近似アルゴリズム

山本真基

概 要

近似アルゴリズムの基礎を学習する．離散最適化問題の多くがＮＰ困難と呼ばれる問題であり，それらは，現実的な時間で最適解を求めることが不可能であると思われている問題である．そのような計算困難性に対処する一つの方法として，最適解に近い解,「近似解」を求めるアルゴリズムが考案されてきた．ここでは，以下の目次にあるような問題に対する近似アルゴリズムを学習する．最後に，近似不可能性について簡単にふれる．

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 $2^{\log x} = x$, $\mathrm{e}^{\ln x} = x$.)

- $G = (V, E)$ を，頂点集合 $V = \{v_1, v_2, \ldots, v_n\}$，辺集合 $E = \{e_1, e_2, \ldots, e_m\}$ のグラフとする．特に断らない限り，グラフといえば無向グラフを指すものとする．グラフ $G = (V, E)$ において，頂点 $v \in V$ に隣接する頂点の集合を N_v と表記する．(頂点集合 $U \subseteq V$ の隣接頂点の集合は $N(U)$ と表記する．) また，$|N_v|$ を頂点 $v \in V$ の次数といい，d_v と表記する．

1　近似アルゴリズムとは

1.1　対象とする問題

近似アルゴリズムが対象としている問題は，以下のような最適化問題である．（以下では，$V = \{v_1, v_2, \ldots, v_n\}$ とする．）

マッチング問題（matching）

- 入力：グラフ $G = (V, E)$
- 解：$M \subseteq E$ s.t. $\forall e, e' \in M : e \neq e'[e \cap e' = \emptyset]$
- 最大化：$|M|$

最短経路問題（shortest path）

- 入力：グラフ $G = (V, E)$, $c : E \to \mathbb{R}^+$，始点 s，終点 t
- 解：$u_1, u_2, \ldots, u_k \in V$ s.t.
  1. $(u_1, u_k) = (s, t)$,
  2. $\forall i, j \in [k] : i \neq j[u_i \neq u_j]$
  3. $\forall i \in [k-1][(u_i, u_{i+1}) \in E]$
- 最小化：$\sum_{i \in [k-1]} c(u_i, u_{i+1})$

事実 1.1. 上の二つは多項式時間で解くことができる問題である．

独立頂点集合問題（independent set）

- 入力：グラフ $G = (V, E)$
- 解：$D \subseteq V$ s.t. $\forall u, v \in D : u \neq v[(u, v) \notin E]$
- 最大化：$|D|$

巡回セールスマン問題（traveling salesman）

- 入力：完全グラフ $G = (V, E)$, $c : E \to \mathbb{R}^+$
- 解：$u_1, u_2, \ldots, u_n \in V$ s.t. $\forall i, j \in [n] : i \neq j[u_i \neq u_j]$
- 最小化：$\sum_{i \in [n]} c(u_i, u_{i+1})$

事実 1.2. 上の二つは NP 困難な問題である[1]．

[1] NP 困難な問題は多項式時間では解く（最適解を求める）ことができないと思われている．

近似アルゴリズムが対象とする問題は,(多項式時間では最適解が求まりそうにない）NP 困難な問題である．アルゴリズムの計算時間を制限しなければ（例えば指数時間かければ）これらの問題は近似しなくても解けるので，近似アルゴリズムといえば（入力の長さの）多項式時間で終了するものを指す.（よって，近似アルゴリズムで最適解は求まらない[2].）

注 1.1. 探索問題（線形探索アルゴリズム）や，整列問題（クイックソート，マージソート，ヒープソート），素因数分解問題などは最適化問題ではない.

問 1.1. NP 困難な最適化問題を（上の例以外に）3 つあげ，上記のように（数学記号を用いて）問題を定式化しなさい.（入力，解，最大化・最小化するものが何かを記述すること.）

1.2 近似率

定義 1.1

$\mathcal{P}$ を任意の（NP 困難な）最適化問題とする．I を $\mathcal{P}$ の任意の入力として，S を I の任意の解とする．このとき，解の「大きさ」を**解の値**といい，$\mathrm{val}(S)$ と表記する．特に，最適解の値を**最適値**という.

例 1.1. 独立頂点集合問題であれば，解 D の値は $|D|$ である．巡回セールスマン問題であれば，解 $u_1, \ldots, u_n$ の値は $\sum_{i\in[n]} c(u_i, u_{i+1})$ である.

問 1.2. 先の問いであげた NP 困難な最適化問題それぞれについて，解の値が何であるのかを示しなさい.

定義 1.2

$\mathcal{P}$ を任意の（NP 困難な）最適化問題とする．I を $\mathcal{P}$ の任意の入力とする．このとき，I の最適解を $\mathrm{OPT}(I)$ と表記する.

例 1.2. 独立頂点集合問題であれば，$\mathrm{OPT}(G)$ は，グラフ G の最大独立頂点集合である．巡回セールスマン問題であれば，$\mathrm{OPT}(G)$ は，グラフ G の最短巡回路である.

定義 1.3

$\mathcal{P}$ を任意の最大化問題とする．問題 $\mathcal{P}$ の入力の全体を $\mathcal{I}$ とする．このとき，**アルゴリズム A の近似率** $r(A) \geq 1$ は,

$$r(A) \stackrel{\mathrm{def}}{=} \max_{I\in\mathcal{I}} \left\{ \frac{\mathrm{val}(\mathrm{OPT}(I))}{\mathrm{val}(A(I))} \right\}.$$

つまり，任意の $I \in \mathcal{I}$ について $\mathrm{val}(\mathrm{OPT}(I)) \leq r(A) \cdot \mathrm{val}(A(I))$.

例 1.3 (最大化問題の近似率)**.** 独立頂点集合問題を解く近似率 r のアルゴリズムを A とする．G を任意のグラフ，$D^* = \mathrm{OPT}(G)$, $D = A(G)$ とする．このとき,

$$|D^*| \ \leq \ r \cdot |D|.$$

[2] P≠NP であれば.

定義 1.4

$\mathcal{P}$ を任意の最小化問題とする．問題 $\mathcal{P}$ の入力の全体を $\mathcal{I}$ とする．このとき，**アルゴリズム A の近似率** $r(A) \geq 1$ は，

$$r(A) \stackrel{\text{def}}{=} \max_{I \in \mathcal{I}} \left\{ \frac{\mathrm{val}(A(I))}{\mathrm{val}(\mathrm{OPT}(I))} \right\}.$$

つまり，任意の $I \in \mathcal{I}$ について $\mathrm{val}(A(I)) \leq r(A) \cdot \mathrm{val}(\mathrm{OPT}(I))$.

例 1.4 (最小化問題の近似率)**.** 巡回セールスマン問題を解く近似率 r のアルゴリズムを A とする．(G, c) を任意の入力，$(u_1, \ldots, u_n) = \mathrm{OPT}(G, c)$, $(w_1, \ldots, w_n) = A(G, c)$ とする．このとき，$s^* = \sum_{i \in [n]} c(u_i, u_{i+1})$, $s = \sum_{i \in [n]} c(w_i, w_{i+1})$ とすれば，

$$s \ \leq \ r \cdot s^*.$$

以降，近似アルゴリズムの「効率」といえば，アルゴリズムの近似率のことを指すものとする．よって，近似アルゴリズムの解析の中心は近似率の解析であり，計算時間の解析は行わない[3].

定義 1.5

$\mathcal{P}$ を任意の最適化問題とする．問題 $\mathcal{P}$ の**近似率が** r であるとは，ある（多項式時間）アルゴリズム A が存在して $r(A) \leq r$ であることである．

[3]先にも述べたように,（入力の長さの）多項式時間であればよい.

2　カット問題

カット問題（cut）

- 入力：グラフ $G = (V, E)$
- 解：$S \subseteq V$
- 最大化：$|\{(u, v) \in E : u \in S, v \notin S\}|$

例 2.1 (カット問題)**.**

定理 2.1. カット問題の近似率は 2 である．

入力：グラフ $G = (V, E)$

1. $S = \{1\}$ とする．(S が出力になる．)
2. それぞれの $i \in [n] \setminus \{1\}$ について（順次）以下を繰り返す．
   (a) $A, B \subseteq E$ を以下のように定義する．
   $$A \stackrel{\text{def}}{=} \{(u, v_i) \in E : u \in S\},$$
   $$B \stackrel{\text{def}}{=} \{(u, v_i) \in E : u \in \{v_j : j \in [i-1]\} \setminus S\}.$$
   (b) $|A| \leq |B|$ であるならば $S = S \cup \{v_i\}$ とする．
3. S を出力する．

図 1: 貪欲アルゴリズム

問 2.1. 7 頂点上の適当なグラフを考案して，そのグラフに対する図 1 のアルゴリズムの動作及び出力を示しなさい．

証明. 図 1 のアルゴリズムの出力を S，最適解を S^* とする．まず，グラフ $G = (V, E)$ の辺集合 E を以下のように分割する．任意の $i \in [n] \setminus \{1\}$ について，

$$E_i \stackrel{\text{def}}{=} \{(v_j, v_i) \in E : j < i\}.$$

このとき，$[E_2, \ldots, E_n]$ は E の分割である．つまり，

1. $E = \bigcup_{i \in [n] \setminus \{1\}} E_i$
2. $\forall i, j \in [n] \setminus \{1\} : i \neq j [E_i \cap E_j = \emptyset]$

よって，$|E| = \sum_{i \in [n] \setminus \{1\}} |E_i|$.

問 2.2. $[E_2, \ldots, E_n]$ が E の分割であることを証明しなさい.

一方，アルゴリズムのステップ 2-(a) において，任意の $i \in [n] \setminus \{1\}$ に対する A, B をそれぞれ A_i, B_i とする．このとき，$E_i = A_i \cup B_i$ かつ $A_i \cap B_i = \emptyset$ である.

問 2.3. 任意の $i \in [n] \setminus \{1\}$ について，$E_i = A_i \cup B_i$ かつ $A_i \cap B_i = \emptyset$ であることを証明しなさい.

アルゴリズムより，任意の $i \in S$ について $|A_i| \leq |B_i|$ である．このとき，

1. $\mathrm{val}(S) = \sum_{i \in [n] \setminus S} |A_i| + \sum_{i \in S \setminus \{1\}} |B_i|$,
2. $\forall i \in [n] \setminus S[|A_i| \geq |E_i|/2]$,
3. $\forall i \in S \setminus \{1\}[|B_i| \geq |E_i|/2]$.

問 2.4. 上の条件 1, 2, 3 が成り立つことを証明しなさい.

以上の三つの条件式より,

$$\begin{aligned}
\mathrm{val}(S) &= \sum_{i \in [n] \setminus S} |A_i| + \sum_{i \in S \setminus \{1\}} |B_i| \\
&\geq \sum_{i \in [n] \setminus \{1\}} \frac{|E_i|}{2} \\
&= \frac{\sum_{i \in [n] \setminus \{1\}} |E_i|}{2} \\
&= \frac{|E|}{2} \\
&\geq \frac{\mathrm{val}(S^*)}{2}.
\end{aligned}$$

よって，$\mathrm{val}(S^*)/\mathrm{val}(S) \leq 2$. ■

問 2.5. 図 1 のアルゴリズムの近似率が（およそ）2 となる入力（ただし，連結グラフとする）の例をあげなさい.（頂点番号を明記すること.）

3　集合被覆問題

集合被覆問題（set cover）

- 入力：集合 U，$S_1, S_2, \ldots, S_m \subseteq U$
- 解：$S_{i_1}, \ldots, S_{i_k}$ s.t. $S_{i_1} \cup \cdots \cup S_{i_k} = U$
- 最小化：k

例 3.1 (集合被覆問題)**.**

定理 3.1. $|U| = n$ のとき，集合被覆問題の近似率は $\ln n + 1$ である．

入力：U，$S_1, S_2, \ldots, S_m \subseteq U$

1. $W = U$, $A = \emptyset$ とする．($A \subseteq [m]$ が出力になる．)
2. $W \neq \emptyset$ である限り以下を繰り返す．
   (a) $j = \arg\max_{i \in [m] \setminus A} \{|S_i \cap W|\}$ とする．
   (b) $W = W \setminus S_j$, $A = A \cup \{j\}$ とする．
3. A を出力する．

図 2: 貪欲アルゴリズム

問 3.1. $U = \{1, \ldots, 7\}$ からなる適当な入力を考案して，その入力に対する図 2 のアルゴリズムの動作及び出力を示しなさい．

証明. 図 2 のアルゴリズムのステップ 2 が k 回繰り返されたとする．アルゴリズムのステップ 2 において，第 i 回目の繰り返し後の A を A_i とする．($A_0 = \emptyset$, $|A_i| = i$ であり，アルゴリズムの出力は A_k となる．) 最適解を A^* とする．第 i 回目の繰り返し後の W を W_i として，$w_i = |W_i|$ とする．($W_0 = U$, $w_0 = n$.)

主張 3.1. 任意の $i \in [k]$ について，$\{S_j \cap W_{i-1} : j \in A^*\}$ が W_{i-1} を被覆する．(つまり，$W_{i-1} = \bigcup_{j \in A^*}(S_j \cap W_{i-1})$.)

問 3.2. 上の主張を証明しなさい．

主張 3.2. 任意の $i \in [k]$ について，次のことが成り立つ．任意の $j \in A^*$ について，$S_j \cap W_{i-1} \neq \emptyset$ なら $j \in [m] \setminus A_{i-1}$.

問 3.3. 上の主張を証明しなさい.

これら二つの主張より，以下のことがいえる.

主張 3.3. 任意の $i \in [k]$ について，$|W_{i-1}| - |W_i| \geq |W_{i-1}|/|A^*|$.

問 3.4. 上の主張を証明しなさい.（ヒント：$\hat{A}^* = \{j \in A^* : S_j \cap W_{i-1} \neq \emptyset\}$ とすれば...）

この主張より，任意の $i \in [k]$ について，

$$w_i \ \leq \ \left(1 - \frac{1}{|A^*|}\right) w_{i-1}.$$

このことから，任意の $i \in [k]$ について，

$$w_i \ \leq \ \left(1 - \frac{1}{|A^*|}\right)^i w_0 \ \leq \ e^{-i/|A^*|} n. \quad (\because \text{ 下の問})$$

このとき，もし（i が）$e^{-i/|A^*|} n < 1$ を満たせば $w_i < 1$，つまり，$w_i = 0$（$W_i = \emptyset$，つまり，ステップ 2 の繰り返しが終了）となる.（w_i は整数なので.）この条件は，

$$e^{-i/|A^*|} n < 1 \iff \ln n < \frac{i}{|A^*|},$$

である. つまり,（i が）$(\ln n)|A^*| < i$ を満たせばアルゴリズムが終了する. これは，k が $(\ln n)|A^*| < k$ を満たす最小の整数であること，つまり，$k \leq (\ln n)|A^*| + 1$ であることを意味する. よって，$k = |A_k| = \mathrm{val}(A_k)$ より，$\mathrm{val}(A_k)/\mathrm{val}(A^*) \leq \ln n + 1$. ■

問 3.5. 任意の $x \in \mathbb{R}$ について $1 + x \leq e^x$ であることを示しなさい.

命題 3.1. このアルゴリズム（近似率 $\ln n + 1$ が保証された図 2 のアルゴリズム）に対して，近似率 $(\log n + 1)/2$ となる入力が存在する.

証明. 次のような集合 $S_0, S_1, S_2 \ldots, S_{m+1}, S_{m+2}$ を考える. $n = 2^m$ として，$U = \{u_1, \ldots, u_n\}$ とする. $S_0 = \{u_1\}$ として，任意の $i \in [m]$ について，

$$S_i \stackrel{\text{def}}{=} \{u_j : 2^{i-1} + 1 \leq j \leq 2^i\},$$

更に，$S_{m+1} = \{u_{2j-1} : j \in [n/2]\}$, $S_{m+2} = \{u_{2j} : j \in [n/2]\}$ とする.

主張 3.4. この入力の最適解は $\{S_{m+1}, S_{m+2}\}$ であり，アルゴリズムの出力は $\{S_0, S_1, \ldots, S_m\}$ となる[4].

[4] アルゴリズムのステップ 2-(a) において，$S_m, S_{m-1}, \ldots, S_1, S_{-1}$ が（S_{m+1}, S_{m+2} より）優先的に選択されたなら.

問 3.6. この主張を証明しなさい.

この主張より,

$$\frac{\mathrm{val}(A)}{\mathrm{val}(A^*)} \;=\; \frac{m+1}{2} \;=\; \frac{\log n + 1}{2}.$$

よって,（この入力 $S_0, S_1, \ldots, S_{m+2}$ に対する）アルゴリズムの近似率は $(\log n + 1)/2$ となる. ■

4　頂点被覆問題

頂点被覆問題（vertex cover）

- 入力：グラフ $G = (V, E)$
- 解：$S \subseteq V$ s.t. $\forall e \in E, \exists v \in S[e \cap v \neq \emptyset]$
- 最小化：$|S|$

例 4.1 (頂点被覆問題)**.**

定理 4.1. $|E| = m$ のとき，頂点被覆問題の近似率は $\ln m + 1$ である．

入力：グラフ $G = (V, E)$

1. $F = E$, $S = \emptyset$ とする．($S \subseteq V$ が出力になる．)
2. $F \neq \emptyset$ である限り以下を繰り返す．
   (a) $G' = (V, F)$ として，$u = \arg\max_{v \in V}\{d_{G'}(v)\}$ とする．
   (b) $S = S \cup \{u\}$ とする．
   (c) $F = F \setminus \{e \in F : \exists v \in N_u[e = (u, v)]\}$ とする．
3. S を出力する．

図 3: 貪欲アルゴリズム

問 4.1. 7 頂点上の適当なグラフを考案して，そのグラフに対する図 3 のアルゴリズムの動作及び出力を示しなさい．

証明. 図 3 のアルゴリズムのステップ 2 が k 回繰り返されたとする．アルゴリズムのステップ 2 において，第 i 回目の繰り返し後の S を S_i とする．($S_0 = \emptyset$, $|S_i| = i$ であり，アルゴリズムの出力は S_k となる．) 最適解を S^* とする．第 i 回目の繰り返し後の F を F_i として，$f_i = |F_i|$ とする．($F_0 = E$, $f_0 = m$.)

主張 4.1. 任意の $i \in [k]$ について，サイズが高々 $|S^*|$ の $S' \subseteq V \setminus S_{i-1}$ が存在して，S' が F_{i-1} を被覆する．

問 4.2. 上の主張を証明しなさい．

この主張より，以下のことがいえる．

主張 4.2. 任意の $i \in [k]$ について，$|F_{i-1}| - |F_i| \geq |F_{i-1}|/|S^*|$.

問 4.3. 上の主張を証明しなさい.

この主張より，任意の $i \in [k]$ について，

$$f_i \;\leq\; \left(1 - \frac{1}{|S^*|}\right) f_{i-1}$$

このことから，任意の $i \in [k]$ について，

$$f_i \;\leq\; \left(1 - \frac{1}{|S^*|}\right)^i f_0 \;\leq\; e^{-i/|S^*|} m.$$

このとき，もし（i が）$e^{-i/|S^*|}m < 1$ を満たせば $f_i < 1$，つまり，$f_i = 0$（$F_i = \emptyset$，つまり，ステップ 2 の繰り返しが終了）となる.（f_i は整数なので.）この条件は，

$$e^{-i/|S^*|}m < 1 \iff \ln m < \frac{i}{|S^*|},$$

である. つまり,（i が）$(\ln m)|S^*| < i$ を満たせばアルゴリズムが終了する. これは，k が $(\ln m)|S^*| < k$ を満たす最小の整数であること，つまり，$k \leq (\ln m)|S^*| + 1$ であることを意味する. よって，$k = |S_k| = \mathrm{val}(S_k)$ より，$\mathrm{val}(S_k)/\mathrm{val}(S^*) \leq \ln m + 1$. ■

命題 4.1. このアルゴリズム（近似率 $\ln m$ が保証された図 3 のアルゴリズム）に対して，近似率 $\ln n$ となる入力 $G = (V, E)$（$|V| \approx (\ln n + 1)n$, $|E| = m \approx n^2$）が存在する.

