The Logic in Computer Science Column

BY

Yuri Gurevich

Microsoft Research
One Microsoft Way, Redmond WA 98052, USA
gurevich@microsoft.com

Who needs category theory?

Andreas Blass
University of Michigan
ablass@umich.edu

Yuri Gurevich
Microsoft Research
gurevich@microsoft.com

Abstract

In computer science, category theory remains a contentious issue, with enthusiastic fans and a skeptical majority. Categories were introduced by Samuel Eilenberg and Saunders Mac Lane as an auxiliary notion in their general theory of natural equivalences. Here we argue that something like categories is needed on a more basic level. As you work with operations on structures, it may be necessary to coherently manipulate isomorphism (or more generally homomorphism) witnesses for various properties of these operations, e.g. associativity, commutativity and distributivity. A working mathematician, to use Mac Lane's term, is well advised to be aware of the coherent witness-manipulation problem and to know that category theory is an appropriate framework to address the problem. Of course, the working mathematician in question may be a computer scientist or physicist.

In computer science, category theory remains a contentious issue. The fans tend to be enthusiastic while the majority remains skeptical. The joke

> I hope most mathematicians continue to fear and despise category theory, so I can continue to maintain a certain advantage over them.

of John Baez [1] works even better in computer science.

In a muted form this split applies to the authors of this note. As we mentioned in [2, §1], "The first author of this paper has long been a fan of category theory; even as a graduate student, he was described by one of his professors as 'functorized'. The second author has been far more skeptical about the value of category theory in computer science, because of its distance from applications and because of the peril of potential (and in some cases actual) over-abstraction."

Quisani[1]**:** You don't mean that category theory itself is an over-abstraction.

Authors[2]**:** No, we don't. As Seneca the Younger said in the first century, "gladius neminem occidit: occidentis telum est," that is "a sword kills nobody; it is a tool of the killer."

There is also the hammer-and-nail phenomenon: "For a person with a hammer, everything looks like a nail." Here is a true life example, but allow us to omit the reference. A computation can be seen as a category where objects are states and morphisms are state transitions. If you take this point of view, then you might want computation transformers to be functorial, which narrows unreasonably your library of computation transformers. For example, you lose compilers.

Q: Why isn't a compiler functorial?

A: Typically, the target language is at a lower abstraction level and uses different data structures. A higher-level step may have no meaning at the lower level, but such steps may combine into a transformation that is meaningful at the lower level. Besides, think of compiler optimization.

It turns out, however, that the only mathematically sound theory of topological quantum computing in the literature is based on category theory; see [10, 11] for example. Why? Is this an accident of history, another nail for the categorical hammer, or there is more to it?

We have been debating this question for a while, and now we agree that something like category theory is necessary for the purpose. The goal of this note is to give a high-level explanation of that necessity, which avoids details and which suggests that the case of topological quantum computing is far from unique.

Consider a collection C of structures together with operations of addition and multiplication defined on C. Up to isomorphism, both operations are commutative, associative and have their respective neutral elements, and multiplication distributes over addition.

`Example 1.` A C structure is a finite-dimensional vector space, over the field of complex numbers, furnished with a fixed basis. If $A, B \in C$ then the vector space $A + B$ is the direct sum, also known as the direct product, of vector spaces A and B, and the fixed basis of $A + B$ is the disjoint union of the fixed bases of A and B. The product $A * B$ is the tensor product of the vector spaces furnished with the cartesian product of the fixed bases of A and B. ◁

[1] A former student of the second author and our frequent interlocutor.

[2] Speaking one at a time

In the case of topological quantum computing, the structures are more sophisticated — involving e.g. tuples of vector spaces, duality, ribbon structures — but this is not important for the purposes of this note. A more relevant peculiarity of topological quantum computing is that the standard isomorphisms from $A * B$ to $B * A$ and from $B * A$ to $A * B$ are not necessarily inverse to each other. It is convenient to think about this topologically: as $A * B$ is transformed into $B * A$, it matters whether A passes in front of or behind B. The two isomorphisms, known as braiding isomorphisms, are in general different.

So far, we are within the realm of universal algebra. But here is a new aspect. For computational purposes, it is not enough for us to know that there are two braiding isomorphisms from $A * B$ to $B * A$ or that there is an associativity isomorphism from $(A * B) * C$ to $A * (B * C)$. We need these isomorphisms, in matrix form with respect to the fixed bases, for computational purposes. These isomorphisms satisfy the appropriate coherence laws identified by Saunders Mac Lane [9].

It is convenient to think of an isomorphism $\xi : A \to B$ as a *witness* that A, B are isomorphic. Multiplication interacts with addition via the distributivity laws. As a result, the necessity of dealing with computationally suitable witnesses for the commutativity and associativity laws of multiplication forces us to also deal with such witnesses for the commutativity and associativity laws of addition and for the distributivity laws. The witnesses for the commutativity and associativity of addition satisfy Mac Lane's coherence laws. The coherence laws for distributivity[3] have been identified by Miguel Laplaza [6, 7] who was a postdoc of Mac Lane.

It would be wonderful if the addition operation on C were literally commutative and associative, i.e., if we could get by with the identity witnesses for the commutativity and associativity of addition. Unfortunately this is not in the cards.

We could use Example 1 for illustration, but let us simplify the situation by abstracting from vector spaces and concentrating on their fixed bases: finite sets with disjoint union as addition. We recall the standard definition of disjoint union of sets.

Definition 1. The disjoint union of sets A, B is the set

$$A + B = \{(a, 0) : a \in A\} \cup \{(b, 1) : b \in B\}. \qquad \triangleleft$$

This disjoint union is neither commutative nor associative. One may think that there is no definition that is better in the sense that it makes disjoint union literally, not just up to isomorphism, commutative and associative. But such a "better" definition does exist. Let $\mathbb{N}$ be the set of natural numbers, i.e., nonnegative integers.

