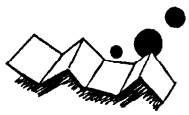
解　説



確率的アルゴリズムの概観†

五十嵐　善　英††

1. まえがき

計算機アルゴリズムの設計と解析理論では，アルゴリズムの最悪の場合の効率と平均的な効率について主に議論されてきた．例えば Quick Sort と呼ばれるアルゴリズムでは，最悪の場合，入力の大きさ（即ち，分類されるものの個数）nに対して，入力データを大きさの順に並べ換えるのに必要な比較演算の回数は$O(n^2)$であるが，比較演算の回数の期待値は$O(n\log_2 n)$である．アルゴリズムのこのような解析理論は，計算機科学の基礎課題の一つとして，活発な研究が続けられるであろう．しかし，組合せ論的な問題や決定問題の多くはNPハードであり，このような問題を解く多項式時間のアルゴリズムが存在するかどうかでさえ現在まで知られておらず，多くの人達を落胆させている．このため，違った立場から，効率のよい計算機アルゴリズムの設計とそれらの解析理論の研究を進めることも必要ではないかと考えられるようになってきた．

1976年4月に Carnegie-Mellon 大学で，「アルゴリズムと複雑さの理論に関する新しい研究方向と結果」と題したシンポジウムが開かれ，California 大学 Berkeley 分校の R. M. Karp[21] と Hebrew 大学の M. O. Rabin[31] が確率的なアルゴリズムの講演を行った．勿論，確率的アルゴリズムの考え方はそれ以前からもあったし，それ等に関するいくつかの結果も導かれていたが[17),18)]，彼等の講演はその後のアルゴリズム理論の研究に大きな影響を与えたといえる．この時，Karp は彼自身による確率的アルゴリズムも含めて，アルゴリズムの確率的な取り扱い方の概要を紹介し，Rabin は，彼の確率的アルゴリズムの方法論を二つの例で説明した．

1976年7月に Edinburgh 大学で開かれた国際会議 (The 3rd International Colloquium on Automata, Languages and Programming) の Conference Dinner Seminar でも，Rabin は確率的アルゴリズムを解説し，その重要性を説いた．その後の確率的アルゴリズムの進歩は急速という訳にいかなかったが，いくつかの興味ある結果も導かれた．進歩の速度のおそさは，確率的アルゴリズムの難しさを意味するようであり，今後もこの分野の発展のために多くの努力が続けられていくと思う．1979年7月オーストリアの Graz で開かれた国際会議 (The 6th International Colloquium on Automata, Languages and Programming) で Karp[25] は，「グラフに関するアルゴリズムの確率的解析理論の最近の進歩」と題する講演を行い，1976年から今日までの確率的アルゴリズムの進歩の概要を紹介した．

2. アルゴリズムの確率的解析

多くの組合せ論的な問題，例えば，巡回セールスマン問題，グラフの色付け問題，ブール関数の CNF (conjunctive normal form) の値を真にする変数の値の組が存在するかどうかを決定する問題などはNP完全であり，$p=NP$ でなければ，これ等の問題を解く多項式時間のアルゴリズムは存在しない．したがって，NPハードな問題については，最適解を与える効率のよいアルゴリズムを見つける努力をするよりも，近似解を与える多項式時間のアルゴリズムとか，正しい最適解を与える確率が高い多項式時間のアルゴリズムを見つける努力をする方がより現実的であると考えられた．このような立場でアルゴリズムを設計しようとした最初の試みはおそらく R. Graham による論文[17]であろう．1973年頃から，この方面の研究もかなり活発になってきた[14),15),35)]．

アルゴリズムの近似度を表わす大きさrをつぎのように定義する．問題pの任意の例Iについて，その最小コスト解のコストを$C^*(I)$とする．この問題のアルゴリズムAで与えられる解のコストを$C_A(I)$とし，

† A Survey of Probablistic Algorithms by Yoshihide IGARASHI (Department of Computer Science, Gunma University).
†† 群馬大学工学部情報工学科

