Cayley graphs based on octonions, and their implementation in MAGMA

Dahan Xavier

Ochanomizu Univeristy, Faculty of General Educational Research

ACA 2017, July 17-21 — Algebraic Graph Theory

Introduction

Lubotzky-Philips-Sarnak, 1986-88 "Ramanujan graphs"
Combinatorica **8**:261-277, 1988

G. Margulis "Explicit group-theoretic constructions of combinatorial schemes and their applications for the construction of expanders and concentrators

Journal of Problems of Information Transmission 24(1):51-60, 1988.

Introduction

Lubotzky-Philips-Sarnak, 1986-88 "Ramanujan graphs"
Combinatorica **8**:261-277, 1988

G. Margulis "Explicit group-theoretic constructions of combinatorial schemes and their applications for the construction of expanders and concentrators

Journal of Problems of Information Transmission 24(1):51-60, 1988.

Ramanujan graph of degee d: undirected, connected graph G, such that: for all $\lambda \neq \pm d$ eigenvalue, $|\lambda| \leq 2\sqrt{d-1}$.

$\rightarrow$ very good certified expander graphs

- **Many** applications in Computer Science, Mathematics etc.

Introduction

Lubotzky-Philips-Sarnak, 1986-88 "Ramanujan graphs"
Combinatorica **8**:261-277, 1988

G. Margulis "Explicit group-theoretic constructions of combinatorial schemes and their applications for the construction of expanders and concentrators
Journal of Problems of Information Transmission 24(1):51-60, 1988.

Ramanujan graph of degee d: undirected, connected graph G, such that: for all $\lambda \neq \pm d$ eigenvalue, $|\lambda| \leq 2\sqrt{d-1}$.

$\rightarrow$ very good certified expander graphs

- **Many** applications in Computer Science, Mathematics etc.

Large girth No small cycle (actual record)

- a classical problem in extremal graph theoery,
- with several applications: LDPC error-correcting codes
- metric embeddings etc

LPS Ramanujan graphs and quaternions

These remarkable graphs are Cayley graphs on some groups of quaternions over finite fields.

What happens with octonions?

LPS Ramanujan graphs and quaternions

These remarkable graphs are Cayley graphs on some groups of quaternions over finite fields.

What happens with octonions?

- Construction possible (and not trivial)
- But very unlikely to be Ramanujan graphs or having large girth.

→ Implementation in Magma, check on “small” parameters the second eigenvalue and the girth of these graphs.

LPS Ramanujan graphs and quaternions

These remarkable graphs are Cayley graphs on some groups of quaternions over finite fields.

What happens with octonions?

- Construction possible (and not trivial)
- But very unlikely to be Ramanujan graphs or having large girth.

→ Implementation in Magma, check on "small" parameters the second eigenvalue and the girth of these graphs.

So any interesting porperties?

- Conjecture: they are non-vertex transitive
- Difficulty: How to describe a non-trivial automorphism?

(Undirected) Cayley graphs

- Let H be a group and $S \subset H$ a symmetric subset : $S^{-1} = S$. (S is called the **Cayley set**).

(Undirected) Cayley graphs

- Let H be a group and $S \subset H$ a symmetric subset : $S^{-1} = S$. (S is called the **Cayley set**).
- $\mathscr{C}ay(H, S)$ has for vertices V the elements of H. And for edges (h, sh) for $h \in H$ an $s \in S$.

(Undirected) Cayley graphs

- Let H be a group and $S \subset H$ a symmetric subset : $S^{-1} = S$. (S is called the **Cayley set**).
- $\mathscr{C}ay(H, S)$ has for vertices V the elements of H. And for edges (h, sh) for $h \in H$ an $s \in S$.
- $\mathscr{C}ay(H, S)$ is $|S|$-regular.

(Undirected) Cayley graphs

- Let H be a group and $S \subset H$ a symmetric subset : $S^{-1} = S$. (S is called the **Cayley set**).
- $\mathscr{C}ay(H,S)$ has for vertices V the elements of H. And for edges (h, sh) for $h \in H$ an $s \in S$.
- $\mathscr{C}ay(H,S)$ is $|S|$-regular.
- If H is a free group on d elements S, then $\mathscr{C}ay(H,S)$ is the d-regular infinite tree.

(Undirected) Cayley graphs

- Let H be a group and $S \subset H$ a symmetric subset : $S^{-1} = S$. (S is called the **Cayley set**).
- $\mathscr{C}ay(H, S)$ has for vertices V the elements of H. And for edges (h, sh) for $h \in H$ an $s \in S$.
- $\mathscr{C}ay(H, S)$ is $|S|$-regular.
- If H is a free group on d elements S, then $\mathscr{C}ay(H, S)$ is the d-regular infinite tree.
- $\mathscr{C}ay(H, S)$ is connected $\iff$ S generates H.

(Undirected) Cayley graphs

- Let H be a group and $S \subset H$ a symmetric subset : $S^{-1} = S$. (S is called the **Cayley set**).
- $\mathscr{C}ay(H, S)$ has for vertices V the elements of H. And for edges (h, sh) for $h \in H$ an $s \in S$.
- $\mathscr{C}ay(H, S)$ is $|S|$-regular.
- If H is a free group on d elements S, then $\mathscr{C}ay(H, S)$ is the d-regular infinite tree.
- $\mathscr{C}ay(H, S)$ is connected $\iff$ S generates H.
- $G := \mathscr{C}ay(H, S)$ is undirected. Let $n := |H|$ be its order:

(Undirected) Cayley graphs

- Let H be a group and $S \subset H$ a symmetric subset : $S^{-1} = S$. (S is called the **Cayley set**).
- $\mathscr{C}ay(H, S)$ has for vertices V the elements of H. And for edges (h, sh) for $h \in H$ an $s \in S$.
- $\mathscr{C}ay(H, S)$ is $|S|$-regular.
- If H is a free group on d elements S, then $\mathscr{C}ay(H, S)$ is the d-regular infinite tree.
- $\mathscr{C}ay(H, S)$ is connected $\iff$ S generates H.
- $G := \mathscr{C}ay(H, S)$ is undirected. Let $n := |H|$ be its order:
  - adjacency matrix $A(G)$ is symmetric: its eigenvalues are denoted: $\lambda_0 \geq \lambda_1 \geq \cdots \geq \lambda_{n-1}$.

(Undirected) Cayley graphs

- Let H be a group and $S \subset H$ a symmetric subset : $S^{-1} = S$. (S is called the **Cayley set**).
- $\mathscr{C}ay(H,S)$ has for vertices V the elements of H. And for edges (h, sh) for $h \in H$ an $s \in S$.
- $\mathscr{C}ay(H,S)$ is $|S|$-regular.
- If H is a free group on d elements S, then $\mathscr{C}ay(H,S)$ is the d-regular infinite tree.
- $\mathscr{C}ay(H,S)$ is connected $\iff$ S generates H.
- $G := \mathscr{C}ay(H,S)$ is undirected. Let $n := |H|$ be its order:
    - adjacency matrix $A(G)$ is symmetric: its eigenvalues are denoted: $\lambda_0 \geq \lambda_1 \geq \cdots \geq \lambda_{n-1}$.
    - let $d = |S|$. G is d-regular: $\lambda_0 = d$.

(Undirected) Cayley graphs

- Let H be a group and $S \subset H$ a symmetric subset : $S^{-1} = S$. (S is called the **Cayley set**).
- $\mathscr{C}ay(H, S)$ has for vertices V the elements of H. And for edges (h, sh) for $h \in H$ an $s \in S$.
- $\mathscr{C}ay(H, S)$ is $|S|$-regular.
- If H is a free group on d elements S, then $\mathscr{C}ay(H, S)$ is the d-regular infinite tree.
- $\mathscr{C}ay(H, S)$ is connected $\iff$ S generates H.
- $G := \mathscr{C}ay(H, S)$ is undirected. Let $n := |H|$ be its order:
  - adjacency matrix $A(G)$ is symmetric: its eigenvalues are denoted: $\lambda_0 \geq \lambda_1 \geq \cdots \geq \lambda_{n-1}$.
  - let $d = |S|$. G is d-regular: $\lambda_0 = d$.
  - $|$connnected components of $G| =$ multiplicity of λ_0

LPS Ramanujan graphs(quaternions): regular tree

- Let A be a commutative ring with units:

$$\mathbb{H}(A) = \{\alpha = a_0 + a_1\mathrm{i} + a_2\mathrm{j} + a_3\mathrm{ij},\ a_i \in A\},$$

with $\mathrm{i}^2 = \mathrm{j}^2 = (\mathrm{ij})^2 = -1$.

