Daniel Tubbenhauer
daniel.tubbenhauer@sydney.edu.au The University of Sydney

THE UNIVERSITY OF SYDNEY

Address
The University of Sydney
F07 - Carslaw Building
Office Carslaw 827
NSW 2006, Australia

web www.dtubbenhauer.com
mobile +61 (0) 422528844
mobile +49 (0) 15126238157

My short- and long-term research goals

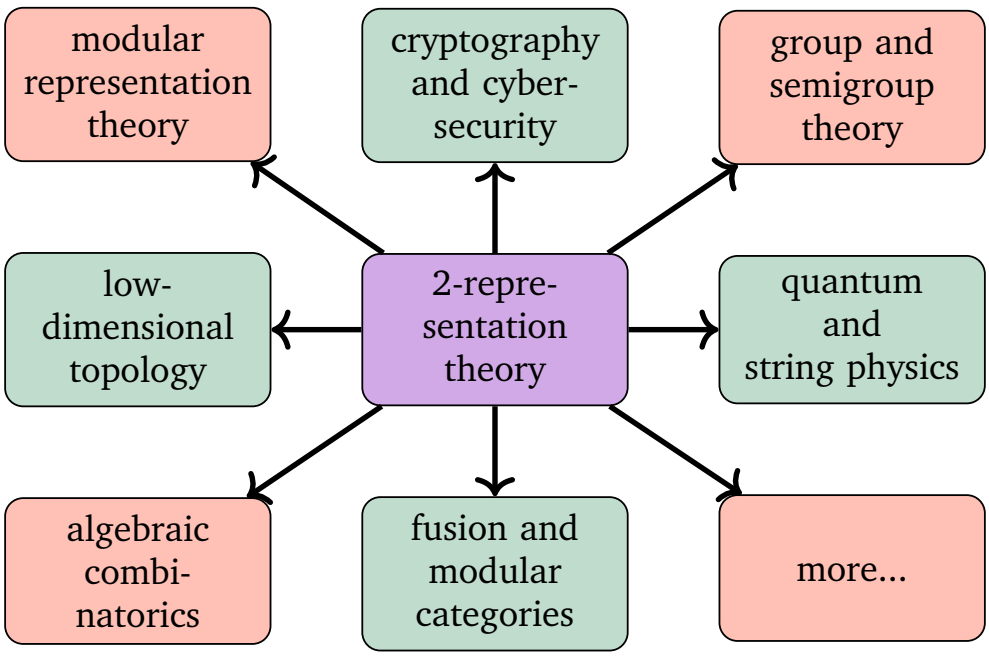
Aims and background

Over the last 20 years we witnessed history of mathematics in its making with Khovanov's discovery of his celebrated categorification of the Jones polynomial [Kh00]. In 2021 google scholar lists more than 1300 citations to [Kh00], while Scopus/MathSciNet list about 500 citations, all phenomenal numbers for mathematics, including citations beyond mathematics from fields such as molecular chemistry. This discovery was transformative, and since then it has become clear that functorial actions provide the right language for understanding Khovanov's work, and its generalizations, and these actions have now been axiomatized into the emerging field of 2-representation theory. (See *e.g.* [CR08], [EGNO15] or [Ma17] for various flavors of 2-representation theory.)

This new field is at heart of an explosion of new discoveries across a range of fields including algebraic geometry, combinatorics, representation theory, low-dimensional topology (see also Aspect (B)), and cryptography (see also Aspect (C)) and it is expected that there will be future applications in physics, chemistry, and potentially cybersecurity.

My research is focused on three aspects involving 2-representation theory:

