

新しい情報社会の扉を開く量子技術

－ 量子コンピューターは本当に実現できるのか？ －

量子コンピューターが開発されたら、
現代コンピューターでは処理できない難
問は全て瞬時に解かれてしまうのだ！



SFでしょう...

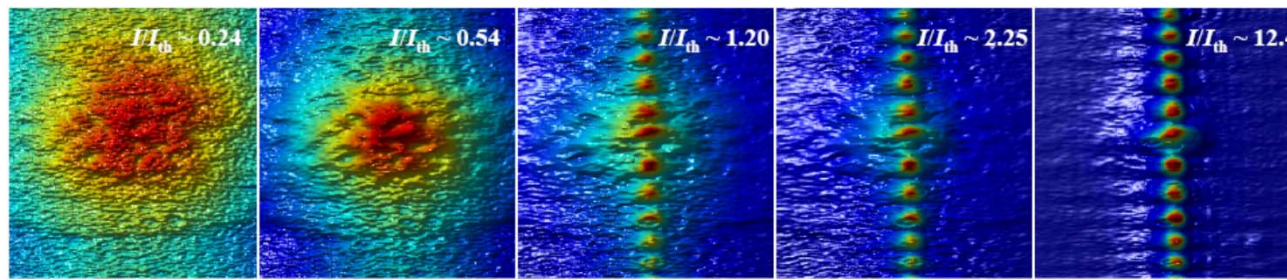
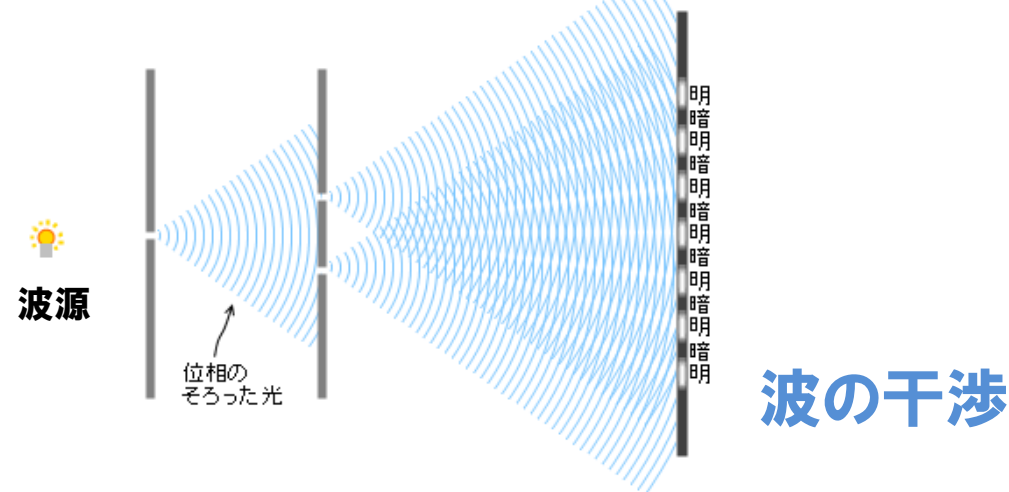
山本 喜久

国立情報学研究所、スタンフォード大学

軽井沢土曜懇話会(国立情報学研究所 国際高等セミナーハウス) 平成24年7月7日

波の干渉

2つのスリットから、位相のそろった波が同時に出力される。2つの波がスクリーンにたどり着くとき、波の山と山(谷と谷)が重なれば、その部分は明るい線となり、波の山と谷が重なれば、その部分は暗い線になる。この明線と暗線が繰り返し現れることを“干渉縞”という。



発光ダイオード
のインコヒーレント光

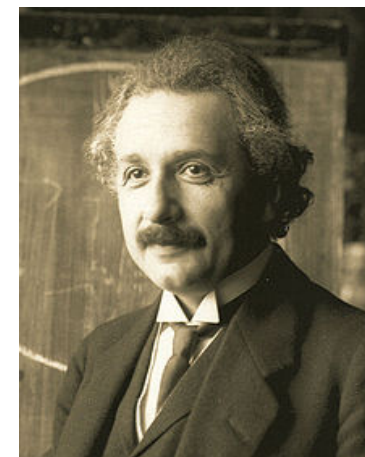
↑
発振しきい値

半導体レーザー
のコヒーレント光

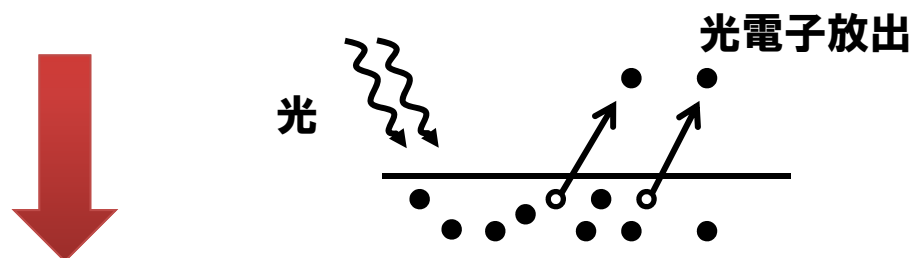
➡ 光は波動である。

アインシュタインの光電効果

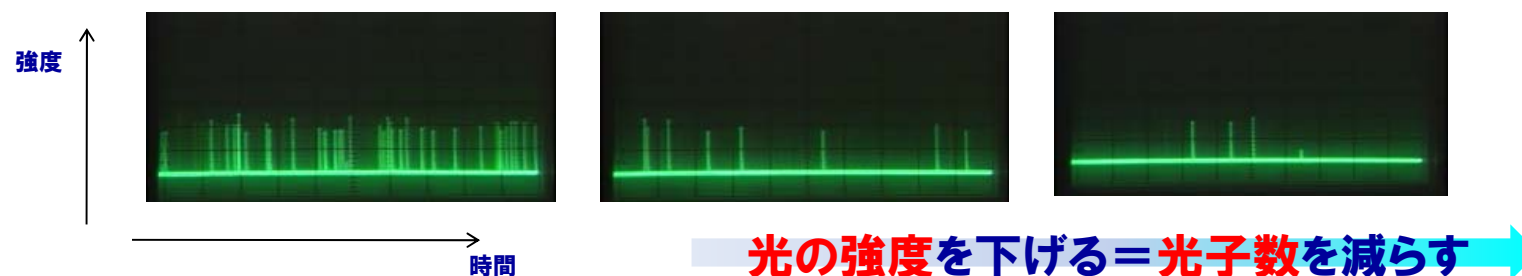
光を物質に当てると、電子が物質表面から飛び出す。光の強度を上げると**たくさんの電子**が飛び出すが、光の強度を下げると**少数の電子**しか飛び出さない。しかし、電子一個当たりのエネルギーに変化はない。



