Tour d'horizon sur des algèbres généralisant les octonions

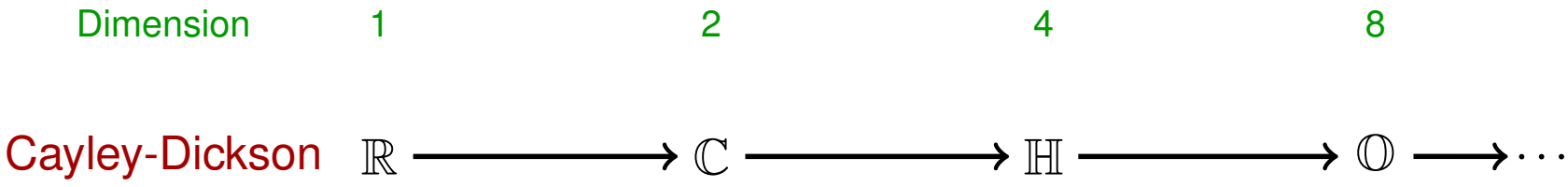
Colloque Inter'Actions : 19 – 23 mai 2014

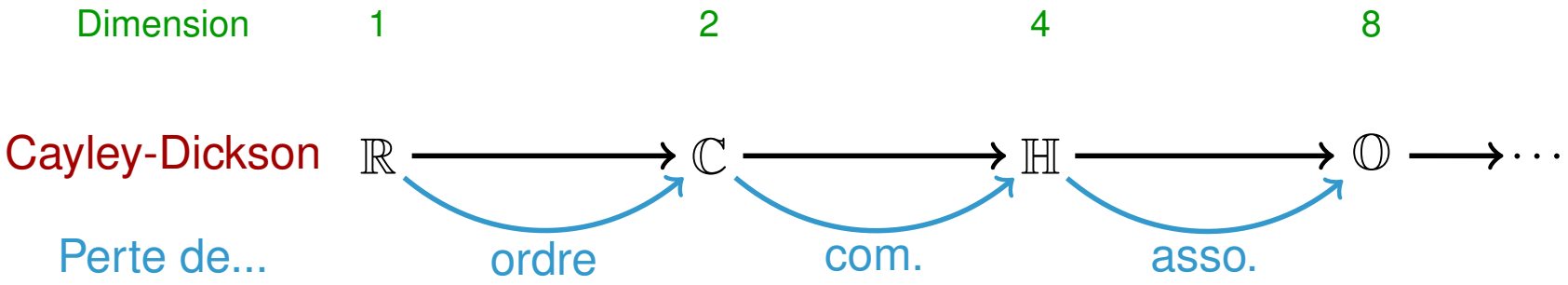