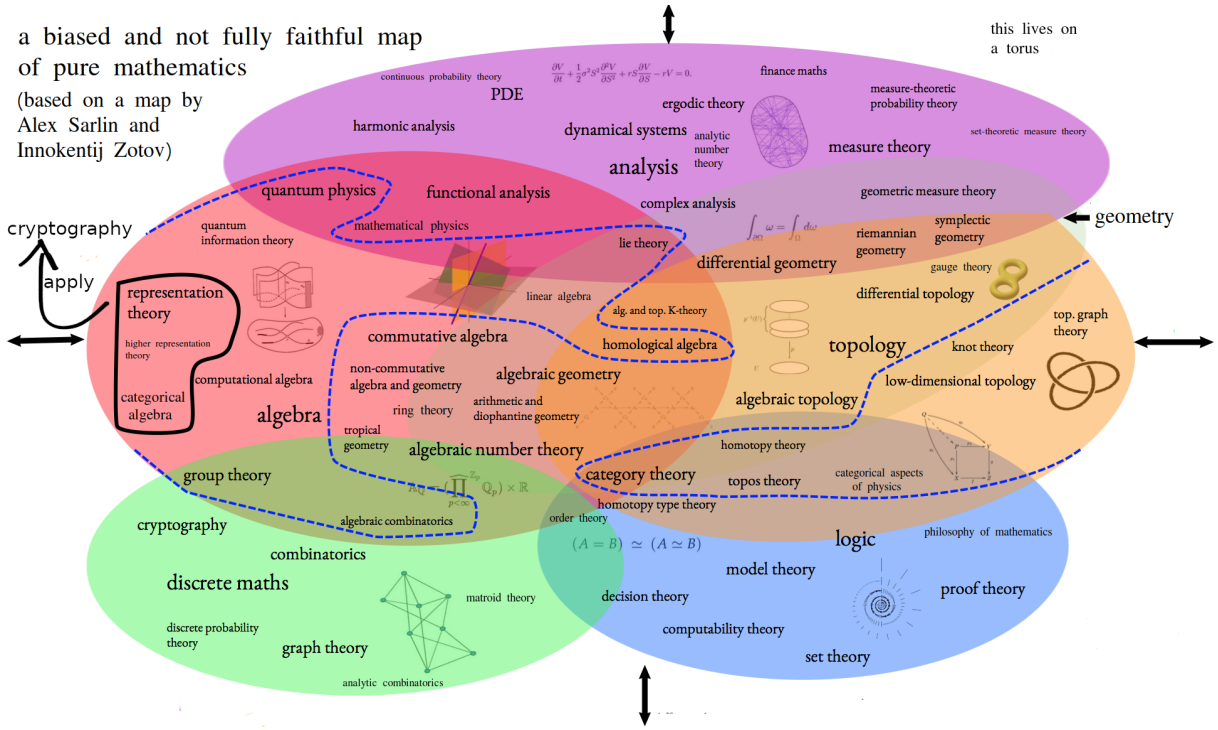
(A) *The abstract theory*: allow infinite 2-categories and work in finite characteristic.
(B) *Low-dimensional topology*: link homologies and 2-representations of braid groups.
(C) *Cryptography*: diagram categories and linear attacks.



(1)

Where do I stand?

Here is a very biased map of pure mathematics (this lives on a torus – if you exit from the top you reenter from the bottom, and similarly for left-right):



The black circle indicates my home, the dashes line where I like to apply representation theory. Recently I added cryptography to the range of my applications, which does not quite fit onto the map so I added.

Background.

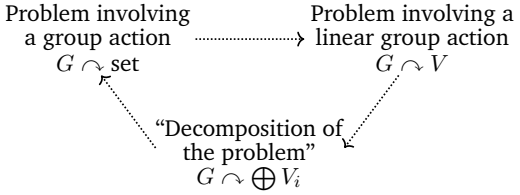
The study of group actions is of critical importance in mathematics and related fields such as physics and chemistry. Its significance can hardly be overestimated.

The approach of Frobenius ∼1895, Burnside ∼1900 and many others, nowadays called **representation theory** (or I would say the representation theory of the 20th century), is to linearly approximate such actions. For example, let G be a group or a ring or an algebra *etc.* Representation theory is the study of linear group actions

$$G \longrightarrow \mathrm{End}(V),\ g \mapsto M(g) \quad \text{or} \quad G \curvearrowright V.$$

That is, representation theory assigns to each group element a matrix $M(g)$ acting on a vector space V – its linear shadow. The representation theory approach is that classifying linear G-actions has, in contrast to arbitrary group actions, a satisfactory answer for many groups.

The basic building blocks V_i of such actions tell us a lot about the problem we started with. (The strategy of representation theorists is summarized on the right.) In fact, experience tells us that the collection of such linear shadows is an interesting structure in its own right and maybe even more worthwhile to study than G itself.

