# Ramanujan graphs of very large girth based on octonions

X. Dahan and J.-P. Tillich

November 16, 2010

**Abstract**

We present a generalization of the construction of graphs by Lubotzky, Phillips and Sarnak in their celebrated article "Ramanujan graphs" [32]. The new approach consists in using octonion algebras rather than quaternions. A key tool is the existing result of the unique factorization of integral octonions. The families obtained by this mean present not only the same spectral property that make them good expanders, but also show a larger girth, yielding a new record for regular graphs.

## 1 Introduction

**Ramanujan graphs and expanders.** Given a $k$-regular undirected graph $G_{n,k}$ of size $n$, the eigenvalues $\lambda_0 \geq \lambda_1 \geq \cdots \geq \lambda_{n-1}$ of the adjacency matrix of $G_{n,k}$, are real (it is a symmetric matrix) and satisfy $|\lambda_i| \leq k$. Moreover, $\lambda_0 = k$ and if the graph is connected, then $\lambda_1 < k$. The graph is bipartite if and only if $\lambda_{n-1} = -k$. The graph $G$ is a *Ramanujan graph* if all its eigenvalues distinct from $\pm k$ are in the interval $[-2\sqrt{k-1}, 2\sqrt{k-1}]$. Ramanujan graphs are in a sense (asymptotically) extremal graphs with respect to the second largest eigenvalue in absolute value because of the following lower bound due to Alon and Boppana [1]

$$\underline{\lim}_{n} \lambda(G_{n,k}) \geq 2\sqrt{k-1},$$

where $\lambda(G_{n,k})$ denotes the second largest eigenvalue in absolute value of $G_{n,k}$.

The fact that $\lambda(G_{n,k})$ is so small implies many other properties since they are then good *expander* graphs. Graphs with large expansion have proved to be a quite useful object in various domains ranging from mathematics and computer science to physics, see the survey [23] which depicts some of these applications. Random $k$-regular graphs are known to typically meet such a behavior (see for instance [8] and [42] for the first existence results of good expanders obtained by probabilistic arguments). However, even if this kind of probabilistic argument shows the existence of graphs with large expansion, it does not provide explicit examples of graphs which are good expanders. The approach consisting in generating a graph randomly and then checking whether or not it has large expansion is considered to be impracticable: even checking a weak form of expansion turns out to be coNP-complete [6]. It has been observed that this problem can be circumvented by relating the expansion properties to the spectral gap (that is $\lambda_0 - \lambda_1$) or to $\lambda(G_{n,k})$, see for instance [1]: the expansion coefficient can be lower bounded by an increasing function of the spectral gap or $\lambda(G_{n,k})$. Since these spectral quantities can be computed efficiently with an arbitrary precision, this gives an efficient method for obtaining graphs displaying at least a certain amount of expansion. Up to now, this spectral method has proved to be the best method for certifying a rather large expansion. Ramanujan graphs represent here the graphs with the best *certified* expansion properties known. At the moment, Ramanujan graphs have been superseded only in one case, namely for the expansion of small subsets of vertices [29]: graphs obtained by the zigzag product [52] have a better certified expansion in this case. The guaranteed expansion obtained by taking Ramanujan graphs together with the aforementioned spectral lower bound on the expansion is not as large as the one known for random graphs, however it is generally sufficient and satisfactory for many applications.

Obtaining explicit infinite families of Ramanujan graphs of a given degree has been quite a breakthrough in spectral graph theory. The first constructions of this kind were obtained by Lubotzky-Philips-Sarnak [32] and Margulis [35]. They were followed by the constructions of [43, 10, 37, 28] for instance. From them, Ramanujan graphs have been obtained for all degrees $k$ of the form $k = q + 1$ where $q$ is any prime power.

**Graphs of large girth.** Besides their expansion property, the Ramanujan graphs constructed in [32, 35, 10, 37] presented another breakthrough. They had a *large girth* (the girth being the smallest size of its cycles) and improved significantly the narrow knowledge on this matter. Let us mention (see for instance [2, p.154]) the following upper bound for the girth,

$$\text{for } k \geq 3, \text{ any } k\text{-regular graph } G \text{ verifies:} \qquad \text{girth}(G) \leq 2 \log_{k-1} |G|, \tag{1}$$

where $|G|$ denotes the number of vertices of $G$ and $\text{girth}(G)$ is the girth $G$. This bound motivates the following definition of Biggs [3]. A family $\{G_i\}_i$ of $k$-regular graphs is of *large girth* if and only if there exists some positive constant $\gamma$ such that for any graph in this family we have

$$\text{girth}(G_i) \geq \gamma \log_{k-1} |G_i|. \tag{2}$$

For a long time, the best result in this direction was the non constructive result of Erdős and Sachs [18] and its improvements by Sauer and Walther (for more details see [7, p. 107]) which showed the existence of families of graphs with $\gamma = 1$. The first explicit constructions were obtained by Margulis [34] but achieved constants $\gamma$ which were strictly smaller than 1. Proving that there exist families of graphs with a value of $\gamma$ greater than 1 was finally obtained in [51] for a family of graphs of degree $k = 3$ suggested by [5], by showing that for these graphs the following inequality holds

$$\text{girth}(G_i) > \frac{4}{3} \log_{k-1} |G_i| - 2.$$

As suggested by [20], large girth needs not be an unusual property for some families of graphs, but those with a constant $\gamma > 1$ tends to be very seldom [1]. The bipartite Ramanujan graphs constructed in [32, 35] also achieved the constant $\gamma = \frac{4}{3}$ but this time for all degrees of the form $k = p + 1$, where $p$ is a prime number strictly greater than 2 (originally, only for the primes $p \equiv 1 \pmod 4$, and for any odd primes, see [13]). Ramanujan graphs of degree 3 which achieved $\gamma = \frac{4}{3}$ were obtained afterwards in [10]. Moreover, Morgenstern in [37] finally obtained infinite families of Ramanujan graphs achieving $\gamma = \frac{4}{3}$ for all degrees of the form $k = q + 1$ where $q$ is any prime power. These Ramanujan constructions do not only overcome the $\gamma = 1$ barrier, they are also explicit which is essential for applications. It should also be mentioned that a quite different graph construction has been proposed in [30] for degrees of the form $k = q$ where $q$ is a prime power, and where it has been shown that it contains connected components $G_i$ which satisfy the inequality

$$\text{girth}(G_i) \geq \frac{4}{3} \log_k (k-1) |G_i|,$$

which is slightly worse than the constant $\gamma = \frac{4}{3}$ achieved in the aforementioned articles but achieves it asymptotically as the degree $k$ goes to infinity.

[1] To quote [20], “it is a miracle that the lower bound constant $\frac{4}{3}$ is greater than 1” (see for example Conjecture 5 in their paper)

**Our contribution.** One of the main result of our paper is to obtain families of graphs which improve upon $\gamma = \frac{4}{3}$ in (2). We give here a construction of infinite families of regular graphs for degrees of the form $k = p^3 + 1$, where $p$ is any odd prime, for which

$$\text{girth}(G_i) \geq \frac{12}{7} \log_{k-1} |G_i| - 2 \log_p 2.$$

We also prove that these graphs are Ramanujan. These graphs exist for all sizes of the form $n = q^7 - q^3$, where $q$ is any odd prime satisfying $q > p$.

The idea underlying our construction is to replace in the Ramanujan graph construction of Lubotzky-Philipps-Sarnak & Margulis the quaternions by octonions. unique factorization property, that is available for integral octonions since the work of Rehm [44]. The Ramanujan graphs of [32, 35] built upon quaternions can be described as Cayley graphs on *groups*. This is no more the case for our construction on octonions. These graphs have a description in terms of Cayley graphs on *loops*, the non-associative counterpart of groups.

**Comments.** The property of large girth, besides its own theoretical interest, can be applied to LDPC codes. This approach was pioneered by Margulis in [34], 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 [48] 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 [19], but that does not hold anymore for a larger number of iterations.

Lower bounds on the code minimum distance and the number of errors which can be decoded with iterative decoding algorithms can also be obtained from lower bounds on the expansion [46, 47]. It makes sense in this context to use graphs which are at the same time of large girth and good expanders. The Ramanujan graphs proposed by [32, 35] are very good candidates for this. This was suggested in [45], see also [31]. It should also be mentioned that there is one particular LDPC code family where both properties of being Ramanujan and having a large girth can be used together, namely for cycle codes which were introduced in [21], where it can be proved (see [49]) that regular cycle codes obtained from the constructions of Ramanujan graphs given in [32, 35, 37] correct the largest possible fraction of errors. It should be pointed out here that the approach used in [49] could also be applied to the Ramanujan graphs based on octonions given here and that the larger girth of our construction compared to the constructions of [32, 35, 37] would lead to improved upper bounds on the probability of error after decoding.

Cayley graphs are usually thought to require groups. This is absolutely not necessary, much weaker algebraic structures like *quasi-groups* are sufficient. For a modern treatment, see [39] and references therein. The algebraic non-associative structures arisen from octonion algebras are well-known, and have the strong property of being *Moufang loops*. It is tempting to think that these would constitute the first algebraic construction of expanders not based on a group. But we do not know whether there exist groups on top of which these graphs could be Cayley graphs. We did not even prove that they are vertex-transitive, which is a stricly weaker property than being a Cayley graph on a group.

## 2 Preliminaries on octonions

All the material on octonions required for this construction is contained in the article of Rehm [44], where a more substantial bibliography can be found. A good complementary material is Ch.9 of [11]. For convenience, we define and cite 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 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*. Here we will choose $R = \mathbb{Z}, \mathbb{Q}, \mathbb{F}_p$. 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

$$\mathsf{i}^2 = \mathsf{j}^2 = \mathsf{k}^2 = -1, \ \mathsf{ij} = \mathsf{k}. \tag{3}$$

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

$$\begin{aligned} \bar{1} &= 1 \\ \overline{\alpha + \beta} &= \overline{\alpha} + \overline{\beta} \\ \overline{\alpha\beta} &= \overline{\beta}\overline{\alpha}. \end{aligned} \tag{4}$$

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

$$(\alpha_1 + \alpha_2\mathsf{t})(\beta_1 + \beta_2\mathsf{t}) = \alpha_1\beta_1 - \bar{\beta}_2\alpha_2 + (\beta_2\alpha_1 + \alpha_2\bar{\beta}_1)\mathsf{t} \tag{5}$$

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 (Cf. [12]) that among the 35 possible triads, only 7 are associative, namely:

$$\mathsf{i}, \mathsf{j}, \mathsf{k} \quad , \quad \mathsf{i}, \mathsf{t}, \mathsf{it} \quad , \quad \mathsf{j}, \mathsf{t}, \mathsf{jt} \quad , \quad \mathsf{k}, \mathsf{t}, \mathsf{kt}, \quad \text{and} \quad \mathsf{k}, \mathsf{jt}, \mathsf{it} \quad , \quad \mathsf{j}, \mathsf{it}, \mathsf{kt} \quad , \quad \mathsf{i}, \mathsf{kt}, \mathsf{jt}. \tag{6}$$

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

$$\text{(alternative algebra identities)} \qquad (\alpha\alpha)\beta = \alpha(\alpha\beta) \quad \text{and} \quad \beta(\alpha\alpha) = (\beta\alpha)\alpha. \tag{7}$$

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

In our case, we will often use the following corollary

**Corollary 1** *Let $\alpha, \beta$ be elements of $\mathbb{O}(\mathbb{Q})$. Then*

$$(\alpha\beta)\bar{\beta} = \alpha(\beta\bar{\beta}), \ \alpha(\bar{\alpha}\beta) = (\alpha\bar{\alpha})\beta. \tag{8}$$

Octonions are endowed with a *norm* $N$, that is a quadratic form. Here, the associated bilinear map will be:

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

Hence, the norm is here simply a sum of 8 squares. It can be defined equivalently by $N(\alpha) = \alpha\bar{\alpha}$. The important property is its *multiplicativity*: $N(\alpha\beta) = N(\alpha)N(\beta)$ for any octonions $\alpha$ and $\beta$. This follows directly from Theorem 1 and the antiautomorphism property (4)

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

Let $\mathbb{O}(R)^\star$ denote the set of invertible octonions. Clearly, if $\alpha$ is invertible, then $\alpha^{-1} = N(\alpha)^{-1}\overline{\alpha}$. It follows that:

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

**Loops.** The set of invertible elements in an alternative ring is a *Moufang loop* (Cf. [9, p. 254] and [11, 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*. We denote in this case by $x^{-1}$ 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:

$$\text{Moufang identities:} \qquad \begin{array}{l} (\alpha\beta\alpha)\gamma = \alpha((\beta\alpha)\gamma) \\ (\alpha\beta)(\gamma\alpha) = \alpha(\beta\gamma)\alpha \\ ((\beta\alpha)\gamma)\alpha = \beta(\alpha\gamma\alpha) \end{array} \tag{9}$$

It is straightforward to check that a Moufang loop is an inverse loop [11, Ch. 7] or [9, 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*[2]. In the quaternions 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 $1 + i + j + k$). Hurwitz noticed that it is possible to obtain a satisfactory arithmetic of quaternions by considering instead quaternions with integer or half integer coordinates [24, 25], and his result was fully understood after Dickson [16] 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 [12]. They allow as in the case of Hurwitz quaternions to obtain a set of octonions which obey the essential divisibility

[2] or that the *class number of ideals* is equal to 1. But for constructive purposes, the Eulidean 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 (6). 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 [44, Prop. 4.1], obtained a kind of distortion of the Euclidean algorithm, by using only the alternative property (7). 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 $1, \mathsf{i}, \mathsf{j}, \mathsf{k}, \mathsf{h}, \mathsf{ih}, \mathsf{jh}, \mathsf{kh}$ (Cf. [12, p 567]). 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 which satisfy*

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

Given an octonion $\alpha = a_0 + a_1\mathsf{i} + \ldots + a_7\mathsf{kt} \in \mathbb{O}(\mathbb{Q})^\star$, we say that it is positive and write $\alpha > 0$ if and only if the smallest $i$ such that $a_i \neq 0$ is $> 0$. Let $p$ be an odd prime number. Related to *unique* factorization, we define (Cf. [44, Prop. 5.6]):

$$\mathscr{P}(p) \overset{\text{def}}{=} \{\alpha \in \mathbb{O}(\mathbb{Z}) : \; \alpha > 0 \;, \quad N(\alpha) = p \;, \quad \alpha - 1 \in 2\mathcal{C}_{\mathbb{O}}\} \tag{10}$$

Rehm also proved that $|\mathscr{P}(p)| = p^3+1$ (Cf. [44, Prop. 6.4]). The main result of him in [44], that is fundamental in the present work is the following:

**Theorem 2** *[44] Let $\alpha \in \mathcal{C}_{\mathbb{O}}$ be primitive, that is 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 prime integers, not necessarily distinct. There exist 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:*

$$\alpha = \big(\cdots(\epsilon\pi_1\pi_2)\pi_3\cdots\big)\pi_s,$$

*with $\epsilon \in \mathcal{C}_{\mathbb{O}}^\star$ and $\pi_i \in \mathscr{P}(p_i)$.*

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

# 3 Arithmetic construction of the infinite $(p^3+1)$-regular tree

**Overview of the whole construction.** Similarly to [32, 35, 10, 37], our Ramanujan graph construction can be decomposed in two steps.
1. The first step consists of constructing the $(p^3+1)$-regular infinite tree in an arithmetic way

by using octonions.
2. Finite Ramanujan graphs are derived from this tree by taking suitable finite quotients of this tree which do not create small cycles.

We will detail the first step in this section. It will also turn out that our construction has a description in terms of Cayley graphs defined over loops. This will be explained in Section 4.

**Several useful lemmas on the factorization of octonions of norm $p^t$.** The main ingredients used for the construction are the unicity of factorization property of Theorem 2 and considering products of elements of $\mathcal{C}_{\mathbb{O}}$ of the following form

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

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 $\mathcal{C}_{\mathbb{O}}$ which are not irreducible can be simplified by using Corollary 1 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 an invertible element* $\epsilon$ *in* $\mathcal{C}_{\mathbb{O}}^\star$ *and elements* $\pi_1, \dots, \pi_t$ *of* $\mathscr{P}(p)$ *is primitive.*

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

$$c(\alpha)|c(\alpha\bar{\pi}) \tag{11}$$

because the coefficients of $\alpha\bar{\pi}$ are integer linear combinations of the coefficients of $\alpha$ in a $\mathbb{Z}$ basis. Since $\alpha\bar{\pi} = (\beta\pi)\bar{\pi} = \beta(\pi\bar{\pi}) = p\beta$ by Corollary 1, we obtain that $c(\alpha\bar{\pi}) = p$. This together with (11) implies that $c(\alpha) = p$ and that $p$ divides $\alpha$. We may therefore write $\alpha$ as $\alpha = \gamma p = \gamma(\bar{\pi}\pi) = (\gamma\bar{\pi})\pi$ (by using Corollary 1 again) for some $\gamma \in \mathcal{C}_{\mathbb{O}}$. Therefore $\beta = \gamma\bar{\pi}$. $\gamma$ is necessarily primitive, since $\beta$ is primitive. By Theorem 2, we can write $\gamma$ as an irreducible product of a unit $\epsilon$ and elements $\pi_1, \dots, \pi_s$ of $\mathscr{P}(p)$:

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

This implies that $\beta$ is of the form

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

This is an irreducible product, for if $\pi_s$ were equal to $\pi$, $\beta$ would be divisible by $p$ and would not be primitive. From Theorem 2 applied to $\beta$, we know that this is the only way we can write $\beta$ as an irreducible product, and therefore that the product $\alpha$ is necessarily of the form

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

which contradicts the assumption on its irreducibility. □

**Proposition 1** *Any element $\alpha \in \mathbb{O}(\mathbb{Z})$ of norm $N(\alpha) = p^t$ and with $\alpha \equiv 1 \bmod 2\mathcal{C}_{\mathbb{O}}$, 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: First of all, let us assume that there exist an non-negative integer $s$, an $\epsilon$ in $\mathcal{C}_{\mathbb{O}}^{\star}$ and elements $\pi_1, \dots, \pi_u$ such that $\alpha$ can be written as an irreducible product

$$\alpha = p^s\big(\dots((\epsilon\alpha_1)\alpha_2)\alpha_3\cdots\big)\alpha_u. \tag{12}$$

By taking norms on both sides, we see that $u = t - 2s$. Moreover, by Lemma 2, the irreducible product $\big(\dots((\epsilon\alpha_1)\alpha_2)\alpha_3\cdots\big)\alpha_u$ is primitive. Therefore $p^s$ is necessarily the largest power of $p$ which divides $\alpha$. We choose now $s$ like this, and since $p^{-s}\alpha$ is in $\mathbb{O}(\mathbb{Z})$ and is primitive, we can apply Rehm's theorem to it and write $p^{-s}\alpha = \big(\dots((\epsilon\alpha_1)\alpha_2)\cdots\big)\alpha_{t-2s}$, with $\epsilon \in \mathcal{C}_{\mathbb{O}}^{\star}$ and $\alpha_i \in \mathscr{P}(p)$. In other words $\alpha$ can be written in the form given in (12). The unicity of this form follows from the discussion above and the unicity of the decomposition of $p^{-s}\alpha$ ensured by Theorem 2.

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

“$a \in \mathcal{C}_{\mathbb{O}} - \mathbb{O}(\mathbb{Z})$ 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 $\mathbb{O}(Z)$ and finishes the proof of the aforementioned property.

