



CC184 - Complejidad Algorítmica

Tema: Problemas de Tipo P - NP
Formato: Esquema de Aprendizaje
Elaborado por: Robert Zubieta
Fuente: Propia

Problemas de Tipo P vs NP

I. 23 Problemas de Hilbert



Los **problemas de Hilbert** conforman una lista de 23 problemas [matemáticos](#) compilada por el matemático alemán [David Hilbert](#) para la conferencia en París del [Congreso Internacional de Matemáticos](#) de **1900**. Los problemas estaban todos por resolver en aquel momento, y varios resultarían ser muy influyentes en la matemática del siglo xx. Hilbert presentó diez de los problemas (1, 2, 6, 7, 8, 13, 16, 19, 21 y 22) en la conferencia, en un acto el 8 de agosto en [La Sorbona](#).

Problem a	Explicación concisa	Estado del problema
1.er	La hipótesis del continuo (esto es, no existe conjunto cuyo tamaño esté estrictamente entre el de los racionales y el de los números reales).	Se ha probado la imposibilidad de probarlo como cierto o falso mediante los axiomas de Zermelo-Fraenkel. No hay consenso al respecto de considerar esto como solución al problema. ¹
2.º	Probar que los axiomas de la aritmética son consistentes (esto es, que la aritmética es un sistema formal que no supone una contradicción).	Parcialmente resuelto: hay quienes sostienen que se ha demostrado imposible de establecer en un sistema consistente, finitista y axiomático; ² sin embargo, Gentzen probó en 1936 que la consistencia de la aritmética se deriva del buen fundamento del ordinal E_0 , un hecho sujeto a la intuición combinatoria.
3.er	Dados dos poliedros de igual volumen, ¿es siempre posible cortar el primero en una cantidad finita de piezas poliédricas que puedan ser ensambladas de modo que quede armado el segundo?	Resuelto. Resultado: no, probado usando invariantes de Dehn.
4.º	Construir todas las métricas cuyas rectas sean geodésicas.	Demasiado vago para decidir si se ha resuelto o no.3
5.º	¿Son los grupos continuos grupos diferenciales de forma automática?	Resuelto por Andrew Gleason (1952).
6.º	Axiomatizar toda la física.	La mecánica clásica: Hamel (1903). La termodinámica: Carathéodory (1909). La relatividad especial: Robb (1914) y Caratheodory (1924) independientemente. La teoría de probabilidades: Kolmogórov (1930). La teoría cuántica de campos: Wightman a finales de los años 1950.
7.º	¿Es a^b trascendental, siendo $a \neq 0,1$ algebraico y b irracional algebraico?	Resuelto. Resultado: sí, ilustrado por el teorema de Gelfond o el teorema de Gelfond-Schneider.
8.º	La hipótesis de Riemann (la parte real de cualquier cero no trivial de la función zeta de Riemann es $\frac{1}{2}$) y la conjetura de Goldbach (cada número par mayor que 2 se puede escribir como la suma de dos números primos).	Sin resolver.4
9.º	Encontrar la ley más general del teorema de reciprocidad en cualquier cuerpo numérico algebraico.	Parcialmente resuelto.5
10.º	Encontrar un algoritmo que determine si una ecuación diofántica polinómica dada con coeficientes enteros tiene solución entera.	Resuelto. Resultado: El teorema de Matiyasevich (1970) implica que no existe tal algoritmo.
11.º	Resolver las formas cuadráticas con coeficientes numéricos algebraicos.	Parcialmente resuelto: Sobre los números racionales: Hasse (1923-1924). Sobre los números enteros: Siegel en los años 1930.
12.º	Extender el teorema de Kronecker-Weber sobre extensiones abelianas de los números racionales a cualquier cuerpo numérico de base.	Sin resolver.
13.º	Resolver todas las ecuaciones de $7.º$ grado usando funciones de dos parámetros.	Resuelto negativamente por Vladímir Arnold y Andréi Kolmogórov en 1957.
14.º	Probar la finitud de ciertos sistemas completos de funciones.	Resuelto. Resultado: no, en general, debido a un contraejemplo, Nagata (1962).
15.º	Fundamento riguroso del cálculo enumerativo de Schubert.	Parcialmente resuelto, Van der Waerden a finales de los años 1930.
16.º	Topología de las curvas y superficies algebraicas.	Sin resolver.
17.º	Expresión de una función definida racional como cociente de sumas de cuadrados.	Resuelto. Resultado: se estableció un límite superior para el número de términos cuadrados necesarios, Pfister (1967). La solución negativa en general se debe a Du Bois (1967).
18.º	¿Existe un poliedro irregular y que construya otros poliedros? ¿Cuál es el apilamiento compacto más denso?	Resuelto.6
19.º	¿Son siempre analíticas las soluciones de los Lagrangianos?	Resuelto por Bernstein (1904). Resultado: sí.
20.º	¿Tienen solución todos los problemas variacionales con ciertas condiciones de contorno?	Resuelto. Ha supuesto un área importante de investigación durante el siglo xx, culminando con las soluciones al caso no lineal.
21.er	Probar la existencia de ecuaciones lineales diferenciales que tengan un grupo monodrómico prescrito.	Resuelto. Resultado: sí o no, dependiendo de una formulación más exacta del problema. Según Gray resuelto de forma negativa por Anosov y Bolibruch (1994).
22º	Uniformización de las relaciones analíticas por medio de funciones automórficas.	Resuelto por Koebe (1907) y Poincaré independientemente (1907).
23.er	Extensión de los métodos del cálculo de variaciones.	Sin resolver.