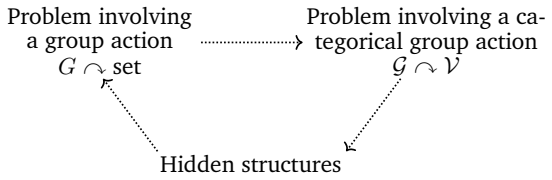


Developing over the past century (and still in development), Frobenius and Burnside's theory is pervasive across many fields of mathematics. The success of representation theory has led to numerous generalizations and applications, *e.g.* in the aforementioned molecular chemistry or quantum physics, but also in engineering such as robotics. (How do you figure out how robots move before building them? Indeed, using representation theory.)

Instead of studying groups, rings or algebras acting on vector spaces, **2-representation theory** studies the categorical actions of these. Or, more generally, actions of (2-)categories $\mathcal{G}$, such that one recovers the classical picture on the decategorified level. (Decategorification is the reverse of categorification and turns an n-category into an (n-1)-category, *e.g.* a category into a set.)

$$\begin{array}{ccc} \mathcal{G} & \xrightarrow[g\mapsto\mathcal{M}(g)]{\text{categorical action}} & \mathcal{E}\mathrm{nd}(\mathcal{V}) \\ \Big\downarrow{\scriptstyle \text{decat}} & & \Big\downarrow{\scriptstyle \text{decat}} \\ G & \xrightarrow[\text{classical action}]{g\mapsto M(g)} & \mathrm{End}(V) \end{array} \quad \text{or} \quad \begin{array}{c} \mathcal{G}\curvearrowright\mathcal{V} \\ \Big\downarrow{\scriptstyle \text{decat}} \\ G\curvearrowright V \end{array}.$$

In other words, 2-representation theory assigns to each group element a functor $\mathcal{M}(g)$ acting on a category $\mathcal{V}$ – its categorical shadow.



The categorical structure is usually richer, and the 2-representation theoretical approach can be summarized by the diagram on the left. That is, starting with a group action in the wild, 2-representation theory turns it into a question involving richer categorical structures, which then reveal hidden symmetries within the original formulation.

2-representation theory links diverse fields, as sketched in Equation 1. For my research the most important incarnations of 2-representation theory are in the green boxes in the diagram in Equation 1. Starting from the bottom and going clockwise (including the red boxes), the relevant connections are *e.g.* via [M^{3}TZ19] connecting to [EGNO15], Kazhdan–Lusztig theory [KL79], Khovanov homology [Kh00], the Riche–Williamson program [RW18], my latest work [KST22], the Mazorchuk–Miemietz approach to cell theory [MM11], Chern–Simons(–Witten) theory [Wi12].

2-representation theory – in general and, specifically, as in my research – is having a strong impact on these fields because it provides richer structures and the tools to analyze them, *e.g.*:

- ▷ Categorifications of Hecke algebras through Soergel bimodules and their 2-representations are of fundamental importance in modern Lie theory [RW18] and low-dimensional topology [Kh07]. For example, they have led to new results in the representation theory of Lie algebras [MS08].
- ▷ There are also remarkable connections between Soergel bimodules and their 2-representations with modern geometry. For example, see the groundbreaking work [Wi17].
- ▷ Pioneering ideas of Chuang–Rouquier [CR08] and Khovanov–Lauda [KL10] opened, on the one hand, a new field of research, 2-representation theory of Lie algebras. On the other hand, their ideas solved longstanding open problems, *e.g.* Broué's abelian defect group conjecture.
- ▷ It is easier to see connections to other fields. For example, while classical representation theory appears crucially in quantum or string theory via 3d Chern–Simons theory, 2-representation theory is expected to play the same role for its 4d counterpart [Wi12].

- ▷ Questions on the de- or categorified level can be proven with more structure; the proof of the Kazhdan–Lusztig conjecture [EW14] or that Khovanov homology detects the unknot [KM11] being examples. The categorical structures are also usually richer, *e.g.* Khovanov's link homology is functorial [ETWe18] (the proof relies on 2-representations).
- ▷ Several classical questions in *e.g.* modular representation theory are stated in terms of functors acting on categories, which is part of what 2-representation theory studies. For example, the Lascoux–Leclerc–Thibon conjecture was proven by using functorial action of an affine Lie algebra on categories of representations of affine Hecke algebras [Ar96].