$C_A(I) \leq rC^*(I)+d$ ならば，アルゴリズムAの近似度はrであるという[21]．但し，rとdはpの例に関係なく，上の不等式が成立する定数である．rが1に近い程，近似性のよいアルゴリズムである．NPハードな問題について，十分小さい値εで，$r=1+\varepsilon$なる近似度の多項式時間のアルゴリズムが存在するのではないかという期待が持たれた．

残念なことに，上の期待に対して，次のような悲観的な結果が1976年に，M. R. Garey と D. S. Johnson[15]によって与えられた．$p=NP$でなければ，どのような多項式時間のアルゴリズムでもグラフの色付け問題を$r<2$なる近似度で解を与えることは出来ない．rの値が2またはそれ以上では，実用的に満足できる近似解ではない場合が多い．巡回セールスマン問題については，$O(n^3)$で$r=3/2$の近似的アルゴリズムが，N. Christofides[4]によって1976年に与えられたが，やはり実用的な観点から，これも満足すべきものではないだろう．

NPハードな問題に対処するもう一つの方法は，問題のすべての例について最適解または近似解を与えるアルゴリズムを見つける努力をするだけでなく，問題のほとんどすべての例について最適解または近似解を与える多項式時間のアルゴリズムの発見に努めることであろう．Karpは1976年に，巡回セールスマン問題のほとんどすべての問題例について，その時間量複雑さが$O(n\log_2 n)$であり，任意の$\varepsilon>0$について近似度が$r=1+\varepsilon$であるような確率的かつ近似的アルゴリズムを与えた[21]．

3. Rabin の方法論と二つの例

Rabinは文献31)の中で，アルゴリズムの複雑さにおけるランダム性の意味を追求し，確率的アルゴリズムの概念と方法を二つの例で示した．最初の例では，ランダム性をアルゴリズムに導入することにより，計算時間の期待値を減少させることができる場合があることを示し，二つ目の例で，間違った答えを出すこともあるが，計算時間が非常に少なく，誤りの可能性を任意の大きさにまで小さくすることができるアルゴリズムを示した．

pの問題例Iの大きさを$|I|$で表わす．例えば，pをソーティングの問題とすると，$I=(x_1, \cdots, x_n)$は，$x_1, \cdots, x_n$を大きさの順，即ち，$x_{\pi(1)} \leq \cdots \leq x_{\pi(n)}$になるように並べ換える問題であり，$|I|=n$である．ただし，ここで$\pi$は，$\{1, \cdots, n\}$上の置換である．アルゴリズムにランダム性を導入するということは，$1 \leq b \leq n$なるbをランダムにm個抽出し，$(b_1, \cdots, b_m)$をアルゴリズムの中で用いることである．ただし，ここでb_iはi番目にランダム抽出された数bである．

$|I|=n$なるpの任意の問題例Iについて，アルゴリズムAがIを解くのに要する計算時間の期待値が$f(n)$である時，Aは期待時間$f(n)$で問題pを解くという．AをRabinのいう確率的アルゴリズムであるとき，そのアルゴリズムの操作の中にランダムに$(b_1, \cdots, b_m)$を抽出するという操作が入っている．そのようなAの計算時間の期待値は，任意に抽出された$(b_1, \cdots, b_m)$についての計算時間の期待値である．アルゴリズムには，$(b_1, \cdots, b_m)$をランダムに抽出すること以外は確率的な操作は含まれていない．即ち，他のすべての操作は決定性であることを強調しておく．

3.1 最近接の点の組を見つけるアルゴリズム

$x_1, \cdots, x_n$を2次元ユークリッド空間R^2のn個の点とする(一般のk次元ユークリッド空間についても，以下の議論は同様に進めることができる)．$d(x, y)$をR^2で普通に定義されるxとy間の距離とする．$d(x_i, x_j)=\min\{d(x_p, x_q) | x_p, x_q \in \{x_1, \cdots, x_n\}$で，$x_p \neq x_q\}$なる$(x_i, x_j)$を見つける問題を考える．すべての点の組について，二つの点の間の距離を求め，その中から最小の距離の組を選びだす方法では，$O(n^2)$回の距離計算が必要である．$O(n\log_2 n)$回の距離計算で解が求まるアルゴリズムは，J. L. Bentley と M. I. Shamos[3]およびG. Yuval[38]によって与えられたが，Rabinはこの問題のランダム抽出の操作を含む興味あるアルゴリズムを示した[31]．その計算時間の期待値は$O(n)$である．アルゴリズムの概要は次のとおりである．

