Logic and **L**ogical **P**hilosophy
Volume 28 (2019), 173–193
DOI: 10.12775/LLP.2018.005

Krzysztof Wójtowicz

THEORY OF QUANTUM COMPUTATION AND PHILOSOPHY OF MATHEMATICS. PART II

Abstract. In the article, the philosophical significance of quantum computation theory for philosophy of mathematics is discussed. In particular, I examine the notion of "quantum-assisted proof" (QAP); the discussion sheds light on the problem of the nature of mathematical proof; the potential empirical aspects of mathematics and the realism-antirealism debate (in the context of the indispensability argument). I present a quasi-empiricist account of QAP's, and discuss the possible impact on the discussions centered around the Enhanced Indispensabity Argument (EIA).

Keywords: quantum computation; quantum-assisted proofs; indispensability argument; mathematical realism; quasi-empiricism

Introduction

This paper discusses the philosophical significance of quantum computation theory for philosophy of mathematics, in particular for the following issues: the nature of mathematical proof; the potential empirical aspects of mathematics and the realism–antirealism debate (in the context of the indispensability argument). It can be viewed as a continuation of [Wójtowicz, 2009], but is essentially self-contained. The former paper was more technical in character, here I concentrate on the philosophical questions.

The article has the following structure: general remarks on quantum algorithms; the concept of quantum-assisted proof (QAP); are there empirical proofs?; quasi-empirical account of quantum proofs; and concluding remarks.

Received September 21, 2017. *Published online* April 18, 2018

The investigations within the paper concern mainly quantum computation, but they apply to the general problem of the relationship between mathematics and physics. I argue, that the possibility of quantum proofs present serious difficulties for the recently much discussed Enhanced Indispensabity Argument (EIA) for mathematical realism — and propose a way of solving the emerging problems. In particular, I claim that the best philosophical account is quasi-empiricism in Quine's manner. The paper therefore gives a support for the realistic account of mathematics.

1. General remarks on quantum algorithms

One of the motivations for investigating quantum-computational models is the intractability of many computational (combinatorial, number-theoretical, graph-theoretical etc.) problems.[1] An important example of such a intractable problem is factorization, where no quick, (i.e. polynomial) classical algorithm is known — but there is a quick quantum algorithm [Shor, 1994].

A natural set of complex computational problems arises, when we consider simulating the behavior of quantum systems. Usually, the computer simulation of the evolution of a quantum system is impossible because we need exponentially many coefficients even to describe the quantum system in question.[2] So the computation corresponding to the evolution of the quantum system is extraordinarily complex. But this gives us the possibility to exploit the specific features of the quantum world in order to solve computational problems.

The general idea here is — broadly speaking — to reverse the way we usually conceive the relationship between the physical system and the computer simulation: instead of providing a computer simulation of the physical system, we use the physical system to perform a physical simulation of the (mathematical) computational process.[3]

[1] [Nielsen and Chuang, 2000] is a monographic survey. A readable survey article is [Montanaro, 2015]. Aaronson [2013] gives a popular presentation, including also a discussion of related problems.

[2] We need 2^n complex coefficients (probability amplitudes) in order to describe the state of n entagled particles (as a superposition of 2^n basic states).

[3] The idea of using quantum phenomena in solving computational problems was presented in [Feynman, 1982].

So consider a computational problem P which corresponds (in some identifiable way) to the evolution of a quantum system $Q(P)$. In particular — the final state of the evolution of the quantum system $Q(P)$ corresponds to the result of the computation P. In such situations we could exploit the (quick) quantum evolution instead of the (slow) computation to solve the computational problem P. Trivially, such a correspondence obtains, when we start with a quantum system Q, and consider its computer simulation P_Q (then of course $Q(P_Q) = Q$). But this is not the point: the crucial question is, whether there are any MATHEMATICALLY MOTIVATED computational problems P (i.e. problem which arise within ordinary mathematics, and not for the purpose of describing quantum systems) for which such quantum systems $Q(P)$ exist. This is indeed the case — as demonstrated by the famous Shor's algorithm for factoring numbers.

Quantum algorithms are mathematical counterparts of certain quantum processes (such as for example a system of photons passing through a system of half-silvered mirrors).[4] They exploit the peculiarities of the quantum world (entanglement and superposition). The class of problems decidable by quantum algorithms is exactly the class of (Turing) decidable problems, so in particular — unsolvable problems remain unsolvable. But — at least in some cases — there can be an enormous increase in computational speed, and this makes them particularly attractive.[5]

However, there are no quantum computers available, because the technical problems to be overcome are formidable (due to the fragility of quantum states, which have to be isolated from their environment, i.e. the external world). It may well be the case, that even the impressive Shor's factoring algorithm remains just a purely theoretical possibility. There is also a perhaps deeper, conceptual problem: the class of known interesting quantum algorithms is limited. Factorization is not

[4] Mathematically, a qubit is an element of the form $\alpha_0|0\rangle + \alpha_1|1\rangle$, where α_0 and α_1 are complex numbers. Passing through a quantum gate corresponds to the action of a certain operator on a Hilbert space on the qubit. A 2-qubit quantum register has the form $\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$. An n-qubit register requires 2^n coefficients for its description, and has the general form $\alpha_{00..0}|00..0\rangle + \alpha_{00..1}|00..1\rangle + \cdots + \alpha_{11..0}|11..0\rangle + \alpha_{11..1}|11..1\rangle$ (being an element of a Hilbert space of dimension 2^n).

[5] Apart of Shor's algorithm, another example is Grover's search algorithm: we are searching an item within an unstructured database of size N. Classically, on average we have to make $N/2$ checks. Grover's search algorithm gives a quadratic speed-up: we need $O(\sqrt{N})$ checks.

