

TECNOLOGÍA

Bits, Ciencia y Sociedad


 ago 18 **El más famoso problema de la computación: ¿resuelto?**

 Posteado a las 18 de Agosto de 2010 - 12:02  12 comentarios

 Tweet 0

 Me gusta


Por Pablo Barceló, profesor del Depto. de Ciencias de la Computación, FCFM, de la Universidad de Chile

Hace poco más de una semana, Vinay Deolalikar, un científico de HP en California, anunció haber resuelto el más grande y famoso problema abierto en ciencia de la computación: el de si la clase P es o no igual a la clase NP (es decir, ¿ $P = NP$?). **Deolalikar cree haber demostrado matemáticamente que estas clases son diferentes, que -vale decir- es lo que la mayoría de los científicos de la computación creemos, pero nadie ha podido demostrar en más de 30 años.** El argumento de Deolalikar se halla lleno de conexiones novedosas y parece un intento serio de resolver el problema por parte de un científico que ciertamente sabe de lo que está hablando. Sin

embargo, esto no es suficiente como para proclamar aún que el problema esté resuelto: la demostración, para considerarse correcta, primero tiene que ser estudiada y verificada por los expertos del área (o en palabras del gran matemático ruso Yuri Manin: "Una demostración sólo se vuelve una demostración luego del acto social de aceptarla como tal"). Y esto, para una demostración de casi 100 páginas, y con interacciones de áreas muy distintas de la matemática, no es un tema sencillo (toma bastante tiempo y esfuerzo).

Vamos por parte. Primero, **¿de qué se trata el problema de si $P = NP$?** Existe una gran clase de problemas computacionales que pueden ser resueltos "fácilmente" por nuestros computadores modernos. Por ejemplo, piense en el siguiente problema: dado un sistema de ciudades y de distancias entre ellas, ¿cuál es el camino más corto que permite ir desde la ciudad A hasta la ciudad B? Este es un problema que (en términos gruesos) puede ser resuelto sin mayor complejidad por cualquier sistema computacional de la actualidad. Una justificación teórica de este hecho es que puede ser resuelto en tiempo polinomial por un modelo abstracto de lo que llamamos computador. Todos los problemas que tienen esta buena propiedad se pueden meter a un mismo saco, el de la clase de problemas que pueden ser resueltos eficientemente: a tal saco de problemas se le denomina la clase de complejidad **P** (por tiempo polinomial).

Por otro lado, existen muchos otros problemas muy naturales, que no caben en esta clase, y que además no se sabe cómo resolver eficientemente con nuestros sistemas computacionales (de hecho, no son posibles de resolver incluso si mejoráramos de modo increíblemente sustancial esos sistemas). Por ejemplo, dada la misma red de ciudades mencionada en el párrafo anterior, ¿es posible que un vendedor viajero comience en una ciudad A y recorra cada ciudad de la red tan sólo una vez hasta volver a A? Este problema (conocido por razones obvias como el del vendedor viajero) no es sólo teórico, sino que además tiene aplicaciones en áreas tan diversas como secuenciamiento de genomas, diseño optimal de rutas, etc. Las mejores formas conocidas de solucionar el problema del vendedor viajero toman tiempo exponencial (en el peor caso), y por tanto se vuelven violentamente prohibitivas para entradas de mediano tamaño (por ejemplo, para una red de 100 ciudades este método requeriría, en el peor caso, 2^{100} operaciones, que es un número enorme). Muchos de estos problemas "difíciles de resolver", incluyendo el del vendedor viajero, se clasifican en una clase de complejidad más técnica llamada **NP** (por tiempo polinomial no determinista). Aunque se cree que muchos de estos problemas no se pueden resolver eficientemente -es decir, que no pertenecen a la clase P- nadie hasta ahora ha podido demostrar este hecho. **En otras palabras, nadie hasta ahora ha podido demostrar que P no es igual a NP. A menos que Deolalikar lo haya logrado.**

Pero, ¿cuál sería la relevancia de que estas clases fueran realmente distintas? Bueno, aparte de que Deolalikar se haría rico por resolver uno de los 7 problemas matemáticos abiertos más importantes, y que la computación habría resuelto su problema teórico más desafiante, sin duda hay que reconocer que la vida de cualquiera de nosotros ciudadanos pedestres no cambiaría en lo más mínimo (sin embargo, lo mismo se podría decir de una gran mayoría de los descubrimientos científicos de cada día, con la honorable excepción de algunos descubrimientos biológicos y médicos). **Por otro lado, una demostración de que P es efectivamente igual a NP -y, por tanto una demostración que contradiga lo que la mayoría de los científicos creen, y lo que, en particular, Deolalikar pretende estar probando- podría llegar a tener consecuencias enormes en la práctica de la computación, en especial si tal demostración muestra efectivamente cómo resolver eficientemente ciertos problemas complejos.** Por ejemplo, tal demostración podría ayudar a romper los códigos criptográficos usados en los trasposos electrónicos entre bancos y en telecomunicaciones.

