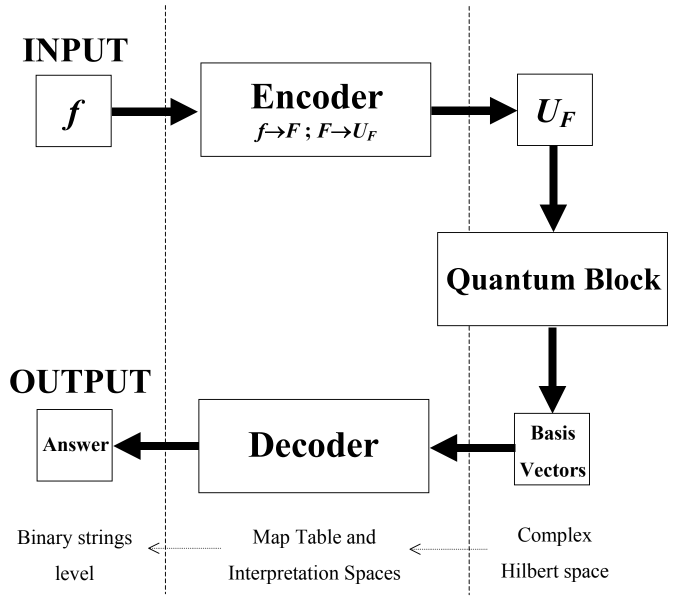
Serguei V. Ulyanov –Serguei A. Panfilov

Ludmila Litvintseva – Serguei S. Ulyanov

Quantum Information and Quantum Computational Intelligence:

Dynamic Evolution of Information Flow and Intelligence of Quantum Algorithms



Under the Scientific Supervision of:

Masahito Suzuki

Giovanni Degli Antoni

Kazuki Takahashi

Yamaha Motor Europe N. V. R&D Office,
Università degli Studi di Milano – Polo Didattico e di Ricerca di Crema

Via Bramante, 65 – 26013 CREMA (CR), Italy – 2005

Acknowledgements

The authors would like to acknowledge Dr. M. Suzuki, Dr. K. Takahashi and Dr. T. Hagiwara (Yamaha Motor Co., Ltd.) for general support and supervision, and Professor G. Degli Antoni (Milan University) for fruitful discussion about general ideas and possible applications of quantum computing.

One of the authors (S.V.U.) would also like to express his gratitude to his "classical and non-standard logic", "probabilistic and information-theoretical", "relativistic", "thermodynamics" and "quantum" friends, especially; Professors L. Zadeh, R. Aliev, M. Jamshidi, A.N. Melikhov, D. Mundici, R.L. Stratonovich, A.N. Kolmogorov, M.S. Pinsker, R.L. Dobrushin, V.A. Fock, B.N. Petrov, I.I. Goldenblat, V.P. Belavkin, L.B. Levitin, Y.I. Samoilenko, P. Shor, P. Knight, A.S. Holevo, O. Hirota and C. Bennett for kind support and discussions.

CONTENTS

CONTENTS **3**

PREFACE **5**

CHAPTER 1: BACKGROUND OF QUANTUM COMPUTATION AND QUANTUM ALGORITHMS **8**

1.1. INTRODUCTION: COMPUTATIONAL AND INFORMATIONAL COMPLEXITY OF QA SIMULATION 9
1.1.1. Quantum algorithm simulation and design techniques. *9*
1.2. SPATIO-TEMPORAL COMPLEXITY OF QA SIMULATION BASED ON THE FULL MATRIX APPROACH 11
1.2.1. Spatio-temporal complexity of Grover's quantum algorithm. *11*
1.2.2. Information analysis of quantum complexity of QAs: Quantum Query Tree Complexity. *18*
1.2.3. Kolmogorov complexity of quantum query algorithms. *21*

