QUANTUM COMPUTING

Formula and Notation Reference

The conventions used throughout the course, every formula it establishes, and every symbol it defines. Nothing here is derived; the derivations are in the lecture notes.

Contains	Edition	Companion
Conventions, formulas, notation	1.0	Lecture notes, Chapters 1 to 6

How to read it

Part 1 states the four conventions this course fixes and the two expressions everything else is built on. Part 2 is the summary of formulas, in the order the course establishes them. Part 3 defines every symbol. Nothing here is derived: where a result needs an argument, the argument is in the lecture notes chapter named beside it.

PART 1

Conventions

These hold everywhere in the course, without local variation. The first two are the ones that fail silently. A wrong qubit order does not make a result approximately wrong — it names a different state, and every number after it is quietly wrong. A phase dropped in the wrong place removes the only mechanism any algorithm here has.

CONVENTION	STATEMENT
Qubit order	A register of n qubits is written $\lvert q_{n-1}\dots q_1q_0\rangle$, and entry x of its column of amplitudes is the amplitude of $\lvert x\rangle$ with x read as a binary number. Circuit drawings put q_0 at the top. Test it before trusting any two-qubit result: prepare $\lvert 10\rangle$, apply X to the qubit you mean, and print all four amplitudes.
Global and relative phase	$e^{i\gamma}\lvert\psi\rangle$ is the same state as $\lvert\psi\rangle$, and the phase may always be dropped. $\alpha\lvert 0\rangle + e^{i\varphi}\beta\lvert 1\rangle$ is **not** the same state as $\alpha\lvert 0\rangle + \beta\lvert 1\rangle$, and that phase may never be dropped. Interference is entirely a statement about the second kind.
The inner product	$\langle u\vert v\rangle = \sum_k u_k^* v_k$: the conjugate sits on the first argument and on nothing else. In NumPy that is `np.vdot(u, v)` and never `np.dot`. Matrix products act on a ket from right to left, so the gate written last in a product is the one applied first.
Units and logarithms	$\hbar = 1$, so a Hamiltonian is measured in angular frequency and evolution is $U(t) = e^{-iHt}$. Where a physical energy is meant, the units are written out. $\log$ without a base means base two, so every entropy and every bit count is in bits.
States and operators	$\lvert\psi\rangle$ is a pure state and ρ a density operator, both normalised: $\langle\psi\vert\psi\rangle = 1$ and $\mathrm{Tr}\,\rho = 1$. $A^\dagger$ is the conjugate transpose, I the identity, and X, Y, Z the three Pauli operators, also written σ_x, σ_y, σ_z.
Exact against sampled	p is an exact Born probability and $\hat{p} = K/N$ is an estimate from N shots of the same circuit. The two differ by about $1/(2\sqrt{N})$ at worst, so a quoted frequency always carries its shot count.
Oracles and cost	$U_f\lvert x\rangle\lvert y\rangle = \lvert x\rangle\lvert y\oplus f(x)\rangle$ is one query. A query count is not a runtime, and a resource claim names five things: the task, the input model, the accuracy, the hardware model, and the classical baseline.

THE TWO EXPRESSIONS THE WHOLE COURSE RESTS ON

$$p(n) = \lvert\langle n\vert\psi\rangle\rvert^2$$

$$\lvert\psi(t)\rangle = U(t)\,\lvert\psi(0)\rangle, \qquad U(t) = e^{-iHt}$$

The first is the Born rule, and it is the only place a state becomes a number an instrument can print. The second is closed-system evolution, and every gate in the course is this expression for some H and some t. Measurement and evolution are the two things the postulates license; everything in Part 2 is one of them carrying more structure.

PART 2

Summary of formulas

Every formula the course establishes, in the order the course establishes it. Nothing here is derived and nothing here is new: each entry names the section that develops it, and the argument is in that section. Read this page to check a result you already understand, never to meet one for the first time.

Four conventions are in force throughout and are not repeated under each entry. A register of n qubits is written $|q_{n-1} \ldots q_1 q_0\rangle$, and entry x of its column of amplitudes is the amplitude of $|x\rangle$ with x read as a binary number. A phase on the whole state is not physical; a phase between two terms is. The inner product conjugates its first argument. And $\hbar = 1$, so a Hamiltonian is in angular frequency, evolution is $U(t) = e^{-iHt}$, and a logarithm of a probability is taken base two.

A.1 Chapter 1 · The mathematics of quantum states

A QUBIT STATE

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{bmatrix}\alpha \\ \beta\end{bmatrix}, \qquad |\alpha|^2 + |\beta|^2 = 1$$

The object every other formula acts on. Chapter 1, section 1.1.

THE INNER PRODUCT

$$\langle a| = |a\rangle^\dagger = \begin{bmatrix} a_1^* & \cdots & a_n^* \end{bmatrix}$$

$$\langle a|b\rangle = \sum_k a_k^* \, b_k$$

The conjugate sits on the first argument and on nothing else, so $\langle b|a\rangle = \langle a|b\rangle^*$. Chapter 1, section 1.1.

A COEFFICIENT IS AN INNER PRODUCT

$$|v\rangle = \sum_i v_i |e_i\rangle \qquad \Longrightarrow \qquad v_j = \langle e_j|v\rangle$$

True only for an orthonormal basis, and it is what an orthonormal basis is chosen for. Chapter 1, section 1.1.

CAUCHY–SCHWARZ, AND THE TWO ENDS OF IT

$$|\langle a|b\rangle| \le \|a\| \, \|b\|, \qquad 0 \le |\langle a|b\rangle|^2 \le 1 \ \text{ for normalised states}$$

Zero means orthogonal and one measurement separates the two with certainty; one means the same state up to a global phase. Chapter 1, section 1.1.

MODULUS AND PHASE

$$z = x + iy = r\,e^{i\varphi}, \qquad zz^* = x^2 + y^2 = |z|^2$$

Every probability in the course is a $|z|^2$ and every interference effect is a difference of two φ. Chapter 1, section 1.2.

A GLOBAL PHASE IS NOT PHYSICAL, A RELATIVE PHASE IS

$$e^{i\gamma}|\psi\rangle \;\equiv\; |\psi\rangle$$

$$\alpha|0\rangle + e^{i\varphi}\beta|1\rangle \;\not\equiv\; \alpha|0\rangle + \beta|1\rangle$$

The second line is the mechanism every algorithm in the course runs on. Chapter 1, section 1.2.

