On the computation of the second largest eigenvalue and of the girth of Cayley graphs based on octonions and quaternions

X. Dahan

xdahan@gmail.com

February 9, 2018

Abstract

The original motivation of this work is to compute the 2^{nd} largest eigenvalue and the girth (and more generally the shortest cycle at any vertex) of new families of Cayley graphs based on octonions. This new construction is modeled after the famous Ramanujan graphs of Lubotzky-Phillips-Sarnak & Margulis, which are Cayley graphs based on quaternions, and famously hold remarkable properties with respect to the 2^{nd} eigenvalue and the girth. As revealed by the computational experiments, the new octonion-based graphs do not hold the same properties. However these new graphs are of interest in graph theory as non-associative Cayley graphs, which likely hold other interesting properties. Implementations are realized in the algebra software Magma. A discussion on the algorithms and a complexity analysis are provided for those Cayley graphs in particular. The package that accompanies this article may serve more general purpose computations with graphs.

1 Introduction

1.1 Overview

Since their introduction in the mid 80's, the *Ramanujan graphs* [16, 18] have attracted a large amount of subsequent works from different communities of researchers. They realized indeed two major breakthroughs, first that of providing excellent explicit expanders, and second, by displaying no short cycle, or equivalently having a *large girth*.

In all these subsequent works, none considered though the possible use of *octonions*, whereas quaternions were used in [16, 18]. This is the main purpose of the present work, showing that by using arithmetic of integral octonions and properties of simple *Moufang Loops* a totally similar construction is indeed possible. For each odd prime number p, an infinite family of p^3+1-regular Cayley graphs based on these octonions are obtained. However, the non-associativity does not allow to prove the same remarkable properties as hold by the Ramanujan graphs after which they are modeled. To check that, we implemented these graphs[1] and computed explicitly their girth and 2^{nd} largest eigenvalue. The outcome of these experiments is a *negative* answer: despite the striking similarities between the construction of Cayley graphs based on quaternions and octonions, they (unfortunately) do not share the same remarkable properties. Though, they are of interest in graph theory as the first construction of Cayley graphs based on *Moufang loops* arising from octonions algebras (for Cayley graphs of degree 3 based on different Moufang loops, obtained "artificially" from doubling groups see [12]).

[1] The package can be downloaded at `http://xdahan.sakura.ne.jp/Package/graph.html`

The implementation that we have realized requires to handle huge graphs and thus we put a particular care on performance. This implementation is focused on Cayley graphs of quaternions and octonions, however may serve for more general Cayley graphs.Indeed the 2^{nd} largest eigenvalue and the large girth property find many applications in theoretical computer science, but also industrial ones. We describe below some of them.

1.2 Applications

Despite that the newly introduced graphs are (likely) not expander graphs and do not have large girth in general, the computation of the second eigenvalue and of the girth is important for the applications below.

Preliminaries When a directed graph $G = (V, E)$ is connected, the largest eigenvalue of its adjacency matrix has multiplicity one and its eigenspace is generated by the vector $(1, \ldots, 1)^t$. If the graph if moreover d-regular this largest eigenvalue is d. The 2^{nd} largest eigenvalue is usually denoted $\lambda(G)$ and for an infinite family of degree d-regular graphs G_n, if $\lambda(G_n)$ remains uniformly small, far away from d, then the graphs are good expanders. If $\lambda(G_n) \leq 2\sqrt{d-1}$ for large n then the family is *Ramanujan*. This is essentially the smallest value a second largest eigenvalue of a regular graph can reach according to the Alon-Boppana bound [23, 29]: $\lambda(G) \geq 2\sqrt{d-1} - O_m(\frac{\sqrt{d-1}}{\log m})$, for any d-regular graph G of order m.

Besides this remarkable property, the graphs [16, 18] hold the current record on the girth: $\text{girth}(G_n) \geq \frac{4}{3}\log_{d-1}|G_n|$. This is to compare with the (theoretical) upper bound $\text{girth}(\mathscr{G}_n) \leq 2\log_{d-1}|\mathscr{G}_n|$ for an infinite family $(\mathscr{G}_n)_n$ of d-regular graphs and for large n. (the tightness of this bound is a notoriously difficult problem.)

Expanders First of all, these graphs provide excellent *expander graphs* which have proved to be quite useful objects. They serve as model to build economical (in the sense of number of connections) but sufficiently connected network, hold naturally some randomness and are useful in a variety of constructions in theoretical computer science. This stems for the fact that a random walk on a good expander graph has typically a rapid *mixing time*: it converges quickly to the random distribution (on the set of all vertices). We are brief on these applications, since otherwise it will be difficult not paraphrasing the survey [13] dedicated to expander graphs and (some) of their applications.

Spectral partitioning & clustering The problem is to compute a partition in two or more sets of vertices with conditions on the number of edges connecting each components. The *sparsest cut* problem is an instance of partitioning where the conductance (or *ratio-cut*) is minimal. It is known to be NP-hard, while a relaxation version (due to Leighton and Rao) which can be stated in term of a Linear Program has a polynomial time solution [28].

Spectral clustering often refers to a more general problem that of graph partitioning in that the number of components is not known in advance and the *balance constraint*, given as an upper bound on the size of each set in the partition, is removed. The term "clustering" refers to clustering of data in Statistics and has a far range of applications in *e.g.* big data visualization and data mining. The technique of spectral clustering is *somehow* related to the computation of the second, or first k largest eigenvalues and their associated eigenspaces. The *power method* or generalization of it like the *Rayleigh quotient* is a key computational tool [2], as it is in the experiments realized here on these newly introduced graphs. However, we put emphasize in that the graphs are *Cayley* graphs for which more efficient, yet more simple algorithms can be set.

Large girth & LDPC Codes Computing the girth of graphs, as we did here for these new graphs, is motivated by applications related to error-correcting codes theory, and more precisely for "Low Density Parity Check" (LDPC) codes. This approach was pioneered by Margulis in [19], where he gave the first constructive example of a family of LDPC codes of unbounded minimum distance by providing explicit families of regular graphs of large girth. Such a property is quite useful in this context for several reasons:
(i) Tanner gave in [26] a construction of codes based on graphs together with a lower bound on the code minimum distance growing exponentially with the girth;
(ii) these LDPC codes are decoded with the help of iterative decoding algorithms working on a certain graph associated to the code construction and the performance of such algorithms is known to deteriorate in the presence of small cycles. This phenomenon is related to the fact that these iterative decoding algorithms compute symbol probabilities conditioned on an exponentially large (in the number of iterations) number of received symbols as long as the number of iterations is smaller than half the girth [10], but that does not hold anymore for a larger number of iterations.

1.3 Organization of the paper

Section 2 introduces quickly the background materials on octonions necessary to grasp the construction of the new octonion based graphs (Subsection 2.1), as well as a comparison with the construction of the LPS Ramanujan graphs which are based on quaternions (Subsection 2.2).

Then in Section 3 we present the outcome of the computations realized with our MAGMA implementation[2]. First, the implementation is tested on the LPS Ramanujan graphs for which explicit theoretical bounds are provided. After checking that the returned values match the theoretical ones, we report on experiments realized on the octonon-based graphs. The conclusion is that the graphs tested do not seem to have large girth and are not Ramanujan. Some tables are reported at the end of the article Appendix D due spacing requirements.

Section 4 reports about the implementation of the algebraic structures underlying the construction of Cayley graphs (that we will denote $X_{p,q}$, $Y_{p,q}$ for the quaternion based ones, and $\mathscr{X}_{p,q}$ and $\mathscr{Y}_{p,q}$ for the octonion-based ones, see Subsection 4.1). The algorithms used to compute the girth, and the 2^{nd} largest eigenvalue through the power method are reported in Subsections 4.2, 4.3 respectively.

Finally, in the first three Appendices, the complete construction of the octonion-based Cayley graphs is given with detailed proofs. This part is crucial but quite technical, justifying the summary given in Subsection 2.1.

2 Graphs based on quaternions and octonions

This section gives an overview of the construction of the new graphs based on octonions, and for readability contains also a short comparison with the famous construction of Ramanujan graphs, which rather use quaternions and after which they are modeled. For a complete and detailed presentation with proofs see Appendices A, B, C.

2.1 A new family of Cayley graphs based on octonions

Moufang loop It is customary to define a Cayley graph by imposing a *group* but the construction allows actually weaker algebraic structures. For example, *left quasi-groups* [22] in which invertible elements do not necessarily exist. With left and right inverses, we have the

[2] `http://xdahan.sakura.ne.jp/Package/graph.thml`

Moufang loops [3] which are the non-associative structures the closest to groups. Structures related to invertible elements of octonion algebras are generally Moufang loops, and thus all Cayley graphs in this work will be on such Moufang loops. A first word about the implementation may be in order: there is no particular change to care of between implementing Cayley graphs based on groups or on Moufang loops.

Overview of octonions. The purpose of this paragraph is to provide a minimal material about octonions to understand how the Cayley graphs were implemented. For a comprehensive presentation with detailed proofs, see Appendix A.

An octonion algebra $\mathbb{O}(R)$ over a commutative ring R is an 8-dimensional R-module which contains two copies of the same quaternion algebra $\mathbb{H}(R)$. Let $(1,\ \mathsf{i},\ \mathsf{j}, \mathsf{k})$ denotes the usual basis of Hamilton quaternions. It yields the equality of R-modules $\mathbb{O}(R) = \mathbb{H}(R) \oplus \mathbb{H}(R)\mathsf{t}$, where t is a new element of the basis of the 8-dimensional R-module. An octonion is written:

$$\alpha = \alpha_0 + \mathsf{i}\alpha_1 + \mathsf{j}\alpha_2 + \mathsf{k}\alpha_3 + \mathsf{t}\alpha_4 + \mathsf{it}\alpha_5 + \mathsf{jt}\alpha_6 + \mathsf{kt}\alpha_7, \quad (\text{ identified with } (\alpha_0, \ldots, \alpha_7)) \tag{1}$$

The standard *conjugation* of the quaternions in $\mathbb{H}(R)$ extends to $\mathbb{O}(R)$ by defining $\bar{1} = 1$ and $\overline{\alpha + \beta\mathsf{t}} = \bar{\alpha} - \beta\mathsf{t}$ for any α, β, $\in \mathbb{H}(R)$. The multiplication follows the *Cayley-Dickson doubling process* [5] which, given four quaternions $q_1, q_2, q_3, q_4 \in \mathbb{H}(R)$, is defined as follows:

$$(q_1 + q_2\mathsf{t})(q_3 + q_4\mathsf{t}) = q_1q_3 - \bar{q_4}q_2 + (q_4q_1 + q_2\bar{q_3})\mathsf{t}.$$

Assuming the equality $\overline{q_iq_j} = \overline{q_jq_i}$ true for quaternions, it follows in particular that $\overline{\alpha\beta} = \bar{\beta}\bar{\alpha}$ for $\alpha, \beta \in \mathbb{O}(R)$. It is noteworthy that if $\mathbb{H}(R)$ is not commutative, then $\mathbb{O}(R)$ is not associative.

The *norm* of an octonion α is $N(\alpha) = \alpha\bar{\alpha} = \bar{\alpha}\alpha$. It can be shown, and it is fundamental that, the norm is *multiplicative*: $N(\alpha\beta) = N(\alpha)N(\beta)$. The set of invertible octonions is then

$$\mathbb{O}(R)^\star = \{\alpha \ :\ N(\alpha) \in R^\star\}.$$

Factorization of integral octonions In the following R will be either a finite prime field $\mathbb{F}_p$ of characteristic $\neq 2$, either $\mathbb{Z}$ or $\mathbb{Q}$. As for Gauss integers, and quaternions, it is possible to define a kind of unique factorization for an octonion in $\mathbb{O}(\mathbb{Z})$, due to Rehm [25]. First of all, we isolate a special set of prime octonions (that is of norm p for a prime p) $\mathscr{P}(p)$ as follows (see (17)). We write $\alpha > 0$ to mean that the firs non-zero component of α is > 0.:

$$\mathscr{P}(p) \stackrel{\text{def}}{=} \{\alpha \in \mathbb{O}(\mathbb{Z}) :\ \alpha > 0\ ,\quad N(\alpha) = p\ ,\quad \alpha - 1 \in 2\mathcal{C}_{\mathbb{O}}\} \tag{2}$$

where $\mathcal{C}_{\mathbb{O}}$ is a set defined by a parity condition on the 8 components forming the octonion, see Lemma 1 for technical details. The cardinal of $\mathscr{P}(p)$ is $p^3 + 1$, and it is stable by conjugation (if $\pi \in \mathscr{P}(p)$, then $\overline{\pi} \in \mathscr{P}(p)$ as well). Given $\alpha \in \mathbb{O}(\mathbb{Z})$, $N(\alpha) = p^\ell$, let $c(\alpha)$ be its *content*: it is the positive gcd of its 8 integer coefficients (taken in any $\mathbb{Z}$-basis). Let m be such that $N(c(\alpha)) = p^{2m}$. Then there exits $\ell - 2m$ octonions in $\mathscr{P}(p)$, $\pi_1, \ldots, \pi_{\ell-2m}$ uniquely determined (see Theorem 4), such that:

$$\alpha = \pm c(\alpha)\,((\cdots((\pi_1\pi_2)\pi_3)\cdots)\,\pi_{\ell-2m})$$

It is important that two consecutive prime octonions in the writing above are *not* conjugate each other: $\pi_i \neq \overline{\pi_{i+1}}$.

This unique factorization property is used to show that two products satisfying the conditions above yield two distinct octonions if at least one prime factor is distinct among the two products. This shows that the regular graph defined hereunder is the infinite $p^3 + 1$-regular tree.

- the root corresponds to the void product
- the p^3+1 neighbors of the root are the p^3+1 prime octonions in $\mathscr{P}(p)$.
- Let N be a vertex defined by the product $(\cdots((\pi_1\pi_2)\pi_3)\cdots)\,\pi_\ell$ ($\pi_i \in \mathscr{P}(p)$, no consecutive prime π_i, π_{i+1} are conjugate). Then, p^3 neighbors are defined as:

$$\{((\cdots((\pi_1\pi_2)\pi_3)\cdots)\,\pi_\ell)\,\pi_{\ell+1} \ : \pi_{\ell+1} \in \mathscr{P}(p),\ \pi_{\ell+1} \neq \overline{\pi_\ell}\}.$$

- And the last neighbor of N is $(\cdots((\pi_1\pi_2)\pi_3)\cdots)\,\pi_{\ell-1}$.

This regular tree admits a description in term of Cayley graphs on a loop (see Appendix B for details and proofs).

The Cayley graphs. Given an octonion $\alpha \in \mathbb{O}(\mathbb{Z})$, a prime q, $\alpha \bmod q$ denotes the octonion in $\mathbb{O}(\mathbb{F}_q)$ where the 8 coordinates of α are reduced modulo q: $(\alpha_0 \bmod q, \alpha_1 \bmod q, \cdots, \alpha_7 \bmod q)$. Let $\mathcal{Z} = \{\alpha \in \mathbb{O}(\mathbb{F}_q)^\star \ : \ \alpha\beta = \beta\alpha,\ \forall \beta \in \mathbb{O}(\mathbb{F}_q)^\star\}$ be the central (sub)group of $\mathbb{O}(\mathbb{F}_q)^\star$. It is equal to $\{\alpha \in \mathbb{O}(\mathbb{F}_q)^\star \ : \ \alpha_1 = \alpha_2 = \ldots = \alpha_7 = 0\}$ and thus can be identified as $\mathcal{Z} \sim \mathbb{F}_q^\star$ (see Appendix C). Define next the subloop of $\mathbb{O}(\mathbb{F}_q)^\star$ consisting of octonions of norm $\equiv 1 \bmod q$

$$M_1 = \{\alpha \in \mathbb{O}(\mathbb{F}_q) : \ N(\alpha) = 1 \bmod q\}$$

Then its central subgroup is simply $\{\pm 1\}$, which are the only two octonions in $\mathcal{Z}$ of norm $\equiv 1 \bmod q$. Here is how the new Cayley graphs are defined. Below p denotes a prime number smaller than q.