So 2-representations play a central role in our way as we understand actions today. **One could call 2-representation theory the representation theory of the 21th century**, with expected wide-ranging applications in mathematics and beyond. So rephrasing the first sentence of this section:

> The study of 2-representations is going to be of critical importance in mathematics and related field such as physics and chemistry. Its future significance can hardly be overestimated.

However, in some sense we are at the same stage Frobenius and Burnside were 120 years ago: we have enough examples to see that our theory is rich and we have a satisfactory theory in specific cases, but we are lacking a general theory and the full range of examples to utilize the full power of 2-representation theory. The main aims of this proposal address these two obstacles in 2-representation theory: we will develop the general theory and study interesting new examples of 2-representations.

Details for running projects.

Frobenius and Burnside's theory of linear actions is at the heart of many different fields of mathematics as well as physics and chemistry. But after its introduction two major questions needed to be tackled: the abstract theory needed to be advanced, and new examples needed to be analyzed in detail. Both of these were successfully addressed by the pioneers in the field, and this theory become the shining pillar of pure mathematics, that we know it as today. Similarly, the future usefulness of 2-representations can hardly be overestimated. The framework provided by 2-representation theory is remarkable because it reveals deeper structures in the mathematics that, until now, we could only see shadows of.

Contribution to a significant problem.

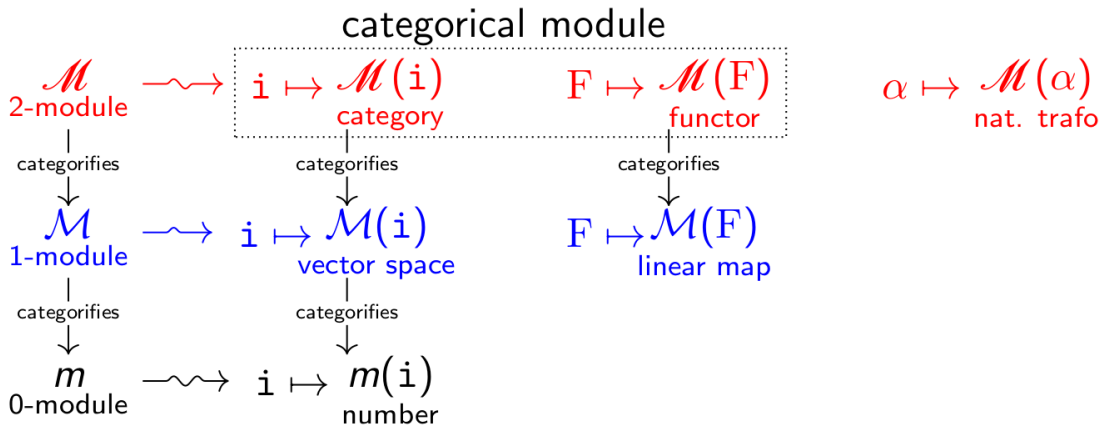
Since the field of 2-representation theory has progressed so quickly, one of the obstacles to future progress is that the foundations of it are still poorly understood, and its position within mathematics and the sciences needs to be strengthened. In other words, the two main problems in the field are to solidify the foundations by developing the abstract theory, and to add new examples together with applications.

The contribution of my research is that it addresses these open problems in 2-representation theory in a threefold way: by generalizing the abstract theory to allow infinite 2-categories and positive characteristic, by using 2-representations of braid groups in connection with link homologies outside of type A, which will clarify our understanding of these significantly, and by making connections to cryptography, which should have an long term impact on cybersecurity. So my research will hopefully play an important role in our future perspective on categorical actions and their applications.

Usually, researchers in my field categorify a specific module of an algebra to tackle some problem at hand. These works are mostly example-based and a general and satisfying theory of 2-representations is still missing. The key innovation driving my research is that, instead of studying each example in a vacuum, I aim to categorify the whole theory itself, namely the theory "representation theory of finite-dimensional algebras", providing a solid foundation to further study the well-known examples within a general theory. Advances in the abstract theory of 2-representations will have significant impact on the whole community studying such categorifications, and with it on fields beyond the abstract theory. In fact, in my research, the abstract theory and applications will advance in parallel, which is an entirely new way of attacking the problems related to my research: because of its abstract incarnation, my approach will have impacts on fields that are not normally considered within the scope of the categorification community, such as cryptography or quantum and string physics, demonstrating the uniqueness of these ideas.

