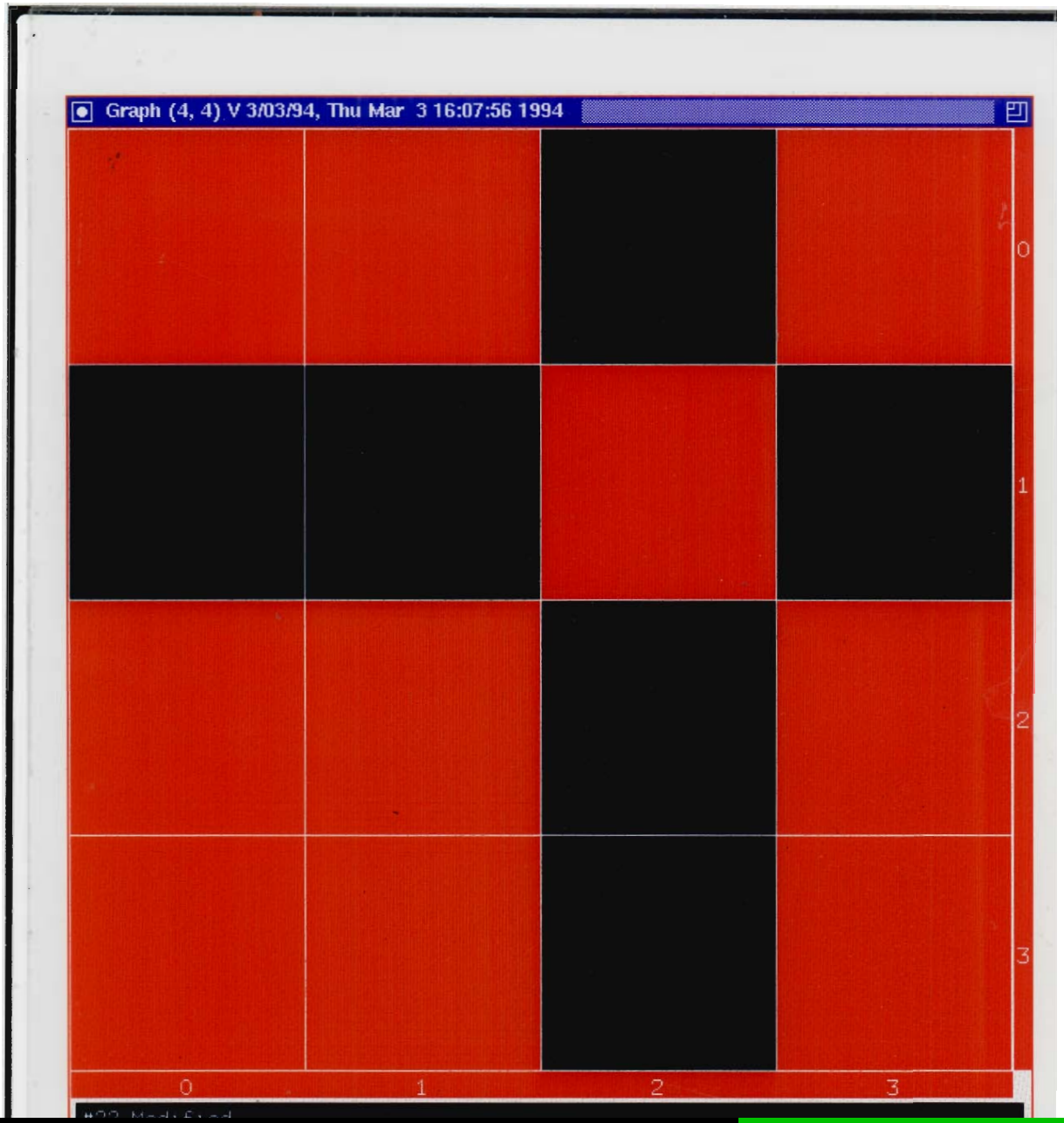
Some *REALLY* Beautiful Hadamard Matrices

J. F. Dillon

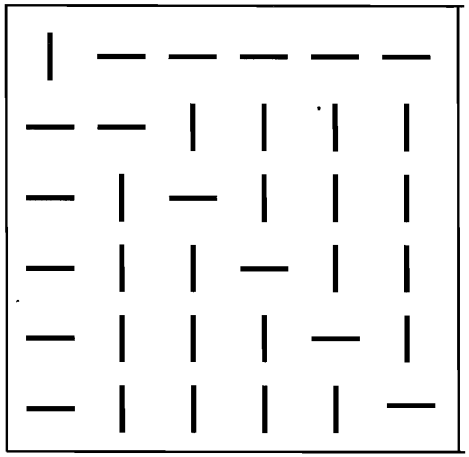
National Security Agency
Fort George G. Meade, MD USA

International Conference on Design Theory and Applications
National University of Ireland, Galway
July 2009

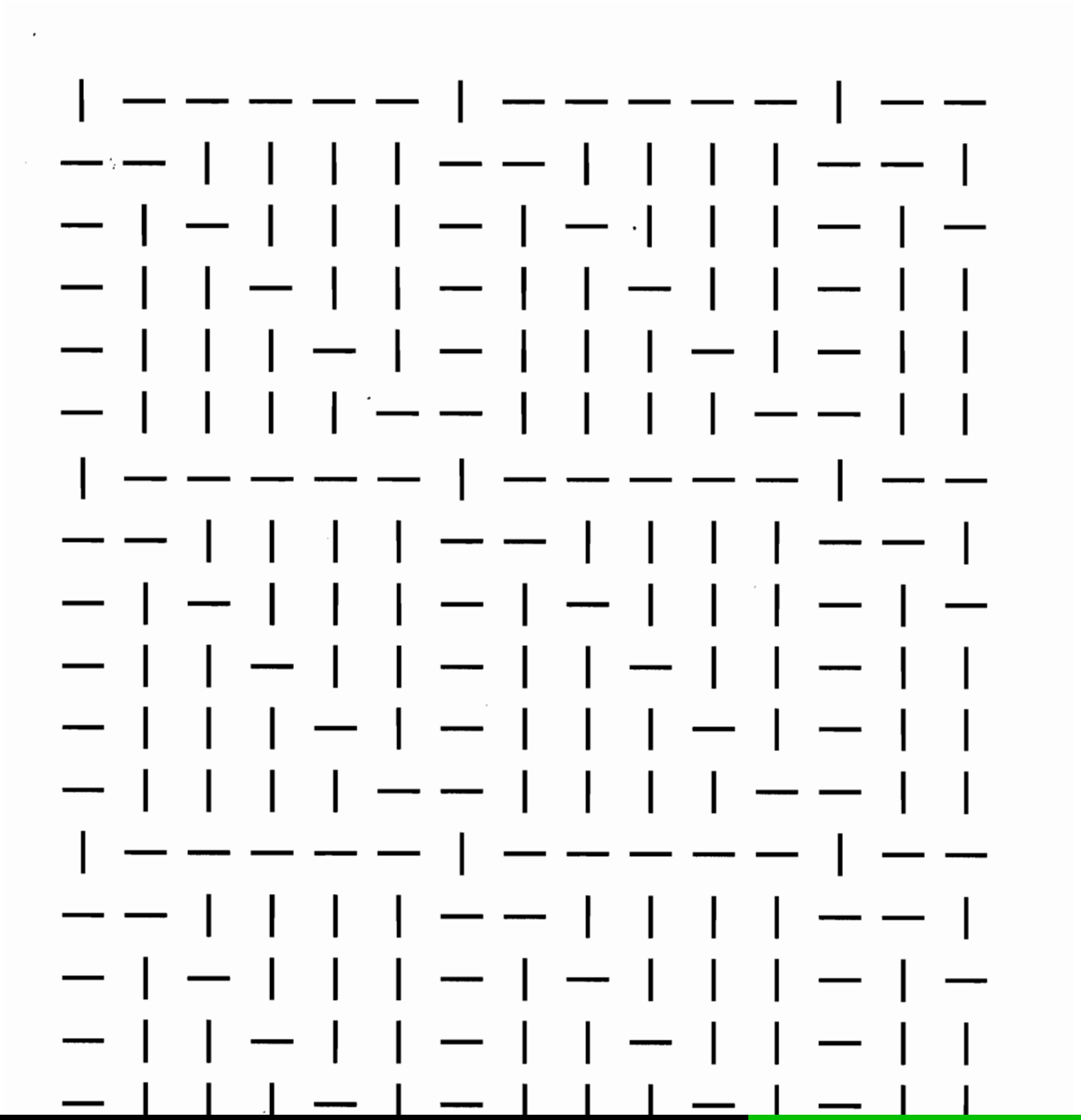
Jordan 4 x 4 Difference Set



$\mathbb{Z}_6 \times \mathbb{Z}_6$ Difference Set



$\mathbb{Z}_6 \times \mathbb{Z}_6$ DS Tiling



Partial Spreads

Partial Spreads

(JFD 74) $|G|=4N^2$
$H_1, H_2, \ldots, H_N \leq G$
$|H_i| = 2N; \quad |H_i \cap H_j| = 1.$

$D= \Sigma(H_i - 1)$ is a Hadamard DS

e.g.N=2; $G=Z_4 \times Z_4$
"Jordan" DS

N=3; $G=Z_6 \times Z_6$ or $S_3 \times S_3$
x=0; y=0; y=x

$N=2^{m-1}; G=Z_2^{2m} = L^2, L=F_2m$
Lines thru origin in $AG(2,2^m)$
(WMK) Exp many inequiv DS

Hadamard difference sets

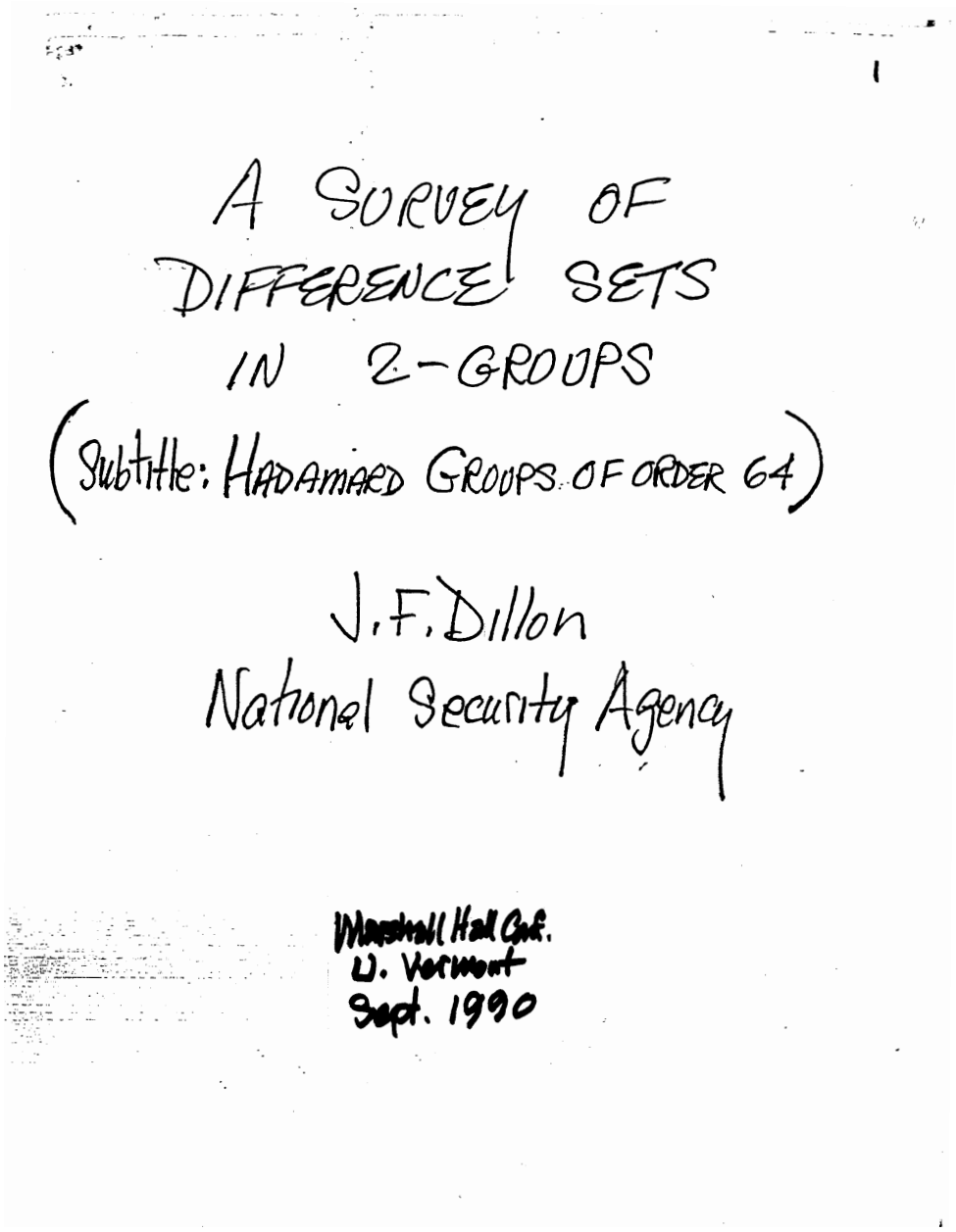
$(v, k, \lambda)=(4N^2, 2N^2\text{-}N, N^2\text{-}N)$

