Pendahuluan

Informasi kuantum adalah studi tentang bagaimana informasi disimpan, diproses, dikirim, dan dilindungi ketika pembawa informasinya adalah sistem kuantum. “Sistem kuantum” berarti sistem fisik yang perilakunya dijelaskan oleh mekanika kuantum, misalnya elektron, foton, atom, ion, atau rangkaian superkonduktor pada suhu sangat rendah. Pada skala sehari-hari, kita biasa membayangkan benda memiliki sifat yang pasti: lampu menyala atau mati, sakelar naik atau turun, koin menunjukkan kepala atau ekor. Pada skala kuantum, cara alam menyimpan kemungkinan lebih halus daripada itu. Kemungkinan tidak sekadar angka peluang biasa; ia diwakili oleh amplitudo kompleks yang dapat saling memperkuat atau saling meniadakan. Dari sinilah muncul kekuatan, keanehan, dan kesulitan informasi kuantum.

Buku ini mengajak Anda membangun bidang tersebut dari dasar. Kita tidak akan mulai dengan janji bahwa komputer kuantum “selalu lebih cepat” daripada komputer klasik, sebab pernyataan itu keliru. Komputer kuantum unggul untuk tugas tertentu yang strukturnya cocok dengan interferensi dan entanglement kuantum, tetapi banyak tugas tetap tidak diketahui memiliki percepatan kuantum yang berarti. Sikap yang tepat adalah lebih tenang: teori kuantum memberi model informasi yang berbeda, dan model berbeda ini membuka algoritma, protokol komunikasi, serta metode koreksi galat yang tidak tersedia dalam teori klasik.

Gagasan bahwa hukum fisika membatasi dan sekaligus memungkinkan cara kita menghitung bukanlah tambahan kecil pada ilmu komputer. Richard Feynman berargumen bahwa mensimulasikan sistem kuantum dengan komputer klasik tampak sangat mahal karena ukuran deskripsi kuantum tumbuh sangat cepat, dan ia mengusulkan bahwa komputer yang sendiri bersifat kuantum dapat menjadi alat alami untuk simulasi fisika kuantum (Feynman, 1982). David Deutsch kemudian merumuskan model komputer kuantum universal, yaitu model abstrak mesin yang dapat menjalankan proses komputasi kuantum secara umum (Deutsch, 1985). Dari titik ini, informasi kuantum berkembang menjadi bidang yang menghubungkan fisika, matematika, ilmu komputer, kriptografi, dan rekayasa perangkat keras.

Dari bit ke qubit

Dalam komputasi klasik, satuan informasi dasar adalah bit. Bit hanya memiliki dua nilai yang mungkin, biasanya ditulis sebagai 0 dan 1. Contohnya, satu bit dapat menyatakan apakah sebuah lampu mati atau menyala, apakah jawaban ujian salah atau benar, atau apakah tegangan listrik berada di bawah atau di atas ambang tertentu. Komputer modern mengolah bit melalui gerbang logika seperti AND, OR, dan NOT.

Dalam informasi kuantum, satuan dasar yang sebanding dengan bit disebut qubit, singkatan dari quantum bit. Qubit juga memiliki dua keadaan basis yang biasanya ditulis sebagai $|0\rangle$ dan $|1\rangle$. Simbol $|\cdot\rangle$ disebut notasi Dirac, dan akan dibahas lebih sistematis pada bab tentang aljabar linear. Untuk sementara, Anda dapat membacanya sebagai cara menulis vektor keadaan kuantum.

Perbedaannya adalah qubit dapat berada dalam superposisi, yaitu keadaan berbentuk

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle,$$

dengan α dan β adalah bilangan kompleks yang disebut amplitudo, serta memenuhi

$$|\alpha|^2 + |\beta|^2 = 1.$$

Bilangan $|\alpha|^2$ dan $|\beta|^2$ adalah peluang mendapatkan hasil 0 atau 1 ketika qubit diukur dalam basis $|0\rangle$, $|1\rangle$, sesuai aturan Born dalam mekanika kuantum (Nielsen & Chuang, 2010). Misalnya, jika

$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle,$$

maka pengukuran menghasilkan 0 dengan peluang 1/2 dan 1 dengan peluang 1/2.

