Quantum Physics, Topology, Formal Languages, Computation: A Categorical View as Homage to David Hilbert

Chiara Marletto and Mario Rasetti
Oxford University
Politecnico di Torino

The deep structural properties of a quantum information theoretic approach to formal languages and universal computation (the unifying tool being the Quantum Spin Network Automaton scheme of computation), as well as those of the topology problem of defining the presentation of the Mapping Class Group of a smooth, compact manifold are shown to be grounded in the common categorical features of the two problems.

1. Hilbert and Physics

The role and presence of David Hilbert in Physics are most probably as relevant as they are in Mathematics. His fundamental contributions to functional analysis, in particular the introduction of the notion of infinite-dimensional space (now universally referred to as Hilbert space) became crucial in quantum mechanics as well as in several areas of classical physics; and his discovery of the action of the field equations, in parallel to and independently from Einstein's, had a tremendous impact in general relativity (Hilbert 1924). However, only recently, with the development of Quantum Information, Hilbert's ideas—in fact, his philosophical views—enter at a very fundamental level, and let his profound nature of a true, dedicated, superb man of science most strongly emerge («*Wir müssen wissen, wir werden wissen*»), standing on two of his famous 23 problems for the XX-th Century.

Hilbert's interest in problems bearing on the foundation of classical mathematics (Hilbert 1900), essentially bracketed between two Interna-

Perspectives on Science 2014, vol. 22, no. 1

doi:10.1162/POSC_a_00120

tional Congresses of Mathematicians, the first in Paris in 1900, the second in Bologna in 1928, has now come to be known as Hilbert's Program. The program calls for a formalization of all of mathematics in axiomatic form, together with a proof that this axiomatisation of mathematics is consistent (Gray and Rowe 2000). Three of the questions posed there are: 1) is mathematics complete? 2) is mathematics consistent? 3) is mathematics decidable? (the *Entscheidungsproblem,* the "decision problem"). Such problems bear on some of the most spectacular progress in mathematics of the past century, for example they have to do with Gödel's second incompleteness theorem. But, also, *quantum information* has cast a new light on these fundamental questions, entering in this intriguing scenario with a novel perspective whose reach and significance have mostly to do with algorithmic complexity and decidability.

In the spirit of this far-reaching, unifying program, this note aims to show that category theory allows one to unveil an unexpected and deep connection between a number of fundamental problems belonging to apparently distant scientific fields. Specifically, by resorting to the language of category theory, one can envisage a surprising equivalence (to wit, a formal identity) between: i) the presentation of the group of diffeomorphisms in the topology of manifolds; ii) the composition of angular momenta in quantum mechanics; iii) Lambda calculus and Pi calculus in the theory of computation and of programming within symbolic manipulation schemes and iv) the proof theory in linear logic. As an illustrative case, here we shall confine attention to the equivalence between the first two problems, leaving the most general case for a future paper.

2. Topology of Manifolds

We enter now the realm of topology. The latter deals with equivalence classes of geometrical objects which are globally invariant under biunivocal, bicontinuous mutual transformations. The main objects of topology are manifolds, i.e., spaces every point of which has a neighbourhood homeomorphic to a Euclidean space. The most general property of 3-manifolds (Thurston 1997) is *prime decomposition:* every compact orientable 3-manifold M decomposes uniquely as a connected sum $M = P_1 \# \cdots \# P_n$ of 3-manifolds P_i, which are referred to as *Prime Manifolds* because they can be decomposed as connected sums only in the trivial way $P_i = P_i \# S^{(3)}$.

The fundamental tool for classifying manifolds is to study their set of *invariants.* In standard topology invariants used to be *created* to distinguish between manifolds according to properties *which could be detected via a geometrical representation;* and the invariant definition would in this case make clear what property the invariant is associated with. For example, the genus g of a smooth, closed, oriented surface S (i.e., the number of handles of S, which fully determines topological type of S) is obtained from the topological invariant known as Euler number χ

$$\chi(S) = 2 - 2g,$$

and the latter can be easily evaluated by Euler's formula $\chi(S) = V + F - E$ upon tessellation of S; with V = #Vertices; F = #Faces; E = #Edges.

New invariants of three-manifolds (hence of knots) were instead 'discovered', whose definition is based on topological quantum field theory 'technology'. These invariants provide information about *purely topological* properties we would be unable to detect, nor even to hint, via the mere geometric representation.

Of particular interest in this context is the set of questions bearing on the topology of surfaces and in particular the **mapping-class-group** presentation problem (Birman, Hilden 1971).

For S a Riemann surface of genus $g \leq 2$, the mapping class group MCG(S) is a discrete group of symmetries of S interpreted as the group of isotopy-classes of the automorphisms of S. Specifically, for M a (smooth) topological manifold, the mapping class group is the group of isotopy-classes of the diffeomorphisms of M:

$$\mathsf{MCG}(M) \equiv \mathrm{Diff}(M)/\mathrm{Diff}_0(M),$$

where Diff(M) is the group of diffeomorphisms of M, whereas $\mathrm{Diff}_0(M)$ is the group of diffeomorphisms of M homotopic to the identity by a homotopy that takes the boundary into itself.

