OTTAWA, 22 June, 2026

NT SEMINAR

UNIVERSITY OF WATERLOO

FROM ORIENTATIONS TO p-ADIC PERIOD VECTORS

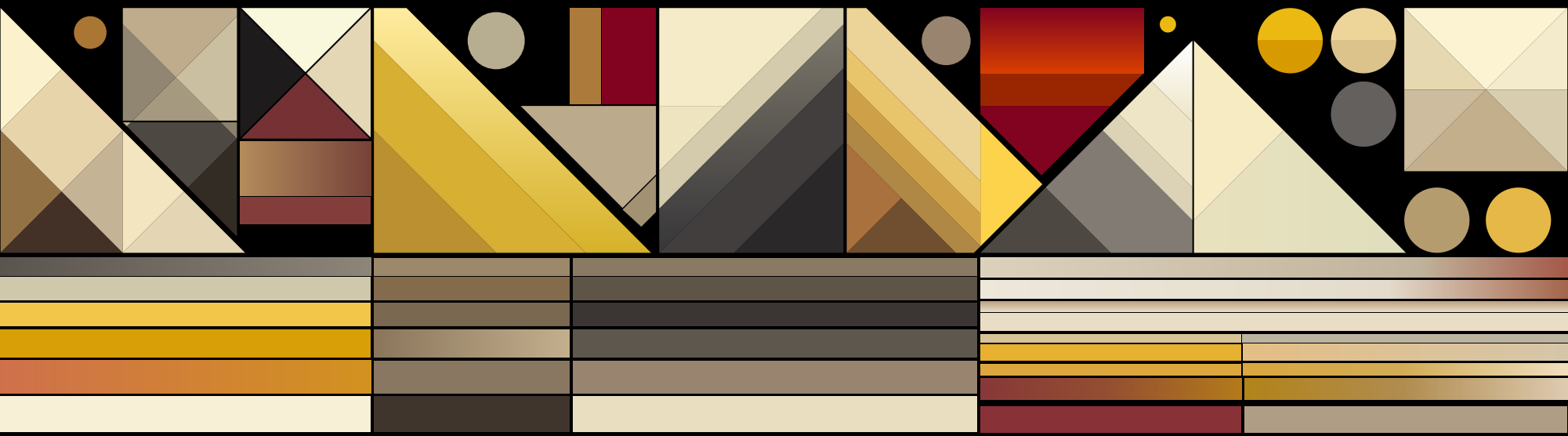
LEONARDO COLÒ



CONTENTS

- Supersingular isogeny graphs.
- Modular curves and level structures.
- Modular symbols and homology.
- p-adic integrals.
- Cryptographic constructions.

ELLIPTIC CURVES & ISOGENY GRAPHS



Elliptic curves

An elliptic curve over a field k (char $\neq 2, 3$):

$$E : y^2 = x^3 + Ax + B, \qquad \Delta = 4A^3 + 27B^2 \neq 0.$$

- Isogeny: non-constant algebraic group morphism $\varphi : E_1 \to E_2$.
- Kernel-theorem: if $\gcd(\deg \varphi, \mathrm{char}(k)) = 1$, then φ is uniquely determined by finite subgroup $\ker \varphi$.
- Dual isogeny and degree multiplication formula: $\widehat{\varphi} \circ \varphi = [\deg \varphi]$.

ISOGENY GRAPHS

L.COLÒ UWAT

Definition

Given an elliptic curve E over k, and a finite set of primes S, we can associate an isogeny graph $G_S(E)$

- whose vertices are elliptic curves isogenous to E over $\bar{k}$, and
- whose edges are isogenies of degree $\ell \in S$.

If $S = \{\ell\}$, then we write $G_\ell(E)$, the ℓ-isogeny graph.

The vertices are defined up to $\bar{k}$-isomorphism and the edges from a given vertex are defined up to a $\bar{k}$-isomorphism of the codomain.

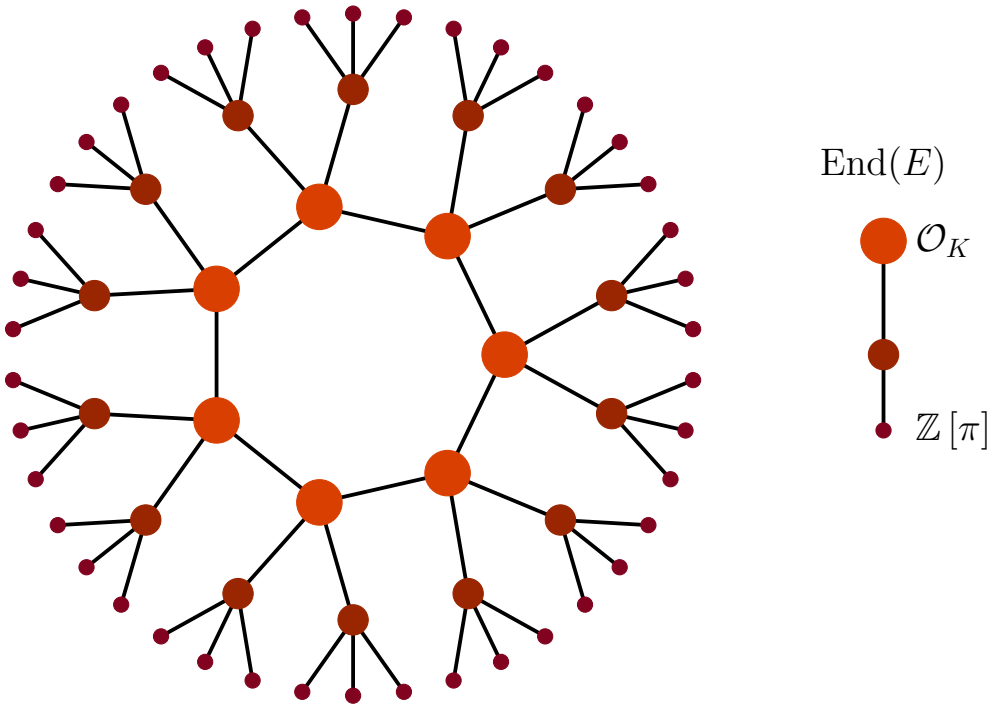
The ℓ-isogeny graph of E is $(\ell + 1)$-regular (as a directed multigraph).

ORDINARY ISOGENY GRAPHS: VOLCANOES

Let $\mathrm{End}(E) = \mathcal{O} \subseteq K$, an imaginary quadratic field. The class group $\mathrm{Cl}(\mathcal{O})$ acts faithfully and transitively on the set of elliptic curves with endomorphism ring $\mathcal{O}$:

$$E \longrightarrow E/E[\mathfrak{a}] \qquad E[\mathfrak{a}] = \{P \in E \mid \alpha(P) = 0 \ \forall \alpha \in \mathfrak{a}\}$$

Thus, the CM isogeny graphs can be modelled by an equivalent category of fractional ideals of K.

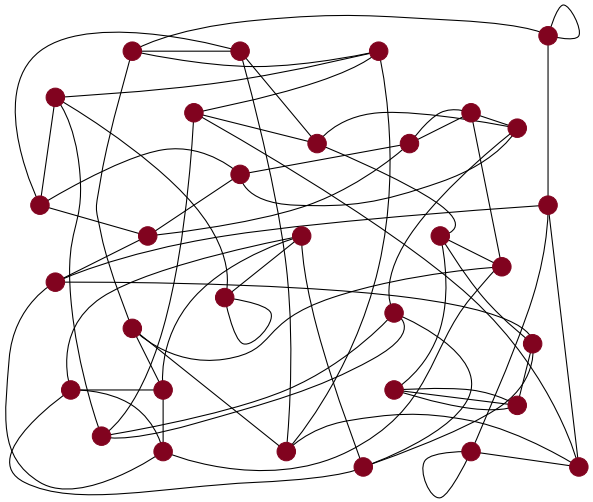


SUPERSINGULAR ISOGENY GRAPHS

The supersingular isogeny graphs are remarkable because the vertex sets are finite : there are $(p+1)/12+\epsilon_p$ curves. Moreover

- every supersingular elliptic curve can be defined over $\mathbb{F}_{p^2}$;
- all ℓ-isogenies are defined over $\mathbb{F}_{p^2}$;
- every endomorphism of E is defined over $\mathbb{F}_{p^2}$.

The lack of a commutative group acting on the set of supersingular elliptic curves/$\mathbb{F}_{p^2}$ makes the isogeny graph more complicated.

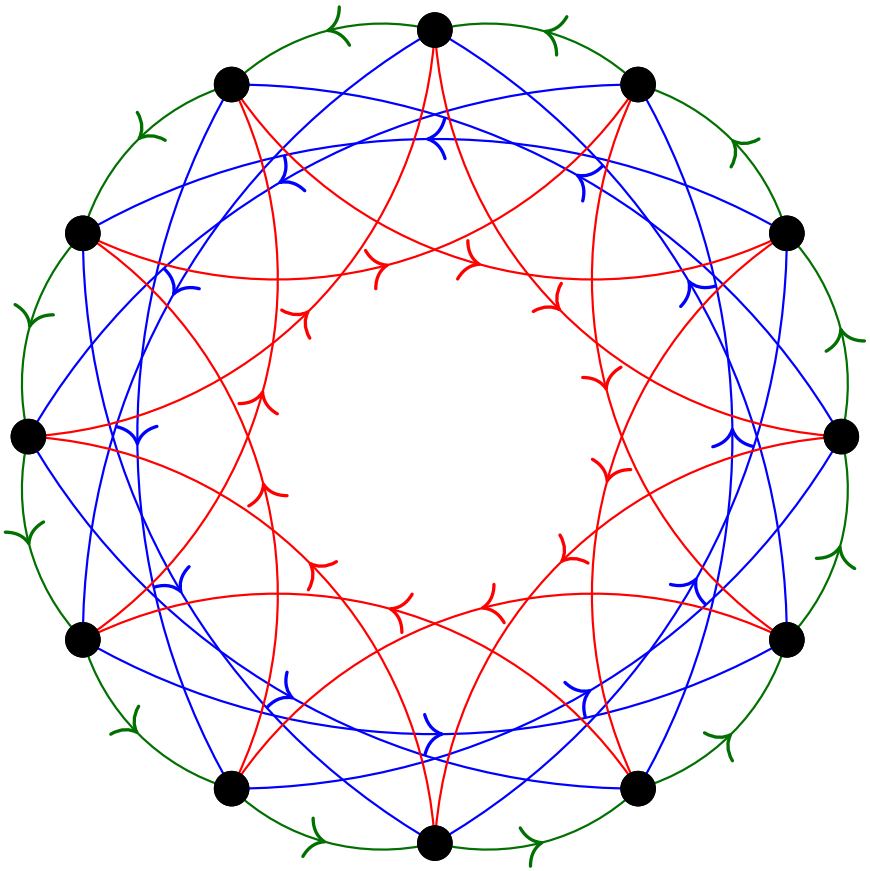


ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

Consider a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\ell_1, \ell_2, \ell_3\}$

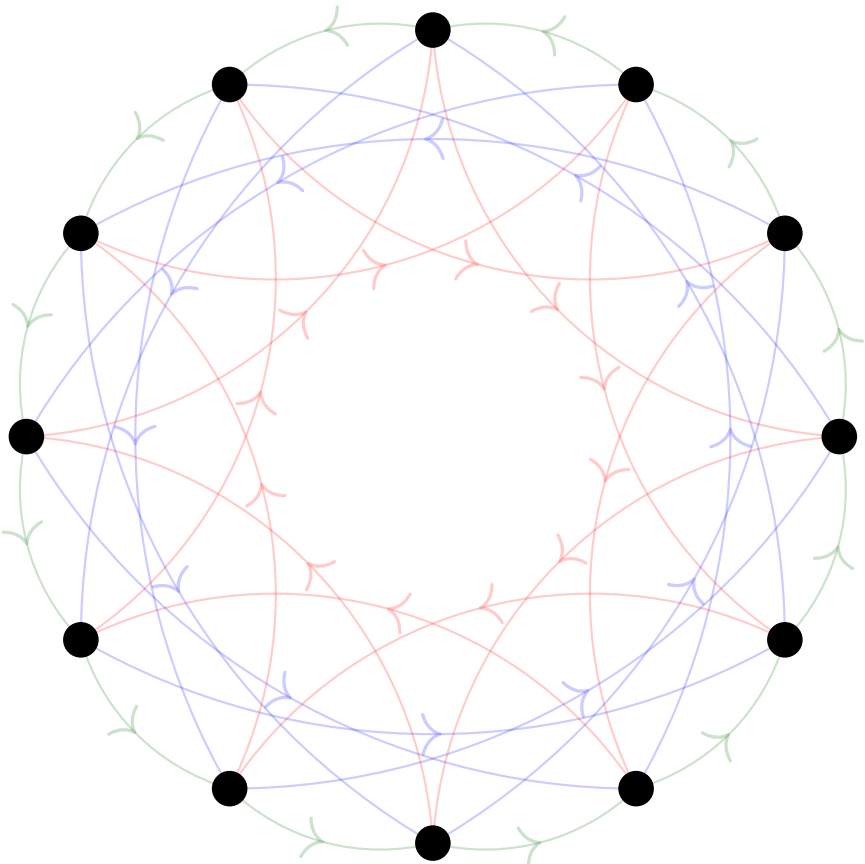


ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

Consider a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\ell_1, \ell_2, \ell_3\}$

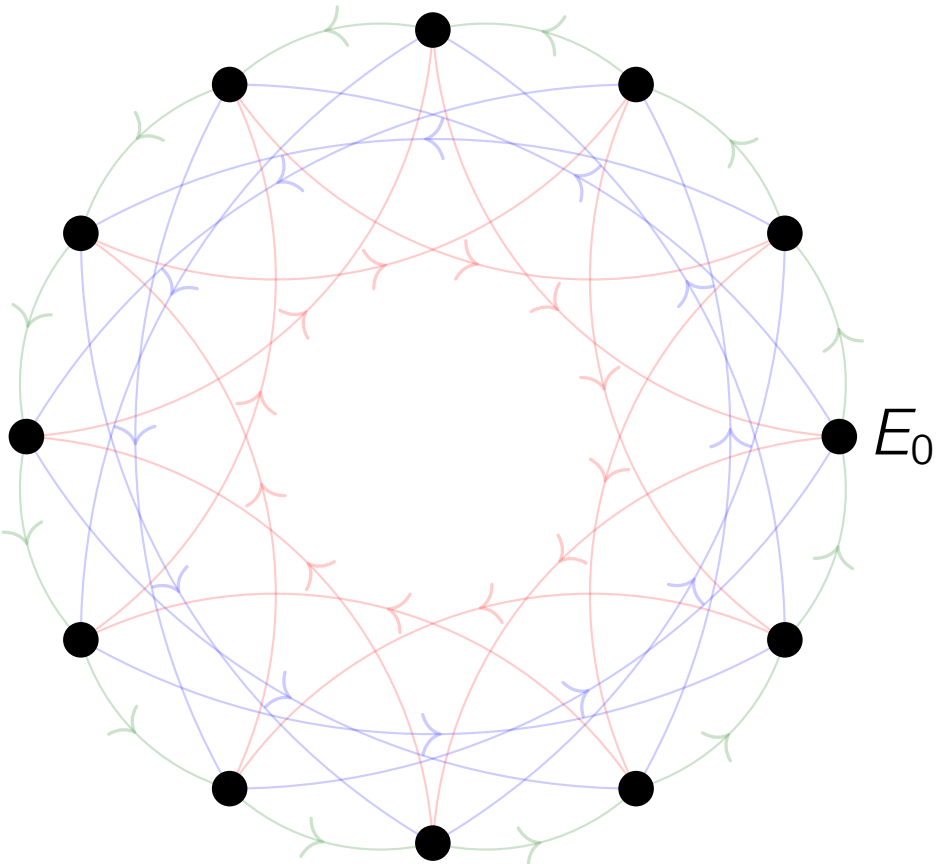


ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

Consider a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\ell_1, \ell_2, \ell_3\}$



ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

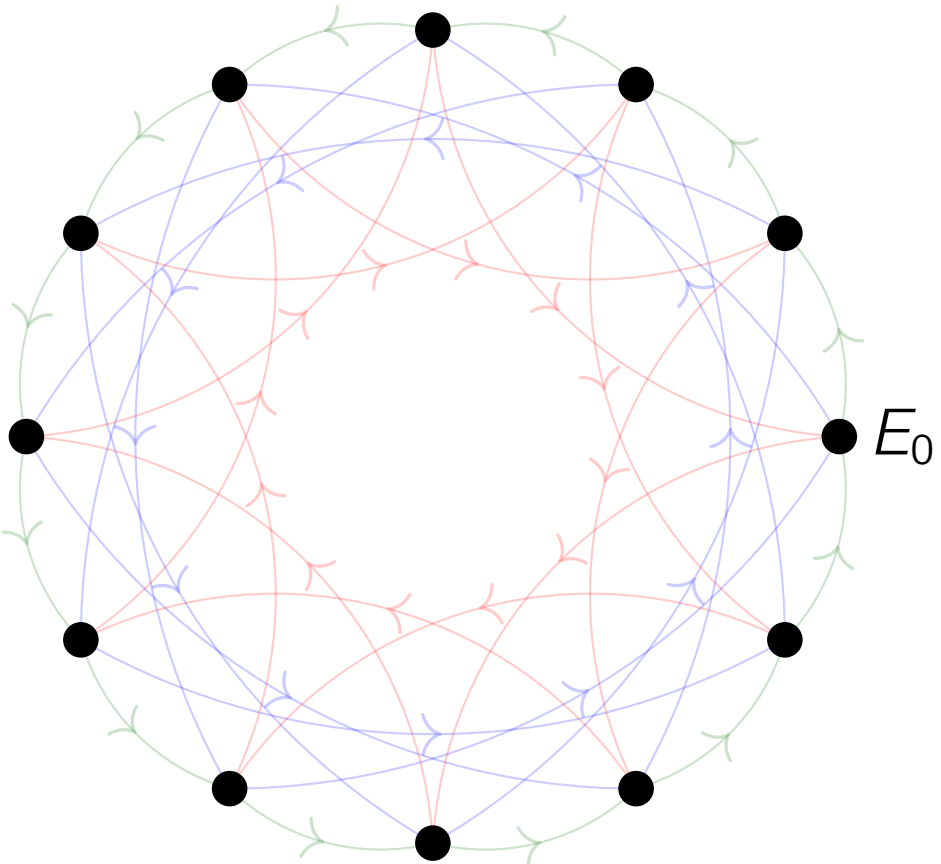
Consider a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$

Alice

$\rho_A = (2, 1, -1)$

$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$



ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

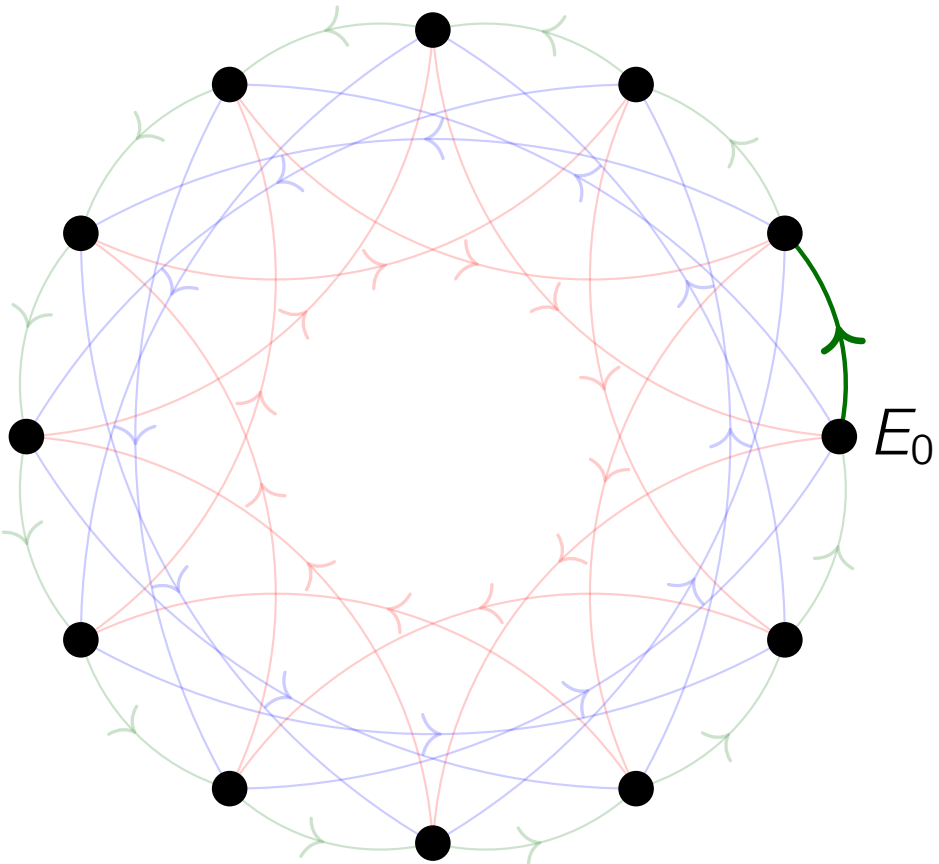
Consider a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$

Alice

$\rho_A = (2, 1, -1)$

$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$



ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

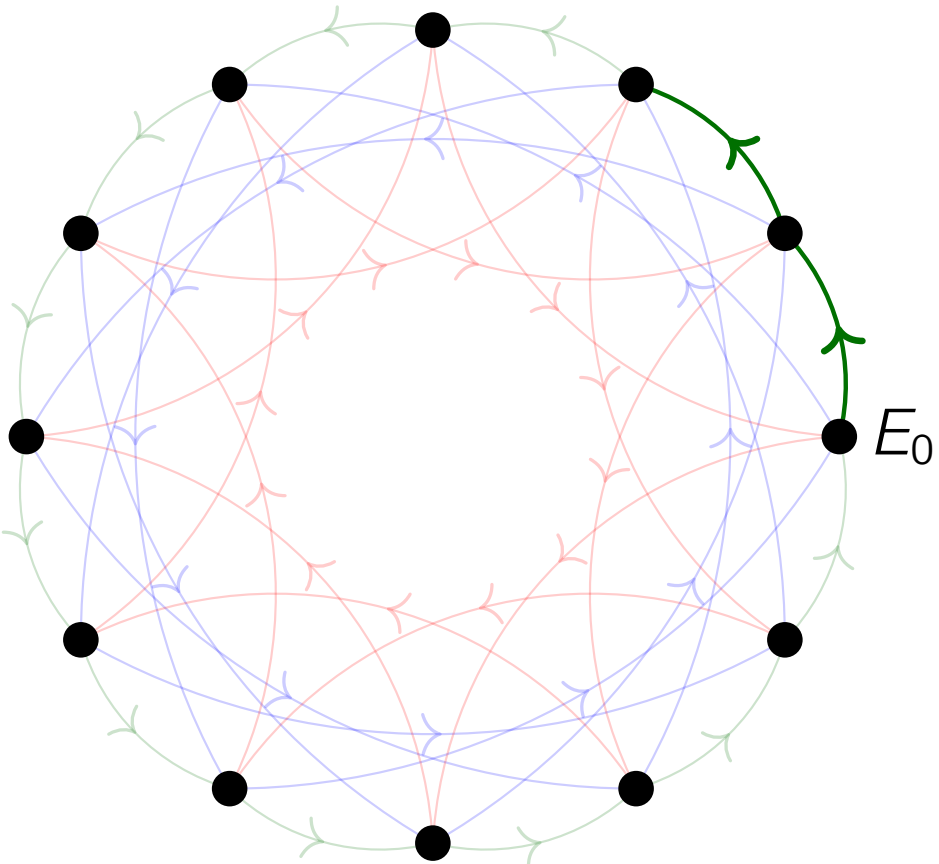
Consider a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$

Alice

$\rho_A = (2, 1, -1)$

$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$



ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

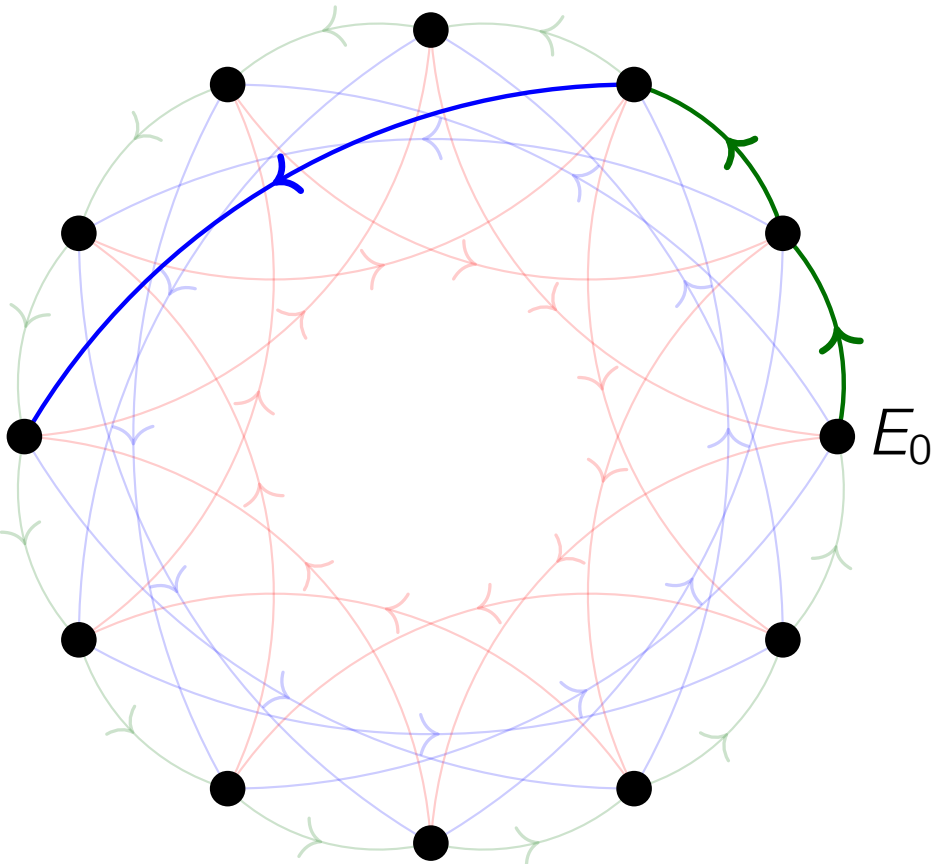
Consider a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$

