



量子光学

第一讲·绪论

从量子力学到量子信息科学

李梓民

中南大学物理学院

zimin.li@csu.edu.cn

2026年下半年

整数分解：寻找质因子

先看一个熟悉的数

$$21 = 3 \times 7$$

再试一个稍大的数

$$221 = 13 \times 17$$

如果换成250位的整数呢？

```
21403246502407449612644230728393335630086147151447
55017797754920881418023447140136643345519095804679
61099285187247091458768739626192155736304745477052
08051190564931066876915900197594056934574522305893
25976697471681738069364894699871578494975937497937
```

RSA-250分解挑战：寻找答案与验证答案

两个125位素数，相乘就能验证答案

$p =$

6413528947707158027879019
0170577389084825014742943
4472081168596320245323446
3023862359875266834770873
7661925585694639798853367

$q =$

3337202759497815655622601
0605355114227940760344767
5546667845209870238417292
1003708025744867329688187
7565718986258036932062711

2020年完成分解 · 约2700核年

P与NP：能高效验证，是否就能高效求解？

P：能在经典多项式时间内判定。

NP：肯定答案有可在经典多项式时间内核验的证明。

RSA：为什么整数分解关系到信息安全？

RSA是一种公钥密码：公钥可以公开，私钥需要保密。

公开的乘积

公钥中包含大整数 N 。

$$N = p \times q$$

保密的质因子

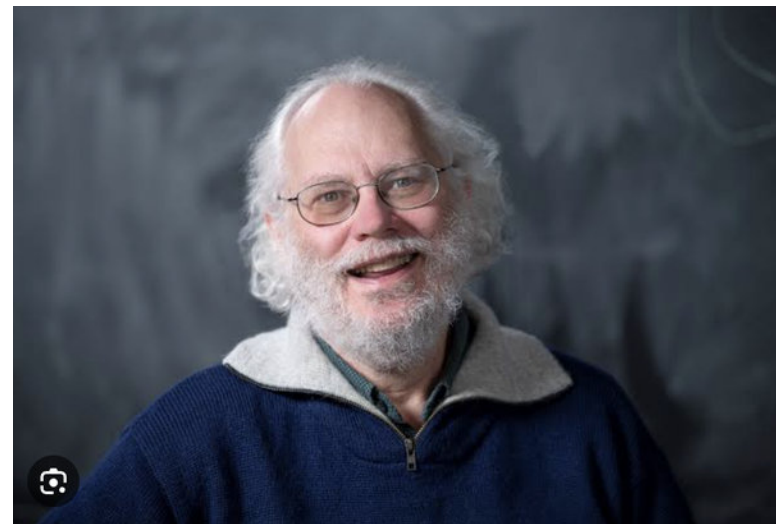
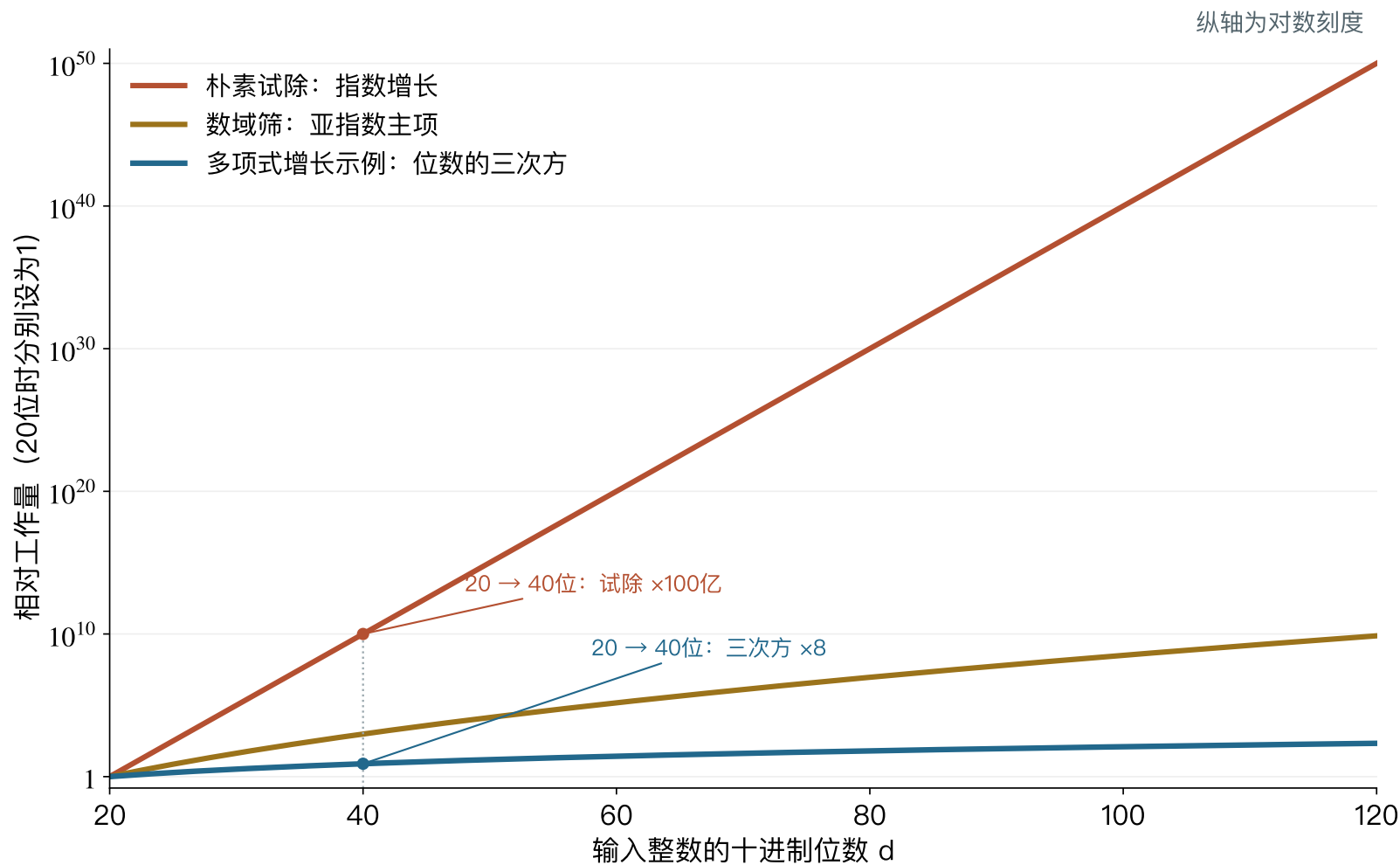
两个大素数 p 、 q
用于生成私钥。

