Available online at www.sciencedirect.com
SCIENCE DIRECT®

Theoretical Computer Science 344 (2005) 134–207

Theoretical Computer Science

www.elsevier.com/locate/tcs

A theory of computation based on quantum logic (I)

Mingsheng Ying*,[1]

State Key Laboratory of Intelligent Technology and Systems, Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China

Received 3 May 2004; received in revised form 4 April 2005; accepted 4 April 2005

Communicated by J. Watrous

Abstract

The (meta)logic underlying classical theory of computation is Boolean (two-valued) logic. Quantum logic was proposed by Birkhoff and von Neumann as a logic of quantum mechanics more than 60 years ago. It is currently understood as a logic whose truth values are taken from an orthomodular lattice. The major difference between Boolean logic and quantum logic is that the latter does not enjoy distributivity in general. The rapid development of quantum computation in recent years stimulates us to establish a theory of computation based on quantum logic. The present paper is the first step toward such a new theory and it focuses on the simplest models of computation, namely finite automata. We introduce the notion of orthomodular lattice-valued (quantum) automaton. Various properties of automata are carefully reexamined in the framework of quantum logic by employing an approach of semantic analysis. We define the class of regular languages accepted by orthomodular lattice-valued automata. The acceptance abilities of orthomodular lattice-valued nondeterministic automata and their various modifications (such as deterministic automata and automata with ε-moves) are compared. The closure properties of orthomodular lattice-valued regular languages are derived. The Kleene theorem about equivalence of regular expressions and finite automata is generalized into quantum logic. We also present a pumping lemma for orthomodular lattice-valued regular languages. It is found that the universal validity of many properties (for example, the Kleene theorem, the equivalence of deterministic and nondeterministic automata) of automata depend heavily upon the distributivity of the underlying logic. This indicates that these properties does not universally hold

*Tel.: 86 10 62771569; fax: 86 10 62771138.
E-mail address: yingmsh@tsinghua.edu.cn

[1]This work was partly supported by the National Foundation of Natural Sciences of China (Grant No: 60321002, 60496321, 60273003) and the Key Grant Project of Chinese Ministry of Education (Grant No: 10403).

doi:10.1016/j.tcs.2005.04.001

in the realm of quantum logic. On the other hand, we show that a local validity of them can be recovered by imposing a certain commutativity to the (atomic) statements about the automata under consideration. This reveals an essential difference between the classical theory of computation and the computation theory based on quantum logic.

Keywords: Quantum logic; Orthomodular lattice; Algebraic semantics; Finite automata; Regular languages; Quantum computation

1. Introduction

It is well-known that an axiomatization of a mathematical theory consists of a system of fundamental notions as well as a set of axioms about these notions. The mathematical theory is then the set of theorems which can be derived from the axioms. Obviously, one needs a certain logic to provide tools for reasoning in the derivation of these theorems from the axioms. As pointed out by Heyting [21, p. 5], in elementary axiomatics logic was used in an unanalyzed form. Afterwards, in the studies for foundations of mathematics beginning in the early of twentieth century, it had been realized that a major part of mathematics has to exploit the full power of classical (Boolean) logic [19], the strongest one in the family of existing logics. For example, group theory is based on first-order logic, and point-set topology is built on a fragment of second-order logic. However, a few mathematicians, including the big names L.E.J. Brouwer, H. Poincare, L. Kronecker and H. Weyl, took some kind of constructive position which is in more or less explicit opposition to certain forms of mathematical reasoning used by the majority of the mathematical community. Some of them even endeavored to establish so-called constructive mathematics, the part of mathematics that could be rebuilt on constructivist principles. The logic employed in the development of constructive mathematics is intuitionistic logic [41] which is truly weaker than classical logic.

Since many logics different from classical logic and intuitionistic logic have been invented in the last century, one may naturally ask the question whether we are able to establish some mathematical theories based on other nonclassical logics besides intuitionistic logic. Indeed, as early as the first nonclassical logics appeared, the possibility of building mathematics upon them was conceived. As mentioned by Mostowski [31], J. Lukasiewicz hoped that there would be some nonclassical logics which can be properly used in mathematics as non-Euclidean geometry does. In 1952, Rosser and Turquette [36, p. 109] proposed a similar and even more explicit idea:

> The fact that it is thus possible to generalize the ordinary two-valued logic so as not only to cover the case of many-valued statement calculi, but of many-valued quantification theory as well, naturally suggests the possibility of further extending our treatment of many-valued logic to cover the case of many-valued sets, equality, numbers, etc. Since we now have a general theory of many-valued predicate calculi, there is little doubt about the possibility of successfully developing such extended many-valued theories. …we shall consider their careful study one of the major unsolved problems of many-valued logic.