The Anti-Field-Descent Method

Bernhard Schmidt
Nanyang Technological University
Joint work with Ka Hin Leung

Bordeaux, June 2017

Ryser (1963)

We digress briefly and remark that the Hadamard matrix of order 4

$$\begin{bmatrix} 1 & -1 & -1 & -1 \\ -1 & 1 & -1 & -1 \\ -1 & -1 & 1 & -1 \\ -1 & -1 & -1 & 1 \end{bmatrix} \tag{1.7}$$

is a circulant. It is conjectured that a Hadamard matrix of order n cannot be a circulant for $n > 4$.

Eigenvalues

$$H^T H = vI$$

$$Hx = \lambda x \Rightarrow \bar{x}^T H^T H x = |\lambda|^2 x \bar{x}^T$$

$$H^T H = vI \Rightarrow \bar{x}^T H^T H x = v x \bar{x}^T$$

$\lambda \in \mathbb{C}$ eigenvalue of Hadamard matrix of order v

$$\Downarrow$$

$$|\lambda|^2 = v$$

Circulants

$$H = \begin{pmatrix} a_0 & a_1 & \cdots & a_{v-1} \\ a_{v-1} & a_0 & \cdots & a_{v-2} \\ \cdots & \cdots & \cdots & \cdots \\ a_1 & a_2 & \cdots & a_0 \end{pmatrix}$$

Eigenvalues:

$\sum_{i=0}^{v-1} a_i \zeta^{ik}$, $k = 0, \ldots, v-1$, $\zeta = \exp(\frac{2\pi i}{v})$

H Hadamard matrix $\Rightarrow \left| \sum_{i=0}^{v-1} a_i \zeta^{ik} \right|^2 = v$

Note: Implies $v = 4u^2$

Basic Idea

What does

$$\left|\sum_{i=0}^{v-1} a_i \zeta^{ik}\right|^2 = v$$

say about the a_i's?

Divisibility Method (Turyn)

Suppose $\left|\sum_{i=0}^{15} a_i \zeta^i\right|^2 = 16,\ \zeta = \exp(\frac{2\pi i}{16})$

Factorization: $2 = (1-\zeta)(1-\zeta^3)\cdots(1-\zeta^{15})$

Hence $(1-\zeta)^{32}$ divides $\left|\sum_{i=0}^{15} a_i \zeta^i\right|^2$ in $\mathbb{Z}[\zeta]$

$$1-\bar{\zeta} = 1-\zeta^{15} = (1+\cdots+\zeta^{14})(1-\zeta)$$
$$1-\zeta = (1+\cdots+\bar{\zeta}^{14})(1-\bar{\zeta})$$

Thus $(1-\zeta)^{16}$ divides $\sum_{i=0}^{15} a_i \zeta^i$

Divisibility Method (Turyn)

$(1-\zeta)^{16}$ divides $\sum_{i=0}^{15} a_i \zeta^i$

4 divides $\sum_{i=0}^{15} a_i \zeta^i$

Basis representation: $\sum_{i=0}^{15} a_i \zeta^i = \sum_{i=0}^{7} (a_i - a_{i+8}) \zeta^i$

4 divides $a_i - a_{i+8}$ for all i

a_i's cannot be ± 1

No circulant Hadamard matrix of order 16

Turyn (1965)

Suppose a circulant Hadamard matrix of order $v = 4u^2, u \geq 2$, exists. Then:

- u is odd and $u \geq 55$
- If q is a prime power dividing u, then $q^3 \leq 2u^2$
- "Self-conjugacy" bound holds

All results based on divisibility conditions for a_i's

coming from $\left|\sum_{i=0}^{v-1} a_i \zeta^{ik}\right|^2 = v$

Further Known Results on Circulant Hadamard Conjecture

Suppose a circulant Hadamard matrix of order $v = 4u^2, u \geq 2$, exists.

- $2^{s-1}F(4u^2, u) \geq u^2$ ($s =$ is number of distinct prime divisors of u) (S. 1999)
- Only finitely many possible u if the prime divisors of u are bounded by a constant (S. 1999)
- $F(4u^2, u)^2/(4\varphi(F(4u^2, u)) \geq u^2$ (S. 2001)
- $F(u^2, u)u/\varphi(u) \geq u^2$ (Leung, S. 2005)
- $u \geq 11715$ (Leung, S. 2005)
- Improved F-bounds (Leung, S. 2012)

Parseval for Polynomials

Let $f(x) = \sum_{i=0}^{v-1} a_i x^i$ and $\zeta = \exp(\frac{2\pi i}{v})$

$$\sum_{k=0}^{v-1} \left|f(\zeta^k)\right|^2 = \sum_{k=0}^{v-1} f(\zeta^k)\overline{f(\zeta^k)}$$

$$= \sum_{k=0}^{v-1} \sum_{i,j} a_i a_j \zeta^{k(i-j)}$$

$$= \sum_{i,j} a_i a_j \sum_{k=0}^{v-1} \zeta^{k(i-j)}$$

$$= v \sum {a_i}^2$$

F-Bound (S.)

