T800 TGFSR A twisted GFSR

25 words x 32 bits = 800 bits

 based on $LGFSR(25, x^{25} + x^{18} + 1)$ twisting vector $\mathbf{a} = \mathbf{0x8ebfd028}$ In [13]: f:x^25+x^18+1 Out[13]: $x^{25} + x^{18} + 1$ In [14]: gf_primitive_poly_p(f,2) Out[14]: **true** In [15]: a:diagmatrix(31,1)\$ Out[15]: n

 1 of 4 4/10/18, 2:14 PM

```
Out[16]:
    0
    0
    0
    0
    0
    0
    0
    0
    0
    0
    0
    0
    0
    0
    0
    0
    0
    0
    0
    0
    0
    0
    0
    0
    0
    0
```

2 of 4 4/10/18, 2:14 PM

3 of 4 4/10/18, 2:14 PM

```
In [ ]: d:charpoly(a,t^25+t^18)
In [ ]:
```

4 of 4 4/10/18, 2:14 PM