Albert Einstein
(1879-1955)



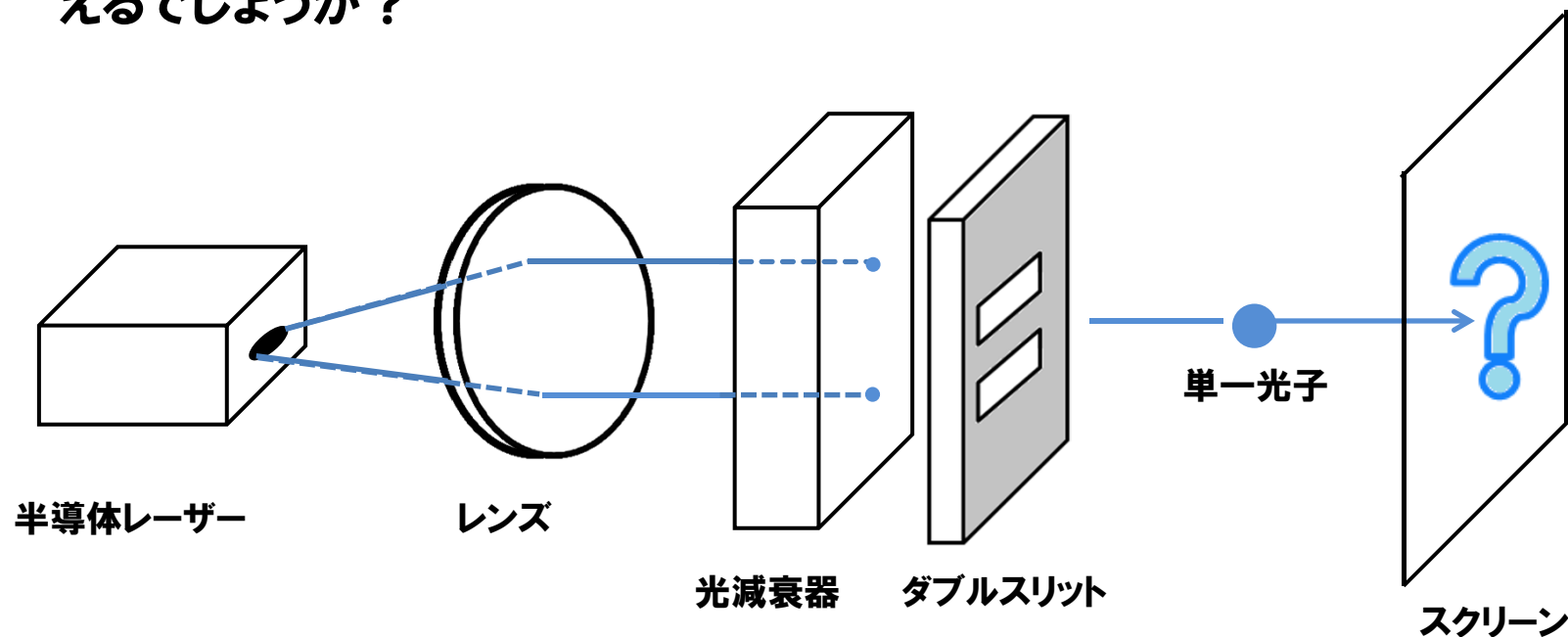
光は一定のエネルギーを持った粒子の集団であり、これを“光量子もしくは光子”と呼ぶ。



➡ 光は粒子である。

単一光子は干渉する？

もし、半導体レーザーからのコヒーレント光の強度を極限まで下げて、ダブルスリット干渉計の中で常に光子が1つしか伝搬しないようにした時、干渉縞は見えるでしょうか？



➡ 1つの光子は2つの異なった場所に同時に存在できる。
(光子の裁判: 朝永振一郎)

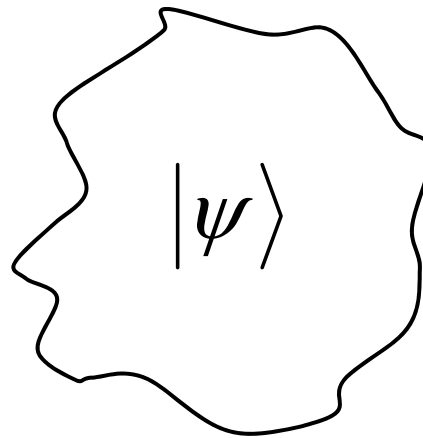
粒子－波動の二重性

古典の世界

量子の世界

古典の世界

波動性という
実在が現れる



粒子性という
実在が現れる

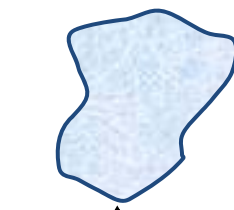
波動関数(もしくは状態ベクトル)と
呼ばれる抽象的な情報だけが存在する。

古典の世界の特徴である実在(粒子の位置や速度、波の振幅や位相が確定している状態)というものは、量子の世界には存在せず、実在は観測により作り出されるものである。

量子の世界の一部である古典の世界

量子の世界 $\hat{\rho} = \begin{bmatrix} |a|^2 & ab^* \\ a^*b & |b|^2 \end{bmatrix}$

(相反する状態に同時に存在できる)