LPS Ramanujan graphs(quaternions): regular tree

- Let A be a commutative ring with units:

$$\mathbb{H}(A) = \{\alpha = a_0 + a_1\mathrm{i} + a_2\mathrm{j} + a_3\mathrm{ij},\ a_i \in A\},$$

  with $\mathrm{i}^2 = \mathrm{j}^2 = (\mathrm{ij})^2 = -1$.
- Conjugate of α: $\overline{\alpha} = a_0 - a_1\mathrm{i} - a_2\mathrm{j} - a_3\mathrm{ij}$.

LPS Ramanujan graphs(quaternions): regular tree

- Let A be a commutative ring with units:

$$\mathbb{H}(A) = \{\alpha = a_0 + a_1\mathrm{i} + a_2\mathrm{j} + a_3\mathrm{ij},\ \ a_i \in A\},$$

  with $\mathrm{i}^2 = \mathrm{j}^2 = (\mathrm{ij})^2 = -1$.
- Conjugate of α: $\overline{\alpha} = a_0 - a_1\mathrm{i} - a_2\mathrm{j} - a_3\mathrm{ij}$.
- Norm of α is $N(\alpha) = \alpha\overline{\alpha} = a_0^2 + a_1^2 + a_2^2 + a_3^2$.

LPS Ramanujan graphs(quaternions): regular tree

- Let A be a commutative ring with units:

$$\mathbb{H}(A) = \{\alpha = a_0 + a_1\mathrm{i} + a_2\mathrm{j} + a_3\mathrm{ij},\ a_i \in A\},$$

with $\mathrm{i}^2 = \mathrm{j}^2 = (\mathrm{ij})^2 = -1$.

- Conjugate of α: $\overline{\alpha} = a_0 - a_1\mathrm{i} - a_2\mathrm{j} - a_3\mathrm{ij}$.
- Norm of α is $N(\alpha) = \alpha\overline{\alpha} = a_0^2 + a_1^2 + a_2^2 + a_3^2$.
- Let q be a prime $q \neq 2$,

$$\mathbb{H}(\mathbb{F}_q) \simeq \mathrm{Mat}_2(\mathbb{F}_q) \ \Rightarrow\ \mathbb{H}(\mathbb{F}_q)^\times / \mathcal{Z} \simeq PGL_2(\mathbb{F}_q).$$

LPS Ramanujan graphs(quaternions): regular tree

- Let A be a commutative ring with units:

$$\mathbb{H}(A) = \{\alpha = a_0 + a_1\mathrm{i} + a_2\mathrm{j} + a_3\mathrm{ij},\ \ a_i \in A\},$$

  with $\mathrm{i}^2 = \mathrm{j}^2 = (\mathrm{ij})^2 = -1$.
- Conjugate of α: $\overline{\alpha} = a_0 - a_1\mathrm{i} - a_2\mathrm{j} - a_3\mathrm{ij}$.
- Norm of α is $N(\alpha) = \alpha\overline{\alpha} = a_0^2 + a_1^2 + a_2^2 + a_3^2$.
- Let q be a prime $q \neq 2$,

$$\mathbb{H}(\mathbb{F}_q) \simeq \mathrm{Mat}_2(\mathbb{F}_q) \ \Rightarrow\ \mathbb{H}(\mathbb{F}_q)^\times/\mathcal{Z} \simeq PGL_2(\mathbb{F}_q).$$

- There is a "nice" family $\mathscr{P}(p) \subset \mathbb{H}(\mathbb{Z})$ of $p+1$-quaternions of norm p such that:

$\mathscr{C}ay(\langle\mathscr{P}(\mathrm{p})\rangle\ ,\ \mathscr{P}(\mathrm{p}))$ is the $p+1$-regular tree.

$p+1$ regular tree

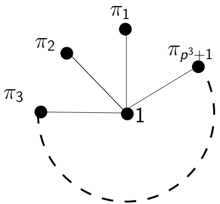
$\mathscr{C}ay(\langle \mathscr{P}(\mathrm{p}) \rangle \ , \ \mathscr{P}(\mathrm{p}))$ is the $p+1$-regular tree.

$$\mathscr{P}(p) = \{\pi_1, \ldots, \pi_{p+1}\}$$

$p+1$ regular tree

$\mathscr{C}ay(\langle\mathscr{P}(\mathrm{p})\rangle\ ,\ \mathscr{P}(\mathrm{p}))$ is the $p+1$-regular tree.

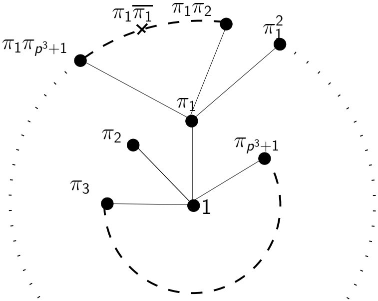
$\mathscr{P}(p) = \{\pi_1, \ldots, \pi_{p+1}\}$



$p+1$ regular tree

$\mathscr{C}ay(\langle \mathscr{P}(\mathrm{p}) \rangle \ , \mathscr{P}(\mathrm{p}))$ is the $p+1$-regular tree.

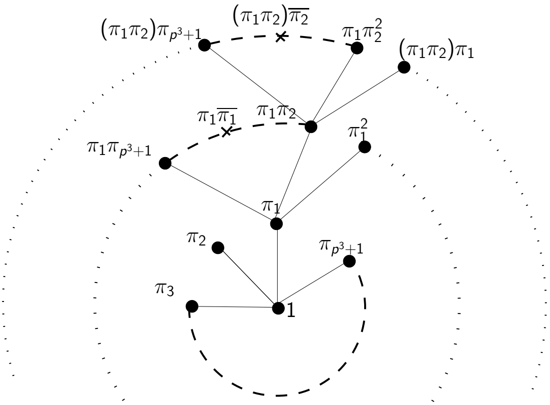
$\mathscr{P}(p) = \{\pi_1, \ldots, \pi_{p+1}\}$



$p + 1$ regular tree

$\mathscr{C}ay(\langle \mathscr{P}(\mathrm{p}) \rangle \ , \ \mathscr{P}(\mathrm{p}))$ is the $p + 1$-regular tree.

$\mathscr{P}(p) = \{\pi_1, \dots, \pi_{p+1}\}$



LPS Ramanujan graphs: finite quotient of the tree

$\mathscr{P}(p) \subset \mathbb{H}(\mathbb{Z})$ nice family of $p+1$ quaternions of norm p.
$\mathscr{C}ay(\langle \mathscr{P}(p) \rangle\ ,\ \mathscr{P}(p))$ is the $p+1$-regular infinite tree.

- Let $q > p$ be another prime.

LPS Ramanujan graphs: finite quotient of the tree

$\mathscr{P}(p) \subset \mathbb{H}(\mathbb{Z})$ nice family of $p+1$ quaternions of norm p.
$\mathscr{C}ay(\langle \mathscr{P}(p) \rangle \ , \ \mathscr{P}(p))$ is the $p+1$-regular infinite tree.

- Let $q > p$ be another prime.
- Let $\mathscr{S}(p,q) \equiv \mathscr{P}(p)$ mod q $(\mathscr{S}(p,q) \hookrightarrow \mathbb{H}(\mathbb{F}_q)^\star / \mathcal{Z} \simeq PGL_2(\mathbb{F}_q))$.

LPS Ramanujan graphs: finite quotient of the tree

$\mathscr{P}(p) \subset \mathbb{H}(\mathbb{Z})$ nice family of $p+1$ quaternions of norm p.
$\mathscr{C}ay(\langle \mathscr{P}(p) \rangle \ , \ \mathscr{P}(p))$ is the $p+1$-regular infinite tree.

- Let $q > p$ be another prime.
- Let $\mathscr{S}(p,q) \equiv \mathscr{P}(p) \bmod q$ $(\mathscr{S}(p,q) \hookrightarrow \mathbb{H}(\mathbb{F}_q)^\star / \mathcal{Z} \simeq PGL_2(\mathbb{F}_q))$.

