Die Cayley Graphen von $(PSL_2(\mathbb{F}_q))_q$ bzw. $(PGL_2(\mathbb{F}_q))_q$ bilden eine Familie von Expandergraphen

Daniel Keppeler

1 Einleitung

Diese Ausarbeitung behandelt den vierten Abschnitt im Kapitel vier des Buches „Elementary Number Theory, Group Theory, and Ramanujan Graphs“ von Davidoff, Sarnak und Valette und wurde im Rahmen des Seminars „Gruppen, Expandergraphen und Bäume“ verfasst. Hierbei wird auf den Ergebnissen der vorigen Vorträge aufgebaut. Es wird gezeigt, dass die Cayley Graphen von $(PSL_2(\mathbb{F}_q))_q$ bzw. $(PGL_2(\mathbb{F}_q))_q$ eine Familie von Expandergraphen bilden, indem die nicht trivialen Eigenwerte der Adjazenmatrizen der Graphen abgeschätzt werden und damit für festes p eine explizite untere Schranke der spektralen Lücke der $X^{p,q}$ bestimmt wird, wenn q groß im Vergleich zu p ist. Damit wird dann zusätzlich gezeigt, dass die Graphen einen großen Umfang und eine hohe Knotenfärbungszahl besitzen. Dies verbessert somit das Ergebnis aus dem sechsten Abschnitt des ersten Kapitels des Buches, in dem lediglich die Existenz solcher Graphen bewiesen wurde.

2 Die Cayley Graphen von $(PSL_2(\mathbb{F}_q))_q$ bzw. $(PSL_2(\mathbb{F}_q))_q$ bilden eine Familie von Expandergraphen

2.1 Konvention *In diesem Kapitel wird die Anzahl der Wege der Länge l mit Start- und Endpunkt 1 in $X^{p,q}$ mit f_l notiert.*
Die Anzahl der Ecken von $X^{p,q}$ wird mit n notiert und das Spektrum der Adjazenzmatrix A mit

$$\mu_0 = p + 1 > \mu_1 \geq \mu_2 \geq \ldots \geq \mu_{n-1}.$$

2.2 Definition Die *Chebyshevpolynome zweiter Art U_m* sind durch folgende rekursive Vorschrift definiert:

$$U_0(x) = 1,\ U_1(x) = 2x,\ U_{m+1}(x) = 2xU_m(x) - U_{m-1}(x)\ f\ddot{u}r\ m \geq 2$$

Es gilt für alle $m \in \mathbb{N} : U_m(cos\ \theta) = \frac{sin\ (m+1)\theta}{sin\ \theta}$ nach [[1], 1.4.4 Definition]
und die Spurformel $\sum_{0 \leq r \leq \frac{m}{2}} f_{m-2r} = \frac{p^{\frac{m}{2}}}{2} \sum_{j=0}^{n-1} U_m(\frac{\mu_j}{2\sqrt{p}})$ nach [[1], 1.4.7 Korollar].
Das erste Ziel ist es, eine neue Interpretation der linken Seite der Spurformel zu geben. Dazu wird an dieser Stelle die quadratische Form in vier Variabeln

$$Q(x_0, x_1, x_2, x_3) = x_0^2 + q^2(x_1^2 + x_2^2 + x_3^2)$$

eingeführt und man setzt für $m \geq 1$

$$\begin{aligned} S_Q(p^m) = |\{(x_0, x_1, x_2, x_3) \in \mathbb{Z}^4 : Q(x_0, x_1, x_2, x_3) = p^m\ und \\ entweder\ x_0\ gerade\ und\ x_1, x_2, x_3\ ungerade \\ oder\ x_0\ ungerade\ und\ x_1, x_2, x_3\ gerade\}| \end{aligned}$$

2.3 Bemerkung Ist m gerade oder $p \equiv 1\ (mod\ 4)$, so ist für jede Lösung $(x_0, x_1, x_2, x_3) \in \mathbb{Z}^4$, mit $Q(x_0, x_1, x_2, x_3) = p^m$ und den oben gegebenen Kongruenzen modulo 2, x_0 ungerade und x_1, x_2, x_3 gerade. Mit der quadratischen Form

$$Q'(x_0,x_1,x_2,x_3) = x_0^2 + 4q^2(x_1^2+x_2^2+x_3^2)$$

ist dann $S_Q(p^m)$ genau die Anzahl der ganzzahligen Lösungen von $Q'(x_0,x_1,x_2,x_3) = p^m$.

Beweis. Da p ungerade Primzahl ist, existiert $k \in \mathbb{N}$ mit $p = 2k+1$.
Ist m nun gerade, so gilt

$$p^m = (2k+1)^m = \sum_{n=0}^{m} \binom{m}{n}(2k)^n * 1^{m-n} \equiv 1 \ (mod\ 4)$$

Ist $p \equiv 1 \ (mod\ 4)$ so gilt auch $p^m \equiv 1 \ (mod\ 4)$.
Sei $(x_0,x_1,x_2,x_3) \in \mathbb{Z}^4$ mit $Q(x_0,x_1,x_2,x_3) = p^m$, und angenommen, x_0 wäre gerade und x_1,x_2,x_3 ungerade. Dann existieren $k_0,k_1,k_2,k_3 \in \mathbb{Z}$ mit $x_0 = 2k_0,\ x_1 = 2k_1+1,\ x_2 = 2k_2+1,\ x_3 = 2k_3+1$.
Weiter gilt $Q(x_0,x_1,x_2,x_3) = p^m$ und somit

