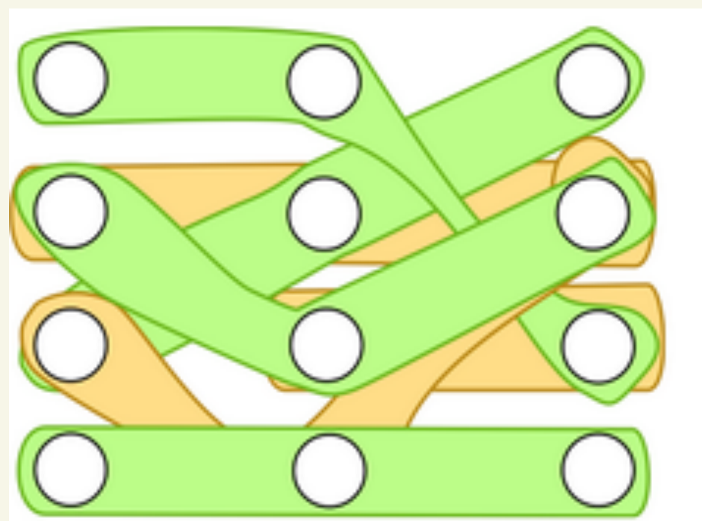
Strong NP-Hardness: 3-dim matching

Given 3 disjoints sets X, Y & Z, each size n, along with a set $T \subseteq X \times Y \times Z$ of ordered triples, can we find a set $S \subseteq T$ s.t. each element of $X \cup Y \cup Z$ is in exactly 1 triple?



Note:
- generalization of bipartite matching
- No #s in sight!

Reduction: from 3SAT

Input: boolean function Φ with n variables & m clauses.

$m = 4$

Variable gadget:

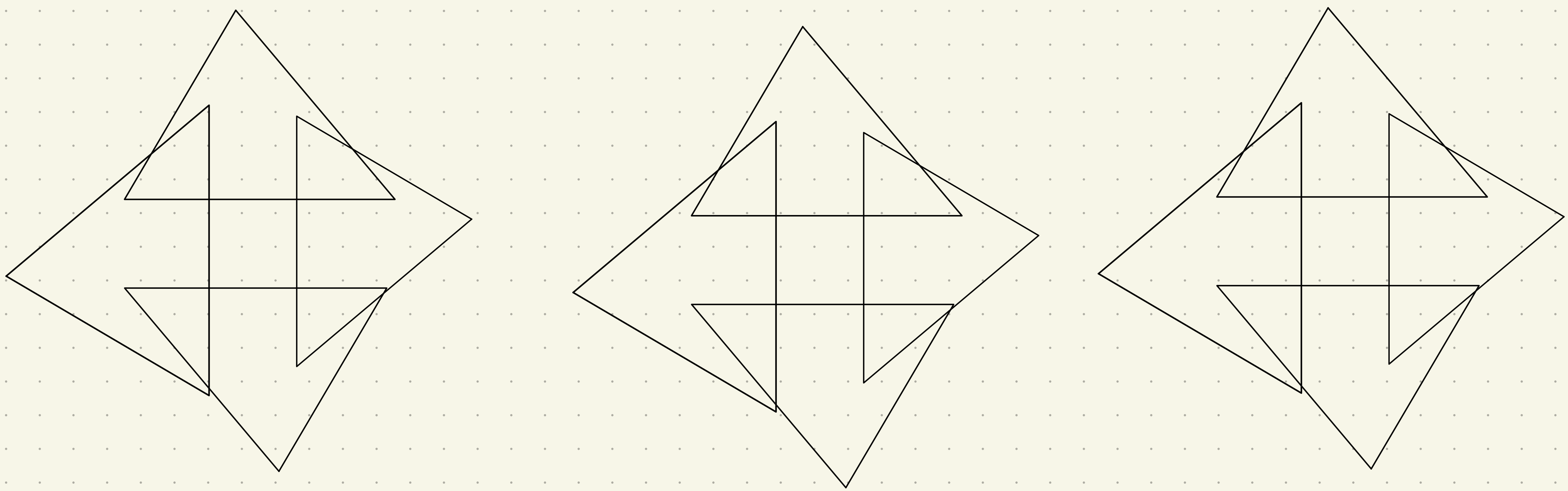
- m elements in core
- m elements in "tips"

