

Primitive polynomials in extended Galois fields

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2007-03/msg00786.html>

- *From:* "Anup" <anupkc@xxxxxxxxxx>
 - *Date:* 27 Mar 2007 05:15:23 -0700
-

Hello All

I am trying to generate multi-level sequences in extended Galois fields, GF(4) to be precise, which satisfy the de Bruijn or window property.

The approach I followed was to use a Linear Shift Register with a primitive polynomial in GF(4) as the generator polynomial. But this requires the primitive polynomials to be generated in the extended finite field. For this I could hardly find any fast algorithm. So I resorted to generating irreducible polynomials (using the inbuilt function from the NTL library at <http://shoup.net/ntl/>) and checking them for primitivity – by ensuring that they are of maximal order.

But this seems to be a costly exercise, since finding out the order requires $4^{\text{degree}-1}$ division checks. (where degree is the degree of primitive polynomial to be generated). This requires quite a lot of time when the degree is more than , say 7. So can somebody suggest a faster method or at least some pointers to any algorithm for this.

Thank you in advance
Anup

.