知道它们，就能计算对应的私钥。

如果能高效分解大整数呢？

RSA赖以保护私钥的计算困难，就会受到挑战。

为什么计算会与量子物理有关？



彼得·肖尔

Peter Shor

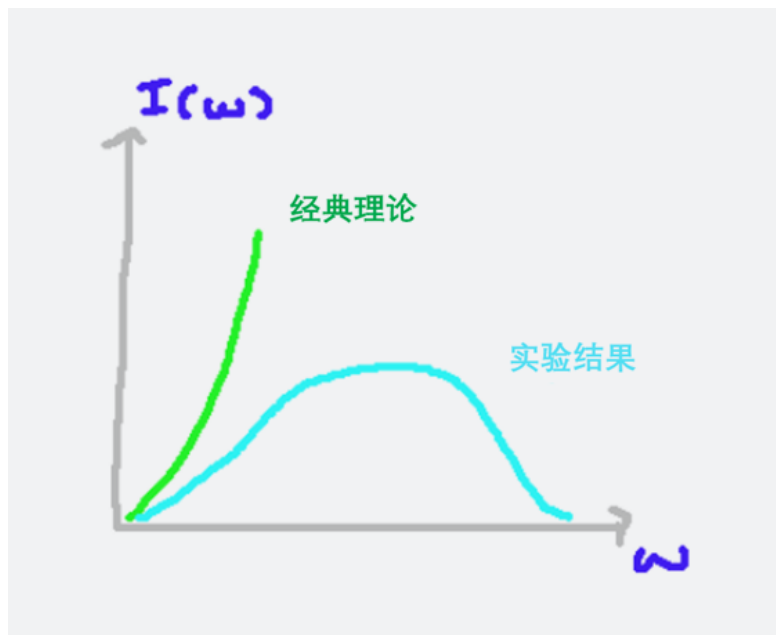
1994

试除：指数

数域筛：亚指数

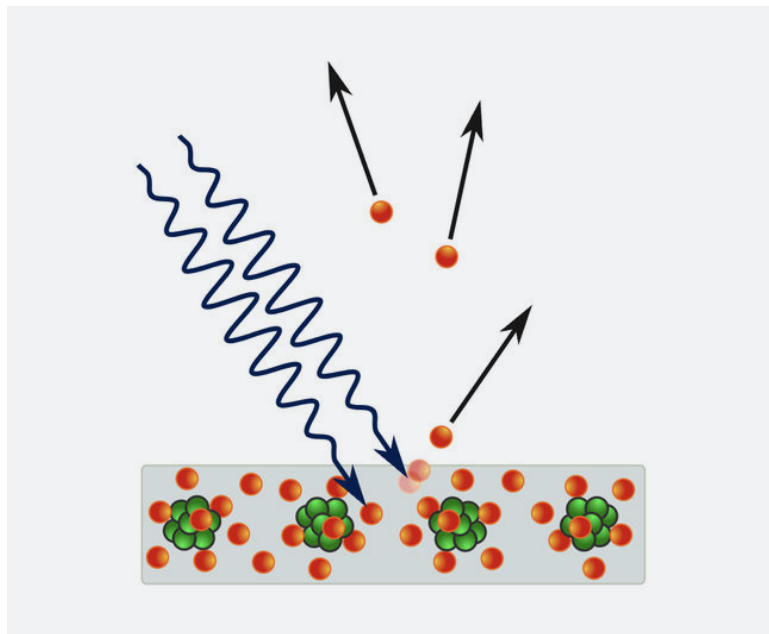
Shor：多项式

经典物理的三大困境



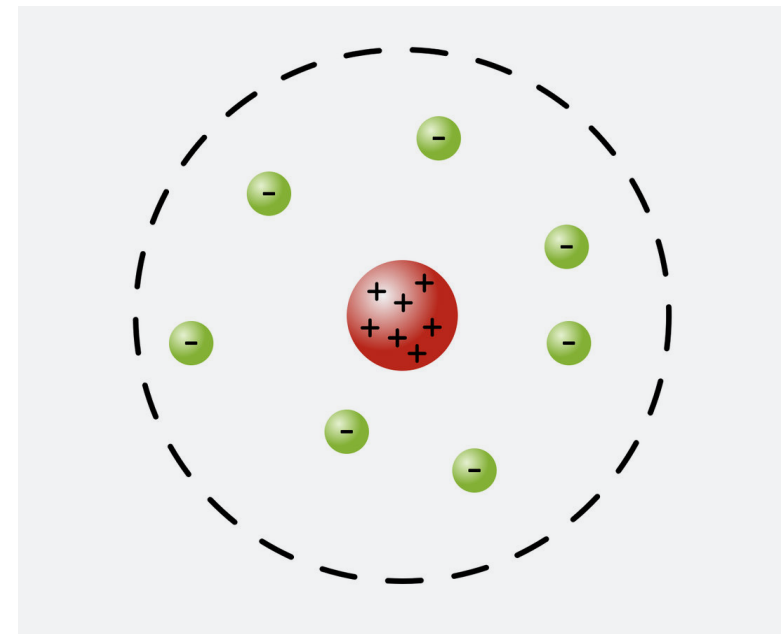
黑体辐射

光谱为什么是这样的？



光电效应

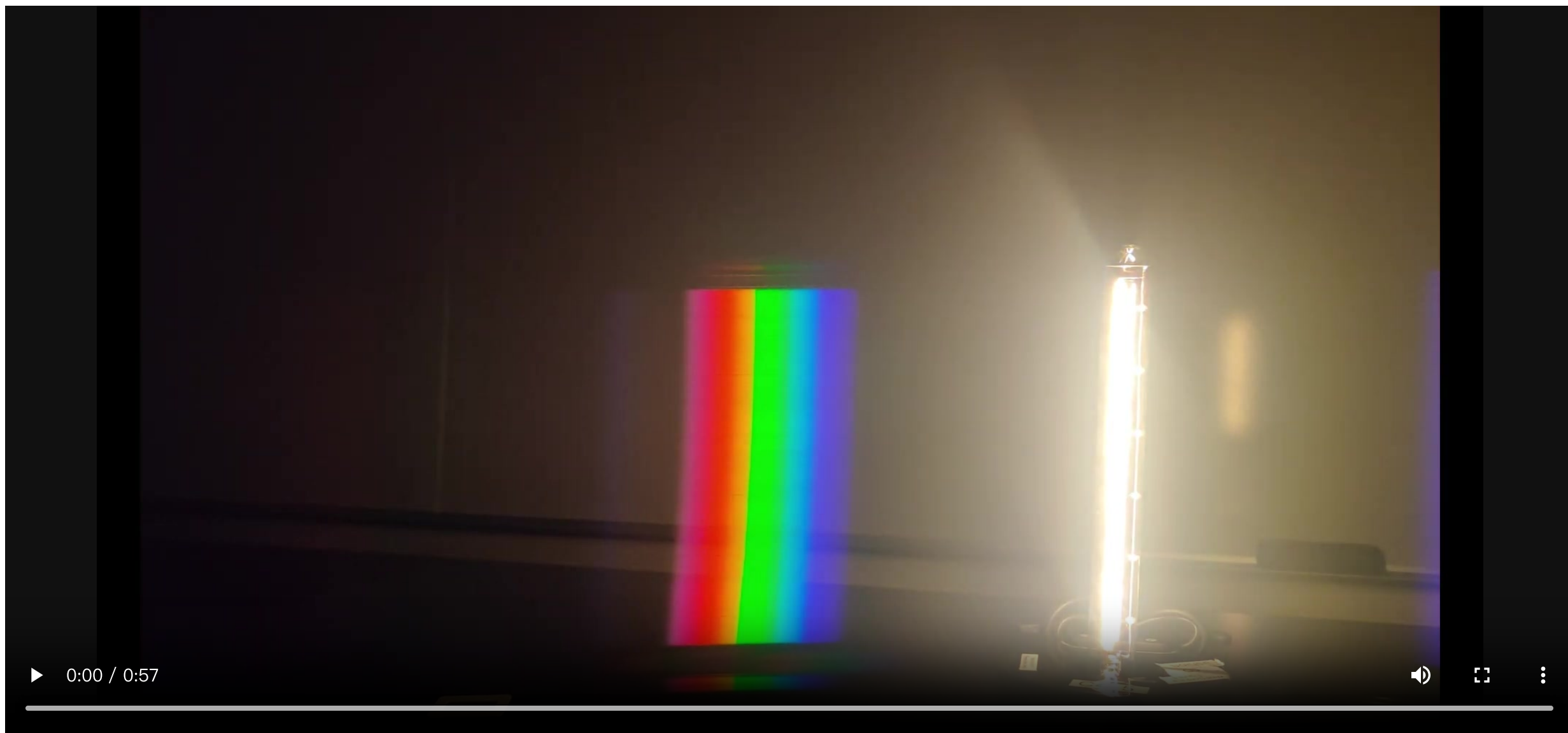
为什么颜色如此关键？



原子稳定性

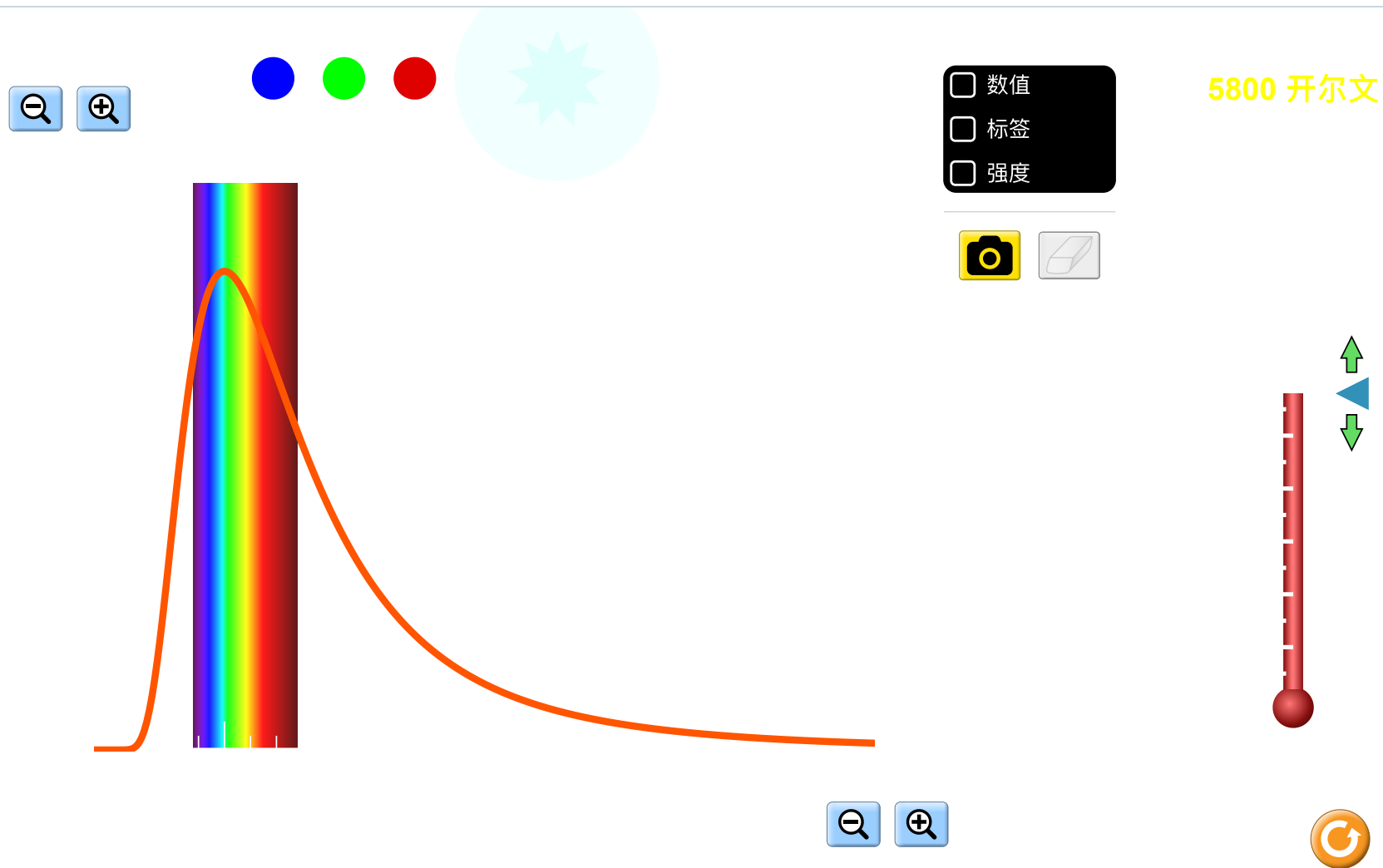
电子为什么不落入原子核？

黑体辐射：加热灯丝，观察光怎样变化



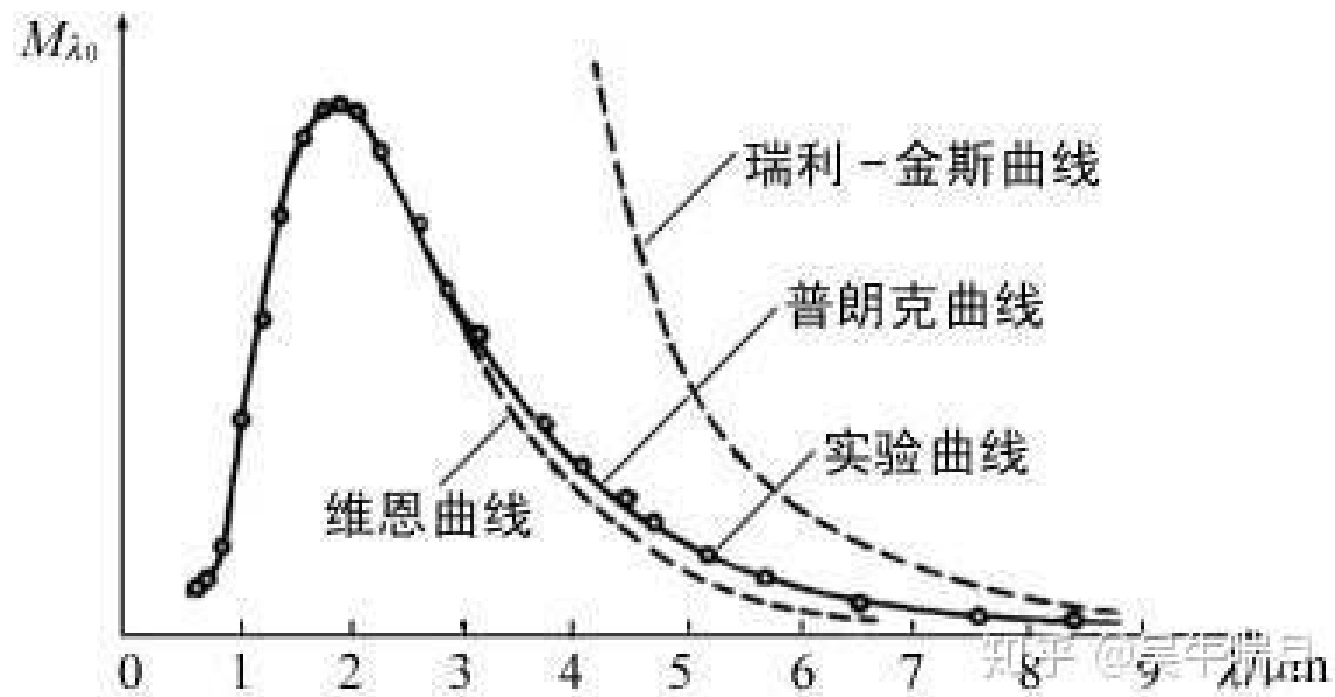
[原站观看](#)

