Quantum Mechanics

A Gentle Introduction

Sebastian Riese

27.12.2018

Concept of This Talk

- key experiments will be reviewed
- not historical: make the modern theory plausible using historical experiments, leave the history be history, modify the experiments to make a point
- quantum mechanics is quite abstract and not "anschaulich" so we will need mathematics (linear algebra, differential equations)
- we'll try to find a new, post-classical, "Anschaulichkeit" however in the end the adage "shut up and calculate" holds
- we'll include maths crash courses where we need them (mathematicians will suffer, sorry guys and gals)

How Scientific Theories Work

- a scientific theory is a net of interdependent propositions
- when extending the theory different propositions are proposed as hypotheses
- the hypotheses that stand the experimental test are added to the theory
- new experimental results are either consistent or inconsistent with the propositions of the theory
- if they are inconsistent, some of the propositions have been *falsified*, and the theory must be amended in the minimal (*Occam's razor*) way that makes it consistent with all experimental results
- new theoretical ideas must explain why the old ones worked

How It All Began

- time frame: late 19$^{\text{th}}$/early 20$^{\text{th}}$ century
- known fundamental theories of physics:
  - classical mechanics ($\boldsymbol{F} = m\boldsymbol{a}$)
  - Newtonian gravitation ($\boldsymbol{F} = G m_1 m_2 \frac{\boldsymbol{r_1} - \boldsymbol{r_2}}{|\boldsymbol{r_1} - \boldsymbol{r_2}|^3}$)
  - Maxwellian electrodynamics ($\partial_\mu F^{\mu\nu} = 4\pi j^\nu$, Lorentz force)
  - (Maxwell-Boltzmann classical statistical physics)
- several experimental results could not be explained by the classical physical theories under reasonable assumptions, e.g.
  - photoelectric effect (Hertz and Hallwachs 1887)
  - discrete spectral lines of atoms (Fraunhofer 1815, Bunsen and Kirchhoff 1858)
  - radioactive rays: single spots on photographic plates
  - stability of atoms composed of compact, positively charged nuclei (Rutherford 1909) and negatively charged cathode ray particles (Thomson 1897)

Cathode Rays

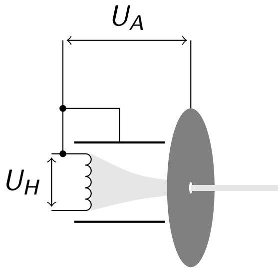

Figure: Schematic of an Electron Gun

- to-do list
  1. have a heated cathode, a simple electrostatic accelerator and a pinhole (an "electron gun")
  2. put it in an evacuated tube (if there's some well chosen gas left it'll glow nicely)
  3. play around (tips: magnetic fields, electric fields, fluorescent screens, etc.)
- results: there are negatively charged particles that can be separated from metal electrodes, hydrogen gas, etc.
- atoms are neutral – conclusion: there is a positively charged component as well

Rutherford(-Marsden-Geiger) Experiment

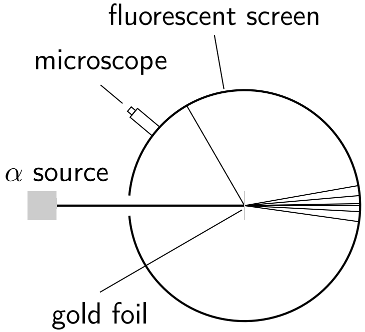

Figure: Schematic of the Rutherford Experiment

- measure the deflection angles of α particles shot perpendicularly through a thin gold foil
- weird result: some of the α are deflected strongly
- conclusion from deflection calculations for different charge/mass distributions: atoms must contain a small and massive concentration of mass and charge (the *nucleus*)

Atoms Are Stable!?