$$\begin{aligned} (2k_0)^2 + q^2((2k_1+1)^2+(2k_2+1)^2+(2k_3+1)^2) &\equiv 1 \ (mod\ 4) \\ \Rightarrow 4k_0^2 + q^2(4k_1^2+4k_1+1+4k_2^2+4k_2+1+4k_3^2+4k_3+1) &\equiv 1 \ (mod\ 4) \\ \Rightarrow q^2 * 3 &\equiv 1 \ (mod\ 4) \end{aligned}$$

q ist aber ungerade, also ist $q^2 \equiv 1 \ (mod\ 4)$ und somit $3 \equiv 1 \ (mod\ 4)$ ↯
Also ist x_0 ungerade und x_1,x_2,x_3 gerade. Sei nun $k_1,k_2,k_3 \in \mathbb{Z}$ mit $x_1 = 2k_1, x_2 = 2k_2, x_3 = 2k_3$, dann gilt:

$$Q(x_0,x_1,x_2,x_3) = x_0^2 + q^2(4k_1^2+4k_2^2+4k_3^2) = x_0^2 + 4q^2(k_1^2+k_2^2+k_3^2) = Q'(x_0,k_1,k_2,k_3)$$

Umgekehrt gilt für eine beliebige Lösung $(x_0,x_1,x_2,x_3) \in \mathbb{Z}^4$ mit $Q'(x_0,x_1,x_2,x_3) = p^m$, dass $Q(x_0,2x_1,2x_2,2x_3) = p^m$ und somit folgt die Behauptung. □

2.4 Lemma *Für $m \in \mathbb{N}$ gilt:* $S_Q(p^m) = 2 \sum_{0 \le r \le \frac{m}{2}} f_{m-2r}$

Beweis. $X^{p,q}$ lässt sich nach [[1], Theorem 4.3.5] mit $Y^{p,q}$ identifizieren.
Seien $x_0 = 1, x_1, ..., x_{l-1}, x_l = 1$ die Ecken eines reduzierten Weges der Länge l mit Anfangs- und Endpunkt 1 in $Y^{p,q}$. Wie im Beweis zu [[1], Proposition 4.3.3] findet man $t_1,...,t_l \in T_{p,q}$, so dass $x_i = t_1 * ... * t_i$ $(1 \le i \le l)$ und $t_i = \Pi_q[\alpha_i]$ für ein eindeutiges $\alpha_i \in S_p$ $(1 \le i \le l)$. Dann ist $[\alpha_1][\alpha_2]...[\alpha_l]$ ein reduziertes Wort der Länge l in Λ, da es der Lift eines reduzierten Weges ist. Wegen $\Pi_q([\alpha_1][\alpha_2]...[\alpha_l]) = x_l = 1$ gilt $[\alpha_1]...[\alpha_l] \in \Lambda(q)$.
Damit ist bewiesen, dass f_l die Anzahl der reduzierten Wörter der Länge l in Λ ist, die zu $\Lambda(q)$ gehören.

Sei $(x_0,x_1,x_2,x_3) \in S_Q(p^m)$. Für die Quaternione $\alpha = x_0 + q(x_1 i + x_2 j + x_3 k) \in \Lambda'$ gilt nach [[1], Lemma 4.3.2], dass ihre Äquivalenzklasse $[\alpha] \in \Lambda$ schon in $\Lambda(q)$ liegt. Es ergibt sich also die Gleichung

$$\begin{aligned} S_Q(p^m) &= |\{\alpha = a_0 + a_1 i + a_2 j + a_3 k \in \Lambda' \mid N(\alpha) = p^m,\ q \ teilt\ a_1,a_2,a_3\}| \\ &= |\{\alpha = a_0 + a_1 i + a_2 j + a_3 k \in \Lambda' \mid N(\alpha) = p^m,\ [\alpha] \in \Lambda(q)\}| \end{aligned}$$

Sei jetzt α aus der rechten Seite der Gleichung beliebig. Nach [[1], Korollar 2.6.14] hat α eine eindeutige Faktorisierung $\alpha = \pm p^l \omega_{m-2l}$, wobei ω_{m-2l} ein reduziertes Wort der Länge $m-2l$ über S_p ist. Die Klasse $[\alpha]$ ist daher ein reduziertes Wort der Länge $m-2l$ in Λ und gehört zu $\Lambda(q)$. Es gilt also

$$|\{\alpha = a_0 + a_1 i + a_2 j + a_3 k \in \Lambda' \mid N(\alpha) = p^m,\ [\alpha] \in \Lambda(q)\}| \leq 2 \sum_{0 \leq r \leq \frac{m}{2}} f_{m-2r}$$

Umgekehrt erzeugt ein reduziertes Wort ω der Länge $m - 2l$ in $\Lambda(q)$ zwei Quaternionen der Form $\alpha = \pm p^l \omega$. Also gilt auch

$$|\{\alpha = a_0 + a_1 i + a_2 j + a_3 k \in \Lambda' \mid N(\alpha) = p^m,\ [\alpha] \in \Lambda(q)\}| \geq 2 \sum_{0 \leq r \leq \frac{m}{2}} f_{m-2r}$$

Insgesamt folgt

$$|\{\alpha = a_0 + a_1 i + a_2 j + a_3 k \in \Lambda' \mid N(\alpha) = p^m,\ [\alpha] \in \Lambda(q)\}| = 2 \sum_{0 \leq r \leq \frac{m}{2}} f_{m-2r}$$

□

Man erhält also folgende Spurformel für $X^{p,q}$

$$S_Q(p^m) = 2\frac{p^{\frac{m}{2}}}{n} \sum_{j=0}^{n-1} U_m\left(\frac{\mu_i}{2\sqrt{p}}\right)$$