THE OUTER PRODUCT AND THE PROJECTOR

$$|a\rangle\langle b| = |a\rangle\,|b\rangle^\dagger, \qquad (|a\rangle\langle b|)_{jk} = a_j\,b_k^*$$

$$P_u = |u\rangle\langle u|, \qquad P_u^\dagger = P_u, \qquad P_u^2 = P_u$$

A bra eats the ket to its right first, so $(|a\rangle\langle b|)\,|v\rangle = \langle b|v\rangle\,|a\rangle$. Chapter 1, section 1.3.

THE RESOLUTION OF THE IDENTITY

$$\sum_k |e_k\rangle\langle e_k| = I$$

Used as a move rather than as a fact: inserting it turns a statement about a vector into a statement about its coefficients. Chapter 1, section 1.3.

GRAM–SCHMIDT

$$u_j = v_j - \sum_{i<j} \langle e_i|v_j\rangle\, e_i, \qquad e_j = \frac{u_j}{\|u_j\|}$$

The modified recursion subtracts against the partly built u_j rather than against v_j, and keeps far more digits. Chapter 1, section 1.4.

THE TENSOR PRODUCT

$$\begin{bmatrix} a_1 \\ a_2 \end{bmatrix} \otimes \begin{bmatrix} b_1 \\ b_2 \end{bmatrix} = \begin{bmatrix} a_1b_1 \\ a_1b_2 \\ a_2b_1 \\ a_2b_2 \end{bmatrix}$$

$$(A \otimes B)_{(i,j)} = A_{ij}B, \qquad \dim = 2^n \;\text{ for } n \text{ qubits}$$

Two qubits are four numbers and not two plus two, and that is where the exponential comes from. Chapter 1, section 1.5.

ADJOINT, HERMITIAN, UNITARY

$$A^\dagger = (A^*)^T, \qquad (AB)^\dagger = B^\dagger A^\dagger$$

$$A = A^\dagger \implies \text{real eigenvalues}, \qquad U^\dagger U = I \iff U^{-1} = U^\dagger$$

A Hermitian operator is a measurable quantity and a unitary one is a reversible motion. Chapter 1, section 1.6.

THE EXPONENTIAL THAT JOINS THEM

$$G = G^\dagger,\ \theta \in \mathbb{R} \qquad \implies \qquad U(\theta) = e^{-i\theta G} \ \text{ is unitary}$$

$$e^{-i\theta\sigma/2} = \cos\left(\tfrac{\theta}{2}\right) I \ - \ i \sin\left(\tfrac{\theta}{2}\right) \sigma$$

The second line holds for any operator whose square is the identity, which is every Pauli and every $\mathbf{n} \cdot \boldsymbol{\sigma}$. Chapter 1, section 1.6.

THE SPECTRAL DECOMPOSITION, AND A FUNCTION OF AN OPERATOR

$$A = \sum_k \lambda_k P_k, \qquad P_j P_k = \delta_{jk} P_k, \qquad \sum_k P_k = I$$

$$f(A) = \sum_k f(\lambda_k)\, P_k, \qquad e^{-iAt} = \sum_k e^{-i\lambda_k t}\, P_k$$

The second line is what makes an evolution operator computable at all. Chapter 1, section 1.7.

FUNCTIONS AS VECTORS, PARSEVAL AND TRUNCATION

$$\langle f|g\rangle = \int_a^b f^*(x) g(x)\,\mathrm{d}x, \qquad |f\rangle = \sum_{n=1}^{\infty} c_n |u_n\rangle, \qquad c_n = \langle u_n|f\rangle$$

$$\|f\|^2 = \sum_{n=1}^{\infty} |c_n|^2, \qquad \left\| f - \sum_{n=1}^{N} c_n u_n \right\|^2 = \sum_{n>N} |c_n|^2$$

The coefficient tail is the exact squared norm error of a truncated complete orthonormal expansion. Chapter 1, section 1.9.

A.2 Chapter 2 · States, measurement and dynamics

THE BORN RULE

$$p(n) = |\langle n|\psi\rangle|^2$$

The one postulate that connects a state to a number an instrument prints. Chapter 2, section 2.1.

PASSIVE COORDINATES AGAINST AN ACTIVE TRANSFORMATION

$$|\psi\rangle' = V^\dagger|\psi\rangle, \qquad A' = V^\dagger A V, \qquad \langle\psi|A|\psi\rangle = \langle\psi'|A'|\psi'\rangle$$

$$|\psi\rangle \longmapsto U|\psi\rangle \qquad \text{with } A \text{ fixed}$$

Passive coordinates preserve every prediction; an active operation generally changes them. Choosing new measurement projectors is a third operation. Chapter 2, section 2.1.

A PROJECTIVE MEASUREMENT, AND THE STATE IT LEAVES

$$p(a) = \langle\psi|P_a|\psi\rangle, \qquad P_j P_k = \delta_{jk} P_k, \qquad \sum_a P_a = I$$

$$|\psi_a\rangle = \frac{P_a|\psi\rangle}{\sqrt{p(a)}}$$

Orthogonality makes the outcomes exclusive and completeness makes them add to one. Chapter 2, section 2.2.

A POVM AND ITS MEASUREMENT INSTRUMENT

$$E_m = \sum_\alpha M_{m\alpha}^\dagger M_{m\alpha}, \qquad p(m) = \mathrm{Tr}(\rho E_m), \qquad \sum_m E_m = I$$

$$\rho_m = \frac{\sum_\alpha M_{m\alpha}\rho M_{m\alpha}^\dagger}{p(m)}$$

The effects fix the probabilities; the instrument also fixes the conditional state. The projective case is $M_m = P_m$. Chapter 2, section 2.2.

EXPECTATION AND VARIANCE

$$\langle A\rangle = \langle\psi|A|\psi\rangle = \sum_a a\, p(a)$$

$$\mathrm{Var}(A) = \langle A^2\rangle - \langle A\rangle^2, \qquad \Delta A = \sqrt{\mathrm{Var}(A)}$$

For any Pauli $A^2 = I$, so $\mathrm{Var}(A) = 1 - \langle A\rangle^2$ and no second sandwich is needed. Chapter 2, section 2.3.

THE ROBERTSON RELATION

$$\Delta A\,\Delta B \;\geq\; \tfrac{1}{2}\,|\langle [A,B]\rangle|\,, \qquad [A,B] = AB - BA$$

The bound depends on the state, so a vanishing right-hand side says nothing rather than saying both spreads are zero. Chapter 2, section 2.4.

