***Assallammu'alaikum Warahmatullahi Wabarakatuh***
***Selamat pagi dan salam sejahtera bagi kita semua***

Yang terhormat,
**Bapak Koordinator Kopertis Wilayah IV, Prof. Dr. Ir.Abdul Hakim Halim**
**Bapak Ketua Pembina Yayasan Cendekia Abditama, Bapak istiqnan Nasution**
**Bapak/Ibu Ketua Yayasan Pendidikan Cendekia Abditama, Drs.H. Islam Akbar Nasution**
**Bapak Ketua Sekolah Tinggi Teknik Cendekia (STTC) , Dr. Muhammad Subali**
**Bapak/Ibu Anggota Senat Akademika Sekolah Tinggi Teknik Cendekia**
**Bapak/Ibu Ketua Jurusan dan Kaprodi di lingkungan Sekolah Tinggi Teknik Cendekia,**
**Para staff pengajar di lingkungan Sekolah Tinggi Teknik Cendekia,**
**Para Orang Tua Wisudawan/wati,**
**Para Wisudawan/wati**
**Serta Para Undangan dan Hadirin yang sangat saya hormati,**

Pada kesempatan yang berbahagia ini, marilah kita bersama-sama memanjatkan puji syukur kehadirat Allah SWT, yang telah melimpahkan rahmat dan karunia-Nya kepada kita semua, sehingga pada pagi hari ini kita diizinkan dapat berkumpul di ruangan ini, dalam keadaan sehat walafiat, untuk mengikuti upacara Wisuda Pertama Angkatan 2004 s/d 2008. Shalawat dan salam kita haturkan pula pada junjungan Nabi besar Muhammad SAW.

Pertama-tama, perkenankanlah saya mengucapkan terima kasih yang setinggi-tingginya kepada Bapak Ketua STTC yang telah memberi kepercayaan dan kesempatan kepada saya untuk menyampaikan orasi ilmiah di hadapan sidang yang terhormat.

Pada hari yang istimewa ini, perkenankanlah pula saya menyampaikan selamat kepada para wisudawan/wait atas keberhasilannya menyelesaikan studi di STTC, dan kepada keluarga wisudawan atas keberhasilan putra-putrinya. Juga ucapan selamat saya sampaikan kepada civitas akademika STTC yang pada hari ini mempersembahkan alumninya kepada bangsa dan Negara Indonesia yang sedang berjuang, mengembangkan diri membangun masa depan yang lebih baik.

Suatu kehormatan bagi saya dapat menyampaikan orasi ilmiah dihadapan para wisudawan/wati dan seluruh civitas akademika STTC.

Oleh karena itu, pada kesempatan ini, izinkanlah saya menyampaikan orasi ilmiah, yang terkait dengan tema wisuda kali ini, dengan judul

# PROSPEK KOMPUTER KUANTUM DI MASA DEPAN

Saya membagi orasi ilmiah atas enam bagian, yaitu *1) Pendahuluan, Sejarah Komputer Kuantum, Perbedaan Utama Antara Komputer Kuantum dan Klasik; 2) Fisika Kuantum, Qubits, Parallelisme Kuantum, Partikel terbelit; 3) Potensi dan Kekuatan Komputasi Kuantum; 4) Permasalahan Dalam Produksi Komputer Kuantum; 5). Manfaat-Manfaat Komputer Kuantum di Masa Depan; 6) Hal Aneh Tentang Komputer Kuantum*

**Hadirin, Wisudawan dan Wisudawati yang saya hormati,**

## PENDAHULUAN

***"Dua gagasan abad ke-20 yang paling kuat, mekanika kuantum dan ilmu komputer, bersatu ke dalam kumpulan pengetahuan (body of knowledge) yang lebih kuat, melahirkan teknologi dan aplikasi baru dalam berbagai industri yang luas."***

Komputer dewasa ini , dengan semua keajaibannya, bekerja dengan prinsip dasar yang sama seperti perangkat mekanik yang dimimpikan oleh Charles Babbage pada abad ke-19 dan yang kemudian diformalkan oleh Alan Turing: ***Satu keadan yang stabil dari mesin merepresentasikan satu bilangan***. Bahkan model komputasi yang tampaknya tidak standar, seperti yang didasarkan pada DNA, berbagi prinsip dasar ini. Namun fisikawan telah menunjukkan bahwa hukum-hukum yang menjelaskan alam bukan hanya hukum sederhana dari mekanika klasik. Hukum tersebut adalah hukum-hukum fisika kuantum, dan hukum-hukum ini mengajak kita untuk berpikir secara berbeda tentang komputasi. Prinsip-prinsip komputasi yang telah memandu kita dengan baik sampai sekarang berasal dari fisika klasik dan dengan demikian, kita dapat pastikan, hanya sebagian saja yang ***benar***.

