



UCD School of
Mathematics and Statistics

University College Dublin
Belfield, Dublin 4, Ireland

Tel +353 1 716 2580
Fax +353 1 716 1196

Scoil na
Matamaitice agus na Staitisticí UCD

An Coláiste Ollscoile, Baile Átha Cliath
Belfield, Baile Átha Cliath 4, Éire

Email seminars@maths.ucd.ie
Web maths.ucd.ie/seminars

Algebra and Number Theory Seminar

Tor Helleseth (University of Bergen, Norway)

will speak on

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

Mon 7th April 2008 at 4:00PM

Location: Mathematical Sciences Seminar Room

Let a_t and b_t be two binary sequences of period n . The cross correlation function between the setwise sequences at shift t , where n , is defined by $C(t) = \sum_{i=0}^{n-1} (-1)^{a_{t+i} + b_i}$.

A maximal linear sequence, or an m-sequence, is a sequence s_t of period $2^m - 1$ that obeys a linear recursion with characteristic sequences in modern communication system. Finding the cross correlation between two m-sequences s_t and s_{t+d} of the same period, 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



**UCD School of
Mathematics and Statistics**

University College Dublin
Belfield, Dublin 4, Ireland

Tel +353 1 716 2580
Fax +353 1 716 1196

**Scoil na
Matamaitice agus na Staitisticí UCD**

An Coláiste Ollscoile, Baile Átha Cliath
Belfield, Baile Átha Cliath 4, Éire

Email seminars@maths.ucd.ie
Web maths.ucd.ie/seminars

sums including Kloosterman sums that may explain why related cases appear rather hard to solve.

This talk is part of the **Algebra and Number Theory** series. For more, see <https://maths.ucd.ie/seminars>