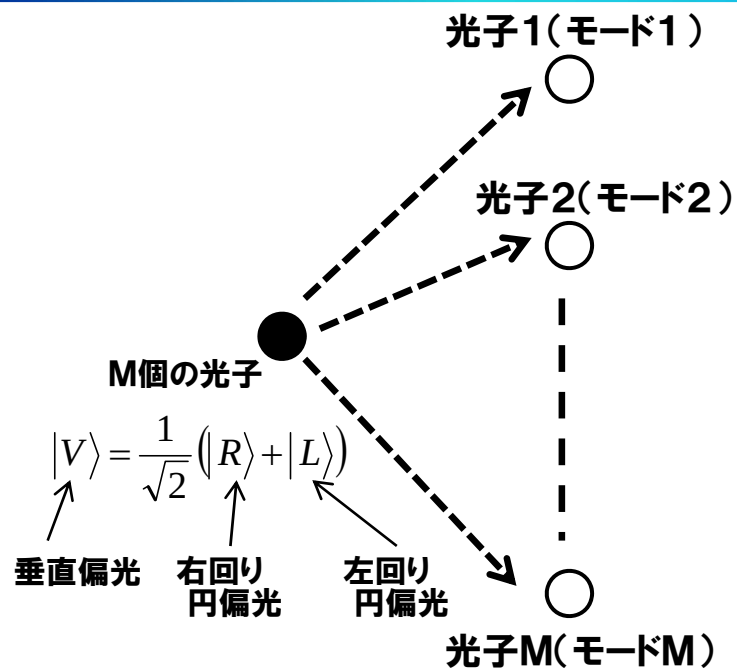
古典の世界 $\hat{\rho} = \begin{bmatrix} |a|^2 & 0 \\ 0 & |b|^2 \end{bmatrix} \begin{matrix} |a\rangle \\ |b\rangle \end{matrix}$

(相反する状態のどちらかにしか存在できない)

↑
生きている猫

↓
死んでいる猫

M個の光子で 2^M の異なった状態を同時に現わす



M個の光子の状態ベクトル

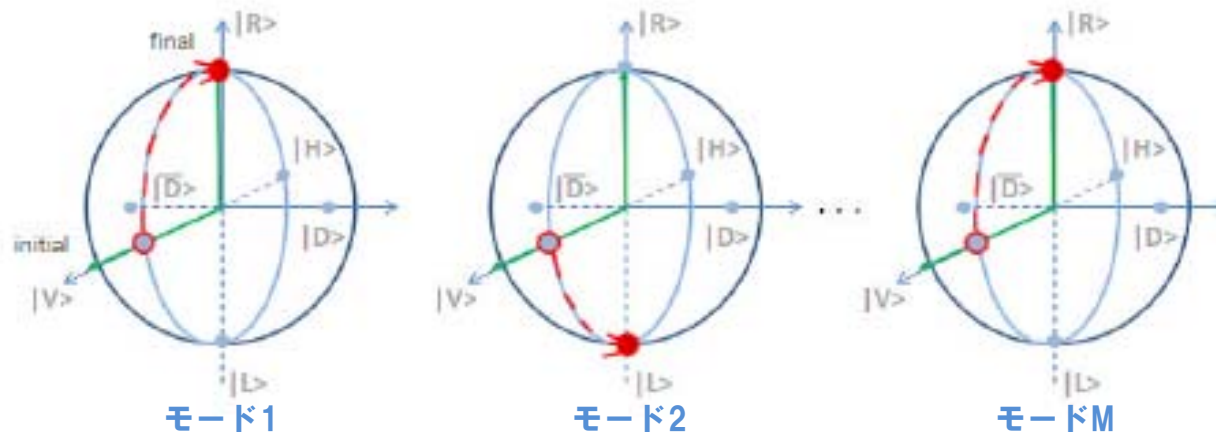
$$\frac{1}{\sqrt{2}}(|R\rangle + |L\rangle)_1 \otimes \frac{1}{\sqrt{2}}(|R\rangle + |L\rangle)_2 \otimes \dots \otimes \frac{1}{\sqrt{2}}(|R\rangle + |L\rangle)_M$$

$$= \frac{1}{\sqrt{2^M}} (|R\rangle_1 |R\rangle_2 \dots |R\rangle_M + \dots + |L\rangle_1 |L\rangle_2 \dots |L\rangle_M)$$

