Toward Quantum Computational Agents

Matthias Klusch

German Research Center for Artifical Intelligence, Deduction and Multiagent Systems, Stuhlsatzenhausweg 3, D-66123 Saarbrücken, Germany.
e-mail: klusch@dfki.de

Abstract. In this chapter, we provide some first thoughts on, and preliminary answers to the question how intelligent software agents could take most advantage of the potential of quantum computation and communication, once practical quantum computers become available in foreseeable future. In particular, we discuss the question whether the adoption of quantum computational and communication means will affect the autonomy of individual and systems of agents. We show that the ability of quantum computing agents to perform certain computational tasks more efficient than classically computing agents is at the cost of limited self-autonomy, due to non-local effects of quantum entanglement.

1 Introduction

Quantum computing technology based on quantum physics promises to eliminate some of the problems associated with the rapidly approaching ultimate limits to classical computers imposed by the fundamental law of thermodynamics. According to Gordon Moore's first law on the growth rate of classical computing power, and the current advances in silicon technology, it is commonly expected that these limits will be reached around 2020. By then, the size of microchip components will be on the scale of molecules and atoms such that quantum physical effects will dominate, hence irrevocably require effective means of quantum computation.

Quantum physics has been developed in the early 1920's by physicists and Nobel laureates such as Max Planck, Niels Bohr, Richard Feynman, Albert Einstein, Werner Heisenberg, and Erwin Schrödinger. It uses quantum mechanics as a mathematical language to explain nature at the atomic scale. In quantum mechanics, quantum objects including neutrons, protons, quarks, and light particles such as photons can display both wave-like and particle-like properties that are considered as complementary. In contrast to macroscopic objects of classical physics, any quantum object can be in a superposition of many different states at the same time that enables for quantum parallelism. In particular, it can exhibit interference effects during the course of its unitary evolution, and can be entangled with other spatially separated quantum objects such that operations

[*] Published in: Nickles, Rovatsos, Weiss (Eds.). Computational Autonomy. LNCS, 2969, Springer, 2004.

on one of them may cause non-local effects that are impossible to realize by means of classical physics.

It has been proven that quantum computing can simulate classical computing. However, the fundamental raison d'être of quantum computation is the fact that quantum physics appears to allow one to transgress the classical boundary between polynomial and exponential computations [25]. Though there is some evidence for that proposition, only very few practical applications of quantum computing and communication have been proposed so far including quantum cryptography [5].

Quantum computing devices have been physically implemented since the late 1990's by use of, for example, nuclear magnetic resonance [43], and solid state technologies such as that of neighbouring quantum dots implanted in regions of silicon based semiconductor on the nanometer scale [27]. As things are now, they work for up to several tens of qubits. Whether large-scale fault-tolerant and networked quantum computers with millions of qubits will ever be built remains purely speculative at this point. Though, rapid progress and current trends in nanoscale molecular engineering, as well as quantum computing research carried out at research labs across the globe could make it happen to let us see increasingly sophisticated quantum computing devices in the era 2020 to 2050.

This leads, in particular, to the question how intelligent software agents [46, 45] could take most advantage of the potential of quantum computation and communication, once practical quantum computers are available. Will quantum computational agents be able to outperform their counterparts on classical von-Neumann computers? What kinds of architectures and progamming languages are required to implement them? Does the adoption of quantum computational and communication means affect the autonomy of individual and systems of agents? This chapter provides some first thoughts on, and preliminary answers to these questions based on known fundamental and recent results of research in quantum computing and communication. It is intended to help bridging the gap between the agent and quantum research community for interdisciplinary research on quantum computational intelligent agents.

In sections 2 and 3, we briefly introduce the reader to the basics of quantum information, computation and communication in terms of quantum mechanics. For more comprehensive and in-depth introductions to quantum physics, and quantum computation we refer the interested reader to, for example, [12], respectively, [33, 23, 42, 1]. [17] provides a well-readable discussion of alternative interpretations of quantum mechanics. Readers who are familiar with the subjects can skip these sections. In section 4, we outline an architecture for a hybrid quantum computer, and propose a conceptual architecture and examples of quantum computational agents for such computers in section 5. Issues of quantum computational agent autonomy are discussed in section 6.

2 Quantum Information

Quantum computation is the extension of classical computation to the processing of quantum information based on physical two-state quantum systems such as photons, electrons, atoms, or molecules. The unit of quantum information is the quantum bit, the analogous concept of the bit in classical computation.

2.1 Quantum Bit

Any physical two-state quantum system such as a polarized photon can be used to realize a single *quantum bit* (qubit). According to the postulates of quantum mechanics, the state space of a qubit ψ is the 2-dimensional complex Hilbert space $H_2 = \mathbb{C}^2$ with given orthonormal computational basis in which the state $|\psi >$ is observed or measured[1]. The standard basis of qubit state spaces is $\{|0 >, |1 >\}$ with coordinate representation $|0 >= (1, 0)^t$, and $|1 >= (0, 1)^t$. Any *quantum state* $|\psi >$ of a qubit ψ is a coherent *superposition* of its basis states

$$|\psi >= \alpha_0|0 > +\alpha_1|1 > \tag{1}$$

where the probability *amplitudes* $\alpha_1, \alpha_2 \in \mathbb{C}$ satisfy the normalization requirement $|\alpha_0|^2 + |\alpha_1|^2 = 1$ for classical probabilities $p(|\psi >= |0 >) \equiv p(0) = |\alpha_1|^2$, respectively, $p(|\psi >= |1 >) \equiv p(1) = |\alpha_2|^2$ of the occurrence of alternative basis states [2]. The decision of the physical quantum system realizing the qubit on one of the alternatives is made non-deterministically upon irreversible measurement in the standard basis. It reduces the superposed qubit state to the bit states '0' and '1' in classical computing. This transition from the quantum to the observable macroscopic world is called *quantum decoherence.*

