869, 922, 961, 1057, 1105, 1121, 1122, 1227, 1228, 1291, 1303, 1306, 1316, 1333, 1389, 1413, 1436, 1478, 1480, 1509, 1510, 1511, 1515, 1521, 1558, 1560, 1563, 1570, 1584, 1631, 1636, 1694, 1701, 1756, 1773, 1774, 1843, 1845, 1848, 1875, 1922, 1928, 1936, 1938, 1939, 1943, 1945, 1991, 2017, 2049, 2052, 2054, 2076, 2077, 2080, 2107, 2144, 2179, 2181, 2182, 2184, 2185, 2187, 2197, 2223, 2252, 2280, 2281, 2343, 2404, 2405, 2445, 2548, 2632, 2637, 2641, 2644, 2667, 2670, 2672, 2681, 2711, 2714, 2719, 2720, 2781, 2793, 2819, 2820, 2849, 2851, 2920, 2921, 2923, 2949, 2950]

## 2.2 Tables

*David Thomson,* *Carleton University*

**2.2.1 Remark** Unless otherwise stated, all of the data given in this section was created by the author and, when possible, was verified with known results. Basic algorithms (for example, brute force) were preferred due to their reliability and ease of verification. Unless stated, all simulations were done in C/C++ using the NTL version 5.5.2 library [2633] for modular computations. NTL was compiled using the GMP version 4.3.2 library [2797] for multi-precision arithmetic. Extended and machine-readable versions of the tables found in this section can be found on the book's website [2180].

**2.2.2 Remark** Since most computer algebra packages can readily handle basic finite field computations, our aim is not to repeat tables whose purpose is to improve hand-calculations. For reference, we briefly recall the list of tables found in [1939].

Tables A and B are aids to perform fast arithmetic by hand over small finite fields. Table A is a list of all elements over small finite fields and their discrete logarithms with respect to a primitive element. Table B provides a list of *Jacobi's logarithms* $L(\cdot)$ for $\mathbb{F}_{2^n}$, $2 \leq n \leq 6$. These logarithms allow the computation of field elements by the relationship $\zeta^\alpha + \zeta^\beta = \zeta^{\alpha+L(\beta-\alpha)}$.

Table C provides a list of all monic irreducible polynomials of degree $n$ over small prime fields. Particularly, these tables cover $p = 2$ and $n \leq 11$, $p = 3$ and $n \leq 7$, $p = 5$ and $n \leq 5$, $p = 7$ and $n \leq 4$.

Tables D, E and F deal with primitive polynomials. Table D lists one primitive polynomial over $\mathbb{F}_2$ for degrees $n \leq 100$. Table E lists all quadratic primitive polynomials for $11 \leq p \leq 31$ and Table F lists one primitive polynomial of degree $n$ over $\mathbb{F}_p$ for all $n \geq 2$ with $p < 50$ and $p^n < 10^9$.

### 2.2.1 Low-weight irreducible and primitive polynomials

**2.2.3 Remark** Low-weight irreducible polynomials are highly desired due to their efficiency in hardware and software implementations of finite fields. Irreducible polynomials of degree at least 2 over $\mathbb{F}_2$ must have an odd number of terms. The use of irreducible trinomials (having 3 terms) and, in their absence, irreducible pentanomials (having 5 terms) are useful; see, for example, [1413, Chapter 2]. For cryptographic use, the irreducible trinomial or pentanomial of lowest lexicographical order (for a fixed $n$, prefer the trinomial $x^n+x^k+1$ over $x^n+x^{k_1}+1$ when $k < k_1$, the analogue for pentanomials is obvious) is often preferred for transparency reasons. However, the irreducible with the optimal performance for a given implementation is not necessarily the lowest lex-order, see [2573] and Section 11.1. A list of the lowest-weight

lowest-lex-order irreducible over $\mathbb{F}_2$ is given in [2582] for degree $n \leq 10000$. Table 2.2.1 gives the lowest-weight, lowest-lex-order irreducible polynomial for $n \leq 1025$. The output of the table follows the format $n, k$ (for trinomials $x^n + x^k + 1$) or $n, k_1, k_2, k_3$ (for pentanomials $x^n + x^{k_1} + x^{k_2} + x^{k_3} + 1$). We have extended these tables to larger $n$ and to larger $q$ for small values of $n$. Furthermore, the computer algebra package Magma [712] contains similar tables, due to Steel (2004-2007), for the following values of $q$ and $n$:

| $q$ | $n \leq$ | $q$ | $n \leq$ | $q$ | $n \leq$ | $q$ | $n \leq$ |
|---|---|---|---|---|---|---|---|
| 2 | $120,000$ | 3 | $50,000$ | $4, 5, 7$ | 2000 | $9 \leq q \leq 127$ | 1000 (or more). |

