乱択アルゴリズム

山本真基

概 要

乱択アルゴリズムの基礎を学習する.「通常の」アルゴリズムの実行過程は，それぞれの実行段階で次に実行する手順が一意に定められている．これに対して，次の手順を乱数を使って決定して進んでいくアルゴリズムが,「乱択アルゴリズム（randomized algorithm）」である．ここでは，以下の目次にあるような乱択アルゴリズムを学習する．

目 次

以降で使われる表記

- $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ をそれぞれ，自然数，整数，有理数，実数の集合とする．($\mathbb{Q}^+, \mathbb{R}^+$ をそれぞれ，正の有理数，正の実数，の集合とする．) また，$\mathbb{N}_0 = \mathbb{N} \cup \{0\}$，$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ とする．更に，任意の $n \in \mathbb{N}$ について，$[n] = \{1, 2, \ldots, n\}$ とする．
- $f(n) = O(g(n))$ とは，$\exists c, \exists n_0, \forall n \geq n_0 [f(n) \leq cg(n)]$ を満たすことである．また，$f(n) = \Omega(g(n))$ とは，$\exists c, \exists n_0, \forall n \geq n_0 [f(n) \geq cg(n)]$ を満たすことである．
- 対数関数 log, ln について，底が 2 であるとき log，底が e であるとき ln，と表記する．(よって，任意の $x \in \mathbb{R}^+$ について $2^{\log x} = x$, $\mathrm{e}^{\ln x} = x$.)

1　乱択アルゴリズムとは

アルゴリズムの実行過程は，機械的な手順の列とみなすことができる．通常のアルゴリズムでは，それぞれの実行段階で次に実行する手順が一意に定められている．「乱択アルゴリズム」（randomized algorithm）とは，（決められた実行段階で）次の手順を乱数を使って決定して進んでいくアルゴリズムである．

1.1　乱択アルゴリズムの例

以下の探索問題を考える．

探索問題（searching）

- 入力：自然数 $x \in \mathbb{N}$ と自然数の列 $a_1, a_2, \ldots, a_n \in \mathbb{N}$
- 質問：x が $a_1, a_2, \ldots, a_n$ に存在するか？

以降，（議論の単純化のため）$a_1, \ldots, a_n$ はすべて「異なる」自然数とする．この問題に対して，以下の線形探索アルゴリズムを考える．

`linear_search`$(x, (a_1, \ldots, a_n))$

1. それぞれの $i \in [n]$ について以下を繰り返す．
   - $a_i = x$ であれば `YES` を出力して終了する．
2. `NO` を出力して終了する．

図 1: 線形探索アルゴリズム

事実 1.1. 入力を $(x, (a_1, \ldots, a_n))$ とする．$x \in \{a_1, \ldots, a_n\}$ であるとき，図 1 のアルゴリズムのステップ 1 において，二つの自然数の比較回数の**最悪は** n である．（$x \in \{a_1, \ldots, a_n\}$ でないときは，**ちょうど** n である．）

注 1.1. $x \in \{a_1, \ldots, a_n\}$ であるとき，（$a_1, \ldots, a_n$ はすべて異なるとしているため）唯一（$!\exists x[x \in \{a_1, \ldots, a_n\}]$）である．

問 1.1. 入力を $(x, (a_1, \ldots, a_n))$ とする．$x \in \{a_1, \ldots, a_n\}$ であるとき，どのような場合に比較回数が（ちょうど）n となるか，具体的な入力例を示しなさい．

探索問題に対して，まず，以下の乱択アルゴリズム `rand_search1` を考える．（これがラスベガスタイプの乱択アルゴリズムの単純な例となる．詳細は次小節を参照．）

定理 1.1. 入力を $(x, (a_1, \ldots, a_n))$ とする．$x \in \{a_1, \ldots, a_n\}$ であるとき，図 2 のアルゴリズムのステップ 1-(b) において，二つの自然数の比較回数の**平均は** $(n+1)/2$ である．（$x \in \{a_1, \ldots, a_n\}$ でないときは，**ちょうど** n である．）

`rand_search1`$(x, (a_1, \ldots, a_n))$　// $S = \{a_1, \ldots, a_n\}$ とする

1. $S \neq \emptyset$ である限り以下を繰り返す.
   (a) S から一様ランダムに要素 $a \in S$ を取り出し $S = S \setminus \{a\}$ とする.
   (b) $a = x$ であれば `YES` を出力して終了する.
2. `NO` を出力する.

図 2: 探索問題を解く乱択アルゴリズム 1

証明. 比較回数が $i \in [n]$ となる確率 p_i は,

$$p_i \;=\; \frac{n-1}{n} \cdot \frac{n-2}{n-1} \cdot \;\cdots\; \cdot \frac{n-(i-1)}{n-(i-2)} \cdot \frac{1}{n-(i-1)} \;=\; \frac{1}{n}.$$

よって，比較回数の平均（期待値）は,

$$\sum_{i \in [n]} i \cdot p_i \;=\; \sum_{i \in [n]} i \cdot \frac{1}{n} \;=\; \frac{1}{n} \sum_{i \in [n]} i \;=\; \frac{1}{n} \cdot \frac{(n+1)n}{2} \;=\; \frac{n+1}{2}.$$

■

確率変数 X の期待値を $\mathrm{E}[X]$ と表記する.（詳細は次節を参照.）

系 1.2. 図 2 のアルゴリズムを A とする．入力を $(1, (a_1, \ldots, a_n))$ とする．ただし，$\{a_1, \ldots, a_n\} = [n]$．二つの自然数の比較回数を C_A とする．このとき, (a を乱択として)

$$\mathop{\mathrm{E}}_{a}[C_A] \;=\; \frac{n+1}{2}.$$

事実 1.3. 図 1 の線形探索アルゴリズムを A_0 とする．入力を $(1, (a_1, \ldots, a_n))$ とする．ただし，$\{a_1, \ldots, a_n\} = [n]$．二つの自然数の比較回数を C_0 とする．このとき, ($a_1, \ldots, a_n$ の並びを乱択として)

$$\mathop{\mathrm{E}}_{a_1, \ldots, a_n}[C_0] \;=\; \frac{n+1}{2} \quad \left(= \mathop{\mathrm{E}}_{a}[C_A]\right).$$

問 1.2. $a_1, \ldots, a_n$ の並びを乱択（$[n]$ の順列上の一様分布）とした場合，上の等式（$\mathrm{E}_{a_1, \ldots, a_n}[C_0] = (n+1)/2$）を示しなさい.

注 1.2 (ラスベガスアルゴリズム)**.** 上の系と事実から，比較回数の「平均」は，乱択アルゴリズム A と通常の線形探索 A_0 とで等しくなる.（A の乱択は a の選び方，A_0 の乱択は入力 $(a_1, \ldots, a_n)$ にある.）乱択アルゴリズムの目的の一つは，全入力例題[1]の最悪時の「平均」計算時間を良くすることである.（通常の線形探索の最悪時のおよそ半分となる.）

[1] この場合は $x \in \{a_1, \ldots, a_n\}$ に限定している.

注 1.3. 線形探索の $\mathrm{E}[C_0]$ を求めたように，アルゴリズムの全入力例題上の平均計算時間を理論的に解析する（未開な）研究分野もある．

次に，以下の乱択アルゴリズム `rand_search2` を考える．（これがモンテカルロタイプの乱択アルゴリズムの単純な例となる．詳細は次小節を参照．）

`rand_search2`$(x, (a_1, \ldots, a_n))$ // $S = \{a_1, \ldots, a_n\}$ とする

1. $|S| \geq n/2$ である限り以下を繰り返す．
   (a) S から一様ランダムに要素 $a \in S$ を取り出し $S = S \setminus \{a\}$ とする．
   (b) $a = x$ であれば `YES` を出力して終了する．
2. `NO` を出力する．

図 3: 探索問題を解く乱択アルゴリズム 2

事象 E のおきる確率を $\Pr\{E\}$ と表記する．（詳細は次節を参照．）

定理 1.2. 図 3 のアルゴリズムを A とする．入力を $(x, (a_1, \ldots, a_n))$ とする．このとき，

$$\begin{aligned} x \in \{a_1, \ldots, a_n\} &: \Pr\{A(x, (a_1, \ldots, a_n)) = \texttt{YES}\} > 1/2, \\ x \notin \{a_1, \ldots, a_n\} &: \Pr\{A(x, (a_1, \ldots, a_n)) = \texttt{NO}\} = 1. \end{aligned}$$

注 1.4. この定理は，$a_1, \ldots, a_n$ がすべて異なる，という仮定を設けなくても成り立つ．

証明. $x \notin \{a_1, \ldots, a_n\}$ の場合，アルゴリズムより A が `NO` を出力する確率は 1 である．$x \in \{a_1, \ldots, a_n\}$ の場合を考える．このとき，x が唯一である場合を考えればよい．

問 1.3. 唯一である場合を考えればよい理由を説明しなさい．

ステップ 1 が k 回実行されたとする．このとき，($|S| = n - k$ より) $n - k < n/2$ となる．ステップ 1 で $a = x$ となる $a \in S$ が取り出されない確率を p_k とする．つまり，ステップ 1-(a) で一様ランダムに取り出した $a \in S$ を s_i とすれば，

$$p_k \stackrel{\text{def}}{=} \Pr_a\{\forall i \in [k][s_i \neq x]\}.$$

このとき，

$$p_k = \frac{n-1}{n} \cdot \frac{n-2}{n-1} \cdot \cdots \cdot \frac{n-k}{n-k+1} = \frac{n-k}{n}.$$

よって，

$$\Pr\{A(x, (a_1, \ldots, a_n)) = \texttt{YES}\} = 1 - p_k > \frac{1}{2}.$$

問 1.4. 不等式 $1 - p_k > 1/2$ を示しなさい．

■

注 1.5 (モンテカルロアルゴリズム)**.** アルゴリズム A の比較回数は（高々）$n/2$ である．乱択アルゴリズムの別の目的の一つとして,「誤り確率」が生じることを犠牲にして，全入力例題の最悪時の計算時間を良くすることである.（通常の線形探索の最悪時のおよそ半分となる.）

1.2 乱択アルゴリズムのタイプ

定義 1.1

乱択アルゴリズム A が**ラスベガスアルゴリズム**であるとは，任意の入力 $x \in \Sigma^*$ に対して，$A(x)$ が正しい解であることである.

注 1.6. ラスベガスアルゴリズムは,（最悪時の）計算時間の期待値（平均計算時間）が解析の中心となる.

定義 1.2

乱択アルゴリズム A が**モンテカルロアルゴリズム**であるとは，任意の入力 $x \in \Sigma^*$ に対して，$A(x)$ が正しい解である確率が保証されることである.

注 1.7. モンテカルロアルゴリズムは,（最悪時の）正しい解を出力する確率が解析の中心となる.

命題 1.4. 図 2 のアルゴリズムはラスベガスアルゴリズムである.

注 1.8. この他に，整列問題を解く乱択クイックソートが代表的なラスベガスアルゴリズムである.（第 3 節参照.）

命題 1.5. 図 3 のアルゴリズムはモンテカルロアルゴリズムである.

注 1.9. この他に，素数性判定問題を解くソロベイ・シュトラッセンテスト（第 4 節），充足可能性問題を解くローカルサーチ（第 6 節），バックトラック（第 6 節），が代表的なモンテカルロアルゴリズムである.

2　離散確率の基礎

定義 2.1

集合 $\mathbb{U}$ を**標本空間**としたとき，$\mathbb{U}$ の部分集合を**事象**という．

以降では，標本空間は有限または可算無限とする．

定義 2.2

$\mathbb{U}$ を標本空間としたとき，**確率関数**を表す記号を $\Pr : 2^{\mathbb{U}} \to [0,1]$ とする．ある事象 $E \subseteq \mathbb{U}$ のおきる確率が $p \in [0,1]$ であることを，$\Pr\{E\} = p$ と表す．

ここでは,「確率空間」の厳密な定義は省略する．

コイン投げ

「偏りのない」（つまり，表と裏が出る確率が等しい）コインを二回「独立に」（つまり，第二回目の試行が第一回目に依存しないで）なげる試行を考える．このとき，表が出る事象を 1，裏が出る事象を 0，と表す．

例 2.1. コイン投げにおいて，標本空間 $\mathbb{U}$ は，$\mathbb{U} = \{(1,1),(1,0),(0,1),(0,0)\}$ である．また，E を第一回目に表が出る事象とすれば，$E = \{(1,1),(1,0)\} \subseteq \mathbb{U}$ である．よって，$\Pr\{E\} = |E|/|\mathbb{U}| = 2/4 = 1/2$ である．

問 2.1. F を第二回目に表が出る事象としたとき，F はどのように表されるか．また，$\Pr\{F\}$ の値を求めなさい．

2.1　論理包含

命題 2.1. 事象 E, F に対して，E がおきれば F がおきるという関係が成り立っているとする．(E, F を命題とみなせば $E \Rightarrow F$.）このとき，$\Pr(E) \leq \Pr(F)$ である．

証明. 仮定は，$E \subseteq F$ を意味する．これより，$\Pr\{E\} \leq \Pr\{F\}$ である． ■

例 2.2. コイン投げにおいて，E を二回とも表が出る事象，F を二回目に表が出る事象とする．このとき，$E \Rightarrow F$ であり，上の命題より，$\Pr\{E\} \leq \Pr\{F\}$ である．(実際，$\Pr\{E\} = 1/4, \Pr\{F\} = 1/2$ である.)

問 2.2. コイン投げにおいて，E を二回とも表が出る事象，F を二回のうち少なくともどちらか一方で表が出る事象とする．上の命題を用いて，$\Pr\{E\}$ と $\Pr\{F\}$ の大小関係を示しなさい．

2.2 ユニオンバウンド

定義 2.3

E, F を任意の事象とする．E または F がおきる事象を E と F の**和事象**といい，$E \cup F$ と表す.（E, F が命題であるとき $E \vee F$ と表す.）E と F の双方がおきる事象を E と F の**積事象**といい，$E \cap F$ と表す.（E, F が命題であるとき $E \wedge F$ と表す.）E がおきない事象を E の**余事象**といい，$\bar{E}$ と表す.

例 2.3. コイン投げにおいて，E を第一回目に表が出る事象，F を第二回目に表が出る事象とする．このとき，

- $\Pr\{E \cup F\} = 3/4$.
- $\Pr\{E \cap F\} = 1/4$.
- $\Pr\{\bar{E}\} = \Pr\{\bar{F}\} = 1/2$.

定義 2.4

E, F を任意の事象とする．$E \cap F = \emptyset$ であるとき，E と F は**排反**であるという．

例 2.4. コイン投げにおいて，E を二回とも表が出る事象，F を二回とも裏が出る事象とする．このとき，E と F は排反である．また，E を第一回目に表が出る事象，F を第二回目に表が出る事象としたとき，E と F は排反でない．

命題 2.2. E, F を事象とする．このとき，

$$\Pr\{E \cup F\} \;=\; \Pr\{E\} + \Pr\{F\} - \Pr\{E \cap F\}.$$

証明. ■

問 2.3. 上の命題を証明しなさい.

系 2.3. E, F を事象とする．このとき，

$$\Pr\{E \cup F\} \;\leq\; \Pr\{E\} + \Pr\{F\}.$$

また，E, F が排反であるとき，

$$\Pr\{E \cup F\} \;=\; \Pr\{E\} + \Pr\{F\}.$$

問 2.4. 上の系が成り立つ理由を説明しなさい.

定理 2.1 (ユニオンバウンド)**.** $E_1, E_2, \ldots, E_n$ を事象とする．このとき，

$$\Pr\{E_1 \cup E_2 \cup \cdots \cup E_n\} \leq \sum_{i \in [n]} \Pr\{E_i\}.$$

また，$E_1, E_2, \ldots, E_n$ が互いに排反であるとき，

$$\Pr\{E_1 \cup E_2 \cup \cdots \cup E_n\} = \sum_{i \in [n]} \Pr\{E_i\}.$$

証明. 上の系を用いて，数学的帰納法により示される． ■

問 2.5. 上の定理の証明を完成させなさい.

2.3 独立，条件付き確率

定義 2.5

$E_1, \ldots, E_n$ を事象とする．$E_1, \ldots, E_n$ が**互いに独立である**とは，次を満たすことである．任意の $I \subseteq [n]$ について，

$$\Pr\left\{\bigcap_{i \in I} E_i\right\} = \prod_{i \in I} \Pr\{E_i\}.$$

任意の $I \in [n]$ s.t. $|I| = 2$ について上の等式が満たされるとき，**対ごとに独立である**という.

注 2.1. $E_1, \ldots, E_n$ が互いに独立であれば，それらは対ごとに独立である.（その逆は成り立たない.）

例 2.5. コイン投げにおいて，三つの事象 E, F, G を以下のように定義する.

$$\begin{aligned} E &\stackrel{\text{def}}{=} \text{第一回目に表が出る} \\ F &\stackrel{\text{def}}{=} \text{第二回目に表が出る} \\ G &\stackrel{\text{def}}{=} \text{第一回目と第二回目に出る面が等しい} \end{aligned}$$

このとき，

$$\Pr\{E\} = \Pr\{F\} = \Pr\{G\} = \frac{1}{2}.$$

また，

$$\Pr\{E \cap F\} = \Pr\{E \cap G\} = \Pr\{F \cap G\} = \frac{1}{4}.$$

更に，

$$\Pr\{E \cap F \cap G\} = \frac{1}{4}.$$

これより，E, F, G は対ごとに独立であるが，互いに独立でない.

問 2.6. 上の例において，E, F, G は対ごとに独立であることの理由を示しなさい．また，互いに独立でないことの理由を示しなさい.

定義 2.6

E, F を事象とする．F がおきたもとで E がおきる**条件付き確率**を $\Pr\{E|F\}$ と表し，以下の式で定義する．

$$\Pr\{E|F\} \stackrel{\text{def}}{=} \frac{\Pr\{E \cap F\}}{\Pr\{F\}}.$$

問 2.7. 上の例のコイン投げにおいて，$\Pr\{E|F\}$, $\Pr\{F|E\}$, $\Pr\{G|(E \cap F)\}$ を求めなさい．

事実 2.4. 任意の事象 E, F について，

$$\Pr\{E \cap F\} \;=\; \Pr\{E\}\Pr\{F|E\} \;=\; \Pr\{F\}\Pr\{E|F\}.$$

問 2.8. 上の例のコイン投げにおいて，上の事実を用いて，$\Pr\{E \cap F\}$, $\Pr\{E \cap F \cap G\}$ を求めなさい．

命題 2.5. E, F を事象とする．E と F が独立であれば，

$$\Pr\{E|F\} \;=\; \Pr\{E\}.$$

証明. ■

問 2.9. 上の命題を証明しなさい．

2.4 期待値と分散

定義 2.7

$\mathbb{U}$ を標本空間とする．$\mathbb{U}$ 上の**確率変数** X とは，$\mathbb{U}$ から $\mathbb{R}$ への関数である．任意の $x \in \mathbb{R}$ に対して，$X = x$ で事象 $\{a \in \mathbb{U} : X(a) = x\}$ を表す．

例 2.6. コイン投げにおいて，X を表の出る回数とする．このとき，

$$\begin{aligned} X = 0 &\;:\; \{(0,0)\} \\ X = 1 &\;:\; \{(1,0),(0,1)\} \\ X = 2 &\;:\; \{(1,1)\} \end{aligned}$$

問 2.10. 上の例において，任意の $i \in \{0,1,2\}$ について，$\Pr\{X = i\}$ の値を求めなさい．

定義 2.8

X を $\mathbb{U}$ 上の確率変数として，$\mathcal{D} = X(\mathbb{U})$（$X$ による $\mathbb{U}$ の像）とする．X の**期待値**を $\mathrm{E}[X]$ と表し，以下の式で定義する．

$$\mathrm{E}[X] \stackrel{\text{def}}{=} \sum_{x \in \mathcal{D}} x \cdot \Pr\{X = x\}.$$

例 2.7. コイン投げにおいて，X を表の出る回数とする．（よって，$\mathcal{D} = \{0, 1, 2\}$.）このとき，

$$\mathrm{E}[X] \;=\; 0 \cdot \Pr\{X = 0\} + 1 \cdot \Pr\{X = 1\} + 2 \cdot \Pr\{X = 2\} \;=\; 1 \cdot \frac{1}{2} + 2 \cdot \frac{1}{4} \;=\; 1.$$

定理 2.2 (期待値の線形性)**.** X, Y を $\mathbb{U}_X, \mathbb{U}_Y$ 上の確率変数とする．このとき，

$$\mathrm{E}[X + Y] \;=\; \mathrm{E}[X] + \mathrm{E}[Y].$$

また，任意の $c \in \mathbb{R}$ について，

$$\mathrm{E}[cX] \;=\; c \cdot \mathrm{E}[X].$$

証明. $\mathcal{D}_X = X(\mathbb{U}_X), \mathcal{D}_Y = Y(\mathbb{U}_Y)$ とする．このとき，

$$\begin{aligned}
\mathrm{E}[X + Y] \;&=\; \sum_{x \in \mathcal{D}_X, y \in \mathcal{D}_y} (x + y) \cdot \Pr\{(X = x) \cap (Y = y)\} \\
&=\; \sum_{x \in \mathcal{D}_X, y \in \mathcal{D}_Y} x \cdot \Pr\{(X = x) \cap (Y = y)\} + \sum_{x \in \mathcal{D}_X, y \in \mathcal{D}_Y} y \cdot \Pr\{(X = x) \cap (Y = y)\}.
\end{aligned}$$

主張 2.1.

$$\begin{aligned}
\sum_{x \in \mathcal{D}_X, y \in \mathcal{D}_Y} x \cdot \Pr\{(X = x) \cap (Y = y)\} \;&=\; \sum_{x \in \mathcal{D}_X} x \cdot \Pr\{X = x\}, \\
\sum_{x \in \mathcal{D}_X, y \in \mathcal{D}_Y} y \cdot \Pr\{(X = x) \cap (Y = y)\} \;&=\; \sum_{y \in \mathcal{D}_Y} y \cdot \Pr\{Y = y\}.
\end{aligned}$$

証明. ■

問 2.11. この主張を証明しなさい.

この主張より，

$$\mathrm{E}[X + Y] \;=\; \sum_{x \in \mathcal{D}_X} x \cdot \Pr\{X = x\} + \sum_{y \in \mathcal{D}_Y} y \cdot \Pr\{Y = y\} \;=\; \mathrm{E}[X] + \mathrm{E}[Y].$$

■

問 2.12. 上の定理の $\mathrm{E}[cX] = c \cdot \mathrm{E}[X]$ を証明しなさい.

系 2.6. $X_1, \ldots, X_n$ を $\mathbb{U}_{X_1}, \ldots, \mathbb{U}_{X_n}$ 上の確率変数とする．このとき，

$$\mathrm{E}\left[\sum_{i\in[n]} X_i\right] \;=\; \sum_{i\in[n]} \mathrm{E}[X_i].$$

問 2.13. この系を証明しなさい．

例 2.8. コイン投げにおいて，X を表の出る回数とする．X_i を次のような確率変数とする．第 i 回目の試行において，

$$X_i \stackrel{\mathrm{def}}{=} \begin{cases} 1 & : \text{表が出る} \\ 0 & : \text{裏が出る} \end{cases}$$

このとき，$X = X_1 + X_2$．また，$\mathrm{E}[X_i] = \Pr\{X_i = 1\} = 1/2$．よって，

$$\mathrm{E}[X] \;=\; \mathrm{E}[X_1 + X_2] \;=\; \mathrm{E}[X_1] + \mathrm{E}[X_2] \;=\; 1.$$

注 2.2. 上の二つの例から分かるように，確率変数 X をいくつかの確率変数の和にすると，(期待値の線形性を用いることにより）X の期待値を求めることが容易になることがある．

命題 2.7. X, Y を $\mathbb{U}_X, \mathbb{U}_Y$ 上の確率変数とする．X, Y が互いに独立であれば，

$$\mathrm{E}[XY] \;=\; \mathrm{E}[X] \cdot \mathrm{E}[Y].$$

証明. $\mathcal{D}_X = X(\mathbb{U}_X), \mathcal{D}_Y = Y(\mathbb{U}_Y)$ とする．このとき，

$$\begin{aligned}
\mathrm{E}[XY] &= \sum_{x\in\mathcal{D}_X, y\in\mathcal{D}_Y} xy \cdot \Pr\{(X = x) \cap (Y = y)\} \\
&= \sum_{x\in\mathcal{D}_X, y\in\mathcal{D}_Y} xy \cdot \Pr\{X = x\} \Pr\{Y = y\} \quad (\because\ X, Y \text{ が独立}) \\
&= \sum_{x\in\mathcal{D}_X} x \cdot \Pr\{X = x\} \sum_{y\in\mathcal{D}_Y} y \cdot \Pr\{Y = y\} \\
&= \mathrm{E}[X] \cdot \mathrm{E}[Y].
\end{aligned}$$

■

系 2.8. $X_1, \ldots, X_n$ を $\mathbb{U}_{X_1}, \ldots, \mathbb{U}_{X_n}$ 上の確率変数とする．$X_1, \ldots, X_n$ が互いに独立であれば，

$$\mathrm{E}[X_1 \cdots X_n] \;=\; \mathrm{E}[X_1] \cdot \cdots \cdot \mathrm{E}[X_n].$$

問 2.14. 上の系を証明しなさい．

定義 2.9

X を $\mathbb{U}$ 上の確率変数として，$\mathcal{D} = X(\mathbb{U})$ とする．$\mu = \mathrm{E}[X]$ とする．X の**分散**を $\mathrm{V}[X]$ と表し，以下の式で定義する．

$$\mathrm{V}[X] \stackrel{\mathrm{def}}{=} \mathrm{E}[(X-\mu)^2] = \sum_{x\in\mathcal{D}} (x-\mu)^2 \cdot \Pr\{X = x\}.$$

また，$\sqrt{V[X]}$ を X の**標準偏差**という．

例 2.9. コイン投げにおいて，X を表の出る回数とする．（よって，$\mathcal{D} = \{0,1,2\}$, $\mathrm{E}[X] = 1$.）このとき，

$$\begin{aligned}\mathrm{V}[X] &= (0-1)^2 \cdot \Pr\{X=0\} + (1-1)^2 \cdot \Pr\{X=1\} + (2-1)^2 \cdot \Pr\{X=2\} \\ &= 1 \cdot \frac{1}{4} + 1 \cdot \frac{1}{4} \\ &= \frac{1}{2}.\end{aligned}$$

補題 2.9. X を $\mathbb{U}$ 上の確率変数，$\mu = \mathrm{E}[X]$ とする．このとき，

$$\mathrm{V}[X] = \mathrm{E}[X^2] - \mu^2.$$

証明. 以下の式変形より：

$$\mathrm{V}[X] = \mathrm{E}[(X-\mu)^2] = \mathrm{E}[X^2 - 2\mu X + \mu^2] = \mathrm{E}[X^2] - \mu^2.$$

■

命題 2.10. $X_1, \ldots, X_n$ を対ごとに独立である確率変数として，$X = \sum_{i\in[n]} X_i$ とする．このとき，

$$\mathrm{V}[X] = \sum_{i\in[n]} \mathrm{V}[X_i].$$

証明. 任意の $i \in [n]$ について $\mu_i \stackrel{\mathrm{def}}{=} \mathrm{E}[X_i]$ として，$\mu \stackrel{\mathrm{def}}{=} \mathrm{E}[X]$ とする．このとき，期待値の線形性より，$\mu = \mathrm{E}[X] = \sum_{i\in[n]} \mu_i$．また，補題 2.9 より，任意の $i \in [n]$ について，

$$\mathrm{V}[X_i] = \mathrm{E}[X_i^2] - \mu_i^2.$$

更に，$\mathrm{V}[X] = \mathrm{E}[X] - \mu$．ここで，$X_i, X_j$ は独立であることから，

$$\mathrm{E}[X^2] = \mathrm{E}\left[\left(\sum_{i\in[n]} X_i\right)^2\right] = \sum_{i\in[n]} \mathrm{E}[X_i^2] + 2\sum_{i<j} \mathrm{E}[X_i X_j] = \sum_{i\in[n]} \mathrm{E}[X_i^2] + 2\sum_{i<j} \mu_i \mu_j.$$

また，

$$\mu^2 = \left(\sum_{i\in[n]} \mu_i\right)^2 = \sum_{i\in[n]} \mu_i^2 + 2\sum_{i<j} \mu_i \mu_j.$$

これらのことから，

$$\begin{aligned} \mathrm{V}[X] &= \mathrm{E}[X^2] - \mu^2 \\ &= \sum_{i\in[n]} \mathrm{E}[X_i^2] + 2\sum_{i<j} \mu_i\mu_j - \left(\sum_{i\in[n]} \mu_i^2 + 2\sum_{i<j} \mu_i\mu_j \right) \\ &= \sum_{i\in[n]} \left(\mathrm{E}[X_i^2] - \mu_i^2 \right). \end{aligned}$$

最後に，$\mathrm{V}[X_i] = \mathrm{E}[X_i^2] - \mu_i^2$ であることから，命題が示される． ■

例 2.10. コイン投げにおいて，X を表の出る回数とする．X_i を次のような確率変数とする．第 i 回目の試行において，

$$X_i \stackrel{\mathrm{def}}{=} \begin{cases} 1 & : \text{表が出る} \\ 0 & : \text{裏が出る} \end{cases}$$

このとき，$X = X_1 + X_2$．また，$\mu_i = \mathrm{E}[X_i] = 1/2$ より，

$$\mathrm{V}[X_i] = \mathrm{E}[(X_i - \mu_i)^2] = \mathrm{E}[X_i^2] - \mu_i^2 = \mathrm{E}[X_i] - \mu_i^2 = 1/4.$$

よって，X_1, X_2 は独立であることから，

$$\mathrm{V}[X] = \mathrm{V}[X_1 + X_2] = \mathrm{V}[X_1] + \mathrm{V}[X_2] = \frac{1}{2}.$$

注 2.3. 上の二つの例から分かるように，確率変数 X をいくつかの確率変数の和にすると，それらが互いに独立であった場合，X の分散を求めることが容易になることがある．

2.5 マルコフの不等式

定理 2.3 (マルコフの不等式)**.** X を非負の実数をとる確率変数，$\mu = \mathrm{E}[X]$ とする．このとき，任意の $t \in \mathbb{R}^+$ について，

$$\Pr\{X \geq t\} \leq \frac{\mu}{t}.$$

証明. $t \in \mathbb{R}^+$ を任意に固定する．X が $\mathbb{U}$ 上の確率変数，$\mathcal{D} = X(\mathbb{U}) \subseteq \mathbb{R}^+ \cup \{0\}$ とする．このとき，任意の $t \in \mathbb{R}^+$ について，

$$\begin{aligned} \mu &= \mathrm{E}[X] = \sum_{x\in\mathcal{D}} x \cdot \Pr\{X = x\} \\ &\geq \sum_{x\in\mathcal{D}:x\geq t} x \cdot \Pr\{X = x\} \geq \sum_{x\in\mathcal{D}:x\geq t} t \cdot \Pr\{X = x\} = t \cdot \Pr\{X \geq t\}. \end{aligned}$$

■

3　整列問題

整列問題（sorting）

- 入力：自然数の列 $a_1, a_2, \ldots, a_n \in \mathbb{N}$
- 解：$[n]$ 上の置換 $\pi : [n] \to [n]$ s.t. $a_{\pi(1)} \leq a_{\pi(2)} \leq \cdots \leq a_{\pi(n)}$

3.1　クイックソート

qsort$(s_1, s_2, \ldots, s_m \in \mathbb{N})$　// $S = \{s_1, s_2, \ldots, s_m\}$ とする
返り値：$s_1, s_2, \ldots, s_m$ の昇順

1. $|S| \leq 1$ であれば S を返す.（初めての呼び出しであれば S を出力する.）
2. $S \setminus \{s_1\}$ のうち，s_1 未満の数の集合を S_1，s_1 以上の数の集合を S_2 とする.
3. S_1, S_2 を，それぞれ再帰的に整列する.（つまり，qsort(S_1), qsort(S_2) を呼び出す．返り値をそれぞれ T_1, T_2 とする.）
4. $T = (T_1, s_1, T_2)$ を返す.（初めての呼び出しであれば T を出力する.）

図 4: クイックソート

注 3.1. qsort アルゴリズムのステップ 2 は，それぞれの $s \in S \setminus \{s_1\}$ と s_1 を比較することによって，$S \setminus \{s_1\}$ を S_1, S_2 に分割する.

