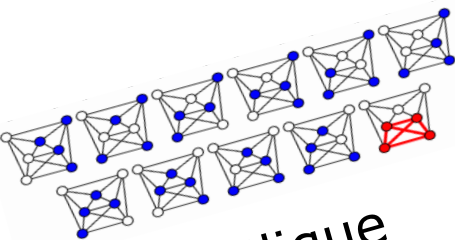
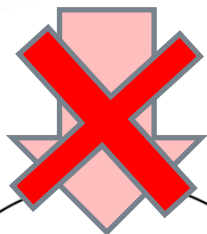


人工知能と量子コンピュータ

NP-完全問題とその含意



Clique



NP-complete

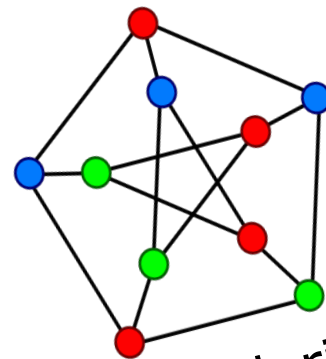
NP



Factoring

BQP

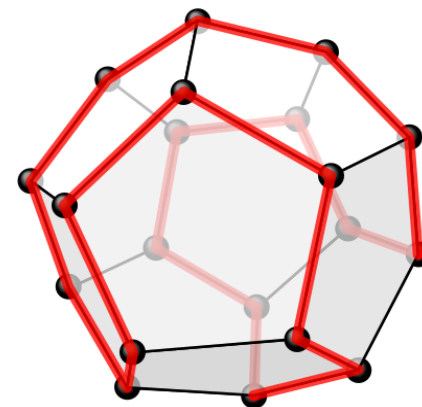
P



Graph Coloring

$$(l_1 \vee l_2 \vee x_2) \wedge$$
$$(\neg x_2 \vee l_3 \vee x_3) \wedge$$
$$(\neg x_3 \vee l_4 \vee x_4) \wedge \dots \wedge$$
$$(\neg x_{n-3} \vee l_{n-2} \vee x_{n-2}) \wedge$$
$$(\neg x_{n-2} \vee l_{n-1} \vee l_n)$$

3-SAT



Hamilton Path

はじめに

- 人工知能のもっとも基本的な問題の一つは、機械と人間にとっての「認識」の限界を正確に知ることであると僕は考えている。量子コンピュータの登場が、こうした問題にどのような新しい地平を切り開くのかということは、人工知能論にとっては大事な問題である。
- こうした観点から、量子コンピュータと量子複雑性理論については、これまでいくつかの機会で紹介してきたのだが、計算可能性理論や複雑性理論そのものについては、あまり語ってこれなかった。
- 今回は、第一部で、改めて複雑性理論の中核である「NP-完全」問題という不思議なコンセプトを説明しようと思う。「NP-完全」の発見なしには、複雑性理論は生まれなかったと言っている。その理論的インパクトは、計算可能性理論の創出にゲーデルの不完全性定理が与えたインパクトと同じものだと思う。

はじめに

- 「NP-完全」問題は、基本的に、力まかせの総当たりでやれば必ず解は見つかるはずというところが、どう頑張っても原理的に証明することが不可能な命題が存在することを主張する「不完全性定理」とは異なっている。
 - ただ、総当たりで問題を解くには、 n 個の条件が成り立つか否かというように問題を単純化しても、試すべき条件の組み合わせは、 2 の n 乗個になる。 n が小さいうちは(例えば、 $n=10$ なら、 1024 個の場合をチェックすればいい)なんとかなるのだが、 n が大きくなるにつれ、問題は、文字通り指数関数的に難しくなる。それは、総当たり法では、現実的には、全く手に負えない問題となる。
-

はじめに

- ❑ 量子コンピュータに対する期待の一つは、それが n -qubitの入力に対して、それに対応する 2^n 個の状態の演算を同時に実行することができるので、それをNP-完全問題の攻略に利用できるのではないかというものである。
- ❑ 量子コンピュータなら、NP-完全問題も解けると思っている人も少なくないのだが、それは誤解である。そんなにうまくはいかないのだ。その誤解を解くことが、「NP-完全」問題を、改めて取り上げた理由の一つである。
- ❑ それでは、複雑な、現実的には手に負えない問題は、量子コンピュータでも手が出ないのかというと、もちろん、そうではない。Shorの素因数分解アルゴリズムのように、古典的(普通のという意味)コンピュータでは、現実的には解けない問題を量子コンピュータは解くことができる。

はじめに

- それだけではないのだ。量子コンピュータを用いた高速化の研究は、驚くべき広がりを持って様々な分野で進んでいる。第二部では、近年の活発な量子アルゴリズムの研究の現状を、Q2BカンファレンスでのPreskillの講演をベースに紹介する。これは以前のマルレクでAppendixに回していた内容である。
 - 様々な応用とは独立に、個人的には、Shorのアルゴリズムの属するBQPという複雑性のクラスの一般化である「BQP-完全」というコンセプトに注目している。「BQP-完全」問題を解く量子デバイスを、我々はいつか手に入れると確信している。
 - その時、人間と機械の「認識」の限界についての我々の認識は、新しい段階に入ることになるだろう。
-

Agenda Part I

NP-完全問題とその含意

- 人間と機械の「認識可能性」の認識の拡大
- NP-完全問題 手におえない問題の存在
- Cook-Levin Theorem: SATはNP完全である
- Karp: 多項式時間で還元可能なNP完全問題
 - Clique 問題
 - Graph Coloring 問題
 - Hamiltonian Path 問題
- 実際に実装されているNP-完全問題のプログラム
- 量子断熱コンピュータとNP-完全問題
- 量子断熱コンピュータと量子ゲート型コンピュータとの「等価性」

Agenda Part II

広がる量子アルゴリズムの世界 -- BQP-完全問題とQRAM

- 量子組み合わせ最適化 QAOAとVQE
- 量子アニーリング
- 量子ディープラーニング
- QRAMと量子逆行列変換 HHLアルゴリズム
- QRAMとは何か？
- 半正定値プログラミング
- 量子リコメンデーション

Part I

NP-完全問題とその含意

人間と機械の 「認識可能性」の認識の拡大

前回の「まとめ」から

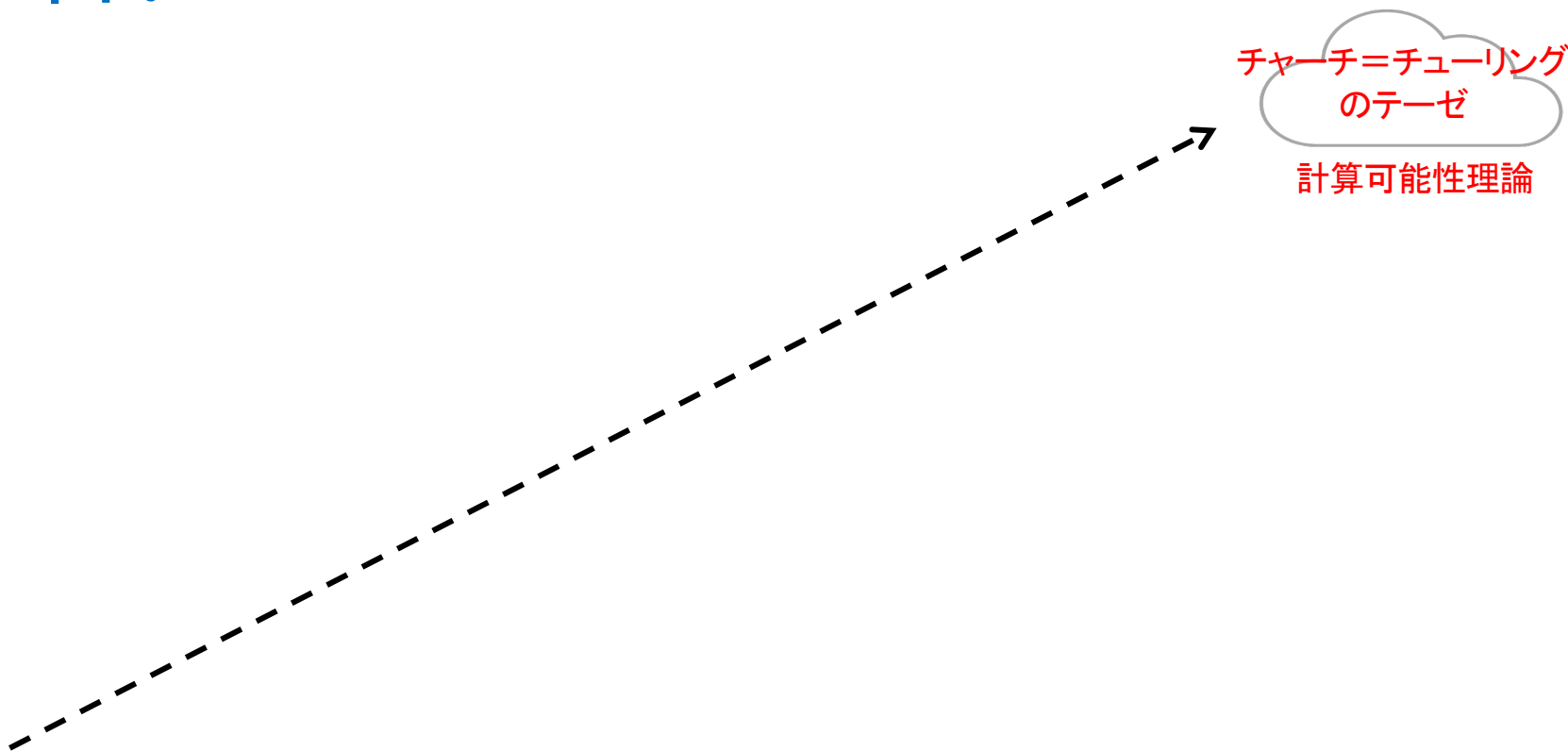
ここでの「前回」は、拙論「人工知能と複雑性理論」を指す

<https://www.marulabo.net/docs/20180927-kadokawa/>

人間と機械の認識の「限界」

- 「人工知能に何ができ、何ができないのか？」という問いを、「人間には何ができ、機械には何ができないのか？」という形の問いにしていけない。
- 人工知能にできることには限界がある。その限界について考えることも、人工知能研究の重要な課題だ。ただ、その限界について知ることは、計算主義的な人工知能観に立つ限りは、人間と機械の双方がともに持つ認識の限界について知ることである。それは、「計算」の限界について知ることだ。
- 人工知能は、その限界に従う。計算の限界については、計算の複雑性の理論が、多くのことを教えてくれる。

50年代



「証明可能＝計算可能」なものには限界があることは、
1950年代には、一般に認められるようになった。
ただ、それは、我々の認識の「限界」としては、非常に
荒い、かつ、抽象的で原理的な限界を与えるものでしかなかった。

70年代

P=NP?

計算複雑性理論

チャーチ=チューリング
のテーゼ

計算可能性理論



ただ、計算複雑性理論の基本問題である、「 $P = NP$? 問題」
(それは、「難しい計算」が「易しい計算」には還元できないこと
を主張する)が未解決のままなこともあり、この理論と人工
知能論との接点は、大きなものには広がらなかった。

80年代

P=NP?

計算複雑性理論

チャーチ=チューリング
のテーゼ

計算可能性理論

計算可能性概念の「物理化」
情報過程 = 物理過程

チャーチ=チューリング=ドイッチェ
のテーゼ

物理的計算可能性



80年代は、まだ、量子コンピュータは概念としてしか存在していなかった。「計算可能性」の物理化という画期的な変化も、まだまだ、抽象的な議論だった。

90年代

P=NP?
計算複雑性理論

チャーチ=チューリング
のテーゼ
計算可能性理論

計算可能性概念の「物理化」
情報過程=物理過程

チャーチ=チューリング=ドイッチェ
のテーゼ

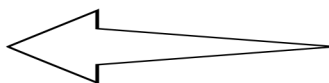
物理的計算可能性



拡大されたチャーチ=チューリング
のテーゼ



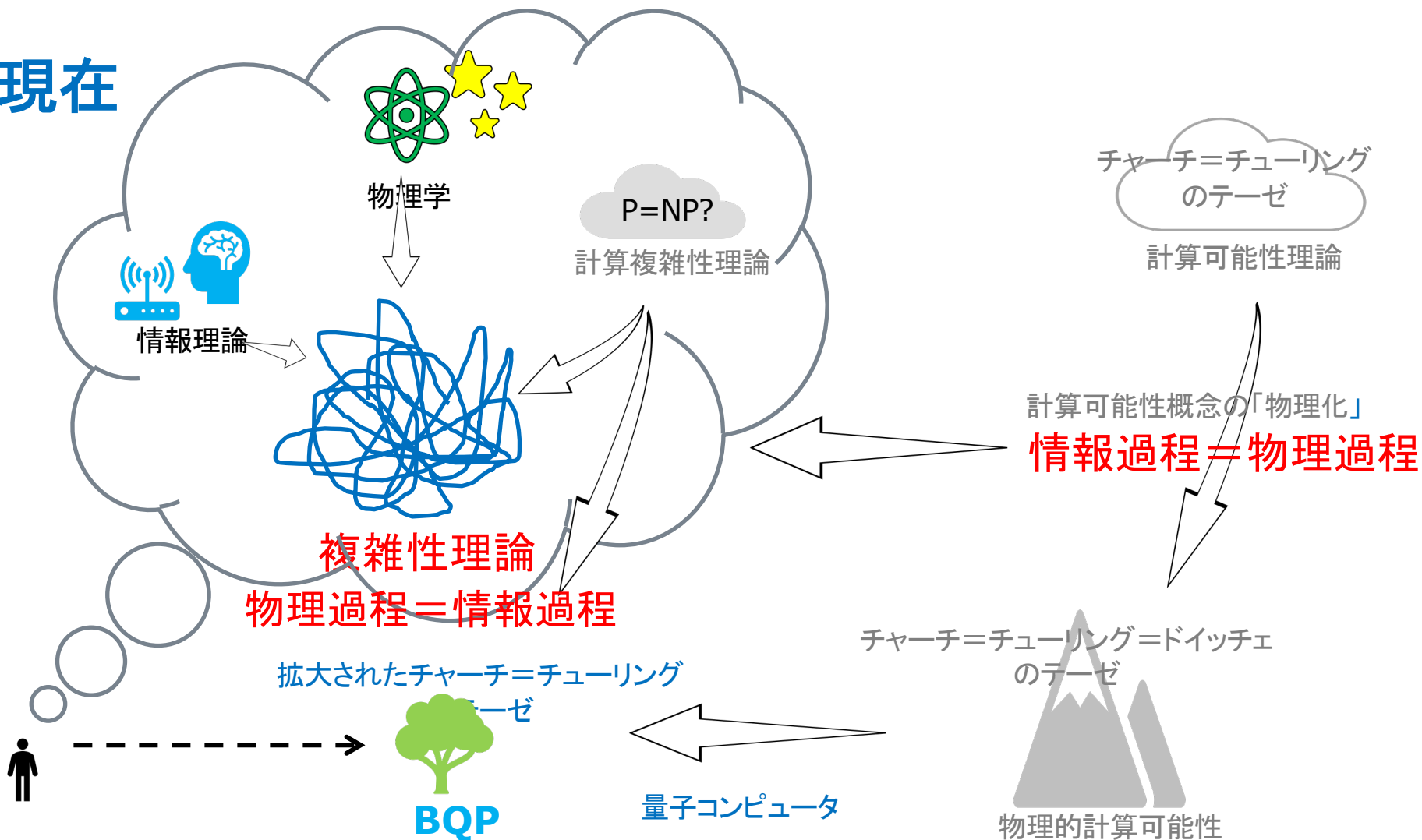
BQP



量子コンピュータ

量子複雑性の理論が登場し、BQPという新しい複雑性の概念が確立する。ショアのアルゴリズムは、広い関心をあつめた。

現在



計算の「限界」は、我々の身近の具体的な問題に近づいてきている。物理学の複雑性理論の発展もめざましい。

知りうることと知りえないこと
手におえることと手におえないこと

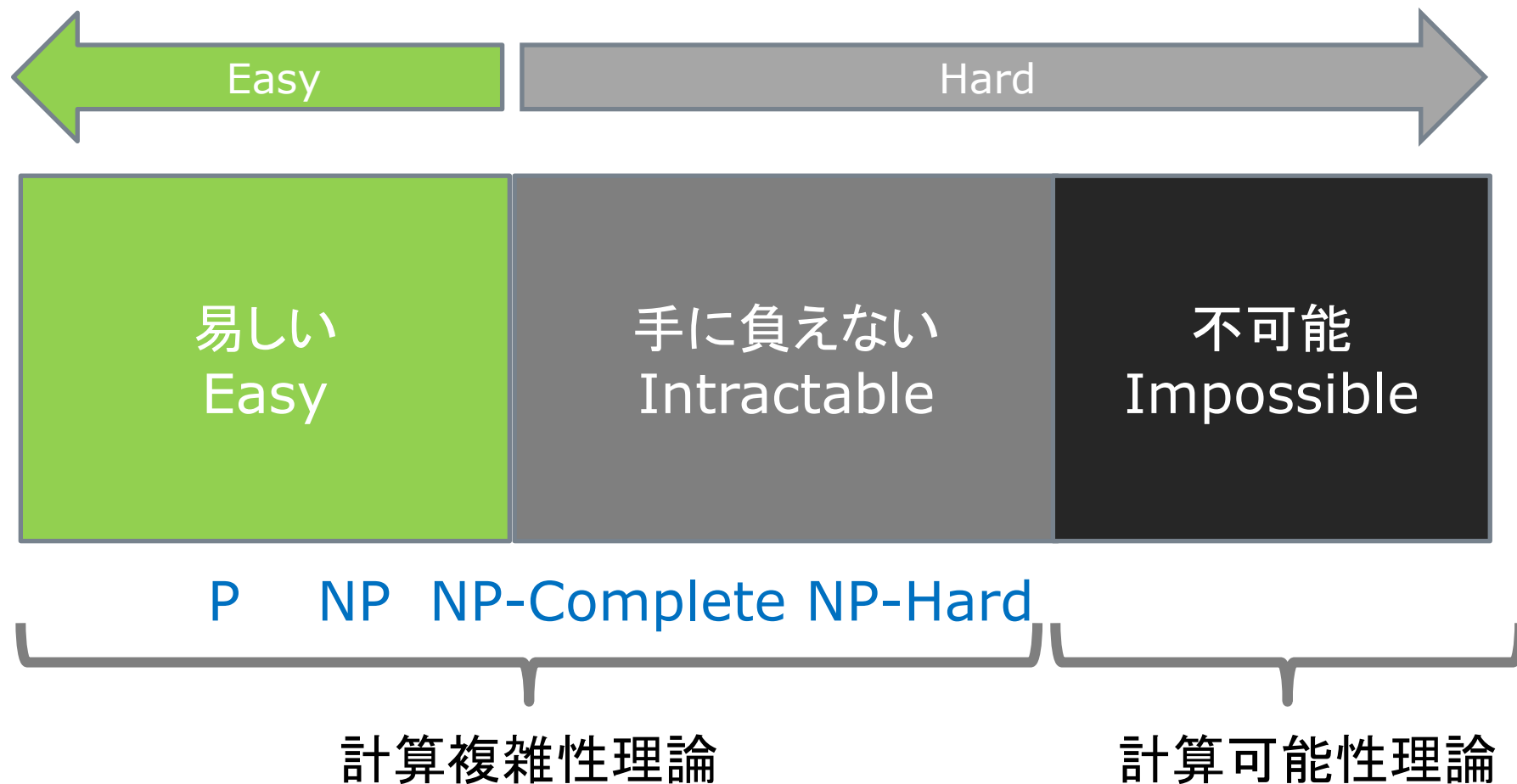
認識の易しさと難しさ

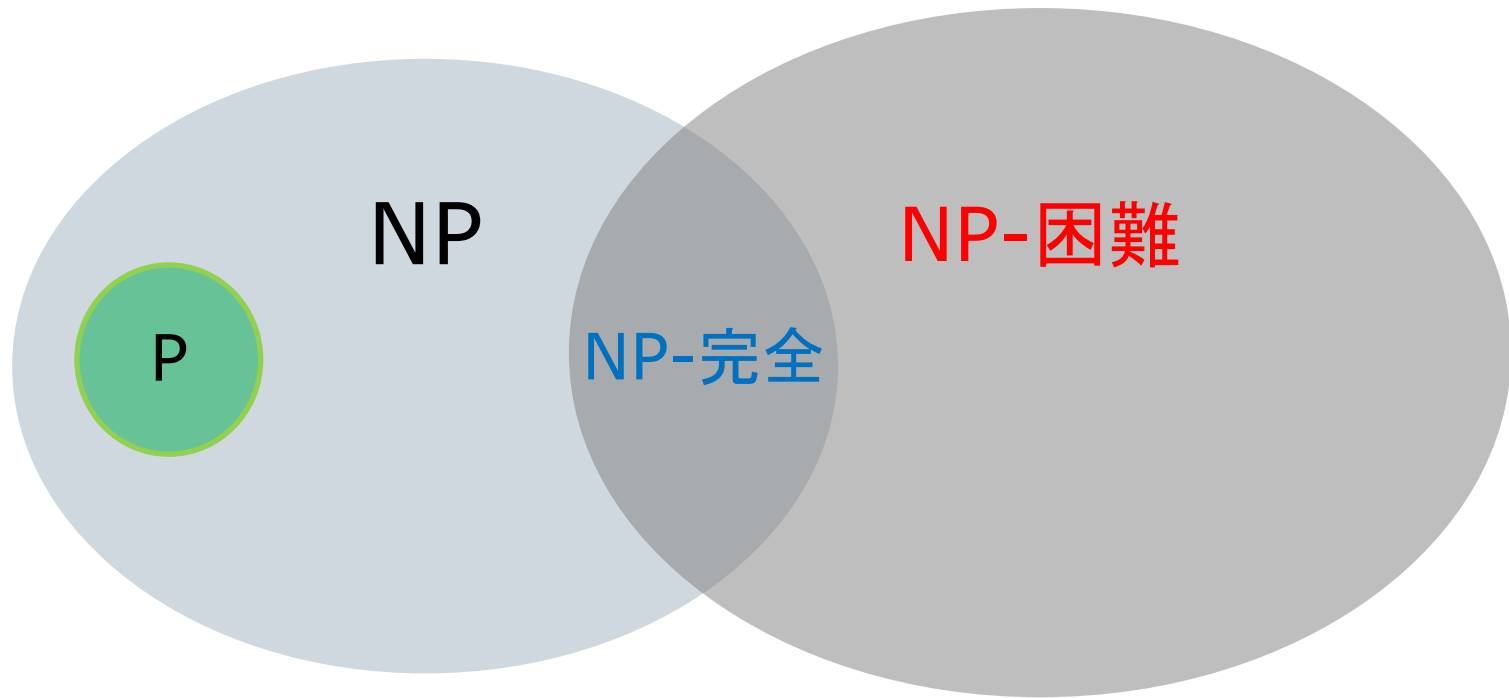
易しい
Easy

手に負えない
Intractable

不可能
Impossible

認識の易しさと難しさ





P: 多項式時間で解ける問題

NP: 多項式時間で解けるとは限らないが、
答えが正しいかは多項式時間でチェックできる問題

NP-困難: 全てのNP問題が、このクラスの問題に帰着される問題
(この帰着は多項式時間で行われなければならない)

NP-完全: NP問題で、かつ、NP-困難な問題

1994年、ショアは驚くべき発見をする。(論文は、1997年)

量子コンピュータでは、古典的なコンピュータでは指数関数的時間を要する素因数分解が、多項式時間で解けるという発見である。

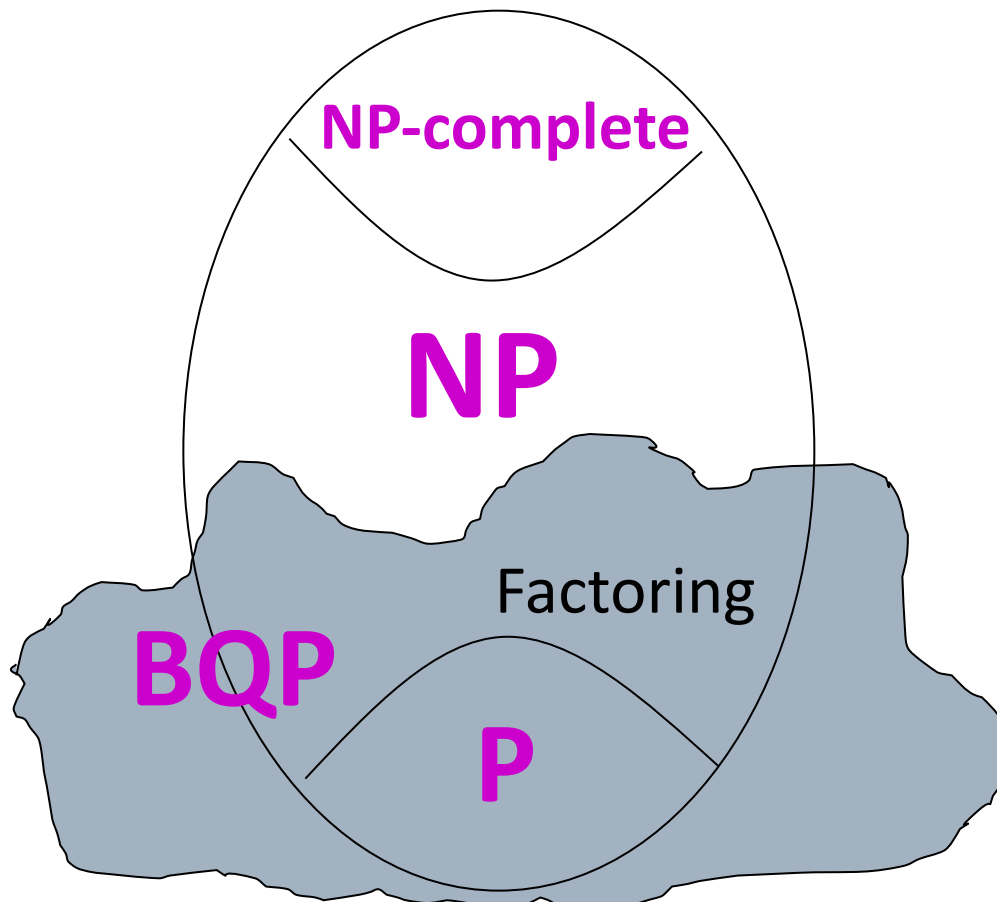
現代のセキュリティ技術の根幹部分が、RSA暗号のように素因数分解の困難性に基礎を置いている事情から、この「ショアのアルゴリズム」の発見は、コンピュータ・サイエンスの枠を超えた、社会的と言っていい大きな反響を呼び起こした。

*If computers that you build are quantum,
Then spies everywhere will all want 'em.
Our codes will all fail,
And they'll read our email,
Till we get crypto that's quantum, and daunt 'em.*

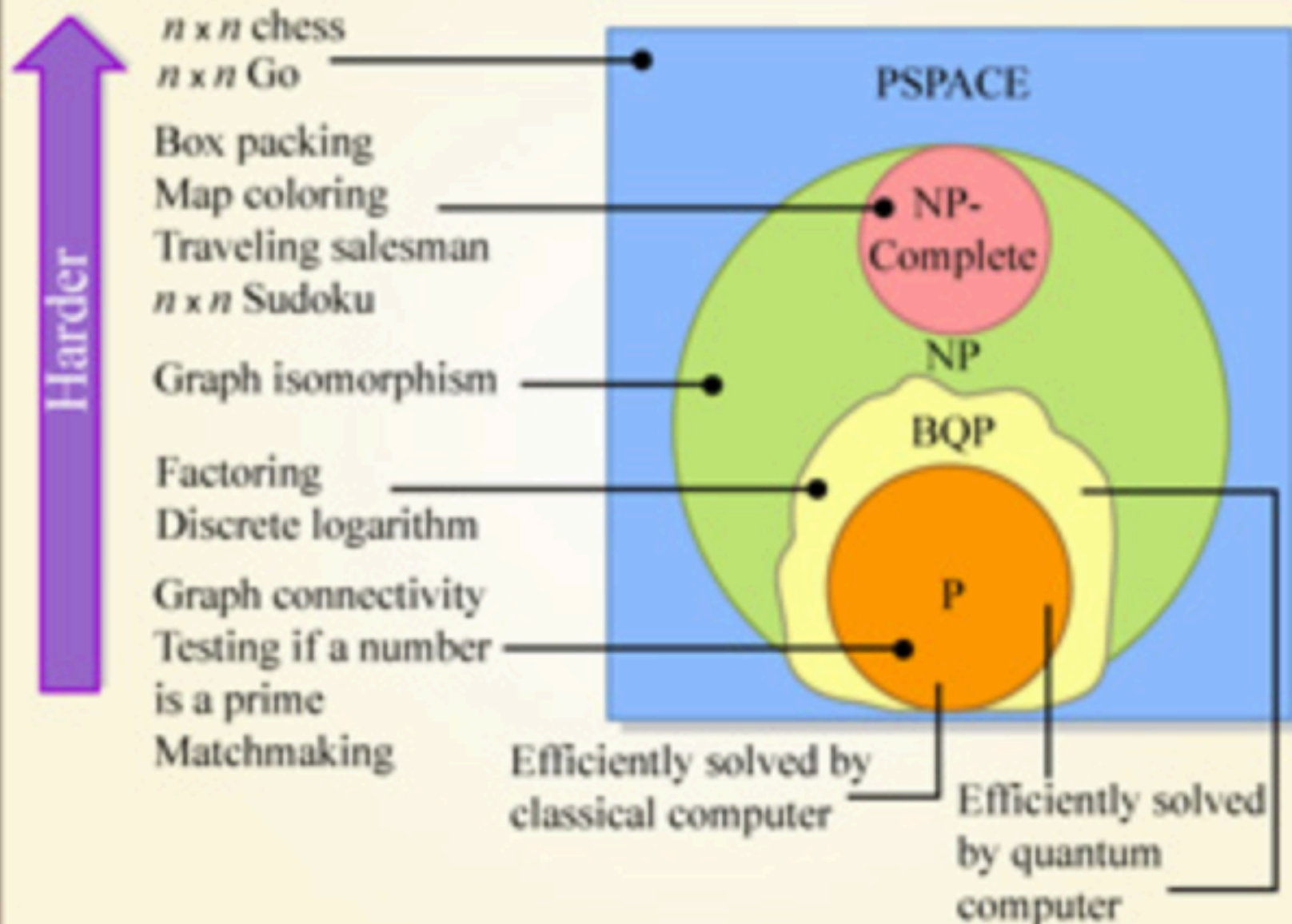
BQP (Bounded-Error Quantum Polynomial-Time): The class of problems solvable efficiently by a quantum computer, defined by Bernstein and Vazirani in 1993