Alice

$\rho_A = (2, 1, -1)$

$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$



ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

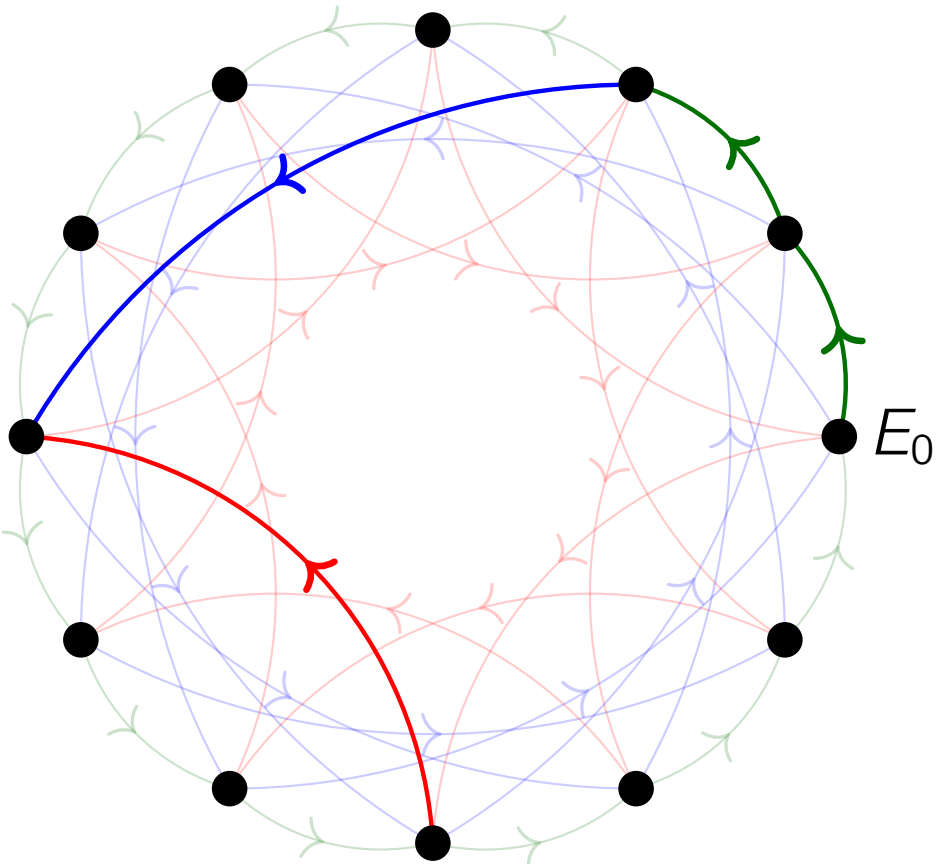
Consider a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$

Alice

$\rho_A = (2, 1, -1)$

$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$



ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

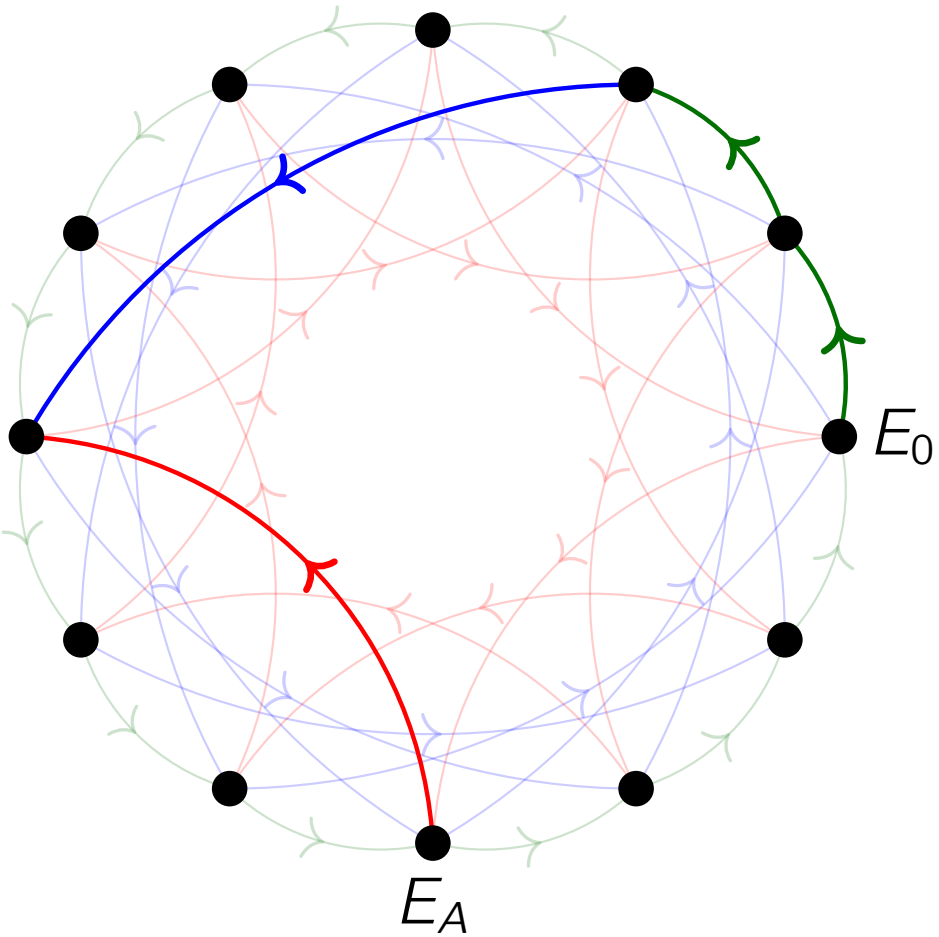
Consider a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$

Alice

$\rho_A = (2, 1, -1)$

$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$

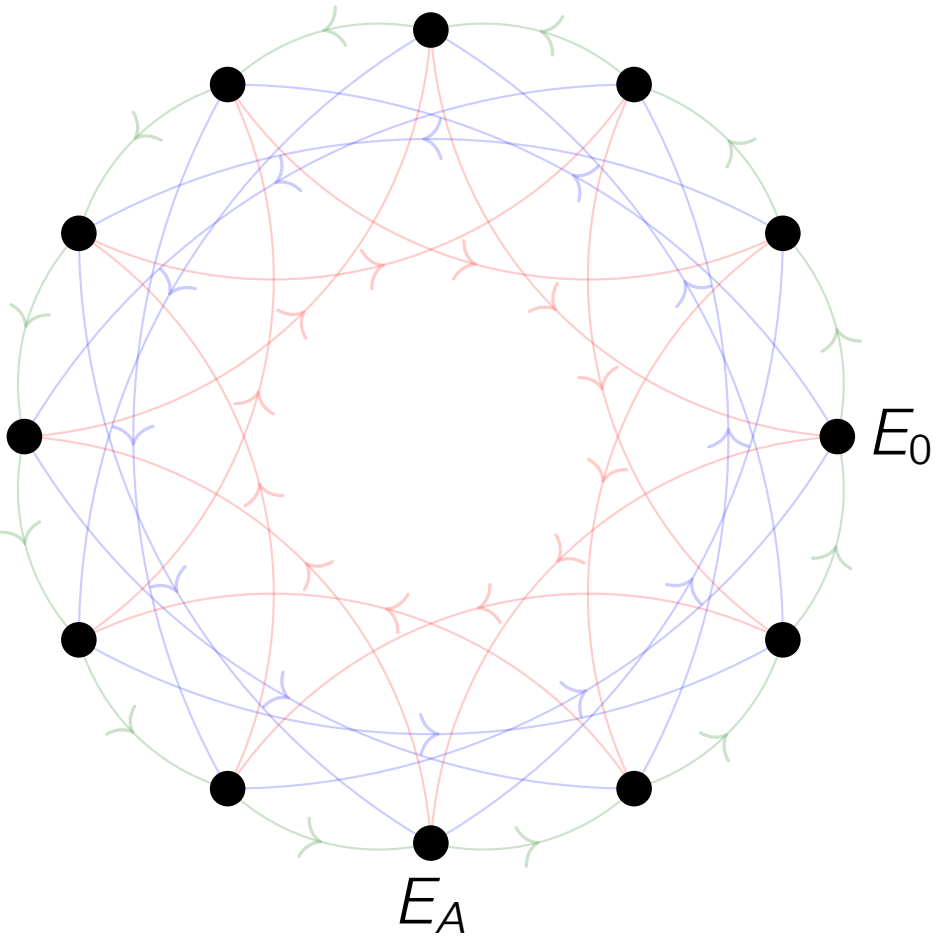


ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

Consider a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$



Alice

$\rho_A = (2, 1, -1)$

$\mathfrak{a} = \mathfrak{l}_1^2\mathfrak{l}_2^1\mathfrak{l}_3^{-1}$

Bob

$\rho_B = (-2, 0, 1)$

$\mathfrak{a} = \mathfrak{l}_1^{-2}\mathfrak{l}_3^1$

ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

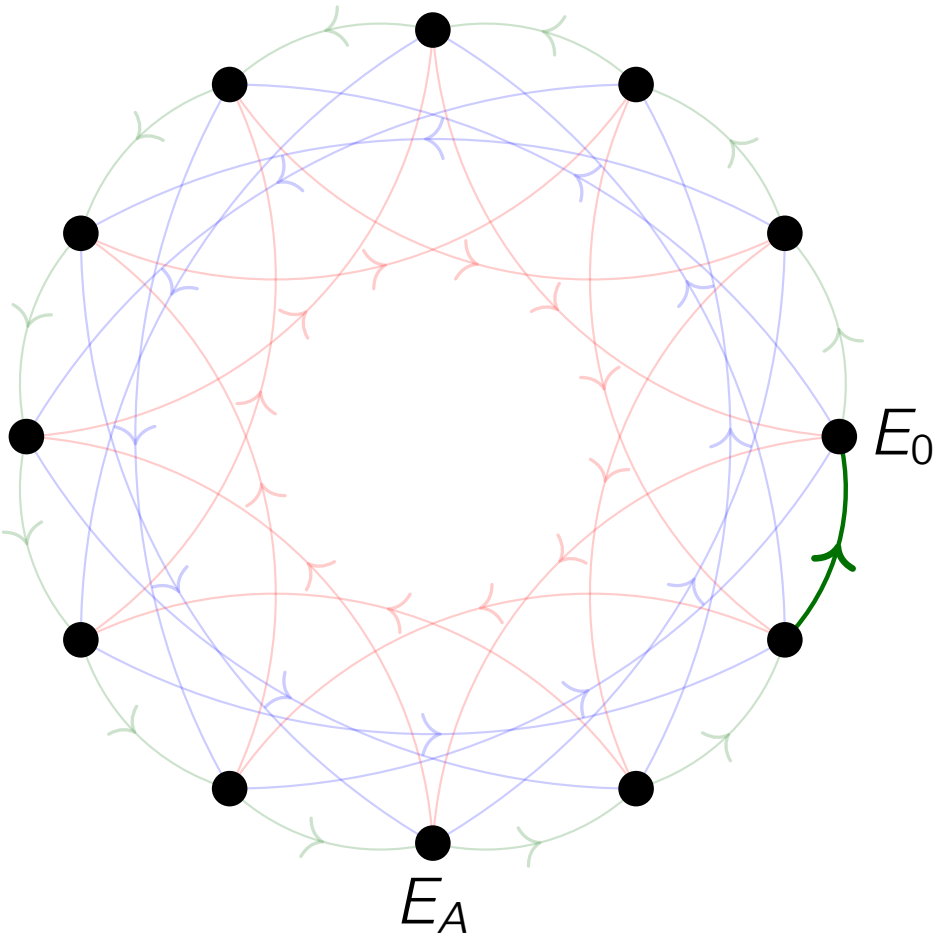
Consider a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$

Alice

$\rho_A = (2, 1, -1)$

$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$



Bob

$\rho_B = (-2, 0, 1)$

$\mathfrak{a} = \mathfrak{l}_1^{-2} \mathfrak{l}_3^1$

ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

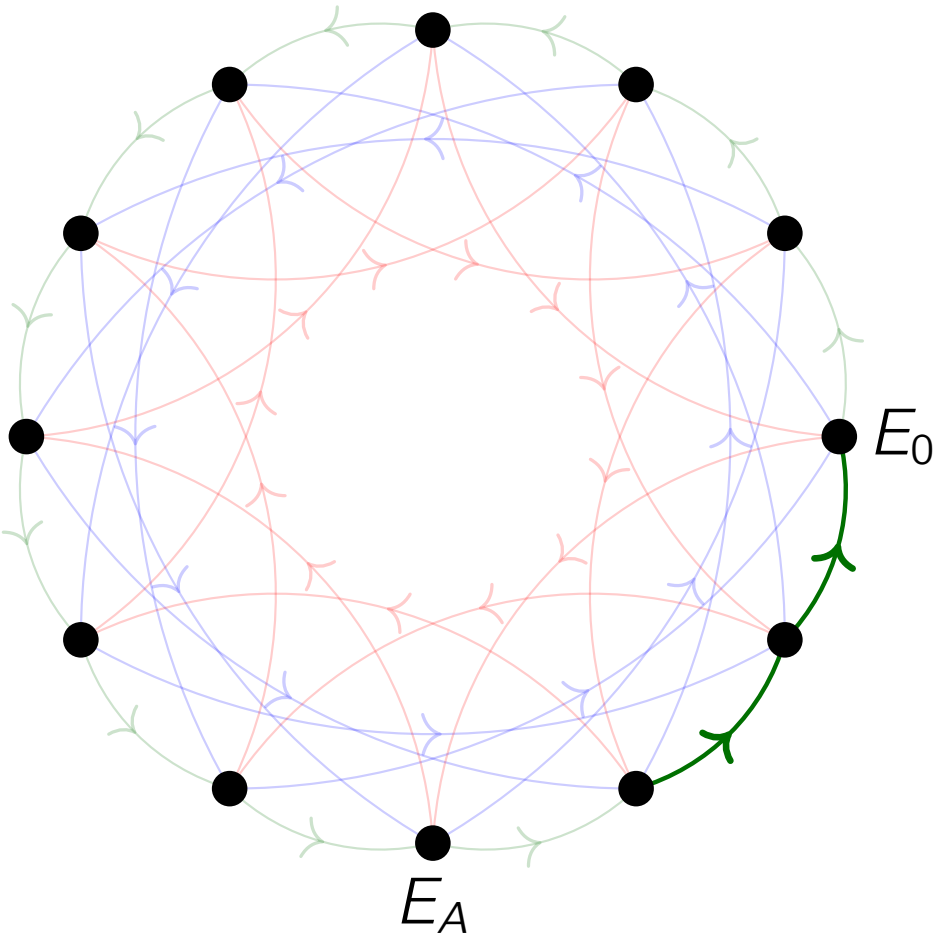
Consider a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$

Alice

$\rho_A = (2, 1, -1)$

$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$



Bob

$\rho_B = (-2, 0, 1)$

$\mathfrak{a} = \mathfrak{l}_1^{-2} \mathfrak{l}_3^1$

ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

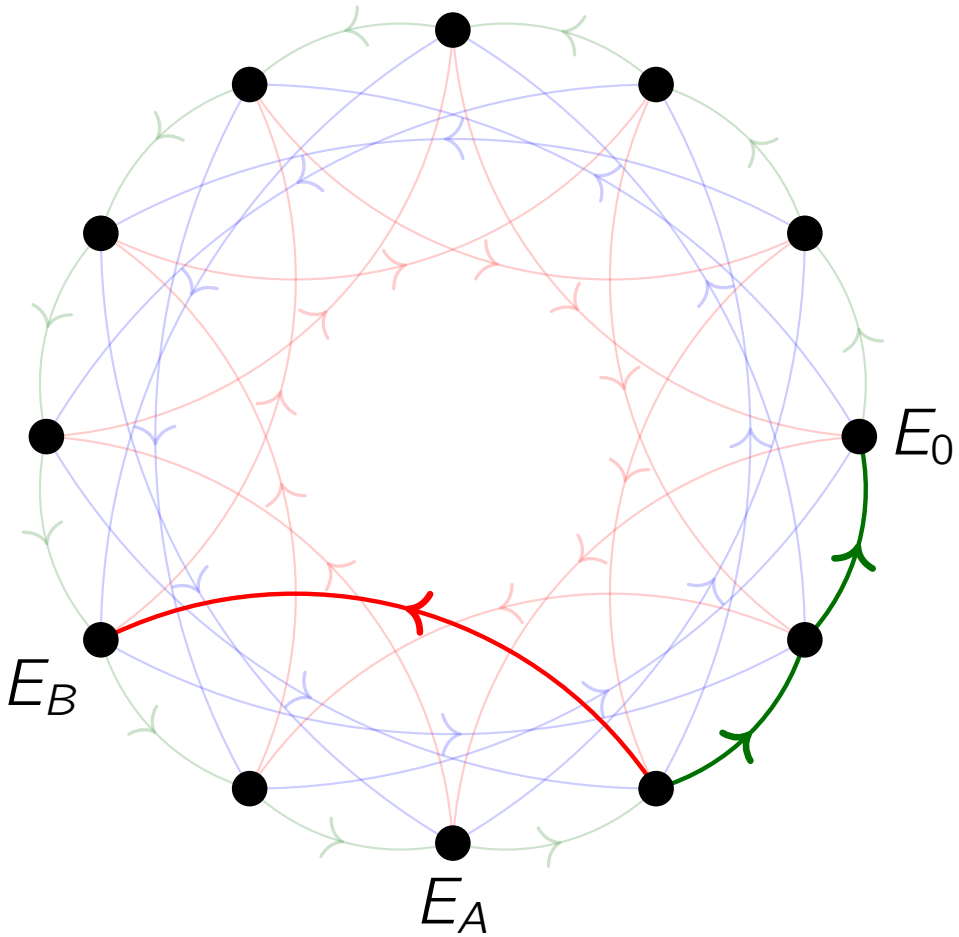
Consider a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$

Alice

$\rho_A = (2, 1, -1)$

$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$



Bob

$\rho_B = (-2, 0, 1)$

$\mathfrak{a} = \mathfrak{l}_1^{-2} \mathfrak{l}_3^1$

ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

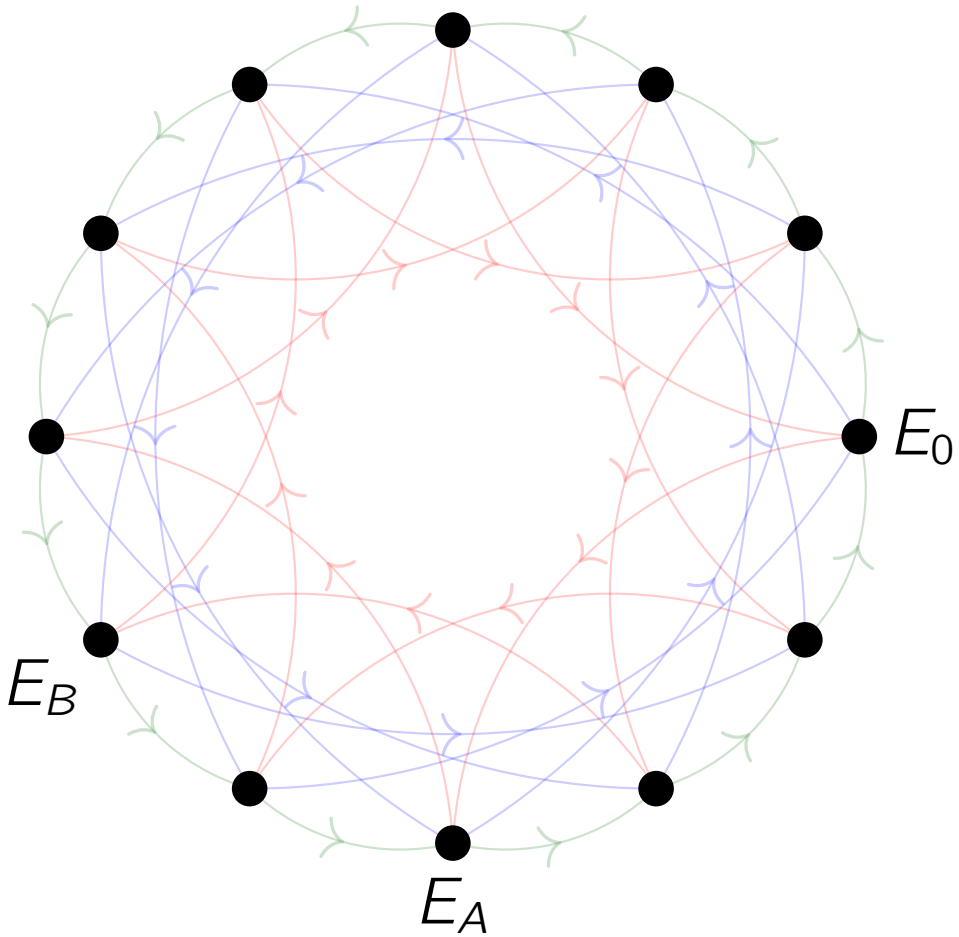
Consider a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$

Alice

$\rho_A = (2, 1, -1)$

$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$



Bob

$\rho_B = (-2, 0, 1)$

$\mathfrak{a} = \mathfrak{l}_1^{-2} \mathfrak{l}_3^1$

ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

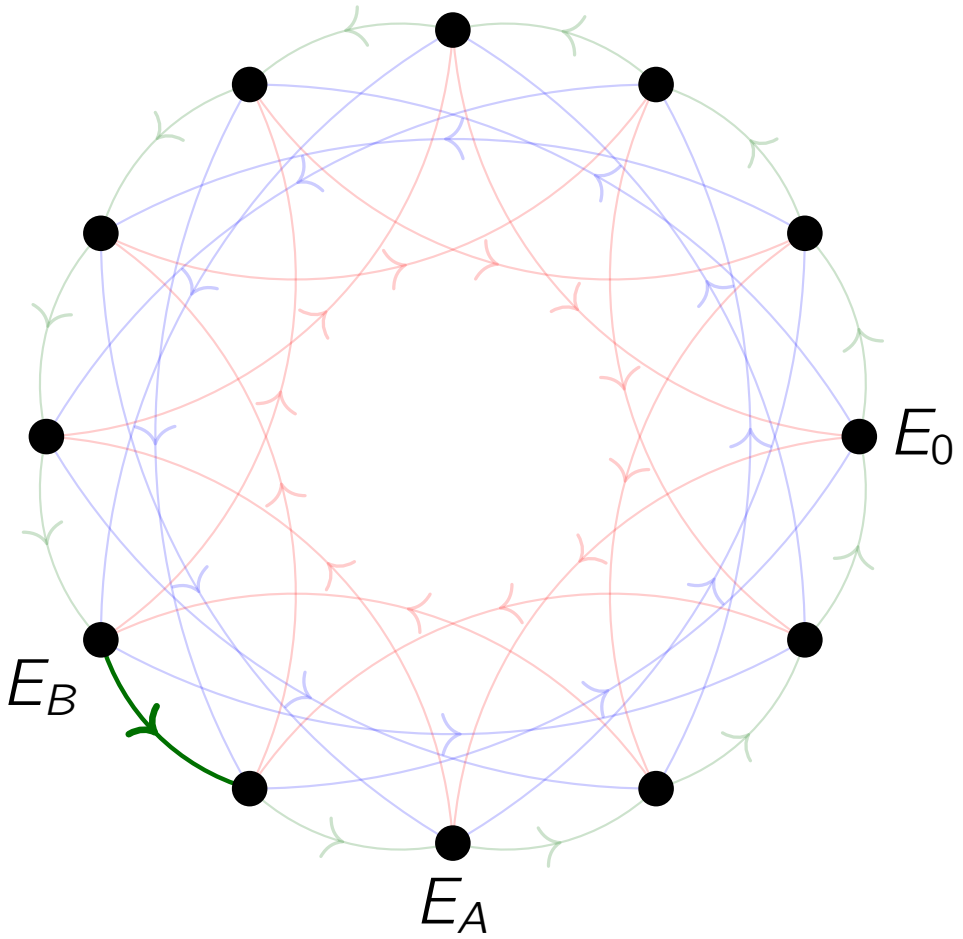
Consider a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$

Alice

$\rho_A = (2, 1, -1)$

$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$



Bob

$\rho_B = (-2, 0, 1)$

$\mathfrak{a} = \mathfrak{l}_1^{-2} \mathfrak{l}_3^1$

ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

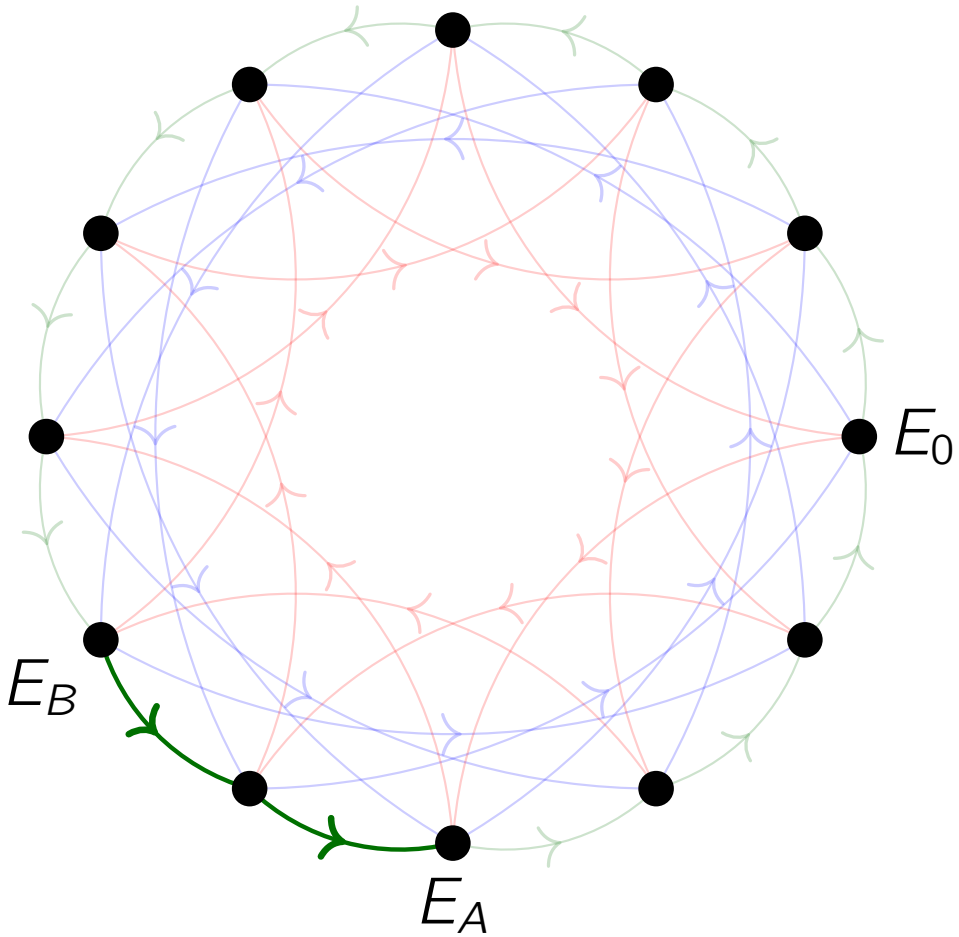
Consider a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$