OBSERVABLE	$+1$ EIGENSTATE	-1 EIGENSTATE
$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$	$\lvert+\rangle = \frac{1}{\sqrt{2}}(1,1)$	$\lvert-\rangle = \frac{1}{\sqrt{2}}(1,-1)$
$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$	$\lvert+i\rangle = \frac{1}{\sqrt{2}}(1,i)$	$\lvert-i\rangle = \frac{1}{\sqrt{2}}(1,-i)$
$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$	$\lvert 0\rangle = (1,0)$	$\lvert 1\rangle = (0,1)$

THE PAULI ALGEBRA

$$\sigma_i\sigma_j = \delta_{ij}\,I + i\sum_k \varepsilon_{ijk}\,\sigma_k$$

$$[\sigma_i,\sigma_j] = 2i\sum_k \varepsilon_{ijk}\sigma_k, \qquad \{\sigma_i,\sigma_j\} = 2\delta_{ij}I$$

Cyclic order $X \to Y \to Z \to X$ carries the plus sign. Two different Pauli operators anticommute. Chapter 2, section 2.5.

MEASURING ALONG A DIRECTION

$$\mathbf{n}\cdot\boldsymbol{\sigma}, \qquad P_\pm = \tfrac{1}{2}\,(I \pm \mathbf{n}\cdot\boldsymbol{\sigma})\,, \qquad r_a = \langle\sigma_a\rangle$$

$$p(\pm) = \tfrac{1}{2}\,(1 \pm \mathbf{n}\cdot\mathbf{r})\,, \qquad p(+) = \cos^2\frac{\alpha}{2}$$

α is the angle between two vectors, which is twice the angle between the two states. Chapter 2, section 2.5.

COORDINATE OPERATORS AND A FREE PARTICLE

$$(\hat{x}\psi)(x) = x\psi(x), \qquad (\hat{p}\psi)(x) = -i\hbar\frac{\mathrm{d}\psi}{\mathrm{d}x}$$

$$\hat{H}_0 = \frac{\hat{p}^2}{2m} = -\frac{\hbar^2}{2m}\frac{\mathrm{d}^2}{\mathrm{d}x^2}, \qquad p = \hbar k, \qquad E = \frac{\hbar^2 k^2}{2m}$$

A plane wave is a generalised eigenfunction; a physical free-particle state is a normalisable wave packet. Chapter 2, section 2.6.

THE INFINITE SQUARE WELL

$$\phi_n(x) = \sqrt{\frac{2}{a}}\sin\left(\frac{n\pi x}{a}\right), \qquad n = 1, 2, \ldots$$

$$E_n = \frac{\hbar^2\pi^2 n^2}{2ma^2}$$

The boundary conditions select discrete wave numbers. There is no $n = 0$ state, and $E_2 = 4E_1$. Chapter 2, section 2.6.

CLOSED-SYSTEM EVOLUTION

$$i\,\frac{\mathrm{d}}{\mathrm{d}t}|\psi(t)\rangle = H\,|\psi(t)\rangle$$

$$|\psi(t)\rangle = U(t)|\psi(0)\rangle, \qquad U(t) = e^{-iHt}$$

Replacing H by $H + cI$ multiplies U by a global phase, so only energy differences are physical. Chapter 2, section 2.6.

A DRIVEN QUBIT

$$H = \tfrac{1}{2}\left(\Omega_x X + \Omega_y Y + \Delta Z\right) = \tfrac{\Omega}{2}\,\mathbf{n}\cdot\boldsymbol{\sigma}, \qquad \Omega = \sqrt{\Omega_x^2 + \Omega_y^2 + \Delta^2}$$

$$U(t) = \cos\left(\tfrac{\Omega t}{2}\right) I - i\sin\left(\tfrac{\Omega t}{2}\right)\mathbf{n}\cdot\boldsymbol{\sigma}, \qquad p_{\max} = \left(\frac{\Omega_x}{\Omega}\right)^2$$

Pulse area sets the angle, drive phase sets the axis in the equator, and detuning tilts that axis towards z. Chapter 2, section 2.6.

WHAT A FINITE RUN IS WORTH

$$K \sim \mathrm{Binomial}(N, p), \qquad \mathrm{SE}\left(\tfrac{K}{N}\right) = \sqrt{\frac{p(1-p)}{N}} \le \frac{1}{2\sqrt{N}}$$

One more decimal place costs a hundred times the shots. This is counting and not physics, so no hardware improvement changes it. Chapter 2, section 2.7.

A.3 Chapter 3 · Mixed states and entanglement

THE DENSITY OPERATOR

$$\rho_\psi = |\psi\rangle\langle\psi|$$

$$\rho = \sum_i p_i\, |\psi_i\rangle\langle\psi_i|, \qquad p_i \geq 0, \qquad \sum_i p_i = 1$$

It does not remember which preparation made it: two different mixtures with the same ρ are the same state. Chapter 3, section 3.1.

WHICH MATRICES ARE STATES, AND EVERY PREDICTION FROM ONE TRACE

$$\rho = \rho^\dagger, \qquad \rho \succeq 0, \qquad \mathrm{Tr}\,\rho = 1$$

$$\langle A\rangle = \mathrm{Tr}\,(\rho A)\,, \qquad p(m) = \mathrm{Tr}\,(\rho E_m)$$

For one qubit positivity is the single inequality $|\rho_{01}|^2 \leq \rho_{00}\rho_{11}$. Chapter 3, section 3.1.

PURITY

$$\gamma = \mathrm{Tr}\left(\rho^2\right) = \sum_k \lambda_k^2, \qquad \frac{1}{d} \leq \gamma \leq 1$$

It says how mixed and never which state: one number where a qubit state needs three. Chapter 3, section 3.2.

A QUBIT STATE AS A VECTOR

$$\rho = \tfrac{1}{2}\,(I + \mathbf{r}\cdot\boldsymbol{\sigma})\,, \qquad r_a = \mathrm{Tr}\,(\rho\,\sigma_a)\,, \qquad |\mathbf{r}| \leq 1$$

$$\lambda_\pm = \tfrac{1}{2}\,(1 \pm |\mathbf{r}|)\,, \qquad \mathrm{Tr}\,\rho^2 = \tfrac{1}{2}\left(1 + |\mathbf{r}|^2\right)$$

From a state vector (a, b) the y component reads $r_y = 2\,\mathrm{Im}(a^*b)$; from ρ it reads $r_y = -2\,\mathrm{Im}\,\rho_{01}$. The two signs are not a contradiction, and both give $r_y = +1$ on $|+i\rangle$. Chapter 3, section 3.2.