Interesting

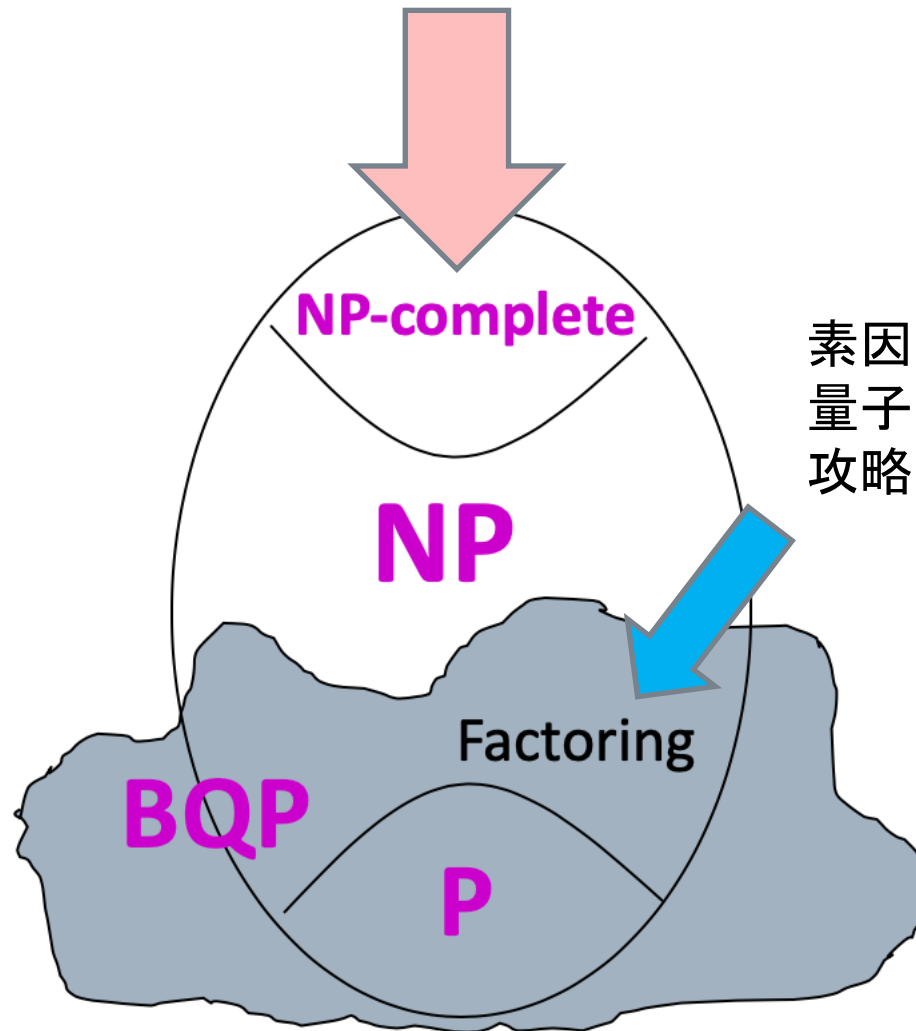
Shor 1994: Factoring integers is in **BQP**



Example Problems

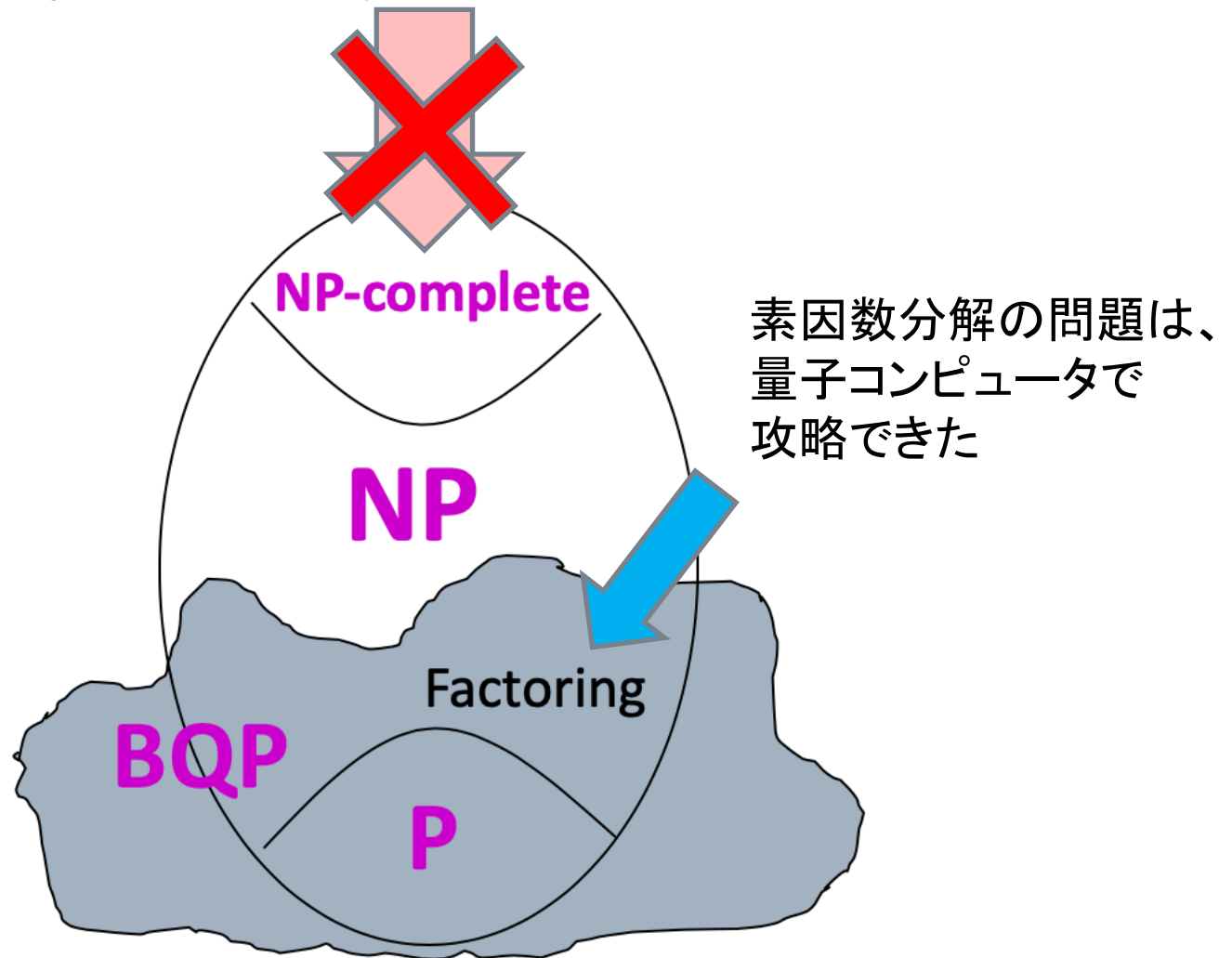


このクラスの問題を、量子コンピュータは、
攻略できるか？



素因数分解の問題は、
量子コンピュータで
攻略できた

NP-Completeの問題が一つでも多項式時間で解ければ、 $P=NP$ になる。 $P \neq NP$ だとすれば、原理的にそれは無理。



量子コンピュータの課題

量子アルゴリズムの原理的探求

- Shorのアルゴリズムのような、BQPに属する、指数関数的高速化が可能な問題の探求。**BQP-完全問題**。
- Groverの検索アルゴリズムのような、 $\sqrt{N}$ の高速化が可能な問題のクラスの探求。
- 量子ゲート型と量子アニーリング型の「等価性」の認識と、新しい量子デバイスの探求。
- 量子エラー訂正回路等、ノイズ耐性を持つ量子回路の探求。

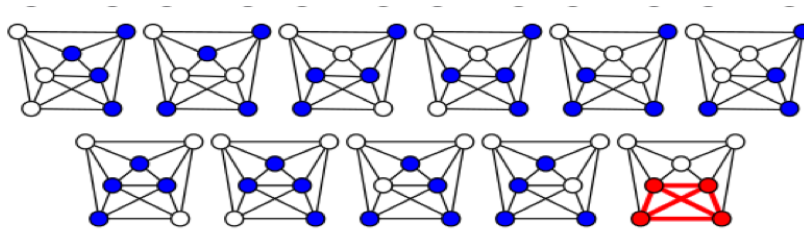
広がる量子アルゴリズムの世界

- 組合せ最適化問題での、厳密解ではなく近似解を求める量子アルゴリズムの研究。
- 量子アニーリング
- 量子ディープラーニング
- QRAMと量子逆行列変換
- 量子リコメンデーション
- 半正定値プログラミング
- ...
- ...
- 量子通信・量子暗号化

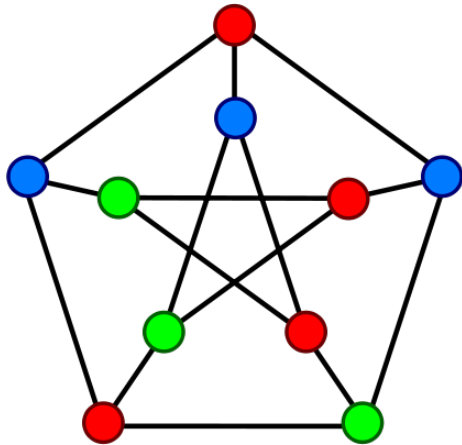
NP-完全問題

手におえない問題の存在

量子複雑性理論が、量子コンピュータの可能性とその限界を与える。複雑性理論の中心問題である $P=NP?$ 問題は、「NP-完全」問題の存在とその性質の理解に帰着する。この状況は、量子コンピュータの登場によっても変わることはない。ここでは、あらためて、人間と機械の認識能力にとって、手におえない(Intractable)である「NP-完全」問題について述べる。



Clique



Graph Coloring

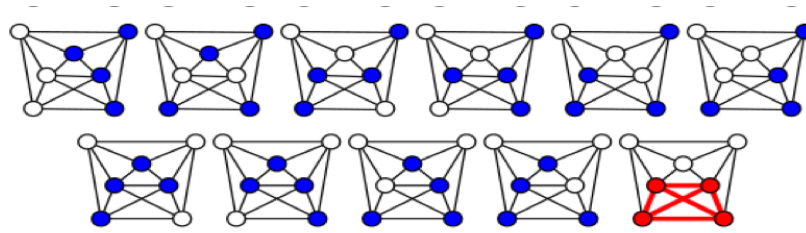
$$\begin{aligned}
 &(l_1 \vee l_2 \vee x_2) \wedge \\
 &(\neg x_2 \vee l_3 \vee x_3) \wedge \\
 &(\neg x_3 \vee l_4 \vee x_4) \wedge \cdots \wedge \\
 &(\neg x_{n-3} \vee l_{n-2} \vee x_{n-2}) \wedge \\
 &(\neg x_{n-2} \vee l_{n-1} \vee l_n)
 \end{aligned}$$

3-SAT



Hamilton Path

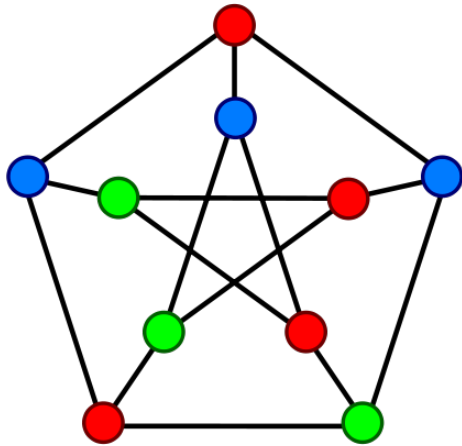
様々なNP-完全問題



Clique

$$\begin{aligned}
 &(l_1 \vee l_2 \vee x_2) \wedge \\
 &(\neg x_2 \vee l_3 \vee x_3) \wedge \\
 &(\neg x_3 \vee l_4 \vee x_4) \wedge \cdots \wedge \\
 &(\neg x_{n-3} \vee l_{n-2} \vee x_{n-2}) \wedge \\
 &(\neg x_{n-2} \vee l_{n-1} \vee l_n)
 \end{aligned}$$

3-SAT

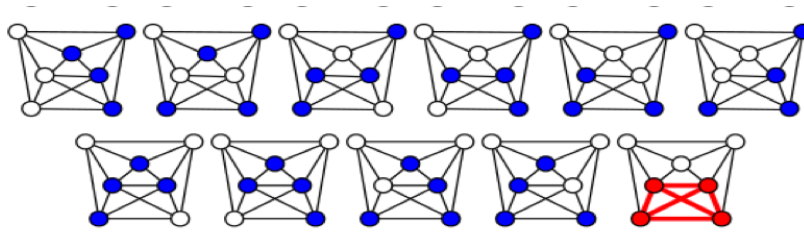


Graph Coloring

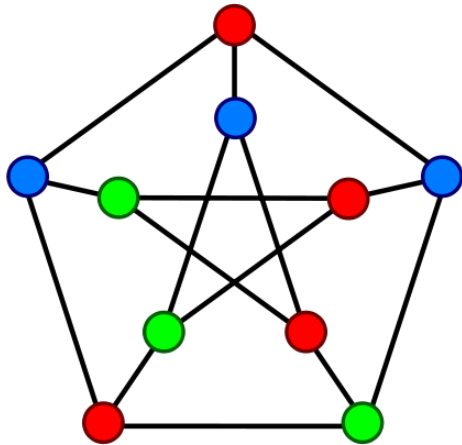


Hamilton Path

これらの問題は、解くのが難しい。もちろん、
力まかせに、総当たりでやれば解けるのだが、
それには指数関数的な膨大な時間がかかる。



Clique



Graph Coloring

$$\begin{aligned}
 &(l_1 \vee l_2 \vee x_2) \wedge \\
 &(\neg x_2 \vee l_3 \vee x_3) \wedge \\
 &(\neg x_3 \vee l_4 \vee x_4) \wedge \cdots \wedge \\
 &(\neg x_{n-3} \vee l_{n-2} \vee x_{n-2}) \wedge \\
 &(\neg x_{n-2} \vee l_{n-1} \vee l_n)
 \end{aligned}$$

3-SAT



Hamilton Path

しかも、この見かけは全く異なる、「現実的には手に負えない問題」は、すべて同一のアルゴリズムで、解くことができるのだ！

NP-完全問題の歴史

- 1971年、Cookは、充足可能性問題が、NP-完全であることを証明した。ここに初めて、NP-完全というコンセプトが登場する。（同じ頃、ソヴィエトの数学者Levinも同じ結果を得ている）現代の複雑性理論は、この発見から始まる。
- 1972年、Karpは、ある問題がNP-完全であることを証明する標準的な「還元」の手法を開発し、多くの問題がNP-完全であることを示した（「Karpの21の問題」）。
- このNP-完全問題のリストは、現在では数百の問題をカバーして拡大している。（例えば、“List of NP-complete problems” <https://goo.gl/XUSvRz> ）
- これらの問題の「手に負えなさ: “Intractability ”」は、例外的なものではなく、一般的なものである。
- Cookは1982年、Karpは1985年、Turing賞を受賞した。

NP完全問題の定義

- NP-complete problems are in NP, the set of all decision problems whose solutions can be verified in polynomial time; *NP* may be equivalently defined as the set of decision problems that can be solved in polynomial time on a non-deterministic Turing machine. A problem p in NP is NP-complete if every other problem in NP can be transformed (or reduced) into p in polynomial time.

P=NP?問題とNP完全問題の関係

- It is not known whether every problem in NP can be quickly solved—this is called the P versus NP problem.
- But *if any NP-complete problem can be solved quickly, then every problem in NP can*, ($P=NP$) because the definition of an NP-complete problem states that every problem in NP must be quickly reducible to every NP-complete problem (that is, it can be reduced in polynomial time). Because of this, it is often said that NP-complete problems are *harder* or *more difficult* than NP problems in general.

還元可能性 $\leq_p$ とNP-完全

- LとMを二つの言語(問題のこと)とする。LがMに、「還元可能」というのは、多項式時間で計算可能な関数 f が存在して、

$$x \in L \iff f(x) \in M$$

が成り立つことをいう。この関係を $L \leq_p M$ と表す。

- 関係 $\leq_p$ は、対称的で推移的である。
また、

$$L \leq_p M \text{ で、かつ、} M \in P \implies L \in P$$

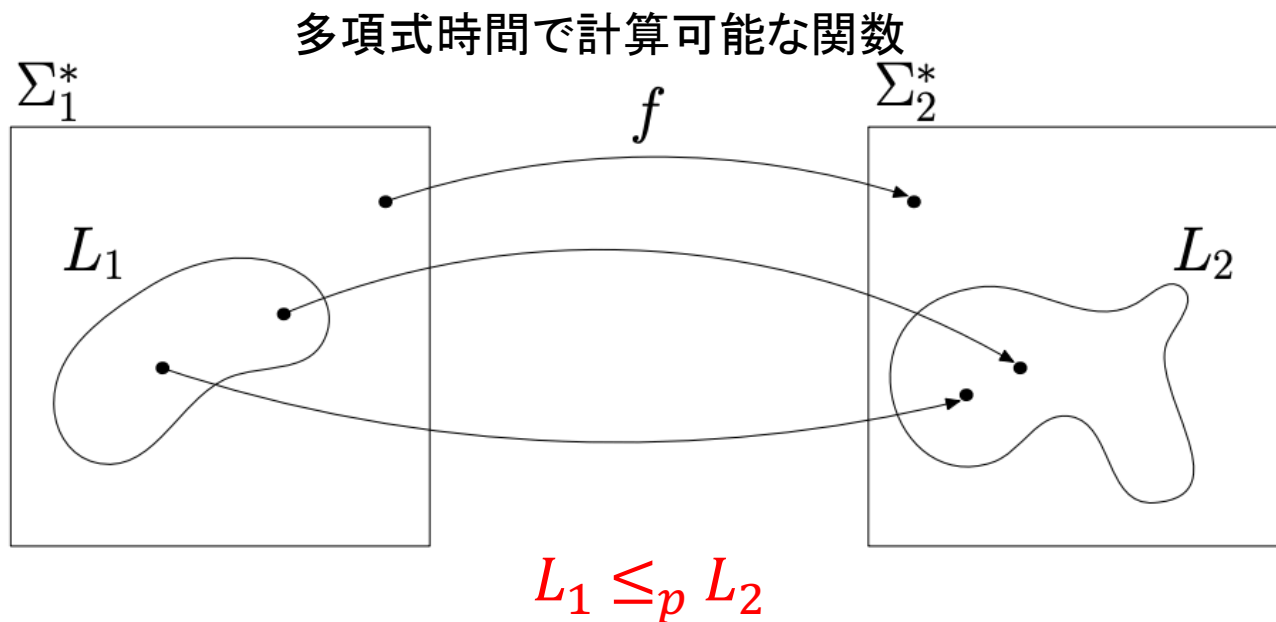
$$L \leq_p M \text{ で、かつ、} M \in NP \implies L \in NP$$

- LがNP-完全であるのは、次の二つの条件が成り立つ時

1. $L \in NP$

2. $L' \in NP$ である全ての N' について $L' \leq_p L$ (L はNP-Hard)

$$L_1 \leq_p L_2$$



- $x \in L_1 \Rightarrow f(x) \in L_2$
- $x \notin L_1 \Rightarrow f(x) \notin L_2$
- f computable in polynomial time

SAT 充足可能性問題

論理式

- 命題論理の「式」は、変数とAND($\wedge$)とOR($\vee$)とNOT($\sim$ あるいは $\neg$)と括弧から構成される。

例 $x_1 \vee x_2$ 、 $x_2 \wedge \sim x_3$ 、 $(x_1 \vee x_2 \vee \sim x_3) \wedge (\sim x_4 \vee x_5 \vee \sim x_6)$ は、論理式である。

- 論理式の値は、次のようにして計算できる。

$0 \wedge 0 = 0$	$0 \vee 0 = 0$	$\overline{0} = 1$
$0 \wedge 1 = 0$	$0 \vee 1 = 1$	$\overline{1} = 0$
$1 \wedge 0 = 0$	$1 \vee 0 = 1$	
$1 \wedge 1 = 1$	$1 \vee 1 = 1$	

ここでは、真は1、偽は0で表している。

リテラル、節、連言正規形

□ リテラル(Literal): 変数または変数の否定を「リテラル」と呼ぶ。
例 x_1 または $\sim x_1$ は、リテラルである。

□ 節(Clause): リテラルをOR($\vee$)で結合したものは「節」である。
例 $(x_1 \vee x_2 \vee \sim x_3)$ 、 $(\sim x_4 \vee x_5 \vee \sim x_6)$ は、節である。

□ 連言正規形(CNF: Conjunctive Normal Form):
式が、節をAND($\wedge$)で結合したものである時、CNFと呼ぶ。
例 $(x_1 \vee x_2 \vee \sim x_3) \wedge (\sim x_4 \vee x_5 \vee \sim x_6)$ は、CNFである。

充足可能性

- 全ての変数に、ある論理値T(真)あるいはF(偽)を割り当てた時、その式を真にできるような割り当てが存在する時、その式は「充足可能」という。
- $x_1 \vee x_2$ は、充足可能である。
 $x_1 = T, x_2 = T$ とすればいい。 $x_1 = T, x_2 = F$ でもいい。
- $x_2 \wedge \sim x_3$ は充足可能である。
 $x_2 = T, x_3 = F$ とすればいい。
- $(x_1 \vee x_2 \vee \sim x_3) \wedge (\sim x_4 \vee x_5 \vee \sim x_6)$ は、充足可能である。
- ある論理式Fが与えられた時、Fを真とする変数への真理値の割り当てが存在するか否かを決定する問題を充足可能性問題という。

N-SAT問題

- ある式 A が、CNFの形をしているとする。 A を構成する節が、高々 N 個のリテラルしか含まない時、 A の充足問題をN-SAT問題という。
- $x_1 \vee x_2$ の充足問題は、2SAT問題である。
- $x_2 \wedge \sim x_3$ の充足問題は、1SAT問題である。
- $(x_1 \vee x_2 \vee \sim x_3) \wedge (\sim x_4 \vee x_5 \vee \sim x_6)$ の充足問題は、3SAT問題である。

2-SAT問題の例

$$\begin{aligned} & (x_0 \vee x_2) \wedge (x_0 \vee \neg x_3) \wedge (x_1 \vee \neg x_3) \wedge (x_1 \vee \neg x_4) \wedge \\ & (x_2 \vee \neg x_4) \wedge (x_0 \vee \neg x_5) \wedge (x_1 \vee \neg x_5) \wedge (x_2 \vee \neg x_5) \wedge \\ & (x_3 \vee x_6) \wedge (x_4 \vee x_6) \wedge (x_5 \vee x_6). \end{aligned}$$

3-SAT問題の例

$$\begin{aligned} & (l_1 \vee l_2 \vee x_2) \wedge \\ & (\neg x_2 \vee l_3 \vee x_3) \wedge \\ & (\neg x_3 \vee l_4 \vee x_4) \wedge \cdots \wedge \\ & (\neg x_{n-3} \vee l_{n-2} \vee x_{n-2}) \wedge \\ & (\neg x_{n-2} \vee l_{n-1} \vee l_n) \end{aligned}$$

それぞれの節が、 n 個の選言 $l_1 \vee \cdots \vee l_n$ からなる n -SAT問題は、元の式には含まれない $n-2$ 個の新しい変数 $x_2, \cdots, x_{n-2}$ を導入して、それぞれの節 $l_1 \vee \cdots \vee l_n$ を上の形の節に変形して置き換えれば、この3-SAT問題は、元の n -SAT問題と同じ割り当てで充足可能になる。 n -SAT問題は、3-SAT問題に還元される。

3-SAT問題の例

$$\begin{aligned} & (l_1 \vee l_2 \vee x_2) \wedge \\ & (\neg x_2 \vee l_3 \vee x_3) \wedge \\ & (\neg x_3 \vee l_4 \vee x_4) \wedge \cdots \wedge \\ & (\neg x_{n-3} \vee l_{n-2} \vee x_{n-2}) \wedge \\ & (\neg x_{n-2} \vee l_{n-1} \vee l_n) \end{aligned}$$

それぞれの節が、 n 個の選言 $l_1 \vee \cdots \vee l_n$ からなる n -SAT問題は、元の式には含まれない $n-2$ 個の新しい変数 $x_2, \dots, x_{n-2}$ を導入して、それぞれの節 $l_1 \vee \cdots \vee l_n$ を上の形の節に変形して置き換えれば、この3-SAT問題は、元の n -SAT問題と同じ割り当てで充足可能になる。 n -SAT問題は、3-SAT問題に還元される。

3-SAT問題を解くアルゴリズム ただし、指数関数的時間で

- ある3-SAT問題に含まれる変数の数を n とする。
変数にランダムに値を割り当てて、それが式を充足するかチェックする。 n 個の全ての変数に、TまたはFという二つの値を割り当てる方法は、 2^n 個しか存在しないので、この手順を、最悪 2^n 回繰り返せば、充足可能か否かはわかる。
- このアルゴリズムは、 n について指数関数的な時間を要する。
多項式時間のアルゴリズムではない。

2-SAT問題は多項式時間で決定可能である

- ある2-SATの式の中の二つの節が、リテラル x とリテラル $\neg x$ を含んでいるとする。例えば、 $(a \vee b)$ と $(\neg b \vee \neg c)$ のように。
- この時、第三の節 $(a \vee \neg c)$ を考える。この節は、最初の二つの節の両方が真となる時に真となる。だから、最初の二つの節をこの第三の節で置き換えて、この2-SAT問題を考えることができる。
- このことは、次のように考えるとわかりやすい。
第一の節 $(a \vee b)$ を、それと論理的に同値な $\neg a \Rightarrow b$ に、
第二の節 $(\neg b \vee \neg c)$ を、それと論理的に同値な $b \Rightarrow \neg c$ に置き換える。この時、
第三の節 $(a \vee \neg c)$ すなわち、 $\neg a \Rightarrow \neg c$ は、次のようにして導かれる。
 $\neg a \Rightarrow b$ で $b \Rightarrow \neg c$ なら、 $\neg a \Rightarrow \neg c$ である。
- ここでは、 $x \Rightarrow y \equiv \neg x \vee y$, $x \equiv \neg \neg x$ を使っている。

2-SAT問題を解くアルゴリズム

- こうした置き換えを繰り返しおこなって、全ての節が、 $(x \vee x)$ あるいは $(\neg x \vee \neg x)$ の形になった時、この2-SATの問題は解ける。
- すなわち、全ての変数 x について、 $(x \vee x)$ あるいは $(\neg x \vee \neg x)$ のどちらか一方しか現れないのであれば、この式は充足可能である。 $(x \vee x)$ と $(\neg x \vee \neg x)$ が、同時に現れれば、この式は充足可能ではない。
- 2-SATの式が、 n 個の節からなっている時、このアルゴリズムは、 $O(n^3)$ の手順で問題を解くことができる。(第三の節の導出には $O(n^2)$ 、最後の整合性のチェックに $O(n)$ の手順が必要だから) よって、**2-SAT $\in P$**

Cook-Levin Theorem



Cook-Levin Theorem

SATはNP完全である

"The Complexity of Theorem Proving Procedures"

Stephen Cook (1971)

<https://www.cs.toronto.edu/~sacook/homepage/1971.pdf>

<https://dl.acm.org/citation.cfm?id=805047>

It is shown that any recognition problem solved by a polynomial time bounded nondeterministic Turing machine can be "reduced" to the problem of determining whether a given propositional formula is a tautology. Here "reduced" means, roughly speaking, that the first problem can be solved deterministically in polynomial time provided an oracle is available for solving the second. From this notion of reducible, polynomial degrees of difficulty are defined, and it is shown that the problem of determining tautologyhood has the same polynomial degree as the problem of determining whether the first of two given graphs is isomorphic to a subgraph of the second. Other examples are discussed. A method of measuring the complexity of proof procedures for the predicate calculus is introduced and discussed.

基本的なアイデア

全てのアルゴリズムは、論理式にコードできる

- SATは、NP問題である。なぜならば、変数へのあるブール値の割り当てが、式を充足するか否かは、多項式時間でチェックできるから。
- NPクラスのある決定問題が与えられたとしよう。その問題を多項式時間で解く、非決定論的なマシンを構成できたとする。
- その時、このマシンへのそれぞれの入力に対して、「この入力はマシンに渡され、マシンは正しく実行され、マシンは停止し、yesと答えた」と主張するブール値をとる論理式を構成する。
- そうすれば、このブール値をとる式は、このマシンが正しく実行されyesと答えた時、かつ、その時に限り充足されることになる。
- よって、構成された論理式の充足可能性は、このマシンがyesと答えるかと問うことと同値になる。

Proof of the Cook-Levin Theorem

- Already know $\text{SAT} \in \text{NP}$, so only need to show SAT is NP-hard.
- Let L be any language in NP. Let M be a NTM that decides L in time n^k .
- We define a polynomial-time reduction $f_L : \text{inputs} \rightarrow \text{formulas}$ such that for every w ,
 M accepts input w iff $f_L(w)$ is satisfiable
- **Proof Idea:**
 satisfying assignments of $f_L(w)$
 $\Leftrightarrow$ accepting computations of M on w

Describe computations of M by boolean variables:

- If $n = |w|$, then any computation of M on w has at most n^k configurations.
- Each configuration is an element of C^{n^k} , where $C = Q \cup \Gamma \cup \{\#\}$ (mark left and right ends with $\{\#\}$).
- computation depicted by $n^k \times n^k$ "tableau" of members of C .
- Represent contents of cell (i, j) by $|C|$ boolean variables $\{x_{i,j,s} : s \in C\}$, where $x_{i,j,s} = 1$ means "cell (i, j) contains s ".
- $0 \leq i, j < n^k$, so $|C| \cdot n^{2k}$ boolean variables in all Subformulas that verify the computation.

Express conditions for an accepting computation on w by boolean formulas

- φ_{cell} = “for each (i, j) , there is exactly one $s \in C$ such that $x_{i,j,s} = 1$ ”.
- φ_{start} = “first row equals start configuration on w ”
- φ_{accept} = “last row is an accept configuration on w ”
- φ_{move} = “every 2×3 window is consistent with the transition function of M ”

Completing the proof

- **Claim:** Each of above can be expressed by a formula of size of size $O((n^k)^2) = O(n^{2k})$, and can be constructed in polynomial time from w .
- **Claim:** M has an accepting computation on w if and only if $f_L(w) = \Phi_{\text{cell}} \wedge \Phi_{\text{start}} \wedge \Phi_{\text{accept}} \wedge \Phi_{\text{move}}$ has a satisfying assignment.
- Thus $w \rightarrow f_L(w)$ is a polynomial-time reduction from L to SAT.