LPS Graphs: $\boxed{\mathscr{C}ay(PGL_2(\mathbb{F}_q)\ ,\ \mathscr{S}(p,q))}$ if $\left(\frac{p}{q}\right) = -1$.
$\boxed{\mathscr{C}ay(PSL_2(\mathbb{F}_q)\ ,\ \mathscr{S}(p,q))}$ if $\left(\frac{p}{q}\right) = 1$.

LPS Ramanujan graphs: finite quotient of the tree

$\mathscr{P}(p) \subset \mathbb{H}(\mathbb{Z})$ nice family of $p+1$ quaternions of norm p.
$\mathscr{C}ay(\langle \mathscr{P}(p) \rangle \ , \ \mathscr{P}(p))$ is the $p+1$-regular infinite tree.

- Let $q > p$ be another prime.
- Let $\mathscr{S}(p,q) \equiv \mathscr{P}(p) \bmod q$
  $(\mathscr{S}(p,q) \hookrightarrow \mathbb{H}(\mathbb{F}_q)^\star / \mathcal{Z} \simeq PGL_2(\mathbb{F}_q))$.

LPS Graphs: $\boxed{\mathscr{C}ay(PGL_2(\mathbb{F}_q)\ , \ \mathscr{S}(p,q))}$ if $\left(\frac{p}{q}\right) = -1$.
$\boxed{\mathscr{C}ay(PSL_2(\mathbb{F}_q)\ , \ \mathscr{S}(p,q))}$ if $\left(\frac{p}{q}\right) = 1$.

If we fix p, then this provides infinite families of Ramanujan graphs of degree p.

LPS Ramanujan graphs: finite quotient of the tree

$\mathscr{P}(p) \subset \mathbb{H}(\mathbb{Z})$ nice family of $p+1$ quaternions of norm p.
$\mathscr{C}ay(\langle \mathscr{P}(p) \rangle\ ,\ \mathscr{P}(p))$ is the $p+1$-regular infinite tree.

- Let $q > p$ be another prime.
- Let $\mathscr{S}(p,q) \equiv \mathscr{P}(p) \bmod q$ $(\mathscr{S}(p,q) \hookrightarrow \mathbb{H}(\mathbb{F}_q)^\star/\mathcal{Z} \simeq PGL_2(\mathbb{F}_q))$.

LPS Graphs: $\boxed{\mathscr{C}ay(PGL_2(\mathbb{F}_q)\ ,\ \mathscr{S}(p,q))}$ if $\left(\frac{p}{q}\right) = -1$.

$\boxed{\mathscr{C}ay(PSL_2(\mathbb{F}_q)\ ,\ \mathscr{S}(p,q))}$ if $\left(\frac{p}{q}\right) = 1$.

If we fix p, then this provides infinite families of Ramanujan graphs of degree p.

To prove the remarkable properties: vertex-transitivity is essential

Outline of the new construction

Step 1 Infinite $p^3 + 1$-regular tree: used unique factorization of integral octonions in $\mathbb{O}(\mathbb{Z})$.

generators $\leftrightarrow$ some integral octonions $\mathscr{P}(p)$ of norm p

Outline of the new construction

Step 1 Infinite p^3+1-regular tree: used unique factorization of integral octonions in $\mathbb{O}(\mathbb{Z})$.

generators $\leftrightarrow$ some integral octonions $\mathscr{P}(p)$ of norm p

Step 2 Finite regular quotients of the tree: reduction mod q of the integral ocotnions family $\mathscr{P}(p)$.

$$\text{vertices} \leftrightarrow \mathbb{O}(\mathbb{F}_q)^\star/\text{center}$$

Outline of the new construction

Step 1 Infinite $p^3 + 1$-regular tree: used unique factorization of integral octonions in $\mathbb{O}(\mathbb{Z})$.

generators $\leftrightarrow$ some integral octonions $\mathscr{P}(p)$ of norm p

Step 2 Finite regular quotients of the tree: reduction mod q of the integral ocotnions family $\mathscr{P}(p)$.

$$\text{vertices} \leftrightarrow \mathbb{O}(\mathbb{F}_q)^\star/\text{center}$$

For each prime $p > 2$, we get an infinite family $\mathscr{X}_p = \{\mathscr{X}_{p,q}\}_{q>p}$ of degree $p^3 + 1$-regular graphs.

Generalities on octonions

Let $\mathbb{O}(R)$ a free R-module of rank 8 with basis:

$$1\,,\ \mathrm{i}\,,\ \mathrm{j}\,,\ \mathrm{k}\,,\ \mathrm{t}\,,\ \mathrm{it}\,,\ \mathrm{jt}\,,\ \mathrm{kt},$$

such that $\mathbb{O}(R) = \mathbb{H}(R) \oplus \mathbb{H}(R)\mathrm{t}$, and $\mathrm{t}^2 = -1$.

Generalities on octonions

Let $\mathbb{O}(R)$ a free R-module of rank 8 with basis:

$$1\,,\ \mathrm{i}\,,\ \mathrm{j}\,,\ \mathrm{k}\,,\ \mathrm{t}\,,\ \mathrm{it}\,,\ \mathrm{jt}\,,\ \mathrm{kt},$$

such that $\mathbb{O}(R) = \mathbb{H}(R) \oplus \mathbb{H}(R)\mathrm{t}$, and $\mathrm{t}^2 = -1$.

Conjugation: Let $a, b \in \mathbb{H}(R)$, $a + b\mathrm{t} \in \mathbb{O}(R)$. $\overline{a + b\mathrm{t}} := \overline{a} - b\mathrm{t}$

Generalities on octonions

Let $\mathbb{O}(R)$ a free R-module of rank 8 with basis:

$$1\,,\ \mathrm{i}\,,\ \mathrm{j}\,,\ \mathrm{k}\,,\ \mathrm{t}\,,\ \mathrm{it}\,,\ \mathrm{jt}\,,\ \mathrm{kt},$$

such that $\mathbb{O}(R) = \mathbb{H}(R) \oplus \mathbb{H}(R)\mathrm{t}$, and $\mathrm{t}^2 = -1$.

Conjugation: Let $a, b \in \mathbb{H}(R)$, $a + b\mathrm{t} \in \mathbb{O}(R)$. $\overline{a + b\mathrm{t}} := \overline{a} - b\mathrm{t}$

Mutliplication in $\mathbb{O}(K)$: (Cayley-Dickson doubling process)
Let $a, b, c, d \in \mathbb{H}(K)$. Then $a + b\mathrm{t}$ and $c + d\mathrm{t} \in \mathbb{O}(K)$.

$$\forall\ a, b, c, d \in \mathbb{H}(K) \quad (a + b\mathrm{t})(c + d\mathrm{t}) = (ac + \lambda \overline{d} b) + (da + b\overline{c})\mathrm{t}.$$

Generalities on octonions II

Norm: non-degenerate quadratic form : $N(x) := x\bar{x}$ on $\mathbb{O}(R)$ that extends the one of $\mathbb{H}(R)$. With our settings, $N(\mathrm{i}) = N(\mathrm{j}) = N(\mathrm{t}) = 1$.

$$N(\alpha_0 + \alpha_1 \mathrm{i} + \cdots + \alpha_7 (\mathrm{ij})\mathrm{t}) = \alpha_0^2 + \cdots + \alpha_7^2$$

Generalities on octonions II

Norm: non-degenerate quadratic form : $N(x) := x\bar{x}$ on $\mathbb{O}(R)$ that extends the one of $\mathbb{H}(R)$. With our settings, $N(\mathrm{i}) = N(\mathrm{j}) = N(\mathrm{t}) = 1$.

$$N(\alpha_0 + \alpha_1 \mathrm{i} + \cdots + \alpha_7 (\mathrm{ij})\mathrm{t}) = \alpha_0^2 + \cdots + \alpha_7^2$$

Alternative algebra: $(\alpha\alpha)\beta = \alpha(\alpha\beta)$ and $(\alpha\beta)\alpha = \alpha(\beta\alpha)$.

