Algebra and Number Theory Seminar

Title: Cross correlation of m-sequences : An overview and recent results on five-valued correlations

Speaker: Tor Helleseth (University of Bergen, Norway)

Date: Mon 7th April 2008 at 4:00PM

Location: Mathematical Sciences Seminar Room

Abstract: Let a$_t$ $and b_t between two binary sequences of period n. The cross correlation function between the set u$
$n, is defined by C(?) = sum_{t=0}^{n} (-1)^{a_{t+?}+b_t}$.

A maximal linear sequence, or an m-sequence, is a sequence s$_t$ $of period 2^m ?1 that obeys a linear recursi$
$sequences in modern communication system. Finding the cross correlation between two m-$
$sequences s_t and s_d of the same period 2^m ?1, that differ by a decimation d where gcd(d, 2^m ?1) =$
$1, is a problem that has been thoroughly studied for the last 40 years.$

In the first part of the talk we give an overview of known results on three and four-valued cross correlation as well as a discussion of some open general problems in this area. In the second part we present some recent results devoted to special values of d of the form d =$(2^l + 1)/(2^k + 1)$.

In some cases these are known to lead to at most five-valued cross correlation. In particular Kasami and Welch showed that the cross correlation is three-valued for l

$= 3k$. The complete correlation distribution for other values of k and l that frequently lead to five-valued correlation is an open problem. We discuss the apparently simple and previously unsolved special case when $l = 2k$, $k = 1$ and m odd. The correlation distribution is completely determined and showed to be five-valued. The results are proved by using evaluations of several exponential sums including Kloosterman sums that may explain why related cases appear rather hard to solve.