

Table of Low-Weight Binary Irreducible Polynomials

Gadiel Seroussi
Computer Systems Laboratory
HPL-98-135
August, 1998

finite fields,
irreducible
polynomials

A table of low-weight irreducible polynomials over the finite field F_2 is presented. For each integer n in the range $2 \leq n \leq 10,000$, a binary irreducible polynomial $f(x)$ of degree n and minimum possible weight is listed. Among those of minimum weight, the polynomial listed is such that the degree of $f(x) - x^n$ is lowest (similarly, subsequent lower degrees are minimized in case of ties). All the polynomials listed are either trinomials or pentanomials. The general question of whether an irreducible polynomial of weight at most 5 (or any other fixed odd weight $w \leq 5$) exists for every value of n is an open one. Low-weight irreducibles are useful when implementing the arithmetic of the finite field F_{2^n} , as the number of operations in the reduction of the product of two polynomials of degree $n - 1$ modulo an irreducible of degree n and weight w is proportional to $(w - 1)n$.

1 Background

Large finite fields are useful in the implementation of cryptographic protocols, and in particular in elliptic curve cryptography. Typical choices of fields include F_p , realized as the integers modulo a prime p , and F_{2^n} , often realized as the set of polynomials of degree at most $n-1$ in $F_2[x]$, modulo an irreducible polynomial $f(x) \in F_2[x]$ of degree n . It is the latter case that motivates this note.

From an algebraic point of view, for the purpose of implementing F_{2^n} , all choices of irreducible f for a given n are equivalent. However, choosing f of low *weight* (number of nonzero coefficients) can lead to more efficient implementation of the arithmetic of F_{2^n} , as the complexity of reducing a polynomial of degree $2n-2$ modulo f is proportional to $(w-1)n$, where w denotes the weight of f . For $n > 1$, the lowest possible weight is $w = 3$, i.e., f being a trinomial. The existence, distribution and other properties of irreducible trinomials over F_2 have been extensively studied in the literature. In particular, it follows from a theorem of Swan [5] that irreducible trinomials do not exist for $n \equiv 0 \pmod{8}$, and that they are rather scarce when $n \equiv 3$ or $5 \pmod{8}$; see also [1],[3], and references therein. The tables in [2] show that up to $n = 5,000$, irreducible trinomials exist for slightly over one half of the values of n .

When an irreducible trinomial of degree n does not exist, the next best choice is a pentanomial, e.g., $w = 5$. In the appendix, we present a table of low-weight binary irreducible polynomials of degree n in the range $2 \leq n \leq 10,000$. For each degree n in that range, an irreducible trinomial is listed if one exists; otherwise an irreducible pentanomial was always found and is listed. The table contains 5,148 trinomials and 4,851 pentanomials.

In fact, there is no known value of n for which an irreducible polynomial of weight $w \leq 5$ does not exist. The general question, however, is open for any fixed odd weight $w > 3$. The following heuristic argument would seem to reinforce the expectation that values of n for which irreducible pentanomials do not exist, if any, must be rare. The probability of a random polynomial of degree n being irreducible is roughly $1/n$ [3]. The number of pentanomials of degree n with constant coefficient equal to one is of the order of n^3 . Therefore, if the density of irreducibles among pentanomials is anywhere near their density among arbitrary polynomials of degree n , then the likelihood of finding an irreducible pentanomial of degree n should be very high. (A similar argument for trinomials pits a probability of $1/n$ against a number of trinomials of the order of n .)

The table in the appendix is organized as follows: A trinomial $x^n + x^j + 1$, $n > j > 0$, is represented by the pair n, j . A pentanomial $x^n + x^{j_1} + x^{j_2} + x^{j_3} + 1$, with $n > j_1 > j_2 > j_3 > 0$, is represented by the quadruple n, j_1, j_2, j_3 . Polynomials are listed in increasing order of n , going in each page from left to right first and top to bottom next. When a trinomial is listed, it has the lowest value j among all irreducible trinomials of the same degree. For pentanomials, the first irreducible in alphabetical order of (j_1, j_2, j_3) is listed (i.e., lowest j_1 , then lowest j_2 , then lowest j_3).