MCG(M) is generated by *Dehn's twists* (Dehn 1938), defined as follows. Consider Γ a simple closed curve in S. A tubular neighborhood A of Γ is an annulus. The Dehn twist τ is the map from S to itself which is the identity outside A and inside A is a full (2π) rotation of the boundaries of A (topologically equivalent to circles) one with respect to the other. Theorems by Dehn, Lickorish and Humpries state that the minimal number of curves necessary to generate MCG(S) is $2g + 1$ for $g > 1$. Typically curves Γ_j, $j = 1, \ldots, 2g + 1$, are chosen to be elements of the homology basis, i.e., representative cycles of the homology, of S.

In general the problem of finding the presentation of MCG(S) requires the introduction of the appropriate combinatorial structure, which resides in the Hatcher-Thurston complex.

3. The Hatcher-Thurston Complex

Consider a set of pairwise disjoint non-separating simple closed curves on S, C_1, C_2, . . . , C_g, such that the surface obtained from S by cutting it along all C_i, $1 = 1, \ldots, g$ is connected (i.e., it is a sphere with $2g$ boundary components). The set of representatives of their equivalence class, $\{c_1, c_2, \ldots, c_g\}$ is called a '*cut system*' and it is customarily denoted by $\langle c_1, c_2, \ldots, c_g \rangle$.

Let v and w be two cut systems. Suppose that there are $c \in \mathsf{v}$ and $d \in \mathsf{w}$ such that the number of mutual intersections $i(c,d) = 1$, and $\mathsf{v} - \{c\} = \mathsf{w} - \{d\}$. In this case, we say that w is obtained from v by an *elementary move* and we write $\mathsf{v} \Leftrightarrow \mathsf{w}$.

If $\langle c_1, c_2, \ldots, c_i, \ldots, c_g \rangle \langle c_1, c_2, \ldots, c_i', \ldots, c_g \rangle$ is an elementary move, we write simply $\langle c_i \rangle \Leftrightarrow \langle c_i' \rangle$.

The graph $\mathsf{HT}_g(S)$, whose vertex set consists of all the cut systems on S and whose (unordered) edge set consists of all pairs of vertices $\{\mathsf{v}, \mathsf{w}\}$ such that $\mathsf{v} \Leftrightarrow \mathsf{w}$, is the 1-skeleton of the *Hatcher-Thurston complex* $\mathsf{HT}(S)$ (Hatcher, Thurston 1980).

Triangles. If three vertices have $g - 1$ common elements and if the remaining classes c, c', c'' satisfy $\mathrm{i}(c,c') = \mathrm{i}(c, c'') = \mathrm{i}(c',c'') = 1$, then there is a triangle relation, which writes

$$\langle c \rangle \Leftrightarrow \langle c' \rangle \Leftrightarrow \langle c'' \rangle \Leftrightarrow \langle c \rangle.$$

Rectangles. If four vertices have $g - 2$ common elements and if the remaining classes c_1, c_2, d_1, d_2 are such that $\mathrm{i}(c_1, c_2) = \mathrm{i}(d_1, d_2) = 1$, $\mathrm{i}(c_i, d_j) = 0$, $i, j = 1{,}2$, then there is a rectangle relation,

$$\langle c_1, d_1 \rangle \Leftrightarrow \langle c_1, d_2 \rangle \Leftrightarrow \langle c_2, d_2 \rangle \Leftrightarrow \langle c_2, d_1 \rangle \Leftrightarrow \langle c_1, d_1 \rangle.$$

Pentagons. If five vertices have $g - 3$ common elements and if the remaining classes c_1, c_2, c_3, c_4, c_5 have representatives intersecting each other in the following way: $\mathrm{i}(c_1, c_2) = \mathrm{i}(c_2, c_3,) = \mathrm{i}(c_3, c_4) = \mathrm{i}(c_4, c_5) = \mathrm{i}(c_5, c_1) = 1$, whereas all other pairs c_i, c_j not listed have $\mathrm{i}(c_i, c_j) \equiv \mathrm{i}(c_j, c_i) = 0$, then there is a pentagon relation,

$$\langle c_1, c_4 \rangle \Leftrightarrow \langle c_2, c_4 \rangle \Leftrightarrow \langle c_2, c_5 \rangle \Leftrightarrow \langle c_3, c_5 \rangle \Leftrightarrow \langle c_1, c_3 \rangle \Leftrightarrow \langle c_1, c_4 \rangle.$$

The Hatcher-Thurston complex $\mathsf{HT}(S)$ is a two-dimensional CW-complex (i.e., a simplicial complex made of a set of basic building blocks [cells] topologically glued together) obtained from $\mathsf{HT}_g(S)$ by attaching a 2-cell along each triangle, rectangle and pentagon. Hatcher and Thurston used this complex to get a presentation for the mapping class group for closed orientable surfaces, proving that HT(S) is connected and simply connected.

This construction has to be kept in mind as we move to *knots,* which play a crucial role in the discussion of topological invariants, because they bear on the whole structure of manifold invariants and can be constructed by a standard "cup/cap" method out of braids.

4. Knots

Knots are equivalence classes with respect to isotopies (Birman 1974). Central problem of knot theory is the classification of knots, i.e., given two knots deciding whether or not they are topologically equivalent. Classification is made in terms of invariants, in the form of polynomials whose coefficients encode the topological properties of a class of knots (Alexander polynomial (Alexander 1928), Jones polynomial (Jones 1985), etc.). The construction is often non-trivial. For example the Alexander polynomial (in the running variable $t \in \mathsf{R}$) is constructed in the following way.

