数理解析研究所講究録
666巻 1988年 81-90

Some basic results about probabilistic pushdown automata

陳　致中（Zhi-Zhong Chen）
笠井琢美（Takumi Kasai）

Abstract: We introduce the concept "probability" into pushdown automata(PDA). By assigning a cut-point $0<\lambda<1$ to a probabilistic pushdown automaton (PPDA)M, the language L(M) accepted by M with cut-point λ is defined. Moreover, according to the properties of errors, PPDA's are classified into unrestricted PPDA's(2-sided error PPDA's), RPDA's(1-sided error PPDA's), and BPDA's(bounded error PPDA's). Some relations among the classsof languages accepted by PDA's, PPDA's, RPDA's, and BPDA's are obtained. It is shown thatthe class of languages accepted by PPDA's or BPDA's is independent of cut-points. It is also shown that there is an infinite hierarchy of the classes of languages accepted by RPDA's with different cut-points.

1．はじめに：

近年種種の効率よい確率アルゴリズムが開発され[1][6][11][12][14][16]，また確率アルゴリズムの理論研究も盛んである[2][13][15][18][19][20]。確率アルゴリズムを実行する媒体としての計算モデルには，確率チューリング機械(PTMと略す)[5]と確率有限オートマトン(PFAと略す)[10][17]がある。プッシュダウン・オートマトン（PDAと略す）[7]がチューリング機械(TMと略す)[7]，有限オートマトン(FAと略す)[7]と並び古くから研究されてきた。よって，PDAに確率を導入し，確率プッシュダウン・オートマトン(PPDAと略す)を考えるのは非常に自然である。

また，切断点(cutpoint,threshold)と言う概念を導入することにより，任意のλ，$0<\lambda<1$に対し，切断点λを持つPPDAによって受理される言語を定義する。

Gillは1977年に確率チューリング機械(PTMと略す)を定義し[5],受理するための条件である誤差の性質により,PTMを両側誤差(2-sided error)PTM, 片側誤差(1-sided error)PTM,有界誤差(bounded error)PTMなどに分類した（Gillの論文[5]の用語法と多少異なるが，本質的なものではない）。ここで誤差は,受理すべきものを受理しない誤差と,受理すべきでないものを受理してしまう誤差に分けられる。通常確率アルゴリズムと言った場合は,この2種類の誤差が起こりうる両側誤差アルゴリズムを指す。片側誤差アルゴリズムは,受理すべきでないものを受理する確率が0であるアルゴリズムで,最近ではよくランダム・アルゴリズムと呼ばれている。有界誤差とは2種類の誤差が共にある定数c,$0<c<1/2$でおさえられるものを言う。本稿では,これらの概念をPPDAに導入し,両側誤差PPDA(単にPPDAと略す),片側誤差PPDA(RPDAと略す),有界誤差 PPDA(BPDAと略す)について考察する。また,これらのPPDAによって受理される言語のクラス,決定性文脈自由言語[7]のクラス,文脈自由言語[7]のクラスの間の関係を考察する。

2. 定義と記法

[定義2.1] 確率プッシュダウン・オートマトン（PPDA)とは $M=(Q,\Sigma,\Gamma,P,q_0,F)$ のことを言う。ここで,(1) Qは状態の集合,(2)Σは入力アルファベット,(3) Γはスタック・アルファベットであり,Γは特別な文字Z_0を含む。Z_0は常にスタックの底にあり，ほかの所に現れない。(4) $q_0\in Q$，q_0は初期状態と呼ばれる。(5) $F\subset Q$,Fの元は受理状態と呼ばれる。(6) pは$X\times Y$から[0,1]への関数である。ただし，$X=Q\times(\Sigma\cup\{\varepsilon\})\times\Gamma$，$Y=Q\times\Gamma^*$，$\varepsilon$ は空語である。[0,1]は $0\leqq r\leqq 1$を満たすr全体からなる集合である。さらに,任意の,$q\in Q$,$a\in\Sigma$,$A\in\Gamma$に対して$\sum_{y\in Y}P(y\mid q,a,A)+\sum_{y\in Y}P(y\mid q,\varepsilon,A)\leqq 1$；かつ任意の，$q\in Q$，$a\in\Sigma\cup\{\varepsilon\}$，$A\in\Gamma$に対して$\{y\in Y:P(y\mid q,a,A)>0\}$が有限である。Pを遷移関数と言う。