Sections 3.4 and 4.3 give more information on weights of irreducible and primitive polynomials.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 2,1 | 3,1 | 4,1 | 5,2 | 6,1 | 7,1 | 8,4,3,1 | 9,1 |
| 10,3 | 11,2 | 12,3 | 13,4,3,1 | 14,5 | 15,1 | 16,5,3,1 | 17,3 |
| 18,3 | 19,5,2,1 | 20,3 | 21,2 | 22,1 | 23,5 | 24,4,3,1 | 25,3 |
| 26,4,3,1 | 27,5,2,1 | 28,1 | 29,2 | 30,1 | 31,3 | 32,7,3,2 | 33,10 |
| 34,7 | 35,2 | 36,9 | 37,6,4,1 | 38,6,5,1 | 39,4 | 40,5,4,3 | 41,3 |
| 42,7 | 43,6,4,3 | 44,5 | 45,4,3,1 | 46,1 | 47,5 | 48,5,3,2 | 49,9 |
| 50,4,3,2 | 51,6,3,1 | 52,3 | 53,6,2,1 | 54,9 | 55,7 | 56,7,4,2 | 57,4 |
| 58,19 | 59,7,4,2 | 60,1 | 61,5,2,1 | 62,29 | 63,1 | 64,4,3,1 | 65,18 |
| 66,3 | 67,5,2,1 | 68,9 | 69,6,5,2 | 70,5,3,1 | 71,6 | 72,10,9,3 | 73,25 |
| 74,35 | 75,6,3,1 | 76,21 | 77,6,5,2 | 78,6,5,3 | 79,9 | 80,9,4,2 | 81,4 |
| 82,8,3,1 | 83,7,4,2 | 84,5 | 85,8,2,1 | 86,21 | 87,13 | 88,7,6,2 | 89,38 |
| 90,27 | 91,8,5,1 | 92,21 | 93,2 | 94,21 | 95,11 | 96,10,9,6 | 97,6 |
| 98,11 | 99,6,3,1 | 100,15 | 101,7,6,1 | 102,29 | 103,9 | 104,4,3,1 | 105,4 |
| 106,15 | 107,9,7,4 | 108,17 | 109,5,4,2 | 110,33 | 111,10 | 112,5,4,3 | 113,9 |
| 114,5,3,2 | 115,8,7,5 | 116,4,2,1 | 117,5,2,1 | 118,33 | 119,8 | 120,4,3,1 | 121,18 |
| 122,6,2,1 | 123,2 | 124,19 | 125,7,6,5 | 126,21 | 127,1 | 128,7,2,1 | 129,5 |
| 130,3 | 131,8,3,2 | 132,17 | 133,9,8,2 | 134,57 | 135,11 | 136,5,3,2 | 137,21 |
| 138,8,7,1 | 139,8,5,3 | 140,15 | 141,10,4,1 | 142,21 | 143,5,3,2 | 144,7,4,2 | 145,52 |
| 146,71 | 147,14 | 148,27 | 149,10,9,7 | 150,53 | 151,3 | 152,6,3,2 | 153,1 |
| 154,15 | 155,62 | 156,9 | 157,6,5,2 | 158,8,6,5 | 159,31 | 160,5,3,2 | 161,18 |
| 162,27 | 163,7,6,3 | 164,10,8,7 | 165,9,8,3 | 166,37 | 167,6 | 168,15,3,2 | 169,34 |
| 170,11 | 171,6,5,2 | 172,1 | 173,8,5,2 | 174,13 | 175,6 | 176,11,3,2 | 177,8 |
| 178,31 | 179,4,2,1 | 180,3 | 181,7,6,1 | 182,81 | 183,56 | 184,9,8,7 | 185,24 |
| 186,11 | 187,7,6,5 | 188,6,5,2 | 189,6,5,2 | 190,8,7,6 | 191,9 | 192,7,2,1 | 193,15 |
| 194,87 | 195,8,3,2 | 196,3 | 197,9,4,2 | 198,9 | 199,34 | 200,5,3,2 | 201,14 |
| 202,55 | 203,8,7,1 | 204,27 | 205,9,5,2 | 206,10,9,5 | 207,43 | 208,9,3,1 | 209,6 |
| 210,7 | 211,11,10,8 | 212,105 | 213,6,5,2 | 214,73 | 215,23 | 216,7,3,1 | 217,45 |
| 218,11 | 219,8,4,1 | 220,7 | 221,8,6,2 | 222,5,4,2 | 223,33 | 224,9,8,3 | 225,32 |
| 226,10,7,3 | 227,10,9,4 | 228,113 | 229,10,4,1 | 230,8,7,6 | 231,26 | 232,9,4,2 | 233,74 |
| 234,31 | 235,9,6,1 | 236,5 | 237,7,4,1 | 238,73 | 239,36 | 240,8,5,3 | 241,70 |
| 242,95 | 243,8,5,1 | 244,111 | 245,6,4,1 | 246,11,2,1 | 247,82 | 248,15,14,10 | 249,35 |
| 250,103 | 251,7,4,2 | 252,15 | 253,46 | 254,7,2,1 | 255,52 | 256,10,5,2 | 257,12 |
| 258,71 | 259,10,6,2 | 260,15 | 261,7,6,4 | 262,9,8,4 | 263,93 | 264,9,6,2 | 265,42 |
| 266,47 | 267,8,6,3 | 268,25 | 269,7,6,1 | 270,53 | 271,58 | 272,9,3,2 | 273,23 |
