Construction of combinatorial structures using rational idempotents

Ken W. Smith

Sam Houston State University

(In memory of Bob Liebler)

Workshop on Coding, Cryptology and Combinatorial Designs
Singapore, June 2, 2011

Motivation

Many combinatorial configurations have a large group of symmetries.

A common theme in algebraic combinatorics: Use the structure of the group and its action on the points to obtain information about the configuration.

If an automorphism group G is sharply transitive on a set of points then we may view the structure from within the group ring $\mathbb{Z}[G]$.

Motivation

Many combinatorial configurations have a large group of symmetries.

A common theme in algebraic combinatorics: Use the structure of the group and its action on the points to obtain information about the configuration.

If an automorphism group G is sharply transitive on a set of points then we may view the structure from within the group ring $\mathbb{Z}[G]$.

Motivation

Many combinatorial configurations have a large group of symmetries.

A common theme in algebraic combinatorics: Use the structure of the group and its action on the points to obtain information about the configuration.

If an automorphism group G is sharply transitive on a set of points then we may view the structure from within the group ring $\mathbb{Z}[G]$.

Examples of combinatorial structures in group rings

If the configuration has a sharply transitive automorphism group:

symmetric (v, k, λ) **design** with sharply transitive G
$\iff$ (v, k, λ) **difference set** $D \in \mathbb{Z}[G]$.

A **strongly regular** (v, k, λ, μ) **graph** with sharply transitive G
$\iff$ (v, k, λ, μ) **partial difference set** $S \in \mathbb{Z}[G]$.

A **group divisible design** (v, m, k, n) with sharply transitive G
$\iff$ (v, m, k, n) **relative difference set** $R \in \mathbb{Z}[G]$.

A **distance regular graph** with sharply transitive G
$\iff$ **translation scheme** $S \in \mathbb{Z}[G]$.
Other examples include **circulant weighing matrices**, **group developed weighing matrices**, **perfect ternary arrays**....

Examples of combinatorial structures in group rings

If the configuration has a sharply transitive automorphism group:

symmetric (v, k, λ) **design** with sharply transitive G
$\iff$ (v, k, λ) **difference set** $D \in \mathbb{Z}[G]$.

A **strongly regular** (v, k, λ, μ) **graph** with sharply transitive G
$\iff$ (v, k, λ, μ) **partial difference set** $S \in \mathbb{Z}[G]$.

A **group divisible design** (v, m, k, n) with sharply transitive G
$\iff$ (v, m, k, n) **relative difference set** $R \in \mathbb{Z}[G]$.

A **distance regular graph** with sharply transitive G
$\iff$ **translation scheme** $S \in \mathbb{Z}[G]$.
Other examples include **circulant weighing matrices**, **group developed weighing matrices**, **perfect ternary arrays**....

Examples of combinatorial structures in group rings

If the configuration has a sharply transitive automorphism group:

symmetric (v, k, λ) **design** with sharply transitive G
$\iff$ (v, k, λ) **difference set** $D \in \mathbb{Z}[G]$.

A **strongly regular** (v, k, λ, μ) **graph** with sharply transitive G
$\iff$ (v, k, λ, μ) **partial difference set** $S \in \mathbb{Z}[G]$.

A **group divisible design** (v, m, k, n) with sharply transitive G
$\iff$ (v, m, k, n) **relative difference set** $R \in \mathbb{Z}[G]$.

A **distance regular graph** with sharply transitive G
$\iff$ **translation scheme** $S \in \mathbb{Z}[G]$.
Other examples include **circulant weighing matrices**, **group developed weighing matrices**, **perfect ternary arrays**....

Examples of combinatorial structures in group rings

If the configuration has a sharply transitive automorphism group:

symmetric (v, k, λ) **design** with sharply transitive G
$\iff$ (v, k, λ) **difference set** $D \in \mathbb{Z}[G]$.

A **strongly regular** (v, k, λ, μ) **graph** with sharply transitive G
$\iff$ (v, k, λ, μ) **partial difference set** $S \in \mathbb{Z}[G]$.

A **group divisible design** (v, m, k, n) with sharply transitive G
$\iff$ (v, m, k, n) **relative difference set** $R \in \mathbb{Z}[G]$.

A **distance regular graph** with sharply transitive G
$\iff$ **translation scheme** $S \in \mathbb{Z}[G]$.
Other examples include **circulant weighing matrices**, **group developed weighing matrices**, **perfect ternary arrays**....

Examples of combinatorial structures in group rings

If the configuration has a sharply transitive automorphism group:

symmetric (v, k, λ) **design** with sharply transitive G
$\iff$ (v, k, λ) **difference set** $D \in \mathbb{Z}[G]$.

A **strongly regular** (v, k, λ, μ) **graph** with sharply transitive G
$\iff$ (v, k, λ, μ) **partial difference set** $S \in \mathbb{Z}[G]$.

A **group divisible design** (v, m, k, n) with sharply transitive G
$\iff$ (v, m, k, n) **relative difference set** $R \in \mathbb{Z}[G]$.

A **distance regular graph** with sharply transitive G
$\iff$ **translation scheme** $S \in \mathbb{Z}[G]$.

Other examples include **circulant weighing matrices**, **group developed weighing matrices**, **perfect ternary arrays**....

Examples of combinatorial structures in group rings

If the configuration has a sharply transitive automorphism group:

symmetric (v, k, λ) **design** with sharply transitive G
$\iff$ (v, k, λ) **difference set** $D \in \mathbb{Z}[G]$.

A **strongly regular** (v, k, λ, μ) **graph** with sharply transitive G
$\iff$ (v, k, λ, μ) **partial difference set** $S \in \mathbb{Z}[G]$.

A **group divisible design** (v, m, k, n) with sharply transitive G
$\iff$ (v, m, k, n) **relative difference set** $R \in \mathbb{Z}[G]$.

A **distance regular graph** with sharply transitive G
$\iff$ **translation scheme** $S \in \mathbb{Z}[G]$.
Other examples include **circulant weighing matrices**, **group developed weighing matrices**, **perfect ternary arrays**....

A little ring theory

Combinatorial objects involve the integers. If the object has a sharply transitive group G then we view it as living in $\mathbb{Z}[G]$.
But analysis of the configuration often involves representations of the underlying group G and so we consider $\mathbb{C}[G]$.

So we consider a tower of group rings

$$\mathbb{Z}[G] \subset \mathbb{Q}[G] \subset K[G] \subset \mathbb{C}[G]$$

(where $K = \mathbb{Q}(\zeta)$ is the splitting field of G.)

The interplay between $\mathbb{Z}[G]$ and $\mathbb{Q}(\zeta)[G]$ determines existence and nonexistence of potential combinatorial structures.
We explore that relationship here.

A little ring theory

Combinatorial objects involve the integers. If the object has a sharply transitive group G then we view it as living in $\mathbb{Z}[G]$.
But analysis of the configuration often involves representations of the underlying group G and so we consider $\mathbb{C}[G]$.

So we consider a tower of group rings

$$\mathbb{Z}[G] \subset \mathbb{Q}[G] \subset K[G] \subset \mathbb{C}[G]$$

(where $K = \mathbb{Q}(\zeta)$ is the splitting field of G.)

The interplay between $\mathbb{Z}[G]$ and $\mathbb{Q}(\zeta)[G]$ determines existence and nonexistence of potential combinatorial structures.
We explore that relationship here.

A little ring theory

Combinatorial objects involve the integers. If the object has a sharply transitive group G then we view it as living in $\mathbb{Z}[G]$.
But analysis of the configuration often involves representations of the underlying group G and so we consider $\mathbb{C}[G]$.

So we consider a tower of group rings

$$\mathbb{Z}[G] \subset \mathbb{Q}[G] \subset K[G] \subset \mathbb{C}[G]$$

(where $K = \mathbb{Q}(\zeta)$ is the splitting field of G.)

The interplay between $\mathbb{Z}[G]$ and $\mathbb{Q}(\zeta)[G]$ determines existence and nonexistence of potential combinatorial structures.
We explore that relationship here.

An example

Consider the $(16, 6, 2)$ difference $D = \{x, x^3, y, y^3, xy, x^3y^3\}$ in $G =< x, y : x^4 = y^4 = [x, y] = 1 >$.
This is a group-developed Hadamard 16×16 matrix with G acting on the rows and columns.

Write $D = x + x^3 + y + y^3 + xy + x^3y^3$. ("Abuse" of notation.)
Abelian G has 16 characters (= linear representations)

1. The trivial character maps D to 6; it simply *counts*.
2. Six characters map D to the real number 2.
3. The remaining nine characters map D to -2.

$D = 6E_0 + 2E_1 - 2E_2$ where E_0, E_1 and E_2 are idempotents corresponding to the eigenvalues (character values.)

This is not new.
But ....

An example

Consider the $(16, 6, 2)$ difference $D = \{x, x^3, y, y^3, xy, x^3y^3\}$ in $G =< x, y : x^4 = y^4 = [x, y] = 1 >$.
This is a group-developed Hadamard 16×16 matrix with G acting on the rows and columns.
Write $D = x + x^3 + y + y^3 + xy + x^3y^3$. ("Abuse" of notation.)
Abelian G has 16 characters (= linear representations)

1. The trivial character maps D to 6; it simply *counts*.
2. Six characters map D to the real number 2.
3. The remaining nine characters map D to -2.

$D = 6E_0 + 2E_1 - 2E_2$ where E_0, E_1 and E_2 are idempotents corresponding to the eigenvalues (character values.)

This is not new.
But ....

An example

Consider the $(16, 6, 2)$ difference $D = \{x, x^3, y, y^3, xy, x^3y^3\}$ in $G =< x, y : x^4 = y^4 = [x, y] = 1 >$.
This is a group-developed Hadamard 16×16 matrix with G acting on the rows and columns.
Write $D = x + x^3 + y + y^3 + xy + x^3y^3$. ("Abuse" of notation.)
Abelian G has 16 characters (= linear representations)

1. The trivial character maps D to 6; it simply *counts*.
2. Six characters map D to the real number 2.
3. The remaining nine characters map D to -2.

$D = 6E_0 + 2E_1 - 2E_2$ where E_0, E_1 and E_2 are idempotents corresponding to the eigenvalues (character values.)

