A Heuristic Subexponential Algorithm to Find Paths in Markoff Graphs over Finite Fields

Joseph H. Silverman

Brown University

Algorithmic Number Theory Symposium
(ANTS XVI), MIT

Friday July 19, 2024, 12:15-12:45pm

Cryptographic Hash Functions

- A **cryptograph hash function** is a function
$$\mathsf{Hash} : \begin{pmatrix}\text{arbitray length}\\ \text{bit strings}\end{pmatrix} \longrightarrow \begin{pmatrix}\text{bit strings of a}\\ \text{specified length}\end{pmatrix}.$$
- They are crucial for modern encrypted communications.
- Required properties:
  - $\mathsf{Hash}()$ is easy to compute.
  - Given a specified output γ, it's hard to find an input β satisfying
$$\mathsf{Hash}(\beta) = \gamma.$$
  - It is hard to find distinct inputs $\beta_1 \neq \beta_2$ satisfying
$$\mathsf{Hash}(\beta_1) = \mathsf{Hash}(\beta_2).$$

Turning an Expander Graph into a Hash Function

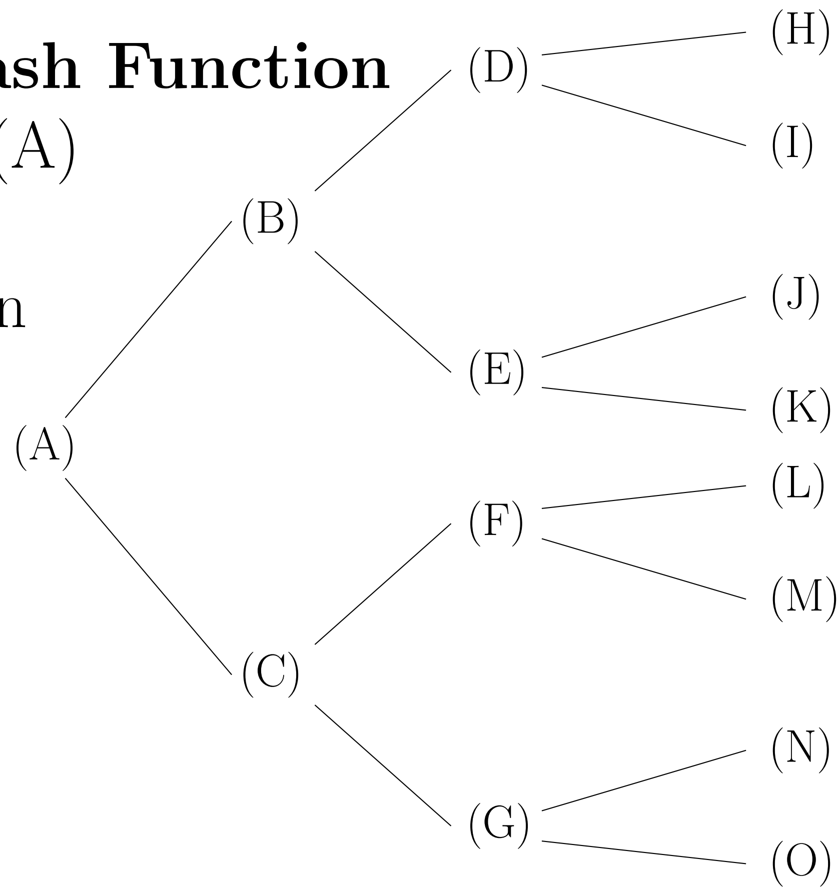
- Charles, Goren, and Lauter [*J. Cryptology* **22** (2009)] explained how to use expander graphs to construct hash functions, assuming that it is hard to find paths between specified initial and final vertices.

Graph to Hash Function

Rule: Start at (A)