黑体辐射：温度怎样改变光谱与颜色？



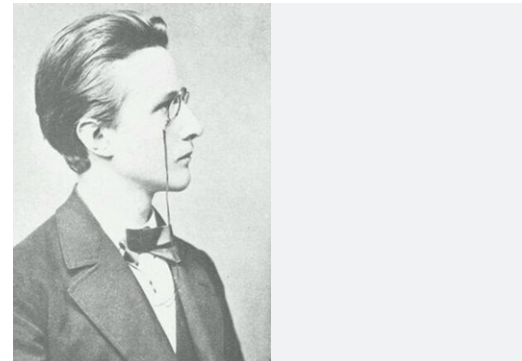
黑体辐射

黑体辐射：光谱两端的近似与普朗克的统一



短波端：Wien近似

长波端：Rayleigh-Jeans近似



马克斯·普朗克

Max Planck

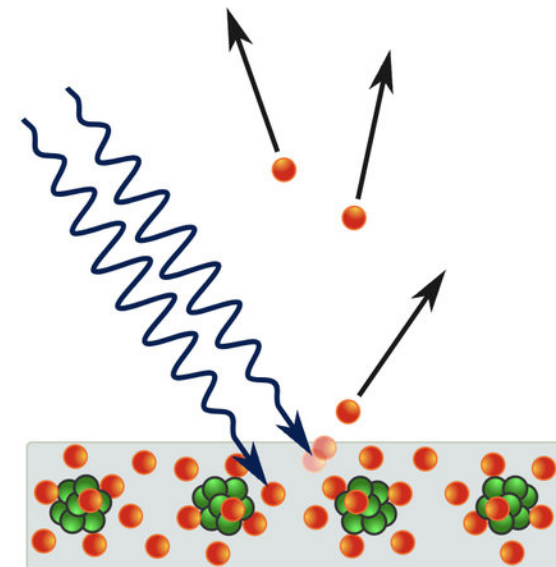
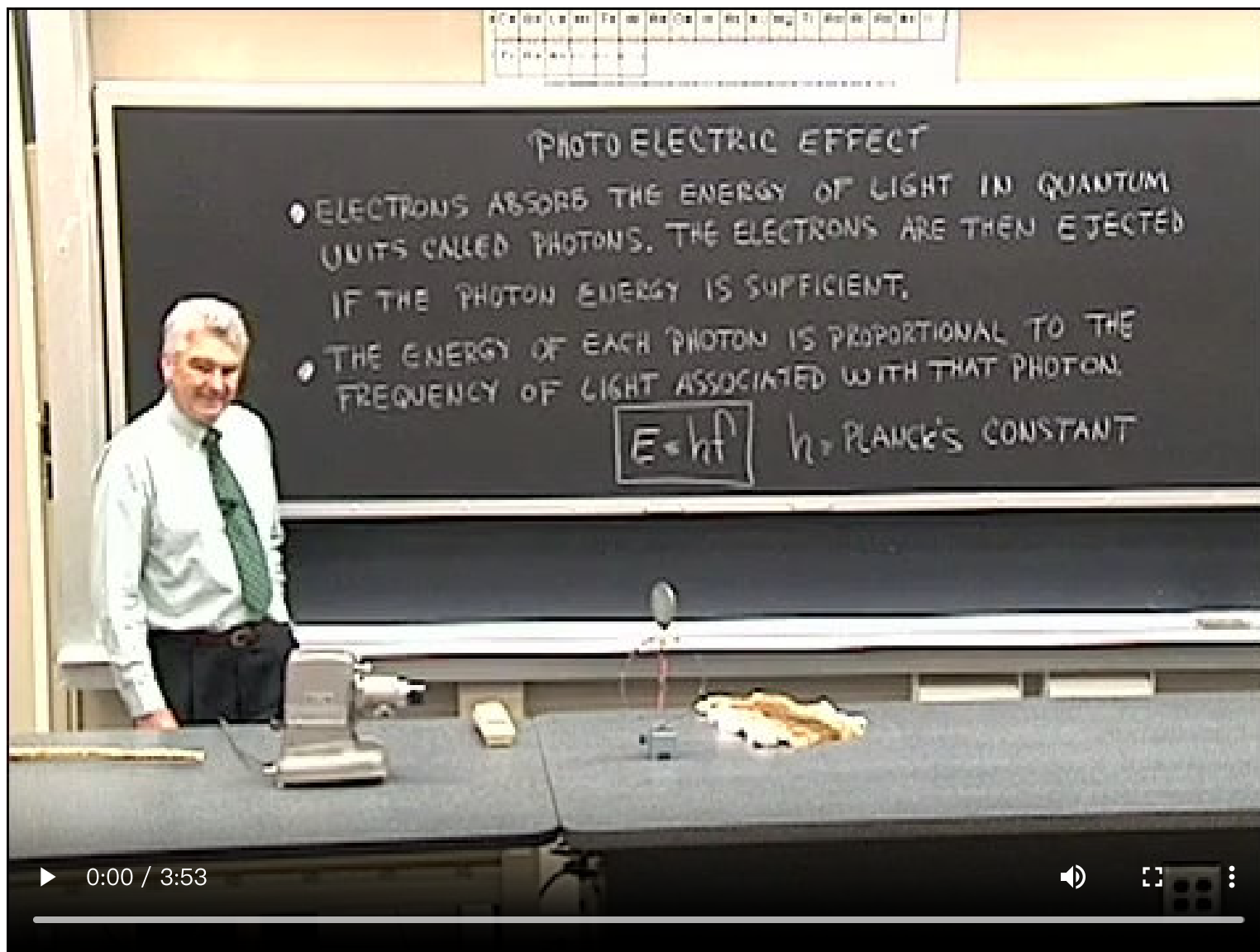
1900

