SUBSET SUM problem (ControleM1Complexity2013)

	x_1	x_2	x_3	C_1	C_2	C_3	C_4
v_1	1	0	0	1	0	0	1
v'_1	1	0	0	0	1	1	0
v_2	0	1	0	0	0	0	1
v'_2	0	1	0	1	0	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	1	0	0	0
s'_1	0	0	0	2	0	0	0
s_2	0	0	0	0	1	0	0
s'_2	0	0	0	0	2	0	0
s_3	0	0	0	0	0	1	0
s'_3	0	0	0	0	0	2	0
s_4	0	0	0	0	0	0	1
s'_4	0	0	0	0	0	0	2
t	1	1	1	4	4	4	4

First check the polynomiality of this construction :
Table has $(2n + 2k + 1)$ rows and $(n + k)$ columns.
This is polynomial (parameters n AND k).

1 SAT $\Rightarrow$ SUBSET SUM

If ϕ is True
Then at least one literal (x_i or $\neg x_i$) per clause C_j is True
According to the rule specified in Question 4, v_i (resp. v'_i) is then picked in A' (because True)
In the column indexed by C_j :

— if 2 others v_l (resp. v'_l) corresponding to x_l (resp. $\neg x_l$) in C_j have also been picked into A' then choose s_j
— if only one v_l (resp. v'_l) corresponding to x_l (resp. $\neg x_l$) in C_j have also been picked into A' then choose s'_j
— if no other v_l (resp. v'_l) corresponding to x_l (resp. $\neg x_l$) in C_j have also been picked into A' then choose s_j and s'_j

This ensures that the numbers in column indexed by C_j sum to 4

Concerning the n first columns :

In the column indexed by x_i, only one of the numbers v_i and v'_i has been picked into A'.

This ensures that the numbers in column indexed by x_i sum to 1

2 SUBSET SUM $\Rightarrow$ SAT

Once again : column by column

n first columns : sum to 1

Thus, **only one** of the numbers v_i and v'_i has been picked into A'

If v_i has been picked, let us set x_i to True If v'_i has been picked, then set $\neg x_i$ to True

This ensures that we have built a truth assignment

k last columns : sum to 4

in column C_j, s_j and s'_j are not sufficient to obtain a 4.

Thus at least one of the value 1 in the $2n$ first rows is required.

It is on a row v_i (resp v'_i) and encodes the occurence of x_i (resp. $\neg x_i$) in C_j.

As v_i(resp v'_i) is in A' then x_i (resp. $\neg x_i$) is set to True (see above) and thus C_j is True

3 NP-hardness

3-SAT is known to be NP-complete, thus NP-hard (Definition 20 in the Slides)

From section 1. and 2., we have : 3-SAT $\leq_P$ SUBSET SUM.

Thus (Prop. 6) SUBSET SUM is NP-hard.

4 NP-complete

SUBSET SUM is in NP : given $A' \subseteq A$ a certificate, it suffices to check if $\sum_{a \in A'} a = t$. This takes $O(|A|)$ operations (as A' is a subset of A).

Together with the fact that SUBSET SUM is NP-hard, we conclude that SUBSET SUM is NP-complete.