¿Y qué si P = NP?

ALGORITMICA

Photo Loic Djim on unsplash.com

Francisco Navarro Morales - GRG121

Segundo curso del Grado de Ingeniería Informática
Universidad de Granada
curso 2016-2017

Llamamos problemas P a aquellos para los que existe un algoritmo eficiente (tiempos de ejecución como funciones polinomiales) que puede ejecutarse en una maquina de Turing determinista, y NP a aquellos problemas para los que la única manera de obtener una respuesta en tiempo eficiente es a través de una etapa aleatoria en la que se establece una solución al azar y se comprueba en tiempo eficiente si esta es correcta. Sin embargo, debido a ese factor aleatorio, los tiempos deseados pueden no darse; para asegurar la ejecución en tiempo eficiente (orden polinómico) necesitaríamos una máquina de Turing no determinista (concepto ficticio), que sería algo así como una máquina capaz de "duplicarsez realizar tantas operaciones en paralelo como quisiera.

Ahora bien, **¿es P = NP?**

Podemos afirmar que $P \subseteq NP$ puesto que, cualquier problema para el que exista un algoritmo con eficiencia de orden polinómico podría ser resuelto por los métodos propios de algoritmos NP; esto es, una maquina de Turing no determinista podría ejecutar cualquier problema P simplemente no clonándose ninguna vez. Ahora bien, si $NP \subseteq P$ y, por tanto $P = NP$, entonces significaría que cualquier algoritmo de la clase NP podría realizarse en un orden de tiempo polinómico con una máquina de Turing determinista y, por tanto, las implicaciones serían cuantiosas.

Y es que, si por ejemplo, necesitáramos encontrar la clave para desencriptar un fichero, una máquina de Turing no determinista podría comprobar todas las claves posibles y determinar cual es la correcta en el mismo tiempo en que una máquina determinista comprobaría si una clave es correcta; sin embargo, dado que las máquinas no deterministas son sólo elementos teóricos, conseguir desencriptar un archivo en tiempo eficiente es imposible. Sin embargo, si $P = NP$, entonces existe un algoritmo tal que una máquina determinista (a las cuales sí tenemos acceso) podría realizar la labor que comentábamos propia de una no determinista en el mismo orden de tiempo, proporcionándonos la posibilidad de desencriptar cualquier archivo (que haya sido encriptado teniendo en cuenta las propiedades de los problemas NP) en un tiempo muy breve.

Esto supone aún más, si supiéramos que $P = NP$ significaría que es sólo cuestión de tiempo ir encontrando algoritmos polinómicos para problemas de la clase NP y, al encontrarlos, podríamos conseguir respuestas para las que esperamos durante meses o años, en cuestión de horas, minutos o segundos; es decir, podríamos obtener una respuesta para la que un supercomputador ha estado trabajando durante un año en menos de una hora sin necesidad de un ordenador especialmente potente, y obtener respuestas que nos sería imposible obtener a día de hoy. Imagina una pregunta para la cual una computadora podría ofrecer una respuesta dentro de 1000 años, la única manera que tendríamos a día de hoy de saber esa respuesta antes de morir sería (aunque es casi tan improbable como vivir 1000 años) viajar en el tiempo para ver la respuesta que dará el ordenador dentro de 1000 años, y luego volver para poder compartirla. Sin embargo, si $P = NP$, entonces no necesitaríamos ese hipotético viaje en el tiempo, podríamos adelantar la respuesta a nuestro tiempo.

Además, esto supondría sin lugar a dudas una nueva revolución tecnológica puesto que permitiría el avance de numerosos estudios en muy poco tiempo y el desarrollo mucho más eficiente de nuevas tecnologías. No obstante, aunque aún es una cuestión abierta, los indicios actuales apuntan a que $P! = NP$, que es la principal hipótesis de los que intentan encontrar una demostración matemática al respecto, ya que parece imposible que fuera real que $P = NP$. En caso de que la mayoría tuviera razón y $P! = NP$, lo único que ganaríamos sería la certeza de que nuestros sistemas actuales de encriptación son seguros, y que es una pérdida de tiempo intentar encontrar soluciones eficientes a los problemas NP, pero esto no supondría ninguna revolución científica ni mucho menos. Es por esto que quizá sería conveniente no descartar del todo la posibilidad de que todos los problemas pertenezcan a un mismo grupo hasta que se demuestre lo contrario, pues si algún día se llegara a demostrar que esta hipótesis es correcta, se produciría un avance tecnológico que afectaría a todo el mundo.