全てのモードが|R>

全てのモードが|L>

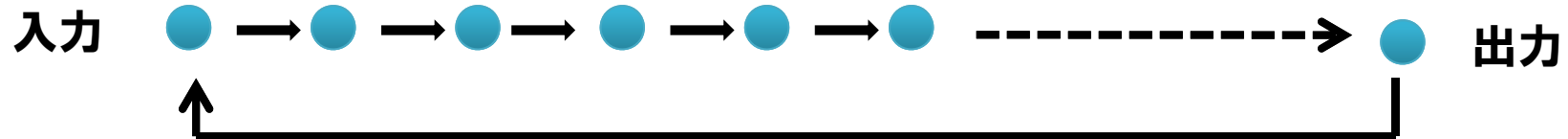
全部で 2^M 通りの異なった状態の線形重ね合わせ



➡ M個の光子は 2^M 個の異なった状態を同時に現せる。

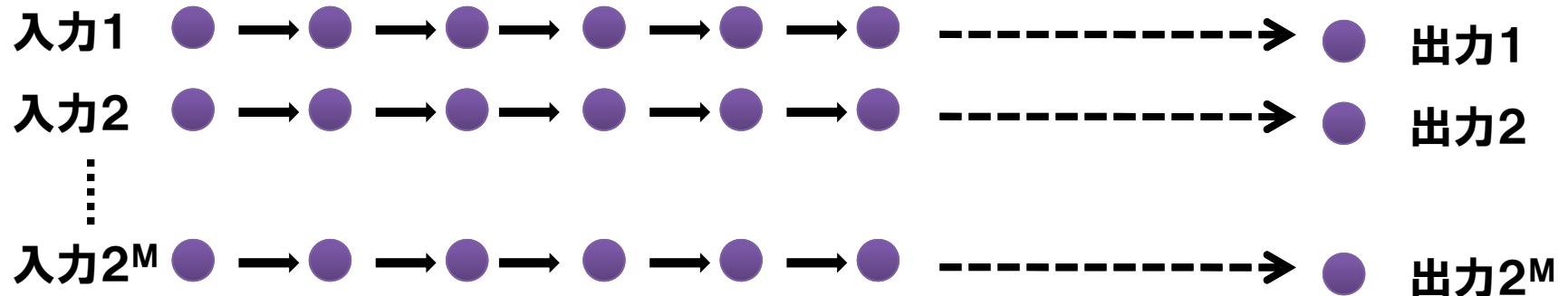
現代コンピューターと量子コンピューター

現代コンピューター



1つの入力値に対して次々と計算が実行され、それが終わると次の入力値に変えて同じ計算を繰り返す。
 2^M 回の計算が繰り返し実行され、最終的に答えを得る。

量子コンピューター



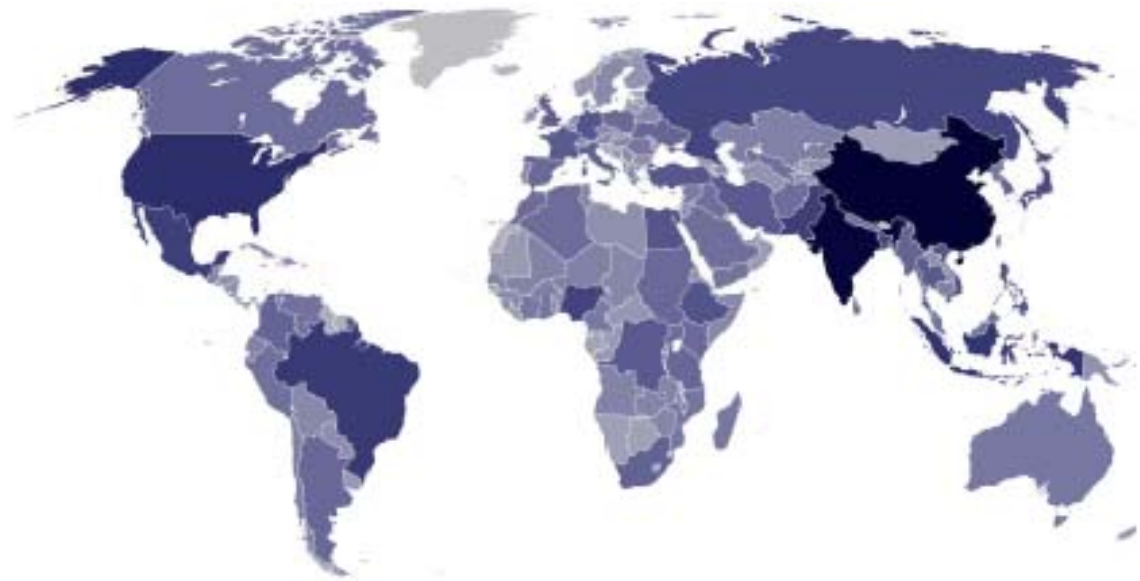
2^M の異なった入力値を線形重ね合わせの原理で実現し、これに対して計算が同時に行われるので、
たった一回の計算で答えが得られる。

➡ 量子パラレリズム: デイビッド・ドイッチ (1985)