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

Therefore, $\epsilon$ is among the 16 units of $\mathbb{O}(\mathbb{Z})^{\star}$. By using Corollary 1, it is straightforward to check that we can write $\epsilon$ as

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

The set $1 + 2\mathcal{C}_{\mathbb{O}}$ is stable by multiplication, therefore $\big(\dots((\alpha\bar{\alpha}_{t-2s})\bar{\alpha}_{t-2s-1}\big)\cdots\alpha_2\big)\bar{\alpha}_1$ belongs to $1 + 2\mathcal{C}_{\mathbb{O}}$ and so does $\epsilon$. 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 $\pm 1$. □

**The construction of the infinite tree** This lemma 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 $\Lambda$ 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 $\Lambda$;

- edge set defined as follows. By Proposition 1, any vertex can be viewed in a unique way as a irreducible product $(\dots(\alpha_1\alpha_2)\cdots\alpha_{s-1})\alpha_s$ where the $\alpha_i$'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

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

  By the convention that the void product is equal to 1, the vertex 1 is linked with all vertices labelled by $\pi$, 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** Let us give an interpretation of this arithmetic construction of the $(p^3+1)$-regular tree in terms of a *Cayley graph on a loop*, which is a slight generalization of the usual Cayley graph definition (see for instance [39]).

**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[3] 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** *[38, Theorem 8] $\mathscr{C}ay(L,S)$ is a $|S|$-regular graph without loops iff*
*(i) $\forall\, l \in L,\ l \notin lS$,*
*(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 Cayley graph on a certain loop [38].

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

**Definition 4** *Let $\alpha, \beta$ be two elements of $\Lambda$. 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 $\gamma$ on $\mathscr{P}(p)$ such that $\alpha\beta = \pm p^\ell\gamma$, with $N(\gamma) = p^{s+t-2\ell}$, that is $\gamma$ is an irreducible product of length $s+t-2\ell$. We define*

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

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

[3] 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.

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

Let $\alpha$ be some element of $\Lambda$. 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 $\Lambda$. 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 $\Lambda$ is a loop. It remains to show that $*$ satisfies the Moufang identities (9).

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

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

for some non-negative integers $s_1, s_2$ and $s_3$. From the Moufang identities (9), $(\alpha(\beta\alpha))\gamma = \alpha((\beta\alpha)\gamma)$, 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 $\Lambda$ 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:*

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

## 4 Obtaining finite graphs from $T$ by reducing $\Lambda$ modulo another prime $q$

**Reducing to finite graphs** Basically, finite graphs are obtained from the arithmetic construction of $T$ by reducing the octonions in $\Lambda$ 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 $\Lambda$ is a power of $p$ which is therefore invertible modulo $q$. Let us denote by $\tau_q$ the reduction modulo $q$ map $\tau_q : \mathbb{O}(\mathbb{Z}) \to \mathbb{O}(\mathbb{F}_q)$. By the definition of the profuct $*$, the following holds:

$$\tau_q(\alpha * \beta) = \tau_q(\epsilon p^{-s}\alpha\beta) = \tau_q(\epsilon p^{-s})\tau_q(\alpha)\tau_q(\beta), \tag{13}$$

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 $\mathbb{O}(\mathbb{F}_q)^\star$. Subset that appears to be precisely the center $\mathcal{Z}$ of $\mathbb{O}(\mathbb{F}_q)^\star$, as can easily be checked. It follows that the two elements $\tau_q(\alpha * \beta)$ and $\tau_q(\alpha)\tau_q(\beta)$ differs 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 word, the map

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

is a loop homomorphism. Indeed, Equality (13) clearly implies $\mu_q(\alpha * \beta) = \mu_q(\alpha)\mu_q(\beta)$. In addition, since $\mathbb{O}(\mathbb{F}_q)^\star$ is a Moufang loop, $\mathbb{O}(\mathbb{F}_q)^\star/\mathcal{Z}$ is itself a Moufang loop. We have proved:

**Lemma 3** *The map $\mu_q$ 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 this 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 $\mu_q$**.** Let us bring in $M_1$ and $M_p$ the subloops of $\mathbb{O}(\mathbb{F}_q)^\star$ consisting of invertible elements of norm 1 for $M_1$, and of norm Let $\mathcal{Z}_p \overset{\text{def}}{=} \{\pm p^s, s = 0, 1, \ldots, q-2\}$ and $\mathcal{Z}_1 \overset{\text{def}}{=} \{-1, 1\}$. Since $\mathcal{Z}_1 \subset \mathcal{Z}_p \subset \mathbb{F}_q^\star$ we can embed the corresponding quotient loops in $\mathbb{O}(\mathbb{F}_q)^\star/\mathcal{Z}$ as follows

$$\begin{array}{ccccc} M_1/\mathcal{Z}_1 & \hookrightarrow & M_p/\mathcal{Z}_p & \hookrightarrow & \mathbb{O}(\mathbb{F}_q)^\star/\mathcal{Z} \\ a\mathcal{Z}_1 & \mapsto & a\mathcal{Z}_p & & \\ & & b\mathcal{Z}_p & \mapsto & b\mathcal{Z} \end{array} \tag{14}$$

*Via* these embeddings, they can be identified as subloops of $\mathbb{O}(\mathbb{F}_q)^\star/\mathcal{Z}$. By a result of Paige [41, Theorem 4.1] $M_1/\mathcal{Z}_1$ is a simple Moufang loop, and an index 2 normal subloop[4] 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 $M_p/\mathcal{Z}_p = M_1/\mathcal{Z}_1$ or $\mathbb{O}(F_q)^\star/\mathcal{Z}$ (Cf. Corollary 2 for an answer to this issue).

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

Proof: Every elements of $\Lambda$ has a norm a 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 $\alpha = a_0 + a_1\mathsf{i} + \ldots + a_7\mathsf{kt} \in \mathbb{O}(\mathbb{Z})$ such that $N(\alpha) \equiv p^r \pmod q$ for some integer $r$, there exists an element $\beta = b_0 + b_1\mathsf{i} + \ldots + b_7\mathsf{k} \in 1 + 2\mathcal{C}_{\mathbb{O}}$ such that
(i) $a_i \equiv b_i \pmod q$,
(ii) $N(\beta) = p^\ell$ for some integer $\ell$.

To prove this claim we use as in [32, Prop. 3.3], a result of Malyshev on the number of solutions of integral definite-positive quadratic forms [33]. 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 $N \geq K(f)$, $N$ generic for $f$ (that is $f \equiv N \pmod r$ has at least one solution for every $r$), $\gcd(m, 2Nd) = 1$ and for which there exist integers $a_i$ such that $\gcd(a_1, \ldots, a_n, m) = 1$, $f(a_1, \ldots, a_n) \equiv N \pmod m$, then there are integers $b_1, \ldots, b_n$ such that
(i) $b_i \equiv a_i \pmod m$,
(ii) $f(b_1, \ldots, b_n) = N$. Let us first assume that $p \equiv 1 \pmod 4$. We apply the aforementioned result of Malyshev to $f(x_0, \ldots, x_7) \overset{\text{def}}{=} x_0^2 + 4(x_1^2 + \cdots + x_7^2)$. This is an integral positive definite quadratic form. The discriminant of $f$, $d = 2^7$, verifies $\gcd(2dp^\ell, q) = 1$ for any $\ell$. 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 $\alpha$ (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 $\ell$ such that $p^\ell \geq K(f)$ and $p^\ell \equiv p^r \pmod q$. It is straightforward to check that $p^\ell$ is generic for $f$ (this follows from the fact that $p^\ell \equiv 1 \pmod 4$). 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 $\beta$ of norm equal to $p^\ell$ 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 before for the case where $\ell$ is even, since in this case $p^\ell \equiv 1 \pmod 4$. In the case of an odd $\ell$, $p^\ell$ 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

$$f(x_0, \ldots, x_7) \overset{\text{def}}{=} 4(x_0^2 + x_1^2 + x_2^2 + x_3^2 + x_4^2) + x_5^2 + x_6^2 + x_7^2. \tag{15}$$

[4] From Corollary of Lemma 3.4 of [41], since $q > p$ is an odd prime.

This time $p^\ell$ is generic for $f$. Moreover a solution in $\mathbb{Z}^8$ of the equation $f(x_0,\dots,x_7)=p^\ell$ gives an element $\beta = 2x_0+2x_1\mathsf{i}+2x_2\mathsf{j}+2x_3\mathsf{k}+2x_4\mathsf{t}+x_5\mathsf{it}+x_6\mathsf{jt}+x_7\mathsf{kt}$ of norm $p^\ell$. Let us show that $\beta$ is also in $1+2\mathcal{C}_{\mathbb{O}}$. By reducing Equation (15) modulo 4, we obtain $x_5^2+x_6^2+x_7^2 \equiv 3 \pmod 4$, hence:

$$x_5 \equiv x_6 \equiv x_7 \equiv 1 \pmod 2.$$

The element $\frac{\beta-1}{2} = \frac{2x_0-1}{2}+x_1\mathsf{i}+x_2\mathsf{j}+x_3\mathsf{k}+x_4\mathsf{t}+\frac{x_5}{2}\mathsf{it}+\frac{x_6}{2}\mathsf{jt}+\frac{x_7}{2}\mathsf{kt}$ 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 $\beta$ in $1+2\mathcal{C}_{\mathbb{O}}$ of norm $p^\ell$. By applying Proposition 1 to it, we can write $\beta$ as

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

for some non-negative integer $s$, $\epsilon$ in $\{-1,1\}$ and $\gamma$ in $\Lambda$. Since $\tau_q(\alpha)=\tau_q(\beta)$ we have that $\tau_q(\beta)\in\tau_q(\alpha)\mathcal{Z}_p$ and therefore $\tau_q(\gamma)\in\tau_q(\alpha)\mathcal{Z}_p$. In other words, $\tau_q(\alpha)\mathcal{Z}_p \in \text{Im } \mu_q$. □

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

**Corollary 2** *If* $\left(\frac{p}{q}\right)=1$, *then* $\text{Im } \mu_q = M_1/\mathcal{Z}_1$.

*Else, when* $\left(\frac{p}{q}\right)=-1$, $\text{Im } \mu_q = \mathbb{O}(\mathbb{F}_q)^\star/\mathcal{Z}$.

Proof: The loop homomorphism $\mathbb{O}(\mathbb{F}_q)^\star \to \mathbb{Z}/2\mathbb{Z}$, $\alpha \mapsto \left(\frac{N(\alpha)}{q}\right)$, regarding the definition of $\mathcal{Z}$, factorizes into this homomorphism: $\varepsilon : \mathbb{O}(\mathbb{F}_q)^\star/\mathcal{Z} \to \mathbb{Z}/2\mathbb{Z}$. Its kernel contains $M_1/\mathcal{Z}_1$.

Besides, for $\pi \in \mathscr{P}(p)$, $\mu_q(\pi)$ is mapped by $\varepsilon$ to 1 or -1 in $\mathbb{Z}/2\mathbb{Z}$, 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 $M_1/\mathcal{Z}_1 \subsetneq M_p/\mathcal{Z}_p = \text{Im } \mu_q$, from which follows $\text{Im } \mu_q = \mathbb{O}(\mathbb{F}_q)^\star/\mathcal{Z}$ by Paige's theorem.

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

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

$$\ker\mu_q \overset{\text{def}}{=} \Lambda(q) = \{\alpha\in\Lambda \text{ s.t } q|a_1,\dots,q|a_7\}, \quad \text{and then} \quad \Lambda/\Lambda(q) \simeq \mathbb{O}(\mathbb{F}_q)^\star/\mathcal{Z}. \tag{16}$$

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

**Definition 5** *We define* $\mathscr{S}(p,q) \overset{def}{=} \mu_q\big(\mathscr{P}(p)\big)$. *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 $|\mathbb{O}(\mathbb{F}_q)^\star/\mathcal{Z}| = q^7-q^3$ [44, 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 $\Lambda$ as a loop. The proof of Corollary 2 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 [44, 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 $\pi$ and $\pi'$ in $\mathscr{P}(p)$ give the same element in $\mathbb{O}(\mathbb{F}_q)^\star/\mathcal{Z}$ through $\mu_q$. The equality $\tau_q(\pi)\mathcal{Z}=\tau_q(\pi')\mathcal{Z}$ is equivalent to $\mu_q(\pi*\overline{\pi'})\in\ker\mu_q=\Lambda(q)$. By Equation (16), taking norm 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 $p^2\geq q^2$, excluded since $p<q$. 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 $\mu_q$ is an homomorphism by Lemma 3 also holds $\mathscr{S}(p,q)^{-1}=\mathscr{S}(p,q)$. Last, $1\mathcal{Z}\notin\mathscr{S}(p,q)$, else there would be a $\pi\in\mathscr{P}(p)$ that would also be in $\Lambda(q)$, by Equation (16), that is easily checked to be 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:

$$M_1/\mathcal{Z}_1\to\mathbb{Z}/2\mathbb{Z}.$$

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

It is interesting to consider the *bipartite double cover* of $\mathscr{Y}_{p,q}$ when $\left(\frac{p}{q}\right)=1$, especially for the treatment of the girth in the next section. Recall here that the double cover of a graph $G$ with vertex set $V$ and edge set $E$ is the graph with vertex set $V'=V\times\{0,1\}$ and there is an edge between $(x,b)$ and $(x',b')$ if and only if $\{x,x'\}\in E$ and $b'\neq b$. The double cover is a bipartite graph and is connected if and only if $G$ is not bipartite.

**Definition 6** *When $\left(\frac{p}{q}\right)=-1$, we define $\mathscr{X}_{p,q}$ as the bipartite double cover of $\mathscr{Y}_{p,q}$.*

It follows that $|\mathscr{X}_{p,q}|=q^7-q^3$ for any primes $2<p<q$.

## 5 Bound on the girth

The result hereunder establishes a new lower bound on the maximal girth of regular graphs.

**Theorem 3** *For all couples $(p, q)$ of odd primes such that $p < q$, denoting $k = p^3 + 1$, we have:*
*(i) that the girth of $\mathscr{X}_{p,q}$, which we denote by* $\mathrm{girth}(\mathscr{X}_{p,q})$, *satisfies*

$$\mathrm{girth}(\mathscr{X}_{p,q}) \geq \frac{12}{7} \log_{k-1} |\mathscr{X}_{p,q}| - 2 \log_p 2.$$

*The constant $\frac{12}{7}$ is the largest possible.*

*(ii) For the non-bipartite graphs $\mathscr{Y}_{p,q}$ (defined when $\left(\frac{p}{q}\right) = 1$), the inequality*

$$\mathrm{girth}(\mathscr{Y}_{p,q}) \geq \frac{6}{7} \log_{k-1} |\mathscr{X}_{p,q}| - \log_p 2 = \frac{6}{7} \log_{k-1} |\mathscr{Y}_{p,q}| - \frac{5}{7} \log_p 2$$

*holds.*

The proof of this theorem follows an approach similar to the one used in [32, 35] for the lower bound, and [35, 4] for the tightness of this bound. However compared to the Ramanujan graphs based on quaternions there is an additional difficulty. The former are Cayley graphs on groups, they are vertex transitive and it is therefore enough to lower bound the size of a cycle starting at the 1 vertex (1 stands here for the identity in the loop). We do not know whether our construction is vertex transitive or not, however it is enough to study the cycles starting at the 1 vertex in our case too. This is a consequence of the following result.

**Lemma 6** *Given $\alpha$ in $\Lambda$, there is a one-one correspondence between:*
*(a) the closed paths without backtracking of length $t'$ starting at the vertex $\mu_q(\alpha)$, and*
*(b) the irreducible products in $\Lambda$ of length $t'$ belonging to the kernel $\Lambda(q)$ of $\mu_q$.*

PROOF: A closed path of length $t'$ without backtracking starting at $\mu_q(\alpha)$ corresponds to an irreducible product in $\Lambda$, of length $t'$, with letters denoted by $\beta_1, \dots, \beta_{t'} \in \mathscr{P}(p)$ such that:

$$\forall 2 \leq i \leq t'{-}1, \quad \mu_q\left((\dots(\alpha * \beta_1) * \cdots) * \beta_{i+1}\right) \neq \mu_q\left((\dots(\alpha * \beta_1) * \cdots) * \beta_{i-1}\right), \quad \text{(no backtracking)}$$

$$\text{and if} \quad \gamma \overset{\text{def}}{=} \big(\dots(\alpha * \beta_1) * \cdots\big) * \beta_{t'}, \text{ then } \mu_q(\alpha) = \mu_q(\gamma) \qquad \text{(closed path).}$$

We must show that the irreducible product $\beta \overset{\text{def}}{=} (\cdots(\beta_1\beta_2)\cdots)\beta_{t'}$ is in $\Lambda(q)$. By Corollary 1,

$$\gamma\overline{\beta_{t'}} = \big(\cdots(\alpha\beta_1)\cdots\beta_{t-1})\beta_{t'}\big)\overline{\beta_{t'}} = \big(\cdots(\alpha\beta_1)\cdots\beta_{t'-1}\big)(\beta_{t'}\overline{\beta_{t'}}) = p\big(\cdots(\alpha\beta_1)\cdots\big)\beta_{t'-1}.$$

By induction it arrives $\gamma\overline{\beta} = p^{t'}\alpha$, or $\gamma * \overline{\beta} = \alpha$, or $\mu_q(\gamma)\mu_q(\overline{\beta}) = \mu_q(\alpha)$. But by assumption, $\mu_q(\gamma) = \mu_q(\alpha)$, which implies $\mu_q(\overline{\beta}) = 1\mathcal{Z}$, since $\mathbb{O}(\mathbb{F}_q)^\star/\mathcal{Z}$ is a loop. Equivalently, $\overline{\beta} \in \ker \mu_q = \Lambda(q)$, and hence $\beta$ as well, as can be easily checked.

Reciprocally, let us consider an irreducible product $\gamma$ in $\Lambda(q)$ of $t'$ elements $\gamma_1, \dots, \gamma_{t'}$ in $\mathscr{P}(p)$. Let:

$$\delta \overset{\text{def}}{=} \big((\dots(\alpha\gamma_1)\cdots\gamma_{t'-1}\big)\gamma_{t'}.$$

As seen above, $\delta * \overline{\gamma} = \alpha$. It follows that $\mu_q(\delta * \overline{\gamma}) = \mu_q(\delta)\mu_q(\overline{\gamma})$. By assumption, $\mu_q(\gamma) = 1.\mathcal{Z}$, therefore we also have $\mu_q(\overline{\gamma}) = 1.\mathcal{Z}$. So $\mu_q(\alpha) = \mu_q(\alpha * \overline{\gamma})$. This corresponds to a path of length $t'$, without backtracking, starting at $\mu_q(\alpha)$. □

The second lemma gives a tight lower bound on the size of irreducible products in $\Lambda$ of *even* length that belong to $\Lambda(q)$. This yields therefore a tight lower bound on the size of cycles of even length in the graphs $\mathscr{X}_{p,q}$ or $\mathscr{Y}_{p,q}$.