[定義2.2] $M=(Q,\Sigma,\Gamma,P,q_0,F)$ を与えられたPPDAとする。$C=Q\times\Sigma^*\times\Gamma^*$とする。Cの元を様相と言う。様相$(q,x,\beta)$は,現在の状態がqで,まだ未処理の入力の部分が x で,スタックの内容がβであることを表す。入力ηが与えられたとする。様相(q_0,η,Z_0)を初期様相,様相(q_f,ε,Z_0)を受理様相と言う。ただし,$q_f\in F$。

[定義2.3] $M=(Q,\Sigma,\Gamma,P,q_0,F)$をPPDAとし，$\eta$をMへの入力とする。様相$C_1,C_2$に対して，$P^M(C_2 \mid C_1)$を次で定義する。 $C_1=(q,ax,A\beta)$かつ$C_2=(q',x,\alpha\beta)$かつ$a\neq\varepsilon$の時,$P^M(C_2 \mid C_1)=P(q',\alpha \mid q,a,A)$; $C_1=(q,x,A\beta)$かつ$C_2=(q',x,\alpha\beta)$の時,$P^M(C_2 \mid C_1)=P(q',\alpha \mid q,\varepsilon,A)$; その他の時,$P^M(C_2 \mid C_1)=0$。様相の列$\mathbb{C}:C_0,C_1,C_2,\cdots,C_m$は$C_0$が初期様相で,かつ$0\leqq i\leqq m-1$に対し,$P^M(C_{i+1} \mid C_i)>0$を満たすとき,入力$\eta$に対するMの計算と言い,mをこの計算の長さと言う。この計算の確率$P^M(\mathbb{C})$を $P^M(C_1 \mid C_0),P^M(C_2 \mid C_1),\cdots,P^M(C_m \mid C_{m-1})$の積と定義する。更に,$C_m$が受理様相であるとき,この計算を受理計算と呼ぶ。語ηがMに受理される確率$ACCEPT^M(\eta)$を入力ηに対するすべての受理計算の確率の和と定義する。

任意の$\eta\in\Sigma^*$に対して,$0\leqq ACCEPT^M(\eta)\leqq 1$となることに注意する。

[定義2.4] $0<\lambda<1$とする。次の二条件が満たされるなら，Mは言語Lを受理する両側誤差PPDAであると言う。(1)$\eta\in L$ならば,$ACCEPT^M(\eta)>\lambda$;(2) $\eta\notin L$ならば，$ACCEPT^M(\eta)\leqq\lambda$。

[定義2.5] $0<\lambda<1$とする。もし,Σ^*の任意の元ηに対し,次の二つの条件が満たされるならば,M は言語Lを受理する切断点λを持つ片側誤差PPDA,即ちRPDAであると言う。(1) ηが L に属するなら，$ACCEPT^M(\eta)>\lambda$; (2) ηが L に属さなければ，$ACCEPT^M(\eta)=0$。

[定義2.6] $0<\lambda<1$とする。もし,$0<c<\lambda$かつ$c<1-\lambda$を満たすcが存在し,Σ^*の任意の元ηに対して次の二つの条件が満たされれば,Mは言語Lを受理する間隔c,切断点λを持つ有界誤差 PPDA,即ちBPDAであると言う。 (1) ηが L に属するなら,$ACCEPT^M(\eta)>\lambda+c$; (2) ηが L に属さないなら，$ACCEPT^M(\eta)\leqq\lambda-c$ 。

