, 2N^2 - N, N^2 - N)$;

Chronology of Hadamard groups

1960-62 P. Kesava Menon:
1960

- Formally introduced characters to prove Multiplier Theorem for abelian groups.
- General construction for ds in $G = \mathbb{Z}_2^{2s+2} := E_{2^{s+2}}$:
- $D := \{v \in G | wt(v) = 0, 1 \pmod 4)\}$

1962 Formally studied ds with $v = 4n$ and proved:

- $(v, k, \lambda) = (4N^2, 2N^2 - N, N^2 - N)$;
- $\mathcal{H}$ contains $\mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2$,

Chronology of Hadamard groups

1960-62 P. Kesava Menon:
1960

- Formally introduced characters to prove Multiplier Theorem for abelian groups.
- General construction for ds in $G = \mathbb{Z}_2^{2s+2} := E_{2^{s+2}}$:
- $D := \{v \in G | wt(v) = 0, 1 \pmod 4\}$

1962 Formally studied ds with $v = 4n$ and proved:

- $(v, k, \lambda) = (4N^2, 2N^2 - N, N^2 - N)$;
- $\mathcal{H}$ contains $\mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_6 \times \mathbb{Z}_6$,

Chronology of Hadamard groups

1960-62 P. Kesava Menon:
1960

- Formally introduced characters to prove Multiplier Theorem for abelian groups.
- General construction for ds in $G = \mathbb{Z}_2^{2s+2} := E_{2^{s+2}}$:
- $D := \{v \in G | wt(v) = 0, 1 \pmod 4)\}$

1962 Formally studied ds with $v = 4n$ and proved:

- $(v, k, \lambda) = (4N^2, 2N^2 - N, N^2 - N)$;
- $\mathcal{H}$ contains $\mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_6 \times \mathbb{Z}_6$, $D_6 \times D_6$.

Chronology of Hadamard groups

1960-62 P. Kesava Menon:
1960

- Formally introduced characters to prove Multiplier Theorem for abelian groups.
- General construction for ds in $G = \mathbb{Z}_2^{2s+2} := E_{2^{s+2}}$:
- $D := \{v \in G | wt(v) = 0, 1 \pmod 4)\}$

1962 Formally studied ds with $v = 4n$ and proved:

- $(v, k, \lambda) = (4N^2, 2N^2 - N, N^2 - N)$;
- $\mathcal{H}$ contains $\mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_6 \times \mathbb{Z}_6$, $D_6 \times D_6$.
- $\mathcal{H}$ is closed under direct product.

PRODUCT THEOREM. $H_1, H_2 \in \mathcal{H}$

$H_1, H_2 \leq G$, $G = H_1 H_2$, $H_1 \cap H_2 = 1$

Then $G \in \mathcal{H}$.

Proof. Let D_i be a difference set in H_i.

Define $D \subseteq G = H_1 H_2$ by

$$D^* = D_1^* D_2^* .$$

Then
$$\begin{aligned} D^* D^{*(-1)} &= (D_1^* D_2^*)(D_1^* D_2^*)^{(-1)} \\ &= D_1^* D_2^* D_2^{*(-1)} D_1^{*(-1)} \\ &= D_1^* |H_2| D_1^{*(-1)} \\ &= D_1^* D_1^{*(-1)} |H_2| \\ &= |H_1||H_2| \\ &= |G|. \end{aligned}$$
QED.

How about $D^* = (-1+a+b+c)\Delta^*$

where $G = H + aH + bH + cH$, $H \in \mathcal{H}$

?

$$D^* D^{*(-1)} = (-1+a+b+c)\Delta^* \Delta^{*(-1)}(-1+a^{-1}+b^{-1}+c^{-1})$$

$$= |H|(-1+a+b+c)(-1+a^{-1}+b^{-1}+c^{-1})$$

$$= |H| \begin{Bmatrix} 4 & -a + ba^{-1} + cb^{-1} - c^{-1} \\ & -b + ca^{-1} - b^{-1} + ac^{-1} \\ & -c - a^{-1} + ab^{-1} + bc^{-1} \end{Bmatrix}$$

$\therefore$ D is a Hadamard difference set iff

$$\{ba^{-1}, ca^{-1}, cb^{-1}\} = \{a^{\pm 1}, b^{\pm 1}, c^{\pm 1}\}$$

Theorem (Generalized Products)

$G \in \mathcal{H}$ if 1) $G = Q_8 H$

or 2) $a^2 = 1$, $ab = ba$

$G = \langle a, b \rangle H$.

