Hash Functions Based On Multi-regular Graphs

（Group-Subgroup Pair graphs）

○Hyungrok Jo（Yokohama National University, IAS）

Cid Reyes Bustos（NTT, IFM）

［This is an on-going research］

情報数理セミナー@日本大学

2024. August 21st.

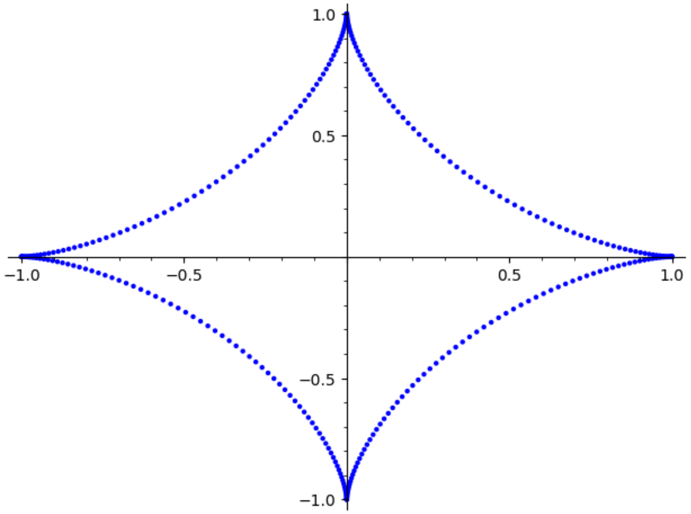
Outline of this talk

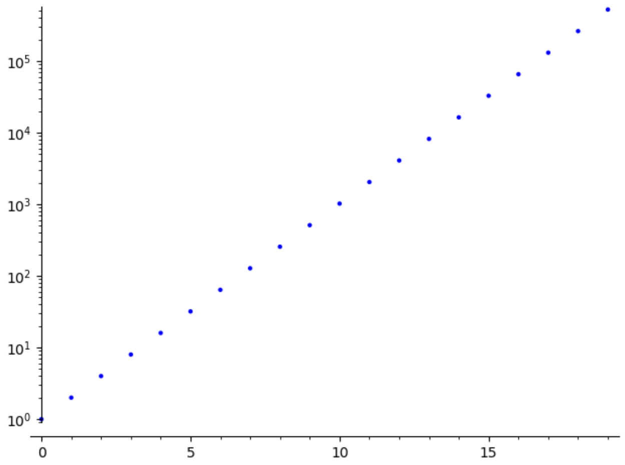
1. Cayley hash function :
   A cryptographic hash function from Cayley graph
2. A **brief history** of Cayley hash function
3. On **security** of Cayley hash function
4. **Group-subgroup pair graph**
   - Motivation / Definition / Examples
5. **Our proposal** :
   A hash function based on **multi-regular graphs**

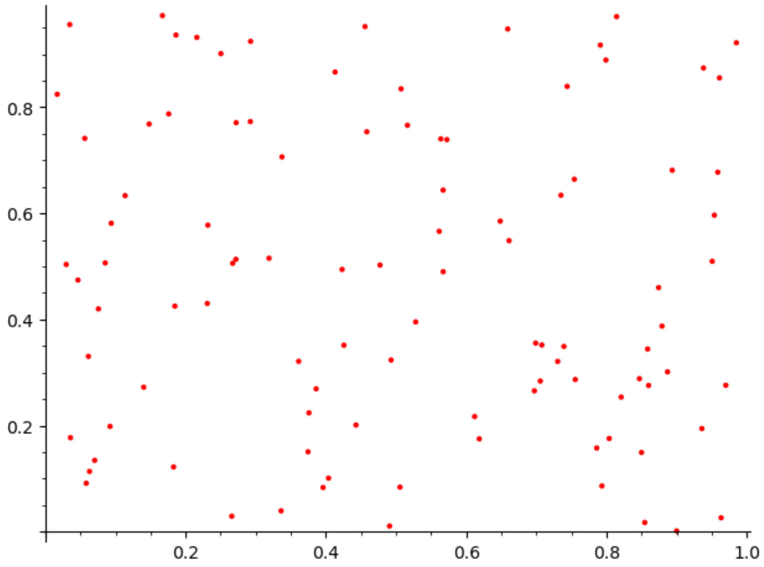
   (A hash function based on **pair-graphs**)
6. Discussions on proposals' **security**

Cayley hash function

Hash.. Function..?







Hash function

(large) data

Between 128 and 1024

$$H : \{0,1\}^* \to \{0,1\}^n$$

$$\text{message} \mapsto \text{hash value}$$

1) It should be efficient to compute!
   (cryptographic primitive)
2) It should digest messages uniformly in a hash space!
   (universality)

With main security properties (resistances)!

Hash function (Main properties)

Collision resistance

: if it is "*computationally infeasible*" to find any two distinct preimage m, m' such that $H(m) = H(m')$.

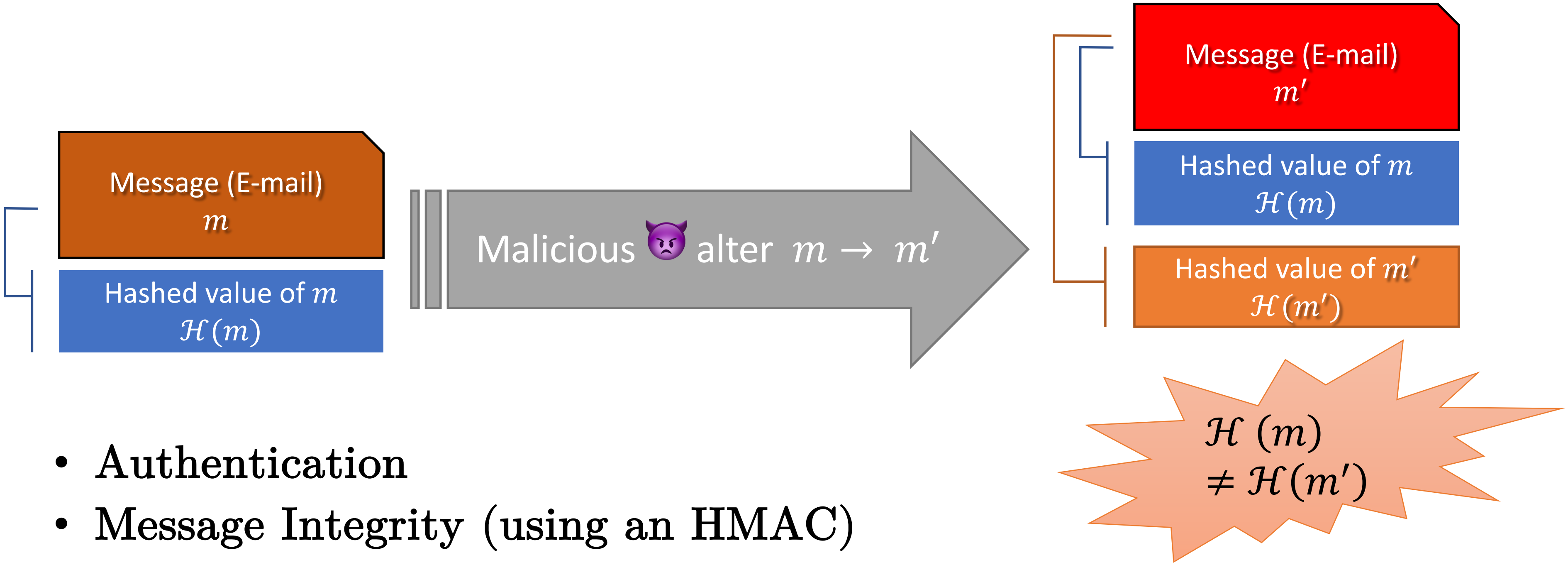
Second preimage resistance

: if given any message $m \in \{0,1\}^*$, it is "*computationally infeasible*" to find any second preimage $m'(\neq m)$ such that $H(m) = H(m')$.

Preimage resistance (Oneway-ness)

: if given any hash value $h \in \{0,1\}^n$, it is "*computationally infeasible*" to find any preimage (message) $m \in \{0,1\}^*$ such that $h = H(m)$.

Standard usages of hash functions



- Authentication
- Message Integrity (using an HMAC)
- Message Fingerprinting
- Data Corruption Detection
- Digital Signature
- Pseudorandom Number Generators
- Advanced Cryptography (IBE/IBS/ABS..)

Cayley graph

G : a finite group,

S : a generating set of G satisfying $S^{-1} = S$ without the identity id.

$\mathrm{Cay}(G, S) = (V, E)$: *Cayley graph* over G with respect to S.

- Vertex-set V : $\{v_g \mid g \in G\}$

- Edge-set E : $\left\{\left(v_{g_i}, v_{g_j}\right) \middle| g_j = g_i s,\ s \in S\right\}$

<u>Remark</u>

$G =< S > \Rightarrow$ Cay(G, S) is a connected graph.

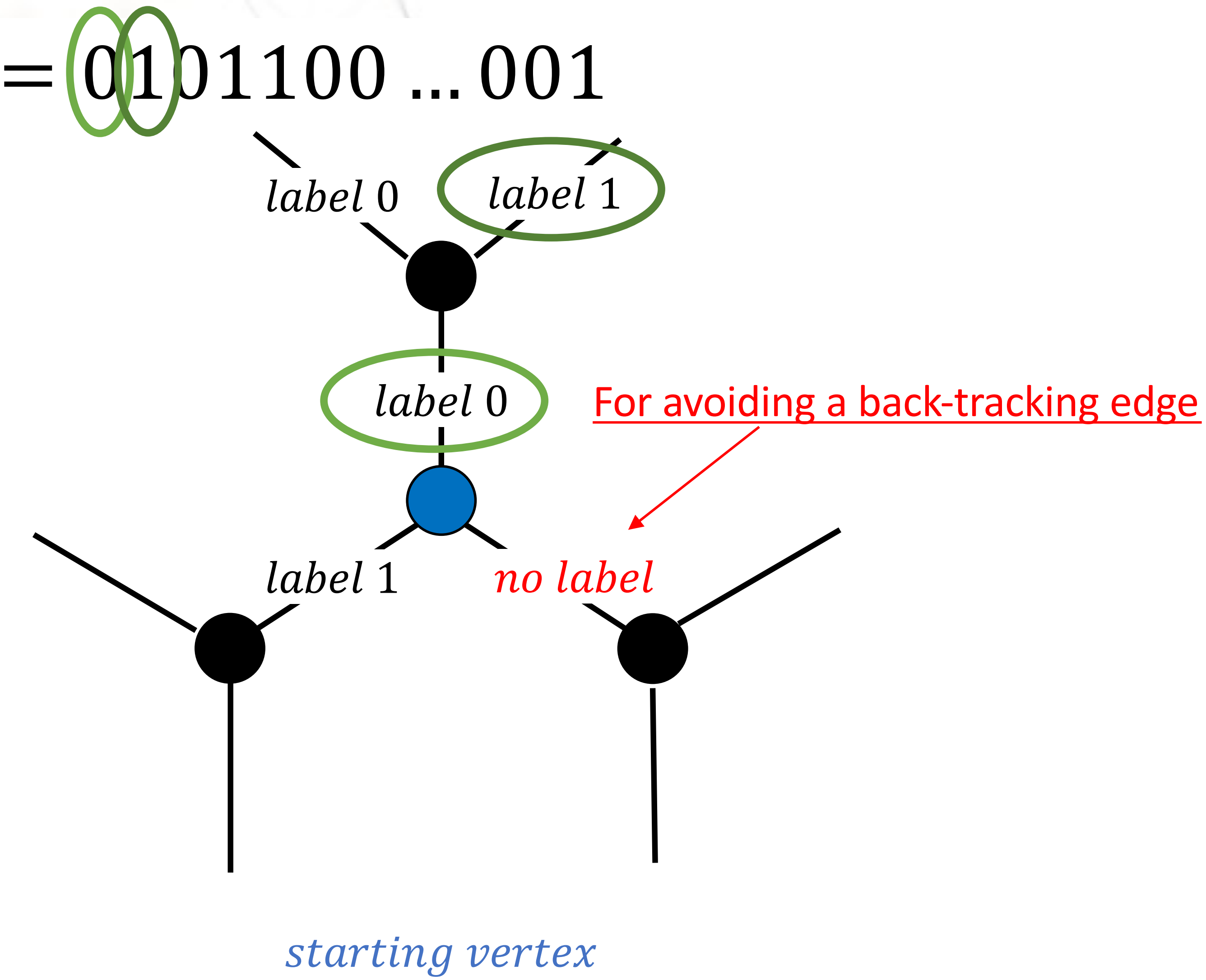
$S^{-1} = S \quad \Rightarrow$ Cay(G, S) is a regular directed graph of degree $|S|$.

$id \notin S \quad \Rightarrow$ Cay(G, S) does not allow loops.

How to walk on graphs

(in a sense of cryptographic hashing)

$$message = 0101100 \ldots 001$$



For avoiding a back-tracking edge

A hash function based on Cayley graphs:

Cayley hash function (how to label edges)

Informally, each bit of a given message transform into $s_{i_j} \in S$ *to walk around* $\mathrm{Cay}(G, S)$*,*

and its hash value is $g \in G$ *s.t.* $g = s_{i_1} s_{i_2} \cdots s_{i_k}$ *for some* $k \in \mathbb{N}$*.*

$p \overset{\mathrm{def}}{=} |S| - 1.$

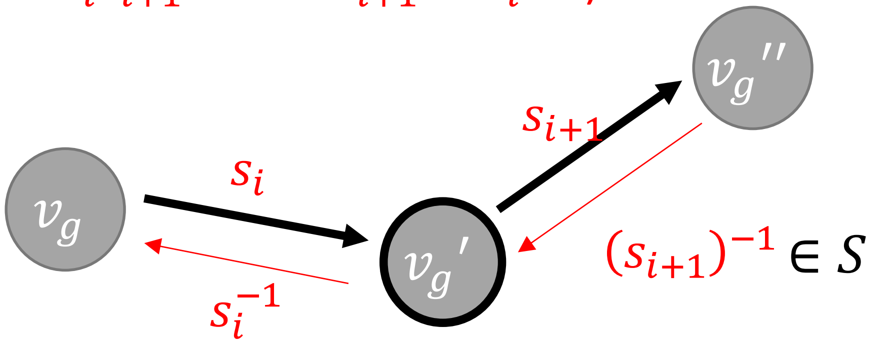
a *choice function*

$$\pi \colon [p] \times S \longrightarrow S$$

such that, $\forall s \in S, \pi([p] \times \{s\}) = S \setminus \{s^{-1}\}$.

Here, $[p] \coloneqq \{1, \ldots, p\}$.

(To avoid trivial collisions $s_i s_{i+1}$ where $s_{i+1} = {s_i}^{-1}$.)



A hash function based on Cayley graphs:

Cayley hash function

- Input message $\mathbb{x}$:

a base-p number as $x_1 \dots x_\ell$ for some $\ell \in \mathbb{N}$.

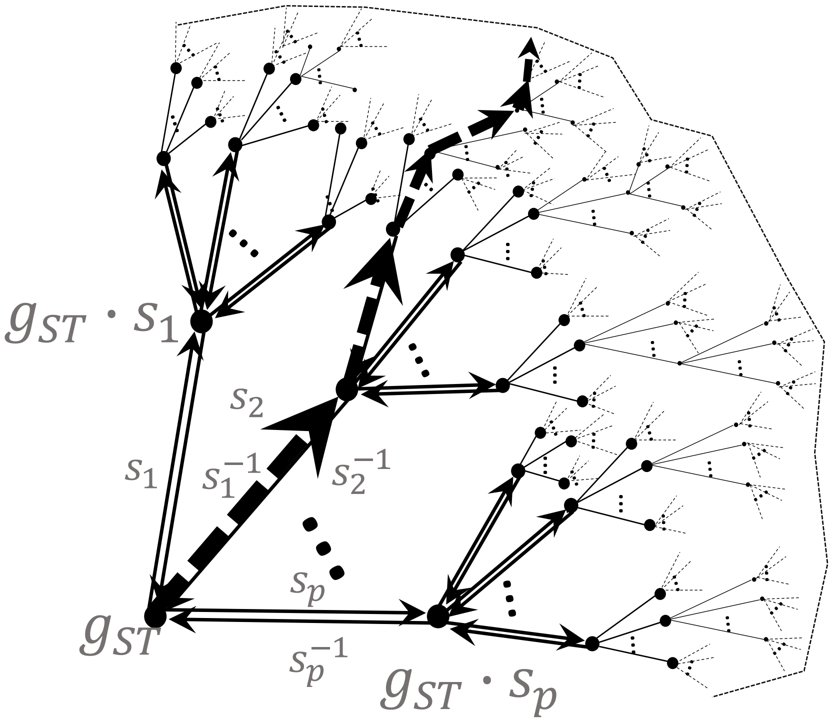
$\mathbb{x} = x_1 \dots x_\ell, x_i \in [p]$.

- Hash function $H : [p]^* \to G$

Define $(s_1, s_2, \dots, s_\ell)$ inductively as follows

$s_i = \pi(x_i, s_{i-1}), i \in \{1, \dots, \ell\}$

$H(\mathbb{x}) = H(x_1 \dots x_\ell) = g_{SV}\ s_1 \dots s_\ell$,



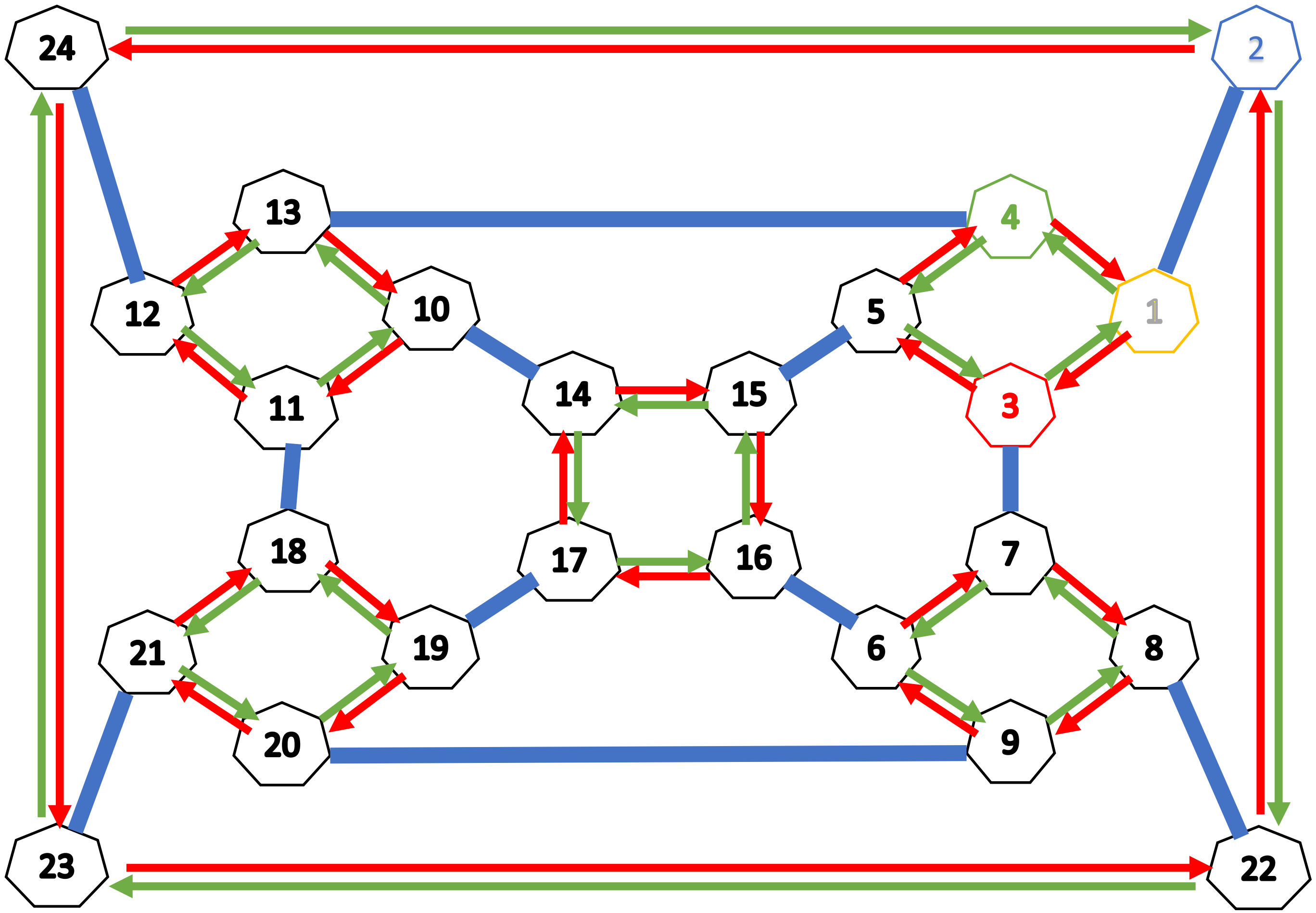
Here, $s_0 := g_{ST}$ (the starting vertex) : some fixed element of G.

$$\boxed{s_0 \xrightarrow{s_1} s_0 s_1 \xrightarrow{s_2} s_0 s_1 s_2 \to \cdots \xrightarrow{s_\ell} s_0 s_1 s_2 \dots s_\ell}$$

A Toy Example of Cayley Hash Functions

1. $\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}$
2. $\begin{bmatrix}1 & 0\\0 & 2\end{bmatrix}$
3. $\begin{bmatrix}0 & 1\\1 & 1\end{bmatrix}$
4. $\begin{bmatrix}1 & 2\\2 & 0\end{bmatrix}$
5. $\begin{bmatrix}1 & 1\\1 & 2\end{bmatrix}$
6. $\begin{bmatrix}2 & 0\\1 & 1\end{bmatrix}$
7. $\begin{bmatrix}0 & 1\\2 & 1\end{bmatrix}$
8. $\begin{bmatrix}1 & 1\\1 & 0\end{bmatrix}$
9. $\begin{bmatrix}1 & 2\\0 & 1\end{bmatrix}$
10. $\begin{bmatrix}2 & 1\\0 & 1\end{bmatrix}$
11. $\begin{bmatrix}1 & 0\\1 & 1\end{bmatrix}$
12. $\begin{bmatrix}0 & 1\\1 & 2\end{bmatrix}$
13. $\begin{bmatrix}1 & 1\\2 & 0\end{bmatrix}$
14. $\begin{bmatrix}1 & 1\\0 & 1\end{bmatrix}$
15. $\begin{bmatrix}1 & 2\\1 & 1\end{bmatrix}$
16. $\begin{bmatrix}1 & 0\\2 & 1\end{bmatrix}$
17. $\begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}$
18. $\begin{bmatrix}1 & 0\\1 & 2\end{bmatrix}$
19. $\begin{bmatrix}0 & 2\\1 & 0\end{bmatrix}$
20. $\begin{bmatrix}1 & 1\\0 & 2\end{bmatrix}$
21. $\begin{bmatrix}2 & 1\\1 & 1\end{bmatrix}$
22. $\begin{bmatrix}1 & 2\\1 & 0\end{bmatrix}$
23. $\begin{bmatrix}1 & 1\\2 & 1\end{bmatrix}$
24. $\begin{bmatrix}0 & 2\\1 & 1\end{bmatrix}$

- $\mathrm{PGL}(2, \mathbb{Z}/3\mathbb{Z})$, $S = \{s_0 \coloneqq \begin{bmatrix}1 & 0\\0 & 2\end{bmatrix}, s_1 \coloneqq \begin{bmatrix}0 & 1\\1 & 1\end{bmatrix}, s_2 := \begin{bmatrix}1 & 2\\2 & 0\end{bmatrix}\}$



$$s_0 = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, s_1 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, s_2 = \begin{pmatrix} 1 & 2 \\ 2 & 0 \end{pmatrix}$$

$$s_0 s_0 = id, \qquad s_1 s_2 = id, \qquad s_2 s_1 = id$$

Choice function π.

