

KU LEUVEN



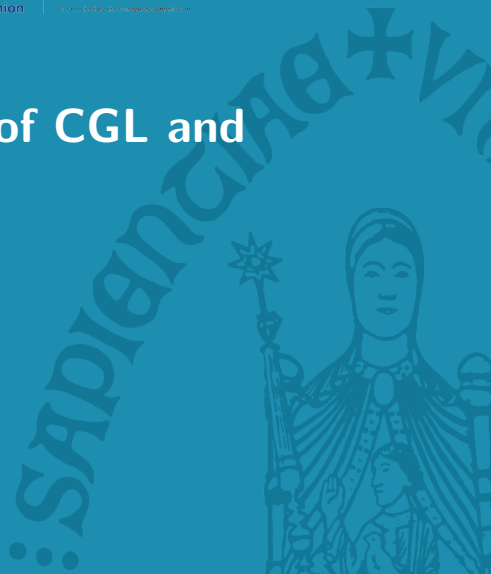
Funded by
the European Union



European Research Council
[europeanresearchcouncil.europa.eu](https://erc.europa.eu/)

The Mixing Time of CGL and Generalizations

Matthias Kerkhofs
COSIC, KU Leuven
NuTMiC 2026



1 Outline

① CGL in general graphs

② (Generalized) CGL in supersingular isogeny graphs

1 Graphs

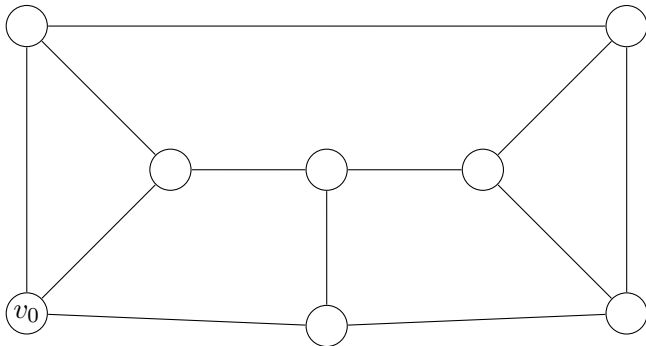
Our graphs will be ...

- ▶ finite
- ▶ undirected
- ▶ simple (no loops, no multi-edges)
- ▶ d -regular for some $d \geq 3$
- ▶ non-bipartite
- ▶ connected

Fix such a graph $\mathcal{G}$

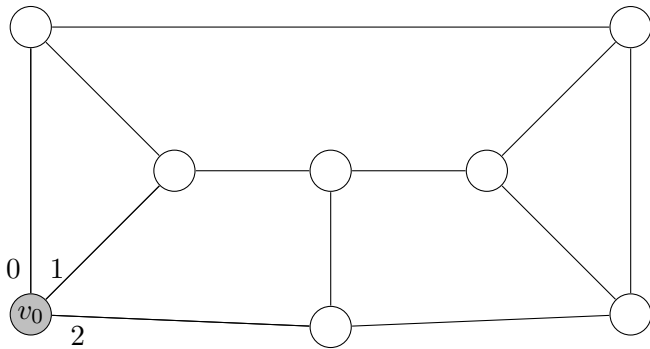
1 CGL hash function (Charles, Goren and Lauter, 2009)

- Fix a vertex v_0 in $\mathcal{G}$
- Example: input = 10011



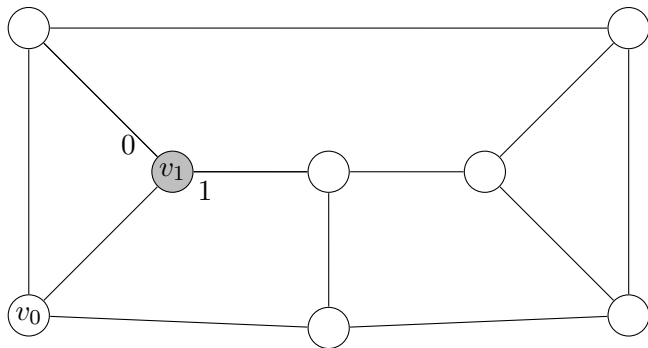
1 CGL hash function (Charles, Goren and Lauter, 2009)

- ▶ Fix a vertex v_0 in $\mathcal{G}$
- ▶ Example: input = $\textcircled{1}0011$



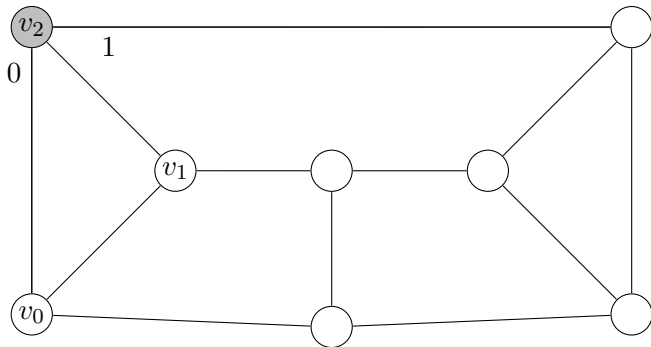
1 CGL hash function (Charles, Goren and Lauter, 2009)

