Why Theory of Quantum Computing Should be Based on Finite Mathematics

Felix M. Lev

Artwork Conversion Software Inc., 1201 Morningside Drive, Manhattan Beach, CA 90266, USA (Email: felixlev314@gmail.com)

Abstract

We discuss finite quantum theory (FQT) developed in our previous publications and give a simple explanation that standard quantum theory is a special case of FQT in the formal limit $p \to \infty$ where p is the characteristic of the ring or field used in FQT. Then we argue that FQT is a more natural basis for quantum computing than standard quantum theory.

Keywords: finite mathematics, quantum theory, quantum computing

1 Motivation

Classical computer science is based on discrete mathematics for obvious reasons. Any computer can operate only with a finite number of bits, a bit represents the minimum amount of information and the notions of one half of the bit, one third of the bit etc. are meaningless. Continuous mathematics can be used in computer science only as a technique for approximate numerical calculations but the foundation of computer science does not involve continuous mathematics.

However, quantum computing is based on the notion of qubit which is a quantum superposition of bits with complex coefficients. As a consequence, quantum computing automatically becomes a theory involving standard notions of continuous mathematics (infinitely small/large, continuity etc.). Is this situation natural? For understanding the answer to this question the following historical remarks might be useful.

Historically the notions of infinitely small/large, continuity etc. have arisen from a belief based on everyday experience that any macroscopic object can be divided into arbitrarily large number of arbitrarily small parts. Classical physics is based on classical mathematics developed mainly when people did not know about existence of elementary particles. However, from the point of view of the present knowledge those notions look problematic.

For example, a glass of water contains approximately 10^{25} molecules. We can divide this water by ten, million, etc. but when we reach the level of atoms and elementary particles the division operation loses its meaning and we cannot obtain arbitrarily small parts. So, *any description of macroscopic phenomena using continuity and differentiability can be only approximate*. In nature there are no continuous

curves and surfaces. For example, if we draw a line on a sheet paper and look at this line by a microscope then we will see that the line is strongly discontinuous because it consists of atoms.

Analogously, in computer science a bit is an analog of elementary particle and, as noted above, a bit is indivisible. Therefore in computer science standard division can be used only for approximate calculations in situations when the number of bits is large but in the general case standard division cannot be treated as a fundamental operation.

Classical mathematics is not in the spirit of the philosophy of quantum theory and the Viennese school of logical positivism that *"A proposition is only cognitively meaningful if it can be definitively and conclusively determined to be either true or false"*. This mathematics proceeds from axioms the validity of which cannot be verified. For example, it cannot be determined whether the statement that $a + b = b + a$ for all natural numbers a and b is true or false.

Another example follows. Let us pose a problem whether 10+20 equals 30. Then we should describe an experiment which will solve this problem. Any computer can operate only with a finite number of bits and can perform calculations only modulo some number p. Say $p = 40$, then the experiment will confirm that 10+20=30 while if $p = 25$ then we will get that 10+20=5. So the statements that 10+20=30 and even that $2 \cdot 2 = 4$ are ambiguous because they do not contain *explicit* information on how they should be verified. On the other hand, the statements

$$10 + 20 = 30\,(mod\,40),\ 10 + 20 = 5\,(mod\,25),\ 2 \cdot 2 = 4\,(mod\,5),\ 2 \cdot 2 = 2\,(mod\,2)$$

are well defined because they do contain such an information. So only operations modulo some number are well defined. This example shows that classical mathematical is based on the implicit assumption that in principle one can have any desired amount of resources and, in particular, one can work with computers having as many bits as desired.

The official birth of quantum theory is 1925, and even the word "quantum" reflects a belief that nature is discrete. The founders of this theory were highly educated physicists but they knew only classical mathematics because even now mathematical education at physics departments does not involve discrete and finite mathematics.

In view of the above remarks it is reasonable to think that in quantum theory classical mathematics might be used for solving special problems but ultimate quantum theory should not be based on classical mathematics. At present, in spite of efforts of thousands of highly qualified physicists and mathematicians to construct such a theory on the basis of classical mathematics, this problem has not been solved. In particular, quantum gravity contains infinities which cannot be removed by renormalization. Nevertheless the following question arises. If classical mathematics is not natural in quantum theory then why is it proven to be so successful for solving many quantum problems?