Given the knot projection over a plane, number the self-intersection over-crossings following the knot along a selected orientation from an arbitrary start point P. Let X_k, with $k = 1, \ldots, n$, denote the arc between overcrossings $k - 1$ and k (mod n). Underpass at k can be of: *type* I, if at k under-pass connecting X_k to X_{k+1} it is crossed by over-passing X_i from right to left; *type* II, if at k under-pass connecting X_k to X_{k+1} it is crossed by over-passing X_i from left to right.

The Alexander matrix $\boldsymbol{A}$, of elements a_{ki} is then constructed as follows. The k-th row of $\boldsymbol{A}$ corresponds to the k-th underpass. Except for a_{kk}, a_{kk+1}, a_{ki}, $i \neq k, k + 1$, all elements of the k-th row of $\boldsymbol{A}$ are zero, with the prescribed exceptions: i) for $i = k$ or $i = k + 1$, $a_{kk} = -1$; $a_{kk+1} = 1$, ii) for $i \neq k, k + 1$, $a_{kk} = 1$, $a_{kk+1} = -t$, $a_{ki} = t - 1$, for type-I underpass; $a_{kk} = -t$, $a_{kk+1} = 1$, $a_{ki} = t - 1$, for type-II underpass.

The Alexander Polynomial $\Delta(t)$ is derived from $\boldsymbol{A}$ calculating any minor of order $n = 1$ and multiplying it by the power $-m$ ($m \in \mathsf{N}$) of $\pm t$ in such a way that the polynomial in t thus obtained has no negative powers and has positive constant term. For example, the 'trefoil' knot has $\Delta(t) = 1 - t + t^2$.

The construction of the Jones Polynomial is still combinatorial, but it is based on a set of subtle properties of topological quantum field theory rather than on the simple algebraic features of the knot incidence matrix.

For the trefoil knot the Jones polynomial in the running variable $q \in \mathbf{C}$ is $J(q) = q^{-1} + q^{-2} - q^{-4}$.

It is crucial here that as far as Algorithmic Complexity is concerned, while evaluation of the Alexander polynomial is P (a lower cost, because this polynomial does not provide a complete classification of knots, for example it is unable to distinguish *amphicheiral* knots), evaluation of the Jones polynomial—which provides a more complete classification—is a $\#P$-hard problem from the computational point of view (Jaeger, Vertigen, Welsh 1990): there exist no efficient classical algorithms for its evaluation. However, the Jones polynomial is efficiently evaluated (i.e., in poly-time and in the additive approximation) by the spin network quantum automaton, discussed in the next section.

5. Physics and Information Manipulation: The Spin Network Quantum Automaton

A discretized, idealized version of physics, quantum mechanics and topological quantum field theory support each a different Turing-machine computational model (or equivalent: circuits, automata, etc.), whose repertoire is determined (and limited) only by the physical theory itself. This bears on hard undecidability questions, such as the Davis-Matijasevich-Putnam-Robinson result on Hilbert's tenth problem about the solution of certain Diophantine equations, or the Boone-Novikov theorem about the insolvability of the word problem for finitely presented groups. Indeed, Quantum Information Theory can efficiently approach these hard topological or geometric problems reducing their computation to polynomial (both space and time) complexity.

A particularly promising scheme is topological quantum computation, which is designed to comply with the behaviour of partition and correlation functions of a non-abelian topological quantum field theory, with gauge group $G = SU(2)$. The action of the theory is the non-linear Chern-Simons-Witten (CSW) action (Witten 1989), (Kohno 1992), characterized by a coupling constant κ, referred to as the level of the theory. The key point here is that, due to their invariance under gauge and diffeomorphism transformations, which freeze out local degrees of freedom, partition and correlation functions of such theory share a global, 'topological' character. It was a seminal result of Witten the discovery that they encode topological information.

We shall focus on a specific topological quantum computational model, the "Spin Network Quantum Automaton" (SNQA) which stems from a discrete, finite version of the non-Abelian topological quantum field theory characterized by the CSW action. The SNQA is capable of solving in the additive approximation a number of $\#P$ problems in topology and formal language theory in polynomial time (Rasetti, Marletto 2009) [a quantum machine of dimension $O(\text{poly}(n))$ is said to operate in the "additive approximation" if the algorithm performed by the unitary U over an n qubit pure state $|\psi\rangle$ which can be prepared in $O(\text{poly}(n))$ time is such that it is possible to construct a statistical ensemble in which, sampling for a $O(\text{poly}(n))$ time two random variables, say X and Y, one finds $E[X + iY] = \langle \psi | U | \psi \rangle$].

The SNQA belongs to the class of quantum automata (Moore, Crutchfield 2000), defined as a 5-tuples $\{H;L;U;|s\rangle_i;|s\rangle_{acc}\}$, where H is a (finite dimensional) Hilbert space, L the language used to provide inputs to the automaton and U a set of transition rules which describe the evolution of the automaton. $|s\rangle_i$ is the initial state of the automaton and $|s\rangle_{acc}$ its final (accepted) state. This model can be thought of as a Turing machine whose tape is constrained to move only in one direction. The states of the automaton coincide with the internal states of the machine, and L is generated by the alphabet A used to write the symbols on the tape. The transition rules are a set of unitary operators, one for each 'letter' of A, to be applied whenever the automaton reads on the tape the corresponding symbol. In the ensuing context the transition rules are but unitary representations of words, namely finite sequences of symbols, in the alphabet. A word is accepted by the automaton with probability p, if p is the quantum probability, i.e., the square absolute value for the evolution amplitude from the initial to the final state represented by that particular word according to the unitary representation adopted.