Alice

$\rho_A = (2, 1, -1)$

$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$



Bob

$\rho_B = (-2, 0, 1)$

$\mathfrak{a} = \mathfrak{l}_1^{-2} \mathfrak{l}_3^1$

ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

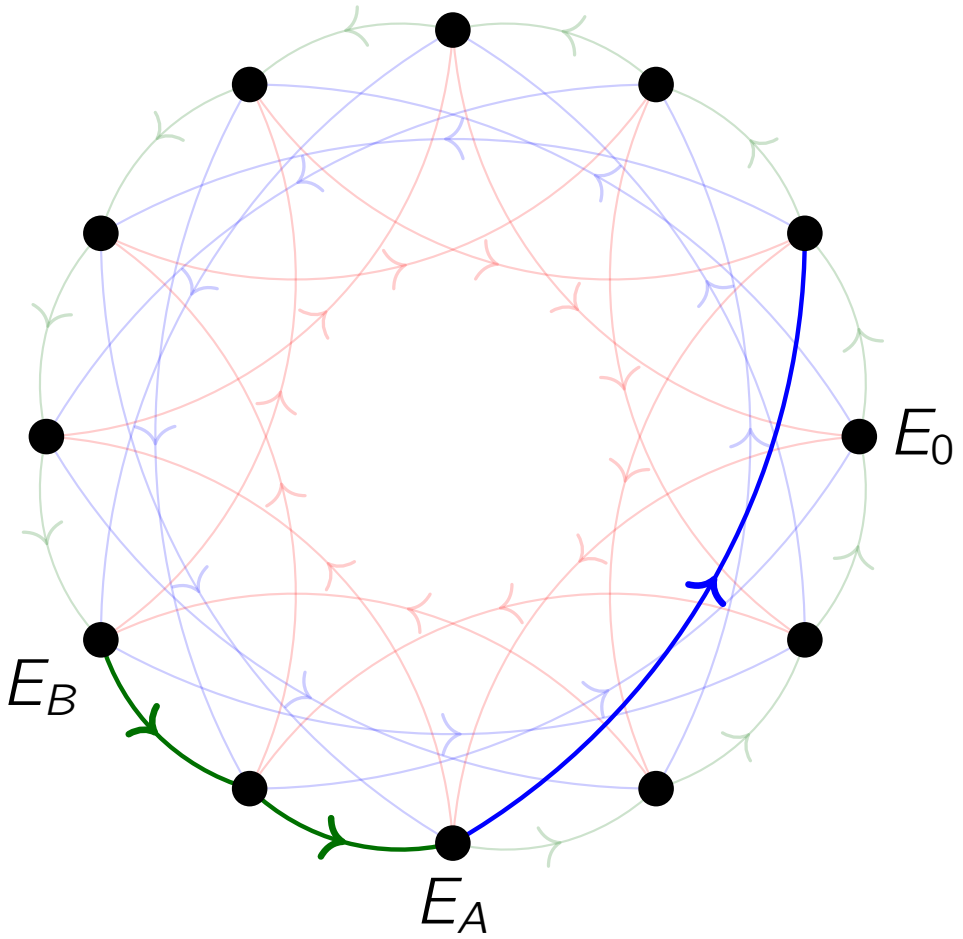
Consider a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$

Alice

$\rho_A = (2, 1, -1)$

$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$



Bob

$\rho_B = (-2, 0, 1)$

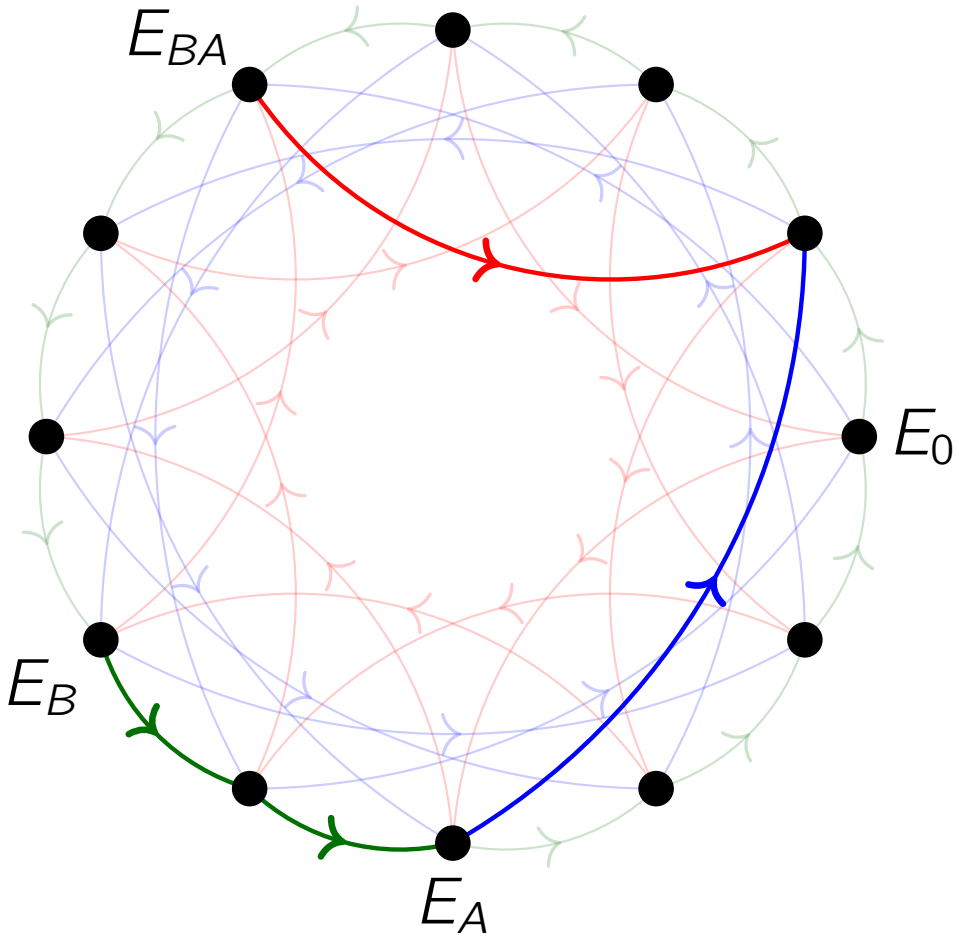
$\mathfrak{a} = \mathfrak{l}_1^{-2} \mathfrak{l}_3^1$

ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

Consider a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$



Alice

$\rho_A = (2, 1, -1)$

$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$

Bob

$\rho_B = (-2, 0, 1)$

$\mathfrak{a} = \mathfrak{l}_1^{-2} \mathfrak{l}_3^1$

ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

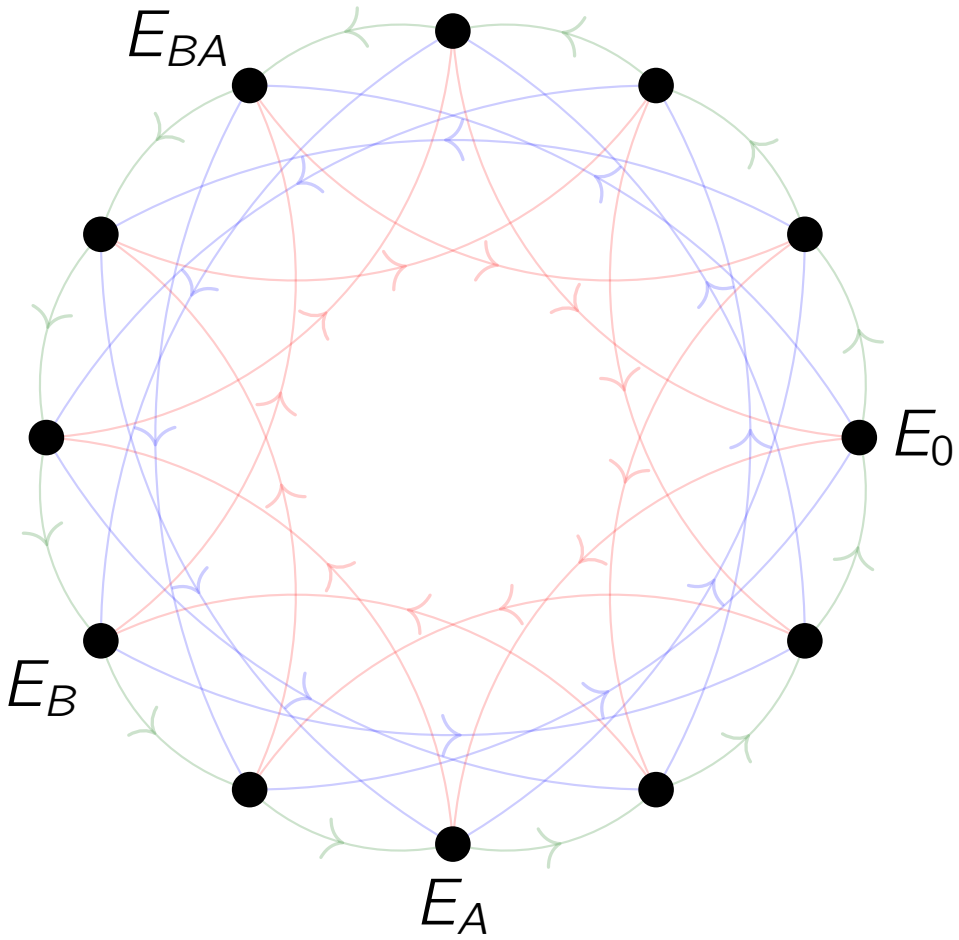
Consider a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$

Alice

$\rho_A = (2, 1, -1)$

$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$



Bob

$\rho_B = (-2, 0, 1)$

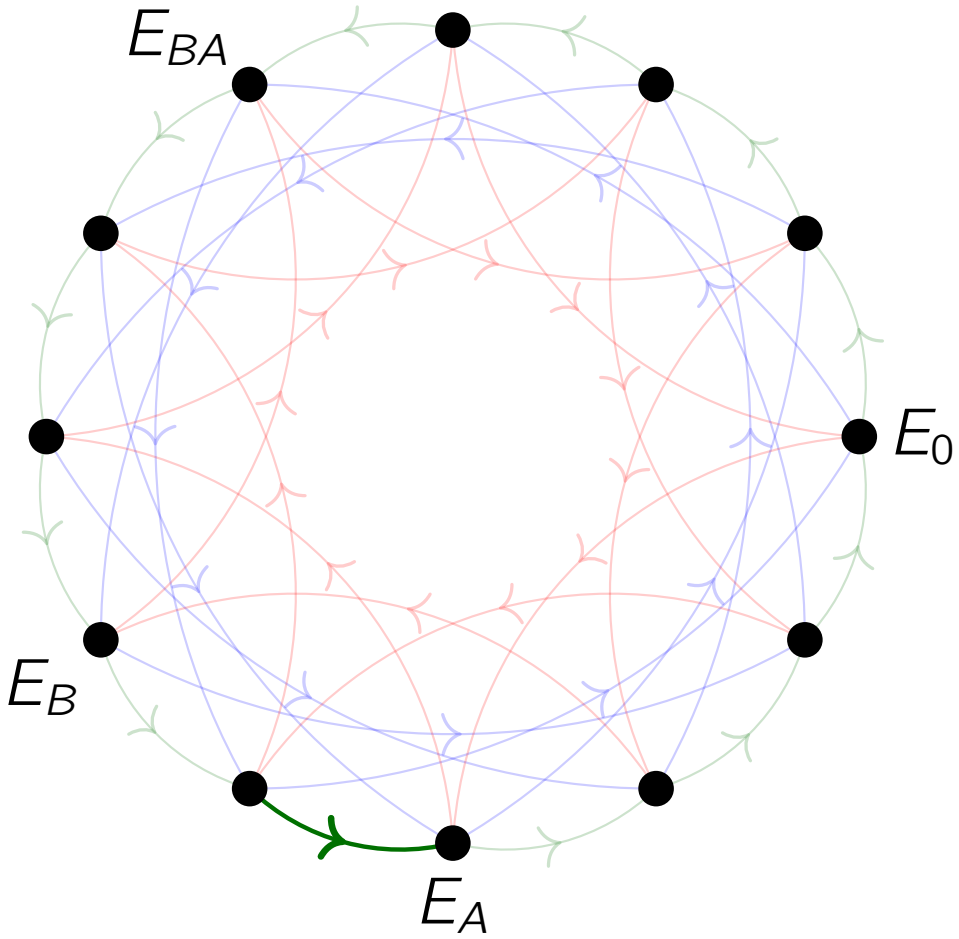
$\mathfrak{a} = \mathfrak{l}_1^{-2} \mathfrak{l}_3^1$

ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

Consider a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$



Alice

$\rho_A = (2, 1, -1)$

$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$

Bob

$\rho_B = (-2, 0, 1)$

$\mathfrak{a} = \mathfrak{l}_1^{-2} \mathfrak{l}_3^1$

ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

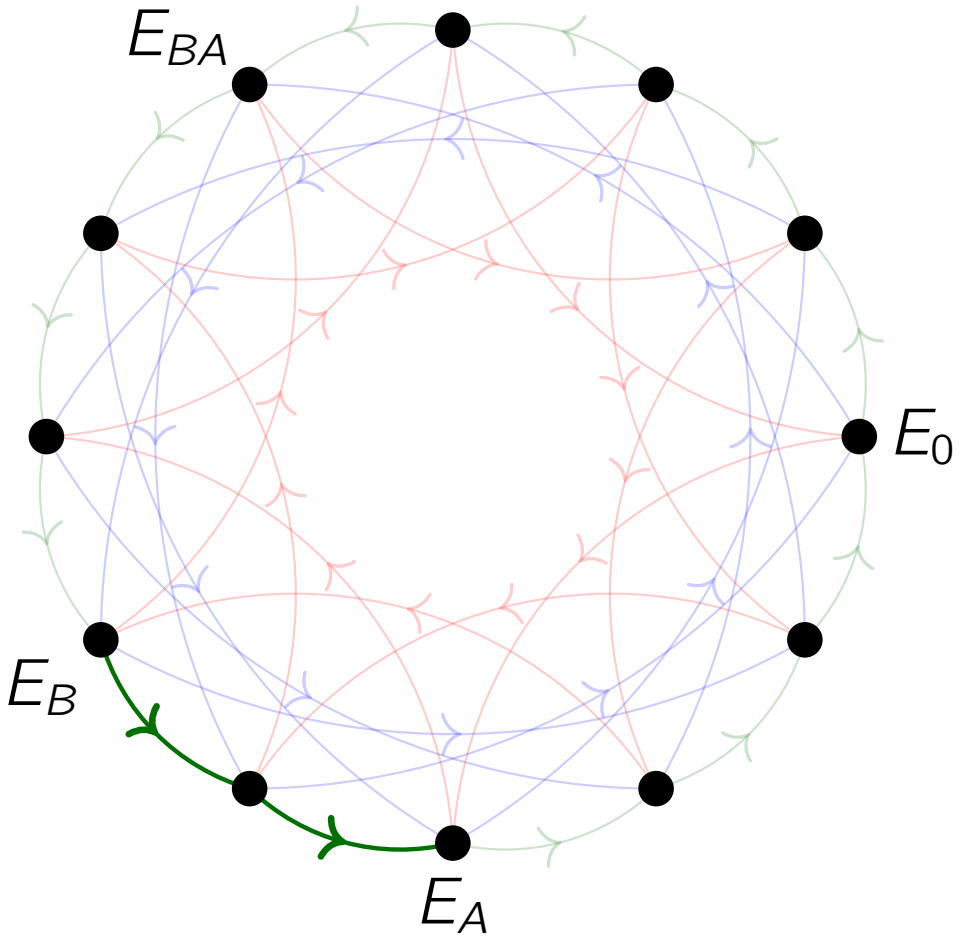
Consider a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$

Alice

$\rho_A = (2, 1, -1)$

$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$



Bob

$\rho_B = (-2, 0, 1)$

$\mathfrak{a} = \mathfrak{l}_1^{-2} \mathfrak{l}_3^1$

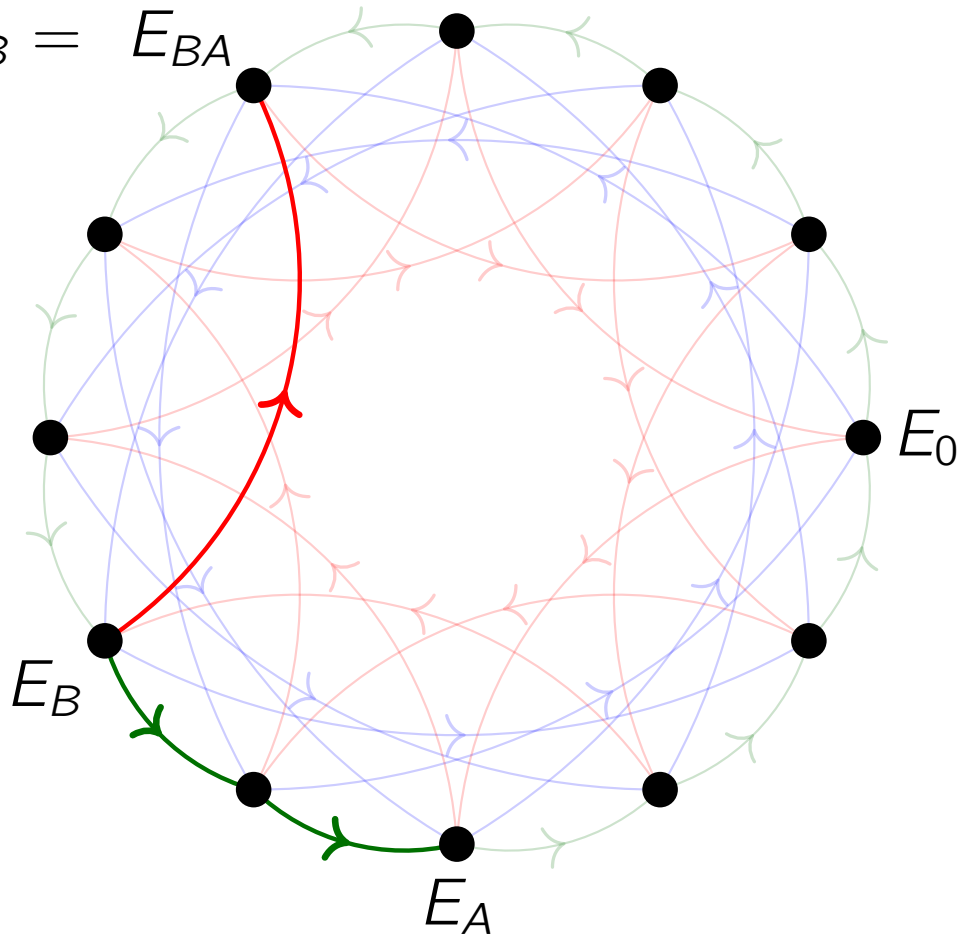
ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

Consider a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$E_{AB} = E_{BA}$

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$



Alice

$\rho_A = (2, 1, -1)$

$\mathfrak{a} = \mathfrak{l}_1^2\mathfrak{l}_2^1\mathfrak{l}_3^{-1}$

Bob

$\rho_B = (-2, 0, 1)$

$\mathfrak{a} = \mathfrak{l}_1^{-2}\mathfrak{l}_3^1$

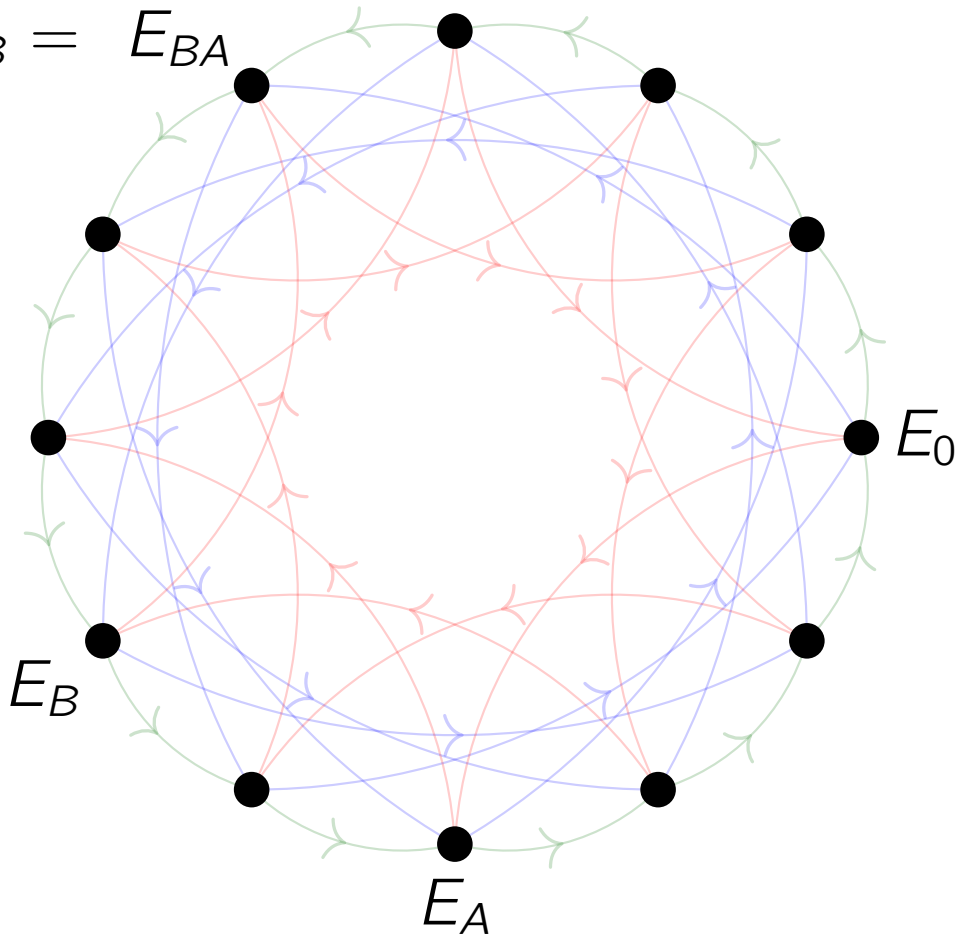
ORDINARY PROTOCOL - COUVEIGNES & ROSTOVTSEV-STOLBUNOV, 2006

Fix a large enough finite field $\mathbb{F}_q$ of large characteristic p and an ordinary elliptic curve $E_0/\mathbb{F}_q$ such that its Frobenius discriminant $D_\pi = t^2 - 4q$ contains a large enough prime factor.

Consider a set of primes $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ such that $\left(\frac{D_\pi}{\ell_i}\right) = 1$.