- Fix a vertex v_0 in $\mathcal{G}$
- Example: input = 1(0)011



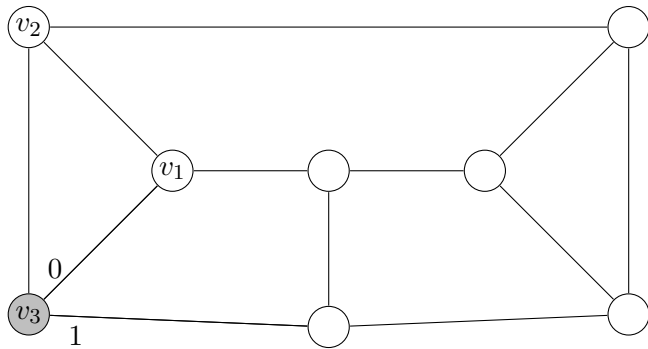
1 CGL hash function (Charles, Goren and Lauter, 2009)

- Fix a vertex v_0 in $\mathcal{G}$
- Example: input = 10(0)11



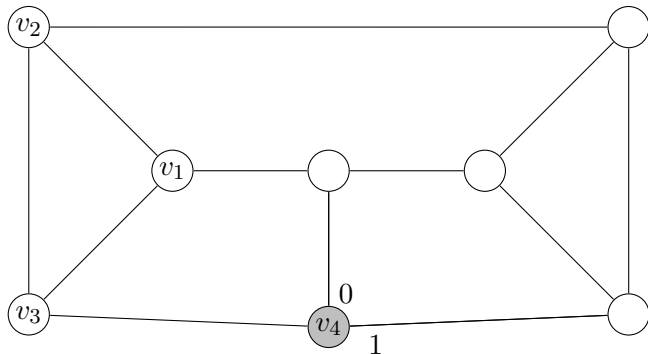
1 CGL hash function (Charles, Goren and Lauter, 2009)

- ▶ Fix a vertex v_0 in $\mathcal{G}$
- ▶ Example: input = 100(1)1



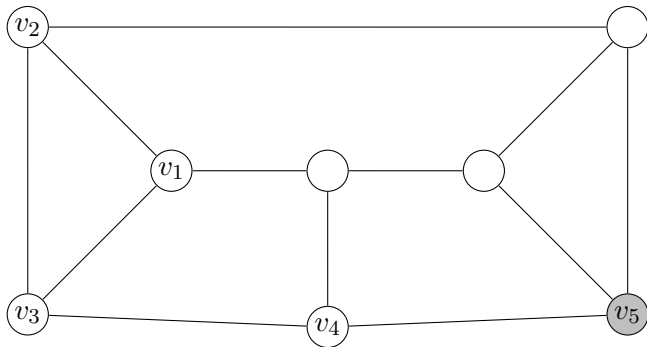
1 CGL hash function (Charles, Goren and Lauter, 2009)

- Fix a vertex v_0 in $\mathcal{G}$
- Example: input = 1001(1)



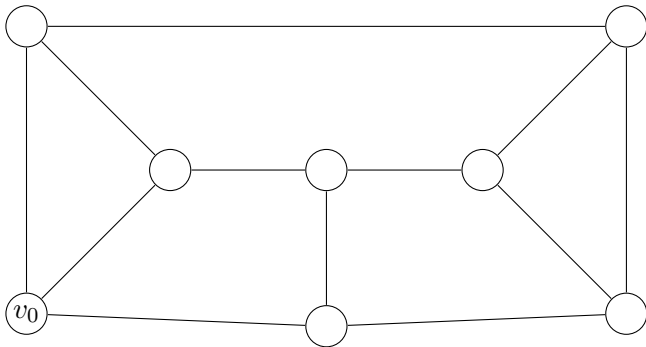
1 CGL hash function (Charles, Goren and Lauter, 2009)

- Fix a vertex v_0 in $\mathcal{G}$
- Example: input = 10011
- Output: v_5



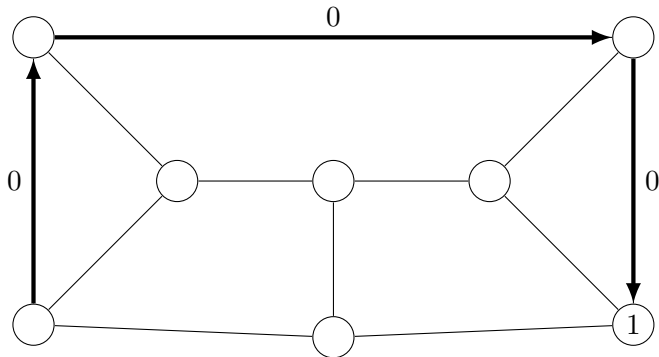
1 Uniformity

- ▶ Outputs should be (approximately) uniformly distributed
- ▶ Example: input length $k = 3$



