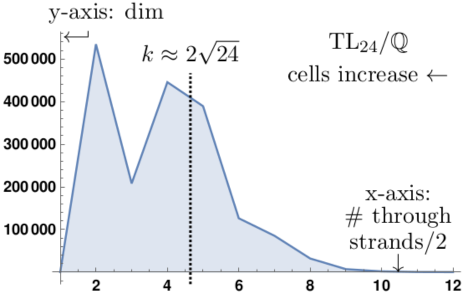
Monoidal categories, representation gap and cryptography

Or: Why I like dimensions

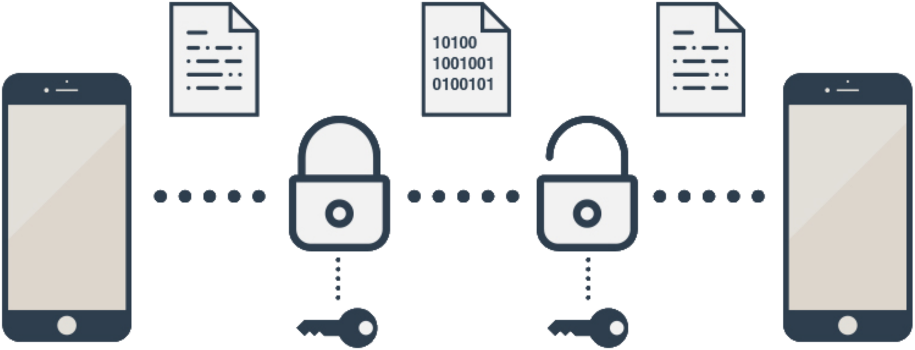
Daniel Tubbenhauer



Joint with Mikhail Khovanov and Maithreya Sitaraman

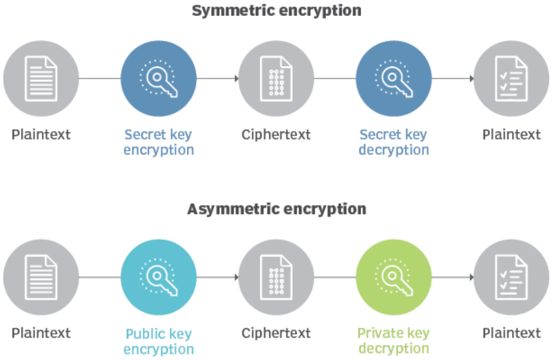
March 2022

End-to-end encryption



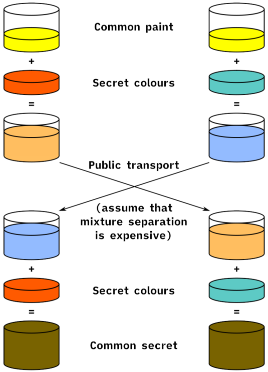
- E2EE Only the two communicating parties should decrypt the message
- Problem How to transfer the encryption key?
- Diffie–Hellman (DH) Addresses this problem

End-to-end encryption



- Symmetric Both parties us the same secret key
- Problem (still) How to transfer the encryption key?
- Asymmetric Both parties have a public and a private key, no sharing needed

End-to-end encryption



- DH Two secrets a, b, public g, send g^a or g^b and get $(g^b)^a = g^{ab} = (g^a)^b$
- Catch Relies on the mixtures to be hard ot decompose (discrete log problem)
- BTW Using colors is not practical ;-), so usually take $a, b \in \mathbb{N}, g \in (\mathbb{Z}/p\mathbb{Z})^x$

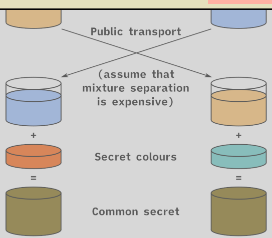
End-to-end encryption

Colors!

The color picture makes it clear that this can easily be generalized

For example, one could take a different group

Varying the protocol and one can even allow arbitrary monoids



- DH Two secrets a, b, public g, send g^a or g^b and get $(g^b)^a = g^{ab} = (g^a)^b$
- Catch Relies on the mixtures to be hard ot decompose (discrete log problem)
- BTW Using colors is not practical ;-), so usually take $a, b \in \mathbb{N}, g \in (\mathbb{Z}/p\mathbb{Z})^x$

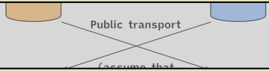
End-to-end encryption

Colors!