能量交换一份一份地进行

$$\varepsilon = h\nu$$

同一个公式，
解释整条实验光谱。

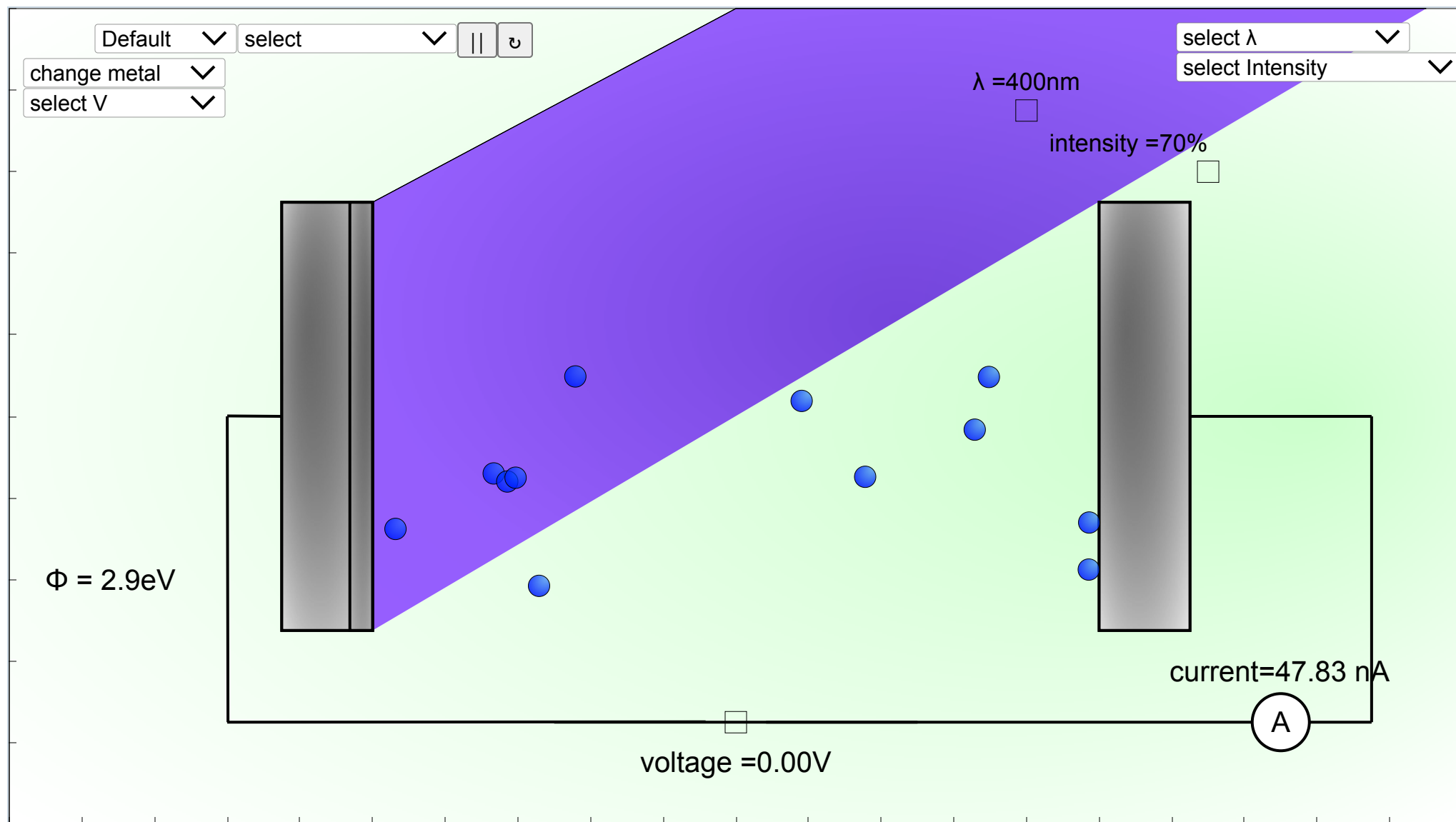
光电效应：光照使金属释放电子



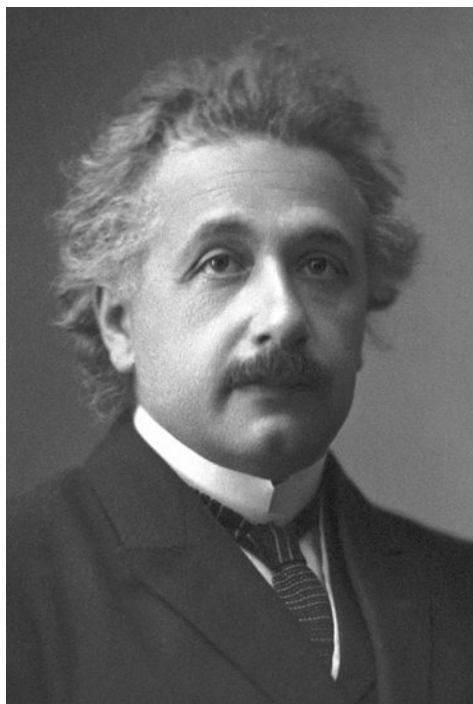
观察验电器指针

比较强可见光与紫外光照射下，指针的变化。

光电效应：分别改变颜色与亮度



爱因斯坦：光以一份一份的能量参与作用



阿尔伯特·爱因斯坦

Albert Einstein

1905

光量子假说 · 1905

每份光能量由频率决定。

$$E = h\nu$$

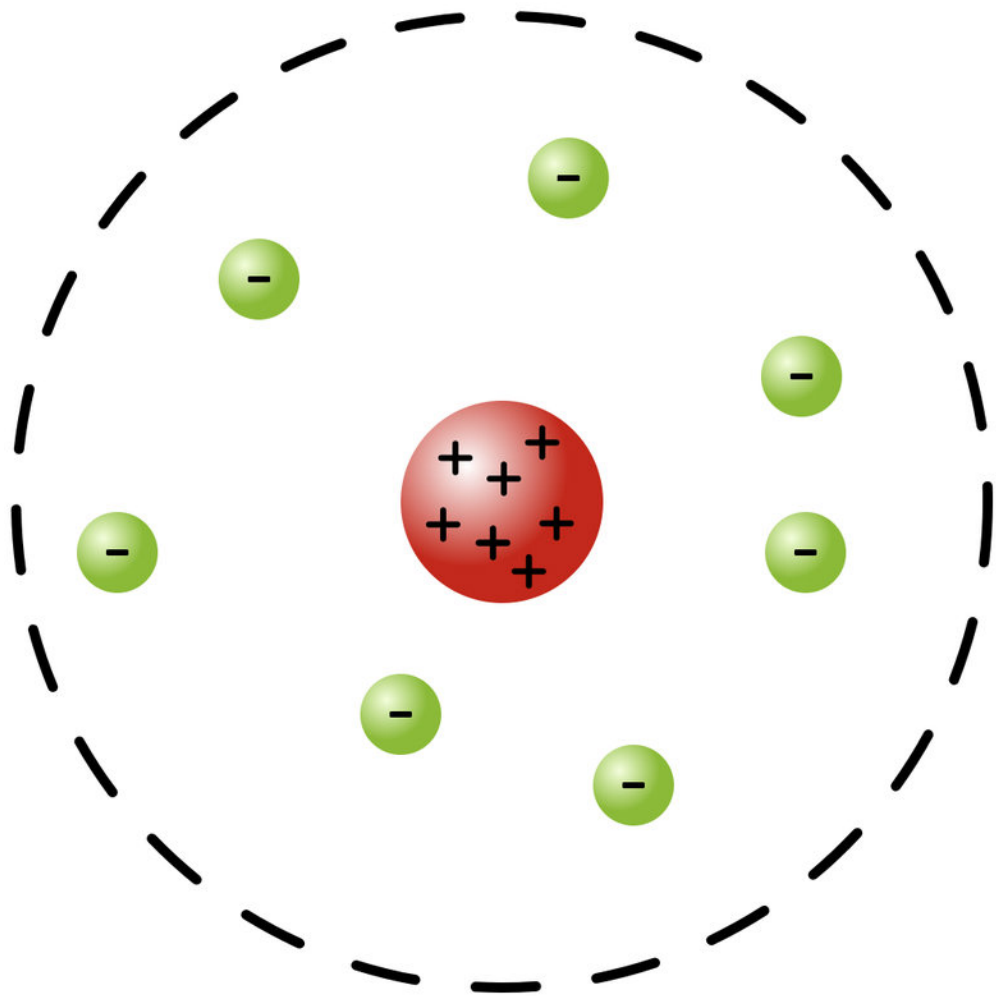
$$h\nu = W + K_{\max}$$

光子能量 = 逸出功 + 电子最大动能

频率够高，才有电子逸出；

固定频率加亮，电子事件增多。

原子为什么不会塌缩？



先尝试经典的绕核图像

电子在原子核周围转弯

带电粒子加速运动

→ 按经典电磁理论辐射能量

不断失去能量

→ 无法保持稳定的绕核运动

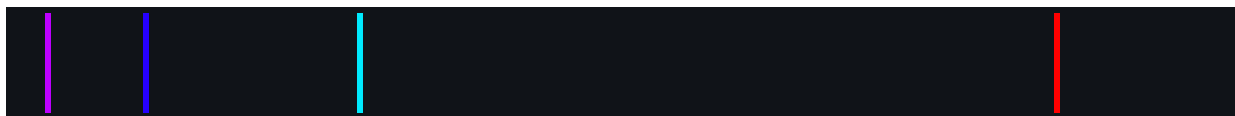
可是，我们身边的原子是稳定的。

原子光谱：为什么只出现特定颜色？

连续谱



氢



氦



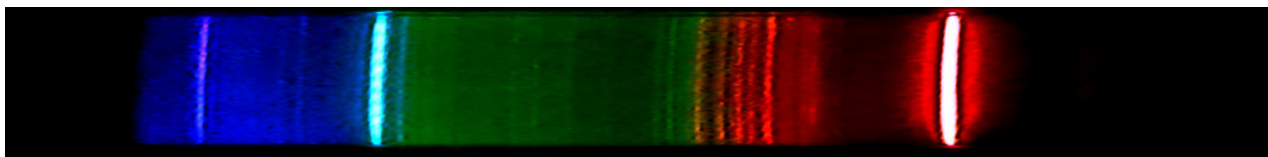
汞



400 500 600 700

波长 / nm

氢的实测光谱



连续光谱

颜色连续相接。

原子光谱

只在特定位置
出现亮线。

不同原子，
有不同的谱线组合。

为什么颜色不是任意的？

玻尔：原子只能处于某些能量状态

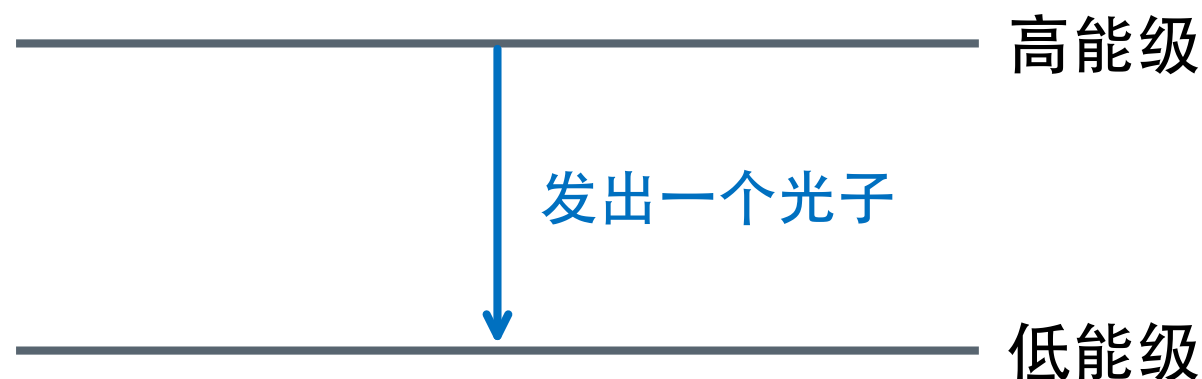


尼尔斯·玻尔

Niels Bohr

1913

定态：处于这些状态时，不持续辐射



跃迁：在两个能量状态之间改变

$$E_{\text{high}} - E_{\text{low}} = h\nu$$

能量差决定吸收或发出的光的颜色。

原子能级：一条谱线对应一个能量差

● 质子
● 电子
★ 光子

H

能量

电子能级

- $n = 6$
- $n = 5$
- $n = 4$
- $n = 3$
- $n = 2$
- $n = 1$

模型 ☒ 玻尔 ☐ 德布罗意 ☐ 薛定谔

● 快
● 正常
● 慢速

白色 单色

+ 光谱仪 (发射光子 / 纳米)

