**Enero 21, 2010**

## Rabin: En el reino de lo incierto y lo indeterminado

Categoría: Sin categoría — Tags: El no determinismo, Michael Rabin, Pablo Barceló — dccuchile - 11:40 am

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

Como lo dice su propio nombre, la Ciencia de la Computación estudia la posibilidad de computar cosas, o en términos técnicos, de resolver problemas algorítmicamente (forma de resolver un problema siguiendo un número fijo de instrucciones, es decir, sin pensar). Para poder entender la noción de computación, y por ende, de algoritmo, es conveniente tener una máquina que sea capaz de computar. En la teoría de la Computación tal máquina se denomina de Turing (de quien ya hemos hablado), una de cuyas posibles implementaciones corresponde al computador moderno.

Detengámonos un momento en la noción de algoritmo, y en particular, en la de instrucción. Un algoritmo es un conjunto de instrucciones que permiten resolver un problema complejo, por ejemplo, determinar si un número es primo. El algoritmo termina después de un número finito de pasos con la respuesta al problema. Por ejemplo, si quiero saber si el número 17 es primo ejecuto las instrucciones del algoritmo paso a paso hasta finalizar. Y al hacerlo el algoritmo debiera responder de manera afirmativa (es decir, debiera reconocer al 17 como número primo).

Esta es la noción clásica. Sin embargo, tempranamente los científicos de la Computación se dieron cuenta que la noción de algoritmo se podía hacer mucho más versátil si se la enriquecía con conceptos tan usuales en la vida diaria como la incertidumbre y la indeterminación. Tales conceptos fueron estudiados por muchos científicos destacados del siglo XX, pero a mi modo de ver nadie llegó tan lejos en ambos en paralelo como Michael Rabin.

Rabin es un abuelito de 1,60 m a quien le brillan los ojos cuando habla de computación y matemáticas. Actualmente es profesor emérito de Harvard, además de haber recibido el Turing Award en 1976. Es una especie de geniecillo israelita que un matemático salvó del ejército para que terminara su magíster y doctorado en un par de años, resolviendo un par de problemas abiertos en el camino. Luego de finalizar ese doctorado se fue a IBM donde - junto con Dana Scott - comenzó a trabajar en uno de los temas de esta columna: El no determinismo.

Suponga que está resolviendo un problema y que el algoritmo que está usando contiene una bifurcación, es decir, en algún paso éste le dice lo siguiente: para poder resolver el problema en este momento usted debe elegir entre ejecutar la acción A o la B, una de las cuáles -no sabemos cuál - le llevará a la respuesta correcta. En ese caso decimos que el algoritmo es no determinista, lo que usualmente en Computación se modela usando máquinas de Turing no deterministas. Esta noción es fundamental en nuestra disciplina. Y aunque en general el no-determinismo no permite resolver más problemas que los que se pueden resolver de manera determinista, sí permite construir algoritmos mucho más concisos y elegantes para ciertos problemas naturales. El trabajo de Rabin y Scott se centró en ciertos casos particulares bastante simples de las máquinas de Turing - llamados autómatas - para los cuales la noción de no-determinismo es clave.

Pasemos entonces a otra extensión de los algoritmos tradicionales: la incertidumbre. Imagine que su algoritmo es bueno aunque no infalible. Es decir, el algoritmo falla pero sabemos que acierta más de lo que falla (es decir, la probabilidad de fallar es estrictamente menor a 50%). Si corremos el algoritmo en un número y éste nos responde que es primo, no podremos estar seguros del hecho. Pero si corremos el algoritmo nuevamente y nos vuelve a decir que el número es primo, entonces estaremos un poco más seguros que esto es así. Si lo corremos diez veces y las diez veces el algoritmo nos entrega la misma respuesta, aún no estaremos seguros. Pero la probabilidad de que no lo sea será menor a 0,01%. Si lo repetimos cien veces y las cien veces nos dice que es primo, podremos estar practica, aunque nunca completamente, seguros de que el número es primo. O en palabras de Rabin: *"La probabilidad de error es menor que la probabilidad de que ninguno de nosotros esté despierto y estamos todos soñando lo que está sucediendo".*

Rabin fue precisamente uno de los impulsores de los algoritmos probabilistas en Computación, área que ha tenido un impacto realmente enorme en los últimos 30 años. Uno de los primeros algoritmos probabilistas que desarrolló Rabin fue el que permitía verificar si un número es primo. Existen varios algoritmos deterministas que permiten verificar esta propiedad, pero todos ellos son demasiado

### Archivos



### Otros Blogueros

complejos para poder ser implementados en la práctica. Por otro lado, el algoritmo de Rabin no sólo puede ser implementado eficientemente, sino que hoy por hoy es una de las bases sobre las que trabaja la industria de la encriptación de mensajes, en especial en la Web y las comunicaciones. Este es un tema sobre el que hablaré en la próxima columna: RSA, el algoritmo desarrollado por Rivest, Shamir y Adleman para intercambiar mensajes que necesitan ser codificados y luego decodificados.

permalink trackback
Comentarios (0)
« Older Posts