CHAPTER 2: CLASSIFICATION AND GENERAL STRUCTURE OF QA GATES **24**

2.1. CLASSIFICATION AND GENERAL STRUCTURE OF QA'S 24
2.1.1. On the classification of QA's: Design strategies of classical algorithms and quantum computation. *24*
2.1.2. General structure of QA's. *26*
2.1.3. The full basis and universal gates with control parameters for quantum computing *29*
2.1.4. Computational conditions of approximate accuracy for classical efficient simulation of bases quantum circuits. *33*
2.1.5. Conservative logic and universal gates. *35*
2.1.6. Universal gates for quantum algorithms and fault–tolerant computations. *37*
2.1.7. Fault-tolerant universal gates. *39*
2.1.8. Mutually unbiased computational bases. *40*
2.1.9. Main QAG's and main quantum operators. *47*
2.2. INFORMATION ANALYSIS AXIOMS OF QAG-DYNAMIC EVOLUTION 48
2.2.1. Information (communication) capacity of quantum computing and axioms of information analysis of dynamic evolution of QA's quantum gates. *49*
2.2.2. Information intelligent measure of QA's (principle 5). *51*
2.3. CLASSICAL EFFICIENT SIMULATION OF QUANTUM FORMULAS BY BOOLEAN CIRCUITS: COMPUTATIONAL AND DESIGN COMPLEXITY 51
2.3.1. Interrelations between Quantum Turing Machine and QA's definitions. *51*
2.3.2. Classical efficient simulation of quantum formulas by Boolean circuits: Computational and design complexity. *53*
2.3.3. Equivalent definition for quantum formulas. *58*
2.3.4. Quantum formulas vs. Boolean circuits. *61*
2.3.5. Quantum query algorithms and computational complexity. *63*

CHAPTER 3: SIMULATION OF QA'S BY CLASSICAL COMPUTATION **69**

3.1. QUANTUM COMPUTATION ON CLASSICAL COMPUTER 69
3.1.1. The role of entanglement in computational process. *71*
3.2. GENERALIZED DESIGN METHOD OF QA'S GATES 83
3.2.1. The generic circuit. *84*
3.3. UNIVERSALITY OF ENTANGLEMENT AND QUANTUM COMPUTATION COMPLEXITY USING EFFICIENT CLASSICAL SIMULATION 89

CHAPTER 4: INFORMATION ANALYSIS AND INTELLIGENT MEASURE OF QA'S: MINIMIZING SHANNON INFORMATION AND VON NEUMANN ENTROPY AS A TERMINATION CRITERION **98**

4.1. ABOUT INFORMATION QUANTITIES 98
4.2. INFORMATION ANALYSIS AND INTELLIGENT MEASURES OF THE QA 101
4.2.1. Information analysis of Deutsch algorithm. *102*
4.2.2. Information analysis of QG dynamics and intelligent output states: Deutsch-Jozsa algorithm *104*
4.2.3. Information analysis of Shor's QA: The information role of entanglement and interference in Shor's QA gate. *114*
4.2.4. Information-theoretical analysis of Grover's QSA. *124*
4.3. THE STEP-BY-STEP NATURAL MAJORIZATION PRINCIPLE IN QAS SIMULATION AND QA-TERMINATION PROBLEM SOLUTION BASED ON PRINCIPLE OF SHANNON/VON NEUMANN MINIMUM ENTROPY 128
4.3.1. Majorization theory and its relation to QAs *128*
4.3.2. Simulation results of QA-termination problem solution based on principle of Shannon/von Neumann minimum entropy. *134*

REFERENCES ... **139**

TEXTBOOKS ON QUANTUM COMPUTING ... 139
RELATED REFERENCES ... 139

APPENDIX 1: *MAIN OPERATIONS OF QUANTUM COMPUTING AND INFORMATION CONTENT OF QUANTUM OPERATORS* ... **144**

A1.1. MAIN QUANTUM OPERATORS AND QUANTUM GATES ... 144
A1.2. UNITARY OPERATION TRANSFORMATIONS OF QUBITS AND QUANTUM ALGORITHM GATES. ... 152
A1.2.1. Computational and measurement basis states, Quantum evolution of two qubits, and Walsh-Hadamard transform applications. ... *152*
A1.2.2. Examples of Walsh-Hadamard transform applications in quantum algorithm computation ... *157*
A1.2.3. An information analysis of quantum systems. ... *164*
A1.2.4. Entanglement in the dynamic behavior of a two-qubit register. ... *173*

APPENDIX 2: MAIN PROPERTIES OF QUANTUM INFORMATION AND ENTROPY AMOUNTS ... **180**

A2.1. SOME BASIC FACTS ABOUT QM SYSTEMS. ... 180
A2.1.1. The partial Trace. ... *180*
A2.1.2. Classical Shannon Entropy Definition. ... *181*
A2.1.3. Relationship Formulas for the Shannon Entropy ... *181*
A2.1.4. Von Neumann Entropy Definition. ... *182*
A2.1.5. Conversion Formulas for the Von Neumann Entropy ... *182*
A2.2. SOME PROPERTIES OF VON NEUMANN ENTROPY FOR QUBIT ENSEMBLES: CASE STUDY ... 185
A2.3. ANALYSIS AND SUMMARY OF CASES I, II, AND III. ... 187
A2.3.1. Case I. (Classical) Independent Qubits: $S(AB) = 2 \,\&\, S(A) = 1 = S(B)$ ... *187*
A2.3.2. Case II. (Classical) Correlated Qubits: $S(AB) = 1 \,\&\, S(A) = 1 = S(B)$ ... *188*
A2.3.3. Case III. (Nonclassical-Purely QM) Entangled (Supercorrelated) Qubits: $S(AB) = 1 \,\&\, S(A) = 1 = S(B)$ ... *188*