Marie Kreusch

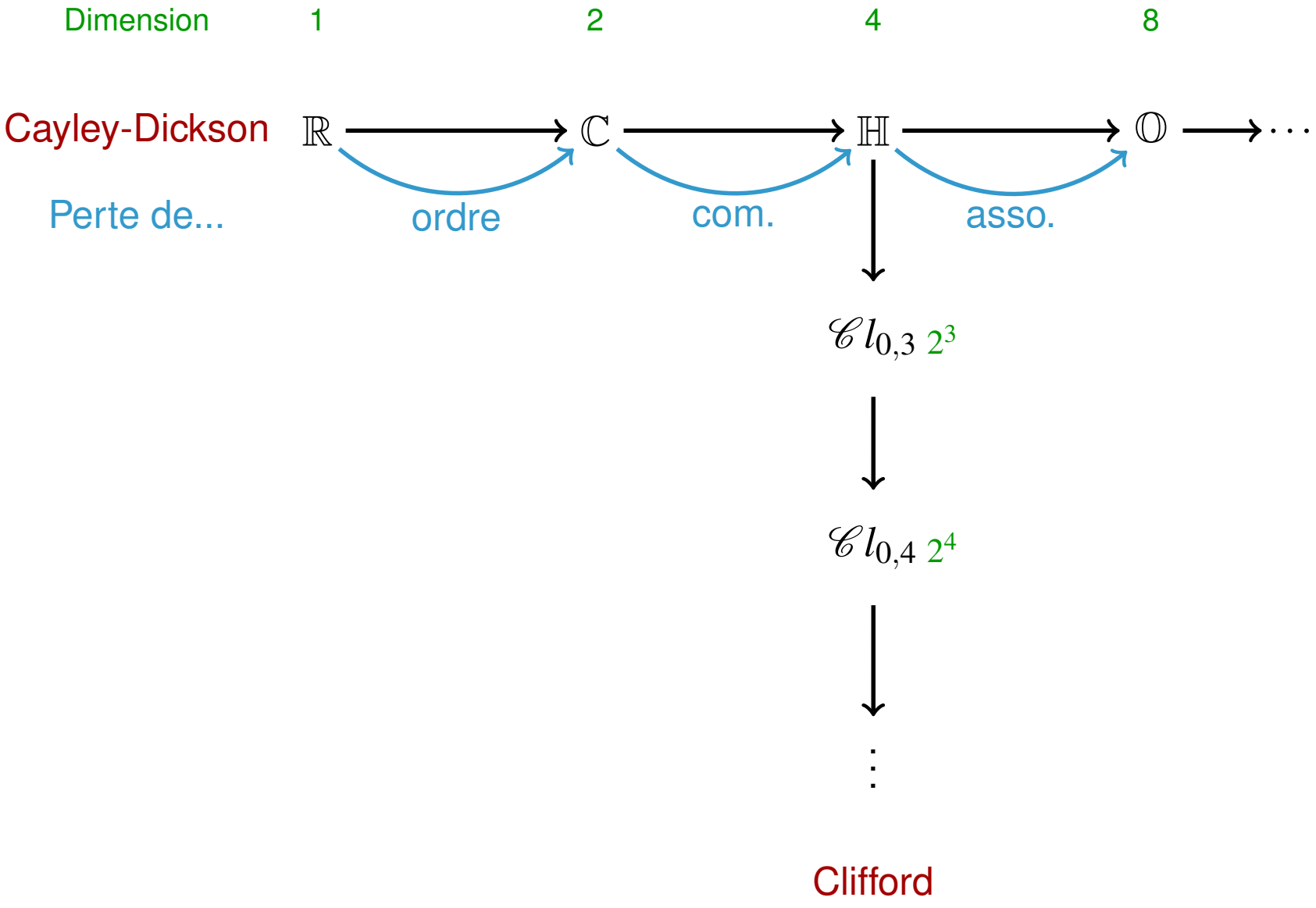
Université de Liège

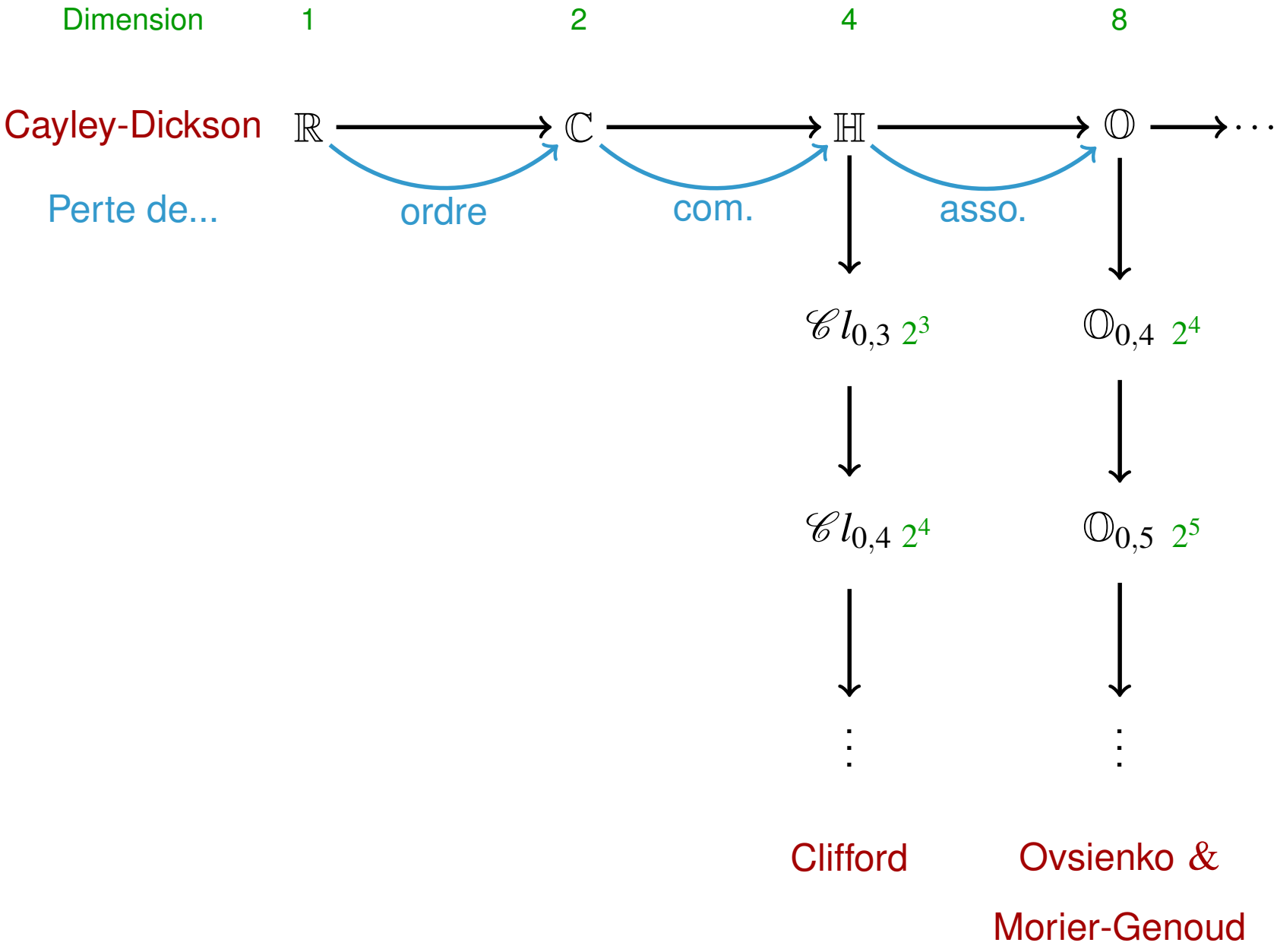
Tour d'horizon sur des algèbres généralisant les octonions


