離散数理工学　第 11 回

離散確率論：乱択データ構造とアルゴリズム (発展)

岡本 吉央
okamotoy@uec.ac.jp

電気通信大学

2022 年 1 月 11 日

最終更新：2021 年 12 月 26 日　17:10

今日の目標

典型的な乱択アルゴリズムの解析ができるようになる

- 多項式の同一性判定 (シュワルツ・ジッペルの補題)
- 多項式の同一性判定の応用：結合性の判定

重要な技法

- 成功確率の増幅

乱択アルゴリズムとは？：復習

乱数を用いる (あるいは，用いてもよい) アルゴリズムのこと

確率的アルゴリズム，乱数使用アルゴリズムとも呼ばれる

乱択アルゴリズムの類型

乱択アルゴリズムは，主に次の 2 種類に分けられる

- ラスベガス型乱択アルゴリズム
  - 必ず正しい出力を行う
  - 計算量が確率的に定まる
- モンテカルロ型乱択アルゴリズム
  - 正しい出力を行う保証がない
  - 正しい出力に対する「ずれ」が確率的に定まる

目次

多項式の同一性判定 (1)

例題

x に関する次の 2 つの ($\mathbb{R}$ 上の) 多項式は「同じ」多項式か？

- $(x-2)^2-(x+4)(x-3)+(2x-1)^2$
- $4x^2-9x+17$

2 つの多項式 $p, q \in \mathbb{R}[x]$ が同じであるとは，任意の $x \in \mathbb{R}$ に対して

$$p(x) = q(x)$$

となること

多項式の同一性判定 (2)

例題

x に関する次の 2 つの ($\mathbb{R}$ 上の) 多項式は「同じ」多項式か？

- $p(x) = (x-2)^2 - (x+4)(x-3) + (2x-1)^2$
- $q(x) = 4x^2 - 9x + 17$

展開すれば，次のようになることが分かる

$$\begin{aligned} p(x) &= (x-2)^2 - (x+4)(x-3) + (2x-1)^2 \\ &= (x^2 - 4x + 4) - (x^2 + x - 12) + (4x^2 - 4x + 1) \\ &= (1 - 1 + 4)x^2 + (-4 - 1 - 4)x + (4 + 12 + 1) \\ &= 4x^2 - 9x + 17 = q(x) \end{aligned}$$

つまり，上の 2 つの多項式は同じである □

多項式の同一性判定 (3)

例題

x に関する次の 2 つの ($\mathbb{R}$ 上の) 多項式は「同じ」多項式か？

- $p(x) = (x-2)^2 - (x+4)(x-3) + (2x-1)^2$
- $q(x) = 4x^2 - 9x + 17$

$p(x), q(x)$ は x に関する (高々) 2 次式なので，3 つの異なる点で評価する

- $x = 0$ のとき，$\begin{cases} p(0) = (-2)^2 - 4 \cdot (-3) + (-1)^2 = 17 \\ q(0) = 17 \end{cases}$
- $x = 1$ のとき，$\begin{cases} p(1) = (-1)^2 - 5 \cdot (-2) + 1^2 = 12 \\ q(1) = 4 - 9 + 17 = 12 \end{cases}$
- $x = -1$ のとき，$\begin{cases} p(-1) = (-3)^2 - 3 \cdot (-4) + (-3)^2 = 30 \\ q(-1) = 4 + 9 + 17 = 30 \end{cases}$

つまり，上の 2 つの多項式は同じである □

多項式の同一性判定 (4)

「展開による方法」のよい点と悪い点

- よい点：同じか同じでないか，必ず分かる
- よい点：多変数多項式でも使える
- 悪い点：展開は大変

「評価による方法」のよい点と悪い点

- よい点：同じか同じでないか，必ず分かる
- よい点：多変数多項式でも使える
- よい点：評価は簡単
- 悪い点：多変数多項式だと，評価する点の数が多くなる

多項式の同一性判定 (5)

「評価による方法」のよい点と悪い点

- 悪い点：多変数多項式だと，評価する点の数が多くなる

例えば，

- 1 変数の多項式，次数が高々 d $\rightsquigarrow$ 評価する点の数 $= d+1$
- 2 変数の多項式，次数が高々 d $\rightsquigarrow$ 評価する点の数 $= \binom{d+2}{2}$

$$p(x,y) = a_{2,0}x^2 + a_{1,1}xy + a_{0,2}y^2 + a_{1,0}x + a_{0,1}y + a_{0,0}$$

- n 変数の多項式，次数が高々 d $\rightsquigarrow$ 評価する点の数 $= \binom{d+n}{n}$

$$n = 100,\ d = 10 \rightsquigarrow \binom{d+n}{n} = 46{,}897{,}636{,}623{,}981 \text{ (約 46 兆)}$$

多項式の同一性判定：乱択アルゴリズム

考える乱択アルゴリズム

評価する点をランダムに選ぶ

ランダムに選ぶ方法

- 評価する点の候補となる有限集合 $S \subseteq \mathbb{R}$ を決めておく
- S^n から一様分布に従って点を選ぶ
  (S から n 個の点を復元抽出によって一様に選ぶ)

多項式の同一性判定：乱択アルゴリズム — シュワルツ・ジッペルの補題

考える状況

- $n \geq 1, d \geq 0$： 自然数
- p： n 変数実多項式で，次数が高々 d であり，恒等的に 0 ではないもの (ある $x \in \mathbb{R}^n$ に対して $p(x) \neq 0$)
- $S \subseteq \mathbb{R}$： 有限集合

性質：シュワルツ・ジッペルの補題

S から一様分布に従って独立に $r_1, r_2, \ldots, r_n$ を選ぶとき

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

この補題は Schwartz ('80) と Zippel ('79) によるが，
DeMillo と Lipton ('78) も同じような命題を証明している

シュワルツ・ジッペルの補題を用いた多項式同一性判定 (1)

