Formalisation et validation d'une méthode de construction de systèmes de blocs

Jessy Colonval et Henri de Boutray

Institut FEMTO-ST, Université Bourgogne Franche-Comté, Besançon, France

13/06/2019

Introduction

- Master recherche et doctorant encadrés par A. Giorgetti
- Cadre : étude de géométries finies dites *quantiques* [PGHS15]
- Constat : nombreux de programmes pour la recherche en mathématiques expérimentales pas suffisamment accessibles, structurés et documentés [SBB+12]
- Langage Magma (Magma Computational Algebra System)
- Bonnes pratiques : test intensif, structuration, factorisation, documentation et distribution libre du code
- Application à une méthode de construction de systèmes de blocs de Key et Moori

[PGHS15] M. Planat, A. Giorgetti, F. Holweck, M. Saniga.
Quantum contextual finite geometries from dessins d'enfants.
2015.

[SBB+12] V. Stodden, D.H. Bailey, J. Borwein, R.J. LeVeque, W. Rider.
Setting the Default to Reproducible. Technical report
2012.

Systèmes de blocs et structure d'incidence

Definition (Système de blocs)

Un bloc est une partie non vide d'un ensemble Ω. Un système de blocs (*block design* en anglais) $\mathcal{B}$ est un ensemble de blocs.

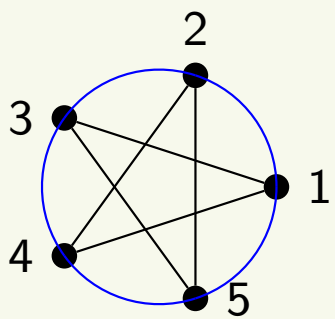
Definition (Structure d'incidence)

Une structure d'incidence est un triplet $\mathcal{D} = (\Omega, \mathcal{B}, \mathcal{I})$ où $\Omega = \{1, \ldots, n\}$ est un ensemble d'éléments fini, $\mathcal{B} = \{b_1, \ldots, b_p\}$ numérote un système de blocs sur Ω et $\mathcal{I} \subseteq \Omega \times \mathcal{B}$ est une *relation d'incidence*, qui définit l'appartenance d'un élément à un bloc.

Exemple de structure d'incidence

$\mathcal{I}$	1	2	3	4	5
b_1	1	1	1	1	1
b_2	1	0	1	0	0
b_3	1	0	0	1	0
b_4	0	1	0	1	0
b_5	0	1	0	0	1
b_6	0	0	1	0	1

$b_1 = \{1, 2, 3, 4, 5\}$
$b_2 = \{1, 3\}$
$b_3 = \{1, 4\}$
$b_4 = \{2, 4\}$
$b_5 = \{2, 5\}$
$b_6 = \{3, 5\}$



La proposition originale et sa correction

Proposition

Let G be a finite primitive permutation group acting on the set Ω of size n. Let $\alpha \in \Omega$, and let $\Delta \neq \{\alpha\}$ be an orbit of the stabilizer G_α of α. If

$$\mathcal{B} = \{\Delta^g : g \in G\}$$

and, given $\delta \in \Delta$,

$$\varepsilon = \{\{\alpha, \delta\}^g : g \in G\},$$

~~*then $\mathcal{B}$ forms a self-dual 1-$(n, |\Delta|, |\Delta|)$ design with n blocks, and ε forms the edge set of a regular connected graph of valency $|\Delta|$ [...]*~~
then $\mathcal{D} = (\Omega, \mathcal{B})$ forms a symmetric 1-$(n, |\Delta|, |\Delta|)$ design. Further, if Δ is a self-paired orbit of G_α then $\Gamma = (\Omega, \varepsilon)$ is a regular connected graph of valency $|\Delta|$, $\mathcal{D}$ is self-dual [...]

[KM02] J.D. Key, J. Moori.
Codes, Designs and Graphs from the Janko Groups J_1 and J_2.
2002.

[KM08] J.D. Key, J. Moori.
Correction to: Codes, Designs and Graphs from the Janko Groups J_1 and J_2.
2008.

Plan

Les types de systèmes de blocs

Definition (Systèmes de blocs t-(v, k, λ))

Un système de blocs t-(v, k, λ) est un système agissant sur v éléments, composé de blocs de cardinalité k, tel qu'un sous-ensemble quelconque de taille t soit présent dans exactement λ blocs [Col10].