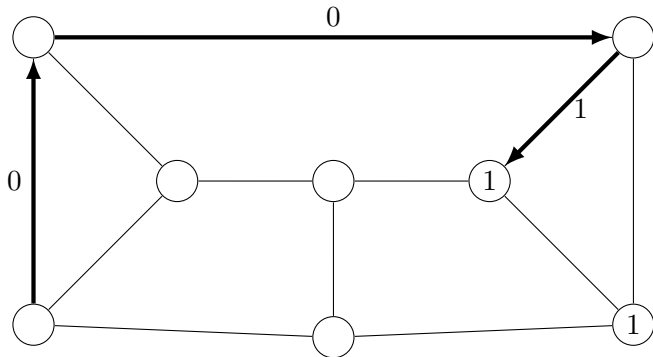
1 Uniformity

- ▶ Outputs should be (approximately) uniformly distributed
- ▶ Example: input length $k = 3$



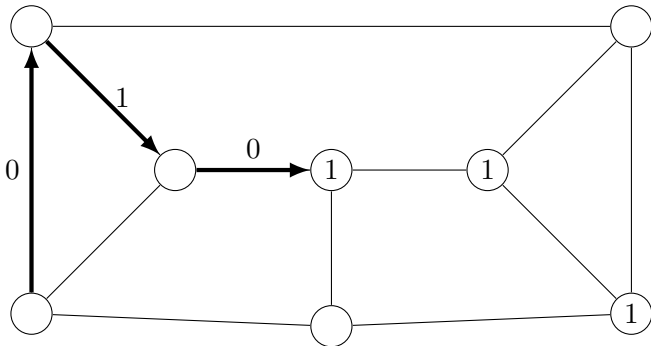
1 Uniformity

- ▶ Outputs should be (approximately) uniformly distributed
- ▶ Example: input length $k = 3$



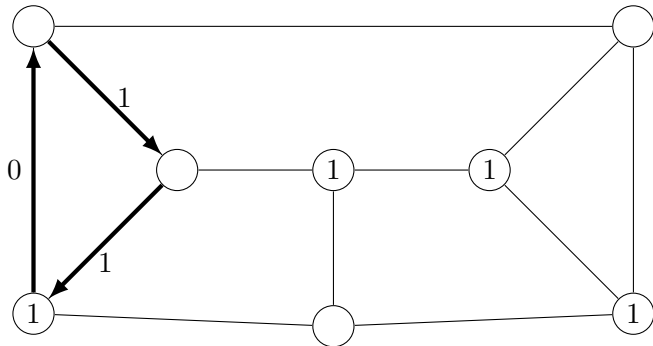
1 Uniformity

- ▶ Outputs should be (approximately) uniformly distributed
- ▶ Example: input length $k = 3$



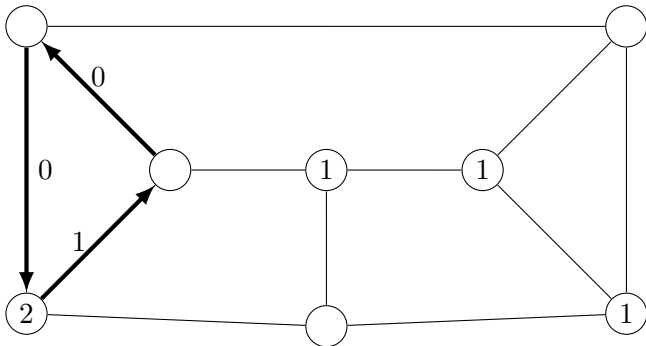
1 Uniformity

- ▶ Outputs should be (approximately) uniformly distributed
- ▶ Example: input length $k = 3$



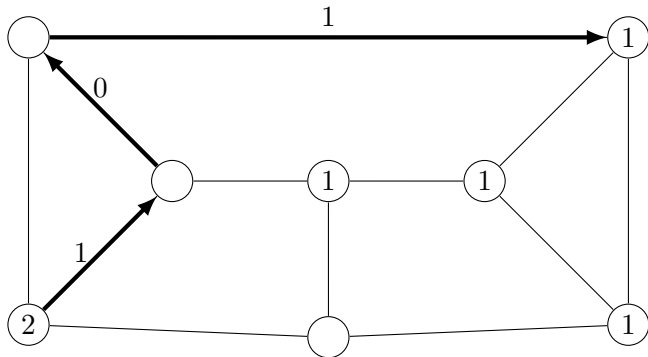
1 Uniformity

- ▶ Outputs should be (approximately) uniformly distributed
- ▶ Example: input length $k = 3$



