

ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო
უნივერსიტეტის ზუსტი და საბუნებისმეტყველო მეცნიერებათა
ფაკულტეტი

სამაგისტრო პროგრამა ინფორმაციული ტექნოლოგიები

ქადაგიშვილი დავითი

ქვანტური კომპიუტერული ტექნოლოგიების არქიტექტურული
იმპლიკაცია

ნაშრომი შესრულებულია ინფორმაციული ტექნოლოგიების მაგისტრის
აკადემიური ხარისხის მოსაპოვებლად

ნაშრომის ხელმძღვანელი: პაატა კერვალიშვილი
ფიზიკა-მათემატიკის მეცნიერებათა დოქტორი

თბილისი
2014

ანოტაცია

ნაშრომში წარმოდგენილია თანამედროვე კომპიუტერულ სისტემების არქიტექტურის მახასიათებლებზე დაფუძნებული ქვანტური გამოთვლითი ტექნოლოგიების კლასიფიკაცია. ასევე აღწერილია ქვანტური გამოთვლითი პროცესების გაშვების ინჟინერული გადაწყვეტილებები, ქვანტური მდგომარეობის დეკოჰერენცია და მოცემული სისტემების ზომები. განხილულია რამოდენიმე ტექნოლოგიური გამოწვევა რომლის პარალელიზმი, ტევადობა და ქსელური ურთიერთკავშირის ტოპოლოგია განსაზღვრავს ალგორითმულ ეფექტურობას, ხოლო ქვანტური შეცდომების გასწორება და საჭირო ქვანტური მდგომარეობის გაზომვა უზრუნველყოფს ლოგიკური მთვლელის სისწრაფეს. ტაქსონომიის გამოყენებით მიღებული არითმეტუკული სქემისთვის გამოკვლეულია არქიტექტურული იმპლიკაცია, ნაჩვენებია ქვანტური შეცდომების გასწორების იმპლიმენტაცია და განხილულია კლასტერული ქვანტური გამოთვლები.

Anotation

In this article we present a classification scheme for quantum computing technologies that is based on the characteristics most relevant to computer systems architecture. The engineering trade-offs of execution speed, decoherence of the quantum states, and size of systems are described. Concurrency, storage capacity, and interconnection network topology influence algorithmic efficiency, while quantum error correction and necessary quantum state measurement are the ultimate drivers of logical clock speed. We discuss several proposed technologies. Finally, we use our taxonomy to explore architectural implications for common arithmetic circuits, examine the implementation of quantum error correction, and discuss cluster-state quantum computation.

სარჩევი

შესავალი	4
1. ფუნდამენტური მოთხოვნილობები	7
2. ტექსონომიის საფუძვლები	9
2.1 ძირითადი მახასიათებლები	9
2.2 მაწარმოებელი და ოპერირებლული გარემო	12
2.3 ალგორითმული ეფექტურობის მახასიათებლები	13
2.4 დროის და კარიბჭის მახასიათებლები	15
2.5 სხვა მახასიათებლები	17
3. ქვანთური ტექნოლოგიები	20
3.1 NMR გადაწყვეტა	22
3.2 იოსეფსონის გადაკვეთა	23
3.3 სილიციუმის NMR	27
3.4 სკალირებადი იონური ხაფანგი	28
3.5 ოპტიკური მთვლელები	30
3.6 ქვანთური ნაწილაკის დამუხტვა	31
3.7 კეინის მოდელი	32
4. არქიტექტურა და აპლიკაცია	33
4.1 არითმეტიკა	33
4.2 შეცდომების მართვა	37
4.3 კლასტერული მდგომარეობის გამოთვლა	38
დასკვნა	39
გამოყენებული ლიტერატურა	41

შესავალი

ქვანტური გამოთვლები წარმოადგენს განვითარებად სფეროს. მკვლევარები მოტივირებულნი არიან კლასიკურ მანქანებზე შედარებით უფრო დიდი გამოთვლითი პოტენციალით. დღესდღეობით ამ საკითხზე კვლევა ძირითადად ფოკუსირებულია ორ უკიდურეს მიმართულებაზე: დაწყებული ალგორითმების და კომპლექსურობის თეორიით, დამთავრებული ქვანტური კარიბჭეების და ქუბითების შენახვის ტექნოლოგიებით. არქიტექტურის როლი ამ პრობლემის მოსაგვარებლად, მოახდინოს ქვანტური ალგორითმების ეფექტურად მუშაობა პრაქტიკულ მანქანებში, დღესაც ჩამოყალიბების პროცესშია.

ამ სისტემების არქიტექტურის ფორმირება არ შეიძლება იყოს მეორეხარისხოვანი. კარგად შემუშავებული სისტემა იქნება უფრო სწრაფი, მაღალი თავსებადობის უნარიანი და შეცდომების მიმართ მდგრადი ვიდრე იგივე საბაზისო ტექნოლოგიაზე აგებული სისტემა. ამის შედეგად მას ექნება უნარი გადაწყვიტოს უფრო დიდი და საინტერესო პრობლემები. სისტემურ არქიტექტურას აგრეთვე შეუძლია სისტემური დონის კომპრომისებით, ფარდობითი მნიშვნელობით და სხვადასხვა ტექნოლოგიური თავისებურების საჭირო სასრული დონის დემონსტრირებით ხელი შეუწყოს კვლევითი პროგრამის მექანიზმის ფორმირებას. ამგვარად, ქვანტური კომპიუტერების სისტემის არქიტექტურას აქვს გადამწყვეტი მნიშვნელობა მათ მნიშვნელოვან კვლევით სფეროში და წარმატებაში.

ამ ნაშრომში ჩვენ შევეცდებით არქიტექტურის კუთხით მომუშავე მკვლევარებზე დაყრდნობით შევქმნათ გეგმა ტაქსონომიის სახით და განვიხილოთ რამოდენიმე პერსპექტიული ქვანტური გამოთვლითი ტექნოლოგია. ასევე ჩვენ ქვანტური არითმეტიკული ალგორითმების შეფასებით, ქვანტური შეცდომების გასწორებით და კლასტერულ ქვანტურ გამოთვლების გამოყენებით გარკვეულ ჭრილში მოვახდენთ იმის დემონსტრირებას, თუ როგორ ავსახოთ ინფორმაცია მოცემული ტაქსონომიიდან.

როდესაც განვიხილავთ ახალ ქვანტურ გამოთვლით ტექნოლოგიის საკითხს, ბუნებრივია გაჩნდეს შემდეგი შეკითხვები:

1. მუშაობს თუ არა (ან შეიძლება თუ არა ამუშავება)?

2. როგორ უნდა აკონტროლო(მოწყობილობა და პროგრამული უზრუნველყოფა)?
3. როგორია მისი მაშტაბები?
4. რამდენად სწრაფია?
5. რის დათმობა მოგვიწევს მის განახორციელებლად?

ამ ნაშრომში ჩვენ ყურადღებას გავამახვილებთ 2-5 შეკითხვაზე, ასევე ყურადღება დაეთმობა 1 შეკითხვის პასუხის არსებულ მდგომარეობას. შეკითხვა 1 მედწილად მოწყობილობის ფიზიკოსებისთვისაა, თუმცა აქრქიტექტორები უნდა აცნობიერებდნენ მაღალ სკალირებად სისტემის პოტენციურ გამოწვევებს, ვინაიდან საბოლოო ჯამში ქვანტური კომპიუტერის შექმნისას ეს გამოწვევა აუცილებლად იჩენს თავს. გარდა ამისა არქიტექტორებს პროექტირების გამოცდილების გამოყენებით შეუძლიათ ამ პრობლემების გარკვეულ წილად გაადვილება.

შეკითხვა 2 მნიშვნელოვანია აქრქიტექტორებისთვის, ვინაიდან ქვანტური ტექნოლოგიების კლასიკური კონტროლი არის რთული არქიტექტურული პრობლემა. რამოდენიმე ასეთი ტექნოლოგია საშუალებას მოგვცემს მოვახდინოთ კლასიკური ლოგიკის ინტეგრირება ქვანტურ ბიტებთან (ქუბიტებთან), ხოლო დანარჩენი ტექნოლოგია გამოიყენებს კლასიკურ კონტროლს. მოწყობილობის ქვანტური მხარის პარალელიზმი, ოპერაციის სისწრაფე, სწრაფი, ზუსტი ქუბითური გაზომვები და კონტროლი საჭიროებს მაღალსიჩქარიან ინტერფეის რომელიც დააკავშირებს სუბსისტემას და თავად ქვანტურ მოწყობილობას.

შეკითხვა 3 გადამწყვეტი მნიშვნელობისაა. თუ ვერ მოხერხდა ასობით და ათასობით პროგრამული დონის ქუბიტებისგან მაღალ სკალირებად სისტემის აგება, მაშინ მოწყობილობა ვერასოდეს იქნება დასრულებული. თუმცა შეკითხვა პასუხის გასაცემად საკმაოდ კომპლექსურია, ის დამოკიდებულია როგორც ტექნოლოგიურ ზღვრებზე, ასევე ფუნდამენტურ ფიზიკურ თავისებურებებზე. ამგვარად , სკალირებას მოგვიანებით განვიხილავთ.

ამ ტექნოლოგიების სიჩქარე (შეკითხვა 4) არის მნიშვნელოვანი ორი მიზეზით: პირველი, გამოთვლების სიჩქარე დაკავშირებულია ამ გამოთვლების შეცდომების სიხშირეზე (დეკონჰერენციაზე) რომელიც განსაზღვრავს ქვანტური კომპიუტერის შესაძლებლობის და

შექმნის საკითხს. მეორე, მიუხედავად იმისა რომ ქვანტურ გამოთვლით მოდელს აქვს კლასიკური მანქანების მსგავსი პრობლემები, ქვანტური ალგორითმების გამოყენებით, საინტერესო შედეგის გამოსათვლელად საჭიროა კარიბჭეების დიდი რაოდენობა. კილობიტური ზომის რიცხვების ფაქტორი მაგ. $O(n^3)$. მყიფე ქვანტური მდგომარეობის შეცდომათა სიხშირის გასამკლავებლად, ჩვეულებრივი მუდმივა (რომელიც შეიძლება იყოს ასობით და ათასობით) მათ რიცხვში უნდა ჩაითვალოს. ამგვარად, ძირითადი გამოთვლითი სიჩქარე ქვანტური სისტემების და მათი საბოლოო გამოყენებისთვის კვლავ მნიშვნელოვან ფაქტორად რჩება.

და ბოლოს, შეკითხვა 5 წარმოადგენს არქიტექტორული კვლევის მთავარ ასპექტს. ჩვენ შევისწავლით სხვადასხვა ტექნოლოგიების თავისებურებებს, რომლებიც იქნება ერთმანეთთან ურთიერთშეთანხმებული. მაგაითად, რამოდენიმე კარიბჭის ამუშავება სასურველია როგორც შეცდომების გასწორების მხრივ, ასევე პროგრამული ალგორითმებისთვის. მიუხედავად იმისა რომ რამოდენიმე ტექნოლოგიის არქიტექტურის წარმოება კომპლექსური და ძვირადღირებულია (მაგ. იონური ხაფანგის სისტემებისთვის დიდი რაოდენობით ლაზერის მოთხოვნილება), სხვა ტექნოლოგიების პარალელიზმი, უფრო მაღალ ცდომილობის სიხშირეში ან კომპლექსურ სიგნალთა დამუშავებაში შედეგის მომტანია (მაგ. ატომურ მაგნიტურ რეზონანსულ სისტემაში ქუბითების იზოლაცია).

ამ ნაშრომისის წაკითხვა არ მოითხოვს ქვანტური გამოთვლების თეორიის დეტალურ ცოდნას. შემდეგ თავში ჩვენ აღვწერთ ცნობილ ქვანტურ გამოთვლითი მოწყობილობების ცნობილ ფუნდამენტურ კრიტერიუმებს, ხოლო შემდეგ მოცემული ტაქსონომიის საფუძვლებს. 4 თავში ეს საფუძვლები გამოყენებულია რამოდენიმე პერსპექტიული ქვანტური ტექნოლოგიების კონტექსტში. 5 თავში მოცემულია პროგრამების, არქიტექტურის და ტექნოლოგიის ურთიერთკავშირის რამოდენიმე გზა; ხოლო 6 თავში გამოვიტანთ ამ განხილვის დასკვნას.

1. ფუნდამენტური მოთხოვნები

დივინჩენომ (1995 წ). აღწერა ხუთი მახასიათებელი, რომელიც უნდა გააჩნდეს რეალურ ქვანტურ გამოთვლით მოწყობილობას. ქვანტური კომპიუტერი უნდა :

1. იყოს სკალარული ფიზიკური სისტემა, კარად განსაზღვრული ქუბითებით.
2. იყოს გამოთვლამდე ინიციალიზებადი საჭირო მდგომარეობაში.
3. ქონდეს ადეკვატური სიდიდის დეკოჰერენცირების დრო.
4. ქონდეს უნივერსალური ქვანტური კარიბჭეების წყობა.
5. ქონდეს მაღალი ეფექტურობის ქვანტური გაზომვების უნარი.

დანარჩენი ორი კრიტერიუმი ფოკუსირებულია ქვანტური ინფორმაციის ერთ ქვანტურ კომპიუტერიდან მეორეში გადატანაზე. ქმედითუნარიან ქვანტურ საკომუნიკაციო ტექნოლოგიას უნდა :

6. შეემდოს სტაციონარული და მოძრავი ქუბითების ფიზიკურ რეალიზაციებში გადაყვანა.
7. შეემდოს ქუბითის ფიზიკური რეალიზაციის განსაზღვრულ ლოკაციებში საიმედოდ გადაცემა.

ამ კრიტერიუმების არსი საკმაოდ მარტივია. 1 პუნქტი ნიშნავს იმას, რომ უნდა არსებობდეს რაიმე ფიზიკური ობიექტი , როგორიცაა ენერგო დონის იონი, ფოტონის პოლარიზაცია, ან ელექტრონის სპინი, რომელიც ფაქტიურად იქნება ქუბითის გადამზიდავი. ის უნდა შეესაბამებოდეს ქვანტური თვისების ძირითად კრიტერიუმს და ქონდეს ორი მდგომარეობის მხარდაჭერა, რომელიც შეიძლება აღვიქვათ როგორც 0 და 1. 1 პუნქტი ასევე ეხება „სკალარულობას“, რასაც სხვადასხვა კონტექსტში სხვადასხვა მნიშვნელობა გააჩნია; ჩვენ ამ ასპექტებსაც განვიხილავთ. 2 პუნქტი საკმაოდ ცხადია: ის უბრალოდ „შეტანა - გამოტანის“ პრინციპის ინტერპრეტაციაა.

დეკოჰერენციის კრიტიკული საკითხი, ან ქვანტური მდგომარეობის დაკარგვა (3 პუნქტი) წარმოადგენს დროის, კარიბჭეების შეცდომების და ქუბითების ტრანსპორტირების საკითხს. ფუნდამენტური და თეორიული გათვლები ქმნიან ზღვარს, რომ

ქვანტური კომპიუტერი ვერ შეძლებს ფუნქციონირებას 10^{-4} შეცდომაზე ან 10^4 კარიბჭიდან თითო შეცდომის გამოვლენის შემთხვევაში. [იაკირ აპარონოვი და ბენორი 1999]. ქვანტური ტექნოლოგიები საჭიროებს შეცდომების სიხშირის მოცემულ ზღვარზე დაბლა დაყვანას, იმისთვის რომ თავიდან ავიცილოთ შეცდომების გასწორების პროცესში გაუთვალისწინებელი შედეგები. ტექნოლოგიური და არქიტექტურული გათვლები ხანდახან შეიძლება დრამატულად განსხვავდებოდეს თეორიული ზღვრისგან, რომელსაც შემდგომ განვიხილავთ.