Fuente de Referencia: https://es.wikipedia.org/wiki/Problemas_de_Hilbert

II. Problemas del Milenio

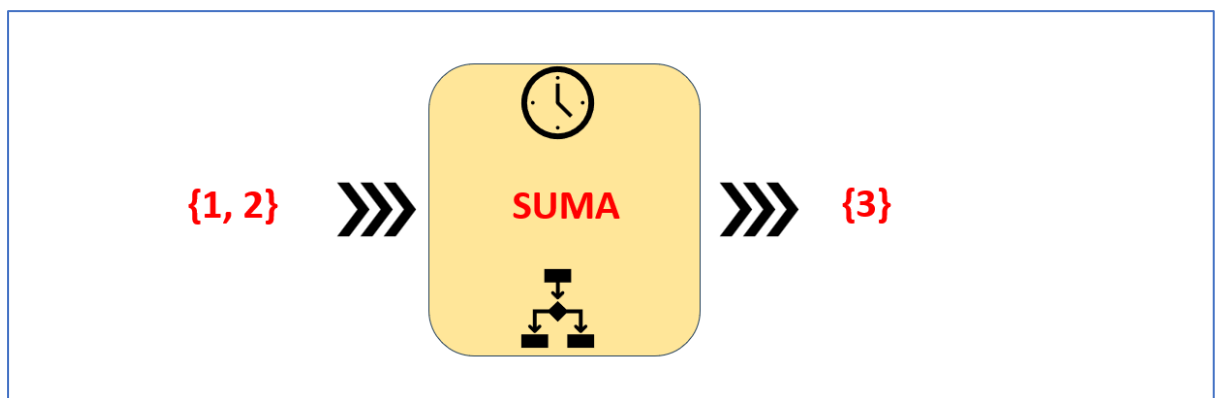
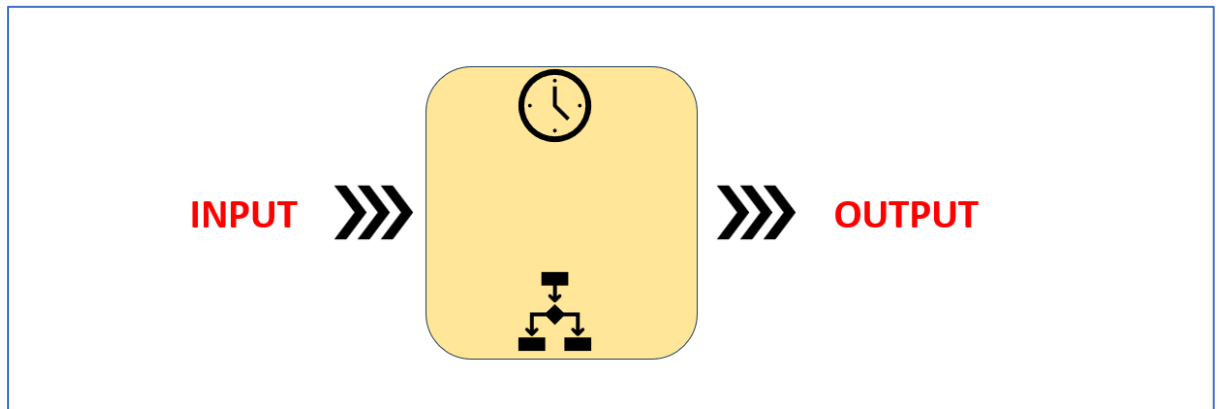
Los problemas del milenio