APPENDIX 3: THE CONTROLLED NOT GATE AND LOGICAL CALCULATIONS ... **192**

APPENDIX 4: NUMBER THEORY DEFINITIONS ... **198**

AIM ... 198
A4.1. CONGRUENCES ... 198
A4. 2. NUMBER THEORY FROM AN ALGEBRIC VIEWPOINT ... 199

APPENDIX 5: ALGORITHMIC AND COMPUTATIONAL COMPLEXITY ... **205**

BRIEF INTRODUCTION IN THE THEORY OF COMPLEXITY ... 205
A5.1. THE COMPLEXITY (C) OF DETERMINISTIC ALGORITHMS ... 205
A5.2. THE COMPLEXITY OF NONDETERMINISTIC (RANDOM) ALGORITHMS ... 206
A5.3. THE SYMBOLS $O(f), o(f), \Omega_\infty(f), \omega(f), \Theta(f)$ IN COMPUTATIONAL COMPLEXITY ... 206
A5.4. ALGORITHMIC KOLMOGOROV (K(x)) COMPLEXITY OF SYMBOLIC REPRESENTATION AND INFORMATION SHANNON ENTROPY ... 207
A5.5. COMPUTATIONAL COMPLEXITY ... 209

APPENDIX 6: VECTOR, INNER, OUTER AND TENSOR PRODUCT ... **216**

A6.1. VECTOR PRODUCT ... 216
A6.2. INNER PRODUCT ... 217
A6.3. OUTER PRODUCT ... 217
A6.4. TENSORS AND TENSOR PRODUCT ... 218

APPENDIX 7: NOTIONS AND DEFINITIONS OF PAULI AND CLIFFORD GROUPS ... **221**

A7.1. INTRODUCTION ... 221
A7.2. PAULI MATRICES ... 221

Preface

Many of the most popular models of quantum computation are direct quantum generalizations of well known classical constructs. This includes quantum Turing machine, gate arrays and walks. These models use unitary evolution as the basic mechanism of information processing and only at the end do we make measurements, converting quantum information into classical information in order to read out classical answer. In the more familiar gate array model computational steps are unitary operations, developing a large entangled state prior to some final measurements for the output. Just two ideas from quantum computing (and some algorithmic ingenuity) are considered. The first of two ideas is amplitude amplification. The second idea is that any classical (either deterministic or probabilistic) computation can be simulated on a quantum computer. More precisely, (i) in the circuit a classical model, a classical circuit with N gates can be simulated by a quantum circuit with $O(N)$ gates; (ii) if the query model (when only the number of queries is counted), a classical computation with queries can be simulated by a quantum computation with N queries.

Thus, this greatly simplifies description of quantum algorithms. Instead of describing a quantum algorithm, we can describe a classical algorithm that succeeds with some small probability ε. Then, we can transform the classical algorithm to a quantum algorithm and apply the amplitude amplification to the quantum algorithm. The result is a quantum algorithm with the running time or the number of queries that is times the one for the classical algorithm with which we started. A similar reasoning can be applied, if instead of a purely classical algorithm, we started with a classical algorithm that involves quantum subroutines. Such algorithms can also be transformed into quantum algorithms with the same complexity.

Another approach in quantum computing consists in the formalism of the measurement based quantum computation. In this case we start with a given fixed entangled state of many qubits and perform computation by applying a sequence of measurements to designated qubits in designated bases. The choice of basis for later measurement may depend on earlier measurement outcomes and the final result of the computation is determined from the classical data of all the measurement outcomes. In contrast to unitary evolution, measurements are irreversibly destructive, involving much loss of potential information about a quantum state's identity. Thus it is interesting, and at first sight surprising, that we can perform universal quantum computation using only measurements as computation steps. Two principle schemes of measurement based computation are teleportation quantum computation and so-called cluster model of one-way quantum computer. From another standpoint, the appeal of hidden-variable theories is that they provide one possible solution to the measurement problem. For example, even if an observer were placed in coherent superposition, that observer would still have a sequence of definite experiences, and the probability of any such sequence could be calculated. For this case, hidden-variable theory is simply a way to convert a unitary matrix that maps one quantum state to another into a stochastic matrix that maps the initial probability distribution to the final one in some fixed basis. A hidden-variable theory can be based on networks flows: if we would examine the entire history of a hidden variable, then we could efficiently solve problems that are believed to be intractable even for quantum computers. By sampling histories, one could, for example, search an unordered database of N items for a single "marked item" using only $O\left(N^{\frac{1}{3}}\right)$ database queries. By comparison, Grover's quantum search algorithm requires $\theta\left(N^{\frac{1}{2}}\right)$ queries, while classical algorithms require $\theta(N)$ queries.

