

Abstract

In the quantum computational framework, there are polynomial time solving algorithms for problems having exponential classical solutions. The quest is - on one hand - to search if there are other possible effective quantum algorithms and - on the other hand - to be able to produce efficient implementations for the already known algorithms. The most feasible implementation of quantum algorithms is based on the quantum circuit (gate network) model.

Our work aims at bridging the gap between classical hardware CAD with design automation techniques, and quantum circuit design rules. This attempt would be extremely difficult without the possibility of the efficient quantum circuit simulation. Thus, our first direction was to try using Hardware Description Languages (HDLs) for simulating quantum circuits, because their property of being able to describe - in a compact manner - the circuit with both structural and behavioral (functional) architectures isolates the inner source of simulation complexity: the entanglement. Our analysis showed that the probability of simulation improvement just by using the HDL procedure is small. Therefore, we developed a special algorithm for avoiding entangled state representations, the *bubble bit technique*, which is effective at least when dealing with specific algorithm states. Our simulation framework has the ability of fault injection, in order to create incentive for validation of quantum circuit fault tolerance strategies and algorithms. The other direction of this Ph.D. work is to find common ground for reliability techniques and assessment methodologies from the Embryonics project and fault tolerant quantum computation. Embryonics is a biologically inspired reconfigurable hardware project, which is suitable for attaining reliability in aggressive, critical environments, similar to quantum computation in terms of fault model and fault occurrence frequency. Adopting the accuracy threshold as reliability measure in Embryonic memories is benefic. Also, when considering a reconfigurable strategy (reconfigurable quantum gate arrays - rQGAs) in quantum computation fault tolerant stabilizer encoding, the appropriate reliability measure is drastically improved.

When entanglement is not present, it is possible to describe the circuit and the processed quantum states in a structural manner, employing only polynomial resources for simulation. By contrast, when entanglement is detected in the processed state, the circuit has to be described with a behavioral architecture, and exponential resources must be used in this case. That happens because, when entanglement occurs between two quantum subsystems, their overall state cannot be represented correctly as a reunion (assuming implicit tensor product state composition) of the two individual subsystem states. The practical implementation of the initial simulation methodology requires that each circuit be described both by structural and functional (behavioral) architectures. For a gate network, if entanglement is detected in the previous or next quantum state, then the functional architecture has to be selected to describe it; otherwise the structural architecture is chosen. We adopted the matrix representation of quantum states and unitary operators; therefore the quantum states are type array of complex signals. Efficient automated extraction of non-entangled qubit group states is not conceivable unless we have some *a priori* information about the overall state: the so-called *simulation shortcuts*. When dealing with states from certain points in the circuits imple-

menting specific algorithms, we have that knowledge because of the characteristic form these states exhibit. We have performed an analysis concerning the effectiveness of our methodology, for specific states from Shor and Grover algorithms. Unfortunately, as shown by our case study for Shor, Deutsch-Jozsa and Grover algorithms, the probability of success for the extraction algorithms is decreasing exponentially with the number of qubits in the processed state. Nevertheless, the HDL-based simulation methodology can be further improved. The bubble bit coding technique creates a new entanglement-free-represented state. Therefore, the simulation works with equivalent gate networks operating on corresponding bubble-coded non-entangled states, and after applying the unitary operator the original state can be restored. This way, the unitary transform is obtained with at most $n [2 \times 1]$ -size matrixes, with the expense of memorizing $\mathcal{O}(n^2)$ size records. The bubble bit procedure can also be used for simulated fault injection, according to the fault models. We present here experimental and assessment results describing the most important contributions of our Ph.D. work in the simulation part. The simulation runtimes show an important runtime improvement at the expense of a polynomial memory overhead, as compared with our reference simulator (QuIDD Pro, developed by the Quantum Circuits Group at University of Michigan).

The need for fault tolerance is vital in quantum computation, due to the omnipresent nature of quantum decoherence errors. A specific reliability parameter was defined, under the form of the *accuracy threshold*. If the quantum circuit's fault tolerance dictates accuracy greater or equal with the threshold, then it could be used for arbitrary long reliable quantum computation. The quantum circuit fault tolerance techniques - even the most recent ones - use the concatenated coding for both protected data and ancilla qubits. Our reconfigurable quantum hardware strategy employs a quantum nature (i.e. superposition of classical basis states) configuration register in order to have a superposition of error detection and correction circuits at the same time. The starting idea is that if the gate error probability is ξ , and we have k superposed correction circuits then, after the measurement of the configuration register, the overall circuit error probability becomes ξ^k (negligible for a small ξ). We developed a reconfigurable quantum circuit, the so-called reconfigurable Quantum Gate Array (rQGA), which we assessed with the accuracy threshold measure. Our analytical estimate of the accuracy threshold shows that the rQGA solution clearly dominates the actual technologic accuracy limit, thus allowing for arbitrary long fault tolerant quantum computation. This way, the rQGA technique can replace the concatenated coding, a solution that is vulnerable in the presence of correlated faults.