Generalities on octonions II

Norm: non-degenerate quadratic form : $N(x) := x\bar{x}$ on $\mathbb{O}(R)$ that extends the one of $\mathbb{H}(R)$. With our settings, $N(\mathrm{i}) = N(\mathrm{j}) = N(\mathrm{t}) = 1$.

$$N(\alpha_0 + \alpha_1 \mathrm{i} + \cdots + \alpha_7 (\mathrm{ij})\mathrm{t}) = \alpha_0^2 + \cdots + \alpha_7^2$$

Alternative algebra: $(\alpha\alpha)\beta = \alpha(\alpha\beta)$ and $(\alpha\beta)\alpha = \alpha(\beta\alpha)$.

Consequence: $\mathbb{O}(\mathbb{F}_q)^\star$ is a Moufang loop.

Generalities on octonions II

Norm: non-degenerate quadratic form : $N(x) := x\bar{x}$ on $\mathbb{O}(R)$ that extends the one of $\mathbb{H}(R)$. With our settings, $N(\mathrm{i}) = N(\mathrm{j}) = N(\mathrm{t}) = 1$.

$$N(\alpha_0 + \alpha_1 \mathrm{i} + \cdots + \alpha_7 (\mathrm{ij})\mathrm{t}) = \alpha_0^2 + \cdots + \alpha_7^2$$

Alternative algebra: $(\alpha\alpha)\beta = \alpha(\alpha\beta)$ and $(\alpha\beta)\alpha = \alpha(\beta\alpha)$.

Consequence: $\mathbb{O}(\mathbb{F}_q)^\star$ is a Moufang loop.

Consequence: Two elements generate an associative subalgebra:

$$(\alpha\beta)\bar{\beta} = \alpha(\beta\bar{\beta}) = \alpha N(\beta)$$

Generalities on octonions II

Norm: non-degenerate quadratic form : $N(x) := x\bar{x}$ on $\mathbb{O}(R)$ that extends the one of $\mathbb{H}(R)$. With our settings,
$N(\mathrm{i}) = N(\mathrm{j}) = N(\mathrm{t}) = 1$.

$$N(\alpha_0 + \alpha_1 \mathrm{i} + \cdots + \alpha_7 (\mathrm{ij})\mathrm{t}) = \alpha_0^2 + \cdots + \alpha_7^2$$

Alternative algebra: $(\alpha\alpha)\beta = \alpha(\alpha\beta)$ and $(\alpha\beta)\alpha = \alpha(\beta\alpha)$.

Consequence: $\mathbb{O}(\mathbb{F}_q)^\star$ is a Moufang loop.

Consequence: Two elements generate an associative subalgebra:

$$(\alpha\beta)\bar{\beta} = \alpha(\beta\bar{\beta}) = \alpha N(\beta)$$

Multiplicativity of the norm: $N(\alpha\beta) = N(\alpha)N(\beta)$

The unique factorization problem

Rational integers $\mathbb{Z}$: $x = \pm p_1^{e_1} \cdots p_s^{e_s}$
The sequence order $[p_1, \cdots, p_s]$ does not matter.

The unique factorization problem

Rational integers $\mathbb{Z}$: $x = \pm p_1^{e_1} \cdots p_s^{e_s}$
The sequence order $[p_1, \cdots, p_s]$ does not matter.

Gauss integers $\mathbb{Z}[i]$: $x = \pm \epsilon \pi_1^{e_1} \cdots \pi_s^{e_s}$ $\epsilon = 1$ or i.
The sequence order $[\pi_1, \cdots, \pi_s]$ does not matter.

The unique factorization problem

Rational integers $\mathbb{Z}$: $x = \pm p_1^{e_1} \cdots p_s^{e_s}$
The sequence order $[p_1, \cdots, p_s]$ does not matter.

Gauss integers $\mathbb{Z}[i]$: $x = \pm \epsilon \pi_1^{e_1} \cdots \pi_s^{e_s}$ $\epsilon = 1$ or i.
The sequence order $[\pi_1, \cdots, \pi_s]$ does not matter.

Quaternions $\mathbb{H}(\mathbb{Z})$: $\alpha = \alpha_0 + \alpha_1 \mathrm{i} + \alpha_2 \mathrm{j} + \alpha_3 \mathrm{k} \in \mathbb{H}(\mathbb{Z})$,
$\gcd(\alpha_0, \alpha_1, \alpha_2, \alpha_3) = 1$.
$N(\alpha) = p_1 \cdots p_s$ ($p_i \equiv 1 \bmod 4$, primes not necessarily disctinct).

Existence: There exists $\pi_i \in \mathbb{H}(\mathbb{Z})$, $N(\pi_i) = p_i$, such that:
$\alpha = \pi_1 \cdots \pi_s$.

The unique factorization problem

Rational integers $\mathbb{Z}$: $x = \pm p_1^{e_1} \cdots p_s^{e_s}$
The sequence order $[p_1, \cdots, p_s]$ does not matter.

Gauss integers $\mathbb{Z}[i]$: $x = \pm \epsilon \pi_1^{e_1} \cdots \pi_s^{e_s}$ $\quad\quad$ $\epsilon = 1$ or i.
The sequence order $[\pi_1, \cdots, \pi_s]$ does not matter.

Quaternions $\mathbb{H}(\mathbb{Z})$: $\alpha = \alpha_0 + \alpha_1 \mathrm{i} + \alpha_2 \mathrm{j} + \alpha_3 \mathrm{k} \in \mathbb{H}(\mathbb{Z})$,
$\gcd(\alpha_0, \alpha_1, \alpha_2, \alpha_3) = 1$.
$N(\alpha) = p_1 \cdots p_s$ ($p_i \equiv 1 \bmod 4$, primes not necessarily disctinct).

Existence: There exists $\pi_i \in \mathbb{H}(\mathbb{Z})$, $N(\pi_i) = p_i$, such that:
$\alpha = \pi_1 \cdots \pi_s$.

Uniqueness ? Impose that $\pi_{i,0} > 0$ and that $\pi_{i,0}$ is odd.
There exists a unique $\epsilon \in \mathbb{H}(\mathbb{Z})^\star = \{\pm 1, \pm \mathrm{i}, \pm \mathrm{j}, \pm \mathrm{ij}\}$,

$$\alpha = \epsilon \pi_1 \cdots \pi_s.$$

The sequence order $[\pi_1, \ldots, \pi_s]$ matters.

The unique factorization problem for octonions

1st step: Euclidean division: Given $\alpha, \beta \in \mathbb{O}(\mathbb{Z})$, $N(\alpha) > N(\beta)$, find $\gamma, \delta \in \mathbb{O}(\mathbb{Z})$ such that:

$$\alpha = \gamma\beta + \delta, \qquad N(\delta) < N(\beta).$$

Equivalently: Given $v \in \mathbb{Q}^8$, is there $w \in \mathbb{Z}^8$ such that $||v - w||_2 < 1$.

Not clear because $||(\frac{1}{2}, \cdots, \frac{1}{2})||_2 = \sqrt{2}$.

The unique factorization problem for octonions

1st step: Euclidean division: Given $\alpha, \beta \in \mathbb{O}(\mathbb{Z})$, $N(\alpha) > N(\beta)$, find $\gamma, \delta \in \mathbb{O}(\mathbb{Z})$ such that:

$$\alpha = \gamma\beta + \delta, \qquad N(\delta) < N(\beta).$$

Equivalently: Given $v \in \mathbb{Q}^8$, is there $w \in \mathbb{Z}^8$ such that $||v - w||_2 < 1$.

Not clear because $||(\frac{1}{2}, \cdots, \frac{1}{2})||_2 = \sqrt{2}$.

Does not work because $\mathbb{O}(\mathbb{Z})$ is not a maximal "order" (in analogy with algebraic integers: $\mathbb{Z}[\alpha] \subset \mathcal{O}_K$, where $K = \mathbb{Q}(\alpha)$).