NP-complete, so even if we had a quantum computer available, Shor's algorithm would not give us a general method of solving NP-complete problems. It far from obvious, that a quantum algorithm for solving NP-complete problems (e.g. SAT) will ever be found.[6]

The emergence of (applicable) quantum computers would certainly lead to major changes in science and technology. And even the theoretical possibility inspires us to reconsider philosophical questions concerning the nature of mathematical knowledge, the role of mathematical proofs and the relationships between mathematics and science. We face the question of the relationships between mathematics and the mathematical notion of computation on one hand — and the laws of physics and the "computational resources" of the universe on the other. And even if these considerations have the character of a thought experiment, they can shed new light on fundamental philosophical problems.

2. Quantum-assisted proofs (QAPs)

The (theoretical) possibility of quantum computation, and executing quantum assisted proofs (for which I will use the acronym QAP) is very exciting. In order to understand the peculiarities of the possible QAP, let us exhibit its most important features. In general, it would consist of the following steps.

1. The mathematical (conceptual) phase. Consider a computational problem P (e.g. factoring numbers). Our task is to define a quantum system $Q(P)$, which is connected to P in an explicit way — in particular there is a way of identifying the outcome of P from the outcome of $Q(P)$. Here we reverse the usual way of viewing the relationship between real-world situations and computer simulations. Instead of running a computer simulation to find out, what would happen in a physical situation (e.g. whether a bridge would break down), we perform the physical experiment in order to learn, what the outcome of the (perhaps extraordinarily long) computation would be. This problem becomes interesting, when

[6] In the case of a NP-complete problem (where 2^n data have to be examined), the lower bound of the unstructured search is $O(2^{n/2})$, as was proved in [Bennett et al., 1997]. They interpret their result in the following way: "There is no black-box approach to solving NP — complete problems by using some uniquely quantum-mechanical features of QTMs". So in order to obtain a quicker algorithm, the structure of the problem should be exploited in some clever way. It is an open question, whether it is possible.

P has a natural mathematical motivation, and arises within a natural mathematical context. In this case, finding a corresponding quantum system $Q(P)$ would allow us to solve P.

2. The experimental phase consists of:

(a) Preparing the quantum system Q(P) in an appropriate initial state.
(b) Initiating the quantum process. The crucial feature of this process is that during this computation we cannot in any way interfere with it, as this would destroy the process (so we have to wait patiently for the outcome).
(c) Performing the final measurement. This means, roughly speaking, that we extract the available information from the quantum system.

The outcome of the experiment with the use of $Q(P)$ yields a solution of the problem P.

A natural question follows: measurements have a probabilistic nature, so in general we cannot identify the state of the quantum system before the measurement, and the information is lost.[7] This is true — but in some cases, it is possible to "extract" enough information from the quantum system. For example, if we knew in advance (i.e. before the measurement), that the qubit could have been only in one of the two basic states, then the measurement would give us complete information. A similar situation can happen with more complicated n-qubit registers: if we know in advance, that they are in one of few possible states, appropriate measurements will enable us to identify it.[8] This is crucial for quantum algorithms.

Many mathematical problems involve a complex computational part, so a quick computational method might settle some of such problems (as it happens in the case of ordinary computer assisted proofs). In partic-

[7] In the measurement of a qubit yields 1, we can only learn from that, that the probability amplitude of the system being in the state $|1\rangle$ was non-zero.

[8] An example of 2-qubit quantum register will illustrate the general rule. Let us assume, that we know IN ADVANCE, that a certain quantum process terminates only in one of the two following states:

S_0: $1/\sqrt{2}(|00\rangle + |01\rangle)$
S_1: $1/\sqrt{2}(|10\rangle + |11\rangle)$

We perform the measurement on the FIRST qubit. The result is either 0 or 1, and there is a clear correspondence: we could obtain 0 if and only if the state of the register is S_0 (analogously for 1). So the measurement on the first qubit informs us definitely, whether the process terminated in S_0 or S_1. (Observe, that the measurement on the second qubit yields 0 or 1 with equal probability for both S_0 and S_1).

ular, we might get quantum-assisted proofs of some mathematical theorems. The outcome might differ from the outcome of the classical computation in one important respect: we would not be able to know which of the theoretically possible computational paths was the successful one. Indeed, there are quantum algorithms, which do not always exhibit CONCRETE solutions, but rather provide some general information about the problem. For example, the quantum algorithm presented in [Harrow et al., 2009] allows to get some information about systems of equations: the algorithm outputs a quantum state with certain properties, and not explicitly the solution.[9] In order to "extract" the solution from this state we would have to perform a large number of measurements. But sometimes we are interested not in the exact solution, but in some general property of it, which might be established by performing just few measurements.[10]

In some cases, solving a computational problem is an essential part of a proof.[11] So we might get a QAP of a possibly important mathematical theorem. The situation becomes philosophically even more interesting, when we consider logical problems in their combinatorial (number-theoretic) formulation/disguise. Formal proofs can be encoded as numbers (via arithmetization of syntax), So — ultimately — the question whether there is a formal proof of a sentence α within a formal theory T becomes a computational problem. Usually this is not a decidable problem (and will not become "quantumly decidable" either[12]), but we can always check, whether a given string σ of symbols is a formal proof of α within T — and we can also check, whether there is a proof of α within a given finite set of strings S). A quick computational procedure would allow us to find answer to questions like: "Is there a proof of α within T of the

[9] "The same algorithm, or closely related ideas, can also be applied to problems beyond linear equations themselves. [...] It should be stressed that in all these cases the quantum algorithm "solves" these problems in the same sense as the HHL algorithm solves them: it starts with a quantum state and produces a quantum state as output. Whether this is a reasonable definition of "solution" depends on the application, and again may depend on whether the input is produced algorithmically or is provided explicitly as arbitrary data [1]." [Montanaro, 2015, p. 9]

[10] We might be interested in the question, whether there exists a solution — and often this very fact is much more important than the particular details. In general, qualitative information might be easier to obtain.

