

「Postの対応問題」 の決定不能性の証明

k.inaba

<http://www.kmonos.net/>

2009/10/10 第1回決定不能の会

Postの対応問題

(PCP : Post's Correspondence Problem)

- 入力

- Σ : 文字集合 (有限)

- $\{(\alpha_1, \beta_1), \dots, (\alpha_n, \beta_n)\}$:

- Σ 上の有限文字列のペアの有限集合

- 出力

- 有限列 i_1, \dots, i_k で

- $\alpha_{i_1} \cdots \alpha_{i_k} = \beta_{i_1} \cdots \beta_{i_k}$

- になるものは存在するか 否か?

例 1

- 入力

— $(\alpha_1, \beta_1) = (\text{“e”}, \text{“abcde”})$

— $(\alpha_2, \beta_2) = (\text{“ababc”}, \text{“ab”})$

— $(\alpha_3, \beta_3) = (\text{“d”}, \text{“cab”})$

- 出力

— Yes! $\alpha_2 \alpha_2 \alpha_3 \alpha_1 = \beta_2 \beta_2 \beta_3 \beta_1$

— ababcababcde

— ababcababcde

例2

- 入力

$$-(\alpha_1, \beta_1) = (\text{"ab"}, \text{"ca"})$$

$$-(\alpha_2, \beta_2) = (\text{"acb"}, \text{"a"})$$

$$-(\alpha_3, \beta_3) = (\text{"b"}, \text{"caab"})$$

- 出力

—No!

- 一つ目のペアとしては α_2, β_2 をとるしかないが、
“cb” が β 側にないので作れない

一般にはYesかNoか決定不可能

- 参考にした資料

- An Introduction to the Theory of Computation

- Eitan Gurari, Ohio State University

- Computer Science Press, 1989,
ISBN 0-7167-8182-4

- <http://www.cse.ohio-state.edu/~gurari/theory-bk/theory-bk.html>

- 4.7 節

証明

方針

- 主参考文献では 0型文法でやっていたけど面倒なのでこれで。実質ほぼ同じ
 - 「チューリングマシンの停止問題」から…
 - TMの停止問題は決定不能
 - 「Semi-Thue System のワード問題」経由で…
 - どんなTM停止問題も、答えがそれと一致するSTSワード問題に変換できる ∴ STSワード問題は決定不能
 - PCP に帰着
 - どんなSTSワード問題も、答えがそれと一致するPCPに変換できる ∴ PCPは決定不能

Semi-Thue System (STS) とは

- $G = (\Delta, P)$
 - Δ : 文字集合 (有限)
 - P : 以下の形の文法規則の有限集合
 - $\alpha \rightarrow \beta \quad (\alpha, \beta \in \Delta^+)$
- Δ^+ 上の二項関係 $w \Rightarrow v$ を以下で定義
 - $w = x_0 y_1 x_1 \cdots y_n x_n, \quad v = x_0 z_1 x_1 \cdots z_n x_n$
 - $\forall i. y_i \rightarrow z_i \in P$

STSのワード問題とは？

- 入力

- $G = (\Delta, P)$: Semi-Thue System

- w_s : Δ 上の(有限長の)文字列

- w_f : Δ 上の(有限長の)文字列

- 出力

- w_s から \Rightarrow を有限回繰り返して w_f に書き換えられるなら “Yes”、できないなら “No”

STSのワード問題：例

- G
 - $\Delta = \{a, b\}$
 - $P = \{aa \rightarrow ab, bb \rightarrow bbb\}$
- $w_s = \text{“aab”}$, $w_f = \text{“abbbbbbb”}$
 - Yes! ($\text{“aab”} \Rightarrow \text{“abb”} \Rightarrow \dots \text{中略} \dots \Rightarrow \text{“abbbbbbb”}$)
- $w_s = \text{“bab”}$, $w_f = \text{“aabaa”}$
 - No! (Pにbの数が増える規則しかないので絶対無理)

STSのワード問題は決定不能 (1/2)

- 「チューリングマシンの停止問題」からの帰着

–チューリングマシンの「状態 q でテープの文字が 0 だったらテープに 1 を書いて左に動き状態 p になる」といった規則を

- $0q0 \rightarrow p01$ と $1q0 \rightarrow p11$

のようにSemi-Thue Systemの規則にエンコードできる

STSのワード問題は決定不能 (2/2)

- 「チューリングマシンの停止問題」からの帰着

–チューリングマシンの受理状態を f とし、

- $0f \rightarrow f$ と $1f \rightarrow f$ と $f0 \rightarrow 0$ と $f1 \rightarrow 1$

という規則をさらに付け加えて、テープ端に関する規則を幾つか追加すると、「TMが停止する iff “初期状態” \Rightarrow^* “ f ”」となる

QED

話を戻してPCPの決定不能性

- 与えられたSTSワード問題 (G, w_s, w_f) から

STSワード問題の解が”Yes”

if and only if

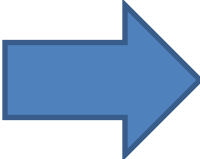
PCPの解が”Yes”

になるようなPCPを作れる

具体的な作り方 (ちょっと間違ってる)

