

Re: Multilevel sequences in extended Galois fields

Source: <http://sci.tech--archive.net/Archive/sci.math.research/2007-03/msg00119.html>

- *From:* Thomas Womack <twomack@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Tue, 27 Mar 2007 21:00:14 +0000 (UTC)
-

In article <eu8u72\$25m\$1@xxxxxxxxxxxxxxxxxxxx>, analhaq@xxxxxxxxxx <analhaq@xxxxxxxxxx> wrote:

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 maximum order.

The order has to be a factor of $4^{\text{degree}} - 1$, so you don't have to check all that many powers of x; and you can calculate x^{2n} by squaring x^n modulo the irreducible polynomial.

What I'd recommend is using a fully-fledged computer algebra package; the one I know is Magma, you can evaluate things on-line at <http://magma.maths.usyd.edu.au/calc/>.

Try the program

```
g:=GF(4); t:=g.1; P<x>:=PolynomialRing(g);
deg:=10;
for r in [1..1000] do
tmp:=x^deg+P![Random(BaseRing(P)) : r in [1..deg]];
if (IsPrimitive(tmp)) then print tmp; end if;
end for;
```

which will produce you some primitive polynomials of degree 10; change the value of 'deg' to get primitive polynomials of a different degree.

'g.1' and 'g.1^2' are the two elements of the GF(4) which aren't 0 and 1.

Re: Multilevel sequences in extended Galois fields

Tom

.