Remark. The readers unfamiliar with asymptotic notation, $O\left(f\left(N\right)\right)$means "at most order $f\left(N\right)$," $\Omega\left(f\left(N\right)\right)$means "at least order $f\left(N\right)$," and $\theta\left(f\left(N\right)\right)$ means "exactly order $f\left(N\right)$" (in details, see Appendix 5).

The results are surprising is that, given a hidden variable, the distribution over its possible values at any single time is governed by standard quantum mechanics and is therefore efficiently samplable on a quantum computer. So if examining the variable's history confers any extra computation power, then it can only be because of correlations between the variable's values at different times.

Quantum computation explores the possibilities of applying quantum mechanics to computer science. If built, quantum computers would provide speed-ups over conventional computers for a variety of problems. The two most famous results in this area are Shor's quantum algorithms for factoring and finding discrete logarithms and Grover's quantum search algorithm show that quantum computers can solve certain computation problems significantly faster than any classical computers. Shor's and Grover's algorithms have been followed by a lot of other results. Each of these algorithms has been generalized and applied to several other problems. New algorithms and new algorithmic paradigms (such as adiabatic computing which is the quantum counterpart of simulated annealing) have been discovered. We can explore several aspects adiabatic quantum-computational model and use a way that directly maps any arbitrary circuit in the standard quantum-computing model to an adiabatic algorithm of the same depth.

Many quantum algorithms are developed for the so-called oracle model in which the input is give as an oracle so that the only knowledge we can gain about the input is in asking queries to the oracle. As our measure of complexity, we use the query complexity. The query complexity of an algorithm A computing a function F is the number of queries used by A. The query complexity of F is the minimum query complexity of any algorithm computing F. We are interested in proving lower bounds of the query complexity of specific functions and consider methods of computing such lower bounds. The two most successful methods for proving lower bounds on quantum computations are following: the adversary method and the polynomial method. An alternative measure of complexity would be to use the time (temporal) complexity which counts the number of basic operations used by an algorithm. The temporal complexity is always at least as large as the query complexity since each query takes one unit step, and thus a lower bound on the query complexity is also a lower bound on the temporal complexity. For most existing quantum algorithms the temporal complexity is within poly-logarithmic factors of the query complexity.

One barrier to better understanding of the quantum query model is the lack of simple mathematical representations of quantum computations. While classical query complexity (both deterministic and randomized) has a natural intuitive description in terms of decision trees, there is no such easy description of quantum query complexity. The main difference between the classical and quantum case is that classical computations branch into non-interacting sub computations (as represented by the tree) while in quantum computations, because of the possibility of destructive interference between sub-computations, there is no obvious analog of branching. The bounded-error model is both relevant to understanding powerful explicit non-query quantum algorithms (such as Shor's factoring algorithm) and theoretically important as the quantum analogue of the classical decision tree model. We are interested in studying classical and quantum complexities because an oracle sometimes gives a separation between them. For example, it was showed one problem where we need an exponentially many queries in the bounded error classical case, but only a single query is needed in the quantum case. Another occasion to study a query complexity is when a temporal complexity is hard. In such case, the number of queries we make gives a lower bound for the temporal complexity. In fact, currently there is no lower bound method for quantum temporal complexity that gives super-linear bounding, and by studying quantum query complexity, we get lower bounds heuristic on quantum temporal complexity.

One of the powers of quantum computation comes from the fact that we can query in superposition. That is, if we are given a set of n elements from 1 to n, we can query an oracle in parallel once to obtain a superposition of $f\left(1\right)$ through $f\left(n\right)$. However, we can in a sense only learn one of the $f(i)$'s from such a query. The real power of quantum computation comes from interference. That is, the information in the state, e.g., $f(i)$'s, can be combined by means of unitary quantum gates in non-trivial way, and we can extract a global property of the input.

Lectures, presented in this manuscript were given in by Prof. S.V. Ulyanov and Prof. L.V. Litvintseva in period from 1975 to 2005 during their stay as professor staff in Moscow State Institute of Radiotechnics, Electronics and Automatics (State Technical University, Moscow, Russia), University of Electro-Communications (Chofu, Tokyo, Japan), University of Montana (USA), and in Polo didattico e di Ricerca di Crema (Milano University, Department of Information Technologies, Crema, Italy).

In present manuscript of Lecture Notes we are concentrate our attention on the description of the efficient simulation and design methodology of quantum algorithm gates using classical computer technology.