証明. 次のような二部グラフ $G = (X, Y, E)$（$|X| \approx n \ln n$, $|Y| = n$）を考える. 以下，E の定義を示す. $X_1, \ldots, X_n$ を X の分割とする. ただし，任意の $i \in [n]$ について $|X_i| = \lfloor n/i \rfloor$. よって，

$$|X| \;=\; \sum_{i \in [n]} |X_i| \;=\; \sum_{i \in [n]} \lfloor n/i \rfloor \;\approx\; n \ln n.$$

任意の $i \in [n]$ について，$Y_1^{(i)}, \ldots, Y_{\lfloor n/i \rfloor}^{(i)}$ を Y の分割とする. ただし，$|Y_1^{(i)}| = \cdots = |Y_{\lfloor n/i \rfloor}^{(i)}| = i$. 任意の $i \in [n]$ について，$X_i = \{a_1, \ldots, a_{\lfloor n/i \rfloor}\}$ としたとき，

$$E_i \;\stackrel{\mathrm{def}}{=}\; \bigcup_{j \in [\lfloor n/i \rfloor]} \{a_j\} \times Y_j^{(i)}.$$

$E \stackrel{\mathrm{def}}{=} \bigcup_{i \in [n]} E_i$ とする. よって，任意の $i \in [n]$ 任意の $a \in X_i$ について，$d_a = i$.（$|E| \approx n^2$.）

主張 4.3. この二部グラフの最適解は Y であり，アルゴリズムの出力は X となる[5].

問 4.4. この主張を証明しなさい.

この主張より，

$$\frac{\mathrm{val}(S)}{\mathrm{val}(S^*)} \;=\; \frac{|X|}{|Y|} \;\approx\; \frac{n \ln n}{n} \;=\; \ln n.$$

よって,（この入力 $G = (X, Y, E)$ に対する）アルゴリズムの近似率は $\ln n$ となる. ■

[5] アルゴリズムのステップ 2-(a) において，X の頂点が優先的に選択されたなら.

アルゴリズムの改良

定理 4.2. 頂点被覆問題の近似率は 2 である.

入力：グラフ $G = (V, E)$

1. $F = E$, $S = \emptyset$ とする.（$S \subseteq V$ が出力になる.）
2. $F \neq \emptyset$ である限り以下を繰り返す.
   (a) 任意に $f = (u, v) \in F$ を選ぶ.
   (b) $S = S \cup \{u, v\}$ とする.
   (c) $F = F \setminus (\{(u, w) \in F : w \in N_u\} \cup \{(v, w) \in F : w \in N_v\})$ とする.
3. S を出力する.

図 4: 単純なアルゴリズム

問 4.5. 7 頂点上の適当なグラフを考案して，そのグラフに対する図 4 のアルゴリズムの動作及び出力を示しなさい.

証明. 図 4 のアルゴリズムの出力を S，最適解を S^* とする．以下，近似率が 2 であることを示す．アルゴリズムのステップ 2 が k 回繰り返されたとして，第 i 回目の $\{u, v\}$ を $S_i = \{a_i, b_i\}$ とする．（$S = S_1 \cup S_2 \cup \cdots \cup S_k$.）

主張 4.4. 任意の $i, j \in [k] : i \neq j$ について $S_i \cap S_j = \emptyset$ である.

問 4.6. 上の主張を証明しなさい.

主張 4.5. 任意の $i \in [k]$ について，$a_i \in S^*$ かまたは $b_i \in S^*$ である.

問 4.7. 上の主張を証明しなさい.

これらの主張より，$|S| \leq 2|S^*|$．よって，$\mathrm{val}(S)/\mathrm{val}(S^*) \leq 2$.

問 4.8. 上の二つの主張から $|S| \leq 2|S^*|$ が示されることを説明しなさい.

■

問 4.9. 図 4 のアルゴリズムの近似率が（ちょうど）2 となる入力（ただし，連結グラフとする）をあげなさい.

5　独立頂点集合問題

独立頂点集合問題（independent set）

- 入力：グラフ $G = (V, E)$
- 解：$S \subseteq V$ s.t. $\forall u, v \in S : u \neq v[(u, v) \notin E]$
- 最大化：$|S|$

例 5.1 (独立頂点集合問題)**.**

定理 5.1. $|E|/|V| = c$ のとき，独立頂点集合問題の近似率は $2c + 1$ である．

入力：グラフ $G = (V, E)$

1. $U = V$, $S = \emptyset$ とする．($S \subseteq V$ が出力になる．)
2. $U \neq \emptyset$ である限り以下を繰り返す．
   (a) グラフ $G[U]$ で次数が最小の頂点 u を選ぶ．
   (b) $S = S \cup \{u\}$ とする．
   (c) $U = U \setminus (N_u \cup \{u\})$ とする．
3. S を出力する．

図 5: 貪欲アルゴリズム

問 5.1. 7 頂点上の適当なグラフを考案して，そのグラフに対する図 5 のアルゴリズムの動作及び出力を示しなさい．

証明. 図 5 のアルゴリズムの出力を S，最適解を S^* とする．アルゴリズムのステップ 2 が k 回繰り返されたとする．($k = |S| = \mathrm{val}(S)$.) アルゴリズムのステップ 2-(a) において，i 番目に選ばれた頂点を u_i，$G[U]$ における u_i の次数を d_i とする．このとき，

$$\sum_{i \in [k]} (d_i + 1) \;=\; n. \tag{1}$$

問 5.2. この等式を示しなさい．

また，i 番目のステップにおいて，削除される辺の個数は少なくとも $\binom{d_i+1}{2}$ あるので，

$$\sum_{i \in [k]} \left(\frac{d_i(d_i + 1)}{2} \right) \;\leq\; m \;=\; cn.$$

問 5.3. この不等式を示しなさい.

つまり,

$$\sum_{i\in[k]} d_i(d_i+1) \;\le\; 2cn. \tag{2}$$

等式 (1)，不等式 (2) より，それぞれ辺々たすと,

$$\sum_{i\in[k]} (d_i+1)^2 \;\le\; (2c+1)n.$$

コーシー・シュワルツの不等式より,

$$\sum_{i\in[k]} (d_i+1)^2 \;\ge\; \frac{\left(\sum_{i\in[k]}(d_i+1)\right)^2}{k} \;=\; \frac{n^2}{k}.$$

これら二つの不等式より,

$$\frac{n^2}{k} \;\le\; (2c+1)n.$$

つまり，$n/k \le 2c+1$．$\mathrm{val}(S) = k$，$n \ge \mathrm{val}(S^*)$ より，$\mathrm{val}(S^*)/\mathrm{val}(S) \le 2c+1$. ■

解析の改良

定理 5.2. $|E|/|V| = c$ のとき，独立頂点集合問題の近似率は $c+1$ である.

証明. 図 5 のアルゴリズムの出力を S，最適解を S^* とする．アルゴリズムのステップ 2 が k 回繰り返されたとする.（$k = |S| = \mathrm{val}(S)$.）アルゴリズムのステップ 2-(a) において，i 番目に選ばれた頂点を u_i，$G[U]$ における u_i の次数を d_i とする．このとき,

$$\sum_{i\in[k]} (d_i+1) \;=\; n.$$

S^* の頂点の中で，i 回目の繰り返しで U から削除された頂点の個数を k_i とする．つまり，$k_i = |S^* \cap (N_{u_i} \cup \{u_i\})|$．このとき,

$$\sum_{i\in[k]} k_i \;=\; |S^*|.$$

また，i 番目のステップにおいて，削除される辺の個数は少なくとも $\binom{d_i+1}{2} + \binom{k_i}{2}$ あるので,

$$\sum_{i\in[k]} \left(\frac{d_i(d_i+1)}{2} + \frac{k_i(k_i-1)}{2} \right) \;\le\; m \;=\; cn.$$

問 5.4. この不等式を示しなさい.

以上の 3 つの等式・不等式より，それぞれ辺々たすと，

$$\sum_{i\in[k]}(d_i+1)^2+\sum_{i\in[k]}k_i^2 \;\le\; 2cn+n+|S^*| \;=\; (2c+1)n+|S^*|.$$

コーシー・シュワルツの不等式より，

$$\sum_{i\in[k]}(d_i+1)^2 \;\ge\; \frac{\left(\sum_i(d_i+1)\right)^2}{k} \;=\; \frac{n^2}{k}$$

$$\sum_{i\in[k]}k_i^2 \;\ge\; \frac{\left(\sum_i k_i\right)^2}{k} \;=\; \frac{|S^*|^2}{k}$$

よって，$k=|S|$ より，

$$\frac{n^2+|S^*|^2}{|S|} \;\le\; (2c+1)n+|S^*|.$$

つまり，

$$\frac{1}{|S|} \;\le\; \frac{(2c+1)n+|S^*|}{n^2+|S^*|^2}.$$

これを式変形すると，

$$\frac{|S^*|}{|S|} \;\le\; \frac{(2c+1)+|S^*|/n}{n/|S^*|+|S^*|/n}. \tag{3}$$

この式の右辺の値が最大になるのは $n/|S^*|=1$ のときであるので，

$$\frac{|S^*|}{|S|} \;\le\; \frac{(2c+1)+1}{1+1} \;=\; c+1.$$

問 5.5. 不等式 (3) の右辺の値が最大になるのが $n/|S^*|=1$ のときであることを示しなさい.

以上より，$\mathrm{val}(S)=|S|$，$\mathrm{val}(S^*)=|S^*|$ から，$\mathrm{val}(S^*)/\mathrm{val}(S)\le c+1$. ■

6　巡回セールスマン問題

巡回セールスマン問題（traveling salesman）

- 入力：完全グラフ $G=(V,E)$, $c: E \to \mathbb{R}^+$
- 解：$u_1, u_2, \ldots, u_n \in V$ s.t. $\forall i, j \in [n] : i \neq j [u_i \neq u_j]$
- 最小化：$\sum_{i \in [n]} c(u_i, u_{i+1})$

例 6.1 (巡回セールスマン問題)**.**

命題 6.1. $|V| = n$ とする．$\mathcal{P} \neq \mathcal{NP}$ ならば，任意の（多項式時間計算可能な）関数 $\alpha : \mathbb{N} \to \mathbb{R}_{\geq 1}$ について，巡回セールスマン問題の近似率は $\alpha(n)$ より大きい．

証明. 対偶を示す．つまり，ある（多項式時間計算可能な）関数 $\alpha : \mathbb{N} \to \mathbb{R}_{\geq 1}$ について，巡回セールスマン問題の近似率が $\alpha(n)$ であったとする．(この仮定のもとで $\mathcal{P} = \mathcal{NP}$ を導く.）巡回セールスマン問題を解く近似率 $\alpha(n)$ の（多項式時間）アルゴリズムを A とする．以下，A を用いれば，ハミルトン閉路問題を多項式時間で解くことができることを示す.（よって，$\mathcal{P} = \mathcal{NP}$ が導かれる.）

$G = (V, E)$ を（ハミルトン閉路問題の）任意の入力とする．まず，関数 $c : V \times V \to \mathbb{R}^+$ を次のように定義する．任意の $e \in V \times V$ について，

$$c(e) \stackrel{\text{def}}{=} \begin{cases} 1 & : \ e \in E \\ n \cdot \alpha(n) & : \ e \notin E \end{cases}$$

次に，V 上の完全グラフと関数 c を入力として A を実行する．A の出力を S とする．このとき，$\mathrm{val}(S) \leq n \cdot \alpha(n)$ であれば `YES` を，そうでなければ `NO` を出力する． ■

問 6.1. 上の証明を完成させなさい.（つまり，証明中で示されたハミルトン閉路問題を解くアルゴリズムの正当性を示しなさい.）

定義 6.1

$G = (V, E)$, $c : E \to \mathbb{R}^+$ が三角不等式を満たすとは，

$$\forall a, b, c \in V [c(a, b) + c(b, c) \geq c(a, c)].$$

定理 6.1. $G = (V, E)$, $c : E \to \mathbb{R}^+$ が三角不等式を満たすとき，巡回セールスマン問題の近似率は $(\log n + 1)/2$ である．

問 6.2. 7 頂点上の適当なグラフを考案して，そのグラフに対する図 6 のアルゴリズムの動作及び出力を示しなさい．

入力：完全グラフ $G=(V,E)$（$V=\{v_1,\ldots,v_n\}$），$c:E\to\mathbb{R}^+$

1. $U=V\setminus\{v_1\}$, $S=(v_1)$, $v=v_1$ とする．（順列 S が出力になる．）
2. $U\neq\emptyset$ である限り以下を繰り返す．
   (a) $u'=\arg\min_{u\in U}\{c(v,u)\}$ とする．
   (b) $U=U\setminus\{u'\}$, $S=S\circ(u')$, $v=u'$ とする．
3. S を出力する．

図 6: 貪欲アルゴリズム

証明. 図 6 のアルゴリズムの出力を $S=(u_1,u_2,\ldots,u_n)$，最適解を S^* とする．関数 $f:V\to\mathbb{R}^+$ を以下のように定義する．

$$f(u_i)\ \stackrel{\text{def}}{=}\ c(u_i,u_{i+1}).$$

よって，

$$\mathrm{val}(S)\ =\ \sum_{i\in[n]} f(u_i).$$

主張 6.1. 任意の $i,j\in[n]$（ただし $i<j$）について $c(u_i,u_j)\geq f(u_i)$.

証明. アルゴリズムの定義より，（$i<j$ より）$f(u_i)=c(u_i,u_{i+1})\leq c(u_i,u_j)$. ■

この主張より，任意の $i,j\in[n]$ について[6]，

$$c(v_i,v_j)\ \geq\ \min\{f(v_i),f(v_j)\}. \tag{4}$$

問 6.3. この事実が成り立つ理由を説明しなさい．

一般性を失うことなく，$f(v_1)\geq f(v_2)\geq\cdots\geq f(v_n)$ とする．ここで，S^* の順で，$\{v_1,v_2,\ldots,v_k\}$ の頂点を巡回する閉路を S_k^* と表記する．（$S_n^*=S^*$.）

主張 6.2. 任意の $k\in[n]$（ただし $k\geq 3$）について，

$$\mathrm{val}(S_k^*)\ \geq\ 2\sum_{i=\lfloor k/2\rfloor+1}^{k} f(v_i).$$

証明. $S_k^*=(s_1,\ldots,s_k)$ とする．（$\{s_1,\ldots,s_k\}=\{v_1,\ldots,v_k\}$.）一般性を失うことなく，$k$ を偶数として，巡回路 S_k^* の辺を以下のように分割する．

$$\begin{aligned} E_1 &= \{(s_1,s_2),(s_3,s_4),\ldots(s_{k-1},s_k)\}\\ E_2 &= \{(s_2,s_3),(s_4,s_5),\ldots(s_k,s_1)\}\end{aligned}$$

$\sum_{e\in E_1}c(e)\leq\sum_{e\in E_2}c(e)$ とする．

[6]頂点が v_i,v_j になっていることに注意．（u_i,u_j でなく．）

問 6.4. この主張の証明を完成させなさい.（不等式 (4) を用いる.）

■

以下，$n = 2^k$（$k = \log n$）として示す.（そうでないときも同様にして示される.）この主張より，

$$\sum_{k=2}^{\log n} \mathrm{val}(S^*_{2^k}) \;\geq\; \sum_{k=2}^{\log n} \left(2 \sum_{i=2^k/2+1}^{2^k} f(v_i) \right) \;=\; 2 \sum_{i \in [n] \setminus \{1,2\}} f(v_i). \tag{5}$$

主張 6.3. 任意の $i \in [n]$ について $f(v_i) \leq \mathrm{val}(S^*)/2$.

証明. S において v_i の次が v_j であるとする.（よって，$f(v_i) = c(v_i, v_j)$.）$S^* = (v_i \to P_1 \to v_j \to P_2 \to v_i)$ とする．このとき，三角不等式より，$c(v_i, v_j) \leq c(P_1)$ かつ $c(v_i, v_j) \leq c(P_2)$．よって，$2c(v_i, v_j) \leq c(P_1) + c(P_2) = \mathrm{val}(S^*)$．$f(v_i) = c(v_i, v_j)$ より $f(v_i) \leq \mathrm{val}(S^*)/2$. ■

主張 6.4. 任意の $k \in [n]$（ただし $k \geq 3$）について，

$$\mathrm{val}(S^*_k) \;\leq\; \mathrm{val}(S^*).$$

証明. 三角不等式より示される. ■

問 6.5. この主張の証明を完成させなさい.

よって，これら二つの主張と不等式 (5) より，

$$\begin{aligned}
(\log n + 1)\mathrm{val}(S^*) &\geq 2\mathrm{val}(S^*) + \sum_{k=2}^{\log n} \mathrm{val}(S^*_{2^k}) \\
&\geq (2f(v_1) + 2f(v_2)) + 2 \sum_{i \in [n] \setminus \{1,2\}} f(v_i) \\
&= 2 \sum_{i \in [n]} f(v_i) \\
&= 2\mathrm{val}(S).
\end{aligned}$$

よって，$\mathrm{val}(S)/\mathrm{val}(S^*) \leq (\log n + 1)/2$. ■

アルゴリズムの改良その１

定理 6.2. $G = (V, E)$, $c : E \to \mathbb{R}$ が三角不等式を満たすとき，巡回セールスマン問題の近似率は 2 である.

定義 6.2

$G = (V, E)$, $c : E \to \mathbb{R}^+$ をグラフとする．G の部分グラフ $T = (V, E')$ が木であるとき，T を G の**全域木**といい，$\sum_{e \in E'} c(e)$ が最小である $T = (V, E')$ を**最小全域木**という.

事実 6.2. 任意のグラフについて，最小全域木は多項式時間で求めることができる．

定義 6.3

$G = (V, E)$ をグラフとする．G のすべての辺をちょうど一回辿る閉路を**オイラー閉路**という．

事実 6.3. 任意のグラフ G について，G の任意の頂点の次数が偶数であるときかつそのときに限り，G にオイラー閉路が存在する．また，その場合，オイラー閉路は多項式時間で求めることができる．

入力：完全グラフ $G = (V, E)$, $c : E \to \mathbb{R}^+$

1. G の最小全域木 $T = (V, E')$ を求める．
2. T の各辺を二重にする．(そのグラフを T' とする．)
3. T' のオイラー閉路 C を求める．
4. v_1 を始点として C が（初めて）辿った順に頂点を出力する．

図 7: 最小全域木を利用したアルゴリズム

問 6.6. 7 頂点上の適当なグラフを考案して，そのグラフに対する図 7 のアルゴリズムの動作及び出力を示しなさい．

問 6.7. 図 7 のアルゴリズムにおいて，T' にオイラー閉路があることを示しなさい．

証明. 図 7 のアルゴリズムの出力を $S = (u_1, u_2, \ldots, u_n)$，最適解を S^* とする．まず，

$$\sum_{e \in E'} c(e) \ \leq \ \mathrm{val}(S^*).$$

問 6.8. この不等式を証明しなさい．

また，三角不等式より，

$$\mathrm{val}(S) \ \leq \ \sum_{e \in C} c(e) \ = \ 2 \sum_{e \in E'} c(e).$$

問 6.9. この不等式を証明しなさい．

これら二つの不等式より，

$$\mathrm{val}(S) \ \leq \ 2\mathrm{val}(S^*).$$

よって，$\mathrm{val}(S)/\mathrm{val}(S^*) \leq 2$. ■

アルゴリズムの改良その２

定理 6.3. $G=(V,E)$, $c:E\to\mathbb{R}$ が三角不等式を満たすとき，巡回セールスマン問題の近似率は 1.5 である．

定義 6.4

$G=(V,E)$, $c:E\to\mathbb{R}$ をグラフとする．$M\subset E$ が $\forall e,e'\in M[e\cap e'=\emptyset]$ であるとき，M を**マッチング**という．マッチング M が $\forall v\in V,\exists e\in M[v\in e]$ であるとき，M を**完全マッチング**という．$\sum_{e\in M}c(e)$ が最小である完全マッチング M を**最小完全マッチング**という．

事実 6.4. 頂点の個数が偶数である完全グラフの最小完全マッチングは多項式時間で求めることができる．

入力：完全グラフ $G=(V,E)$, $c:E\to\mathbb{R}^+$

1. G の最小全域木 $T=(V,E')$ を求める．
2. T の次数が奇数の頂点を V' とする．
3. $G[V']$ の最小完全マッチング M を求める．
4. $T'=(V,E'\cup M)$ のオイラー閉路 C を求める．
5. v_1 を始点として C が（初めて）辿った順に頂点を出力する．