命題 3.1. qsort は整列問題を解く.

証明. 任意の入力に対して，qsort が正しい解を出力する（整列する）ことを示せばよい．これを，入力される自然数の個数 n についての帰納法により示す．$n \leq 1$ のときは明らか.

k を任意の自然数とする．k 以下の任意の自然数 n に対して，更に，n 個の任意の自然数の列 $(s_1, \ldots, s_n)$ に対して，qsort$(s_1, \ldots, s_n)$ が正しい解を出力するとする．$n = k+1$ とする．$(a_1, \ldots, a_n)$ を任意の入力とする．qsort$(a_1, \ldots, a_n)$ の実行を考える．$|S_1| \leq k$ かつ $|S_2| \leq k$ より，帰納仮定から，qsort(S_1), qsort(S_2) はそれぞれ正しい解（つまり S_1, S_2 の昇順）を返す.（返り値をそれぞれ T_1, T_2 とする.）よって，任意の $s \in S_1$ について $s < a_1$，任意の $s \in S_2$ について $s \geq a_1$ より，(T_1, s, T_2) は昇順である．以上より，$n = k+1$ に対して qsort は正しい解を出力することがいえる．よって，任意の入力に対して，qsort は正しい解を出力する．■

命題 3.2. 入力される自然数の個数を $n \geq 2$ とする．アルゴリズム全体を通してステップ 2 で行われる二つの自然数の比較回数の総合計を $f(n) \geq 1$ とする．このとき，(単一コスト RAM モデルのもと）アルゴリズムの計算時間は $O(f(n))$ である.

定理 3.1. 入力される自然数の個数を n とする．このとき，qsort アルゴリズムの計算時間（の最悪）は $O(n^2)$ である．

証明. 上の命題より，比較回数の合計（の最悪）が $O(n^2)$ であることを示せばよい．n 個の自然数に対して，アルゴリズムの計算時間を $T(n)$ とする． ■

問 3.1. 上の定理の証明を完成させなさい．($T(n)$ に関する漸化式を示すこと．)

問 3.2. qsort アルゴリズムの計算時間（の最悪）が $\Omega(n^2)$ であることを示しなさい．(そのようになる具体的な入力を示す．)

3.2 乱択クイックソート

qsort アルゴリズムにおいて，s_1 を**ピボット**という．図 5 で示される乱択クイックソート rand_qsort は，このピボットを S から一様ランダムに選ぶクイックソートである．

rand_qsort$(s_1, s_2, \ldots, s_m \in \mathbb{N})$ // $S = \{s_1, s_2, \ldots, s_m\}$ とする
返り値：$s_1, s_2, \ldots, s_m$ の昇順

1. $|S| \leq 1$ であれば S を返す．(初めての呼び出しであれば S を出力する．)
2. S の中から一様ランダムに要素を選ぶ．(それを s とする．)
3. $S \setminus \{s\}$ のうち，s 未満の数の集合を S_1，s 以上の数の集合を S_2 とする．
4. S_1, S_2 を，それぞれ再帰的に整列する．(つまり，rand_qsort(S_1), rand_qsort(S_2) を呼び出す．返り値をそれぞれ T_1, T_2 とする．)
5. $T = (T_1, s, T_2)$ を返す．(初めての呼び出しであれば T を出力する．)

図 5: 乱択クイックソート

問 3.3. 7 個の適当な自然数の列を考案して，その列に対する図 5 のアルゴリズムの動作及び出力を示しなさい．

定理 3.2. 入力される自然数の個数を n とする．このとき，rand_qsort アルゴリズムの平均計算時間は $O(n \ln n)$ である．

証明. アルゴリズムの入力を $a_1, \ldots, a_n$，その集合を A とする．一般性を失うことなく $A = [n]$ とする.（重複した自然数があるときも同様にして示される.）命題 3.2 より，アルゴリズムのステップ 2 で行われる二つの自然数の比較回数の合計の期待値を求めればよい.（この期待値は，アルゴリズムのステップ 2 で一様ランダムに選ぶ一連の確率に依存する.）任意の $i, j \in [n]$ について，確率変数 $X_{i,j}$ を以下のように定義する.

$$X_{i,j} \stackrel{\text{def}}{=} \begin{cases} 1 & : \ i \text{ と } j \text{ が比較される} \\ 0 & : \ \text{o.w.} \end{cases}$$

よって,（i と j が比較されるのは高々一回であることから）比較回数 X は,

$$X \ = \ \sum_{i \in [n]} \sum_{j \in [n]: j > i} X_{i,j}.$$

問 3.4. i と j が比較されるのは高々一回である理由を説明しなさい.

よって，X の期待値は，期待値の線形性より,

$$\mathrm{E}[X] \ = \ \mathrm{E}\left[\sum_{i \in [n]} \sum_{j \in [n]: j > i} X_{i,j} \right] \ = \ \sum_{i \in [n]} \sum_{j \in [n]: j > i} \mathrm{E}[X_{i,j}].$$

ここで，任意の $i, j \in [n]$ について,

$$\mathrm{E}[X_{i,j}] \ = \ 1 \cdot \Pr(X_{i,j} = 1) + 0 \cdot \Pr(X_{i,j} = 0) \ = \ \Pr(X_{i,j} = 1).$$

よって，i と j が比較される確率 $p_{i,j} \stackrel{\text{def}}{=} \Pr(X_{i,j} = 1)$ を求めればよい.（この確率は，アルゴリズムのステップ 2 で一様ランダムに選ぶ一連の確率に依存する.）

以降，$i, j \in [n]$ を任意に固定する．$p_{i,j}$ を求めるために，アルゴリズムの実行（計算過程）を表す次のような二分木を考える．各頂点は，次のように A の要素でラベル付けされる．まず，根は，最初の呼び出し $\texttt{rand\_qsort}(A)$ のステップ 2 で選ばれた要素でラベル付けされる.（それを s として，$A \setminus \{s\}$ が S_1, S_2 に分割されたとする.）次に，再帰呼び出し $\texttt{rand\_qsort}(S_1)$, $\texttt{rand\_qsort}(S_2)$ のステップ 2 で選ばれた要素を，それぞれ $s' \in S_1$, $s'' \in S_2$ としたとき，二分木の根の二つの子は，それぞれ左から s', s'' でラベル付けされる．以下，同様にして，二分木の各頂点はアルゴリズムのステップ 2 で選ばれた要素でラベル付けされる.（ただし，ステップ 1 で S が返された場合は，その要素でラベル付けされる.）以下，二分木の各頂点をそのラベルで呼ぶ.（例えば，二分木の根を s，その二つの子を s', s'' と呼ぶ.）

事実 3.3. 二分木について以下の事実が成り立つ.

- 頂点の個数は n である.
- 頂点のラベルの集合は $[n]$ である.
- $\texttt{rand\_qsort}(A)$ の実行は，二分木を深さ優先探索で辿る計算過程となる.

問 3.5. この事実が成り立つ理由を説明しなさい.

主張 3.1. i と j が比較されるのは，i と j が（二分木において）先祖・子孫または子孫・先祖の関係にあるときかつそのときに限る.

問 3.6. この主張を証明しなさい.

主張 3.2. $K = \{k : i \le k \le j\}$ とする．`rand_qsort`(A) の実行において，K の中で最初に $k \in K$ がピボットとして選ばれたとする．このときの再帰呼び出しを `rand_qsort`(S) とする．このとき，$K \subseteq S$ である.

証明. 二分木において，根から頂点 k までのパスを $v_1, v_2, \ldots, v_d = k$ とする．また，任意の $\ell \in [d]$ について，v_ℓ がピボットとして選ばれた再帰呼び出しを `rand_qsort`(V_ℓ) とする.（$V_1 = A, V_d = S$，更に，$V_1 \supseteq V_2 \supseteq \cdots \supseteq V_d$.）仮定より，任意の $\ell \in [d-1]$ について $v_\ell \notin K$.（$v_d = k \in K$.）つまり，$v_\ell < i$ または $j < v_\ell$．よって，$v_\ell < i$ であれば（$k \in V_{\ell+1}$ であるはずなので）$V_{\ell+1} = \{v \in V_\ell : v > v_\ell\}$，$j < v_\ell$ であれば（$k \in V_{\ell+1}$ であるはずなので）$V_{\ell+1} = \{v \in V_\ell : v < v_\ell\}$.（いずれも，$K \subseteq V_{\ell+1}$.）これより，任意の $\ell \in [d]$ について $K \subseteq V_\ell$．つまり，$K \subseteq V_d = S$. ■

主張 3.3. $K = \{k : i \le k \le j\}$ とする．このとき，i と j が比較されることは，次の事象と同値である．`rand_qsort`(A) の実行において，ピボットとして，i または j が K の中で最初に選ばれる.

証明. ($\Rightarrow$) 対偶をとって示す．つまり，ある $k \in K \setminus \{i, j\}$ が最初に選ばれたとする．このときの再帰呼び出しを `rand_qsort`(S) とする．このとき，i と j は比較されないことを示す．主張 3.2 より，$K \subseteq S$ である．よって,（$i < k < j$ より）$i \in S_1, j \in S_2$．これより，i と j は二分木において先祖・子孫の関係になりえない．よって，主張 3.1 より，i と j は比較されない.

($\Leftarrow$) i が最初に選ばれたとする.（j である場合も同様にして示される.）主張 3.2 より，$K \subseteq S$ である．よって，i がピボットとして選ばれているので，i とすべての $S \setminus \{i\}$ は比較される，つまり,（$j \in K \subseteq S \setminus \{i\}$ より）i と j は比較される. ■

主張 3.4. $K = \{k : i \le k \le j\}$ とする．このとき,

$$\Pr(i \text{ または } j \text{ が } K \text{ の中で最初に選ばれる}) = \frac{2}{j - i + 1}.$$

証明. K のどの要素も，ピボットとして，K の中で最初に選ばれる確率は同様に確かであるので. ■

これらの主張より,（命題 8.12 を用いて）

$$\begin{aligned}
\mathrm{E}[X] &= \sum_{i \in [n]} \sum_{j \in [n] : j > i} \mathrm{E}[X_{i,j}] = \sum_{i \in [n]} \sum_{j \in [n] : j > i} p_{i,j} = \sum_{i \in [n]} \sum_{j \in [n] : j > i} \frac{2}{j - i + 1} \\
&= \sum_{i \in [n]} \left(\sum_{j=1}^{n-i+1} \frac{2}{j} - 2 \right) = 2 \sum_{i \in [n]} \sum_{j \in [i]} \frac{1}{j} - 2n \\
&\le 2 \sum_{i \in [n]} \ln i \quad (\because \text{命題 8.12}) \\
&\le 2n \ln n.
\end{aligned}$$

問 3.7. 最後の不等式を示しなさい.（ヒント：スターリングの公式（定理 8.3））

問 3.8. 命題 8.12 を証明しなさい.

■

系 3.4. X を二つの自然数 a_i, a_j（$i, j \in [n]$）の比較回数の合計とすれば,

$$\Pr\{X \geq 32n \ln n\} \ \leq \ 1/16.$$

問 3.9. この系を証明しなさい.（ヒント：マルコフの不等式を用いる.）

4　素数性判定問題

定義 4.1

整数 $a, b \in \mathbb{Z}$ に対して，$a = bc$ を満たす整数 $c \in \mathbb{Z}$ が存在するとき，b は a を**割り切る**（a は b で**割り切れる**）といい，$b \mid a$ と表す．このとき，b は a の**約数**，a は b の**倍数**という．b が a を割り切らない（a が b で割り切れない）とき，$b \nmid a$ と表す．

定義 4.2

a, b を整数とする．$c \mid a$ かつ $c \mid b$ のとき，c を a, b の**公約数**といい，正の公約数の最大を**最大公約数**という．整数 a, b の最大公約数を $\gcd(a, b)$ と表す．整数 a, b が $\gcd(a, b) = 1$ を満たすとき，a, b は**互いに素**であるという．

$a \mid c$ かつ $b \mid c$ のとき，c を a, b の**公倍数**といい，正の公倍数の最小を**最小公倍数**という．整数 a, b の最小公倍数を $\mathrm{lcm}(a, b)$ と表す．

定義 4.3

自然数 $p \geq 2$ が，$\pm 1, \pm p$ 以外の約数を持たないとき，p を**素数**といい，素数の集合を PRIME と表す．素数でない（2 以上の）自然数を**合成数**という．

素数性判定問題（primality testing）

- 入力：自然数 $n \in \mathbb{N}$
- 出力：n が素数であるなら `YES`，合成数であるなら `NO`.

4.1　群論の基礎

定義 4.4

G を集合，$*$ を G 上の二項演算とする．$(G, *)$ が以下を満たすとき，$(G, *)$ を**群**という．

1. $* : G \times G \to G$ である．（つまり，二項演算 $*$ が G で「閉じている」．）
2. 任意の $a, b, c \in G$ について $a * (b * c) = (a * b) * c$.
3. ある $e \in G$ が存在して，任意の $a \in G$ について $a * e = e * a = a$.
4. 任意の $a \in G$ について，ある $a' \in G$ が存在して（条件 3 の e に対して）$a * a' = a' * a = e$.

条件 2 を**結合則**という．条件 3 の e を**単位元**という．条件 4 の a' を a の**逆元**という．

例 4.1. 二項演算 $+$ を通常の四則演算の和としたとき，$(\mathbb{Z}, +)$ は群である．この場合，単位元は 0，$a \in \mathbb{Z}$ の逆元は $-a \in \mathbb{Z}$ となる．

例 4.2. 二項演算 $\cdot$ を通常の四則演算の積としたとき，$(\mathbb{Q} \setminus \{0\}, \cdot)$ は群である．この場合，単位元は 1，$a \in \mathbb{Q}$ の逆元は $1/a \in \mathbb{Q}$ となる．

問 4.1. 上の例において，$(\mathbb{Q}, \cdot)$ は群であるか．

命題 4.1. 群 $(G,*)$ の単位元は唯一である．また，任意の $a \in G$ について，a の逆元は唯一である．

証明. まず，単位元の唯一性を示す．e, e' を単位元とする．単位元の定義より，

$$\begin{aligned} e' * e = e * e' = e', \qquad & (\because e \text{ が単位元}) \\ e * e' = e' * e = e. \qquad & (\because e' \text{ が単位元}) \end{aligned}$$

これら二つの等式より $e = e'$．よって，$(G,*)$ の単位元は唯一である．

次に，逆元の唯一性を示す．$a \in G$ を任意の元とする．a', a'' を a の逆元とする．逆元の定義より，

$$\begin{aligned} a * a' = a' * a = e, \qquad & (\because a' \text{ が逆元}) \\ a * a'' = a'' * a = e. \qquad & (\because a'' \text{ が逆元}) \end{aligned}$$

これら二つの等式より $a * a' = a * a''$．よって，

$$\begin{aligned} a * a' = a * a'' \quad &\iff \quad a' * (a * a') = a' * (a * a'') \\ &\iff \quad (a' * a) * a' = (a' * a) * a'' \\ &\iff \quad e * a' = e * a'' \\ &\iff \quad a' = a''. \end{aligned}$$

よって，a の逆元は唯一である． ■

定義 4.5

$(G,*)$ を群とする．$(G,*)$ が以下を満たすとき，$(G,*)$ を**可換群**（または**アーベル群**）という．

- 交換律：任意の $a, b \in G$ について $a * b = b * a$.

例 4.3. 二項演算 $+$ を通常の四則演算の和，$\cdot$ を積としたとき，$(\mathbb{Z}, +)$，$(\mathbb{Q} \setminus \{0\}, \cdot)$ は可換群である．

定義 4.6

$(G,*)$ を群とする．$|G|$ を群 $(G,*)$ の**位数**という．位数が有限であるとき，$(G,*)$ を**有限な群**という．

例 4.4. n を自然数とする．$\mathbb{Z}_n$ 上の二項演算 $*$ を次のように定義する．任意の $a, b \in \mathbb{Z}_n$ について $a * b \stackrel{\text{def}}{=} a + b \pmod{n}$．このとき，$(\mathbb{Z}_n, *)$ は有限な可換群である．(単位元は 0 である．)

例 4.5. p を素数とする．$\mathbb{Z}_p$ 上の二項演算 $*$ を次のように定義する．任意の $a, b \in \mathbb{Z}_p$ について，$a * b \stackrel{\text{def}}{=} a \cdot b \pmod{p}$ とする．このとき，$(\mathbb{Z}_p \setminus \{0\}, *)$ は有限な可換群である．(単位元は 1 である．)

問 4.2. 上の例において，$(\mathbb{Z}_p, *)$ は群になるか．また，p が素数であるのはなぜか．(p が合成数のとき群になるか.)

定義 4.7

n を自然数とする．$\mathbb{Z}_n^*$ を n と互いに素な $\mathbb{Z}_n$ の要素の集合とする．つまり，

$$\mathbb{Z}_n^* \stackrel{\text{def}}{=} \{a \in \mathbb{Z}_n \setminus \{0\} : \gcd(n, a) = 1\}.$$

事実 4.2. p を素数 p とする．このとき，

$$\mathbb{Z}_p^* \;=\; \mathbb{Z}_p \setminus \{0\} \;=\; \{1, 2, \ldots, p-1\}.$$

事実 4.3. n を自然数とする．$\mathbb{Z}_n^*$ 上の二項演算 $*$ を次のように定義する．任意の $a, b \in \mathbb{Z}_n^*$ について，$a * b \stackrel{\text{def}}{=} a \cdot b \pmod{n}$ とする．このとき，$(\mathbb{Z}_n^*, *)$ は群である．（単位元は 1 である．）（証明は，命題 4.15 を参照．）

定義 4.8

G を集合とする．群の「表記法」として，以下の二つがよく用いられる．

- **加法的な表記**：G 上の演算記号を $+$ と表記した場合の群 $(G, +)$．この場合，群 $(G, +)$ は**加法群**といわれる．加法群において，単位元は 0，$a \in G$ の逆元は $-a \in G$ と表す．また，

$$\begin{array}{rclcrcl} 1a & = & a & & -1a & = & -a \\ 2a & = & a + a & & -2a & = & -a + (-a) \\ 3a & = & a + a + a & & -3a & = & -a + (-a) + (-a) \\ & \vdots & & & & \vdots & \end{array}$$

  と表す．更に，$a + (-b)$ を $a - b$ と表す．

- **乗法的な表記**：G 上の演算記号を $\cdot$ と表記した場合の群 $(G, \cdot)$．この場合，群 $(G, \cdot)$ は**乗法群**といわれる．乗法群において，単位元は 1，$a \in G$ の逆元は $a^{-1} \in G$ と表す．また，

$$\begin{array}{rclcrcl} a^1 & = & a & & a^{-1} & = & a^{-1} \\ a^2 & = & a \cdot a & & a^{-2} & = & a^{-1} \cdot a^{-1} \\ a^3 & = & a \cdot a \cdot a & & a^{-3} & = & a^{-1} \cdot a^{-1} \cdot a^{-1} \\ & \vdots & & & & \vdots & \end{array}$$

  と表す．

注 4.1. これは，「表記法」についての一般的な定義である．よって，上の二項演算 $+, \cdot$ は，必ずしも通常の四則演算の和 $+$，積 $\cdot$ を意味するものではない．

以降，特に断らない限り，群の表記法として乗法群 $(G, \cdot)$ を扱う．（加法群 $(G, +)$ についても同じように議論できる．）

事実 4.4. $(G, \cdot)$ を（乗法）群とする．任意の $a \in G$，任意の $i \in \mathbb{N}$ について，a^i の逆元は a^{-i} である．

問 4.3. この事実を証明しなさい．

部分群

定義 4.9

$(G, \cdot)$ を群とする．$H \subseteq G$（$H \neq \emptyset$）について $(H, \cdot)$ が群であるとき，$(H, \cdot)$ を $(G, \cdot)$ の**部分群**という．（$(\{1\}, \cdot)$ 及び $(G, \cdot)$ は，$(G, \cdot)$ の自明な部分群である．）$H \subsetneq G$ であるとき，$(H, \cdot)$ を $(G, \cdot)$ の**真部分群**という．

例 4.6. $G = \{1, -1, i, -i\}$ とする．ただし，i は虚数単位である．G 上の二項演算 $\cdot$ を複素数の積とする．このとき，$(G, \cdot)$ は群となる．また，$H = \{1, -1\} \subsetneq G$ としたとき，$(H, \cdot)$ は $(G, \cdot)$ の真部分群となる．

問 4.4. 上の例において，$(H, \cdot)$, $(G, \cdot)$ が群となることを示しなさい．

命題 4.5. $(G, \cdot)$ を群，$(H, \cdot)$ を $(G, \cdot)$ の部分群とする．このとき，$(G, \cdot)$ と $(H, \cdot)$ の単位元は同一である．

証明. $(G, \cdot)$ の単位元を 1 とする．このとき，任意の $a \in G$ について $a \cdot 1 = 1 \cdot a = a$．よって，任意の $a \in H$ について $a \cdot 1 = 1 \cdot a = a$．$(H, \cdot)$ は群であり，その単位元は唯一であることから，$(H, \cdot)$ の単位元は（$(G, \cdot)$ の単位元である）1 である． ■

例 4.7. 上の例において，$(H, \cdot)$, $(G, \cdot)$ の単位元は（整数の）1 である．

定理 4.1 (ラグランジュの定理)**.** $(G, \cdot)$ を有限な群，$(H, \cdot)$ を $(G, \cdot)$ の部分群とする．このとき，$|H|$ は $|G|$ を割り切る．

証明. 任意の $a \in G$ について，$aH \stackrel{\text{def}}{=} \{a \cdot h : h \in H\}$ とする．

主張 4.1. 任意の $a, a' \in G$ について，

$$aH \cap a'H \neq \emptyset \implies aH = a'H.$$

証明. $aH \cap a'H \neq \emptyset$ とする．このとき，$aH \subseteq a'H$ かつ $aH \supseteq a'H$ を示せばよい．$aH \subseteq a'H$ を示す．（$aH \supseteq a'H$ も同様にして示される．）$a \cdot h \in aH$ を任意とする．（以降，$a \cdot h \in a'H$ であることを示す．）$aH \cap a'H \neq \emptyset$ より，ある $h_1, h_2 \in H$ が存在して $a \cdot h_1 = a' \cdot h_2$．$H$ が群であることから $h_1 \in H$ の逆元 $h_1^{-1} \in H$ が存在する．よって，

$$(a \cdot h_1) \cdot h_1^{-1} = (a' \cdot h_2) \cdot h_1^{-1} \iff a = a' \cdot (h_2 \cdot h_1^{-1})$$

よって，

$$a \cdot h \ = \ (a' \cdot (h_2 \cdot h_1^{-1})) \cdot h \ = \ a' \cdot (h_2 \cdot h_1^{-1} \cdot h).$$

$h_2 \cdot h_1^{-1} \cdot h \in H$ より，上の式は $a \cdot h \in a'H$ を意味する． ■

主張 4.2. ある $a_1, \ldots, a_s \in G$ が存在して，$[a_1 H, \ldots, a_s H]$ は G の分割である．つまり，

1. $G = a_1 H \cup \cdots \cup a_s H$,
2. $\forall i, j \in [s] : i \neq j [a_i H \cap a_j H = \emptyset]$.

問 4.5. この主張を証明しなさい．

主張 4.3. 任意の $a \in G$ について，$|H| = |aH|$.

証明. 任意の $h \in H$ について $f(h) \stackrel{\text{def}}{=} a \cdot h$ とする．このとき，$f : H \to aH$ が全単射であることを示せばよい．

問 4.6. 写像 f が全単射であることを示しなさい．

■

後の二つの主張より，$|H|$ が $|G|$ を割り切ることがいえる． ■

巡回群

命題 4.6. $(G, \cdot)$ を群とする．任意の $a \in G$ について，$\langle a \rangle = \{a^i : i \in \mathbb{Z}\}$ とする．(a^0 を $(G, \cdot)$ の単位元とする．) このとき，$(\langle a \rangle, \cdot)$ は $(G, \cdot)$ の部分群となる．

証明. $(\langle a \rangle, \cdot)$ が群であることを示せばよい．$a^i, a^j \in \langle a \rangle$ を任意にとる．$i, j \geq 0$ のとき，

$$\begin{aligned} a^i \cdot a^j &= \underbrace{a \cdots\cdots a}_{i} \cdot \underbrace{a \cdots\cdots a}_{j} \\ &= \underbrace{a \cdots\cdots a}_{i+j} \quad (\because\ G \text{ の結合則}) \\ &= a^{i+j}. \end{aligned}$$

$i < 0$ または $j < 0$ の場合でも同様にして示される．よって，任意の $x, y \in \langle a \rangle$ について $x \cdot y \in \langle a \rangle$．つまり，二項演算 $\cdot$ が $\langle a \rangle$ で閉じている．結合則，単位元・逆元の存在性は容易に示される．よって，$(\langle a \rangle, \cdot)$ は群である． ■

問 4.7. 上の命題において，結合則，単位元・逆元の存在性を示しなさい．

定義 4.10

$(G, \cdot)$ を群とする．任意の $a \in G$ について，$\langle a \rangle = \{a^i : i \in \mathbb{Z}\}$ とする．$\langle a \rangle$ の大きさを a の**位数**という．ある $a \in G$ が存在して $G = \langle a \rangle$ となるとき，$(G, \cdot)$ を**巡回群**といい，a を G の**生成元**という．(単位元は a^0 である．)

事実 4.7. 巡回群は可換群である．

問 4.8. この事実を証明しなさい．

命題 4.8. n を任意の自然数とする．ある $a \in \mathbb{N}$，ある $k \in \mathbb{N}$ に対して $a^k = 1 \pmod{n}$ であるとき，$\{a^i : i \in [k]\}$ は巡回群である．

問 4.9. この命題を証明しなさい.（何を示せばよいか？）

系 4.9. n を任意の自然数とする．ある $a \in \mathbb{N}$（$a \neq 1$），ある $k \in \mathbb{N}$ に対して $a^k = 1 \pmod{n}$, かつ $\forall i \in [k-1][a^i \neq 1 \pmod{n}]$ であるとき，巡回群 $\{a^i : i \in [k]\}$ の位数は k である．

問 4.10. この系を証明しなさい.（何を示せばよいか？）

命題 4.10 (巡回群の基本定理)**.** 巡回群の部分群は巡回群となる．

証明. $\langle a \rangle = \{a^i : i \in \mathbb{Z}\}$ を巡回群とする.（a^0 を単位元とする.）G を $\langle a \rangle$ の部分群とする.（命題 4.5 より，$a^0 \in G$.）$d \stackrel{\text{def}}{=} \min\{i \in [k] : a^i \in G\}$ とする．このとき，$G = \langle a^d \rangle$．というのも，$G \neq \langle a^d \rangle$ でないなら，$d \nmid i$ となる $a^i \in G$ が存在することになり，$a^{d'} \in G$（$1 \leq d' < d$）となる．

問 4.11. この事実を証明しなさい.

これは，d の定義に矛盾する．よって，$G = \langle a^d \rangle$，つまり，G は巡回群となる． ■

定理 4.2. 任意の自然数 n について，$\mathbb{Z}_n^*$ 上の二項演算 $*$ を次のように定義する．任意の $a, b \in \mathbb{Z}_n^*$ について，$a * b \stackrel{\text{def}}{=} a \cdot b \pmod{n}$ とする．任意の奇素数 p，任意の自然数 k について，$(\mathbb{Z}_{p^k}^*, *)$ は巡回群である．

注 4.2. $p = 2$ は除外される．例えば，$q = 2^3$ とすれば，$\mathbb{Z}_q^* = \{1, 3, 5, 7\}$．このとき，任意の $a \in \mathbb{Z}_q^*$ について $a^2 \equiv_q 1$．よって，$\mathbb{Z}_q^*$ には生成元が存在しない．

注 4.3. この定理は，$(\mathbb{Z}_{p^k}^*, *)$ が巡回群になることだけ，つまり，生成元の存在性のみに言及している.（その証明は，多項式の次数と解の個数の関係を利用する.）一方，生成元を効率よく見つけるアルゴリズムは知られていない.（$p-1$ の素因数分解が与えられれば（高い確率で）見つけられる.）

4.2 初等整数論の諸定理

以降では，$\cdot$ は通常の四則演算の積を表す.

定義 4.11

a, b を整数，n を自然数とする．$a \bmod n = b \bmod n$ であるとき，a と b は**法** n のもとで**合同**であるといい，$a \equiv_n b$（または $a \equiv b \pmod{n}$）と表す．$a \equiv_n b$ を**合同式**という．また，$a \equiv_n b$ でないとき，$a \not\equiv_n b$ と表す.

