Modelling Parallel Quantum Computing using Transactional Memory

Juliana Kaizer Vizzotto
Centro Regional Sul-CRS
Instituto Nacional de Pesquisas Espaciais-INPE
Santa Maria, Brazil

André Rauber Du Bois
Programa de Pós-Graduação em Informática
Universidade Católica de Pelotas
Pelotas, Brazil

Abstract
We propose a model for parallel quantum computing in a single ensemble quantum computer using Haskell’s software transaction memory. The parallel ensemble quantum computer possesses, besides quantum parallelism, a kind of classical single-instruction-multiple-data parallelism. It explores additional speedup by making quantum computers working in parallel, as in classical computation. The whole state is prepared in such a way a subset of qubits is in a mixed state representing the communicating quantum computers while the other qubits in pure state are the proper argument registers of each quantum computer. Essentially, this particular way of structuring the state of the parallel quantum computer fits with what is well know as multithreading programming. Software transactional memory is a promising new approach to programming shared-memory parallel programs. The functional programming language Haskell elegantly implements this abstraction for concurrent communication.

Keywords: Ensemble quantum computing, parallel quantum computing, transactional memory

1 Introduction

Ensemble quantum computing [3] (EQC) is in general physically realized by some scheme using NMR. It essentially differs from traditional quantum computing only in that it uses many copies of a quantum system (e.g., a liquid solution - such as each molecule is potentially a single quantum computer) and the result of a measurement is the expectation value of the observable, rather than a random eigenvalue. Parallel quantum computing in a single ensemble quantum computer [9] (PQC from here) explores the ensemble to gain additional speedup. Besides quantum parallelism, intrinsic from the use of superposed quantum states, a kind of classical single-instruction-multiple-data parallelism is achieved.
by making quantum systems (the molecules) working in parallel, as in classical computation. In the PQC the whole state is prepared in such a way a subset of qubits is in a mixed state representing the communicating quantum computers while the other qubits in pure state are the proper argument registers of each quantum computer. The authors have shown that the PQC enables additional speedup to important quantum algorithms like Grover and Shor. Specially, unsorted database search can be speedup greatly.

We have noted that this particular way of structuring the state of the PQC fits with what is well know as multithreading programming. Basically, in a multithreading environment, a process has many execution threads, each of which run independently and which may share a common memory area. What is interesting here is that computationally, the PQC quantum state, living in a Hilbert space, is interpreted as global. Hence, all quantum computer of the PQC share a commom global memory area.

That is not new the need of synchronization mechanisms for parallel programs and there are many alternative approaches in the literature, such as locks and mutexes. However has been claimed by several authors [11,8,7] that those programming styles are hard to use and may easily produce programs with errors.

Software transactional memory is a promising new approach to programming shared-memory parallel programs. The functional programming language Haskell elegantly implements this abstraction for concurrent communication.

This work is a stepping stone towards the development of a high level and elegant approach to structure and project parallel quantum algorithms.

2 Parallel Quantum Computing in a Single Ensemble Quantum Computer

The idea in the PQC [9] is to run many copies of quantum systems, which are in the ensemble, in parallel. The goal, as in classical computation, is to achieve additional speedup running tasks in parallel. By running several identical quantum computers in parallel, unsorted database search, for instance, can be speeded up greatly [4].

Consider an EQC quantum computer model with $N_1 = 2^{n_1}$ molecules, such that each molecule can be operated and measured. The PQC computer works in a state called argument register which is divided into two parts: one part with $n_1$ qubits called $n_1$-register and another part with $n_2$ qubits called $n_2$-register, and $n = n_1 + n_2$. Before a computation, the argument register is in a mixed state with $N_1$ constituents. Each constituent is characterized by the state of the $n_1$-register. The $n_2$-register in a given constituent is in a superposed state of its $N_2 = 2^{n_2}$ basis states. The density operator of the ensemble is

$$
\rho = \frac{1}{N_1} \sum_{j_1=0}^{N_1-1} \left[ \sum_{j_2=0}^{N_2-1} c_{j_1,j_2} |j_1,j_2\rangle \langle j_1,j_2| \right]
$$

In the EQC, there are $N_1$ constituents and $N_1$ molecules. Each molecule is in a different state $\sum_{j_2=0}^{N_2-1} c_{j_1,j_2} |j_1,j_2\rangle$, which is a superposition of $N_2$ number of computational basis states.

A unitary transformation on the computation state described above can be denoted by:

$$
\rho \rightarrow \rho_c = U_c \rho U_c^{-1} = \frac{1}{N_1} \sum_{j_1=0}^{N_1-1} \left[ \sum_{j_2=0}^{N_2-1} c_{j_1,j_2} U_c |j_1,j_2\rangle \langle j_1,j_2| U_c^\dagger \right]
$$
This quantum computation is defined as the parallel quantum computing. In fact it is $N_1$ quantum computers working in parallel. The computation $U_c$ can be the same for all molecules, but the databases, numbers represented by different molecules, can be different.