Namun superposisi bukan sekadar “kita belum tahu apakah nilainya 0 atau 1”. Dalam ketidakpastian klasik, seperti koin tertutup di atas meja, koin sebenarnya sudah kepala atau ekor; kita hanya belum melihatnya. Pada qubit, amplitudo dapat mengalami interferensi. Interferensi berarti kontribusi amplitudo dari beberapa jalur proses dapat bertambah atau mengurangi satu sama lain. Inilah salah satu mekanisme inti algoritma kuantum. Sebuah algoritma kuantum yang baik bukan hanya “mencoba banyak jawaban sekaligus”, melainkan mengatur agar amplitudo jawaban salah saling meniadakan dan amplitudo jawaban benar saling memperkuat.

Contoh sederhana: jika dua jalur menghasilkan amplitudo +1/2 dan -1/2 untuk hasil tertentu, keduanya dapat berjumlah nol sehingga hasil itu tidak muncul. Sebaliknya, jika dua jalur menghasilkan amplitudo +1/2 dan +1/2, keduanya menjadi 1, sehingga hasil itu diperkuat. Ide ini akan muncul berulang kali, terutama dalam algoritma Deutsch-Jozsa, Bernstein-Vazirani, Simon, Shor, dan Grover.

Mengapa informasi perlu dilihat secara fisik?

Informasi tidak pernah hidup di ruang abstrak tanpa wadah. Bit dalam laptop Anda diwujudkan oleh muatan listrik, magnetisasi, transistor, atau keadaan fisik lain. Pesan dalam serat optik dibawa oleh pulsa cahaya. Memori dalam otak juga diwujudkan oleh proses fisik. Karena informasi selalu memiliki pembawa fisik, hukum fisika menentukan apa yang mungkin dilakukan terhadap informasi.

Dalam dunia klasik, sering kali kita dapat mengabaikan detail fisika dan hanya memakai model bit. Ini berhasil luar biasa baik untuk komputer digital biasa. Tetapi ketika pembawa informasi menjadi sangat kecil, sangat dingin, atau sangat terisolasi sehingga perilaku kuantumnya penting, model bit klasik tidak lagi cukup. Qubit tidak dapat disalin sembarangan seperti bit klasik; pengukuran dapat mengubah keadaan; dan dua sistem kuantum dapat memiliki hubungan gabungan yang tidak dapat dijelaskan hanya dengan keadaan masing-masing bagian. Hubungan terakhir ini disebut entanglement.

Entanglement adalah salah satu konsep paling penting dalam buku ini. Dua qubit dikatakan terjerat jika keadaan gabungannya tidak dapat ditulis sebagai keadaan qubit pertama dikalikan keadaan qubit kedua. Contoh terkenalnya adalah keadaan Bell

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

Jika dua qubit berada dalam keadaan ini, pengukuran qubit pertama dan kedua dalam basis komputasi akan selalu memberikan hasil yang sama: keduanya 0 atau keduanya 1, masing-masing dengan peluang 1/2. Tetapi korelasi ini bukan sekadar korelasi klasik seperti dua amplop yang sejak awal berisi kartu warna sama. Eksperimen dan teori ketaksamaan Bell menunjukkan bahwa korelasi kuantum tertentu tidak dapat dijelaskan oleh teori variabel tersembunyi lokal sederhana, yaitu teori yang menganggap hasil sudah ditentukan sebelumnya secara lokal dan tidak ada pengaruh lebih cepat dari cahaya (Bell, 1964). Dalam informasi kuantum, entanglement menjadi sumber daya: ia dapat dipakai untuk teleportasi kuantum, superdense coding, distribusi kunci kuantum, dan berbagai protokol lainnya.

