

Bab 1: Mengapa Informasi Menjadi Kuantum

Informasi kuantum lahir dari satu kalimat sederhana: informasi selalu harus disimpan dalam sesuatu yang fisik. Sebuah angka di buku catatan disimpan sebagai tinta di atas kertas. Sebuah foto di ponsel disimpan sebagai keadaan listrik dan magnetik di perangkat memori. Sebuah pesan radio dibawa oleh gelombang elektromagnetik. Gagasan bahwa informasi tidak terpisah dari fisika menjadi sangat penting dalam teori informasi modern; Landauer menekankan hubungan antara pemrosesan informasi dan hukum fisika, khususnya ketika operasi logis yang tidak dapat dibalik dikaitkan dengan disipasi energi (Landauer, 1961).

Selama pembawa informasinya dapat dipahami dengan fisika klasik, kita memperoleh teori informasi klasik: bit, kode koreksi galat klasik, kompresi data, kriptografi klasik, dan komputer digital. Tetapi jika pembawa informasinya adalah sistem mikroskopik seperti foton, elektron, atom, ion, atau rangkaian superkonduktor yang perilakunya mengikuti mekanika kuantum, maka aturan lama tidak lagi cukup. Informasi masih dapat disimpan, dikirim, dan diproses, tetapi caranya berubah.

Bab ini adalah orientasi awal. Kita belum akan membangun semua matematika secara lengkap; itu dimulai pada Bab 2 dan Bab 3. Tujuan bab ini adalah memberi gambaran jernih tentang pertanyaan besar:

> Mengapa teori kuantum memaksa kita memperluas konsep informasi?

Untuk menjawabnya, kita mulai dari bit, lalu bergerak ke qubit, superposisi, pengukuran, entanglement, komputasi kuantum, komunikasi kuantum, dan akhirnya peta besar bidang informasi kuantum.

1.1 Informasi sebagai perbedaan yang dapat dibedakan

Dalam kehidupan sehari-hari, “informasi” sering berarti isi pesan: nama seseorang, hasil ujian, suhu udara, atau lokasi sebuah paket. Dalam teori informasi, kita mulai lebih sederhana. Informasi muncul ketika ada beberapa kemungkinan yang dapat dibedakan.

Misalnya, sebuah lampu indikator dapat berada dalam dua keadaan:

- mati,
- menyala.

Jika kita sepakat bahwa “mati” berarti 0 dan “menyala” berarti 1, maka lampu itu menyimpan satu bit.

Bit adalah unit dasar informasi klasik. Secara abstrak, bit hanya memiliki dua nilai:

0 atau 1.

Namun secara fisik, bit dapat direalisasikan dengan banyak cara:

- tegangan rendah dan tegangan tinggi dalam transistor,
- orientasi magnetik pada media penyimpanan,
- lubang dan tidak ada lubang pada kartu lama,
- pulsa cahaya lemah dan kuat dalam komunikasi optik.

Hal pentingnya adalah ini: bit bukan benda tertentu, melainkan abstraksi dari dua keadaan fisik yang dapat dibedakan secara andal.

Claude Shannon membangun teori matematis tentang komunikasi dengan memandang pesan sebagai pilihan dari sekumpulan kemungkinan dan mengukur informasi melalui ketidakpastian probabilistik; teori ini menjadi dasar kompresi, kapasitas kanal, dan komunikasi digital modern (Shannon, 1948). Dalam teori Shannon, detail fisik pembawa pesan sering disederhanakan. Kita dapat membahas bit seolah-olah ia objek matematis murni.

Namun pada akhirnya, setiap bit tetap hidup dalam dunia fisik. Jika perangkat menjadi terlalu kecil, terlalu dingin, terlalu cepat, atau memakai partikel individual, hukum mekanika kuantum tidak bisa diabaikan.

Di situlah informasi menjadi kuantum.

1.2 Bit klasik: pilihan yang pasti atau ketidaktahuan klasik

Sebuah bit klasik ideal memiliki nilai pasti: 0 atau 1. Jika kita tidak tahu nilainya, ketidaktahuan itu biasanya digambarkan dengan probabilitas.