- accelerated charges *always* radiate classically (Maxwell equations)
- to form stable atoms the electrons have to be bound to the nuclei in some orbits implying accelerated motion

$\Rightarrow$ classical electrodynamics and the above = WAT

- so the simple experimental fact that there are stable atoms nukes classical physics (plus reasonable assumptions)

Photoelectric Effect

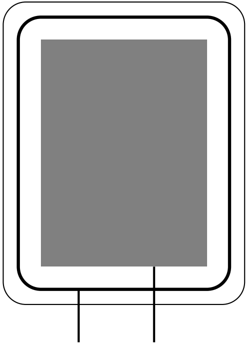

Figure: Schematic of a Phototube

- a current flows when light falls on a metal surface in a vacuum (phototube)
- when biasing the electrodes with a voltage U_B no current flows above some threshold voltage U_T
- the threshold voltage is proportional to the wavelength λ of the light
- for different metals there are different threshold wavelengths, below which no current flows for $U_B = 0$

Spectral Lines of Atoms – Experimental Setup

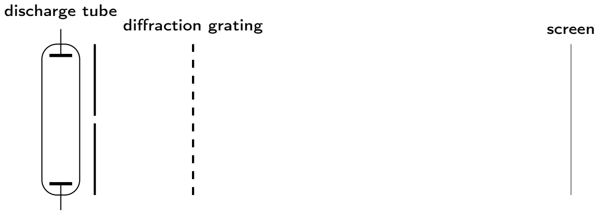

Figure: Schematic of a Discharge Tube and Spectrograph

- discrete emission lines – together with the photon hypothesis: discrete energies!
- characteristic spectra for each atom species
- absorption lines complementary to the emission lines

Davisson-Germer Experiment

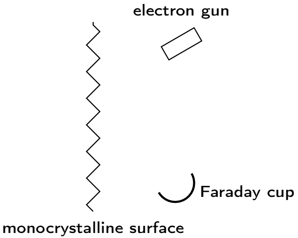

Figure: Schematic: Davisson-Germer Experiment

- the electrons show a diffraction pattern (that can be seen by moving the Faraday cup around)
- we can determing the wavelength of the matter wave from the diffraction pattern (and the lattice parameters of the crystal)
- this confirms the de Broglie relation

Radioactivity and Experiments with Single Particles

- radioactivity is random – you can't predict when the next decay will happen – this hints at the intrinsic randomness of subatomic physics
- we can do interference experiments with single particles, to do so we need a set of sensitive detectors
- *at most one* of a set of such sensors detects the electron or photon
- while the particle is extended in transit, it will be forced to a sharp measurement result on detection!
- if we do a double slit interference experiment and *detect* which slit the particle went through, then the interference pattern vanishes!
- if we do the above and then discard the which-way-information in a coherent manner there will again be interference (quantum eraser)

Crash Course: Complex Numbers

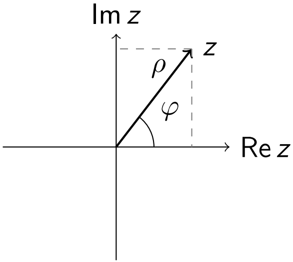

Figure: Complex Plane

- $\mathbb{C} = \{a + bi | a, b \in \mathbb{R}\}$, $i^2 = -1$, usual rules of calculation
- can be thought of as *phasors* in the complex plane
- polar representation: $z = \rho\big(\cos(\varphi) + i\sin(\varphi)\big) = \rho e^{i\varphi}$
- addition: component wise
- multiplication: $z_1 z_2 = \rho_1\rho_2 e^{i(\varphi_1+\varphi_2)}$ – turning angle plus length
- multiplication in Cartesian components $(a + bi)(c + di) = (ac - bd) + i(ad + cb)$
- complex conjugation $(a + bi)^* = a - bi$, modulus $|z| = \sqrt{z^* z}$

complex numbers make everything cool ($e^{ix} = \cos(x) + i\sin(x)$, fundamental theorem of algebra, function theory, etc.)