In order to explain the SNQA construction in some detail, we shall first describe the Spin-Network Quantum Simulator (SNQS) (Marzuoli, Rasetti 2002), (Marzuoli, Rasetti 2005), a computational model that exploits the tensor algebra associated with the (binary) coupling and recoupling theory of $SU(2)$ quantum angular momenta. The SNQA generalises the latter from simulator to automaton, to embrace the tensor (co-)algebra (Bergen, Catoiu, Chin 2004) associated with the *quantum group* (Majid 1995), (Kassel 1995) $SU_q(2)$. Consider n (quantum) angular momenta with given, fixed sum $\boldsymbol{J}$. Each computational block of the spin-network represents a particular way of combining pairwise irrep subspaces of the Hilbert space associated with the given $\boldsymbol{J}$. The Hilbert spaces thus generated, each $(2J + 1)$-dimensional ($J(J + 1)$ being the eigenvalue of $\boldsymbol{J}^2$), are the simultaneous eigenspace of the squares of $2(n + 1)$ Hermitean, mutually commuting angular momentum operators with fixed sum, of the intermediate angular momentum operators and of the operator J_z (the projection of the total angular momentum $\boldsymbol{J}$ along the quantization axis). For any given pair $(n; J)$, allowed binary coupling schemes involve all the $n + 1$ angular momentum quantum numbers $\{j_1, \ldots, j_{n+1}$ and also the quantum numbers $\{k_1, \ldots, k_{n-1}$ (corresponding to the $n - 1$ intermediate angular momenta). Hilbert spaces corresponding to different coupling schemes, although isomorphic, are not identical since they actually correspond to (partially) different complete sets of physical observables. This happens because the tensor product is not an associative operation. The j_s quantum numbers can be integers or half-odd rationals, while the range of the k_r is constrained by Clebsch-Gordan decompositions; they provide the alphabet in which quantum information is encoded (the rules and constraints of the coupling schemes are instead part of the 'syntax' of the resulting coding language). The finite-dimensional Hilbert space in which computations are performed is the graph G_n with a finite number of vertices, corresponding to the computational blocks, and a set of edges corresponding to the allowed 'elementary' unitary evolutions (*gates*) connecting different blocks.

The gates can be realized in a combinatorial way by noticing that each computational block is actually a binary tree, whose leaves are labeled by the irreps of the incoming spins, while the root is labeled by the quantum number J of $\mathbf{J}$. Any operation/transformation one can perform on such tree can be reduced to the application of a set of elementary moves which are of one of only two possible types: the twist operation, that simply swaps two nearest Hilbert subspaces in the tensor product of characterizing the total Hilbert space, and the rotation operation, which changes the binary coupling structure of the concurrent Hilbert spaces in minimal way. The twist amounts to modifying the computational states by a phase factor, whereas the rotation is related to the unitary transformation implemented by an $SU(2)$ $6j$-symbol (or $6j_q$). More specifically, the unitary transformations associated with recoupling coefficients ($3nj$ symbols) of $SU(2)$ can be split into elementary j-gates, namely Racah and phase transforms. A Racah transform is defined formally as $R{:}|\ldots((ab)_d c)_f \ldots ; JM\rangle \mapsto |\ldots(a(bc)_e)_f \ldots ; JM\rangle$; where $a, b, c, \ldots$ denote generic, both incoming (j_s's) and intermediate (k_r's) spin quantum numbers, and the brackets (ab) denote the coupling between a and b. A phase transform amounts instead to introducing a phase factor whenever two angular momentum labels are swapped $P{:}|\ldots(ab)_c \ldots ; JM\rangle \mapsto (-)^{a+b-c}|\ldots(ba)_c \ldots ; JM\rangle$.

The initial state of the automaton is a particular vector lying in the selected computational graph of the spin-network. The transition rules of the automaton—that describe the unitary processing of a word—can be easily recast into sequences of elementary unitary gates. A projective measurement on the final state of the automaton will provide the probability of acceptance for the input word. Thus, on the spin-network graph a particular computation can be seen as a path (i.e., a sequence of edges) starting from the vertex corresponding to the initial state and ending into the vertex corresponding to the final state. The crucial feature of G_n arises from compatibility conditions satisfied by the *6j*-symbols: the Racah and the Biedenharn-Elliott identities, and the orthogonality conditions (Biedenharn, Louck 1981). The latter ensure that any simple path in G_n with fixed endpoints can be freely deformed into any other, providing identical quantum transition amplitudes at the kinematical level. In this model, a program is a collection of single-step transition rules, namely a family of elementary unitary operations. Such prescriptions amount to selecting a family of directed paths in the fiber space structure, all starting from the same input state and ending in an admissible output state. A single path in this family is associated with a particular algorithm supported by the program. Those programs, which employ only gates that do not imply any transport along the fibre share their structural features with discretized topological quantum field theories. The combinatorial structure becomes here prominent owing to the existence of a one-to-one correspondence between allowed elementary operations (Racah and phase tranforms) and the edge set of G_n. When working in such purely discrete modes, the spin network complies with all Feynman's requirements for a universal simulator.