4 კრიტერიუმის დასაკმაყოფილებლად კომპიუტერს უნდა შეეძლოს მცირე რაოდენობის „უნივერსალური კარიბჭეების“ გამოთვლა, რომელის შესაძლებელი იქნება გამოყენებულ იქნას უფრო დიდი და კომპლექსური კარიბჭეების სინთეზისთვის. ეს იმას ნიშნავს რომ კლასიკურ კომპიუტერულ ტექნოლოგიას როგორც მინიმუმ უნდა შეეძლოს NOR ან NAND ოპერაციის შესრულება. ქვანტური კომპიუტერებისთვის ერთ-ერთ ასეთ უნივერსალურ კარიბჭეების ნაკრებს წარადგენს X, H, T, და CNOT კარიბჭეები. მნიშვნელოვანია ვიცოდეთ, რომ X, H და T კარიბჭეები ერთბიტიანი ოპერაციებია, ხოლო CNOT მოიცავს 2 ქუბიტს. ასევე მნიშვნელოვანია, რომ X, H და CNOT შედარებით მარტივია შეცდომების გასწორების მიმართ, მაშინ როცა T მოითხოვს უფრო კომპლექსურ სქემას.

5 პუნქტი მოითხოვს ქუბიტების მდომარეობის წასაკითხად საჭირო, საიმედო გზის არსებობას. გამოთვლების დასასრულს მიღებულ შედეგზე უფრო მნიშვნელოვანია გაზომვა, რომელიც საჭიროა განვახორციელოთ ქვანტური შეცდომების გასწორების თითქმის უწყვეტ რეჟიმში და ასევე დარღვევების მიმართ ტოლერანტული კარიბჭეების კოდურ ბიტებზე გაშვების პროცესში.

6 და 7 პუნქტები უშუალოდ გამოთვლების მიზნით ქვანტური ინფორმაციის დიდ მანძილზე გადატანას უკავშირდება. 6 პუნქტის ერთ-ერთი მნიშვნელოვანი შენიშვნა გახლავთ ის, რომ იგი ასიხაზება მხოლოდ იმ სისტემებზე, რომლებიც გამოითვლიან ქვანტურ ალგორითმებს საერთო მდგომარეობების მეშვეობით. ის არ იმუშავებს სხვა ისეთ ქვანტურ ეფექტების გამოყენებებში, როგორიცაა ქვანტური კრიპტოგრაფია და ქვანტური ტელეპორტაციის ძირითადი დემონსტრირებები. [ბენეტი 1993, ფურუსავა 1998] (თუმცა

ტელეპორტაცია შესაძლებელია გამოყენებულ იქნას ქვანტურ კომპიუტერულ არქიტექტურაში. [გოთსმანი 1997]).

ეს კრიტერიუმები გამოყენებულია როგორც ქვანტური გამოთვლის ევოლუციის საწყისად. [ნილსენი და ხუანგი 2000, ARDA 2004]. ის წარმოადგენს შესაძლებლობების ნაკრებს, მაგრამ არ არის საკმარისი ქვანტური კომპიუტერის აგების სირთულის ან მისი სიჩქარის და გამოყენების გასააზრებლად.

2. ტაქსონომიის საფუძვლები

იმისათვის, რომ შევქმნათ არქიტექტურული კვლევების შემფასებელი ქვანტური კომპიუტერული ტექნოლოგიებისთვის საჭირო სახელმძღვანელო, უნდა შევქმნათ კლასიფიკაციურ კრიტერიუმთა ნუსხა. ამ ნაშრომში აღვწერთ თითოეულ კრიტერიუმს და ასევე რამოდენიმე მის არქიტექტურულ იმპლიკაციას. მომდევნო თავში ჩვენ გამოვიყენებთ ამ ტაქსონომიას რამოდენიმე კომპიუტერული ტექნოლოგიის შეფასებისთვის.

2.1 ძირითადი მახასიათებლები

სტაციონატული, მფრინავი და მობილური. ქვანტური კომპიუტერული ტექნოლოგიები შეიძლება დავყოთ ორ კატეგორიად: სადაც ქუბითები წარმოდგენილია როგორც მუდმივად მოძრავი მოვლენა (ფოტონები), და სადაც ქუბითები წარმოდგენილია როგორც სტატიკური მოვლენა (ატომური ელექტრო სპინები). მოძრავი მოვლენისთვის კარიბჭეები არის ფიზიკური მოწყობილობა, რომელიც მოქმედებს ქუბითზე თუ როგორ გამოივლის კარიბჭეს. ასეთ ქუბითებს ეწოდება „მფრინავი ქუბითები“. ამ კატეგორიაში აგრეთვე შედის ოპტიკური იმპლიმენტაციები. „სტაციონარული“ მოვლენისთვის ქუბითები იკავებენ ფიზიკურ ადგილს და ასრულებენ ოპერაციებს იმ აპლიკაციის მიხედვით, რომელიც მასზეა ასახული. „სტაციონარული“ ცნება მხოლოდ კარიბჭის ოპერაციის დროს მოქმედებს. რამოდენიმე სტაციონარული ტექნოლოგია, როგორიცაა სკალირებადი იონების ხაფანგი, ქუბითის ფიზიკურ მატარებელს საშუალებას აძლევს გადაიტანოს იგი კარიბჭის აპლიკაციამდე. ასეთ ქუბითებს ეწოდება „მობილური“ ქუბითები. [კელპინსკი 2002].

სტაციონარული და მფრინავი იმპლიმენტაციის ერთმანეთისგან გამოყოფის ძირითადი მიზეზი დინამიური კონტროლია. მფრინავი ქუბითების მოწყობილობაში, ქუბითთა მწკრივი წინასწარ უნდა იყოს დაფიქსირებული. კლასიკური გადამრთველების კონტროლი, რომელიც აძლევს მიმართულებას ქუბითებს სხვადასხვა დანაყოფებში, უზრუნველყოფს რამოდენიმე პროგრამის ერთდროულად გაშვებას. სტაციონარულ ქუბითის მოწყობილობა უფრო მოქნილია ქუბითების ხელახალი კონფიგურაციისთვის. სტაციონარული მოწყობილობები წააგავს კლასიკურ პროგრამირებას, ისევე როგორც მფრინავი ქუბითების პროექტირება კლასიკურ სქემურ ტექნიკას. [იאו 1993].

მთლიანი და გაერთიანებული სისტემა. ქვანტური კომპიუტერული ტექნოლოგიები ერთმანეთისგან ნიშნულგვანად განსხვავდებიან ერთიანი და ცალკეულ გამოთვლებით. გაერთიანებულ გამოთვლებში, რომლებიც ძირითადად იმპლიმენტირებულია სტატიკურ ქუბითურ სისტემებზე, მოცემულია მრავალი იდენტური ქვანტური კომპიუტერი, რომლებიც დებულობენ იგივე ოპერატორებს და აშუშავებენ იგივე პროგრამას. მთლიან სისტემებს აქვთ უნარი უშუალოდ გააკონტროლოს ფიზიკური ელემენტი, რომელიც წარმოადგენს ქუბითს. ტექნოლოგიური თვალთახედვით, გაერთიანებული სისტემები ექსპერიმენტის ჩასატარებლად შედარებით უფრო მარტივია, ვინაიდან დიდი რაოდენობის ატომის ან მოლეკულის გაზომვა და მანიპულირება უკეთ აღსაქმელია. ამგვარად, ქვანტური გამოთვლითი სისტემის დემონსტრირება დღესდღეობით შესაძლებელია სპინური სიმრავლით, რომელიც გამოსათვლელად იყენებს მოლეკულურ მწკრივს [ვანდერსიპენი 2001].

გაზომვა. საიმედო გამოთვლებისთვის და გამოთვლების შედეგზე დაკვირვებისთვის გამოთვლით ტექნოლოგიებს უნდა ჰქონდეთ პროცესების წარმოდგენის მხარდაჭერა. ასეთ წარმოდგენას ეწოდება გაზომვა, რომელის მეშვეობითაც ვაკვირდებით ქვანტური ბიტის (ქუბითის) მდგომარეობას და ვაწარმოებთ კლასიკურ შედეგს. განვიხილოთ გაზომვის სქემის ოთხი მახასიათებელი: (1) შესაძლებელია თუ არა რამოდენიმე ქუბითის პარალელურად გაზომვა, თუ მათი გაზომვა უნდა იყოს სერიული? (2) იმისათვის რომ მივიღოთ შედეგი, მოითხოვს თუ არა ქუბითის გაზომვა სხვა „ცარიელ“ ქუბითთან ურთიერთქმედებას? (3) არის თუ არა გაზომვის სიჩქარე (მაგნიტუდის მწკრივში) ისეთი როგორიც მოქმედების

შესრულების დროსაა? (4) შესაძლებელია თუ არა განვახორციელოთ გაზომვა ყველგან, რომელიმე კონკრეტულ არეში?

ქვანტური სისტემის საიმედო გამოთვლები გულისხმობს იმას, რომ ქვანტური ოპერაციების დიდი (თუარა უმეტესი) ნაწილი უნდა იყოს გაზომვები. [სტინი 2002]. არქიტექტორული თვალსაზრისით თუ გაზომვები განხორციელდება სერიულად ან უჩვეულოდ ნელა, მაშინ ეს შექმნის ამ გამოთვლებისთვის ვიწრო ადგილს. გარდა ამისა, თუ გაზომვისთვის საჭიროა დამატებითი „ცარიელი“ ქუბითების დამატება, მაშინ ჩვენ უნდა ჩამოვყალიბოთ ინიციალიზების პროცესი რათა ხშირად განვახორციელოთ გაზომვა. ანალოგიურად, თუ ტექნოლოგიებში არის გაზომვის ადგილის შეზღუდვა, მაშინ ეს შეზღუდვები უნდა ჩამოყალიბდეს არქიტექტურაში.

შეცდომების დამუშავება და გასწორება. ქვანტური შეცდომების გასწორების თეორია (QEC) თითქმის ათწლეულებია რაც არსებობს, თუმცა მისი პროგრამული უზრუნველყოფა დამოკიდებულია ტექნოლოგიურ მიღწევებზე. ქვანტური შეცდომების გასწორების თეორია ტრადიციულად დამყარებულია თანმიმდევრულ გამოთვლებსა და ლოგიკურ კარიბჭეებზე, სადაც ახლახანს მიაღწიეს ექსპერიმენტულ პროგრესს. [რუზი 2004]. ქვანტური შეცდომების გასწორება შესაძლებელია გაზომვების გარეშეც, „დროებითი“ ქუბითური ცვლადებით, რომელიც შედაგენს შეცდომების გასწორების პროგრამულ რიცხვებს. [ნილსენი და ხუანგი 2007]

რამოდენიმე ტექნოლოგიაში ქუბითები განიცდიან დამოუკიდებელ შეცდომებს, რომლიც QEC -ით გასწორებას ექვემდებარება. დამატებითი მეთოდები როგორიცაა თავისუფალი განზომილების დეკოჰერენცია (DFSees), გასნაკუთრებულად სასარგებლოა დაახლოებული ქუბითების შეცდომების გასასწორებლად. [ნილსენი და ხუანგი 2000].

ოპტიკურ სისტემებში შეცდომების დაკარგვის წყარო ფოტონების დაკარგვაა. ასეთ შემთხვევაში ეფექტურია კოდების გასუფთავება (შეცდომების გამსწორებელ კოდებისგან გასწავებით [ნილი 2000]), ვინაიდან დაკარგული ქუბითების დადგენა ადვილია.

2.2 მაწარმოებელი და ოპერირებული გარემო

დღესდღეობით ყველა სკალირებადი ქვანტური გამოთვლითი ტექნოლოგია არის თანამედროვე გამოწვევა, რომელიც მოითხოვს წარმოების მნიშვნელოვან განვითარებას იმასათვის რომ მოვახდინოთ მათი რეალიზება. რამოდენიმე ასეთი გამოწვევა შედარებით ნაკლებ ტექნოლოგიურ ძალისხვევას საჭიროებს ვიდრე დანარჩენი. გარდა ამისა, რამოდენიმე ტექნოლოგიური მოთხოვნილებები უკეთ ახდენს არსებულ კლასიკურ გამოთვლებთან ინტეგრირებას.

ტექნოლოგიური გამოწვევები. საინტერესოა ტექნოლოგიური მიღწევების რომელ საფეხურზე შევხვდებით წარმოების განვითარების სირთულეებს. მაგალითად, სილიციუმზე დაფუძნებული ატომურ მაგნიტური რეზონანსი ემყარება ზუსტად განლაგებულ ფოსფორის ატომის წმინდა სილიციუმს და მათი ფენურ სტრუქტურაზე დაყვანა ხდება სტანდარტული მაღალ სკალირებად ინტეგრაციის (VLSI) ლიტოგრაფიით [კეინი 1998]. ყველა მყარი ტექნოლოგიური სქემა მოითხოვს კლასიკურ კონტროლის ხაზს. (მაგ. [ფუჯიცავა 1998; ნაკამურა 1999]), რის სასარგებლოდაც შეიძლება გამოვიყენოთ VLSI-ის ზომების მურის კანონით მოსალოდნელი გაუმჯობესება. [მური 1965, ESIA 2003]. ჩვენს ტაქსონომიაში გამოვყოფთ ქვანტური გამოთვლების მთავარ ტექნოლოგიურ გამოწვევებს და განვიხილავთ მათ ბოლო მიღწევებს.

კონტროლის პარალელიზმი. ქვანტურ გამოთვლებში ალგორითმული უპირატესობების მიუხედავად, მნიშვნელოვანია ქვანტური ალგორითმებიდან პარალელიზმის გამოყოფა. რამოდენიმე მოცემულ ტექნოლოგიაზე , როგორიცაა სილიციუმის ატომურ მაგნიტური რეზონანსი, ალგორითმების სერიული გაშვება დროის თვალსაზრისით საკმაოდ შრომატევადი იქნება [სკინერი 2003]. მაგალითად, კუნიჰირომ [2005] შეაფასა შორის ალგორითმის სამუშაო დრო. 530-ბიტის რიცხვის ფაქტორიზაციას 1kHz-იან მოწყობილობაზე დასჭირდება 1.18 წელი, 10 საათი 1MHz-იან მოწყობილობას ან 37 წამი 1GHz-იან მოწყობილობას.

საბედნიეროდ ქვანტურ პროგრამულ უზრუნველყოფაში (შეცდომების გასწორებასა [სტინი 2003] და დამუშავებაში [ვან მეტერი და იტო 2005]) ხელმისაწვდომია მნიშვნელოვანი

პარალელიზმი. თუმცა ამ პარალელიზმის გამოყენება საჭიროებს პარალელური კონტროლის ტექნოლოგიებს. პარალელური კონტროლი მოითხოვს მნიშვნელოვან კლასიკურ სქემატიკას. თუ ეს სქემატიკა მოთავსებული იქნება ქუბითებთან დაახლოებულ „ჩიპზე“, მაშინ საჭირო იქნება ვუზრუნველყოთ მაღალ გამტარობის უნარიანი ინტერფეისი კონტროლის იმპულსის წარმომქმნელ კლასიკური მოწყობილობასა და არსებული ქუბითების მქონე ქვანტურ მოწყობილობას შორის.

სამუშაო ტემპერატურა. ხმაურის კონტროლისთვის ტექნოლოგიტრ გამოწვევების დიდი ნაწილი მოითხოვს ტემპერატურის ძალიან დაბალ მაჩვენებელს, რისი მიღწევაც შესაძლებელია თხევადი ჰელიუმის საშუალებით. სხვა ტექნოლოგიები მოითხოვენ კიდევ უფრო ცივ (მილიკელვინურ) ტემპერატურას, რომელიც მოითხოვს დილუციურ (ქიმიური კონცენტრაციების შემცირებით) გაციებას. ტემპერატურის ასეთი მდგომარეობა არამხოლოდ ტექნოლოგიური გამოწვევა, არამედ იგი ავლენას იქონიებს კლასიკურ სქემათა მართვაზე. [ოსკინი 2003].

