計算量理論特論 1 レポート課題

251903014 社会情報学専攻 川嶋 康太

2019 年 12 月 2 日

序文

本文書は，名古屋大学情報学研究科における，２０１９年春学期 1 期の授業科目「計算量理論特論 1 」のレポート課題の回答用紙である．

課題における問題の直接の回答となる箇所は「定理」という形で述べられている．必要に応じて定義や事実，補題を補いながら課題の回答を進めていくため，一見どこに回答があるのかわからなくなる．そのため，この序文を設けた．

なお，選択問題では「問題 B」を選択した．また，参考文献は文書の最後にまとめた．

1　必須問題

必須問題として「MAX 2SAT」「単純最大カット問題」の 2 つを取り上げた．なお，この「単純最大カット問題」への帰着を通していくつかの問題が NP 完全であるということを示せる（例えば，以下で取り上げた「同じサイズの部分集合への最小カット問題」などがある）．

定義 1.1 MAX 2SAT

MAX 2SAT とは，以下のような問題である．

入力：リテラル数が高々 2 であるような節の集合 $\{C_1, ..., C_P\}$，および $1 \leq k < p$ を満たす自然数 k

出力：k 個以上の節が充足されるような真理値割り当てが存在するか？

この MAX 2SAT が NP 完全であることを示すために，以下の事実を用いる．

事実 1.2

3SAT は NP 完全である．

定理 1.3 必須問題 – 回答$_1$ **[1]**

MAX 2SAT は NP 完全である．

Proof. 示すべきことは，MAX 2SAT が NP のクラスに属することと，NP 困難であることの二つである．まず，NP のクラスに属することを示す．少なくとも k 個の節が充足されるような真理値割り当てが与えられたとする．この時，各節が与えられた真理値割り当てによって真となるか偽となるかは，節のリテラル数が 2 なので，容易に確かめることができる．確かめた節が真ならば，その都度カウントするようにし，真となる節が確かめた中でいくつあるかわかるようにする．以下これを繰り返す．このようにアルゴリズムを組めば，明ら

かに多項式時間内に判定可能である．ゆえに，NP クラスに属する．

次に，NP 困難であることを示す．事実 1.2 を用いれば，3SAT に帰着することを示すだけで十分である．つまり，3SAT の与えられたインスタンスから，MAX 2SAT のインスタンスを構成し，3SAT の出力条件を満たす真理値割り当てを，新たに構成したインスタンスに関して，MAX 2SAT の出力条件を満たすものに拡張しうることを示し，その必要十分性を言えば良い．

$S = \{C_1, ..., C_m\}$ を 3SAT のインスタンスとする．この時，任意の $i(1 \leq i \leq m)$ について，節 C_i はリテラル x_i, y_i, z_i の和で表すことができる．よって，S から MAX 2SAT のインスタンス S' を以下のように構成することができる：

S における任意の C_i について，S' における節の群 C'_i を

$$C'_i = \{w_i, x_i, y_i, z_i, \neg x_i \vee \neg y_i, \neg y_i \vee \neg z_i, \neg z_i \vee \neg x_i, \neg w_i \vee x_i, \neg w_i \vee y_i, \neg w_i \vee z_i\}$$

とし，$k = 7m$ とする．なお，w_i は変数である．

上のように定義された S' の節は，いずれも高々リテラル数が 2 であるので，構成は well-defined である．また，このようにして S の節から S' の節を生成するのにかかる時間は，構成の仕方から明らかに多項式時間内に収まる．

最後に，3SAT の出力条件を満たす真理値割り当てを，新たに構成したインスタンスに関して，MAX 2SAT の出力条件を満たすものに拡張しうることと，その必要十分性を示す．

$(\Rightarrow)$: S が 3SAT の出力条件を満たすとする．この時，任意の節 C_i を構成するリテラル x_i, y_i, z_i は 1 つ，2 つ，もしくは全てが真である．ゆえ，この 3 つの場合に分けて考えていく：

(case1 : $x_i = T, y_i = F, z_i = F$) : この時，$w_i = T$ なら C'_i の 6 個の節が真となり，$w_i = F$ なら 7 個の節が真となる（単なる真理値計算は省略する）．