Contoh:

Sebuah bit disiapkan oleh seseorang dengan melempar koin. Jika koin menunjukkan kepala, ia menulis 0. Jika ekor, ia menulis 1. Sebelum kita melihatnya, kita dapat mengatakan:

$$P(0)=\frac{1}{2}, P(1)=\frac{1}{2}.$$

Namun dalam pandangan klasik, bit itu sendiri sudah memiliki nilai tertentu. Kita hanya belum mengetahuinya. Jika ternyata nilainya 0, maka ia 0 sejak tadi; jika 1, maka ia 1 sejak tadi.

Inilah ketidakpastian klasik: ketidakpastian karena kurangnya pengetahuan pengamat.

Pada komputer biasa, register 8 bit selalu berada pada salah satu dari 256 kemungkinan pola:

00000000, 00000001, 00000010, ..., 11111111.

Jika kita tidak tahu pola mana yang tersimpan, kita memakai distribusi probabilitas atas 256 pola itu. Tetapi setiap kali register dibaca dalam kondisi ideal, ia mengungkapkan satu pola tertentu.

Mekanika kuantum memperkenalkan jenis keadaan yang tidak dapat dipahami hanya sebagai “kita belum tahu nilainya”. Di sinilah qubit muncul.

1.3 Qubit: sistem kuantum dua tingkat

Qubit adalah unit dasar informasi kuantum. Kata “qubit” berasal dari “quantum bit”. Seperti bit, qubit berkaitan dengan dua label dasar, biasanya ditulis sebagai

$|0\rangle$ dan $|1\rangle$.

Simbol $|0\rangle$ dan $|1\rangle$ memakai notasi Dirac, yaitu notasi standar dalam mekanika kuantum. Untuk saat ini, kita dapat membacanya sebagai “keadaan nol” dan “keadaan satu”. Notasi ini akan dipelajari dengan lebih formal pada Bab 2.

Secara fisik, qubit dapat direalisasikan oleh sistem kuantum yang memiliki dua keadaan yang dapat dipilih sebagai basis. Contohnya:

- dua tingkat energi sebuah atom,
- dua polarisasi foton, misalnya horizontal dan vertikal,
- dua keadaan spin elektron,

- dua keadaan arus atau energi dalam rangkaian superkonduktor.

Perbedaan pentingnya adalah bahwa keadaan umum qubit tidak hanya $|0\rangle$ atau $|1\rangle$. Keadaan murni satu qubit dapat ditulis sebagai

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

dengan α dan β bilangan kompleks yang memenuhi

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

Bilangan α dan β disebut amplitudo. Amplitudo bukan probabilitas, tetapi dari amplitudo kita memperoleh probabilitas hasil pengukuran. Jika qubit $|\psi\rangle$ diukur dalam basis $|0\rangle$, $|1\rangle$, maka peluang memperoleh hasil 0 adalah

$$|\alpha|^2,$$

dan peluang memperoleh hasil 1 adalah

$$|\beta|^2.$$

Aturan ini adalah bentuk khusus dari aturan Born, salah satu postulat dasar mekanika kuantum yang akan dibahas secara formal pada Bab 3. Buku Nielsen dan Chuang menyajikan formulasi standar postulat keadaan, evolusi, dan pengukuran yang banyak digunakan dalam informasi kuantum (Nielsen & Chuang, 2010).

Contoh sederhana:

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

Jika diukur dalam basis $|0\rangle$, $|1\rangle$, hasilnya 0 dengan peluang $1/2$ dan 1 dengan peluang $1/2$.

Tetapi qubit ini tidak sama dengan bit klasik acak yang bernilai 0 atau 1 dengan peluang masing-masing $1/2$. Mengapa? Karena amplitudo dapat memiliki fase, dan fase dapat memengaruhi hasil percobaan lain.

1.4 Superposisi bukan “sekaligus 0 dan 1” secara sederhana

Keadaan

$$(1/\sqrt{2})|0\rangle + (1/\sqrt{2})|1\rangle$$

sering disebut superposisi dari $|0\rangle$ dan $|1\rangle$. Superposisi berarti keadaan kuantum dapat merupakan kombinasi linear dari beberapa keadaan dasar.