- Moufang loop (defining the vertices): $\mathbb{O}(\mathbb{F}_q)^\star/\mathcal{Z}$ if $\left(\frac{p}{q}\right) = -1$, and $M_1/\{\pm 1\}$ if $\left(\frac{p}{q}\right) = 1$.
- Cayley set (defining the adjacency): $\mathscr{S}_{p,q} := \{(\pi \bmod q)\mathcal{Z} \ : \ \pi \in \mathscr{P}(p)\} \subset \mathbb{O}(\mathbb{F}_q)^\star/\mathcal{Z}$ if $\left(\frac{p}{q}\right) = -1$, or

  $\mathscr{S}_{p,q} := \{(\pi \bmod q)\{\pm 1\} : \ \pi \in \mathscr{P}(p)\} \subset M_1/\{\pm 1\}$ if $\left(\frac{p}{q}\right) = 1$.

  It is the image of $\mathscr{P}(p)$ by the map μ_q defined below ($\mu_q(\mathscr{P}(p)) = \mathscr{S}_{p,q}$)

$$\mu_q : \{\alpha \in \mathbb{O}(\mathbb{Z}) : N(\alpha) \not\equiv 0 \bmod q\} \xrightarrow{\bmod q} \mathbb{O}(\mathbb{F}_q)^\star \xrightarrow{\bmod \mathcal{Z}} \mathbb{O}(\mathbb{F}_q)^\star/\mathcal{Z}. \tag{3}$$

  We have indeed $\mathrm{Image}(\mu_q) = \mathbb{O}(\mathbb{F}_q)^\star/\mathcal{Z}$ if $\left(\frac{p}{q}\right) = -1$ and $\mathrm{Image}(\mu_q) \simeq M_1/\{\pm 1\}$ if $\left(\frac{p}{q}\right) = 1$ (See Lemma 4).

- Denote $\mathscr{X}_{p,q} = \mathscr{C}ay(\mathbb{O}(\mathbb{F}_q)^\star/\mathcal{Z}\ ,\ \mathscr{S}_{p,q})$ if $\left(\frac{p}{q}\right) = -1$, or
  $\mathscr{Y}_{p,q} = \mathscr{C}ay(M_1/\{\pm 1\}\ ,\ \mathscr{S}_{p,q})$ if $\left(\frac{p}{q}\right) = 1$.

Cayley graphs of Moufang loops are not necessarily vertex-transitive (multiplication by an element yields no more an automorphism of graphs as it is trivially the case for Cayley graphs on groups). The following properties hold.

Property: (see Appendix C: Definition 5, Lemma 5,Propositions 5 and 6)

- $\mathscr{X}_{p,q}$ is bipartite of order $q^7 - q^3$
- $\mathscr{Y}_{p,q}$ is non-bipartite of order $\frac{1}{2}(q^7 - q^3)$
- Both are p^3+1-regular and connected.
- the length of a shortest cycle at the *identity vertex* is $\geq \frac{12}{7}\log_{p^3}|\mathscr{X}_{p,q}| - 2\log_p 2$.

2.2 Comparison with the quaternion-based Ramanujan graphs

The construction above is inspired by that of Lubotzky-Philips-Sarnak's Ramanujan graphs. In order to compare the two constructions, and since we include experimental results on those graphs as well, this subsection briefly recalls how the LPS Ramanujan graphs were built.

For two prime numbers $p < q$, let $\mathbb{H}(\mathbb{F}_p)^\star$ and $\mathbb{H}_1$ denote the set of invertible quaternions and the set of quaternions of norm 1 respectively, over $\mathbb{F}_p$. We exclude the case $p \equiv 1 \bmod 4$ in this succinct presentation since it induces some slight complications (See [7, Proposition 2.3, Equality (8)] for the whole generality).

Similarly to the set $\mathscr{P}(p)$ defined above (and in detail in Equality (17)) for octonions, unique factorization in quaternions (known since Hurwitz...) requires a special set of prime quaternions

$$\mathscr{Q}(p) := \{\pi = (a_0 + a_1\mathsf{i} + a_2\mathsf{j} + a_3\mathsf{k}) \in \mathbb{H}(\mathbb{Z}) : N(\pi) = p, a_0 > 0, \pi - 1 \in 2\mathbb{H}(\mathbb{Z})\}. \tag{4}$$

The cardinal of this set is $p + 1$.

We denote $\mathscr{D}_{p,q} := (\mathscr{Q}(p) \bmod q)$ modulo $\mathcal{Z}$, where $\mathcal{Z} \sim \mathbb{F}_q^\star$ is the central subgroup of $\mathbb{H}(\mathbb{F}_q)^\star$. It is the image of $\mathscr{Q}(p)$ through $\{\alpha \in \mathbb{H}(\mathbb{Z}) \ : \ N(\alpha) \not\equiv 0 \bmod q\} \to \mathbb{H}(\mathbb{F}_q)^\star/\mathcal{Z}$. If $\left(\frac{p}{q}\right) = -1$ then $\langle \mathscr{D}_{p,q} \rangle = \mathbb{H}(\mathbb{F}_q)^\star/\mathcal{Z}$ and $\langle \mathscr{D}_{p,q} \rangle = \mathbb{H}_1/\{\pm 1\} \subset \mathbb{H}(\mathbb{F}_q)^\star/\mathcal{Z}$ if $\left(\frac{p}{q}\right) = 1$.

Then $X_{p,q} := \mathscr{C}ay(\mathbb{H}(\mathbb{F}_q)^\star/\mathcal{Z}, \mathscr{D}_{p,q})$ when $\left(\frac{p}{q}\right) = -1$ and $Y_{p,q} = \mathscr{C}ay(\mathbb{H}_1/\{\pm 1\}, \mathscr{D}_{p,q})$ when $\left(\frac{p}{q}\right) = 1$.

Property:

- (see [16]) $X_{p,q}$ is bipartite of order $q^3 - q$ and $Y_{p,q}$ is not bipartite of order $\frac{1}{2}(q^3 - q)$. Both are connected and $p + 1$-regular.
- The girth of graphs $X_{p,q}$ verifies (see [1]):

$$4\log_p q - \log_p 4 \leq \mathrm{girth}(X_{p,q}) < 4\log_p q + \log_p 4 + 2, \tag{5}$$

  and $\mathrm{girth}(Y_{p,q}) \geq 2\log_p q - \log_p 2$.

- (see [16], or [18]) The second largest eigenvalue verifies: $\lambda(X_{p,q}) \overset{(\star)}{\leq} 2\sqrt{p}$ (which means that for each prime p, the infinite families of graphs $\{X_{p,q}\}_q$ and $\{Y_{p,q}\}_q$ are *Ramanujan*).

3 Experimental Results

The girth and the spectral properties of the graphs of Subsection 2.2 could be thoroughly checked with the implementation presented in the next section. For the octonion-based graphs $\mathscr{X}_{p,q}$ and $\mathscr{Y}_{p,q}$, being larger, checking whether these properties hold is more difficult than for the quaternion-based $X_{p,q}$ and $Y_{p,q}$. However on each graph we have checked, none seem to have large girth and none are Ramanujan.

Implementation details and algorithms are discussed in the next section.

3.1 Checking the Ramanujan property of the Lubotzky-Philips-Sarnak graphs

In this subsection are presented some experimental results of our implementation of the LPS graphs. For these graphs, precise theoretical results are known on the girth (Equation (5)) and on the 2^{nd} largest eigenvalue (inequality $(\star)$ below Equality (5)) and it is thus possible to check the correctness of the implementation.

Example of $p = 37$ We start by experimental results verifying the Ramanujan property, with a sample of graphs of degree $p + 1 = 38$: $Y_{37,41}$ (Table 4), $Y_{37,71}$ (Table 5), $X_{37,109}$ (Table 6). The property to check is namely $\lambda(X_{37,q})$ or $\lambda(Y_{37,q}) \leq 2\sqrt{37} \approx 12.165$. As the tables show this inequality is verified.

Example of $p = 47$ Next, we have checked the Ramanujan property for graphs of degree $p + 1 = 48$ and for all primes q from 53 up to 113. We reproduce the results for $q = 53, 83, 113$ (Tables 7, 8, 9 respectively). The Ramanujan bound is $2\sqrt{47} \approx 13.71$. As the tables show this inequality is verified.

How to read the tables? The first line shows the time necessary to generate all the nodes, denoted $H_{p,q}$ (for quaternions it is either $\mathbb{H}(\mathbb{F}_q)^\star/\mathcal{Z}$ or $\mathbb{H}_1/\{\pm 1\}$) and it is the first Step of Algorithm 2. The second line displays the time necessary to construct the initial vector $x^{(0)}$ as described in Step 2 of Algorithm 2. The third line is the timing required to build the adjacency table. It requires a lot of memory but induces considerable speed-up at each iteration of the power method. Lines coming after these three ones are easy to understand: they show the iteration number, the corresponding timing to achieve the current iteration and the approximation of the eigenvalue obtained.

3.2 Eigenvalue computation for the new octonion based graphs

Due to the quickly increasing order of these graphs that exhausts the computational resources, only few experiments with the smallest parameters could have been undertaken: $\mathscr{X}_{3,5}$ (Table 10), $\mathscr{X}_{3,7}$ (Table 11), $\mathscr{Y}_{3,11}$ (Table 12). These are sufficient to see that the Ramanujan bound $2\sqrt{27} \approx 10.392$ is not verified in each case which clearly show that the graphs are *not* Ramanujan, according to Corollary 1.

See the previous subsection for explanations on how to read the tables.

3.3 Checking the girth of LPS Ramanujan graphs

After presenting experimental results about the 2^{nd} largest eigenvalue here are presented some others, related to the computation of the girth. In the tables 13, 14 of Appendix D, are displayed experimental results related to the girth of LPS Ramanujan graphs of degree 12 and degree 108. The column "Girth Range" indicates the possible values as predicted by Inequality (5). Dots like $x\ldots$ means "any value larger than x". The results perfectly confirm what the theoretical bounds predict. Many more experiments not reproduced in the paper have been run with the same conclusion.

Remark: The time to find the girth of some non-bipartite graphs of degree 108 as reported in Table 14 (values of $q = 491,487,\ 479,461,\ 457,419,\ 397,379,\ 367,337,\ 311, \cdots$) can be ≈ 500 times slower than some other computations. The girth is even and is "large". The reason of this extra cost is due the generation and management of two lists of nodes necessary to take into account cycles of odd length (see Algorithm 1) as well as the depth reached in the breadth search (not indicated in the tables).

3.4 Girth of octonion graphs

In the case of vertex-transitive graphs (like Cayley graphs on groups) it suffices to compute the length of a shortest cycle at *one* node to find the girth. The Cayley graphs on Moufang loops introduced are (likely) *not* vertex-transitive requiring to check the length of shortest cycles at *each* node.

Lemma 6 states that the cycles going through the *identity* vertex are long, so the purpose of these experiments is to answer the question:

Are there such long cycles at all vertices ?

The experimental investigations yield a negative answer in general. The rather "chaotic" results of the experiments on on small graphs suggest a negative answer for larger graphs as well.

It was possible to do this without exhausting the 1Gb memory only for the three smallest graphs $\mathscr{X}_{3,5}, \mathscr{Y}_{3,7}$ and $\mathscr{Y}_{3,11}$. For **larger graphs**, we could only take a sample of nodes randomly selected and compute the length of a shortest cycle at each nodes of the sample. This way of doing supplies only an upper bound on the girth, that is why in the column girth of Tables 1, 2, 3, only an inequality symbol $\leq$ is written. Nonetheless, the results show that the girth is much smaller than expected and unlikely bring anything interesting in terms of *large girth* graphs.

We undertook three kinds of experiments concerning the length of cycles.

1. the existence of short cycles (quite cheap and allows to investigate large graphs)
2. Computing the girth
3. Computing the distribution of the length of the shortest cycle going through all/a sample of vertices

The order of the graphs prohibits to compute the girth in 2. except for rather small values of p and q, and for 3. to consider large samples. It is however possible to look in 1. for short cycles for rather large graphs since short cycles do exist and tend to be abundant.

graphs	order	bipartite	girth	cycle at identity	distrib
$\mathscr{X}_{3,5}$	78000	yes	6	6	6 (100%)
$\mathscr{X}_{3,7}$	823200	yes	6	8	6 (98.81%) and 8 (1.18%)
$\mathscr{Y}_{3,11}$	9742920	no	5	9	5 (54.5%), 6 (41.6%) , 7 (3,8%) , 8 (0.003%), 9 (41 vertices)
$\mathscr{Y}_{3,13}$	31373160	no	≤ 6	9	
$\mathscr{Y}_{3,23}$	1702406640	no	≤ 5	memory	
$\mathscr{Y}_{3,37}$	47465913240	no	≤ 6	memory	

Table 1: Experiments for various degree 28 graphs. The column "distrib" displays the minimal length of cycles found at each vertices, and inside parentheses the percentage or the number of vertices through which the shortest cycle has this length

Experiments on degree 28 graphs. They are summarized in Table 1. For example the table shows that in $\mathscr{Y}_{3,13}$ the girth is lower or equal to 6. Here is a cycle of length 6:

Cycle of length 6 in $\mathscr{Y}_{3,13}$: consider the following 6 elements of $\mathscr{P}(3)$

$$\begin{array}{cc} \beta_4 = (0,0,0,0,0,1,-1,-1) & \beta_2 = (0,0,0,0,0,1,-1,1) \\ \beta_{15} = (0,0,1,-1,0,1,0,0) & \beta_{18} = (0,1,0,0,1,1,0,0) \\ \beta_{13} = (0,0,1,1,0,1,0,0) & \beta_{28} = (0,1,-1,0,0,0,0,-1) \end{array}$$

And consider the element $x = (3, 3, 9, 2, 6, 3, 10, 0) \in \mathbb{O}(\mathbb{F}_{13})^\star$. Then $N(x) = 1$ in $\mathbb{F}_{13}$, so that $x \in M_1$. The normal form of x in $\mathbb{O}(\mathbb{F}_{13})^\star/\mathcal{Z}$ is $\tilde{x} = (-3^{-1} \bmod 13)x = (1, 1, 3, 5, 2, 1, 12, 0)$. Recall the map μ_q introduced in (3) (or in more details in (21) of Annex C). We can verify that:

$$((\tilde{x} * \mu_{13}(\beta_{18})) * \mu_{13}(\beta_{13})) * \mu_{13}(\beta_{28}) = ((\tilde{x} * \mu_{13}(\beta_4)) * \mu_{13}(\beta_2)) * \mu_{13}(\beta_{15}) = (1, 8, 2, 1, 0, 1, 9, 6).$$

This shows a cycle of length 6 going through the vertex $\tilde{x}$.