量子パラレルイズムの威力

$$M=30 \Rightarrow 2^M \sim 10^9$$

30個の光子を30のモードに分配すると、全世界の総人口と同じ数だけの異なった入力値を同時に表わせる。



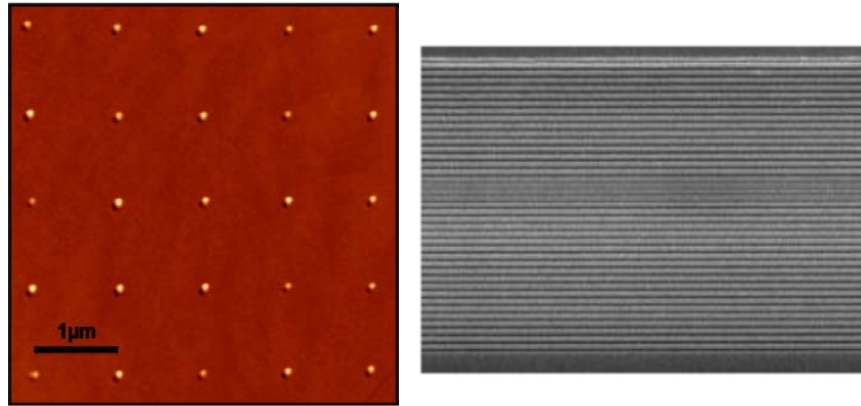
$$M=90 \Rightarrow 2^M \sim 10^{42}$$

90個の光子を90のモードに分配すると、地球を構成する全原子数に等しい入力値を同時に表わせる。

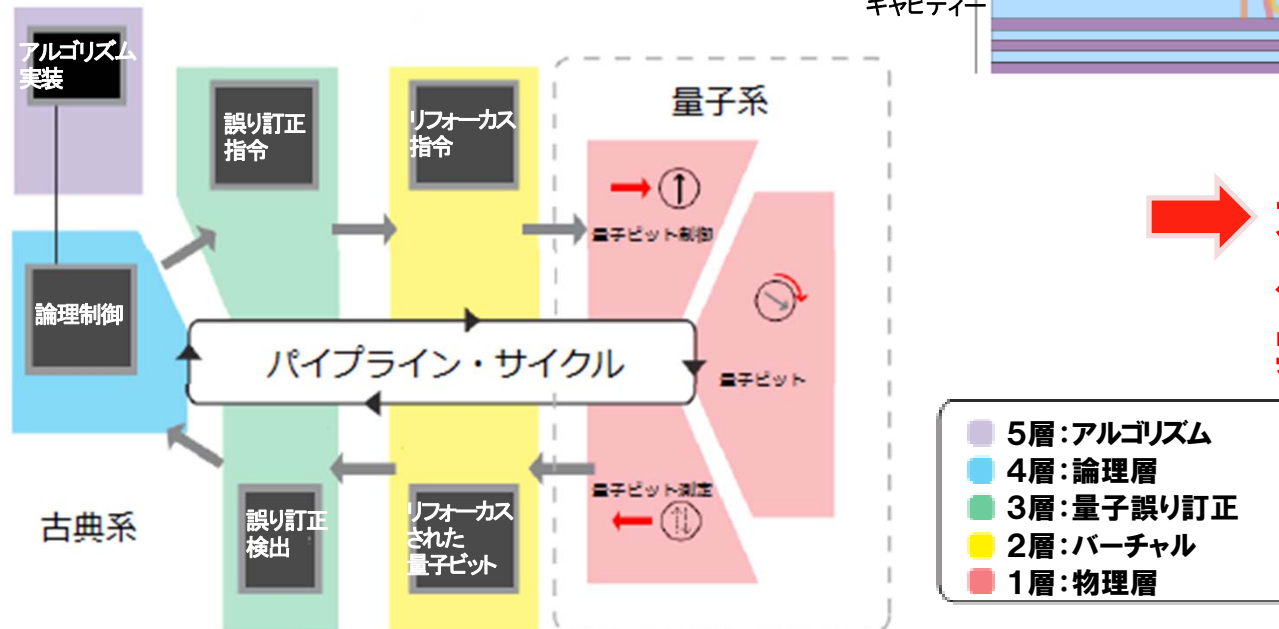
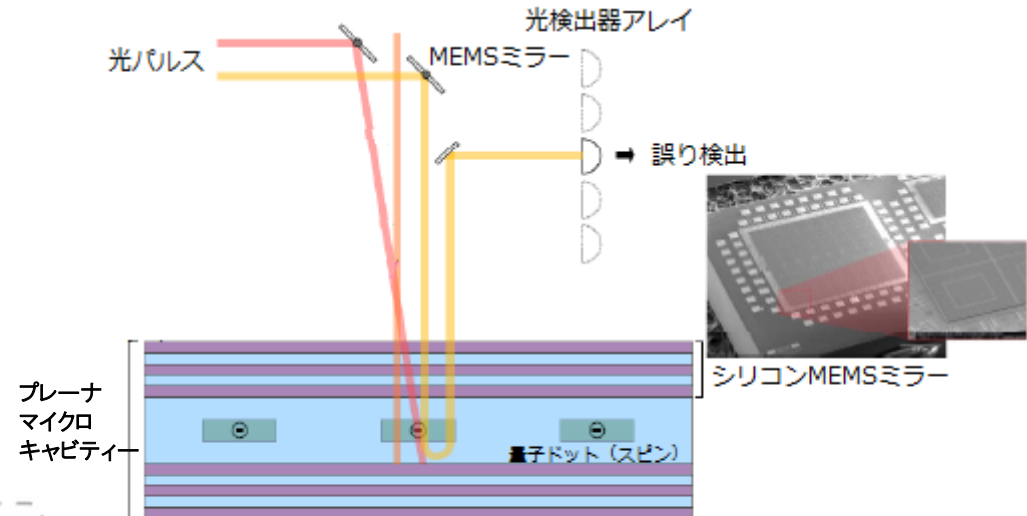


量子コンピューターをどうやって作るか

量子ドットスピンをマイクロキャビティーへ埋め込む



量子ドットスピンを光パルスで初期化、制御、測定する



不完全な量子ビットと量子ゲートで完全な量子計算を実現する。

階層構造アーキテクチャを用いて誤り耐性量子コンピューターを実現する

何が間違っていたのか？ －従来型量子コンピューターの本当の話－

M個のスピン(量子ドット)を使って 2^M 通りの異なった入力値を表わす。

$$\frac{1}{\sqrt{2}}(|\uparrow\rangle + |\downarrow\rangle)_1 \otimes \frac{1}{\sqrt{2}}(|\uparrow\rangle + |\downarrow\rangle)_2 \otimes \dots \otimes \frac{1}{\sqrt{2}}(|\uparrow\rangle + |\downarrow\rangle)_M$$

↑ ↑ ↑
スピン1 スピン2 スピンM

- ➡ 多スピン干渉計(エンタングルメントで計算を実行する。)
- ➡ 1つのスピン位相が失われる(デコヒーレンスする)と、全ての状態ベクトルが崩壊する。
- ➡ このデリケートな量子ビットをデコヒーレンスから守るために量子誤り訂正コードを何重にもかける。

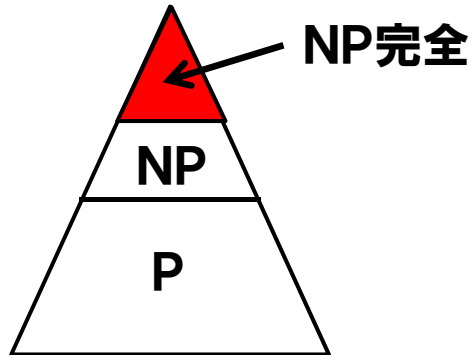
2048ビットの整数の素因数分解を世界最高速度の光制御半導体スピン量子コンピューターで解くには、

- 約50000個のスピンで量子ビット1つを表わさなければならない。
- 約10億個のスピンを1チップ上に実装し、その各々を99.99%の精度で個別に制御しなければならない。
- 各スピンを100ピコ秒以下の高速で制御できたとしても、計算には1～10日間もかかる。

量子誤り訂正コードで量子ビットを守る ー 過保護に育てられたひ弱な子供のように ー



クラスPとクラスNP



P: 決定性チューリングマシンにおいて多項式時間で解ける問題

NP: 非決定性チューリングマシンにおいて多項式時間で解ける問題

⇒ **P ≠ NP 予想**

NP完全: クラスNPに属し、クラスNPの全ての問題が多項式時間でこれに帰着される問題。

充足可能性問題(SAT)

ハミルトン閉路問題(巡回セールスマン問題の特殊例)

