# Optimal complex projective designs

Aidan Roy

November 6, 2009

# Complex $t$-designs

Let $S_d = \{v \in \mathbb{C}^d : v^* v = 1\}$.
$X \subseteq S_d$ is a complex $t$-design if

$$\frac{1}{|X|} \sum_{v \in X} (vv^*)^{\otimes t} = \int_{S_d} (vv^*)^{\otimes t} \, \mathrm{d}v.$$

## Theorem (Renes, Blume-Kohout, Scott, Caves '03)

*For any finite $X \subseteq \Omega$,*

$$\frac{1}{|X|^2} \sum_{u,v \in X} |u^* v|^{2t} \geq \binom{d+t-1}{t}^{-1},$$

*with equality if and only if $X$ is a $t$-design.*

# Complex $t$-designs

Let $S_d = \{v \in \mathbb{C}^d : v^*v = 1\}$.
$X$ is a weighted complex $t$-design if for some weighting $w : X \to \mathbb{R}$ such that $\sum_{v \in X} w(v) = 1$,

$$\sum_{v \in X} w(v)(vv^*)^{\otimes t} = \int_{S_d} (vv^*)^{\otimes t} \, \mathrm{d}v.$$

## Theorem

*For any finite $X \subseteq \Omega$,*

$$\sum_{u,v \in X} w(u)w(v) \left| u^*v \right|^{2t} \geq \binom{d+t-1}{t}^{-1},$$

*with equality if and only if $X$ is a weighted $t$-design.*

# Complex $s$-distance sets

$X \subseteq S_d$ is a $s$-distance set if

$$\left| \{ |x^* y|^2 : x, y \in X, x \neq y \} \right| = s.$$

## Theorem (Delsarte, Goethals, Seidel, 1975)

*If $X \subseteq S_d$ is an $s$-distance set, then*

$$|X| \leq \binom{d+s-1}{s}^2,$$

*with equality if and only if $X$ is a $2s$-design.*
*If $X$ is a $2t$-design, then*

$$|X| \geq \binom{d+t-1}{t}^2,$$

*with equality if and only if $X$ is an $t$-distance set.*

# Distance distributions

The distance distribution of $X \subseteq S_d$ is

$$\lambda(\alpha) = \frac{\left|\{(u,v) \in X^2 : |u^*v|^2 = \alpha\}\right|}{|X|}.$$

Note:

- $\lambda(\alpha) \geq 0$
- $\lambda(1) = 1$
- $\sum_\alpha \lambda(\alpha) = |X|$
- $\sum_\alpha \lambda(\alpha) P_k^{(d-2,0)}(\alpha) \geq 0$,

where $P_k^{(d-2,0)}(x)$ is a Jacobi polynomial of degree $k$.

# Delsarte's LP bound

## Theorem (Delsarte, Goethals, Seidel, 1975)

*If* $X \subseteq S_d$ *has inner products* $\{\alpha_0 = 1, \alpha_1, \ldots, \alpha_s\}$, *then*

$$
\begin{aligned}
|X| \leq \max \quad & \sum_{i=0}^{s} \lambda_i \\
\textit{s.t.} \quad & \lambda_i \geq 0, \\
& \lambda_0 = 1, \\
& \sum_{i=0}^{s} \lambda_i P_k^{(d-2,0)}(\alpha_i) \geq 0.
\end{aligned}
$$

# Delsarte's LP bound

## Theorem (Delsarte, Goethals, Seidel, 1975)

*If* $X \subseteq S_d$ *has inner products* $\{\alpha_1, \ldots, \alpha_s\}$, *then*

$$
\begin{aligned}
|X| \leq \min \quad & \sum_{k \geq 0} c_k \\
\text{s.t.} \quad & \sum_{k \geq 0} c_k P_k^{(d-2,0)}(\alpha_i) \leq 0, \\
& c_k \geq 0, \\
& c_0 = 1.
\end{aligned}
$$

# 2-designs from bases

## Corollary

*If* $X$ *is a complex* $2$*-design in* $\mathbb{C}^d$ *formed from the union of* $m$ *orthonormal bases, then*

$$m \geq d + 1,$$

*with equality if and only if* $X$ *is a* $2$*-distance set with inner products* $\{0, \frac{1}{d}\}$*.*