(case2 : $x_i = T, y_i = T, z_i = F$) : この時，$w_i = T$ であっても，$w_i = F$ であっても 7 個の節が真となる．

(case3 : $x_i = T, y_i = T, z_i = T$) : この時，$w_i = T$ なら C'_i の 7 個の節が真となり，$w_i = F$ なら 6 個の節が真となる．

以上の結果より，新たに追加する変数を適切に定めれば，C'_i の節の内，ちょうど 7 個が真となることがわかる．つまり，$k = 7m$ と定めているので，MAX 2SAT の出力条件を満たしているということである．よって，3SAT の出力条件を満たす真理値割り当てを，MAX 2SAT の出力条件を満たすものに拡張することができると言える．

$(\Leftarrow)$: 対偶を示す．つまり，S が条件を満たさないときには S' も条件を満たさないことを示す．S を条件を満たさないと仮定する．この時，S における少なくとも一つの節 C_i を構成するリテラル x_i, y_i, z_i は全て偽である．つまり，$x_i = F, y_i = F, z_i = F$ を得る．この真理値割り当てのもとで，S' の節の群 C'_i の節は $w_i = T$ の場合 4 個，$w_i = F$ の場合 6 個の節が真となる．よって，(case1〜3) の結果も考慮に入れると，S' の充足する節は $K = 7m$ に達し得ない．ゆえに，S' は条件を満たさない．

ゆえに，MAX 2SAT は NP 困難である．従って，NP 完全である． □

定義 1.4 最大カット問題

最大カット問題とは，以下のような問題である．

入力：グラフ $G = (N, A)$ と重み関数 $w : A \to Z$(Z は非負整数の集合) と正数 W

出力：$\sum_{\{u,v\} \in A, u \in S, v \in (N-S)} w(\{u, v\}) \geq W$ を満たす N の部分集合 S は存在するか？

事実 1.5 Karp [5]

最大カット問題は NP 完全である．

この「最大カット問題」を単純にした問題である「単純最大カット問題」も同様に NP 完全であるということが知られている．

定義 1.6 単純最大カット問題

単純最大カット問題とは，以下のような問題である．

入力：グラフ $G = (N, A)$ と正数 W

出力：$\sum_{\{u,v\}\in A, u\in S, v\in(N-S)}(1) \geq W$ を満たす N の部分集合 S は存在するか？

定理 1.7 必須問題 − 回答$_2$ **[2]**

単純最大カット問題は NP 完全である．

Proof. 定理 1.3 と事実 1.4 より，MAX 2SAT に帰着することを示すだけで十分である． MAX 2SAT の入力として節 $C_1, C_2, ..., C_p$ と整数 k が与えられたとする．この時，それぞれの節がちょうど 2 つのリテラルを含むと仮定することができる．なぜなら，リテラルを 1 つしか持たない節は同じリテラルの和 (つまり 2 つのリテラルを持つ) と表現することができるからである．そして，それら節を以下のようにラベル付けする：

$$(a_1 \vee b_1), (a_2 \vee b_2), ..., (a_p \vee b_p)$$

さらに，これらの節は全て異なると仮定することもできる．なぜなら，仮に必ずしも異なるとは限らない節 $C'_1, C'_2, ..., C'_q$ と整数 k' が与えられた時には，これと同値の全ての節が異なっているような入力を次のように置き換え手順を踏むことによって得られるからである．つまり，それぞれの節 $C'_i = (u_i \vee v_i)$ を 2 つの節 $(u_i \vee c_i)$ と $(v_i \vee \neg c_i)$ によって置き換え，k を $k + q$ に置き換えれば良いということである．

上記のような MAX 2SAT の入力に対して，単純最大カット問題の入力となるグラフ G を二つの手順を踏んで構成する．すなわち，まずはじめに，G のノード集合と一部のエッジの集合を定め，その後で，出力条件を満たすのに不足しているエッジを追加するという仕方で構成する．

