P≠NPの世界

東北大学大学院理学研究科

樋口 幸治郎

言わずと知れたＰ対ＮＰ問題

Thm(S.A.Cook, 1971)

SATはNP完全問題.

Thm(R.E.Ladner, 1975)

P$\neq$NP$\Longrightarrow$NP$\setminus$P内にNP不完全問題が存在する.

計算機

次の3拍子揃いの理想化されたパソコンを考える.
・メモリーは無限!
・計算にミスはない!!
・無限のメモリを持つディスクのドライバが備え付けられている!!!

$2^{<\omega}$ は0,1有限列全体, $A \subset 2^{<\omega}$ とする.

Aのディスクとは,
各$n \in \omega$に対し, ディスクのn番目のメモリに値$A(x)$ (ただし, $\lceil x \rceil = n$) が書き込まれているディスクのこと.

計算機

次の3拍子揃いの理想化されたパソコンを考える.
・メモリーは無限!
・計算にミスはない!!
・無限のメモリを持つディスクのドライバが備え付けられている!!!

$2^{<\omega}$ は0,1有限列全体, $A \subset 2^{<\omega}$ とする.

Aのディスクとは,
各$n \in \omega$に対し, ディスクの**n番目のメモリに値**$A(x)$ (ただし, $\lceil x \rceil = n$) が書き込まれているディスクのこと.

計算機の計算

$A,B \subset 2^{<\omega}$ とする.

C言語＋“ディスク参照命令”で書かれたプログラムPを考える.

入力xに対し,
ディスクドライバが空なら出力を$P(x)$と書き,
Bのディスクが入っているとき出力を$P(B;x)$と書く.

以下では, $2^{<\omega}$ の部分集合をその特性関数と同一視する.
Aが計算可能 $\Longleftrightarrow$
$(\exists$プログラム$P)(\forall x \in 2^{<\omega})[A(x)=P(x)]$.

$A \leq_T B \Longleftrightarrow$
$(\exists$プログラム$P)(\forall x \in 2^{<\omega})[A(x)=P(B;x)]$.

計算機の計算

$A,B \subset 2^{<\omega}$ とする.

C言語＋“ディスク参照命令”で書かれたプログラムPを考える.

入力xに対し,
ディスクドライバが空なら出力を$P(x)$と書き,
Bのディスクが入っているとき出力を$P(B;x)$と書く.

以下では, $2^{<\omega}$ の部分集合をその特性関数と同一視する.

Aが計算可能 $\Longleftrightarrow$

$(\exists$プログラム$P)(\forall x \in 2^{<\omega})[A(x)=P(x)]$.

$A \leq_T B \Longleftrightarrow$

$(\exists$プログラム$P)(\forall x \in 2^{<\omega})[A(x)=P(B;x)]$.

計算機の計算

$A,B \subset 2^{<\omega}$ とする.

C言語＋“ディスク参照命令”で書かれたプログラムPを考える.

入力xに対し,
ディスクドライバが空なら出力を$P(x)$と書き,
Bのディスクが入っているとき出力を$P(B;x)$と書く.

以下では, $2^{<\omega}$ の部分集合をその特性関数と同一視する.
Aが計算可能 $\Longleftrightarrow$
$(\exists \text{プログラム} P)(\forall x \in 2^{<\omega})[A(x)=P(x)]$.

$A \leq_T B \Longleftrightarrow$
$(\exists \text{プログラム} P)(\forall x \in 2^{<\omega})[A(x)=P(B;x)]$.

計算機の計算

$A,B \subset 2^{<\omega}$ とする.

C言語＋“ディスク参照命令”で書かれたプログラムPを考える.

入力xに対し,
ディスクドライバが空なら出力を$P(x)$と書き,
Bのディスクが入っているとき出力を$P(B;x)$と書く.

以下では, $2^{<\omega}$ の部分集合をその特性関数と同一視する.
Aが計算可能 $\Longleftrightarrow$
$(\exists$プログラム$P)(\forall x \in 2^{<\omega})[A(x)=P(x)]$.