1 = Up

0 = Down



Turning an Expander Graph into a Hash Function

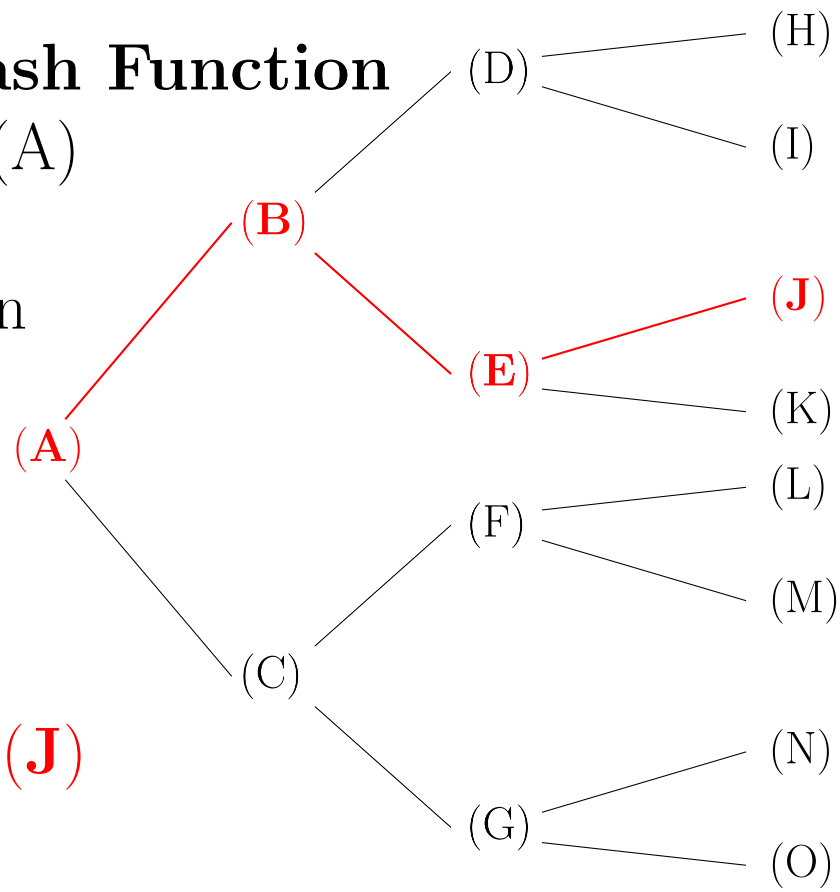
- Charles, Goren, and Lauter [*J. Cryptology* **22** (2009)] explained how to use expander graphs to construct hash functions, assuming that it is hard to find paths between specified initial and final vertices.

Graph to Hash Function

Rule: Start at (A)

1 = Up

0 = Down



$\mathbf{101} \xrightarrow{\text{Hash}} \mathbf{(J)}$

Turning an Expander Graph into a Hash Function

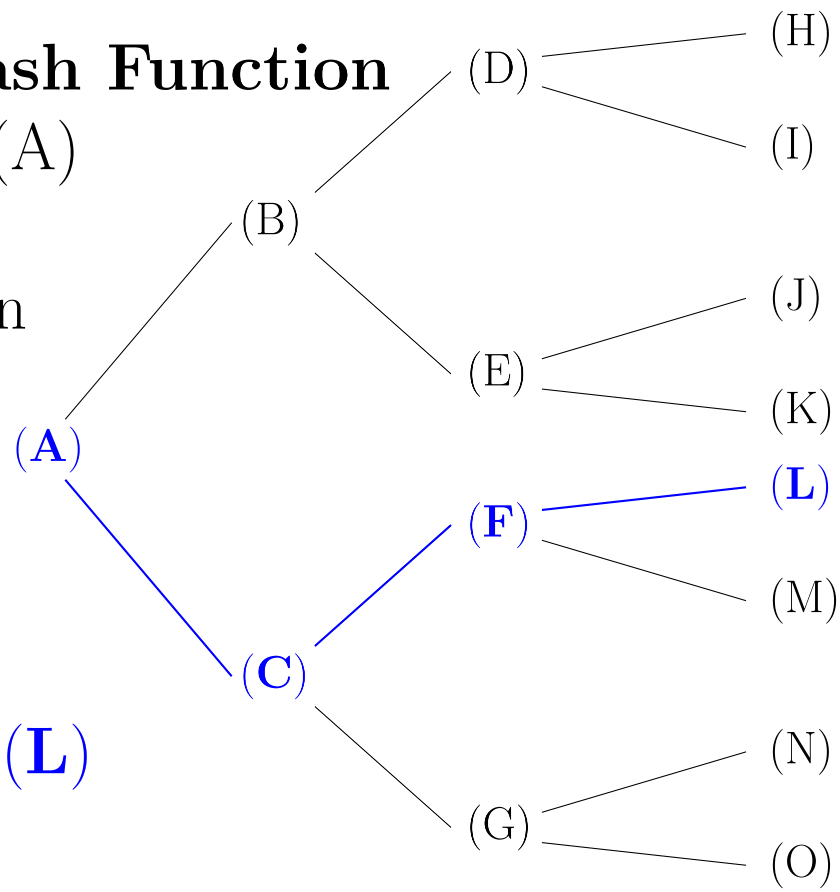
- Charles, Goren, and Lauter [*J. Cryptology* **22** (2009)] explained how to use expander graphs to construct hash functions, assuming that it is hard to find paths between specified initial and final vertices.

