量子コンピューティング

とその周辺

北野 正雄
京都大学工学研究科電子工学専攻

2004 年 5 月 14 日
COE 講義「電気電子基盤技術の展望」

あらまし

- 量子と工学
- 量子ビットと量子ゲート
- 量子計算
- 量子暗号と量子テレポーテーション
- 原子時計
- 光の速度制御と量子メモリー

量子と工学

- 量子力学はミクロ世界のルール
  — マクロな系にも現れる
- 量子力学の本質を利用した技術は案外少ない
  - 現行の “量子” デバイスの動作は, ほぼ古典的に説明できる
    (古典的粒子と古典的波動)
  - 電気系学科には本格的な量子力学の講義がなかった
    (でもあまり困らなかった)
- 量子の機微を生かした “Full-fledged quantum engineering” は新たなフロンティア

量子的世界

- 粒子性と波動性の共存
- 部分と全体 — エンタングルメント (entanglement)
- 観測 — 本質的ランダムネス
- 自由度の大きさ (指数的爆発 2^{2^N})
- $\hbar$ の小ささ

$$(\text{アボガドロ数}) \times (\text{光の周波数}) \times \hbar$$
$$= \quad 6 \cdot 10^{23} \times 10^{15}\text{Hz} \times 10^{-34}\text{Js} = 60\,\text{J}$$

巨大な数をかけて, やっと日常的レベル

- 無差別性 — 同種原子には全く区別はない

シュレディンガーの猫

猫 : $\begin{cases} |\text{  }\rangle & (\text{生きている}) \\ |\text{  }\rangle & (\text{死んでいる}) \end{cases}$ 原子核 : $\begin{cases} |0\rangle & (\text{崩壊前}) \\ |1\rangle & (\text{崩壊後}) \end{cases}$

- 初期状態

$$|\text{  }\rangle|0\rangle$$

- 原子核の崩壊

$$|\text{  }\rangle(\alpha|0\rangle + \beta|1\rangle)$$

- 猫と原子核の状態を結ぶ装置 (cat killer)

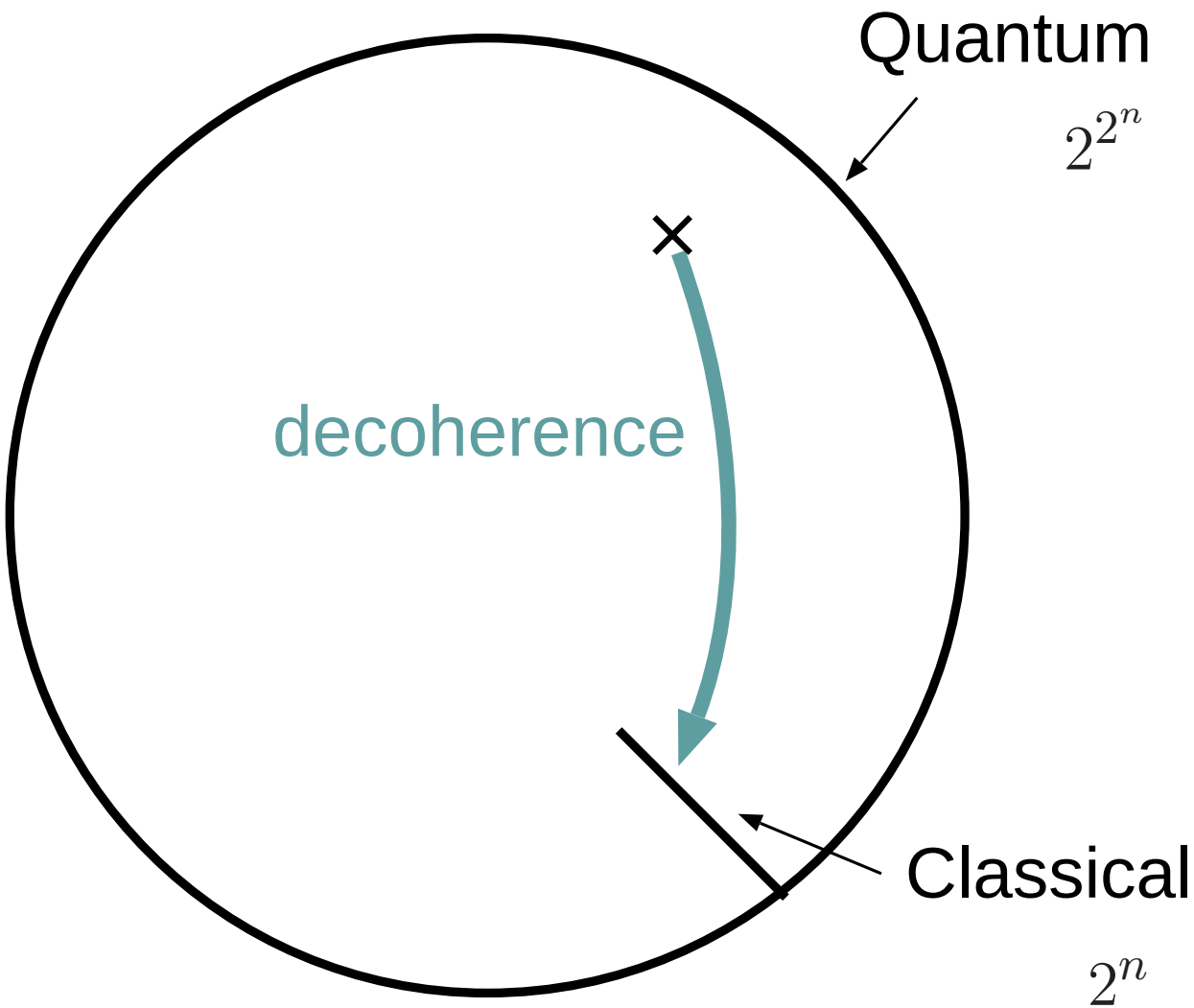
$$\alpha|\text{  }\rangle|0\rangle + \beta|\text{  }\rangle|1\rangle$$

エンタングルメント

$$\alpha|\text{猫}\rangle|0\rangle + \beta|\text{悪魔}\rangle|1\rangle$$

- 2 つの可能な状態が同時に存在する
- 量子相関
- 絡まった状態, 縺れた状態　(Entanglement)
- 古典力学的な直感 (日常間隔) とは相容れない
  — しかし自然のルールである

量子 >> 古典



量子マンダラ

量子と情報

- 量子暗号通信
  - クローン不可能定理 → 盗聴が必ず検知できる
  - 短距離 10 km ならすでに実用レベル (鍵配送)
- 量子計算
  - エンタングルメントの利用
  - 量子並列性, 自由度の大きさ → 計算量的に困難な計算が可能
- 量子標準
  - 純粋な量子系の安定性, 普遍性, 無差別性
  - 極限的精度の追求 (時間, 周波数, 電気標準, 重力, ...)