A CHANNEL IN KRAUS FORM

$$\mathcal{E}(\rho) = \sum_k K_k\,\rho\,K_k^\dagger, \qquad \sum_k K_k^\dagger K_k = I$$

Every channel arises this way, and two different sets of Kraus operators can describe one channel. Chapter 3, section 3.3.

AMPLITUDE DAMPING

$$K_0 = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{bmatrix}, \qquad K_1 = \begin{bmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{bmatrix}$$

$$\rho_{11} \mapsto (1-\gamma)\rho_{11}, \qquad \rho_{01} \mapsto \sqrt{1-\gamma}\,\rho_{01}$$

At $\gamma = 1$ every state becomes $|0\rangle$, which is why this is the model of relaxation. Chapter 3, section 3.3.

THE PHASE-FLIP CHANNEL

$$\mathcal{E}_Z(\rho) = (1-p)\,\rho + p\,Z\rho Z$$

$$\rho_{00}, \rho_{11} \text{ unchanged}, \qquad \rho_{01} \mapsto (1-2p)\,\rho_{01}$$

The damage peaks at $p = \frac{1}{2}$ and vanishes at $p = 1$, where the channel is the gate Z. Chapter 3, section 3.3.

THE TWO DECAY TIMES

$$\rho_{11}(t) = \rho_{11}^{\mathrm{eq}} + [\rho_{11}(0) - \rho_{11}^{\mathrm{eq}}]\,e^{-t/T_1}, \qquad \rho_{01}(t) = e^{-t/T_2}\rho_{01}(0)$$

$$\frac{1}{T_2} = \frac{1}{2T_1} + \frac{1}{T_\phi} \qquad \Longrightarrow \qquad T_2 \le 2T_1$$

Populations decay on T_1 and the coherence on T_2, and the inequality is a theorem rather than a measurement. Chapter 3, section 3.4.

THE ORDERING THIS COURSE FIXES

$$\begin{bmatrix} a \\ b \end{bmatrix} \otimes \begin{bmatrix} c \\ d \end{bmatrix} = \begin{bmatrix} ac \\ ad \\ bc \\ bd \end{bmatrix}, \qquad |q_1 q_0\rangle$$

Read under the other convention this names a different state, and every number downstream is quietly wrong. Chapter 3, section 3.5.

THE PARTIAL TRACE

$$\rho_A = \mathrm{Tr}_B\,(\rho_{AB}) = \sum_j (I_A \otimes \langle j|)\,\rho_{AB}\,(I_A \otimes |j\rangle)$$

$$\mathrm{Tr}\,(\rho_A A) = \mathrm{Tr}\,[\rho_{AB}\,(A \otimes I_B)] \quad \text{for every } A$$

The second line is the property that makes it the right operation: it is the state that answers every question about A alone. Chapter 3, section 3.5.

SEPARABILITY, AND THE SCHMIDT FORM

$$|\psi\rangle \text{ is a product } \iff c_0c_3 - c_1c_2 = 0$$

$$|\psi\rangle_{AB} = \sum_{k=1}^{r} \sqrt{\lambda_k}\, |u_k\rangle_A |v_k\rangle_B, \qquad \lambda_k > 0, \quad \sum_k \lambda_k = 1$$

The Schmidt rank r is one exactly when the pair is a product. Chapter 3, section 3.6.

ENTANGLEMENT ENTROPY

$$S(\rho) = -\operatorname{Tr}(\rho \log_2 \rho) = -\sum_k \lambda_k \log_2 \lambda_k, \qquad S(\rho_A) = S(\rho_B)$$

Zero for a product and one bit for a Bell state. Chapter 3, section 3.6.

THE BELL STATES

$$|\Phi^{\pm}\rangle = \frac{|00\rangle \pm |11\rangle}{\sqrt{2}}, \qquad |\Psi^{\pm}\rangle = \frac{|01\rangle \pm |10\rangle}{\sqrt{2}}$$

$$\text{for } |\Phi^{+}\rangle: \quad \langle X \otimes X\rangle = 1, \qquad \langle Y \otimes Y\rangle = -1, \qquad \langle Z \otimes Z\rangle = 1$$

All four share the same reduced state $I/2$ and differ only in their joint correlations. Chapter 3, section 3.7.

CHSH, AND THE TWO CEILINGS

$$S = \langle A_0B_0\rangle + \langle A_0B_1\rangle + \langle A_1B_0\rangle - \langle A_1B_1\rangle$$

$$|S| \le 2 \text{ for pre-existing values}, \qquad |S| \le 2\sqrt{2} \text{ for quantum states}$$

Both bounds are theorems. A measured value above two is what rules out the first model. Chapter 3, section 3.7.

A.4 Chapter 4 · The Bloch sphere and quantum gates

A PURE QUBIT STATE, AND THE POINT IT NAMES

$$|\psi(\theta,\varphi)\rangle = \cos\frac{\theta}{2}\,|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}\,|1\rangle, \qquad 0\le\theta\le\pi, \quad 0\le\varphi<2\pi$$

$$\mathbf{r} = (\sin\theta\cos\varphi,\ \sin\theta\sin\varphi,\ \cos\theta)\,, \qquad |\mathbf{r}| = 1$$

At a pole the azimuth means nothing, because $\sin 0 = 0$ leaves nothing for the phase to multiply. Chapter 4, section 4.1.

THE OVERLAP OF TWO PURE STATES

$$|\langle\chi|\psi\rangle|^2 = \frac{1+\mathbf{r}\cdot\mathbf{s}}{2} = \cos^2\frac{\Theta}{2}$$

Orthogonal states sit at opposite points; points at a right angle overlap with probability one half. Chapter 4, section 4.1.

A FULL TURN IS NOT THE IDENTITY

$$R_{\mathbf{n}}(2\pi) = -I, \qquad R_{\mathbf{n}}(4\pi) = +I$$

U and $-U$ give the same rotation of the sphere, so the map from gates to rotations is two to one. Chapter 4, section 4.2.

THE ROTATION OPERATOR

$$R_{\mathbf{n}}(\alpha) = e^{-i\alpha\,\mathbf{n}\cdot\boldsymbol{\sigma}/2} = \cos\frac{\alpha}{2}\,I - i\sin\frac{\alpha}{2}\,\mathbf{n}\cdot\boldsymbol{\sigma}$$

$$\text{every } 2\times 2 \text{ unitary} = e^{i\gamma}R_{\mathbf{n}}(\alpha) \ \text{ for some } \gamma,\ \mathbf{n},\ \alpha$$

Rotation is not one family of one-qubit gates among many; it is all of them. Chapter 4, section 4.3.