Baru-baru ini, fisikawan dan ilmuwan komputer telah menyadari bahwa tidak hanya ide-ide tentang komputasi yang menyisakan prinsip-prinsip yang ***hanya sebagian akurat***, tetapi mereka juga kehilangan seluruh kelas komputasi. Fisika kuantum menawarkan metode yang kuat dari pengkodean sampai manipulasi informasi yang tidak mungkin dapat dilakukan dalam kerangka klasik. Aplikasi potensial dari metode pengolahan informasi kuantum meliputi distribusi kunci aman yang dapat dibuktikan untuk kriptografi, Pemfaktoran bilangan bulat cepat, dan simulasi kuantum.

Teori informasi dan teori kuantum adalah di antara revolusi konseptual yang paling signifikan abad ke-20. Pemahaman akan teori-teori ini menyebabkan kemajuan besar teknologi abad ini. Pada abad ke-21 ini, kita berharap dapat melihat teori-teori ini bersatu untuk membentuk sebuah kekuatan yang lebih kuat untuk kemajuan: *teori kuantum informasi.*

Para ilmuwan memprediksi bahwa sekitar 2030 ada kemungkinan komputer sudah tidak memiliki transistor dan chip. Bayangkan sebuah komputer yang jauh lebih cepat daripada komputer silikon umum klasik saat ini. Komputer tersebut boleh jadi adalah sebuah komputer kuantum. Secara teoritis komputer kuantum dapat beroperasi tanpa konsumsi energi yang besar dan miliar kali lebih cepat dari komputer saat ini. Para ilmuwan sudah berpikir dan memandang bahwa sebuah komputer kuantum sebagai generasi berikutnya dari komputer klasik.

Gershenfeld mengatakan bahwa jika pembuatan transistor lebih kecil dan lebih kecil lagi dilanjutkan dengan tingkat yang sama seperti di tahun-tahun terakhir, maka sekitar tahun 2020, lebar kawat dalam sebuah chip komputer akan menjadi tidak lebih dari ukuran atom tunggal. Dalam ukuran skala atomik ini hukum fisika klasik tidak lagi berlaku. Komputer yang dirancang dengan teknologi chip saat ini ***tidak akan*** terus didapatkan lebih murah dan lebih baik. Karena kekuatannya yang besar, komputer kuantum merupakan langkah berikutnya yang menarik dalam teknologi komputer (Manay, 1998, hal. 5).

Teknologi komputer kuantum juga sangat berbeda. Untuk operasi, komputer kuantum menggunakan bit kuantum (qubit). Qubit memiliki sifat kuartener. Hukum mekanika kuantum sangat berbeda dengan hukum-hukum fisika klasik. Qubit dapat eksis tidak hanya pada keadaan-keadaan yang sesuai dengan nilai-nilai logika 0 atau 1 seperti dalam kasus sebuah bit klasik, tetapi juga dalam keadaan superposisi.

Qubit adalah sebuah bit informasi yang dapat menjadi 0 dan 1 secara bersamaan (keadaan superposisi). Dengan demikian, sebuah komputer yang lebih banyak beroperasi dengan sebuah qubit daripada dengan bit standar dapat melakukan perhitungan dengan menggunakan kedua nilai secara bersamaan. Sebuah Qubyte, terdiri dari delapan qubit dan dapat memiliki semua nilai dari 0 sampai 255 secara bersamaan. "Sistem multi-qubyte memiliki kekuatan melebihi apa pun yang mungkin dengan komputer klasik" (Quantum Komputer & Hukum Moore, hal.1) .

Empat puluh qubit dapat memiliki kekuatan yang sama dengan superkomputer modern. Menurut Chuang superkomputer membutuhkan sekitar satu bulan untuk menemukan sebuah nomor telepon dari database yang terdiri dari buku telepon dunia, sedangkan sebuah komputer kuantum dapat menyelesaikan tugas ini dalam 27 menit.

Massachusetts Institute of Technology, Oxford University, IBM and Los Alamos National Laboratory adalah sebuah contoh-contoh institusi paling sukses dalam pengembangan computer kuantum (West, 2000, &7).