2.2 Quantum Bit Register

A *n-qubit register* $\psi = \psi_1...\psi_n$ of n qubits $\psi_i, i \in \{1, ..n\}$ is an ordered, composite n-quantum system. According to quantum mechanics, its state space is the n-folded *tensor (Kronecker) product* $H_2^{\otimes n} = \overbrace{H_2 \otimes ... \otimes H_2}^{n}$ of the (inner product) state spaces H_2 of its n component qubits. Each of the 2^n n-qubit basis states $|x_i >$, $x_i \in \{0, 1\}^n$ of the register can be viewed as the binary representation of

[1] Paul Dirac's bra-ket notation $< \psi| = (\alpha_1, ..., \alpha_k)^T$ (bra) and $|\psi >= (\alpha_1^*, , ..., \alpha_k^*)$ (ket) with complex conjugates $\alpha_i^*, i \in \{1, .., k\}$ is the standard notation for system states in quantum mechanics. The inner product of quantum state vectors in H_k is defined as $< \psi_1|\psi_2 >= (\alpha_i^*)_{i\in\{1,..,k\}} \otimes (\beta_i)_{i\in\{1,..,k\}} = \sum_{i=1}^{k} \alpha_i^* \beta_i$. The orthonormal basis of H_k can be chosen freely, but if fixed refers to one physical observable of the quantum system ψ such as position, momentum, velocity, or spin orientation of a polarized photon, that can take k values.

[2] In contrast to physical probabilistic systems, a quantum system can destructively interfere with itself which can be described by negative amplitude values.

a number k between 0 and $2^n - 1$. Any *composite state* of a n-qubit register is in a superposition of its basis states

$$|\psi >= |\psi_1 \psi_2 ... \psi_n >= \sum_{k=0}^{2^n-1} \alpha_k |k >, \sum_{k=0}^{2^n-1} |\alpha_k|^2 = 1 \tag{2}$$

As the state of any n- and m-qubit register can be described by 2^n, respectively, 2^m amplitudes, any distribution on the joint state space of the $n + m$-qubit register takes 2^{n+m} amplitudes. Hence, in contrast to classical memory, quantum memory increases exponentially in the size of the number of qubits stored in a quantum register. It can be doubled by adding just one qubit.

2.3 Measurement of Qubits

Measurement of a n-qubit register ψ in the standard basis yields a n-bit post-measurement quantum state $|\psi_k >$ with probability $|\alpha_k|^2$. Measurement of the first $z < n$ qubits corresponds to the orthogonal measurement with 2^z projectors $M_i = |i >< i| \otimes I_{2^{n-z}}, i \in \{0,1\}^z$ which collapses it into a probabilistic classical bit vector, yielding a single state randomly selected from the exponential set of possible states[3]. Measurement of the individual qubit ψ_m of a n-qubit register $\psi = \psi_1 ... \psi_m ... \psi_n, n \geq m$ in compound state $|\psi >= \sum_{i=0}^{2^n-1} c_i |i_1..i_n >$ with measurement operator M_m will give the classical outcome $x_m \in \{0,1\}$ with probability $p(x_m) = \sum_{i_1..i_n} |c_{i_1..i_{m-1} x i_{m+1}..i_n}|^2 =< \psi | M_m^* M_m | \psi >$, and post-measurement state is

$$|\psi >' = \frac{1}{\sqrt{p(x_m)}} \sum_{i_1..i_{m-1} i_{m+1}..i_n} c_{i_1..i_{m-1} x i_{m+1}..i_n} |i_1..i_{m-1} x i_{m+1}..i_n >$$

where $c_{i_1..i_{m-1} x i_{m+1}..i_n}$ denote the amplitudes of those 2^n alternatives for which x could be observed as state value of the m-th qubit of ψ upon measurement. In general, the post-measurement quantum state $|\psi_k >'$ of $|\psi_k >$ is $\frac{M_m |\psi_k>}{\sqrt{<\psi|M_m^* M_m|\psi>}}$.

2.4 Unitary Evolution of Quantum States

According to the postulates of quantum mechanics, the time evolution of any n-qubit register, $n \geq 1$, is determined by any linear, unitary[4] operator U in the 2^n-dimensional Hilbert space $H_2^{\otimes n}$. The size of the unitary matrix of a n-qubit operator is $2^n \times 2^n$, hence exponential in the physical size of the system. Since any unitary transformation U has an inverse $U^{-1} = U^*$, any non-measuring quantum operation is reversible, its action can always be undone. Measurement of a qubit ψ is an irreversible operation since we cannot reconstruct its state $|\psi >$ from the observed classical state after measurement.

[3] According to the *standard interpretation of quantum mechanics* it is meaningfully to attribute a definite state to a qubit only *after* a precisely defined measurement has been made. Due to Heisenberg's *uncertainty principle* complementary observables such as position and momentum cannot be exactly determined at the same time.

[4] *Unitarity* preserves the inner product ($< \phi | U^* U | \psi >$), similar to a rotation of the Hilbert space that preserves angles between state vectors during computation.

2.5 Entangled Qubits

Entangled n-qubit register states cannot be described as a tensor product of its component qubit states. Central to entanglement is the fact that measuring one of the entangled qubits can affect the probability amplitudes of the other entangled qubits no matter how far they are spatially separated. Such kind of non-local or holistic correlations between qubits captures the essence of the *non-locality principle of quantum mechanics* which has been experimentally verified by John Bell in 1964 [3] but is impossible to realize in classical physics.