Cook-Levin

Theorem: SAT is NP-complete.

Let $L \in NP$ and let M be a NTM that decides L in time $\leq p(n)$, where p is a polynomial.

Cook-Levin

Theorem: SAT is NP-complete.

Let $L \in NP$ and let M be a NTM that decides L in time $\leq p(n)$, where p is a polynomial.

	State	Pos	Ser 1		Ser n	...	Ser $p(n)$
Step 0	q_0	0	w_1	---	w_n	$\sqcup \dots$	$\sqcup$
Step 1				---			
Step 2							
Step $p(n)$	q_{accept}						

Cook-Levin

Theorem: SAT is NP-complete.

Let $L \in NP$ and let M be a NTM that decides L in time $\leq p(n)$, where p is a polynomial.

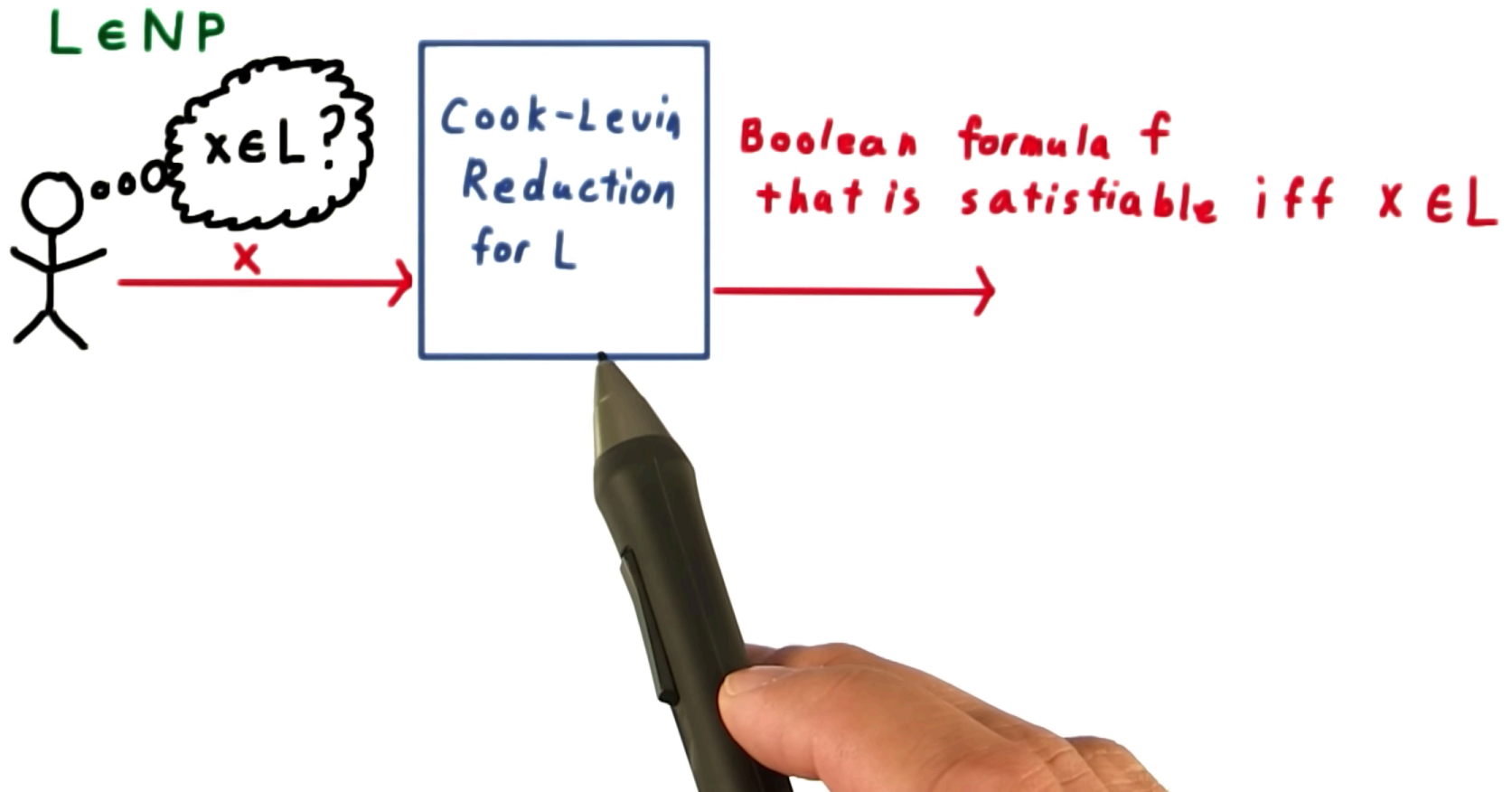
	State	Pos	Ser 1		Ser n	...	Ser $p(n)$
Step 0	q_0	0	w_1	---	w_n	$\sqcup \dots$	$\sqcup$
Step 1				---			
Step 2							
Step $p(n)$	q_{accept}						

Existence of
accepting computation

$\equiv$

Satisfying all
constraints on filling
out the table.

Cook-Levin Summary



Cook-Levin Summary



Is the reduction Correct?

$x \in L \Rightarrow f$ is satisfiable

Cook-Levin Summary

$L \in NP$



Is the reduction Correct? Yes!

$x \in L \Rightarrow f$ is satisfiable ✓

f is satisfiable $\Rightarrow x \in L$ ✓

1. Tableaux is well-defined
2. Starts in initial config.
3. Every transition is valid
4. Ends in accept config.

Cook-Levin Summary



Is the reduction Correct? Yes!

$x \in L \Rightarrow f$ is satisfiable ✓

f is satisfiable $\Rightarrow x \in L$ ✓

Is it polynomial?

1. Running time is polynomial in output formula length.
2. Output formula is polynomial in input length.

Configuration Clauses

Meaning

1. In exactly one state after each step.

$O(p(n) \log n)$ string length

2. Head in exactly one position after each step. $O(p(n)^3 \log n)$ string length

3. Each square has exactly one symbol after each step

$O(p(n)^2 \log n)$ string length

Clauses

of states
↑

$$(Q_{i0} \vee Q_{i1} \vee \dots \vee Q_{ir}) \forall i$$

$$(\overline{Q_{ij}} \vee \overline{Q_{ij'}}) \forall i \text{ and } \forall j \neq j'$$

$$(H_{i0} \vee H_{i1} \vee \dots \vee H_{ip(n)}) \forall i$$

$$(\overline{H_{ij}} \vee \overline{H_{ij'}}) \forall i \text{ and } \forall j \neq j'$$

$$(S_{ij0} \vee S_{ij1} \vee \dots \vee S_{ij|r|}) \forall i \text{ and } j$$

$$(\overline{S_{ijk}} \vee \overline{S_{ijk'}}) \forall i, \forall j, \forall k \neq k'$$

Configuration Clauses

Meaning

4. In initial configuration
at step 0.

$O(pn \log n)$ string length

5. Ends in a accepting
state. $O(\log n)$ string length

Clauses

(Q_{00}) q_0 is initial state

(H_{01}) Head over 1st square

$(S_{01k_1}) (S_{02k_2}) \dots (S_{0|w|k_{|w|}})$

(First part of tape contains
input string w)

$(S_{0|w|+1,0}) \dots (S_{0pn,0})$

(Rest of the tape is blank.)

$(Q_{p(w)y})$ q_y is the accepting
state

Transition Clauses

A tuple $(k, \ell, k', \ell', \Delta)$ is valid if $(q_{k'}, s_{\ell'}, \Delta) \in \delta(q_k, s_\ell)$.

For every step i , position j , and invalid $(k, \ell, k', \ell', \Delta)$ include in the formula the clause

$$(\overline{H_{ij}} \vee \overline{Q_{ik}} \vee \overline{S_{ij\ell}} \vee \overline{H_{i+1j+\Delta}} \vee \overline{Q_{i+1k'}} \vee \overline{S_{i+1j\ell'}})$$

if $\delta(q_k, s_\ell)$ applies,

the machine didn't follow an invalid transition.

$O(p(n)^2 \log n)$ string length

Cook-Levin Summary



Is the reduction Correct? Yes!

$x \in L \Rightarrow f$ is satisfiable ✓

f is satisfiable $\Rightarrow x \in L$ ✓

Is it polynomial? Yes!

1. Running time is polynomial in output formula length.
2. Output formula is polynomial in input length.

多項式時間で還元可能なNP完全問題

"Reducibility Among Combinatorial Problems"

Richard M Karp 1972

<https://people.eecs.berkeley.edu/~luca/cs172/karp.pdf>

A large class of computational problems involve the determination of properties of graphs, digraphs, integers, arrays of integers, finite families of finite sets, boolean formulas and elements of other countable domains. Through simple encodings from such domains into the set of words over a finite alphabet these problems can be converted into language recognition problems, and we can inquire into their computational complexity. It is reasonable to consider such a problem satisfactorily solved when an algorithm for its solution is found which terminates within a number of steps bounded by a polynomial in the length of the input. Many problems with wide applicability – e.g., set cover, knapsack, hitting set, max cut, and satisfiability – lack a polynomial algorithm for solving them, but also lack a proof that no such polynomial algorithm exists. Hence, they remain “open problems.”

<https://goo.gl/r9wf6w>

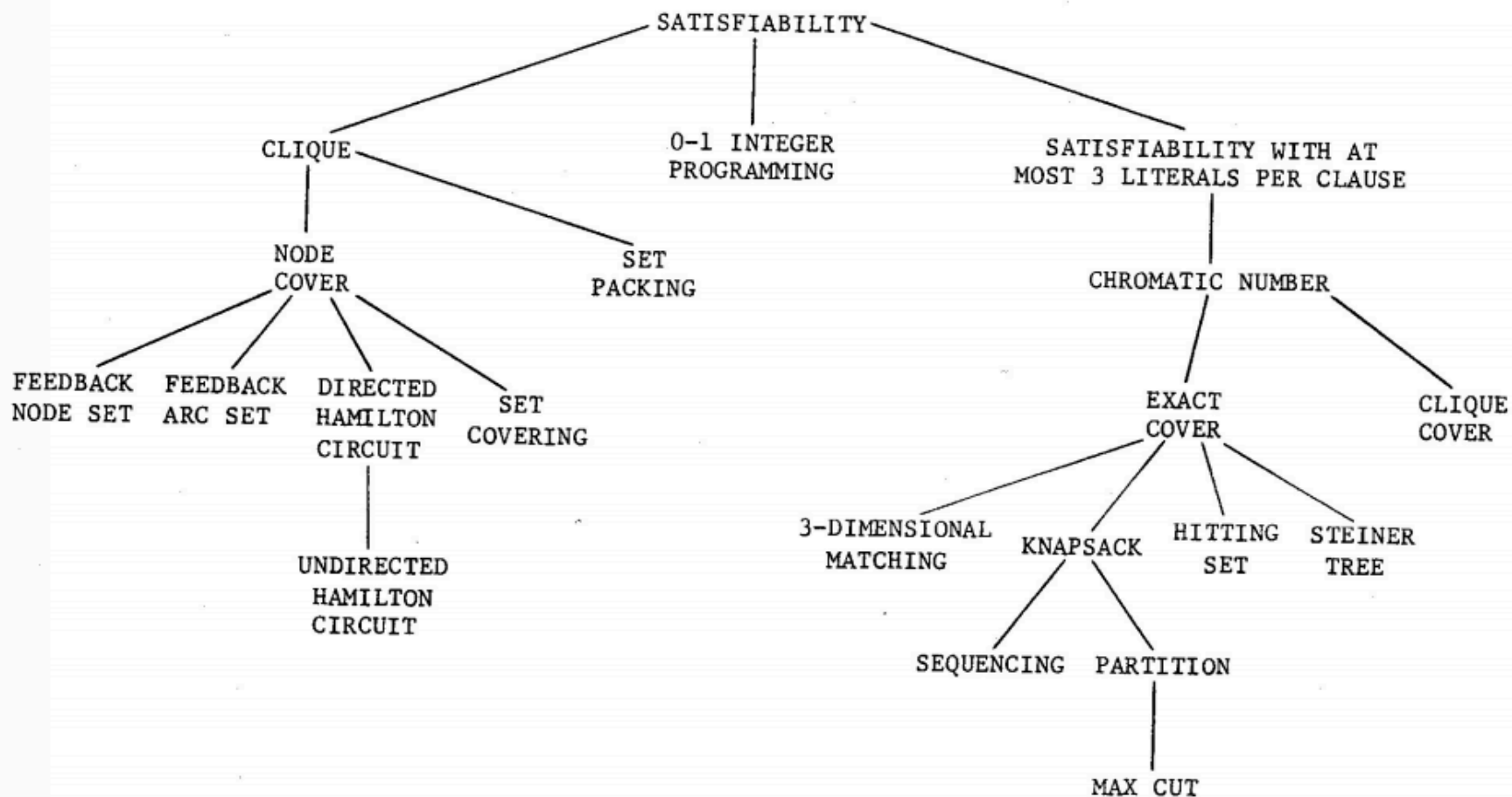


FIGURE 1 - Complete Problems

Karp's 21 NP-complete problems

- **Satisfiability**: the boolean satisfiability problem for formulas in conjunctive normal form (often referred to as SAT)
- **0–1 integer programming** (A variation in which only the restrictions must be satisfied, with no optimization)
- **Clique** (see also independent set problem)
 - **Set packing**
 - **Vertex cover**
 - **Set covering**
 - **Feedback node set**
 - **Feedback arc set**
 - **Directed Hamilton circuit** (Karp's name, now usually called **Directed Hamiltonian cycle**)
 - **Undirected Hamilton circuit** (Karp's name, now usually called **Undirected Hamiltonian cycle**)

Karp's 21 NP-complete problems

- **Satisfiability with at most 3 literals per clause** (equivalent to 3-SAT)
- **Chromatic number** (also called the Graph Coloring Problem)
 - **Clique cover**
 - **Exact cover**
 - **Hitting set**
 - **Steiner tree**
 - **3-dimensional matching**
 - **Knapsack** (Karp's definition of Knapsack is closer to Subset sum)
 - **Job sequencing**
 - **Partition**
 - **Max cut**

<https://goo.gl/56qLWk>

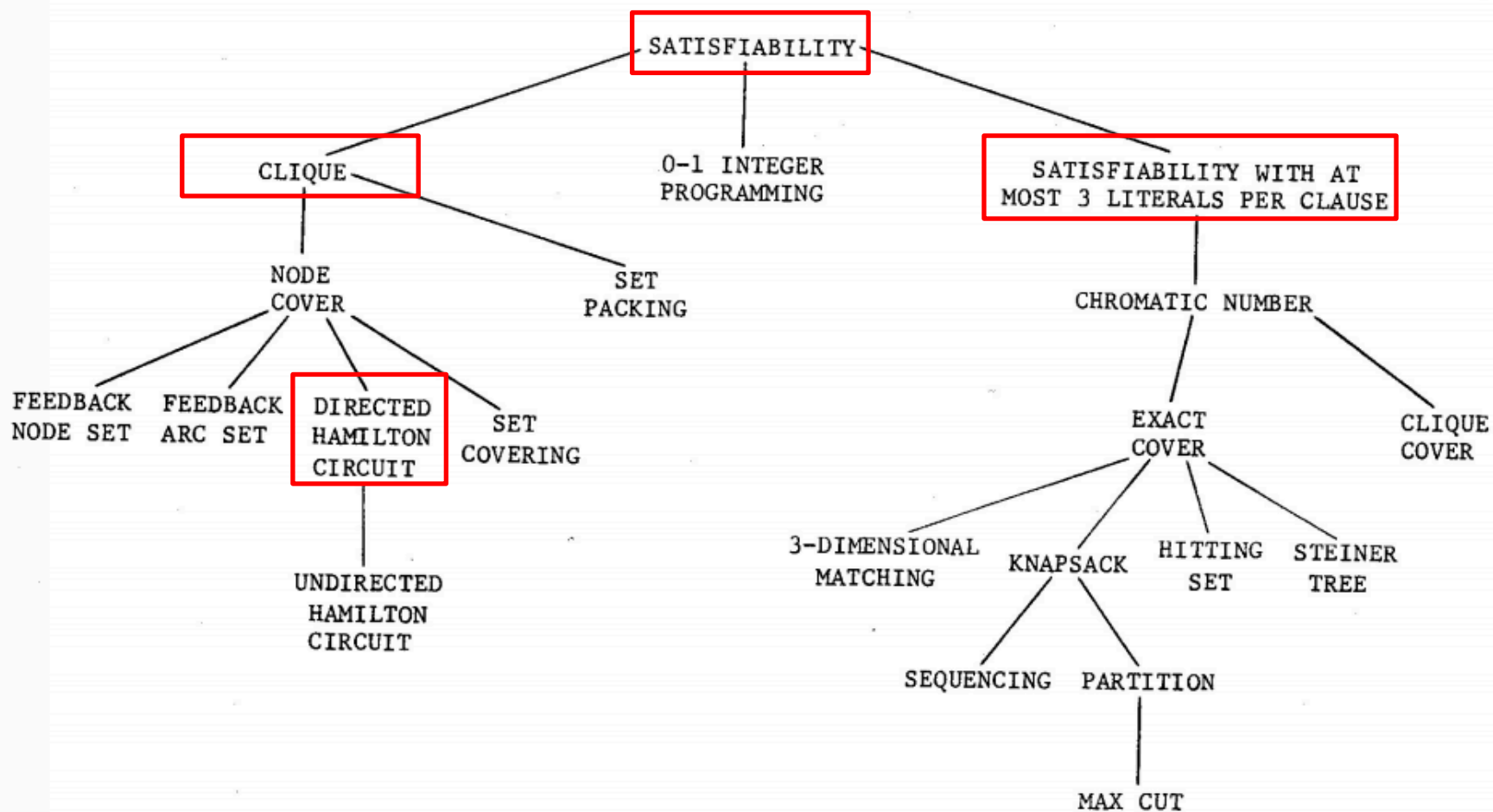


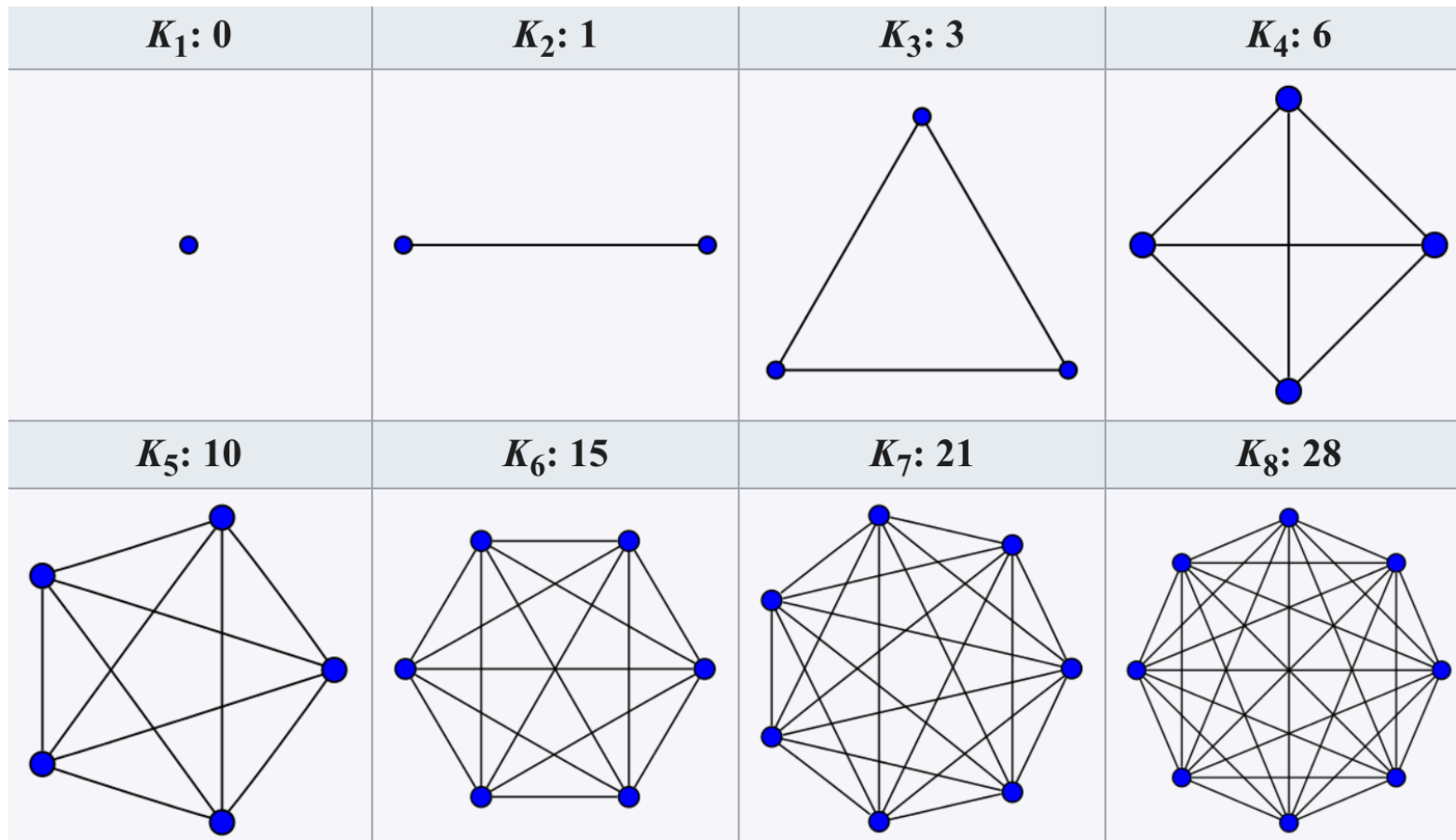
FIGURE 1 - Complete Problems

Clique問題

Cliqueとは？

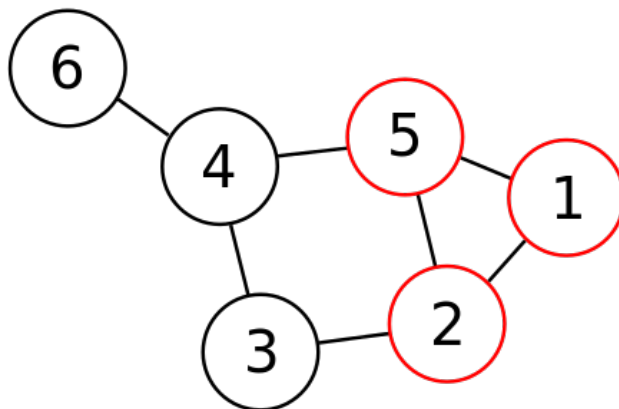
- Cliqueは、「一派」とか「派閥」を表す言葉である。例えば、あるSNS上で、全員がお互いに「友達」であるような個人のグループをCliqueと呼ぶ。
- 個人をグラフ上のノードとし、友達関係にある個人をエッジで結ぶことにすると、全員がお互いに「友達」であるような個人のグループは、全てのノードがエッジで結びついているグラフで表現される。
- こうしたグラフを「完全グラフ」という。

完全グラフの例

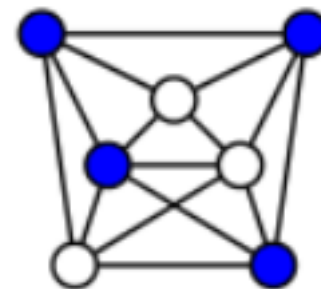


Clique問題

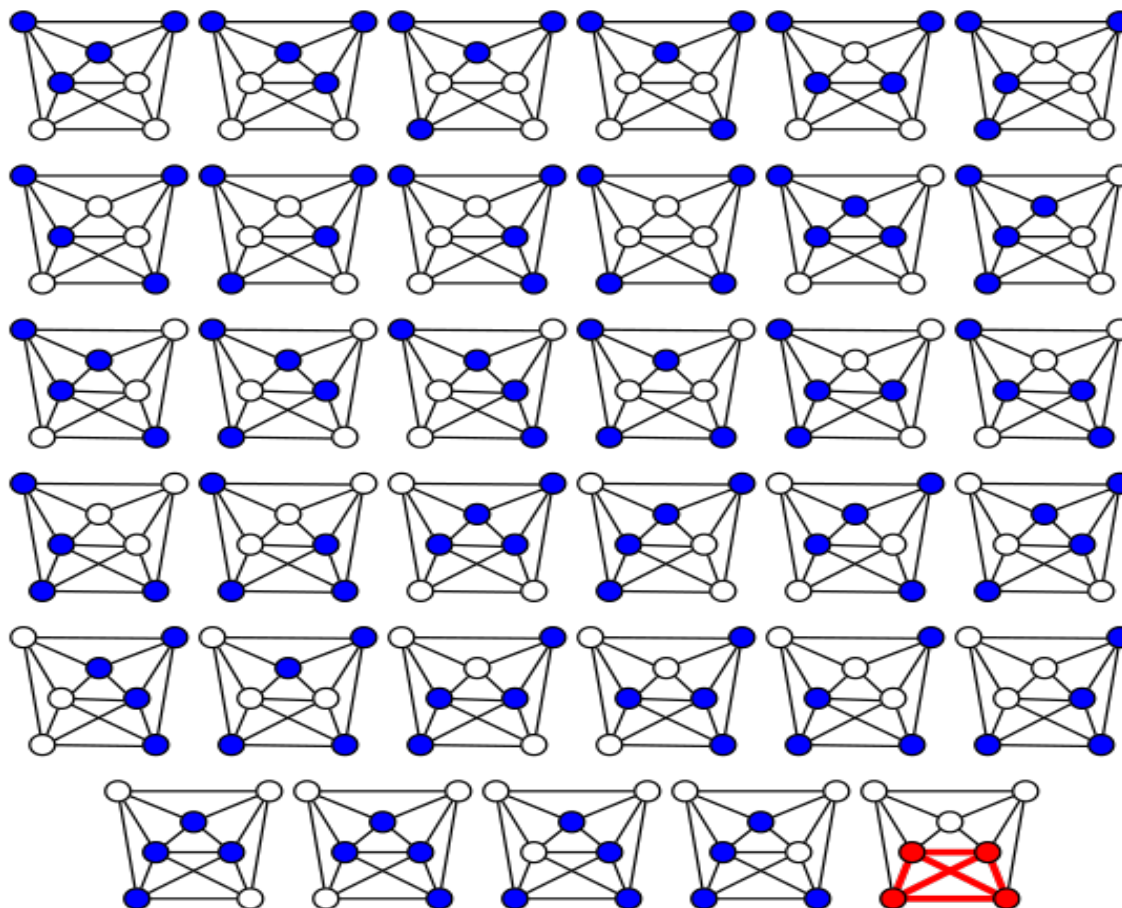
- あるグラフGと、ある整数kが与えられた時、Gの部分グラフでサイズがkの完全グラフが存在するか否かという問題をClique問題という。
- 例えば、次のグラフは、サイズ3の完全グラフ(1,2,5)を含んでいる。



