Hadamard matrices and their applications: an update

K. J. Horadam

Mathematics, RMIT
Melbourne, Australia

International Conference on Design Theory and Applications (incorporating 2^{nd} IWHCMA), Galway, July 1-3 2009

Outline

Outline

The Hadamard and cocyclic Hadamard conjecture: RPs 1 and 38

- Do (cocyclic) HM of all orders $4n$ exist?
- Asymptotic results: Warwick has been working on versions of the following problem: Show that for any $\epsilon > 0$, there is an integer k such that for all $q > k$, there is a (cocyclic) HM of order $2^{2+\epsilon log_2 q} q$.
- Warwick and Hadi show that a cocyclic HM of order $2^t q$ exists whenever $t \geq 10 + 8\lfloor \frac{\log_2 q}{10} \rfloor$, compared to the earlier $t \geq \lfloor 8 \log_2 q \rfloor$ (found by Warwick and Michael Smith)
- exponent is only twice the best bound $t \geq 5 + 4\lfloor \frac{\log_2 q}{10} \rfloor$ (found by Rob, W. Holzmann and Hadi) for HM in general. [J. Combin. Theory A 116 (2009) 1140–1153]

The (cocyclic) Hadamard conjecture: RPs 1 and 38

- Asymptotic results: Warwick [preprint].
  $H(x)$ number of odd $k \in \mathbb{Z}^+, k \leq x$ for which there is a HM of order $2^\ell k$, for some $\ell \leq 2 + \epsilon \log_2 k \in \mathbb{Z}^+$.
  $\exists$ constant $c_1(\epsilon)$: for all sufficiently large x, $H(x) > c_1(\epsilon)x$, ie, $H(x)$ has positive density in $\mathbb{Z}^+$.
- Proof of the Hadamard Conjecture would involve showing $c_1(\epsilon) = 1/2$.
- Warwick uses Paley Hadamard and Sylvester Hadamard matrices in his construction and notes that as these are cocyclic, his result applies to cocyclic Hadamard matrices as well.
- Warwick has suggested more complicated arguments along the lines of his paper might show it can be taken very close to $1/2$.

The Hadamard conjecture: RP 7

- Smallest orders $4n$ for which no HM is known?
- 2007 Dragomir Djokovic constructed several HM of order 764 of Goethals-Seidel type. He lists the 13 orders less than 2000. [Combinatorica 28(4) (2008), 487–489]
  Hence revised list of Hadamard matrices of order < 1000 is 668, 716 and 892.
- Research Problem 7′ : Do Hadamard matrices of orders $4n$ exist, for $n =$
  $167, 179, 223, 251, 283, 311, 347, 359, 419, 443, 479, 487$ and 491?

Binary Rank of Hadamard codes: RP 9

- What is the rank of binary HM (and their Hadamard codes)?
- For C_n (HM rows + complements) Phelps, Rifa, Villanueva use ranks and kernels to distinguish.
- *Kernel* of a binary code C
  $K(C) = \{x \in GF(2)^n \mid x + C = C\}$. ker is its dimension.
- $n = 16$, 5 inequivalent codes:
  $(rank(C_n), ker(C_n)) = (5,5), (6,3), (7,2), (8,2), (8,1)$.
- HM order $4s$, s odd $\Rightarrow$ construct Hadamard codes length $n = 2^t s$, $t \geq 3$, with any rank, $r \in \{4s + t - 3, ..., n/2\}$, and any possible ker $k \in \{1, ..., t - 1\}$.
  [IEEE Trans. IT 51(11), 3931–3937, 2005; LNCS 3857, 2006, 328–337]

Outline

GHMs and their transposes: RPs 16 and 21

- RP 16: Find a GHM whose transpose is not a GHM or prove that no such matrix exists.
- Solved. Rob and Warwick: every GHM over nonabelian N has either: a transpose which is NOT a GHM or: its transpose is a GHM but is equivalent to a GHM whose transpose is NOT a GHM.
- Examples show result not vacuous; smallest are $GH(8, 8)$ over D_8 or Q_8.
- Research Problem 16′: is every GHM equivalent to one whose transpose is also a GHM?

