12.2.4 補足 1 ：カウント関数のクラスとしての #P

簡潔還元 (parsimonious reduction) はかなりきつい還元法なので，数え上げ問題の還元には以下に述べるチューリング還元の数え上げ版を普通用いる．チューリング還元は A.M. チューリングがオラクル TM (OTM) を定義する際に初めて用いたもので，2 つの問題（言語）A, B に対して，B をオラクルとして使う DTM M によって A が受理できる（すなわち，$A = L(M^B)$ である）とき A は B に**チューリング還元可能** (Turing reducible) であるといい，$A \leq_T B$ と書く．これの数え上げ版では（特に，#**P** の還元においては），M は $p(n)$ 時間限定（$p(n)$ は多項式）であるとし（オラクルへの 1 回の質問は M の 1 ステップにしかカウントされないことに注意），M が行なうオラクルへの質問回数も多項式限定（すなわち，M の入力が x のとき，たかだか $p(|x|)$ 回）であるとする．このような還元によって A を B に還元できるとき，A は B に**多項式時間チューリング還元可能** (polynomial-time Turing reducible) であるといい，

$$A \leq_T^{poly} B \quad \text{あるいは，単に} \quad A \leq_T^{p} B$$

と書く．

命題 12.1. $\leq_T^{poly}$ の性質：
(1) $\leq_T^{poly}$ は反射律 $A \leq_T^{poly} A$ および推移律 $A \leq_T^{poly} B \wedge B \leq_T^{poly} C \Longrightarrow A \leq_T^{poly}$ を満たす．
(2) $A \leq_m^{poly} B$（すなわち，$A \leq_{poly} B$）$\Longrightarrow A \leq_T^{poly} B$. □

数え上げ問題は Σ^*（Σ は有限アルファベット．$\{0,1\}$ に限定してもよい）から $\mathbb{N}$ への関数 f（**カウント関数** (counting function) という） を求めることにほかならない（12.1.1 項冒頭の関数 f_L 参照）．入力 x に対して $f(x)$ の 2 進数表現を出力する多項式 $p(n)$ 時間限定の変換機 (transducer) が存在するとき，f は**多項式時間で計算可能** (polynomial-time computable) であるという．したがって，$f \in \mathbf{FP}$ であり，$0 \leqq f(x) \leqq 2^{p(|x|)}$ である．そのため，#**P** はこれまでのように言語としてではなく，関数の集合

$$\#\mathbf{P} := \left\{ f : \Sigma^* \to \mathbb{N} \;\middle|\; \exists p \exists M \left[f(x) = \left| \{ y \in \{0,1\}^{p(|x|)} \mid M(\langle x, y \rangle) = 1 \} \right| \right] \right\}$$

（ただし，p は多項式 M は多項式時間限定の変換機）と定義することも多く，それに対応する決定問題が言語としての #**P** である．

一方，CTM によって定義される関数の集合も #**P** と定義する．すなわち，M を $p(n)$ 時間限定の NTM（$p(n)$ は多項式）とするとき，関数 $f_M : \Sigma^* \to \mathbb{N}$ を

$$f_M(x) := \text{“入力 } x \text{ に対する受理計算の個数 } \#accept(x)_M\text{”}$$

と定義し（したがって，$0 \leqq f_M(x) \leqq c^{p(n)}$ である．$c > 0$ は定数），#**P** を

$$\#\mathbf{P} := \{ f_M \mid M \text{ は多項式時間限定の NTM} \}$$

と定義する．これら 2 つの定義，および 12.2.1 項の冒頭で述べた #**P** の定義が一致することを証明しよう．

定理 12.6. f をカウント関数とする．次の (1)〜(3) は同値である．
(1) $f \in \#\mathbf{P}$.
(2) 次の条件を満たす NTM M と多項式 p が存在する：
  (i) M の各ステップでの遷移はたかだか 2 分岐である．
  (ii) 任意の入力 x に対する M の計算木におけるどの葉も深さが $p(|x|)$ である．
  (iii) $f = f_M$.