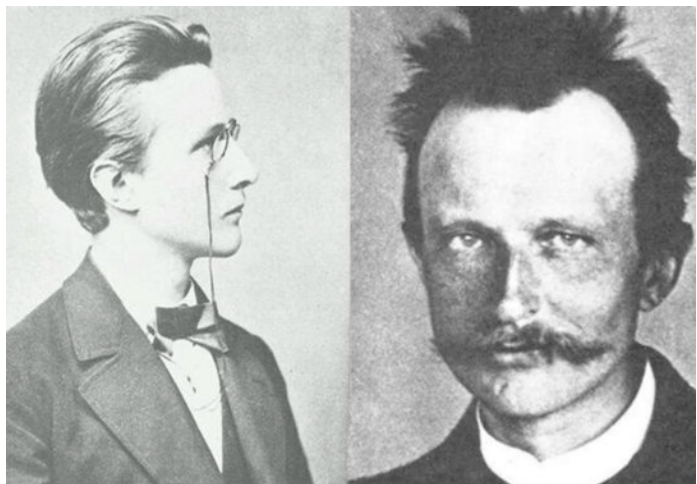
跃迁

选择玻尔模型

打开光源，
观察能级跃迁。

$$E_{\text{高}} - E_{\text{低}} = h\nu$$

三次突破：量子观念逐步形成

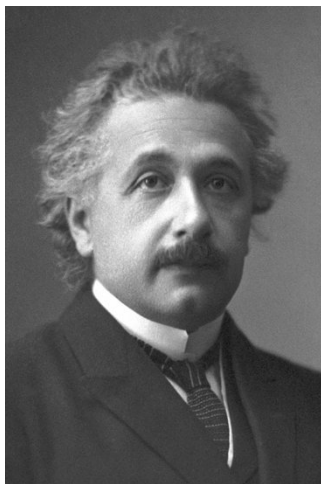


马克斯·普朗克

Max Planck

1900

能量交换的基本单位



阿尔伯特·爱因斯坦

Albert Einstein

1905

光量子解释光电效应



尼尔斯·玻尔

Niels Bohr

1913

定态与能级跃迁

这些成功的假设，能否来自一套统一理论？

德布罗意：物质也具有波动性

把波长与粒子的动量联系起来

$$\lambda = \frac{h}{p}$$

动量越大，波长越短。



路易·德布罗意

Louis de Broglie

1924

怎样检验这个假设？

让电子照射晶体，
观察是否出现衍射。

电子的波动性：从早期验证到单电子演示

1927 · 电子衍射

戴维孙—革末实验、汤姆孙的薄膜实验：
电子束照射晶体，呈现波的衍射特征。

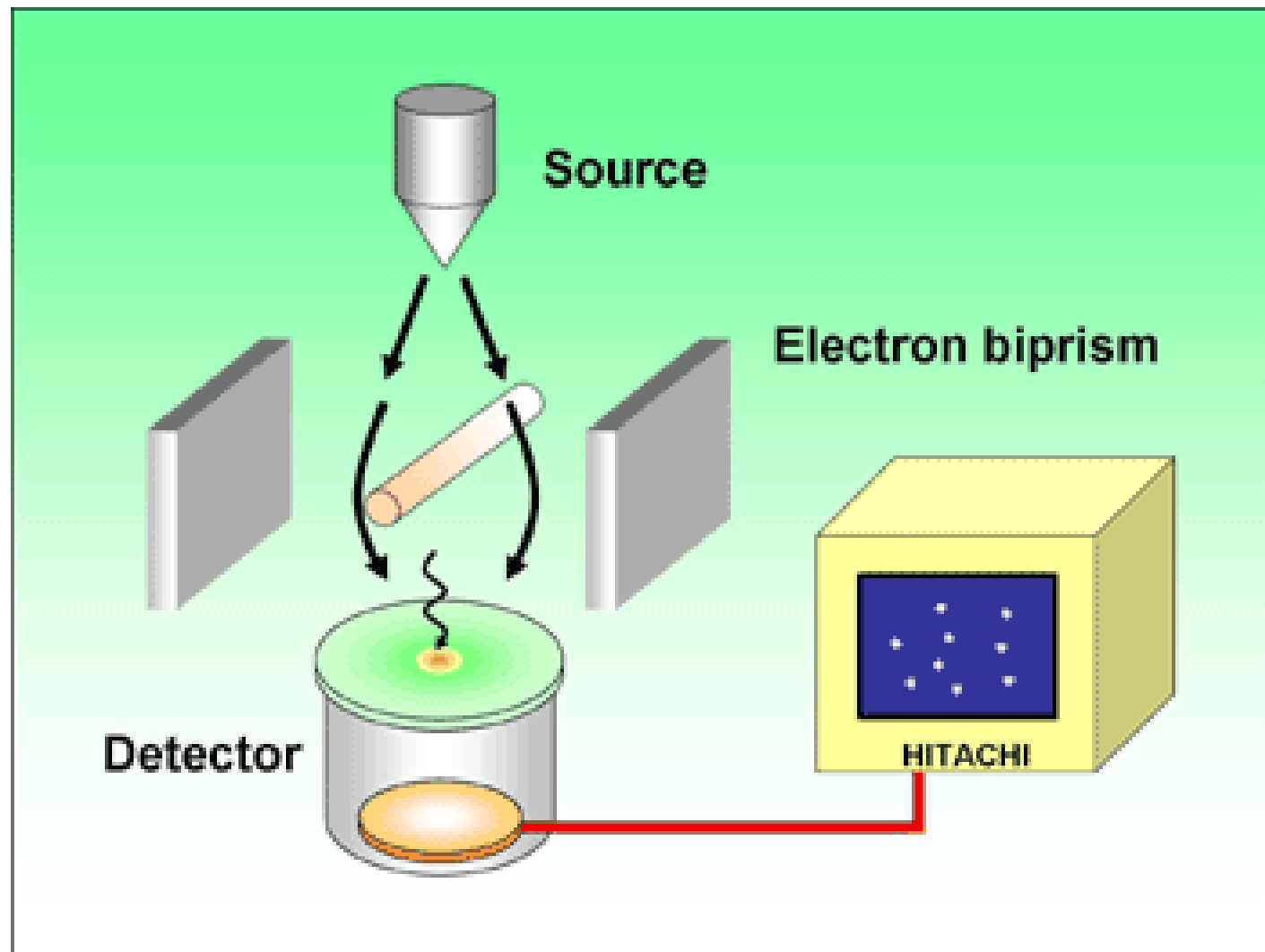
1929 · 德布罗意获诺贝尔物理学奖

物质波的预言已有电子衍射实验支持。

1989 · 单电子累积演示

接下来借助外村彰团队的实验，
看清“一次一个亮点，累积形成条纹”。

电子波的干涉：怎样观察到条纹？



外村彰

Akira Tonomura

1989

团队的单电子实验

- 电子源发射并加速电子。
- 细丝两侧的电子波在下游重叠。
- 探测器登记每次到达的位置。

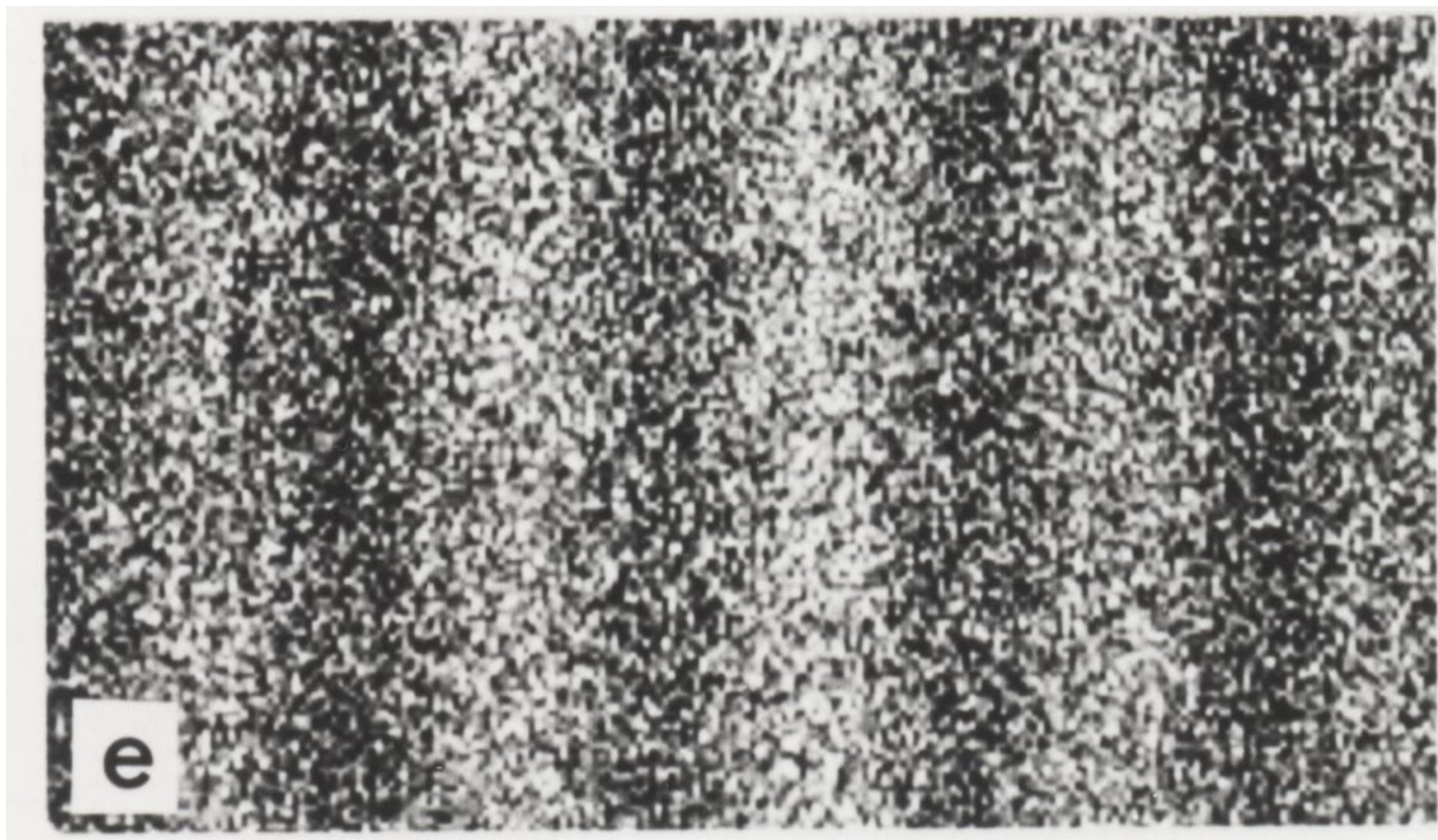
一次一个电子：从亮点到干涉条纹

相邻电子平均间隔

0.1 s

电子穿越装置的时间

10^{-8} s



记录逐渐增加 · 5 / 5

波粒二象性：从动画理解双缝干涉



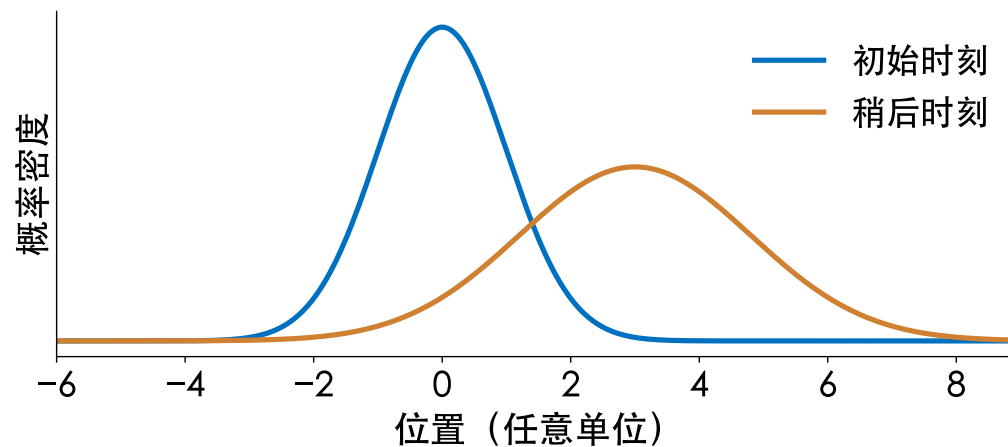
薛定谔：用方程描述物质波的演化



埃尔温·薛定谔

Erwin Schrödinger

1926



$$i\hbar \frac{\partial \psi}{\partial t} = \hat{H} \psi$$

ψ : 描述量子状态的波函数

$\hat{H}$: 描述系统能量与相互作用

已知初始状态，就能计算它怎样演化。

玻恩：波函数怎样联系实验结果？