事実 4.11. a, b を整数，n を自然数とする．このとき，

$$a \equiv_n b \iff n \mid (a-b).$$

事実 4.12. a, a', b, b' を整数，n を自然数とする．$a \equiv_n a'$, $b \equiv_n b'$ のとき，

$$\begin{aligned} a+b &\equiv_n a'+b' \\ a-b &\equiv_n a'-b' \\ ab &\equiv_n a'b' \end{aligned}$$

事実 4.13 (合同式における移項)**.** 任意の $a, b, c, d \in \mathbb{Z}$，任意の $n \in \mathbb{N}$ について，

$$a+b \equiv_n c+d \iff a+b-c \equiv_n d.$$

事実 4.14. 任意の $a, b, c \in \mathbb{Z}$ 任意の $n \in \mathbb{N}$ に対して，以下の二つが成り立つ．

$$\begin{aligned} &1.\quad b \equiv_n 0 \quad \Rightarrow \quad a+b \equiv_n a, \\ &2.\quad c \equiv_n 1 \quad \Rightarrow \quad ca \equiv_n a. \end{aligned}$$

命題 4.15. n を自然数とする．$\mathbb{Z}_n^*$ 上の二項演算 $*$ を次のように定義する．任意の $a, b \in \mathbb{Z}_n^*$ について，$a * b \stackrel{\text{def}}{=} a \cdot b \pmod{n}$ とする．このとき，$(\mathbb{Z}_n^*, *)$ は群である．(単位元は 1 である．)

証明. 群の定義の条件 1,2,3 が満たされることは明らか．

問 4.12. この事実を説明しなさい．

$\mathbb{Z}_n^* = \{a_1, a_2, \ldots, a_m\}$ とする．($a_1 = 1$ である．) $a \in \mathbb{Z}_n^*$ を任意とする．以下，a の逆元が存在することを示す．任意の $i \in [m]$ について，$r_i \stackrel{\text{def}}{=} a \cdot a_i \pmod{n}$ とする．このとき，

- 任意の $i \in [m]$ について，$r_i \in \mathbb{Z}_n^*$.
- 任意の $i, j \in [m]$ について，$i \neq j$ なら $r_i \neq r_j$.

問 4.13. これら二つの事実を証明しなさい．

よって[2]，ある $i \in [m]$ が存在して $r_i = a_1 = 1$．つまり，その $i \in [m]$ に対して $a \cdot a_i \equiv_n 1$．これは，a の逆元が存在することを意味する． ■

事実 4.16. p を素数，x を $x \not\equiv_p 0$ を満たす任意の整数とする．このとき，任意の整数 a, b に対して，

$$ax \equiv_p bx \iff a \equiv_p b.$$

注 4.4. この事実の $\Rightarrow$ は次のことを意味する．両辺に共通因数 x があった場合，$x \not\equiv_p 0$ であれば，両辺をその共通因数 x で「割る」ことができる．更に一般的に，p と x が互いに素であれば（p が素数でなくても），両辺を共通因数 x で割ることができる．

[2] $f(a_i) = r_i$ とすれば，これら二つの事実は，写像 $f : \mathbb{Z}_n^* \to \mathbb{Z}_n^*$ が全単射であることを意味する．

問 4.14. n と x が互いに素であれば，$ax \equiv_n bx$ なら $a \equiv_n b$ であることを証明しなさい．

定理 4.3 (フェルマーの小定理)**.** p を素数とする．任意の $a \in \mathbb{N}$ について，$a \not\equiv_p 0$ ならば，

$$a^{p-1} \equiv_p 1.$$

定理 4.4 (ユークリッドの補題)**.** a, b を自然数とする．$r = a \bmod b$ とする．($0 \leq r < b$.) このとき，

$$\gcd(a, b) = \gcd(b, r).$$

注 4.5. この定理により，ユークリッドの互除法（の正当性）が得られる．

定理 4.5 (ベズーの等式)**.** a, b を自然数とする．このとき，ある整数 s, t が存在して，

$$\gcd(a, b) = sa + tb.$$

注 4.6. この定理により，拡張版ユークリッドの互除法（の正当性）が得られる．

命題 4.17. n を任意の自然数とする．ある $a \in \mathbb{N}$（$a \neq 1$）に対して，ある $k, \ell \in \mathbb{N}$ が存在して $a^k \equiv_n 1$ かつ $a^\ell \equiv_n 1$ なら，$a^{\gcd(k,\ell)} \equiv_n 1$.

証明. ベズーの等式より，ある s, t が存在して，$\gcd(k, \ell) = sk + t\ell$．よって，

$$a^{\gcd(k,\ell)} = a^{sk+t\ell} = a^{sk}a^{t\ell} = (a^k)^s(a^\ell)^t \equiv_n 1.$$

■

定理 4.6. 任意の自然数 $n > 2$ について，

$$n \in \mathrm{PRIME} \iff \exists a \in \mathbb{Z}_n^* \setminus \{1\} \left[\begin{array}{ll} 1. & a^{n-1} \equiv_n 1 \\ 2. & \forall b \in \mathbb{Z}_n \setminus \{1\} \left[b | (n-1) \Rightarrow a^{\frac{n-1}{b}} \not\equiv_n 1 \right] \end{array} \right].$$

注 4.7. この条件を Pratt certificate と呼ぶ．これは，言語 PRIME が NP であることを意味する．PRIME が coNP であること，つまり，$\overline{\mathrm{PRIME}}$ が NP であることは明らか．よって，PRIME は NP $\cap$ coNP である．更に，PRIME が P であることも証明されている．

証明. ($\Rightarrow$) $n \in$ PRIME とする．(素数 n を p と表す.) フェルマーの小定理より，任意の $a \in \mathbb{Z}_p^*$ について $a^{p-1} \equiv_p 1$．よって，一つ目の条件が成り立つ．定理 4.2 より，$(\mathbb{Z}_p^*, *)$ は巡回群である．よって，生成元 $g \in \mathbb{Z}_p^*$ が存在する．これより，二つ目の条件が成り立つ．

($\Leftarrow$) 集合 $\mathbb{Z}_n^* \subseteq \mathbb{Z}_n$ を考える．命題 4.15 より，$(\mathbb{Z}_n^*, *)$ は群である．以下，$|\mathbb{Z}_n^*| = n - 1$ を示す．(よって，$n \in$ PRIME.)

主張 4.4. 任意の $c \in \mathbb{Z}_n \setminus \{n-1\}$ について $a^c \not\equiv_n 1$.

問 4.15. この主張を証明しなさい.（ヒント：命題 4.17 を用いる.）

よって，系 4.9 より，$|\mathbb{Z}_n^*| = n-1$. ■

定理 4.7 (中国人剰余定理). $n_1, \ldots, n_t \in \mathbb{N}$ を互いに素とする．$n = n_1 \cdots n_t$ とする．このとき，任意の $r_1 \in \mathbb{Z}_{n_1}, \ldots, r_t \in \mathbb{Z}_{n_t}$ に対して，ある $r \in \mathbb{Z}_n$ が唯一に存在して，

$$\forall i \in [t][r \equiv_{n_i} r_i].$$

証明. まず，そのような $r \in \mathbb{Z}_n$ が存在することを示す．$n_1, \ldots, n_t \in \mathbb{N}$ は互いに素であることから，

$$\forall i \in [t][\gcd(n/n_i, n_i) = 1].$$

よって，ベズーの等式より，ある整数 r_i, s_i が存在して，

$$r_i \cdot n_i + s_i \cdot \frac{n}{n_i} \;=\; 1.$$

$x_i \stackrel{\text{def}}{=} s_i n/n_i \in \mathbb{Z}$ とすれば，

$$\begin{array}{lll} x_i & \equiv_{n_i} & 1 \\ x_i & \equiv_{n_j} & 0 \qquad \forall j \in [t] \setminus \{i\} \end{array}$$

よって，$r \stackrel{\text{def}}{=} \sum_{i \in [t]} r_i x_i \pmod n$ とすれば，

$$\forall i \in [t][r \equiv_{n_i} r_i].$$

問 4.16. この事実を証明しなさい．つまり，次を示す．任意の $i \in [t]$ について，

$$\left.\begin{array}{lll} r & \equiv_{n_i} & \displaystyle\sum_{j \in [t]} r_j x_j \\ \displaystyle\sum_{j \in [t]} r_j x_j & \equiv_{n_i} & r_i \end{array}\right\} \implies r \equiv_{n_i} r_i$$

次に，r が唯一に存在することを示す．$r, r' \in \mathbb{Z}_n$ が定理の条件を満たすものとする.（一般性を失うことなく $r > r'$ とする.）このとき，$r \equiv_{n_i} r_i$, $r' \equiv_{n_i} r_i$ より，

$$\forall i \in [t][r - r' \equiv_{n_i} 0].$$

よって，ある自然数 q_i が存在して，

$$r - r' = q_1 n_1 = \quad \cdots \quad = q_t n_t.$$

$n_1, \ldots, n_t$ は互いに素であることから，任意の $i \in [t] \setminus \{1\}$ について $n_i | q_1$．よって,（$n_1, \ldots, n_t$ は互いに素であることから）ある自然数 q が存在して，$q_1 = q n_2 \cdots n_t$．これより，

$$r - r' \;=\; q n_1 n_2 \cdots n_t \;=\; qn.$$

これは,（$r, r' \in \mathbb{Z}_n$, $r > r'$ より）$r - r' \leq n-1$ であることに反する．よって，$r = r'$. ■

系 4.18 (中国人剰余定理（$\mathbb{Z}_n^*$ 版）). $n_1, \ldots, n_t \in \mathbb{N}$ を互いに素とする．$n = n_1 \cdots n_t$ とする．このとき，任意の $r_1 \in \mathbb{Z}_{n_1}^*, \ldots, r_t \in \mathbb{Z}_{n_t}^*$ に対して，ある $r \in \mathbb{Z}_n^*$ が唯一に存在して，

$$\forall i \in [t][r \equiv_{n_i} r_i].$$

問 4.17. この系を証明しなさい．

定義 4.12

$\phi(n) \stackrel{\text{def}}{=} |\mathbb{Z}_n^*|$ を**オイラー関数**と呼ぶ．

命題 4.19 (オイラーの積公式). n を自然数とする．n の素因数分解が $n = p_1^{k_1} \ldots p_t^{k_t}$ であるとき，

$$\phi(n) \;=\; \prod_{i \in [t]} p_i^{k_i - 1}(p_i - 1).$$

証明. 以下の主張より示される[3]．

主張 4.5. オイラー関数 ϕ について以下の等式が成り立つ．

1. $\phi(1) = 1$.
2. 素数 p について $\phi(p^k) = p^{k-1}(p-1)$.
3. $\gcd(a, b) = 1$ である $a, b \in \mathbb{N}$ について $\phi(ab) = \phi(a)\phi(b)$.

証明. 最初の二つは（ほぼ）明らか．（下の問を参照．）以降，等式 3 を示す．$\mathbb{Z}_a^* = \{a_1, \ldots, a_s\}$, $\mathbb{Z}_b^* = \{b_1, \ldots, b_t\}$ とする．以下，$|\mathbb{Z}_{ab}^*| = st$ を示す．(a, b が互いに素なので）中国人剰余定理より，任意の $i \in [s]$, $j \in [t]$ について，ある $r_{ij} \in \mathbb{Z}_{ab}$ が唯一に存在して，$r_{ij} \equiv_a a_i$ かつ $r_{ij} \equiv_b b_j$．このとき，$\mathbb{Z}_{ab}^* = \{r_{ij} : i \in [s], j \in [t]\}$ が成り立つことを示せば十分である．つまり，

$$\begin{array}{lll} 1. & \subseteq & : \forall x \in \mathbb{Z}_{ab}^*, \exists i \in [s], j \in [t][x = r_{ij}] \\ 2. & \supseteq & : \forall i \in [s], j \in [t], \exists x \in \mathbb{Z}_{ab}^*[r_{ij} = x] \end{array}$$

問 4.18. $|\{r_{ij} : i \in [s], j \in [t]\}| = st$ が成り立つ理由を説明しなさい．

($\subseteq$) $x \in \mathbb{Z}_{ab}^*$ を任意に固定する．これは，($\gcd(a, b) = 1$ より）$\gcd(x, a) = \gcd(x, b) = 1$ であることを意味する．$\alpha = x \bmod a$ とする．ユークリッドの補題より，

$$\gcd(x, a) \;=\; \gcd(a, \alpha)$$

これは，($\gcd(x, a) = 1$ より）$\alpha \in \mathbb{Z}_a$ と a が互いに素であることを意味する．よって，$\alpha \in \mathbb{Z}_a^*$，つまり，ある $i \in [s]$ が存在して $x \equiv_a a_i$．同様にして，ある $j \in [t]$ が存在して $x \equiv_b b_j$．これより，ある $i \in [s], j \in [t]$ が存在して $x = r_{ij}$.（そのような x は唯一に存在する.）

[3] ここでは，中国人剰余定理を用いて証明する．包除原理を用いて示すこともできる．

($\supseteq$) $i \in [s], j \in [t]$ を任意に固定する.(つまり，任意に r_{ij} をとる.) r_{ij} の定義より，$a_i = r_{ij} \bmod a$. よって，ユークリッドの補題より，

$$\gcd(r_{ij}, a) \;=\; \gcd(a, a_i) \;=\; 1.$$

これは，r_{ij} と a が互いに素であることを意味する．同様にして，r_{ij} と b が互いに素である．これら二つより，r_{ij} と ab が互いに素であることが示される．つまり，$r_{ij} \in \mathbb{Z}^*_{ab}$. ■

問 4.19. 主張の等式 2 を証明しなさい.

この主張より，主張の等式 3 を $n = p_1^{k_1} \dots p_t^{k_t}$ に（再帰的に）適用し，主張の等式 2 をそれぞれの $\phi(p_i^{k_i})$ に適用すれば，命題の等式が得られる. ■

系 4.20 (オイラーの積公式). n を自然数とする．n の素因数分解が $n = p_1^{k_1} \dots p_t^{k_t}$ であるとき，

$$\phi(n) \;=\; n \prod_{i \in [t]} \left(1 - \frac{1}{p_i}\right).$$

定理 4.8 (オイラーの定理). n を自然数とする．a を n と互いに素な自然数とする．このとき，

$$a^{\phi(n)} \;\equiv_n\; 1.$$

注 4.8. この定理はフェルマーの小定理の一般化である.

問 4.20. この定理を証明しなさい.(離散数学のフェルマーの小定理の証明，及び，注 4.4 を参照.)

定理 4.9 (ウィルソンの定理). 任意の自然数 $n \geq 2$ について，

$$n \in \mathrm{PRIME} \iff (n-1)! \equiv_n -1.$$

証明. ($\Rightarrow$) $n \in \mathrm{PRIME}$ とする．$a \in \{2, \dots, n-2\}$ を任意とする．群 $(\mathbb{Z}^*_n, \cdot)$ において，1 の逆元は 1 であり，$n-1$ の逆元は $n-1$ である．よって，a の逆元は $\{2, \dots, n-2\}$ の要素である．また，a の逆元が a となることはない.(もしそうであるならば，$a^2 \equiv_n 1$ となり，これは $(a+1)(a-1) \equiv_n 0$ となり，n が素数であることに矛盾する.) よって，$\{2, \dots, n-2\}$ は，$(n-3)/2$ 個の組 (a, b) ($ab \equiv_n 1$) に分割できる．これより，

$$2 \cdot 3 \cdot \dots \cdot (n-2) \;\equiv_n\; 1.$$

よって，

$$(n-1)! \;\equiv_n\; 1 \cdot (n-1) \cdot (2 \cdot 3 \cdot \dots \cdot (n-2)) \;\equiv_n\; (n-1) \;\equiv_n\; -1.$$

($\Leftarrow$) $(n-1)! \equiv_n -1$ とする．背理法により示す．つまり，$n \notin \mathrm{PRIME}$ とする．このとき，ある素数 p について（$p|n$, $(n-1)! \equiv_n -1$ より）$(n-1)! \equiv_p -1$. 一方,（$p|n$ より）$p < n$ だから $p|(n-1)!$, つまり，$(n-1)! \equiv_p 0$ である．この二つは矛盾する．よって，$n \in \mathrm{PRIME}$. ■

4.3 フェルマーテスト

ここでは，フェルマーの小定理を利用した（条件付きの）素数性判定アルゴリズムを示す．

定義 4.13

自然数 n が**カーマイケル数**であるとは，n が合成数であり，かつ以下の条件を満たすことである．

$$\forall a \in \mathbb{Z}_n^*[a^{n-1} \equiv_n 1].$$

定理 4.10 (コルセルト判定（Korselt's Criterion）)**.** 合成数 n がカーマイケル数であることは，次のことに同値である：n の任意の素因数 p に対して，

$$p^2 \nmid n \ \wedge \ (p-1)|(n-1).$$

証明. $p_1^{k_1} \cdots p_t^{k_t}$（$t \geq 1, k_i \geq 1$）を n の素因数分解とする．$q_i = p_i^{k_i}$ として，$n = q_1 \cdots q_t$ とする．

($\Rightarrow$) まず，$\forall i \in [t][k_i = 1]$（つまり，$p_i^2 \nmid n$）であることを示す．任意の $i \in [t]$ について，$a_i \in \mathbb{Z}_{q_i}^*$ を（巡回群 $\mathbb{Z}_{q_i}^*$ の）生成元とする．このとき，中国人剰余定理（系 4.18）より，ある $a \in \mathbb{Z}_n^*$ が存在して，$a \equiv_{q_i} a_i$．よって，

$$a_i^{n-1} \ \equiv_{q_i} \ a^{n-1} \ \equiv_{q_i} \ 1.$$

問 4.21. 二つ目の合同式を示しなさい．（ヒント：カーマイケル数であるという仮定がどう用いられているか．）

よって，$|\mathbb{Z}_{q_i}^*| = p_i^{k_i-1}(p_i - 1)$ より，$p_i^{k_i-1}(p_i-1)|(n-1)$.

問 4.22. この事実が成り立つ理由を説明しなさい．（ヒント：$a_i \in \mathbb{Z}_{q_i}^*$ は（$\mathbb{Z}_{q_i}^*$ の）生成元．）

よって，$\exists i \in [t][k_i > 1]$ であれば，$\exists i \in [t][n \equiv_{p_i} 1]$．これは，$\forall i \in [t][p_i|n]$ であることに矛盾する．よって，$\forall i \in [t][k_i = 1]$，つまり，$p_i^2 \nmid n$．更に，$\forall i \in [t][(p_i - 1)|(n-1)]$.

($\Leftarrow$) 合成数 n が定理の条件を満たすとする．$p^2 \nmid n$ より $n = p_1 \cdots p_t$.（n は合成数なので $t \geq 2$.）任意に $a \in \mathbb{Z}_n^*$ を固定する．（$a^{n-1} \equiv_n 1$ を示す．）このとき，中国人剰余定理（系 4.18）より，任意の $i \in [t]$ について，ある $a_i \in \mathbb{Z}_{p_i}^*$ が存在して，$a \equiv_{p_i} a_i$．フェルマーの小定理より，$a^{p_i-1} \equiv_{p_i} a_i^{p_i-1} \equiv_{p_i} 1$. $(p_i - 1)|(n-1)$ より，$a^{n-1} \equiv_{p_i} 1$．よって，$a^{n-1} \equiv_n 1$.

問 4.23. 任意の $i \in [t]$ について $a^{n-1} \equiv_{p_i} 1$ であることから，$a^{n-1} \equiv_n 1$（$n = p_1 \cdots p_t$）が示される理由を説明しなさい．

■

系 4.21. $n = p_1^{k_1} \cdots p_t^{k_t}$ がカーマイケル数であれば $t \geq 3$.

証明. n がカーマイケル数であることから，$\forall i \in [t][k_i = 1]$，かつ，$\forall i \in [t][(p_i - 1)|(n-1)]$．$n$ は合成数であるので（$t > 1$ となり），$t = 2$ であるとして矛盾を導く．このとき，$n = p_1 p_2$ とすれば，$p_1 = p_2$ となり，$t = 1$（更に $k_1 = 2$）となって矛盾する．

問 4.24. $p_1 = p_2$ となる理由を説明しなさい.（ヒント：$n - 1 = p_1 p_2 - 1 = p_1(p_2 - 1) + (p_1 - 1)$.）

■

命題 4.22. 任意の $k \in \mathbb{N}$，任意の $a \in \mathbb{Z}_n$ について，$a \notin \mathbb{Z}_n^*$ なら $a^k \not\equiv_n 1$.

証明. 対偶をとって示す．つまり，$a^k \equiv_n 1$ なら $a \in \mathbb{Z}_n^*$.（$\gcd(a, n) = 1$.）仮定より，$a^{k-1} a \equiv_n 1$.

主張 4.6. ある $c \in \mathbb{N}$ が存在して $ca \equiv_n 1$ なら $\gcd(a, n) = 1$.

証明. $ca \equiv_n 1$ なら，ある $m \in \mathbb{N}$ が存在して $ca - mn = 1$．$d = \gcd(a, n)$ とする．このとき，$d|a$ かつ $d|n$．よって，$d|(ca - mn)$，つまり，$d|1$．これは $d = 1$ を意味する． ■

この主張より（$c = a^{k-1}$ とすれば），$\gcd(a, n) = 1$，つまり，$a \in \mathbb{Z}_n^*$ となる． ■

入力：自然数 n

1. 以下を k 回繰り返す.
   (a) 一様ランダムに $a \in \mathbb{Z}_n \setminus \{0\}$ を選ぶ.
   (b) $a^{n-1} \not\equiv_n 1$ であるなら `NO` を出力して終了する.
2. `YES` を出力する.

図 6: フェルマーテスト

注 4.9. 命題 4.22 より，ステップ 1-(a) にて $a \notin \mathbb{Z}_n^*$（つまり，$\gcd(n, a) \neq 1$）である $a \in \mathbb{Z}_n$ が選ばれたら，ステップ 1-(b) で `NO` が出力される．

定理 4.11. 図 6 のアルゴリズムを A とする．このとき，$n \in \mathbb{N}$ がカーマイケル数でないならば，

$$\begin{aligned} n \in \mathrm{PRIME} \quad &: \quad \Pr\{A(n) = \texttt{YES}\} = 1, \\ n \notin \mathrm{PRIME} \quad &: \quad \Pr\{A(n) = \texttt{YES}\} \leq 1/2^k. \end{aligned}$$

注 4.10. よって，フェルマーテストは，入力がカーマイケル数でない場合に限り有効な素数判定アルゴリズムになる．

証明. $n \in \mathrm{PRIME}$ のとき,（$a \not\equiv_n 0$ から）フェルマーの小定理より，アルゴリズムのステップ 1-(b) の条件を満たすことはない．これより，確率 1 で `YES` を出力する．

$n \notin \mathrm{PRIME}$ のとき，$F_n \stackrel{\mathrm{def}}{=} \{a \in \mathbb{Z}_n^* : a^{n-1} \equiv_n 1\}$ とする．

主張 4.7. $|F_n| \leq |\mathbb{Z}_n^*|/2$.

証明. n がカーマイケル数でないことから，$F_n \neq \mathbb{Z}_n^*$．よって，ラグランジュの定理より，$(F_n, \cdot)$ が群であることを示せばよい．(F_n が $\mathbb{Z}_n^*$ の真部分集合となるので.) ■

問 4.25. この主張の証明を完成させなさい．(つまり，F_n が群であることを示しなさい．命題 4.15 より，$\mathbb{Z}_n^*$ は群である.)

この主張より，アルゴリズムのステップ 1 の一回の繰り返しにおいて，ステップ (b) の条件が満たされない（つまり，$a \in F_n$ である）確率は，

$$\begin{aligned} \Pr_{a \in \mathbb{Z}_n \setminus \{0\}} \{a \in F_n\} &\leq \Pr_{a \in \mathbb{Z}_n^*} \{a \in F_n\} \quad (\because \text{命題 4.22}) \\ &= \frac{|F_n|}{|\mathbb{Z}_n^*|} \\ &\leq \frac{1}{2} \quad (\because \text{上の主張}). \end{aligned}$$

ステップ 1 の繰り返しは各回独立であるので，すべての繰り返しでステップ (b) の条件が満たされない確率は，高々 $(1/2)^k$ である．この確率はアルゴリズムが YES を出力する確率である． ■

4.4 ソロベイ・シュトラッセンテスト

ここでは，カーマイケル数も扱える（条件なしの）素数性判定アルゴリズムを示す[4].

定義 4.14

n を自然数とする．自然数 a（ただし $\gcd(n, a) = 1$）が n **を法として平方剰余**であるとは，以下を満たすことである．

$$\exists x \in \mathbb{Z}_n^* [a \equiv_n x^2].$$

定理 4.12 (オイラー基準)**.** $p \geq 3$ を素数とする．このとき，任意の $a \in \mathbb{Z}_p^*$ について，

$$\begin{aligned} a \text{ が } p \text{ を法として平方剰余である} &: a^{\frac{p-1}{2}} \equiv_p 1 \\ a \text{ が } p \text{ を法として平方剰余でない} &: a^{\frac{p-1}{2}} \equiv_p -1 \end{aligned}$$

証明. a が平方剰余であるとする．このとき，ある $x \in \mathbb{Z}_p^*$ が存在して $a \equiv_p x^2$ である．よって，($a \equiv_p x^2$ の両辺を $(p-1)/2$ 乗して)

$$a^{\frac{p-1}{2}} \equiv_p (x^2)^{\frac{p-1}{2}} \equiv_p x^{p-1} \equiv_p 1. \quad (\because x \not\equiv_p 0 \text{ よりフェルマーの小定理})$$

a が平方剰余でないとする．任意の $b \in \mathbb{Z}_p^*$ について，x についての方程式 $bx \equiv_p a$ の解は，($(\mathbb{Z}_p^*, *)$ が群であり，b^{-1} を b の逆元とすれば $x = b^{-1} * a$ より) $x \in \mathbb{Z}_p^*$ であり，(a が平方剰余でないことより) $x \neq b$ である．このことから，$\mathbb{Z}_p^*$ は $(p-1)/2$ 個の組に分割できる．つまり，

$$\{(b, c) \in \mathbb{Z}_p^* \times \mathbb{Z}_p^* : b \neq c,\ bc \equiv_p a\}$$

[4] ミラー・ラビン（Miller-Rabin）テスト，と呼ばれる素数性判定アルゴリズムもある.(次節参照.)

このことから，

$$(p-1)! \equiv_p a^{\frac{p-1}{2}}.$$

よって，ウィルソンの定理（p が素数であれば $(p-1)! \equiv_p -1$）より，$a^{\frac{p-1}{2}} \equiv_p -1$. ■

事実 4.23. この定理は，（任意の $a \in \mathbb{Z}_p^*$ に対してだけでなく）$\gcd(p,a)=1$ である任意の自然数 a について成り立つ．一方，$\gcd(p,a) \neq 1$ である $a \in \mathbb{N}$ については，$a^{\frac{p-1}{2}} \equiv_p 0$.

問 4.26. この事実を証明しなさい.

系 4.24. $p \geq 3$ を素数とする．このとき，$\mathbb{Z}_p^*$ の任意の生成元 $g \in \mathbb{Z}_p^*$ について，g は p を法として平方剰余でない.

証明. g は生成元であるこから，$g^{\frac{p-1}{2}} \neq_p 1$．定理より，$g$ は p を法として平方剰余でない. ■

定義 4.15

$p \geq 3$ を素数とする．任意の自然数 a について，

$$\left[\frac{a}{p}\right] \stackrel{\text{def}}{=} \begin{cases} 0 & : \ \gcd(p,a) \neq 1 \\ \begin{cases} 1 & : \ a \text{ が } p \text{ を法として平方剰余} \\ -1 & : \ \text{o.w.} \end{cases} & : \ \gcd(p,a)=1 \end{cases}$$

上記の左辺を**ルジャンドル記号**という.

事実 4.25. $p \geq 3$ を素数とする．任意の自然数 a について，

$$\left[\frac{a}{p}\right] = a^{\frac{p-1}{2}} \pmod{p}.$$

命題 4.26. $p \geq 3$ を素数とする．任意の自然数 a,b について，

$$\left[\frac{ab}{p}\right] \equiv_p \left[\frac{a}{p}\right]\left[\frac{b}{p}\right].$$

命題 4.27. $p \geq 3$ を素数とする．任意の自然数 a,b について，$a \equiv_p b$ なら，

$$\left[\frac{a}{p}\right] \equiv_p \left[\frac{b}{p}\right].$$

問 4.27. 上の二つの命題を証明しなさい.

定義 4.16

$n \geq 3$ を奇数とする．n の素因数分解を $n = p_1^{k_1} \dots p_t^{k_t}$ とする．($p_1, \dots, p_t \geq 3$.) 任意の自然数 a について，

$$\left[\frac{a}{n}\right] \stackrel{\text{def}}{=} \prod_{i \in [t]} \left[\frac{a}{p_i}\right]^{k_i}.$$

上記の左辺を**ヤコビ記号**という．(右辺はルジャンドル記号の積である.)

事実 4.28. $n \geq 3$ を奇数とする．任意の自然数 a について，$\left[\frac{a}{n}\right] \in \{-1, 0, 1\}$．また，$\left[\frac{a}{n}\right] = 0$ は $\gcd(n, a) \neq 1$ に同値である．

問 4.28. この事実を証明しなさい.

注 4.11. n と互いに素な任意の自然数 a について，$\left[\frac{a}{n}\right] = -1$ のとき，(オイラー基準と同様) a は (n を方として) 平方剰余**でない**．一方，$\left[\frac{a}{n}\right] = 1$ のとき，a は平方剰余であるとは**限らない**.

命題 4.29. ヤコビ記号について，以下の等式が成り立つ.

1. $\left[\frac{ab}{n}\right] = \left[\frac{a}{n}\right]\left[\frac{b}{n}\right]$.
2. $a \equiv_n b$ のとき，$\left[\frac{a}{n}\right] = \left[\frac{b}{n}\right]$.
3. $\gcd(n, a) = 1$ である奇数 n, a について，$\left[\frac{a}{n}\right] = (-1)^{\frac{n-1}{2}\frac{a-1}{2}}\left[\frac{n}{a}\right]$.
4. $\left[\frac{1}{n}\right] = 1$.
5. $\left[\frac{2}{n}\right] = \begin{cases} -1 & : \ n \equiv_8 3, 5 \\ 1 & : \ n \equiv_8 1, 7 \end{cases}$

証明. ■

問 4.29. 上の命題のうち，1, 2 の等式を証明しなさい.(ヒント：命題 4.26, 4.27.)

系 4.30. $n \geq 3$ を奇数とする．任意の $a \in \mathbb{Z}_n^*$ について，$\left[\frac{a}{n}\right]$ を (入力の大きさ $\log n, \log a$ の) 多項式時間で求めることができる.