Degree $126 = 5^3 + 1$ regular graphs Let us move to the next "smallest" case where $p = 5$, yielding degree 126 graphs. Table 2 shows the results of the experiments. Surprisingly, very short cycles of length 4 are found, indicating that the girth does not necessarily grow with p nor with the order of the graphs.

graphs	order	bipartite	girth	cycle at identity
$\mathscr{X}_{5,7}$	823200	yes	4	6
$\mathscr{Y}_{5,11}$	9742920	no	4	6
$\mathscr{X}_{5,13}$	62746320	yes	≤ 6	8
$\mathscr{X}_{3,17}$	410333760	yes	≤ 6	8
$\mathscr{Y}_{5,19}$	446932440	no	≤ 5	5
$\mathscr{X}_{5,23}$	3404813280	yes	≤ 6	8
$\mathscr{Y}_{5,29}$	8624925960	no	≤ 5	memory
$\mathscr{Y}_{5,31}$	13756292160	no	≤ 6	
$\mathscr{X}_{5,37}$	94931826480	yes	≤ 6	
$\mathscr{Y}_{5,41}$	97377102480	no	≤ 6	
$\mathscr{X}_{5,43}$	271818531600	yes	≤ 6	
$\mathscr{X}_{5,47}$	506623016640	yes	≤ 6	

Table 2: Computations of the smallest cycle going through the identity vertex in various graphs for $p = 5$ (degree 126). And search for the existence of cycles of length 4, 5 or 6 at a sample of other vertices

Cycle of length 4 in $\mathscr{X}_{5,7}$. There is such a cycle going through the node corresponding to $x = (1, 5, 5, 4, 6, 6, 0, 0) \in \mathbb{O}(\mathbb{F}_7)^\star/\mathcal{Z}$. Consider the 4 elements $\gamma_1, \gamma_3, \gamma_{12}, \gamma_{32} \in \mathscr{P}(5)$.

$$\gamma_7 = (1, 0, 0, 0, -2, 0, 0, 0) \quad \gamma_{86} = (1, 1, 0, -1, 0, -1, 0, -1)$$
$$\gamma_5 = (1, 0, 0, 0, 0, 2, 0, 0) \quad \gamma_{119} = (1, -1, 1, -1, 1, 0, 0, 0)$$

The cycle of length 4 is defined by the following equalities:

$$(x * \mu_7(\gamma_7)) * \mu_7(\gamma_{86}) = (x * \mu_7(\gamma_5)) * \mu_7(\gamma_{119}) = (1, 2, 4, 3, 4, 1, 5, 5)$$

Graphs of degree 344. Taking $p = 7$, the existence of short cycles was verified until $q = 43$. This confirms the observation that the girth does not seem to be a growing function with the order of the graphs, as should be graphs of large girth.

Cycle of length 4 in $\mathscr{Y}_{7,29}$. Such a short cycle is going through the vertex indexed by the octonion in normal form $x = (1, 10, 1, 8, 11, 4, 25, 8) \in \mathbb{O}(\mathbb{F}_{29})^\star/\mathcal{Z}$. The four elements $\delta_{217}, \delta_{199}, \delta_{326}, \delta_{151} \in \mathscr{P}(7)$

$$\delta_{217} = (0, 1, 1, 0, -2, 0, 0, 1) \quad \delta_{199} = (0, 1, 0, -2, 1, -1, 0, 0)$$
$$\delta_{151} = (0, 0, 2, -1, -1, 0, 0, -1) \quad \delta_{326} = (0, 2, 0, -1, 1, 0, 0, 1)$$

graphs	order	bipartite	girth	cycle at identity
$\mathscr{X}_{7,11}$	19485840	yes	4	6
$\mathscr{X}_{7,13}$	62746320	yes	4	6
$\mathscr{X}_{7,17}$	410333760	yes	4	6
$\mathscr{Y}_{7,19}$	446932440	no	4	memory
$\mathscr{X}_{7,23}$	3404813280	yes	≤ 6	
$\mathscr{Y}_{7,29}$	8624925960	no	4	
$\mathscr{Y}_{7,31}$	13756292160	no	≤ 5	
$\mathscr{Y}_{7,37}$	47465913240	no	≤ 5	
$\mathscr{X}_{7,41}$	194754204960	yes	≤ 6	
$\mathscr{X}_{7,43}$	271818531600	yes	≤ 6	

Table 3: Search for cycles of length 6 or less in huge degree 344 regular graphs was actually not difficult: they are abundant

yield to following equality in $\mathbb{O}(\mathbb{F}_{29})^\star/\mathcal{Z}$:

$$(x * \mu_{29}(\delta_{217})) * \mu_{29}(\delta_{199}) = (x * \mu_{29}(\delta_{151})) * \mu_{29}(\delta_{326}) = (1, 28, 12, 18, 3, 15, 16, 23),$$

and thus a cycle of length 4.

4 Implementation details

4.1 Representation of Cayley graphs

A Cayley graph is fully encoded by the set of nodes (a quaternion group or a Moufang loop in our case) and the Cayley set. Note that to reduce memory consumption, it is sufficient to encode the Cayley set *only* and build vertices on-demand. This way of doing is commonplace in iterative methods in linear algebra where only matrix/vector products are needed, and where the matrix is stored as a "black-box". This is the case for computing the girth. For computing the 2^{nd} largest eigenvalue, it is faster to pre-compute all the vertices if memory space is not a problem. Indeed, having this list acts as a "look-up table". When the memory demand is too excessive to store the adjacency table, the computation may still be possible while much slower. For an example of graph whose adjacency table's construction exceeds the memory capacity, see the graph $\mathscr{Y}_{3,11}$ (Section 3.2) and timings in Table 12.

Quaternions and octonions We implemented the Cayley-Dickson doubling process [5] to generate the multiplication rules of quaternions and octonions. While quaternions are already implemented in Magma, octonions are not and the flexibility of this process, which allows to perform various checking for correctness motivated choosing this process to compute the multiplication table of both quaternions and octonions. Once the multiplication table is constructed, Magma provides a functionality to create algebras. It also supplies with homomorphism maps which we used to generate the algebras $\mathbb{O}(\mathbb{F}_q)$ from $\mathbb{O}(\mathbb{Z})$. In those algebras an octonion is coded by a 8-dimensional vector, or a list of 8 elements easier to manipulate.

Next, the special set of prime octonions $\mathscr{P}(p)$ (see (3), (21)) or of quaternions $\mathscr{Q}(p)$ is generated without difficulty by brute force (with some obvious refinements as suggested by the properties held by the elements in $\mathscr{P}(p)$) since this set is small. In the code, this set is recorded in the global variable named PGLOBAL in the remainder of the implementation.

Representation of in quotient of "Moofang loop" We use **normal forms** to represent an element in $\mathbb{O}(\mathbb{F}_q)^\star/\mathcal{Z}$ or $M_1/\{\pm 1\}$, where $M_1 = \{\alpha \in \mathbb{O}(\mathbb{F}_q) : N(\alpha) = 1\}$. A list of 8 elements in $\mathbb{Z}$ is in *normal form* if its first non-zero coordinate is equal to 1.

Indeed given $\alpha \in \mathbb{O}(\mathbb{F}_q)^\star$ (or M_1) there is a unique vector $\tilde{\alpha} = (a_0, a_1, \ldots, a_7)$ (with entries in $\mathbb{Z}$) which encodes the classes $\alpha\mathcal{Z} \in \mathbb{O}(\mathbb{F}_q)^\star/\mathcal{Z}$ (or the classes $\pm\alpha \in M_1/\{\pm 1\}$). It is defined by inverting the first non-zero coefficient x_{first} and multiplying it by α: $\tilde{\alpha} = x_{first}^{-1}\alpha$ is in normal form.

In the package that accompanies this article, the set denoted $H_{p,q}$ is a set of elements in $\mathbb{O}(\mathbb{F}_q)^\star$ in normal form (hence representing $\mathbb{O}(\mathbb{F}_q)^\star/\mathcal{Z}$ if $\left(\frac{p}{q}\right) = -1$ or the set of elements in $M_1/\{\pm 1\}$ when $\left(\frac{p}{q}\right) = 1$). This necessary step in the implementation has a running-time *linear* in the order of the graphs.

4.2 Computing the girth

We search for the shortest cycle at the identity for Cayley graphs based on groups $X_{p,q}$ and $Y_{p,q}$ (quaternions), or, at each cycle for the Cayley graphs $\mathscr{X}_{p,q}$ and $\mathscr{Y}_{p,q}$ based on octonions. This latter computation was done only for $p = 3$ and $q = 5, 7, 11, 13$ where the outcome is displayed in Table 1.

To find the shortest cycle at a given node we use the following "breadth-first" search algorithm adapted to Cayley graphs.

Two tables Tab and $newTab$ are maintained. The former contains vertices computed at a given distance $\ell - 1$ from the starting vertex v_0 and the latter table contains vertices at distance ℓ currently being computed from a vertex x in Tab: $newTab = newTab \cup \{NormalForm(xy) : y \in \mathscr{P}(p)\}$. A cycle is detected if an element currently being computed and to be input in $newTab$ happens to be already in one of the two tables (a kind of *collision*). The size of the tables increase exponentially so we have optimized our code to maintain only necessary elements in the two tables (this is not written in Line 15, where all elements in $newTab$ are computed before filling its content to Tab at the end of an iteration).

The record of the edges forming a path from the starting vertex x_0 and to the currently computed vertex is *not* written in Algorithm 1 since it complicates unnecessarily the matter. Following the construction of Cayley graphs in this work, by taking " finite quotients" of an infinite regular tree, this simply amounts to track record of indices of elements in $\mathscr{P}(p)$ used for the walk, and to check for a "collision" by reduction modulo q of the coordinates. We recall that elements of $\mathscr{P}(p)$ in normal form are stored in a global variable called $PGLOBAL$.

Comparison with built-in function "girth" of MAGMA**.** Octonions are not pre-implemented in MAGMA but quaternions are. In this case, it is actually more natural to use matrix groups $PGL_2(\mathbb{F}_q)$ or $PSL_2(\mathbb{F}_q)$: it is a well-known fact that $PGL_2(\mathbb{F}_p) \simeq \mathbb{H}(\mathbb{F}_q)^\star/\mathcal{Z}$ and $PSL_2(\mathbb{F}_q) \simeq \mathbb{H}_1/\{\pm 1\}$ with the notations of Subsection 2.2 (see *e.g.* [8, Proposition 2.5.2]). Then to construct a Cayley graph using the function `CayleyGraph`, and finally use the `Girth` function. The first obstacle is the way MAGMA represents matrix groups $PSL_2(\mathbb{F}_q)$ and $PGL_2(\mathbb{F}_q)$, not well-suited for our purpose: it uses *representation* though permutation groups. This representation is indeed customary in the realm of Computational Group Theory, but for performance computing in Cayley graphs, the simpler normal forms as mentioned above are more suited. Moreover, the function `CayleyGraph` does not support such data, complicating the matter furthermore.

Algorithm 1: Shortest cycle at a node v_0 (high-level algorithm)

Input: An element $v_0 \in H_{p,q}$ in normal form ($H_{p,q}$ represents either $\mathbb{O}(\mathbb{F}_q)^\star/\mathcal{Z}$ or $\mathbb{H}(\mathbb{F}_q)^\star/\mathcal{Z}$ if graphs are bipartite, either $M_1/\{\pm 1\}$ or $\mathbb{H}_1/\{\pm 1\}$ otherwise)
PGLOBAL, set representing $\mathscr{P}(p)$

Output: Length of a shortest cycle, and coordinates of the edges in this cycle

$\ell = 1, \quad Tab = [v_0]$ `// store vertices at distance` $\ell - 1$ `from` v_0
$newTab = [\,]$ `// store vertices at distance` ℓ `from` v_0
while *no cycle found* **do**
  for $x \in Tab$ **do**
    for $y \in PGLOBAL$ **do**
      $z = x * y$ (computed in $H_{p,q}$: first in $\mathbb{H}(\mathbb{F}_p)$ or $\mathbb{O}(\mathbb{F}_p)$ and then the normal form is taken)
      if $z \in newTab$ **then** `// test for a cycle of even length`
        return 2ℓ, *and the two paths from* x *to* z*: the one just computed* $v_0 \to \cdots \to x \to z$, *and the one previously computed*
      else if $z \in Tab$ **then** `// test for a cycle of odd length`
        return $2\ell - 1$ *and two paths from* v_0 *to* z*: the one of length* ℓ *just computed* $v_0 \to \cdots \to x \to z$ *and one of length* $\ell - 1$ *previously computed*
      else `// no cycle found`
        $newTab = newTab$ cat $[z]$
    end
  end
  $\ell = \ell + 1, \;\; Tab = newTab, \;\; newTab = [\,]$
end

4.3 Computing the 2nd largest eigenvalue

The standard method to approximate largest eigenvalues of graphs is the *power method*. There is an extensive literature on the subject, and in the context of regular expanders the introductory reference that we recommend is that of Luca Trevisan [27].

The power method fundamentally approximates the largest eigenvalue and its eigenspace, but can easily be adapted to compute the 2nd largest one *if* the eigenspace of the largest one is known. The algorithm is probabilistic Las Vegas, the rate of convergence depends partly on how far is the initial guess from the eigenspace of the 2nd largest eigenvalue. But it depends especially on the quotient between the 3rd and 2nd one largest eigenvalue.

The main iteration is the following, where A is the adjacency matrix.

$$\text{Choose } x^{(0)} \in \{-1,0,1\}^n \text{ randomly and for } i \geq 0 \quad x^{(i+1)} = A \cdot x^{(i)}, \quad \lambda^{(i+1)^2} \stackrel{\text{def}}{=} \frac{\|x^{(i+1)}\|^2}{\|x^{(i)}\|^2} \quad (6)$$

Theorem 1 *Let $\lambda_0 = d > \lambda_1 = \lambda(G) \geq \lambda_2 \cdots \geq \lambda_{n-1}$ be the eigenvalues of the graph G. Let μ the smallest eigenvalue in absolute value: $\mu \stackrel{def}{=} \inf_i\{|\lambda_i| > 0\}$, and σ the 3rd largest eigenvalue: $\sigma \stackrel{def}{=} \max_{i\leq 2}\{\lambda_i\} = \max_i\{\lambda_i < \lambda_1\}$.*

(H) Assume that the initial vector $x^{(0)} \in \ker(A - \lambda_0 \mathrm{Id})^\perp = \langle(1,1,\ldots,1)\rangle^\perp$. (in the bipartite case, assume additionally that $x^{(0)} \in \ker(A - \lambda_{n-1}\mathrm{Id})^\perp = \langle(1,\ldots,1,-1,\ldots,-1)\rangle^\perp$)
Let p_1 be orthogonal projection on $\ker(A - \lambda_1 \mathrm{Id})$ (or on $\ker(A - \lambda_1 \mathrm{Id}) \oplus \ker(A - \lambda_{n-2}\mathrm{Id})$ in the bipartite case), and assume that $n_1^2 = \|p_1(x^{(0)})\|^2$ is $\neq 0$.

Denote by m the multiplicity of λ_1 (so that $\sigma = \lambda_{1+m}$) and by α the ratio of non-zero coefficients in the choice of $x^{(0)}$. Then the sequence $\lambda^{(i)}$ defined in (6) converges to $\lambda(G) = \lambda_1$ with:

$$1 - \left(\frac{n^2\alpha^2 - n_1^2}{n_1^2}\right)\left(\frac{\sigma}{\lambda_1}\right)^{2i-2}\left(1 - \left(\frac{\mu}{\lambda_1}\right)^2\right) \leq \frac{\lambda^{(i)^2}}{\lambda_1^2} \leq 1 \quad (7)$$

Remark 2 A few remarks before the proof:

(a) The convergence rate depends on how far is the 3rd largest eigenvalue σ from λ_1. Since $0 < \frac{\sigma}{\lambda_1} < 1$, the convergence rate decreases with the number of iterations. Experiments in Subsections 3.1, 3.2 perfectly reflects this speed decrease: higher iterations produce little precision gain.

(b) This kind of theorem is classic but in most cases, $\lambda^{(i)}$ is approximated by $\frac{x^{(i-1)^t} A x^{(i-1)}}{x^{(i-1)^t} x^{(i-1)}}$ $(*)$ rather than by $\pm\frac{\|Ax^{(i-1)}\|}{\|x^{(i-1)}\|}$ which has the advantage to keep record of the sign: the convergence rate does not involve squares of $\lambda^{(i)}$ like in (7). Note that since $\lambda_1 > 0$ in our case, the sign does not matter.