It should be noted that for all pentanomials listed, the value of j_1 is quite low, which has some other implementation advantages. The maximum value of j_1 for pentanomials in the table is $j_1 = 56$ for $n = 9760$. In fact, the value of j_1 for most pentanomials in the table is quite close to (and below) the real solution t to the equation $n = t(t-1)(t-2)/6$, consistent with the heuristic argument above. For $n = 10,000$, we have $t \approx 40$.

The polynomials in the table were generated with a C++ program based on V. Shoup's NTL library [4], using a deterministic irreducibility test. The first 2048 entries were independently verified with the Maple symbolic package. The table is available in machine-readable form from the author.

The choice of $n = 10,000$ as the stopping point for the table is quite arbitrary, and only intended to amply cover all presently envisioned cryptographic applications where F_{2^n} is used. It follows from the table that in implementing F_{2^n} for those applications, one can safely assume that an irreducible of weight $w \leq 5$ is available. Since binary irreducibility testing can be implemented quite efficiently, it should not be particularly difficult to extend the table to larger values of n .

References

- [1] E.R. Berlekamp. *Algebraic Coding Theory*. Aegean Park Press, Laguna Hills, 1984.
- [2] I.F. Blake, S. Gao and R.J. Lambert. Construction and distribution problems for irreducible trinomials over finite fields, in *Applications of Finite Fields*, D. Gollman, editor, Oxford: Oxford University Press, 1996.
- [3] R. Lidl and H. Niederreiter. *Finite Fields*, in *Encyclopedia of Mathematics and its Applications*, G.-C. Rota, editor, Addison-Wesley, 1983.
- [4] V. Shoup. NTL: A library for doing number theory, on the World Wide Web at <http://www.cs.wisc.edu/~shoup/ntl/>.
- [5] R.G. Swan. Factorization of polynomials over finite fields. *Pacific J. Math.*, **12**, pp. 1099–1106, 1962.

Appendix: Table of Low-Weight Binary Irreducible Polynomials for $2 \leq n \leq 10,000$.