Integral octonions

Characteristic equation: $\forall \alpha \in \mathbb{O}(K)$, holds:

$$X^2 - (\alpha + \bar{\alpha})X + N(\alpha) \equiv 0 \qquad \text{in} \qquad K[X]$$

Integral octonions: Given $K = \mathbb{Q}$, in analogy with algebraic integers: $N(\alpha) \in \mathbb{Z}$ and if $\alpha + \bar{\alpha} \in \mathbb{Z}$

Integral octonions

Characteristic equation: $\forall \alpha \in \mathbb{O}(K)$, holds:

$$X^2 - (\alpha + \bar{\alpha})X + N(\alpha) \equiv 0 \qquad \text{in} \qquad K[X]$$

Integral octonions: Given $K = \mathbb{Q}$, in analogy with algebraic integers: $N(\alpha) \in \mathbb{Z}$ and if $\alpha + \bar{\alpha} \in \mathbb{Z}$

New difficulty: The integral octonions is a $\mathbb{Z}$-algebra of $\mathbb{O}(\mathbb{Q})$, **but** is not a lattice (no $\mathbb{Z}$-basis).

Integral octonions

Characteristic equation: $\forall \alpha \in \mathbb{O}(K)$, holds:

$$X^2 - (\alpha + \bar{\alpha})X + N(\alpha) \equiv 0 \qquad \text{in} \qquad K[X]$$

Integral octonions: Given $K = \mathbb{Q}$, in analogy with algebraic integers: $N(\alpha) \in \mathbb{Z}$ and if $\alpha + \bar{\alpha} \in \mathbb{Z}$

New difficulty: The integral octonions is a $\mathbb{Z}$-algebra of $\mathbb{O}(\mathbb{Q})$, **but is not a lattice** (no $\mathbb{Z}$-basis).

Coxeter, 1946 The integral octonions contains 7 distinct sub-algebras that are also maximal orders (lattices).

The 7 associative triads: Let k := ij. Each of the following 7 triplets generate a quaternion sub-algebra.

k, jt, it , j, it, kt , i, kt, jt , i, j, k , i, t, it , j, t, jt , k, t, kt

Coxeter algebra (E_8 lattice)

Coxeter's algebra $\mathcal{C}_{\mathbb{O}}$: This is one of the 7 maximal orders, associated to the associative triplet $\mathrm{i}, \mathrm{j}, \mathrm{k}$:

$$\mathrm{h} := \frac{1}{2}(\mathrm{i}+\mathrm{j}+\mathrm{k}+\mathrm{t}), \quad \mathcal{C}_{\mathbb{O}} := \mathbb{Z}+\mathrm{i}\mathbb{Z}+\mathrm{j}\mathbb{Z}+\mathrm{k}\mathbb{Z}+\mathrm{h}\mathbb{Z}+\mathrm{ih}\mathbb{Z}+\mathrm{jh}\mathbb{Z}+\mathrm{kh}\mathbb{Z}.$$

Coxeter algebra (E_8 lattice)

Coxeter's algebra $\mathcal{C}_{\mathbb{O}}$: This is one of the 7 maximal orders, associated to the associative triplet $\mathrm{i}, \mathrm{j}, \mathrm{k}$:

$$\mathrm{h} := \frac{1}{2}(\mathrm{i}+\mathrm{j}+\mathrm{k}+\mathrm{t}), \quad \mathcal{C}_{\mathbb{O}} := \mathbb{Z}+\mathrm{i}\mathbb{Z}+\mathrm{j}\mathbb{Z}+\mathrm{k}\mathbb{Z}+\mathrm{h}\mathbb{Z}+\mathrm{ih}\mathbb{Z}+\mathrm{jh}\mathbb{Z}+\mathrm{kh}\mathbb{Z}.$$

Theorem. In $\mathcal{C}_{\mathbb{O}}$, the Euclidean division holds.

No associativity $\Rightarrow$ No induction possible to deduce existence of a factorization.

Coxeter algebra (E_8 lattice)

Coxeter's algebra $\mathcal{C}_{\mathbb{O}}$: This is one of the 7 maximal orders, associated to the associative triplet $\mathrm{i}, \mathrm{j}, \mathrm{k}$:

$$\mathrm{h} := \frac{1}{2}(\mathrm{i}+\mathrm{j}+\mathrm{k}+\mathrm{t}), \quad \mathcal{C}_{\mathbb{O}} := \mathbb{Z}+\mathrm{i}\mathbb{Z}+\mathrm{j}\mathbb{Z}+\mathrm{k}\mathbb{Z}+\mathrm{h}\mathbb{Z}+\mathrm{ih}\mathbb{Z}+\mathrm{jh}\mathbb{Z}+\mathrm{kh}\mathbb{Z}.$$

Theorem. In $\mathcal{C}_{\mathbb{O}}$, the Euclidean division holds.

No associativity $\Rightarrow$ No induction possible to deduce existence of a factorization.

Rehm (1993) Deduce a distortion of the Euclidean algorithm.
Existence of factorization.
Uniqueness of factorization: counting argument

Unique factorization: H. P. Rehm (1993)

Special case: $\alpha \in \mathbb{O}(\mathbb{Z})$, $N(\alpha) = p^k$, $p \equiv 1 \bmod 8$.

$$\alpha = \alpha_0 + \alpha_1 \mathrm{i} + \alpha_2 \mathrm{j} + \alpha_3 \mathrm{k} + \alpha_4 \mathrm{t} + \alpha_5 \mathrm{it} + \alpha_6 \mathrm{jt} + \alpha_7 \mathrm{kt}$$

α is primitive $\Leftrightarrow \gcd(\alpha_0, \ldots, \alpha_7) = 1$.

Existence: there are prime octonions $\pi_1, \ldots, \pi_k$, $N(\pi_i) = p$, such that:

$$\alpha = (\cdots(\pi_1\pi_2)\ldots)\pi_k.$$

Unique factorization: H. P. Rehm (1993)

Special case: $\alpha \in \mathbb{O}(\mathbb{Z})$, $N(\alpha) = p^k$, $p \equiv 1 \bmod 8$.

$$\alpha = \alpha_0 + \alpha_1 \mathrm{i} + \alpha_2 \mathrm{j} + \alpha_3 \mathrm{k} + \alpha_4 \mathrm{t} + \alpha_5 \mathrm{it} + \alpha_6 \mathrm{jt} + \alpha_7 \mathrm{kt}$$

α is primitive $\Leftrightarrow \gcd(\alpha_0, \ldots, \alpha_7) = 1$.

Existence: there are prime octonions $\pi_1, \ldots, \pi_k$, $N(\pi_i) = p$, such that:

$$\alpha = (\cdots(\pi_1\pi_2)\ldots)\pi_k.$$

Uniqueness: Restrict the set of octonions of norm p to:

$$\mathscr{P}(p) := \{\alpha \in \mathbb{O}(\mathbb{Z}) \ : \ N(\alpha) = p \ , \alpha_0 \text{ is odd } \ , \ \alpha_0 > 0\}$$

There exists a unique sequence $[\mu_1, \ldots, \mu_k]$ in $\mathscr{P}(p)$ such that :

$$\alpha = \pm(\cdots(\mu_1\mu_2)\ldots)\mu_k \qquad (\mu_{i+1} \neq \overline{\mu_i})$$

$p^3 + 1$-regular infinite tree T_p

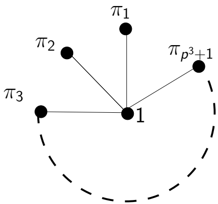
$\mathscr{C}ay(\langle \mathscr{P}(\mathrm{p}) \rangle \ , \ \mathscr{P}(\mathrm{p}))$ is the $p^3 + 1$-regular inifinite tree.

$\mathscr{P}(p) = \{\pi_1, \ldots, \pi_{p^3+1}\}$

$p^3 + 1$-regular infinite tree T_p

$\mathscr{C}ay(\langle \mathscr{P}(\mathrm{p}) \rangle\ ,\ \mathscr{P}(\mathrm{p}))$ is the $p^3 + 1$-regular inifinite tree.

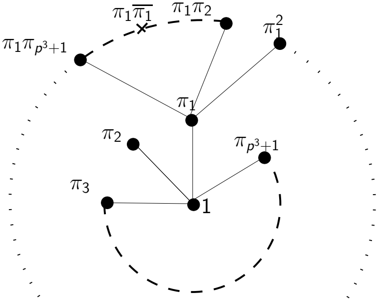
$\mathscr{P}(p) = \{\pi_1, \ldots, \pi_{p^3+1}\}$



$p^3 + 1$-regular infinite tree T_p

$\mathscr{C}ay(\langle \mathscr{P}(\mathrm{p}) \rangle\ ,\ \mathscr{P}(\mathrm{p}))$ is the $p^3 + 1$-regular inifinite tree.