量子工学を支える技術

- レーザ (半導体レーザ,　固体レーザ, ...)
- 近接場光学/ フォトニック結晶
- レーザによる原子冷却 (1997, 2001 ノーベル物理学賞)
- イオントラップ
- 非線形光学
- 超電導技術

量子ビット

- キュビット (Qubit, quantum bit)

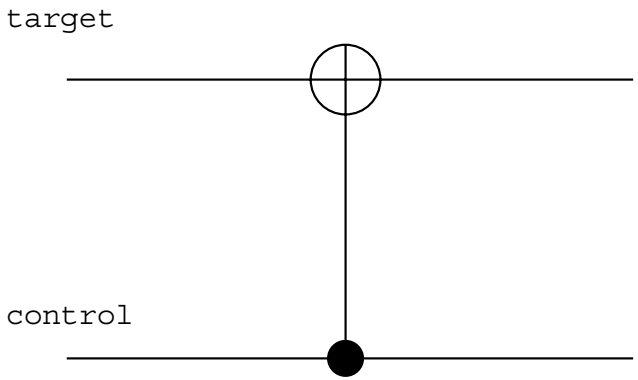
  2 つの量子状態 $|0\rangle$, $|1\rangle$ にビット情報を割り当てる.

系	状態
核スピン	上向き, 下向き
光子偏光	水平, 垂直
ジョゼフソン素子	磁束量子の有無
量子ドット	電子の有無

- 重ね合わせ状態

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

量子ゲート



$$|0\rangle|0\rangle \rightarrow |0\rangle|0\rangle$$
$$|0\rangle|1\rangle \rightarrow |0\rangle|1\rangle$$
$$|1\rangle|0\rangle \rightarrow |1\rangle|1\rangle$$
$$|1\rangle|1\rangle \rightarrow |1\rangle|0\rangle$$

- CNOT (controlled NOT) が基本ゲート. これと, 1qubit の操作ができれば, 任意の演算か可能.
- しかし, 1 量子の差異で, 他の量子を制御するのは結構むずかしい.
- qubit 数が増えると, 全体系のコヒーレンスを保つのが困難 (デコヒーレンス問題)

量子計算の歴史

- Feynman

  量子系を古典計算機でシミュレートすると　計算時間が系のサイズの指数関数で増大する (1982)

- 量子ゲート (Deutsch, Yao)

  ユニタリー変換による計算 1qubit, 2qubit の操作ができれば任意の操作が可能 (普遍ゲート, cf. NAND)

- Shor のアルゴリズム

  素因数分解の効率的アルゴリズム　RSA 暗号を破ることができる!! (1994)

RSA 公開鍵暗号

- “古典” 暗号
- 計算の容易さの非対称性
  - 掛算と割算
  - 多項式の掛算と因数分解
  - 初等関数の微分と積分
  - 素因数分解
- RSA 暗号は大きい数の素因数分解の困難さを利用

$$g \circ f \circ m = m$$

g: 秘密鍵 (受信者が秘蔵), f: 公開鍵, m: 送信データ.

- $g \circ f = 1$ であるが, f から g を求めるのが困難.
- $f \circ m$ を送ってもらえば安全.

量子暗号 — クローン不可能定理

- 量子状態

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

- 所与の α, β をもつ量子系はいくらでも生産できる.
- しかし, $|\phi\rangle$ (1 個あるいは有限個のサンプル) から, α, β を決めることはできない.
- したがって, 量子系のコピーをつくることはできない.
- 元の系を壊すことを許せば, コピーは可能

  量子テレポーテーション

量子暗号の原理

- 光子の偏光を利用する場合
- 2つのコーディング

コーディング/データ	0	1
I	$0°$	$90°$
II	$45°$	$135°$

- 検出確率

送信コード	I		II	
送信データ	0	90	45	135
受信コードI	1	0	1/2	1/2
受信コードII	1/2	1/2	1	0

量子暗号の原理(2)

- 送信・受信者はそれぞれ光子ごとにランダムにコーディングを切替える.
- コーディングが一致する確率は 1/4.
- 送信者が事後にコーディングを公開すると, 受信者は有効なデータを選別できる.
- 盗聴者は, 各光子について測定は一回しかできない (I または II). 再送する場合, コーディングをいい加減に決めざるを得ない.
- 受信者と送信者がデータの照合を (抜打ち的に) 行うと, 盗聴の事実を知ることができる.

時計の歴史

- 天体
- 機械じかけ　$(10^{-4}, 1\mathrm{mHz} \sim 1\mathrm{Hz})$
  Harrison の時計 — 航海における経度問題
- 電子回路 水晶 $(10^{-8}, 10\mathrm{kHz} \sim 10\mathrm{MHz})$
- 原子のマイクロ波遷移 $(10^{-11}, 10\mathrm{GHz})$ セシウム原子時計 (応用: GPS)