Graph to Hash Function

Rule: Start at (A)

$1 = \text{Up}$

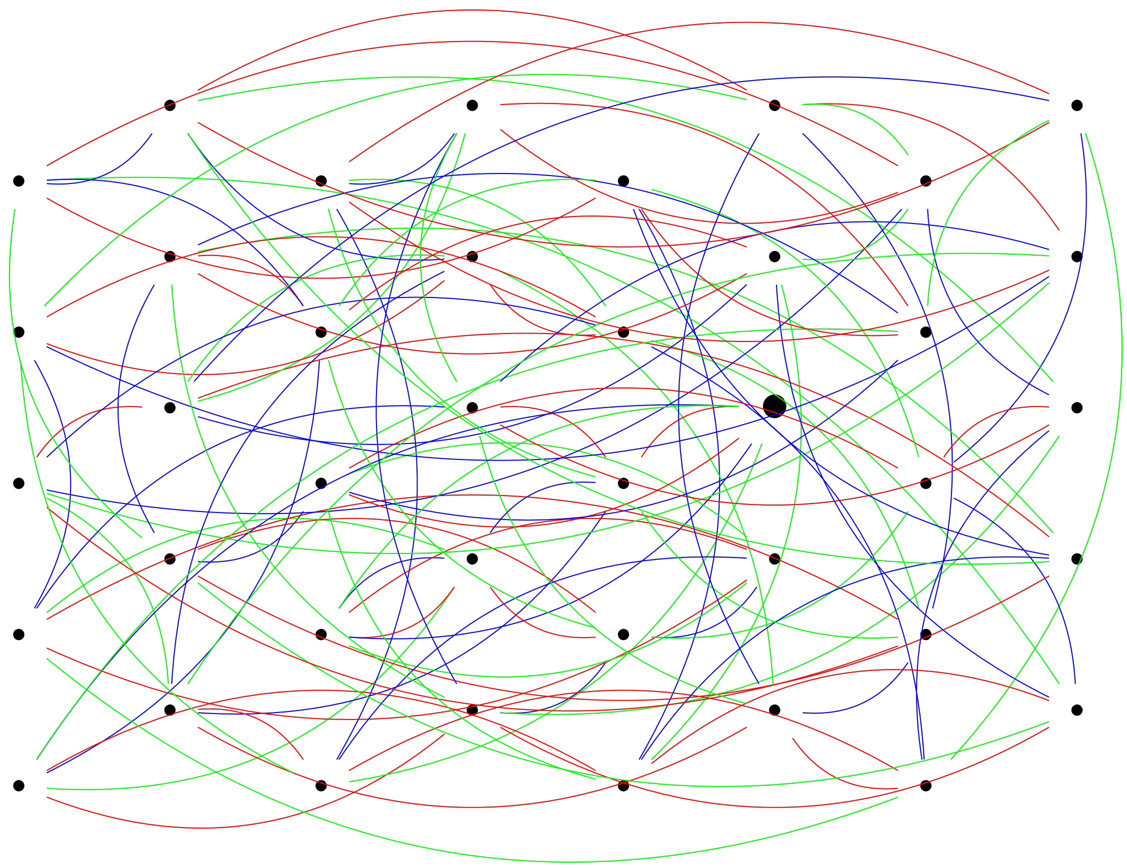
$0 = \text{Down}$



$\mathbf{011} \xrightarrow{\text{Hash}} (\mathbf{L})$

Turning an Expander Graph into a Hash Function

In practice one uses a large finite graph with a marked initial point.



The Markoff Equation

The **Markoff equation** is

$$\mathcal{M} : x^2 + y^2 + z^2 = 3xyz.$$

The equation is quadratic in each variable, so if we're given any solution (x_0, y_0, z_0), we can create a new solution by fixing two of the coordinates and switching the third coordinate to the other root of the quadratic equation.

