Markoff Triples and Linear Recurrence Sequences

Elisa Bellah

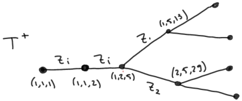
University of Toronto

January 30, 2025

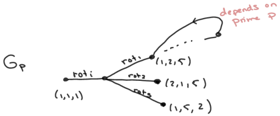
Plan

Markoff mod p graphs

Recall that the Markoff triples can be organized into a tree via Γ



Analogously, the Markoff mod p points can be organized into a graph via Γ



where

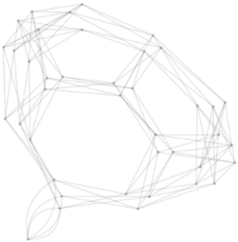
$$Z_1 = \sigma_{23} R_2, Z_2 = \sigma_{23}\sigma_{12} R_1, Z_3 = R_3$$

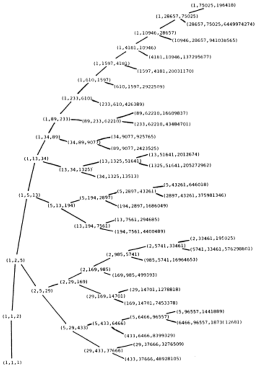
$$\mathrm{rot}_1 = \sigma_{23} R_2, \mathrm{rot}_2 = \sigma_{13} R_1, \mathrm{rot}_3 = \sigma_{12} R_1$$

Markoff mod p graphs

Key Observation

- Strong Approximation $\Leftrightarrow$ G_p connected.
- Lifts of mod p points correspond to paths in $\mathcal{G}_p$ from $(1, 1, 1)$





Rotation Orders

Define *ith rotation order* of a Markoff mod p point $\mathbf{x}$ to be

$$\mathrm{ord}_{p,i}(\mathbf{x}) := \min\{n \in \mathbb{Z}_{>1} : \mathrm{rot}_i^n(\mathbf{x}) = \mathbf{x}\},$$

and the *rotation order* to be $\mathrm{ord}_p(\mathbf{x}) := \max_i\{\mathrm{ord}_{p,i}(\mathbf{x})\}$.

Observation.

If $\mathbf{x} = (x_1, x_2, x_3)$ is a Markoff mod p point, then $\mathrm{ord}_{p,i}(\mathbf{x})$ is equal to the order of

$$A_{x_i} := \begin{pmatrix} 0 & 1 \\ -1 & 3x_i \end{pmatrix}$$

in $\mathrm{GL}_2(\mathbb{F}_p)$.

<u>ex:</u> $\mathrm{rot}_1(x_1, x_2, x_3) = (x_1, x_3, 3x_1x_3 - x_2)$ and

$$\begin{pmatrix} 0 & 1 \\ -1 & 3x_1 \end{pmatrix} \begin{pmatrix} x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} x_3 \\ 3x_1x_3 - x_2 \end{pmatrix}.$$

Rotations and Recurrence

Observation 1.

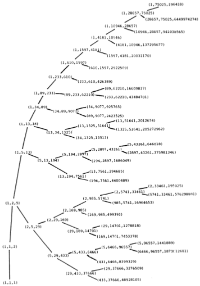
We have $\mathrm{rot}_1^n(x_1, x_2, x_3) = (x_1, a_n, a_{n+1})$, where $\{a_n\}$ is order two LRS with $a_0 = x_2, a_1 = x_3$ and

$$a_{n+2} = 3x_1 a_{n+1} - a_n.$$

and similarly for other rotations ($\mathrm{rot}_i^n(x_1, x_2, x_3) = \sigma(x_i, a_n, a_{n+1})$)

ex:

$$\mathrm{rot}_1^n(1, 1, 1) = (1, f_{2n-1}, f_{2n+1})$$



Rotation Orders and Pisano Periods

The *Lucas sequence* $u_n = u_n(P, Q)$ is the order two linear recurrence sequence with $u_0 = 0$, $u_1 = 1$ and $u_{n+2} = Pu_{n+1} - Qu_n$.

Observation 2.

The ith rotation order of a point (x_1, x_2, x_3) is equal to the period of the Lucas sequence $u_n = u_n(3x_i, 1)$.