The SNQA (Marzuoli, Rasetti 2006), (Garnerone, Marzuoli, Rasetti 2006) is obtained from the SNQS, switching to the tensor (co-)algebra associated with the *quantum group* $SU_q(2)$, necessary as gauge group in the associated topological quantum field theory. The fibered-graph structure which characterizes the computational space of the SNQA exhibits the same combinatorial properties as the one related to the SNQS, because the combinatorial features of the *6j* coefficients and the ones of their deformed counterpart, $6j_q$, are the same. In addition, it profits of the topological insight provided by the deformation of the gauge group. Its computational features derive from the rules of quantum angular-momentum addition, enriched by the braiding structure induced by the deformation of the gauge group. It is crucial to notice that switching to the $SU_q(2)$ representation theory induces two important properties. On the one hand, due to the breaking of symmetry between Hilbert spaces induced by the coproduct (a deeply quantum feature, that has no counterpart at the classical level nor in the $SU(2)$ case), the basic element of the graph—the single three-valent elementary vertex—is turned into a topological object, a sphere with three holes referred to as pants, and the generation of the full graph by gluing basic elements becomes a sequence of cobordism operations. On the other hand, within the *q*-deformed counterpart of the *6j*-symbol coming into play, the twist has a natural (unitary) generalization which accounts for the two basic operations associated with over/

under crossings of braids and link diagrams. Hence, in the SNQA the state transformations consist of cobordism and pant decomposition, instead of reducing to mere addition of quantum angular momenta (Garnerone, Marzuoli, and Rasetti 2007; Garnerone, Marzuoli, and Rasetti 2009) and sum of the corresponding complex amplitudes (similar to Feynman path sum) typical of the SNQS. In view of these topological features, the SNQA recognizes the language of the braid group.

Notice that the structure above rests on the characteristic properties of the building blocks of the theory: the *6j* symbols. In particular, it is the Biedenharn-Elliott identity, proper just to the *6j* symbols (both conventional and 'quantum'), that leads to Pentagon relations among the symbols themselves. The Racah identity instead generates Triangle relations, while the Orthonormality Condition (Catalan trees with pairs of labels identified) gives rise to Rectangle relations. This is what will allow us to understand, in the next, conclusive section, that the global structure of the SNQA—like that of the Mapping Class Group presentation, which is obviousy related, through Dehn's twists and cobordism, to the spin network qwholeuantum automaton—is determined by a Closed Symmetric Braided Monoidal Category.

6. Categories

In this final section we want to show that the two sets of problems discussed previously are different—in representation, not in structure—realizations of the same scheme: a *Closed Symmetric Braided Monoidal Category.* We proceed now to doing so, recalling first very concisely the necessary prerequisite notions of category theory (Mac Lane 1998), (Eilenberg, Kelly 1966), (Eilenberg, Mac Lane 1945).

A category consists of two classes, one whose elements are 'objects', the other whose elements are 'arrows' (*morphisms*) between objects. The arrows are composable: if $f{:}A \rightarrow B$ and $g{:}B \rightarrow C$, there is a composite arrow $g \cdot f{:}a \rightarrow C$. The composition has two properties: 1. *Associativity:* for all $f{:}A \rightarrow B$, $g{:}B \rightarrow C$, $h{:}C \rightarrow D$, $(h \cdot g) \cdot f = h \cdot (g \cdot f)$; 2. *Identity.* For all objects A in the category there is an 'identity' arrow ι_A such that for all $f{:}A \rightarrow B$, $f \cdot \iota_A = f = \iota_B f$.

Hence, a category can also be thought of as a directed graph G whose vertices are all mathematical structures of the same kind (e.g., vector spaces, sets, topological spaces) and whose edges correspond to morphisms between such structures. Its toolkit of composition rules is defined in such a way that, for any two directed bonds in G (arrows) that form a path of (chemical) length two from A to C via B, there is an arrow closing the triangle ABC. In analogy with how one defines morphisms between structures in the same category, one defines functors: a functor is a map between categories which sends objects and morphisms of a category to objects and morphisms of another preserving the composition rules.

Category theory is the ultimate abstraction of the (arrow) relation occurring diffusely in set theory, algebra, topology and logic, $f{:}a \to b$, were a and b are the entities we attributed to the vertices of G, and f is an arrow whose source is object a and target is object b. A straightforward example is: a and b are sets, and f may then denote a total function from a to b, or may be a partial function from set a to set b; or a and b are algebras of the same type, and f is a homomorphism between them; or a and b are topological spaces and f a may be a continuous map between them; or a and b may be propositions and f a proof of a b (a entails b). It was just to support such general definitions in terms of arrows, that Eilenberg and Mac Lane introduced the structures named categories.

Indeed, it is by representing structures in terms of the existence and properties of arrows and functors that category theory achieves its wide applicability and its tremendous strength in generality and abstraction. The typical representation mode of mathematics is by reference to the internal structure of objects. The applicability of the related description is then limited to objects supporting such structure. Categorical descriptions make no assumption about the internal structure of objects; they are concerned exclusively with the 'transfer' of whatever structure is preserved by the arrows. They are, in this sense, data-independent descriptions, i.e., one may expect that the same description applies to sets, graphs, algebras and whatever else can be considered as objects in a category.