秒の定義

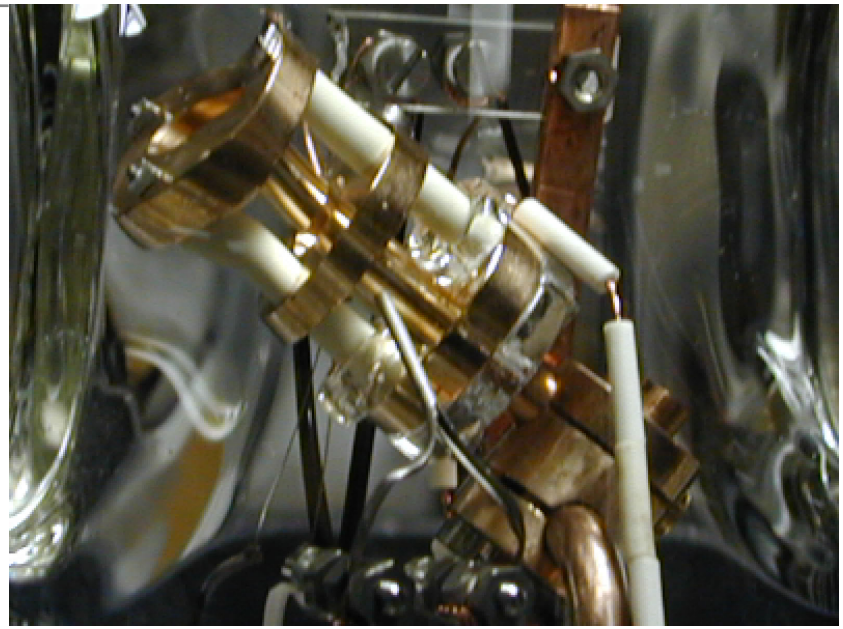
- 秒は暦表時の 1900 年 1 月 0 日 12 時に対する太陽年の $1/31\,556\,925.974\,7$ 倍である (1956).
- 秒はセシウム 133 の原子の基底状態の 2 つの超微細準位の間の遷移に対応する放射の周期の $9\,192\,631\,770$ 倍の継続時間である (1967–68).

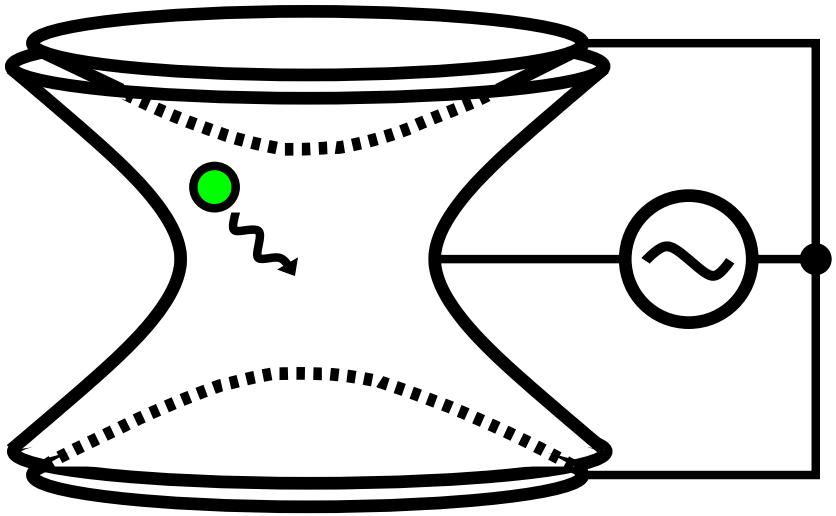
次世代の周波数標準

マイクロ波から光 ($\sim$ 1PHz) へ
精度は, 10^{-18} を目指す
重力ポテンシャルによる時間のずれ (一般相対論効果) を数メートルの高度差で検出可能な精度

- 周波数チェーン
- イオントラップ
- モード同期レーザ — 周波数コム

イオントラップ





- ひと粒のイオンを真空中に保持
- 長時間 (T) 連続して観測が可能 $\rightarrow$ 鋭いスペクトル ($\Delta f = 1/T$)
- より精度の高い「時計」を作る $\rightarrow$ $\mathbf{Yb}^{+}$

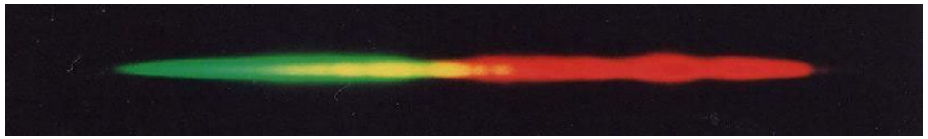
さらに, トラップされたイオンを**レーザ光により冷却**

光波長以下の領域に閉じ込め, ドップラーシフトを無くす

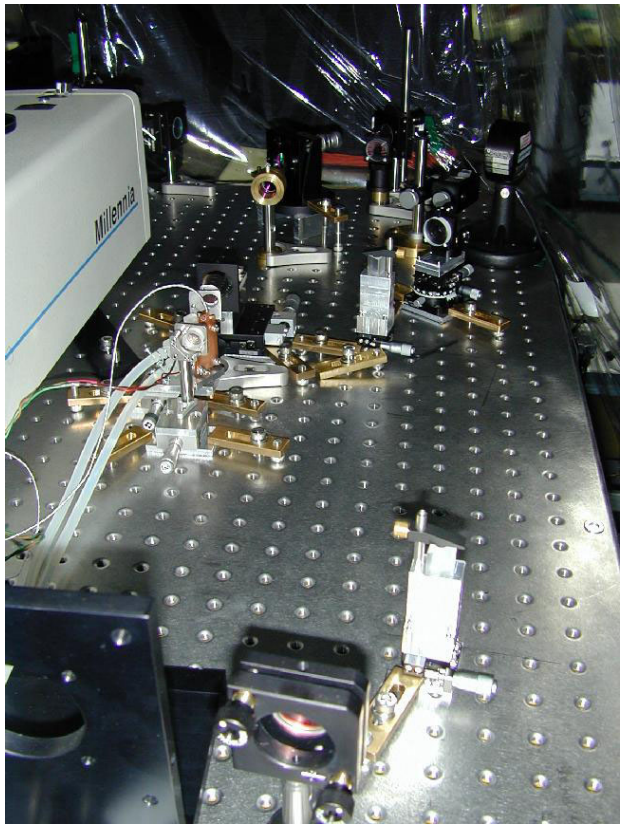
モードロックレーザの開発

科学技術の発達によりこれまで以上に高精度な時計が必要
光領域の周波数の測定 → 超短パルスモード同期レーザを利用

- モードロックレーザの開発
- 周波数コムの拡大
  - フォトニック結晶ファイバ



フォトニック結晶ファイバによるコムの広帯域化



チタンサファイアレーザ

光の速度制御

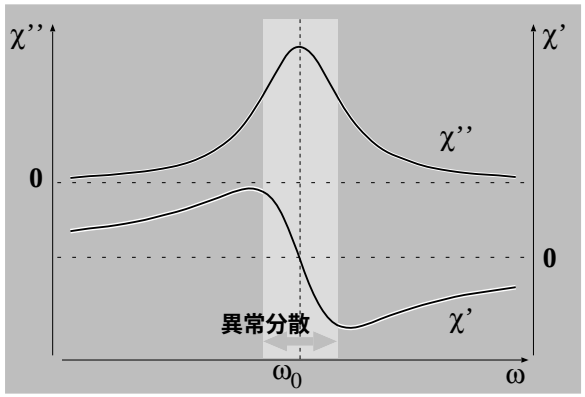
- 群速度
- 速い光
  - 光速を越える群速度
  - 負群遅延
  - 因果律との関係
- 遅い光, 止った光
  - EIT による異常分散と低群速度
  - ダーク状態ポラリトンとパルスの凍結
  - 量子メモリへの応用