დამხმარე ხელსაწყოები. რამოდენიმე ტექნოლოგია მოითხოვს კომპლექსურ დამხმარე აღჭურვილობას, განსაკუთრებით მაღალი სიხშირის მქონე მიკროტალღური გამათბობელი და ძაბვის სიგნალების გენერატორები. შესაძლოა თითოეულ ქუბითზე დაგვჭირდეს ერთი ან მეტი ასეთი ხელსაწყო. სისტემის ზომის ცვლილების გამო შესაძლოა საჭირო გახდეს ამ ხელსაწყოების გადატანა ან გაზიარება, ან უბრალოდ მათი ჩიპურ სისტემაში პირდაპირი ინტეგრირება.

2.3 ალგორითმული ეფექტურობის მახასიათებლები

ქვანტურ ალგორითმებზე მუშაობისთვის სხვადასხვა ქვანტურ გამოთვლების ბევრ მახასიათებელს ექნება რეალისტური აქტიტექტურის ღრმა იმპლიკაცია.

ქუბითების საერთო რაოდენობა. კომპიუტერის სკალარულობის, გამოყენების და სანდოობის დიდ გავლენის მახასიათებელს წარმოადგენს ფიზიკური ქუბითების საერთო რაოდენობა. მოცემული ალგორითმის მინიმალური მოთხოვნილობაზე მეტი, დამატებითი

ქუბითები შესაძლებელია გამოყენებულ იქნას ალგორითმის საიმედოობის ასამაღლებლად. ამის განხორციელება შესაძლებელია ალგორითმული პარალელიზმის შეცდომების გასწორებით, რასაც განვიხილავთ 5 თავში.

2 ცხრილის პუნქტებში მოყვანილია კითხვის ნიშნები, ვინაიდან რამოდენიმე საკითხში არ არსებობს საკმარისი ინფორმაცია. უფრო მეტიც, ჯერჯერობით კაურკვეველია რომელი ფაქტორი წარმოადგენს პრაქტიკული ზღვრების მტკიცებულებას. მკვლევარების უმეტესობა ჯერ კიდევ ფოკუსირებულია ქუბითების ძალიან ცოტა რაოდენობაზე. ამგვარად, ეს ზედა ზღვარი ჯერჯერობით არ არის განსაზღვრული.

დამისამართება. რამოდენიმე სისტემაში ქუბითების დამისამართება რთულია, ვინაიდან კლასილური კონტროლის (მაგ. მიკროტალღური სიხშირის ელექტრო-მაგნიტური ველის) ლოკალიზება იმ ზომაზე რასაც ერთეული ქუბითი მოითხოვს საკმაოდ შრომატევადია. ამ პრობლემის ერთ-ერთი გადაწყვეტაა ლოიდის მოდელი, რომელიც პატარა ქუბითების ჯგუფების უჯრედოვან ავტომატად გარდაქმნას გვთავაზობს [ლოიდი 1993]. ამ ჯგუფის თითოეული ქუბითის დამისამართება შესაძლებელი იქნება სპეციალური ელექტრომაგნიტური სიხშირით. ყოველი ავტომატა იმუშავებს მთლიან მოწყობილობაზე ელექტრომაგნიტური დასხივების პროგრამით, რის მეშვეობითაც მივიღებთ რამოდენიმე მონაცემზე ერთდროულად მომუშავე (SIMD) მანქანას. უჯრედული ავტომატას უფრო ადვილად კონტროლირებად სერიულ მანქანად გარდაქმნის ერთ-ერთი მეთოდია ავტომატონიდან ავტომატონში უჯრედული ავტომატას ნიშნულის შენახვა; ხოლოდ ის ავტომატონები განახორციელებენ მითითებულ მოქმედებას, რომლებიც შეიცავენ ამ ნიშნულს. დამისამართების და სპეციფიკურ ქუბითების კონტროლის გარეშე არქიტექტურის და პროგრამული სისტემების ტექნოლოგიის შემუშავება ძალიან რთული იქნება.

ჩაწერა. ერთ-ერთი გადამწყვეტი მიმართულება, სადაც კომპიუტერის არქიტექტორებმა შეიძლება იმუშაონ, არის ალგორითმის მნიშვნელოვან კლასების არქიტექტურის ოპტიმიზირება, რათა უზრუნველყონ მათი სწრაფი გადაცემა. რამოდენიმე სამომავლო ტექნოლოგიებში მხოლოდ მეზობელ ქუბითებს შეუძლიათ ორ ქუბითიან კარიბჭეების შექმნა. გამოთვლების ჩასატარებლად მანქანაში უნდა იყოს გადატანილი ქუბითების ფიზიკურ ელემენტებად (კონტროლის პროცესის გამოყენებით [კელპინსკი 2002])

ან მდგომარეობად (ქვანტური ხვრელების გამოყენებით [ოსკინი 2003]) წარმოდგენა. ერთის მხრივ, ტექნოლოგიური ფაქტორები კავშირის ტოპოლოგიას შემოსაზღვრავს ერთ-განზომილებიანი ხაზით, ხოლო მეორეს მხრივ არსებობს ორ-განზომილებიანი ჯაჭვის და ასევე სამ-განზომილებიანი სტრუქტურის საჭიროება [ლოიდი 1993]. ამ პრობლემის რამოდენიმე გადაწყვეტილებას აქვს მრავალ განზომილებიან კარიბჭეების მხარდაჭერა გარკვეული შეზღუდვებით, როგორიცაა პარალელიზმის შემოსაზღვრულობა [იოუ 2002].

2.4 დროის და კარიბჭის მახასიათებლები

ბუნებრივი კარიბჭეები. ბაზისური ნაკრების ფორმირებისთვის წარმოდგენილია სხვადასხვა კარიბჭის ნაკრებები. [ბარენკო 1995; დივინჩენზო 1994]. ერთ-ერთი ასეთი მაგალითია უნივერსალური კარიბჭეების სტანდარტული ნაკრები (X,H,T,CNOT). ყველა მნიშვნელოვანი ქვანტური გამოთვლების გამოწვევები მოითხოვს ექვივალენტურ უნივერსალურ ნაკრებს. უნივერსალურობის თვალსაზრისით არსებობს შემდეგი სამი მნიშვნელოვანი მახასიათებელი. (1) შეუძლია თუ არა სისტემას აწარმოოს დამოუკიდებლად მბრუნავი ქუბითი,თუ იგი უნდა იყოს სინთეზირებული X, H და T -დან [ნილსენი და ზუანგი 2000]; (2) რამდენად კომპლექსურია სამ ქუბითიან კონტროლერის (ე.წ ტოფოლის კარიბჭის) სინთეზი, რომელიც ფართოდ განოიყენება ქვანტურ ალგორითმებში [ბარენკო 1995]. (3) აქვთ თუ არა სპეციფიკურ კარიბჭეებს არასასურველი ეფექტი ქუბითებზე , რომლებიც არ არიან ოპერანდებად გათვალისწინებული. ქვემოთ დეტალურად განვიხილავთ ყველა ამ მახასიათებელს.

არბიტრალური ცალკეული ქუბითის ბრუნვა და კონტროლირებადი არბიტრალური ბრუნვა საკმაოდ საჭირო პრიმიტივებია. ტექნოლოგიები, რომლებსაც არბიტრალური ცალკეული ქუბითის ბრუნვის მხარდაჭერა აქვთ , არ საჭიროებს არც ერთ სინთეზურ მეთოდის გამოყენებას , რითაც დავზოგავთ ქუბითების დაახლოების პოლინომურ დროს. კონტროლირებადი არბიტრალური ბრუნვა (ორ ქუბითიანი ოპერაცია) განსაკუთრებით სასარგებლოა ფურიეს ქვანტური გარდაქმნისთვის (QFT), რომელიც გამოიყენება შორის ალგორითმში [შორი 1994; ჰეილში და ჰალგრენი 2000; ბარენკო 1996].

ტოფოლის კარიბჭე შედგება სამი ქუბითისგან და შესაძლებელია გამოყენებულ იქნას ჩვეულებრივი ლოგიკის ქვანტურ ბიტებად გარდასაქმნელად (მაგ. NAND, NOR და ა.შ.). იგი დამყარებულია არითმეტიკულ სქემებზე, რომელიც თვალსაჩინოა შორის ალგორითმში. ამას უფრო ახლო განვიხილავთ 5.1 თავში. ტოფოლის კარიბჭის ეფექტურად აგება შესაძლებელია იმ შემთხვევაში თუ სისტემს გააჩნია ერთ ქუბითიანი ოპერაციების და არბიტრალური ცალკეული ქუბითის ბრუნვის მხარდაჭერა.

სტატკურ ქუბითურ მოწყობილობებში, როგორცაა იონური ხაფანგები ან NMR სისტემა, რამოდენიმე ელექტრომაგნიტური იმპულსი საჭიროებს თითოეულ კარიბჭის იმპლემენტაციას. მათი საშუალო რიცხვია ხუთი ან ექვსი, თუმცა ეს რაოდენობა დამოკიდებულია თავად კარიბჭეზე. NMR სისტემების ერთ-ერთი ნაკლოვანება არის ის, რომ ეს პულსები ეფექტს ახდენს ახლო მდებარე ქუბითებზე და უშუალოდ ოპერირებს მათზე. ამის თავიდან ასაცილებლად საჭიროა დამატებითი კონტროლური სიხშირეები, რომელსაც გამყოფ სიხშირეებს უწოდებენ [ბეკმენი 1996; ლუნგი 2000].

ოპერაციის დრო და კოჰერენცია. გარემოს ეფექტისგან კარგი იზოლურება ქმნის დიდ კოჰერენციის ან ქუბითის „შენახვის“ დროს. ფართო განზოგადებით, ის ტექნოლოგიები რომლებიც ქვანტური მდგომარეობის მისაღწევად ელექტრონებს იყენებენ, მოკლე კოჰერენციული დროისაა, ვინაიდან არსებულ გარემოზე მოქმედი ელექტრონი მობუღური და ტენდენციურია. ტექნოლოგიები, რომლებიც გარემოს ეფექტისგან იზოლირებისთვის იყენებენ ატომურ ეფექტს, უფრო სტაბილურია, თუმცა მისი უარყოფითი მხარე არის ორ ქუბითიან კარიბჭეებთან მუშაობის დაბალი დრო. ჩვენს მიერ განხილული ტექნოლოგიებიდან, კარიბჭის სიჩქარე და დეკოჰერენციის დრო მერყეობს რვა ან უფრო მეტი მაგნიტუდამდე. [ლადი 2003]. კოჰერენცირების დრო წარმოადგენს განსაკუთრებულად მნიშვნელოვან კვლევის საგანს, ვინაიდან ის განავითარებს ქვანტური გამოთვლითი ტექნოლოგიების წინსვლას. კარიბჭის ოპერაციის დრო ხირად პირდაპირ დამოკიდებულია ფიზიკურ პროცესებთან, რომელის საინჟინრო პარამეტრები და მოქნილობა შეზღუდულია.

2.5 სხვა მახასიათებლები

ლოგიკური კოდირება. ქვანტური ალგორითმები კანკუთვნილია აბსტრაქტული და ლოგიკური ქუბითების მანიპულაციისთვის. თუმცა ლოგიკური ქუბითები ყოველთვის არ არის წარმოდგენილი როგორც ფიზიკური მოვლენის ერთეული, როგორცაა ცალკეული იონი ან ფოტონი. ასეთ მოვლენებს, რომელზეც მანიპულირებას ვახდენთ პროგრამულად, ვუწოდებთ „ლოგიკურ ქუბითს“ (ქვანტური შეცდომების გასწორების შემთხვევაში - „კოდირებულ ქუბითს“), ხოლო მოვლენებს რომლის იმპლიმენტირებას ახდენს ტექნოლოგია, ვუწოდებთ „ელემენტარულ ქუბითებს“.

რამოდენიმე ტექნოლოგიაში, როგორცაა ქვანტურ წერტილებში ელექტრონების დამუხტვა, კოდირება ხდება „dual rail“ მეთოდის გამოყენებით. ანალოგიურად, ცალკეულ ფოტონს სქემაში შეუძლია დაიკავოს მარცხენა ან მარჯვენა მიმართულება, რომელიც განსაზღვრავს სხვადასხვა ლოგიკურ მდგომარეობას (მაგ. 0 ან 1). ამ ორივე ტექნოლოგიაში ცალკეული ქვანტური წერტილი (ნაწილაკი) შესაძლებელია წამროვიდგინოთ როგორც ქვანტური ქუბითი, იმ შემთხვევაში თუ მათი გამოთვლა და გაზომვა ხდება კოდირებულ გარემოში.

სკალირების ზღვარი. არქიტექტურაში დიდი რაოდენობით ქუბითების სკალირება მეტ წილად წარმოადგენს ზემოთ ჩამოვლილი ფაქტორების ფუნქციას. ფაქტორები, რომელიც არ იყო ზემოთ მოყვანილი, არის კონკრეტულ ტექნოლოგიაზე დამოკიდებული. მაგალითად, ლითოგრაფიაზე დაფუძნებულ სისტემებში შეტანა/გამოტანის (I/O) კონტროლერი მოთავსებულია ჩიპზე, რომელსაც აქვს ჩაშენებული მიკროტალღური გენერატორები და მცირე მოწყობილობისთვის საკმარისი ოდენობის კონტროლის სადენები. ამ ფაქტორებიდან გამომდინარე, რამოდენიმე ტექნოლოგიური გადაწყვეტილება განსაზღვრულ ზედა ზღვარს არსებობას საჭიროებს. ამ ქვეთავში ჩვენ გამოვყოფთ თითოეულ ტექნოლოგიისთვის მიღებულ სკალირების ზღვარს.

ცხრილი 1. ქუბითური ტექნოლოგიის ძირითადი მახასიათებლები (QIO აღნიშნავს ქვანტურ შეტანა/გამოტანას, ? - არ გაუვლია ექსპერიმენტული შემოწმება)					
ტექნოლოგია	სტაციონარული/ მფრინავი/მობილური	მთლიანი/ გაერთიანებული	QIO	გამზომი	რეფერენსი
სილიციუმის NMR	სტაციონარული	გაერთიანებული	არა	მექანიკური ვიბრაცია, სიხშირის ანალიზი	[ლადი 2002]
NMR გადაწყვეტა	სტაციონარული	გაერთიანებული	არა	პარალელური, სიხშირის ანალიზი	[ვანდერსიპე ნი 2001]
ქვანტური ნაწილაკის დამუხტვა	სტაციონარული	მთლიანი	კი?	პარალელური, ჩიპზე დაფუძნებული სტრუქტურა	[ლოსი და დივინჩენზო 1998]
სკალირებადი იონური ხაფანგი	მობილური	მთლიანი	კი?	შეზღუდულად პარალელური, ოპრიკურად იდნუცირებულ იფლუარესენსი	[ცირაკი და ზოლერი 1995;კელპინ სკი 2002]
იოსეფსონის გადაკვეთით დამუხტვა	სტაციონარული	მთლიანი	კი?	პარალელური, ჩიპზე მოთავსებული სენსორი	[პაშკინი 2003;იოუ 2003]
კეინის მოდელი	სტაციონარული	მთლიანი	არა	პარალელური, ერთეული ელექტრული სპინის გაზომვა	[კეინი 1998]
წრფივი ოპტიკური ქვანტური გამოთვლა	მფრინავი	მთლიანი	კი	ფოტონური ოპტიკური დეტექტორები თ ცალკეული ქუბითის პოლარიზაცია	[ნილი 2011]

ქვანტური შეტანა/გამოტანა (QIO). ჩვენ შესაძლებელია დაგვჭირდეს ქვანტური მდგომარეონის ერთი მოწყობილობიდან მეორეში გადატანა. არსებობს სხვადასხვა მიზეზი თუ რატომ შეიძლება იყოს ეს მნიშვნელოვანი: ჩვენ შესაძლოა უბრალოდ დაგვჭირდეს რამოდენიმე მოწყობილობის გაერთიანება, შორეული კვანძისთვის სხვადასხვა გამოთვლითი შესაძლებლობები (მაგ. გრძელვადიანი მონაცემების შენახვა) , ან სხვადასხვა მონაცემებზე წვდომა. რამოდენიმე შემთხვევაში, შესაძლებელია ქვანტური მომაცემები მოწყობილობებს შორის სხვადასხვა ტექნოლოგიებით გადავცეთ.