- STSメンバシップ問題のインスタンス
 - $G = (\Delta, P) \quad w_s, w_f \in \Delta^+$
- 対応する PCP のインスタンス
 - $\Sigma = \{\text{始}, \text{終}, \text{次}\} \cup \Delta$
 - (始, 始次 w_s)
 - (次 w_f 終, 終)
 - (x , x) for all $x \in \{\text{次}\} \cup \Delta$
 - (α , β) for all $\alpha \rightarrow \beta \in P$

作り方の例 (左: STS、右: PCP)

- $\Delta = \{a, b\}$
 -
 - $P = \{aa \rightarrow ab, bb \rightarrow bbb\}$
 - $w_s = \text{“aab”}$
 - $w_f = \text{“abb”}$
- 
- $\Sigma = \{\text{始, 次, 終, a, b}\}$
 - (**始**, **始次** aab)
 - (**次** abbb **終**, **終**)
 - (a, a)
 - (b, b)
 - (**次**, **次**)
 - (aa, ab)
 - (bb, bbb)

作り方の例:

PCPの方を解いてみる

- (始, 始次aab) でスタート

始

始次aab

- つぎは、上側に次が来ないといけない

始次

始次aab次

(始, 始次aab)

(次abbb終, 終)

(a, a)

(b, b)

(次, 次)

(aa, ab)

(bb, bbb)

作り方の例： PCPの方を解いてみる

- (aa, ab) を使ってみる

始 **次** aa

始 **次** aab **次** ab

- つぎは、(b, b) しかない

始 **次** aab

始 **次** aab **次** abb

(始, 始 **次** aab)

(**次** abbb 終, 終)

(a, a)

(b, b)

(**次**, **次**)

(aa, ab)

(bb, bbb)

作り方の例： PCPの方を解いてみる

- (中略)

始 次 aab 次 abb

始 次 aab 次 abb 次 abbb

- 最後は 終 ペア

始 次 aab 次 abb 次 abbb 終

始 次 aab 次 abb 次 abbb 終

(始, 始次 aab)

(次 abbb 終, 終)

(a, a)

(b, b)

(次, 次)

(aa, ab)

(bb, bbb)

作り方の例： PCPの方を解いてみる

- PCPの解は”Yes”

始 **次** aab **次** abb **次** abbb 終
始 **次** aab **次** abb **次** abbb 終

(始, 始次aab)
(次abbb終, 終)
(a, a)
(b, b)
(次, 次)
(aa, ab)
(bb, bbb)

- STSの解は？ “Yes”

“次” で区切られた部分に着目すると…

$$- w_s = aab \Rightarrow abb \Rightarrow abbb = w_f$$

- フォーマルに言うと、次ページの補題が成り立つ

補題

- $w_s = \gamma_0 \Rightarrow \gamma_1 \Rightarrow \dots \Rightarrow \gamma_m = w_f$
という書き換え列がSTSにある

if and only if

- **始**次 γ_0 **次** γ_1 **次** γ_2 **次** \dots **次** γ_m **終**
で一致するようなマッチングがPCPにある

補題の証明

帰納法で $m \geq 0$ に関して以下を示す

- $\gamma_0 \Rightarrow \gamma_1 \Rightarrow \dots \Rightarrow \gamma_m = W_f$

if and only if

- $\exists i_1 \dots i_n$

$$x_{i_1} \dots x_{i_n} = \text{決} \gamma_0 \text{ 決} \gamma_1 \text{ 決} \dots \text{決} \gamma_m \text{ 終}$$

$$y_{i_1} \dots y_{i_n} = \text{決} \gamma_1 \text{ 決} \dots \text{決} \gamma_m \text{ 終}$$

($\gamma_0 = W_s$ の場合を考えれば補題がすぐ従う)

補題の証明

- $\gamma_0 \Rightarrow \gamma_1 \Rightarrow \dots \Rightarrow \gamma_m = w_f$
if and only if

- $\exists i_1 \dots i_n$

$$x_{i_1} \dots x_{i_n} = \text{始 } \gamma_0 \text{ 次 } \gamma_1 \text{ 次 } \dots \text{ 次 } \gamma_m \text{ 終}$$

$$y_{i_1} \dots y_{i_n} = \text{次 } \gamma_1 \text{ 次 } \dots \text{ 次 } \gamma_m \text{ 終}$$

(始,	始次 w_s)
(次 w_f 終,	終)
(x, x)	for all $x \in \{\text{次}\} \cup \Delta$
(α, β)	for all $\alpha \rightarrow \beta \in P$

- $m = 0$ の場合

– (次 w_f 終, 終) がPCPのペアにあるので成立

補題の証明

(**決**w**終**, **終**)

(**x**, **x**)

for all $x \in \{\text{決}\} \cup \Delta$

(α , β)

for all $\alpha \rightarrow \beta \in P$

- $\gamma_0 \Rightarrow \gamma_1 \Rightarrow \dots \Rightarrow \gamma_m = w$

- $\exists i_1 \dots i_n$

$$x_{i_1} \dots x_{i_n} = \text{決 } \gamma_0 \text{ 決 } \gamma_1 \text{ 決 } \dots \text{ 決 } \gamma_m \text{ 終}$$

$$y_{i_1} \dots y_{i_n} = \text{決 } \gamma_1 \text{ 決 } \dots \text{ 決 } \gamma_m \text{ 終}$$