**Hadirin, Wisudawan dan Wisudawati yang saya hormati,**

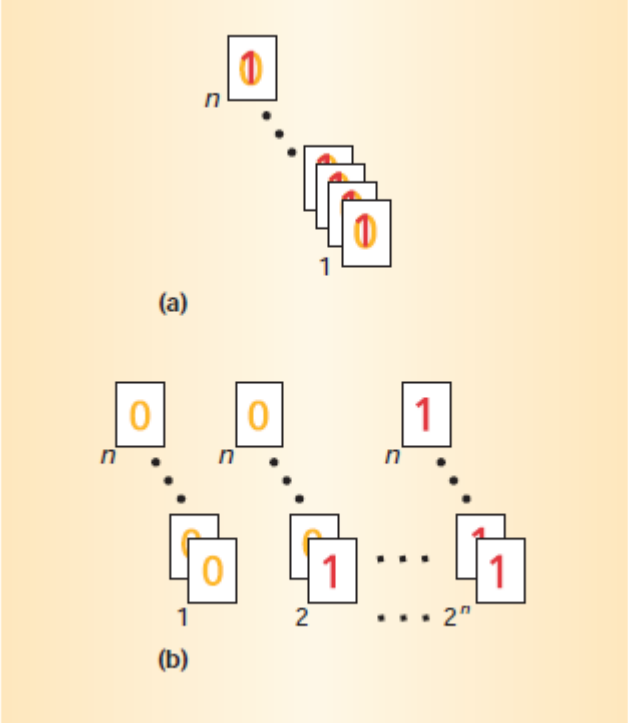
## *Sejarah Komputer Kuantum*

Pada tahun 1982 R.P. Feynman menyajikan sebuah ide yang menarik yaitu bagaimana sistem kuantum dapat digunakan untuk penalaran komputasi. Dia juga memberikan penjelasan bagaimana efek fisika kuantum dapat disimulasikan oleh komputer kuantum tersebut. Hal tersebut merupakan ide yang sangat menarik yang dapat digunakan untuk penelitian efek kuantum masa depan. Setiap percobaan yang menyelidiki efek dan hukum fisika kuantum adalah rumit dan mahal. Komputer Kuantum akan menjadi sebuah sistem yang mampu melakukan percobaan tersebut secara permanen. Kemudian pada akhir tahun 1985, terbukti bahwa komputer kuantum akan jauh lebih kuat (powerful) daripada komputer klasik (West, 2000, hal. 3).

## *Perbedaan Utama Antara Komputer Kuantum dan Klasik*

Memori komputer klasik merupakan string dari 0s dan 1s, dan ia mampu melakukan perhitungan hanya pada sekumpulan bilangan secara simultan. Memori komputer kuantum merupakan sebuah keadaan kuantum yang merupakan superposisi dari bilangan-bilangan yang berbeda. Sebuah komputer kuantum dapat melakukan perhitungan klasik reversible secara bebas pada semua bilangan secara bersamaan. Pelaksanaan sebuah komputasi pada bilangan yang berbeda pada saat yang sama dan kemudian penginterferesian semua hasil untuk mendapatkan satu jawaban, menjadikan sebuah komputer kuantum jauh lebih kuat daripada komputer klasik (West, 2000).

Sepanjang sejarah komputasi, bit tetap merupakan unit komputasi dasar informasi. Mekanika kuantum memungkinkan pengkodean informasi dalam bit kuantum (qubit). Tidak seperti bit klasik, yang hanya bisa menyimpan nilai tunggal - baik 0 atau 1 - qubit dapat menyimpan baik 0 dan 1 pada saat yang sama. Selanjutnya, register kuantum 64 qubit dapat menyimpan nilai $2^{64}$ sekaligus. Komputer Kuantum dapat melakukan perhitungan pada semua nilai-nilai ini pada saat yang sama. Namun, penggalian hasil dari perhitungan paralel masif telah terbukti sulit, membatasi jumlah aplikasi yang telah menunjukkan peningkatan kecepatan yang signifikan dibandingkan komputasi klasik. Paralelisme klasik juga dapat meningkatkan jumlah nilai yang ditangani secara bersamaan, tapi lama sebelum mencapai jumlah paralelisme yang dicapai oleh sebuah komputer kuantum, sebuah sistem klasik kehabisan ruang. Untuk sistem klasik, jumlah paralelisme meningkat dalam proporsi langsung dengan ukuran sistem; untuk sistem kuantum, paralelisme meningkat secara eksponensial dengan ukuran, seperti digambarkan pada Gambar 1.




Gambar 1. Parallelime klasik vs kuantu,: Untuk mencapai derajat parallelisme yang sama seperti (a) 300 prosessor kuantum (n = 300), kita memerlukan (b) $2^{300}$ prosessor klasik. Karena $2^{300}$ lebih banyak dari jumlah partikel di alam semesta, dapat dikatakan bahwa komputasi kuantum jelas memungkinkan peningkatan parallelisme secara astronomi.

Sistem kuantum dapat beroperasi pada keadaan terbelit. Belitan adalah istilah yang digunakan dalam teori kuantum untuk menggambarkan cara bahwa partikel energi/materi dapat menjadi berkorelasi, diduga dan diprediksi berinteraksi satu sama lain terlepas dari seberapa jauh mereka berada. Keadaan ini tidak memiliki analogi klasiknya. Keadaan terbelit, seperti pasangan EPR yang akan kita bahas segera, bertanggung jawab atas sebagian besar pencapaian paralelisme sistem kuantum. Dengan demikian, komputasi yang memanfaatkan paralelisme kuantum sering disebut pengolahan informasi "belitan" yang disempurnakan (*entanglement–enhanced information processing* ).