| | | | | | | | | | |
|---------------|---------------|---------------|---------------|---------------|---------------|---------------|---------------|---------------|---------------|
| 9601,963 | 9602,21,5,2 | 9603,19,10,4 | 9604,13,11,9 | 9605,37,26,12 | 9606,15,12,1 | 9607,262 | 9608,14,13,1 | 9609,1526 | 9610,2883 |
| 9611,14,6,5 | 9612,93 | 9613,32,16,3 | 9614,4577 | 9615,361 | 9616,25,8,2 | 9617,1385 | 9618,16,3,1 | 9619,29,14,10 | 9620,557 |
| 9621,29,20,11 | 9622,2145 | 9623,2429 | 9624,31,17,7 | 9625,508 | 9626,7,6,1 | 9627,25,19,18 | 9628,31 | 9629,16,15,10 | 9630,37 |
| 9631,295 | 9632,30,23,5 | 9633,2333 | 9634,3075 | 9635,26,21,10 | 9636,515 | 9637,21,18,6 | 9638,21,19,13 | 9639,700 | 9640,33,7,3 |
| 9641,3287 | 9642,3591 | 9643,18,14,11 | 9644,1671 | 9645,9,7,6 | 9646,31,30,17 | 9647,1227 | 9648,31,24,21 | 9649,657 | 9650,32,18,11 |
| 9651,22,14,4 | 9652,2733 | 9653,22,15,2 | 9654,1969 | 9655,3558 | 9656,19,16,2 | 9657,1192 | 9658,3691 | 9659,15,14,8 | 9660,57 |
| 9661,22,14,6 | 9662,22,9,8 | 9663,446 | 9664,35,21,1 | 9665,2763 | 9666,435 | 9667,34,22,6 | 9668,225 | 9669,29,27,24 | 9670,35,34,3 |
| 9671,1086 | 9672,17,9,3 | 9673,3538 | 9674,759 | 9675,44,25,23 | 9676,3367 | 9677,30,27,12 | 9678,4277 | 9679,864 | 9680,25,6,2 |
| 9681,910 | 9682,3175 | 9683,46,37,21 | 9684,2405 | 9685,17,14,4 | 9686,2333 | 9687,2054 | 9688,20,9,2 | 9689,84 | 9690,1503 |
| 9691,17,14,1 | 9692,3381 | 9693,10,6,3 | 9694,50,18,17 | 9695,207 | 9696,36,27,21 | 9697,1201 | 9698,38,27,24 | 9699,30,6,1 | 9700,565 |
| 9701,23,12,3 | 9702,1533 | 9703,13,7,1 | 9704,7,3,2 | 9705,1802 | 9706,22,15,11 | 9707,26,15,1 | 9708,1753 | 9709,16,13,10 | 9710,30,15,9 |
| 9711,917 | 9712,27,19,17 | 9713,2933 | 9714,1227 | 9715,27,10,6 | 9716,263 | 9717,9,6,2 | 9718,46,29,11 | 9719,3492 | 9720,37,4,2 |
| 9721,171 | 9722,12,11,8 | 9723,32,29,25 | 9724,30,28,15 | 9725,14,8,5 | 9726,29,28,23 | 9727,760 | 9728,30,5,2 | 9729,938 | 9730,663 |
| 9731,16,12,10 | 9732,3747 | 9733,22,21,8 | 9734,4125 | 9735,2086 | 9736,15,7,6 | 9737,275 | 9738,3663 | 9739,15,14,2 | 9740,3015 |
| 9741,11,8,1 | 9742,30,18,15 | 9743,869 | 9744,36,9,2 | 9745,2361 | 9746,2559 | 9747,26,8,1 | 9748,889 | 9749,20,7,6 | 9750,833 |
| 9751,1093 | 9752,42,17,3 | 9753,1078 | 9754,3891 | 9755,6,5,1 | 9756,1701 | 9757,22,14,6 | 9758,1557 | 9759,706 | 9760,56,49,47 |
| 9761,2588 | 9762,4455 | 9763,30,18,1 | 9764,25,13,9 | 9765,28,17,11 | 9766,585 | 9767,1668 | 9768,41,23,22 | 9769,1390 | 9770,1091 |
| 9771,29,8,1 | 9772,741 | 9773,32,10,6 | 9774,401 | 9775,537 | 9776,24,19,1 | 9777,773 | 9778,24,18,15 | 9779,40,21,20 | 9780,711 |
| 9781,40,28,15 | 9782,161 | 9783,88 | 9784,38,37,9 | 9785,2036 | 9786,4147 | 9787,20,13,9 | 9788,2007 | 9789,17,8,2 | 9790,177 |