$A \leq_T B \Longleftrightarrow$
$(\exists$プログラム$P)(\forall x \in 2^{<\omega})[A(x)=P(B;x)]$.

多項式時間還元可能性

A が計算可能 $\Longleftrightarrow$

$(\exists$**プログラム** $P)(\forall x \in 2^{<\omega})[A(x)=P(x)]$.

このとき, $p(t) \in \mathbb{N}[t]$ **があって**, **各入力** x **に対し**, $P(x)$ **の計算が常に** $p(lh(x))$ **時間以内で終わるとき**, $A \in P$ **と書く**.

$A \leq_T B \Longleftrightarrow$

$(\exists$**プログラム** $P)(\forall x \in 2^{<\omega})[A(x)=P(B;x)]$.

このとき, **計算時間が多項式で抑えられるとき**, $A \leq_T^p B$ **と書く**.

Thm(S.A.Cook, 1971)

SAT **は** NP **完全問題**.

Thm(R.E.Ladner, 1975)

$P \neq NP \Longrightarrow NP \setminus P$ **内に** NP **不完全問題が存在する**.

多項式時間還元可能性

A**が計算可能** $\Longleftrightarrow$

$(\exists$**プログラム**$P)(\forall x\in 2^{<\omega})[A(x)=P(x)]$.

このとき, $p(t)\in\mathbb{N}[t]$**があって**, **各入力**x**に対し**, $P(x)$**の計算が常に** $p(lh(x))$**時間以内で終わるとき**, $A\in P$ **と書く**.

$A\leq_T B$ $\Longleftrightarrow$

$(\exists$**プログラム**$P)(\forall x\in 2^{<\omega})[A(x)=P(B;x)]$.

このとき, **計算時間が多項式で抑えられるとき**, $A\leq_T^p B$ **と書く**.

Thm(S.A.Cook, 1971)

SAT **は**NP **完全問題**.

Thm(R.E.Ladner, 1975)

$P\neq NP\Longrightarrow NP\setminus P$ **内に**NP **不完全問題が存在する**.

多項式時間還元可能性

A**が計算可能** $\Longleftrightarrow$

$(\exists$**プログラム**P$)(\forall x \in 2^{<\omega})[A(x)=P(x)]$.

このとき, $p(t) \in \mathbb{N}[t]$**があって**, **各入力**x**に対し**, P(x)**の計算が**常に**$p(lh(x))$**時間以内で終わる**と**き**, $A \in P$**と書く**.

$A \leq_T B \Longleftrightarrow$

$(\exists$**プログラム**P$)(\forall x \in 2^{<\omega})[A(x)=P(B;x)]$.

このとき, **計算時間が多項式で抑えられるとき**, $A \leq_T^p B$**と書く**.

Thm(S.A.Cook, 1971)

SAT**は**NP**完全問題**.

Thm(R.E.Ladner, 1975)

$P \neq NP \Longrightarrow NP \setminus P$**内に**NP**不完全問題が存在する**.

多項式時間還元可能性

A**が計算可能** $\Longleftrightarrow$

$(\exists$**プログラム**P$)(\forall x\in 2^{<\omega})[A(x)=P(x)]$.

このとき, $p(t)\in\mathbb{N}[t]$**があって**, **各入力**x**に対し**, P(x)**の計算が**常に**$p(lh(x))$**時間以内で終わる**と**き**, $A\in P$**と書く**.

$A\leq_T B \Longleftrightarrow$

$(\exists$**プログラム**P$)(\forall x\in 2^{<\omega})[A(x)=P(B;x)]$.

このとき, **計算時間が多項式で抑えられるとき**, $A\leq^p_T B$**と書く**.

Thm(S.A.Cook, 1971)

$SAT\in NP$**かつ**$(\forall A\in NP)[A\leq^p_T SAT]$.

Thm(R.E.Ladner, 1975)

$P\neq NP\Longrightarrow(\exists A\in NP)[\emptyset <^p_T A<^p_T SAT]$.

幾つかの基本性質

$A \leq_m^p B \iff$
多項式時間で計算できるプログラムPが存在して,
$(\forall x \in 2^{<\omega})[A(x)=B(P(x))]$.