N=1 $(v, k, \lambda)=(4, 1, 0)$
Trivial

N=2 $(v, k, \lambda)=(16, 6, 2)$
14 groups; Z_{16}, $D_{16} \notin \mathcal{H}$
3 inequivalent designs
2-ranks 6,7,8;all regular
Jordan "miracle"

N=3 $(v, k, \lambda)=(36, 15, 6)$
14 groups; 9 in $\mathcal{H}$
9 inequivalent designs
all self-dual (VMB)
(Kibler(75): ***all***(!) DS k<20)
N=4 $(v, k, \lambda)=(64, 28, 12)$

Hadamard Groups of order 64

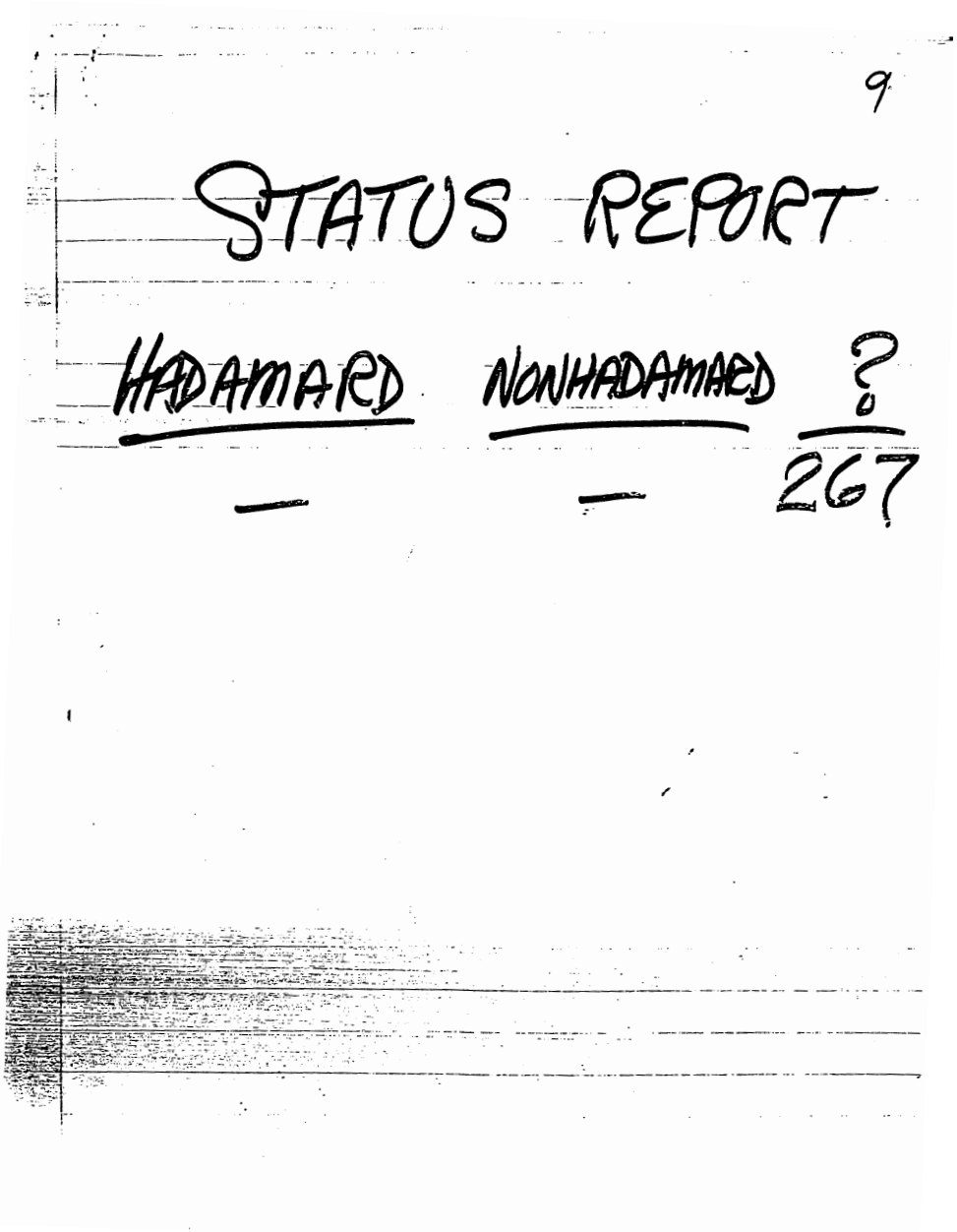


A SURVEY OF
DIFFERENCE SETS
IN 2-GROUPS
(Subtitle: HADAMARD GROUPS OF ORDER 64)

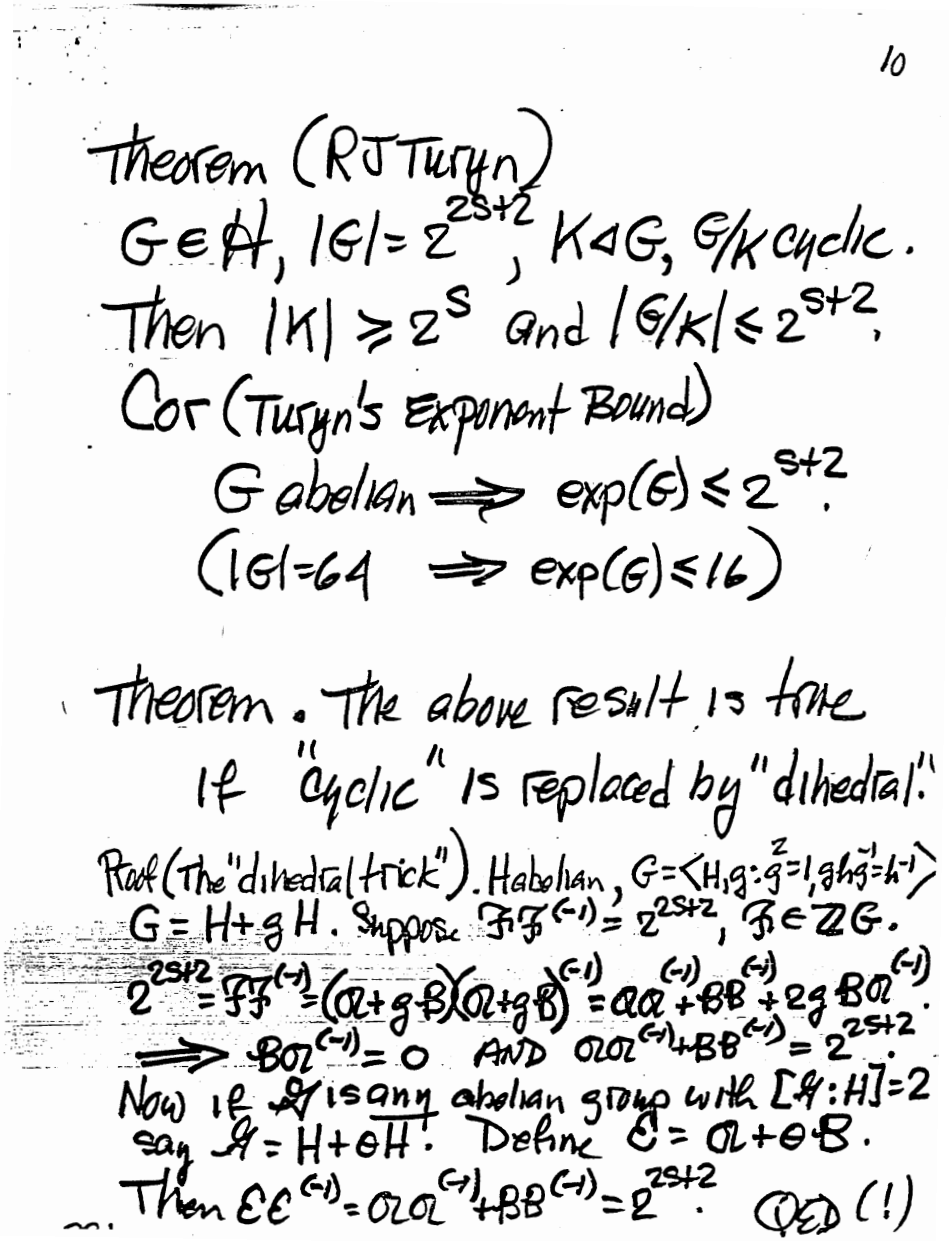
J. F. Dillon
National Security Agency

Marshall Hall Conf.
U. Vermont
Sept. 1990

Hadamard Groups of order 64



Hadamard Groups of order 64



10

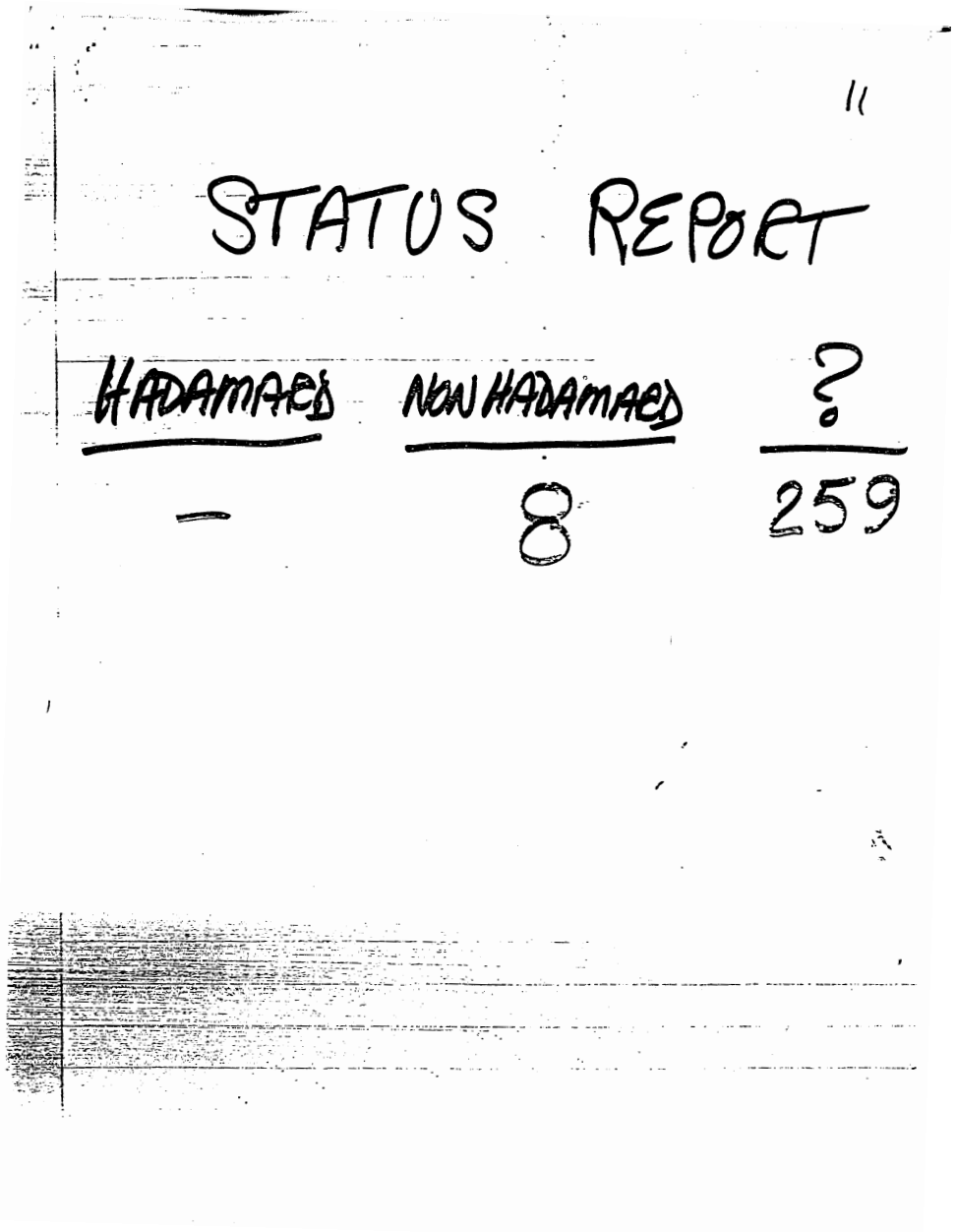
Theorem (RJ Turyn)
$G \in \mathcal{H}$, $|G| = 2^{2s+2}$, $K \lhd G$, G/K cyclic.
Then $|K| \geq 2^s$ and $|G/K| \leq 2^{s+2}$.

