

12.2.5 補足 2 : PERMANENT の #P 完全性

PERMANENT が #P 完全であることの証明はきわめて巧妙なうえに、さまざまな興味深い意味合いもあるので、ここではそのことに触れておこう。

まず、定理 12.3 より $\text{PERMANENT} \in \mathbf{FP}$ ならば $\mathbf{P} = \mathbf{NP}$ となることから、PERMANENT が #P 完全であるという結果は 1970 年代当時、研究者たちから驚きをもって迎えられた。また、興味深いことの 1 つは、PERMANENT は、解を 1 つだけ求めることは易しいがすべての解を求めることは難しいという問題の一例になっていることである。すなわち、頂点が n 個ずつの 2 つの部からなる 2 部グラフ G において完全マッチングを 1 つ求めることは多項式時間でできるのに対し、 G の完全マッチングの個数は G の隣接行列（成分が 0, 1 だけの $n \times n$ 行列）のパーマネントに等しい（その証明には、成分を 0, 1 に限定した行列のパーマネントを計算する問題も #P 完全であることを使う）ことと、 $\mathbf{NP} \subseteq \#P$ であることから、 G の完全マッチングの個数を求めることは $\mathbf{P}$ よりもずっと難しい（と思われる）のである。

PERMANENT と密接な関係があるもう一つの問題は、有向グラフのサイクル被覆の重みの和を求める問題である（この問題を #CC で表すことにする）。重み付き有向グラフ $G = (V, E)$, $w : E \rightarrow \mathbb{Z}$ のサイクル被覆 (cycle cover) とは、頂点を共有しないようなサイクルの集合 $\mathbf{C}$ のうち G の全頂点を含むようなものである（すなわち、 $C, C' \in \mathbf{C} \implies V(C) \cap V(C') = \emptyset$ かつ $\forall v \in V \exists C \in \mathbf{C} [v \in V(C)]$ を満たす $\mathbf{C}$ 。ただし、ここではサイクルは辺の集合であるとし、その頂点の集合を $V(C)$ で表した）。また、サイクル C の重み (weight) とは C 上の辺の重みの積 $\prod_{e \in C} w(e)$ のことである。以後、 C の重みを $w(C)$ で表す。また、サイクル被覆の集合 $\mathbf{C}$ の重みを $\sum_{C \in \mathbf{C}} w(C)$ （すなわち、 $\mathbf{C}$ に属すサイクル被覆の重みの和）と定義し、これも $w(\mathbf{C})$ で表す。 $n \times n$ 整数行列 A に対し、

$$V(G_A) = \{v_1, \dots, v_n\}, \quad w(v_i, v_j) = A[i, j] \quad ((v_i, v_j) \in E(G_A))$$

と定義した有向グラフ G_A を考える。ただし、 $A[i, j]$ は A の (i, j) 成分である。

定理 12.8. (1) 任意の整数を成分とする行列 A に対し、 $\text{perm}(A)$ は G_A のすべてのサイクル被覆の重みの和に等しい。

(2) $\text{PERMANENT} \leq_T^{\text{poly}} \#CC$ かつ $\#CC \leq_T^{\text{poly}} \text{PERMANENT}$ が成り立つ。このとき、 $\text{PERMANENT} \equiv_T^{\text{poly}} \#CC$ と書くことにする。

証明 (1) A を $n \times n$ 整数行列とする。 G_A のそれぞれのサイクル被覆 C に対し、 $\{1, \dots, n\}$ の置換 σ_C を $\sigma_C(i) = j \iff (v_i, v_j) \in C$ と定義すると、 C の重みは $\prod_{1 \leq i \leq n} A[i, \sigma_C(i)]$ である。

(2) (1) より、 $\text{PERMANENT} \leq_T^{\text{poly}} \#CC$ である。逆に、辺に重み $w : E \rightarrow \mathbb{N}$ が付けられた任意の有向グラフ $G = (V, E)$, $V = \{v_1, \dots, v_n\}$ に対し、その隣接行列 A を $A[i, j] = w(v_i, v_j)$ と定義する。ただし、 $(v_i, v_j) \notin E$ の場合には $w(v_i, v_j) = 0$ とする。明らかに、 $G_A = G$ であるから $\#CC(G) = \text{perm}(A)$ であり、したがって $\#CC \leq_T^{\text{poly}} \text{PERMANENT}$ である。 $\square$

さて、PERMANENT が #P 完全であることを証明しよう。#3SAT を PERMANENT に還元したいので、次の補題が必要である。

補題 12.1. #3SAT は #P 完全である。

証明 定理 12.4 と, SAT を 3SAT へ還元した定理 9.3 の還元はどちらも充足する付値の個数を変えないことから. $\square$

定理 12.9 (L.G.Valiant (ヴァリアント) の定理). PERMANENT は #P 完全である.