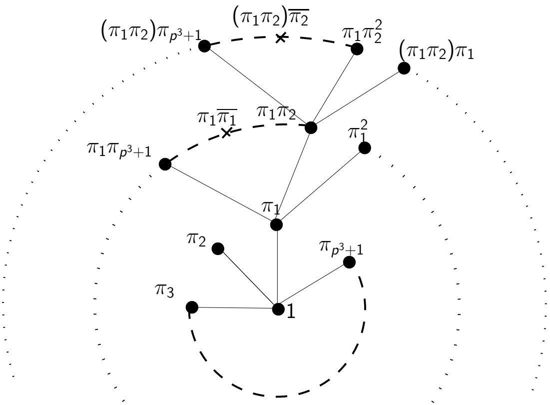
$\mathscr{P}(p) = \{\pi_1, \ldots, \pi_{p^3+1}\}$



p^3+1-regular infinite tree T_p

$\mathscr{C}ay(\langle\mathscr{P}(\mathrm{p})\rangle\ ,\ \mathscr{P}(\mathrm{p}))$ is the p^3+1-regular inifinite tree.

$\mathscr{P}(p)=\{\pi_1,\dots,\pi_{p^3+1}\}$



$p^3 + 1$-regular infinite tree T_p

$$\mathscr{P}(p) := \{\alpha \in \mathbb{O}(\mathbb{Z}) \ : \ N(\alpha) = p \ , \alpha_0 \text{ is odd } \ , \ \alpha_0 > 0\}$$

$\mathscr{P}(p) := \{\pi_1, \pi_2, \ldots, \pi_{p^3+1}\}$

Stable by conjugation: For $\pi_i \in \mathscr{P}(p)$, the conjugate $\overline{\pi_i} = \pi_{i'} \in \mathscr{P}(p)$

Alternative algebra rules ... $(\alpha\beta)\bar{\beta} = \alpha(\beta\bar{\beta}) = \alpha N(\beta)$

This implies that for $\ell \neq i, i'$, $(\pi_\ell \pi_i)\overline{\pi_i} = p\pi_\ell$ is not primitive.

...in the unique factorization: α primitive in $\mathbb{O}(\mathbb{Z})$, $N(\alpha) = p^k$:

$$\alpha = \pm(\cdots(\mu_1\mu_2)\ldots)\mu_k, \quad \mu_i \in \mathscr{P}(p) \qquad \textbf{with} \qquad \mu_i \neq \overline{\mu_{i+1}}.$$

$p^3 + 1$-regular infinite tree T_p

$$\mathscr{P}(p) := \{\alpha \in \mathbb{O}(\mathbb{Z}) \ : \ N(\alpha) = p \ , \alpha_0 \text{ is odd } \ , \ \alpha_0 > 0\}$$

$\mathscr{P}(p) := \{\pi_1, \pi_2, \ldots, \pi_{p^3+1}\}$

Stable by conjugation: For $\pi_i \in \mathscr{P}(p)$, the conjugate $\overline{\pi_i} = \pi_{i'} \in \mathscr{P}(p)$

Alternative algebra rules . . . $(\alpha\beta)\bar{\beta} = \alpha(\beta\bar{\beta}) = \alpha N(\beta)$

This implies that for $\ell \neq i, i'$, $(\pi_\ell \pi_i)\overline{\pi_i} = p\pi_\ell$ is not primitive.

. . . in the unique factorization: α primitive in $\mathbb{O}(\mathbb{Z})$, $N(\alpha) = p^k$:

$$\alpha = \pm(\cdots(\mu_1\mu_2)\ldots)\mu_k, \quad \mu_i \in \mathscr{P}(p) \qquad \textbf{with} \qquad \mu_i \neq \overline{\mu_{i+1}}.$$

Walking on the tree: vertice $v \leftrightarrow \alpha = (\cdots(\pi_{i_1}\pi_{i_2})\ldots)\pi_{i_s}$, with $\pi_{i_\ell} \neq \overline{\pi_{i_\ell}}$.

Go forward (from the root) at v: right multiply α by $\pi \in \mathscr{P}(p) - \{\overline{\pi_{i_s}}\}$.

Go backward (from the root) at v: right multiply α by $\overline{\pi_{i_s}}$.

Finite regular quotients of the tree

$$\tau_q : \mathbb{O}(\mathbb{Z}) \to \mathbb{O}(\mathbb{F}_q)$$

Equivalence relation on the vertices: $v_1, v_2 \in V(T_p)$

$$v_1 \leftrightarrow \alpha_1 = (\cdots(\pi_{i_1}\pi_{i_2})\pi_{i_3}\cdots)\pi_{i_s} \qquad \text{with } \pi_{i_k} \neq \overline{\pi_{i_{k-1}}}.$$

$$v_2 \leftrightarrow \alpha_2 = (\cdots(\pi_{j_1}\pi_{j_2})\pi_{j_3}\cdots)\pi_{j_t} \qquad \text{with } \pi_{j_k} \neq \overline{\pi_{j_{k-1}}}.$$

$$v_1 \sim v_2 \iff \tau_q(\alpha_1) = \lambda\tau_q(\alpha_2) \text{ for some } \lambda \in \mathbb{F}_q^\star.$$

Finite regular quotients of the tree

$$\tau_q : \mathbb{O}(\mathbb{Z}) \to \mathbb{O}(\mathbb{F}_q)$$

Equivalence relation on the vertices: $v_1, v_2 \in V(T_p)$

$v_1 \leftrightarrow \alpha_1 = (\cdots(\pi_{i_1}\pi_{i_2})\pi_{i_3}\cdots)\pi_{i_s}$ with $\pi_{i_k} \neq \overline{\pi_{i_{k-1}}}$.

$v_2 \leftrightarrow \alpha_2 = (\cdots(\pi_{j_1}\pi_{j_2})\pi_{j_3}\cdots)\pi_{j_t}$ with $\pi_{j_k} \neq \overline{\pi_{j_{k-1}}}$.

$v_1 \sim v_2 \iff \tau_q(\alpha_1) = \lambda\tau_q(\alpha_2)$ for some $\lambda \in \mathbb{F}_q^\star$.

$\iff \tau_q(\alpha_1) \equiv \tau_q(\alpha_2)$ in $\mathbb{O}(\mathbb{F}_q)^\star/\mathcal{Z}$,

where $\mathcal{Z} = \{x \mid xy = yx,\ \forall y \in \mathbb{O}(\mathbb{F}_q)^\star\} \simeq \mathbb{F}_q^\star$ is the center of $\mathbb{O}(\mathbb{F}_q)^\star$.

Finite regular quotients of the tree

$$\tau_q : \mathbb{O}(\mathbb{Z}) \to \mathbb{O}(\mathbb{F}_q)$$

Equivalence relation on the vertices: $v_1, v_2 \in V(T_p)$

$v_1 \leftrightarrow \alpha_1 = (\cdots(\pi_{i_1}\pi_{i_2})\pi_{i_3}\cdots)\pi_{i_s}$ with $\pi_{i_k} \neq \overline{\pi_{i_{k-1}}}$.

$v_2 \leftrightarrow \alpha_2 = (\cdots(\pi_{j_1}\pi_{j_2})\pi_{j_3}\cdots)\pi_{j_t}$ with $\pi_{j_k} \neq \overline{\pi_{j_{k-1}}}$.

$v_1 \sim v_2 \iff \tau_q(\alpha_1) = \lambda\tau_q(\alpha_2)$ for some $\lambda \in \mathbb{F}_q^\star$.

$\iff \tau_q(\alpha_1) \equiv \tau_q(\alpha_2)$ in $\mathbb{O}(\mathbb{F}_q)^\star/\mathcal{Z}$,

where $\mathcal{Z} = \{x \mid xy = yx, \ \forall y \in \mathbb{O}(\mathbb{F}_q)^\star\} \simeq \mathbb{F}_q^\star$

is the center of $\mathbb{O}(\mathbb{F}_q)^\star$.

Theorem: The relation $\sim$ preserves the adjacency.