Setiap upaya untuk mengekstrak informasi dari sebuah keadaan memerlukan pengukuran. Sayangnya, dalam komputasi kuantum, pengukuran apapun mengganggu keadaan, sehingga menghancurkan paralelisme kuantum. Pada dasarnya, kita dapat mengajukan satu, dan hanya satu, pertanyaan tentang hasil yang dihasilkan oleh paralelisme kuantum sebelum melakukan komputasi ulang. Selain itu, jenis pertanyaan terbatasi dan merupakan subyek penelitian yang aktif. Peter Shor (Shor, 1997, hal.1.484) menemukan pertanyaan tunggal terkait masalah pemfaktoran, namun para peneliti telah menemukan pertanyaan yang demikian hanya untuk beberapa masalah.

Untuk pemfaktoran, paralelisme kuantum memberikan peningkatan kecepatan sangat besar sehingga tidak mungkin dijadikan menjadi komputasi praktis. Komputer kuantum juga secara eksponensial lebih baik dari komputer klasik pada perhitungan sifat-sifat sistem kuantum. Perhitungan tersebut tampaknya hanya menjadi perhatian sekelompok fisikawan, tetapi sebenarnya mereka akan berdampak luas bagi industri. Misalnya, fisika kuantum sangat penting untuk pembuatan perangkat yang semakin kecil atau kompleks, dan ia secara langsung mendasari kimia. Misalkan kita ingin memfabrikasi secara mikro perangkat nano yang presisi tinggi dan rumit. Kita perlu memahami sejumlah efek kuantum dalam merancang perangkat tersebut, dan waktu yang dihabiskan untuk sebuah komputer kuantum untuk mendapatkan pemahaman ini akan sangat berharga. Atau dalam bidang farmasi. Di antara molekul biologi yang dikendalikan oleh evolusi, kita dapat berharap untuk menemukan beberapa yang memanfaatkan efek kuantum yang secara komputasi klasik akan sulit diungkapkan. Sekali lagi, disini waktu komputer kuantum akan sangat penting.

Kenyataan bahwa pengukuran mengganggu keadaan kuantum ternyata menjadi manfaat dalam situasi lain. Misalkan kita ingin berkomunikasi secara rahasia. Jika kita menggunakan bit kuantum, “mata-mata” tidak dapat memperoleh apa pun tanpa mengganggunya, sebuah gangguan akan tercatat atau terdeteksi. Bahkan, dan ini menggambarkan bagaimana fisika kuantum, satu-satunya jenis pesan yang kita tahu bagaimana berbaginya dengan cara kuantum yang aman ini merupakan ***string bit yang benar-benar acak*** !. Akan tetapi, seperti kita ketahui, string acak merupakan kunci sempurna yang menjadi dasar skema kriptografi standar (klasik). Dengan memanfaatkan sistem komunikasi yang memiliki transmisi kunci dijamin oleh hukum alam, pemegang rekening bank dan komandan militer nantinya tak perlu lagi memiliki perasaan tidak aman.

**Hadirin, Wisudawan dan Wisudawati yang saya hormati,**

## FISIKA KUANTUM

Fisika kuantum adalah deskripsi prinsip-prinsip yang mendasari segala sesuatu yang bersifat fisik ("hukum alam") sebagaimana pemahaman para ilmuwan saat ini. Tetapi konsep kuantum seperti belitan dan masalah pengukuran tidak ada analoginya dalam kehidupan sehari-hari, dan hal ini sulit dipahami. Untuk abad yang lalu, fisikawan telah sering melakukan debat intens dan belum memperoleh jawaban yang memuaskan tentang bagaimana menafsirkan beberapa aspek mekanika kuantum, dan debat ini terus berlangsung sampai saat ini. Namun demikian, secara matematis teori fisika kuantum ini sepenuhnya dipahami dan sangat sukses, dan dari semua teori

fisika, fisika kuantum membuat prediksi yang paling tepat. Pemahaman rinci tentang cara kerja alam ini telah memungkinkan pengembangan berbagai macam aplikasi, termasuk transistor, laser, dan teknik pencitraan medis. Dengan demikian, fenomena kuantum, meskipun dalam beberapa hal sulit dijelaskan, dapat dimanfaat dan berguna.

## *Qubits*

Dalam sebuah percobaan yang terkenal, cahaya dari satu sumber melewati dua celah, menciptakan sebuah pola interferensi pada layar. Bahkan ketika sumber cahaya hanya memancarkan satu foton pada suatu waktu, pola interferensi muncul. Standar teori kuantum mendalilkan bahwa setiap foton bergerak pada kedua jalur (*path*) sekaligus. Dengan demikian, partikel dapat berada di dua tempat pada saat yang sama. Dalam situasi tersebut, kita mengatakan bahwa posisi partikel berada dalam superposisi dari dua keadaan.