The color picture makes it clear that this can easily be generalized

For example, one could take a different group

Varying the protocol and one can even allow arbitrary monoids



Example (Shpilrain–Ushakov (SU) key exchange protocol)

The public data is a monoid S, and two sets $A, B \subset S$ of commuting elements and $g \in S$

Party A chooses privately $a, a' \in A$ and party B chooses privately $b, b' \in A$

Party A communicates aga', B sends bgb' and the common secret is $abgb'a' = baga'b'$

Note that S can be an arbitrary monoid in this protocol

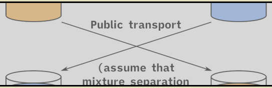
The complexity of S determines how difficult it
is to find the common secret from the public data

Colors!

The color picture makes it clear that this can easily be generalized

For example, one could take a different group

Varying the protocol and one can even allow arbitrary monoids



Example (Stickel's (St) key exchange protocol)

The public data is a monoid S, and two noncommuting elements $g, h \in S$, $gh \neq hg$

Party A chooses privately $a, a' \in \mathbb{N}$ and party B chooses privately $b, b' \in \mathbb{N}$

Party A communicates $g^a h^{a'}$, B sends $g^b h^{b'}$ and the common secret is $g^a g^b h^{b'} h^{a'} = g^b g^a h^{a'} h^{b'}$

Note that S can be an arbitrary monoid in this protocol

The complexity of S determines how difficult it
is to find the common secret from the public data

Linear attack (Myasnikov–Roman'kov ~2015)

"All" protocol involving monoids can be attacked
if the monoid admits a small non-trivial representation

Enter representation theory

No algebras, please (Myasnikov–Roman'kov ~2015)

Stay set-theoretical: algebras are easier to attack linearly

Computers and fields

The important ground fields in this business are $\mathbb{Q}$ or $\mathbb{F}_q$
(A computer doesn't know what $\mathbb{R}$ or $\mathbb{C}$ are)

- DH Two secrets a, b, public g, send g^a or g^b and get $(g^b)^a = g^{ab} = (g^a)^b$
- Catch Relies on the mixtures to be hard ot decompose (discrete log problem)
- BTW Using colors is not practical ;-), so usually take $a, b \in \mathbb{N}, g \in (\mathbb{Z}/p\mathbb{Z})^x$

Linear attack (Myasnikov–Roman'kov ∼2015)

"All" protocol involving monoids can be attacked
if the monoid admits a small non-trivial representation

Enter representation theory

No algebras, please (Myasnikov–Roman'kov ∼2015)

Stay set-theoretical: algebras are easier to attack linearly

Our idea

Systematically study and construct monoids with no small non-trivial representations

The abstract theory is governed by Green's theory of cells (Green's relations)

The good finite examples come from quantum topology and monoidal categories

Monoidal categories provide families of examples $S_n = \mathrm{End}_C(X^{\otimes n})$

Other examples we know come from 2-representation theory and fusion categories

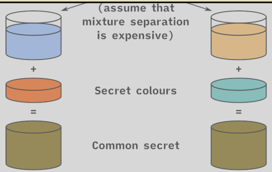
End-to-end encryption

A measure

A measure of whether a monoid resists linear attacks is the representation gap $\mathrm{gap}_{\mathbb{K}}(S)$:

The minimal m such that $M \ncong \mathbb{1}_{bt}^{\oplus k}$ with $\dim M = m$ exists

Up to extensions, the gap is $\min\{\dim L | L \text{ simple, non-trivial}\}$



- DH Two secrets a, b, public g, send g^a or g^b and get $(g^b)^a = g^{ab} = (g^a)^b$
- Catch Relies on the mixtures to be hard ot decompose (discrete log problem)
- BTW Using colors is not practical ;-), so usually take $a, b \in \mathbb{N}, g \in (\mathbb{Z}/p\mathbb{Z})^x$

End-to-end encryption

A measure

A measure of whether a monoid resists linear attacks is the representation gap $\mathrm{gap}_{\mathbb{K}}(S)$:

The minimal m such that $M \ncong \mathbb{1}_{bt}^{\oplus k}$ with $\dim M = m$ exists

Up to extensions, the gap is $\min\{\dim L | L \text{ simple, non-trivial}\}$

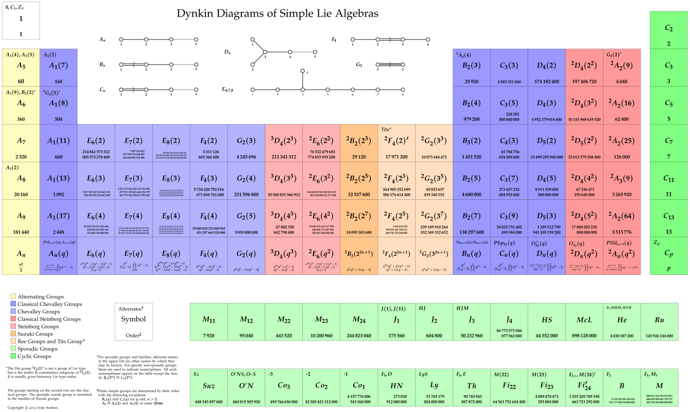
The point

Make a list of families of monoids S_n
with large $\mathrm{gap}_{\mathbb{K}}(S_n)$ compared to $|S_n|$