$\pi: \{0,1\} \times S \longrightarrow S$ such that, $\forall s \in S, \pi(\{0,1\} \times \{s\}) = S \setminus \{s^{-1}\}$.

$$\pi(0, s_0) = s_1$$

$$\pi(1, s_0) = s_2$$

$$\pi(0, s_1) = s_0$$

$$\pi(1, s_1) = s_1$$

$$\pi(0, s_2) = s_0$$

$$\pi(1, s_2) = s_2$$

$$S := \left\{ s_0 = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, s_1 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, s_2 = \begin{pmatrix} 1 & 2 \\ 2 & 0 \end{pmatrix} \right\}$$

message
$\mathbb{x} = 10110100$

$\pi(0, s_0) = s_1$

$\pi(1, s_0) = s_2$

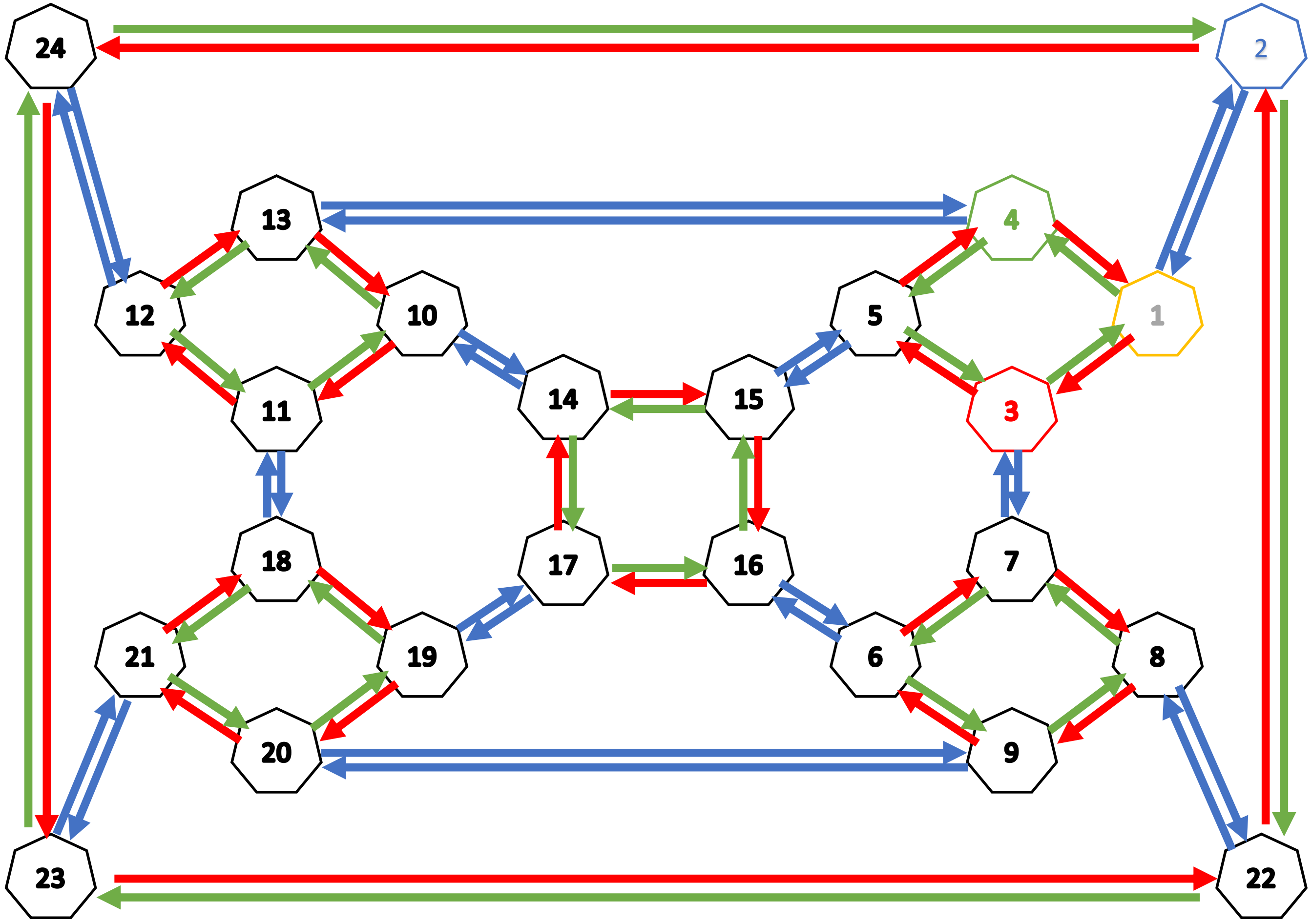
$\pi(0, s_1) = s_0$

$\pi(1, s_1) = s_1$

$\pi(0, s_2) = s_0$

$\pi(1, s_2) = s_2$

$H(\mathbb{x}) =$



$$S := \left\{ s_0 = \begin{pmatrix}1 & 0\\0 & 2\end{pmatrix}, s_1 = \begin{pmatrix}0 & 1\\1 & 1\end{pmatrix}, s_2 = \begin{pmatrix}1 & 2\\2 & 0\end{pmatrix} \right\}$$

message
$\mathbb{x} = 10110100$

$\pi(0, s_0) = s_1$

$\pi(1, s_0) = s_2$

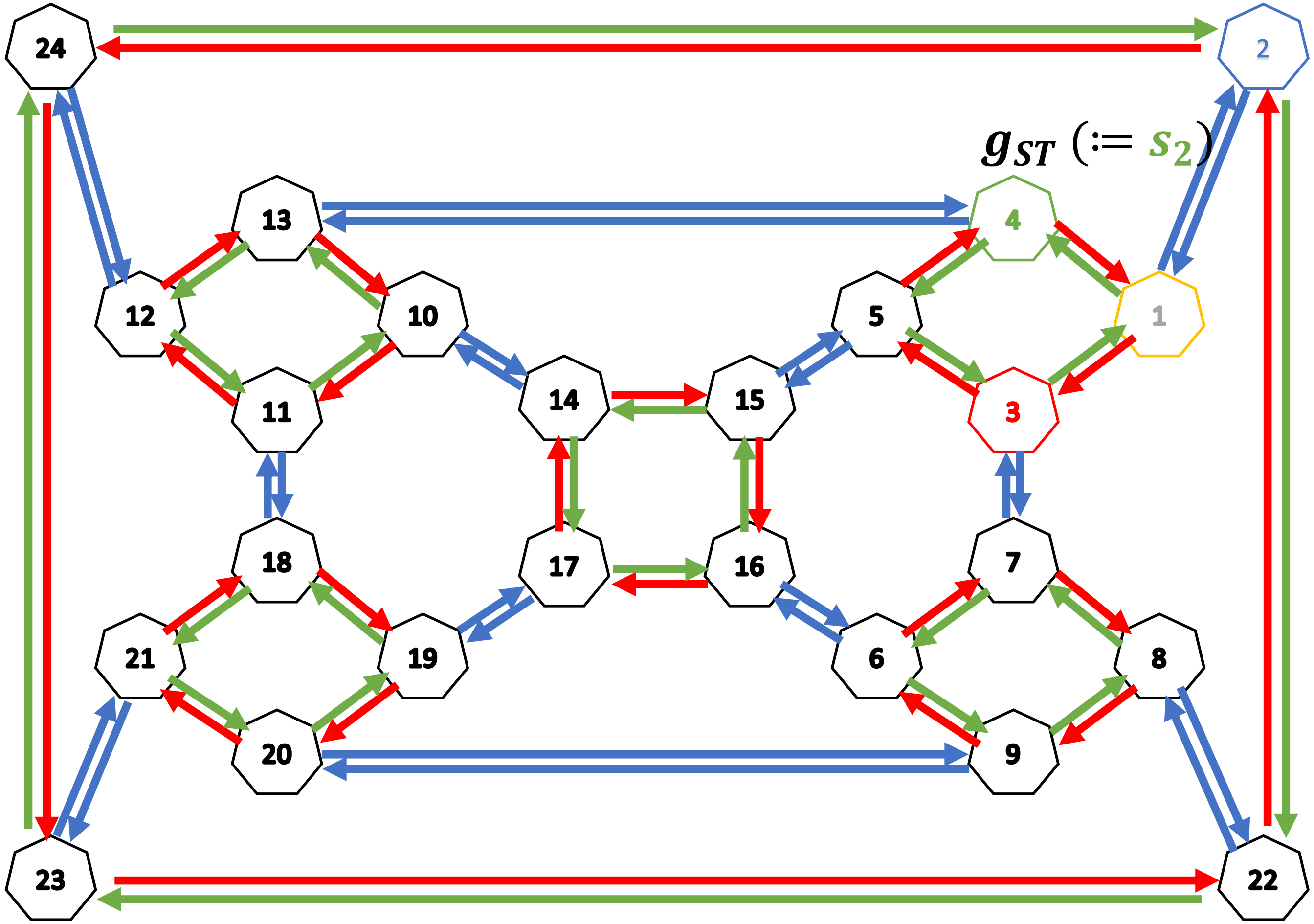
$\pi(0, s_1) = s_0$

$\pi(1, s_1) = s_1$

$\pi(0, s_2) = s_0$

$\pi(1, s_2) = s_2$

$H(\mathbb{x}) = g_{ST}$



$$S \coloneqq \left\{ s_0 = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, s_1 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, s_2 = \begin{pmatrix} 1 & 2 \\ 2 & 0 \end{pmatrix} \right\}$$

message

$\mathbb{x} = 10110100$

$\pi(0, s_0) = s_1$

$\pi(1, s_0) = s_2$

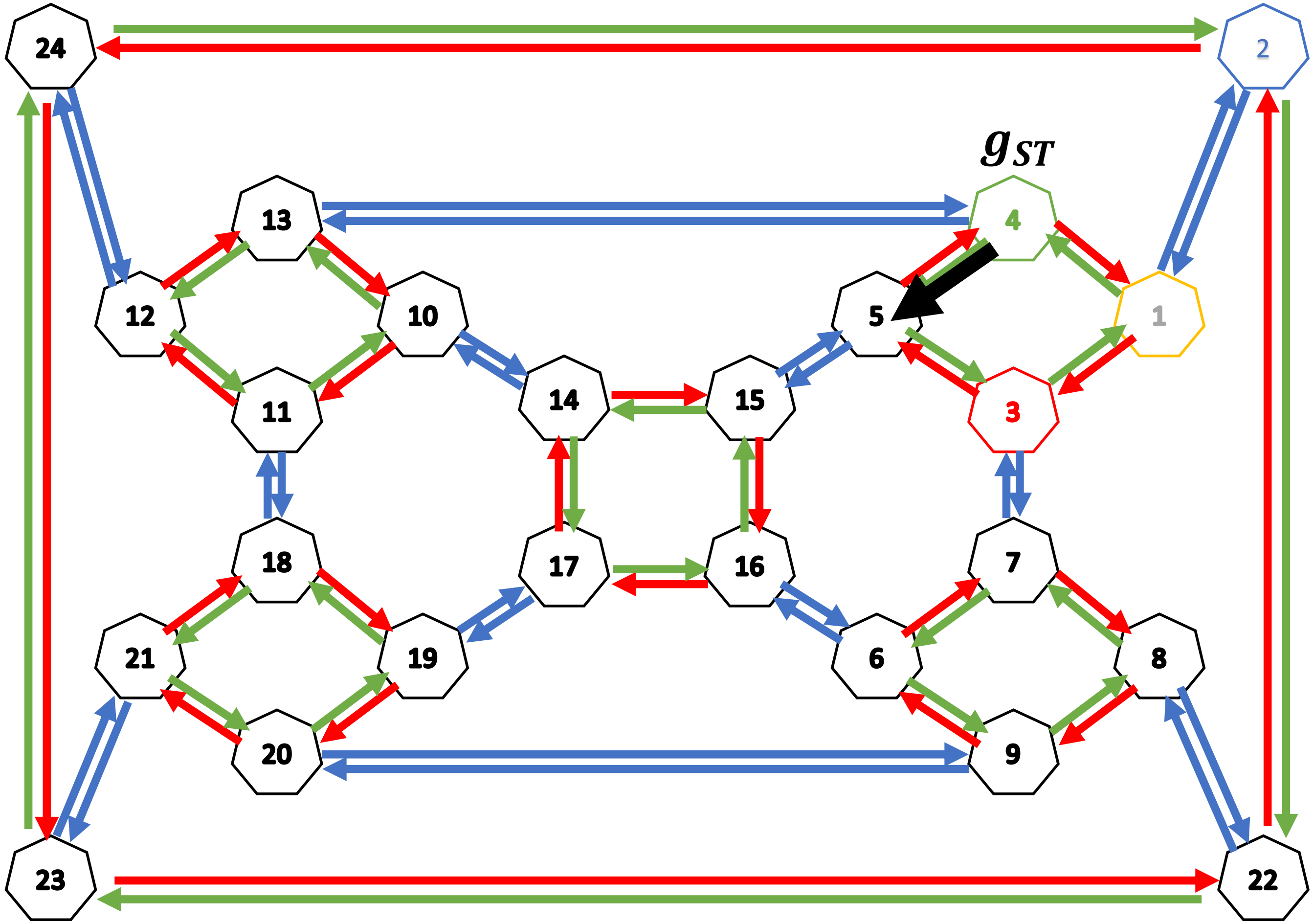
$\pi(0, s_1) = s_0$

$\pi(1, s_1) = s_1$

$\pi(0, s_2) = s_0$

$\boxed{\pi(1, s_2) = s_2}$

$H(\mathbb{x}) = g_{ST} s_2$



$$S \coloneqq \left\{ s_0 = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, s_1 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, s_2 = \begin{pmatrix} 1 & 2 \\ 2 & 0 \end{pmatrix} \right\}$$

message

$\mathbb{x} = 10110100$

$\pi(0, s_0) = s_1$

$\pi(1, s_0) = s_2$

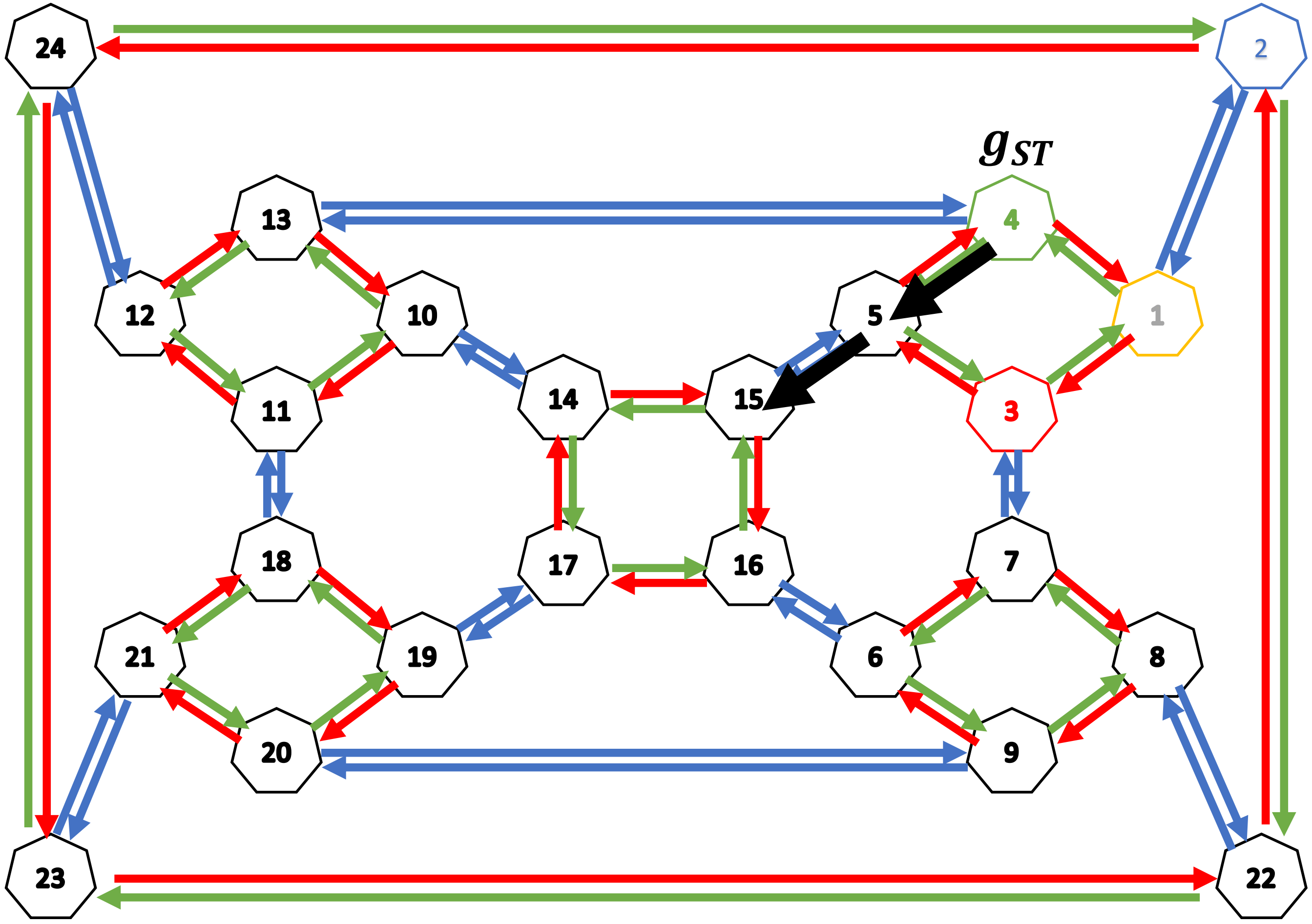
$\pi(0, s_1) = s_0$

$\pi(1, s_1) = s_1$

$\boxed{\pi(0, s_2) = s_0}$

$\pi(1, s_2) = s_2$

$H(\mathbb{x}) = g_{ST} s_2 s_0$



$$S \coloneqq \left\{ s_0 = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, s_1 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, s_2 = \begin{pmatrix} 1 & 2 \\ 2 & 0 \end{pmatrix} \right\}$$

message
$\mathbb{x} = 10110100$

$\pi(0, s_0) = s_1$

$\boxed{\pi(1, s_0) = s_2}$

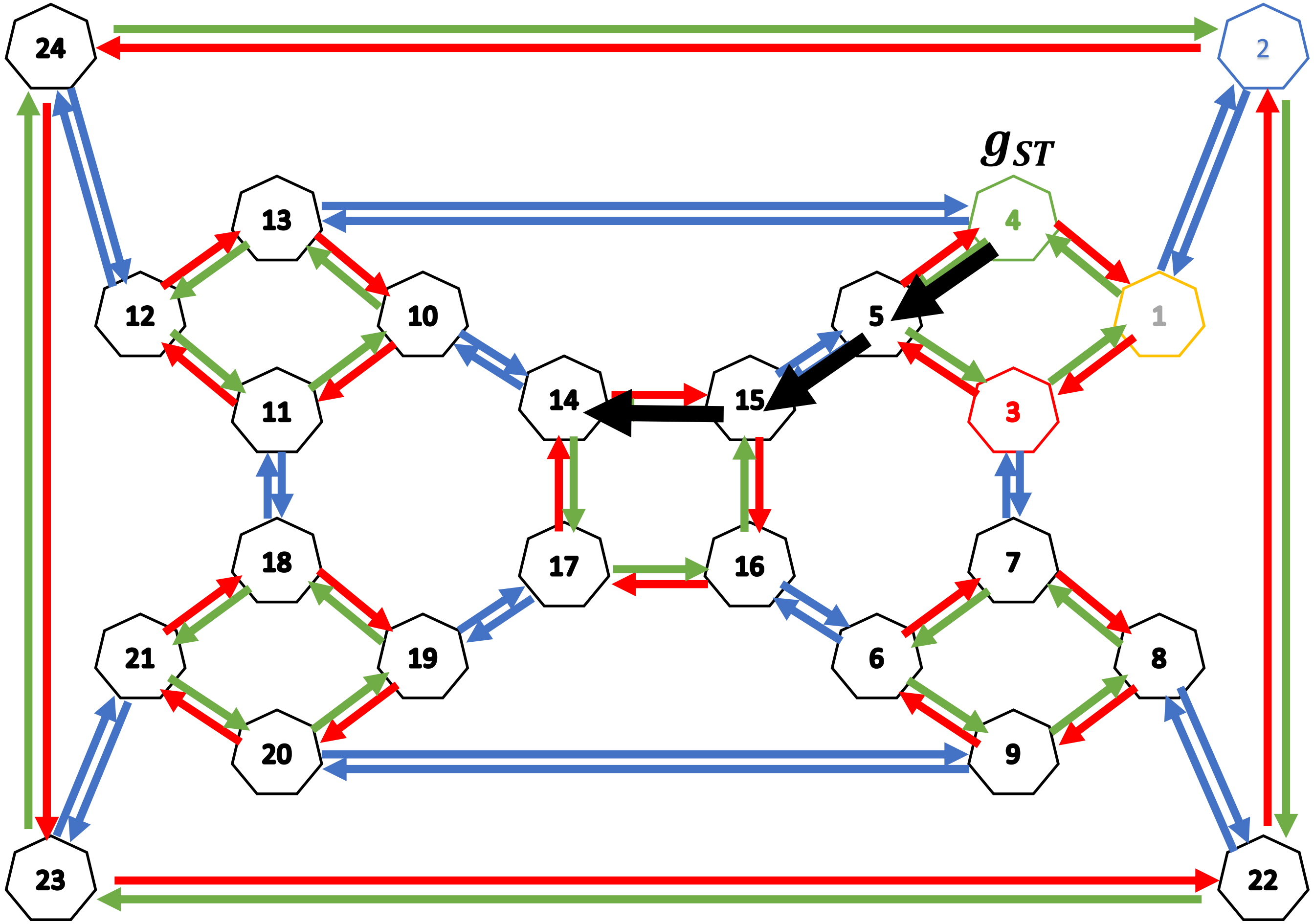
$\pi(0, s_1) = s_0$

$\pi(1, s_1) = s_1$

$\pi(0, s_2) = s_0$

$\pi(1, s_2) = s_2$

$H(\mathbb{x}) = g_{ST} s_2 s_0 s_2$



$$S \coloneqq \left\{ s_0 = \begin{pmatrix}1 & 0\\ 0 & 2\end{pmatrix}, s_1 = \begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix}, s_2 = \begin{pmatrix}1 & 2\\ 2 & 0\end{pmatrix} \right\}$$

message

$\mathbb{x} = 10110100$

$\pi(0, s_0) = s_1$

$\pi(1, s_0) = s_2$

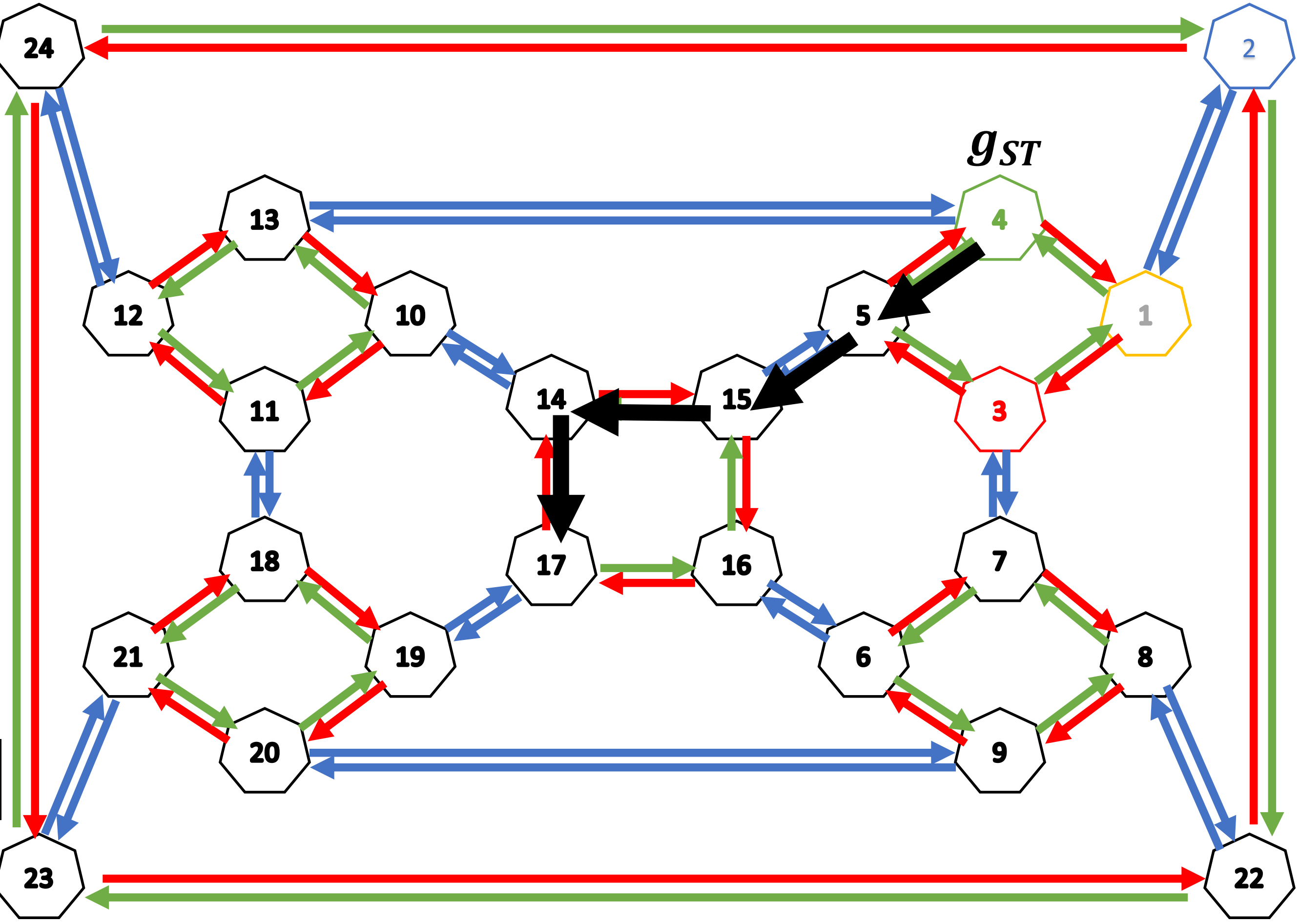
$\pi(0, s_1) = s_0$

$\pi(1, s_1) = s_1$

$\pi(0, s_2) = s_0$

$\boxed{\pi(1, s_2) = s_2}$

$H(\mathbb{x}) = g_{ST} s_2 s_0 s_2 s_2$



$$S \coloneqq \left\{ s_0 = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, s_1 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, s_2 = \begin{pmatrix} 1 & 2 \\ 2 & 0 \end{pmatrix} \right\}$$