Dua jalur perjalanan partikel dapat mewakili dua keadaan dari sebuah bit, 0 dan 1. Dalam mekanika kuantum, apabila sistem memiliki dua atau lebih peluang yang memungkinkan, ia dapat menjelajahi mereka secara bersamaan. Setiap sistem dua keadaan, seperti jalur foton, dapat mewakili qubit. Dalam komputer kuantum, kita malah mungkin menggunakan dua orbit elektron dalam atom untuk mewakili qubit. Atom bisa eksis dalam superposisi dari 0 dan 1, mirip seperti lonceng yang dipukul dapat bergetar pada dua frekuensi yang berbeda secara bersamaan.

## *Paralelisme Kuantum*

Komputer kuantum beroperasi pada kedua nilai yang disimpan pada setiap qubit pada waktu sama. Selain itu, ***n qubits***, masing-masing superposisi dari 0 dan 1, mengkodekan $2^n$ nilai, dan komputer kuantum dapat menghitung pada seluruh nilai ini sekaligus. Paralelisme yang besar ini, fungsi eksponen dari jumlah partikel yang digunakan dalam komputasi, disebut paralelisme kuantum. Setiap rangkaian klasik memiliki rangkaian kuantum yang sesuai (Deutsch, 1985, hal.97). Jadi sebuah komputer kuantum dapat melakukan perhitungan pada "***semua nilai***" dalam waktu hampir sama yang dibutuhkan oleh komputer biasa untuk melakukan perhitungan pada "***nilai tunggal***".

## *Partikel Terbelit*

Pada inti paralelisme kuantum terdapat kenyataan bahwa superposisi kuantum multi-partikel mengakui beberapa korelasi aneh (*strange*) tanpa analogi klasiknya. Untuk mendapatkan ide dari korelasi ini, bayangkan bahwa Alice dan Bob masing-masing diberi uang logam (yang akan kita anggap berperilaku seperti partikel). Ketika Alice dan Bob bermain dengan koin mereka masing-masing, koin-koin tampak berperilaku normal; khusus, pelemparan uang logam masing-masing memberikan hasil acak sempurna. Namun, kita segera melihat bahwa setiap kali koin Alice menujukan bagian kepala, begitu juga Bob, dan sebaliknya. Tidak ada cara komunikasi yang mungkin diantara koin. Sihir? Tidak, itulah mekanika kuantum (lihat Gambar 2).

Gambar 2. Korelasi kuantum aneh (Strange): Ketika Alice dan Bob bermain dengan koinnya masing, koin tampaknya berperilaku normal, pelemparan setiap koin memberikan hasil acak sempurna. Akan tetapi, kita akan segera mendapatkan bahwa setiap kali koin Alice muncul kepala, demikian juga koin Bob, dan sebaliknya. Karena tidak ada komunikasi yang mungkian antar koin, tentunya kita dapat beranggap hal tersebut adalah sulap "magic", bukan ? Bukan, itulah mekanika kuantum.

Meskipun fisikawan belum melihat korelasi demikian diantara objek besar yang terpisah, termasuk koin, mereka telah menemukan korelasi demikian diantara atom secara individu. Kita menyebut objek berkorelasi dengan cara ini ***kuantum mekanis belitan*** (*quantum mechanically entangled*). Pasangan obyek yang menunjukkan korelasi seperti itu disebut pasangan EPR (singkatan Einstein, Podolsky, dan Rosen, yang pertama kali membahasnya). Keadaan kuantum yang paling mungkin mengandung korelasi kuantum, dan fakta ini bertanggung jawab atas sifat eksponensial paralelisme kuantum dan keberhasilan kuantum algoritma. Hal tersebut merupakan pengamatan ***Richard Feynman*** yang menyatakan "bahwa komputer klasik tidak dapat secara efisien mensimulasikan beberapa jenis belitan" yang dipromosikan sebagai langkah awal ketertarikan pada komputasi kuantum" (Feynmen, 1996, hal.185).

## *Masalah Pengukuran*

Pengaksesan hasil yang diperoleh dari paralelisme kuantum memerlukan pengukuran keadaan akhir dari qubits. Setiap instrumen pengukuran mencatat hasil tunggal, meskipun komputer kuantum dapat menyimpan superposisi, kemungkinan sangat besar, dari nilai-nilai yang berbeda. Alam menyelesaikan paradoks ini dengan menghancurkan nilai-nilai lain dalam superposisi setiap kali pengukuran dilakukan, mengubah keadaan dari superposisi yang mungkin kompleks ke keadaan sederhana yang terdiri dari nilai tunggal terbaca. Untuk komputasi kuantum, kesulitan dalam mengakses nilai-nilai ini adalah satu keterbatasan yang sulit, membutuhkan teknik pemrograman yang sangat tidak konvensional untuk menyiasati masalah, seperti yang dilakukan ***Peter Shor*** dan ***Lov Grover*** (Shor, 1997. hal. 1.484; Gorver, 1996, hal. 212) .