[記法] 決定性プッシュダウン・オートマトンを DPDA[7];切断点λを持つPPDAをλ－PPDA,切断点λを持つRPDAをλ－RPDA,切断点λを持つBPDAをλ－BPDAと書く。DPDAによって受理される言語のクラスをDCFL,NPDAによって受理される言語のクラスをCFL,λ－PPDAによって受理される言語のクラスをPPDA(λ),λ－RPDAによって受理される言語のクラスをRPDA(λ),λ－BPDAによって受理される言語のクラスをBPDA(λ)と書く。また,便宜上,Mが PPDAであるかBPDAであるかRPDAであるかに関わらず，Mによって受理される言語をL(M)で表す。

3．DCFL, CFL, PPDA(λ), BPDA(λ), RPDA(λ)間の関係

[定理3.1] 任意の$0<\lambda_1<\lambda_2<1$に対して,$PPDA(\lambda_1)=PPDA(\lambda_2)$, $BPDA(\lambda_1)=BPDA(\lambda_2)$。

(証明) ほとんど自明である。 ■

定理3.1より,$PPDAL=\bigcup_{0<\lambda<1} PPDA(\lambda)$とすれば,$0<\lambda<1$を満たす任意の常数$\lambda$に対して,$PPDAL=PPDA(\lambda)$。$BPDAL=\bigcup_{0<\lambda<1} BPDA(\lambda)$とすれば,$0<\lambda<1$を満たす任意の常数$\lambda$に対して,$BPDAL=BPDA(\lambda)$。したがって,以下では, $PPDA(\lambda)$と$BPDA(\lambda)$のかわりに,PPDALとBPDALと書く。

[定理3.2] $CFL\subsetneq PPDAL$。

(証明) ChenとHuの結果よりほとんど明か。■

[補題3.1] $L_1\in RPDA(\lambda_1)$,$L_2\in RPDA(\lambda_2)$, $\lambda_1+\lambda_2>1$ならば, $L_1\cap L_2\in BPDAL$ 。

(証明) ほとんど自明。 ■

[定理3.3] $L\notin CFL$かつ$L\in BPDAL$となる言語Lが存在する。

(証明) 言語$L_1=\{a^i b^j c^k : i\geqq 1, i=j, k\geqq 1\}$と言語$L_2=\{a^i b^j c^k : i\geqq 1, j\geqq 1, j=k\}$を考えよう。明らかに,$L_1$と$L_2$はDCFLに属する。それに,$L_1\cap L_2\notin CFL$ 。一方,明らかに$1/2<\lambda<1$ を満たす任意のλに対して, $DCFL\in RPDA(\lambda)$補題3.1より, $L_1\cap L_2\in BPDA$ となる。 よって, $L\notin CFL$かつ$L\in BPDAL$となる言語Lが存在する。 ■

[補題3.2] 任意の $0<\lambda_1<\lambda_2<1$ に対して,$RPDA(\lambda_2)\subset RPDA(\lambda_1)\subset CFL$。また$BPDAL\subset PPDAL$。

(証明) 定義より明か。 ■

4. RPDA(λ)における階層

Σをアルファベットとする。$w=b_1b_2\cdots b_n$をΣ上の語とし,w^Rで$b_n\cdots b_2b_1$を表し,$|w|$でwの長さnを表す。

以下では,$\Sigma=\{0,1\}$と固定する。言語$L=\{¢w_1\#w_2\$w_3\#w_4¢ : w_i\in\Sigma^+, 1\leqq i\leqq 4, (w_3=w_1^R \text{ または } w_4=w_2^R)\}$について考える。