Example 2.1: *Entangled qubits*

Prominent examples of entangled 2-qubit are the *Bell states*

$$|\psi^+ > = \frac{1}{\sqrt{2}}((|01> + |10>), |\phi^+ >= \frac{1}{\sqrt{2}}((|00> + |11>),$$
$$|\psi^- > = \frac{1}{\sqrt{2}}((|01> - |10>), |\phi^- >= \frac{1}{\sqrt{2}}((|00> - |11>)$$

The Bell state $|\phi^+ >= (\frac{1}{\sqrt{2}}, 0, 0, \frac{1}{\sqrt{2}})$ is not decomposable. Otherwise we could find amplitudes of a 2-qubit product state $(\alpha_{11}|0> + \alpha_{12}|1>)(\alpha_{21}|0> + \alpha_{22}|1>) = \alpha_{11}\alpha_{21}|00> + \alpha_{11}\alpha_{22}|01> + \alpha_{12}\alpha_{21}|10> + \alpha_{12}\alpha_{22}|11>$ such that $\alpha_{11}\alpha_{21} = \frac{1}{\sqrt{2}}$, $\alpha_{11}\alpha_{22} = 0$, $\alpha_{12}\alpha_{21} = 0$ and $\alpha_{12}\alpha_{22} = \frac{1}{\sqrt{2}}$ which is impossible. We cannot reconstruct the total state of the register from the measurement outcomes of its component qubits. $|\phi^+ >$ can be produced by applying the conditioned-not 2-qubit operator $M_{cnot} = ((1,0,0,0),(0,1,0,0),(0,0,0,1),(0,0,1,0))$ to the separable register state $|\psi_1\psi_2 >= \frac{1}{\sqrt{2}}(|00> + |10>)$.

Suppose we have measured 0 as definite state value of the second qubit in state $|\phi^+ >\equiv a|00> + b|01> + c|10> + d|11> \equiv (a,b,c,d)$ with amplitudes normalized to 1. The corresponding measurement operator is the self-adjoint, non-unitary projector $M_{2:0} = ((1,0,0,0),(0,0,0,0),(0,1,0,0),(0,0,0,0))$, which yields the outcome 0 or 1 with equal probability, for example, $p(0) = <\phi^+|M^*_{2:0}M_{2:0}|\phi^+ >= (\frac{1}{\sqrt{2}}, 0, 0, \frac{1}{\sqrt{2}})(\frac{1}{\sqrt{2}}, 0, 0, 0)^t = \frac{1}{2}$, and the post-measurement state $|\phi^+ >' = \frac{M_{2:0}|\psi>}{\sqrt{<\psi|M_{2:0}|\psi>}}$ $= \frac{(\frac{1}{\sqrt{2}},0,0,0)}{\sqrt{1/2}} = \sqrt{2}(\frac{1}{\sqrt{2}}, 0, 0, 0) = (1,0,0,0) = |00 > \neq a|00> + c|10>$.

That means, measurement of the second qubit caused also the entangled first qubit to instantaneously assume a classical state without having operated on it.

○

Pairs of entangled qubits are called *EPR pairs* with reference to the associated Einstein-Podolsky-Rosen (EPR) thought experiment [20]. The *non-local effect of instantaneous state changes* between spatially separated but entangled quantum states upon measurement belongs to the most controversial issue and debated phenomenon of quantum physics, and caused interesting attempts of developing a quantum theory of the humand mind and brain [39, 38]. Entanglement links information across qubits, but does not create more of it [22], nor does it allow to communicate any classical information faster than light.

Entangled qubits can be physically created either by having an EPR pair of entangled particles emerge from a common source, or by allowing direct interaction between the particles, or by projecting the state of two particles each from different EPR pairs onto an entangled state without any interaction between them (*entanglement swapping*) [12]. Entanglement of qubits is considered as one essential feature of, and resource for quantum computation and quantum communication [25, 11].

3 Quantum Computation and Communication

The quantum Turing machine model [37], and the quantum circuit model [18] are equivalent models of quantum computation. In this paper, we adopt the latter model.

3.1 Quantum Logic Gates and Circuits

A *n-qubit gate* is a unitary mapping in $H_2^{\otimes n}$ which operates on a fixed number of qubits (independent of n) given n input qubits. Most quantum algorithms to date are described through a *quantum circuit* that is represented as a finite sequence of concatenated quantum gates. Basic quantum gates are the 1-qubit *Hadamard* (H) and *Pauli* (X, Y, Z) gates, and the 2-qubit XOR, called *conditioned not* (CNOT), gate. These operators are defined by unitary matrices as follows

$$\begin{aligned} M_H &= \frac{1}{\sqrt{2}}((1,1),(1,-1)) \\ M_{CNOT} &= ((1,0,0,0),(0,1,0,0),(0,0,0,1),(0,0,1,0)) \\ M_X &= ((0,1),(1,0)), M_Z = ((1,0),(0,-1)), M_Y = ((0,-i),(i,0)) \end{aligned}$$

The Hadamard gate creates a superposed qubit state for standard basis states, demonstrates *destructive quantum interference* if applied to superposed quantum states ($M_H(\frac{1}{\sqrt{2}}(|0> + |1>)) = |0>$), and can be physically realized, for example, by a 50/50-beamsplitter in a Mach-Zehnder interferometer [12]. The CNOT gate flips the second (target) qubit if and only if the first (control) qubit is in state $|1>$. The quantum circuit consisting of a Hadamard gate followed by a CNOT gate creates an entangled *Bell state* for each computational basis state. The X gate is analogous to the classical bit-flip NOT gate, and the Z gate flips the phase (amplitude sign) of the basis state $|1>$ in superposition. Other common basic qubit gates include the NOP, S, and T gates for quantum operations of identity, phase rotation by $\pi/4$, respectively $\pi/8$. The set {H, X, Z, CNOT, T} is universal [33].

3.2 Quantum Vs. Classical Computation

The constraint of unitary evolution of qubit states yields a generalization of the restriction of classical (Turing machine or logic circuit based) models of computation to unitary, hence reversible computation [4]. It has been shown that each classical algorithm computing a function f can be converted into an equivalent quantum operator U_f with the same order of efficiency [49, 1], which means that quantum systems can imitate all classical computations. However, the fundamental raison d'être of quantum computation is the expectation that quantum physics allows one to do even better than that.