message

$\mathbb{x} = 10110100$

$\pi(0, s_0) = s_1$

$\pi(1, s_0) = s_2$

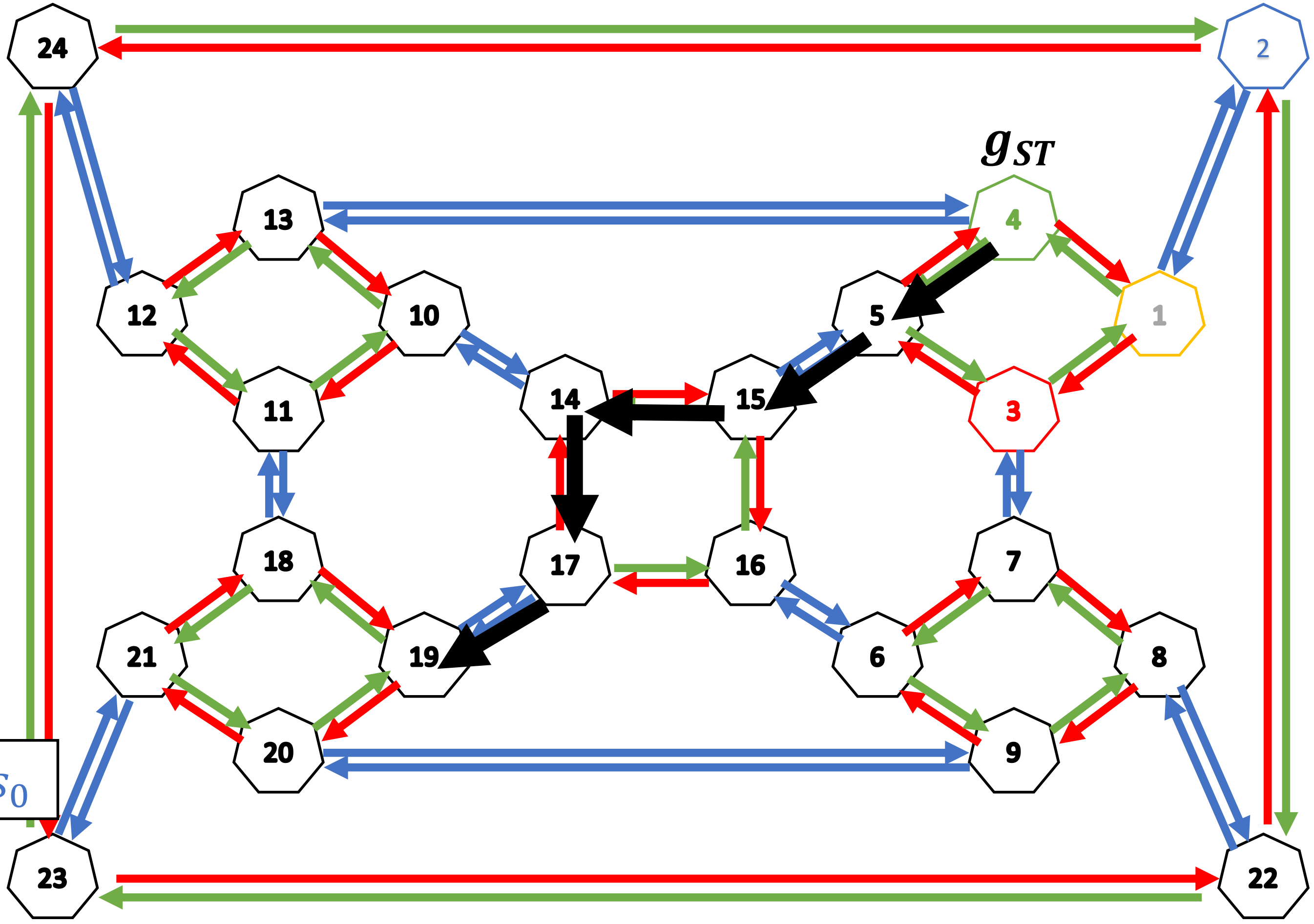
$\pi(0, s_1) = s_0$

$\pi(1, s_1) = s_1$

$\boxed{\pi(0, s_2) = s_0}$

$\pi(1, s_2) = s_2$

$H(\mathbb{x}) = g_{ST} s_2 s_0 s_2 s_2 s_0$



$$S := \left\{ s_0 = \begin{pmatrix}1 & 0\\ 0 & 2\end{pmatrix}, s_1 = \begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix}, s_2 = \begin{pmatrix}1 & 2\\ 2 & 0\end{pmatrix} \right\}$$

message

$\mathbb{x} = 10110\textcircled{1}00$

$\pi(0, s_0) = s_1$

$\boxed{\pi(1, s_0) = \textcircled{s_2}}$

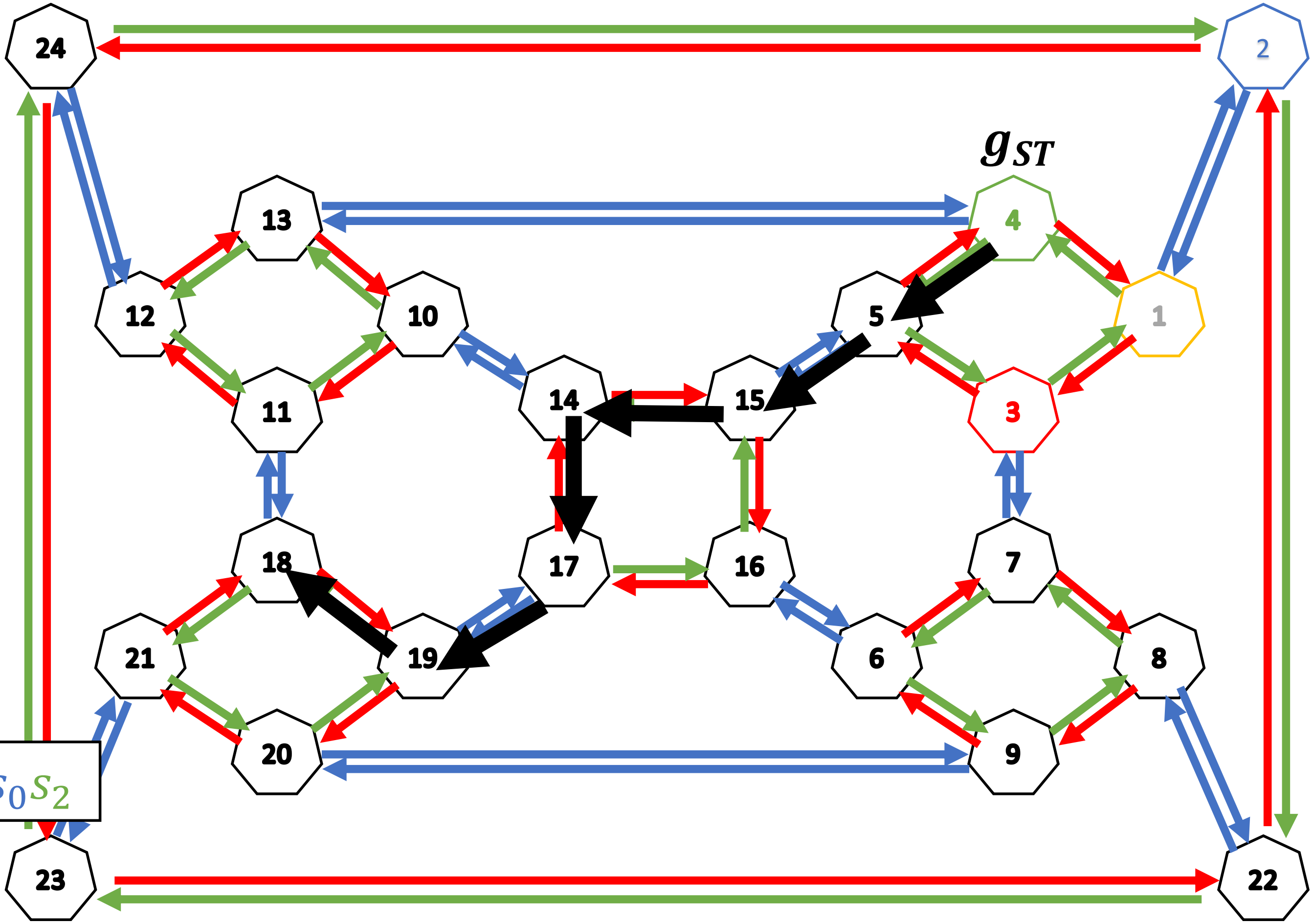
$\pi(0, s_1) = s_0$

$\pi(1, s_1) = s_1$

$\pi(0, s_2) = s_0$

$\pi(1, s_2) = s_2$

$H(\mathbb{x}) = g_{ST} s_2 s_0 s_2 s_2 s_0 s_2$



$$S \coloneqq \left\{ s_0 = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, s_1 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, s_2 = \begin{pmatrix} 1 & 2 \\ 2 & 0 \end{pmatrix} \right\}$$

message

$\mathbb{x} = 10110100$

$\pi(0, s_0) = s_1$

$\pi(1, s_0) = s_2$

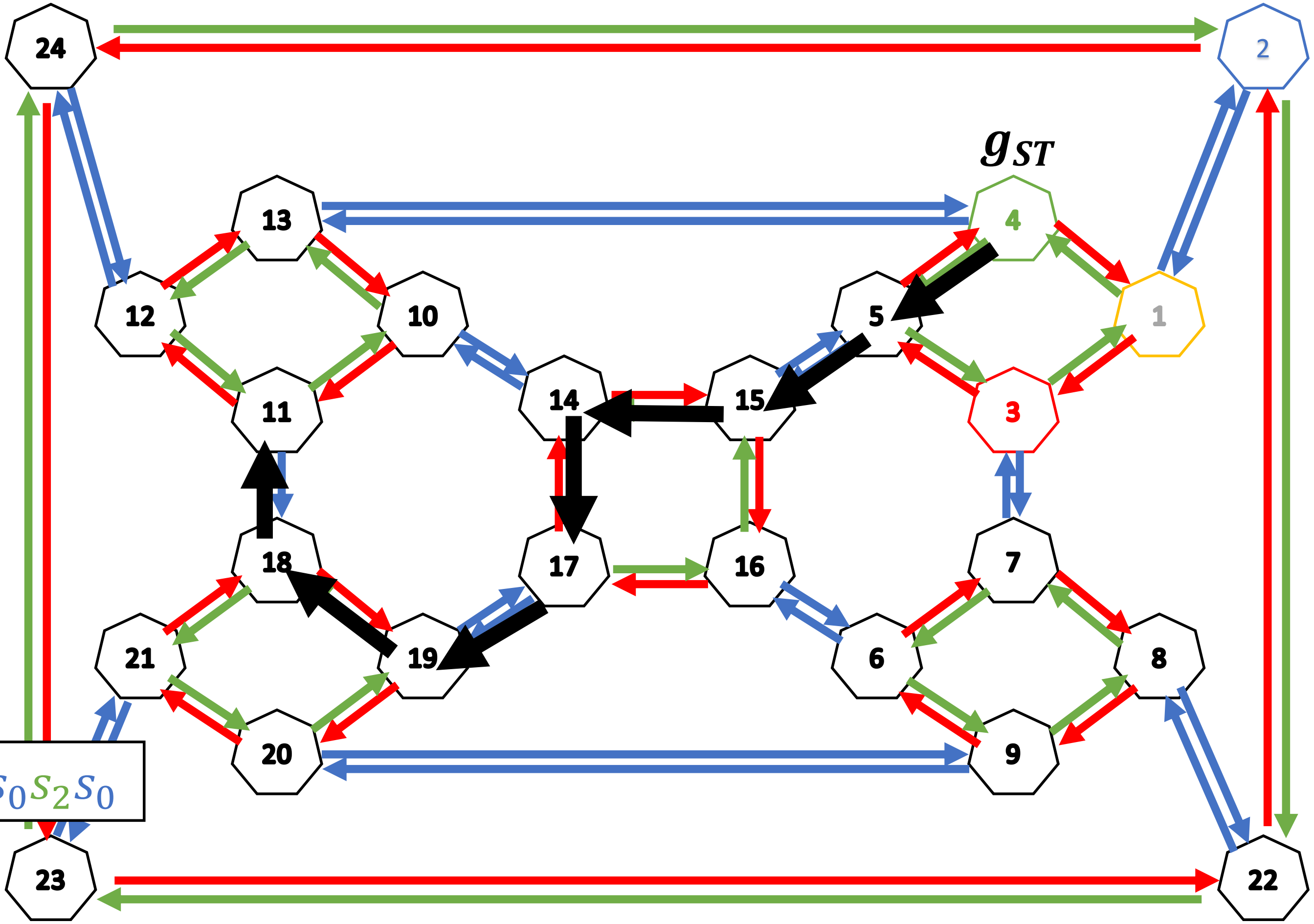
$\pi(0, s_1) = s_0$

$\pi(1, s_1) = s_1$

$\boxed{\pi(0, s_2) = s_0}$

$\pi(1, s_2) = s_2$

$H(\mathbb{x}) = g_{ST} s_2 s_0 s_2 s_2 s_0 s_2 s_0$



$$S \coloneqq \left\{ s_0 = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, s_1 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, s_2 = \begin{pmatrix} 1 & 2 \\ 2 & 0 \end{pmatrix} \right\}$$

message

$\mathbb{x} = 10110100$

$\boxed{\pi(0, s_0) = s_1}$

$\pi(1, s_0) = s_2$

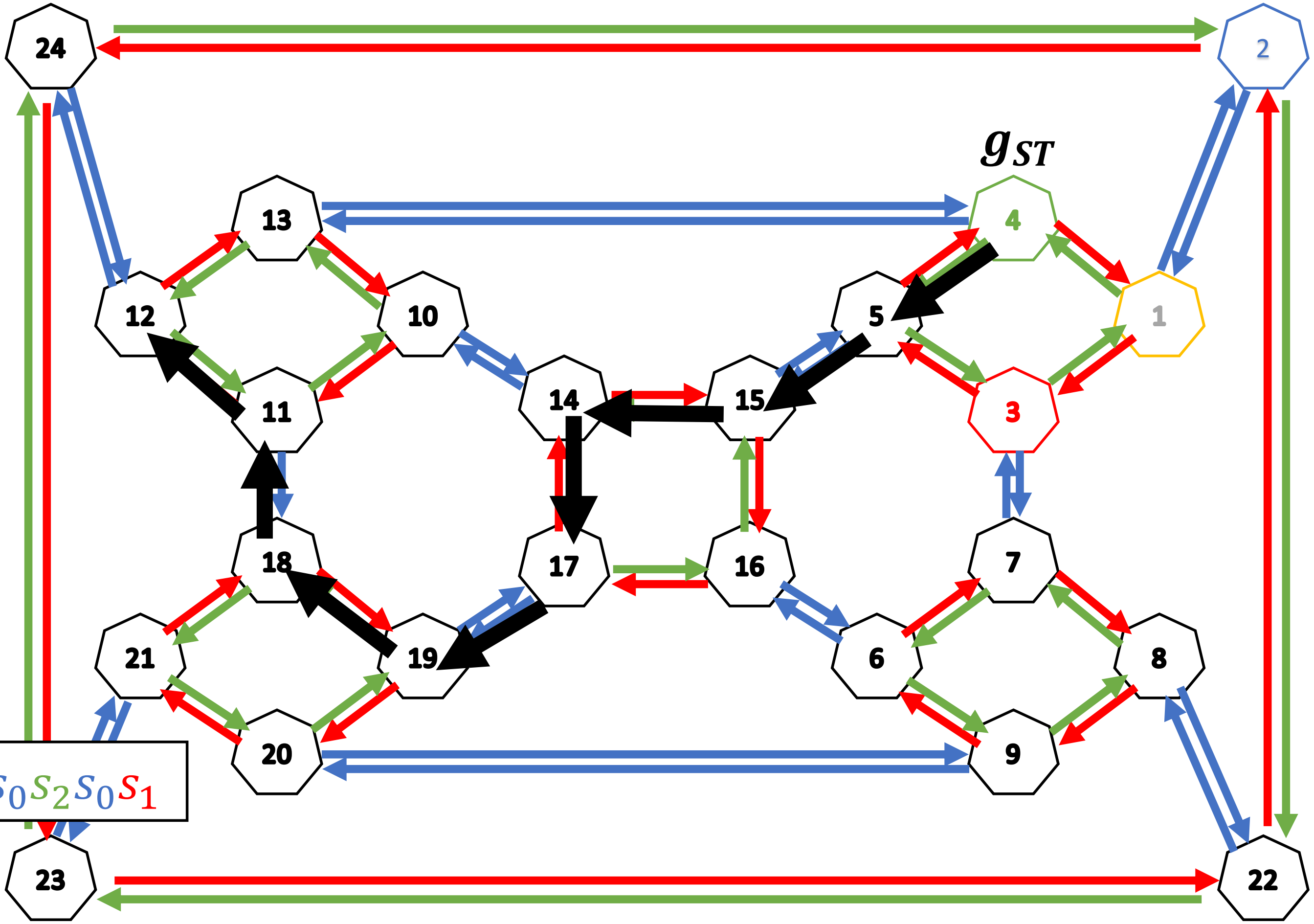
$\pi(0, s_1) = s_0$

$\pi(1, s_1) = s_1$

$\pi(0, s_2) = s_0$

$\pi(1, s_2) = s_2$

$H(\mathbb{x}) = g_{ST} s_2 s_0 s_2 s_2 s_0 s_2 s_0 s_1$



$$S \coloneqq \left\{ s_0 = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, s_1 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, s_2 = \begin{pmatrix} 1 & 2 \\ 2 & 0 \end{pmatrix} \right\}$$

message
$\mathbb{x} = 10110100$

$\pi(0, s_0) = s_1$

$\pi(1, s_0) = s_2$

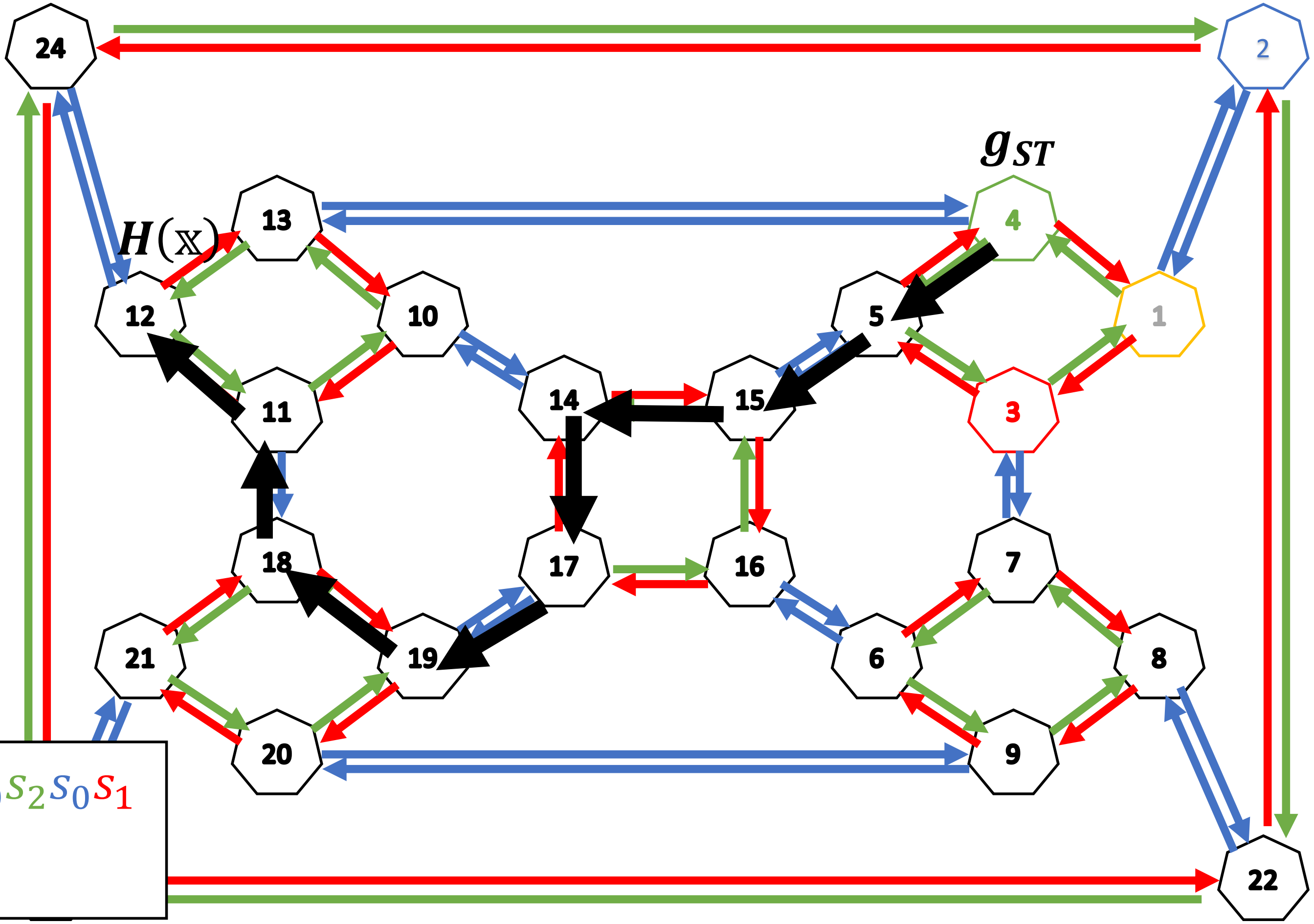
$\pi(0, s_1) = s_0$

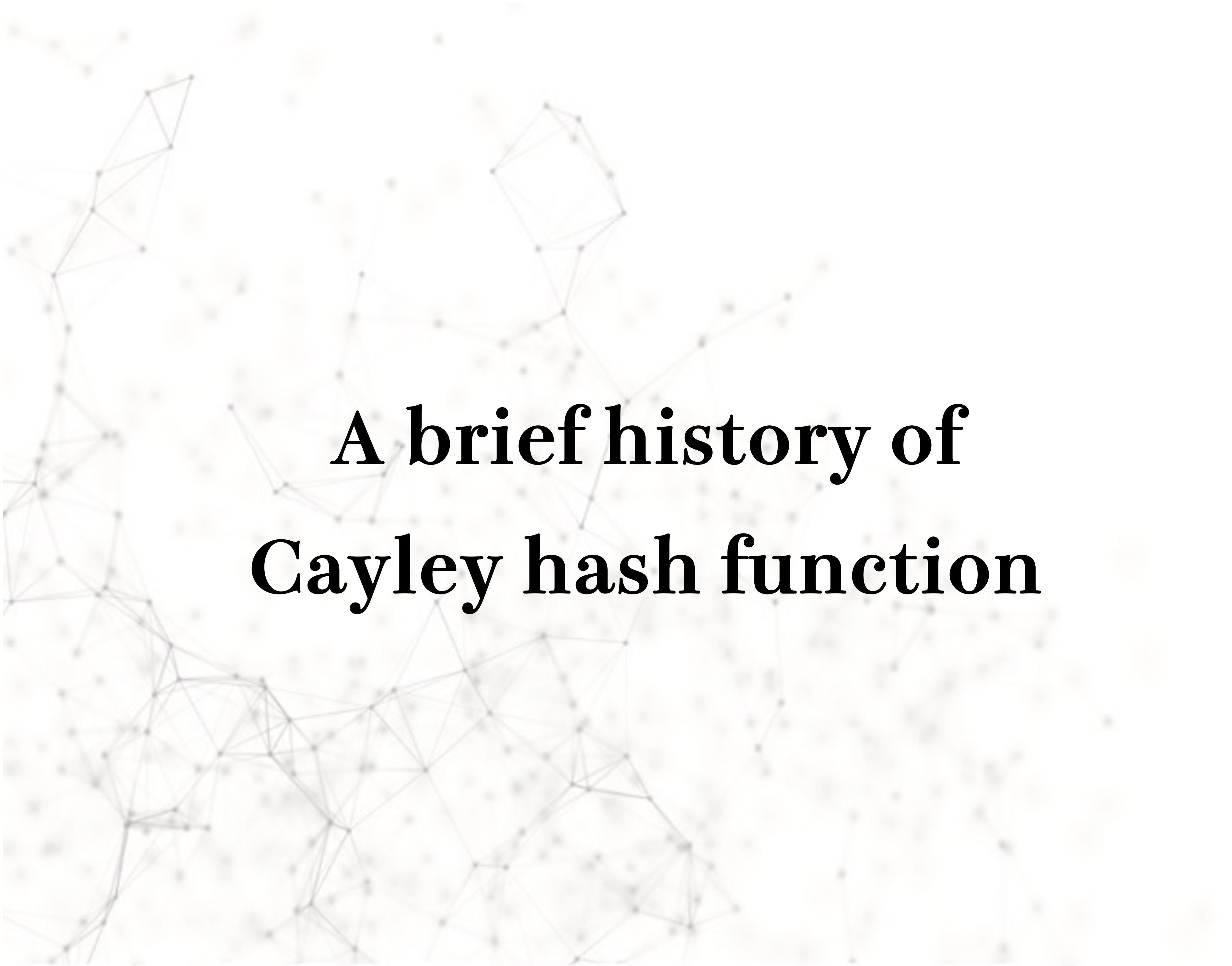
$\pi(1, s_1) = s_1$

$\pi(0, s_2) = s_0$

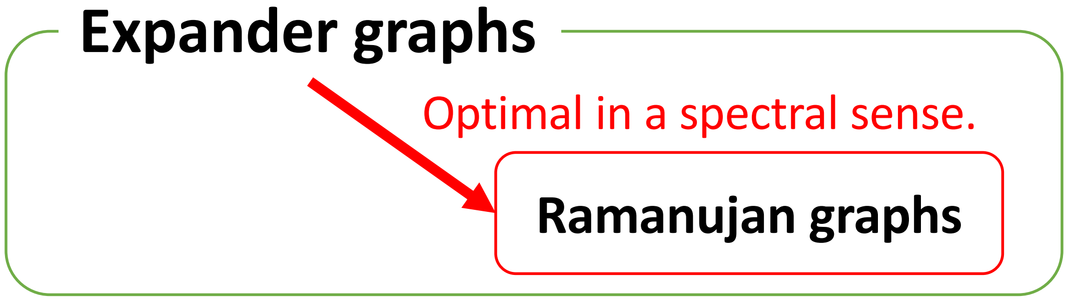
$\pi(1, s_2) = s_2$

$H(\mathbb{x}) = s_2 s_2 s_0 s_2 s_2 s_0 s_2 s_0 s_1$
$= \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}$





A brief history of Cayley hash function



Expander graphs

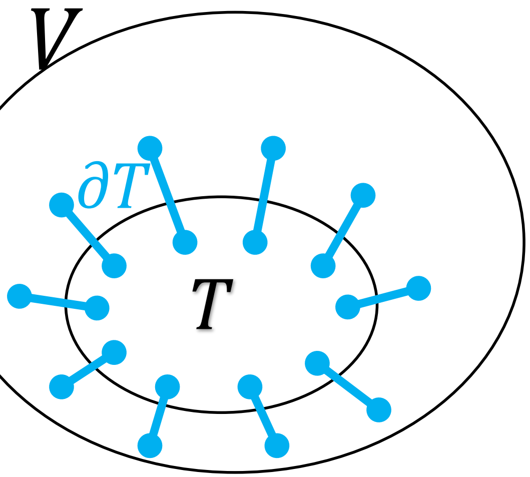
Optimal in a spectral sense.