Whether these are really useful for cryptography
is a question for later ;-)

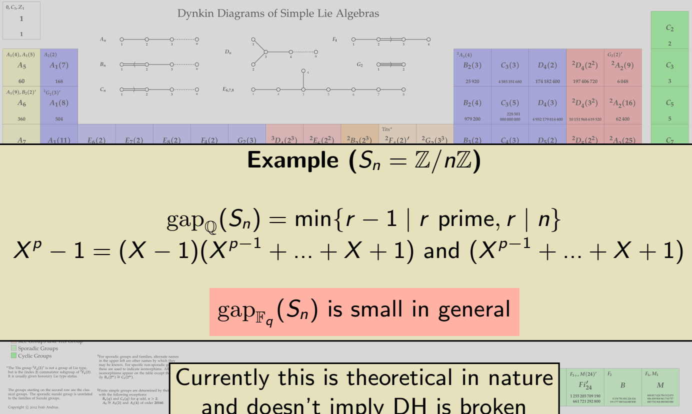
- DH Two se… $\ldots{}^{b})^{a} = g^{ab} = (g^{a})^{b}$
- Catch Relies … screte log problem)
- BTW Using colors is not practical ;-), so usually take $a, b \in \mathbb{N}, g \in (\mathbb{Z}/p\mathbb{Z})^{x}$

Examples and non-examples



- Classical examples Cyclic groups have a big representation gap over $\mathbb{Q}$
- Non-examples Groups of Lie type have quite small representations
- Non-examples Sporadic groups are too sporadic to be useful

Examples and non-examples



Example ($S_n = \mathbb{Z}/n\mathbb{Z}$)

$$\mathrm{gap}_{\mathbb{Q}}(S_n) = \min\{r-1 \mid r \text{ prime}, r \mid n\}$$

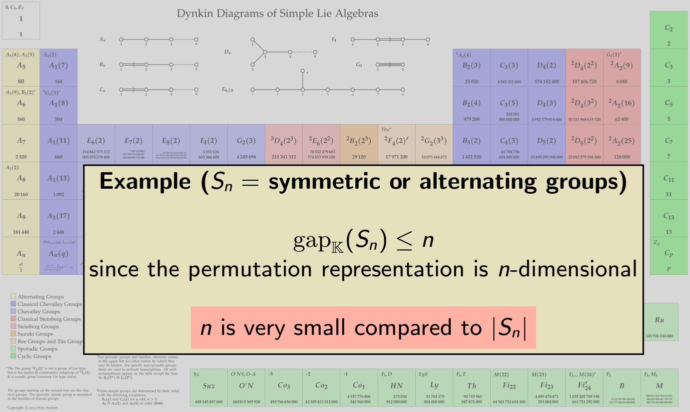
since *e.g.* $X^p - 1 = (X-1)(X^{p-1} + \dots + X + 1)$ and $(X^{p-1} + \dots + X + 1)$ is irreducible

$\mathrm{gap}_{\mathbb{F}_q}(S_n)$ is small in general

Currently this is theoretical in nature and doesn't imply DH is broken

- Classical examples Cyclic groups have a big representation gap over $\mathbb{Q}$
- Non-examples Groups of Lie type have quite small representations
- Non-examples Sporadic groups are too sporadic to be useful

Examples and non-examples



Example (S_n = symmetric or alternating groups)

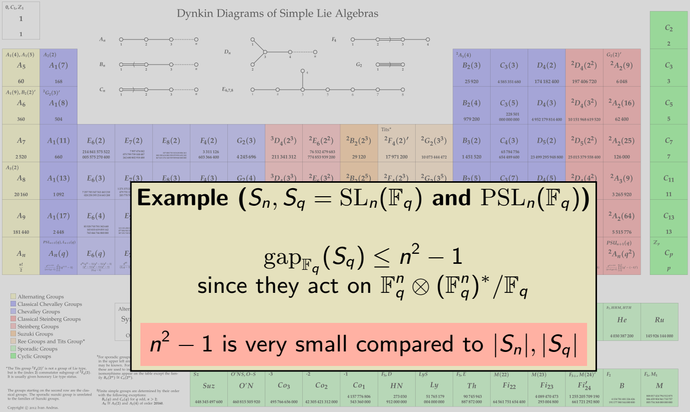
$$\mathrm{gap}_{\mathbb{K}}(S_n) \leq n$$

since the permutation representation is n-dimensional

n is very small compared to $|S_n|$

- Classical examples Cyclic groups have a big representation gap over $\mathbb{Q}$
- Non-examples Groups of Lie type have quite small representations
- Non-examples Sporadic groups are too sporadic to be useful

