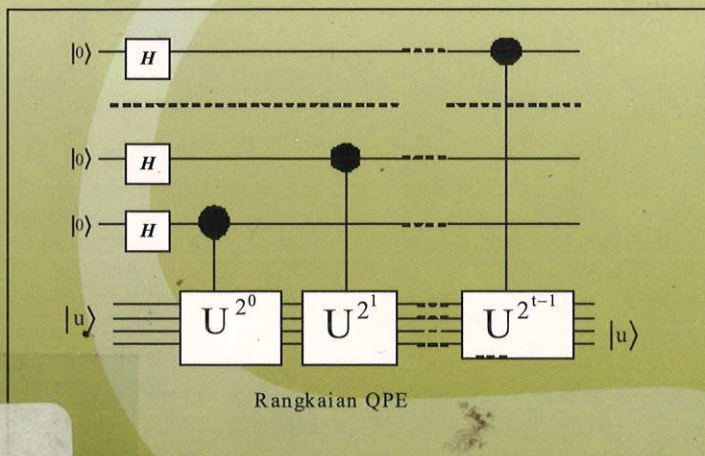


PENGANTAR TEORI **Komputasi kuantum**

B. Suprpto Brotosiswojo



Penerbit ITB

13. 8. 09 2011 R

Pengantar teori komputasi kuantum

No. Klass 530.12 BRO P.
No. Induk 125403 Tgl 12.8.09
Had/ah/Beli
Dari Ibu Lusi

Pengantar teori komputasi kuantum

B. Suprpto Brotosiswojo



530.12
BRO
P.



Penerbit ITB

R/
125403 SB / P.T.T/S
12.8.09.

Cetakan 1, 2006

Hak cipta dilindungi undang-undang
All rights reserved
© Penerbit ITB, 2006

Dilarang mengutip atau memperbanyak sebagian atau seluruh isi buku ini tanpa izin tertulis dari Penerbit ITB

Hak cipta pada Penerbit ITB, 2006

Data katalog dalam terbitan

BROTOSIWOJO, B. Suprpto

Pengantar teori komputasi kuantum. – Bandung:
Penerbit ITB, 2006.

8a, 105h., 21 cm.

530.12

ISBN 979-3507-81-0

Penerbit ITB, Jl. Ganesa 10 Bandung 40132
Telp.: 022-2504257, Fax.: 022-2534155
e-mail: itbpress@bdg.centrin.net.id

Daftar isi



Prakata 7a

Bab 1 Pendahuluan 1

- 1.1 Mengapa harus melibatkan fisika kuantum 2
- 1.2 Unsur dasar pada komputasi klasik 4
- 1.3 Cellular automata dengan quantum dot 5

Bab 2 Berhitung dengan ungkapan biner 9

- 2.1 Penggunaan lambang 13
- 2.2 Variabel bilangan kompleks 14
 - 2.2.1 Pasangan bilangan kompleks 16
 - 2.2.2 Lukisan dalam bidang kompleks 16
- 2.3 Basis logaritma e 17
- 2.4 Fungsi $\exp(i\varphi)$ 18

Bab 3 Pokok-pokok mekanika kuantum 20

- 3.1 Kaitan antara penalaran dan pengamatan (1) 22
 - 3.1.1 Aturan dasar (1) 24
 - 3.1.2 Aturan dasar (2) 24
 - 3.1.3 Aturan dasar (3) 25
- 3.2 Elemen dasar qubit 25
 - 3.2.1 Perwujudan fisik spin-(1/2) dalam ruang nyata 3-dimensi 26

Bab 4 Komputasi satu qubit 30

- 4.1 Lambang rangkaian kuantum 33

Bab 5 Kiriman kunci-sandi kriptografi yang aman 36

- 5.1 Cara sederhana pengiriman kunci-sandi 39

Bab 6 Komputasi dengan dua qbit 43

- 6.1 Keterikatan kuantum (*quantum entanglement*) 46

Bab 7	Memanfaatkan <i>quantum entanglement</i>	52
	7.1 Teleportasi kuantum	55
	7.2 Pengiriman informasi yang hemat (<i>superdense coding</i>)	58
Bab 8	Gate Toffoli	60
	8.1 Proses penjumlahan	65
Bab 9	Merentang fungsi gate cNOT	68
	9.1 Algoritma Deutsch-Jozsa	71
Bab 10	Transformasi fourier pada komputasi kuantum	78
	10.1 Vektor basis dan pengukuran	78
	10.2 Merentang Hadamard	79
	10.3 Evaluasi sebuah fungsi	83
	10.4 <i>Quantum phase estimation</i>	85
Bab 11	Kriptografi RSA	88
Bab 12	Faktorisasi lewat kumputasi kuantum	95
	12.1 Aljabar modulo	95
	12.2 <i>Continued fraction</i>	101
	12.3 Perbandingan kerja dengan faktorisasi klasik	102

Prakata

Menjelang akhir abad ke-20 kita menyaksikan perkembangan teknologi informasi dan komunikasi yang cepat dan telah mengubah pola hidup bermasyarakat. Sistem perkantoran, bisnis perbankan, komunikasi telpon genggam, internet, dan lain-lain, saat ini sudah mewarnai kehidupan masyarakat luas.