多項式同一性判定に対する乱択アルゴリズム

1. 適当に $S \subseteq \mathbb{R}$ を選ぶ
2. $r_1, \ldots, r_n \in S$ を一様分布に従って独立に選ぶ
3. $p(r_1, \ldots, r_n) - q(r_1, \ldots, r_n) = 0$ ならば，「同一である」と出力
   $p(r_1, \ldots, r_n) - q(r_1, \ldots, r_n) \neq 0$ ならば，「同一でない」と出力

任意の $x \in \mathbb{R}^n$ に対して $p(x) = q(x)$ であるとき，

- 任意の $r_1, \ldots, r_n \in S$ に対して，$p(r_1, \ldots, r_n) = q(r_1, \ldots, r_n)$
- $\therefore$ アルゴリズムは正しく「同一である」と必ず出力

シュワルツ・ジッペルの補題を用いた多項式同一性判定 (2)

多項式同一性判定に対する乱択アルゴリズム

1. 適当に $S \subseteq \mathbb{R}$ を選ぶ
2. $r_1, \ldots, r_n \in S$ を一様分布に従って独立に選ぶ
3. $p(r_1, \ldots, r_n) - q(r_1, \ldots, r_n) = 0$ ならば，「同一である」と出力
   $p(r_1, \ldots, r_n) - q(r_1, \ldots, r_n) \neq 0$ ならば，「同一でない」と出力

ある $x \in \mathbb{R}^n$ に対して $p(x) \neq q(x)$ であるとき，

- $p - q$ は恒等的に 0 ではない多項式
- シュワルツ・ジッペルの補題から，$p - q$ の次数が d のとき

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

- $\therefore$ 正しく「同一でない」と出力する確率 $\geq 1 - \dfrac{d}{|S|}$

多項式の同一性判定：よい点と悪い点

「乱択アルゴリズム」のよい点と悪い点

- よい点：評価は簡単
- よい点：多変数多項式でも，評価する点の数が少ない
- 悪い点：同じか同じでないか，必ず分かるわけではない

「展開による方法」のよい点と悪い点

- よい点：同じか同じでないか，必ず分かる
- 悪い点：展開は大変

「評価による方法」のよい点と悪い点

- よい点：同じか同じでないか，必ず分かる
- よい点：評価は簡単
- 悪い点：多変数多項式だと，評価する点の数が多くなる

多項式の同一性判定：よい点と悪い点 (表)

	展開	評価	評価 (乱択)
必ず分かる	○	○	×
計算が簡単	×	○	○
点の数が少ない	–	×	○

評価する点の数

$n = 100, d = 10$ のとき

- 乱択ではない $\rightsquigarrow \binom{d+n}{n}$ 約 46 兆
- 乱択 $\rightsquigarrow 1$ 1

間違える確率

- 乱択 $\rightsquigarrow$ 同じでないとき，間違える確率 $\leq \dfrac{d}{|S|}$

間違える確率を小さくするには？ (1)

アイディア 1 : $|S|$ を大きくする

- 例えば，$d = 10$ のとき
  - $|S| = 100$ ならば，$\dfrac{d}{|S|} = \dfrac{10}{100} = \dfrac{1}{10}$
  - $|S| = 200$ ならば，$\dfrac{d}{|S|} = \dfrac{10}{200} = \dfrac{1}{20}$

アイディア 2 : 同じアルゴリズムを繰り返して実行する

間違える確率を小さくするには？ (2)

乱択アルゴリズムの反復実行

K = 反覆回数

1. 先ほどの乱択アルゴリズムを K 回独立に実行する
2. 1 回でも $p(r_1, \ldots, r_n) \neq q(r_1, \ldots, r_n)$ $\Rightarrow$ 「同一でない」と出力
   そうでない $\Rightarrow$ 「同一である」と出力

ある $x \in \mathbb{R}^n$ に対して $p(x) \neq q(x)$ であるとき

- K 回とも $p(r_1, \ldots, r_n) = q(r_1, \ldots, r_n)$ となるとき，出力が間違い
- 出力が間違いである確率 $\leq \left(\dfrac{d}{|S|}\right)^K$

結論：**確率増幅**

反覆実行により，間違う確率を指数関数的に小さくできる

反覆実行は，モンテカルロ型乱択アルゴリズムにおける常套手段

目次

シュワルツ・ジッペルの補題 (再掲)

考える状況

- $n \geq 1, d \geq 0$： 自然数
- p： n 変数実多項式で，次数が高々 d であり，恒等的に 0 ではないもの (ある $x \in \mathbb{R}^n$ に対して $p(x) \neq 0$)
- $S \subseteq \mathbb{R}$： 有限集合

性質：シュワルツ・ジッペルの補題 (再掲)