**Hadirin, Wisudawan dan Wisudawati yang saya hormati,**

## POTENSI DAN KEKUATAN KOMPUTASI KUANTUM

Komputer kuantum dengan 500 qubit menghasilkan $2^{500}$ keadaan superposisi. Setiap keadaan akan setara secara klasik dengan sebuah daftar tunggal dari 500 0's dan 1's. Komputer yang demikian dapat beroperasi pada $2^{500}$ keadaan secara simultan (bersamaan). Pada akhirnya, pengamatan sistem akan menyebabkan runtuh menjadi sebuah keadaan kuantum tunggal yang sesau dengan sebuah jawaban tunggal, sebuah daftar tunggal dari 500 0's dan 1's, sebagaimana ditetapkan oleh aksioma pengukuran dari mekanika kuantum. Komputer jenis ini setara dengan komputer klasik yang memiliki prosesor kira $10^{150}$ (West, 2000, p. 3).

### *Hukum Moore Komputer Kuantum*

Menurut Hukum Moore, jumlah transistor dari sebuah mikroprosesor bertambah dua kali lipat setiap 18 bulan. Menurut evolusi tersebut jika terdapat komputer klasik di tahun 2020, maka ia akan beroperasi pada kecepatan CPU 40 GHz dengan 160 Mb RAM. Jika kita menggunakan analogi hukum Moore untuk komputer kuantum, jumlah bit kuantum akan menjadi dua kali lipat dalam setiap 18 bulan. Tetapi penambahan hanya satu qubit sudah cukup untuk meningkatkan kecepatan dua kali lipat . Jadi, kecepatan kuantum komputer akan meningkat lebih dari sekedar dua kali lipat itu (Quantum Komputer & Hukum Moore, § 1).

**Hadirin, Wisudawan dan Wisudawati yang saya hormati,**

## PERMASALAHAN DALAM PRODUKSI KOMPUTER KUANTUM

Setiap jenis pengukuran parameter keadaan kuantum memperhitungkan proses interaksi dengan lingkungan (dengan partikel lain - partikel cahaya misalnya), yang menyebabkan terjadinya perubahan beberapa parameter keadaan kuantum. Pengukuran keadaan kuantum superposisi akan meruntuhkan menjadi keadaan klasik. Kondisi ini disebut dekoherensi. Dekoherensi ini adalah kendala utama dalam proses produksi dari sebuah komputer kuantum. Jika masalah dekoherensi tidak dapat diselesaikan, sebuah komputer kuantum tidak akan menjadi "lebih baik" dibandingkan komputer klasik (Daniel, 1999).

Untuk membangun komputer kuantum yang kuat, banyak operasi harus dilakukan sebelum koherensi kuantum hilang. Hal ini dapat menjadi mustahil, membangun kuantum komputer yang akan melakukan perhitungan sebelum dekoherensi. Tapi jika kita membangun kuantum komputer, di mana jumlah kesalahan cukup rendah, maka hal itu dimungkinkan dengan menggunakan *"error-correcting code"* untuk mencegah kehilangan data bahkan ketika qubit di computer ber-dekoherensi. Terdapat banyak *"error-correcting codes"*. Salah satu error-correcting codes klasik yang paling sederhana adalah "repetition code". 0 dikodekan sebagai 000 dan 1 sebagai 111. Kemudian jika hanya satu bit membalik, kita akan memperoleh sebuah keadaan misalnya 011 yang dapat dikoreksi menjadi keadaan semulanya 111. Tanda-tanda keadaan dalam superposisi kuantum juga penting, tetapi kesalahan tanda juga dapat diperbaiki. Bahkan sudah tersedia teori tentang *"error-correcting codes"* kuantum (Daniel, 1999, p. 1).

Masalah lain adalah perangkat keras untuk komputer kuantum. Teknologi Nuclear Magnetic Resonance (NMR) adalah teknologi paling populer saat ini, karena beberapa percobaannya telah sukses. MIT dan Los Alamos National Laboratory telah dibangun sebuah kuantum komputer sederhana dengan menggunakan teknologi NMR. Beberapa desain lain didasarkan pada perangkap ion (*ion trape*) dan elektrodinamika kuantum (QED). Semua metode ini memiliki keterbatasan signifikan. Tidak ada yang tahu akan seperti apa arsitektur perangkat keras komputer kuantum di masa depan. (West, 2000, hal. 6)