Namun kita harus berhati-hati. Kalimat “qubit berada sekaligus dalam 0 dan 1” sering dipakai sebagai slogan populer, tetapi dapat menyesatkan. Qubit dalam superposisi bukan berarti ada bit kecil tersembunyi yang secara klasik bernilai 0 dan 1 sekaligus. Yang benar adalah:

> Keadaan qubit direpresentasikan oleh vektor amplitudo, dan hasil pengukuran bergantung pada amplitudo tersebut serta basis pengukuran yang dipilih.

Untuk melihat mengapa superposisi berbeda dari ketidaktahuan klasik, bandingkan dua keadaan berikut:

$$|+\rangle = (1/\sqrt{2})|0\rangle + (1/\sqrt{2})|1\rangle,$$

dan

$$|-\rangle = (1/\sqrt{2})|0\rangle - (1/\sqrt{2})|1\rangle.$$

Jika keduanya diukur dalam basis $|0\rangle, |1\rangle$, hasilnya sama-sama 0 dengan peluang $1/2$ dan 1 dengan peluang $1/2$. Jadi dari pengukuran itu saja, keduanya tampak seperti bit acak yang sama.

Tetapi $|+\rangle$ dan $|-\rangle$ adalah dua keadaan kuantum yang berbeda dan dapat dibedakan secara sempurna dengan pengukuran dalam basis lain, yaitu basis $|+\rangle, |-\rangle$. Perbedaannya terletak pada tanda relatif antara dua amplitudo. Tanda relatif ini adalah contoh paling sederhana dari fase relatif.

Fase relatif sangat penting karena operasi kuantum dapat membuat amplitudo saling memperkuat atau saling meniadakan. Fenomena ini disebut interferensi.

Contoh intuisi:

- Jika dua jalur kuantum menuju jawaban salah memiliki amplitudo yang berlawanan tanda, keduanya dapat saling meniadakan.
- Jika dua jalur menuju jawaban benar memiliki amplitudo yang searah, keduanya dapat saling memperkuat.

Banyak algoritma kuantum bekerja bukan karena “mencoba semua jawaban sekaligus” dalam arti sederhana, melainkan karena merancang interferensi agar jawaban yang diinginkan memperoleh peluang besar saat diukur.

1.5 Pengukuran: memperoleh informasi sekaligus mengubah keadaan

Dalam fisika klasik ideal, kita sering membayangkan pengukuran sebagai tindakan pasif. Jika sebuah bola berada di meja, kita dapat melihat posisinya tanpa mengubah posisi bola secara berarti. Dalam mekanika kuantum, pengukuran memiliki peran yang lebih halus.

Jika qubit

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

diukur dalam basis $|0\rangle, |1\rangle$, kita memperoleh hasil 0 dengan peluang $|\alpha|^2$ atau hasil 1 dengan peluang $|\beta|^2$. Setelah pengukuran, keadaan qubit berubah menjadi keadaan yang sesuai dengan hasil yang diperoleh. Jika hasilnya 0, keadaan menjadi $|0\rangle$. Jika hasilnya 1, keadaan menjadi $|1\rangle$.

Contoh:

Misalkan

$$|\psi\rangle = \frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle.$$

Maka

$$P(0) = \left| \frac{\sqrt{3}}{2} \right|^2 = \frac{3}{4},$$

dan

$$P(1) = \left| \frac{1}{2} \right|^2 = \frac{1}{4}.$$

Jika kita mengukur dan mendapat hasil 0, maka pengukuran berikutnya dalam basis yang sama akan memberikan 0 dengan peluang 1, selama tidak ada operasi lain di antara keduanya.

Ini menunjukkan dua hal:

1. Pengukuran kuantum menghasilkan keluaran klasik.
2. Pengukuran biasanya mengubah keadaan kuantum.

Akibatnya, informasi kuantum tidak bisa dibaca seperti membaca file klasik. Kita tidak bisa mengambil satu qubit tak dikenal, mengukurnya sekali, lalu mengetahui seluruh nilai α dan β . Satu pengukuran hanya memberi satu hasil klasik. Untuk memperkirakan keadaan, kita memerlukan banyak salinan identik dan prosedur statistik. Bahkan dengan banyak salinan, proses ini disebut tomografi kuantum dan dapat menjadi mahal untuk sistem besar.