S から一様分布に従って独立に $r_1, r_2, \ldots, r_n$ を選ぶとき

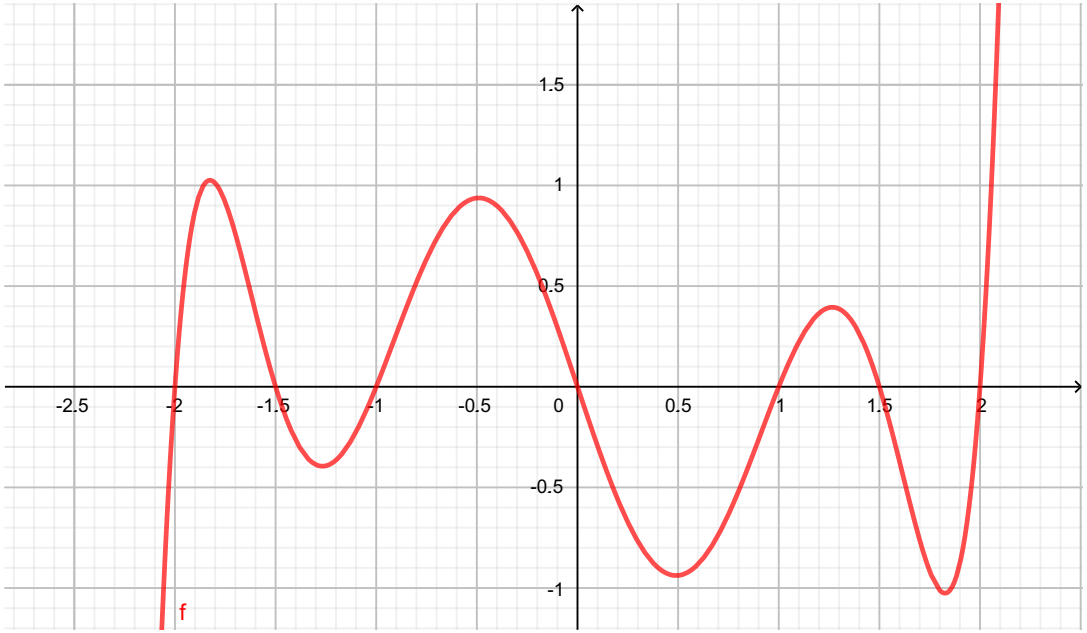
$$\Pr(p(r_1, r_2, \ldots, r_n) = 0) \leq \frac{d}{|S|}$$

証明は n に関する帰納法

シュワルツ・ジッペルの補題：証明 (1)

$n = 1$ のとき

- $p(r) = 0$ となる r の数 $\leq d$ ($\because$ p は高々 d 次多項式)
- $\therefore \Pr(p(r) = 0) \leq \dfrac{d}{|S|}$



シュワルツ・ジッペルの補題：証明 (2)

$\boxed{n = k \geq 2 \text{ のとき}}$ ($n < k$ のときは成り立つと仮定する)

- $p(x_1, x_2, \ldots, x_k)$ を次の形に書く

$$p(x_1, x_2, \ldots, x_k) = \sum_{i=0}^{d} q_i(x_1, \ldots, x_{k-1}) \cdot x_k^i$$

例：$k = 3,\ d = 2$

$$p(x_1, x_2, x_3) = \underbrace{(x_1^2 - 3x_1x_2)}_{q_0(x_1,x_2)} + \underbrace{(-2x_1 + x_2 - 4)}_{q_1(x_1,x_2)} x_3 + \underbrace{3}_{q_2(x_1,x_2)} x_3^2$$

- q_i は $n-1$ 変数多項式で，次数は高々 $d - i$
- ある i に対して，q_i は恒等的に 0 ではない

($\because p$ が恒等的に 0 ではない)

- そのような i の中で最大のものを考え，i^* とする

シュワルツ・ジッペルの補題：証明 (3)

このとき，$p(x_1, x_2, \ldots, x_k) = \sum_{i=0}^{i^*} q_i(x_1, \ldots, x_{k-1}) \cdot x_k^i$

- q_{i^*} は恒等的に 0 ではないので，帰納法の仮定から

$$\Pr(q_{i^*}(r_1, r_2, \ldots, r_{k-1}) = 0) \leq \frac{d - i^*}{|S|}$$

- $q_{i^*}(r_1, r_2, \ldots, r_{k-1}) \neq 0$ という仮定の下で，
  $p(r_1, r_2, \ldots, r_{k-1}, x_n)$ は 1 変数 i^* 次多項式
- したがって，帰納法の仮定から

$$\Pr(p(r_1, r_2, \ldots, r_{k-1}, r_k) = 0 \mid q_{i^*}(r_1, r_2, \ldots, r_{k-1}) \neq 0) \leq \frac{i^*}{|S|}$$

シュワルツ・ジッペルの補題：証明 (4)

したがって，

$$
\begin{aligned}
&\Pr(p(r_1,\ldots,r_k)=0)\\
&=\Pr(p(r_1,\ldots,r_k)=0 \mid q_{i^*}(r_1,\ldots,r_{k-1})=0)\cdot\Pr(q_{i^*}(r_1,\ldots,r_{k-1})=0)\\
&\quad+\Pr(p(r_1,\ldots,r_k)=0 \mid q_{i^*}(r_1,\ldots,r_{k-1})\neq 0)\cdot\Pr(q_{i^*}(r_1,\ldots,r_{k-1})\neq 0)\\
&\leq \Pr(q_{i^*}(r_1,\ldots,r_{k-1})=0)+\Pr(p(r_1,\ldots,r_k)=0 \mid q_{i^*}(r_1,\ldots,r_{k-1})\neq 0)\\
&\leq \frac{d-i^*}{|S|}+\frac{i^*}{|S|}\\
&=\frac{d}{|S|}
\end{aligned}
$$

□

目次

結合性を満たすか？

$G = \{e, a, b, c, d, f, g, h\}$

$\circ$	e	a	b	c	d	f	g	h
e	e	a	b	c	d	f	g	h
a	a	e	c	g	f	d	h	b
b	b	h	e	a	g	c	d	f
c	c	b	f	e	h	g	a	d
d	d	f	g	h	e	a	b	c
f	f	d	h	b	a	e	c	g
g	g	c	d	f	b	h	e	a
h	h	g	a	d	c	b	f	e