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

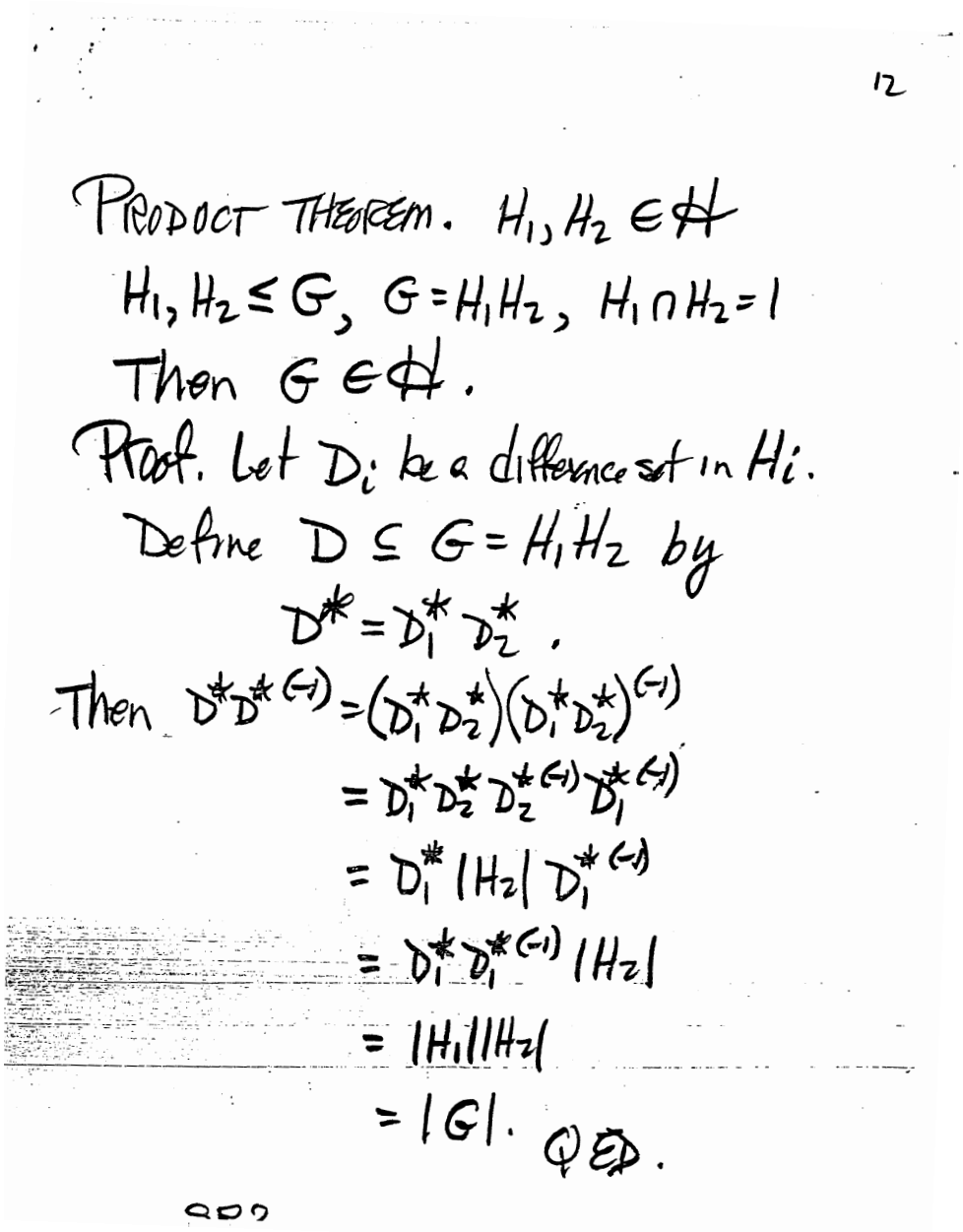
Theorem. The above result is true if "cyclic" is replaced by "dihedral."

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

Hadamard Groups of order 64



Hadamard Groups of order 64



12

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 $D^* D^{*(-1)} = (D_1^* D_2^*)(D_1^* D_2^*)^{(-1)}$

$$= D_1^* D_2^* D_2^{*(-1)} D_1^{*(-1)}$$

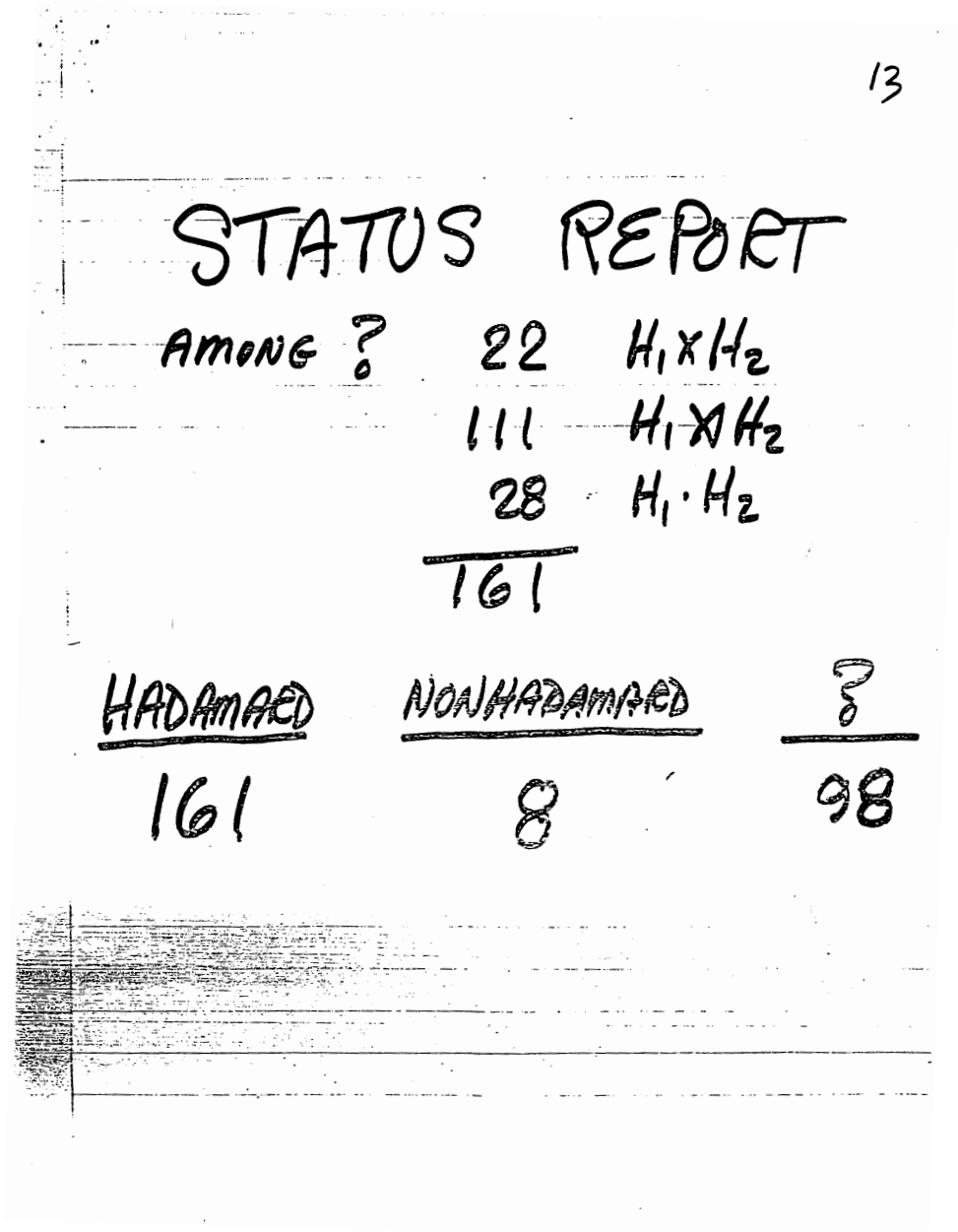
$$= D_1^* |H_2| D_1^{*(-1)}$$

$$= D_1^* D_1^{*(-1)} |H_2|$$

$$= |H_1||H_2|$$

$$= |G|. \quad \text{Q.E.D.}$$

Hadamard Groups of order 64



13

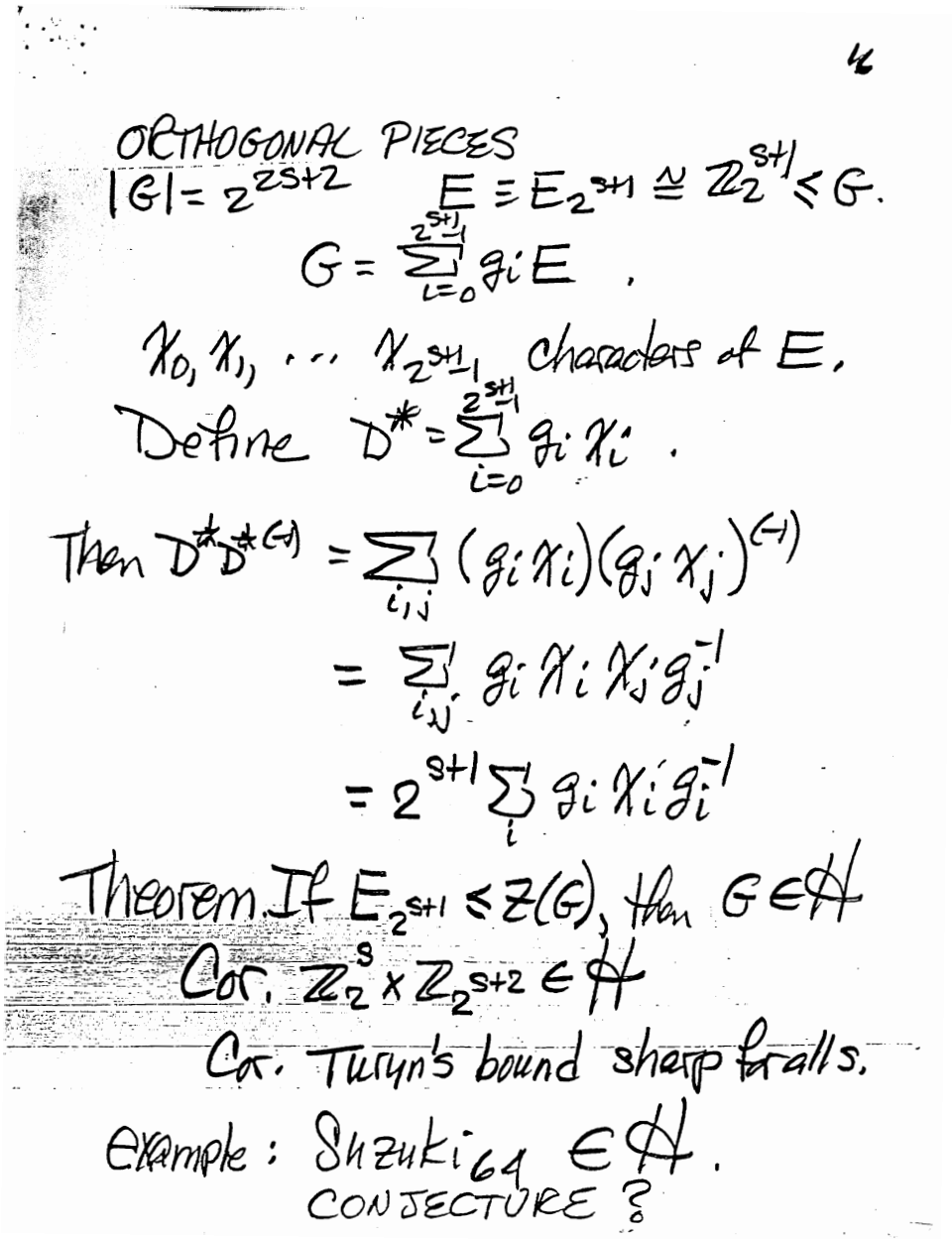
STATUS REPORT

AMONG ?