(3) 多項式時間で計算可能な述語 $R(x,y)$ と多項式 p が存在して，任意の文字列 x に対して，$f(x)$ は $R(x,y)$ が成り立つような長さが $p(|x|)$ の文字列 y の個数に等しい．

証明 (2) と (3) が同値であること（第 9 章の定理 9.1 の証明を参照せよ）と，(2)$\Longrightarrow$(1) は明らかである．(1)$\Longrightarrow$(2) を証明しよう．

M を $p(n)$ 時間限定 NTM とする（$p(n)$ は多項式）．M は各ステップでたかだか k 分岐するものとする．M を次のように修正した NTM を M' とする．

(i) M の各 1 ステップに対し M' は 2 分岐するステップを $\lceil \log_2 k \rceil$ 回実行する．したがって，M の非決定性の動作（計算が進行する道）1 つに対し M' では $2^{\lceil \log_2 n \rceil}$ 個の道が対応する．M' はその中の最初の k 個の道が M の最初の k 個の道と同じになるように M を模倣し，残りの道ではすべて入力を拒否する．

(ii) $p'(n)$ を $p'(n) \geqq \lceil \log_2 n \rceil \cdot p(n)$ を満たす時間構成可能関数とする．長さが n の任意の入力 x が与えられたとき，M' はちょうど $p'(n)$ ステップ動作してから停止する．もし，その途中で M の停止状態に入った場合には，M' は $p'(n)$ ステップに達するまで同じように動作し続ける．

明らかに，M' と M の受理に至る道の個数は等しい． □

次に，$\leq_{poly}^{\#}$ に対応する ‘数え上げ版の還元’ は次のように定義する．

まず，オラクル TM (OTM) M を次のように一般の関数 $f : \Sigma^* \to \{0,1\}^*$ をオラクルとする M^f に拡張する（Σ は任意の有限アルファベットであるが，$\{0,1\}$ に制限してもよい．また，$f(x) \in \{0,1\}^*$ を自然数の 2 進数展開だとみなして，f は Σ^* から $\mathbb{N}$ への（全域）関数であるともみなす）．すなわち，M は出力テープをもつ OTM（すなわち，オラクル付きの変換機）であるとし，M は質問状態に入ると，質問テープ上に書かれた語 y を $f(y)$ に書き換え[†6]，テープヘッドを $f(y)$ の左端に戻して回答状態に入る．これを 1 ステップで行なう．M が受理状態に入ったとき入力は受理される．M は受理された入力語の集合 $L(M^f)$ を定義すると同時に，$L(M^f)$ を定義域とする（部分）関数 $g : \Sigma^* \to \{0,1\}^*$ も定義する（M の出力 $g(y) \in \{0,1\}^*$ を 2 進数だとみなすことによって $g : \Sigma^* \to \mathbb{N}$ であるともみなす）．

これまでに登場したオラクル TM は文字列の集合（すなわち，言語 $A \subseteqq \Sigma^*$）をオラクルとするものであったが，言語 A はその特性関数

$$\chi_A(x) = \begin{cases} 1 & (x \in A \text{ のとき}) \\ 0 & (x \notin A \text{ のとき}) \end{cases}$$

と同一視できるから，M^{χ_A} は M^A と同一視でき，このような ‘関数をオラクルとする OTM’ はこれまでの ‘言語をオラクルとする OTM’ の自然な一般化である．

関数をオラクルとする多項式時間限定の DTM M^f によって定義される関数が g であるとき，$g \leq_T^{poly} f$ と書く．関数 $f : \Sigma^* \to \mathbb{N}$ が **#P 完全**であるとは，(i) $f \in \#\mathbf{P}$ かつ (ii) $g \leq_T^{poly} f$ が任意の $g \in \#\mathbf{P}$ に対して成り立つことである，と定義する．

最後に，関数の集合としての $\#\mathbf{P}$ の観点から数え上げ問題と確率性計算の関係を述べておこう．そのため，2.1 節では関数問題のクラス **FP** をカウント関数に限定しない関数のクラスとして定義したが，上記で $\#\mathbf{P}$ をカウント関数のクラスとして定義したのに倣って定義し直すことにしよう．

出力テープをもつ DTM M すなわち変換機は入力アルファベットが Σ^* で出力アルファベットが Δ^* のとき，関数 $M : \Sigma^* \to \Delta^*$ を定める：

[†6] $f(x)$ を表す言語 $A := \{\langle x, i\rangle \mid f(x)$ の i ビット目が 1$\}$ をオラクルとする OTM と考えてもよい．

$M(x)=y \overset{\text{def}}{\iff} M$ は入力 x を受理して停止したとき出力テープ上には y が書かれている．

アルファベット Σ や Δ は $\{0,1\}$ に制限しても一般性は失われない（符号化）．また，出力 y を整数の 2 進数表現だとみなすと，M はカウント関数を定義している．多項式時間限定のこのような M によって定義される関数（カウント関数と思ってよい）のクラスを **FP** で表す．(i) 12.1 節で定義した **FP** と (ii) この定義による **FP** は等しい．

問 12.11. (i) と (ii) の **FP** が等しいことを説明せよ．

定理 12.7. $\mathbf{PP}=\mathbf{P} \iff \#\mathbf{P}=\mathbf{FP}$.