[11] It might be factoring numbers, pattern matching, multiplying (big) matrices, establishing a property of graphs etc.

[12] Remember, that quantum algorithms have the same computational power as classical algorithms (but can be quicker).

length bounded by n?" (T being for example ZFC or PA or RCA_0 or any other formal theory of interest). At least in the case of some open problems, the answer would be positive.[13] But then, from our point of view, after the process terminates, only a big "YES!" is displayed on the screen .... Even if it happened only in one single case, i.e. even if one such a quantum demonstration of the existence of a formal proof succeeded only once, the question of the status of such knowledge would become philosophically intriguing.

So, in general we might think of two possible scenarios:

1. A "direct" QAP: i.e. a computation, which solves a computational problem, yielding a proof of a mathematical theorem α.[14]
2. A "meta-QAP": the computation has a direct metamathematical interpretation, yielding a positive answer to the question "Is there is a formal proof of α within T of length bounded by n?"[15]

Could either of these processes be considered a proof of α? We cannot even dream of reading out any details of this proof from the process, as measurements cannot be performed during the computation. In particular, in the "meta-QAP" case we would be confronted with a kind of of "quantum non-constructive existence argument": we only learn, that such a formal proof (of the length $\leqslant n$) exists — and NOTHING MORE.

Observe the following crucial features of a potential QAP:

1. It is quick (it might even be exponentially quicker that the classical algorithms).
2. We have no insight into the process — we only can perform the final measurement.
3. We have to rely strongly of physical theories in order to treat these procedures as reliable.

[13] Trivially, the question would be positive in many cases, as there are also formal proofs of length 1. But the question is, whether there are any MATHEMATICALLY INTERESTING facts, which could be given answers in this way. By the way, negative answers (i.e. that there is no such a proof) would also provide valuable information, as we would get some kind of lower bound concerning the logical complexity of the problem.

[14] So we would think of a situation similar to e.g. the four-color theorem, where a formidable computation yields the result. In the case of a QAP, this computation would become "formidable$^{\text{formidable}}$".

[15] Nevertheless, it is not very probable, that such "meta-QAPs", confirming that a theory T formally proves α will be invented. It would require a very specific insight into the structure of the "database" to check (i.e. the collection of possible proofs).

We are therefore faced with a situation, where we exploit some physical processes (resources) in order to solve computationally difficult problems. The analyses given here apply to all cases, in which these three conditions are met.[16] In some cases such a computational support can lead to new important results. Indeed, this was exactly the case of computer-assisted proofs (CAPs). The most famous example is probably the proof of the four-color theorem (4CT).[17] Its computer-assisted proof was presented in [Appel and Haken, 1977; Appel et al., 1997]. As the proof required the use of a computer (in its original form, they needed ca. 1200 hours), several methodological, conceptual and philosophical questions concerning the proof and the epistemological status of 4CT arose.[18] The fundamental question is whether this CAP REALLY is a mathematical proof, i.e. whether the four color HYPOTHESIS turned into a mathematical THEOREM.

The problem becomes more intricate in the case of QAP's. We can even imagine, that one of the big mathematical open problems (say, Riemann's hypothesis or Goldbach's conjecture) is proved with the help of a QAP, which would surely be sensational. But even if α is just an ordinary mathematical problem, the philosophical status of α remains to be examined.

3. Are there empirical proofs?

The received view considers mathematical activity to be purely intellectual. The mathematician is idealized as a purely rational subject, who begins with some self-evident truths as a starting point, and proceeds

[16] Admittedly, the possibility of the existence of such a physical process is debatable. Aaronson discusses the "NP Hardness assumption": the thesis, that NP-complete problems of intractable in our physical universe, and speculates, that in future it might be considered a fundamental principle (like the second law of thermodynamics) [Aaronson, 2005, p. 17]. Aaronson's claims directly contradict the speculations concerning the possibility of quick natural computation, in particular concerning hypercomputational procedures solving mathematical problems [cf. Andréka et al., 2009; Németi and Dávid, 2006; Wójtowicz, 2015].

[17] Another interesting example is the proof of Kepler's conjecture, which claims that the "ordinary" packing of spheres is best [Hales, 2005].

[18] The first articles concerning 4 CT are: [Detlefsen and Luker, 1980; Krakowski, 1980; Levin, 1981; Swart, 1980; Teller, 1980; Tymoczko, 1979], followed by a lively discussion.

through a sequence of logically connected intellectual acts to arrive at the conclusion of the argument. Of course, in this process, understanding of mathematical concepts is involved. Speaking metaphorically, we need some "insight" into the mathematical realm (however we conceive it), and mathematical proofs reveal the interplay of mathematical ideas. In the process of proving theorems there are some "mechanical fragments", but — on the whole — it amounts to grasping inferential connections between the premises of the mathematical argument and its conclusions (and not to checking, whether some strings of symbols conform to formal rules).

From this point of view, already ordinary CAPs might be viewed as problematic. The following issues are often mentioned in this context: (1) our lack of understanding of the proof; (2) the explanatory value of these proofs; (3) the role of empirical elements. An important feature is the lack of (full) control over what is going on during the proof. We have to rely on the algorithms and the hardware, and believe, that the computer performs exactly the task it was designed to perform. There is an empirical ingredient in the proof, which makes it difficult to reconcile it with the traditional vision of mathematics as an *a priori* science, whose claims are justified by conceptual analysis. What — ultimately — is the epistemological warrant for 4CT? In the context of (possible) QAPs, these questions become much more dramatic, because the strange and counterintuitive laws of the quantum world are involved here.