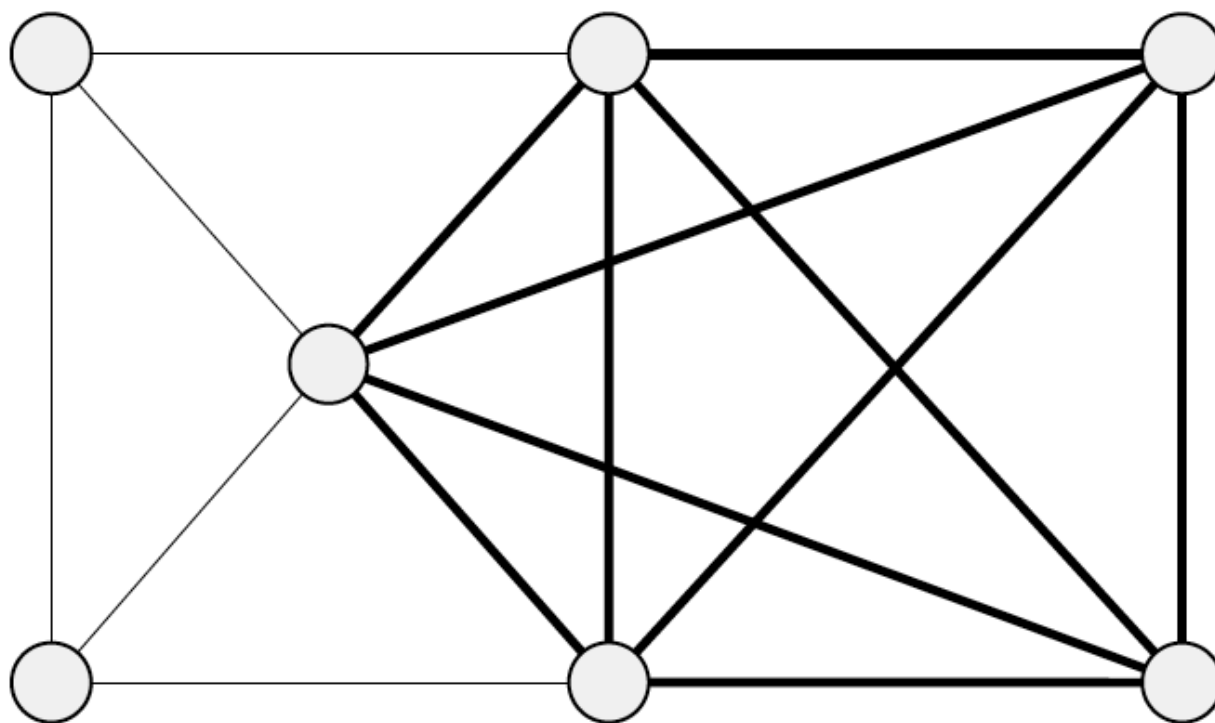
- 次のグラフに、サイズ4のCliqueは存在するだろうか？



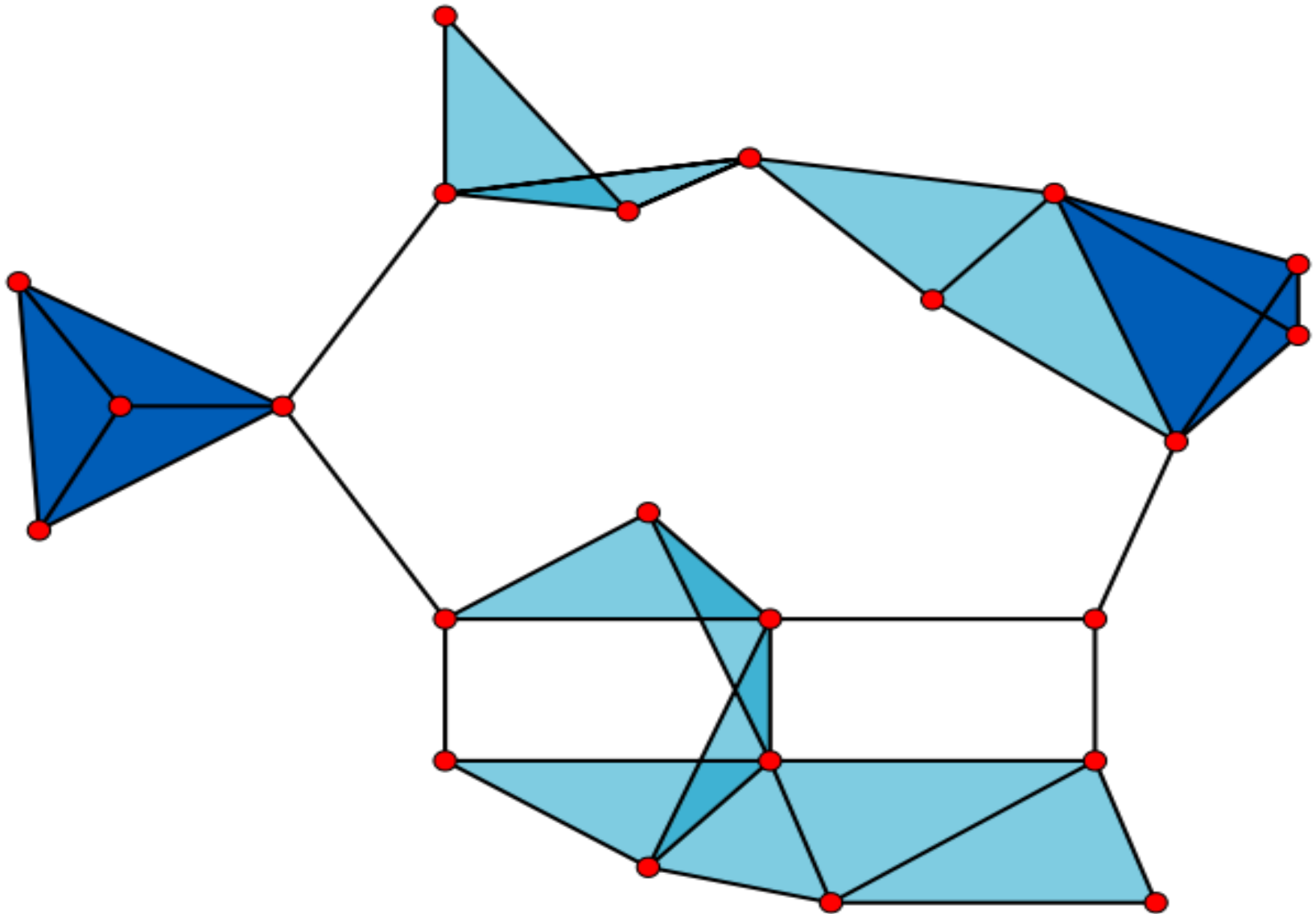
Clique問題 - 総当たり



5-cliqueの例



Clique問題の例



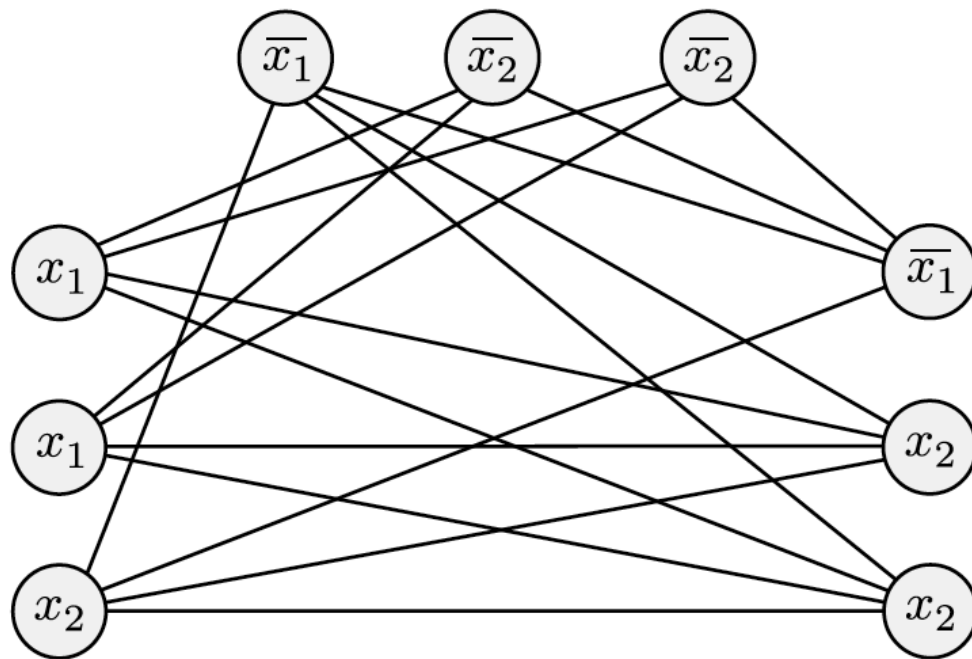
3-SAT問題をグラフで表現する

- φ をk個の節を持った次のような式だとしてよう。
$$\varphi = (a_1 \vee b_1 \vee c_1) \wedge (a_2 \vee b_2 \vee c_2) \wedge \cdots \wedge (a_k \vee b_k \vee c_k)$$

この式に、次のようにグラフGを対応づける。
- Gは、三つのノードの組(triple) $t_1, t_2, \dots, t_k$ のk個の集まりとしてよう。tripletは、 φ の一つの節に対応している。またtripletの中のノードは、対応する節のリテラルに対応している。
- Gのエッジは、次の二つの場合を除いて、全てのノードを結びつけている。Gのノードで線が引かれない場合は次の二つである。
 1. ノードが、同じtripletに属する場合。
 2. ノードが、 x と $\sim x$ のように矛盾している場合。

3-SATとグラフの対応づけの例

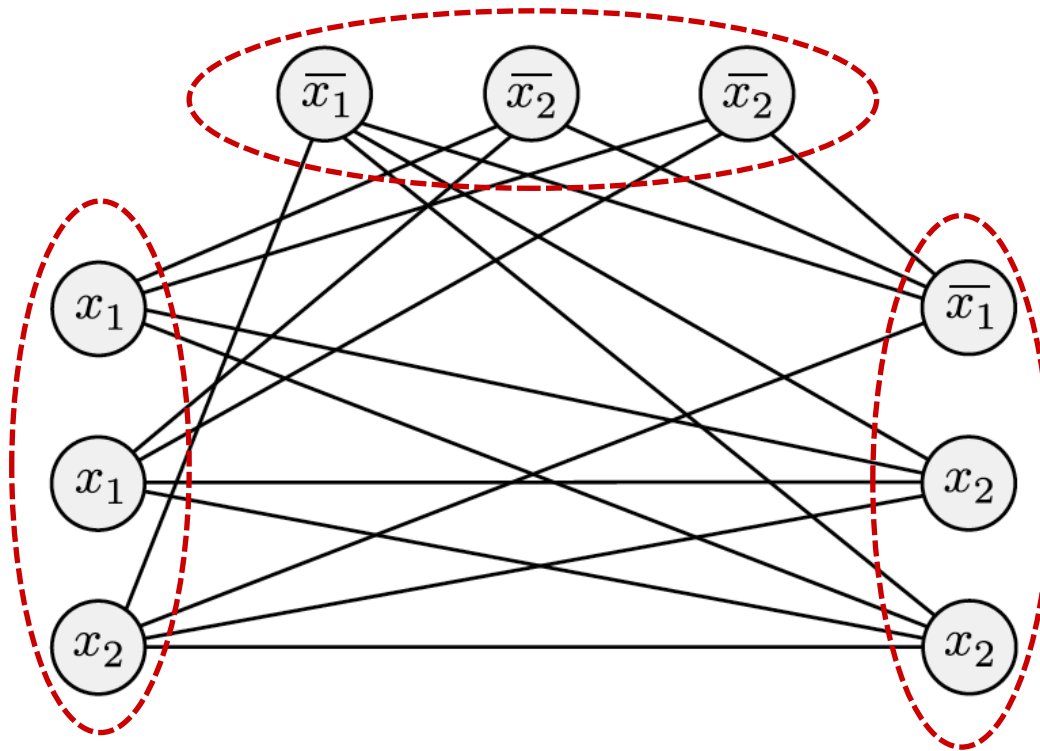
□ $\varphi = (x_1 \vee x_1 \vee x_2) \wedge (\overline{x_1} \vee \overline{x_2} \vee \overline{x_2}) \wedge \overline{x_1} \vee x_2 \vee x_2).$



$\overline{x_1}$ は、 $\sim x_1$, $\neg x_1$ と同じで、 x_1 の否定を表している。

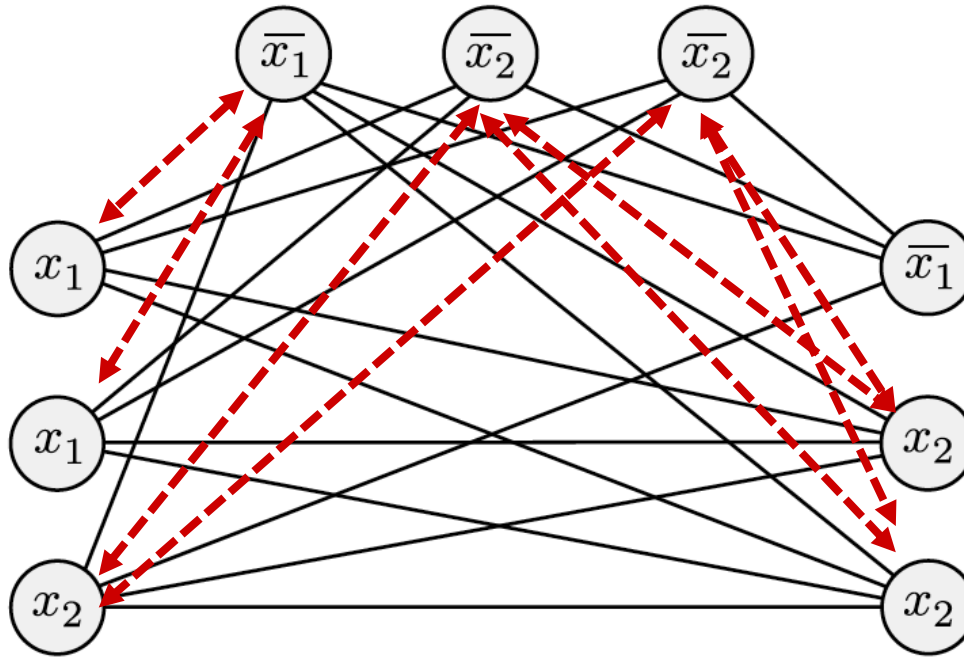
禁じられているエッジ1

□ 同じTripletの内部



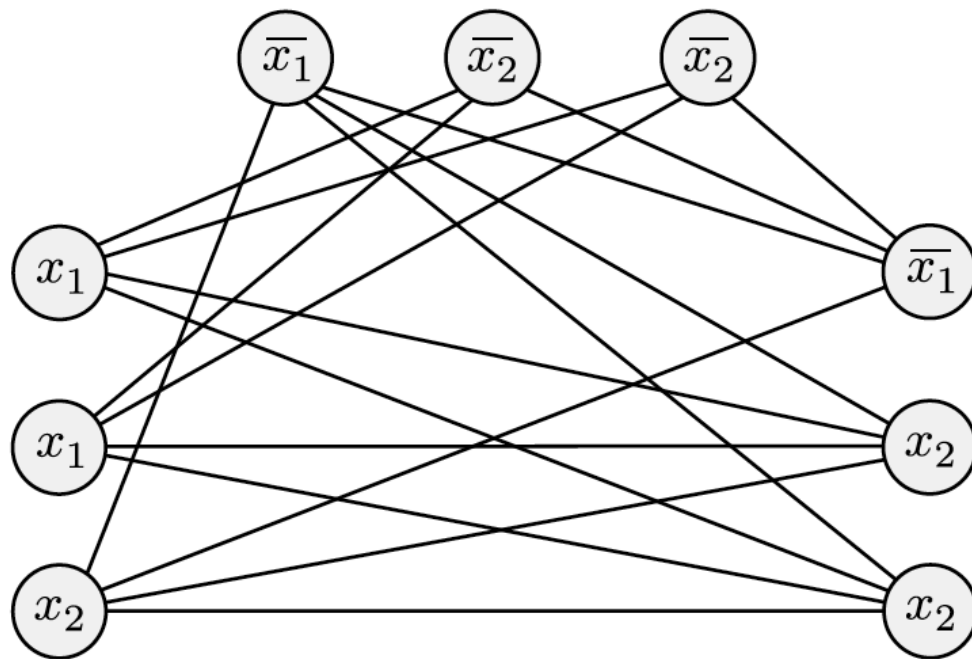
禁じられているエッジ2

□ 矛盾するノード間のエッジ



3-SATとグラフの対応づけの例

□ $\varphi = (x_1 \vee x_1 \vee x_2) \wedge (\overline{x_1} \vee \overline{x_2} \vee \overline{x_2}) \wedge \overline{x_1} \vee x_2 \vee x_2).$



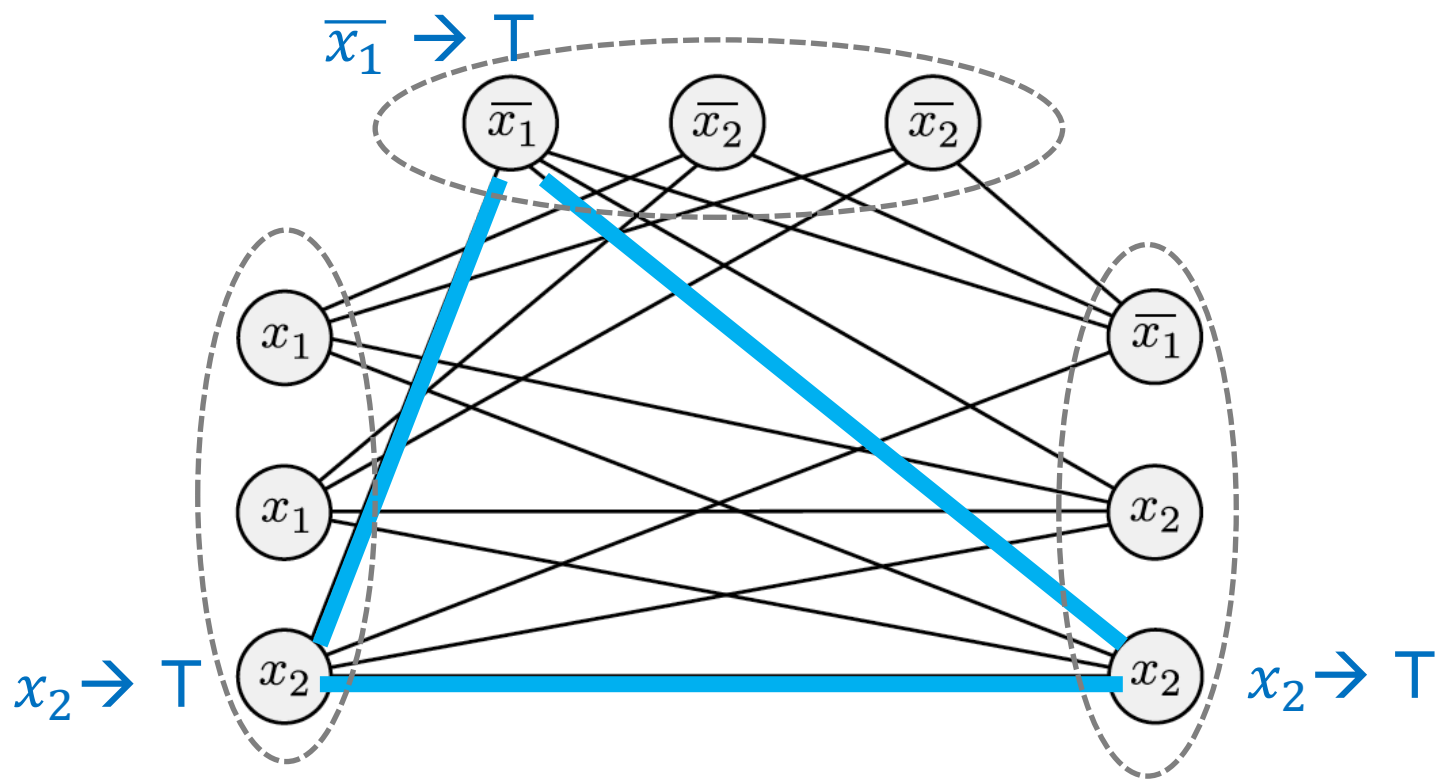
$\overline{x_1}$ は、 $\sim x_1$, $\neg x_1$ と同じで、 x_1 の否定を表している。

- 今、 φ を充足するような割り当てが一つあったとしよう。
この時、全ての節で、少なくとも一つのリテラルは真でなければならない。この割り当てで真になるリテラルに対応するGのtripleのノードを一つ選ぶ。特定の節で、一つ以上のリテラルが真になるなら、どちらか一つを任意に選ぶ。Gのtripleから、こうして選ばれたk個のノードは、cliqueになる。
- k個のtripleから、一個のノードを選んだのだから、選ばれたノードの数はkになる。また、選ばれたノードは、互いに元のグラフでのエッジで結ばれている。tripleにつき一個のノードを選び、また、矛盾したラベルを含まないので、この割り当てのもとで対応するリテラルは、両方とも真になる。よって、Gはcliqueを含む。

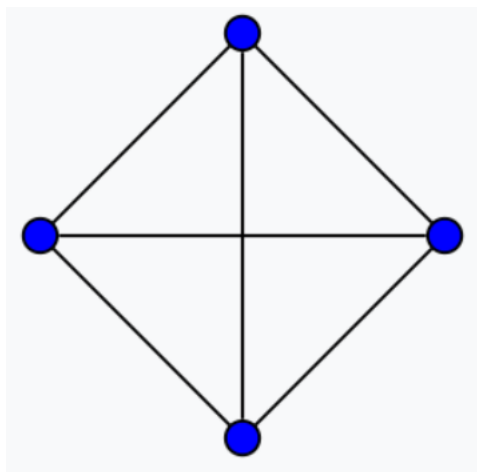
- G に、 k -cliqueがあったとしよう。cliqueの二つのノードが、同じtriple上にあることはない。それゆえ、 k 個のtripleは、正確に一個のcliqueのノードを含む。
- clique上のノードが、真になるように変数の値の割り当てを行えばいい。clique上のノードが真になれば、そのノードを含むtripleに対応する節は真になる。こうして、この割り当てのもとで、 ϕ は真となり、充足される。

3-SATに対応する3-clique

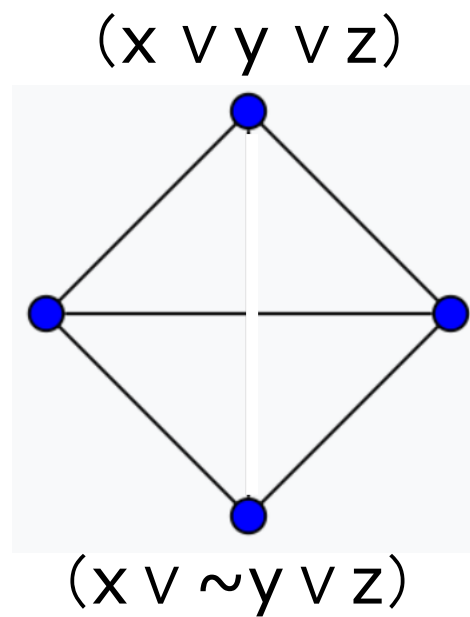
□ $\varphi = (x_1 \vee x_1 \vee x_2) \wedge (\overline{x_1} \vee \overline{x_2} \vee \overline{x_2}) \wedge \overline{x_1} \vee x_2 \vee x_2).$



4-cliqueの場合



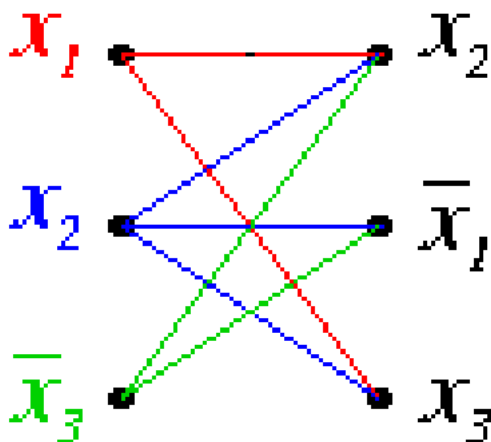
充足可能



充足不能

グラフに含まれるcliqueは、一個とは限らない

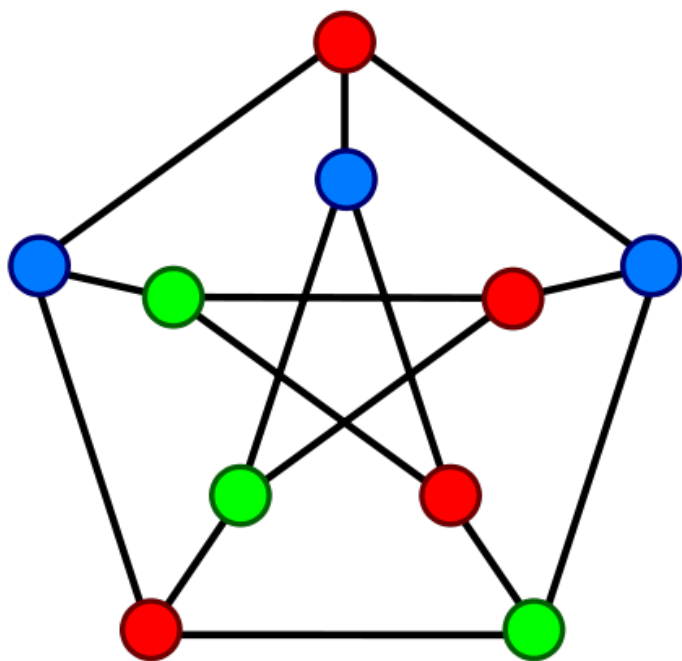
$$F = (\textcolor{red}{x}_1 \vee \textcolor{blue}{x}_2 \vee \textcolor{green}{\bar{x}}_3) \wedge (x_2 \vee \bar{x}_1 \vee x_3)$$



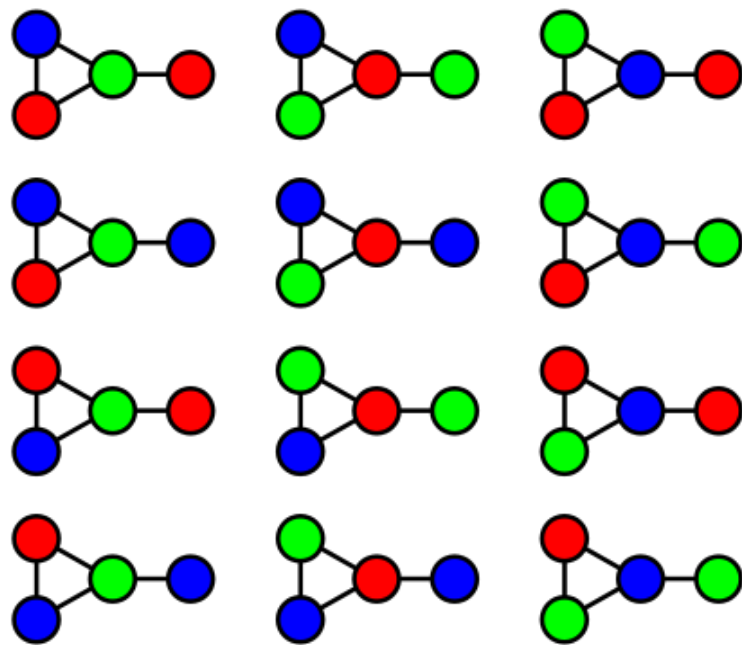
Graph Coloring 問題

Graph Coloring 問題

- Graph Coloring問題とは、グラフの頂点や辺に、ある条件のもとに、複数の色のラベルをつけるという問題である。隣り合うノードは同じ色でラベルづけけないという条件でノードに色付けするNode Coloring 問題が基本的である。
- 最大 k 色を使ったColoringを k -Coloringという。あるグラフが与えられた時、そのColoringに必要な最小の k を chromatic 数という。例えば、 n 個のノードを持つ完全グラフのchromatic数は、 n である。
- $k = 1$ および $k = 2$ 以外の k について「与えられたグラフが k -彩色可能か」という決定問題は、NP完全問題である。

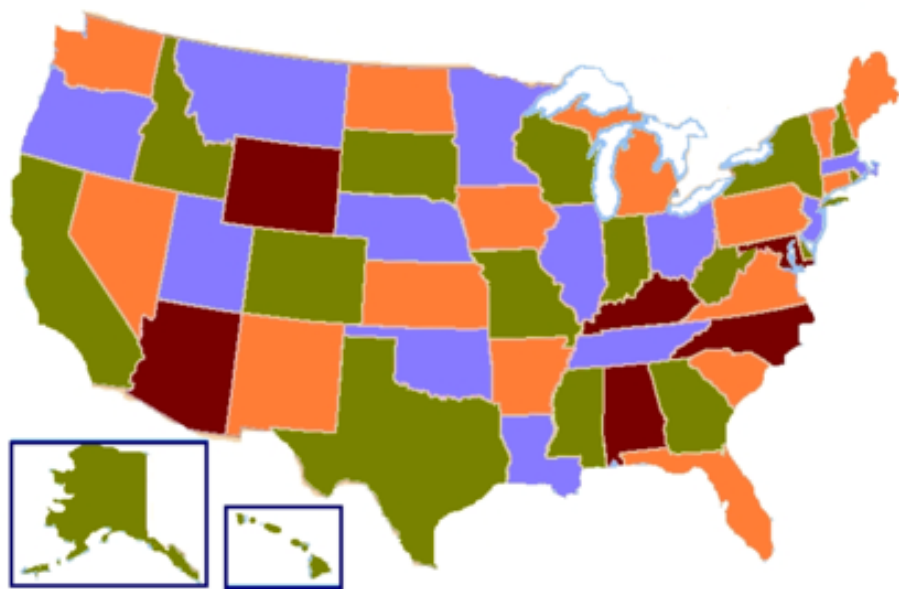


3色で彩色可能なグラフ

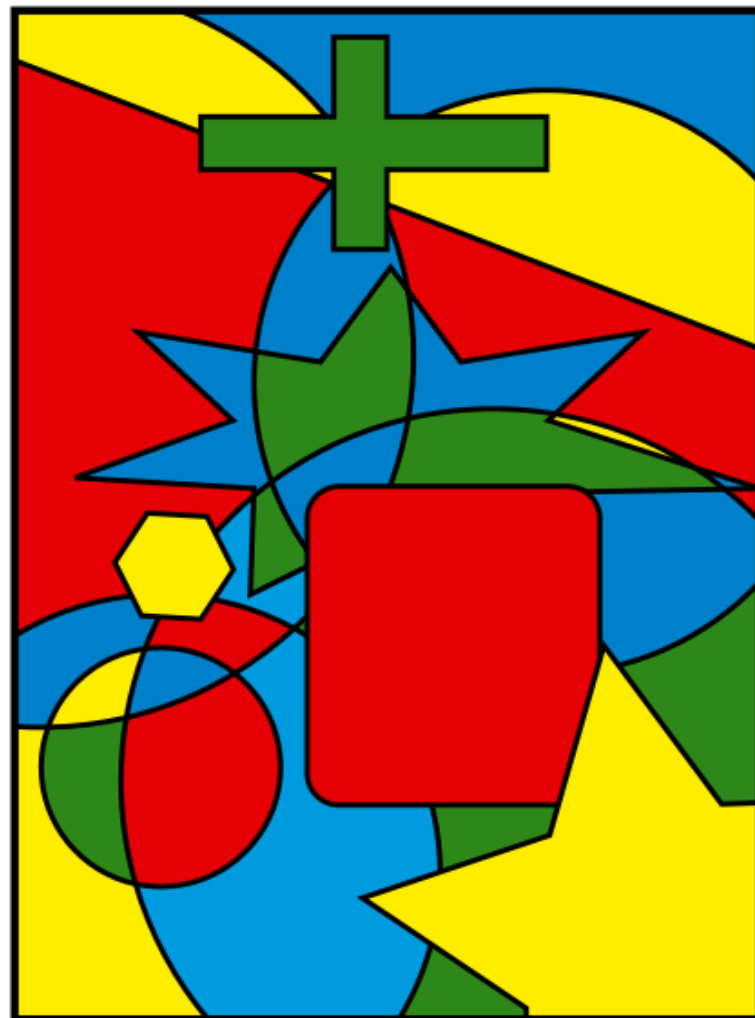


このグラフは、12通りの方法で
3色で彩色される。

四色定理



平面グラフの場合、どんなグラフも4色あれば塗り分け可能である。多項式時間で塗り分けを決定するアルゴリズムが存在する。



Graph Coloring問題のSAT問題への還元

□ グラフのノードを c_i ($1 \leq i \leq n$)、ノード c_i がカラー j を持つことを c_{ij} で表そう。この時、例えば、3色彩色可能かという問題は、次の二つの種類の論理式で表現できる。

1. 全てのノード c_i は、カラー j を持つことを主張する論理式群。
$$(c_{i1} \wedge \neg c_{i2} \wedge \neg c_{i3}) \vee (\neg c_{i1} \wedge c_{i2} \wedge \neg c_{i3}) \vee (\neg c_{i1} \wedge \neg c_{i2} \wedge c_{i3})$$
2. 全ての隣り合ったノード c_i, c_j は、違った色を持つことを主張する論理式群。
$$\neg((c_{i1} \wedge c_{j1}) \vee (c_{i2} \wedge c_{j2}) \vee (c_{i3} \wedge c_{j3}))$$

