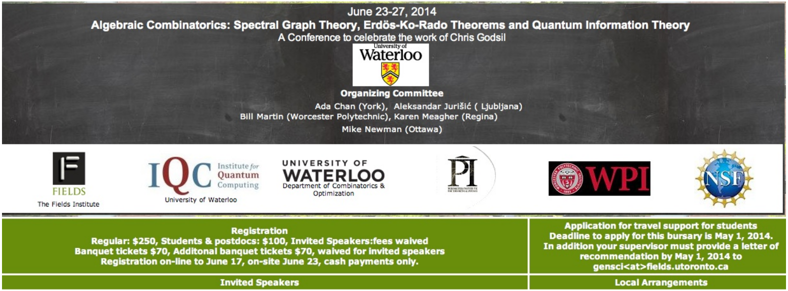
Girth and Dual Girth Parameters in Polynomial Association Schemes

William J. Martin

Department of Mathematical Sciences
and
Department of Computer Science
Worcester Polytechnic Institute

Colloquium on Galois Geometry
in memory of Frédéric Vanhove
February 28, 2014

Godsil65 Conference, Waterloo, June 23-27



I wanted to call it "Wombats, Bilbies and Quolls"

Entrywise products of eigenvectors

Suppose we have a symmetric association scheme with primitive idempotents $\{E_j\}_{j=0}^{d}$ and eigenspaces $V_j = \text{colsp}\, E_j$.

Lemma

If $u \in V_i$ and $v \in V_j$ and $q_{ij}^k = 0$ then $u \circ v \perp V_k$.

Entrywise products of eigenvectors

Suppose we have a symmetric association scheme with primitive idempotents $\{E_j\}_{j=0}^{d}$ and eigenspaces $V_j = \text{colsp}\, E_j$.

Lemma

If $u \in V_i$ and $v \in V_j$ and $q_{ij}^k = 0$ then $u \circ v \perp V_k$.

Here, $\circ$ denotes entrywise product of vectors and q_{ij}^k is the *Krein parameter* appearing in the expansion

$$E_i \circ E_j = \frac{1}{|X|} \sum_{k=0}^{d} q_{ij}^k E_k$$

Entrywise products of eigenvectors

Suppose we have a symmetric association scheme with primitive idempotents $\{E_j\}_{j=0}^d$ and eigenspaces $V_j = \text{colsp}\, E_j$.

Lemma

If $u \in V_i$ and $v \in V_j$ and $q_{ij}^k = 0$ then $u \circ v \perp V_k$.

Here, $\circ$ denotes entrywise product of vectors and q_{ij}^k is the *Krein parameter* appearing in the expansion

$$E_i \circ E_j = \frac{1}{|X|} \sum_{k=0}^{d} q_{ij}^k E_k$$

P. J. Cameron, J.-M. Goethals, and J. J. Seidel, *The Krein condition, spherical designs, Norton algebras and permutation groups.* Proc. Kon. Nederl. Akad. Wetensch. (1978).

Application to Ovoids

Consider the 3-class association scheme whose vertices are the points $\mathcal{P}$ and planes $\mathcal{B}$ of $PG(3, q)$. The non-trivial relations are: *incidence*, *non-incidence* and *same type*.

Application to Ovoids

Consider the 3-class association scheme whose vertices are the points $\mathcal{P}$ and planes $\mathcal{B}$ of $PG(3,q)$. The non-trivial relations are: *incidence*, *non-incidence* and *same type*.

This is a Q-polynomial association scheme with

- V_0 spanned by the all-ones vector
- $V_0 + V_1$ spanned by all the characteristic vectors $\mathbf{1}_S$ where S is of the form $\{p \in \mathcal{P} \mid p \in \ell\} \cup \{\pi \in \mathcal{B} \mid \ell \subset \pi\}$ as ℓ ranges over the lines of $PG(3,q)$.

Application to Ovoids

Consider the 3-class association scheme whose vertices are the points $\mathcal{P}$ and planes $\mathcal{B}$ of $PG(3,q)$. The non-trivial relations are: *incidence*, *non-incidence* and *same type*.

This is a Q-polynomial association scheme with

- V_0 spanned by the all-ones vector
- $V_0 + V_1$ spanned by all the characteristic vectors $\mathbf{1}_S$ where S is of the form $\{p \in \mathcal{P} \mid p \in \ell\} \cup \{\pi \in \mathcal{B} \mid \ell \subset \pi\}$ as ℓ ranges over the lines of $PG(3,q)$.
- V_3 is spanned by $\mathbf{1}_{\mathcal{P}} - \mathbf{1}_{\mathcal{B}}$

Application to Ovoids in $PG(3, q)$

- V_0 spanned by the all-ones vector
- $V_0 + V_1$ spanned by all the characteristic vectors $\mathbf{1}_S$ where S is of the form $\{p \in \mathcal{P} \mid p \in \ell\} \cup \{\pi \in \mathcal{B} \mid \ell \subset \pi\}$ as ℓ ranges over the lines of $PG(3, q)$.
- V_3 is spanned by $\mathbf{1}_{\mathcal{P}} - \mathbf{1}_{\mathcal{B}}$

One easily checks that, if $\mathcal{O}$ is any *ovoid* and S consists of the $q^2 + 1$ points on $\mathcal{O}$ together with the $q^2 + 1$ planes tangent to $\mathcal{O}$, then

$$\mathbf{1}_S \in V_0 + V_2$$

Application to Ovoids in $PG(3, q)$

- V_0 spanned by the all-ones vector
- $V_0 + V_1$ spanned by all the characteristic vectors $\mathbf{1}_S$ where S is of the form $\{p \in \mathcal{P} \mid p \in \ell\} \cup \{\pi \in \mathcal{B} \mid \ell \subset \pi\}$ as ℓ ranges over the lines of $PG(3, q)$.
- V_3 is spanned by $\mathbf{1}_\mathcal{P} - \mathbf{1}_\mathcal{B}$

One easily checks that, if $\mathcal{O}$ is any *ovoid* and S consists of the $q^2 + 1$ points on $\mathcal{O}$ together with the $q^2 + 1$ planes tangent to $\mathcal{O}$, then

$$\mathbf{1}_S \in V_0 + V_2$$

Since $q^3_{00} = q^3_{02} = q^3_{22} = 0$, $(\mathbf{1}_S \circ \mathbf{1}_{S'}) \perp V_3$ for any two "ovoids" S and S' in this geometry:

Application to Ovoids in $PG(3,q)$

- V_0 spanned by the all-ones vector
- $V_0 + V_1$ spanned by all the characteristic vectors $\mathbf{1}_S$ where S is of the form $\{p \in \mathcal{P} \mid p \in \ell\} \cup \{\pi \in \mathcal{B} \mid \ell \subset \pi\}$ as ℓ ranges over the lines of $PG(3,q)$.
- V_3 is spanned by $\mathbf{1}_{\mathcal{P}} - \mathbf{1}_{\mathcal{B}}$

One easily checks that, if $\mathcal{O}$ is any *ovoid* and S consists of the q^2+1 points on $\mathcal{O}$ together with the q^2+1 planes tangent to $\mathcal{O}$, then

$$\mathbf{1}_S \in V_0 + V_2$$

Since $q^3_{00} = q^3_{02} = q^3_{22} = 0$, $(\mathbf{1}_S \circ \mathbf{1}_{S'}) \perp V_3$ for any two "ovoids" S and S' in this geometry:

Corollary

Any two ovoids $\mathcal{O}$ and $\mathcal{O}'$ in $PG(3,q)$ have equally many points in common as they do tangent planes.

