Cryptology ePrint Archive: Report 2011/245

On the Number of Carries Occuring in an Addition $\mod 2^k-1$

Jean-Pierre Flori and Hugues Randriam

Abstract: In this paper we study the number of carries occurring while performing an addition modulo 2^k-1. For a fixed modular integer t, it is natural to expect the number of carries occurring when adding a random modular integer a to be roughly the Hamming weight of t. Here we are interested in the number of modular integers in $\Zk$ producing strictly more than this number of carries when added to a fixed modular integer $t \in \Zk$. In particular it is conjectured that less than half of them do so. An equivalent conjecture was proposed by Tu and Deng in a different context~\cite{DCC:TD}.

Although quite innocent, this conjecture has resisted different attempts of proof~\cite{DBLP:conf/seta/FloriRCM10, cryptoeprint:2010:170, cusick_combinatorial_2011, Carlet:Private} and only a few cases have been proved so far. The most manageable cases involve modular integers t whose bits equal to $\textttup{0}$ are sparse. In this paper we continue to investigate the properties of $\Ptk$, the fraction of modular integers a to enumerate, for t in this class of integers. Doing so we prove that $\Ptk$ has a polynomial expression and describe a closed form of this expression. This is of particular interest for computing the function giving $\Ptk$ and studying it analytically. Finally we bring to light additional properties of $\Ptk$ in an asymptotic setting and give closed forms for its asymptotic values.

Category / Keywords: foundations / boolean functions

Date: received 16 May 2011

Contact author: flori at enst fr