光の速度

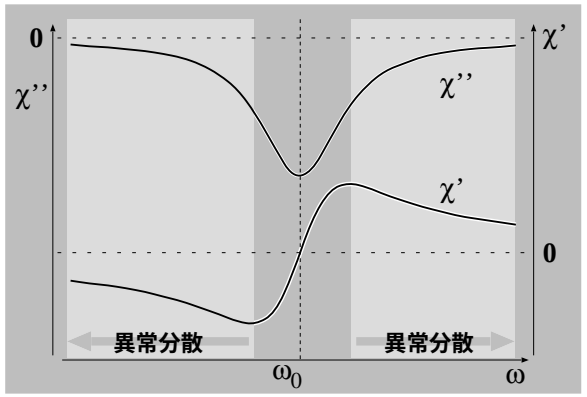
名称	定義	対象	制限
位相速度	$v_{\mathsf{p}} = \dfrac{\omega}{k}$	単色波の等位相面 (群)	なし
群速度	$v_{\mathsf{g}} = \dfrac{\mathrm{d}\omega}{\mathrm{d}k}$	波束/変調波の包絡線	なし
波頭速度	$v_{\mathsf{f}} = \left.\dfrac{\omega}{k}\right\|_{\omega\to\infty}$	波頭, 不連続点	$= c$

- 群速度も位相速度と同じく c を越えてもよい. (Brillouin, Stratton)
- 「群速度は情報やエネルギーに関係しており c を越えることはない」は間違い！
- (相対論的) 因果律に直接関係するのは波頭速度.

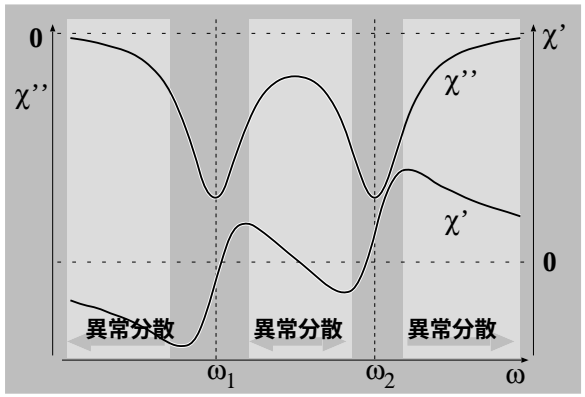
分散関係と群速度



(a)



(b)



(c)

(a) single absorption line

(b) single gain line

(c) double gain lines

感受率: $\chi = \chi' - \mathrm{i}\chi''$; 波数: $k = k_0(1 + \chi'/2)$, 吸収 $k_0\chi''/2$.

$$\frac{\mathrm{d}\chi'}{\mathrm{d}\omega} < 0 \Rightarrow \text{群速度が } c \text{ より大きくなる}$$

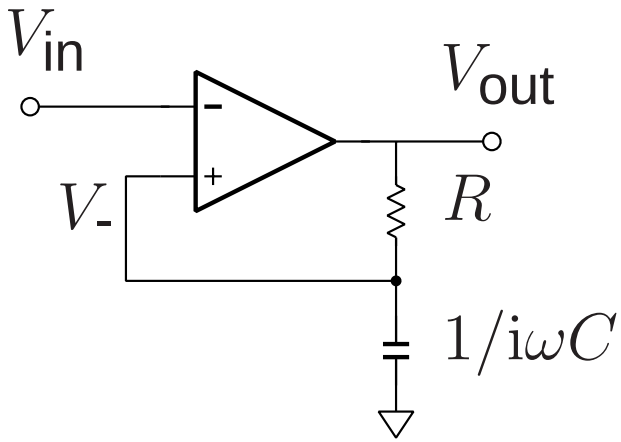
超光速伝搬の実験

- 群速度 $v_{\mathrm{g}} = -c/310$, 群屈折率 $n_{\mathrm{g}} = 1/310$
- 幅 $3.7\,\mu\mathrm{s}$ のパルスが, $6\,\mathrm{cm}$ のセルを通過し, 真空の場合より, $62\,\mathrm{ns}$ 速かった.

超光速をめぐる迷信と議論

- 群速度が c を越えないと書いてある教科書も多い
- 理論的には納得できるが, 何か腑に落ちない
  - 群速度に代る速度 (時間) の導入
    - トンネル現象における
      Büttiker-Landauer time, Larmor time, ...
  - 時変過渡応答による解釈
- 電子回路による負群遅延 —
  曖昧さのない系 → 誤解や俗説を正す