Frédéric: 2-Ovoids in Generalized Hexagons

Theorem (Theorem 6.4.20 in dissertation of Vanhove)

Any two distance-2-ovoids $\mathcal{O}$ and $\mathcal{O}'$ in a generalized hexagon of order (s, s^3) with $s > 1$ are either disjoint or have exactly $h(s^2 + s + 1)$ points in common for some $h > s^3 - s$.

A *distance-2-ovoid* $\mathcal{O}$ in a generalized hexagon is a set of pairwise non-collinear points hitting every line

Distance-Regular Graphs

A graph (X, R) is distance-regular if there exist scalars

$$\begin{array}{cccccc} b_0 = k & b_1 & b_2 & \cdots & b_{d-1} & \\ a_0 = 0 & a_1 & a_2 & \cdots & a_{d-1} & a_d \\ & c_1 & c_2 & \cdots & c_{d-1} & c_d \end{array}$$

such that whenever $x, y \in X$ with $d(x, y) = i$, vertex y has

- c_i neighbors at distance $i - 1$ from x
- a_i neighbors at distance i from x
- b_i neighbors at distance $i + 1$ from x

We know very little about distance-regular graphs of large girth.

Girth of Distance-Regular Graphs

Aside from the polygons, we know no distance-regular graphs of large girth.

Conjecture[Suzuki, Koolen] Any distance-regular graph Γ of valency $k \geq 3$ has girth $g_1(\Gamma)$ at most 12.

Girth of Distance-Regular Graphs

Conjecture[Suzuki, Koolen] Any distance-regular graph Γ of valency $k \geq 3$ has girth at most 12.

Examples:

- incidence graphs of generalized hexagons of order (s, s) have girth 12
- Foster graph has girth 10 $(k = 3)$
- Biggs-Smith graph has girth 9 $(k = 3)$
- incidence graphs of generalized quadrangles $GQ(s, s)$ have girth 8

Weiss (1985) proved that the only distance-**transitive** graphs with $k \geq 3$ and $g \geq 9$ those appearing in the first 3 items above.

Girth of Distance-Regular Graphs

Related Facts:

- (Ivanov, 1983): If Γ has valency $k \geq 3$, girth g then its diameter is bounded by $d < g \cdot 2^{2k-3}$
- (BCN): Only three distance-regular graphs known with $d \geq 2k$ (all with $k = 3$)
- some graphs of small numerical girth can still have large "geometric girth"
- (Tanaka-WJM): The only distance-regular graphs we know with $k > 2$ and a splitting field which is more than a degree two extension of $\mathbb{Q}$ are the Biggs-Smith graph, the above generalized hexagons, and their line graphs

Polynomial association schemes

A *(symmetric) association scheme* consists of a finite set X together with a partition $\{R_0, \ldots, R_d\}$ of $X \times X$ into symmetric binary relations whose adjacency matrices $A_0, \ldots, A_d$ span a real vector space closed under matrix multiplication and containing I.

Polynomial association schemes

A *(symmetric) association scheme* consists of a finite set X together with a partition $\{R_0, \ldots, R_d\}$ of $X \times X$ into symmetric binary relations whose adjacency matrices $A_0, \ldots, A_d$ span a real vector space closed under matrix multiplication and containing I.

P-**polynomial:** For some ordering, A_i is a polynomial of degree i in A_1 (This occurs iff (X, R_1) is a *distance-regular graph* of diameter d.)

Polynomial association schemes

A *(symmetric) association scheme* consists of a finite set X together with a partition $\{R_0, \ldots, R_d\}$ of $X \times X$ into symmetric binary relations whose adjacency matrices $A_0, \ldots, A_d$ span a real vector space closed under matrix multiplication and containing I.

P-**polynomial:** For some ordering, A_i is a polynomial of degree i in A_1 (This occurs iff (X, R_1) is a *distance-regular graph* of diameter d.)

Q-**polynomial:** For some ordering of primitive idempotents (orthogonal projections onto maximal common eigenspaces) $E_0, E_1, \ldots, E_d$, each E_i is an entrywise polynomial of degree i in E_1.

Example – An association scheme and its E_1

Consider the 3-cube. $A_0 = I, A_1 = \begin{bmatrix} 0&1&1&0&1&0&0&0\\ 1&0&0&1&0&1&0&0\\ 1&0&0&1&0&0&1&0\\ 0&1&1&0&0&0&0&1\\ 1&0&0&0&0&1&1&0\\ 0&1&0&0&1&0&0&1\\ 0&0&1&0&1&0&0&1\\ 0&0&0&1&0&1&1&0 \end{bmatrix}$,

$$A_2 = \begin{bmatrix} 0&0&0&1&0&1&1&0\\ 0&0&1&0&1&0&0&1\\ 0&1&0&0&1&0&0&1\\ 1&0&0&0&0&1&1&0\\ 0&1&1&0&0&0&0&1\\ 1&0&0&1&0&0&1&0\\ 1&0&0&1&0&1&0&0\\ 0&1&1&0&1&0&0&0 \end{bmatrix}, A_3 = \begin{bmatrix} 0&0&0&0&0&0&0&1\\ 0&0&0&0&0&0&1&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 1&0&0&0&0&0&0&0 \end{bmatrix}$$

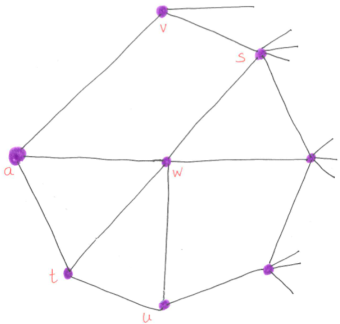
Example – An association scheme and its E_1

For the 3-cube,

$$E_1 = \frac{1}{8}\begin{bmatrix} 3 & 1 & 1 & -1 & 1 & -1 & -1 & -3 \\ 1 & 3 & -1 & 1 & -1 & 1 & -3 & -1 \\ 1 & -1 & 3 & 1 & -1 & -3 & 1 & -1 \\ -1 & 1 & 1 & 3 & -3 & -1 & -1 & 1 \\ 1 & -1 & -1 & -3 & 3 & 1 & 1 & -1 \\ -1 & 1 & -3 & -1 & 1 & 3 & -1 & 1 \\ -1 & -3 & 1 & -1 & 1 & -1 & 3 & 1 \\ -3 & -1 & -1 & 1 & -1 & 1 & 1 & 3 \end{bmatrix}$$

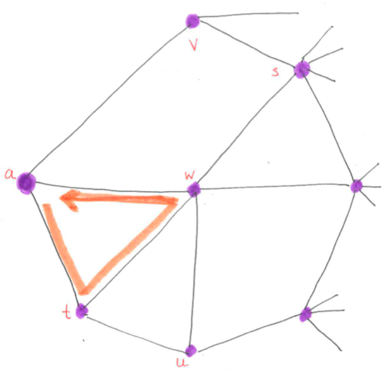
An Excursion into Homotopy

The following idea appears in the thesis work of Heather Lewis (*Discrete Math.* (2000))
under the supervision of Paul Terwilliger.



Consider equivalence classes of closed walks in Γ starting and ending at basepoint *a*.