ქვანტური შეტანა/გამოტანა საკმაოდ ცდომილებიანი პროცესია. ამგვარად, იგი შედგება საწყისი „ცარიელი“ ქუბითებისგან შემდგარი QIO-სგან, რომელიც მოწყობილობებს შორის წარმოქმნის გადამზულ მდგომარეობას. ასეთ მდგომარეობას ეწოდება QIO მიდამოები. გასუფთავების პროცესის შემდგომ, როდესაც დადასტურებული იქნება გადამზული მდგომარეობის არსებობა, შესაძლებელი იქნება ნებისმიერი ქვანტური მდგომარეობის ტელეპორტაციით გადაცემა *[ბენეტი 1993; ფურუსავა 1998; ლოიდი 2000; კუზმიჩი და მაცუკევიჩი 2004]*.

1 ცხრილში QIO ველში შემავალი კითხვისნიშნები აღნიშნავენ იმას რომ შესაბამის მოსალოდნელ ქვანტურ გამოთვლელ სტრუქტურებზე არ განხორციელებულა სადემონსტრაციო ექსპერიმენტი ან ადეკვატური მტკიცებულებები ვერ იქნა ნაჩვენები. რამოდენიმე შემთხვევაში არსებობს საკმაოდ მყარი ანალიზით მიღებული ტექნიკური გადაწყვეტილებები ან ექსპერიმენტული დადასტურება, რასაც მომდევნო თავში განვიხილავთ.

3. ქვანტური ტექნოლოგიები

წინა თავში მოყვანილ ტაქსონომიის საფუძველების გამოყენებით ამ თავში ჩვენ განვიხილავთ ქვანტურ გამოთვლით ტექნოლოგიების სხვადასხვა გადაწყვეტილებებს. ძირითად ყურადღებას დავუთმობთ შვიდ ტექნოლოგიას: სიცილიუმის ატომურ მაგნიტურ რეზონანს (Si NMR) , ატომურ მაგნიტურ რეზონანსულ გადაწყვეტას, ქვანტურ ნაწილაკის დამუხტვას, სკალირებად იონურ ხაფანგს, იოსეფსონის გადაკვეთით დამუხტვას, კეინის მოდელს და წრფივ ოპტიკაზე დაფუძნებულ სისტემებს. ამ ტექნოლოგიების შერჩევა არ შეიძლება მივიჩნიოთ ამომწურავად, ვინაიდან არსებობს კიდევ ბევრი ტექნოლოგიური გადაწყვეტილებები [ბრენენი 1999; ფოლმენი 2000; შარიარი 2002; პელიზარი 1995; ჩილდრესი 2005]. ეს სისტემები შევარჩიეთ გამომდინარე იქიდან, რომ მათ აქვთ შედარებით ფართო იმპლიმენტაციის და სკალირების უნარი. ინფორმაცია შეჯამებულია 1-4 ცხრილებში. ქვემოთ განვიხილავთ თითოეულ ტექნოლოგიას და მის არქიტექტურულ იმპლიკაციას.

ცხრილი 2. ქუბითურ ტექნოლოგიებში ასახულ ალგორითმის ეფექტურობის მახასიათებლები
(ქუბითების მაქსიმალური რაოდენობა ყველა ტექნოლოგიაში რჩება გაურკვეველად.)

ტექნოლოგია	პარალელიზმი	ქუბითების რაოდენობა	ჩაწერის ტოპოლოგია	დამისამართება	ყველა ქუბითზე ოპერირება
სილიციუმის NMR	არაწევრ ქობითზე მოქმედების შეჩერების შეზღუდვა	ასობით?	წრფივი უახლოესი მდებარეობა	სიხშირით, დამუკიდებელი	კი
NMR გადაწყვეტა	არაწევრ ქობითზე მოქმედების შეჩერების შეზღუდვა	ათობით?	შეზღუდული წრფივი უახლოესი მდებარეობა	სიხშირით, დამუკიდებელი	კი
ქვანტური ნაწილაკის დამუხტვა	კონტროლის მექანიზმის შეზღუდვა	ძალიან დიდი	წრფივი უახლოესი მდებარეობა	ლოკალიზებული, ჩიპური სისტემის დამოუკიდებელი კონტროლით	კი
სკალირებადი იონური ხაფანგი	ლაზერული არის შეზღუდვა	ძალიან დიდი	ღია, არარეგულარ აბადი, ორი და მეტ განზომილებ იანი	ინდივიდუალური იონების სამისამართო ადგილიდან მოქმედების არეში გადატანა	არა
იოსეფსონის გადაკვეთით დამუხტვა	გადაბმის მექანიზმის შეზღუდვა	ძალიან დიდი	ერთი,ორი ან რამოდენიმე განზომილებ იანი	ლოკალიზებული, ჩიპური სისტემის დამოუკიდებელი კონტროლით	კი
კეინის მოდელი	კონტროლის მექანიზმის შეზღუდვა	ძალიან დიდი	ერთი ან ორ განზომილებ იანი	ლოკალიზებული, ჩიპური სისტემის დამოუკიდებელი კონტროლით	კი
წრფივი ოპტიკური ქვანტური გამოთვლა	შეუზღუდავი	ძალიან დიდი	ფიზიკური დამისამართე ბა	ფიზიკური პოზიცია	კი

3.1 NMR გადაწყვეტა

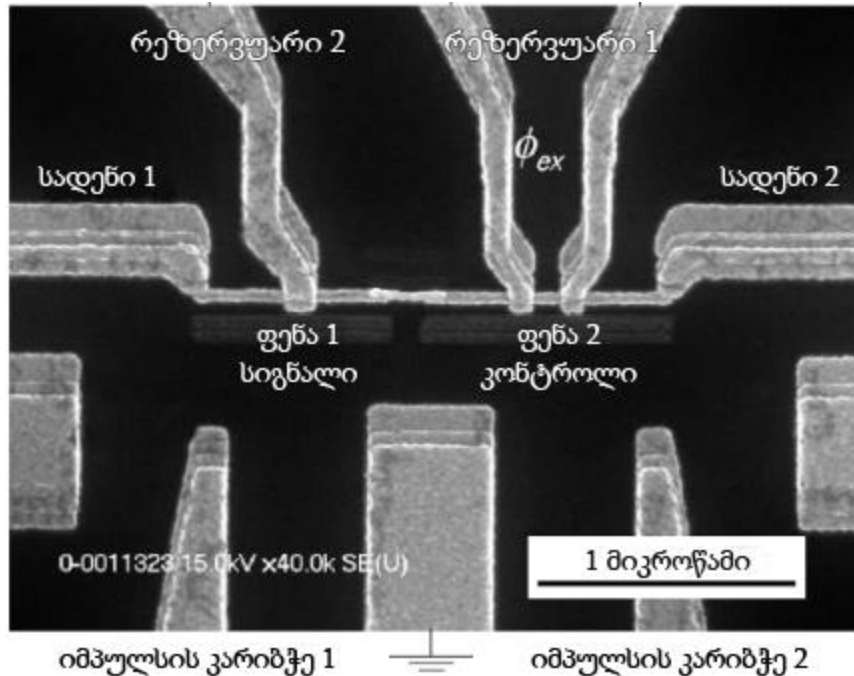
ქვანტური გამოთვლების ერთ-ერთი ყველაზე სრულყოფილი დემონსტრაცია დღესდღეობით არის NMR გადაწყვეტის ექსპერიმენტები. [ვადერსიპენი 2001; ბოულანტი 2003]. NMR სისტემაში ქუბითი წარმოდგენილია როგორც ატომის ბირთვის სპინი. სპინის მაგნიტურ ველში მოთავსების შემდგომ მიკროტალღური დასხივებით შესაძლებელი ხდება მისი მანიპულირება. NMR გადაწყვეტაში გამოიყენება გულდასმით შედგენილი მოლეკულები. რამოდენიმე მოლეკულის ატომი შეიცავს ატომურ სპინს და დასხივების სიხშირით, რომელიც მოლეკულურ პოზიციის მიხედვით იცვლის მნიშვნელობას. ამ გზით ხდება სხვადასხვა ქუბითების სიხშირით დამისამართება. ასეთი მოლეკულის დიდი ნაწილი არის თხევად მდომარეობაში; თითოეული მოლეკულა წარმოადგენს ცალკეულ ქვანტურ კომპიუტერს, რომელიც ფუნქციონირებს დამოუკიდებლად და წარმოქმნის წაკითხვისთვის საჭირო რაოდენობის სიგნალს. ეს არის კანონიკური, შეთანხმებული სისტემა. NMR დადაწვეტა შორის ალგორითმის გამოყენებით ითვლის 15-ის ფაქტორიულ რიცხვის, რომელსაც სჭირდება 720 მილიწამი შესასრულებლად. [ვანდესიპენი 2001]. დღესდღეობით ყველაზე მასშტაბური დემონსტრაცია არის 12 ქუბითიანი [ქორი 2004]. ამგვარი შეთანხმებული სისტემა არ საჭიროებს განსაკუთრებულ გამაგრებულ აპარატურას თუმცა მისი სკალარულობა შეზღუდულია, ვინაიდან ქუბითების რაოდენობის გაზრდის შემთხვევაში მისი სიგნალის დონე ეცემა.

-*ძლირი მხარე*. კარგი დეკოპერენციის დრო, ოთახის ტემპერატურაზე მუშაობა, სხვადასხვა ექსპერიმენტული მიმართულებები.

-*სუსტი მხარე*. ნელი კარიბჭეები, სუსტი სკალირებადობა, რთული პარალელური ოპერაციები.

3.2 იოსეფსონის გადაკვეთა

იოსეფსონის გადაკვეთაზე დაფუძნებული ქვანტური გამოთვლითი მოწყობილობები წარმოადგენენ ზეგამტარ სისტემებს. [შნირმანი 1997]. მათ აქვთ სამი დადებითი მახასიათებელი: ისინი წარმოიქმნებიან ქუბითს დამუხტვის საშუალებით (როგორც 1 სურათზე ნაჩვენებ მოწყობილობით) [ნაკამურა 1999; პაშკინი 2003], ისინი იყენებენ ნაკადს [მუიჟი 1999; ჩიორესკო 2004] და ისინი იყენებენ ფაზებს [იუ 2002; მარტინისი 2002]; სამივე მახასიათებელის ინფორმაცია მოცემულია ცხრილებზე. მათი წარმოება ხდება ჩვეულებრივი ელექტრო სხივის ლითოგრაფიით და ალუმინის საიზოლაციო სუბსტრატზე ჩრდილოვანი აორთქლებით. იოსეფსონის გადაკვეთით დამუხტვისას, ქუბითი, როგორც სუბ-მიკრონული ზომის (საჭიროდ მცირე მოცულობის) ზეგამტარი ფენა წყვილდება უფრო დიდ ზეგამტარ რეზერვუართან. ზეგამტარ ფენაში ელექტრონები წყვილად მოძრაობენ (კუპერის წვილი). ფენაში არსებული კუპერის წტილის რაოდენობა წარმოადგენს ქუბითს, რომელიც იღებს ნულოვან ან ერთეულ მნიშვნელობას, ან ორივე მნიშვნელობის სუპერპოზიციას. ნაკადური ქუბითების შემთხვევაში, კუპერის წვილი მოთავსებულია ზეგამტარ სარტყელში, რომელშიც ახდენენ ცირკულაციას და წარმოქმნიან დაქვანტულ მაგნიტურ ნაკადს. იმის გამო, რომ ნაკადურ ქუბითის კარიბჭეს შედარებით ნელი სიჩქარე და შესაბამისად უფრო დიდი კოჰერენციული დრო ახასიათებს, ნაკადური ქუბითების განვითარებისთვის შედარებით ნაკლები ექსპერიმენტული ძალისხმევა იხარჯება.



სურათი 1. იოსეფსონის გადაკვეთით დამუხტული ქუბითის წყვილი (ფენა 1, ფენა 2). ეს მოწყობილობა განკუთვნილია ორ-ქუბითიან კარიბჭეს შორის არსებულ „კონტროლის“ და „სიგნალის“ ქუბითების გარდასაქმნელად. ამ მოწყობილობაში ორი ქუბითის დაწყვილება ფიქსირებულია [ი.ნაკამურა და ტ.იამამოტო].

ერთ-ერთ ასეთ დამუხტული ქუბითის სკალირებად გადაწყვეტის ფორმაში შესაძლებელია ნებისმიერი ორი ქუბითის დამისამართება და დაწყვილება. [იოუ 2002]. ამის განხორციელება შესაძლებელია სერთო ინდუქტირებით. ასეთ შემთხვევაში მეზომელ ქუბითზე მოქმედების შეზღუდვა იხსნება, მაგრამ თითო ჯერზე მხოლოდ ერთი კარიბჭის მოქმედება შესაძლებელი. მეზომილ ქუბითებზე სხვადასხვა ერთგანზომილებიანი სტრუქტურული გადაწყვეტაა დამყარებული, თუმცა შესაძლებელია დამოუკიდებელ ქუბითებზე დაფუძნებული პარალელური კარიბჭეების უზრუნველყოფა. [ლანცი 2004].

-*ზლიერი მხარე*. ძალიან სწრაფი კარიბჭეები, დახვეწილი ექსპერიმენტული დემონსტრირება, მარტივი წარმოება.

-*სუსტი მხარე*. გაზომვის დროის გამო დაბალი კოჰერენციის დრო, ლოკალურ მაგნიტურ ველების მიმართ მგრძნობელობა.