図 8: 完全マッチングを利用したアルゴリズム

問 6.10. ７頂点上の適当なグラフを考案して，そのグラフに対する図 8 のアルゴリズムの動作及び出力を示しなさい．

問 6.11. 図 8 のアルゴリズムにおいて，$G[V']$ に完全マッチングがあることを示しなさい．

問 6.12. 図 8 のアルゴリズムにおいて，T' にオイラー閉路があることを示しなさい．

証明. 図 8 のアルゴリズムの出力を $S=(u_1,u_2,\ldots,u_n)$，最適解を S^* とする．先の定理の証明と同様に，

$$\begin{aligned}1.\quad \sum_{e\in E'}c(e) &\le \mathrm{val}(S^*),\\ 2.\quad \mathrm{val}(S) &\le \sum_{e\in C}c(e).\end{aligned}$$

主張 6.5.

$$\sum_{e\in M} c(e) \ \leq \ \frac{\mathrm{val}(S^*)}{2}.$$

証明. $S^* = (s_1, \ldots, s_n)$ とする．このうち，M の頂点を $s_{i_1}, \ldots, s_{i_{2k}}$ （$i_1 \leq i_2 \leq \cdots \leq i_{2k}$）とする．ここで，

$$\begin{array}{rcll} S_1 & \stackrel{\mathrm{def}}{=} & \{(s_{i_1}, s_{i_2}), (s_{i_3}, s_{i_4}), \ldots, (s_{i_{2k-1}}, s_{i_{2k}})\} & \subseteq \ E, \\ S_2 & \stackrel{\mathrm{def}}{=} & \{(s_{i_2}, s_{i_3}), (s_{i_4}, s_{i_5}), \ldots, (s_{i_{2k}}, s_{i_1})\} & \subseteq \ E. \end{array}$$

三角不等式（と $S_1 \cap S_2 = \emptyset$）より，

$$\sum_{e\in S_1\cup S_2} c(e) \ \leq \ \mathrm{val}(S^*).$$

問 6.13. この不等式を証明しなさい．

また，M が最小マッチングであることから，($S_1 \cap S_2 = \emptyset$ より)

$$\sum_{e\in M} c(e) \ \leq \ \min\left\{\sum_{e\in S_1} c(e), \sum_{e\in S_2} c(e)\right\} \ \leq \ \frac{1}{2}\sum_{e\in S_1\cup S_2} c(e).$$

問 6.14. この不等式を証明しなさい．

これら二つの不等式より，

$$\sum_{e\in M} c(e) \ \leq \ \frac{\mathrm{val}(S^*)}{2}.$$

■

この主張より，

$$\begin{aligned} \mathrm{val}(S) \ &\leq \ \sum_{e\in C} c(e) \ = \ \sum_{e\in E'\cup M} c(e) \\ &= \ \sum_{e\in E'} c(e) + \sum_{e\in M} c(e) \ \leq \ \mathrm{val}(S^*) + \frac{\mathrm{val}(S^*)}{2} \ = \ \frac{3}{2}\mathrm{val}(S^*). \end{aligned}$$

■

7　ナップサック問題

ナップサック問題（knapsack）

- 入力：集合 $U = \{u_1, u_2, \ldots, u_n\}$，$(a_1, p_1), (a_2, p_2), \ldots, (a_n, p_n) \in \mathbb{N} \times \mathbb{N}$, $b \in \mathbb{N}$
- 解：$S \subseteq [n]$ s.t. $\sum_{i \in S} a_i \leq b$
- 最大化：$\sum_{i \in S} p_i$

注 7.1. 入力 $U = \{u_1, u_2, \ldots, u_n\}$，$(a_1, p_1), (a_2, p_2), \ldots, (a_n, p_n) \in \mathbb{N} \times \mathbb{N}$, $b \in \mathbb{N}$ において，$\forall i \in [n][a_i \leq b]$ が成り立つと仮定してよい．（$a_i > b$ である u_i は U から除外して考えてよいので．）

例 7.1 (ナップサック問題)**.**

定理 7.1. $U = \{u_1, \ldots, u_n\}$, $(a_1, p_1), \ldots, (a_n, p_n) \in \mathbb{N} \times \mathbb{N}$, $b \in \mathbb{N}$ を入力とする．ナップサック問題は $O(nb)$ 時間で（厳密に）解くことができる．

注 7.2. 計算時間 $O(nb)$ のようなアルゴリズムは擬多項式時間アルゴリズムと呼ばれる．（計算時間 nb は必ずしも（入力長の！）多項式とはならない．）

証明. 次のような関数 $S : [n] \times [b] \to 2^{[n]}$ を考える．任意の $i \in [n]$, $w \in [b]$ について，

$$S(i, w) \stackrel{\text{def}}{=} \arg\max_{S \subseteq [i]} \left\{ \sum_{j \in S} p_j \ : \ \sum_{j \in S} a_j \leq w \right\}.$$

このとき，任意の $i \in [n] \setminus \{1\}$, $w \in [b]$ について，以下の漸化式が成り立つ．

$$S(i, w) = \begin{cases} \arg \max_{S \in \{S(i-1,w), S(i-1,w-a_i) \cup \{i\}\}} \left\{ \sum_{j \in S} p_j \right\} & : \ w \geq a_i \\ S(i-1, w) & : \ w < a_i \end{cases} \tag{6}$$

ただし，$\sum_{j \in \emptyset} p_j = 0$ とする．漸化式の初期値について，任意の $i \in [n]$ について $S(i, 0) = \emptyset$，また，任意の $w \in [b]$ について，$w < a_1$ なら $S(1, w) = \emptyset$，$w \geq a_1$ なら $S(1, w) = \{1\}$ とする．

問 7.1. この漸化式が成り立つことを示しなさい．

最適解は，$S(i, w)$ の定義より $S(n, b)$ である．よって，$S(i, w)$（$i \in [n]$, $w \in [b]$）を求めればナップサック問題が解ける．$S(n, b)$ を求めることにかかる計算時間は $O(nb)$ である．　■

注 7.3. ナップサック問題は，入力について $(a_i, p_i) \in \mathbb{N} \times \mathbb{N}$ であるが，p_i に整数性がなくてもこの定理は成り立つ．（a_i には整数性が必要である．）

問 7.2. ナップサック問題を解く $O(nb)$ 時間アルゴリズムを示しなさい．（漸化式 (6) をもとに $S(i, w)$ を求める擬似コードを示す．）

系 7.1. $b = \mathbf{poly}(n)$ のとき，ナップサック問題は（n の）多項式時間で解くことができる．

定理 7.2. ナップサック問題の近似率は 2 である．

入力：集合 $U = \{u_1, u_2, \ldots, u_n\}$，$(a_1, p_1), (a_2, p_2), \ldots, (a_n, p_n) \in \mathbb{N} \times \mathbb{N}$, $b \in \mathbb{N}$

1. $S = \emptyset$，$x = \arg\max_{i \in [n]} \{p_i\}$ とする．($S \subseteq [n]$ が出力になる．)
2. p_i/a_i について U を降順に並べ替える．(その結果，$p_1/a_1 \geq \cdots \geq p_n/a_n$ であったとする．)
3. それぞれの $i \in [n]$ について（順次）以下を繰り返す．
   (a) $(\sum_{j \in S} a_j) + a_i \leq b$ であれば $S = S \cup \{i\}$ とする．
4. $\sum_{j \in S} p_j < p_x$ であれば $\{x\}$ を，そうでなければ S を出力する．

図 9: 貪欲アルゴリズム

問 7.3. 7 個からなる適当な入力を考案して，その入力に対する図 9 のアルゴリズムの動作及び出力を示しなさい．

証明. 図 9 のアルゴリズムの出力を S，最適解を S^* とする．アルゴリズムのステップ 3-(c) において，S に含められなかった最初のものを $i_0 \in [n]$ とする．つまり，$i_0 \in [n]$ は以下を満たす．

$$\sum_{j \in [i_0 - 1]} a_j \leq b \text{ かつ } \sum_{j \in [i_0]} a_j > b$$

このとき，$[i_0 - 1] \subseteq S$ より，

$$\sum_{j \in [i_0 - 1]} p_j \ \leq \ \mathrm{val}(S).$$

ここで，$b_0 = \sum_{j \in [i_0 - 1]} a_j$ とする．

主張 7.1.

$$\sum_{j \in [i_0 - 1]} p_j + \frac{p_{i_0}}{a_{i_0}}(b - b_0) \ \geq \ \mathrm{val}(S^*).$$

問 7.4. この主張が成り立つ理由を説明しなさい．

主張 7.2.

$$\mathrm{val}(S^*) \ < \ \sum_{j \in [i_0]} p_j.$$

証明. 上の主張より示される． ■

問 7.5. この主張の証明を完成させなさい.

$\sum_{j\in[i_0-1]} p_j \geq p_{i_0}$ のとき，上の主張より，

$$\mathrm{val}(S^*) \;<\; \sum_{j\in[i_0-1]} p_j + p_{i_0} \;\leq\; 2\sum_{j\in[i_0-1]} p_j \;\leq\; 2\mathrm{val}(S). \quad \left(\because \sum_{j\in[i_0-1]} p_j \leq \mathrm{val}(S)\right)$$

$\sum_{j\in[i_0-1]} p_j < p_{i_0}$ のとき，上の主張より，

$$\mathrm{val}(S^*) \;<\; \sum_{j\in[i_0-1]} p_j + p_{i_0} \;<\; 2p_{i_0} \;\leq\; 2p_x \;\leq\; 2\mathrm{val}(S). \quad (\because\ p_x \leq \mathrm{val}(S))$$

よって，$\mathrm{val}(S^*)/\mathrm{val}(S) \leq 2$. ■

問 7.6. 図 9 のアルゴリズムにおいて，$\sum_{j\in S} p_j < p_x$ となるような入力をあげなさい.

8　近似スキーム

定義 8.1

$\mathcal{P}$ を任意の（NP 困難な）最適化問題とする．問題 $\mathcal{P}$ の入力の全体を $\mathcal{I}$ とする．近似アルゴリズム A が**多項式時間近似スキーム（polynomial time approximation scheme: PTAS）**であるとは，任意の $\epsilon > 0$ について，

$$\text{最大化問題} \quad : \quad \max_{I \in \mathcal{I}} \left\{ \frac{\mathrm{val}(\mathrm{OPT}(I))}{\mathrm{val}(A(I,\epsilon))} \right\} \quad \leq \quad (1+\epsilon)$$

$$\text{最小化問題} \quad : \quad \max_{I \in \mathcal{I}} \left\{ \frac{\mathrm{val}(A(I,\epsilon))}{\mathrm{val}(\mathrm{OPT}(I))} \right\} \quad \leq \quad (1+\epsilon)$$

を満たすことである．（ただし，A は $|I|$ の多項式時間で終了する．）

定義 8.2

近似アルゴリズム A が**完全多項式時間近似スキーム（fully polynomial time approximation scheme: FPTAS）**であるとは，A が PTAS であり，かつ，A が $|I|, 1/\epsilon$ の多項式時間で終了することである．

8.1　PTAS（ナップサック問題）

定理 8.1. ナップサック問題は PTAS をもつ．

入力：集合 $U = \{u_1, u_2, \ldots, u_n\}$，$(a_1, p_1), (a_2, p_2), \ldots, (a_n, p_n) \in \mathbb{N} \times \mathbb{N}$, $b \in \mathbb{N}$, $\epsilon > 0$

1. $k = 1/\epsilon$ とする．
2. それぞれの $S \subseteq [n] : |S| \leq k$ について，以下を繰り返す．
   (a) $T = [n] \setminus S$ とする．（$|T| = n'$ とする．）
   (b) p_i/a_i について T を降順に並べ替える．（その結果，$p_1/a_1 \geq \cdots \geq p_{n'}/a_{n'}$ であったとする．）
   (c) それぞれの $i \in [n']$ について（順次）以下を繰り返す．
   - $(\sum_{j \in S} a_j) + a_i \leq b$ であれば $S = S \cup \{i\}$ とする．
3. 最大の $\sum_{i \in S} p_i$ の値をもつ S を出力する．

図 10:　ＰＴＡＳアルゴリズム

問 8.1. ５個からなる適当な入力を考案して，$\epsilon = 0.5$ として，その入力に対する図 10 のアルゴリズムの動作及び出力を示しなさい．

証明. 図 10 のアルゴリズムの出力を S，最適解を S^* とする．$\mathrm{val}(S^*) \leq (1+\epsilon)\mathrm{val}(S)$ を示せば十分である．($\epsilon = 1/k$ である．) 以降，$\{u_1, \ldots, u_n\}$ を $\{1, \ldots, n\}$ と表記する．一般性を失うことなく[7]，ある自然数 $k^* \in [n]$ に対して $S^* = [k^*]$ とする．($\mathrm{val}(S^*) = \sum_{i \in [k^*]} p_i$.) このとき，$k^* > k$ が満たされていると仮定してよい．

問 8.2. $k^* > k$ と仮定してよい理由を述べなさい．

S^* の中で p_i の最も大きい k 個を $[k]$ とする．更に，$[k^*] \setminus [k]$ が p_i/a_i の大きい順に並んでいるものとする．(つまり，任意の $i, j \in [k^*] \setminus [k] : i < j$ について，$p_i/a_i \geq p_j/a_j$.) 図 11 を参照[8]．

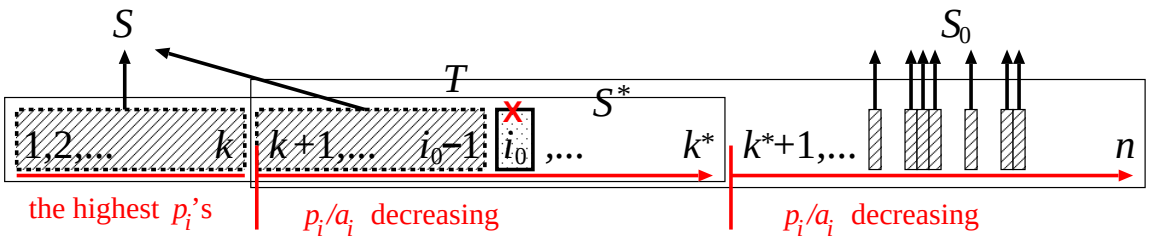

図 11: $S^* = [k^*]$, $S \supseteq [i_0 - 1]$, $i_0 \notin S$

$S \supseteq [k]$ である場合を考える．(ステップ 2 が，それぞれの $S \subseteq [n] : |S| \leq k$ となっているので，いずれ，アルゴリズムの S が $[k]$ になって貪欲アルゴリズムが開始されるから.) このとき，ステップ 2-(b), 2-(c) は，$[n] \setminus [k]$ ($T = [n] \setminus [k]$) に対する貪欲アルゴリズムとなっている．$[k^*] \setminus [k]$ の中で，ステップ 2-(c) において S に含められなかった最初のものを $i_0 \in [k^*] \setminus [k]$ とする．

問 8.3. そのような i_0 が $[k^*] \setminus [k]$ に存在する理由を述べなさい．

$[n] \setminus [k^*]$ の中で「i_0 選択以前に」S に含められたものを S_0 とする．($S_0 \cap [i_0 - 1] = \emptyset$, $S_0 \cup [i_0 - 1] \subseteq S$.) 更に，$b_0 = \sum_{j \in [i_0 - 1]} a_j + \sum_{j \in S_0} a_j$ とする．ナップサック問題を解く貪欲アルゴリズムの近似率の解析と同様に[9]，

$$\begin{aligned} \mathrm{val}(S^*) &\leq \sum_{j \in [i_0 - 1]} p_j + \sum_{j \in S_0} p_j + \frac{p_{i_0}}{a_{i_0}}(b - b_0) \\ &\leq \mathrm{val}(S) + p_{i_0}. \end{aligned}$$

問 8.4. これら二つの不等式を示しなさい．(一つ目のヒント：$[n] \setminus [k^*]$ で i_0 選択以前に S に入らなかったものは考慮しなくてよい.)

仮定より，任意の $i \in [k]$ について $p_{i_0} \leq p_i$ であることから，$k \cdot p_{i_0} \leq \mathrm{val}(S)$.

問 8.5. この不等式を示しなさい．

[7] 証明の「表記」の都合上.
[8] $[n] \setminus [k^*]$ も p_i/a_i の大きい順に並んでいるものとする.
[9] 主張 7.1 参照.

以上より，

$$\begin{aligned}\mathrm{val}(S^*) &\leq \mathrm{val}(S) + p_{i_0}\\ &\leq \mathrm{val}(S) + \mathrm{val}(S)/k\\ &= (1+1/k)\mathrm{val}(S)\\ &= (1+\epsilon)\mathrm{val}(S).\end{aligned}$$

アルゴリズムの計算時間について，ステップ 2 の繰り返し回数は $\sum_{i\in[k]}\binom{n}{i} = O(n^k)$．ステップ 2 の一回の繰り返しにかかる計算時間は $O(n)$.（ステップ 2 の直前で，U 全体を p_i/a_i について昇順に並べておけば，ステップ 2-(b) で T を昇順に並べる手順が必要なくなるので.）これより，アルゴリズム全体にかかる計算時間は（$n^k \geq \log n$ より），

$$O(n^k \cdot n + n\log n) \;=\; O(n^{1+k}) \;=\; O(n^{1+1/\epsilon}).$$

■

8.2 FPTAS（ナップサック問題）

補題 8.1. $U = \{u_1,\ldots,u_n\}$, $(a_1,p_1),\ldots,(a_n,p_n) \in \mathbb{N}\times\mathbb{N}$, $b \in \mathbb{N}$ を入力とする．$P = \max\{p_1,\ldots,p_n\}$ のとき，ナップサック問題は $O(n^2P)$ 時間で（厳密に）解くことができる．

証明. 次のような関数 $S : [n]\times[nP] \to 2^{[n]}$ を考える．任意の $i\in[n]$, $p\in[nP]$ について，

$$S(i,p) \stackrel{\mathrm{def}}{=} \arg\min_{S\subseteq[i]}\left\{\sum_{j\in S} a_j \;:\; \sum_{j\in S} p_j \geq p\right\}.$$

このとき，任意の $i\in[n]\setminus\{1\}$, $p\in[nP]$ について，以下の漸化式が成り立つ．

$$S(i,p) \;=\; \begin{cases} \arg \min_{S\in\{S(i-1,p),S(i-1,p-p_i)\cup\{i\}\}} \left\{\sum_{j\in S} a_j\right\} & : \; p \leq \sum_{j\in[i]} p_j \\ \emptyset & : \; p > \sum_{j\in[i]} p_j \end{cases} \tag{7}$$

ただし，$\sum_{j\in\emptyset} a_j = \infty$ とする．漸化式の初期値について，任意の $i\in[n]$ について，$p\leq 0$ なら $S(i,p)=\emptyset$ とする．また，任意の $p\in[nP]$ について，$p\leq p_1$ なら $S(1,p)=\{1\}$，$p>p_1$ なら $S(1,p)=\emptyset$ とする．

問 8.6. 漸化式 (7) が成り立つことを示しなさい．

このとき，最適解は以下となる[10]．

$$\arg\max_{S(n,p):p\in[nP]}\left\{p \;:\; \sum_{j\in S(n,p)} a_j \leq b\right\}. \tag{8}$$

[10] $\sum_{j\in\emptyset} a_j = \infty$ であることに注意．

問 8.7. 最適解が (8) で表されることを示しなさい.

よって，$S(i,p)$ ($i \in [n], p \in [nP]$) を求めればナップサック問題が解ける．関数 S の定義域 $[n]\times[nP]$ の大きさは n^2P であることから，アルゴリズムの計算時間は $O(n^2P)$ である． ■

注 8.1. ナップサック問題は，入力について $(w_i, p_i) \in \mathbb{N}\times\mathbb{N}$ であるが，w_i に整数性がなくてもこの補題は成り立つ.（一方，p_i には整数性が必要である.）

注 8.2. この補題の証明より，図 12 のアルゴリズム[11]によって最適解が求められる.

入力：集合 $U = \{u_1, \ldots, u_n\}$, $(a_1, p_1), \ldots, (a_n, p_n) \in \mathbb{N}\times\mathbb{N}$, $b \in \mathbb{N}$

1. 任意の $p \in [p_1]$ について $S(1,p) = \{1\}$，任意の $p \in [nP] \setminus [p_1]$ について $S(1,p) = \emptyset$ とする.
2. それぞれの $i \in [n] \setminus \{1\}$ について以下を実行する.
   (a) $Q = \sum_{j\in[i]} p_j$ とする.
   (b) それぞれの $p \in [Q]$ について以下を実行する.
   - $X = S(i-1,p)$, $Y = S(i-1,p-p_i)\cup\{i\}$ とする．このとき，$p - p_i \le 0$ なら $Y = \{i\}$ とする.
   - $X \neq \emptyset$ であるとき，$\sum_{j\in X} a_j \le \sum_{j\in Y} a_j$ なら $S(i,p) = X$，そうでないなら $S(i,p) = Y$ とする．$X = \emptyset$ なら $S(i,p) = Y$ とする.