Fact. $A \leq_m^p B \Longrightarrow A \leq_T^p B$.
Fact. $A \leq_m^p B \in NP \Longrightarrow A \in NP$.

以下の議論では, NPが何であるかは重要でなく, このFactが成り立つことが重要.

幾つかの基本性質

$A \leq_m^p B \iff$
多項式時間で計算できるプログラムPが存在して,
$(\forall x \in 2^{<\omega})[A(x)=B(P(x))]$.

Fact. $A \leq_m^p B \Longrightarrow A \leq_T^p B$.
Fact. $A \leq_m^p B \in NP \Longrightarrow A \in NP$.

以下の議論では, NPが何であるかは重要でなく, このFactが成り立つことが重要.

Ladnerらの結果

$A \oplus B = 0A \cup 1B$. **このオペレータはA,Bの上限(w.r.t.$\leq_m^p$)を与える.**

以下では, $2^{<\omega}$ の計算可能な部分集合のみを考える.

Thm(Ladner, 1975).
$(\forall B \notin P)(\exists A \notin P)[A \leq_m^p B$ **かつ** $A \not\geq_T^p B]$.

Thm(Ladner, 1975).
$(\forall B \notin P)(\exists A, A' \notin P)[A \oplus A' \equiv_m^p B$ **かつ** $A, A' \not\geq_T^p B]$.

Thm(Landweber et al., 1978).
$(\forall B \notin P)(\exists A, A' \notin P)[A, A' \leq_m^p B$ **かつ** $(\forall C \leq_T^p A, A')[C \in P]]$.

Cor. (P≠NP **のもとで**)
NP\P **の中にNP不完全問題がある.**
上限がNP完全問題となる $\leq_T^p$ **比較不可能な2つの問題がある.**
NP\P **内にNP不完全問題で下限がPになる2つの問題がある.**

Ladnerらの結果

$A \oplus B = 0A \cup 1B$. **このオペレータはA,Bの上限(w.r.t.$\leq_m^p$)を与える.**

以下では, $2^{<\omega}$ の計算可能な部分集合のみを考える.

Thm(Ladner, 1975).

$(\forall B \notin P)(\exists A \notin P)[A \leq_m^p B$ **かつ** $A \not\geq_T^p B]$.

Thm(Ladner, 1975).

$(\forall B \notin P)(\exists A, A' \notin P)[A \oplus A' \equiv_m^p B$ **かつ** $A, A' \not\geq_T^p B]$.

Thm(Landweber et al., 1978).

$(\forall B \notin P)(\exists A, A' \notin P)[A, A' \leq_m^p B$ **かつ** $(\forall C \leq_T^p A, A')[C \in P]]$.

Cor. (P≠NPのもとで)

NP\Pの中にNP不完全問題がある.

上限がNP完全問題となる$\leq_T^p$比較不可能な2つの問題がある.

NP\P内にNP不完全問題で下限がPになる2つの問題がある.

Ladnerらの結果

$A \oplus B = 0A \cup 1B$. **このオペレータはA,Bの上限(w.r.t.$\leq_m^p$)を与える.**

以下では, $2^{<\omega}$ の計算可能な部分集合のみを考える.

Thm(Ladner, 1975).

$(\forall B \notin P)(\exists A \notin P)[A \leq_m^p B$ **かつ** $A \not\geq_T^p B]$.

Thm(Ladner, 1975).

$(\forall B \notin P)(\exists A, A' \notin P)[A \oplus A' \equiv_m^p B$ **かつ** $A, A' \not\geq_T^p B]$.

Thm(Landweber et al., 1978).

$(\forall B \notin P)(\exists A, A' \notin P)[A, A' \leq_m^p B$ **かつ** $(\forall C \leq_T^p A, A')[C \in P]]$.

Cor. (P≠NPのもとで)

NP\Pの中にNP不完全問題がある.

上限がNP完全問題となる $\leq_T^p$ 比較不可能な2つの問題がある.

NP\P内にNP不完全問題で下限がPになる2つの問題がある.