THE PAULI GATES AS ROTATIONS

$$R_x(\pi) = -iX, \qquad R_y(\pi) = -iY, \qquad R_z(\pi) = -iZ$$

$$\begin{aligned} X:&\ \ |0\rangle \leftrightarrow |1\rangle, \qquad |+\rangle \text{ and } |-\rangle \text{ fixed} \\ Z:&\ \ |+\rangle \leftrightarrow |-\rangle, \qquad |0\rangle \text{ and } |1\rangle \text{ fixed} \end{aligned}$$

Which gate looks like a flip depends entirely on the basis the state is written in. Chapter 4, section 4.3.

THE HADAMARD

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \frac{X+Z}{\sqrt{2}}, \qquad H^2 = I$$

$$HXH = Z, \qquad HZH = X, \qquad HYH = -Y$$

Measuring X is applying H and then measuring Z, which is the only reading a machine offers. Chapter 4, section 4.3.

THE PHASE FAMILY

$$P(\varphi) = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{bmatrix} = e^{i\varphi/2} \, R_z(\varphi)$$

$$S = P\left(\tfrac{\pi}{2}\right), \qquad T = P\left(\tfrac{\pi}{4}\right), \qquad S^2 = Z, \quad T^2 = S$$

S is a Clifford gate and cheap to correct for; T is not, and that difference sets the cost of fault tolerance. Chapter 4, section 4.3.

THE ORDER A CIRCUIT MULTIPLIES IN

$$U_1 \text{ first}, \ U_2 \text{ next}, \ U_3 \text{ last} \qquad \Longrightarrow \qquad U = U_3 \, U_2 \, U_1$$

$$(A \otimes I)\,(I \otimes B) = A \otimes B = (I \otimes B)\,(A \otimes I)$$

Gates on different qubits always commute; gates sharing a qubit usually do not. Chapter 4, section 4.4.

THE EULER DECOMPOSITION, AND THE GATE WITH THREE DIALS

$$U = e^{i\alpha} \, R_z(\phi) \, R_y(\theta) \, R_z(\lambda)$$

$$U(\theta, \phi, \lambda) = \begin{bmatrix} \cos\frac{\theta}{2} & -e^{i\lambda} \sin\frac{\theta}{2} \\ e^{i\phi} \sin\frac{\theta}{2} & e^{i(\phi+\lambda)} \cos\frac{\theta}{2} \end{bmatrix}$$

$H = U(\frac{\pi}{2}, 0, \pi)$, $X = U(\pi, 0, \pi)$ and $P(\varphi) = U(0, \varphi, 0)$. Chapter 4, section 4.4.

REVERSIBLE EMBEDDINGS AND THE ORACLE PATTERN

$$(a,\ b) \longmapsto (a,\ \ a \oplus b) \qquad \text{is exactly CNOT}$$

$$|x\rangle|y\rangle \longmapsto |x\rangle \, |y \oplus f(x)\rangle \qquad \text{for any } f$$

AND needs a third wire, $(a, b, c) \mapsto (a, b, c \oplus ab)$, which is the Toffoli gate. Chapter 4, section 4.5.

A REVERSIBLE HALF ADDER

$$(a, b, 0, 0) \longmapsto (a, b, a \oplus b, ab)$$

Two CNOTs write the sum and one Toffoli writes the carry. Preserving the inputs makes the map invertible. Chapter 4, section 4.5.

COMPUTE, COPY OUT, UNCOMPUTE

$$V_f^\dagger \;(\text{copy})\; V_f \;:\; |x\rangle|0\rangle|y\rangle \;\longmapsto\; |x\rangle|0\rangle|y \oplus f(x)\rangle$$

An ancilla that leaves in a state depending on x stays entangled with the register, and the interference at the end does not happen. Chapter 4, section 4.5.

A ONE-QUBIT GATE ON A NAMED QUBIT

$$\text{on } q_0 : \; I \otimes A, \qquad \text{on } q_1 : \; A \otimes I$$

$$(I \otimes X)\,|10\rangle = |11\rangle, \qquad (X \otimes I)\,|10\rangle = |00\rangle$$

Both are valid gates and they do different things. Nothing in the mathematics protects a reader who picks the wrong one. Chapter 4, section 4.6.

THE TWO CNOT MATRICES, IN THE BASIS ORDER $|00\rangle, |01\rangle, |10\rangle, |11\rangle$

$$\text{CNOT} : \; |c\rangle|t\rangle \longmapsto |c\rangle|c \oplus t\rangle$$

$$\text{CNOT}_{0\to1} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}, \qquad \text{CNOT}_{1\to0} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

The subscript reads control to target. Chapter 4, section 4.6.

CZ AND SWAP

$$\text{CZ} = \text{diag}(1, 1, 1, -1) = (H \otimes I)\;\text{CNOT}_{0\to1}\;(H \otimes I)$$

$$\text{SWAP} = \text{CNOT}_{0\to1}\;\text{CNOT}_{1\to0}\;\text{CNOT}_{0\to1}$$

Three two-qubit gates to move a state one step across a chip, which is what routing costs. Chapter 4, section 4.6.

MAKING A BELL PAIR, AND TWO UNIVERSAL SETS

$$|00\rangle \xrightarrow{I \otimes R_y(\theta)} \cos\tfrac{\theta}{2}|00\rangle + \sin\tfrac{\theta}{2}|01\rangle \xrightarrow{\text{CNOT}_{0\to1}} \cos\tfrac{\theta}{2}|00\rangle + \sin\tfrac{\theta}{2}|11\rangle$$

$$\{\text{every one-qubit gate}\} \cup \{\text{CNOT}\} \;\text{ exactly}, \qquad \{H,\; S,\; T,\; \text{CNOT}\} \;\text{ to any } \varepsilon > 0$$

A gate is entangling if it entangles some input, not every input. The price of ε is a length growing like a power of $\log(1/\varepsilon)$. Chapter 4, section 4.7.

A.5 Chapter 5 · Circuits and protocols

THE CIRCUIT MODEL, IN ONE LINE

$$|0\rangle^{\otimes n} \xrightarrow{U_d \cdots U_2 U_1} |\psi\rangle \xrightarrow{\text{measure}} x \in \{0,1\}^n$$

Fixed input, fixed gate set, fixed measurement basis, and one string per run. Chapter 5, section 5.1.