(c) It is also more customary to state the convergence rate *additively*. For example [11, Theorem 8.2.1] the approximation of the largest eigenvalue λ_0 by $\lambda^{(1)}$, $\lambda^{(2)}, \ldots$ is defined though the iteration $(*)$ in (b). The convergence rate is given by: $|\lambda^{(k)} - \lambda_0| \leq \frac{1 - x^{(0)^t} \cdot q_0}{x^{(0)^t} \cdot q_0} |\lambda_0 - \lambda_{n-1}| \left|\frac{\lambda_1}{\lambda_0}\right|^{2k}$, where λ_0 is assumed to be *simple* that is $\lambda_0 > \lambda_1$, where q_0 is a vector of 2-norm 1 that generates the eigenspace for the eigenvalue λ_0, and where the initial vector $x^{(0)} \in \langle q_0\rangle^\perp$ (equivalently $x^{(0)^t} \cdot q_0 \neq 0$) is of 2-norm 1. In our case, the convergence rate (7) stated additively is very similar:

$$0 \leq \lambda_1^2 - \lambda^{(i)^2} \leq \left(\frac{n^2\alpha^2 - n_1^2}{n_1^2}\right)\left(\frac{\sigma}{\lambda_1}\right)^{2i-2}(\lambda_1^2 - \mu^2).$$

(d) Choosing α small, that is choosing $x^{(0)}$ with any zero entries among $\{-1, 0, 1\}$, accelerates slightly the convergence, but on the other hand it is more difficult to guarantee that $x^{(0)}$ is "far" from the eigenspace $\ker(A - \lambda_1 \mathrm{Id})$ (and of $\ker(A - \lambda_{n-1}\mathrm{Id})$ in the bipartite case). Note that his latter condition is impossible to check in advance.

PROOF: Consider an orthonormal basis $q_0,\ q_1,\ q_2,\ \ldots$ of eigenvectors for A, so that $A^i \cdot q_\ell = \lambda_\ell^i q_\ell$. If we write the initial vector $x^{(0)}$ in this basis $x^{(0)} = \sum_{\ell=0}^{n-1} a_\ell q_\ell$, then $x^{(i)} = \sum_{\ell=0}^{n-1} a_\ell \lambda_\ell^i q_\ell$, where $a_\ell = q_\ell^t \cdot x^{(0)}$. Note that by assumption $a_0 = 0$ (also $a_{n-1} = 0$ in the bipartite case), and $n_1^2 = \|p_1(x^{(0)})\|^2 \neq 0$. From $\|x^{(i)}\|^2 = \sum_{\ell=0}^{n-1} a_\ell^2 \lambda_\ell^{2i}$ and regarding the multiplicity m of λ_1, we have: $\|x^{(i)}\|^2 = \lambda_1^2 n_1^2 + \sum_{\ell>m} a_\ell^2 \lambda_\ell^{2i}$ (in the bipartite case, change $\sum_{\ell>m}$ by $\sum_{\ell=m+1}^{n-2-m}$ and recall that $\lambda_{n-2} = -\lambda_1$)

By definition of the approximated sequence $({\lambda^{(0)}}^2,\ {\lambda^{(1)}}^2,\ {\lambda^{(2)}}^2,\ \ldots\ )$ in (6):

$$\begin{aligned} {\lambda^{(i)}}^2 = \frac{\|x^{(i)}\|^2}{\|x^{(i-1)}\|^2} &= \frac{n_1^2\lambda_1^{2i} + \sum_{\ell>m} a_\ell^2 \lambda_\ell^{2i}}{n_1^2\lambda_1^{2i-2} + \sum_{\ell>m} a_\ell^2 \lambda_\ell^{2i-2}} \\ &= \frac{|\lambda_1|^{2i}}{|\lambda_1|^{2i-2}} \cdot \frac{n_1^2 + \sum_{\ell>m}\left(\frac{\lambda_\ell}{\lambda_1}\right)^{2i}}{n_1^2 + \sum_{\ell>m}\left(\frac{\lambda_\ell}{\lambda_1}\right)^{2i-1}} = \lambda_1^2 \cdot \frac{n_1^2 + B_i}{n_1^2 + B_{i-1}}, \end{aligned} \tag{8}$$

where $B_i = \sum_{\ell>m} a_\ell^2 \left|\frac{\lambda_\ell}{\lambda_1}\right|^{2i}$. (in the bipartite case, replace $\sum_{\ell>m}$ by $\sum_{\ell=m+1}^{n-2-m}$). Regarding the definition of μ and σ, we obtain $\frac{\mu}{\lambda_1} \leq \frac{|\lambda_\ell|}{\lambda_1} \leq \frac{\sigma}{\lambda_1}$. Moreover, regarding the definition of α, we get $\|x^{(0)}\|^2 = \alpha^2 n^2$:

$$(n^2\alpha^2 - n_1^2)\left(\frac{\mu}{\lambda_1}\right)^{2i} \leq B_i \leq (n^2\alpha^2 - n_1^2)\left(\frac{\sigma}{\lambda_1}\right)^{2i}$$

On the other hand,

$$\frac{n_1^2 + B_i}{n_1^2 + B_{i-1}} = \frac{n_1^2 + B_{i-1} - (B_{i-1} + B_i)}{n_1^2 + B_{i-1}} = 1 - \frac{B_{i-1} - B_i}{n_1^2 + B_{i-1}}. \tag{9}$$

Next, we bound this latter term. Thanks to the formula for $B_{i-1} - B_i$ hereunder:

$$B_{i-1} - B_i = \sum_{\ell>m} a_\ell^2 \left|\frac{\lambda_\ell}{\lambda_1}\right|^{2i-2} - a_\ell^2 \left|\frac{\lambda_\ell}{\lambda_1}\right|^{2i} = \sum_{\ell>m} a_\ell^2 \left(\frac{\lambda_\ell}{\lambda_1}\right)^{2i-2}\left(1 - \left|\frac{\lambda_\ell}{\lambda_1}\right|^2\right),$$

(in the bipartite case, replace $\sum_{\ell>m}$ by $\sum_{\ell=m+1}^{n-2-m}$) we obtain the following upper and lower bounds:

$$\begin{aligned} B_{i-1} - B_i &\leq (n^2\alpha^2 - n_1^2)\left(\frac{\sigma}{\lambda_1}\right)^{2i-2}\left(1 - \left(\frac{\mu}{\lambda_1}\right)^2\right) \\ n_1^2 + B_{i-1} &\geq n_1^2 + \left(\frac{\mu}{\lambda_1}\right)^{2i-2} > n_1^2. \end{aligned}$$

From Equation (9),

$$\frac{n_1^2 + B_i}{n_1^2 + B_{i-1}} \geq 1 - \frac{(n^2\alpha^2 - n_1^2)\left(\frac{\sigma}{\lambda_1}\right)^{2i-2}\left(1 - (\frac{\mu}{\lambda_1})^2\right)}{n_1^2}$$

Now by equality (8) $\frac{{\lambda^{(i)}}^2}{\lambda_1^2} = \frac{n_1^2 + B_i}{n_1^2 + B_{i-1}}$, achieving the proof. □

To check if the graphs are Ramanujan or not we use the following Corollary.

Corollary 1 *If $x^{(0)}$ verifies the condition (H) of Theorem 1, then the sequence $(\lambda^{(k)})_k$ is growing and converging to $\lambda(G) = \lambda_1$.*

In particular, if $|\lambda^{(k)}| > 2\sqrt{d-1}$ for some k, then the graph is not *Ramanujan. (even if the condition that $x^{(0)}$ must not be orthogonal to the eigenspace of λ_1 is not met, since it implies that the approximates $\lambda^{(i)}$ are even smaller).*

Algorithm There is no built-in functionality in MAGMA to approximate the eigenvalue of graphs. The implementation follows the above power method, with some minor adaptations that allow Cayley graphs, in the following way. As major iterative methods for matrices, the power methods only handle *matrix/vector* products making unnecessary the storage of the whole matrix. This is particularly beneficial here for two reasons: the adjacency matrix is sparse and the product matrix/vector simply amounts to look-up for the neighbors of a given entry (=vertex, denoted $x^{(i)}[\ell]$):

$$x^{(i)}[\ell] = \sum_{\ell' \sim \ell} x^{(i-1)}[\ell']$$

where $x^{(i)}[\ell]$ denotes the ℓ-th entry of the vector $x^{(i)}$, and the neighborhood of the vertex indexed by ℓ is computed within d operations in $\mathbb{O}(\mathbb{F}_q)$. This can be computed in time $O(nd)$, which is almost linear in $O(n)$ since $d \ll n$, still yielding an almost linear time algorithm to compute the vector $x^{(i)}$ from $x^{(i-1)}$.

While the iterations are computed, huge numbers appear but the underlying algorithms in MAGMA are designed to handle exact arithmetic very efficiently and doing numerical approximations in order to reduce the sizes of these numbers did not accelerate substantially the computations. The bottleneck that actually restricts the range of tests is the memory usage limitation to 1Gb. This appears quickly insufficient to store the octonions representing each vertices, all these data being indeed required at each iteration. Neither is provided a parallelization facility by MAGMA that would allow several processes to communicate their results each other.

Algorithm 2: Power method to approximate the 2nd largest eigenvalue

Input: symmetric subset $S = S^{-1}$ of a group or a Moufang loop G
Number of iterations L

Output: Approximation of the 2nd largest eigenvalue $\lambda(\mathscr{G})$ of the Cayley graph $\mathscr{G} = \mathscr{C}ay(G, S)$

1 Generate all elements in normal form in the group or Moufang loop $\langle S \rangle$ `// This allows fast access to coordinates of vector in Line 6 (but requires more memory)`
2 Choose a random vector $x^{(0)} \in \{-1, 0, 1\}^n$ verifying Condition (H) in Theorem 1
3 $N_0 = \|x^{(0)}\|^2$; $N_1 = 0$
4 **for** *i from 1 to L* **do**
5 **for** $\ell \in G$ **do**
6 $x^{(i)}[\ell] = \sum_{g \in S} x^{(i-1)}[\ell \cdot g]$ `// ⌈·⌋ refers to the product in` G
7 $N_1 = N_1 + |x^{(i)}[\ell]|^2$ `// the vertex` $\ell \cdot g$ `is a neighbor of` g
8 **end**
9 $\lambda = \sqrt{N_1}/\sqrt{N_0}$ `// Here,` λ `is equal to` $\lambda^{(i)}$
10 $N_0 = N_1$; $N_1 = 0$
11 **end**
12 **return** λ `// Here,` λ `is equal to` $\lambda^{(L)}$.

Appendix A Preliminaries on octonions

All the material on octonions required for this work is contained in the article of Rehm [25], where a more substantial bibliography can be found. A good complementary material is Ch.9 of [5]. For convenience, we recall the main theorems along with setting notation.

Octonions. We denote by $\mathbb{O}(R)$ (or simply by $\mathbb{O}$ when the meaning of R is clear from the context) the octonion algebra over a commutative ring R, that is the 8-dimensional R-module with canonical basis denoted by $1, \mathsf{i}, \mathsf{j}, \mathsf{k}, \mathsf{t}, \mathsf{it}, \mathsf{jt}, \mathsf{kt}$, usually referred as the *unit bases*. The only rings considered here are $R = \mathbb{Z}, \mathbb{Q}, \mathbb{F}_p$. A unit basis $x \neq 1$ verifies $x^2 = -1$. Here $1, \mathsf{i}, \mathsf{j}, \mathsf{k}$ is the usual quaternion basis and satisfies

$$\mathsf{i}^2 = \mathsf{j}^2 = \mathsf{k}^2 = -1, \ \mathsf{ij} = \mathsf{k}. \tag{10}$$

The *conjugate* of an octonion $\alpha = a_0 + a_1\mathsf{i} + \cdots + a_7\mathsf{kt}$ is $\overline{\alpha} \stackrel{\text{def}}{=} 2a_0 - \alpha$. It is a (ring) antiautomorphism of $\mathbb{O}$, that is a bijection of $\mathbb{O}$ that satisfies for any α, β in $\mathbb{O}$:

$$\begin{aligned} \overline{1} &= 1 \\ \overline{\alpha+\beta} &= \overline{\alpha} + \overline{\beta} \\ \overline{\alpha\beta} &= \overline{\beta}\,\overline{\alpha}. \end{aligned} \tag{11}$$

If we let the quaternion algebra $\mathbb{H}$ be the R-module with basis $1, \mathsf{i}, \mathsf{j}, \mathsf{k}$, then the octonions can be viewed as $\mathbb{O} = \mathbb{H} + \mathbb{H}\mathsf{t}$. The multiplication of octonions is completely determined by the multiplication of quaternions and the rule

$$(\alpha_1 + \alpha_2\mathsf{t})(\beta_1 + \beta_2\mathsf{t}) = \alpha_1\beta_1 - \bar{\beta}_2\alpha_2 + (\beta_2\alpha_1 + \alpha_2\bar{\beta}_1)\mathsf{t} \tag{12}$$

for $\alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathbb{H}$. It is easy to check that the multiplication of octonions is not associative. For instance, if we define a *triad* to be a set of 3 elements among the seven unit bases $\{\mathsf{i}, \mathsf{j}, \mathsf{ij}, \mathsf{t}, \mathsf{it}, \mathsf{jt}, \mathsf{kt}\}$, then it is well known (see [6]) that among the 35 possible triads, only 7 are associative, namely:

$$\mathsf{i},\mathsf{j},\mathsf{k} \quad , \quad \mathsf{i},\mathsf{t},\mathsf{it} \quad , \quad \mathsf{j},\mathsf{t},\mathsf{jt} \quad , \quad \mathsf{k},\mathsf{t},\mathsf{kt}, \quad \text{and} \quad \mathsf{k},\mathsf{jt},\mathsf{it} \quad , \quad \mathsf{j},\mathsf{it},\mathsf{kt} \quad , \quad \mathsf{i},\mathsf{kt},\mathsf{jt}. \tag{13}$$

Each of these associative triads generates, with the additional unit basis 1, a quaternion subalgebra. Octonion algebras are never associative but are *alternative* algebras:

$$\text{(alternative algebra identities)} \qquad (\alpha\alpha)\beta = \alpha(\alpha\beta) \quad \text{and} \quad \beta(\alpha\alpha) = (\beta\alpha)\alpha. \tag{14}$$

These 2 conditions are equivalent to the fact that the trilinear map called *associator* $[a, b, c] = a(bc) - (ab)c$ is alternating. It follows that octonion algebras verify the *Artin theorem*:

Theorem 3 (E. Artin) *In an alternative algebra, any two elements generate an associative subalgebra.*

In our case, we will often use the following corollary

Corollary 2 *Let α, β be elements of $\mathbb{O}(R)$. Then*

$$(\alpha\beta)\bar{\beta} = \alpha(\beta\bar{\beta}) \ , \quad \alpha(\bar{\alpha}\beta) = (\alpha\bar{\alpha})\beta. \tag{15}$$

Octonions are endowed with a quadratic form N, commonly called *norm*. For the specific octonion algebra defined above, the associated bilinear map is simply:

$$\langle\, a_0 + a_1\mathsf{i} + \cdots + a_7\mathsf{kt}\,,\, b_0 + b_1\mathsf{i} + \cdots + b_7\mathsf{kt}\,\rangle = a_0b_0 + \cdots + a_7b_7,$$

meaning that the norm N is a sum of 8 squares. It can be defined equivalently by $N(\alpha) = \alpha\bar{\alpha}$. The fundamental property is the *multiplicativity* of N: $N(\alpha\beta) = N(\alpha)N(\beta)$ for any octonions α and β (it deserves to be emphasized: this property does not hold for division algebras of larger dimension). This rule follows directly from Theorem 3 and the antiautomorphism property (11)

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

Let $\mathbb{O}(R)^\star$ denote the set of invertible octonions. Because if α is invertible, then $\alpha^{-1} = N(\alpha)^{-1}\overline{\alpha}$, we have:

$$\mathbb{O}(R)^\star = \{\alpha \in \mathbb{O}(R) \;:\; N(\alpha) \in R^\star\}.$$

Loops. The set of invertible elements in an alternative ring is a *Moufang loop* (see [3, p. 254] and [5, p. 87-88]). Recall that

Definition 1 (loop) *A* loop *is a set L with a binary operation $*$, such that*
(i) for each a and b in L, there exist unique elements x and y in L such that: $a * x = b$ and $y * a = b$;
(ii) there exists a unique element e such that $x * e = x = e * x$ for all x in L.