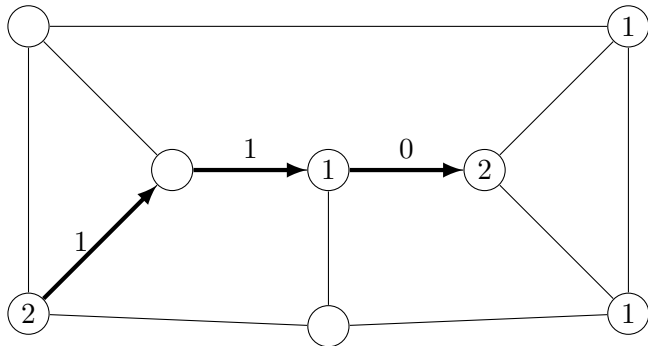
1 Uniformity

- ▶ Outputs should be (approximately) uniformly distributed
- ▶ Example: input length $k = 3$



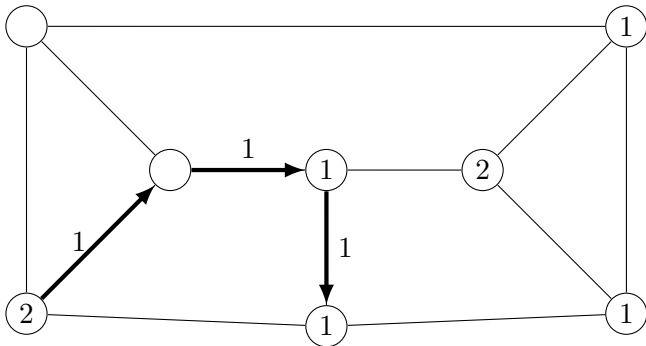
1 Uniformity

- ▶ Outputs should be (approximately) uniformly distributed
- ▶ Example: input length $k = 3$



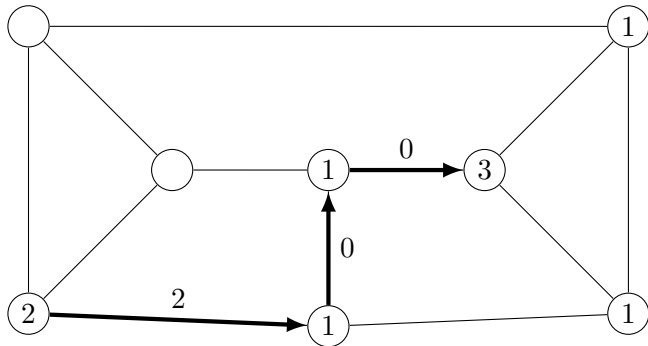
1 Uniformity

- ▶ Outputs should be (approximately) uniformly distributed
- ▶ Example: input length $k = 3$



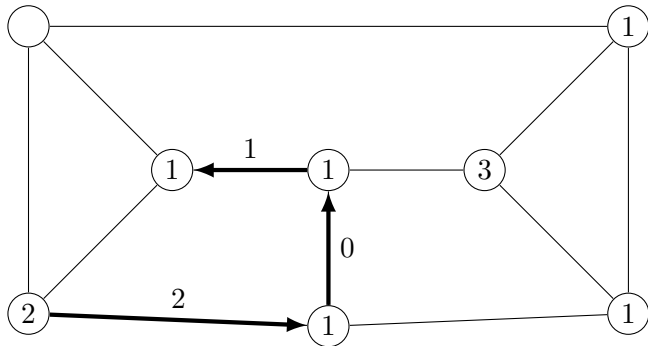
1 Uniformity

- ▶ Outputs should be (approximately) uniformly distributed
- ▶ Example: input length $k = 3$



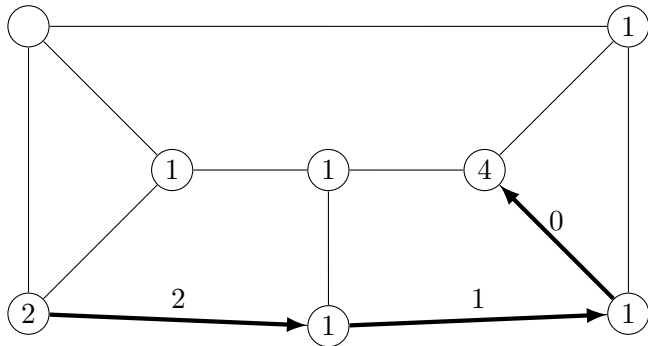
1 Uniformity

- ▶ Outputs should be (approximately) uniformly distributed
- ▶ Example: input length $k = 3$