R^2のn個の点の集合，$S=\{x_1, \cdots, x_n\}$を互いに共通元を持たないk個のクラス，$S_1, \cdots, S_k$に分けたとする．これをSの分割といい，$D=(S_1, \cdots, S_k)$で表わす．各S_i $(1 \leq i \leq k)$の元の数をn_iとし，$N(D)=\sum_{i=1}^{k} n_i(n_i-1)/2$を分割$D$の測度と呼ぶ．もし，最近接の点の組が，上の分割$D$で同じクラスに入っていることが分っていれば，距離計算と比較計算の回数が$O(N(D))$で，最近接の組が見つかる．したがって，上の条件を満す分割が$O(n)$の計算時間ででき，$N(D)$の期待値が$O(n)$ならば，最近接の組を求めるのに必要な計算時間の期待値が$O(n)$のアルゴリズムが設計できる．

Rabinは文献31)の中で，次の定理を証明した．

定理1 $S=\{x_1, \cdots, x_n\}$をR^2のn個の点の集合

とする．Sの中からランダムに $m=\lceil n^{2/3}\rceil$ 個選び，その集合を $S_1=\{x_{i_1},\cdots,x_{i_m}\}$ とする．S_1 を用いて，次の条件を満足する分割，$\Gamma_1,\Gamma_2,\Gamma_3,\Gamma_4$ を $O(n)$ の計算時間で構成できる．

（1） 各 i $(1\leq i\leq 4)$ について，$N(\Gamma_i)\leq cn$ であるような確率は少なくとも，$1-e^{-cn^{1/6}}$ である．ここで，c は n に無関係な定数である．

（2） 最近接の点の組が同じクラスに入る分割が，$\Gamma_1,\Gamma_2,\Gamma_3,\Gamma_4$ の中に少なくとも一つ存在する．

上の定理の分割，Γ_i $(1\leq i\leq 4)$ の構成方法は文献31）で与えられている．定理1とその定理の前に述べたことから，計算時間の期値値が $O(n)$ で，最近接の点の組を見つけるアルゴリズムを設計できることが分る．

今のところ，Rabinのこのアルゴリズムは，誤り率が0で，同じ問題を解く決定性のアルゴリズム（即ち，ランダム抽出の操作の入らないもの）よりも計算量の複雑さが小さい唯一の確率的アルゴリズムである．

3.2 素数であるかどうかの判定アルゴリズム

n を与えられた自然数とする．$1\leq b\leq n$ なる自然数 b について，次の（1）又は（2）であるという命題を $W_n(b)$ とする．

（1） b^{n-1} を n で割ると余りは1ではない．

（2） $m=(n-1)/2^t$ は整数であり，b^m-1 と n の最大公約数は1でも n でもない i が存在する．

$W_n(b)$ が真であると n は素数ではないことが知られている[28]．$W_n(b)$ に関する次の定理は Rabin によって与えられた[31]．

定理2 n が素数でなければ，$\{b\mid W_n(b)\}$ の元の数は，$(n-1)/2$ 以上である．

$W_n(b)$ が真であるかどうかを判定するのに必要な計算時間は僅かである．$\{1,\cdots,n\}$ からランダムに m 個の整数，$b_1,\cdots,b_m$ を抽出し，各 b_i $(1\leq i\leq m)$ について，$W_n(b_i)$ が成立するかどうか調べる．$W_n(b_i)$ が成立する b_i が一つでも存在すれば，n は素数ではない．ランダムに抽出した m 個の n よりも小さい自然数 $(b_1,\cdots,b_m)$ について，$W_n(b_i)$ $(1\leq i\leq m)$ がすべて真でないとき，n は素数であると判断する．勿論この判断は間違っているかもしれないが，それが間違いである確率は定理2から $1/2^m$ 以下である．例えば，$m=50$ のとき，誤りの確率は約千兆分の1となり，基本演算の所要時間が $1\,\mu s$ で，3万年間連続稼動している間に一度の割にしか基本演算の誤動作が生じない電子計算機よりも信頼性の高い判定方法である．