   (c) それぞれの $p \in [nP] \setminus [Q]$ について $S(i,p) = \emptyset$ とする.
3. 式 (8) を求める.

図 12: ナップサック問題を解く動的計画法

問 8.8. 図 12 のアルゴリズムを，以下のように再帰関数 $\mathtt{RS}(i,p)$ を用いて記述した.

- それぞれの $p \in \{nP, nP-1, nP-2, \ldots, 2, 1\}$ について（降順に）以下を実行する.
  1. $S = \mathtt{RS}(n,p)$ とする.（再帰関数 $\mathtt{RS}(n,p)$ を実行する.）
  2. $S \neq \emptyset$ かつ $\sum_{i\in S} a_i \le b$ であれば S を出力して終了する.

このとき，$\mathtt{RS}(i,p)$ の擬似コードを記述しなさい.

定理 8.2. ナップサック問題は FPTAS をもつ.

[11] これは問 7.2 の解答（擬似コード）のヒントにもなっていた！

入力：集合 $U = \{u_1, \ldots, u_n\}$, $(a_1, p_1), \ldots, (a_n, p_n) \in \mathbb{N} \times \mathbb{N}$, $b \in \mathbb{N}$, $\epsilon > 0$

1. $P = \max\{p_1, \ldots, p_n\}$ として $K = P \cdot (\epsilon/n)$ とする．
2. $p'_i = \lfloor p_i/K \rfloor$ として，上の補題で示された動的計画法 A を実行する．
3. A の出力を出力する．

図 13: ＦＰＴＡＳアルゴリズム

証明. 図 13 のアルゴリズムの出力を S，最適解を S^* とする．$(1-\epsilon)\mathrm{val}(S^*) \leq \mathrm{val}(S)$ を示せば十分である．（十分小さな $\epsilon > 0$ に対して，$\mathrm{val}(S^*)/\mathrm{val}(S) \leq 1/(1-\epsilon) \leq 1 + 2\epsilon$ なので．）p'_i の定義より，任意の $i \in [n]$ について，

$$p'_i K \ \leq \ p_i \ \leq \ p'_i K + K.$$

また，$\{p'_1, \ldots, p'_n\}$ において S は最適解であるから，$\sum_{i \in S} p'_i \geq \sum_{i \in S^*} p'_i$．これらより，

$$\begin{aligned} \mathrm{val}(S) &= \sum_{i \in S} p_i \ \geq \ \sum_{i \in S} p'_i K \ \geq \ \sum_{i \in S^*} p'_i K \ \geq \ \sum_{i \in S^*} (p_i - K) \\ &\geq \sum_{i \in S^*} p_i - nK \quad (\because \ |S^*| \leq n) \\ &= \mathrm{val}(S^*) - nK. \end{aligned}$$

よって，（$K = P \cdot (\epsilon/n)$，$\mathrm{val}(S^*) \geq P$ より）

$$\mathrm{val}(S) \ \geq \ \mathrm{val}(S^*) - nK \ = \ \mathrm{val}(S^*) - \epsilon P \ \geq \ \mathrm{val}(S^*) - \epsilon \mathrm{val}(S^*) \ = \ (1-\epsilon)\mathrm{val}(S^*).$$

アルゴリズムの計算時間は，$P' = \max\{p'_i\} = n/\epsilon$ より，$O(n^2 P') = O(n^3/\epsilon)$ である． ■

9　充足可能性問題

定義 9.1

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 9.1 (充足可能性問題)**.** 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．

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

事実 9.1. 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．

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

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．

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

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，$\bar{x} \in C$ と表記する．)

定義 9.2

φ を X 上の任意の 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．

充足可能性問題（satisfiability）

- 入力：X 上の CNF 論理式 φ
- 解：X への真理値割り当て $t : X \to \{0,1\}$
- 最大化：t により充足する φ の節の個数

例 9.2. 先の例の 3-CNF 論理式 φ において（$|\varphi| = 6$），$t(X) = (1,1,1,1,1)$ により充足する φ の節の個数は 4，$t(X) = (1,1,1,1,0)$ により充足する φ の節の個数は 5.

9.1　貪欲法

定理 9.1. 充足可能性問題の近似率は 2 である．

入力：X 上の CNF 論理式 φ

1. $t : X \to \{0,1\}$ を未定義とする．(t が出力になる．)
2. それぞれの $x \in X$ について（順次）以下を繰り返す．
   (a) $P, N \subseteq \varphi$ を以下のように定義する．
   $$\begin{aligned} P &\stackrel{\text{def}}{=} \{C \in \varphi : x \in C\}, \\ N &\stackrel{\text{def}}{=} \{C \in \varphi : \bar{x} \in C\}. \end{aligned}$$
   (b) 以下のようにする．
   $$\begin{aligned} t(x) = 1,\ \varphi = \varphi \setminus P &\quad : \quad |P| \geq |N|, \\ t(x) = 0,\ \varphi = \varphi \setminus N &\quad : \quad \text{o.w.} \end{aligned}$$
3. t を出力する．

図 14: 貪欲アルゴリズム

問 9.1. 3 変数で 5 個の節からなる適当な入力を考案して，その入力に対する図 14 のアルゴリズムの動作及び出力を示しなさい．

証明. 図 14 のアルゴリズムの出力を t，最適解を t^* とする．$|X| = n$ とする．アルゴリズムのステップ 2 の第 i 回目（$i \in [n]$）の繰り返しにおいて，$|P| \geq |N|$ であるとき $A_i = P$, $B_i = N$，そうでないとき $A_i = N$, $B_i = P$ とする．

主張 9.1. 以下の二つが成り立つ．

$$\begin{aligned} &1. \quad \mathrm{val}(t) \ = \ \sum_{i \in [n]} |A_i| \\ &2. \quad \bigcup_{i \in [n]} (A_i \cup B_i) \ = \ \varphi. \end{aligned}$$

問 9.2. この主張を証明しなさい．

この主張より，

$$\begin{aligned} \mathrm{val}(t) \ &= \ \sum_{i \in [n]} |A_i| \ = \ \sum_{i \in [n]} |A_i| \cdot \frac{|A_i| + |B_i|}{|A_i| + |B_i|} \ = \ \sum_{i \in [n]} \frac{|A_i|}{|A_i| + |B_i|} \cdot (|A_i| + |B_i|) \\ &\geq \ \frac{1}{2} \sum_{i \in [n]} (|A_i| + |B_i|) \quad (\because \ |A_i| \geq |B_i|) \\ &\geq \ \frac{1}{2} \sum_{i \in [n]} |A_i \cup B_i| \quad (\because \ |A_i| + |B_i| \geq |A_i \cup B_i|) \\ &\geq \ \frac{1}{2} \left| \bigcup_{i \in [n]} (A_i \cup B_i) \right| \quad (\because \ \text{上と同等の理由}) \end{aligned}$$

$$= \frac{1}{2} \cdot |\varphi|$$
$$\geq \frac{\mathrm{val}(t^*)}{2}.$$

よって，$\mathrm{val}(t^*)/\mathrm{val}(t) \leq 2$. ■

問 9.3. 図 14 のアルゴリズムの近似率が 2 となる入力の例をあげなさい.

9.2 乱択アルゴリズム

定義 9.3

A を任意の事象とする．A が起きる確率を $\Pr\{A\}$ と表記する．ランダムビット列 r によって A が決まるとき，その確率を $\Pr_r\{A\}$ と表記する.

定義 9.4

Z を任意の確率変数とする．Z の期待値を $\mathrm{E}[Z]$ と表記する．ランダムビット列 r によって Z の値が決まるとき，その期待値を $\mathrm{E}_r[Z]$ と表記する.

例 9.3. 「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．このコイン投げにおいて，X を表の出る回数とする．このとき,

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

命題 9.2. Z を任意の確率変数とする．このとき，任意の定数 $a \in \mathbb{R}$ に対して，$\mathrm{E}[a \cdot Z] = a \cdot \mathrm{E}[Z]$.

命題 9.3. Z_1, Z_2 を任意の確率変数とする．このとき，$\mathrm{E}[Z_1 + Z_2] = \mathrm{E}[Z_1] + \mathrm{E}[Z_2]$.

問 9.4. 上の二つの命題を証明しなさい.

系 9.4. $\mathrm{E}[a_1 Z_1 + a_2 Z_2] = a_1 \mathrm{E}[Z_1] + a_2 \mathrm{E}[Z_2]$.

例 9.4. 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 9.1. 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 9.5. $t : \{x_1, \ldots, x_n\} \to \{0, 1\}$ を一様ランダムな割り当てとする．このとき，節 $C = (x_1 \vee \cdots \vee x_k)$（$k \leq n$）に対して，

$$\Pr_t\{t \text{ により } C \text{ が充足する}\} \;=\; 1 - 2^{-k}.$$

問 9.5. 上の命題を証明しなさい．

定義 9.5

任意の $k \in \mathbb{N}$ について，$f(k) \stackrel{\text{def}}{=} 1 - 2^{-k}$ とする．

注 9.2. $f(k)$ は，大きさ k の節が（一様ランダムな割り当てにより）充足する確率を意味する．$f(k)$ は単調増加関数であり，任意の $k \in \mathbb{N}$ に対して，$1/2 \leq f(k) < 1$.

入力：X 上の CNF 論理式 φ

1. 一様ランダムな割り当て $t : X \to \{0, 1\}$ を出力する．

図 15: 乱択アルゴリズム

問 9.6. 3 変数で 5 個の節からなる適当な入力を考案して，その入力に対する図 15 のアルゴリズムの動作及び出力を示しなさい．

定理 9.2. φ を，X 上の任意の k-CNF 論理式とする．図 15 のアルゴリズムの出力を t，φ の最適解を t^* とする．すべての節の大きさが（ちょうど）k であるとき，

$$\mathrm{E}_t[\mathrm{val}(t)] \;\geq\; f(k) \cdot \mathrm{val}(t^*).$$

証明. $\varphi = \{C_j : j \in [m]\}$ とする．$\mathrm{E}_t[\mathrm{val}(t)] \geq f(k) \cdot m$ を示せばよい．($m \geq \mathrm{val}(t^*)$ なので.）任意の $j \in [m]$ について，以下のような確率変数 Z_j を導入する．

$$Z_j \;=\; \begin{cases} 1 & : \; t \text{ により } C_j \text{ が充足する} \\ 0 & : \; \text{それ以外} \end{cases}$$

$Z = \sum_{j \in [m]} Z_j$ とすれば，$\mathrm{val}(t) = Z$ より $\mathrm{E}_t[\mathrm{val}(t)] = \mathrm{E}_t[Z]$．よって，期待値の線形性より，

$$\mathrm{E}_t[\mathrm{val}(t)] \;=\; \mathrm{E}_t[Z] \;=\; \mathrm{E}_t\left[\sum_{j \in [m]} Z_j\right] \;=\; \sum_{j \in [m]} \mathrm{E}_t[Z_j].$$

主張 9.2. $\mathrm{E}_t[Z_j] = f(k)$.

問 9.7. この主張を証明しなさい.

この主張より,

$$\mathop{\mathrm{E}}_{t}[\mathrm{val}(t)] \;=\; \sum_{j\in[m]} \mathop{\mathrm{E}}_{t}[Z_j] \;=\; \sum_{j\in[m]} f(k) \;\geq\; f(k)\cdot m.$$

■

系 9.6. $\mathrm{E}_t[\mathrm{val}(t)] \geq \mathrm{val}(t^*)/2$.

9.3 線形計画法の適用

充足可能性問題は，**整数計画問題** $P_{\mathbf{int}}$ として以下のように定式化される．$\varphi = \{C_j : j \in [m]\}$ を $X = \{x_1, \ldots, x_n\}$ 上の CNF 論理式として,

$$\begin{aligned}
&\text{目的関数} \quad : \quad \sum_{j\in[m]} y_j \\
&\text{制約式} \quad : \quad \sum_{x_i\in C_j} z_i + \sum_{\bar{x}_i\in C_j} (1-z_i) \geq y_j \text{ for } j \in [m] \\
&\qquad\qquad\quad\; y_j, z_i \in \{0,1\}
\end{aligned}$$

例 9.5. $X = \{x_1, \ldots, x_5\}$ 上の 3-CNF 論理式 φ が以下のようであるとき,

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

φ が入力である整数計画問題は以下のようになる.

$$\begin{aligned}
&\text{目的関数} \quad : \quad \sum_{j\in[6]} y_j \\
&\text{制約式} \quad : \quad \begin{cases}
z_1 & \geq\; y_1 \\
(1-z_1) + z_2 & \geq\; y_2 \\
z_1 + (1-z_2) + (1-z_3) & \geq\; y_3 \\
(1-z_1) + (1-z_3) + z_4 & \geq\; y_4 \\
1 - z_2 & \geq\; y_5 \\
(1-z_3) + (1-z_4) + (1-z_5) & \geq\; y_6
\end{cases} \\
&\qquad\qquad\quad\; y_j, z_i \in \{0,1\}
\end{aligned}$$

上の定式化において，変数 y_j, z_i のとる値を緩和して，以下のような**線形計画問題** $P_{\mathbf{lin}}$ を考える．($y_j, z_i \in \{0,1\}$ が $y_j, z_i \in [0,1]$ に緩和される.)

$$\begin{aligned}
&\text{目的関数} \quad : \quad \sum_{j\in[m]} y_j \\
&\text{制約式} \quad : \quad \sum_{x_i\in C_j} z_i + \sum_{\bar{x}_i\in C_j} (1-z_i) \geq y_j \text{ for } j \in [m] \\
&\qquad\qquad\quad\; y_j, z_i \in [0,1]
\end{aligned}$$

事実 9.7. 一般に，整数計画問題は NP 困難である．一方，線形計画問題は多項式時間計算可能である．

補題 9.8. $\varphi = \{C_j : j \in [m]\}$ の最適解を t^* とする．φ に対する線形計画問題 P_{lin} の最適解を $y_j, z_i \in [0,1]$ とする．このとき，

$$\sum_{j\in[m]} y_j \ \geq\ \mathrm{val}(t^*).$$

問 9.8. この補題を証明しなさい．

入力：X 上の CNF 論理式 φ

1. 線形計画問題 P_{lin} を解く．(最適解を $y \in [0,1]^m$, $z \in [0,1]^n$ とする．)
2. 以下のような確率で決められるランダムな割り当て $t : X \to \{0,1\}$ を出力する．

$$\begin{aligned}\Pr_t\{x_i = 1\} &= z_i\\ \Pr_t\{x_i = 0\} &= 1 - z_i\end{aligned}$$

図 16: 線形計画法を用いた乱択アルゴリズム

問 9.9. 3 変数で 5 個の節からなる適当な入力を考案して，その入力に対する図 16 のアルゴリズムの動作及び出力を示しなさい．(線形計画問題を解くときは，単体法などを用いて手計算で解くこと．ソルバを利用しないこと．)

定理 9.3. φ を，X 上の任意の k-CNF 論理式とする．図 16 のアルゴリズムの出力を t，φ の最適解を t^* とする．このとき，

$$\mathop{\mathrm{E}}_{t}[\mathrm{val}(t)] \ \geq\ (1 - (1 - 1/k)^k)\mathrm{val}(t^*).$$

証明. $\varphi = \{C_j : j \in [m]\}$ とする．φ に対する線形計画問題 P_{lin} の最適解を $y_j, z_i \in [0,1]$ とする．まず，任意の $j \in [m]$ について，C_j が充足する確率を求める．$C_1 = (x_1 \vee \cdots \vee x_k)$ とした場合，C_1 が充足する確率は，

$$\begin{aligned}\Pr_t\{t \text{ により } C_1 \text{ が充足する }\} &= 1 - \prod_{i\in[k]}(1 - z_i)\\ &\geq 1 - \left(\frac{\sum_{i\in[k]}(1 - z_i)}{k}\right)^k \quad (\because \text{ 相加相乗平均の公式})\end{aligned}$$

$$
\begin{aligned}
&= 1 - \left(1 - \frac{\sum_{i\in[k]} z_i}{k}\right)^k \\
&\geq 1 - (1 - y_1/k)^k \quad \left(\because \sum_{i\in[k]} z_i \geq y_1\right) \\
&\geq (1 - (1 - 1/k)^k) y_1. \quad (\because \text{下の問})
\end{aligned}
$$

問 9.10. $h(y) = 1 - (1 - y/k)^k$ とする.（k は任意の自然数.）このとき，$0 \leq y \leq 1$ について，

$$h(y) \ \geq \ (1 - (1 - 1/k)^k) y.$$

（ヒント：関数 $h(y)$ は上に凸で不等式の右辺は線形.）

この導出からも分かるように，$C_1 = (x_1 \vee \cdots \vee x_k)$ としても一般性を失わない.

問 9.11. $C_1 = (x_1 \vee \bar{x}_2 \vee \bar{x}_3)$ のとき，C_1 が充足する確率の下界はどうなるか．それを導出するための途中計算式を示しなさい.

任意の $j \in [m]$ について上の式が成り立つから，定理 9.2 と同様（$\mathrm{val}(t) = Z = \sum_{j\in[m]} Z_j$）にして，

$$
\begin{aligned}
\mathop{\mathrm{E}}_{t}[\mathrm{val}(t)] &= \sum_{j\in[m]} \mathop{\mathrm{E}}_{t}[Z_j] \\
&= \sum_{j\in[m]} \Pr_t\{t \text{ により } C_j \text{ が充足する }\} \\
&\geq \sum_{j\in[m]} (1 - (1 - 1/k_j)^{k_j}) y_j \quad (\because |C_j| = k_j) \\
&\geq (1 - (1 - 1/k)^k) \sum_{j\in[m]} y_j \quad (\because 1 - (1 - 1/k)^k \text{ は減少関数}) \\
&\geq (1 - (1 - 1/k)^k) \mathrm{val}(t^*). \quad (\because \text{上の補題})
\end{aligned}
$$

問 9.12. $1 - (1 - 1/k)^k$ が単調減少関数（$k \geq 1$）であることを示しなさい.

■

定義 9.6

任意の $k \in \mathbb{N}$ について，$g(k) \stackrel{\mathrm{def}}{=} 1 - (1 - 1/k)^k$ とする.

注 9.3. $g(k) y_j$ は，大きさ k の節 C_j が（P_{lin} を解くことにより得られたランダムな割り当てにより）充足する確率（の下界）を意味する．$g(k)$ は単調減少関数であり，任意の $k \in \mathbb{N}$ に対して，$1 - 1/e \leq g(k) < 1$.