Crash Course: Vector Spaces

- vectors $x, y \in V$, scalars $\alpha, \beta \in S$ (a field, here only $\mathbb{C}$ and $\mathbb{R}$)
- null vector $\mathbf{0}$
- operations: addition of vectors $x + y \in V$, additive inverse of a vector $-x \in V$, $x + (-x) = 0$, multiplication by a scalar $\alpha x \in V$
- $\alpha(x + y) = \alpha x + \alpha y$, $(\alpha + \beta)x = \alpha x + \beta y$
- $\alpha(\beta x) = (\alpha\beta)x$
- $1x = x$

TL;DR: a vector space is a set of objects which can be added and which can be multiplied by scalars (real or complex numbers) in a compatible way

Crash Course: L^2 Space (and Analogy to Finite Dimensional Vector Spaces)

- vector space of square integrable functions (insert maths disclaimer here)

$$\|f\|^2 = \int dx\ |f(x)|^2 < \infty \qquad |\boldsymbol{x}|^2 = \sum_i x_i^2 < \infty \text{ (trivial here)}$$

- the norm $\|x\| := \sqrt{(x,x)}$ is induced by a scalar product $(\cdot,\cdot)$

$$(f,g) = \int dx\, f^*(x) g(x) \qquad \langle \boldsymbol{x}, \boldsymbol{y} \rangle = \sum_i x_i^* y_i$$

$\Rightarrow$ Hilbert space (= complete scalar-product space)

Nice surprise: almost everything works like in the finite dimensional case[1]

[1] mathematicians will deny this, but it usually just works with the physicists careful carelessness

Modelling the Wave-like Behaviour of Particles

- the Davisson-Germer experiments (1920s) show diffraction of electrons on a monocrystalline nickel surface – wave-like behaviour
- de Broglie hypothesis: particles have the wavelength $\lambda = h/p$
- idea: complex wave function $\psi(\boldsymbol{r}) = \rho(\boldsymbol{r})e^{i\varphi(\boldsymbol{r})}$ describing the quantum state of *a single particle*
  - $|\psi(\boldsymbol{r})|^2 = \psi(\boldsymbol{r})\psi^*(\boldsymbol{r})$ describes the probability of measuring the particle at $\boldsymbol{r}$
  - the phase is not directly measurable, but makes interference possible

$$|\psi_1 + \psi_2|^2 = |\psi_1|^2 + |\psi_2|^2 + 2\mathrm{Re}\,\psi_1^*(\boldsymbol{r})\psi_2(\boldsymbol{r})$$

- my stance: denounce the wave-particle dualism – quantum particles are *quantum* neither wave nor particle

States of Definite Momentum

- follow the de Broglie hypothesis $\boldsymbol{p} = h\boldsymbol{k}$ (k is the wavenumber, $k = 2\pi/\lambda$)

$$\psi_{\boldsymbol{k}}(\boldsymbol{r}) = \frac{1}{2\pi} e^{i\boldsymbol{k}\cdot\boldsymbol{r}}$$

- occupies the whole space (!)
- (mathematical catch: this state does not belong to the Hilbert space of valid normalizable states, neither do the states of definite position)
- we can write any state as superposition of $\psi_k(\boldsymbol{r})$ (Fourier transform)
- conclusion: by Fourier transformation[2] the state $\psi(\boldsymbol{r})$ can be written in terms of $\tilde{\psi}(\boldsymbol{k})$ – both contain all information about the system

[2]this implies the uncertainty relation $\Delta x \cdot \Delta k \geq \frac{1}{2}$; the uncertainty relation is *unimportant* in the grand scheme of things

Operators

- observables in quantum mechanics are *linear operators* (“matrices”) on the state space
- measuring an observable results in *one* of its eigenvalues
- if the system is in an eigenstate of the operator the measurement result is certain
- non-commuting operators have eigenstates that are not common
- momentum operator: $p = -i\hbar\nabla$, positions operator: x
- observation: p and x do not commute ($[A, B] = AB - BA$ is called commutator and quantifies the failure to commute, A and B commute iff $[A, B] = 0$)

$$px\psi = -i\hbar\psi - i\hbar x\partial_x\psi = xp\psi - i\hbar\psi =: \big(xp + [p, x]\big)\psi$$
$$[p, x] = -i\hbar$$