**Lemma 7** *Given $t > 0$, there exists an irreducible product in $\Lambda(q)$ of length $2t$ if and only if $2p^t > q^2$.*

PROOF: Let $\beta \in \Lambda(q)$ be as in the statement. It can be written as $\beta = b_0 + q(b_1\mathsf{i} + \cdots + b_7\mathsf{kt})$ where the $b_i$'s are integer coefficients. Moreover, $N(\beta) = p^{2t}$ gives:

$$b_0^2 + q^2(b_1^2 + \cdots + b_7^2) = p^{2t}. \tag{17}$$

At least one $b_i$ (with $i > 0$) is non zero, 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 $p^t \equiv \pm b_0 \pmod{q}^2$. We 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

$$\begin{aligned} p^{2t} &= (p^t - mq^2)^2 + q^2(b_1^2 + \cdots + b_7^2) \\ &= p^{2t} - 2mq^2p^t + m^2q^4 + q^2(b_1^2 + \cdots + b_7^2) \\ &\Leftrightarrow 2mp^t - m^2q^2 = b_1^2 + \cdots + b_7^2. \end{aligned} \tag{18}$$

Then it follows that $2p^t - mq^2 > 0$. This is because at least one $b_i$ (with $i > 0$) is different from 0, achieving the first part of the proof.

Reciprocally, if $m$ is such that $2p^t > mq^2$, then $2mp^t - m^2q^2$ can be represented by a sum of seven squares: $2mp^t - m^2q^2 = a_1^2 + \cdots + a_7^2$. We choose $a_0 = p^t - mq^2$, and notice that:

$$\begin{aligned} a_0 &\equiv a_0^2 \pmod 2 \\ &\equiv p^{2t} - q^2(a_1^2 + \ldots + a_7^2) \pmod 2 \\ &\equiv 1 + a_1 + \ldots + a_7 \pmod 2 \end{aligned} \tag{19}$$

This implies that among the 8 integers $\{a_0 - 1, a_1, a_2, \ldots, a_7\}$, the number of odd ones is *even*, as well as is the number of even ones. Therefore, after eventually performing a permutation of the set $\{a_1, \ldots, a_7\}$, we can always assume that the two subsets $\{a_0 - 1, a_1, a_2, a_3\}$ and $\{a_4, a_5, a_6, a_7\}$ contains the same number of odd and even integers. Moreover the permutation can also be chosen so that the following congruence is verified:

$$(a_0 - 1, a_1, a_2, a_3) \equiv (a_4, a_5, a_6, a_7) \pmod 2$$

With the congruence (19), this shows that the octonion $a_0 - 1 + a_1\mathsf{i} + \cdots + a_7\mathsf{kt}$ verifies the conditions of Lemma 1 and that it belongs to $2\mathcal{C}_{\mathbb{O}}$. Finally the octonion $a_0 + qa_1\mathsf{i} + \cdots + qa_7\mathsf{kt} \in 1 + 2\mathcal{C}_{\mathbb{O}}$, hence is in $\Lambda(q)$, since its norm is equal to $p^{2t}$ by construction. □

Using both lemmas together we obtain

**Proposition 7** *The length of the smallest closed non backtracking walk of even length in $\mathscr{X}_{p,q}$ or in $\mathscr{Y}_{p,q}$ is equal to $2\lceil 2\log_p q - \log_p 2\rceil$*

PROOF: Such a walk of length $2t$ exists if and only if there exists an irreducible product of length $2t$ which belongs to $\Lambda(q)$ by Lemma 6. Using now Lemma 7, we know that such a product exists if and only if $2p^t > q^2$. The smallest $t$ which satisfies this inequality is clearly equal to $\lceil 2\log_p q - \log_p 2\rceil$. □

We can now prove Theorem 3.

PROOF: (of Theorem 3) The first part of (i) is a consequence of the fact that $\mathscr{X}_{p,q}$ is bipartite, therefore any cycle it contains is of even length. We can apply now Proposition 7 and lower bound the length of such a cycle by $2\lceil 2\log_p q - \log_p 2\rceil$. Hence

$$\mathrm{girth}(\mathscr{X}_{p,q}) = 2\lceil 2\log_p q - \log_p 2\rceil = 2\left\lceil \frac{6}{7}\log_{p^3} q^7 - \log_p 2\right\rceil \geq \frac{12}{7}\log_{k-1}(q^7 - q^3) - 2\log_p 2,$$

and the first part of (i) follows. The optimality of the constant $\frac{12}{7}$ follows at once from the fact that

$$\mathrm{girth}(\mathscr{X}_{p,q}) = 2\lceil 2\log_p q - \log_p 2\rceil = (1+o(1))\frac{12}{7}\log_{p^3}(q^7-q^3) = (1+o(1))\frac{12}{7}\log_{k-1}|\mathscr{X}_{p,q}|$$

as $q$ tends to infinity.

To prove (ii), notice that the double cover graph of $\mathscr{Y}_{p,q}$ is equal to $\mathscr{X}_{p,q}$ by definition and that the length of the smallest cycle of the double cover is at most twice the length of a cycle in $\mathscr{Y}_{p,q}$, therefore

$$\mathrm{girth}(\mathscr{X}_{p,q}) \leq 2\,\mathrm{girth}(\mathscr{Y}_{p,q}).$$

and (ii) follows immediately. □

# 6 Spectral estimate

The proof that the graph families presented here are Ramanujan follows the proof technique of Lubotzky Phillips and Sarnak in [32, § 4]. Basically their approach can be summarized as this.

(i) A classical graph spectral argument is first used to relate the number of cycles of a certain length without backtracking to the spectrum of the graph.

(ii) In the particular case of the Ramanujan family based on quaternions of [32], the number of cycles without backtracking can be related to the number of integer solutions of a certain quadratic equation in 4 variables. In our case, a similar result holds with a quadratic diophantine equation in 8 variables.

(iii) The number of solutions of the quadratic equation is estimated through modular forms considerations. Basically, it can be expressed as a sum of a Fourier coefficient of an Eisenstein series and one of a cusp form, both of weight 2. The Fourier coefficient of the Eisenstein series can be computed explicitly, whereas the Fourier coefficient of the cusp form is upper-bounded by deep results proving the Ramanujan-Petersson conjectures for modular forms of weight 2 (using here Eichler and Igusa results [17, 26] relating such a conjecture to the Riemann hypothesis for algebraic curves on finite fields which was proved by Weil [50]). In our case, we relate the number of integer to the estimation of Fourier coefficients of weight 4, where we rely instead on the more general Deligne's proof [14, 15] of the Ramanujan-Petersson conjectures for modular forms of even weight, which was obtained by proving Riemann's hypothesis for varieties over finite fields.

With the same approach we obtain the following theorem.

**Theorem 4** *The graphs $\mathscr{X}_{p,q}$ are Ramanujan.*

**Remarks:**

1. We consider here in a unified way the case where $\mathscr{X}_{p,q}$ is a Cayley graph over the Moufang loop $\mathbb{O}(\mathbb{F}_q)/\mathcal{Z}$ (which corresponds to the case $\left(\frac{p}{q}\right) = -1$) and where $\mathscr{X}_{p,q}$ is the double cover of $\mathscr{Y}_{p,q}$ (i.e. $\left(\frac{p}{q}\right) = 1$).

2. This will allow for instance to obtain as a direct corollary (see Corollary 3) that the $\mathscr{Y}_{p,q}$'s are also Ramanujan.

**Step 1: relating the graph spectrum to the numbers of non-backtracking cycles.** We recall that if $A$ is the adjacency matrix of a graph, then $A^\ell$ is the matrix whose $i, j$-entry is the number of paths of length $\ell$ between the vertices labeled $i$ and $j$. Assume that the graph is regular of valency $k$. The sequence of matrices $(B_\ell)_{\ell\in\mathbb{N}}$ defined by the order 2 recurrence relation (Cf. [13, 1.4.1 Lemma]):

$$B_0 = \mathrm{Id},\ B_1 = A,\ B_2 = A^2 - k\mathrm{Id}, \qquad B_\ell = AB_{\ell-1} - (k-1)B_{\ell-2},\ \text{for } \ell \geq 3,$$

counts the number of paths *without backtracking* of length $\ell$ between two vertices. We recall that a path $(x_0, x_1, \dots, x_\ell)$ is said to be without backtracking if and only if $x_{i-1} \neq x_{i+1}$ for any $i \in \{1, \dots, \ell-1\}$. The Chebychev polynomials (of the second kind) $U_m(X)$, defined by $U_m(\cos\theta) = \frac{\sin(m+1)\theta}{\sin\theta}$, verify an order 2 recurrence relation as well:

$$U_m(X) = 2XU_{m-1}(X) - U_{m-2}(X).$$

Hence, it is possible to link the $B_\ell$ and the $U_m$ in the following way. Defining matrices $(T_m)_{m\in\mathbb{N}}$,

$$T_m \overset{\text{def}}{=} \sum_{0\leq\ell\leq\frac{m}{2}} B_{m-2\ell}, \tag{20}$$

comes (Cf. [13, 1.4.5 Proposition]):

$$T_m = (k-1)^{m/2} U_m\left(\frac{A}{2\sqrt{k-1}}\right). \tag{21}$$

Suppose that the graph whose adjacency matrix is $A$ has vertex set $V$, that $|V| = n$. Let $\lambda_0 = k \geq \lambda_1 \geq \cdots \geq \lambda_{n-1}$ the eigenvalues of this graph. Given a vertex $x \in V$, let $f_{\ell,x}$ be the number of closed paths of length $\ell$ without backtracking starting at $x$. By definition of the matrices $(B_\ell)_{\ell\in\mathbb{N}}$, $f_{\ell,x}$ is the entry of the diagonal element of $B_\ell$ labeled by the vertex $x$. By taking the trace of the matrix $T_m$ using Equation (21) and Equation (20) comes (Cf. [13, 1.4.6 Theorem]):

$$\sum_{x\in V}\sum_{0\leq\ell\leq\frac{m}{2}} f_{m-2\ell,x} = (k-1)^{m/2}\sum_{j=0}^{n-1} U_m\left(\frac{\lambda_j}{2\sqrt{k-1}}\right). \tag{22}$$

We go back now to the graphs $\mathscr{X}_{p,q}$, so that the size is $n = q^7 - q^3$ and the valency is $k = p^3 + 1$.

We differ now slightly from the proof given in [13]. It is not clear that these graphs are vertex transitive as was the case for the Ramanujan graphs of [32, 35] (these graphs were constructed as Cayley graphs on *groups*, and were therefore vertex-transitive). In our case, we obtain that $f_{\ell,x}$ is independent of the vertex $x$ in a different way by a reformulation of Lemma 6:

**Lemma 8** *For the graphs $\mathscr{X}_{p,q}$, the number $f_{\ell,x}$ is independent of the vertex $x$. When $\ell$ is even, this number is equal to the number of irreducible products $(\dots(\alpha_1\alpha_2)\cdots)\alpha_s$ of length $\ell$ such that $(\dots(\alpha_1\alpha_2)\cdots)\alpha_s \in \Lambda(q)$.*

Proof: If $\ell$ is odd, then $f_{\ell,x}$ is equal to zero for every $x$ because $\mathscr{X}_{p,q}$ is bipartite. If $\ell$ is even, the statement given is a straightforward consequence of Lemma 6 and the very definition of $\mathscr{X}_{p,q}$ in terms of a Cayley graph over $\mathbb{O}(\mathbb{F}_q)^\star/\mathscr{Z}$ (when $\left(\frac{p}{q}\right) = -1$) or in terms of a double cover of a Cayley graph over $M_1/\mathscr{Z}_1$ (when $\left(\frac{p}{q}\right) = 1$). □

With this lemma, we denote $f_{\ell,x}$ simply by $f_\ell$. The degree of the graphs $\mathscr{X}_{p,q}$ is $k = p^3 + 1$, therefore Equation (22) becomes (Cf. [13, 1.4.7 Corollary]):

$$n\sum_{0\leq\ell\leq\frac{m}{2}} f_{m-2\ell} = p^{3m/2}\sum_{j=0}^{n-1} U_m\left(\frac{\lambda_j}{2p^{3/2}}\right). \tag{23}$$

**Step 2: Expressing the number $f_\ell$ of non-backtracking cycles of length $\ell$ in terms of the number of solutions of certain quadratic diophantine equations.** To start with, let us introduce briefly some preliminary materials. Given a positive definite quadratic form $R$, anf for $t \in \mathbb{N}$ fixed, let

$$N_R(t) \overset{\text{def}}{=} \left\{ \mathbf{x} = (x_0, \dots, x_7) \in \mathbb{Z}^8 \ : \ R(\mathbf{x}) = t \right\}, \quad \text{and} \quad n_R(t) = |N_R(t)|. \tag{24}$$

We consider now the positive definite quadratic form

$$Q(x) = x_0^2 + q^2(x_1^2 + \cdots + x_7^2).$$

For $\mathbf{a} \in \{0,1\}^8$, let us define also the sets

$$E_{\mathbf{a}} \overset{\text{def}}{=} \left\{ \mathbf{x} \in \mathbb{Z}^8 \ : \ Q(\mathbf{x}) = t \ , \quad \mathbf{x} \equiv \mathbf{a} \pmod 2 \right\}$$

and for $i \in \{0, 1, \dots, 7\}$:

$$F_i \overset{\text{def}}{=} \left\{ \mathbf{x} = (x_0, \dots, x_7) \in \mathbb{Z}^8 \ : \ Q(\mathbf{x}) = t \ , \quad x_i \equiv 0 \pmod 2 \right\}.$$

In the light of the property of Lemma 1 verified by elements in $\Lambda$, the relevant quantity to consider is not the whole number of integer solutions $n_Q(t)$ of $Q = t$, but the following:

**Definition 7** *Let $r_Q(t)$ denotes the number of solutions of $Q(\mathbf{x}) = t$ with $\mathbf{x} = (x_0, \dots, x_7) \in \mathbb{Z}^8$ and satisfying*

$$\begin{aligned}
(x_0, x_1, x_2, x_3) &\equiv (1 - x_4, x_5, x_6, x_7) \pmod 2 \ \text{ if } x_0 + x_1 + x_2 + x_3 \equiv 1 \pmod 2, \\
(x_0, x_1, x_2, x_3) &\equiv (x_4, 1 - x_5, 1 - x_6, 1 - x_7) \pmod 2 \ \text{ if } x_0 + x_1 + x_2 + x_3 \equiv 0 \pmod 2.
\end{aligned}$$

Indeed, this quantity verifies:

**Lemma 9** *Let $m$ be a non-negative* even *integer. The following equality holds:*

$$r_Q(p^m) = 2 \sum_{0 \le \ell \le \frac{m}{2}} f_{m-2\ell}.$$

Proof: We already know from Lemma 6 that $f_{m-2\ell}$ counts the number of irreducible products in $\Lambda(q)$ of length $m - 2\ell$. Let $\alpha = a_0 + a_1\mathsf{i} + \cdots + a_7\mathsf{kt}$ be such an irreducible product. It belongs to $\Lambda(q) \subset 1 + 2\mathcal{C}_{\mathbb{O}}$ therefore, from Lemma 1

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

And moreover, $a_i = qa'_i$ for some integers $a'_i$ and for $1 \le i \le 7$. Hence, $N(\alpha) = p^{m-2\ell} = Q(a_0, a'_1, \dots, a'_7)$. This $\alpha$ gives two solutions contributing to $r_Q(p^m)$, namely $\pm(a_0p^\ell, a'_1p^\ell, \dots, a'_7p^\ell)$.

Conversely, a solution $(x_0, \dots, x_7)$ contributing to $r_Q(p^m)$ above yields an element $\beta = x_0 + q(x_1\mathsf{i} + \cdots + x_7\mathsf{kt}) \in 1 + 2\mathcal{C}_{\mathbb{O}}$ of norm $N(\beta) = p^m$. That is, $\beta$ verifies the conditions of Proposition 1 and there exists a unique irreducible product $\beta' \in \Lambda$ such that $\beta = \pm p^\ell \beta'$. It is easily verified that $\beta'$ is also in $\Lambda(q)$. Since, $N(\beta') = p^{2m-\ell}$, this is a contribution to $f_{m-2\ell}$. □

The next step is to relate $r_Q(t)$ to the whole number of integer solutions $n_{Q_S}(t)$ of certain quadratic equations $Q_S$ defined hereunder. Indeed, these $n_{Q_S}(t)$ can be estimated sharply (see the next step), whereas it is not the case for the partial number of solutions $r_Q(t)$.

**Definition 8** *Given a subset $S \subset \{0, 1, \ldots, 7\}$, we define the following quadratic form*

$$Q_S(x_0, \ldots, x_7) \overset{def}{=} \phi_S(0)x_0^2 + q^2 \sum_{1 \le i \le 7} \phi_S(i)x_i^2,$$

*where $\phi_S(i) = 4$ if $i \in S$ and $1$ otherwise.*

It is not difficult to see that $n_{Q_S}(t)$ has the following interpretation in terms of the number of integer solutions of $Q(\mathbf{x}) = t$:

$$n_{Q_S}(t) = \left|\{\mathbf{x} = (x_0, \ldots, x_7) \in \mathbb{Z}^8 \ : \ Q(\mathbf{x}) = t \ , \quad x_i \equiv 0 \pmod 2 \text{ if } i \in S\}\right|. \qquad (25)$$

With the help of the definition above, now we can prove that:

**Lemma 10** *There exist integers $a_S$ for $S$ ranging over all subsets of $\{0, \ldots, 7\}$ such that*

$$r_Q(t) = \sum_S a_S n_{Q_S}(t).$$

PROOF: Let $A$ be the set of $\mathbf{a} = (a_i)_{0 \le i \le 7} \in \{0, 1\}^8$ satisfying

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

By definition of $E_{\mathbf{a}}$, we clearly have:

$$r_Q(t) = \sum_{\mathbf{a} \in A} |E_{\mathbf{a}}|. \qquad (26)$$

Next, we show that for any $\mathbf{a} \in \{0, 1\}^8$ there is a family of integers $(u_S)_{S \subset \{0, \ldots, 7\}}$ such that

$$|E_{\mathbf{a}}| = \sum_{S \subset \{0, \ldots, 7\}} u_S n_{Q_S}(t). \qquad (27)$$

The above plugged in Equation (26) will prove the lemma. To do so, notice that:

$$E_{\mathbf{a}} = \bigcap_{i : a_i = 0} F_i \cap \bigcap_{i : a_i = 1} (N_Q - F_i), \qquad (28)$$

where $N_Q$ denotes the set $N_Q(t)$ of (24). This follows directly from the definitions of these sets. . For $b = 0$ or $1$, let us define $S_b \overset{\text{def}}{=} \{i : a_i = b\}$. Let also $G$ be the set $\cap_{i : a_i = 0} F_i$. Equation (28) can be rewritten as:

$$E_{\mathbf{a}} \ = \ \bigcap_{i \in S_0} F_i \cap \bigcap_{i \in S_1} (N_Q - F_i) \ = \ G \cap \Big(N_Q - \bigcup_{i \in S_1} F_i\Big) \ = \ G - \Big(G \cap \bigcup_{i \in S_1} F_i\Big).$$

The last equality is justified by the inclusion $G \subset N_Q$. We now take cardinal:

$$\begin{aligned} |E_{\mathbf{a}}| &= |G| - \left|G \cap \bigcup_{i \in S_1} F_i\right| = |G| - \left|\bigcup_{i \in S_1} G \cap F_i\right| \\ &= |G| - \sum_{T \subseteq S_1} (-1)^{|T|-1} \left|G \cap \bigcap_{i \in T} F_i\right| \quad \text{(by the inclusion/exclusion principle)} \\ &= \left|\bigcap_{i \in S_0} F_i\right| - \sum_{T \subseteq S_1} (-1)^{|T|-1} \left|\bigcap_{i \in T \cup S_0} F_i\right| \\ &= n_{Q_{S_0}}(t) - \sum_{T \subseteq S_1} (-1)^{|T|-1} n_{Q_{T \cup S_0}}(t) \quad \text{(by using (25))} \end{aligned}$$

This proves Equality (27), which is sufficient to conclude the proof as already mentionned. □

We assume from now on that $m$ is *even*, say $m = 2\ell$. Equality (23) is then rewritten as:

$$r_Q(p^{2\ell}) = \frac{2p^{3\ell}}{n} \sum_{j=0}^{n-1} U_m\left(\frac{\lambda_j}{2p^{3/2}}\right). \tag{29}$$

For every $0 \leq j \leq n-1$, there exists a unique $\theta_j \in [\frac{3i}{2}\ln p, 0] \cup [0,\pi] \cup [\pi, \pi + \frac{3i}{2}\ln p] \subset \mathbb{C}$ such that: $\lambda_j = 2p^{3/2}\cos\theta_j$ (precisely, $\theta_j \in [0,\pi]$ if $|\lambda_j| \leq 2p^{3/2}$, $\theta_j \in [\frac{3i}{2}\ln p, 0)$ for $2p^{3/2} < \lambda_j \leq p^3+1$ and $\theta_j \in (\pi, \pi + \frac{3i}{2}\ln p]$ for $-p^3-1 \leq \lambda_j < -2p^{3/2}$). Recall that $\lambda_0 = p^3+1$ and since the graphs are bipartite $\lambda_{n-1} = -p^3-1$, so $\theta_0 = \frac{3i}{2}\ln p$ and $\theta_{n-1} = \pi + \frac{3i}{2}\ln p$. As a consequence, the graphs are Ramanujan if and only if the $\theta_j$'s are real for $1 \leq j \leq n-1$, which will be proved in the 3rd step below.