| 9791,390 | 9792,27,26,21 | 9793,339 | 9794,24,15,6 | 9795,26,5,4 | 9796,321 | 9797,35,32,2 | 9798,2677 | 9799,139 | 9800,42,41,10 |
| 9801,284 | 9802,12,10,3 | 9803,18,10,2 | 9804,1165 | 9805,22,21,18 | 9806,30,9,8 | 9807,337 | 9808,43,32,21 | 9809,19,15,10 | 9810,711 |
| 9811,41,28,27 | 9812,31,30,22 | 9813,26,17,12 | 9814,1545 | 9815,27,26,8 | 9816,46,33,22 | 9817,4420 | 9818,30,19,10 | 9819,18,4,3 | 9820,105 |
| 9821,34,23,18 | 9822,305 | 9823,144 | 9824,13,10,3 | 9825,2563 | 9826,22,10,7 | 9827,13,12,5 | 9828,207 | 9829,4,3,1 | 9830,1541 |
| 9831,1159 | 9832,39,37,25 | 9833,104 | 9834,32,25,7 | 9835,32,29,1 | 9836,18,13,10 | 9837,35,16,2 | 9838,25,19,12 | 9839,389 | 9840,49,47,13 |
| 9841,1788 | 9842,35,28,24 | 9843,18,12,2 | 9844,565 | 9845,38,18,11 | 9846,2349 | 9847,3537 | 9848,25,23,10 | 9849,329 | 9850,19,16,4 |
| 9851,11,6,5 | 9852,3379 | 9853,18,11,10 | 9854,317 | 9855,803 | 9856,36,15,1 | 9857,4386 | 9858,4235 | 9859,34,28,1 | 9860,2997 |
| 9861,33,18,16 | 9862,13,10,3 | 9863,1809 | 9864,35,32,21 | 9865,2604 | 9866,34,27,14 | 9867,26,8,2 | 9868,339 | 9869,23,8,6 | 9870,2681 |
| 9871,903 | 9872,13,11,3 | 9873,3842 | 9874,4279 | 9875,19,18,2 | 9876,183 | 9877,19,16,15 | 9878,573 | 9879,1181 | 9880,35,28,5 |
| 9881,27,7,5 | 9882,747 | 9883,35,34,11 | 9884,389 | 9885,38,15,3 | 9886,3673 | 9887,710 | 9888,33,6,4 | 9889,2019 | 9890,2583 |
| 9891,46,38,7 | 9892,31,4,1 | 9893,32,28,18 | 9894,27,7,1 | 9895,787 | 9896,39,38,26 | 9897,430 | 9898,23,13,5 | 9899,34,21,13 | 9900,11 |
| 9901,10,4,3 | 9902,27,19,10 | 9903,40 | 9904,21,10,2 | 9905,219 | 9906,2027 | 9907,10,7,1 | 9908,2699 | 9909,11,10,7 | 9910,27,16,15 |
| 9911,483 | 9912,42,35,15 | 9913,1899 | 9914,95 | 9915,29,17,8 | 9916,4483 | 9917,32,9,6 | 9918,381 | 9919,1185 | 9920,49,18,14 |
| 9921,901 | 9922,2691 | 9923,37,33,26 | 9924,30,29,26 | 9925,12,9,7 | 9926,1445 | 9927,1987 | 9928,39,38,31 | 9929,1382 | 9930,331 |
| 9931,34,10,3 | 9932,2397 | 9933,23,6,2 | 9934,34,7,3 | 9935,2216 | 9936,22,21,1 | 9937,451 | 9938,25,19,9 | 9939,32,26,17 | 9940,2059 |
| 9941,29,12,10 | 9942,133 | 9943,3069 | 9944,15,14,6 | 9945,1882 | 9946,2355 | 9947,23,17,8 | 9948,1535 | 9949,32,24,10 | 9950,2453 |
| 9951,1334 | 9952,31,30,11 | 9953,539 | 9954,343 | 9955,9,8,5 | 9956,851 | 9957,25,11,4 | 9958,17,14,4 | 9959,381 | 9960,30,15,10 |
| 9961,2707 | 9962,20,14,3 | 9963,34,29,20 | 9964,2691 | 9965,34,24,23 | 9966,1701 | 9967,4399 | 9968,36,3,2 | 9969,295 | 9970,2587 |
| 9971,11,8,5 | 9972,519 | 9973,27,24,12 | 9974,2045 | 9975,124 | 9976,21,19,5 | 9977,2954 | 9978,1483 | 9979,26,10,2 | 9980,707 |
| 9981,30,27,22 | 9982,993 | 9983,785 | 9984,27,10,7 | 9985,1974 | 9986,1143 | 9987,14,11,10 | 9988,3129 | 9989,21,20,6 | 9990,573 |
| 9991,495 | 9992,7,4,2 | 9993,121 | 9994,29,22,3 | 9995,41,40,31 | 9996,1447 | 9997,26,10,6 | 9998,4013 | 9999,2951 | 10000,19,13,9 |