Apa yang sebenarnya dijanjikan oleh komputasi kuantum?

Komputasi kuantum sering dipopulerkan dengan kalimat seperti “komputer kuantum mencoba semua kemungkinan sekaligus”. Kalimat ini mengandung sedikit intuisi tetapi mudah menyesatkan. Jika komputer kuantum hanya menghasilkan superposisi banyak kemungkinan lalu diukur, kita biasanya hanya mendapat satu hasil acak. Keunggulan kuantum muncul ketika rangkaian gerbang dirancang agar amplitudo saling berinterferensi dengan cara yang sistematis.

Contoh besar pertama adalah algoritma Shor untuk faktorisasi bilangan bulat dan logaritma diskret. Algoritma ini menunjukkan bahwa komputer kuantum ideal dapat memfaktorkan bilangan bulat besar secara efisien dalam model kompleksitas yang relevan, dengan konsekuensi penting bagi kriptografi kunci publik seperti RSA jika komputer kuantum berskala besar dan toleran-galat tersedia (Shor, 1994). Contoh lain adalah algoritma Grover, yang memberi percepatan kuadratik untuk pencarian tak terstruktur: dari kira-kira N percobaan klasik menjadi sekitar √(N) langkah kuantum dalam model oracle (Grover, 1996). Percepatan Grover tidak eksponensial, tetapi sangat umum dan konseptual penting.

Perhatikan dua nuansa. Pertama, algoritma kuantum biasanya dianalisis dalam model matematika ideal: qubit sempurna, gerbang tepat, dan derau terkendali. Kedua, perangkat nyata mengalami derau, yaitu gangguan yang mengubah keadaan kuantum secara tidak diinginkan. Karena itu, jalan dari algoritma di papan tulis menuju komputer kuantum praktis membutuhkan koreksi galat kuantum dan komputasi toleran-galat. Pada era perangkat kuantum skala menengah yang derau masih signifikan, sering disebut era NISQ (Noisy Intermediate-Scale Quantum), banyak eksperimen menarik dapat dilakukan, tetapi klaim manfaat praktis harus dinilai hati-hati (Preskill, 2018).

Komunikasi dan kriptografi kuantum

Informasi kuantum bukan hanya tentang komputer. Ia juga mengubah cara kita berpikir tentang komunikasi aman. Dalam kriptografi klasik, keamanan sering bergantung pada asumsi bahwa masalah matematika tertentu sulit diselesaikan oleh penyerang. Dalam kriptografi kuantum, sebagian protokol bertujuan memperoleh keamanan dari hukum fisika kuantum.

Contoh paling terkenal adalah BB84, protokol distribusi kunci kuantum yang diperkenalkan oleh Bennett dan Brassard (Bennett & Brassard, 1984). Tujuan distribusi kunci adalah membuat dua pihak, biasanya disebut Alice dan Bob, memiliki string bit rahasia yang sama, yang kemudian dapat dipakai sebagai kunci enkripsi. Pada BB84, jika pihak ketiga mencoba mengukur qubit yang dikirim, tindakan pengukuran itu dapat meninggalkan jejak statistik yang terdeteksi. Ada juga protokol E91 yang menghubungkan keamanan distribusi kunci dengan entanglement dan pelanggaran ketaksamaan Bell (Ekert, 1991).

Contoh sederhana untuk intuisi: bayangkan Alice mengirim qubit dalam salah satu dari beberapa basis pengukuran yang tidak semuanya kompatibel. Jika penyadap, Eve, tidak tahu basis yang benar, ia harus menebak cara mengukur. Tebakan yang salah dapat mengganggu keadaan dan meningkatkan tingkat galat yang dilihat Alice dan Bob. Dalam praktik nyata, tentu ada banyak detail tambahan: kehilangan foton, ketidaksempurnaan detektor, autentikasi kanal klasik, serta analisis keamanan formal. Buku ini akan membahas prinsip dasarnya terlebih dahulu sebelum menyentuh tantangan implementasi.