By coming back to the definition of Chebychev polynomials, Equality (29) becomes:

$$r_Q(p^{2\ell}) = \frac{2p^{3\ell}}{n} \sum_{j=0}^{n-1} \frac{\sin(2\ell+1)\theta_j}{\sin\theta_j}. \tag{30}$$

With the aforementioned values for $\theta_0$ and $\theta_{n-1}$, namely $\theta_0 = \frac{3i}{2}\ln p$ and $\theta_{n-1} = \pi + \frac{3i}{2}\ln p$, we check that:

$$r_Q(p^{2\ell}) = \frac{4}{n}\frac{1-p^{3(2\ell+1)}}{1-p^3} + \frac{2p^{3\ell}}{n} \sum_{j=1}^{n-2} \frac{\sin(2\ell+1)\theta_j}{\sin\theta_j}. \tag{31}$$

**Step 3: Using modular forms techniques to estimate $r_Q(p^m)$.** Similarly to [32], let us bring in the Theta series:

$$\Theta_S(z) \overset{\text{def}}{=} \sum_{k=0}^{\infty} n_{Q_S}(k) e^{2i\pi kz}. \tag{32}$$

By using classical results about Theta series (see for instance [36, §4.9.5] or [40, Chapter VI-3]), we obtain

**Lemma 11** *$\Theta_S(z)$ is a modular form*[5] *of weight* 4 *for* $\Gamma(16q^2)$*.*

$\Gamma(16q^2)$ denotes here the group of matrices

$$\Gamma(16q^2) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{16q^2} \right\}.$$

The modular forms $\Theta_S$ can be decomposed in a unique way as a sum of a linear combination of Eisenstein series $E_S(z) = \sum_{k=0}^{\infty} e_{k,S} e^{2i\pi kz}$ and a cusp form $C_S(z) = \sum_{k=1}^{\infty} c_{k,S} e^{2i\pi kz}$ of weight 4 for $\Gamma(16q^2)$ (see [22, article 24, Satz 1. II] for instance), i.e $\Theta_S(z) = E_S(z) + C_S(z)$. We can therefore write by using Lemma 10

$$\sum_{S \subseteq \{0,\ldots,7\}} a_S \left(e_{p^{2\ell},S} + c_{p^{2\ell},S}\right) = \frac{4}{n}\frac{1-p^{3(2\ell+1)}}{1-p^3} + \frac{2p^{3\ell}}{n} \sum_{j=1}^{n-2} \frac{\sin(2\ell+1)\theta_j}{\sin\theta_j}. \tag{33}$$

The central argument for estimating accurately $r_Q(p^{2\ell})$ is that the Fourier coefficients of a cusp form $C(z) = \sum_{k=1}^{\infty} c_k e^{2i\pi kz}$ of weight 4 satisfy for every $\epsilon > 0$:

$$|c_k| = O_\epsilon(k^{3/2+\epsilon}) \text{ as } k \to \infty. \tag{34}$$

[5] Actually, $\Theta_S(z)$ even belongs to $\Gamma_0(16q^2)$ as is readily checked from [36]. However, this allows us to make directly use of certain results related to $\Gamma_{16q^2}$ as will appear later on.

This comes from the proof of the Ramanujan conjecture for cusp forms of even weight obtained by using the work of Ihara [27], which reduced the proof of the conjecture to the Riemann hypothesis for varieties over finite field which was later settled by Deligne in [14, 15].

Since the remaining sum $\frac{2p^{3\ell}}{n}\sum_{j=1}^{n-2}\frac{\sin(2\ell+1)\theta_j}{\sin\theta_j}$ is clearly of the form $o(p^{6\ell})$ as $m$ tends to infinity, it follows from the upper-bound (34) and from Equation (33) that

$$\sum_{S\subseteq\{0,\ldots,7\}} a_S e_{p^{2\ell},S} = \frac{4}{n}\frac{1-p^{3(2\ell+1)}}{1-p^3} + o\big(p^{6\ell}\big). \tag{35}$$

Following [32], we observe now that the sum of the Fourier coefficients $\sum_{S\subseteq\{0,\ldots,7\}} a_S e_{p^{2\ell},S}$ are exactly equal to the right-hand side without remainder term, by using the fact that the coefficients $e_k$ of any linear combination $E(z)=\sum_{k=0}^{\infty} e_k e^{2i\pi kz}$ of Eisenstein series of weight 4 for $\Gamma(N)$ are of the form

$$e_k = \sum_{d|k} d^3 F(d) \tag{36}$$

for some periodic function $F:\mathbb{N}\to\mathbb{C}$ of period $N$ (see for instance [40, Proposition 17, Chapter IV]). We invoke now a slight variation of [32, Lemma 4.4]:

**Lemma 12** *Let $G:\mathbb{N}\to\mathbb{C}$ be periodic and satisfy*

$$\sum_{d|p^m} d^3 G(d) = o(p^{3m}) \ \ \textit{as } m\to\infty$$

*then*

$$\sum_{d|p^m} d^3 G(d) = 0 \ \ \textit{for all } m.$$

PROOF: Let $u_m \overset{\text{def}}{=} \sum_{d|p^m} d^3 G(d)$, then

$$G(p^m) = \frac{u_m - u_{m-1}}{p^{3m}} = \frac{u_m}{p^{3m}} - \frac{u_{m-1}}{p^{3(m-1)}p^3}. \tag{37}$$

We notice now that the right-hand-side term $\frac{u_m}{p^{3m}} - \frac{u_{m-1}}{p^{3(m-1)}p^3}$ tends to 0 as $m$ goes to infinity. $G$ is periodic, therefore $G(p^m)=0$ for all $m$. □

By noticing that

$$\frac{4}{n}\frac{1-p^{3(2\ell+1)}}{1-p^3} = \sum_{d|p^{2\ell}} \frac{4}{n} d^3,$$

writing that

$$\sum_{S\subseteq\{0,\ldots,7\}} a_S e_{p^{2\ell},S} = \sum_{d|p^{2\ell}} d^3 F(d)$$

for some periodic function $F:\mathbb{N}\to\mathbb{C}$ of period $16q^2$, and using Equation (36), we obtain that

$$\sum_{S\subseteq\{0,\ldots,7\}} a_S e_{p^{2\ell},S} - \frac{4}{n}\frac{1-p^{3(2\ell+1)}}{1-p^3} = \sum_{d|p^m} d^3\left(F(d)-\frac{4}{n}\right).$$

From Equation (35) we see that we can apply Lemma 12 to $\sum_{S\subseteq\{0,\ldots,7\}} a_S e_{p^{2\ell},S} - \frac{4}{n}\frac{1-p^{3(2\ell+1)}}{1-p^3}$ and obtain

$$\sum_{S\subseteq\{0,\ldots,7\}} a_S e_{p^{2\ell},S} = \frac{4}{n}\frac{1-p^{3(2\ell+1)}}{1-p^3}. \tag{38}$$

This reduces Equation (33) to

$$\sum_{S\subseteq\{0,\ldots,7\}} a_S c_{p^{2\ell},S} = \frac{2p^{3\ell}}{n}\sum_{j=1}^{n-2}\frac{\sin(2\ell+1)\theta_j}{\sin\theta_j}.$$

and by using the upperbound (34) we finally obtain

$$\frac{2}{n}\sum_{j=1}^{n-2}\frac{\sin(2\ell+1)\theta_j}{\sin\theta_j} = O_\epsilon(p^{2\ell\varepsilon}).$$

Suppose that there is some $\lambda_j \notin [-2p^{3/2}, 2p^{3/2}]$ with $j \in \{1,\ldots,n-2\}$, or equivalently that there is some $\theta_j$ which is not real. There exists a unique $0 < t_j < 1$ such that either $\theta_j = \frac{3i}{2}t_j \ln p$ or $\theta_j = \pi + \frac{3i}{2}t_j \ln p$. Consider the index $j$ of this kind which maximizes $|\lambda_j|$. It is straightforward to check that

$$\frac{2}{n}\sum_{j=1}^{n-2}\frac{\sin(2\ell+1)\theta_j}{\sin\theta_j} = \frac{2|\{i : |\lambda_i| = |\lambda_j|\}|}{n} p^{3\ell t_j}\frac{1-p^{-3t_j(2\ell+1)}}{1-p^{-3t_j}}(1+o(1))$$

as $\ell$ goes to infinity. If $\varepsilon$ is small enough, the right-hand term can not be upper-bounded by $O(p^{2\ell\varepsilon})$ and therefore the same thing holds for $\frac{2}{n}\sum_{j=1}^{n-2}\frac{\sin(2\ell+1)\theta_j}{\sin\theta_j}$. So for $1 \le j \le n-2$, the $\theta_j$'s are real, or equivalently the $\lambda_j$'s are in $[-2p^{3/2}, 2p^{3/2}]$. This proves that the graphs $\mathscr{X}_{p,q}$ are Ramanujan.

**Corollary 3** *For $p < q$ such that $\left(\frac{p}{q}\right) = 1$, the graphs $\mathscr{Y}_{p,q}$ are also Ramanujan.*

Proof: Let $\mu_0 \ge \cdots \ge \mu_{n-1}$ be the spectrum of $\mathscr{Y}_{p,q}$. The equality $\mu_0 = p^3 + 1$ holds. The graphs are not bipartite by Proposition 6 so there is the inequality $\mu_{n-1} > -p^3 - 1$. The spectrum of the bipartite double cover $\mathscr{X}_{p,q}$ of $\mathscr{Y}_{p,q}$ is given by $\pm\mu_0, \ldots, \pm\mu_{n-1}$, counted with multiplicities. But the graphs $\mathscr{X}_{p,q}$ are Ramanujan, that implies $\mu_j \le 2p^{3/2}$ for $j \ne 0$. That is $\mathscr{Y}_{p,q}$ are also Ramanujan. □

## Conclusions

The contributions of this work are twofold. First, the girth problem consisting of finding for an infinite growing family of $k$-regular graphs $\{G_n\}$ what is the largest constant

$$\gamma(\{G_n\}) \overset{\text{def}}{=} \lim_{n\to\infty}\inf\left\{\frac{\text{girth}(G_n)}{\log_{k-1}|G_n|}\right\}$$

reduces now to $\frac{12}{7} \le \gamma \le 2$, for the values of $k = p^3 + 1$, $p$ an odd prime. This is a clear improvement on the 25 years old result $\frac{4}{3} \le \gamma \le 2$.

Second, this is the first construction of Cayley expanders non explicitely based on a group. However, as already mentionned in introduction, we stress that the graphs presented here may be Cayley graphs on groups. The question is then which groups ? A weaker open problem is the vertex-transitivity of these graphs. In any case, it might be interesting to pursue further research toward expansion properties in non-associative algebraic structures. Indeed, the expansion property of Cayley graphs on groups has been thoroughly studied recently. Similar questions arise for loops.

In addition, it may be interesting to carry over the construction of Morgenstern [37] based on quaternions over function fields, to octonions. There would be indeed a hope to build Ramanujan graphs of girth $\frac{12}{7}\log_{k-1} n$ for various degrees $k$, not of the form $k = p^3 + 1$, $p$ is prime.

To conclude, let us recall that the graphs constructed here display other properties shared by all Ramanujan graphs, namely a small diameter $D$ satisfying $D \leq 2\log_{d-1} n + O(1)$ and in the non bipartite case, an independence number $i$ verifying $i \leq \frac{2\sqrt{d-1}}{d}n$ and therefore a chromatic number $\chi$ of the form $\chi \geq \frac{d}{2\sqrt{d-1}}$.

**Acknowledgment** We would like to thank Eiichi Bannai for having pointing out the result of Paige [41] to us.

# References

[1] N. Alon. Eigenvalues and expanders. *Combinatorica*, 6(2):83–96, 1986. Theory of computing (Singer Island, Fla., 1984).

[2] N. L. Biggs. *Algebraic graph theory.* Cambridge University Press, London, 1974. Cambridge Tracts in Mathematics, No. 67.

[3] N. L. Biggs. Graphs with large girth. *Ars Combin.*, 25(C):73–80, 1988. Eleventh British Combinatorial Conference (London, 1987).

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

[5] N. L. Biggs and M. J. Hoare. The sextet construction for cubic graphs. *Combinatorica*, 3:153–165, 1983.

[6] M. Blum, R. M. Karp, O. Vornberger, C. H. Papadimitriou, and M. Yannakakis. The complexity of testing whether a graph is a superconcentrator. *Inform. Process. Lett.*, 13(4-5):164–167, 1981.

[7] B. Bollobás. *Extremal graph theory*, volume 11 of *London Mathematical Society Monographs.* Academic Press Inc. [Harcourt Brace Jovanovich Publishers], London, 1978.

[8] B. Bollobás. The isoperimetric number of random regular graphs. *European J. Combin.*, 9(3):241–244, 1988.

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

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

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

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

[13] 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.

[14] P. Deligne. Formes modulaires et représentations $\ell$-adiques. *Séminaire N. Bourbaki*, exp. n° 355:139–172, 1969.

[15] P. Deligne. La conjecture de Weil. I. *Inst. Hautes Études Sci. Publ. Math.*, 43:273–307, 1974.

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

[17] M. Eichler. Quaternäre quadratische Formen und die Riemannsche Vermutung für die Kongruenzzetafunktion. *Arch. Math.*, 5:355–366, 1954.

[18] P. Erdős and H. Sachs. Reguläre Graphen gegebener Tailenweite mit minimaler Knollenzahh. *Wiss. Z. Univ. Halle-Willenberg Math. Nat.*, 12:251–258, 1963.

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

[20] A. Gamburd, S. Hoory, M. Shahshahani, A. Shalev, and B. Virg. On the girth of random Cayley graphs. *Random Structures and Algorithms*, 35(1):100 – 117, 2009.

[21] S. Hakimi and J. Bredeson. Graph theoretic error-correcting codes. *IEEE Trans. on Inform. Theory,*, 14(4):584 – 591, jul. 1968.

[22] E. Hecke. *Mathematische Werke*. Herausgegeben im Auftrage der Akademie der Wissenschaften zu Göttingen. Vandenhoeck & Ruprecht, Göttingen, 1959.

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

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

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

[26] J. Igusa. Fibre systems of Jacobian varieties. III. Fibre systems of elliptic curves. *Amer. J. Math.*, 81:453–476, 1959.

[27] Y. Ihara. Hecke Polynomials as congruence $\zeta$ functions in elliptic modular case. *Ann. of Math. (2)*, 85:267–295, 1967.

[28] B. W. Jordan and R. Livné. Ramanujan local systems on graphs. *Topology*, 36(5):1007–1024, 1997.

[29] N. Kahale. Eigenvalues and expansion of regular graphs. *J. Assoc. Comput. Mach.*, 42(5):1091–1106, 1995.

[30] F. Lazebnik and V. A. Ustimenko. Explicit construction of graphs with an arbitrary large girth and of large size. *Discrete Appl. Math.*, 60(1-3):275–284, 1995. ARIDAM VI and VII (New Brunswick, NJ, 1991/1992).

[31] W.-C. Winnie Li, M. Lu, and C. Wang. Recent developments in low-density parity-check codes. In *IWCC*, pages 107–123, 2009.

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

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

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

[35] 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.

[36] T. Miyake. *Modular forms*. Springer, 1989.

[37] 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.

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

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

[40] A. Ogg. *Modular forms and Dirichlet series*. W. A. Benjamin, Inc., New York-Amsterdam, 1969.

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

[42] M. S. Pinsker. On the complexity of a concentrator. In *Proc. 7th International Teletraffic Conference*, pages 318/1–318/4, Stockholm, June 1973.

[43] A. Pizer. Ramanujan graphs and Hecke operators. *Bull. Amer. Math. Soc.*, 23(1):127–137, 1990.

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

[45] P. Rosenthal and P. O. Vontobel. Constructions of LDPC codes using Ramanujan graphs and ideas from Margulis. In *Proc. of the 38-th Allerton Conference on Communication, Control, and Computing*, pages 248–257, 2000.

[46] M. Sipser and D. A. Spielman. Expander codes. *IEEE Trans. on Inform. Theory*, 42(6):1710–1722, 1996.

[47] D. A. Spielman. Linear-time encodable and decodable error-correcting codes. *IEEE Trans. on Inform. Theory*, 42(6):1723–1731, 1996.

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

[49] J.-P. Tillich and G. Zémor. Optimal cycle codes constructed from Ramanujan graphs. *SIAM J. Discrete Math.*, 10(3):447–459, 1997.

[50] A. Weil. *Sur les courbes algébriques et les variétés qui s'en déduisent.* Actualités Sci. Ind., no. 1041 = Publ. Inst. Math. Univ. Strasbourg **7** (1945). Hermann et Cie., Paris, 1948.

[51] A. Weiss. Girths of bipartite sextet graphs. *Combinatorica*, 4(2-3), 1984.

[52] A. Wigderson and D. Zuckerman. Expanders that beat the eigenvalue bound: explicit construction and applications. *Combinatorica*, 19(1):125–138, 1999.

# Ramanujan graphs of very large girth based on octonions

X. Dahan and J.-P. Tillich

November 16, 2010

**Abstract**

We present a generalization of the construction of graphs by Lubotzky, Phillips and Sarnak in their celebrated article “Ramanujan graphs” [32]. The new approach consists in using octonion algebras rather than quaternions. A key tool is the existing result of the unique factorization of integral octonions. The families obtained by this mean present not only the same spectral property that make them good expanders, but also show a larger girth, yielding a new record for regular graphs.