ONE STATE, NAMED FOUR WAYS

$$|q_{n-1} \, \ldots \, q_1 q_0\rangle, \qquad x = \sum_k 2^k q_k$$

A run that prints 101 read $q_2 = 1$, $q_1 = 0$, $q_0 = 1$, which is entry 5 of the state vector. Chapter 5, section 5.1.

DEPTH, GATE COUNT AND SIMULATION COST

$$\text{depth} = \text{layers of gates that must run in order}, \qquad \text{count} = \text{gates}$$

$$\text{bytes} = 16 \cdot 2^n, \qquad n = 30 \Rightarrow 17\,\text{GB}, \qquad n = 50 \Rightarrow 18\,\text{PB}$$

A coherence time is spent against depth and an error budget against the two-qubit count. The size of the vector is an upper bound on the difficulty of simulation and never a lower one. Chapter 5, sections 5.1 and 5.2.

THE ERROR BAR ON A PROBABILITY READ FROM A FINITE RUN

$$K \sim \text{Binomial}(N, p), \qquad \text{SE}(\hat{p}) = \sqrt{\frac{p(1-p)}{N}}$$

An estimate near one half to within ± 0.005 needs ten thousand shots. Chapter 5, section 5.2.

DEFERRED MEASUREMENT

$$\text{measure } q_0, \text{ then } X^m \text{ on } q_1 \;\equiv\; \text{CNOT}_{0\to 1}, \text{ then measure } q_0$$

The rule is about a measured wire used as a control and about nothing else. Chapter 5, section 5.2.

TWO EXACT REWRITES A COMPILER USES

$$H = e^{i\pi/2} R_z\left(\tfrac{\pi}{2}\right) R_x\left(\tfrac{\pi}{2}\right) R_z\left(\tfrac{\pi}{2}\right)$$

$$\text{CNOT}_{0\to 1} = (H \text{ on } q_1) \;\text{CZ}\; (H \text{ on } q_1)$$

What is lost is only length; the two-qubit count does not move. The phase in the first line becomes observable the moment the gate is controlled. Chapter 5, section 5.3.

THE FAULT-TOLERANCE THRESHOLD CONDITION

$$p < p_{\mathrm{th}}$$

For a stated code, noise model and control system, increasing the code distance can then reduce the logical error rate. The threshold is not one universal number. Chapter 5, section 5.3.

TURNING A PHASE INTO COUNTS

$$|0\rangle \xrightarrow{H} \tfrac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \xrightarrow{P(\varphi)} \tfrac{1}{\sqrt{2}}\left(|0\rangle + e^{i\varphi}|1\rangle\right)$$
$$\xrightarrow{H} \tfrac{1}{2}\left(1 + e^{i\varphi}\right)|0\rangle + \tfrac{1}{2}\left(1 - e^{i\varphi}\right)|1\rangle, \qquad p(0) = \cos^2\frac{\varphi}{2}$$

Measuring in the middle learns nothing; the second Hadamard is what makes the phase readable. Chapter 5, section 5.4.

TELEPORTATION, AS ONE IDENTITY

$$|\Psi_2\rangle = \tfrac{1}{2}\sum_{m_1, m_0 \in \{0,1\}} |m_1 m_0\rangle_{10} \otimes X^{m_1} Z^{m_0} |\psi\rangle_2$$

Exact, and independent of α and β. Bob applies Z^{m_0} and then X^{m_1} to undo it. Chapter 5, section 5.5.

WHAT BOB HOLDS BEFORE THE BITS ARRIVE

$$\rho_B = \tfrac{1}{4}\sum_{m_1, m_0} X^{m_1} Z^{m_0}\, \rho\, Z^{m_0} X^{m_1} = \frac{I}{2}$$

No ρ on the right-hand side, which is why the protocol sends nothing ahead of the two classical bits. Chapter 5, section 5.5.

PHASE KICKBACK

$$X|-\rangle = -|-\rangle$$
$$U_f\,|x\rangle|-\rangle = (-1)^{f(x)}\,|x\rangle|-\rangle$$

The target comes out unchanged, so the answer has landed on the first register as a sign. Chapter 5, section 5.6, and again in chapter 6.

THE PLANE GROVER SEARCH LIVES IN

$$|G\rangle = \frac{1}{\sqrt{M}} \sum_{f(x)=1} |x\rangle, \qquad |B\rangle = \frac{1}{\sqrt{N-M}} \sum_{f(x)=0} |x\rangle$$

$$|s\rangle = \sin\theta\,|G\rangle + \cos\theta\,|B\rangle, \qquad \sin\theta = \sqrt{\frac{M}{N}}$$

A real two-dimensional plane inside a complex space of 2^n dimensions. It is not a Bloch sphere. Chapter 5, section 5.6.

THE GROVER SUCCESS PROBABILITY, AND WHERE IT PEAKS

$$P_{\text{good}}(r) = \sin^2\big((2r+1)\theta\big)$$

$$r_* = \frac{\pi}{4\theta} - \frac{1}{2}, \qquad r_* \approx \frac{\pi}{4}\sqrt{\frac{N}{M}} \text{ when } M \ll N$$

Each iteration adds a fixed angle 2θ, and a right angle has to be reached. Iterating past r_* makes the answer less likely. Chapter 5, section 5.6.

WHAT A RESOURCE CLAIM MUST NAME

The task, the input model, the accuracy, the hardware model, and the classical baseline it is measured against. A claim missing one of the five is not yet a claim, and a query count is not a runtime. Chapter 5, section 5.7.

A.6 Chapter 6 · Quantum algorithms

THE ORACLE, AND WHAT ONE QUERY MEANS

$$U_f\,|x\rangle|y\rangle = |x\rangle\,|y \oplus f(x)\rangle$$

Building U_f costs gates and those gates are not counted. A query separation is a theorem about one column of the table. Chapter 6, section 6.1.

KICKBACK WITH AN ARBITRARY UNITARY

$$U\,|u\rangle = e^{2\pi i\varphi}\,|u\rangle$$

$$cU\,\tfrac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big)|u\rangle = \tfrac{1}{\sqrt{2}}\big(|0\rangle + e^{2\pi i\varphi}|1\rangle\big)|u\rangle$$

On a superposition of eigenstates the procedure samples one eigenphase with probability $|c_k|^2$; it does not list the spectrum. Chapter 6, section 6.2.