問 9.13. 任意の自然数 k について，$(1-1/k)^k \leq 1/\mathrm{e}$ であることを示しなさい．（ヒント：任意の $x \in \mathbb{R}$ について $1+x \leq \mathrm{e}^x$．）

注 9.4. 二つの関数 $f(k)$ と $g(k)$ を比較する．$f(k)$ は増加関数であり，$g(k)$ は減少関数である．$f(k)=g(k)$ となるのは $k=2$ のときで，$f(2)=g(2)=0.75$.

k	1	2	3	4	5
$f(k)$	0.5	0.75	0.875	0.9375	0.9687
$g(k)$	1	0.75	0.7037	0.6835	0.6723

入力：X 上の CNF 論理式 φ

1. 線形計画問題 P_{lin} を解く．（最適解を $y \in [0,1]^m$, $z \in [0,1]^n$ とする．）
2. 以下のような確率で決められるランダムな割り当てを $t_1 : X \to \{0,1\}$ とする．

$$\begin{aligned} \Pr\{x_i = 1\} &= z_i \\ \Pr\{x_i = 0\} &= 1 - z_i \end{aligned}$$

3. t_2 を一様ランダムな割り当てとして，等確率で t_1 または t_2 を t として出力する．

図 17: 二つのアルゴリズムの融合

定理 9.4. φ を，X 上の任意の k-CNF 論理式とする．図 17 のアルゴリズムの出力を t，φ の最適解を t^* とする．このとき，

$$\mathop{\mathrm{E}}_{t}[\mathrm{val}(t)] \;\geq\; (3/4)\mathrm{val}(t^*).$$

証明. $\varphi = \{C_j : j \in [m]\}$ とする．まず，任意の $j \in [m]$ について，C_j が充足する確率を求める．$C_1 = (x_1 \vee \cdots \vee x_k)$ とした場合，C_1 が充足する確率は，

$$\begin{aligned} \Pr_t\{t \text{ により } C_1 \text{ が充足する }\} &\geq \frac{1}{2}f(k) + \frac{1}{2}g(k)y_1 \\ &= \frac{1}{2}(1-2^{-k}) + \frac{1}{2}(1-(1-1/k)^k)y_1 \\ &\geq \frac{1}{2}y_1\left((1-2^{-k}) + (1-(1-1/k)^k)\right) \quad (\because\ y_1 \leq 1) \\ &= \frac{1}{2}y_1\left(2 - 2^{-k} - (1-1/k)^k\right) \\ &\geq \frac{3}{4}y_1 \quad (\because\ \text{下の問}) \end{aligned}$$

問 9.14. 任意の自然数 k について，$2-2^{-k}-(1-1/k)^k \geq 3/2$ であることを示しなさい．（ヒント：$k \geq 3$ については問 9.13 が適用できる．）

任意の $j \in [m]$ について上の式が成り立つから，定理 9.2 と同様（$\mathrm{val}(t) = Z = \sum_{j\in[m]} Z_j$）にして，

$$\begin{aligned}
\mathop{\mathrm{E}}_{t}[\mathrm{val}(t)] &= \sum_{j\in[m]} \mathop{\mathrm{E}}_{t}[Z_j] \\
&= \sum_{j\in[m]} \Pr_t\{t \text{ により } C_j \text{ が充足する}\} \\
&\geq \sum_{j\in[m]} (3/4)y_i \\
&\geq (3/4)\mathrm{val}(t^*).
\end{aligned}$$

■

9.4 脱乱択化

定義 9.7

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．

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

例 9.6. 「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．

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

このとき，

$$\begin{aligned}
\Pr\{E|F\} &= \frac{1}{2} \\
\Pr\{F|E\} &= \frac{1}{2} \\
\Pr\{G|(E \cup F)\} &= \frac{1}{3} \quad \left(= \frac{\Pr\{G \cap (E \cup F)\}}{\Pr\{E \cup F\}} = \frac{1/4}{3/4} = \frac{1}{3}\right)
\end{aligned}$$

命題 9.9. 任意の事象 E, F について，

$$\Pr\{E\} = \Pr\{F\} \cdot \Pr\{E|F\} + \Pr\{\bar{F}\} \cdot \Pr\{E|\bar{F}\}.$$

問 9.15. 上の命題を証明しなさい．

定義 9.8

$\varphi = \{C_j : j \in [m]\}$ を，X 上の任意の CNF 論理式とする．$t : X \to \{0,1\}$ をランダムな割り当てとする．(一様ランダムとは限らない.) 任意の $j \in [m]$ について確率変数 Z_j を以下のように定義する．

$$Z_j \;=\; \begin{cases} 1 & : \; t \text{ により } C_j \text{ が充足する} \\ 0 & : \; \text{それ以外} \end{cases}$$

$Z = \sum_{j\in[m]} Z_j$ としたとき，

$$\alpha(\varphi) \;\stackrel{\text{def}}{=}\; \mathrm{E}_t[Z] \;=\; \sum_{j\in[m]} \mathrm{E}_t[Z_j] \;=\; \sum_{j\in[m]} \Pr_t\{t \text{ により } C_j \text{ が充足する }\}.$$

例 9.7. $\varphi = \{C_j : j \in [m]\}$ を，X 上の任意の CNF 論理式とする．$t : X \to \{0,1\}$ を一様ランダムな割り当てとすれば，$\alpha(\varphi) \geq m/2$. (定理 9.2 より.)

定義 9.9

$\varphi = \{C_j : j \in [m]\}$ を，X 上の任意の CNF 論理式とする．$t' : X' \to \{0,1\}$ を変数 $X' \subseteq X$ への任意の割り当てとする．このとき，t' を φ へ「適用した」後の CNF 論理式を，$\varphi|_{t'}$ と表記する．

例 9.8 (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．

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

$X' = \{x_2, x_5\}$ として，部分割り当て $t : X' \to \{0,1\}$ を $t(x_2, x_5) = (1,0)$ とする．このとき，

$$\varphi|_t \;=\; \{x_1, \phi_2, (x_1 \vee \bar{x}_3), (\bar{x}_1 \vee \bar{x}_3 \vee x_4), \phi_6\}.$$

ここで，充足した節 C_j を ϕ_j と表記する．(充足する可能性がなくなった節は削除する.) よって，$t(x_1, x_2, x_3, x_4, x_5) = (0,0,0,0,0)$ に対して，

$$\varphi|_t \;=\; \{\phi_2, \phi_3, \phi_4, \phi_6\}.$$

この場合，$\mathrm{val}(t) = \left|\varphi|_t\right| = 4$.

問 9.16. 3 変数で 5 個の節からなる適当な入力を考案して，その入力に対する図 18 のアルゴリズムの動作及び出力を示しなさい.

定理 9.5. φ を，X 上の任意の CNF 論理式とする．図 18 のアルゴリズムの出力を t，φ の最適解を t^* とする．このとき，

$$\mathrm{val}(t) \;\geq\; \mathrm{val}(t^*)/2.$$

つまり，$\mathrm{val}(t^*)/\mathrm{val}(t) \leq 2$.

図 18 のアルゴリズムは，図 15 のアルゴリズム（乱択アルゴリズム）の脱乱択化である.(定理 9.2 では，$\mathrm{E}_t[\mathrm{val}(t)] \geq \mathrm{val}(t^*)/2$ となっている.)

入力：$X = \{x_1, \ldots, x_n\}$ 上の CNF 論理式 φ

1. $t : X \to \{0, 1\}$ を未定義とする．
2. それぞれの $i \in [n]$ について（順次）以下を繰り返す．
   (a) $\alpha(\varphi|_{x_i=1}) \geq \alpha(\varphi|_{x_i=0})$ であるなら $t(x_i) = 1$，そうでないなら $t(x_i) = 0$ とする．
   (b) $\varphi = \varphi|_t$ とする．
3. t を出力する．

図 18: 脱乱択化アルゴリズム

証明. $\varphi = \{C_j : j \in [m]\}$ とする．図 18 のアルゴリズムの出力を t，φ の最適解を t^* とする．

主張 9.3.

$$\begin{aligned} \alpha(\varphi) &\geq \mathrm{val}(t^*)/2 \\ \alpha(\varphi|_t) &= \mathrm{val}(t) \end{aligned}$$

問 9.17. この主張を証明しなさい．

アルゴリズムのステップ 2 の第一回目の繰り返しにおいて，$\alpha(\varphi|_{x_1=1}) \geq \alpha(\varphi|_{x_1=0})$ であったとする．(以下，そうでない場合も同様にして示される．) $r : X \to \{0, 1\}$ を一様ランダムな割り当てとする．

主張 9.4.

$$\sum_{j \in [m]} \Pr_r\{C_j \text{ が充足する } | x_1 = 1\} \;\geq\; \sum_{j \in [m]} \Pr_r\{C_j \text{ が充足する } | x_1 = 0\}.$$

問 9.18. この主張を証明しなさい．

この主張より，

$$\begin{aligned} \alpha(\varphi) &= \sum_{j \in [m]} \mathrm{E}_r[Z_j] = \sum_{j \in [m]} \Pr_r\{C_j \text{ が充足する }\} \\ &= \Pr_r\{x_1 = 1\} \sum_{j \in [m]} \Pr_r\{C_j \text{ が充足する } | x_1 = 1\} + \Pr_r\{x_1 = 0\} \sum_{j \in [m]} \Pr_r\{C_j \text{ が充足する } | x_1 = 0\} \\ &= \frac{1}{2} \sum_{j \in [m]} \Pr_r\{C_j \text{ が充足する } | x_1 = 1\} + \frac{1}{2} \sum_{j \in [m]} \Pr_r\{C_j \text{ が充足する } | x_1 = 0\} \\ &= \frac{1}{2} \left(\sum_{j \in [m]} \Pr_r\{C_j \text{ が充足する } | x_1 = 1\} + \sum_{j \in [m]} \Pr_r\{C_j \text{ が充足する } | x_1 = 0\} \right) \\ &\leq \sum_{j \in [m]} \Pr_r\{C_j \text{ が充足する } | x_1 = 1\} \quad (\because \text{ 主張より}) \\ &= \alpha(\varphi|_{x_1=1}). \end{aligned}$$

同様にして，任意の $i \in [n]$ について $t(x_i) = 1$ である場合，

$$\alpha(\varphi) \;\leq\; \alpha(\varphi|_{x_1=1}) \;\leq\; \alpha(\varphi|_{x_1=1, x_2=1}) \;\leq\; \cdots \;\leq\; \alpha(\varphi|_{x_1=1, x_2=1, \ldots, x_n=1}).$$

そうでない場合もこれと同じ不等式が得られる．上の主張より，

$$\mathrm{val}(t^*)/2 \ \leq \ \alpha(\varphi) \ \leq \ \alpha(\varphi|_{x_1=1,x_2=1,\ldots,x_n=1}) \ = \ \alpha(\varphi|_t) \ = \ \mathrm{val}(t).$$

よって，$\mathrm{val}(t^*)/\mathrm{val}(t) \leq 2$. ■

問 9.19. 図 14 の貪欲アルゴリズムと図 18 の脱乱択化アルゴリズムとの違いを述べなさい.（双方ともに近似率は 2 である.）

問 9.20. 図 18 のアルゴリズムは，図 15 で示された乱択アルゴリズムの脱乱択化である．図 16 で示された乱択アルゴリズムの脱乱択化はどのようにすればよいか．アルゴリズムとその近似率の解析をを示しなさい.（ヒント：α を定義するのに必要な t の確率分布を適切に定義する.）

更に，図 17 で示された乱択アルゴリズムの脱乱択化はどのようにすればよいか.（アルゴリズムとその近似率の解析をを示しなさい.）

9.5 半正定値計画法の適用 *

MAX2SAT 問題

- 入力：X 上の 2-CNF 論理式 φ
- 解：X への真理値割り当て $t : X \to \{0,1\}$
- 最大化：t により充足する φ の節の個数

変数 $X = \{x_1, \ldots, x_n\}$ 上の任意の 2-CNF 論理式 φ を考える．各変数 $x_i \in \{0,1\}$ に対して，変数 $y_i \in \{-1,1\}$ を導入する．変数 x_i の真理値を以下のように対応づける．

$$\begin{array}{ll} x_i = 0 & \text{のとき} \quad y_i = 1 \\ x_i = 1 & \text{のとき} \quad y_i = -1 \end{array} \tag{9}$$

節 $(x_i), (\bar{x}_i)$ に対して，

$$\begin{aligned} (x_i) \quad &\Longleftrightarrow \quad \frac{1-y_i}{2} \\ (\bar{x}_i) \quad &\Longleftrightarrow \quad \frac{1+y_i}{2} \end{aligned}$$

このとき，節 (x_i) について，

$$\begin{aligned} (x_i) = 0 \quad &\Longleftrightarrow \quad \frac{1-y_i}{2} = 0 \quad (\because \ x_i = 0, \ y_i = 1) \\ (x_i) = 1 \quad &\Longleftrightarrow \quad \frac{1-y_i}{2} = 1 \quad (\because \ x_i = 1, \ y_i = -1) \end{aligned}$$

また，節 $(\bar{x}_i)$ について，

$$\begin{aligned} (\bar{x}_i) = 0 \quad &\Longleftrightarrow \quad \frac{1+y_i}{2} = 0 \quad (\because \ x_i = 1, \ y_i = -1) \\ (\bar{x}_i) = 1 \quad &\Longleftrightarrow \quad \frac{1+y_i}{2} = 1 \quad (\because \ x_i = 0, \ y_i = 1) \end{aligned}$$

同様にして，節 $(x_i \vee x_j)$ について，

$$\begin{aligned}(x_i \vee x_j) &\iff 1 - \frac{1+y_i}{2}\frac{1+y_j}{2} \\ &= 1 - \frac{1+y_i+y_j+y_iy_j}{4} \\ &= \frac{1-y_i}{4} + \frac{1-y_j}{4} + \frac{1-y_iy_j}{4}.\end{aligned}$$

問 9.21. 節 $(\bar{x}_i \vee x_j)$ に対応する式を求めなさい．

ここで，便宜上，更に，定数変数 $y_0 = 1$ を導入する．このとき，節 $(x_i \vee x_j)$ は，

$$\begin{aligned}(x_i \vee x_j) &= \frac{1-y_i}{4} + \frac{1-y_j}{4} + \frac{1-y_iy_j}{4} \\ &= \frac{1-y_0y_i}{4} + \frac{1-y_0y_j}{4} + \frac{1-y_iy_j}{4}\end{aligned}$$

以上より，MAX2SAT 問題は，**二次計画問題 $P_{\mathbf{quad}}$** として以下のように定式化される．$\varphi = \{C_j : j \in [m]\}$ を $X = \{x_1, \ldots, x_n\}$ 上の CNF 論理式として，

$$\begin{aligned}&\text{目的関数} \quad : \quad \sum_{i,j \in [n]_0 : i<j} a_{ij}(1+y_iy_j) + b_{ij}(1-y_iy_j) \\ &\text{制約式} \quad : \quad y_i^2 = 1 \\ &\qquad\qquad\ \ y_i \in \mathbb{Z},\ y_0 = 1\end{aligned}$$

問 9.22. 3 変数 5 個の節からなる適当な 2-CNF 論理式を考案して，その論理式に対する二次計画問題を示しなさい．

上の定式化において，変数 y_i のとる値を緩和して，以下のような**ベクトル計画問題 $P_{\mathbf{vect}}$** を考える．($y_i \in \mathbb{Z}$ がベクトル $v_i \in \mathbb{R}^{n+1}$ に緩和される．)

$$\begin{aligned}&\text{目的関数} \quad : \quad \sum_{i,j \in [n]_0 : i<j} a_{ij}(1+v_iv_j) + b_{ij}(1-v_iv_j) \\ &\text{制約式} \quad : \quad |v_i| = 1 \\ &\qquad\qquad\ \ v_i \in \mathbb{R}^{n+1},\ v_0 = (1, 0, \ldots, 0)\end{aligned}$$

ただし，v_iv_j は v_i と v_j の内積を表す．

事実 9.10. 一般に，整数計画問題は NP 困難である．一方，ベクトル計画問題は（任意の近似率 ϵ で）多項式時間計算可能である．(次元 n と $\ln(1/\epsilon)$ の多項式．)

補題 9.11. $\varphi = \{C_j : j \in [m]\}$ の最適解を t^* とする．φ に対するベクトル計画問題 P_{vec} の最適解を $v_i \in \mathbb{R}^{n+1}$ とする．このとき，

$$\sum_{i,j \in [n]_0 : i<j} a_{ij}(1+v_iv_j) + b_{ij}(1-v_iv_j) \ \geq\ \mathrm{val}(t^*).$$

入力：X 上の 2-CNF 論理式 φ

1. ベクトル計画問題 P_{vect} を解く．（最適解を $v_0, v_1, \ldots, v_n \in \mathbb{R}^{n+1}$ とする．）
2. 一様ランダムなベクトルを $r \in \mathbb{R}^{n+1}$（ただし $|r| = 1$）とする．
3. 以下のように（r と v_i から）決められる割り当てを $t : X \to \{0,1\}$ とする．

$$t(x_i) \;=\; \begin{cases} 1 & : \quad r \cdot v_i \geq 0 \\ 0 & : \quad \text{o.w.} \end{cases}$$

4. t を出力する．

図 19: 半正定値計画法を用いた乱択アルゴリズム

定理 9.6. φ を，X 上の任意の 2-CNF 論理式とする．図 19 のアルゴリズムの出力を t，φ の最適解を t^* とする．このとき，

$$\mathop{\mathrm{E}}_{t}[\mathrm{val}(t)] \;\geq\; \alpha \cdot \mathrm{val}(t^*).$$

ただし，

$$\alpha \stackrel{\mathrm{def}}{=} \frac{2}{\pi} \cdot \min_{0 \leq \theta \leq \pi} \frac{\theta}{1 - \cos\theta}.$$

証明. 以下では，（式 (9) で対応が示されたように）$t(x_i) \in \{0,1\}$ に応じて $y_i \in \{-1,1\}$ がランダムに振る舞うとする．二次計画問題 P_{quad} より，

$$\begin{aligned} \mathop{\mathrm{E}}_{t}[\mathrm{val}(t)] &= \mathop{\mathrm{E}}_{t}\left[\sum_{i,j \in [n]_0 : i<j} (a_{ij}(1 + y_i y_j) + b_{ij}(1 - y_i y_j))\right] \\ &= \sum_{i,j \in [n]_0 : i<j} \left(a_{ij} \cdot \mathrm{E}_t[1 + y_i y_j] + b_{ij} \cdot \mathrm{E}_t[1 - y_i y_j]\right). \end{aligned}$$

主張 9.5. 任意の $i, j \in [n]_0 : i \neq j$ について，

$$\begin{aligned} \mathrm{E}_t[1 + y_i y_j] &= 2 \Pr_t\{y_i = y_j\}. \\ \mathrm{E}_t[1 - y_i y_j] &= 2 \Pr_t\{y_i \neq y_j\}. \end{aligned}$$

問 9.23. この主張を証明しなさい．

この主張より，

$$\begin{aligned} \mathop{\mathrm{E}}_{t}[\mathrm{val}(t)] &= \sum_{i,j \in [n]_0 : i<j} \left(a_{ij} \cdot \mathrm{E}_t[1 + y_i y_j] + b_{ij} \cdot \mathrm{E}_t[1 - y_i y_j]\right) \\ &= \sum_{i,j \in [n]_0 : i<j} \left(2a_{ij} \cdot \Pr_t\{y_i = y_j\} + 2b_{ij} \cdot \Pr_t\{y_i \neq y_j\}\right). \end{aligned}$$

φ に対するベクトル計画問題 P_{vec} の最適解を $v_i \in \mathbb{R}^{n+1}$ とする．任意の $i,j \in [n]_0$ について，v_i, v_j のなす角を $\theta_{ij} \in [0,\pi]$ とする．(よって，$v_i v_j = |v_i||v_j| \cos\theta_{ij} = \cos\theta_{ij}$.)

主張 9.6. 任意の $i,j \in [n]_0 : i \neq j$ について，

$$\begin{aligned} \Pr_t\{y_i = y_j\} &= \Pr_t\{x_i = x_j\} &= 1 - \frac{\theta_{ij}}{\pi}. \\ \Pr_t\{y_i \neq y_j\} &= \Pr_t\{x_i \neq x_j\} &= \frac{\theta_{ij}}{\pi}. \end{aligned}$$

問 9.24. この主張を証明しなさい.

この主張より，

$$\begin{aligned} \mathop{\mathrm{E}}_t[\mathrm{val}(t)] &= \sum_{i,j\in[n]_0 : i<j} \left(2a_{ij} \cdot \Pr_t\{y_i = y_j\} + 2b_{ij} \cdot \Pr_t\{y_i \neq y_j\} \right) \\ &= \sum_{i,j\in[n]_0 : i<j} \left(2a_{ij} \cdot (1 - \theta_{ij}/\pi) + 2b_{ij} \cdot \theta_{ij}/\pi \right). \end{aligned}$$

主張 9.7. 任意の $\theta : 0 \leq \theta \leq \pi$ について，

$$\begin{aligned} 1 - \frac{\theta}{\pi} &\geq \frac{\alpha}{2}(1 + \cos\theta). \\ \frac{\theta}{\pi} &\geq \frac{\alpha}{2}(1 - \cos\theta). \end{aligned}$$

問 9.25. この主張を証明しなさい.

この主張より，

$$\begin{aligned} \mathrm{E}[\mathrm{val}(t)] &= \sum_{i,j\in[n]_0 : i<j} (2a_{ij} \cdot (1 - \theta_{ij}/\pi) + 2b_{ij} \cdot \theta_{ij}/\pi) \\ &\geq \sum_{i,j\in[n]_0 : i<j} a_{ij} \cdot \alpha(1 + \cos\theta_{ij}) + b_{ij} \cdot \alpha(1 - \cos\theta_{ij}) \\ &= \alpha \cdot \left(\sum_{i,j\in[n]_0 : i<j} a_{ij}(1 + \cos\theta_{ij}) + b_{ij}(1 - \cos\theta_{ij}) \right) \\ &= \alpha \cdot \left(\sum_{i,j\in[n]_0 : i<j} a_{ij}(1 + v_i v_j) + b_{ij}(1 - v_i v_j) \right) \\ &\geq \alpha \cdot \mathrm{val}(t^*). \quad (\because \text{上の補題}) \end{aligned}$$

■

系 9.12. MAX2SAT 問題は，近似率 0.87856 である.