$E_{AB} = E_{BA}$

$\mathcal{L} = \{\mathfrak{l}_1, \mathfrak{l}_2, \mathfrak{l}_3\}$



Alice

$\rho_A = (2, 1, -1)$

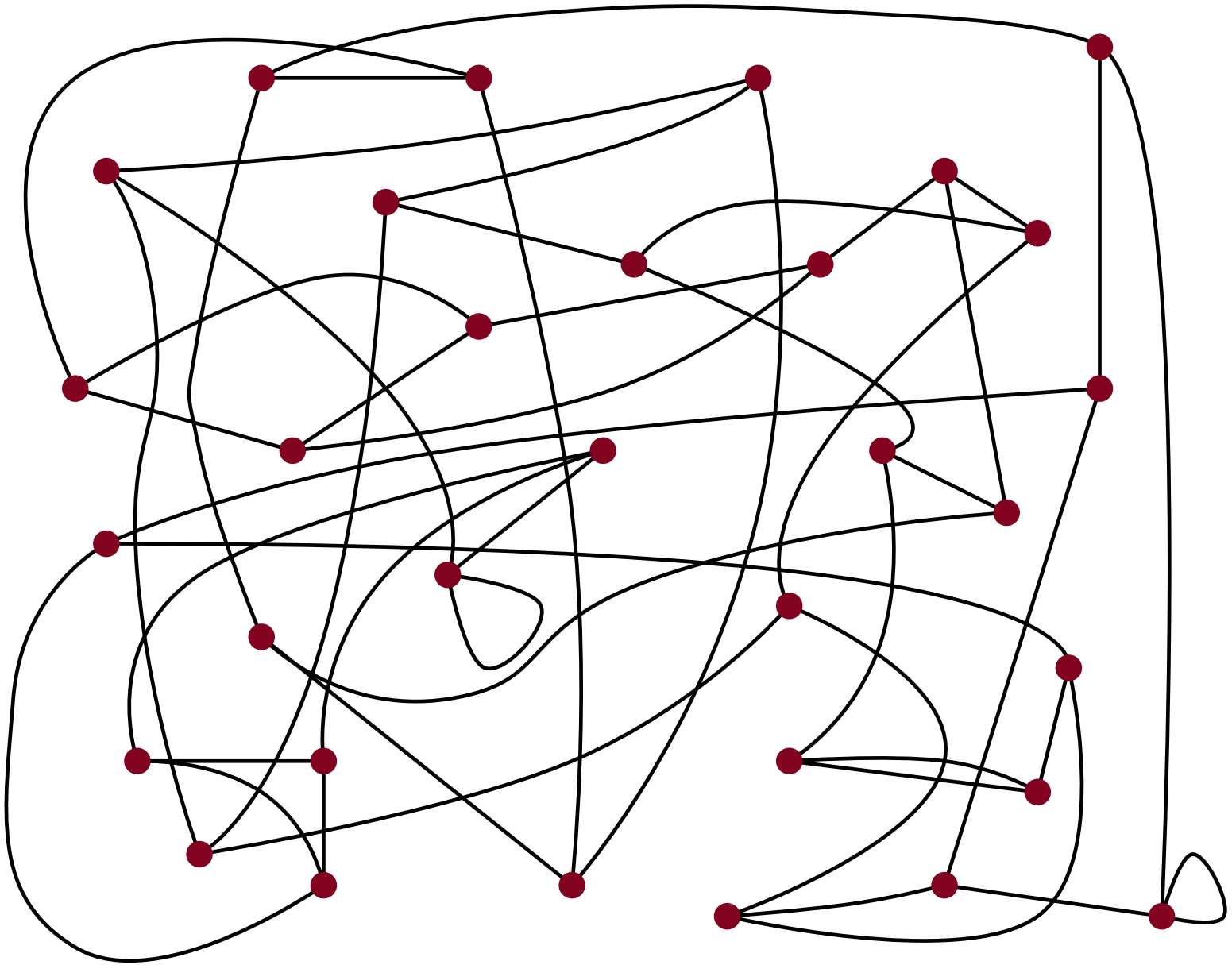
$\mathfrak{a} = \mathfrak{l}_1^2 \mathfrak{l}_2^1 \mathfrak{l}_3^{-1}$

Bob

$\rho_B = (-2, 0, 1)$

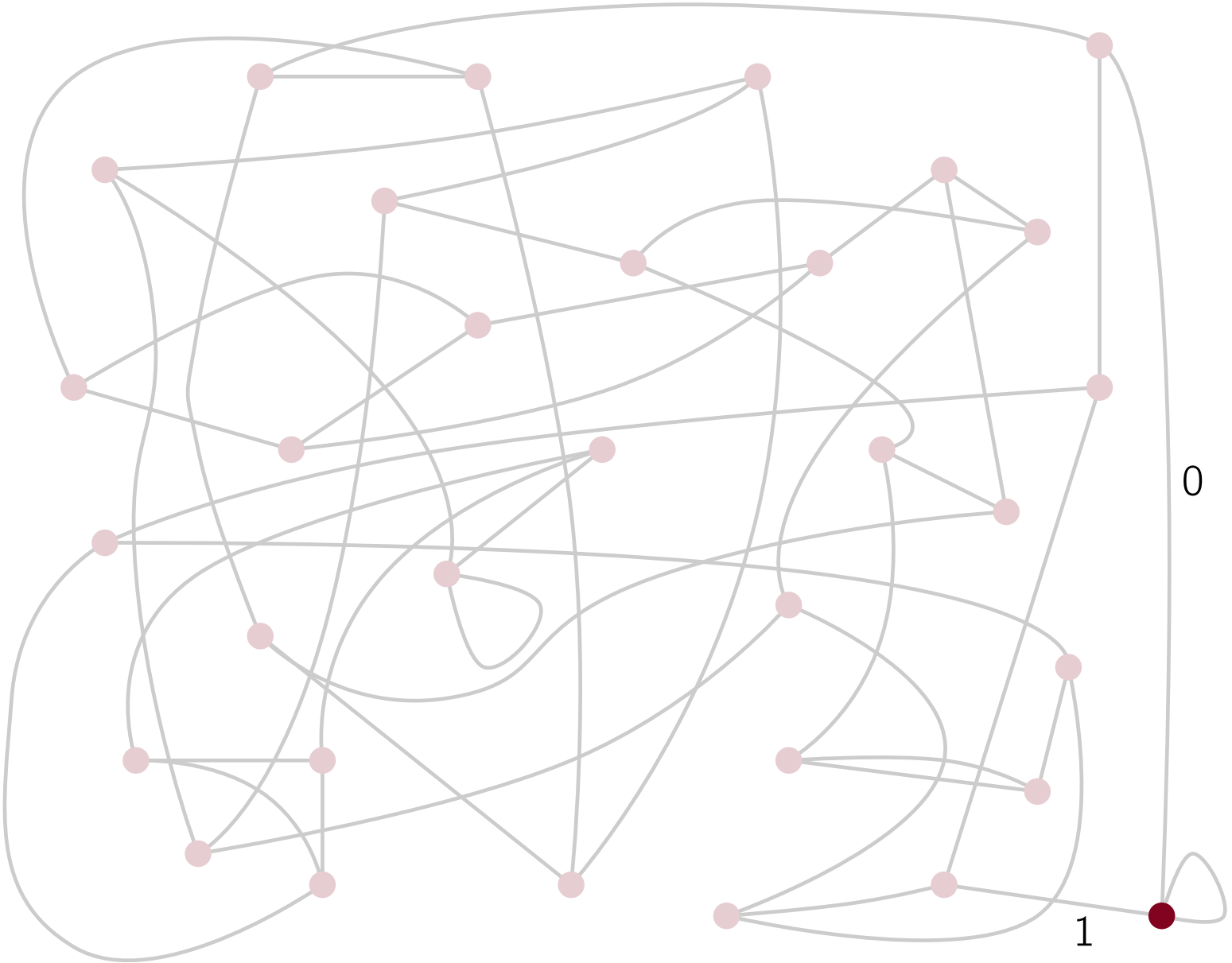
$\mathfrak{a} = \mathfrak{l}_1^{-2} \mathfrak{l}_3^1$

HASH FUNCTION - CHARLES, GOREN, LAUTER, 2006

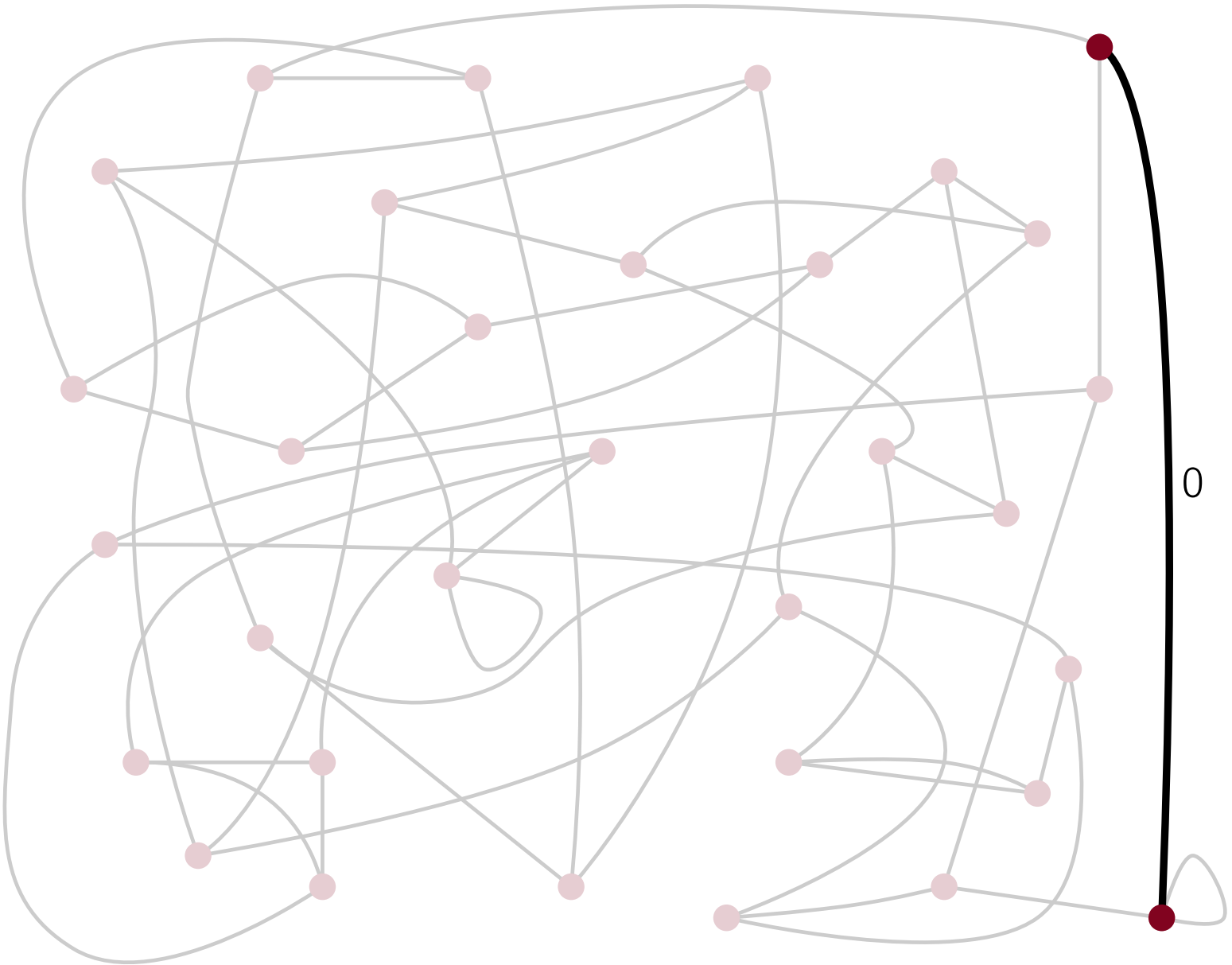


HASH FUNCTION - CHARLES, GOREN, LAUTER, 2006

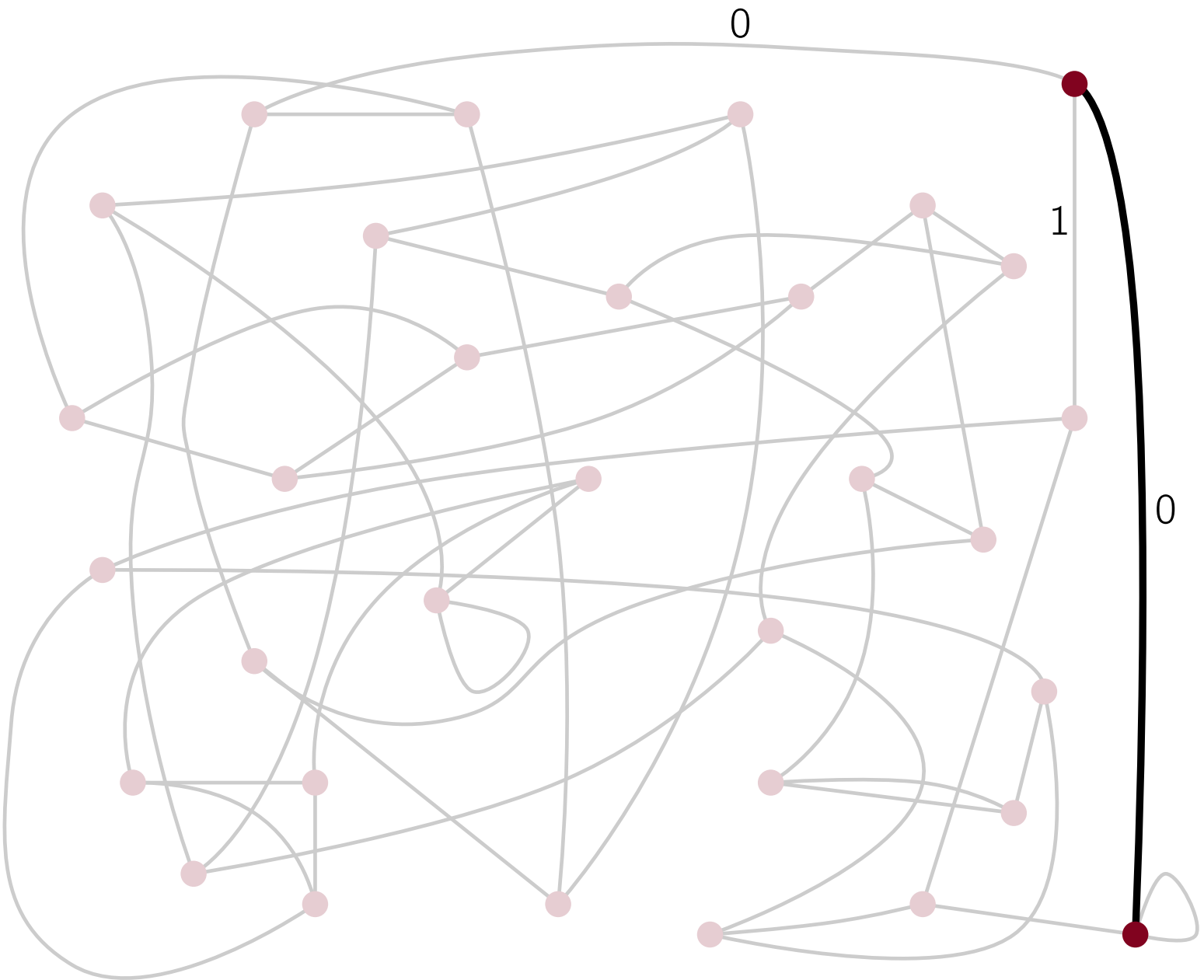
HASH FUNCTION - CHARLES, GOREN, LAUTER, 2006



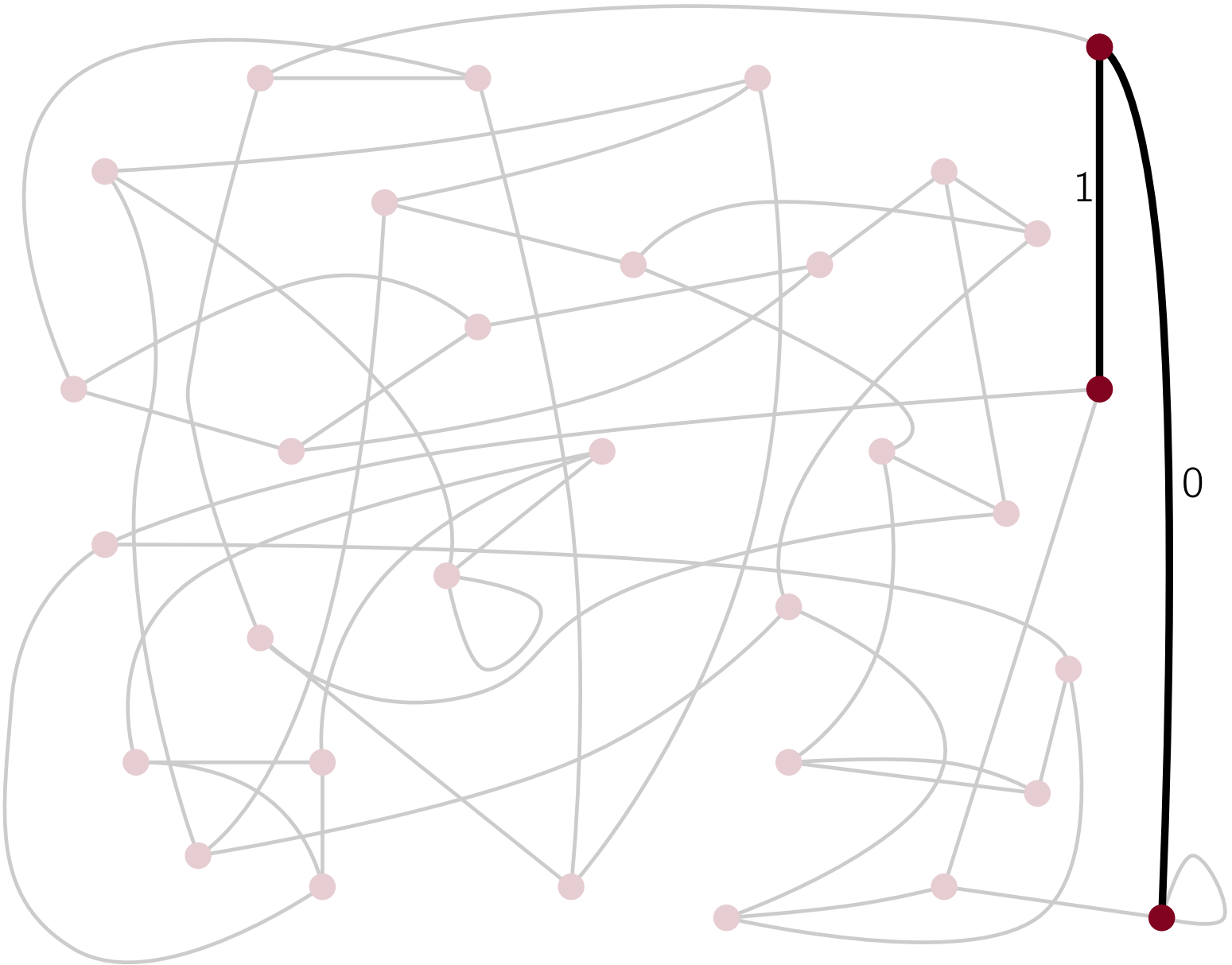
HASH FUNCTION - CHARLES, GOREN, LAUTER, 2006



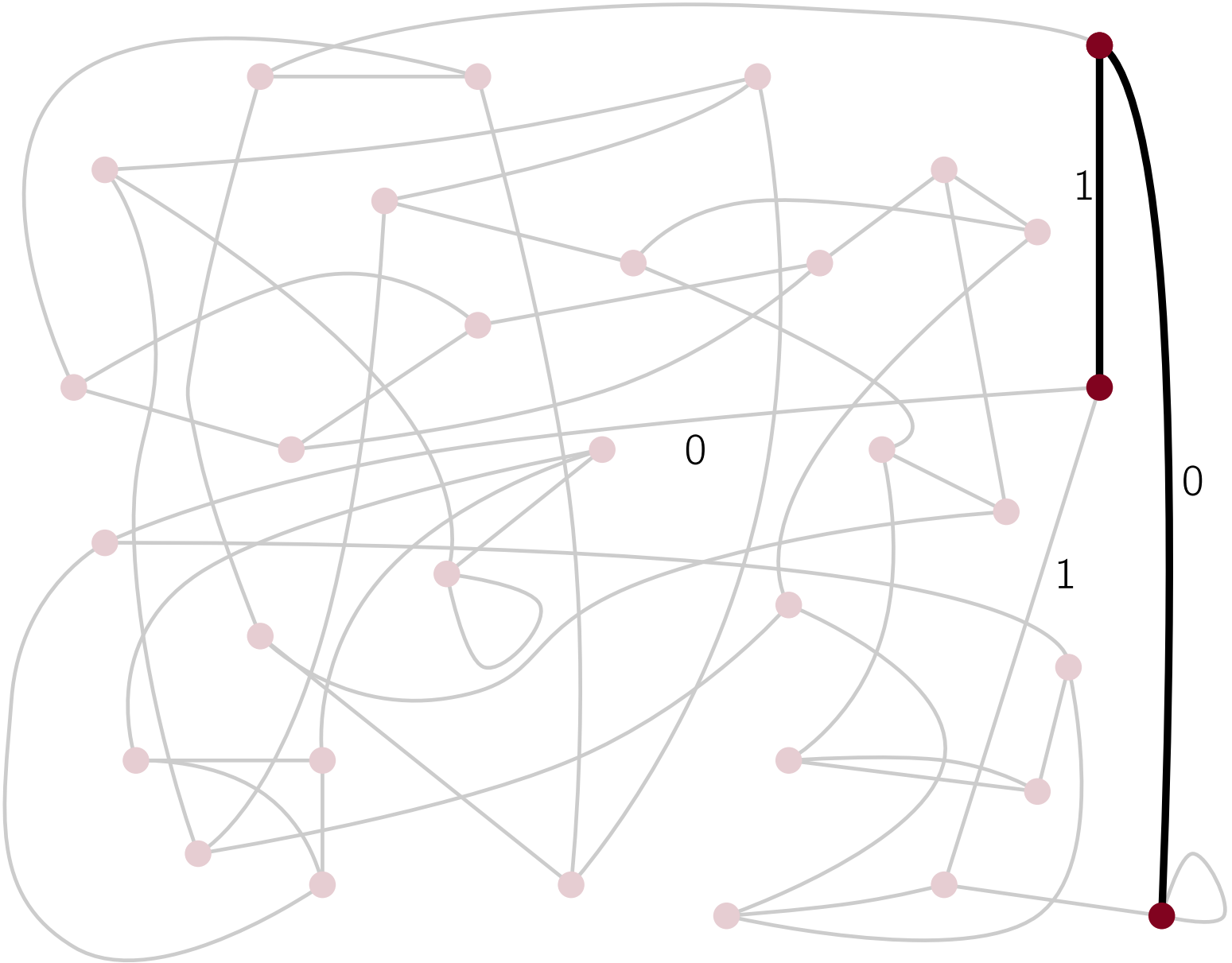
HASH FUNCTION - CHARLES, GOREN, LAUTER, 2006



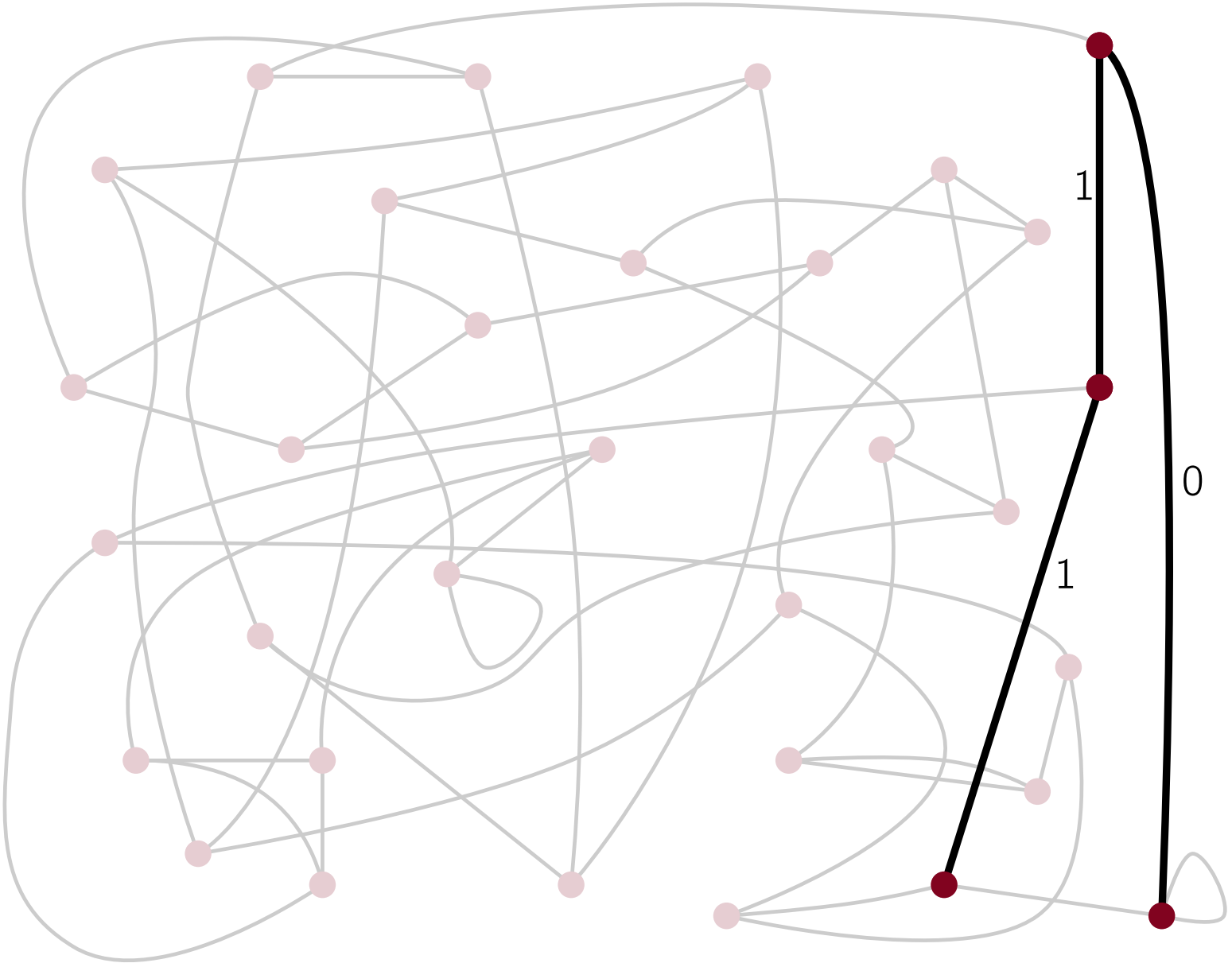
HASH FUNCTION - CHARLES, GOREN, LAUTER, 2006



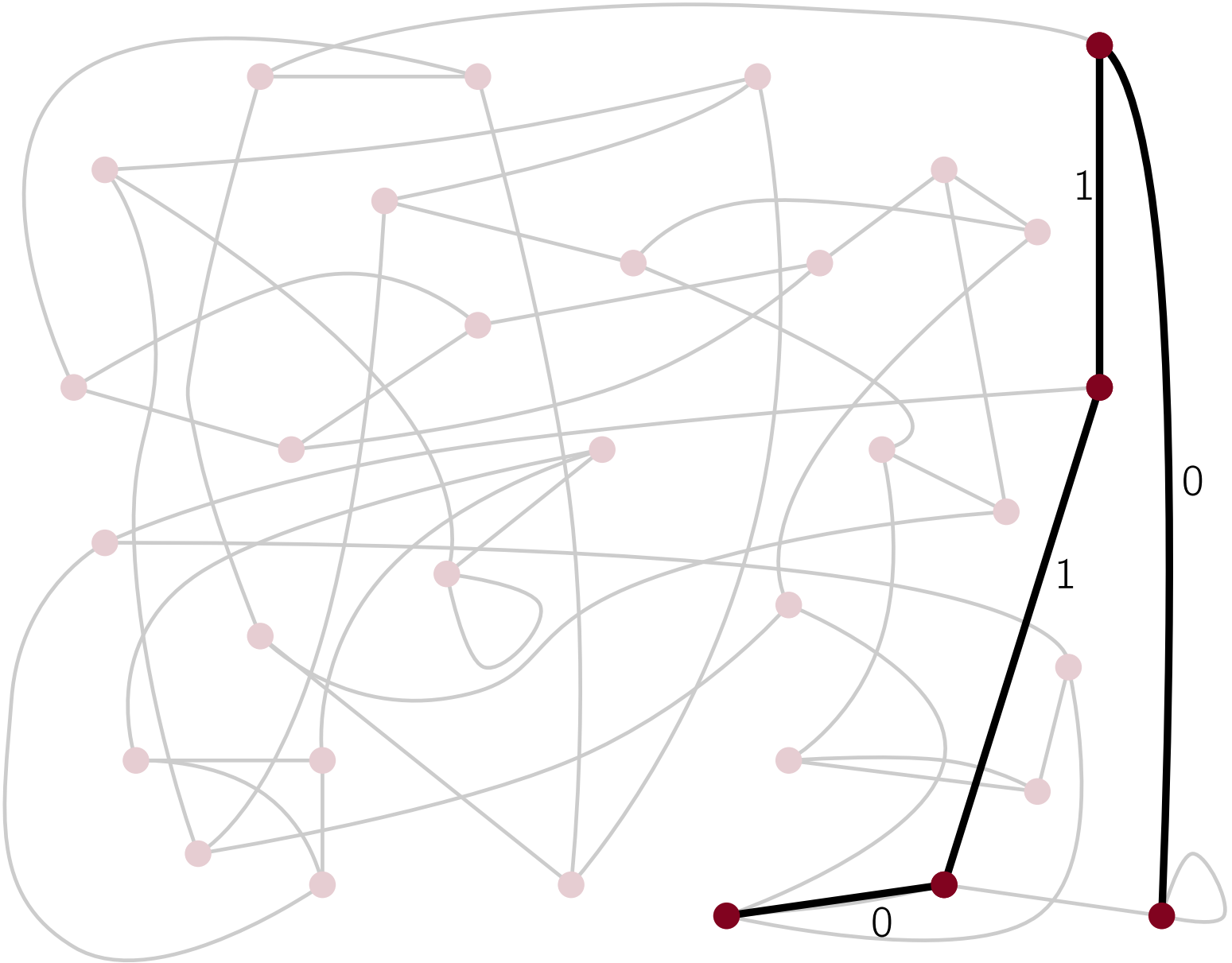
HASH FUNCTION - CHARLES, GOREN, LAUTER, 2006