Ramanujan graphs

✓ *uniform distribution.*

✓ *“sparse graphs with*
strong connectivity property”.

$X=(V,E)$: a finite, connected, k-regular graph.



- Expanding constant :

$$h(X)=\inf\left\{\frac{|\partial T|}{|T|}: T\subseteq V, 0<|T|\leq\frac{|V|}{2}\right\},$$

where $\partial T=\{(x,y)\in E|x\in T \text{ and } y\in V\setminus \mathrm{T}\}$.

- λ_1 : Second largest eigenvalues of an adjacency matrix of X.

Theorem (Alon-Milman (1985))

$$\frac{k-\lambda_1}{2}\leq h(X)\leq\sqrt{2k(k-\lambda_1)}$$

($k-\lambda_1$: the spectral gap).

λ_1: small ⟷ $k-\lambda_1$: big ⟶ $h(X)$: big!

Ramanujan graphs

Theorem (Alon-Boppana)

$(X_j)_{j\geq 1}$: a family of k-regular graphs with $|V_j| \to \infty \ (j \to \infty)$,

$$\lim_{j\to\infty} inf\, \lambda_1\,(X_j) \geq 2\sqrt{k-1}$$

Definition

$X = (V, E)$: a finite, connected, k-regular graph is *Ramanujan graph,*

if it satisfies

$$\lambda_1(X) \leq 2\sqrt{k-1}$$

We call $2\sqrt{k-1}$ *Ramanujan bound (RB)*.

A brief history of Cayley hash functions.

Zémor [Z91]	• $SL_2(\mathbb{F}_p)$, $s_0 = \begin{pmatrix}1 & 1\\0 & 1\end{pmatrix}, s_1 = \begin{pmatrix}1 & 0\\1 & 1\end{pmatrix}$	Broken
Zémor-Tillich [ZT94]	• $SL_2(\mathbb{F}_{2^n})$, $s_0 = \begin{bmatrix}X & 1\\1 & 0\end{bmatrix}, s_1 = \begin{bmatrix}X & X+1\\1 & 1\end{bmatrix}$	Broken
ZesT [PQ09]	• $SL_2(\mathbb{F}_{2^n})$, the vectorial version of the ZT hash ftn.	Assume to be broken
LPS [CGL09]	• $PSL_2(\mathbb{F}_p)$, Using Lubotzky-Phillips-Sarnak Ramanujan graphs *Combinatorica* ‘88 .	Broken
Morgenstern [PLQ07]	• $PSL_2(\mathbb{F}_{p^n})$, Using generalized graphs of LPS graphs. *J. Combinatorial Theory* ‘94 .	Broken
Cubic [JPT17]	• $PSL_2(\mathbb{F}_p)$, Using cubic Ramanujan graphs by P. Chiu *Combinatorica* ‘92 .	Broken
Navigation [BSC17]	• $SL_2(\mathbb{F}_p)$, $A(a) = \begin{bmatrix}1 & a\\0 & 1\end{bmatrix}, B(b) = \begin{bmatrix}1 & 0\\b & 1\end{bmatrix}$ $(a, b > 1)$	Not broken
GL_2 [TNS20]	• $GL_2(\mathbb{F}_{p^n})$, refer to [TNS20].	Not broken
Arc-transitive [SJ22]	• $PGL_2(\mathbb{F}_p)$, Using arc-transitive graphs (triplet graph/ sextet graph).	Not broken
Left-Right Cay [AJS23]	• $SL_2(\mathbb{F}_p)$, Using Left-Right Cayley complex. (with Navigation elements)	Not broken

Ex) Lifting attack against [Z91]

$$G = SL_2(\mathbb{F}_p),\ S = \left\{ s_0 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, s_1 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \right\}$$

The Lifting Attack by Tillich- Zémor [ZT94]

For a given $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{F}_p),$ compute a lifting $\begin{bmatrix} A & B \\ C & D \end{bmatrix} \in SL_2(\mathbb{Z})$.

Factor $\begin{bmatrix} A & B \\ C & D \end{bmatrix}$ as a product of $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ and $\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ on $SL_2(\mathbb{Z})$ by using Euclidean algorithm (continued fraction).

On security of Cayley hash function

Group word problem

$L(\approx \log|G|) \in \mathbb{N}$.

G : a finite group,

S : a generating set

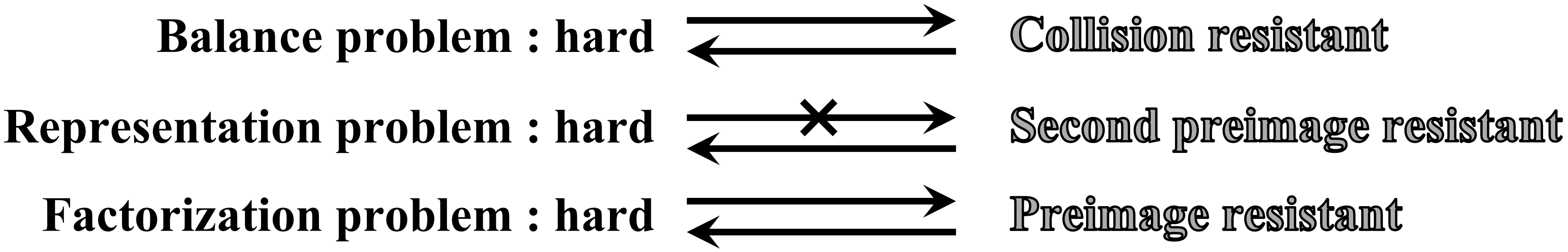
$\prod s_{m_i} = s_{m_1} s_{m_2} \cdots s_{m_\ell}$ such that $s_{m_1}, s_{m_2}, \cdots, s_{m_\ell} \in S$.

- **Balance problem**
  : Find an "*efficient*" algorithm that returns two words $m_1 \cdots m_\ell$ and $m'_1 \cdots m'_{\ell'}$, with $\ell, \ell' < L$, $m_i, m'_i \in \{0, \ldots, p-1\}$ and $\prod s_{m_i} = \prod s_{m'_i}$.
- **Representation problem**
  : Find an "*efficient*" algorithm that returns a word $m_1 \cdots m_\ell$ with $\ell < L$, $m_i \in \{0, \ldots, p-1\}$ and $\prod s_{m_i} = id$.
- **Factorization problem**
  : Find an "*efficient*" algorithm that given any element $g \in G$, returns a word $m_1 \cdots m_\ell$ with $\ell < L$, $m_i \in \{0, \ldots, p-1\}$ and $\prod s_{m_i} = g$.

Correspondence

Group word problems

Cayley hash function



Balance problem : hard

Representation problem : hard

Factorization problem : hard

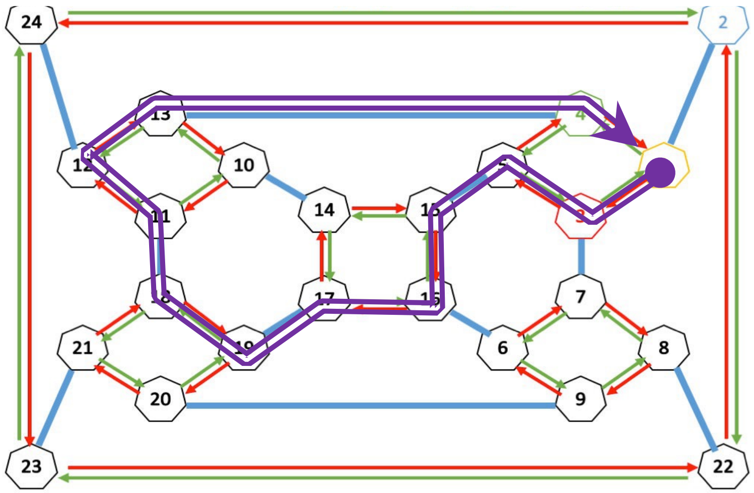
Collision resistant

Second preimage resistant

Preimage resistant

Security and large girth

Representation problem
: Find an "*efficient*" algorithm that returns a word $m_1 \cdots m_\ell$ with $\ell < L$, $m_i \in \{0, \dots, p-1\}$ and $\prod s_{m_i} = id$.



Cycle in $\boldsymbol{Cay}(G, S)$

$$\underbrace{s_1 s_1 s_0 s_1 s_1 s_0 s_2 s_0 s_1 s_1 s_0 s_1}_{\ell = 12} = id$$

$$\underbrace{s_1 s_1 s_0 s_1 s_1 s_0}_{\ell/2 = 6} = \underbrace{s_1^{-1} s_0^{-1} s_1^{-1}\ s_1^{-1}\ s_0^{-1} s_2^{-1}}_{\ell/2 = 6}$$

Finding collisions of Cayley hash function.

- Large girth : the length of shortest cycles in a given graph.

Malleability

$$\mathcal{H}\ (m||m') = \mathcal{H}(m) \cdot \mathcal{H}(m')$$

- It gives the functionality of parallel computing.
- It can derive the vulnerabilities when used within protocols. [BCFW09]

Usually, Cayley hash functions has malleability.
It is one of the important tasks to achieve

“non-malleability”

for applications of Cayley hash functions to protocols widely.

Main objectives

1. Can we construct a secure graph-based hash function?

>> Heuristic cryptanalysis algorithms, so far… Maybe, Yes!

2. Are there new graphs with large girth?

>> It seems possible! There are some on-going works.

3. Is it possible to construct a hash function from graphs with multiple degrees?

>> In this talk, we suggest a new hash function based on THE graph.

Group-subgroup pair graph

Motivation of pair graphs

By its definition, Cayley graphs are intimately related to the right (or left) regular action of the group.

Since edges (g,h) of a Cayley graph satisfy

$$g = hs \text{ for } s \in S \ ,$$

left actions on vertices (edges) give graph automorphisms.

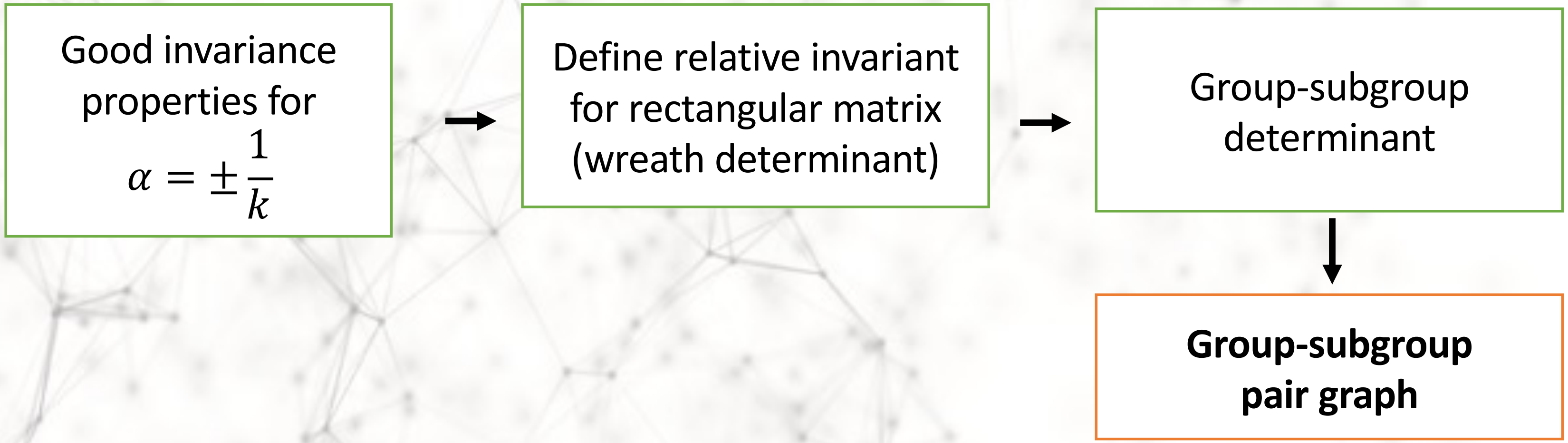
This is the reason why the spectrum of the Cayley graphs (and thus the expansion and other graphs properties) are determined by the representations of the group.

Motivation of pair graphs

One idea, coming from the study of invariant theory of the α-determinant, is to consider a weaker form of symmetry (a relative invariance).

$$\det^{(\alpha)} A = \sum_{\omega\in\mathfrak{S}_n} \alpha^{n-\nu(\omega)} a_{\omega(1),1}a_{\omega(2),2}\cdots a_{\omega(n),n}$$

In this case, it reduces to limiting the action to a subgroup of the group, resulting on the definition of group-subgroup pair graph.



Good invariance properties for $\alpha = \pm\frac{1}{k}$

Define relative invariant for rectangular matrix (wreath determinant)

Group-subgroup determinant

Group-subgroup pair graph

Pair-graph

Definition

G : a group

H : a subgroup of index $k+1$

For a subset $S \subset G$ s.t. $\boldsymbol{S \cap H}$ **: a symmetric set**

The ***group-subgroup pair graph*** (or ***pair-graph***) is

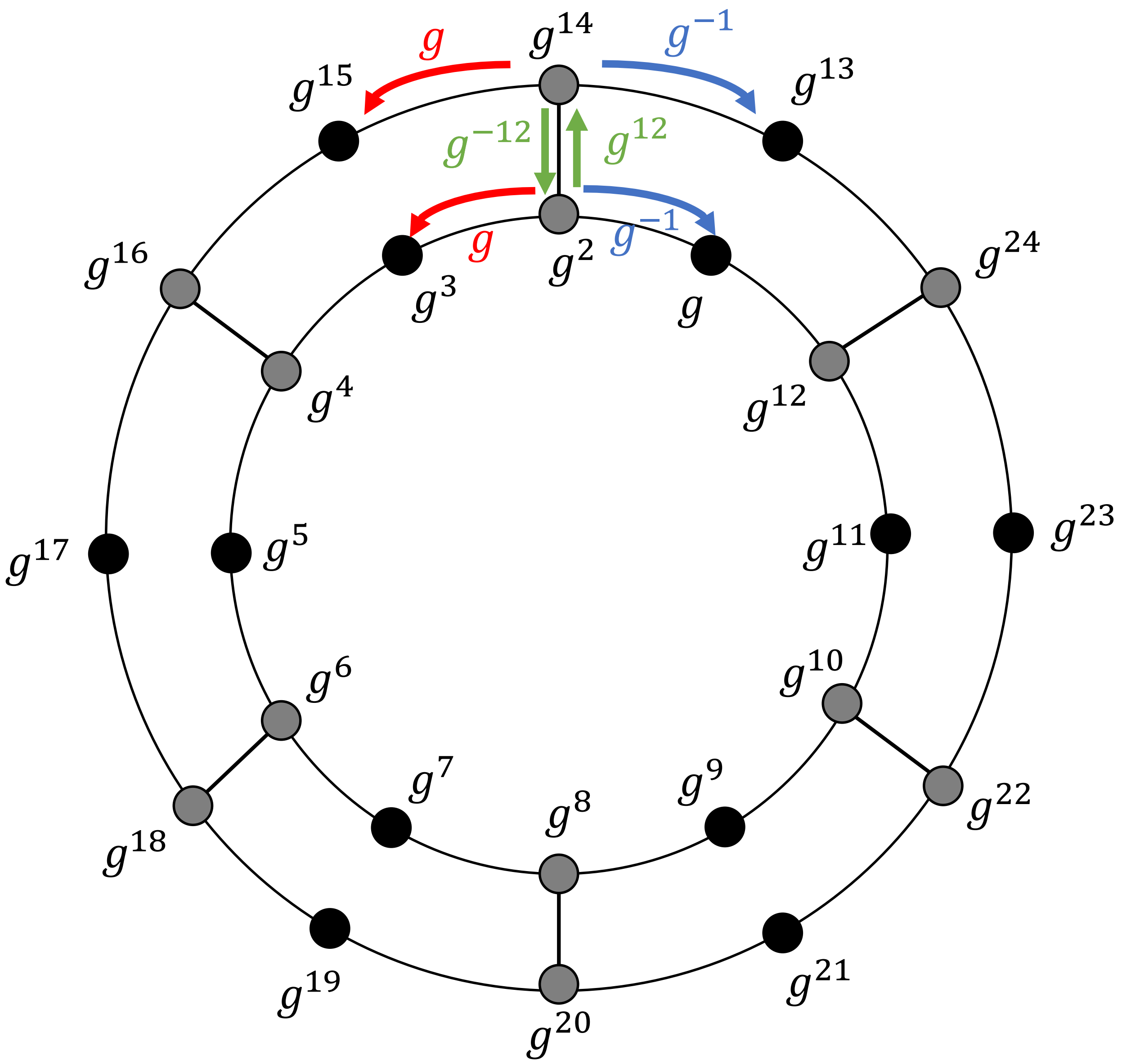
$$\mathcal{G}(G, H, S) = (V, E)$$

where

- Vertex-set $V : \{v_g | g \in G\}$

- Edge-set $E : \{(v_h, v_{hs}) | h \in H, s \in S\}$

$\mathbf{Cay}(C_{24}, < g^2 >, \{g, g^{-1}, g^{12}\})$



Pair-graph

Notations

$$S_H := S \cap H$$

$$S_O := S - H$$

Since we have H : a subgroup of index $k+1$ of G, we consider a set of representatives of the cosets,

$$\{x_0 = e, x_1, \dots, x_k\}$$

and a partition of S_O given by sets

$$S_i := S \cap Hx_i,$$

for $i \in [k]$.

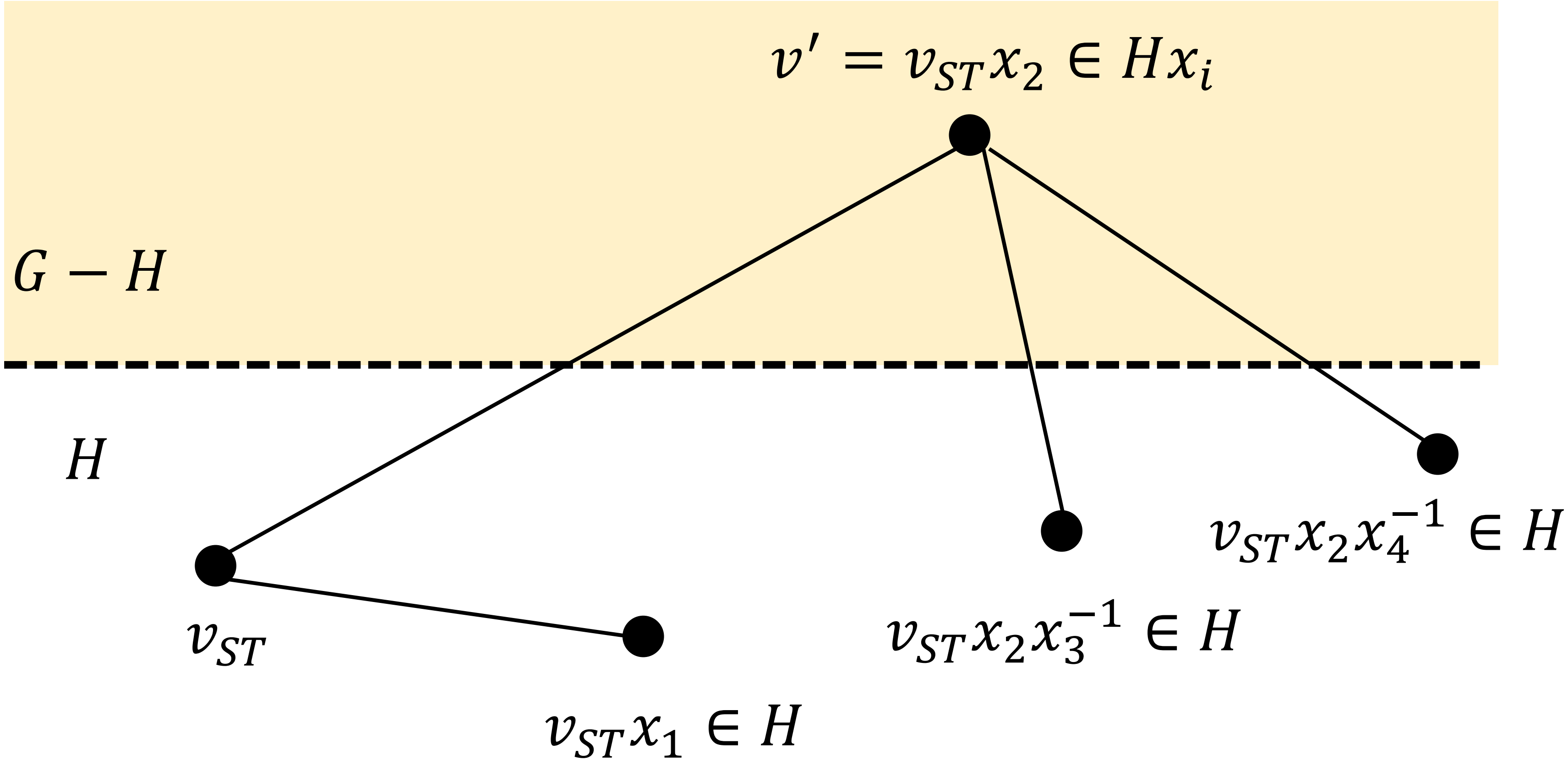
Remarks

- If $G = H$, we recover the definition of Cayley graph, that is
$$\mathcal{G}(G, G, S) = Cay(G, S),$$

- In general, $\mathcal{G}(G, H, S)$ is a non-regular graph, in fact, it can only be regular for index 1 or 2.

- While $\mathcal{G}(G, H, S)$ is not vertex transitive, the action (right of left) of H in a coset Hx is transitive (H homogeneous).

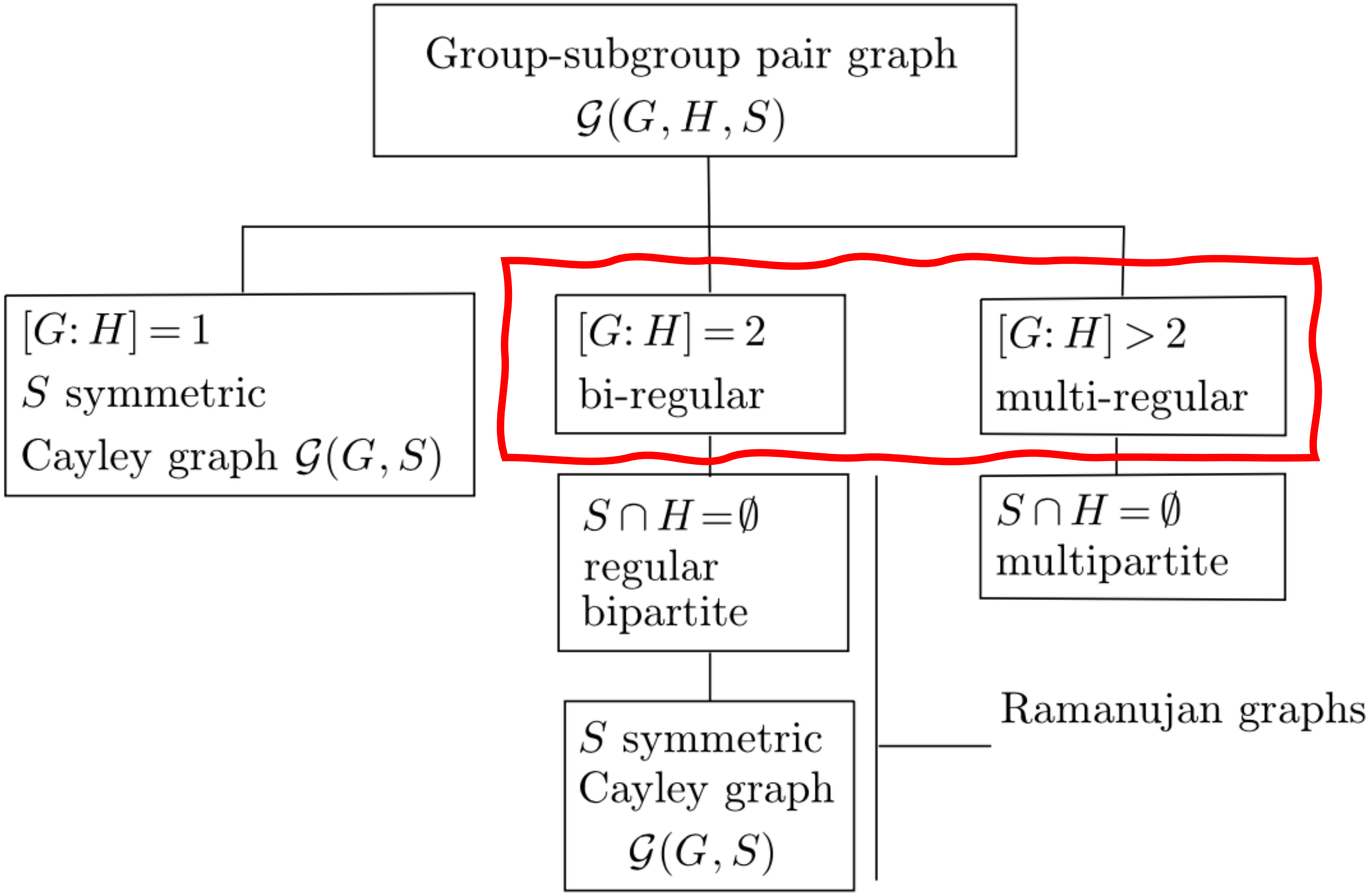
How to make a path in pair-graph


$v' = v_{ST}x_2 \in Hx_i$
$G - H$
H
v_{ST}
$v_{ST}x_1 \in H$
$v_{ST}x_2x_3^{-1} \in H$
$v_{ST}x_2x_4^{-1} \in H$

Assume that $x_1 \in S_o$ and $x_2, x_3, x_4 \in S_i$

Note that the possible vertices in the path depend on whether the current vertex $v \in H$ or $v' \in G - H$.

Families of group-subgroup pair graphs



Group-subgroup pair graph $\mathcal{G}(G, H, S)$

$[G:H]=1$
S symmetric
Cayley graph $\mathcal{G}(G,S)$

$[G:H]=2$
bi-regular

$[G:H]>2$
multi-regular

$S \cap H = \emptyset$
regular
bipartite

$S \cap H = \emptyset$
multipartite

S symmetric
Cayley graph
$\mathcal{G}(G,S)$

Ramanujan graphs

Multi-regular graphs

- The degree of the vertices of a coset Hx (for $x \in G$) is constant.