$x_1, ..., x_k (1 \leq k \leq p)$ を与えられた p 個の節に現れている変数とする（ただし，それぞれの変数が属する節はそれぞれ異なる節であるとする）．この時，グラフ G に対するノードの集合 N を以下のように定める：

$$\begin{aligned} N = \{T_i : 0 \leq i \leq 3p\} \cup \{F_i : 0 \leq i \leq 3p\} \cup \{t_{ij} : 1 \leq i \leq n, 0 \leq j \leq 3p\} \cup \{f_{ij} : 1 \leq i \leq n, 0 \leq j \leq 3p\} \\ \cup \{x_i : 1 \leq i \leq n\} \cup \{\neg x_i : 1 \leq i \leq n\} \end{aligned}$$

一部のエッジの集合 A_1 は以下のように定める：

$$\begin{aligned} A_1 = \{\{T_i, F_j\} : 0 \leq i \leq 3p, 0 \leq j \leq 3p\} \cup \{\{t_{ij}, f_{ij}\} : 1 \leq i \leq n, 0 \leq j \leq 3p\} \\ \cup \{\{x_i, f_{ij}\} : 1 \leq i \leq n, 0 \leq j \leq 3p\} \\ \cup \{\{\neg x_i, t_{ij}\} : 1 \leq i \leq n, 0 \leq j \leq 3p\} \end{aligned}$$

ここで，任意の分割 $N = S_1 \cup S_2, S_1 \cap S_2 = \emptyset$ に対して，エッジ $\{u, v\}$ におけるノード u, v がどちらも同じ分割集合に属する場合，そのエッジ $\{u, v\}$ を「悪エッジ」と言い，そうでない場合を「良エッジ」ということにする．この時，以下の二つの条件 (a) と (b) を満たす任意の分割 $N = S_1 \cup S_2$ に対して，A_1 における全てのエッジが「悪エッジ」となることが A_1 の構成の仕方から明らかに成り立つ：

(a) 全ての T_i が同じ分割集合に属し，全ての F_i がもう一方に属する

(b) 各 i に対して，x_i と全ての t_{ij} が同じ分割集合に属し，$\neg x_i$ と全ての f_{ij} がもう一方に属する

さらに，任意の組 F_i, F_j が異なる分割集合に属するなら，A_1 に属する少なくとも $3p+1$ 個のエッジは「悪エッジ」である．なぜなら，x_i と $\neg x_i$ の間に $3p+1$ 個の異なる 3-エッジ のパスが存在するからである．

次に，G のエッジの集合に追加するエッジの集合 A_2 を以下のように定める：

$$A_2 = \{\{a_i, b_i\} : 1 \leq i \leq p, a_i \neq b_i\} \cup \{\{a_i, F_{2i-1}\} : 1 \leq i \leq p\} \cup \{\{b_i, F_{2i}\} : 1 \leq i \leq p\}$$

ここで，単純最大カット問題としての入力をグラフ $G = (N, A_1 \cup A_2)$ と正数 $W = |A_1| + 2k$ とする．明らかに入力として well-defined である．また，この構成は構成の仕方から明らかに多項式時間内に収まる．さらに，「良エッジ」の定義から，出力の問いは「(良エッジの数) $\geq W$ となる分割が存在するか？」と同値であると分かる．

最後に，MAX 2SAT の出力が yes となるような真理値割り当てが与えられた時，上記の構成によって定まるグラフ G と正数 W による入力により，単純最大カット問題の出力が yes となることと，その必要十分性を示す．

($\Rightarrow$) : MAX 2SAT の入力として，k もしくはそれ以上の節を充足するような n 個の変数に対する真理値割り当てが与えられたとする．この時，分割 $N = S_1 \cup S_2$ を以下のように構成する：

$$\begin{aligned} S_1 = \{F_i : 0 \leq i \leq 3p\} &\cup \{x_i : x_i = F, 1 \leq i \leq n\} \\ &\cup \{t_{ij} : x_i = F, 1 \leq i \leq n, 0 \leq j \leq 3p\} \\ &\cup \{\neg x_i : x_i = T, 1 \leq i \leq n\} \\ &\cup \{f_{ij} : x_i = T, 1 \leq i \leq n, 0 \leq j \leq 3p\} \end{aligned}$$

$$S_2 = N - S_1$$

この時，任意の充足している節に対して，リテラル a_i, b_i の一方，もしくは両方が S_2 に属しているので，その節によって定まる A_2 におけるちょうど 2 つのエッジは「良エッジ」でなければならない．さらに，この分割が条件 (a)(b) を満たすので，前述の議論により A_1 の全てのエッジは「良エッジ」である．従って，少なくとも $W = |A_1| + 2k$ 個の「良エッジ」を得る．よって，この分割によって単純最大カット問題の出力は yes となる．