One of the key principles of physics is the correspondence principle. It means that at some conditions any new theory should reproduce results of the old

well tested theory with a good accuracy. Usually the correspondence principle is applied such that the new theory contains a parameter and reproduces results of the old theory in a formal limit when the parameter is infinitely large or infinitely small. Known examples are that nonrelativistic theory is a special case of relativistic one in the formal limit $c \to \infty$ and classical (i.e. nonquantum) theory is a special case of quantum one in the formal limit $\hbar \to 0$. In view of the above remarks it is reasonable to think that standard continuous quantum theory is a special case of a quantum theory based on other mathematics in the formal limit when some parameter becomes zero or infinity. So a problem arises what mathematics should be used in ultimate quantum theory and what parameter describes a correspondence between the new quantum theory and standard one.

Classical mathematics starts from natural numbers and the famous Kronecker's expression is: *"God made the natural numbers, all else is the work of man"*. However here only addition and multiplication are always possible. In order to make addition invertible we introduce negative integers. They do not have a direct physical meaning (e.g. the phrases "I have -2 apples" or "this computer has -100 bits of memory" are meaningless) and their only goal is to get the ring of integers Z.

However, if instead of all natural numbers we consider only a set R_p of p numbers 0, 1, 2, ... $p-1$ where addition and multiplication are defined as usual but modulo p then we get a ring without adding new elements. If, for example, p is odd then one can consider R_p as a set of elements $\{0, \pm i\}$ $(i = 1, ...(p-1)/2)$. If elements of Z are depicted as integer points on the x axis of the xy plane then it is natural to depict the elements of R_p as points of the circumference in Fig. 1.

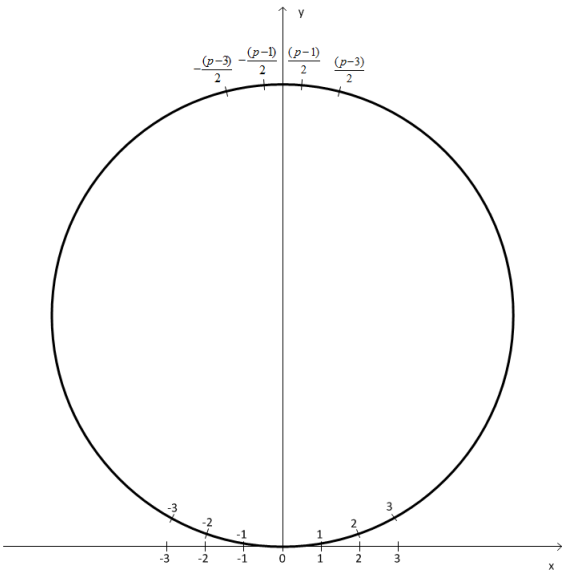

Figure 1: Relation between R_p and Z

Let f be a function from R_p to Z such that $f(a)$ has the same notation in Z as a in R_p. Then for elements $a \in R_p$ such that $|f(a)| \ll p$, addition, subtraction

and multiplication are the same as in Z. In other words, for such elements we do not feel the existence of p. Indeed, for elements $a_j \in R_p$ $(j = 1, 2)$ such that $|f(a_j)| < [(p-1)/2]^{1/2}$ we have that $f(a_1 \pm a_2) = f(a_1) \pm f(a_2)$ and $f(a_1 a_2) = f(a_1) f(a_2)$ which shows that f is a local isomorphism of some vicinities of zero in R_p and Z.

As explained in textbooks, both R_p and Z are cyclic groups with respect to addition. However, R_p has a higher symmetry because, in contrast to Z, R_p has a property which we call *strong cyclicity*: for any fixed $a \in R_p$ any element of R_p can be obtained from a by successively adding 1.

When p increases, the bigger and bigger part of R_p becomes the same as Z. Hence Z can be treated as a degenerate case of R_p in the formal limit $p \to \infty$ because in this limit operations modulo p disappear and strong cyclicity is broken. *Therefore, at the level of rings standard mathematics is a degenerate case of finite one when formally* $p \to \infty$.

The transition from R_p to Z is similar to the procedure, which in group theory is called contraction. This notion is used when the Lie algebra of a group with a lower symmetry can be treated as a formal limit of the Lie algebra of a group with a higher symmetry when some parameter goes to zero or infinity. Known examples are the contraction from the de Sitter to the Poincare group and from the Poincare to the Galilei group.