[補題4.1] 任意の定数 $0<\lambda<1/2$ に対して,$L\in RPDA(\lambda)$。

(証明) ほとんど自明。 ■

次に$L\notin RPDA(1/2)$を示す。これを示す前に,まずいくつかの定義と命題を述べる。

［定義4.1］コルモゴロフの計算量：チューリング機械の標準的枚挙を一つ固定する。チューリング機械Mに対し，MのΣ上の符号化を$c(M)$で表す。文字列$u,v\in\Sigma^*$に対して，vに関するuの条件付きコルモゴロフ計算量$K(u|v)$とは，前もってMの一つの作業用テープにvが書かれているとき，Mが入力xのもとでuを出力するといったMのうちの最短の長さ$|c(M)x|$のことである。uのコルモゴロフ計算量$K(u)$は$K(u|\varepsilon)$である。

［定義4.2］ランダムな文字列：文字列xがランダムであるとは$K(x)\geqq|x|$のときをいう。

［命題4.1］任意の正整数nに対して，長さがnであるランダムな文字列は常に存在する。

（証明）Paulらの論文[9]を参照。 ■

［命題4.2］文字列uvwがランダムであれば，$K(v|uw)\geqq|v|-O(\log|uvw|)$。

（証明）Paulの論文[8]を参照。 ■

［定義4.3］ηをRPDA Mへの入力とし，Mの入力ηに対する計算を一つ固定する。$\eta=xwy$とする。Mの入力ヘッドがηの部分語wを通過する間にスタックに文字aを積んだとする。このとき文字aのことを部分語wがスタックに積んだ文字と呼ぶ。部分語wが積んだ文字列のうち，入力ヘッドがwを出た直後に，スタックに残っている文字列をαとし，入力ヘッドがyの間にいるある時点tで，スタックに残っている部分をα'とすると，α'はαの前部分語(initial subword)となることに注意する。以下でαのことを部分語wが積んだ文字列と呼ぶ。α'のことをwに関する時刻tでのスタック残っている文字列と呼ぶ。即ち，wが積んだ文字列は入力ヘッドがwを出た後，次第にポップされ減少する（完全にポップされたら消える）。

［定義4.4］$\eta=xw_1yw_2z$をRPDA Mへの入力とし，ηに対するある計算を考える。入力ヘッドがw_2の間にいるあるとき，Mのスタック・ヘッドが部分語w_1が積んだ文字の一つを読んだなら，語w_1とw_2は対照(check)されたと言う。

［補題4.2］$\eta=¢w_1\#w_2\$w_3\#w_4¢$とし，Lを受理する任意の$\lambda$−RPDA ($0<\lambda<1$)をMとし，$\eta$をMへの入力とする。すると，Mのどんな計算も，$w_1$と$w_3$，$w_2$と$w_4$を同時に対照することはできない。

（証明）省略する。 ■

十分に長いランダムな文字列ξをとる。命題4.1より$|\xi|$を偶数と仮定してよい。ξを同じ

長さに二等分し,$\xi = w_1w_2$, $|w_1|=|w_2|$と書く。$w_3, w_4, \eta', \eta'', n$ を次のように定める。

$w_3=w_1^R$,　$w_4=w_2^R$,

$\eta'=¢w_1\#w_2\$w_3\#w_4 1¢$,　$\eta''=¢w_1\#w_2\$w_3 1\#w_4¢$

$|\eta'|=|\eta''|=n$ 。

以下では,η', η''をこのように固定し,議論する。また,Lを受理するλ-RPDAをMとする。

[補題4.3](主補題) η'を受理するのに,Mはw_1とw_3を対照しなければならない。

(証明)　Mがη'をw_1とw_3を対照せずに受理したと仮定し矛盾を導く。η'を受理するw_1とw_3を対照しない計算のうち長さが最短のものをSHORTEST とする。このとき,次の(*)が成立する。証明方法はChrobakとLiを参照のこと[4]。