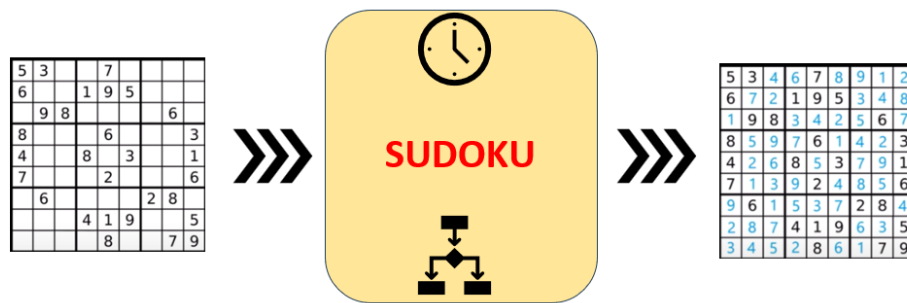
1. La Conjetura de Poincare.
2. La conjetura de Birch y Swinnerton-Dyer.
3. La conjetura de Hodge.
4. La teoría de Yang-Mills.
5. Las ecuaciones de Navier-Stokes.
6. La hipótesis de Riemann.
7. P vs NP.

1.000.000 \$



III. Algoritmo

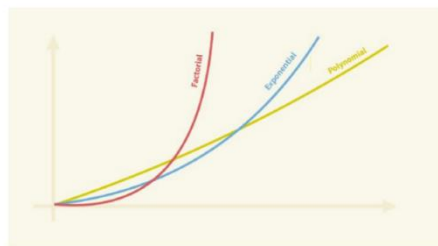




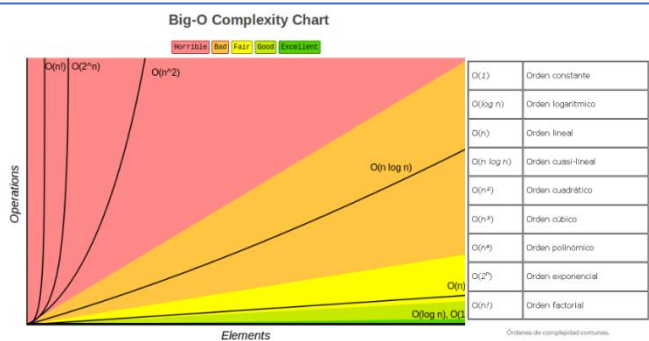
P vs NP se refiere a la COMPLEJIDAD DEL ALGORITMO
(Respecto al **Tiempo** y al Espacio)

- Como son de difíciles ?
- Cuáles son los mejores algoritmos ?