This gives three non-commuting involutions

$$\sigma : \mathcal{M} \longrightarrow \mathcal{M},$$

and composing them with a coordinate permutation gives three *non-commuting rotations* given by the easily computed formulas

$$\begin{aligned} \rho_1(x, y, z) &= (x, z, 3xz - y), \\ \rho_2(x, y, z) &= (3xy - z, y, x), \\ \rho_3(x, y, z) &= (y, 3yz - x, z). \end{aligned}$$

The Markoff Graph

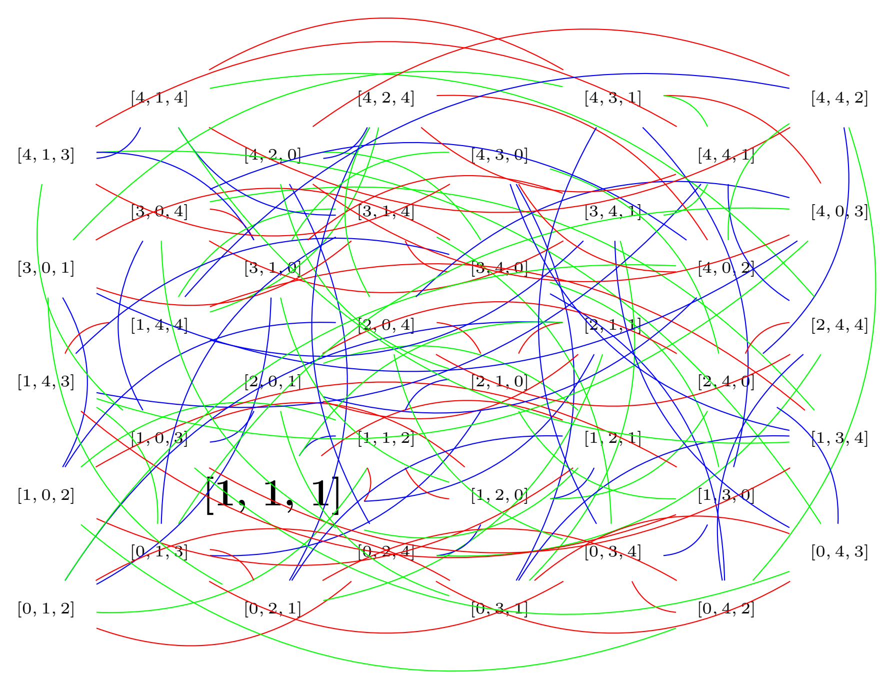
We use the set of non-zero points

$$\mathcal{M}(\mathbb{F}_p) = \left\{ \begin{matrix} \text{solutions to } x^2 + y^2 + z^2 = 3xyz \\ \text{with } x, y, z \text{ in the finite field } \mathbb{F}_p \end{matrix} \right\}$$

to create a graph with

$$\text{Vertices} = \mathcal{M}(\mathbb{F}_p), \quad \text{Initial Point} = [1,1,1],$$
$$\text{Edges} = \Big\{ \big[P, \rho_i(P)\big] : i = 1,2,3 \Big\}.$$

$\mathcal{M}(\mathbb{F}_5)$



Properties of the Markoff Graph

- $\mathcal{M}(\mathbb{F}_p)$ has roughly p^2 vertices. [Elementary]
- $\mathcal{M}(\mathbb{F}_p)$ is a connected graph for all sufficiently large p. [Bourgain–Gamburd–Sarnak, W. Chen]
- $\mathcal{M}(\mathbb{F}_p)$ is a family of expander graphs [Conjecture]

- Fuchs, Lauter, Litman, and Tran (2022) suggested that the Markoff graphs "may be good candidates" for the CGL hash function construction.
- In the remainder of this talk, I will sketch a heuristic path-finding algorithm for $\mathcal{M}(\mathbb{F}_p)$ that is subexponential time on a classical computer and polynomial time on a quantum computer.
- More precisely, to connect points in $\mathcal{M}(\mathbb{F}_p)$, it suffices to factor $p-1$ and to solve three discrete logarithm in $\mathbb{F}_p^*$.

Proof Sketch (as time permits)

We exploit ideas used by Bourgain–Gamburd–Sarnak. They note that for fixed x_0,

$$\rho_1(x_0, y, z) = \left[x_0, \begin{pmatrix} 3x_0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} y \\ z \end{pmatrix} \right].$$

Thus ρ_1 acts on the $x = x_0$ fiber via the matrix

$$L_{x_0} := \begin{pmatrix} 3x_0 & -1 \\ 1 & 0 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{F}_p).$$

$$L_{x_0} \text{ has order } p-1 \quad \Longrightarrow \quad \begin{pmatrix} \rho_1 \text{ acts transitively} \\ \text{on the } x = x_0 \text{ fiber} \end{pmatrix}.$$

If this occurs, we say that x_0 is **maximally hyperbolic**. And similarly for ρ_2 and ρ_3.