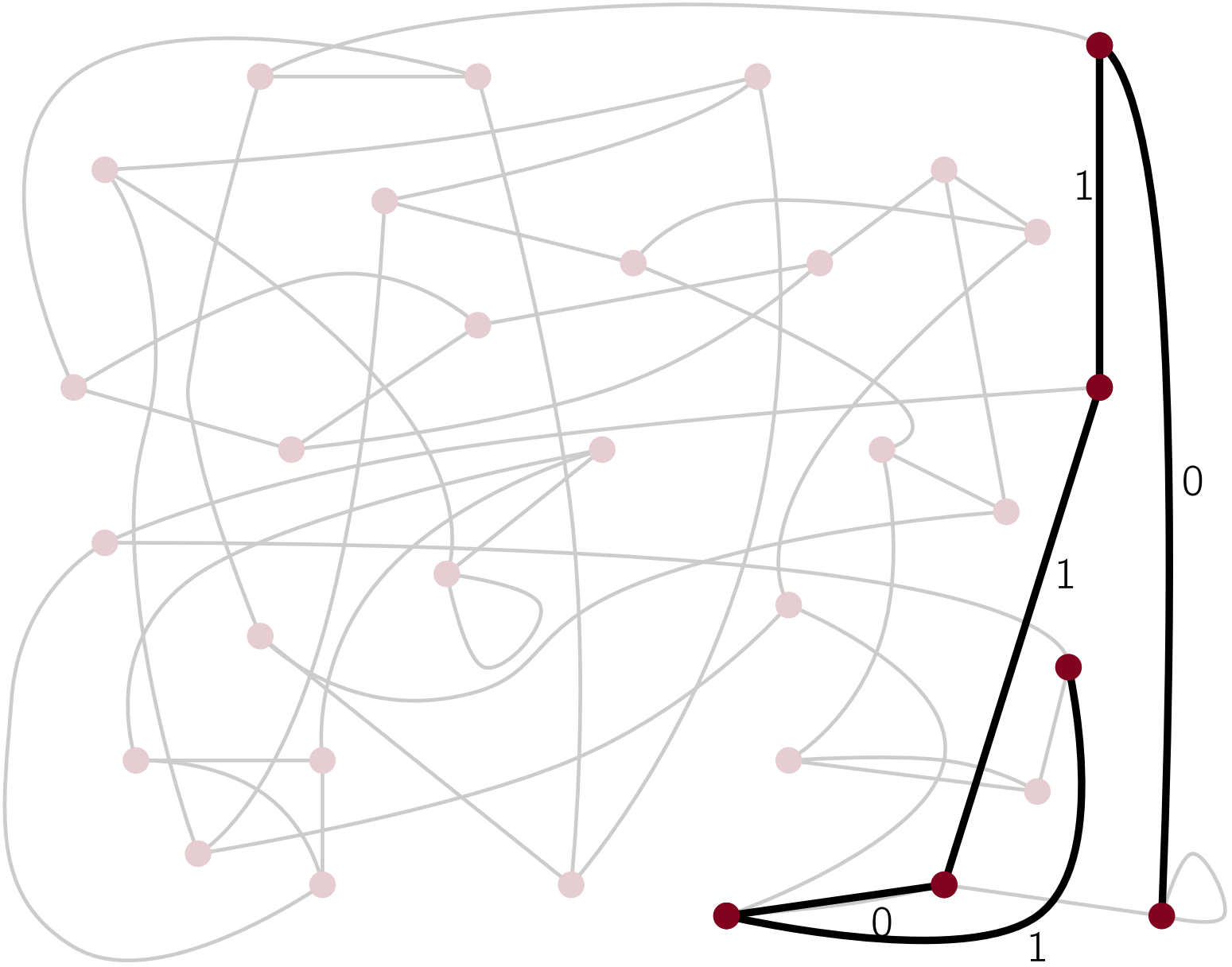
HASH FUNCTION - CHARLES, GOREN, LAUTER, 2006



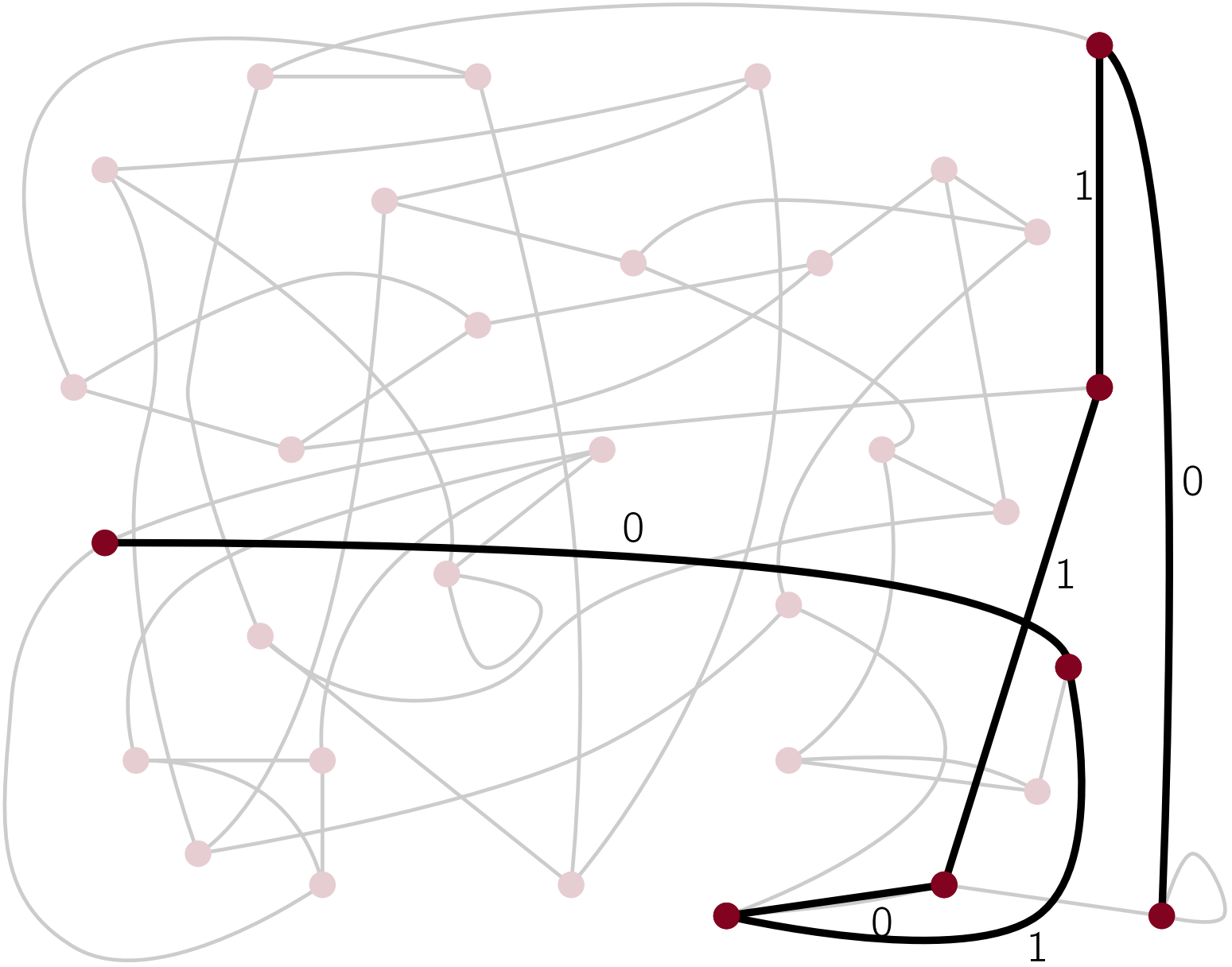
HASH FUNCTION - CHARLES, GOREN, LAUTER, 2006



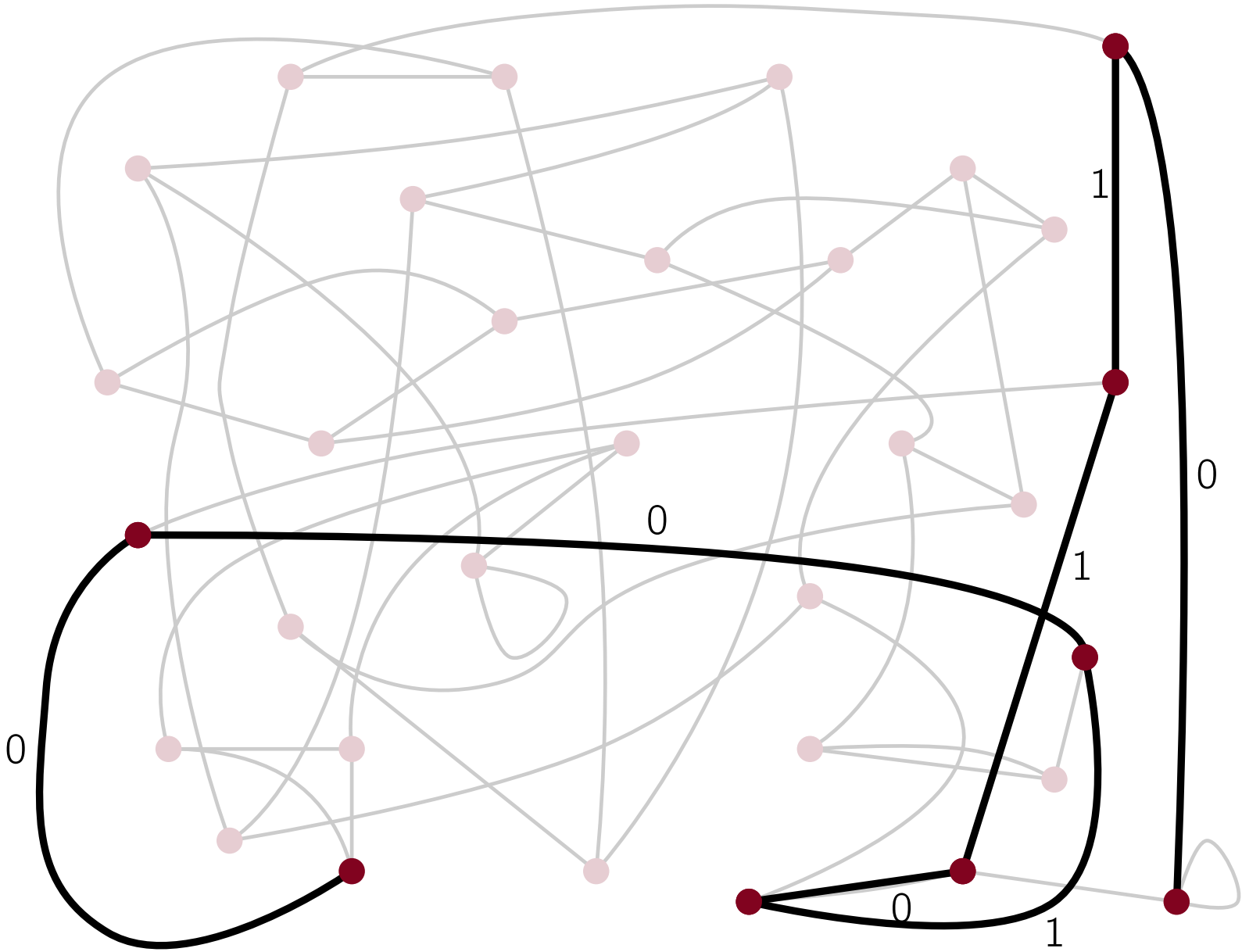
HASH FUNCTION - CHARLES, GOREN, LAUTER, 2006



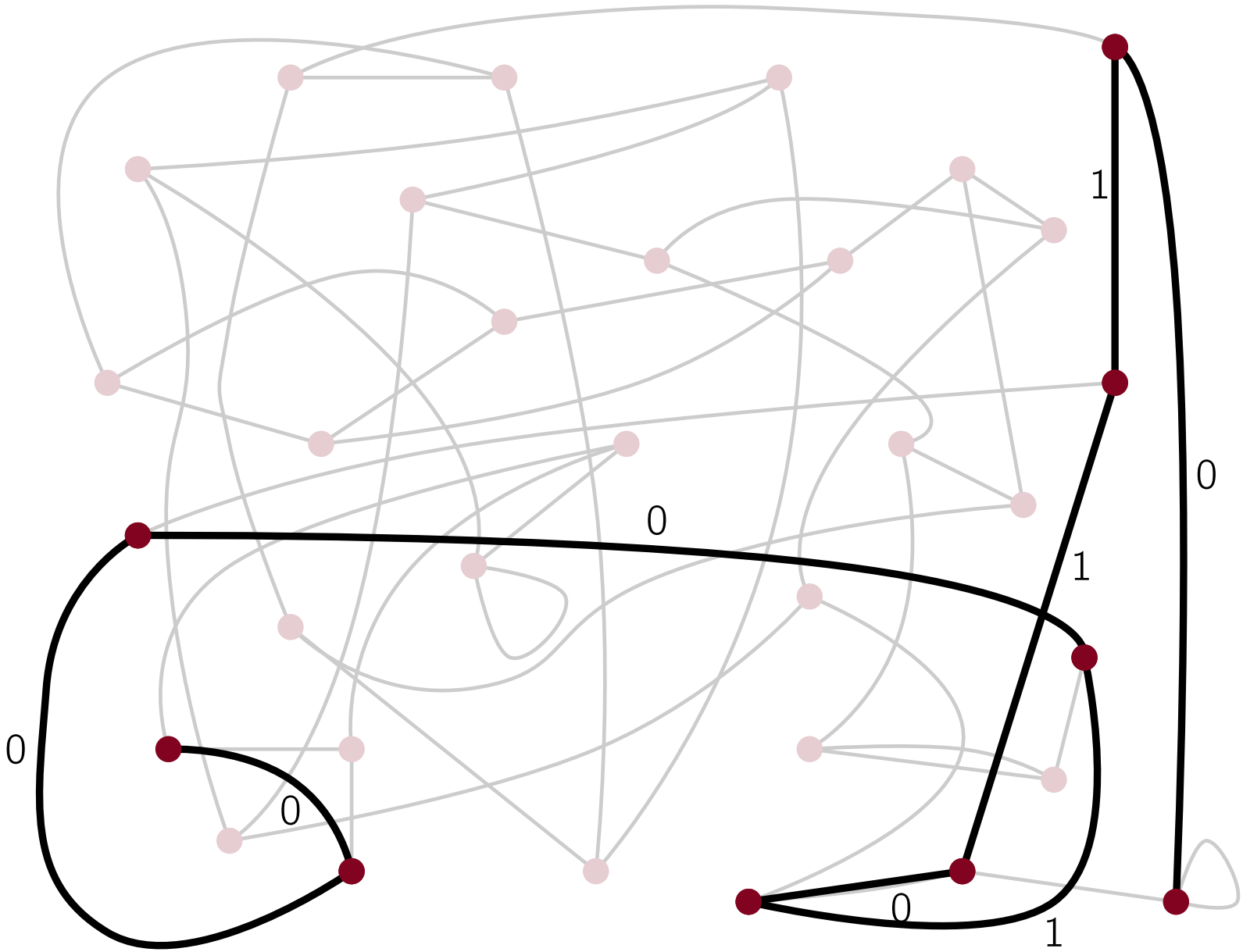
HASH FUNCTION - CHARLES, GOREN, LAUTER, 2006



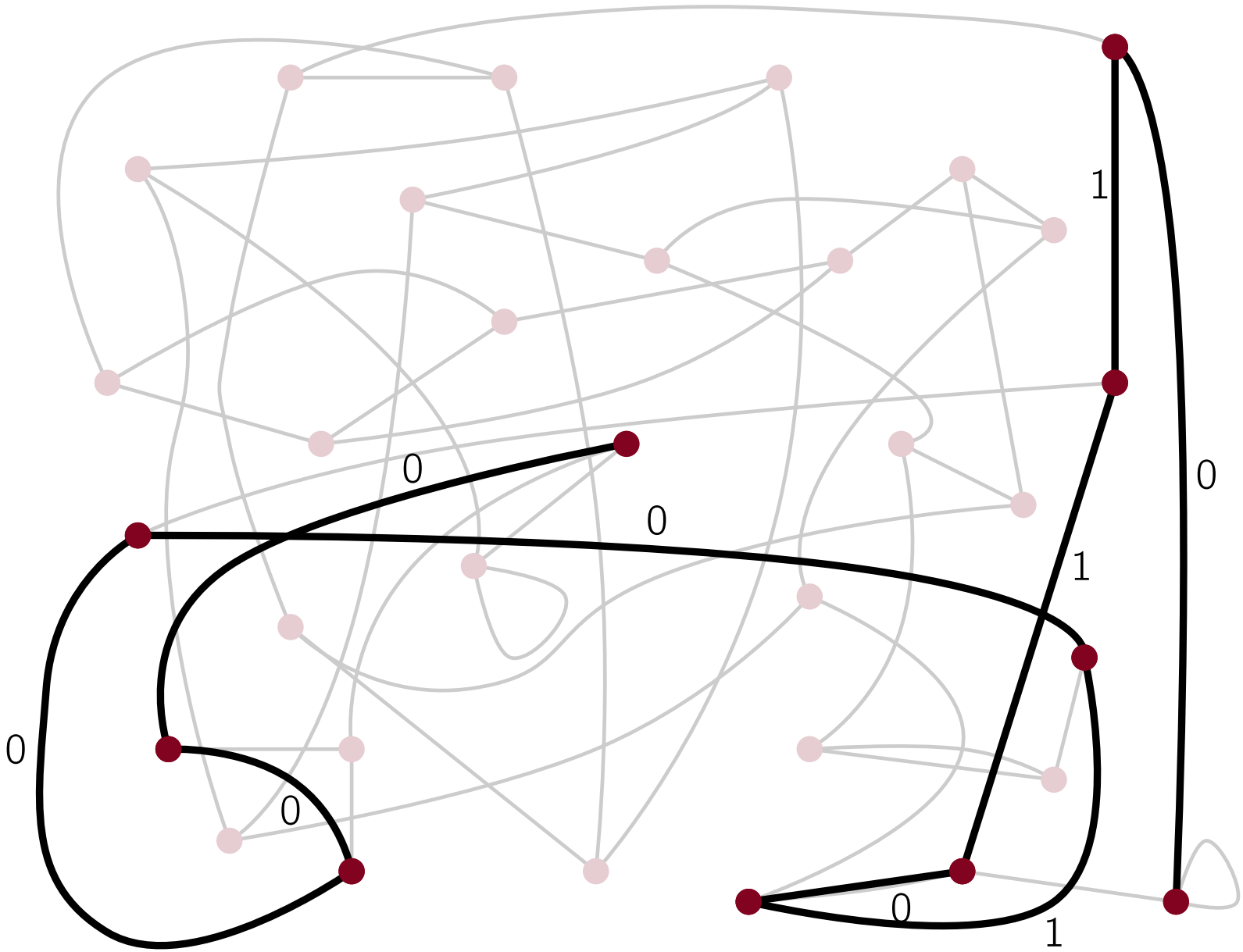
HASH FUNCTION - CHARLES, GOREN, LAUTER, 2006



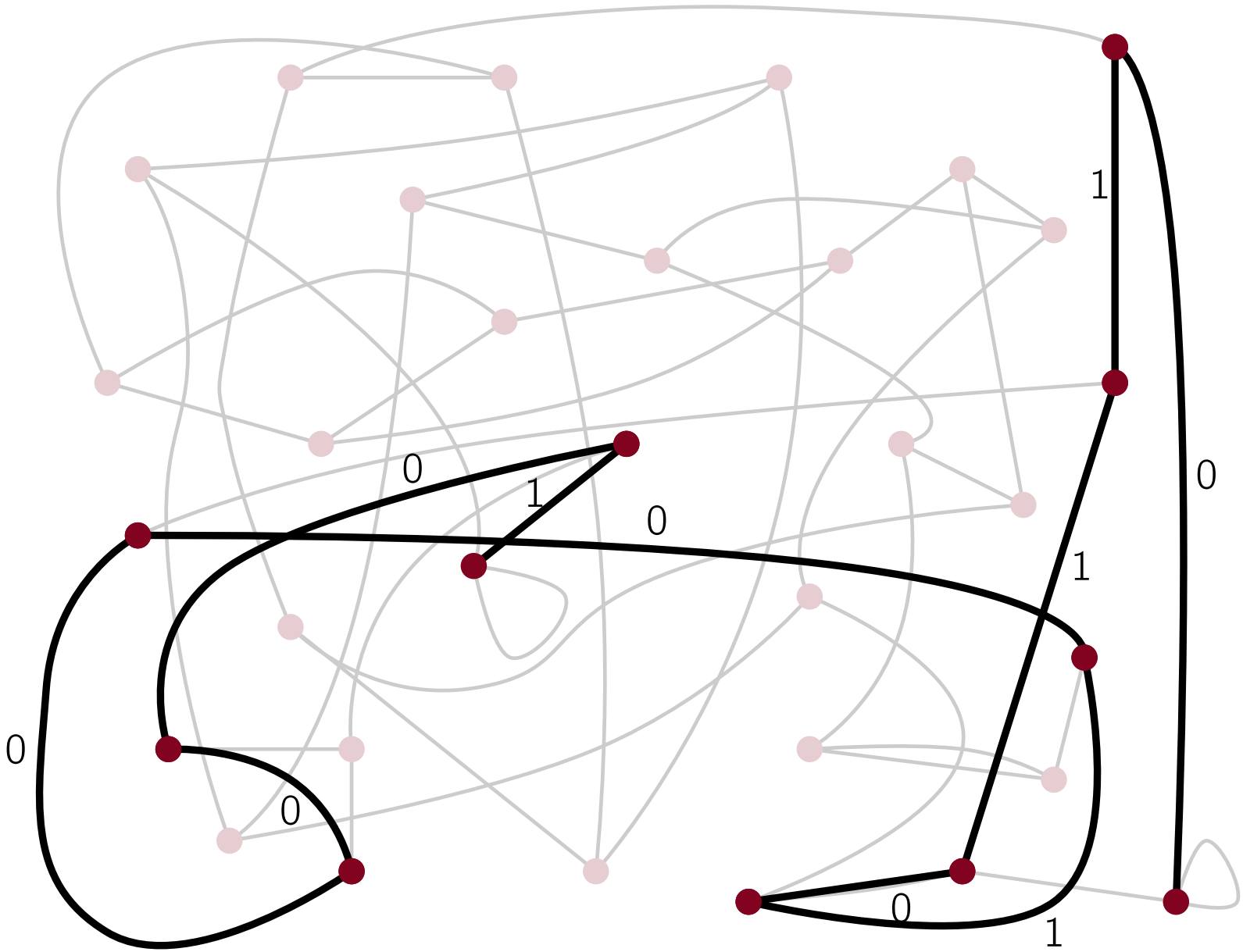
HASH FUNCTION - CHARLES, GOREN, LAUTER, 2006



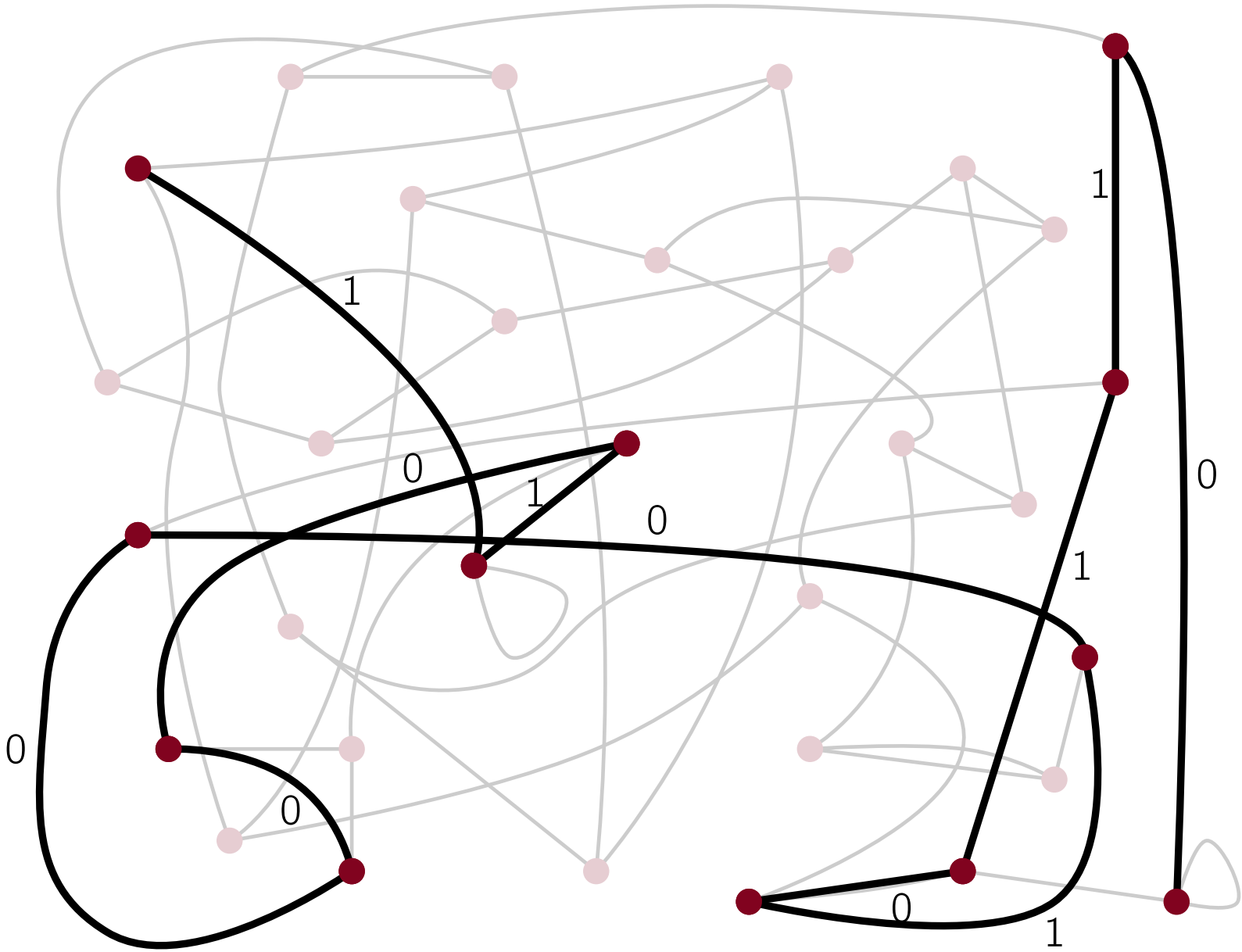
HASH FUNCTION - CHARLES, GOREN, LAUTER, 2006