| 274,67 | 275,11,10,9 | 276,63 | 277,12,6,3 | 278,5 | 279,5 | 280,9,5,2 | 281,93 |
| 282,35 | 283,12,7,5 | 284,53 | 285,10,7,5 | 286,69 | 287,71 | 288,11,10,1 | 289,21 |
| 290,5,3,2 | 291,12,11,5 | 292,37 | 293,11,6,1 | 294,33 | 295,48 | 296,7,3,2 | 297,5 |
| 298,11,8,4 | 299,11,6,4 | 300,5 | 301,9,5,2 | 302,41 | 303,1 | 304,11,2,1 | 305,102 |
| 306,7,3,1 | 307,8,4,2 | 308,15 | 309,10,6,4 | 310,93 | 311,7,5,3 | 312,9,7,4 | 313,79 |
| 314,15 | 315,10,9,1 | 316,63 | 317,7,4,2 | 318,45 | 319,36 | 320,4,3,1 | 321,31 |
| 322,67 | 323,10,3,1 | 324,51 | 325,10,5,2 | 326,10,3,1 | 327,34 | 328,8,3,1 | 329,50 |
| 330,99 | 331,10,6,2 | 332,89 | 333,2 | 334,5,2,1 | 335,10,7,2 | 336,7,4,1 | 337,55 |
| 338,4,3,1 | 339,16,10,7 | 340,45 | 341,10,8,6 | 342,125 | 343,75 | 344,7,2,1 | 345,22 |
| 346,63 | 347,11,10,3 | 348,103 | 349,6,5,2 | 350,53 | 351,34 | 352,13,11,6 | 353,69 |
| 354,99 | 355,6,5,1 | 356,10,9,7 | 357,11,10,2 | 358,57 | 359,68 | 360,5,3,2 | 361,7,4,1 |
| 362,63 | 363,8,5,3 | 364,9 | 365,9,6,5 | 366,29 | 367,21 | 368,7,3,2 | 369,91 |
| 370,139 | 371,8,3,2 | 372,111 | 373,8,7,2 | 374,8,6,5 | 375,16 | 376,8,7,5 | 377,41 |
| 378,43 | 379,10,8,5 | 380,47 | 381,5,2,1 | 382,81 | 383,90 | 384,12,3,2 | 385,6 |
| 386,83 | 387,8,7,1 | 388,159 | 389,10,9,5 | 390,9 | 391,28 | 392,13,10,6 | 393,7 |
| 394,135 | 395,11,6,5 | 396,25 | 397,12,7,6 | 398,7,6,2 | 399,26 | 400,5,3,2 | 401,152 |
| 402,171 | 403,9,8,5 | 404,65 | 405,13,8,2 | 406,141 | 407,71 | 408,5,3,2 | 409,87 |
| 410,10,4,3 | 411,12,10,3 | 412,147 | 413,10,7,6 | 414,13 | 415,102 | 416,9,5,2 | 417,107 |
| 418,199 | 419,15,5,4 | 420,7 | 421,5,4,2 | 422,149 | 423,25 | 424,9,7,2 | 425,12 |
| 426,63 | 427,11,6,5 | 428,105 | 429,10,8,7 | 430,14,6,1 | 431,120 | 432,13,4,3 | 433,33 |
| 434,12,11,5 | 435,12,9,5 | 436,165 | 437,6,2,1 | 438,65 | 439,49 | 440,4,3,1 | 441,7 |
| 442,7,5,2 | 443,10,6,1 | 444,81 | 445,7,6,4 | 446,105 | 447,73 | 448,11,6,4 | 449,134 |
| 450,47 | 451,16,10,1 | 452,6,5,4 | 453,15,6,4 | 454,8,6,1 | 455,38 | 456,18,9,6 | 457,16 |
| 458,203 | 459,12,5,2 | 460,19 | 461,7,6,1 | 462,73 | 463,93 | 464,19,18,13 | 465,31 |
| 466,14,11,6 | 467,11,6,1 | 468,27 | 469,9,5,2 | 470,9 | 471,1 | 472,11,3,2 | 473,200 |
| 474,191 | 475,9,8,4 | 476,9 | 477,16,15,7 | 478,121 | 479,104 | 480,15,9,6 | 481,138 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 482,9,6,5 | 483,9,6,4 | 484,105 | 485,17,16,6 | 486,81 | 487,94 | 488,4,3,1 | 489,83 |
| 490,219 | 491,11,6,3 | 492,7 | 493,10,5,3 | 494,17 | 495,76 | 496,16,5,2 | 497,78 |
| 498,155 | 499,11,6,5 | 500,27 | 501,5,4,2 | 502,8,5,4 | 503,3 | 504,15,14,6 | 505,156 |
| 506,23 | 507,13,6,3 | 508,9 | 509,8,7,3 | 510,69 | 511,10 | 512,8,5,2 | 513,26 |
| 514,67 | 515,14,7,4 | 516,21 | 517,12,10,2 | 518,33 | 519,79 | 520,15,11,2 | 521,32 |
| 522,39 | 523,13,6,2 | 524,167 | 525,6,4,1 | 526,97 | 527,47 | 528,11,6,2 | 529,42 |