22	$H_1 \times H_2$
111	$H_1 \times H_2$
28	$H_1 \cdot H_2$
161	

HADAMARD	NONHADAMARD	?
161	8	98

Hadamard Groups of order 64



4

ORTHOGONAL PIECES

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

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

$\chi_0, \chi_1, \ldots \chi_{2^{s+1}-1}$ 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

Hadamard Groups of order 64

19

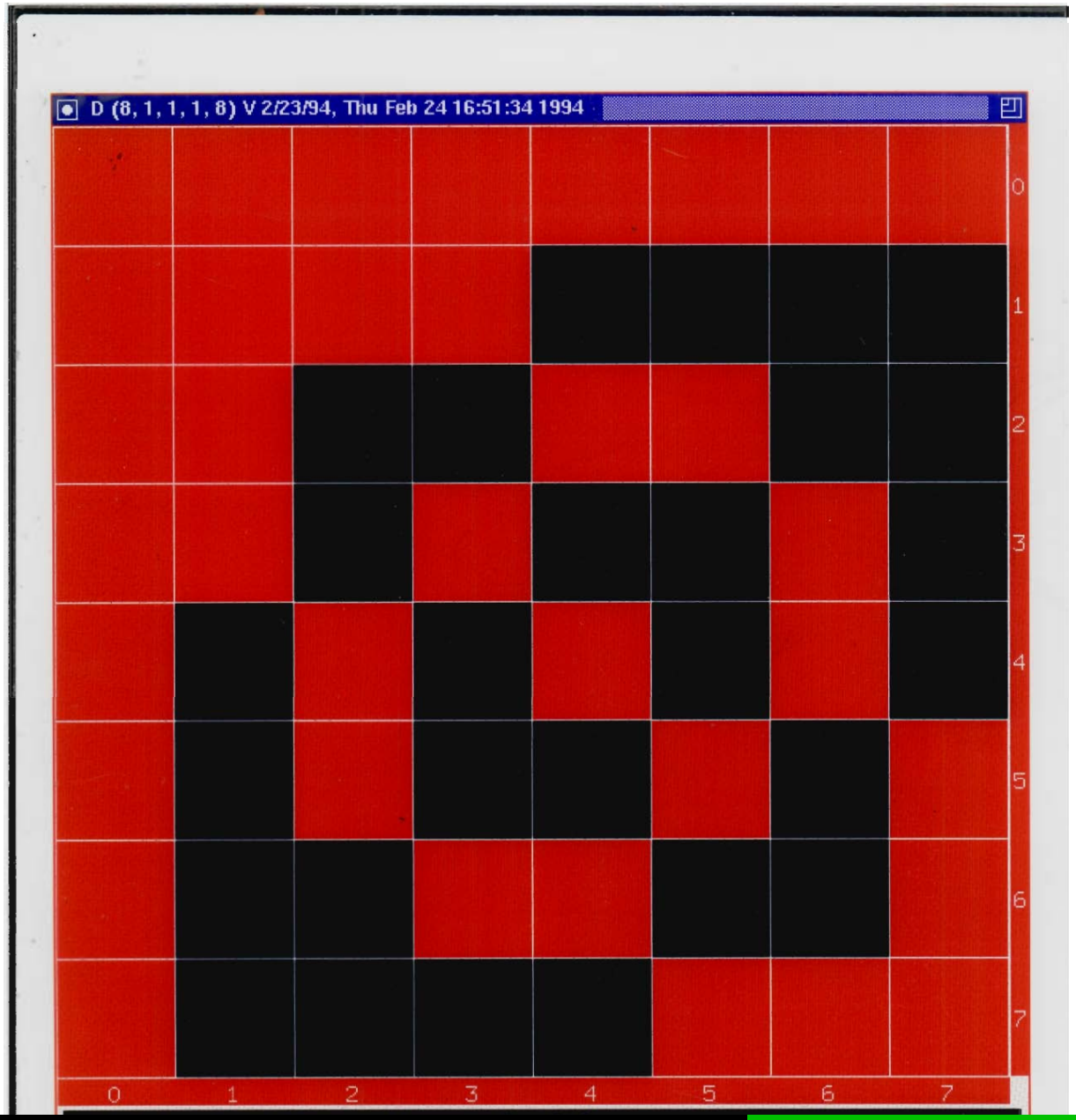
TURYN'S EXAMPLE IN $Z_8 \times Z_8$

$D^* =$

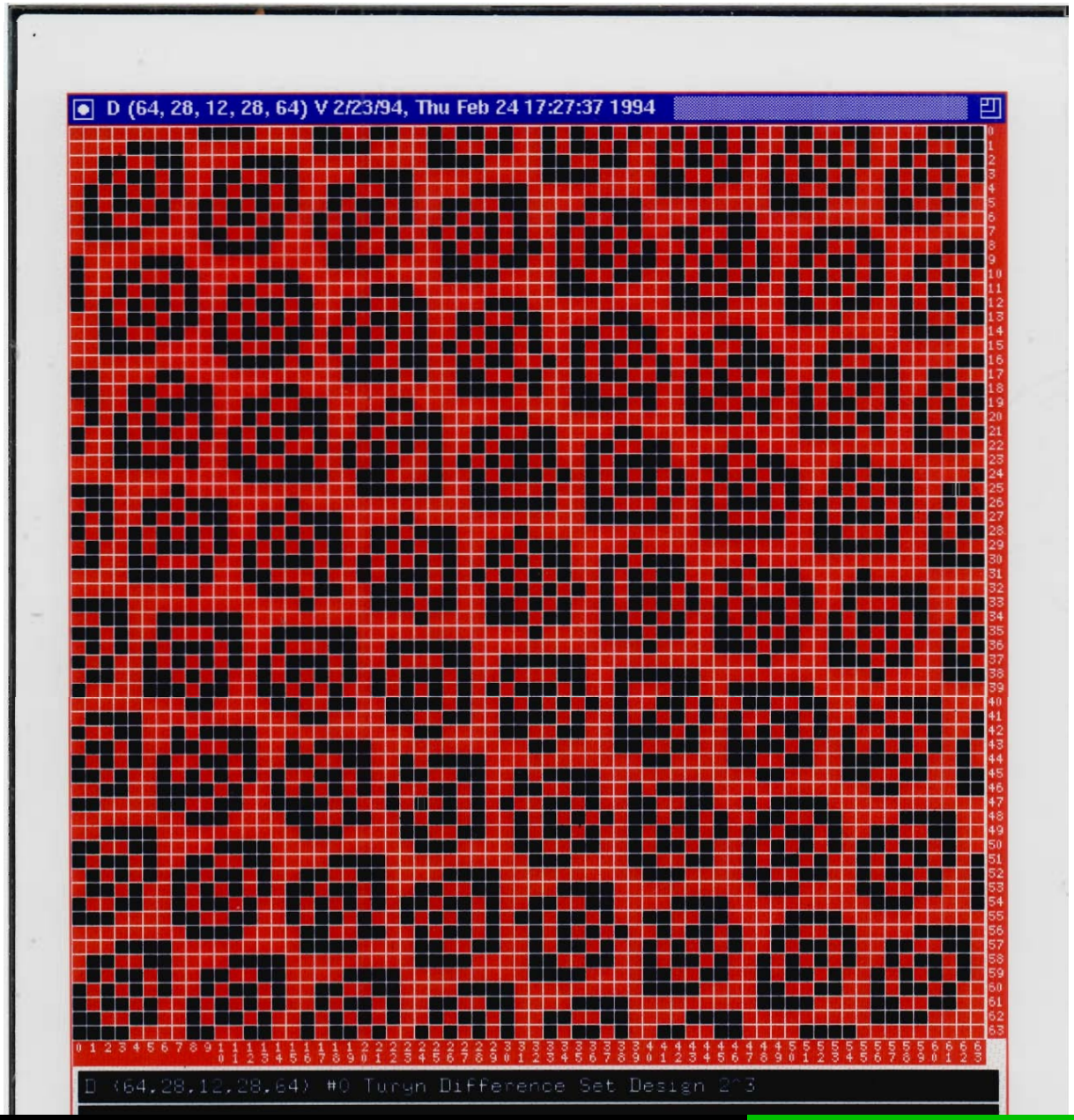
	0	1	2	3	4	5	6	7
0	1	1	1	1	1	1	1	1
1	1	1	1	1	−	−	−	−
2	1	1	−	−	1	1	−	−
3	1	1	−	1	−	−	1	−
4	1	−	1	−	1	−	1	−
5	1	−	1	−	−	1	−	1
6	1	−	−	1	1	−	−	1
7	1	−	−	−	−	1	1	1

12

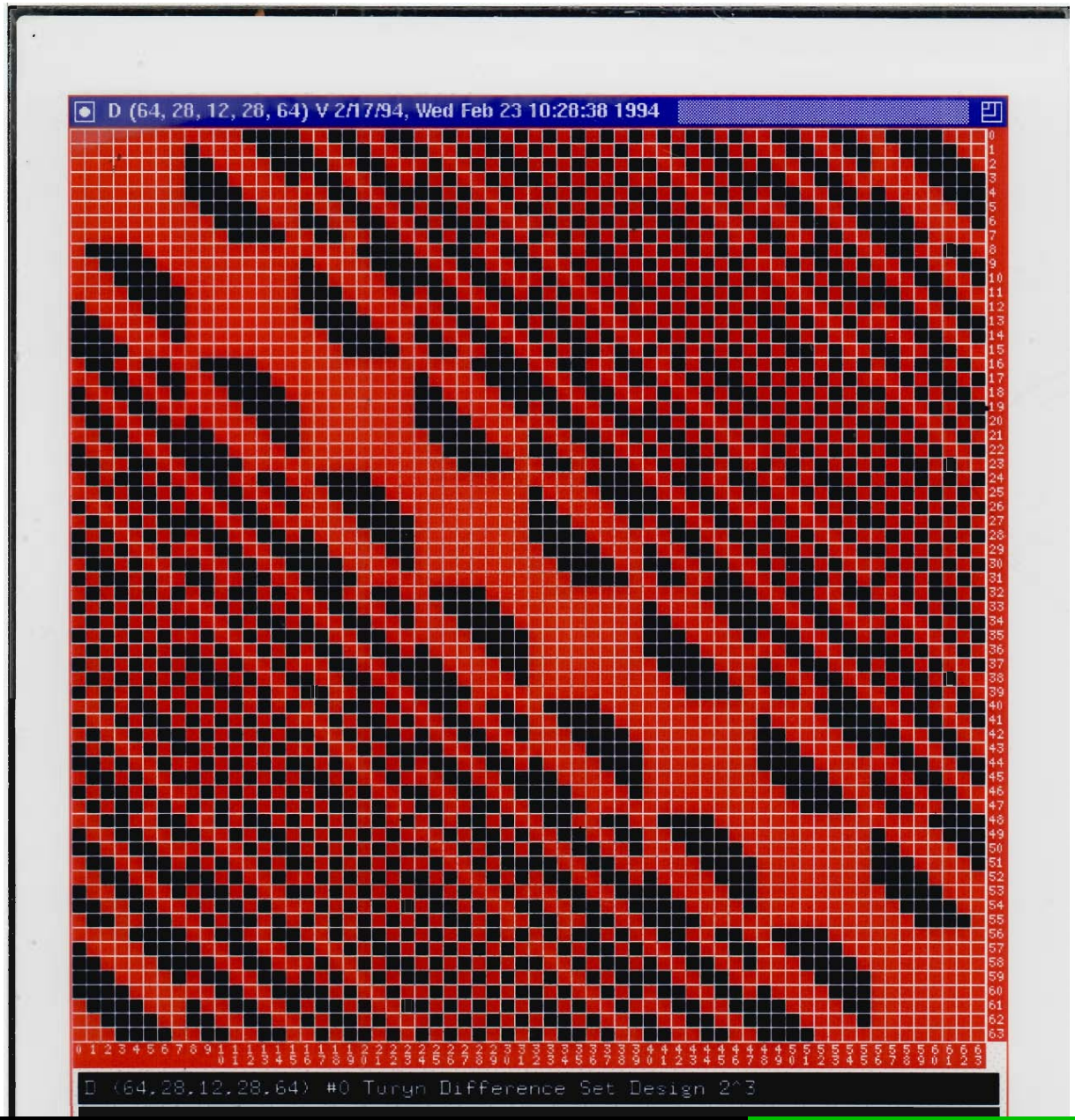
Turyn $\mathbb{Z}_8 \times \mathbb{Z}_8$ difference set