SR 3

Chronology of Hadamard groups

1965 Richard J. Turyn

- Motivated by $v = 4n$ (group-developed Hadamard matrices);

1965 Richard J. Turyn

- Motivated by $v = 4n$ (group-developed Hadamard matrices); called the ds H-sets

Chronology of Hadamard groups

1965 Richard J. Turyn

- Motivated by $v = 4n$ (group-developed Hadamard matrices); called the ds H-sets
- Says of Menon *"The connection with Hadamard matrices is mentioned in neither paper."*

Chronology of Hadamard groups

1965 Richard J. Turyn

- Motivated by $v = 4n$ (group-developed Hadamard matrices); called the ds H-sets
- Says of Menon *"The connection with Hadamard matrices is mentioned in neither paper."*
- $\mathbb{Z}_8 \times \mathbb{Z}_2 \in \mathcal{H}$

Chronology of Hadamard groups

1965 Richard J. Turyn

- Motivated by $v = 4n$ (group-developed Hadamard matrices); called the ds H-sets
- Says of Menon *"The connection with Hadamard matrices is mentioned in neither paper."*
- $\mathbb{Z}_8 \times \mathbb{Z}_2 \in \mathcal{H}$
- characteristic artistry finished off Hall's undecided and many noncyclic ds as well

Chronology of Hadamard groups

1965 Richard J. Turyn

- Motivated by $v = 4n$ (group-developed Hadamard matrices); called the ds H-sets
- Says of Menon *"The connection with Hadamard matrices is mentioned in neither paper."*
- $\mathbb{Z}_8 \times \mathbb{Z}_2 \in \mathcal{H}$
- characteristic artistry finished off Hall's undecided and many noncyclic ds as well
- in particular . . .

The only known nonexistence criterion for 2-groups

Theorem (R. J. Turyn, JFD dihedral trick)

G of order 2^{2s+2} is NOT Hadamard if G/K is cyclic or dihedral of order greater than 2^{s+2}.

The only known nonexistence criterion for 2-groups

Theorem (R. J. Turyn, JFD dihedral trick)

G of order 2^{2s+2} is NOT Hadamard if G/K is cyclic or dihedral of order greater than 2^{s+2}.

$s = 1$, $|G| = 16$: 2 groups ruled out: $\mathbb{Z}_{16}$ and D_{16}.

The only known nonexistence criterion for 2-groups

Theorem (R. J. Turyn, JFD dihedral trick)

G of order 2^{2s+2} is NOT Hadamard if G/K is cyclic or dihedral of order greater than 2^{s+2}.

$s = 1$, $|G| = 16$: 2 groups ruled out: $\mathbb{Z}_{16}$ and D_{16}.
$s = 2$, $|G| = 64$: 8 groups ruled out

The only known nonexistence criterion for 2-groups

Theorem (R. J. Turyn, JFD dihedral trick)

G of order 2^{2s+2} is NOT Hadamard if G/K is cyclic or dihedral of order greater than 2^{s+2}.

$s = 1$, $|G| = 16$: 2 groups ruled out: $\mathbb{Z}_{16}$ and D_{16}.
$s = 2$, $|G| = 64$: 8 groups ruled out
$s = 3$, $|G| = 256$: 43 groups ruled out

The only known nonexistence criterion for 2-groups

Theorem (R. J. Turyn, JFD dihedral trick)

G of order 2^{2s+2} is NOT Hadamard if G/K is cyclic or dihedral of order greater than 2^{s+2}.

$s = 1$, $|G| = 16$: 2 groups ruled out: $\mathbb{Z}_{16}$ and D_{16}.
$s = 2$, $|G| = 64$: 8 groups ruled out
$s = 3$, $|G| = 256$: 43 groups ruled out
$\{1, 371, 406, 432, 438, 448, 459, 497, 500, 525,$
526, 527, 528, 529, 530, 531, 533, 534, 535, 537,
538, 539, 540, 541, 6601, 6619, 6637, 6649, 6673, 6682,
6691, 6699, 6707, 6713, 6719, 6723, 6726, 6727, 6728, 6729,
6730, 6731, 26963 $\}$

JFD MH talk (1990):Hadamard Groups of order 64

Theorem (RJ Turyn)
$G \in \mathcal{H}$, $|G| = 2^{2s+2}$, $K \triangleleft G$, G/K cyclic.
Then $|K| \geqslant 2^s$ and $|G/K| \leqslant 2^{s+2}$.