Let's try to prove

$$\left|\sum_{i=0}^{v-1} a_i \zeta^i\right|^2 < v$$

Write $f(x) = \sum_{i=0}^{v-1} a_i x^i$. Then $\left|f\left(\zeta^k\right)\right|^2 = v$ for all k

Parseval $\Rightarrow v^2 = v \sum {a_i}^2 = \sum_{k=0}^{v-1} \left|f\left(\zeta^k\right)\right|^2 = v^2$

In particular, $v^2 \geq \sum_{k:\gcd(k,v)=1} \left|f\left(\zeta^k\right)\right|^2 = \varphi(v)v$

F-Bound (S.)

Suppose there is a divisor F of v such that

$$\sum_{i=0}^{v-1} a_i \zeta^i = \sum_{i=0}^{F-1} a_{iv/F} \zeta^{iv/F}$$

By the same argument,

$$F^2 \geq \sum_{k:\gcd(k,F)=1} \left| f\left(\zeta^{kv/F}\right) \right|^2 = \varphi(F) v$$

Thus $v \leq \frac{F^2}{\varphi(F)}$ (F-bound)

Field Descent (S. 1999)

Goal: Find divisor F of v with

$$\sum_{i=0}^{v-1} a_i \zeta^i = \sum_{i=0}^{F-1} a_{iv/F} \zeta^{iv/F} \quad (*)$$

Let p is the largest prime divisor of $v = 4u^2$

If $\mathrm{ord}_{p^2}(q) \equiv 0 \pmod{p}$ for all prime divisors $q \neq p$ of u, then $(*)$ holds with $F = v/p$

Hence $v \leq \frac{(v/p)^2}{\varphi(v/p)} \quad \Rightarrow \quad \frac{v}{\varphi(v)} \geq p$

What if Field Descent Fails?

$v = 4u^2$, u odd, p largest prime divisor of u

If field descent fails, then $\mathrm{ord}_{p^2}(q) \not\equiv 0 \pmod{p}$ for some prime divisor $q \neq p$ of u. In fact,

$$\sum_{i=0}^{v-1} a_i \zeta^i \neq \sum_{i=0}^{v/p-1} a_{ip} \zeta^{ip} \quad (**)$$

Idea: Use $(**)$ to construct another cyclotomic integer with “strange” properties

“Twisted” Cyclotomic Integer

$$X = \sum_{i=0}^{v-1} a_i \zeta^i \neq \sum_{i=0}^{v/p-1} a_{ip} \zeta^{ip} \quad (**)$$

$$\mathrm{ord}_{p^2}(q) \not\equiv 0 \pmod{p}$$
$$\mathrm{ord}_{p^2}(r) \equiv 0 \pmod{p} \text{ for } r|u,\ r \neq p, q$$

Let $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ with $\mathrm{Fix}(\sigma) = \mathbb{Q}(\zeta^p)$. Recall $|X|^2 = v$

Thus $|\bar{X}X^\sigma|^2 = v^2$ and $\bar{X}X^\sigma \equiv 0 \pmod{v/q^2}$

“Twisted” Cyclotomic Integer

$$|\bar{X}X^{\sigma}|^2 = v^2$$
$$\bar{X}X^{\sigma} \equiv 0 \pmod{v/q^2}$$

Set $Y = \bar{X}X^{\sigma}/(v/q^2)$. Then Y is a cyclotomic integer with

$$|Y|^2 = q^4 \text{ and } Y \notin \mathbb{Q}(\zeta^p)$$

Now write $Y = \sum_{b \in B} Y_b b$ with $Y_b \in \mathbb{Z}[\zeta^p]$, where B is an integral basis of $\mathbb{Q}(\zeta)/\mathbb{Q}(\zeta^p)$

Let $\tau \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}), \zeta^{\tau} = \zeta^q$. Then $Y^{\tau} = \eta Y$ for some root of unity η