証明. まず，(以降で) 命題の条件 3 を適用する場合，n が (もともと) 奇数であるので，(適用するときの) n が奇数になることに注意する.

a が偶数であるなら，命題の条件 1 を適用する．$a < n$ であるなら，命題の条件 3 を適用する.(そうすれば，$a \geq n$ となる.) そうでないなら，$a = qn + b$ として，$a \equiv_n b$ より，命題の条件 2 を適用する．以上を繰り返し適用すれば，最後は，命題の条件 4, 5 が適用できる． ■

問 4.30. $n = 123$, $a = 50$ として，$\left[\frac{a}{n}\right]$ の値を求めなさい．

入力：自然数 n

1. 以下を k 回繰り返す．
   (a) 一様ランダムに $a \in \mathbb{Z}_n \setminus \{0\}$ を選ぶ．
   (b) $b \stackrel{\text{def}}{=} [\frac{a}{n}]$ を求める．
   (c) $b = 0$ または $b \not\equiv_n a^{\frac{n-1}{2}}$ であるなら NO を出力して終了する．
2. YES を出力する．

図 7: ソロベイ・シュトラッセンテスト

注 4.12. ステップ 1-(c) にて，$b = 0$ であることは $\gcd(n, a) \neq 1$ に同値である．

定理 4.13. 図 7 のアルゴリズムを A とする．このとき，

$$\begin{aligned} n \in \text{PRIME} \quad &: \quad \Pr\{A(n) = \texttt{YES}\} = 1, \\ n \notin \text{PRIME} \quad &: \quad \Pr\{A(n) = \texttt{YES}\} \leq 1/2^k. \end{aligned}$$

証明. $n \in$ PRIME のとき，($b \neq 0$ であり）事実 4.25 より，アルゴリズムのステップ 1-(c) の条件を満たすことはない．つまり，NO を出力することはない．よって，確率 1 で YES を出力する．

$n \notin$ PRIME のとき，一般性を失うことなく $b \neq 0$ とする．つまり，$a \in \mathbb{Z}_n^*$ とする．$J_n \stackrel{\text{def}}{=} \{a \in \mathbb{Z}_n^* : [\frac{a}{n}] \equiv_n a^{\frac{n-1}{2}}\}$ とする．

主張 4.8. $|J_n| \leq |\mathbb{Z}_n^*|/2$.

証明. J_n が群であることは容易に確かめられる．(下の問を参照.）よって，ラグランジュの定理より，$J_n \subsetneq Z_n^*$ であることを示せばよい．

背理法により証明する．つまり，$J_n = \mathbb{Z}_n^*$ とする．n の素因数分解を $n = p_1^{k_1} p_2^{k_2} \ldots p_t^{k_t}$ とする．$q \stackrel{\text{def}}{=} p_1^{k_1}$, $m \stackrel{\text{def}}{=} n/q$ とする．g を $\mathbb{Z}_q^*$ の生成元とする．(定理 4.2 より，生成元の存在は保証される.）中国人剰余定理より，($g \in \mathbb{Z}_q$, $1 \in \mathbb{Z}_m$ に対して）ある $a \in \mathbb{Z}_n$ が存在して，

$$\begin{aligned} a \quad &\equiv_q \quad g \\ a \quad &\equiv_m \quad 1 \end{aligned} \tag{1}$$

ここで，$\gcd(n, a) = 1$，つまり，$a \in \mathbb{Z}_n^*$ である．($a \equiv_q g$ より $a \equiv_{p_1} g \not\equiv_{p_1} 0$，更に，$a \equiv_m 1$ より任意の $i \in [t] \setminus \{1\}$ について $a \equiv_{p_i} 1$ であることから，任意の $i \in [t]$ について $a \not\equiv_{p_i} 0$，なので.）

以下，$k_1 = 1$ かどうかで場合分けをして示す．まず，$k_1 \geq 2$ のとき，$J_n = \mathbb{Z}_n^*$（背理法の仮定）より（$a^{\frac{n-1}{2}} \equiv_n [\frac{a}{n}] \in \{-1, 1\}$ なので[5]），

$$a^{\frac{n-1}{2}} \equiv_n \pm 1 \implies a^{n-1} \equiv_n 1 \implies a^{n-1} \equiv_q 1 \quad (\because\ q|n)$$

[5] n が合成数であれば，必ずしも $a^{\frac{n-1}{2}} \equiv_n \pm 1$ とはならない．(n が素数であればそうなる．(オイラー基準より.))

更に，(1) の $a \equiv_q g$ より（$a^{n-1} \equiv_q g^{n-1}$ であるから）$g^{n-1} \equiv_q 1$．これより，(g は $\mathbb{Z}_q^*$ の生成元であるから）$\phi(q)|(n-1)$．また，オイラーの積公式（命題 4.19）より（$k_1 \geq 2$ であるから）$p_1|\phi(q)$ である．よって，$p_1|(n-1)$．これより，$p_1|(n-1)$ かつ（$q|n$ より）$p_1|n$．これは，どのような素数も $n-1$ と n の両方を割り切ることはないという事実に矛盾する．

次に，$k_1 = 1$ のとき（つまり，$q = p_1$ のとき），

$$\begin{aligned}
\left[\frac{a}{n}\right] &= \prod_{i\in[t]} \left[\frac{a}{p_i}\right]^{k_i} \\
&= \left[\frac{a}{q}\right] \cdot \prod_{i\in[t]\setminus\{1\}} \left[\frac{a}{p_i}\right]^{k_i} \\
&= \left[\frac{g}{q}\right] \cdot \prod_{i\in[t]\setminus\{1\}} \left[\frac{a}{p_i}\right]^{k_i} \quad (\because\ a \equiv_q g) \\
&= \left[\frac{g}{q}\right] \cdot \prod_{i\in[t]\setminus\{1\}} \left[\frac{1}{p_i}\right]^{k_i} \quad (\because\ a \equiv_m 1,\ \forall i \in [t]\setminus\{1\}[p_i|m] \text{ より } a \equiv_{p_i} 1) \\
&= \left[\frac{g}{q}\right]
\end{aligned}$$

また，系 4.24 より，$\left[\frac{g}{q}\right] = -1$．よって，$\left[\frac{a}{n}\right] = \left[\frac{g}{q}\right] = -1$．$J_n = \mathbb{Z}_n^*$（背理法の仮定）より，任意の $b \in \mathbb{Z}_n^*$ について $\left[\frac{b}{n}\right] \equiv_n b^{\frac{n-1}{2}}$ であることから，($\left[\frac{a}{n}\right] \equiv_n a^{\frac{n-1}{2}}$ であり）

$$a^{\frac{n-1}{2}} \equiv_n -1.$$

$m|n$ より，

$$a^{\frac{n-1}{2}} \equiv_m -1.$$

これは，(1) の $a \equiv_m 1$ に矛盾する．いずれの場合（$k_1 = 1$ かどうか）にも矛盾が生じることから，$J_n \neq \mathbb{Z}_n^*$. ■

問 4.31. $(J_n, \cdot)$ が群であることを示しなさい．

この主張より，アルゴリズムのステップ 1 の一つの繰り返しにおいて，ステップ (c) の条件が満たされない確率は高々 1/2 である．ステップ 1 の繰り返しは各回独立であるので，($b \neq 0$ である条件のもと）すべての繰り返しでステップ (c) の条件が満たされない（条件付き）確率は，高々 $(1/2)^k$ である．この確率はアルゴリズムが `YES` を出力する確率である． ■

4.5 ミラー・ラビンテスト

ここでは，ソロベイ・シュトラッセンテストよりも効率の良い（誤り確率の小さい）素数性判定アルゴリズムを示す．

命題 4.31. $p \geq 3$ を任意の素数とする．$p - 1 = 2^s t$（ただし t は奇数）とする．($s \geq 1$.）このとき，任意の $a \in \mathbb{Z}_p^*$ について，以下を満たす．

$$a^t \equiv_p 1 \quad \vee \quad a^t \equiv_p -1 \quad \vee \quad \exists i \in [s-1] \left[a^{2^i t} \equiv_p -1\right]. \tag{2}$$

証明. 任意の $a \in \mathbb{Z}_p^*$ について，

$$\begin{aligned} 0 &\equiv_p a^{p-1} - 1 \quad (\because \text{フェルマーの小定理}) \\ &= a^{2^s t} - 1 \\ &= (a^{2^{s-1}t} - 1)(a^{2^{s-1}t} + 1) \\ &\vdots \\ &= (a^t - 1)(a^t + 1)(a^{2^1 t} + 1)(a^{2^2 t} + 1) \cdots (a^{2^{s-1}t} + 1) \\ &= (a^t - 1)(a^{2^0 t} + 1)(a^{2^1 t} + 1)(a^{2^2 t} + 1) \cdots (a^{2^{s-1}t} + 1). \end{aligned}$$

この等式より，命題の条件を満たす[6]ことは明らか． ■

注 4.13. この命題の逆が成り立つことが以降で示される．つまり，n が合成数であるとき，ある $a \in \mathbb{Z}_n^*$ が存在して，命題 4.31 の条件 (2) が満たされない．ただし，そのような $a \in \mathbb{Z}_n^*$ の個数の割合が素数判定の効率のよさになる．

$n \geq 3$ を任意の**奇数**とする．以降，任意の $a \in \mathbb{Z}_n^*$ に対して，命題 4.31 の条件 (2) を $\texttt{MR-liar}(n, a)$ と表記する．つまり，$n - 1 = 2^s t$（t が奇数，よって，$s \geq 1$）としたとき，

$$\texttt{MR-liar}(n, a) \quad \stackrel{\text{def}}{=} \quad a^t \equiv_n 1 \ \vee \ a^t \equiv_n -1 \ \vee \ \exists i \in [s-1] \left[a^{2^i t} \equiv_n -1 \right].$$

事実 4.32. 任意の $a \in \mathbb{Z}_n^*$ に対して，$\texttt{MR-liar}(n, a)$ が成り立てば $a^{n-1} \equiv_n 1$.

問 4.32. この事実が成り立つ理由を説明しなさい．

入力：自然数 n // 奇数であるとする

1. 以下を k 回繰り返す．
   (a) 一様ランダムに $a \in \mathbb{Z}_n \setminus \{0\}$ を選ぶ．
   (b) $n - 1 = 2^s t$ とする．$\texttt{MR-liar}(n, a) = \texttt{false}$ なら NO を出力して終了する．
2. YES を出力する．

図 8: ミラー・ラビンテスト

注 4.14. フェルマーテストと同様，注 4.9 にあるよう，命題 4.22 より，ステップ 1-(b) では $a \in \mathbb{Z}_n^*$ としてよい[7]．

問 4.33. この注の事実が成り立つ理由を説明しなさい．

[6] p が素数であるので．
[7] ステップ 1-(a) にて $a \notin \mathbb{Z}_n^*$ である $a \in \mathbb{Z}_n$ が選ばれたら，ステップ 1-(b) で NO が出力される．

定理 4.14. 図 8 のアルゴリズムを A とする．このとき，

$$\begin{aligned} n \in \mathrm{PRIME} &: \Pr\{A(n) = \texttt{YES}\} = 1, \\ n \notin \mathrm{PRIME} &: \Pr\{A(n) = \texttt{YES}\} \leq 1/4^k. \end{aligned}$$

証明. $n \in \mathrm{PRIME}$ のとき，命題 4.31 より，アルゴリズムのステップ 1-(b) の条件を満たすことはない．つまり，NO を出力することはない．よって，確率 1 で YES を出力する．

以降，$n \notin \mathrm{PRIME}$（更に n は奇数）のとき，アルゴリズムが YES を出力する確率を見積もる．つまり，以下が満たされることを示す[8]：

$$\Pr_{a \in \mathbb{Z}_n^*}\{\texttt{MR-liar}(n,a) = \texttt{true}\} \ \leq \ 1/4. \tag{3}$$

合成数 n の素因数分解を $n = p_1^{e_1} \dots p_r^{e_r}$ とする．($p_1, \dots, p_r \geq 3, r \geq 1$.) まず，$r = 1$ のとき，つまり，$n = p^e$（$p \geq 3, e > 1$）のときを考える．

主張 4.9. 任意の $a \in \mathbb{Z}_n^*$ について，$\texttt{MR-liar}(n,a)$ が成り立てば $a^{p-1} \equiv_{p^e} 1$ が成り立つ[9].

証明. $\texttt{MR-liar}(n,a)$ が成り立つことから，事実 4.32 より $a^{p^{e-1}} \equiv_{p^e} 1$．また，オイラーの定理（定理 4.8）より，$a^{p^{e-1}(p-1)} \equiv_{p^e} 1$．このとき，$\gcd(p^e - 1, p^{e-1}(p-1)) = p - 1$.

問 4.34. この事実を証明しなさい.（ヒント：$p^e - 1 = (p-1)(p^{e-1} + \cdots)$.）

よって，命題 4.17 より，$a^{p-1} \equiv_{p^e} 1$. ■

$S = \{a \in \mathbb{Z}_n^* : a^{p-1} \equiv_{p^e} 1\}$ とする．このとき，S は巡回群となる．

問 4.35. この事実を証明しなさい.（ヒント：定理 4.2 と命題 4.10 を用いる.）

S の生成元を $g \in S$ とすれば，$S = \langle g \rangle$．このとき，$g^{p-1} \equiv_n 1$．よって，$|S| = p - 1$ となる．

問 4.36. この事実が成り立つ理由を説明しなさい.

以上より[10]，

$$\begin{aligned} \Pr_{a \in \mathbb{Z}_n^*}\{\texttt{MR-liar}(n,a) = \texttt{true}\} &\leq \Pr_{a \in \mathbb{Z}_n^*}\{a^{p-1} \equiv_{p^e} 1\} \\ &= \frac{|S|}{|\mathbb{Z}_n^*|} = \frac{p-1}{\phi(p^e)} = \frac{p-1}{p^{e-1}(p-1)} = \frac{1}{p^{e-1}} \\ &\leq 1/4. \quad (\because\ p > 3) \end{aligned}$$

よって，$r = 1$ のとき，不等式 (3) が満たされることが示された．以降，$r \geq 2$ のときを考える．まず，以下のように非負整数 b を定義する．

$$b \stackrel{\text{def}}{=} \max\left\{ i \in [s-1]_0 : \exists a \in \mathbb{Z}_n^* \left[a^{2^i t} \equiv_n -1 \right] \right\}.$$

[8] 注 4.14 より，$a \in \mathbb{Z}_n^*$ としてよい

[9] 実際，この逆も成り立つ．更に，$r > 1$ の場合，$e_i > 1$ である $\mathbb{Z}_{q_i}^*$（$q_i = p_i^{e_i}$）について成り立つ．

[10] この場合だけ $p \geq 3$ とする．こうしても一般性を失わない．

次に，L_n, G_n, H_n を以下のように定義する．

$$\begin{aligned} L_n &\stackrel{\text{def}}{=} \{a \in \mathbb{Z}_n^* : \texttt{MR-liar}(n,a) = \texttt{true}\}, \\ G_n &\stackrel{\text{def}}{=} \left\{a \in \mathbb{Z}_n^* : a^{2^b t} \equiv_n \pm 1\right\}, \\ H_n &\stackrel{\text{def}}{=} \left\{a \in \mathbb{Z}_n^* : \forall i \in [r]\left[a^{2^b t} = \pm 1 \pmod{p_i^{e_i}}\right]\right\}. \end{aligned}$$

事実 4.33. $(G_n, \cdot)$, $(H_n, \cdot)$ は群となる．（$(F_n, \cdot)$, $(\mathbb{Z}_n^*, \cdot)$ は群である[11]．）

問 4.37. この事実を示しなさい．

事実 4.34. $L_n \subseteq G_n \subseteq H_n \subseteq F_n \subseteq \mathbb{Z}_n^*$.

問 4.38. この事実を証明しなさい．

以下，$|G_n|/|H_n| = 1/2^{r-1}$（$r \geq 2$）を示す．そのために，以下のような関数 $f : H_n \to \{-1,+1\}^r$ を考える．任意の $a \in H_n$ について，

$$f(a) \stackrel{\text{def}}{=} (a_1, \ldots, a_r), \quad \text{ただし，} a_i = a^{2^b t} \pmod{p_i^{e_i}}.$$

主張 4.10. $f : H_n \to \{-1,+1\}^r$ は準同型写像である．つまり，任意の $a, a' \in H_n$ について，$f(aa' \pmod n) = f(a)f(a') \stackrel{\text{def}}{=} (a_1 a'_1, \ldots, a_r a'_r)$.

問 4.39. この主張を証明しなさい．

主張 4.11. $f : H_n \to \{-1,+1\}^r$ は全射である．

証明. 任意の $(a'_1, \ldots, a'_r) \in \{(a_1, \ldots, a_r) \in \{-1,+1\}^r : \exists! i \in [r][a_i = -1]\}$ について，ある $a' \in H_n$ が存在して $f(a') = (a'_1, \ldots, a'_r)$ を示せばよい．

問 4.40. その理由を説明しなさい．（f が準同型写像であることを用いる．）

対称性より，ある $a' \in H_n$ が存在して $f(a') = (-1, 1, \ldots, 1)$ であることを示せばよい．まず，b の定義より，ある $c \in \mathbb{Z}_n^*$ が存在して，$c^{2^b t} = -1 \pmod{p_1^{e_1}}$．中国人剰余定理（系 4.18）より，ある $a' \in \mathbb{Z}_n^*$ が存在して，

$$\begin{aligned} a' &= c \pmod{p_1^{e_1}}, \\ a' &= 1 \pmod{p_i^{e_i}}, \quad \text{for } i \geq 2. \end{aligned}$$

これより，

$$\begin{aligned} a'^{2^b t} &= c^{2^b t} = -1 \pmod{p_1^{e_1}}, \\ a'^{2^b t} &= 1^{2^b t} = 1 \pmod{p_i^{e_i}}, \quad \text{for } i \geq 2. \end{aligned}$$

これは $f(a') = (-1, 1, \ldots, 1)$ を意味する． ■

[11] $(L_n, \cdot)$ が群になるとは限らない．

この主張より，$f(H_n) = \{-1,+1\}^r$．準同型定理（定理 4.15）より，H_n/K_n と $\{-1,+1\}^r$ は同型となる．ただし，

$$K_n \stackrel{\text{def}}{=} \{a \in H_n : f(a) = (1,\ldots,1)\}.$$

特に，$|H_n|/|K_n| = 2^r$，$|G_n|/|K_n| = 2$．よって，

$$\frac{|G_n|}{|H_n|} = \frac{|K_n|}{|H_n|}\frac{|G_n|}{|K_n|} = \frac{1}{2^r}\cdot 2 = \frac{1}{2^{r-1}}.$$

以上より，$|G_n|/|H_n| = 1/2^{r-1}$（$r \geq 2$）が示された．n がカーマイケル数**でない**とき，$F_n \subsetneq \mathbb{Z}_n^*$ より，$|F_n|/|\mathbb{Z}_n^*| \leq 1/2$．よって，

$$\frac{|L_n|}{|Z_n^*|} \leq \frac{|G_n|}{|Z_n^*|} = \frac{|G_n|}{|H_n|}\frac{|H_n|}{|\mathbb{Z}_n^*|} \leq \frac{|G_n|}{|H_n|}\frac{|F_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2^{r-1}}\frac{1}{2} = \frac{1}{2^r}.$$

よって，$|L_n|/|Z_n^*| \leq 1/4$.（$r \geq 2$.）最後に，n がカーマイケル数**である**ときを考える．この場合，コルセルト判定（の系 4.21）より，$r \geq 3$．よって，$|L_n|/|Z_n^*| \leq |G_n|/|H_n| \leq 1/2^{r-1} \leq 1/4$. ■

定理 4.15 (準同型定理)**.** $f : A \to B$ を「B の上への」（つまり，$f(A) = B$）準同型写像とする．K を f の核とする.（つまり，$K = \{a \in A : f(a) = 1\}$.）このとき，$A/K$ と B は同型である.

4.6 SS-test vs. MR-test*

ここでは，素数性判定の成功確率について，ミラー・ラビンテスト（MR-test）がソロベイ・シュトラッセンテスト（SS-test）以上であることを示す．以下，n を合成数とする．それぞれの素数性判定テストについて，以下の集合を考える．

$$\begin{aligned}\texttt{SS}(n) &\stackrel{\text{def}}{=} \{a \in \mathbb{Z}_n^* : \left[\tfrac{a}{n}\right] \equiv_n a^{\frac{n-1}{2}}\},\\ \texttt{MR}(n) &\stackrel{\text{def}}{=} \{a \in \mathbb{Z}_n^* : \texttt{MR-liar}(n,a) = \texttt{true}\}.\end{aligned}$$

命題 4.35. 任意の奇数 $n \geq 3$ について，

$$\left[\frac{-1}{n}\right] = (-1)^{\frac{n-1}{2}}.$$

証明. $n = p_1^{k_1}\cdots p_t^{k_t}$ とする.（$p_i \geq 3$.）ヤコビ記号の定義，更に，事実 4.25 より，

$$\begin{aligned}\left[\frac{-1}{n}\right] &= \prod_{i\in[t]}\left[\frac{-1}{p_i}\right]^{k_i} = \prod_{i\in[t]}\left((-1)^{\frac{p_i-1}{2}} \bmod p_i\right)^{k_i} = \prod_{i\in[t]}\left((-1)^{\frac{p_i-1}{2}}\right)^{k_i}\\ &= (-1)^{\sum_i (p_i-1)k_i/2}.\end{aligned}$$

主張 4.12. 任意の奇数 $a, b > 0$ について，

$$(a-1)/2 + (b-1)/2 \equiv_2 (ab-1)/2.$$

問 4.41. この主張を証明しなさい.

この主張より,

$$\sum_{i\in[t]}(p_i-1)k_i/2 \ \equiv_2 \ (n-1)/2.$$

問 4.42. この合同式が成り立つ理由を説明しなさい.

よって,

$$\left[\frac{-1}{n}\right] \ = \ (-1)^{\sum_i (p_i-1)k_i/2} \ = \ (-1)^{\frac{n-1}{2}}.$$

■

定理 4.16. n を奇数の合成数とする．このとき，$\mathtt{MR}(n) \subseteq \mathtt{SS}(n)$.

注 4.15. $a \in \mathtt{SS}(n)$, $a \in \mathtt{MR}(n)$ は，それぞれの素数性判定が（一度の繰り返しで）失敗する事象である．これより，成功確率に関して，ミラー・ラビンテスト（MR-test）がソロベイ・シュトラッセンテスト（SS-test）以上であるといえる.

証明. $n-1 = 2^s t$ とする.（ただし，t は奇数．よって，$s \geq 1$.）任意に $a \in \mathtt{MR}(n)$ を固定する．このとき，$\mathtt{MR\text{-}liar}(n,a) = \mathtt{true}$．以下，$a \in \mathtt{SS}(n)$ を示す．まず，$s = 1$ の場合，$a^{\frac{n-1}{2}} = a^t \equiv_n \pm 1$. よって，$\epsilon \stackrel{\text{def}}{=} a^{\frac{n-1}{2}} \pmod n$ とすれば，$\left[\frac{a}{n}\right] = \pm 1$ より,

$$\begin{aligned}
\left[\frac{a}{n}\right] &= \left[\frac{a}{n}\right]^{\frac{n-1}{2}} \quad (\because\ (n-1)/2 = t \text{ が奇数}) \\
&= \left[\frac{a^{\frac{n-1}{2}}}{n}\right] \quad (\because\ \text{命題 4.29 の 1}) \\
&= \left[\frac{\epsilon}{n}\right] \quad (\because\ \text{命題 4.29 の 2}) \\
&= \epsilon. \quad (\because\ \text{命題 4.29 の 4 と命題 4.35})
\end{aligned}$$

問 4.43. 最後の等式が成り立つ理由を説明しなさい.

よって，$s = 1$ のとき，$\left[\frac{a}{n}\right] \equiv_n a^{\frac{n-1}{2}}$．次に，$s > 1$ の場合を考える．ある非負整数 $b : 0 \leq b \leq s-1$ について $a^{2^b t} \equiv_n -1$ とする.（よって， $a^{2^{b+1}t} \equiv_n 1$.）b の定義より，以下を示せばよい[12].

$$\left[\frac{a}{n}\right] \ = \ \begin{cases} -1 & : \ b = s-1 \\ 1 & : \ b < s-1 \end{cases}$$

問 4.44. これを示せばよい理由を説明しなさい.

[12] よって，$s > 1$ である必要がある.

$p|n$ である任意の素数 p について，$k_p \stackrel{\text{def}}{=} \max\{k : p^k|n\}$.（よって，$n = \prod_{p|n} p^{k_p}$.）このとき，

$$\left[\frac{a}{n}\right] \;=\; \prod_{p|n}\left[\frac{a}{p}\right]^{k_p} \;=\; \prod_{p|n}\left(a^{\frac{p-1}{2}}\right)^{k_p}.$$

$p|n$ である任意の素数 p について，$p-1 = 2^{s_p}t_p$ とする.（ただし，t_p は奇数．よって，$s_p \geq 1$.）

主張 4.13. $b < s_p$.

証明. $a^{2^b t} \equiv_n -1$ より，$a^{2^b t} \equiv_p -1$．これより，$a^{2^{b+1}t} \equiv_p 1$．よって，$c \stackrel{\text{def}}{=} a^t \pmod p \in \mathbb{Z}_p^*$ とすれば，$c^{2^{b+1}} \equiv_p 1$．これは，$c \in \mathbb{Z}_p^*$ の位数が 2^{b+1} であることを意味する．

問 4.45. この事実が成り立つ理由を説明しなさい.（ヒント：もしそうでなければ，c の位数は $2^{b'}$（$b' \leq b$）となる.）

よって，$2^{b+1}|(p-1)$，つまり，$2^{b+1}|2^{s_p}t_p$．よって，$b+1 \leq s_p$. ■

この主張より,（$p|n$ である任意の素数 p について）$b = s_p - 1$ か $b < s_p - 1$．前者である素数 p の集合を S とする．つまり，$S \stackrel{\text{def}}{=} \{p : p|n, b = s_p - 1\}$．このとき，

$$\left[\frac{a}{n}\right] \;=\; \prod_{p|n}\left(a^{\frac{p-1}{2}}\right)^{k_p} \;=\; \prod_{p\in S}(-1)^{k_p} \;=\; (-1)^{\sum_{p\in S} k_p}.$$

問 4.46. 二つ目の等式が成り立つ理由を説明しなさい.

これより，以下を示せばよい.

$$\sum_{p\in S} k_p \;=\; \begin{cases} \text{奇数} & : \; b = s-1 \\ \text{偶数} & : \; b < s-1 \end{cases}$$

一方，$n = \prod_{p|n} p^{k_p}$ より,

$$n \;=\; \prod_{p|n}(1+2^{s_p}t_p)^{k_p} \;\equiv_{2^{b+2}}\; \prod_{p\in S}(1+2^{b+1}t_p)^{k_p}.$$

問 4.47. 最後の合同式が成り立つ理由を説明しなさい.

よって,

$$\begin{aligned} n \;&\equiv_{2^{b+2}}\; \prod_{p\in S}(1+2^{b+1}t_p)^{k_p} \\ &\equiv_{2^{b+2}}\; 1 + \left(\sum_{p\in S} t_p k_p\right) 2^{b+1} \\ &\equiv_{2^{b+2}}\; 1 + \left(\sum_{p\in S} k_p\right) 2^{b+1}. \end{aligned}$$

問 4.48. 最後の二つの合同式が成り立つ理由を説明しなさい.

よって,

$$n-1 \equiv_{2^{b+2}} \left(\sum_{p\in S} k_p\right) 2^{b+1}.$$

$b = s-1$ のとき，$n-1 = 2^s t$ より,

$$2^s t \equiv_{2^{s+1}} \left(\sum_{p\in S} k_p\right) 2^s.$$

よって，$\sum_{p\in S} k_p$ は奇数となる.（$\left[\frac{a}{n}\right] = -1$.）$b < s-1$ のとき,

$$\begin{aligned} 2^s t \equiv_{2^{b+2}} \left(\sum_{p\in S} k_p\right) 2^{b+1} &\iff 2^{b+2} \mid \left(2^{s-(b+1)} t - \sum_{p\in S} k_p\right) 2^{b+1} \\ &\iff 2 \mid \left(2^{s-(b+1)} t - \sum_{p\in S} k_p\right). \end{aligned}$$

よって，$s-(b+1) \geq 1$ より，$\sum_{p\in S} k_p$ は偶数となる.（$\left[\frac{a}{n}\right] = 1$.） ■

4.7 成功確率の増幅

ここでは，素数を利用した[13]成功確率の増幅手法を示す[14]．以下のような（言語 L のための[15]）乱択アルゴリズム A（$|r| = \ell$）を考える.

$$\begin{aligned} x \in L &: \Pr_{r\in\{0,1\}^\ell}\{A(x,r) = \texttt{YES}\} = 1, \\ x \notin L &: \Pr_{r\in\{0,1\}^\ell}\{A(x,r) = \texttt{YES}\} \leq 1/4. \end{aligned}$$

以降，$|x| = n$ とする.（よって，$\ell = n^{O(1)}$.）

事実 4.36. $A(x,r)$ を（独立に）k 回繰り返すことにより，$x \notin L$ の場合，A の誤り確率は $1/4^k$ に減少する．つまり，成功確率は $1-1/4^k$ に増幅される．ただし，その増幅に必要なランダムビット長は $\ell \cdot k$ となる.（$x \in L$ の場合，成功確率は 1 のまま.）

以下，この単純な成功確率の増幅より効率のよい増幅手法を示す．以下のように $B_0, B_1 \subseteq \{0,1\}^\ell$ を定義する.

$$\begin{aligned} B_1 &\stackrel{\text{def}}{=} \{r \in \{0,1\}^\ell : x \in L \wedge A(x,r) = \texttt{YES}\}, \\ B_0 &\stackrel{\text{def}}{=} \{r \in \{0,1\}^\ell : x \notin L \wedge A(x,r) = \texttt{YES}\}. \end{aligned}$$

事実 4.37. $|B_1| = 2^\ell$（$B_1 = \{0,1\}^\ell$），$|B_0| \leq 2^\ell/4$.

[13] よって，素数が与えれた上での増幅手法である.
[14] 第 8.2 節では，エクスパンダーを利用した成功確率の増幅手法を示す.
[15] 対象とする言語は素数性判定問題と同様にクラス coRP に属するもの.

問 4.49. この事実が成り立つ理由を説明しなさい.

定理 4.17 (チェビシェフの不等式). X を確率変数，$\mu = \mathrm{E}[X]$，$\sigma = V[X]$ とする．このとき，任意の $t \in \mathbb{R}^+$ について，

$$\Pr\{|X - \mu| \geq t\} \ \leq \ \frac{\sigma}{t^2}.$$

証明. 確率変数 $(X-\mu)^2 \geq 0$ にマルコフの不等式を用いれば，任意の $t \in \mathbb{R}^+$ について，

$$\Pr\{(X-\mu)^2 \geq t\} \ \leq \ \frac{\mathrm{E}[(X-\mu)^2]}{t} \ = \ \frac{\sigma}{t}.$$

よって，

$$\frac{\sigma}{t} \ \geq \ \Pr\{(X-\mu)^2 \geq t\} \ = \ \Pr\{|X-\mu| \geq \sqrt{t}\}.$$

この不等式の t を t^2 に置き換えれば，定理の不等式が得られる． ■

任意の $t \in \mathbb{N}$ について，以下のようなアルゴリズム A_t を考える[16].