Cayley-Dickson
$\mathbb{R}$
$\mathbb{C}$
$\mathbb{H}$
$\mathbb{O}$
$\cdots$


Dimension
1
2
4
8
Cayley-Dickson
$\mathbb{R}$
$\mathbb{C}$
$\mathbb{H}$
$\mathbb{O}$
$\cdots$


Dimension
1
2
4
8
Cayley-Dickson
$\mathbb{R}$
$\mathbb{C}$
$\mathbb{H}$
$\mathbb{O}$
$\cdots$
Perte de...
ordre
com.
asso.


Dimension
1
2
4
8
Cayley-Dickson
$\mathbb{R}$
$\mathbb{C}$
$\mathbb{H}$
$\mathbb{O}$
$\cdots$
Perte de...
ordre
com.
asso.
$\mathscr{C}l_{0,3}$ 2^3
$\mathscr{C}l_{0,4}$ 2^4
Clifford


Dimension
1
2
4
8
Cayley-Dickson
Perte de...
$\mathbb{R}$
$\mathbb{C}$
$\mathbb{H}$
$\mathbb{O}$
$\cdots$
ordre
com.
asso.
$\mathscr{C}l_{0,3}$ 2^3
$\mathbb{O}_{0,4}$ 2^4
$\mathscr{C}l_{0,4}$ 2^4
$\mathbb{O}_{0,5}$ 2^5
Clifford
Ovsienko &
Morier-Genoud

Algèbre $\mathscr{C}l_{p,q}$

Définition

L'algèbre $\mathscr{C}l_{p,q}$ $(p+q=n\geq 0)$ est une algèbre sur $\mathbb{R}$ associative et unitaire (l'unité est notée $\mathbb{1}$) générée par les éléments $v_1,\ldots,v_n$ tels que

$$(v_i)^2=\begin{cases} +1 & si \quad 1\leq i\leq p,\\ -1 & si \quad p+1\leq i\leq n,\end{cases}$$

$$v_i\cdot v_j=-v_j\cdot v_i, \qquad i\neq j.$$

Algèbre $\mathscr{C}l_{p,q}$

Exemples

$$\mathscr{C}l_{0,0} \simeq \mathbb{R}$$

$$\mathscr{C}l_{1,0} \simeq \mathbb{R} \oplus \mathbb{R} \quad \text{et} \quad \mathscr{C}l_{0,1} \simeq \mathbb{C}$$

$$\mathscr{C}l_{2,0} \simeq \mathscr{C}l_{1,1} \simeq Mat(2,\mathbb{R}) \quad \text{et} \quad \mathscr{C}l_{0,2} \simeq \mathbb{H}$$

Algèbre $\mathscr{C}l_{p,q}$

Théroème

Toute algèbre de Clifford est isomorphe à une algèbre de matrice à coefficients dans $\mathbb{R}$, $\mathbb{C}$ ou $\mathbb{H}$ ou bien à une somme directe de celles-ci.

Théroème

$$\begin{aligned} \mathrm{Cl}_{p+2,q} &\simeq \mathrm{Cl}_{q,p} \otimes_{\mathbb{R}} \mathrm{Cl}_{2,0} \\ \mathrm{Cl}_{p,q+2} &\simeq \mathrm{Cl}_{q,p} \otimes_{\mathbb{R}} \mathrm{Cl}_{0,2} \\ \mathrm{Cl}_{p+1,q+1} &\simeq \mathrm{Cl}_{p,q} \otimes_{\mathbb{R}} \mathrm{Cl}_{1,1} \end{aligned}$$

Corollaire

$$\mathrm{Cl}_{p+8,q} \simeq \mathrm{Cl}_{p,q+8} \simeq \mathrm{Cl}_{p,q} \otimes_{\mathbb{R}} \mathit{Mat}(16,\mathbb{R})$$

Algèbre $\mathscr{C}l_{p,q}$

Les éléments de base de $\mathscr{C}l_{p,q}$ sont

$$v_{i_1} \cdots v_{i_k}$$

où $1 \leq i_1 < \cdots < i_k \leq n$ peuvent être codé par un n-uplet de 0 ou de 1.