Examples and non-examples



Example ($S_n, S_q = \mathrm{SL}_n(\mathbb{F}_q)$ **and** $\mathrm{PSL}_n(\mathbb{F}_q)$)

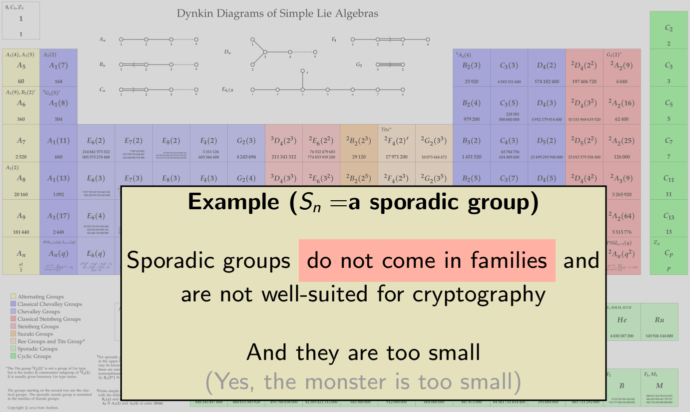
$$\mathrm{gap}_{\mathbb{F}_q}(S_q) \leq n^2 - 1$$

since they act on $\mathbb{F}_q^n \otimes (\mathbb{F}_q^n)^* / \mathbb{F}_q$

$n^2 - 1$ is very small compared to $|S_n|, |S_q|$

- Classical examples Cyclic groups have a big representation gap over $\mathbb{Q}$
- Non-examples Groups of Lie type have quite small representations
- Non-examples Sporadic groups are too sporadic to be useful

Examples and non-examples



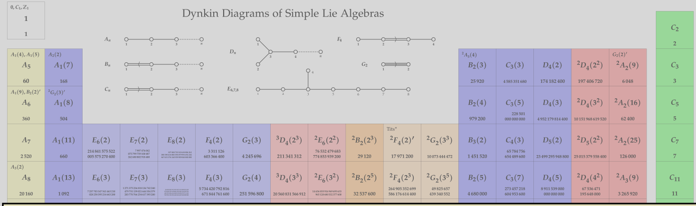
Example (S_n =a sporadic group)

Sporadic groups do not come in families and are not well-suited for cryptography

And they are too small
(Yes, the monster is too small)

- Classical examples Cyclic groups have a big representation gap over $\mathbb{Q}$
- Non-examples Groups of Lie type have quite small representations
- Non-examples Sporadic groups are too sporadic to be useful

Examples and non-examples



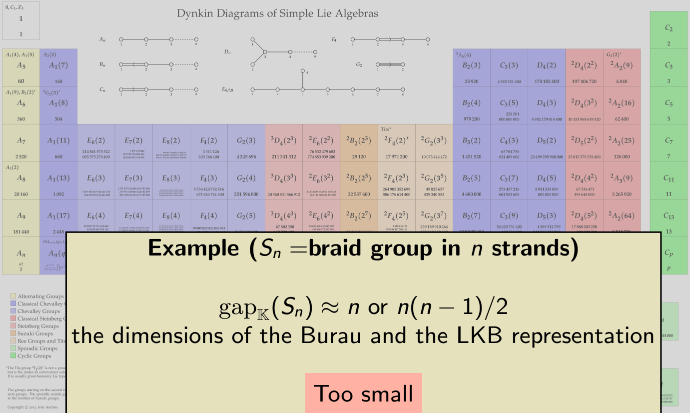
Summary

The finite simple groups (not quite all finite groups)
are not well-suited for cryptography, or are abelian

In the realm of groups, one mostly needs to stay with infinite groups
such as Artin, Thompson, Grigorchuk groups and alike

- Classical examples Cyclic groups have a big representation gap over $\mathbb{Q}$
- Non-examples Groups of Lie type have quite small representations
- Non-examples Sporadic groups are too sporadic to be useful

Examples and non-examples



Example (S_n =braid group in n strands)