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 x H,

$H = Z_2s+1 = \{0,1,2, \ldots, 2^{s+1}-1\}$

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

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

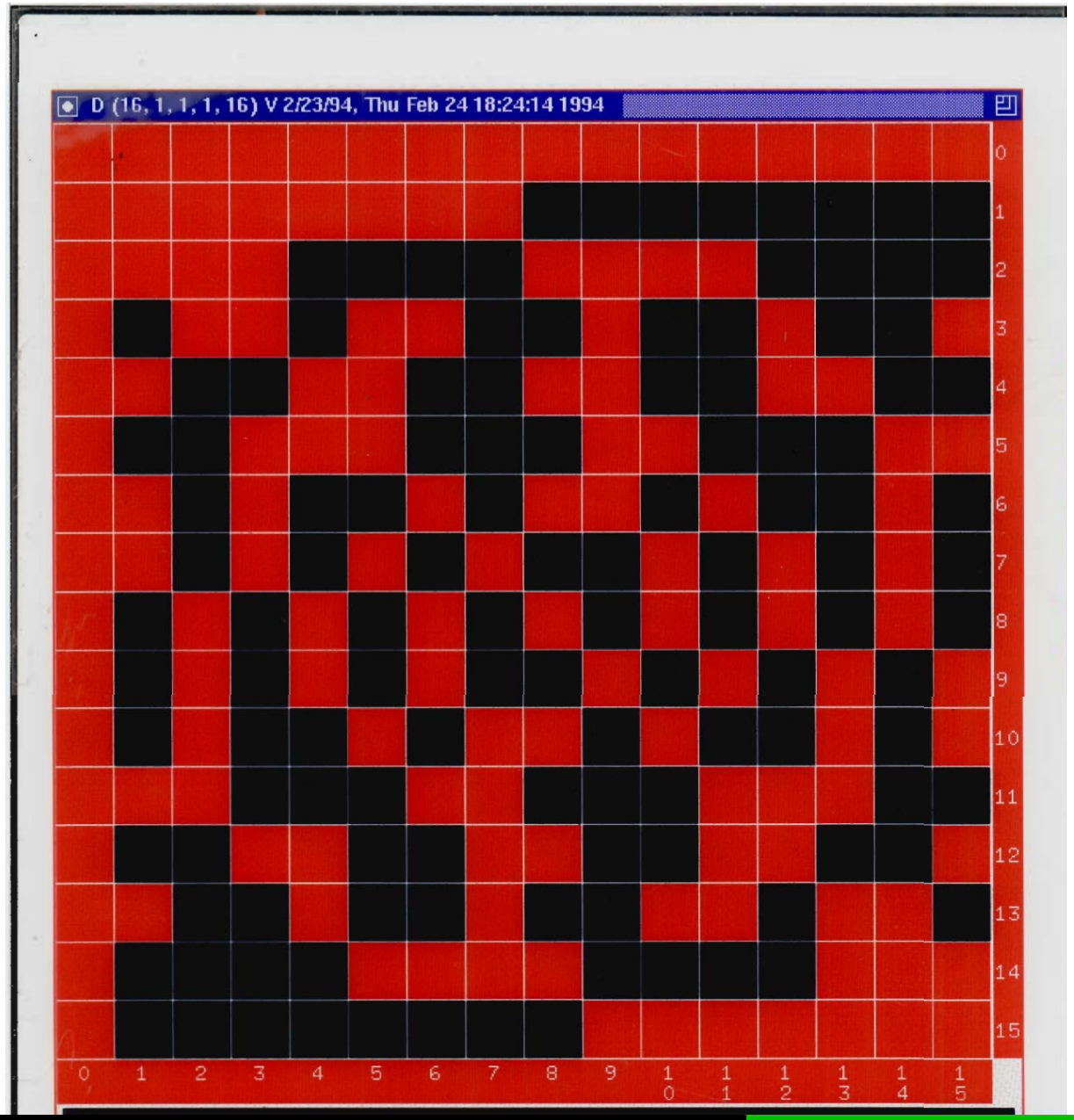
D={(x,y): $f^*(\Pi(x)y)=-1$} is a DS fixed by -1.

Exp many inequiv DS in G

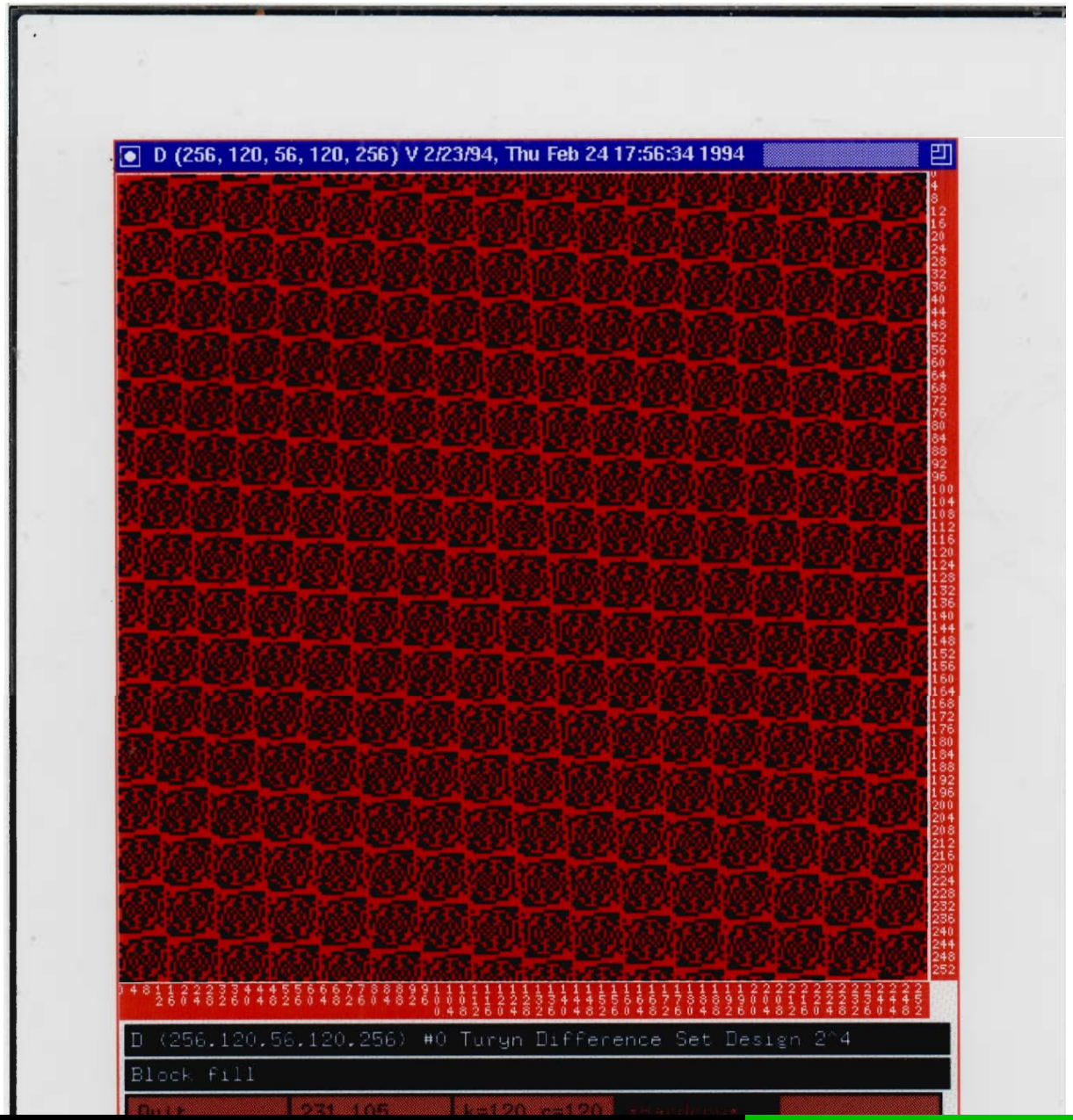
e.g. f(x)="high order bit" of x

s=2 coincides with RJT

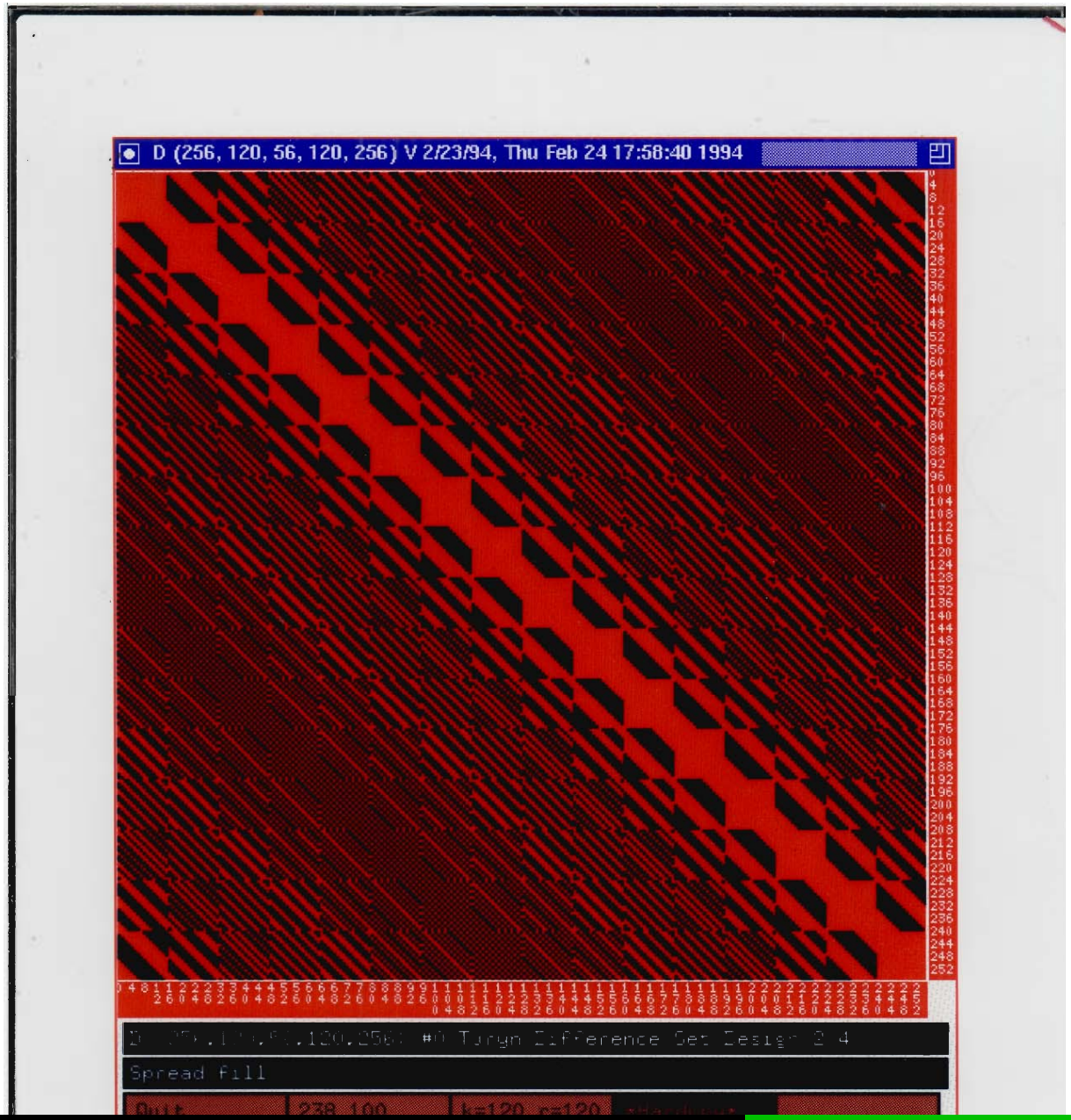
JFD $\mathbb{Z}_{16} \times \mathbb{Z}_{16}$ difference set