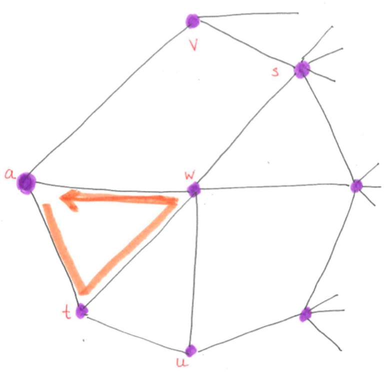
Discrete Homotopy on a Graph



Closed walk *atwa* is in the same equivalence class as *atwswa* and

avswsvatutwa

Discrete Homotopy on a Graph

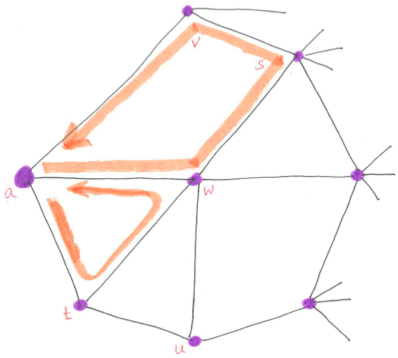


Closed walk *atwa* is in the same equivalence class as *atwswa* and

avswsvatutwa

These all have "essential length" 3.

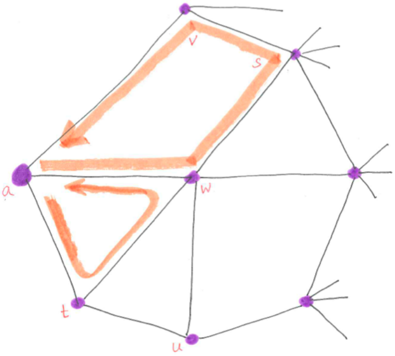
Discrete Homotopy on a Graph



Closed walk *awsva* represents the same group element as

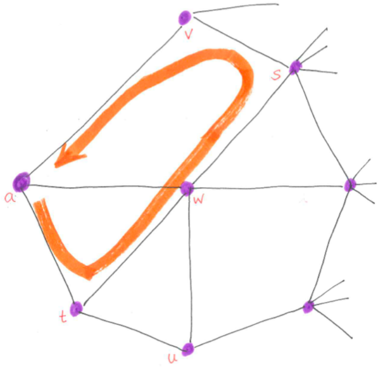
awtuwutwsva

Discrete Homotopy on a Graph



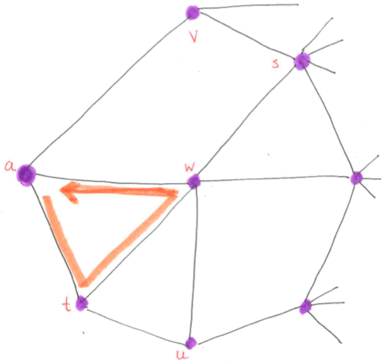
Our group operation is concatenation of walks. Of course, the concatenation of these two walks is represented by another cycle.

Homotopy: the group operation



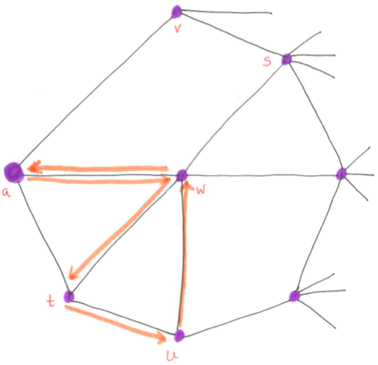
$$atwa \;\star\; awsva \;=\; atwsva$$

Homotopy: the group operation



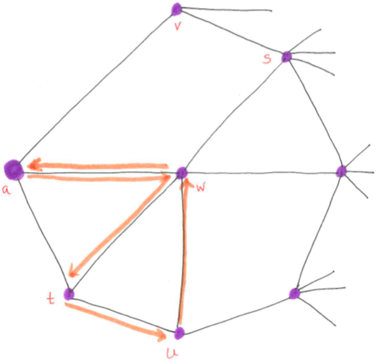
In this way, larger cycles are built from smaller ones. For example, take our first walk *atwa*

Homotopy: the group operation



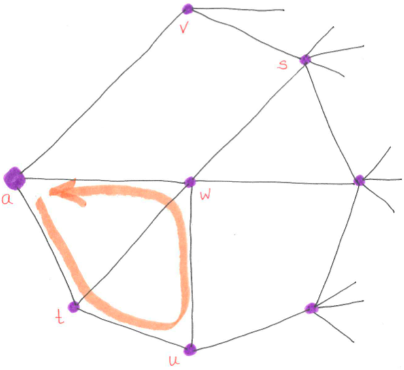
. . . and concatenate with the walk *awtuwa*

Homotopy: the group operation



...and concatenate with the walk *awtuwa*
which also has *essential length* 3 as it has form $\mathbf{pqp}^{-1}$ for a walk $\mathbf{q} = wtuw$ of length three and a path $\mathbf{p}$.

Homotopy: the group operation



In our fundamental group, we have $atwa \star awtuwa = atuwa$

Subgroups of the Fundamental Group

Let $\pi(\Gamma, a)$ be the homotopy group, as just defined, w/ basepoint a.

Subgroups of the Fundamental Group

Let $\pi(\Gamma, a)$ be the homotopy group, as just defined, w/ basepoint a.

For each k, let $\pi_k(\Gamma, a)$ be the subgroup generated by walks of essential length k.

Subgroups of the Fundamental Group

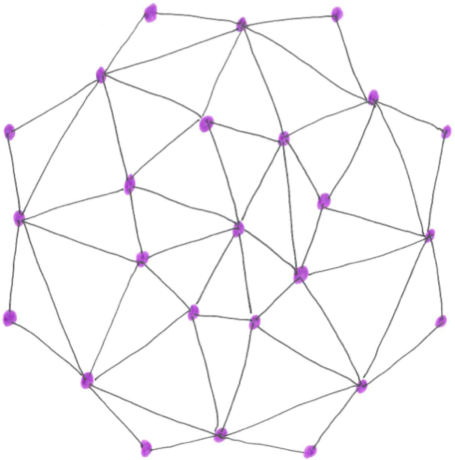
Let $\pi(\Gamma, a)$ be the homotopy group, as just defined, w/ basepoint a.

For each k, let $\pi_k(\Gamma, a)$ be the subgroup generated by walks of essential length k.

For example, if Γ is a simple graph, $\pi_k(\Gamma, a) = 1$ for $k = 0, 1, 2$.

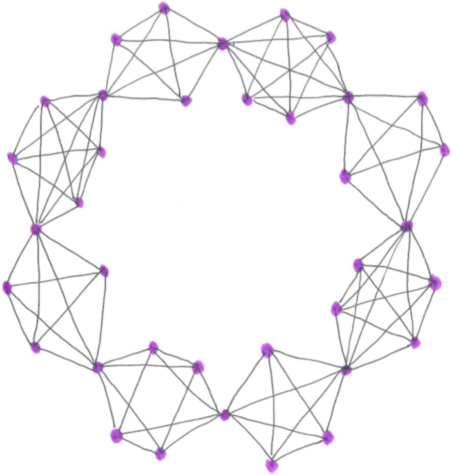
Discrete Homotopy on a Graph

In this example, $\pi(\Gamma, a) = \pi_3(\Gamma, a)$



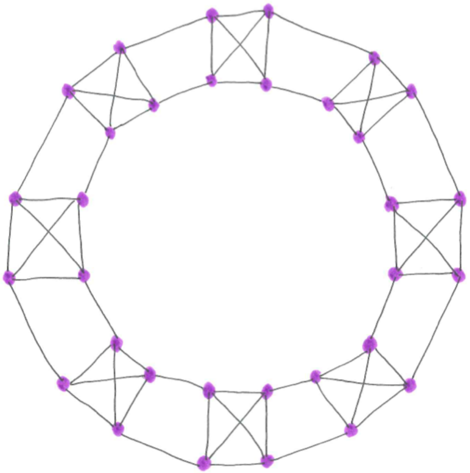
Discrete Homotopy on a Graph

In this example, $\pi_3(\Gamma, a) = \pi_4(\Gamma, a) = \pi_5(\Gamma, a) \neq \pi(\Gamma, a)$