IV. Complejidad



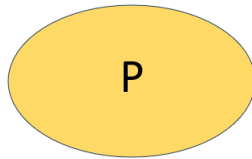
La complejidad temporal de un algoritmo se describe como una función asintótica que depende del tamaño de entrada del algoritmo. Se hace una distinción principal entre las funciones de complejidad **Factorial**, **Exponencial** y **Polinomial**.



En Tiempo polinomial: $O(n^4)$, $O(n^2)$, $O(n^3)$, $O(1)$, $O(n \lg n)$

Los algoritmos que tienen una complejidad de tiempo polinomial se denominan **"eficientes"**.

V. P vs NP



P: Aquellos **problemas** de decisión que se pueden **resolver** con una Máquina de Turing **determinista** usando un **tiempo polinómico**, en función de la entrada de los datos.

Ejemplo:

- Sumar 2 números.
- Multiplicar 2 números.
- Calcular el determinante de una matriz.

¿y un SUDOKU se podrá resolver en un tiempo polinómico ?

	4		1
3			
			4

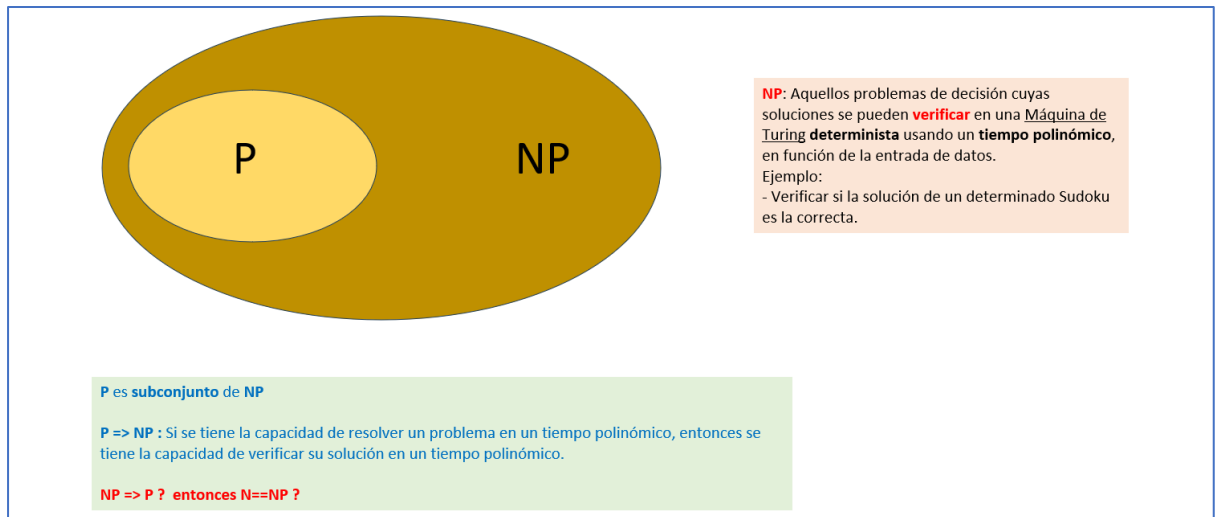
7		8	3		5
	5	7		3	
	4		6		2
5	6	4			2
				2	9
2					6
	7		2		8
	8	3	6		
6		4	9		7