Even/odd:

Clause gadget

- x_i "even" covered $\Rightarrow$ true
- "odd" covered $\Rightarrow$ false

$x_i \vee \overline{x_j} \vee x_k$:



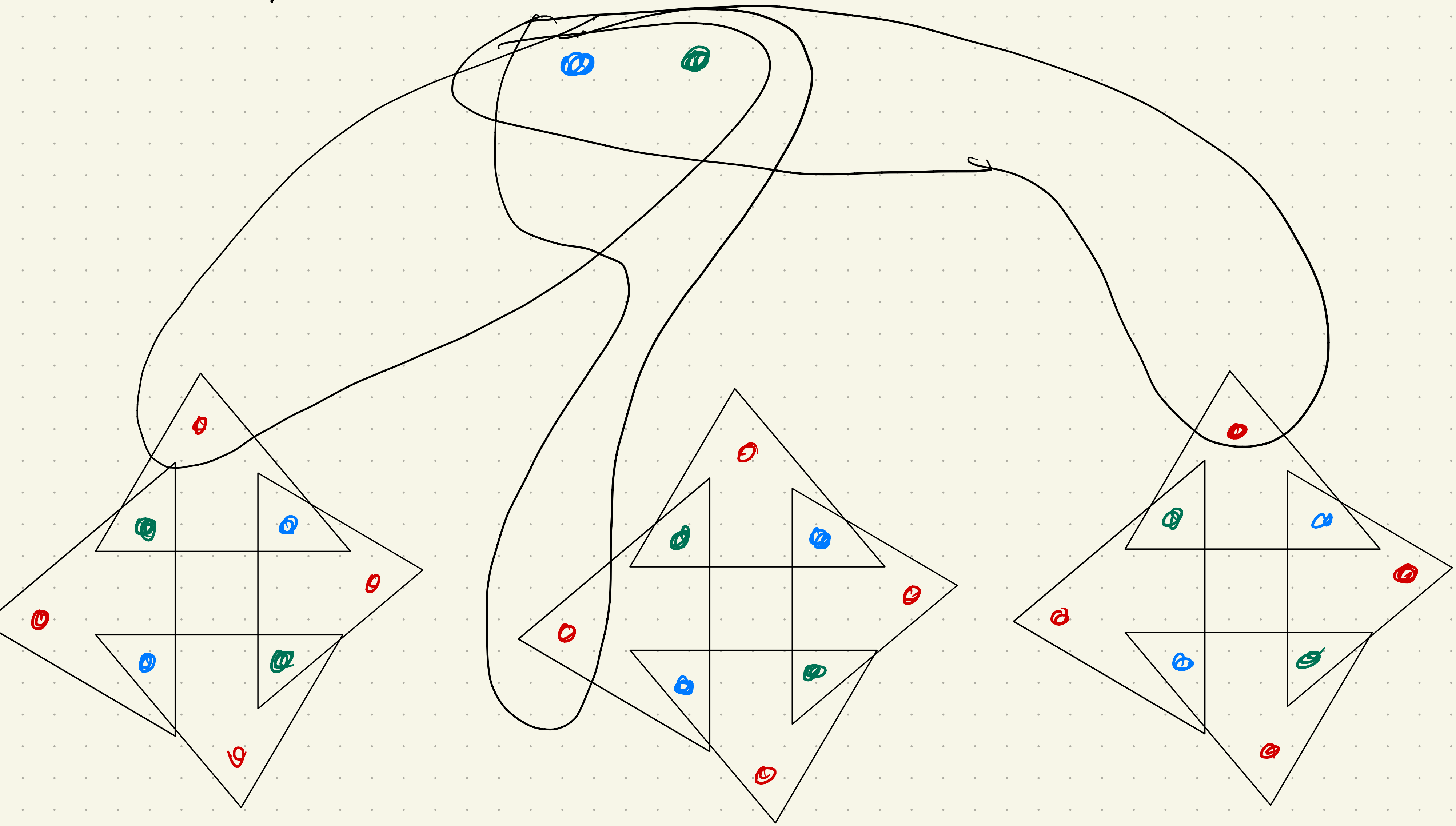
x_i x_j x_k

So: almost there!