A general objection might be formulated, which *prima facie* seems reasonable: it is ALWAYS necessary to rely on some laws of physics — so does it really matter, whether the physical theory in question is classical mechanics, quantum mechanics, general relativity, thermodynamics or electromagnetism? Even if we built a steam-powered mechanical computing device (say, an universal Turing machine...), we would have to rely on the laws of thermodynamics and classical mechanics in order to trust it. Even if we use paper and pencil, we make some empirical assumptions — e.g. we assume, that the symbols do not change during the proof.[19] The same applies to ordinary computers — but we accept them as legitimate devices. From this point of view, a (hypothetical) quantum computer would not differ in principle from the ordinary one

[19] Of course, they change: ink evaporates, certain chemical processes take place, the shape of the piece of paper changes etc. But these changes are not essential, and our idealization is justified.

(and from the steam-powered calculating device). So, finally — no new interesting philosophical questions arise.

This objection is — in my opinion — seriously flawed. The differences between classical computers and quantum computers are much deeper, as we have no access during the quantum process to the temporary state of the computation. A classical computer performs the computations we could also perform. So in principle we could proceed with the proof in the traditional way. We can stop the computation at any stage, examine the temporary state and continue with the process — so in particular, we could analyze fragments of the computation, and reconstruct an ordinary proof (so the computer would serve as heuristic device). We could imagine a group of 1000 mathematicians examining a computer assisted proof, but in the case of QAPs, the situation is radically different. A quantum proof is a kind of black box — as there are no knowable intermediate states: regardless of the size of the quantum circuit, we only have access to the final outcome (through measurement). And quantum phenomena, like entanglement and interference are built into the procedure.

From the epistemological point of view, the "minimal item" is the experiment conceived as a whole. QAPs are not even partially verifiable or acceptable in any way — we have to accept them as certain wholes, as "atomic procedures". A part (usually a significant part) of the information, which is present during the quantum computation, is definitely lost in the final step and cannot be retrieved in any way. The quantum system does not "remember" which of the computational paths involved (simulated in the experiment) corresponds to the successful proof. In a sense, we are presented with a kind of empirical oracle, which can answer some questions, leading to the acceptance of a sentence α. Maybe it can even answer questions of the kind "Does T formally prove α within n steps?" — but the answers can only be 'YES' and 'NO' (or perhaps: 'YES' and 'TRY A LARGER n') — without giving any hints concerning the structure and general ideas of the proof.[20]

[20] In [Rav, 1999] an example of PYTHIAGORA, a super-quick computer answering all possible mathematical questions is discussed. Rav claims, that this would be rather destructive for mathematics: "A universal decision method would have dealt a death blow to mathematics, for we would cease having ideas and candidates for conjectures" [Rav, 1999, p. 6]. Tymoczko [1979] discusses Simon, a hypothetical mathematical genius. After becoming an outstanding and highly respected expert mathematician, Simon claims some theorems to be proved, but refuses to inform us about the details of his proofs, as he claims them to be too complicated for us.

4. Quasi-empiricical account of QAPs

Some mathematicians have still an uneasy feeling about CAPs, but new proofs of this kind are presented, are accepted as legitimate — and probably this will lead to a permanent change in mathematical practice and standards. And if quantum computers existed, surely they would be widely used, also to settle mathematical questions — even if some (perhaps many?) mathematicians would have doubts about them. It would be better to know, that e.g. Riemann's hypothesis is true (even without learning the details of the proof and being forced to rely on the quantum device) — then to remain ignorant on this subject (I shortly comment on the case of Riemann's hypothesis in footnote 33). "Quantum-assisted knowledge is better than classical ignorance" — one might say. But even if there were QAPs available, and mathematical practice changed, this would not settle the philosophical issue of the status of this kind of knowledge.

The situation is particularly problematic for the mathematical realists, who claim, that mathematical statement have truth values. They should decide, whether a sentence α demonstrated via a quantum experiment (without exhibiting any details of this proof whatsoever) is a mathematical truth. And if it is — what is the truthmaker for this sentence, the warrant of its truth?

I will argue, that the best account can be given within the quasi-empiricist stance, where a natural source of inspiration is Quine's position. It is well known, and has been discussed extensively, so I will only briefly recall some important points. According to Quine, our knowledge forms a web of beliefs, where the ultimate criterion is the given data (i.e., the sensory stimulation). This seamless web should be viewed as a logically coherent whole, even if — for psychological reasons — we might tend to differentiate between its fragments. But: "our statements about the external world face the tribunal of sense experience not individually but only as a corporate body" [Quine, 1953]. Quine's famous indispensability argument for mathematical realism rests on two premises: (1) we are committed to the existence of those entities, which are indispensable to our best scientific theories; (2) mathematical objects are such entities.[21]

[21] Of course, the special role of proof as a method of argumentation is not questioned. But metascientific analyses concerning the role of mathematics in science are necessary in order to justify claims concerning the truth of mathematical claims, and the ontological status of mathematical theories.

It is the role in science, which is the warrant of truth of mathematical claims — not any kind of mathematical intuition or some purely philosophically motivated metaphysical claims.