| 530,10,7,3 | 531,10,5,4 | 532,1 | 533,4,3,2 | 534,161 | 535,8,6,2 | 536,7,5,3 | 537,94 |
| 538,195 | 539,10,5,4 | 540,9 | 541,13,10,4 | 542,8,6,1 | 543,16 | 544,8,3,1 | 545,122 |
| 546,8,2,1 | 547,13,7,4 | 548,10,5,3 | 549,16,4,3 | 550,193 | 551,135 | 552,19,16,9 | 553,39 |
| 554,10,8,7 | 555,10,9,4 | 556,153 | 557,7,6,5 | 558,73 | 559,34 | 560,11,9,6 | 561,71 |
| 562,11,4,2 | 563,14,7,3 | 564,163 | 565,11,6,1 | 566,153 | 567,28 | 568,15,7,6 | 569,77 |
| 570,67 | 571,10,5,2 | 572,12,8,1 | 573,10,6,4 | 574,13 | 575,146 | 576,13,4,3 | 577,25 |
| 578,23,22,16 | 579,12,9,7 | 580,237 | 581,13,7,6 | 582,85 | 583,130 | 584,14,13,3 | 585,88 |
| 586,7,5,2 | 587,11,6,1 | 588,35 | 589,10,4,3 | 590,93 | 591,9,6,4 | 592,13,6,3 | 593,86 |
| 594,19 | 595,9,2,1 | 596,273 | 597,14,12,9 | 598,7,6,1 | 599,30 | 600,9,5,2 | 601,201 |
| 602,215 | 603,6,4,3 | 604,105 | 605,10,7,5 | 606,165 | 607,105 | 608,19,13,6 | 609,31 |
| 610,127 | 611,10,4,2 | 612,81 | 613,19,10,4 | 614,45 | 615,211 | 616,19,10,3 | 617,200 |
| 618,295 | 619,9,8,5 | 620,9 | 621,12,6,5 | 622,297 | 623,68 | 624,11,6,5 | 625,133 |
| 626,251 | 627,13,8,4 | 628,223 | 629,6,5,2 | 630,7,4,2 | 631,307 | 632,9,2,1 | 633,101 |
| 634,39 | 635,14,10,4 | 636,217 | 637,14,9,1 | 638,6,5,1 | 639,16 | 640,14,3,2 | 641,11 |
| 642,119 | 643,11,3,2 | 644,11,6,5 | 645,11,8,4 | 646,249 | 647,5 | 648,13,3,1 | 649,37 |
| 650,3 | 651,14 | 652,93 | 653,10,8,7 | 654,33 | 655,88 | 656,7,5,4 | 657,38 |
| 658,55 | 659,15,4,2 | 660,11 | 661,12,11,4 | 662,21 | 663,107 | 664,11,9,8 | 665,33 |
| 666,10,7,2 | 667,18,7,3 | 668,147 | 669,5,4,2 | 670,153 | 671,15 | 672,11,6,5 | 673,28 |
| 674,11,7,4 | 675,6,3,1 | 676,31 | 677,8,4,3 | 678,15,5,3 | 679,66 | 680,23,16,9 | 681,11,9,3 |
| 682,171 | 683,11,6,1 | 684,209 | 685,4,3,1 | 686,197 | 687,13 | 688,19,14,6 | 689,14 |
| 690,79 | 691,13,6,2 | 692,299 | 693,15,8,2 | 694,169 | 695,177 | 696,23,10,2 | 697,267 |
| 698,215 | 699,15,10,1 | 700,75 | 701,16,4,2 | 702,37 | 703,12,7,1 | 704,8,3,2 | 705,17 |
| 706,12,11,8 | 707,15,8,5 | 708,15 | 709,4,3,1 | 710,13,12,4 | 711,92 | 712,5,4,3 | 713,41 |
| 714,23 | 715,7,4,1 | 716,183 | 717,16,7,1 | 718,165 | 719,150 | 720,9,6,4 | 721,9 |
| 722,231 | 723,16,10,4 | 724,207 | 725,9,6,5 | 726,5 | 727,180 | 728,4,3,2 | 729,58 |
| 730,147 | 731,8,6,2 | 732,343 | 733,8,7,2 | 734,11,6,1 | 735,44 | 736,13,8,6 | 737,5 |
| 738,347 | 739,18,16,8 | 740,135 | 741,9,8,3 | 742,85 | 743,90 | 744,13,11,1 | 745,258 |
| 746,351 | 747,10,6,4 | 748,19 | 749,7,6,1 | 750,309 | 751,18 | 752,13,10,3 | 753,158 |
| 754,19 | 755,12,10,1 | 756,45 | 757,7,6,1 | 758,233 | 759,98 | 760,11,6,5 | 761,3 |
| 762,83 | 763,16,14,9 | 764,6,5,3 | 765,9,7,4 | 766,22,19,9 | 767,168 | 768,19,17,4 | 769,120 |
| 770,14,5,2 | 771,17,15,6 | 772,7 | 773,10,8,6 | 774,185 | 775,93 | 776,15,14,7 | 777,29 |