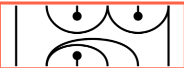
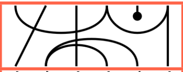
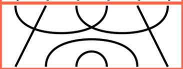
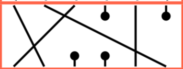
$$\mathrm{gap}_{\mathbb{K}}(S_n) \approx n \text{ or } n(n-1)/2$$

the dimensions of the Burau and the LKB representation

Too small

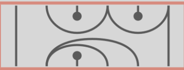
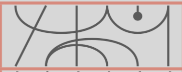
- Classical examples Cyclic groups have a big representation gap over $\mathbb{Q}$
- Non-examples Groups of Lie type have quite small representations
- Non-examples Sporadic groups are too sporadic to be useful

Examples and non-examples

Symbol	Diagrams	Useful?	Symbol	Diagrams	Useful?
pPa_n		YES*	Pa_n		YES*
Mo_n		YES	$RoBr_n$		YES*
TL_n		YES	Br_n		YES*
pRo_n		YES*	Ro_n		YES*
pS_n		EX	S_n		NO

- New examples Finite monoids coming from quantum topology
- More specific Submonoids of the partition monoid above
- Widely open I claim your favorite example from quantum topology will also work

Examples and non-examples

Symbol	Diagrams	Useful?	Symbol	Diagrams	Useful?
pPa_n		YES*	Pa_n		YES*
Mo_n		YES	RoBr_n		YES*
T					
pl					
p					

Task

Find good lower bounds and growth rates for the representation gap

Observation

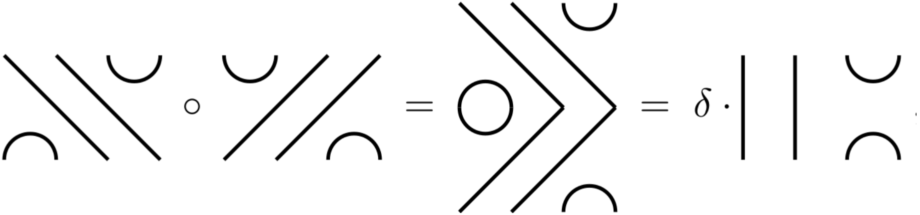
This is mostly open, even for groups:
in representation theory researchers prefer(?) precise numbers
and bounds are not very common

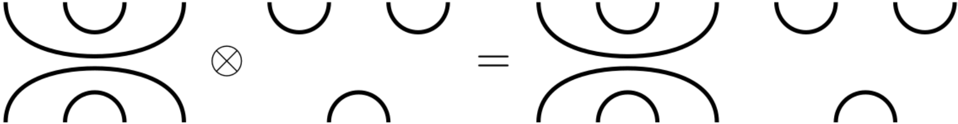
- New examples Finite monoids coming from quantum topology

I will zoom in on Temperley–Lieb now

- More specific Submonoids of the partition monoid above
- Widely open I claim your favorite example from quantum topology will also work

Temperley–Lieb works!

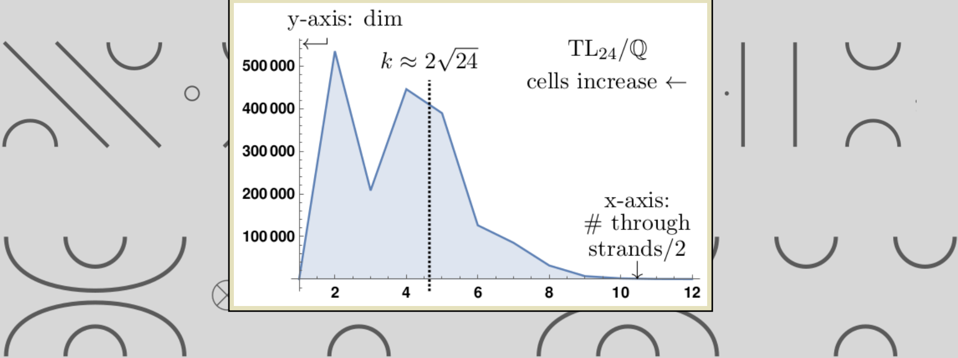




- Monoidal category example The Temperley–Lieb monoid TL_n (circle$=\delta=$1)
- TL_n has one simple L_k per $k \in \{n, n-2, ..., 1 \text{ or } 0\}$ (through strands)
- Extensions $\mathbb{1}_{bt} \to M \to \mathbb{1}_{bt}$ are all trivial

Temperley–Lieb works!