ცხრილი 3. მოქმედების სიხშირე და კარიბჭის მახასიათებლები

ტექნოლოგია	დეკოპერენციის დრო	გაზომვის დრო	ერთეუბითიანი კარიბჭის მოქმედების სიჩქარე	ორეუბითიანი კარიბჭის მოქმედების სიჩქარე	ბუნებრივი ორ-ეუბითიანი კარიბჭე
სილიციუმის NMR	25 წამი	დიდი	40kHz	400Hz	1 დაწყვილება
NMR გადაწყვეტა	წამები	დიდი	50GHz	50Hz	1 დაწყვილება
ქვანტური ნაწილაკის დამუხტვა	რამოდენიმე ნანოწამი	10-100 ნანოწამი	10GHz	10GHz	გაცვლა
სკალირებადი იონური ხაფანგი	1 მილი მილი/წამი	100 მიკროწამი - 10 მილიწამი	14kHz - დან 100kHz - მდე	~10 მიკროწამი	მდგომარეობის ფაზაში გასასვლა
იოსეფსონის გადაკვეთით დამუხტვა	რამოდენიმე ნანო/წამი	10 ნანოწამი	10GHz	10GHz	მდგომარეობის ფაზაში გასასვლა
კეინის მოდელი	დიდი?	დიდი	75kHz	75kHz	1 დაწყვილება
წრფივი ოპტიკური ქვანტური გამოთვლა	გაფანტავით და შთანთქმით შეზღუდული	5-10 ნანოწამი	1 ნანოწამზე ნაკლები	დეტექტორის დროით შეზღუდული	მდგომარეობის ფაზაში გასასვლის ხვდასხვა შესაძლებლობები

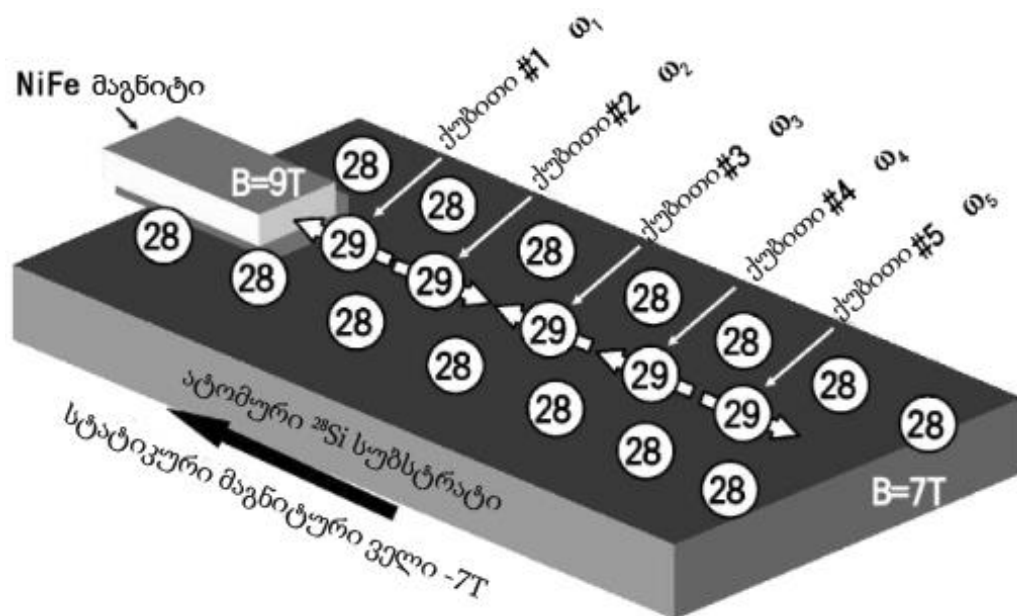
ცხრილი 4. სხვა მახასიათებლები			
ტექნოლოგია	ლოგიკური:საწყისი კოდირება	კარიბჭის სინქრონის კონტროლი	სკალირების ზღვარი
სილიციუმის NMR	1:1	ნელი კარიბჭეები უზრუნველყოფს ზუსტ სინქრონს	ინიციალიზების ხარისხი,სტატიკურ მაგნიტურ ველში ზუსტი განთავსების და მაგნიტური ველის მოდების ხარისხი.
NMR გადაწყვეტა	1:1	ნელი კარიბჭეები უზრუნველყოფს ზუსტ სინქრონს	სიგნალის ხმაურად გარდაქმნა (SNR) ექპონენციალურად ვარდება n-ში
ქვანტური ნაწილაკის დამუხტვა	1:3	რყევების მიუხედავად კარიბჭეები ზუსტია	გარე ჩაწერის კონტროლი
სკალირებადი იონური ხაფანგი	1:1	რყევების შესამცირებლად რეკომენდირებულია დეკოჰერენციისგან თავისუფალი სივცრის გამოყოფა	დიდი ონდენობის ინდივიდუალური იონების გადაცემის და მათი მოძრაობის დროის ალბათური სიზუსტით შესრულება
იოსფსონის გადაკვეთით დამუხტვა	1:1	ფაზების აქტიური კონტროლი	გადამკვეთი ქუბითების ინტერფეისი;დიდი რაოდენობის მიკროტალღური გენარატორების ჩადშენება
კეინის მოდელი	1:1	-	წარმოების სირთულე
წრფივი ოპტიკური ქვანტური გამოთვლა	1:1	„გაჩერებული“ სინათლე [ლუკინი 2000]	შიდა გენარეტორების და კარიბჭეების უზუსტობა და რყევა; ქუბითების დიდ რაოდენობის შემთხვევაში ფოტოდეტექტორს უჭირს სკალირება;

3.3 სილიციუმის NMR

თადეუს ლადმა წარმოადგინა სილიციუმის NMR-ზე დაფუძნებული ქვანტური კომპიუტერი, რომელიც ქუბიტებს სილიციუმის ატომურ სპინში (^{29}Si) ანთავსებს. ქუბიტები წრფივად ჩამწკრივებულია 0-ბირთვიან მიკრომექანიკურ სპინების ხიდის გასწვრივ. (^{28}Si და ^{30}Si), რომელიც ნაჩვენებია 2 სურათზე. ეს არის გაერთანებული სისტემა, რომელიც ადეკვატური სიგნალის მისაღებად საჭიროებს 10^5 ეგზემპლარს. წაკითხვა ხდება მაგნიტურ რეზონანსული ძალის მქონე მიკროსკოპით (MRFM), რომელიც კითხულობს ამ ხიდის ოსილაციებს. ინიციალიზება ხორციელდება ელექტრონებით, რომელთა სპინებიც პოლარული სინათლით (ოპტიკური სატუმბით) არის მოწყობილი. ოპერაცია ხორციელდება მოწყობილობაზე მოდებული მიკროტალღური დასხივებით. მიკრომაგნიტი უზრუნველყოფს მაღალ გრადიენტულ ველს, რომელიც ატომს საშუალებას აძლევს მიიღოს სიხშირით დამისამართება.

-ძლიერი მხარე. ყველაზე დიდი დეკოჰერენციის დრო რაც აქამდე ცნობილია.

-სუსტი მხარე. ნელი კარიბჭეები, არ აქვს QIO (ქვანტური შეტანა/გამოტანა) მხარდაჭერა, ჯერ არ არის შემუშავებული მისი გაზომვა.



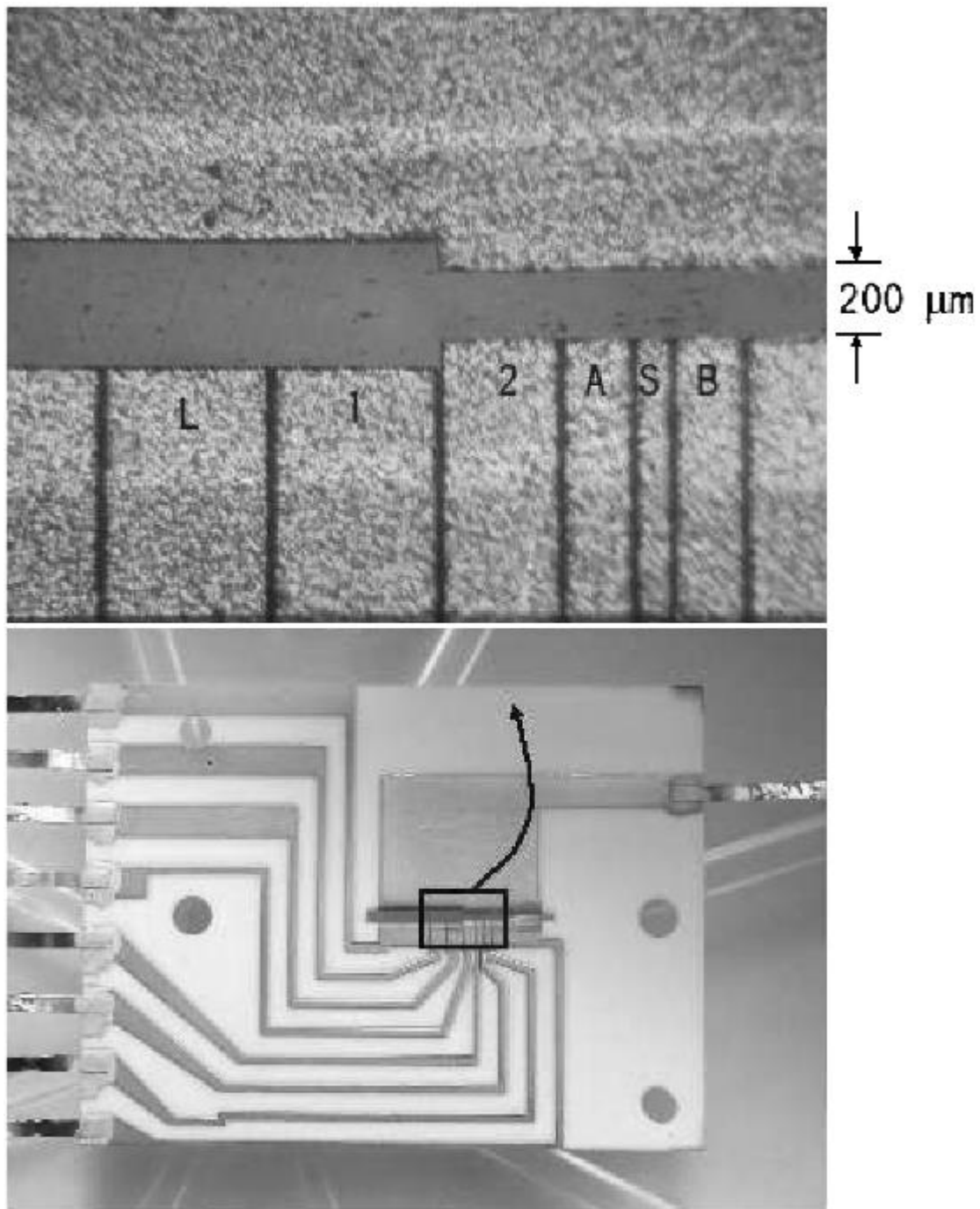
სურათი 2. სილიციუმის NMR-ზე დაფუძნებული გამომთვლელის სქემა. ქუბითები ^{29}Si ატომის სპინები წარმოადგენენ ქუბითებს, რომელიც მოთავსებულია სპინისგან თავისუფალ ^{28}Si ბაზაზე. მიკრომაგნიტს შორის მანძილი განსაზღვრავს ოსილაციის სიხშირეს და უზრუნველყოფს ქუბითის დამისამართებას [იტო, კეიოს უნივერსიტეტი].

3.4 სკალირებადი იონური ხაფანგი

სლაკირბული იონური ხაფანგი ერთ-ერთია იმ იშვიათ სისტემებიდან, რომელიც შემნახავ მიდამოებს რადიკალურად განსხვავებს ურთიერთქმედების მიდამოებისგან [კელპინსკი 2002; ვაინლენდი 2005; კიმი 2005; მეტოდიევი 2003]. იგი წარმოადგენს სტანდარტებისა და ტექნოლოგიების ნაციონალური ინსტიტუტის (NIST) მიერ შემუშავებულ გადაწყვეტილებას. [ცირაკი და ზოლერი 1995; სტინი 1997]. იონურ ხაფანგის სისტემებში ქუბითები წარმოადგენს ინდივიდუალ იონში არსებულ ენერგულ დონეებს. ცალკეულ ხაფანგში მოთავსებულ იონის მცირე რაოდენობაზე ადრე ჩატარებულმა ექსპერიმენტებმა, ინდივიდუალურად კონტროლირებად დიდ სისტემებს ურთიერთკავშირის საშუალება მისცა. სკალირებად იონურ ხაფანგში იონები მოძრაობენ მაგნიტური ველის საშუალებით მანამდე, სანამ ისინი მიაღწევენ სისტემურ ოპერაციისთვის სამუშაო ლოკაციებს (სურათი 3). რამოდენიმე ქუბითური კარიბჭეების უზუნველსაყოფად, მცირე რაოდენობის იონები რმანეთთან ჯგუფდებიან და ქმნიან ჯაჭვს. ტომის მდგომარეობის მიხედვით, ლაზერული იმპულსები ქმნიან ფლურესენციას რომელიც განსაზღვრავს 1 (ფლურესენციის არ არსებობის შემთხვევაში 0), რაც საშუალებას იძლევა შევასრულოთ კარიბჭეებზე ზემოქმედება და წაკითხვა. კარიბჭის მოქმედების სიჩქარე საშუალოდ 14-100kHz-ით განისაზღვრება. მთლიანი სისტემის სისწრაის მახასიათებელი დამოკიდებულია იონის გადაცემის დროზე, ატომის ჯაჭვის წარმოქმნა/დაშლაზე, მოძრაობის დროს დახურებული ატომის გაციებაზე და მულტიპლექსორულ კარიბჭის ოპერაციებზე. მოძრაობის ოპერაცია არ აძლევს კარიბჭეს საშუალებას განავითაროს მოქმედების დრო 20kHz-ზე მეტი სიჩქარით.

-ძლიერი მხარე. მოცულობის სკალარულობა;

-სუსტი მხარე. ნელი კარიბჭეები; შეზღუდვა პარალელურ ოპერაციებზე და გაზომვებზე.



სურათი 3. ექვს ზონიანი იონური ხაფანგი, რომელსაც შეუძლია ინდივიდუალური იონების გადატანა. იონები თავსდება საწყის L ზონაში და მანიპულირებულ A, S ,B ზონაში [დ.ვაინლუნდი NIST].

3.5 ოპტიკური მთვლელები

ყველა ოპტიკურ ქვანტურ გამოთვლით სისტემას აქვს ორი ნაირსახეობა: სისტემები რომლებიც კარიბჭეების ასამუშავებლად იყენებენ არაწრფივ ეფექტებს და სისტემები რომლებშიც ერთადერთ არაწრფივ ეფექტს წარმოადგენს გაზომვა, რომელსაც ეწოდება წრფივი ოპტიკური ქვანტური გამოთვლა (LOQC) [ნილი 2001]. ოპტიკურ ქვანტურ სისტემებზე კვლევა ფოკუსირებულია ფოტონთა წყაროზე, რომელსაც შეუძლია საჭირო დროში განსაზღვრული, გაზომვაზე დაფუძნებული კარიბჭეების და მაღალ ხარისხიან დეტექტორის ფოტონთა ზუსტი რაოდენობის გენერირება. [ნილი 2003; მილერი 2003; სანტორი 2002].

ბუნებაში, გაზომვაზე დაფუძნებული კარიბჭეები ალბათური ხასიათისაა, თუმცა ექსპერიმენტებმა აჩვენეს, რომ ამ კარიბჭეების აგება შესაძლებელია სლაკირებად ცალმხრივ ქსელებში. [ნილი 2001; რალფი 2005]. დღესდღეობით ექსპერიმენტების უმეტესობა ამგვარი მიდგომით მიმდინარეობს და უკვე ნაჩვენებია ინდივიდუალური კარიბჭეები [პიტმენი 2002; ობრიენი 2003; გასპარონი 2004; სანაკა 2004].

ოპტიკურ ქვანტურ მთვლელში სიგნალის დანაწევრება ხდება „გაჩერებული სინათლით“, რომელსაც წარმოქმნის ელექტრომაგნიტურად ინდუცირებულ გამჭირვალობით [ფლაიშჰაუერი და ლუკინი 2000; რაისი 1997].

-ძლიერი მხარე. კარგად გასაგები ფიზიკა და ადვილი წარმოება.

-სუსტი მხარე. ფოტონების დაკარგვა; არაწრფივი სისტემებისთვის დამასახიათებელი სუსტი არაწრფივი ეფექტები განაპირობებს კარიბჭის დაბალ ხარისხს; ალბათური კარიბჭეები მოითხოვს დიდ რესურსებს.

3.6 ქვანტური ნაწილაკის დამუხტვა

ქვანტურ იფორმაციულ გამოთვლებში „ქვანტური ნაწილაკი“ წარმოადგენს ლითოგრაფიულად განსაზღვრულ სტრუქტურას. ეს სტრუქტურა, შემომსაზღვრელი შრის გამოყენებით, ორ მატერიას შორის აცალკევებს ელექტრონებს, რომელიც წარმოქმნის ორ განზომილებიან ელექტრონის აირს (2DEG). სხვადასხვა ახლომდებარე ელექტრონული პოტენციალის მეშვეობით შესაძლებელია ინდივიდუალური ელექტრონების პატარა სივრცეში მოთავსება, რომელსაც ქვანტური ნაწილაკი ეწოდება. ქუბითი განისაზღვრება ქვანტურ ნაწილაკში ელექტრონების რაოდენობით ან ქვანტურ ნაწილაკში არსებულ ცალკეულ ელექტრონის ენერგულ დონით.