GHMs and their transposes: RPs 16 and 21

- RP 21: Must a GHM M over a nonabelian group $N \leq R^*$, satisfying $MM^* = vI_v$, satisfy $M^*M = vI_v$?
- Solved in same way as RP 16 if there exists GHM M over nonabelian group $N \leq R^*$, satisfying $MM^* = vI_v$.
- Take isomorphic copy of $D_8 =< a, b : a^4 = b^2 = e, ba = a^3b >$ in quotient R of $\mathbb{Z}D_8$ by $< 1a^2 + 1e >$ to obtain such an N.
- So Research Problem 21 must be reformulated similarly.

Outline

Equivalence of HDHM: RP 30

- Proper n-dimensional Hadamard matrix of order v: n-dimensional $v \times v \times ... \times v$ array of 1s and -1s s.t. every two-dimensional $v \times v$ submatrix is a HM. Hyperplane: $n-1$ dimensional subarray.
- Equivalence (Ma) Original defn. Allow negation of hyperplanes and swapping pairs of parallel hyperplanes (Warwick and Dick) Allow these, and swapping pairs of indexes (corresponding in 2-dim case to allowing $H \sim H^{\top}$).

Equivalence of HDHM: RP 30

- RP 30: Number of equivalence classes of proper n-dimensional Hadamard matrices of order 2 ?
- Solved. Warwick and Dick. All proper n-dimensional Hadamard matrices of order 2 are (WD-)equivalent to matrix obtained by applying Product Construction to Sylvester Hadamard matrix of order 2. [J. Combin. Designs DOI 10.1002/jcd]

Outline

The Sevilla Group - Alvarez, Armario, Frau, Gudiel, Guemes, Osuna, Martin, Real: RPs 33 and 34

- Have used homological reduction to find all G-cocyclic CHM for all G of small orders. [J. Symbolic Comp. 44 (2009) 558–570]
- Have used basis matrices for coboundaries and analysis of distribution of -1s in them to design genetic algorithms to search for CHM. [eg LNCS 3857, 144–153, 2006; LNCS 5527, 204–214, 2009; LNCS 5495, 150–160, 2009]
- Several talks in this meeting.

Non-cocyclic constructions - O'Cathain: RPs 39,40,41,42 and 43

- RPs 39,40,41,42 and 43 all ask if specific construction techniques for HM are cocyclic.
- Padraig O'Cathain has partial solutions to these RPs. [M. Litt. thesis, Nov 2008, NUIG]

Outline

Factor Pairs, Extensions and Transversals

G, N finite groups
We always have 3 correspondences:

- Factor pair (ψ, ε) of N by G, that is:
  Two-variable function $\psi : G \times G \longrightarrow N$,
  Action ε of G on N by automorphisms,
  satisfying additional conditions
- Extension $N \overset{\iota}{\rightarrowtail} E \overset{\pi}{\twoheadrightarrow} G$
- Transversal $\{t_g : g \in G\}$ of $\iota(N)$ in E, $\pi(t_g) = g$

Special Case:

Splitting factor pairs/extensions/transversals

Factor Pairs, Extensions and Transversals

G, N finite groups
We always have 3 correspondences:

- Factor pair (ψ, ε) of N by G, that is:
  Two-variable function $\psi : G \times G \to N$,
  Action ε of G on N by automorphisms,
  satisfying additional conditions
- Extension $N \overset{\iota}{\rightarrowtail} E \overset{\pi}{\twoheadrightarrow} G$
- Transversal $\{t_g : g \in G\}$ of $\iota(N)$ in E, $\pi(t_g) = g$

Special Case:

Splitting factor pairs/extensions/transversals

Factor Pairs, Extensions and Transversals

G, N finite groups
We always have 3 correspondences:

- Factor pair (ψ, ε) of N by G, that is:
  Two-variable function $\psi : G \times G \longrightarrow N$,
  Action ε of G on N by automorphisms,
  satisfying additional conditions
- Extension $N \overset{\iota}{\rightarrowtail} E \overset{\pi}{\twoheadrightarrow} G$
- Transversal $\{t_g : g \in G\}$ of $\iota(N)$ in E, $\pi(t_g) = g$