## 1 Introduction

**Ramanujan graphs and expanders.** Given a $k$-regular undirected graph $G_{n,k}$ of size $n$, the eigenvalues $\lambda_0 \geq \lambda_1 \geq \cdots \geq \lambda_{n-1}$ of the adjacency matrix of $G_{n,k}$, are real (it is a symmetric matrix) and satisfy $|\lambda_i| \leq k$. Moreover, $\lambda_0 = k$ and if the graph is connected, then $\lambda_1 < k$. The graph is bipartite if and only if $\lambda_{n-1} = -k$. The graph $G$ is a *Ramanujan graph* if all its eigenvalues distinct from $\pm k$ are in the interval $[-2\sqrt{k-1}, 2\sqrt{k-1}]$. Ramanujan graphs are in a sense (asymptotically) extremal graphs with respect to the second largest eigenvalue in absolute value because of the following lower bound due to Alon and Boppana [1]

$$\underline{\lim}_n \lambda(G_{n,k}) \geq 2\sqrt{k-1},$$

where $\lambda(G_{n,k})$ denotes the second largest eigenvalue in absolute value of $G_{n,k}$.

The fact that $\lambda(G_{n,k})$ is so small implies many other properties since they are then good *expander* graphs. Graphs with large expansion have proved to be a quite useful object in various domains ranging from mathematics and computer science to physics, see the survey [23] which depicts some of these applications. Random $k$-regular graphs are known to typically meet such a behavior (see for instance [8] and [42] for the first existence results of good expanders obtained by probabilistic arguments). However, even if this kind of probabilistic argument shows the existence of graphs with large expansion, it does not provide explicit examples of graphs which are good expanders. The approach consisting in generating a graph randomly and then checking whether or not it has large expansion is considered to be impracticable: even checking a weak form of expansion turns out to be coNP-complete [6]. It has been observed that this problem can be circumvented by relating the expansion properties to the spectral gap (that is $\lambda_0 - \lambda_1$) or to $\lambda(G_{n,k})$, see for instance [1]: the expansion coefficient can be lower bounded by an increasing function of the spectral gap or $\lambda(G_{n,k})$. Since these spectral quantities can be computed efficiently with an arbitrary precision, this gives an efficient method for obtaining graphs displaying at least a certain amount of expansion. Up to now, this spectral method has proved to be the best method for certifying a rather large expansion. Ramanujan graphs represent here the graphs with the best *certified* expansion properties known. At the moment, Ramanujan graphs have been superseded only in one case, namely for the expansion of small subsets of vertices [29]: graphs obtained by the zigzag product [52] have a better certified expansion in this case. The guaranteed expansion obtained by taking Ramanujan graphs together with the aforementioned spectral lower bound on the expansion is not as large as the one known for random graphs, however it is generally sufficient and satisfactory for many applications.

Obtaining explicit infinite families of Ramanujan graphs of a given degree has been quite a breakthrough in spectral graph theory. The first constructions of this kind were obtained by Lubotzky-Philips-Sarnak [32] and Margulis [35]. They were followed by the constructions of [43, 10, 37, 28] for instance. From them, Ramanujan graphs have been obtained for all degrees $k$ of the form $k = q + 1$ where $q$ is any prime power.

**Graphs of large girth.** Besides their expansion property, the Ramanujan graphs constructed in [32, 35, 10, 37] presented another breakthrough. They had a *large girth* (the girth being the smallest size of its cycles) and improved significantly the narrow knowledge on this matter. Let us mention (see for instance [2, p.154]) the following upper bound for the girth,

$$\text{for } k \geq 3, \text{ any } k\text{-regular graph } G \text{ verifies:} \qquad \text{girth}(G) \leq 2\log_{k-1}|G|, \tag{1}$$

where $|G|$ denotes the number of vertices of $G$ and girth$(G)$ is the girth $G$. This bound motivates the following definition of Biggs [3]. A family $\{G_i\}_i$ of $k$-regular graphs is of *large girth* if and only if there exists some positive constant $\gamma$ such that for any graph in this family we have

$$\text{girth}(G_i) \geq \gamma \log_{k-1}|G_i|. \tag{2}$$

For a long time, the best result in this direction was the non constructive result of Erdős and Sachs [18] and its improvements by Sauer and Walther (for more details see [7, p. 107]) which showed the existence of families of graphs with $\gamma = 1$. The first explicit constructions were obtained by Margulis [34] but achieved constants $\gamma$ which were strictly smaller than 1. Proving that there exist families of graphs with a value of $\gamma$ greater than 1 was finally obtained in [51] for a family of graphs of degree $k = 3$ suggested by [5], by showing that for these graphs the following inequality holds

$$\text{girth}(G_i) > \frac{4}{3}\log_{k-1}|G_i| - 2.$$

As suggested by [20], large girth needs not be an unusual property for some families of graphs, but those with a constant $\gamma > 1$ tends to be very seldom[1]. The bipartite Ramanujan graphs constructed in [32, 35] also achieved the constant $\gamma = \frac{4}{3}$ but this time for all degrees of the form $k = p + 1$, where $p$ is a prime number strictly greater than 2 (originally, only for the primes $p \equiv 1 \pmod 4$, and for any odd primes, see [13]). Ramanujan graphs of degree 3 which achieved $\gamma = \frac{4}{3}$ were obtained afterwards in [10]. Moreover, Morgenstern in [37] finally obtained infinite families of Ramanujan graphs achieving $\gamma = \frac{4}{3}$ for all degrees of the form $k = q + 1$ where $q$ is any prime power. These Ramanujan constructions do not only overcome the $\gamma = 1$ barrier, they are also explicit which is essential for applications. It should also be mentioned that a quite different graph construction has been proposed in [30] for degrees of the form $k = q$ where $q$ is a prime power, and where it has been shown that it contains connected components $G_i$ which satisfy the inequality

$$\text{girth}(G_i) \geq \frac{4}{3}\log_k(k-1)|G_i|,$$

which is slightly worse than the constant $\gamma = \frac{4}{3}$ achieved in the aforementioned articles but achieves it asymptotically as the degree $k$ goes to infinity.

[1] To quote [20], "it is a miracle that the lower bound constant $\frac{4}{3}$ is greater than 1" (see for example Conjecture 5 in their paper)

**Our contribution.** One of the main result of our paper is to obtain families of graphs which improve upon $\gamma = \frac{4}{3}$ in (2). We give here a construction of infinite families of regular graphs for degrees of the form $k = p^3 + 1$, where $p$ is any odd prime, for which

$$\text{girth}(G_i) \geq \frac{12}{7} \log_{k-1} |G_i| - 2 \log_p 2.$$

We also prove that these graphs are Ramanujan. These graphs exist for all sizes of the form $n = q^7 - q^3$, where $q$ is any odd prime satisfying $q > p$.

The idea underlying our construction is to replace in the Ramanujan graph construction of Lubotzky-Philipps-Sarnak & Margulis the quaternions by octonions. An important tool to build these graphs is a unique factorization property, that is available for integral octonions since the work of Rehm [44]. The Ramanujan graphs of [32, 35] built upon quaternions can be described as Cayley graphs on *groups*. This is no more the case for our construction on octonions. These graphs have a description in terms of Cayley graphs on *loops*, the non-associative counterpart of groups.

**Comments.** The property of large girth, besides its own theoretical interest, can be applied to LDPC codes. This approach was pioneered by Margulis in [34], 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 [48] 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 [19], but that does not hold anymore for a larger number of iterations.

Lower bounds on the code minimum distance and the number of errors which can be decoded with iterative decoding algorithms can also be obtained from lower bounds on the expansion [46, 47]. It makes sense in this context to use graphs which are at the same time of large girth and good expanders. The Ramanujan graphs proposed by [32, 35] are very good candidates for this. This was suggested in [45], see also [31]. It should also be mentioned that there is one particular LDPC code family where both properties of being Ramanujan and having a large girth can be used together, namely for cycle codes which were introduced in [21], where it can be proved (see [49]) that regular cycle codes obtained from the constructions of Ramanujan graphs given in [32, 35, 37] correct the largest possible fraction of errors. It should be pointed out here that the approach used in [49] could also be applied to the Ramanujan graphs based on octonions given here and that the larger girth of our construction compared to the constructions of [32, 35, 37] would lead to improved upper bounds on the probability of error after decoding.

Cayley graphs are usually thought to require groups. This is absolutely not necessary, much weaker algebraic structures like *quasi-groups* are sufficient. For a modern treatment, see [39] and references therein. The algebraic non-associative structures arisen from octonions algebra are well-known, and have the strong property of being *Moufang loops*. It is tempting to think that these would constitute the first algebraic construction of expanders not based on a group. But we do not know whether there exist groups on top of which these graphs could be Cayley graphs. We did not even prove that they are vertex-transitive, which is a stricly weaker property than being a Cayley graph on a group.

## 2 Preliminaries on octonions

All the material on octonions required for this construction is contained in the article of Rehm [44], where a more substantial bibliography can be found. A good complementary material is Ch.9 of [11]. For convenience, we define and cite 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 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.* Here we will choose $R = \mathbb{Z}, \mathbb{Q}, \mathbb{F}_p$. 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

$$\mathsf{i}^2 = \mathsf{j}^2 = \mathsf{k}^2 = -1, \; \mathsf{ij} = \mathsf{k}. \tag{3}$$

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

$$\begin{aligned} \bar{1} &= 1 \\ \overline{\alpha + \beta} &= \overline{\alpha} + \overline{\beta} \\ \overline{\alpha\beta} &= \overline{\beta}\overline{\alpha}. \end{aligned} \tag{4}$$

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

$$(\alpha_1 + \alpha_2\mathsf{t})(\beta_1 + \beta_2\mathsf{t}) = \alpha_1\beta_1 - \bar{\beta}_2\alpha_2 + (\beta_2\alpha_1 + \alpha_2\bar{\beta}_1)\mathsf{t} \tag{5}$$

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 (Cf. [12]) that among the 35 possible triads, only 7 are associative, namely:

$$\mathsf{i}, \mathsf{j}, \mathsf{k} \quad , \quad \mathsf{i}, \mathsf{t}, \mathsf{it} \quad , \quad \mathsf{j}, \mathsf{t}, \mathsf{jt} \quad , \quad \mathsf{k}, \mathsf{t}, \mathsf{kt}, \quad \text{and} \quad \mathsf{k}, \mathsf{jt}, \mathsf{it} \quad , \quad \mathsf{j}, \mathsf{it}, \mathsf{kt} \quad , \quad \mathsf{i}, \mathsf{kt}, \mathsf{jt}. \tag{6}$$

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

$$\text{(alternative algebra identities)} \qquad (\alpha\alpha)\beta = \alpha(\alpha\beta) \quad \text{and} \quad \beta(\alpha\alpha) = (\beta\alpha)\alpha. \tag{7}$$

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

In our case, we will often use the following corollary

**Corollary 1** *Let $\alpha, \beta$ be elements of $\mathbb{O}(\mathbb{Q})$. Then*

$$(\alpha\beta)\bar{\beta} = \alpha(\beta\bar{\beta}), \; \alpha(\bar{\alpha}\beta) = (\alpha\bar{\alpha})\beta. \tag{8}$$

Octonions are endowed with a *norm* $N$, that is a quadratic form. Here, the associated bilinear map will be:

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

Hence, the norm is here simply a sum of 8 squares. It can be defined equivalently by $N(\alpha) = \alpha\bar{\alpha}$. The important property is its *multiplicativity*: $N(\alpha\beta) = N(\alpha)N(\beta)$ for any octonions $\alpha$ and $\beta$. This follows directly from Theorem 1 and the antiautomorphism property (4)

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

Let $\mathbb{O}(R)^\star$ denote the set of invertible octonions. Clearly, if $\alpha$ is invertible, then $\alpha^{-1} = N(\alpha)^{-1}\overline{\alpha}$. It follows that:

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

**Loops.** The set of invertible elements in an alternative ring is a *Moufang loop* (Cf. [9, p. 254] and [11, 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*. We denote in this case by $x^{-1}$ 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:

$$\text{Moufang identities:} \qquad \begin{array}{l} (\alpha\beta\alpha)\gamma = \alpha((\beta\alpha)\gamma) \\ (\alpha\beta)(\gamma\alpha) = \alpha(\beta\gamma)\alpha \\ ((\beta\alpha)\gamma)\alpha = \beta(\alpha\gamma\alpha) \end{array} \tag{9}$$

It is straightforward to check that a Moufang loop is an inverse loop [11, Ch. 7] or [9, 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*[2]. In the quaternions 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 $1 + i + j + k$). Hurwitz noticed that it is possible to obtain a satisfactory arithmetic of quaternions by considering instead quaternions with integer or half integer coordinates [24, 25], and his result was fully understood after Dickson [16] 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 [12]. They allow as in the case of Hurwitz quaternions to obtain a set of octonions which obey the essential divisibility

[2] or that the *class number of ideals* is equal to 1. But for constructive purposes, the Eulidean 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 (6). 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 [44, Prop. 4.1], obtained a kind of distortion of the Euclidean algorithm, by using only the alternative property (7). 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 $1, \mathsf{i}, \mathsf{j}, \mathsf{k}, \mathsf{h}, \mathsf{ih}, \mathsf{jh}, \mathsf{kh}$ (Cf. [12, p 567]). 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 which satisfy*

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

Given an octonion $\alpha = a_0 + a_1\mathsf{i} + \ldots + a_7\mathsf{kt} \in \mathbb{O}(\mathbb{Q})^\star$, we say that it is positive and write $\alpha > 0$ if and only if the smallest $i$ such that $a_i \neq 0$ is $> 0$. Let $p$ be an odd prime number. Related to *unique* factorization, we define (Cf. [44, Prop. 5.6]):

$$\mathscr{P}(p) \overset{\text{def}}{=} \{\alpha \in \mathbb{O}(\mathbb{Z}) : \ \alpha > 0 \ , \quad N(\alpha) = p \ , \quad \alpha - 1 \in 2\mathcal{C}_{\mathbb{O}}\} \tag{10}$$

Rehm also proved that $|\mathscr{P}(p)| = p^3 + 1$ (Cf. [44, Prop. 6.4]). The main result of him in [44], that is fundamental in the present work is the following:

**Theorem 2** *[44] Let $\alpha \in \mathcal{C}_{\mathbb{O}}$ be primitive, that is 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 prime integers, not necessarily distinct. There exist 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:*

$$\alpha = \big(\cdots(\epsilon\pi_1\pi_2)\pi_3\cdots\big)\pi_s,$$

*with $\epsilon \in \mathcal{C}_{\mathbb{O}}^\star$ and $\pi_i \in \mathscr{P}(p_i)$.*

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

# 3 Arithmetic construction of the infinite $(p^3+1)$-regular tree

**Overview of the whole construction.** Similarly to [32, 35, 10, 37], our Ramanujan graph construction can be decomposed in two steps.

1. The first step consists of constructing the $(p^3+1)$-regular infinite tree in an arithmetic way

by using octonions.
2. Finite Ramanujan graphs are derived from this tree by taking suitable finite quotients of this tree which do not create small cycles.

We will detail the first step in this section. It will also turn out that our construction has a description in terms of Cayley graphs defined over loops. This will be explained in Section 4.

**Several useful lemmas on the factorization of octonions of norm $p^t$.** The main ingredients used for the construction are the unicity of factorization property of Theorem 2 and considering products of elements of $\mathcal{C}_{\mathbb{O}}$ of the following form

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

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 $\mathcal{C}_{\mathbb{O}}$ which are not irreducible can be simplified by using Corollary 1 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 an invertible element $\epsilon$ in $\mathcal{C}_{\mathbb{O}}^\star$ and elements $\pi_1, \dots, \pi_t$ of $\mathscr{P}(p)$ is primitive.*

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

$$c(\alpha)|c(\alpha\bar{\pi}) \tag{11}$$

because the coefficients of $\alpha\bar{\pi}$ are integer linear combinations of the coefficients of $\alpha$ in a $\mathbb{Z}$ basis. Since $\alpha\bar{\pi} = (\beta\pi)\bar{\pi} = \beta(\pi\bar{\pi}) = p\beta$ by Corollary 1, we obtain that $c(\alpha\bar{\pi}) = p$. This together with (11) implies that $c(\alpha) = p$ and that $p$ divides $\alpha$. We may therefore write $\alpha$ as $\alpha = \gamma p = \gamma(\bar{\pi}\pi) = (\gamma\bar{\pi})\pi$ (by using Corollary 1 again) for some $\gamma \in \mathcal{C}_{\mathbb{O}}$. Therefore $\beta = \gamma\bar{\pi}$. $\gamma$ is necessarily primitive, since $\beta$ is primitive. By Theorem 2, we can write $\gamma$ as an irreducible product of a unit $\epsilon$ and elements $\pi_1, \dots, \pi_s$ of $\mathscr{P}(p)$:

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

This implies that $\beta$ is of the form

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

This is an irreducible product, for if $\pi_s$ were equal to $\pi$, $\beta$ would be divisible by $p$ and would not be primitive. From Theorem 2 applied to $\beta$, we know that this is the only way we can write $\beta$ as an irreducible product, and therefore that the product $\alpha$ is necessarily of the form

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

which contradicts the assumption on its irreducibility. □

**Proposition 1** *Any element $\alpha \in \mathbb{O}(\mathbb{Z})$ of norm $N(\alpha) = p^t$ and with $\alpha \equiv 1 \bmod 2\mathcal{C}_{\mathbb{O}}$, 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: First of all, let us assume that there exist an non-negative integer $s$, an $\epsilon$ in $\mathcal{C}_{\mathbb{O}}^{\star}$ and elements $\pi_1, \dots, \pi_u$ such that $\alpha$ can be written as an irreducible product

$$\alpha = p^s\big(\dots((\epsilon\alpha_1)\alpha_2)\alpha_3\cdots\big)\alpha_u. \tag{12}$$

By taking norms on both sides, we see that $u = t - 2s$. Moreover, by Lemma 2, the irreducible product $\big(\dots((\epsilon\alpha_1)\alpha_2)\alpha_3\cdots\big)\alpha_u$ is primitive. Therefore $p^s$ is necessarily the largest power of $p$ which divides $\alpha$. We choose now $s$ like this, and since $p^{-s}\alpha$ is in $\mathbb{O}(\mathbb{Z})$ and is primitive, we can apply Rehm's theorem to it and write $p^{-s}\alpha = \big(\dots((\epsilon\alpha_1)\alpha_2)\cdots\big)\alpha_{t-2s}$, with $\epsilon \in \mathcal{C}_{\mathbb{O}}^{\star}$ and $\alpha_i \in \mathscr{P}(p)$. In other words $\alpha$ can be written in the form given in (12). The unicity of this form follows from the discussion above and the unicity of the decomposition of $p^{-s}\alpha$ ensured by Theorem 2.

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

"$a \in \mathcal{C}_{\mathbb{O}} - \mathbb{O}(\mathbb{Z})$ 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 $\mathbb{O}(Z)$ and finishes the proof of the aforementioned property.

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

Therefore, $\epsilon$ is among the 16 units of $\mathbb{O}(\mathbb{Z})^{\star}$. By using Corollary 1, it is straightforward to check that we can write $\epsilon$ as

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

The set $1 + 2\mathcal{C}_{\mathbb{O}}$ is stable by multiplication, therefore $\big(\dots((\alpha\bar{\alpha}_{t-2s})\bar{\alpha}_{t-2s-1}\big)\cdots\alpha_2\big)\bar{\alpha}_1$ belongs to $1 + 2\mathcal{C}_{\mathbb{O}}$ and so does $\epsilon$. 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 $\pm 1$. □

**The construction of the infinite tree** This lemma 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 $\Lambda$ 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 $\Lambda$;

- edge set defined as follows. By Proposition 1, any vertex can be viewed in a unique way as a irreducible product $(\ldots(\alpha_1\alpha_2)\cdots\alpha_{s-1})\alpha_s$ where the $\alpha_i$'s belong to $\mathscr{P}(p)$. There is an edge between $(\ldots(\alpha_1\alpha_2)\cdots\alpha_{s-1})\alpha_s$ and vertices of the set
$$\{(\ldots(\alpha_1\alpha_2)\cdots)\alpha_{s-1}\} \cup \{((\ldots(\alpha_1\alpha_2)\cdots\alpha_{s-1})\alpha_s)\pi : \pi \in \mathscr{P}(p) - \{\bar{\alpha_s}\}\}$$
By the convention that the void product is equal to 1, the vertex 1 is linked with all vertices labelled by $\pi$, 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** Let us give an interpretation of this arithmetic construction of the $(p^3+1)$-regular tree in terms of a *Cayley graph on a loop*, which is a slight generalization of the usual Cayley graph definition (see for instance [39]).