Measurements are treated as average expectation values in the PQC and will be discussed in the further version of this work.

3 Software Transaction Memory in Haskell

In [5], STM Haskell, a new concurrency model for Haskell based on software transactional memory is proposed. In this model, programmers define atomic blocks that are executed atomically with respect to every other atomic block. STM Haskell provides the atomically primitive to define atomic blocks:

$$\text{atomically} :: STM \ a \to IO \ a$$

The atomically primitive takes a memory transaction ($STM \ a$) as an argument and executes it atomically. A memory transaction is committed only if no other transaction has modified the memory its execution depends on. If there was concurrent access to shared variables the transaction is restarted. An execution of atomically block must guarantee [10]:

- **Atomicity**: The effects of an atomically block are visible all at once to other threads
- **Isolation**: The execution of an atomically block can not be affected by the execution of other threads. An atomically block executes as if it had its own copy of the state of the program

Inside of a memory transaction a program can read and write into transactional variables. A variable of type $TVar \ a$ is a transactional variable that can hold a value of type $a$. STM Haskell provides the following primitives for reading and writing on transactional variables:

$$\text{readTVar} :: TVar \ a \to STM \ a$$

$$\text{writeTVar} :: TVar \ a \to a \to STM \ ()$$

The readTVar primitive takes a TVar as an argument and returns an STM action that, when executed, returns the current value of the TVar. The writeTVar primitive is used to write a new value into a TVar. STM actions can be composed together using the same do notation used to compose IO actions in Haskell:

$$\text{addTVar} :: TVar \ Int \to Int \to STM \ ()$$

$$\text{addTVar} \ tvar \ i = \text{do} \ {v \leftarrow \text{readTVar} \ tvar \ ; \ \text{writeTVar} \ tvar \ (v + i)}$$

The addTVar function can be used to read and then write a new value into a TVar. These two actions can be executed atomically by using the atomically primitive:

$$\text{incTVar} :: TVar \ Int \to IO \ ()$$

$$\text{incTVar} \ tvar = \text{atomically} \ (\text{addTVar} \ tvar \ 1)$$

Inside a memory transaction, only pure functions and STM actions can be executed. As a transaction may be aborted and re-run, the type system guarantees that no other irrevocable side-effects like IO actions can be performed inside an atomic block.

STM Haskell also provides a retry$::STM ()$ primitive that is used to abort a transaction so that it can be restarted from the beginning:
\[
\text{withdraw :: TVar Float } \to \text{ Float } \to \text{ STM ()}
\]

\[
\text{withdraw tvar v = do \{ r } \leftarrow \text{readTVar tvar ; if } (r < v) \text{ then retry else writeTVar tvar (r } - v) \}}\]

Transactions can also be composed as alternatives using the orElse function. The transaction \( t_1 \text{ orElse } t_2 \) will first attempt to execute \( t_1 \), if it retries then transaction \( t_2 \) will be executed. If \( t_2 \) also retries then the entire call retries.

4 Quantum Arrows

In an early work [12] we have shown that the superoperators formalism used to express general quantum operations is an instance of a generalization of monads called arrows [6].

In this section, we briefly review state vectors represented as monads and the density matrix approach. Then we discuss how superoperators can be well fit in the concept of arrows. The presentation is in the context of the functional programming language Haskell.

4.1 Vectors as Monads

Given a set \( a \) representing observable (classical) values, i.e. a basis set, a pure quantum state is a vector \( a \to \mathbb{C} \) which associates each basis element with a complex probability amplitude. In Haskell, a finite set \( a \) can be represented as an instance of the class Basis, shown below, in which the constructor \( \text{basis} :: \{a\} \) explicitly lists the basis elements. The basis elements must be distinguishable from each other, which explains the constraint \( \text{Eq a} \) on the type of elements:

\[
\text{class Eq a } \Rightarrow \text{Basis a where basis :: \{a\}}
\]

\[
\text{type K = Complex Double}
\]

\[
\text{type Vec a = a } \to \text{K}
\]

The type \( K \) (notation from the base field) is the type of probability amplitudes.