証明 $L\in\mathbf{PP}$ であるとは，多項式時間で計算可能な述語 $M(x,y)$ と多項式 $p(n)$ が存在して（M は入力 x に対して y を出力する変換機と考えてよい），任意の $x\in\{0,1\}^*$ に対して

$$x\in L \iff \left|\{y\in\{0,1\}^{p(|x|)} \mid M(x,y)=\mathbf{true}\}\right| \geqq \tfrac{1}{2}\cdot 2^{p(|x|)}$$

が成り立つことである（定理 12.5 の直前の注を参照せよ）[†7]．y は $x\in L$ であることの証書である（定理 9.1 参照）．

($\Longleftarrow$) NTM M に対して，新しい初期状態 q_0' から 2 分岐し，一方の分岐ではそれ以降の計算においてすべてが入力を受理し，もう一方の分岐では M の動作の模倣をするような確率性 TM M' によって

$$x\in L(M) \Longleftrightarrow \#accept_{M'}(x)/\#total_{M'}(x)>\tfrac{1}{2} \overset{\text{def}}{\Longleftrightarrow} x\in L(M')$$

が成り立つから，$\mathbf{NP}\subseteqq\mathbf{PP}$ である．ゆえに，$\mathbf{P}\subseteqq\mathbf{PP}$.

もし $\#\mathbf{P}=\mathbf{FP}$ だとすると，$L\in\mathbf{PP}$ を受理する確率性 TM M に対し，入力 x に対する M の受理計算の個数 $\#accept_M(x)$ を計算する DTM が存在するので，$L\in\mathbf{P}$ である．ゆえに，$\mathbf{PP}\subseteqq\#\mathbf{P}$.

($\Longrightarrow$) $\mathbf{FP}\subseteqq\#\mathbf{P}$ が成り立つことは明らかであるから，$\#\mathbf{P}\subseteqq\mathbf{FP}$ であることを示そう．$f\in\#\mathbf{P}$ とすると，$f(x)=\left|\{y\in\{0,1\}^{p(|x|)} \mid M(\langle x,y\rangle)=1\}\right|$ を満たす多項式時間限定の変換機 M と多項式 p が存在する．ここで，$M(\langle x,y\rangle)=1$ のとき y は $x\in L(M)$ であることの証書である．このような y の個数 すなわち $f(x)$ を $\#_M(x)$ で表すことにする．

変換機 M_0 と M_1 では証書 y の長さが m であったとき，証書の長さが $m+1$ となる変換機 M' を $M'(\langle x,by\rangle)=M_b(\langle x,y\rangle)$ $(b\in\{0,1\})$ と定義すると $\#_{M'}(x)=\#_{M_0}(x)+\#_{M_1}(x)$ である．このような M' を M_0+M_1 と表すことにする．同様に，$n\in\{0,1,\ldots,2^m\}$ に対し，“$M_n(\langle x,y\rangle)=1 \iff y$ を 2 進数と見たとき $y<n$” を満たす変換機 M_n を考えると，明らかに $\#_{M_n}(x)=n$ である．

もし $\mathbf{PP}=\mathbf{P}$ だとすると，

$$\#_{M_n+M}(x)=n+\#_M(x)\geqq 2^m \tag{12.2.1}$$

か否かを多項式時間で判定することができる．よって，$\#_M(x)$ を計算するには，(12.2.1) を満たす最小の n を 2 分探索によって見つければよい．それにかかる時間は $O(\log_2 2^m)=O(m)$ すなわち多項式時間である．ゆえに，$f\in\mathbf{FP}$ であり，したがって $\#\mathbf{P}\subseteqq\mathbf{FP}$ である． □

直感的に言うと，**PP** は $\#\mathbf{P}$ に属す関数 f の 最大 有意ビット（下位のビットから数えて初めて 1 が現れる箇所：f の値域が $[0,N-1]$ のとき，$f(x)\geqq N/2$ となるところ）を計算することに相当する．これに対して，最小 の有意ビットを計算する確率性アルゴリズムによって定義されるクラスが $\oplus\mathbf{P}$ である．

[†7] L のアルファベットを $\{0,1\}$ に制限しているが，一般性を失わない．また，M は x と y のペアの符号化 $\langle x,y\rangle$ を入力とする変換機と考えてもよい．