It follows that every element of a loop has a unique left and right inverse. A loop where the right and left inverses coincide is an *inverse loop*. In this case, x^{-1} denotes the unique element such that $x * x^{-1} = x^{-1} * x = e$. A *Moufang loop* is a loop satisfying one of the three equivalent following identities:

$$\text{Moufang identities:} \qquad \begin{array}{l} (\alpha\beta\alpha)\gamma = \alpha(\beta(\alpha\gamma)) \\ (\alpha\beta)(\gamma\alpha) = \alpha(\beta\gamma)\alpha \\ ((\beta\alpha)\gamma)\alpha = \beta(\alpha\gamma\alpha) \end{array} \tag{16}$$

It is straightforward to check that a Moufang loop is an inverse loop [5, Ch. 7] or [3, Lemma 2A and 2B, p. 292].

Unique factorization As for integers (and Gauß integers, and integral quaternions), the first step toward a factorization property is an *Euclidean division*[3]. In the quaternion case, unlike what happens with ordinary integers and Gauss integers, two integral quaternions whose norms have a common divisor do not necessarily have a common divisor which is an integral quaternion (consider for instance 2 and $1+\mathsf{i}+\mathsf{j}+\mathsf{k}$). Hurwitz [14, 15] noticed that it is possible to obtain a satisfactory arithmetic of quaternions by considering instead quaternions having its 4 coordinates all in $\mathbb{Z}$, or all in $\frac{1}{2} + \mathbb{Z}$. His result was fully understood after Dickson [9] and his concept of *maximal arithmetic* (also called a maximal order). Recall here that an arithmetic (or an order) for a ring R which is a finite-dimensional algebra over the rational number field $\mathbb{Q}$, is at the same time a subring of R and a finitely generated $\mathbb{Z}$-module which spans R over $\mathbb{Q}$. It is maximal if is not contained in a larger arithmetic. For octonions, there are 7 distinct maximal arithmetics which were identified by Coxeter [6]. They allow as in the case of Hurwitz quaternions to obtain a set of octonions which obey the essential divisibility

[3] or that the *class number of ideals* is equal to 1. But for constructive purposes, the Euclidean division is essential, and anyway, there is no concept of class number in octonion rings.

properties of ordinary integers. Each of them is related to one associative triad in (13). While for quaternions the Euclidean algorithm can then be directly initiated to obtain left and right gcds, the lack of associativity of octonions complicates the matter. Rehm [25, Prop. 4.1], obtained a kind of distortion of the Euclidean algorithm, by using only the alternative property (14). With clever counting arguments, unique factorization follows in a similar fashion to integral quaternions, except that of course some *bracketing* must be specified.

The result of Rehm is stated in the *Coxeter maximal arithmetic* $\mathcal{C}_{\mathbb{O}}$ associated to the associative triad $\mathsf{i},\mathsf{j},\mathsf{k}$. Defining $\mathsf{h}=\frac{1}{2}(\mathsf{i}+\mathsf{j}+\mathsf{k}+\mathsf{t})$, $\mathcal{C}_{\mathbb{O}}$ is the $\mathbb{Z}$-module with basis $1,\mathsf{i},\mathsf{j},\mathsf{k},\mathsf{h},\mathsf{ih},\mathsf{jh},\mathsf{kh}$ (see [6, p. 567], or for a more comprehensive description [5, Fig. 9.1, p. 101]). It contains strictly $\mathbb{O}(\mathbb{Z})$ (and the 6 other maximal arithmetics associated to the 6 other triads are isomorphic to this one). Therein, there are not only 16 units as in $\mathbb{O}(\mathbb{Z})$ but rather 240. Since

$$\begin{aligned}\mathsf{ih} &= \frac{1}{2}(-1-\mathsf{j}+\mathsf{k}+\mathsf{it})\\ \mathsf{jh} &= \frac{1}{2}(-1+\mathsf{i}-\mathsf{k}+\mathsf{jt})\\ \mathsf{kh} &= \frac{1}{2}(-1-\mathsf{i}+\mathsf{j}-\mathsf{kt})\end{aligned}$$

it is straightforward to check that

Lemma 1 *$\mathcal{C}_{\mathbb{O}}$ is the set of octonions of the form $\frac{1}{2}(a_0+a_1\mathsf{i}+a_2\mathsf{j}+a_3\mathsf{k}+a_4\mathsf{t}+a_5\mathsf{it}+a_6\mathsf{jt}+a_7\mathsf{kt})$ where the a_i's are integers satisfying*

$$\begin{aligned}(a_0,a_1,a_2,a_3) &\equiv (a_4,a_5,a_6,a_7) \pmod 2 \ \textit{if}\ a_0+a_1+a_2+a_3\equiv 0 \pmod 2,\\ (a_0,a_1,a_2,a_3) &\equiv (1-a_4,1-a_5,1-a_6,1-a_7) \pmod 2 \ \textit{if}\ a_0+a_1+a_2+a_3\equiv 1 \pmod 2.\end{aligned}$$

Given an octonion $\alpha=a_0+a_1\mathsf{i}+\cdots+a_7\mathsf{kt}\in\mathbb{O}(\mathbb{Q})^\star$, we say that it is positive and write $\alpha>0$ if and only if for the smallest i such that $a_i\neq 0$ one has $a_i>0$. Let p be an odd prime number. Related to *unique* factorization, we define (see [25, Prop. 5.6]):

$$\mathscr{P}(p)\stackrel{\text{def}}{=}\{\alpha\in\mathbb{O}(\mathbb{Z}):\ \alpha>0\ ,\quad N(\alpha)=p\ ,\quad \alpha-1\in 2\mathcal{C}_{\mathbb{O}}\} \tag{17}$$

Rehm proved that $|\mathscr{P}(p)|=p^3+1$ (see [25, Prop. 6.4]). His main result in [25], which is fundamental in the present work, is the following:

Theorem 4 *[25] Let $\alpha\in\mathcal{C}_{\mathbb{O}}$ be primitive, meaning that the gcd of its coefficients in any $\mathbb{Z}$-basis is 1. Suppose that $N(\alpha)=p_1\cdots p_s$ where the p_i's are odd prime integers, not necessarily distinct. There exists a unique $\epsilon\in\mathcal{C}_{\mathbb{O}}^\star$ and unique $\pi_i\in\mathscr{P}(p_i)$ for $i=1,\ldots,s$, such that:*

$$\alpha=\underbrace{\Big(\ldots\big(\big(}_{\text{open brackets}}\epsilon\pi_1\big)\pi_2\big)\pi_3\cdots\Big)\pi_s.$$

Remarks: 1. This writing depends heavily on the order in which the factorization sequence $p_1\cdots p_s$ of $N(\alpha)$ is chosen.

2. The primes p_i are supposed to be odd. Let us mention that Rehm has treated the case of occurrence of primes equal to 2 in the factors of $N(\alpha)$ as well. However, the set of prime octonions of norm 2 presents a more complicated structure which prevents to define graphs in the same way as in the case $p_i>2$.

Appendix B Arithmetic construction of the infinite (p^3+1)-regular tree

Overview of the whole construction. Similarly to [16, 18, 4, 20], the Ramanujan graphs construction of this paper can be decomposed in two steps.
1. The first step consists in constructing the (p^3+1)-regular infinite tree in an arithmetic way by using octonions.
2. Finite regular graphs are derived from this tree by taking suitable finite quotients of it which do not create small cycles.

The first step is detailed in this section. It will also turn out that the construction has a description in terms of Cayley graphs defined over loops. This will be explained in Appendix C.

Preliminary lemmas on the factorization of octonions of norm p^t. The main ingredients used for the construction are the uniqueness of the factorization property of Theorem 4 and considering products of elements of $\mathcal{C}_{\mathbb{O}}$ of the following form

$$\underbrace{\Big(\dots\big(\big(}_{\text{open brackets}}\epsilon\alpha_1\big)\alpha_2\big)\alpha_3\cdots\Big)\alpha_\ell,$$

where $\epsilon \in \mathcal{C}_{\mathbb{O}}^\star$, $\alpha_i \in \mathcal{C}_{\mathbb{O}} - \mathcal{C}_{\mathbb{O}}^\star$ and $\alpha_i \neq \overline{\alpha_{i+1}}$ for $i = 1, \dots, \ell-1$. We say that such products are *irreducible products*. This terminology comes from the fact that products of elements of $\mathcal{C}_{\mathbb{O}}$ that are not irreducible can be simplified by using Corollary 2 of Artin's theorem. We also use the following lemma.

Lemma 2 *Any irreducible product $(\dots((\epsilon\pi_1)\pi_2)\pi_3\cdots)\pi_t$ of a unit ϵ in $\mathcal{C}_{\mathbb{O}}^\star$ by elements $\pi_1, \dots, \pi_t$ of $\mathscr{P}(p)$ is primitive.*

Proof: We proceed by contradiction and consider an irreducible product α of a unit by elements of $\mathscr{P}(p)$ of minimal length that is not primitive. We may write this element as $\alpha = \beta\pi$, where β is a primitive irreducible product of an invertible element and elements of $\mathscr{P}(p)$ and π is an element of $\mathscr{P}(p)$. For an element γ of $\mathcal{C}_{\mathbb{O}}$, let us denote by $c(\gamma)$ the content of γ, which is the largest integer dividing γ (it is also the greatest common divisor of the coefficients of γ in some $\mathbb{Z}$ basis of $\mathcal{C}_{\mathbb{O}}$). Obviously,

$$c(\alpha) | c(\alpha\bar{\pi}) \tag{18}$$

because the coefficients of $\alpha\bar{\pi}$ are integer linear combinations of the coefficients of α in a $\mathbb{Z}$ basis. Since $\alpha\bar{\pi} = (\beta\pi)\bar{\pi} = \beta(\pi\bar{\pi}) = p\beta$ by Corollary 2, we obtain that $c(\alpha\bar{\pi}) = p$. This together with (18) implies that $c(\alpha) = p$ and that p divides α. We may therefore write α as $\alpha = \gamma p = \gamma(\bar{\pi}\pi) = (\gamma\bar{\pi})\pi$ (by using Corollary 2 again) for some $\gamma \in \mathcal{C}_{\mathbb{O}}$. Hence, $\beta = \gamma\bar{\pi}$. But γ is necessarily primitive, since β is primitive. Then by Theorem 4, γ is an irreducible product of a unit ϵ by elements $\pi_1, \dots, \pi_s$ of $\mathscr{P}(p)$:

$$\gamma = (\dots((\epsilon\pi_1)\pi_2)\cdots)\pi_s.$$

This shows that β is of the form

$$\beta = ((\dots((\epsilon\pi_1)\pi_2)\cdots)\pi_s)\bar{\pi}.$$

This is an irreducible product, for if π_s were equal to π, β would be divisible by p and would not be primitive. From Theorem 2 applied to β, this is the only way we can write β as an irreducible product, and therefore the product α is necessarily of the form

$$\alpha = \beta\pi = (((\dots((\epsilon\pi_1)\pi_2)\cdots)\pi_s)\bar{\pi})\pi,$$

contradicting the assumption on its irreducibility. □

Proposition 1 *Any element $\alpha \in \mathbb{O}(\mathbb{Z})$ of norm $N(\alpha) = p^t$ such that $\alpha - 1 \in 2\mathcal{C}_{\mathbb{O}}$, can be uniquely written as:*

$$\alpha = \pm p^s((\dots(\alpha_1\alpha_2)\cdots)\alpha_{t-2s-1})\alpha_{t-2s},$$

where $((\dots(\alpha_1\alpha_2)\cdots)\alpha_{t-2s-1})\alpha_{t-2s}$ is an irreducible product with elements $\alpha_i \in \mathscr{P}(p)$.

Proof: Let $c(\alpha) = p^s$ be the content α (defined in the previous proof). Then $p^{-s}\alpha$ is primitive. Theorem 4 insures existence and uniqueness of elements $\alpha_1, \dots, \alpha_{t-2s} \in \mathscr{P}(p)$ and of a unit $\epsilon \in \mathcal{C}^\star_{\mathbb{O}}$ such that α is written as an irreducible product

$$\alpha = p^s\big(\dots((\epsilon\alpha_1)\alpha_2)\alpha_3\cdots\big)\alpha_{t-2s}. \tag{19}$$

Suppose that α admits another writing as in (19) $\alpha = p^{s'}\big(\dots(\epsilon'\alpha'_1)\alpha'_2\cdots\big)\alpha'_{t-2s'}$. Then necessarily $s' \le s$, otherwise $p^{s'}$ would be larger than the content $c(\alpha)$. And if $s' < s$ then $p^{-s'}\alpha$ would not be primitive, implying that $\big(\dots(\epsilon'\alpha'_1)\alpha'_2\cdots\big)\alpha'_{t-2s'}$ would also not be primitive, in contradiction with Lemma 2. Hence $s = s'$, and the following holds:

$$\big(\dots(\epsilon'\alpha'_1)\alpha'_2\cdots\big)\alpha'_{t-2s'} = \big(\dots(\epsilon\alpha_1)\alpha_2\cdots\big)\alpha_{t-2s}.$$

Both sides are irreducible products which are therefore primitive by Lemma 2. Then Theorem 4 insures that $\epsilon' = \epsilon$ and $\alpha_i = \alpha'_i$ for $i = 1, \dots, t-2s$. Therefore, the writing of α in (19) is unique.

The invertible element ϵ is necessarily in $\mathbb{O}(\mathbb{Z})$. Suppose this is not true, $\epsilon \in \mathcal{C}^\star_{\mathbb{O}} - \mathbb{O}(\mathbb{Z})^\star$. Let us first prove the following

(P) "$a \in \mathcal{C}_{\mathbb{O}} - \mathbb{O}(\mathbb{Z})$ and $b \in 1 + 2\mathcal{C}_{\mathbb{O}}$ implies $ab \in \mathcal{C}_{\mathbb{O}} - \mathbb{O}(\mathbb{Z})$".

Notice that a has necessarily in the $1, \mathsf{i}, \mathsf{j}, \mathsf{k}, \mathsf{t}, \mathsf{it}, \mathsf{jt}, \mathsf{kt}$ basis at least one coordinate which is of the form $\frac{m}{2}$ where m is an odd integer. Write now $ab = a(1 + 2c) = a + 2ac$ for some $c \in \mathcal{C}_{\mathbb{O}}$. But $2ac$ is in $\mathbb{O}(\mathbb{Z})$, which implies that ab has some coordinate of the form $\frac{m}{2} + n$, where n is some integer. This shows that ab is not in $\mathbb{O}(\mathbb{Z})$ and finishes the proof of Property (P).

When we apply this property recursively to $\epsilon\alpha_1$, $(\epsilon\alpha_1)\alpha_2, \dots, \big(\dots((\epsilon\alpha_1)\alpha_2)\cdots\big)\alpha_{t-2s}$, we see that they are all in $\mathcal{C}_{\mathbb{O}} - \mathbb{O}(\mathbb{Z})$, and therefore so is also $\alpha = p^s\big(\dots((\epsilon\alpha_1)\alpha_2)\cdots\big)\alpha_{t-2s}$. This is a contradiction, because α is in $1 + 2\mathcal{C}_{\mathbb{O}}$ and hence also in $\mathbb{O}(\mathbb{Z})$.