Discrete Homotopy on a Graph

In this example, $\pi_3(\Gamma, a) \neq \pi_4(\Gamma, a) \neq \pi(\Gamma, a)$



Some results of Heather Lewis

- $\pi_0(\Gamma, x) = \pi_1(\Gamma, x) = \pi_2(\Gamma, x) \subseteq \pi_{2d+1}(\Gamma, x) = \pi(\Gamma, x)$
- a Q-polynomial distance-regular graph has girth at most 6
- For any Q-polynomial distance-regular graph, $\pi_6(\Gamma, x) \neq \{e\}$
- and either $\pi_6(\Gamma, x) = \pi(\Gamma, x)$ or
  - Γ is a "pseudoquotient" with $D \in \{2d, 2d+1\}$ and
  - $\pi_6(\Gamma, x) = \pi_{D-1}(\Gamma, x) \neq \pi_D(\Gamma, x) = \pi(\Gamma, x)$

Girth Parameters

So it makes sense to consider not only the *numerical girth*

$$g_1(\Gamma)$$

of a distance-regular graph, but also

$$g_2(\Gamma) = \min\{k \mid \pi_k(\Gamma, x) = \pi(\Gamma, x)\}$$

It's Important to have Open Problems

"It's fine to discover cures, but, remember, chronic conditions are our bread and butter."

The Ideal of a Cometric Scheme

Consider a cometric association scheme $(X, \mathcal{R})$ with Q-polynomial ordering

$$E_0, E_1, \ldots, E_d$$

of its primitive idempotents.

We consider the columns of E_1 as $|X|$ vectors in $\mathbb{R}^|X|$ and wish to determine the ideal of all polynomials in $|X|$ variables which vanish on all of these points.

If $m = \operatorname{rank} E_1$, we may instead find a matrix U with $|X$ rows and m columns satisfying $E_1 = UU^\top$ and find the ideal of all polynomials in m variables that vanish on each row of U.

In fact, we will identify X with this set (or something equivalent) and denote by $\mathcal{I}(X)$ this ideal.

Ideal of a finite set

Let X be a finite subset of $\mathbb{R}^m$. For $a \in X$, write

$$a = (a_1, \ldots, a_m).$$

Now consider polynomials in m variables $F(Y) = F(Y_1, \ldots, Y_m)$ from the polynomial ring $\mathcal{R} = \mathbb{C}[Y_1, \ldots, Y_m]$.

We wish to study the ideal

$$\mathcal{I}(X) = \{F \in \mathcal{R} \mid F(a_1, \ldots, a_m) = 0 \ \forall \ a \in X\}$$

of all polynomials in m variables that vanish at every point of X.

Ideal of a finite set

Let X be a finite subset of $\mathbb{R}^m$. For $a \in X$, write

$$a = (a_1, \ldots, a_m).$$

Now consider polynomials in m variables $F(Y) = F(Y_1, \ldots, Y_m)$ from the polynomial ring $\mathcal{R} = \mathbb{C}[Y_1, \ldots, Y_m]$.

We wish to study the ideal

$$\mathcal{I}(X) = \{F \in \mathcal{R} \mid F(a_1, \ldots, a_m) = 0 \ \forall \ a \in X\}$$

of all polynomials in m variables that vanish at every point of X.

Ideal of a finite set

Let X be a finite subset of $\mathbb{R}^m$. For $a \in X$, write

$$a = (a_1, \ldots, a_m).$$

Now consider polynomials in m variables $F(Y) = F(Y_1, \ldots, Y_m)$ from the polynomial ring $\mathcal{R} = \mathbb{C}[Y_1, \ldots, Y_m]$.

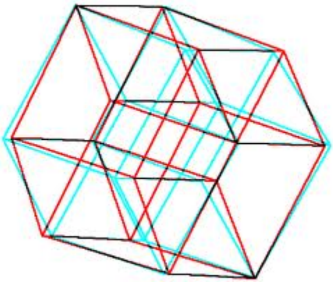
We wish to study the ideal

$$\mathcal{I}(X) = \{F \in \mathcal{R} \mid F(a_1, \ldots, a_m) = 0 \ \forall \ a \in X\}$$

of all polynomials in m variables that vanish at every point of X.

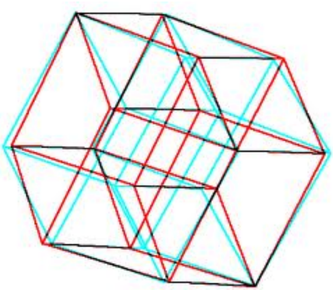
Cubes

Let X consist of the 2^m points $a = (\pm 1, \pm 1, \ldots, \pm 1)$



Cubes

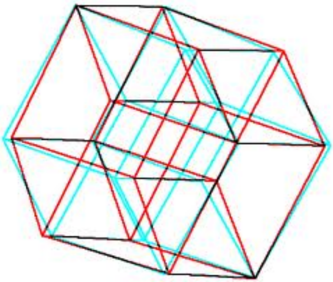
Let X consist of the 2^m points $a = (\pm 1, \pm 1, \ldots, \pm 1)$



- For each i, the quadratic $Y_i^2 - 1$ vanishes at a for each $a \in X$
- The ideal $\mathsf{I} = \langle Y_1^2 - 1, \ldots, Y_m^2 - 1 \rangle$ clearly has exactly X as its zero set: $\mathcal{Z}(\mathsf{I}) = X$

Cubes

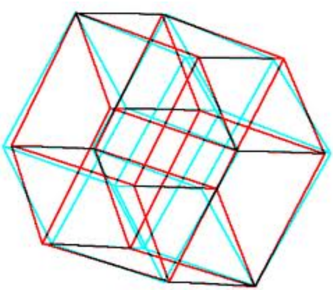
Let X consist of the 2^m points $a = (\pm 1, \pm 1, \ldots, \pm 1)$



- For each i, the quadratic $Y_i^2 - 1$ vanishes at a for each $a \in X$
- The ideal $\mathsf{I} = \langle Y_1^2 - 1, \ldots, Y_m^2 - 1 \rangle$ clearly has exactly X as its zero set: $\mathcal{Z}(\mathsf{I}) = X$
- Since each zero is a simple zero of I, the ideal is *radical*

Cubes

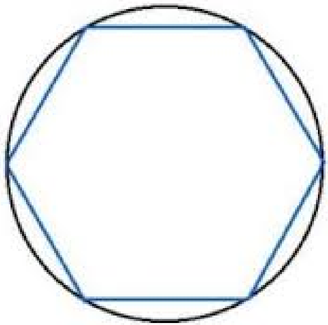
Let X consist of the 2^m points $a = (\pm 1, \pm 1, \ldots, \pm 1)$



- For each i, the quadratic $Y_i^2 - 1$ vanishes at a for each $a \in X$
- The ideal $\mathsf{I} = \langle Y_1^2 - 1, \ldots, Y_m^2 - 1 \rangle$ clearly has exactly X as its zero set: $\mathcal{Z}(\mathsf{I}) = X$
- Since each zero is a simple zero of I, the ideal is *radical*
- So $\mathsf{I} = \mathcal{I}(X)$, the ideal of all polynomials that vanish on X.

Polygons

Let $m = 2$ and consider the regular n-gon X on the unit circle, with equation
$Y_1^2 + Y_2^2 = 1$



Polygons

Let $m = 2$ and consider the regular n-gon X on the unit circle.

$Y_1^2 + Y_2^2 - 1 \in \mathcal{I}(X)$.

Polygons

Let $m = 2$ and consider the regular n-gon X on the unit circle.