(*) SHORTESTにおいて,任意の時刻tに,スタックの長さは$O(n^2)$である。

計算SHORTESTに関するいくつかのパラメータを定める:t_1は入力ヘッドがw_1を出た時刻,αは部分語w_1がスタックに積んだ(時刻t_1での)文字列,cはαの長さ,dはスタックのαより下の部分の長さである。t_0はαのすぐ下の文字Aがスタックに積まれた時刻である。従って$t_0<t_1$。t_2はスタック・ヘッドがαの先頭の文字Bに達した時刻,t_3はαが完全にポップされた時刻である。仮定より,SHORTESTはw_1とw_3とを対照しないので,時刻t_2からt_3までの間は,Mの入力ヘッドはw_3にいないことに注意する。

時刻tの表面様相ID_tを次のように定義する。ID_t=(入力ヘッドの位置,状態,スタックの先頭の文字)。ここで,$ID_{t0}, ID_{t1}, ID_{t2}, ID_{t3}$,c,dを使って$w_1$を出力するチューリング機械M′がMから構成できることを示す。最初,M′の入力テープには$x=(ID_{t0}, ID_{t1}, ID_{t2}, ID_{t3}, c, d)$があり,一つの作業用テープに$w_2$があるとする。(*)よりxの長さは$O(\log n)$であることに注意する。

$|w_1|=h$とし,Σ^*の長さhの各元uに対し,次の形の入力I_uを考える。

$I_u=¢0^h\#w_2\$u\#w_4 1¢$

M′は,入力I_uの下でのMの次の条件を満たす計算COM_uを見つける。

(i) 時刻t_0'までの計算はMの初期様相からの計算であり,時刻 t_0'でのスタックの長さはdで,表面様相はID_{t0}と一致する。

(ii) 時刻t_0'からt_1'までは計算をスキップする。即ちスタックに0^{c-1}を積み,Mの状態,入力ヘッドの位置,スタックの先頭の文字をID_{t_1}にセットする。(したがって入力の0^{h}は読み飛ばされる。)

(iii) 時刻t_1'からt_2'まではMの計算である。ただし時刻t_2'でのスタックの長さは$c+d$で,表面様相はID_{t_2}と一致しなければならない。

(iv) 時刻t_2'からt_3'までは計算をスキップする。即ちスタックから$B0^{c-1}$を取り除いてスタックの長さをdとし,Mの状態,入力ヘッドの位置をID_{t_3}にセットする。

(v) 時刻t_3'からはMの計算である。ただし最後(時刻t_a'とする)は受理様相でなければならない。

上の条件を満たす計算COM_uが見つかったなら,u^Rを出力して停止する。$u^R=w_1$のとき,条件を満たす計算は存在する(少なくともSHORTESTがそうである)。従ってM'はいずれは停止する。

次にM'が出力する語はw_1以外にないことを示そう。

今,M'が$u^R \neq w_1$なる語u^Rを出力したと仮定し矛盾を導く。$\eta_u = ¢w_1\#w_2\$u\#w_4 1¢$ とする。η_uに対するMの計算をSHORTESTとCOM_uより次のように構成する。時刻0(即ち初期様相)より時刻t_0'までの計算はCOM_uに従う。t_0'よりt_1まではSHORTESTに従う。t_1よりt_2'まではCOM_uに従う。t_2'よりt_3まではSHORTESTに従う。t_3よりt_a'まではCOM_uに従う。すると,仮定より構成した計算はη_uに対するMの受理計算である。従ってη_uがMによって受理される確率は0ではない。しかし,これは$\eta_u \notin L(w_1 \neq u^R, w_4 1 \neq w_2^R)$に矛盾する。よって,M'は$w_1$を正しく出力する。M'を符号化し，得られたものを $c(M')$ とする。明らかに$|c(M')|$が定数で抑えられる。よって,