The linearity of quantum mechanics gives rise to *quantum parallelism* that allows a quantum computer to simultaneously evaluate a given function $f(x)$ for all inputs x by applying its unitary transformation $U_f : |x > |0 > \mapsto |x > |0 \oplus f(x) >= |x > |f(x) >$ to a suitable superposition of these inputs such that

$$U_f \left(\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x > |0 > \right) = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x > |f(x) > \tag{3}$$

Though this provides, in essence, not more than classical randomization, if combined with the effects of *quantum interference* such as in the Deutsch-Josza algorithm ([33], p.36) and/or quantum entanglement [11] it becomes a fundamental feature of many quantum algorithms for speeding-up computations. The basic idea is to compute some global property of f by just one evaluation based on a combination of interfered alternative values of f, whereas classical probabilistic computers only can evaluate different but forever mutually excluding alternative values of f with equal probability.

In general, *quantum algorithms* appear to be best at problems that rely on promises or *oracle* settings, hence use some hidden structure in a problem to find an answer that can be easily verified through, for example, means of amplitude amplification. Prominent examples include the quantum search developed by Grover (1996) for searching sets of n unordered data items [21], and the quantum prime factorization of n-bit integers developed by Shor (1994) [41] with complexity of $O(\sqrt{n})$, respectively, $O(n^3)$ time, which is a quadratic and exponential speed-up compared to the corresponding classical case. It is not known to date whether quantum computers are in general more powerful than their classical counterparts [5]. However, it is widely believed that the existence of an efficient solution of the NP-hard problem of integer prime factoring using the quantum computation model [41], as well as the quadratically speed up of classical solutions of some NP-complete problems such as the Hamiltonian cycle problem by quantum search ([33], p.264), provides evidence in favor of this proposition.

3.3 Quantum Communication Models

In this paper, we consider the following models of quantum based communication between two quantum computational agents A and B.

[5] In terms of the computational complexity classes P, BPP, NP, and $PSPACE$ with $P \subseteq NP \subseteq PSPACE$, it is known that $P \subseteq QP$, $BPP \subseteq BQP$, and $BQP \subseteq PSPACE$ [10]. QP and BQP denote the class of computational problems that can be solved efficiently in polynomial time with success probability of 1 (exact), or at least 2/3 (bounded probability of error), respectively, on uniformly polynomial quantum circuits.

1. **QCOMM-1**. Agents A and B share entangled qubits and use a classical channel to communicate.
2. **QCOMM-2**. Agents A and B share entangled qubits and use a quantum channel to communicate.
3. **QCOMM-3**. Agents A and B share no entangled qubits and use a quantum channel to communicate.

QCOMM-1: Quantum teleportation of n qubits with $2n$ bits. The standard process of teleporting a qubit ϕ from agent A to agent B based on a shared EPR pair $\psi_1\psi_2$ and classical channel works as follows [7]. Suppose agent A (B) keeps qubit ψ_1 (ψ_2). A entangles ϕ with ψ_1 by applying the CNOT, and the Hadamard gate to the 2-qubit register $[\phi\psi_1]$ into one of four Bell states $|\phi\psi_1>$. It then sends the measurement outcome (00, 10, 01, or 11) to agent B through a classical communication channel at the cost of two classical bits. Only upon receipt of A's 2-bit notification message, agent B is able to create $|\phi>$ by applying the identity or Pauli operator gates to its qubit ψ_2 depending on the content of the message (00: I, 01: X; 10: Z; 11: XZ) [6].

QCOMM-2: Quantum dense coding of n-bit strings in $n/2$ qubits. Agent A dense codes each of consecutive pairs of bits b_1b_2 at the cost of one qubit as follows [8]. Suppose agent A (B) keeps qubit ψ_1 (ψ_2) of shared EPR pair in entangled Bell state $|\psi>=|\psi_1\psi_2>=\frac{1}{\sqrt{2}}(|00>+|11>)$. According to prior coding agreement with B, agent A applies the identity or Pauli operators to its qubit depending on the 2-bit message to be communicated (for example, 00: $I\otimes I|\psi>$, 01: $X\otimes I|\psi>$, 11: $Z\otimes I|\psi>$, 10: $(XZ)^t\otimes I|\psi>$) which results in one of four Bell states $|\psi>'$ and physically transmits the qubit ψ_1 to B. Upon receipt of ψ_1, agent B performs $M_{CNOT}|\psi>'$ yielding separable state $|\gamma_0\gamma_1>$, applies the Hadamard operation to the first qubit $M_H|\gamma_0>=|\delta_0>$ and decodes the classical 2-bit message depending on measured states of $\delta_0\gamma_1$ (e.g., $\delta_0\gamma_1=00$: 00, 01: 01, 11: 10, 10: 11).

A fundamental result in quantum information theory by Holevo (1973) [24] implies that by sending n qubits one cannot convey more than n classical bits of information. However, for every classical (probabilistic) communication problem [48] where agents exchange classical bits according to their individual inputs and then decide on an answer which must be correct (with some probability), quantum protocols where agents exchange qubits of communication are at least as powerful [31].

[6] Due to (Bell state) measurement of $|\phi\psi_1>$ agent A lost the original state $|\phi>$ to be communicated. However, since ψ_1 and ψ_2 were entangled, this measurement instantaneously affected the state of B's qubit ψ_2 (cf. Ex. 2.1) such that B can recover $|\phi>$ from $|\psi_2>$.

4 Quantum Computers

All known quantum algorithms require the determinism and reliability of classical control for the execution of suitable quantum circuits consisting of a finite sequence of quantum gates and measurement operations. Figure 1 shows a master-slave architecture of a *hybrid quantum computer* based on proposals in [35] and [9] in which classical signals and processing of a classical machine (CM) are used to control the timing and sequence of quantum operations carried out in a *quantum machine* (QM).

The QM consists of *quantum memory*, *quantum processing unit* (QPU) with error correction, *quantum bus*, and *quantum device controller* (QDC) with interface to the classical machine (CM). The classical machine consists of a CPU for high-level dynamic control and scheduling of the QM components, and memory that can be addressed by both classical and quantum addressing schemes (e.g., [9] p.20, [33] p.268). Quantum memory can be implemented as a lattice of static physical qubits, which state is factorized in tensor states over its nodes[7]. Qubit states can be transported within the QM along point-to-point quantum wires either via teleportation (cf. section 3.3), or chained quantum swapping and repeaters [36][8].