Cor (Turyn's Exponent Bound)
G abelian $\Longrightarrow$ $\exp(G) \leqslant 2^{s+2}$.
$(|G| = 64 \Longrightarrow \exp(G) \leqslant 16)$

Theorem. The above result is true if "cyclic" is replaced by "dihedral".

Proof (The "dihedral trick"). H abelian, $G = \langle H, g : g^2 = 1, ghg^{-1} = h^{-1} \rangle$
$G = H + gH$. Suppose $\mathcal{F}\mathcal{F}^{(-1)} = 2^{2s+2}$, $\mathcal{F} \in \mathbb{Z}G$.
$2^{2s+2} = \mathcal{F}\mathcal{F}^{(-1)} = (\mathcal{A} + g\mathcal{B})(\mathcal{A} + g\mathcal{B})^{(-1)} = \mathcal{A}\mathcal{A}^{(-1)} + \mathcal{B}\mathcal{B}^{(-1)} + 2g\mathcal{B}\mathcal{A}^{(-1)}$.
$\Longrightarrow \mathcal{B}\mathcal{A}^{(-1)} = 0$ AND $\mathcal{A}\mathcal{A}^{(-1)} + \mathcal{B}\mathcal{B}^{(-1)} = 2^{2s+2}$.
Now if $\mathcal{G}$ is <u>any</u> abelian group with $[\mathcal{G} : H] = 2$
say $\mathcal{G} = H + \theta H$. Define $\mathcal{E} = \mathcal{A} + \theta\mathcal{B}$.
Then $\mathcal{E}\mathcal{E}^{(-1)} = \mathcal{A}\mathcal{A}^{(-1)} + \mathcal{B}\mathcal{B}^{(-1)} = 2^{2s+2}$. QED (!)

1973 R. L. McFarland: $G = K \times E_{q^{s+1}}$, $|K| = 1 + \frac{q^{s+1}-1}{q-1}$, K any!

Chronology of Hadamard groups

1973 R. L. McFarland: $G = K \times E_{q^{s+1}}$, $|K| = 1 + \frac{q^{s+1}-1}{q-1}$, K any!
$q = 2$ gives $K \times E_{2^{s+1}} \in \mathcal{H}$, $|E| = |K| = 2^{s+1}$, E e.a., K any.

Chronology of Hadamard groups

1973 R. L. McFarland: $G = K \times E_{q^{s+1}}$, $|K| = 1 + \frac{q^{s+1}-1}{q-1}$, K any!
$q = 2$ gives $K \times E_{2^{s+1}} \in \mathcal{H}$, $|E| = |K| = 2^{s+1}$, E e.a., K any.
$K = E$ gives bent functions constructed earlier by O. S. Rothaus and J. A. Maiorana

$$[D^*(x,y)] := \Delta^* P\,[(-1)^{x \cdot y}] = \Delta^* P \otimes^{s+1} \begin{bmatrix} 1 & 1 \\ 1 & - \end{bmatrix}$$

Family M (aka Maiorana-McFarland): $f(x,y) := \pi(x) \cdot y + g(x)$

Chronology of Hadamard groups

1973 R. L. McFarland: $G = K \times E_{q^{s+1}}$, $|K| = 1 + \frac{q^{s+1}-1}{q-1}$, K any!
$q = 2$ gives $K \times E_{2^{s+1}} \in \mathcal{H}$, $|E| = |K| = 2^{s+1}$, E e.a., K any.
$K = E$ gives bent functions constructed earlier by O. S. Rothaus and J. A. Maiorana

$$[D^*(x,y)] := \Delta^* P\,[(-1)^{x\cdot y}] = \Delta^* P \otimes^{s+1} \begin{bmatrix} 1 & 1 \\ 1 & - \end{bmatrix}$$

Family M (aka Maiorana-McFarland): $f(x,y) := \pi(x)\cdot y + g(x)$
$K = \mathbb{Z}_{2^{s+1}}$ gives $\mathbb{Z}_{2^{s+1}} \times E_{2^{s+1}} \in \mathcal{H}$

JFD MH talk (1990):Hadamard Groups of order 64

4

ORTHOGONAL PIECES

$|G| = 2^{2s+2}$ $\quad E \equiv E_{2^{s+1}} \cong \mathbb{Z}_2^{s+1} \leq G.$

$$G = \sum_{i=0}^{2^{s+1}-1} g_i E \quad .$$

$\chi_0, \chi_1, \ldots \chi_{2^{s+1}-1}$ characters of E.