- 単位元は e
- 任意の $x \in G$ に対して，x の逆元は x

結合性を満たすか？

$G = \{e, a, b, c, d, f, g, h\}$

$\circ$	e	a	b	c	d	f	g	h
e	e	a	b	c	d	f	g	h
a	a	e	c	g	f	d	h	b
b	b	h	e	a	g	c	d	f
c	c	b	f	e	h	g	a	d
d	d	f	g	h	e	a	b	c
f	f	d	h	b	a	e	c	g
g	g	c	d	f	b	h	e	a
h	h	g	a	d	c	b	f	e

- $(a \circ b) \circ g = c \circ g = a$
- $a \circ (b \circ g) = a \circ d = f$

$\therefore (a \circ b) \circ g \neq a \circ (b \circ g)$

$\rightsquigarrow$ 結合性を満たさない

結合性の確認法：乱数を使わないアルゴリズム

有限集合 G，G 上の二項演算 $\circ$ (表で与えられる)

結合性の確認法：乱数を使わないアルゴリズム

1. すべての $x, y, z \in G$ に対して，次を確認

$$(x \circ y) \circ z \stackrel{?}{=} x \circ (y \circ z)$$

2. ある $x, y, z \in G$ に対して $(x \circ y) \circ z \neq x \circ (y \circ z) \Rightarrow$ No を出力
   すべての $x, y, z \in G$ に対して $(x \circ y) \circ z = x \circ (y \circ z) \Rightarrow$ Yes を出力

$|G| = n$ のとき，$O(n^3)$ のアルゴリズム　　(注：表の大きさ $= n^2$)

結合性の確認法：乱数を使うアルゴリズムへ向けて

有限集合 G，G 上の二項演算 $\circ$ (表で与えられる)

目標

「結合性の確認」を行う $O(n^2)$ 時間アルゴリズムを作る

これは Rajagopalan と Schulman ('00) による

特徴

- 乱数を用いたモンテカルロ型アルゴリズムを設計する
- シュワルツ・ジッペルの補題を用いる
- 反覆実行を行うことで，誤り確率をとても小さくできる

結合性を満たすか？：小さい例

$G = \{0, 1, 2\}$

$\circ$	0	1	2
0	0	1	2
1	1	0	1
2	2	1	0

$x \circ y = |x - y|$ と定義している

- $(1 \circ 1) \circ 2 = 0 \circ 2 = 2$
- $1 \circ (1 \circ 2) = 1 \circ 1 = 0$

結合性の確認法：アイディア (1)

有限集合 G，G 上の二項演算 $\circ$ (表で与えられる)

アイディア

- 次のような多項式 p を考える

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

変数は各 $a \in G$ に対する x_a，係数 α_a は (例えば) 実数

例：先ほどの小さい例に対して

$$p(x_0, x_1, x_2) = 3x_0 - 4x_1 + 2x_2$$

結合性の確認法：アイディア (2)

有限集合 G，G 上の二項演算 $\circ$ (表で与えられる)

アイディア (続き)

- そのような多項式 p, q に対して，$p \odot q$ を次のように定義する

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

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

例：$p(x_0, x_1, x_2) = 3x_0 - 4x_1 + 2x_2$, $q(x_0, x_1, x_2) = 2x_0 + x_1 - x_2$ のとき

$$\begin{aligned}
(p \odot q)(x_0, x_1, x_2) &= 3 \cdot 2x_{0\circ 0} + 3 \cdot 1x_{0\circ 1} + 3 \cdot (-1)x_{0\circ 2} \\
&\quad + (-4) \cdot 2x_{1\circ 0} + (-4) \cdot 1x_{1\circ 1} + (-4) \cdot (-1)x_{1\circ 2} \\
&\quad + 2 \cdot 2x_{2\circ 0} + 2 \cdot 1x_{2\circ 1} + 2 \cdot (-1)x_{2\circ 2} \\
&= 6x_0 + 3x_1 - 3x_2 - 6x_1 - 4x_0 + 4x_1 + 4x_2 + 2x_1 - 2x_0 \\
&= 3x_1 + x_2
\end{aligned}$$

結合性の確認法：結合性の同値性

有限集合 G，G 上の二項演算 $\circ$ (表で与えられる)

重要な性質：$\circ$ の結合性と $\odot$ の結合性

次の 2 つは同値

1. $\circ$ は結合性を持つ
2. $\odot$ は結合性を持つ，
   すなわち，任意のそのような多項式 p, q, r に対して
   $(p \odot q) \odot r = p \odot (q \odot r)$

証明：

- 「1 $\Rightarrow$ 2」は演習問題
- 「2 $\Rightarrow$ 1」を今から証明する

結合性の確認法：結合性の同値性 — 証明 (1)

2 ⇒ 1 の証明：

- p, q, r は次の形をしているとする

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

- 任意の p, q, r に対して，$(p \odot q) \odot r = p \odot (q \odot r)$ が成り立つと仮定

証明するべき目標：$\circ$ の結合性

任意の $s, t, u \in G$ に対して，$(s \circ t) \circ u = s \circ (t \circ u)$

計算すると，次のようになることが分かる

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

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

結合性の確認法：結合性の同値性 — 証明 (2)

2 ⇒ 1 の証明 (続き)：

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

- $\alpha_s = \beta_t = \gamma_u \neq 1$ かつ，他の $\alpha_a, \beta_b, \gamma_c$ がすべて 0 であるときを考えると

$$((p \odot q) \odot r)(\mathbf{x}) = x_{(s\circ t)\circ u},$$
$$(p \odot (q \odot r))(\mathbf{x}) = x_{s\circ(t\circ u)}$$

- 仮定 $(p \odot q) \odot r = p \odot (q \odot r)$ より，$(s \circ t) \circ u = s \circ (t \circ u)$ □

結合性の確認法：アイディア (3)

有限集合 G，G 上の二項演算 $\circ$ (表で与えられる)

