

Subset Sum is NP-complete.

Subset Sum is the following problem:

Given numbers x_1, \dots, x_n , is there a subset $S \subseteq [n]$ st $\sum_{i \in S} x_i = t$?

prop $3SAT \leq_p \text{SubsetSum}$

Given CNF $F = C_1 \wedge C_2 \wedge \dots \wedge C_m$ over variables x_1, \dots, x_n , we build instance as follows.

Numbers are $y_1, \dots, y_n, z_1, \dots, z_n, u_1, \dots, u_m, v_1, \dots, v_m$; defined as in the following table:

	x_1	\dots	x_n	C_1	\dots	C_m
y_1						
z_1						
1						
y_n						
z_n						
u_1						
v_1						
\dots						
u_m						
v_m						

Annotations:

- y_i has a 1 in C_j if $x_i \in C_j$
- z_i has a 1 in C_j if $\bar{x}_i \in C_j$.
- u_j, v_j have a 1 in position C_j
- 0s elsewhere

Example values:

y_i, z_i have a 1 in position x_i

$t = 1 \dots 1 \quad 3 \dots 3$
 $\quad \quad \quad n \quad \quad \quad m$

Intuitively, y_i corresponds to x_i , z_i to \bar{x}_i , and u_j, v_j are slack for clause C_j .

e.g.

	x_1	x_2	x_3	x_4	C_1	C_2
y_1	1	0	0	0	1	0
z_1	1	0	0	0	0	0
y_2		1	0	0	1	1
z_2		1	0	0	0	0
y_3			1	0	0	1
z_3			1	0	1	0
y_4				1	0	1
z_4				1	0	0
u_1					1	0
v_1					1	0
u_2						1
v_2						1
t	1	1	1	1	3	3

So problem is choose subset of $(100010, 100000, 10011, 10000, 1001, 1010, 101, 100, 10, 10, 1, 1)$ that sums up to 111133.

Claim: the reduction is poly-time.

Claim: the reduction is correct.

proof: $F \in \text{SAT} \Rightarrow f(F) \in \text{SubsetSum}$.

Assume α satisfies F . Pick y_i if $\alpha(x_i) = T$, and z_i if $\alpha(x_i) = \perp$. Let s_j be the number of literals in C_j that α satisfies. Cases:

- $s_j = 0$: impossible because α satisfies F .
- $s_j = 1$: pick u_j and v_j .
- $s_j = 2$: pick u_j but not v_j .
- $s_j = 3$: do not pick u_j or v_j .

Easy to check picked numbers sum to t .

proof: $f(F) \in \text{SubsetSum} \Rightarrow F \in \text{SAT}$.

Assume S is a subset summing up to t . Obs there is no carry, so we can treat columns independently. Obs S contains exactly one of y_i and z_i $\forall i$, so we can set $\alpha(x_i) = T$ if $y_i \in S$ and $\alpha(x_i) = \perp$ if $z_i \in S$. def s_j as before. Obs $3 = t_j \leq s_j + 2 \Rightarrow s_j \geq 1$, hence every clause is satisfied.