Subset Sum Problem

問題:給定一集合 A 和 s，其中: $\forall a \in A$，$a \in \mathbb{Z}$ 且 $s \in \mathbb{Z}$
是否存在 $B \subseteq A$，$\sum_{b \in B} b = s$?

①. claim: $SS \in NP$:

給定一組 certificate 為 $B = \{b_1, b_2, \ldots, b_k\}$

在 polynomial time 內可得 $\sum_{b \in B} b$ 驗證是否為 s

$\therefore SS \in NP$

②. claim: $3\text{-SAT} \le_p SS$

給定 $\phi = C_1 \land C_2 \land C_3 \land \ldots \land C_k$ 為 3-SAT 之 instance 其中: ϕ 含 $x_1, \ldots, x_n$ 個 variables

建構一 (S, t) 為 subset sum problem 对應之 instance

不失一般性假設，$\forall C_i$，$x_j \in C_i \Leftrightarrow \overline{x_j} \notin C_i$，若存在則該 clause 自然為 satisfied

其中: $S = \{V_i \mid i = 1, \ldots, n\} \cup \{V_i' \mid i = 1, \ldots, n\} \cup \{S_i \mid i = 1, \ldots, k\} \cup \{S_i' \mid i = 1, \ldots, k\}$

而 $\forall a \in S$，a 為 10 進制，$n+k$ 个位元數，而前 n 个 digit 对應到 $x_1, \ldots, x_n$，後 k 个 digit 对應到 $C_1, \ldots, C_k$

其中: V_i 為前 n 个 digit，x_i 為 1，x_j 為 0，$\forall j \ne i$，後 k 个 digit 中，若 $x_i \in C_j$ 則為 1，否則為 0

V_i' 為前 n 个 digit，x_i 為 1，x_j 為 0，$\forall j \ne i$，後 k 个 digit 中，若 $\overline{x_i} \in C_j$ 則為 1，否則為 0

S_i 為前 n 个 digit 皆為 0，後 k 个 digit 中，C_i 為 1，其餘為 0

S_i' 為前 n 个 digit 皆為 0，後 k 个 digit 中，C_i 為 2，其餘為 0

t 為前 n 个 digit 皆為 1，後 k 个 digit 皆為 4

Note: ①. V_i, V_i' 的值皆唯一，因為若 $m \ne i$，則在 MSB 中，V_i 和 V_m 就不同

而若 $V_i = V_i'$ 則 x_i 和 $\overline{x_i}$ 同時在相同 clause，不滿足假設

②. S_i, S_i' 的值皆唯一，trivial

可見任一 digit 的 sum 皆最大為 6

$\because$ 3 SAT 中 clause 皆為 3 个 variables

$\therefore$ 取 $b \ge 7$ 以上基底，就不會有相加進位問題

顯然該 reduction 為 polynomial-time sovable

		x_1	x_2	x_3	C_1	C_2	C_3	C_4
v_1	=	1	0	0	1	0	0	1
S' v_1'	=	1	0	0	0	1	1	0
v_2	=	0	1	0	0	0	0	1
v_2'	=	0	1	0	1	1	1	0
v_3	=	0	0	1	0	0	1	1
v_3'	=	0	0	1	1	1	0	0
s_1	=	0	0	0	$\boxed{1}$	0	0	0
s_1'	=	0	0	0	$\boxed{2}$	0	0	0
s_2	=	0	0	0	0	1	0	0
s_2'	=	0	0	0	0	$\boxed{2}$	0	0
s_3	=	0	0	0	0	0	$\boxed{1}$	0
s_3'	=	0	0	0	0	0	2	0
s_4	=	0	0	0	0	0	0	$\boxed{1}$
s_4'	=	0	0	0	0	0	0	$\boxed{2}$
t	=	1	1	1	4	4	4	4

