One more example, for a problem in NP:

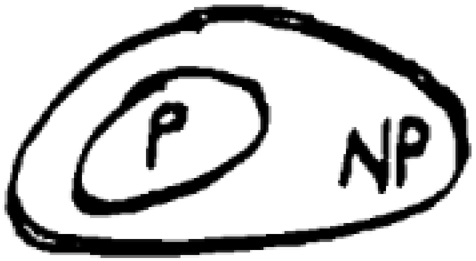
· Given a graph, and 2 vertices u & v, is there a path from u to v containing all the vertices of G?

- 'Certificate' for a YES answer:
  The vertices on the path, in sequence.

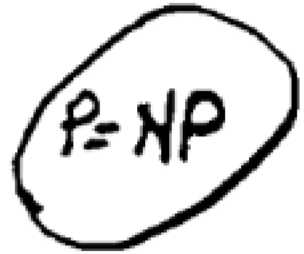
- Another one:

  Given a graph G, is there a closed 'walk' (vertices may repeat) on G that covers all the edges?

- This is in NP, and it is in P also.



Is P = NP?



- We saw 2 definitions:

  (i) YES answer has a certificate that can be verified in polynomial time

  (ii) $NP = \bigcup_k NTIME(n^k)$.

Why are these 2 equivalent?

Proof idea: (i) $\Rightarrow$ (ii) and (ii) $\Rightarrow$ (i).

First part, (i) $\Rightarrow$ (ii):

If we have a polynomial time verifier algorithm (it could use a certificate), how to design a non-deterministic TM that decides it?

Idea: "Guess" the certificate c.

Steps of the non-deterministic TM:

On input w, of Length n:

1. Non-deterministically 'guess' a certificate c, of Length $O(n^k)$.
2. Run verifier V on $\langle w, c \rangle$.
3. If YES, say YES. Else say NO.

The other direction: (ii) $\Rightarrow$ (i)

- Given a non-deterministic TM N, construct a verifier algorithm $V\langle w, c\rangle$.

- Idea: Use the symbols in the certificate 'c' to make the choice of move on N.

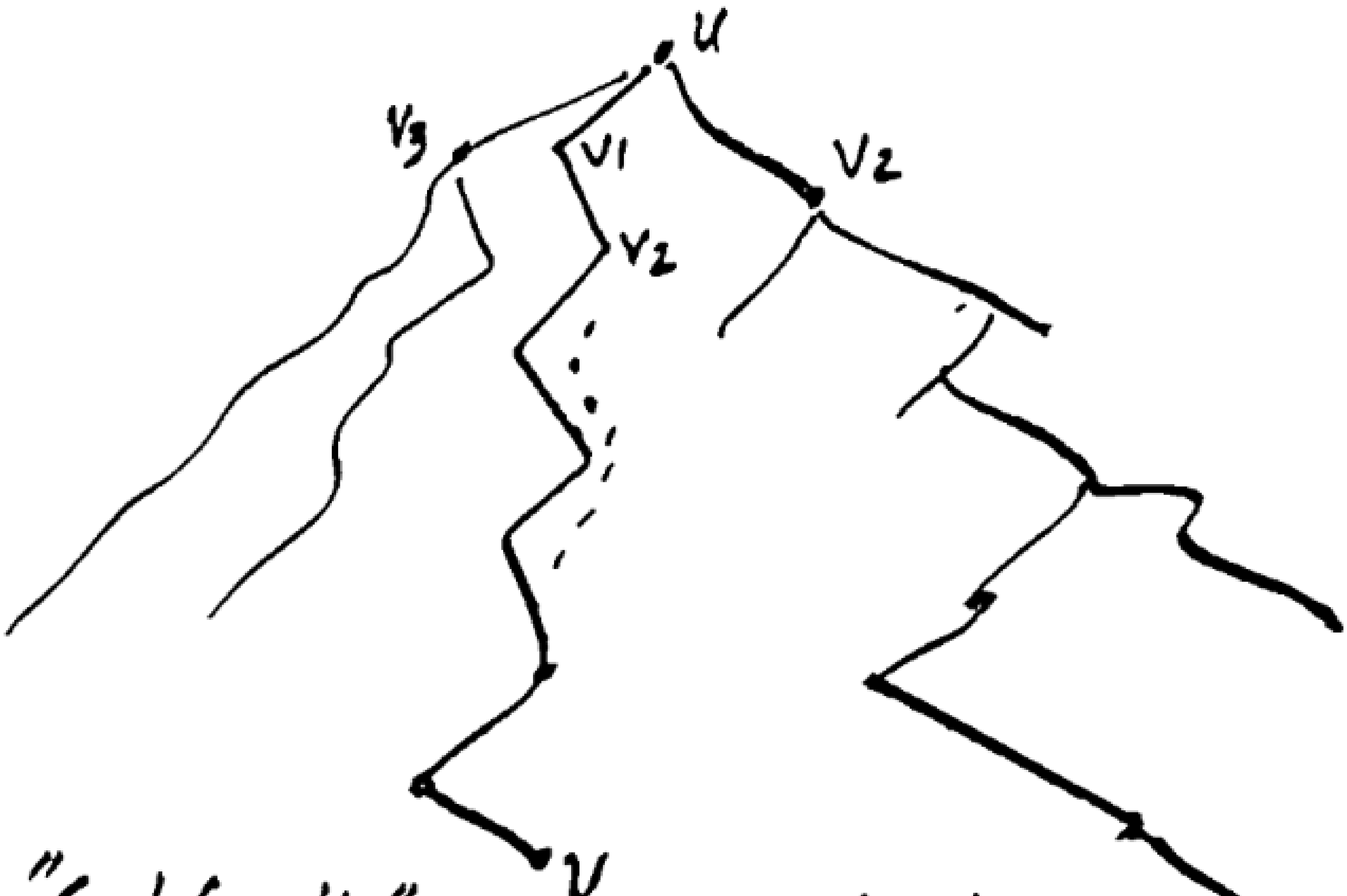
- If this branch accepts, YES. else NO.

(SUDEEP)

- Example: Given G and (u,v),
  If there a path from u to v, through all vertices of G?

- If there is a non-deterministic algorithm that finds such a path...

(SUDEEP)



"certificate" corresponds to the "right branch".

More examples:

- Given a graph G, is G bipartite?
  (this is in P also).
- Is G 4-colorable?
- Is there a cycle through all vertices of G?

?

- Given a boolean formula ϕ

eg: ϕ: $(x_1 \vee \bar{x}_2) \wedge (x_2 \vee x_3 \vee x_4)$
$\wedge (\bar{x}_3 \vee x_4) \wedge (\bar{x}_1 \vee x_5)$

Is ϕ satisfiable?

[i.e. can we give true/false values to variables so that ϕ becomes TRUE?]