結合性の確認法：アイディア

$\circ$ の結合性の確認	$\Rightarrow$	$\odot$ の結合性の確認
計算量が大きい		計算量を小さくできる
		(なぜ？)

$\rightsquigarrow$ シュワルツ・ジッペルの補題を用いる

結合性の確認法：アルゴリズム

有限集合 $S \subseteq \mathbb{R}$

結合性の確認法：アルゴリズム

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選ぶ
2. p, q, r を次のように定義する

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

3. $(p \odot q) \odot r$ と $p \odot (q \odot r)$ を計算する
4. $(p \odot q) \odot r \equiv p \odot (q \odot r) \Rightarrow$ Yes を出力
   $(p \odot q) \odot r \not\equiv p \odot (q \odot r) \Rightarrow$ No を出力

注：$p \odot q$ の計算にかかる時間 $= O(n^2)$ $(n = |G|)$

結合性の確認法：アルゴリズム

有限集合 $S \subseteq \mathbb{R}$

結合性の確認法：アルゴリズム

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選ぶ
2. p, q, r を次のように定義する

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

3. $(p \odot q) \odot r$ と $p \odot (q \odot r)$ を計算する
4. $(p \odot q) \odot r \equiv p \odot (q \odot r) \Rightarrow$ Yes を出力
   $(p \odot q) \odot r \not\equiv p \odot (q \odot r) \Rightarrow$ No を出力

注：$p \odot q$ の計算にかかる時間 $= O(n^2)$ $(n = |G|)$
$\therefore$ 全体の計算時間 $= O(n^2)$

結合性の確認法：アルゴリズム — 正当性 (1)

有限集合 $S \subseteq \mathbb{R}$

結合性の確認法：アルゴリズム

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選ぶ
2. p, q, r を次のように定義する

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

3. $(p \odot q) \odot r$ と $p \odot (q \odot r)$ を計算する
4. $(p \odot q) \odot r \equiv p \odot (q \odot r) \Rightarrow$ Yes を出力
   $(p \odot q) \odot r \not\equiv p \odot (q \odot r) \Rightarrow$ No を出力

- $\circ$ が結合性を持つ $\Rightarrow$ $\odot$ も結合性を持つ (前述の性質)
  $\Rightarrow$ アルゴリズムは必ず Yes を出力
  $\therefore$ アルゴリズムの出力は必ず正しい

結合性の確認法：アルゴリズム — 正当性 (2)

有限集合 $S \subseteq \mathbb{R}$

結合性の確認法：アルゴリズム

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選ぶ
2. p, q, r を次のように定義する

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

3. $(p \odot q) \odot r$ と $p \odot (q \odot r)$ を計算する
4. $(p \odot q) \odot r \equiv p \odot (q \odot r) \Rightarrow$ Yes を出力
   $(p \odot q) \odot r \not\equiv p \odot (q \odot r) \Rightarrow$ No を出力

- $\circ$ が結合性を持たない $\Rightarrow$ $\odot$ も結合性を持たない (前述の性質)
  $\Rightarrow$ アルゴリズムの作る特定の p, q, r が
  $(p \odot q) \odot r \not\equiv p \odot (q \odot r)$ を満たすか分からない
  $\therefore$ アルゴリズムの出力は正しくないかもしれない

結合性の確認法：シュワルツ・ジッペルの補題の利用 (1)

- $\circ$ が結合性を持たないと仮定
  - ある $s, t, u \in G$ に対して，$(s \circ t) \circ u \neq s \circ (t \circ u)$
  - このとき，$\alpha_s, \beta_t, \gamma_u$ が最後に選ばれるとして，
    それまでに選ばれた $\alpha_a, \beta_b, \gamma_c$ は既に定められているとする

例

$\circ$	0	1	2
0	0	1	2
1	1	0	1
2	2	1	0

$s = 1, t = 1, u = 2$

- $(1 \circ 1) \circ 2 = 2$
- $1 \circ (1 \circ 2) = 0$

$\alpha_1, \beta_1, \gamma_2$ 以外は既に選択済み

$$\alpha_0 = 3, \quad \alpha_1 = ???, \quad \alpha_2 = 1,$$
$$\beta_0 = 2, \quad \beta_1 = ???, \quad \beta_2 = -1,$$
$$\gamma_0 = -2, \quad \gamma_1 = 1, \quad \gamma_2 = ???$$

結合性の確認法：シュワルツ・ジッペルの補題の利用 (2)

$\circ$	0	1	2
0	0	1	2
1	1	0	1
2	2	1	0

$\alpha_1, \beta_1, \gamma_2$ 以外は既に選択済み

$$\alpha_0 = 3, \quad \alpha_1 = ???, \quad \alpha_2 = 1,$$
$$\beta_0 = 2, \quad \beta_1 = ???, \quad \beta_2 = -1,$$
$$\gamma_0 = -2, \quad \gamma_1 = 1, \quad \gamma_2 = ???$$

$s = 1, t = 1, u = 2$

- $(1 \circ 1) \circ 2 = 2$
- $1 \circ (1 \circ 2) = 0$

$$\begin{aligned}(p \odot q)(\mathbf{x}) &= 3 \cdot 2x_{0\circ 0} + 3 \cdot \beta_1 x_{0\circ 1} + 3 \cdot (-1)x_{0\circ 2} \\ &\quad + \alpha_1 \cdot 2x_{1\circ 0} + \alpha_1 \cdot \beta_1 x_{1\circ 1} + \alpha_1 \cdot (-1)x_{1\circ 2} \\ &\quad + 1 \cdot 2x_{2\circ 0} + 1 \cdot \beta_1 x_{2\circ 1} + 1 \cdot (-1)x_{2\circ 2} \\ &= (5 + \alpha_1\beta_1)x_0 + (\alpha_1 + 4\beta_1)x_1 - x_2\end{aligned}$$