$K(w_1 | w_2)=|c(M')x|=O(\log n)=O(\log(|w_1 w_2|))<|w_1|-O(\log(|w_1 w_2|))$

命題4.2より,これは矛盾であり,よって補題4.3が成立する。 ■

[補題4.4] η''を受理するのに,Mはw_2とw_4を対照しなければならない。

(証明) 補題4.3とほとんど同じように示せる。 ■

[補題4.5] $L \notin RPDA(1/2)$。

(証明) まず, $\min(ACCEPT^M(\eta'), ACCEPT^M(\eta''))\leq 1/2$を示す。入力$¢w_1\#w_2\$w_3$に対する計

算を考える。$¢w_1\#w_2\$w_3$は$\eta'$と$\eta''$の共通の前部分語であり，入力$¢w_1\#w_2\$w_3$に対する計算は入力$\eta'$,入力$\eta''$の計算の部分計算となることに注意する。入力$¢w_1\#w_2\$w_3$に対する，$w_1$と$w_3$を対照する計算の確率の総和を$P_1$とおく。補題4.3より，$ACCEPT^M(\eta')\leqq P_1$を得る。一方補題4.2より,入力$\eta''$に対する計算で$w_2$と$w_4$を対照するものの確率の総和は$1-P_1$以下である。従って補題4.4より,$ACCEPT^M(\eta'')\leqq 1-P_1$を得る。 $ACCEPT^M(\eta')\leqq P_1$と $ACCEPT^M(\eta'')\leqq 1-P_1$より,$ACCEPT^M(\eta'')\leqq 1-ACCEPT^M(\eta')$。 従って，$\min(ACCEPT^M(\eta'),ACCEPT^M(\eta''))\leqq 1/2$。RPDA(λ)の定義より,$L\in RPDA(\lambda)$なら,$\lambda<1/2$。 ■

［定理4.1］ $0<\lambda<1/2$を満たす任意のλに対して,$RPDA(1/2)\subsetneq RPDA(\lambda)$。

（証明） 補題3.2と補題4.1と補題4.5より明か。 ■

［定理4.2］ 任意の整数$m>1$と任意のλ,$0<\lambda<1/m$に対して，$RPDA(1/m)\subsetneq RPDA(\lambda)$。

（証明） $L_m=\{¢w_1\#w_2\#\cdots\#w_m\$w_{m+1}\#w_{m+2}\#\cdots\#w_{2m}¢ : w_{m+1}=w_1^R$ または $w_{m+2}=w_2^R$ または…または $w_{2m}=w_m^R\}$を考えよう。定理4.1とほとんど同じようりり証明できる。 ■