Problem: some uncovered "tips".

What if x_i is in only 1 clause?

Finally: X, Y + Z!



Construction time!

Note: No numbers really anywhere!

So: nothing polynomially bounded.

Really about combinatorial structure of inclusion in the solution.

Complexity Hierarchy

We saw P, NP, & co-NP.

In formal Turing machines, these are tied up with language recognition:

A language is in Time(f(n)) if it can be decided by a Turing machine in time f(n).

Ex: TSP & an input graph G

Time & space Complexity

$$\begin{aligned}\textbf{TIME}(t(n)) = \{X \subseteq \{0,1\}^* \;&:\; \exists T \in \mathfrak{T} \forall n (\text{time}_T(n) \leq t(n)) \\ &\quad \text{and } T \text{ decides } X\} \\ \textbf{SPACE}(s(n)) = \{X \subseteq \{0,1\}^* \;&:\; \exists T \in \mathfrak{T} \forall n (\text{space}_T(n) \leq s(n)) \\ &\quad \text{and } T \text{ decides } X\}\end{aligned}$$

Non-determinism

$$\begin{aligned}\textbf{NTIME}(t(n)) = \{X \subseteq \{0,1\}^* \;&:\; \exists N \in \mathfrak{N} \forall n (\text{time}_N(n) \leq t(n)) \\ &\quad \text{and } N \text{ decides } X\} \\ \textbf{NSPACE}(s(n)) = \{X \subseteq \{0,1\}^* \;&:\; \exists N \in \mathfrak{N} \forall n (\text{space}_N(n) \leq s(n)) \\ &\quad \text{and } N \text{ decides } X\}\end{aligned}$$

These are connected in a natural way!

Theorem 3.2 Suppose that $f(n)$ is both time and space constructible. Then

i. $\mathbf{NTIME}(f(n)) \subseteq \mathbf{SPACE}(f(n))$

ii. $\mathbf{NSPACE}(f(n)) \subseteq \mathbf{TIME}(2^{O(f(n))})$

Why?

What we know:

$$\mathbf{L} \subseteq \mathbf{NL} \subseteq \mathbf{P} \subseteq \mathbf{NP} \subseteq \mathbf{PSPACE} \subseteq \mathbf{EXP} \subseteq \mathbf{NEXP} \subseteq \mathbf{EXPSPACE}$$