More on Operators

- linear: $O(\alpha x + \beta y) = \alpha O x + \beta O y$
- multiplication of operators is defined by consecutive application $(OU)x = O(Ux)$
- a linear operator is defined by its action on any set of vectors spanning the vector space
- inverse operator: some operators have an inverse operator O^{-1} such that $OO^{-1} = \mathrm{id}$
- every operator has an adjoint defined by $(\varphi, A\psi) = (A^\dagger\varphi, \psi)$ for all ψ, φ
- there are commonly defined classes of operators

Hermitian $A = A^\dagger$ (in terms of the scalar product $(\psi, A\varphi) = (A\psi, \varphi)$)

anti-Hermitian $A = -A^\dagger$

unitary $U^\dagger = U^{-1}$

projectors $P^2 = P$

Expectation Values

- the expectation value of an operator is defined as

$$\langle O \rangle = \int d^3r\, \psi^*(\mathbf{r}) O \psi(\mathbf{r}) = (\psi, O\psi)$$

- the expectation values of Hermitian operators are real

$$\langle O \rangle = (\psi, O\psi) = (O\psi, \psi) = (\psi, O\psi)^*$$

- can be shown to agree with the expectation value of the quantity represented by the operator when measuring it

Crash Course: Eigenvalue Problems

- important question: which vectors are just scaled by a linear operator: $A\psi = \lambda\psi$
- remember linear algebra – this is diagonalizing matrices
- if such a ψ exists it is called eigenvector and λ is the corresponding eigenvalue
- the dimension of the space spanned by the eigenvectors can be larger than one (degeneracy), in this case we can always choose an orthonormal base in the eigenspace
- we write $\psi_{\lambda n}$ for the normalized n^{th} basis vector in the eigenspace corresponding to λ
- Hermitian operators have real eigenvalues ($H = H^\dagger$ means $\lambda = \lambda^*$ for the diagonal, so for the eigenvalues in the eigenbasis)

Crash Course: Eigenvalue Problems (cont.)

- spectral theorem[3]: all Hermitian operators have a complete (= spanning the whole vector space) system of eigenvectors, for any vector φ we have

$$\varphi = \sum (\psi_{\lambda n}, \varphi)\psi_{\lambda n}$$

- eigenvectors φ, ψ of a Hermitian operator A for difference eigenvalues λ, κ are orthogonal, proof:
$\kappa^*(\psi,\varphi) = (\varphi, A\psi)^* = (\psi, A\varphi) = \lambda(\psi,\varphi) \Rightarrow (\kappa^* - \lambda)(\psi,\varphi) = 0$

[3] this is a lie if the dimensions are not finite, but the differences are mathematical nitpicking

Equation of Motion – Requirements

(R1) a sharp (Gaussian) wave packet constructed from momentum states with similar momenta should follow the classical equation of motion in the limit $\hbar \to 0$

(R2) the time evolution must conserve the total probability of finding the particle

(R3) the equation should be first-order in time (otherwise the wave-function contains insufficient information for the time development)

(R4) the equation should be linear to allow interference effects[4]

from the requirements $(R3)$ and $(R4)$ we can write (with a linear operator H)

$$i\hbar\partial_t\psi(\boldsymbol{r}, t) = H\psi(\boldsymbol{r}, t)$$

[4] there was some work on non-linear quantum mechanics, but it is non-standard and not supported by experimental evidence

Equation of Motion – Conservation of Probability

- require conservation of probability ($R2$) for all states

$$0 = \partial_t \int d^3r\, \psi^*(\boldsymbol{r},t)\psi(\boldsymbol{r},t) = -\frac{i}{\hbar}\int d^3r \Big(\big(-H^*\psi^*(\boldsymbol{r},t)\big)\psi(\boldsymbol{r},t) + \psi^*(\boldsymbol{r},t)H\psi(\boldsymbol{r},t)\Big)$$
$$= -\frac{i}{\hbar}\int d^3r \Big(-\psi^*(\boldsymbol{r},t)H^\dagger\psi(\boldsymbol{r},t) + \psi^*(\boldsymbol{r},t)H\psi(\boldsymbol{r},t)\Big)$$