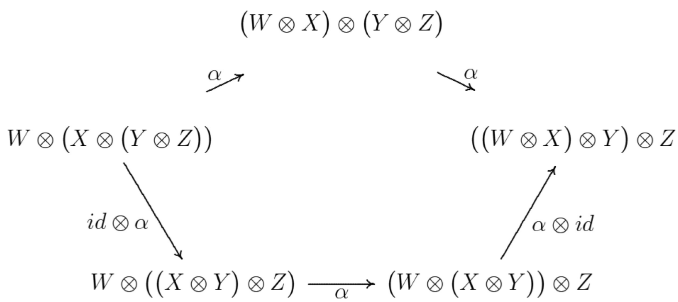
A very efficient way to look at algebra is to consider not only the elements at issue (sets, groups, rings) but also at the mappings between them (functions between sets, homomorphisms between groups or rings). In general, "objects" and "arrows" connecting them. Generality comes from the fact that a similar approach efficiently fits topology (where arrows are continuous maps and objects are spaces), geometry (here arrows are smooth maps and objects are manifolds), and in general the entire body of mathematics (including logic and the theory of formal languages) that can ultimately—and universally—be connected with set theory.

Particularly amenable to description in terms of arrows are those constructions which are 'canonical'. For example, in algebra, free and generated algebras are quite common canonical structures. An intriguing 'circular' feature here is that the arrow-theoretical description of such constructions captures all the basic structural features of the construct, including the sense in which it can be considered to be canonical itself.

A *monoidal category* C is a category characterized by four specific basic ingredients:

i) a **bifunctor** $\otimes : \mathsf{C} \times \mathsf{C} \to \mathsf{C}$;
ii) an **associator** α, i.e., a natural isomorphism $\alpha : X \otimes (Y \otimes Z) \cong (X \otimes Y) \otimes Z$, for $X, Y, Z \in \mathsf{C}$;
iii) a **unit object** E with two associated natural isomorphisms ℓ, r; $\ell : E \otimes X \cong X$; $r : X \otimes E \cong X$;
iv) a **symmetry** σ, i.e., an *involutive* natural isomorphism $\sigma : X \otimes Y \cong Y \otimes X$.

The associator implies a *pentagonal* condition, which in turn implies associativity at the level of objects:



Notice that in the frame of the category of sets, **Set,** on the contrary, it is true in general that $(X \times Y) \times Z \neq X \times (Y \times Z)$.

For M a monoid in a monoidal category, **automata** (Buchholz 2008) can be viewed as objects of a category of representations of M, possibly equipped with a *start state* and an *observation function.* If M is a monoid in **Set,** this naturally yields a generalization of the standard notion of deterministic automaton, in which the inputs to the automaton are elements of an arbitrary monoid. Dropping the requirement that such generalized automata have start states gives rise to categories whose final objects can be utilized to deal with deterministic automata.

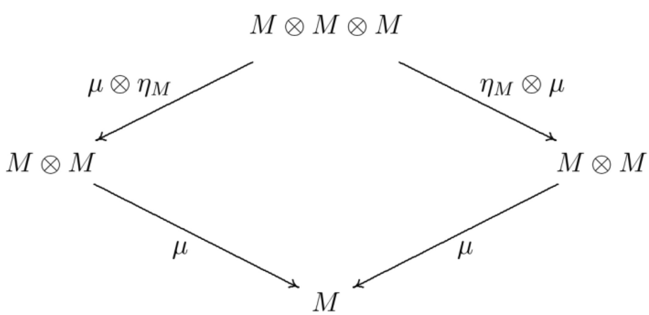
In order to implement this and to express non-determinism within this new framework, so as to be able to incorporate quantum mechanics in the picture, we need a number of auxiliary algebraic tools.

We can now proceed to an operation that generates in the frame of categories the analogue of what (quantum) deformation and the notion of coalgebra, i.e., the definition of associated Hopf algebras, give rise to with respect to Lie algebras. The construction is a bit formal, but easy to be understood if one keeps such analogy in mind.

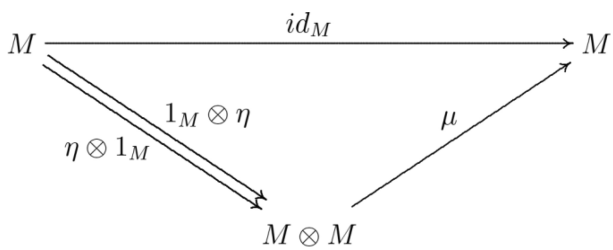
Let K be a commutative semi-ring and consider the category whose objects are K-semi-modules and whose arrows are K-linear maps. Such category turns out to be a monoidal category in which one can assume *K*-algebras as monoids of the category. The corresponding automata are referred to as *K*-linear automata. *K*-linear automata are such that with input *K*-algebra *A* they generate the category, whose elements correspond to *K*-linear extensions of formal power series (Worthington 2009).

In such case of *K*-linear extension, one can define a notion of *addition of states,* which is essentially identical with the superposition of states of quantum mechanics, holding in fact for both states and inputs. It is this addition that can be used to represent non-determinism. Moreover, addition of inputs allows us to define *co-multiplication,* which in turn endows the category with a *K*-algebra structure. Co-multiplication of inputs corresponds essentially to "multiplication of languages." If multiplication and co-multiplication satisfy the necessary compatibility conditions, the input elements generate finally the structure of a *K*-bi-algebra. This raises numerous parallels between the theory of bi-algebras and the theory of automata and formal languages, which prove that co-multiplication is indeed a sort of hidden structural element in many standard constructions involving automata and formal languages.