2.5 Lemma *Sei* $\Theta_p = [i * log\sqrt{p}, 0] \cup [0, \pi] \cup [\pi, \pi + i * log\sqrt{p}] \subset \mathbb{C}$. *Dann wird* Θ_p *durch* $z \mapsto 2\sqrt{p} * cos(z)$ *bijektiv auf* $[-(p+1), p+1]$ *abgebildet. Insebsondere* $[0, \pi] \to [-2\sqrt{p}, 2\sqrt{p}]$ *bijektiv auf das Ramanujanintervall.*

Beweis. Es gilt $cos(z) = \frac{e^{iz}+e^{-iz}}{2}$ und $sin(z) = \frac{e^{iz}-e^{-iz}}{2}$. Θ_p lässt sich als Intervall mit entsprechender Ordnung, zusammengesetzt aus seinen Teilintervallen auffassen, indem das erste Teilintervall "rückwärts"durchlaufen wird, d.h. ist $x, y \in [0, i * log\sqrt{p}]$ mit $x \leq y$ (im Sinne von $\Im(x) \leq \Im(y)$), so gilt in Θ_p $x \geq y$, also reicht es zu zeigen, dass sie auf Θ_p streng monoton fällt, um die Injektivität zu beweisen.
Die Funktion ist genau dann streng monoton fallend, wenn sie auf $[0, i * log\sqrt{p}]$ streng monoton steigt und auf $[0, \pi]$ und $[\pi, \pi + i * log\sqrt{p}]$ streng monoton fällt.
Da $cos : [0, \pi] \to [1, -1]$ bijektiv und streng monoton fallend ist, ist auch $2\sqrt{p} * cos : [0, \pi] \to [2\sqrt{p}, -2\sqrt{p}]$ bijektiv und streng monoton fallend.
Sei $x \in [0, i * log\sqrt{p}]$, also $x = i * x_0$ für ein $x_0 \in [0, log\sqrt{p}]$ und somit gilt $cos(x) = cosh(x_0)$. Der Cosinus Hyperbolicus ist auf $[0, \infty)$ streng monoton steigend, also auch $2\sqrt{p} * cosh(x_0)$.
Sei jetzt $x \in [\pi, \pi + i * log\sqrt{p}]$, also $x = \pi + i * x_0$ für ein $x_0 \in [0, log\sqrt{p}]$. Damit gilt nach den Additiontstheoremen

$$\begin{aligned} cos(x) &= cos(\pi) * cos(i * x_0) - sin(\pi) * sin(i * x_0) = (-1) * cosh(x_0) - 0 * i * sinh(x_0) \\ &= -cosh(x_0) \end{aligned}$$

und somit ist $2\sqrt{p} * cos$ auch auf $[\pi, \pi + i * log\sqrt{p}]$ streng monoton fallend.
Es gilt

$$2\sqrt{p} * cos(i * log\sqrt{p}) = 2\sqrt{p}\frac{e^{-log\sqrt{p}} + e^{log\sqrt{p}}}{2} = 2\sqrt{p}\frac{\frac{1}{\sqrt{p}} + \sqrt{p}}{2} = p + 1$$

$$2\sqrt{p} * cos(\pi + i * log\sqrt{p}) = 2\sqrt{p}\frac{e^{i\pi - log\sqrt{p}} + e^{-i\pi + log\sqrt{p}}}{2} = 2\sqrt{p}\frac{e^{i\pi}\frac{1}{\sqrt{p}} + e^{-i\pi}\sqrt{p}}{2} = -(p+1)$$

Die Funktion ist stetig, also folgt aus dem Mittelwertsatz die Surjektivität. □

Mit dieser Bijektion lässt sich nun für $j = 0, 1, ..., n-1$ ein eindeutiges $\theta_j \in \Theta_p$ finden mit $\mu_j = 2\sqrt{p} * cos\theta_j$. Insbesondere gilt $\theta_0 = i * log\sqrt{p}$ und falls $(\frac{p}{q}) = -1$: $\theta_{n-1} = \pi + i * log\sqrt{p}$ nach [[1], 4.3.6 Korollar]. Nach der Definition der Chebyshevpolynome U_m gilt damit

$$S_Q(p^m) = 2\frac{p^{\frac{m}{2}}}{n}\sum_{j=0}^{n-1} U_m(\frac{2\sqrt{p}*cos\theta_j}{2\sqrt{p}}) = 2\frac{p^{\frac{m}{2}}}{n}\sum_{j=0}^{n-1} U_m(cos\theta_j) = 2\frac{p^{\frac{m}{2}}}{n}\sum_{j=0}^{n-1}\frac{sin(m+1)\theta_j}{sin\theta_j}$$

Um zu zeigen, dass $X^{p,q}$ Ramanujangraphen sind, muss gezeigt werden, dass $|\mu_j| \leq 2\sqrt{p}$ oder äquivalent nach obiger Bijektion: $\theta_j \in \mathbb{R}$.
Mit elementaren Methoden ist dies nicht so leicht zu zeigen. Im Folgenden wird daher nur ein Beweis dafür gegeben, dass für sehr große q der Imaginärteil von θ_j durch eine Konstante in Abhängigkeit von p beschränkt ist. Damit kann dann gezeigt werden, dass die $X^{p,q}$ eine Familie von Expandergraphen bilden.