**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[3] 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** *[38, Theorem 8] $\mathscr{C}ay(L,S)$ is a $|S|$-regular graph without loops iff*
*(i) $\forall\, l \in L,\ l \notin lS$,*
*(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 Cayley graph on a certain loop [38].

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

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

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

[3] 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.

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

Let $\alpha$ be some element of $\Lambda$. 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 $\Lambda$. 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 $\Lambda$ is a loop. It remains to show that $*$ satisfies the Moufang identities (9).

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

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

for some non-negative integers $s_1, s_2$ and $s_3$. From the Moufang identities (9), $(\alpha(\beta\alpha))\gamma = \alpha((\beta\alpha)\gamma)$, 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 $\Lambda$ 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:*

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

# 4 Obtaining finite graphs from $T$ by reducing $\Lambda$ modulo another prime $q$

**Reducing to finite graphs** Basically, finite graphs are obtained from the arithmetic construction of $T$ by reducing the octonions in $\Lambda$ 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 $\Lambda$ is a power of $p$ which is therefore invertible modulo $q$. Let us denote by $\tau_q$ the reduction modulo $q$ map $\tau_q : \mathbb{O}(\mathbb{Z}) \to \mathbb{O}(\mathbb{F}_q)$. By the definition of the profuct $*$, the following holds:

$$\tau_q(\alpha * \beta) = \tau_q(\epsilon p^{-s}\alpha\beta) = \tau_q(\epsilon p^{-s})\tau_q(\alpha)\tau_q(\beta), \tag{13}$$

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 $\mathbb{O}(\mathbb{F}_q)^\star$. Subset that appears to be precisely the center $\mathcal{Z}$ of $\mathbb{O}(\mathbb{F}_q)^\star$, as can easily be checked. It follows that the two elements $\tau_q(\alpha * \beta)$ and $\tau_q(\alpha)\tau_q(\beta)$ differs 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 word, the map

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

is a loop homomorphism. Indeed, Equality (13) clearly implies $\mu_q(\alpha * \beta) = \mu_q(\alpha)\mu_q(\beta)$. In addition, $\mathbb{O}(\mathbb{F}_q)^\star$ is a Moufang loop, $\mathbb{O}(\mathbb{F}_q)^\star/\mathcal{Z}$ is itself a Moufang loop. We have proved:

**Lemma 3** *The map $\mu_q$ is a homomorphism of Moufang loops.*

Our graphs will be defined as $\mathscr{C}ay(\mathrm{Im}\ \mu_q, \mu_q(\mathscr{P}(p))$ when these graphs are bipartite or by double covers of this 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 $\mathscr{C}ay(\mathrm{Im}\ \mu_q, \mu_q(\mathscr{P}(p))$ 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 $\mu_q$**.** Let us bring in $M_1$ and $M_p$ the subloops of $\mathbb{O}(\mathbb{F}_q)^\star$ consisting of invertible elements of norm 1 for $M_1$, and of norm a power of $p$ for $M_p$. Let $\mathcal{Z}_p \overset{\text{def}}{=} \{\pm p^s, s = 0, 1, \ldots, q-2\}$ and $\mathcal{Z}_1 \overset{\text{def}}{=} \{-1, 1\}$. Since $\mathcal{Z}_1 \subset \mathcal{Z}_p \subset \mathbb{F}_q^\star$ we can embed the corresponding quotient loops in $\mathbb{O}(\mathbb{F}_q)^\star/\mathcal{Z}$ as follows

$$\begin{tikzcd}[row sep=small] M_1/\mathcal{Z}_1 \arrow[r, hook] & M_p/\mathcal{Z}_p \arrow[r, hook] & \mathbb{O}(\mathbb{F}_q)^\star/\mathcal{Z} \\ a\mathcal{Z}_1 \arrow[r, mapsto] & a\mathcal{Z}_p & \\ & b\mathcal{Z}_p \arrow[r, mapsto] & b\mathcal{Z} \end{tikzcd} \qquad (14)$$

*Via* these embeddings, they can be identified as subloops of $\mathbb{O}(\mathbb{F}_q)^\star/\mathcal{Z}$. By a result of Paige [41, Theorem 4.1] $M_1/\mathcal{Z}_1$ is a simple Moufang loop, and an index 2 normal subloop[4] 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 $M_p/\mathcal{Z}_p = M_1/\mathcal{Z}_1$ or $\mathbb{O}(F_q)^\star/\mathcal{Z}$ (Cf. Corollary 2 for an answer to this issue).

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

PROOF: Every elements of $\Lambda$ has a norm a 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 $\alpha = a_0 + a_1\mathsf{i} + \ldots + a_7\mathsf{kt} \in \mathbb{O}(\mathbb{Z})$ such that $N(\alpha) \equiv p^r \pmod{q}$ for some integer $r$, there exists an element $\beta = b_0 + b_1\mathsf{i} + \ldots + b_7\mathsf{k} \in 1 + 2\mathcal{C}_{\mathbb{O}}$ such that
(i) $a_i \equiv b_i \pmod{q}$,
(ii) $N(\beta) = p^\ell$ for some integer $\ell$.

To prove this claim we use as in [32, Prop. 3.3], a result of Malyshev on the number of solutions of integral definite-positive quadratic forms [33]. 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 $N \geq K(f)$, $N$ generic for $f$ (that is $f \equiv N \pmod{r}$ has at least one solution for every $r$), $\gcd(m, 2Nd) = 1$ and for which there exist integers $a_i$ such that $\gcd(a_1, \ldots, a_n, m) = 1$, $f(a_1, \ldots, a_n) \equiv N \pmod{m}$, then there are integers $b_1, \ldots, b_n$ such that
(i) $b_i \equiv a_i \pmod{m}$,
(ii) $f(b_1, \ldots, b_n) = N$. Let us first assume that $p \equiv 1 \pmod{4}$. We apply the aforementioned result of Malyshev to $f(x_0, \ldots, x_7) \overset{\text{def}}{=} x_0^2 + 4(x_1^2 + \cdots + x_7^2)$. This is an integral positive definite quadratic form. The discriminant of $f$, $d = 2^7$, verifies $\gcd(2dp^\ell, q) = 1$ for any $\ell$. 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 $\alpha$ (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 $\ell$ such that $p^\ell \geq K(f)$ and $p^\ell \equiv p^r \pmod{q}$. It is straightforward to check that $p^\ell$ is generic for $f$ (this follows from the fact that $p^\ell \equiv 1 \pmod{4}$). 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 $\beta$ of norm equal to $p^\ell$ 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 before for the case where $\ell$ is even, since in this case $p^\ell \equiv 1 \pmod{4}$. In the case of an odd $\ell$, $p^\ell$ 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

[4] From Corollary of Lemma 3.4 of [41], since $q > p$ is an odd prime.

$x_0^2 \equiv 3 \pmod 4$ which has no solution. In order to treat this case we consider another quadratic form, namely

$$f(x_0, \dots, x_7) \overset{\text{def}}{=} 4(x_0^2 + x_1^2 + x_2^2 + x_3^2 + x_4^2) + x_5^2 + x_6^2 + x_7^2. \tag{15}$$

This time $p^\ell$ is generic for $f$. Moreover a solution in $\mathbb{Z}^8$ of the equation $f(x_0, \dots, x_7) = p^\ell$ gives an element $\beta = 2x_0 + 2x_1\mathsf{i} + 2x_2\mathsf{j} + 2x_3\mathsf{k} + 2x_4\mathsf{t} + x_5\mathsf{it} + x_6\mathsf{jt} + x_7\mathsf{kt}$ of norm $p^\ell$. Let us show that $\beta$ is also in $1 + 2\mathcal{C}_{\mathbb{O}}$. By reducing Equation (15) modulo 4, we obtain $x_5^2 + x_6^2 + x_7^2 \equiv 3 \pmod 4$, hence:

$$x_5 \equiv x_6 \equiv x_7 \equiv 1 \pmod 2.$$

The element $\frac{\beta-1}{2} = \frac{2x_0-1}{2} + x_1\mathsf{i} + x_2\mathsf{j} + x_3\mathsf{k} + x_4\mathsf{t} + \frac{x_5}{2}\mathsf{it} + \frac{x_6}{2}\mathsf{jt} + \frac{x_7}{2}\mathsf{kt}$ 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 $\beta$ in $1 + 2\mathcal{C}_{\mathbb{O}}$ of norm $p^\ell$. By applying Proposition 1 to it, we can write $\beta$ as

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

for some non-negative integer $s$, $\epsilon$ in $\{-1, 1\}$ and $\gamma$ in $\Lambda$. Since $\tau_q(\alpha) = \tau_q(\beta)$ we have that $\tau_q(\beta) \in \tau_q(\alpha)\mathscr{Z}_p$ and therefore $\tau_q(\gamma) \in \tau_q(\alpha)\mathscr{Z}_p$. In other words, $\tau_q(\alpha)\mathscr{Z}_p \in \mathrm{Im}\ \mu_q$. □

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

**Corollary 2** *If* $\left(\frac{p}{q}\right) = 1$, *then* $\mathrm{Im}\ \mu_q = M_1/\mathscr{Z}_1$.

*Else, when* $\left(\frac{p}{q}\right) = -1$, $\mathrm{Im}\ \mu_q = \mathbb{O}(\mathbb{F}_q)^\star/\mathscr{Z}$.

PROOF: The loop homomorphism $\mathbb{O}(\mathbb{F}_q)^\star \to \mathbb{Z}/2\mathbb{Z}$, $\alpha \mapsto \left(\frac{N(\alpha)}{q}\right)$, regarding the definition of $\mathscr{Z}$, factorizes into this homomorphism: $\varepsilon : \mathbb{O}(\mathbb{F}_q)^\star/\mathscr{Z} \to \mathbb{Z}/2\mathbb{Z}$. Its kernel contains $M_1/\mathscr{Z}_1$.

Besides, for $\pi \in \mathscr{P}(p)$, $\mu_q(\pi)$ is mapped by $\varepsilon$ to 1 or -1 in $\mathbb{Z}/2\mathbb{Z}$, according to the sign of $\left(\frac{p}{q}\right)$. This shows that if $\left(\frac{p}{q}\right) = -1$, then $\mu_q(\mathscr{P}(p)) \subset \mathbb{O}(\mathbb{F}_q)^\star/\mathscr{Z} - M_1/\mathscr{Z}_1$. From Lemma 4, we know that $M_1/\mathscr{Z}_1 \subsetneq M_p/\mathscr{Z}_p = \mathrm{Im}\ \mu_q$, from which follows $\mathrm{Im}\ \mu_q = \mathbb{O}(\mathbb{F}_q)^\star/\mathscr{Z}$ by Paige's theorem.

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

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

$$\ker\mu_q \overset{\text{def}}{=} \Lambda(q) = \{\alpha \in \Lambda \text{ s.t } q|a_1, \dots, q|a_7\}, \quad \text{and then} \quad \Lambda/\Lambda(q) \simeq \mathbb{O}(\mathbb{F}_q)^\star/\mathscr{Z}. \tag{16}$$

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

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

We have $|\mathbb{O}(\mathbb{F}_q)^\star/\mathscr{Z}| = q^7 - q^3$ [44, 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 $\Lambda$ as a loop. The proof of Corollary 2 showed that $\mathscr{S}(p,q)$ generates $M_1/\mathscr{Z}_1$ if $\left(\frac{p}{q}\right) = 1$, and $\mathbb{O}(\mathbb{F}_q)^\star/\mathscr{Z}$ 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 [44, 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 $\pi$ and $\pi'$ in $\mathscr{P}(p)$ give the same element in $\mathbb{O}(\mathbb{F}_q)^\star/\mathscr{Z}$ through $\mu_q$. The equality $\tau_q(\pi)\mathscr{Z} = \tau_q(\pi')\mathscr{Z}$ is equivalent to $\mu_q(\pi * \overline{\pi'}) \in \ker \mu_q = \Lambda(q)$. By Equation (16), taking norm 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 $p^2 \geq q^2$, excluded since $p < q$. If $x = 0$, then $\pi * \overline{\pi'} \in \mathscr{Z}$, 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 $\mu_q$ is an homomorphism by Lemma 3 also holds $\mathscr{S}(p,q)^{-1} = \mathscr{S}(p,q)$. Last, $1\mathscr{Z} \notin \mathscr{S}(p,q)$, else there would be a $\pi \in \mathscr{P}(p)$ that would also be in $\Lambda(q)$, by Equation (16), that is easily checked to be 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 $\mathcal{A} \cup \mathcal{B} = \mathbb{O}(\mathbb{F}_q)^\star/\mathscr{Z}$ of the set of vertices of $\mathscr{X}_{p,q}$:

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

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 $M_1/\mathscr{Z}_1$ would imply a non trivial loop homomorphism:

$$M_1/\mathscr{Z}_1 \to \mathbb{Z}/2\mathbb{Z}.$$

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

It is interesting to consider the *bipartite double cover* of $\mathscr{Y}_{p,q}$ when $\left(\frac{p}{q}\right) = 1$, especially for the treatment of the girth in the next section. Recall here that the double cover of a graph $G$ with vertex set $V$ and edge set $E$ is the graph with vertex set $V' = V \times \{0,1\}$ and there is an edge between $(x,b)$ and $(x',b')$ if and only if $\{x,x'\} \in E$ and $b' \neq b$. The double cover is a bipartite graph and is connected if and only if $G$ is not bipartite.

**Definition 6** *When $\left(\frac{p}{q}\right) = -1$, we define $\mathscr{X}_{p,q}$ as the bipartite double cover of $\mathscr{Y}_{p,q}$.*

It follows that $|\mathscr{X}_{p,q}| = q^7 - q^3$ for any primes $2 < p < q$.

## 5 Bound on the girth

The result hereunder establishes a new lower bound on the maximal girth of regular graphs.

**Theorem 3** *For all couples $(p, q)$ of odd primes such that $p < q$, denoting $k = p^3 + 1$, we have:*
*(i) that the girth of $\mathscr{X}_{p,q}$, which we denote by $\mathrm{girth}(\mathscr{X}_{p,q})$, satisfies*

$$\mathrm{girth}(\mathscr{X}_{p,q}) \geq \frac{12}{7} \log_{k-1} |\mathscr{X}_{p,q}| - 2 \log_p 2.$$

*The constant $\frac{12}{7}$ is the largest possible.*

*(ii) For the non-bipartite graphs $\mathscr{Y}_{p,q}$ (defined when $\left(\frac{p}{q}\right) = 1$), the inequality*

$$\mathrm{girth}(\mathscr{Y}_{p,q}) \geq \frac{6}{7} \log_{k-1} |\mathscr{X}_{p,q}| - \log_p 2 = \frac{6}{7} \log_{k-1} |\mathscr{Y}_{p,q}| - \frac{5}{7} \log_p 2$$

*holds.*

The proof of this theorem follows an approach similar to the one used in [32, 35] for the lower bound, and [35, 4] for the tightness of this bound. However compared to the Ramanujan graphs based on quaternions there is an additional difficulty. The former are Cayley graphs on groups, they are vertex transitive and it is therefore enough to lower bound the size of a cycle starting at the 1 vertex (1 stands here for the identity in the loop). We do not know whether our construction is vertex transitive or not, however it is enough to study the cycles starting at the 1 vertex in our case too. This is a consequence of the following result.

**Lemma 6** *Given $\alpha$ in $\Lambda$, there is a one-one correspondence between:*
*(a) the closed paths without backtracking of length $t'$ starting at the vertex $\mu_q(\alpha)$, and*
*(b) the irreducible products in $\Lambda$ of length $t'$ belonging to the kernel $\Lambda(q)$ of $\mu_q$.*

Proof: A closed path of length $t'$ without backtracking starting at $\mu_q(\alpha)$ corresponds to an irreducible product in $\Lambda$, of length $t'$, with letters denoted by $\beta_1, \ldots, \beta_{t'} \in \mathscr{P}(p)$ such that:

$$\forall 2 \leq i \leq t' {-} 1, \quad \mu_q\left(\left(\ldots(\alpha * \beta_1) * \cdots\right) * \beta_{i+1}\right) \neq \mu_q\left(\left(\ldots(\alpha * \beta_1) * \cdots\right) * \beta_{i-1}\right), \quad \text{(no backtracking)}$$

$$\text{and if} \quad \gamma \overset{\text{def}}{=} \big(\ldots(\alpha * \beta_1) * \cdots\big) * \beta_{t'}, \text{ then } \mu_q(\alpha) = \mu_q(\gamma) \qquad \text{(closed path).}$$

We must show that the irreducible product $\beta \overset{\text{def}}{=} (\cdots(\beta_1\beta_2)\cdots)\beta_{t'}$ is in $\Lambda(q)$. By Corollary 1,

$$\gamma\overline{\beta_{t'}} = \big(\cdots(\alpha\beta_1)\cdots\beta_{t-1})\beta_{t'}\big)\overline{\beta_{t'}} = \big(\cdots(\alpha\beta_1)\cdots\beta_{t'-1}\big)(\beta_{t'}\overline{\beta_{t'}}) = p\big(\cdots(\alpha\beta_1)\cdots\big)\beta_{t'-1}.$$

By induction it arrives $\gamma\overline{\beta} = p^{t'}\alpha$, or $\gamma * \overline{\beta} = \alpha$, or $\mu_q(\gamma)\mu_q(\overline{\beta}) = \mu_q(\alpha)$. But by assumption, $\mu_q(\gamma) = \mu_q(\alpha)$, which implies $\mu_q(\overline{\beta}) = 1\mathcal{Z}$, since $\mathbb{O}(\mathbb{F}_q)^\star/\mathcal{Z}$ is a loop. Equivalently, $\overline{\beta} \in \ker \mu_q = \Lambda(q)$, and hence $\beta$ as well, as can be easily checked.

Reciprocally, let us consider an irreducible product $\gamma$ in $\Lambda(q)$ of $t'$ elements $\gamma_1, \ldots, \gamma_{t'}$ in $\mathscr{P}(p)$. Let:

$$\delta \overset{\text{def}}{=} \big((\ldots(\alpha\gamma_1)\cdots\gamma_{t'-1}\big)\gamma_{t'}.$$

As seen above, $\delta * \overline{\gamma} = \alpha$. It follows that $\mu_q(\delta * \overline{\gamma}) = \mu_q(\delta)\mu_q(\overline{\gamma})$. By assumption, $\mu_q(\gamma) = 1.\mathscr{Z}$, therefore we also have $\mu_q(\overline{\gamma}) = 1.\mathscr{Z}$. So $\mu_q(\alpha) = \mu_q(\alpha * \overline{\gamma})$. This corresponds to a path of length $t'$, without backtracking, starting at $\mu_q(\alpha)$. □

The second lemma gives a tight lower bound on the size of irreducible products in $\Lambda$ of *even* length that belong to $\Lambda(q)$. This yields therefore a tight lower bound on the size of cycles of even length in the graphs $\mathscr{X}_{p,q}$ or $\mathscr{Y}_{p,q}$.