Define $D^* = \sum_{i=0}^{2^{s+1}-1} g_i \chi_i$.

Then $D^* D^{*(-1)} = \sum_{i,j} (g_i \chi_i)(g_j \chi_j)^{(-1)}$

$$= \sum_{i,j} g_i \chi_i \chi_j g_j^{-1}$$

$$= 2^{s+1} \sum_i g_i \chi_i g_i^{-1}$$

Theorem If $E_{2^{s+1}} \leq Z(G)$, then $G \in \mathcal{H}$

Cor. $\mathbb{Z}_2^s \times \mathbb{Z}_{2^{s+2}} \in \mathcal{H}$

Cor. Turyn's bound sharp for all s.

example: Suzuki$_{64} \in \mathcal{H}$.

CONJECTURE ?

The Conjecture is TRUE! :)

Apr 9 12:43 1997 standard input Page 1

Art Drisko proved the combinatorial

THEOREM. Any (2n-1) x n array with no repeats in any row has a transversal;
i.e. there are n distinct entries no two in the same row or column.

COROLLARY. Dillon's "transversal conjecture" is TRUE! i.e.

COROLLARY. If a group G of order 2^m acts by automorphisms on an elementary
abelian group E of order 2^m, then there exists a bijection

pi: E --> G

such that {e^(pi(e)): e in E } = E.

COROLLARY. Let G be a group of invertible 2^m x 2^m matrices over F_2 and
let M be the 2^m x 2^m array whose rows (resp columns) are
indexed by the elements of G (resp. V = (F_2)^m) and whose
(g,v)^th entry is gv.
Then M has a transversal.

COROLLARY. Every group of order 4^m which has a normal elementary abelian
subgroup of order 2^m has a (Hadamard) difference set.

What a great result!...it'll be fun to think up other applications!

cheers,
jfd

1987

- Jim Davis: $\mathbb{Z}_{2^{s+1}} \times \mathbb{Z}_{2^{s+1}}$, $\mathbb{Z}_{2^s} \times \mathbb{Z}_{2^{s+2}} \in \mathcal{H}$.

Chronology of Hadamard groups

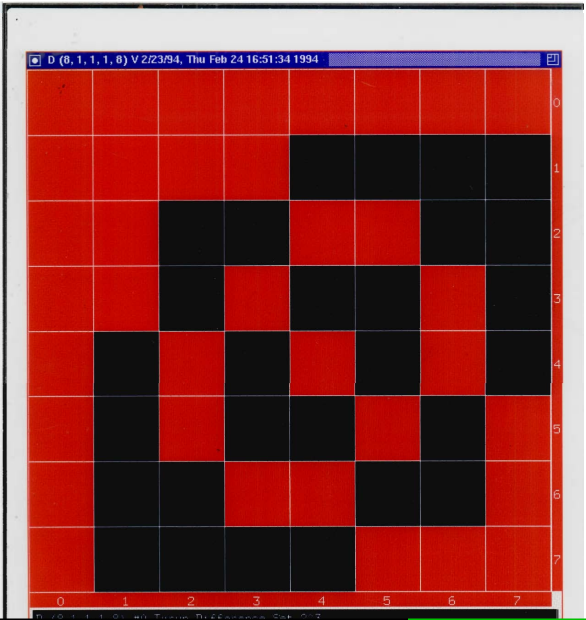
1987

- Jim Davis: $\mathbb{Z}_{2^{s+1}} \times \mathbb{Z}_{2^{s+1}}$, $\mathbb{Z}_{2^s} \times \mathbb{Z}_{2^{s+2}} \in \mathcal{H}$.
- RJT Robert Kraemer: Abelian Hadamard 2-groups are characterized as those meeting Turyn's exponent bound.