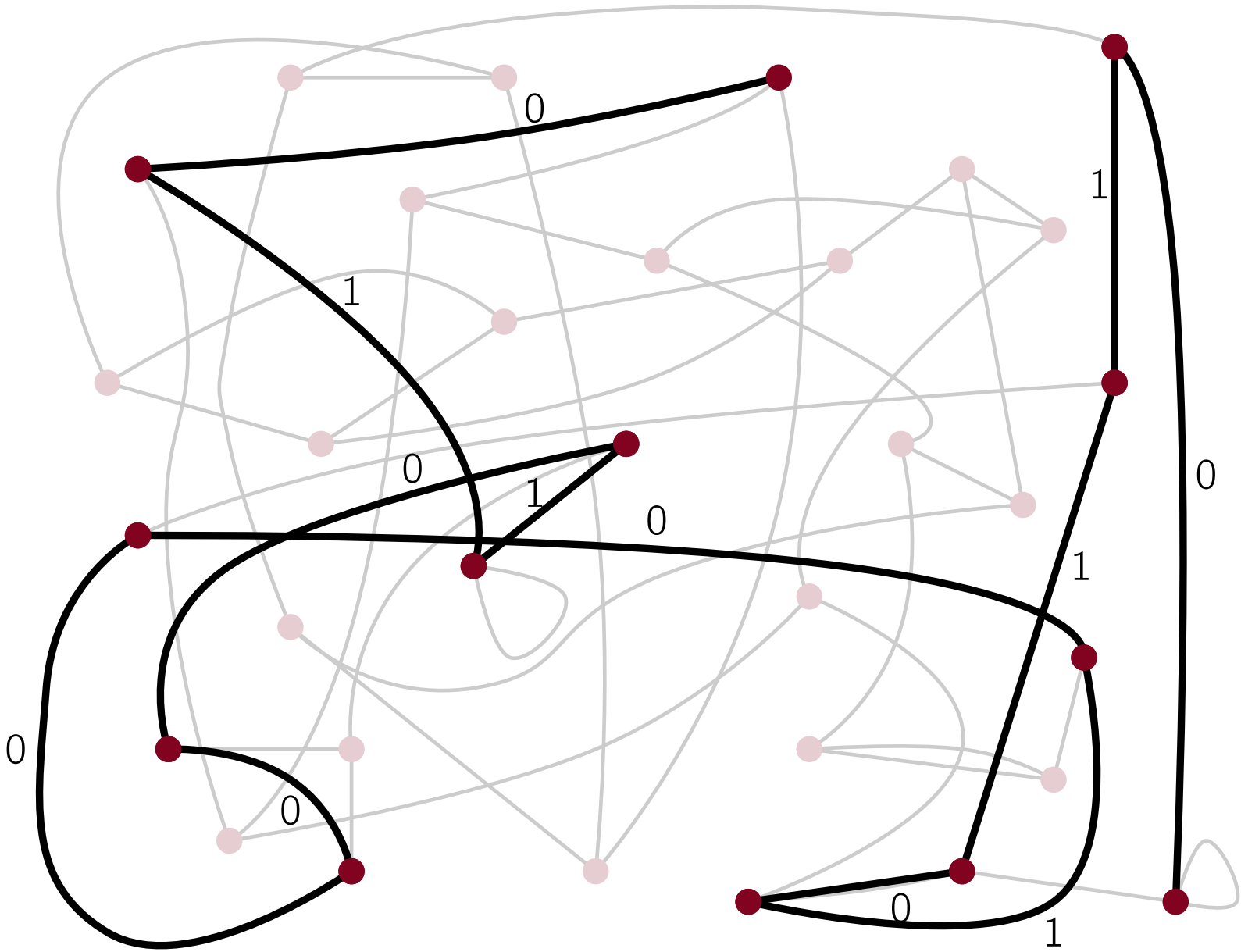
HASH FUNCTION - CHARLES, GOREN, LAUTER, 2006



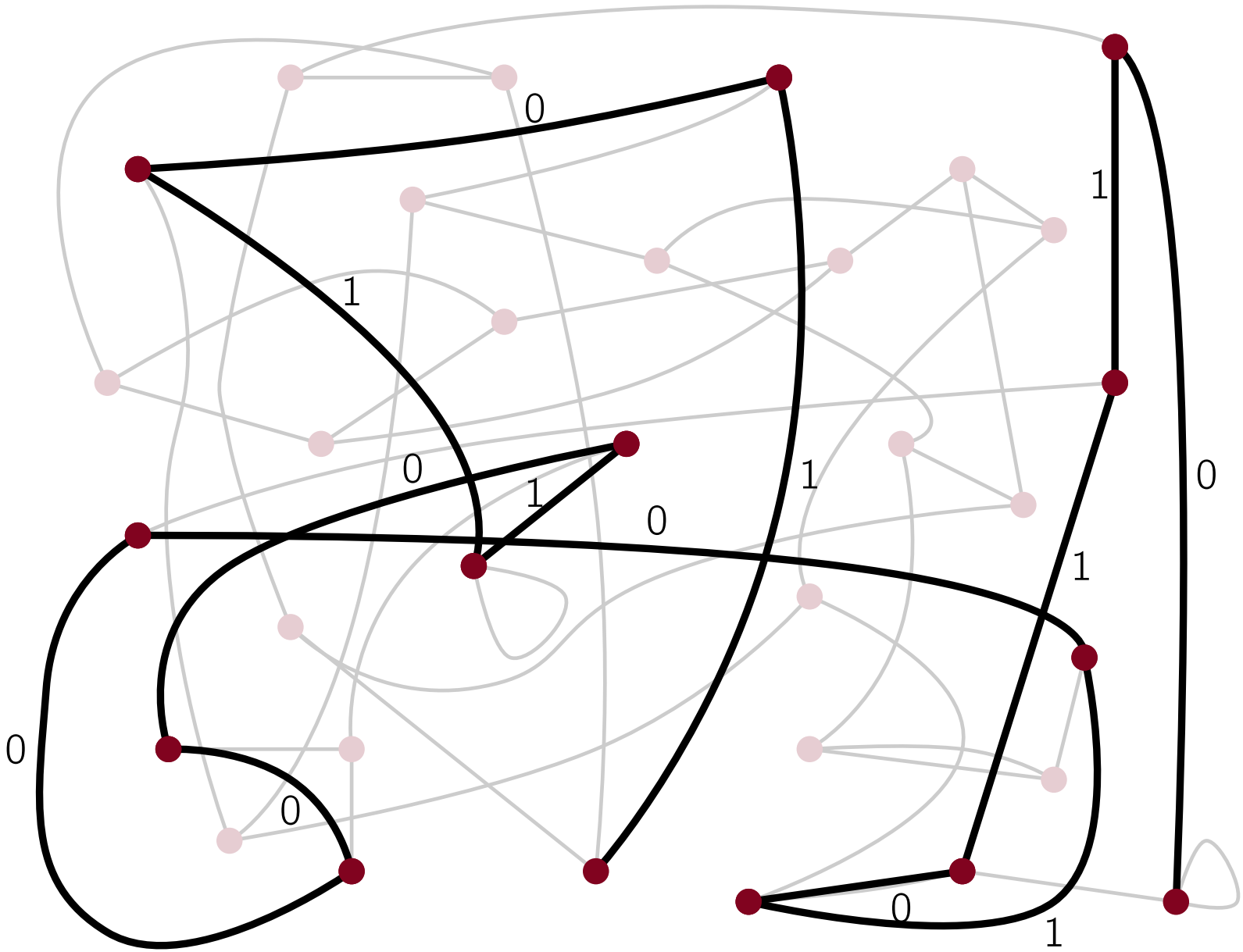
HASH FUNCTION - CHARLES, GOREN, LAUTER, 2006



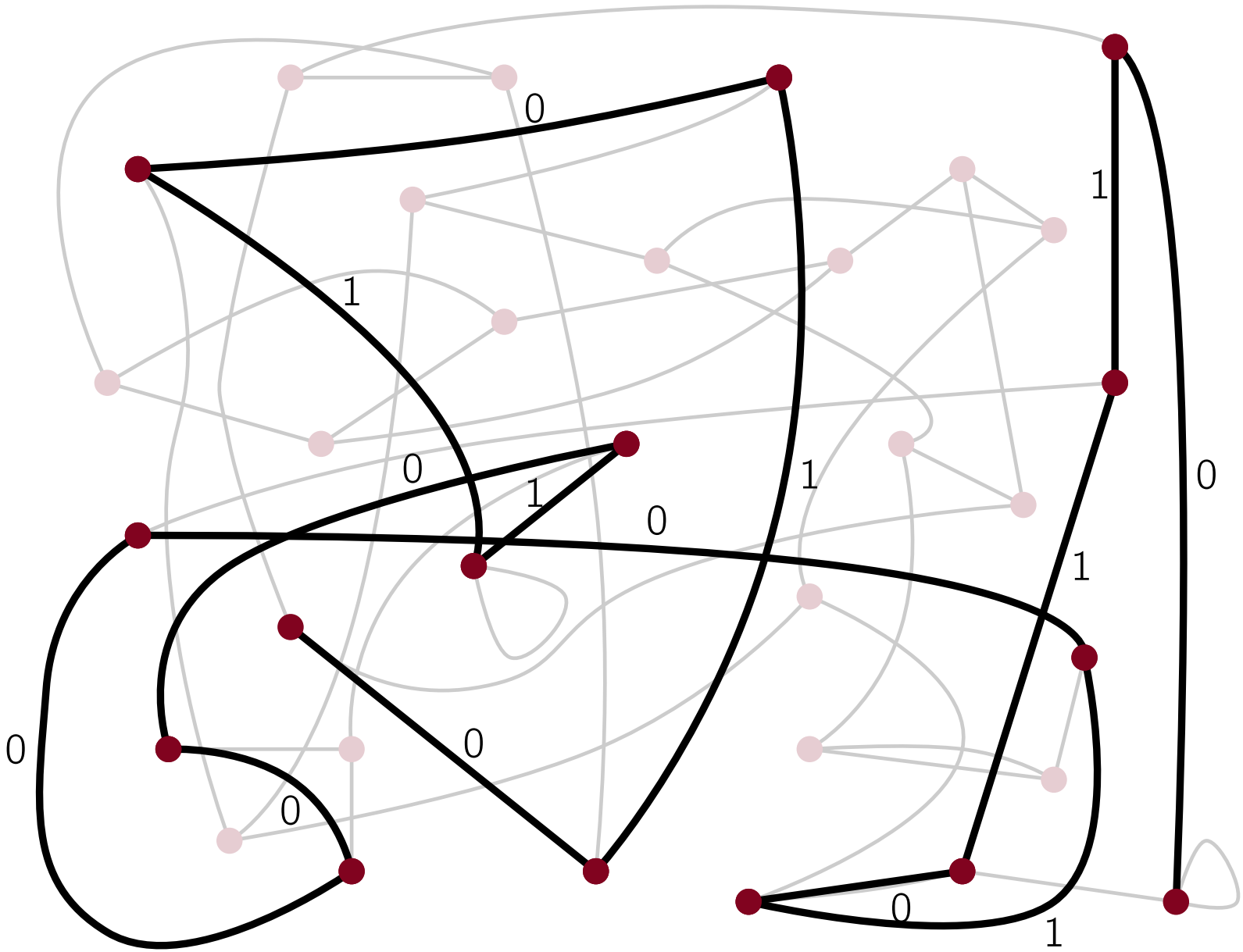
HASH FUNCTION - CHARLES, GOREN, LAUTER, 2006



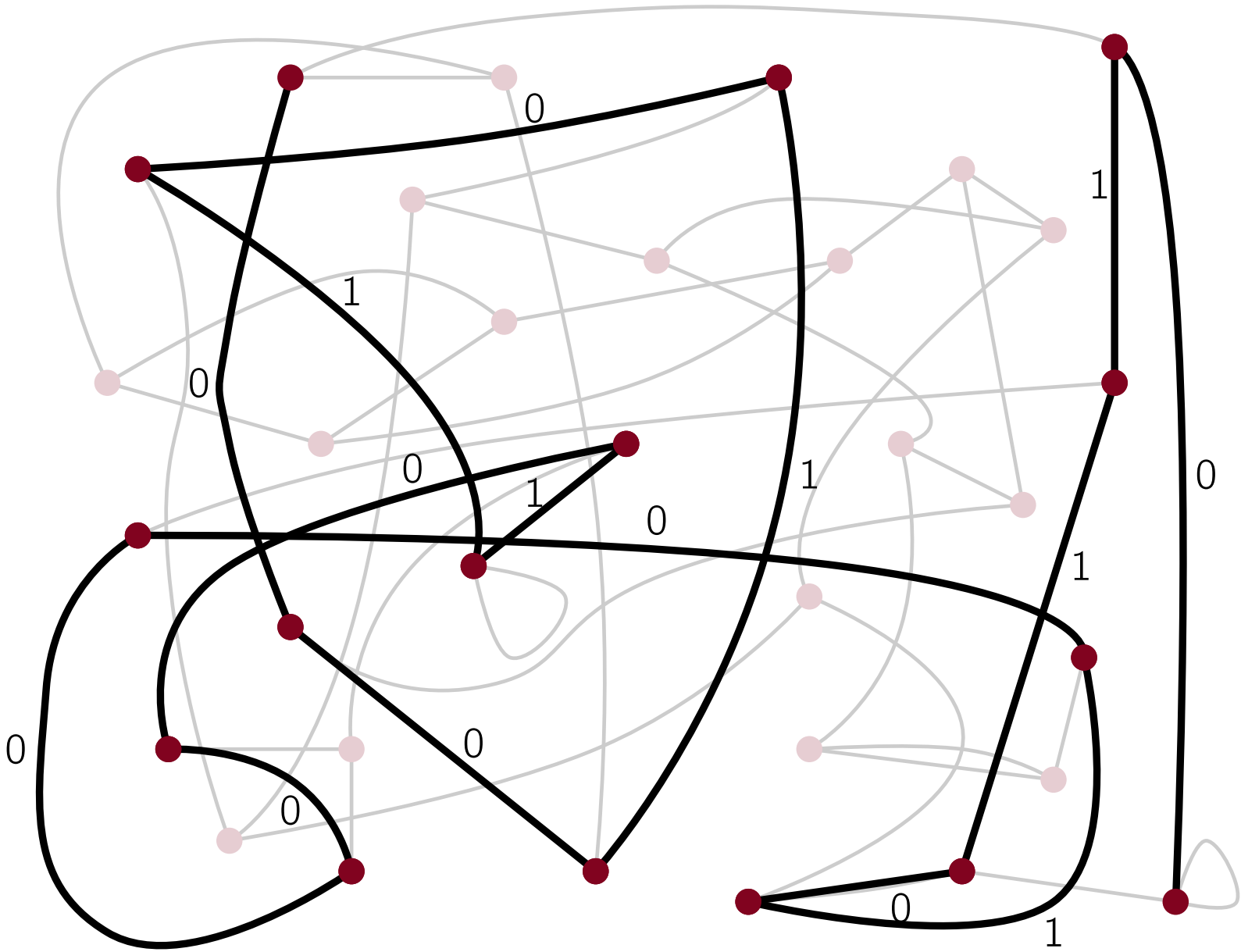
HASH FUNCTION - CHARLES, GOREN, LAUTER, 2006



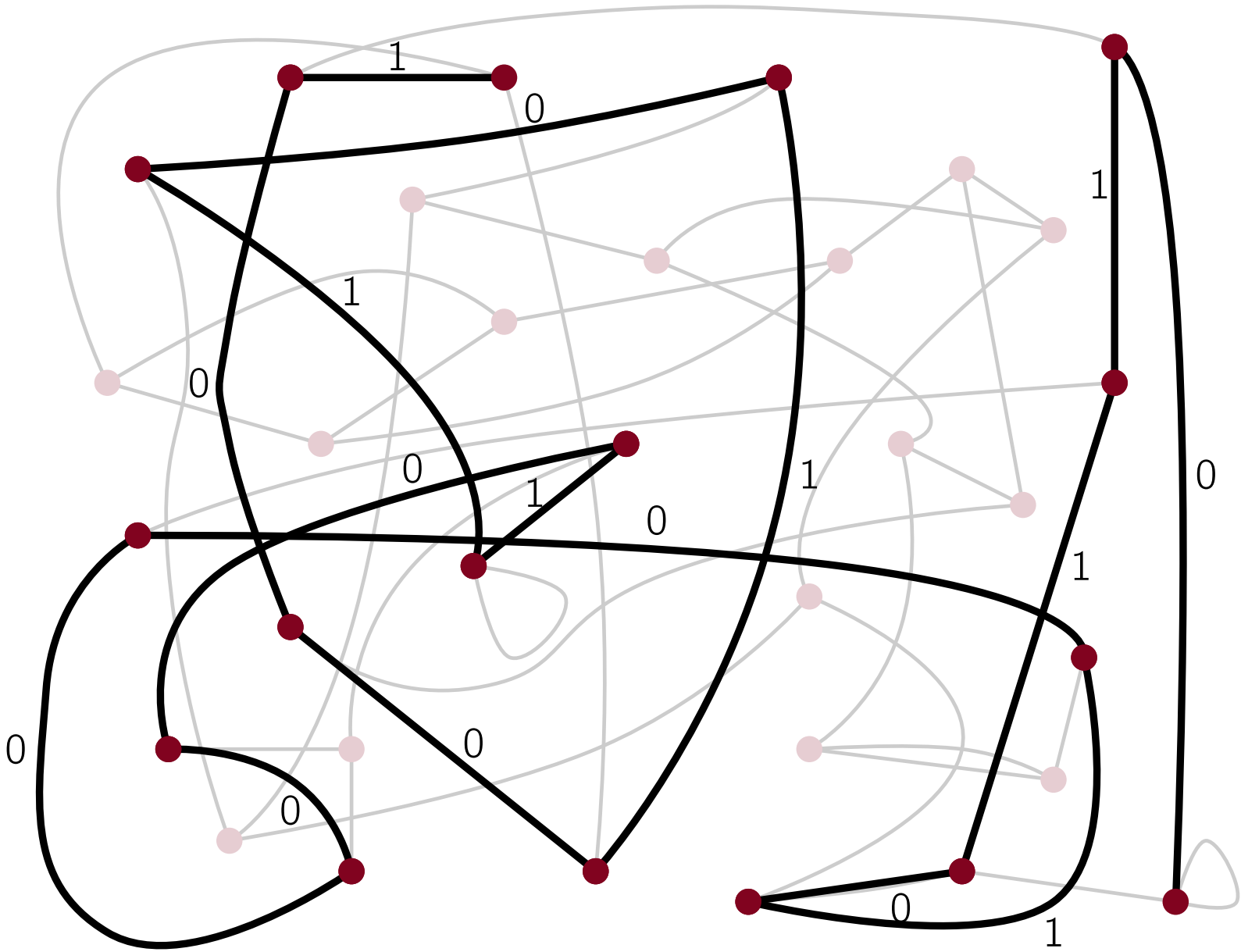
HASH FUNCTION - CHARLES, GOREN, LAUTER, 2006



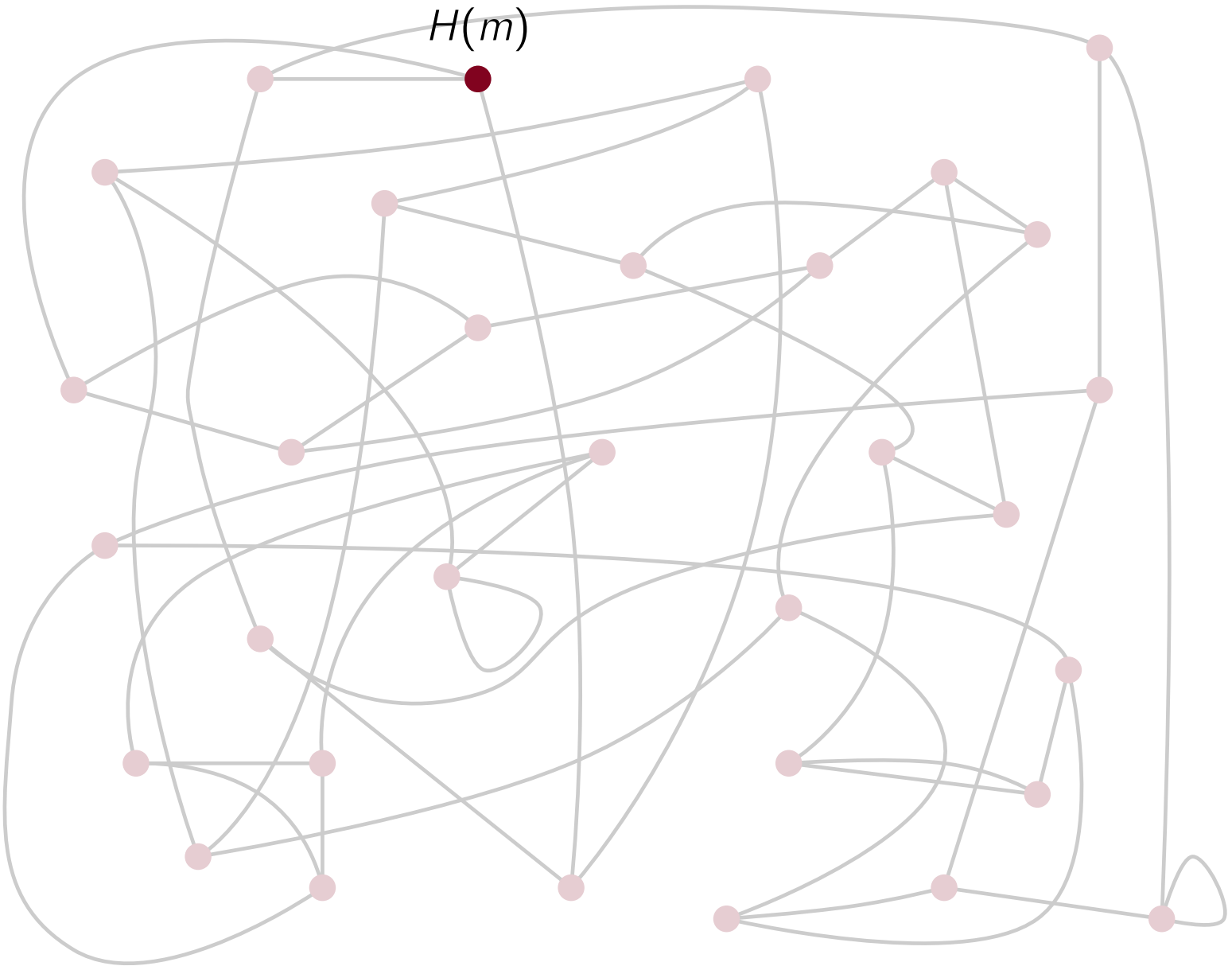
HASH FUNCTION - CHARLES, GOREN, LAUTER, 2006



HASH FUNCTION - CHARLES, GOREN, LAUTER, 2006

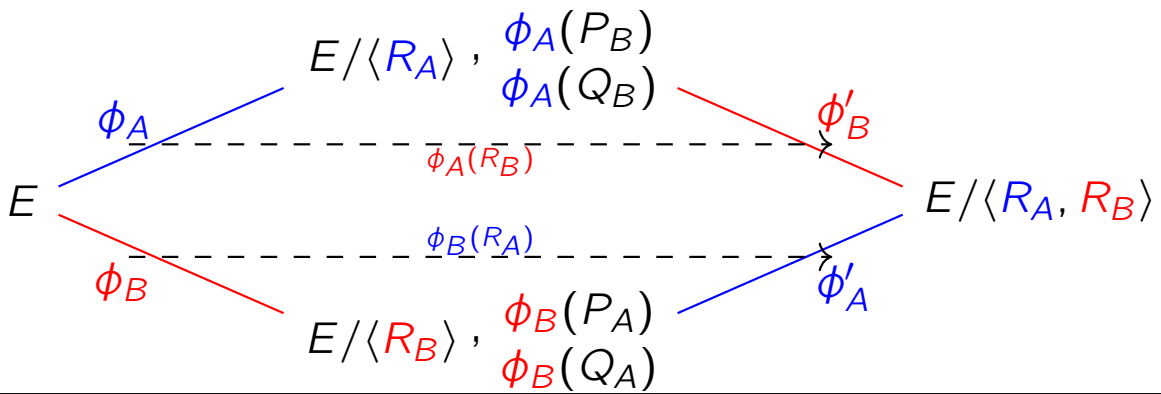


HASH FUNCTION - CHARLES, GOREN, LAUTER, 2006



Supersingular isogeny Diffie-Hellman

- Fix two small primes ℓ_A and ℓ_B;
- Choose a prime p such that $p+1 = \ell_A^a \ell_B^b f$ for a small correction term f;
- Pick a supersingular elliptic curve $E/\mathbb{F}_{p^2}$: $E\left(\mathbb{F}_{p^2}\right) \simeq \left(\frac{\mathbb{Z}}{(p+1)\mathbb{Z}}\right)^2$
- Alice consider $E\left[\ell_A^a\right] = \langle P_A, Q_A \rangle$ while Bob takes $E\left[\ell_B^b\right] = \langle P_B, Q_B \rangle$.
- **Secret Data:** $R_A = m_A P_A + n_A Q_A$ and $R_B = m_B P_B + n_B Q_B$.
- **Private Key:** isogenies $\phi_A : E \to E_A = E/\langle R_A \rangle$ and $\phi_B : E \to E_B = E/\langle R_B \rangle$.
- **Shared Data:** $E_A, \phi_A(P_B), \phi_A(Q_B)$ and $E_B, \phi_B(P_A), \phi_B(Q_A)$.
- **Shared Key:** $E/\langle R_A, R_B \rangle = E_B/\langle \phi_B(R_A) \rangle = E_A/\langle \phi_A(R_B) \rangle$.