We define a graph with a partition of the vertices $V_1, \dots, V_k$ that the degree of vertices on each partition is constant is called a *multi-regular graph* or $(\boldsymbol{d_1}, \dots, \boldsymbol{d_k})$-regular graph, where d_i is the degree of the vertices on a given partition.

- Notice that the d_i need not to be distinct.

Properties (spectrum)

- Similarly to the Cayley graph case, the spectrum is controlled by the irreducible representations of H.

- For the case of abelian H we can obtain explicit formulas for the usual spectrum, Laplacian spectrum and other spectrums of pair-graphs.

  e.g. Normalized Laplacian eigenvalues

$$\mu_{\pm} = \frac{1}{2}\left(\lambda_{\chi}^{(0)} \pm \sqrt{\left(\lambda_{\chi}^{(0)}\right)^2 + 4\sum_{i=1}^{k}\lambda_{\chi}^{(i)}}\right)$$

$\lambda_{\chi}^{(i)}$: character sums with respect to character χ of H and i-th coset.

Notice that the formulas are not linear, which make the analysis complicated, especially for non-abelian subgroups.

Our proposal

A hash function based on **multi-regular graphs**

A hash function based on multi-regular graphs

Definition

$\boldsymbol{G(V,E)}$: $(\boldsymbol{d_1}, \dots, \boldsymbol{d_k})$-regular graph for some $k \in \mathbb{N}$.

m : a binary message.

v_{ST} : a starting vertex.

We label edges from 0 to $d_i - 2$ for each vertex $(1 \le i \le k)$ along its regularity.

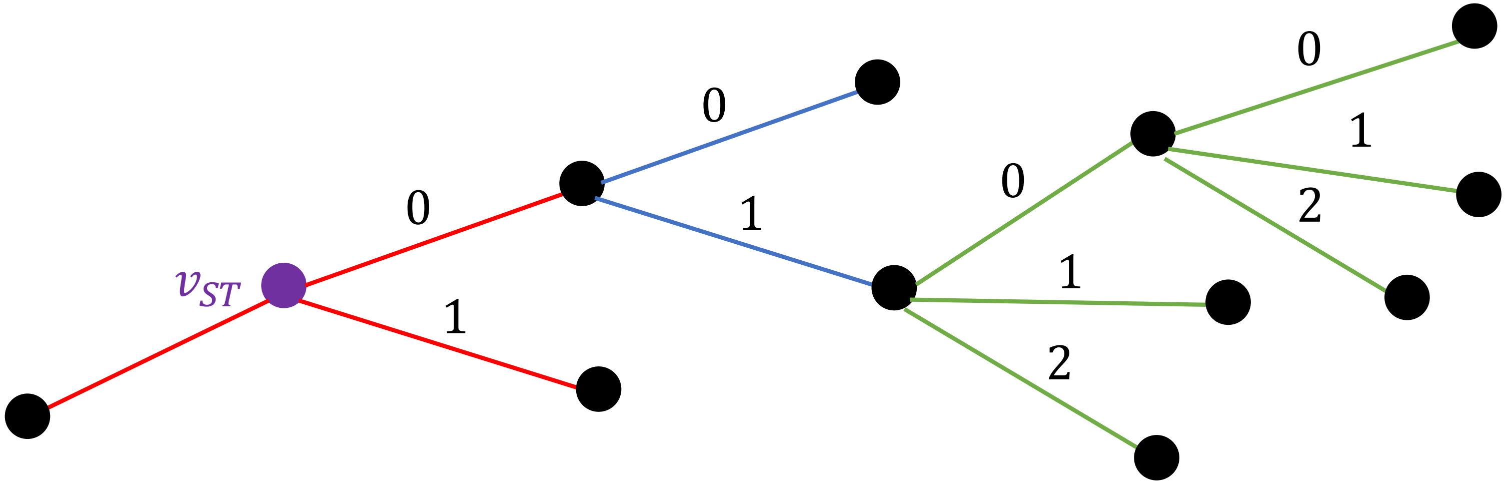


Figure. (3,3,4)-regular graph

A hash function based on multi-regular graphs

Definition

We transform m into $m_{d_1}, \ldots, m_{d_k}$ along the multi-regularity as follows:

$$m \mapsto m_{d_1} \text{ } (d_1)\text{-base number } (|m_{d_1}| \leq \ell_{d_1});$$

$$\vdots$$

$$m \mapsto m_{d_k} \text{ } (d_k)\text{-base number } (|m_{d_k}| \leq \ell_{d_k}).$$

$$\mathcal{H}: \{0,1\}^* \to [d_1]^* \times \cdots \times [d_k]^* \to G$$

Here, $[d_i] \coloneqq \{0,1, \ldots, d_1 - 1\}$ for convenience.

A hash function based on multi-regular graphs

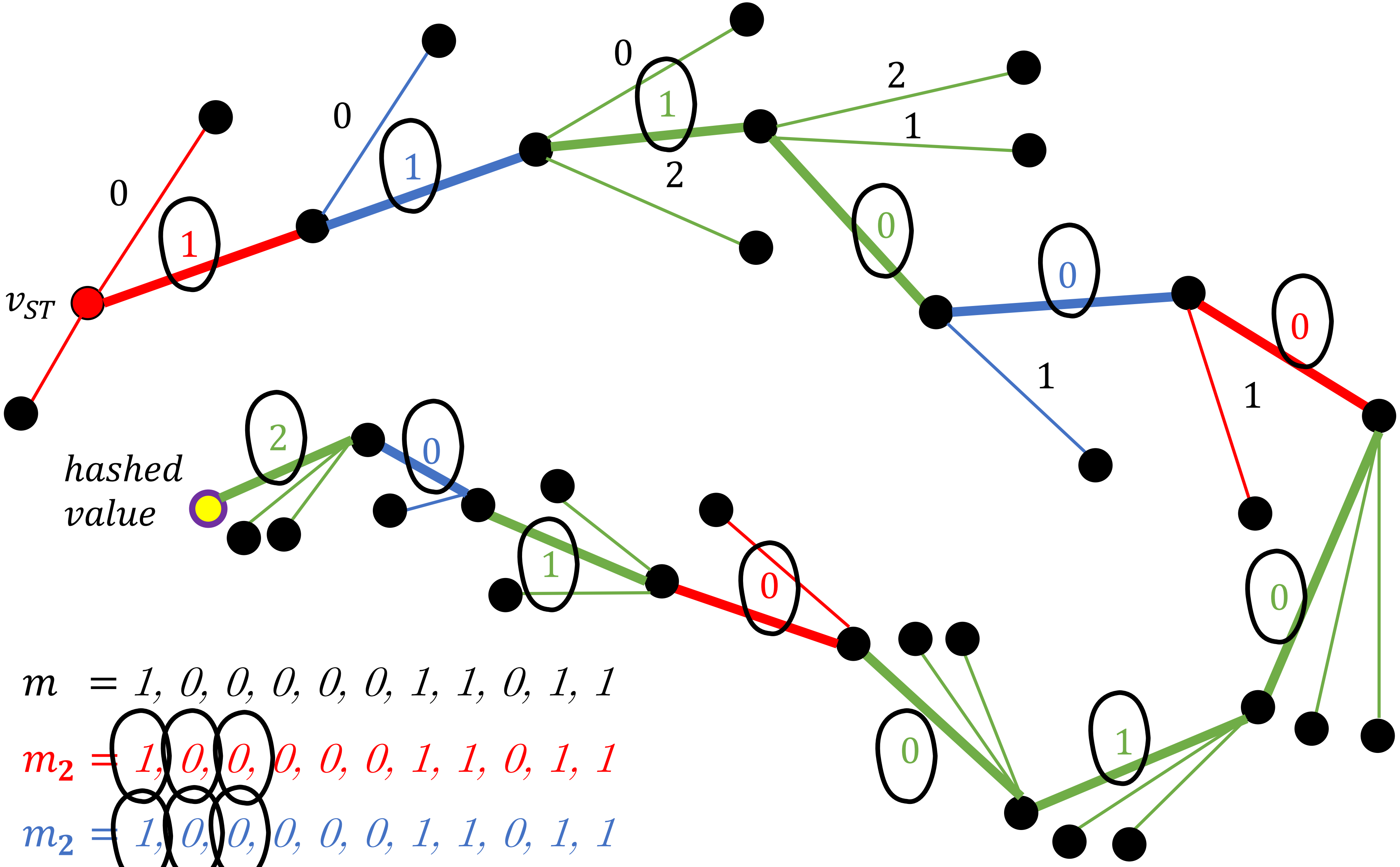
A hashing process

(1) If a starting vertex v_{ST} has d_{ST} degree ($1 \leq ST \leq k$), walk on the labelled edge assigned by the first bit of the corresponding message $m_{d_{ST}}$.

(2) Next, check the regularity of a present vertex. Then walk along the labelled edge assigned by the next bit of the corresponding transformed message.

(3) In the manner of those, keep doing (2) until we consume **all the bits one of the transformed messages**.

(4) The final destinated vertex is the hashed value of m.



$m \;\; = 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1$

$m_2 = 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1$

$m_2 = 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1$

$m_3 = 1, 0, 0, 1, 0, 1, 2$

Figure. A hash function based on (3,3,4)-regular graph

Hash function from pair-graphs

Let $\boldsymbol{G} = \mathcal{G}(G, H, S)$.

Denote S by $S_O = \left\{s_1, s_2, \dots, s_{d_1}\right\}$ and $S_i = \left\{s_1^{(i)}, s_2^{(i)}, \dots, s_{d_1}^{(i)}\right\}$.

Fix a starting vertex $v_{ST} \in H$.

$$\mathcal{H}_{pair}: \{0,1\}^* \to [d_1]^* \times \cdots \times [d_k]^* \to G$$

Set ***choice functions***

$$\pi_{O,j}: [d_i] \times S_O \longrightarrow S_O$$

such that, $\forall s \in S_O, \pi_{O,j}([d_i] \times \{s\}) = S_O \setminus \{s^{-1}\}$,

$$\pi_{i,j}: [d_i] \times S_i^{-1} \longrightarrow S_i^{-1}$$

such that, $\forall s \in S_i, \pi_{i,j}([d_i] \times \{s^{-1}\}) = S_i^{-1} \setminus \{s\}$,

for each case from coset Hx_i to coset Hx_j $(1 \le i, j \le k)$.

Hash function from pair-graphs

We prepare messages

$$m \mapsto m_{d_1} \ (d_1)\text{-base number } (|m_{d_1}| \leq \ell_{d_1});$$

$$\vdots$$

$$m \mapsto m_{d_k} \ (d_k)\text{-base number } (|m_{d_k}| \leq \ell_{d_k}).$$

A hashing process

We fixed a starting vertex $v_{ST} \in H$.

(1) According to $\pi_{O,j}$, walk on the labelled edge assigned by the first bit of the corresponding message m_{d_1}. (Say, v_i)

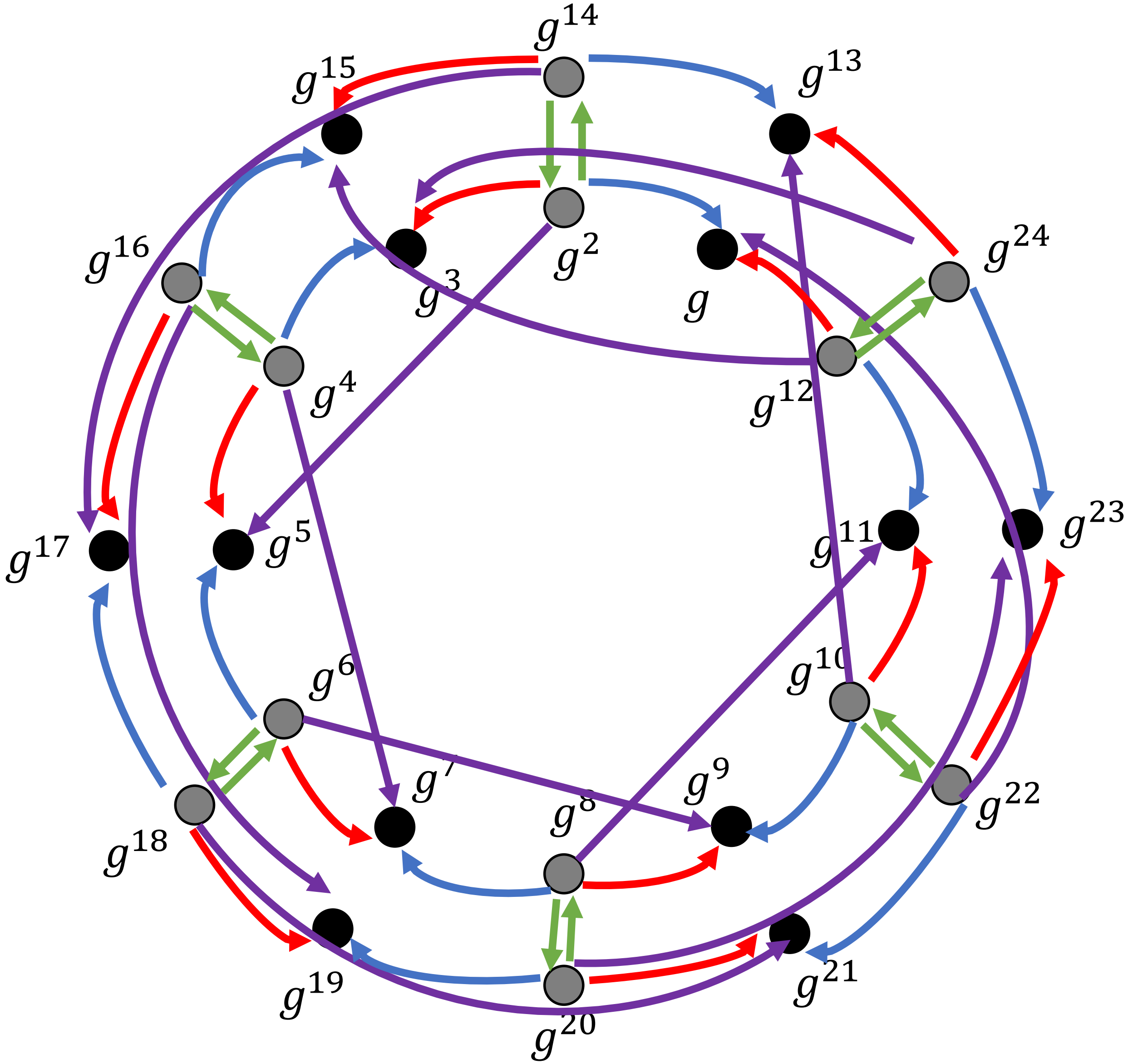
(2) Next, if $v_i \in H$, according to $\pi_{O,j}$, $\boldsymbol{v_{i+1} = v_i s_{m_i}}$;

if $v_i \in Hx_i$, according to $\pi_{i,j}$, $\boldsymbol{v_{i+1} = v_i \left(s_{m_i}^{(i)}\right)^{-1}}$.

(3) Repeat (2) until we consume all the bits one of the transformed messages.

(4) The final destinated vertex is the hashed value of m.

Toy Ex) Cay(C_{24},$< g^2 >$,$\{g, g^{-1}, g^3, g^{12}\}$)

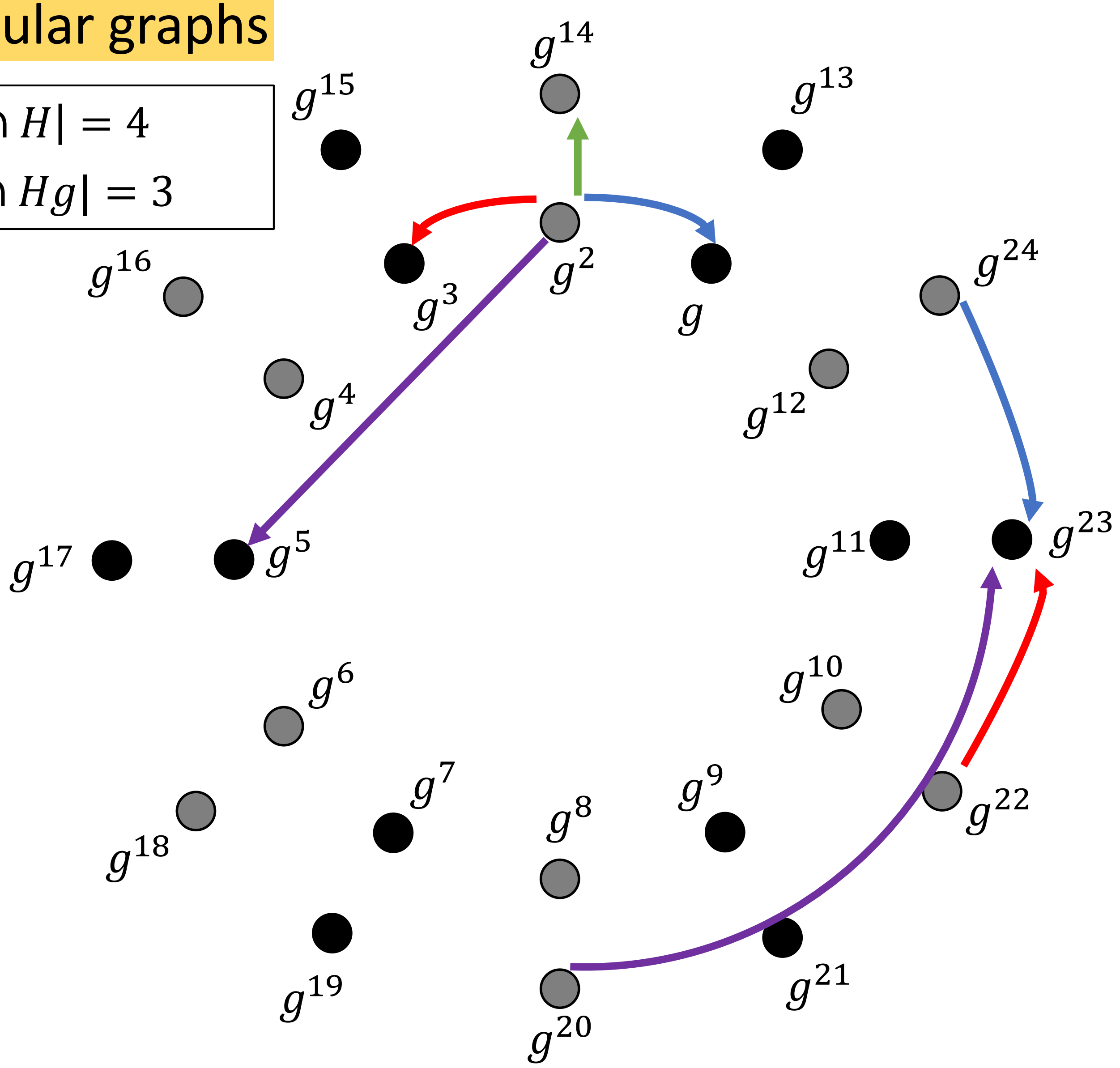


$\mathbf{Cay}(C_{24}, < g^2 >, \{g, g^{-1}, g^3, g^{12}\})$

(3,4)-regular graphs

$|S_H| = |S \cap H| = 4$

$|S_O| = |S \cap Hg| = 3$



Read the previous edges case by case and avoid the trivial collision!

Case. $H \to \boldsymbol{H}$

Choice function $\pi_{0,0}$

$\pi_{0,0}(0, g) = g$

$\pi_{0,0}(1, g) = g^3$

$\pi_{0,0}(2, g) = g^{12}$

$\pi_{0,0}(0, g^{-1}) = g^{-1}$

$\pi_{0,0}(1, g^{-1}) = g^3$

$\pi_{0,0}(2, g^{-1}) = g^{12}$

$\pi_{0,0}(0, g^3) = g$

$\pi_{0,0}(1, g^3) = g^{-1}$

$\pi_{0,0}(2, g^3) = g^{12}$

$\pi_{0,0}(0, g^{12}) = g$

$\pi_{0,0}(1, g^{12}) = g^3$

$\pi_{0,0}(2, g^{12}) = g^{-1}$

Case. $G - H \to \boldsymbol{H}$

Choice function $\pi_{0,1}$

$\pi_{0,1}(0, g) = g$

$\pi_{0,1}(1, g) = g^3$

$\pi_{0,1}(2, g) = g^{12}$

$\pi_{0,1}(0, g^{-1}) = g^{-1}$

$\pi_{0,1}(1, g^{-1}) = g^3$

$\pi_{0,1}(2, g^{-1}) = g^{12}$

$\pi_{0,1}(0, g^{21}) = g$

$\pi_{0,1}(1, g^{21}) = g^{-1}$

$\pi_{0,1}(2, g^{21}) = g^{12}$

Case. $H \to \boldsymbol{G - H}$

Choice function $\pi_{1,0}$

$\pi_{1,0}(0, g) = g$

$\pi_{1,0}(1, g) = g^{21}$

$\pi_{1,0}(0, g^{-1}) = g^{21}$

$\pi_{1,0}(1, g^{-1}) = g^{-1}$

$\pi_{1,0}(0, g^3) = g$

$\pi_{1,0}(1, g^3) = g^{-1}$

$\pi_{1,0}(0, g^{12}) = g$

$\pi_{1,0}(1, g^{12}) = g^{-1}$

Case. $G - H \to \boldsymbol{G - H}$

Choice function $\pi_{1,1}$

$\pi_{1,1}(0, g) = g$

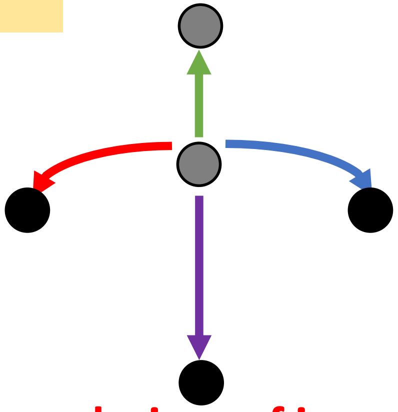
$\pi_{1,1}(1, g) = g^{21}$

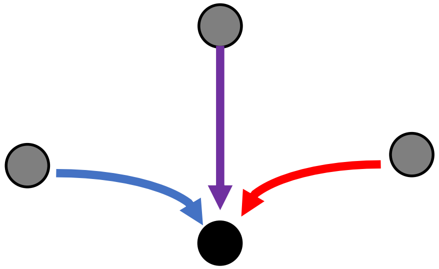
$\pi_{1,1}(0, g^{-1}) = g^{-1}$

$\pi_{1,1}(1, g^{-1}) = g^{21}$

$\pi_{1,1}(0, g^{21}) = g$

$\pi_{1,1}(1, g^{21}) = g^{-1}$





Caution! : For cases $\boldsymbol{G - H \to *}$, the edge colorings of inverses are chosen same as generators.

$H \rightarrow H$

Choice function $\pi_{0,0}$

$\pi_{0,0}(0, g^{12}) = g$

$\pi_{0,0}(1, g^{12}) = g^{3}$

$\pi_{0,0}(2, g^{12}) = g^{-1}$

$G - H \rightarrow H$

Choice function $\pi_{0,1}$

$\pi_{0,1}(0, g) = g$

$\pi_{0,1}(1, g) = g^{3}$

$\pi_{0,1}(2, g) = g^{12}$

$\pi_{0,1}(0, g^{-1}) = g^{-1}$

$\pi_{0,1}(1, g^{-1}) = g^{3}$

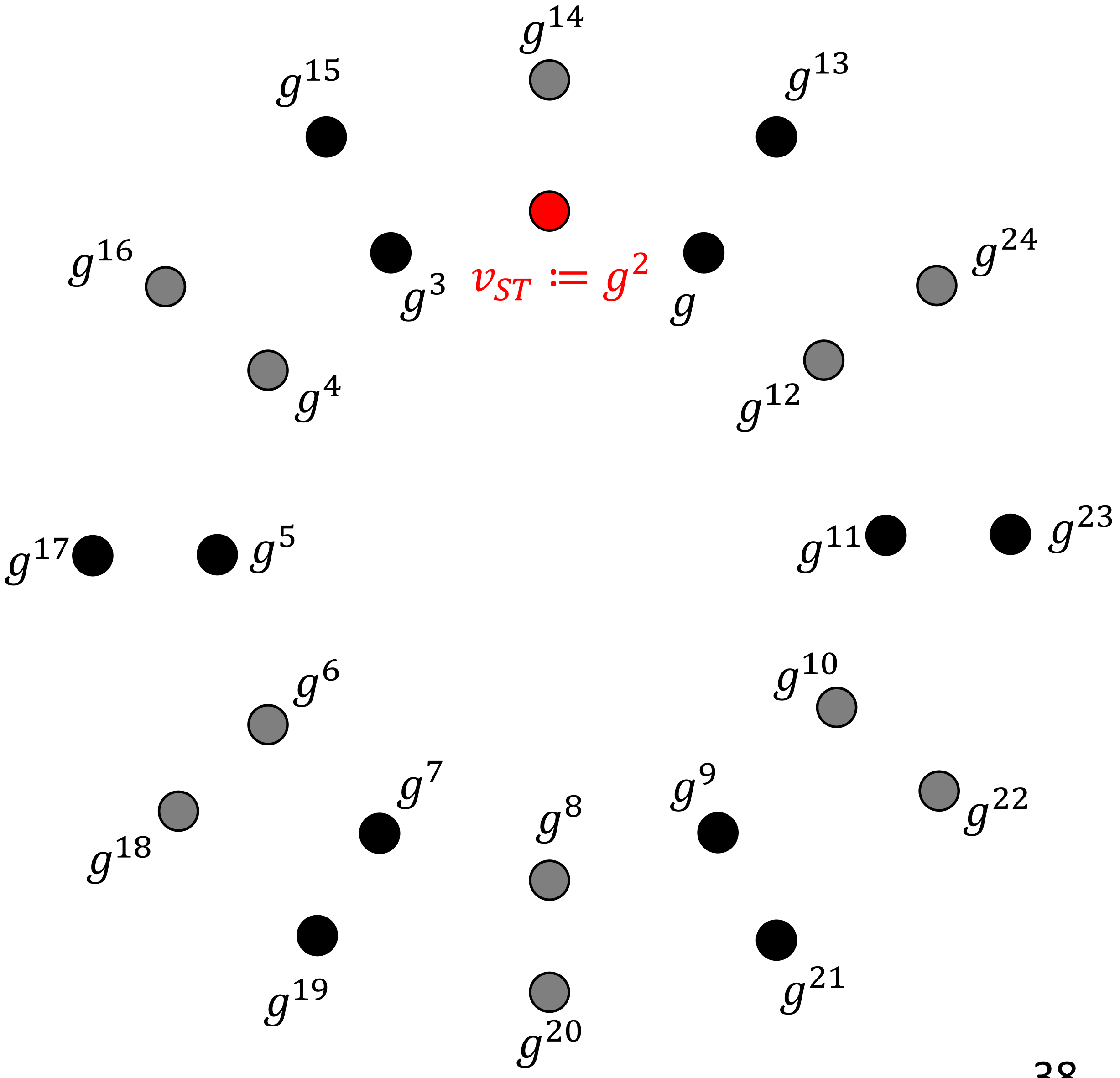
$\pi_{0,1}(2, g^{-1}) = g^{12}$

$\pi_{0,1}(0, g^{21}) = g$

$\pi_{0,1}(1, g^{21}) = g^{-1}$

$\pi_{0,1}(2, g^{21}) = g^{12}$

$$m \ = 1,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 1,\ 0,\ 1,\ 1$$
$$m_3 = 1,\ 0,\ 0,\ 1,\ 0,\ 1,\ 2$$
$$m_2 = 1,\ 0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 1,\ 0,\ 1,\ 1$$



$H \rightarrow G - H$

Choice function $\pi_{1,0}$

$\pi_{1,0}(0, g) = g$

$\pi_{1,0}(1, g) = g^{21}$

$\pi_{1,0}(0, g^{-1}) = g^{21}$

$\pi_{1,0}(1, g^{-1}) = g^{-1}$

$\pi_{1,0}(0, g^{3}) = g$

$\pi_{1,0}(1, g^{3}) = g^{-1}$

$G - H \rightarrow G - H$

Choice function $\pi_{1,1}$

$\pi_{1,1}(0, g) = g$

$\pi_{1,1}(1, g) = g^{21}$

$\pi_{1,1}(0, g^{-1}) = g^{-1}$

$\pi_{1,1}(1, g^{-1}) = g^{21}$

$\pi_{1,1}(0, g^{21}) = g$

$\pi_{1,1}(1, g^{21}) = g^{-1}$

Caution! : For cases $G - H \rightarrow *$, the edge colorings of inverses are chosen same as generators.