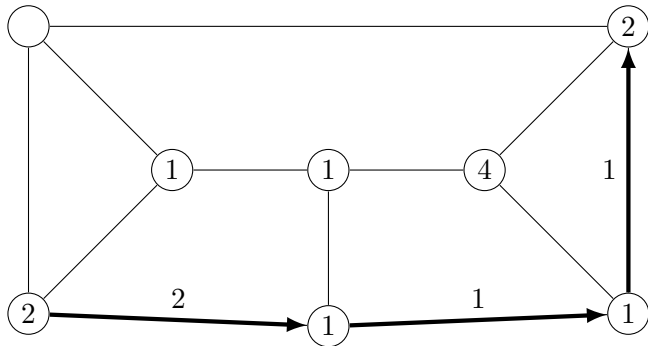
1 Uniformity

- ▶ Outputs should be (approximately) uniformly distributed
- ▶ Example: input length $k = 3$



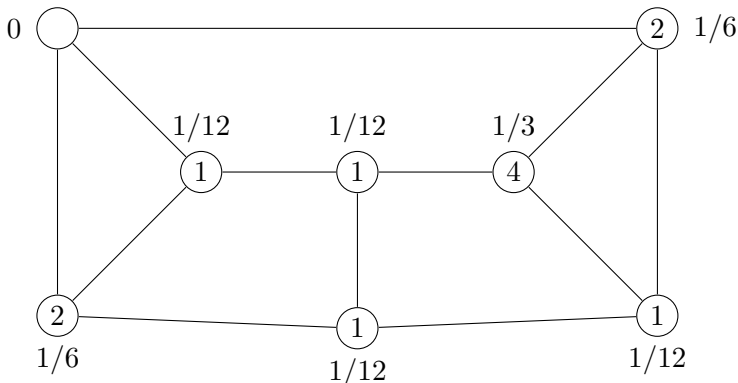
1 Uniformity

- ▶ Outputs should be (approximately) uniformly distributed
- ▶ Example: input length $k = 3$



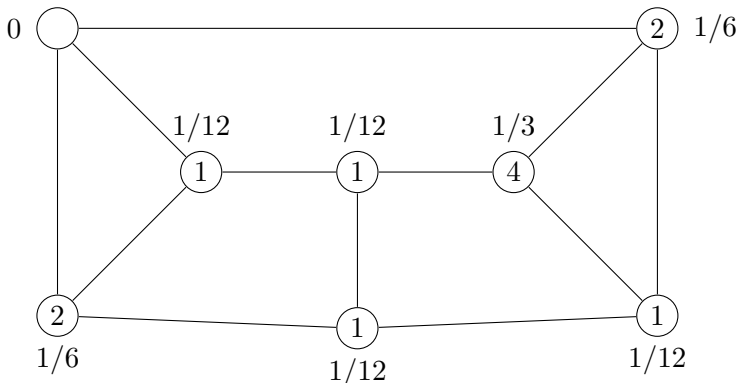
1 Uniformity

- ▶ Outputs should be (approximately) uniformly distributed
- ▶ Example: input length $k = 3$



1 Uniformity

- ▶ Outputs should be (approximately) uniformly distributed
- ▶ Example: input length $k = 3$
- ▶ $|1/3 - 1/8| = 5/24$ -close to uniform



1 Uniformity

- ▶ **Mixing time of $\mathcal{G}$ w.r.t. ε :** smallest k such that endpoints of random non-backtracking paths are ε -close to uniform
- ▶ Formally, set

$$P_{v,w}^{(k)} = \frac{\#\{\text{non-backtracking paths of length } k \text{ from } v \text{ to } w\}}{\#\{\text{non-backtracking paths of length } k \text{ from } v\}}$$

- ▶ Mixing time w.r.t. ε is smallest k such that

$$\max_{v,w \in V(\mathcal{G})} \left| P_{v,w}^{(k)} - \frac{1}{|V(\mathcal{G})|} \right| \leq \varepsilon$$

Smaller mixing time means smaller inputs, so more efficient!

1 Ramanujan graphs

- ▶ Recall: $\mathcal{G}$ is d -regular
- ▶ $A_{\mathcal{G}}$ adjacency matrix of $\mathcal{G}$
- ▶ Eigenvalues $d = \mu_0 > \mu_1 \geq \dots$ of $A_{\mathcal{G}}$
- ▶ $\mu(\mathcal{G}) = \max\{|\mu_i| \mid |\mu_i| \neq d\}$
- ▶ Smaller $\mu(\mathcal{G})$ means smaller mixing time
- ▶ Asymptotic minimum: $2\sqrt{d-1}$ (Alon-Boppana, 1991)

1 Ramanujan graphs

- ▶ Recall: $\mathcal{G}$ is d -regular
- ▶ $A_{\mathcal{G}}$ adjacency matrix of $\mathcal{G}$
- ▶ Eigenvalues $d = \mu_0 > \mu_1 \geq \dots$ of $A_{\mathcal{G}}$
- ▶ $\mu(\mathcal{G}) = \max\{|\mu_i| \mid |\mu_i| \neq d\}$
- ▶ Smaller $\mu(\mathcal{G})$ means smaller mixing time
- ▶ Asymptotic minimum: $2\sqrt{d-1}$ (Alon-Boppana, 1991)