This is not new.
But ....

An example

Consider the $(16, 6, 2)$ difference $D = \{x, x^3, y, y^3, xy, x^3y^3\}$ in $G =< x, y : x^4 = y^4 = [x, y] = 1 >$.
This is a group-developed Hadamard 16×16 matrix with G acting on the rows and columns.
Write $D = x + x^3 + y + y^3 + xy + x^3y^3$. ("Abuse" of notation.)
Abelian G has 16 characters (= linear representations)

1. The trivial character maps D to 6; it simply *counts*.
2. Six characters map D to the real number 2.
3. The remaining nine characters map D to -2.

$D = 6E_0 + 2E_1 - 2E_2$ where E_0, E_1 and E_2 are idempotents corresponding to the eigenvalues (character values.)

This is not new.
But ....

An example

Consider the $(16, 6, 2)$ difference $D = \{x, x^3, y, y^3, xy, x^3y^3\}$ in $G =< x, y : x^4 = y^4 = [x, y] = 1 >$.
This is a group-developed Hadamard 16×16 matrix with G acting on the rows and columns.
Write $D = x + x^3 + y + y^3 + xy + x^3y^3$. ("Abuse" of notation.)
Abelian G has 16 characters (= linear representations)

1. The trivial character maps D to 6; it simply *counts*.
2. Six characters map D to the real number 2.
3. The remaining nine characters map D to -2.

$D = 6E_0 + 2E_1 - 2E_2$ where E_0, E_1 and E_2 are idempotents corresponding to the eigenvalues (character values.)

This is not new.
But ....

An example

Consider the $(16, 6, 2)$ difference $D = \{x, x^3, y, y^3, xy, x^3y^3\}$ in $G =< x, y : x^4 = y^4 = [x, y] = 1 >$.
This is a group-developed Hadamard 16×16 matrix with G acting on the rows and columns.
Write $D = x + x^3 + y + y^3 + xy + x^3y^3$. ("Abuse" of notation.)
Abelian G has 16 characters (= linear representations)

1. The trivial character maps D to 6; it simply *counts*.
2. Six characters map D to the real number 2.
3. The remaining nine characters map D to -2.

$D = 6E_0 + 2E_1 - 2E_2$ where E_0, E_1 and E_2 are idempotents corresponding to the eigenvalues (character values.)

This is not new.
But ....

An example

Consider the $(16, 6, 2)$ difference $D = \{x, x^3, y, y^3, xy, x^3y^3\}$ in $G =< x, y : x^4 = y^4 = [x, y] = 1 >$.
This is a group-developed Hadamard 16×16 matrix with G acting on the rows and columns.
Write $D = x + x^3 + y + y^3 + xy + x^3y^3$. ("Abuse" of notation.)
Abelian G has 16 characters (= linear representations)

1. The trivial character maps D to 6; it simply *counts*.
2. Six characters map D to the real number 2.
3. The remaining nine characters map D to -2.

$D = 6E_0 + 2E_1 - 2E_2$ where E_0, E_1 and E_2 are idempotents corresponding to the eigenvalues (character values.)

This is not new.
But ....

An example

Consider the $(16, 6, 2)$ difference $D = \{x, x^3, y, y^3, xy, x^3y^3\}$ in $G =< x, y : x^4 = y^4 = [x, y] = 1 >$.
This is a group-developed Hadamard 16×16 matrix with G acting on the rows and columns.
Write $D = x + x^3 + y + y^3 + xy + x^3y^3$. ("Abuse" of notation.)
Abelian G has 16 characters (= linear representations)

1. The trivial character maps D to 6; it simply *counts*.
2. Six characters map D to the real number 2.
3. The remaining nine characters map D to -2.

$D = 6E_0 + 2E_1 - 2E_2$ where E_0, E_1 and E_2 are idempotents corresponding to the eigenvalues (character values.)

This is not new.
But ....

Array notation

If $G =< x, y >$ then an element of $S \in \mathbb{Z}[G]$ has form

$$S = \sum_{i,j} s_{i,j} x^i y^j$$

We write this as an array

$$\begin{pmatrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1,0} & s_{1,1} & s_{1,2} & s_{1,3} \\ s_{2,0} & s_{2,1} & s_{2,2} & s_{2,3} \\ s_{3,0} & s_{3,1} & s_{3,2} & s_{3,3} \end{pmatrix}$$

Example: $S = y + 2y^2 + 3y^3 + 4x + 5xy + 6xy^2 + 7xy^3$ in $\mathbb{Z}[C_2 \times C_4]$ is written

$$\begin{pmatrix} 0 & 1 & 2 & 3 \\ 4 & 5 & 6 & 7 \end{pmatrix}$$

Array notation

If $G =< x, y >$ then an element of $S \in \mathbb{Z}[G]$ has form

$$S = \sum_{i,j} s_{i,j} x^i y^j$$

We write this as an array

$$\begin{pmatrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1,0} & s_{1,1} & s_{1,2} & s_{1,3} \\ s_{2,0} & s_{2,1} & s_{2,2} & s_{2,3} \\ s_{3,0} & s_{3,1} & s_{3,2} & s_{3,3} \end{pmatrix}$$

Example: $S = y + 2y^2 + 3y^3 + 4x + 5xy + 6xy^2 + 7xy^3$ in $\mathbb{Z}[C_2 \times C_4]$ is written

$$\begin{pmatrix} 0 & 1 & 2 & 3 \\ 4 & 5 & 6 & 7 \end{pmatrix}$$

Homomorphisms

$$D = x + x^3 + y + y^3 + xy + x^3y^3 = \left(\begin{array}{cc|cc} 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{array}\right)$$

has homomorphic images

$$D/ < x^2 > = (2x + y + y^3 + xy + xy^3) < x^2 > = \left(\begin{array}{cc|cc} 0 & 1 & 0 & 1 \\ 2 & 1 & 0 & 1 \end{array}\right) < x^2 >$$

$$D/ < x^2, y^2 > = (2x + 2y + 2xy) < x^2, y^2 > = \begin{pmatrix} 0 & 2 \\ 2 & 2 \end{pmatrix} < x^2, y^2 >$$

and $\begin{pmatrix} 2 & 4 \end{pmatrix}$ and $\begin{pmatrix} 6 \end{pmatrix}$.

Homomorphisms

$$D = x + x^3 + y + y^3 + xy + x^3y^3 = \left(\begin{array}{cc|cc} 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{array}\right)$$

has homomorphic images

$$D/ < x^2 > = (2x + y + y^3 + xy + xy^3) < x^2 > = \left(\begin{array}{cc|cc} 0 & 1 & 0 & 1 \\ 2 & 1 & 0 & 1 \end{array}\right) < x^2 >$$

$$D/ < x^2, y^2 > = (2x + 2y + 2xy) < x^2, y^2 > = \begin{pmatrix} 0 & 2 \\ 2 & 2 \end{pmatrix} < x^2, y^2 >$$

and $\begin{pmatrix} 2 & 4 \end{pmatrix}$ and $\begin{pmatrix} 6 \end{pmatrix}$.

Homomorphisms

$$D = x + x^3 + y + y^3 + xy + x^3y^3 = \left(\begin{array}{cc|cc} 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{array}\right)$$

has homomorphic images

$$D/ < x^2 > = (2x+y+y^3+xy+xy^3) < x^2 > = \left(\begin{array}{cc|cc} 0 & 1 & 0 & 1 \\ 2 & 1 & 0 & 1 \end{array}\right) < x^2 >$$

$$D/ < x^2, y^2 > = (2x + 2y + 2xy) < x^2, y^2 > = \begin{pmatrix} 0 & 2 \\ 2 & 2 \end{pmatrix} < x^2, y^2 >$$

and $\begin{pmatrix} 2 & 4 \end{pmatrix}$ and $\begin{pmatrix} 6 \end{pmatrix}$.

Homomorphisms

$$D = x + x^3 + y + y^3 + xy + x^3y^3 = \left(\begin{array}{cc|cc} 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{array}\right)$$

has homomorphic images

$$D/ < x^2 > = (2x+y+y^3+xy+xy^3) < x^2 > = \left(\begin{array}{cc|cc} 0 & 1 & 0 & 1 \\ 2 & 1 & 0 & 1 \end{array}\right) < x^2 >$$

$$D/ < x^2, y^2 > = (2x + 2y + 2xy) < x^2, y^2 > = \begin{pmatrix} 0 & 2 \\ 2 & 2 \end{pmatrix} < x^2, y^2 >$$

and $\begin{pmatrix} 2 & 4 \end{pmatrix}$ and $\begin{pmatrix} 6 \end{pmatrix}$.