$H \to H$

Choice function $\pi_{0,0}$

$\pi_{0,0}(0, g^{12}) = g$

$\pi_{0,0}(1, g^{12}) = g^{3}$

$\pi_{0,0}(2, g^{12}) = g^{-1}$

$G - H \to H$

Choice function $\pi_{0,1}$

$\pi_{0,1}(0, g) = g$

$\pi_{0,1}(1, g) = g^{3}$

$\pi_{0,1}(2, g) = g^{12}$

$\pi_{0,1}(0, g^{-1}) = g^{-1}$

$\pi_{0,1}(1, g^{-1}) = g^{3}$

$\pi_{0,1}(2, g^{-1}) = g^{12}$

$\pi_{0,1}(0, g^{21}) = g$

$\pi_{0,1}(1, g^{21}) = g^{-1}$

$\pi_{0,1}(2, g^{21}) = g^{12}$

$H \to G - H$

Choice function $\pi_{1,0}$

$\pi_{1,0}(0, g) = g$

$\pi_{1,0}(1, g) = g^{21}$

$\pi_{1,0}(0, g^{-1}) = g^{21}$

$\pi_{1,0}(1, g^{-1}) = g^{-1}$

$\pi_{1,0}(0, g^{3}) = g$

$\pi_{1,0}(1, g^{3}) = g^{-1}$

$G - H \to G - H$

Choice function $\pi_{1,1}$

$\pi_{1,1}(0, g) = g$

$\pi_{1,1}(1, g) = g^{21}$

$\pi_{1,1}(0, g^{-1}) = g^{-1}$

$\pi_{1,1}(1, g^{-1}) = g^{21}$

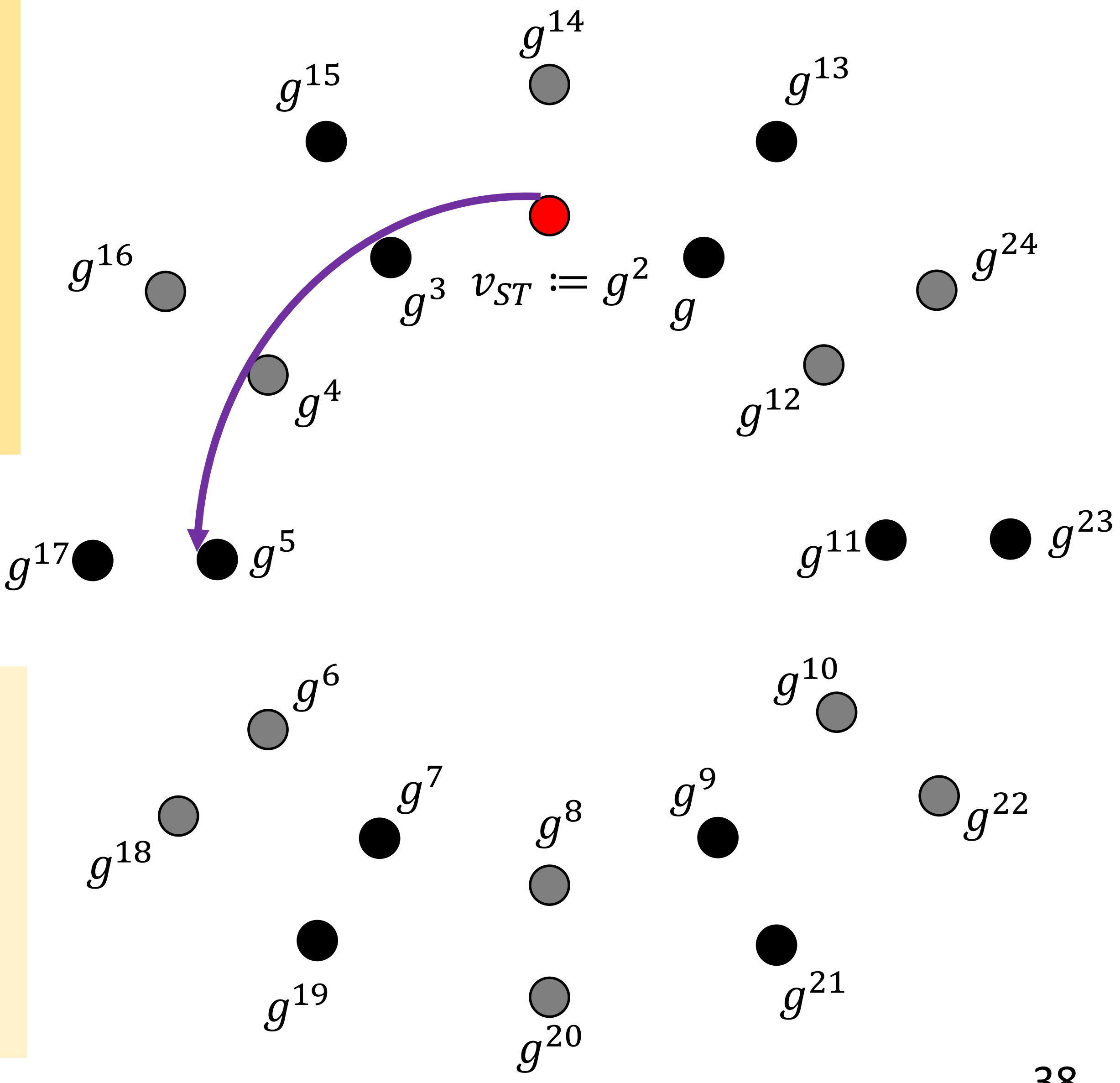
$\pi_{1,1}(0, g^{21}) = g$

$\pi_{1,1}(1, g^{21}) = g^{-1}$

$m \;\; = 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1$

$m_3 = 1, 0, 0, 1, 0, 1, 2$

$m_2 = 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1$



$H \to H$

Choice function $\pi_{0,0}$

$\pi_{0,0}(0, g^{12}) = g$

$\pi_{0,0}(1, g^{12}) = g^{3}$

$\pi_{0,0}(2, g^{12}) = g^{-1}$

$G - H \to H$

Choice function $\pi_{0,1}$

$\pi_{0,1}(0, g) = g$

$\pi_{0,1}(1, g) = g^{3}$

$\pi_{0,1}(2, g) = g^{12}$

$\pi_{0,1}(0, g^{-1}) = g^{-1}$

$\pi_{0,1}(1, g^{-1}) = g^{3}$

$\pi_{0,1}(2, g^{-1}) = g^{12}$

$\pi_{0,1}(0, g^{21}) = g$

$\pi_{0,1}(1, g^{21}) = g^{-1}$

$\pi_{0,1}(2, g^{21}) = g^{12}$

$H \to G - H$

Choice function $\pi_{1,0}$

$\pi_{1,0}(0, g) = g$

$\pi_{1,0}(1, g) = g^{21}$

$\pi_{1,0}(0, g^{-1}) = g^{21}$

$\pi_{1,0}(1, g^{-1}) = g^{-1}$

$\pi_{1,0}(0, g^{3}) = g$

$\pi_{1,0}(1, g^{3}) = g^{-1}$

$G - H \to G - H$

Choice function $\pi_{1,1}$

$\pi_{1,1}(0, g) = g$

$\pi_{1,1}(1, g) = g^{21}$

$\pi_{1,1}(0, g^{-1}) = g^{-1}$

$\pi_{1,1}(1, g^{-1}) = g^{21}$

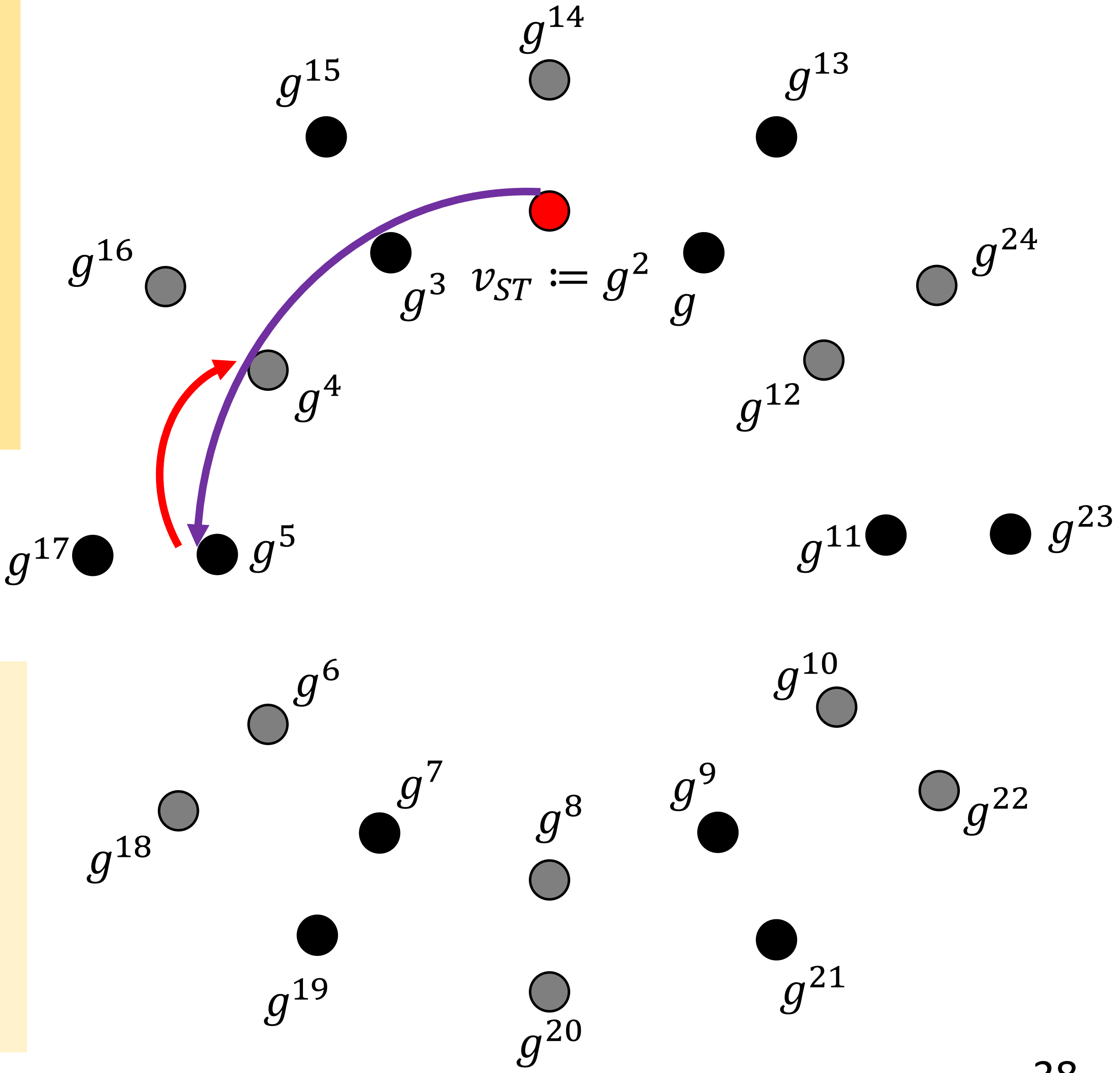
$\pi_{1,1}(0, g^{21}) = g$

$\pi_{1,1}(1, g^{21}) = g^{-1}$

$m\ = 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1$

$m_3 = 1, 0, 0, 1, 0, 1, 2$

$m_2 = 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1$



$H \to H$

Choice function $\pi_{0,0}$

$\pi_{0,0}(0, g^{12}) = g$

$\pi_{0,0}(1, g^{12}) = g^{3}$

$\pi_{0,0}(2, g^{12}) = g^{-1}$

$G - H \to H$

Choice function $\pi_{0,1}$

$\pi_{0,1}(0, g) = g$

$\pi_{0,1}(1, g) = g^{3}$

$\pi_{0,1}(2, g) = g^{12}$

$\pi_{0,1}(0, g^{-1}) = g^{-1}$

$\pi_{0,1}(1, g^{-1}) = g^{3}$

$\pi_{0,1}(2, g^{-1}) = g^{12}$

$\pi_{0,1}(0, g^{21}) = g$

$\pi_{0,1}(1, g^{21}) = g^{-1}$

$\pi_{0,1}(2, g^{21}) = g^{12}$

$H \to G - H$

Choice function $\pi_{1,0}$

$\pi_{1,0}(0, g) = g$

$\pi_{1,0}(1, g) = g^{21}$

$\pi_{1,0}(0, g^{-1}) = g^{21}$

$\pi_{1,0}(1, g^{-1}) = g^{-1}$

$\pi_{1,0}(0, g^{3}) = g$

$\pi_{1,0}(1, g^{3}) = g^{-1}$

$G - H \to G - H$

Choice function $\pi_{1,1}$

$\pi_{1,1}(0, g) = g$

$\pi_{1,1}(1, g) = g^{21}$

$\pi_{1,1}(0, g^{-1}) = g^{-1}$

$\pi_{1,1}(1, g^{-1}) = g^{21}$

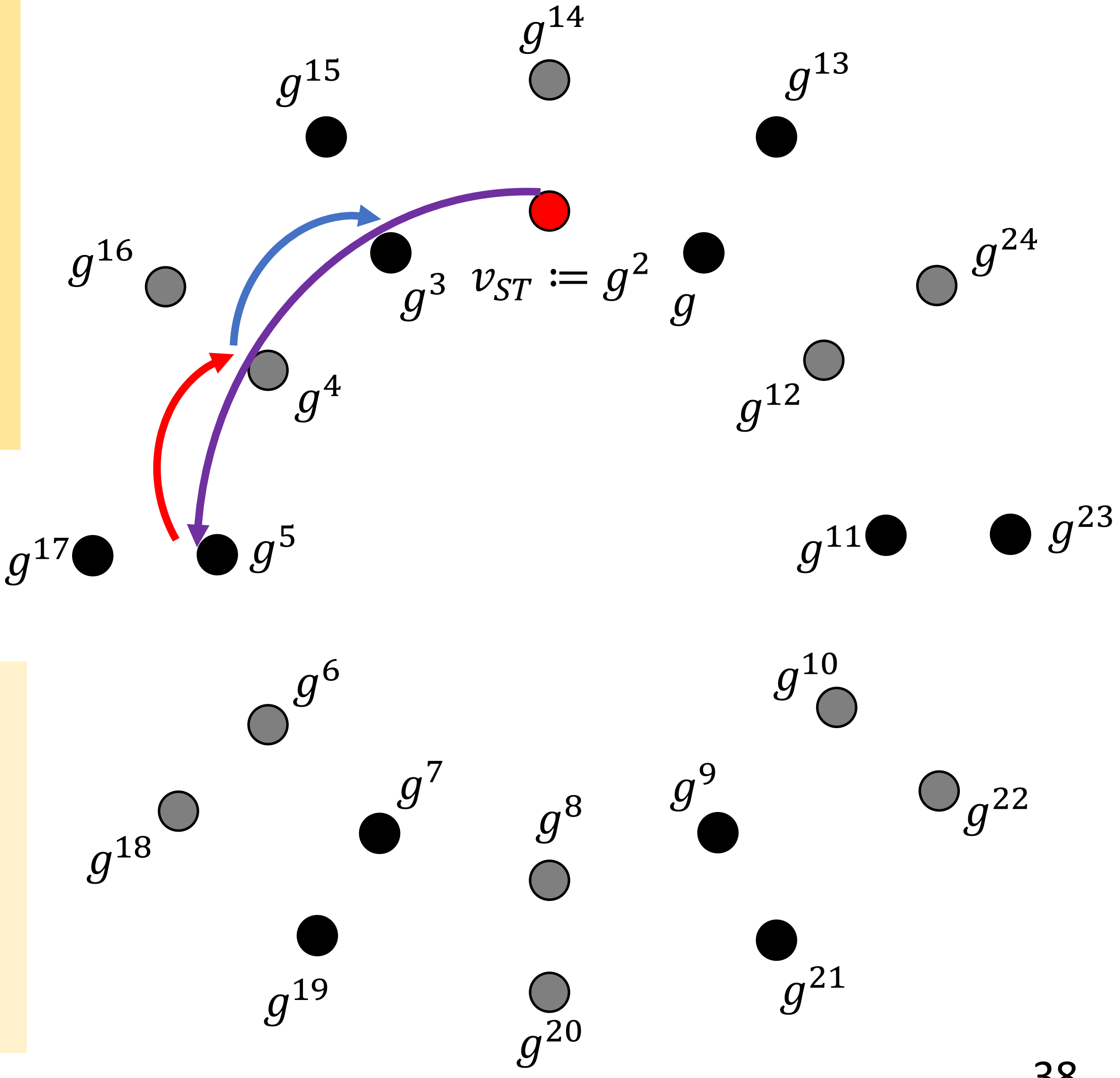
$\pi_{1,1}(0, g^{21}) = g$

$\pi_{1,1}(1, g^{21}) = g^{-1}$

$m\ = 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1$

$m_3 = 1, 0, 0, 1, 0, 1, 2$

$m_2 = 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1$



$H \to H$

Choice function $\pi_{0,0}$

$\pi_{0,0}(0, g^{12}) = g$

$\pi_{0,0}(1, g^{12}) = g^3$

$\pi_{0,0}(2, g^{12}) = g^{-1}$

$G - H \to H$

Choice function $\pi_{0,1}$

$\pi_{0,1}(0, g) = g$

$\pi_{0,1}(1, g) = g^3$

$\pi_{0,1}(2, g) = g^{12}$

$\pi_{0,1}(0, g^{-1}) = g^{-1}$

$\pi_{0,1}(1, g^{-1}) = g^3$

$\pi_{0,1}(2, g^{-1}) = g^{12}$

$\pi_{0,1}(0, g^{21}) = g$

$\pi_{0,1}(1, g^{21}) = g^{-1}$

$\pi_{0,1}(2, g^{21}) = g^{12}$

$H \to G - H$

Choice function $\pi_{1,0}$

$\pi_{1,0}(0, g) = g$

$\pi_{1,0}(1, g) = g^{21}$

$\pi_{1,0}(0, g^{-1}) = g^{21}$

$\pi_{1,0}(1, g^{-1}) = g^{-1}$

$\pi_{1,0}(0, g^3) = g$

$\pi_{1,0}(1, g^3) = g^{-1}$

$G - H \to G - H$

Choice function $\pi_{1,1}$

$\pi_{1,1}(0, g) = g$

$\pi_{1,1}(1, g) = g^{21}$

$\pi_{1,1}(0, g^{-1}) = g^{-1}$

$\pi_{1,1}(1, g^{-1}) = g^{21}$

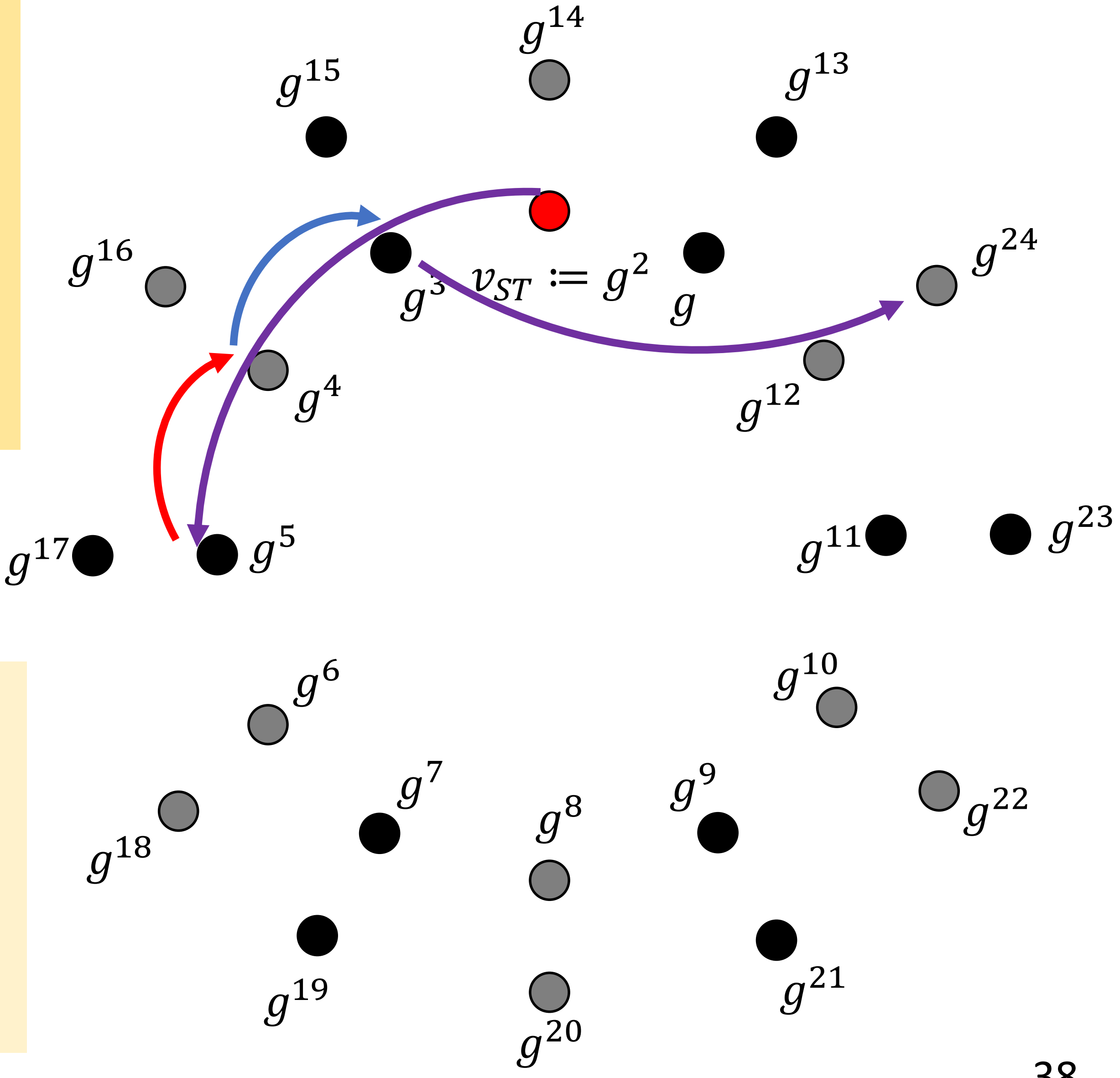
$\pi_{1,1}(0, g^{21}) = g$

$\pi_{1,1}(1, g^{21}) = g^{-1}$

$m \;\; = 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1$

$m_3 = 1, 0, 0, 1, 0, 1, 2$

$m_2 = 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1$



$H \to H$

Choice function $\pi_{0,0}$

$\pi_{0,0}(0, g^{12}) = g$

$\pi_{0,0}(1, g^{12}) = g^{3}$

$\pi_{0,0}(2, g^{12}) = g^{-1}$

$G - H \to H$

Choice function $\pi_{0,1}$

$\pi_{0,1}(0, g) = g$

$\pi_{0,1}(1, g) = g^{3}$

$\pi_{0,1}(2, g) = g^{12}$

$\pi_{0,1}(0, g^{-1}) = g^{-1}$

$\pi_{0,1}(1, g^{-1}) = g^{3}$

$\pi_{0,1}(2, g^{-1}) = g^{12}$

$\pi_{0,1}(0, g^{21}) = g$

$\pi_{0,1}(1, g^{21}) = g^{-1}$

$\pi_{0,1}(2, g^{21}) = g^{12}$

$H \to G - H$

Choice function $\pi_{1,0}$

$\pi_{1,0}(0, g) = g$

$\pi_{1,0}(1, g) = g^{21}$

$\pi_{1,0}(0, g^{-1}) = g^{21}$

$\pi_{1,0}(1, g^{-1}) = g^{-1}$

$\pi_{1,0}(0, g^{3}) = g$

$\pi_{1,0}(1, g^{3}) = g^{-1}$

$G - H \to G - H$

Choice function $\pi_{1,1}$

$\pi_{1,1}(0, g) = g$

$\pi_{1,1}(1, g) = g^{21}$

$\pi_{1,1}(0, g^{-1}) = g^{-1}$

$\pi_{1,1}(1, g^{-1}) = g^{21}$

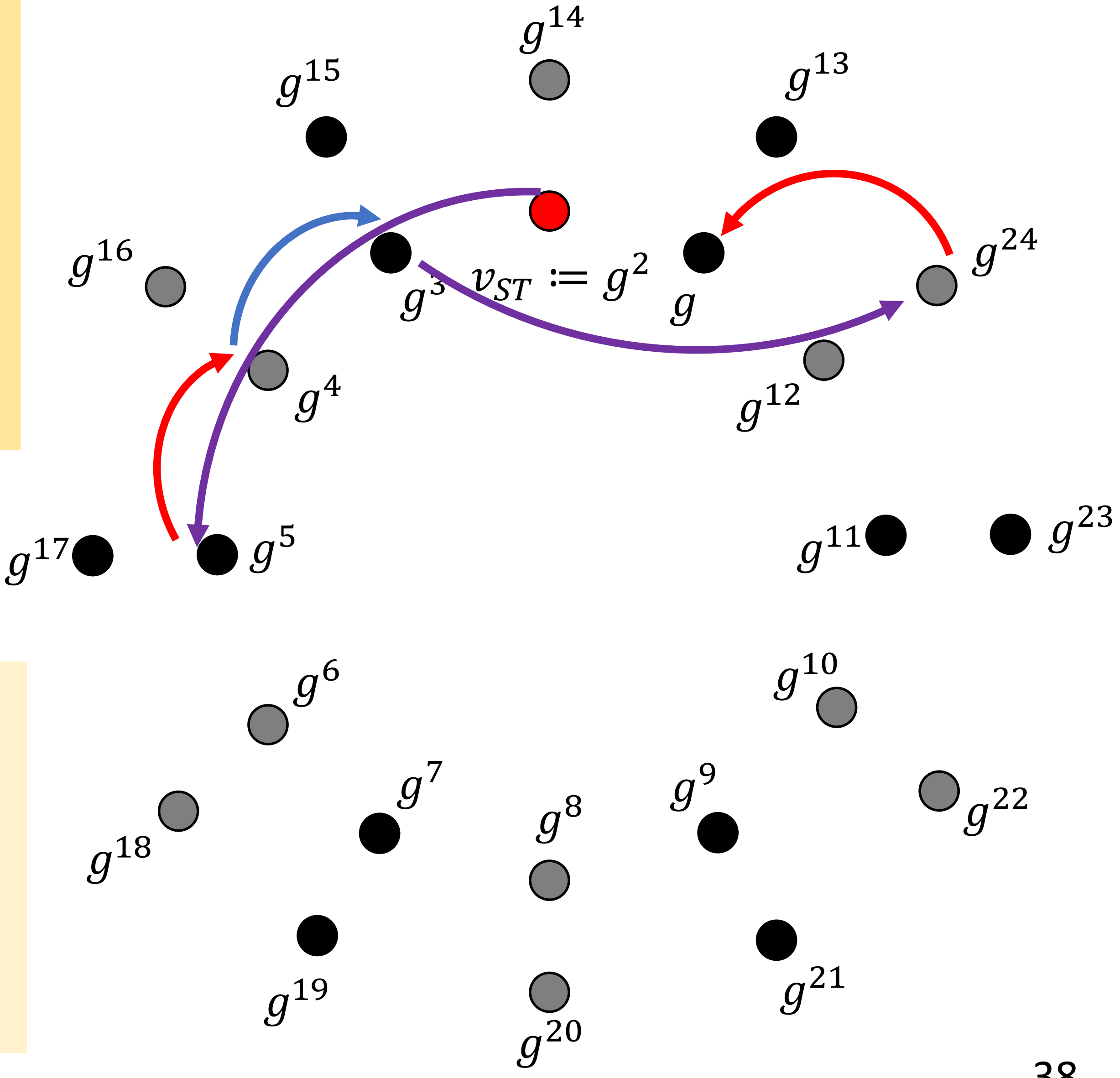
$\pi_{1,1}(0, g^{21}) = g$

$\pi_{1,1}(1, g^{21}) = g^{-1}$

$m = 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1$

$m_3 = 1, 0, 0, 1, 0, 1, 2$

$m_2 = 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1$



$H \to H$

Choice function $\pi_{0,0}$

$\pi_{0,0}(0, g^{12}) = g$