The last part of the thesis is dedicated to the implementation of the Quantum Genetic Algorithms (QGA). Our solution is based on an already known quantum algorithm (the maximum finding algorithm) and on a specially designed oracle, which reduces the entire QGA problem to Grover's search algorithm. The conclusion is that the genetic strategy is not applicable to the quantum computation environment, with the crossover and mutation genetic operators becoming useless. The complexity of the proposed Reduced Quantum Genetic Algorithm is linear, thus proving the superiority of the quantum computing in yet another computation field.

Rezumat

În cadrul computației cuantice există algoritmi care rezolvă în timpi polinomiali probleme care au soluții clasice exponențiale. Obiectivul este – pe de o parte – de a proiecta alți algoritmi cuantici eficienți și – pe de altă parte – de a putea produce implementări eficiente pentru algoritmi deja cunoscuți. Cea mai fezabilă implementare a algoritmilor cuantici este bazată pe modelul circuit (sau rețea de porți). Lucrarea noastră este concepută pentru a face legătura între proiectarea asistată de calculator (CAD) din hardware-ul clasic, bazată pe proiectarea automatizată, și regulile de proiectare ale circuitelor cuantice. Această tentativă ar fi extrem de dificilă în absența posibilității de a simula circuitele cuantice în mod eficient. Astfel, prima direcție a acestei teze de doctorat constă în încercarea de a folosi limbajele de descriere hardware (HDL) pentru simularea circuitelor cuantice, datorită proprietății acestora de a putea descrie – într-o manieră compactă – circuitul cu arhitecturi structurale și comportamentale (funcționale) și care face ca izolarea entanglement-ului ca sursă principală a complexității de simulare să fie posibilă. Analiza pe care am efectuat-o arată faptul că probabilitatea de a reduce timpii de simulare doar prin folosirea procedurii de simulare HDL este mică. Prin urmare, am dezvoltat un algoritm special, pentru evitarea reprezentărilor afectate de entanglement ale stărilor cuantice, așa-numita tehnică *bubble bit*, care este eficientă cel puțin atunci când sunt procesate stări specifice anumitor algoritmi. Metodologia noastră de simulare este înzestrată și cu abilitatea de a injecta defecte, în ideea de a face posibilă procedura de validare a strategiilor și algoritmilor de toleranță la defectare. Cealaltă direcție a activității doctorale reflectate în această teză constă în încercarea de a găsi teren comun pentru tehnicile de fiabilizare și metodologiile de evaluare aferente proiectului Embryonics pe de o parte, și calculul cuantic tolerant la defecte pe de altă parte. Embryonics este un proiect hardware inspirat din biologie, care este pretabil obținerii fiabilității în medii critice, agresive, similare calculului cuantic în termeni de model al defectului și al frecvenței de apariție. Adoptarea *pragului de acuratețe* ca măsură a fiabilității în memoriile Embryonics este benefică. Deasemenea, atunci când luăm în considerație o strategie reconfigurabilă (matrici reconfigurabile de porți cuantice – rQGAs) pentru computația cuantică tolerantă la defectare și coduri stabilizatoare, se îmbunătățește drastic gradul de fiabilitate.

Atunci când fenomenul de entanglement nu este prezent, este posibil să descriem circuitul cuantic și stările procesate în manieră structurală, revendicând doar resurse polinomiale pentru simulare. În schimb, atunci când entanglement-ul este detectat în starea procesată, circuitul trebuie să fie descris printr-o arhitectură comportamentală, și simularea va dicta acum utilizarea unor resurse exponențiale. Acest lucru se întâmplă deoarece, atunci când apare entanglement-ul pentru două subsisteme cuantice, starea lor generală nu poate fi reprezentată corect ca simpla reuniune a stărilor cuantice aferente celor două subsisteme individuale (am presupus că produsul tensorial este unealta implicită de compunere a stărilor individuale). Implementarea practică a metodologiei inițiale de simulare necesită ca fiecare circuit să fie descris prin ambele arhitecturi: structurală și comportamentală (funcțională). Dacă pentru o rețea de porți cuantice entanglement-ul este detectat în starea precedentă sau următoare, atunci arhitectura funcțională este selectată pentru a o descrie; altminteri se selectează arhitectura structurală. În cadrul acestei abordări, am ales reprezentarea matriceală a stărilor cuantice și a operatorilor unitari; prin urmare, stările cuantice sunt reprezentate ca tip vector de numere complexe. Extragerea automată eficientă, a stărilor cuantice reprezentând