($\Leftarrow$) : まず，W かそれ以上の「良エッジ」が存在する分割 $N = S_1 \cup S_2$ が与えられたとする．この時，$k > 0$ かつ $|A_2| \leq 3p$ なので，「悪エッジ」の数は $3p$ を超えることはありえない．前述の議論により，これは全ての F_i が同じ分割集合 S_1 に属することを含意する．同じ理由により，組 $x_1, \neg x_i$ のちょうどどちらか一方が S_1 に属する．ここで，真理値割り当て V を以下のように定義する：

$$x_i = T \iff x_i \in S_2$$

この V の定義は上記の議論により well-defined である．ゆえ，真理値割り当て V の定義から，節 C_i は a_i, b_i のどちらか一方かもしくは両方が S_2 に属する時に充足すると分かる．さらに，a_i, b_i のどちらか一方，もしくは両方が S_2 に属する時，節 C_i によって定まる A_2 におけるエッジのちょうど 2 個が「良エッジ」となり，a_i も b_i も S_1 に属する時，「良エッジ」は 0 個となる，ということは容易にチェックすることができる．それゆえ，A_2 に属する少なくとも $2k$ 個のエッジは「良エッジ」でなければならない．よって，「良エッジ」の定義より，少なくとも k 個の変数は S_2 に属し，変数 x_i の取り方により少なくとも k 個の節は充足すると分かる．よって，MAX 2SAT の出力は yes となる．

ゆえに，単純最大カット問題は MAX 2SAT に帰着する．従って，単純最大カット問題は NP 完全である． □

定義 1.8 同じサイズの部分集合への最小カット問題

同じサイズの部分集合への最小カット問題とは，以下のような問題である．

入力：グラフ $G=(N,A)$ と二つの異なるノード s,t と正数 W

出力：$S_1 \cap S_2 = \emptyset, |S_1| = |S_2|, s \in S_1, t \in S_2, |\{\{u,v\} \in A : u \in S_1, v \in S_2\}| \leq W$ を満たすような分割 $N = S_1 \cup S_2$ が存在するか？

定理 1.9 必須問題 – 回答$_3$ [2]

同じサイズの部分集合への最小カット問題は NP 完全である．

Proof. 単純最大カット問題への帰着から示せる．詳しくは省略する． □

2 選択問題 (B)

まずはじめに，選択問題 (B) を解くに当たって，クラス $\sum_k$，$\prod_k$ を定義するが，授業プリントにおける定義とはいくらか異なる．しかし，授業プリント定理 15 を介してそれら定義は授業プリントに書かれているものと同値であることが示せる（詳細は省略）．なお，各定義は [3] を参照にした．また，問題 (i) は [3] を問題 (ii) は [3][4] を参照し解き進めた（問題 (ii) は二通りの方法で証明した）．問題を解くのに必要な補題にも証明を与えた．

定義 2.1 クラス $\sum_k$

ある自然数 k に対して，決定問題 $S \subseteq \{0,1\}^*$ がクラス $\sum_k$ に属するとは，以下の条件を満たすような，ある多項式 p と多項式時間アルゴリズム V が存在することである：

$$x \in S \iff \exists y_1 \in \{0,1\}^{p(|x|)} \forall y_2 \in \{0,1\}^{p(|x|)} ... Q_k y_k \in \{0,1\}^{p(|x|)} [V(x, y_1, ..., y_k) = 1]$$

ここで，Q_k は k が奇数なら存在量化子，偶数なら全称量化子であるとする．

定義 2.2 クラス $\prod_k$

ある自然数 k に対して，決定問題 $S \subseteq \{0,1\}^*$ がクラス $\prod_k$ に属するとは，以下の条件を満たすような，ある多項式 p と多項式時間アルゴリズム V が存在することである：

$$x \in S \iff \forall y_1 \in \{0,1\}^{p(|x|)} \exists y_2 \in \{0,1\}^{p(|x|)} ... Q_k y_k \in \{0,1\}^{p(|x|)} [V(x, y_1, ..., y_k) = 1]$$