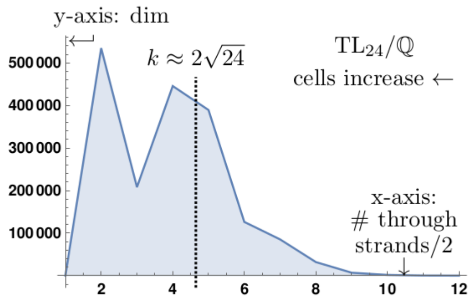
Dimensions of simple TL_{24}-representations



- Monoidal category example The Temperley–Lieb monoid TL_n (circle$=\delta=1$)
- TL_n has one simple L_k per $k \in \{n, n-2, \dots, 1 \text{ or } 0\}$ (through strands)
- Extensions $\mathbb{1}_{bt} \to M \to \mathbb{1}_{bt}$ are all trivial

Temperley–Lieb works!

Dimensions of simple TL_{24}-representations



- Monoida ... (circle= δ =1)
- TL_n has ... strands)
- Extension

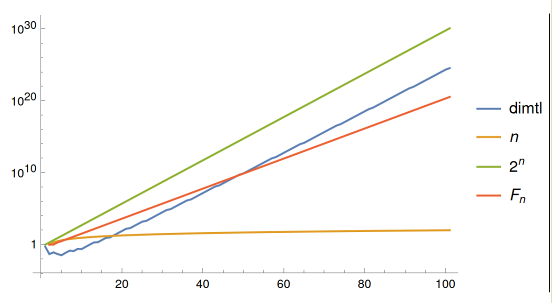
Example (following Spencer ∼2021)

After appropriate truncation
the representation gap of TL_n is bounded from below by

$$\frac{4}{(n+\lfloor 2\sqrt{n}\rfloor+2)(n+\lfloor 2\sqrt{n}\rfloor+4)}\binom{n}{(n+\lfloor 2\sqrt{n}\rfloor)/2} \in \Theta(2^n n^{-5/2})$$

Temperley–Lieb works!

Logplot of the lower bound



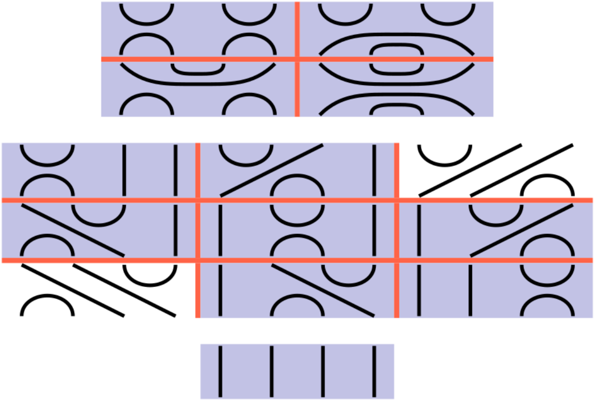
Example (following Spencer ∼2021)

After appropriate truncation
the representation gap of TL_n is bounded from below by

$$\frac{4}{(n+\lfloor 2\sqrt{n}\rfloor+2)(n+\lfloor 2\sqrt{n}\rfloor+4)}\binom{n}{(n+\lfloor 2\sqrt{n}\rfloor)/2} \in \Theta(2^n n^{-5/2})$$

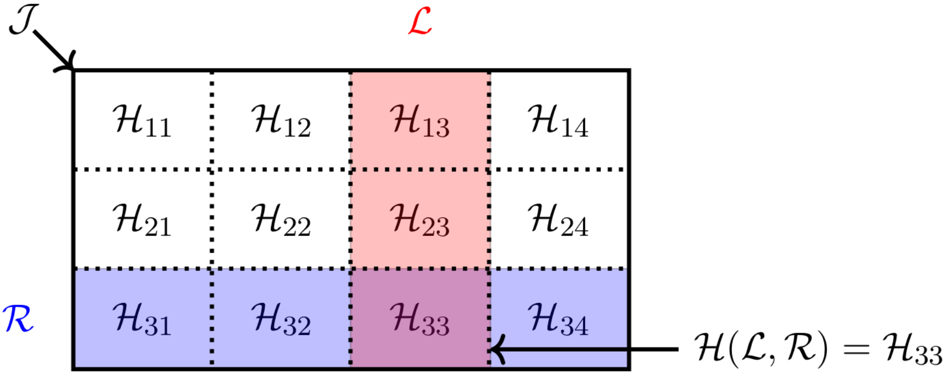
- Monoida (circle= δ =1)
- TL_n has strands)
- Extension

The "How to" – some theory



- Left order $\leq_l$: $a \leq_l b \Leftrightarrow \exists c : b = ca$
- Left cells: $(a \sim_l b) \Leftrightarrow (a \leq_l b \text{ and } b \leq_l a)$
- Right and two-sided are defined similar
- Green cells structure monoids