$Y_1^2 + Y_2^2 - 1 \in \mathcal{I}(X)$. We call this Nm and consider it "trivial".

Polygons

Let $m = 2$ and consider the regular n-gon X on the unit circle.

$Y_1^2 + Y_2^2 - 1 \in \mathcal{I}(X)$. We call this Nm and consider it "trivial".

By Bezout's Theorem, any polynomial in $\mathcal{I}(X)$ which is not a multiple of Nm has degree $\lceil n/2 \rceil$ or larger.

Polygons

Let $m = 2$ and consider the regular n-gon X on the unit circle.

$Y_1^2 + Y_2^2 - 1 \in \mathcal{I}(X)$. We call this Nm and consider it "trivial".

By Bezout's Theorem, any polynomial in $\mathcal{I}(X)$ which is not a multiple of Nm has degree $\lceil n/2 \rceil$ or larger.

We can choose two zonal polynomials F and G and see that

$$\mathcal{I}(X) = \langle \mathrm{Nm}, F, G \rangle$$

E.g., for the regular hexagon, we may choose
$F(Y) = Y_2(Y_2^2 - 3/4)$ and

$$G(Y) = (\sqrt{3}Y_1 + Y_2)(\sqrt{3}Y_1 + Y_2 - \sqrt{3})(\sqrt{3}Y_1 + Y_2 + \sqrt{3})$$

Basic notation and facts from algebraic geometry

- For $X \subseteq \mathbb{C}^m$, $\mathcal{I}(X)$ is ideal of polynomials that vanish on X

Basic notation and facts from algebraic geometry

- For $X \subseteq \mathbb{C}^m$, $\mathcal{I}(X)$ is ideal of polynomials that vanish on X
- For $\mathcal{S} \subseteq \mathbb{C}[Y_1, \ldots, Y_m]$,
  $\mathcal{Z}(\mathcal{S})$ is the set of common zeros of all $F \in \mathcal{S}$

Basic notation and facts from algebraic geometry

- For $X \subseteq \mathbb{C}^m$, $\mathcal{I}(X)$ is ideal of polynomials that vanish on X
- For $\mathcal{S} \subseteq \mathbb{C}[Y_1, \ldots, Y_m]$,
  $\mathcal{Z}(\mathcal{S})$ is the set of common zeros of all $F \in \mathcal{S}$
- When X is finite $\mathcal{Z}(\mathcal{I}(X)) = X$

Basic notation and facts from algebraic geometry

- For $X \subseteq \mathbb{C}^m$, $\mathcal{I}(X)$ is ideal of polynomials that vanish on X
- For $\mathcal{S} \subseteq \mathbb{C}[Y_1, \ldots, Y_m]$,
  $\mathcal{Z}(\mathcal{S})$ is the set of common zeros of all $F \in \mathcal{S}$
- When X is finite $\mathcal{Z}(\mathcal{I}(X)) = X$
- If $Y \subseteq X$, then $\mathcal{I}(X) \subseteq \mathcal{I}(Y)$

Basic notation and facts from algebraic geometry

- For $X \subseteq \mathbb{C}^m$, $\mathcal{I}(X)$ is ideal of polynomials that vanish on X
- For $\mathcal{S} \subseteq \mathbb{C}[Y_1, \ldots, Y_m]$,
  $\mathcal{Z}(\mathcal{S})$ is the set of common zeros of all $F \in \mathcal{S}$
- When X is finite $\mathcal{Z}(\mathcal{I}(X)) = X$
- If $Y \subseteq X$, then $\mathcal{I}(X) \subseteq \mathcal{I}(Y)$
- For an ideal J, $\mathcal{I}(\mathcal{Z}(\mathrm{J})) = \mathrm{Rad}(\mathrm{J})$ (Nullstellensatz)
  where $\mathrm{Rad}(\mathrm{J}) = \{F \mid \exists n\ F^n \in \mathrm{J}\}$

Basic notation and facts from algebraic geometry

- For $X \subseteq \mathbb{C}^m$, $\mathcal{I}(X)$ is ideal of polynomials that vanish on X
- For $\mathcal{S} \subseteq \mathbb{C}[Y_1, \ldots, Y_m]$,
  $\mathcal{Z}(\mathcal{S})$ is the set of common zeros of all $F \in \mathcal{S}$
- When X is finite $\mathcal{Z}(\mathcal{I}(X)) = X$
- If $Y \subseteq X$, then $\mathcal{I}(X) \subseteq \mathcal{I}(Y)$
- For an ideal J, $\mathcal{I}(\mathcal{Z}(\mathrm{J})) = \mathrm{Rad}(\mathrm{J})$ (Nullstellensatz)
  where $\mathrm{Rad}(\mathrm{J}) = \{F \mid \exists n \; F^n \in \mathrm{J}\}$
- If $\mathcal{Z}(J)$ is finite and J is radical (i.e., $\mathrm{J} = \mathrm{Rad}(\mathrm{J})$), then any ideal containing J is radical

Two "dual girth" parameters

For interesting structures represented by subsets X of Euclidean space, we are interested in two measures of complexity:

- $\gamma_1(X)$: the smallest degree of a non-trivial polynomial in $\mathcal{I}(X)$
- $\gamma_2(X)$: the smallest k for which $\mathcal{I}(X)$ admits a generating set of polynomials of degree k or less

Observe: These two values are invariant under invertible affine transformation.

Two Dual Girth Parameters

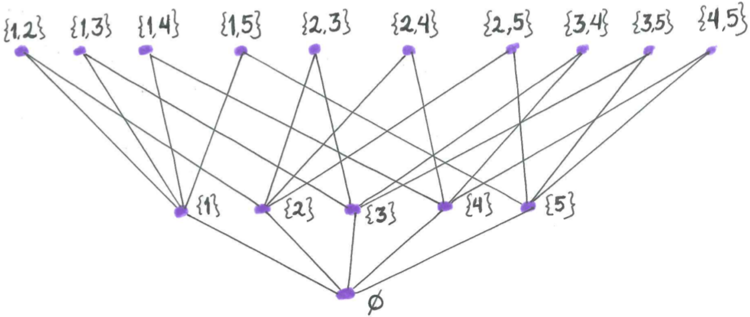
Recap: Trivial polynomials don't depend on X in $\mathcal{X}$. In our case, we will take $\mathcal{X}$ to be the set of all spherical codes in $\mathbb{R}^m$.

If $\mathcal{T}$ denotes the ideal of trivial polynomials, a principal ideal in this case, we may write

$$\gamma_1(X) := \min \{\deg F \mid F \in \mathcal{I}(X),\ F \notin \mathcal{T}\}$$

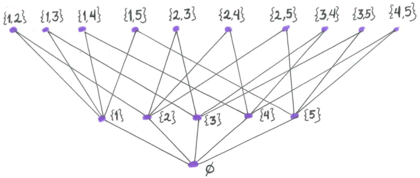
$$\gamma_2(X) := \min \{\max\{\deg F \mid F \in \mathcal{G}\} \ \mid \langle \mathcal{G} \rangle = \mathcal{I}(X)\}$$

Truncated Boolean Lattice



For $n = 5$, $\Omega = \{1, 2, 3, 4, 5\}$ and $k = 2$, we take all subsets of Ω of size at most k, ordered by inclusion.