Ladnerらの結果

$A \oplus B = 0A \cup 1B$. **このオペレータはA,Bの上限**(w.r.t.$\leq_m^p$)**を与える**.

以下では, $2^{<\omega}$ **の計算可能な部分集合のみを考える**.

Thm(Ladner, 1975).

$(\forall B \notin P)(\exists A \notin P)[A \leq_m^p B$ **かつ** $A \not\geq_T^p B]$.

Thm(Ladner, 1975).

$(\forall B \notin P)(\exists A, A' \notin P)[A \oplus A' \equiv_m^p B$ **かつ** $A, A' \not\geq_T^p B]$.

Thm(Landweber et al., 1978).

$(\forall B \notin P)(\exists A, A' \notin P)[A, A' \leq_m^p B$ **かつ** $(\forall C \leq_T^p A, A')[C \in P]]$.

Cor. (P$\neq$NP **のもとで**)

NP$\setminus$P **の中にNP不完全問題がある**.

上限がNP完全問題となる $\leq_T^p$ **比較不可能な2つの問題がある**.

NP$\setminus$P **内にNP不完全問題で下限がPになる2つの問題がある**.

証明のための準備

Fact. **次のような2つのプログラムが存在する**:

入力$e \in \omega$**に対し, 常に多項式時間で出力するプログラムのソース** Q_e(resp. R_e)**を出力**,
しかも, 任意の$A \in P$(resp. $A \leq_T^p B$)**に対し, ある**$e \in \omega$**があって, 各** $x \in 2^{<\omega}$ **について**, $A(x)=Q_e(x)$(resp. $A(x)=R_e(B;x)$).

Fact(**再帰定理**). **プログラム**P**を定義するときに**, $\ulcorner P \urcorner$ **を知っているものとしていてよい**.

証明のための準備

Fact. **次のような2つのプログラムが存在する**:

入力$e \in \omega$ **に対し, 常に多項式時間で出力するプログラムのソース** Q_e(resp. R_e) **を出力**,
しかも, 任意の$A \in P$(resp. $A \leq_T^p B$) **に対し, ある**$e \in \omega$ **があって, 各** $x \in 2^{<\omega}$ **について**, $A(x) = Q_e(x)$(resp. $A(x) = R_e(B;x)$).

Fact(**再帰定理**). **プログラム**P **を定義するときに**, $\ulcorner P \urcorner$ **を知っているものとしていてよい**.

$(\forall B \notin P)(\exists A \notin P)[A \leq_m^p B$ かつ $A \not\geq_T^p B]$

証明. 多項式時間で計算される関数 $F:2^{<\omega} \to 1^{<\omega}$ を構成した後, $A=\{x \in B \mid lh(F(x)) \text{ is even}\}$ と定める. このとき, $A \leq_m^p B$ は明らか.
よって, 次の2種の要件を全て満たすようにFを構成すれば十分.

P_e: $A \neq Q_e$.

N_e: $B \neq R_e(A)$.

構成: Stage λ: $F(\lambda)=\lambda$.

Stage $x \in 2^{<\omega} \setminus 1^{<\omega}$: $F(x)=F(0^{lh(x)})$.

Stage $0^n \in 1^{<\omega}$:

n時間使って今までの計算 $F(\lambda), F(0), F(00), \cdots$ を復元(再帰定理).

最後の値を 0^{2e+i} ($e \in \omega$, $i<2$) とする.

(甲) $i=0$ のとき. (P_e: $A \neq Q_e$ を満たす)

(乙) $i=1$ のとき. (N_e: $B \neq R_e(A)$ を満たす)

$(\forall B \notin P)(\exists A \notin P)[A \leq_m^p B$ かつ $A \not\geq_T^p B]$

証明. 多項式時間で計算される関数 $F:2^{<\omega} \to 1^{<\omega}$ を構成した後, $A=\{x \in B \mid lh(F(x)) \text{ is even}\}$ と定める. このとき, $A \leq_m^p B$ は明らか. よって, 次の2種の要件を全て満たすようにFを構成すれば十分.