Rabin 等はこの方法で，2^p-1 なる形の整数が素数であるかどうかの判定を計算機を用いて行った．p が1から500までの判定をたった数分で行い，すべての判定は正しかったと報じている[31]．つまり，この方法は素数であるかどうかを判定するどの決定性アルゴリズムよりも桁違いに速く，サンプル数 m を適当な大きさ以上にすることにより，誤りの確率を非常に低くすることができる．Rabin はこの例から，信頼性が高くて効率のよい確率的アルゴリズムを設計するためには，答えを出すのに必要な情報がランダム抽出された要素の中になるべく多く現われるような性質を調べるべきだと主張している．一般に，そのような性質を見つけることは難しいことではあるが，効率のよい確率的アルゴリズムを設計するためには重要なことであり，この方面の努力も大いに必要であると思われる．このことについて，もう少し具体的な説明を続けるために，次の命題（3）（これを $p_n(b)$ で表わす）の真偽を調べることにより，素数であるかどうかを判定するありきたりのアルゴリズムを考える．

（3） n は b で割り切れる．

2から $\sqrt{n}$ までのすべての整数について，（3）の命題の真偽を調べれば，確実な答えが出るのはあきらかである．しかし，ランダムに抽出した m 個の $r_i(b_1,\cdots,b_m)$ について，$p_n(b_i)$ $(1\leq i\leq m)$ を調べる場合，$\bigvee_{i=1}^{m} p_n(b_i)$ が真でなければ n は素数であると判定するのは，m が $\sqrt{n}$ に近いときを除いて，その答えが正しい確率は高くはない．この事実は，n が二つの大きな素数の積である場合を考えればあきらかである．つまり，$p_n(b)$ ではなく $W_n(b)$ という命題とその性質に気がついたことが，Rabin の効率のよい素数判定アルゴリズムが生れた鍵であった．

4. Angluin と Valiant のアルゴリズム

Karp と Rabin 等の論文[21),31)]に刺激されて，いくつかの興味ある確率的アルゴリズムとそれ等の解析理論が発表されたが[1),2),5),12),18),19),22)~24),26),27),32)~34)]，D. Angluin と L. G. Valiant による多項式時間のハミルトン順路を求める確率的アルゴリズム[1)]は特記すべきだと思う．ハミルトン順路を求める問題は NP 完全であるが，それが誤り率の極めて低い確率的アルゴリズムにより，多項式時間で求まることは，確率的アルゴリズムの有用性を強く主張したことになる．

Angluin は1976年 California 大学 Berkley 分校

で Ph. D を取得し，1976年8月に，当時イギリスの Leeds 大学の講師だった Valiant の研究員として赴任してきた．Angluin の Berkley での指導教官は M. Blum であったが，あきらかに Karp の影響で確率的アルゴリズムに興味を持っていた．Leeds 大学に赴任早々，彼女はグラフ問題の確率的アルゴリズムの仕事に取りかかった．彼女の計算機アルゴリズムの設計に関する感覚のよさと Valiant の非凡な組合せ論的な解析力により，彼等の仕事を発展させていった．P. Erdös[6)~10)] や L. Pósa[30)] 等のランダムグラフに関する結果などを用いたりして，1976年の終り頃までに，ハミルトン順路を求める確率的アルゴリズムを導き，それは多項式時間で実行されることを示した[1)]．1977年1月，Angluin と Valiant は Edinburgh 大学に移り，そこでその論文を仕上げた．Karp 等に送られたその論文の前刷りは，たちまち高く評価されたという．余談になるが，Angluin は1978年8月にイギリスを去り，California 大学 Santa Barbara 分校に一年間勤めたあと，1979年9月から Yale 大学で仕事をしている．

グラフ G を (V, E) で表わす．但し，V は G の節の集合で，E は G の枝の集合である．$E \subseteq \{(v, w) \mid v, w \in V;\ v \neq w\}$ のとき，G を有向グラフといい，$E \subseteq \{\{v, w\} \mid v, w \in V;\ v \neq w\}$ のとき，G を無向グラフという．u から v のハミルトン順路は，G の各節を正確に一度だけ通る u から v の順路をいい，特に $u = v$ のとき，ハミルトン順回路という．