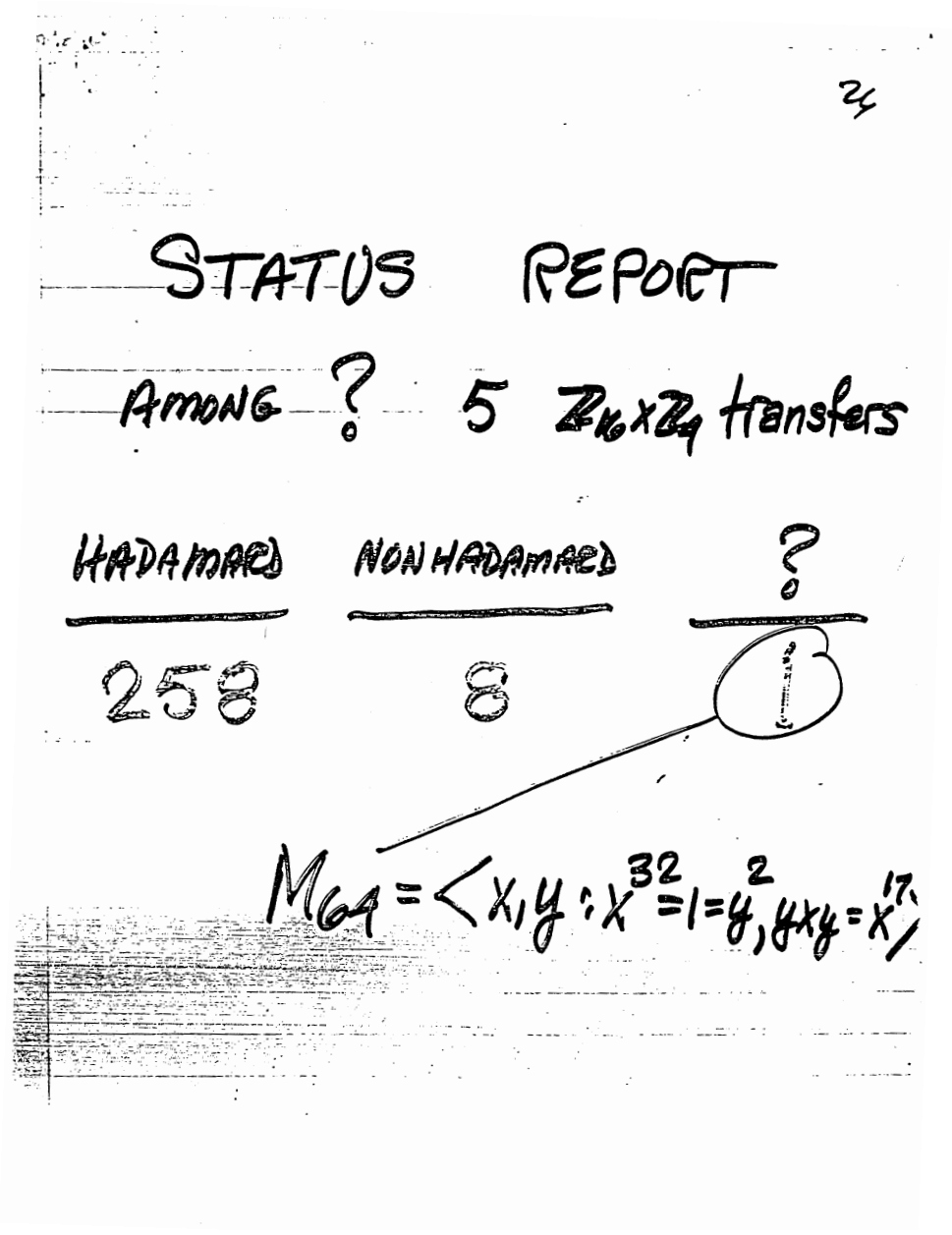
JFD $\mathbb{Z}_{16} \times \mathbb{Z}_{16}$ Hadamard



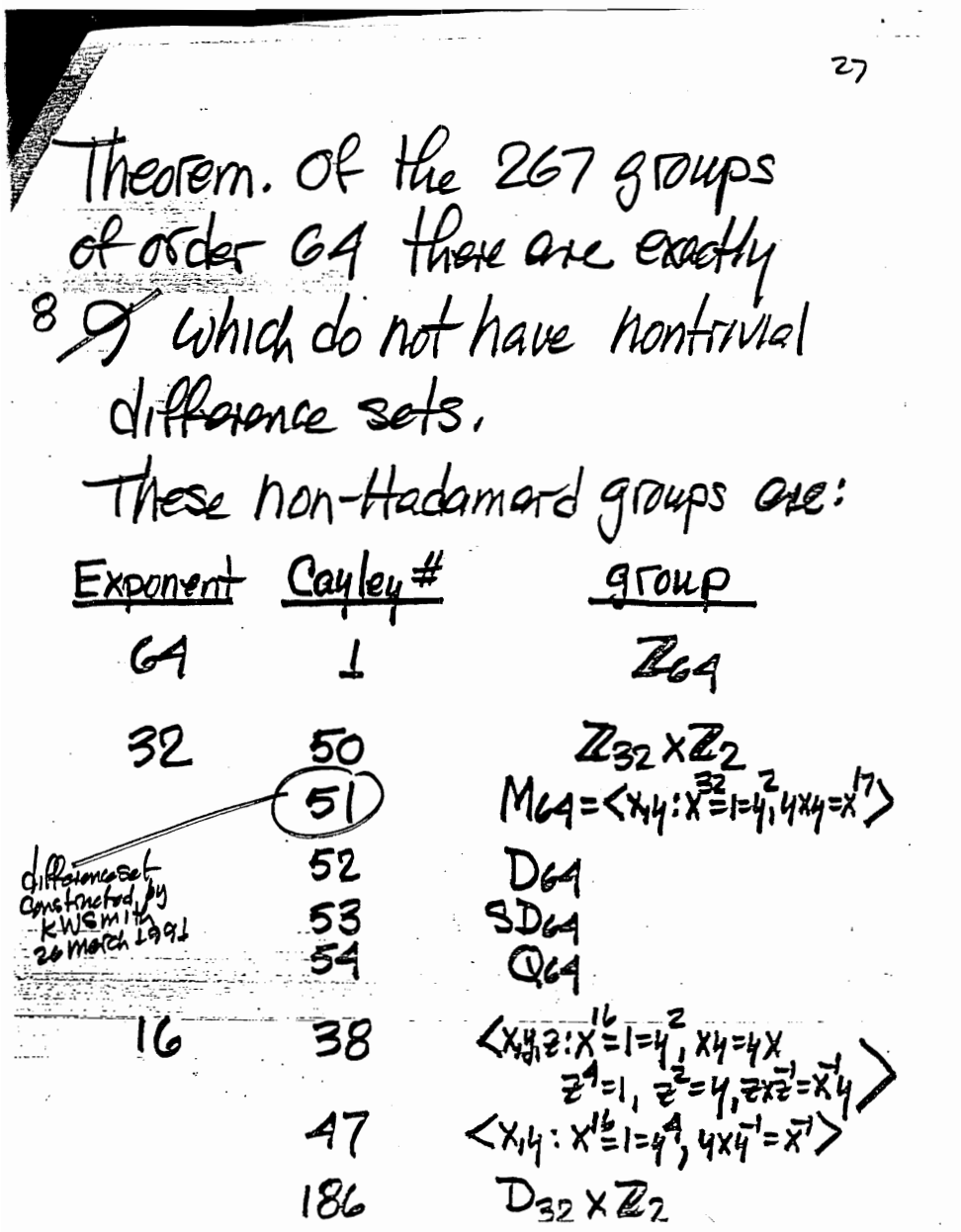
JFD $\mathbb{Z}_{16} \times \mathbb{Z}_{16}$ Hadamard .2



Hadamard Groups of order 64



Hadamard Groups of order 64



27

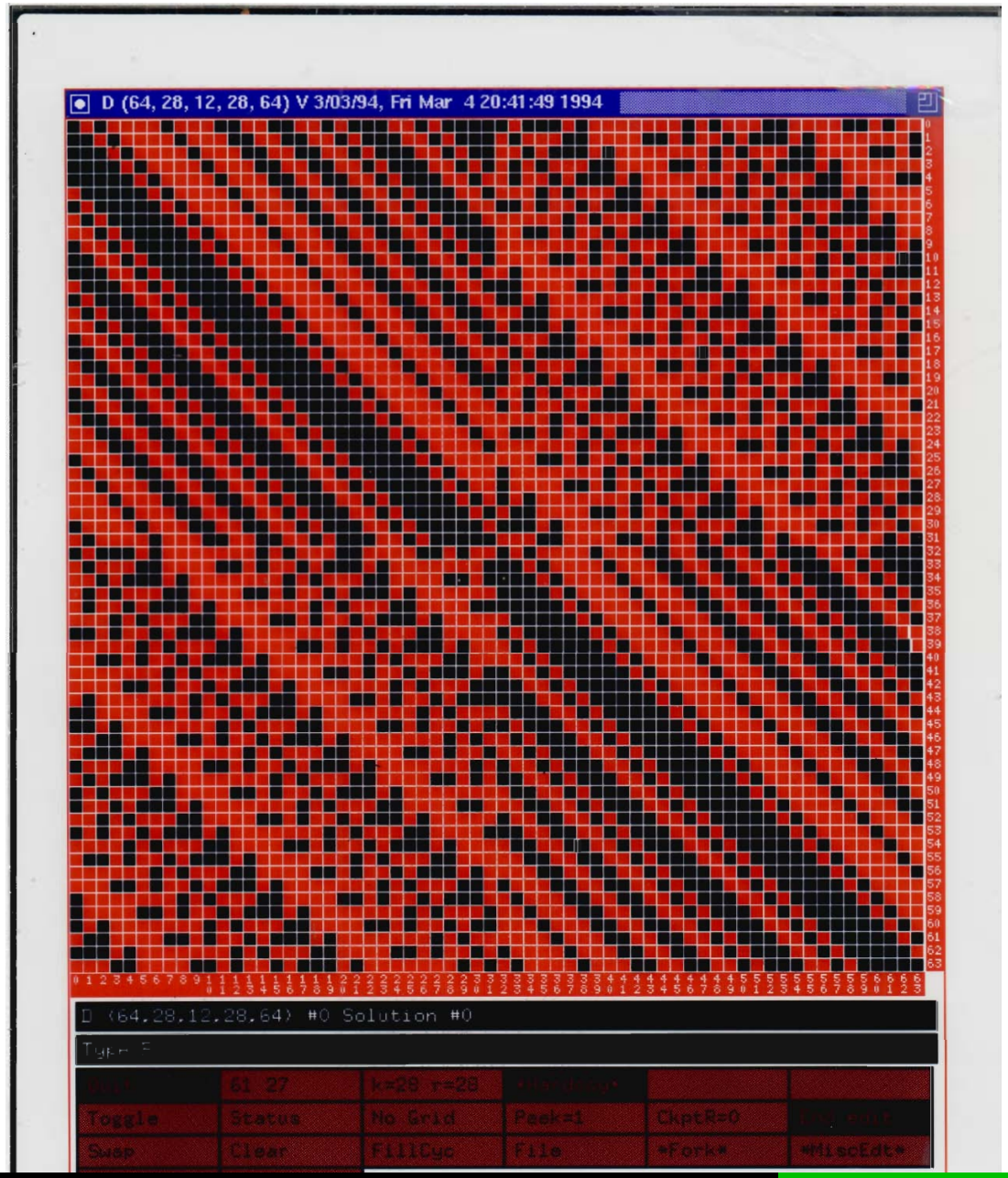
Theorem. Of the 267 groups of order 64 there are exactly 8 ~~9~~ which do not have nontrivial difference sets.