Homomorphisms and character values

These images are determined by certain character values:

$$D/ < x, y >= (6)\,.$$

$D/ < x, y^2 >= \begin{pmatrix} 2 & 4 \end{pmatrix}$ adds an eigenvalue -2.

$$D/ < x^2, y^2 >= \begin{pmatrix} 0 & 2 \\ 2 & 2 \end{pmatrix} < x^2, y^2 >$$

adds two more copies of -2 as eigenvalue

$$D/ < x^2 >= \left(\begin{array}{cc|cc} 0 & 1 & 0 & 1 \\ 2 & 1 & 0 & 1 \end{array}\right) < x >$$

add 2 eigenvalues equal to -2 and 2 equal to $+2$ and eventually we get

$$D = \left(\begin{array}{cc|cc} 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{array}\right)$$

Homomorphisms and character values

These images are determined by certain character values:

$$D/ < x, y >= (6) .$$

$D/ < x, y^2 >= \begin{pmatrix} 2 & 4 \end{pmatrix}$ adds an eigenvalue -2.

$$D/ < x^2, y^2 >= \begin{pmatrix} 0 & 2 \\ 2 & 2 \end{pmatrix} < x^2, y^2 >$$

adds two more copies of -2 as eigenvalue

$$D/ < x^2 >= \left(\begin{array}{cc|cc} 0 & 1 & 0 & 1 \\ 2 & 1 & 0 & 1 \end{array}\right) < x >$$

add 2 eigenvalues equal to -2 and 2 equal to $+2$ and eventually we get

$$D = \left(\begin{array}{cc|cc} 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{array}\right)$$

Homomorphisms and character values

These images are determined by certain character values:

$$D/ < x, y >= (6) .$$

$D/ < x, y^2 >= \begin{pmatrix} 2 & 4 \end{pmatrix}$ adds an eigenvalue -2.

$$D/ < x^2, y^2 >= \begin{pmatrix} 0 & 2 \\ 2 & 2 \end{pmatrix} < x^2, y^2 >$$

adds two more copies of -2 as eigenvalue

$$D/ < x^2 >= \left(\begin{array}{cc|cc} 0 & 1 & 0 & 1 \\ 2 & 1 & 0 & 1 \end{array}\right) < x >$$

add 2 eigenvalues equal to -2 and 2 equal to $+2$ and eventually we get

$$D = \left(\begin{array}{cc|cc} 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{array}\right)$$

Homomorphisms and character values

These images are determined by certain character values:

$$D/ < x, y >= (6) .$$

$D/ < x, y^2 >= \begin{pmatrix} 2 & 4 \end{pmatrix}$ adds an eigenvalue -2.

$$D/ < x^2, y^2 >= \begin{pmatrix} 0 & 2 \\ 2 & 2 \end{pmatrix} < x^2, y^2 >$$

adds two more copies of -2 as eigenvalue

$$D/ < x^2 >= \left(\begin{array}{cc|cc} 0 & 1 & 0 & 1 \\ 2 & 1 & 0 & 1 \end{array}\right) < x^2 >$$

add 2 eigenvalues equal to -2 and 2 equal to $+2$ and eventually we get

$$D = \left(\begin{array}{cc|cc} 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{array}\right)$$

Homomorphisms and character values

These images are determined by certain character values:

$$D/ < x, y >= (6) .$$

$D/ < x, y^2 >= \begin{pmatrix} 2 & 4 \end{pmatrix}$ adds an eigenvalue -2.

$$D/ < x^2, y^2 >= \begin{pmatrix} 0 & 2 \\ 2 & 2 \end{pmatrix} < x^2, y^2 >$$

adds two more copies of -2 as eigenvalue

$$D/ < x^2 >= \left(\begin{array}{cc|cc} 0 & 1 & 0 & 1 \\ 2 & 1 & 0 & 1 \end{array}\right) < x^2 >$$

add 2 eigenvalues equal to -2 and 2 equal to $+2$ and eventually we get

$$D = \left(\begin{array}{cc|cc} 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{array}\right)$$

Rational Idempotents

If G is an abelian group, the group ring $\mathbb{C}[G]$ has two natural bases, the "standard" basis and the "Fourier" basis:

The standard basis is

$$B_1 = \{g : g \in G\}.$$

If $\chi \in G^*$ is a character of G then define

$$e_\chi := \frac{1}{|G|} \sum_{g \in G} \overline{\chi(g)}\ g.$$

The "Fourier basis" is

$$B_2 = \{e_\chi : \chi \in G^*\}$$

We extend a character $\chi \in G^*$ to $\mathbb{C}[G]$ as follows:

$$\sum_{g \in G} s_g\ g \mapsto \sum_{g \in G} s_g\ \chi(g).$$

Rational Idempotents

If G is an abelian group, the group ring $\mathbb{C}[G]$ has two natural bases, the "standard" basis and the "Fourier" basis:
The standard basis is

$$B_1 = \{g : g \in G\}.$$

If $\chi \in G^*$ is a character of G then define

$$e_\chi := \frac{1}{|G|} \sum_{g \in G} \overline{\chi(g)}\ g.$$

The "Fourier basis" is

$$B_2 = \{e_\chi : \chi \in G^*\}$$

We extend a character $\chi \in G^*$ to $\mathbb{C}[G]$ as follows:

$$\sum_{g \in G} s_g\ g \mapsto \sum_{g \in G} s_g\ \chi(g).$$

Rational Idempotents

If G is an abelian group, the group ring $\mathbb{C}[G]$ has two natural bases, the "standard" basis and the "Fourier" basis:
The standard basis is

$$B_1 = \{g : g \in G\}.$$

If $\chi \in G^*$ is a character of G then define

$$e_\chi := \frac{1}{|G|} \sum_{g \in G} \overline{\chi(g)}\ g.$$

The "Fourier basis" is

$$B_2 = \{e_\chi : \chi \in G^*\}$$

We extend a character $\chi \in G^*$ to $\mathbb{C}[G]$ as follows:

$$\sum_{g \in G} s_g\ g \mapsto \sum_{g \in G} s_g\ \chi(g).$$

Rational Idempotents

If G is an abelian group, the group ring $\mathbb{C}[G]$ has two natural bases, the "standard" basis and the "Fourier" basis:
The standard basis is

$$B_1 = \{g : g \in G\}.$$

If $\chi \in G^*$ is a character of G then define

$$e_\chi := \frac{1}{|G|} \sum_{g \in G} \overline{\chi(g)}\, g.$$

The "Fourier basis" is

$$B_2 = \{e_\chi : \chi \in G^*\}$$

We extend a character $\chi \in G^*$ to $\mathbb{C}[G]$ as follows:

$$\sum_{g \in G} s_g\, g \mapsto \sum_{g \in G} s_g\, \chi(g).$$

Rational Idempotents

If G is an abelian group, the group ring $\mathbb{C}[G]$ has two natural bases, the "standard" basis and the "Fourier" basis:
The standard basis is

$$B_1 = \{g : g \in G\}.$$

If $\chi \in G^*$ is a character of G then define

$$e_\chi := \frac{1}{|G|} \sum_{g \in G} \overline{\chi(g)}\ g.$$

The "Fourier basis" is

$$B_2 = \{e_\chi : \chi \in G^*\}$$

We extend a character $\chi \in G^*$ to $\mathbb{C}[G]$ as follows:

$$\sum_{g \in G} s_g\ g \ \mapsto \ \sum_{g \in G} s_g\ \chi(g).$$

The significance of the Fourier basis

Recall $e_\chi := \frac{1}{|G|} \sum_{g \in G} \overline{\chi(g)}\, g$.

Theorem. Let $\chi, \psi \in G^*,\ \chi \neq \psi$. Then (via orthogonality relations on characters)

1. $e_\chi e_\psi = 0$.
2. $e_\chi^2 = e_\chi$.

Thus the set $B_2 = \{e_\chi : \chi \in G^*\}$ is a set of "orthogonal" principle central idempotents.

Theorem. If $S \in \mathbb{C}[G]$ then $S = \sum_{\chi \in G^*} \chi(S)\, e_\chi$.

The significance of the Fourier basis

Recall $e_\chi := \frac{1}{|G|} \sum_{g \in G} \overline{\chi(g)}\, g$.

Theorem. Let $\chi, \psi \in G^*,\ \chi \neq \psi$. Then (via orthogonality relations on characters)

1. $e_\chi e_\psi = 0$.
2. $e_\chi^2 = e_\chi$.

Thus the set $B_2 = \{e_\chi : \chi \in G^*\}$ is a set of "orthogonal" principle central idempotents.

Theorem. If $S \in \mathbb{C}[G]$ then $S = \sum_{\chi \in G^*} \chi(S)\, e_\chi$.

The significance of the Fourier basis

Recall $e_\chi := \frac{1}{|G|} \sum_{g \in G} \overline{\chi(g)}\, g$.

Theorem. Let $\chi, \psi \in G^*,\ \chi \neq \psi$. Then (via orthogonality relations on characters)

1. $e_\chi e_\psi = 0$.
2. $e_\chi^2 = e_\chi$.

Thus the set $B_2 = \{e_\chi : \chi \in G^*\}$ is a set of "orthogonal" principle central idempotents.

Theorem. If $S \in \mathbb{C}[G]$ then $S = \sum_{\chi \in G^*} \chi(S)\, e_\chi$.

The significance of the Fourier basis

Recall $e_\chi := \frac{1}{|G|} \sum_{g \in G} \overline{\chi(g)}\, g$.

Theorem. Let $\chi, \psi \in G^*,\ \chi \neq \psi$. Then (via orthogonality relations on characters)

1. $e_\chi e_\psi = 0$.
2. $e_\chi^2 = e_\chi$.

Thus the set $B_2 = \{e_\chi : \chi \in G^*\}$ is a set of "orthogonal" principle central idempotents.

Theorem. If $S \in \mathbb{C}[G]$ then $S = \sum_{\chi \in G^*} \chi(S)\, e_\chi$.

An alias for S

Theorem. If $S \in \mathbb{C}[G]$ then

$$S = \sum_{\chi \in G^*} \chi(S)\ e_\chi.$$

Furthermore, let α_χ be any element of $\mathbb{C}[G]$ such that $\chi(\alpha_\chi) = \chi(S)$. Then

$$S = \sum_{\chi \in G^*} \chi(\alpha_\chi)\ e_\chi.$$

An element α_χ is an **alias** for S (with respect to χ.)

An alias for S

Theorem. If $S \in \mathbb{C}[G]$ then

$$S = \sum_{\chi \in G^*} \chi(S)\ e_\chi.$$

Furthermore, let α_χ be any element of $\mathbb{C}[G]$ such that $\chi(\alpha_\chi) = \chi(S)$. Then

$$S = \sum_{\chi \in G^*} \chi(\alpha_\chi)\ e_\chi.$$

An element α_χ is an **alias** for S (with respect to χ.)

An alias for S

Theorem. If $S \in \mathbb{C}[G]$ then

$$S = \sum_{\chi \in G^*} \chi(S)\ e_\chi.$$

Furthermore, let α_χ be any element of $\mathbb{C}[G]$ such that $\chi(\alpha_\chi) = \chi(S)$. Then

$$S = \sum_{\chi \in G^*} \chi(\alpha_\chi)\ e_\chi.$$

An element α_χ is an **alias** for S (with respect to χ.)

Rational idempotents

Define an equivalence relation $\sim$ on G^* by

$$\chi \sim \chi' \iff Ker(\chi) = Ker(\chi').$$

and define

$$[e_\chi] := \sum_{\chi' \sim \chi} e_{\chi'}.$$

$[e_\chi]$ is an idempotent fixed by all Galois automorphisms of the splitting field K of G.
Therefore $[e_\chi]$ is in $\mathbb{Q}[G]$; it is a rational idempotent.
Furthermore, *all* the "primitive" rational idempotents of $\mathbb{Q}[G]$ have this form.

