量子オートマトンの空判定は決定不能だったり可能だったりする

稲葉 一浩 (k.inaba)
http://www.kmonos.net/

2010/01/16　第4回決定不能の会

参考文献

- V. D. Blondel, E. Jeandel, P. Koiran, and N. Portier

"Decidable and Undecidable Problems about Quantum Automata"

SIAM J. Comput. 34-6, pp. 1464-1473 (2005)
http://arxiv.org/abs/quant-ph/0304082

量子オートマトンとは何か

（いくつかの定義がある。この論文での定義）

- n 状態の量子オートマトン (QFA) とは
  - n次元行ベクトル　s
  - n×n ユニタリ行列　Xa,　Xb, … (文字が {a,b,…}の時)
  - n×n 射影行列　P
  - 閾値　λ

ユニタリ = 列ベクトルが直交基底
（(v1 v2 … vn) なら vi と vj の内積が
If i=j then 1 else 0 ）
射影行列

量子オートマトンの例

- s = (0.6　0　0.8)

  状態1　と　状態3　の重ね合わせ状態

  観測すると 36% の確率で状態1、64%で3に見える

- Xa =　　Xb =　　P =

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \qquad \begin{bmatrix} 1/\sqrt{2} & -1/\sqrt{2} & 0 \\ 0 & 0 & 1 \\ 1/\sqrt{2} & 1/\sqrt{2} & 0 \end{bmatrix} \qquad \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

  文字 a を読んだときは状態変わらない　　λ =0.5

  文字 b を読んだら↑こんな感じに変わる

文字列を受理　⇔　読んだ後、状態1にいる確率が0.5以上 !?

数学的に言うと

QFA が文字列 $c_1\ c_2\ c_3 \cdots c_n$ を受理する

if and only if

(案1) $\| s\ Xc_1\ Xc_2 \cdots Xc_n\ P \| \geqq \lambda$

(案2) $\| s\ Xc_1\ Xc_2 \cdots Xc_n\ P \| > \lambda$

※ $\|v\|$ = ベクトルの長さ

今日のお話

QFAの空判定問題

『入力: QFA

出力: そのQFAが受理する文字列は存在するか？』

は

(案1) $\| s\, Xc_1\, Xc_2 \cdots Xc_n\, P \| \geqq \lambda$ ならば、決定不能

(案2) $\| s\, Xc_1\, Xc_2 \cdots Xc_n\, P \| > \lambda$ ならば、決定可能

余談

量子オートマトン (QFA)

- 状態ベクトルは
  成分の二乗和が 1
- 遷移行列はユニタリ
  - 列ベクトルが直交基底
  - 必ず逆行列がある

$\geqq \lambda$, $\leqq \lambda$　決定不能

$> \lambda$, $< \lambda$　決定可能

確率オートマトン (PFA)