- $m > 0$ の場合 (“only if” part)

- $\gamma_0 \Rightarrow \gamma_1 \Rightarrow \dots \Rightarrow \gamma_m = w$

- implies $\gamma_0 \Rightarrow \gamma_1$ かつ $\gamma_1 \Rightarrow \dots \Rightarrow \gamma_m = w$

- by IH **決** γ_1 **決** γ_2 **決** \dots **決** γ_m **終**

と **決** γ_2 **決** \dots **決** γ_m **終** がマッチ

- $\gamma_0 \Rightarrow \gamma_1$ なので **決** γ_0 と **決** γ_1 もマッチ [要証明]

- よって、合わせると全体もマッチ

補題の証明

(**決**w**終**, **終**)

(x, x)

for all $x \in \{\text{決}\} \cup \Delta$

(α , β)

for all $\alpha \rightarrow \beta \in P$

• $\gamma_0 \Rightarrow \gamma_1 \Rightarrow \dots \Rightarrow \gamma_m = w$

• $\exists i_1 \dots i_n$

$x_{i_1} \dots x_{i_n} = \text{決 } \gamma_0 \text{ 決 } \gamma_1 \text{ 決 } \dots \text{ 決 } \gamma_m \text{ 終}$

$y_{i_1} \dots y_{i_n} = \text{決 } \gamma_1 \text{ 決 } \dots \text{ 決 } \gamma_m \text{ 終}$

• $m > 0$ の場合 (“if” part)

– $\text{決 } \gamma_0 \text{ 決 } \gamma_1 \text{ 決 } \gamma_2 \text{ 決 } \dots \text{ 決 } \gamma_m \text{ 終}$

と $\text{決 } \gamma_1 \text{ 決 } \gamma_2 \text{ 決 } \dots \text{ 決 } \gamma_m \text{ 終}$ がマッチ

– Implies $\text{決 } \gamma_0$ と $\text{決 } \gamma_1$ がマッチ、かつ

$\text{決 } \gamma_1 \text{ 決 } \gamma_2 \text{ 決 } \dots \text{ 決 } \gamma_m \text{ 終}$

と $\text{決 } \gamma_2 \text{ 決 } \dots \text{ 決 } \gamma_m \text{ 終}$ がマッチ

∴ (**決**, **決**) のペアを使うしかないので

– 以下 straightforward

QED

補題の系

- If STSが”Yes” then PCPが”Yes”
- 問題点
 - If PCPが”Yes” then STSが”Yes”
 - ではない
 - そもそもこんなペアが…
(x, x) for all $x \in \{\text{決}\} \cup \Delta$

正しい作り方

$G = (\Delta, P), w_s, w_f$ に対して...

• $\Sigma = \{\text{始}, \text{終}, \text{次}, \underline{\text{次}}\} \cup \Delta \cup \underline{\Delta}$

• $(\text{始}, \text{始次}_{w_s})$

• $(\text{始}, \underline{\text{始次}}_{w_s})$

• $(\text{次}_{w_f} \text{終}, \text{終})$

• (\underline{x}, x)

• (x, \underline{x})

• $(\alpha, \underline{\beta})$

• $(\underline{\alpha}, \beta)$

こうすると

「始」で始まり

「終」で終わらざるを得ない

for all $x \in \{\text{次}\} \cup \Delta$

for all $x \in \{\text{次}\} \cup \Delta$

for all $\alpha \rightarrow \beta \in P$

for all $\alpha \rightarrow \beta \in P$

補題二つ (証明はさっきとほぼ同じなので略)

- $W_s = \gamma_0 \Rightarrow \gamma_1 \Rightarrow \dots \Rightarrow \gamma_{2m} = W_f$
iff

- **始** 次 γ_0 次 γ_1 \dots 次 γ_{2m-1} 次 γ_{2m} **終**
で一致するようなマッチングがPCPにある

- $W_s = \gamma_0 \Rightarrow \gamma_1 \Rightarrow \dots \Rightarrow \gamma_{2m+1} = W_f$
iff

- **始** 次 γ_0 次 γ_1 \dots 次 γ_{2m} 次 γ_{2m+1} **終**
で一致するようなマッチングがPCPにある

系

- If STSが”Yes” then PCPが”Yes”
- 追加の補題 (easy):
 - このPCPのマッチは、必ず 始(次 Δ^*)?(次 Δ^* 次 Δ^*)*終 の形
- 系: If PCPが”Yes” then STSが”Yes”
- 系: PCPは決定不能

QED

まとめ

- チューリングマシンの停止性
 - Semi-Thue System (or 0型文法)のワード問題
 - Postの対応問題
- 計算履歴 (文法の導出履歴)がPCPのマッチング結果になるようにエンコード
 - 導出規則をそのままPCPの文字列ペアに
 - 最初と最後を1つずらす

Thank you for listening!