$G=(V, E)$ の $u \in V$ からの枝をランダムに選ぶ手続 SELECT は次のようになる．

```
procedure SELECT (u)
  begin if for all v∈V (u, v)∉E
          then return "*"
          else select at random with equal probabilities one of the edges (u, v)∈E,
          delete (u, v) from E, and return the value v
  end
```

有向グラフ $G=(V, E)$ の節 s から t へのハミルトン順路を求める確率的アルゴリズムは下の手続，DHC (G, s, t) で示される．この手続の中で，上の手続 SELECT が何度か呼び出される．

```
procedure DHC (G, s, t)
  begin: ndp←s; p←φ;
  2: (comment: P consists of a directed path from s to ndp);
    if P includes every node of V (except t, in the case s≠t) and if we previously explored and deleted (ndp, t) from E then add (ndp, t) to P and return "success";
    v←SELECT (ndp);
    if v="*" then return "failure";
    if v≠t and v is not in P then add (ndp, v) to P, ndp←v and go to 2;
    if v≠s and v is in P and there are at least n/2 nodes in P between v and ndp (inclusive) then
      begin
        u←predecessor of v in P;
        delete (u, v) from P;
        add (ndp, v) to P;
        ndp←u;
        go to 3
      end
    else (i.e. if v=s or v=t or cycle is too small) go to 2;
  3: (comment: P consists of a directed path from s to ndp and a disjoint directed cycle of at least n/2 nodes);
    v←SELECT (ndp);
    if v="*" then return "failure";
    if v≠t and v is not in P then begin add (ndp, v) to P;
      ndp←v; go to 3
    end;
    if v is in the cycle part of P then begin
      u←predecessor of v in P;
        delete (u, v) from P;
        add (ndp, v) to P;
        ndp←u; go to 2
      end
    else go to 3
  end
```

ランダム有向グラフ $D_{n,N}$ は正確に n 個の節と N 個の枝を持ち，枝の存在確率がすべて等しいと定義される[6)]．Angluin と Valiant は，このようなランダムグラフ上での彼等のハミルトン順路を見つけるアルゴリズムの動作を解析し，次の結果を得た．

定理 3 任意の α と，$cn\log_2 n$ より小さくない任

意のNについて，つぎのような定数kが存在する．ここで，cは与えられた定数である．

DHP$(D_{n,N,s,t})$が SELECT を $kn(\log_2 n)^2$ 回呼び出す前に "success" を出力として出す確率は少なくとも $1-O(n^{-\alpha})$である．このアルゴリズムをランダムアクセス計算機で実行した時の時間量複雑さは $O(n(\log_2 n)^2)$ である．

上の定理のαは，cを増加させ，計算時間を定係数倍増加させることにより，任意の大きさに増加させることができる[1]．したがって，Angluin と Valiant のアルゴリズムにより，枝の密度が十分大きいグラフのハミルトン順路は，$O(n(\log_2 n)^2)$ の計算時間で見つかる確率を1にいくらでも近くすることができる．

定理3では，ランダムグラフの枝の数Nは $cn\log_2 n$ より少なくないという制限があるが，次の理由により，この制限を定係数の範囲以上に緩めることはできない．任意の $\varepsilon>0$ について，$N<(1/2-\varepsilon)n\log_2 n$ のとき，$G_{n,N}$ が弧立した節を持つ確率は1に近づくことが P. Erdös と A. Rónyi によって証明されている[6]．弧立した節を持てば，ハミルトン順路を持たないので，$N<(1/2-\varepsilon)n\log_2 n$ なる $G_{n,N}$ のハミルトン順路が見つかる可能性は少ないといえる．

Angluin と Valiant は無向グラフのハミルトン順路を見つける確率的アルゴリズムも与え，それについて，定理3に相当する結果も与えた．無向グラフの完全マッチングを見つける決定性アルゴリズムの最良の計算量複雑さの上限は $O(n^{5/2})$ である[11]．彼等は，この問題の計算量複雑さが $O(n\log_2 n)$ なる確率的アルゴリズムも与えた[1]．