Mungkin kurang disadari bahwa bersamaan dengan itu juga berkembang ilmu yang menggarap objek-obyek alam dalam skala yang lebih kecil dari ukuran nanometer. Pemahaman manusia tentang perangai objek semacam itu, yang ternyata sangat berbeda dengan perangai objek-obyek alam dengan ukuran yang lebih besar, seperti yang kita lihat dalam kehidupan sehari-hari, sudah hampir mapan dengan berkembangnya fisika kuantum. Kini sejumlah teknologi skala nanometer mulai dapat diwujudkan.

Oleh karena itu, berkembanglah pula gagasan untuk merentang apa yang saat ini sudah digarap oleh teknologi informasi dan komunikasi untuk memanfaatkan objek-objek skala nanometer. Upaya untuk memahaminya tentu saja harus menggunakan aturan-aturan serta paradigma berpikir fisika kuantum, yang kadang-kadang sering dianggap "*counter intuitive*", karena ada kalanya keluar dari apa yang sudah kita pahami selama ini.

Sejumlah upaya dalam memahami bidang Komputasi Kuantum sudah menjadi garapan pakar-pakar di banyak negara. Beberapa hasilnya telah terwujud secara nyata.

Tertarik akan masalah tersebut yang mungkin dampaknya akan melanda seluruh dunia, penulis merasa perlu untuk membekali generasi muda dengan sebuah cakrawala baru. Tahun-tahun terakhir ini penulis mencoba mewujudkannya dalam bentuk kuliah Komputasi Kuantum pada

mahasiswa di Institut Teknologi Bandung dan Universitas Katolik Parahyangan. Bahan-bahan kuliah itulah yang akhirnya melahirkan buku ini.

Bandung, April 2006

B Suprpto Brotosiswojo

Bab 1

Pendahuluan



Pada semester kedua tahun ajaran 2004-2005 penulis bertugas mengisi kuliah “Kapita Selekta Fisika Komputasi” untuk mahasiswa tingkat akhir program studi fisika di Institut Teknologi Bandung dan Universitas Katolik Parahyangan Bandung. Menilik judul kuliahnya, dirasa perlu menyajikan bahan yang sifatnya khusus, serta merupakan topik keilmuan yang sedang berkembang, dalam arti masih menjadi objek penelitian yang digeluti banyak pakar di pelbagai tempat di dunia. Oleh karena itu, dipilihlah topik “komputasi kuantum”.

Perkembangan teknologi yang terkait dengan komputasi serta telekomunikasi informasi telah berjalan sangat cepat serta dirasakan dampaknya dalam mengubah perilaku kehidupan masyarakat. Hal itu tentunya juga memicu upaya para peneliti dalam mengembangkan arena ini secara berkelanjutan. Bersamaan dengan berkembangnya teknologi untuk objek-objek alam berukuran nanometer, rasanya tidak ada salahnya proses komputasi yang sekarang sudah mencatat prestasi yang menakjubkan juga direntang kemungkinannya untuk digarap dengan objek-objek skala nanometer tersebut.

Topik tersebut, meski materinya sudah banyak beredar di internet, tetapi tampaknya belum banyak disadari di Indonesia. Buku ini ditulis untuk membantu mereka yang memiliki keinginan memperluas cakrawala pandangannya agar dapat mengantisipasi masa depan “teknologi informasi dan komunikasi”, sebelum teknologi semacam itu melanda masyarakat kita. Penulis berusaha agar materi dalam buku ini dapat dipahami oleh para mahasiswa tingkat akhir strata-1, atau mereka yang belajar pada jenjang pascasarjana. Selain itu, buku ini tidak hanya ditujukan untuk mereka yang mengambil program studi fisika, tetapi diharapkan juga berguna bagi mereka yang berkecimpung dalam arena teknologi informasi dan komunikasi. Penggunaan ‘mekanika kuantum’ dibatasi hanya pada hal-hal yang sangat mendasar. Fokus sajian

dipusatkan pada perkiraan munculnya hal-hal baru yang tidak sanggup diwujudkan oleh komputasi klasik yang selama ini sudah kita miliki.