頂点被覆問題

など数千のNP完全問題がこれまで見つかった。

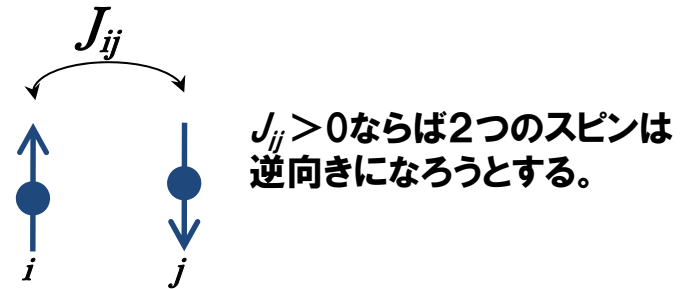
⇒ **全てのNP問題は多項式時間でNP完全問題へマッピングできる。**

イジング・マシーン

ある種の磁性体では、系のエネルギーはスピンの向きが(アップ、ダウン)のいずれか、によって以下のように決められる:

$$H = \sum_{i < j} J_{ij} \sigma_{iz} \sigma_{jz}$$

σ_{iz} : イジングスピン(+1:アップ、-1:ダウン)
 J_{ij} : 相互作用の強さ



1/2次元イジング・モデル ➡ クラスP

3次元イジング・モデル ➡ クラスNP完全

➡ 3次元イジング・モデルを多項式時間で解くマシーンが発見されたら、全てのNP問題は多項式時間で解ける。

レーザー・ネットワークでイジング・モデルを解けるか？

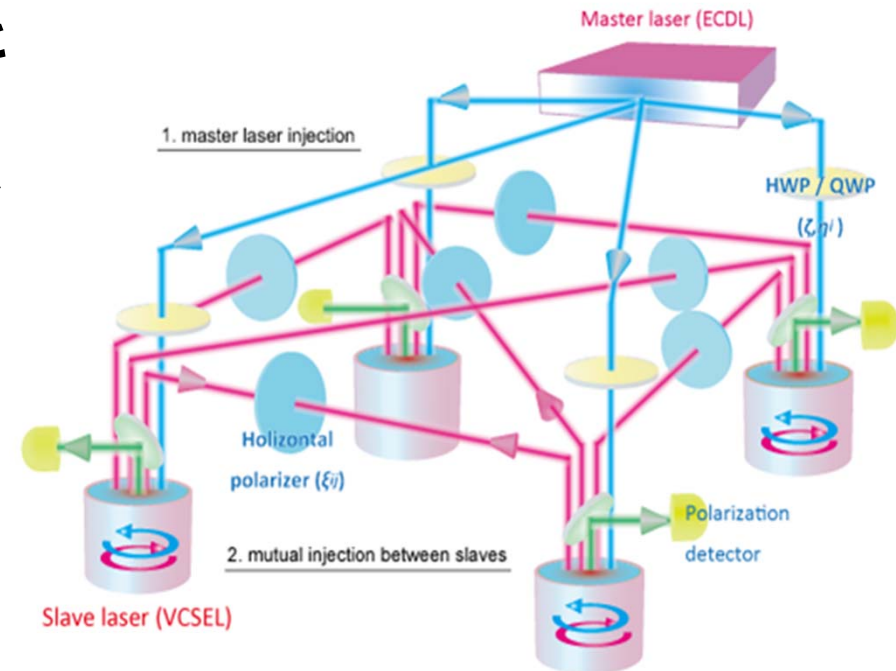


YES, 注入同期レーザーシステム！

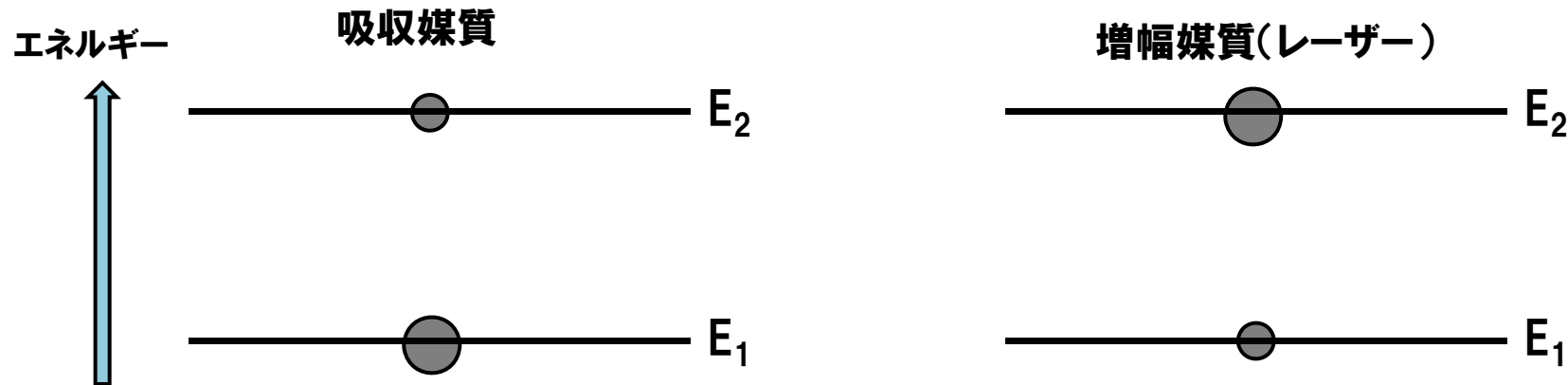


宇都宮聖子（NII助教）

- 干渉計(量子パラレリズム)
 - ➡ 全てのスレーブレザーを
マスターレーザー光の周波数と
位相に同期する
 - ➡ マスターレーザーからの光子は
全てのスレーブレザーに
同時に存在する。
- 相互注入(量子フィードバック)
 - ➡ J_{ij} をスレーブレザー間の
相互注入同期で実現する。
- 最小損失の偏光モード(イジング・
モデルの基底状態)が選択される。



負の温度



2準位原子が正の有限温度 $T (>0)$ にある時、2つのエネルギー準位 E_1 と E_2 を電子が占有する確率はボルツマン分布に従う:

$$\frac{P_1}{P_2} = \exp\left(\frac{E_2 - E_1}{k_B T}\right) > 1$$

$T > 0$ ➡ 正常分布

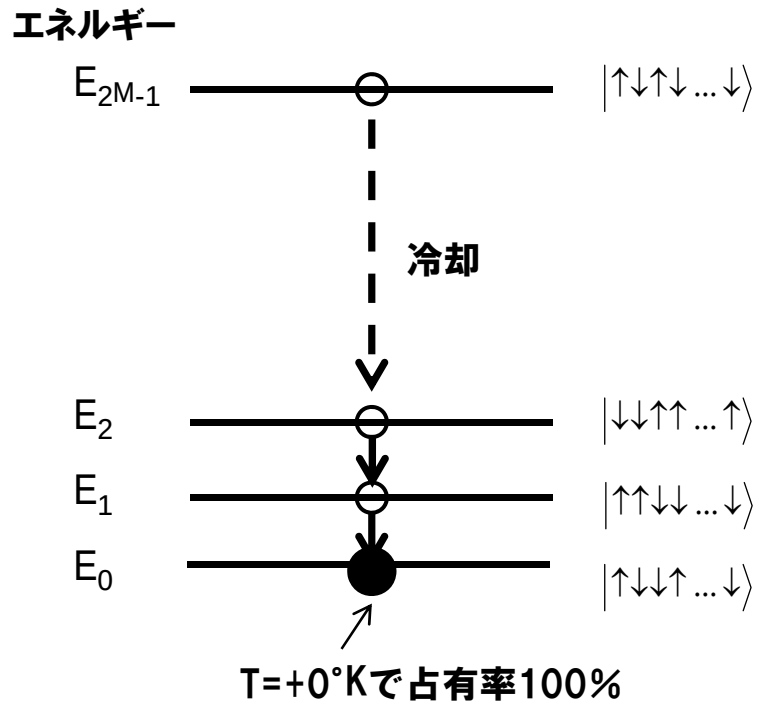
2準位原子に外部からエネルギーを注入(ポンピング)すると、電子がエネルギーの高い準位 E_2 を占有する確率を、エネルギーが低い準位 E_1 を占有する確率よりも大きくすることができる。

$$\frac{P_1}{P_2} = \exp\left(\frac{E_2 - E_1}{k_B T}\right) < 1$$

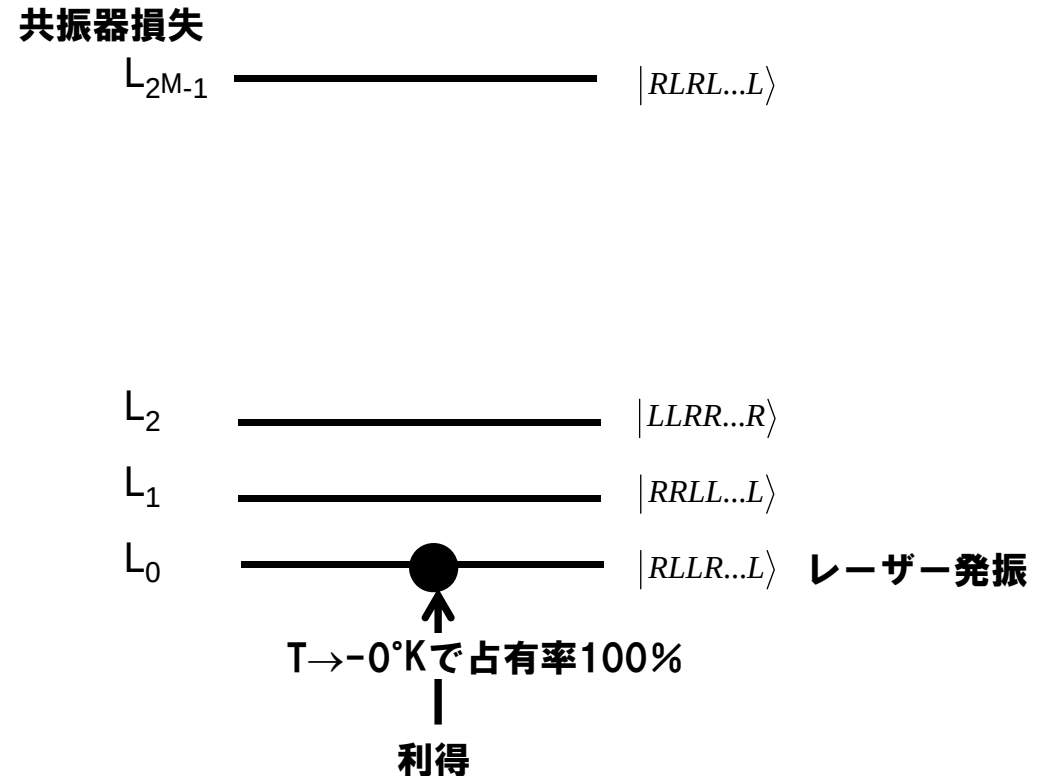
$T < 0$ ➡ 反転分布(負温度)

イジング・マシン: 2つの絶対零度

M個のスピンのエネルギー状態



M個のレーザー系の偏光状態



➡ M個のスピンの最低エネルギー状態は絶対(正)零度 ($T=+0^\circ\text{K}$)で実現される (実験的には困難)。

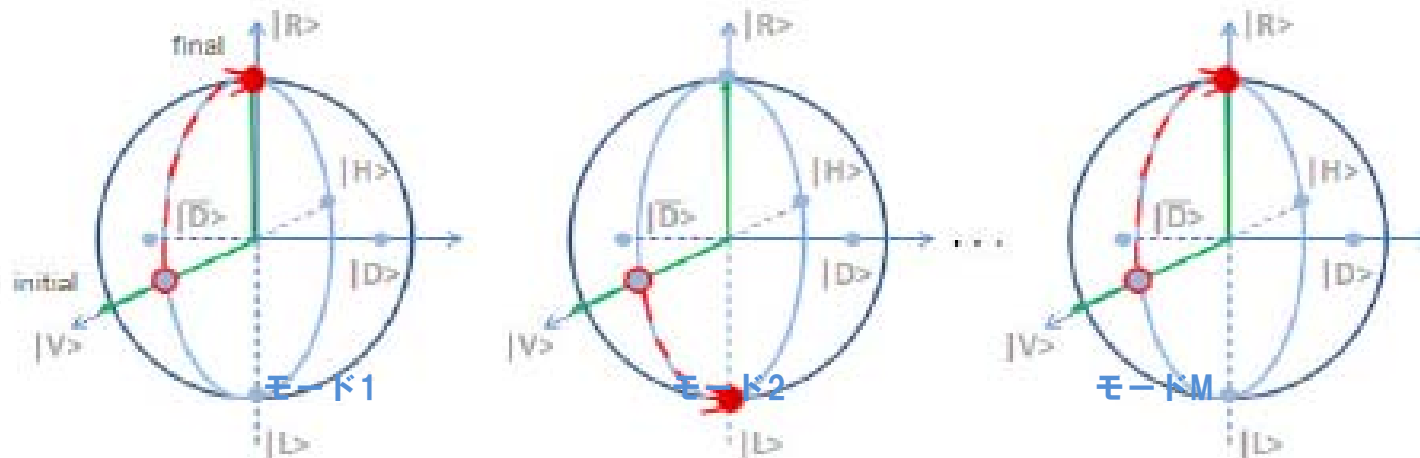
➡ M個の注入同期レーザーの最小損失偏光状態は絶対(負)零度 ($T=-0^\circ\text{K}$)で実現される (実験的には容易)。