負群遅延回路



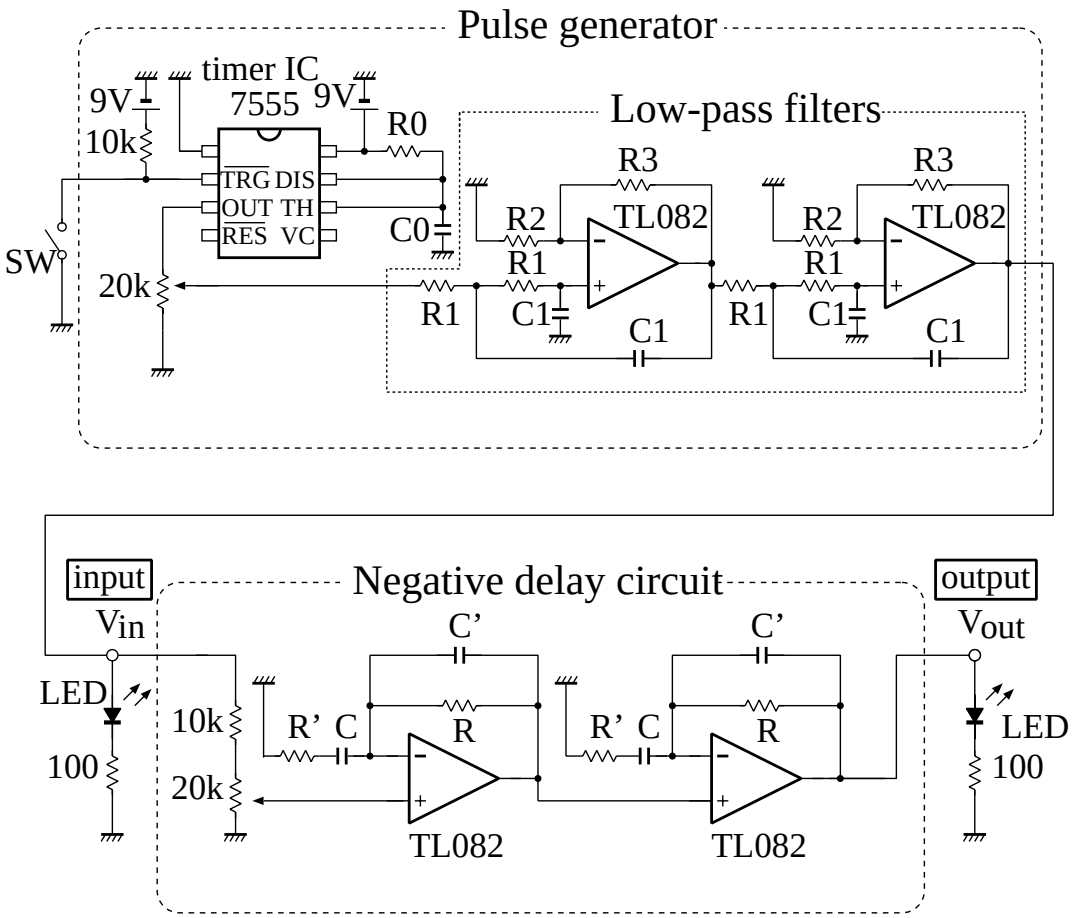
$$V_- = \frac{(\mathrm{i}\omega C)^{-1}}{R + (\mathrm{i}\omega C)^{-1}} V_{\text{out}} = \frac{1}{1 + \mathrm{i}\omega CR} V_{\text{out}}$$

仮想短絡 $V_{\text{in}} \sim V_-$

$$V_{\text{out}} = (1 + \mathrm{i}\omega CR) V_{\text{in}}$$

帰還回路によって極が零に変換された.