Definition (BIBD)

Un BIBD (*Balanced Incomplete Block Design*) est un système de blocs 2-(v, k, λ) [Col10].

Plan de Fano

Le système de blocs $\{ \{2,3,5\}, \{3,4,6\}, \{4,5,7\}, \{7,1,3\}, \{6,1,5\}, \{2,4,1\}, \{7,2,6\} \}$, sur 7 éléments, est composé de blocs de 3 éléments, tels que tous les sous-ensembles de taille 2 soient présents dans exactement 1 bloc. C'est donc un système de blocs 2-$(7, 3, 1)$.

[Col10] C. Colbourn.
CRC Handbook of Combinatorial Designs.
2010.

Les groupes de permutations

Definition (Permutations)

Une permutation d'un ensemble Ω est une bijection de Ω sur lui-même.

- Notation matricielle
  - $1^{\text{ère}}$ ligne : éléments à permuter
  - 2^{e} ligne : images
- Notation en produit de cycles disjoints

Exemple de permutation

L'une des permutations possibles de l'ensemble $\Omega = \{1 \dots 7\}$ est

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

La même permutation en produit de cycles disjoints s'écrit $(1, 2, 4)(3, 6, 5)$.

Definition (Groupes de permutations)

Un groupe de permutations est un groupe G composé de permutations d'un ensemble Ω avec pour opération la composition des permutations.

Les groupes de permutations primitifs

Definition (Groupes transitifs)

Le groupe de permutations G sur un ensemble fini Ω est un groupe transitif si, pour tous les éléments x et y de Ω, il existe une permutation g de G telle que $g \bullet x = y$.

Definition (Groupes primitifs)

Le groupe de permutations G est un groupe primitif s'il est transitif et s'il ne préserve aucune partition non triviale de Ω, i.e. les partitions dont le seul élément est Ω et les partitions dont tous les éléments sont des singletons.

Exemple de groupe non primitif

Le groupe de permutations $H = \{ \text{Id}, (1,2,3,4), (1,4,3,2), (1,3)\ (2,4) \}$ sur $\{1,2,3,4\}$ est transitif mais n'est pas primitif. La partition (X_1, X_2) où $X_1 = \{1,3\}$ et $X_2 = \{2,4\}$ est préservée par $(1,2,3,4)$, i.e. $(1,2,3,4)X_1 = X_2$ et $(1,2,3,4)X_2 = X_1$.

Stabilisateurs et orbites d'un groupe

Definition (Stabilisateurs)

Le stabilisateur d'un élément α de Ω sous l'action de G est l'ensemble des permutations de G qui laissent α invariant sous leur action, soit $G_\alpha =_{\text{def}} \{g \in G : g \bullet \alpha = \alpha\}$.

Exemple de stabilisateurs

Soit le groupe G généré par les permutations $(1,2,3,4,5,6,7)$ et $(1,2,4)(3,6,5)$ agissant sur l'ensemble $\Omega = \{1 \dots 7\}$ et $\alpha = 1$. Le stabilisateur de G sur α est le groupe $G_\alpha = \{$ Id, $(2,3,5)\ (4,7,6)$, $(2,5,3)\ (4,6,7)$ $\}$.

Stabilisateurs et orbites d'un groupe

Definition (Stabilisateurs)

Le stabilisateur d'un élément α de Ω sous l'action de G est l'ensemble des permutations de G qui laissent α invariant sous leur action, soit $G_\alpha =_{\text{def}} \{g \in G : g \bullet \alpha = \alpha\}$.

Exemple de stabilisateurs

Soit le groupe G généré par les permutations $(1,2,3,4,5,6,7)$ et $(1,2,4)(3,6,5)$ agissant sur l'ensemble $\Omega = \{1 \dots 7\}$ et $\alpha = 1$. Le stabilisateur de G sur α est le groupe $G_\alpha = \{$ Id, $(2,3,5)\,(4,7,6)$, $(2,5,3)\,(4,6,7)$ $\}$.

Definition (Orbites)

L'orbite $O_x =_{\text{def}} \{g \bullet x : g \in H\}$ d'un élément x de Ω selon un groupe de permutations H sur Ω est l'ensemble des images de x par ses permutations.