ここで，Q_k は k が奇数なら全称量化子，偶数なら存在量化子であるとする．

補題 2.3 重要

任意の $k \geq 0$ に対して，以下の主張 (1)(2) は同値である：

(1) 集合 S が $\sum_{k+1}$ に属する．

(2) $S = \{x : \exists y \in \{0,1\}^{p(|x|)} [(x,y) \in S']\}$ を満たすような多項式 p と集合 $S' \in \prod_k$ が存在する．

Proof. ((1)⇒(2)) : $S \in \sum_{k+1}$ とし，これに関連した多項式と多項式時間アルゴリズムをそれぞれ p, V とする．つまり，以下が成立しているとする：

$$x \in S \iff \exists z_0 \in \{0,1\}^{p(|x|)} \forall z_1 \in \{0,1\}^{p(|x|)} \exists z_2 \in \{0,1\}^{p(|x|)} ... Q_k z_k \in \{0,1\}^{p(|x|)} [V(x, z_0, z_1, ..., z_k) = 1]$$

この時，集合 S' を以下のように定義する：

$$S' = \{(x,y) : |y| = p(|x|) \,\&\, \forall z_1 \in \{0,1\}^{p(|x|)} \exists z_2 \in \{0,1\}^{p(|x|)} ... Q_k z_k \in \{0,1\}^{p(|x|)} [V(x,y,z_1,...,z_k) = 1]\}$$

ゆえ，以下が成立する：

$$\begin{aligned} x \in S &\iff \exists z_0 \in \{0,1\}^{p(|x|)} \forall z_1 \in \{0,1\}^{p(|x|)} \exists z_2 \in \{0,1\}^{p(|x|)} ... Q_k z_k \in \{0,1\}^{p(|x|)} [V(x,z_0,z_1,...,z_k) = 1] \\ &\iff \exists y \in \{0,1\}^{p(|x|)} [|y| = p(|x|) \,\&\, \forall z_1 \in \{0,1\}^{p(|x|)} \exists z_2 \in \{0,1\}^{p(|x|)} ... Q_k z_k \in \{0,1\}^{p(|x|)} [V(x,y,z_1,...,z_k) = 1]] \\ &\iff \exists y \in \{0,1\}^{p(|x|)} [(x,y) \in S'] \end{aligned}$$

ゆえ，多項式 p と集合 S' は $S = \{x : \exists y \in \{0,1\}^{p(|x|)} [(x,y) \in S']\}$ を満たす．また，$S' \in \prod_k$ となる．なぜなら，$p'(|(x,y)|) = p(|x|)$，$V'((x,y),z_1,...,z_k) \iff V(x,y,z_1,...,z_k)$ と多項式 p' と多項式時間アルゴリズム V' を定義すれば，以下が明らかに成立するからである：

$$(x,y) \in S' \iff \forall z_1 \in \{0,1\}^{p'(|(x,y)|)} \exists z_2 \in \{0,1\}^{p'(|(x,y)|)} ... Q_k z_k \in \{0,1\}^{p'(|(x,y)|)} [V'((x,y),z_1,...,z_k) = 1]]$$

((2)⇒(1))：ある多項式 p と集合 $S' \in \prod_k$ に対して，$S = \{x : \exists y \in \{0,1\}^{p(|x|)} [(x,y) \in S']\}$ が成り立つと仮定する．また，$S' \in \prod_k$ に関連した多項式と多項式時間アルゴリズムをそれぞれ p', V' とする．この時，以下のことが成立する：

$$\begin{aligned} (x,y) \in S' &\iff |y| = p(|x|) \,\&\, \forall z_1 \in \{0,1\}^{p'(|(x,y)|)} \exists z_2 \in \{0,1\}^{p'(|(x,y)|)} ... Q_k z_k \in \{0,1\}^{p'(|(x,y)|)} [V'((x,y),z_1,...,z_k) = 1] \\ &\iff |y| = p(|x|) \,\&\, \forall z_1 \in \{0,1\}^{p''(|(x)|)} \exists z_2 \in \{0,1\}^{p''(|(x)|)} ... Q_k z_k \in \{0,1\}^{p''(|(x)|)} [V(x,y,z_1,...,z_k) = 1] \end{aligned}$$