The above construction has a well-known historical analogy. For many years people believed that the Earth was flat and infinite, and only after a long period of time they realized that it was finite and curved. It is difficult to notice the curvature when we deal only with distances much less than the radius of the curvature. Analogously one might think that the set of numbers describing physics in our Universe has a "curvature" defined by a very large number p but we do not notice it when we deal only with numbers much less than p.

One might argue that introducing a new fundamental constant p is not justified. However, as noted above, history of physics tells us that more general theories arise when a parameter, which in the old theory was treated as infinitely small or infinitely large, becomes finite. Therefore, it is natural to think that in quantum physics the quantity p should be not infinitely large but finite.

From mathematical point of view standard quantum theory can be treated as a theory of representations of special real Lie algebras in complex Hilbert spaces. In Refs. [1, 2, 3, 4] and other publications we have proposed an approach called FQT (Finite Quantum Theory) when Lie algebras and representation spaces are over a finite field or ring with characteristic p. It has been shown that in the formal limit $p \to \infty$ FQT recovers predictions of standard continuous theory. Therefore classical mathematics describes many experiments with a high accuracy as a consequence of the fact that the number p is very large.

In Sec. 2 we explicitly describe the correspondence between FQT and standard quantum theory and in Sec. 3 we argue that FQT is a natural basis for the theory of quantum computing.

2 Correspondence between FQT and standard quantum theory

In standard quantum theory one starts from the choice of the space-time background. The background has the symmetry group and the operators characterizing the system under consideration should satisfy the commutation relation of the Lie algebra for this group. However, as argued in Ref. [4], the approach should be opposite to standard one. Every quantum system is described by a set of operators which somehow commute with each other and the rules of their commutation define the symmetry algebra. Therefore in quantum theory one should start not from the space-time background, which is the classical notion, but from the symmetry algebra. Then every physical system is described by a representation of this algebra by Hermitian operators in a separable Hilbert space H. We will use a "tilde" to denote elements of Hilbert spaces and complex numbers.

Let $(\tilde{e}_1, \tilde{e}_2, ...)$ be a basis in H. This means that $\tilde{x}$ can be represented as

$$\tilde{x} = \tilde{c}_1\tilde{e}_1 + \tilde{c}_2\tilde{e}_2 + ... \tag{1}$$

where $(\tilde{c}_1, \tilde{c}_2, ...)$ are complex numbers. It is assumed that there exists a complete set of commuting selfadjoint operators $(\tilde{A}_1, \tilde{A}_2, ...)$ in H such that each $\tilde{e}_i$ is the eigenvector of all these operators: $\tilde{A}_j\tilde{e}_i = \tilde{\lambda}_{ji}\tilde{e}_i$. Then the elements $(\tilde{e}_1, \tilde{e}_2, ...)$ are mutually orthogonal: $(\tilde{e}_i, \tilde{e}_j) = 0$ if $i \neq j$ where (...,...) is the scalar product in H. In that case the coefficients can be calculated as

$$\tilde{c}_i = \frac{(\tilde{e}_i, \tilde{x})}{(\tilde{e}_i, \tilde{e}_i)} \tag{2}$$

Their meaning is that $|\tilde{c}_i|^2(\tilde{e}_i, \tilde{e}_i)/(\tilde{x}, \tilde{x})$ represents the probability to find $\tilde{x}$ in the state $\tilde{e}_i$. In particular, when $\tilde{x}$ and the basis elements are normalized to one, the probability equals $|\tilde{c}_i|^2$.

Let us note that the Hilbert space contains a big redundancy of elements, and we do not need to know all of them. Indeed, with any desired accuracy we can approximate each $\tilde{x} \in H$ by a finite linear combination

$$\tilde{x} = \tilde{c}_1\tilde{e}_1 + \tilde{c}_2\tilde{e}_2 + ...\tilde{c}_n\tilde{e}_n \tag{3}$$

where $(\tilde{c}_1, \tilde{c}_2, ...\tilde{c}_n)$ are rational complex numbers. This is a consequence of the known fact that the set of elements given by Eq. (3) is dense in H. In turn, this set is redundant too. Indeed, we can use the fact that Hilbert spaces in quantum theory are projective: ψ and $c\psi$ $(c \neq 0)$ represent the same physical state. Then we can multiply both parts of Eq. (3) by a common denominator of the numbers $(\tilde{c}_1, \tilde{c}_2, ...\tilde{c}_n)$. As a result, we can always assume that in Eq. (3) $\tilde{c}_j = \tilde{a}_j + i\tilde{b}_j$ where $\tilde{a}_j$ and $\tilde{b}_j$ are integers.