入力：$x \notin L$

1. $p \in \mathbb{N}$ を $2^{\ell-1} \leq p$ を満たす最小の素数とする.
2. $a, b \in \mathbb{Z}_p$ を一様ランダムに選ぶ.
3. 任意の $i \in \mathbb{Z}_t$ について $r_i = ai + b \pmod{p}$ とする.
4. $a_0 = A(x, r_0), a_1 = A(x, r_1), \ldots, a_{t-1} = A(x, r_{t-1})$ を実行する.
5. $a_0, \ldots, a_{t-1}$ のうち一つでも `NO` があれば `NO` を出力，そうでなければ `YES` を出力する.

図 9: A_t：成功確率の増幅

注 4.16. ステップ 1 の素数 p は $p < 2^\ell$ を満たすことが知られている．よって，$|p| = \ell$ となる．A_t は，これが与えられた（1 ステップで求められた）上での成功確率の増幅となる.

注 4.17. ステップ 2 の a, b の選択のみにランダムビットが必要となる.（$|a|, |b| = \ell$）よって，合計のランダムビット長は 2ℓ．ステップ 4 では，r_i を $|r_i| = \ell$ であるランダムビットとみなす.

定理 4.18. 任意の $t \in \mathbb{N}$ に対して，アルゴリズム A_t の誤り確率は $4/t$ 以下である.

証明. $t \in \mathbb{N}$ を任意に固定する．$p \in \mathbb{N}$ 及び $r_i \in \mathbb{Z}_p$ をアルゴリズムで定義された整数とする.

[16] $x \notin L$ の場合を考えればよい.

主張 4.14. 以下の二つが成り立つ.

1. $\forall i \in \mathbb{Z}_t, \forall r \in \mathbb{Z}_p \ \left[\Pr_{a,b}\{r_i = r\} = \frac{1}{p}\right]$,
2. $\forall i, j \in \mathbb{Z}_t : i \neq j, \forall x, y \in \mathbb{Z}_p \ \left[\Pr_{a,b}\{(r_i = x) \wedge (r_j = y)\} = \frac{1}{p^2}\right]$.

証明. まず，一つ目を示す．$i \in \mathbb{Z}_t$, $r \in \mathbb{Z}_p$ を任意に固定する.（$i \neq 0$ としてよい.）$r_i \equiv_p ai + b$ より（更に，$\mathbb{Z}_p^*$ が群であることより），

$$\Pr_{a,b}\{r_i = r\} \ = \ \Pr_{a,b}\{ai + b \equiv_p r\} \ = \ \sum_{\beta \in \mathbb{Z}_p} \Pr_b\{b = \beta\} \Pr_a\{ai \equiv_p r - \beta\} \ = \ p \cdot \frac{1}{p} \cdot \frac{1}{p} \ = \ \frac{1}{p}.$$

問 4.50. 二つ目と三つ目の等式を示しなさい.

次に二つ目を示す．$i, j \in \mathbb{Z}_t$（$i \neq j$），$x, y \in \mathbb{Z}_p$ を任意に固定する．$r_i \equiv_p ai + b$, $r_j \equiv_p aj + b$ より，

$$(r_i = x) \wedge (r_j = y) \iff (x \equiv_p ai + b) \wedge (y \equiv_p aj + b).$$

右辺を変数 a, b の連立方程式とみなせば,（$i \neq j$ の場合）a, b の値が（$i, j \in \mathbb{Z}_t$, $x, y \in \mathbb{Z}_p$ により）唯一に定まることがいえる．a, b が互いに独立であることから，上の事象が起きる確率は $(1/p)(1/p) = 1/p^2$ となる.

問 4.51. この値が導かれる理由を説明しなさい.

■

一つ目より，$r_i \in \mathbb{Z}_p$ は一様ランダムであることを意味する．二つ目より，$r_i, r_j \in \mathbb{Z}_p$ は対ごとに独立であることを意味する．任意の $i \in \mathbb{Z}_t$ について,

$$X_i \stackrel{\text{def}}{=} \begin{cases} 0 & A(x, r_i) = \texttt{YES} \\ 1 & \text{o.w.} \end{cases}$$

このとき，$X_i, X_j \in \{0, 1\}$ は対ごとに独立である．$X = \sum_{i \in \mathbb{Z}_t} X_i$ とすれば．アルゴリズムが誤りすることは $X = 0$ と同値である.

問 4.52. この事実が成り立つ理由を説明しなさい.

主張 4.15. 任意の $i \in \mathbb{Z}_t$ について，$\Pr\{X_i = 1\} \geq 1/2$.

問 4.53. この主張を証明しなさい.（ヒント：事実 4.37 を参照.）

よって，$\mathrm{E}[X] = \sum_{i \in \mathbb{Z}_t} \mathrm{E}[X_i] \geq t/2$．また，$X_1, \ldots, X_t$ が対ごとに独立であることから，命題 2.10 より，

$$\mathrm{V}[X] \ = \ \sum_{i \in \mathbb{Z}_t} \mathrm{V}[X_i] \ \leq \ \frac{t}{4}. \quad (\because \ \mathrm{V}[X_i] \leq 1/4)$$

問 4.54. $\mathrm{V}[X_i] \leq 1/4$ を示しなさい.

よって，チェビシェフの不等式より，アルゴリズムの誤り確率は,

$$\Pr\{X = 0\} \;\leq\; \Pr\{|X - \mathrm{E}[X]| \geq t/4\} \;\leq\; \frac{\mathrm{V}[X]}{(t/4)^2} \;\leq\; \frac{t/4}{t^2/16} \;=\; \frac{4}{t}.$$

■

系 4.38. アルゴリズム A_t を利用することにより，任意の $k \in \mathbb{N}$ について，$\frac{4\ell k}{\log t - 2}$ のランダムビット長で，誤り確率が $1/4^k$ 以下になる.

注 4.18. アルゴリズム全体の計算時間が多項式時間であるためには，$t = n^{O(1)}$ である必要がある. よって，必要なランダムビット長は $O(\ell k / \log n)$ となる.（事実 4.36 を参照.）

問 4.55. 上の系を示しなさい.（アルゴリズムを明記すること.）

5　チェルノフバウンド

5.1　チェルノフバウンド

$X_1, X_2, \ldots, X_n$ を次のような互いに独立な確率変数とする．それぞれの $i \in [n]$ について，

$$\begin{aligned} \Pr(X_i = 1) &= p_i \quad (0 < p_i < 1) \\ \Pr\{X_i = 0\} &= 1 - p_i \end{aligned}$$

以下，$X = \sum_{i\in[n]} X_i$，$\mu = \mathrm{E}[X] = \sum_{i\in[n]} p_i$ とする．

定理 5.1 (チェルノフバウンド（下界）). 任意の $\epsilon > 0$ について，

$$\Pr\{X > (1+\epsilon)\mu\} < \left(\frac{\mathrm{e}^{\epsilon}}{(1+\epsilon)^{(1+\epsilon)}}\right)^{\mu}.$$

証明. 任意の実数 $t \in \mathbb{R}^+$ について，

$$\Pr\{X > (1+\epsilon)\mu\} = \Pr\{\exp(tX) > \exp(t(1+\epsilon)\mu)\}.$$

マルコフの不等式を右辺に適用することにより，

$$\Pr\{X > (1+\epsilon)\mu\} < \frac{\mathrm{E}[\exp(tX)]}{\exp(t(1+\epsilon)\mu)}.$$

主張 5.1.

$$\mathrm{E}[\exp(tX)] \le \exp((\mathrm{e}^t - 1)\mu).$$

証明. X_i は互いに独立であることから，

$$\mathrm{E}[\exp(tX)] = \mathrm{E}\left[\mathrm{e}^{t\sum_{i\in[n]} X_i}\right] = \mathrm{E}\left[\prod_{i\in[n]} \mathrm{e}^{tX_i}\right] = \prod_{i\in[n]} \mathrm{E}\left[\mathrm{e}^{tX_i}\right]$$

任意の $i \in [n]$ について，$\mathrm{E}[\mathrm{e}^{tX_i}] = e^t p_i + \mathrm{e}^0(1-p_i) = 1 + p_i(\mathrm{e}^t - 1)$ より，

$$\mathrm{E}[\exp(tX)] = \prod_{i\in[n]} (1 + p_i(\mathrm{e}^t - 1)).$$

命題 8.13 より，

$$\prod_{i\in[n]} (1 + p_i(\mathrm{e}^t - 1)) \le \prod_{i\in[n]} \mathrm{e}^{(p_i(\mathrm{e}^t-1))} = \mathrm{e}^{(\mathrm{e}^t-1)\sum_{i\in[n]} p_i} = \mathrm{e}^{(\mathrm{e}^t-1)\mu}.$$

■

この主張より，

$$\Pr\{X > (1+\epsilon)\mu\} < \frac{\exp((\mathrm{e}^t-1)\mu)}{\exp(t(1+\epsilon)\mu)} = \left(\frac{\exp(\mathrm{e}^t-1)}{\exp(t(1+\epsilon))}\right)^{\mu}.$$

この不等式の右辺を $(f(t))^{\mu}$ とおく．$t > 0$ の範囲で $f(t)$ の最小値を求めると，$t = \ln(1+\epsilon)$ のとき $f(t) = \mathrm{e}^{\epsilon}/(1+\epsilon)^{(1+\epsilon)}$ となる．

問 5.1. $t > 0$ の範囲で $f(t)$ の最小値がそのようになることを示しなさい.

■

問 5.2. 命題 8.13 を証明しなさい.

系 5.1 (チェルノフバウンド（下界）). 任意の $\epsilon > 0$ について,

$$\begin{aligned} \Pr\{X > (1+\epsilon)\mu\} &< \exp\left(-\frac{\epsilon^2\mu}{5}\right) \quad : \quad 0 < \epsilon \leq 2\mathrm{e}-1 \\ \Pr\{X > (1+\epsilon)\mu\} &< 2^{-(1+\epsilon)\mu} \quad : \quad \epsilon \geq 2\mathrm{e}-1 \end{aligned}$$

証明. まず，最初の不等式を示すためには，任意の $0 < \epsilon \leq 2\mathrm{e}-1$ について，以下が成り立つことを示せばよい.

$$\left(\frac{\mathrm{e}^\epsilon}{(1+\epsilon)^{(1+\epsilon)}}\right)^\mu \leq \exp(-\epsilon^2\mu/5).$$

両辺の対数をとると,

$$\mu \cdot \ln\left(\frac{\mathrm{e}^\epsilon}{(1+\epsilon)^{(1+\epsilon)}}\right) \leq -\frac{\epsilon^2\mu}{5}.$$

更に，この不等式は以下のように式変形できる.

$$\begin{aligned} &\iff \quad \epsilon - (1+\epsilon)\ln(1+\epsilon) \leq -\frac{\epsilon^2}{5} \\ &\iff \quad (1+\epsilon)\ln(1+\epsilon) - \epsilon - \frac{\epsilon^2}{5} \geq 0 \end{aligned}$$

この不等式の左辺を $f_1(\epsilon)$ としたとき，$0 < \epsilon \leq 2\mathrm{e}-1$ について $f_1(\epsilon) \geq 0$ である.

問 5.3. この事実（$0 < \epsilon \leq 2\mathrm{e}-1$ について $f_1(\epsilon) \geq 0$）を示しなさい.

次に，二番目の不等式を示すためには，任意の $\epsilon \geq 2\mathrm{e}-1$ について，以下が成り立つことを示せばよい.

$$\left(\frac{\mathrm{e}^\epsilon}{(1+\epsilon)^{(1+\epsilon)}}\right)^\mu \leq 2^{-(1+\epsilon)\mu}.$$

両辺の対数をとると,

$$\mu \cdot \ln\left(\frac{\mathrm{e}^\epsilon}{(1+\epsilon)^{(1+\epsilon)}}\right) \leq -(1+\epsilon)\mu\ln 2.$$

更に，この不等式は以下のように式変形できる.

$$\begin{aligned} &\iff \quad \epsilon - (1+\epsilon)\ln(1+\epsilon) \leq -(1+\epsilon)\ln 2 \\ &\iff \quad (1+\epsilon)\ln(1+\epsilon) - \epsilon - (1+\epsilon)\ln 2 \geq 0 \end{aligned}$$

この不等式の左辺を $f_2(\epsilon)$ としたとき，$\epsilon \geq 2\mathrm{e}-1$ について $f_2(\epsilon) \geq 0$ である.

問 5.4. この事実（$\epsilon \geq 2\mathrm{e}-1$ について $f_2(\epsilon) \geq 0$）を示しなさい.

■

定理 5.2 (チェルノフバウンド（上界）). 任意の $\epsilon : 0 < \epsilon \leq 1$ について,

$$\Pr\{X < (1-\epsilon)\mu\} \ < \ \exp(-\epsilon^2\mu/2).$$

証明. $\epsilon = 1$ のときは明らか. 以降, $0 < \epsilon < 1$ とする. 下界の証明と同様にして, 任意の実数 $t \in \mathbb{R}^+$ について,

$$\Pr\{X < (1-\epsilon)\mu\} \ = \ \Pr\{-X > -(1-\epsilon)\mu\} \ = \ \Pr\{\exp(-tX) > \exp(-t(1-\epsilon)\mu)\}$$

マルコフの不等式を右辺に適用することにより,

$$\Pr\{X < (1-\epsilon)\mu\} \ < \ \frac{\mathrm{E}[\exp(-tX)]}{\exp(-t(1-\epsilon)\mu)}$$

下界の証明と同様にして,

$$\Pr\{X < (1-\epsilon)\mu\} \ < \ \left(\frac{\exp(\mathrm{e}^{-t}-1)}{\exp(-t(1-\epsilon))}\right)^{\mu}.$$

この不等式の右辺を $(f(t))^{\mu}$ とおく. $t > 0$ の範囲で $f(t)$ の最小値を求めると, $t = \ln(1/(1-\epsilon))$ のとき $f(t) = \mathrm{e}^{-\epsilon}/(1-\epsilon)^{(1-\epsilon)}$ となる.

問 5.5. $t > 0$ の範囲で $f(t)$ の最小値がそのようになることを示しなさい.

また, $|x| < 1$ について $\ln(1+x) = x - x^2/2 + x^3/3 - \ldots$（テーラー展開）であることから,

$$(1-\epsilon)^{(1-\epsilon)} \ > \ \exp(-\epsilon + \epsilon^2/2). \tag{4}$$

問 5.6. 不等式 (4) を示しなさい.

これより, $(f(t))^{\mu} = (\mathrm{e}^{-\epsilon}/(1-\epsilon)^{(1-\epsilon)})^{\mu} < \exp(-\epsilon^2\mu/2)$. ■

5.2 乱択クイックソート

定理 5.3. 入力される自然数の個数を n とする. `rand_qsort` アルゴリズムにおいて, 確率変数 X を, アルゴリズム全体を通して行われる二つの自然数の比較回数とする. このとき,

$$\Pr(X > 32n\ln n) \ \leq \ 1/n.$$

注 5.1. 系 3.4 を参照.

証明. アルゴリズムの入力を $a_1, \ldots, a_n$，その集合を A とする．一般性を失うことなく $A = [n]$ とする.（重複した自然数があるときも同様にして示される.）定理 3.2 の証明で用いた二分木を考える.（以下，頂点とそのラベルを同一視する.）任意の $i \in [n]$ について，i でラベル付けされた頂点の深さを d_i とする.（根の深さは 0 とする.）

主張 5.2. $X = \sum_{i \in [n]} d_i$.

証明. 二分木のある頂点 v での再起呼び出し $\texttt{rand\_qsort}(S)$ を考える．この再起呼び出しの中で行われる（v との）比較回数は，v を根とした部分木の頂点の個数（マイナス 1）に等しい. ■

問 5.7. この主張の証明を完成させなさい.（v との比較回数が v を根とした部分木の頂点の個数であることが，主張の証明になる理由を説明しなさい.）

主張 5.3. 任意の $i \in [n]$ について，

$$\Pr\{d_i > 32 \ln n\} \ < \ \frac{1}{n^2}.$$

証明. 任意に $i \in [n]$ を固定する．$d = 32 \ln n$ とする．$\texttt{rand\_qsort}(A)$ から始め，$i \in S$ である再帰呼び出し $\texttt{rand\_qsort}(S)$ を高々 d 回呼び出すことを考える．任意の $\ell \in [d]$ について，Y_ℓ を次のような確率変数とする．第 ℓ 回目の（$i \in S$ である）再帰呼び出し $\texttt{rand\_qsort}(S)$ において，

$$Y_\ell \stackrel{\text{def}}{=} \begin{cases} 1 & : \text{（}S\text{ を昇順に並べた場合）ピボットが中間の } |S|/2 \text{ 個の要素から選ばれる} \\ 0 & : \text{o.w.} \end{cases}$$

$Y = \sum_{\ell \in [d]} Y_\ell$ とする．このとき，$\mathrm{E}[Y_\ell] = 1/2$ より[17]，$\mu \stackrel{\text{def}}{=} \mathrm{E}[Y] = 16 \ln n$．$d$ 回の再帰呼び出しのうち，$Y_\ell = 1$（という事象）が y 回おきたとする.（つまり，$Y = y$.）$Y_\ell = 1$ であるとき，$i \in S_1$ の場合は $|S_1| \leq (3/4)|S|$ となり，$i \in S_2$ の場合は $|S_2| \leq (3/4)|S|$ となる.（いずれも大きさが 3/4 になる.）このことから,（$Y_\ell = 1$ が y 回おきたので）$(3/4)^y n \leq 1$ であれば $d_i \leq d$（再帰呼び出しが d 回までに終わる）となる．この関係（$(3/4)^y n \leq 1 \Rightarrow d_i \leq d$）の仮定について以下が成り立つ.

$$(3/4)^y n \leq 1 \iff \ln n \leq y \ln(4/3) \impliedby 4 \ln n \leq y$$

これより，$y \geq 4 \ln n$ であれば $d_i \leq d$．この対偶をとれば，$d_i > d$ であれば $y < 4 \ln n$．よって，

$$\Pr\{d_i > d\} \ \leq \ \Pr\{y < 4 \ln n\} \ = \ \Pr\{Y < 4 \ln n\}.$$

よって，$Y_1, \ldots, Y_d$ は互いに独立であることから，チェルノフバウンドより，

$$\begin{aligned} \Pr\{d_i > 32 \ln n\} \ &\leq \ \Pr\{Y < 4 \ln n\} \ = \ \Pr\{Y < (1 - 3/4)\mu\} \\ &< \ \exp\left(-\frac{(3/4)^2 \cdot \mu}{2}\right) \ \leq \ \exp(-2 \ln n) \ = \ \frac{1}{n^2}. \end{aligned}$$

■

この主張より，ユニオンバウンドを用いれば，

$$\begin{aligned} \Pr\{X > 32 n \ln n\} \ &\leq \ \Pr\{\exists i \in [n][d_i > 32 \ln n]\} \ \leq \ n \max_{i \in [n]} \{\Pr\{d_i > 32 \ln n\}\} \\ &\leq \ n \cdot \frac{1}{n^2} \ = \ \frac{1}{n}. \end{aligned}$$

■

[17] 厳密にはほぼ 1/2.

6　充足可能性問題

定義 6.1

X を論理変数の集合とする．任意の変数 $x \in X$ について，x 及び $\bar{x}$ を**リテラル**という．いくつかのリテラルを論理和 $\vee$ で結合したものを**節**という．節をなすリテラルの個数をその節の**大きさ**という．いくつかの節を論理積 $\wedge$ で結合したものを**和積標準形（CNF）論理式**という．特に，すべての節の大きさが k 以下であるとき，**k-CNF 論理式**という．

例 6.1 (CNF 論理式)**.** 以下の φ は，変数 x_1, x_2, x_3, x_4, x_5 上の 3-CNF 論理式である．

$$\varphi \ = \ x_1 \wedge (\bar{x}_1 \vee x_2) \wedge (x_1 \vee \bar{x}_2 \vee \bar{x}_3) \wedge (\bar{x}_1 \vee \bar{x}_3 \vee x_4) \wedge x_2 \wedge (\bar{x}_3 \vee \bar{x}_4 \vee \bar{x}_5).$$

事実 6.1. 任意の論理関数 $f : \{0,1\}^n \to \{0,1\}$ は，CNF 論理式で表される．

以降では，CNF 論理式は，記号 $\wedge$ を省略して表記する．例えば，上の φ は以下のように表記される．

$$\varphi \ = \ x_1(\bar{x}_1 \vee x_2)(x_1 \vee \bar{x}_2 \vee \bar{x}_3)(\bar{x}_1 \vee \bar{x}_3 \vee x_4)x_2(\bar{x}_3 \vee \bar{x}_4 \vee \bar{x}_5).$$

また，CNF 論理式を，節の集合とみなすこともある．例えば，上の φ は以下のように表記される．

$$\varphi \ = \ \{x_1, (\bar{x}_1 \vee x_2), (x_1 \vee \bar{x}_2 \vee \bar{x}_3), (\bar{x}_1 \vee \bar{x}_3 \vee x_4), x_2, (\bar{x}_3 \vee \bar{x}_4 \vee \bar{x}_5)\}.$$

よって，C が φ の節であるとき，$C \in \varphi$ と表記する．また，$|\varphi|$ は節の個数になる．(節に関しても同様である．例えば，$\bar{x}$ が節 C のリテラルであるとき，$\bar{x} \in C$ と表記され，$|C|$ は節の大きさとなる．)

定義 6.2

φ を X 上の CNF 論理式，C を φ の任意の節とする．$t : X \to \{0,1\}$ を X への任意の真理値割り当てとする．割り当て t のもとで節 C が真になるとき，C が t により**充足する**という．また，割り当て t のもとで φ のすべての節が真になるとき，φ が t により**充足する**という．このとき，t を φ の**充足割り当て**という．

例 6.2 (充足割り当て)**.** 先の例の 3-CNF 論理式 φ は充足割り当てをもつ．($(x_1, \ldots, x_5) = (1,1,1,1,0)$.) 一方，以下の 3-CNF 論理式 φ' には充足割り当てがない．

$$\varphi' \ = \ x_1(\bar{x}_1 \vee x_2)(x_1 \vee \bar{x}_2 \vee \bar{x}_3)(\bar{x}_1 \vee \bar{x}_3 \vee x_4)\bar{x}_2(\bar{x}_3 \vee \bar{x}_4 \vee \bar{x}_5).$$

充足可能性問題（satisfiability）

- 入力：X 上の CNF 論理式 φ
- 出力：φ の充足割り当てがあれば 1，そうでなければ 0.

以降，充足可能性問題を SAT と略す．また，入力が k-CNF 論理式に限定された問題を k-SAT 問題といい，k-SAT と略す．

定義 6.3

φ を X 上の CNF 論理式とする．$X' \subseteq X$ を任意として，$t : X' \to \{0,1\}$ を任意の部分割り当てとする．このとき，$\varphi|_t$ を，φ に割り当て t を「適用した」論理式とする．

例 6.3 (割り当ての適用)**.** 変数 x_1, x_2, x_3, x_4, x_5 上の 3-CNF 論理式 φ を以下とする.

$$\varphi \ = \ \{x_1, (\bar{x}_1 \vee x_2), (x_1 \vee \bar{x}_2 \vee \bar{x}_3), (\bar{x}_1 \vee \bar{x}_3 \vee x_4), x_2, (\bar{x}_3 \vee \bar{x}_4 \vee \bar{x}_5)\}.$$

$X' = \{x_1, x_2\}$ として，部分割り当て $t : X' \to \{0, 1\}$ を $t(x_1, x_2) = (1, 0)$ とする．このとき,

$$\varphi|_t \ = \ \{\emptyset, (\bar{x}_3 \vee x_4), \emptyset, (\bar{x}_3 \vee \bar{x}_4 \vee \bar{x}_5)\}.$$

6.1 決定性アルゴリズム

定義 6.4

関数 $f(n)$ が，n の指数関数 $g(n)$ と多項式関数 $h(n)$ の積で表されていたとする．(つまり，$f(n) = h(n) \cdot g(n)$.) このとき，$\widetilde{O}(\cdot)$ 記法は多項式関数を省いた関数を表す：$f(n) = \widetilde{O}(g(n))$.

SAT を解くアルゴリズムを考える．CNF 論理式の変数の個数を n として，計算時間を n の関数で見積もる．SAT は NP 完全であることから，n の多項式時間で解くことはできないと考えられている．以下は，SAT を解く全探索（brute-force search）アルゴリズムである.

入力：n 変数上の CNF 論理式 φ

1. それぞれの割り当て $t \in \{0, 1\}^n$ について以下を繰り返す.
   - φ が t で充足されるならば `YES` を出力して終了
2. `NO` を出力

図 10: SAT を解く全探索アルゴリズム

事実 6.2. 図 10 で示されたアルゴリズムの計算時間は $\widetilde{O}(2^n)$.

問 6.1. 上の事実を示しなさい.

このように単純に考えれば，SAT は $\widetilde{O}(2^n)$ 時間で解くことができる．では，SAT を $\widetilde{O}(1.999^n)$ 時間で解くことはできるだろうか？ 残念ながら，これまでのところ，SAT を解く $\widetilde{O}(1.999^n)$ 時間アルゴリズムは知られていない．では，k-SAT ならば $\widetilde{O}(1.999^n)$ 時間で解くことはできるだろうか？

命題 6.3. 図 11 で示されたアルゴリズムの計算時間は，$\widetilde{O}((2^k - 1)^{n/k})$.（例えば，$k = 3$ の場合は $\widetilde{O}(1.913^n)$.）

証明. n 変数上の k-CNF 論理式 φ に対するアルゴリズム `bt_ksat`(φ) の計算時間を $T(n)$ とする．`bt_ksat`(φ) が呼び出された場合，任意に選ばれた節を C として，$|C| = k' \leq k$ とする．C を充足させる割り当てはちょうど $2^{k'} - 1$ 個あるので，ちょうど $2^{k'} - 1$ 個の再帰呼び出しがなされる．ま

bt_ksat(φ) // CNF 論理式 φ

1. $\varphi = \emptyset$ ならば YES を出力して終了.
2. $\emptyset \in \varphi$ ならばリターン.
3. 任意に，節 $C \in \varphi$ を選ぶ.
4. それぞれの $t \in \{0,1\}^{|C|}$ s.t. t は C を充足，について以下を繰り返す.
   - bt_ksat($\varphi|_t$) を実行.
5. 最初の呼び出しなら NO を出力.

図 11: k-SAT を解く $\widetilde{O}((2^k-1)^{n/k})$ 時間アルゴリズム

た，それぞれの再帰呼び出しは，$n-k'$ 変数上の論理式に対してなされる．よって，$T(n)$ は以下のように表される：

$$T(n) \ \leq \ (2^{k'}-1)T(n-k') + \mathbf{poly}(n).$$

この漸化式を解けば，$T(n) \leq \mathbf{poly}(n)(2^{k'}-1)^{n/k'}$ が得られる．$(2^{k'}-1)^{1/k'}$ は k' について増加関数であるので，$T(n) \leq \mathbf{poly}(n)(2^k-1)^{n/k} = \widetilde{O}((2^k-1)^{n/k})$ となる． ■

問 6.2. 上の証明中，$T(n)$ の漸化式を解くとそのような値になることを示しなさい.

このように単純に考えれば，k-SAT は 2 よりも真に小さな定数 c_k （k が定数である限り c_k も定数）に対して $\widetilde{O}(c_k^n)$ で解くことができる．更に，このアルゴリズムに少し変更を加えれば，いくらかよい計算時間が得られる.

bt_ksat2(φ) // CNF 論理式 φ

1. $\varphi = \emptyset$ ならば YES を出力して終了.
2. $\emptyset \in \varphi$ ならばリターン.
3. 任意に，節 $C \in \varphi$ を選ぶ.（すべて正のリテラルだとする.）
4. それぞれの $i : 0 \leq i \leq |C|-1$ について以下を繰り返す.
   - $t = 0^i 1$ とする.
   - bt_ksat2($\varphi|_t$) を実行.
5. 最初の呼び出しなら NO を出力.

図 12: k-SAT を解く $\widetilde{O}(f(k)^n)$ 時間アルゴリズム

命題 6.4. 図 12 で示されたアルゴリズムの計算時間は，$\widetilde{O}(f(k)^n)$，ただし，$f(k)$ は方程式 $x^k - x^{k-1} - \cdots - x^2 - x - 1 = 0$ の（唯一の）正の解，である．(例えば，$k = 3$ の場合は $\widetilde{O}(1.840^n)$.)

証明. 先の証明と同様にして，アルゴリズム $\texttt{bt\_ksat2}(\varphi)$ の計算時間を $T(n)$ とおけば，$T(n)$ は以下のように表される：

$$T(n) \ \leq \ T(n-1) + T(n-2) + \cdots + T(n-k') + \mathbf{poly}(n).$$

この漸化式を解けば，$T(n) \leq \mathbf{poly}(n) f(k')^n$，ただし，$f(k')$ は方程式 $x^{k'} - x^{k'-1} - \cdots - x^2 - x - 1 = 0$ の（唯一の）正の解，が得られる．この解（を表す関数）は k' について増加関数であることから，命題が示される． ■

問 6.3. 上の証明中，$T(n)$ の漸化式を解くとそのような値になることを示しなさい.

6.2 ローカルサーチアルゴリズム

入力：CNF 論理式 φ

1. 以下を c 回繰り返す.
   (a) $t \in \{0,1\}^n$ を一様ランダムに選ぶ
   (b) $3n$ 回繰り返す
      i. t が φ を充足させるならば YES を出力して終了
      ii. t で充足しない節 $C \in \varphi$ を「任意に」選ぶ
      iii. C の変数 x を一様ランダムに選ぶ
      iv. $t := t \oplus e_x$
2. NO を出力

図 13: ローカルサーチアルゴリズム

CNF 論理式 φ に対して，図 13 のアルゴリズムのステップ 1 の一回の繰り返しを $\texttt{SCH\_RW}(\varphi)$ と表記する.

定理 6.1. 任意の k-CNF 論理式 φ に対して，

$$\begin{aligned} \varphi \in \mathrm{SAT} \ &: \ \Pr_{t,x}(\texttt{SCH\_RW}(\varphi) = \texttt{YES}) \ \geq \ \frac{(2-2/k)^{-n}}{3n}, \\ \varphi \notin \mathrm{SAT} \ &: \ \Pr_{t,x}(\texttt{SCH\_RW}(\varphi) \neq \texttt{YES}) \ = \ 1. \end{aligned}$$

ただし，この確率は，ステップ 1-(a) で選ぶ t，ステップ 1-(b)-(iii) で選ぶ x，の確率に依存する.