CSIDH - CASTRYCK, LANGE, MARTINDALE, PANNY & RENES, 2018

It is an adaptation of the CouveignesâRostovtsevâStolbunov scheme to supersingular elliptic curves.

Commutative Supersingular isogeny Diffie-Hellman

- Fix a prime $p = 4 \cdot \ell_1 \cdot \ldots \cdot \ell_t - 1$ for small distinct odd primes ℓ_i.
- The elliptic curve $E_0 : y^2 = x^3 + x/\mathbb{F}_p$ is supersingular and its endomorphism ring over $\mathbb{F}_p$ is $\mathcal{O} = \mathbb{Z}[\pi]$ (commutative).
- A supersingular Montgomery curve $E_A : y^2 = x^3 + Ax^2 + x/\mathbb{F}_p$ appear in the $\mathcal{Cl}(\mathcal{O})$-orbit of E_0.
- **Private Key:** it is an n-tuple of integers $(e_1, \ldots, e_t)$ sampled in a range $\{-m, \ldots, m\}$ representing an ideal class $[\mathfrak{a}] = [\mathfrak{l}_1^{e_1} \cdot \ldots \cdot \mathfrak{l}_t^{e_t}] \in \mathcal{Cl}(\mathcal{O})$ where $\mathfrak{l}_i = (\ell_i, \pi - 1)$.
- **Public Key:** The Montgomery coefficients A of the elliptic curve $E_A = [\mathfrak{a}] \cdot E_0 : y^2 = x^3 + Ax^2 + x$.
- **Shared Key:** If Alice and Bob have private key $(\mathfrak{a}, A)$ and $(\mathfrak{b}, B)$ then they can compute the shared key $E_{AB} = [\mathfrak{a}][\mathfrak{b}] \cdot E_0 = [\mathfrak{b}][\mathfrak{a}] \cdot E_0$.

ORIENTATIONS

L.COLÒ UWAT

Let $\mathcal{O}$ be an order in an imaginary quadratic field K.
An $\mathcal{O}$-*orientation* on a supersingular elliptic curve E is an embedding

$$\iota : \mathcal{O} \hookrightarrow \mathrm{End}(E).$$

A K-*orientation* is an embedding

$$\iota : K \hookrightarrow \mathrm{End}^0(E) = \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

An $\mathcal{O}$-orientation is *primitive* if

$$\mathcal{O} \simeq \mathrm{End}(E) \cap \iota(K).$$

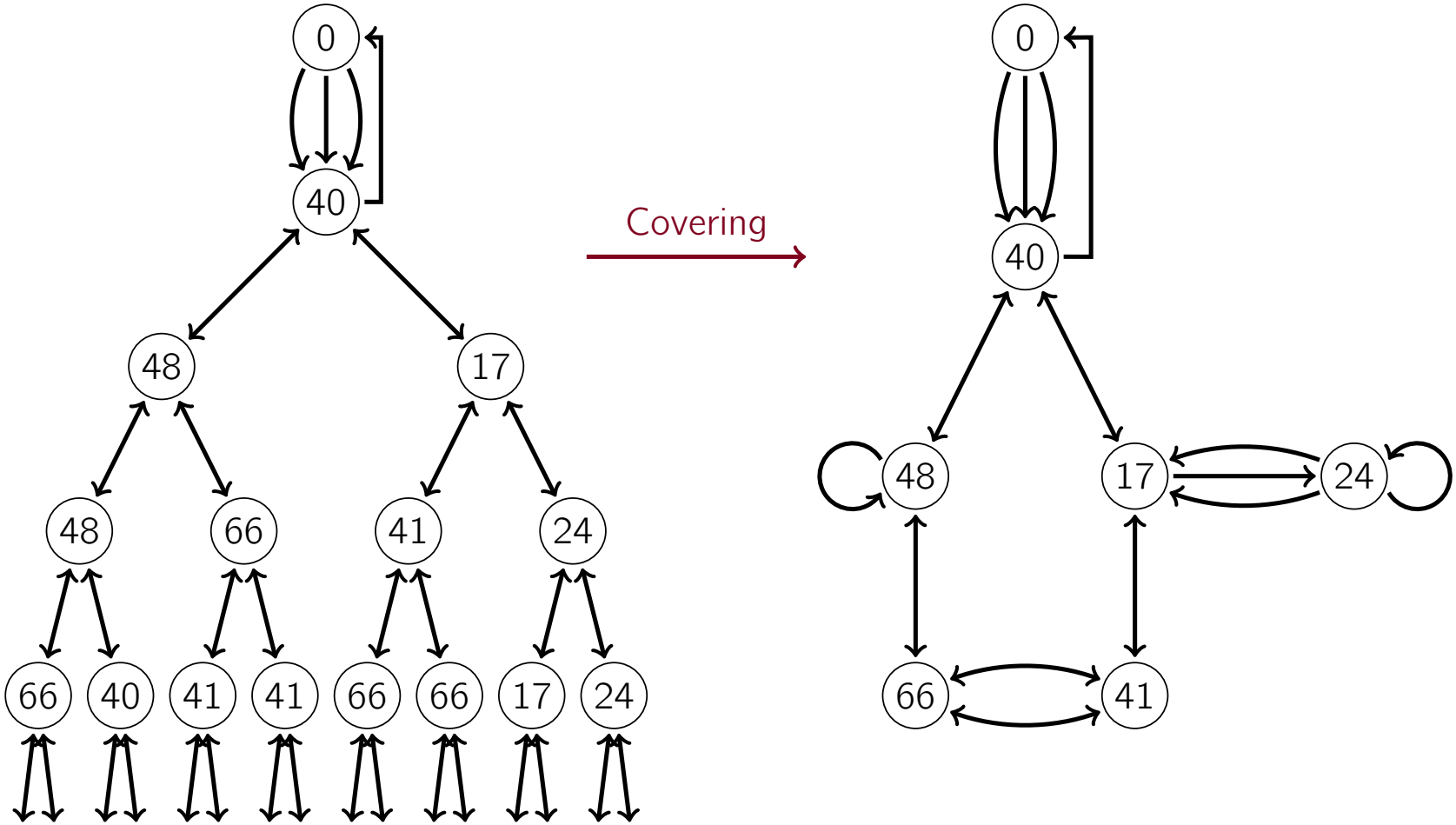
Theorem

The category of K-oriented supersingular elliptic curves (E, ι), whose morphisms are isogenies commuting with the K-orientations, is equivalent to the category of elliptic curves with CM by K.

ORIENTED ISOGENY GRAPHS - AN EXAMPLE

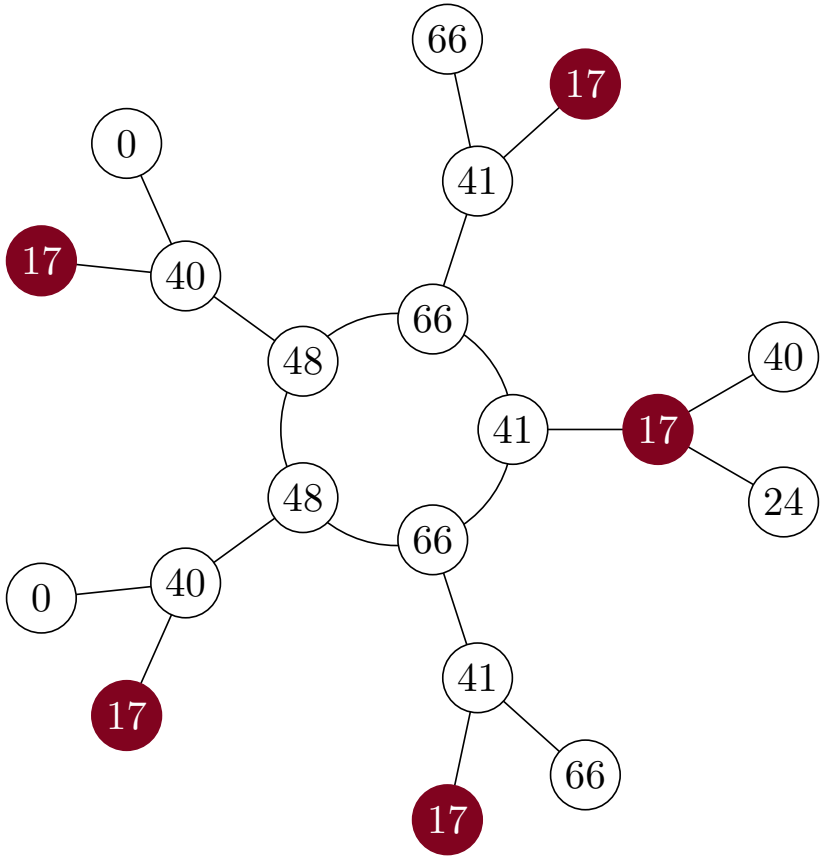
Let $p = 71$ and $E_0/\mathbb{F}_{71}$ be the supersingular elliptic curve with $j(E) = 0$ oriented by the $\mathcal{O}_K = \mathbb{Z}[\omega]$, where $\omega^2 + \omega + 1 = 0$.

The orientation by $K = \mathbb{Q}[\omega]$ differentiates vertices in the descending paths from E_0, determining an infinite graph shown here to depth 4:

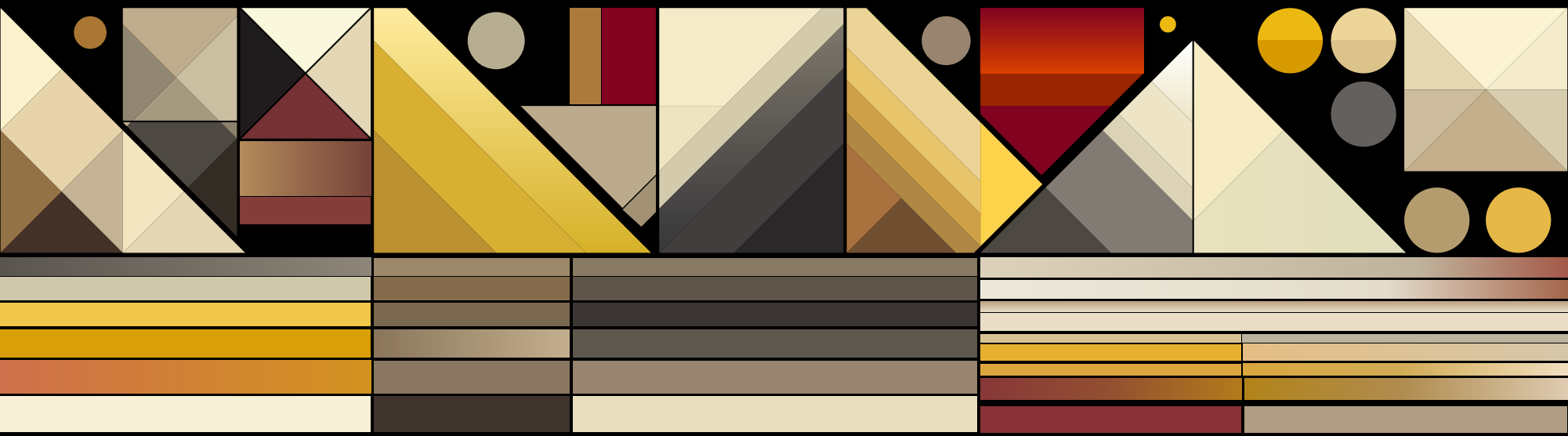


ORIENTED ISOGENY GRAPHS - YET ANOTHER EXAMPLE

We let again $p = 71$ and we consider the isogeny graph oriented by $\mathbb{Z}[\omega_{79}]$ where ω_{79} generates the ring of integers of $\mathbb{Q}(\sqrt{-79})$.



ISOGENY GRAPHS & MODULAR CURVES



MODULAR CURVES

The modular group acts on the upper half plane and its quotient classifies homothety classes of lattices or, equivalently, isomorphism classes of elliptic curves. As a geometric object it is a sphere with one point missing.

Define the extended upper-half plane

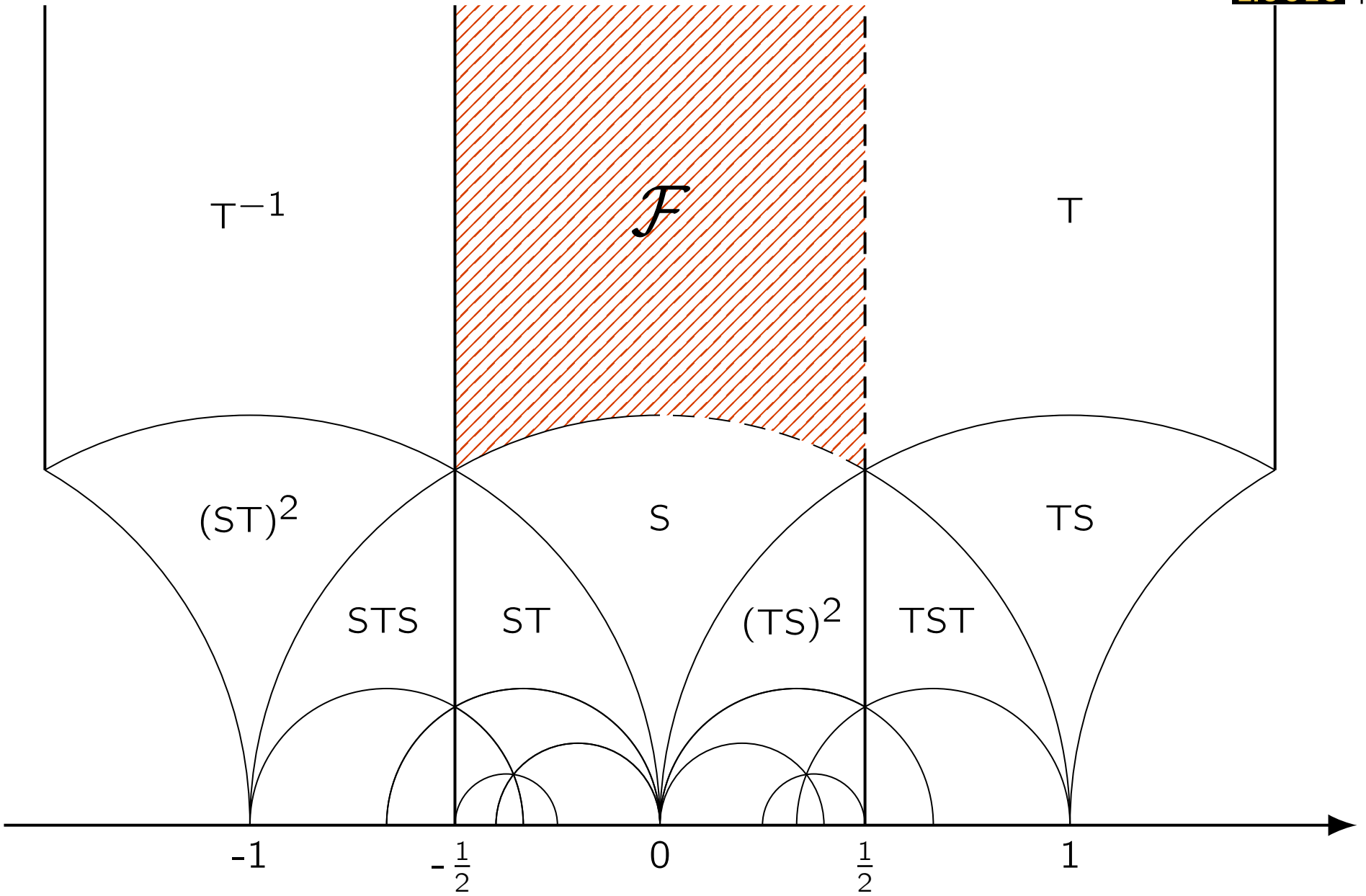
$$\mathbb{H}^* = \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$$

Definition

The affine modular curve over $\mathbb{C}$ attached to Γ is an algebraic curve $Y(\Gamma)$ whose complex points are identified with $\Gamma\backslash\mathbb{H}$ with its natural Riemann surface structure.

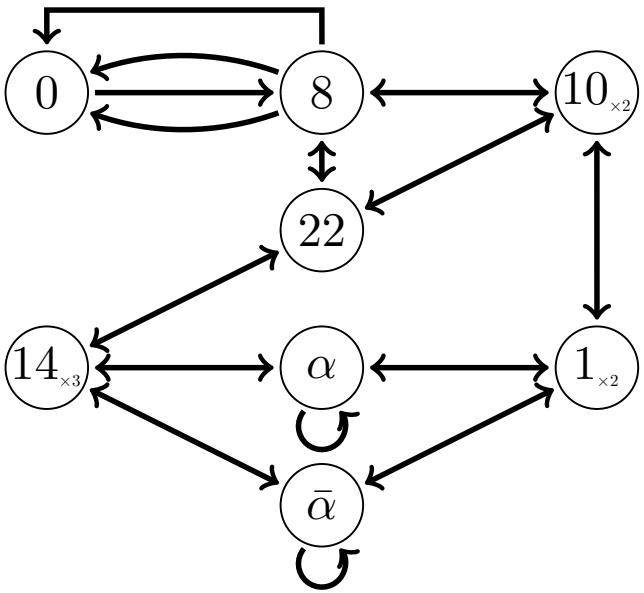
The complete modular curve over $\mathbb{C}$ attached to Γ is an algebraic curve $X(\Gamma)$ whose complex points are identified with $\Gamma\backslash\mathbb{H}^*$ equipped with some Riemann surface structure.

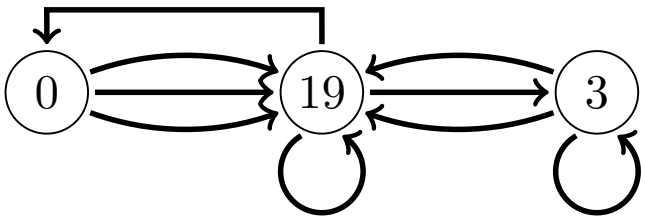
MODULAR CURVES - AN EXAMPLE



ISOGENY GRAPHS WITH LEVEL STRUCTURE

For any congruence subgroup Γ of level coprime to the characteristic, we have a covering $G_S(E, \Gamma) \to G_S(E)$ whose vertices are pairs $(E, \Gamma(P, Q))$ of supersingular elliptic curves/$\mathbb{F}_{p^2}$ and a Γ-level structure, and edges are isogenies $\psi : (E, \Gamma(P, Q)) \to (E', \Gamma(P', Q'))$ such that $\psi(\Gamma(P, Q)) = \Gamma(P', Q')$.





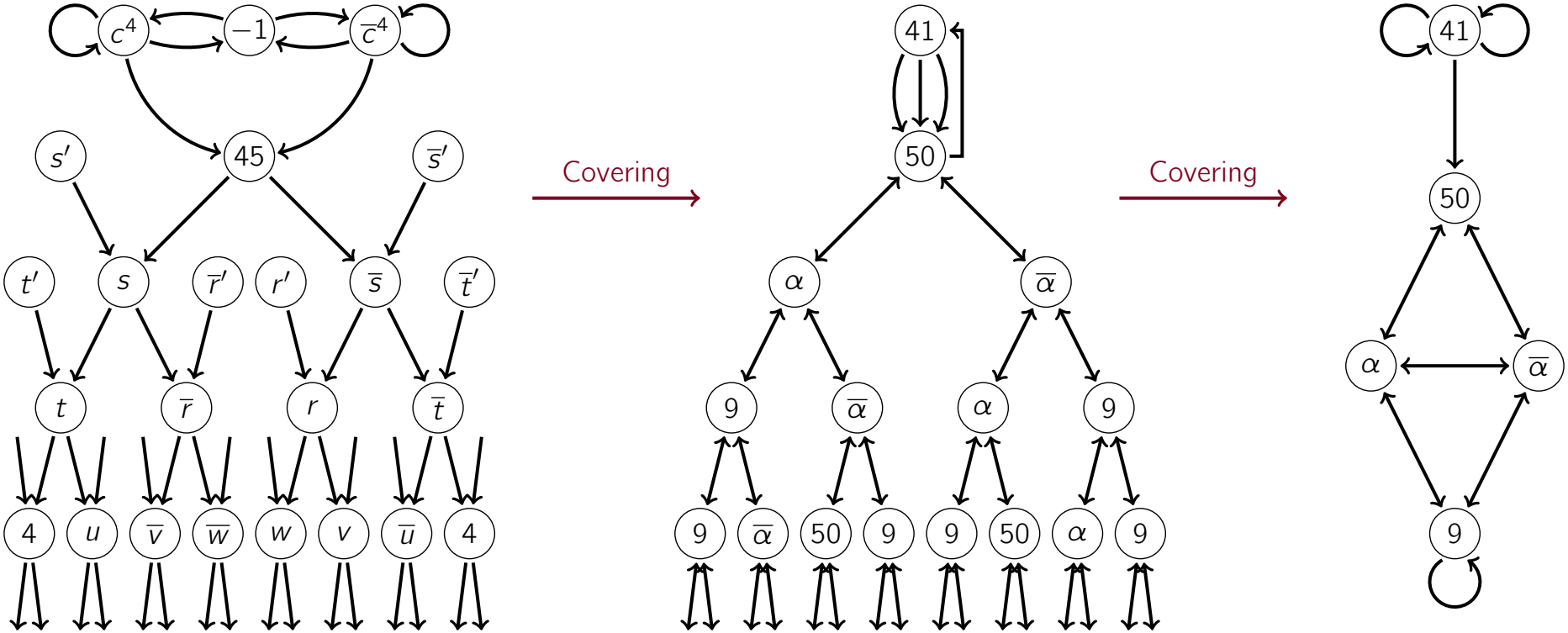
Eg. $\Gamma_0(N)$-structures.
Vertices (E, G) with $G \leq E[N]$ of order N
$\mathrm{End}(E, G) = \{\alpha \in \mathrm{End}(E) \,|\, \alpha(G) \subseteq G\}$
isomorphic to Eichler order.

On the left the $\Gamma_0(3)$ supersingular 2-isogeny graph.

$14 \leftrightarrow \{(E_0, G_1), (E_0, G_2), (E_0, G_3)\}$ where G_1, G_2, G_3 maps to each other under the automorphism of E_0; they define 3 isogenies to E_3.

ORIENTED GRAPHS WITH LEVEL STRUCTURE - AN EXAMPLE

We orient the supersingular 2-isogeny graph in characteristic 61 by $\mathbb{Q}(\sqrt{-7})$ and we then climb the modular tower.



SUPERSINGULAR CURVES AND MODULAR FORMS - ORIGINS

The relations between supersingular elliptic curves and the ideal theory in a quaternion algebra appears in a classical work of Deuring (1941).

The basis problem of Eichler (1973) provides the means to relate the ideal theory to modular forms.

Using this theory, Pizer (1980) describes an algorithm for computing modular forms.

The method of graphs of Oesterlé and Mestre (1986) rephrases the theory of Quaternion ideals in terms of supersingular elliptic curves.

BRANDT MATRICES

Let p be a prime number and $\mathfrak{A}_{p,\infty}$ the quaternion algebra ramified at p and infinity. Let R be a fixed maximal order in $\mathfrak{A}_{p,\infty}$.

For $\{J_1, \ldots, J_h\}$ a list of representatives for the isomorphism classes of left R-ideals and $n \geq 1$, we can construct the $h \times h$ matrix $B(n) = (b_{i,j}(n))$ by

$$\begin{aligned} b_{i,j}(n) &= \#\{I \subset J_i \,|\, \mathrm{Nr}(I) = n\mathrm{Nr}(J_i) \text{ and } [I] = [J_i]\} = \\ &= \#\{I \subset J_i \,\big|\, [J_i : I] = n^2 \text{ and } [I] = [J_i]\} = \\ &= \frac{1}{2\omega_i}\#\{\alpha \in J_j J_i^{-1} \mid \mathrm{Nr}(\alpha) q_i/q_j = n\} \end{aligned}$$

We can construct the $h \times h$ matrix valued function

$$\Theta(z) = \sum_{n \geq 0} B(n) q^n$$

whose i, j component is

$$\theta_{i,j}(z) = \sum_{n \geq 0} b_{i,j}(n) q^n \in \mathrm{M}_2(\Gamma_0(p))$$

BRANDT MATRICES - AN EXAMPLE

Let $p = 23$. The quaternion algebra $\mathfrak{A}_{p,\infty}$ has maximal order

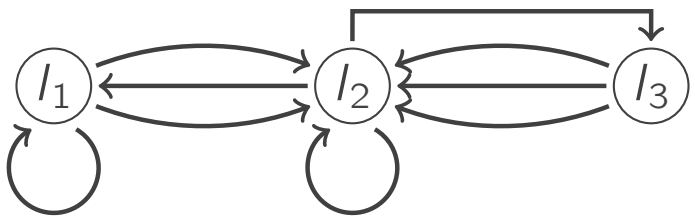
$$R = \mathbb{Z} + \mathbb{Z}\, i + \mathbb{Z}\, \frac{1+j}{2} + \mathbb{Z}\, i\, \frac{1+j}{2}$$

with three ideal classes$\{[J_1], [J_2], [J_3]\}$. We find

$$B(2) = \begin{pmatrix} 1 & 1 & 0 \\ 2 & 1 & 3 \\ 0 & 1 & 0 \end{pmatrix} \qquad B(3) = \begin{pmatrix} 0 & 1 & 3 \\ 2 & 3 & 0 \\ 2 & 0 & 1 \end{pmatrix} \qquad B(101) = \begin{pmatrix} 30 & 28 & 24 \\ 56 & 54 & 60 \\ 16 & 20 & 18 \end{pmatrix}$$

Giving normic forms

$$\mathrm{nr}_1(X_1, X_2, X_3, X_4) = X_1^2 + X_2^2 + 6X_3^2 + 6X_4^2 + X_1X_3 + X_2X_4$$
$$\mathrm{nr}_2(X_1, X_2, X_3, X_4) = X_1^2 + X_2^2 + 8X_3^2 + 8X_4^2 + X_1X_2 + X_1X_3 + X_2X_3 + X_2X_4 + 4X_3X_4$$
$$\mathrm{nr}_3(X_1, X_2, X_3, X_4) = X_1^2 + 2X_2^2 + 3X_3^2 + 6X_4^2 + X_1X_4 + X_2X_3$$



EICHLERS BASIS PROBLEM - BRANDT MODULES

We define the Brandt Module $\mathbb{M}_{\mathbb{C}}(R)$ as the $\mathbb{C}$-vector space with basis $\mathcal{C}\ell(R)$ equipped with the right action of Brandt matrices.