Idea. Use familiar Lucas sequence identity

$$\begin{pmatrix} 3x_i & -1 \\ 1 & 0 \end{pmatrix}^n = \begin{pmatrix} u_{n+1} & -u_n \\ u_n & -u_{n-1} \end{pmatrix} \Rightarrow A_{x_i}^n = \begin{pmatrix} -u_{n-1} & u_n \\ -u_n & u_{n+1} \end{pmatrix}$$

Remark. Lucas sequences have nice arithmetic properties. For example $k \mid n \Rightarrow u_k \mid u_n$.

Sizes Under Action of Rotations

Question. For Markoff mod p points which have an integer lift, what is the size of a smallest lift?

Proposition (B., Chen, Fuchs, Ye, 2022+)

Let $n_i \in \mathbb{Z}_{\geq 1}$ and $i_j \in \{1, 2, 3\}$. Then we have

$$\mathrm{size}(\mathrm{rot}_{i_s}^{n_s} \cdots \mathrm{rot}_{i_1}^{n_1}(1,1,1)) \leq (3\varepsilon)^{2^{s-1}(n_1+1)\cdots(n_s+1)},$$

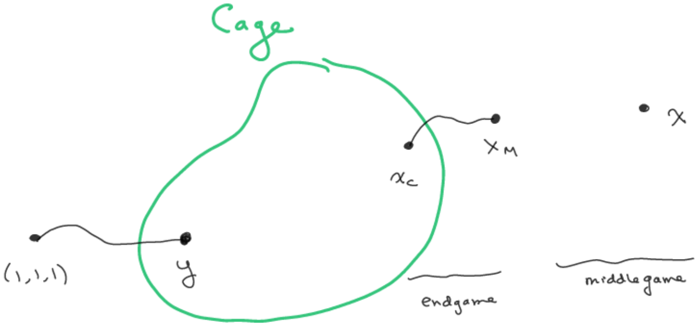
where $\varepsilon = \frac{3+\sqrt{5}}{2}$.

Remark: Bound is not tight.

Guiding principle: To find small lifts, want short paths that minimize the number of switches between distinct rotations.

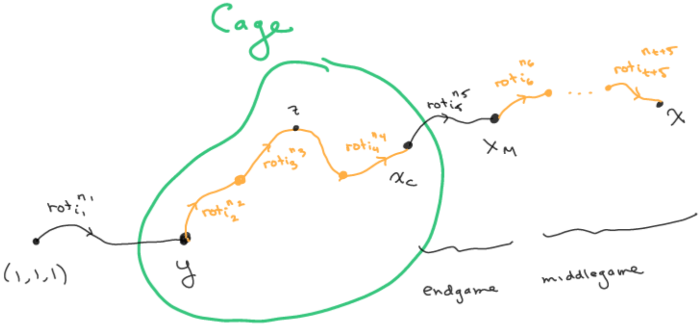
First Bound: BGS-style paths

BGS Algorithm.



First Bound: BGS-style paths

BGS Algorithm.



First Bound: BGS-style paths

Proposition (B., Chen, Fuchs, Ye, 2022+)

Let $n_i \in \mathbb{Z}_{\geq 1}$ and $i_j \in \{1, 2, 3\}$. Then we have

$$\mathrm{size}(\mathrm{rot}_{i_s}^{n_s} \cdots \mathrm{rot}_{i_1}^{n_1}(1,1,1)) \leq (3\varepsilon)^{2^{s-1}(n_1+1)\cdots(n_s+1)},$$

where $\varepsilon = \frac{3+\sqrt{5}}{2}$.

Theorem 1 (B., Chen, Fuchs, Ye, 2022+)

Let p be a prime so that $\mathrm{ord}_p(\mathrm{rot}_1^n(1,1,1)) \geq p-1$ for some n, and suppose that $\mathbf{x}$ is Markoff mod p point with $\mathrm{ord}_p(\mathbf{x}) > p^{\varepsilon}$ for $\varepsilon > 0$ fixed. Let $\tilde{\mathbf{x}}$ be a lift of $\mathbf{x}$ of minimal size. Then

$$\mathrm{size}(\tilde{\mathbf{x}}) < (3\varepsilon)^{2^{t+4}(2p+1)^{t+5}}$$

where $\varepsilon = (3+\sqrt{5})/2$ and $t = \tau(p^2-1)$.