The “How to” – some theory



- Left cells $\mathcal{L}$
- Right cells $\mathcal{R}$
- Two-sided cells $\mathcal{J}$
- *H*-cells = intersection of a left and a right cell

The "How t

$\mathcal{J}$

$\mathcal{H}_{11}$

$\mathcal{H}_{21}$

$\mathcal{R}$ $\mathcal{H}_{31}$ $\mathcal{H}_{32}$

$\mathcal{H}(\mathcal{L}, \mathcal{R}) = \mathcal{H}_{33}$

Example (transformation monoid $T_n = \mathrm{End}(\{1, ..., n\})$)

(111)
(222)
(333)

$(122), (221)$	$(121), (212)$	$(221), (112)$
$(133), (331)$	$(313), (131)$	$(113), (311)$
$(233), (322)$	$(323), (232)$	$(223), (332)$

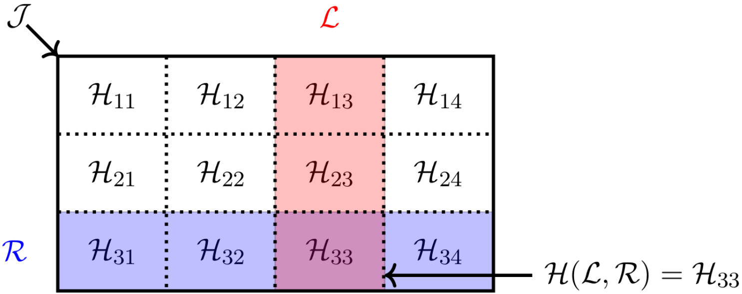
$(123), (213), (132)$ $(231), (312), (321)$

Example ($C_{3,2} = \langle a | a^{3+2} = a^3 \rangle$)

a^3, a^4
a^2
a
1

- Left cells $\mathcal{L}$
- Right cells $\mathcal{R}$
- Two-sided cells $\mathcal{J}$
- H-cells $=$ intersecti

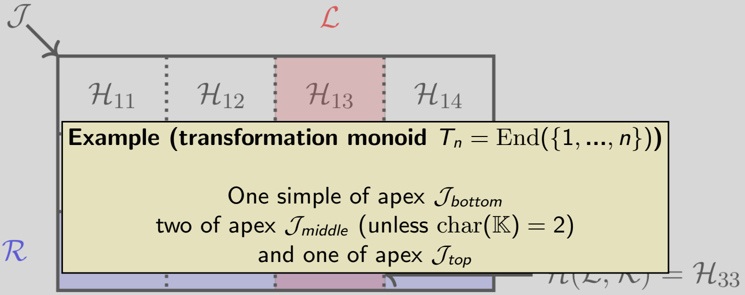
The “How to” – some theory



- If H-cells contain idempotents, then they are groups
- Each simple S-representation has an associated apex $\mathcal{J}$
- Clifford–Munn–Ponizovskiĭ theorem For a monoid S:

$$\{\text{simple } S\text{-representations of apex } \mathcal{J}\}/\cong \xleftrightarrow{1:1} \{\text{simple } \mathcal{H}(e)\text{-representations}\}/\cong,$$

where $\mathcal{H}(e) \subset \mathcal{J}$ is any idempotent H-cell.



Example (transformation monoid $T_n = \mathrm{End}(\{1, ..., n\})$)

One simple of apex $\mathcal{J}_{bottom}$
two of apex $\mathcal{J}_{middle}$ (unless $\mathrm{char}(\mathbb{K}) = 2$)
and one of apex $\mathcal{J}_{top}$

- If H-cells contain idempotents, then they are groups
- Each simple S-rep
- Clifford–Munn–P

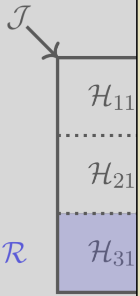
Example ($C_{3,2} = \langle a | a^{3+2} = a^3 \rangle$)

One simple of apex $\mathcal{J}_{bottom}$
two of apex $\mathcal{J}_{top}$ (unless $\mathrm{char}(\mathbb{K}) = 2$)

$$\{\text{simple } S\text{-representations of apex } \mathcal{J}\}/\cong \xleftrightarrow{1:1} \{\text{simple } \mathcal{H}(e)\text{-representations}\}/\cong,$$

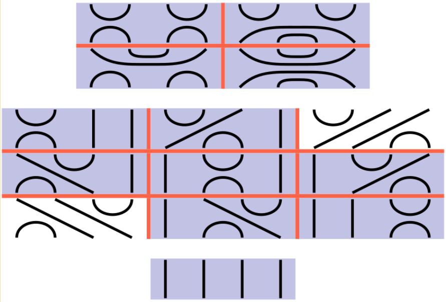
where $\mathcal{H}(e) \subset \mathcal{J}$ is any idempotent H-cell.