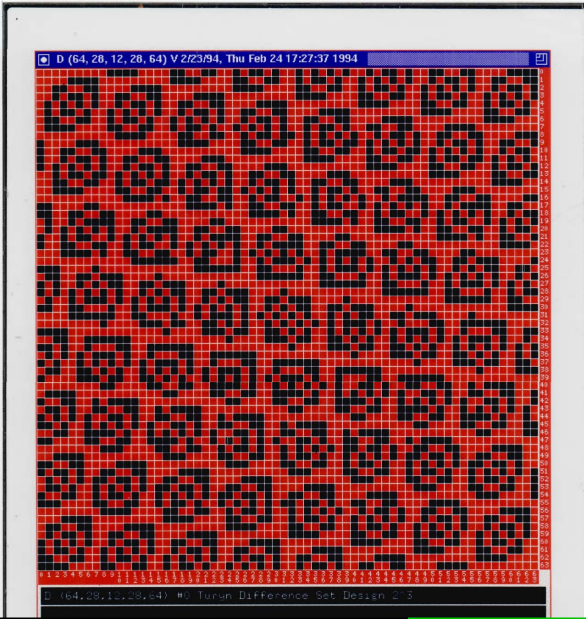
1987

- Jim Davis: $\mathbb{Z}_{2^{s+1}} \times \mathbb{Z}_{2^{s+1}}$, $\mathbb{Z}_{2^s} \times \mathbb{Z}_{2^{s+2}} \in \mathcal{H}$.
- RJT Robert Kraemer: Abelian Hadamard 2-groups are characterized as those meeting Turyn's exponent bound.
- RJT JFD: simple construction.

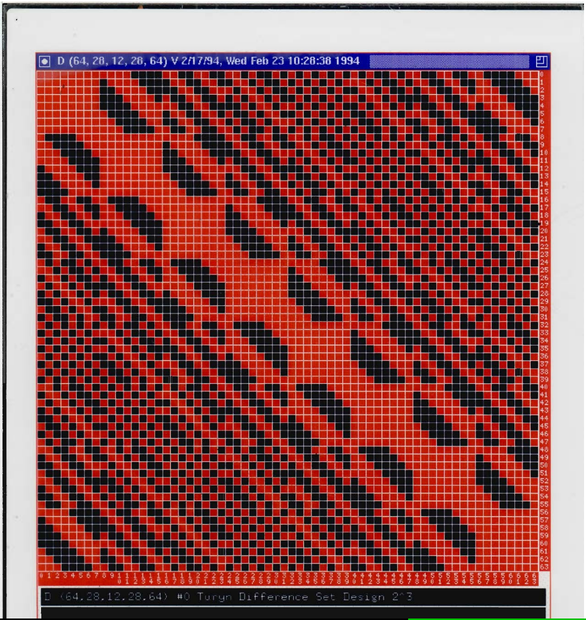
Turyn $\mathbb{Z}_8 \times \mathbb{Z}_8$ difference set



Turyn $\mathbb{Z}_8 \times \mathbb{Z}_8$ ds Hadamard matrix



Turyn $\mathbb{Z}_8 \times \mathbb{Z}_8$ ds Hadamard matrix .2



JFD Generalization

12

(JFD 87) $G = H \times H$,

$H = Z_{2^{s+1}} = \{0,1,2, \ldots, 2^{s+1}-1\}$

$f^*: H \to \{1,-1\}, f^*(x+2^s) = -f^*(x)$

$\Pi: H \to H, \Pi(2^r t) = 2^r t^{-1}$, t odd

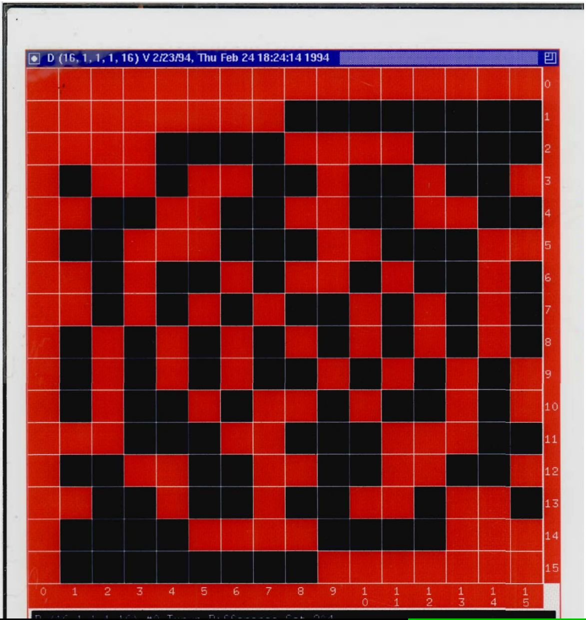
$D = \{(x,y): f^*(\Pi(x)y) = -1\}$ is a DS fixed by -1.