Illustration

$$\begin{aligned} \mathbb{1} &\longleftrightarrow (0,\ldots,0) \\ v_i &\longleftrightarrow (0,\ldots,0,1,0\ldots,0) = e_i \\ v_1 \cdots v_n &\longleftrightarrow (1,\ldots,1) \end{aligned}$$

Algèbre $\mathbb{O}_{p,q}$

Définition

L' algèbre $\mathbb{O}_{p,q}$ $(p+q \geq 3)$ est une algèbre sur $\mathbb{R}$ ayant pour base les éléments u_x, $x \in (\mathbb{Z}_2)^n$ et munie du produit

$$u_x \cdot u_y = (-1)^{f(x,y)} u_{x+y}$$

avec

$$f_{\mathbb{O}_{p,q}}(x,y) = \sum_{1 \leq i < j < k \leq n} (x_i x_j y_k + x_i y_j x_k + y_i x_j x_k) + \sum_{1 \leq i \leq j \leq n} x_i y_j + \sum_{1 \leq i \leq p} x_i$$

pour $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n) \in (\mathbb{Z}_2)^n$.

O. & M.-G. [2011]

Algèbre $\mathbb{O}_{p,q}$

Définition

L' algèbre $\mathbb{O}_{p,q}$ $(p+q \geq 3)$ est une algèbre sur $\mathbb{R}$ ayant pour base les éléments u_x, $x \in (\mathbb{Z}_2)^n$ et munie du produit

$$u_x \cdot u_y = (-1)^{f(x,y)} u_{x+y}$$

avec

$$f_{\mathbb{O}_{p,q}}(x,y) = \sum_{1 \leq i < j < k \leq n} (x_i x_j y_k + x_i y_j x_k + y_i x_j x_k) + \sum_{1 \leq i \leq j \leq n} x_i y_j + \sum_{1 \leq i \leq p} x_i$$

Notation

$(\mathbb{R}[\mathbb{Z}_2^n], f)$ (algèbre de groupe twistée)

Algèbre $\mathscr{C}l_{p,q}$

Définition équivalente

L' algèbre $\mathscr{C}l_{p,q}$ $(p+q \geq 0)$ est une algèbre sur $\mathbb{R}$ ayant pour base les éléments u_x, $x \in (\mathbb{Z}_2)^n$ et munie du produit

