Potential master or Ph.D. project of I WANT YOU in 2023

Daniel Tubbenhauer

2023

Key information

Candidate. I WANT YOU.

Email. YOUR EMAIL.

Research areas. Algebra, representation theory, and cryptography, more specifically diagrammatic categories and algebras and the size of their representations.

Title. *"Monoidal categories and cryptography"*.

First read. [KST22].

Some of the most important cryptographic protocols in use today are based on commutative groups and deliver a gold standard for cryptography (modulo the fear of quantum computers). On the other hand, noncommutative group-based and monoid-based protocols seem to be less understood and in many cases admit efficient attacks.

There has been many ideas and there is an extensive literature on constructing cryptographic protocols from noncommutative groups and monoids (monoids generalize groups and we switch to saying monoids from now on), see *e.g.* [MSU08], [MSU11] and references therein. As shown by Myasnikov and Roman'kov [MR15] (and also based on earlier work), most protocols and can be successfully attacked if the monoids in question admits small nontrivial representations. This is called a linear attack.

One of the consequences of linear attacks is that finite noncommutative groups may not be suited for cryptographic purposes as they admit nontrivial representations of moderate size. For a toy example, the symmetric group on $\{1,\dots,n\}$ has $n!$ elements, but admits a faithful $(n-1)$-dimensional representation. The dimension of this representation is logarithmic in the size of the group, and the symmetric group would be a poor choice for various standard noncommutative group protocols.

The paper [KST22] explores finite monoids (mostly coming from monoidal categories), and proposes a systematic study of such monoids with an eye on big representations. That is, to overcome linear attacks [KST22] proposes to look at monoids with only big representations, in the sense made precise in that paper, and undertake a systematic study of such monoids. A large supply of monoids is delivered by monoidal categories. Usually, one considers examples of monoidal categories of diagrammatic origin, including the Temperley–Lieb, the Brauer and partition categories, and one discusses lower bounds for their representations.

Minimal goal. Summarize the paper of about representation gaps and cryptography in your own words.
Average goal. There are a many questions left open in [KST22] which should be treated. For example, regarding the Motzkin monoid.
Optimal goal (for Ph.D.). Address some of the open questions mentioned below.
Key. Use diagrammatic methods and combinatorial ways to bound dimensions of, or give growth rates for, representations of diagram monoids.

The thesis in details – minimal goal

The minimal master project should be structured as follows.

- Write an introduction and explain the main ideas of monoidal, see *e.g.* [EGNO15] or [TV17]. Explain how your mater thesis fits into this framework, *i.e.* in what sense diagrammatic monoids
- Summarize basics about diagrammatic algebra, see *e.g.* [TV17, Chapter I].
- Explain the diagrammatic monoids in [KST22, (1E.1)].
- Explain [KST22, Section 4] and how it relates to questions in cryptography.

The thesis in details – average goal

As above, but add:

- Address the question left open in [KST22, Section 4F] regarding extensions of the Motzkin monoid.
- Try to find better bounds for the dimensions of simple representations of the Motzkin monoid, *cf.* [KST22, Section 4F] where the bounds are based on the Temperley–Lieb monoid.

The thesis in details – optimal goal

Here are some open question which (if time suffices) deserve further study.

- Can one obtain better bounds for dimensions of the simple representations of the Temperley–Lieb monoid than the ones in [Spe20]?
- Can one find any bounds or formulas for the dimensions of the simple representations of the Brauer monoid, *i.e.* not just the semisimple ones discussed in, for example, [HJ20]?
- Is there good abstract theory that can be used for bounding dimensions of monoid representations, *e.g.* by diving into [Ste16] and implementing this theory further into [KST22]?
- As for applications to cryptography, you need a platform that provides not only security, but also efficiency, and it also has to be computer-friendly, *i.e.* operations should be easily translated to a computer code. Can this be addressed for diagram monoids?

References

[EGNO15] P. Etingof, S. Gelaki, D. Nikshych, and V. Ostrik. *Tensor categories*, volume 205 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2015. doi:10.1090/surv/205.

[HJ20] T. Halverson and T.N. Jacobson. Set-partition tableaux and representations of diagram algebras. *Algebr. Comb.*, 3(2):509–538, 2020. URL: https://arxiv.org/abs/1808.08118, doi:10.5802/alco.102.

[KST22] M. Khovanov, M. Sitaraman, and D. Tubbenhauer. Monoidal categories, representation gap and cryptography. 2022. URL: https://arxiv.org/abs/2201.01805.

[MR15] A. Myasnikov and V. Roman'kov. A linear decomposition attack. *Groups Complex. Cryptol.*, 7(1):81–94, 2015. URL: https://arxiv.org/abs/1412.6401, doi:10.1515/gcc-2015-0007.

[MSU08] A. Myasnikov, V. Shpilrain, and A. Ushakov. *Group-based cryptography*. Advanced Courses in Mathematics. CRM Barcelona. Birkhäuser Verlag, Basel, 2008.

[MSU11] A. Myasnikov, V. Shpilrain, and A. Ushakov. *Non-commutative cryptography and complexity of group-theoretic problems*, volume 177 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2011. With an appendix by Natalia Mosina. doi:10.1090/surv/177.

[Spe20] R.A. Spencer. The modular Temperley–Lieb algebra. 2020. URL: https://arxiv.org/abs/2011.01328.

[Ste16] B. Steinberg. *Representation theory of finite monoids*. Universitext. Springer, Cham, 2016. doi:10.1007/978-3-319-43932-7.

[TV17] V.G. Turaev and A. Virelizier. *Monoidal categories and topological field theory*, volume 322 of *Progress in Mathematics*. Birkhäuser/Springer, Cham, 2017. doi:10.1007/978-3-319-49834-8.