If we accept this way of addressing ontological issues and identifying ontological commitments of theories, we get to the realistic account of mathematics in a very natural way. The criterion of existence is given *via* logical analysis and allows us to identify the ontology of scientific theories.[22]

4.1. The enhanced indispensability argument

Quine's ontological stance faces some problems, and it has been questioned.[23] In the last years, however, a modified version of the argument has been presented — in the form of the Enhanced Indispensability Argument, and the debate has gained new impetus.[24]

The modified version stresses the explanatory role played by mathematics in science and in particular assumes the existence of entities presupposed by our best explanations. If mathematics plays a genuine and indispensable EXPLANATORY role in science, we have a stronger argument for mathematical realism. The problem of the explanatory power of mathematics in science becomes therefore crucial for the debate. The main question is whether mathematics *per se* can provide an explanation of physical facts, i.e. whether there is some explanatory power inherent to mathematics. Many authors claim, that this is ineed the case, and treat some scientific explanations as non-causal — because mathematical theorems are present in the *explanans*. Broadly speaking, the general claim is that it is NOT the laws of physics, but rather the truths of mathematics, which explain the phenomena. One of the much discussed examples is Baker's example of the periodical life-cycle of cicadas (13 and 17 years).

[22] "The common man's ontology is vague and untidy in two ways. It takes in many purported objects that are vaguely or inadequately defined. But also, what is more significant, it is vague in its scope; we cannot even tell in general which of these vague things to ascribe to a man's ontology at all, which things to count him as assuming" [Quine, 1981, p. 9].

[23] Examples of "classical" antirealist accounts are: Field's [1980] nominalization strategy, Hellman's [1989] modal structuralism, Chihara's [1990] modalism or Balaguer's [1998] fictionalist account (followed by a vast number of papers and monographs).

[24] E.g. Colyvan [1999, 2001] stresses the importance of epistemic virtues for the discussion.

The fact, that these cycles are prime numbers is considered by some authors to have a distinctive mathematical explanation (due to certain properties of prime numbers expressed in a series of lemmas). Similarly, the Borsuk-Ulam theorem in claimed to provide an explanation of some meteorological phenomena [cf. Baker, 2005, 2009; Baker and Colyvan, 2011] Another interesting phenomenon is the regular, hexagonal structure of the honeycombs, and here again a mathematical explanation is proposed — it is the honeycomb conjecture [Hales, 2000]: hexagonal tiling is optimal with respect to the total perimeter length (so bees use as little wax as possible).[25] The topic is much discussed, and the problem, what constitutes the special character of mathematical explanations in science is acute.[26] We might dismiss EIA or claim, that mathematics "an sich" has no explanatory powers. But if we accept EIA (even as a working hypothesis), we have to address the question, what exactly warrants the explanatory virtues of the theorem α in question. Generally, there are two possible answers: (1) it is the theorem *per se*, independent of its proof; (2) the theorem AND its proof (and — so to say — the conceptual environment).

These two distinct points of view lead to quite different conclusions concerning the possible explanatory role of "quantumly demonstrated theorems".

Ad 1. If we claim, that it is the very theorem itself, which provides the explanatory power, (regardless of how it was proved), we need not bother about the details of the proof, the ideas and concepts involved, the necessary technical prerequisites etc. Even if we knew α (explaining the

[25] There are much more examples, to mention just a few: Lipton [2004] analyses a geometric explanation of a simple physical process (the distribution of rigid sticks in the air). Bangu [2013] considers the law of large numbers as explaining the outcomes of a simple game. Lyon and Colyvan [2008] examine the explanatory virtues of the use of phase spaces in physics. Baron [2014] examines the behavior of predators, where a mathematical explanation is offered by theorems on stochastic processes.

[26] Lange [2013] discusses the problem in details. Some authors claim, that mathematics imposes a kind of modal constraints on the world, or consider mathematical facts as a kind of "programming properties" [see, e.g., Lyon, 2012]. Due to some antirealistic accounts, mathematics has only a kind of representational function [see, e.g., Daly and Langford, 2009 for the "indexing account"]. Liggins [2014] discusses the doctrine of "abstract expressivism", i.e. the thesis that mathematics serves only as a tool of saying things about the concrete world, which otherwise would be difficult (or impossible) to say [cf. Yablo, 2005, 2012]. The literature on the subject is vast, and only few examples can be mentioned here.

behavior of a physical system S) from a (reliable) oracle — this would be satisfactory. From this point of view, to understand, why nobody has ever passed the famous bridges in Königsberg (crossing every bridge exactly once) it is enough to know Euler's theorem — and we do not need to examine the proof.[27]

Ad 2. I consider (1) to be an oversimplified point of view. The proof of the theorem is crucial also for the explanation — it reveals the necessary assumptions, the concepts involved (which might be exhibited only by the proof), the role the theorem plays in the conceptual structure etc.[28] In particular, the proof might exhibit not only the mathematical assumptions and techniques (this is obvious), but also allow to identify the necessary assumptions concerning the relationship between the physical reality and the mathematics involved (bridge laws). In particular, we have to get a deeper understanding of the meaning of the theorem, its role in the overall conceptual (mathematical) system, so we need to know its proof.[29]

This poses a problem for the adherent of the EIA in the context of QAPs. If the explanatory power of mathematics is conveyed by the ideas and concepts (exploited in the proof), then the story becomes complicated, as we do not know the proof of the theorem α demonstrated by a quantum computer. The theory using α can happen to be empirically adequate, can serve us well as a predictive tool, but we do not understand, why it works, and what features of the empirical situation made it work.[30]

[27] "Given that the proof justifies the theorem, we are then entitled to make use of the theorem, e.g., in applications to physical facts. [...] The role of the proof of that theorem is to justify the acceptance of that theorem. In neither case is mathematics being taken to explain facts in the concrete world." [Daly and Langford, 2009, p. 648]

[28] According to Baker and Colyvan [2011, p. 327]: "intra-mathematical explanations may spill over into the empirical realm. The idea is that if, say, the Borsuk-Ulam theorem is explained by its proof and the antipodal weather patterns are explained by the Borsuk-Ulam theorem, it would seem that the proof of the theorem is at least part of the explanation of the antipodal weather patterns."