[3] Unfortunately for us, Laplaza considered only the symmetric case, where the two braiding isomorphisms from $A * B$ to $B * A$ always coincide.

Definition 2. The disjoint union of finite sets A, B is the set

$$A\dotplus B = \{n \in \mathbb{N} : n < |A| + |B|\}. \qquad \triangleleft$$

Let's adopt the set-theoretic convention that a natural number is the set of smaller natural numbers. Then Definition 2 says that the disjoint union $A\dotplus B$ is the number $|A| + |B|$. It is easy to see that $A\dotplus B$ is indeed commutative and associative, so that the standard witnesses for the commutativity and associativity can be taken to be identities.

Q: Hmm, Definition 1 does not look standard to me. If fact, it looks rather arbitrary. Instead of 0 and 1, I can use different tags, say, 1 and 2.

A: In any of these variations, there is a natural enhancement of the definition with canonical embeddings of A and B into $A + B$; the resulting operation has the universal property of the coproduct. That is what makes the definition, in any of these variations, standard.

Q: Definition 2 does not have this property.

A: No, it does not. It is really the up-to-isomorphism definition, except that the isomorphism class of the disjoint union is replaced with its canonical representative.

Q: Still, the operation $A\dotplus B$ has the advantage of being commutative and associative so that, as you said, the standard witnesses for commutativity and associativity can be taken to be identities.

A: This is true, but this advantage cannot be pushed too far. For example, if a finite set A is not a number then the equality $A = A\dotplus\emptyset$ cannot be witnessed by the identity. For, if A is identical to $A\dotplus\emptyset$, then A is a number.

Categories were introduced by Samuel Eilenberg and Saunders Mac Lane as an auxiliary notion in their general theory of natural equivalences [4]. "It is not too misleading, at least historically, to say that categories are what one must define in order to define functors, and that functors are what one must define in order to define natural transformations," writes Peter Freyd in the introduction to his book [5].

Here we argue that something like categories is needed on a more basic level. As you work with operations on structures, it may be necessary to coherently manipulate witnesses for various properties of these operations. We mentioned associativity, commutativity and distributivity, but many additional properties are in play in topological quantum computing and elsewhere. The coherent witness-manipulation problem may be hard.

This necessity of coherent witness-manipulation cannot be proven mathematically, and in some cases one can get around the coherent witness-manipulation problem. For example, for limited purposes, the narrow problem of a reasonable definition of commutative and associative disjoint union of sets can be solved by generalizing sets to multisets. Unfortunately this solution is of little help if the sets in question are vector-space bases.

In general, a working mathematician, to use Mac Lane's term [9], is well advised to be aware of the coherent witness-manipulation problem and to know that category theory is an appropriate framework to address the problem. Of course, the working mathematician in question may be a computer scientist or physicist.

> **Q:** You say that "something like category theory" is needed. Are there alternatives to category theory?
>
> **A:** We didn't want to rule out possible alternatives. In some situations, it suffices to consider groupoids, i.e., to restrict attention to isomorphisms. This setting can be presented in a way closer to traditional algebra [3].
>
> **Q:** Is there an objective need to deal with more general homomorphisms?
>
> **A:** Yes, isomorphisms are sometimes insufficient. Consider, for example, Definition 2 of disjoint union. Why does it feel so lousy? One reason is that it does not say where *A* and *B* are in the disjoint union. To have a useful disjoint union, one needs even more, namely where individual elements of *A* and *B* lie in the disjoint union. That information amounts to embeddings of *A* and *B* into the disjoint union, and those are not isomorphisms.

Acknowledgement

This note was written, rather quickly, when it became clear that the author who was scheduled to write an article for the present issue of this column may not be ready. We thank Samson Abramsky, John Baez, Bob Coecke and Prakash Panangaden for giving us their comments on short notice.

References

[1] John Baez, in *Opinions of Category Theory*, `https://www.arsmathematica.net/2006/06/24/opinions-of-category-theory/`, June 29, 2006.

[2] Andreas Blass and Yuri Gurevich, "On quantum computation, anyons, and categories," in *Martin Davis on Computability, Computational Logic, and Mathematical Foundations*, 209–241, Springer 2016.

[3] Andreas Blass and Yuri Gurevich, "Witness algebra and anyon braiding," a manuscript in preparation.

[4] Samuel Eilenberg and Saunders Maclane, "General theory of natural equivalences," Trans. Amer. Math. Society 58:2 (1945), 231–294.

[5] Peter J. Freyd, "Abelian categories," in *Reprints in Theory and Applications of Categories*, No. 3 (2003), `http://www.tac.mta.ca/tac/reprints/`, originally published by Harper and Raw in 1964.

[6] Miguel Laplaza, "Coherence for categories with associativity, commutativity and distributivity," Bull. Amer. Math. Soc. 78 (1972), 220–222.

[7] Miguel Laplaza, "Coherence for distributivity," in *Coherence in Categories*, Springer Lecture Notes in Mathematics 281 (1972), 29–65.

[8] Saunders Mac Lane, "Coherence and canonical maps," Symposia Mathematica, IV (1970), 231–241.

[9] Saunders Mac Lane, "Categories for working mathematician," Springer 1971.

[10] Prakash Panangaden and Éric O. Paquette, "A categorical presentation of quantum computation with anyons," Chapter 15 in *New Structures for Physics,* ed. Bob Coecke, Springer Lecture Notes in Physics 813 (2011), 983–1025.

[11] Zhenghan Wang, *Topological Quantum Computation,* CBMS Regional Conference Series in Mathematics, vol. 112, American Mathematical Society (2010).