2		3	14	8							13	4	24	7	1			
10	17			6	18		22	16	12						13	19		
15	24	13	7			4	10			3	14		18		22	2	6	
	1	21		15	22				19	13		8			16	18	20	
5	20	7	25	19			21	17	18	2	10	12	22	9	15	11		
11		22	8	24	7	1	5			13	16	17	25	23	2	4	6	19
16	9	12	17	19	22			18	21		20	6	13	7		23	11	
	6	21	9	16		3		22	20	19			15	8	25			
	23	5		2		11	17	8			16	12	9		21	3	10	
			6		12	9	1	25	3	11	7			21				
9	23	5	17	4	16	11	22	18	2	10	12	21	13		7			
4	6	5		2		18	21	24		19	3	12	23		17			
	12	11		7	3	24	17	20	15	13	19	1	5	8	6	9		
	22		14	19	6	16		8	9	7		24	3		1	18		
	21		25	13	20	8	12	14	10	9	16	15	6		4			
	25		24		18		4	3	10	5	1		14					
	5	3		17		23	7	13			18	19	21		22		11	12
		18	10	8				25	23	2		5	16	11	9		3	
17	20		2	22	16	6		7	12			9	3	16		23	24	25
6	4	16	1	11	12	25	3	19			21	17	23	8	18	2		14
		4	14	24	11	19	23	21	17	16	8			1	2	9	13	5
	1	14	23				9		19	5		24	12			8	17	
16	11	8				1	6	4		23	15			14	12	9	10	
21	3			17				15	25	20		4	10			16	11	
	20	2		16	5	8						6	19	25			3	

El algoritmo del SUDOKU generalizado tiene Complejidad **EXPONENCIAL** (no Polinómica)

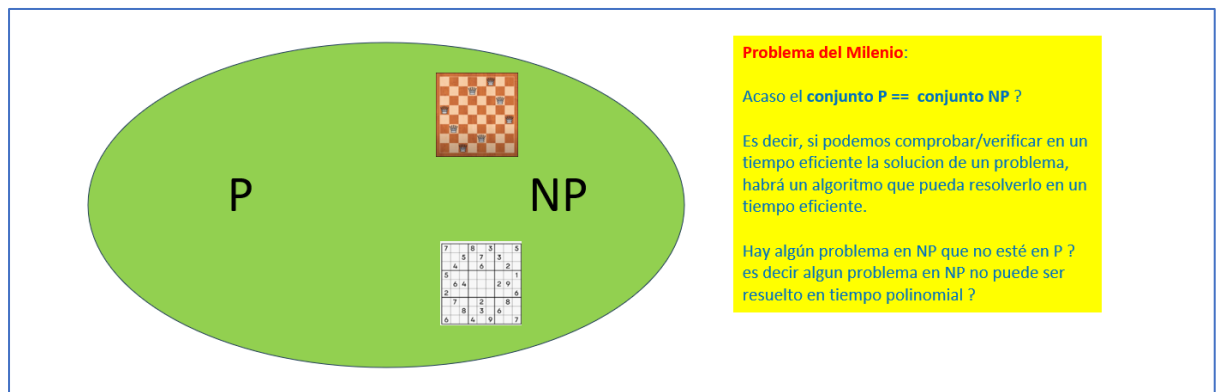
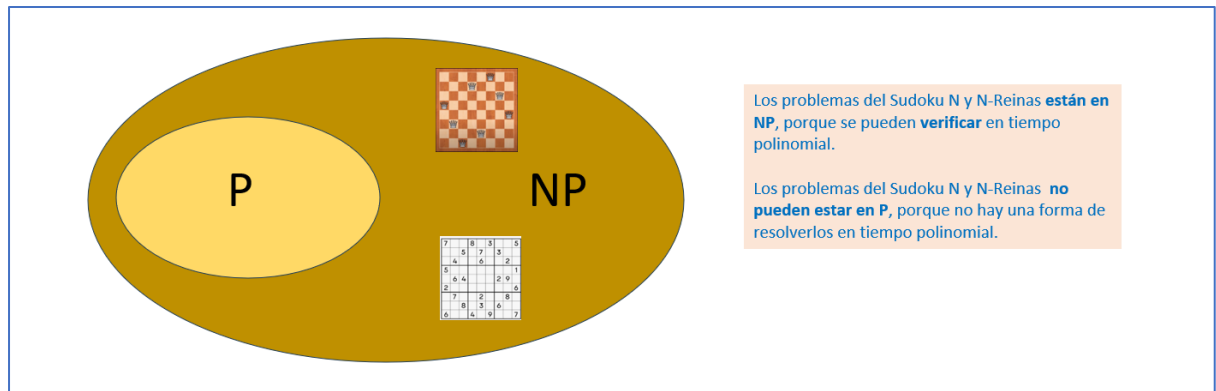
Entonces **no** tenemos un Algoritmo "bueno" (eficiente en tiempo) o **SOLUCIÓN** para resolver el SUDOKU generalizado N, pero sí tenemos una forma de **VERIFICAR/COMPROBAR** su solución en un tiempo razonable (eficiente en tiempo)