2.6 Proposition *Sei μ ein nicht trivialer Eigenwert von $X^{p,q}$, d.h. $|\mu| \neq p+1$, sei $M(\mu)$ die Multiplizität von μ. Dann gilt*

$$M(\mu) \geq \frac{q-1}{2}$$

Beweis. Sei G die $X^{p,q}$ unterliegende Gruppe, also $G = \begin{cases} PSL_2(q), & falls\ (\frac{p}{q}) = 1 \\ PGL_2(q), & falls\ (\frac{p}{q}) = -1 \end{cases}$.
Sei $V_\mu \subset l^2(G)$ der Eigenraum zum Eigenwert μ, dann gilt $M(\mu) = dim_{\mathbb{C}} V_\mu$.
Sei $\lambda_G : G \to GL(l^2(G))$ die linksreguläre Darstellung, definiert durch $(\lambda_G(g)f)(x) = f(g^{-1} * x)$ für $f \in l^2(G)$ und $x, g \in G$. Dann ist $\lambda_{PSL_2(q)} : PSL_2(q) \to GL(l^2(G))$ eine Darstellung von $PSL_2(q)$ auf $l^2(G)$, da $PSL_2(q) \subset G$ in beiden Fällen. Nach [[1], Aufgabe 4.1.4] ist V_μ λ_G-invariant, also ist V_μ mit der Einschränkung von $\lambda_{PSL_2(q)}$ ebenfalls eine Darstellung. Ist diese Darstellung nicht trivial, so folgt $dim_{\mathbb{C}} V_\mu \geq \frac{q-1}{2}$ nach [[1], Theorem 3.5.1] und somit die Behauptung.
Angenommen, die Darstellung wäre trivial, also $\lambda_{PSL_2(q)} : PSL_2(q) \to GL(V_\mu),\ g \mapsto id_{V_\mu}$.
1.Fall: $(\frac{p}{q}) = 1$. Dann ist $G = PSL_2(q)$ und somit gilt für alle $x, g \in G,\ f \in V_\mu : (\lambda_G(g)f)(x) = f(g^{-1}x) = f(x)$. Sei $f(1_G) = c \in \mathbb{C}$, dann gilt insbesondere für alle $g \in G$: $f(g) = f(g^{-1}g) = f(1_G) = c$, also ist f konstant. Sei jetzt $f \neq 0$ eine Eigenfunktion zum Eigenwert μ, insbesondere also $f \equiv c$ für ein $c \in \mathbb{C}$. Dann gilt für alle $g \in G$: $\mu * c = Af(g) = \sum_{h\in G} A_{g,h}f(h) = (p+1) * c$.
Es folgt also $\mu = p + 1$↯
2.Fall: $(\frac{p}{q}) = -1$. Dann ist $G = PGL_2(q)$ und $PGL_2(q)/PSL_2(q) \cong \{\pm 1\}$. Sei $\hat{x} \in G - PSL_2(q)$, also insbesondere $\hat{x}PSL_2(q) \neq 1_G PSL_2(q)$ in $PGL_2(q)/PSL_2(q)$. Da die Darstellung von $PSL_2(q)$ trivial ist, gilt für alle $g \in PSL_2(q)$ und $x \in G$ und $f \in V_\mu$: $(\lambda_G(g)f)(x) = f(g^{-1}x) = f(x)$. Setze $a_+ = f(1_G)$ und $a_- = f(\hat{x})$. Sei $x \in G$ beliebig, dann gilt entweder $x \in PSL_2(q)$, d.h. $f(x) = f(x^{-1}x) = f(1_G) = a_+$, oder $xPSL_2(q) = \hat{x}PSL_2(q)$, d.h. es gibt $g \in PSL_2(q)$ mit $g^{-1}x = \hat{x}$ und damit $f(x) = f(g^1 x) = f(\hat{x}) = a_-$. Insgesamt gilt also:

$$f(x) = \begin{cases} a_+, & falls\ x \in PSL_2(q) \\ a_-, & falls\ x \in PGL_2(q) - PSL_2(q) \end{cases}$$

Nach [[1], Bemerkung 4.2.3] ist $X^{p,q}$ in diesem Fall bipartit, insbesondere gilt für alle $g \in PSL_2(q)$, $h \in PGL_2(q) - PSL_2(q)$: $A_{g,h} = A_{h,g} = 0$.
Sei jetzt $f \in V_\mu$ mit $f \neq 0$, $g \in PSL_2(q)$, $\hat{g} \in PGL_2(q) - PSL_2(q)$, dann gilt:

$$\mu * a_+ = Af(g) = \sum_{h \in G} A_{g,h} f(h) = \sum_{h \in PGL_2(q) - PSL_2(q)} A_{g,h} f(h) = (p+1)a_-$$
$$\mu * a_- = Af(\hat{g}) = \sum_{h \in G} A_{g,h} f(h) = \sum_{h \in PSL_2(q)} A_{g,h} f(h) = (p+1)a_+$$

und da $f \neq 0$ folgt aus den Gleichungen $a_+ \neq 0$ und $a_- \neq 0$. Es folgt also

$$\begin{cases} \mu = \frac{(p+1)*a_+}{a_-} \\ \mu = \frac{(p+1)*a_-}{a_+} \end{cases}$$
$$\Rightarrow \mu^2 = \frac{(p+1)^2 * a_+ * a_-}{a_+ * a_-} = (p+1)^2$$

Und somit $|\mu| = p + 1$↯

2.7 Notation *Sei $f(n)$ ein Term in Abhängigkeit von $n \in \mathbb{N}$. Sei $\varepsilon \in \mathbb{R}$, $\varepsilon > 0$. Sei $g(n)(\varepsilon)$ ein Term in Abhängigkeit von n und ε. Dann schreibt man*

$$f(n) = O_\varepsilon(g(n)(\varepsilon))$$

falls eine Konstante $C(\varepsilon)$ existiert, so dass gilt

$$f(n) \leq C(\varepsilon) * g(n)(\varepsilon) \text{ für alle } n \in \mathbb{N}.$$

Weiter schreibt man für $n, k \in \mathbb{N}$

$$r_k(n) = |\{(x_0, ..., x_{k-1}) \in \mathbb{Z}^k : \sum_{i=0}^{k-1} x_i^2 = n\}|.$$

Mit anderen Worten ist $r_k(n)$ die Anzahl der ganzzahligen Lösungen, durch die sich n als Summe von k Quadraten schreiben lässt.