**Hadirin, Wisudawan dan Wisudawati yang saya hormati,**

## MANFAAT-MANFAAT KOMPUTER KUANTUM DI MASA DEPAN

### *1. Kriptografi dan Algoritma Peter Shor*

Pada tahun 1994 Peter Shor (Bell Laboratories) menemukan algoritma kuantum pertama yang secara prinsip dapat melakukan faktorisasi yang efisien. Hal ini menjadi sebuah aplikasi kompleks yang hanya dapat dilakukan oleh sebuah komputer kuantum. Pemfaktoran adalah salah satu masalah yang paling penting dalam kriptografi. Misalnya, keamanan RSA (sistem keamanan perbankan elektronik) - kriptografi kunci publik - tergantung pada pemfaktoran dan hal itu akan menjadi masalah yang besar. Karena banyak fitur yang bermanfaat dari komputer kuantum, para ilmuwan berupaya lebih untuk membangunnya. Apabila, pemecahan segala jenis enkripsi saat ini memerlukan waktu hampir seabad pada komputer yang ada, mungkin hanya memakan waktu beberapa tahun pada komputer kuantum (Maney, 1998).

### *2. Kecerdasan Buatan* (*Artificial Intelligence*)

Seperti telah dijelaskan sebelumnya bahwa computer kuantum akan jauh lebih cepat dan konsekuensinya akan mampu melaksanakan sejumlah besar operasi dalam periode waktu yang sangat singkat. Di sisi lain, peningkatan kecepatan operasi akan membantu komputer untuk belajar lebih cepat meskipun dengan menggunakan salah satu metode yang paling sederhana, yaitu "*mistake bound model for learning*".

### *3. Manfaat Lain*

Kinerja tinggi akan memungkinkan kita untuk mengembangkan algoritma kompresi yang kompleks, pengenalan suara dan citra, simulasi molekular, keacakan sesungguhnya (*true randomness*) dan komunikasi kuantum. Keacakan sangat penting dalam simulasi. Simulasi Molekular sangat penting untuk pengembangan aplikasi simulasi pada bidang kimia dan biologi. Dengan bantuan komunikasi kuantum baik pengirim maupun penerima akan diberitahukan jika ada penyusup yang akan mencoba untuk menangkap sinyal. Qubits juga memungkinkan lebih banyak informasi yang dapat dikomunkasikan per bit. Komputer kuantum menjadikan komunikasi lebih aman.

**Hadirin, Wisudawan dan Wisudawati yang saya hormati,**

# HAL ANEH TENTANG KOMPUTER KUANTUM

"Di sisi teori, mekanika kuantum menggali jauh ke daerah yang hampir tak terpikirkan. Sebagai contoh, mungkin saja sebuah komputer kuantum mem-pertahankan jumlah tak terbatas jawaban yang tepat bagi jumlah tak terbatas alam semesta paralel. Ini terjadi begitu saja untuk memberikan jawaban yang tepat tentang alam semesta dimana kita berada pada saat itu. "Dibutuhkan banyak keberanian untuk menerima hal-hal ini," kata Charles Bennett dari IBM, salah satu ilmuwan komputasi kuantum terbaik. "Jika Anda melakukannya, Anda harus percaya pada banyak hal aneh lainnya" (Manay, 1998).

## *Tarian Atom Khloroform*

Beberapa tahun yang lalu, Gershenfeld dan Chuang membuat komputer kuantum pertama, berbasis teknologi resonansi magnetik nuklir. Program ini melakukan pencarian sederhana menggunakan algoritma Grover. Dibandingkan dengan komputer klasik, komputer kuantum ini mengambil satu item dari empat hanya dalam satu langkah, bukan dua atau tiga langkah seperti pada komputer klasik. Harga untuk membuat komputer 2-qubit pertama adalah sekitar $ 1 juta.

## *Belitan* (*Entanglement*) *dari Sistem Kuantum*

Menurut mekanika kuantum kekuatan luar yang bekerja pada dua partikel dari sistem kuantum dapat menyebabkan mereka menjadi terbelit. Keadaan kuantum dari sistem ini dapat berisi semua posisi spin (momen magnetik internal) dari setiap partikel. Spin total sistem hanya bisa sama untuk nilai diskrit tertentu dengan probabilitas yang berbeda. Pengukuran spin total sistem kuantum tertentu menunjukkan bahwa posisi spin beberapa partikel tidak independen dari yang lainnya. Untuk sistem tersebut, ketika orientasi spin dari satu partikel diubah dengan beberapa alasan, orientasi spin dari partikel lain akan berubah secara otomatis dan cepat. Hukum yang yang telah dikembangkan sejauh ini tentang kecepatan cahaya tidak taati dalam kasus ini, karena perubahan orientasi spin terjadi segera. Setidaknya ada hipotesis untuk menggunakan fenomena ini dalam komputasi kuantum.

Kita telah mengetahui bahwa kecepatan komunikasi dibatasi oleh kecepatan cahaya karena tidak ada sesuatupun dapat melakukan perjalanan lebih cepat dari kecepatan cahaya. Pertanyaannya adalah bagaimana partikel dari sistem kuantum berkomunikasi ketika mereka mengubah orientasi spinnya dan akibatnya keadaan vektornya. Ilmuwan terkenal menghabiskan banyak waktu membahas masalah ini. Ide Einstein, bahwa beberapa "parameter tersembunyi" yang tidak diketahui dari sistem kuantum berkontribusi terhadap efek ini, telah ditolak secara teoritis dan eksperimental.