証明. まず，$\varphi \notin \mathrm{SAT}$ のときは明らか.（YES を出力することはない.）$\varphi \in \mathrm{SAT}$ のとき，一般性を失うことなく，0^n が φ の充足解（の一つ）であるとする[18]．任意の $t \in \{0,1\}^n$ に対して，ステップ 1-(b)（の $3n$ 回の繰り返し全体）を $\mathtt{SCH\_RW}(\varphi, t)$ と表記する．$d(t, 0^n)$ を t と 0^n とのハミング距離とする.（つまり，t により 1 が割り当てられている変数の個数.）任意の $i \in [n] \cup \{0\}$，$d(t, 0^n) = i$ である任意の $t \in \{0,1\}^n$ に対して，

$$q_i \stackrel{\mathrm{def}}{=} \Pr_x\{\mathtt{SCH\_RW}(\varphi, t) \text{ finds } 0^n | t\},$$

とする[19].（$q_0 = 1$.）このとき，ステップ 1 の一回の繰り返しで YES が出力される確率は，

$$\begin{aligned}
\Pr_{t,x}(\mathtt{SCH_RW}(\varphi) = \mathtt{YES}) &= \Pr_{t,x}\{\mathtt{SCH_RW}(\varphi, t) = \mathtt{YES}\} \\
&\geq \Pr_{t,x}\{\mathtt{SCH_RW}(\varphi, t) \text{ finds } 0^n\} \\
&= \sum_{i=0}^{n} \Pr_t\{d(t, 0^n) = i\} \cdot q_i \\
&= \frac{1}{2^n} \sum_{i=0}^{n} \binom{n}{i} \cdot q_i.
\end{aligned}$$

以降，q_i の下界を見積もる．整数 $i \in [n] \cup \{0\}$ を任意に固定する．更に，$d(t_0, 0^n) = i$ である割り当て $t_0 \in \{0,1\}^n$ を任意に固定する．アルゴリズムのステップ 1-(b) において，t_0 から 0^n へ初めて到達する（高々 $3n$ ステップの）確率過程を考える．ステップ 1-(b) の一回の繰り返しでは，(t で充足しない節の）変数 x が一様ランダムに選ばれ，x への割り当てが反転される.（$0 \to 1$ または $1 \to 0$.）

主張 6.1. ステップ 1-(b) の任意の繰り返しを考える．その繰り返しにおける割り当てを t，任意に選ばれた（t で充足しない）節を C とする．$|C| = k' \in [k]$ とする．C の変数の中で，0^n で 1 が割り当てられている変数の個数を a とする.（$a \neq 0$.）このとき，

$$\begin{aligned}
\Pr_x\{1 \to 0\} &= a/k', \\
\Pr_x\{0 \to 1\} &= 1 - a/k'.
\end{aligned}$$

証明. ■

問 6.4. この主張を証明しなさい.

t_0 から 0^n までの確率過程において，$0 \to 1$ の遷移（0^n から遠くなる）が j 回あったとする．このとき，$1 \to 0$ の遷移（0^n に近くなる）は $i + j$ 回あったことになる．この i, j に対して，t_0 から 0^n への遷移の種類の個数を $S_{i,j}$ とおく.

主張 6.2 (ballot theorem)**.** 任意の i, j に対して，

$$S_{i,j} = \frac{i}{i+2j} \cdot \binom{i+2j}{j}.$$

証明. ■

全体の遷移は $j + (i + j) = i + 2j$ 回あったことになるので，j は $i + 2j \leq 3n$ を満たす必要がある.（よって，$j \leq (3n - i)/2$.）

[18]後で分かるように，以降の解析は充足解の選び方に依存しない.
[19]後で分かるように，q_i は t の選び方に依存しない.（i のみに依存する.）

主張 6.3. 任意の $i \in [n] \cup \{0\}$ について，

$$q_i \;\geq\; \sum_{j=0}^{(3n-i)/2} S_{i,j} \cdot \left(\frac{1}{k}\right)^{i+j} \left(1-\frac{1}{k}\right)^{j}.$$

証明. ■

この主張より，

$$\begin{aligned}
q_i &= \sum_{j=0}^{(3n-i)/2} S_{i,j} \cdot \left(\frac{1}{k}\right)^{i+j} \left(1-\frac{1}{k}\right)^{j} \\
&= \sum_{j=0}^{(3n-i)/2} \frac{i}{i+2j} \cdot \binom{i+2j}{j} \cdot \left(\frac{1}{k}\right)^{i+j} \left(1-\frac{1}{k}\right)^{j} \\
&\geq \frac{1}{3} \cdot \sum_{j=0}^{i} \binom{i+2j}{j} \cdot \left(\frac{1}{k}\right)^{i+j} \left(1-\frac{1}{k}\right)^{j} \quad (\because\ j \leq i \leq n.) \\
&\geq \frac{1}{3} \cdot \max_{j \in [i] \cup \{0\}} \left\{ \binom{i+2j}{j} \cdot \left(\frac{1}{k}\right)^{i+j} \left(1-\frac{1}{k}\right)^{j} \right\}.
\end{aligned}$$

ここで，$j = \alpha i$（$0 \leq \alpha \leq 1$）とおくと，任意の $i \in [n] \cup \{0\}$ に対して，

$$\binom{i+2j}{j} \;=\; \binom{(1+2\alpha)i}{\alpha i} \;\geq\; \frac{1}{n} \cdot 2^{H(\alpha/(1+2\alpha)) \cdot (1+2\alpha) i}. \quad (\because\ \text{命題 8.14})$$

ただし，$H(p) = -p \log p - (1-p)\log(1-p)$.（$H(0) = H(1) = 0$.）よって，

$$\begin{aligned}
q_i &\geq \frac{1}{3n} \cdot \max_{0 \leq \alpha \leq 1} \left\{ 2^{H(\alpha/(1+2\alpha)) \cdot (1+2\alpha) i} \cdot \left(\frac{1}{k}\right)^{(1+\alpha) i} \left(1-\frac{1}{k}\right)^{\alpha i} \right\} \\
&= \frac{1}{3n} \max_{0 \leq \alpha \leq 1} \left\{ 2^{H(\alpha/(1+2\alpha)) \cdot (1+2\alpha)} \cdot \left(\frac{1}{k}\right)^{(1+\alpha)} \left(1-\frac{1}{k}\right)^{\alpha} \right\}^{i} \\
&= \frac{1}{3n} \max_{0 \leq \alpha \leq 1} \left\{ \left(\frac{1+2\alpha}{\alpha}\right)^{\alpha} \left(\frac{1+2\alpha}{1+\alpha}\right)^{1+\alpha} \left(\frac{1}{k}\right)^{(1+\alpha)} \left(1-\frac{1}{k}\right)^{\alpha} \right\}^{i} \\
&= \frac{1}{3n} \max_{0 \leq \alpha \leq 1} \left\{ \left(\frac{1+2\alpha}{\alpha} \cdot \frac{k-1}{k}\right)^{\alpha} \left(\frac{1+2\alpha}{1+\alpha} \cdot \frac{1}{k}\right)^{1+\alpha} \right\}^{i}.
\end{aligned}$$

$\alpha = 1/(k-2)$ とおけば[20]，

$$q_i \;\geq\; \frac{1}{3n} \left(\frac{1}{k-1}\right)^{i}.$$

問 6.5. 上の q_i の下界の解析において，$\alpha = 1/(k-2)$ となることを証明しなさい.

よって，

$$\Pr_{t,x}(\texttt{SCH\_RW}(\varphi) = \texttt{YES}) \;\geq\; \frac{1}{2^n} \sum_{i=0}^{n} \binom{n}{i} \cdot q_i$$

[20] $f_k(\alpha) = \left(\frac{1+2\alpha}{\alpha} \cdot \frac{k-1}{k}\right)^{\alpha} \left(\frac{1+2\alpha}{1+\alpha} \cdot \frac{1}{k}\right)^{1+\alpha}$ とおいて，$df_k(\alpha)/d\alpha = 0$ を解く.（cf. $f(x) = x^x$ の微分は $df(x)/dx = x^x(\ln x + 1)$.）

$$
\begin{aligned}
&\geq \frac{1}{3n}\cdot\frac{1}{2^n}\sum_{i=0}^{n}\binom{n}{i}\left(\frac{1}{k-1}\right)^i \\
&= \frac{1}{3n}\cdot\frac{1}{2^n}\left(1+\frac{1}{k-1}\right)^n \\
&= \frac{1}{3n}\cdot\left(\frac{k}{2(k-1)}\right)^n \\
&= \frac{1}{3n}\cdot\left(\frac{1}{2-2/k}\right)^n.
\end{aligned}
$$

■

系 6.5. 図 13 で示されたアルゴリズム $\mathtt{SCH}(\varphi)$ について，$c = 3n^2\cdot(2-2/k)^n$ とすれば（よって，計算時間は $\widetilde{O}((2-2/k)^n)$），以下のことが成り立つ：

$$
\begin{aligned}
\varphi\in\mathrm{SAT} \quad &: \quad \Pr\{\mathtt{SCH}(\varphi)=\mathtt{YES}\} \quad \geq \quad 1-e^{-n}, \\
\varphi\notin\mathrm{SAT} \quad &: \quad \Pr\{\mathtt{SCH}(\varphi)=\mathtt{NO}\} \quad = \quad 1.
\end{aligned}
$$

例えば，$k=3$ の場合，計算時間は $\widetilde{O}((4/3)^n)=\widetilde{O}(1.334^n)$.

証明. $\varphi\notin\mathrm{SAT}$ のときは明らか.（YES を出力することはない.）$\varphi\in\mathrm{SAT}$ のとき，$\mathtt{SCH}(\varphi)$ が NO を出力する確率の上界を見積もる．$p=(2-2/k)^{-n}/(3n)$ とおく.（よって，$c=n/p$.）定理より，ステップ 1 の一回の繰り返しで YES を出力する確率は，少なくとも p.（YES を出力しない確率は高々 $1-p$.）よって，NO を出力する確率，つまり，c 回の繰り返しすべてにおいて YES を出力しない確率は，高々

$$
(1-p)^c \quad\leq\quad \mathrm{e}^{c\cdot(-p)} \quad=\quad \mathrm{e}^{-(n/p)p} \quad=\quad \mathrm{e}^{-n}.
$$

■

6.3 バックトラックアルゴリズム

定理 6.2. 任意の k-CNF 論理式 φ に対して，

$$
\begin{aligned}
\varphi\in\mathrm{SAT} \quad &: \quad \Pr_{\sigma,t}\{\mathtt{PPZ}(\varphi)=\mathtt{YES}\} \quad \geq \quad 2^{-n(1-1/k)}, \\
\varphi\notin\mathrm{SAT} \quad &: \quad \Pr_{\sigma,t}\{\mathtt{PPZ}(\varphi)=\mathtt{NO}\} \quad = \quad 1.
\end{aligned}
$$

ただし，この確率は，ステップ 1 で選ぶ σ，ステップ 2 で選ぶ t，の確率に依存する.

以下，この定理を示す．まず，$\varphi\notin\mathrm{SAT}$ のときは明らか.（YES を出力することはない.）以降，$\varphi\in\mathrm{SAT}$ のときを示す．$\varphi\in\mathrm{SAT}$ を任意とする．φ の充足解の集合を $\mathrm{SAT}(\varphi)$ と表記する．$\mathtt{PPZ}(\varphi)$ が充足解 $z\in\mathrm{SAT}(\varphi)$ を見つける（ステップ 5 において $a=z$ となる）確率を $\tau(\varphi,z)$ と表記する．このとき，

$$
\Pr_{\sigma,t}\{\mathtt{PPZ}(\varphi)=\mathtt{YES}\} \quad=\quad \sum_{z\in\mathrm{SAT}(\varphi)}\tau(\varphi,z).
$$

入力：CNF 論理式 φ

1. 以下を c 回繰り返す.
   - PPZ(φ)
2. NO を出力する.

PPZ(φ)

1. 置換 $\sigma : [n] \to [n]$ を一様ランダムに選ぶ.
2. 割り当て $t \in \{0,1\}^n$ を一様ランダムに選ぶ.
3. $a = (*, *, \ldots, *)$ とする.
4. それぞれの $i \in [n]$ について以下を繰り返す.
   (a) $\emptyset \in \varphi|_a$ ならばリターン.
   (b) i. $x_{\sigma(i)} \in \varphi|_a$ であれば $a(x_{\sigma(i)}) = 1$.
   ii. $\bar{x}_{\sigma(i)} \in \varphi|_a$ であれば $a(x_{\sigma(i)}) = 0$.
   iii. $a(x_{\sigma(i)}) = t(x_{\sigma(i)})$ とする.
5. $a \in \{0,1\}^n$ が φ の充足解ならば YES を出力して終了.

図 14: バックトラックアルゴリズム

任意の置換 σ，任意の割り当て t に対して，PPZ(φ) のステップ 4-(c) の条件 (i), (ii) により 0/1 が割り当てられた変数の集合を $F_{\varphi,t}(\sigma)$ と表記する.

補題 6.6. 任意の置換 σ，任意の $t \in \{0,1\}^n$ に対して，次のことが成り立つ．PPZ(φ) が充足解 z を見つけるためには,

$$\forall x \in X \setminus F_{\varphi,z}(\sigma)\ [t(x) = z(x)]$$

を満たすことが必要十分である.

注 6.1. PPZ(φ) が充足解 z を見つけることが，次の事と同値であることを意味する．$F_{\varphi,z}(\sigma)$ 以外については t が z に同じである，また逆に，$F_{\varphi,z}(\sigma)$ については t は任意でよい.

証明. ($\Rightarrow$) 対偶をとって示す．つまり，$t(x) \neq z(x)$ であるような $x \in X \setminus F_{\varphi,z}(\sigma)$ が存在したとする．そのような x を次の条件を満たす x_{σ_i} とする．任意の $j \in [i-1]$ について $x_{\sigma_j} \in X \setminus F_{\varphi,z}(\sigma)$ であるとき $t(x_{\sigma_j}) = z(x_{\sigma_j})$ であり，かつ $t(x_{\sigma_i}) \neq z(x_{\sigma_i})$ である．このとき，$x \notin F_{\varphi,z}(\sigma)$ であること，更に，任意の $j \in [i-1]$ について $t(x_{\sigma_j}) = z(x_{\sigma_j})$ であることから，$x \notin F_{\varphi,t}(\sigma)$ となる．アルゴリズムより，$a(x) = t(x)$ となる．よって，($t(x) \neq z(x)$ より) $a(x) \neq z(x)$ となり，PPZ(φ) が z を見つけることがないことがいえる.

($\Leftarrow$) ステップ 4 における $i \in [n]$ についての帰納法により示す．任意の $j \in [i-1]$ について，$a(x_{\sigma(j)}) = z(x_{\sigma(j)})$ であるとする．この部分割り当て a に対して，$x_{\sigma(i)} \in \varphi|_a$ である場合を考え

る．($\bar{x}_{\sigma(i)} \in \varphi|_a$ のときも同様.）$x_{\sigma(i)}$ を含んでいた φ の節を C とする．このとき，帰納仮定より，$x_{\sigma(i)}$ 以外の C の任意の変数 x に対して（a による割り当てが決まっており）$a(x) = z(x)$ である．よって，$a(x_{\sigma(i)}) = z(x_{\sigma(i)})$.（そうでなければ z が充足解にならない.）そうでないとき（つまり，ステップ 4-(b)-(iii)），アルゴリズムより $a(x_{\sigma(i)}) = t(x_{\sigma(i)})$．更に，任意の $j \in [i-1]$ について，$a(x_{\sigma(j)}) = z(x_{\sigma(j)})$ であることから，$x_{\sigma(i)} \in X \setminus F_{\varphi,z}(\sigma)$ である．仮定より，$t(x_{\sigma(i)}) = z(x_{\sigma(i)})$．よって，$a(x_{\sigma(i)}) = z(x_{\sigma(i)})$. ■

問 6.6. 上の証明中，以下の二つ（証明の下線のついた部分）が成り立つ理由を詳説しなさい.

- ($\Rightarrow$) $x \notin F_{\varphi,t}(\sigma)$.
- ($\Leftarrow$) $x_{\sigma(i)} \in X \setminus F_{\varphi,z}(\sigma)$.

この補題（及びその後の注）より，任意の σ について，$\mathtt{PPZ}(\varphi)$ が z を見つける t の個数は $2^{|F_{\varphi,z}(\sigma)|}$．よって，

$$\tau(\varphi, z) \;=\; \frac{\sum_\sigma 2^{|F_{\varphi,z}(\sigma)|}}{n! \cdot 2^n} \;=\; 2^{-n} \cdot \frac{\sum_\sigma 2^{|F_{\varphi,z}(\sigma)|}}{n!} \;=\; 2^{-n} \mathop{\mathrm{E}}_{\sigma}\left[2^{|F_{\varphi,z}(\sigma)|}\right]$$

命題 8.15（イェンセンの不等式）より，

$$\tau(\varphi, z) \;=\; 2^{-n} \mathop{\mathrm{E}}_{\sigma}\left[2^{|F_{\varphi,z}(\sigma)|}\right] \;\geq\; 2^{-n} 2^{\mathrm{E}_\sigma[|F_{\varphi,z}(\sigma)|]} \;=\; 2^{-n+\mathrm{E}_\sigma[|F_{\varphi,z}(\sigma)|]}.$$

定義 6.5

任意の $d \in [n]$ について，φ の充足解 z が d-**孤立している**とは，以下の条件を満たすことである.

$$|\{i \in [n] : z \oplus e_i \notin \mathrm{SAT}(\varphi)\}| \;=\; d.$$

このとき，$z \oplus e_i \notin \mathrm{SAT}(\varphi)$ である x_i を d-**孤立変数**と呼ぶ．また，$z \oplus e_i \notin \mathrm{SAT}(\varphi)$ の要因となる節を d-**孤立節**と呼ぶ.

補題 6.7. φ の充足解 z が d-孤立しているとき，

$$\mathop{\mathrm{E}}_{\sigma}[F_{\varphi,z}(\sigma)] \;\geq\; \frac{d}{k}.$$

証明. 任意の $i \in [n]$ について，X_i を以下のような確率変数とする.

$$X_i \overset{\mathrm{def}}{=} \begin{cases} 1 & : \quad x_i \in F_{\varphi,z}(\sigma) \\ 0 & : \quad \text{o.w.} \end{cases}$$

よって，$F_{\varphi,z}(\sigma) = \sum_{i\in[n]} X_i$．期待値の線形性より，

$$\mathop{\mathrm{E}}_{\sigma}[F_{\varphi,z}(\sigma)] \;=\; \mathop{\mathrm{E}}_{\sigma}\left[\sum_{i\in[n]} X_i\right] \;=\; \sum_{i\in[n]} \mathop{\mathrm{E}}_{\sigma}[X_i].$$

主張 6.4. d-孤立変数 x_i について，

$$\mathop{\mathrm{E}}_{\sigma}[X_i] \;=\; \Pr_{\sigma}\{X_i = 1\} \;\geq\; \frac{1}{k}.$$

証明. 一般性を失うことなく $z(x_i) = 1$ とする．$z \oplus e_i \notin \mathrm{SAT}(\varphi)$ であることから，ある節 $C = (x_i \vee l_1 \vee l_2 \cdots \vee l_{k'-1}) \in \varphi$（$k' \in [k]$）が存在して，$z(x_i) = 1, z(l_1) = 0, z(l_2) = 0, \ldots, z(l_{k'-1}) = 0$. よって，

$$\Pr\{X_i = 1\} \;\geq\; \Pr_{\sigma}\{x_i \text{ が } \{x_i, l_1, \ldots, l_{k'-1}\} \text{ の中で最後}\} \;=\; \frac{1}{k'} \;\geq\; \frac{1}{k}.$$

■

この主張より，z は d-孤立していることから，

$$\mathop{\mathrm{E}}_{\sigma}[F_{\varphi,z}(\sigma)] \;=\; \sum_{i\in[n]} \mathop{\mathrm{E}}_{\sigma}[X_i] \;\geq\; \frac{d}{k}.$$

■

以上，二つの補題より，z が d_z-孤立しているとすれば，

$$\begin{aligned}
\Pr_{\sigma,t}\{\mathtt{PPZ}(\varphi) = \mathtt{YES}\} &= \sum_{z\in\mathrm{SAT}(\varphi)} \tau(\varphi, z) \\
&= \sum_{z\in\mathrm{SAT}(\varphi)} 2^{-n+\mathrm{E}_\sigma[|F_{\varphi,z}(\sigma)|]} \\
&\geq \sum_{z\in\mathrm{SAT}(\varphi)} 2^{-n+d_z/k}.
\end{aligned}$$

補題 6.8. （任意の $\varphi \in \mathrm{SAT}$ に対して）任意の充足解 z について，

$$\sum_{z\in\mathrm{SAT}(\varphi)} 2^{-(n-d_z)} \;\geq\; 1.$$

証明. $\sum_{z\in\mathrm{SAT}(\varphi)} 2^{d_z} \geq 2^n$ を示せばよい．これを n についての帰納法により示す．$n-1$ 変数論理式について不等式が成り立つとする．$n-1$ 変数論理式 $\varphi_0 \stackrel{\mathrm{def}}{=} \varphi|_{x_n=0}$ を考える．任意の $z \in \mathrm{SAT}(\varphi_0)$ について，

$$\begin{aligned}
d_z &= \{i \in [n-1] : z \oplus e_i \notin \mathrm{SAT}(\varphi_0)\} \\
d_{z0} &= \{i \in [n] : z0 \oplus e_i \notin \mathrm{SAT}(\varphi)\}
\end{aligned}$$

任意の $z \in \mathrm{SAT}(\varphi_0)$ について，$d_{z0} \geq d_z$.

問 6.7. $d_{z0} \geq d_z$ を証明しなさい.

よって，$\varphi_1 \stackrel{\mathrm{def}}{=} \varphi|_{x_n=1}$ についても同様であることから，

$$\begin{aligned}
\sum_{z\in\mathrm{SAT}(\varphi)} 2^{d_z} &= \sum_{z\in\mathrm{SAT}(\varphi):z(x_n)=0} 2^{d_z} + \sum_{z\in\mathrm{SAT}(\varphi):z(x_n)=1} 2^{d_z} \\
&= \sum_{z\in\mathrm{SAT}(\varphi_0)} 2^{d_{z0}} + \sum_{z\in\mathrm{SAT}(\varphi_1)} 2^{d_{z1}} \\
&\geq \sum_{z\in\mathrm{SAT}(\varphi_0)} 2^{d_z} + \sum_{z\in\mathrm{SAT}(\varphi_1)} 2^{d_z} \\
&\geq 2^{n-1} + 2^{n-1} \quad (\because \text{帰納仮定}) \\
&= 2^n.
\end{aligned}$$

■

この補題より，

$$\begin{aligned}
\Pr_{\sigma,t}\{\mathtt{PPZ}(\varphi)=\mathtt{YES}\} &\geq \sum_{z\in \mathrm{SAT}(\varphi)} 2^{-n+d_z/k} \\
&= 2^{-n+n/k} \sum_{z\in \mathrm{SAT}(\varphi)} 2^{-n/k+d_z/k} \\
&= 2^{-n(1-1/k)} \sum_{z\in \mathrm{SAT}(\varphi)} 2^{-(n-d_z)/k} \\
&\geq 2^{-n(1-1/k)} \sum_{z\in \mathrm{SAT}(\varphi)} 2^{-(n-d_z)} \\
&\geq 2^{-n(1-1/k)}.
\end{aligned}$$

系 6.9. 図 14 で示されたアルゴリズム $\mathtt{PPZ}(\varphi)$ について，$c = n\cdot 2^{n(1-1/k)}$ とすれば（よって，計算時間は $\widetilde{O}(2^{n(1-1/k)})$），以下のことが成り立つ：

$$\begin{aligned}
\varphi\in \mathrm{SAT} \quad &: \quad \Pr\{\mathtt{PPZ}(\varphi)=\mathtt{YES}\} \geq 1-e^{-n}, \\
\varphi\notin \mathrm{SAT} \quad &: \quad \Pr\{\mathtt{PPZ}(\varphi)=\mathtt{NO}\} = 1.
\end{aligned}$$

例えば，$k=3$ の場合，計算時間は $\widetilde{O}(2^{(2/3)n}) = \widetilde{O}(1.588^n)$.

問 6.8. 系 6.5 の証明にならって，この系を示しなさい.

7　ランダムサンプリング ～全域木を例に～

7.1　全域木の個数

定義 7.1

$G=(V,E)$ を任意の無向グラフとする．$V=[n]$ とする．A を G の隣接行列とする.（それゆえ，A は $n\times n$ の対称行列となる.）任意の $i\in[n]$ について，頂点 i の次数を d_i とする．D を $\mathrm{diag}(d_i)$ の対角行列とする．このとき，

$$L(G) \stackrel{\mathrm{def}}{=} D-A.$$

$L(G)$ を G の**ラプラシアン**と呼ぶ.

定義 7.2

$G=(V,E)$ を任意の無向グラフとする．$V=[n]$, $E=\{e_1,\ldots,e_m\}$ とする．グラフ G について，$n\times m$ 行列 M を次のように定義する．任意の $k\in[m]$ について，$e_k=(i,j)$ であるとき，$M_{i,k}=1$, $M_{j,k}=-1$.（それ以外の要素はすべて０.）

注 7.1. 行列 M の定義において,（表記を簡略化させるため）一般性を失うことなく，$e_k=(i,j)$ が $i<j$ を満たすものとする.

命題 7.1. $G=(V,E)$ を任意の無向グラフとする．$V=[n]$, $E=\{e_1,\ldots,e_m\}$ とする．このとき，

$$L(G)=MM^t.$$

証明. 任意の $i,j\in[n]$ について，

$$(MM^t)_{i,j} \;=\; \sum_{k\in[m]} M_{i,k}M_{j,k} \;=\; \begin{cases} -1 & : \; i\neq j \\ d_i & : \; i=j \end{cases}$$

■

定理 7.1 (ビネー・コーシーの定理)**.** X,Y をそれぞれ $n\times m$, $m\times n$ の行列とする.（ただし，$n\leq m$.）このとき，

$$\det(XY) \;=\; \sum_{S\subseteq[m]:|S|=n} \det(X(S))\det(Y(S)).$$

ただし，$X(S)$ は X から j 列（$j\in S$）を抜き出した $n\times n$ 行列，$Y(S)$ は Y から i 行（$i\in S$）を抜き出した $n\times n$ 行列，とする.

証明. $X=(x_{i,j}), Y=(y_{i,j})$ とする．このとき，

$$XY = \begin{pmatrix} \sum_{j\in[m]} x_{1,j}y_{j,1} & \cdots & \sum_{j\in[m]} x_{1,j}y_{j,n} \\ \vdots & \ddots & \vdots \\ \sum_{j\in[m]} x_{n,j}y_{j,1} & \cdots & \sum_{j\in[m]} x_{n,j}y_{j,n} \end{pmatrix}$$

よって，

$$\begin{aligned} \det(XY) &= \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma) \left(\sum_{j\in[m]} x_{1,j}y_{j,\sigma_1}\right) \cdots \left(\sum_{j\in[m]} x_{n,j}y_{j,\sigma_n}\right) \\ &= \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma) \sum_{j_1,\ldots,j_n\in[m]} x_{1,j_1}y_{j_1,\sigma_1}\cdots x_{n,j_n}y_{j_n,\sigma_n} \\ &= \sum_{j_1,\ldots,j_n\in[m]} x_{1,j_1}\cdots x_{n,j_n} \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma)\cdot y_{j_1,\sigma_1}\cdots y_{j_n,\sigma_n} \\ &= \sum_{j_1,\ldots,j_n\in[m]} x_{1,j_1}\cdots x_{n,j_n} \det(Y(j_1,\ldots,j_n)) \\ &= \sum_{j_1,\ldots,j_n\in[m]:j_a\neq j_b} x_{1,j_1}\cdots x_{n,j_n} \det(Y(j_1,\ldots,j_n)). \end{aligned}$$

一方，

$$\begin{aligned} &\sum_{S\subseteq[m]:|S|=n} \det(X(S))\det(Y(S)) \\ =\ &\sum_{1\le j_1<\cdots<j_n\le m} \det(X(j_1,\ldots,j_n))\det(Y(j_1,\ldots,j_n)) \\ =\ &\sum_{1\le j_1<\cdots<j_n\le m} \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma)\cdot x_{1,j_{\sigma_1}}\cdots x_{n,j_{\sigma_n}} \det(Y(j_1,\ldots,j_n)). \end{aligned}$$

主張 7.1. 任意の $\sigma\in S_n$，任意の $1\le j_1<\cdots<j_n\le m$ について，

$$\operatorname{sgn}(\sigma)\cdot\det(Y(j_1,\ldots,j_n)) = \det(Y(j_{\sigma_1},\ldots,j_{\sigma_n})).$$

問 7.1. 上の主張を示しなさい．

この主張より，

$$\begin{aligned} &\sum_{S\subseteq[m]:|S|=n} \det(X(S))\det(Y(S)) \\ =\ &\sum_{1\le j_1<\cdots<j_n\le m} \sum_{\sigma\in S_n} x_{1,j_{\sigma_1}}\cdots x_{n,j_{\sigma_n}} \det(Y(j_{\sigma_1},\ldots,j_{\sigma_n})). \end{aligned}$$

主張 7.2. 任意の関数 $f:[m]^n\to\mathbb{R}$ について，

$$\sum_{1\le j_1<\cdots<j_n\le m} \sum_{\sigma\in S_n} f(j_{\sigma_1},\ldots,j_{\sigma_n}) = \sum_{j_1,\ldots,j_n\in[m]:j_a\neq j_b} f(j_1,\ldots,j_n).$$

問 7.2. 上の主張を示しなさい.

この主張より，$f(j_1,\ldots,j_n) = x_{1,j_1}\ldots x_{n,j_n}\det(Y(j_1,\ldots,j_n))$ とすれば,

$$\begin{aligned}
&\sum_{S\subseteq[m]:|S|=n} \det(X(S))\det(Y(S)) \\
=\ &\sum_{j_1,\ldots,j_n\in[m]:j_a\neq j_b} x_{1,j_1}\ldots x_{n,j_n}\det(Y(j_1,\ldots,j_n)) \\
=\ &\det(XY).
\end{aligned}$$

■

定義 7.3

$G=(V,E)$ を任意の無向グラフとする．G の部分グラフ $G'=(V,E')$（$E'\subseteq E$）が木であるとき，G' を**全域木**という．G の全域木の集合を $\mathcal{T}_G$，その大きさを $\kappa(G)$ と表記する．

定理 7.2 (行列木定理)**.** $G=(V,E)$ を任意の無向グラフとする．L' を $L(G)$ から最後の行と列を削除して得られる $(n-1)\times(n-1)$ の（対称）行列とする．このとき,

$$\kappa(G) \ = \ \det(L').$$

注 7.2. $L(G)$ から削除する行と列は，任意の $i\in[n]$ の行と列でも同じことがいえる.