**Lemma 7** *Given $t > 0$, there exists an irreducible product in $\Lambda(q)$ of length $2t$ if and only if $2p^t > q^2$.*

Proof: Let $\beta \in \Lambda(q)$ be as in the statement. It can be written as $\beta = b_0 + q(b_1\mathsf{i} + \cdots + b_7\mathsf{kt})$ where the $b_i$'s are integer coefficients. Moreover, $N(\beta) = p^{2t}$ gives:

$$b_0^2 + q^2(b_1^2 + \cdots + b_7^2) = p^{2t}. \tag{17}$$

At least one $b_i$ (with $i > 0$) is non zero, 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 $p^t \equiv \pm b_0 \pmod{q^2}$. We 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

$$\begin{aligned} p^{2t} &= (p^t - mq^2)^2 + q^2(b_1^2 + \cdots + b_7^2) \\ &= p^{2t} - 2mq^2p^t + m^2q^4 + q^2(b_1^2 + \cdots + b_7^2) \\ &\Leftrightarrow 2mp^t - m^2q^2 = b_1^2 + \cdots + b_7^2. \end{aligned} \tag{18}$$

Then it follows that $2p^t - mq^2 > 0$. This is because at least one $b_i$ (with $i > 0$) is different from 0, achieving the first part of the proof.

Reciprocally, if $m$ is such that $2p^t > mq^2$, can be represented by a sum of seven squares: $2mp^t - m^2q^2 = a_1^2 + \cdots + a_7^2$. We may even choose arbitrarily two of them since any positive integer is a sum of 5 squares. This will be done as follows. First we choose $a_0 = p^t - mq^2$. Then we choose $a_1, a_2$ in such a way that their parity is different from the parity of $a_0$. Notice also that

$$\begin{aligned} a_0 &\equiv a_0^2 \pmod 2 \\ &\equiv p^{2t} - q^2(a_1^2 + \ldots + a_7^2) \pmod 2 \\ &\equiv 1 + a_1 + \ldots + a_7 \pmod 2 \end{aligned}$$

This implies that the number of the $a_i$'s which are odd is also odd. Moreover from the choice of $a_1$ and $a_2$ we know that if $a_0$ is even then either three, five or seven of the $a_i$'s (with $i > 0$) are odd, and if $a_0$ is odd, then either 0, 2 or 4 of the $a_i$'s (with $i > 0$) are odd. From this, we deduce that there is a suitable permutation of $(a_1, \ldots, a_7)$, such that
(i) if $a_0$ is even, $|\{i; 1 \leq 3, a_i \text{ is odd}\}|$ is odd and $a_4$ is odd (this is possible because in this case the number of $a_i$'s with $i > 0$ which are odd is greater than 2)
(ii) if $a_0$ is odd, $|\{i; 1 \leq 3, a_i \text{ is odd}\}|$ is even and $a_4$ is even (this is possible because in this case the number of $a_i$'s with $i > 0$ which are even is greater than 2).
Therefore there exists a suitable permutation of $(a_1, \ldots, a_7)$ such that

$$(a_4, a_5, a_6, a_7) \equiv (1 - a_0, a_1, a_2, a_3) \pmod 2 \text{ and } a_0 + a_1 + a_2 + a_3 \equiv 1 \pmod 2$$

This implies by using Lemma 1 that $a_0 + q(a_1\mathsf{i} + \ldots + a_7\mathsf{kt})$ lies in $1 + 2\mathcal{C}_{\mathbb{O}}$ and therefore also in $\Lambda(q)$. □

Using both lemmas together we obtain

**Proposition 7** *The length of the smallest closed non backtracking walk of even length in $\mathscr{X}_{p,q}$ or in $\mathscr{Y}_{p,q}$ is equal to* $2\lceil 2\log_p q - \log_p 2\rceil$

Proof: Such a walk of length $2t$ exists if and only if there exists an irreducible product of length $2t$ which belongs to $\Lambda(q)$ by Lemma 6. Using now Lemma 7, we know that such a product exists if and only if $2p^t > q^2$. The smallest $t$ which satisfies this inequality is clearly equal to $\lceil 2\log_p q - \log_p 2\rceil$. □

We can now prove Theorem 3.

Proof: (of Theorem 3) The first part of (i) is a consequence of the fact that $\mathscr{X}_{p,q}$ is bipartite, therefore any cycle it contains is of even length. We can apply now Proposition 7 and lower bound the length of such a cycle by $2\lceil 2\log_p q - \log_p 2\rceil$. Hence

$$\mathrm{girth}(\mathscr{X}_{p,q}) = 2\lceil 2\log_p q - \log_p 2\rceil = 2\left\lceil \frac{6}{7}\log_{p^3} q^7 - \log_p 2\right\rceil \geq \frac{12}{7}\log_{k-1}(q^7 - q^3) - 2\log_p 2,$$

and the first part of (i) follows. The optimality of the constant $\frac{12}{7}$ follows at once from the fact that

$$\mathrm{girth}(\mathscr{X}_{p,q}) = 2\lceil 2\log_p q - \log_p 2\rceil = (1+o(1))\frac{12}{7}\log_{p^3}(q^7 - q^3) = (1+o(1))\frac{12}{7}\log_{k-1}|\mathscr{X}_{p,q}|$$

as $q$ tends to infinity.

To prove (ii), notice that the double cover graph of $\mathscr{Y}_{p,q}$ is equal to $\mathscr{X}_{p,q}$ by definition and that the length of the smallest cycle of the double cover is at most twice the length of a cycle in $\mathscr{Y}_{p,q}$, therefore

$$\mathrm{girth}(\mathscr{X}_{p,q}) \leq 2\,\mathrm{girth}(\mathscr{Y}_{p,q}).$$

and (ii) follows immediately. □

## 6 Spectral estimate

Basically their approach can be summarized as this.

(i) A classical graph spectral argument is first used to relate the number of cycles of a certain length without backtracking to the spectrum of the graph.

(ii) In the particular case of the Ramanujan family based on quaternions of [32], the number of cycles without backtracking can be related to the number of integer solutions of a certain quadratic equation in 4 variables. In our case, a similar result holds with a quadratic diophantine equation in 8 variables.

(iii) The number of solutions of the quadratic equation is estimated through modular forms considerations. Basically, it can be expressed as a sum of a Fourier coefficient of an Eisenstein series and one of a cusp form, both of weight 2. The Fourier coefficient of the Eisenstein series can be computed explicitly, whereas the Fourier coefficient of the cusp form is upper-bounded by deep results proving the Ramanujan-Petersson conjectures for modular forms of weight 2 (using here Eichler and Igusa results [17, 26] relating such a conjecture to the Riemann hypothesis for algebraic curves on finite fields which was proved by Weil [50]). In our case, we relate the number of integer to the estimation of Fourier coefficients of weight 4, where we rely instead on the more general Deligne's proof [14, 15] of the Ramanujan-Petersson conjectures for modular forms of even weight, which was obtained by proving Riemann's hypothesis for varieties over finite fields.

With the same approach we obtain the following theorem.

**Theorem 4** *The graphs $\mathscr{X}_{p,q}$ are Ramanujan.*

**Remarks:**

1. We consider here in a unified way the case where $\mathscr{X}_{p,q}$ is a Cayley graph over the Moufang loop $\mathbb{O}(\mathbb{F}_q)/\mathcal{Z}$ (which corresponds to the case $\left(\frac{p}{q}\right) = -1$) and where $\mathscr{X}_{p,q}$ is the double cover of $\mathscr{Y}_{p,q}$ (i.e. $\left(\frac{p}{q}\right) = 1$).
2. This will allow for instance to obtain as a direct corollary (see Corollary 3) that the $\mathscr{Y}_{p,q}$'s are also Ramanujan.

**Step 1: relating the graph spectrum to the numbers of non-backtracking cycles.** We recall that if $A$ is the adjacency matrix of a graph, then $A^\ell$ is the matrix whose $i, j$-entry is the number of paths of length $\ell$ between the vertices labeled $i$ and $j$. Assume that the graph is regular of valency $k$. The sequence of matrices $(B_\ell)_{\ell\in\mathbb{N}}$ defined by the order 2 recurrence relation (Cf. [13, 1.4.1 Lemma]):

$$B_0 = \mathrm{Id},\ B_1 = A,\ B_2 = A^2 - k\mathrm{Id}, \qquad B_\ell = AB_{\ell-1} - (k-1)B_{\ell-2},\ \text{for } \ell \geq 3,$$

counts the number of paths *without backtracking* of length $\ell$ between two vertices. We recall that a path $(x_0, x_1, \ldots, x_\ell)$ is said to be without backtracking if and only if $x_{i-1} \neq x_{i+1}$ for any $i \in \{1, \ldots, \ell-1\}$. The Chebychev polynomials (of the second kind) $U_m(X)$, defined by $U_m(\cos\theta) = \frac{\sin(m+1)\theta}{\sin\theta}$, verify an order 2 recurrence relation as well:

$$U_m(X) = 2XU_{m-1}(X) - U_{m-2}(X).$$

Hence, it is possible to link the $B_\ell$ and the $U_m$ in the following way. Defining matrices $(T_m)_{m\in\mathbb{N}}$,

$$T_m \stackrel{\text{def}}{=} \sum_{0\leq\ell\leq\frac{m}{2}} B_{m-2\ell}, \tag{19}$$

comes (Cf. [13, 1.4.5 Proposition]):

$$T_m = (k-1)^{m/2} U_m\left(\frac{A}{2\sqrt{k-1}}\right). \tag{20}$$

Suppose that the graph whose adjacency matrix is $A$ has vertex set $V$, that $|V| = n$. Let $\lambda_0 = k \geq \lambda_1 \geq \cdots \geq \lambda_{n-1}$ the eigenvalues of this graph. Given a vertex $x \in V$, let $f_{\ell,x}$ be the number of closed paths of length $\ell$ without backtracking starting at $x$. By definition of the matrices $(B_\ell)_{\ell\in\mathbb{N}}$, $f_{\ell,x}$ is the entry of the diagonal element of $B_\ell$ labeled by the vertex $x$. By taking the trace of the matrix $T_m$ using Equation (20) and Equation (19) comes (Cf. [13, 1.4.6 Theorem]):

$$\sum_{x\in V}\sum_{0\leq\ell\leq\frac{m}{2}} f_{m-2\ell,x} = (k-1)^{m/2}\sum_{j=0}^{n-1} U_m\left(\frac{\lambda_j}{2\sqrt{k-1}}\right). \tag{21}$$

We go back now to the graphs $\mathscr{X}_{p,q}$, so that the size is $n = q^7 - q^3$ and the valency is $k = p^3 + 1$.

We differ now slightly from the proof given in [13]. It is not clear that these graphs are vertex transitive as was the case for the Ramanujan graphs of [32, 35] (these graphs were constructed as Cayley graphs on *groups*, and were therefore vertex-transitive). In our case, we obtain that $f_{\ell,x}$ is independent of the vertex $x$ in a different way by a reformulation of Lemma 6:

**Lemma 8** *For the graphs $\mathscr{X}_{p,q}$, the number $f_{\ell,x}$ is independent of the vertex $x$. When $\ell$ is even, this number is equal to the number of irreducible products $(\dots(\alpha_1\alpha_2)\cdots)\alpha_s$ of length $\ell$ such that $(\dots(\alpha_1\alpha_2)\cdots)\alpha_s \in \Lambda(q)$.*

Proof: If $\ell$ is odd, then $f_{\ell,x}$ is equal to zero for every $x$ because $\mathscr{X}_{p,q}$ is bipartite. If $\ell$ is even, the statement given is a straightforward consequence of Lemma 6 and the very definition of $\mathscr{X}_{p,q}$ in terms of a Cayley graph over $\mathbb{O}(\mathbb{F}_q)^\star/\mathscr{Z}$ (when $\left(\frac{p}{q}\right) = -1$) or in terms of a double cover of a Cayley graph over $M_1/\mathscr{Z}_1$ (when $\left(\frac{p}{q}\right) = 1$). □

With this lemma, we denote $f_{\ell,x}$ simply by $f_\ell$. The degree of the graphs $\mathscr{X}_{p,q}$ is $k = p^3 + 1$, therefore Equation (21) becomes (Cf. [13, 1.4.7 Corollary]):

$$n \sum_{0 \le \ell \le \frac{m}{2}} f_{m-2\ell} = p^{3m/2} \sum_{j=0}^{n-1} U_m\left(\frac{\lambda_j}{2p^{3/2}}\right). \tag{22}$$

**Step 2: Expressing the number $f_\ell$ of non-backtracking cycles of length $\ell$ in terms of the number of solutions of certain quadratic diophantine equations.** To start with, let us introduce briefly some preliminary materials. Given a positive definite quadratic form $R$, anf for $t \in \mathbb{N}$ fixed, let

$$N_R(t) \overset{\text{def}}{=} \left\{\mathbf{x} = (x_0, \dots, x_7) \in \mathbb{Z}^8 \mid R(\mathbf{x}) = t\right\}, \quad \text{and} \quad n_R(t) = |N_R(t)|. \tag{23}$$

We consider now the positive definite quadratic form

$$Q(x) = x_0^2 + q^2(x_1^2 + \cdots + x_7^2).$$

For $\mathbf{a} \in \{0,1\}^8$, let us define also the sets

$$E_{\mathbf{a}} \overset{\text{def}}{=} \left\{\mathbf{x} \in \mathbb{Z}^8 \mid Q(\mathbf{x}) = t\ , \quad \mathbf{x} \equiv \mathbf{a} \pmod 2\right\}$$

and for $i \in \{0, 1, \dots, 7\}$:

$$F_i \overset{\text{def}}{=} \left\{\mathbf{x} = (x_0, \dots, x_7) \in \mathbb{Z}^8 \mid Q(\mathbf{x}) = t\ , \quad x_i \equiv 0 \pmod 2\right\}.$$

In the light of the property of Lemma 1 verified by elements in $\Lambda$, the relevant quantity to consider is not the whole number of integer solutions $n_Q(t)$ of $Q = t$, but the following:

**Definition 7** *Let $r_Q(t)$ denotes the number of solutions of $Q(\mathbf{x}) = t$ with $\mathbf{x} = (x_0, \dots, x_7) \in \mathbb{Z}^8$ and satisfying*

$$\begin{aligned}
(x_0, x_1, x_2, x_3) &\equiv (1 - x_4, x_5, x_6, x_7) \pmod 2 \ \textit{ if } x_0 + x_1 + x_2 + x_3 \equiv 1 \pmod 2,\\
(x_0, x_1, x_2, x_3) &\equiv (x_4, 1 - x_5, 1 - x_6, 1 - x_7) \pmod 2 \ \textit{ if } x_0 + x_1 + x_2 + x_3 \equiv 0 \pmod 2.
\end{aligned}$$

Indeed, this quantity verifies:

**Lemma 9** *Let $m$ be a non-negative* even *integer. The following equality holds:*

$$r_Q(p^m) = 2 \sum_{0 \le \ell \le \frac{m}{2}} f_{m-2\ell}.$$

Proof: We already know from Lemma 6 that $f_{m-2\ell}$ counts the number of irreducible products in $\Lambda(q)$ of length $m-2\ell$. Let $\alpha = a_0 + a_1\mathsf{i} + \cdots + a_7\mathsf{kt}$ be such an irreducible product. It belongs to $\Lambda(q) \subset 1 + 2\mathcal{C}_{\mathbb{O}}$ therefore, from Lemma 1

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

And moreover, $a_i = qa'_i$ for some integers $a'_i$ and for $1 \le i \le 7$. Hence, $N(\alpha) = p^{m-2\ell} = Q(a_0, a'_1, \ldots, a'_7)$. This $\alpha$ gives two solutions contributing to $r_Q(p^m)$, namely $\pm(a_0p^\ell, a'_1p^\ell, \ldots, a'_7p^\ell)$.

Conversely, a solution $(x_0, \ldots, x_7)$ contributing to $r_Q(p^m)$ above yields an element $\beta = x_0 + q(x_1\mathsf{i} + \cdots + x_7\mathsf{kt}) \in 1 + 2\mathcal{C}_{\mathbb{O}}$ of norm $N(\beta) = p^m$. That is, $\beta$ verifies the conditions of Proposition 1 and there exists a unique irreducible product $\beta' \in \Lambda$ such that $\beta = \pm p^\ell \beta'$. It is easily verified that $\beta'$ is also in $\Lambda(q)$. Since, $N(\beta') = p^{2m-\ell}$, this is a contribution to $f_{m-2\ell}$. □

The next step is to relate $r_Q(t)$ to the whole number of integer solutions $n_{Q_S}(t)$ of certain quadratic equations $Q_S$ defined hereunder. Indeed, these $n_{Q_S}(t)$ can be estimated sharply (see the next step), whereas it is not the case for the partial number of solutions $r_Q(t)$.

**Definition 8** *Given a subset $S \subset \{0, 1, \ldots, 7\}$, we define the following quadratic form*

$$Q_S(x_0, \ldots, x_7) \overset{def}{=} \phi_S(0)x_0^2 + q^2 \sum_{1 \le i \le 7} \phi_S(i)x_i^2,$$

*where $\phi_S(i) = 4$ if $i \in S$ and $1$ otherwise.*

It is not difficult to see that $n_{Q_S}(t)$ has the following interpretation in terms of the number of integer solutions of $Q(\mathbf{x}) = t$:

$$n_{Q_S}(t) = \left|\{\mathbf{x} = (x_0, \ldots, x_7) \in \mathbb{Z}^8 \mid Q(\mathbf{x}) = t\ , \quad x_i \equiv 0 \pmod 2 \text{ if } i \in S\}\right|. \tag{24}$$

With the help of the definition above, now we can prove that:

**Lemma 10** *There exist integers $a_S$ for $S$ ranging over all subsets of $\{0, \ldots, 7\}$ such that*

$$r_Q(t) = \sum_S a_S n_{Q_S}(t).$$

Proof: Let $A$ be the set of $\mathbf{a} = (a_i)_{0 \le i \le 7} \in \{0,1\}^8$ satisfying

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

By definition of $E_{\mathbf{a}}$, we clearly have:

$$r_Q(t) = \sum_{\mathbf{a} \in A} |E_{\mathbf{a}}|. \tag{25}$$

Next, we show that for any $\mathbf{a} \in \{0,1\}^8$ there is a family of integers $(u_S)_{S \subset \{0,\ldots,7\}}$ such that

$$|E_{\mathbf{a}}| = \sum_{S \subset \{0,\ldots,7\}} u_S n_{Q_S}(t). \tag{26}$$

The above plugged in Equation (25) will prove the lemma. To do so, notice that:

$$E_{\mathbf{a}} = \bigcap_{i:a_i=0} F_i \cap \bigcap_{i:a_i=1} (N_Q - F_i), \tag{27}$$

where $N_Q$ denotes the set $N_Q(t)$ of (23). For $b = 0$ or 1, let us define $S_b \overset{\text{def}}{=} \{i : a_i = b\}$. Let also $G$ be the set $\cap_{i:a_i=0} F_i = \cap_{i \in S_0} F_i$. Equation (27) can be rewritten as:

$$E_{\mathbf{a}} \;=\; \bigcap_{i \in S_0} F_i \cap \bigcap_{i \in S_1} (N_Q - F_i) \;=\; G \cap \Big(N_Q - \bigcup_{i \in S_1} F_i\Big) \;=\; G - \Big(G \cap \bigcup_{i \in S_1} F_i\Big).$$

The last equality is justified by the inclusion $G \subset N_Q$. We now take cardinal:

$$\begin{aligned}
|E_{\mathbf{a}}| \;&=\; |G| - \left|G \cap \bigcup_{i \in S_1} F_i\right| \;=\; |G| - \left|\bigcup_{i \in S_1} G \cap F_i\right| \\
&=\; |G| - \sum_{T \subseteq S_1} (-1)^{|T|-1} \left|G \cap \bigcap_{i \in T} F_i\right| \quad \text{(by the inclusion/exclusion principle)} \\
&=\; \left|\bigcap_{i \in S_0} F_i\right| - \sum_{T \subseteq S_1} (-1)^{|T|-1} \left|\bigcap_{i \in T \cup S_0} F_i\right| \\
&=\; n_{Q_{S_0}}(t) - \sum_{T \subseteq S_1} (-1)^{|T|-1} n_{Q_{T \cup S_0}}(t) \quad \text{(by using (24))}
\end{aligned}$$

This proves Equality (26), which is sufficient to conclude the proof as already mentionned. □

We assume from now on that $m$ is *even*, say $m = 2\ell$. Equality (22) is then rewritten as:

$$r_Q(p^{2\ell}) = \frac{2p^{3\ell}}{n} \sum_{j=0}^{n-1} U_m\left(\frac{\lambda_j}{2p^{3/2}}\right). \tag{28}$$

For every $0 \le j \le n-1$, there exists a unique $\theta_j \in [\frac{3i}{2}\ln p, 0] \cup [0, \pi] \cup [\pi, \pi + \frac{3i}{2}\ln p] \subset \mathbb{C}$ such that: $\lambda_j = 2p^{3/2}\cos\theta_j$ (precisely, $\theta_j \in [0, \pi]$ if $|\lambda_j| \le 2p^{3/2}$, $\theta_j \in [\frac{3i}{2}\ln p, 0)$ for $2p^{3/2} < \lambda_j \le p^3 + 1$ and $\theta_j \in (\pi, \pi + \frac{3i}{2}\ln p]$ for $-p^3 - 1 \le \lambda_j < -2p^{3/2}$). Recall that $\lambda_0 = p^3 + 1$ and since the graphs are bipartite $\lambda_{n-1} = -p^3 - 1$, so $\theta_0 = \frac{3i}{2}\ln p$ and $\theta_{n-1} = \pi + \frac{3i}{2}\ln p$. As a consequence, the graphs are Ramanujan if and only if the $\theta_j$'s are real for $1 \le j \le n-1$, which will be proved in the 3rd step below.