Truncated Boolean Lattice

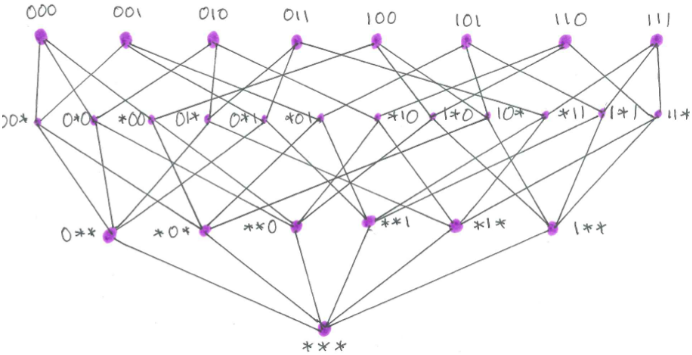


Incidence matrix:

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

X consists of 10 points in $\mathbb{R}^5$ and $\mathcal{I}(X)$ is generated by the obvious quadratics (trivial polynomials for designs).

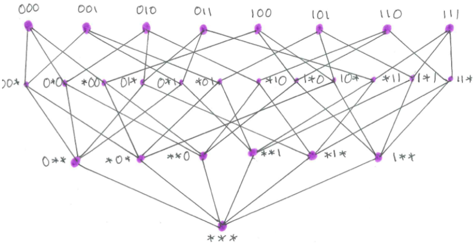
Hamming Lattice



For $n = 3$ and $q = 2$, we consider all "partial" n-tuples over $\mathbb{Z}_q$, marking unspecified entries with '*'. Partial order relation is:

$$a \preceq b \text{ if } a_i = b_i \text{ whenever } a_i \neq *$$

Hamming Lattice



Incidence matrix:

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

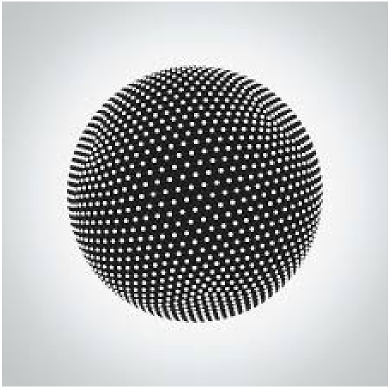
X consists of 8 points in $\mathbb{R}^6$ and $\mathcal{I}(X)$ is generated by trivial polynomials together with

$$Y_1 + Y_6 - 1, \quad Y_2 + Y_5 - 1, \quad Y_3 + Y_4 - 1.$$

Similar ideas work for the Grassmann scheme and the bilinear forms scheme.

Spherical designs

From now on, we will assume that X is contained in some sphere, of radius r say, centered at the origin.



Spherical designs

From now on, we will assume that X is contained in some sphere, of radius r say, centered at the origin.

Spherical designs

From now on, we will assume that X is contained in some sphere, of radius r say, centered at the origin.

So the ideal $\mathcal{I}(X)$ contains the "norm" polynomial

$$\mathrm{Nm} = Y_1^2 + Y_2^2 + \cdots + Y_m^2 - r^2$$

as well as every polynomial in the principal ideal $\langle \mathrm{Nm} \rangle$. In this setting, these polynomials are called "trivial".

Spherical designs

From now on, we will assume that X is contained in some sphere, of radius r say, centered at the origin.

So the ideal $\mathcal{I}(X)$ contains the "norm" polynomial

$$\mathrm{Nm} = Y_1^2 + Y_2^2 + \cdots + Y_m^2 - r^2$$

as well as every polynomial in the principal ideal $\langle \mathrm{Nm} \rangle$. In this setting, these polynomials are called "trivial".

A subset X of the unit sphere is a *spherical t-design* if the average over X of any polynomial F of degree $\leq t$ in m variables is exactly equal to the average of F over the sphere.

Lower Bound on $\gamma_1(X)$ for Spherical t-Designs

The following observation is due to Bannai (probably also known in cubature community).

Lemma

If X is a spherical t-design, then every polynomial in $\mathcal{I}(X)$ of degree $t/2$ or less is trivial.

Lower Bound on $\gamma_1(X)$ for Spherical t-Designs

The following observation is due to Bannai (probably also known in cubature community).

Lemma

If X is a spherical t-design, then every polynomial in $\mathcal{I}(X)$ of degree $t/2$ or less is trivial.

Proof: If $F \in \mathcal{I}(X)$, then F^2 is zero on X, so F^2 averages to zero on the sphere.

Lower Bound on $\gamma_1(X)$ for Spherical t-Designs

The following observation is due to Bannai (probably also known in cubature community).

Lemma

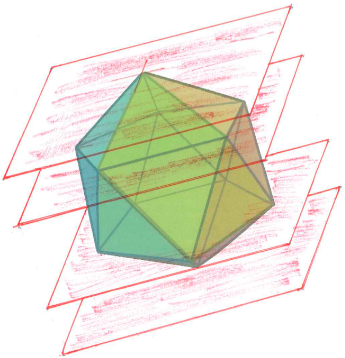
If X is a spherical t-design, then every polynomial in $\mathcal{I}(X)$ of degree $t/2$ or less is trivial.

Proof: If $F \in \mathcal{I}(X)$, then F^2 is zero on X, so F^2 averages to zero on the sphere. But F^2 is a non-negative polynomial function, so F^2 is identically zero on the sphere.

Zonal Polynomials

For a single-variable polynomial $f(t)$ and a point $a \in \mathbb{R}^m$, we define the *zonal polynomial*

$$Z_{f,a}(Y) = f(a \cdot Y)$$



Zonal Polynomials

For a single-variable polynomial $f(t)$ and a point $a \in \mathbb{R}^m$, we define the *zonal polynomial*

$$Z_{f,a}(Y) = f(a \cdot Y)$$

Zonal Polynomials

For a single-variable polynomial $f(t)$ and a point $a \in \mathbb{R}^m$, we define the *zonal polynomial*

$$Z_{f,a}(Y) = f(a \cdot Y)$$

For example, if $f(t) = \prod_{h=0}^{d}(t - \omega_h)$, then

$$Z_{f,a}(Y) = (a_1 Y_1 + \cdots + a_m Y_m - \omega_0) \cdots (a_1 Y_1 + \cdots + a_m Y_m - \omega_d)$$

is a polynomial of degree $d + 1$ in m variables.

Zonal Polynomials

For a single-variable polynomial $f(t)$ and a point $a \in \mathbb{R}^m$, we define the *zonal polynomial*

$$Z_{f,a}(Y) = f(a \cdot Y)$$

For example, if $f(t) = \prod_{h=0}^{d}(t - \omega_h)$, then

$$Z_{f,a}(Y) = (a_1 Y_1 + \cdots + a_m Y_m - \omega_0) \cdots (a_1 Y_1 + \cdots + a_m Y_m - \omega_d)$$

is a polynomial of degree $d+1$ in m variables.

In this case, if $\{a \cdot b \mid b \in X\} \subseteq \{\omega_0, \ldots, \omega_d\}$, then $Z_{f,a} \in \mathcal{I}(X)$.

Ideal of zonals

Now suppose X has inner product set

$$\{a \cdot b \mid a, b \in X\} = \{\omega_0, \ldots, \omega_d\}.$$

Then, for each $a \in X$, the ideal $\mathcal{I}(X)$ contains the zonal polynomial $Z_{f,a}(Y)$ where

$$f(t) = (t - \omega_0) \cdots (t - \omega_d).$$

Ideal of zonals

Now suppose X has inner product set

$$\{a \cdot b \mid a, b \in X\} = \{\omega_0, \ldots, \omega_d\}.$$

Then, for each $a \in X$, the ideal $\mathcal{I}(X)$ contains the zonal polynomial $Z_{f,a}(Y)$ where

$$f(t) = (t - \omega_0) \cdots (t - \omega_d).$$

Observe that, if X spans $\mathbb{R}^m$, then the tangent space at every solution to this system of equations is zero-dimensional.