1.6 Tidak semua informasi dapat disalin: no-cloning theorem

Dalam komputer klasik, menyalin informasi adalah operasi biasa. Jika sebuah bit bernilai 0, kita dapat membuat salinan 0. Jika bernilai 1, kita dapat membuat salinan 1. Operasi salin klasik dapat ditulis secara ideal sebagai

$$0 \mapsto 00, 1 \mapsto 11.$$

Untuk informasi kuantum, ada batas mendasar: tidak ada proses fisik yang dapat menyalin secara sempurna setiap keadaan kuantum tak dikenal. Pernyataan ini dikenal sebagai no-cloning theorem. Wootters dan Zurek menunjukkan bahwa keadaan kuantum umum tidak dapat dikloning secara sempurna oleh operasi kuantum yang diizinkan (Wootters & Zurek, 1982).

Mengapa ini masuk akal? Secara sangat ringkas, operasi kuantum pada sistem tertutup bersifat linear. Jika sebuah alat dapat menyalin $|0\rangle$ dan $|1\rangle$,

$$|0\rangle|b\rangle \mapsto |0\rangle|0\rangle,$$

$$|1\rangle|b\rangle \mapsto |1\rangle|1\rangle,$$

maka karena linearitas, untuk superposisi

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

alat itu akan menghasilkan

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle),$$

bukan

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle).$$

Ekspresi terakhir jika dikembangkan menjadi

$$\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle),$$

yang berbeda dari hasil linear di atas.

No-cloning theorem bukan sekadar keterbatasan teknologi. Ia adalah batas prinsipil dari teori kuantum. Dampaknya besar:

- penyadap tidak dapat menyalin keadaan kuantum tak dikenal tanpa risiko mengganggunya,
- koreksi galat kuantum tidak bisa dilakukan dengan menyalin qubit seperti kode pengulangan klasik biasa,
- komunikasi kuantum harus dirancang dengan hati-hati karena informasi kuantum rapuh terhadap pengukuran.

1.7 Entanglement: korelasi yang tidak dapat dijelaskan secara klasik sederhana

Jika satu qubit sudah berbeda dari satu bit, dua qubit lebih menarik lagi. Keadaan gabungan dua qubit dapat berupa superposisi atas empat basis komputasi:

$$|00\rangle, |01\rangle, |10\rangle, |11\rangle.$$

Salah satu keadaan paling penting adalah keadaan Bell:

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

Keadaan ini disebut entangled atau terjerat. Secara intuitif, dua sistem terjerat memiliki keadaan bersama yang tidak dapat dijelaskan hanya dengan memberikan keadaan masing-masing bagian secara terpisah.

Jika kita mengukur qubit pertama dan kedua dalam basis $|0\rangle, |1\rangle$, hasilnya selalu sama:

- kadang 00,
- kadang 11,

masing-masing dengan peluang $1/2$.

Sejauh ini, ini tampak seperti korelasi klasik biasa. Misalnya, seseorang dapat memasukkan dua kartu dengan warna sama ke dalam dua amplop, lalu mengirim amplop ke dua kota. Ketika satu amplop dibuka dan ternyata merah, kita langsung tahu amplop lain juga merah. Tidak ada misteri.

Tetapi entanglement lebih dalam daripada korelasi klasik semacam itu. Jika pasangan terjerat diukur dalam berbagai basis yang dipilih dengan tepat, korelasinya dapat melanggar batas yang dipenuhi oleh teori variabel tersembunyi lokal tertentu. John Bell merumuskan ketaksamaan yang memungkinkan perbedaan antara prediksi mekanika kuantum dan kelas teori lokal klasik diuji secara eksperimental (Bell, 1964). Kita akan membahas ini secara lebih lengkap pada Bab 7.

Hal penting untuk saat ini:

> Entanglement adalah sumber daya informasi kuantum.

Ia digunakan dalam teleportasi kuantum, protokol kriptografi, komputasi kuantum, dan koreksi galat. Namun entanglement tidak memungkinkan pengiriman pesan lebih cepat dari cahaya. Hasil lokal pada satu sisi tetap acak; korelasi penuh baru terlihat ketika hasil dari kedua sisi dibandingkan melalui komunikasi klasik.