$$u_x \cdot u_y = (-1)^{f(x,y)} u_{x+y}$$

avec

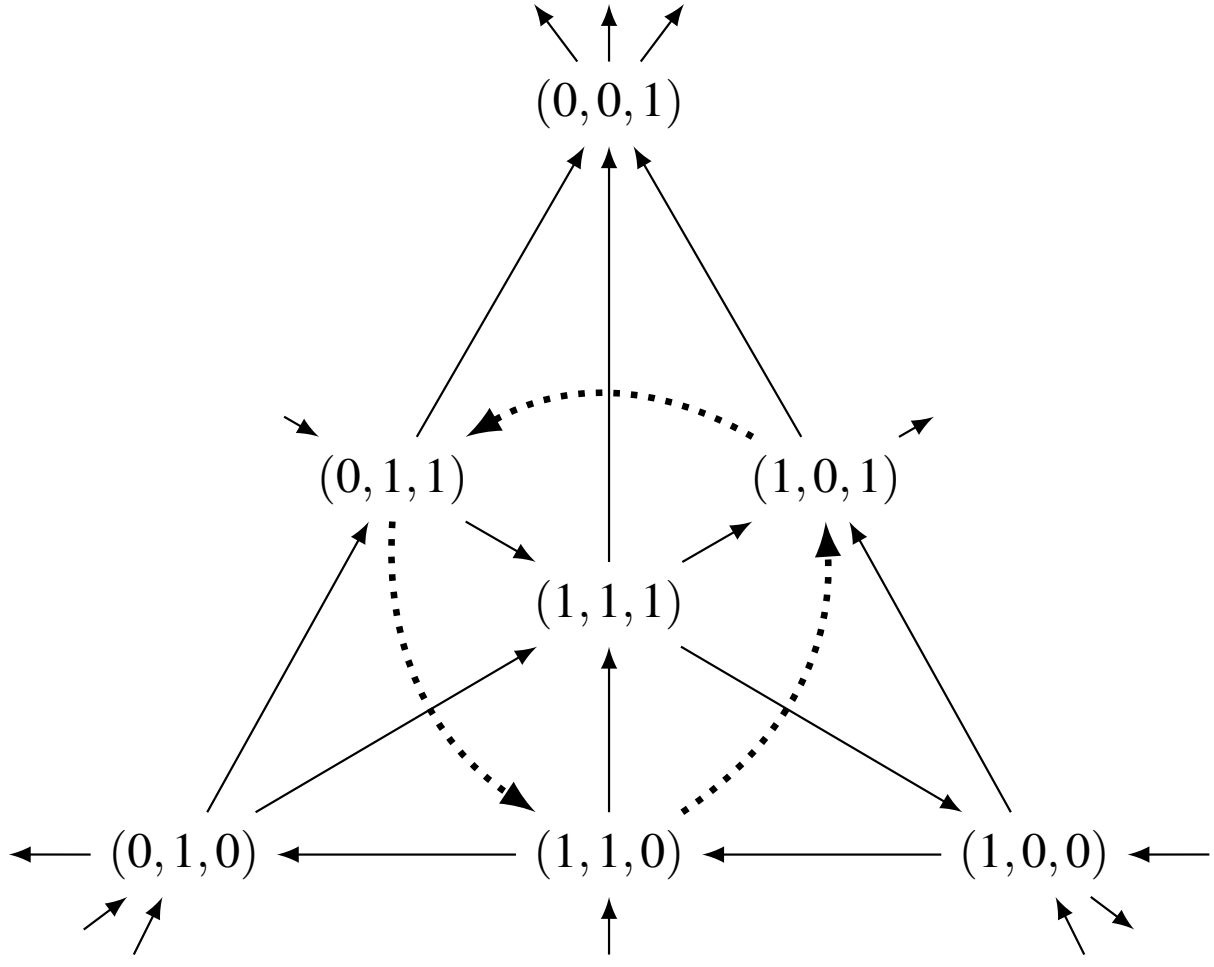
$$f_{\mathscr{C}l_{p,q}}(x,y) = \sum_{1 \leq i < j < k \leq n} (x_i x_j y_k + x_i y_j x_k + y_i x_j x_k) + \sum_{1 \leq i \leq j \leq n} x_i y_j + \sum_{1 \leq i \leq p} x_i$$

Albuquerque & Majid [2000]

Algèbre $\mathbb{O}_{p,q}$

Exemple

$$\mathbb{O}_{0,3} \simeq \mathbb{O}$$



A. & M. [2000]

Algèbre $\mathbb{O}_{p,q}$

Remarques

L'unité $\mathbb{1} := u_{(0,\ldots,0)}$

Notons $|x|$ le poids de $x \in (\mathbb{Z}_2)^n$

Système de générateurs : $u_i = u_{e_i}$ où $e_i = (0,\ldots,0,1,0\ldots,0) \in (\mathbb{Z}_2)^n$

Sous algèbre associative maximale $\mathscr{C}l_{p,q-1} \subset \mathbb{O}_{p,q}$

(sélectionner u_x où $x \in (\mathbb{Z}_2)^n$ tels que $|x| \equiv 0 \bmod 2$)

Résultat

Question

Existe-il une périodicité entre ces algèbres ?

Résultat

Question

Existe-il une périodicité entre ces algèbres ?

Théorème

i) $\mathbb{O}_{0,n+4} \cong \mathbb{O}_{0,n} \otimes_{\mathbb{C}} \mathbb{O}_{0,5}$

ii) $\mathbb{O}_{n+4,0} \cong \mathbb{O}_{n,0} \otimes_{\mathbb{R}\oplus\mathbb{R}} \mathbb{O}_{5,0}$

iii) $\mathbb{O}_{p+2,q+2} \cong \mathbb{O}_{p,q} \otimes_{\mathbb{C}} \mathbb{O}_{2,3}$

$\cong \mathbb{O}_{p,q} \otimes_{\mathbb{R}\oplus\mathbb{R}} \mathbb{O}_{3,2}$

K. [soumis]

Résultat

Question

Existe-il une périodicité entre ces algèbres ?

