Complexidade Computacional De Problemas de Curvas Elípticas

Campinas, 19 de Junho de 2015

Apresentado por

Thomas Michael Bartlett
DCA-FEEC-UNICAMP
Campinas

Resumo

Não é novidade que o intercâmbio de ideias de Computação e Geometria Algébrica é interessante. Dessa forma, tendo como base [1] e [2], nessa palestra serão apresentados dois problemas ditos NP-difíceis no estudo de curvas elípticas, o cálculo da distância de Hamming e a decodificação de máxima verossemelhança. Num primeiro momento, será dada uma introdução da definição de Máquina de Turing e da definição da classe de problemas P , NP e NP-completos. Dessa maneira será possível demonstrar que o cálculo da distância de Hamming entre duas palavras-código gerados por um código algebro-geométrico é NP-difícil a partir de uma redução polinomial randomizada do problema de soma de subconjunto. Usando esse resultado serão enunciados os resultados provados em [1] que dão suporte ao fato de a decodificação de máxima verossemelhança é NP-difícil. Como perspectiva de trabalho futuro, serão feitos comentários a cerca do plano de conjecturas de Ketan Mulmuley [3] e como elas se encaixam no estudo de curvas elípticas.

Referências

[1] CHENG, Qi. Hard problems of algebraic geometry codes. Information Theory, IEEE Transactions on, v. 54, n. 1, p. 402-406, 2008.

[2] COOPER, S. Barry. Computability theory. CRC Press, 2003.

[3] MULMULEY, Ketan D.; SOHONI, Milind. Geometric complexity theory I: An approach to the P vs. NP and related problems. SIAM Journal on Computing, v. 31, n. 2, p. 496-526, 2001.