- 状態はベクトルは
  成分の和が 1
- 遷移行列
  - 列ベクトルの成分和が1
  - 逆行列が無いかも

$\geqq \lambda$, $\leqq \lambda$　決定不能

$> \lambda$, $< \lambda$　決定不能

≧，≦ の場合の決定不能性

方針

PCP (Post's Correspondence Problem) に帰着

- 第１回でお勉強した通り、PCP は決定不能
- 全てのPCPのインスタンスに対して、
  それと空判定の答えが一致する QFA が作れる

方針

- wlog. 文字が2種類 {a, b} のPCPだけ考えます

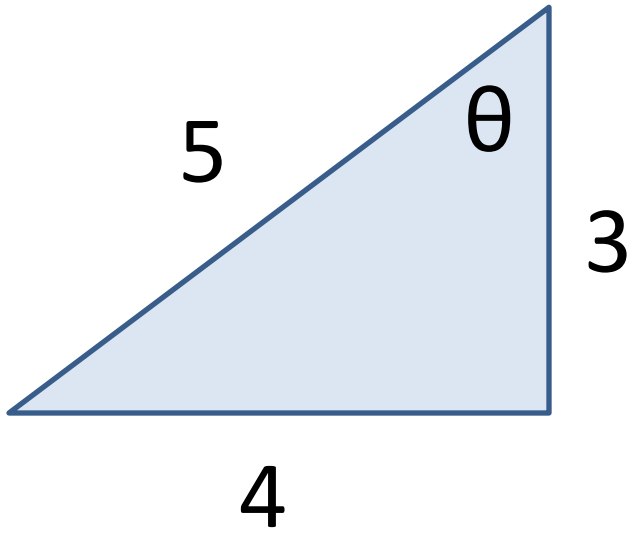
1. 「文字」をユニタリ行列にエンコード
2. 「文字列」をユニタリ行列にエンコード
3. PCPの「文字列ペア」をユニタリ行列にエンコード
   - これがQFAの「遷移行列」
   - k個ペアがあるPCP なら、文字がk種類のQFAになる
4. うまい初期状態と観測行列をとると、
   「PCPに解がある　⇔　$\|sX\cdots P\| \leqq 0$ に！」

「文字」のエンコード

- Xa =

$$\begin{bmatrix} 3/5 & -4/5 & 0 \\ 4/5 & 3/5 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Z軸周りに θ 回転



- Xb =

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 3/5 & -4/5 \\ 0 & 4/5 & 3/5 \end{bmatrix}$$

X軸周りに θ 回転

[Swierczkowski 1958]

証明スキップ
マーク

- 定理：3次元軸回りの arccos(有理数) 回転は自由群を生成する（0, ±1/2, ±1は除く）

- 系：Xa, Xb は自由群を生成する
  - 要は
  - Xa と Xb を違う順で掛け算すると必ず違う結果になる
    - 例:　Xa Xb ≠ Xa Xb,　Xa Xa Xb ≠ Xb Xa Xa,　…
  - （直感的な理由：arccos(3/5) は”切りが悪い”角度）

「文字列」のエンコード

- $w = c_1\ c_2\ c_3 \cdots c_n$

  を

- $Xw = Xc_1\ Xc_2\ Xc_3 \cdots Xc_n$

  にエンコード

- さっきの定理より、$Xw = Xu$ iff $w = u$

「文字列ペア」のエンコード

- 文字列 u と文字列 v のペア (u, v)
  を
- $Y_{u,v} = \frac{1}{2}\begin{bmatrix} X_u + X_v & X_u - X_v \\ X_u - X_v & X_u + X_v \end{bmatrix}$

- これが QFA の「文字」

[EXERCISE]

エンコードしたペアの重要な性質

- $Y_{u,v} =$

$$\frac{1}{2}\begin{bmatrix} X_u + X_v & X_u - X_v \\ X_u - X_v & X_u + X_v \end{bmatrix}$$

と定義したとき

- $Y_{uv,wx} = Y_{u,w} \; Y_{v,x}$

「PCPに解がある」と同値な条件は？

- PCP　{ (u1,v1), (u2,v2), …, (uk,vk) } に解がある
- $\exists\ i_1 \cdots i_n :\quad ui_1 ui_2 ui_3 \cdots ui_n = vi_1 vi_2 vi_3 \cdots vi_n$
- $\exists\ i_1 \cdots i_n :\quad X ui_1 ui_2 ui_3 \cdots ui_n = X vi_1 vi_2 vi_3 \cdots vi_n$
- $\exists\ i_1 \cdots i_n :\quad X ui_1 ui_2 ui_3 \cdots ui_n - X vi_1 vi_2 vi_3 \cdots vi_n = 0$
- $\exists\ i_1 \cdots i_n :\quad Y ui_1 ui_2 ui_3 \cdots ui_n, vi_1 vi_2 vi_3 \cdots vi_n$ の右上=0
- $\exists\ i_1 \cdots i_n :\quad Y ui_1, vi_1\ \ Y ui_2, vi_2 \cdots Y ui_n, vi_n$ の右上=0

「PCPに解がある」と同値な条件は？

- $\exists\ i_1 \cdots i_n :\quad Yui_1,vi_1\ \ Yui_2,vi_2 \cdots Yui_n,vi_n$ の右上=0
- と同値な条件を
- $\exists\ i_1 \cdots i_n : \| s\ Yui_1,vi_1\ \ Yui_2,vi_2 \cdots Yui_n,vi_n\ P \|=0$
- の形で書ければ勝利！