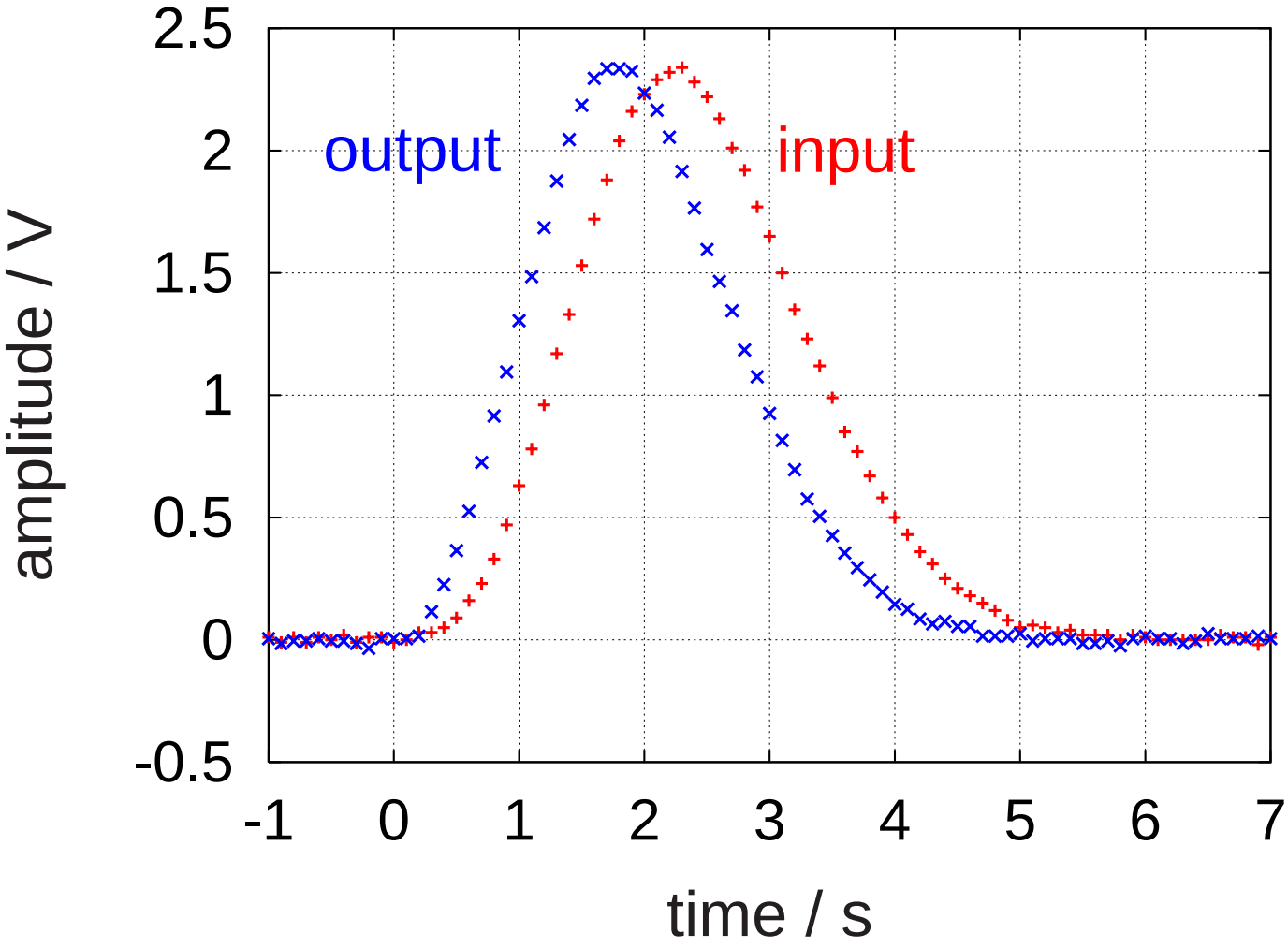
Circuit Diagram



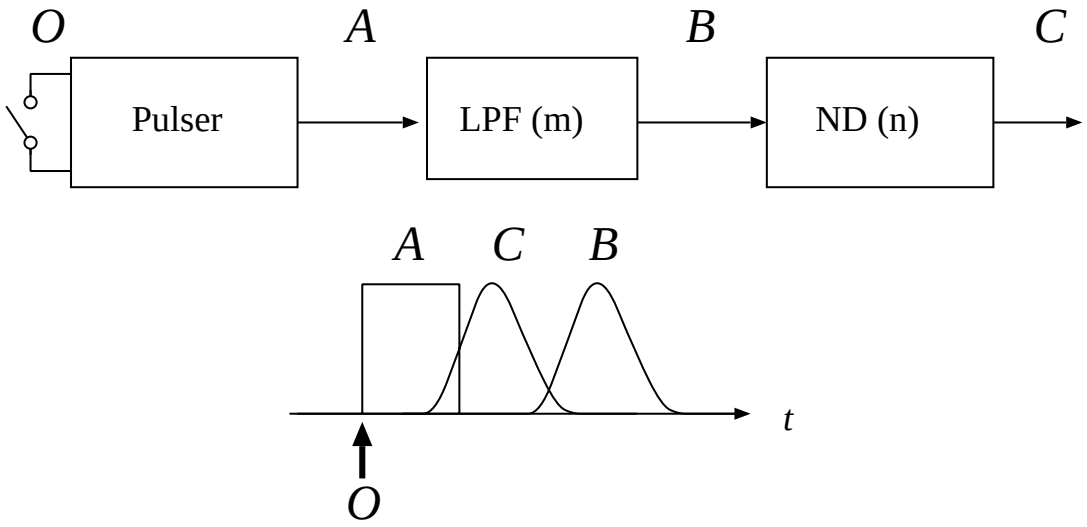
Nakanishi *et al.*, Am. J. Phys. **70**, 1117 (2002),
Kitano *et al.*, IEEE JSTQE **9**, 43 (2003).

入力/出力波形

$m = 4, n = 2$



因果律



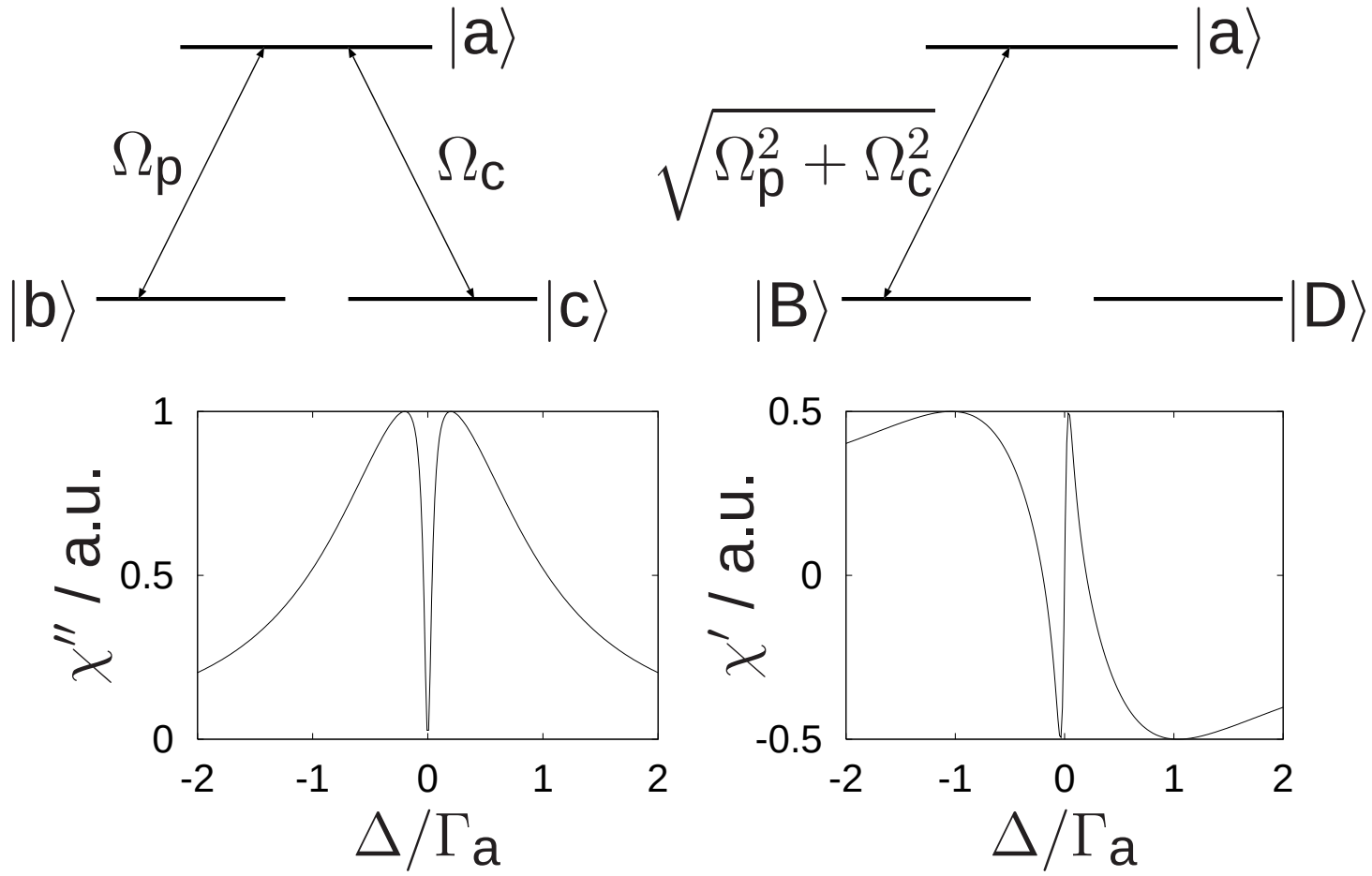
- 日常感覚における因果律 (集中定数系)

$$O \Rightarrow A \Rightarrow B \stackrel{?}{\Rightarrow} C$$

- 厳密な意味での因果律

$$A \Leftrightarrow B \Leftrightarrow C$$

量子干渉による透明化



低群速度の実験

Hau *et al.*, Nature **397**, 594 (1999).