Exemple d'orbites

Les orbites de G_α sont $O_1 = \{1\}$, $O_2 = O_3 = O_5 = \{2,3,5\}$ et $O_4 = O_6 = O_7 = \{4,6,7\}$.

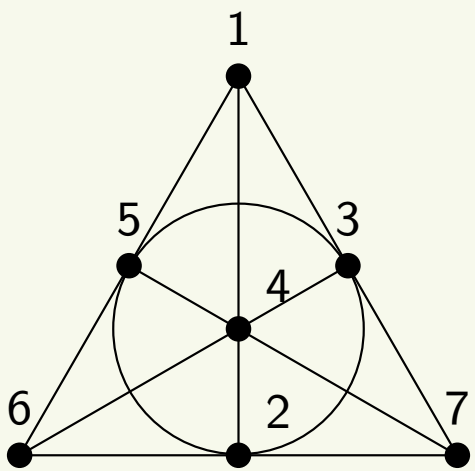
Exemple de construction d'un système de blocs

Construction du plan de Fano

Soit le groupe de permutations primitif G généré par les permutations $(1,2,3,4,5,6,7)$ et $(1,2,4)(3,6,5)$ agissant sur l'ensemble $\Omega = \{1 \dots 7\}$ et $\alpha = 1$.

Rappel : $G_\alpha = \{ \text{Id}, (2,3,5)(4,7,6), (2,5,3)(4,6,7) \}$ et $O_1 = \{1\}$, $O_2 = O_3 = O_5 = \{2,3,5\}$ et $O_4 = O_6 = O_7 = \{4,7,6\}$.

Pour l'orbite $\Delta = \{2,3,5\}$, le système de blocs construit est $\mathcal{B} = \{ \{2,3,5\}, \{3,4,6\}, \{4,5,7\}, \{7,1,3\}, \{6,1,5\}, \{2,4,1\}, \{7,2,6\} \}$.



Auto-dualité

Definition (Structure duale)

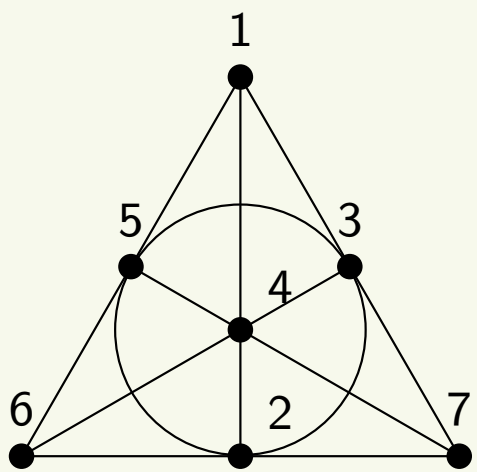
La structure d'incidence $\mathcal{D} = (\Omega, \mathcal{B}, \mathcal{I})$ a pour structure d'incidence duale $\mathcal{D}^{-1} =_{\text{def}} (\mathcal{B}, \Omega, \mathcal{I}^{-1})$ où $(y, x) \in \mathcal{I}^{-1}$ si et seulement si $(x, y) \in \mathcal{I}$.

Definition (Auto-dual)

Un système de blocs est auto-dual (*self-dual* en anglais) s'il est isomorphe à son dual.

Exemple de structure auto-duale

$\mathcal{I}$	1	2	3	4	5	6	7
b_1	1	0	0	0	1	1	0
b_2	0	1	1	0	1	0	0
b_3	0	1	0	0	0	1	1
b_4	0	0	0	1	1	0	1
b_5	1	1	0	1	0	0	0
b_6	1	0	1	0	0	0	1
b_7	0	0	1	1	0	1	0



Exemple de construction de graphes

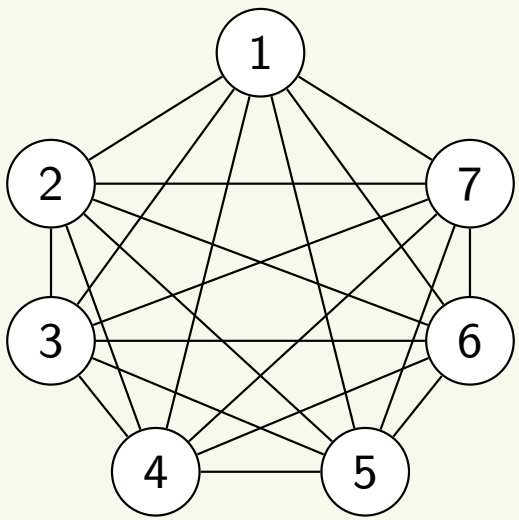
Proposition (Extrait)