Rational idempotents

Define an equivalence relation $\sim$ on G^* by

$$\chi \sim \chi' \iff Ker(\chi) = Ker(\chi').$$

and define

$$[e_\chi] := \sum_{\chi' \sim \chi} e_{\chi'}.$$

$[e_\chi]$ is an idempotent fixed by all Galois automorphisms of the splitting field K of G.

Therefore $[e_\chi]$ is in $\mathbb{Q}[G]$; it is a rational idempotent.

Furthermore, *all* the "primitive" rational idempotents of $\mathbb{Q}[G]$ have this form.

Rational idempotents

Define an equivalence relation $\sim$ on G^* by

$$\chi \sim \chi' \iff Ker(\chi) = Ker(\chi').$$

and define

$$[e_\chi] := \sum_{\chi' \sim \chi} e_{\chi'}.$$

$[e_\chi]$ is an idempotent fixed by all Galois automorphisms of the splitting field K of G.
Therefore $[e_\chi]$ is in $\mathbb{Q}[G]$; it is a rational idempotent.
Furthermore, *all* the "primitive" rational idempotents of $\mathbb{Q}[G]$ have this form.

Rational idempotents

Define an equivalence relation $\sim$ on G^* by

$$\chi \sim \chi' \iff Ker(\chi) = Ker(\chi').$$

and define

$$[e_\chi] := \sum_{\chi' \sim \chi} e_{\chi'}.$$

$[e_\chi]$ is an idempotent fixed by all Galois automorphisms of the splitting field K of G.
Therefore $[e_\chi]$ is in $\mathbb{Q}[G]$; it is a rational idempotent.
Furthermore, *all* the "primitive" rational idempotents of $\mathbb{Q}[G]$ have this form.

Rational Idempotents,Main Theorem

Since

$$\mathbb{Z}[G] \subseteq \mathbb{Q}[G] \subseteq K[G] \subseteq \mathbb{C}[G],$$

we seek to write all elements of $\mathbb{Z}[G]$ in terms of the rational idempotents.

Theorem. (EMPHASIZE!)
If $S \in \mathbb{Z}[G]$ then for each equivalence class of characters $\chi/\sim$ choose any alias $\alpha_\chi \in \mathbb{Z}[G]$ for S.
Then

$$S = \sum_{\chi \in G^*/\sim} \alpha_\chi \, [e_\chi]$$

The aliases α_χ will vary with the equivalence classes of the characters but are constant across equivalence classes.
(Notice the flexibility in the choice of aliases.)

Rational Idempotents,Main Theorem

Since

$$\mathbb{Z}[G] \subseteq \mathbb{Q}[G] \subseteq K[G] \subseteq \mathbb{C}[G],$$

we seek to write all elements of $\mathbb{Z}[G]$ in terms of the rational idempotents.

Theorem. (EMPHASIZE!)
If $S \in \mathbb{Z}[G]$ then for each equivalence class of characters $\chi/\sim$ choose any alias $\alpha_\chi \in \mathbb{Z}[G]$ for S.
Then

$$S = \sum_{\chi \in G^*/\sim} \alpha_\chi \, [e_\chi]$$

The aliases α_χ will vary with the equivalence classes of the characters but are constant across equivalence classes.
(Notice the flexibility in the choice of aliases.)

Rational Idempotents,Main Theorem

Since

$$\mathbb{Z}[G] \subseteq \mathbb{Q}[G] \subseteq K[G] \subseteq \mathbb{C}[G],$$

we seek to write all elements of $\mathbb{Z}[G]$ in terms of the rational idempotents.

Theorem. (EMPHASIZE!)
If $S \in \mathbb{Z}[G]$ then for each equivalence class of characters $\chi/\sim$ choose any alias $\alpha_\chi \in \mathbb{Z}[G]$ for S.
Then

$$S = \sum_{\chi \in G^*/\sim} \alpha_\chi \, [e_\chi]$$

The aliases α_χ will vary with the equivalence classes of the characters but are constant across equivalence classes.
(Notice the flexibility in the choice of aliases.)

Rational Idempotents, cont.

If $G =< x : x^{p^b} = 1 >$ is a cyclic p-group then the primitive rational idempotents of G have the form

$$[e_\chi] = \frac{p < x^{p^{j+1}} > - < x^{p^j} >}{p^{b-j}}.$$

If G is cyclic, the primitive rational idempotents of G are products of primitive idempotents from the Sylow subgroups.

So we know all the primitive rational idempotents of cyclic groups.

Rational Idempotents, cont.

If $G =< x : x^{p^b} = 1 >$ is a cyclic p-group then the primitive rational idempotents of G have the form

$$[e_\chi] = \frac{p < x^{p^{j+1}} > - < x^{p^j} >}{p^{b-j}}.$$

If G is cyclic, the primitive rational idempotents of G are products of primitive idempotents from the Sylow subgroups.

So we know all the primitive rational idempotents of cyclic groups.

Rational Idempotents, cont.

If $G =< x : x^{p^b} = 1 >$ is a cyclic p-group then the primitive rational idempotents of G have the form

$$[e_\chi] = \frac{p < x^{p^{j+1}} > - < x^{p^j} >}{p^{b-j}}.$$

If G is cyclic, the primitive rational idempotents of G are products of primitive idempotents from the Sylow subgroups.

So we know all the primitive rational idempotents of cyclic groups.

Rational Idempotents, cont.

(Repeating...) Any element $X \in \mathbb{Z}[G]$ can be written (uniquely) in the form

$$X = \sum_{\chi \in G^*/\sim} \chi(X)[e_\chi]$$

An effective means to constructing a combinatorial object in a cyclic group is to build it up from the rational idempotents, using the possible character values of the object.

This is particularly effective if we also take advantage of various homomorphic images.

Rational Idempotents, cont.

(Repeating...) Any element $X \in \mathbb{Z}[G]$ can be written (uniquely) in the form

$$X = \sum_{\chi \in G^*/\sim} \chi(X)[e_\chi]$$

An effective means to constructing a combinatorial object in a cyclic group is to build it up from the rational idempotents, using the possible character values of the object.

This is particularly effective if we also take advantage of various homomorphic images.

Rational Idempotents, cont.

(Repeating...) Any element $X \in \mathbb{Z}[G]$ can be written (uniquely) in the form

$$X = \sum_{\chi \in G^*/\sim} \chi(X)[e_\chi]$$

An effective means to constructing a combinatorial object in a cyclic group is to build it up from the rational idempotents, using the possible character values of the object.

This is particularly effective if we also take advantage of various homomorphic images.

Cyclic groups, example

Suppose $G = C_{24} \cong C_3 \times C_8 =< y, z : y^3 = z^8 = [y, z] = 1 >$.
There are 4 rational idempotents for $C_8 =< z : z^8 = 1 >$.
They are

$$\frac{< z >}{8}, \frac{2 < z^2 > - < z >}{8} = \frac{(1 - z) < z^2 >}{8},$$

$$\frac{2 < z^4 > - < z^2 >}{4} = \frac{(1 - z^2) < z^4 >}{4},$$

$$\frac{2 < z^8 > - <^4>}{2} = \frac{(1 - z^4)}{2}$$

There are 2 rational idempotents for $C_3 =< y : y^3 = 1 >$.
They are

$$\frac{< y >}{3} \text{ and } \frac{3 < y^3 > - < y >}{3} = \frac{2 - y - y^2}{3}.$$

Cyclic groups, example

Suppose $G = C_{24} \cong C_3 \times C_8 =< y, z : y^3 = z^8 = [y, z] = 1 >$.
There are 4 rational idempotents for $C_8 =< z : z^8 = 1 >$.
They are

$$\frac{< z >}{8}, \frac{2 < z^2 > - < z >}{8} = \frac{(1 - z) < z^2 >}{8},$$

$$\frac{2 < z^4 > - < z^2 >}{4} = \frac{(1 - z^2) < z^4 >}{4},$$

$$\frac{2 < z^8 > - <^4>}{2} = \frac{(1 - z^4)}{2}$$

There are 2 rational idempotents for $C_3 =< y : y^3 = 1 >$.
They are

$$\frac{< y >}{3} \text{ and } \frac{3 < y^3 > - < y >}{3} = \frac{2 - y - y^2}{3}.$$

Cyclic groups, example

Suppose $G = C_{24} \cong C_3 \times C_8 =< y, z : y^3 = z^8 = [y, z] = 1 >$.
There are 4 rational idempotents for $C_8 =< z : z^8 = 1 >$.
They are

$$\frac{< z >}{8}, \frac{2 < z^2 > - < z >}{8} = \frac{(1 - z) < z^2 >}{8},$$

$$\frac{2 < z^4 > - < z^2 >}{4} = \frac{(1 - z^2) < z^4 >}{4},$$

$$\frac{2 < z^8 > - <^4>}{2} = \frac{(1 - z^4)}{2}$$

There are 2 rational idempotents for $C_3 =< y : y^3 = 1 >$.
They are

$$\frac{< y >}{3} \text{ and } \frac{3 < y^3 > - < y >}{3} = \frac{2 - y - y^2}{3}.$$

Cyclic groups, example

In array notation the idempotents of C_8 and C_3 are

$$\frac{1}{8}\begin{pmatrix}1 & 1 & 1 & 1 & 1 & 1 & 1 & 1\end{pmatrix},$$

$$\frac{1}{8}\begin{pmatrix}1 & -1 & 1 & -1 & 1 & -1 & 1 & -1\end{pmatrix},$$

$$\frac{1}{8}\begin{pmatrix}2 & 0 & -2 & 0 & 2 & 0 & -2 & 0\end{pmatrix},$$

$$\frac{1}{8}\begin{pmatrix}4 & 0 & 0 & 0 & -4 & 0 & 0 & 0\end{pmatrix},$$

and

$$\frac{1}{3}\begin{pmatrix}1\\1\\1\end{pmatrix}, \frac{1}{3}\begin{pmatrix}2\\-1\\-1\end{pmatrix}.$$

