A FAST ALGORITHM FOR COMPUTING BINOMIAL COEFFICIENTS MODULO POWERS OF TWO

Ph.D. Eng. MUGUREL IONUȚ ANDREICA[1]

Abstract

In this paper I present a new algorithm for computing binomial coefficients modulo 2^N. The proposed method has an $O(N^3 \cdot Multiplication(N))$ preprocessing time, after which a binomial coefficient $C(P,Q)$ with $0 \le Q \le P \le 2^N-1$ can be computed modulo 2^N in $O(N^2 \cdot \log(N) \cdot Multiplication(N))$ time. Multiplication(N) denotes the time complexity of multiplying two N-bit numbers, which can range from $O(N^2)$ to $O(N \cdot \log(N) \cdot \log(\log(N)))$ or better. Thus, the overall time complexity for evaluating M binomial coefficients $C(P,Q)$ with $0 \le Q \le P \le 2^N-1$ modulo 2^N is $O((N^3+M \cdot N^2 \cdot \log(N)) \cdot Multiplication(N))$. After preprocessing we can actually compute binomial coefficients modulo any 2^R with $R \le N$. For larger values of P and Q variations of Lucas' theorem must be used first in order to reduce the computation to the evaluation of multiple ($O(\log(P))$) binomial coefficients $C(P',Q')$ (or restricted types of factorials $P'!$) modulo 2^N with. $0 \le Q' \le P' \le 2^N-1$.

[1] Computer Science Department, Politehnica University of Bucharest, Bucharest, Romania, email: mugurel.andreica@cs.pub.ro