Théorème

i) $\mathbb{O}_{0,n+4} \cong \mathbb{O}_{0,n} \otimes_{\mathbb{C}} \mathbb{O}_{0,5}$ $\quad \mathrm{Cl}_{p,q+2} \simeq \mathrm{Cl}_{q,p} \otimes_{\mathbb{R}} \mathrm{Cl}_{0,2}$

ii) $\mathbb{O}_{n+4,0} \cong \mathbb{O}_{n,0} \otimes_{\mathbb{R}\oplus\mathbb{R}} \mathbb{O}_{5,0}$ $\quad \mathrm{Cl}_{p+2,q} \simeq \mathrm{Cl}_{q,p} \otimes_{\mathbb{R}} \mathrm{Cl}_{2,0}$

iii) $\mathbb{O}_{p+2,q+2} \cong \mathbb{O}_{p,q} \otimes_{\mathbb{C}} \mathbb{O}_{2,3}$ $\quad \mathrm{Cl}_{p+1,q+1} \simeq \mathrm{Cl}_{p,q} \otimes_{\mathbb{R}} \mathrm{Cl}_{1,1}$

$\cong \mathbb{O}_{p,q} \otimes_{\mathbb{R}\oplus\mathbb{R}} \mathbb{O}_{3,2}$

K. [soumis]

Forme cubique

Théorème

Dans notre cas, il existe une fonction génératrice cubique $\alpha : (\mathbb{Z}_2)^n \longrightarrow \mathbb{Z}_2$ qui caractérise complètement l'algèbre $(\mathbb{R}[\mathbb{Z}_2^n], f)$ définie par

$$\alpha_{\mathbb{O}_{p,q}}(x) = f_{\mathbb{O}_{p,q}}(x,x) = \sum_{1 \leq i < j < k \leq n} x_i x_j x_k + \sum_{1 \leq i \leq j \leq n} x_i x_j + \sum_{1 \leq i \leq p} x_i$$

M.-G. & O. [2011]

Forme cubique

Théorème

Dans notre cas, il existe une fonction génératrice cubique $\alpha : (\mathbb{Z}_2)^n \longrightarrow \mathbb{Z}_2$ qui caractérise complètement l'algèbre $(\mathbb{R}[\mathbb{Z}_2^n], f)$ définie par

$$\alpha_{\mathbb{O}_{p,q}}(x) = f_{\mathbb{O}_{p,q}}(x,x) = \sum_{1 \leq i < j < k \leq n} x_i x_j x_k + \sum_{1 \leq i \leq j \leq n} x_i x_j + \sum_{1 \leq i \leq p} x_i$$

M.-G. & O. [2011]

Forme cubique

Théorème

Dans notre cas, il existe une fonction génératrice cubique $\alpha : (\mathbb{Z}_2)^n \longrightarrow \mathbb{Z}_2$ qui caractérise complètement l'algèbre $(\mathbb{R}[\mathbb{Z}_2^n], f)$ définie par

$$\alpha_{\mathbb{O}_{p,q}}(x) = f_{\mathbb{O}_{p,q}}(x,x) = \underbrace{\sum_{1\leq i<j<k\leq n} x_i x_j x_k + \sum_{1\leq i\leq j\leq n} x_i x_j}_{\alpha_{\mathbb{O}_n}(x)} + \sum_{1\leq i\leq p} x_i$$

où

$$\alpha_{\mathbb{O}_n}(x) = \begin{cases} 0 \text{ si } |x| \equiv 0 \bmod 4 \\ 1 \text{ sinon} \end{cases}$$

M.-G. & O. [2011]

Forme quadratique

Dans le cas Clifford, il existe une fonction génératrice $\alpha : (\mathbb{Z}_2)^n \longrightarrow \mathbb{Z}_2$ qui caractérise complètement l'algèbre $(\mathbb{R}[\mathbb{Z}_2^n], f)$ définie par

$$\alpha_{\mathscr{C}l_{p,q}}(x) = f_{\mathscr{C}l_{p,q}}(x,x) = \sum_{1\leq i<j<k\leq n} x_i x_j x_k + \underbrace{\sum_{1\leq i\leq j\leq n} x_i x_j}_{\alpha_{\mathscr{C}l_n}(x)} + \sum_{1\leq i\leq p} x_i$$

où

$$\alpha_{\mathscr{C}l_n}(x) = \begin{cases} 0 \text{ si } |x| \equiv 0 \bmod 2 \\ 1 \text{ sinon} \end{cases}$$

Forme cubique

Définition

Les formes cubiques α et α' sont *équivalentes* si

$$\exists G \in \mathrm{GL}_n(\mathbb{Z}_2) \quad \text{telle que} \quad \alpha(x) = \alpha'(Gx).$$

Proposition

Si deux algèbres de groupe twistées $(\mathbb{K}\left[\mathbb{Z}_2^n\right], f)$ et $(\mathbb{K}\left[\mathbb{Z}_2^n\right], f')$ ont des fonctions génératrices équivalentes α et α', alors

$$(\mathbb{K}\left[\mathbb{Z}_2^n\right], f) \cong (\mathbb{K}\left[\mathbb{Z}_2^n\right], f')$$