Therefore, ϵ is among the 16 units of $\mathbb{O}(\mathbb{Z})^\star$. By using Corollary 2, it is straightforward to check that we can write ϵ as

$$\epsilon = p^{s-t}\big(\dots((\alpha\bar{\alpha}_{t-2s})\bar{\alpha}_{t-2s-1})\cdots\alpha_2\big)\bar{\alpha}_1$$

The set $1 + 2\mathcal{C}_{\mathbb{O}}$ is stable by multiplication, therefore $\big(\dots((\alpha\bar{\alpha}_{t-2s})\bar{\alpha}_{t-2s-1})\cdots\alpha_2\big)\bar{\alpha}_1$ belongs to $1 + 2\mathcal{C}_{\mathbb{O}}$ and so does ϵ. We conclude the proof by observing that the only invertible elements in $\mathbb{O}(\mathbb{Z})^\star$ which are also in $1 + 2\mathcal{C}_{\mathbb{O}}$ are ± 1. □

The construction of the infinite tree This proposition above has a simple corollary, namely that all irreducible products $(\dots(\alpha_1\alpha_2)\cdots\alpha_{s-1})\alpha_s$ of elements of $\mathscr{P}(p)$ are different. These will be the vertices of a tree we want to build.

Definition 2 *Let Λ be the set of all irreducible products with elements in $\mathscr{P}(p)$ (with the convention that the void product belongs to it and is equal to 1).*

Let T be the infinite graph with:

- vertex set Λ;
- edge set defined as follows. By Proposition 1, any vertex can be viewed in a unique way as an irreducible product $(\dots(\alpha_1\alpha_2)\cdots\alpha_{s-1})\alpha_s$ where the α_i's belong to $\mathscr{P}(p)$. There is an edge between $(\dots(\alpha_1\alpha_2)\cdots\alpha_{s-1})\alpha_s$ and vertices of the set

$$\{(\dots(\alpha_1\alpha_2)\cdots)\alpha_{s-1}\} \cup \{((\dots(\alpha_1\alpha_2)\cdots\alpha_{s-1})\alpha_s)\pi : \pi \in \mathscr{P}(p) - \{\overline{\alpha_s}\}\}$$

  By the convention that the void product is equal to 1, the vertex 1 is adjacent to all vertices labeled by π, for $\pi \in \mathscr{P}(p)$.

It is clear by construction of the graph that T is the infinite (p^3+1)-regular tree.

Cayley graphs on loops There is an interpretation of the arithmetic construction of this (p^3+1)-regular tree in terms of a Cayley graph *on a loop*. This is a slight generalization of the usual Cayley graph definition (see for instance [22]) that uses loops instead of groups.

Definition 3 (directed/undirected Cayley graph on a loop) *Let L be a loop and S be a generating set for it. The directed Cayley graph $\overrightarrow{\mathscr{C}ay}(L,S)$ has for vertices the elements of L and for edges $\{(l,ls), l \in L,\ s \in S\}$. The undirected Cayley graph $\mathscr{C}ay(L,S)$ is obtained from $\overrightarrow{\mathscr{C}ay}(L,S)$ by replacing each directed edge (l,ls) by an undirected edge $\{l,ls\}$. Equivalently, there is an edge between l and l' if and only if there exists s in S such that either $l' = ls$ or $l = l's$.*

For the usual Cayley graph on a group, the undirected version is a $|S|$-regular graph without self-loops[4] if and only if $S = S^{-1}$ and $1 \notin S$. There is a generalization of this property for Cayley graphs on loops.

Proposition 2 *[21, Theorem 8] $\mathscr{C}ay(L,S)$ is an $|S|$-regular graph without loops if and only if for all $l \in L$ we have:*
(i) $l \notin lS$,
(ii) $l \in (ls)S$ for any $s \in S$.

Note that if L is a Moufang loop, then this is equivalent to $1 \notin S$ and $S^{-1} = S$, as in a group. Cayley graphs on groups are of course vertex transitive, this is not necessarily the case for Cayley graphs defined on loops. The problem is that left multiplication by a loop element does not necessarily yield a graph automorphism because of the lack of associativity. Indeed, any regular graph can be realized as a Cayley graph on a certain loop [21].

To view the tree T as a Cayley graph on a loop, we endow the vertex set Λ with the following operation

[4] a *self-loop*, that is an edge with the same origin and extremity, should not be confused with the meaning of a *loop* here, i.e. a weaker algebraic structure than a group.

Definition 4 *Let α, β be two elements of Λ. By Proposition 1, these vertices can be written in a unique way as irreducible products over $\mathscr{P}(p)$, $\alpha = (\dots(\alpha_1\alpha_2)\cdots)\alpha_s, \beta = (\dots(\beta_1\beta_2)\cdots)\beta_t$. By using Proposition 1 again, there exists a* unique *irreducible product γ on $\mathscr{P}(p)$ such that $\alpha\beta = \pm p^\ell\gamma$, with $N(\gamma) = p^{s+t-2\ell}$, that is γ is an irreducible product of length $s+t-2\ell$. We define*

$$\alpha * \beta \stackrel{def}{=} \gamma.$$

Proposition 3 *The set Λ endowed with the multiplicative law $*$ is a Moufang loop generated by $\mathscr{P}(p)$.*

Proof: Clearly $1 * \alpha = \alpha * 1 = \alpha$ for any $\alpha \in \Lambda$.

Let α be some element of Λ. It belongs to $1 + 2\mathcal{C}_{\mathbb{O}}$ and is primitive by Lemma 2. This is therefore also the case for $\bar{\alpha}$. By Proposition 1 we know that either $\bar{\alpha}$ or $-\bar{\alpha}$ belongs to Λ. If $\overline{\alpha} \in \Lambda$, then since $\alpha\bar{\alpha} = p^s$ where $p^s = N(\alpha)$, we get $\alpha * \bar{\alpha} = 1$. The case $-\overline{\alpha} \in \Lambda$ is treated similarly. This shows that Λ is a loop. It remains to show that $*$ satisfies the Moufang identities (16).

The following equalities come from the definition of $*$:

$$\begin{aligned} \alpha * (\beta * (\alpha * \gamma)) &= \alpha * (\beta * (p^{-s_1}\alpha\gamma)), \\ &= p^{-s_1}\alpha * (p^{-s_2}\beta(\alpha\gamma)) \\ &= p^{-s_1-s_2}p^{-s_3}\alpha(\beta(\alpha\gamma)) \end{aligned}$$

for some non-negative integers s_1, s_2 and s_3. From the Moufang identities (16), $\alpha(\beta(\alpha\gamma)) = (\alpha\beta\alpha)\gamma$, it comes that $\alpha * (\beta * (\alpha * \gamma)) = (\alpha * \beta * \alpha) * \gamma$. □

With this definition, it is straightforward to check that the one to one mapping between elements of Λ and their representation as irreducible products of elements of $\mathscr{P}(p)$ gives an isomorphism between T and $\mathscr{C}ay(\Lambda, \mathscr{P}(p))$.

Proposition 4 *The following graph isomorphism holds:*

$$T \simeq \mathscr{C}ay(\Lambda, \mathscr{P}(p)).$$

Appendix C Obtaining finite graphs from T by reducing Λ modulo another prime q

Reducing to finite graphs Basically, finite graphs are obtained from the arithmetic construction of T by reducing the octonions in Λ modulo another prime q. For reasons which will appear later on we also assume that q is chosen to be greater than p. Notice that we obtain in this way elements in $\mathbb{O}(\mathbb{F}_q)^\star$, because the norm of elements of Λ is a power of p which is therefore invertible modulo q. Let τ_q denotes the reduction modulo q map, $\tau_q : \mathbb{O}(\mathbb{Z}) \to \mathbb{O}(\mathbb{F}_q)$. By the definition of the product $*$, the following holds:

$$\tau_q(\alpha * \beta) = \tau_q(\epsilon p^{-s}\alpha\beta) = \tau_q(\epsilon p^{-s})\tau_q(\alpha)\tau_q(\beta), \tag{20}$$

for some nonnegative integer s and $\epsilon \in \{-1, 1\}$. We note that $\tau_q(\epsilon p^{-s})$ is in $\mathbb{F}_q^\star$, identified as a subset of $\mathbb{O}(\mathbb{F}_q)^\star$. This subset appears to be precisely the center $\mathcal{Z}$ of $\mathbb{O}(\mathbb{F}_q)^\star$, as is easily verified. It follows that the two elements $\tau_q(\alpha * \beta)$ and $\tau_q(\alpha)\tau_q(\beta)$ differ only by an element in the center. Therefore, they yield the same element in the quotient loop $\mathbb{O}(\mathbb{F}_q)^\star/\mathcal{Z}$. In other words, the map

$$\begin{aligned} \mu_q : \Lambda &\to \mathbb{O}(\mathbb{F}_q)^\star/\mathcal{Z}, \\ \alpha &\mapsto \tau_q(\alpha)\mathcal{Z}. \end{aligned} \tag{21}$$

is a loop homomorphism. Indeed, Equality (20) clearly implies $\mu_q(\alpha * \beta) = \mu_q(\alpha)\mu_q(\beta)$. In addition, $\mathbb{O}(\mathbb{F}_q)^\star$ being a Moufang loop, $\mathbb{O}(\mathbb{F}_q)^\star/\mathcal{Z}$ is itself a Moufang loop. We have proved:

Lemma 3 *The map μ_q is a homomorphism of Moufang loops.*

Our graphs will be defined as $\mathscr{C}ay(\text{Im } \mu_q, \mu_q(\mathscr{P}(p)))$ when these graphs are bipartite or by double covers of these Cayley graphs (which are therefore bipartite) when this is not the case. The reason for this, is that bipartite graphs have only even cycles and we have in the case of $\mathscr{C}ay(\text{Im } \mu_q, \mu_q(\mathscr{P}(p)))$ a very good lower bound on the size of cycles of even length, but the lower bound on cycles of odd length is only half the aforementioned bound.

Determining Im μ_q**.** Let $M_1 \stackrel{\text{def}}{=} \{\alpha \in \mathbb{O}(\mathbb{F}_q)^\star \ : \ N(\alpha) = 1\}$ and $M_p \stackrel{\text{def}}{=} \{\alpha \in \mathbb{O}(\mathbb{F}_q)^\star \ : \ N(\alpha) \text{ is a power of } p\}$. They are Moufang subloops of $\mathbb{O}(\mathbb{F}_q)^\star$ and the inclusions of Moufang loops $M_1 \subset M_p \subset \mathbb{O}(\mathbb{F}_q)^\star$ hold. The central subgroups of M_1 and M_p are respectively $\mathcal{Z}_1 = \mathcal{Z} \cap M_1$, and $\mathcal{Z}_p = \mathcal{Z} \cap M_p$. If we identify $\mathcal{Z}$ with $\mathbb{F}_q^\star$, then $\mathcal{Z}_p = \{\pm p^s, s = 0, 1, \ldots, q-2\}$ and $\mathcal{Z}_1 = \{-1, 1\}$. This gives the following embeddings of Moufang loops:

$$M_1/\mathcal{Z}_1 \hookrightarrow M_p/\mathcal{Z}_p \hookrightarrow \mathbb{O}(\mathbb{F}_q)^\star/\mathcal{Z}. \tag{22}$$

By a result of Paige [24, Theorem 4.1] $M_1/\mathcal{Z}_1$ is a simple Moufang loop, and an index 2 normal subloop[5] of $\mathbb{O}(\mathbb{F}_q)^\star/\mathcal{Z}$ (in total analogy with $PGL_2(\mathbb{F}_q)$ and $PSL_2(\mathbb{F}_q)$). It follows that either $M_p/\mathcal{Z}_p = M_1/\mathcal{Z}_1$ or $\mathbb{O}(\mathbb{F}_q)^\star/\mathcal{Z}$ (see Corollary 3 below for an answer to this issue).

Lemma 4 (the image of μ_q) *We have* Im $\mu_q = M_p/\mathcal{Z}_p$.

Proof: Every element of Λ has norm some power of p, so the inclusion Im $\mu_q \subset M_p/\mathcal{Z}_p$ is clear. To obtain the other inclusion, we first show that for any element $\alpha = a_0 + a_1\mathsf{i} + \cdots + a_7\mathsf{kt} \in \mathbb{O}(\mathbb{Z})$ such that $N(\alpha) \equiv p^r \pmod q$ for some integer r, there exists an element $\beta = b_0 + b_1\mathsf{i} + \cdots + b_7\mathsf{kt} \in 1 + 2\mathcal{C}_\mathbb{O}$ such that
(i) $a_i \equiv b_i \pmod q$,
(ii) $N(\beta) = p^\ell$ for some integer ℓ.

To prove this claim we use as in [16, Prop. 3.3], a result of Malyshev on the number of solutions of integral definite-positive quadratic forms [17]. This result can be described as follows. Let $f(x_1, \ldots, x_n)$ be a quadratic form in $n \geq 4$ variables with integral coefficients and discriminant d. Let m be an integer prime to $2d$. Malyshev proved that there exists some constant depending on f, $K(f)$ such that for any integer $N \geq K(f)$, verifying additionally:
(i) N generic for f (that is $f \equiv N \pmod r$ has at least one solution for every r),
(ii) $\gcd(m, 2Nd) = 1$,
(iii) and for which there exist integers a_i such that $\gcd(a_1, \ldots, a_n, m) = 1$, $f(a_1, \ldots, a_n) \equiv N \pmod m$,
there are integers $b_1, \ldots, b_n$ verifying:

$$b_i \equiv a_i \pmod m \text{ and } f(b_1, \ldots, b_n) = N.$$

Let us first assume that $p \equiv 1 \pmod 4$. We apply the aforementioned result of Malyshev to $f(x_0, \ldots, x_7) \stackrel{\text{def}}{=} x_0^2 + 4(x_1^2 + \cdots + x_7^2)$. This is an integral positive definite quadratic form. The discriminant of f, $d = 2^7$, verifies $\gcd(2dp^\ell, q) = 1$ for any ℓ. There are obviously integers $(a'_0, \ldots, a'_7)$ such that $f(a'_0, \ldots, a'_7) \equiv p^r \pmod q$ by the assumption on α (by taking $a'_0 = a_0$ and $a'_i \equiv 2^{-1}a_i \pmod q$ for $i \in \{1, \ldots, 7\}$), and such that $\gcd(a'_0, \ldots, a'_7, q) = 1$. Now choose

[5] From Corollary of Lemma 3.4 of [24], since $q > p$ is an odd prime.

ℓ such that $p^\ell \geq K(f)$ and $p^\ell \equiv p^r \pmod q$. It is straightforward to check that p^ℓ is generic for f (this follows from the fact that $p^\ell \equiv 1 \pmod 4$ and, for example, the 4 squares theorem). Therefore there exist integers $(b'_0, \ldots, b'_7)$ satisfying

$$b'^2_0 + 4b'^2_1 + \cdots + 4b'^2_7 = p^\ell.$$

This implies the existence of the aforementioned octonion β of norm equal to p^ℓ which is congruent to p^r modulo q by setting $b_0 = b'_0$, $b_i = 2b'_i$ for $i \in \{1, \ldots, 7\}$. This octonion belongs to $1 + 2\mathcal{C}_\mathbb{O}$ since $b_0 \equiv 1 \pmod 2$.