马克斯·玻恩

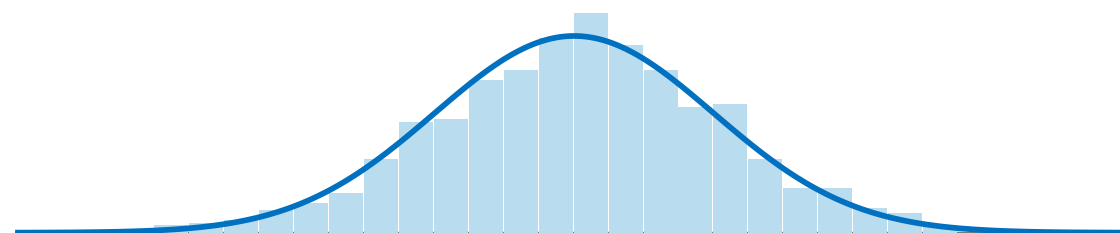
Max Born

1926

少量记录



累积记录



位置（任意单位）

一次探测：得到一个位置。

重复测量：位置分布呈现统计规律。

$$\rho(x) = |\psi(x)|^2$$

波函数模的平方，给出位置的概率密度。

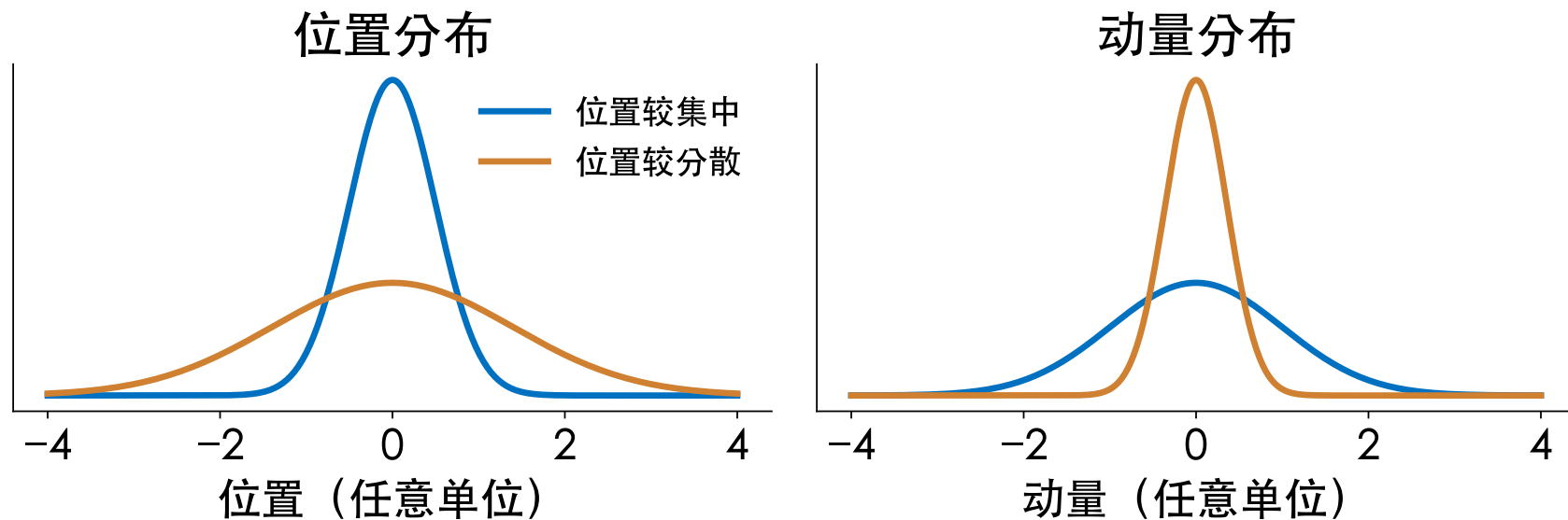
海森堡：位置与动量的共同限制



维尔纳·海森堡

Werner Heisenberg

1927



$$\Delta x \Delta p \geq \frac{\hbar}{2}$$

位置越集中，动量就越分散。

Δ 表示重复制备、测量得到的分布宽度。

从量子假设到量子力学

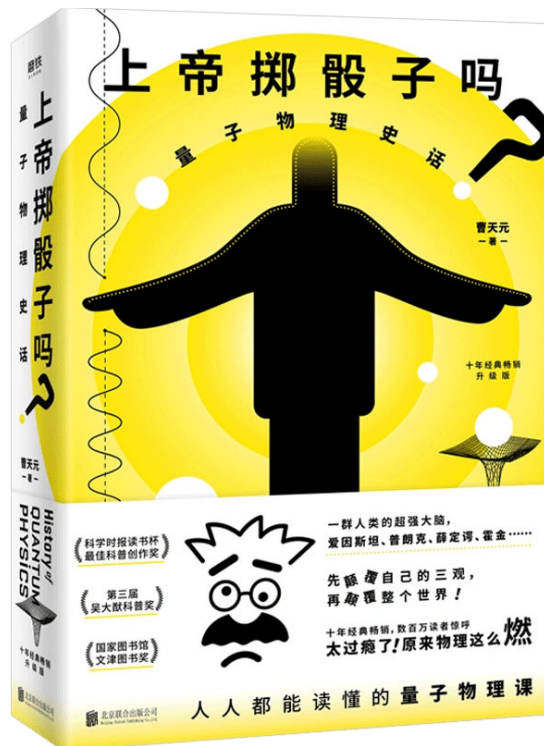
1900—1913 普朗克、爱因斯坦、玻尔：量子假设解释实验

1924 德布罗意：物质波

1925—1926 海森堡、薛定谔：建立量子力学的演化规律

1926—1927 玻恩、海森堡：概率解释与不确定性关系

历史背景：更多量子力学的故事



《上帝掷骰子吗？》

曹天元



《群星闪耀》 ——量子物理史话

张天蓉



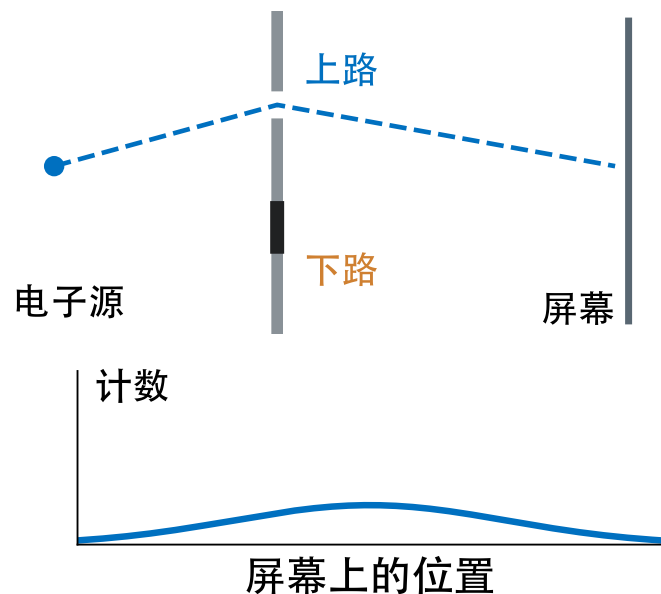
《奥本海默》

电影·2023

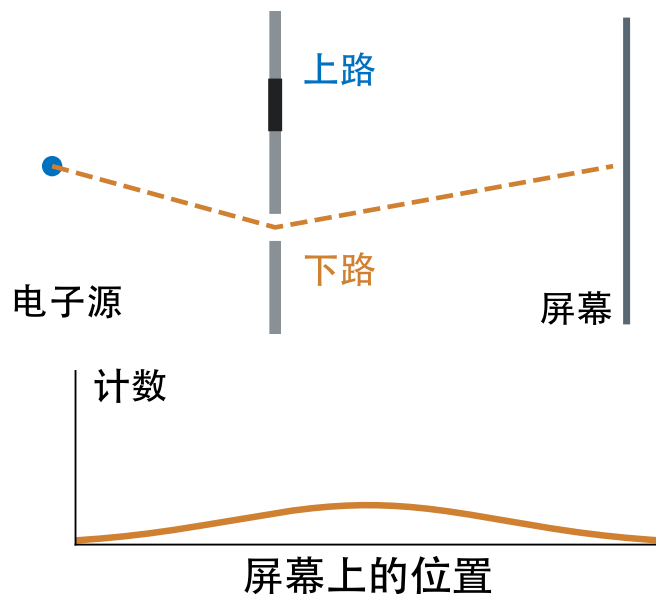
叠加态：先叠加概率幅，再计算概率

刚才看到了条纹：两路都开，为什么不是简单相加？

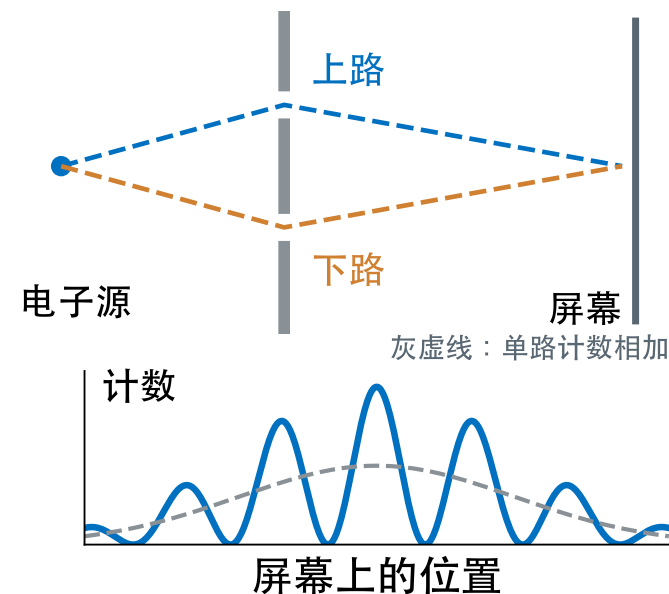
只开上路： ψ_1



只开下路： ψ_2



两路都开



$$\psi = \psi_1 + \psi_2$$

两路相干开放时，先叠加概率幅，再计算探测概率。

叠加态与随机选择，怎样区分？

叠加态：上、下路径态 $|u\rangle$ 、 $|d\rangle$ 的相干线性组合。

相干叠加

$$|\psi\rangle = \frac{|u\rangle + |d\rangle}{\sqrt{2}}$$

直接测路径

上、下各有一半概率。

用平衡合束器重新合并两路

调好相位后，全部从 D_0 输出。

随机选择一路

每次只制备上路或下路，两种制备各占一半。

直接测路径

上、下各有一半概率。

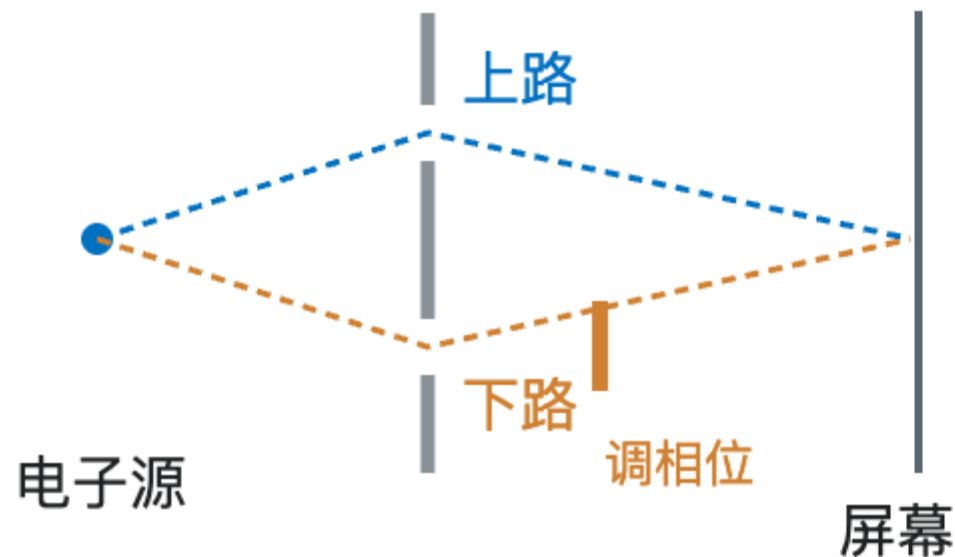