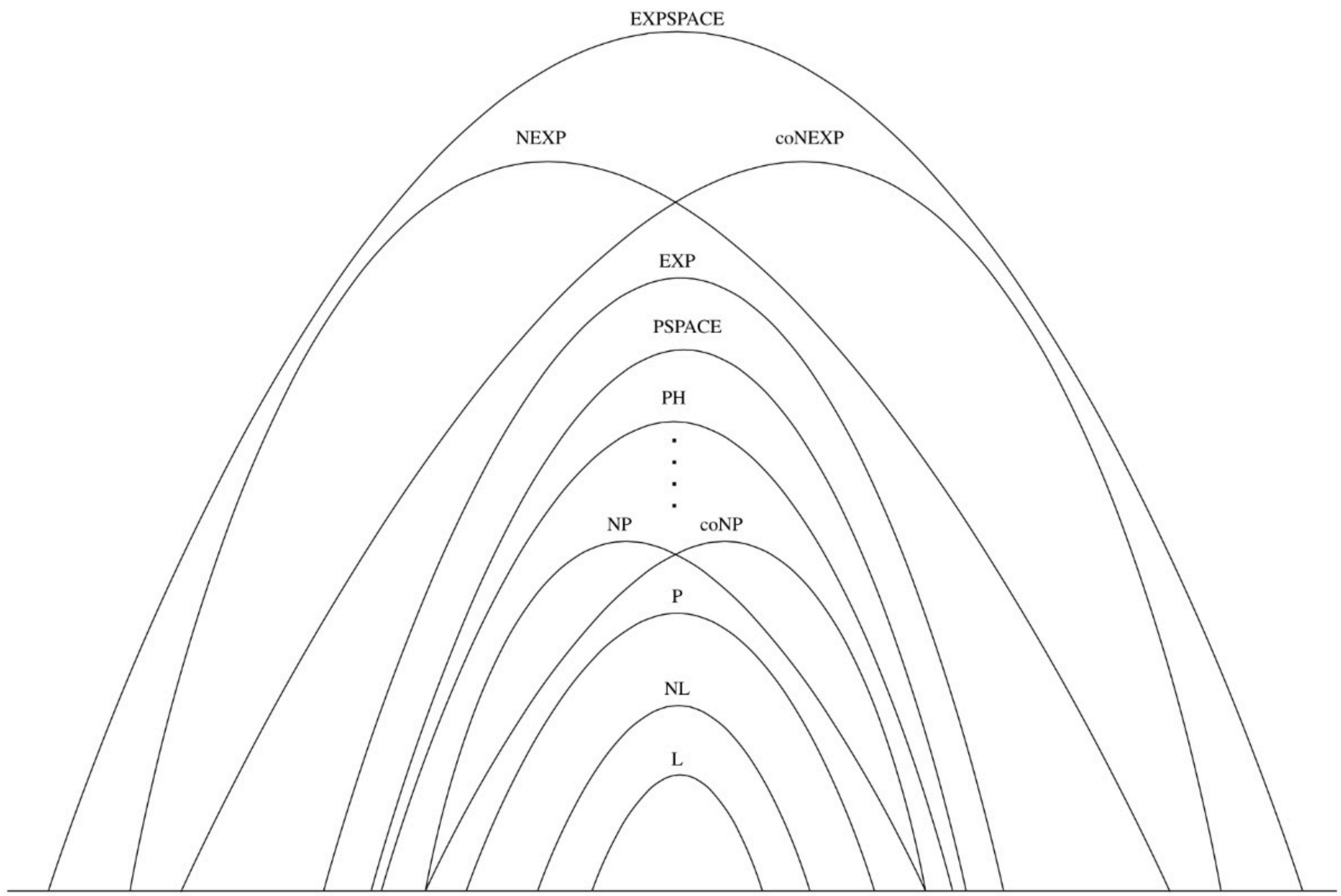


FIGURE 2. Inclusion relationships among major complexity classes. The only depicted inclusions which are currently known to be proper are $\mathbf{L} \subsetneq \mathbf{PSPACE}$ and $\mathbf{P} \subsetneq \mathbf{EXP}$.

What is in PSPACE?

First problem:
Word problem for deterministic context sensitive grammars.

Given a word + grammatical transformations that only increase length, determine if a sentence could be produced via the transformations.

INFORMATION AND CONTROL 7, 207–223 (1964)

Classes of Languages and Linear-Bounded Automata*

S.-Y. KURODA

Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge, Massachusetts

0. Let V_T and V_N be disjoint finite sets, and put $V = V_T \cup V_N$. A *grammar* G over the *terminal vocabulary* V_T and the *nonterminal vocabulary* V_N is a semi-Thue system (cf. Davis (1958)) in which the axiom is an element S of V_N, called the *initial symbol* of G, and for each production $PgQ \rightarrow P\bar{g}Q$ there are strings φ, ψ, ω in V and a string χ in V_N, such that $g = \varphi\chi\psi$ and $\bar{g} = \varphi\omega\psi$. Here P and Q are variables over strings in V. However, we will denote this production simply by $g \rightarrow \bar{g}$, dropping variables, and call it a *rule* of G. In general, for any strings σ, τ in V, we write $\sigma \rightarrow \tau$ if (σ, τ) satisfies a production of G, or in other words, if there is a rule $g \rightarrow \bar{g}$ of G such that $\sigma = \pi g \rho$, $\tau = \pi \bar{g} \rho$ for some π and ρ. By $\sigma \Rightarrow \tau$ we mean that τ is a theorem of G under the premise σ in the sense of the theory of combinatorial system, that is to say, $\sigma = \tau$ or there exist a finite number of strings $\sigma_1, \sigma_2, \cdots, \sigma_n$ such that $\sigma \rightarrow \sigma_1$, $\sigma_1 \rightarrow \sigma_2$, $\cdots$, $\sigma_{n-1} \rightarrow \sigma_n$, $\sigma_n \rightarrow \tau$. A string x *in* V_T is a *sentence* of G, if x is a theorem of G, that is to say, if $S \Rightarrow x$. The set of sentences of G is the *language generated* by G, which will be denoted by $L(G)$. It is a subset of the free semigroup V_T^{*} [1] generated by V_T. Conversely, a subset of the free semigroup V_1^* generated by a finite set V_1 is a *language*, if there exists a finite set V_2 and a grammar G with the terminals V_1 and the nonterminals V_2 which generates L. G is then *a grammar of L*. According to Chomsky (1959) G is context-sensitive, if each rule is of the type