Forme cubique et graphe triangulé

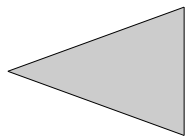
Définition

$$\alpha(x) = \sum_{1 \leq i < j < k \leq n} A_{ijk} x_i x_j x_k + \sum_{1 \leq i \leq j \leq n} B_{ij} x_i x_j + \sum_{1 \leq i \leq p} C_i x_i$$

1. Si x_i apparait dans α $(C_i = 1)$ $\longleftrightarrow$ •

   Si x_i n'apparait pas dans α $(C_i = 0)$ $\longleftrightarrow$ ∘

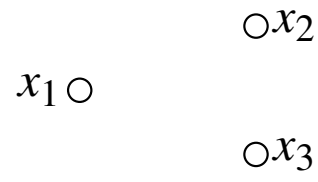
2. Si $x_i x_j$ apparait dans α $(B_{ij} = 1)$ $\longleftrightarrow$

3. Si $x_i x_j x_k$ apparait dans α $(A_{ijk} = 1)$ $\longleftrightarrow$ 

Forme cubique et graphe triangulé

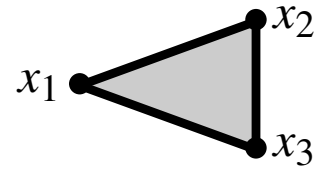
Exemple

$$\alpha(x_1,x_2,x_3) \equiv 0 \quad \longleftrightarrow$$

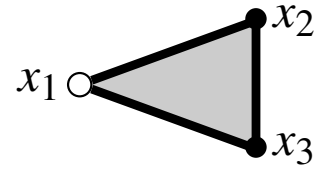


$$\alpha_{0,2}(x_1,x_2) = x_1x_2 + x_1 + x_2 \quad \longleftrightarrow$$

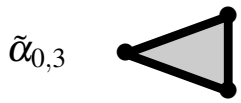
$$\alpha_{0,3}(x_1,x_2,x_3) = x_1x_2x_3 + x_1x_2 + x_1x_3 + x_2x_3 + x_1 + x_2 + x_3, \quad \longleftrightarrow$$

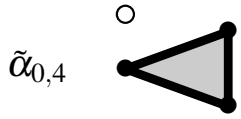


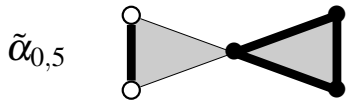
$$\alpha_{1,2}(x_1,x_2,x_3) = x_1x_2x_3 + x_1x_2 + x_1x_3 + x_2x_3 + x_2 + x_3, \quad \longleftrightarrow$$