რამოდენიმე ქვანტური ნაწილაკის მოწყობილობა ჩამოყალიბების პროცესშია. ერთ-ერთი ასეთი განვითარებული ექსპერიმენტული მიდგომა იყენებს ქვანტური ნაწილაკის წყვილს როგორც ორმაგ მიმართულებით კოდირებულ ლოგიკურ კუბიტს, რომლის მარცხენა ნაწილაკში ცალკეული ელექტრონი წარმოადგენს ლოგიკურ 0-ს, ხოლო მარჯვენა ნაწილაკის ელექტრონი 1-ს [ფუჯიცავა 1998]. სხვა ექსპერიმენტულ მიდგომებში გამოყენებულია ცალკეული ელექტრონის წრფოვი მასივის ქვანტური ნაწილაკები, რომელიც ქუბითის კოდირებას ახდენს ჭარბი ელექტრონის სპინში. [ლოსი და დივინჩენზო 1998].

ექსპერიმენტული მიდგომის მესამე ვარიანტი წარმოადგინა დივინჩენზომ, სადაც გამოიყენება მხოლოდ ერთი ოპერაცია - ორი მეზობელი ქუბითის ადგილის გაცვლა. ეს მიიღწევა ელექტრული პოტენციალის შემცირებით, რაც ელექტრონებს გადაადგილების საშუალებას აძლევს. [დივინჩენზო 2000; ლოსი და დივინჩენზო 1998; მირგრენი და უალეი 2003]. მაგნიტური ველის ზუსტი კონტროლისგან განსხვავებით ეს ოპერაცია შედარებით ადვილად განხორციელებადია, ვინაიდან ეს არ საჭიროებს კარიბჭეების სპეციფიკურ სამისამართო ბიტებთან მოქმედებას.

ამგვარი მიდგომის ყველაზე დიდი დაბრკოლება ალბათ ის არის, რომ გაცვლაზე დამყარებული გამოთვლა საჭიროებს ცალკეულ ლოგიკურ ქუბითის მრავალ ფიზიკურ ქუბითებად გარდაქმნას. მაგალითად CNOT ოპერაცია მოითხოვს თითოეული ქუბითის სამ ფიზიკურ ქუბითზე კოდირებას და გაცვლის დრო საკმაოდ ზუსტად უნდა

კონტროლირდებოდა. CNOT ოპერაცია მეზობელ ლოგიკურ ქუბითებზე მოითხოვს 19 გაცვლით ოპერაციას, [დივიჩენზო 2000], თუმცა მირგრინმა და უაღიშ შეიმუშავეს საინტერესო ოპტიმიზაციები რომელიც საშუალებას იძლევა 28%-ით ნაკლები ოპერაციების გამოყენებას ვიდრე ჩვეულებრივი 19 CNOT ოპერაციის ფორმულირება. უწყვეტად მომუშავე კომპილატორს შეუძლია კოდირების შესრულების დროის შემცირება, თუმცა ინფორმაციის შესანახი მოცულობა იგივე რჩება.

-*ძლიერი მხარე*. განვითარებული წარმოება.

-*სუსტი მხარე*. დაბალი კოჰერენციის დრო.

3.7 კეინის მოდელი

კეინმა წარმოადგინა კარგად სკალირებადი მყარი მდომარეობის NMR სისტემური გადაწყვეტილება, რომელიც კონტროლურად იყენებს მაღალი სკალირებულ ინტეგრაციის (VLSI) მეთოდებს [კეინი 1998]. ამ გადაწყვეტილების ინჟინერულ მხარის კვლევა განავითარა ოსკინმა და კოფსეიმ, რომლებმაც შემოგვთავაზეს ქუბითების დიდი დისტანციაზე გადატანა ტელეპორტიტების გამოყენებით. [ოსკინი 2003; კოფსეი 2003]. მის შეცდომების გასწორებაში და წარმოებაში მიღწეულია პროგრესი [კლარკი 2003]. ამ სისტემაში ინდივიდუალური ფოსფორის ატომები შეერთებულია სიკილონის სუბსტრატთან და მის ზედაპირზე კონტროლის სტრუქტურების ასაგებად გამოყენებულია სტანდარტული ფოტოლითოგრაფიული მეთოდები. ქუბითი მოთავსებულია ფოსფორის ბირთვის სპინში და მეზობელ ქუბითებზე მოქმედება ხდება ბირთვებზე დაწყვილებული ელექტრონებით. ელექტრონის ტალღის ფუნქციონირება კონტროლირდება სილიციუმის ზედაპირზე ჩაშენებული კონტროლერით. ფოსფორის მეზობელ ატომებს შორის მანძილი და კონტროლის კარიბჭეების ზუსტი განლაგება განსაზღვრავს ქუბითის მოქმედების სარისხს.

-*ძლიერი მხარე*. დიდი კოჰერენციის დრო.

-*სუსტი მხარე*. რთული წარმოება, ელექტრონის ტალღის ფუნქციონირების ადეკვატური გადაფარვა.

4. არქიტექტურა და აპლიკაცია

ამ თავში ქვანტური არითმეტიკის, სხვადასხვა შეცდომების გასწორების ფორმებით და კლასტერული მდგომარეობის გამოთვლების ახალი მიღწევებით, ნაჩვენები იქნება რამოდენიმე ტექნოლოგიის არქიტექტურული ასახვა.

4.1 არითმეტიკა

დღესდღეობით ფაქტორინგის მსოფლიო რეკორდია 768 ბიტი *[RSA Security Inc. 2009]*. წინა რეკორდი წარმოადგენდა 576 ბიტს, რომელსაც ერთი თვის განმავლობაში გამოყენებულ 104 კომპიუტერით და სამუშაო სადგურებით მიაღწიეს. მურის კანონზე გამომთვლელ პროცესორის სიჩქარიდან გამომდინარე (კომუნიკაციის, მეხსიერების და შეტანა/გამოტანის გამორიცხვით), რიცხვითი ველის მრიხცველის (NFS) უდიდესი გამოსათვლელი რიცხვი წელიწადში საშუალოდ 18 ბიტით იზრდება. დღევანდელი პროგრესის გათვალისწინებით 2018 წლისთვის მოსალოდნელია 1024 ბიტთან რიცხვის ფაქტორინგი ხოლო მისი გაუმჯობესება სავარაუდოდ 25 წლის შემდგომ მოხდება. *[კალვარი 2004; ლენსტრა 2007]*.

ქვანტური კომპიუტერის გამოყენებით შორის ალგორითმით 576 ბიტის რიცხვის ერთ თვიანი ფაქტორინგი უპირველეს ყოვლისა მოითხოვს ათასობით ლოგიკური ქუბითის ერთ თვიან კოპერენტულ მდგომარეობას. აგრეთვე ლოგიკური მოქმედების სიძქარე უნდა იყოს 0.3Hz - დან 27Hz -მდე *[ვან მეტერი 2005]*. ამ თავში არითმეტიკის გამოყენებით ნაცვენები იქნება მაგალითი იმისა, თუ როგორ გავლენას ახდენს ქვანტური კომპიუტერის არქიტექტურა ალგორითმის ასიმპტოტურ ($O(\cdot)$) მაჩვენებელზე და მის მუდმივ ფაქტორებზე *[ლანგი 2004]*. რამოდენიმე ალგორითმის რესურსების მოთხოვნილება და სესრულების გრაფიკი ფიქსირებულია, ხოლო სხვა ალგორითმები იყენებს გაზრდილ მოცულობას და პარალილელობას, რომელიც სექმის სიგრძის შემცირების და შედარებით დიდი პარალელიზმის საშუალებას იძლევა.

მაგალითისთვის განვიხილოთ მოდალური ექსპონენციალობა, რომელიც შორის ფაქტორინგის ალგორითმში გამოთვლების მხრივ ყველაზე ინტენსიურია. მკვლევარები

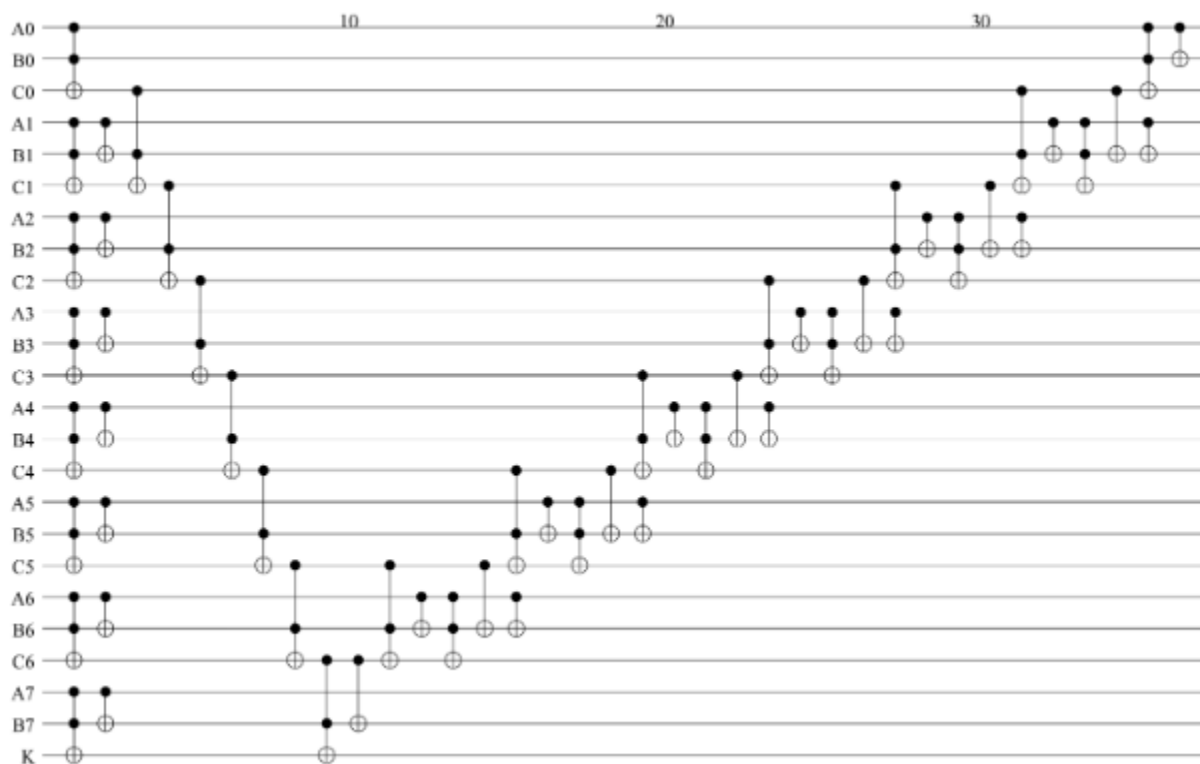
მუშაობდნენ საერთო ექსპონენციალურ ალგორითმზე [ვედრალი 1996; ბეკმენი 1996; ზალკა 1998] და არითმეტიკულ სტრუქტურებზე [გოსეტი 1998; კუკარო 2004], თუმცა შედარებით ცოტა რამ გაკეთდა ამ ალგორითმების რეალურ არქიტექტურაზე ასახვისთვის. [დევიტი 2004; ფოლვერი 2004; ვან მეტერი და იტო 2005; ვარტიანენი 2004].

მათემატიკურად ნაჩვენებია რომ მიუხედავად ქვანტური გამოთვლების სირთულსა, რომელიც არის $O(n^3)$, მისი სქემატური სიგრძე არის $O(\log^3 n)$ n ბიტთან რიცხვის ექსპონენციალური მაშინ როდესაც სრულდება სამი მნიშვნელოვანი პირობა : არქიტექტურას ყოველ ქუბითზე უნდა ქონდეს პარალელური კარიბჭეების მხარდაწერა, უნდა არსებობდეს $O(n^3)$ პროგრამული დონის ქუბითები და სისტემაში არსებულ ყველა ნებისმიერ ქუბითს უნდა შეემდოს ურთიერთკავშირი. [ქლივი და ვარტროსი 2000; ვან მეტერი და იტო 2005].

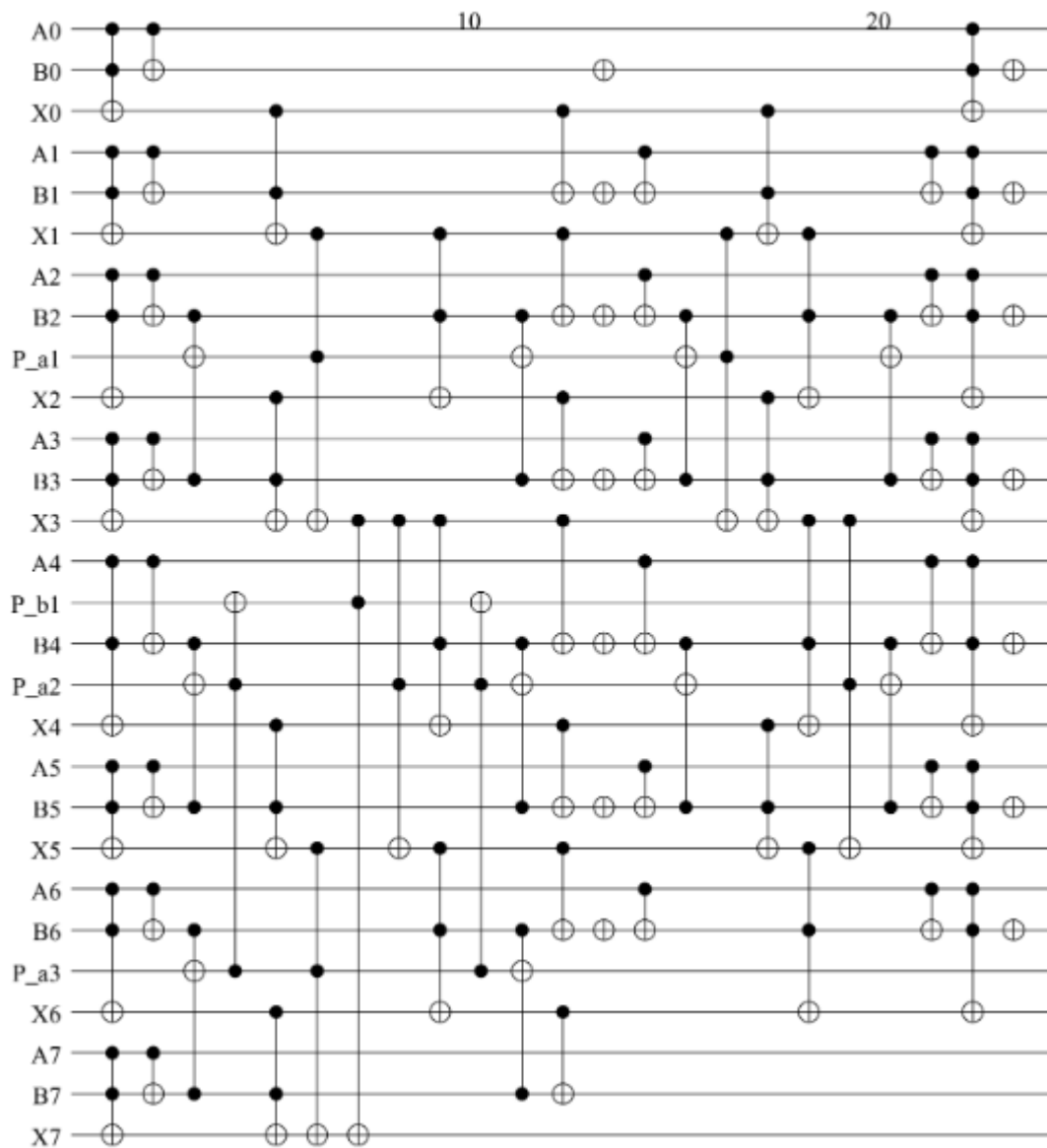
როდესაც ეს სამი პირობა არ სრულდება, სისტემური მახასიათებლები განიცდის სირთულეებს. მაშინ, როდესაც მხოლოდ $O(n^2)$ რაოდენობის ქუბითია ხელმისაწვდომი, ალგორითმის პარალელიზმი შემოსაზღვრულია და სიღრმე იზრდება $O(n \log^2 n)$ -მდე. მიღებული არქიტექტურული გადაწყვეტილებაა მხოლოდ მეზობელ ქუბითზე მოქმედი ქუბითების წრფივი ჯაჭვი, რომელიც სიღრმეს $O(n^2 \log n)$ -მდე ზრდის. არსებული სიღრმის შემდგომი შემცირებით გაიზრდება მისი ასიმპტოტური სიღრმე. 0.3Hz სიჩქარით მომუშავე ნელ ქვანტურ კომპიუტერის მუშაობისთვის საჭიროა რაც შეიძლება დიდი პარალელიზმი და შორ-გამტარი კარიბჭეები, ხოლო 27Hz სიჩქარის კომპიუტერი იყენებს დიდი პარალელიზმს მაგრამ მხოლოდ ახლომდებარე მეზობელ კარიბჭეების მოქმედებებს.