結合性の確認法：シュワルツ・ジッペルの補題の利用 (3)

$\circ$	0	1	2
0	0	1	2
1	1	0	1
2	2	1	0

$\alpha_1, \beta_1, \gamma_2$ 以外は既に選択済み

$$\alpha_0 = 3, \quad \alpha_1 = ???, \quad \alpha_2 = 1,$$
$$\beta_0 = 2, \quad \beta_1 = ???, \quad \beta_2 = -1,$$
$$\gamma_0 = -2, \quad \gamma_1 = 1, \quad \gamma_2 = ???$$

$s = 1, t = 1, u = 2$

- $(1 \circ 1) \circ 2 = 2$
- $1 \circ (1 \circ 2) = 0$

$$(p \odot q)(\mathbf{x}) = (5 + \alpha_1\beta_1)x_0 + (\alpha_1 + 4\beta_1)x_1 - x_2$$

$$\begin{aligned}((p \odot q) \odot r)(\mathbf{x}) &= (5 + \alpha_1\beta_1) \cdot (-2)x_{0\circ 0} + (5 + \alpha_1\beta_1) \cdot 1x_{0\circ 1} + (5 + \alpha_1\beta_1) \cdot \gamma_2 x_{0\circ 2} \\ &\quad + (\alpha_1 + 4\beta_1) \cdot (-2)x_{1\circ 0} + (\alpha_1 + 4\beta_1) \cdot 1x_{1\circ 1} + (\alpha_1 + 4\beta_1) \cdot \gamma_2 x_{1\circ 2} \\ &\quad + (-1) \cdot (-2)x_{2\circ 0} + (-1) \cdot 1x_{2\circ 1} + (-1) \cdot \gamma_2 x_{2\circ 2} \\ &= (-10 - 2\alpha_1\beta_1 + \alpha_1 + 4\beta_1 - \gamma_2)x_0 \\ &\quad + (5 + \alpha_1\beta_1 - 2\alpha_1 - 8\beta_1 + \alpha_1\gamma_2 + 4\beta_1\gamma_2 - 1)x_1 \\ &\quad + (5\gamma_2 + \alpha_1\beta_1\gamma_2 + 2)x_2\end{aligned}$$

結合性の確認法：シュワルツ・ジッペルの補題の利用 (3)

$\circ$	0	1	2
0	0	1	2
1	1	0	1
2	2	1	0

$\alpha_1, \beta_1, \gamma_2$ 以外は既に選択済み

$$\alpha_0 = 3, \quad \alpha_1 = ???, \quad \alpha_2 = 1,$$
$$\beta_0 = 2, \quad \beta_1 = ???, \quad \beta_2 = -1,$$
$$\gamma_0 = -2, \quad \gamma_1 = 1, \quad \gamma_2 = ???$$

$s = 1, t = 1, u = 2$

- $(1 \circ 1) \circ 2 = 2$
- $1 \circ (1 \circ 2) = 0$

$$(p \odot q)(\mathbf{x}) = (5 + \alpha_1\beta_1)x_0 + (\alpha_1 + 4\beta_1)x_1 - x_2$$

$$\begin{aligned}((p \odot q) \odot r)(\mathbf{x}) &= (5 + \alpha_1\beta_1) \cdot (-2)x_{0\circ0} + (5 + \alpha_1\beta_1) \cdot 1x_{0\circ1} + (5 + \alpha_1\beta_1) \cdot \gamma_2 x_{0\circ2} \\ &\quad + (\alpha_1 + 4\beta_1) \cdot (-2)x_{1\circ0} + (\alpha_1 + 4\beta_1) \cdot 1x_{1\circ1} + (\alpha_1 + 4\beta_1) \cdot \gamma_2 x_{1\circ2} \\ &\quad + (-1) \cdot (-2)x_{2\circ0} + (-1) \cdot 1x_{2\circ1} + (-1) \cdot \gamma_2 x_{2\circ2} \\ &= (-10 - 2\alpha_1\beta_1 + \alpha_1 + 4\beta_1 - \gamma_2)x_0 \\ &\quad + (5 + \alpha_1\beta_1 - 2\alpha_1 - 8\beta_1 + \alpha_1\gamma_2 + 4\beta_1\gamma_2 - 1)x_1 \\ &\quad + (5\gamma_2 + \alpha_1\beta_1\gamma_2 + 2)x_2\end{aligned}$$

結合性の確認法：シュワルツ・ジッペルの補題の利用 (4)

$\circ$	0	1	2
0	0	1	2
1	1	0	1
2	2	1	0

$\alpha_1, \beta_1, \gamma_2$ 以外は既に選択済み

$$\alpha_0 = 3, \quad \alpha_1 = ???, \quad \alpha_2 = 1,$$
$$\beta_0 = 2, \quad \beta_1 = ???, \quad \beta_2 = -1,$$
$$\gamma_0 = -2, \quad \gamma_1 = 1, \quad \gamma_2 = ???$$

$s = 1, t = 1, u = 2$

- $(1 \circ 1) \circ 2 = 2$
- $1 \circ (1 \circ 2) = 0$

$$\begin{aligned}(q \odot r)(\mathbf{x}) &= 2 \cdot (-2)x_{0\circ 0} + 2 \cdot 1x_{0\circ 1} + 2 \cdot \gamma_2 x_{0\circ 2} \\ &\quad + \beta_1 \cdot (-2)x_{1\circ 0} + \beta_1 \cdot 1x_{1\circ 1} + \beta_1 \cdot \gamma_2 x_{1\circ 2} \\ &\quad + (-1) \cdot (-2)x_{2\circ 0} + (-1) \cdot 1x_{2\circ 1} + (-1) \cdot \gamma_2 x_{2\circ 2} \\ &= (-4 + \beta_1 - \gamma_2)x_0 + (1 - 2\beta_1 + \beta_1\gamma_2)x_1 + (2\gamma_2 + 2)x_2\end{aligned}$$