$\bar{x}_1, \bar{x}_2, x_3 = 1$

Figure 34.19 The reduction of 3-CNF-SAT to SUBSET-SUM. The formula in 3-CNF is $\phi = C_1 \wedge C_2 \wedge C_3 \wedge C_4$, where $C_1 = (x_1 \vee \neg x_2 \vee \neg x_3)$, $C_2 = (\neg x_1 \vee \neg x_2 \vee \neg x_3)$, $C_3 = (\neg x_1 \vee \neg x_2 \vee x_3)$, and $C_4 = (x_1 \vee x_2 \vee x_3)$. A satisfying assignment of ϕ is $\langle x_1 = 0, x_2 = 0, x_3 = 1 \rangle$. The set S produced by the reduction consists of the base-10 numbers shown; reading from top to bottom, $S = \{1001001, 1000110, 100001, 101110, 10011, 11100, 1000, 2000, 100, 200, 10, 20, 1, 2\}$. The target t is 1114444. The subset $S' \subseteq S$ is lightly shaded, and it contains v_1', v_2', and v_3, corresponding to the satisfying assignment. It also contains slack variables $s_1, s_1', s_2', s_3, s_4$, and s_4' to achieve the target value of 4 in the digits labeled by C_1 through C_4.

claim: 3-SAT is satisfiable $\Leftrightarrow \exists S' \subseteq S \ni \sum_{a \in S'} a = t$

(⇒) 令 ϕ 為一 satisfying assignment 為 $<x_1, \dots, x_n>$

若 $x_i = 1$ 則 $v_i \in S'$, $\forall i = 1, \dots, n$

$\bar{x}_i = 1$ 則 $v_i' \in S'$

∴ 可知 v_i 和 v_i' 不同時存在 S' 中，∴ $\sum_{a \in S} a$ 中前n个digit皆為1

又∵ 為 satisfied，∴ $C_1, \dots C_k$ 必含某些 literal 為 1

∴ $\forall a \in S$, $\sum_{a \in S'} a$ 的後k个bit中的 C_i 對應的digit至少有一个1

而 C_i 中又可能有1~3个literal為1，∴ v_i 貢獻之和中後面k个digit中 C_i 對應之和為1~3

又∵ s_i, s_i' 唯一且後k个digit皆為 $C_i = 1, 2$，其餘為0

目前: $S' = \{v_i \mid x_i = 1\} \cup \{v_i' \mid x_i = 0\}$

令 a_i 為 $\sum_{a \in S'} a$ 之第a个digit之數，則: $t_i - a_i \in \{1, 2, 3\}$，令為 b_i

若 $b_i = 1$, $\forall i = 0, \dots k-1$ 取 s_i 加入 S'

若 $b_i = 2$, $\forall i = 0, \dots, k-1$ 取 s_i' 加入 S'

若 $b_i = 3$, $\forall i = 0, \dots, k-1$ 取 s_i, s_i' 加入 S'

最終得到 S' 之 $\sum_{a \in S'} a = t$

(⇐): 設 $S' \subseteq S$ 且 $\sum_{a \in S'} a = t$

∵ 令 t_i 為 t 的第i个digit 且 ∵ $t_i = 1$, $\forall i = k, \dots, n-1$

∴ 可知 S' 必含恰一个 v_i 或 v_i', $\forall i = 1, \dots, n$

<u>claim: $C_j = 1$, $\forall j = 1, \ldots, k$</u>

$\because t_i = 4$, $\forall i = 0, \ldots, k-1$ 又 $S_i + S_i' \le 3$

$\therefore$ 可知每个 V_i 或 V_i' 必在 C_j 上貢獻至少為 1

設 $V_i \in S'$ 且 V_i 在 C_j 的 digit 上為 1, 則 $x_i \in C_j$

又 $\because$ 當 $x_i = 1$ 時, $V_i \in S'$, $\therefore C_j$ 為 1

若 $V_i' \in S'$ 且 V_i' 在 C_j 的 digit 上為 1, 則 $\overline{x_i} \in C_j$

又 $\because$ 當 $x_i = 0$ 時, $V_i' \in S'$, $\therefore C_j$ 為 1

故 $C_i \in \phi$, $C_i = 1$, $\forall i = 1, \ldots, k$

$\Rightarrow \phi$ 為 satisfiable