Others: Reconfiguration problems

Graph example: Given two 4-colorings of a graph, can you change one vertex color at a time, while maintaining no edge has endpoints of same color, & transform from the first coloring to the second?

Polynomial Heirarchy: Recursive function theory

Beyond P & NP!

Let Δ_0^P, Σ_0^P, & Π_0^P all be $= P$.

Let $NP = \Sigma_1^P$

$co\text{-}NP = \Pi_1^P$

Then:

$L \in \Sigma_i^P$ if $\exists$ polynomial $p(n)$ & Turing machine T s.t.

$$x \in L \iff \exists y_1 \forall y_2 \cdots y_i,$$

$$T(x, y_1, \ldots, y_i).$$

$$\begin{tikzcd}
 & \vdots & \\
\Sigma_3^{\mathrm{P}} & & \Pi_3^{\mathrm{P}} \\
 & \Delta_3^{\mathrm{P}} \arrow[ul] \arrow[ur] & \\
\Sigma_2^{\mathrm{P}} \arrow[uu] \arrow[ur] & & \Pi_2^{\mathrm{P}} \arrow[uu] \arrow[ul] \\
 & \mathrm{P}^{\mathrm{NP}} = \Delta_2^{\mathrm{P}} \arrow[ul] \arrow[ur] & \\
\mathrm{NP} = \Sigma_1^{\mathrm{P}} \arrow[uu] \arrow[ur] & & \Pi_1^{\mathrm{P}} = \mathrm{coNP} \arrow[uu] \arrow[ul] \\
 & \Delta_0^{\mathrm{P}} = \Sigma_0^{\mathrm{P}} = \mathrm{P} = \Pi_0^{\mathrm{P}} = \Delta_1^{\mathrm{P}} \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

$\boxed{PH}$

Intuitively:

Problems solvable in polynomial time with a bounded number of alternation between "exists" players & "for all" players.

Σ_1^P: $\exists$ certificate s.t. verifier accepts

Π_1^P: $\forall$ certificates, verifier accepts

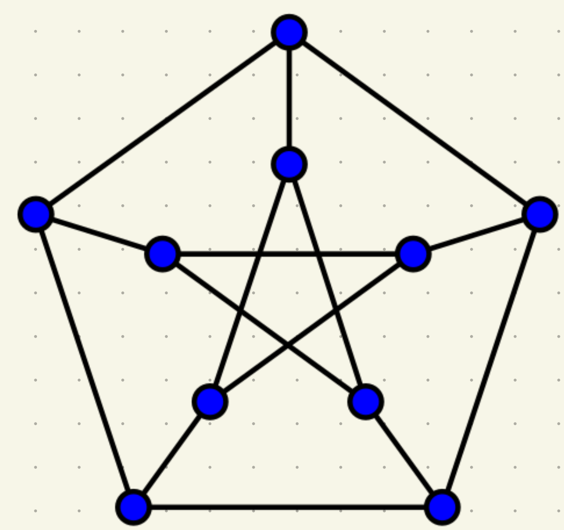
Σ_2^P: $\exists$ a strategy s.t. no matter the challenge, we win.

Σ_2^P example

Given G + k, is there a set of S vertices, $|S|=k$, s.t. for all vertices not in S, $S \cup \{v\}$ is not a clique?

<u>Ex:</u> Let $k=1$

$k=2$



I'll stop here

↳ but happy to discuss if you have questions!

(Note: Not on HW next week...)