5．結論

本稿の結果は図1に示されている。

図1で,太線は真に包含されていることを示し,細線は真に包含されるかどうかまだわかっていないことを示す。

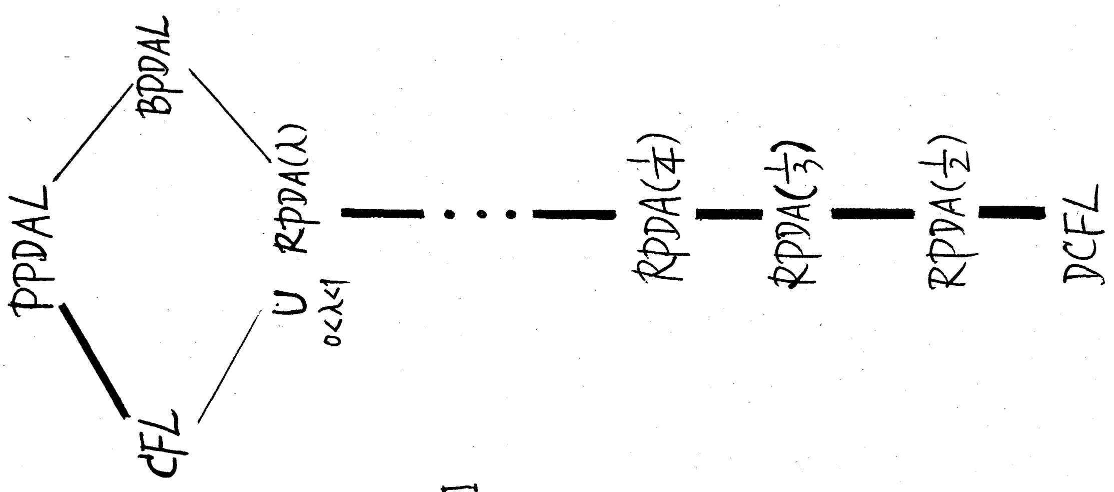

図1

参考文献：

(1) Angluin,D. and Valiant,L.G.:"Fast Probabilistic Algorithms For Hamiltonian Circuits and Matching",J.Comput.& Syst.Sci.,18,pp.155-193(1979).

(2) Borodin,A. and Cook,S.:"Parallel Computation For Well-Endowed Rings and Space-Bounded Probabilistic Machines",Inf.&Control,58,pp.113-136(1983).

(3) Chen,K.A. and Hu,M.K.:"A Finite State Probabilistic Automaton that Accepts a Context Senstive Language that is Not Context Free",Inf.&Control,35,pp.196-208 (1977).

(4) Chrobak,M. and Li,M.:"k+1 Heads are Better Than k for PDA's",Proc. 27th Annual IEEE Symposiumon on FOCS,pp.361-367(1986).

(5) Gill,J.:"Computational Complexity of Probabilistic Turing Machine ",SIAM J.Comput.,6,4,pp.675-695(1977).

(6) Karp,R.M.:"The probabilistic Analysis of Some Combinatorial Search Algorithms", Algorithms and Complexity,New Direction and Recent Results,J.F.Traub,ed.,Academic Press,New York,pp.1-19(1976).

(7) Kasai,T.:"計算量の理論"，近代科学社，1986.

(8) Paul,W.:"On-line Simulation of k+1 Tapes by k tapes Require Nonlinear Time", Proc.23rd Annual IEEE Symposium on FOCS,pp.53-56(1982)

(9) Paul,W. and Seiferas,J. and Simon,J.:"An Information-theoretic Approach to Time Bounds for On-line Computations",Proc.12th Symposium on Theory of Computing,pp. 357-367(1980).

(10) Rabin,M.O.:"Probabilistic Automata",Inf.&Control,6,pp.230-245(1963).

(11) Rabin,M.O.:"Probabilistic Algorithms",Algorithms and Complexity,New Direction and Recent Results,J.F.Traub,ed.,Academic Press, New York,pp.21-39(1976).

(12) Rabin,M.O.:"Probabilistic Algorithms In Finite Fields",SIAM J.Comput.,9,2,pp.

273-280(May,1980).

(13) Ruzzo,W.L. and Simon,J. and Tompa,M.:"Space-bounded Hierarchies and Probabilistic Computations",J.Comput.& Syst.Sci.,28,pp.216-230(1984).

(14) Schwartz,J.T.:"Fast Probabilistic Algorithms For Verification of Polynomial Identities",J.Assoc.Comput.Mach.,Vol.27,No.2,pp.273-280(May,1980).

(15) Shoning,U.:"Probabilistic Complexity Classes and Lowness",2nd Annual Structure in Complexity Theory,pp.2-8(1987).

(16) Solovay,R. and Strassen,V.:"A Fast Monte-Carlo Test For Primality",SIAM J.Comput.,6,pp.84-85(1977).

(17) Turakainen,P.:"On Stoshastic Languages",Inf.&Control,12,pp.304-313(1968).

(18) Zachos,S.:"Robustness of Probabilistic Computational Complexity Class under Definitional Perturbations",Inf.&Control,54,pp.143-154(1982).

(19) Zachos,S. and Heller,H.:"A Decisive Characterization of BPP",Inf.&Control,69, pp.125-135(1986).

(20) Zachos,S.:"Probabilistic Quantifiers,Adversaries,and Complexity Classes",1st Annual Structure in Complexity Theory,pp.383-400(1986).