A few *quantum programming languages* (QPL) for hybrid quantum computers exist, such as the procedural `QCL` [34], and `QL` [9], and the functional `qpl` [40]. A QPL program contains high-level primitives for logical quantum operations, interleaved with classical work-flow statements. The QPL primitives are compiled by the CPU into low-level instructions for qubit operators that are passed to and then translated by the QDC to physical qubit (register) operations which are executed by the QPU. The QPU performs scheduled sequences of measurement and basic qubit operations from a universal set of 1- and 2-qubit quantum gates (cf. section 3.1) with error correction[9] to minimize quantum decoherence caused by imperfect control over qubit operations, measurement errors, number of entangled qubits, and the pysical limits of the quantum systems such as nuclear spins used to realize qubits [19]. The QM returns only the results of quantum measurements to the CM.

[7] According to the *no-cloning theorem* of quantum computing [47], a qubit state cannot be perfectly copied unless it is known upon measurement. Thus, no backup copies of quantum data can be created in due course of quantum computation.

[8] In short *quantum wires* a qubit state can be progressively swapped between pairs of qubits in a line, where each qubit is represented, for example, by the nuclear spin of a phosporus atom implanted in silicon (quantum dot). Each swap operation along this line of atoms is realized by three back-to-back CNOT gates.

[9] According to the *threshold theorem* of quantum computing[28, 2], scalable quantum computers with faulty components can be built by using quantum error correction codes as long as the probability of error of each quantum operation is less than 10^{-4}.

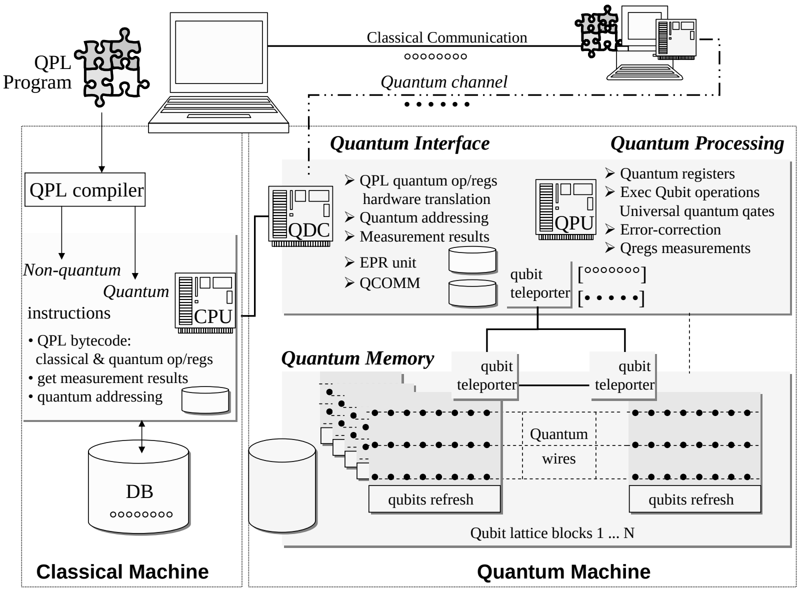

Fig. 1. Master-slave architecture of a hybrid quantum computer.

5 Agents on Quantum Computers

5.1 QC Agents

A *quantum computational agent* (QCA) extends an intelligent software agent by its ability to perform both classical, and quantum computing and communication on a quantum computer to accomplish its goals individually, or in joint interaction with other agents. QC agents on hybrid quantum computers are coded in an appropriate QPL. The deliberative component of a QC agent uses sensed input, beliefs, actions, and plans that are classically or quantum coded depending on the kind of respective QPL data types and statements. The QPL agent program is executed on both the classical and the quantum machine in an interleaved master-slave fashion using the QPL interface of the quantum machine (cf. section 4).

QC agents are supposed to exploit the power of quantum computing to reduce the computational complexity of certain problems, where appropriate. For example, a *quantum computational information agent* (QCIA) is a special kind of QC agent which extends an intelligent information agent on a classical computer [29] by its ability to perform quantum computation and communication for information search and management tasks. How can a QCIA exploit oracle-based quantum search algorithms for searching local data or knowledge bases?

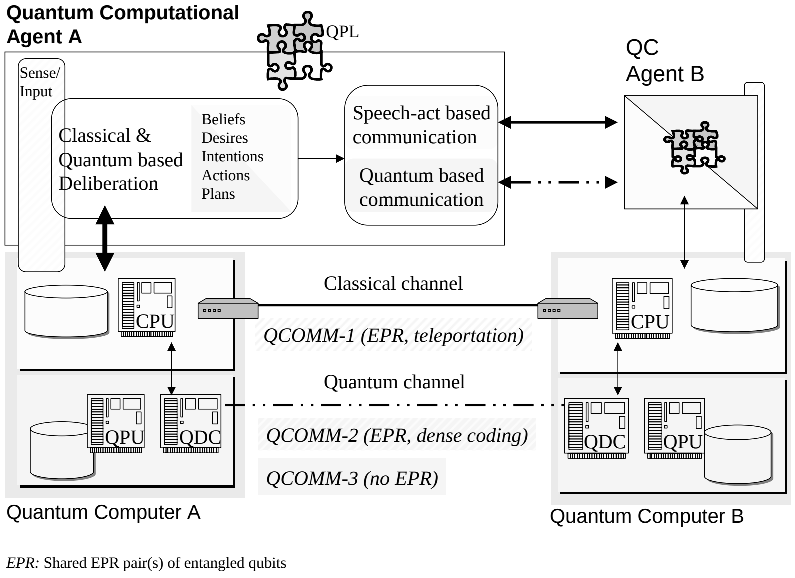

Fig. 2. Conceptual scheme of a quantum computational agent.