Cyclic groups, example

In array notation the idempotents of C_8 and C_3 are

$$\frac{1}{8}\begin{pmatrix}1 & 1 & 1 & 1 & 1 & 1 & 1 & 1\end{pmatrix},$$

$$\frac{1}{8}\begin{pmatrix}1 & -1 & 1 & -1 & 1 & -1 & 1 & -1\end{pmatrix},$$

$$\frac{1}{8}\begin{pmatrix}2 & 0 & -2 & 0 & 2 & 0 & -2 & 0\end{pmatrix},$$

$$\frac{1}{8}\begin{pmatrix}4 & 0 & 0 & 0 & -4 & 0 & 0 & 0\end{pmatrix},$$

and

$$\frac{1}{3}\begin{pmatrix}1\\1\\1\end{pmatrix}, \frac{1}{3}\begin{pmatrix}2\\-1\\-1\end{pmatrix}.$$

Cyclic groups, example

In array notation the idempotents of C_8 and C_3 are

$$\frac{1}{8}\begin{pmatrix}1 & 1 & 1 & 1 & 1 & 1 & 1 & 1\end{pmatrix},$$

$$\frac{1}{8}\begin{pmatrix}1 & -1 & 1 & -1 & 1 & -1 & 1 & -1\end{pmatrix},$$

$$\frac{1}{8}\begin{pmatrix}2 & 0 & -2 & 0 & 2 & 0 & -2 & 0\end{pmatrix},$$

$$\frac{1}{8}\begin{pmatrix}4 & 0 & 0 & 0 & -4 & 0 & 0 & 0\end{pmatrix},$$

and

$$\frac{1}{3}\begin{pmatrix}1\\1\\1\end{pmatrix},\ \frac{1}{3}\begin{pmatrix}2\\-1\\-1\end{pmatrix}.$$

Cyclic groups, example

The eight rational idempotents of $C_3 \times C_8$ are just the products of these. (In our array notation, that is just the pointwise (Schur) product of these arrays.)

For example, the idempotent corresponding to any character of order 21 is

$$\frac{1}{8}\begin{pmatrix}4 & 0 & 0 & 0 & -4 & 0 & 0 & 0\end{pmatrix} \circ \frac{1}{3}\begin{pmatrix}2\\-1\\-1\end{pmatrix} =$$

$$\frac{1}{24}\begin{pmatrix}8 & 0 & 0 & 0 & -8 & 0 & 0 & 0\\ -4 & 0 & 0 & 0 & 4 & 0 & 0 & 0\\ -4 & 0 & 0 & 0 & 4 & 0 & 0 & 0\end{pmatrix}$$

Cyclic groups, example

The eight rational idempotents of $C_3 \times C_8$ are just the products of these. (In our array notation, that is just the pointwise (Schur) product of these arrays.)

For example, the idempotent corresponding to any character of order 21 is

$$\frac{1}{8}\begin{pmatrix}4 & 0 & 0 & 0 & -4 & 0 & 0 & 0\end{pmatrix} \circ \frac{1}{3}\begin{pmatrix}2\\-1\\-1\end{pmatrix} =$$

$$\frac{1}{24}\begin{pmatrix}8 & 0 & 0 & 0 & -8 & 0 & 0 & 0\\ -4 & 0 & 0 & 0 & 4 & 0 & 0 & 0\\ -4 & 0 & 0 & 0 & 4 & 0 & 0 & 0\end{pmatrix}$$

Some notation

If

$$G = C_s \times C_t = < x : x^s = 1 > \times < y : y^t = 1 >,$$

write $\chi_{i,j}$ for the character which maps x to ζ_s^i and y to ζ_t^j.

If $G = \{x^i y^j\}$ then $G^* = \{\chi_{i,j}\}$

Extend this notation to $e_{i,j}$ and $[e_{i,j}]$.

The unique $CW(24, 9)$

$G := C_3 \times C_8 =< y, z : y^3 = z^8 = [y, z] = 1 >$
We seek $S \in \mathbb{Z}[G]$ such that $SS^{(-1)} = 9$ and $\forall g \in G,\ s_g \in \{-1, 0, 1\}$.

$$S = \alpha_{0,0}e_{0,0} + \alpha_{0,4}e_{0,4} + \alpha_{0,2}[e_{0,2}] + \alpha_{0,1}[e_{0,1}]$$
$$+\alpha_{1,0}[e_{1,0}] + \alpha_{1,4}[e_{1,4}] + \alpha_{1,2}[e_{1,2}] + \alpha_{1,1}[e_{1,1}].$$

The C_4 image is $\alpha_{0,0}e_{0,0} + \alpha_{0,4}e_{0,4} + \alpha_{0,2}[e_{0,2}]$

$$= \frac{\alpha_{0,0}}{4}\begin{pmatrix}1 & 1 & 1 & 1\end{pmatrix}$$

$$+\frac{\alpha_{0,4}}{4}\begin{pmatrix}1 & -1 & 1 & -1\end{pmatrix}$$

$$+\frac{\alpha_{0,2}}{4}\begin{pmatrix}2 & 0 & -2 & 0\end{pmatrix}$$

where the $\alpha_{i,j}$ are aliases for $\chi(S)\overline{\chi S} = 9$ in the appropriate number theoretic ring.

The unique $CW(24, 9)$

$G := C_3 \times C_8 =< y, z : y^3 = z^8 = [y, z] = 1 >$
We seek $S \in \mathbb{Z}[G]$ such that $SS^{(-1)} = 9$ and $\forall g \in G,\ s_g \in \{-1, 0, 1\}$.

$$S = \alpha_{0,0} e_{0,0} + \alpha_{0,4} e_{0,4} + \alpha_{0,2}[e_{0,2}] + \alpha_{0,1}[e_{0,1}]$$
$$+\alpha_{1,0}[e_{1,0}] + \alpha_{1,4}[e_{1,4}] + \alpha_{1,2}[e_{1,2}] + \alpha_{1,1}[e_{1,1}].$$

The C_4 image is $\alpha_{0,0} e_{0,0} + \alpha_{0,4} e_{0,4} + \alpha_{0,2}[e_{0,2}]$

$$= \frac{\alpha_{0,0}}{4} \begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix}$$

$$+ \frac{\alpha_{0,4}}{4} \begin{pmatrix} 1 & -1 & 1 & -1 \end{pmatrix}$$

$$+ \frac{\alpha_{0,2}}{4} \begin{pmatrix} 2 & 0 & -2 & 0 \end{pmatrix}$$

where the $\alpha_{i,j}$ are aliases for $\chi(S)\overline{\chi S} = 9$ in the appropriate number theoretic ring.

The unique $CW(24, 9)$

The C_4 image of S is

$$S/ < y, z^4 >= (\frac{3}{4}) \begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix}$$

$$+(\frac{3}{4}) \begin{pmatrix} 1 & -1 & 1 & -1 \end{pmatrix}$$

$$+(\frac{3x^i}{4}) \begin{pmatrix} 2 & 0 & -2 & 0 \end{pmatrix}$$

$$= \frac{1}{4} \begin{pmatrix} 6 & 6 & 6 & -6 \end{pmatrix} \text{ or } \frac{1}{4} \begin{pmatrix} 12 & 0 & 0 & 0 \end{pmatrix}.$$

The unique $CW(24, 9)$

The C_4 image of S is

$$S/ < y, z^4 >= (\frac{3}{4}) \begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix}$$

$$+(\frac{3}{4}) \begin{pmatrix} 1 & -1 & 1 & -1 \end{pmatrix}$$

$$+(\frac{3x^i}{4}) \begin{pmatrix} 2 & 0 & -2 & 0 \end{pmatrix}$$

$$= \frac{1}{4} \begin{pmatrix} 6 & 6 & 6 & -6 \end{pmatrix} \text{ or } \frac{1}{4} \begin{pmatrix} 12 & 0 & 0 & 0 \end{pmatrix}.$$

The C_3 and C_6 images of $CW(24, 9)$

The C_3 image is $3e_{0,0} \pm 3[e_{1,0}] = \begin{pmatrix}1\\1\\1\end{pmatrix} \pm \begin{pmatrix}2\\-1\\-1\end{pmatrix}$

giving

$$\begin{pmatrix}3\\0\\0\end{pmatrix} \text{ or } \begin{pmatrix}-1\\2\\2\end{pmatrix}$$

When we move on to C_6, we get four solutions

$$3e_{0,0} \pm 3[e_{1,0}] + 3e_{0,4} \pm 3[e_{1,4}] =$$

$$\begin{pmatrix}3&0\\0&0\\0&0\end{pmatrix}, \begin{pmatrix}1&2\\1&-1\\1&-1\end{pmatrix}, \begin{pmatrix}1&-2\\1&1\\1&1\end{pmatrix} \text{ or } \begin{pmatrix}-1&0\\2&0\\2&0\end{pmatrix},$$

The C_3 and C_6 images of $CW(24, 9)$

The C_3 image is $3e_{0,0} \pm 3[e_{1,0}] = \begin{pmatrix}1\\1\\1\end{pmatrix} \pm \begin{pmatrix}2\\-1\\-1\end{pmatrix}$

giving

$$\begin{pmatrix}3\\0\\0\end{pmatrix} \text{ or } \begin{pmatrix}-1\\2\\2\end{pmatrix}$$

When we move on to C_6, we get four solutions

$$3e_{0,0} \pm 3[e_{1,0}] + 3e_{0,4} \pm 3[e_{1,4}] =$$

$$\begin{pmatrix}3&0\\0&0\\0&0\end{pmatrix}, \begin{pmatrix}1&2\\1&-1\\1&-1\end{pmatrix}, \begin{pmatrix}1&-2\\1&1\\1&1\end{pmatrix} \text{ or } \begin{pmatrix}-1&0\\2&0\\2&0\end{pmatrix},$$