2.8 Beispiel

$$i)\ n^3 + n^2 + n = O(n^3) = O_\varepsilon(n^{3+\varepsilon}),\ denn\ n^3 + n^2 + n \leq 3n^3 \leq 3n^{3+\varepsilon}\ für\ alle\ n \in \mathbb{N}.$$
$$ii)\ Nach\ [[1],\ 2.2.13\ Korollar]\ gilt\ für\ alle\ \varepsilon > 0:\ r_3(n) = O_\varepsilon(n^{\frac{1}{2}+\varepsilon}).$$

Damit ist genug gezeigt, um eine Abschätzung der Eigenwerte zu geben.

2.9 Theorem *Sei $\varepsilon \in (0, \frac{1}{6}) \subset \mathbb{R}$ fest. Dann gilt für große q und jeden nicht trivialen Eigenwert μ von $X^{p,q}$:*

$$|\mu| \leq p^{\frac{5}{6}+\varepsilon} + p^{\frac{1}{6}-\varepsilon}$$

Beweis. Nach Lemma 2.5 gilt für alle $m \in \mathbb{N}$ die Spurformel

$$S_Q(p^m) = 2\frac{p^{\frac{m}{2}}}{n} \sum_{j=0}^{n-1} \frac{sin(m+1)\theta_j}{sin\theta_j}$$

Ist $\mu_j \notin [-2\sqrt{p}, 2\sqrt{p}]$, so gilt

$$\theta_j = \begin{cases} i * \psi_j & \text{, falls } 2\sqrt{p} < \mu_j \leq p+1 \\ \pi + i * \psi_j & \text{, falls } -(p+1) \leq \mu_j < -2\sqrt{p} \end{cases}$$

mit $0 < \psi_j \leq log\sqrt{p}$ in beiden Fällen, nach Lemma 2.5. Es gilt für alle $z \in \mathbb{R}$:
$i * sin(-i * z) = \frac{e^z - e^{-z}}{2} = sinh(z)$ und $sinh$ streng monoton steigend und $cos(-iz) = \frac{e^z + e^{-z}}{2} = cosh(z)$.
Ist außerdem m gerade, gilt $e^{i(m+1)\pi} = -1$ und somit in beiden Fälle

$$\frac{sin(m+1)\theta_j}{sin\theta_j} = \frac{sin(i*(m+1)\psi_j)}{sin(i*\psi_j)} = \frac{sinh((m+1)\psi_j)}{sinh(\psi_j)} \geq 0$$

Sei also ab jetzt m gerade. Mit der Spurformel folgt also für einen festen nicht trivialen Eigenwert $\mu_k \notin [-2\sqrt{p}, 2\sqrt{p}]$

$$\begin{aligned} S_Q(p^m) &= \frac{2}{n} p^{\frac{m}{2}} \sum_{j=0}^{n-1} \frac{sin(m+1)\theta_j}{sin\theta_j} = \frac{2}{n} p^{\frac{m}{2}} M(\mu_k) \frac{sin(m+1)\theta_k}{sin\theta_k} + \frac{2}{n} p^{\frac{m}{2}} \sum_{j \neq k} \frac{sin(m+1)\theta_j}{sin\theta_j} \\ &= \frac{2}{n} p^{\frac{m}{2}} M(\mu_k) \frac{sinh(m+1)\psi_k}{sinh\psi_k} + \frac{2}{n} p^{\frac{m}{2}} \sum_{j \neq k} \frac{sin(m+1)\theta_j}{sin\theta_j} \\ &\geq \frac{2}{n} p^{\frac{m}{2}} M(\mu_k) \frac{sinh(m+1)\psi_k}{sinh\psi_k} + \frac{2}{n} p^{\frac{m}{2}} \sum_{j:\, |\mu_j| \leq 2\sqrt{p}} \frac{sin(m+1)\theta_j}{sin\theta_j} \end{aligned}$$

Für $|\mu_j| \leq 2\sqrt{p}$ ist $\theta_j \in \mathbb{R}$. Es gilt also $|\frac{sin(m+1)\theta_j}{sin\theta_j}| \leq m+1$ nach folgender Induktion nach m:

$$\begin{aligned} m = 0 : &|\frac{sin(0+1)\theta_j}{sin\theta_j}| = |1| \leq 0+1 \\ m \mapsto m+1 : &|\frac{sin(m+1)\theta_j}{sin\theta_j}| = |\frac{sin\theta_j * cos(m\theta_j) + cos\theta_j * sin(m\theta_j)}{sin\theta_j}| \leq |cos(m\theta_j)| + |cos\theta_j \frac{sin(m\theta_j)}{sin\theta_j}| \\ &\overset{(Induktionsannahme)}{\leq} |cos(m\theta_j)| + m|cos\theta_j| \overset{|cos(r)| \leq 1 \; f\ddot{u}r \; r \in \mathbb{R}}{\leq} 1 + m \end{aligned}$$

Mit obiger Ungleichung erhält man also folgende untere Schranke für $S_Q(p^m)$

$$\begin{aligned} S_Q(p^m) &\geq \frac{2}{n} p^{\frac{m}{2}} M(\mu_k) \frac{sinh(m+1)\psi_k}{sinh\psi_k} - \frac{2}{n} p^{\frac{m}{2}} \sum_{j:\, |\mu_j| \leq 2\sqrt{p}} (m+1) \\ &\geq \frac{2}{n} p^{\frac{m}{2}} M(\mu_k) \frac{sinh(m+1)\psi_k}{sinh\psi_k} - \frac{2}{n} p^{\frac{m}{2}} n * (m+1) \\ &= \frac{2}{n} p^{\frac{m}{2}} M(\mu_k) \frac{sinh(m+1)\psi_k}{sinh\psi_k} - 2p^{\frac{m}{2}} (m+1) \end{aligned}$$