$\mathscr{X}_{p,q} := T_p/\sim$, finite p^3+1-regular quotient of T_p.

Algebraic interpretation in terms of Cayley graphs

$$\tau_q : \mathbb{O}(\mathbb{Z}) \to \mathbb{O}(\mathbb{F}_q) \qquad p \equiv 1 \bmod 8 \quad \text{and} \quad \left(\frac{p}{q}\right) = -1$$

Definition: Let

$$\Lambda := \{\alpha \in \mathbb{O}(\mathbb{Z}),\ \text{s.t. } \alpha = (\cdots(\pi_{i_1}\pi_{i_2})\ldots)\pi_{i_s}, \text{with } \pi_{i_{\ell-1}} \neq \overline{\pi_{i_\ell}}\}.$$

Algebraic interpretation in terms of Cayley graphs

$$\tau_q : \mathbb{O}(\mathbb{Z}) \to \mathbb{O}(\mathbb{F}_q) \qquad p \equiv 1 \bmod 8 \quad \text{and} \quad \left(\frac{p}{q}\right) = -1$$

Definition: Let

$\Lambda := \{\alpha \in \mathbb{O}(\mathbb{Z}),\ \text{s.t. } \alpha = (\cdots(\pi_{i_1}\pi_{i_2})\ldots)\pi_{i_s}, \text{with } \pi_{i_{\ell-1}} \neq \overline{\pi_{i_\ell}}\}.$

- $\Lambda \longleftrightarrow V(T_p)$.

Algebraic interpretation in terms of Cayley graphs

$$\tau_q : \mathbb{O}(\mathbb{Z}) \to \mathbb{O}(\mathbb{F}_q) \qquad p \equiv 1 \bmod 8 \quad \text{and} \quad \left(\frac{p}{q}\right) = -1$$

Definition: Let

$\Lambda := \{\alpha \in \mathbb{O}(\mathbb{Z}),$ s.t. $\alpha = (\cdots(\pi_{i_1}\pi_{i_2})\ldots)\pi_{i_s}$, with $\pi_{i_{\ell-1}} \neq \overline{\pi_{i_\ell}}\}$.

- $\Lambda \longleftrightarrow V(T_p)$.
- $\Lambda := \{\alpha \in \mathbb{O}(\mathbb{Z}) \mid \alpha$ is primitive, $N(\alpha) = p^k$ and $\alpha_0 > 0\}$

Algebraic interpretation in terms of Cayley graphs

$$\tau_q : \mathbb{O}(\mathbb{Z}) \to \mathbb{O}(\mathbb{F}_q) \qquad p \equiv 1 \bmod 8 \quad \text{and} \quad \left(\frac{p}{q}\right) = -1$$

Definition: Let

$\Lambda := \{\alpha \in \mathbb{O}(\mathbb{Z}),$ s.t. $\alpha = (\cdots(\pi_{i_1}\pi_{i_2})\ldots)\pi_{i_s},$ with $\pi_{i_{\ell-1}} \neq \overline{\pi_{i_\ell}}\}$.

- $\Lambda \longleftrightarrow V(T_p)$.
- $\Lambda := \{\alpha \in \mathbb{O}(\mathbb{Z}) \mid \alpha$ is primitive, $N(\alpha) = p^k$ and $\alpha_0 > 0\}$
- $\tau_q(\Lambda) \subset \mathbb{O}(\mathbb{F}_q)^\star$.

Algebraic interpretation in terms of Cayley graphs

$$\tau_q : \mathbb{O}(\mathbb{Z}) \to \mathbb{O}(\mathbb{F}_q) \qquad p \equiv 1 \bmod 8 \quad \text{and} \quad \left(\frac{p}{q}\right) = -1$$

Definition: Let

$\Lambda := \{\alpha \in \mathbb{O}(\mathbb{Z}),$ s.t. $\alpha = (\cdots(\pi_{i_1}\pi_{i_2})\ldots)\pi_{i_s}$, with $\pi_{i_{\ell-1}} \neq \overline{\pi_{i_\ell}}\}$.

- $\Lambda \longleftrightarrow V(T_p)$.
- $\Lambda := \{\alpha \in \mathbb{O}(\mathbb{Z}) \mid \alpha$ is primitive, $N(\alpha) = p^k$ and $\alpha_0 > 0\}$
- $\tau_q(\Lambda) \subset \mathbb{O}(\mathbb{F}_q)^\star$.
- Defining $\mathcal{Z}$ as the center of $\mathbb{O}(\mathbb{F}_q)^\star$,

$$\mu_q : \Lambda \to \mathbb{O}(\mathbb{F}_q)^\star/\mathcal{Z} \qquad \text{is onto.}$$

Algebraic interpretation in terms of Cayley graphs

$$\tau_q : \mathbb{O}(\mathbb{Z}) \to \mathbb{O}(\mathbb{F}_q) \qquad p \equiv 1 \bmod 8 \quad \text{and} \quad \left(\frac{p}{q}\right) = -1$$

Definition: Let

$\Lambda := \{\alpha \in \mathbb{O}(\mathbb{Z}),$ s.t. $\alpha = (\cdots(\pi_{i_1}\pi_{i_2})\ldots)\pi_{i_s},$ with $\pi_{i_{\ell-1}} \neq \overline{\pi_{i_\ell}}\}$.

- $\Lambda \longleftrightarrow V(T_p)$.
- $\Lambda := \{\alpha \in \mathbb{O}(\mathbb{Z}) \mid \alpha$ is primitive, $N(\alpha) = p^k$ and $\alpha_0 > 0\}$
- $\tau_q(\Lambda) \subset \mathbb{O}(\mathbb{F}_q)^\star$.
- Defining $\mathcal{Z}$ as the center of $\mathbb{O}(\mathbb{F}_q)^\star$,

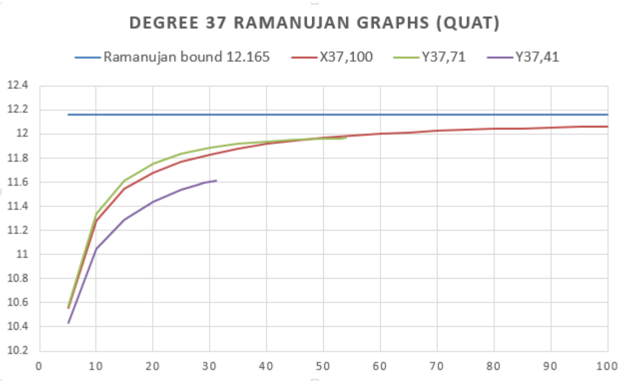
$$\mu_q : \Lambda \to \mathbb{O}(\mathbb{F}_q)^\star/\mathcal{Z} \qquad \text{is onto.}$$

Let $\mathscr{S}(p,q) := \mu_q(\mathscr{P}(p))$, $\mathscr{X}_{p,q} = \mathscr{C}ay(\ \mathbb{O}(\mathbb{F}_q)^\star/\mathcal{Z}\ ,\ \mathscr{S}(p,q)\ )$

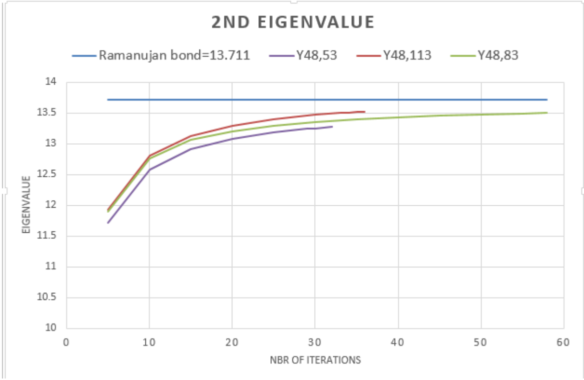
Some Numerical Experiments

- Implementation in Magma. $\leftarrow$ More than 2000 lines of codes.
- Computation of λ_1 the 2nd largest eigenvalue: Power Method.
- Computation of the girth: classical breadth-first search in the "mother" $p^3 + 1$-regular tree, until a "collision" is found when reducing mod q.