“Twisted” Cyclotomic Integer

$$|Y|^2 = q^4 \text{ and } Y \notin \mathbb{Q}(\zeta^p)$$

$$Y = \sum_{b \in B} Y_b b \text{ with } Y_b \in \mathbb{Z}[\zeta^p]$$

$$Y^\tau = \eta Y$$

$Y_b \neq 0$ for some $b \neq 1 \Rightarrow Y_b \neq 0$ for at least $\mathrm{ord}_p(q)$ elements b

$$\Rightarrow \sum_{\alpha \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})} |Y^\alpha|^2 \geq \mathrm{ord}_p(q) |\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})|$$

“Twisted” Cyclotomic Integer

$$\sum_{\alpha \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})} |Y^{\alpha}|^2 \geq \mathrm{ord}_p(q)|\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})|$$

$$|Y|^2 = q^4$$

$$\Rightarrow \mathrm{ord}_p(q) \leq q^4$$

Result (Leung, S. 2016), Simplified

Suppose a circulant Hadamard matrix of order $4u^2$ exists

Write $u = p^a w$ where p is the largest prime divisor of u and $\gcd(p, w) = 1$

Let q be the prime divisor of w which "prevents" the field descent $p^{2a} \to p^{2a-x}$

Then $\mathrm{ord}_p(q) \leq q^{4b} \max\left\{\left\{\frac{2}{q^2}\right\} \cup \left\{\frac{s-1}{f_s(s-f_s)} : s \in S\right\}\right\}$

Circulant Hadamard Open Cases

Order $4u^2$

- Smallest open cases: $u = 11715, 82005, 550605, 3854235$.
- 1371 open cases with $u \leq 10^{13}$ (computation by Borwein, Mossinghoff 2014)
- 423 of the 1371 cases ruled out by twisted cyclotomic integer result (Leung, S. 2016)

Barker Sequences

$a_0, \ldots, a_{v-1}$ with $a_i = \pm 1$ such that

$$\left| \sum_{i=0}^{n-k-1} a_i a_{i+k} \right| \leq 1, \qquad k = 1, \ldots, v-1$$

Exist for: $v = 1, 2, 3, 4, 5, 7, 11, 13$

Conjecture: Barker sequences of length $v > 13$ do not exist

Known Results

Suppose a Barker sequence of length v exists.

- v even $\Rightarrow \exists$ circulant Hadamard matrix of order v
- v odd $\Rightarrow v \leq 13$ (Storer, Turyn 1961)
- $v > 13 \Rightarrow v \geq 12{,}100$ (Turyn 1965)
- $v > 13 \Rightarrow v \geq 1{,}898{,}884$ and $p \equiv 1 \pmod 4$ for all odd primes p dividing v (Eliahou, Kervaire, Saffari 1990)

Known Results (continued)

Suppose a Barker sequence of length $v > 13$ exists.

- $v > 4 \cdot 10^{12}$ (“field descent”, S. 1999)
- $v > 10^{22}$ (Leung, S. 2005)
- $v > 2 \cdot 10^{30}$ (Leung, S. 2012, Mossinghoff 2009)

Open Cases with Length $\leq 10^{50}$

u	Factorization
31 540 455 528 264 605	$5 \cdot 13 \cdot 29 \cdot 41 \cdot 2953 \cdot 138200401$
66 687 671 978 077 825	$5^2 \cdot 53 \cdot 193 \cdot 4877 \cdot 53471161$
866 939 735 715 011 725	$5^2 \cdot 13 \cdot 53 \cdot 193 \cdot 4877 \cdot 53471161$
1 293 740 836 374 709 805	$5 \cdot 53 \cdot 97 \cdot 193 \cdot 4877 \cdot 53471161$
6 468 704 181 873 549 025	$5^2 \cdot 53 \cdot 97 \cdot 193 \cdot 4877 \cdot 53471161$
16 818 630 872 871 227 465	$5 \cdot 13 \cdot 53 \cdot 97 \cdot 193 \cdot 4877 \cdot 53471161$
84 093 154 364 356 137 325	$5^2 \cdot 13 \cdot 53 \cdot 97 \cdot 193 \cdot 4877 \cdot 53471161$
2 487 505 958 525 418 181 705	$5 \cdot 29 \cdot 41 \cdot 2953 \cdot 1025273 \cdot 138200401$
6 467 515 492 166 087 272 433	$13 \cdot 29 \cdot 41 \cdot 2953 \cdot 1025273 \cdot 138200401$
19 417 213 258 149 231 605 065	$5 \cdot 17 \cdot 613 \cdot 1974353 \cdot 188748146801$
32 337 577 460 830 436 362 165	$5 \cdot 13 \cdot 29 \cdot 41 \cdot 2953 \cdot 1025273 \cdot 138200401$
863 383 081 390 130 269 759 645	$5 \cdot 41 \cdot 193 \cdot 2953 \cdot 53471161 \cdot 138200401$
1 686 504 775 565 176 744 556 405	$5 \cdot 13 \cdot 29 \cdot 41 \cdot 2953 \cdot 53471161 \cdot 13820040$
1 890 448 348 089 674 770 182 781	$53 \cdot 97 \cdot 4794006457 \cdot 76704103313$
2 630 496 319 975 038 327 042 325	$5^2 \cdot 193 \cdot 24697 \cdot 53471161 \cdot 412835053$
2 988 996 856 098 832 119 836 165	$5 \cdot 13 \cdot 123397 \cdot 1974353 \cdot 188748146801$
3 080 894 677 428 239 302 747 085	$5 \cdot 5333 \cdot 612142549 \cdot 188748146801$
3 770 469 237 344 599 632 723 365	$5 \cdot 53 \cdot 97 \cdot 193 \cdot 4877 \cdot 2914393 \cdot 53471161$
4 316 915 406 950 651 348 798 225	$5^2 \cdot 41 \cdot 193 \cdot 2953 \cdot 53471161 \cdot 138200401$