P_e: $A \neq Q_e$.

N_e: $B \neq R_e(A)$.

構成: Stage λ: $F(\lambda)=\lambda$.

Stage $x \in 2^{<\omega} \setminus 1^{<\omega}$: $F(x)=F(0^{lh(x)})$.

Stage $0^n \in 1^{<\omega}$:

n時間使って今までの計算 $F(\lambda), F(0), F(00), \cdots$ を復元(再帰定理).

最後の値を 0^{2e+i} ($e \in \omega$, $i<2$) とする.

(甲) $i=0$ のとき. (P_e: $A \neq Q_e$ を満たす)

(乙) $i=1$ のとき. (N_e: $B \neq R_e(A)$ を満たす)

$(\forall B \notin P)(\exists A \notin P)[A \leq_m^p B$ かつ $A \not\geq_T^p B]$

証明. 多項式時間で計算される関数 $F:2^{<\omega} \to 1^{<\omega}$ を構成した後, $A=\{x \in B \mid lh(F(x)) \text{ is even}\}$ と定める. このとき, $A \leq_m^p B$ は明らか. よって, 次の2種の要件を全て満たすようにFを構成すれば十分.

P_e: $A \neq Q_e$.

N_e: $B \neq R_e(A)$.

構成: Stage λ: $F(\lambda)=\lambda$.

Stage $x \in 2^{<\omega} \setminus 1^{<\omega}$: $F(x)=F(0^{lh(x)})$.

Stage $0^n \in 1^{<\omega}$:

n時間使って今までの計算 $F(\lambda), F(0), F(00), \cdots$ を復元(再帰定理).

最後の値を 0^{2e+i} ($e \in \omega$, $i<2$) とする.

(甲) $i=0$ のとき. (P_e: $A \neq Q_e$ を満たす)

(乙) $i=1$ のとき. (N_e: $B \neq R_e(A)$ を満たす)

$(\forall B \notin P)(\exists A \notin P)[A \leq_m^p B$ かつ $A \not\geq_T^p B]$

証明. 多項式時間で計算される関数 $F:2^{<\omega} \to 1^{<\omega}$ を構成した後, $A=\{x \in B \mid lh(F(x)) \text{ is even}\}$ と定める. このとき, $A \leq_m^p B$ は明らか. よって, 次の2種の要件を全て満たすようにFを構成すれば十分.

P_e: $A \neq Q_e$.

N_e: $B \neq R_e(A)$.

構成: Stage λ: $F(\lambda)=\lambda$.

Stage $x \in 2^{<\omega} \setminus 1^{<\omega}$: $F(x)=F(0^{lh(x)})$.

Stage $0^n \in 1^{<\omega}$:

n時間使って今までの計算 $F(\lambda), F(0), F(00), \cdots$ を復元(再帰定理).

最後の値を 0^{2e+i} ($e \in \omega$, $i<2$) とする.

(甲) $i=0$ のとき. (P_e: $A \neq Q_e$ を満たす)

(乙) $i=1$ のとき. (N_e: $B \neq R_e(A)$ を満たす)

$(\forall B \notin P)(\exists A \notin P)[A \leq_m^p B$ かつ $A \not\geq_T^p B]$

証明. 多項式時間で計算される関数 $F:2^{<\omega} \to 1^{<\omega}$ を構成した後, $A=\{x \in B \mid lh(F(x)) \text{ is even}\}$ と定める. このとき, $A \leq_m^p B$ は明らか. よって, 次の2種の要件を全て満たすようにFを構成すれば十分.

P_e: $A \neq Q_e$.

N_e: $B \neq R_e(A)$.

構成: Stage λ: $F(\lambda)=\lambda$.

Stage $x \in 2^{<\omega} \setminus 1^{<\omega}$: $F(x)=F(0^{lh(x)})$.

Stage $0^n \in 1^{<\omega}$:

n時間使って今までの計算 $F(\lambda), F(0), F(00), \cdots$ を復元(再帰定理).

最後の値を 0^{2e+i} ($e \in \omega$, $i<2$) とする.