1.1 Mengapa harus melibatkan fisika kuantum?

Kalau kita tengok dari sejarah perkembangannya, teknologi komputasi saat ini dapat diwujudkan, awalnya, karena ditemukannya cara membuat transistor dengan memanfaatkan perkembangan fisika zat padat di sekitar masa akhir Perang Dunia II. Sejak saat itu, pesawat radio yang menggunakan elektronika dalam bentuk “tabung hampa udara” yang ukurannya besar dan mudah pecah dapat digantikan oleh objek bahan semikonduktor yang ukurannya kecil. Zaman itu, pesawat radio berubah bentuk dari yang ukurannya besar sehingga sebaiknya tidak dipindah tempat, menjadi yang diberi istilah “radio transistor” dengan ukuran kecil, dapat dibawa ke mana-mana karena cukup menggunakan tenaga listrik dari baterai.

Terpikir kemudian bahwa “mesin komputer” yang waktu itu juga menggunakan “tabung hampa udara” dapat pula diubah sehingga ukurannya kecil lewat proses “miniaturisasi” rangkaian elektroniknya. Proses tersebut berlanjut hingga saat ini, dan manusia mampu membuat prosesor dengan kecepatan 10^9 langkah dalam satu detiknya. Juga ukuran alat penyimpan datanya dapat diperkecil hingga “hard-disk” dengan kapasitas sekitar 40 GB pun dapat dimasukkan kantong saku untuk dibawa ke mana-mana. Sudah dapat dipastikan bahwa perlombaan proses miniaturisasi ini akan berlanjut terus sampai tiba pada tahap kejenuhan.

Batas “kejenuhan” semacam itu dapat terjadi karena dua hal. Yang pertama, karena tidak diperlukan lagi prosesor yang lebih cepat lagi, seperti kejenuhan pada kecepatan kendaraan mobil. Bukan berarti secara teknis manusia tidak dapat membuat mobil yang kecepatannya lebih tinggi, melainkan kejenuhan itu terjadi akibat keterbatasan reaksi pengemudinya ataupun karena kemacetan jalan. Yang kedua, kejenuhan terjadi karena memang secara teknis proses semacam itu sukar untuk diwujudkan. Tampaknya alasan yang pertama tidak berlaku dalam hal ini, tetapi alasan yang kedua itu lebih terasa. Sekarang pun, kalau kita cermati apa yang ada pada mesin komputer kecil kita dengan kecepatan prosesor sekitar 10^9 langkah per detik, selalu ditemukan sebuah kipas

pendingin. Maknanya, proses komputasi itu menimbulkan panas yang dapat mengganggu jika suhunya menjadi terlalu tinggi. Lalu, apa akar permasalahannya?

Proses “miniaturisasi” pada dasarnya hanya memperkecil ukuran rangkaian elektroniknya. Proses “nyala-padam” yang digunakan dalam rangkaian tersebut masih mengandalkan pada **arus listrik** lewat “kawat penghubung”. Kita mengetahui dari pengetahuan tentang arus listrik bahwa arus tersebut menimbulkan panas. Elektron-elektron dalam jumlah sangat besar yang ada pada bahan konduktor itu harus saling mendesak ketika terdapat beda potensial antara ujung yang satu dengan ujung yang lainnya untuk dapat menuju lokasi potensial yang lebih rendah.

Bahan yang kita sebut konduktor itu masih “menghambat” jalannya elektron, karena itu ada istilah “hambatan”, biasanya diberi lambang R . Kalau arus listrik yang mengalir besarnya I , maka panas yang dihasilkan setiap detiknya adalah I^2R . Kipas angin yang ada pada mesin komputer kita digunakan untuk mengimbangi akibat panas yang dihasilkan oleh arus itu.

Lalu apa masalahnya? Bukankah kalau nanti jumlah “kawat-kawat” penyalur makin banyak, kipas anginnya kita perkuat untuk mengimbangi timbulnya panas tadi? Betul, tetapi kita perlu bertanya berapa ukuran diameter “kawat” penyalur arus listrik itu agar “kawat” yang satu tidak mengganggu proses aliran listrik pada “kawat” yang lain? Inilah akar masalahnya! Kalau diameter “kawat” menjadi sangat kecil mendekati ukuran atom, maka kita tidak lagi dapat menyebutnya sebagai “kawat” dalam arti dapat digunakan secara bebas mengarahkan jalannya arus listrik tanpa ada gangguan oleh “kawat” yang lain, yang dalam rangkaian elektronik tersebut letaknya berdekatan.