1.8 Mengapa komputasi berubah?

Komputer klasik memproses bit dengan gerbang logika seperti AND, OR, NOT, dan XOR. Komputer kuantum memproses qubit dengan operasi yang diizinkan oleh mekanika kuantum. Untuk sistem tertutup ideal, operasi ini direpresentasikan oleh transformasi uniter, yaitu transformasi linear yang mempertahankan norma vektor keadaan. Istilah ini akan dibahas secara formal pada Bab 2 dan Bab 3.

Satu register berisi n bit klasik berada pada salah satu dari 2^n pola. Sebaliknya, keadaan murni n qubit secara umum dapat ditulis sebagai superposisi

$$|\psi\rangle = \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle,$$

dengan

$$\sum_x |\alpha_x|^2 = 1.$$

Ada 2^n amplitudo kompleks α_x . Ini sering disebut sebagai pertumbuhan dimensi ruang keadaan secara eksponensial.

Tetapi kita harus menghindari kesimpulan keliru:

> Komputer kuantum bukan komputer yang secara ajaib menjalankan semua kemungkinan lalu membaca semua jawabannya.

Masalahnya, ketika register diukur, kita hanya memperoleh satu hasil x , bukan seluruh daftar amplitudo α_x . Kekuatan komputasi kuantum muncul ketika operasi dirancang agar amplitudo jawaban yang salah saling melemahkan, sedangkan amplitudo jawaban yang benar saling menguatkan. Inilah peran interferensi.

Richard Feynman mengamati bahwa mensimulasikan sistem kuantum dengan komputer klasik tampak sulit karena deskripsi keadaan kuantum dapat tumbuh sangat besar, dan ia mengusulkan bahwa sistem komputasi yang mengikuti hukum kuantum dapat menjadi alat alami untuk mensimulasikan fisika kuantum (Feynman, 1982). David Deutsch kemudian memformulasikan gagasan komputer kuantum universal dalam kerangka teori komputasi (Deutsch, 1985).

Beberapa algoritma kemudian menunjukkan bahwa model kuantum dapat memberikan percepatan nyata untuk tugas tertentu:

- Algoritma Shor memberikan algoritma kuantum waktu polinomial untuk faktorisasi bilangan bulat dan logaritma diskret, dua masalah yang penting dalam kriptografi kunci publik klasik (Shor, 1997).
- Algoritma Grover memberikan percepatan kuadratik untuk pencarian tak terstruktur, dari orde klasik N kueri menjadi orde kuantum \sqrt{N} kueri dalam model oracle (Grover, 1996).

Namun tidak benar bahwa komputer kuantum mempercepat semua komputasi. Banyak masalah belum diketahui memiliki algoritma kuantum yang jauh lebih cepat daripada algoritma klasik terbaik. Bahkan untuk masalah tertentu, batas bawah menunjukkan bahwa percepatan kuantum terbatas. Karena itu, sikap ilmiah yang sehat adalah bertanya:

1. Struktur masalah apa yang dapat dieksploitasi oleh interferensi kuantum?
2. Apakah ada oracle, periodisitas, simetri, atau struktur linear yang cocok?
3. Berapa biaya koreksi galat dan implementasi fisiknya?
4. Apakah keunggulan teoretis tetap berarti pada ukuran masalah nyata?

Pertanyaan-pertanyaan ini akan kembali muncul pada bab-bab algoritma dan kompleksitas.

1.9 Mengapa komunikasi berubah?

Komunikasi klasik mengirim bit melalui kanal. Kanal dapat berupa kabel, serat optik, udara, atau media penyimpanan. Jika kanal berderau, kita memakai kode koreksi galat klasik. Jika pesan harus dirahasiakan, kita memakai kriptografi.

Komunikasi kuantum memakai sistem kuantum sebagai pembawa informasi. Karena pengukuran dapat mengubah keadaan dan keadaan tak dikenal tidak dapat disalin sempurna, komunikasi kuantum memiliki kemungkinan baru.

Salah satu contoh awal dan paling terkenal adalah BB84, protokol distribusi kunci kuantum yang diperkenalkan oleh Bennett dan Brassard (1984). Tujuannya bukan mengirim pesan rahasia secara langsung, melainkan membuat dua pihak, biasanya disebut Alice dan Bob, berbagi kunci rahasia. Kunci itu kemudian dapat digunakan untuk enkripsi klasik.