(甲) $i=0$ のとき. (P_e: $A \neq Q_e$ を満たす)

(乙) $i=1$ のとき. (N_e: $B \neq R_e(A)$ を満たす)

$(\forall B \notin P)(\exists A \notin P)[A \leq_m^p B$ かつ $A \not\geq_T^p B]$

証明. 多項式時間で計算される関数 $F:2^{<\omega} \to 1^{<\omega}$ を構成した後, $A=\{x \in B \mid lh(F(x)) \text{ is even}\}$ と定める. このとき, $A \leq_m^p B$ は明らか. よって, 次の2種の要件を全て満たすようにFを構成すれば十分.

P_e: $A \neq Q_e$.

N_e: $B \neq R_e(A)$.

構成: Stage λ: $F(\lambda)=\lambda$.

Stage $x \in 2^{<\omega} \setminus 1^{<\omega}$: $F(x)=F(0^{lh(x)})$.

Stage $0^n \in 1^{<\omega}$:

n時間使って今までの計算 $F(\lambda), F(0), F(00), \cdots$ を復元(再帰定理).

最後の値を 0^{2e+i} ($e \in \omega$, $i<2$) とする.

(甲) $i=0$ のとき. (P_e: $A \neq Q_e$ を満たす)

(乙) $i=1$ のとき. (N_e: $B \neq R_e(A)$ を満たす)

$(\forall B \notin P)(\exists A \notin P)[A \leq_m^p B$ かつ $A \not\geq_T^p B]$

証明. 多項式時間で計算される関数 $F:2^{<\omega} \to 1^{<\omega}$ を構成した後, $A=\{x \in B \mid lh(F(x)) \text{ is even}\}$ と定める. このとき, $A \leq_m^p B$ は明らか. よって, 次の2種の要件を全て満たすようにFを構成すれば十分.

P_e: $A \neq Q_e$.

N_e: $B \neq R_e(A)$.

構成: Stage λ: $F(\lambda)=\lambda$.

Stage $x \in 2^{<\omega} \setminus 1^{<\omega}$: $F(x)=F(0^{lh(x)})$.

Stage $0^n \in 1^{<\omega}$:

n時間使って今までの計算 $F(\lambda), F(0), F(00), \cdots$ を復元(再帰定理).

最後の値を 0^{2e+i} ($e \in \omega$, $i<2$) とする.

(甲) $i=0$ のとき. (P_e: $A \neq Q_e$ を満たす)

(乙) $i=1$ のとき. (N_e: $B \neq R_e(A)$ を満たす)

$(\forall B \notin P)(\exists A \notin P)[A \leq_m^p B$ かつ $A \not\geq_T^p B]$

証明. 多項式時間計算可能関数 $F:2^{<\omega} \longrightarrow 1^{<\omega}$ を構成した後,
$A=\{x \in B \mid lh(F(x)) \text{ is even}\}$ と定める.
Stage λ: $F(\lambda)=\lambda$.
Stage $0^n \in 1^{<\omega}$: n時間使ってF(λ),F(0),F(00),・・・を復元.
最後の値を 0^{2e+i} ($e \in \omega$, $i<2$) とする.
(甲) $i=0$ のとき. (P_e: $A \neq Q_e$ を満たす)
n時間使って $A(z) \neq Q_e(z)$ なるzを探す.
あれば, $F(0^n)=0^{2e+i+1}$. なければ, $F(0^n)=0^{2e+i}$.
(乙) $i=1$ のとき. (N_e: $B \neq R_e(A)$ を満たす)
n時間使って $B(z) \neq R_e(A)(z)$ なるzを探す.
あれば, $F(0^n)=0^{2e+i+1}$. なければ, $F(0^n)=0^{2e+i}$.
補題. $F(0^n) \subset F(0^{n+1}) \subset F(0^n)0$.