結合性の確認法：シュワルツ・ジッペルの補題の利用 (5)

$\circ$	0	1	2
0	0	1	2
1	1	0	1
2	2	1	0

$\alpha_1, \beta_1, \gamma_2$ 以外は既に選択済み

$$\alpha_0 = 3, \quad \alpha_1 = ???, \quad \alpha_2 = 1,$$
$$\beta_0 = 2, \quad \beta_1 = ???, \quad \beta_2 = -1,$$
$$\gamma_0 = -2, \quad \gamma_1 = 1, \quad \gamma_2 = ???$$

$s = 1, t = 1, u = 2$

- $(1 \circ 1) \circ 2 = 2$
- $1 \circ (1 \circ 2) = 0$

$$(q \odot r)(\mathbf{x}) = (-4 + \beta_1 - \gamma_2)x_0 + (1 - 2\beta_1 + \beta_1\gamma_2)x_1 + (2\gamma_2 + 2)x_2$$

$$\begin{aligned}(p \odot (q \odot r))(\mathbf{x}) &= 3 \cdot (-4 + \beta_1 - \gamma_2)x_{0\circ 0} + 3 \cdot (1 - 2\beta_1 + \beta_1\gamma_2)x_{0\circ 1} + 3 \cdot (2\gamma_2 + 2)x_{0\circ 2} \\ &\quad + \alpha_1 \cdot (-4 + \beta_1 - \gamma_2)x_{1\circ 0} + \alpha_1 \cdot (1 - 2\beta_1 + \beta_1\gamma_2)x_{1\circ 1} + \alpha_1 \cdot (2\gamma_2 + 2)x_{1\circ 2} \\ &\quad + 1 \cdot (-4 + \beta_1 - \gamma_2)x_{2\circ 0} + 1 \cdot (1 - 2\beta_1 + \beta_1\gamma_2)x_{2\circ 1} + 1 \cdot (2\gamma_2 + 2)x_{2\circ 2} \\ &= (-10 + 3\beta_1 - \gamma_2 + \alpha_1 - 2\alpha_1\beta_1 + \alpha_1\beta_1\gamma_2)x_0 \\ &\quad + (4 - 8\beta_1 + 4\beta_1\gamma_2 - 2\alpha_1 + \alpha_1\beta_1 + \alpha_1\gamma_2)x_1 + (5\gamma_2 + 2 + \beta_1)x_2\end{aligned}$$

結合性の確認法：シュワルツ・ジッペルの補題の利用 (5)

$\circ$	0	1	2
0	0	1	2
1	1	0	1
2	2	1	0

$\alpha_1, \beta_1, \gamma_2$ 以外は既に選択済み

$$\alpha_0 = 3, \quad \alpha_1 = ???, \quad \alpha_2 = 1,$$
$$\beta_0 = 2, \quad \beta_1 = ???, \quad \beta_2 = -1,$$
$$\gamma_0 = -2, \quad \gamma_1 = 1, \quad \gamma_2 = ???$$

$s = 1, t = 1, u = 2$

- $(1 \circ 1) \circ 2 = 2$
- $1 \circ (1 \circ 2) = 0$

$$(q \odot r)(\mathbf{x}) = (-4 + \beta_1 - \gamma_2)x_0 + (1 - 2\beta_1 + \beta_1\gamma_2)x_1 + (2\gamma_2 + 2)x_2$$

$$\begin{aligned}(p \odot (q \odot r))(\mathbf{x}) &= 3 \cdot (-4 + \beta_1 - \gamma_2)x_{0\circ 0} + 3 \cdot (1 - 2\beta_1 + \beta_1\gamma_2)x_{0\circ 1} + 3 \cdot (2\gamma_2 + 2)x_{0\circ 2} \\ &\quad + \alpha_1 \cdot (-4 + \beta_1 - \gamma_2)x_{1\circ 0} + \alpha_1 \cdot (1 - 2\beta_1 + \beta_1\gamma_2)x_{1\circ 1} + \alpha_1 \cdot (2\gamma_2 + 2)x_{1\circ 2} \\ &\quad + 1 \cdot (-4 + \beta_1 - \gamma_2)x_{2\circ 0} + 1 \cdot (1 - 2\beta_1 + \beta_1\gamma_2)x_{2\circ 1} + 1 \cdot (2\gamma_2 + 2)x_{2\circ 2} \\ &= (-10 + 3\beta_1 - \gamma_2 + \alpha_1 - 2\alpha_1\beta_1 + \alpha_1\beta_1\gamma_2)x_0 \\ &\quad + (4 - 8\beta_1 + 4\beta_1\gamma_2 - 2\alpha_1 + \alpha_1\beta_1 + \alpha_1\gamma_2)x_1 + (5\gamma_2 + 2 + \beta_1)x_2\end{aligned}$$

結合性の確認法：シュワルツ・ジッペルの補題の利用 (6)

- このとき，$((p \odot q) \odot r)(\mathbf{x})$ と $(p \odot (q \odot r))(\mathbf{x})$ における項 $x_{(s \circ t) \circ u}$ の係数は $\alpha_s, \beta_t, \gamma_u$ に関する (高々) 3 次式
- 次のように $\alpha_s, \beta_t, \gamma_u$ に関する多項式 f, g を定義する

$$f(\alpha_s, \beta_t, \gamma_u) = ((p \odot q) \odot r)(\mathbf{x}) \text{ における項 } x_{(s \circ t) \circ u} \text{ の係数}$$
$$g(\alpha_s, \beta_t, \gamma_u) = (p \odot (q \odot r))(\mathbf{x}) \text{ における項 } x_{(s \circ t) \circ u} \text{ の係数}$$