初期状態 s の選び方

- s Yui_1,vi_1 Yui_2,vi_2 … Yui_n,vi_n =

$$\frac{1}{2}\begin{bmatrix} Xu + Xv & Xu - Xv \\ Xu - Xv & Xu + Xv \end{bmatrix}$$

$(s_1\ s_2\ s_3\ 0\ 0\ 0)$ (… $(s_1\ s_2\ s_3)(Xu-Xv)$)

(s1 s2 s3) (Xu -Xv) = (0 0 0)

iff (Xu-Xv) = 0 になるように選びたい

[EXERCISE]
素晴らしい初期状態

- 定理: (3 0 4) Xw = (3 0 4) Xu　iff　Xw = Xu

- 証明は k に関する帰納法
  - {Xa, Xb, Xa^{-1}, Xb^{-1}} を、キャンセルしないように
    k 個掛け算した行列 M は
    　∃x1,x2,x3∈Z : (3 0 4) M = (x1, x2, x3) / 5^k
    かつ
    　このとき x2 は(k=0の場合を除き)5で割れない
- Then, (3 0 4) Xw Xu^{-1} = (3 0 4)　iff Xw Xu^{-1} = I

「PCPに解がある」と同値な条件は？

- PCP　{ (u1,v1), (u2,v2), …, (uk,vk) } に解がある
- 中略
- ∃ $i_1 \cdots i_n$:　Yui_1,vi_1　Yui_2,vi_2 … Yui_n,vi_n の右上=0
- ∃ $i_1 \cdots i_n$: ‖ s Yui_1,vi_1　Yui_2,vi_2 … Yui_n,vi_n　P ‖=0
  - where　s = (3/5　0　4/5　0　0　0)
    P = (0 0 0 1 1 1) が対角線に並んだ対角行列
- ∃ $i_1 \cdots i_n$: ‖ s Yui_1,vi_1　Yui_2,vi_2 … Yui_n,vi_n　P ‖=1
  - where　s = (3/5　0　4/5　0　0　0)
    P = (1 1 1 0 0 0) が対角線に並んだ対角行列

ここまでに示されたこと

- QFA に対して、
  - $\{w \mid \|s\, X_w\, P\| \leqq 0\}$ の空判定は決定不能
  - $\{w \mid \|s\, X_w\, P\| \geqq 1\}$ の空判定は決定不能

- ここまでの構成から、s, X, P の成分を全て有理数に限っても決定不能

[EXERCISE]
0, 1 以外の受理境界

- 系：任意の有理数 λ に対し、
  - {w | ‖s Xw P‖ ≦ λ} の空判定は決定不能
  - {w | ‖s Xw P‖ ≧ λ} の空判定は決定不能

- 証明：任意のQFA（受理条件:≧1）A に対し、
  ∀w（ wをAが受理する　iff　wをBが受理する）
  となるような QFA（受理条件: ≧ λ）B が作れる
- ≦0 からの帰着も同様

こうやる

$$X_i^B = \begin{pmatrix} X_i^A & 0 \\ 0 & 1 \end{pmatrix},$$

and define $s^B = \begin{pmatrix} \sqrt{\lambda}\, s^A & \sqrt{1-\lambda} \end{pmatrix}$. If we choose

$$P^B = \begin{pmatrix} P^A & 0 \\ 0 & 0 \end{pmatrix},$$

新しいQFAが
無理数成分を持つのが気持ち悪い

- 補題：任意のQFA（受理条件:≧1）A に対し、
  ∀ｗ（ ｗをAが受理する　iff　 ｗをBが受理する ）
  となるような有理数成分 QFA（受理条件: ≧ λ）
  B が作れる