- Na ボーズ凝縮体 (D_2 線)
- 群速度

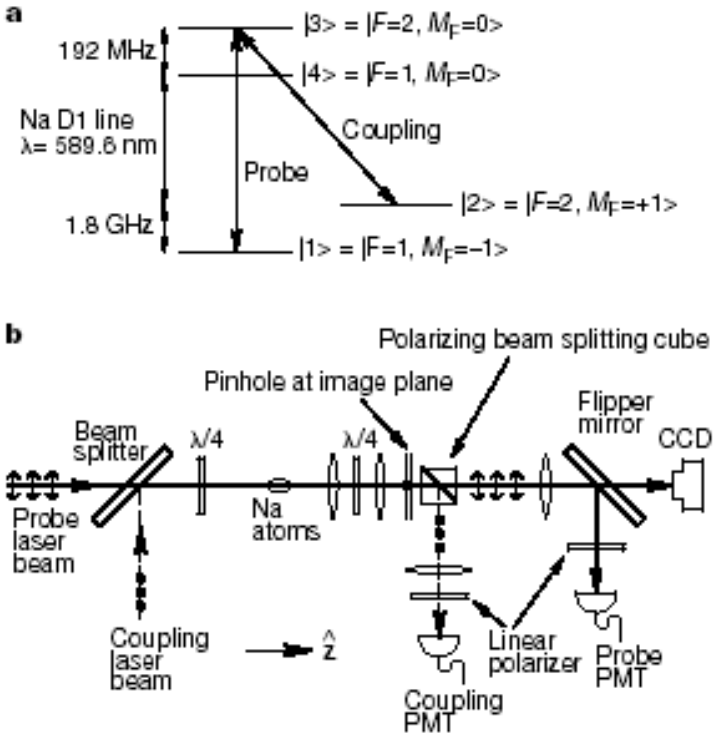
$$v_{\mathrm{g}} \sim 10^{-7} c = 30\,\mathrm{m/s}$$

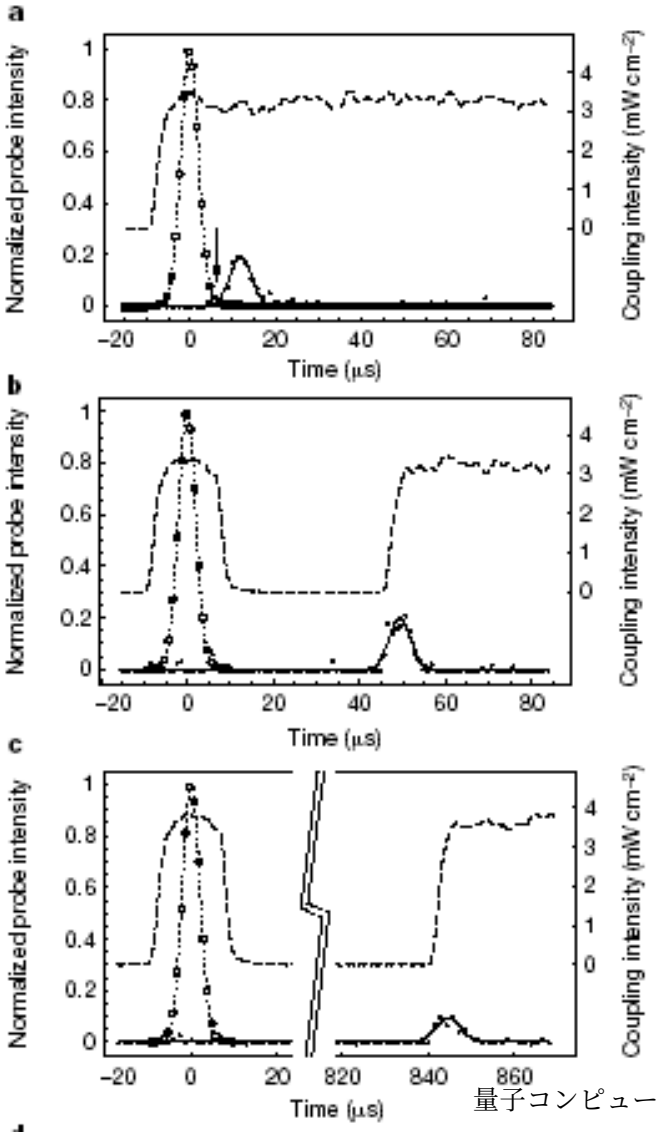
- 幅 $2.5\,\mu\mathrm{s}$ のパルスが, $0.3\,\mathrm{mm}$ の媒質を通過し, 真空の場合より, $7\,\mathrm{ns}$ 遅れた.
- パルス幅の圧縮

$$\frac{L_{\mathrm{p}}(\mathrm{medium})}{L_{\mathrm{p}}(\mathrm{vacuum})} = \frac{43\,\mu\mathrm{m}}{750\,\mathrm{m}} \sim 10^{-7}$$