Exp many inequiv DS in G

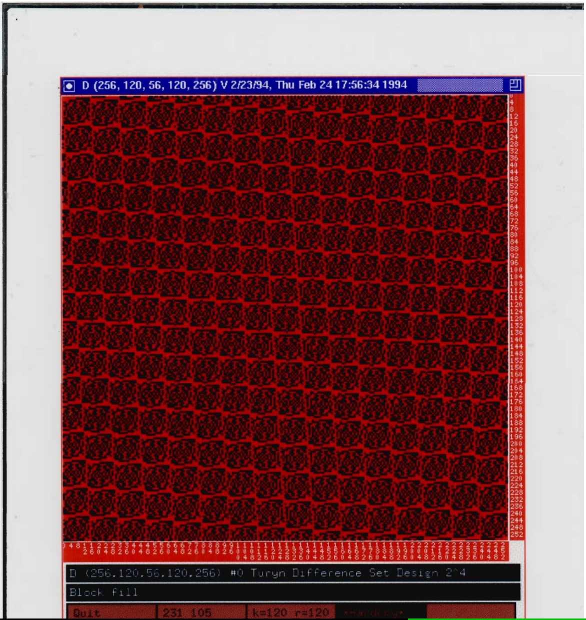
e.g. f(x)="high order bit" of x

s=2 coincides with RJT

JFD $\mathbb{Z}_{16} \times \mathbb{Z}_{16}$ difference set



JFD $\mathbb{Z}_{16} \times \mathbb{Z}_{16}$ Hadamard



JFD $\mathbb{Z}_{16} \times \mathbb{Z}_{16}$ Hadamard .2

JFD MH talk (1990):Hadamard Groups of order 64

TRANSFER OF $\mathbb{Z}_8 \times \mathbb{Z}_8$ d.s. TO OTHER GROUPS.

$$\underset{\mathbb{Z}_8\times\mathbb{Z}_8}{G=\langle a\rangle\times\langle b\rangle} > \underset{\mathbb{Z}_4\times\mathbb{Z}_8}{H=\langle a^2\rangle\times\langle b\rangle} > \underset{\mathbb{Z}_4\times\mathbb{Z}_4}{K=\langle a^2\rangle\times\langle b^2\rangle} > \underset{\mathbb{Z}_2\times\mathbb{Z}_2}{E=\langle a^4\rangle\times\langle b^4\rangle}$$

$$G = K + bK + aK + abK$$

$$D^* = \Delta_0^* + b\Delta_1^* + a\Delta_2^* + ab\Delta_3^*$$

FACTS: $\Delta_i^* \Delta_j^{*(-1)} = 0 \quad \forall i \neq j$

$\Delta_i^* \Delta_i^{*(-1)} = 16\,\chi_i \quad , 0 \le i \le 3,$

where χ_i's are characters of $E \equiv E_4$.

Also $G = H + aH$

$D^* = A^* + aB^*$

where $A^* = \Delta_0^* + b\Delta_1^*$ and $B^* = \Delta_2^* + b\Delta_3^*$

$$\therefore \left.\begin{array}{l} A^*A^{*(-1)} = 32(1+b^4) \\ B^*B^{*(-1)} = 32(1-b^4) \\ A^*B^{*(-1)} = 0\,. \end{array}\right\} \begin{array}{l} D^*D^{*(-1)} = A^*A^{*(-1)} + B^*B^{*(-1)} \\ = 64. \end{array}$$

Note: $\langle b^4\rangle$ char H.

JFD MH talk (1990):Hadamard Groups of order 64

23

$$[\mathcal{G}:K]=4 \qquad K \lhd \mathcal{G}.$$

$$\mathcal{G} = \sum g_i K$$

Define $\mathcal{D}^* = \sum g_i \Delta_i^*$

Then $\mathcal{D}^*\mathcal{D}^{*(-1)} = \sum g_i \Delta_i^* \Delta_i^{*(-1)} g_i^{-1}$

$$= 16 \sum g_i \chi_i g_i^{-1}$$

But $K \lhd \mathcal{G} \Rightarrow E \lhd \mathcal{G} \Rightarrow \mathcal{G}/K$ acts on E

$|\mathcal{G}/K| = 4 = |E| \Rightarrow \exists$ transversal i.e.

$$\{g_i \chi_i g_i^{-1}\} = \{\chi_i\}$$

$\therefore \mathcal{D}^*\mathcal{D}^{*(-1)} = 16 \sum \chi_i = 16 \cdot 4 = 64.$

Theorem. $\mathbb{Z}_4 \times \mathbb{Z}_4 \lhd G_{64} \Rightarrow G_{64} \in \mathcal{H}$.