なお，最後の変形では，$p''(|x|) = p'(|(x,y)|)$,$V(x,y,z_1,...,z_k) \iff V'((x,y),z_1,...,z_k)$ と多項式 p'' と多項式時間アルゴリズム V を新たに定義している．よって，上の諸々の結果を踏まえると以下が成立する：

$$\begin{aligned} x \in S &\iff \exists y \in \{0,1\}^{p(|x|)} [(x,y) \in S'] \\ &\iff \exists y \in \{0,1\}^{p(|x|)} [|y| = p(|x|) \,\&\, \forall z_1 \in \{0,1\}^{p''(|(x)|)} \exists z_2 \in \{0,1\}^{p''(|(x)|)} ... Q_k z_k \in \{0,1\}^{p''(|(x)|)} [V(x,y,z_1,...,z_k) = 1]] \\ &\iff \exists y \in \{0,1\}^{p(|x|)} \forall z_1 \in \{0,1\}^{p''(|(x)|)} \exists z_2 \in \{0,1\}^{p''(|(x)|)} ... Q_k z_k \in \{0,1\}^{p''(|(x)|)} [V(x,y,z_1,...,z_k) = 1] \\ &\iff \exists u_0 \in \{0,1\}^{\bar{p}(|x|)} \forall u_1 \in \{0,1\}^{\bar{p}(|(x)|)} \exists u_2 \in \{0,1\}^{\bar{p}(|(x)|)} ... Q_k u_k \in \{0,1\}^{\bar{p}(|(x)|)} [\bar{V}(x,u_0,u_1,...,u_k) = 1] \end{aligned}$$

なお，最後の式変形の際に登場する $\bar{p}$ は $\bar{p}(|x|) = \max(p(|x|), p''(|x|))$ で定義される多項式で，変数 $u_0,...,u_k$ は以下のようにエンコーディングすることによって新たに定義される変数である：

$$\begin{aligned} &(p(|x|) \leq p''(|x|) \text{ の時}): && u_0 = (y,0,...,0) && \text{(ただし，0 は } p''(|x|) - p(|x|) \text{ 個である)} \\ & && u_i = z_i (1 \leq i \leq k) && \\ &(p''(|x|) \leq p(|x|) \text{ の時}): && u_0 = y && \\ & && u_i = (z_i,0,...,0) (1 \leq i \leq k) && \text{(ただし，0 は } p(|x|) - p''(|x|) \text{ 個である)} \end{aligned}$$

また，$\bar{V}$ は $\bar{V}(x,u_0,u_1,...,u_k) \iff V(x,y,z_1,...,z_k)$ と定義される多項式時間アルゴリズムのことである．

以上の結果より，多項式 $\bar{p}$ と多項式時間アルゴリズム $\bar{V}$ は $S \in \sum_{k+1}$ であるための条件を満たすと分かる．よって $S \in \sum_{k+1}$ である．

以上により，証明が完了した． □

定理 2.4 問題 (i)-回答

ある $k \geq 1$ に対して，$\sum_k = \prod_k$ が成り立つとする．この時，全ての $m \geq k$ に対して，$\sum_m = \prod_m = \sum_k$ が成り立つ．

Proof. $\sum_k = \prod_k$ が成り立つと仮定する．この時，$\sum_{k+1} = \sum_k$ と $\prod_{k+1} = \prod_k$ が成り立つことを示せば十分である．なぜならば，もしこれらが示されたならば，仮定より $\sum_{k+1} = \prod_{k+1} = \sum_k$ となり，同様にして $\sum_{k+2} = \sum_{k+1}$ と $\prod_{k+2} = \prod_{k+1}$ が示せ，$\sum_{k+2} = \prod_{k+2} = \sum_k$ を得られる．よって帰納的に，全ての $m \geq k$ に対して，$\sum_m = \prod_m = \sum_k$ を得られるからである．