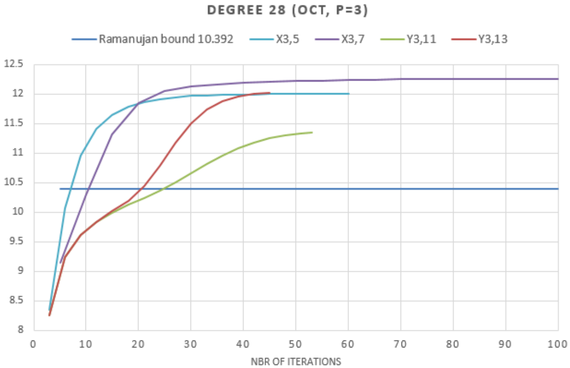
Results: 2nd eigenvalue for various degree 38 LPS graphs



Results: 2nd eigenvalue for various degree 48 LPS graphs



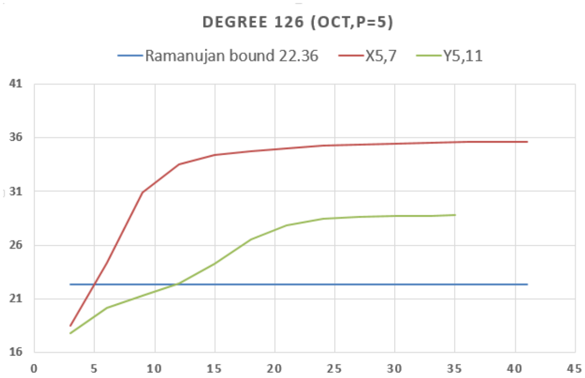
Results: 2nd eigenvalue for smallest degree 28 octo. graphs



31,373,160 vertices $Y_{3,13}$ required 24Go and 5h40 (one iteration 450s)

Failed for 410,333,760 vertices graph $X_{3,17}$ (after 30Go and 59hurs)

Results: 2nd eigenvalue for smallest degree 126 octo. graphs



$Y_{5,11}$ has 9,742,920 vertices. Required 11Go and 10hours (500s by iterations).

Implementation in MAGMA

Representation of Moufang loops $\mathbb{O}(\mathbb{F}_q)^\times/\mathcal{Z}$ (and of $\mathbb{H}(\mathbb{F}_q)^\star/\mathcal{Z}$)

- Construction of the doubling Cayley Dickson porocess $(\mathbb{R} \to \mathbb{C} \to \mathbb{H} \to \mathbb{O} \to \cdots)$ to generate automatically the multiplication tables on free modules of rank $2, 4, 8, \ldots$.

Implementation in MAGMA

Representation of Moufang loops $\mathbb{O}(\mathbb{F}_q)^\times/\mathcal{Z}$ (and of $\mathbb{H}(\mathbb{F}_q)^\star/\mathcal{Z}$)

- Construction of the doubling Cayley Dickson porocess $(\mathbb{R} \to \mathbb{C} \to \mathbb{H} \to \mathbb{O} \to \cdots)$ to generate automatically the multiplication tables on free modules of rank $2, 4, 8, \ldots$.
- Coefficients ring can be changed from $\mathbb{Z}$ to $\mathbb{F}_p$ using `ChangeRing`.

Implementation in MAGMA

Representation of Moufang loops $\mathbb{O}(\mathbb{F}_q)^\times/\mathcal{Z}$ (and of $\mathbb{H}(\mathbb{F}_q)^\star/\mathcal{Z}$)

- Construction of the doubling Cayley Dickson porocess $(\mathbb{R} \to \mathbb{C} \to \mathbb{H} \to \mathbb{O} \to \cdots)$ to generate automatically the multiplication tables on free modules of rank $2, 4, 8, \ldots$.
- Coefficients ring can be changed from $\mathbb{Z}$ to $\mathbb{F}_p$ using `ChangeRing`.
- Use a "normal form" to represent quater/octo-nions in $\mathbb{H}(\mathbb{F}_q)^\times/\mathcal{Z}$ or $\mathbb{O}(\mathbb{F}_q)^\times/\mathcal{Z}$:

$$\mathbf{a} = (\alpha_0, \ldots, \alpha_7) \xrightarrow{\textit{Normal form}} \alpha_{\textit{first}}^{-1}\mathbf{a},$$

where $\alpha_{\textit{first}}$ is the first coordinate $\neq 0$.

Power method

Aim: Approximate largest eigenvalues of (symmetric) matrices.

$$\text{If } x_0 \notin E_{\lambda_0}, \qquad \lim_{\ell\to\infty} \frac{\|A^\ell x_0\|_2}{\|A^{\ell-1} x_0\|_2} = |\lambda_0|,$$

Power method

Aim: Approximate largest eigenvalues of (symmetric) matrices.

$$\text{If } x_0 \notin E_{\lambda_0}, \qquad \lim_{\ell\to\infty} \frac{\|A^\ell x_0\|_2}{\|A^{\ell-1}x_0\|_2} = |\lambda_0|,$$

- Now we know that $\lambda_0 = d$ and $E_{\lambda_0} = \langle (1, \ldots, 1)^t \rangle$.

Power method

Aim: Approximate largest eigenvalues of (symmetric) matrices.

$$\text{If } x_0 \notin E_{\lambda_0}, \qquad \lim_{\ell\to\infty} \frac{\|A^\ell x_0\|_2}{\|A^{\ell-1} x_0\|_2} = |\lambda_0|,$$

- Now we know that $\lambda_0 = d$ and $E_{\lambda_0} = \langle (1, \dots, 1)^t \rangle$.
- Choose randomly $x_0 \in E_{\lambda_0}^\perp$ (easy). With high probability $x_0 \notin E_{\lambda_1}$ also, so

$$\lim_{\ell\to\infty} \frac{\|A^\ell x_0\|_2}{\|A^{\ell-1} x_0\|_2} = |\lambda_1|,$$

Power method

Aim: Approximate largest eigenvalues of (symmetric) matrices.

$$\text{If } x_0 \notin E_{\lambda_0}, \qquad \lim_{\ell\to\infty} \frac{\|A^\ell x_0\|_2}{\|A^{\ell-1}x_0\|_2} = |\lambda_0|,$$

- Now we know that $\lambda_0 = d$ and $E_{\lambda_0} = \langle (1,\dots,1)^t \rangle$.
- Choose randomly $x_0 \in E_{\lambda_0}^{\perp}$ (easy). With high probability $x_0 \notin E_{\lambda_1}$ also, so

$$\lim_{\ell\to\infty} \frac{\|A^\ell x_0\|_2}{\|A^{\ell-1}x_0\|_2} = |\lambda_1|,$$

- It suffices to compute successively $Ax_0,\ A^2x_0, \cdots, A^\ell x_0, \dots$.

Power method

Aim: Approximate largest eigenvalues of (symmetric) matrices.

$$\text{If } x_0 \notin E_{\lambda_0}, \qquad \lim_{\ell\to\infty} \frac{\|A^\ell x_0\|_2}{\|A^{\ell-1} x_0\|_2} = |\lambda_0|,$$

- Now we know that $\lambda_0 = d$ and $E_{\lambda_0} = \langle (1, \ldots, 1)^t \rangle$.
- Choose randomly $x_0 \in E_{\lambda_0}^{\perp}$ (easy). With high probability $x_0 \notin E_{\lambda_1}$ also, so

$$\lim_{\ell\to\infty} \frac{\|A^\ell x_0\|_2}{\|A^{\ell-1} x_0\|_2} = |\lambda_1|,$$

- It suffices to compute successively $Ax_0,\ A^2x_0, \cdots, A^\ell x_0, \ldots$.
- The product Ay can be done in case of Cayley graphs: $O(nd) = \tilde{O}(n)$ (if all elements are pre-computed and stored in an array).

Perspective

- Uneveness of the girth: *separate .pdf file*

Perspective

- Uneveness of the girth: *separate .pdf file*
- MAGMA has some functionalities to compute automorphisms. Unlikley to work on large graphs, but is it possible to use these to guess at least some automorphism on smallest octonion graphs ?

Perspective

- Uneveness of the girth: *separate .pdf file*
- MAGMA has some functionalities to compute automorphisms. Unlikley to work on large graphs, but is it possible to use these to guess at least some automorphism on smallest octonion graphs ?
- THANK YOU FOR YOUR ATTENTION ! COMMENTS?

file:///C:/Program_Files_(x86)/Magma/htmlhelp/text1804.htm