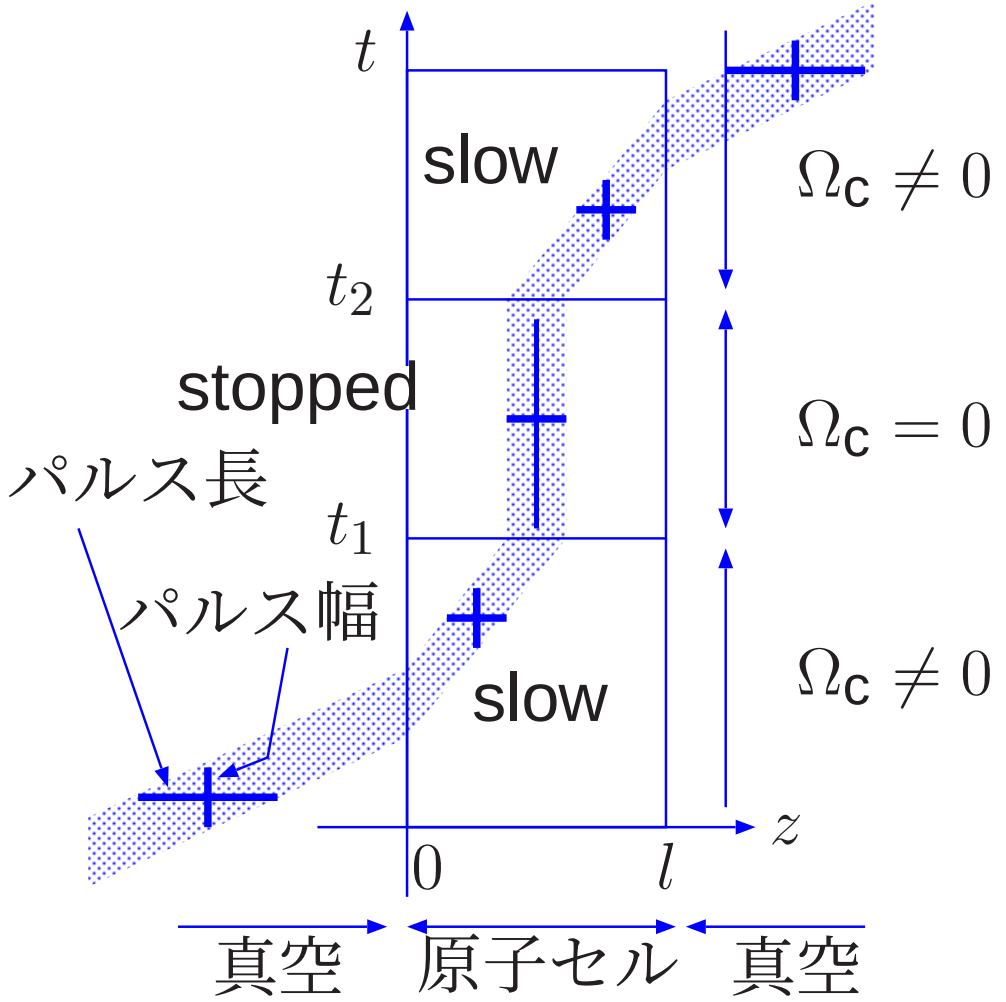
光凍結の実験

Liu *et al.*: Nature **409**, 490 (2001).





パルス凍結のダイアグラム



光凍結

Phillips *el al.*: Phys. Rev. Lett. **86**, 783 (2001).
Liu *et al.*: Nature **409**, 490 (2001).

- 光の包絡線の持つすべての情報を記憶できる (振幅, 位相, 時空間形状)
- コヒーレンス時間 ($\sim$ ms) 以内なら再出発可能
- 原子状態で操作し, 加工された光パルスを生成
- 光の量子状態も (原理的には) 記憶可能
  $\rightarrow$ 量子情報処理への応用

光凍結の応用 — 量子メモリ (1)

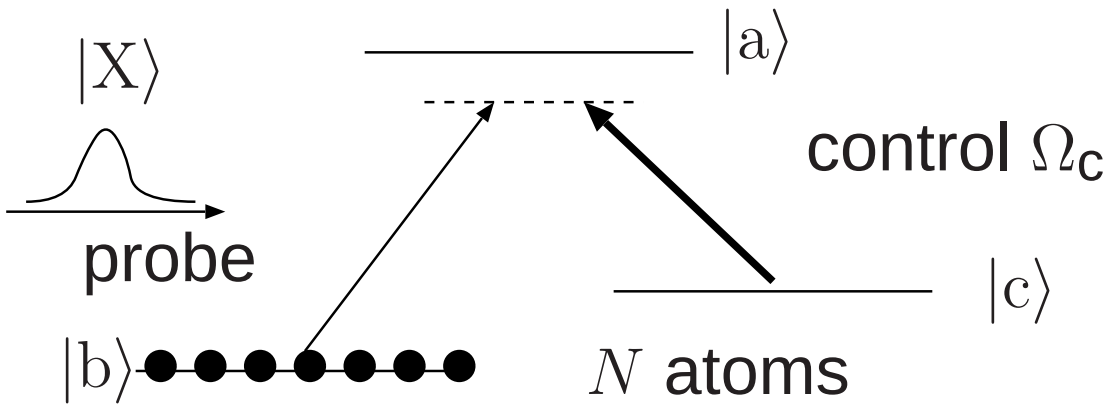
Fleischhauer and Lukin: Phys. Rev. Lett **84**, 5094 (2000).

- Probe photon state (Fock state)

$$|\mathrm{X}\rangle = \sum_n a_n |n\rangle$$

- Atomic ground state (N atoms)

$$|0_\mathrm{c}\rangle = |b_1, b_2, \ldots, b_N\rangle$$



光凍結の応用 — 量子メモリ (2)

- adiabatic change ($\Omega_{\mathsf{c}} \to 0$)

$$\sum_n a_n |n\rangle \otimes |0_{\mathsf{c}}\rangle \to |0\rangle \otimes \sum_n a_n |n_{\mathsf{c}}\rangle$$

- Symmetric atomic states

$$|1_{\mathsf{c}}\rangle = \frac{1}{\sqrt{N}} \sum_i |b_1, b_2, \ldots, c_i, \ldots, b_N\rangle$$

$$|2_{\mathsf{c}}\rangle = {}_N C_2^{-1/2} \sum_{i \neq j} |b_1, \ldots, c_i, \ldots, c_j, \ldots, b_N\rangle$$

$$\ldots$$

- Photon detector with photon number resolution is possible.

まとめ

自然界における最も基本的なルールである量子力学を利用したエンジニアリングが着実に発展している.

- 古典力学とは定性的に異なる特徴を生かす盗聴不可能な通信, 古典計算機では解けない問題を解く
- 標準や計測において, 究極的な精度や感度の実現をめざす
- 量子系を自在に操作することで, 自然のルールをより深いレベルで理解できる