□ これら全ての式が同時に成り立つという論理式が、3-彩色問題と同値になる。

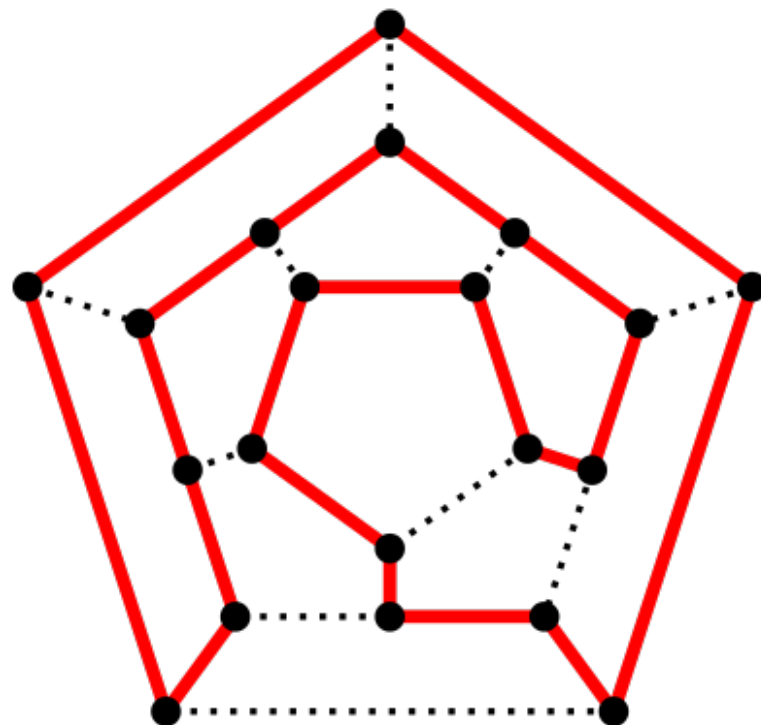
Hamiltonian Path 問題

Hamiltonian Path 問題

- Hamiltonian Path 問題は、あるグラフ(有向・無向)が与えられた時、その全ての頂点を一度だけ通るような経路が存在するかという問題である。経路が閉じている時、Hamiltonian Circleという。
- 「一筆書き」の問題に似ているが、「一筆書き」の場合は、同じ頂点を何回でも通っていいところが、Hamiltonian Path 問題とは異なっている。「一筆書き」が可能かどうかは、次のようなアルゴリズムで、簡単に決定可能である。
 - すべての頂点の次数(頂点につながっている辺の数)が偶数 → 運筆が起点に戻る
 - 次数が奇数である頂点の数が2で、残りの頂点の次数は全て偶数 → 運筆が起点に戻らない
- ところが、Hamiltonian Path 問題は、NP-完全である。



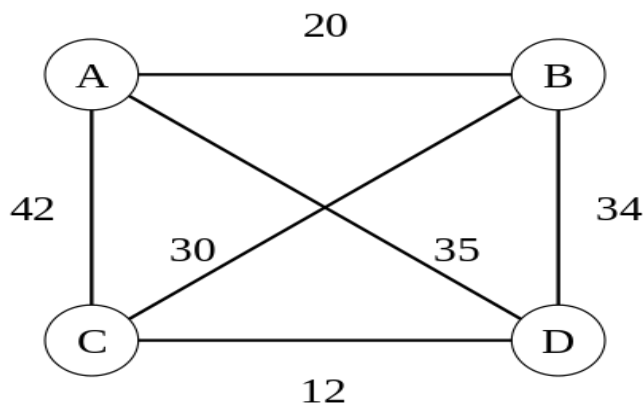
十二面体上のHamiltonian Path

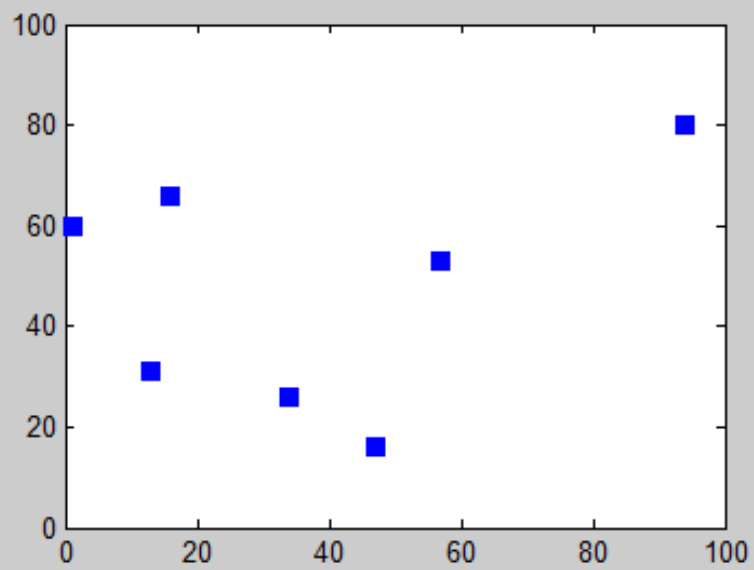
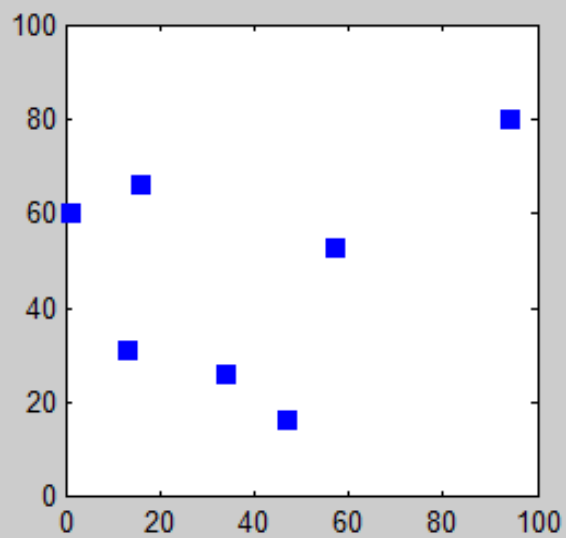
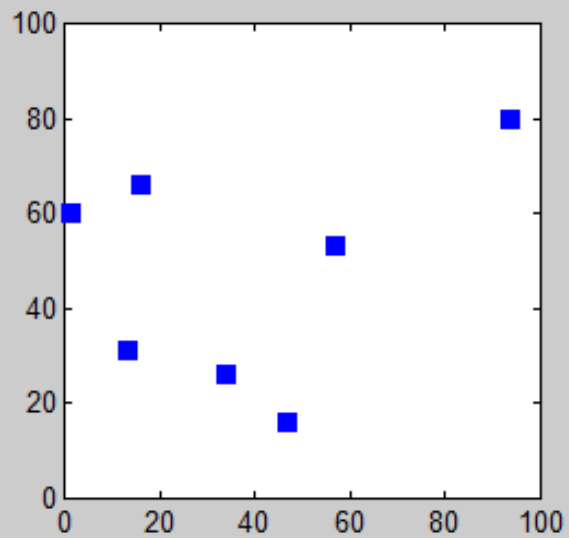


それと等価な二次元平面グラフ

巡回セールスマン問題

- 「巡回セールスマン問題 (traveling salesman problem, TSP) は、都市の集合と各2都市間の移動コスト (たとえば距離) が与えられたとき、全ての都市をちょうど一度ずつ巡り出発地に戻る巡回路の総移動コストが最小のものを求める (セールスマンが所定の複数の都市を1回だけ巡回する場合の最短経路を求める) 組合せ最適化問題である。」
- 巡回セールスマン問題は、すべてのHamiltonian Cycleを求める問題に還元できるのでNP-完全である。





実際に実装されている
NP-完全問題のプログラム

Algorithms for solving SAT

- Since the SAT problem is NP-complete, only algorithms with exponential worst-case complexity are known for it. In spite of this, efficient and scalable algorithms for SAT were developed over the last decade. A SAT-solving engine is now considered to be an essential component in the [EDA](#) toolbox.
- The PPSZ algorithm has a runtime of $O(2^{0.386n})$ for 3-SAT with a single satisfying assignment.

SAT 2018 Competition

Organizers [Marijn Heule](#), [Matti Järvisalo](#), [Martin Suda](#)

Past Competitions

SAT 2017 Competition

Organizers [Marijn Heule](#), [Matti Järvisalo](#), [Tomáš Balyo](#)

Slides [Slides used at SAT 2017](#)

Proceedings [Descriptions of the solvers and benchmarks](#)

Benchmarks [Available here](#)

Solvers [Available here](#)

	Gold	Silver	Bronze	Gold	Silver	Bronze	Gold	Silver	Bronze
	Agile Track			Main Track			Random Track		
SAT+UNSAT	CaDiCaL Agile, CaDiCaL NoProof	Glu_VC	Glucose 4.1	Maple LCM Dist, Maple LCM, MapleLRB LCMOccRestart, MapleLRB LCM	MapleCOMSPS LRB VSIDS 2, MapleCOMSPS LRB VSIDS	COMiniSATPS Pulsar	YaSAT	tch glucose3	Score2
	Parallel Track			No-Limit Track			Incremental Library Track		
SAT+UNSAT	Syrup24, Syrup48	Plingeling	Painless MapleCOMSPS	COMiniSATPS Pulsar	MapleCOMSPS LRB VSIDS 2, MapleCOMSPS LRB VSIDS	CaDiCaL NoProof	AbcdSAT	Glucose	Riss

SAT 2016 Competition

Organizers [Marijn Heule](#), [Matti Järvisalo](#), [Tomáš Balyo](#)

Proceedings [Descriptions of the solvers and benchmarks](#)

Benchmarks [Available here](#)

Solvers [Available here](#)

	Gold	Silver	Bronze	Gold	Silver	Bronze	Gold	Silver	Bronze
--	------	--------	--------	------	--------	--------	------	--------	--------

<https://www.satcompetition.org/>

Finding maximum cliques in arbitrary graphs

- It is possible to find the maximum clique, or the clique number, of an arbitrary n -vertex graph in time $O(3^{n/3}) = O(1.4422^n)$
- The algorithm of [Tarjan & Trojanowski](#) solves this problem in time $O(2^{n/3}) = O(1.2599^n)$
- [Jian \(1986\)](#) improved the time to $O(2^{0.304n}) = O(1.2346^n)$, and [Robson \(1986\)](#) improved it to $O(2^{0.276n}) = O(1.2108^n)$
- [Robson \(2001\)](#) which runs in time $O(2^{0.249n}) = O(1.1888^n)$

Graph Coloring Exact algorithms

- Using dynamic programming and a bound on the number of maximal independent sets, k -colorability can be decided in time and space $O(2.445^n)$
- Using the principle of inclusion–exclusion and Yates’s algorithm for the fast zeta transform, k -colorability can be decided in time $O(2^n n)$ for any k .
- Faster algorithms are known for 3- and 4-colorability, which can be decided in time $O(1.3289^n)$ and $O(1.7272^n)$ respectively.

Hamilton Path Algorithms

- a [dynamic programming](#) algorithm of Bellman, Held, and Karp can be used to solve the problem in time $O(n^2 2^n)$.
- Andreas Björklund showed how to solve the Hamiltonian cycle problem in arbitrary n -vertex graphs by a [Monte Carlo algorithm](#) in time $O(1.657^n)$; for [bipartite graphs](#) this algorithm can be further improved to time $\underline{o}(1.415^n)$.
- For graphs of maximum degree three, a careful backtracking search can find a Hamiltonian cycle (if one exists) in time $O(1.251^n)$.

Traveling salesman problem

Exact algorithms

- ❑ The most direct solution would be to try all permutations (ordered combinations) and see which one is cheapest (using brute force search). The running time for this approach lies within a polynomial factor of $O(n!)$, the factorial of the number of cities, so this solution becomes impractical even for only 20 cities.
- ❑ One of the earliest applications of dynamic programming is the Held–Karp algorithm that solves the problem in time $O(n^2 2^n)$.

量子断熱コンピュータとNP-完全問題

- ❑ 断熱型の量子コンピュータが、NP-完全問題の攻略に利用できるのではという問題提起を初めて行ったのは、Edward Farhiのグループである。2000年のことだ。2001年には、Science誌に彼らの論文が掲載され、大きな話題になる。ただ、彼らが考察したのは、“One-, Two-, and Three-Qubit Examples” という小さな範囲での考察だった。
- ❑ 2002年には、Wim van Dam らVaziraniのグループが反論する。2004年のB.Reichardtの論文は、Farhiの方法では、3-SATを解くのに指数関数的な時間がかかることを明らかにする。こうした状況は、エネルギー・ギャップが小さい場合に起きることもわかってくる。

Quantum Computation by Adiabatic Evolution

Edward Farhi, Jeffrey Goldstone, Sam Gutmann,
Michael Sipser

<https://arxiv.org/abs/quant-ph/0001106>

Submitted on 28 Jan 2000

We give a quantum algorithm for solving instances of the satisfiability problem, based on adiabatic evolution. The evolution of the quantum state is governed by a time-dependent Hamiltonian that interpolates between an initial Hamiltonian, whose ground state is easy to construct, and a final Hamiltonian, whose ground state encodes the satisfying assignment. To ensure that the system evolves to the desired final ground state, the evolution time must be big enough. The time required depends on the minimum energy difference between the two lowest states of the interpolating Hamiltonian. We are unable to estimate this gap in general. We give some special symmetric cases of the satisfiability problem where the symmetry allows us to estimate the gap and we show that, in these cases, our algorithm runs in polynomial time.

<https://arxiv.org/abs/quant-ph/0001106>

We present a quantum algorithm for the satisfiability problem (and other combinatorial search problems) that works on the principle of quantum adiabatic evolution. An n -bit instance of satisfiability is a formula

$$C_1 \wedge C_2 \wedge \cdots \wedge C_M$$

where each clause C_a is True or False depending on the values of some subset of the bits. For a single clause, involving only a few bits, it is easy to imagine constructing a quantum device that evolves to a state that encodes the satisfying assignments of the clause. The real difficulty, of course, lies in constructing a device that produces an assignment that satisfies all M clauses.

Our algorithm is specified by an initial state in an n -qubit Hilbert space and a time-dependent Hamiltonian $H(t)$ that governs the state's evolution according to the Schrödinger equation.

The Hamiltonian takes the form

$$H(t) = H_{C_1}(t) + H_{C_2}(t) + \cdots + H_{C_M}(t)$$

where each H_{C_a} depends only on clause C_a and acts only on the bits in C_a . $H(t)$ is defined for t between 0 and T and is slowly varying. The initial state, which is always the same and easy to construct, is the ground state of $H(0)$. For each a , the ground state of $H_{C_a}(T)$ encodes the satisfying assignments of clause C_a .

The ground state of $H(T)$ encodes the satisfying assignments of the intersection of all the clauses. According to the adiabatic theorem, if the evolution time T is big enough, the state of the system at time T will be very close to the ground state of $H(T)$, thus producing the desired solution. For this algorithm to be considered successful we require that T grow only polynomially in n , the number of bits. In this paper we analyze three examples where T grows only polynomially in n . We are unable to estimate the required running time T in general.

$$h_C(z_{i_C}, z_{j_C}, z_{k_C}) = \begin{cases} 0, & \text{if } (z_{i_C}, z_{j_C}, z_{k_C}) \text{ satisfies clause } C \\ 1, & \text{if } (z_{i_C}, z_{j_C}, z_{k_C}) \text{ violates clause } C. \end{cases}$$

$$h = \sum_C h_C .$$

- Clearly $h \geq 0$ and $h(z_1, z_2, \dots, z_n) = 0$ if and only if $(z_1, z_2, \dots, z_n)$ satisfies all of the clauses. Thus finding the minimum energy configuration of h tells us if the formula has a satisfying assignment.

□ 3 One-, Two-, and Three-Qubit Examples

□ 4 Examples with an Arbitrary Number of Bits

- 4.1 2-SAT on a Ring: Agree and Disagree
- 4.2 The Grover Problem
- 4.3 The Bush of Implications
- 4.4 Overconstrained 2-SAT

A Quantum Adiabatic Evolution Algorithm Applied to Random Instances of an NP-Complete Problem

**Edward Farhi,^{1*} Jeffrey Goldstone,¹ Sam Gutmann,²
Joshua Lapan,³ Andrew Lundgren,³ Daniel Preda³**

A quantum system will stay near its instantaneous ground state if the Hamiltonian that governs its evolution varies slowly enough. This quantum adiabatic behavior is the basis of a new class of algorithms for quantum computing. We tested one such algorithm by applying it to randomly generated hard instances of an NP-complete problem. For the small examples that we could simulate, the quantum adiabatic algorithm worked well, providing evidence that quantum computers (if large ones can be built) may be able to outperform ordinary computers on hard sets of instances of NP-complete problems.

A quantum system will stay near its instantaneous ground state if the Hamiltonian that governs its evolution varies slowly enough. This quantum adiabatic behavior is the basis of a new class of algorithms for quantum computing. We tested one such algorithm by applying it to randomly generated hard instances of an NP-complete problem. For the small examples that we could simulate, the quantum adiabatic algorithm worked well, providing evidence that quantum computers (if large ones can be built) may be able to outperform ordinary computers on hard sets of instances of NP-complete problems.

How Powerful is Adiabatic Quantum Computation?

Wim van Dam, Michele Mosca, Umesh Vazirani
2002

<https://people.eecs.berkeley.edu/~vazirani/pubs/adiabatic.pdf>

Conclusion

Adiabatic quantum computation is a novel paradigm for the design of quantum algorithms — it is truly quantum in the sense that it can be used to speed up searching by a quadratic factor over any classical algorithm.

On the question of whether this new paradigm may be used to efficiently solve NP-complete problems on a quantum computer — we showed that the usual query complexity arguments cannot be used to rule out a polynomial time solution.

Conclusion

On the other hand, we argue that the adiabatic approach may be thought of as a kind of 'quantum local search'. We designed a family of minimization problems that is hard for such local search heuristics, and established an exponential lower bound for the adiabatic algorithm for these problems. This provides insights into the limitations of this approach. In an upcoming paper [5], we generalize these techniques to show a similar exponential slowdown for 3SAT. It remains an open question whether adiabatic quantum computation can establish an exponential speed-up over traditional computing or if there exists a classical algorithm that can simulate the quantum adiabatic process efficiently.

The Quantum Adiabatic Optimization Algorithm and Local Minima

B.Reichardt

2004

<https://dl.acm.org/citation.cfm?id=1007428>

Abstract

The quantum adiabatic optimization algorithm uses the adiabatic theorem from quantum physics to minimize a function by interpolation between two Hamiltonians. The quantum wave function can sometimes tunnel through significant obstacles. However it can also sometimes get stuck in local minima, even for fairly simple problems. An initial Hamiltonian which insufficiently mixes computational basis states is analogous to a poorly mixing Markov transition rule.

We study a physical system – the Ising quantum chain with alternating sector interaction defects, but constant transverse field – which is equivalent to applying the quantum adiabatic algorithm to a particular SAT problem. We prove that for a constant range of values for the transverse field, the spectral gap is exponentially small in the sector length. Indeed, we prove that there are exponentially many eigenvalues all exponentially close to the ground state energy. Applying the adiabatic theorem therefore takes exponential time, even for this simple problem.

量子断熱コンピュータと 量子ゲート型コンピュータとの 「等価性」

2004年には、Dorit Aharonovらが、量子断熱コンピュータと量子ゲート型コンピュータとの能力は、原理的には等しいことを証明する。これは、重要な認識である。

Adiabatic Quantum Computation is Equivalent to Standard Quantum Computation

Dorit Aharonov, Wim van Dam, Julia Kempe, Zeph
Landau, Seth Lloyd, Oded Regev
2005

<https://arxiv.org/abs/quant-ph/0405098>

Abstract

- Adiabatic quantum computation has recently attracted attention in the physics and computer science communities, but its computational power was unknown. We describe an efficient adiabatic simulation of any given quantum algorithm, which implies that the adiabatic computation model and the conventional quantum computation model are polynomially equivalent. Our result can be extended to the physically realistic setting of particles arranged on a two-dimensional grid with nearest neighbor interactions.

Abstract

- The equivalence between the models provides a new vantage point from which to tackle the central issues in quantum computation, namely designing new quantum algorithms and constructing fault tolerant quantum computers. In particular, by translating the main open questions in the area of quantum algorithms to the language of spectral gaps of sparse matrices, the result makes these questions accessible to a wider scientific audience, acquainted with mathematical physics, expander theory and rapidly mixing Markov chains.

Introduction

- The study of adiabatic quantum computation was initiated several years ago by Farhi, Goldstone, Gutmann and Sipser, who suggested a novel quantum algorithm for solving classical optimization problems such as Satisfiability (Sat). Their algorithm is based on a celebrated theorem in quantum mechanics known as the adiabatic theorem. Although the exact worst-case behavior of this algorithm is not known, several simulations (see, e.g.,) on random instances of up to 20 quantum bits led to various optimistic speculations.

Introduction

- The bad news is that there is now mounting evidence [9, 10, 29] that the algorithm of [14] takes exponential time in the worst-case for NP-complete problems. Nevertheless, adiabatic computation was since shown to be promising in other less ambitious directions: it possesses several interesting algorithmic capabilities, as we will soon review, and in addition, it exhibits inherent robustness against certain types of quantum errors [8]. We note that a small scale adiabatic algorithm has already been implemented experimentally, using a Nuclear Magnetic Resonance (NMR) system [36]

Introduction

- We briefly describe the model of adiabatic computation (a more precise description appears in Section 2.2). A computation in this model is specified by two Hamiltonians named H_{init} and H_{final} (a Hamiltonian is simply a Hermitian matrix). The eigenvector with smallest eigenvalue (also known as the ground state) of H_{init} is required to be an easy to prepare state, such as a tensor product state. The output of the adiabatic computation is the ground state of the final Hamiltonian H_{final} .

Introduction

- Hence, we choose an H_{final} whose ground state represents the solution to our problem. We require the Hamiltonians to be local, i.e., we require them to only involve interactions between a constant number of particles (this can be seen as the equivalent of allowing gates operating on a constant number of qubits in the standard model). This, in particular, makes sure that the Hamiltonians have a short classical description, by simply listing the matrix entries of each local term. The running time of the adiabatic computation is determined by the minimal spectral gap of all the Hamiltonians on the straight line connecting H_{init} and H_{final} : $H(s) = (1-s)H_{\text{init}} + sH_{\text{final}}$ for $s \in [0, 1]$. More precisely, the adiabatic computation is polynomial time if this minimal spectral gap is at least inverse polynomial.

The pitfalls of planar spin-glass benchmarks: Raising the bar for quantum annealers (again)

Salvatore Mandrà, Helmut G. Katzgraber,
Creighton Thomas
2017

<https://arxiv.org/pdf/1703.00622.pdf>

Abstract

- In an effort to overcome the limitations of random spin-glass benchmarks for quantum annealers, focus has shifted to carefully-crafted gadget-based problems whose logical structure has typically a planar topology. Recent experiments on these gadget problems using a commercially-available quantum annealer have demonstrated an impressive performance over a selection of commonly-used classical optimization heuristics. Here we show that efficient classical optimization techniques, such as minimum-weight perfect matching, can solve these gadget problems exactly and in polynomial time. We present approaches on how to mitigate this shortcoming of commonly-used benchmark problems based on planar logical topologies.

Introduction

- The quest for quantum speedup using analog quantum annealing machines with a transverse field remains elusive. There have been multiple attempts to demonstrate that the D-Wave Systems Inc. quantum annealers can outperform classical optimization methods. Unfortunately, it has been relatively straightforward for classical optimization algorithms to stay ahead in this race. Either the random spin-glass benchmark problems were too easy on the quasi-planar topology of the D-Wave quantum annealer, or the logical structure of carefully-crafted problems designed to give the annealer an advantage have a trivial structure.

- The notable advances made by D-Wave Systems Inc. in the development of medium-scale quantum annealing technologies has inspired multiple corporations (e.g., Microsoft, Google, and IBM) to further invest in quantum computing, in addition to large-scale government-funded projects. The D-Wave 2000Q device is a special-purpose quantum optimization machine specialized in minimizing quadratic unconstrained binary cost functions by means of quenching quantum fluctuations induced by a transverse field.

Adiabatic Quantum Computing

Tameem Albash, Daniel A. Lidar

2018

<https://arxiv.org/pdf/1611.04471.pdf>

Abstract

- Adiabatic quantum computing (AQC) started as an approach to solving optimization problems, and has evolved into an important universal alternative to the standard circuit model of quantum computing, with deep connections to both classical and quantum complexity theory and condensed matter physics. In this review we give an account of most of the major theoretical developments in the field, while focusing on the closed system setting. The review is organized around a series of topics that are essential to an understanding of the underlying principles of AQC, its algorithmic accomplishments and limitations, and its scope in the more general setting of computational complexity theory.

Abstract

- We present several variants of the adiabatic theorem, the cornerstone of AQC, and we give examples of explicit AQC algorithms that exhibit a quantum speedup. We give an overview of several proofs of the universality of AQC and related Hamiltonian quantum complexity theory. We finally devote considerable space to Stoquastic AQC, the setting of most AQC work to date, where we discuss obstructions to success and their possible resolutions.

Contents

I. Introduction

II. Adiabatic Theorems

III. Algorithms

IV. Universality of AQC

V. Hamiltonian quantum complexity theory and universal AQC

VI. Stoquastic Adiabatic Quantum Computation

VII. Circumventing slowdown mechanisms for AQC

VIII. Outlook and Challenges

Part II

広がる量子アルゴリズムの世界

BQP-完全問題とQRAM

Agenda Part II

広がる量子アルゴリズムの世界 -- BQP-完全問題とQRAM

- 量子組み合わせ最適化 QAOAとVQE
- 量子アニーリング
- 量子ディープラーニング
- QRAMと量子逆行列変換 HHLアルゴリズム
- QRAMとは何か？
- 半正定値プログラミング
- 量子リコメンデーション

量子コンピュータの課題

量子アルゴリズムの原理的探求

- Shorのアルゴリズムのような、BQPに属する、指数関数的高速化が可能な問題の探求。**BQP-完全問題**。
- Groverの検索アルゴリズムのような、 $\sqrt{N}$ の高速化が可能な問題のクラスの探求。
- 量子ゲート型と量子アニーリング型の「等価性」の認識と、新しい量子デバイスの探求。
- 量子エラー訂正回路等、ノイズ耐性を持つ量子回路の探求。

広がる量子アルゴリズムの世界

- 組合せ最適化問題での、厳密解ではなく近似解を求める量子アルゴリズムの研究。
- 量子アニーリング
- 量子ディープラーニング
- QRAMと量子逆行列変換
- 量子リコメンデーション
- 半正定値プログラミング
- ...
- ...
- 量子通信・量子暗号化

量子組み合わせ最適化 QAOAとVQE

John Preskill “Quantum Computing in the NISQ era and beyond”
<https://arxiv.org/pdf/1801.00862.pdf> から

量子最適化の問題

- 量子コンピュータが、組み合わせ最適化問題のようなNP困難な問題の最悪の場合を効率的に解くことを、我々は期待していないことは、すでに強調してきた。それでも、量子デバイスがより良い近似解を見つけたり、そのような近似解をより早く見つけれられることは、考えられる(保証されてはいないのだが)。
- 例えば、 n 個のビットに m 個の制約を課して、 m 個の制約をできるだけ多く満たす n ビットの文字列を求めることができる。同時に満たすことができる制約の最大数 k を見つけることができれば、この最適化問題を正確に解決できたと言えるかもしれない。また、満たすべき制約の最大数が少なくともいくつかの k' に対して、 $k' < k$ であることを保証できれば、近似解を得たことになる。近似比 k'/k は、近似解の品質の尺度となる。

- いくつかの最適化問題では、近似解が1に十分近くても近似解を見つけることさえNP困難である。そのような場合には、量子計算機が、難しい問題の近似解を効率的に求めることは期待できない。しかし、多くの問題に対して、我々が現在知っている最高の古典的アルゴリズムによって達成される近似解とNP困難との障壁との間には大きなギャップがある。だから、量子コンピュータが、近似解を見つけるという仕事には、古典的コンピュータよりも利点があることを発見することは衝撃的ではないだろう。
- こうした量子の利点が実際に存在するかどうかは現在未解決の問題だが、量子ハードウェアを使用して実験的にこうした問題を探求する機会は、すぐに来るだろう。もちろん、近似最適化のための量子的利点があるとしても、NISQ技術はその利点を実証するには不十分かもしれない。それでも、それを試して、それがどれほどうまくいくかを知ることは楽しいことだろう。

最適化問題を解決する 量子・古典のハイブリッド・アルゴリズム

- 量子技術を用いた最適化問題を解決するため新登場のパラダイムは、量子・古典のハイブリッド・アルゴリズムである。
- このスキームでは、量子プロセッサを使用して n -qubit状態を準備し、古典的オプティマイザを使用してすべてのqubitを測定し、測定の出力を処理する。古典的オプティマイザは、量子プロセッサに、 n -qubit状態がどのように準備されるかをわずかに変更するよう指示する。このサイクルは、近似解を抽出することができる量子状態に収束するまで何度も繰り返される。

QAOAとVQE

- 従来の組み合わせ論的最適化問題に適用すると、この手順は量子近似最適化アルゴリズム(QAOA)という名前になる。
- しかし、これはまた、多粒子量子系(例えば、大きな分子)の低エネルギー状態を見出すような量子問題にも適用することができる。量子問題に適用する場合、この量子・古典のハイブリッド手順は、Variation Quantum Eigensolver(VQE)という名前で行われる。

可能性は高い

- QAOAまたはVQEを実行しているNISQ技術は、同じ問題に対するおおよその解決策を見出す古典的なアルゴリズムより優れた性能を発揮できるだろうか？誰も知らない。我々は、それを試して、どれくらいうまくいくかを見ていこう。
- これらの問題を解決するために使用する古典的な方法は、何十年にもわたって開発されて以来、磨きがかけられているため、野心的な目標である。一方、たとえ初期の世代のNISQデバイスが最高の古典的なコンピュータと競合する準備ができていなくても、実験結果は、QAOAやVQEが将来古典的な方法を上回るだろうという我々の期待を勇気づけるものになる可能性がある。そして、さらなる技術的改良に拍車がかかるだろう。

QAOA

A Quantum Approximate Optimization Algorithm

Edward Farhi, Jeffrey Goldstone, Sam Gutmann

<https://arxiv.org/pdf/1411.4028.pdf>

Submitted on 14 Nov 2014

We introduce a quantum algorithm that produces approximate solutions for combinatorial optimization problems. The algorithm depends on an integer $p \geq 1$ and the quality of the approximation improves as p is increased. The quantum circuit that implements the algorithm consists of unitary gates whose locality is at most the locality of the objective function whose optimum is sought. The depth of the circuit grows linearly with p times (at worst) the number of constraints. If p is fixed, that is, independent of the input size, the algorithm makes use of efficient classical preprocessing. If p grows with the input size a different strategy is proposed. We study the algorithm as applied to MaxCut on regular graphs and analyze its performance on 2-regular and 3-regular graphs for fixed p . For $p = 1$, on 3-regular graphs the quantum algorithm always finds a cut that is at least 0.6924 times the size of the optimal cut.