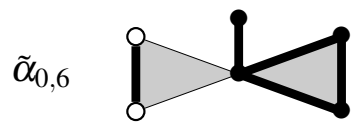


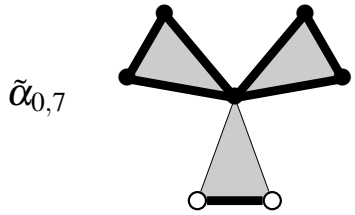
Classification

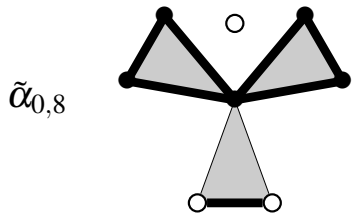


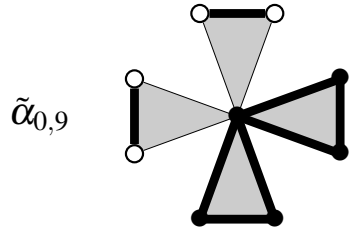


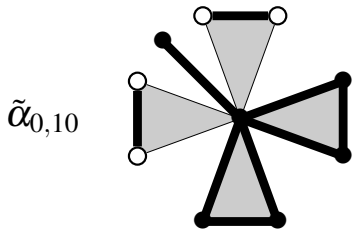


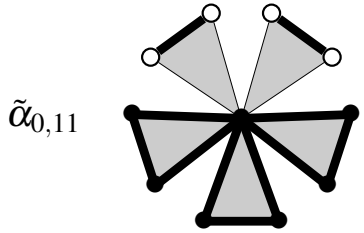


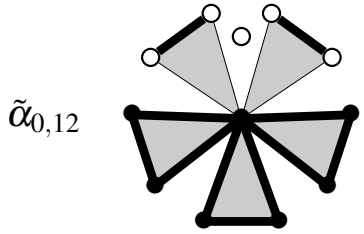


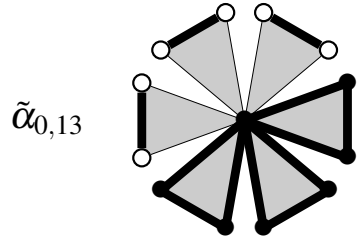


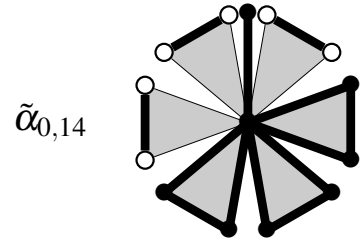




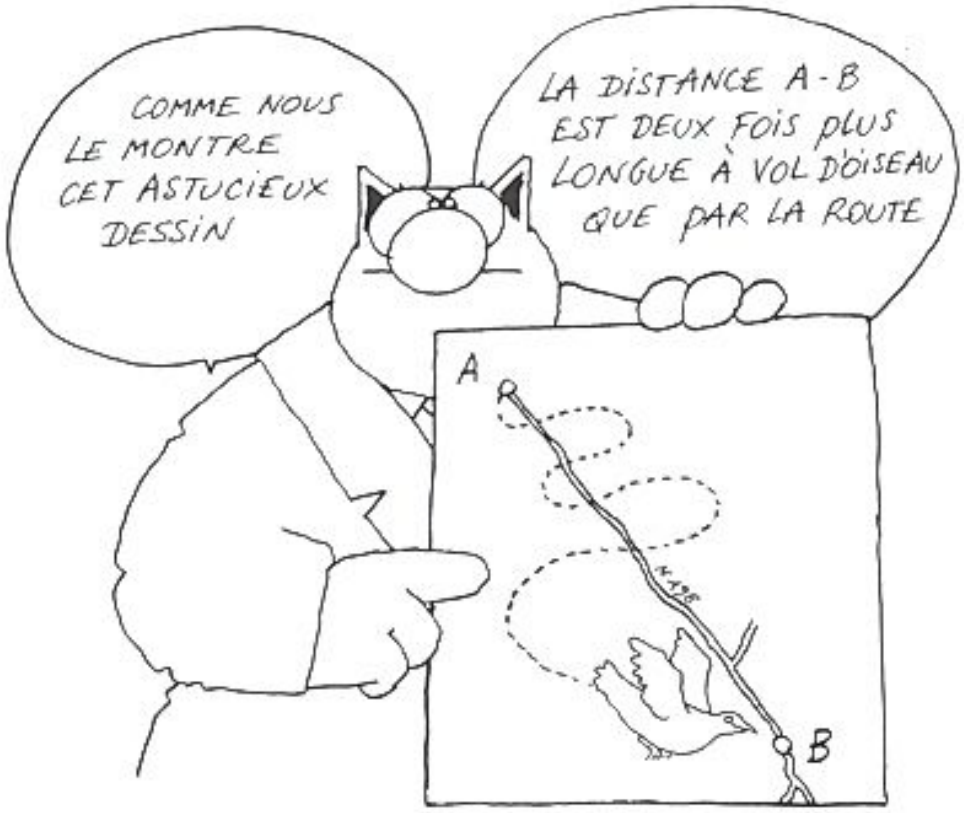








(Dé)tour sur des algèbres généralisant les octonions



Forme cubique et forme triangulée

Question ouverte

Classification des formes cubiques

Forme cubique et forme triangulée

Question ouverte

Classification des formes cubiques

"When we pass from quadratic to cubic functions, the complexity of the classification problem increases sharply."

Boolean functions in coding theory and cryptography, L., S. & Y. [2004]

Forme cubique et forme triangulée

Question ouverte

Classification des formes cubiques

"When we pass from quadratic to cubic functions, the complexity of the classification problem increases sharply."

Boolean functions in coding theory and cryptography, L., S. & Y. [2004]

"With computer assist, we also determine all the *cubic bent functions* in 8 variables."

Cubic Bent Functions, H. [1997]

Forme cubique et forme triangulée

Question ouverte

Classification des formes cubiques

"When we pass from quadratic to cubic functions, the complexity of the classification problem increases sharply."

Boolean functions in coding theory and cryptography, L., S. & Y. [2004]

"With computer assist, we also determine all the *cubic bent functions* in 8 variables."

Cubic Bent Functions, H. [1997]

"We describe a new invariant that we have used to obtain the complete classification of the cubic forms of nine variables."

Classification of Boolean Cubic Forms in Nine Variables, B. & L. [2003]

Forme cubique et forme triangulée

Question ouverte

Etude d’invariants

Par exemple, l’invariant de Arf ou "democratic invariant"

Forme cubique et forme triangulée

Question ouverte

Etude d’invariants

Par exemple, l’invariant de Arf ou "democratic invariant"

Question ouverte

Utiliser les propriétés des graphes pour en déduire celles des formes cubiques.

Détour sur des algèbres généralisant les octonions