WHAT THE LAST LAYER OF HADAMARDS IS FOR

$$\langle 0^n|\,H^{\otimes n}\Big(\tfrac{1}{2^{n/2}}\textstyle\sum_x(-1)^{f(x)}|x\rangle\Big) = \tfrac{1}{2^n}\textstyle\sum_x(-1)^{f(x)}$$

A superposition that never interferes has bought nothing. The readout returns n bits, never 2^n numbers. Chapter 6, section 6.2.

DEUTSCH, AND DEUTSCH–JOZSA

$$\tfrac{1}{\sqrt{2}}\Big((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\Big) \xrightarrow{H} \pm|\,f(0)\oplus f(1)\,\rangle$$

$$\text{amplitude of } |0^n\rangle = \frac{1}{2^n}\sum_x(-1)^{f(x)} = \begin{cases}\pm 1 & \text{constant}\\ 0 & \text{balanced}\end{cases}$$

One query against $2^{n-1}+1$ exact classical queries, on a promised input. Chapter 6, section 6.3.

THE QUANTUM FOURIER TRANSFORM, AND ITS CIRCUIT

$$F_Q\,|x\rangle = \frac{1}{\sqrt{Q}}\sum_{k=0}^{Q-1} e^{2\pi i\,xk/Q}\,|k\rangle, \qquad Q = 2^n$$

$$R_k = \begin{bmatrix}1 & 0\\ 0 & e^{2\pi i/2^k}\end{bmatrix}, \qquad n + \tfrac{1}{2}n(n-1) = \tfrac{1}{2}n(n+1)\text{ gates}$$

It is a change of basis and returns one index, never a spectrum. F_2 is the Hadamard. Chapter 6, section 6.4.

PHASE ESTIMATION

$$\frac{1}{\sqrt{2^t}}\sum_{k=0}^{2^t-1} e^{2\pi i k\varphi}\,|k\rangle \xrightarrow{F^\dagger} y, \qquad \hat{\varphi} = \frac{y}{2^t}$$

$$P(y) = \frac{1}{2^{2t}}\left|\frac{\sin\left(\pi\, 2^t\delta\right)}{\sin(\pi\delta)}\right|^2, \qquad \delta = \varphi - \frac{y}{2^t}$$

Costs $2^t - 1$ applications of U against $\frac{1}{2}t(t+1)$ gates in the inverse transform. Chapter 6, section 6.5.

THE TWO FLOORS, AND HOW MANY COUNTING QUBITS TO TAKE

$$P(\text{nearest}) \geq \frac{4}{\pi^2} \approx 0.405, \qquad P(\text{two nearest}) \geq \frac{8}{\pi^2} \approx 0.811$$

$$t = n + \left\lceil \log_2\left(2 + \frac{1}{2\varepsilon}\right)\right\rceil$$

Neither floor moves as the register grows: extra qubits buy accuracy and never confidence. Chapter 6, section 6.5.

ORDER FINDING

$$U_a\,|y\rangle = |\,a\,y \bmod N\,\rangle, \qquad U_a\,|u_s\rangle = e^{2\pi i s/r}\,|u_s\rangle$$

$$\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}|u_s\rangle = |1\rangle, \qquad |u_s\rangle = \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1} e^{-2\pi i s k/r}\,|a^k \bmod N\rangle$$

The order sits in the denominators of the eigenphases, and starting the work register in the state one costs a single gate. Chapter 6, section 6.6.

WHY THE READING IS ENOUGH

$$\left|\frac{y}{Q} - \frac{s}{r}\right| \leq \frac{1}{2Q}, \qquad Q > N^2 \implies \frac{s}{r} \text{ is the only such fraction}$$

Continued fractions recover s/r from the reading, and one modular exponentiation confirms r. The condition $Q > N^2$ is what doubles the counting register. Chapter 6, section 6.6.

THE FACTORS, FROM THE ORDER

$$\gcd\left(a^{r/2} - 1,\, N\right) \quad \text{and} \quad \gcd\left(a^{r/2} + 1,\, N\right)$$

Needs r even and $a^{r/2} \not\equiv -1 \bmod N$; a random a satisfies both at least half the time. Chapter 6, section 6.7.

WHERE THE WORK IS

$$\text{modular exponentiation } O(L^3), \qquad \text{transform } O(L^2), \qquad \text{everything else classical}$$

The arithmetic is the algorithm, and the quantum step exists only to supply the exponent that makes the algebra apply. Chapter 6, section 6.7.

PART 3

Notation

Every symbol the course defines, with the chapter that defines it. A symbol is never reused for a second meaning.

$|\psi\rangle$

A quantum state, written as a column of complex numbers once a basis has been chosen. Normalised: $\langle\psi|\psi\rangle = 1$.

$\langle\psi|$

The dual of $|\psi\rangle$: the same column transposed and conjugated, so it is a row that eats a ket and returns a number.

$\langle\phi|\psi\rangle$

Inner product, conjugating the first argument. It measures overlap: zero when the two states are perfectly distinguishable, unit modulus when they are the same state.

$\|\psi\|$

Length of a state, $\sqrt{\langle\psi|\psi\rangle}$. A physical state has length one, which is what makes the Born probabilities sum to one.

$|\phi\rangle\langle\psi|$

Outer product: a ket beside a bra is an operator, not a number. It is the one construction that turns states into the things that act on states.

P_k

A projector, $P_k = |k\rangle\langle k|$ for a basis state. Idempotent, $P_k^2 = P_k$, and Hermitian.

$\sum_k |k\rangle\langle k| = I$

Resolution of the identity. Inserting it is how a basis expansion is derived rather than guessed.

$\otimes$

Tensor product. Two systems of dimension d_1 and d_2 make one system of dimension $d_1 d_2$, not $d_1 + d_2$: this is where the exponential comes from.

$A^\dagger$

Adjoint: transpose and conjugate. In NumPy, `A.conj().T`.

$A = A^\dagger$

Hermitian. Its eigenvalues are real, which is why observables are Hermitian: a measurement returns a real number.

$U^\dagger U = I$

Unitary. It preserves inner products and therefore norms, which is why closed-system evolution and every gate is unitary.

$A|v\rangle = \lambda|v\rangle$

Eigenvalue equation. The eigenvectors are the states the operator leaves in place, up to a scale.

$A = \sum_k \lambda_k P_k$

Spectral decomposition of a Hermitian operator: the eigenvalues, and the projectors onto the eigenspaces they belong to.

$f(A) = \sum_k f(\lambda_k) P_k$

A function of an operator is that function applied to the eigenvalues. This is what an operator exponential means, and it is why e^{-iHt} can be computed at all.