- this implies that $H = H^\dagger$ for conservation of probability (mathematical disclaimer: there are intricacies with the adjoint of operators)
- actually there is even *local* conservation of probability for local Hamiltonians, encoded in the continuity equation: $\partial_t \rho + \nabla \cdot \boldsymbol{j} = 0$

The Hamiltonian

- begin with the classical Hamiltonian $H = \frac{\boldsymbol{p}^2}{2m} + V(\boldsymbol{r})$
- replace p and x by their corresponding operators (sometimes called: correspondence principle – in the classical limit we must retrieve the classical equations)
- with a magnetic field we get: $H = \frac{\left(\boldsymbol{p} - \boldsymbol{A}(\boldsymbol{r})\right)^2}{2m} + V(\boldsymbol{r})$

Consistency with Newtonian Mechanics

- the new theory must explain *all* previous experimental evidence
- in some limiting case quantum mechanics has to reproduce Newtonian mechanics
- Ehrenfest theorem
  - in general

$$d_t \left\langle \hat{O} \right\rangle = d_t(\psi, O\psi) = \frac{i}{\hbar} \left\langle [\hat{H}, \hat{O}] \right\rangle + \langle \partial_t O \rangle$$

  - for position and momentum with the Schrödinger Hamiltonian $H = \frac{p^2}{2m} + V(\boldsymbol{r})$

$$\partial_t \langle \hat{\boldsymbol{p}} \rangle = -\left\langle \nabla \hat{V} \right\rangle$$

$$\partial_t \langle \hat{\boldsymbol{r}} \rangle = \langle \hat{\boldsymbol{p}} \rangle / m$$

  - can almost be brought to the form of the Newtonian equation of motion

$$m\partial_t^2 \langle \hat{\boldsymbol{r}} \rangle = -\left\langle \nabla \hat{V} \right\rangle = \left\langle \hat{F} \right\rangle$$

Solving the Schrödinger Equation

- ansatz: separation of variables – $\Psi(x,t) = \Phi(t)\psi(x)$

$$i\hbar\dot{\Phi}(t)\psi(x) = \Phi(t)H\psi(x),$$

$$i\hbar\frac{\dot{\Phi}(t)}{\Phi(t)} = \frac{H\psi(x)}{\psi(x)} = \text{const} := E.$$

- this gives the two equations[5]

$$\dot{\Phi}(t) = -\frac{iE}{\hbar}\Phi(t), \qquad H\psi_n(x) = E_n\psi_n(x).$$

- general solution of the time-dependent Schrödinger equation

$$\Psi(x,t) = \sum_n e^{-iE_n t/\hbar}\big(\psi_n, \Psi(\cdot, 0)\big)\psi_n(x).$$

[5] the second one is an eigenvalue problem

Measurement or How I measured my cat and now it's dead

- given a system in state ψ and an operator A
  - the possible outcomes for A are given by its eigenvalues a_n
  - the probability of measuring a_n is $\langle\psi|P_n|\psi\rangle$, where P_n projects to the eigenspace corresponding to a_n
  - (idealized measurement) after having measured A the state is projected to the eigenspace of the measured value (and normalized)
- this is weird, indeterministic and apparently non-*unitary* and completely different from the nice deterministic equation for ψ (possible solution: decoherence with the environment)

TL;DR:

quantum measurement is probabilistic and
inherently changes the system's state

Crash Course: Tensor Product

- there are different products of (vector) spaces
- fundamental: Cartesian product $X \times Y$, the set-of tuples of elements from X and Y
- clever: the tensor product $X \otimes Y$ over vector spaces over the same field preserves the full vector space structure[6]
  - compatible with multiplication by scalars $(\alpha x) \otimes y = x \otimes (\alpha y) =: \alpha(x \otimes y)$
  - compatible with addition in the constituent vector spaces $(x + y) \otimes z = (x \otimes z) + (y \otimes z)$
  - for vectors that also defined a multiplication (e.g. linear operators) $(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$