Special Case:

Splitting factor pairs/extensions/transversals

Factor Pairs, Extensions and Transversals

G, N finite groups
We always have 3 correspondences:

- Factor pair (ψ, ε) of N by G, that is:
  Two-variable function $\psi : G \times G \longrightarrow N$,
  Action ε of G on N by automorphisms,
  satisfying additional conditions
- Extension $N \overset{\iota}{\rightarrowtail} E \overset{\pi}{\twoheadrightarrow} G$
- Transversal $\{t_g : g \in G\}$ of $\iota(N)$ in E, $\pi(t_g) = g$

Special Case:

Splitting factor pairs/extensions/transversals

Factor Pairs, Extensions and Transversals

G, N finite groups
We always have 3 correspondences:

- Factor pair (ψ, ε) of N by G, that is:
  Two-variable function $\psi : G \times G \to N$,
  Action ε of G on N by automorphisms,
  satisfying additional conditions
- Extension $N \overset{\iota}{\rightarrowtail} E \overset{\pi}{\twoheadrightarrow} G$
- Transversal $\{t_g : g \in G\}$ of $\iota(N)$ in E, $\pi(t_g) = g$

Special Case:

Splitting factor pairs/extensions/transversals

Optimal Case: The Five-fold Constellation

$N \rightarrowtail E \twoheadrightarrow G$, where $|N|$ divides $|G|$
In optimal case, two more correspondences:
existence of the following five objects is equivalent:

- Orthogonal factor pair of N by G
- Semiregular relative difference set in E relative to N
- Coupled G-cocyclic generalised Hadamard matrix over N
- Semiregular divisible design with regular group E and class regular normal subgroup N
- Base sequence (generalised form of PN) $\phi : G \rightarrow N$

Special Case

$N \rightarrowtail N \rtimes_{\varrho} G \twoheadrightarrow G$ **split (We assume** $\varrho \equiv 1$ **in this talk)**

Bundles (Equivalence Classes) of Factor Pairs

- Two factor pairs of N by G are in the same **Bundle** if their corresponding transversals are equivalent.
- Equivalence of transversals defined from equivalence of relative difference sets in E wrt N. If R, R' are RDS wrt N, N' in E,
  $R \sim R' \Leftrightarrow \exists\, \alpha \in \mathrm{Aut}(E), e \in E \ : \ \alpha(N) = N'$ and $\alpha(R) = R'$.
- Bundle of (ψ, ε) is denoted $\mathcal{B}((\psi, \varepsilon))$.
- Bundles propagate around the Five-fold Constellation.

Outline

RDSs and Presemifields: RPs 50 and 53

- A special case of the correspondence: RDS class $\Leftrightarrow$ bundle of factor pairs (cocycles).
- Equivalence class of multiplicative central $(p^n, p^n, p^n, 1)$-RDSs relative to $\mathbb{Z}_n^p$ in E with $E/\mathbb{Z}_n^p \cong \mathbb{Z}_n^p \Leftrightarrow$ strong isotopism class of presemifields of order p^n.
- 1 bundle over $GF(p)$. Exactly p bundles over $GF(p^2)$. Always at least $3(p-1)$ bundles over $GF(p^3)$.
- RP 53. Solved for $p = 2$. 1446 equivalence classes of central (16, 16, 16, 1)-RDS relative to $\mathbb{Z}_4^2$; not power of 2. Even if restrict to fields, number of RDS equivalence classes not power of 2. [Farmer and Horadam, DCC 2008]

Outline

Bundles and equivalence classes of nonlinear functions: RP 66

- A special case of the correspondence: splitting RDS class $\Leftrightarrow$ bundle of splitting factor pairs (coboundaries).
- In cryptography, want to collect functions into equivalence classes which preserve measures of two types: *differential uniformity* (combinatorial/geometric condition) and *nonlinearity* (discrete Fourier spectrum condition). Best functions over $GF(p^n)$ are APN ($p = 2$) and PN (p odd).
- Two types of equivalence crystallising as important for functions $f(x)$ over $GF(p^n)$:
  CCZ equivalence and EA equivalence.