証明

- ラグランジュの四平方定理 [Lagrange 1770]
  - 任意の自然数は4つ以下の平方数の和で書ける
  - 系：任意の有理数は4つ以下の有理数平方の和

nbers, say $\lambda = a_1^2 + a_2^2 + a_3^2 + a_4^2$ and $1 - \lambda = b_1^2 + b_2^2 + b_3^2 + b_4^2$.
Now, if we define

$$s^B = \begin{pmatrix} a_1 s^A & a_2 \cdots a_4 & b_1 \cdots b_4 \end{pmatrix} \; X_i^B = \begin{pmatrix} X_i^A & 0 \\ 0 & I_7 \end{pmatrix} \; P^B = \begin{pmatrix} P^A & 0 & 0 \\ 0 & I_3 & 0 \\ 0 & 0 & 0_4 \end{pmatrix}$$

まとめ:決定不能性

- QFA に対して、
  - $\{w \mid \|s\ Xw\ P\| \leqq \lambda\}$ の空判定は決定不能
  - $\{w \mid \|s\ Xw\ P\| \geqq \lambda\}$ の空判定は決定不能
  - arccos(3/5) 回転のなす自由群を、PCPのための文字列のエンコードに使う

$>, <$ の場合の決定可能性

方針 （＜λの場合も全く同じ）
{w | ‖s Xw P‖ ＞ λ} の空判定Algorithm

- ‖s Xw P‖ ＞ λ な w が存在すれば
  有限時間で“No”を返し、しないなら止まらない
  セミアルゴリズムを与える
- すべての w で ‖s Xw P‖ ≦ λ ならば
  有限時間で“Yes”を返し、しないなら止まらない
  セミアルゴリズムを与える
- 定理 [Who:19??] A と Aの補集合 が recursively enumerable なら A は recursive

簡単な方

- $\|s\ Xw\ P\| > \lambda$ な w が存在すれば
  有限時間で“No”を返し、しないなら止まらない
  セミアルゴリズムを与える

- アルゴリズム
  – 文字列 w を短い順に全て試してみるだけ

難しい方

- すべての w で ‖s Xw P‖ ≦ λ ならば
  有限時間で“Yes”を返し、しないなら止まらない
  セミアルゴリズムを与える

- 方針:
  - 「‖s Xw P‖ ≦ λ な w が存在」と同値な一階述語論理の論理式(が有限回で現れる無限列)を作る
  - 定理 [Tarski1951]: 実数体上の一階述語論理は決定可能 (via quantifier elimination)

同値な条件

- すべての w で $\|s\ Xw\ P\| \leqq \lambda$
- $\forall X \in \xi$: $\|s\ X\ P\| \leqq \lambda$
  - where ξ = {Xa と Xb の生成するモノイド}
- $\forall X \in clo(\xi)$: $\|s\ X\ P\| \leqq \lambda$
  - where $clo(\xi)$ = ξ の閉包 = $\{x \mid \forall\ \varepsilon\ \exists y \in \xi : \|y-x\| < \varepsilon\}$

why? ←は明らか。

→は、$\|s \cdot P\|$ が連続より $\|s\ clo(\xi)\ P\| \subseteq clo(\|s\ \xi\ P\|)$

∴ $\|s\ \xi\ P\| \leqq \lambda$ ➔ $clo(\|s\ \xi\ P\|) \leqq \lambda$

➔ $\|s\ clo(\xi)\ P\| \leqq \lambda$

※ 注意

- $\|s\,\xi\,P\| \leqq \lambda$ ➔ $clo(\|s\,\xi\,P\|) \leqq \lambda$

  ➔ $\|s\ clo(\xi)\ P\| \leqq \lambda$

- ここが、前半の決定不能な場合との唯一の違い

  $\|s\,\xi\,P\| < \lambda$ ➔ $clo(\|s\,\xi\,P\|) < \lambda$

  は成り立たない！

閉包をとると何が嬉しいか:モノイドが群に

- 定理: clo(ξ) はコンパクト群
- 証明:
  - Fact: コンパクト ＝ 点列コンパクト ＝ 有界閉集合
  - clo(ξ)は明らかに有界で閉なので、コンパクト。
  - 点列コンパクト = 任意の点列が収束部分列を持つ
  - $X \in \mathrm{clo}(\xi)$ に対し $X^0, X^1, X^2, \cdots$ は収束部分列を持つ
  - つまり $\forall\ \varepsilon > 0,\ \exists i < k,\ \| X^i - X^k \| < \varepsilon$
  - このとき両辺に X^{-i-1}を掛けて、$\| X^{-1} - X^{k-i-1} \| < \varepsilon$
  - つまり X^{-1} に任意に近いclo(ξ)の元がとれる。
  - よって $X^{-1} \in \mathrm{clo}(\xi)$

