Pruebas de conocimiento cero

Andrea González Luis Mayo Carlos Acosta

11 de junio de 2017

Índice

1. Introducción

En nuestras experiencias tanto dentro como fuera del mundo académico, por lo general se nos exige (esto no aplica en el caso de Jorjona) que cualquier proposición comunicada al otro, sea sustentada con evidencias claramente expuestas como acompañamiento de nuestra declaración. A fin de inducir en ella un carácter de verdad, la defensa de nuestros enunciados debe apoyarse de argumentos que conserven su validez dentro del objetivo que perseguimos.
Pero, ¿qué ocurre cuando no podemos permitir que nuestra audiencia se entere de los detalles del camino que nos condujo al resultado que le presentamos?, ¿es posible mantener la confiabilidad, sin necesidad de proveer información más allá de la afirmación de que lo que decimos es verdad?
Sin cruzar apresuradamente al terreno de la magia o de la fe, consideremos primero la noción de las ***pruebas de conocimiento cero***. Imaginemos que estamos solicitando un trabajo para una organización o empresa y es necesario que les convenzamos de nuestra valía, sin embargo toda la experiencia con la que contamos ha sido obtenida en los círculos del bajo mundo o la clandestinidad y no estamos en libertad de proporcionar un *curriculim vitae* o documento que demuestre nuestra competencia. En ese caso la empresa podría someternos a un periodo de prueba que consista en resolver problemas o tareas que atañen a nuestras habilidades, aún sin conocer el proceso que estamos llevando a cabo para ninguna de ellas -ya que no podemos revelar dichas técnicas por su naturaleza secreta-, entre más labores sean requeridas más certeza tendrán de aceptar nuestra solicitud de trabajo y menor probabilidad de que estemos engañándolos. Así, en una prueba de conocimiento cero, si A busca probar a B que una proposición X es verdadera, al término del proceso A estará completamente convencida de X, pero no habrá obtendido nuevo conocimiento (not arora but barak [1]). De ahí el nombre.

l'histoire et la relevance

2. Sistemas de Demostración Interactivos

La clase de complejidad IP [1]

3. Aplicaciones

4. Instancia

4.1. Análisis

5. Conclusiones

Referencias

[1] Arora, S., Barak, B. *Computational complexity: a Modern Approach.* Beijing: World Publishing Corporation. 2012.

[2] Goldwasser, S., Micali, S., Rackoff, C. *The knowledge complexity of interactive proof-systems.* Proceedings of the seventeenth annual ACM symposium on Theory of computing - STOC 85. doi:10.1145/22145.22178. 1985.

[3] Quisquater, Jean-Jacques; Guillou, Louis C.; Berson, Thomas A. *How to Explain Zero-Knowledge Protocols to Your Children.* Advances in Cryptology - CRYPTO '89: Proceedings 435: 628-631. 1990.