5. 確率的チューリング機械

1974年に J. T. Gill III[16] は，ランダム発生機を備えたチューリング機械を定義し，確率的チューリング機械と名付けた．これは，確率的アルゴリズムと本質的に同じ考え方で作られた計算機のモデルである．よく知られているように言語 $L=\{\omega c\omega|\omega\in\Sigma^*\}$ は，一本のテープをもつチューリング機械で，$O(n^2)$ で認識されるが，$\sup_{n\to\infty}(T(n)/n^2)>0$ でなければ，$O(T(n))$ では認識されない(文献20の定理 10.7)．ソ連の数学者，R. V. Freivald によって，次のような興味ある結果が導かれた[13]．$O(n(\log_2 n)^2)$ なる時間量複雑さの一本のテープを持つ確率的チューリング機械によって，$L=\{\omega c\omega|\omega\in\Sigma^*\}$ を非常に小さい誤り率で認識できる．1977年に，N. Pippenger により[29]，上の結果の上限 $O(n(\log_2 n)^2)$ を $O(n\log_2 n)$ に改良された．この問題については，誤りの確率を犠牲にしても，計算時間の上限 $O(n\log_2 n)$ を下げることができないことは，A. C. Yao によって証明された[37]．

確率的チューリング機械に関する結果は，現在までごく僅かであるが，今後の発展は期待できると思う[36]．

6. あとがき

確率的アルゴリズムの設計と解析理論はまだ揺籃期にあると思う．確率的アルゴリズムの効率を解析的に評価することは困難である場合が多いが，そのような時は，実験的にアルゴリズムの効率を評価することも必要である．確率的アルゴリズムに，発見的な方法を積極的に取り入れ，効率をよくしたり，誤りの確率を下げることもこれからの課題と思う．

参考文献

1) Angluin, D. and Valiant, L. G.: Fast probabilistic algorithms for Hamiltonian circuits and matchings, Proc. 9 th ACM Symposium on Theory of Computing, pp. 30-41 (1977).
2) Apers, P.: The expected number of phases of the Dinic-Karzanov network flow algorithm, Informatica Report IR 27, Vrije Universiteit, Amsterdam (1978).
3) Bentley, J. L. and Shamos, M. I.: Divide-and-conquer in multidimensional space, Proc. 8 th ACM Symposium on Theory of Computing, pp. 220-230 (1976).
4) Christofides, N.: Worst-case analysis of a new heuristic for the traveling salesman problem, in Algorithms and Complexity: New Directions and Recent Results, J. F. Traub ed., Academic Press, New York, pp. 441-441 (1976).
5) Chvátal, V.: Determining the stability number of a graph, SIAM J. Computing, Vol. 6, pp. 643-662 (1977).
6) Erdös, P. and Rényi, A.: On random graphs I, Publicatione Mathematicae, Vol. 6, pp. 290-297 (1959).
7) Erdös, P. and Rényi, A.: On the evolution of random graphs, Publ. Math. Inst. Hung. Acad. Sci. Vol. 5A, pp. 17-61 (1960).
8) Erdös, P. and Rényi, A.: On random matrices, Publ. Math. Inst. Hung. Acad. Sci., Vol. 8A, pp. 455-461 (1963).
9) Erdös, P. and Rényi, A.: On the existence of a factor of degree one of a connected random graph, Acta Math. Acad. Sci. Hung., Vol. 17, pp. 359-368 (1966).