The C_{12} images of $CW(24, 9)$

We take previous C_{12} solution, multiply it by $\frac{1+z^2}{2}$ and *add* to that

$$3y^{i_1}[e_{0,2}] \pm 3y^{i_2}[e_{1,2}]$$

$$= \frac{1}{2}y^{i_1}\begin{pmatrix} 1 & 0 & -1 & 0 \\ 1 & 0 & -1 & 0 \\ 1 & 0 & -1 & 0 \end{pmatrix}$$

$$\pm\frac{1}{2}y^{i_2}\begin{pmatrix} 2 & 0 & -2 & 0 \\ -1 & 0 & 1 & 0 \\ -1 & 0 & 1 & 0 \end{pmatrix}$$

The C_{12} images of $CW(24, 9)$, II

This allows only four $C_{12} = C_3 \times C_4$ solutions. (The first is then prohibited by the coset bound.)

$$\begin{pmatrix} 3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & -2 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}$$

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

The final idempotents

To get the final object in C_{24}, we take the C_{12} image (one of three above), multiply it by $\frac{1+z^4}{2}$ and add alias-idempotent combinations

$$\alpha_{0,1}[e_{0,1}] + \alpha_{0,1}[e_{1,1}].$$

The character of order 8 allows us to work in $\mathbb{Z}[\zeta_8]$ ($\zeta_8 := e^{\pi i/4}$) where we may write $9 = (1+2\sqrt{2}i)(-1-2\sqrt{2}i) = (1+2\zeta_8+2\zeta_8^3)(1-2\zeta_8-2\zeta_8^3)$. Thus $\alpha_{0,1}$ might be ± 3 or might be something more interesting like $\pm(1+2z+2z^3)$!
The order-24 alias can even more interesting since there we allow a Gauss sum. In this case,

$$\chi_{1,1}(\alpha_{1,1}) = (\omega-\omega^2)(1+\sqrt{2}i) = (\omega-\omega^2)(1+\zeta_8+\zeta_8^3)$$

(where ω is a primitive cube root of unity.)

The final idempotents

To get the final object in C_{24}, we take the C_{12} image (one of three above), multiply it by $\frac{1+z^4}{2}$ and add alias-idempotent combinations

$$\alpha_{0,1}[e_{0,1}] + \alpha_{0,1}[e_{1,1}].$$

The character of order 8 allows us to work in $\mathbb{Z}[\zeta_8]$ ($\zeta_8 := e^{\pi i/4}$) where we may write $9 = (1+2\sqrt{2}i)(-1-2\sqrt{2}i) = (1+2\zeta_8+2\zeta_8^3)(1-2\zeta_8-2\zeta_8^3)$.
Thus $\alpha_{0,1}$ might be ± 3 or might be something more interesting like $\pm(1+2z+2z^3)$!
The order-24 alias can even more interesting since there we allow a Gauss sum. In this case,

$$\chi_{1,1}(\alpha_{1,1}) = (\omega-\omega^2)(1+\sqrt{2}i) = (\omega-\omega^2)(1+\zeta_8+\zeta_8^3)$$

(where ω is a primitive cube root of unity.)

The final idempotents

To get the final object in C_{24}, we take the C_{12} image (one of three above), multiply it by $\frac{1+z^4}{2}$ and add alias-idempotent combinations

$$\alpha_{0,1}[e_{0,1}] + \alpha_{0,1}[e_{1,1}].$$

The character of order 8 allows us to work in $\mathbb{Z}[\zeta_8]$ ($\zeta_8 := e^{\pi i/4}$) where we may write $9 = (1+2\sqrt{2}i)(-1-2\sqrt{2}i) = (1+2\zeta_8+2\zeta_8^3)(1-2\zeta_8-2\zeta_8^3)$. Thus $\alpha_{0,1}$ might be ± 3 or might be something more interesting like $\pm(1+2z+2z^3)$!

The order-24 alias can even more interesting since there we allow a Gauss sum. In this case,

$$\chi_{1,1}(\alpha_{1,1}) = (\omega-\omega^2)(1+\sqrt{2}i) = (\omega-\omega^2)(1+\zeta_8+\zeta_8^3)$$

(where ω is a primitive cube root of unity.)

The final idempotents

To get the final object in C_{24}, we take the C_{12} image (one of three above), multiply it by $\frac{1+z^4}{2}$ and add alias-idempotent combinations

$$\alpha_{0,1}[e_{0,1}] + \alpha_{0,1}[e_{1,1}].$$

The character of order 8 allows us to work in $\mathbb{Z}[\zeta_8]$ ($\zeta_8 := e^{\pi i/4}$) where we may write $9 = (1+2\sqrt{2}i)(-1-2\sqrt{2}i) = (1+2\zeta_8+2\zeta_8^3)(1-2\zeta_8-2\zeta_8^3)$. Thus $\alpha_{0,1}$ might be ± 3 or might be something more interesting like $\pm(1+2z+2z^3)$!
The order-24 alias can even more interesting since there we allow a Gauss sum. In this case,

$$\chi_{1,1}(\alpha_{1,1}) = (\omega-\omega^2)(1+\sqrt{2}i) = (\omega-\omega^2)(1+\zeta_8+\zeta_8^3)$$

(where ω is a primitive cube root of unity.)

The choices

$$A_1 = \frac{1}{2}\begin{pmatrix} 1 & 0 & -2 & 0 & 1 & 0 & -2 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}$$

$$A_2 = \frac{1}{2}\begin{pmatrix} 1 & 0 & 2 & 0 & 1 & 0 & 2 & 0 \\ 1 & 0 & -1 & 0 & 1 & 0 & -1 & 0 \\ 1 & 0 & -1 & 0 & 1 & 0 & -1 & 0 \end{pmatrix}$$

$$A_3 = \frac{1}{2}\begin{pmatrix} -1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 2 & 0 & 0 & 0 & 2 & 0 & 0 & 0 \\ 2 & 0 & 0 & 0 & 2 & 0 & 0 & 0 \end{pmatrix}$$

$$B_1 = \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \end{pmatrix}$$

$$B_2 = \frac{1}{6}\begin{pmatrix} 1 & 2 & 0 & 2 & -1 & -2 & 0 & -2 \\ 1 & 2 & 0 & 2 & -1 & -2 & 0 & -2 \\ 1 & 2 & 0 & 2 & -1 & -2 & 0 & -2 \end{pmatrix}$$

$$B_3 = \frac{1}{6}\begin{pmatrix} 1 & -2 & 0 & -2 & -1 & 2 & 0 & 2 \\ 1 & -2 & 0 & -2 & -1 & 2 & 0 & 2 \\ 1 & -2 & 0 & -2 & -1 & 2 & 0 & 2 \end{pmatrix}$$

$$C_1 = \frac{1}{2}\begin{pmatrix} 2 & 0 & 0 & 0 & -2 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

$$C_2 = \frac{1}{6}\begin{pmatrix} 2 & 4 & 0 & 4 & -2 & -4 & 0 & -4 \\ -1 & -2 & 0 & -2 & 1 & 2 & 0 & 2 \\ -1 & -2 & 0 & -2 & 1 & 2 & 0 & 2 \end{pmatrix}$$

$$C_3 = \frac{1}{6}\begin{pmatrix} 2 & -4 & 0 & -4 & -2 & 4 & 0 & 4 \\ -1 & 2 & 0 & 2 & 1 & -2 & 0 & -2 \\ -1 & 2 & 0 & 2 & 1 & -2 & 0 & -2 \end{pmatrix}$$

$$C_4 = \frac{1}{2}\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & -1 & -1 & 0 & -1 \\ -1 & -1 & 0 & -1 & 1 & 1 & 0 & 1 \end{pmatrix}$$

$$C_5 = \frac{1}{2}\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & -1 & 0 & -1 & -1 & 1 & 0 & 1 \\ -1 & 1 & 0 & 1 & 1 & -1 & 0 & -1 \end{pmatrix}$$

The choices

$$\text{So } A_3 + B_2 + C_2 = \begin{pmatrix} 0 & 1 & 0 & 1 & -1 & -1 & 0 & -1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

$$\text{Similarly } A_3 + B_3 + C_3 = \begin{pmatrix} 0 & -1 & 0 & -1 & -1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

But these are equivalent under the automorphism $g \mapsto g^{-1}$.

The choices

$$\text{So } A_3 + B_2 + C_2 = \begin{pmatrix} 0 & 1 & 0 & 1 & -1 & -1 & 0 & -1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

$$\text{Similarly } A_3 + B_3 + C_3 = \begin{pmatrix} 0 & -1 & 0 & -1 & -1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

But these are equivalent under the automorphism $g \mapsto g^{-1}$.

The choices

So $A_3 + B_2 + C_2 = \begin{pmatrix} 0 & 1 & 0 & 1 & -1 & -1 & 0 & -1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$

Similarly $A_3 + B_3 + C_3 = \begin{pmatrix} 0 & -1 & 0 & -1 & -1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$

But these are equivalent under the automorphism $g \mapsto g^{-1}$.

The unique $CW(24, 9)$

$$S = -1 + (y + y^2)(1 + z^4) + (z + z^3)(1 - z^4)$$

$$= \begin{pmatrix} -1 & 1 & 0 & 1 & 0 & -1 & -1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}.$$

is a $CW(24, 9)$ and it is unique up to a common notion of equivalence.

This object was first found by Vincent in 1989 by computer search.
It was later re-discovered by Arasu, Ma and Strassler in 1998.

The unique $CW(24, 9)$

$$S = -1 + (y + y^2)(1 + z^4) + (z + z^3)(1 - z^4)$$

$$= \begin{pmatrix} -1 & 1 & 0 & 1 & 0 & -1 & -1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}.$$

is a $CW(24, 9)$ and it is unique up to a common notion of equivalence.

This object was first found by Vincent in 1989 by computer search.
It was later re-discovered by Arasu, Ma and Strassler in 1998.

The unique $CW(24,9)$

Write $G := C_3 \times C_8 =< y, z : y^3 = z^8 = [y,z] = 1 >$

1. $A =< y > -(3- < y >) = 2 < y > -3 = \begin{pmatrix} -1 \\ 2 \\ 2 \end{pmatrix}$ has character values of length 3 for *all* characters of G.
2. $B = -1 + (z + z^3) = \begin{pmatrix} -1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}$ has character values of length 3 for *most* characters of G
   Therefore,
3. $(\frac{1+z^4}{2})A + (\frac{1-z^4}{2})B = -1 + (y + y^2)(1 + z^4) + (z + z^3)(1 - z^4)$

$$= \begin{pmatrix} -1 & 1 & 0 & 1 & 0 & -1 & -1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}.$$

gives a $CW(24,9)$.