The meaning of the fact that Hilbert spaces in quantum theory are projective is very clear. The matter is that not the probability itself but the relative

probabilities of different measurement outcomes have a physical meaning. We believe, the notion of probability is a good illustration of the Kronecker expression about natural numbers (see Sect. 1). Indeed, this notion arises as follows. Suppose that conducting experiment N times we have seen the first event n_1 times, the second event n_2 times etc. such that $n_1+n_2+... = N$. We define the quantities $w_i(N) = n_i/N$ (these quantities depend on N) and $w_i = lim\, w_i(N)$ when $N \to \infty$. Then w_i is called the probability of the ith event. We see that all the information about the experiment is given by a finite set of natural numbers, and all those numbers are finite. However, in order to define probabilities, people introduce additionally the notion of rational numbers and the notion of limit. Another example is the notion of mean value. Suppose we measure a physical quantity such that in the first event its value is q_1, in the second event - q_2 etc. Then the mean value of this quantity is defined as $(q_1n_1 + q_2n_2 + ...)/N$ if N is very large. Therefore, even if all the q_i are integers, the mean value might be not an integer. We again see that rational numbers arise only as a consequence of our convention on how the results of experiments should be interpreted.

Consider now how quantum states are described in FQT. In Sect. 1 we described the ring R_p. It is well known that if p is prime then R_p becomes not only the ring but also the field F_p if division is defined as usual but modulo p. We can introduce a formal element i such that $i^2 = -1$. Then we can consider the ring $R_{p^2} = R_p + iR_p$ which consists of elements $a + bi$, $a, b \in R_p$.

Analogously, one might think that it is possible to define the field $F_{p^2} = F_p + iF_p$ which consists of elements $a + bi$, $a, b \in F_p$. However, this is not obvious for the following reason. The definition of division as $(a + bi)^{-1} = (a - bi)/(a^2 + b^2)$ can be consistent only if $(a^2 + b^2) \neq 0$ in F_p if $a \neq 0$ or $b \neq 0$. A well known fact in number theory is that this is the case if $p = 3\ (mod\ 4)$ while if $p = 1\ (mod\ 4)$ this is not the case. A simple example is that $2^2 + 1^2 = 0$ in F_5.

However, a well known fact in number theory is that the field F_{p^2} of p^2 elements can be constructed as follows. Let the equation $x^2 = -a_0$ ($a_0 \in F_p$) has no solutions in F_p. Then F_{p^2} can be formally defined as the set of elements $a + b\kappa$ where $a, b \in F_p$, and κ satisfies the condition $\kappa^2 = -a_0$. In the special case when $p = 3\ (mod\ 4)$, $a_0 = 1$ one can choose $\kappa = i$ but in other cases it is always possible to find a pair (κ, a_0). In what follows for simplicity we will consider only this special case.

In FQT one can describe quantum states by elements in a linear space V over R_{p^2} or F_{p^2} and operators of physical quantities as operators in this space. Since complex conjugation is the automorphism of $R_{p^2} = R_p + iR_p$ and the automorphism of $F_{p^2} = F_p + iF_p$ if $p = 3\ (mod\ 4)$ then, by analogy with conventional quantum theory, in FQT it is possible to consider situations when V is supplied by a scalar product (...,...) such that for any $x, y \in V$ and $a \in R_{p^2}$, (x, y) is an element of R_{p^2} and the following properties are satisfied:

$$(x, y) = \overline{(y, x)}, \quad (ax, y) = \bar{a}(x, y), \quad (x, ay) = a(x, y) \tag{4}$$

Then in the space V one can choose a basis $(e_1, e_2, ...)$ consisting of mutually orthog-

onal elements such that any element $x \in V$ can be represented as

$$x = c_1 e_1 + c_2 e_2 + ...c_n e_n \tag{5}$$

where the coefficients are elements of R_{p^2} or F_{p^2}. One can also formally define Hermitian operators A in V such that $(Ax, y) = (x, Ay)$.