証明 PERMANENT も #CC も #P に属することは容易に示すことができる.

問 12.12. PERMANENT, #CC $\in$ #P を示せ.

定理 12.8 より, #3SAT を PERMANENT に $\leq_T^{poly}$ 還元できることを示せばよい.

n 変数 $x_1, \dots, x_n$ かつ m 個の節 $C_1, \dots, C_m$ からなる 3-CNF のブール式 φ が与えられたら, 次の条件を満たす重み付き有向グラフ $G_\varphi = (V, E)$, $w: E \rightarrow \mathbb{N}$ を構成する:

(i) G_φ のサイクル被覆のうち, φ を充足する付値に対応するサイクル被覆の集合 $\mathcal{C}$ の重みの和 $w(\mathcal{C})$ は 4^{3m} であり,

(ii) G_φ の (i) 以外のサイクル被覆の重みの和は 0 である.

したがって, φ を充足する付値の個数を $\#\varphi$ とすると, G_φ の隣接行列のパーマネントは $4^{3m} \cdot \#\varphi$ である.

G_φ の構成にあたって重要な役割を演じるのは次の行列 X である:

$$X = \begin{pmatrix} 0 & 1 & -1 & -1 \\ 1 & -1 & 1 & 1 \\ 0 & 1 & 1 & 2 \\ 0 & 1 & 3 & 0 \end{pmatrix}$$

この行列 X は図 12.2.1 の左図に示したグラフ (接合ガジェットと呼ぶ) の隣接行列である (赤色で示したのは頂点の番号, 青色は辺の重みである. 重みが書いてない辺の重みは 1 である). X は次のような注目すべき性質をもっている:

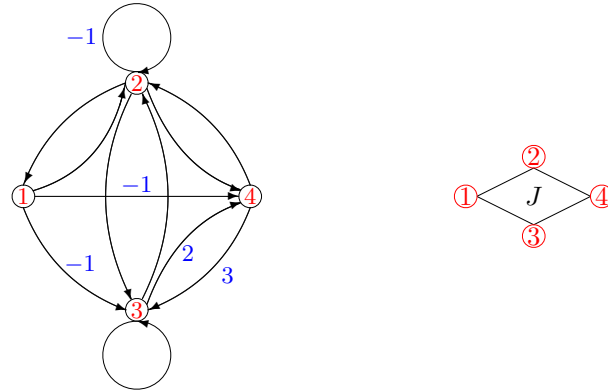
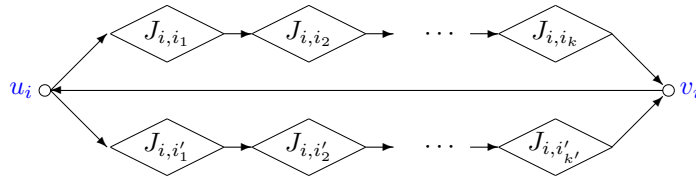
(i) (a) X 自身, (b) X の第 1 行と第 1 列を削除した行列, (c) X の第 4 行と第 4 列を削除した行列, (d) X の第 1 行と第 4 行および第 1 列と第 4 列を削除した行列, のいずれもそのパーマネントは 0 である.

(ii) (a) X の第 1 行と第 4 列を削除した行列と (b) X の第 4 行と第 1 列を削除した行列はいずれもそのパーマネントが 4 である.

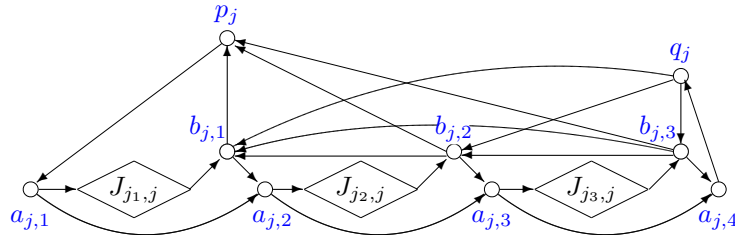
G_φ は以下で述べるように, 部品となるガジェットを組合わせて構成するが, その基となるのが接合ガジェットである.