Local quantum based search. Suppose a QCIA has to search its local unstructured classical database LDB with $N = 2^n$ l-bit data entries d_x each of which is indexed by value $x = 0...N-1$ for given l-bit input s and search oracle O with $1 \leq M \leq N$ solutions. The oracle is implemented by an appropriate quantum circuit U_f that checks whether the input is a solution to the search problem ($f(x) = 1$ if $d_x = s$, else $f(x) = 0$). No further structure to the problem is given. Any classical search would take an average of $O(N/M)$ oracle calls to find a solution. Using Grover's quantum search algorithm [21] the QCIA can do the same in $O(\sqrt{N/M})$ time. The basic idea is that (a) the search is performed on a $logN$-qubit index register $|x>$ which state is in superposition of all $N = 2^n$ index values x[10], and (b) the oracle O marks the M solutions ($|x> \rightarrow (-1)^{f(x)}|x>$ with $f(x) = 1$ if $d_x = s$, 0 else) which are amplified to increase the probability that they will be found upon measurement of the index register after $O(\sqrt{N/M})$ iterations. Type and cost of each oracle call (matching operation U_f) depends on the application. Implementation of the search uses n-qubit index, l-qubit data and input, and 1-qubit oracle register of the QPU. Like in the classical search, we need a quantum addressing scheme ([33] p.268) with $O(logN)$ per operation to access, load, and restore indexed data d_x to the data register, and recreate respectively measured index states $|x>$ for further processing.

[10] The initial superposed index state $|x>$ is created by n-folded Hadamard operation ($H^{\otimes n}|0> = \frac{1}{\sqrt{2^n}} \sum_{i \in \{0,1\}^n} |i>$).

Local quantum based matchmaking is a special case of local quantum search for binary coded service descriptions. The type of service matching depends on the implemented search oracle. We assume that both service requests and service ads are encoded in the same way to allow for meaningful comparison by a *quantum computational matchmaker agent*. Componentwise quantum search with bounded rather than exact success probability for partial matching could be used for syntactic but not semantic service matching such as in LARKS [44].

5.2 QC Multi-Agent Systems

A *quantum computational multi-agent system* (QCMAS) is a multi-agent system that consists of both classical and quantum computing agents which can interact to jointly accomplish their goals. A *pure QCMAS* consists of QC agents only. QCMAS which members cannot interact with each other using a quantum communication model (cf. section 3.3) are called *type-I QCMAS*, and *type-II QCMAS* otherwise. QC agents of type-I or type-II QCMAS are called *type-I QC agents*, respectively, *type-II QC agents*.

Inter-agent communication between type-I QC agents bases on the use of classical channels without sharing any EPR pairs. None of the quantum communication models is applicable. As a consequence, quantum computation is performed locally at each individual agent. In addition, type-II QC agents can use quantum communication models which cannot be simulated in any type-I QCMAS. It is assumed that type-II QC agents share a sufficient number of EPR pairs, and have prior knowledge on used quantum coding operations for this purpose. Any QC agent communicates appropriate speech-act based messages via classical channels to synchronize its actions, if required. Messages related to quantum communication between type-II QC agents concern, for example, the notification in quantum teleportation (QCOMM-1), the prior agreement on the order of operations in quantum dense coding (QCOMM-2), and the semantics of qubits (QCOMM-3).

What are the main benefits of QCMAS? In certain cases, QCMAS can be computationally more powerful than any MAS by means of properly designed and integrated QC agents. The main challenge is the development of application-specific quantum algorithms that can do better than any classical algorithm.

Quantum-based communication between type-II QC agents is inherently secure. Standard quantum teleportation (QCOMM-1) ensures data integrity, since it is impossible to deduce the original qubit state from eavesdropped 2-bit notification messages of the sender without possessing the respective entangled qubit of the receiver. Quantum dense coding (QCOMM-2) is secure, since any quantum operation on the physically transmitted qubit in any of the four Bell states takes the same value. The physical transmission of qubits via a quantum channel (QCOMM-3) is secure due to the no-cloning theorem of quantum mechanics, a fact that is also used in quantum key distribution [5]. Any attempt of eavesdropping will reckognizably interfere with the physical quantum states of transmitted qubits.

Finally, certain communication problems [48], that is the joint computation of some boolean function f minimizing the number of qubits to communicate for this purpose, can be solved more efficiently by type-II QC agents. In general, it has been proven in [15] that the gap between bounded-error (zero-error) classical and (exact) quantum communication complexity is near quadratic (exponential), and that each quantum communication model is at least as powerful than a classical one for every communication problem on n-bit inputs [31]. More interesting, they can do even better for certain communication problems such as the computation of inner product, equality, and disjointness of boolean functions $f(x), g(x)$ according to individual n-bit inputs $x \in \{0,1\}^n$. Quantum based solutions to latter problems can be applied to quantum based collaborative search, and matchmaking [30], with respective quadratic or exponential reduction of communication complexity.

5.3 Examples of Type-I and Type-II QCMAS

Quantum based collaborative search in type-I QCMAS. Upon receipt of a multicasted l-bit request s from QCIA A_1, each agent $A_j, j = 2..n$ locally computes $M_j \geq 1$ solutions to the given search problem $LQS(s, \mathrm{O}, LDB_j)$ in $O(\sqrt{N_j/M_j})$ time, instead of $O(N)$ in the classical case, and returns the found data items to A_1. Due to non-quantum based interaction, both requests and replies have to be binary coded for transmission via classical channel, and binary requests are directly quantum coded prior to quantum search (cf. section 5.1).

Quantum based collaborative search in type-II QCMAS. Suppose two QCIAs A_1, A_2 want to figure out whether a n-bit request s matches with data item $s' \in LDB_2$ $(N = 1)$ with the promise that their Hamming distance is $h(s, s') = 0$ else $n/2$. In this case, it suffices to solve the corresponding equality problem with $O(logn)$ qubits of communication, instead of $O(n)$ in the classical case [15]. Basic idea is that A_1 prepares its n-bit s in a superposition of $logn + 1$ qubits such that A_2 can test, upon receipt of s, whether $s_i \oplus s'_i = 0, i = 1..n$ by applying the known oracle-based Deutsch-Josza quantum algorithm ([33], p.34) to $|s > |o \oplus s \oplus s' >$, followed by Hadamard operations $(H^{\otimes(logn+1)})$, and measurement of the final state yields the desired result.

