離散数理工学 (11) 2022 年 1 月 11 日

演習問題 岡本 吉央

提出締切： 2022 年 1 月 18 日 午前 9:00

授業内問題 11.1 任意の自然数 $d \geq 1$ を考え，$S = \{0, 1, \ldots, d\}$ とする．1 変数 d 次実多項式 $p, q \in \mathbb{R}[x]$ で，

$$\Pr(p(r) = q(r)) = \frac{d}{|S|}$$

となるものを構成し，その性質を持つことを証明せよ．ただし，確率は S から一様分布に従って r を選ぶことを考えたときのものであるとする．

復習問題 11.2 自然数 $n \geq 1$ と $d \geq 0$ に対して，p を n 変数実多項式で，次数が高々 d であるものとする．(ただし，次数はすべての変数に対する次数の和として定義する．) 任意の有限集合 $S \subseteq \mathbb{R}$ を考える．このとき，S から一様分布に従って独立に n 個の実数を選び，それらを $r_1, r_2, \ldots, r_n$ とする．多項式 p が恒等的に 0 ではない，すなわち，ある $x \in \mathbb{R}^n$ に対して $p(x) \neq 0$ であるとき，

$$\Pr(p(r_1, r_2, \ldots, r_n) = 0) \leq \frac{d}{|S|}$$

が成り立つことを証明せよ．

復習問題 11.3 自然数 $n \geq 1$ と $d \geq 0$ に対して，p, q を n 変数実多項式で，次数が高々 d であるものとする．(ただし，次数はすべての変数に対する次数の和として定義する．) 多項式 p と q が同じであるか，つまり，任意の $x \in \mathbb{R}^n$ に対して $p(x) = q(x)$ が成り立つか，判定する問題を考える．演習問題 11.2 の結果を利用して，次の性質を持つ乱択アルゴリズムを設計せよ．

- p と q が同じであるとき，正しく「同じである」と必ず判定する．
- p と q が同じではないとき，正しく「同じでない」と判定する確率が $1/2$ 以上である．
- p と q をある 1 点でしか評価しない．

ただし，n と d はアルゴリズムの入力として与えられるとする．

復習問題 11.4 演習問題 11.3 の乱択アルゴリズムを考える．このアルゴリズムを K 回反復実行することで，p と q が同じではないときに，正しく「同じでない」と判定する確率を $1 - (1/2)^K$ 以上にできることを証明せよ．

復習問題 11.5 有限集合 G と G 上の二項演算 $\circ$ を考える．任意の $x, y, z \in G$ に対して

$$(x \circ y) \circ z = x \circ (y \circ z)$$

が成り立つことを確率的に判定したい．そのために，次のような方法を考える．

各要素 $a \in G$ に対して，変数 x_a を用意し，それらを変数とする，次のような多項式

$$p(\mathbf{x}) = \sum_{a \in G} \alpha_a x_a$$

を考える．ただし，任意の $a \in G$ に対して α_a は実数であるとする．そして，そのような多項式

$$p(\mathbf{x}) = \sum_{a \in G} \alpha_a x_a,$$
$$q(\mathbf{x}) = \sum_{b \in G} \beta_b x_b$$

に対して，多項式 $p \odot q$ を

$$(p \odot q)(\mathbf{x}) = \sum_{a \in G} \sum_{b \in G} \alpha_a \beta_b x_{a \circ b}$$

で定義する．

1. そのような任意の多項式 p, q, r に対して，

   $$(p \odot q) \odot r = p \odot (q \odot r)$$

   が成り立つとき，任意の $x, y, z \in G$ に対して

   $$(x \circ y) \circ z = x \circ (y \circ z)$$

   が成り立つことを証明せよ．
2. (発展問題) 任意の有限集合 $S \subseteq \mathbb{R}$ に対して，次のアルゴリズムを考える．

   ステップ 1： 任意の $a \in G$ に対して，$\alpha_a, \beta_a, \gamma_a$ を S から一様分布に従って独立に選択する．

   ステップ 2： 多項式 p, q, r を次のように定義する．

   $$p(\mathbf{x}) = \sum_{a \in G} \alpha_a x_a,$$
   $$q(\mathbf{x}) = \sum_{b \in G} \beta_b x_b,$$
   $$r(\mathbf{x}) = \sum_{c \in G} \gamma_c x_c.$$