Als nächstes wird eine obere Schranke für $S_Q(p^m)$ bestimmt.
Da m gerade ist, ist nach Bemerkung 2.3 $S_Q(p^m)$ die Anzahl der ganzzahligen Lösungen von

$$x_0^2 + 4q^2(x_1^2 + x_2^2 + x_3^2) = p^m$$

Um die Anzahl der möglichen Lösungen abzuschätzen, werden zunächst die möglichen Wahlen für x_0 bestimmt.
Es gilt $|x_0| \leq p^{\frac{m}{2}}$ und $x_0^2 \equiv p^m \ (mod\ q^2)$, also nach [[1], Aufgabe 4.3.1] $x_0 \equiv \pm p^{\frac{m}{2}} \ (mod\ q^2)$. Da außerdem x_0 und p ungerade sind (also kongruent mod 2), führt dies zu $x_0 \equiv \pm p^{\frac{m}{2}} \ (mod\ 2q^2)$. Nach Teilen mit Rest ergeben sich also $\lfloor \frac{p^{\frac{m}{2}}}{q^2} \rfloor$ Möglichkeiten für $|x_0| < p^{\frac{m}{2}}$ und die Möglichkeit $|x_0| = p^{\frac{m}{2}}$. Ohne die Beträge ergibt dies also höchstens $2 * (\frac{p^{\frac{m}{2}}}{q^2} + 1)$ Möglichkeiten für die Wahl von x_0.
Ist x_0 bestimmt, so muss die Gleichung $x_1^2 + x_2^2 + x_3^2 = \frac{p^m - x_0^2}{4q^2}$ ganzzahlig gelöst werden. Mit der Notation 2.7 und nach Beispiel 2.8ii) ergibt dies für $\varepsilon > 0$ höchstens

$$r_3(\tfrac{p^m - x_0^2}{4q^2}) = O_\varepsilon((\tfrac{p^m - x_0^2}{4q^2})^{\frac{1}{2}+\varepsilon}) = O_\varepsilon((\tfrac{p^m}{q^2})^{\frac{1}{2}+\varepsilon})$$

mögliche Lösungen. Sei $C(\varepsilon)$ eine, wie in 2.7 gewählte, Konstante. Dann gilt

$$\begin{aligned}
S_Q(p^m) &\leq 2 * (\frac{p^{\frac{m}{2}}}{q^2} + 1) * r_3(\frac{p^m - x_0^2}{4q^2}) \leq 2 * (\frac{p^{\frac{m}{2}}}{q^2} + 1) * C(\varepsilon)(\frac{p^m}{q^2})^{\frac{1}{2}+\varepsilon} \\
&= 2C(\varepsilon) * (\frac{p^{\frac{m}{2}}}{q^2} + 1) * (\frac{p^m}{q^2})^{\frac{1}{2}+\varepsilon} = 2C(\varepsilon) * \frac{p^{m(\frac{1}{2}+\varepsilon)}}{q^{2(\frac{1}{2}+\varepsilon)}} * (\frac{p^{\frac{m}{2}}}{q^2} + 1) \\
&= 2C(\varepsilon) * \frac{p^{\frac{m}{2}+\varepsilon m}}{q^{1+2\varepsilon}} * (\frac{p^{\frac{m}{2}}}{q^2} + 1) = 2C(\varepsilon) * (\frac{p^{\frac{m}{2}+\varepsilon m} * p^{\frac{m}{2}}}{q^{1+2\varepsilon} * q^2} + \frac{p^{\frac{m}{2}+\varepsilon m}}{q^{1+2\varepsilon}}) \\
&= 2C(\varepsilon) * (\frac{p^{m(1+\varepsilon)}}{q^{3+2\varepsilon}} + \frac{p^{\frac{m}{2}(1+2\varepsilon)}}{q^{1+2\varepsilon}}) = 2C(\varepsilon) * (\frac{p^{m(1+\varepsilon)}}{q^3 * q^{2\varepsilon}} + \frac{p^{\frac{m}{2}(1+2\varepsilon)}}{q * q^{2\varepsilon}}) \\
&\leq 2C(\varepsilon) * (\frac{p^{m(1+\varepsilon)}}{q^3} + \frac{p^{\frac{m}{2}(1+2\varepsilon)}}{q}) \\
\Rightarrow \ S_Q(p^m) &= O_\varepsilon(\frac{p^{m(1+\varepsilon)}}{q^3} + \frac{p^{\frac{m}{2}(1+2\varepsilon)}}{q})
\end{aligned}$$

Sei jetzt C_ε eine, wie in 2.7 gewälte, Konstante (z.B. $C_\varepsilon = 2 * C(\varepsilon)$ wie oben).Es gilt $n \leq q^3$ nach [[1], 3.1.1 Proposition]. Dann gilt

$$\begin{aligned}
&\frac{2}{n} p^{\frac{m}{2}} M(\mu_k) \frac{sinh(m+1)\psi_k}{sinh\psi_k} - 2p^{\frac{m}{2}}(m+1) \leq S_Q(p^m) \leq C_\varepsilon(\frac{p^{m(1+\varepsilon)}}{q^3} + \frac{p^{\frac{m}{2}(1+2\varepsilon)}}{q}) \\
\Leftrightarrow\ & M(\mu_k)\frac{sinh(m+1)\psi_k}{sinh\psi_k} \leq \frac{1}{2} C_\varepsilon(\frac{n * p^{m(\frac{1}{2}+\varepsilon)}}{q^3} + \frac{n * p^{m\varepsilon}}{q}) + n(m+1) \\
\Rightarrow\ & M(\mu_k)\frac{sinh(m+1)\psi_k}{sinh\psi_k} \overset{n \leq q^3}{\leq} \frac{1}{2} C_\varepsilon(p^{m(\frac{1}{2}+\varepsilon)} + q^2 * p^{m\varepsilon}) + q^3(m+1)
\end{aligned}$$