By coming back to the definition of Chebychev polynomials, Equality (28) becomes:

$$r_Q(p^{2\ell}) = \frac{2p^{3\ell}}{n} \sum_{j=0}^{n-1} \frac{\sin(2\ell+1)\theta_j}{\sin\theta_j}. \tag{29}$$

With the aforementioned values for $\theta_0$ and $\theta_{n-1}$, namely $\theta_0 = \frac{3i}{2}\ln p$ and $\theta_{n-1} = \pi + \frac{3i}{2}\ln p$, we check that:

$$r_Q(p^{2\ell}) = \frac{4}{n} \frac{1 - p^{3(2\ell+1)}}{1 - p^3} + \frac{2p^{3\ell}}{n} \sum_{j=1}^{n-2} \frac{\sin(2\ell+1)\theta_j}{\sin\theta_j}. \tag{30}$$

**Step 3: Using modular forms techniques to estimate $r_Q(p^m)$.** Similarly to [32], let us bring in the Theta series:

$$\Theta_S(z) \overset{\text{def}}{=} \sum_{k=0}^{\infty} n_{Q_S}(k) e^{2i\pi kz}. \tag{31}$$

By using classical results about Theta series (see for instance [36, §4.9.5] or [40, Chapter VI-3]), we obtain

**Lemma 11** *$\Theta_S(z)$ is a modular form*[5] *of weight* 4 *for* $\Gamma(16q^2)$.

$\Gamma(16q^2)$ denotes here the group of matrices

$$\Gamma(16q^2) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{16q^2} \right\}.$$

The modular forms $\Theta_S$ can be decomposed in a unique way as a sum of a linear combination of Eisenstein series $E_S(z) = \sum_{k=0}^{\infty} e_{k,S} e^{2i\pi kz}$ and a cusp form $C_S(z) = \sum_{k=1}^{\infty} c_{k,S} e^{2i\pi kz}$ of weight 4 for $\Gamma(16q^2)$ (see [22, article 24, Satz 1. II] for instance), i.e $\Theta_S(z) = E_S(z) + C_S(z)$. We can therefore write by using Lemma 10

$$\sum_{S \subseteq \{0,\dots,7\}} a_S \left( e_{p^{2\ell},S} + c_{p^{2\ell},S} \right) = \frac{4}{n} \frac{1 - p^{3(2\ell+1)}}{1 - p^3} + \frac{2p^{3\ell}}{n} \sum_{j=1}^{n-2} \frac{\sin(2\ell+1)\theta_j}{\sin \theta_j}. \tag{32}$$

The central argument for estimating accurately $r_Q(p^{2\ell})$ is that the Fourier coefficients of a cusp form $C(z) = \sum_{k=1}^{\infty} c_k e^{2i\pi kz}$ of weight 4 satisfy for every $\epsilon > 0$:

$$|c_k| = O_\epsilon(k^{3/2+\epsilon}) \text{ as } k \to \infty. \tag{33}$$

This comes from the proof of the Ramanujan conjecture for cusp forms of even weight obtained by using the work of Ihara [27], which reduced the proof of the conjecture to the Riemann hypothesis for varieties over finite field which was later settled by Deligne in [14, 15].

Since the remaining sum $\frac{2p^{3\ell}}{n} \sum_{j=1}^{n-2} \frac{\sin(2\ell+1)\theta_j}{\sin\theta_j}$ is clearly of the form $o(p^{6\ell})$ as $m$ tends to infinity, it follows from the upper-bound (33) and from Equation (32) that

$$\sum_{S \subseteq \{0,\dots,7\}} a_S e_{p^{2\ell},S} = \frac{4}{n} \frac{1 - p^{3(2\ell+1)}}{1 - p^3} + o\big(p^{6\ell}\big). \tag{34}$$

Following [32], we observe now that the sum of the Fourier coefficients $\sum_{S \subseteq \{0,\dots,7\}} a_S e_{p^{2\ell},S}$ are exactly equal to the right-hand side without remainder term, by using the fact that the coefficients $e_k$ of any linear combination $E(z) = \sum_{k=0}^{\infty} e_k e^{2i\pi kz}$ of Eisenstein series of weight 4 for $\Gamma(N)$ are of the form

$$e_k = \sum_{d|k} d^3 F(d) \tag{35}$$

for some periodic function $F : \mathbb{N} \to \mathbb{C}$ of period $N$ (see for instance [40, Proposition 17, Chapter IV]). We invoke now a the slight variation of [32, Lemma 4.4]:

**Lemma 12** *Let $G : \mathbb{N} \to \mathbb{C}$ be periodic and satisfy*

$$\sum_{d|p^m} d^3 G(d) = o(p^{3m}) \text{ as } m \to \infty$$

*then*

$$\sum_{d|p^m} d^3 G(d) = 0 \text{ for all } m.$$

[5] Actually, $\Theta_S(z)$ even belongs to $\Gamma_0(16q^2)$ as is readily checked from [36]. However, this allows us to make directly use of certain results related to $\Gamma_{16q^2}$ as will appear later on.

Proof: Let $u_m \overset{\text{def}}{=} \sum_{d|p^m} d^3 G(d)$, then

$$G(p^m) = \frac{u_m - u_{m-1}}{p^{3m}} = \frac{u_m}{p^{3m}} - \frac{u_{m-1}}{p^{3(m-1)}p^3}. \tag{36}$$

We notice now that the right-hand-side term $\frac{u_m}{p^{3m}} - \frac{u_{m-1}}{p^{3(m-1)}p^3}$ tends to 0 as $m$ goes to infinity. $G$ is periodic, therefore $G(p^m) = 0$ for all $m$. □

By noticing that

$$\frac{4}{n}\frac{1-p^{3(2\ell+1)}}{1-p^3} = \sum_{d|p^{2\ell}} \frac{4}{n} d^3,$$

writing that

$$\sum_{S\subseteq\{0,\dots,7\}} a_S e_{p^{2\ell},S} = \sum_{d|p^{2\ell}} d^3 F(d)$$

for some periodic function $F : \mathbb{N} \to \mathbb{C}$ of period $16q^2$, and using Equation (35), we obtain that

$$\sum_{S\subseteq\{0,\dots,7\}} a_S e_{p^{2\ell},S} - \frac{4}{n}\frac{1-p^{3(2\ell+1)}}{1-p^3} = \sum_{d|p^m} d^3\left(F(d) - \frac{4}{n}\right).$$

From Equation (34) we see that we can apply Lemma 12 to $\sum_{S\subseteq\{0,\dots,7\}} a_S e_{p^{2\ell},S} - \frac{4}{n}\frac{1-p^{3(2\ell+1)}}{1-p^3}$ and obtain

$$\sum_{S\subseteq\{0,\dots,7\}} a_S e_{p^{2\ell},S} = \frac{4}{n}\frac{1-p^{3(2\ell+1)}}{1-p^3}. \tag{37}$$

This reduces Equation (32) to

$$\sum_{S\subseteq\{0,\dots,7\}} a_S c_{p^{2\ell},S} = \frac{2p^{3\ell}}{n}\sum_{j=1}^{n-2}\frac{\sin(2\ell+1)\theta_j}{\sin\theta_j}.$$

and by using the upperbound (33) we finally obtain

$$\frac{2}{n}\sum_{j=1}^{n-2}\frac{\sin(2\ell+1)\theta_j}{\sin\theta_j} = O_\epsilon(p^{2\ell\varepsilon}).$$

Suppose that there is some $\lambda_j \notin [-2p^{3/2}, 2p^{3/2}]$ with $j \in \{1,\dots,n-2\}$, or equivalently that there is some $\theta_j$ which is not real. There exists a unique $0 < t_j < 1$ such that either $\theta_j = \frac{3i}{2}t_j \ln p$ or $\theta_j = \pi + \frac{3i}{2}t_j \ln p$. Consider the index $j$ of this kind which maximizes $|\lambda_j|$. It is straightforward to check that

$$\frac{2}{n}\sum_{j=1}^{n-2}\frac{\sin(2\ell+1)\theta_j}{\sin\theta_j} = \frac{2|\{i : |\lambda_i| = |\lambda_j|\}|}{n} p^{3\ell t_j}\frac{1-p^{-3t_j(2\ell+1)}}{1-p^{-3t_j}}(1+o(1))$$

as $\ell$ goes to infinity. If $\varepsilon$ is small enough, the right-hand term can not be upper-bounded by $O(p^{2\ell\varepsilon})$ and therefore the same thing holds for $\frac{2}{n}\sum_{j=1}^{n-2}\frac{\sin(2\ell+1)\theta_j}{\sin\theta_j}$. So for $1 \le j \le n-2$, the $\theta_j$'s are real, or equivalently the $\lambda_j$'s are in $[-2p^{3/2}, 2p^{3/2}]$. This proves that the graphs $\mathscr{X}_{p,q}$ are Ramanujan.

**Corollary 3** *For $p < q$ such that $\left(\frac{p}{q}\right) = 1$, the graphs $\mathscr{Y}_{p,q}$ are also Ramanujan.*

PROOF: Let $\mu_0 \geq \cdots \geq \mu_{n-1}$ be the spectrum of $\mathscr{Y}_{p,q}$. The equality $\mu_0 = p^3 + 1$ holds. The graphs are not bipartite by Proposition 6 so there is the inequality $\mu_{n-1} > -p^3 - 1$. The spectrum of the bipartite double cover $\mathscr{X}_{p,q}$ of $\mathscr{Y}_{p,q}$ is given by $\pm\mu_0, \ldots, \pm\mu_{n-1}$, counted with multiplicities. But the graphs $\mathscr{X}_{p,q}$ are Ramanujan, that implies $\mu_j \leq 2p^{3/2}$ for $j \neq 0$. That is $\mathscr{Y}_{p,q}$ are also Ramanujan. □

## Conclusions

The contributions of this work are twofold. First, the girth problem consisting of finding for an infinite growing family of $k$-regular graphs $\{G_n\}$ what is the largest constant

$$\gamma(\{G_n\}) \stackrel{\text{def}}{=} \lim_{n\to\infty} \inf \left\{ \frac{\text{girth}(G_n)}{\log_{k-1} |G_n|} \right\}$$

reduces now to $\frac{12}{7} \leq \gamma \leq 2$, for the values of $k = p^3 + 1$, $p$ an odd prime. This is a clear improvement on the 25 years old result $\frac{4}{3} \leq \gamma \leq 2$.

Second, this is the first construction of Cayley expanders non explicitely based on a group. However, as already mentionned in introduction, we stress that the graphs presented here may be Cayley graphs on groups. The question is then which groups ? A simpler open problem is the vertex-transitivity of these graphs. In any case, it might be interesting to pursue further research toward expansion properties in non-associative algebraic structures. Indeed, the expansion property of Cayley graphs on groups has been thoroughly studied recently. Similar questions arise for loops.

In addition, it may be interesting to carry over the construction of Morgenstern [37] based on quaternions over function fields, to octonions. There would be indeed a hope to build Ramanujan graphs of girth $\frac{12}{7} \log_{k-1} n$ for various degrees $k$, not only of the form $k = p^3 + 1$, $p$ is prime, like in the present paper.

To conclude, let us recall that the graphs constructed here display other properties shared by all Ramanujan graphs, namely a small diameter $D$ satisfying $D \leq 2 \log_{d-1} n + O(1)$ and in the non bipartite case, an independence number $i$ verifying $i \leq \frac{2\sqrt{d-1}}{d} n$ and therefore a chromatic number $\chi$ of the form $\chi \geq \frac{d}{2\sqrt{d-1}}$.

**Acknowledgment** We would like to thank Eiichi Bannai for having pointing out the result of Paige [41] to us.

## References

[1] N. Alon. Eigenvalues and expanders. *Combinatorica*, 6(2):83–96, 1986. Theory of computing (Singer Island, Fla., 1984).

[2] N. L. Biggs. *Algebraic graph theory*. Cambridge University Press, London, 1974. Cambridge Tracts in Mathematics, No. 67.

[3] N. L. Biggs. Graphs with large girth. *Ars Combin.*, 25(C):73–80, 1988. Eleventh British Combinatorial Conference (London, 1987).

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

[5] N. L. Biggs and M. J. Hoare. The sextet construction for cubic graphs. *Combinatorica*, 3:153–165, 1983.

[6] M. Blum, R. M. Karp, O. Vornberger, C. H. Papadimitriou, and M. Yannakakis. The complexity of testing whether a graph is a superconcentrator. *Inform. Process. Lett.*, 13(4-5):164–167, 1981.

[7] B. Bollobás. *Extremal graph theory*, volume 11 of *London Mathematical Society Monographs*. Academic Press Inc. [Harcourt Brace Jovanovich Publishers], London, 1978.

[8] B. Bollobás. The isoperimetric number of random regular graphs. *European J. Combin.*, 9(3):241–244, 1988.

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

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

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

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

[13] 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.

[14] P. Deligne. Formes modulaires et représentations $\ell$-adiques. *Séminaire N. Bourbaki*, exp. n$^o$ 355:139–172, 1969.

[15] P. Deligne. La conjecture de Weil. I. *Inst. Hautes Études Sci. Publ. Math.*, 43:273–307, 1974.

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

[17] M. Eichler. Quaternäre quadratische Formen und die Riemannsche Vermutung für die Kongruenzzetafunktion. *Arch. Math.*, 5:355–366, 1954.

[18] P. Erd ős and H. Sachs. Reguläre Graphen gegebener Tailenweite mit minimaler Knollenzahh. *Wiss. Z. Univ. Halle-Willenberg Math. Nat.*, 12:251–258, 1963.

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

[20] A. Gamburd, S. Hoory, M. Shahshahani, A. Shalev, and B. Vir. On the girth of random Cayley graphs. *Random Structures and Algorithms*, 35(1):100 – 117, 2009.

[21] S. Hakimi and J. Bredeson. Graph theoretic error-correcting codes. *IEEE Trans. on Inform. Theory,*, 14(4):584 – 591, jul. 1968.

[22] E. Hecke. *Mathematische Werke.* Herausgegeben im Auftrage der Akademie der Wissenschaften zu Göttingen. Vandenhoeck & Ruprecht, Göttingen, 1959.

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

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

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

[26] J. Igusa. Fibre systems of Jacobian varieties. III. Fibre systems of elliptic curves. *Amer. J. Math.*, 81:453–476, 1959.

[27] Y. Ihara. Hecke Polynomials as congruence $\zeta$ functions in elliptic modular case. *Ann. of Math. (2)*, 85:267–295, 1967.

[28] B. W. Jordan and R. Livné. Ramanujan local systems on graphs. *Topology*, 36(5):1007–1024, 1997.

[29] N. Kahale. Eigenvalues and expansion of regular graphs. *J. Assoc. Comput. Mach.*, 42(5):1091–1106, 1995.

[30] F. Lazebnik and V. A. Ustimenko. Explicit construction of graphs with an arbitrary large girth and of large size. *Discrete Appl. Math.*, 60(1-3):275–284, 1995. ARIDAM VI and VII (New Brunswick, NJ, 1991/1992).

[31] Wen-Ching Winnie Li, Min Lu, and Chenying Wang. Recent developments in low-density parity-check codes. In *IWCC*, pages 107–123, 2009.

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

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

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

[35] 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.

[36] T. Miyake. *Modular forms.* Springer, 1989.

[37] 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.

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

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

[40] A. Ogg. *Modular forms and Dirichlet series.* W. A. Benjamin, Inc., New York-Amsterdam, 1969.

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

[42] M. S. Pinsker. On the complexity of a concentrator. In *Proc. 7th International Teletraffic Conference*, pages 318/1–318/4, Stockholm, June 1973.

[43] A. Pizer. Ramanujan graphs and Hecke operators. *Bull. Amer. Math. Soc.*, 23(1):127–137, 1990.

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

[45] P. Rosenthal and P. O. Vontobel. Constructions of LDPC codes using Ramanujan graphs and ideas from Margulis. In *Proc. of the 38-th Allerton Conference on Communication, Control, and Computing*, pages 248–257, 2000.

[46] M. Sipser and D. A. Spielman. Expander codes. *IEEE Trans. on Inform. Theory*, 42(6):1710–1722, 1996.

[47] D. A. Spielman. Linear-time encodable and decodable error-correcting codes. *IEEE Trans. on Inform. Theory*, 42(6):1723–1731, 1996.

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

[49] J.-P. Tillich and G. Zémor. Optimal cycle codes constructed from Ramanujan graphs. *SIAM J. Discrete Math.*, 10(3):447–459, 1997.

[50] A. Weil. *Sur les courbes algébriques et les variétés qui s'en déduisent.* Actualités Sci. Ind., no. 1041 = Publ. Inst. Math. Univ. Strasbourg **7** (1945). Hermann et Cie., Paris, 1948.

[51] A. Weiss. Girths of bipartite sextet graphs. *Combinatorica*, 4(2-3), 1984.

[52] A. Wigderson and D. Zuckerman. Expanders that beat the eigenvalue bound: explicit construction and applications. *Combinatorica*, 19(1):125–138, 1999.