先ほどの例では，

$$f(\alpha_1, \beta_1, \gamma_2) = 5\gamma_2 + \alpha_1\beta_1\gamma_2 + 2,$$
$$g(\alpha_1, \beta_1, \gamma_2) = 5\gamma_2 + 2 + \beta_1$$

結合性の確認法：シュワルツ・ジッペルの補題の利用 (6)

- このとき，$((p \odot q) \odot r)(\mathbf{x})$ と $(p \odot (q \odot r))(\mathbf{x})$ における項 $x_{(s \circ t) \circ u}$ の係数は $\alpha_s, \beta_t, \gamma_u$ に関する (高々) 3 次式
- 次のように $\alpha_s, \beta_t, \gamma_u$ に関する多項式 f, g を定義する

$$f(\alpha_s, \beta_t, \gamma_u) = ((p \odot q) \odot r)(\mathbf{x}) \text{ における項 } x_{(s \circ t) \circ u} \text{ の係数}$$
$$g(\alpha_s, \beta_t, \gamma_u) = (p \odot (q \odot r))(\mathbf{x}) \text{ における項 } x_{(s \circ t) \circ u} \text{ の係数}$$

先ほどの例では，

$$f(\alpha_1, \beta_1, \gamma_2) = 5\gamma_2 + \alpha_1\beta_1\gamma_2 + 2,$$
$$g(\alpha_1, \beta_1, \gamma_2) = 5\gamma_2 + 2 + \beta_1$$

結合性の確認法：シュワルツ・ジッペルの補題の利用 (7)

- $(s \circ t) \circ u \neq s \circ (t \circ u)$ なので，多項式として，$f \neq g$　　(なぜ？)
- シュワルツ・ジッペルの補題より，
  $\alpha_s, \beta_t, \gamma_u$ を S から一様分布に従って選ぶとき，

$$\Pr(f(\alpha_s, \beta_t, \gamma_u) = g(\alpha_s, \beta_t, \gamma_u)) \leq \frac{3}{|S|}$$

- すなわち，アルゴリズムが誤って Yes を出力する確率は $\frac{3}{|S|}$ 以下

性質：シュワルツ・ジッペルの補題

S から一様分布に従って独立に $r_1, r_2, \ldots, r_n$ を選ぶとき

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

結合性の確認法：アルゴリズム — 正当性 (3)

有限集合 $S \subseteq \mathbb{R}$

結合性の確認法：アルゴリズム

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選ぶ
2. p, q, r を次のように定義する

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

3. $(p \odot q) \odot r$ と $p \odot (q \odot r)$ を計算する
4. $(p \odot q) \odot r \equiv p \odot (q \odot r) \Rightarrow$ Yes を出力
   $(p \odot q) \odot r \not\equiv p \odot (q \odot r) \Rightarrow$ No を出力

- が結合性を持たない $\Rightarrow \Pr(\text{No を出力}) \geq 1 - \dfrac{3}{|S|}$

この例で実験：結合性を満たさない

$G = \{e, a, b, c, d, f, g, h\}$

$\circ$	e	a	b	c	d	f	g	h
e	e	a	b	c	d	f	g	h
a	a	e	c	g	f	d	h	b
b	b	h	e	a	g	c	d	f
c	c	b	f	e	h	g	a	d
d	d	f	g	h	e	a	b	c
f	f	d	h	b	a	e	c	g
g	g	c	d	f	b	h	e	a
h	h	g	a	d	c	b	f	e

$|S|$ を変えて，アルゴリズムの成功確率を実験で確かめる

この例で実験

各 $|S|$ に対して 100 回計測

$\lvert S\rvert$	正しく No を出力した回数	実行時間 [s]
2	55/100	0.07895
3	87/100	0.08095
4	96/100	0.07396
5	97/100	0.06896
6	98/100	0.06398
7	100/100	0.06796
8	99/100	0.06597
9	98/100	0.06996

- $|G| = 8$, $|\{(a, b, c) \in G^3 \mid (a \circ b) \circ c \neq a \circ (b \circ c)\}| = 96$
- $\therefore \dfrac{1017}{8^3} \approx 0.1875$
- 単純な $O(|G|^3)$ 時間アルゴリズムの計測：0.002998 [s]

注：時間計測は真面目にやっていないので，あまり信用できない

別の例で実験

各 $|S|$ に対して 100 回計測

$\lvert S\rvert$	正しく No を出力した回数	実行時間 [s]
2	77/100	86.19
3	89/100	78.32
4	89/100	88.47
5	93/100	94.14
6	97/100	73.33
7	98/100	82.59
8	99/100	73.89
9	98/100	75.83

- $|G| = 256$, $|\{(a, b, c) \in G^3 \mid (a \circ b) \circ c \neq a \circ (b \circ c)\}| = 1017$
- $\therefore \dfrac{1017}{256^3} \approx 0.00006$
- 単純な $O(|G|^3)$ 時間アルゴリズムの計測：116.7 [s]

注：時間計測は真面目にやっていないので，あまり信用できない

目次

今日のまとめ

今日のまとめ

典型的な乱択アルゴリズムの解析ができるようになる

- 多項式の同一性判定 (シュワルツ・ジッペルの補題)
- 多項式の同一性判定の応用：結合性の判定

重要な技法

- 成功確率の増幅

シュワルツ・ジッペルの補題 は応用をとても多く持ち，極めて有用

目次