$\mathcal{G}$ is called **Ramanujan** if $\mu(\mathcal{G}) \leq 2\sqrt{d-1}$

1 Mixing time of a Ramanujan graph

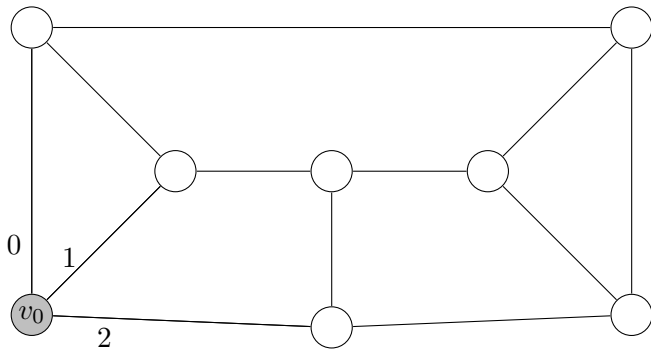
Proposition (Alon et al., 2007; Basso et al., 2023)

If $\mathcal{G}$ is Ramanujan, then

$$\left| P_{v,w}^{(k)} - \frac{1}{|V(\mathcal{G})|} \right| \leq \frac{dk - 2k + d}{d(d-1)^{k/2}}$$

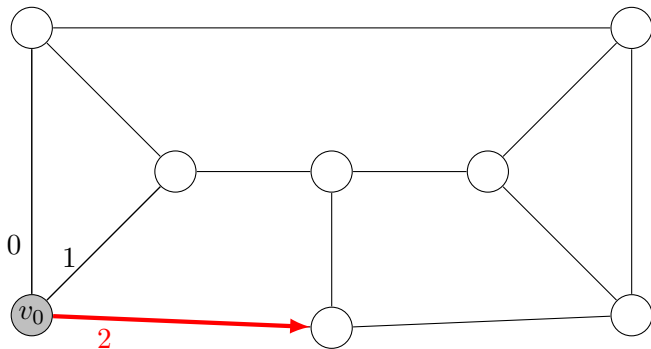
1 Back to CGL

- $d - 1$ choices at every step, except the first one



1 Back to CGL

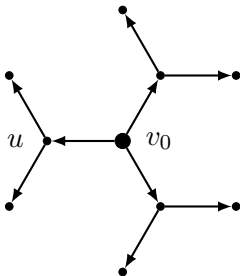
- ▶ $d - 1$ choices at every step, except the first one
- ▶ Compute mixing time w.r.t. non-backtracking paths not taking this edge in the first step



1 Mixing time of CGL

- ▶ Let $A_{v_0,w}^{(k,u)}$ be the number of non-backtracking paths of length k from v_0 to w not taking u in the first step
- ▶ Now, set $P_{v_0,w}^{(k,u)} = A_{v_0,w}^{(k,u)} / (d-1)^k$

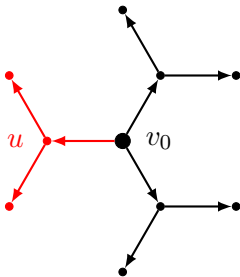
$$A_{v_0,w}^{(k,u)} = ?$$



1 Mixing time of CGL

- ▶ Let $A_{v_0,w}^{(k,u)}$ be the number of non-backtracking paths of length k from v_0 to w not taking u in the first step
- ▶ Now, set $P_{v_0,w}^{(k,u)} = A_{v_0,w}^{(k,u)} / (d-1)^k$

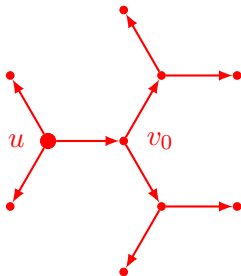
$$A_{v_0,w}^{(k,u)} = A_{v_0,w}^{(k)} - ?$$



1 Mixing time of CGL

- ▶ Let $A_{v_0,w}^{(k,u)}$ be the number of non-backtracking paths of length k from v_0 to w not taking u in the first step
- ▶ Now, set $P_{v_0,w}^{(k,u)} = A_{v_0,w}^{(k,u)} / (d-1)^k$

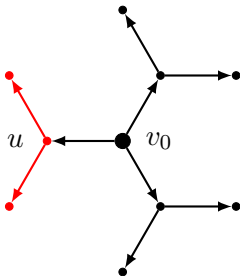
$$A_{v_0,w}^{(k,u)} = A_{v_0,w}^{(k)} - A_{u,w}^{(k-1)}?$$



1 Mixing time of CGL

- ▶ Let $A_{v_0,w}^{(k,u)}$ be the number of non-backtracking paths of length k from v_0 to w not taking u in the first step
- ▶ Now, set $P_{v_0,w}^{(k,u)} = A_{v_0,w}^{(k,u)} / (d-1)^k$