Let now $\mathsf{C}_\mathsf{m} = \langle C, \otimes, E \rangle$ be a monoidal category. A *monoid* m in C_m is a triple $\mathsf{m} = \langle M, \mu, \eta \rangle$ that consists of an object M of C and two morphisms $\mu{:}M \otimes M \to M$ (associative multiplication) and $\eta{:}E \to M$ such that for the associative multiplication μ the diagram



is commutative, and for the unit map η the diagram



(recall that $(M \otimes E) \cong (E \otimes M) \cong M$) commutes. In other words, we have here the fundamental characteristic building blocks, realizing the basic *pentagonal, square* and *triangular* relations.

Notice that, in a perfectly analogous way, we can define a *co-monoid* in a monoidal category C simply resorting to the notion of *opposite.* To each category C one can formally associate an opposite category C^{op} which has the same objects and for each arrow $f{:}A \rightarrow B$ has an arrow $f^{op}{:}B \rightarrow A$, with the composition $f^{op} \cdot g^{op} = (g \cdot f)^{op}$. A *contravariant* functor F on category C to category D is just an ordinary (*covariant*) functor $\mathsf{C}^{op} \rightarrow \mathsf{D}$. Manifestly, $\mathsf{C}_{\mathrm{d}} = \langle \mathsf{C}^{op}, \otimes^{op}, E \rangle$ is a monoidal category if C is monoidal.

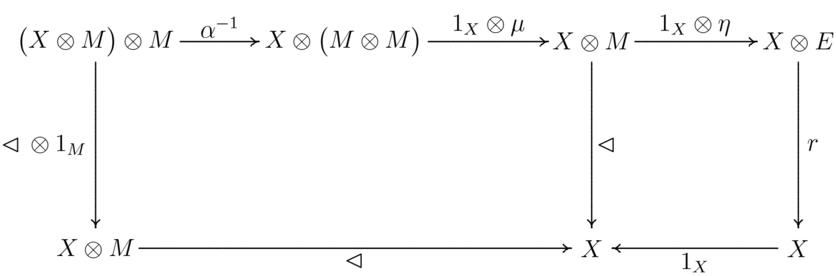
A *comonoid* d in C_{d} is a triple $\mathsf{d} = \langle C, \nu, \xi \rangle$ that consists of an object $C \in$ C and two morphisms $\Delta{:}C \rightarrow C \otimes C$. (coassociative comultiplication) and $\epsilon{:}E \rightarrow C$ such that comultiplication Δ is coassociative:

$$(1_P \otimes \Delta_P) \circ \Delta_P(W) = (1_P \otimes \Delta_P)(W \otimes W) = W \otimes (W \otimes W),$$

$$(\Delta_P \otimes 1_P) \circ \Delta_P(W) = (\Delta_P \otimes 1_P)(W \otimes W) = (W \otimes W) \otimes W.$$

Notice that $\Delta_P{:}P \rightarrow P \otimes P$ is an element in the category of monoids. One could actually think of a category which is the monoid category extended K-linearly, where K is a two-element idempotent semiring.

An important theorem, which provides a powerful working tool in the frame of the scenario described, is the theorem stating that for m a monoid and c a comonoid of a given monoidal category C in general hom(c,m) is a monoid in the category of sets. This allows us to define the action of monoids: for $\mathsf{m} = \langle M, \mu, \eta \rangle$ in C a *right action* of M on $X \in$ C is the arrow $\lhd{:}X \otimes M \rightarrow X$ satisfying the commutative diagram, *representation* of M:



Since a *bimonoid* B is nothing but a monoid in the category of comonoids, or—equivalently, a comonoid in the category of monoids, a bimonoid in

K-linear monoid category is indeed a *K*-biagebra. This closes our circular identification process.

Conclusions

The construction of previous section completes the proof of the statement given in the introduction. Category theory provides a unifying framework, where the following fundamental problems belonging to apparently from unrelated areas of science are found to be equivalent: i) *Topology;* the presentation of the the mapping class group $\mathsf{MCG}(S)$ for a Riemann surface *S,* namely of the group of diffeomorphisms in the topology of manifolds, consisting in a discrete group of symmetries of *S* generated by isotopy-classes of the automorphisms of *S;* ii) the composition of quantum angular momenta with fixed sum ***J,*** basic tool for the construction of the finite dimensional Hilbert space in which quantum computation is performed by unitary evolution operators, i.e., the graph G_n, with a finite number of vertices, basis for the construction of the quantum finite state automaton known as *Spin Network Quantum Automaton* (SNQA); [and two others, not discussed here: iii) Λ calculus and Π calculus in the theory of computation and programming in symbolic manipulation schemes; iv) proof theory in linear logic]. These problems, when formulated in the language of category theory exhibit a substantial formal identity, as they are but equivalent schemes in the frame of braided, symmetric *K*-monoidal category, *K* being a commutative semiring.

This fits pretty well into the global vision of mathematics which consistently and constantly characterized Hilbert's work: an inextricable mixture of rigor and elegance, universality, deep unity in spite of the apparent diversification of objectives and techniques.