4 და 5 სურათში ნაჩვენებია ქვანტური შესაკრების ორი ტიპი, ვედრალ-ბარენკო-ეკერტის (VBE) მიღება-გადამცემის შესაკრები [ვედრალი 1996] და დტაპერ-კუტინ-რეინს-სვორის კომბინაციური გადაცემის შესაკრები [დრაპერი 2004]. ამ ორი შეკრების პირველი, თვალშისაცემი განსხვავებაა ის თუ როგორი „დატვირთულია“ მათი დიაგრამები. მიღება-გადაცემაში ჩანს რომ ქუბითების დიდი ნაწილი გამოთვლის მიმდინარეობის დროს უმეტესად უმოქმედო მდგომარეობაშია, ისინი ელოდებიან სიგნალის მიღებას, რის შემდგომაც გადაცემენ სქემის მიმდევრო წევრს (გაწმედნის დროს პირიქით). კომბინაციური გადაცემა უფრო მოქნილია, ერთდლოულად შესრულებულ კარიბჭეების ოპერაციით შეუძლია რამოდენიმე ბიჯში დაასრულოს მუშაობა.

მეორე ასეთი თვალსაჩინო განსხვავებაა კარიბჭეების სიგრძე (ვერტიკალური ხაზის სეგმენტები). მიღება-გადაცემის შესაკრები მოქმედებს მხოლოდ ახლო მდებარე ქუბითებზე, მაშინ როდესაც კომბინაციური გადაცემის შესაკრები შორ მანძილზე ოპერირებს. შორ მანძილზე მდებარე კარიბჭეების შემთხვევაში, მიღება-გადაცემის შესაკრები $O(n)$ კომბინაციურ გადაცემის შესაკრებთან შედარებით $O(\log n)$ უფრო ნელა იმუშავებს. მოცემული სქემების დიაგრამა აბსტრაქტულად წარმოაჩენს ქუბითების ფიზიკურ მდგომარეობას, ამის გამო შესაძლოა გაჩნდეს „ახლომდებარე“ ქუბითების არასწორი ინტერპრეტაცია.



სურათი 4. რვა-ბიტური ქვანტური (VBE) მიღება-გადაცემის შესაკრები. თითოეული ჰორიზონტალური ხაზი აღნიშნავს ქუბითს; ვერტიკალური ხაზის სეგმენტები წარმოადგენს ერთ, ორ ან სამ ქუბითიან კარიბჭეს.



სურათი 5. რვა-ბიტიანი ქვანტური კომბინაციური გადაცემის შესაკრები. თითოეული ჰორიზონტალური ხაზი აღნიშნავს ქუბიტს; ვერტიკალური ხაზის სეგმენტები წარმოადგენს ერთ, ორ ან სამ ქუბიტიან კარიბჭეს.

4.2 შეცდომების მართვა

შეცდომების მართვის სფერო შედგება რამოდენიმე ტიპის მეთოდისგან, თითოეული მათგანი სხვადასხვა შეცდომით პროცესების თავიდან აცილებას ემსახურება. ქვანტური შეცდომების გასწორების (QEC) და ასოცირებული შეცდომების უგულებელყოფის (FT) მეთოდები დაფუძნებულია კლასიკურ შეცდომების გასწორების კოდებზე. მათი პირველი და ყველაზე მნიშვნელოვანი კლასია კალდერმანკ-შორ-სტინის (CSS) კოდები [კალდერმანი და შორი 1996; სტინი 1996; პრესკილი 1998]. QEC და FT ოპერაციების თეორია და პრაქტიკა საკმაოდ ფართოა; ამ საკითხს დეტალურად ვერ განვიხილავთ, თუმცა საჭიროა მათი ძირითადი მახასიათებლების ჩამოყალიბება. QEC და FT მოითხოვს ანცილური (დროებით მომუშავე) ქუბიტების უწყვეტ მზადებას და გაზომვას. ის აგრეთვე ზრდის ქვანტური გამოთვლების საერთო მოთხოვნილებას, ვინაიდან სისტემაში QEC ყოველი დონეში ჩაშენებულია მაგნიტუდის ოთხი წყობა, რაც დამატებით ორი დონის მოთხოვნილებას ქმნის. QEC -ის შესრულების დრო მთლიანად აისახება სისტემის ლოგიკური მთვლელის სიჩქარეზე, თუმცა ზუსტი მაჩვენებელი დამოკიდებული იქნება ტექნოლოგიაზე და მექანიზმებზე დეტალებზე.

მოცემული QEC კოდები ერთ ან მეტ ქუბიტის კოდურ სიტყვად გარდაქმნის. ამ კოდურ სიტყვებში შეცდომის სინდრომი მუდმივად მოწმდება და იზომება, შემდგომ მათზე მოქმედებს გასწორების ოპერაციები. შეცდომების გასწორების სინდრომის გაზომვა გადაწყვეტს როლს თამაშობს შეცდომის კონტროლის პროცესზე; იგი მდგომარეობას აბრუნებს მაღალ ალბათობაში და გადასცემს ნულს (არ არის შეცდომა) ან შეცდომის მდგომარეობაში დაბალი ალბათობით რომელიც გადასცემს არანულოვან სინდრომს. როცა სინდრომი არანულოვანია, მასზე მოქმედებას იწყებს ერთი ან ორი გამსწორებელი კარიბჭე. სამწუხაროდ ასეთი სინდრომის გამოთვლას და გაზომვის დროსაც შეიძლება წარმოიქმნას სეცდომები. ტექნოლოგიები, რომელთაც მხოლოდ ახლომდებარე მოქმედებების მხარდაჭერა აქვთ, შეცდომების სინდრომის გამოსათვლელად მოითხოვენ ამ სინდრომის მატარებელ კარიბჭეების სხვა კარიბჭეებით ჩანაცვლებას, რაც სისტემურ მოთხოვნილებებს სამჯერ ზრდის. ქუბიტის მდგომარეობის გაზომვა რამოდენიმე ტექნოლოგიაში კარიბჭის

მოქმედებასთან შედარებით ნელია, ამგვარად შეცდომების გაცოცხლების დროზე ეს ფაქტორიც მნიშვნელოვნად მოქმედებს.

4.3 კლასტერული მდგომარეობის გამოთვლა

ბოლო წლებში ქვანტურ გამოთვლების თეორიულ წინსვლაში ყველაზე დიდი მიღწევა ალბათ კლასტერული მდგომარეობის (ერთ-მიმართულებიანი) გამოთვლების განვითარებაა [რაუზენდორფი 2003; ნილსენი 2005; ვალდერი 2005]. თეორიულად კლასტერული მდგომარეობის გამოთვლა გვთავაზობს გამოთვლითი გადაწყვეტილების ფართო მათემატიკურ პალიტრას; პრაქტიკული გამოყენებისთვის საუკეთესო მაგალითია ალუმინის საიზოლაციო სუბსტრატი რომელიც ზემოთ განვიხილეთ. კლასტერული მდგომარეობის გამოთვლა ქვანტური გამოთვლების შესაძლებლობებს იყენებს განსხვავებულად ვიდრე ძირითადი სქემატური მოდელი. ზუსტი გამოთვლების დაწყებამდე იქმნება საკმაო გადახლართული მდგომარეობა, რომელსაც კლასტერული მდგომარეობა ეწოდება. თავად გამოთვლა სრულდება სპეციფიკური სიხშირით განხორციელებულ თითო ქუბითურ გაზომვების საშუალებით. კლასტერული მდგომარეობის ზრდა შეიძლება იყოს ალბათური მაგრამ წინასწარ განსაზღვრავს ოპერაციის წარმატებულობას, რომელიც საჭიროების შემთხვევაში ოპერაციის უკან დაბრუნების საშუალებას იძლევა. ეს კარგადაა მორგებული წრფივი ოპტიკური ქვანტური გამოთვლის (LOQC) შესაძლებლობებთან. მიუხედავად იმისა, რომ კლასტერული მდგომარეობის გამოთვლა აბსტრაქტულია, არსებობს დიდი მოლოდინი რომ რეალიზებული ქვანტური გამოთვლები ამგვარ ტექნოლოგიებზე იქნება დაფუძნებული. [ნილი 2001; ნილსენი 2004].

დასკვნა

ეს ნაშრომში წარმოადგენს ქვანტურ კომპიუტერებზე არსებული ინფორმაციის ორგანიზების მცდელობას, რომელიც ფოკუსირებულია სკალირებადობაზე, იმპლიკაციაზე და არქიტექტურულ იმპლიმენტაციაზე. ქვანტური ტექნოლოგიებიდან გამოვყავით სტაციონარული და მფრინავი ქუბითები, ასევე განვიხილეთ სტაციონარული, მობუღური ქუბითების ქვეკლასი. სტაციონარული ქუბითური ტექნოლოგიები მოიცავს ცალკეულ და გაერთიანებულ სისტემებს. მოყვანილი შეფასების კრიტერიუმების საფუძველზე შესაძლებელი ხდება ტექნოლოგიების შედარება და გადაწყვეტა, თუ რომელი მათგანი იქნება სისტემის სხვადასხვა კომპონენტისთვის სასარგებლო. ასევე ეს საშუალებას მოგვცემს განვსაზღვროთ როგორ გადავიტანოთ და ავამუშავოთ პროგრამული ალგორითმები სხვადასხვა არქიტექტურაზე.

ზემოთ განხილული თითოეული ტექნოლოგია საჭიროებს გარკვეულ სიძნეელების გადალახვას იმისათვის, რომ შემდგომ ისინი პრაქტიკული კუთხით წარმოდგინდეს. NMR-ზე დაფუძნებულ სისტემებს აქვთ დაბალი კარიბჭის მოქმედების თუმცა კარგი კოჰერენციის დრო; თუ შესაძლებელი გახდება ქვანტური QIO მექანიზმის შემუშავება, მაშინ ისინი გახდებიან საუკეთესო შემნახველი მოწყობილობები, თუმცა სუფთა NMR სისტემები ვერ ქმნიან ადეკვატურ საწარმოო მექანიზმებს. იოსეფსონის გადაკვეთის მოწყობილობებს და ქვანტურ ნაწილაკებს აქვთ საკმაოდ სწრაფი კარიბჭის მოქმედების, მაგრამ დაბალი კოჰერენციის დრო. მოიხედავით იმისა, რომ ორივე ტექნოლოგია უკვე შემუშავებულია, ჯერ არ არის დემონსტრირებული მათი სკალირების იმპლიმენტაცია და ქუბითების დამისამართება. სუფთა ოპტიკური სისტემები საჭიროებს უფრო ეფექტურ ცალკეულ-ფოტონის დეტექტორებს. იონის ხაფანგებს გააჩნიათ ბევრი საჭირო მახასიათებელი, იმისათვის რომ შესაძლებელი გახდეს მათი არქიტექტურული სკალირებადობა.

ქვანტური კომპიუტერის კონტროლისათვის საჭიროა ისეთ დათმობაზე წასვლა, როგორიცაა სიჩქარის ხარჯზე კოჰერენციის დროის გაზრდა. ქვანტური ჩაწერა და კლასიკური კონტროლი ტექნოლოგიის და თეორიის კუთხით დღესაც ჩამოყალიბების პროცესშია, თუმცა ბევრი სკალირებდობის საკითხი ჯერაც რჩება შესამუშავებელი. ახლახან დაიწყო ქვანტური გამოთვლებისთვის და სპეციფიკური არქიტექტურული მახასიათებლების

ოპტიმიზაციისთვის საჭირო პროგრამული ენის შემუშავება. ამ ალგორითმების მოცემულ არქიტექტურებზე რეალიზაცია განსაზღვრავს კონკრეტული არქიტექტურის შესაძლებლობებს და პრაქტიკულობას.

დიდ რიცხვების გამოთვლებში, შორის ალგორითმი წარმოადგენს ქვანტური კომპიუტერების ყველაზე გამოკვეთილ გამოყენებას, რომელსაც შესწევს უნარი გაანეიტრალოს ფართოდ გამოყენებული უსაფრთხოების მექანიზმები როგორცაა: RSA კრიპტოსისტემა და დიფი-ჰელმანის გაცვლის პროტოკოლი. ქვანტური კოდირების ოპერაციებს და შორის ალგორითმის შესრულებას შემთხვევით არ აქვთ ერთი და იგივე n -ბიტთან გასაღებზე $O(n^3)$ მოქმედების დრო. უახლოეს მომავალში ორივე ტექნოლოგიის ქუბითების და კარიბჭეების წარმოებისათვის და ოპერირებისთვის საჭირო იქნება უფრო დიდი მაგნიტუდის მწკრივი, ვიდრე კლასიკური ბიტები მოითხოვენ. კლასიკურ სისტემებს უფრო ადვილათ შეუძლიათ გადალახონ დიდი მოცულობის კოდები ვიდრე ქვანტურ სისტემებს (მაგრამ ეს სიმარტივე აისახება მომხმარებლებზე და არა კოდის გატეხვაზე). მიუხედავად ამისა, თუნდაც ერთ ქვანტურ კომპიუტერის არსებობას შეუძლია გამოიწვიოს დღევანდელი კრიპტოსისტემის მიღწევების უკუსვლა და არასანდოობა. ამდენად, შორის ალგორითმი ვერ გახდება ეკონომიკური სტიმული ქვანტური კომპიუტერების წარმოების განვითარებისთვის. ამისათვის საჭიროა მნიშვნელოვანი ქვანტური გამოთვლითი ალგორითმის შემუშავება.

შეიძლება ითქვას, რომ ქვანტური კომპიუტერული არქიტექტურის სფერო განვითარების საწყის ეტაპზეა. დღესდღეობით მკვლევარები რომელიც ფოკუსირებულნი არიან ფუნდამენტურ ტექნოლოგიებზე, განიხილავენ ქვანტური გამოთვლითი სისტემების შემუშავებას. სისტემური არქიტექტორების ძალისხმევის შედეგად, უკვე პრაქტიკულად შესაძლებელი ხდება ერთზე მეტი ასეთი ტექნოლოგიის ხორცშესხმა. მოვლენების ამ სცენარით განვითარება იმედს გვაძლევს ქვანტური გამოთვლითი მოწყობილობები ჩამოყალიბდება იმ დონემდე, რომ შესაძლებელი გახდება მათი გამოყენებით რეალური პრობლემების გადაჭრა.