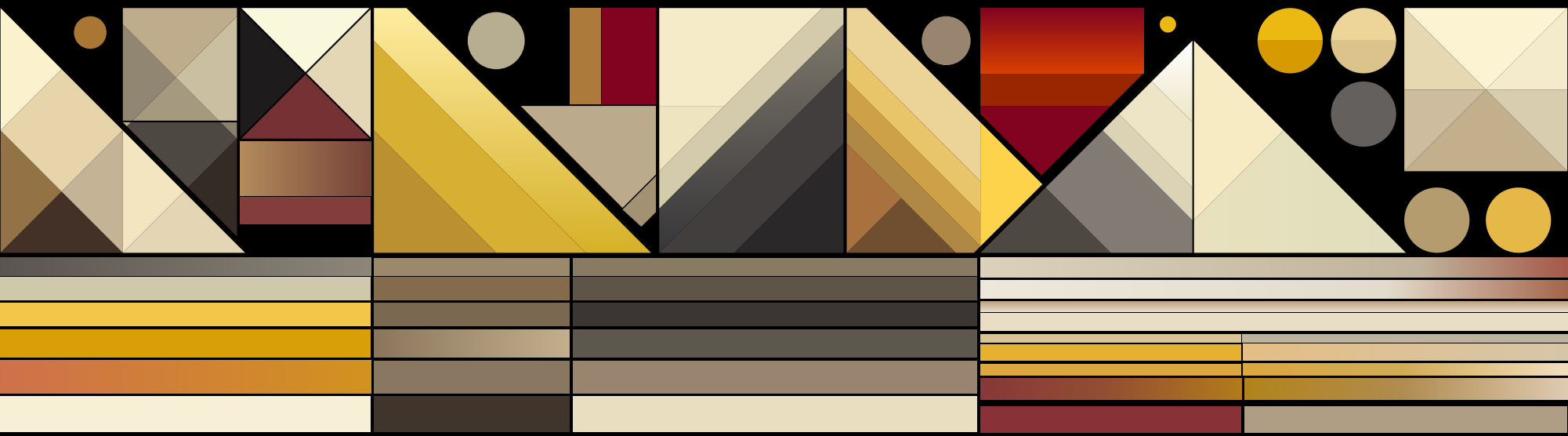
Define the Brandt morphism as

$$\begin{aligned}\mathbb{M}_{\mathbb{C}}(R) \times \mathbb{M}_{\mathbb{C}}(R) &\longrightarrow \mathrm{M}_2(\Gamma_0(p), \mathbb{Q}) \\ (J_i, J_j) &\longmapsto \sum b_{i,j}(n) q \\ &= \frac{1}{\omega_i} \sum_{\gamma} q^{Q_{i,j(\gamma)}} \\ &= \sum \langle B(n)E, F \rangle q^n\end{aligned}$$

Theorem

As part of the basis problem Eichler proved that the morphism above is surjective, equivalently that $\mathrm{M}_2(\Gamma_0(p), \mathbb{Q})$ is spanned by theta series.

MODULAR SYMBOLS & HOMOLOGY



RELATIVE HOMOLOGY & MANIN SYMBOLS

We let H denote the relative homology group

$$H := H_1(X_0(N), C; \mathbb{Z}).$$

Let Δ be the free abelian group on formal symbols $\{r \to s\}$ with $r, s \in \mathbb{P}^1(\mathbb{Q})$, modulo the relations

$$\{r \to s\} + \{s \to t\} + \{t \to r\} = 0 \qquad \text{for all } r, s, t \in \mathbb{P}^1(\mathbb{Q}),$$
$$\{r \to r\} = 0 \qquad \text{for all } r \in \mathbb{P}^1(\mathbb{Q}).$$

The group $\Gamma_0(N)$ acts on Δ by

$$\gamma \cdot \{r \to s\} := \{\gamma r \to \gamma s\}.$$

Proposition

There is a natural isomorphism of abelian groups

$$H_1(X_0(N), C; \mathbb{Z}) \cong \Delta_{\Gamma_0(N)},$$

where $\Delta_{\Gamma_0(N)} := \Delta / \langle \gamma \cdot x - x : \gamma \in \Gamma_0(N), x \in \Delta \rangle$

RANK FORMULA

The rank of the relative homology H can be expressed in terms of the genus and the number of cusps.

proposition

Let $g = g(X_0(N))$ be the genus of $X_0(N)$ and let $c = \#C$ be the number of cusps. Then

$$\operatorname{rank}_{\mathbb{Z}} H_1(X_0(N), C; \mathbb{Z}) = 2g + (c - 1).$$

Note that $\#C = \sum_{b|N} \varphi\left(\gcd\left(b, \frac{N}{b}\right)\right)$

BRANDT HOMOLOGY

Input: A base $\mathcal{O}$–oriented supersingular point (E_0, C_0, ι_0) and an ideal class $[\mathfrak{a}] \in \mathrm{Pic}(\mathcal{O})$.

- The class-group action gives an oriented curve

$$[\mathfrak{a}] * (E_0, C_0, \iota_0) = (E_\mathfrak{a}, C_\mathfrak{a}, \iota_\mathfrak{a}),$$

  and hence a quaternion ideal class $[I_\mathfrak{a}] \in \mathcal{Cl}(\mathcal{O}_B)$.
- The Brandt module

$$\mathbb{B} = \mathbb{Z}[\mathcal{Cl}(\mathcal{O}_B)]$$

  carries a Hecke action. Associate to $[\mathfrak{a}]$ the cuspidal vector

$$v_\mathfrak{a} = \mathrm{pr}_{\mathrm{cusp}}\left(e_{I_\mathfrak{a}} - e_{I_0}\right).$$

- Via Jacquet–Langlands + Eichler–Shimura:

$$\iota_{\mathrm{JL}} : \mathbb{B} \hookrightarrow H_1(X_0(pN), C; \mathbb{Z}) \otimes \mathbb{Q}.$$

- This defines the Brandt homology class

$$\gamma^{\mathrm{Br}}([\mathfrak{a}]) := (\mathrm{ES} \circ \mathrm{JL})(v_\mathfrak{a}) \in H_1\left(X_0(pN), C, \mathbb{Q}\right)$$

CM DIVISORS ON $X_0(N)$

Input: The same ideal class $[\mathfrak{a}]$.

- CM theory yields a Heegner point:

$$[\mathfrak{a}] \longmapsto x_{\mathfrak{a}} \in X_0(N)(\mathbb{C}),$$

compatible with the class group action.

- Fix:

$$x_0 := x_{\mathcal{O}_f}, \qquad c_\infty \in \text{cusps}.$$

Choose analytic paths:

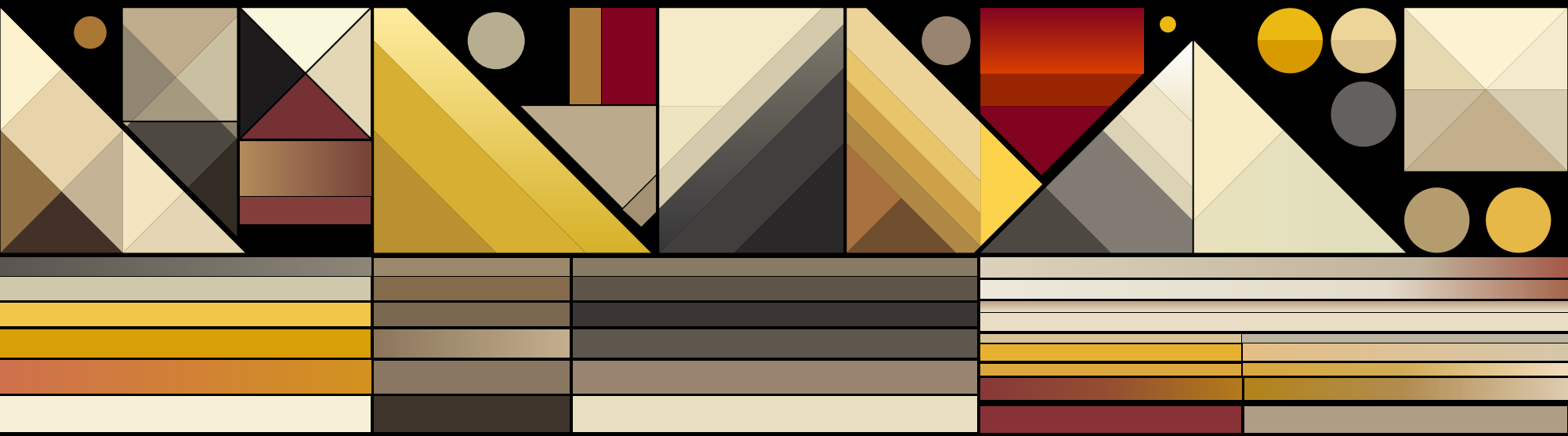
$$\delta_{\mathfrak{a}} : x_{\mathfrak{a}} \to c_\infty, \qquad \delta_0 : x_0 \to c_\infty.$$

- Relative homology:

$$\gamma^{(2)}([\mathfrak{a}]) := \delta_{\mathfrak{a}} - \delta_0 \in H_1(X_0(N), C; \mathbb{Z}).$$

This is well-defined modulo absolute cycles and depends only on $[\mathfrak{a}]$.

p-ADIC INTEGRATION



p-ADIC INTEGRATION - THE PROBLEM

Is there a Theory of p-adic integration?

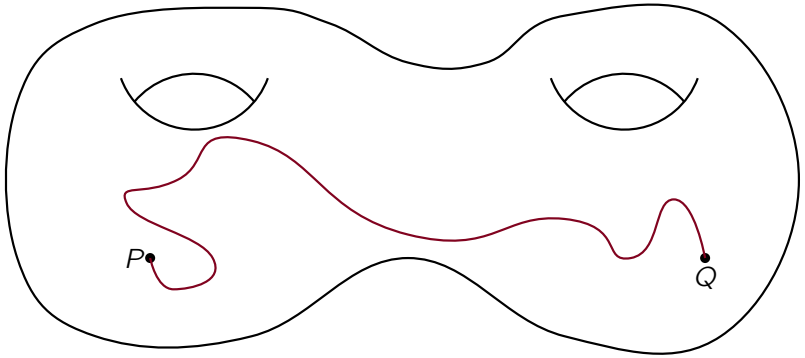
We cannot use the same methods that we have in $\mathbb{R}$ or in $\mathbb{C}$ because of the totally disconnected topology of rigid analytic spaces.

Theorem (Coleman)

- Additivity at points: $\int_P^Q \omega + \int_Q^R \omega = \int_P^R \omega$
- Linearity on forms: $\lambda_1 \int_P^Q \omega_1 + \lambda_2 \int_P^Q \omega_2 = \int_P^Q (\lambda_1\omega_1 + \lambda_2\omega_2)$
- Change of variables: if X' is another rigid space and $\Psi : X \to X'$ is a rigid analytic map, then $\int_P^Q \Psi^*\omega' = \int_{\Psi(P)}^{\Psi(Q)} \omega'$.
- Fundamental Theorem of Calculus: $\int_P^Q df = f(Q) - f(P)$.

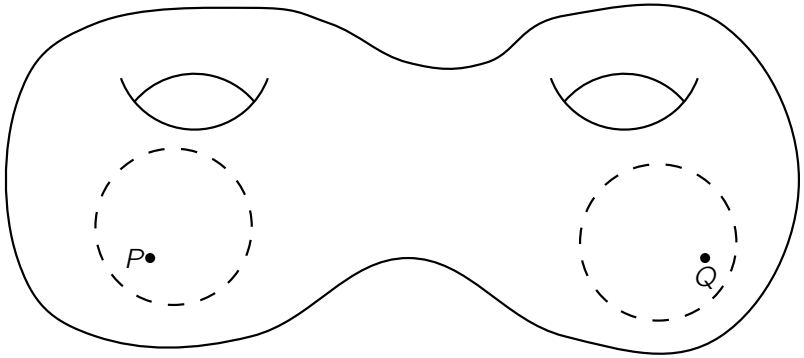
COLEMAN INTEGRATION

There is no obvious way of integrating over affinoids.



COLEMAN INTEGRATION

There is no obvious way of integrating over affinoids.

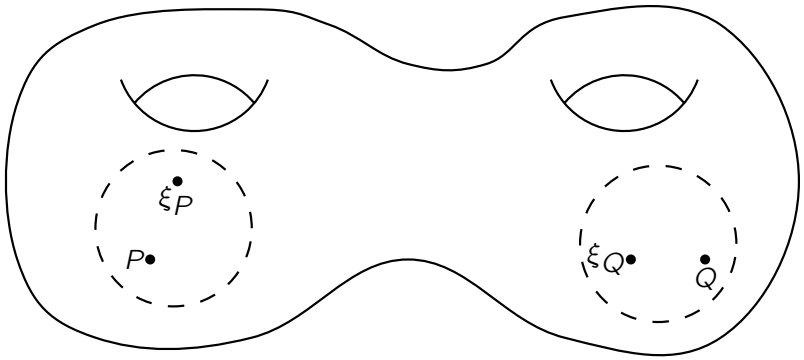


Coleman's Solution

- Cover the Affinoid space by residue disks.
- Integrate on each residue disk.
- **Problem:** Residue disks have no intersection.
- Connect integrals on different residue disks using Frobenius.

COLEMAN INTEGRATION

There is no obvious way of integrating over affinoids.



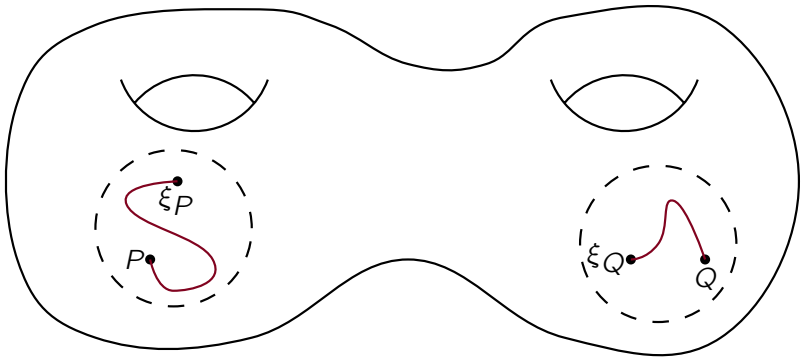
Coleman's Solution

- Find Teichmüller points

$$\int_P^Q \omega = \int_P^{\xi_P} \omega + \int_{\xi_P}^{\xi_Q} \omega + \int_{\xi_Q}^{Q} \omega$$

COLEMAN INTEGRATION

There is no obvious way of integrating over affinoids.



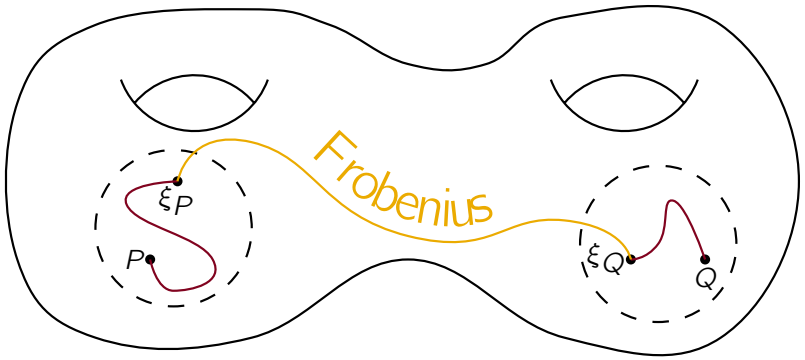
Coleman's Solution

- Find Teichmüller points
- Compute tiny integrals

$$\int_P^Q \omega = \int_P^{\xi_P} \omega + \int_{\xi_P}^{\xi_Q} \omega + \int_{\xi_Q}^{Q} \omega$$

COLEMAN INTEGRATION

There is no obvious way of integrating over affinoids.



Coleman's Solution

- Find Teichmüller points
- Compute tiny integrals
- Connect integrals using Frobenius

$$\int_P^Q \omega = \int_P^{\xi_P} \omega + \int_{\xi_P}^{\xi_Q} \omega + \int_{\xi_Q}^{Q} \omega$$

COMPUTING INTEGRALS ON $X_\emptyset(N)$

L.COLÒ UWAT

Computing $\int_Q^R \omega$ for $Q, R \in X = X_0(N)$ and $\omega \in H^0(X, \Omega^1)$

We can leverage the existence of Hecke operators.

Algorithm (Chen, Kedlaya, Lau)

- Write $\int_Q^R \omega$ as a sum of tiny integrals.
- Find a basis of holomorphic 1-forms and a suitable uniformizer.
- Compute the action of Hecke operators on cusp forms and points
- Write 1-forms as a power series in the uniformizer. This involves algebraic approximation after solving a system of equations over $\mathbb{C}$.
- Formally integrate and evaluate at the end points.

BREAKING INTO TINY INTEGRALS

Let $X/\mathbb{Q}$ be a modular curve associated to a congruence subgroup Γ.

- The Hecke operator T_p, acts on the weight 2 cusp forms, which correspond to the holomorphic 1-forms:

$$T_p^* \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_g \end{pmatrix} = A \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_g \end{pmatrix}$$

BREAKING INTO TINY INTEGRALS

Let $X/\mathbb{Q}$ be a modular curve associated to a congruence subgroup Γ.

- Since the Hecke operators are linear, integrating between the points Q and R gives:

$$\begin{pmatrix} \int_R^Q T_p^* \omega_1 \\ \vdots \\ \int_R^Q T_p^* \omega_g \end{pmatrix} = A \begin{pmatrix} \int_R^Q \omega_1 \\ \vdots \\ \int_R^Q \omega_g \end{pmatrix}$$

BREAKING INTO TINY INTEGRALS

Let $X/\mathbb{Q}$ be a modular curve associated to a congruence subgroup Γ.

- Since the Hecke operators are linear, integrating between the points Q and R gives:

$$\begin{pmatrix} \int_R^Q T_p^*\omega_1 \\ \vdots \\ \int_R^Q T_p^*\omega_g \end{pmatrix} = A \begin{pmatrix} \int_R^Q \omega_1 \\ \vdots \\ \int_R^Q \omega_g \end{pmatrix}$$

- For any $\omega \in H^0(X, \Omega^1)$ we obtain

$$\int_Q^R T_p^*\omega = \int_{T_p^*(Q)}^{T_p^*(R)} \omega = \sum_{i=0}^{p} \int_{R_i}^{Q_i} \omega$$

BREAKING INTO TINY INTEGRALS

Let $X/\mathbb{Q}$ be a modular curve associated to a congruence subgroup Γ.

- Since the Hecke operators are linear, integrating between the points Q and R gives:

$$\begin{pmatrix} \int_R^Q T_p^*\omega_1 \\ \vdots \\ \int_R^Q T_p^*\omega_g \end{pmatrix} = A \begin{pmatrix} \int_R^Q \omega_1 \\ \vdots \\ \int_R^Q \omega_g \end{pmatrix}$$

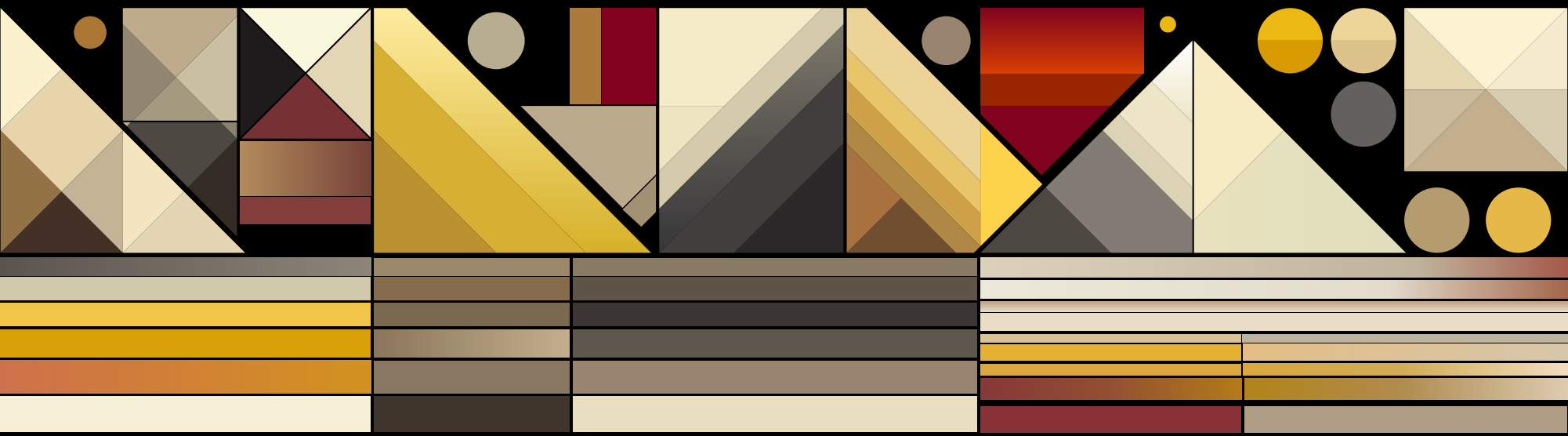
- For any $\omega \in H^0(X, \Omega^1)$ we obtain

$$\int_Q^R T_p^*\omega = \int_{T_p^*(Q)}^{T_p^*(R)} \omega = \sum_{i=0}^{p} \int_{R_i}^{Q_i} \omega$$

- We have the following fundamental equation

$$((p+1)I - A) \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_g \end{pmatrix} = \begin{pmatrix} \sum_{i=0}^p \int_{Q_i}^Q \omega_1 - \sum_{i=0}^p \int_{R_i}^R \omega_1 \\ \vdots \\ \sum_{i=0}^p \int_{Q_i}^Q \omega_g - \sum_{i=0}^p \int_{R_i}^R \omega_g \end{pmatrix}$$

CRYPTOGRAPHIC CONSTRUCTIONS



DEFINING THE PERIOD VECTOR

Let $\omega_1, \ldots, \omega_d$ be a fixed collection of holomorphic differential 1-forms on the modular curve $X_0(N)$. For $\gamma \in H_1(X_0(N), C; \mathbb{Z})$, we define the (infinite precision) p-adic period vector

$$\Pi(\gamma) := \left(\langle \omega_1, \gamma \rangle_p, \ldots, \langle \omega_d, \gamma \rangle_p\right) \in \mathbb{Q}_p^d \qquad \langle \omega_i, \gamma \rangle_p = \int_\gamma \omega_i.$$

Definition

Let q be a prime distinct from p and not dividing N. For $m \geq 1$ and $\gamma \in H$, the *truncated p-adic period vector* of γ is

$$\Pi_m(\gamma) := \left(\langle \omega_1, \gamma \rangle_p, \ldots, \langle \omega_d, \gamma \rangle_p\right) \bmod p^m \in (\mathbb{Z}/p^m\mathbb{Z})^d.$$

The map $\Pi_m : H \to (\mathbb{Z}/p^m\mathbb{Z})^d$ is $\mathbb{Z}$-linear, and its image is contained in a subgroup whose size depends on d, p, and m.

DEFINITION OF MSI

Let $\Pi_m : H \to (\mathbb{Z}/p^m\mathbb{Z})^d$ be the truncated p-adic period map. Fix parameters L, p, m, d, and consider the following relation.

MSI relation

The *Modular Symbol Inversion relation* R_{MSI} is the subset of $(\mathbb{Z}/p^m\mathbb{Z})^d \times \mathcal{W}_L$ given by

$$R_{\mathrm{MSI}} := \{(y, \gamma) : \gamma \in \mathcal{W}_L,\ y = \Pi_m(\gamma)\}.$$

We will write $(y, \gamma) \in R_{\mathrm{MSI}}$ to mean that γ is a valid "short" homology preimage of y under Π_m.

MSI problem

Given a value $y \in (\mathbb{Z}/p^m\mathbb{Z})^d$ known (or promised) to satisfy $y = \Pi_m(\gamma^\star)$ for some unknown $\gamma^\star \in \mathcal{W}_L$, the *Modular Symbol Inversion (MSI) problem* is to find a $\gamma \in \mathcal{W}_L$ such that $(y, \gamma) \in R_{\mathrm{MSI}}$.

SPARSE CM DIVISORS AND ℓ-ADIC PERIODS

Let $\Sigma_{\mathcal{O}} = \{x_{\mathfrak{a}} : [\mathfrak{a}] \in \mathrm{Pic}(\mathcal{O})\} \subset X_0(pN)(\overline{\mathbb{Q}})$ be the CM orbit.

A sparse degree-zero divisor supported on $\Sigma_{\mathcal{O}}$ is

$$D = \sum_{i=1}^{t} n_i [x_{\mathfrak{a}_i}], \qquad \sum_{i=1}^{t} n_i = 0,$$

where t and the coefficients n_i are small.

SDIP problem

Given

$$y = \Pi_{\ell,m}(D) = \left(\langle \omega_1, D\rangle_\ell, \ldots, \langle \omega_d, D\rangle_\ell\right) \bmod \mathfrak{l}^m \qquad \langle \omega_j, D\rangle_\ell = \sum_{i=1}^{t} n_i \int_{x_0}^{x_{\mathfrak{a}_i}} \omega_j$$

recover a sparse degree-zero divisor D' such that

$$\Pi_{\ell,m}(D') = y.$$

A FIAT-SHAMIR SIGNATURE BASED ON MSI

Public parameters:

$$(p, m, N, q), \quad \Pi_m : H_1(X_0(N), C; \mathbb{Z}) \to (\mathbb{Z}/p^m\mathbb{Z})^d.$$

Public key: $\mathbf{v} = \Pi_m(\gamma)$.
Secret key: short representative γ.

- **Commitment:** Pick random short $r \in H_1(X_0(N), C; \mathbb{Z})$, send

$$c = \Pi_m(r + \gamma).$$

- **Challenge:** Verifier samples

$$b \xleftarrow{\$} \{0, 1, \ldots, q-1\}.$$

- **Response:** Send

$$z = r + b\gamma.$$

  Apply rejection sampling to ensure $\|z\|$ stays within bounds.

Verification:

$$\Pi_m(z) \stackrel{?}{\equiv} c - b \cdot \mathbf{v} \quad \text{in } (\mathbb{Z}/p^m\mathbb{Z})^d.$$

(Security relies on hardness of MSI: recovering γ from $v = \Pi_m(\gamma)$.)

THANK YOU FOR THE ATTENTION