Mengapa koreksi galat kuantum tidak mustahil?

Pada awalnya, koreksi galat kuantum tampak hampir mustahil. Dalam komputer klasik, kita dapat melindungi bit dengan menyalinnya. Misalnya, bit 0 dapat disimpan sebagai 000 dan bit 1 sebagai 111. Jika satu bit terbalik, 010 masih dapat dikenali sebagai 000 melalui suara mayoritas. Tetapi qubit tidak dapat disalin secara sempurna dalam keadaan tak dikenal, dan pengukuran langsung dapat merusak superposisi.

Keajaiban koreksi galat kuantum adalah bahwa kita tidak perlu menyalin keadaan kuantum sembarangan atau membaca informasi logisnya secara langsung. Yang diukur adalah sindrom galat, yaitu informasi tentang jenis galat yang terjadi, bukan informasi tentang nilai qubit logis. Misalnya, kode sederhana dapat dirancang agar pengukuran tertentu memberi tahu apakah terjadi bit-flip pada salah satu qubit fisik, tanpa mengungkap apakah keadaan logisnya berhubungan dengan $|0\rangle$, $|1\rangle$, atau superposisi keduanya. Prinsip ini menjadi dasar kode Shor, kode stabilizer, dan kode permukaan yang akan dipelajari pada bab-bab akhir. Pembahasan standar tentang koreksi galat kuantum dan model informasi kuantum dapat ditemukan dalam Nielsen dan Chuang (2010).

Cara memandang matematika dalam buku ini

Informasi kuantum memakai aljabar linear sebagai bahasa utama. Keadaan kuantum ditulis sebagai vektor, pengukuran sebagai operator, evolusi tertutup sebagai matriks uniter, dan sistem gabungan sebagai tensor product. Jika istilah-istilah ini belum akrab, tidak apa-apa. Bab 2 dibangun untuk mempersiapkan alat tersebut dari awal.

Yang penting sejak pendahuluan adalah memahami peran matematika. Persamaan dalam buku ini bukan hiasan, melainkan alat untuk menjaga agar intuisi tetap jujur. Misalnya, mengatakan “qubit berada di dua keadaan sekaligus” dapat membantu di awal, tetapi persamaan

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

memberi informasi yang lebih tepat: ada amplitudo, ada normalisasi, ada basis, dan ada aturan probabilitas ketika diukur. Demikian juga, mengatakan “entanglement adalah hubungan misterius” kurang berguna dibanding memeriksa apakah suatu keadaan dua qubit dapat difaktorkan menjadi keadaan masing-masing qubit.

Anda tidak perlu menghafal semua bentuk persamaan sejak pertama kali melihatnya. Cara belajar yang lebih baik adalah menanyakan tiga hal:

1. Apa objek matematisnya?
2. Apa makna fisiknya?
3. Bagaimana cara menghitung contoh sederhana?

Misalnya, ketika melihat gerbang Hadamard, jangan hanya menghafal matriksnya. Tanyakan: gerbang ini bekerja pada berapa qubit? Apa yang dilakukan pada $|0\rangle$ dan $|1\rangle$? Bagaimana ia menciptakan superposisi? Mengapa jika diterapkan dua kali hasilnya kembali seperti semula? Pertanyaan seperti ini menghubungkan simbol, operasi, dan intuisi.

Peta perjalanan buku

Bagian awal buku membangun fondasi. Kita mulai dari alasan informasi menjadi kuantum, lalu mempelajari aljabar linear, postulat mekanika kuantum, qubit tunggal, dan sistem banyak qubit. Setelah itu, kita masuk ke model rangkaian kuantum, entanglement, matriks densitas, pengukuran umum, kanal kuantum, dan entropi. Ini adalah bahasa inti bidang informasi kuantum.