*If* $X$ *is a* $2$*-distance set in* $\mathbb{C}^d$ *with with inner products* $\{0, \frac{1}{d}\}$ *formed from* $m$ *bases, then*

$$m \leq d + 1,$$

*with equality if and only if* $X$ *is a* $2$*-design.*

# Mutually unbiased bases

Mutually unbiased bases: orthonormal bases such that for every pair of vectors $u$ and $v$ from different bases,

$$|u^* v|^2 = \frac{1}{d}.$$

complete set of MUBs: $d+1$ bases in $\mathbb{C}^d$.

A complete set of $3$ MUBs in $\mathbb{C}^2$:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \ \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \ \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix}$$

Constructions of $d+1$ mutually unbiased bases in $\mathbb{C}^d$:

- Alltop (1980), Ivanovic (1981): $d = p$ prime
- Wootters & Fields (1989): $d = p^k$ prime-power

# Difference sets

A difference set in an abelian group $G$ is a subset $D$ such that every $g \neq 0$ of $G$ occurs exactly $\lambda$ times as a difference in $D$, for some $\lambda$:

$$\{u - v : u, v \in D, u \neq v\} = \lambda(G \backslash \{0\}).$$

- $\{0, 1, 3\}$ is a difference set in $\mathbb{Z}_7$.

# Difference sets construction

## Theorem (König ’99)

*Let $D$ be a difference set in an abelian group $G$. Then the characters of $G$, restricted to $D$ and normalized, form a $1$-distance set in $\mathbb{C}^{|D|}$.*

Characters of $\mathbb{Z}_7$ (with $\omega^7 = 1$), $D = \{0, 1, 3\}$:

$$\begin{pmatrix} \color{red}{1} \\ \color{red}{1} \\ 1 \\ \color{red}{1} \\ 1 \\ 1 \\ 1 \end{pmatrix} \begin{pmatrix} \color{red}{1} \\ \color{red}{\omega} \\ \omega^2 \\ \color{red}{\omega^3} \\ \omega^4 \\ \omega^5 \\ \omega^6 \end{pmatrix} \begin{pmatrix} \color{red}{1} \\ \color{red}{\omega^2} \\ \omega^4 \\ \color{red}{\omega^6} \\ \omega \\ \omega^3 \\ \omega^5 \end{pmatrix} \cdots \begin{pmatrix} \color{red}{1} \\ \color{red}{\omega^6} \\ \omega^5 \\ \color{red}{\omega^4} \\ \omega^3 \\ \omega^2 \\ \omega \end{pmatrix}$$

# Proof of difference sets construction

If $\chi_a$ and $\chi_b$ are characters of $G$,

$$\begin{aligned}\langle \chi_a|_D, \chi_b|_D\rangle &= \sum_{d\in D} \overline{\chi_a(d)}\chi_b(d) \\ &= \sum_{d\in D} \chi_{b-a}(d) \\ &:= \chi_{b-a}(D).\end{aligned}$$

For any non-trivial character $\chi_{b-a} = \chi$,

$$\begin{aligned}|\chi(D)|^2 &= \chi(D)\overline{\chi(D)} \\ &= \chi(D)\chi(-D) \\ &= |D|\chi(0) + \lambda\chi(G\backslash\{0\}) \\ &= |D| - \lambda.\end{aligned}$$

# Relative difference sets

- Relative difference set: a set $D \subseteq G$ such that for some $\lambda$ and some subgroup $N \leq G$, every $g \in G \backslash N$ occurs exactly $\lambda$ times as a difference in $D$:

$$\{u - v : u, v \in D, u \neq v\} = \lambda(G \backslash N).$$

eg)

$$G = \mathbb{Z}_4, \quad D = \{0, 1\}, \quad N = \{0, 2\}.$$

- Semiregular: $|G| = |D||N|$.