SRC

Chronology of Hadamard groups

1990 Marshall Hall Conference.

1991-1997

- Smith-Liebler: $M_{64} \in \mathcal{H}$

Chronology of Hadamard groups

1991-1997

- Smith-Liebler: $M_{64} \in \mathcal{H}$
- Davis-Smith: $\mathbb{Z}_{2^{s+3}} \rtimes_{2^{s+2}+1} \mathbb{Z}_{2^{s-1}} \in \mathcal{H}$

Chronology of Hadamard groups

1991-1997

- Smith-Liebler: $M_{64} \in \mathcal{H}$
- Davis-Smith: $\mathbb{Z}_{2^{s+3}} \rtimes_{2^{s+2}+1} \mathbb{Z}_{2^{s-1}} \in \mathcal{H}$
- Davis-Iiams: $\mathbb{Z}_{2^{3t+2}} \rtimes_{2^{2t+2}+1} \mathbb{Z}_{2^t} \in \mathcal{H}$

Chronology of Hadamard groups

1991-1997

- Smith-Liebler: $M_{64} \in \mathcal{H}$
- Davis-Smith: $\mathbb{Z}_{2^{s+3}} \rtimes_{2^{s+2}+1} \mathbb{Z}_{2^{s-1}} \in \mathcal{H}$
- Davis-Iiams: $\mathbb{Z}_{2^{3t+2}} \rtimes_{2^{2t+2}+1} \mathbb{Z}_{2^{t}} \in \mathcal{H}$
- Iiams, Davis-Jedwab, et al

Hadamard Groups of order 64 redux

Status Report for $|G| = 64$

Test	Hadamard	non-Hadamard	?
Start	—	—	267

Status Report for $|G| = 64$

Test	Hadamard	non-Hadamard	?
Start	—	—	267
TBDT	—	8	259

Hadamard Groups of order 64 redux

Status Report for $|G| = 64$

Test	Hadamard	non-Hadamard	?
Start	—	—	267
TBDT	—	8	259
$H4H16$	166	8	93

Hadamard Groups of order 64 redux

Status Report for $|G| = 64$

Test	Hadamard	non-Hadamard	?
Start	—	—	267
TBDT	—	8	259
$H4H16$	166	8	93
$[G : H] = 4$	233	8	26

Hadamard Groups of order 64 redux

Status Report for $|G| = 64$

Test	Hadamard	non-Hadamard	?
Start	—	—	267
TBDT	—	8	259
$H4H16$	166	8	93
$[G : H] = 4$	233	8	26
transfers	258	8	1

Hadamard Groups of order 64 redux

Status Report for $|G| = 64$

Test	Hadamard	non-Hadamard	?
Start	—	—	267
TBDT	—	8	259
$H4H16$	166	8	93
$[G : H] = 4$	233	8	26
transfers	258	8	1
M_{64}	259	8	0

Hadamard Groups of order 64 redux

Status Report for $|G| = 64$

Test	Hadamard	non-Hadamard	?
Start	—	—	267
TBDT	—	8	259
$H4H16$	166	8	93
$[G:H] = 4$	233	8	26
transfers	258	8	1
M_{64}	259	8	0

Contributors include Jim Davis, Ken Smith

Hadamard Groups of order 64 redux

Status Report for $|G| = 64$

Test	Hadamard	non-Hadamard	?
Start	—	—	267
TBDT	—	8	259
$H4H16$	166	8	93
$[G : H] = 4$	233	8	26
transfers	258	8	1
M_{64}	259	8	0

Contributors include Jim Davis, Ken Smith and Bob Liebler!

Thanks for help!:

Hadamard Groups of order 256 ???

Thanks for help!: Al Schwartz

Hadamard Groups of order 256 ???

Thanks for help!: Al Schwartz Joe Bohanon

Hadamard Groups of order 256 ???

Thanks for help!: Al Schwartz Joe Bohanon

Status Report for $|G| = 256$

Test	Hadamard	non-Hadamard	?
Start	—	—	56092

Hadamard Groups of order 256 ???