Now, let us consider the remaining case $p \equiv 3 \pmod 4$. We can use the same proof as above for the case where ℓ is even, since in this case $p^\ell \equiv 1 \pmod 4$. In the case of an odd ℓ, p^ℓ is no more generic for f, indeed $f(x_0, \ldots, x_7) \equiv p^\ell \pmod 4$ has no solution: this equation reduces to $x_0^2 \equiv 3 \pmod 4$ which has no solution. In order to treat this case we consider another quadratic form, namely

$$f(x_0, \ldots, x_7) \stackrel{\text{def}}{=} 4(x_0^2 + x_1^2 + x_2^2 + x_3^2 + x_4^2) + x_5^2 + x_6^2 + x_7^2. \tag{23}$$

This time p^ℓ is generic for f. Moreover a solution $(b_0, b_1, \ldots, b_7)$ in $\mathbb{Z}^8$ to the equation $f(x_0, \ldots, x_7) = p^\ell$ gives an element $\beta = 2b_0 + 2b_1\mathsf{i} + 2b_2\mathsf{j} + 2b_3\mathsf{k} + 2b_4\mathsf{t} + b_5\mathsf{it} + b_6\mathsf{jt} + b_7\mathsf{kt}$ of norm p^ℓ. Let us show that β is also in $1 + 2\mathcal{C}_\mathbb{O}$. By reducing Equation (23) modulo 4, we obtain $b_5^2 + b_6^2 + b_7^2 \equiv 3 \pmod 4$, hence:

$$b_5 \equiv b_6 \equiv b_7 \equiv 1 \pmod 2.$$

The element $\frac{\beta - 1}{2} = \frac{2b_0 - 1}{2} + b_1\mathsf{i} + b_2\mathsf{j} + b_3\mathsf{k} + b_4\mathsf{t} + \frac{b_5}{2}\mathsf{it} + \frac{b_6}{2}\mathsf{jt} + \frac{b_7}{2}\mathsf{kt}$ is therefore in $\mathcal{C}_\mathbb{O}$ by using the characterization of $\mathcal{C}_\mathbb{O}$ provided by Lemma 1.

Summing up the whole discussion we obtain in both cases an element β in $1 + 2\mathcal{C}_\mathbb{O}$ of norm p^ℓ. By applying Proposition 1 to it, we can write β as

$$\beta = \epsilon p^s \gamma$$

for some non-negative integer s, ϵ in $\{-1, 1\}$ and γ in Λ. Since $\tau_q(\alpha) = \tau_q(\beta)$ it comes that $\tau_q(\gamma) \in \tau_q(\alpha)\mathcal{Z}_p$ and therefore $\tau_q(\alpha)\mathcal{Z}_p \in \operatorname{Im} \mu_q$. □

Since $M_1/\mathcal{Z}_1$ is of index 2 in $\mathbb{O}(\mathbb{F}_q)^\star/\mathcal{Z}_p$, the image loop $\mu_q\big(\Lambda\big) = M_p/\mathcal{Z}_p$ is either equal to $M_1/\mathcal{Z}_1$ or $\mathbb{O}(\mathbb{F}_q)^\star/\mathcal{Z}$. A direct consequence is:

Corollary 3 *If* $\left(\frac{p}{q}\right) = 1$, *then* $\operatorname{Im}\, \mu_q = M_1/\mathcal{Z}_1$. *Else, when* $\left(\frac{p}{q}\right) = -1$, $\operatorname{Im}\, \mu_q = \mathbb{O}(\mathbb{F}_q)^\star/\mathcal{Z}$.

Proof: The loop homomorphism $\mathbb{O}(\mathbb{F}_q)^\star \to \{-1, 1\}$, $\alpha \mapsto \left(\frac{N(\alpha)}{q}\right)$, regarding the definition of $\mathcal{Z}$, factorizes into this homomorphism: $\varepsilon : \mathbb{O}(\mathbb{F}_q)^\star/\mathcal{Z} \to \{-1, 1\}$. Its kernel contains $M_1/\mathcal{Z}_1$.

Besides, for $\pi \in \mathscr{P}(p)$, $\mu_q(\pi)$ is mapped by ε to 1 or -1 in $\{-1, 1\}$, according to the sign of $\left(\frac{p}{q}\right)$. This shows that if $\left(\frac{p}{q}\right) = -1$, then $\mu_q\left(\mathscr{P}(p)\right) \subset \mathbb{O}(\mathbb{F}_q)^\star/\mathcal{Z} - M_1/\mathcal{Z}_1$. From Lemma 4, we know that $M_1/\mathcal{Z}_1 \subsetneq M_p/\mathcal{Z}_p = \operatorname{Im}\, \mu_q$, from which $\operatorname{Im}\, \mu_q = \mathbb{O}(\mathbb{F}_q)^\star/\mathcal{Z}$ follows by Paige's theorem.

On the other hand, if $\left(\frac{p}{q}\right) = 1$, then $\mu_q\big(\mathscr{P}(p)\big) \subset \ker \varepsilon$. The multiplicativity of the Legendre symbol shows that $\operatorname{Im}\, \mu_q \subset \ker \varepsilon$. It comes, with Lemma 4, $M_1/\mathcal{Z}_1 \subset M_p/\mathcal{Z}_p = \operatorname{Im}\, \mu_q \subsetneq \mathbb{O}(\mathbb{F}_q)^\star/\mathcal{Z}$, and $\operatorname{Im}\, \mu_q = M_1/\mathcal{Z}_1$ by Paige's theorem. □

What is $\ker \mu_q$ **?** By definition, $\ker \mu_q = \{\alpha \in \Lambda \ : \ \tau_q(\alpha) \in \mathcal{Z}\}$. Write $\alpha = a_0 + a_1\mathsf{i} + \cdots + a_7\mathsf{kt}$. This means that $q|a_i$ for $i = 1, \ldots, 7$, and $N(\alpha) \in \mathbb{F}_q^\star$. This last condition is already verified for elements of Λ. If we denote $\Lambda(q) \stackrel{\text{def}}{=} \ker \mu_q$, this gives:

$$\Lambda(q) = \{\alpha \in \Lambda \ : \ q|a_1 \ , \ \ldots \ , \ q|a_7\}, \text{ then } \Lambda/\Lambda(q) \simeq \begin{cases} \mathbb{O}(\mathbb{F}_q)^\star/\mathcal{Z} & \text{if } \left(\frac{p}{q}\right) = -1 \\ M_1/\mathcal{Z}_1 & \text{if } \left(\frac{p}{q}\right) = 1 \end{cases} \tag{24}$$

Definition and properties of $\mathscr{X}_{p,q}$ **and** $\mathscr{Y}_{p,q}$**.** As mentioned before our finite regular graphs will be obtained as Cayley graphs defined over loops.

Definition 5 *We define* $\mathscr{S}(p,q) \stackrel{def}{=} \mu_q\big(\mathscr{P}(p)\big)$*. If* $\left(\frac{p}{q}\right) = -1$ *let* $\mathscr{X}_{p,q}$ *be the Cayley graphs* $\mathscr{C}ay\big(\mathbb{O}(\mathbb{F}_q)^\star/\mathcal{Z}, \mathscr{S}(p,q)\big)$*, and if* $\left(\frac{p}{q}\right) = 1$*, let* $\mathscr{Y}_{p,q}$ *be the Cayley graph* $\mathscr{C}ay\big(M_1/\mathcal{Z}_1, \mathscr{S}(p,q)\big)$*.*

We have $|\mathbb{O}(\mathbb{F}_q)^\star/\mathcal{Z}| = q^7 - q^3$ [25, Lemma 3.2]. It follows that $|\mathscr{X}_{p,q}| = q^7 - q^3$ and $|\mathscr{Y}_{p,q}| = \frac{1}{2}(q^7 - q^3)$.

Lemma 5 *The graphs* $\mathscr{X}_{p,q}$ *and* $\mathscr{Y}_{p,q}$ *are connected.*

Proof: The set $\mathscr{P}(p)$ generates Λ as a loop. The proof of Corollary 3 showed that $\mathscr{S}(p,q)$ generates $M_1/\mathcal{Z}_1$ if $\left(\frac{p}{q}\right) = 1$, and $\mathbb{O}(\mathbb{F}_q)^\star/\mathcal{Z}$ if $\left(\frac{p}{q}\right) = -1$. It follows that the graphs $\mathscr{X}_{p,q}$ and $\mathscr{Y}_{p,q}$ are all connected. □

Before giving the degree regularity of these graphs, we recall that $|\mathscr{P}(p)| = p^3 + 1$ by [25, Proposition 6.4].

Proposition 5 *The graphs* $\mathscr{X}_{p,q}$ *and* $\mathscr{Y}_{p,q}$ *are* (p^3+1)*-regular.*

Proof: First let us show that $|\mathscr{S}(p,q)| = |\mathscr{P}(p)| = p^3+1$. Suppose that two distinct elements π and π' in $\mathscr{P}(p)$ give the same element in $\mathbb{O}(\mathbb{F}_q)^\star/\mathcal{Z}$ through μ_q. The equality $\tau_q(\pi)\mathcal{Z} = \tau_q(\pi')\mathcal{Z}$ is equivalent to $\pi * \overline{\pi'} \in \ker \mu_q = \Lambda(q)$. By Equation (24), taking norms gives an equation of the form $p^2 = a_0^2 + q^2x^2$, for an a_0 and x. If $x \neq 0$, then $p^2 \geq q^2$, which is excluded by $p < q$. If $x = 0$, then $\pi * \overline{\pi'} \in \mathcal{Z}$, that is $\pi = \pi'$, also excluded. Finally, $\mu_q(\pi) = \mu_q(\pi')$ is impossible if $\pi \neq \pi'$.

To prove that they are $|\mathscr{S}(p,q)|$-regular, we must show that $\mathscr{S}(p,q)$ satisfies the hypotheses of Proposition 2, as aforementioned. We already know that if $\pi \in \mathscr{P}(p)$ then its inverse for $*$ is $\overline{\pi}$ and is in $\mathscr{P}(p)$. Hence, $\mathscr{P}(p)^{-1} = \mathscr{P}(p)$ for $*$, and since μ_q is an homomorphism by Lemma 3 also holds $\mathscr{S}(p,q)^{-1} = \mathscr{S}(p,q)$. Last, $1\mathcal{Z} \notin \mathscr{S}(p,q)$, or else there would be a $\pi \in \mathscr{P}(p)$ that would also be in $\Lambda(q)$ by Equation (24), which is clearly impossible. □

Proposition 6 *The graphs* $\mathscr{X}_{p,q}$ *are bipartite, and the graphs* $\mathscr{Y}_{p,q}$ *are not.*

Proof: First, assume that $\left(\frac{p}{q}\right) = -1$ (this concerns $\mathscr{X}_{p,q}$). Consider the partition $\mathcal{A} \cup \mathcal{B} = \mathbb{O}(\mathbb{F}_q)^\star/\mathcal{Z}$ of the set of vertices of $\mathscr{X}_{p,q}$:

$$\mathcal{A} = M_1/\mathcal{Z}_1 \qquad \text{and} \qquad \mathcal{B} = \mathbb{O}(\mathbb{F}_q)^\star/\mathcal{Z} - M_1/\mathcal{Z}_1.$$

Let $v \in \mathcal{A}$ be a vertex with $v = \mu_q(\alpha)$, and let $w = \mu_q(\beta)$ be a neighbor of v. By construction of Cayley graphs, there exists $\pi \in \mathscr{P}(p)$, such that $\mu_q(\alpha * \pi) = \mu_q(\alpha)\mu_q(\pi) = \mu_q(\beta)$. This leads to:

$$\left(\frac{N(\beta)}{q}\right) = \left(\frac{N(\alpha)p}{q}\right) = \left(\frac{p}{q}\right) = -1,$$

since $v \in \mathcal{A}$ implies $\left(\frac{N(\alpha)}{q}\right) = 1$. This means that $w \in \mathcal{B}$. In the same way any neighbor x of w is in $\mathcal{A}$, so the graph is bipartite.

Now assume that $\left(\frac{p}{q}\right) = 1$ (this concerns the graphs $\mathscr{Y}_{p,q}$). As seen above, a bipartition $\mathcal{A} \cup \mathcal{B}$ of the set of vertices $M_1/\mathcal{Z}_1$ would imply a non trivial loop homomorphism:

$$M_1/\mathcal{Z}_1 \to \{-1, 1\}.$$

The kernel of it would consist of a non trivial normal subloop of $M_1/\mathcal{Z}_1$, which is impossible since $M_1/\mathcal{Z}_1$ is simple by Paige's theorem. □

Lemma 6 *The length $2t$ of each cycle in $\mathscr{X}_{p,q}$ going through the identity verifies $2t > 4\log_p q - 2\log_p 2 = \frac{12}{7}\log_{p^3} |\mathscr{X}_{p,q}| - 2\log_p 2$.*

PROOF: Let β be an irreducible product of length $2t$ such that $\mu_q(\beta) \in \Lambda(q)$, and let $\beta_1, \ldots, \beta_{2t}$ its $2t$ letters. This corresponds to a cycle path without backtracking going through the vertex identity of $\mathbb{O}(\mathbb{F}_q)^\star/\mathcal{Z}$, regarding that $\mu_q(1) = \ker \mu_q = \mathcal{Z}$. Thus β can be written as follows $\beta = b_0 + q(b_1\mathsf{i} + \cdots + b_7\mathsf{kt})$ where the b_i's are integer coefficients. Moreover, $N(\beta) = p^{2t}$, yielding the equation:

$$b_0^2 + q^2(b_1^2 + \cdots + b_7^2) = p^{2t}. \tag{25}$$

At least one b_i (with $i > 0$) is non zero, or else $\beta = b_0$ would yield an irreducible product of length 0, in contradiction with the assumption $t > 0$. This implies $p^{2t} \equiv b_0^2 \pmod{q^2}$, or equivalently $p^t \equiv \pm b_0 \pmod{q^2}$. Observe that $b_0^2 < p^{2t}$, so $|b_0| < p^t$, and $p^t = \pm b_0 + mq^2$, for a positive integer m. This implies

$$\begin{aligned} p^{2t} &= (p^t - mq^2)^2 + q^2(b_1^2 + \cdots + b_7^2) \\ &= p^{2t} - 2mq^2p^t + m^2q^4 + q^2(b_1^2 + \cdots + b_7^2) \end{aligned}$$

Equivalently, $2mp^t - m^2q^2 = b_1^2 + \cdots + b_7^2$. It follows that $2p^t - mq^2 > 0$. This is because at least one b_i (with $i > 0$) is different from 0. Therefore $t > 2\log_p q - \log_p 2$. □

Appendix D Reference tables of Section "Experimental Results"

Construction of $H_{p,q}$ takes: 0.780 s		
Construction of $x^{(0)}$ takes: 0.016 s		
Adjacency table built in: 11.840 s		
iteration nb.	time (sec)	$\lambda(Y_{37,41})$ approx.
5	0.358	10.434716
10	0.405	11.047467
15	0.577	11.286008
20	0.577	11.434530
25	0.499	11.535968
28	0.531	11.580817
29	0.578	11.593612
30	0.577	11.605451
31	0.577	11.616401

Table 4: Non-bipartite Ramanujan graphs $Y_{37,41}$ of degree 38 and order $\frac{1}{2}(41^3 - 41) = 34,440$ (Ramanujan's bound: $2\sqrt{37} \approx 12.165$)

Construction of $H_{p,q}$ takes: 18.954 s		
Construction of $x^{(0)}$ takes: 0.827 s		
Adjacency table built in: 172.958 s		
iteration nb.	time (sec)	$\lambda(Y_{37,71})$ approx.
5	8.237	10.574894
10	8.596	11.338621
15	10.717	11.615755
20	10.686	11.757395
25	10.515	11.837835
30	10.748	11.886180
35	10.639	11.916605
40	9.828	11.936646
45	9.890	11.950488
50	10.281	11.960524
51	10.187	11.962210
52	10.250	11.963809
53	10.203	11.965328
54	10.234	11.966775

Table 5: Non-bipartite Ramanujan graphs $Y_{37,71}$ of degree 38 with $\frac{1}{2}(71^3 - 71) = 178,920$ (Ramanujan's bound: $2\sqrt{37} \approx 12.165$)

Construction of $H_{p,q}$ takes: 60.030 s		
Construction of $x^{(0)}$ takes: 5.772 s		
Adjacency table built in: 1222.502 s		
iteration nb.	time (sec)	$\lambda(X_{37,109})$ approx.
5	59.452	10.557072
10	66.145	11.283166
15	72.884	11.545344
20	73.461	11.682997
25	72.494	11.770558
30	74.584	11.832848
35	74.101	11.879901
40	74.444	11.916577
45	72.088	11.945661
50	73.617	11.968980
55	74.600	11.987837
60	73.258	12.003205
65	74.865	12.015826
70	74.615	12.026275
75	72.463	12.034995
80	73.430	12.042331
85	74.819	12.048555
90	75.005	12.053879
95	72.369	12.058470
100	75.848	12.062460