Ideal of zonals

Now suppose X has inner product set

$$\{a \cdot b \mid a, b \in X\} = \{\omega_0, \ldots, \omega_d\}.$$

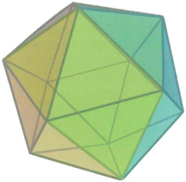
Then, for each $a \in X$, the ideal $\mathcal{I}(X)$ contains the zonal polynomial $Z_{f,a}(Y)$ where

$$f(t) = (t - \omega_0) \cdots (t - \omega_d).$$

Observe that, if X spans $\mathbb{R}^m$, then the tangent space at every solution to this system of equations is zero-dimensional.
So this ideal is radical, as is any ideal that contains it.
We can also show that every solution to this system of polynomial equations lies in $\mathbb{R}^m$
(except for the orthoplex! E.g. the octahedron.)

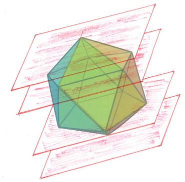
Sliced zonals

Consider the icosahedron



Sliced zonals

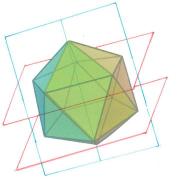
Consider the icosahedron



Not only does our ideal contain the degree four zonal polynomials, but it also contains many degree three *"sliced zonal polynomials"*.

Sliced zonals

Consider the icosahedron



Not only does our ideal contain the degree four zonal polynomials, but it also contains many degree three *"sliced zonal polynomials"*. If $\omega_0 = 1 > \omega_1 > \cdots > \omega_d = -1$, replace

$$Z_{f,a}(Y) = (a \cdot Y - \omega_0)(a \cdot Y - \omega_1) \cdots (a \cdot Y - \omega_d) \qquad \text{by}$$

$$S_{f,a,b}(Y) = (b \cdot Y)(a \cdot Y - \omega_1) \cdots (a \cdot Y - \omega_{d-1})$$

for any $b \perp a$ in $\mathbb{R}^m$ and this also vanishes at each point in X, including a and $-a$.

The Icosahedron and Famous Lattices

These sliced zonal polynomials generate $\mathcal{I}(X)$ in these cases:

Name	Dim	strength	$\gamma_1(X)$	$\gamma_2(X)$
icos.	3	5	3	3
E_6	6	5	3	3
E_7	7	5	3	3
E_8	8	7	4	4
Leech	24	11	6	6

(joint with Corre Love Steele `arXiv:1310.6626`)

These are examples of Q-bipartite association schemes, where $\gamma_1(E_1) \leq d$ is shown using sliced zonals.

Basic Inequalities

$$2 \leq \gamma_1(E_1) \leq \gamma_2(E_1) \leq d + 1$$

The zonal ideal is not always equal to the full ideal (e.g., non-maximal sets of real mutually unbiased bases), but we need only throw in some polynomials of degree d to "shave off" phantom vertices.

A possible dual to homotopy

What we are doing is, in some sense, dual to this.

A possible dual to homotopy

What we are doing is, in some sense, dual to this.

We associate an ideal $\mathcal{I}(X)$ to our combinatorial object X. It is natural to ask

- What is the smallest degree of a non-trivial polynomial in $\mathcal{I}(X)$?

A possible dual to homotopy

What we are doing is, in some sense, dual to this.

We associate an ideal $\mathcal{I}(X)$ to our combinatorial object X. It is natural to ask

- What is the smallest degree of a non-trivial polynomial in $\mathcal{I}(X)$?
- When is $\mathcal{I}(X)$ generated by its small-degree polynomials?

A possible dual to homotopy

What we are doing is, in some sense, dual to this.

We associate an ideal $\mathcal{I}(X)$ to our combinatorial object X. It is natural to ask

- What is the smallest degree of a non-trivial polynomial in $\mathcal{I}(X)$?
- When is $\mathcal{I}(X)$ generated by its small-degree polynomials?
- If the polynomials of degree $\leq k$ do <u>not</u> generate $\mathcal{I}(X)$, what is the variety of the ideal they do generate?

A dual pair of association schemes

The Q-polynomial association scheme (it's just a strongly regular graph) $K_{3,3}$ has eigenmatrix $P = \begin{bmatrix} 1 & 3 & 2 \\ 1 & 0 & -1 \\ 1 & -3 & 2 \end{bmatrix}$ with inverse $\frac{1}{6}\begin{bmatrix} 1 & 4 & 1 \\ 1 & 0 & -1 \\ 1 & -2 & 1 \end{bmatrix}$.

A dual pair of association schemes

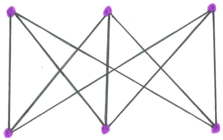
The Q-polynomial association scheme $K_{3,3}$ has eigenmatrix

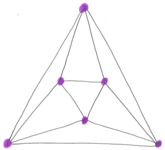
$$P = \begin{bmatrix} 1 & 3 & 2 \\ 1 & 0 & -1 \\ 1 & -3 & 2 \end{bmatrix} \text{ with inverse } \frac{1}{6} \begin{bmatrix} 1 & 4 & 1 \\ 1 & 0 & -1 \\ 1 & -2 & 1 \end{bmatrix}.$$

A dual pair of association schemes

The Q-polynomial association scheme $K_{3,3}$ has eigenmatrix

$$P = \begin{bmatrix} 1 & 3 & 2 \\ 1 & 0 & -1 \\ 1 & -3 & 2 \end{bmatrix} \text{ with inverse } \frac{1}{6}\begin{bmatrix} 1 & 4 & 1 \\ 1 & 0 & -1 \\ 1 & -2 & 1 \end{bmatrix}.$$





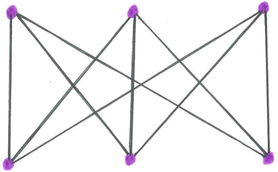
The dual association scheme is the one coming from the octahedron. It has eigenmatrix $\begin{bmatrix} 1 & 4 & 1 \\ 1 & 0 & -1 \\ 1 & -2 & 1 \end{bmatrix}$ with inverse $\frac{1}{6}P$.

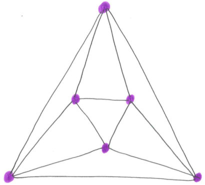
Claim: ideal of $K_{3,3}$ is closely linked to homotopy of octahedron.

A dual pair of association schemes

$K_{3,3}$ has eigenmatrix

$$P = \begin{bmatrix} 1 & 3 & 2 \\ 1 & 0 & -1 \\ 1 & -3 & 2 \end{bmatrix} \text{ with inverse } \frac{1}{6}\begin{bmatrix} 1 & 4 & 1 \\ 1 & 0 & -1 \\ 1 & -2 & 1 \end{bmatrix}.$$





The octahedron has eigenmatrix $\begin{bmatrix} 1 & 4 & 1 \\ 1 & 0 & -1 \\ 1 & -2 & 1 \end{bmatrix}$ with inverse $\frac{1}{6}P$.

Claim: ideal of $K_{3,3}$ is closely linked to homotopy of octahedron.

Association Scheme Duality

Association scheme $(X, \{R_0, \ldots, R_d\})$ has eigenmatrix P whose columns are the eigenvalues of the graphs (X, R_i). (These $d+1$ adjacency matrices are simultaneously diagonalizable. Take my word for it.)

Association Scheme Duality

Association scheme $(X, \{R_0, \ldots, R_d\})$ has eigenmatrix P whose columns are the eigenvalues of the graphs (X, R_i). (These $d+1$ adjacency matrices are simultaneously diagonalizable. Take my word for it.)