[6] formal construction by factoring the Cartesian product by an equivalence relation

Multiple Particles

- the Hilbert space for a compound system $\mathcal{H} = \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_n$ (tensor product)
- one-particle operator acting on the n^{th} particle: $\hat{O} = \mathbf{1} \otimes \cdots \otimes \hat{O}_1 \otimes \cdots \otimes \mathbf{1}$
- two-particle operator: $\hat{O} = \hat{O}_1 \otimes \hat{O}_2$
- Caveat: Identical Particles
  - experimental result: there are two kinds of particles – bosons and fermions
  - different behaviour as $T \to 0$: additional pressure or lowered pressure compared to the hypothetical ideal gas
  - using the formula above leads to paradoxical results
  - identical fermions have anti-symmetrized, identical bosons have symmetrized wave-functions
  - $\mathcal{H} = H_1^{\otimes n S_\pm}$

Summary: The Axioms of Quantum Mechanics

(A1) All information about a quantum system is carried in a L^2 function $\psi : R \to \mathbb{C}$.

(A2) Each observable is given by a Hermitian operator A.

(A3) The possible measurement values are given by the eigenvalues von A.

(A4) The eigenvectors must be orthonormalized.

(A5) The probability for of measuring a is given by (where ν is the degeneracy index).

$$P(a,t) = \sum_{\nu} \left| \int dx \, \psi^*_{a\nu}(x)\psi(x,t) \right|^2 .$$

(A6) The equation of motion of ψ is the Schrödinger equations

$$i\hbar\partial_t\psi = H\psi$$

(A7) Pauli principle (where the two signs are for bosons resp. fermions):

$$\psi(1,2,\ldots) = \pm\psi(2,1,\ldots)$$

How not to Be Afraid of the Dirac (or Bra-Ket-) Notation

- the wave-function $\psi(\boldsymbol{r})$ can be thought of as a the position-basis components of an abstract wave-function vector $|\psi\rangle$ (read: ket psi)
- $\langle\psi|\cdots = \int d^3r\,\psi^*(\boldsymbol{r})\cdots$ (read: bra psi) is the adjoint linear functional of $|\psi\rangle$ so that $\langle\psi|\varphi\rangle = \int d^3r\,\psi^*(\boldsymbol{r})\varphi(\boldsymbol{r})$ is the L^2 inner product[7]
- $|\psi\rangle = \int d^3r\,\psi(\boldsymbol{r})\,|\boldsymbol{r}\rangle$ just like $\boldsymbol{a} = a_x\boldsymbol{e}_x + a_y\boldsymbol{e}_y + a_z\boldsymbol{e}_z$
- now we can develop the coefficients in different bases
- especially common (since it makes the time evolution easy): the energy eigenstates $|\psi\rangle = \sum_n c_n\,|n\rangle$, $H\,|n\rangle = E_n\,|n\rangle$
- matrix elements of operators:

$$O\,|\psi\rangle = \sum_{nm} |n\rangle\,\langle n|O|m\rangle\,\langle m|\psi\rangle = |n\rangle\,O_{nm}\psi_m$$

[7] mathematical pedants define states to be continuous linear functionals and thereby solve the position eigenstate problem.