Table 6: Bipartite Ramanujan graphs $X_{37,109}$ of degree 38 and order $109^3 - 109 = 1,294,920$ (Ramanujan's bound: $2\sqrt{37} \approx 12.165$)

Construction of $H_{p,q}$ takes: 21.700 s		
Construction of $x^{(0)}$ takes: 2.012 s		
Adjacency table built in: 636.235 s		
iteration nb.	time (sec)	$\lambda(X_{47,83})$ approx.
5	33.197	11.892675
10	39.796	12.754317
15	41.200	13.058563
20	42.323	13.205139
25	40.342	13.290773
30	42.510	13.348382
35	42.104	13.390707
40	42.900	13.423511
45	41.340	13.449890
50	42.370	13.471756
55	40.498	13.490388
58	41.621	13.500396

Table 8: Non-bipartite Ramanujan graph of degree 48 and order $\frac{1}{2}(83^3 - 83) = 571,704$ (Ramanujan's bound: $2\sqrt{47} \approx 13.711$)

Construction of $H_{p,q}$ takes: 1.779 s		
Construction of $x^{(0)}$ takes: 0.031 s		
Adjacency table built in: 34.258 s		
iteration nb.	time (sec)	$\lambda(Y_{47,53})$ approx.
5	1.030	11.718370
10	1.622	12.579286
15	1.997	12.909203
20	1.841	13.076825
25	1.856	13.180004
29	1.966	13.238521
30	1.982	13.250846
31	1.996	13.262404
32	1.982	13.273255

Table 7: Non-bipartite Ramanujan graph $Y_{47,53}$ of degree 48 and order $\frac{1}{2}(53^3-53) = 74412$ (Ramanujan's bound: $2\sqrt{47} \approx 13.711$)

Construction of $H_{p,q}$ takes: 16.723 s		
Construction of $x^{(0)}$ takes: 1.420 s		
Adjacency table built in: 1535.611 s		
time (sec)	iteration nb.	$\lambda(X_{47,113})$ approx.
5	70.419	11.928329
10	90.605	12.803581
15	94.271	13.123996
20	88.531	13.294066
25	88.188	13.398118
30	92.602	13.466084
33	90.418	13.495743
34	90.106	13.504235
35	90.293	13.512125
36	90.762	13.519464

Table 9: Non-bipartite Ramanujan graph of degree 48 and order $\frac{1}{2}(113^3 - 113) = 1,442,784$ (Ramanujan's bound: $2\sqrt{47} \approx 13.711$)

Construction of $H_{p,q}$ takes: 0.936 s		
Construction of $x^{(0)}$ takes: 0.047 s		
Adjacency table built in: 20.873 s		
iteration nb.	time (sec)	$\lambda(\mathscr{X}_{3,5})$ approx.
5	0.670	9.5978624
10	0.764	11.054285
15	1.108	11.574964
20	1.092	11.802923
25	1.077	11.906630
28	1.029	11.939458

Table 10: Proof that the degree $28 = 3^3 + 1$-regular bipartite octonion based graph $\mathscr{X}_{3,5}$ of order $5^7 - 5^3 = 78,000$ is not Ramanujan (Ramanujan bound: $2\sqrt{27} \approx 10.392$)

Construction of $H_{p,q}$ takes: 12.995 s		
Construction of $x^{(0)}$ takes: 0.765 s		
Adjacency table built in: 505.318 s		
iteration nb.	time (sec)	$\lambda(\mathscr{X}_{3,7})$ approx.
5	21.747	9.1201917
10	23.416	10.259195
15	29.095	11.293992
20	28.923	11.854913
25	28.486	12.053509
30	29.375	12.132786
32	29.343	12.151599

Table 11: Proof that the degree $28 = 3^3 + 1$-regular bipartite octonion based graph $\mathscr{X}_{3,7}$ of order $7^7 - 7^3 = 8,232,000$ is not Ramanujan. (Ramanujan bound: $2\sqrt{27} \approx 10.392$)

Construction of $H_{p,q}$ takes: 741.426 s		
Construction of $x^{(0)}$ takes: 63.165 s		
No adjacency table built (> 1Gb memory)		
iteration nb.	time (sec)	$\lambda(\mathscr{Y}_{3,11})$ approx.
1	9543.127	5.2904058
2	9539.321	7.4130549
3	9531.754	8.2581244
4	9525.639	8.7245532
5	9855.504	9.0238248
6	9848.281	9.2342039
7	9958.667	9.3916022
8	9771.716	9.5148749
9	9539.243	9.6149043
Memory failure (> 1Gb) at the 10^{th} iteration		

Table 12: Evidence that the degree $28 = 3^3 + 1$-regular non- bipartite octonion based graph $\mathscr{Y}_{3,11}$ of order $\frac{1}{2}(11^7 - 11^3) = 9,742,920$ vertices is not Ramanujan. (the 9 iterations do not overtake the Ramanujan bound: $2\sqrt{27} \approx 10.392$, but more iterations would)

Graphs	Bipartite	Order	Girth Range	time (sec)	girth
$X_{11,13}$	yes	2184	4 6	0.00	6
$X_{11,17}$	yes	4896	6	0.01	6
$Y_{11,19}$	no	3420	3 ...	0.03	6
$X_{11,23}$	yes	12144	6	0.00	6
$X_{11,29}$	yes	24360	6 8	0.00	6
$X_{11,31}$	yes	29760	6 8	0.00	6
$Y_{11,37}$	no	25308	3 ...	0.06	7
$X_{11,41}$	yes	68880	6 8	0.04	8
$Y_{11,43}$	no	39732	3 ...	0.04	7
$X_{11,47}$	yes	103776	6 8	0.04	8
$Y_{11,53}$	no	74412	4 ...	0.04	7
$X_{11,59}$	yes	205320	8	0.04	8
$X_{11,61}$	yes	226920	8	0.06	8
$X_{11,67}$	yes	300696	8	0.04	8
$X_{11,71}$	yes	357840	8	0.04	8
$X_{11,73}$	yes	388944	8	0.06	8
$Y_{11,79}$	no	246480	4 ...	1.02	8
$Y_{11,83}$	no	285852	4 ...	1.02	8
$Y_{11,89}$	no	352440	4 ...	1.04	8
$Y_{11,97}$	no	456288	4 ...	1.06	9

Table 13: Girth of degree 12 Ramanujan graphs for primes q raging from 13 to 97. Column "Girth range" displays the possible theoretical values predicted by Inequality (5), and $x \ldots$ means values "x and larger"

Graphs	Bipartite	Order	Girth Range	time (sec)	girth
$X_{107,109}$	yes	1294920	4 6	.37	6
$X_{107,113}$	yes	1442784	4 6	.37	6
$Y_{107,127}$	no	1024128	2 ...	0.00	3
$Y_{107,131}$	no	1123980	2 ...	.25	5
$Y_{107,137}$	no	1285608	2 ...	.23	5
$Y_{107,139}$	no	1342740	2 ...	.26	5
$Y_{107,149}$	no	1653900	2 ...	0.00	3
$X_{107,151}$	yes	3442800	4 6	.39	6
$X_{107,157}$	yes	3869736	6	.37	6
$X_{107,163}$	yes	4330584	6	.39	6
$Y_{107,167}$	no	2328648	3 ...	.37	5
$X_{107,173}$	yes	5177544	6	.37	6
$Y_{107,179}$	no	2867580	3 ...	.21	5
$X_{107,181}$	yes	5929560	6	.39	6
$Y_{107,191}$	no	3483840	3 ...	.53	5
$Y_{107,193}$	no	3594432	3 ...	.32	5
$Y_{107,197}$	no	3822588	3 ...	.26	5
$X_{107,199}$	yes	7880400	6	.39	6
$Y_{107,211}$	no	4696860	3 ...	.23	5
$X_{107,223}$	yes	11089344	6	.39	6
$X_{107,227}$	yes	11696856	6	.39	6
$X_{107,229}$	yes	12008760	6	.39	6
$Y_{107,233}$	no	6324552	3 ...	.35	5
$X_{107,239}$	yes	13651680	6	.40	6
$Y_{107,241}$	no	6998640	3 ...	.68	5
$X_{107,251}$	yes	15813000	6	.39	6
$X_{107,257}$	yes	16974336	6	.39	6
$X_{107,263}$	yes	18191184	6	.43	6
$X_{107,269}$	yes	19464840	6	.39	6
$X_{107,271}$	yes	19902240	6	.37	6
$X_{107,277}$	yes	21253656	6	.39	6
$X_{107,281}$	yes	22187760	6	.39	6
$X_{107,283}$	yes	22664904	6	.39	6
$Y_{107,293}$	no	12576732	3 ...	.57	5
$Y_{107,307}$	no	14467068	3 ...	1.80	5
$Y_{107,311}$	no	15039960	3 ...	524.13	6
$Y_{107,313}$	no	15331992	3 ...	.40	5
$X_{107,317}$	yes	31854696	6	.37	6
$X_{107,331}$	yes	36264360	6	.43	6
$Y_{107,337}$	no	19136208	3 ...	563.19	6
$Y_{107,347}$	no	20890788	3 ...	.63	5
$X_{107,349}$	yes	42508200	6	.39	6
$X_{107,353}$	yes	43986624	6	.39	6
$Y_{107,359}$	no	23133960	3 ...	.60	5
$Y_{107,367}$	no	24715248	3 ...	534.10	6
$Y_{107,373}$	no	25947372	3 ...	.63	5
$Y_{107,379}$	no	27219780	3 ...	562.44	6
$X_{107,383}$	yes	56181504	6	.43	6
$X_{107,389}$	yes	58863480	6	.37	6
$Y_{107,397}$	no	31285188	3 ...	591.26	6
$X_{107,401}$	yes	64480800	6	.39	6
$X_{107,409}$	yes	68417520	6	.40	6
$Y_{107,419}$	no	36779820	3 ...	631.96	6
$Y_{107,421}$	no	37309020	3 ...	1.49	5
$X_{107,431}$	yes	80062560	6	.59	6
$X_{107,433}$	yes	81182304	6	.43	6
$X_{107,439}$	yes	84604080	6	.54	6
$Y_{107,443}$	no	43468932	3 ...	.71	5
$X_{107,449}$	yes	90518400	6	.68	6
$Y_{107,457}$	no	47721768	3 ...	643.70	6
$Y_{107,461}$	no	48985860	3 ...	640.50	6
$X_{107,463}$	yes	99252384	6	.40	6
$X_{107,467}$	yes	101847096	6	.70	6
$Y_{107,479}$	no	54950880	3 ...	669.58	6
$Y_{107,487}$	no	57750408	3 ...	639.60	6
$Y_{107,491}$	no	59185140	3 ...	638.04	6
$Y_{107,499}$	no	62125500	3 ...	.32	5

Table 14: Degree 108 Ramanujan graphs of various order, and their girth. Column "Girth Range" displays possible values of the girth as predicted from theoretical bound (5), and $x \ldots$ means values "x and larger". Column "girth" displays the actual computed girth, and the column "time" the time required to find it.

Acknowledgment

We would like to thank Eiichi Bannai for having pointing out the result of Paige [24] to us. Many thanks also to Shotaro Makisumi for his pertinent comments and computations.

References

[1] N. L. Biggs and A. G. Boshier. Note on the girth of Ramanujan graphs. *J. Combin. Theory Ser. B*, 49(2):190–194, 1990.

[2] C. Boutsidis, A. Gittens, and P. Kambadur. Spectral clustering via the power method-provably. In *Proceedings of the 24th International Conference on Machine Learning (ICML)*, 2015.

[3] R. H. Bruck. Contributions to the theory of loops. *Trans. Amer. Math. Soc.*, 60:245–354, 1946.

[4] P. Chiu. Cubic Ramanujan graphs. *Combinatorica*, 12(3):275–285, 1992.

[5] J. Conway and D. Smith. *On quaternions and octonions*. A.K. Peters, 2003.

[6] H. S. M. Coxeter. Integral Cayley numbers. *Duke Math. J.*, 13:561–578, 1946.

[7] X. Dahan. Regular graphs of large girth and arbitrary degree. *Combinatorica*, 34(4):407–426, 2014.

[8] G. Davidoff, P. Sarnak, and A. Valette. *Elementary number theory, group theory, and Ramanujan graphs*, volume 55 of *London Math. Soc. Student Texts*. Cambridge U. Press, 2003.

[9] L. E. Dickson. Algebras and their arithmetics. *Bull. Amer. Math. Soc.*, 30(5-6):247–257, 1924.

[10] R. G. Gallager. *Low density parity check codes*. M.I.T. Press, 1963. Monograph.

[11] Gene H Golub and Charles F Van Loan. *Matrix computations*, volume 3. JHU Press, 2012.

[12] T.S. Griggs, J. Širáň, and R.B. Richter. Graphs obtained from moufang loops and regular maps. *Journal of Graph Theory*, 70(4):427–434, 2012.

[13] S. Hoory, N. Linial, and A. Wigderson. Expander graphs and their applications. *Bull. Amer. Math. Soc. (N.S.)*, 43(4):439–561 (electronic), 2006.

[14] A. Hurwitz. Über die Zahlentheorie der Quaternionen. *Nachr. Akad. Wiss. Göttingen*, pages 313–340, 1896.

[15] A. Hurwitz. *Vorlesungen über die Zahlentheorie der Quaternionen*. Berlin, J. Springer, 1919.

[16] A. Lubotzky, R. Phillips, and P. Sarnak. Ramanujan graphs. *Combinatorica*, 8(3):261–277, 1988.

[17] Malyshev. On the representation of integers by positive definite quadratic forms (*in Russian*). *Trudy Math. Inst. Steklov*, 65:3–212, 1962.

[18] G. A. Margulis. Explicit group-theoretic constructions of combinatorial schemes and their applications in the construction of expanders and concentrators. *Problemy Peredachi Informatsii*, 24(1):51–60, 1988.

[19] G.A. Margulis. Explicit constructions of graphs without short cycles and low density codes. *Combinatorica*, 2(1):71–78, 1982.

[20] M. Morgenstern. Existence and explicit constructions of $q + 1$-regular Ramanujan graphs for every prime power q. *J. Combin. Theory Ser. B*, 62(1):44–62, 1994.

[21] E. Mwambene. Characterisation of regular graphs as loop graphs. *Quaest. Math.*, 28(2):243–250, 2005.

[22] E. Mwambene. Cayley graphs on left quasi-groups and groupoids representing k-generalised Petersen graphs. *Discrete Math.*, 309(8):2544–2547, 2009.

[23] A. Nilli. On the second eigenvalue of a graph. *Discrete Mathematics*, 91(2):207 – 210, 1991.

[24] L.J. Paige. A class of simple Moufang loops. *Proc. Amer. Math. Soc.*, 7:471–482, 1956.

[25] H.P. Rehm. Prime factorization of integral Cayley octaves. *Ann. Fac. Sci. Toulouse Math. (6)*, 2(2):271–289, 1993.

[26] R. M. Tanner. A recursive approach to low complexity codes. *IEEE Trans. on Inform. Theory*, 27(5):533–547, 1981.

[27] L. Trevisan. CS359G Lecture 7: Computing Eigenvectors, 2011. `https://lucatrevisan.wordpress.com/2011/01/29/cs359g-lecture-7-computing-eigenvectors/`[Online; accessed 23-September-2016].

[28] L. Trevisan. CS359G Lecture 8: The Leighton-Rao relaxation, 2011. `https://lucatrevisan.wordpress.com/2011/02/02/cs359g-lecture-8-the-leighton-rao-relaxation/` [Online; accessed 23-September-2016].

[29] L. Trevisan. The Alon-Boppana theorem, 2014. `https://lucatrevisan.wordpress.com/2014/09/01/the-alon-boppana-theorem-2/` [Online; accessed 23-September-2016].