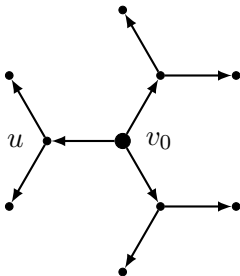
$$A_{v_0,w}^{(k,u)} = A_{v_0,w}^{(k)} - A_{u,w}^{(k-1,v_0)}$$



1 Mixing time of CGL

- ▶ Let $A_{v_0,w}^{(k,u)}$ be the number of non-backtracking paths of length k from v_0 to w not taking u in the first step
- ▶ Now, set $P_{v_0,w}^{(k,u)} = A_{v_0,w}^{(k,u)} / (d-1)^k$

$$A_{v_0,w}^{(k,u)} = A_{v_0,w}^{(k)} - A_{u,w}^{(k-1)} + A_{v_0,w}^{(k-2,u)}$$



1 Mixing time of CGL

- ▶ Let $A_{v_0,w}^{(k,u)}$ be the number of non-backtracking paths of length k from v_0 to w not taking u in the first step
- ▶ Now, set $P_{v_0,w}^{(k,u)} = A_{v_0,w}^{(k,u)} / (d-1)^k$

$$A_{v_0,w}^{(k,u)} = A_{v_0,w}^{(k)} - A_{u,w}^{(k-1)} + A_{v_0,w}^{(k-2,u)}$$

Proposition

If $\mathcal{G}$ is Ramanujan, then

$$\left| P_{v,w}^{(k,u)} - \frac{1}{|V(\mathcal{G})|} \right| \leq \frac{k + (k+1)\sqrt{d-1}}{(d-1)^{(k+1)/2}}$$

1 Mixing time of $\mathcal{G}$ versus CGL

Comparing upper bounds:

Example

- ▶ $d = 3$
- ▶ $|V(\mathcal{G})| \approx 2^{256}$
- ▶ $\varepsilon = 2^{-257}$
- ▶ The previous bounds give:

$$\left| P_{v,w}^{(k)} - \frac{1}{|V(\mathcal{G})|} \right| \leq \varepsilon \text{ if } k \geq 529 \text{ (corresponding to 530 bits)}$$

$$\left| P_{v,w}^{(k,u)} - \frac{1}{|V(\mathcal{G})|} \right| \leq \varepsilon \text{ if } k \geq 534$$

2 Outline

- ① CGL in general graphs
- ② (Generalized) CGL in supersingular isogeny graphs

2 Supersingular isogeny graphs

- Fix a large prime p

Definition

Let ℓ be coprime to p . The supersingular isogeny graph $\mathcal{G}_\ell$ consists of:

- Vertices: (isomorphism classes of) supersingular elliptic curves over $\mathbb{F}_{p^2}$
- Edges: isogenies of degree ℓ between elliptic curves representing the vertices

2 Facts about supersingular isogeny graphs

$\mathcal{G}_\ell$ is ...

- ▶ finite
- ▶ undirected if $p \equiv 1 \pmod{12}$
- ▶ simple if p satisfies certain congruence conditions
- ▶ $(\ell + 1)$ -regular if ℓ is prime
- ▶ non-bipartite
- ▶ connected
- ▶ Ramanujan if ℓ is prime (Pizer, 1998)

2 Facts about supersingular isogeny graphs

Corollary

If ℓ is prime, then the mixing time of CGL in $\mathcal{G}_\ell$ is given by

$$\left| P_{v,w}^{(k,u)} - \frac{1}{|V(\mathcal{G}_\ell)|} \right| \leq \frac{k + (k+1)\sqrt{\ell}}{\ell^{(k+1)/2}}$$

2 Facts about supersingular isogeny graphs

Corollary

If ℓ is prime, then the mixing time of CGL in $\mathcal{G}_\ell$ is given by

$$\left| P_{v,w}^{(k,u)} - \frac{1}{|V(\mathcal{G}_\ell)|} \right| \leq \frac{k + (k+1)\sqrt{\ell}}{\ell^{(k+1)/2}}$$

More nice properties:

- ▶ **Preimage resistance:** hard to find paths between given vertices (supersingular isogeny problem)
- ▶ **Collision resistance:** hard to find cycles (supersingular endomorphism problem)

2 First (naive) generalization of CGL

Let ℓ and m be distinct primes

Idea:

At every step, choose isogeny of either degree ℓ or m (without backtracking)

2 First (naive) generalization of CGL

Let ℓ and m be distinct primes

Idea:

At every step, choose isogeny of either degree ℓ or m (without backtracking)