| 778,375 | 779,10,8,3 | 780,13 | 781,17,16,2 | 782,329 | 783,68 | 784,13,9,6 | 785,92 |
| 786,12,10,3 | 787,7,6,3 | 788,17,10,3 | 789,5,2,1 | 790,9,6,1 | 791,30 | 792,9,7,3 | 793,253 |
| 794,143 | 795,7,4,1 | 796,9,4,1 | 797,12,10,4 | 798,53 | 799,25 | 800,9,7,1 | 801,217 |
| 802,15,13,9 | 803,14,9,2 | 804,75 | 805,8,7,2 | 806,21 | 807,7 | 808,14,3,2 | 809,15 |
| 810,159 | 811,12,10,8 | 812,29 | 813,10,3,1 | 814,21 | 815,333 | 816,11,8,2 | 817,52 |
| 818,119 | 819,16,9,7 | 820,123 | 821,15,11,2 | 822,17 | 823,9 | 824,11,6,4 | 825,38 |
| 826,255 | 827,12,10,7 | 828,189 | 829,4,3,1 | 830,17,10,7 | 831,49 | 832,13,5,2 | 833,149 |
| 834,15 | 835,14,7,5 | 836,10,9,2 | 837,8,6,5 | 838,61 | 839,54 | 840,11,5,1 | 841,144 |
| 842,47 | 843,11,10,7 | 844,105 | 845,2 | 846,105 | 847,136 | 848,11,4,1 | 849,253 |
| 850,111 | 851,13,10,5 | 852,159 | 853,10,7,1 | 854,7,5,3 | 855,29 | 856,19,10,3 | 857,119 |
| 858,207 | 859,17,15,4 | 860,35 | 861,14 | 862,349 | 863,6,3,2 | 864,21,10,6 | 865,1 |
| 866,75 | 867,9,5,2 | 868,145 | 869,11,7,6 | 870,301 | 871,378 | 872,13,3,1 | 873,352 |
| 874,12,7,4 | 875,12,8,1 | 876,149 | 877,6,5,4 | 878,12,9,8 | 879,11 | 880,15,7,5 | 881,78 |
| 882,99 | 883,17,16,12 | 884,173 | 885,8,7,1 | 886,13,9,8 | 887,147 | 888,19,18,10 | 889,127 |
| 890,183 | 891,12,4,1 | 892,31 | 893,11,8,6 | 894,173 | 895,12 | 896,7,5,3 | 897,113 |
| 898,207 | 899,18,15,5 | 900,1 | 901,13,7,6 | 902,21 | 903,35 | 904,12,7,2 | 905,117 |
| 906,123 | 907,12,10,2 | 908,143 | 909,14,4,1 | 910,15,9,7 | 911,204 | 912,7,5,1 | 913,91 |
| 914,4,2,1 | 915,8,6,3 | 916,183 | 917,12,10,7 | 918,77 | 919,36 | 920,14,9,6 | 921,221 |
| 922,7,6,5 | 923,16,14,13 | 924,31 | 925,16,15,7 | 926,365 | 927,403 | 928,10,3,2 | 929,11,4,3 |
| 930,31 | 931,10,9,4 | 932,177 | 933,16,6,1 | 934,22,6,5 | 935,417 | 936,15,13,12 | 937,217 |
| 938,207 | 939,7,5,4 | 940,10,7,1 | 941,11,6,1 | 942,45 | 943,24 | 944,12,11,9 | 945,77 |
| 946,21,20,13 | 947,9,6,5 | 948,189 | 949,8,3,2 | 950,13,12,10 | 951,260 | 952,16,9,7 | 953,168 |
| 954,131 | 955,7,6,3 | 956,305 | 957,10,9,6 | 958,13,9,4 | 959,143 | 960,12,9,3 | 961,18 |
| 962,15,8,5 | 963,20,9,6 | 964,103 | 965,15,4,2 | 966,201 | 967,36 | 968,9,5,2 | 969,31 |
| 970,11,7,2 | 971,6,2,1 | 972,7 | 973,13,6,4 | 974,9,8,7 | 975,19 | 976,17,10,6 | 977,15 |
| 978,9,3,1 | 979,178 | 980,8,7,6 | 981,12,6,5 | 982,177 | 983,230 | 984,24,9,3 | 985,222 |
| 986,3 | 987,16,13,12 | 988,121 | 989,10,4,2 | 990,161 | 991,39 | 992,17,15,13 | 993,62 |
| 994,223 | 995,15,12,2 | 996,65 | 997,12,6,3 | 998,101 | 999,59 | 1000,5,4,3 | 1001,17 |
| 1002,5,3,2 | 1003,13,8,3 | 1004,10,9,7 | 1005,12,8,2 | 1006,5,4,3 | 1007,75 | 1008,19,17,8 | 1009,55 |
| 1010,99 | 1011,10,7,4 | 1012,115 | 1013,9,8,6 | 1014,385 | 1015,186 | 1016,15,6,3 | 1017,9,4,1 |
| 1018,12,10,5 | 1019,10,8,1 | 1020,135 | 1021,5,2,1 | 1022,317 | 1023,7 | 1024,19,6,1 | 1025,294 |