証明. $V=[n]$, $E=\{e_1,\ldots,e_m\}$ とする．M' を M から最後の行を削除して得られる $(n-1)\times m$ 行列とすれば，命題 7.1 より,

$$L' \ = \ M'M'^t.$$

よって，定理 7.1 より,

$$\begin{aligned}
\det(L') &= \det(M'M'^t) \\
&= \sum_{S\subseteq[m]:|S|=n-1} \det(M'(S))\det(M'^t(S)) \\
&= \sum_{S\subseteq[m]:|S|=n-1} \det(M'(S))\det(M'(S)) \\
&= \sum_{S\subseteq[m]:|S|=n-1} \det(M'(S))^2.
\end{aligned}$$

主張 7.3. 任意の $S\subseteq[m]:|S|=n-1$ について,

$$\det(M'(S)) \ = \ \begin{cases} \pm 1 & : \ \{e_k : k\in S\} \text{ が全域木である} \\ 0 & : \ \text{o.w.} \end{cases}$$

証明. $\{e_k : k\in S\}$ が全域木である場合，$\det(M'(S))=\pm1$ であることを $|V|$ についての帰納法により示す．$|V|=2$（$|S|=1$）のとき，$M'(S)=(1)$（1×1 の行列）より明らか.

問 7.3. $|V| = 2$（$|S| = 1$）のとき，$M'(S) = (1)$ である理由を説明しなさい．

$|V| = n-1$（$|S| = n-2$）のとき主張が成り立つ（任意の G，任意の S に対して，$\{e_k : k \in S\}$ が全域木であれば $\det(M'(S)) = \pm 1$）とする．$|V| = n$（$|S| = n-1$）のとき，$\{e_k : k \in S\}$ が全域木であるとする．一般性を失うことなく，$1 \in S$ かつ $e_1 = (n-1, n)$ とする．このとき，M'' を M' から最後の行を削除（M から最後の二行を削除）して得られる $(n-2) \times m$ 行列とすれば，$\det(M'(S)) = \det(M''(S \setminus \{1\})) = \pm 1$.（下図参照.）

$$M(S) = \left(\begin{array}{c:c} \begin{matrix} 0 \\ 0 \\ \vdots \\ 0 \\ 0 \end{matrix} & M''(S \setminus \{1\}) \\ \hdashline 1 & \\ \hline -1 & \end{array}\right) \begin{matrix} 1 \\ 2 \\ \vdots \\ n-3 \\ n-2 \\ n-1 \\ n \end{matrix}$$

問 7.4. $\det(M''(S \setminus \{1\})) = \pm 1$ となることを示しなさい.（ヒント：頂点 $n-1$ と頂点 n を縮約した全域木 $\{e_k : k \in S \setminus \{1\}\}$ に帰納仮定が適用できる.）

$\{e_k : k \in S\}$ が全域木でないとする．このとき，$\{e_k : k \in S\}$ に閉路 C が存在する．一般性を失うことなく $C = \{e_1, \ldots, e_c\}$ とする．更に，$e_1 = (1, 2), \ldots, e_c = (c, 1)$ とする．このとき，$M'(S)$ の第 1 列から第 c 列は独立でない．よって，$\det(M'(S)) = 0$.

問 7.5. $M'(S)$ の第 1 列から第 c 列が独立でないことを示しなさい．

■

この主張より，$\det(L')$ は G の全域木の個数となる． ■

7.2 行列木定理を用いたサンプリング

定義 7.4

$G = (V, E)$ を任意の無向グラフとする．任意の辺 $e = (u, v) \in E$ について，e を**縮約する**とは，G を以下のように定義されるグラフ $G' = (V', E')$ にする操作である．

$$\begin{aligned} V' &= V \setminus \{v\} \\ E' &= \{(a, b) \in E : a \neq v \wedge b \neq v\} \cup \{(a, u) : (a, v) \in E, a \neq u\} \end{aligned}$$

一方，e を**除去する**とは，G を $G' = (V, E \setminus \{e\})$ にする操作である．辺の縮約を $G/\{e\}$，辺の除去を $G \backslash \{e\}$ と表記する．

命題 7.2. $G = (V, E)$ を任意のグラフ，$e \in E$ を任意の辺とする．このとき，$\{T \in \mathcal{T}_G : e \in T\}$ と $\mathcal{T}_{G/\{e\}}$ に全単射が存在する．また，$\{T \in \mathcal{T}_G : e \notin T\}$ と $\mathcal{T}_{G \backslash \{e\}}$ に全単射が存在する．

証明. ■

問 7.6. この命題を証明しなさい.

この命題より，$p(G,e) \stackrel{\text{def}}{=} \kappa(G/\{e\})/\kappa(G)$ とすれば，G の全域木の一様サンプリングは，図 15 のようになる.

入力：無向グラフ $G=(V,E)$　// $E=\{e_1,\ldots,e_m\}$

1. $S=\emptyset$ とする.（S が出力になる.）
2. それぞれの $i\in[m]$ について以下を繰り返す.
   (a) 確率 $p(G,e_i)$ で $e_i\in S$ とする.（確率 $1-p(G,e_i)$ で $e_i\notin S$ とする.）
   (b) $e_i\in S$ なら $G=G/\{e_i\}$，$e_i\notin S$ なら $G=G\backslash\{e_i\}$ とする.
3. S を出力する.

図 15: 全域木のサンプリング

定理 7.3. 図 15 のアルゴリズムを A とする．任意のグラフ $G=(V,E)$，任意の全域木 $T\in\mathcal{T}_G$ について，

$$\Pr\{A(G)=T\} \;=\; \frac{1}{|\mathcal{T}_G|}.$$

証明. 命題 7.2 より[21]，任意の $e\in E$ について，

$$\begin{aligned} |\mathcal{T}_G| &= |\{T\in\mathcal{T}_G : e\in T\}| + |\{T\in\mathcal{T}_G : e\notin T\}| \\ &= |\mathcal{T}_{G/\{e\}}| + |\mathcal{T}_{G\backslash\{e\}}| \\ &= \kappa\left(\mathcal{T}_{G/\{e\}}\right) + \kappa\left(\mathcal{T}_{G\backslash\{e\}}\right) \end{aligned}$$

よって，e が全域木の辺である割合が $p(G,e)$，そうでない割合が $1-p(G,e)$ となる. ■

7.3 マルコフ連鎖

定義 7.5

状態空間を Ω と表記する．確率過程 $X_0,X_1,X_2,\cdots\in\Omega$ が**マルコフ連鎖**であるとは，任意の時刻 $t\in\mathbb{N}_0$，任意の状態 $x_0,x_1,\ldots,x_t\in\Omega$ について，以下を満たすことである.

$$\Pr\{X_t=x_t|X_0=x_0,X_1=x_1,\ldots,X_{t-1}=x_{t-1}\} \;=\; \Pr\{X_t=x_t|X_{t-1}=x_{t-1}\}.$$

以降では，状態空間は有限である（$|\Omega|<\infty$）ものとする.

[21] 厳密には，$i\in[m]$ についての帰納法により示す.

定義 7.6

$X_0, X_1, X_2, \cdots \in \Omega$ をマルコフ連鎖 $\mathcal{M}$ とする．任意の状態 $i, j \in \Omega$ について，$P_{i,j} = \Pr\{X_t = j | X_{t-1} = i\}$ を $\mathcal{M}$ の**遷移確率**という．遷移確率 P は，任意の $i \in \Omega$ について，$\sum_{j \in \Omega} P_{i,j} = 1$ を満たす．

Ω 上の確率分布を π とする．($\sum_{x \in \Omega} \pi(x) = 1.$) P を $|\Omega| \times |\Omega|$ の行列，π を $|\Omega|$ 次元のベクトルとみなしたとき，π が ${}^t\pi P = {}^t\pi$ を満たしたとき，π を**定常分布**という．

例 7.1 (マルコフ連鎖)**.** 任意の $n \in \mathbb{N}$ に対して，$\Omega = \{0,1\}^n$ とする．任意の $x, x' \in \Omega$ に対して，遷移確率 P を以下のように定義する．

$$P(x, x') \stackrel{\text{def}}{=} \begin{cases} \dfrac{1}{n} & : \quad d(x, x') = 1 \\ 0 & : \quad \text{o.w.} \end{cases}$$

ただし，$d(x, x')$ をハミング距離とする．

事実 7.3. 上の例において，$\pi(x) = 1/2^n$ は定常分布である．

問 7.7. この事実を示しなさい．

定義 7.7

$\mathcal{M}$ を Ω 上のマルコフ連鎖，P を $\mathcal{M}$ の遷移確率とする．以下の条件を満たす分布 π が存在するとき，$\mathcal{M}$ は**可逆**であるという．

$$\forall x, y \in \Omega [\pi(x) P(x, y) = \pi(y) P(y, x)]. \tag{5}$$

事実 7.4. 上の例のマルコフ連鎖は可逆である．

問 7.8. この事実を示しなさい．

定理 7.4. 可逆性の式 (5) を満たす分布 π は定常分布である．

証明. 横ベクトル ${}^t\pi P$ の j 番目の要素は，

$$\sum_{i \in \Omega} \pi_i P_{i,j} \;=\; \sum_{i \in \Omega} \pi_j P_{j,i} \;=\; \pi_j.$$

よって，${}^t\pi P = {}^t\pi$ を満たす．これは，π が $\mathcal{M}$ の定常分布であることを意味する． ■

定義 7.8

$\mathcal{M}$ を Ω 上のマルコフ連鎖，P を $\mathcal{M}$ の遷移確率とする．$\mathcal{M}$ が**既約**であるとは，任意の状態 $i, j \in \Omega$ について，ある $t \in \mathbb{N}$ が存在して，$P^t(i, j) > 0$ であることである．$\mathcal{M}$ が**非周期的**であるとは，任意の状態 $i \in \Omega$ について，$\gcd\{t \in \mathbb{N} : P^t(i, i) > 0\} = 1$ であることである．すべての状態が既約かつ非周期的であるマルコフ連鎖は**エルゴード的**であるという．

定理 7.5. エルゴード的であるマルコフ連鎖は，唯一の定常分布をもつ．

例 7.2 (エルゴード的)**.** 任意の $n \in \mathbb{N}$ に対して，$\Omega = \{0,1\}^n$ とする．任意の $x, x' \in \Omega$ に対して，P を以下のように定義する．

$$P(x,x') \stackrel{\text{def}}{=} \begin{cases} \frac{1}{2} & : \quad x = x' \\ \frac{1/2}{n} & : \quad d(x,x') = 1 \\ 0 & : \quad \text{o.w.} \end{cases}$$

事実 7.5. 上の例のマルコフ連鎖はエルゴード的である．

問 7.9. この事実を示しなさい．

7.4 ランダムウォークを用いたサンプリング

$G = (V,E)$ を任意の（連結な）無向グラフとする．G 上の次のようなランダムウォーク $X_0, X_1, X_2, \cdots \in V$ を考える．任意の時刻 $t \in \mathbb{N}_0$ について，

$$\forall u \in V \left[\left(\Pr\{X_{t+1} = u | X_t = u\} = \frac{1}{2} \right) \wedge \left(\forall v \in N_u \left[\Pr\{X_{t+1} = v | X_t = u\} = \frac{1/2}{d_u} \right] \right) \right].$$

事実 7.6. 確率過程 $X_0, X_1, X_2, \ldots$ はマルコフ連鎖である．

問 7.10. この事実を示しなさい．

事実 7.7. マルコフ連鎖 $X_0, X_1, X_2, \ldots$ はエルゴード的である．

問 7.11. この事実を示しなさい．

命題 7.8. マルコフ連鎖 $X_0, X_1, X_2, \ldots$ の（唯一の）定常分布 π は，$\pi(v) = d_v/(2|E|)$．（よって，$\pi(v)/d_v$ は一定．）

証明. $\sum_{v \in V} \pi(v) = \sum_{v \in V} d_v/(2|E|) = 1$ であり，更に，π が可逆性の式 (5) を満たすので，定理 7.4 より，π は定常分布となる．

問 7.12. $\sum_{v \in V} \pi(v) = 1$，及び，式 (5) が満たされることを示しなさい．

■

定義 7.9

T を G の任意の部分木，$v \in V$ を T の任意の頂点とする．頂点 v を根とした根付き木 (T, v) を T_v と表記する．このとき，T_v のすべての無向辺を v に向かう向きにした有向木 T_v を B**木**（*backward tree*）と呼び，すべての辺をその逆にした有向木 T_v を F**木**（*forward tree*）と呼ぶ．G の全域木の集合 $\mathcal{T}_G$ に対して，

$$\mathcal{B}_G \stackrel{\text{def}}{=} \bigcup_{v \in V} \mathcal{B}_G(v), \quad \mathcal{B}_G(v) \stackrel{\text{def}}{=} \{T_v : T \in \mathcal{T}_G,\ T_v \text{ は B 木}\}$$
$$\mathcal{F}_G \stackrel{\text{def}}{=} \bigcup_{v \in V} \mathcal{F}_G(v), \quad \mathcal{F}_G(v) \stackrel{\text{def}}{=} \{T_v : T \in \mathcal{T}_G,\ T_v \text{ は F 木}\}$$

事実 7.9. 任意の頂点 $v \in V$ について，$\mathcal{B}_G(v)$ と $\mathcal{T}_G$，及び，$\mathcal{F}_G(v)$ と $\mathcal{T}_G$，は一対一対応である．

問 7.13. この事実を示しなさい．

先のランダムウォーク $X_0, X_1, X_2, \cdots \in V$ に対して，任意の時刻 $t \in \mathbb{N}_0$ について，以下のような有向木 $B_t = (V_t, E_t)$ を考える．

$$\begin{aligned} V_t &= \{X_0, X_1, \ldots, X_t\} \\ E_t &= \{(X_{\ell_v(t)}, X_{\ell_v(t)+1}) : v \in V_t \setminus \{X_t\}\} \end{aligned}$$

ただし，$\ell_v(t) \in [t] \cup \{0\}$ は，v を最後に訪問した時刻，つまり，

$$\ell_v(t) \stackrel{\text{def}}{=} \max\{i \in [t] \cup \{0\} : X_i = v\}.$$

事実 7.10. B_t は X_t を根とした B 木である．

問 7.14. この事実を示しなさい．

B 木 B_t が最初に全域木になった時刻を C，つまり，

$$C \stackrel{\text{def}}{=} \min\{t \cup \{0\} : B_t \in \mathcal{B}_G\}.$$

命題 7.11. 任意の $t \geq C$ について，B_t は $\mathcal{B}_G$ 上のマルコフ連鎖である．また，B_t はエルゴード的である．

問 7.15. この命題を示しなさい．

定理 7.5 より，マルコフ連鎖 B_t は唯一の定常分布 σ をもつ．（マルコフ連鎖 $X_0, X_1, X_2, \ldots$ の定常分布は π.）任意の有向辺 $e = (u, v)$ について，$w(e) = 1/d_u$ とする．

補題 7.12. 任意の $v \in V$，任意の B 木 $T_v \in \mathcal{B}_G(v)$ について，

$$\sigma(T_v) \propto \prod_{e \in T_v} w(e) = \frac{d_v}{\prod_{u \in V} d_u}.$$

証明. ■

系 7.13. 任意の $v \in V$，任意の B 木 $T_v, T'_v \in \mathcal{B}_G(v)$ について，$\sigma(T_v) = \sigma(T'_v)$.

問 7.16. この系を証明しなさい.

次に，先のランダムウォーク $X_0, X_1, X_2 \cdots \in V$ に対して，任意の時刻 $t \in \mathbb{N}_0$ について，以下のような有向木 $F_t = (V_t, E_t)$ を考える.

$$\begin{aligned} V_t &= \{X_0, X_1, \ldots, X_t\} \\ E_t &= \{(X_{f_v(t)-1}, X_{f_v(t)}) : v \in V_t \setminus \{X_0\}\} \end{aligned}$$

ただし，$f_v(t) \in [t] \cup \{0\}$ は，v を最初に訪問した時刻，つまり，

$$f_v(t) \stackrel{\text{def}}{=} \min\{i \in [t] \cup \{0\} : X_i = v\}.$$

事実 7.14. F_t は X_0 を根とした F 木である.

F 木 F_t が最初に全域木になった時刻を C，つまり，

$$C \stackrel{\text{def}}{=} \min\{t \cup \{0\} : F_t \in \mathcal{F}_G\}.$$

補題 7.15. 任意の $v \in V$，任意の F 木 $T_v \in \mathcal{F}_G(v)$ について，

$$\Pr\{F_C = T_v | X_0 = v\} = \frac{\sigma(T_v)}{\pi(v)}.$$

証明. 任意の頂点列 $u_0, u_1, \ldots, u_t \in V$（ただし，$(u_i, u_{i+1}) \in E$）について，

$$\begin{aligned} \Pr\{\forall i \in [t] \cup \{0\}[X_i = u_i] | X_0 \leftarrow \pi\} &= \pi(u_0) \prod_{i \in [t-1] \cup \{0\}} 1/d(u_i) \\ &= \pi(u_0)/d(u_0) \prod_{i \in [t-1]} 1/d(u_i) \\ &= \pi(u_t)/d(u_t) \prod_{i \in [t-1]} 1/d(u_i) \quad (\because \text{命題 7.8}) \\ &= \pi(u_t) \prod_{i \in [t]} 1/d(u_i) \\ &= \Pr\{\forall i \in [t] \cup \{0\}[X_i = u_{t-i}] | X_0 \leftarrow \pi\}. \end{aligned}$$

よって，任意の $t \in \mathbb{N}_0$，任意の頂点 $u, v \in V$，任意の頂点列 $u = u_0, u_1, \ldots, u_t = v$，それに，その頂点列から形成される B 木及び F 木 T_v について，

$$\Pr\{B_t = T_v | X_0 \leftarrow \pi\} = \Pr\{F_t = T_v | X_0 \leftarrow \pi\}.$$

問 7.17. この事実を示しなさい.（同じ頂点列から形成される B 木と F 木が同じになることを示す.）

これより，任意の根付き木 T_v について，

$$\begin{aligned}
\sigma(T_v) &= \lim_{N\to\infty} \sum_{t\in[N]} \Pr\{B_t = T_v | X_0 \leftarrow \pi\} \\
&= \lim_{N\to\infty} \sum_{t\in[N]} \Pr\{F_t = T_v | X_0 \leftarrow \pi\} \\
&= \lim_{N\to\infty} \sum_{t\in[N]} \pi(v) \Pr\{F_t = T_v | X_0 = v\} \\
&= \pi(v) \Pr\{F_C = T_v | X_0 = v\}.
\end{aligned}$$

■

定理 7.6. 任意の $v \in V$，任意の F 木 $T_v \in \mathcal{F}_G(v)$ について，

$$\Pr\{F_C = T_v | X_0 = v\} \propto \frac{d_v/\pi(v)}{\prod_{u\in V} d_u}.$$

証明. 補題 7.12，補題 7.15 より. ■

系 7.16. 任意の $v \in V$，任意の F 木 $T_v \in \mathcal{F}_G(v)$ について，

$$\Pr\{F_C = T_v | X_0 = v\} = \frac{1}{|\mathcal{F}_G(v)|} = \frac{1}{|\mathcal{T}_G|}.$$

この系より，G の全域木の一様サンプリングは，図 16 のようになる.

入力：無向グラフ $G = (V, E)$

1. $v \in V$ を任意の頂点とする.
2. $X_0 = v$ として，$\{X_0, X_1, X_2, \ldots, X_t\} \neq V$ である限りランダムウォークを繰り返す.
3. F_t を出力する.

図 16: 全域木のサンプリング

7.5 カップリング補題を用いたサンプリング

定義 7.10

Ω を状態空間とする．Ω 上の分布 π_1, π_2 の**距離** を $|\pi_1 - \pi_2|$ と表記して，以下のように定義する．

$$|\pi_1 - \pi_2| \stackrel{\text{def}}{=} \frac{1}{2}\sum_{x\in\Omega}|\pi_1(x) - \pi_2(x)|$$

命題 7.17.

$$\frac{1}{2}\sum_{x\in\Omega}|\pi_1(x) - \pi_2(x)| = \max_{S\subseteq\Omega}|\pi_1(S) - \pi_2(S)|.$$

事実 7.18. この命題を証明しなさい．

定義 7.11

$\mathcal{M}$ を Ω 上のマルコフ連鎖，P を $\mathcal{M}$ の遷移確率，π を $\mathcal{M}$ の定常分布とする．状態 $x \in \Omega$ から始めて，t 回の状態遷移を行った後の確率分布を p_x^t と表記する．つまり，$\mathbf{1}_x$ を x の指示ベクトルとすれば，

$$p_x^t \stackrel{\text{def}}{=} P^t \cdot \mathbf{1}_x.$$

このとき，任意の $\epsilon > 0$ について，

$$\tau(\epsilon) \stackrel{\text{def}}{=} \max_{x\in\Omega}\min\{t \in \mathbb{N}_0 : |p_x^t - \pi| \le \epsilon\}.$$

$\tau(\epsilon)$ を $\mathcal{M}$ の**混合時間**と呼ぶ．

定義 7.12

Z_t を Ω 上のマルコフ連鎖，P を Z_t の遷移確率とする．Z_t の**カップリング**とは，次を満たす $\Omega \times \Omega$ 上のマルコフ連鎖 (A_t, B_t) である．任意の $a, a', b, b' \in \Omega$ について，

$$\begin{aligned}\Pr\{A_1 = a' | A_0 = a, B_0 = b\} &= P(a, a')\\ \Pr\{B_1 = b' | A_0 = a, B_0 = b\} &= P(b, b')\end{aligned}$$

事実 7.19. Z_t を Ω 上のマルコフ連鎖，P を Z_t の遷移確率，(A_t, B_t) を Z_t のカップリングとする．このとき，任意の $t \in \mathbb{N}_0$，任意の $a, a', b, b' \in \Omega$ について，

$$\begin{aligned}\Pr\{A_t = a' | A_0 = a, B_0 = b\} &= P^t(a, a')\\ \Pr\{B_t = b' | A_0 = a, B_0 = b\} &= P^t(b, b')\end{aligned}$$

補題 7.20 (カップリング補題)**.** Z_t を Ω 上のマルコフ連鎖，$\tau(\epsilon)$ を Z_t の混合時間とする．このとき，Z_t の任意のカップリング (A_t, B_t) について以下が成り立つ．任意の $t \in \mathbb{N}_0$，任意の $\epsilon > 0$ について，

$$\Pr\{A_t \neq B_t | A_0 = a, B_0 = b\} \le \epsilon \implies \tau(\epsilon) \le t.$$

証明. (A_t, B_t) を Z_t のカップリングとする．$a \in \Omega$ を任意，$b \in \Omega$ を π に従う任意のものとする．任意の $S \subseteq \Omega$ について，

$$\begin{aligned}
\Pr\{A_t \in S | A_0 = a\} &= \Pr\{A_t \in S | A_0 = a, B_0 = b\} \\
&\geq \Pr\{A_t = B_t \wedge A_t \in S | (*)\} \\
&= 1 - \Pr\{A_t \neq B_t \vee B_t \notin S | (*)\} \\
&\geq 1 - \Pr\{A_t \neq B_t | (*)\} - \Pr\{B_t \notin S | (*)\} \\
&= (1 - \Pr\{B_t \notin S | (*)\}) - \Pr\{A_t \neq B_t | (*)\} \\
&\geq \Pr\{B_t \in S | (*)\} - \epsilon \\
&= \Pr\{B_t \in S\} - \epsilon \\
&= \pi(S) - \epsilon.
\end{aligned}$$

ただし，$(*)$ を事象 $A_0 = a, B_0 = b$ とする．上の式において，$S = \Omega \setminus S$ とすれば，$\Pr\{A_t \in S | A_0 = a\} \leq \pi(S) + \epsilon$ も同様に示される．

問 7.18. この事実を示しなさい．

これらより，$|\Pr\{A_t \in S | A_0 = a\} - \pi(S)| \leq \epsilon$，つまり，任意の $a \in \Omega$ について $|p_a^t - \pi| \leq \epsilon$ が示される．よって，$\tau(\epsilon) \leq t$ となる． ■

$G = (V, E)$ を任意の無向グラフとする．前節のランダムウォーク $X_0, X_1, X_2, \cdots \in V$ に対して，全域木 $T_i = (V, E_i)$ を次のように定義する．T_0 を任意の全域木として，

$$E_i \stackrel{\text{def}}{=} \begin{cases} E_{i-1} & (X_{i-1}, X_i) \in E_{i-1} \\ E_{i-1} \cup \{(X_{i-1}, X_i)\} \setminus \{D_i\} & (X_{i-1}, X_i) \notin E_{i-1} \end{cases}$$

ただし，D_i を次のように定義する．$(X_{i-1}, X_i) \notin E_{i-1}$ であるとき，$T_{i-1} \cup \{(X_{i-1}, X_i)\}$ に（唯一の）閉路 $(X_{i-1}, X_i, u_1, u_2, \ldots, X_{i-1})$ が存在する．これについて，$D_i = (X_i, u_1)$ とする．

事実 7.21. T_i は $\mathcal{T}_G$ 上のマルコフ連鎖である．また，T_i はエルゴード的である．

問 7.19. この事実を示しなさい．

定理 7.5 より，マルコフ連鎖 T_i は唯一の定常分布 σ をもつ．（マルコフ連鎖 $X_0, X_1, X_2, \ldots$ の定常分布は π.）

事実 7.22. マルコフ連鎖 T_i は可逆である．よって，その定常分布は一様分布となる．

問 7.20. この事実を示しなさい．

$\{X_0, X_1, \ldots, X_t\} = V$ となった最初の時刻を C，つまり，

$$C \stackrel{\text{def}}{=} \min\{t \cup \{0\} : \{X_0, X_1, \ldots, X_t\} = V\}.$$

定理 7.7. 任意のグラフ $G = (V, E)$，任意の全域木 $T \in \mathcal{T}_G$ について，

$$\Pr\{T_C = T\} = \frac{1}{|\mathcal{T}_G|}.$$

証明. マルコフ連鎖 T_i のカップリング (A_i, B_i) を次のように定義する．A_0, B_0 を任意の全域木として，A_0, B_0 に（共通の）ランダムウォーク $X_0, X_1, \ldots, X_C \in V$ を適用する．

主張 7.4. $(A_i B_i)$ は T_i のカップリングである．

問 7.21. この主張を示しなさい．

任意の $i \in [C]$ について，$W_i = \{X_0, X_1, \ldots, X_i\} \subseteq V$ とする．

主張 7.5. 任意の $i \in [C]$ について，$A[W_i], B[W_i]$ は同一の（$A[W_i] = B[W_i]$ となる）木である．

証明. ランダムウォークの遷移回数 i についての帰納法により示す．$i = 0$ のとき，$|W_0| = |\{X_0\}| = 1$ より，$A[W_i], B[W_i]$ が同一の木であることは明らか．$i = k - 1$ のとき，$A[W_i], B[W_i]$ が同一の木であるとする．$i = k$ のとき，$X_k \in \{X_0, X_1, \ldots, X_{k-1}\}$ であれば，$W_k = W_{k-1}$ であることから，帰納仮定より，$A[W_k], B[W_k]$ が同一の木であることは明らか．

問 7.22. この事実を示しなさい．

$X_k \notin \{X_0, X_1, \ldots, X_{k-1}\}$ であるとき，$X_k \notin W_{k-1}$ であり，帰納仮定から $A[W_{k-1}], B[W_{k-1}]$ が（同一の）木であることから，$N_A(X_k) = N_B(X_k) = \{X_{k-1}\}$ となる．

問 7.23. この事実を示しなさい．

よって，帰納仮定より，$A[W_k], B[W_k]$ は同一の木となる． ■

この主張より，$A[W_C] = B[W_C]$ となる．よって，カップリング補題を適用（$t = C$, $\epsilon = 0$）すれば定理が示される． ■

この命題より，全域木のサンプリングは以下の図 17 のようになる．

入力：無向グラフ $G = (V, E)$

1. T_0 を任意の全域木とする．
2. $\{X_0, X_1, X_2, \ldots, X_t\} \neq V$ である限りランダムウォークを繰り返す．
3. T_t を出力する．

図 17: 全域木のサンプリング

8　エクスパンダーグラフ

ここでは，d-正則無向グラフを扱う．$|V| = n$ のとき，d-正則無向グラフ G を (n, d)-グラフと呼ぶ．任意の $u \in V$ について，$\Gamma(u) \stackrel{\text{def}}{=} \{v \in V : (u, v) \in E\}$ とする．任意の $S \subseteq V$ について，$\Gamma(S) \stackrel{\text{def}}{=} \bigcup_{u \in S} \Gamma(u)$，$\partial(S) \stackrel{\text{def}}{=} E(S, \bar{S}) \stackrel{\text{def}}{=} (S \times \bar{S}) \cap E$，とする．

定義 8.1

G を (n, d)-グラフとする．以下の条件を満たすとき，G を (n, d, α)-**頂点エクスパンダー**（(n, d, α)-**vertex expander**）と呼ぶ．

$$\min_{S \subseteq V : |S| \leq n/2} \left\{ \frac{|\Gamma(S)|}{|S|} \right\} \ \geq \ \alpha.$$

このとき，α を**頂点拡張度**（**vertex-expansion**）という．また，以下の条件を満たすとき，G を (n, d, β)-**辺エクスパンダー**（(n, d, β)-**edge expander**）と呼ぶ．

$$\min_{S \subseteq V : |S| \leq n/2} \left\{ \frac{|\partial(S)|}{d|S|} \right\} \ \geq \ \beta.$$

このとき，β を**辺拡張度**（**edge-expansion**）という．上記不等式の左辺を $h(G)$ と表記する．

事実 8.1. $0 \leq \alpha, \beta \leq 1$.

問 8.1. この事実が成り立つ理由を説明しなさい．

8.1　スペクトル拡張度

ここでは，スペクトル拡張度と，頂点拡張度・辺拡張度との関係を示す．

定義 8.2

G を (n, d)-グラフとする．A を G の隣接行列とする．A の固有値を $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$ とする．$\lambda \stackrel{\text{def}}{=} \min\{|\lambda_2|, |\lambda_n|\}$ としたとき，G を (n, d, λ)-**エクスパンダー**（(n, d, λ)-**expander**）と呼ぶ．このとき，λ を**スペクトル拡張度**（**spectral expansion**）という．

以降，隣接行列 A の固有値 λ_i に対応する正規固有ベクトルを $\boldsymbol{v}_i$ と表す．つまり，任意の $i \in [n]$ について，$A\boldsymbol{v}_i = \lambda_i \boldsymbol{v}_i$, $\|\boldsymbol{v}_i\|_2 = 1$.

事実 8.2. (n, d)-グラフ G の隣接行列 A の固有値 λ_i，正規固有ベクトル $\boldsymbol{v}_i$ に関して，以下のことが成り立つ．

- $\lambda_1 = d$, $\boldsymbol{v}_1 = \mathbf{1}/\sqrt{n}$．更に，任意の $i \in [n]$ について，$|\lambda_i| \leq d$.
- G が連結であることは $\lambda_2 < d$ と同値である．
- G が連結であるとき，G が二部グラフであることは $\lambda_n = -d$ と同値である．

以降，この事実より，(d-正則無向で）連結非二部グラフを扱う．

8.1.1 辺拡張度との関係

スペクトル拡張度と辺拡張度の関係は，チーガーの不等式（cheeger's inequality）の離散版（グラフ版）と呼ばれ，以下の不等式で示される．

$$\left(\frac{1-(\lambda/d)}{2} \leq\right) \quad \frac{1-(\lambda_2/d)}{2} \;\leq\; h(G) \;\leq\; \sqrt{2(1-(\lambda_2/d))} \quad \left(\leq\; \sqrt{2(1-(\lambda/d))}\right).$$

命題 8.3. $(1-(\lambda_2/d))/2 \leq h(G)$.