The correspondence between FQT and standard quantum theory can now be described as follows. As noted above, every element of the Hilbert space can be approximated with any desired accuracy by elements $\tilde{x}$ in Eq. (3) such that $\tilde{c}_j = \tilde{a}_j + i\tilde{b}_j$ where $\tilde{a}_j$ and $\tilde{b}_j$ are integers. Consider now the elements x in Eq. (5) where $c_j = a_j + ib_j$. Then, as follows from the discussion in Sec. 1, for elements such that $f(a_j) = \tilde{a}_j$, $f(b_j) = \tilde{b}_j$, $|f(a_j)| \ll p$, $|f(b_j)| \ll p$ $\forall j = 1, 2, ...n$ the description in terms of Hilbert spaces and spaces over R_{p^2} or F_{p^2} are practically indistinguishable. Therefore if p is very large then for a large number of elements FQT and standard quantum theory give practically the same results. The theories essentially differ from each other only in the description of elements x in Eq. (5) for which some of the numbers $|f(a_j)|$, $|f(b_j)|$ are comparable to p. Therefore standard quantum theory can be treated as a special case of FQT in the formal limit $p \to \infty$.

3 Discussion and conclusion

It follows from the above discussion that in FQT probabilistic interpretation can be only approximate in situations when the coefficients in Eq. (5) are much less than p. A difference between FQT and standard quantum theory is also as follows. As follows from the Zassenhaus theorem [5], all irreducible representations of Lie algebras with nonzero characteristics are finite-dimensional. As a consequence, elementary particles in FQT are described by finite-dimensional representations, not infinite-dimensional ones as in standard quantum theory. It is also obvious that since the ring R_{p^2} and the field F_{p^2} are finite, infinities in FQT cannot exist in principle, in contrast to the situation in standard quantum theory.

One can pose a problem whether the ultimate quantum theory will involve FQT based on a ring or on a field. Known facts from standard algebra are that invariance of dimension, basis and linear independence are well defined only in spaces over a field or body. In addition, existence of division is often convenient for calculations. At the same time, as argued in Sec. 1, in quantum theory division is not fundamental. History of physics tells us that it is desirable to construct physical theories with the least required notions. Therefore a problem arises whether ultimate quantum theory can be constructed without using division at all. For the first time this possibility has been discussed in Ref. [6]. A discussion of this problem can be also found in Ref. [7].

We now argue why the theory of quantum computing should be based on FQT rather than standard quantum theory. As noted in Sec. 1, the notions of standard division, continuity etc. are fully unnatural in computer science and when we define qubit as a quantum superposition of bits with complex coefficients we

bring those unnatural notions to quantum computing. Then in numerical quantum computations a problem always arises how to approximate complex numbers by a finite set because in such calculations we can work only with such sets. This again shows that by using complex numbers in quantum computing we create additional artificial difficulties.

Therefore it is much more natural to define qubit as a quantum superposition of bits with coefficients from R_{p^2} or F_{p^2}. Then a question arises what value of p should be taken for this purpose. As discussed in Refs. [4, 7], gravity can be treated as a consequence of the fact that physics in our Universe is described by a finite ring or field with a very large characteristic such that lnp is of the order of 10^{80} and therefore p is a huge number of the order of $exp(10^{80})$. However, in quantum computing there is no need to work with such a huge number. By analogy with classical computing problem where each computer cannot work with numbers described by a number of bits exceeding the computer capacity, for each problem in quantum computing the number p should be chosen such that the total number of states should not exceed the number of states available in the quantum computer under consideration.

References

[1] Lev F M *Modular Representations as a Possible Basis of Finite Physics* J. Math. Phys. **30** 1985-1998 (1989).

[2] Lev F M *Finiteness of Physics and its Possible Consequences* J. Math. Phys. **34** 490-527 (1993).

[3] Lev F M *Why is Quantum Theory Based on Complex Numbers?* Finite Fields and Their Applications **12** 336-356 (2006).

[4] Lev F M *de Sitter Symmetry and Quantum Theory* Phys. Rev. **D85** 065003 (2012).

[5] Zassenhaus H *The Representations of Lie Algebras of Prime Characteristic* Proc. Glasgow Math. Assoc. **2** 1-36 (1954).

[6] Saniga M and Planat M *Finite Geometries in Quantum Theory: From Galois (fields) to Hjelmslev (rings).* J. Mod. Phys. **B20** 1885-1892 (2006).

[7] Lev F M *Finite Quantum Theory and Applications to Gravity and Particle Theory* arxiv:1104.4647 (2016).