**Table 2.2.1** Lowest weight lowest-lexicographical order irreducible polynomial of degree $n$ over $\mathbb{F}_2$. Output: $n, k$ (for trinomials $x^n + x^k + 1$) or $n, k_1, k_2, k_3$ (for pentanomials $x^n + x^{k_1} + x^{k_2} + x^{k_3} + 1$).

**2.2.4 Remark** Constructions of irreducible low-weight polynomials are rare; see Sections 3.4 and 3.5. Instead, conditions for reducibility are often more tractable; see Section 3.3. Swan [2753] gives conditions for when a trinomial $x^n + x^k + 1 \in \mathbb{F}_2[x]$ is reducible. In particular, the trinomial is reducible when 8 divides $n$. Only partial results for Swan-like conditions on pentanomials over $\mathbb{F}_2$ exist in the literature; see, for example, [1777] and Section 3.3.

**2.2.5 Conjecture** [2582] For every $n$, there exists either an irreducible trinomial of degree $n$ over $\mathbb{F}_2$ or, in the absence of an irreducible trinomial, there exists an irreducible pentanomial of degree $n$ over $\mathbb{F}_2$.

**2.2.6 Remark** A polynomial over $\mathbb{F}_q$ is *primitive* if all of its roots are generators of the (cyclic) multiplicative group $\mathbb{F}_q^*$. We give an analogous table to Table 2.2.1 but instead list the lowest-weight lowest-lexicographical order primitive polynomial of degree $n \leq 577$ over $\mathbb{F}_2$. To compute primitivity, we used the *Cunningham project* to find the factorization of $2^n - 1$; see Section 2.2.3 for more details.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 2,1 | 3,1 | 4,1 | 5,2 | 6,1 | 7,1 | 8,4,3,2 | 9,4 |
| 10,3 | 11,2 | 12,6,4,1 | 13,4,3,1 | 14,5,3,1 | 15,1 | 16,5,3,2 | 17,3 |
| 18,7 | 19,5,2,1 | 20,3 | 21,2 | 22,1 | 23,5 | 24,4,3,1 | 25,3 |
| 26,6,2,1 | 27,5,2,1 | 28,3 | 29,2 | 30,6,4,1 | 31,3 | 32,7,6,2 | 33,13 |
| 34,8,4,3 | 35,2 | 36,11 | 37,6,4,1 | 38,6,5,1 | 39,4 | 40,5,4,3 | 41,3 |
| 42,7,4,3 | 43,6,4,3 | 44,6,5,2 | 45,4,3,1 | 46,8,7,6 | 47,5 | 48,9,7,4 | 49,9 |
| 50,4,3,2 | 51,6,3,1 | 52,3 | 53,6,2,1 | 54,8,6,3 | 55,24 | 56,7,4,2 | 57,7 |
| 58,19 | 59,7,4,2 | 60,1 | 61,5,2,1 | 62,6,5,3 | 63,1 | 64,4,3,1 | 65,18 |
| 66,9,8,6 | 67,5,2,1 | 68,9 | 69,6,5,2 | 70,5,3,1 | 71,6 | 72,10,9,3 | 73,25 |
| 74,7,4,3 | 75,6,3,1 | 76,5,4,2 | 77,6,5,2 | 78,7,2,1 | 79,9 | 80,9,4,2 | 81,4 |
| 82,9,6,4 | 83,7,4,2 | 84,13 | 85,8,2,1 | 86,6,5,2 | 87,13 | 88,11,9,8 | 89,38 |
| 90,5,3,2 | 91,8,5,1 | 92,6,5,2 | 93,2 | 94,21 | 95,11 | 96,10,9,6 | 97,6 |
| 98,11 | 99,7,5,4 | 100,37 | 101,7,6,1 | 102,6,5,3 | 103,9 | 104,11,10,1 | 105,16 |