Para VERIFICAR/COMPROBAR la solución del Sudoku, solo tenemos que verificar las filas y columnas. Esto se puede lograr en un tiempo polinomial.
=> NP



VI. Problema del Milenio

Hasta el momento, el problema de las N-Reinas, como el Sudoku generalizado N, no tienen una forma de resolverlos en tiempo polinomial; sin embargo si podemos verificar su solución en un tiempo polinomial \Rightarrow Son Problemas tipo **NP**



VII. NP-Hard y NP-Completo

Problemas NP-Hard

Podemos reducir el Problema B al Problema A si, dada una solución al Problema A, puedo construir fácilmente una solución al Problema B. (En este caso, "fácilmente" significa "en tiempo polinomial")

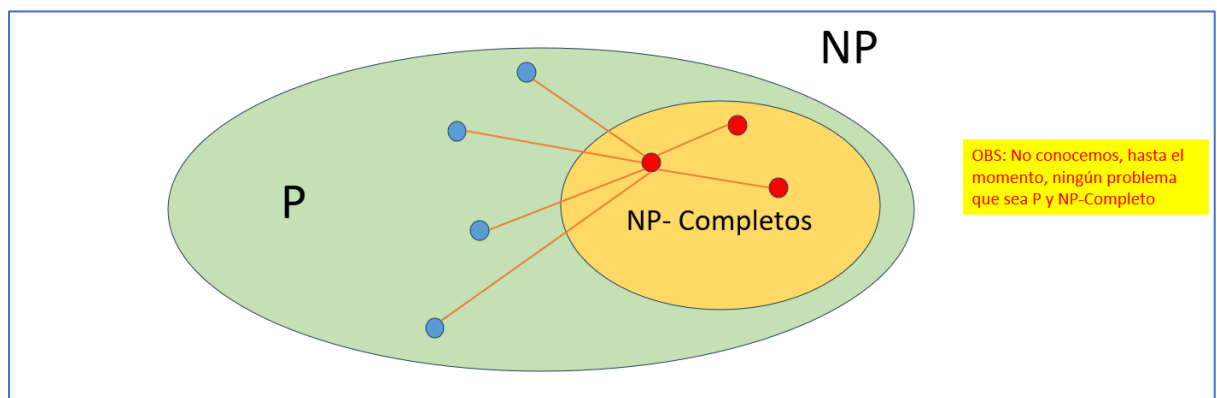
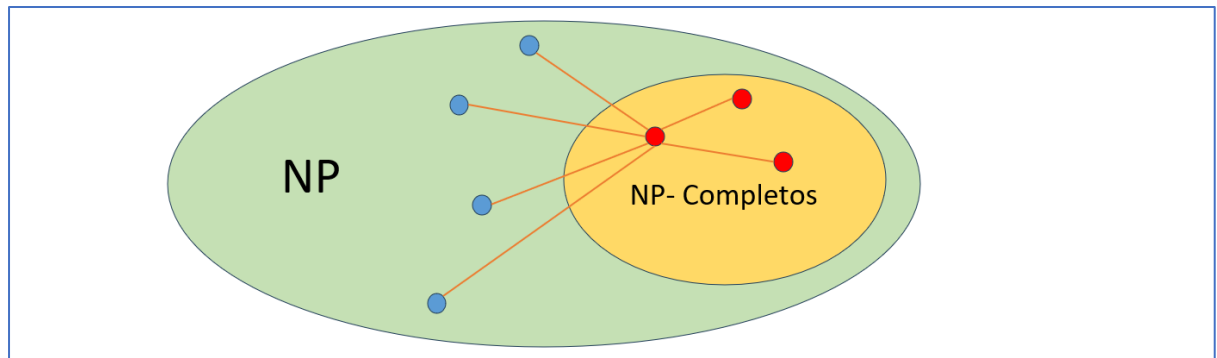
=> Un problema es **NP-Hard** si todos los problemas en NP se reducen a tiempos polinómicos.