証明.

$$\alpha = \frac{2}{\pi} \cdot \min_{0\leq\theta\leq\pi} \frac{\theta}{1 - \cos\theta} \geq 0.87856.$$

■

10　頂点彩色問題

頂点彩色問題（coloring）

- 入力：グラフ $G = (V, E)$
- 解：$c : V \to [k]$ s.t. $\forall (u, v) \in E[c(u) \neq c(v)]$
- 最小化：k

例 10.1 (頂点彩色問題).

事実 10.1. グラフが 2 彩色可能かどうかは多項式時間で判定できる．更に，グラフが 2 彩色可能である場合，グラフの 2 彩色（の一つ）を多項式時間で求めることができる．

事実 10.2. 任意の $k \geq 3$ に対して，グラフが k-彩色可能かどうか判定する問題はＮＰ困難である．

以降では，入力を 3 彩色可能なグラフに限定した問題を考える．（その制約付きの問題を，単に，頂点彩色問題と呼ぶ．）

10.1　貪欲法

定理 10.1. $|V| = n$ のとき，頂点彩色問題の近似率は $(4/3)\sqrt{n}$ である．

入力：グラフ $G = (V, E)$

1. $U = V$ として，関数 $c : V \to [k]$ を未定義とする．（c が出力になる．）
2. $G[U]$ の最大次数が $\lfloor \sqrt{n} \rfloor + 1$ 以上である限り以下を繰り返す．
   (a) $G' = G[U]$ として，$u = \arg\max_{v \in U} \{d_{G'}(v)\}$ とする．
   (b) $G'' = G[N_u \cup \{u\}]$ として，G'' を 3 彩色する．（その 3 彩色を c とする．）
   (c) $U = U \setminus (N_u \cup \{u\})$ とする．
3. $G[U]$ を $\lfloor \sqrt{n} \rfloor$ 彩色する．
4. c を出力する．

図 20: 貪欲アルゴリズム

注 10.1. アルゴリズムのステップ 2-(b) において，G が 3 彩色可能であることから，u をある色で彩色した場合，$G[N_u]$ は 2 彩色可能である．（グラフの 2 彩色は多項式時間で求められる．）このとき，彩色に用いた 3 つの色は，以降の彩色に使用されないものとする．

注 10.2. アルゴリズムのステップ 3 において，グラフ $G[U]$ の最大時数は $\lfloor\sqrt{n}\rfloor$ 以下となっている．Brooks の定理より，$G[U]$ を $\lfloor\sqrt{n}\rfloor$ 彩色する[12]多項式時間アルゴリズムが存在する．

問 10.1. 7 頂点上の適当なグラフを考案して，そのグラフに対する図 20 のアルゴリズムの動作及び出力を示しなさい．

証明. 図 20 のアルゴリズムの出力を c，最適解を c^* とする．まず，ステップ 2 の繰り返し回数を見積もる．任意の繰り返しにおいて，頂点 u の次数は $\lfloor\sqrt{n}\rfloor+1$ 以上であることから，それぞれの繰り返しで U の大きさは少なくとも $\lfloor\sqrt{n}\rfloor+2$ は小さくなる．よって，繰り返し回数は高々，

$$\frac{n}{\lfloor\sqrt{n}\rfloor+2} \leq \frac{n}{\sqrt{n}} \leq \sqrt{n}.$$

それぞれの繰り返しで 3 つの色が使用されることから，ステップ 2 では高々 $3\sqrt{n}$ 色が使用される．ステップ 3 では高々 $\sqrt{n}$ 色が使用されることから，全体では高々 $4\sqrt{n}$ 色が使用される．よって，最適値は 3 であることから，$\mathrm{val}(c)/\mathrm{val}(c^*) \leq 4\sqrt{n}/3$. ■

問 10.2. 図 20 のアルゴリズムを簡単に修正することで，近似率を $(2\sqrt{3}/3)\sqrt{n}$ にすることができる．($2\sqrt{3}/3 < 4/3$.) どのように修正すればよいか示しなさい．

10.2 半正定値計画法を用いたアルゴリズム

命題 10.3. E, F を事象とする．このとき，

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

よって，

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

問 10.3. 上の命題を証明しなさい．

定理 10.2 (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，

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

証明. 上の系を用いて，数学的帰納法により示される． ■

[12] $G[U]$ が完全グラフでなければ．

問 10.4. 上の定理の証明を完成させなさい.

$G=(V,E)$ を 3 彩色可能なグラフとする.($V=[n]$ とする.) 以下のような**ベクトル計画問題** $P_{\mathbf{vect}}$ (最小化問題) を考える.

$$\begin{array}{lll} \text{目的関数} & : & d \\ \text{制約式} & : & v_i \cdot v_j \le d \text{ for } (i,j) \in E \\ & & |v_i| = 1 \\ & & v_i \in \mathbb{R}^n \end{array}$$

命題 10.4. d^* を P_{vect} の最適値とする. $G=(V,E)$ が 3 彩色可能なグラフであれば, $d^* \le -1/2$.

問 10.5. この命題を証明しなさい.

補題 10.5. $G=(V,E)$ をグラフとする. G の最大次数を Δ とする. 図 21 のアルゴリズムにおいて $t=\lfloor \log_3 \Delta \rfloor$ としたとき, アルゴリズムの近似率は ($1-1/\log n$ 以上の確率で) $\Delta^{0.63}\log n/3$ である.

注 10.3. アルゴリズムのステップ 3-(d) において, グラフ $G[U]$ は 2^t 彩色可能である.(任意の $s \in \{+,-\}^t$ について, U_s は独立頂点集合であるため.) このとき, 彩色に用いた 2^t 個の色は, 以降の彩色に使用されないものとする.

証明. 図 21 のアルゴリズムの出力を c, 最適解を c^* とする. まず, ステップ 3 の繰り返し回数を見積もる. 第 i 回目の繰り返しにおける V を V_i とする.($V_1=V=[n]$.)

主張 10.1. 任意の i について $\mathrm{E}[|V_{i+1}|\big||V_i|] \le |V_i|/3$ である.

証明. 任意のグラフ $G=(V,E)$ に対して $|V| \le 2|E|$ であることから, $|E(G[V_{i+1}])|$ を見積もる. 任意に $(x,y) \in E(G[V_i])$ を固定する. まず, 頂点 x,y が同色になる確率を見積もる. 任意の $j \in [t]$ について,

$$\Pr_{r_j}\{\mathrm{sgn}(v_x,r_j)=\mathrm{sgn}(v_y,r_j)\} \;\le\; \frac{1}{3}.$$

問 10.6. 上の不等式が成り立つ理由を説明しなさい.

この不等式より,

$$\begin{array}{rcl} \Pr\{x,y \text{ が同色 }\} & = & \Pr\{\forall j \in [t][\mathrm{sgn}(v_x,r_j)=\mathrm{sgn}(v_y,r_j)]\} \\ & \le & (1/3)^t \\ & \le & \dfrac{1}{3\Delta}. \end{array}$$

入力：グラフ $G = (V, E)$ // $V = [n]$

1. 関数 $c : V \to [k]$ を未定義とする.（c が出力になる.）
2. ベクトル計画問題 P_{vect} を解く.（最適解を $v_1, \ldots, v_n \in \mathbb{R}^n$ とする.）
3. $V \neq \emptyset$ である限り以下を繰り返す.
   (a) 一様ランダムなベクトルを $r_1, \ldots, r_t \in \mathbb{R}^n$（ただし $|r_i| = 1$）とする.
   (b) 任意の $s \in \{+, -\}^t$ について,
   $$C_s \;=\; \{i \in V : \forall j \in [t][\mathrm{sgn}(v_i, r_j) = s_j]\}.$$
   (c) 任意の $s \in \{+, -\}^t$ について,
   $$U_s \;=\; \{i \in C_s : \forall j \in C_s[(i, j) \notin E]\},$$
   として，$U = \bigcup_{s \in \{+,-\}^t} U_s$ とする.
   (d) $G[U]$ を 2^t 彩色する.（その彩色を c とする.）
   (e) $V = V \setminus U$ とする.
4. c を出力する.

図 21: 半正定計画を用いたアルゴリズム

よって，

$$\begin{aligned}\mathrm{E}[|E(G[V_{i+1}])|\big|V_i] &= \sum_{(x,y)\in E(G[V_i])} \Pr\{(x,y)\text{ が同色 }\}\\ &\le \frac{|V_i|\cdot\Delta}{2}\cdot\frac{1}{3\Delta}\\ &= \frac{|V_i|}{6}.\end{aligned}$$

よって，

$$\mathrm{E}[|V_{i+1}|\big|V_i] \;\le\; 2\cdot\mathrm{E}[|E(G[V_{i+1}])|\big|V_i] \;\le\; |V_i|/3.$$

■

主張 10.2. 任意の i について，

$$\Pr_{r_1,\ldots,r_t}\{|V_{i+1}| > |V_i|/2\big|V_i] \;\le\; \frac{1}{\log^2 n}.$$

この主張より，繰り返し回数が高々 $\log n$ である確率は，少なくとも $1-1/\log n$ である．

問 10.7. この事実が成り立つ理由を説明しなさい．

よって，それぞれの繰り返しで 2^t 個の色が使用されることから，アルゴリズム全体で使用される色の個数は，（少なくとも $1-1/\log n$ の確率で）高々，

$$\begin{aligned}2^t\log n &\le 2^{\log_3\Delta}\log n\\ &= \Delta^{\log_3 2}\log n\\ &\le \Delta^{0.63}\log n.\end{aligned}$$

よって，最適値は 3 であることから，$\mathrm{val}(c)/\mathrm{val}(c^*) \le \Delta^{0.63}\log n/3$. ■

この補題より，貪欲法の場合と同様にすれば，以下の定理が示される．

定理 10.3. $|V|=n$ のとき，頂点彩色問題の近似率は（$1-1/\log n$ 以上の確率で）$n^{0.39}$ である．

問 10.8. この定理を証明しなさい．アルゴリズムとその近似率の解析を示しなさい．（ヒント：半正値計画を用いたアルゴリズムを貪欲アルゴリズムのステップ 3 に用いる．）

11　最短ベクトル問題

ここでは，ベクトル $\boldsymbol{v}$ の長さを $|\boldsymbol{v}|$ と表記する．

最短ベクトル問題（shortest vector）

- 入力：一次独立な n 次元ベクトル $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n \in \mathbb{R}^n$
- 解：$a_1, a_2, \ldots, a_n \in \mathbb{Z}$
- 最小化：$\left|\sum_{i\in[n]} a_i \boldsymbol{v}_i\right|$

例 11.1 (最短ベクトル問題)**.**

以降，入力の n 次元ベクトルを $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n \in \mathbb{R}^n$ と表記して，それらは一次独立であるとする．

定義 11.1

任意のベクトル $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n \in \mathbb{R}^n$ について，

$$\mathcal{L}_u \stackrel{\text{def}}{=} \mathcal{L}_{\boldsymbol{u}_1,\ldots,\boldsymbol{u}_n} \stackrel{\text{def}}{=} \left\{ \sum_{i\in[n]} a_i \boldsymbol{u}_i : a_1, \ldots, a_n \in \mathbb{Z} \right\}.$$

$\mathcal{L}_u$ をベクトル $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n \in \mathbb{R}^n$ の**格子**，その要素を**格子点**と呼ぶ．また，入力ベクトル $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n \in \mathbb{R}^n$ について，

$$\mathcal{L} \stackrel{\text{def}}{=} \mathcal{L}_{\boldsymbol{v}_1,\ldots,\boldsymbol{v}_n}.$$

最短ベクトル問題は，格子 $\mathcal{L}$ の中で（原点からの）距離が最短の格子点（長さが最小のベクトル）を求める問題となる．

定義 11.2

任意の $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_n \in \mathbb{R}^n$ について，それら n 個のベクトルを行とする $n \times n$ 行列を $U \in \mathbb{R}^{n\times n}$ とする．つまり，

$$U = \left(\begin{array}{c} \boldsymbol{u}_1 \\ \hline \boldsymbol{u}_2 \\ \hline \vdots \\ \hline \boldsymbol{u}_n \end{array}\right)$$

同様にして，$\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ を行とする $n \times n$ 行列を $V \in \mathbb{R}^{n\times n}$ とする．

事実 11.1. 任意の $i \in [n]$ について，$\boldsymbol{u}_i$ が $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ の一次結合で表されるなら，その係数を行列 A とした場合，$U = AV$ となる．つまり，A の (i, j) 成分を a_{ij} とした場合，$\boldsymbol{u}_i = \sum_{j\in[n]} a_{ij} \boldsymbol{v}_j$.

行列 A の行列式を $\det(A)$ と表記する．($|A|$ と表記する教科書もある．)

事実 11.2. 任意の $i \in [n]$ について $\boldsymbol{u}_i \in \mathcal{L}$ なら，($U = AV$ とした) 行列 A は整数行列となる．よって，$\det(U)$ は $\det(V)$ の整数倍となる．

問 11.1. この事実を示しなさい.

事実 11.3. 任意の $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n \in \mathbb{R}^n$ について,

$$\mathcal{L} \subseteq \mathcal{L}_u \iff \exists A \in \mathbb{Z}^{n\times n}[V = AU].$$

問 11.2. この事実を示しなさい.

命題 11.4. n 次元ベクトル $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n \in \mathbb{R}^n$ の格子を $\mathcal{L}$ とする．任意の格子点 $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n \in \mathcal{L}$ について，$\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ の格子を $\mathcal{L}_u$ とする．このとき，以下の二つは同値である.

- $\mathcal{L}_u = \mathcal{L}$
- $|\det(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n)| = |\det(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n)|$

証明. $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n \in \mathcal{L}$ であることから,（事実 11.2 より）ある整数行列 A_v が存在して $U = A_v V$.

（⇒）$\mathcal{L}_u \supseteq \mathcal{L}$ より,（事実 11.3 から）ある整数行列 A_u が存在して $V = A_u U$. よって，$V = A_u A_v V$. これより，$\det(V) = \det(A_u A_v V) = \det(A_u)\det(A_v)\det(V)$. よって,（$\det(V) \neq 0$ より）$\det(A_u)\det(A_v) = 1$. これは，$|\det(A_v)| = |\det(A_u)| = 1$ であることを意味する. よって,

$$|\det(V)| \;=\; |\det(A_u U)| \;=\; |\det(A_u)\det(U)| \;=\; |\det(U)|.$$

（⇐）$\mathcal{L}_u \subseteq \mathcal{L}$ かつ $\mathcal{L}_u \supseteq \mathcal{L}$ を示す. $U = A_v V$ より（事実 11.3 から）$\mathcal{L}_u \subseteq \mathcal{L}$ は明らか. $\mathcal{L}_u \supseteq \mathcal{L}$ を示す. $U = A_v V$ より,

$$|\det(U)| \;=\; |\det(A_v V)| \;=\; |\det(A_v)| \cdot |\det(V)|.$$

$|\det(V)| = |\det(U)|$ より $|\det(A_v)| = 1$. この事実と A_v が整数行列であることから，A_v^{-1} は整数行列となる.

問 11.3. 整数行列となる理由を説明しなさい.（ヒント：逆行列は余因子行列で表される.）

よって，$V = A_v^{-1} U$ となり,（事実 11.3 から）$\mathcal{L}_u \supseteq \mathcal{L}$ が示される. ■

定義 11.3

ベクトル $\boldsymbol{u}_i, \boldsymbol{u}_j$ について,

$$\mu_{ij} \stackrel{\text{def}}{=} \frac{(\boldsymbol{u}_i, \boldsymbol{u}_j)}{|\boldsymbol{u}_j|^2}.$$

更に,

$$\lfloor \mu_{ij} \rceil \stackrel{\text{def}}{=} \arg\min_{z\in\mathbb{Z}} \{|z - \mu_{ij}|\}.$$

ベクトル $\boldsymbol{u}_i, \boldsymbol{u}_j$ に対して，μ_{ij} は次のように解釈できる. $\boldsymbol{u}_i, \boldsymbol{u}_j$ のなす角度を θ としたとき,

$$\mu_{ij} \;=\; \frac{(\boldsymbol{u}_i, \boldsymbol{u}_j)}{|\boldsymbol{u}_j|^2} \;=\; \frac{|\boldsymbol{u}_i|\cos\theta}{|\boldsymbol{u}_j|}.$$

よって，μ_{ij} は，$\boldsymbol{u}_i$ を $\boldsymbol{u}_j$ に射影したベクトルの長さの $|\boldsymbol{u}_j|$ に対する「比」となる．

命題 11.5. 任意のベクトル $\boldsymbol{u}_1, \boldsymbol{u}_2$ について，

$$\lfloor \mu_{21} \rceil \;=\; \arg\min_{m \in \mathbb{Z}} \{ |\boldsymbol{u}_2 - m\boldsymbol{u}_1| \}.$$

証明. $|\boldsymbol{u}_2 - m\boldsymbol{u}_1|^2$ の値が最小となる整数 m を考える．

$$\begin{aligned} |\boldsymbol{u}_2 - m\boldsymbol{u}_1|^2 &= |\boldsymbol{u}_2|^2 + m^2|\boldsymbol{u}_1|^2 - 2m(\boldsymbol{u}_2, \boldsymbol{u}_1) \\ &= |\boldsymbol{u}_2|^2 + |\boldsymbol{u}_1|^2 \left(m^2 - 2m \cdot \frac{(\boldsymbol{u}_2, \boldsymbol{u}_1)}{|\boldsymbol{u}_1|^2} \right) \\ &= |\boldsymbol{u}_2|^2 + |\boldsymbol{u}_1|^2 \left(m^2 - 2m\mu_{21} \right). \end{aligned}$$

この式より，$|\boldsymbol{u}_2 - m\boldsymbol{u}_1|$ の値が最小となる整数 m は，$|m - \mu_{21}|$ が最小となる整数 m である．

問 11.4. この事実が成り立つ理由を説明しなさい．

これは，$\lfloor \mu_{21} \rceil$ の定義に同じである． ■

11.1 二次元アルゴリズム

ここでは，二次元空間を考える．入力を $\boldsymbol{v}_1, \boldsymbol{v}_2$ として，その格子を $\mathcal{L}$ とする．最短ベクトルだけでなく，同時に，二番目に最短な（最短ベクトルと独立した）ベクトルも求める多項式時間アルゴリズムを考える．

命題 11.6. 格子が $\mathcal{L}$ となる任意の格子点 $\boldsymbol{u}_1, \boldsymbol{u}_2 \in \mathcal{L}$ について（つまり，$\mathcal{L} = \mathcal{L}_{\boldsymbol{u}_1, \boldsymbol{u}_2}$），$|\boldsymbol{u}_1| \leq |\boldsymbol{u}_2|$ かつ $|\mu_{21}| \leq 1/2$ であれば，$\mathcal{L}$ の最短ベクトルは $\boldsymbol{u}_1$ であり，二番目に最短な（最短ベクトルと独立した）ベクトルは $\boldsymbol{u}_2$ となる．

証明. 任意の $\boldsymbol{u} \in \mathcal{L}$ について $|\boldsymbol{u}| \geq |\boldsymbol{u}_2|$ を示せばよい．任意の整数 a_1, a_2 について，$\boldsymbol{u} = a_1\boldsymbol{u}_1 + a_2\boldsymbol{u}_2$ とする．このとき，$a_1 \neq 0$ かつ $a_2 \neq 0$ としてよい．

問 11.5. そのように仮定してよい理由を説明しなさい．

$|\mu_{21}| \leq 1/2$ より，

$$\begin{aligned} |\boldsymbol{u}|^2 &= |a_1\boldsymbol{u}_1 + a_2\boldsymbol{u}_2|^2 \\ &= a_1^2|\boldsymbol{u}_1|^2 + a_2^2|\boldsymbol{u}_2|^2 + 2a_1a_2(\boldsymbol{u}_2, \boldsymbol{u}_1) \\ &= a_1^2|\boldsymbol{u}_1|^2 + a_2^2|\boldsymbol{u}_2|^2 + 2a_1a_2|\boldsymbol{u}_1|^2\mu_{21} \\ &\geq a_1^2|\boldsymbol{u}_1|^2 + a_2^2|\boldsymbol{u}_2|^2 - |a_1||a_2||\boldsymbol{u}_1|^2. \end{aligned}$$

問 11.6. 上の不等式を示しなさい.