[. . .] given $\delta \in \Delta$,

$$\varepsilon = \{\{\alpha, \delta\}^g : g \in G\},\ [\ldots]$$

Construction d'un des graphes correspondants

Soit le précédent groupe primitif G généré par les permutations $(1, 2, 3, 4, 5, 6, 7)$ et $(1, 2, 4)(3, 6, 5)$ agissant sur l'ensemble $\Omega = \{1 \ldots 7\}$, $\alpha = 1$ et l'orbite $\Delta = \{2, 3, 5\}$. Avec $\delta = 2$, le graphe construit est le graphe complet K_7.



Sommaire

Fonction de calcul des orbites Δ

Proposition (Extrait)

Let G be a finite primitive permutation group acting on the set Ω of size n. Let $\alpha \in \Omega$, and let $\Delta \neq \{\alpha\}$ be an orbit of the stabilizer G_α of α. [...]

```
/**
 * Compute orbits of stabilizers of a primitive group [KM02, Proposition 1].
 *
 * @param G::GrpPerm A primitive group
 * @return Deltas::Assoc An associative array indexed by alpha
 *     and containing the corresponding delta set
 */
AllDelta := function(G)
  n := Degree(G);
  Omega := {1..n};
  Deltas := AssociativeArray();
  for alpha in Omega do
    Galpha := Stabilizer(G, alpha);
    orbits := Orbits(Galpha);
    Deltas[alpha] := { IndexedSetToSet(Delta) : Delta in orbits | Delta ne { alpha } };
  end for;
  return Deltas;
end function;
```

Fonction de construction de systèmes de blocs

Proposition (Extrait)

Let G be a finite primitive permutation group acting on the set Ω of size n. [...]

$$\mathcal{B} = \{\Delta^g : g \in G\}[\ldots]$$

```
/**
 * Builds all block designs from a primitive group [KM02, Proposition 1]
 *
 * @param G::GrpPerm A primitive group
 * @return blocks::Assoc An associative array indexed by delta indexes
 *     and containing corresponding block designs
 */
BlckDsgnsFromPrmtvGrp := function(G)
  Deltas := AllDelta(G);
  blocks := AssociativeArray();
  for alpha in Keys(Deltas) do
    for Delta in Deltas[alpha] do
      blocks[Delta] := { Delta^g : g in G };
    end for;
  end for;
  return blocks;
end function;
```

Fonction de construction de graphes

Proposition (Extrait)

Let G be a finite primitive permutation group acting on the set Ω of size n. [...] given $\delta \in \Delta$,

$$\varepsilon = \{\{\alpha, \delta\}^g : g \in G\}, [...]$$

```
/**
 * Construct all graphs from a primitive group [KM02,KM08]
 *
 * @param G::GrpPerm A primitive group
 * @return graphs::Assoc An associative array indexed by delta indexes
 *    and containing the corresponding graph represented by a set of edges
 */
GraphFromPrmtvGrp := function(G)
  Deltas := AllDelta(G);
  graphs := AssociativeArray();
  for alpha in Keys(Deltas) do
    graphs[alpha] := AssociativeArray();
    for Delta in Deltas[alpha] do
      graphs[alpha][Delta] := [ { {alpha, delta}^g : g in G } : delta in Delta ];
    end for;
  end for;
  return graphs;
end function;
```

Sommaire

Fonctions proposées par Magma

Proposition (Extrait)

[. . .]
~~then $\mathcal{B}$ forms a self-dual 1-$(n, |\Delta|, |\Delta|)$ design with n blocks, and ε forms the edge set of a regular connected graph of valency $|\Delta|$ [. . .]~~
then $\mathcal{D} = (\Omega, \mathcal{B})$ forms a symmetric 1-$(n, |\Delta|, |\Delta|)$ design. Further, if Δ is a self-paired orbit of G_α then $\Gamma = (\Omega, \varepsilon)$ is a regular connected graph of valency $|\Delta|$, $\mathcal{D}$ is self-dual [. . .]