<https://arxiv.org/pdf/1411.4028.pdf>

充足性とその近似の定式化

- 長さ n のビット列 $z = z_1 z_2 \dots z_n$ と、 z についての m 個の制約条件 C_α があるとする。
- z が制約条件 C_α を満たす時、 $C_\alpha(z) = 1$
そうでない時、 $C_\alpha(z) = 0$ とする。

- この時、
$$C(z) = \sum_{\alpha=1}^m C_\alpha(z)$$
 とする。

要は、 $C(z)$ は、 z が満たす制約条件の数である。

- 充足性の問題とは、 m 個すべての条件を満たす z 、すなわち、 $C(z) = m$ となる z をすべて見つける問題である。
- 最適化の近似問題とは、 C の最大値に近い値を与える z を求める問題である。

定式の量子化

- ある角度 γ に依存するユニタリ演算子 $U(C, \gamma)$ を、次のように定義する。

$$U(C, \gamma) = e^{-i\gamma C} = \prod_{\alpha=1}^m e^{-i\gamma C_{\alpha}} .$$

- 全てのシングル・ビットの σ^x 演算子の和として、演算子 B を定義する。

$$B = \sum_{j=1}^n \sigma_j^x .$$

- 今度は、可換なシングル・ビット演算子の積と β に依存する演算子を次のように定義する。

$$U(B, \beta) = e^{-i\beta B} = \prod_{j=1}^n e^{-i\beta \sigma_j^x}$$

- 初期状態 $|s\rangle$ は、計算基底上のユニフォームな重ね合わせにする。

$$|s\rangle = \frac{1}{\sqrt{2^n}} \sum_z |z\rangle.$$

- 全ての整数 $p \geq 1$ と $2p$ 個の角度 $\gamma_1 \dots \gamma_p \equiv \gamma$ と $\beta_1 \dots \beta_p \equiv \beta$ に対して、この角度に依存する次の量子状態を考える。

$$|\gamma, \beta\rangle = U(B, \beta_p) U(C, \gamma_p) \cdots U(B, \beta_1) U(C, \gamma_1) |s\rangle.$$

- F_p を、この状態の C の期待値とする。

$$F_p(\gamma, \beta) = \langle \gamma, \beta | C | \gamma, \beta \rangle.$$

- M_p を、この角度上での F_p の最大値とする。

$$M_p = \max_{\gamma, \beta} F_p(\gamma, \beta).$$

- $p - 1$ での最大化は、 p での制限された最大化と見ることができるので、次の式が成り立つことに注意。

$$M_p \geq M_{p-1}.$$

- のちに、次のことを示す。

$$\lim_{p \rightarrow \infty} M_p = \max_z C(z).$$

- These results suggest a way to design an algorithm. Pick a p and start with a set of angles (γ, β) that somehow make F_p as large as possible. Use the quantum computer to get the state $|\gamma, \beta\rangle$. Measure in the computational basis to get a string z and evaluate $C(z)$. Repeat with the same angles. Enough repetitions will produce a string z with $C(z)$ very near or greater than $F_p(\gamma, \beta)$. The rub is that it is not obvious in advance how to pick good angles.

new quantum algorithm for NP-hard optimization problems

1. starts with a uniform superposition over all n -bit strings,
2. applies a set of unitary transformations, one for each variable and constraint of the NP-hard instance,
3. repeats the set some number of times p (the case $p=1$ is already interesting), and then
4. measures the state in the computational basis to see what solution was obtained.

Beating the random assignment on constraint satisfaction problems of bounded degree

Boaz Barak, Ankur Moitra, Ryan O'Donnell, Prasad
Raghavendra, Oded Regev, David Steurer, Luca
Trevisan, Aravindan Vijayaraghavan, David
Witmer, John Wright

2015

<https://eccc.weizmann.ac.il//report/2015/082/>

- この複数の著者の論文は、量子コンピュータを利用するFarhiの論文の結果を上回ることが、古典的なアルゴリズムで可能であることを示す。
- アルゴリズムの実効的な性能をめぐるのは、「量子断熱型 vs 量子ゲート型」という対立軸の他に、「量子アルゴリズム vs 古典アルゴリズム」という対立軸も存在することを、鮮やかに示すことになった。

A Quantum Approximate Optimization Algorithm Applied to a Bounded Occurrence Constraint Problem

Edward Farhi, Jeffrey Goldstone, Sam Gutmann

<https://arxiv.org/abs/1412.6062>

last revised 25 Jun 2015

Combinatorial Optimization on Gate Model Quantum Computers: A Survey

Ehsan Zahedinejad · Arman Zaribafiyan

2017

<https://arxiv.org/pdf/1708.05294.pdf>

The advent of quantum computing processors with possibility to scale beyond experimental capacities magnifies the importance of studying their applications. Combinatorial optimization problems can be one of the promising applications of these new devices. These problems are recurrent in industrial applications and they are in general difficult for classical computing hardware. In this work, we provide a survey of the approaches to solving different types of combinatorial optimization problems, in particular quadratic unconstrained binary optimization (QUBO) problems on a gate model quantum computer. We focus mainly on four different approaches including digitizing the adiabatic quantum computing, global quantum optimization algorithms, the quantum algorithms that approximate the ground state of a general QUBO problem, and quantum sampling. We also discuss the quantum algorithms that are custom designed to solve certain types of QUBO problems.

VQE

The theory of variational hybrid quantum-classical algorithms

J. R. McClean, J. Romero, R. Babbush, and A.
Aspuru-Guzik,
<https://arxiv.org/pdf/1509.04279.pdf>

I. INTRODUCTION

- Eigenvalue and more general optimization problems lie at the heart of applications and technologies ranging from Google's Page Rank and aircraft design to quantum simulation and quantum chemistry. Quantum computers promise to provide ground breaking advances in our ability to solve these problems by offering solutions that may be exponentially faster than the classical equivalent in some cases. However, delivering on these promises may require overcoming considerable technological challenges.

Error Resilience

- The VQE has the notable property that it can run on any quantum device, making it a candidate for exploring the performance of early quantum computers. Moreover, the algorithm is designed to take advantage of the strengths of a given architecture. That is, if some gates or quantum operations may be performed with higher fidelity, then the algorithm can leverage these strengths in the design of the quantum hardware ansatz. Perhaps one of the most interesting features of the algorithm is its ability to variationally suppress some forms of quantum errors, which is discussed later in this work.

Hamiltonian

- Let us consider a quantum system S composed of N qubits which will act as our quantum computer, and a Hamiltonian H of a different system Q that need have no relation to S other than acting on a space of $\leq N$ qubits. This Hamiltonian could be derived from a physical system such as a collection of interacting spins or the discretization of an interacting electronic system. Similarly it could come from the encoding of an optimization problem or the problem Hamiltonian in adiabatic quantum computation. In all of these instances, one is interested in the eigenvectors $|\lambda_i\rangle$ and eigenvalues, λ_i of the Hamiltonian H , and the goal will be to find and study these eigenvectors and eigenvalues using S .

Low Energy State

- We order the eigenvectors by the eigenvalues such that $\lambda_1 \leq \lambda_2 \leq \dots \leq \lambda_N$. Indeed in many cases, the eigenvectors corresponding to the lowest few eigenvalues and their properties are of primary interest. In physical systems this is because low-energy states play a dominant role in the properties of the system at modest temperatures, and in optimization problems they often encode the optimal solution.

Algorithm Outline

1. Prepare the state $|\psi(\vec{\theta})\rangle$ or $\rho(\vec{\theta})$ on the quantum computer, where $\vec{\theta}$ can be any adjustable experimental or gate parameter.
2. Measure the expectation value $\langle H \rangle(\vec{\theta})$
3. Use a classical non-linear optimizer such as the Nelder-Mead simplex method to determine new values of $\vec{\theta}$ that decrease $\langle H \rangle(\vec{\theta})$
4. Iterate this procedure until convergence in the value of the energy. The parameters $\vec{\theta}$ at convergence define the desired state

A variational eigenvalue solver on a quantum processor

Alberto Peruzzo et al.

2013

<https://arxiv.org/pdf/1304.3061.pdf>

Quantum computers promise to efficiently solve important problems that are intractable on a conventional computer. For quantum systems, where the dimension of the problem space grows exponentially, finding the eigenvalues of certain operators is one such intractable problem and remains a fundamental challenge. The quantum phase estimation algorithm can efficiently find the eigenvalue of a given eigenvector but requires fully coherent evolution. We present an alternative approach that greatly reduces the requirements for coherent evolution and we combine this method with a new approach to state preparation based on ansatzes and classical optimization. We have implemented the algorithm by combining a small-scale photonic quantum processor with a conventional computer.

量子アニーリング

John Preskill “Quantum Computing in the NISQ era and beyond”
<https://arxiv.org/pdf/1801.00862.pdf> から

量子アニーラー

- 量子技術の現在のマイルストーンとして50～100qubitを強調したが、実際には2000qubitの量子デバイス、D-Wave 2000Qマシンがある。このマシンは、量子ゲート回路ベースの量子コンピュータではない。我々は、それをむしろ量子アニーラーと呼んでいる。量子回路の実行とは異なる方法を用いて最適化の問題を解こうとし、これらの問題を成功裏に解決することも多い。
- しかし今のところ、量子アニーラーが、同じ問題に対して最良のアルゴリズムを実行する最高の古典的ハードウェアと比較して、解答までの時間を本当に高速化できるのかという点で説得力のある理論的議論や説得的な実験的証拠はない。状況は少し微妙である。

断熱量子コンピューティング

- ❑ 量子アニーラーは、断熱量子コンピューティング (adiabatic quantum computing) と呼ばれるもののノイズの多いバージョンである (D-Waveマシンの場合、量子ビットは、かなり品質は低い)。ノイズのない量子ビットの場合、断熱量子コンピューティングが回路ベースの量子コンピューティングと同じくらい強力であることを示す論理的な議論が実際にある。
- ❑ しかし、断熱的方法と量子ゲート回路に基づく量子計算の等価性を示す議論は、断熱的方法が、量的アニーラーが現在使用されている方法とはかなり異なる付加的な物理的量子ビットで高いオーバーヘッドコストを必要とする形式で実行される場合にのみ適用される。

non-stoquasticな量子アニーラー

- いずれにしても、この正式な議論はノイズのない量子ビットにのみ適用され、回路ベースの量子コンピューティングとは対照的に、量子アニーリング装置がスケールラブルであることを証明する良い理論的議論はない。つまり、ノイズの多い量子ビットの場合、ノイズに対して頑強なものにする為のオーバーヘッドコストを受け入れたとしても、量子アニーラーが問題サイズの増加とともに正常に動作することを示す方法は分らないのだ。
- 今のところ量子アニーラーは、アニーリングが安定している場合に主に適用されている。このことは、古典的なコンピュータが量子アニーラーの動作をシミュレートすることは比較的容易だということを意味する。間もなく予定されているのは、non-stoquasticな量子アニーラーである。これは、最高の古典的なアルゴリズムで可能な速度よりも高速化を達成する可能性がある。

- 理論家は量子アニーリングが強力であるかどうかを決定していないので、さらなる実験が必要である。今後数年間の量子アニーラーの実験は、かなり有益である可能性が高い。特に、量子アニーラーの古典的な最適化問題への応用以外にも、量子シミュレーション問題への応用も検討すべきである。

量子ディープラーニング

John Preskill “Quantum Computing in the NISQ era and beyond”
<https://arxiv.org/pdf/1801.00862.pdf> から

量子機械学習

- 機械学習は技術を変革し、科学にも大きな影響を与えている。それゆえ、量子技術と機械学習の組み合わせの可能性について、いろいろ考えるは当然である。「量子機械学習」には様々な概念がある。この主題に関する文献の多くは、線形代数とそれに関連するタスクを高速化する量子アルゴリズムをベースにしており、そのような応用については今後のサブセクションで取り上げたい。
- まず最初に、量子ディープラーニングの可能性について述べたい。ディープラーニングそのものは広い主題を扱うのだが、ここでは、具体的には制限付きボルツマンマシンrestricted Boltzmann machine (RBM)を検討しよう。

制限付きボルツマンマシン

- 制限付きボルツマンマシンは、低いがゼロではない温度で熱平衡状態にあるスピン系とみなされ、多くの隠れたスピン層が入力と出力を分離する。（「制限された」という言葉は、所与の層内のスピン間に結合がなく、連続する層のスピンのみが結合されることを意味している）
- システムは、入力と出力の間の望ましい結合確率分布を達成するために、訓練段階中に最適化される。訓練は教師付きで行われてもいい。例えば、ネットワークにラベル付けされた写真のセットを認識するように教えることができる。教師なしの場合、訓練の目標はラベルなしのトレーニングデータセットのパターンを識別することである。

量子制限付きボルツマンマシン

- こうしたマシンの量子類似版は、古典的制限付きボルツマンマシン RBMと類似の構造および機能を有することができる。ただし、スピンは古典的なビットではなく量子ビットである。
- 量子ディープラーニング・ネットワークは古典的なものよりも利点があるかもしれない。たとえば、いくつかの目的のためには、量子版を訓練するほうが簡単かもしれない。しかし、我々はそれを本当に知っていない。それを試して、それがどれくらいうまくいくかを試して見るいい機会である。

量子機械学習とQRAM

- 量子機械学習の可能性に期待する理由の1つは、QRAM(量子ランダムアクセスメモリ)という概念にある。QRAMとは、 N 個の成分をもつベクトルを $\log N$ 個のqubitで符号化することで、大量の古典的データを非常に簡潔に表現することを意味する。
- しかし、量子機械学習の応用の典型的な提案では、厳しい入力/出力ボトルネックによって混乱することになる。大規模な古典的なデータセットへの応用では、QRAMへの入力を符号化するコストを考慮に入れるべきであり、それが潜在的な利点を無効にする可能性がある。
- さらにいえば、量子ネットワークからの出力自体が量子状態である。すなわち、有益な情報を得るためには、この量子状態を測定する必要がある。 $\log N$ 個のqubitの一回の測定では、 $\log N$ ビット以上の古典的な情報を取得することはできない。

QRAMのボトルネック

- これらのボトルネックは、古典的なデータの相関を知るために量子ネットワークを訓練しようとするときに発生する。おそらく、入力と出力の両方が量子状態であるという設定で、量子機械学習について考えてみるのが、より自然である。
- したがって、例えば、それが、複雑な量子システムを制御するために使用される場合、量子ネットワークが古典的ネットワークよりも利点があると期待することができる。より広く言えば、量子もつれが重要な役割を果たす確率分布を学習しようとする場合、量子ディープラーニングは古典的なそれよりも強力であると思われる。
- つまり、量子ディープラーニング・ネットワークは量子的なタスクに非常に適しているかもしれないのだが、今日広く普及しているディープラーニングのアプリケーションでは、量子ネットワークに利点があるのかどうかは不明である。

- 量子ディープラーニングの可能性を励ます側で述べれば、量子ディープラーニング・マシンは、必ずしも汎用回路ベースの量子コンピュータである必要はないという点に注目する価値がある。それは特別な目的のデバイスになるかもしれない。おそらく、ノイズが低いものであれば、量子アニーラーが、それにあたる可能性がある。

QRAMと量子逆行列変換

John Preskill “Quantum Computing in the NISQ era and beyond”
<https://arxiv.org/pdf/1801.00862.pdf> から

HHLアルゴリズム

- QRAMは、量子アルゴリズムでは、さらに別の意味を持っている。特に、行列反転のタスクは、指数関数的な量子高速化を可能にし、多くの応用が可能である。
- HHLアルゴリズム（9年前に最初に議論した3人の著者 Hallow, Hassidim, Lloydの名前をとった）は、簡潔に表現された非常に大きな $N \times N$ 行列 A を入力とする。 A は十分に疎で条件づけされているものとする。入力の N 個の成分をもつベクトル $|b\rangle$ は、QRAMで符号化され $\log N$ 個のqubitの量子状態にエンコードされる。
- 量子アルゴリズムの出力は、小さな誤差で量子状態 $|A^{-1}b\rangle$ すなわち、入力ベクトル $|b\rangle$ に行列 A の逆行列を適用した結果である。この量子アルゴリズムは、古典的な行列反転に対して指数関数的に高速な時間 $O(\log N)$ で実行される。

HHLのボトルネック

- ただ、行列 A はスパースであり条件がよくなければならないという注意点とは別に、入力ベクトル $|b\rangle$ と出力ベクトル $|A^{-1}b\rangle$ の両方が量子状態であることに留意されたい。いったん出力状態になると、出力ベクトル $|A^{-1}b\rangle$ の特徴を学ぶための測定を実行することができ、このスキームを何度も繰り返すことにより、出力ベクトルについてより詳細に知ることができる。
- しかし、この行列反転アルゴリズムを古典的な入力データに適用しようとする場合、その古典的なデータをQRAMにロードする潜在的なコストを考慮する必要がある。これは指数関数的な高速化を無効にする可能性がある。代わりに、QRAMに古典的なデータをロードすることは、データベースから入力するのではなく、量子コンピュータ上で $|b\rangle$ を計算することによって回避することができる。

BQP-完全な問題

- この量子行列反転アルゴリズムは、我々がBQP-完全問題と呼ぶものを解決するもので、強力なものであると信じる十分な理由がある。つまり、量子コンピュータで効率的に解決できるどんな問題も、この行列反転問題の一例として問題をエンコードすることができる。
- また、潜在的に有用な多くのアプリケーションが提案されている。たとえば、この行列反転アルゴリズムを使用して、古典的な線形方程式（場を空間格子上で離散化し、適切な前処器を適用した後）に近似解を見つけることができる。この手順は、例えば、アンテナの性能を最適化するために、複雑な3次元形状の電磁気方程式を解くために使用することができる。

- 私は、HHLが最終的に影響の大きい応用を持つことを期待しているが、NISQ時代には実現することはない。このアルゴリズムはおそらく、エラー訂正を使用しない量子コンピュータでうまく実行されるには高いものにつきすぎる。

Preconditioned quantum linear system algorithm

B. D. Clader, B. C. Jacobs, C. R. Sprouse

2013

<https://arxiv.org/abs/1301.2340>

We describe a quantum algorithm that generalizes the quantum linear system algorithm [Harrow et al., Phys. Rev. Lett. 103, 150502 (2009)] to arbitrary problem specifications. We develop a state preparation routine that can initialize generic states, show how simple ancilla measurements can be used to calculate many quantities of interest, and integrate a quantum-compatible preconditioner that greatly expands the number of problems that can achieve exponential speedup over classical linear systems solvers. To demonstrate the algorithm's applicability, we show how it can be used to compute the electromagnetic scattering cross section of an arbitrary target exponentially faster than the best classical algorithm.

- We have demonstrated a quantum algorithm that generalizes the QLSA to solve arbitrary linear systems. We show how simple ancilla measurements can efficiently calculate many useful quantities of interest from the exponentially large solution space.
- Additionally, we have greatly expanded the class of problems that can be solved with exponential speedup, by incorporating matrix preconditioning into the quantum algorithm.

- To demonstrate its functionality we showed how one could use it to solve an electromagnetic scattering problem using the finite element method and estimate the scattering cross section. We show that this can be done in a time exponentially faster than the best classical algorithm.
- This opens up the potential for quantum computing to be applied to a broad class of problems of practical interest to the computational physics community.

Quantum algorithms and the finite element method

Ashley Montanaro, Sam Pallister

2016

<https://arxiv.org/pdf/1512.05903.pdf>

The finite element method is used to approximately solve boundary value problems for differential equations. The method discretises the parameter space and finds an approximate solution by solving a large system of linear equations. Here we investigate the extent to which the finite element method can be accelerated using an efficient quantum algorithm for solving linear equations. We consider the representative general question of approximately computing a linear functional of the solution to a boundary value problem, and compare the quantum algorithm's theoretical performance with that of a standard classical algorithm – the conjugate gradient method.

Prior work had claimed that the quantum algorithm could be exponentially faster, but did not determine the overall classical and quantum runtimes required to achieve a predetermined solution accuracy. Taking this into account, we find that the quantum algorithm can achieve a polynomial speedup, the extent of which grows with the dimension of the partial differential equation. In addition, we give evidence that no improvement of the quantum algorithm could lead to a super-polynomial speedup when the dimension is fixed and the solution satisfies certain smoothness properties.

Appendix A: Use of HHL for approximating the norm of the solution

- Assume that we have an s -sparse system of linear equations $Ax = b$, for some Hermitian $N \times N$ matrix A such that $\lambda_{\max}(A) \leq 1$, $\lambda_{\min}(A) \geq 1/\kappa$. We would like to approximate $\|x\|$ up to accuracy $\epsilon\|x\|$ using the HHL algorithm.
- Note that quantum linear equations algorithms subsequent to HHL achieved better dependence on κ, ϵ or both for the task of producing $|x\rangle$; however, it does not seem obvious how to use these to achieve improved accuracy for estimating $\|x\|$.

Quantum Algorithm for Simulating the Wave Equation

Pedro C.S. Costa, Stephen Jordan, Aaron
Ostrander

2017

<https://arxiv.org/pdf/1711.05394.pdf>

We present a quantum algorithm for simulating the wave equation under Dirichlet and Neumann boundary conditions. The algorithm uses Hamiltonian simulation and quantum linear system algorithms as subroutines. It relies on factorizations of discretized Laplacian operators to allow for improved scaling in truncation errors and improved scaling for state preparation relative to general purpose linear differential equation algorithms. We also consider using Hamiltonian simulation for Klein-Gordon equations and Maxwell's equations.

Future Work

- It is an interesting open question whether our quantum algorithm is optimal. In particular, it is natural to ask whether an analogue of the no-fast-forwarding theorem from [18] could yield a lower bound for the complexity of the problem of simulating wave equations that matches the complexity of the algorithm presented here. It is also interesting to investigate the performance of quantum algorithms for simulating the wave equation based on finite element methods, rather than finite difference methods, as considered here. Lastly, one can consider extending the quantum algorithm presented here to more complicated wave equations.

HHLアルゴリズム QRAMと行列反転

Quantum algorithm for solving linear systems of equations

Aram W. Harrow, Avinatan Hassidim, Seth Lloyd
2009

<https://arxiv.org/pdf/0811.3171.pdf>

Abstract

Solving linear systems of equations is a common problem that arises both on its own and as a subroutine in more complex problems: given a matrix A and a vector b , find a vector x such that $Ax=b$. We consider the case where one doesn't need to know the solution x itself, but rather an approximation of the expectation value of some operator associated with x , e.g., $x'Mx$ for some matrix M . In this case, when A is sparse, N by N and has condition number κ , classical algorithms can find x and estimate $x'Mx$ in $O(N \sqrt{\kappa})$ time. Here, we exhibit a quantum algorithm for this task that runs in $\text{poly}(\log N, \kappa)$ time, an exponential improvement over the best classical algorithm.

- Linear equations play an important role in virtually all fields of science and engineering. The sizes of the data sets that define the equations are growing rapidly over time, so that terabytes and even petabytes of data may need to be processed to obtain a solution. In other cases, such as when discretizing partial differential equations, the linear equations may be implicitly defined and thus far larger than the original description of the problem.

Algorithm

- We sketch here the basic idea of our algorithm, and then discuss it in more detail in the next section. Given a Hermitian $N \times N$ matrix A , and a unit vector $\vec{b}$, suppose we would like to find $\vec{x}$ satisfying $A\vec{x} = \vec{b}$. (We discuss later questions of efficiency as well as how the assumptions we have made about A and $\vec{b}$ can be relaxed.)
- First, the algorithm represents $\vec{b}$ as a quantum state
$$|b\rangle = \sum_{i=1}^N b_i |i\rangle$$

Algorithm

- Next, we use techniques of Hamiltonian simulation to apply e^{iAt} to $|b\rangle$ for a superposition of different times t . This ability to exponentiate A translates, via the well known technique of phase estimation, into the ability to decompose $|b\rangle$ in the eigenbasis of A and to find the corresponding eigenvalues λ_j .
- Informally, the state of the system after this stage is close to $\sum_{j=1}^N \beta_j |u_j\rangle |\lambda_j\rangle$, where u_j is the eigenvector basis of A , and $|b\rangle = \sum_{j=1}^N \beta_j |u_j\rangle$

Algorithm

- We would then like to perform the linear map taking $|\lambda_i\rangle$ to $C_\lambda^{-1}|\lambda_j\rangle$, where C is a normalizing constant. As this operation is not unitary, it has some probability of failing, which will enter into our discussion of the run-time below.
- After it succeeds, we uncompute the $|\lambda_j\rangle$ register and are left with a state proportional to $\sum_{j=1}^N \beta_j \lambda_j^{-1} |u_j\rangle = A^{-1}|b\rangle = |x\rangle$.

QRAMとは何か？

Quantum random access memory

Vittorio Giovannetti, Seth Lloyd, Lorenzo Maccone

26 Mar 2008

<https://arxiv.org/pdf/0708.1879.pdf>

The quantum Random Access Memory

International Iran Conference on
Quantum Information (IICQI)

Kish Island

7-10 September 2007

Lorenzo Maccone

Quantum Information theory group,
Dip. "A. Volta", Univ. of Pavia

Vittorio Giovannetti
Scuola Normale Superiore

Seth Lloyd
MIT

Qubit
quantum information
theory group



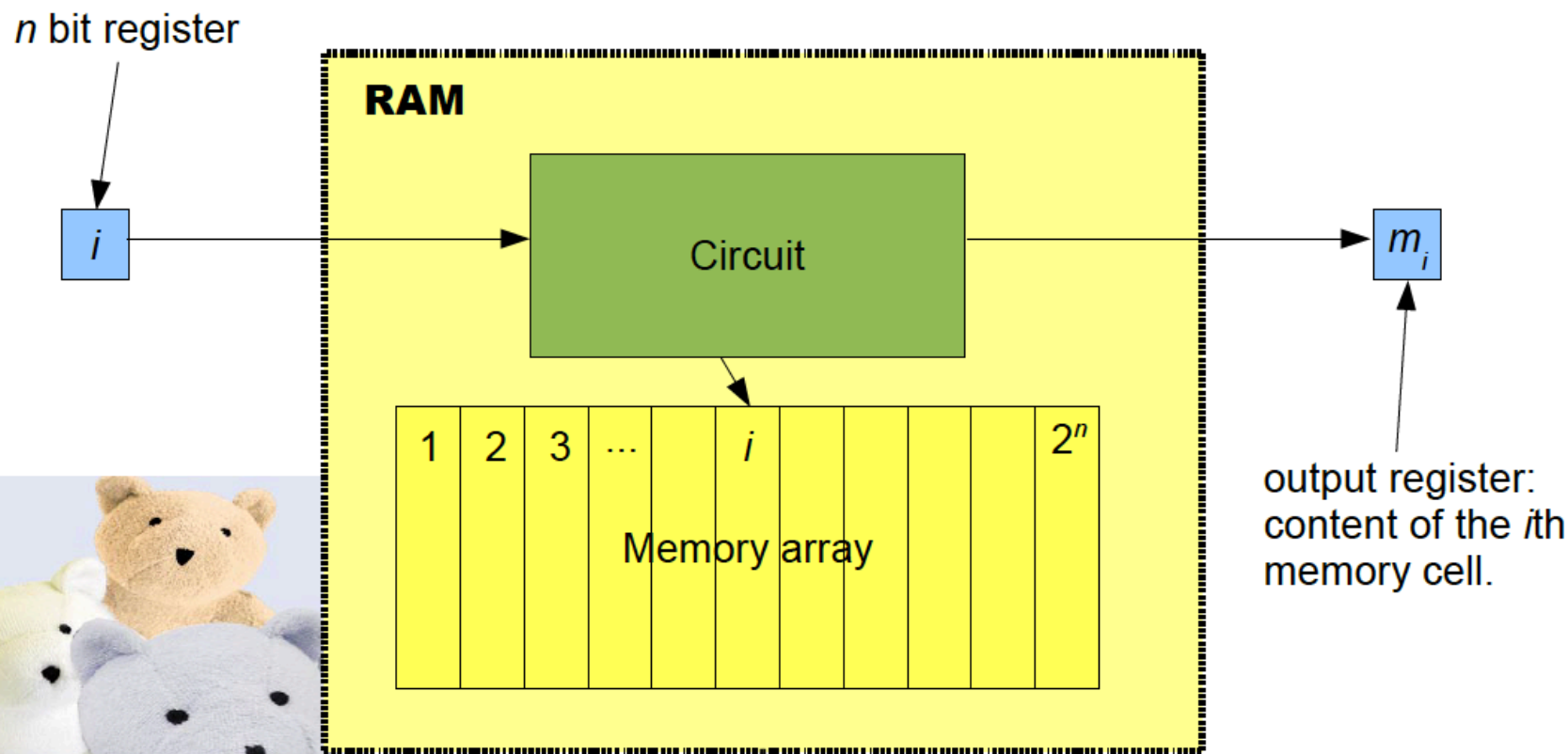
<https://goo.gl/2E9UbP>



www.qubit.it

Random Access Memory (RAM)

Each cell of a memory array can be univocally determined by its numerical address. An n -bit register can then address 2^n possible locations:

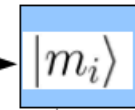
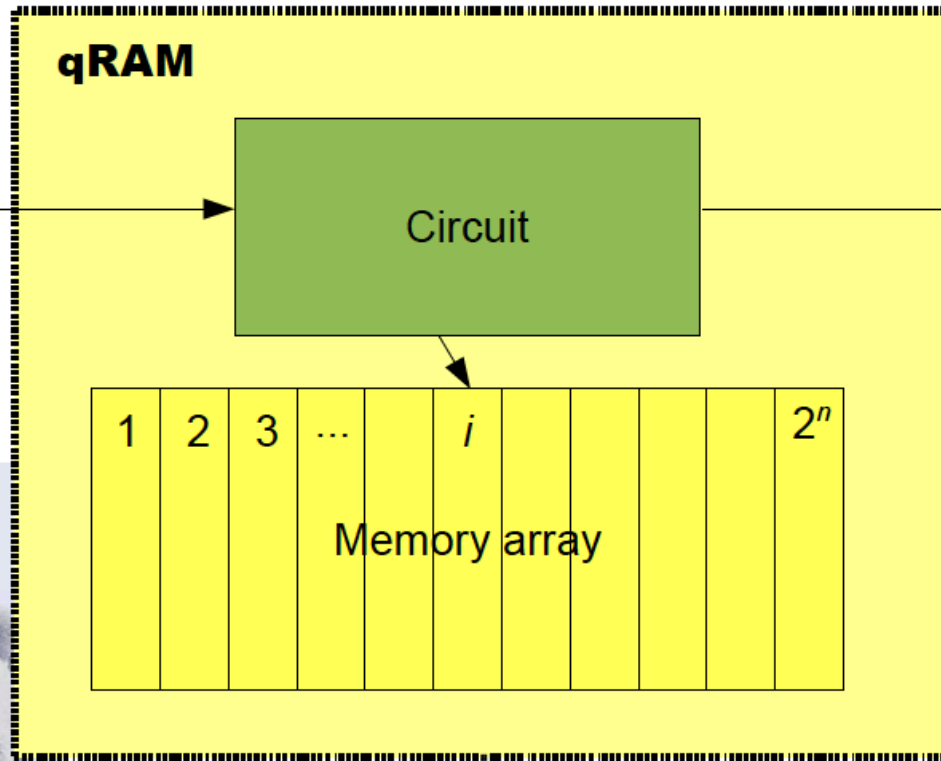


takes an n bit address as input,
provides the content of the memory cell as output

quantum Random Access Memory (qRAM)

Same as the previous, but the **index** and **output** registers are made of **qubits**!
(Eventually also is the memory array):

n qubit register



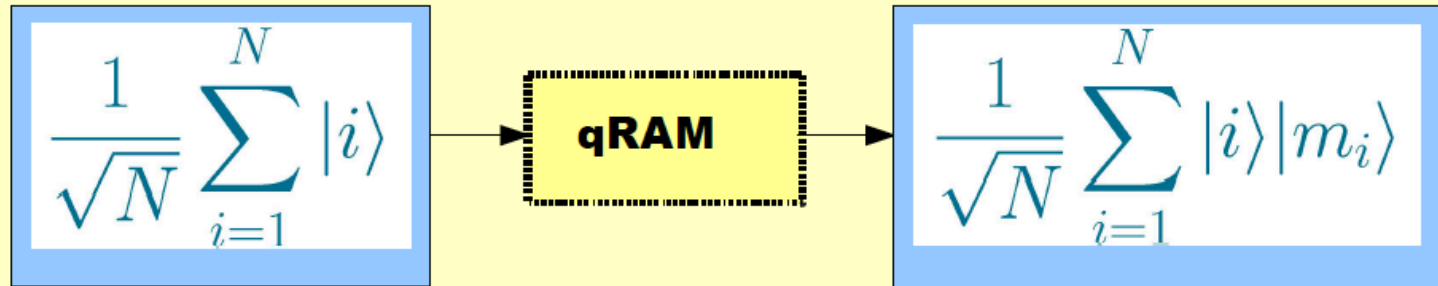
output register:
content of the i th
memory cell.



takes an n qubit address as input,
provides the content of the memory cell as output

...this has important consequences!