Angenommen, m sei jetzt so gewählt, dass $p^{\frac{m}{2}} \leq q^3$. Dann gilt

$$M(\mu_k)\tfrac{sinh(m+1)\psi_k}{sinh\psi_k} \leq \tfrac{1}{2} C_\varepsilon(q^{3+6\varepsilon} + q^{2+6\varepsilon}) + q^3(m+1)$$

Außerdem gilt $p^{\frac{m}{2}} \leq q^3 \;\Leftrightarrow\; \frac{m}{2} \leq log_p q^3 \;\Leftrightarrow\; m \leq 6log_p q$ und somit

$$\begin{aligned} M(\mu_k)\frac{sinh(m+1)\psi_k}{sinh\psi_k} &\leq \frac{1}{2}C_\varepsilon(q^{3+6\varepsilon} + q^{2+6\varepsilon}) + q^3(1 + 6log_p q) \\ \Leftrightarrow\; M(\mu_k)sinh(m+1)\psi_k &\leq sinh(\psi_k)\frac{1}{2}C_\varepsilon(q^{3+6\varepsilon} + q^{2+6\varepsilon}) + q^3(1 + 6log_p q) \\ &\overset{sinh\psi_k \leq sinh(log\sqrt{p})}{\leq} sinh(log\sqrt{p})\frac{1}{2}C_\varepsilon(q^{3+6\varepsilon} + q * q^{2+6\varepsilon}) + q^3(1 + 6log_p q) \end{aligned}$$

Für große q gilt nun $log_p q \leq q^{6\varepsilon}$ und somit gilt

$$\begin{aligned} M(\mu_k)sinh(m+1)\psi_k &\leq sinh(log\sqrt{p})\frac{1}{2}C_\varepsilon * 2 * q^{3+6\varepsilon} + q^3(1 + 6q^{6\varepsilon}) \\ &\leq sinh(log\sqrt{p})C_\varepsilon * q^{3+6\varepsilon} + q^3 * q^{6\varepsilon} + 6q^{3+6\varepsilon}) \\ &\leq (sinh(log\sqrt{p})C_\varepsilon + 7)q^{3+6\varepsilon} \\ \Rightarrow\; M(\mu_k)sinh(m+1)\psi_k &= O_\varepsilon(q^{3+6\varepsilon}). \end{aligned}$$

Sei jetzt m die größte ganze gerade Zahl, für die gilt $p^{\frac{m}{2}} \leq q^3$ und sei q groß. Dann gilt $2e^{-(m+1)\psi_k} \leq e^{(m+1)\psi_k}$ und $q^3 \leq p^{\frac{m+2}{2}} \;\Leftrightarrow\; -1 + 6log_p q \leq m+1$. Weiterhin gilt $\psi_k \leq log\sqrt{p}$, es folgt

$$sinh(m+1)\psi_k \geq \frac{e^{(m+1)\psi_k}}{3} \geq \frac{e^{(-1+6log_p q)\psi_k}}{3} \geq \frac{p^{-\frac{1}{2}}}{3}e^{6log_p(q)*\psi_k}$$

Insgesamt gilt nun also

$$\begin{aligned} M(\mu_k) &= \frac{1}{sinh(m+1)\psi_k}O_\varepsilon(q^{3+6\varepsilon}) = \frac{3 * e^{-6log_p(q)*\psi_k}}{p^{-\frac{1}{2}}}O_\varepsilon(q^{3+6\varepsilon}) \\ &= O_\varepsilon(q^{3+6\varepsilon} * q^{-\frac{6\psi_k}{log\,p}}) = O_\varepsilon(q^{3+6\varepsilon-\frac{6\psi_k}{log\,p}}) \end{aligned}$$

Da μ_k nicht trivial ist, gilt nach Proposition 2.6 $M(\mu_k) \geq \frac{q-1}{2}$. Folglich existiert eine konstante C_ε mit

$$\begin{aligned} \frac{q-1}{2} &\leq M(\mu_k) \leq C_\varepsilon(q^{3+6\varepsilon-\frac{6\psi_k}{log\,p}}) \\ \Leftrightarrow\; q &\leq 2C_\varepsilon(q^{3+6\varepsilon-\frac{6\psi_k}{log\,p}}) + 1 \end{aligned}$$

Für große q (im vergleich zu C_ε), muss folglich gelten

$$3 + 6\varepsilon - \frac{6\psi_k}{log\,p} \geq 1 \text{ und somit } \psi_k \leq (\tfrac{1}{3} + \varepsilon)log\,p$$

Abschließend kann nun der Betrag von μ_k berechnet werden:

$$\begin{aligned} |\mu_k| = 2\sqrt{p}|cos\theta_k| &= \begin{cases} 2\sqrt{p}|cos(i\psi_k)| & \text{oder} \\ 2\sqrt{p}|cos(\pi + i\psi_k)| \end{cases} \\ &= 2\sqrt{p}|\pm cosh\psi_k| \leq \sqrt{p} * (p^{\frac{1}{3}+\varepsilon} + p^{-\frac{1}{3}-\varepsilon}) = p^{\frac{5}{6}+\varepsilon} + p^{\frac{1}{6}-\varepsilon} \end{aligned}$$