The problem

A CW(24,9) is used by Vincent to construct a CW(96,36).

Is there a CW(48,36)?

This question has been open since at least 1989.

A student of Arasu's (Alex Gutman) lists it as still open in his masters thesis in 2007.

The problem

A CW(24,9) is used by Vincent to construct a CW(96,36).

Is there a CW(48,36)?

This question has been open since at least 1989.

A student of Arasu's (Alex Gutman) lists it as still open in his masters thesis in 2007.

The problem

A CW(24,9) is used by Vincent to construct a CW(96,36).

Is there a CW(48,36)?

This question has been open since at least 1989.

A student of Arasu's (Alex Gutman) lists it as still open in his masters thesis in 2007.

The problem

A CW(24,9) is used by Vincent to construct a CW(96,36).

Is there a CW(48,36)?

This question has been open since at least 1989.

A student of Arasu's (Alex Gutman) lists it as still open in his masters thesis in 2007.

A CW(48,36)

Suppose D is a $CW(48,36)$ in $G =< y, z : y^3 = z^{16} = [y,z] = 1 >$.
Write

$$D = A(\frac{1+z^8}{2}) + B(\frac{1-z^8}{2})$$

where A is a $CW(24,9)$ in $G/ < z^8 > \cong C_{24}$.

(We can show that the entries in B must be even. Since B is even, so is A. Therefore $\frac{1}{2}A$ has the coefficients and character values to be a $CW(24,9)$ in $G/ < z^8 >$.)

A CW(48,36)

Suppose D is a $CW(48,36)$ in $G =< y, z : y^3 = z^{16} = [y,z] = 1 >$. Write

$$D = A(\frac{1+z^8}{2}) + B(\frac{1-z^8}{2})$$

where A is a $CW(24,9)$ in $G/ < z^8 > \cong C_{24}$.

(We can show that the entries in B must be even. Since B is even, so is A. Therefore $\frac{1}{2}A$ has the coefficients and character values to be a $CW(24,9)$ in $G/ < z^8 >$.)

A CW(48,36)

Suppose D is a $CW(48,36)$ in $G =< y, z : y^3 = z^{16} = [y,z] = 1 >$. Write

$$D = A(\frac{1+z^8}{2}) + B(\frac{1-z^8}{2})$$

where A is a $CW(24,9)$ in $G/ < z^8 > \cong C_{24}$.

(We can show that the entries in B must be even. Since B is even, so is A. Therefore $\frac{1}{2}A$ has the coefficients and character values to be a $CW(24,9)$ in $G/ < z^8 >$.)

A CW(48,36)

$$A(\frac{1+z^8}{2}) = \left[-1+(y+y^2)(1+z^4)+(z+z^3)(1-z^4)\right](1+z^8).$$

$$= \left(\begin{array}{cccccccc|c} -1 & 1 & 0 & 1 & 0 & -1 & -1 & 0 & \dots \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & \dots \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & \dots \end{array}\right).$$

satisfies the character requirements for all characters which are principle on $< z^8 >$

A CW(48,36)

$$(1+y+y^2)(1-z^8) = \left(\begin{array}{cccccccc|c} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots \end{array}\right)$$

satisfies the character requirements for characters principle on $< y >$ but not principle on $< z^8 >$.

$$(y-y^2)(1+z^2+z^6)(1-z^8) = \left(\begin{array}{cccccccc|c} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & \dots \\ -1 & 0 & -1 & 0 & 0 & 0 & -1 & 0 & \dots \end{array}\right)$$

satisfies the character requirements for characters of order 48.

A CW(48,36)

$$(1+y+y^2)(1-z^8) = \left(\begin{array}{cccccccc|c} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots \end{array}\right)$$

satisfies the character requirements for characters principle on $< y >$ but not principle on $< z^8 >$.

$$(y-y^2)(1+z^2+z^6)(1-z^8) = \left(\begin{array}{cccccccc|c} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & \dots \\ -1 & 0 & -1 & 0 & 0 & 0 & -1 & 0 & \dots \end{array}\right)$$

satisfies the character requirements for characters of order 48.

A CW(48,36)

$$\left(\begin{array}{cccccccc|c} -1 & 1 & 0 & 1 & 0 & -1 & -1 & 0 & \dots \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & \dots \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & \dots \end{array}\right).$$

$$\left(\begin{array}{cccccccc|c} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots \end{array}\right)$$

$$\left(\begin{array}{cccccccc|c} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & \dots \\ -1 & 0 & -1 & 0 & 0 & 0 & -1 & 0 & \dots \end{array}\right)$$

Shifting does not change the modulus of images under characters, so we may shift these three elements to form a set satisfying all the character requirements.

Three pieces to the jigsaw puzzle

$$\left(\begin{array}{cccccccc|c} - & + & 0 & + & 0 & - & - & 0 & \dots \\ + & 0 & 0 & 0 & + & 0 & 0 & 0 & \dots \\ + & 0 & 0 & 0 & + & 0 & 0 & 0 & \dots \end{array}\right).$$

$$+g_1 \left(\begin{array}{cccccccc|c} + & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots \\ + & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots \\ + & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots \end{array}\right)$$

$$+g_2 \left(\begin{array}{cccccccc|c} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots \\ + & 0 & + & 0 & 0 & 0 & + & 0 & \dots \\ - & 0 & - & 0 & 0 & 0 & - & 0 & \dots \end{array}\right)$$

$$= \left(\begin{array}{cccccccc|c} - & + & + & + & 0 & - & - & 0 & \dots \\ + & + & + & + & + & 0 & + & 0 & \dots \\ + & - & + & - & + & 0 & - & 0 & \dots \end{array}\right).$$

!!

Three pieces to the jigsaw puzzle

$$\left(\begin{array}{cccccccc|c} - & + & 0 & + & 0 & - & - & 0 & \dots \\ + & 0 & 0 & 0 & + & 0 & 0 & 0 & \dots \\ + & 0 & 0 & 0 & + & 0 & 0 & 0 & \dots \end{array}\right).$$

$$+g_1 \left(\begin{array}{cccccccc|c} + & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots \\ + & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots \\ + & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots \end{array}\right)$$

$$+g_2 \left(\begin{array}{cccccccc|c} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots \\ + & 0 & + & 0 & 0 & 0 & + & 0 & \dots \\ - & 0 & - & 0 & 0 & 0 & - & 0 & \dots \end{array}\right)$$

$$= \left(\begin{array}{cccccccc|c} - & + & + & + & 0 & - & - & 0 & \dots \\ + & + & + & + & + & 0 & + & 0 & \dots \\ + & - & + & - & + & 0 & - & 0 & \dots \end{array}\right).$$

!!

Three pieces to the jigsaw puzzle

$$\left(\begin{array}{cccccccc|c} - & + & 0 & + & 0 & - & - & 0 & \dots \\ + & 0 & 0 & 0 & + & 0 & 0 & 0 & \dots \\ + & 0 & 0 & 0 & + & 0 & 0 & 0 & \dots \end{array}\right).$$

$$+g_1 \left(\begin{array}{cccccccc|c} + & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots \\ + & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots \\ + & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots \end{array}\right)$$

$$+g_2 \left(\begin{array}{cccccccc|c} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots \\ + & 0 & + & 0 & 0 & 0 & + & 0 & \dots \\ - & 0 & - & 0 & 0 & 0 & - & 0 & \dots \end{array}\right)$$

$$= \left(\begin{array}{cccccccc|c} - & + & + & + & 0 & - & - & 0 & \dots \\ + & + & + & + & + & 0 & + & 0 & \dots \\ + & - & + & - & + & 0 & - & 0 & \dots \end{array}\right).$$

!!

Three pieces to the jigsaw puzzle

$$\begin{pmatrix} - & + & 0 & + & 0 & - & - & 0 & | & \dots \\ + & 0 & 0 & 0 & + & 0 & 0 & 0 & | & \dots \\ + & 0 & 0 & 0 & + & 0 & 0 & 0 & | & \dots \end{pmatrix}.$$

$$+g_1 \begin{pmatrix} + & 0 & 0 & 0 & 0 & 0 & 0 & 0 & | & \dots \\ + & 0 & 0 & 0 & 0 & 0 & 0 & 0 & | & \dots \\ + & 0 & 0 & 0 & 0 & 0 & 0 & 0 & | & \dots \end{pmatrix}$$

$$+g_2 \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & | & \dots \\ + & 0 & + & 0 & 0 & 0 & + & 0 & | & \dots \\ - & 0 & - & 0 & 0 & 0 & - & 0 & | & \dots \end{pmatrix}$$

$$= \begin{pmatrix} - & + & + & + & 0 & - & - & 0 & | & \dots \\ + & + & + & + & + & 0 & + & 0 & | & \dots \\ + & - & + & - & + & 0 & - & 0 & | & \dots \end{pmatrix}.$$

!!

One last example

Davis: Is there a $(64, 18, 2, 6)$ PDS in $C_8 \times C_8$?

Exercise. The image of D in $G/ < x^2, y^2 >$ is

$$18[e_{0,0}]+2([e_{0,4}]+[e_{4,0}]+[e_{4,4}]) = \begin{pmatrix} 6 & 4 \\ 4 & 4 \end{pmatrix} = (6+4x+4y+4xy) < x^2, y^2 >$$

This leaves

$$\begin{pmatrix} 2 & 2 & 4 & 2 \\ 0 & 2 & 4 & 2 \end{pmatrix}, \ \{\chi_{0,2}, \chi_{0,6}\} \subset S^*$$

(I can use a multiplier theorem and a natural duality to *eliminate* all choices in my search at this level.)

One last example

Davis: Is there a $(64, 18, 2, 6)$ PDS in $C_8 \times C_8$?