References

Alexander, James W. 1928. "Topological Invariants of Knots and Links". *Transactions of the American Mathematical Society* 30: 275–306.

Bergen, Jeggrey, Stefan Catoiu, and William Chin (eds.). 2004. *Hopf Algebras.* Volume 237 of *Lecture Notes in Pure and Applied Mathematics.* New York: Marcel Dekker Inc.

Biedenharn, Lawrence C., and James D. Louck. 1981. "Angular Momentum in Quantum Physics: Theory and Applications." In *Encyclopedia of Mathematics and its Applications* 8. Edited by Giancarlo Rota. Reading, Penn.: Addison-Wesley.

Birman, Joan S., and Hugh M. Hilden. 1971. "On Mapping Class Groups of Closed Surfaces as Covering Spaces." Pp. 81–115 in *Advances in the theory of Riemann surfaces.* Volume 66 of *Annals of Mathematics Studies.* Princeton: Princeton University Press

Birman Joan S. 1974. "Braids, Links and Mapping Class Groups." *Annals of Mathematics Studies* 82. Princeton: Princeton University Press.

Buchholz, Peter. 2008. "Bisimulation Relations for Weighted Automata." *Theoretical Computer Science* 393: 109–123.

Dehn, Max. 1938. "Die Gruppe der Abbildungsklassen." *Acta Mathematica* 69:135–206.

Eilenberg, Samuel, and Saunders Mac Lane. 1945. "General Theory of Natural Equivalences." *Transactions of the American Mathematical Society* 58:231–294.

Eilenberg, Samuel, and Gregory M. Kelly. 1966. "Closed Categories." In *Proceedings of the Conference on Categorical Algebra* (La Jolla, 1965). Berlin: Springer Verlag.

Garnerone, Silvano, Annalisa Marzuoli, and Mario Rasetti. 2006. "Spin Networks, Quantum Automata and Link Invariants." *Journal of Physics: Conference Series* 33:95–106.

Garnerone, Silvano, Annalisa Marzuoli, and Mario Rasetti. 2007. "Quantum Geometry and Quantum Algorithms." *Journal of Physics A: Mathematical and Theoretical* 40:3047–3066.

Garnerone, Silvano, Annalisa Marzuoli, and Mario Rasetti. 2009. "Efficient quantum processing of three–manifold topological invariants." *Advances in Theoretical and Mathematical Physics* 13:1601–1652.

Gray, Jeremy, and David Rowe. 2000. *The Hilbert Challenge.* Oxford: Oxford University Press.

Hatcher, Allen, and William P. Thurston. 1980. "A Presentation for the Mapping Class Group of a Closed Orientable Surface." *Topology* 19:221–237.

Hilbert, David. (1900) 1902. "Mathematical Problems." *Bulletin of the American Mathematical Society* 8:437–479.

Hilbert, David. 1924. "Die Grundlagen der Physik." *Mathematische Annalen* 92:1–32.

Jaeger, François, Vertigen, Dirk, and Dominic J. A. Welsh. 1990. "On the Computational Complexity of the Jones and Tutte polynomials." *Mathematical Proceedings of the Cambridge Philosophical Society* 108:35–53.

Jones, Vaughan F. R. 1985. "A Polynomial Invariant for Knots Via Von Neumann Algebras." *Bulletin of the American Mathematical Society* 12:103–111.

Kassel, Christian. 1995. *Quantum Groups.* Berlin: Springer Verlag.

Kohno, Toshitake. 1992. "Topological Invariants for 3-Manifolds Using Representations of Mapping Class Groups." *Topology* 31:203–230.

Mac Lane, Saunders. 1998. *Categories for the Working Mathematician.* Berlin: Springer Verlag.

Majid, Shahn. 1995. *Foundations of Quantum Group Theory.* Cambridge: Cambridge University Press.

Marzuoli, Annalisa, and Mario Rasetti. 2002. "Spin Network Quantum Simulator." *Physics Letters A* 306: 79–87.

Marzuoli, Annalisa, and Mario Rasetti. 2005. "Computing Spin Networks." *Annals of Physics* 318:345–407.

Marzuoli, Annalisa, and Mario Rasetti. 2006. "Coupling of Quantum Angular Momenta: An Insight into Analogic/Discrete and Local/Global Models Of Computation." *Natural Computing* 6:151–168.

Moore, Cristopher, and James P. Crutchfield. 2000. "Quantum Automata and Quantum Grammars." *Theoretical Computer Science* 237:275–306.

Rasetti, Mario, and Chiara Marletto. 2009. "Quantum Information Manipulation: Topology, Formal Languages, Groups." In *The Nature Description in Quantum Field Theory: Open Problems and Epistemological Perspective.* Edited by Ignazio Licata and Ammar S. J. Sakaji. New York: Springer.

Thurston, William P. 1997. *The Geometry and Topology of Three-Manifolds.* Princeton: Princeton University Press.

Witten, Edward. 1989. "Quantum Field Theory and the Jones Polynomial." *Communications in Mathematical Physics* 121:351.

Worthington, James. 2009. "A Bialgebraic Approach to Automata and Formal Language Theory." Pp. 451–467 in *Proceedings Logical Foundations of Computer Science.* Vol. 5407 of LNCS. Edited by Sergei N. Artemov and Anil Nerode. New York: Springer.