Lalu bagaimana solusinya? Kita bertanya lebih jauh lagi ... apa gunanya arus listrik itu? Bukankah yang ingin kita proses itu bukan arus listrik melainkan sebuah “informasi” tentang sifat yang dapat diungkapkan dalam dua besaran: “benar” dan “salah” (dalam ungkapan logika), “0” dan “1” (dalam ungkapan bilangan sistem biner), atau “nyala” dan “padam” (dalam ungkapan listrik). Bagaimana caranya kita menggantikan aliran elektron yang berduyun-duyun saling bertabrakan pada arus listrik itu?

1.2 Unsur dasar pada komputasi klasik

Seperti dimaklumi, pada proses komputasi klasik (yang digunakan saat ini) dikenal objek yang disebut **register**, yaitu deretan bit untuk melukiskan data. Lalu ada lagi objek yang diberi nama **gate** yang melukiskan bagaimana data tersebut akan diubah menjadi data lain. Tentu saja data pada register hanya berisi lambang “0” dan “1”, misalnya untuk register dengan 8-bit 01011011. Dalam ungkapan berhitung memakai basis desimal, objek semacam itu melukiskan bilangan desimal $0 \times 2^7 + 1 \times 2^6 + 0 \times 2^5 + 1 \times 2^4 + 1 \times 2^3 + 0 \times 2^2 + 1 \times 2^1 + 1 \times 2^0 = 64 + 16 + 8 + 2 + 1 = 91$.

Dengan register 8-bit, kita hanya dapat mengungkap bilangan dari 0 hingga 255, jumlah semuanya ada $2^8 = 256$ macam. Jadi, bilangan desimal 300, misalnya, jika diungkap dalam register 8-bit, muncul sebagai 44 (= 300 modulo 256). Artinya, besarnya ukuran register menentukan banyaknya bilangan asli desimal yang dapat ungkapkan. Mesin komputer yang paling sederhana menggunakan register 8-bit, cukup untuk mengkaitkan bilangan-bilangan yang sanggup diungkapkannya dengan jumlah tombol alfabet (huruf kecil dan huruf besar), tanda-tanda kalimat, serta lambang bilangan 0 s/d 9 yang ada di keyboard. Dengan demikian, mesin tersebut dapat kita gunakan untuk mengetik surat.

Ada sejumlah gate yang selama ini digunakan sebagai unsur dasar dalam komputasi klasik. Ada gate untuk satu bit, yaitu gate **NOT**, yang mengubah “0” menjadi “1” dan mengubah “1” jadi “0”. Dalam ungkapan rangkaian listrik, itu berupa “switch” atau dapat diperankan oleh sebuah komponen transistor. Ada lagi gate **OR** yang dapat diperankan oleh rangkaian paralel. Dua bit masukan menghasilkan satu bit keluaran. Kalau “0” melambangkan situasi tak ada arus (“padam”) dan “1” melambangkan adanya arus (“nyala”), maka:

* jika masukan yang kesatu “padam” yang kedua “padam” hasil keluarannya “padam”

* jika masukan yang kesatu “padam” yang kedua “nyala” hasil keluarannya “nyala”

* jika masukan yang kesatu “padam” yang kedua “padam” hasil keluarannya “nyala”

* jika masukan yang kesatu “nyala” yang kedua “nyala” hasil keluarannya “nyala”

Ada lagi gate **AND** yang dapat diperankan oleh rangkaian seri:

* jika masukan yang kesatu “padam” yang kedua “padam” hasil keluarannya “padam”

* jika masukan yang kesatu “padam” yang kedua “nyala” hasil keluarannya “padam”

* jika masukan yang kesatu “padam” yang kedua “padam” hasil keluarannya “padam”

* jika masukan yang kesatu “nyala” yang kedua “nyala” hasil keluarannya “nyala”

Dengan tiga unsur dasar gate ini kemudian dapat disusun rangkaian yang lebih rumit yang sanggup melakukan tugas-tugas tertentu dalam masalah komputasi. Jadi, yang ingin kita cari adalah bagaimana caranya agar “arus listrik” itu tidak lagi menjadi andalan utama berfungsinya ketiga gate dasar tadi

1.3 Cellular automata dengan quantum dot

Saat ini, teknologi telah memungkinkan orang membuat objek yang namanya quantum dot, berupa keping logam atau semikonduktor, yang menjerat sejumlah elektron di dalamnya. Ukurannya yang terkecil dapat mencapai sekitar 30 nanometer sehingga dipikirkanlah alternatif lain untuk menggarap cara kerja mesin komputer dengan menggunakan objek ini. Gagasan itu pertama kali diungkapkan oleh Craig Lent dari The University of Notre Dame (USA) di tahun 1995 pada seminar di MIT (USA).

Andaikan kita punya elemen quantum dot, yang satu berisi satu elektron dan yang lain tidak berisi satu elektron.