

2.  $y = az$ ,  $|a| = 1$ ,  $|z| = p(n)$  とする.
3. 「 $a = 0$  であり, かつ  $z$  が長さが  $p(n)$  である  $2^{p(n)}$  個の文字列のうちの最初の  $2^{p(n)} - m$  個の中の 1 つである」か, または「 $a = 1$  かつ  $R(x, z) = \text{true}$  である」ならば  $M$  は入力を受理し, そうでなければ拒否する.

このとき,  $M$  が入力を受理するのは  $\#accept_M / \#total_M$  が  $(2^{p(n)} - m + f(x))2^{-(p(n)+1)}$  のときであり, この値は  $> \frac{1}{2}$  である. すなわち,  $\#P$  の一般的な問題 ' $R(x, y)$  が成り立つ  $y$  の個数を求めよ' を PTM  $M$  で模倣することができたので,  $P\#P \subseteq P^{PP}$  が示された.  $\square$

問 12.9. なぜ ' $R(x, y)$  が成り立つ  $y$  の個数を求めよ' が  $\#P$  の一般的な問題なのか?

この定理は, 多項式時間アルゴリズムにおいて実行の途中で補助計算を何度でも外部 (オラクル) に依頼することができるとしたとき, 補助計算として (i) ある数え上げ問題の答である個数を質問すること (オラクル  $\#P$  への質問) と (ii) 各ステップでランダムに遷移するような多項式時間アルゴリズムを使って計算してもらうこと ( $PP$  への質問. その計算が正しい確率は  $> \frac{1}{2}$ ) とが等価であると主張している. すなわち, これは場合の数と確率とのある種の関係である.

前述したように  $NP \subseteq \#P$  であるが,  $\#P$  に属すどんな数え上げ問題も多項式領域を使えば解くことができる. すなわち,  $\#P$  を言語のクラスと見た場合,  $\#P \subseteq PSPACE$  である. 上記の各クラス  $FewP$ ,  $PP$ ,  $\oplus P$  についても同様である. これらのクラスについては第 2 巻の確率性アルゴリズムの項で扱う.

問 12.10.  $NP \subseteq \#P \subseteq PSPACE$  であることを証明せよ.