$\pi_{0,0}(1, g^{12}) = g^3$

$\pi_{0,0}(2, g^{12}) = g^{-1}$

$G - H \to H$

Choice function $\pi_{0,1}$

$\pi_{0,1}(0, g) = g$

$\pi_{0,1}(1, g) = g^3$

$\pi_{0,1}(2, g) = g^{12}$

$\pi_{0,1}(0, g^{-1}) = g^{-1}$

$\pi_{0,1}(1, g^{-1}) = g^3$

$\pi_{0,1}(2, g^{-1}) = g^{12}$

$\pi_{0,1}(0, g^{21}) = g$

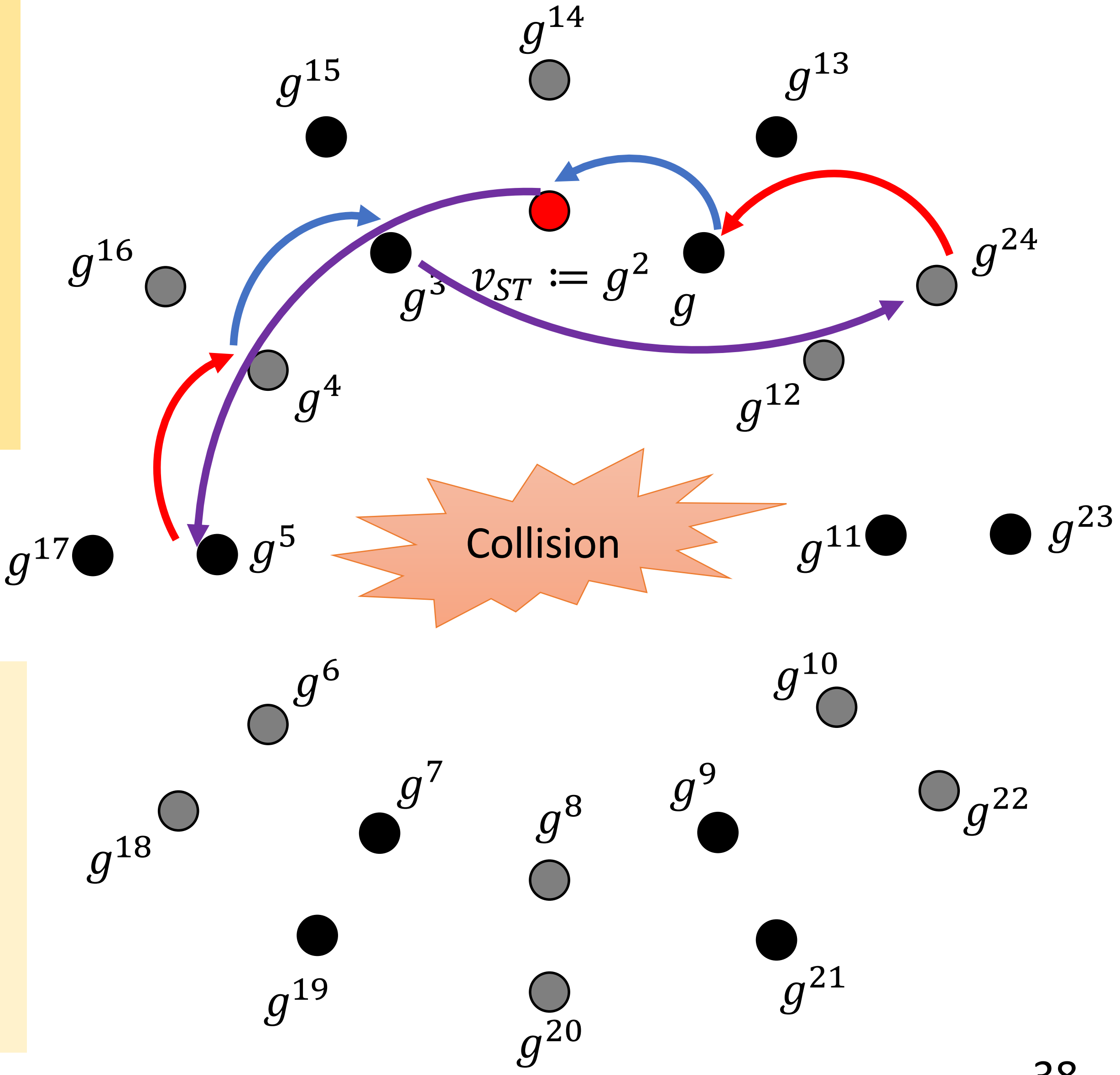
$\pi_{0,1}(1, g^{21}) = g^{-1}$

$\pi_{0,1}(2, g^{21}) = g^{12}$

$m \;\; = 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1$

$m_3 = 1, 0, 0, 1, 0, 1, 2$

$m_2 = 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1$



$H \to G - H$

Choice function $\pi_{1,0}$

$\pi_{1,0}(0, g) = g$

$\pi_{1,0}(1, g) = g^{21}$

$\pi_{1,0}(0, g^{-1}) = g^{21}$

$\pi_{1,0}(1, g^{-1}) = g^{-1}$

$\pi_{1,0}(0, g^3) = g$

$\pi_{1,0}(1, g^3) = g^{-1}$

$G - H \to G - H$

Choice function $\pi_{1,1}$

$\pi_{1,1}(0, g) = g$

$\pi_{1,1}(1, g) = g^{21}$

$\pi_{1,1}(0, g^{-1}) = g^{-1}$

$\pi_{1,1}(1, g^{-1}) = g^{21}$

$\pi_{1,1}(0, g^{21}) = g$

$\pi_{1,1}(1, g^{21}) = g^{-1}$

$H \to H$

Choice function $\pi_{0,0}$

$\pi_{0,0}(0, g^{12}) = g$

$\pi_{0,0}(1, g^{12}) = g^3$

$\pi_{0,0}(2, g^{12}) = g^{-1}$

$G - H \to H$

Choice function $\pi_{0,1}$

$\pi_{0,1}(0, g) = g$

$\pi_{0,1}(1, g) = g^3$

$\pi_{0,1}(2, g) = g^{12}$

$\pi_{0,1}(0, g^{-1}) = g^{-1}$

$\pi_{0,1}(1, g^{-1}) = g^3$

$\pi_{0,1}(2, g^{-1}) = g^{12}$

$\pi_{0,1}(0, g^{21}) = g$

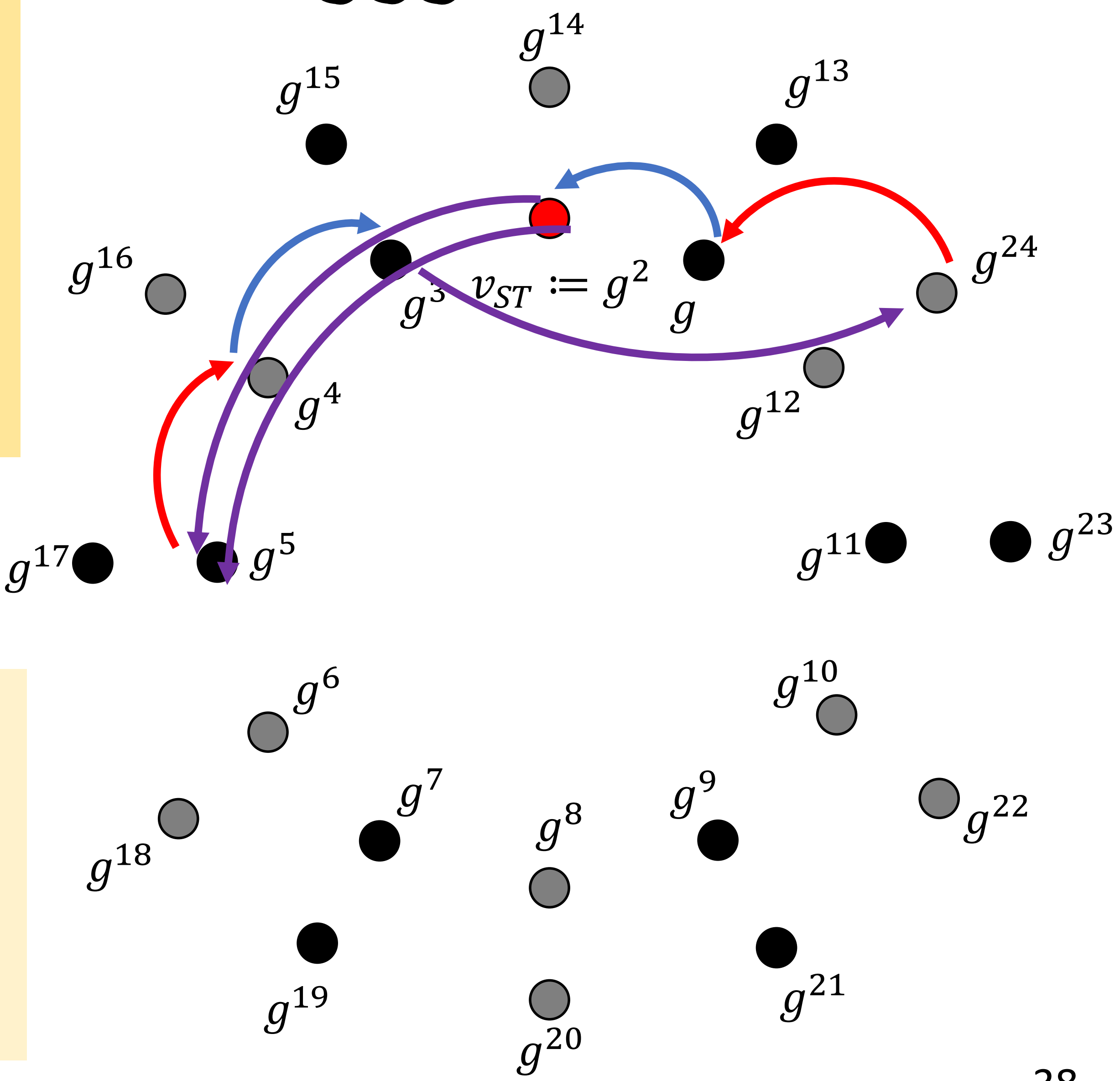
$\pi_{0,1}(1, g^{21}) = g^{-1}$

$\pi_{0,1}(2, g^{21}) = g^{12}$

$m \ = 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1$

$m_3 = 1, 0, 0, 1, 0, 1, 2$

$m_2 = 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1$



$H \to G - H$

Choice function $\pi_{1,0}$

$\pi_{1,0}(0, g) = g$

$\pi_{1,0}(1, g) = g^{21}$

$\pi_{1,0}(0, g^{-1}) = g^{21}$

$\pi_{1,0}(1, g^{-1}) = g^{-1}$

$\pi_{1,0}(0, g^3) = g$

$\pi_{1,0}(1, g^3) = g^{-1}$

$G - H \to G - H$

Choice function $\pi_{1,1}$

$\pi_{1,1}(0, g) = g$

$\pi_{1,1}(1, g) = g^{21}$

$\pi_{1,1}(0, g^{-1}) = g^{-1}$

$\pi_{1,1}(1, g^{-1}) = g^{21}$

$\pi_{1,1}(0, g^{21}) = g$

$\pi_{1,1}(1, g^{21}) = g^{-1}$

$H \rightarrow H$

Choice function $\pi_{O,0}$

$\pi_{O,0}(0, g^{12}) = g$

$\pi_{O,0}(1, g^{12}) = g^{3}$

$\pi_{O,0}(2, g^{12}) = g^{-1}$

$G - H \rightarrow H$

Choice function $\pi_{O,1}$

$\pi_{O,1}(0, g) = g$

$\pi_{O,1}(1, g) = g^{3}$

$\pi_{O,1}(2, g) = g^{12}$

$\pi_{O,1}(0, g^{-1}) = g^{-1}$

$\pi_{O,1}(1, g^{-1}) = g^{3}$

$\pi_{O,1}(2, g^{-1}) = g^{12}$

$\pi_{O,1}(0, g^{21}) = g$

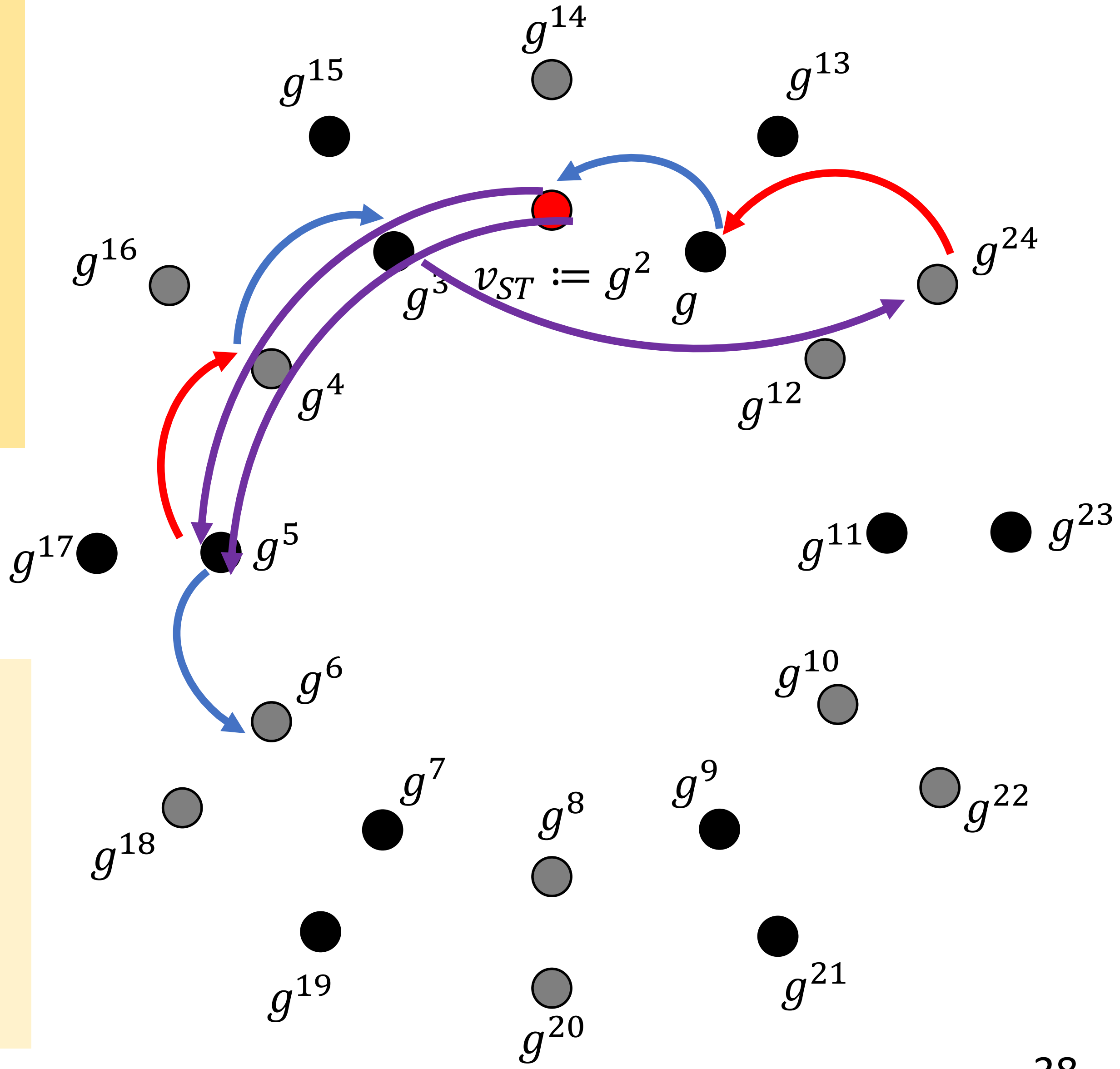
$\pi_{O,1}(1, g^{21}) = g^{-1}$

$\pi_{O,1}(2, g^{21}) = g^{12}$

$m \;\; = 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1$

$m_3 = 1, 0, 0, 1, 0, 1, 2$

$m_2 = 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1$



$H \rightarrow G - H$

Choice function $\pi_{1,0}$

$\pi_{1,0}(0, g) = g$

$\pi_{1,0}(1, g) = g^{21}$

$\pi_{1,0}(0, g^{-1}) = g^{21}$

$\pi_{1,0}(1, g^{-1}) = g^{-1}$

$\pi_{1,0}(0, g^{3}) = g$

$\pi_{1,0}(1, g^{3}) = g^{-1}$

$G - H \rightarrow G - H$

Choice function $\pi_{1,1}$

$\pi_{1,1}(0, g) = g$

$\pi_{1,1}(1, g) = g^{21}$

$\pi_{1,1}(0, g^{-1}) = g^{-1}$

$\pi_{1,1}(1, g^{-1}) = g^{21}$

$\pi_{1,1}(0, g^{21}) = g$

$\pi_{1,1}(1, g^{21}) = g^{-1}$

$H \to H$

Choice function $\pi_{0,0}$

$\pi_{0,0}(0, g^{12}) = g$

$\pi_{0,0}(1, g^{12}) = g^3$

$\pi_{0,0}(2, g^{12}) = g^{-1}$

$G - H \to H$

Choice function $\pi_{0,1}$

$\pi_{0,1}(0, g) = g$

$\pi_{0,1}(1, g) = g^3$

$\pi_{0,1}(2, g) = g^{12}$

$\pi_{0,1}(0, g^{-1}) = g^{-1}$

$\pi_{0,1}(1, g^{-1}) = g^3$

$\pi_{0,1}(2, g^{-1}) = g^{12}$

$\pi_{0,1}(0, g^{21}) = g$

$\pi_{0,1}(1, g^{21}) = g^{-1}$

$\pi_{0,1}(2, g^{21}) = g^{12}$

$H \to G - H$

Choice function $\pi_{1,0}$

$\pi_{1,0}(0, g) = g$

$\pi_{1,0}(1, g) = g^{21}$

$\pi_{1,0}(0, g^{-1}) = g^{21}$

$\pi_{1,0}(1, g^{-1}) = g^{-1}$

$\pi_{1,0}(0, g^3) = g$

$\pi_{1,0}(1, g^3) = g^{-1}$

$G - H \to G - H$

Choice function $\pi_{1,1}$

$\pi_{1,1}(0, g) = g$

$\pi_{1,1}(1, g) = g^{21}$

$\pi_{1,1}(0, g^{-1}) = g^{-1}$

$\pi_{1,1}(1, g^{-1}) = g^{21}$

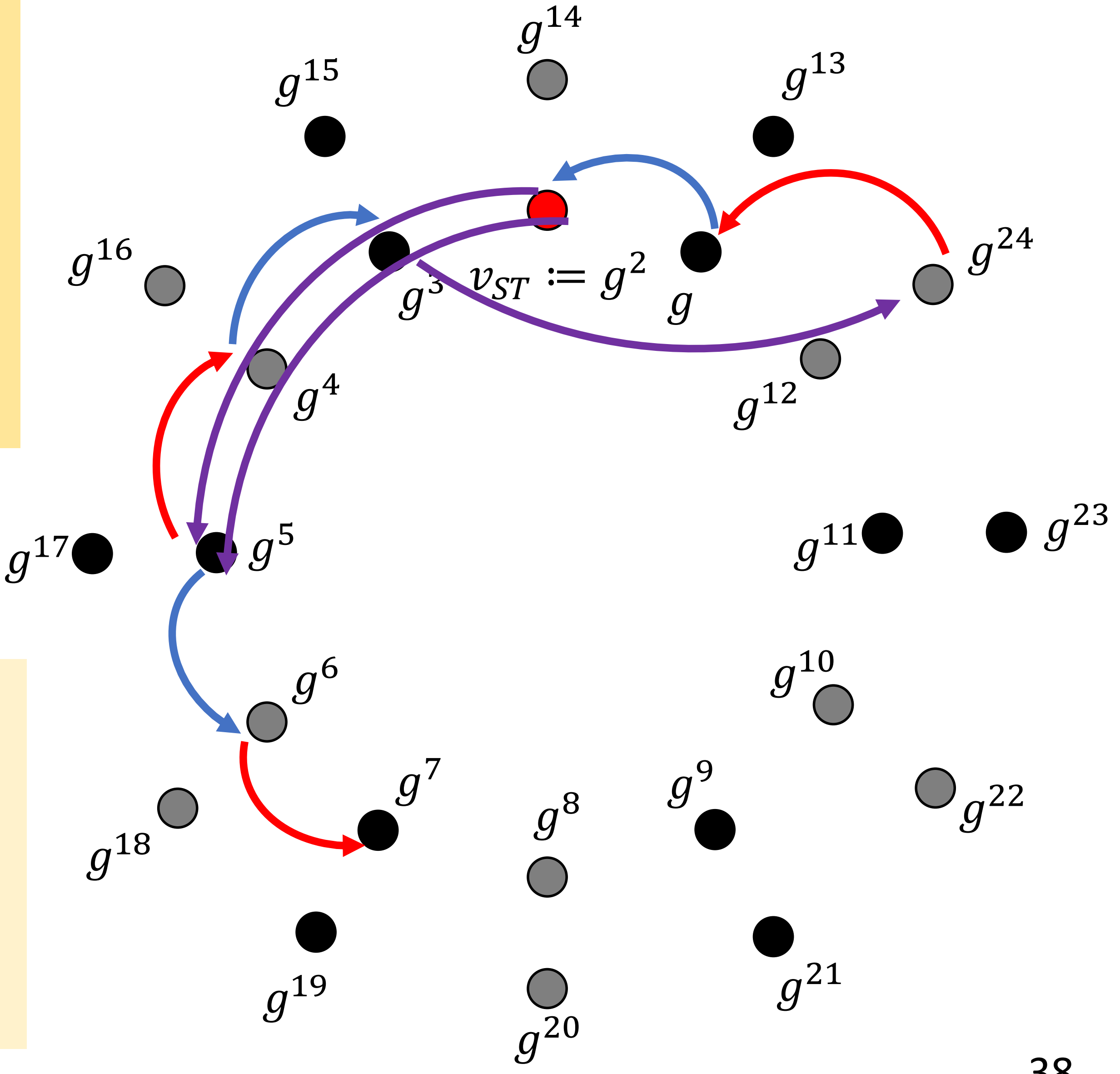
$\pi_{1,1}(0, g^{21}) = g$

$\pi_{1,1}(1, g^{21}) = g^{-1}$

$m = 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1$

$m_3 = 1, 0, 0, 1, 0, 1, 2$

$m_2 = 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1$



$H \to H$

Choice function $\pi_{0,0}$

$\pi_{0,0}(0, g^{12}) = g$

$\pi_{0,0}(1, g^{12}) = g^{3}$

$\pi_{0,0}(2, g^{12}) = g^{-1}$

$G - H \to H$

Choice function $\pi_{0,1}$

$\pi_{0,1}(0, g) = g$

$\pi_{0,1}(1, g) = g^{3}$

$\pi_{0,1}(2, g) = g^{12}$

$\pi_{0,1}(0, g^{-1}) = g^{-1}$

$\pi_{0,1}(1, g^{-1}) = g^{3}$

$\pi_{0,1}(2, g^{-1}) = g^{12}$

$\pi_{0,1}(0, g^{21}) = g$

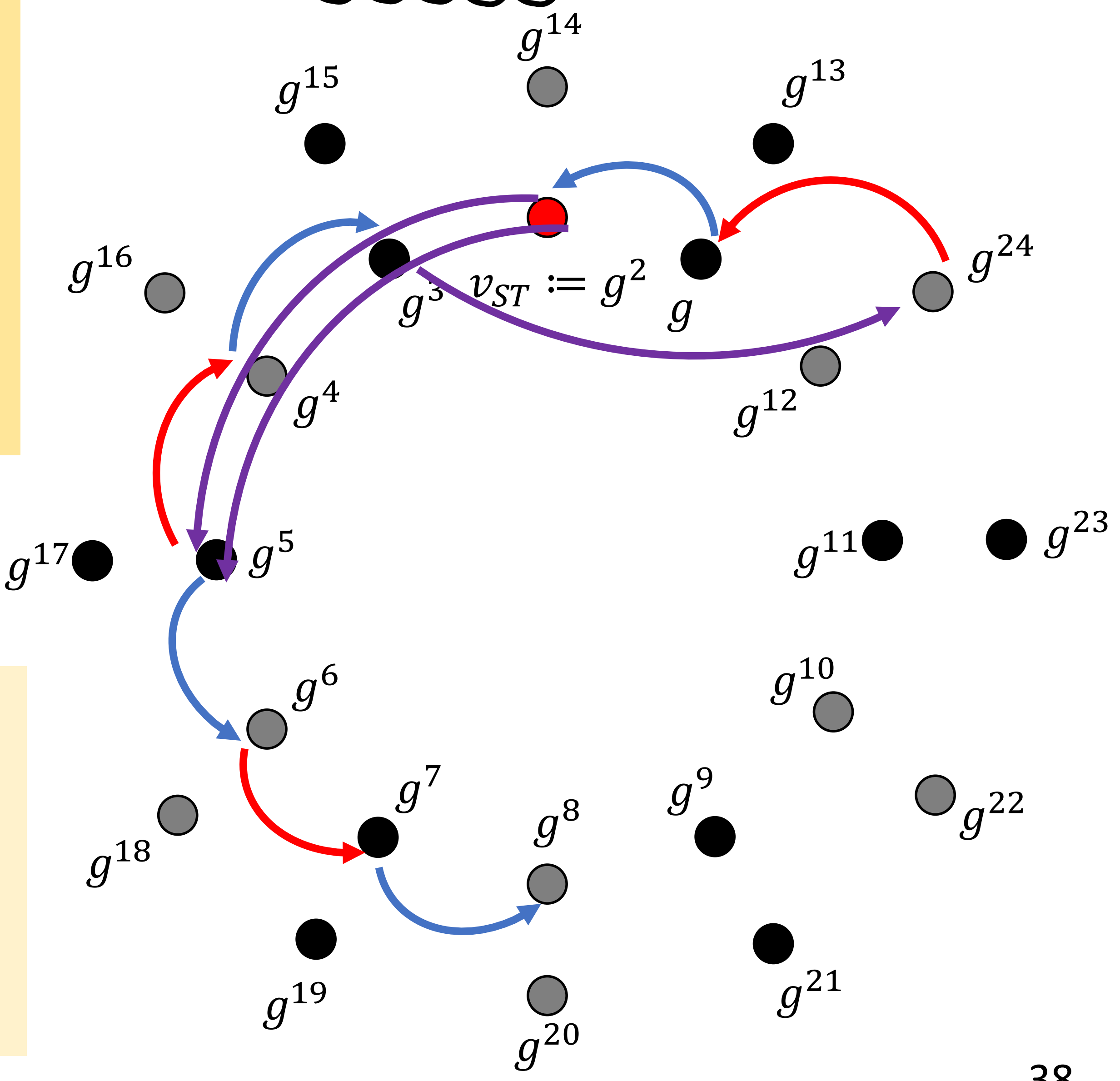
$\pi_{0,1}(1, g^{21}) = g^{-1}$

$\pi_{0,1}(2, g^{21}) = g^{12}$

$m \ \ = 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1$

$m_3 = 1, 0, 0, 1, 0, 1, 2$

$m_2 = 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1$



$H \to G - H$

Choice function $\pi_{1,0}$

$\pi_{1,0}(0, g) = g$

$\pi_{1,0}(1, g) = g^{21}$

$\pi_{1,0}(0, g^{-1}) = g^{21}$

$\pi_{1,0}(1, g^{-1}) = g^{-1}$

$\pi_{1,0}(0, g^{3}) = g$

$\pi_{1,0}(1, g^{3}) = g^{-1}$

$G - H \to G - H$

Choice function $\pi_{1,1}$

$\pi_{1,1}(0, g) = g$

$\pi_{1,1}(1, g) = g^{21}$

$\pi_{1,1}(0, g^{-1}) = g^{-1}$

$\pi_{1,1}(1, g^{-1}) = g^{21}$

$\pi_{1,1}(0, g^{21}) = g$

$\pi_{1,1}(1, g^{21}) = g^{-1}$

$H \to H$

Choice function $\pi_{0,0}$

$\pi_{0,0}(0, g^{12}) = g$

$\pi_{0,0}(1, g^{12}) = g^3$