The monadic functions for vectors are defined as:

\[
\text{return :: Basis a } \Rightarrow \text{Vec a}
\]

\[
\text{return a b = if } a \equiv b \text{ then 1.0 else 0.0}
\]

\[
(\gg ) :: (\text{Basis a}, \text{Basis b}) \Rightarrow \text{Vec a } \to (a \to \text{Vec b}) \to \text{Vec b}
\]

\[
va \gg f = \lambda b \to \text{sum } [(va a) * (f a b) \mid a \leftarrow \text{basis}]
\]

\[
\text{return just lifts values to vectors, and } \text{bind, given a unitary operator (i.e., unitary operator) represented as a function } a \to \text{Vec b, and given a Vec a, returns a Vec b (that is, it specifies how a Vec a can be turned in a Vec b). Actually, as explained in [12], because of the Basis constraint over the sets which we can build vectors, we use a slight more general concept of monads called kleisli structure [1] or indexed monads.}
\]

4.2 Superoperators as Arrows

Intuitively, density matrices can be understood as a statistical perspective of the state vector. In the density matrix formalism, a quantum state that used to be modelled by a vector \( v \) is now modelled by its outer product.

\[
\text{type Dens a = Vec (a, a)}
\]

\[
\text{pureD :: Basis a } \Rightarrow \text{Vec a } \to \text{Dens a}
\]
\[
pureD v = \text{lin2vec} (v) \ast (v)
\]
\[
\text{lin2vec} :: (a \rightarrow \text{Vec} b) \rightarrow \text{Vec} (a, b)
\]
\[
\text{lin2vec} = \text{uncurry}
\]

The function \text{pureD} embeds a state vector in its density matrix representation. For convenience, we uncurl the arguments to the density matrix so that it looks more like a “matrix.”

Operations mapping density matrices to density matrices are called \text{superoperators}:

\[
\text{type} \ Super \ a \ b = (a, a) \rightarrow \text{Dens} b
\]

The application function \( > > \) above defines how the superoperator is going to act over the matrix.

The concept of arrows [6] extends the core lambda calculus with one type and three constants satisfying nine laws. The type is \( A \rightarrow B \) denoting a computation that accepts a value of type \( A \) and returns a value of type \( B \), possibly performing some side effects. The three constants are: \( \text{arr} \), which promotes a function to a pure arrow with no side effects; \( > > > \), which composes two arrows; and \( \text{first} \), which extends an arrow to act on the first component of a pair leaving the second component unchanged.

Just as the probability effect associated with vectors is not strictly a monad because of the \( \text{Basis} \) constraint, the type \( \text{Super} \) is not strictly an arrow as the following types include the additional constraint requiring the elements to be comparable. We have defined the concept of \text{indexed arrows} in [12], which allows the constraint. Bellow we show the instantiation of type \( \text{Super} \) as an arrow.

\[
\text{arr} :: (\text{Basis} b, \text{Basis} c) \Rightarrow (b \rightarrow c) \rightarrow \text{Super} b c
\]
\[
\text{arr} f = \text{fun2lin} (\lambda (b_1, b_2) \rightarrow (f b_1, f b_2))
\]
\[
> > :: (\text{Basis} b, \text{Basis} c, \text{Basis} d) \Rightarrow \text{Super} b c \rightarrow \text{Super} c d \rightarrow \text{Super} b d
\]
\[
f > > g b = (f b > > g)
\]
\[
\text{first} :: (\text{Basis} b, \text{Basis} c, \text{Basis} d) \Rightarrow \text{Super} b c \rightarrow \text{Super} (b, d) (c, d)
\]
\[
\text{first} f ((b_1, d_1), (b_2, d_2)) = \text{permute} \ ((f (b_1, b_2)) \ast (\text{return} (d_1, d_2)))
\]

The function \( \text{arr} \) constructs a superoperator from a pure function by applying the function to both the vector and its dual. The composition of arrows just composes two superoperators using the \text{bind} from Section 4.1. The function \( \text{first} \) applies the superoperator \( f \) to the first component (and its dual) and leaves the second component unchanged. The definition calculates each part separately and then permutes the results to match the required type.

4.3 A Better Notation for Arrows

Following the Haskell’s monadic do-notation, Paterson (2001) presented an extension to Haskell with an improved syntax for writing computations using arrows. We concentrate only on the explanation of new forms which we use in our examples. Here is a simple example to illustrate the notation:

\[
e_1 :: \text{Super} (\text{Bool}, a) (\text{Bool}, a)
e_1 = \text{proc} (a, b) \rightarrow \text{do}
\]
\[
r \leftarrow \text{lin2super hadamard} \prec a
\]
\[
\text{returnA} \prec (r, b)
\]
The do-notation simply sequences the actions in its body. The function return\(A\) is the equivalent for arrows of the monadic function return. The two additional keywords are:

- the arrow abstraction proc which constructs an arrow instead of a regular function.
- the arrow application \(\prec\) which feeds the value of an expression into an arrow.