| 106,15 | 107,9,7,4 | 108,31 | 109,5,4,2 | 110,6,4,1 | 111,10 | 112,11,6,4 | 113,9 |
| 114,11,2,1 | 115,8,7,5 | 116,6,5,2 | 117,5,2,1 | 118,33 | 119,8 | 120,9,6,2 | 121,18 |
| 122,6,2,1 | 123,2 | 124,37 | 125,7,6,5 | 126,7,4,2 | 127,1 | 128,7,2,1 | 129,5 |
| 130,3 | 131,8,3,2 | 132,29 | 133,9,8,2 | 134,57 | 135,11 | 136,8,3,2 | 137,21 |
| 138,8,7,1 | 139,8,5,3 | 140,29 | 141,13,6,1 | 142,21 | 143,5,3,2 | 144,7,4,2 | 145,52 |
| 146,5,3,2 | 147,11,4,2 | 148,27 | 149,10,9,7 | 150,53 | 151,3 | 152,6,3,2 | 153,1 |
| 154,9,5,1 | 155,7,5,4 | 156,9,5,3 | 157,6,5,2 | 158,8,6,5 | 159,31 | 160,5,3,2 | 161,18 |
| 162,8,7,4 | 163,7,6,3 | 164,12,6,5 | 165,9,8,3 | 166,10,3,2 | 167,6 | 168,16,9,6 | 169,34 |
| 170,23 | 171,6,5,2 | 172,7 | 173,8,5,2 | 174,13 | 175,6 | 176,12,11,9 | 177,8 |
| 178,87 | 179,4,2,1 | 180,12,10,7 | 181,7,6,1 | 182,8,6,1 | 183,56 | 184,9,8,7 | 185,24 |
| 186,9,8,6 | 187,7,6,5 | 188,6,5,2 | 189,6,5,2 | 190,13,6,2 | 191,9 | 192,15,11,5 | 193,15 |
| 194,87 | 195,8,3,2 | 196,11,9,2 | 197,9,4,2 | 198,65 | 199,34 | 200,5,3,2 | 201,14 |
| 202,55 | 203,8,7,1 | 204,10,4,3 | 205,9,5,2 | 206,10,9,5 | 207,43 | 208,9,3,1 | 209,6 |
| 210,12,4,3 | 211,11,10,8 | 212,105 | 213,6,5,2 | 214,5,3,1 | 215,23 | 216,7,3,1 | 217,45 |
| 218,11 | 219,8,4,1 | 220,12,10,9 | 221,8,6,2 | 222,8,5,2 | 223,33 | 224,12,7,2 | 225,32 |
| 226,10,7,3 | 227,10,9,4 | 228,12,11,2 | 229,10,4,1 | 230,8,7,6 | 231,26 | 232,11,9,4 | 233,74 |
| 234,31 | 235,9,6,1 | 236,5 | 237,7,4,1 | 238,5,2,1 | 239,36 | 240,8,5,3 | 241,70 |
| 242,11,6,1 | 243,8,5,1 | 244,9,4,1 | 245,6,4,1 | 246,11,2,1 | 247,82 | 248,15,14,10 | 249,86 |
| 250,103 | 251,7,4,2 | 252,67 | 253,7,3,2 | 254,7,2,1 | 255,52 | 256,10,5,2 | 257,12 |
| 258,83 | 259,10,6,2 | 260,10,8,7 | 261,7,6,4 | 262,9,8,4 | 263,93 | 264,10,9,1 | 265,42 |
| 266,47 | 267,8,6,3 | 268,25 | 269,7,6,1 | 270,53 | 271,58 | 272,9,6,2 | 273,23 |
| 274,67 | 275,11,10,9 | 276,6,3,1 | 277,12,6,3 | 278,5 | 279,5 | 280,9,5,2 | 281,93 |
| 282,35 | 283,12,7,5 | 284,119 | 285,10,7,5 | 286,69 | 287,71 | 288,11,10,1 | 289,21 |
| 290,5,3,2 | 291,12,11,5 | 292,97 | 293,11,6,1 | 294,61 | 295,48 | 296,11,9,4 | 297,5 |
| 298,11,8,4 | 299,11,6,4 | 300,7 | 301,9,5,2 | 302,41 | 303,13,12,6 | 304,11,2,1 | 305,102 |
| 306,7,3,1 | 307,8,4,2 | 308,15,9,2 | 309,10,6,4 | 310,8,5,1 | 311,7,5,3 | 312,11,10,5 | 313,79 |
| 314,15 | 315,10,9,1 | 316,135 | 317,7,4,2 | 318,8,6,5 | 319,36 | 320,4,3,1 | 321,31 |