注 8.1. この命題は次のことを意味する．G が (n,d,λ)-エクスパンダーであれば，(n,d,β)-辺エクスパンダーである．ただし，$\beta = (1-(\lambda/d))/2$.

証明. 任意の $S \subseteq V$（$|S| \leq |V|/2$）について，$\partial(S) \geq ((d-\lambda_2)/2)|S|$ であることを示す．$S \subseteq V$（$|S| \leq |V|/2$）を任意に固定する．G の隣接行列を A とする．このとき，

$$\partial(S) \;=\; \mathbf{1}_S^\top A \mathbf{1}_{\bar{S}} \;=\; d|S| - \mathbf{1}_S^\top A \mathbf{1}_S.$$

問 8.2. これら二つの等式を示しなさい．

A の（正規）固有ベクトルを $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ とする．（$\boldsymbol{v}_1 = \mathbf{1}/\sqrt{n}$.）これらは直交基底であることから，$c_1, \ldots, c_n$ が存在して，

$$\mathbf{1}_S \;=\; c_1\boldsymbol{v}_1 + \cdots + c_n\boldsymbol{v}_n.$$

このとき，$\sum_{i\in[n]} c_i^2 = |S|$．また，$(\mathbf{1}_S, \boldsymbol{v}_1) = |S|/\sqrt{n}$ より，$c_1 = (\sum_{i\in[n]} c_i\boldsymbol{v}_i, \boldsymbol{v}_1) = |S|/\sqrt{n}$.

問 8.3. これらの事実が成り立つ理由を説明しなさい．

以上より，

$$\begin{aligned}
\mathbf{1}_S^\top A \mathbf{1}_S &= \left(\sum_i c_i\boldsymbol{v}_i, \sum_i c_i\lambda_i\boldsymbol{v}_i\right) \\
&= \sum_i c_i^2\lambda_i \\
&\leq \frac{|S|^2}{n}d + \lambda_2(|S| - |S|^2/n) \quad (\because\; \lambda_1 = d) \\
&= \frac{|S|^2}{n}(d-\lambda_2) + \lambda_2|S|.
\end{aligned}$$

問 8.4. 上の不等式が成り立つ理由を説明しなさい．

よって，

$$\partial(S) \;\geq\; (d-\lambda_2)(1-|S|/n)|S| \;\geq\; \frac{d-\lambda_2}{2}|S|.$$

■

命題 8.4. $h(G) \leq \sqrt{2(1-(\lambda_2/d))}$.

注 8.2. この命題は次のことを意味する．G が (n,d,β)-辺エクスパンダーであれば，(n,d,λ)-エクスパンダーである．ただし，$\lambda = d(1-(\beta^2/2))$.

証明. ある $S \subseteq V$（$|S| \leq |V|/2$）が存在して，$\partial(S) \leq \sqrt{2d(d-\lambda_2)}|S|$ であることを示す[22]．G の隣接行列 A の第 2（正規）固有ベクトルを $\boldsymbol{v}$ として，$\boldsymbol{v}^+, \boldsymbol{v}^-$ を次のように定義する．任意の $x \in V$ について，

$$\boldsymbol{v}_x^+ \stackrel{\text{def}}{=} \begin{cases} \boldsymbol{v}_x & : \ \boldsymbol{v}_x > 0 \\ 0 & : \ \text{o.w.} \end{cases} \qquad \boldsymbol{v}_x^- \stackrel{\text{def}}{=} \begin{cases} -\boldsymbol{v}_x & : \ \boldsymbol{v}_x < 0 \\ 0 & : \ \text{o.w.} \end{cases}$$

このとき，$\boldsymbol{v} = \boldsymbol{v}^+ - \boldsymbol{v}^-$．また，$V^+ \stackrel{\text{def}}{=} \{x \in V : \boldsymbol{v}_x^+ > 0\}, V^- \stackrel{\text{def}}{=} \{x \in V : \boldsymbol{v}_x^- > 0\}$ とする．一般性を失うことなく，$|V^+| \leq |V^-|$ とする．以下，$\boldsymbol{v}^+, V^+$ に着眼する．次のような確率変数 $S \subseteq V$ を考える．任意の $x \in V$ について独立に，

$$\Pr\{x \in S\} \ = \ (\boldsymbol{v}_x^+)^2 \quad (\text{cf. } (\boldsymbol{v}_x^+)^2 \leq 1 \ \because \ \boldsymbol{v}_x \leq 1).$$

このとき，

$$\mathop{\mathrm{E}}_{S}[|S|] \ = \ \|\boldsymbol{v}^+\|_2^2. \tag{6}$$

問 8.5. この事実を示しなさい.

主張 8.1.

$$\mathop{\mathrm{E}}_{S}[|\partial(S)|] \ = \ \sum_{(x,y)\in E} \left|(\boldsymbol{v}_x^+)^2 - (\boldsymbol{v}_y^+)^2\right|.$$

問 8.6. この主張を証明しなさい.

この主張より，

$$\begin{aligned} \mathop{\mathrm{E}}_{S}[|\partial(S)|] \ &= \ \sum_{(x,y)\in E} \left|(\boldsymbol{v}_x^+)^2 - (\boldsymbol{v}_y^+)^2\right| \\ &= \ \sum_{(x,y)\in E} |\boldsymbol{v}_x^+ + \boldsymbol{v}_y^+| \cdot |\boldsymbol{v}_x^+ - \boldsymbol{v}_y^+| \\ &\leq \ \sqrt{\sum_{(x,y)\in E} (\boldsymbol{v}_x^+ + \boldsymbol{v}_y^+)^2} \sqrt{\sum_{(x,y)\in E} (\boldsymbol{v}_x^+ - \boldsymbol{v}_y^+)^2} \quad (\because \ \text{コーシー・シュワルツの不等式}) \\ &\leq \ \sqrt{2d}\sqrt{d-\lambda_2} \cdot \|\boldsymbol{v}^+\|_2^2 \quad (\because \ \text{主張 8.2，主張 8.3}). \end{aligned} \tag{7}$$

主張 8.2.

$$\sum_{(x,y)\in E} (\boldsymbol{v}_x^+ + \boldsymbol{v}_y^+)^2 \ \leq \ 2d\|\boldsymbol{v}^+\|_2^2.$$

[22] 以下では，S は確率変数となる.

証明. 以下より，この主張が示される．

$$\begin{aligned}\sum_{(x,y)\in E}(\boldsymbol{v}_x^+ + \boldsymbol{v}_y^+)^2 &\leq 2\sum_{(x,y)\in E}((\boldsymbol{v}_x^+)^2 + (\boldsymbol{v}_y^+)^2) \quad (\because\ 2ab \leq a^2+b^2)\\ &= 2d\sum_{x\in V}(\boldsymbol{v}_x^+)^2\\ &= 2d\|\boldsymbol{v}^+\|_2^2.\end{aligned}$$

■

主張 8.3.

$$\sum_{(x,y)\in E}(\boldsymbol{v}_x^+ - \boldsymbol{v}_y^+)^2 \;=\; (\boldsymbol{v}^+, (D-A)\boldsymbol{v}^+) \;\leq\; (d-\lambda_2)\|\boldsymbol{v}^+\|_2^2.$$

証明. まず，等式について．

問 8.7. 等式が成り立つ理由を説明しなさい．

次に，不等式について．任意の $x \in V^+$ について，

$$((D-A)\boldsymbol{v}^+)_x \;\leq\; ((D-A)\boldsymbol{v})_x \;=\; (d-\lambda_2)\boldsymbol{v}_x \;=\; (d-\lambda_2)\boldsymbol{v}_x^+.$$

問 8.8. この不等式が成り立つ理由を説明しなさい．

これより，

$$\begin{aligned}(\boldsymbol{v}^+, (D-A)\boldsymbol{v}^+) &= \sum_{x\in V^+}\boldsymbol{v}_x^+((D-A)\boldsymbol{v}^+)_x\\ &\leq \sum_{x\in V^+}\boldsymbol{v}_x^+(d-\lambda_2)\boldsymbol{v}_x^+\\ &= (d-\lambda_2)\|\boldsymbol{v}^+\|_2^2.\end{aligned}$$

■

よって，等式 (6)，不等式 (7) より，

$$\frac{\mathrm{E}[|\partial(S)|]}{\mathrm{E}[|S|]} \;\leq\; \sqrt{2d(d-\lambda_2)}.$$

期待値の線型性より，これは，以下と同値である．

$$\mathop{\mathrm{E}}_{S}\left[|\partial(S)| - \sqrt{2d(d-\lambda_2)}|S|\right] \;\leq\; 0.$$

問 8.9. この不等式が成り立つ理由を説明しなさい．

よって，ある $S \subseteq V$ が存在して，以下が満たされる．

$$\begin{aligned}&|\partial(S)| - \sqrt{2d(d-\lambda_2)}|S| \;\leq\; 0\\ \iff\quad &\frac{|\partial(S)|}{|S|} \;\leq\; \sqrt{2d(d-\lambda_2)}.\end{aligned}$$

■

8.1.2 頂点拡張度との関係

補題 8.5. 任意の $\boldsymbol{u} \in \mathbb{R}^n$ について，$|\mathrm{supp}(\boldsymbol{u})| \geq \|\boldsymbol{u}\|_1^2/\|\boldsymbol{u}\|_2^2$.

証明. $S \stackrel{\mathrm{def}}{=} \mathrm{supp}(\boldsymbol{u})$ とする．$\boldsymbol{w} \stackrel{\mathrm{def}}{=} (|\boldsymbol{u}_i|)_{i\in[n]}$，$\boldsymbol{w}' \stackrel{\mathrm{def}}{=} \mathbf{1}_S$ とする．このとき，

$$(\boldsymbol{w}, \boldsymbol{w}') \;=\; \sum_{i\in S} |\boldsymbol{u}_i| \;=\; \sum_{i\in[n]} |\boldsymbol{u}_i| \;=\; \|\boldsymbol{u}\|_1.$$

問 8.10. これらの等式が成り立つ理由を説明しなさい.

また，

$$\begin{aligned} \|\boldsymbol{w}\|_2^2 &= \|\boldsymbol{u}\|_2^2, \\ \|\boldsymbol{w}'\|_2^2 &= |S|. \end{aligned}$$

よって，コーシ・シュワルツの不等式より，$\|\boldsymbol{u}\|_2^2 \cdot |S| \geq \|\boldsymbol{u}\|_1^2$，つまり，$|S| \geq \|\boldsymbol{u}\|_1^2/\|\boldsymbol{u}\|_2^2$. ■

命題 8.6. G が (n,d,λ)-エクスパンダーであれば，(n,d,α)-頂点エクスパンダーである．ただし，$\alpha = 2/(1+(\lambda/d)^2)$．よって，$\epsilon = (1-(\lambda/d)^2)/(1+(\lambda/d)^2)$ とすれば，$\Gamma(S) \geq (1+\epsilon)|S|$.

注 8.3. 任意の $S \subseteq V$（$|S| \leq |V|/2$）について，$|\Gamma(S) \setminus S| \geq \epsilon|S|$.

証明. $S \subseteq V$ を任意に固定する．G の隣接行列を A とする．$\boldsymbol{u} \stackrel{\mathrm{def}}{=} A\mathbf{1}_S$ として，上の補題を適用する．まず，$\mathrm{supp}(\boldsymbol{u}) = \Gamma(S)$ となる.

問 8.11. この事実が成り立つ理由を説明しなさい.

以降，$\|\boldsymbol{u}\|_1^2$, $\|\boldsymbol{u}\|_2^2$ を求める．まず，$\|\boldsymbol{u}\|_1 = d|S|$ となる.（よって，$\|\boldsymbol{u}\|_1^2 = d^2|S|^2$.）

問 8.12. この事実が成り立つ理由を説明しなさい.

次に，$\|\boldsymbol{u}\|_2^2$ を求める．A の（正規）固有ベクトルを $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ とする.（$\boldsymbol{v}_1 = \mathbf{1}/\sqrt{n}$.）これらは直交基底であることから，$c_1, \ldots, c_n$ が存在して，

$$\mathbf{1}_S \;=\; c_1\boldsymbol{v}_1 + \cdots + c_n\boldsymbol{v}_n.$$

このとき，$\sum_{i\in[n]} c_i^2 = |S|$．また，$(\mathbf{1}_S, \boldsymbol{v}_1) = |S|/\sqrt{n}$ より，$c_1 = (\sum_{i\in[n]} c_i\boldsymbol{v}_i, \boldsymbol{v}_1) = |S|/\sqrt{n}$.

問 8.13. これらの事実が成り立つ理由を説明しなさい.

$\boldsymbol{u} = A\mathbf{1}_S = \sum_{i\in[n]} c_i\lambda_i\boldsymbol{v}_i$ であることから，

$$\|\boldsymbol{u}\|_2^2 \;=\; \sum_{i\in[n]} c_i^2\lambda_i^2$$

$$
\begin{aligned}
&\leq \frac{|S|^2}{n}d^2 + \lambda^2(|S| - |S|^2/n) \quad (\because\ \lambda_1 = d) \\
&= |S|\left(d^2(|S|/n) + \lambda^2(1 - |S|/n)\right).
\end{aligned}
$$

問 8.14. 上の不等式が成り立つ理由を説明しなさい.

以上より,

$$
\begin{aligned}
|\Gamma(S)| &\geq \frac{d^2|S|^2}{|S|(d^2(|S|/n) + \lambda^2(1 - |S|/n))} \\
&= \frac{1}{(\lambda/d)^2 + (1 - (\lambda/d)^2)|S|/n} \cdot |S| \\
&\geq \frac{1}{(\lambda/d)^2 + (1 - (\lambda/d)^2)/2} \cdot |S| \\
&= \frac{2}{1 + (\lambda/d)^2} \cdot |S|.
\end{aligned}
$$

問 8.15. $\Gamma(S) \geq (1+\epsilon)|S|$ が成り立つ理由を説明しなさい.

■

この命題より，エクスパンダーであれば，グラフの直径（距離の最長）の上界が得られる.

系 8.7. $G = (V, E)$ を (n, d, λ)-エクスパンダーとする．$\lambda/d = \Omega(1)$ なら，G の直径は $O(\log n)$ である.

証明. $u, v \in V$ を任意に固定する．$S_0 \stackrel{\text{def}}{=} \{u\}$ とする．$S_1 \stackrel{\text{def}}{=} \Gamma(S_0)$ とする．同様に，$S_i \stackrel{\text{def}}{=} \Gamma(S_{i-1})$ とする．このとき，$S_0 \subseteq S_1 \subseteq \cdots \subseteq S_i$.

問 8.16. この事実が成り立つ理由を説明しなさい.

上の命題より，$|S_i \setminus S_{i-1}| \geq \epsilon|S_{i-1}|$.

問 8.17. この事実が成り立つ理由を説明しなさい.

このとき，ある $\ell = O(\log n)$ が存在して，$|S_\ell| > n/2$.

問 8.18. この事実が成り立つ理由を説明しなさい.

$S'_0 \stackrel{\text{def}}{=} \{v\}$, $S'_i \stackrel{\text{def}}{=} \Gamma(S'_{i-1})$ についても同様のことがいえる．つまり，ある $\ell' = O(\log n)$ が存在して，$|S'_{\ell'}| > n/2$．よって，$S_\ell \cap S'_{\ell'} \neq \emptyset$．このことから，$u, v$ 間の距離が $O(\log n)$ であることがいえる.

問 8.19. この事実が成り立つ理由を説明しなさい.

■

8.2 成功確率の増幅

ここでは，エクスパンダーを利用した成功確率の増幅手法を示す[23]．G を (n,d)-グラフとする．$G=(V,E)$ 上のランダムウォーク，$X_0,X_1,\ldots,X_T\in V$（$T\geq 0$），を考える．つまり[24]，任意の $t\in[T]$，任意の $u\in V$，任意の $(u,v)\in E$ について，$\Pr\{X_t=v|X_{t-1}=u\}=1/d$，とする．ただし，任意の $v\in V$ について，$\Pr\{X_0=v\}=1/n$．

定理 8.1. G が (n,d,λ)-エクスパンダーであれば，任意の $S\subseteq V$ について，$|S|=\gamma n$（$0\leq\gamma<1$）ならば，任意の $T\in\mathbb{N}_0$ について，

$$\Pr\{\forall t\in[T]_0[X_t\in S]\}\ \leq\ (\gamma+\lambda/d)^T.$$

ここで[25]，この定理を用いた成功確率の増幅を示す．以下のような（言語 L のための[26]）乱択アルゴリズム A（$|r|=\ell$）を考える．

$$\begin{aligned} x\in L\ &:\ \Pr_{r\in\{0,1\}^\ell}\{A(x,r)=\texttt{YES}\}=1,\\ x\notin L\ &:\ \Pr_{r\in\{0,1\}^\ell}\{A(x,r)=\texttt{YES}\}\leq 1/4. \end{aligned}$$

事実 8.8. $A(x,r)$ を（独立に）T 回繰り返すことにより，$x\notin L$ の場合，A の誤り確率は $1/4^T$ に減少する．つまり，成功確率は $1-1/4^T$ に増幅される．ただし，その増幅に必要なランダムビット長は $\ell\cdot T$ となる．($x\in L$ の場合，成功確率は 1 のまま.)

以下，$x\notin L$ の場合を考える．$n=2^\ell$ である (n,d,λ)-エクスパンダー $G=(V,E)$，更に，G 上のランダムウォーク $X_0,X_1,\ldots,X_T\in V$ を考える．このとき，$V\stackrel{\text{def}}{=}\{0,1\}^\ell$，つまり，$V$ を長さ ℓ のランダムビットの集合とする．定理 8.1 について，$S\subseteq V$ を以下のように定義する．

$$S\ \stackrel{\text{def}}{=}\ \{r\in V:A(x,r)=\texttt{YES}\}.$$

このとき，$|S|\leq 2^\ell/4$.

問 8.20. この事実が成り立つ理由を説明しなさい．

以下のようなアルゴリズムを考える．

注 8.4. ステップ 1 の r_0, $d_1,\ldots,d_T$ の選択のみにランダムビットが必要となる．よって，合計のランダムビット長は，$\ell+O(T)$.

問 8.21. この事実が成り立つ理由を説明しなさい．

注 8.5. ステップ 2 について，(n,d,λ)-エクスパンダーの隣接行列が（ℓ の多項式時間で決定的に）得られることが示されている．つまり，そういったエクスパンダーの構築手法があり，更に，それによって求まるグラフの隣接行列が（多項式時間かつ多項式領域で）得られる．

[23] 第 4.7 節では，素数を利用した成功確率の増幅手法を示した．
[24] $T\geq 1$ の場合．
[25] 定理 8.1 の証明はその後に．
[26] 対象とする言語は素数性判定問題と同様にクラス coRP に属するもの．

入力：$x \notin L$

1. $r_0 \in \{0,1\}^\ell$，更に，$d_1, \ldots, d_T \in [d]$ を一様ランダムに選ぶ．
2. $r_1, \ldots, r_T$ を求める．（任意の $t \in [T]$ について，r_{t-1} の d_t 番目の隣接頂点は r_t．）
3. 任意の $t \in [T]_0$ に対して，$a_0 = A(x, r_0), a_1 = A(x, r_1) \ldots, a_T = A(x, r_T)$ を実行する．
4. $a_0, a_1, \ldots, a_T$ のうち一つでも `NO` があれば `NO` を出力，そうでなければ `YES` を出力する．

図 18: 成功確率の増幅

定理 8.2. 任意の $T \in \mathbb{N}$ に対して，図 18 のアルゴリズムの誤り確率は $(1/4 + \lambda/d)^T$ 以下である．

問 8.22. この定理を証明しなさい．（ヒント：定理 8.1 を用いる．）

以下，定理 8.1 の証明を示す．G を (n, d, λ)-エクスパンダーとする．$S \subseteq V$（$|S| = \gamma n$）を任意に固定する．$n \times n$ 行列 P を次のように定義する．任意の $i, j \in [n]$ について，

$$P_{ij} \stackrel{\text{def}}{=} \begin{cases} 1 & : \quad i = j, \text{ かつ } i, j \in S \\ 0 & : \quad \text{o.w.} \end{cases}$$

また，G の隣接行列を A とすれば，$M \stackrel{\text{def}}{=} (1/d)A$．このとき，行列 M の固有値は λ_i/d となる．更に，$\pi \stackrel{\text{def}}{=} (1/n, \ldots, 1/n)$．

補題 8.9. 任意の $T \in \mathbb{N}_0$ について，

$$\Pr_{X_i}\{\forall t \in [T]_0 [X_t \in S]\} \;=\; \|(PM)^T P\pi\|_1.$$

証明. $\boldsymbol{p}^{(T)} \stackrel{\text{def}}{=} (PM)^T P\pi$ とする．

主張 8.4. 任意の $x \in V$ について，

$$\boldsymbol{p}_x^{(T)} \;=\; \begin{cases} \Pr\{(X_T = x) \wedge (\forall t \in [T-1]_0 [X_t \in S])\} & : \quad x \in S, \\ 0 & : \quad x \notin S. \end{cases}$$

証明. T に関する帰納法により示す．$T = 0$ のとき，P の定義より，

$$\boldsymbol{p}_x^{(0)} \;=\; ((PM)^0 P\pi)_x \;=\; (P\pi)_x \;=\; \begin{cases} 1/n & : \quad x \in S, \\ 0 & : \quad x \notin S. \end{cases}$$

よって，X_0 の定義より，任意の $x \in V$ について，

$$\boldsymbol{p}_x^{(0)} \;=\; \begin{cases} \Pr\{X_0 = x\} & : \quad x \in S, \\ 0 & : \quad x \notin S. \end{cases}$$

$T-1$（$T \geq 1$）のとき，主張が成り立つとする．T のとき，$\boldsymbol{p}^{(T)}$ の定義より，

$$\boldsymbol{p}^{(T)} \;=\; (PM)^T P\pi \;=\; (PM)\left((PM)^{T-1}P\pi\right) \;=\; PM\boldsymbol{p}^{(T-1)}.$$

よって，帰納仮定より，任意の $x \in V$ について，

$$\begin{aligned}
\boldsymbol{p}_x^{(T)} &= [x \in S]\sum_{y\in V} M_{xy}\boldsymbol{p}_y^{(T-1)} \quad (\because\ \boldsymbol{p}_x^{(T)} = (PM\boldsymbol{p}^{(T-1)})_x) \\
&= [x \in S]\sum_{y\in S} M_{xy}\Pr\{(X_{T-1}=y)\wedge(\forall t\in[T-2]_0[X_t\in S])\} \\
&= [x \in S]\Pr\{(X_T=x)\wedge(\forall t\in[T-1]_0[X_t\in S])\}.
\end{aligned}$$

問 8.23. 三つ目の等式が成り立つ理由を説明しなさい．（ヒント：$M_{xy} = M_{yx} = \Pr\{X_T = x|X_{T-1} = y\} = \Pr\{X_T = x|X_{T-1} = y \wedge (*)\}$．）

■

この主張より，任意の $T \in \mathbb{N}_0$ について，

$$\begin{aligned}
\|(PM)^T P\pi\|_1 &= \sum_{x\in V}\boldsymbol{p}_x^{(T)} \quad (\because\ \boldsymbol{p}^{(T)}\ \text{の定義}) \\
&= \sum_{x\in S}\Pr_{X_i}\{(X_T=x)\wedge(\forall t\in[T-1]_0[X_t\in S])\} \\
&= \Pr_{X_i}\left\{\left(\bigvee_{x\in S}X_T=x\right)\wedge(\forall t\in[T-1]_0[X_t\in S])\right\} \\
&= \Pr_{X_i}\{\forall t\in[T]_0[X_t\in S]\}.
\end{aligned}$$

問 8.24. 三つ目の等式が成り立つ理由を説明しなさい．

■

補題 8.10. 任意の確率ベクトル $\boldsymbol{p} \in \mathbb{R}^n$（$\boldsymbol{p}_x \geq 0, \|\boldsymbol{p}\|_1 = 1$）について，

$$\|PMP\boldsymbol{p}\|_2 \;\leq\; (\gamma + \lambda/d)\|\boldsymbol{p}\|_2.$$

注 8.6. この不等式は，任意の $\boldsymbol{p} \in \mathbb{R}^n$ に対して（確率ベクトルでなくても）成り立つ．

証明. 一般性を失うことなく，$\boldsymbol{p} \in \mathbb{R}^n$ が $P\boldsymbol{p} = \boldsymbol{p}$ を満たすと仮定してよい．

問 8.25. この理由を説明しなさい．（ヒント：もしそうでなければ，そういうような $\boldsymbol{p}'$ に対して示せば，そうでない（$P\boldsymbol{p} = \boldsymbol{p}$ を満たす）$\boldsymbol{p}$ に対しても示される．なぜ？）

このとき，ある $\boldsymbol{q}$（$\sum_{x\in V}\boldsymbol{q}_x = 0$）が存在して，

$$P\boldsymbol{p} \;=\; \boldsymbol{p} \;=\; \pi + \boldsymbol{q}. \quad (\because\ (\pi, \boldsymbol{q}) = 0)$$

補題の不等式の左辺にこれを代入すると，$M\pi = \pi$ より，

$$PMP\boldsymbol{p} \;=\; PM\boldsymbol{p} \;=\; PM\pi + PM\boldsymbol{q} \;=\; P\pi + PM\boldsymbol{q}.$$

よって，三角不等式より，

$$\|PMP\boldsymbol{p}\|_2 \;\leq\; \|P\pi\|_2 + \|PM\boldsymbol{q}\|_2.$$

主張 8.5.

$$\begin{aligned} \|P\pi\|_2 &= \sqrt{\gamma/n}, \\ \|PM\boldsymbol{q}\|_2 &\leq (\lambda/d)\|\boldsymbol{p}\|_2. \end{aligned}$$

証明. 一つ目は，定義より明らか．二つ目は，以下の不等式より示される．$(\pi, \boldsymbol{q}) = 0$ より，$\boldsymbol{q} = \sum_{i>1} c_i \boldsymbol{v}_i$ とすれば，

$$\|PM\boldsymbol{q}\|_2 \;\leq\; \|M\boldsymbol{q}\|_2 \;=\; \left\|\sum_{i>1} c_i(\lambda_i/d)\boldsymbol{v}_i\right\|_2 \;\leq\; (\lambda/d)\left\|\sum_{i>1} c_i\boldsymbol{v}_i\right\|_2 \;=\; (\lambda/d)\|\boldsymbol{q}\|_2 \;\leq\; (\lambda/d)\|\boldsymbol{p}\|_2.$$

問 8.26. 不等式 $\|\boldsymbol{q}\|_2 \leq \|\boldsymbol{p}\|_2$ を証明しなさい．

■

この主張より，

$$\begin{aligned} \|PMP\boldsymbol{p}\|_2 &\leq \|P\pi\|_2 + \|PM\boldsymbol{q}\|_2 \\ &\leq \sqrt{\gamma/n} + (\lambda/d)\|\boldsymbol{p}\|_2 \\ &\leq \gamma\|\boldsymbol{p}\|_2 + (\lambda/d)\|\boldsymbol{p}\|_2 \quad (\because\; 1 \leq \sqrt{\gamma n}\|\boldsymbol{p}\|_2) \\ &= (\gamma + \lambda/d)\|\boldsymbol{p}\|_2. \end{aligned}$$

問 8.27. 不等式 $1 \leq \sqrt{\gamma n}\|\boldsymbol{p}\|_2$ を証明しなさい．（ヒント：$\boldsymbol{p}$ が確率ベクトルであるから $1 = \sum_x \boldsymbol{p}_x$ となり，右辺にコーシ・シュワルツの不等式を適用する．）

■

系 8.11. 任意の確率ベクトル $\boldsymbol{p} \in \mathbb{R}^n$（$\boldsymbol{p}_x \geq 0$, $\|\boldsymbol{p}\|_1 = 1$）について，

$$\|(PMP)^T\boldsymbol{p}\|_2 \;\leq\; (\gamma + \lambda/d)^T\|\boldsymbol{p}\|_2.$$

証明. T に関する帰納法により示す．$T = 0$ の時は明らか．$T-1$ のとき，系の不等式が成り立つとする．このとき，$\boldsymbol{p}' \stackrel{\text{def}}{=} (PMP)^{T-1}\boldsymbol{p}$ とすれば，

$$\|(PMP)^T\boldsymbol{p}\|_2 \;=\; \|(PMP)\boldsymbol{p}'\|_2 \;\leq\; (\gamma + \lambda/d)\|\boldsymbol{p}'\|_2 \;\leq\; (\gamma + \lambda/d)^T.$$

■

上記の補題と系より，

$$\begin{aligned}
\Pr\{\forall t \in [T]_0[X_t \in S]\} &= \|(PM)^T P\pi\|_1 \quad (\because \text{補題 8.9}) \\
&\leq \sqrt{n}\|(PM)^T P\pi\|_2 \quad (\because \text{ノルムの性質}) \\
&= \sqrt{n}\|(PMP)^T \pi\|_2 \quad (\because P \text{ の定義}) \\
&\leq \sqrt{n}(\gamma + \lambda/d)^T \|\pi\|_2 \quad (\because \text{系 8.11}) \\
&= (\gamma + \lambda/d)^T.
\end{aligned}$$

問 8.28. 事実 8.8 と定理 8.2 にてそれぞれ示された，ランダムビット長に対する誤り確率の比率を比較しなさい.（系 4.38 と同様に.）

付録

命題 8.12. 任意の $n \in \mathbb{N}$ について,

$$\sum_{i \in [n]} \frac{1}{i} \ \leq \ \ln n + 1.$$

証明. ■

命題 8.13. 任意の $x \in \mathbb{R}$ について $1 + x \leq \mathrm{e}^x$.

命題 8.14. 任意の自然数 n，任意の p（$0 \leq p \leq 1$）について,

$$\frac{2^{H(p)n}}{n} \ \leq \ \binom{n}{pn} \ \leq \ 2^{H(p)n}.$$

ただし，$H(p) = -p \log p - (p) \log(1-p)$.

証明. ■

命題 8.15 (イェンセンの不等式)**.** X を確率変数，$f : \mathbb{R} \to \mathbb{R}$ を下に凸な関数とする．このとき,

$$f(\mathrm{E}[X]) \ \leq \ \mathrm{E}[f(X)].$$

証明. ■

定理 8.3 (スターリングの公式)**.** 任意の $n \in \mathbb{N}$ について,

$$\sqrt{2\pi n} \left(\frac{n}{\mathrm{e}}\right)^n \ \leq \ n! \ = \ (1 + o_n(1)) \sqrt{2\pi n} \left(\frac{n}{\mathrm{e}}\right)^n.$$