$L^2[a,b]$
: The vector space of square-integrable functions on an interval, with inner product $\langle f|g\rangle = \int_a^b f^*(x)g(x)\,\mathrm{d}x$.

$\|f\|^2 = \sum_n |c_n|^2$
: Parseval identity for a complete orthonormal basis. The omitted coefficient tail is the exact squared error of a truncated expansion.

$|0\rangle,\ |1\rangle$
: The computational basis of one qubit, the eigenvectors of Z. Every measurement in this course is in this basis unless a scene says otherwise.

$|+\rangle,\ |-\rangle$
: The X basis, $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. A state definite in X is maximally uncertain in Z.

$|+i\rangle,\ |-i\rangle$
: The Y basis, $(|0\rangle \pm i|1\rangle)/\sqrt{2}$.

$p(k) = |\langle k|\psi\rangle|^2$
: The Born rule. The amplitude is complex and unobservable; its squared modulus is the probability, and that is the only bridge from the mathematics to a laboratory count.

A
: An observable: a Hermitian operator whose eigenvalues are the outcomes that can be seen and whose eigenvectors are the states that give them with certainty.

$\langle A\rangle$
: Expectation value, $\langle\psi|A|\psi\rangle$. It is an average over repetitions, never the result of one run.

ΔA
: Standard deviation of an observable in a state, $\sqrt{\langle A^2\rangle - \langle A\rangle^2}$.

$[A,B]$
: Commutator, $AB - BA$. It is zero exactly when the two observables share an eigenbasis and can both be definite at once.

$X,\ Y,\ Z$
: The Pauli operators. Each is Hermitian and unitary at once, so each is both an observable and a gate.

H
: Hamiltonian: the Hermitian operator that generates evolution. With $\hbar = 1$ it is measured in angular frequency.

$U(t) = e^{-iHt}$
: The evolution operator of a closed system. Every gate in this course is one of these for some H and some duration.

$\{E_k\}$
: A POVM: positive operators summing to the identity. It fixes the outcome probabilities, but not the state left by the measurement.

$\{M_{m\alpha}\}$
: A measurement instrument. It realises each POVM effect and fixes the conditional state after an outcome.

$\hat{x},\ \hat{p}$
: Position and momentum in the coordinate representation: position multiplies a wavefunction and momentum differentiates it.

$\phi_n,\ E_n$
: The stationary states and discrete energies of the infinite square well, selected by boundary conditions at the two walls.

N_{shots}
: The number of repetitions a circuit is run for. A probability read from N shots carries a standard error of about $\sqrt{p(1-p)/N}$, which is sampling noise and not physical noise.

ρ
: Density operator: positive semidefinite, Hermitian, unit trace. It describes a state that is either genuinely mixed or a piece of a larger entangled state.

$\operatorname{Tr}\rho^2$
: Purity. Equal to one for a pure state and as low as $1/d$ for the maximally mixed state of dimension d.

$\mathcal{E}(\rho) = \sum_k K_k \rho K_k^\dagger$
: A quantum channel in Kraus form, with $\sum_k K_k^\dagger K_k = I$. This is what a gate becomes once the system is no longer closed.

Tr_B
: Partial trace: the operation that answers "what is the state of A alone". Its result is mixed exactly when A and B are entangled.

λ_i
: Schmidt coefficients of a bipartite pure state. One non-zero coefficient means the state is a product; more than one means it is entangled.

$S(\rho)$
: Von Neumann entropy, $-\operatorname{Tr}\rho\log_2\rho$, in bits. For a pure state it is zero, and for the reduced state of an entangled pair it is how much entanglement the pair carries.

$|\Phi^\pm\rangle,\ |\Psi^\pm\rangle$
: The four Bell states: an orthonormal basis of two qubits in which every state is maximally entangled.

$T_1,\ T_2$
: Relaxation and dephasing times. T_1 is how long a population survives, T_2 how long a relative phase does, and $T_2 \le 2T_1$ always.

$\mathbf{r}$
: Bloch vector, $r_a = \operatorname{Tr}(\rho\,\sigma_a)$ for $a = x, y, z$. Its length is one for a pure state and less for a mixed one, so the sphere is really a ball.

$\theta,\ \varphi$
: Polar and azimuthal angles of a pure qubit state, $\cos(\theta/2)|0\rangle + e^{i\varphi}\sin(\theta/2)|1\rangle$. The half angle is not a typographic accident: it is the double cover.

$R_a(\theta)$
: Rotation of the Bloch vector by θ about axis a, $e^{-i\theta\sigma_a/2}$. Every single-qubit gate is one of these up to a global phase.

H
: The Hadamard gate, which exchanges the Z and X bases. Written the same way as a Hamiltonian, and told apart by where it stands: a gate acts in a circuit, a Hamiltonian sits in an exponential.

S, T

The quarter- and eighth-turn phase gates about Z, $S = \mathrm{diag}(1, i)$ and $T = \mathrm{diag}(1, e^{i\pi/4})$.

CNOT

The controlled-NOT gate. Together with the single-qubit gates it is universal, and on its own it is what turns a product state into an entangled one.

d

Circuit depth: the number of layers of gates that must run one after another. It is the quantity a coherence time is spent against, and it is not the gate count.

ISA

The instruction set a particular machine actually runs. A circuit written in ideal gates is transpiled into it, and the transpiled depth is the one that matters.

F

Fidelity between a prepared state and its target, $F = \langle\psi|\rho|\psi\rangle$ for a pure target. A protocol is claimed to work only against a fidelity that beats the best classical strategy.

k_{opt}

The number of Grover iterations that maximises the success probability, about $\frac{\pi}{4}\sqrt{N/M}$. Running past it makes the answer less likely, not more.

U_f

A reversible embedding of a classical function, $U_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$. Counting queries to it is not the same as counting the gates it costs to build.

phase kickback

The mechanism behind every algorithm in this chapter: an oracle written to change a target register instead writes a phase onto the control register, because the target was prepared in an eigenstate of the operation.

QFT_N

The quantum Fourier transform on $N = 2^n$ amplitudes. It costs $O(n^2)$ gates, and it does not hand back the spectrum: the amplitudes it produces still have to be measured.

φ

The phase estimated by quantum phase estimation, defined by $U|u\rangle = e^{2\pi i\varphi}|u\rangle$. The number of counting qubits fixes both the precision and the success probability.

r

The order of a modulo N: the smallest $r > 0$ with $a^r \equiv 1 \pmod{N}$. Finding it is the only quantum step in factoring; everything around it is classical.