まず，仮定のもとで $\sum_{k+1} = \sum_k$ が成り立つことを示す．任意の $S \in \sum_{k+1}$ に対して，補題 2.3 より，$S = \{x : \exists y \in \{0,1\}^{p(|x|)}[(x,y) \in S']\}$ を満たすような多項式 p と集合 $S' \in \prod_k$ が存在すると分かる．さらに，仮定より $S' \in \sum_k$ を得る．そして，再び補題 2.3 と $k \geq 1$ であるという条件から，$S' = \{x' : \exists y' \in \{0,1\}^{p'(|x'|)}[(x',y') \in S'']\}$ を満たすような多項式 p' と集合 $S'' \in \prod_{k-1}$ が存在すると分かる．よって，以下が成立する：

$$
\begin{aligned}
S =& \{x : \exists y \in \{0,1\}^{p(|x|)}[(x,y) \in S']\} \\
=& \{x : \exists y \in \{0,1\}^{p(|x|)}[(x,y) \in \{x' : \exists y' \in \{0,1\}^{p'(|x'|)}[(x',y') \in S'']\}]\} \\
=& \{x : \exists y \in \{0,1\}^{p(|x|)} \exists z \in \{0,1\}^{p'(|(x,y)|)}[((x,y),z) \in S'']\} \\
=& \{x : \exists y \in \{0,1\}^{p(|x|)} \exists z \in \{0,1\}^{p'(|(x,y)|)}[((x,y),z) \in S'']\} \\
=& \{x : \exists (y,z) \in \{0,1\}^{p(|x|)+p'(|(x,y)|)}[(x,(y,z)) \in \bar{S''}]\} \\
=& \{x : \exists t \in \{0,1\}^{p''(|x|)}[(x,t) \in \bar{S''}]\}
\end{aligned}
$$

最後から二番目の式変形は，存在量化子を 1 つにまとめている．また，$S'' \cong \bar{S''}$ なので，明らかに $\bar{S''} \in \prod_{k-1}$ となる．最後の式変形は，$p''(|x|) = p(|x|) + p'(|(x,y)|)$ と p'' を定義し，$t = (y,z)$ とおいた．また，$\bar{S''} \in \prod_{k-1}$ であることと補題 2.3 より $S \in \sum_k$ を得る．従って，$\sum_{k+1} \subseteq \sum_k$．よって，$\sum_{k+1} = \sum_k$ を得る．

また，同様にして $\prod_{k+1} = \prod_k$ を示すことができる（詳細は省略）．

以上により，証明が完了した． □

補題 2.5

$P = NP$ と仮定する．この時，$NP = coNP$ となる．

Proof. P の定義より $P = coP$(P の補クラス) である．よって，仮定より $NP = coP = coNP$ が成立する． □

定理 2.6 問題 (ii)-回答

以下の主張 (1)(2) は同値である：

(1) $P \neq NP$ (2) $P \neq PH$

問題 (i) **の系として示す方法**. まず，定理の主張は「$P = NP \iff P = PH$」と同値である．また，「$P = PH \implies P = NP$」は $NP = \sum_1$ という事実と PH の定義から明らかに成り立つ．よって，「$P = NP \implies P = PH$」を示すだけで十分である．

$P = NP$ であると仮定する．この時, 補題 2.5 より $NP = coNP$ である．よって, $NP = \sum_1, coNP = \prod_1$ なので問題 (i) とより，全ての $m \geq 1$ に対して $\sum_m = \prod_m = NP$ となる．さらに，$P = NP$ なので，全ての $m \geq 1$ に対して $\sum_m = \prod_m = P(= \sum_0)$ である．ゆえに，$PH = \bigcup_{k \geq 0} \sum_k = P$ となる．

以上により，証明が完了した． □

直接示す方法. まず，定理の主張は「$P = NP \iff P = PH$」と同値である．また，「$P = PH \implies P =$

NP」は $NP = \sum_1$ という事実と PH の定義から明らかに成り立つ．よって，「$P = NP \implies P = PH$」を示すだけで十分である．