Suppose that the input register is in a superposition of querying for N different addresses:



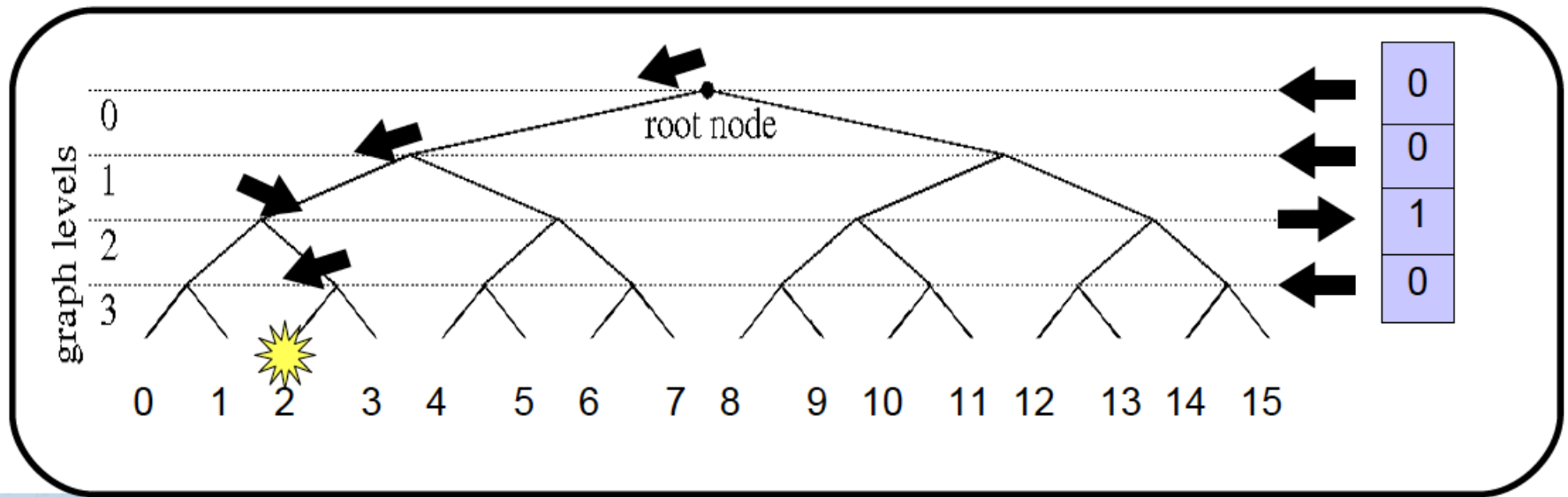
Now the output register is **ENTANGLED** with the input register!

Internal workings of conventional RAMs

E.g. address register = "2" =

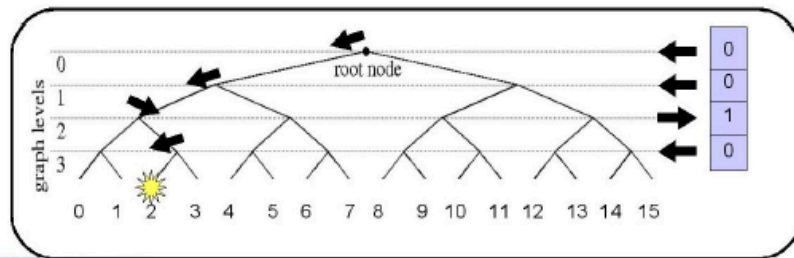
0	0	1	0
---	---	---	---

each register bit deviates the signal in one level of a bifurcation tree:

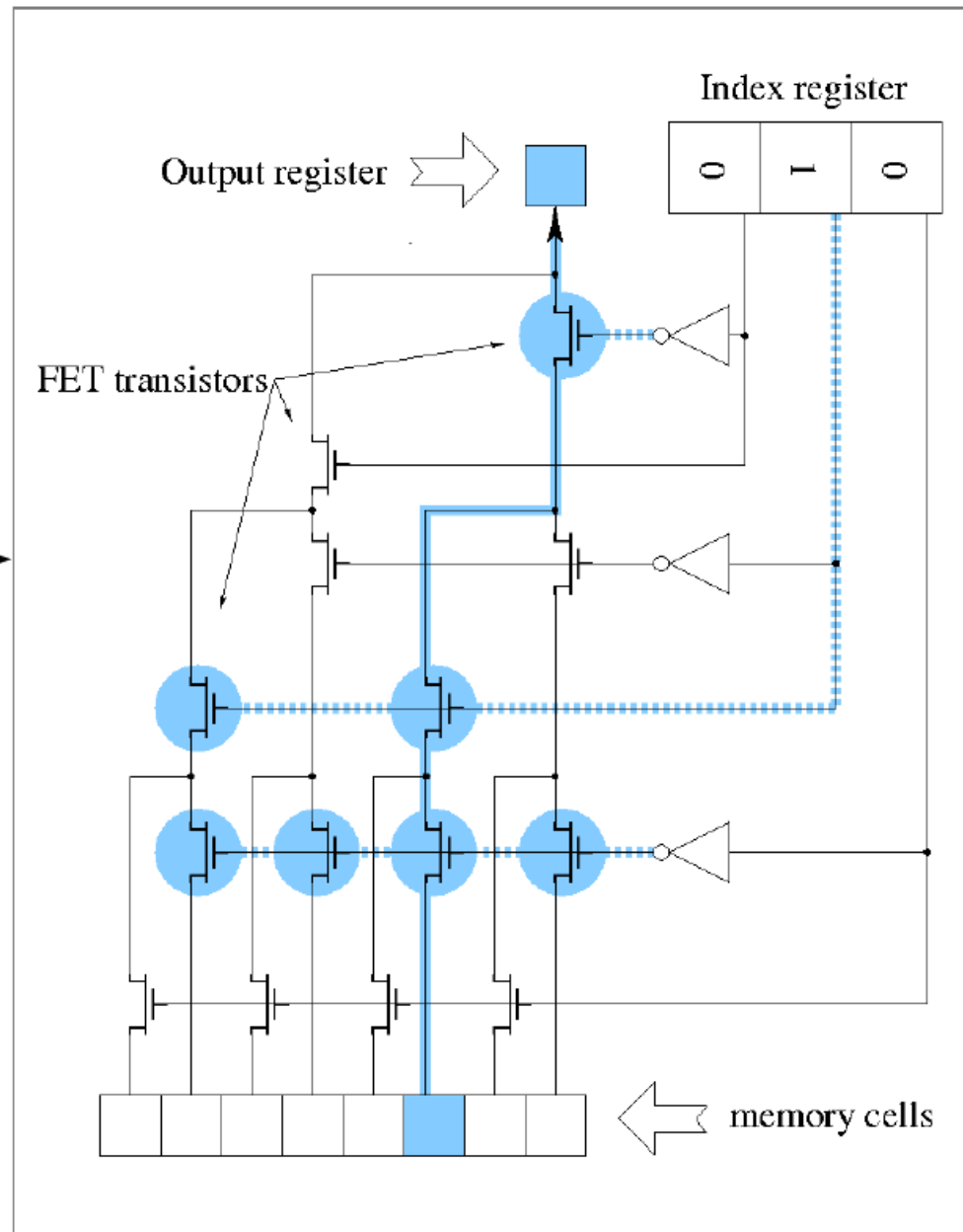


Internal workings of conventional RAMs 2

This ideal structure



is almost faithfully copied in circuit diagrams of conventional RAMs →

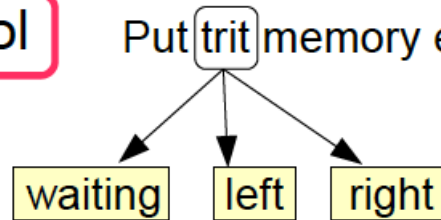


Bucket brigade

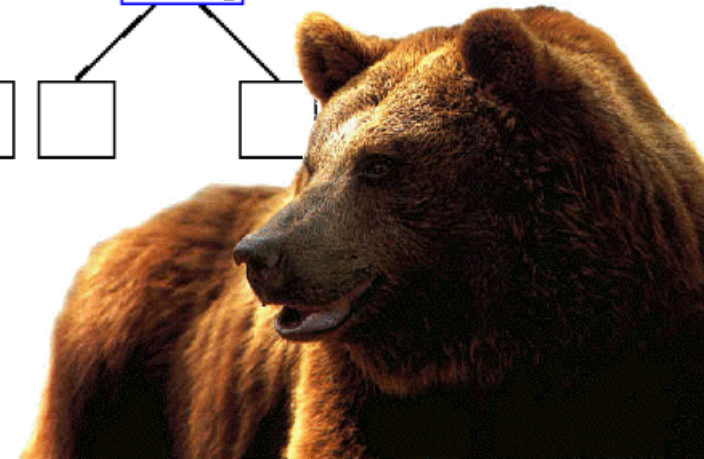
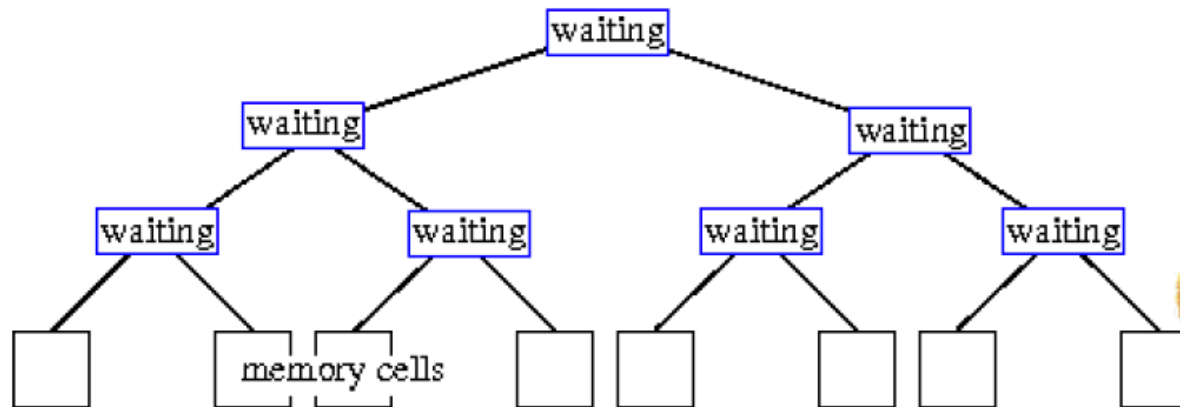
there's another way to implement the binary decision tree

bucket brigade protocol

Put trit memory elements in the tree nodes.



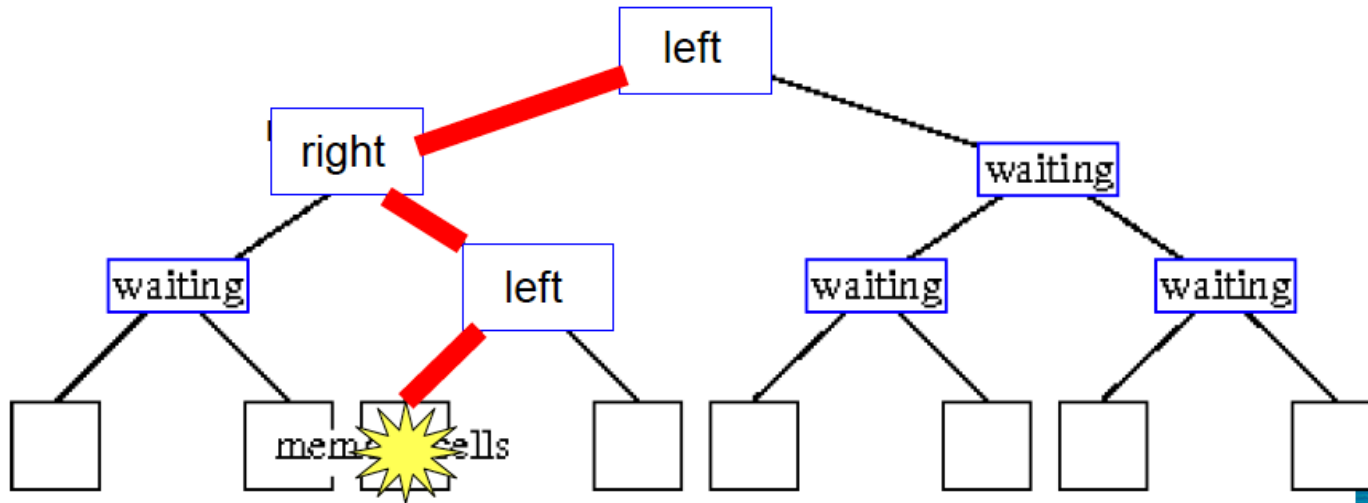
1. Initialize all of them in the “waiting” state:



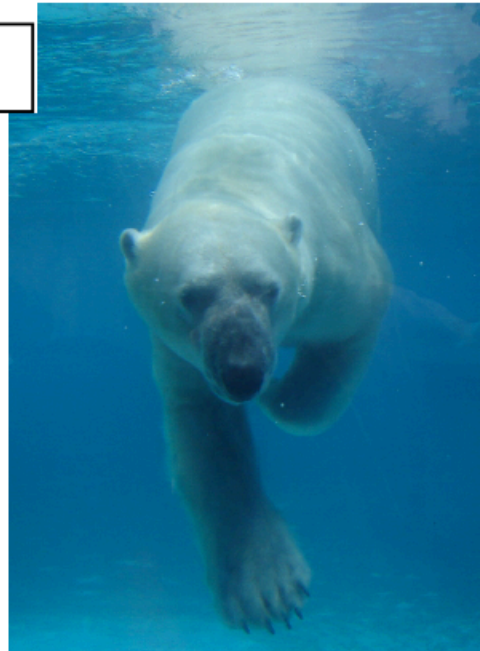
Bucket brigade 3

3. when all the address bits have been sent, there's a route carved in the tree:

e.g. for address register = 010:



4. extract the information through this route.



bucket brigade qRAM

It's very simple to quantize this RAM architecture:

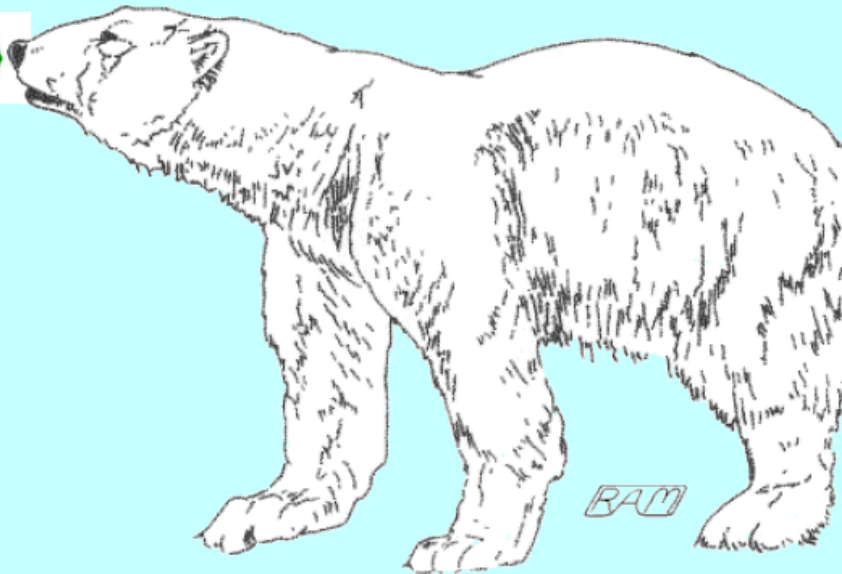
just use **qutrits** in place of trits (and little else)

three-level quantum systems

$|waiting\rangle$

$|left\rangle$

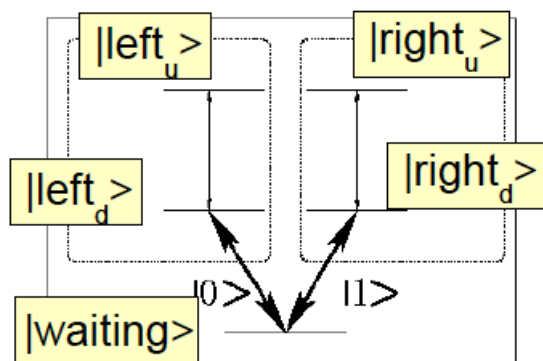
$|right\rangle$



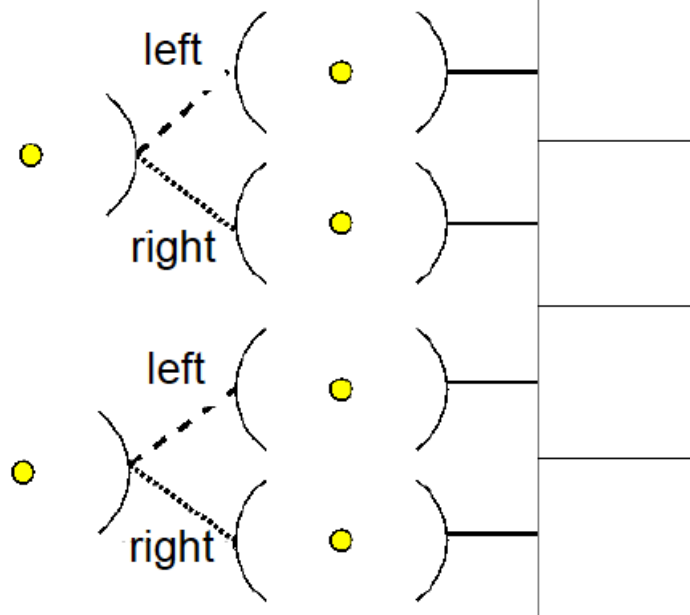
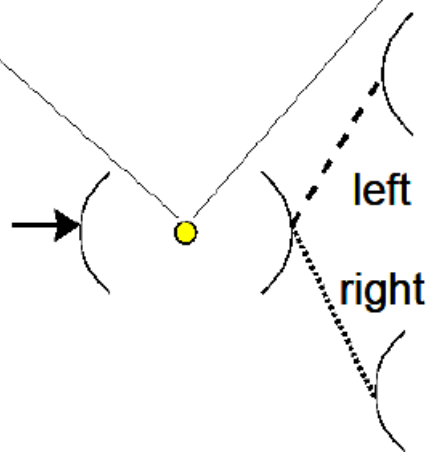
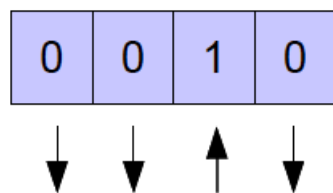
Implementation 2



Ions level structure



photons:



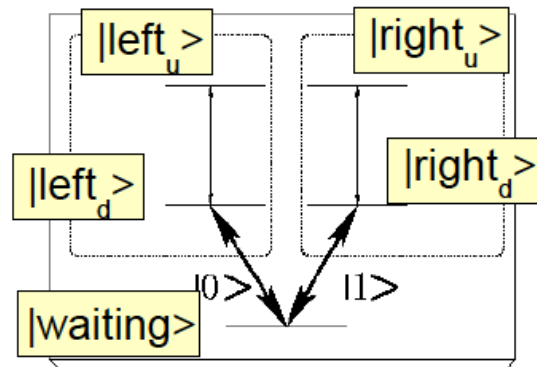
1. All the photons of the address register are sent in.

- if they encounter a ion in $|waiting\rangle$, they are stored either in level $|left_d\rangle$ or $|right_d\rangle$, depending on their polarization.
- if they encounter a ion in $|left_d\rangle$ or $|right_d\rangle$, they are re-emitted (using a Raman transition mediated through $|left_u\rangle$ and $|right_u\rangle$) and continue along the tree, to the left or to the right, respectively (the $|left_x\rangle$ and $|right_x\rangle$ levels are spatially coupled only to the left and right outgoing modes).

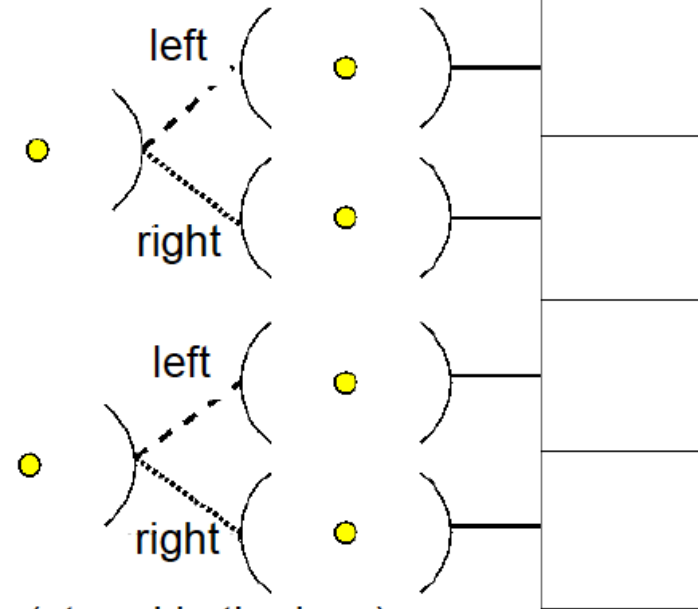
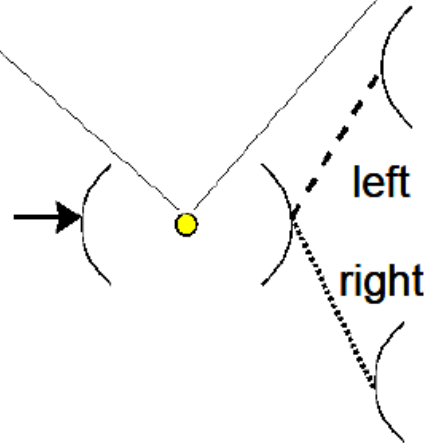
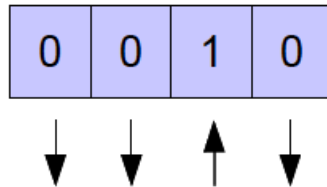
Implementation 3



Ions level structure



photons:



2. Now the bus photon is sent in
It follows the path carved by the address register photons (stored in the ions).
It reaches the memory cell, where it copies (or swaps) its content.
It is reflected back and exits at the tree root node with the memory cell content.
3. The address register photons are re-emitted one by one (starting from the last nodes in the tree
4. The memory has been accessed, the address register reobtained, and the network reset.

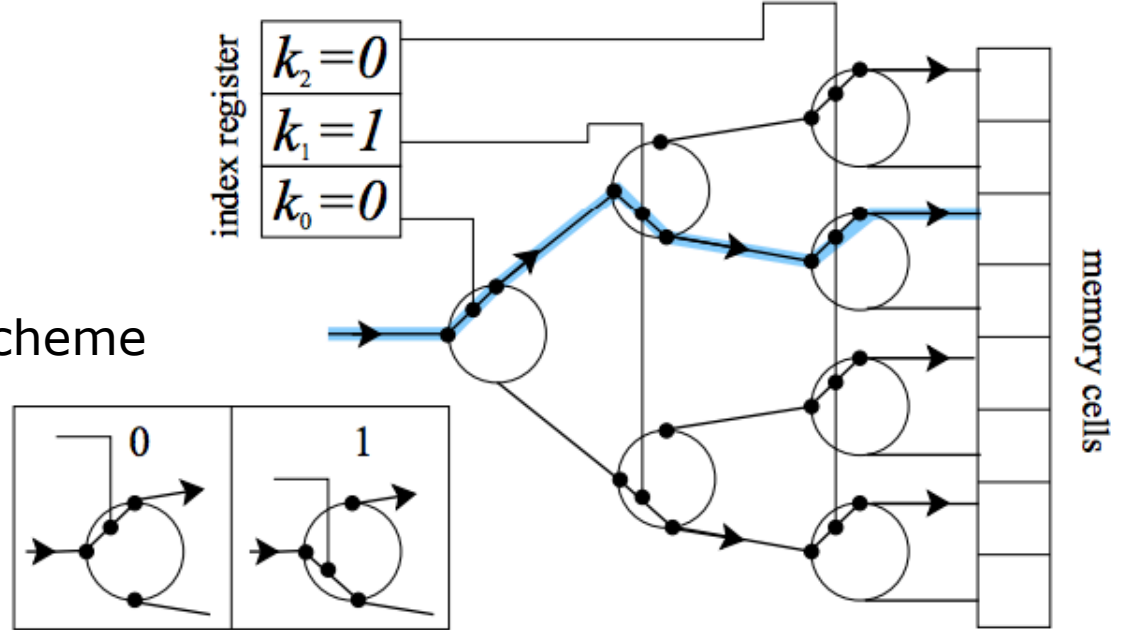
Architectures for a quantum random access memory

Vittorio Giovannetti , Seth Lloyd , Lorenzo Maccone

<https://arxiv.org/pdf/0807.4994.pdf>

- Here we analyze two different RAM architectures (the conventional fanout and the “bucket brigade”) and propose some proof-of-principle implementations which show that in principle only $O(n)$ two-qubit physical interactions need take place during each qRAM call. *That is, although a qRAM needs $O(2^n)$ quantum logic gates, only $O(n)$ need to be activated during a memory call.* The resulting decrease in resources could give rise to the construction of large qRAMs that could operate without the need for extensive quantum error correction.