① 接合ガジェット 変数 x_i ($1 \leq i \leq n$) が節 C_j の正リテラルあるいは負リテラルであることを接合ガジェット $J_{i,j}$ で表す (i, j が付いているが, それは他の $J_{i',j'}$ と結合するときに区別するためだけである. $J_{i,j}$ も $J_{i',j'}$ も G_φ の一部になるが, 有向グラフとしては図 12.2.1 の左図 J と同型なものである: $J_{i,j} \cong J_{i',j'} \cong J$). J の省略形を図 12.2.1 の右図に示した. このガジェット J は頂点 1 と 4 において G_φ の他の部分と一辺で接合する (頂点 1 へ入る有向辺と頂点 4 から出る有向辺).

② 変数ガジェット 変数 x_i ($1 \leq i \leq n$) には図 12.2.2 に示したようなガジェットを対応させる. このガジェットを V_i と呼ぶ. すなわち, x_i は節 $C_{i_1}, \dots, C_{i_k}$ に正リテラルとして現われ, 節 $C_{i'_1}, \dots, C_{i'_k'}$ に負リテラルとして現われる場合, V_i は頂点 u_i と v_i を含み, 図 12.2.2 に示したように有向辺で接合ガジェットたちを結んだものとする.

図 12.2.1: 接合ガジェット J (左) とその省略形 (右)図 12.2.2: 変数 x_i に対するガジェット V_i

③ 節ガジェット: 節 C_j ($1 \leq j \leq m$) に対し, 図 12.2.3 に示したようなガジェット R_j をつくる. C_j を構成している変数が $x_{j_1}, x_{j_2}, x_{j_3}$ の場合, R_j は 9 個の頂点 $p_j, q_j, a_{j,k}$ ($1 \leq k \leq 4$), $b_{j,k}$ ($1 \leq k \leq 3$) と 3 つの接合ガジェット $J_{j_k,j}$ ($1 \leq k \leq 3$) を図 12.2.3 に示したように有向辺で結んで構成する. ただし, この R_j では, 有向辺は接合ガジェットの頂点 4 から入り頂点 1 から出ているものとする (V_j の図とは接合ガジェットの左右が逆になっているので注意のこと).

図 12.2.3: 節 C_j に対するガジェット R_j

上記のガジェット①~③において, どの辺の重みも 1 であるとする. 以上で G_φ の構成を終わる. 以下で, G_φ の性質を考察する.

「接合ガジェットの外にある辺の集合が等しいようなサイクル被覆」すべてを集めたもの $\mathcal{C}$ を 順路と呼ぶことにする. $\mathcal{C}$ が G_φ の中のすべての接合ガジェットをちょうど 1 回だけ通る (頂点 1 から入って頂点 4 から出るか, あるいは頂点 4 から入って頂点 1 から出る) とき, $\mathcal{C}$ は良い順路であるといい, そうでないとき悪い順路であるということにする. 証明のキーは, 行列 X が (したがって, 接合ガジェットが) 悪い順路の重みの和が 0 になるように構成されているところにある.

C を順路とするとき, C に属すサイクル被覆すべての重みの和を $w(C)$ で表す.

性質 1 C が悪い順路ならば $w(C) = 0$ である.

$\therefore$ 定義より, C が悪い順路であるのは次のいずれかが成り立つときである.

- (a) どの接合ガジェット J にも入っていない.
- (b) 接合ガジェット J にちょうど 1 回だけ頂点 1 から入り頂点 4 から出ている.
- (c) 接合ガジェット J にちょうど 1 回だけ頂点 4 から入り頂点 1 から出ている.
- (d) 接合ガジェット J に 2 回入っている.

いずれの場合にも, 行列 X の性質 (i) より, J を被覆する局所サイクル (C の部分サイクル) の重みは 0 である. 例えば, (b) の場合を考えよう. この場合, J の構成の仕方より, C のすべてのサイクル被覆は J の頂点 4 から出る (または, 頂点 2, 3 で終わる) しかない. これには J の頂点 1 を削除した部分グラフのサイクル被覆が対応するが, その重みの和は 0 である. (b) は行列 X の第 1 行と第 1 列を削除したグラフのサイクル被覆に対応する (X の削除条件 (i) の (b) がこれにあたる). 同様に, (a), (c), (d) の場合は X の削除条件 (i) の (a), (c), (d) がそれぞれ対応する.

性質 2 C が良い順路ならば $w(C) = 4^{3m}$ である.