A Quantum Eraser at Home

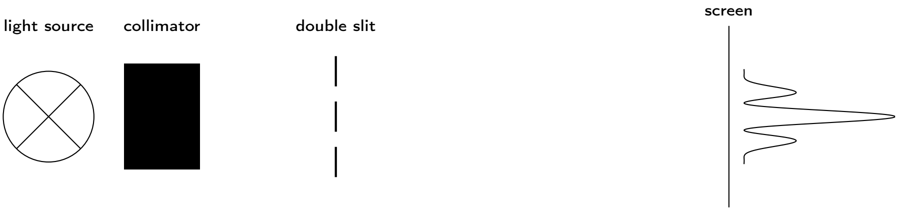

Figure: Setup

disclaimer: this can be explained classically as well, but the photon-wise quantum interpretation is totally valid (and the classical result can be explained in terms of it)

A Quantum Eraser at Home

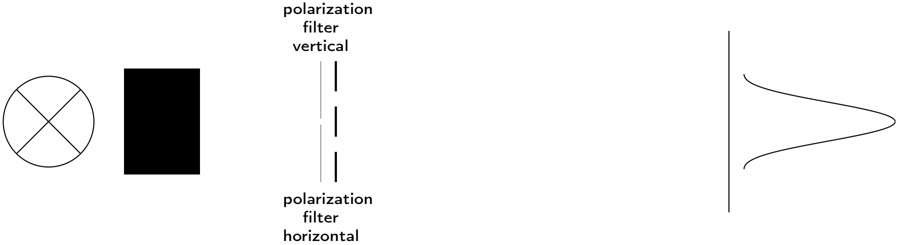

Figure: Setup

disclaimer: this can be explained classically as well, but the photon-wise quantum interpretation is totally valid (and the classical result can be explained in terms of it)

A Quantum Eraser at Home

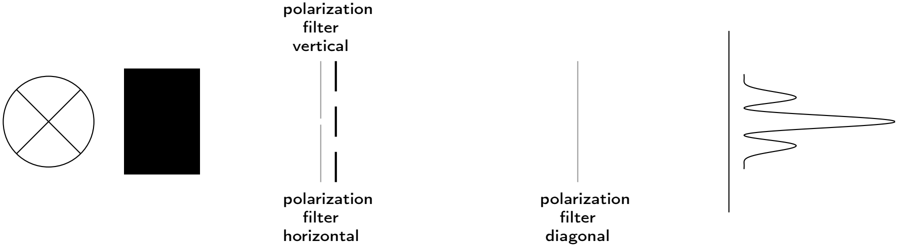

Figure: Setup

disclaimer: this can be explained classically as well, but the photon-wise quantum interpretation is totally valid (and the classical result can be explained in terms of it)

A Quantum Eraser at Home

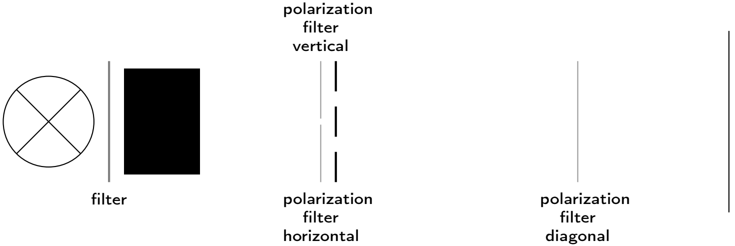

Figure: Setup

disclaimer: this can be explained classically as well, but the photon-wise quantum interpretation is totally valid (and the classical result can be explained in terms of it)

Harmonic Oscillator

$$H = \frac{p^2}{2m} + \frac{1}{2}m\omega^2x^2 = \hbar\omega\left(a^\dagger a + \frac{1}{2}\right), \quad a = \sqrt{\frac{\omega m}{2\hbar}}\,x + \frac{ip}{\sqrt{2\hbar\omega m}}, \quad [a, a^\dagger] = 1$$

- if there is a state such that $a\left|0\right\rangle = 0$ it will be an eigenstate of H with the energy $\frac{1}{2}\hbar\omega$
- induction: assume a state $\left|n\right\rangle$ with $a^\dagger a\left|n\right\rangle = n\left|n\right\rangle$, then we have $a^\dagger a a^\dagger\left|0\right\rangle = a^\dagger(a^\dagger a + 1)\left|n\right\rangle = (n+1)a^\dagger\left|n\right\rangle := (n+1)\mathcal{N}\left|n+1\right\rangle$
- normalization: $\left\langle n\right| a a^\dagger \left|n\right\rangle = \left|n+1\right\rangle \mathcal{N}^*\mathcal{N}\left|n+1\right\rangle$, so $\mathcal{N} = \sqrt{n}$
- therefore, there is an eigenstate for each natural number n with $a^\dagger a\left|n\right\rangle = n\left|n\right\rangle$ and energies $E_n = \hbar\omega\left(n + \frac{1}{2}\right)$

Harmonic Oscillator (cont.)