My research is about 2-representation theory and its applications in categorification, low-dimensional topology, cryptography, mathematical physics and related fields. To develop the vibrant field of 2-representation theory, to strengthen its impact and to find novel applications is the objective of myself. More precisely, my research is focused on three aspects of 2-representation theory, all of which are part of the research envisioned in the present application:

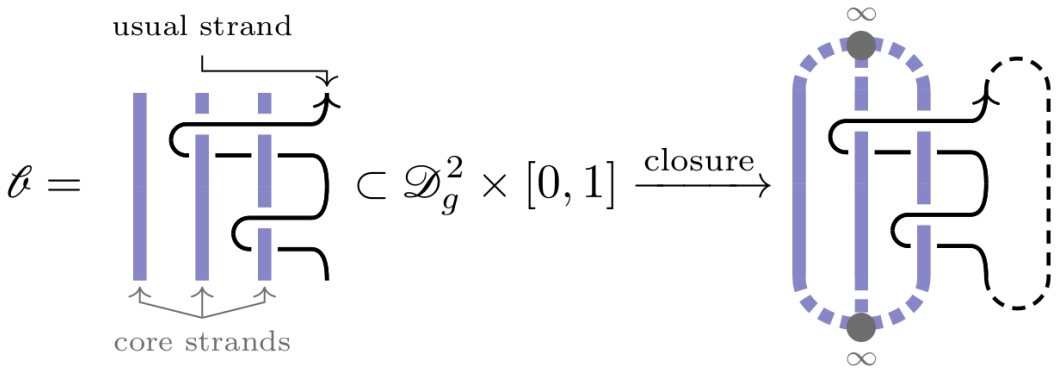
▷ *2-representation theory* ("the representation theory of the 21^{th} century"). `Ingredients.` (Modular) representation theory, categorical algebra, (higher) category theory, group and semigroup theory. `My latest results.` [M^{3}T19], [M^{3}T18], [M^{3}TZ19], [M^{3}TZ20]. `A picture from one of my papers.`



This picture illustrates the ladder fo categorification (stopping with a 2-category). A 2-representation (also called 2-module) is a functor from a 2-category to a nice target 2-category, assigning a category to each object, a functor to each arrow and a natural transformation to each 2-arrow.

▷ *Knot homologies*, topological quantum field theories, Lie theory and geometry. `Ingredients.` Low-dimensional topology, representation theory, quantum Lie theory, quantum or string physics, homological algebra. `My latest results.` [RT19], [TV21], [LT21] (honestly speaking, this paper is my students work, and part of their Ph.D. thesis). `A picture is worth a`

thousand words.



This picture from my paper [RT19] illustrates an algebraic presentation of a braid in a handlebody, and its closure. We use this presentation in [RT19] to construct an associated link homology; the main ingredient being Soergel bimodules.

▷ *Representation theory* of algebras, monoids and semigroups, especially, their diagrammatic presentations and properties such as cellularity. `Ingredients.` Monoidal categories, diagram categories, combinatorics. `My latest results.` [TW19], [TW20], [TV21], [STWZ21], [MT21], [KST22], [MT22], [LTV22]. `A picture is worth a thousand words.`

Symbol	Diagrams	Big reps?	Symbol	Diagrams	Big reps?
pPa_n		YES*	Pa_n		YES_c^*
Mo_n		YES_c	RoBr_n		YES_c^*
TL_n		YES	Br_n		YES*
pRo_n		YES*	Ro_n		YES*
pS_n		EX	S_n		NO

This picture (stolen from [KST22]) shows the various monoids that we study from the viewpoint of the sizes of their representations, and whether they are potentially suitable for cryptographical applications because they only have big representations.

(A). The analog of simple modules in 2-representation theory are *simple transitive 2-representations*, and a question of fundamental importance is to ask for a classification of these. One of the crucial new and exciting developments in the field was the observation that the classification of simple transitive 2-representations, in many cases, can be reduced to the study of fusion categories, while still being the richer structure as finitary 2-representation theory is non-semisimple, non-abelian. The first observation in this direction was made in [MT16], and this is made rigorous in [M^{3}T19] using quantum Satake and (co)algebra 1-morphisms.