$P = NP$ であると仮定する．この時，$P = PH$ を示せば良いが，「$P \subseteq PH$」であることは $P \subseteq NP$ であることと $NP \subseteq PH$ であることから明らかに成り立つ．よって，「$PH \subseteq P$」が成り立つことを示すだけで十分である．また，PH の定義から「$PH \subseteq P$ が成り立つ」を示すには「全ての $k \geq 0$ に対して $\sum_k, \prod_k \subseteq P$ が成り立つ」ことを示すだけで十分である．「全ての $k \geq 0$ に対して $\sum_k, \prod_k \subseteq P$ が成り立つ」ことを k についての帰納法で示す．

($k = 0, 1$ の場合)：$k = 0$ のときは P の定義から自明に成り立つ．$k = 1$ のときは，$\sum_1, \prod_1 \subseteq P$ を示す必要があるが，これは $P = NP$ の仮定と補題 2.5 より即座に成り立つ．

(帰納ステップ)：$k - 1 (k \geq 2)$ のとき上記の主張が成り立つ，つまり $\sum_{k-1}, \prod_{k-1} \subseteq P$ が成立すると仮定する．この時，$\sum_k, \prod_k \subseteq P$ が成り立つことを示す．しかし，$\sum_k \subseteq P$ を示すだけで十分である．なぜなら，$P = coP$ であり，$\prod_k = co\sum_k$ だからである．

まず，$S \in \sum_k$ とする．定義から，以下を満たすような多項式 p と多項式時間アルゴリズム V が存在する：

$$x \in S \iff \exists y_1 \in \{0,1\}^{p(|x|)} \forall y_2 \in \{0,1\}^{p(|x|)} ... Q_k y_k \in \{0,1\}^{p(|x|)} [V(x, y_1, ..., y_k) = 1]$$

ここで，クラス S' を以下のように定義する：

$$(x, y_1) \in S' \iff \forall y_2 \in \{0,1\}^{p(|x|)} ... Q_k y_k \in \{0,1\}^{p(|x|)} [V(x, y_1, ..., y_k) = 1]$$

ここで $p'(|(x, k_1)|) = p(|x|)$，$V'((x, y_1), ..., y_k) \iff V(x, y_1, ..., y_k)$ と新たに多項式 p' と多項式時間アルゴリズム V' を定義すれば，この p' と V' は S' が $\prod_{k-1}$ に属するための条件を満たす．よって，$S' \in \prod_{k-1}$ である．さらに，帰納法の仮定から $S' \in P$ である．従って，S' を決定的に計算する多項式アルゴリズム $\bar{V}$ が存在する．つまり，以下のことが成立する：

$$(x, y_1) \in S' \iff \bar{V}(x, y_1) = 1$$

ゆえに「$\forall y_2 \in \{0,1\}^{p(|x|)} ... Q_k y_k \in \{0,1\}^{p(|x|)} [V(x, y_1, ..., y_k) = 1] \iff \bar{V}(x, y_1) = 1$」であるので，以下のことが成立する：

$$\begin{aligned} x \in S &\iff \exists y_1 \in \{0,1\}^{p(|x|)} \forall y_2 \in \{0,1\}^{p(|x|)} ... Q_k y_k \in \{0,1\}^{p(|x|)} [V(x, y_1, ..., y_k) = 1] \\ &\iff \exists y_1 \in \{0,1\}^{p(|x|)} [\bar{V}(x, y_1) = 1] \end{aligned}$$

よって，上の $p, \bar{V}$ は S が NP 属するための条件を満たすとわかる．ゆえに，$S \in NP$．仮定より $P = NP$ であるので，$S \in P$ である．従って，$\sum_k \subseteq P$ である．

以上により，証明が完了した． □

参考文献

[1] NP-Completeness of 3SAT and MAX 2SAT, Rafael Accorsi

[2] SOME SIMPLIFIED NP-COMPLETE GRAPH PROBLEMS, M.R.Garey, D.S.Johnson and L.Stockmeyer

[3] Computational Complexity A Conceptual Perspective, Oded Goldreich

[4] Computational Complexity: A Modern Approach, Sanjeev Arora and Boaz Barak

[5] Reducibility among combinatorial problems, Richard M.Karp