QC matchmaking in type-I and type-II QCMAS. As in the classical case, quantum based service matchmaking can be directly performed by pairs of QC agents in both types of QCMAS. In fact, it is a special case of the collaborative search scenario where two QC agents can both advertise and request a set of N (N') $l-$bit services from each other. For example, QC service agents A of a type-II QCMAS can physically send a set of (QCOMM-2: dense coded) n-bit service request each of size $n/2$ qubits to a QC matchmaker A^* via a quantum channel (QCOMM-3). In cases where only classical channels are available (QCOMM-1), A can teleport the qubit request to A^* at the cost of $2n$ bits. In any case, upon receipt of the request, A^* quantum searches its classical database of N service ads, and returns those that matches it according to the given search ("matching") oracle. Using quantum search, the disjointness of sets of quantum coded service descriptions interpreted as ads and/or requests can be decided with just $logN + 1$ qubits of communication [15], instead of at least N bits in the classical randomized setting [26].

6 Autonomy of QC Agents

Following the classification of different types of agent autonomy in [16], we define a QC agent A autonomous from QC agent B for given autonomy object o in the context c, if, in c, its behaviour regarding o is not imposed by B. The ability of an individual QC agent in type-I QCMAS to exhibit autonomous behaviour is not affected by its local quantum computation, since non-local effects are restricted to local quantum machine components. Hence, the self-autonomy of individual type-I QC agents in terms of the ability to autonomously reason about sets of goals, plans, and motivations for decision-making remains intact. That is independent from the fact that the computational complexity of deliberative actions could possibly be reduced by, for example, quantum searching of complex plan libraries. Regarding user autonomy, any external physical interaction with the quantum machine by the user will cause massive quantum decoherence which puts the success of any quantum computational process and associated accomplishment of tasks and goals of individual type-I QC agents at risk.

A type-II QC agent shall be able to adjust its behaviour to the current quantum computing context of the overall task or goal to accomplish. It can freely decide on whether and with which agents to share a sufficient number of EPR pairs, or to make prior coding agreements according to the used quantum communication model. However, both its adjustable interaction and computational autonomy, turn out to be limited to the extent of entanglement based joint computation and communication with other type-II QC agents. Any type-II QC agent can change the state of non-local qubits that are entangled with its own qubits by local Bell state measurements. This way, if malevolent, it can misuse its holistic correlations with other type-II QC agents to corrupt their computations by manipulating their respective entangled quantum data. Even worse, there is no way for these agents to avoid such kind of influence.

For example, suppose that agents A and B share EPR pairs to interact using quantum teleportation (QCOMM-1). Since the change of B's entangled qubits caused by A's local Bell state measurements is instantaneous, B cannot avoid it at all. B does not even know that such changes occurred until it receives A's 2-bit notification messages (cf. section 3.3). B is not able to clone its entangled qubits, and measuring their state prior to A's notification would let communication fail completely. The same situation occurs when entanglement swapping is used to teleport qubit states along a path of correlated QC agents in a type-II QCMAS; in fact, it holds for any kind of entanglement based computation in general.

To summarize, the use of entanglement as a resource for computation and communication requires type-II QC agents to strictly trust each other. The ability of individual type-II QC agents to influence other type-II QC agents is inherently coupled with the risk of being influenced in turn by exactly the same agents in the same way. Though, for an individual agent the degree of its influence can be quantified based on the number, and the frequency of respective usage of its entangled quantum data.

7 Conclusions

In essence, quantum computational agents and multi-agent systems are feasible to implement on hybrid quantum computers, and can be used to solve certain problems in practical applications such as information search and service matchmaking more efficiently than with classically computing agents. Type-II QC agents can take most computational advantages of quantum computing and communication, but at the cost of limited self-autonomy, due to non-local effects of quantum entanglement. Quantum-based communication between type-II agents is inherently secure.

Ongoing and future research on QC agents and multi-agent systems focuses on appropriate integration architectures for QCMAS of both types, type-II QC information and matchmaker agents, as well as potential new applications such as secure quantum based distributed constraint satisfaction, and qualitative measures and patterns of quantum computational autonomy in type-II QCMAS.

References

1. D. Aharonov. Quantum Computation. LANL Archive quant-ph/981203, 1998.
2. D. Aharonov, M. Ben-Or. Polynomial Simulations of Decohered Quantum Computers. Proc. 37th Ann. Symp. Foundations of Computer Science (FOCS), 1996.
3. J.S. Bell. Speakable and Unspeakable in Quantum Mechanics. Cambridge University Press, 1987.
4. C.H. Bennett. Time/Space Trade-offs for Reversible Computation. SIAM Journal of Computing, 18(4):766-776, 1989.
5. C.H. Bennett, G. Brassard. Quantum Cryptography: Public Key Distribution and Coin Tossing. Proc. IEEE Intl. Conference on Computers, Systems, and Signal Processing, pp 175-179, 1984.
6. C.H. Bennett, D.P. DiVincenzo. Quantum Information and Computation. Nature, 404(6775):247-254, 2000.
7. C.H. Bennett, G. Brassard, C. Crepau, R. Josza, A. Peres, W.K. Wootters. Phys. Reviews Letters, 70, 1895, 1993.
8. C.H. Bennett,, S.J. Wiesner. Communication via one- and two-particle operators on EPR states. Phys. Review Letters, 69(20), 1992.
9. S. Betteli, T. Calarco, L. Serafini. Toward an Architecture for Quantum Programming. LANL Archive cs.PL/0103009, March 2003.
10. E. Bernstein, U. Vazirani. Quantum complexity theory. SIAM Journal of Computing, 26(5):1411-1473, 1997.

