計算量理論

先週の続きは次回

平成26年11月18日

代講　河村彰星（今井研助教）

http://www-imai.is.s.u-tokyo.ac.jp/~kawamura/teaching/0510021/

片側誤り
誤受理なし
誤拒否あり

定義

randomized の R

判定問題 A が級 **RP** に属するとは
或る多項式時間（乱択）機械 M が存在し
任意の入力 x に対し

「>0」にすると **NP**

$A(x)=$ 真　のとき　$M(x,r)$ は**確率** $>\frac{1}{2}$ で受理

$A(x)=$ 偽　のとき　$M(x,r)$ は**必ず**拒否

$\frac{1}{2}$ の代りに $\frac{99}{100}$ にしたければ…

P ⊆ RP ⊆ NP

乱数を独立に 7 回取って $r_1,\cdots,r_7$
$M(x,r_1),\ \cdots,\ M(x,r_7)$ のうち一つ以上が受理したら受理

問題　与えられた整数係数多項式 $p(X_1,\ldots,X_m)$ が**非零**であるか判定せよ

P に属するかは未解決だが　次の算法により **RP** に属する
（多項式**零判定**が **coRP** に属する）

算法　数 $r_1,\ldots,r_m \in \{1,\ldots,2d\}$ を一様独立に乱択し
$p(r_1,\ldots,r_m)\neq 0$ ならば受理

（d は p の全次数）

➡ p が零なら確実に拒否
非零なら次の補題により確率 $>\frac{1}{2}$ で受理

乱択

乱数を利用した計算

例　与えられた整数係数多項式が零か判定

$$(z-x)(x+y)(yy+zz)-xxyz$$
$$+xy(z+x)(y-z)$$
$$-(x-z)(xx+xy-yz)(x+y-z)$$
$$+xyyz+(x+y)y(z-x+y)(x+y-z)$$
$$-(x-z)(xy+xz+yz)(x+y-z)$$
$$+(x-y)(x+z)(y+z)(y-z)+yyzz$$

文字式のまま全部展開して計算　➡　大変

適当に数値を代入して計算し
0 になるか調べる　➡　ラク（高速）
高確率で正解

$(x,y,z)=(1,2,3)$ とか

注意

NPとかRPとかの定義について

「多項式時間で決定的に解けるのが **P**」

定義	定義
機械が**決定的** **多項式時間限定**であるとは…	機械 M が問題 A を **計算する**とは…

➡ **P**

「多項式時間で非決定的に解けるのが **NP**」

定義	定義
機械が**非決定的** **多項式時間限定**であるとは…	機械 M が問題 A を **計算する**とは…

こうではない

➡ **NP**

「多項式時間で乱択で解けるのが **RP**」

定義	定義
機械が**乱択的** **多項式時間限定**であるとは…	機械 M が問題 A を **計算する**とは…

こうではない

➡ **RP**

補題

全次数 d の非零多項式 p について

$$\Pr[p(r_1,r_2,\ldots,r_m)\neq 0]\geq 1-\frac{d}{B}$$

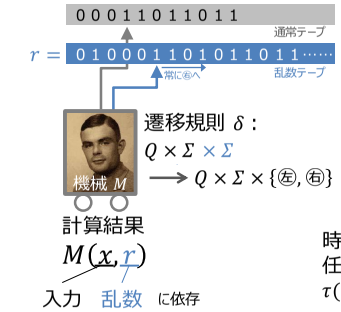
但し確率は $r_1,r_2,\ldots,r_m\in\{1,\ldots,B\}$ を無作為に取ったもの

証明

m に関する帰納法　$m>0$ とする　X_1 の次数を i として
$p(X_1,X_2,\ldots,X_m)=X_1^i\cdot q(X_2,\ldots,X_m)+(X_1$の低次の項$)$
と書く　帰納法の仮定より $\Pr[q(r_2,\ldots,r_m)\neq 0]\geq 1-\frac{d-i}{B}$
もし□ ならば $p(X_1,r_2,\ldots,r_m)$ は
X_1 に関する i 次の非零な多項式で　その根は高々 i 個　故に

$$\Pr[\square]\geq\Pr[\square]\cdot\left(1-\frac{i}{B}\right)\geq\left(1-\frac{d-i}{B}\right)\left(1-\frac{i}{B}\right)\geq 1-\frac{d}{B}$$

非決定性（＝乱択）機械



次の遷移を複数の分岐から
非決定的に（等確率で）選ぶ

＝

初めに「乱数テープ」上に
乱数列が~~無限に~~供給される
$\tau(|x|)$ ビットで十分

時間量が $\tau:\mathbf{N}\to\mathbf{N}$ とは
任意の x と**任意の r について**
$\tau(|x|)$ 時間以内で停止すること