გამოყენებული ლიტერატურა

- AHARONOV, D. AND BEN-OR, M. 1999. Fault-tolerant quantum computation with constant error rate. <http://arXiv.org/quant-ph/9906129>. (Extended version of STOC 1997 paper.)
- BARENCO, A., EKERT, A., SUOMINEN, K.-A., AND TOFFINO, P. 1996. Approximate quantum Fourier transform and decoherence. *Phys. Rev. A* 54, 139–146.
- BECKMAN, D., CHARI, A. N., DEVABHAKTUNI, S., AND PRESKILL, J. 1996. Efficient networks for quantum factoring. *Phys. Rev. A* 54, 1034–1063. <http://arXiv.org/quant-ph/9602016>.
- BENNETT, C. H. AND BRASSARD, G. 1984. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*. IEEE. 175–179.
- BRENNEN, G. K., CAVES, C. M., JESSEN, P. S., AND DEUTSCH, I. H. 1999. Quantum logic gates in optical lattices. *Phys. Rev. Lett.* 82, 5 (Feb.), 1060–1063.
- BROWNE, D. E. AND RUDOLPH, T. 2005. Resource-efficient linear optical quantum computation. *Phys. Rev. Lett.* 95, 010501.
- CLARK, R. G. ET AL. 2003. Progress in silicon-based quantum computing. *Phil. Trans. R. Soc. London A* 361, 1451–1471.
- CLEVE, R. AND WATROUS, J. 2000. Fast parallel circuits for the quantum Fourier transform. In *Proceedings of the 41st Annual Symposium on Foundations of Computer Science*. ACM, New York, 526–536.
- DEVITT, S. J., FOWLER, A. G., AND HOLLENBERG, L. C. 2004. Simulations of Shor’s algorithm with implications to scaling and quantum error correction. <http://arXiv.org/quant-ph/0408081>.
- DIVINCENZO, D. P. 1994. Two-bit gates are universal for quantum computation. *Phys. Rev. A*. <http://arXiv.org/cond-mat/9407022>.
- DIVINCENZO, D. P. 1995. Quantum computation. *Science* 270, 5234, 255–261.
- DIVINCENZO, D. P., BACON, D., KEMPE, J., BURKARD, G., AND WHALEY, K. B. 2000. Universal quantum computation with the exchange interaction. *Nature* 408, 339–342.
- DRAPER, T. G. 2000. Addition on a quantum computer. <http://arXiv.org/quant-ph/0008033>. (First draft dated Sept. 1998.)
- ELLIOTT, C., PEARSON, D., AND TROXEL, G. 2003. Quantum cryptography in practice. In *Proceedings of the SIGCOMM 2003*. ACM, New York. <http://arXiv.org/quant-ph/0307049>.
- ERCEGOVAC, M. D. AND LANG, T. 2004. *Digital Arithmetic*. Morgan Kaufmann, San Francisco, CA.
- ESIA, JEITIA, KSIA, TSIA, AND SIA. 2003. International technology roadmap for semiconductors. Tech. Rep., ESIA and JEITIA and KSIA and TSIA and SIA. <http://public.itrs.net/Files/2003ITRS/Home2003.htm>.
- FLEISCHHAUER, M. AND LUKIN, M. D. 2000. Dark-state polaritons in

electromagnetically induced transparency. *Phys. Rev. Lett.* **84**, 5094–5097.

FOWLER, A. G., HILL, C. D., AND HOLLENBERG, L. C. L. 2004. Quantum error correction on linear nearest neighbor qubit arrays. *Phys. Rev. A* **69**, 042314.

FUJISAWA, T., OOSTERKAMP, T. H., VAN DER WIEL, W. G., BROER, B. W., AGUADO, R., TARUCHA, S., AND KOUWENHOVEN, L. P. 1998. Spontaneous emission spectrum in double quantum dot devices. *Science* **282**, 932–935.

FURUSAWA, A., SØRENSEN, J. L., BRAUNSTEIN, S. L., FUCHS, C. A., KIMBLE, H. J., AND POLZIK, E. S. 1998. Unconditional quantum teleportation. *Science* **282**, 5389, 706–709.

GALINDO, A. AND MARTIN-DELGADO, M. A. 2002. Information and computation: Classical and quantum aspects. *Rev. Modern Phys.* **74**, 347–423.

GASPARONI, S., PAN, J., WALTHER, P., RUDOLPH, T., AND ZEILINGER, A. 2004. Realization of a photonic controlled-NOT gate sufficient for quantum computation. *Phys. Rev. Lett.* **93**, 020504.

GOSSETT, P. 1998. Quantum carry-save arithmetic. <http://arXiv.org/quant-ph/9808061>.

GOTTESMAN, D. 1999. Fault tolerant quantum computation with local gates. <http://arXiv.org/quant-ph/9903099>.

GOTTESMAN, D. AND CHUANG, I. L. 1999. Quantum teleportation is a universal computational primitive. *Nature* **402**, 390–393.

GROVER, L. 1996. A fast quantum-mechanical algorithm for database search. In *Proceedings of the 28th Annual ACM Symposium on the Theory of Computation*. 212–219. <http://arXiv.org/quant-ph/9605043>.

GROVER, L. K. 1997. Quantum telecomputation. <http://arXiv.org/quant-ph/9704012>.

HALES, L. AND HALLGREN, S. 2000. An improved quantum Fourier transform algorithm and applications. In *Proceedings of the 41st Annual Symposium on Foundations of Computer Science*. ACM, New York.

CHONG, F. T., CHUANG, I. L., AND OSKIN, M. 2004. Datapath and control for quantum wires. *ACM Trans. Architecture and Code Optimization* **1**, 1 (Mar.).

JAMES, D. F. V. AND KWIAT, P. G. 2002. Atomic-vapor-based high efficiency optical detectors with photon number resolution. *Phys. Rev. Lett.* **89**, 183601.

WRATCHTRUP, J. 2004. Observation of coherence oscillation of a single nuclear spin and realization of a two-qubit conditional quantum gate. *Phys. Rev. Lett.* **93**, 130501.

KANE, B. E. 1998. A silicon-based nuclear spin quantum computer. *Nature* **393**, 133–137.

KAWANO, Y., YAMASHITA, S., AND KITAGAWA, M. 2005. Explicit implementation of quantum circuits on a unidirectional periodic structure. *Phys. Rev. A* **72**, 012301.

KIELPINSKI, D., MONROE, C., AND WINELAND, D. J. 2002. Architecture for a large-scale ion-trap quantum computer. *Nature* **417**, 709–711.

KIM, J. ET AL. 2005. System design for large-scale ion trap quantum information processor. *Quantum Inf. and Comput.* **5**, 7, 515–537.

KNILL, E. 2003. Bounds on the probability of success of postselected nonlinear sign shifts implemented with linear optics. *Phys. Rev. A* **68**, 064303.

KNILL, E., LAFLAMME, R., AND MILBURN, G. J. 2000. Thresholds for linear optics quantum computation. <http://arXiv.org/quant-ph/0006120>.

KNILL, E., LAFLAMME, R., AND MILBURN, G. J. 2001. A scheme for efficient

quantum computation with linear optics. *Nature* 409, 46–52.

KUNIHIO, N. 2005. Exact analyses of computational time for factoring in quantum computers. *IEICE Trans. Fundamentals E88-A*, 1, 105–111.

LADD, T. D., MARYENKO, D., YAMAMOTO, Y., ABE, E., AND ITOH, K. M. 2003. Coherence time of a solid-state nuclear qubit. <http://arXiv.org/quant-ph/0309164>.

LANTZ, J., WALLQUIST, M., SHUMEIKO, V. S., AND WENDIN, G. 2004. Josephson junction qubit network with current-controlled interaction. *Phys. Rev. B* 70, 140507.

LENSTRA, A., TROMER, E., SHAMIR, A., KORTSMIT, W., DODSON, B., HUGHES, J., AND LEYLAND, P. 2003. Factoring estimates for a 1024-bit RSA modulus. In *AsiaCrypt 2003*. Lecture Notes in Computer Science. Springer-Verlag, New York.

LEUNG, D. W., CHUANG, I. L., YAMAGUCHI, F., AND YAMAMOTO, Y. 2000. Efficient implementation of selective recoupling in heteronuclear spin systems using Hadamard matrices. *Phys. Rev. A* 61. <http://arXiv.org/quant-ph/9904100>.

LLOYD, S. 1993. A potentially realizable quantum computer. *Science* 261, 1569–1571.

LLOYD, S., SHAHRIAR, M. S., AND HEMMER, P. 2000. Teleportation and the quantum internet. <http://arXiv.org/quant-ph/0003147>.

LOSS, D. AND DIVINCENZO, D. P. 1998. Quantum computation with quantum dots. *Phys. Rev. A* 57, 120.

MARTINIS, J. M., NAM, S., AUMENTADO, J., AND URBINA, C. 2002. Rabi oscillations in a large Josephson-junction qubit. *Phys. Rev. Lett.* 89, 117901.

MOOIJ, J. E., ORLANDO, T. P., LEVITOV, L., TIAN, L., VAN DER WAL, C. H., AND LLOYD, S. 1999. Josephson persistent-current qubit. *Science* 285, 1036–1039.

MOORE, C. AND NILSSON, M. 2001. Parallel quantum computation and quantum codes. *SIAM J. Comput.* 31, 3, 799–815. <http://arxiv.org/abs/quant-ph/9808027>.

MOORE, G. E. 1965. Cramming more components onto integrated circuits. *Electronics* 38, 8 (Apr.).

MYRGREN, E. S. AND WHALEY, K. B. 2003. Implementing a quantum algorithm with exchange-coupled quantum dots: A feasibility study. *Quantum Inf. Proces.* to appear. <http://arXiv.org/quant-ph/0309051>.

NAKAJIMA, Y., KAWANO, Y., AND SEKIGAWA, H. 2005. A new algorithm for producing quantum circuits using KAK decompositions. <http://arXiv.org/quant-ph/0509196>.

NIELSEN, M. A. 2005. Cluster-state quantum computation. <http://arxiv.org/abs/quant-ph/0504097>.

NIELSEN, M. A. AND DAWSON, C. M. 2004. Fault-tolerant quantum computation with cluster states. <http://arXiv.org/quant-ph/0405134>.

O'BRIEN, J. L., PRYDE, G. J., WHITE, A. G., RALPH, T. C., AND BRANNING, D. 2003. Demonstration of an all-optical quantum controlled-NOT gate. *Nature* 426, 264–267.

Ó MER, B. 2002. Classical concepts in quantum programming. In *Proc. Quantum Structures*.

OSKIN, M., CHONG, F. T., CHUANG, I. L., AND KUBIATOWICZ, J. 2003. Building quantum wires: The long and short of it. In *Computer Architecture News, Proceedings of the 30th Annual International Symposium on Computer Architecture*. ACM, New York.

PASHKIN, Y. A., YAMAMOTO, T., ASTAFIEV, O., NAKAMURA, Y., AVERIN, D. V., AND TSAI, J. S. 2003. Quantum oscillations in two coupled charge qubits. *Nature* 421, 823–826.

PATERSON, K. G., PIPER, F., AND SCHACK, R. 2004. Why quantum cryptography? <http://arxiv.org/quant-ph/0406147>.

PATTERSON, D. A., GIBSON, G., AND KATZ, R. H. 1988. A case for redundant arrays of inexpensive disks (RAID). In *Proceedings of the 1998 ACM SIGMOD Conference*. ACM, New York, 109–116.

PELLIZZARI, T., GARDINER, S. A., CIRAC, J. RAUSSENDORF, R., BROWNE, D. E., AND BRIEGEL, H. J. 2003. Measurement-based quantum computation on cluster states. *Phys. Rev. A* **68**, 022312.

SANTORI, C., FATTAL, D., VUCKOVIC, J., SOLOMON, G. S., AND YAMAMOTO, Y. 2002. Indistinguishable photons from a single-photon device. *Nature* **419**, 594–597.

SHAHRIAR, M. S., HEMMER, P. R., LLOYD, S., BHATIA, P. S., AND CRAIG, A. E. 2002. Solid-state quantum computing using spectral holes. *Phys. Rev. A* **66**, 032301.

SHNIRMAN, A., SCHOEN, G., AND HERMON, Z. 1997. Quantum manipulations of small Josephson junctions. *Phys. Rev. Lett.* **79**, 2371–2374.

SHOR, P. W. 1994. Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings of the 35th Symposium on Foundations of Computer Science*. IEEE Computer Society Press, Los Alamitos, CA, 124–134.

SHOR, P. W. 1996. Fault-tolerant quantum computation. In *Proceedings of the 37th Symposium on Foundations of Computer Science*. IEEE Computer Society Press, Los Alamitos, CA, 56–65.

SHOR, P. W. 1997. Polynomial time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.* **26**, 5, 1484–1509. <http://arXiv.org/quant-ph/9508027>.

SKINNER, A. J., DAVENPORT, M. E., AND KANE, B. E. 2003. Hydrogenic spin quantum computing in silicon: A digital approach. *Phys. Rev. Lett.* **90**, 087901. <http://arXiv.org/quant-ph/0206159>.

SØRENSEN, A. AND MØLMER, K. 2000. Entanglement and quantum computation with ions in thermal motion. *Phys. Rev. A* **62**.

SPILLER, T. P., MUNRO, W. J., BARRETT, S. D., AND KOK, P. 2005. An introduction to quantum information processing: Applications and realisations. Tech. Rep. HPL-2005-192. Oct.

STEANE, A. 1996. Error correcting codes in quantum theory. *Phys. Rev. Lett.* **77**, 793–797.

STEANE, A. 1997. The ion trap quantum information processor. *Appl. Phys. B* **64**, 623–642.

STEANE, A. ET AL. 2000. Speed of ion trap quantum information processors. *Phys. Rev. A* **62**. <http://arXiv.org/quant-ph/0003087>.

STEANE, A. M. 2003. Overhead and noise threshold of fault-tolerant quantum error correction. *Phys. Rev. A* **68**, 042322. <http://arXiv.org/quant-ph/0207119>.

STEANE, A. M. AND IBINSON, B. 2003. Fault-tolerant logical gate networks for CSS codes. <http://arXiv.org/quant-ph/0311014>.

STEANE, A. M. AND LUCAS, D. M. 2000. Quantum computing with trapped ions, atoms, and light. *Fortschritte der Physik*. <http://arXiv.org/quant-ph/0004053>.

VAN METER, R. 2005. <http://www.tera.ics.keio.ac.jp/person/rdv/quantum/arithmetic.html>.

VAN METER, R. AND ITOH, K. M. 2005. Fast quantum modular exponentiation. *Phys. Rev. A* **71**, 5 (May), 052320. <http://arXiv.org/quant-ph/0408006>.

VAN METER, R., ITOH, K. M., AND LADD, T. D. 2005. Architecture-dependent execution time of Shor's algorithm. <http://arXiv.org/quant-ph/0507023>.

VANDERSYPEN, L. M. AND CHUANG, I. 2004. NMR techniques for quantum computation and control. *Rev. Modern Phys.* 76, 1037.

VANDERSYPEN, L. M. K., STEFFEN, M., BREYTA, G., YANNONI, C. S., SHERWOOD, M. H., AND CHUANG, I. L. 2001. Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance. *Nature* 414, 883–887.

VEDRAL, V., BARENCO, A., AND EKERT, A. 1996. Quantum networks for elementary arithmetic operations. *Phys. Rev. A* 54, 147–153. <http://arXiv.org/quant-ph/9511018>.

WALTHER, P., RESCH, K. J., RUDOLPH, T., SCHENCK, E., WEINFURTER, H., VEDRAL, V., ASPELMEYER, M., AND WINELAND, D. J. ET AL. 2005. Quantum control, quantum information processing, and quantum-limited metrology with trapped ions. In *Proceedings of the International Conference on Laser Spectroscopy (ICOLS)*. <http://arxiv.org/quant-ph/0508025>.

YAO, A. 1993. Quantum circuit complexity. In *Proceedings of the 34th Annual Symposium on Foundations of Computer Science*. IEEE Computer Society Press, Los Alamitos, CA, 352–361.

YIMSIRIWATTANA, A. AND LOMONACO JR., S. J. 2004. Distributed quantum computing: A distributed Shor algorithm. <http://arxiv.org/quant-ph/0403146>.

YORAN, N. AND REZNIK, B. 2003. Deterministic linear optics quantum computation with single photon qubits. *Phys. Rev. Lett.* 91, 037903.

YOU, J. Q., TSAI, J. S., AND NORI, F. 2003. Quantum computing with many superconducting qubits. <http://arXiv.org/cond-mat/0306208>.

YU, Y., HAN, S., CHU, X., CHU, S.-I., AND WANG, Z. 2002. Coherent temporal oscillations of macroscopic quantum states in a Josephson junction. *Science* 296, 5569, 889–892.