# Construction from relative difference sets

## Theorem (Godsil & R. '06)

*Let $D$ be a semiregular relative difference set in an abelian group $G$. Then the characters of $G$, restricted to $D$ and normalized, are a set of $|G|/|D|$ mutually unbiased bases in $\mathbb{C}^{|D|}$.*

- For odd $q$,

$$D = \{(x, x^2) : x \in \mathbb{F}_q\}$$

  is a semiregular relative difference set in $\mathbb{F}_q^2$.

# Bounds for 2-designs

$m(d)$: the minimum number of orthonormal bases needed for a 2-design in $\mathbb{C}^d$.

- Delsarte: $m(d) \geq d + 1$, equality if $d = p^k$ (MUBs)
- Conjecture: $m(d) \geq d + 2$ if $d \neq p^k$
- Seymour and Zaslavsky: $m(d) < \infty$.

# Highly nonlinear finite functions

Let $G, H$ be finite abelian groups.
$f : G \to H$ is differentially 1-uniform if

$$f(x+a) - f(x) = b$$

has at most 1 solution for fixed $(a, b) \neq (0, 0)$.

Example: $f : \mathbb{Z}_5 \to \mathbb{Z}_6$

| $x$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| $f(x)$ | 0 | 1 | 0 | 2 | 2 |

# Differentially 1-uniform functions

Example: $f : \mathbb{F}_{p^k} \to \mathbb{F}_{p^k}$ given by

$$f(x) := x^2$$

is differentially 1-uniform for $p > 2$.

Proof:

$$\begin{aligned} & (x+a)^2 - x^2 = (y+a)^2 - y^2 \\ \Rightarrow \quad & 2ax = 2ay \qquad (a \neq 0) \\ \Rightarrow \quad & x = y. \end{aligned}$$

# Construction from highly nonlinear functions

## Theorem (R & Scott '07)

*If $f : G \to H$ is differentially 1-uniform, then there is a weighted 2-design formed from the union of $|H| + 1$ orthonormal bases for $\mathbb{C}^{|G|}$.*

$\chi_j : G \to \mathbb{C}^*$, $\psi_a : H \to \mathbb{C}^*$ characters, $j \in G, a \in H$.
The $j$-th element of the $a$-th basis is

$$v_j^a := \frac{1}{\sqrt{|G|}} \sum_{x \in G} \chi_j(x)\psi_a(f(x))e_x. \quad (1)$$

# Differentially 1-uniform functions - survey

- $f : G \to H$ is not 1-uniform for $|G| > |H|$
- perfect nonlinear functions $f : \mathbb{F}_{p^k} \to \mathbb{F}_{p^k}$ $(f(x) = x^2)$
- $f : \mathbb{Z}_d \to \mathbb{F}_{d+1}$ defined by

$$f(j) := y^j,$$

  where $y$ is a generator of $\mathbb{F}^*_{d+1}$.
- $f : \mathbb{Z}_d \to \mathbb{Z}_n$, $n \geq \frac{3}{4}(d-1)^2$, defined by

$$f(j) := \binom{j}{2}.$$

- $f : G \to H$ almost always 1-uniform as $|H| \to \infty$

# 2-designs from orthonormal bases

## Corollary (R & Scott '07)

*There exists a* $2$*-design formed from the union of* $m$ *orthonormal bases in* $\mathbb{C}^d$ *satisfying*

$$\begin{cases} m = d+1, & d \text{ is a prime power;} \\ m = d+2, & d-1 \text{ is a prime power;} \\ m = O(d^2), & \text{otherwise.} \end{cases}$$

# Open problems

## Conjecture

*There exists a $2$-design formed from the union of $d + 1$ orthonormal bases in $\mathbb{C}^d$ if and only if $d$ is a prime power.*

- "if" part is true.

## Conjecture

*There exists a $1$-distance $2$-design of size $d^2$ in $\mathbb{C}^d$, for every $d$.*

- True for $d = 2, \ldots, 15, 19, 24, 35, 48$.

# References

- Mutually unbiased bases:
  Godsil & R., arxiv.org/quant-ph/0511004
- Weighted 2-designs from bases:
  R. & Scott, arxiv.org/quant-ph/0703025
- 1-distance 2-designs:
  Renes, Blume-Kohout, Scott, Caves,
  arxiv.org/quant-ph/0310075