11. E. Biham, G. Brassard, D. Kenigsberg, T. Mor. Quantum Computing Without Entanglement. LANL Archive quant-ph/0306182, 2003.
12. D. Bouwmeester, A. Ekert, A. Zeilinger. The Physics of Quantum Information. Springer, Heidelberg, 2000.
13. G. Brassard, I. Chuang, S. Lloyd, and C. Monroe. Quantum Computing. Proc. National Academy of Sciences, USA, vol. 95, p. 11032-11033, 1998.
14. G.K. Brennen, D.Song, C.J. Williams. A Quantum Computer Architecture using Nonlocal Interactions. LANL Archive quant-ph/0301012, 2003.
15. H. Buhrman, R. Cleve, A. Wigderson. Quantum vs. Classical Communication and Computation. Proc. 30th Ann. ACM Symp. Theory of Computing (STOC 98), 1998.
16. C. Carabelea, O. Boissier, A. Florea. Autonomy in Multi-agent Systems: A Classification Attempt. Proc. Intl. Autonomous Agents and Multiagent Systems Conference Workshop on Computational Autonomy, M Rovatso, M Nickles (eds.), Melbourne, Australia, 2003.
17. P.C.W. Davies, J.R. Brown (Eds.). The Ghost in the Atom. Cambridge University Press, Canto edition reprint, 2000.
18. D. Deutsch. Quantum Theory, the Church-Turing Principle, and the Universal Quantum Computer. Proc. Royal Society London A, 400:97, 1985
19. D.P. DiVincenzo. The Pysical Implementation of Quantum Computation. LANL Archive quant-ph/0002077, 2000.
20. A. Einstein, B. Podolsky, N. Rosen. Can quantum mechancial description of physics be considered complete?. Phys. Review, 47:777-780, 1935.
21. L. Grover. A Fast Quantum Mechanical Algorithm for Database Search. Proc. 28th Annual ACM Symposium on Theory of Computation, ACM Press, NY USA, pp 212-219, 1996.
22. Gruska, Imai. Power, Puzzles and Properties of Entanglement. M. Margenster, Y. Rogozhin (eds.), Lecture Notes in Computer Science LNCS, 2055, Springer, 2001.
23. M. Hirvensalo. Quantum Computing. Natural Computing Series, Springer, 2001.
24. A.S. Holevo. Some estimates of the information transmitted by quantum communication channels. Problems of Information Transmission, 9:177-183, 1973.
25. R. Josza. Entanglement and Quantum Computation. Geometric Issues in the Foundations of Science, S. Huggett et al. (eds.), Oxford University Press, 1997.
26. B. Kalyanasundra, G. Schnitger. The probabilistic communication complexity of set intersection. SIAM Journal on Discrete Mathematics, 5(4), 1992.
27. B. Kane. A Silicon-Based Nuclear Spin Quantum Computer. Nature, 393, 1998
28. E. Knill, R. Laflamme, W.H. Zurek. Resilient Quantum Computation. Science, 279:342-345, 1998
29. M. Klusch. Information Agent Technology for the Internet: A Survey. Data and Knowledge Engineering, 36(3), Elsevier Science, 2001.
30. M. Klusch, K. Sycara. Brokering and Matchmaking for Coordination of Agent Societies: A Survey. Coordination of Internet Agents, A. Omicini et al. (eds), Springer, 2001.
31. I. Kremer. Quantum Communication. Master Thesis, Hebrew University, Jerusalem, Israel, 1995.
32. Los Alamos National Lab Archive, USA: http://xxx.lanl.gov/archive/
33. M.A. Nielsen, I.L. Chuang. Quantum Computation and Quantum Information. Cambridge University Press, Cambrige, UK, 2000.
34. B. Oemer. Quantum Programming in QCL. Master Thesis, Technical University of Vienna, Computer Science Department, Vienna, Austria, 2000.
35. M. Oskin, F.T. Chong, I.L. Chuang. A Practical Architecture for Reliable Quantum Computers. IEEE Computer, 35:79-87, January 2002.

36. M. Oskin, F.T. Chong, I.L. Chuang, J. Kubiatowicz. Building Quantum Wires: The Long and the Short of it. Proc. 30th Intnl Symposium on Computer Architecture (ISCA), 2003.
37. M. Ozawa. Quantum Turing Machines: Local Transitions, Preparation, Measurement, and Halting Problem. LANL Archive quant-ph/9809038, 1998.
38. R. Penrose. The Large, the Small, and the Human Mind. Cambridge University Press, 1997.
39. A. Pereira. The Quantum Mind/Classical Brain Problem. NeuroQuantology, 1:94-118, ISSN 1303-5150, Neuroscience & Quantum Physics, 2003.
40. P. Selinger. Towards a Quantum Programming Language. Mathematical Structures in Computer Science, 2003.
41. P. Shor. Algorithms for Quantum Computation: Discrete Logarithms and Factoring. Proc. 35th Annual Symposium on Foundations of Computer Science, Los Alamitos, USA, 1994.
42. A. Steane. Quantum computing. LANL Archive quant-ph/9708022, 1997.
43. M. Steffen, L.M.K. Vandersypen, I.L. Chuang. Toward Quantum Computation: A Five-Qubit Quantum Processor. IEEE Micro, March/April, 2001.
44. K. Sycara, S. Widoff, M. Klusch, J. Lu. LARKS: Dynamic Matchmaking Among Heterogeneous Software Agents in Cyberspace. Autonomous Agents and Multi-Agent Systems, 5(2), 2002.
45. G. Weiss. Introduction to Multiagent Systems. MIT Press, 1999.
46. M. Wooldridge. An Introduction to Multiagent Systems. John Wiley & Sons, Chichester, UK, 2002.
47. W.K. Wootters, W.H. Zurek. A Single Quantum Cannot be Cloned. Nature, 299:802-803, 1982.
48. A.C-C. Yao. Quantum Circuit Complexity. Proc. 33rd Annual Symposium on Foundations of Computer Science (FOCS), pp. 352-361, 1993.
49. P. Zuliani. Logical Reversibility. IBM Journal of Res. & Devel., 45, 2001.