Gagasan dasarnya:

1. Alice mengirim qubit dalam beberapa basis yang dipilih acak.
2. Bob mengukur qubit dalam basis yang juga dipilih acak.

3. Setelah transmisi, mereka membandingkan sebagian informasi basis melalui kanal klasik.
4. Jika ada penyadap, pengukuran penyadap cenderung menimbulkan gangguan statistik yang dapat dideteksi.

Protokol lain, E91, menghubungkan distribusi kunci kuantum dengan entanglement dan pelanggaran ketaksamaan Bell (Ekert, 1991). Di sini entanglement bukan hanya fenomena aneh, melainkan alat operasional untuk menguji keamanan.

Contoh lain adalah teleportasi kuantum. Namanya terdengar seperti fiksi ilmiah, tetapi maknanya teknis: keadaan kuantum tak dikenal dapat dipindahkan dari satu sistem ke sistem lain dengan memakai pasangan entangled dan komunikasi klasik. Protokol ini diperkenalkan oleh Bennett, Brassard, Crépeau, Jozsa, Peres, dan Wootters (1993). Teleportasi kuantum tidak mengirim materi, tidak menggandakan keadaan, dan tidak mengirim informasi lebih cepat dari cahaya. Ia memindahkan keadaan dengan cara yang konsisten dengan no-cloning theorem: keadaan asal dihancurkan dalam proses pengukuran, sedangkan keadaan tujuan dapat dipulihkan setelah informasi klasik diterima.

Komunikasi kuantum mengajarkan pelajaran penting:

> Mekanika kuantum tidak hanya membatasi apa yang dapat diketahui penyadap; ia juga menyediakan cara baru untuk mendeteksi penyadapan dan memindahkan keadaan informasi.

1.10 Mengapa koreksi galat kuantum tampak mustahil, tetapi ternyata mungkin?

Qubit sangat rentan terhadap derau. Derau adalah gangguan yang membuat keadaan berubah secara tak diinginkan. Dalam sistem fisik nyata, derau dapat berasal dari interaksi dengan lingkungan, ketidaksempurnaan kontrol, kehilangan foton, fluktuasi medan, atau proses termal.

Pada awalnya, koreksi galat kuantum tampak hampir mustahil karena tiga alasan:

1. Kita tidak dapat menyalin qubit tak dikenal secara sempurna.
2. Mengukur qubit secara langsung dapat menghancurkan superposisi.
3. Galat kuantum tampak kontinu, bukan hanya bit flip 0 menjadi 1 atau 1 menjadi 0.

Namun teori koreksi galat kuantum menunjukkan bahwa hambatan ini dapat diatasi. Kuncinya adalah menyimpan informasi logis secara terdistribusi dalam beberapa qubit fisik dan mengukur sindrom galat, yaitu informasi tentang jenis galat yang terjadi, tanpa mengukur informasi logis yang ingin dilindungi.

Peter Shor memperkenalkan salah satu kode koreksi galat kuantum pertama yang dapat melindungi satu qubit logis dengan menggunakan sembilan qubit fisik (Shor, 1995). Kode ini menunjukkan secara konkret bahwa koreksi galat kuantum mungkin dilakukan tanpa melanggar no-cloning theorem.

Contoh intuisi:

Dalam kode klasik sederhana, kita dapat menyimpan satu bit sebagai tiga salinan:

$$0 \mapsto 000, 1 \mapsto 111.$$

Jika terjadi satu bit flip dan kita membaca 010, kita menebak bahwa pesan aslinya 000. Ini disebut voting mayoritas.

Dalam kuantum, kita tidak boleh sekadar menyalin keadaan

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

menjadi tiga salinan independen. Tetapi kita dapat menyandikan informasi ke keadaan gabungan beberapa qubit dengan cara yang menjaga superposisi logis. Sindrom galat kemudian memberi tahu “galat terjadi di lokasi mana” tanpa memberi tahu apakah keadaan logisnya $|0\rangle$, $|1\rangle$, atau superposisinya.

Koreksi galat kuantum adalah alasan serius mengapa komputasi kuantum skala besar dianggap mungkin secara prinsip, meskipun sangat sulit secara teknik.