   ステップ 3： 多項式 $(p \odot q) \odot r$ と $p \odot (q \odot r)$ を計算する．

   ステップ 4： $(p \odot q) \odot r$ と $p \odot (q \odot r)$ が恒等的に等しいとき，Yes を出力する．そうでないとき，No を出力する．

任意の $x, y, z \in G$ に対して，$(x \circ y) \circ z = x \circ (y \circ z)$ が成り立つとき，このアルゴリズムが Yes を出力することを証明せよ．(ヒント：演習問題 11.6 の結果を用いてもよい．)

3. (発展問題) ある $x, y, z \in G$ に対して，$(x \circ y) \circ z \neq x \circ (y \circ z)$ が成り立つとき，このアルゴリズムが Yes を出力する確率が $3/|S|$ 以下になることを証明せよ．(ヒント：演習問題 11.2 の結果を用いてもよい．)

補足問題 11.6 演習問題 11.5 の設定を考える．このとき，任意の $x, y, z \in G$ に対して

$$(x \circ y) \circ z = x \circ (y \circ z)$$

が成り立つならば，そこで定義したような任意の多項式 p, q, r に対して，

$$(p \odot q) \odot r = p \odot (q \odot r)$$

が成り立つことを証明せよ．

追加問題 11.7 自然数 $n \geq 1$ と $d \geq 0$ に対して，p を n 変数実多項式とする．ここで，多項式 p の次数列 $(d_1, d_2, \ldots, d_n)$ を次のように定義する．まず，d_1 を，p における x_1 の次数とし，$x_1^{d_1}$ の係数を p_1 とする．次に，d_2 を，p_1 における x_2 の次数とし，p_1 における $x_2^{d_2}$ の係数を p_2 とする．そして，d_3 を，p_2 における x_3 の次数として，...と続けていく．任意の有限集合 $S_1, S_2, \ldots, S_n \subseteq \mathbb{R}$ を考える．このとき，各 $i \in \{1, 2, \ldots, n\}$ に対して S_i から一様分布に従って実数を選び r_i とする．このとき，$r_1, r_2, \ldots, r_n$ の選択は互いに独立であるとする．多項式 p が恒等的に 0 ではない，すなわち，ある $x \in \mathbb{R}^n$ に対して $p(x) \neq 0$ であるとき，

$$\Pr(p(r_1, r_2, \ldots, r_n) = 0) \leq \sum_{i=0}^{n} \frac{d_i}{|S_i|}$$

が成り立つことを証明せよ．

追加問題 (発展) 11.8 有限集合 G と G 上の二項演算 $\circ$ が表として与えられる．任意の $s, t, u, v \in G$ に対して

$$(s \circ t) \circ (u \circ v) = ((u \circ t) \circ v) \circ s$$

が成り立つことを確率的に判定したい．次の 3 つの要求をすべて満たす乱択アルゴリズムを設計し，確かにその要求を満たすことを証明せよ．

- 計算量は $O(|G|^2)$ である
- 任意の $s, t, u, v \in G$ に対して，$(s \circ t) \circ (u \circ v) = ((u \circ t) \circ v) \circ s$ が成り立つとき，アルゴリズムは必ず正しく「Yes」と出力する．
- あるの $s, t, u, v \in G$ に対して，$(s \circ t) \circ (u \circ v) \neq ((u \circ t) \circ v) \circ s$ が成り立つとき，アルゴリズムが間違えて「Yes」と出力する確率は 1/2 以下である．