(computation by Borwein, Mossinghoff 2014)

Result

$$\mathrm{ord}_p(q) \leq q^{4b} \max\left\{\left\{\frac{2}{q^2}\right\} \cup \left\{\frac{s-1}{f_s(s-f_s)} : s \in S\right\}\right\}$$

Application to Length $\leq 10^{50}$

Factorization of u	p	q^b	d	q^{4b}	$\mathrm{ord}_p(q)$	max	LHS/RHS
5·13·29·41·2953·138200401	138200401	41	1885	2.8e+06	9.6e+05	2.4e-02	1.4e+01
5·5·53·193·4877·53471161	53471161	5	1325	3.9e+05	1.3e+07	3.7e-02	9.2e+02
5·5·13·53·193·4877·53471161	53471161	5	325	3.9e+05	1.3e+07	7.4e-02	4.6e+02
5·53·97·193·4877·53471161	53471161	5	265	6.2e+02	1.3e+07	8.0e-02	2.7e+05
5·5·53·97·193·4877·53471161	53471161	5	1325	3.9e+05	1.3e+07	7.4e-02	4.6e+02
5·13·53·97·193·4877·53471161	53471161	5	3445	6.2e+02	1.3e+07	8.0e-02	2.7e+05
5·5·13·53·97·193·4877·53471161	53471161	5	325	3.9e+05	1.3e+07	7.4e-02	4.6e+02
5·29·41·2953·1025273·138200401	138200401	41	5945	2.8e+06	9.6e+05	1.4e-03	2.5e+02
13·29·41·2953·1025273·138200401	138200401	41	377	2.8e+06	9.6e+05	2.4e-02	1.4e+01
5·17·613·1974353·188748146801	188748146801	5	52105	6.2e+02	1.2e+10	8.0e-02	2.4e+08
5·13·29·41·2953·1025273·138200401	138200401	41	1885	2.8e+06	9.6e+05	2.4e-02	1.4e+01
5·41·193·2953·53471161·138200401	138200401	41	205	2.8e+06	9.6e+05	2.1e-02	1.6e+01
5·13·29·41·2953·53471161·138200401	138200401	41	1885	2.8e+06	9.6e+05	2.4e-02	1.4e+01
53·97·4794006457·76704103313	76704103313	97	5141	8.9e+07	3.8e+10	2.1e-04	2.0e+06
5·5·193·24697·53471161·412835053	53471161	5	4825	3.9e+05	1.3e+07	3.2e-03	1.1e+04
5·13·123397·1974353·188748146801	188748146801	5	65	6.2e+02	1.2e+10	8.0e-02	2.4e+08
5·5333·612142549·188748146801	188748146801	5	26665	6.2e+02	1.2e+10	8.0e-02	2.4e+08
5·53·97·193·4877·2914393·53471161	53471161	5	265	6.2e+02	1.3e+07	8.0e-02	2.7e+05
5·5·41·193·2953·53471161·138200401	138200401	41	1025	2.8e+06	9.6e+05	2.1e-02	1.6e+01

Consequences for Barker Sequences

- There is no Barker sequence of length v with $13 < v \leq 4 \cdot 10^{33}$
- All known open cases with $v \leq 10^{50}$ ruled out
- $229{,}305$ out of $237{,}807$ open cases with $v \leq 10^{100}$ ruled out
- Smallest case known not to be ruled out:

$$v = 4 \cdot 30109^2 \cdot 1128713^2 \cdot 167849^2 \cdot 268813277^2$$
$$\approx 1.57 \cdot 10^{51}$$

Thank you!