grupuri de qubiți care nu se află în entanglement, nu este de conceput fără a avea la dispoziție informație *apriorică* referitoare la starea cuantică generală: așa-numitele *scurtături de simulare*. Atunci când avem de a face cu stări din anumite puncte ale circuitelor ce implementează algoritmi specifici, vom avea la dispoziție acea informație apriorică, datorită aspectului caracteristic pe care îl au aceste stări. Am efectuat o analiză privitoare la eficiența metodologiei de simulare HDL, pentru stări specifice din algoritmi Shor și Grover. Din nefericire, așa cum se arată în studiul nostru de caz pentru algoritmi Shor, Deutsch-Jozsa și Grover, probabilitatea ca algoritmi de extracție să fie încununați de succes descrește exponențial cu numărul de qubiți ai stării procesate. Fără îndoială, metodologia de simulare bazată pe limbajele de descriere hardware (HDLs) poate fi îmbunătățită în continuare. Tehnica de codificare bubble bit crează o nouă reprezentare lipsită de entanglement. Prin urmare, simularea se face cu rețele de porți cuantice echivalente ce operează pe stări codificate prin metoda bubble bit; după aplicarea transformării unitare starea originală poate fi restaurată. În acest fel, transformarea unitară este obținută cu cel mult n matrici de dimensiune $[2 \times 1]$, cu prețul memorării unor înregistrări de dimensiune $\mathcal{O}(n^2)$. Procedura bubble bit poate deasemenea să fie folosită pentru injecția simulată de defecte, în concordanță cu modelul de defectare. În cadrul acestei lucrări se prezintă rezultate experimentale și analitice ce descriu cele mai importante contribuții în domeniul simulării HDL-bubble-bit. Timpii de simulare arată o îmbunătățire semnificativă cu prețul unui consum suplimentar polinomial de memorie, prin comparație cu simulatorul referință (QuIDD Pro, dezvoltat de către Quantum Circuits Group de la University of Michigan).

Necesitatea toleranței la defectare este vitală în calculul cuantic, datorită naturii omniprezente a erorilor de decoerență. În plus, a fost definit un parametru specific fiabilității, sub forma *pragului de acuratețe*. Dacă toleranța la defectare a circuitului cuantic dictează o acuratețe mai mare sau egală cu pragul, atunci poate fi folosit pentru un calcul cuantic fiabil pe o perioadă arbitrar de lungă. Tehnicile de toleranță la defectare pentru circuitele cuantice (chiar și cele mai recente) folosesc codificarea concatenată atât pentru datele codificate cât și pentru qubiții auxiliari (ancilla). Strategia noastră pentru hardware-ul cuantic face uz de un registru de configurare de natură cuantică (superpoziție de stări clasice ale bazei), pentru a avea o superpoziție simultană de circuite corectoare de erori. Ideea de plecare este că dacă probabilitatea de defectare a porților este ξ , și avem k circuite corectoare de erori superpuse, atunci, după măsurarea registrului de configurare, probabilitatea de apariție a erorii în circuitul ca întreg devine ξ^k (neglijabilă pentru un ξ suficient de mic). Am proiectat un circuit reconfigurabil cuantic (rQGA), pe care l-am evaluat cu ajutorul pragului de acuratețe. Estimarea noastră analitică pentru pragul de acuratețe demonstrează că soluția rQGA este mult deasupra limitei tehnologice de acuratețe, permițând calculul cuantic tolerant la defectare arbitrar de lung. Astfel, tehnica rQGA poate înlocui codificarea concatenată, o soluție vulnerabilă la acțiunea defectelor corelate.

Ultima parte a tezei este dedicată implementării Algoritmilor Genetici Cuantici (QGA). Soluția propusă este bazată pe un algoritm cuantic deja cunoscut (algoritmul găsirii maximumului) și pe un oracol proiectat în mod special, care reduce întreaga problemă rQGA la algoritm de căutare al lui Grover. Concluzia este că strategia genetică nu poate fi aplicată în mediul computațional cuantic, deoarece operatorii genetici de crossover și mutație sunt inutili. Complexitatea algoritmului propus (Reduced Quantum Genetic Algorithm) este liniară, probând astfel superioritatea calculului cuantic într-un nou domeniu computațional.