These non-Hadamard groups are:

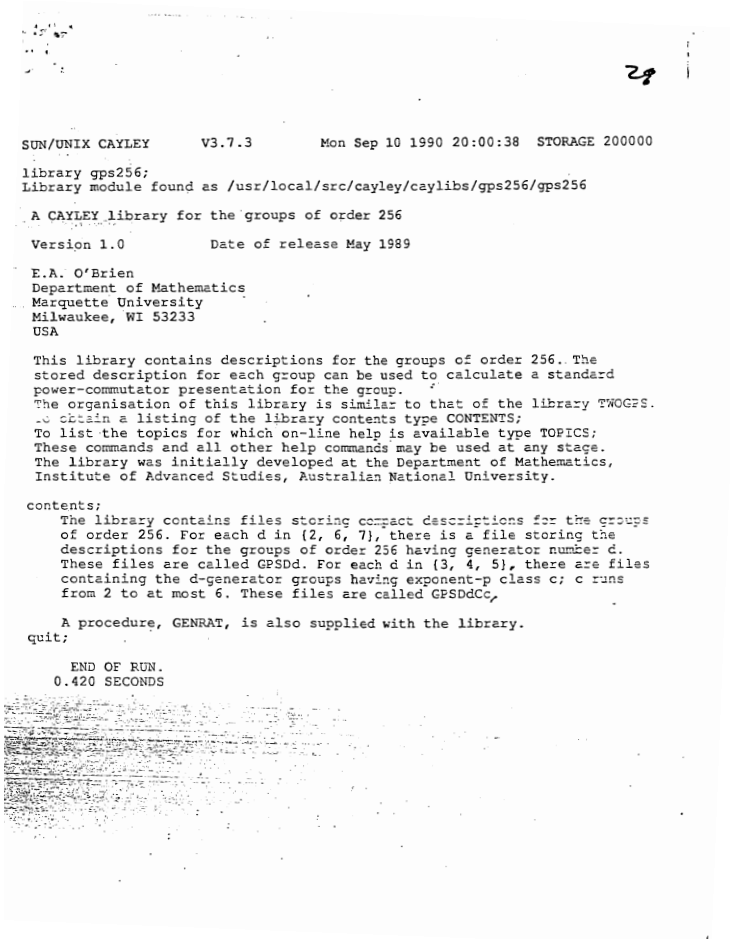
Exponent	Cayley #	group
64	1	$\mathbb{Z}_{64}$
32	50	$\mathbb{Z}_{32} \times \mathbb{Z}_2$
	51	$M_{64} = \langle x,y : x^{32}=1=y^2, yxy=x^{17} \rangle$
	52	D_{64}
	53	SD_{64}
	54	Q_{64}
16	38	$\langle x,y,z : x^{16}=1=y^2, xy=yx, z^4=1, z^2=y, zxz^{-1}=x^{-1}y \rangle$
	47	$\langle x,y : x^{16}=1=y^4, yxy^{-1}=x^7 \rangle$
	186	$D_{32} \times \mathbb{Z}_2$

difference set constructed by K W Smith 26 March 1991

M64 Hadamard matrix

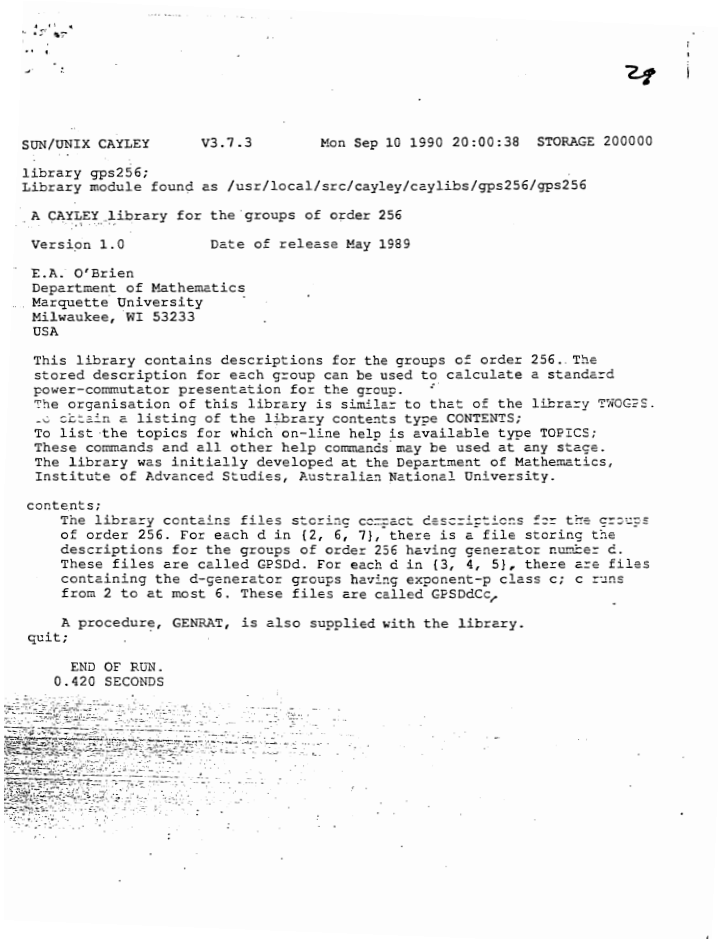


Hadamard Groups of order 256 ???



```
                                                              29

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
```

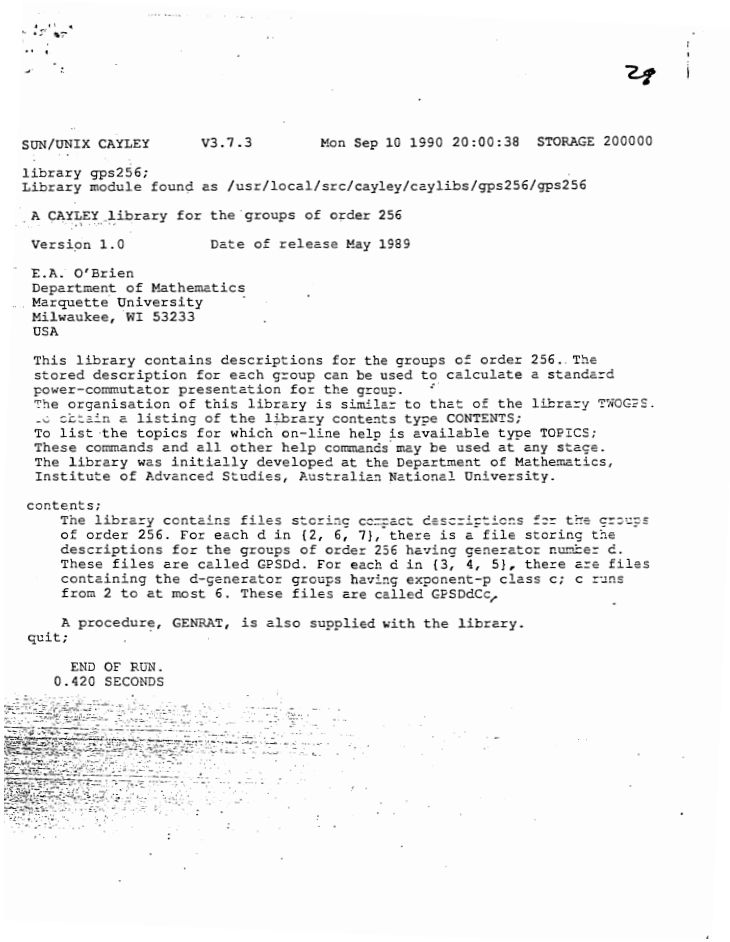
Hadamard Groups of order 256 ???



```
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 ???

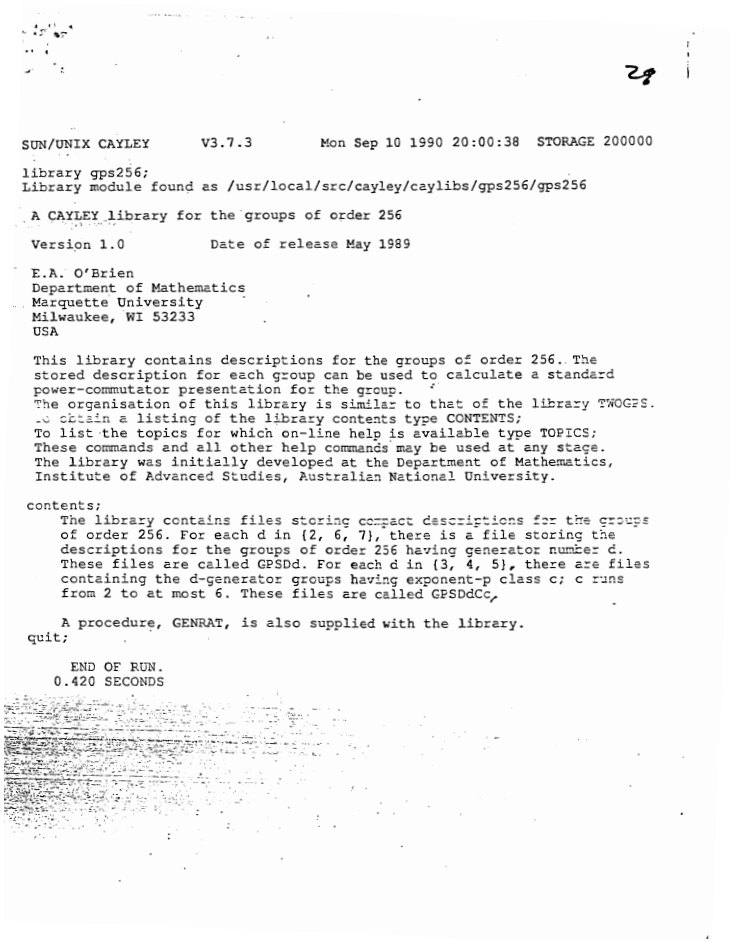


```
SUN/UNIX CAYLEY      V3.7.3        Mon Sep 10 1990 20:00:38  STORAGE 200000

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! :)

$N = 5$

N=5 (v, k, λ)=(100, 45, 20)

(8 April 92) DS found in

$$G_9 = (Z_5 \times Z_5) \times|_2 Z_4$$

Ken Smith, Dick Stafford, Bob Morris, Ted Shorter, JFD

Counterexample to

Conjecture(Storer):
Nonabelian DS⇒Abelian DS.
(RLM: "No abelian DS!")

(Shorter)16 inequivalent DS,
4 pairs not self-dual;
(CAYLEY) |Aut(Γ)|=100

$G_9 = \mathbb{Z}_5^2 \lhd_{17} \mathbb{Z}_2$: the saga

CHRONOLOGY

OCTOBER 91 The players:
JFD, Dick Stafford, Steve Schibell, Bob Morris (R51)
Ken Smith, Central Michigan U.
Mike Boyle (P1 working with JFD)

THERE ARE 16 GROUPS OF ORDER 100:
4 ABELIAN AND 12 NONABELIAN
McFarland ruled out abelian case..... only 12 left!

NOVEMBER 91
Theorems of JFD, RJT, RLM eliminate 5 .....only 7 left!