10) Erdös, P. and Spencer, J.: Probabilistic Methods in Combinatorics, Academic Press, New York (1974).
11) Even, S. and Kariv, O.: An $O(n^{2.5})$ algorithm for maximum maching in general graphs, Proc. IEEE 16 th Symposium on Foundations of Computer Science, pp. 100-112 (1975).
12) Fortune, S. and Hopcroft, J.: A note on Rabin's nearest-neighbor algorithm, Computer Science Report TR 78-340, Cornell University, Ithaca, N. Y. (1978).
13) Freivald, R. V.: Fast computation by probabilistic Turing machines, Theory of Algorithms, No. 2, Latvian State University, Riga, pp. 201-205 (in Russian) (1975).
14) Garey, M. R., Graham, R. L. and Johnson, D. S.: Some *NP*-complete geometric problems, Proc. 8 th ACM Symposium on Theory of Computing, pp. 10-22 (1976).
15) Garey, M. R. and Johnson, D. S.: The complexity of near-optimal graph coloring, J. ACM, Vol. 23, pp. 43-49 (1976).
16) Gill III, J. T.: Computational complexity of probabilistic Turing machines, Proc. 6 th ACM Symposium on Theory of Computing, pp. 91-95 (1974). The revised version appeared in SIAM J. Computing, Vol. 6, pp. 675-695 (1977).
17) Graham, R. L.: Bounds for certain multiprocessing anomalies, Bell System Tech. J., Vol. 45, pp. 1563-1581 (1966).
18) Grimmett, G. R. and McDiamid, C. J. H.: On coloring randam graphs, Math. Proc. Camb. Plil. Soc. Vol. 77, pp. 313-324 (1975).
19) Hamacher, H.: Numerical investigations on the maximal flow algorithm of Karzanov, Report 78-7, Mathematishes Institut, Universität zu Köln (1978).
20) Hopcroft, J. E. and Ullman, J. D.: Formal Languages and Their Relation to Automata, Addison-Wesley, Reading, Mass. (1969).
21) Karp, R. M.: The probabilistic analysis of some combinatorial search algorithms, in Algorithms and Complexity: New Directions and Recent Results, J. F. Traub ed., Academic Press, New York, pp. 1-19 (1976).
22) Karp, R. M.: An algorithm to solve the $m \times n$ assignment problem in expected time $O(mn \log n)$, Memorandum No. UCB/ERL M 78/67, Electronics Research Laboratory, University of California, Berkeley (1978).
23) Karp, R. M.: A patching algorithm for the nonsymmetric traveling-salesman problem, to appear in SIAM J. Computing (1979).
24) Karp, R. M.: Probabilistic analysis of canonocal numbering algorithm for graphs, Proc. AMS Symposia in Applied Mathematics, Vol. 34 (1979).
25) Karp, R. M.: Recent advances in the probabilistic analysis of graph-theoretic algorithms, Proc. 6 th Colloquium on Automata, Languages and Programming, pp. 338-339 (1979).
26) Lueker, G. S.: Maximization problems on graphs with edge weights chosen from a normal distribution, Proc. 10 th ACM Symposium on Theory of Computing, pp. 13-18 (1978).
27) McDiamid, C.: Determining the chromatic number of a graph, SIAM J. Computing, Vol. 8, pp. 1-14 (1978).
28) Miller, G. L.: Riemann's hypothesis and test for primality, Proc. 7 th ACM Symposium on Theory of Computing, pp. 234-239 (1976).
29) Pippenger, N.: Unpublished Memo (1977).
30) Pósa, L.: Hamiltonian circuits in random graphs, Discrete Math. Vol. 14, pp. 359-368 (1976).
31) Rabin, M. O.: Probabilistic algorithms, in Algorithms and Complexity: New Directions and Recent Results, J. F. Traub ed., Academic Press, New York, pp. 21-39 (1976).
32) Rabin, M. O.: Probabilistic algorithms in finite fields, Laboratory for Computer Science Report, Tr-213, M. I. T., Cambridge, Mass. (1979).
33) Rohlf, F. J.: A probabilistic minimum spanning tree algorithm, IBM Research Report, RC-6502, Yorktown Heights, New York (1977).
34) Schnorr, C. P.: An algorithm for transitive closure with linear expected time, SIAM J. Computing, Vol. 7, pp. 127-133 (1978).
35) Solovay, R. and Strassen, V.: A fast monte-Carlo test for primality, SIAM J. Computing, Vol. 6, pp. 84-85 (1977).
36) Yao, A. C.: Probabilistic computations-toward a unified measure of complexity, Proc. 18 th IEEE Symposium on Foundations of Computer Science, pp. 222-227 (1977).
37) Yao, A. C.: A lower bound to palindrome recognition by probabilistic turing machines, Computer Science Report, STAN-CS-77-647, Stanford University, Stanford, California(1977).
38) Yuval, G.: Finding nearest neighbors, Information Processing Letters, Vol. 5, pp. 63-65 (1976).

(昭和54年9月17日受付)