$\pi_{0,0}(2, g^{12}) = g^{-1}$

$G - H \to H$

Choice function $\pi_{0,1}$

$\pi_{0,1}(0, g) = g$

$\boxed{\pi_{0,1}(1, g) = g^3}$

$\pi_{0,1}(2, g) = g^{12}$

$\pi_{0,1}(0, g^{-1}) = g^{-1}$

$\pi_{0,1}(1, g^{-1}) = g^3$

$\pi_{0,1}(2, g^{-1}) = g^{12}$

$\pi_{0,1}(0, g^{21}) = g$

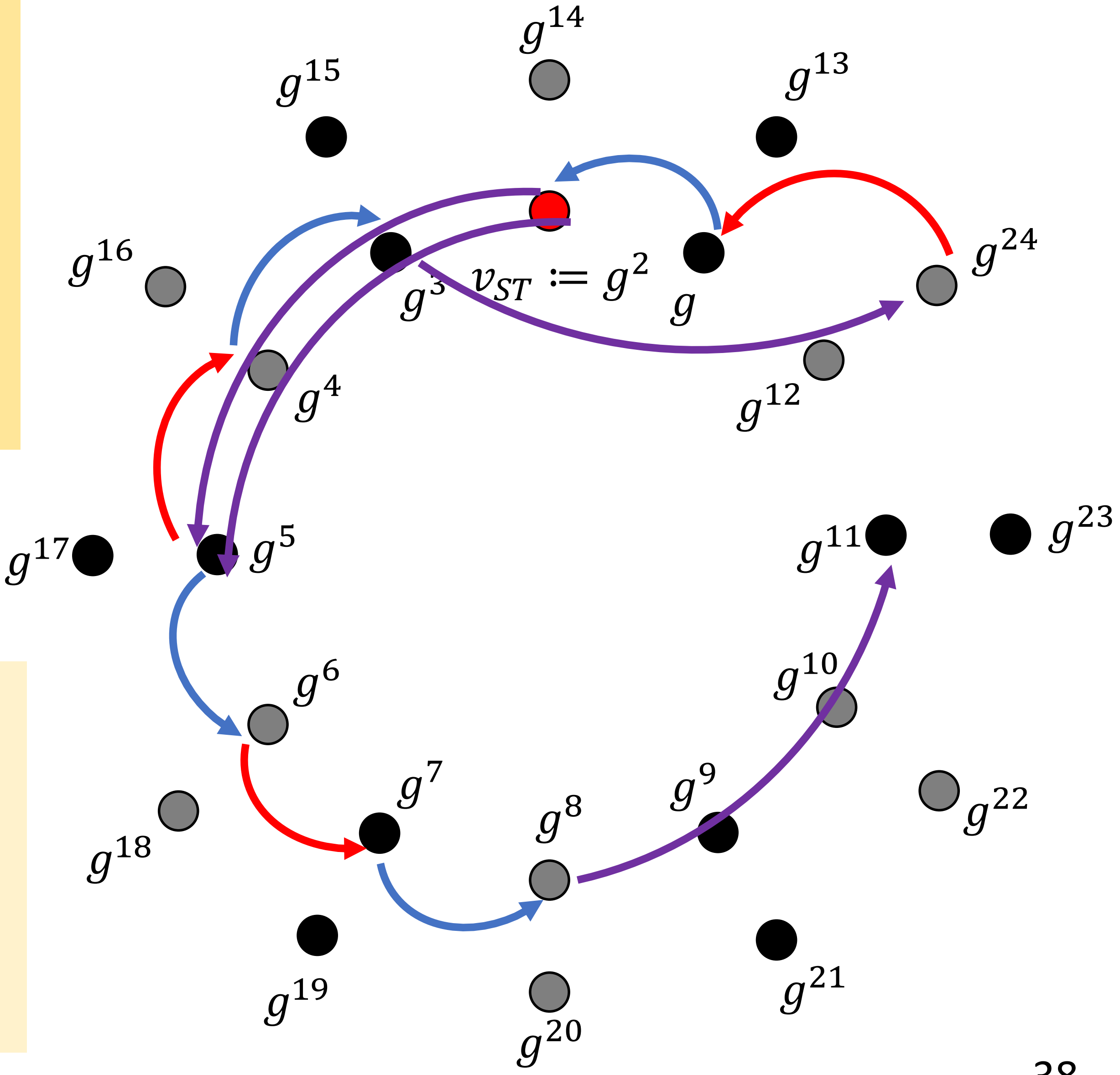
$\pi_{0,1}(1, g^{21}) = g^{-1}$

$\pi_{0,1}(2, g^{21}) = g^{12}$

$m\ \ = 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1$

$m_3 = 1, 0, 0, 1, 0, 1, 2$

$m_2 = 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1$



$H \to G - H$

Choice function $\pi_{1,0}$

$\pi_{1,0}(0, g) = g$

$\pi_{1,0}(1, g) = g^{21}$

$\pi_{1,0}(0, g^{-1}) = g^{21}$

$\pi_{1,0}(1, g^{-1}) = g^{-1}$

$\pi_{1,0}(0, g^3) = g$

$\pi_{1,0}(1, g^3) = g^{-1}$

$G - H \to G - H$

Choice function $\pi_{1,1}$

$\pi_{1,1}(0, g) = g$

$\pi_{1,1}(1, g) = g^{21}$

$\pi_{1,1}(0, g^{-1}) = g^{-1}$

$\pi_{1,1}(1, g^{-1}) = g^{21}$

$\pi_{1,1}(0, g^{21}) = g$

$\pi_{1,1}(1, g^{21}) = g^{-1}$

$H \to H$ $\qquad$ $G - H \to H$

Choice function $\pi_{0,0}$

$\pi_{0,0}(0, g^{12}) = g$

$\pi_{0,0}(1, g^{12}) = g^{3}$

$\pi_{0,0}(2, g^{12}) = g^{-1}$

Choice function $\pi_{0,1}$

$\pi_{0,1}(0, g) = g$

$\pi_{0,1}(1, g) = g^{3}$

$\pi_{0,1}(2, g) = g^{12}$

$\pi_{0,1}(0, g^{-1}) = g^{-1}$

$\pi_{0,1}(1, g^{-1}) = g^{3}$

$\pi_{0,1}(2, g^{-1}) = g^{12}$

$\pi_{0,1}(0, g^{21}) = g$

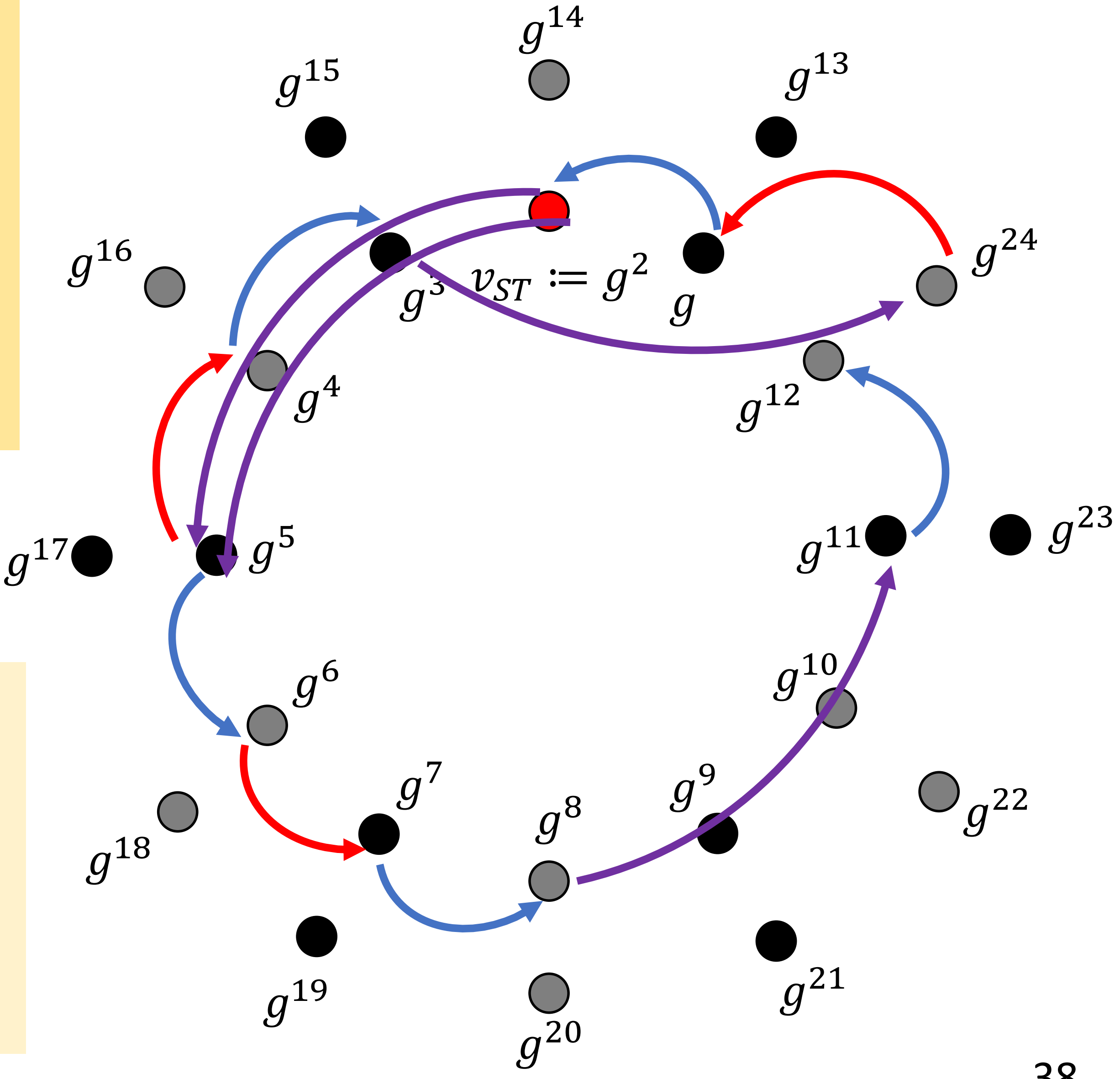
$\pi_{0,1}(1, g^{21}) = g^{-1}$

$\pi_{0,1}(2, g^{21}) = g^{12}$

$m \;\; = 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1$

$m_3 = 1, 0, 0, 1, 0, 1, 2$

$m_2 = 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1$



$H \to G - H$ $\qquad$ $G - H \to G - H$

Choice function $\pi_{1,0}$

$\pi_{1,0}(0, g) = g$

$\pi_{1,0}(1, g) = g^{21}$

$\pi_{1,0}(0, g^{-1}) = g^{21}$

$\pi_{1,0}(1, g^{-1}) = g^{-1}$

$\boxed{\pi_{1,0}(0, g^{3}) = g}$

$\pi_{1,0}(1, g^{3}) = g^{-1}$

Choice function $\pi_{1,1}$

$\pi_{1,1}(0, g) = g$

$\pi_{1,1}(1, g) = g^{21}$

$\pi_{1,1}(0, g^{-1}) = g^{-1}$

$\pi_{1,1}(1, g^{-1}) = g^{21}$

$\pi_{1,1}(0, g^{21}) = g$

$\pi_{1,1}(1, g^{21}) = g^{-1}$

$H \to H$

Choice function $\pi_{0,0}$

$\pi_{0,0}(0, g^{12}) = g$

$\pi_{0,0}(1, g^{12}) = g^{3}$

$\pi_{0,0}(2, g^{12}) = g^{-1}$

$G - H \to H$

Choice function $\pi_{0,1}$

$\pi_{0,1}(0, g) = g$

$\pi_{0,1}(1, g) = g^{3}$

$\pi_{0,1}(2, g) = g^{12}$

$\pi_{0,1}(0, g^{-1}) = g^{-1}$

$\pi_{0,1}(1, g^{-1}) = g^{3}$

$\pi_{0,1}(2, g^{-1}) = g^{12}$

$\pi_{0,1}(0, g^{21}) = g$

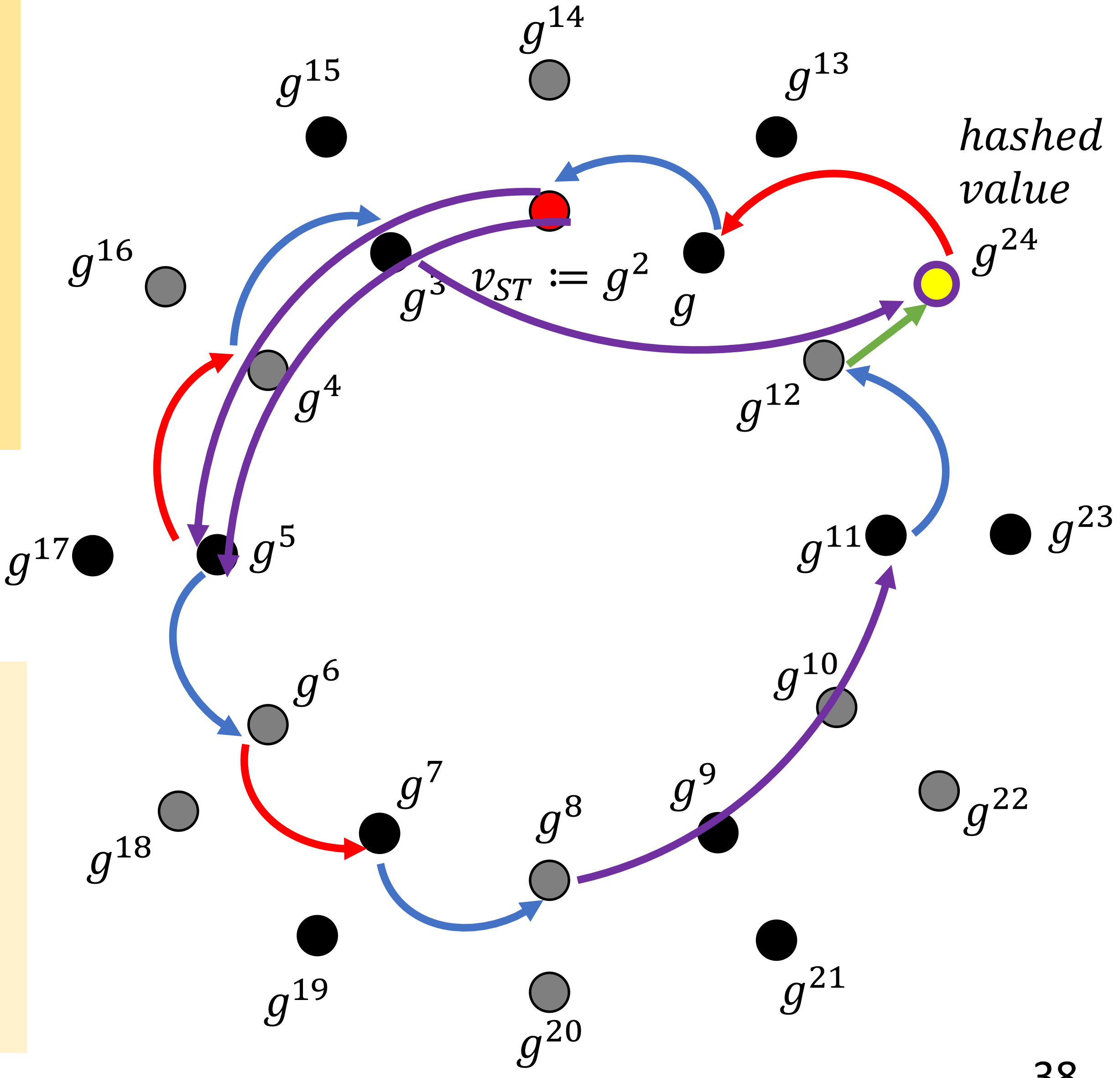
$\pi_{0,1}(1, g^{21}) = g^{-1}$

$\pi_{0,1}(2, g^{21}) = g^{12}$

$m \;= 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1$

$m_3 = 1, 0, 0, 1, 0, 1, 2$

$m_2 = 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1$



$H \to G - H$

Choice function $\pi_{1,0}$

$\pi_{1,0}(0, g) = g$

$\pi_{1,0}(1, g) = g^{21}$

$\pi_{1,0}(0, g^{-1}) = g^{21}$

$\pi_{1,0}(1, g^{-1}) = g^{-1}$

$\pi_{1,0}(0, g^{3}) = g$

$\pi_{1,0}(1, g^{3}) = g^{-1}$

$G - H \to G - H$

Choice function $\pi_{1,1}$

$\pi_{1,1}(0, g) = g$

$\pi_{1,1}(1, g) = g^{21}$

$\pi_{1,1}(0, g^{-1}) = g^{-1}$

$\pi_{1,1}(1, g^{-1}) = g^{21}$

$\pi_{1,1}(0, g^{21}) = g$

$\pi_{1,1}(1, g^{21}) = g^{-1}$

Discussions on proposals' security

Observations on the termination for hashing on multi-based messages

1) For a (d_1, d_2)-regular case, the hashing indicator is going in and out each messages almost alternatively.

2) A hashing process is terminated within $2|m_{d_1}|$ when $d_1 \geq d_2$.

3) If the degree are too big, a hashing process will be terminated quickly.

4) Recommend to choose degrees where $|d_1 - d_2|$ as small as possible.

A useful construction for instantiation

There is a convenient way to construct pair-graphs from existing Cayley graphs.

1. Start from a Cayley graph $Cay(H,S)$ with good properties (i.e. large girth or expansion).

2. Consider supergroup $\mathrm{H} \subseteq G$ and subset S' (derived from S') to construct pair-graph $\mathcal{G}\ (G,H,S')$ that inherits some of the group-properties.

The general idea

For a transversal $x_0, x_1, \cdots, x_k$ we obtain define subsets

$$S_i{}' = \{\, x_0\ \phi_i(s_i) :\ \ s \in S\,\}$$

for functions $\phi_i\colon H \to H$ and $i \le k$.

Then, $S' = S_1' \cup \cdots \cup S_k'$.

In this way we can obtain pair-graphs with large girth and we expect that high expansion can also be obtained in this way (but difficult).

Non-malleability

$$\mathcal{H}\ (m||m') \neq \mathcal{H}(m) \cdot \mathcal{H}(m')$$

Since our hash process is working on multi-number based messages, the malleability is NOT valid.

It seems one of the good virtues comparing to existed Cayley hashes.

Group word problems

It can be classified for a hash function from pair-graphs as similar as usual Cayley hashes.

It will be shown at “Towards hash functions based on group-subgroup pair graphs by Cid Reyes Bustos” CREST CryptoMath Book.

Some questions on pair-graphs

1. It is interesting **to find pair-graphs with large girth and expansion directly from the definitions**. (On-going work)

2. While the eigenvalues (both regular and Laplacian) are known for some cases, it would be interesting and useful to consider **characterizations of pair-graphs in terms only of the Laplacian operator**.

3. We may consider for **the constructions the extensions of groups-subgroup pair graphs** defined by **Kazufumi Kimoto** that offer more flexibility for the resulting graphs. (ex. Moore graph)

Thank you for your attention.

Q&A

jo-hyungrok-xz@ynu.ac.jp