The "How to" – some theory



$, \mathcal{R}) = \mathcal{H}_{33}$

Example (back to Temperley–Lieb)

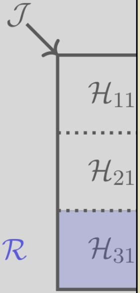


One simple of apex $\mathcal{J}_k$
where k =number of through strands)

- If H-cells conta
- Each simple S-r
- Clifford–Munn–Ponizovskiĭ theorem For a monoid S:

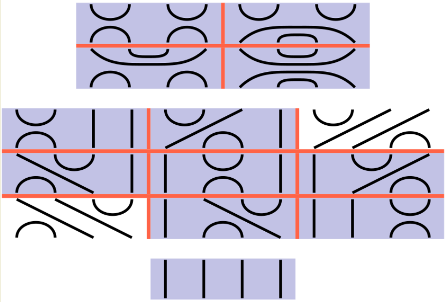
$$\{\text{simple } S\text{-representations of apex } \mathcal{J}\}/\cong \xleftrightarrow{1:1} \{\text{simple } \mathcal{H}(e)\text{-representations}\}/\cong,$$

where $\mathcal{H}(e) \subset \mathcal{J}$ is any idempotent H-cell.



$\mathcal{C}, \mathcal{R}) = \mathcal{H}_{33}$

Example (back to Temperley–Lieb)



One simple of apex $\mathcal{J}_k$
where k =number of through strands)

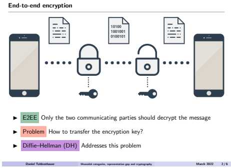
- If H-cells conta
- Each simple S-r
- Clifford–Mun

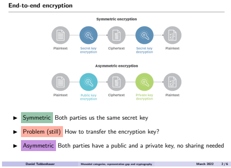
Remark

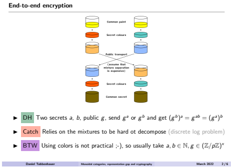
Using Gram/pairing matrices (works in general)
one can compute the simple dimensions

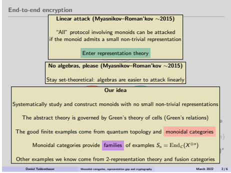
{simple S-represent … resentations}/ $\cong$,

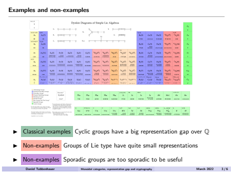
where $\mathcal{H}(e) \subset \mathcal{J}$ is any idempotent H-cell.

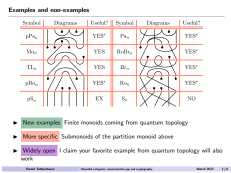


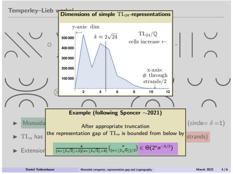


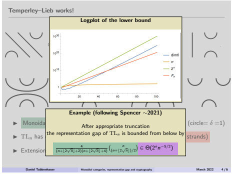


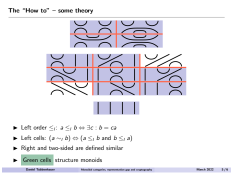




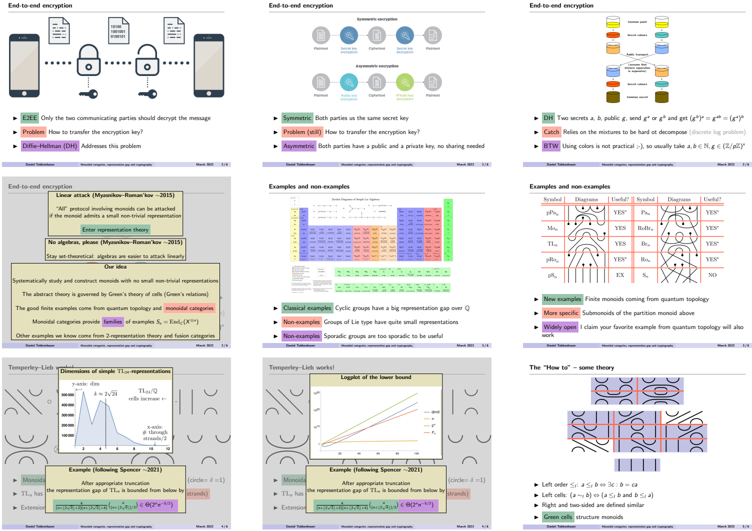








There is still much to do...



Thanks for your attention!