$(\forall B \notin P)(\exists A \notin P)[A \leq_m^p B$ かつ $A \not\geq_T^p B]$

証明. 多項式時間計算可能関数 $F:2^{<\omega} \longrightarrow 1^{<\omega}$ を構成した後,
$A=\{x \in B \mid lh(F(x)) \text{ is even}\}$ と定める.
Stage λ: $F(\lambda)=\lambda$.
Stage $0^n \in 1^{<\omega}$: n時間使ってF(λ),F(0),F(00),・・・を復元.
最後の値を 0^{2e+i} ($e \in \omega$, $i<2$) とする.
(甲) $i=0$ のとき. (P_e: $A \neq Q_e$ を満たす)
n時間使ってA(z)≠Q_e(z)なるzを探す.
あれば, $F(0^n)=0^{2e+i+1}$. なければ, $F(0^n)=0^{2e+i}$.
(乙) $i=1$ のとき. (N_e: $B \neq R_e(A)$ を満たす)
n時間使ってB(z)≠R_e(A)(z)なるzを探す.
あれば, $F(0^n)=0^{2e+i+1}$. なければ, $F(0^n)=0^{2e+i}$.
補題. $F(0^n) \subset F(0^{n+1}) \subset F(0^n)0$.

$(\forall B \notin P)(\exists A \notin P)[A \leq_m^p B$ かつ $A \not\geq_T^p B]$

証明. 多項式時間計算可能関数 $F:2^{<\omega} \longrightarrow 1^{<\omega}$ を構成した後,
$A=\{x \in B \mid lh(F(x)) \text{ is even}\}$ と定める.
Stage λ: $F(\lambda)=\lambda$.
Stage $0^n \in 1^{<\omega}$: n時間使ってF(λ),F(0),F(00),・・・を復元.
最後の値を 0^{2e+i} ($e \in \omega$, $i<2$) とする.
(甲) $i=0$ のとき. (P_e: $A \neq Q_e$ を満たす)
n時間使ってA(z)≠Q_e(z)なるzを探す.
あれば, $F(0^n)=0^{2e+i+1}$. なければ, $F(0^n)=0^{2e+i}$.
(乙) $i=1$ のとき. (N_e: $B \neq R_e(A)$ を満たす)
n時間使ってB(z)≠R_e(A)(z)なるzを探す.
あれば, $F(0^n)=0^{2e+i+1}$. なければ, $F(0^n)=0^{2e+i}$.
補題. $F(0^n) \subset F(0^{n+1}) \subset F(0^n)0$.

$(\forall B \notin P)(\exists A \notin P)[A \leq_m^p B$ かつ $A \not\geq_T^p B]$

証明. 多項式時間計算可能関数 $F:2^{<\omega} \longrightarrow 1^{<\omega}$ を構成した後,
$A=\{x \in B \mid lh(F(x)) \text{ is even}\}$ と定める.
Stage λ: $F(\lambda)=\lambda$.
Stage $0^n \in 1^{<\omega}$: n時間使ってF(λ),F(0),F(00),・・・を復元.
最後の値を 0^{2e+i} ($e \in \omega$, $i<2$) とする.
(甲) $i=0$ のとき. (P_e: $A \neq Q_e$ を満たす)
n時間使ってA(z)≠Q_e(z)なるzを探す.
あれば, $F(0^n)=0^{2e+i+1}$. なければ, $F(0^n)=0^{2e+i}$.
(乙) $i=1$ のとき. (N_e: $B \neq R_e(A)$ を満たす)
n時間使ってB(z)≠R_e(A)(z)なるzを探す.
あれば, $F(0^n)=0^{2e+i+1}$. なければ, $F(0^n)=0^{2e+i}$.
補題. $F(0^n) \subset F(0^{n+1}) \subset F(0^n)0$.