Exercise. The image of D in $G/ < x^2, y^2 >$ is

$$18[e_{0,0}]+2([e_{0,4}]+[e_{4,0}]+[e_{4,4}]) = \begin{pmatrix} 6 & 4 \\ 4 & 4 \end{pmatrix} = (6+4x+4y+4xy) < x^2, y^2 >$$

This leaves

$$\begin{pmatrix} 2 & 2 & 4 & 2 \\ 0 & 2 & 4 & 2 \end{pmatrix}, \ \{\chi_{0,2}, \chi_{0,6}\} \subset S^*$$

(I can use a multiplier theorem and a natural duality to *eliminate* all choices in my search at this level.)

One last example

Davis: Is there a $(64, 18, 2, 6)$ PDS in $C_8 \times C_8$?

Exercise. The image of D in $G/ < x^2, y^2 >$ is

$$18[e_{0,0}]+2([e_{0,4}]+[e_{4,0}]+[e_{4,4}]) = \begin{pmatrix} 6 & 4 \\ 4 & 4 \end{pmatrix} = (6+4x+4y+4xy) < x^2, y^2 >$$

This leaves

$$\begin{pmatrix} 2 & 2 & 4 & 2 \\ 0 & 2 & 4 & 2 \end{pmatrix}, \ \{\chi_{0,2}, \chi_{0,6}\} \subset S^*$$

(I can use a multiplier theorem and a natural duality to *eliminate* all choices in my search at this level.)

One last example

Davis: Is there a $(64, 18, 2, 6)$ PDS in $C_8 \times C_8$?

Exercise. The image of D in $G/ < x^2, y^2 >$ is

$$18[e_{0,0}]+2([e_{0,4}]+[e_{4,0}]+[e_{4,4}]) = \begin{pmatrix} 6 & 4 \\ 4 & 4 \end{pmatrix} = (6+4x+4y+4xy) < x^2, y^2 >$$

This leaves

$$\begin{pmatrix} 2 & 2 & 4 & 2 \\ 0 & 2 & 4 & 2 \end{pmatrix}, \ \{\chi_{0,2}, \chi_{0,6}\} \subset S^*$$

(I can use a multiplier theorem and a natural duality to *eliminate* all choices in my search at this level.)

All $C_4 \times C_4$ solutions are equivalent to the following:

$$\begin{pmatrix} 0 & 0 & 2 & 0 \\ 0 & 0 & 2 & 2 \\ 2 & 2 & 2 & 2 \\ 0 & 2 & 2 & 0 \end{pmatrix}$$

All $C_4 \times C_8$ solutions are equivalent to the following:

$$= \left(\begin{array}{cccc|cccc} 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 2 & 1 & 0 & 0 & 0 & 1 \\ 2 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 2 & 0 \end{array}\right)$$

We can easily finish this off to find 4 solutions. (These are nonequivalent but give the same strongly regular graph.)

All $C_4 \times C_4$ solutions are equivalent to the following:

$$\begin{pmatrix} 0 & 0 & 2 & 0 \\ 0 & 0 & 2 & 2 \\ 2 & 2 & 2 & 2 \\ 0 & 2 & 2 & 0 \end{pmatrix}$$

All $C_4 \times C_8$ solutions are equivalent to the following:

$$= \left(\begin{array}{cccc|cccc} 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 2 & 1 & 0 & 0 & 0 & 1 \\ 2 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 2 & 0 \end{array}\right)$$

We can easily finish this off to find 4 solutions. (These are nonequivalent but give the same strongly regular graph.)

All $C_4 \times C_4$ solutions are equivalent to the following:

$$\begin{pmatrix} 0 & 0 & 2 & 0 \\ 0 & 0 & 2 & 2 \\ 2 & 2 & 2 & 2 \\ 0 & 2 & 2 & 0 \end{pmatrix}$$

All $C_4 \times C_8$ solutions are equivalent to the following:

$$= \left(\begin{array}{cccc|cccc} 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 2 & 1 & 0 & 0 & 0 & 1 \\ 2 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 2 & 0 \end{array}\right)$$

We can easily finish this off to find 4 solutions. (These are nonequivalent but give the same strongly regular graph.)

Comments

This rational idempotent construction is essentially an algorithm for creating combinatorial objects with prescribed eigenvalues and a sharply transitive automorphism group.

1. When does this work best? (There are three main ingredients.)
   - 1.1 When the exponent of the group is relatively high, the rational idempotents collect *lots* of primitive idempotents.
   - 1.2 When the character values (eigenvalues) are tightly constrained, we have a limited number of choices for the aliases.
   - 1.3 We would like a nice sieve of homomorphic images of our group.
2. What if the group is nonabelian?
   There is an analogous theory for nonabelian groups, but the "idempotent decomposition" is not nearly as clean.
   And then there may be some "noncommutative number theory"!
   And the sieve of images may be more complicated too!

Comments

This rational idempotent construction is essentially an algorithm for creating combinatorial objects with prescribed eigenvalues and a sharply transitive automorphism group.

1. When does this work best? (There are three main ingredients.)
   - 1.1 When the exponent of the group is relatively high, the rational idempotents collect *lots* of primitive idempotents.
   - 1.2 When the character values (eigenvalues) are tightly constrained, we have a limited number of choices for the aliases.
   - 1.3 We would like a nice sieve of homomorphic images of our group.
2. What if the group is nonabelian?
   There is an analogous theory for nonabelian groups, but the "idempotent decomposition" is not nearly as clean.
   And then there may be some "noncommutative number theory"!
   And the sieve of images may be more complicated too!

Comments

This rational idempotent construction is essentially an algorithm for creating combinatorial objects with prescribed eigenvalues and a sharply transitive automorphism group.

1. When does this work best? (There are three main ingredients.)
   - 1.1 When the exponent of the group is relatively high, the rational idempotents collect *lots* of primitive idempotents.
   - 1.2 When the character values (eigenvalues) are tightly constrained, we have a limited number of choices for the aliases.
   - 1.3 We would like a nice sieve of homomorphic images of our group.
2. What if the group is nonabelian?
   There is an analogous theory for nonabelian groups, but the "idempotent decomposition" is not nearly as clean.
   And then there may be some "noncommutative number theory"!
   And the sieve of images may be more complicated too!

Comments

This rational idempotent construction is essentially an algorithm for creating combinatorial objects with prescribed eigenvalues and a sharply transitive automorphism group.

1. When does this work best? (There are three main ingredients.)
   - 1.1 When the exponent of the group is relatively high, the rational idempotents collect *lots* of primitive idempotents.
   - 1.2 When the character values (eigenvalues) are tightly constrained, we have a limited number of choices for the aliases.
   - 1.3 We would like a nice sieve of homomorphic images of our group.
2. What if the group is nonabelian?
   There is an analogous theory for nonabelian groups, but the "idempotent decomposition" is not nearly as clean.
   And then there may be some "noncommutative number theory"!
   And the sieve of images may be more complicated too!

Comments

This rational idempotent construction is essentially an algorithm for creating combinatorial objects with prescribed eigenvalues and a sharply transitive automorphism group.

1. When does this work best? (There are three main ingredients.)
   - 1.1 When the exponent of the group is relatively high, the rational idempotents collect *lots* of primitive idempotents.
   - 1.2 When the character values (eigenvalues) are tightly constrained, we have a limited number of choices for the aliases.
   - 1.3 We would like a nice sieve of homomorphic images of our group.
2. What if the group is nonabelian?
   There is an analogous theory for nonabelian groups, but the "idempotent decomposition" is not nearly as clean.
   And then there may be some "noncommutative number theory"!
   And the sieve of images may be more complicated too!

Comments

This rational idempotent construction is essentially an algorithm for creating combinatorial objects with prescribed eigenvalues and a sharply transitive automorphism group.

1. When does this work best? (There are three main ingredients.)
   - 1.1 When the exponent of the group is relatively high, the rational idempotents collect *lots* of primitive idempotents.
   - 1.2 When the character values (eigenvalues) are tightly constrained, we have a limited number of choices for the aliases.
   - 1.3 We would like a nice sieve of homomorphic images of our group.
2. What if the group is nonabelian?
   There is an analogous theory for nonabelian groups, but the "idempotent decomposition" is not nearly as clean.
   And then there may be some "noncommutative number theory"!
   And the sieve of images may be more complicated too!

Comments

This rational idempotent construction is essentially an algorithm for creating combinatorial objects with prescribed eigenvalues and a sharply transitive automorphism group.

1. When does this work best? (There are three main ingredients.)
   - 1.1 When the exponent of the group is relatively high, the rational idempotents collect *lots* of primitive idempotents.
   - 1.2 When the character values (eigenvalues) are tightly constrained, we have a limited number of choices for the aliases.
   - 1.3 We would like a nice sieve of homomorphic images of our group.
2. What if the group is nonabelian?

   There is an analogous theory for nonabelian groups, but the "idempotent decomposition" is not nearly as clean.
   And then there may be some "noncommutative number theory"!
   And the sieve of images may be more complicated too!

Comments

This rational idempotent construction is essentially an algorithm for creating combinatorial objects with prescribed eigenvalues and a sharply transitive automorphism group.

1. When does this work best? (There are three main ingredients.)
   - 1.1 When the exponent of the group is relatively high, the rational idempotents collect *lots* of primitive idempotents.
   - 1.2 When the character values (eigenvalues) are tightly constrained, we have a limited number of choices for the aliases.
   - 1.3 We would like a nice sieve of homomorphic images of our group.
2. What if the group is nonabelian?
   There is an analogous theory for nonabelian groups, but the "idempotent decomposition" is not nearly as clean.
   And then there may be some "noncommutative number theory"!
   And the sieve of images may be more complicated too!

Parts of this work involve collaborations with Jim Davis, John Polhill, Jessica Stuckey and Bernhard Schmidt,

More extensive notes will be available on my professional webpage at web.me.com/kenwsmith/Professional (link here)

THANKS!

Parts of this work involve collaborations with Jim Davis, John Polhill, Jessica Stuckey and Bernhard Schmidt,

More extensive notes will be available on my professional webpage at web.me.com/kenwsmith/Professional (link here)

THANKS!

Parts of this work involve collaborations with Jim Davis, John Polhill, Jessica Stuckey and Bernhard Schmidt,

More extensive notes will be available on my professional webpage at web.me.com/kenwsmith/Professional (link here)

THANKS!