□

2.10 Korollar *Für festes $\varepsilon \in (0, \frac{1}{6})$ und großes q gilt*

$$h(X^{p,q}) \geq \frac{p+1-p^{\frac{5}{6}+\varepsilon}-p^{\frac{1}{6}-\varepsilon}}{2} > 0.$$

Insbesondere bilden die $X^{p,q}$ damit eine Familie von Expandergraphen.
Gilt außerdem noch $(\frac{p}{q}) = 1$, so gilt

$$\chi(X^{p,q}) \geq \frac{p+1}{p^{\frac{5}{6}+\varepsilon}+p^{\frac{1}{6}-\varepsilon}}$$

Beweis. Nach [[1], 1.2.3 Theorem] gilt $h(X^{p,q}) \geq \frac{(p+1)-\mu_1}{2}$ und nach [[1], 1.5.4 Korollar] gilt $\chi(X^{p,q}) \geq \frac{p+1}{max\{|\mu_1|,|\mu_{n-1}|\}}$. □

2.11 Korollar *Für $N \in \mathbb{N}$ existiert eine ungerade Primzahl p, sodass für große q gilt*

$$g(X^{p,q}) \geq N \text{ und } \chi(X^{p,q}) \geq N.$$

Beweis. Sei p groß genug, sodass $\frac{p+1}{p^{\frac{11}{12}}+p^{\frac{1}{12}}} \geq N$. Sei dann q so groß gewählt, dass folgende vier Bedingungen erfüllt sind:

$$\text{(i) } q > p^8 \text{ (ii) } 2log_p q \geq N \text{ (iii) } (\tfrac{p}{q}) = 1 \text{ (iv) } \chi(X^{p,q}) \geq \frac{p+1}{p^{\frac{11}{12}}+p^{\frac{1}{12}}}$$

(für (i)-(iii) findet man unendlich viele mögliche q und (iv) lässt sich dann nach Korollar 2.10 erfüllen).
Dann ist nach [[1], 4.3.3 Proposition] und [[1], 4.3.5 Theorem]

$$min\{g(X^{p,q}), \chi(X^{p,q})\} \geq N.$$

□

2.12 Bemerkung Die Familie der $X^{p,q}$ bilden eine Familie von Ramanujangraphen. Der Beweis dazu benötigt allerdings tiefere Ergebnisse, welche von Eichler gezeigt wurden [2]. An diese Ergebnisse anknüpfend lässt sich $S_Q(p^m)$ neu abschätzen und man erhält für $\varepsilon > 0$

$$S_Q(p^m) = \frac{4}{q(q^2-1)}\frac{p^{m+1}-1}{p-1} + O_\varepsilon(p^{\frac{m}{2}(1+\varepsilon)}).$$

(Für Details hierzu siehe [3],[4], und [5]). An dieser Stelle wird an die Spurformel vor Proposition 2.6 erinnert

$$S_Q(p^m) = \frac{2}{n}p^{\frac{m}{2}}\sum_{j=0}^{n-1}\frac{sin(m+1)\theta_j}{sin\theta_j}$$

Setzt man hier die trivialen Eigenwerte

$$\begin{cases} \theta_0 &= i * log\sqrt{p},\ falls\ (\frac{p}{q}) = 1 \\ \theta_0 &= i * log\sqrt{p}\ und\ \theta_{n-1} = \pi + i * log\sqrt{p},\ falls\ (\frac{p}{q}) = -1 \end{cases}$$

ein, so sieht man, dass deren Anteil an der Summe genau dem dominanten Term $\frac{4}{q(q^2-1)} \frac{p^{m+1}-1}{p-1}$ entspricht. Kürzt man diese also gegenseitig, so erhält man im ersten Fall

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

(Auf den zweiten Fall wird an dieser Stelle zur Einfachheit verzichtet.) Wäre also ein $\theta_j \notin \mathbb{R}$, so lässt sich dieses analog zum Beweis von Theorem 2.9 als $\theta_j = i\psi_j$ oder $\theta_j = \pi + i\psi_j$ mit $\psi_j \in (0, \ log\sqrt{p}]$ schreiben und erhält den folgenden Term

$$\frac{2}{n} \frac{sin(m+1)\theta_j}{sin\theta_j} = \frac{2}{n} \frac{sinh(m+1)\psi_j}{sinh\psi_j} > 0,$$

da m gerade ist. Für die realen θ_i gilt aber

$$|\frac{2}{n} \sum_{i:\theta_i \in \mathbb{R}} \frac{sin(m+1)\theta_i}{sin\theta_i}| \leq 2(m+1).$$

Diese beiden Terme können sich also sicher nicht gegenseitig aufheben. Für klein genügendes ε und großes gerades m erhält man also einen Widerspruch. Daher ist $X^{p,q}$ ein Ramanujangraph.

Literatur

[1] G. Davidoff, P. Sarnak & A. Valette, Elementary Number Theory, Group Theory, and Ramanujan Graphs, *Press Syndicate of the University of Cambridge*, 2003.

[2] M. Eichler, Quaternäre quadratische Formen und die Riemannsche Vermutung für die Kongruenz zeta funktion, *Arch. Math.*, 1954.

[3] A. Lubotzky, R. Phillips & P. Sarnak, Ramanujan graphs, *Combinatorica*, 1988.

[4] P. Sarnak, Some applications of modular forms, *Cambridge Trusts in math. Cambridge University Press*, 1990.

[5] A. Valette, Graphs de Ramanujan et applications, *Soc. Math. France*, 1997.