Paterson (2001) shows that the above notation is general enough to express arrow computations and implemented a Haskell’s module which translates the new syntax to regular Haskell. In the case of \(e_1\) above, the translation to Haskell produces the following code:

\[
e_2 :: Super (Bool, a) (Bool, a) \\
e_2 = \text{first (lin2super hadamard)}
\]

Hence, using the arrows approach in Haskell one can manipulate the quantum state in a high level way. For instance, having defined the right operations, the teleportation algorithm [2] can be programmed as the following:

\[
\text{teleport} :: Super (Bool, Bool, Bool) Bool \\
\text{teleport} = \text{proc (eprL, eprR, q) \rightarrow do} \\
\hspace{1cm} (m_1, m_2) \leftarrow \text{alice} \prec (\text{eprL}, q) \\
\hspace{1cm} q' \leftarrow \text{bob} \prec (\text{eprR}, m_1, m_2) \\
\hspace{1cm} \text{returnA} \prec < q'
\]

The code would be a superoperator which acts over a three qubit density matrix (of type \(\text{Dens (Bool, Bool, Bool)}\)) and returns a one qubit matrix (of type \(\text{Dens Bool}\)). Using superoperators as arrows, the quantum state can be easily manipulated as above.

## 5 Modelling Parallel Quantum Computing using STM

We propose to use density matrices inside TVars:

\[
\text{type } QSt a = \text{TVar (Dens a)}
\]

In such a way we can define a global quantum state which can be accessed and manipulated by all parallel/distributed processes. This seems to be exactly what we need to code the multithreading PQC presented in Section 2. The use of superoperators can greatly help the processes to access only small parts of the state.

The goal of using STM is to synchronize the access of critical parts of the state when doing critical operations like measurements.

A very simple example of an operation on the \(QSt a\) is the identity operation coded below:

\[
\text{qid} :: (\text{Basis } a) \Rightarrow QSt a \rightarrow \text{Super } a a \rightarrow STM () \\
\text{qid qtvar } s = \text{do} \{ d \leftarrow \text{readTVar qtvar} \\
\hspace{1cm} \text{writeTVar qtvar (d }\gg\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!\gg\text{ s)}\}
\]

Teleportation is a typical distributed quantum algorithm. The idea of teleportation is to disintegrate an object in one place making a perfect replica of it somewhere else. Instead quantum teleportation [2] enables the transmission, using a classical communication channel, of an unknown quantum state via a previously shared epr pair.

Using arrows and the notation introduced by Patterson, we have expressed quantum teleportation in [12].

We break the algorithm in two individual procedures, alice and bob. Besides the use of the arrows notation to express the action of superoperators on specific qubits, we incor-
porate the measurement in Alice’s procedure, and trace out the irrelevant qubits from the answer returned by Bob.

\[
\begin{align*}
\text{alice} &:: \text{Super}(\text{Bool}, \text{Bool}) (\text{Bool}, \text{Bool}) \\
\text{alice} = &\text{proc} (\text{eprL}, q) \to \text{do} \\
& (q_1, e_1) \leftarrow (\text{lin}2\text{super} (\text{controlled \, qnot})) \prec (q, \text{eprL}) \\
& q_2 \leftarrow (\text{lin}2\text{super} \, \text{hadamard}) \prec q_1 \\
& ((q_3, e_2), (m_1, m_2)) \leftarrow \text{meas} \prec (q_2, e_1) \\
& (m_1', m_2') \leftarrow \text{trL} ((q_3, e_2), (m_1, m_2)) \\
& \text{return} A \prec (m_1', m_2') \\
\text{bob} &:: \text{Super}(\text{Bool}, \text{Bool}, \text{Bool}) \, \text{Bool} \\
\text{bob} = &\text{proc} (\text{eprR}, m_1, m_2) \to \text{do} \\
& (m_2', e_1) \leftarrow (\text{lin}2\text{super} (\text{controlled \, qnot})) \prec (m_2, \text{eprR}) \\
& (m_1', e_2) \leftarrow (\text{lin}2\text{super} (\text{controlled \, z})) \prec (m_1, e_1) \\
& q' \leftarrow \text{trL} (q_1', m_2') \prec (m_1, m_2) \\
& \text{return} A \prec q'
\end{align*}
\]

Having defined Alice and Bob procedures we can now codify the teleportation procedure using the \textit{QSt}. The idea is to arrange the state inside the \textit{QSt} as proposed in Section 2. In this way we will have a quantum state shared by Alice and Bob. The first qubit inside the \textit{QSt} is the identifier, saying if the state is from Alice or Bob.

6 Conclusion

We have proposed a model for parallel quantum computing in a single ensemble quantum computer using Haskell’s software transaction memory. We hope this approach will give us a simple and high level way to write and develop parallel quantum algorithms.

Acknowledgements

We would like to thank our colleagues Amr Sabry and Antônio Carlos da Rocha Costa for interesting discussions and feedback on our work.

References