[29] The explanatoriness of a proof within mathematics is a different problem, and will not be discussed here. Another important problem is the more general question of the interactions between mathematics and physics — and what exactly is meant by the phrase "explaining the phenomena".

[30] Consider chess- or go-playing programs — they are already better that humans. If human chess or go masters play their games, they can explain the meaning of the moves (using technical terms, figurative language or even metaphors to enhance understanding). But the computer will win all games and give precise answers to

4.2. "Quantum theorems" as empirical data

The standard scheme of using mathematics as an explanatory tool is (more or less) as follows:

1. We are presented with a physical (biological, chemical etc.) phenomenon S.
2. We learn, that there is a theorem α (of standard mathematics M).
3. We see, that α (including its proof) helps us to explain the phenomenon S.
4. (And — being adherents of EIA — we consider this fact to be an important argument in the discussion).

But what if α is proved via a QAP? A QAP certainly does not offer any understanding or explanation, attributed usually to traditional proofs. The only information we could get from a QAP is the fact, that a sentence α can be demonstrated, and nothing more. An "oracle proof" would not preserve the explanatory virtues of the theorem α, being a part of the mathematical theory. This would weaken the pro-realistic argument (as one of the premises of EIA would lose its fundaments).

To overcome this difficulty, I propose to view these new results (i.e. quantumly demonstrated propositions) not as full-fledged mathematical theorems, but rather as available empirical data, which have to be explained. So they would become rather a part of the *explanandum*, not the *explanans*.

Let M be standard mathematics[31], and α a QAP-proved theorem. Accepting $M+\alpha$ better fits and explains the empirical data (including the quantum experiment yielding α) than other choices. Even if we refrain from accepting the quantum process as a legitimate mathematical proof, and even if we share the doubts resulting from the "explanatoriness postulate" (on which EIA rests), we are entitled to include α into our system of beliefs. This rests on the fact, that we equipped the physical experiment (performed for example on a system of photons flying around) with a semantics: we interpret the results of the experiment as

questions like "given a position P on the chess/go board — who is more likely to win?". But — ultimately — it will offer explanations of the form: "I played this move because my evaluating function judged it to be the best one." So as a predictive device the chess computer is clearly better, but it cannot explain the underlying "deep reasons".

[31] This is a vague notion — but it is obvious, that M is not one of the formal theories, but rather "the subject mathematicians are working on and physicists make use of". It is clear enough for our purposes.

information about the provability of α.[32] Of course, in this case $M+\alpha$ fits the empirical data well, and is a very natural rounding out of our knowledge. But its acceptance does not follow from the fact, that α is MATHEMATICALLY reliable (e.g. completes a theory in a mathematically natural way, fits the mathematical intuitions of the experts etc.), but rather from the fact, that $M+\alpha$ proves to be a good tool in physics.[33]

To give a better feeling for this way of viewing "quantumly proved theorems", consider the case, where the status of a mathematical claim α is unknown (i.e. we have no proof and do not even know, whether it is consistent with M). It might be the case, that $M+\alpha$ suits the purposes of physics (it provides better methods of describing and explaining certain phenomena, it has a better predictive power etc.) — but as we do not know, whether it is consistent, we have an uneasy feeling about it.[34] Now, if we prove, that $M+\alpha$ is (relatively) consistent, the methodological obstacle is overcome. But what is the MATHEMATICAL status of α? We haven't proved α (perhaps it is even independent from M, so unprovable). Should we accept α as a new MATHEMATICAL axiom only because it suits the purposes of physics?

Consider now a different situation, where we use a (relatively) consistent theory $M+\alpha$ in physics, and — later on — α happens to be proved by a QAP. This would give us perhaps an even stronger belief in the consistency of $M+\alpha$ (than just having the "old fashioned" metamathematical proof, e.g. by some exotic forcing or model-theoretic arguments). Consider the following two situations:

[32] We have in particular to assume some bridge laws concerning the empirical situation with the mathematical theories.

[33] Riemann's hypothesis is one the the great unsolved mathematical problems. But it also exhibits some connections with physics: indeed, Berry and Keating [1999] formulated a hypothesis concerning the existence of a certain quantum system whose energy levels exactly correspond to the nontrivial zeros of the Riemann zeta function. In [Bender et al., 2017] such a quantum system is defined (but it should be noted, that it is not obvious, whether this quantum system has a physical meaning, is realistic, not too "weird" etc.). We might therefore speculate, that quantum mechanics could have a contribution to solving Riemann's hypothesis. To be exact: we would accept Riemann's hypothesis because of empirical arguments — and not because a purely mathematical argumentation. I think that if quantum physics (perhaps even quantum computation) could contribute to the solution of Riemann's hypothesis in any way, this would not happen by a metamathematically interpreted computation, but rather by a direct "check".

[34] We might perhaps consider using inconsistent theories, but I do not discuss the problem here [cf. Colyvan, 2008].

(i) We know, that $M+\alpha$ is relatively consistent (but do not know, whether α is provable within M) — and it fits the empirical data well.
(ii) We have a QAP of α.

Is there — from the point of view of the EIA-realist — an important difference between (i) and (ii)? Anyway, we have already decided to make use of $M+\alpha$ as a tool in science, and — being EIA-realists — we included $M+\alpha$ into our system of beliefs (in particular, accepting its ontological commitments). $M+\alpha$ was accepted before the QAP of α, and its provability within M becomes a question of the internal logical structure of $M+\alpha$ — not the question of accepting α.