これより，以下の不等式を示せばよい.

$$\begin{aligned} & a_1^2|\boldsymbol{u}_1|^2 + a_2^2|\boldsymbol{u}_2|^2 - |a_1||a_2||\boldsymbol{u}_1|^2 \ \geq \ |\boldsymbol{u}_2|^2 \\ \iff \quad & (a_1^2 - |a_1||a_2|)|\boldsymbol{u}_1|^2 + (a_2^2 - 1)|\boldsymbol{u}_2|^2 \ \geq \ 0 \\ \iff \quad & (a_1^2 - |a_1||a_2|) + (a_2^2 - 1)\frac{|\boldsymbol{u}_2|^2}{|\boldsymbol{u}_1|^2} \ \geq \ 0 \end{aligned}$$

最後の不等式を示すためには，以下の不等式を示せばよい.

$$(a_1^2 - |a_1||a_2|) + (a_2^2 - 1) \ \geq \ 0. \tag{10}$$

問 11.7. 不等式 (10) を示せばよい理由を示しなさい．更に，不等式 (10) を示しなさい.

よって，最短ベクトルの二つは $\boldsymbol{u}_1, \boldsymbol{u}_2$ となる． ■

定理 11.1. $n = 2$ の（二次元である）とき，最短ベクトル問題は多項式時間で（厳密に）解くことができる.

入力：2 次元ベクトル $\boldsymbol{v}_1, \boldsymbol{v}_2 \in \mathbb{R}^2$

1. $\boldsymbol{u}_1, \boldsymbol{u}_2$ を $\boldsymbol{v}_1, \boldsymbol{v}_2$ の大きさの小さい方・大きい方とする.
2. $|\mu_{21}| > 1/2$ である限り以下を繰り返す.
   (a) $\boldsymbol{u}_2 = \boldsymbol{u}_2 - \lfloor \mu_{21} \rceil \boldsymbol{u}_1$ とする.
   (b) $|\boldsymbol{u}_1| > |\boldsymbol{u}_2|$ なら $\boldsymbol{u}_1$ と $\boldsymbol{u}_2$ を交換する.
3. $\boldsymbol{u}_1, \boldsymbol{u}_2$ を出力する.

図 22: ガウスのアルゴリズム

問 11.8. 二つの適当なベクトルを考案して，そのベクトルに対する図 22 のアルゴリズムの動作及び出力を示しなさい.

証明. アルゴリズムの正当性に関しては，命題 11.6 より，ステップ 2 の任意の繰り返しにおいて，$\boldsymbol{u}_1, \boldsymbol{u}_2$ の格子が $\mathcal{L}$ であることを示せばよい.

問 11.9. $\boldsymbol{u}_1, \boldsymbol{u}_2$ の格子が $\mathcal{L}$ であることを示しなさい.（ステップ 2 の繰り返し回数についての帰納法より示される．帰納段階の証明は，命題 11.4 を用いる.）

次に，計算時間を見積もる.

注 11.1. 計算時間を見積もる場合，入力ベクトル $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ の成分は有理数であるとしてよい．更に，計算時間が「入力長」の多項式であることを示すためには，それらはすべて整数であるとしてよい.（$\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n \in \mathbb{Z}^n$.）

主張 11.1. ステップ 2-(a) において,（更新された $\boldsymbol{u}_2$ に対して）$|\mu_{21}| \leq 1/2$ となる.（よって，$|\boldsymbol{u}_1| \leq |\boldsymbol{u}_2|$ なら，ステップ 2 が終了する.）

問 11.10. この主張を証明しなさい.

主張 11.2. ステップ 2-(b) において，$|\boldsymbol{u}_1| > |\boldsymbol{u}_2|$ であるとき，更に，$|\boldsymbol{u}_1|/\sqrt{3} < |\boldsymbol{u}_2|$ であるなら，その次の繰り返しでステップ 2 が終了する.

証明. ステップ 2 の繰り返しが第 k 回目であるとする.（よって，第 $k+1$ 回目で終了することを示す.）第 $k-1$ 回目の繰り返しが終了した直後の $\boldsymbol{u}_1, \boldsymbol{u}_2$ を $\boldsymbol{w}_1, \boldsymbol{w}_2$ と表記する.（よって，$|\boldsymbol{w}_1| \leq |\boldsymbol{w}_2|$.）$\boldsymbol{w}_1, \boldsymbol{w}_2$ に対する μ_{21} の値を $\mu_{21}^{(k-1)}$ と表記する.（よって，$|\mu_{21}^{(k-1)}| > 1/2$.）第 k 回目の繰り返しが終了した直後,（$|\boldsymbol{u}_1| > |\boldsymbol{u}_2|$ より交換されるので）$\boldsymbol{u}_1 = \boldsymbol{w}_2 - \lfloor \mu_{21}^{(k-1)} \rceil \boldsymbol{w}_1$, $\boldsymbol{u}_2 = \boldsymbol{w}_1$ となる．これらを $\boldsymbol{w}_1', \boldsymbol{w}_2'$ と表記する.（よって，$|\boldsymbol{w}_1'| \leq |\boldsymbol{w}_2'|$.）$\boldsymbol{w}_1', \boldsymbol{w}_2'$ に対する μ_{21} の値を $\mu_{21}^{(k)}$ と表記する.

繰り返し	$\boldsymbol{u}_1$	$\boldsymbol{u}_2$	μ_{21}
$k-1$	$\boldsymbol{w}_1$	$\boldsymbol{w}_2$	$\mu_{21}^{(k-1)}$
k	$\boldsymbol{w}_1' = \boldsymbol{w}_2 - \lfloor \mu_{21}^{(k-1)} \rceil \boldsymbol{w}_1$	$\boldsymbol{w}_2' = \boldsymbol{w}_1$	$\mu_{21}^{(k)}$

主張の仮定より，$|\boldsymbol{w}_1'| > |\boldsymbol{w}_2'|/\sqrt{3} = |\boldsymbol{w}_1|/\sqrt{3}$. よって,

$$\begin{aligned} \left|\mu_{21}^{(k)}\right| &= \left|\frac{(\boldsymbol{w}_2', \boldsymbol{w}_1')}{|\boldsymbol{w}_1'|^2}\right| = \left|\frac{(\boldsymbol{w}_1, \boldsymbol{w}_2 - \lfloor \mu_{21}^{(k-1)} \rceil \boldsymbol{w}_1)}{|\boldsymbol{w}_1'|^2}\right| \\ &< \left|\frac{(\boldsymbol{w}_2, \boldsymbol{w}_1) - ((\boldsymbol{w}_2, \boldsymbol{w}_1)/|\boldsymbol{w}_1|^2 \pm 1/2)|\boldsymbol{w}_1|^2}{|\boldsymbol{w}_1|^2/3}\right| \leq \frac{|\boldsymbol{w}_1|^2/2}{|\boldsymbol{w}_1|^2/3} = \frac{3}{2}. \end{aligned}$$

よって，$\lfloor \mu_{21}^{(k)} \rceil \in \{-1, 0, 1\}$. 第 $k+1$ 回目の繰り返しを考える.（よって，$\lfloor \mu_{21}^{(k)} \rceil \in \{-1, 1\}$.）ステップ 2-(a) において，$\lfloor \mu_{21}^{(k)} \rceil = 1$ のとき,

$$\begin{aligned} \boldsymbol{u}_2 = \boldsymbol{w}_2' - \boldsymbol{w}_1' &= \boldsymbol{w}_1 - (\boldsymbol{w}_2 - \lfloor \mu_{21}^{(k-1)} \rceil \boldsymbol{w}_1) \\ &= -(\boldsymbol{w}_2 - (\lfloor \mu_{21}^{(k-1)} \rceil + 1)\boldsymbol{w}_1) \end{aligned}$$

命題 11.5 より,

$$|\boldsymbol{u}_1| = |\boldsymbol{w}_1'| = |\boldsymbol{w}_2 - \lfloor \mu_{21}^{(k-1)} \rceil \boldsymbol{w}_1| \leq |-(\boldsymbol{w}_2 - (\lfloor \mu_{21}^{(k-1)} \rceil + 1)\boldsymbol{w}_1)| = |\boldsymbol{u}_2|.$$

つまり，$|\boldsymbol{u}_1| \leq |\boldsymbol{u}_2|$. よって，主張 11.1 より，ステップ 2 が終了する．$\lfloor \mu_{21}^{(k)} \rceil = -1$ のときも同様にして示される.

■

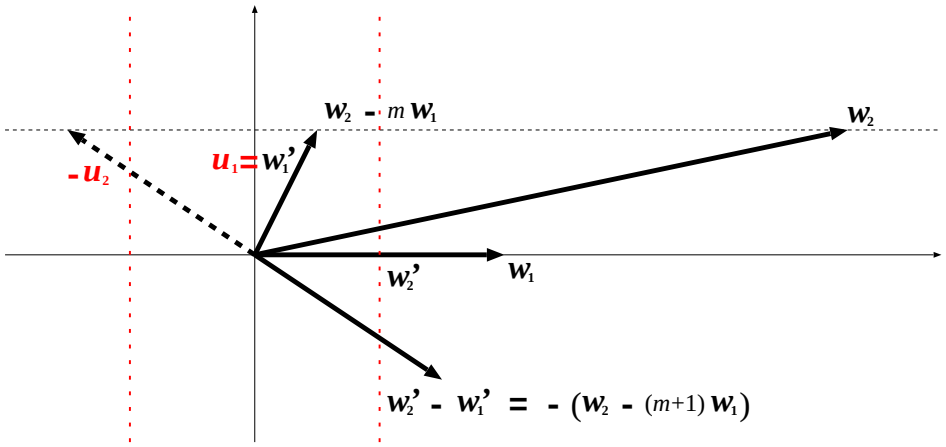

図 23: ベクトル $\boldsymbol{w}_1, \boldsymbol{w}_2, \boldsymbol{w}'_1, \boldsymbol{w}'_2$（$\lfloor \mu_{21}^{(k-1)} \rceil = m$ とする）

この主張より，アルゴリズムのステップ 2 の繰り返し回数は（注 11.1 より）$O(\log(\min\{|\boldsymbol{v}_1|, |\boldsymbol{v}_2|\}))$ となる．

問 11.11. この事実を証明しなさい．（ヒント：第 i 回目の繰り返しについて，$|\boldsymbol{w}_i|/\sqrt{3} \geq |\boldsymbol{w}_{i+1}|$．）

よって，アルゴリズムは多項式時間で終了する． ■

11.2 グラム・シュミットの直交基底

任意の $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n \in \mathbb{R}^n$ について，次のように定義された $\boldsymbol{u}_1^*, \ldots, \boldsymbol{u}_n^* \in \mathbb{R}^n$ を**グラム・シュミットの直交基底**という[13]．$\boldsymbol{u}_1^* \stackrel{\text{def}}{=} \boldsymbol{u}_1$，任意の $i \in [n] \setminus \{1\}$ について，

$$\boldsymbol{u}_i^* \stackrel{\text{def}}{=} \boldsymbol{u}_i - \left(\sum_{j \in [i-1]} \frac{(\boldsymbol{u}_i, \boldsymbol{u}_j^*)}{|\boldsymbol{u}_j^*|^2} \boldsymbol{u}_j^* \right).$$

事実 11.7. ベクトル $\boldsymbol{u}_1^*, \ldots, \boldsymbol{u}_n^*$ は互いに直交する．

問 11.12. この事実を示しなさい．

命題 11.8. 任意の $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n \in \mathbb{R}^n$ について，

$$|\det(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n)| \;=\; |\det(\boldsymbol{u}_1^*, \ldots, \boldsymbol{u}_n^*)| \;=\; |\boldsymbol{u}_1^*| \cdots |\boldsymbol{u}_n^*|.$$

証明. まず，一つ目の等式を示す．任意の $i \in [n]$ について，$\boldsymbol{u}_i = \sum_{j \in [i]} a_j \boldsymbol{u}_j^*$ とする[14]．ただし，$\boldsymbol{u}_i^*$

[13] 正規化はされていない．
[14] $\boldsymbol{u}_i^*$ の定義より．

の定義より，$a_i = 1$ である．行列式の性質より，

$$\begin{vmatrix} \boldsymbol{u}_1 \\ \boldsymbol{u}_2 \\ \vdots \\ \boldsymbol{u}_n \end{vmatrix} = \begin{vmatrix} \sum_{j\in[1]} a_j \boldsymbol{u}_j^* \\ \sum_{j\in[2]} a_j \boldsymbol{u}_j^* \\ \vdots \\ \sum_{j\in[n]} a_j \boldsymbol{u}_j^* \end{vmatrix}$$

$$= \begin{vmatrix} \boldsymbol{u}_1^* \\ \sum_{j\in[2]} a_j \boldsymbol{u}_j^* \\ \vdots \\ \sum_{j\in[n]} a_j \boldsymbol{u}_j^* \end{vmatrix} = \begin{vmatrix} \boldsymbol{u}_1^* \\ \boldsymbol{u}_2^* \\ \vdots \\ \sum_{j\in[n]} a_j \boldsymbol{u}_j^* \end{vmatrix} = \cdots\cdots$$

$$= \begin{vmatrix} \boldsymbol{u}_1^* \\ \boldsymbol{u}_2^* \\ \vdots \\ \boldsymbol{u}_n^* \end{vmatrix}$$

次に，二つ目の等式を示す．$\boldsymbol{u}_1^*, \ldots, \boldsymbol{u}_n^*$ を行とする行列を X とすれば，

$$\begin{aligned} \det(\boldsymbol{u}_1^*, \ldots, \boldsymbol{u}_n^*)^2 &= \det(X)^2 = \det(X)\det(X^{\mathbf{t}}) = \det(XX^{\mathbf{t}}) \\ &= \begin{vmatrix} |\boldsymbol{u}_1^*|^2 & & & 0 \\ & |\boldsymbol{u}_2^*|^2 & & \\ & & \ddots & \\ 0 & & & |\boldsymbol{u}_n^*|^2 \end{vmatrix} \\ &= |\boldsymbol{u}_1^*|^2 \cdots |\boldsymbol{u}_n^*|^2. \end{aligned}$$

■

命題 11.9. 任意の $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n \in \mathbb{R}^n$ について，

- $\boldsymbol{u}_1^*, \ldots, \boldsymbol{u}_{i-1}^*, \boldsymbol{u}_i^*, \ldots, \boldsymbol{u}_n^*$: $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{i-1}, \boldsymbol{u}_i, \ldots, \boldsymbol{u}_n \in \mathbb{R}^n$ に対する直交基底
- $\boldsymbol{w}_1^*, \ldots, \boldsymbol{w}_{i-1}^*, \boldsymbol{w}_i^*, \ldots, \boldsymbol{w}_n^*$: $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_i, \boldsymbol{u}_{i-1}, \ldots, \boldsymbol{u}_n \in \mathbb{R}^n$ に対する直交基底

このとき，

$$\begin{aligned} \boldsymbol{u}_j^* &= \boldsymbol{w}_j^* \quad : \ j \in [n] \setminus \{i-1, i\} \\ |\boldsymbol{u}_{i-1}^*||\boldsymbol{u}_i^*| &= |\boldsymbol{w}_{i-1}^*||\boldsymbol{w}_i^*| \end{aligned}$$

証明. まず，二つ目は，一つ目と命題 11.8 より示される．以下，一つ目を示す．$j \in [i-2]$ のときは（直交基底の定義より）明らか．$j = i+1$ のときを考える．($j \in [n] \setminus [i+1]$ のときも同様に示される.）証明を単純化するため，$|\boldsymbol{u}_{i-1}^*| = |\boldsymbol{u}_i^*| = |\boldsymbol{w}_{i-1}^*| = |\boldsymbol{w}_i^*| = 1$ とする．(そのように仮定しても一般性を失わない.）よって，直交基底の定義より，以下の等式を示せばよい．

$$(\boldsymbol{u}_{i+1}, \boldsymbol{u}_{i-1}^*)\boldsymbol{u}_{i-1}^* + (\boldsymbol{u}_{i+1}, \boldsymbol{u}_i^*)\boldsymbol{u}_i^* = (\boldsymbol{u}_{i+1}, \boldsymbol{w}_{i-1}^*)\boldsymbol{w}_{i-1}^* + (\boldsymbol{u}_{i+1}, \boldsymbol{w}_i^*)\boldsymbol{w}_i^*. \tag{11}$$

$\boldsymbol{u}^*_{i-1}, \boldsymbol{u}^*_i, \boldsymbol{w}^*_{i-1}, \boldsymbol{w}^*_i$ の定義より，ある実数 a, b, c, d に対して，

$$\boldsymbol{w}^*_{i-1} = a\boldsymbol{u}^*_{i-1} + b\boldsymbol{u}^*_i \tag{12}$$
$$\boldsymbol{w}^*_i = c\boldsymbol{u}^*_{i-1} + d\boldsymbol{u}^*_i \tag{13}$$

問 11.13. この事実を示しなさい.

このとき，以下の条件が成り立つ.

$$(*) \cdots \begin{cases} a^2 + b^2 = 1 & \because\ |\boldsymbol{w}^*_{i-1}| = 1 \\ c^2 + d^2 = 1 & \because\ |\boldsymbol{w}^*_i| = 1 \\ ac + bd = 0 & \because\ (\boldsymbol{w}^*_{i-1}, \boldsymbol{w}^*_i) = 0 \end{cases}$$

(12), (13) を (11) の右辺に代入して，

$$\begin{aligned} & (\boldsymbol{u}_{i+1}, a\boldsymbol{u}^*_{i-1} + b\boldsymbol{u}^*_i)(a\boldsymbol{u}^*_{i-1} + b\boldsymbol{u}^*_i) + (\boldsymbol{u}_{i+1}, c\boldsymbol{u}^*_{i-1} + d\boldsymbol{u}^*_i)(c\boldsymbol{u}^*_{i-1} + d\boldsymbol{u}^*_i) \\ = \ & \big((a^2 + c^2)(\boldsymbol{u}_{i+1}, \boldsymbol{u}^*_{i-1}) + (ab + cd)(\boldsymbol{u}_{i+1}, \boldsymbol{u}^*_i)\big)\, \boldsymbol{u}^*_{i-1} \\ & + \big((ab + cd)(\boldsymbol{u}_{i+1}, \boldsymbol{u}^*_{i-1}) + (b^2 + d^2)(\boldsymbol{u}_{i+1}, \boldsymbol{u}^*_i)\big)\, \boldsymbol{u}^*_i \end{aligned}$$

(11) の左辺と比較すれば，以下を示せばよい.

$$\begin{aligned} (a^2 + c^2)(\boldsymbol{u}_{i+1}, \boldsymbol{u}^*_{i-1}) + (ab + cd)(\boldsymbol{u}_{i+1}, \boldsymbol{u}^*_i) &= (\boldsymbol{u}_{i+1}, \boldsymbol{u}^*_{i-1}) \\ (ab + cd)(\boldsymbol{u}_{i+1}, \boldsymbol{u}^*_{i-1}) + (b^2 + d^2)(\boldsymbol{u}_{i+1}, \boldsymbol{u}^*_i) &= (\boldsymbol{u}_{i+1}, \boldsymbol{u}^*_i) \end{aligned}$$

これを示すためには，以下を示せばよい.

$$\begin{aligned} a^2 + c^2 &= 1 \\ b^2 + d^2 &= 1 \\ ab + cd &= 0 \end{aligned}$$

問 11.14. これら三つの等式を示しなさい.（ヒント：条件 $(*)$ から導かれる．その条件より，(a, b), (c, d) は単位円上にあり，更に直交している．これは (a, c), (b, d) としても同様である.）

この問より，$\boldsymbol{u}^*_{i+1} = \boldsymbol{w}^*_{i+1}$ が示される.（$j \in [n] \setminus [i+1]$ のときも同様.） ■

11.3 LLL アルゴリズム

任意の $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n \in \mathbb{R}^n$ について，これらのグラム・シュミット直交基底を $\boldsymbol{u}^*_1, \ldots, \boldsymbol{u}^*_n \in \mathbb{R}^n$ とする．ここでは[15]，任意の $i, j \in [n]$（ただし $j \leq i$）について，

$$\mu_{ij} \stackrel{\text{def}}{=} \frac{(\boldsymbol{u}_i, \boldsymbol{u}^*_j)}{|\boldsymbol{u}^*_j|^2}.$$

便宜上，$j > i$ について $\mu_{ij} = 0$ と定義する.