$\therefore G_\varphi$ は全部で $3m$ 個の接合ガジェットを含んでいる. それぞれの接合ガジェット J に対し, C は J に頂点 1 から入って頂点 4 から出る (そのあと, J の外側の道を経て頂点 1 に戻ってくる) か, あるいは頂点 4 に入って頂点 1 から出る (そのあと, J の外側の道を経て頂点 4 に戻ってくる). 前者の場合, J を被覆する C のサイクル被覆は 6 通りあり (問 1), これらには X の第 4 行と第 1 列を削除した行列のパーマネントである値 4 が対応する (問 2). 同様に, 後者の場合は X の第 1 行と第 4 列を削除した行列のパーマネントである値 4 が対応する. よって, これらを合わせた重みは 4^{3m} である (サイクルの重みはサイクル上の辺の重みの積であったことを思い出されたい).

問 12.13. (1) 上記の問 1 を説明せよ (ヒント: X の第 4 行と第 1 列を削除した行列のパーマネントの積項とサイクルとの対応を考えよ. ただし, サイクルとはいってはいるが, 実際はサイクルの J 内の部分だけである).

(2) 上記の問 2: サイクルの J 内の部分の重みの和, および対応する行列のパーマネントを具体的に計算せよ.

性質 3 R_j ($1 \leq j \leq m$) は次の性質を満たす.

(1) R_j に対する良い順路は存在しない.

(2) R_j から $J_{j,k,j}$ ($1 \leq k \leq 3$) の中の少なくとも 1 つを削除したものを R'_j とすると, R'_j に対する良い順路が唯一つ存在する.

$\therefore$ 図 12.2.3 をよく観察すると, R_j が次の 1~6. を満たすことを容易に確かめることができる.

1. R_j や R'_j に対する良い順路は頂点 $p_j, a_{j,1}, a_{j,2}, a_{j,3}, a_{j,4}, q_j$ を通る大きなサイクルを含んでいなければならない.

2. この大きなサイクルが R_j の中の $J_{j,k,j}$ を被覆しているとする, それは $a_{j,k} \rightarrow J_{j,k,j} \rightarrow b_{j,k}$ と経由する道を通っていないといけない.

3. この大きなサイクルの q_j から p_j への道は $b_{j,k}$ ($1 \leq k \leq 3$) の中の 1 つ以上の頂点を通っていないといけない.

4. 一方, $a_{j,1}$ から $a_{j,4}$ への道は 3 つの $J_{j,k,j}$ ($1 \leq k \leq 3$) のすべてを被覆していなければならない. したがって, $b_{j,k}$ ($1 \leq k \leq 3$) のすべてを通らなければならない.

5. これは、1. の大きなサイクルは q_j から p_j へ行く道を選ぶことができないという矛盾を導く。よって、 R_j に対する良い順路はない。

一方、 R'_j については、 $a_{j,1}$ から $a_{j,4}$ への道は $b_{j,k}$ ($1 \leq k \leq 3$) の中の少なくとも 1 つを通らない (削除されているので通れない) から、それを q_j から p_j への道に利用すれば R'_j に対する良い順路が得られる。

6. 最後に、 R'_j に対するこの良い順路は 1. の大きなサイクルによって一意的に定まることに注意する。

性質 4 G_φ 全体に対する良い順路の個数は $\#\varphi$ である ($\#\varphi$ は φ に対する付値の個数であったことを思い出されたい)。

$\therefore$ 良い順路はどれも変数ガジェット V_i ($1 \leq i \leq n$) を正のサイクル (u_i から v_i へ向かう道をたどるサイクル) または負のサイクル (v_i から u_i へ向かう道をたどるサイクル) によって被覆しているはずである (この両方のサイクルとも各 $J_{i,j}$ に頂点 1 から入り頂点 4 から出ている)。したがって、これはブール変数 x_i に対する付値を表しているとみなすことができる。上記の性質 3 より、 G_φ に対する良い順路は V_{j_k} に対するサイクルによって各 R_j の中の少なくとも 1 つの $J_{j_k,j}$ を被覆している。換言すると、それに対応する付値は節 C_j の少なくとも 1 つのリテラルを 1 (=true) にする。すなわち C_j は充足可能である。また、逆も成り立つ、