In recent work, which will be available soon and which is based on [M^{3}TZ19], we solved the classification problem of simple transitive 2-representations of Soergel bimodules (non-semisimple, non-abelian) for finite Weyl groups in characteristic 0 by solving the analog classification question for certain fusion categories (semisimple). The case of characteristic p is still widely open, thus:

Problem. Study the 2-representation theory of Soergel bimodules and related 2-categories in characteristic p. Explore the connections to fusion categories with an eye on applications.

`Subprogram 1.` A main focus of this aspect is to develop machinery to study 2-representations of Soergel bimodules similarly to [M^{3}TZ19], but in characteristic p. We have precise ideas how to attack this in type A, using the technology of H-reduction [M^{3}TZ20]. The other types need work as the cell theory in finite characteristic is very different from characteristic 0. To this end, new ideas and approaches will be needed, replacing or adapting the H-reduction, and will have impact beyond the theory.

Parts will be done quickly, but some parts are hard and will take time.

`Subprogram 2.` The fusion categories arising from exceptional Coxeter groups are exotic examples of such categories – not fitting in the general philosophy that almost all fusion categories are of the form $\mathcal{V}\mathrm{ect}(G)$, $\mathcal{R}\mathrm{ep}(G)$ or $\mathcal{R}\mathrm{ep}^{ss}(U_q(\mathfrak{g}))$. Usually these exceptional examples tell a lot about the the general theory, and having more of them is desirable. A source of these potential examples is the application of the arguments from [M^{3}TZ19] and [M^{3}T18] where we expect several such examples to turn up.

This is expected to be a fruitful direction, with results in the near future.

`Subprogram 3.` In the dihedral case the fusion categories obtained from Soergel bimodules are modular, which means they give rise to 3-manifold invariants by the Witten–Reshetikhin–Turaev approach and its siblings. As they arise as the semisimple part of the bigger, non-semisimple 2-category of Soergel bimodules, we expect Soergel bimodules to give richer invariants. These will be related to invariants studied under the slogan of modified traces, *cf.* [GPMT09], and will reveal structures in topology.

For the dihedral case I expect results quickly; in general this will be hard.

(B). Homology theories are ubiquitous in modern mathematics, ranging from singular homology of topological spaces to knot homologies. These homological invariants take values in, say, isomorphism classes of vector spaces instead of in numbers as *e.g.* Betti numbers do. One main point is that these homology theories usually extend to functors and provide information about how certain structures are related. In his pioneering work, Khovanov introduced what is nowadays called Khovanov homology [Kh00] – his celebrated categorification of the Jones polynomial – which is a homological invariant of links. Studying link homologies has become a big industry after Khovanov's breakthrough, and many link homologies are known by now, coming from and connecting various fields, from mathematics to physics. The most important example of such homologies is the categorification of the HOMFLYPT polynomial [Kh07], called HOMFLYPT homology.

Almost all variants of Khovanov's invariant stay in type A, meaning for us that they are related to the classical braid group. For example, Khovanov's construction of triply-graded homology uses *Soergel bimodules of type A*. Thus, an exciting problem is:

Problem. Construct link homologies and categorical braid group actions outside of type A by using 2-representation theory.

`Subprogram 1.` A main motivation for me is to generalize these HOMFLYPT invariants to different braid groups. A first step is [RT19], defining a HOMFLYPT invariant for links in handlebodies using type A Soergel bimodules, which is functorial on handlebody braids – a fact which I can only prove using 2-representations. Considering other types of Soergel bimodules and topology, as in *e.g.* [TV21], is my aim. These homologies will turn out to be very interesting.

This is an exciting direction, and I expect to have new results appearing soon.

`Subprogram 2.` An ingredient in the construction of triply-graded homology is the Rouquier complex, *cf.* [Kh07], which categorifies the representation of braid groups on Hecke algebras. The categorification has more structure: using cell 2-representations one can show that the Rouquier complex gives a faithful braid group action, see *e.g.* [Je17], while this is still open for the algebras. 2-representations will allow me to extend these ideas to affine braid groups.