Thanks for help!: Al Schwartz Joe Bohanon

Status Report for $|G| = 256$

Test	Hadamard	non-Hadamard	?
Start	—	—	56092
TBDT	—	43	56049

Hadamard Groups of order 256 ???

Thanks for help!: Al Schwartz Joe Bohanon

Status Report for $|G| = 256$

Test	Hadamard	non-Hadamard	?
Start	—	—	56092
TBDT	—	43	56049
$E_{16} \triangleleft G$	42268	43	13781

Hadamard Groups of order 256 ???

Thanks for help!: Al Schwartz Joe Bohanon

Status Report for $|G| = 256$

Test	Hadamard	non-Hadamard	?
Start	—	—	56092
TBDT	—	43	56049
$E_{16} \triangleleft G$	42268	43	13781
$H4H64$	48921	43	7128

Hadamard Groups of order 256 ???

Thanks for help!: Al Schwartz Joe Bohanon

Status Report for $|G| = 256$

Test	Hadamard	non-Hadamard	?
Start	—	—	56092
TBDT	—	43	56049
$E_{16} \lhd G$	42268	43	13781
$H4H64$	48921	43	7128
$H16H16$	51752	43	4297

Hadamard Groups of order 256 ???

Thanks for help!: Al Schwartz Joe Bohanon

Status Report for $|G| = 256$

Test	Hadamard	non-Hadamard	?
Start	—	—	56092
TBDT	—	43	56049
$E_{16} \lhd G$	42268	43	13781
$H4H64$	48921	43	7128
$H16H16$	51752	43	4297
$[G : H] = 4$	55254	43	795

Hadamard Groups of order 256 ???

Thanks for help!: Al Schwartz Joe Bohanon

Status Report for $|G| = 256$

Test	Hadamard	non-Hadamard	?
Start	—	—	56092
TBDT	—	43	56049
$E_{16} \lhd G$	42268	43	13781
$H4H64$	48921	43	7128
$H16H16$	51752	43	4297
$[G : H] = 4$	55254	43	795
transfers	?	43	?

Hadamard Groups of order 256 ???

Thanks for help!: Al Schwartz Joe Bohanon

Status Report for $|G| = 256$

Test	Hadamard	non-Hadamard	?
Start	—	—	56092
TBDT	—	43	56049
$E_{16} \triangleleft G$	42268	43	13781
$H4H64$	48921	43	7128
$H16H16$	51752	43	4297
$[G : H] = 4$	55254	43	795
transfers	?	43	?
regs	?	43	?

A modest proposal

A modest proposal

Let's all work together on this!

A modest proposal

Let's all work together on this!

- Surely there are known results/techniques I have not yet incorporated

A modest proposal

Let's all work together on this!

- Surely there are known results/techniques I have not yet incorporated e.g. Davis-Jedwab "building sets, etc."

A modest proposal

Let's all work together on this!

- Surely there are known results/techniques I have not yet incorporated e.g. Davis-Jedwab "building sets, etc."
- Surely when we look at the groups that are left we will discover new theorems!

A modest proposal

Let's all work together on this!

- Surely there are known results/techniques I have not yet incorporated e.g. Davis-Jedwab "building sets, etc."
- Surely when we look at the groups that are left we will discover new theorems!
- Such work could well lead to a complete classification of Hadamard 2-groups!

A modest proposal

Let's all work together on this!

- Surely there are known results/techniques I have not yet incorporated e.g. Davis-Jedwab "building sets, etc."
- Surely when we look at the groups that are left we will discover new theorems!
- Such work could well lead to a complete classification of Hadamard 2-groups!
- Let's do it to honor the memory of Bob Liebler! :)

Acknowledgments

Thanks to . . .

Acknowledgments

Thanks to . . .

- Allan Schwartz

Acknowledgments

Thanks to . . .

- Allan Schwartz for the beautiful matrices! :)

Acknowledgments

Thanks to ...

- Allan Schwartz for the beautiful matrices! :)
- John Cannon and MAGMA :)

Acknowledgments

Thanks to . . .

- Allan Schwartz for the beautiful matrices! :)
- John Cannon and MAGMA :)
- Joe Bohanon

Acknowledgments

Thanks to . . .

- Allan Schwartz for the beautiful matrices! :)
- John Cannon and MAGMA :)
- Joe Bohanon for independently checking the SmallGroups! :)