Bagian tengah buku membahas protokol dan algoritma. Kita akan melihat teleportasi kuantum dan superdense coding, lalu memahami komputasi kuantum sebagai model perhitungan. Setelah itu, kita mempelajari algoritma Deutsch-Jozsa, Bernstein-Vazirani, Simon, transformasi Fourier kuantum, estimasi fase, algoritma Shor, dan algoritma Grover. Tujuannya bukan sekadar mengikuti langkah-langkah, tetapi memahami pola berpikir: bagaimana informasi dikodekan dalam amplitudo, bagaimana interferensi digunakan, dan bagaimana pengukuran akhir mengekstraksi jawaban.

Bagian akhir buku bergerak ke keamanan, keandalan, kompleksitas, implementasi, dan riset modern. Kita membahas kriptografi kuantum, koreksi galat, komputasi toleran-galat, kelas kompleksitas seperti BQP dan QMA, platform fisik qubit, simulasi kuantum, algoritma variasional, serta cara membaca literatur penelitian. Pada titik itu, Anda diharapkan tidak hanya mengenal istilah, tetapi mampu memeriksa klaim: apakah percepatannya jelas, model derau apa yang dipakai, asumsi keamanan apa yang dibutuhkan, dan apakah eksperimen mendukung kesimpulannya.

Sikap belajar yang disarankan

Informasi kuantum sering terasa asing karena bertentangan dengan kebiasaan berpikir klasik. Tetapi asing tidak berarti kabur. Setiap konsep dalam buku ini akan diperlakukan sebagai objek yang dapat didefinisikan, dihitung, diuji dengan contoh, dan dihubungkan dengan fenomena fisik.

Saat membaca, izinkan diri Anda bergerak perlahan. Jika sebuah persamaan tampak rumit, coba masukkan angka sederhana. Jika sebuah konsep terasa abstrak, cari contoh dua qubit atau satu qubit terlebih dahulu. Jika sebuah klaim terdengar terlalu besar, tanyakan modelnya: apakah ini tentang algoritma ideal, perangkat nyata, keamanan teoretis, atau eksperimen tertentu?

Tujuan buku ini bukan membuat mekanika kuantum terasa “magis”. Justru sebaliknya: kita ingin mengurangi kabut. Keanehan kuantum tetap ada, tetapi ia dapat dipelajari dengan bahasa yang rapi. Pada akhirnya, informasi kuantum adalah pelajaran tentang batas dan kemungkinan: batas dari apa yang dapat diketahui tanpa mengganggu, batas dari apa yang dapat dihitung secara efisien, batas dari komunikasi aman, dan kemungkinan baru yang muncul ketika informasi diperlakukan sesuai hukum kuantum.

References

Bell, J. S. (1964). On the Einstein Podolsky Rosen paradox. Physics Physique Fizika, 1(3), 195–200.

Bennett, C. H., & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing (pp. 175–179). Bangalore, India.

Deutsch, D. (1985). Quantum theory, the Church-Turing principle and the universal quantum computer. Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences, 400(1818), 97–117.

Ekert, A. K. (1991). Quantum cryptography based on Bell’s theorem. Physical Review Letters, 67(6), 661–663.

Feynman, R. P. (1982). Simulating physics with computers. International Journal of Theoretical Physics, 21(6–7), 467–488.

Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. In Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing (pp. 212–219).

Nielsen, M. A., & Chuang, I. L. (2010). Quantum Computation and Quantum Information: 10th Anniversary Edition. Cambridge University Press.

Preskill, J. (2018). Quantum computing in the NISQ era and beyond. Quantum, 2, 79.

Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. In Proceedings 35th Annual Symposium on Foundations of Computer Science (pp. 124–134).

Document information

Pendahuluan

Project	Informasi Kuantum
Document	Document 1.4
Author	mujirin
Verifier	Not verified
Downloaded	July 04, 2026 19:17 KST
Status	Working
Document link	https://theorytrace.com/projects/informasi-kuantum/documents/pendahuluan/