用同一个合束器重新合并

D_0 、 D_1 各有一半概率。

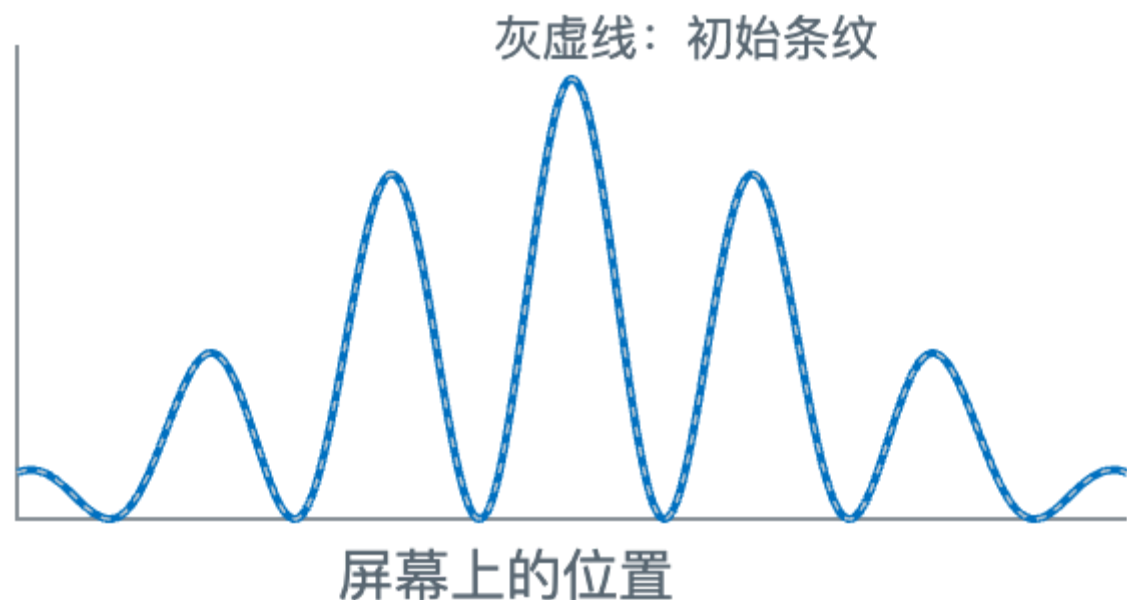
相同的路径概率，可以对应不同的量子态。

控制相位：让干涉条纹移动

同一个双缝装置



屏上的相对计数



下路相位：0°

0°

90°

180°

改变相位，就改变哪些位置容易出现电子。

相位描述两路波动的相对进度；调节后，条纹随之移动。

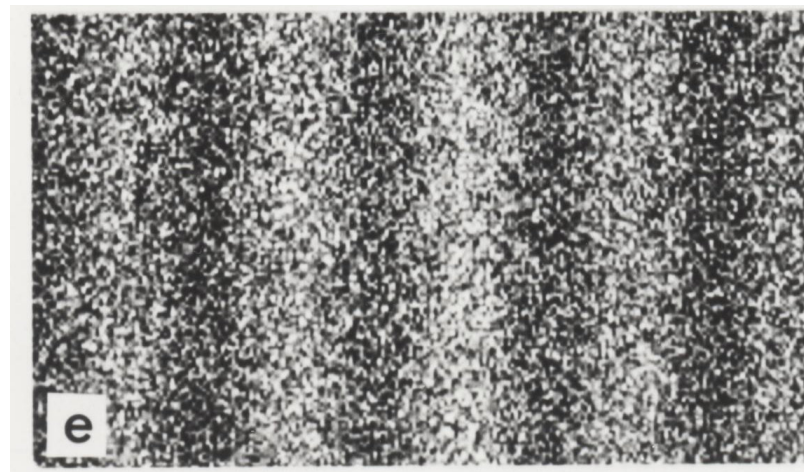
测量：一次一个结果，重复才看见分布

刚才改变的是整组条纹；一次探测能告诉我们什么？

少量电子：分散的落点



累积记录：稳定的条纹

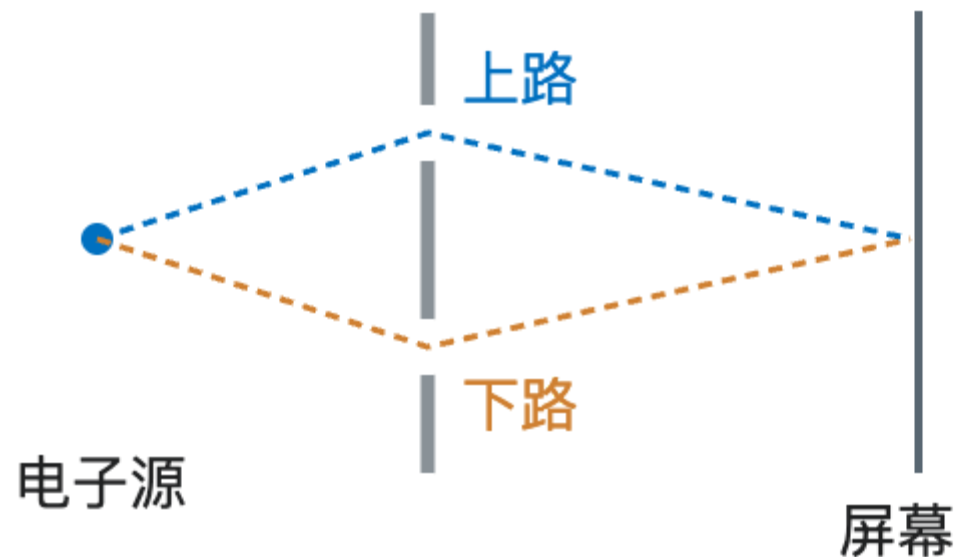


每次重新制备，再测量；统计结果，才能读出分布。

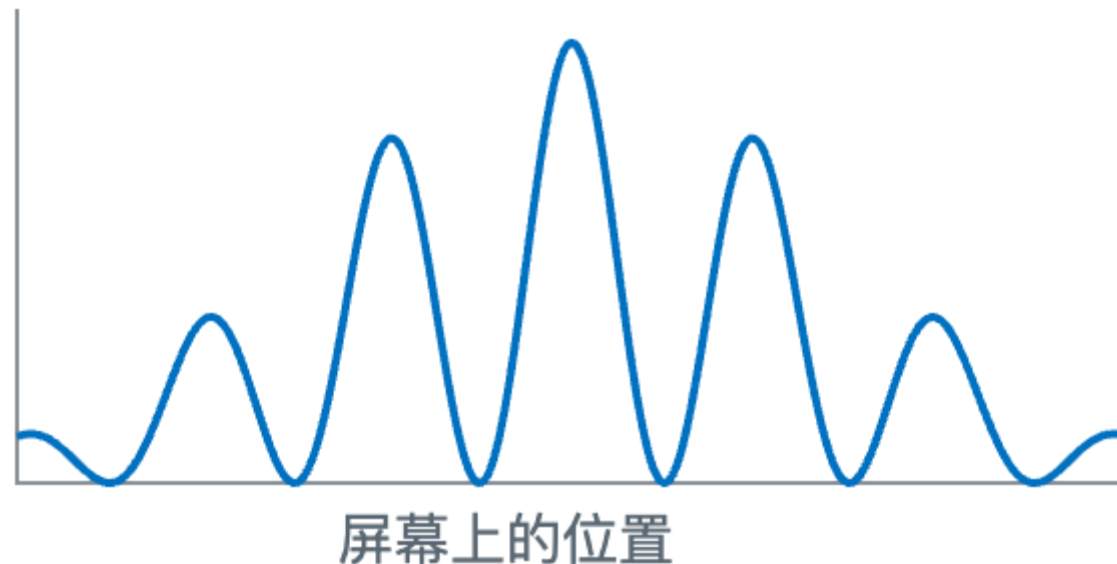
如果还想知道它走哪条路，会改变这幅分布吗？

如果先记录路径，干涉还在吗？

同一个双缝装置



屏上的相对计数



两路始终开放

不记录路径

完整记录路径

没有可区分的路径记录：屏幕上出现干涉条纹。

电子路径与装置记录关联起来；无需人读取记录。

纠缠：两个光子构成不可分的联合态

A 、 B ：两个光子； H 、 V ：水平、竖直偏振。

$$|\Phi\rangle = \frac{|H\rangle_A |H\rangle_B + |V\rangle_A |V\rangle_B}{\sqrt{2}}$$

“都水平”与“都竖直”的相干叠加，属于两个光子的整体。

不能用两个光子各自独立的状态，代替这个联合态。

只看一个光子

按水平、竖直方向测量：
 H 、 V 各有一半概率。

对照两个光子的结果

都水平，或都竖直；
在这组测量中，结果总相同。

仅凭结果相同还不够：换个测量方向，再比较。

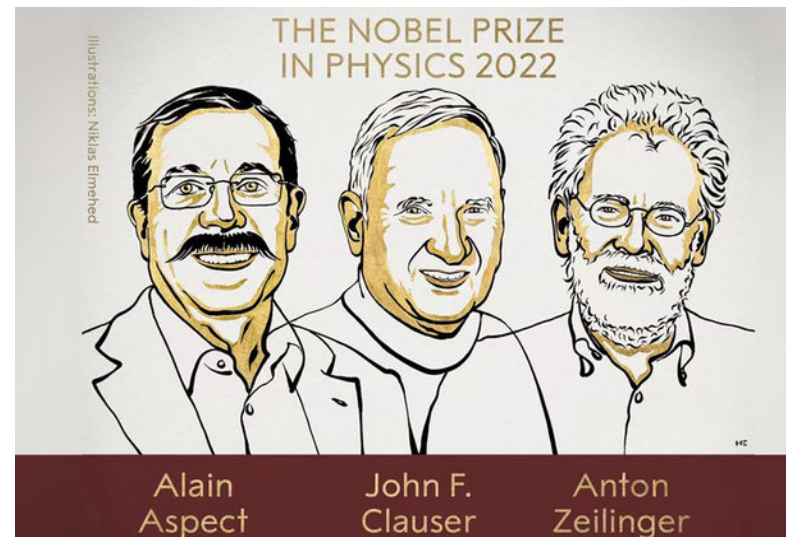
这些关联，能用预先约定的答案解释吗？

EINSTEIN ATTACKS QUANTUM THEORY

Scientist and Two Colleagues
Find It Is Not 'Complete'
Even Though 'Correct.'

SEE FULLER ONE POSSIBLE

Believe a Whole Description of
'the Physical Reality' Can Be
Provided Eventually.