I claim, that this way of viewing quantumly proved theorems gives a better philosophical explanation of the status of $M+\alpha$ from the point of view of mathematical realism based on the indispensability argument. In particular, it solves the problem of the lack of explanatoriness, which presents a difficulty for the EIA-realist. Our system of beliefs (including mathematical beliefs) has to fit the data, and these data include in particular the outcomes of the experiments, including (quantum) computer simulations. Ultimately — from the point of view of EIA-realism — what matters is the fact, that mathematical sentences gain the status of truths *via* the empirical theory they are part of — not via conceptual, *a priori* insights.[35]

5. Concluding remarks

Quantum computation is a quickly developing area. However, there are no quantum computers, and there are also theoretical limitations to quantum algorithms. It might well happen, that Shor's factoring algorithm will remain the most spectacular theoretical achievement for a long time — and also that there quantum computers of a practical importance will never be build.[36] Nevertheless, quantum computation theory is philosophically intriguing, also for philosophy of mathematics.

[35] This point of view does not dispute the status of classical proof. But according to this point of view, it is the applicability which elevates the mathematical theorems to the status of truths (to paraphrase Frege's famous phrase).

[36] So far, Shor's algorithm is the only quantum algorithm, for which a quantum computer is significantly faster than any KNOWN classical one. This is situation might be called embarrassing — and possibly connected with the fact, that it is still not clear, what exactly is the deep reason for the efficiency of the quantum algorithms.

The possibility of "oracle-like QAPs" poses some difficulties for the pro-realistic EIA. I have argued, that they are best explained within the holistic account, where traditional theorems, computer-assisted theorems, "quantum theorems" etc. are all integrated within one coherent system of knowledge.

There has been an extensive discussion concerning the role of empirical procedures in mathematics [e.g. Baker, 2008] — and the hypothetical QAPs would constitute an important theoretical and philosophical novelty. I hope, that the thought experiment presented here contributes to the discussion concerning the empirical aspects of mathematics and the interplay between physical and mathematical knowledge.

Acknowledgment. The preparation of this paper was supported by National Science Center, Poland, grant number: 2016/21/B/HS1/01955.

References

Aaronson, S., 2005, "NP-complete problems and physical reality", *Electronic Colloquium on Computational Complexity*, Report no. 26. arXiv:quant-ph/0502072v2.

Aaronson, S., 2013, *Quantum Computing Since Democritus*, Cambridge University Press, Cambridge, New York. DOI: 10.1017/CBO9780511979309

Andréka, H., I. Németi and P. Németi, 2009, "General relativistic hypercomputing and foundation of mathematics", *Natural Computing* 8 (3): 499–516. DOI: 10.1007/s11047-009-9114-3

Appel, K., and W. Haken, 1977, "Every planar map is four colorable. Part I: discharging", *Illinois Journal of Mathematics* 21: 429–490.

Appel, K., W. Haken and J. Koch, 1977, "Every planar map is four colorable. Part II: reducibility", *Illinois Journal of Mathematics* 21: 491–567.

Baker, A., 2005, "Are there genuine mathematical explanations of physical phenomena?", *Mind* 114 (454): 223–238. DOI: 10.1093/mind/fzi223

Baker, A., 2008, "Experimental mathematics", *Erkenntnis* 68: 331–344. DOI: 10.1007/s10670-008-9109-y

Baker, A., 2009, "Mathematical explanation in science", *British Journal for the Philosophy of Science* 60 (3): 611–633. DOI: 10.1093/bjps/axp025

Baker, A., and A. Colyvan, 2011, "Indexing and mathematical explanation", *Philosophia Mathematica* 19: 232–224. DOI: 10.1093/philmat/nkr026

Balaguer, M., 1998, *Platonism and Anti-Platonism in Mathematics*, Oxford University Press, New York, Oxford.

Bangu, S., 2013, "Indispensability and explanation", *British Journal for the Philosophy of Science* 64 (2): 255–277. DOI: 10.1093/bjps/axs026

Baron, S., 2014, "Optimisation and mathematical explanation: doing the Lévy Walk", *Synthese* 191: 459-479. DOI: 10.1007/s11229-013-0284-2

Bender, C. M., D. C. Brody and M. P. Müller, 2017, "Hamiltonian for the zeros of the Riemann zeta function", *Physical Review Letters* 118, 130201. DOI: 10.1103/PhysRevLett.118.130201 (available as: https://journals.aps.org/prl/pdf/10.1103/PhysRevLett.118.130201)

Bennett, C., E. Bernstein, G. Brassard and U. Vazirani, 1997, "Strengths and weaknesses of quantum computing" , *SIAM J. Comput.* 26 (5): 1510–1523; arXiv:quant-ph/9701001. DOI: 10.1137/S0097539796300933

Berry, M. V., and J. P. Keating, 1999, "$H = xp$ and the Riemann zeros", pages 355–367 in J. P. Keating, D. E. Khmelnitski and I. V. Lerner (eds.), *Supersymmetry and Trace Formulae: Chaos and Disorder*, Kluwer Academic/Plenum, New York. DOI: 10.1007/978-1-4615-4875-1_19

Colyvan, M., 1999, "Confirmation theory and indispensability", *Philosophical Studies* 96: 1–19.