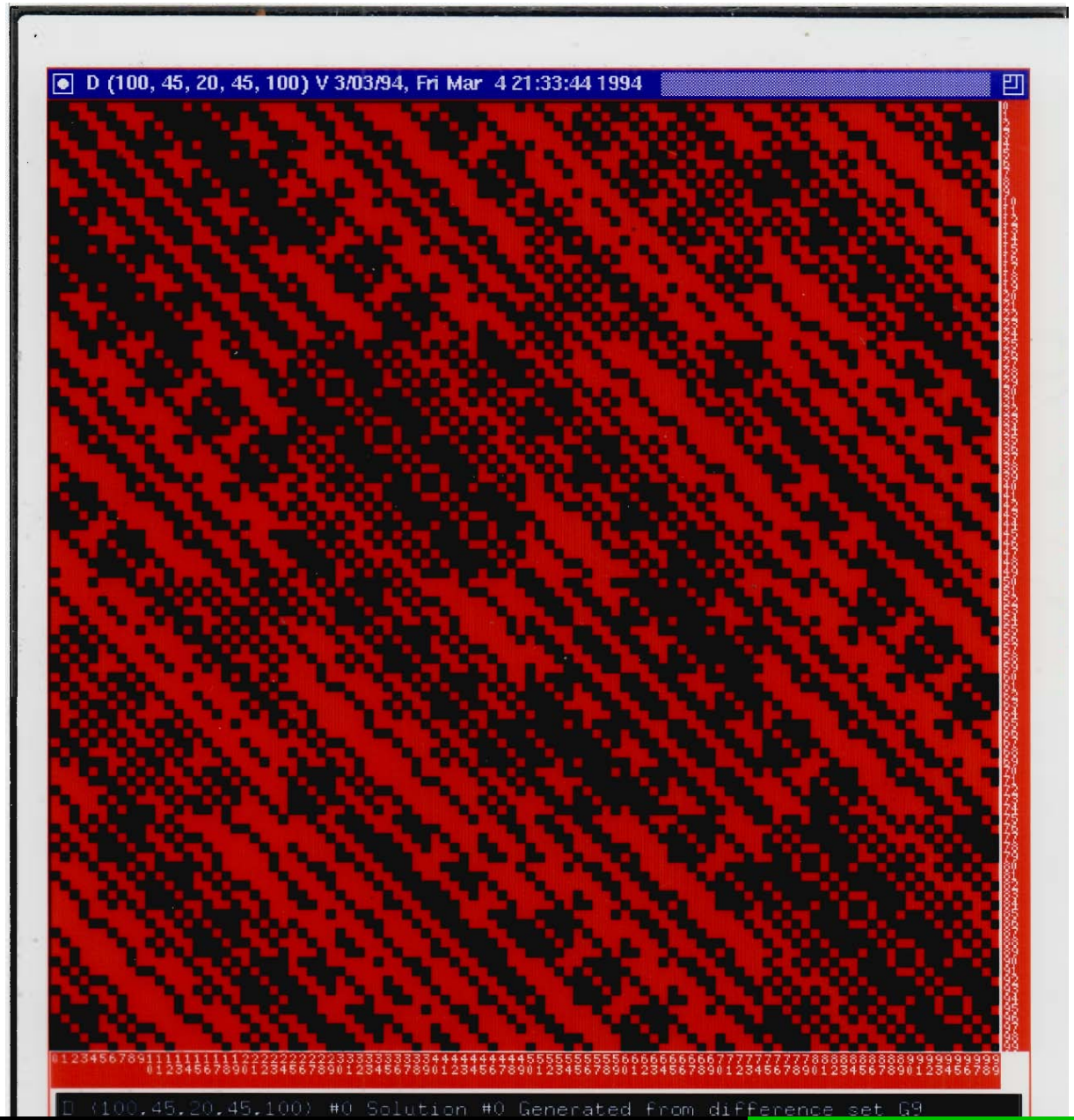
DECEMBER 91 Progress slowing down;
JFD & VMB eliminate one more.....only 6 left!
Focus is on G9;KWS has good idea; does clever reduction to make computer search feasible.
Holidays and other duties intervene.

JANUARY 92 RMS gives status report at Baltimore;
expresses optimism at G9 prospects;
other duties intervene.

MARCH 92 Bob Morris resurrects his work and does more computing to make testing more manageable;has brilliant idea to enlist "new kid" Ted Shorter to make final assault.

8 APRIL 92 Ted writes ingenius C-program which manipulates Morris data and churns out zillions of "answers".
JFD verifies difference sets with CAYLEY.
12 APRIL 92 KWS & VMB announce results at Lehigh.

G_9 Hadamard matrix



DD and Jacobi-like Sums

Theorem 4.1. *Let $G := GF(2^m)^*$ and suppose k is an integer relatively prime to m. Define the function $F_k : G \to \mathbb{C}$ by*

$$\chi(F_k) = \frac{\mathcal{G}(\chi)\mathcal{G}(\chi^{2^k+1})}{\mathcal{G}(\chi^3)}, \ \forall\ \chi \in \hat{G}.$$

Then:

(i) $F_k = (-1)^{f_k}$ *for some balanced function* $f_k : GF(2^m) \to GF(2)$ *with* $f_k(0) = 0$;

(ii) f_k *is a perfect function, i.e. the binary sequence* $\{f_k(\omega^t)\}$ *of period* $2^m - 1$, *where* ω *is primitive in* $GF(2^m)$, *has ideal autocorrelation;*

(iii) the $2^m \times 2^m$ *matrix* $\mathcal{F} = [F_k(xy)]$ *is Hadamard;*

(iv) the set $D_k := \{g \in G : f_k(g) = 1\}$ *is a cyclic difference set with Singer parameters.*

DD and Jacobi-like Sums

Theorem 4.1. *Let $G := GF(2^m)^*$ and suppose k is an integer relatively prime to m. Define the function $F_k : G \to \mathbb{C}$ by*

$$\chi(F_k) = \frac{\mathcal{G}(\chi)\mathcal{G}(\chi^{2^k+1})}{\mathcal{G}(\chi^3)}, \ \forall\ \chi \in \hat{G}.$$

Then:

(i) $F_k = (-1)^{f_k}$ *for some balanced function* $f_k : GF(2^m) \to GF(2)$ *with* $f_k(0) = 0$;

(ii) f_k *is a perfect function, i.e. the binary sequence* $\{f_k(\omega^t)\}$ *of period* $2^m - 1$, *where* ω *is primitive in* $GF(2^m)$, *has ideal autocorrelation;*

(iii) the $2^m \times 2^m$ *matrix* $\mathcal{F} = [F_k(xy)]$ *is Hadamard;*

(iv) the set $D_k := \{g \in G : f_k(g) = 1\}$ *is a cyclic difference set with Singer parameters.*

Neeraj Kashyap proved this in his Master's thesis at UMBC

DD and Jacobi-like Sums

Theorem 4.1. *Let $G := GF(2^m)^*$ and suppose k is an integer relatively prime to m. Define the function $F_k : G \to \mathbb{C}$ by*

$$\chi(F_k) = \frac{\mathcal{G}(\chi)\mathcal{G}(\chi^{2^k+1})}{\mathcal{G}(\chi^3)}, \ \forall\ \chi \in \hat{G}.$$

Then:

(i) $F_k = (-1)^{f_k}$ *for some balanced function* $f_k : GF(2^m) \to GF(2)$ *with* $f_k(0) = 0$;

(ii) f_k *is a perfect function, i.e. the binary sequence* $\{f_k(\omega^t)\}$ *of period* $2^m - 1$, *where* ω *is primitive in* $GF(2^m)$, *has ideal autocorrelation;*

(iii) the $2^m \times 2^m$ *matrix* $\mathcal{F} = [F_k(xy)]$ *is Hadamard;*

(iv) the set $D_k := \{g \in G : f_k(g) = 1\}$ *is a cyclic difference set with Singer parameters.*

Neeraj Kashyap proved this in his Master's thesis at UMBC

$p = 2$ case of more general results of Arasu, Player, and JFD

Even More Bent Functions via Hadamard Equivalence

Theorem 2.0.1 (Fourier Equivalence) *Let $f : K \to GF(2)$ be a balanced Boolean function, with corresponding real valued function $F = (-1)^f$. Given an integer e such that $gcd(e, 2^m - 1) = 1$, define $v : K^2 \to GF(2)$ as*

$$v(x,y) = \begin{cases} f(x^{-e}y) \text{ if } x \neq 0, \\ 0 \text{ otherwise.} \end{cases}$$

with corresponding real valued function $V = (-1)^v$. Then v is bent if and only if there exists a Boolean function $h : K \to GF(2)$ with corresponding real valued function $H = (-1)^h$ such that $\widehat{F}(x^e) = \widehat{H}(x)$. In this case, the dual bent function of v is given by

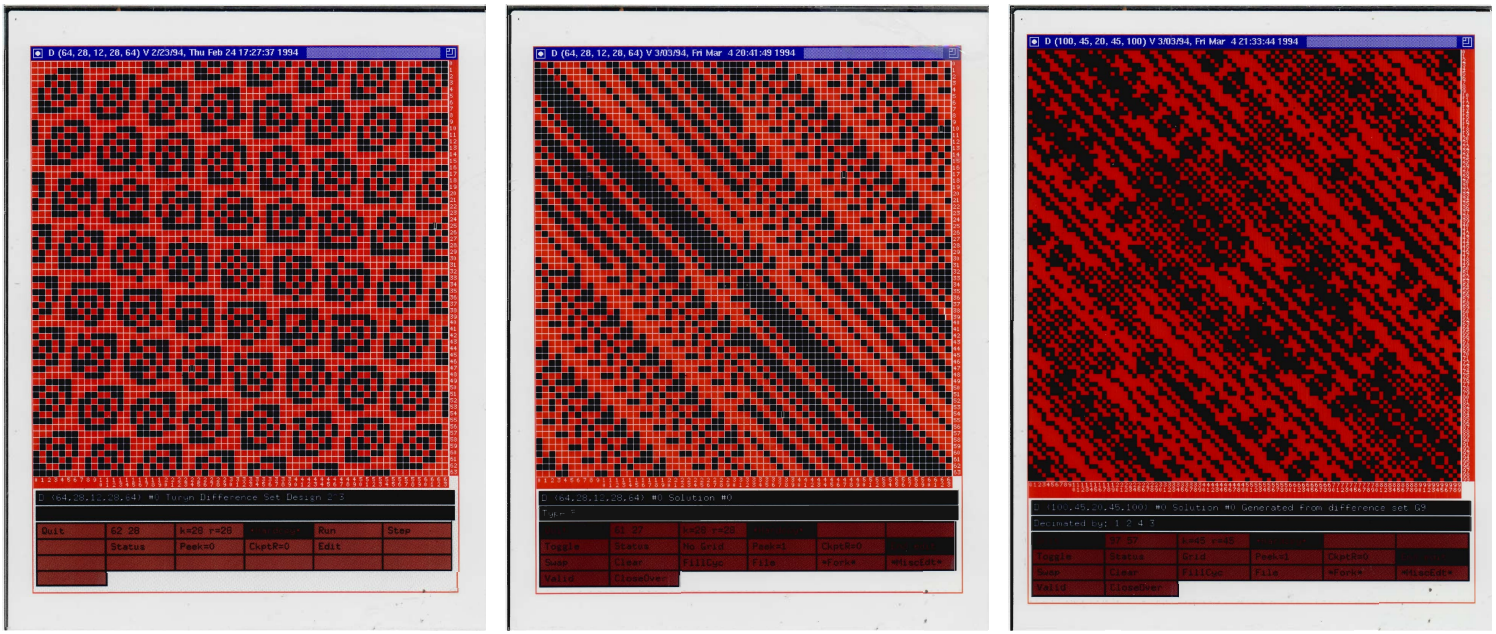
$$v^{dual}(x,y) = \begin{cases} h(xy^{-\frac{1}{e}}) \text{ if } y \neq 0, \\ 0 \text{ otherwise.} \end{cases}$$

Some REALLY Beautiful Hadamard Matrices

Thanks to Al Schwartz for the REALLY beautiful matrices! :)

Some REALLY Beautiful Hadamard Matrices

Thanks to Al Schwartz for the REALLY beautiful matrices! :)



Happy Birthday, Warwick! :)