1935 · EPR

量子理论是否完备？

1964 · 贝尔

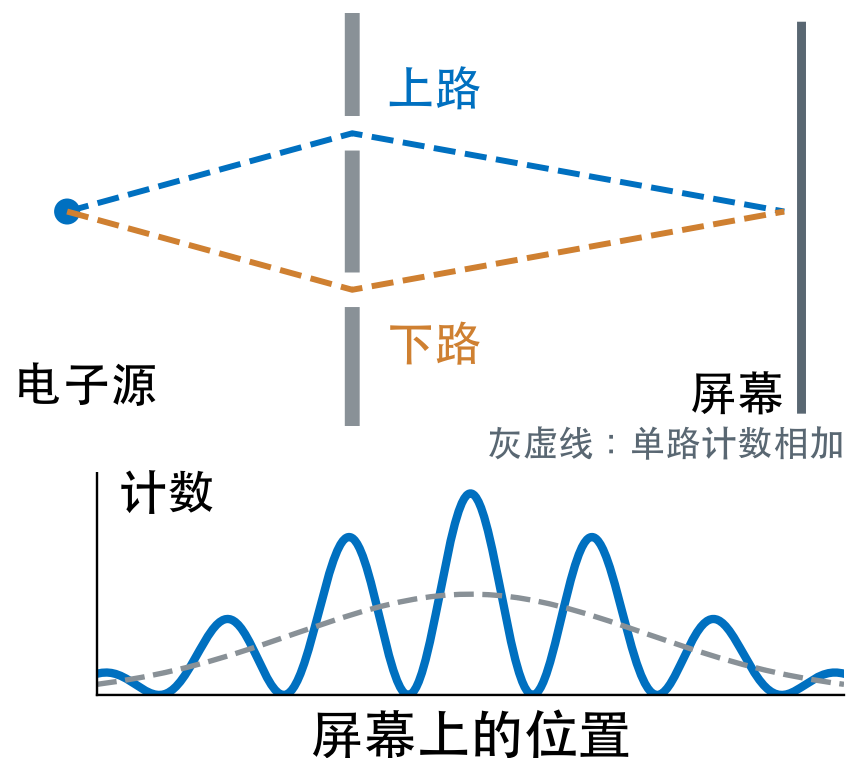
比较不同设置的测量关联。

2022 · 诺贝尔物理学奖

纠缠实验与量子信息科学。

能否用可控的量子态处理信息？

量子比特：用两个状态承载信息



上路记为0，下路记为1

$$|0\rangle \quad |1\rangle$$

它们的叠加，构成一个量子比特

$$|\psi\rangle = a|0\rangle + b|1\rangle$$

a 、 b ：两路的概率幅，
包含大小和相位。

按路径读出，每次得到0或1。

多个量子比特：叠加的是联合状态

两个量子比特的计算基底由四个基矢组成：

$$|\Psi\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle$$

1个量子比特

2 个基矢

2个量子比特

4 个基矢

n 个量子比特

2^n 个基矢

联合态可以纠缠，不能总拆成各个比特的独立状态。

测量全部比特，一次只得到一个比特串。

量子操作：制备、控制，再读出

从两条路径出发，把操作推广到多个量子比特。

1 · 制备

从已知状态开始，
产生可控的相干叠加。

2 · 控制

调节相位与比特间耦合，
操控联合态的概率幅。

3 · 读出

探测一个结果；
重复制备，统计分布。

控制量子态，是为了让有用的结果更容易出现。

经典波也能干涉，量子优势还需要什么？

经典波也能干涉，量子优势在哪里？

干涉并非量子独有

经典波也能叠加、调相，并模拟单比特干涉。

比较的是随规模增长的资源需求

用经典波逐项编码 2^n 个概率幅，需要 2^n 个模式。

算法决定能否获得加速

高效制备与控制，利用干涉提取问题的结构。

叠加、纠缠和干涉，都不自动保证计算更快。

稍后看Shor：提取周期，再用它分解整数。

量子信息科学：获取、处理与传递信息

获取信息 · 量子精密测量

用量子态感知时间、场和微小变化。

处理信息 · 量子计算

设计量子演化，解决计算任务。

传递信息 · 量子通信

用量子态建立关联，完成通信任务。

量子计算的想法怎样发展起来？



理查德·费曼

Richard Feynman

1982

用量子系统
模拟量子物理。

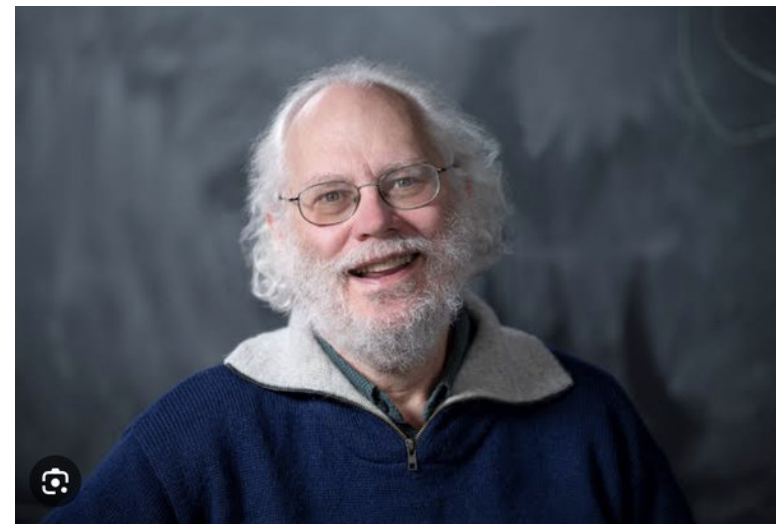


戴维·多伊奇

David Deutsch

1985

建立通用量子
计算的理论模型。



彼得·肖尔

Peter Shor

1994

找到高效分解
整数的量子算法。

回到开头：怎样帮助整数分解？

大整数很难直接找因子。

$$N = p \times q$$

Shor的转化：先找一个模幂序列的周期。

课堂上的小例子

取 $N=21$ ，从2的幂开始。

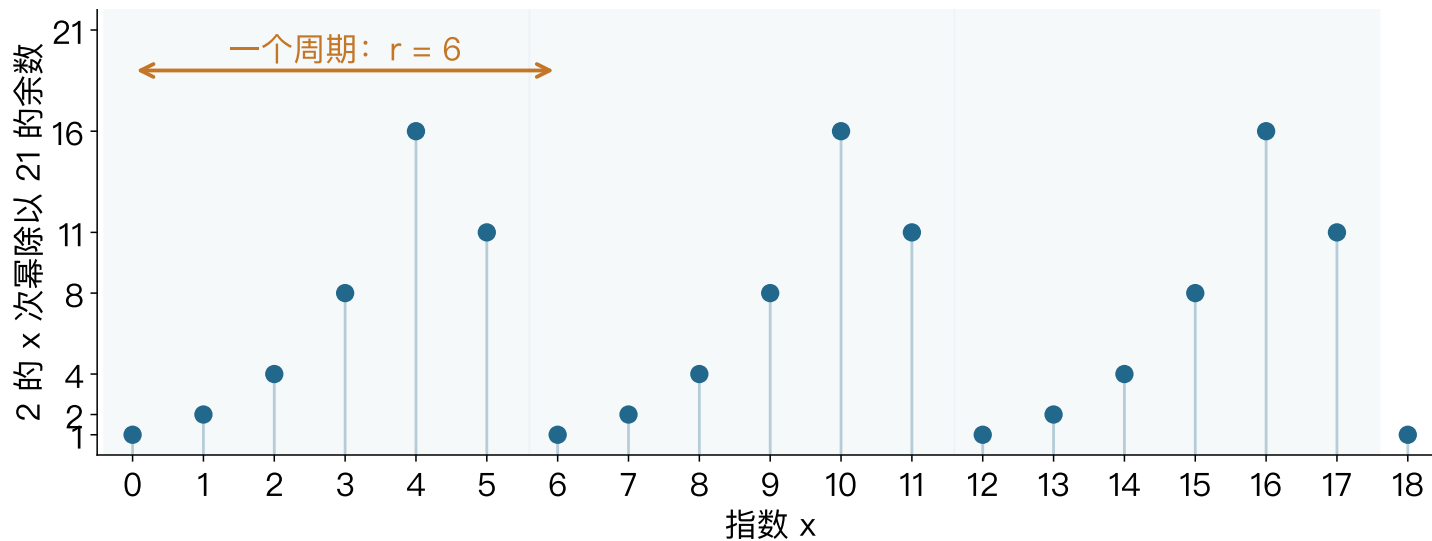
要观察的量

每次只保留除以21的余数。

寻找周期：不断乘2，再除以21取余数

从1开始，每一步乘2，再取余数。

1 → 2 → 4 → 8 → 16 → 11 → 1



经过6步回到1，随后重新重复。

知道周期，怎样得到因子？

6步回到余数1

所以 $2^6 - 1$ 能被21整除。

$$2^6 - 1 = (2^3 - 1)(2^3 + 1) = 7 \times 9$$

7与21的最大公因数

7

9与21的最大公因数

3

$$21 = 3 \times 7$$

Shor的量子步骤：让周期显现在测量中

叠加输入

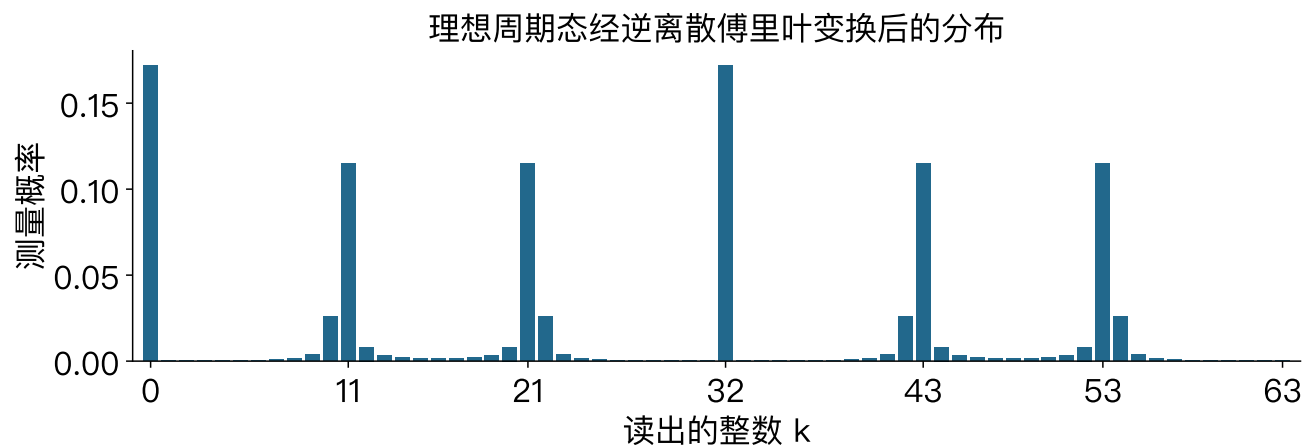
制备多个指数的相干叠加

模幂运算

建立指数与余数的关联

干涉与读出

把周期信息转成测量分布



一次测量提供一条线索。

重复取样，用经典计算恢复周期，再检验并提取因子。

高效分解大整数，将威胁开头介绍的RSA密码。

怎样制造一台量子计算机？



IBM Quantum System Two
超导量子计算系统·美国波基普西

制备

从可重复的初态开始。

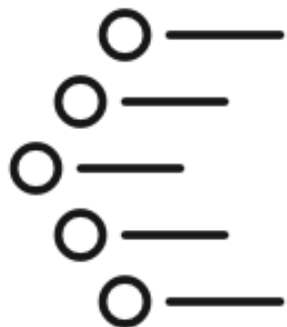
控制

用微波脉冲操控量子比特。

读出

把微波测量信号变成记录。

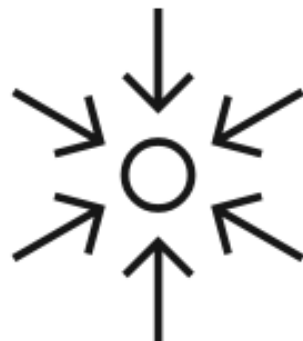
量子比特可以由什么实现？



超导电路

电路的两个量子能级

用微波脉冲控制



囚禁离子

原子内部的两个状态

用激光或微波控制

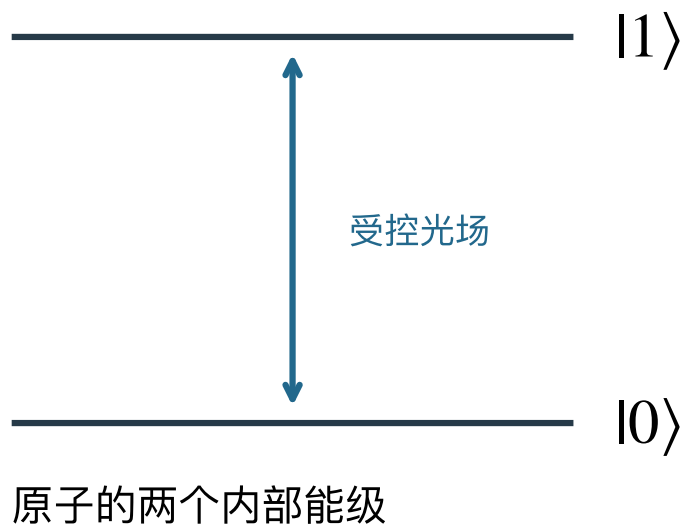


半导体量子点

电子的两个自旋状态

用电场、磁场等控制

怎样控制量子态？光与原子再次相遇



调节光的频率

选择要驱动的跃迁。

调节光的强度与作用时间

控制两个状态的概率幅。

调节光的相位

控制叠加态的相对相位。

从量子力学到量子信息科学

认识量子规律

从光谱、电子干涉到状态与测量

学会制备与控制

光的量子态、原子的量子态与相互作用

理解量子信息任务

计算、通信与精密测量

这门课：研究光与物质怎样在量子层面相互作用。