Colyvan, M., 2001, *The Indispensability of Mathematics*, New York, Oxford University Press. DOI: 10.1093/019513754X.001.0001

Colyvan, M., 2008, "The ontological commitments of inconsistent theories", *Philosophical Studies* 141: 115–123. DOI: 10.1007/s11098-008-9266-5

Chihara, C., 1990, *Constructibility and Mathematical Existence*, Clarendon Press, Oxford. DOI: 10.1093/0198239750.001.0001

Daly, C., and S. Langford, 2009, "Mathematical explanation and indispensability arguments", *The Philosophical Quarterly* 59: 641–658. DOI: 10.1111/j.1467-9213.2008.601.x

Detlefsen, M., and M. Luker, 1980, "The four color-problem and mathematical proof'", *Journal of Philosophy* 77: 803–820. DOI: 10.1111/10.2307/2025806

Field, H., 1980, *Science Without Numbers*, Basil Blackwell, Oxford. DOI: 10.1093/acprof:oso/9780198777915.001.0001

Feynman, R. P., 1982, "Simulating physics with computers", *International Journal of Theoretical Physics* 21 (6/7): 467–488. DOI: 10.1007/BF02650179

Hales, T. C., 2000, "Cannonballs and honeycombs", *Notices of the American Mathematical Society* 47 (4): 440–449.

Hales, T. C., 2005, "A proof of the Kepler conjecture", *Annals of Mathematics. Second Series* 162 (3): 1065–1185. DOI: 10.4007/annals.2005.162.1065

Harrow, A., A. Hassidim and S. Lloyd, 2009, "Quantum algorithm for linear systems of equations", *Phys. Rev. Lett.* 15 (103): 150502, arXiv:0811.3171. DOI: 10.1103/PhysRevLett.103.150502

Hellman, G., 1989, *Mathematics Without Numbers*, Clarendon Press, Oxford. DOI: 10.1093/0198240341.001.0001

Krakowski, I., 1980, "The four-color problem reconsidered", *Philosophical Studies* 38: 91–96. DOI: 10.1007/BF00354531

Lange, M., 2013, "What makes a scientific explanation distinctively mathematical?", *British Journal for the Philosophy of Science* 64 (3): 485–511. DOI: 10.1093/bjps/axs012

Levin, M. A., 1981, "On Tymoczko's argument for mathematical empiricism", *Philosophical Studies* 39: 79–86. DOI: 10.1007/BF00354815

Liggins, D., 2014, "Abstract expressionism and the communication problem", *British Journal for the Philosophy of Science* 65: 599-620.

Lipton, P., 2004, "What good is an explanation", pages 1-21 in J. Cornwell (ed.), *Explanations. Styles of Explanation in Science*, Oxford: Oxford University Press. DOI: 10.1007/978-94-015-9731-9_2

Lyon, A., 2012, "Mathematical explanations of empirical facts, and mathematical realism", *Australasian Journal of Philosophy* 90 (3): 559–578. DOI: 10.1080/00048402.2011.596216

Lyon, A., and M. Colyvan, 2008, "The explanatory power of phase spaces", *Philosophia Mathematica* 16 (2): 227–243. DOI: 10.1093/philmat/nkm025

Montanaro, A., 2015, "Quantum algorithms: an overview", https://www.nature.com/articles/npjqi201523 (also: arXiv:1511.04206v2). DOI: 10.1038/npjqi.2015.23

Németi, I., and G. Dávid, 2006, "Relativistic computers and the Turing barrier", *Journal of Applied Mathematics and Computation* 178 (1): 118–142. DOI: 10.1016/j.amc.2005.09.075

Nielsen, M. A., and I. L. Chuang, 2000, *Quantum Computation and Quantum Information*, Cambridge University Press. DOI: 10.1017/CBO9780511976667

Quine, W. V. O., 1953, "Two dogmas of empiricism", pages 20–46 in *From a Logical Point of View*, Harvard University Press, Cambridge, Mass.

Quine, W. V. O., 1981, "Things and their place in theories", pages 1–23 in *Theories and Things*, The Belknap Press of Harvard University Press, Cambridge, Mass.

Rav, Y., 1999, "Why do we prove theorems?", *Philosophia Mathematica* 7: 5–41. DOI: 10.1093/philmat/7.1.5

Shor, P., 1994, "Algorithms for quantum computation: Discrete logarithms and factoring", pages 124–134 in *Proc. 35th Annual Symposium on Foundations of Computer Science*, IEEE. DOI: 10.1109/SFCS.1994.365700

Swart, E. R., 1980, "The philosophical implications of the four-color problem", *American Mathematical Monthly* 87: 697–707. DOI: 10.2307/2321855

Teller, P., 1980, "Computer proof"', *The Journal of Philosophy* 77: 797–803. DOI: 10.2307/2025805

Tymoczko, T., 1979, "The four-color problem and its philosophical significance", *The Journal of Philosophy* 76 (2): 57–83. DOI: 10.2307/2025976

Yablo, S., 2005, "The myth of the seven", pages 90–115 in M. E. Kalderon (ed.), *Fictionalism in Metaphysics*, Oxford, Oxford University Press. DOI: 10.1093/acprof:oso/9780199266487.003.0010

Yablo, S., 2012, "Explanation, extrapolation, and existence", *Mind* 121 (484): 1007–1029. DOI: 10.1093/mind/fzs120

Wójtowicz, K., 2009, "Theory of quantum computation and philosophy of mathematics. Part I", *Logic and Logical Philosophy* 18 (3–4): 313–332. DOI: 10.12775/LLP.2009.016

Wójtowicz, K., 2015, "Could empirical facts become mathematical truths?", pages 213–230 in J. Ladyman, S. Presnell, G. McCabe, M. Eckstein and S. J. Szybka (eds.), *Road to Reality with Roger Penrose*, Copernicus Center Press, Kraków.

Krzysztof Wójtowicz
Institute of Philosophy
Warsaw University, Poland
kwojtowi@uw.edu.pl