1.11 Peta besar informasi kuantum

Bidang informasi kuantum dapat dilihat sebagai pertemuan tiga tradisi:

1. Mekanika kuantum, yang menjelaskan keadaan, evolusi, pengukuran, dan sistem gabungan.
2. Teori informasi, yang mempelajari penyimpanan, pengiriman, kompresi, dan keamanan informasi.

3. Ilmu komputer, yang mempelajari algoritma, kompleksitas, model komputasi, dan koreksi galat.

Dari pertemuan itu muncul beberapa cabang utama.

Komputasi kuantum

Komputasi kuantum bertanya: apa yang dapat dihitung secara efisien jika komputer mengikuti hukum kuantum?

Topiknya mencakup:

- rangkaian kuantum,
- gerbang kuantum,
- algoritma kuantum,
- oracle dan kompleksitas kueri,
- algoritma Shor dan Grover,
- simulasi Hamiltonian,
- komputasi toleran-galat.

Pertanyaan utamanya bukan “apakah kuantum selalu lebih cepat?”, melainkan “untuk struktur masalah apa model kuantum memberi keuntungan?”

Komunikasi kuantum

Komunikasi kuantum bertanya: apa yang dapat dikirim, diamankan, atau ditransformasikan jika pesan dibawa oleh sistem kuantum?

Topiknya mencakup:

- distribusi kunci kuantum,
- teleportasi,
- superdense coding,
- kanal kuantum,
- kapasitas komunikasi,
- jaringan kuantum.

Di sini pengukuran, no-cloning, dan entanglement menjadi alat komunikasi, bukan sekadar keanehan fisika.

Teori informasi kuantum

Teori informasi kuantum membangun ukuran dan hukum umum tentang informasi dalam sistem kuantum.

Topiknya mencakup:

- matriks densitas,
- entropi von Neumann,
- mutual information kuantum,
- Holevo bound,
- entanglement entropy,
- strong subadditivity.

Cabang ini menjawab pertanyaan seperti: berapa banyak informasi klasik yang dapat dikirim melalui sistem kuantum? Berapa banyak entanglement yang dimiliki suatu keadaan? Apa batas fundamental kompresi kuantum?

Koreksi galat dan toleransi galat

Koreksi galat kuantum bertanya: bagaimana menjaga informasi kuantum tetap hidup meski perangkat fisik berderau?

Topiknya mencakup:

- kode bit-flip dan phase-flip,
- kode Shor,
- kode stabilizer,
- kode permukaan,
- sindrom galat,
- gerbang logis,
- ambang toleransi galat.

Tanpa koreksi galat, komputasi kuantum besar akan sangat sulit. Dengan koreksi galat, kita dapat membahas qubit logis yang lebih andal daripada qubit fisik penyusunnya.

Implementasi fisik

Informasi kuantum juga merupakan bidang eksperimental. Kita perlu membangun qubit nyata.

Platform utama meliputi:

- ion terperangkap,

- qubit superkonduktor,
- fotonik,
- spin dalam semikonduktor,
- atom netral,
- pusat cacat dalam kristal.

Setiap platform memiliki kelebihan dan tantangan: waktu koherensi, kecepatan gerbang, fidelitas pengukuran, konektivitas, skalabilitas, dan kemudahan koreksi galat.

1.12 Apa yang perlu dipegang sejak awal?

Sebelum masuk ke matematika, ada beberapa prinsip yang sebaiknya diingat.

Pertama, qubit bukan bit yang samar-samar. Qubit adalah objek informasi dengan struktur amplitudo kompleks. Ketika diukur, ia menghasilkan bit klasik, tetapi sebelum pengukuran ia tidak dapat dipahami hanya sebagai bit klasik yang tidak kita ketahui.

Kedua, superposisi bukan jawaban lengkap atas kekuatan kuantum. Superposisi memberi ruang kemungkinan, tetapi interferensi menentukan apakah kemungkinan itu berguna. Tanpa rancangan interferensi yang tepat, pengukuran hanya menghasilkan sampel acak yang mungkin tidak berguna.