$(\forall B \notin P)(\exists A \notin P)[A \leq_m^p B$ かつ $A \not\geq_T^p B]$

証明. 多項式時間計算可能関数 $F:2^{<\omega} \longrightarrow 1^{<\omega}$ を構成した後,
$A=\{x \in B \mid lh(F(x)) \text{ is even}\}$ と定める.
Stage λ: $F(\lambda)=\lambda$.
Stage $0^n \in 1^{<\omega}$: n時間使って $F(\lambda), F(0), F(00), \cdots$ を復元.
最後の値を 0^{2e+i} ($e \in \omega$, $i<2$) とする.
(甲) $i=0$ のとき. (P_e: $A \neq Q_e$ を満たす)
n時間使って $A(z) \neq Q_e(z)$ なるzを探す.
あれば, $F(0^n)=0^{2e+i+1}$. なければ, $F(0^n)=0^{2e+i}$.
(乙) $i=1$ のとき. (N_e: $B \neq R_e(A)$ を満たす)
n時間使って $B(z) \neq R_e(A)(z)$ なるzを探す.
あれば, $F(0^n)=0^{2e+i+1}$. なければ, $F(0^n)=0^{2e+i}$.
補題. $F(0^n) \subset F(0^{n+1}) \subset F(0^n)0$.

稠密分割定理の証明

Thm. $(\forall B \not\in P)(\exists A, A' \not\in P)[A \oplus A' \equiv^p_m B$ **かつ** $A, A' \not\geq^p_T B]$.

Proof. **多項式時間計算可能関数** $F:2^{<\omega} \longrightarrow 1^{<\omega}$ **を構成した後**,

$A=\{x \in B \mid lh(F(x)) \text{ is even}\}$,

$A'=\{x \in B \mid lh(F(x)) \text{ is odd}\}$ **と定める**.

このとき, $A \oplus A' \equiv^p_m B$ **は明らか**.

よって, **次の** 4 **種の要件を全て満たすように** F **を構成すれば十分**.

I_e: $A \neq Q_e$,

II_e: $A' \neq Q_e$,

III_e: $B \neq R_e(A)$,

IV_e: $B \neq R_e(A')$,

構成は先の定理と同じ.

稠密分割定理の証明

Thm. $(\forall B \not\in P)(\exists A, A' \not\in P)[A \oplus A' \equiv^p_m B$ **かつ** $A, A' \not\geq^p_T B]$.

Proof. **多項式時間計算可能関数** $F:2^{<\omega} \longrightarrow 1^{<\omega}$ **を構成した後**,

$A=\{x \in B \mid lh(F(x)) \text{ is even}\}$,

$A'=\{x \in B \mid lh(F(x)) \text{ is odd}\}$ **と定める**.

このとき, $A \oplus A' \equiv^p_m B$ **は明らか**.

よって, **次の** 4 **種の要件を全て満たすように** F **を構成すれば十分**.

I_e: $A \neq Q_e$,

II_e: $A' \neq Q_e$,

III_e: $B \neq R_e(A)$,

IV_e: $B \neq R_e(A')$,

構成は先の定理と同じ.

稠密分割定理の証明

Thm. $(\forall B \not\in P)(\exists A, A' \not\in P)[A \oplus A' \equiv^p_m B$ **かつ** $A, A' \not\geq^p_T B]$.

Proof. **多項式時間計算可能関数** $F: 2^{<\omega} \longrightarrow 1^{<\omega}$ **を構成した後,**

$A = \{x \in B \mid lh(F(x)) \text{ is even}\}$,

$A' = \{x \in B \mid lh(F(x)) \text{ is odd}\}$ **と定める.**

このとき, $A \oplus A' \equiv^p_m B$ **は明らか.**

よって, 次の 4 **種の要件を全て満たすように** F **を構成すれば十分.**

I_e: $A \neq Q_e$,

II_e: $A' \neq Q_e$,

III_e: $B \neq R_e(A)$,

IV_e: $B \neq R_e(A')$,

構成は先の定理と同じ.

問題集

Question.
$(\forall B \not\in P)(\exists A, A' \leq_m^p B)$[A,A′は下限(w.r.t.$\leq_T^p$)を持たない].

Question.
$(\forall B \not\in P)(\exists A, A' \leq_m^p B)$[A,A′の下限がP, 上限がB].

参考文献

[1] R.E.Ladner, On the Structure of Polynomial Time Reducibility, JACM, 22(1975), 155-171.

[2] L.H.Landweber, R.J.Lipton and E.L.Robertson, On the structure of sets in NP and other complexity classes, Computer Sciences Technical Report 342(1978).