- ▶ Walk through “union” $\mathcal{G}$ of $\mathcal{G}_\ell$ and $\mathcal{G}_m$
- ▶ Adjacency matrix = $A_{\mathcal{G}_\ell} + A_{\mathcal{G}_m}$
- ▶ $A_{\mathcal{G}_\ell}$ and $A_{\mathcal{G}_m}$ have same eigenspaces (Pizer, 1980)
- ▶ $\mu(\mathcal{G})$ bounded above by $\mu(\mathcal{G}_\ell) + \mu(\mathcal{G}_m)$
- ▶ This gives us a bound on the mixing time

2 First (naive) generalization of CGL

- ▶ **But:** not collision-resistant!
- ▶ Push-forward of isogenies:

$$\begin{array}{ccc} E & \xrightarrow{\phi_m} & E_m \\ \phi_\ell \downarrow & & \downarrow \phi'_\ell \\ E_\ell & \dashrightarrow_{\phi'_m} & E' \end{array}$$

2 Second generalization of CGL

Let ℓ and m be distinct primes

Idea:

At every step, choose isogenies of both degrees ℓ and m , and take push-forward (without backtracking)

2 Second generalization of CGL

Let ℓ and m be distinct primes

Idea:

At every step, choose isogenies of both degrees ℓ and m , and take push-forward (without backtracking)

- ▶ Walk through $\mathcal{G}_{\ell m}$
- ▶ Adjacency matrix = $A_{\mathcal{G}_{\ell}} A_{\mathcal{G}_m}$
- ▶ $\mu(\mathcal{G}_{\ell m})$ bounded above by $\mu(\mathcal{G}_{\ell})\mu(\mathcal{G}_m)$
- ▶ This gives us a bound on the mixing time

2 Second generalization of CGL

Let ℓ and m be distinct primes

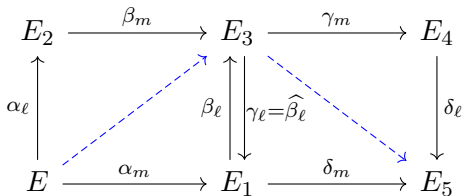
Idea:

At every step, choose isogenies of both degrees ℓ and m , and take push-forward (without backtracking)

- ▶ Walk through $\mathcal{G}_{\ell m}$
- ▶ Adjacency matrix = $A_{\mathcal{G}_\ell} A_{\mathcal{G}_m}$
- ▶ $\mu(\mathcal{G}_{\ell m})$ bounded above by $\mu(\mathcal{G}_\ell)\mu(\mathcal{G}_m)$
- ▶ This gives us a bound on the mixing time
- ▶ **Parallelization**

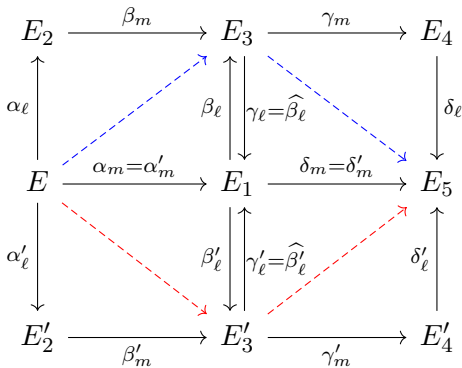
2 Second generalization of CGL

- **But:** not collision-resistant!
- “Partial backtracking”:



2 Second generalization of CGL

- **But:** not collision-resistant!
- “Partial backtracking”:



2 Second generalization of CGL (fixed)

- ▶ **Solution:** disallow partial backtracking
- ▶ The result is theoretically equivalent to a non-backtracking chain:

$$E_1 \xrightarrow{\ell} E'_2 \xrightarrow{\ell} \dots \xrightarrow{\ell} E'_{k+1} \xrightarrow{m} E'_{k+2} \xrightarrow{m} \dots \xrightarrow{m} E'_{2k} \xrightarrow{m} E_{2k+1}$$

2 Second generalization of CGL (fixed)

- ▶ **Solution:** disallow partial backtracking
- ▶ The result is theoretically equivalent to a non-backtracking chain:

$$E_1 \xrightarrow{\ell} E'_2 \xrightarrow{\ell} \dots \xrightarrow{\ell} E'_{k+1} \xrightarrow{m} E'_{k+2} \xrightarrow{m} \dots \xrightarrow{m} E'_{2k} \xrightarrow{m} E_{2k+1}$$

- ▶ Bound on mixing time: $\varepsilon = \varepsilon_\ell \varepsilon_m$
- ▶ Collision resistance

2 Conclusion

- ▶ Bound on mixing time of CGL, taking into account first step
- ▶ Bounds on mixing time of generalizations of CGL:
 - Naive first method: collisions through push-forward
 - Second method: collisions by partially backtracking
 - Fix of second method: Disallow partial backtracking

2 Conclusion

- ▶ Bound on mixing time of CGL, taking into account first step
- ▶ Bounds on mixing time of generalizations of CGL:
 - Naive first method: collisions through push-forward
 - Second method: collisions by partially backtracking
 - Fix of second method: Disallow partial backtracking

Thank you!