- `IsSelfDual`
- `IsSymmetric`
- `Parameters`
- `IsConnected`
- `IsRegular`
- `Valence`
- `IncidenceStructure`
- `Design`
- `Graph`
- `PrimitiveGroups`

Fonction caractéristique d'un système de blocs t-(v, k, λ)

Proposition (Extrait)

[. . .]
~~then $\mathcal{B}$ forms a self-dual 1-$(n, |\Delta|, |\Delta|)$ design with n blocks [. . .]~~
then $\mathcal{D} = (\Omega, \mathcal{B})$ forms a symmetric 1-$(n, |\Delta|, |\Delta|)$ design. [. . .]

```
/**
 * Characterization of t-(v,k,lambda) block designs
 *
 * @param blocks::Set The design blocks
 * @param t::RngIntElt The number of elements distinct in lambda blocks
 * @param v::RngIntElt The number of blocks
 * @param k::RngIntElt The cardinality of blocks
 * @param lambda::RngIntElt The number of blocks contains t elements distinct
 * @return BoolElt Indicates that blocks design is a t-(v,k,lambda) block design
 */
CorrectDesign := function(blocks, t, v, k, lambda)
  incidence := IncidenceStructure<v | blocks>;
  if not IsDesign(incidence, t) then
    return false;
  end if;
  record := Parameters(Design(incidence, t));
  return record`v eq v and record`k eq k and record`lambda eq lambda;
end function;
```

Symétrie

Definition (Symétrie selon Key et Moori)

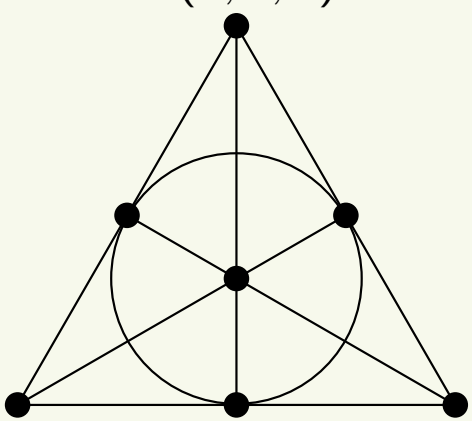
Un système de blocs est symétrique s'il possède autant d'éléments que de blocs.

Definition (Symétrie selon Magma)

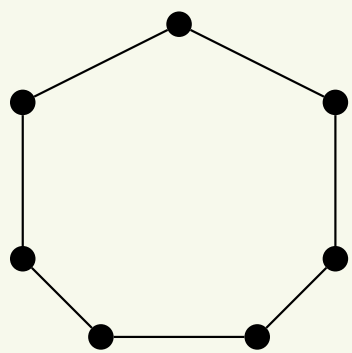
Un système de blocs est symétrique si c'est un BIBD et s'il possède autant d'éléments que de blocs.

Exemples de symétries

$2\text{-}(7, 3, 1)$



$1\text{-}(7, 2, 2)$



Résultats

Systèmes de blocs

- 74 groupes de permutations primitifs (tous jusqu'au degré 13)
- 926 systèmes de blocs construits
- 574 107 secondes (environ 7 jours)
- 0 contre-exemple pour la proposition originale
- 0 contre-exemple pour la correction (définition symétrie de Key et Moori)
- 398 contre-exemples pour la correction (définition symétrie de Magma)

Résultats

Graphes

- 49 groupes de permutations primitifs (tous jusqu'au degré $n = 10$)
- 2 546 graphes construits
- 1 606 secondes (environ 27 minutes)
- 110 contre-exemples pour la proposition originale
- 0 contre-exemple pour la correction

Conclusion

- Exemple d'implémentation et de validation d'une proposition mathématique
- Confirmation d'une erreur dans la proposition originale
- Validation de la correction pour tous les groupes primitifs de degré entre 1 et 13
- Révélation d'une ambiguïté sur la définition de symétrie
- Code complet accessible à l'adresse `https://quantcert.github.io/Designs/`

Questions

- Merci pour votre attention
- Questions ?