Problemas NP-Completo

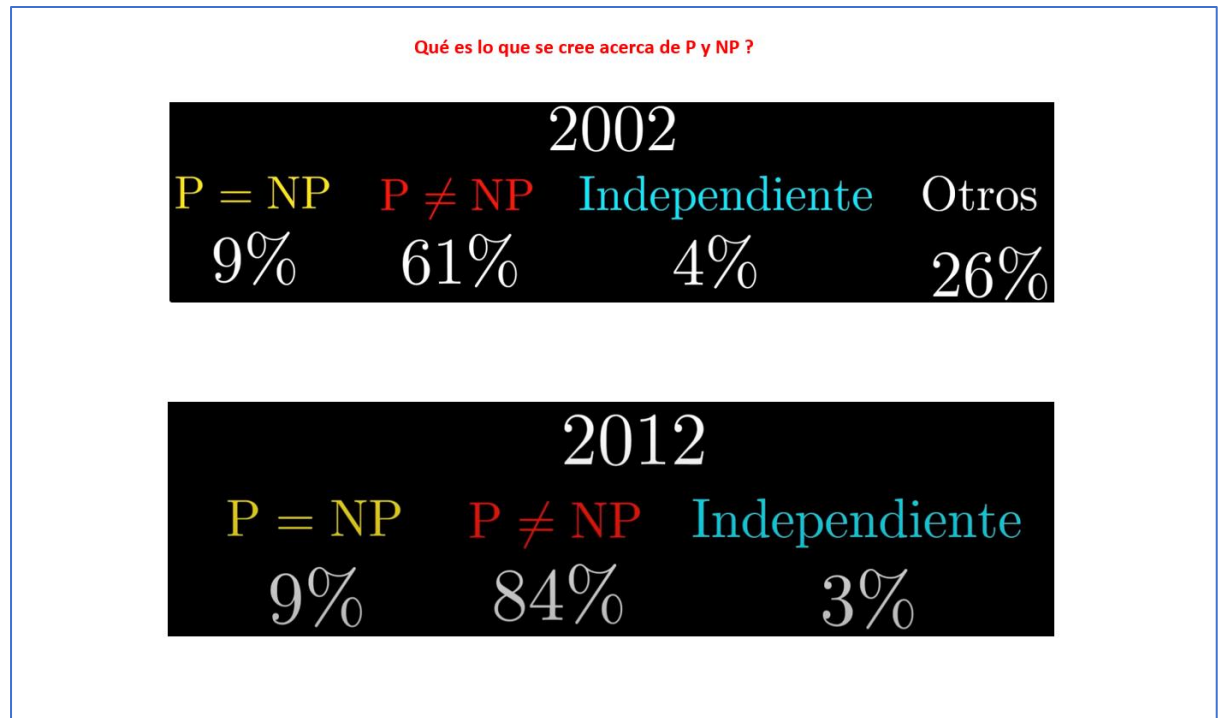
Los problemas NP-Completo están conectados a los problemas NP. Entonces si podemos resolver los problemas NP-Completo (rojos) en tiempo polinómico, entonces los problemas NP (azules) también se podrían resolver en tiempo polinómico, ya que están conectados.

Es decir, los problemas P se pueden REDUCIR a NP-Completo de forma polinómica.

Un problema es NP-completo si el problema es a la vez NP-Hard y NP.



VIII. Estadísticas



Fuente de Referencia: <https://www.youtube.com/watch?v=1x4VbYerGsA>