- the eigenvalue equation $a\,|0\rangle = 0$ in the position representation $\psi(x) = \langle x|0\rangle$ reads

$$\partial_x \psi(x) = -\frac{\omega m}{\hbar} x \psi(x)$$

- we guess a solution

$$\psi(x) = \mathcal{N} \exp\left(-\frac{\omega m x^2}{2\hbar}\right)$$

- since the differential equation is linear and homogeneous, this must be *the* solution
- normalization $|\mathcal{N}|^2 = \sqrt{\frac{\hbar}{\pi\omega m}}$ (from $\int dx\, e^{-x^2} = \sqrt{\pi}$ and substitution)
- all eigenfunctions of $a^\dagger a$ (and therefore H) can now be obtained by repeatedly applying $a^\dagger$

Tunnelling

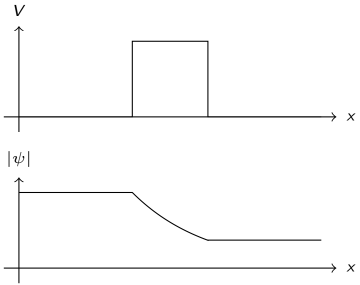

Figure: Scattering Eigenstate of a Tunnelling Problem

- in quantum mechanics particles can move through barriers of higher energy than their own
- the wave function decays exponentially in barriers but does not vanish immediately
- Myth: tunnelling makes a particle travel instantaneously from *a* to *b*
- Busted: states of particles are extended, only when measuring its position does a particle get a definite position (also: nothing disallows faster than light movement in non-relativistic quantum mechanics, the Schrödinger equation is not Lorentz invariant but Galilei invariant)

Entanglement

- consider a two-particle system, measurement of one of the particles projects the total state to the respective subspace
- now we have a state with two particles

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle |0\rangle + |1\rangle |1\rangle \right)$$

- measure the first particle, depending on the result of this measurement, the second particle will be *in the same state*
- this means that measurements of the two single particles in this state will be perfectly correlated!
- Einstein called this "spooky action at distance"

Entanglement – Remarks

- there are no *hidden variables* – the result is not intrinsically determined before measurement
- utterly weird but experimentally proven with so called Bell tests
- Myth: Entanglement allows to transfer information between two sites instantaneously
- Busted: no communication theorem: you can't exchange information faster than light via entangled particle pairs (but you can generate correlated noise)

Quantum Information

- a qubit is a quantum system with two states $|0\rangle$ and $|1\rangle$
- quantum computers
  - really bad for most computing tasks – binary-on-silicon folks don't fear for your job
  - can compute some things faster than a classical computer (e.g. factoring primes and similar problems – this would nuke our public-key crypto)
  - use linear superposition to construct a weird kind of parallelism using superpositions (we can compute something simultaneously for the 2^N basis states)
- quantum cryptography
  - solves the same problem as DH exchange
  - we can generate a shared key and can check that there was no eavesdropper
  - we can't detect a man in the middle without having a shared secret or PKI (quantum particles don't know who's on the other side)
  - essentially useless as there are classical quantum computer safe key-exchanges
  - commercial implementations: susceptible to side channel attacks

References

- L. D. Landau, E. M. Lifschitz, *Lehrbuch der Theoretischen Physik, Band III, Quantenmechanik*, (Verlag Harri Deutsch, ed. 9, 1992).
- H. Schulz, *Physik mit Bleistift*, (Verlag Harri Deutsch, ed. 6, 2006).
- F. Schwabl, *Quantenmechanik*, (Springer, ed. 7, 2007).