We say $(Y, \{R'_0, \ldots, R'_d\})$ is *formally dual* to the scheme above if its eigenmatrix is $\frac{1}{|X|}P^{-1}$ for some ordering of its rows and columns.

Association Scheme Duality

Association scheme $(X, \{R_0, \ldots, R_d\})$ has eigenmatrix P whose columns are the eigenvalues of the graphs (X, R_i). (These $d+1$ adjacency matrices are simultaneously diagonalizable. Take my word for it.)

We say $(Y, \{R'_0, \ldots, R'_d\})$ is *formally dual* to the scheme above if its eigenmatrix is $\frac{1}{|X|}P^{-1}$ for some ordering of its rows and columns.

True duality of association schemes comes to us via the character theory of abelian groups.
Recall that a finite abelian group Γ has $|G|$ linear characters (homomorphisms $\chi : G \to \mathbb{C}^*$) and these form a group under multiplication of functions.

Association Scheme Duality

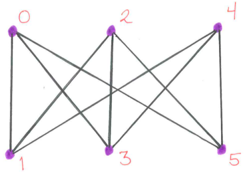
Association scheme $(X, \{R_0, \ldots, R_d\})$ has eigenmatrix P whose columns are the eigenvalues of the graphs (X, R_i). (These $d+1$ adjacency matrices are simultaneously diagonalizable. Take my word for it.)

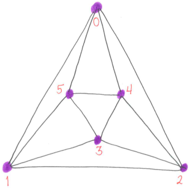
We say $(Y, \{R'_0, \ldots, R'_d\})$ is *formally dual* to the scheme above if its eigenmatrix is $\frac{1}{|X|}P^{-1}$ for some ordering of its rows and columns.

True duality of association schemes comes to us via the character theory of abelian groups.
Recall that a finite abelian group Γ has $|G|$ linear characters (homomorphisms $\chi : G \to \mathbb{C}^*$) and these form a group under multiplication of functions. This group $G^\dagger$ is isomorphic to Γ.

Association Scheme Duality

Both $K_{3,3}$ and the octahedron are translation association schemes: the abelian group $\mathbb{Z}_6$ acts on each as a regular group of automorphisms.





Connection set for $K_{3,3}$ is $\{1, 3, 5\}$; connection set for octahedron is $\{1, 2, 4, 5\}$.

Association Scheme Duality

Connection set for the octahedron is $\{1, 2, 4, 5\}$.

The corresponding characters of $\mathbb{Z}_6$ form a basis for the first eigenspace of $K_{3,3}$. Let ω be a primitive sixth root of unity in $\mathbb{C}$. Then we have

$$\chi_1 = \begin{bmatrix} 1 \\ \omega \\ \omega^2 \\ -1 \\ \omega^4 \\ \omega^5 \end{bmatrix}, \ \chi_2 = \begin{bmatrix} 1 \\ \omega^2 \\ \omega^4 \\ 1 \\ \omega^8 \\ \omega^{10} \end{bmatrix}, \ \chi_4 = \begin{bmatrix} 1 \\ \omega^4 \\ \omega^8 \\ 1 \\ \omega^{16} \\ \omega^{20} \end{bmatrix}, \ \chi_5 = \begin{bmatrix} 1 \\ \omega^5 \\ \omega^4 \\ -1 \\ \omega^2 \\ \omega \end{bmatrix}$$

Characters yield spherical representation of $K_{3,3}$

We put these characters together in a matrix and map vertex i to the i^{th} column of

$$\begin{bmatrix} 1 & \omega & \omega^2 & -1 & \omega^4 & \omega^5 \\ 1 & \omega^2 & \omega^4 & 1 & \omega^2 & \omega^4 \\ 1 & \omega^4 & \omega^2 & 1 & \omega^4 & \omega^2 \\ 1 & \omega^5 & \omega^4 & -1 & \omega^2 & \omega \end{bmatrix}$$

to obtain

$$X = \{(1,1,1,1), (\omega,\omega^2,\omega^4,\omega^5), (\omega^2,\omega^4,\omega^2,\omega^4),$$
$$(-1,1,1,-1), (\omega^4,\omega^2,\omega^4,\omega^2), (\omega^5,\omega^4,\omega^2,\omega)\}$$

Discrete Homotopy on a Graph

Now we observe that every closed walk in the octahdron gives us a nice polynomial in $\mathcal{I}(X)$. E.g. $w = 0450$ gives $Y_4 Y_1 Y_1 - 1$ in $\mathcal{I}(X)$.

Homotopy, Ideals and Duality

The upshot of all this is the following theorem:

If a translation distance-regular graph G has its fundamental group generated by small cycles, then the dual (Q-polynomial) scheme has its ideal generated by small degree polynomials.

$$\pi_k(\Gamma, 0) = \pi(\Gamma, 0) \quad \Rightarrow \quad \gamma_2(E_1) \le \lceil k/2 \rceil \ .$$

Homotopy, Ideals and Duality

Theorem

Let $(X, \{R_0, \ldots, R_d\})$ be a cometric translation association scheme defined on abelian group X and let $(X^\dagger, \{R_0', \ldots, R_d'\})$ be the (metric) dual association scheme defined on the group of characters $X^\dagger$. Let $\Gamma = (X^\dagger, R_1')$ denote the underlying translation distance-regular graph. Let E_1 denote the first primitive idempotent in the corresponding Q-polynomial ordering for the original scheme.

If the homotopy group $\pi(\Gamma, \mathbf{1})$ is generated by closed walks of essential length k or less,then the ideal $\mathcal{I}(E_1)$ is generated by polynomials of degree k or less.

$$\pi_k(\Gamma, 0) = \pi(\Gamma, 0) \quad \Rightarrow \quad \gamma_2(E_1) \le \lceil k/2 \rceil \ .$$

Conjectures

In all six statements, exclude polygons.

- [P] **Conj (Suzuki/Koolen):** Any distance-regular graph has girth at most 12
- [Q] **Conj (WJM):** For any Q-polynomial scheme, $\gamma_2(E_1) \leq 6$
- [P] **Thm (Lewis):** A Q-polynomial drg has girth at most 6
- [Q] **Thm:** For any P- and Q-poly scheme, $\gamma_1(E_1) \leq 3$
- [P] **Thm (Lewis):** When Γ is a Q-poly drg, and not a pseudo-quotient, $\pi_6(\Gamma, a) = \pi(\Gamma, a)$
- [Q] **Conj (WJM):** For any P- and Q-poly scheme, $\gamma_2(E_1) \leq 3$

Consequences and Partial Results

- If we prove $\gamma_1(E_1) \leq 6$ for cometric schemes, we get a new proof of a result of Bannai and Damerell showing the non-existence of tight spherical t-designs
- Note that $\gamma_1 \leq 3$ for a Q-polynomial distance-regular graph with $k > 2$, so these have spherical strength at most five
- Likewise, we would rule out t-designs with $t \geq 12$ in the regular semilattices that induce Q-polynomial schemes
- (WJM & Williford): For Q-polynomial association schemes, $\gamma_2(E_1)$ is bounded by a function of $m_1 := \operatorname{rank} E_1$

Open Problems

- Prove $\gamma_1(E_1) \leq 6$ for important classes of Q-poly schemes
- ... real MUBs, hemisystems in GQs, relative hemisystems, ...
- For regular semilattices, $\gamma_2(E_1) \leq 2$?
- What happens for other (Euclidean) lattices?
- Finite bounds for special classes of schemes would be of value
- as would any finite bounds on γ_2 (or γ_1) even if not at the conjectured optimum
- Can we close the gap between $t/2$ and t for **block designs** or **nonlinear codes**?

Thank You

Frédéric Vanhove, Bled Slovenia, 2011