Ya ha pasado más de una semana de intensas discusiones sobre la demostración de Deolalikar (ver, por ejemplo, en el blog de Richard Lipton <http://rjlipton.wordpress.com/>). La sensación general es que, por un lado, las ideas en la demostración han traído nuevos aires al estudio del problema y que es muy bueno que los investigadores se interesen en estos problemas grandes y difíciles, pero que, por otro, hay varios detalles en la demostración que son al menos dudosos, y que es muy probable que la demostración no sea correcta. Conociendo personalmente bastante bien una línea de los ataques que se le está haciendo a la demostración (la que tiene que ver con métodos lógicos en computación) me atrevería a aventurar que la demostración, como está ahora, es falsa. Otra cosa es si la demostración actual puede ser arreglada: me temo que la respuesta a esta pregunta es también negativa. Sin embargo, es probable que algo interesante finalmente salga de ella, por ejemplo, la separación de otras clases más débiles de complejidad, o el estudio de ciertas relaciones interesantes entre propiedades probabilistas y clases de complejidad.

Habiendo leído parte de la demostración, uno se da cuenta que refutar una demostración de este alcance es una cosa bastante compleja. **En el caso de la propuesta de Deolalikar el mayor problema radica en que muchas de las suposiciones matemáticas que utiliza están sólo bosquejadas, a menudo no desarrolladas completamente.** Para mí esto no es forma de presentar una solución científica, menos de un problema de esta naturaleza. Además, lo que sucede es que el tipo de errores potenciales en la demostración de Deolalikar no son nunca tan claros como el tipo de afirmaciones $2+2=3$, sino que más bien aparecen en afirmaciones de si A y B son ciertos entonces obviamente C es cierto. El demostrar que obviamente C es cierto a partir de A y B es dejado al lector. Entonces, cuando alguien sugiere que no obviamente C se sigue de A y B, siempre es posible para Deolalikar reformular sus hipótesis o decir que hay que pensarlo con más detalle. Esto no quiere decir que Deolalikar esté engañando, sino que dentro de la complejidad de una demostración hay detalles que no pensó con todo cuidado. Detalles que podrían ser falsos, pero que también podrían ser ciertos cuando se demuestren y formalicen con mayor rigurosidad.

Tags:



perfil del autor



El blog Bits, Ciencia y Sociedad de la sección de Tecnología de Terra es un espacio donde académicos del Departamento de Ciencias de la Computación de la Universidad de Chile hablarán de la Tecnología y su impacto político y social en nuestro país.

Aquí escribirán semanalmente José Miguel Piquer, Claudio Gutiérrez, Juan Álvarez, Tomás Barros, Nancy Hirschfeld, Benjamin Bustos, Alejandro Hevia, Pablo Barceló y Cecilia Bastarrica."

posteos

 VER: **MÁS RECIENTES** MÁS COMENTADOS

Aplicación de la Ley de Neutralidad

25 de Julio de 2011 - 16:07

¡Contra el virus del lucro!

13 de Julio de 2011 - 8:54

¿Es regresivo apoyar a las universidades tradicionales?

7 de Julio de 2011 - 13:33

"Protestas 2.0"

30 de Junio de 2011 - 11:31

La Revolución Pingüina 2.0

22 de Junio de 2011 - 10:20

Se solicita

Personas que quieran mejorar sus ingresos mensuales!

Empresa de Mercado de Divisas requiere personas con o sin experiencia para operar en el mundo Forex convirtiéndolo en un hombre de éxitos y ganancias.

► **Consulte aquí** ◀

últimos comentarios

“ Seria tambien bueno recordar, que esto sucedio hace mas... ”

Claudio en ¡Contra el virus del lucro! ►

“ Buen post... ahora hay que entender, que para que... ”

Victor en Aplicación de la Ley de Neutralidad ►

“ Un verdadero fraude para los mismos clientes chilenos que... ”