Ketiga, entanglement adalah korelasi kuantum yang menjadi sumber daya. Ia bukan sinyal lebih cepat dari cahaya, tetapi memungkinkan protokol yang tidak tersedia secara klasik, seperti teleportasi dan beberapa bentuk distribusi kunci kuantum.

Keempat, pengukuran menghasilkan informasi klasik tetapi dapat mengganggu keadaan. Ini membuat desain protokol kuantum berbeda dari desain algoritma klasik. Kita harus memilih kapan dan bagaimana mengukur.

Kelima, derau bukan detail kecil. Informasi kuantum sangat sensitif terhadap interaksi dengan lingkungan. Karena itu, kanal kuantum, matriks densitas, dan koreksi galat bukan tambahan opsional; semuanya merupakan bagian inti bidang ini.

1.13 Contoh penutup: satu qubit sebagai pelajaran kecil

Misalkan kita memiliki qubit dalam keadaan

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle).$$

Jika kita mengukurnya langsung dalam basis $|0\rangle, |1\rangle$, kita memperoleh 0 atau 1 secara acak dengan peluang sama. Dari sudut pandang pengukuran itu, ia tampak seperti koin adil.

Sekarang bandingkan dengan

$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

Pengukuran dalam basis $|0\rangle, |1\rangle$ juga memberi 0 atau 1 dengan peluang sama. Namun kedua keadaan ini berbeda. Ada pengukuran lain yang dapat membedakan $|+\rangle$ dari $|-\rangle$ secara pasti.

Dari satu contoh kecil ini, kita sudah melihat inti informasi kuantum:

- probabilitas berasal dari kuadrat amplitudo,
- fase relatif dapat membawa informasi,
- pilihan basis pengukuran penting,
- keadaan kuantum tidak sama dengan distribusi probabilitas klasik,
- informasi yang dapat diambil bergantung pada operasi fisik yang dilakukan.

Seluruh buku ini dapat dianggap sebagai pengembangan sistematis dari pelajaran kecil tersebut.

Ringkasan

Informasi menjadi kuantum ketika pembawa informasinya harus dijelaskan oleh mekanika kuantum. Bit klasik memiliki nilai 0 atau 1, sedangkan qubit dapat berada dalam superposisi $\alpha|0\rangle + \beta|1\rangle$, dengan amplitudo kompleks yang menentukan peluang hasil pengukuran. Superposisi berbeda dari ketidaktahuan klasik karena fase relatif dapat memengaruhi hasil melalui interferensi.

Pengukuran kuantum menghasilkan keluaran klasik dan umumnya mengubah keadaan. Keadaan kuantum tak dikenal tidak dapat disalin sempurna, sebagaimana dinyatakan oleh no-cloning theorem. Sistem banyak qubit dapat memiliki entanglement, yaitu korelasi kuantum yang tidak dapat direduksi menjadi keadaan masing-masing bagian secara terpisah.

Komputasi kuantum memanfaatkan superposisi, interferensi, dan entanglement untuk tugas tertentu seperti faktorisasi, pencarian, dan simulasi sistem kuantum. Komunikasi kuantum memakai sifat pengukuran dan no-cloning untuk protokol seperti distribusi kunci kuantum dan teleportasi. Koreksi galat kuantum menunjukkan bahwa informasi kuantum dapat dilindungi meski tidak dapat disalin secara klasik.

Bab berikutnya akan membangun bahasa matematika yang diperlukan: vektor kompleks, ruang Hilbert, basis, inner product, matriks, operator uniter, tensor product, dan notasi Dirac.

References

Bell, J. S. (1964). On the Einstein Podolsky Rosen paradox. *Physics*, 1, 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, Bangalore, India*, 175-179.

Bennett, C. H., Brassard, G., Crépeau, C., Jozsa, R., Peres, A., Wootters, W. K. (1993). Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Physical Review Letters*, 70(13), 1895-1899.

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

Ekert, A. K

Document information

Bab 1: Mengapa Informasi Menjadi Kuantum

Project	Informasi Kuantum
Document	Document 1.5
Author	mujirin
Verifier	Not verified
Downloaded	July 04, 2026 19:39 KST
Status	Working
Document link	https://www.theorytrace.com/projects/informasi-kuantum/documents/bab-1-mengapa-informasi-menjadi-kuantum/