CZ and EA Equivalence

- Carlet-Charpin-Zinoviev (CCZ) Equivalence (CCZ 1998) $\phi \sim \varphi$ iff their graphs are equivalent, ie there exists (additive) affine permutation A of $GF(2^n)^2$: $A(\{(\phi(x), x), x \in GF(2^n)\}) = \{(\varphi(x), x), x \in GF(2^n)\}$.
- CCZ equivalence preserves differential uniformity, the nonlinearity and the resistance to algebraic cryptanalysis. CCZ equivalence does not preserve algebraic degree.
- Extended Affine (EA) Equivalence (Budaghyan, Carlet, Pott 2006) $\phi \sim \varphi$ iff there exist affine functions γ, θ, χ with γ, θ permutations: $\phi = \gamma \circ \varphi \circ \theta + \chi$.
- Definitions extend immediately to $GF(p^n)$ and functions $f : G \to N$ between arbitrary finite groups.

EA Equivalence and CCZ Equivalence over $GF(p^n)$

EA equivalence $\Rightarrow$ CCZ equivalence BUT it is hard to tell when CCZ equivalent functions are EA-inequivalent.

- Inverse of a permutation ϕ over $GF(2^n)$ is CCZ-equivalent to ϕ, can be EA-inequivalent (if ϕ not an automorphism).
- $GF(2^4)$: 1 CCZ class of APN functions containing 2 EA-classes.
  $GF(2^5)$: 3 CCZ class of APN functions, containing 1, 3, 3 EA-classes — by computation. Brinkmann, Leander (2007)
- $\geq$ 12 CCZ classes of APN functions over $GF(2^6)$, $\geq$ 18 over $GF(2^7)$, $\geq$ 12 over $GF(2^8)$ — by computation. Browning, Dillon, Kibler, McQuistan (2006)
- Each CCZ class of PN functions is a single EA-class: Kyureghyan, Pott (2008)

We can describe the relationship between CCZ and EA equivalence via the Five-fold Constellation.

- EA equivalence of ϕ and φ corresponds to equivalence of the transversals T_ϕ and and T_φ, where in the extension $N \overset{\iota}{\rightarrowtail} N \times G \overset{\kappa}{\twoheadrightarrow} G$, $\iota(N) = N \times \{1\}$,
  $T_\phi = \{t_x = (\phi(x), x), x \in G\}$ with $\kappa((\phi(x), x)) = x$
- CCZ equivalence permits restricted permutations of T_ϕ. [Horadam preprint 2009]

EA-classes inside CCZ-classes

Theorem

Let $\phi : \mathbb{Z}_p^n \to \mathbb{Z}_p^n$, *with* $\phi(0) = 0$. *Define*

$$A_\phi = \{(s, \imath \times \eta) \in \mathbb{Z}_p^n \times \mathrm{Aut}(\mathbb{Z}_p^{2n}) : (\imath_2 \circ (\phi \cdot s)) + \eta_2 \in \mathrm{Sym}_1(\mathbb{Z}_p^n)\},$$
$$B_\phi = \{(s, \imath \times \eta) \in \mathbb{Z}_p^n \times \mathrm{Aut}(\mathbb{Z}_p^{2n}) : (\imath_2 \circ (\phi \cdot s)) + \eta_2 \in \mathrm{Aut}(\mathbb{Z}_p^n)\} \subseteq A_\phi$$

and, for each $(s, \imath \times \eta) \in A_\phi$, *put* $\sigma = \mathrm{inv}[\,(\imath_2 \circ (\phi \cdot s)) + \eta_2\,]$,

$$\phi^{(s,\imath\times\eta)} = (\imath_1 \circ (\phi \cdot s) \circ \sigma) + (\eta_1 \circ \sigma). \quad \textit{Then}$$

$$\begin{aligned} \mathcal{B}(\phi) &= \{\, \phi^{(s,\imath\times\eta)} : (s, \imath \times \eta) \in A_\phi\} \\ \mathbf{b}(\phi) &= \{\, \phi^{(s,\imath\times\eta)} : (s, \imath \times \eta) \in B_\phi\}. \end{aligned}$$