量子進化論 (Quantum Darwinism)

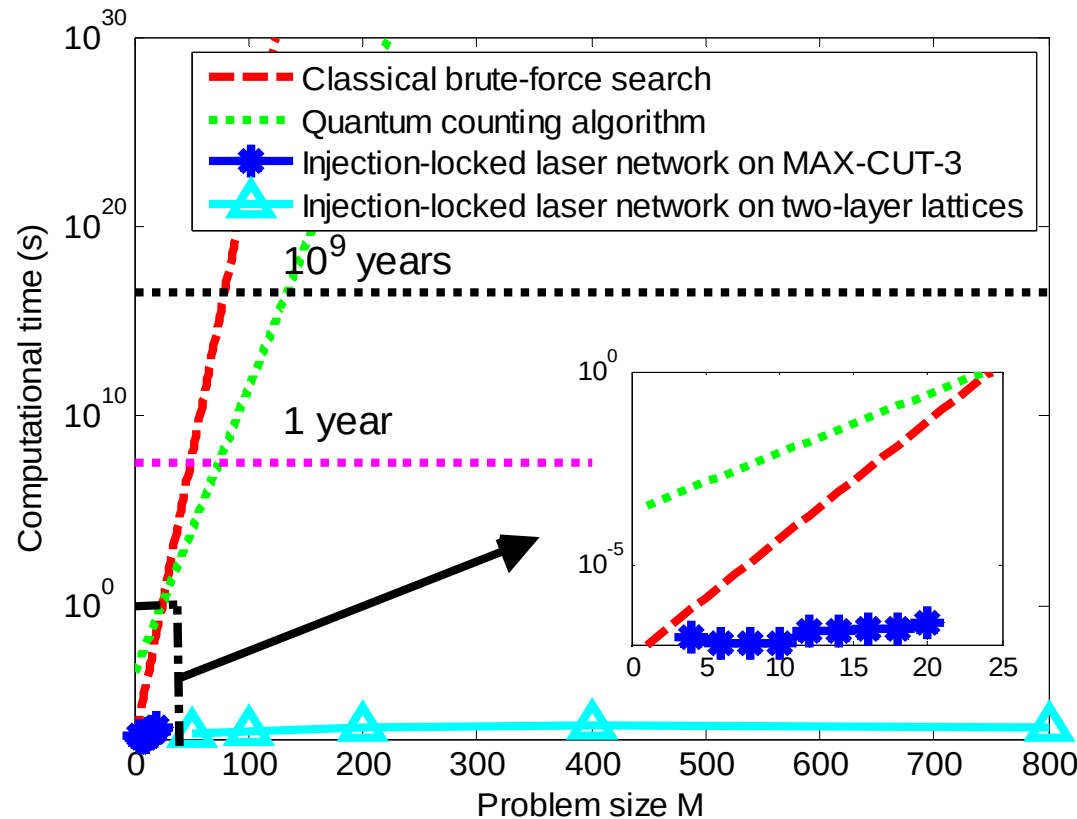
注入同期レーザーシステムは、まるで生き物のように与えられた環境でポピュレーション(光子数)を最大とするような特定の偏光状態を自ら見つけ出し、その生存競争に勝ち残った最適状態を実現し生存し続ける。この状態がイジング・モデルの解そのものである。



Charles Darwin
(1809-1882)



スーパーコンピューターが宇宙の寿命かかっても できない計算を一瞬で終わらせる？



高田健太(東大D1)



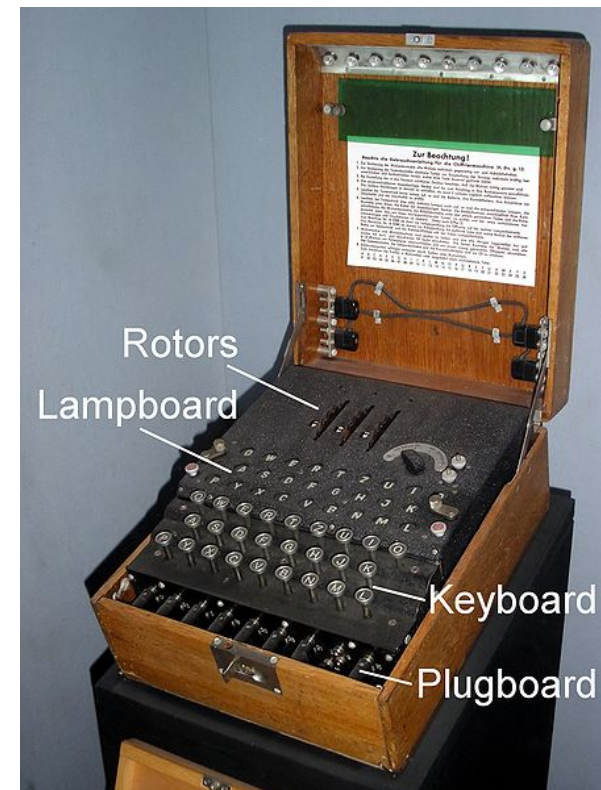
Kai Wen (Stanford Univ. D3)

提案したイジング・マシンの計算時間 $t_c \lesssim 1\mu\text{sec}$

➡ 提案した注入同期レーザー・ネットワークは(NP完全)イジング・モデルを多項式時間で解ける可能性を示している。

今日の結論

- 多スピン干渉計である量子コンピューターはすぐに実現できるようなものではない。現在はまだSFの世界である。
- 1光子干渉計に単純化した注入同期レーザー・ネットワークにはNP完全問題を多項式時間で解く可能性がある。(それが本当かどうか、その答えは5年後には明らかになっているはずである。)



Enigma