Answering these questions using 2-representations is a goal for the long-run.

(C). In current joint work with *M. Khovanov* and *M. Sitaraman* we start to develop monoidal-category-based cryptography. Monoid-based protocols often admit efficient attacks based on linear algebra [MR15], that is, on the existence of a non-trivial representation of moderate dimension. Turns out that varying the field can best be encoded using integral representations, which need to be of large dimension to resist linear attacks. To find suitable monoids we propose to look at monoidal categories since their endomorphism spaces provide examples of monoids. The biggest obstacle to overcome is that current literature on monoidal categories, *e.g.* [EGNO15], mostly studies linear categories. Such categories are not immediately useful for cryptography, and we rather look for set-theoretic counterparts of categories that appear in quantum topology, mathematical physics, and TQFTs. The most striking examples are Temperley–Lieb monoids and (variations of) Soergel bimodules. It turns out that large integral representations of the corresponding monoids are crucial to resist linear attacks, and such representation naturally appear as *shadows of 2-representations*.

Thus, we propose a new application of diagrammatic methods in cryptography. Specifically:

Problem. Apply integral and 2-representations of Temperley–Lieb-like categories and Soergel bimodules to cryptography.

`Subprogram 1.` The first step is to look at the Temperley–Lieb monoid and various diagrammatic monoids along the same lines, see *e.g.* [HJ20] for a candidate list. This has the advantage of being set-theoretical without extra works. Making the integral and 2-representations set-theoretical will be one of the crucial steps for diagram monoids to enter cybersecurity. Maybe this will be of importance in the future.

Obtaining first results will happen quickly; the general picture is a mammoth task.

`Subprogram 2.` From the numerical data I collected, Soergel bimodules seem to give very promising examples of monoids useful for cryptography. However, the literature on Soergel bimodules their 2-representations is linear, see *e.g.* [EW14], [M^{3}TZ19]. It is important to figure out how these can be interpreted set-theoretical, and this is what this aspect will focus on. This is an important questions on its own and I will delve into it.

This is a task of paramount importance, and will be attacked soon.

References

[Ar96] S. Ariki. On the decomposition numbers of the Hecke algebra of G(m,1,n). *J. Math. Kyoto Univ.* 36 (1996), 789–808.

[CR08] J. Chuang, R. Rouquier. Derived equivalences for symmetric groups and $\mathfrak{sl}_2$-categorification. *Ann. of Math.* (2) 167 (2008), no. 1, 245–298.

[ETWe18] M. Ehrig, D. Tubbenhauer, P. Wedrich. Functoriality of colored link homologies. *Proc. Lond. Math. Soc.* (3) 117 (2018), no. 5, 996–1040.

[EW14] B. Elias, G. Williamson. The Hodge theory of Soergel bimodules. *Ann. of Math.* (2) 180 (2014), 1089–1136.

[EGNO15] P. Etingof, S. Gelaki, D. Nikshych, V. Ostrik. Tensor categories. *Mathematical Surveys and Monographs*, 205. American Mathematical Society, Providence, RI, 2015. xvi+343 pp.

[GPMT09] N. Geer, B. Patureau-Mirand, V. Turaev. Modified quantum dimensions and re-normalized link invariants. *Compos. Math.* 145 (2009), no. 1, 196–212.

[HJ20] T. Halverson, T.N. Jacobson. Set-partition tableaux and representations of diagram algebras. *Algebr. Comb.* 3 (2020), no. 2, 509–538.

[Je17] L. Jensen. The 2-braid group and Garside normal form. *Math. Z.* 286 (2017), no. 1-2, 491–520.

[KL79] D. Kazhdan, G. Lusztig. Representations of Coxeter groups and Hecke algebras. *Invent. Math.* 53 (1979), no. 2, 165–184.

[Kh00] M. Khovanov. A categorification of the Jones polynomial. *Duke Math. J.* 101 (2000), 359–426.

[Kh07] M. Khovanov. Triply-graded link homology and Hochschild homology of Soergel bimodules. *Internat. J. Math.* 18 (2007), no. 8, 869–885.

[KL10] M. Khovanov, A. Lauda. A categorification of quantum sl(n). *Quantum Topol.* 1 (2010), 1–92.