コンパクト群になると何が嬉しいか

- 定理 [Who ????]
  行列のコンパクト群 G は多項式で特徴付けられる

  具体的には、(実数係数)多項式集合
  $R^G = \{f(X) \mid f(I) = 0 \ \& \ f(gX)=f(X) \text{ forall } g \text{ in } G\}$
  をとったとき、G の元はそのゼロ点
  $g \in G \quad \text{iff} \quad \forall f \in R^G.\ f(g)=0$

※実数係数： 実際は、有理数係数のものに限っても成り立つらしい→ R^G(の有理数係数のsubset)はrecusively enumerable

多項式で特徴付けられると何が…

- 仮に
  $R^G = \{f(X) \mid f(I) = 0 \ \& \ f(gX)=f(X) \ \text{forall } g \text{ in } G\}$
  これが有限基底を持つとする
  i.e, f1～fn があって、R^Gの元はその結合で書ける
- $\forall X \in clo(\xi)$: $\|s\ X\ P\| \leqq \lambda$
  - where clo(ξ) = ξの閉包
- $\forall X$: ($f1(X)=0 \ \& \ \cdots \ \& \ fn(X)=0 \ \rightarrow \ \|s\ X\ P\| \leqq \lambda$)
  - where f1 .. fn は $R^{clo(\xi)}$の有限基底

一階述語論理の式！

ヒルベルトの基底定理(の系)

- 定理 [Hilbert 1888]
  実数係数多項式環はネーター環である

  ※ネーター環の定義:
  イデアルの上昇列 $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$
  が必ず有限長 $\cdots I_n = I_{n+1} = I_{n+2} = \cdots$
  ※イデアルの定義:
  $\forall a,b \in I,\ a+b \in I$ かつ $\forall x \forall a \in I,\ xa,ax \in I$

- R^G ={f1,f2,…} はイデアル。I_k を{f1, …, fk} の生成するイデアルとすると、↑より、以下のようなnが存在 ∴有限基底
  $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots I_n = I_{n+1} = I_{n+2} = R^G$

まとめ：決定可能性

文字列 w を順に試す。

$||s\ Xw\ P|| > \lambda$

で No 。それ以外では停止しない

ξ := {Xa, Xb} の生成する半群
clo(ξ) := コンパクト群になる
$\forall X \in clo(\xi) : ||s\ X\ P|| \leqq \lambda$

で Yes。それ以外では停止しない

行列コンパクト群の性質
$R^{clo(\xi)}$ = {f1, f2, …} が存在して、
$g \in clo(\xi)$ と $\forall i\ fi(g)=0$ が同値

ヒルベルトの基底定理
$R^{clo(\xi)}$ の有限基底 {f1,…,fn} が存在し
$g \in clo(\xi)$ と $\forall i \leqq n.\ fi(g)=0$ が同値

n=1,2,… に対しFO論理式
$\forall X: f1(X)=0\ \&\ldots\&\ fn(X)=0$
➔ $||s\ X\ P|| \leqq \lambda$

なら Yes。それ以外では停止しない

実閉体の決定可能性
個々の式の真偽は決定可能

nが幾つか不明なので順に試す

おまけ

- その他にこの論文にあった結果
  - 文字が 2 種類のQFAの空判定(≦)も決定不能
    - PCPへの帰着だと「ペア7個以上のPCPが決定不能」しかわかっていないので、文字7種以上のQFAの決定不能性しか証明できていない
    - 証明はペア7個のケースを無理矢理2つの行列に押込む
  - 境界値 λ が「きわどい」かどうかも 決定可能
    - フォーマルに書くと
      $\exists\ \varepsilon > 0.\ \forall w.\ |\|s\ Xw\ P\|- \lambda| > \varepsilon$　は決定可能