Second Bound: Shortest paths

Idea:

- Take the shortest path from $(1,1,1)$ to $\mathbf{x}$ in $\mathcal{G}_p$.
- Length of this path is upper bounded by $\mathrm{diam}(G_p)$.
- Use upper bound for $\mathrm{diam}(G_p)$, depends on $h(G_p)$
- Assume your short path is as bad as possible

Theorem 2 (B., Chen, Fuchs, Ye, 2022+)

Let p be a prime where Strong Approximation holds and let $h(p)$ be the expansion constant of the Markoff mod p graph $\mathcal{G}_p$. For a Markoff triple $\mathbf{x}$, let $\tilde{\mathbf{x}}$ be a lift of $\mathbf{x}$ of minimal size. Then

$$\mathrm{size}(\tilde{\mathbf{x}}) < (3\varepsilon)^{\left(\frac{p^3+3}{2}\right)^{20/\log\left(1+\frac{h(p)}{3}\right)}}.$$

Large Pisano Periods and the Cage

Question: Is $(1, 1, 1)$ connected to the cage?

Remark. Point $\mathbf{x}$ is in the cage if $\mathrm{ord}_p(\mathbf{x}) \geq p - 1$.

Observation 2.

The ith rotation order of a point (x_1, x_2, x_3) is equal to the period of the Lucas sequence $u_n = u_n(3x_i, 1)$. In particular,

$$\mathrm{ord}_p(1, 1, 1) = \pi(p)/2,$$

where $\pi(p)$ is the Pisano period of the Fibonacci sequence.

Theorem (Vince, 1978).

If $p \equiv \pm 2 \pmod 5$ then $2^{\nu+1} \mid \pi(p)$, where $\nu = \nu_2(p + 1)$.

Large Pisano Periods and the Cage

Proposition

If $p > 5$ is a Mersenne prime with $p \equiv \pm 2 \pmod 5$, then $(1, 1, 1) \in \mathcal{C}(p)$.

Note: Lower bounds on the 2-adic valuation of $p + 1$ give lower bounds on the order of $(1, 1, 1)$, so you can say things like:

Proposition'

If $p > 5$ is a prime with $2^{\nu_2(p+1)} > p^{1/2+\delta}$, then $\mathrm{rot}_i^n(1, 1, 1)$ is in the cage for some $i \in \{1, 2, 3\}$.

Extending Vince's Result

For a Markoff triple (x_1, x_2, x_3), let $f(T) = T^2 - 3x_i T + 1$. Let Δ_{x_i} be the discriminant of f_{x_i} and η_{x_i} be a root of f_{x_i}.

Theorem (B., Dunn, Naidu, Wells, 2025++).

If $p \equiv \pm 2 \pmod 5$ and $\left(\frac{\Delta_{x_i}}{p}\right) = \left(\frac{\mathrm{Tr}(\eta_{x_i})+2}{p}\right) = -1$, then

$$2^{\nu_2(p+1)} \mid \mathrm{ord}_{p,i}(\mathbf{x}).$$

Corollary.

Let $p \equiv \pm 2 \pmod 5$ and suppose that $\mathbf{x} = (x_1, x_2, x_3)$ is a Markoff triple with x_i satisfying the conditions above.

(1) If $\nu_2(p+1) > \log_2(p-1)$ (e.g. p Mersenne) then $\mathbf{x} \in \mathcal{C}(p)$

(2) If $\nu_2(p+1) > \log_2(p^{1/2+\delta})$, then $\mathrm{rot}_i^n(\mathbf{x}) \in \mathcal{C}(p)$.

Next Steps

- Extend Vince's result beyond 2-adic valuation.
- Look at density of primes where $(1, 1, 1)$ is in the cage. Experimentally, seems to be around 40%. Maybe we can verify this for families of primes from previous result.
- Look at percentage of points in the cage for families of primes from previous results