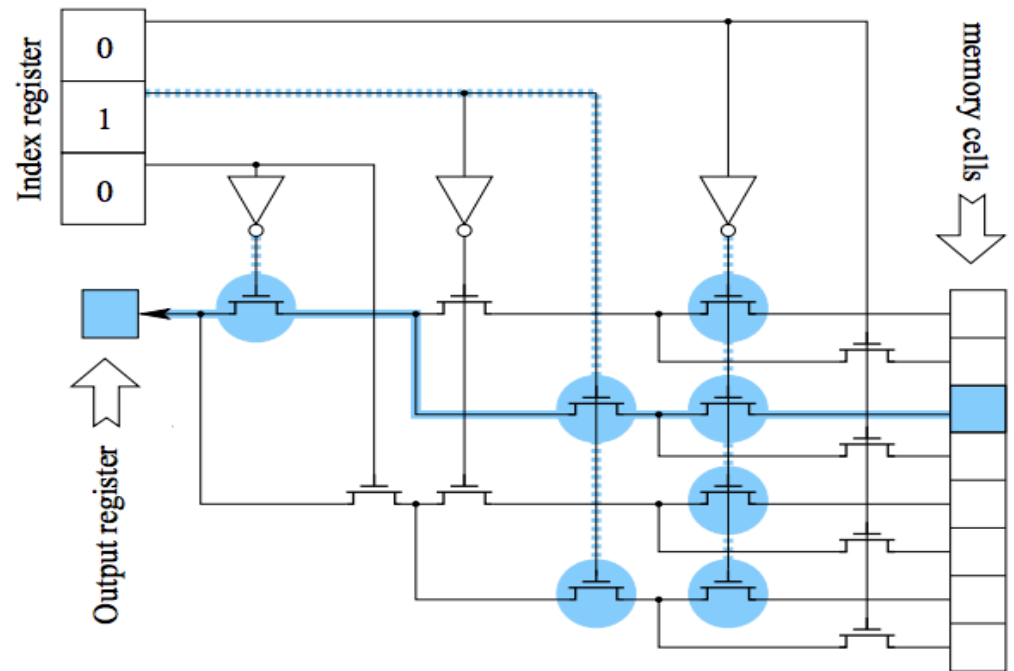
Schematic of the fanout addressing scheme



fanout

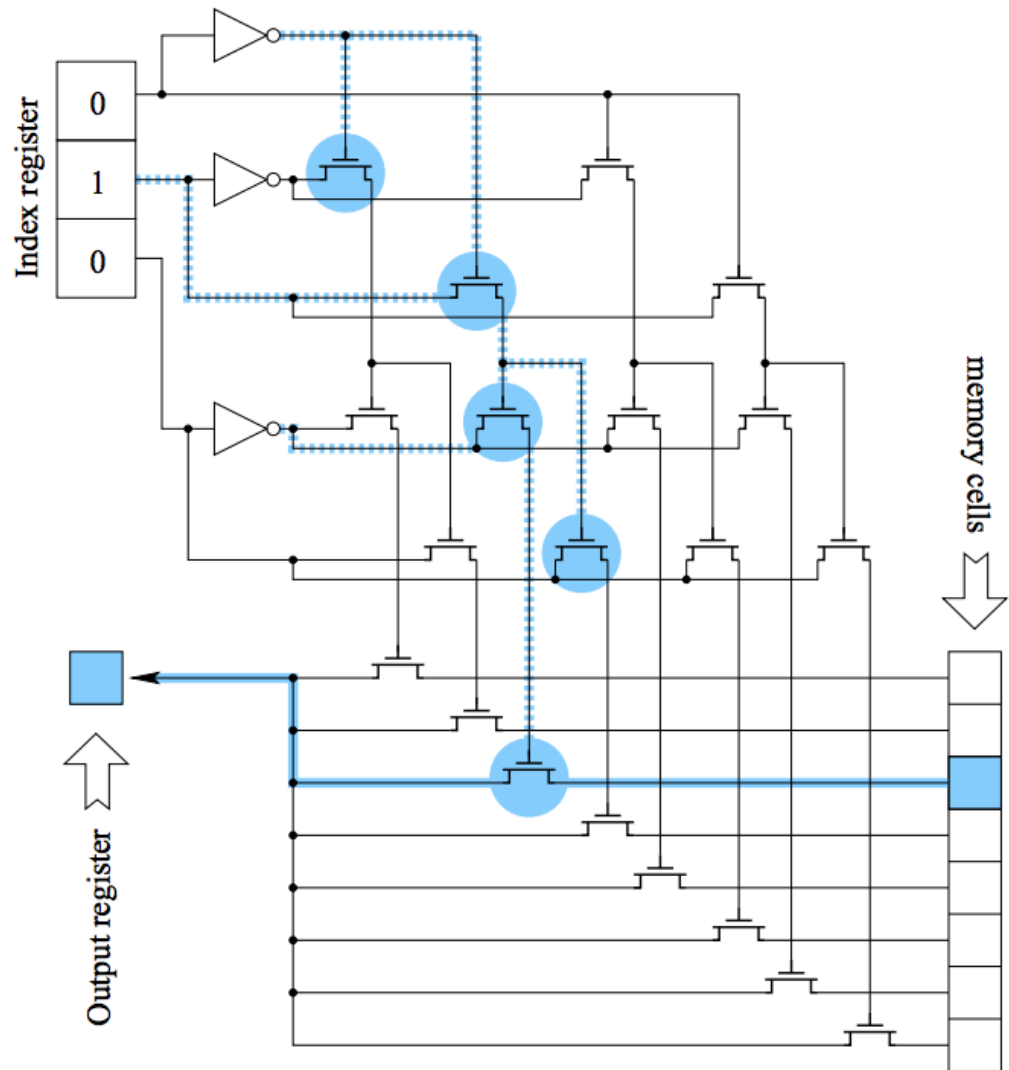
a)

typical electronic implementation



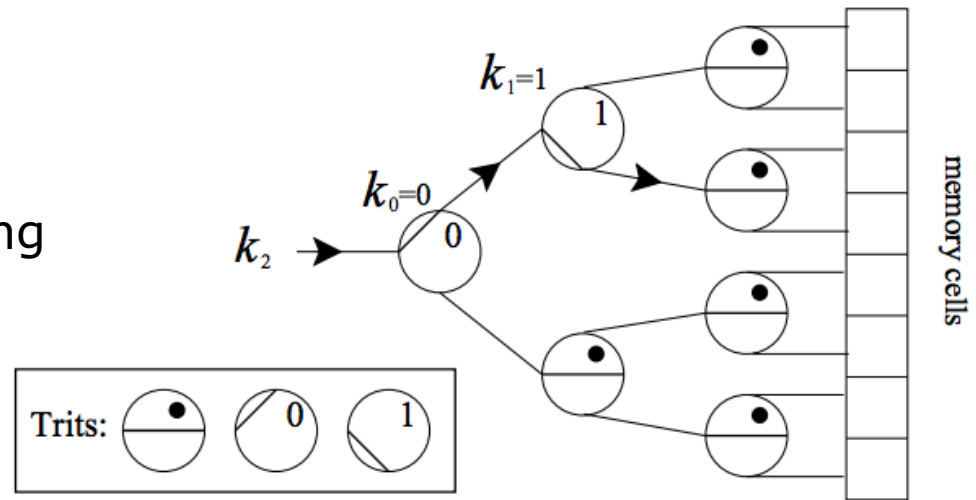
b)

fanout



Modification of the conventional fanout circuit of Fig. 1b. This architecture achieves memory addressing with the activation of only $O(n)$ transistors

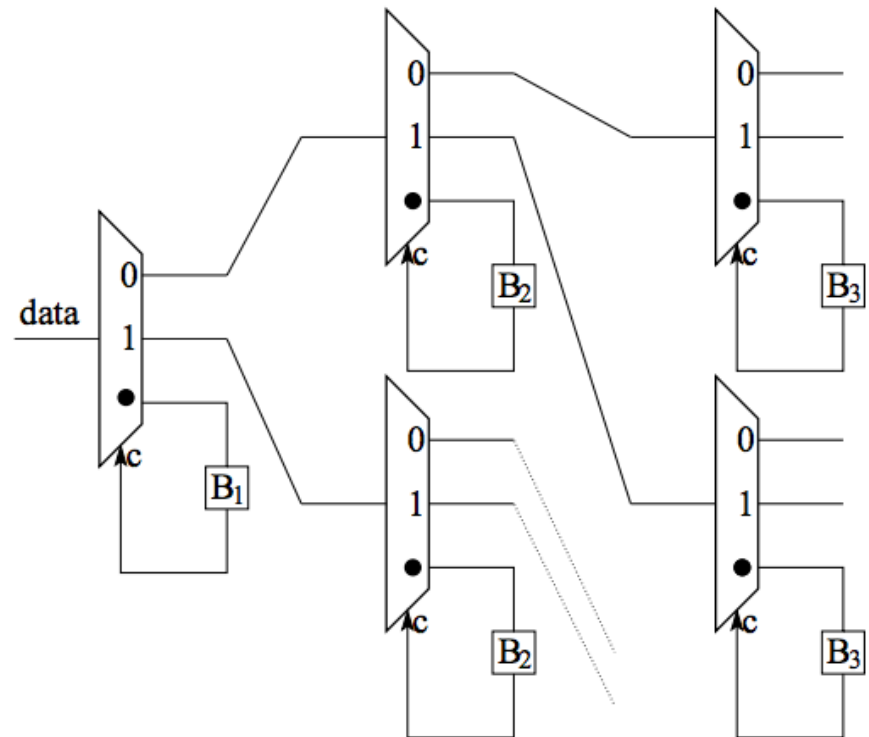
Schematics for the
bucket-brigade addressing
scheme



a)

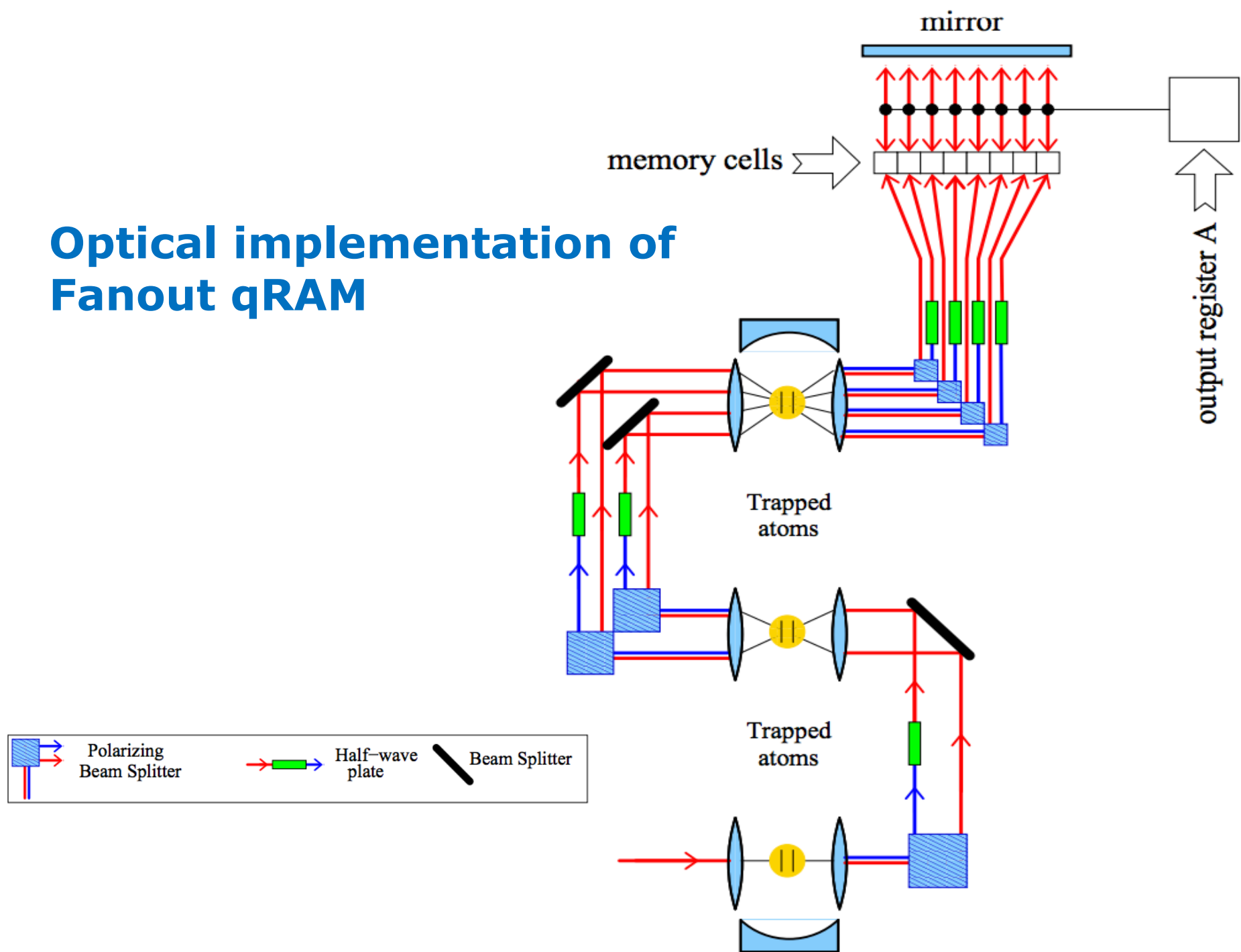
bucket-brigade

Electronic implementation
of the bucket-brigade

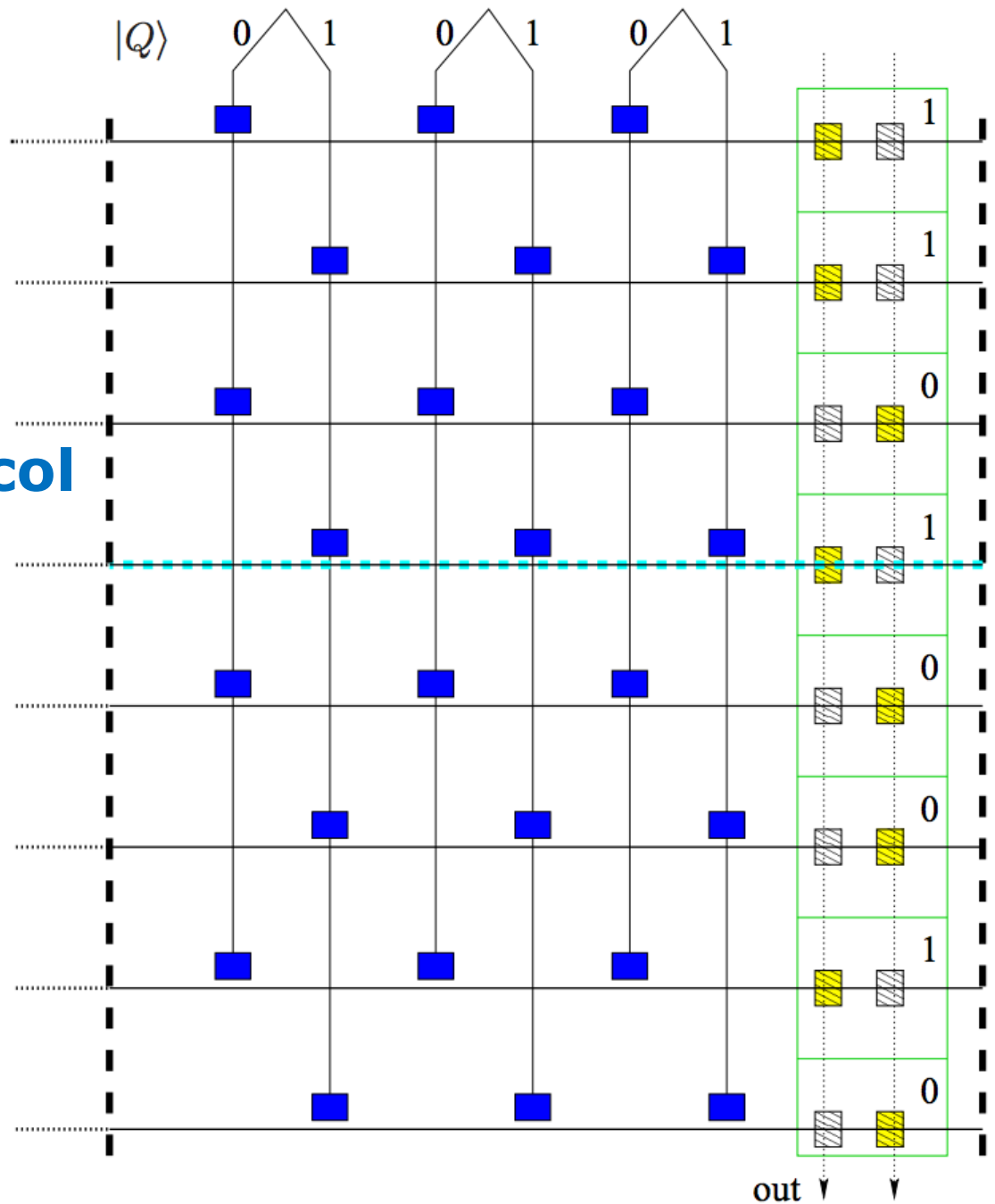


b)

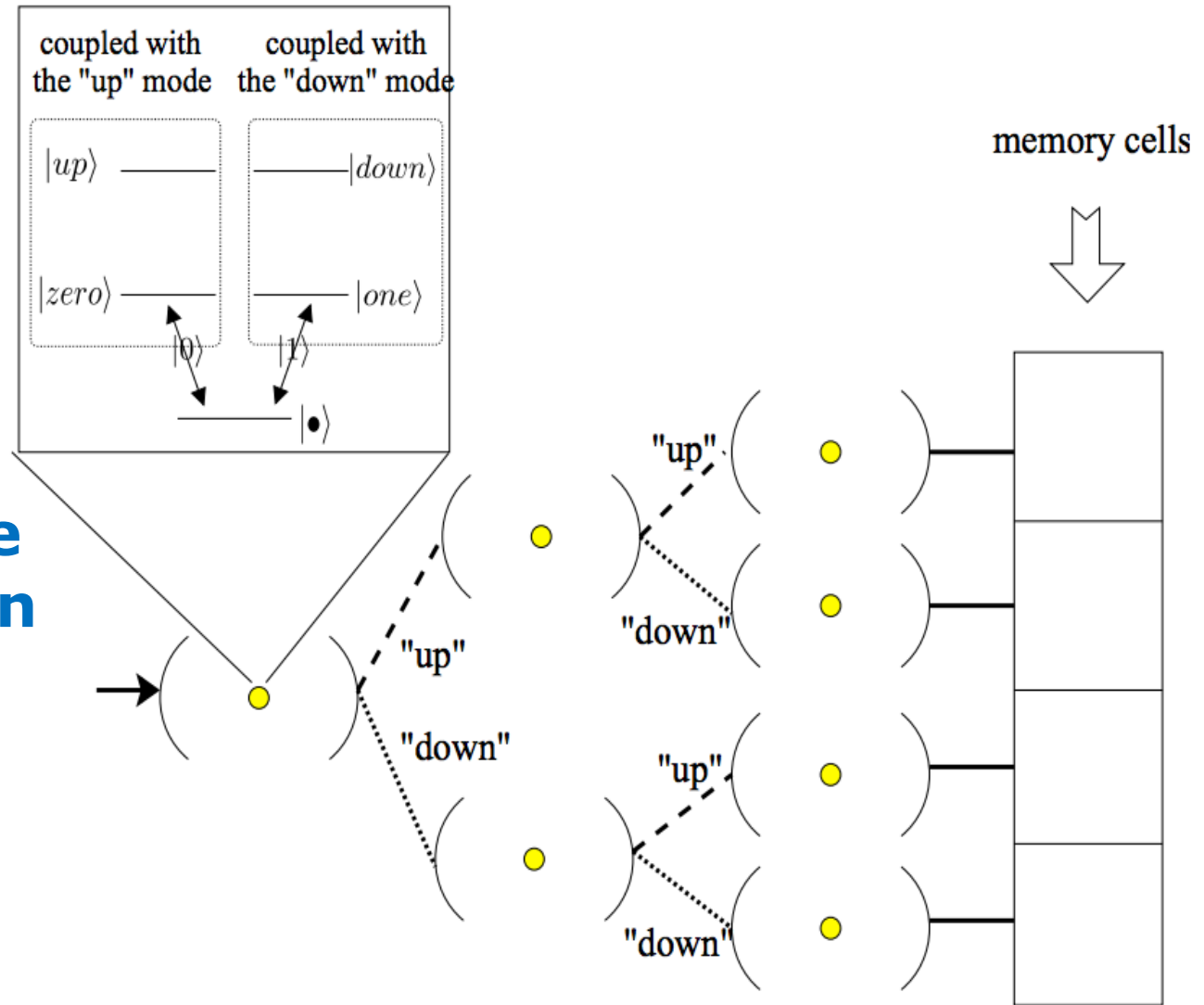
Optical implementation of Fanout qRAM



Phase-gate implementation of Fanout qRAM protocol



Bucket-brigade implementation



- This paper showed how quantum random access memories (qRAMs) might be implemented by using quantum optical and solid-state quantum information processing techniques. We proposed a new paradigm for constructing both classical and quantum RAMs, the bucket-brigade paradigm, in which the degree of fanout required to perform a memory call can be reduced exponentially, from $O(2^n)$ to $O(n)$.

半正定値プログラミング

John Preskill “Quantum Computing in the NISQ era and beyond”
<https://arxiv.org/pdf/1801.00862.pdf> から

半正定値プログラミング

- 半正定値プログラミングは、行列がある不等式の制約条件に従うという条件のもとで線形関数を最適化するタスクである。
- 具体的には、 $m + 1$ 個の $N \times N$ のエルミート行列 $\{C, A_1, A_2, \dots, A_m\}$ および実数 $\{b_1, b_2, \dots, b_m\}$ が入力として与えられた時、制約条件 $\text{tr}(A_i X) \leq b_i$ に従う $\text{tr}(CX)$ を最大にする正の半正定値の $N \times N$ 行列 X を見つけるという問題である。このタイプの凸最適化問題は広範な応用を有し、古典的には $\text{poly}(m, N)$ 時間で解くことができる。
- 最近発見された量子アルゴリズムは、 $\text{polylog}(N)$ 時間で近似解を発見する。これは指数関数的な高速化である。この量子アルゴリズムでは、出力は量子状態を表す密度演算子 ρ であり、それが最適な行列 X を近似することになる。この量子状態は、 X に関する情報を抽出するために測定することができ、その手順は詳細な情報を得る為、何回も繰り返される。

この量子アルゴリズムの利点

- しかし、この量子アルゴリズムの解析では、ある特定の形式の量子初期状態が利用可能であることを仮定している。その状態である熱的Gibbs状態は、半正定値プログラムの入力行列の線形結合であるハミルトニアンに関連付けられている。指数関数的な高速化が実際に実現できるかどうかは、このギブス状態が量子コンピュータを用いて効率的に準備できるかどうかにかかっている。
- 正しい構造の半正定値プログラムの場合、ギブス状態の効率的な準備が可能である。したがって、指数関数的な高速化が実際に可能となる。特に、半正定値プログラムのすべての入力行列が低いランクを有する場合、すなわち対応するハミルトニアンシステムが急速に熱平衡化する場合、量子アルゴリズムは指数関数的な高速化を達成する。

- これらの特性が実質的に関心のある半正定値的なプログラムにどの程度適用されるかはまだ明らかではない。この問題を明確にすることが、さらなる研究の重要な目標である。
- この量子アルゴリズムの重要なステップが、非ゼロ温度での熱的平衡状態の準備であることは興味深いことである。これは、このアルゴリズムが熱的ノイズに対して本質的な頑健性を有すること、また、このアルゴリズムの熱的平衡化の段階が量子アニーリングによって実行可能であることを示唆することができる。
おそらく、半正定値的プログラムのための量子ソルバーは、NISQ技術の範囲内にあるかもしれない。

線型計画法と半正定値プログラミング

線型計画法

- いくつかの1次不等式および1次等式(制約条件)を満たす変数の値の中で、ある1次式(目的関数)を最大化または最小化する値を求める方法。
- 例) 農業を営む人が、小麦と大麦のための A 平方キロメートルの農地を持っているとする。農家は限度 F で肥料、限度 P で殺虫剤を使用することができる。これらはそれぞれ単位面積あたり小麦が (F_1, P_1) 、大麦が (F_2, P_2) を必要とする。小麦の販売価格を S_1 、大麦の販売価格を S_2 、小麦を育てる領域を x_1 大麦を育てる領域を x_2 とすると、大麦と小麦をどれだけ育てればいいか

最大化: $S_1 x_1 + S_2 x_2$ (利益の最大化)

制約条件: $x_1 + x_2 \leq A$ (耕作地の制約)

$F_1 x_1 + F_2 x_2 \leq F$ (肥料の制約)

$P_1 x_1 + P_2 x_2 \leq P$ (殺虫剤の制約)

$x_1 \geq 0, x_2 \geq 0$ (非負制約)

シンプレックス法

- 「シンプレックス法は、実行可能解（超多面体の頂点）の1つから出発して目的関数の値をなるべく大きく（小さく）するようなところに移動させていく動作を繰り返して最適解を見つけ出す方法である。各ステップで必ず目的関数の値は改善される。」
- 「このアルゴリズムは、実用上は高速。ほとんど常に、変数の数・条件式の数の大きな方のオーダーの回数だけ反復を繰り返せば解ける。そのことは、1982年に スティーヴン・スメイル (Stephen Smale) が証明した。しかし、Dantzig が提唱したもの（ピボット規則）は多項式時間で終了しない問題例がある。常に多項式時間で解が得られるピボット規則の存在性は、現在も未解決問題である。」

半正定値計画問題

semidefinite programming

- エルミート行列 A の固有値が全て**非負**の場合に、その行列 A は**半正定値**であるという。(全て正の場合は**正定値**)
- 「半正定値計画問題 (semidefinite programming) とは半正定値行列全体によって作られる凸錐体上での凸最適化問題 (convex optimization) の一つである. 半正定値計画問題は近年いくつかの理由で成長している最適化の一分野である. その理由として多くの実用例が考えられることがあげられるが, 特にオペレーションズ・リサーチや組み合わせ最適化などの分野で広く研究が行われている. 自動制御理論の分野では半正定値計画問題が線形不等式制約のもとで行われることが多い.また半正定値計画問題の階層化により多項式最適化問題が近似的に解けるほか, 複雑系の最適化にも応用が可能である. 」

半正定値計画問題 semidefinite programming

- 線形計画問題はある空間上で多面体に含まれるような実数の組に対して、線形の目的関数を最小化・最大化する問題である。ここで、多面体というのは、より厳密には凸集合であるということを指す。一方で、半正定値計画問題においては、ベクトルの内積を最適化する。

$$\begin{aligned} \min_{x^1, \dots, x^n \in \mathbb{R}^n} \quad & \sum_{i,j \in [n]} c_{i,j} (x^i \cdot x^j) \\ \text{subject to} \quad & \sum_{i,j \in [n]} a_{i,j,k} (x^i \cdot x^j) \leq b_k \quad \forall k. \end{aligned}$$

量子リコメンデーション

John Preskill “Quantum Computing in the NISQ era and beyond”
<https://arxiv.org/pdf/1801.00862.pdf> から

量子リコメンデーション

- 最近提案されたもう1つの量子アルゴリズムは、有益なタスクのための現在知られている最高の古典的アルゴリズムよりも指数関数的な高速化を提供する。このアルゴリズムの目標は、顧客および他の顧客の好みの限られた知識に基づいて、顧客がおそらく好むであろう製品を顧客に推奨することである。
- 問題の簡略化されたバージョンを定式化するには、 m 人の顧客と n 個の製品を考え、 P を次のような二値の値をとる $m \times n$ の行列とする。顧客 a が製品 i を好む場合は $P_{ai} = 1$ 、顧客が製品 i を嫌う場合は $P_{ai} = 0$ となるようにする。実際には、 $m \approx 10^8$ 人のユーザーと $n \approx 10^6$ の製品を持つかもしれないが、行列のランク k は比較的小さく、おそらく $k \approx 100$ となる。このランクの小ささは、顧客のタイプの数に限られていることを示している。したがって、新しい顧客の好みのいくつかを知ったら、顧客が好む他の製品を正確に推奨することができる。

リコmend・システムのアルゴリズム

- リコmend・システムのためのアルゴリズムは2つの段階もつ。オフラインで実行される第1段階では、嗜好行列 P に対する低いランクの近似が構築される。第2段階では、オンラインで実施され、新しい顧客はいくつかの嗜好を明らかにし、システムは、その顧客が高い確率で好む推奨を出力する。
- 量子スピードアップを認めるのはこの第2のオンラインステージである。量子ランタイムは $O(\text{poly}(k)\text{polylog}(mn))$ だが、既知の最良の古典的なアルゴリズムでは、 $\text{poly}(mn)$ が高い値の推奨値を返すために時間が必要となる。
- 重要なのは、古典的アルゴリズムとは対照的に、量子アルゴリズムは完全な推奨行列を再構成しようとはしないということである。代わりに、 P の低ランクの近似から効率的にサンプリングをする。

- これは、機械学習の現実の応用のための重要な量子高速化であり、こうした別の高速化が発見されるだろうという希望を励ますものだ。
- しかし、現在、量子リコメンデーションシステム ($\text{polylog}(mn)$ 時間で高品質のリコmendを返す) によって実行されるタスクが古典的に不可能であることを示す納得のいく理論的議論はない。そのような議論を定式化することは、量子コンピュータが機械学習に重大な影響を及ぼすという我々の自信を強めるだろう。しかし、ここでもこのアルゴリズムはNISQ時代に確かに妥当性が確認されるには高価すぎるだろう。

Quantum Recommendation Systems

Iordanis Kerenidis, Anupam Prakash

<https://arxiv.org/pdf/1603.08675.pdf>

Abstract

- In this work, we present a quantum algorithm for recommendation systems that has running time $O(\text{poly}(k)\text{polylog}(mn))$. All known classical algorithms for recommendation systems that work through reconstructing an approximation of the preference matrix run in time polynomial in the matrix dimension. Our algorithm provides good recommendations by sampling efficiently from an approximation of the preference matrix, without reconstructing the entire matrix. For this, we design an efficient quantum procedure to project a given vector onto the row space of a given matrix.

Introduction

- A recommendation system uses information about past purchases or ratings of products by a group of users in order to provide personalized recommendations to individual users. More precisely, we assume there are m users, for example clients of an online platform like Amazon or Netflix, each of whom have some inherent preference or utility about n products, for example books, movies etc. The user preferences are modeled by an $m \times n$ matrix P , where the element P_{ij} denotes how much the user i values product j .

The low-rank assumption

- The underlying assumption in recommendation systems is that one can infer information about a specific user from the information about all other users because, in some sense, the majority of users belong to some well-defined “types”. In other words, most people’s likes are not unique but fall into one of a small number of categories. Hence, we can aggregate the information of “similar” users to predict which products have high utility for an individual user. More formally, the assumption in recommendation systems is that the preference matrix P can be well approximated (according to some distance measure) by a low-rank matrix.

Our model

- First, we describe a simple and general model for online recommendation systems. We start with a hidden preference matrix T , where the element T_{ij} takes values 0 or 1 and indicates whether product j is “good” for user i . Such boolean matrices arise naturally in a “thumbs up / thumbs down” system, where users can declare whether they like or not a certain product. We can also easily construct such matrices from non-boolean preference matrices. For each user, we split the products into two categories, the “good” and the “bad” recommendations, based on the matrix entries.

- Our assumption is that the matrix T has a good low-rank approximation. The reasons that justify this assumption are the ones used already in the literature. As before, we believe that there is a small number of user types, and within each type the users “agree” on the high-value elements. This modelling of the users gives rise to a matrix T with a good low-rank approximation. Once we have defined the matrix T , then any algorithm that reconstructs a matrix close to T , will provide a good recommendation, since T is the indicator matrix of good recommendations.

Recommendations by Matrix Sampling.

- The low-rank approximation of the matrix T can be computed as follows: first, define the matrix $\hat{T}$, where with some probability each element of $\hat{T}$ is equal to the corresponding element in T normalized and otherwise it is zero. This matrix, that we call a subsample matrix, corresponds to the information the recommendation system has already gathered about the matrix T .
- Then, by performing a Singular Value Decomposition and computing the projection of this matrix to its top- k row singular vectors, we compute a matrix $\hat{T}_k$ which can be proven to be close to the matrix T , as long as T had a good rank- k approximation.

An efficient quantum algorithm for Matrix Sampling

- Here is where quantum computing becomes useful: we design a quantum procedure that samples from the row $(\hat{T}_k)_i$ in time $\text{polylog}(mn)$. Note that the quantum algorithm does not output the row $(\hat{T}_k)_i$, which by itself would take time linear in the dimension n , but only samples from this row. But this is exactly what is needed for recommendation systems: Sample a high-value element of the row, rather than explicitly output the entire row.