For randomly chosen points in $\mathcal{M}(\mathbb{F}_p)$, we have

$$\mathrm{Prob}\begin{pmatrix} P \in \mathcal{M}(\mathbb{F}_p) \text{ is } x(P)\text{-} \\ \text{maximally hyperbolic} \end{pmatrix} \approx \frac{\phi(p-1)}{2(p-1)} \geq \frac{1}{4\log\log p}.$$

Finding a path from $P \in \mathcal{M}(\mathbb{F}_p)$ to $Q \in \mathcal{M}(\mathbb{F}_p)$

(1) Randomly apply ρ_1 and ρ_3 to P until reaching a point P' that is y-maximally hyperbolic.

(2) Randomly apply ρ_1^{-1} and ρ_2^{-1} to Q until reaching a point Q' that is z-maximally hyperbolic.

(3) Let $F(X,Y,Z) = X^2 + Y^2 + Z^2 - 3XYZ$. Randomly select maximally hyperbolic $x_0 \in \mathbb{F}_p$ until the pair of quadratic equations

$$F\bigl(x_0, y(P'), Z\bigr) = F\bigl(x_0, Y, z(Q')\bigr) = 0$$

has a solution $(y_0, z_0) \in \mathbb{F}_q^2$. Set

$$P'' \leftarrow \bigl(x_0, y(P'), z_0\bigr) \quad \text{and} \quad Q'' \leftarrow \bigl(x_0, y_0, z(Q')\bigr).$$

- P'' and Q'' are on the maximally hyperbolic x_0-fiber.
- P' and P'' are on the maximally hyperbolic $y(P')$-fiber.
- Q' and Q'' are on the maximally hyperbolic $z(Q')$-fiber.

Finding a path from $P \in \mathcal{M}(\mathbb{F}_p)$ to $Q \in \mathcal{M}(\mathbb{F}_p)$

(4) Solve three DLPs in $\mathbb{F}_p^*$ to find k, m, n satisfying

$$P'' = \rho_2^k(P'), \quad Q' = \rho_3^m(Q''), \quad Q'' = \rho_1^n(P'').$$

These are DLPs because maximal hyperbolicity means that the associated matrices diagonalize over $\mathbb{F}_p$, so we end up needing to solve equations of the form

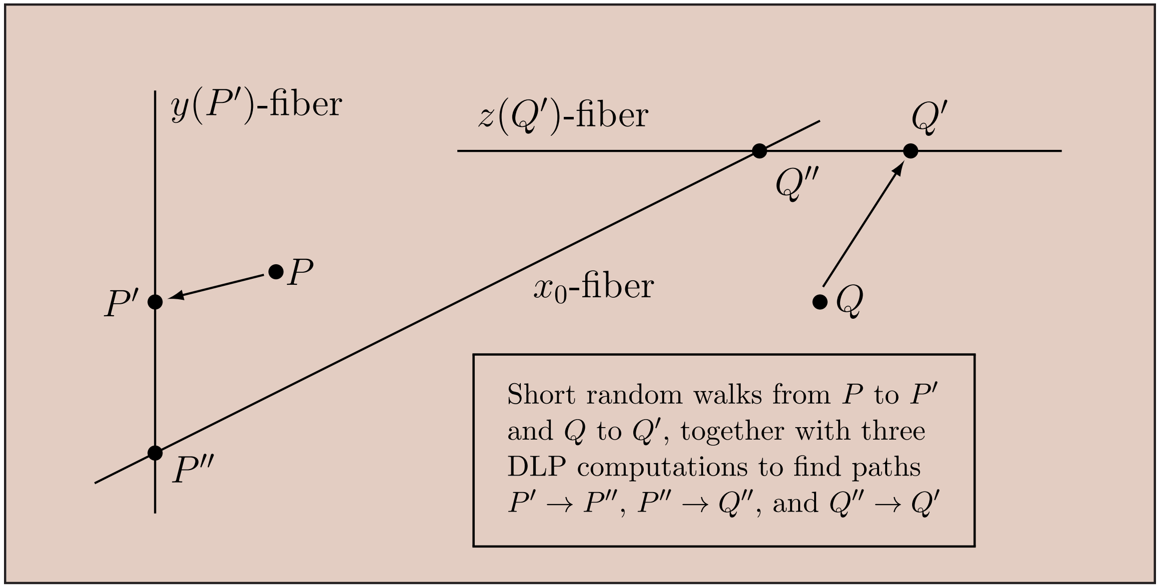
$$\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}^n \begin{pmatrix} \alpha \\ \alpha^{-1} \end{pmatrix} = \begin{pmatrix} \beta \\ \beta^{-1} \end{pmatrix} \quad \text{for known } \lambda, \alpha, \beta.$$