[KST22] M. Khovanov, M. Sitaraman, D. Tubbenhauer. Monoidal categories, representation gap and cryptography. arXiv:2201.01805.

[KM11] P. Kronheimer, T. Mrowka. Khovanov homology is an unknot-detector. *Publ. Math. Inst. Hautes Études Sci. No.* 113 (2011), 97–208.

[LTV22] A. Lacabanne, D. Tubbenhauer, P. Vaz. Annular webs and Levi subalgebras. arXiv:2204.00947.

[LT21] G. Latifi, D. Tubbenhauer. Minimal presentations of $\mathfrak{gl}_n$-web categories. arXiv:2112.12688.

[M^{3}T19] M. Mackaay, V. Mazorchuk, V. Miemietz, D. Tubbenhauer. Simple transitive 2-representations via (co)algebra 1-morphisms. *Indiana Univ. Math. J.* 68 (2019), no. 1, 1–33.

[M^{3}T18] M. Mackaay, V. Mazorchuk, V. Miemietz, D. Tubbenhauer. Trihedral Soergel bimodules. *Fund. Math.* 248 (2020), no. 3, 219–300.

[M^{3}TZ19] M. Mackaay, V. Mazorchuk, V. Miemietz, D. Tubbenhauer, X. Zhang. Simple transitive 2-representations of Soergel bimodules for finite Coxeter types. arXiv:1906.11468.

[M^{3}TZ20] M. Mackaay, V. Mazorchuk, V. Miemietz, D. Tubbenhauer, X. Zhang. Finitary birepresentations of finitary bicategories. *Forum Math.* 33 (2021), no. 5, 1261–1320

[MT16] M. Mackaay, D. Tubbenhauer. Two-color Soergel calculus and simple transitive 2-representations. *Canad. J. Math.* 71 (2019), no. 6, 1523–1566.

[MT22] A. Mathas, D. Tubbenhauer Cellularity for weighted KLRW algebras of types B, $A^{(2)}$, $D^{(2)}$. arXiv:2201.01998.

[MT21] A. Mathas, D. Tubbenhauer Subdivision and cellularity for weighted KLRW algebras. arXiv:2111.12949.

[Ma17] V. Mazorchuk. Classification problems in 2-representation theory. *São Paulo J. Math. Sci.* 11 (2017), no. 1, 1–22.

[MM11] V. Mazorchuk, V. Miemietz. Cell 2-representations of finitary 2-categories. *Compositio Math.* 147 (2011), 1519–1545.

[MS08] V. Mazorchuk, C. Stroppel. Categorification of (induced) cell modules and the rough structure of generalised Verma modules. *Adv. Math.* 219 (2008), no. 4, 1363–1426.

[MR15] A. Myasnikov, V. Romankov. A linear decomposition attack. *Groups Complex. Cryptol.* 7 (2015), no. 1, 81–94

[RW18] S. Riche, G. Williamson. Tilting modules and the p-canonical basis. *Astérisque* 2018, 184 pp.

[RT19] D.E.V. Rose, D. Tubbenhauer. HOMFLYPT homology for links in handlebodies via type A Soergel bimodules. *Quantum Topol.* 12 (2021), no. 2, 373–410.

[STWZ21] L. Sutton, D. Tubbenhauer, P. Wedrich, J, Zhu. SL_2 tilting modules in the mixed case. arXiv:2105.07724.

[TV21] D. Tubbenhauer, P. Vaz. Handlebody diagram algebras. To appear in *Rev. Mat. Iberoam*. arXiv:2105.07049.

[TW19] D. Tubbenhauer, P. Wedrich. Quivers for SL_2 tilting modules. *Represent. Theory.* 25 (2021), 440–480.

[TW20] D. Tubbenhauer, P. Wedrich. The center of SL_2 tilting modules. *Glasg. Math. J.* 64 (2022), no. 1, 165–184.

[Wi17] G. Williamson. Schubert calculus and torsion explosion. *J. Amer. Math. Soc.* 30 (2017), 1023–1046.

[Wi12] E. Witten. Fivebranes and knots. *Quantum Topol.* 3 (2012), no. 1, 1–137.

Daniel Tubbenhauer (digital signature); April 27, 2022