Hal ini adalah salah satu contoh yang menunjukkan perbedaan antara realitas klasik dan kuantum. Efek sistem kuantum ini dapat menjelaskan banyak aspek alam (misalkan karakteristik kimia dari atom dan molekul) dan telah dibuktikan melalui oleh eksperimen.

"Secara fakta, teori tentang belitan (*entanglement*) telah menyebabkan para ilmuwan untuk percaya bahwa ada cara untuk mempercepat komputasi. Bahkan

komputer saat ini telah mendekati titik di mana kecepatan mereka dibatasi oleh seberapa cepat elektron dapat bergerak melalui kabel - kecepatan cahaya. Baik dalam komputer kuantum atau tradisional, belitan (*entanglement*) bisa memecahkan masa lalu yang membatasi "(Manay, 1998).

**Hadirin, Wisudawan dan Wisudawati yang saya hormati,**

## KESIMPULAN

Kita perlu mengetahui bahwa realisasi pembangunan komputer kuantum praktis hanya masalah waktu di masa depan. Gaya pemrograman untuk komputer kuantum juga akan sangat berbeda. Pengembangan kuantum komputer membutuhkan banyak uang. Bahkan para ilmuwan terbaik tidak dapat menjawab banyak pertanyaan tentang fisika kuantum. Komputer kuantum didasarkan pada teori fisika dan beberapa ekaperimen telah dilakukan. Komputer kuantum mudah memecahkan aplikasi yang tidak dapat dilakukan dengan bantuan komputer saat ini. Hal ini akan menjadi salah satu langkah terbesar dalam ilmu pengetahuan dan niscaya akan merevolusi dunia komputasi praktis.

**Hadirin, Wisudawan dan Wisudawati yang saya hormati,**

Dari mimbar yang mulia ini, dan juga dipenghujung orasi ini, dengan segala kerendahan hati, perkenankanlah saya menyampaikan puji syukur kepada ALLAH SWT atas segala rahmat dan karuniaNYA. Ucapan terima kasih yang tak terhingga saya sampaikan kepada: Ketua STTC, Ketua Senat Akademika STTC, Para Pembantu Ketua, Para Ketua Jurusan yang telah memberikan kesempatan dan kepercayaan kepada saya untuk memberikan orasi ilmiah ini.

Akhirnya tak lupa saya ucapkan terima kasih yang sebesar-besarnya kepada bapak ibu, saudara-saudara serta tamu undangan sekalian, atas kesabaran dan perhatiannya mengikuti orasi saya ini. Saya juga mohon maaf yang sedalam-dalamnya sekiranya dalam penyampaian orasi ini ada hal yang kurang berkenan di hati bapak dan ibu. Semoga ALLAH yang Maha Pengasih dan Penyayang membalas budi baik bapak dan ibu sekalian.

*Wa billahi taufik wal hidayah, wassallammu'alaikum warohmatullahi wabarakaatuh.*

## Daftar Pustaka


Daniel, G. (1999). Quantum Error-Correcting Codes. Retrieved on November 31st , 2002 from: http://qso.lanl.gov/~gottesma/QECC.html

Deutsch, D. (1985). Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer, *Proc. Royal Society of London*, Series A, A400, pp. 97-117.

R.P. Feynman,R.P. (1996). Quantum Mechanical Computers, *Lectures on Computation*, A.J.G. Hey and R.W. Alice, eds., Addison-Wesley, Reading, Mass., pp. 185-211.

Grover, L.K. (1996). A Fast Quantum Mechanical Algorithm for Database Search," *Proc. 28th Ann. ACM Symp. Theory of Computing*, ACM Press, New York, pp. 212-219.

Shor, P. (1997). Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, *SIAM J. Computing*, Oct. , pp. 1,484-1,509.

Manay, K. (1998). Quantum computers could be a billion times faster than Pentium III. *USA Today.* Retrieved on December 1st, 2002 from: http://www.amd1.com/quantumcomputers.html

Quantum Computers. Retrieved on December 1st , 2002 from: http://www.ewh.ieee. org/r10/bombay/news4/Quantum_Computers.htm

Quantum Computers & Moore's Law. Retrieved on December 1st , 2002 from: http://www.qubyte.com

Quantum Computers: What are They and What Do They Mean to Us? Retrieved on December 1st, 2002 from: http://www.carolla.com/quantum/QuantumCompu ters. htm

West, J (2000). Quantum Computers. Retrieved December 1st , 2002 from California Institute of Technology, educational website: http://www.cs.caltech.edu/~westside/quantum-intro.html#qc