Finding a path from $P \in \mathcal{M}(\mathbb{F}_p)$ to $Q \in \mathcal{M}(\mathbb{F}_p)$

(5) This gives the path

$$P \xrightarrow{\langle\rho_1,\rho_3\rangle} P' \xrightarrow{\rho_2^k} P'' \xrightarrow{\rho_1^n} Q'' \xrightarrow{\rho_3^m} Q' \xrightarrow{\langle\rho_1,\rho_2\rangle} Q.$$

Illustrating the Markoff Path-Finding Algorithm



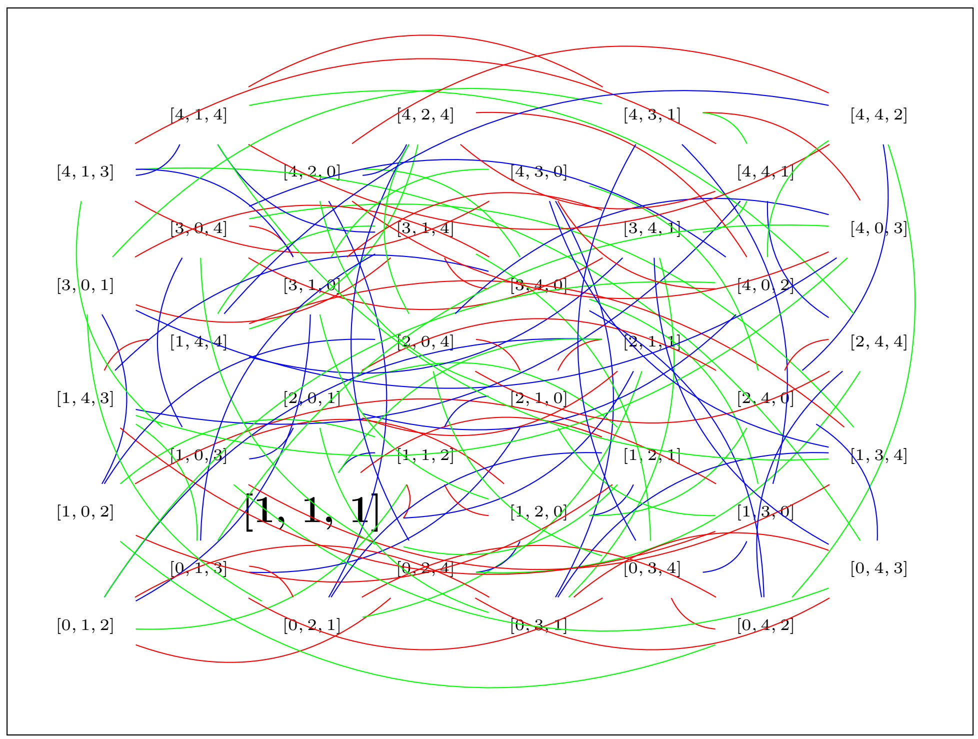
Please join me in thanking the ANTS XVI organizing committee:

Jennifer Balakrishnan, Kiran Kedlaya, Drew Sutherland, John Voight,

and the ANTS XVI program committee for putting together and running this fantastic conference.

ANTS XVI Program Committee

Eran Assaf
Edgar Costa
Alyson Deines
Andreas Enge
Steven Galbraith
Tommy Hofmann
Everett Howe
Fredrik Johansson
Valentijn Karemaker
Wanlin Li
Elisa Lorenzo García
Jonathan Love
Pascal Molin
Travis Morrison
Steffen Müller
Alina Ostafe
Ekin Ozman
Jen Paulhus
Christophe Ritzenthaler
David Roe
Renate Scheidler
Jeroen Sijsling
Benjamin Smith
Padma Srinivasan
Michael Stoll
Marco Streng
Lola Thompson
Anthony Várilly-Alvarado
Christelle Vincent
Bianca Viray
Isabel Vogt
Jonathan Webster
Benjamin Wesolowski
Yifan Yang



A Heuristic Subexponential Algorithm to Find Paths in Markoff Graphs over Finite Fields

Joseph H. Silverman

Brown University

Algorithmic Number Theory Symposium
(ANTS XVI), MIT

Friday July 19, 2024, 12:15-12:45pm