事実 11.10. 任意の $i \in [n]$ について，

$$\boldsymbol{u}_i = \sum_{j \in [i-1]} \mu_{ij} \boldsymbol{u}^*_j + \boldsymbol{u}^*_i.$$

[15] これまでの μ_{ij} の定義と異なる.

問 11.15. この事実を示しなさい.

事実 11.11. 任意の $i \in [n]$ について $\mu_{ii} = 1$. よって，任意の $i \in [n]$ について，

$$\boldsymbol{u}_i \;=\; \sum_{j \in [i]} \mu_{ij} \boldsymbol{u}_j^*.$$

問 11.16. この事実（$\mu_{ii} = 1$）を示しなさい.

命題 11.12. 格子 $\mathcal{L}$ の最短ベクトルを $\boldsymbol{v}^*$ とする．格子が $\mathcal{L}$ となる任意の格子点 $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n \in \mathcal{L}$ について（つまり，$\mathcal{L}_u = \mathcal{L}$），そのグラム・シュミット直交基底を $\boldsymbol{u}_1^*, \ldots, \boldsymbol{u}_n^* \in \mathbb{R}^n$ とする．このとき，

$$|\boldsymbol{v}^*| \;\geq\; \min_{i \in [n]} \{|\boldsymbol{u}_i^*|\}.$$

証明. $\boldsymbol{v}^*$ は格子点であり $\mathcal{L}_u = \mathcal{L}$ であるから，ある整数 $a_1, \ldots, a_n \in \mathbb{Z}$ が存在して，$\boldsymbol{v}^* = \sum_{i \in [n]} a_i \boldsymbol{u}_i$ である．ここで，ある $k \in [n]$ に対して，$a_k \neq 0$ かつ $a_{k+1} = \cdots = a_n = 0$ であるとする．事実 11.10 より，ある実数 $b_1, \ldots, b_{k-1} \in \mathbb{R}$ に対して，

$$\boldsymbol{v}^* \;=\; \sum_{i \in [k-1]} b_i \boldsymbol{u}_i^* + \boldsymbol{u}_k^*.$$

よって，

$$|\boldsymbol{v}^*|^2 \;=\; \sum_{i \in [k-1]} b_i^2 |\boldsymbol{u}_i^*|^2 + |\boldsymbol{u}_k^*|^2 \;\geq\; |\boldsymbol{u}_k^*|^2 \;\geq\; \min_{i \in [n]} \{|\boldsymbol{u}_i^*|^2\}.$$

■

以下の条件を満たす $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n \in \mathbb{R}^n$ を**ガウス既約**という．任意の $i \in [n-1]$ について，

$$\begin{array}{lrcl} 1. & \left|\mu_{(i+1)i}\right| & \leq & 1/2 \\ 2. & |\boldsymbol{u}_i^*| & \leq & \dfrac{2}{\sqrt{3}} \left|\mu_{(i+1)i} \boldsymbol{u}_i^* + \boldsymbol{u}_{i+1}^*\right| \end{array}$$

定理 11.2. 最短ベクトル問題の近似率は $2^{(n-1)/2}$ である.

注 11.2. $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n \in \mathbb{R}^n$ の格子を $\mathcal{L}_{\boldsymbol{v}}$，ステップ 2（全体）の繰り返し後の $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n \in \mathbb{R}^n$ の格子を $\mathcal{L}_{\boldsymbol{u}}$，とする．このとき，$\mathcal{L}_{\boldsymbol{v}} = \mathcal{L}_{\boldsymbol{u}}$.（問 11.9 を参照.）

問 11.17. $n = 3$ について，三つの適当なベクトルを考案して，そのベクトルに対する図 24 のアルゴリズムの動作及び出力を示しなさい.

事実 11.13. ステップ 2-(a) の前後で直交基底 $\boldsymbol{u}_1^*, \ldots, \boldsymbol{u}_n^*$ は変わらない.

入力：ベクトル $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n \in \mathbb{R}^n$

1. 任意の $i \in [n]$ について $\boldsymbol{u}_i = \boldsymbol{v}_i$ とする．（グラム・シュミットの直交基底を $\boldsymbol{u}_i^*$ とする．）
2. $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ がガウス既約でない限り以下を繰り返す．
   (a) それぞれの $i \in [n-1]$ について，以下を繰り返す．
   - $|\mu_{(i+1)i}| > 1/2$ なら $\boldsymbol{u}_{i+1} = \boldsymbol{u}_{i+1} - \lfloor \mu_{(i+1)i} \rceil \boldsymbol{u}_i$.

   (b) ガウス既約の条件を満たさない任意の $i \in [n-1]$ 一つについて，$\boldsymbol{u}_i$ と $\boldsymbol{u}_{i+1}$ を交換する．
3. $\boldsymbol{u}_1$ を出力する．

図 24: LLL のアルゴリズム

問 11.18. この事実を示しなさい．（ステップ 2-(a) の繰り返し回数についての帰納法により示す．）

事実 11.14. ステップ 2-(a) の実行終了後，任意の $i \in [n-1]$ について $|\mu_{(i+1)i}| \leq 1/2$．（つまり，ガウス既約の一つ目の条件が満たされる．）

問 11.19. この事実を示しなさい．（事実 11.10 を用いる．）

注 11.3. この事実より，ステップ 2-(b) において，ガウス既約の条件を満たさないとは，二つ目の条件が満たされないことになる．

証明. アルゴリズムの出力を $\boldsymbol{v}$（$= \boldsymbol{u}_1$），最適解を $\boldsymbol{v}^*$ とする．近似率 $2^{(n-1)/2}$ を示すためには，$|\boldsymbol{v}| \leq 2^{(n-1)/2}|\boldsymbol{v}^*|$ を示せばよい．アルゴリズムの終了時には，$\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ はガウス既約であることから，任意の $i \in [n-1]$ について，

$$\begin{aligned} |\boldsymbol{u}_i^*|^2 &\leq \frac{4}{3}\left|\mu_{(i+1)i}\boldsymbol{u}_i^* + \boldsymbol{u}_{i+1}^*\right|^2 \\ &= \frac{4}{3}\left(\left|\mu_{(i+1)i}\boldsymbol{u}_i^*\right|^2 + \left|\boldsymbol{u}_{i+1}^*\right|^2\right) \\ &\leq \frac{4}{3}\left(\frac{1}{4}\left|\boldsymbol{u}_i^*\right|^2 + \left|\boldsymbol{u}_{i+1}^*\right|^2\right) \end{aligned}$$

よって，$|\boldsymbol{u}_i^*| \leq \sqrt{2}|\boldsymbol{u}_{i+1}^*|$．これより，

$$|\boldsymbol{u}_1^*| \leq \sqrt{2}|\boldsymbol{u}_2^*| \leq \cdots \leq (\sqrt{2})^{n-1}|\boldsymbol{u}_n^*| = 2^{(n-1)/2}|\boldsymbol{u}_n^*|.$$

よって，命題 11.12 より[16]，$|\boldsymbol{v}| = |\boldsymbol{u}_1| = |\boldsymbol{u}_1^*| \leq 2^{(n-1)/2}|\boldsymbol{v}^*|$ が示される．

[16]注 11.2 より $\mathcal{L}_u = \mathcal{L}$.

問 11.20. この事実を示しなさい.（命題 11.12 によって近似率がどのように導かれるか.）

次に計算時間を見積もる.

注 11.4. 計算時間を見積もる場合，入力ベクトル $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ の成分は有理数であるとしてよい．更に，計算時間が「入力長」の多項式であることを示すためには，それらはすべて整数であるとしてよい.（$\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n \in \mathbb{Z}^n$.）

アルゴリズムが多項式時間で終了することを示すためには，アルゴリズムのステップ 2 の繰り返し回数が（入力長の）多項式であることを示せばよい．そのために，$\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ に対する以下のような（ポテンシャル）関数 ϕ を考える[17].

$$\phi(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n) \stackrel{\text{def}}{=} \prod_{i \in [n]} |\boldsymbol{u}_i^*|^{n-i}.$$

ステップ 2 の k 回目の繰り返し直前の（$\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ に対する）ϕ を ϕ_k と表記する.

主張 11.3. 任意の k について，$(\sqrt{3}/2)\phi_k \geq \phi_{k+1}$.

証明. ステップ 2 の k, $k+1$ 回目の繰り返し直前の $(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n)$ を，それぞれ，$(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n)$, $(\boldsymbol{w}_1, \ldots, \boldsymbol{w}_n)$ とする．k 回目の繰り返しで $\boldsymbol{u}_{i-1}$ と $\boldsymbol{u}_i$ が交換されたとする．また，$\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$, $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_n$ に対するグラム・シュミット直交基底を，$(\boldsymbol{u}_1^*, \ldots, \boldsymbol{u}_n^*)$, $(\boldsymbol{w}_1^*, \ldots, \boldsymbol{w}_n^*)$ とする．事実 11.13 より，ステップ 2-(a) の前後で直交基底は変わらない．よって，命題 11.9 より，

$$\begin{aligned}
\phi_k &= |\boldsymbol{u}_1^*|^{n-1} \cdots |\boldsymbol{u}_{i-2}^*|^{n-(i-2)} \quad |\boldsymbol{u}_{i-1}^*|^{n-(i-1)} |\boldsymbol{u}_i^*|^{n-i} \quad |\boldsymbol{u}_{i+1}^*|^{n-(i+1)} \cdots |\boldsymbol{u}_n^*|^0 \\
&= |\boldsymbol{w}_1^*|^{n-1} \cdots |\boldsymbol{w}_{i-2}^*|^{n-(i-2)} \quad |\boldsymbol{w}_{i-1}^*|^{n-(i-1)} |\boldsymbol{w}_i^*|^{n-i} \frac{|\boldsymbol{u}_{i-1}^*|}{|\boldsymbol{w}_{i-1}^*|} \quad |\boldsymbol{w}_{i+1}^*|^{n-(i+1)} \cdots |\boldsymbol{u}_w^*|^0 \\
&= \frac{|\boldsymbol{u}_{i-1}^*|}{|\boldsymbol{w}_{i-1}^*|} \phi_{k+1}.
\end{aligned}$$

ここで，$\boldsymbol{u}_{i-1}$ と $\boldsymbol{u}_i$ が交換されたことから，

$$\begin{aligned}
\boldsymbol{w}_{i-1}^* &= \boldsymbol{w}_{i-1} - \sum_{j \in [i-2]} \mu_{(i-1)j} \boldsymbol{w}_j^* \\
&= \boldsymbol{u}_i - \sum_{j \in [i-2]} \mu_{ij} \boldsymbol{u}_j^* \\
&= \left(\sum_{j \in [i-1]} \mu_{ij} \boldsymbol{u}_j^* + \boldsymbol{u}_i^* \right) - \sum_{j \in [i-2]} \mu_{ij} \boldsymbol{u}_j^* \quad (\because \text{事実 11.10}) \\
&= \mu_{i(i-1)} \boldsymbol{u}_{i-1}^* + \boldsymbol{u}_i^*.
\end{aligned}$$

よって，$\boldsymbol{u}_{i-1}$ と $\boldsymbol{u}_i$ が交換されたことから，

$$|\boldsymbol{w}_{i-1}^*| = |\mu_{i(i-1)} \boldsymbol{u}_{i-1}^* + \boldsymbol{u}_i^*| \leq \frac{\sqrt{3}}{2} |\boldsymbol{u}_{i-1}^*|.$$

この不等式より，

$$\phi_k = \frac{|\boldsymbol{u}_{i-1}^*|}{|\boldsymbol{w}_{i-1}^*|} \phi_{k+1} \geq \frac{2}{\sqrt{3}} \phi_{k+1}.$$

■

[17] $\boldsymbol{u}_1^*, \ldots, \boldsymbol{u}_n^*$ は，$\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ のグラム・シュミット直交基底である.

主張 11.4. 任意の k について，$\phi_k \geq 1$.

証明. 任意の $\ell \in [n]$，任意の $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_\ell \in \mathbb{Z}^n$ について，$|\boldsymbol{u}_1^*| \cdots |\boldsymbol{u}_\ell^*| \geq 1$ を示せばよい．ただし，$\boldsymbol{u}_1^*, \ldots, \boldsymbol{u}_\ell^*$ を $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_\ell$ のグラム・シュミット直交基底とする．

問 11.21. この事実を示せば主張が証明できる理由を説明しなさい．

以下のような $\ell \times \ell$ 行列 A を考える[18]．

$$A = \begin{pmatrix} |\boldsymbol{u}_1^*| & 0 & 0 & \cdots & 0 \\ \mu_{21}|\boldsymbol{u}_1^*| & |\boldsymbol{u}_2^*| & 0 & \cdots & 0 \\ \vdots & & \ddots & & \vdots \\ \vdots & & & \ddots & 0 \\ \mu_{\ell 1}|\boldsymbol{u}_1^*| & \mu_{\ell 2}|\boldsymbol{u}_2^*| & \mu_{\ell 3}|\boldsymbol{u}_3^*| & \cdots & |\boldsymbol{u}_\ell^*| \end{pmatrix}.$$

ここで，$\det(A) = |\boldsymbol{u}_1^*| \cdots |\boldsymbol{u}_\ell^*|$．一方，任意の $i, j \in [\ell]$（$i < j$）について，

$$\begin{aligned} (\boldsymbol{u}_i, \boldsymbol{u}_j) &= \left(\sum_{a \in [i]} \mu_{ia} \boldsymbol{u}_a^*, \sum_{b \in [j]} \mu_{jb} \boldsymbol{u}_b^* \right) \\ &= \sum_{a \in [i]} \mu_{ia}^2 |\boldsymbol{u}_a^*|^2. \end{aligned}$$

ただし，$\mu_{ii} = 1$ とする．これは，A の第 i 行と第 j 行を成分ごとかけた和に等しい．よって，

$$\begin{aligned} |\boldsymbol{u}_1^*|^2 \cdots |\boldsymbol{u}_\ell^*|^2 &= \det(A)^2 \\ &= \det(AA^{\mathbf{t}}) \\ &= \det \begin{pmatrix} (\boldsymbol{u}_1, \boldsymbol{u}_1) & (\boldsymbol{u}_1, \boldsymbol{u}_2) & \cdots & (\boldsymbol{u}_1, \boldsymbol{u}_\ell) \\ (\boldsymbol{u}_2, \boldsymbol{u}_1) & (\boldsymbol{u}_2, \boldsymbol{u}_2) & \cdots & (\boldsymbol{u}_2, \boldsymbol{u}_\ell) \\ \vdots & & \ddots & \vdots \\ (\boldsymbol{u}_\ell, \boldsymbol{u}_1) & (\boldsymbol{u}_\ell, \boldsymbol{u}_2) & \cdots & (\boldsymbol{u}_\ell, \boldsymbol{u}_\ell) \end{pmatrix}. \end{aligned}$$

$\boldsymbol{u}_1, \ldots, \boldsymbol{u}_\ell \in \mathbb{Z}^n$ は整数成分である（注 11.4）ことから $(\boldsymbol{u}_i, \boldsymbol{u}_j)$ も整数となり，上の行列式の値は（0 でない）整数となる．よって，$|\boldsymbol{u}_1^*|^2 \cdots |\boldsymbol{u}_\ell^*|^2 \geq 1$ より，$|\boldsymbol{u}_1^*| \cdots |\boldsymbol{u}_\ell^*| \geq 1$ となる． ■

主張 11.5. $\phi_1 \leq (\max_i\{|\boldsymbol{v}_i|\})^{n(n-1)/2}$.

証明. 事実 11.11 より，任意の $i \in [n]$ について $|\boldsymbol{v}_i^*| \leq |\boldsymbol{v}_i|$．よって，

$$\phi_1 = \prod_{j \in [n]} |\boldsymbol{v}_j^*|^{n-j} \leq \prod_{j \in [n]} |\boldsymbol{v}_j|^{n-j} \leq \prod_{j \in [n]} (\max_i\{|\boldsymbol{v}_i|\})^{n-j} = (\max_i\{|\boldsymbol{v}_i|\})^{\frac{n(n-1)}{2}}$$

■

[18] この行列は次のように見なせる．グラム・シュミットの「正規」直交基底 $\boldsymbol{u}_1^*/|\boldsymbol{u}_1^*|, \ldots, \boldsymbol{u}_\ell^*/|\boldsymbol{u}_\ell^*|$ の一次結合を考える．事実 11.10 より，任意の $i \in [\ell]$ について，

$$\boldsymbol{u}_i = \sum_{j \in [i-1]} \left(\mu_{ij}|\boldsymbol{u}_j^*|\right) \frac{\boldsymbol{u}_j^*}{|\boldsymbol{u}_j^*|} + |\boldsymbol{u}_i^*| \frac{\boldsymbol{u}_i^*}{|\boldsymbol{u}_i^*|}.$$

行列 A の第 i 行は $\boldsymbol{u}_j^*/|\boldsymbol{u}_j^*|$ の係数となる．

これら三つの主張より，アルゴリズムのステップ 1 の繰り返し回数は，高々，

$$\frac{n(n-1)\max_i\{\log|\boldsymbol{v}_i|\}}{2\log(2/\sqrt{3})}.$$

問 11.22. この事実を示しなさい.（三つの主張によって繰り返し回数がどのように導かれるか.）

以上のことから，LLL のアルゴリズムが多項式時間で終了することが示される. ■

12　近似不可能性 *

(under construction)

13　付録

定理 13.1 (コーシー・シュワルツの不等式)**.** 二つの n 次元ベクトル $a, b \in \mathbb{R}^n$ について，$(a, b) \leq |a| \cdot |b|$，つまり，

$$\sum a_i b_i \ \leq \ \sqrt{\sum a_i^2} \cdot \sqrt{\sum b_i^2}.$$

系 13.1. n 次元ベクトル $a \in \mathbb{R}^n$ について，

$$\frac{(\sum a_i)^2}{n} \ \leq \ \sum a_i^2.$$

証明. コーシー・シュワルツの不等式において，$b = 1^n$ とすればよい. ■

命題 13.2. i, j を任意の自然数とする．$p_1, \ldots, p_i \in \mathbb{R}^+, a_1, \ldots, a_i \in \mathbb{R}^+$，$q_1, \ldots, q_j \in \mathbb{R}^+, b_1, \ldots, b_j \in \mathbb{R}^+$ を任意とする．このとき，

$$\begin{aligned} &\frac{q_j}{b_j} \leq \cdots \leq \frac{q_1}{b_1} \leq \frac{p_i}{a_i} \leq \cdots \leq \frac{p_1}{a_1} \\ &b_1 + \cdots + b_j \leq a_1 + \cdots + a_i \end{aligned}$$

ならば，

$$q_1 + \cdots + q_j \ \leq \ p_1 + \cdots + p_i.$$

証明. 背理法により示す．つまり，

$$q_1 + \cdots + q_j \ > \ p_1 + \cdots + p_i$$

と仮定する．$b_1 + \cdots + b_j \leq a_1 + \cdots + a_i$ より，

$$\frac{q_1 + \cdots + q_j}{b_1 + \cdots + b_j} \ > \ \frac{p_1 + \cdots + p_i}{a_1 + \cdots + a_i}$$

このとき，

$$\begin{aligned} \frac{q_1 + \cdots + q_j}{b_1 + \cdots + b_j} \ &\leq \ \frac{q_1}{b_1} \quad \left(\because \ \frac{q_j}{b_j} \leq \cdots \leq \frac{q_1}{b_1} \right) \\ \frac{p_1 + \cdots + p_i}{a_1 + \cdots + a_i} \ &\geq \ \frac{p_i}{a_i} \quad \left(\because \ \frac{p_i}{a_i} \leq \cdots \leq \frac{p_1}{a_1} \right) \end{aligned}$$

よって，$q_1/b_1 > p_i/a_i$ となり，$q_1/b_1 \leq p_i/a_i$ に矛盾する. ■

定理 13.2 (相加平均・相乗平均)**.** 任意の自然数 $n \in \mathbb{N}$，任意の非負実数 $a_1, \ldots, a_n$ に対して，

$$\sqrt[n]{\prod_{i \in [n]} a_i} \ \leq \ \frac{\sum_{i \in [n]} a_i}{n}.$$

事実 13.3. 任意の実数 $x \in \mathbb{R}$ に対して，$1 + x \leq e^x$.

事実 13.4. 任意の自然数 $n \in \mathbb{N}$ に対して，

$$\sum_{i \in [n]} \frac{1}{i} \ \leq \ \log n + 1.$$

定理 13.3 (期待値の線形性)**.** $Z = \sum_{i \in [n]} Z_i$ とする．このとき，$\mathrm{E}[Z] = \sum_{i \in [n]} Z_i$.