以上の議論より、 G のすべてのサイクル被覆の重みの和は $4^{3m} \cdot \#\varphi$ に等しいことが示された。 $\square$

系 12.1. $\#\text{CC}$ は $\#\text{P}$ 完全である。 $\square$

ところで、パーマメントの計算は行列の成分を 0, 1 に制限しても $\#\text{P}$ 完全のままである：

定理 12.10. 成分が 0, 1 の行列に対する PERMANENT も $\#\text{P}$ 完全である。

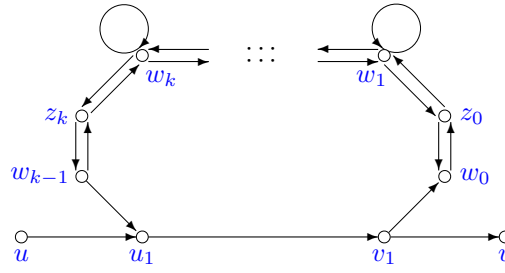
証明 まず、 n 次正方行列 A と任意の素数 $p < n^2$ に対して、 $\text{perm}(A) \bmod p$ の計算も $\#\text{P}$ 完全であることを証明しよう。

定理 12.9 では、成分が $-1, 0, 1, 2, 3$ である行列のパーマメントの計算が $\#\text{P}$ 完全であることを証明した。そのような行列 A では $|\text{perm}(A)| \leq 3^n \cdot n!$ である。素数定理¹⁸より、 n^2 以下の素数すべての積が $3^n \cdot n!$ よりも大きくなる n が存在する ($\rightarrow$ 問)。また、中国の剰余定理により、 $p_i < n^2$ であるような素数 p_i たちについての連立合同式 $\text{perm}(A) \bmod p_i$ から $\text{perm}(A)$ を多項式時間で求めることができる (第 I 巻第 10 章の 10.4.3 項を参照せよ)。よって、 $\text{perm}(A)$ の計算は $\text{perm}(A) \bmod p$ ($p < n^2$) の計算に還元することができる。

問 12.14. 上記の問を示せ。

次に、 $\text{perm}(A) \bmod p$ ($p < n^2$) の計算を成分が 0, 1 である行列 B の $\text{perm}(B)$ の計算に還元する。定理 12.8 で述べた PERMANENT と $\#\text{CC}$ の間の還元を思い出されたい。隣接行列が A であるような有向グラフを G_A とする。 $\text{perm}(A) \bmod p$ を計算したいのだから、 G_A の各辺 e の重み w は $0 \leq w(e) \leq p-1$ であると仮定してもよい (なぜか?)。 G_A の辺 $e = uv$ のうち、 $k := w(e) \notin \{0, 1\}$ であるものすべてを図 12.2.5 に示した有向グラフ H_k で置き換える。 H_k の各辺の重みは 1 とする。

¹⁸ 1 から n までの整数の中にある素数の個数を $\pi(n)$ とすると $\lim_{n \rightarrow \infty} \frac{\pi(n) \log n}{n} = 1$ が成り立つ。よって、 $\pi(n) \log n = \Theta(n)$ である。

図 12.2.4: 有向グラフ H_k

一般に、有向グラフ G の辺 $e := (u, v)$ で重みが k であるものを H_k で置き換えたものを G' とすると、 G の任意のサイクル被覆 C で e を含んでいないものに対し、 G' のサイクル被覆 C' で $C \subseteq C'$ かつ $H_k - \{u, v\}$ に対する唯一のサイクル被覆も含むようなものが唯一だけ存在する。 G の任意のサイクル被覆 C で e を含んでいるものに対しては、 $C - \{u, v\}$ に道 $u \rightarrow u_1 \rightarrow v_1 \rightarrow v$ を足したサイクルと、 $H_k - \{u, u_1, v_1, v\}$ のサイクル被覆の 1 つを含むような k 個のサイクル被覆 $C_1, \dots, C_k$ が存在する。したがって、 $\#CC(G) = \#CC(G')$ である。

そこで、 G_A の辺で重みが $k > 1$ であるものすべてを H_k で置き換えて得られる有向グラフを $G_{0,1}$ とすると、 $G_{0,1}$ の辺の重みはどれも 0 か 1 であり、かつ $\#CC(G_A) = \#CC(G_{0,1})$ である。□

$G = (V_1, V_2, E)$ を $V_1 = V_2 = \{v_1, \dots, v_n\}$ を部とする 2 部グラフとする。成分が 0, 1 の行列 A_G を

$$A_G[i, j] = \begin{cases} 1 & ((v_i, v_j) \in E \text{ のとき}) \\ 0 & (\text{その他}) \end{cases}$$

と定義する。明らかに、 $\text{perm}(A_G)$ は G の完全マッチングの個数に等しい。よって、定理 12.10 より、本項の冒頭で述べた次の系が得られる。

系 12.2. 2 部グラフの完全マッチングの個数を求める問題は $\#P$ 完全である。□