注意

NPとかRPとかの定義について

「多項式時間で決定的に解けるのが **P**」

定義	定義
機械が **多項式時間限定**であるとは…	機械 M が問題 A を **計算する**とは…

➡ **P**

「多項式時間で非決定的に解けるのが **NP**」

定義	定義
非決定性機械が **多項式時間限定**であるとは…	機械 M が問題 A を ●●●する とは…

➡ **NP**

他にも色々
BPP
ZPP
PP
UP
#P
⋮

「多項式時間で乱択で解けるのが **RP**」

定義	定義
非決定性機械が **多項式時間限定**であるとは…	機械 M が問題 A を ▲▲▲する とは…

➡ **RP**

↑こっちは殆ど同じ　↑ここを変える

両側誤り
誤受理あり
誤拒否あり

定義

bounded probabilistic

判定問題 A が級 **BPP** に属するとは
或る多項式時間（乱択）機械 M が存在し
任意の入力 x に対し

$>\frac{1}{2}$ ではダメ

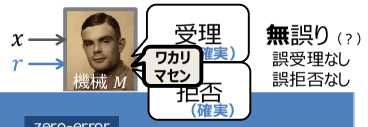
$A(x)=$ 真　のとき　$M(x,r)$ は**確率** $>\frac{2}{3}$ で受理

$A(x)=$ 偽　のとき　$M(x,r)$ は**確率** $>\frac{2}{3}$ で拒否

$\frac{2}{3}$ の代りに $\frac{99}{100}$ にしたければ…

RP ⊆ BPP
BPP = coBPP

乱数を十分な回数取って $r_1,\cdots,r_k$
$M(x,r_1),\ \cdots,\ M(x,r_k)$ の多数決で受理・拒否



定義

zero-error

判定問題 A が級 ZPP に属するとは
或る多項式時間（乱択）機械 M が存在し
任意の入力 x に対し

$A(x) =$ 真 のとき $M(x,r)$ は**必ず**受理または「？」

$A(x) =$ 偽 のとき $M(x,r)$ は**必ず**拒否または「？」

「？」の確率は常に $< \frac{1}{2}$ 繰返せば $< \frac{1}{100}$ にもできる

決着がつくまで繰返す → 時間の期待値 $\mathrm{poly}(|x|)$

定理

$\mathbf{ZPP = RP \cap coRP}$

証明

$\mathbf{ZPP \subseteq RP}$ 「？」の代りに拒否

$\mathbf{ZPP \subseteq coRP}$ 「？」の代りに受理

$\mathbf{RP \cap coRP \subseteq ZPP}$ 両方の算法を実行してみて

P = 現実に解ける

BPP = 現実に解ける (真の乱数があれば)

本当に異なるのか？

どれほど重要なのか？

0 と 1 が確率ちょうど $\frac{1}{2}$ で出る乱数であること

どうでもよい。例えば「$\frac{1}{100}$ ～ $\frac{99}{100}$ の未知の確率で 1 が出るとわかっている」乱数があれば何とかなる。

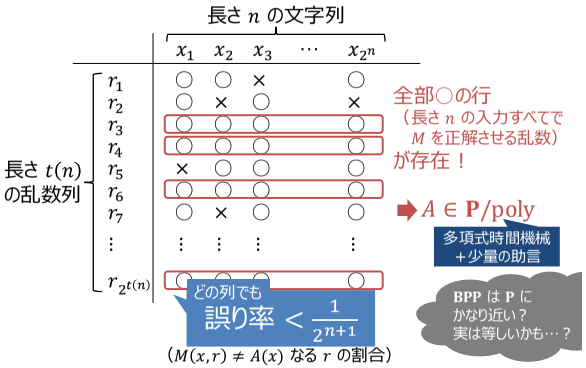
乱数の各ビットがそれなりに独立であること

或る程度は重要。
前のビットから完全に決ってしまうようでは役立たず。

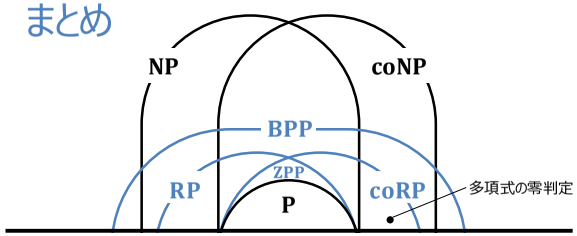
乱数の量

或る程度は重要。
$O(\log n)$ビットなら代りに決定的に全部試せる。

$A \in \mathbf{BPP}$ とすると 多項式時間機械 M が存在して



まとめ



未解決 $\mathbf{BPP} \stackrel{?}{=} \mathbf{P}$
(等しいと予想する人が多い)

終