| 322,67 | 323,10,3,1 | 324,6,4,3 | 325,10,5,2 | 326,10,3,1 | 327,34 | 328,9,7,5 | 329,50 |
| 330,8,7,2 | 331,10,6,2 | 332,123 | 333,2 | 334,7,4,1 | 335,10,7,2 | 336,7,4,1 | 337,55 |
| 338,6,3,2 | 339,16,10,7 | 340,11,4,3 | 341,14,11,5 | 342,125 | 343,75 | 344,11,10,6 | 345,22 |
| 346,11,7,2 | 347,11,10,3 | 348,8,7,4 | 349,6,5,2 | 350,53 | 351,34 | 352,13,11,6 | 353,69 |
| 354,14,13,5 | 355,6,5,1 | 356,10,9,7 | 357,11,10,2 | 358,14,8,7 | 359,68 | 360,26,25,1 | 361,7,4,1 |
| 362,63 | 363,8,5,3 | 364,67 | 365,9,6,5 | 366,29 | 367,21 | 368,17,9,7 | 369,91 |
| 370,139 | 371,8,3,2 | 372,15,7,3 | 373,8,7,2 | 374,8,6,5 | 375,16 | 376,8,7,5 | 377,41 |
| 378,43 | 379,10,8,5 | 380,47 | 381,5,2,1 | 382,81 | 383,90 | 384,16,15,6 | 385,6 |
| 386,83 | 387,9,8,2 | 388,14,3,1 | 389,10,9,5 | 390,89 | 391,28 | 392,13,10,6 | 393,7 |
| 394,135 | 395,11,6,5 | 396,25 | 397,12,7,6 | 398,14,6,5 | 399,86 | 400,5,3,2 | 401,152 |
| 402,9,4,3 | 403,9,8,5 | 404,189 | 405,17,8,7 | 406,157 | 407,71 | 408,7,5,1 | 409,87 |
| 410,10,4,3 | 411,12,10,3 | 412,147 | 413,10,7,6 | 414,16,13,9 | 415,102 | 416,9,5,2 | 417,107 |
| 418,15,3,1 | 419,15,5,4 | 420,13,10,8 | 421,5,4,2 | 422,149 | 423,25 | 424,9,7,2 | 425,12 |
| 426,14,12,11 | 427,11,6,5 | 428,105 | 429,10,8,7 | 430,15,13,11 | 431,120 | 432,13,4,3 | 433,33 |
| 434,12,11,5 | 435,12,9,5 | 436,165 | 437,6,2,1 | 438,65 | 439,49 | 440,4,3,1 | 441,31 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 442,7,5,2 | 443,10,6,1 | 444,13,12,9 | 445,7,6,4 | 446,105 | 447,73 | 448,11,6,4 | 449,134 |
| 450,79 | 451,16,10,1 | 452,6,5,4 | 453,15,6,4 | 454,10,9,5 | 455,38 | 456,23,11,2 | 457,16 |
| 458,203 | 459,12,5,2 | 460,61 | 461,7,6,1 | 462,73 | 463,93 | 464,23,9,4 | 465,59 |
| 466,14,11,6 | 467,11,6,1 | 468,15,9,4 | 469,9,5,2 | 470,149 | 471,1 | 472,11,3,2 | 473,8,6,3 |
| 474,191 | 475,9,8,4 | 476,15 | 477,16,15,7 | 478,121 | 479,104 | 480,16,13,7 | 481,138 |
| 482,9,6,5 | 483,9,6,4 | 484,105 | 485,17,16,6 | 486,14,8,5 | 487,94 | 488,4,3,1 | 489,83 |
| 490,219 | 491,11,6,3 | 492,8,7,1 | 493,10,5,3 | 494,137 | 495,76 | 496,16,5,2 | 497,78 |
| 498,11,9,3 | 499,11,6,5 | 500,10,6,1 | 501,5,4,2 | 502,8,5,4 | 503,3 | 504,21,14,2 | 505,156 |
| 506,95 | 507,13,6,3 | 508,109 | 509,8,7,3 | 510,12,10,9 | 511,10 | 512,8,5,2 | 513,85 |
| 514,7,5,3 | 515,14,7,4 | 516,7,5,2 | 517,12,10,2 | 518,33 | 519,79 | 520,17,13,11 | 521,32 |
| 522,15,13,4 | 523,13,6,2 | 524,167 | 525,6,4,1 | 526,9,5,1 | 527,47 | 528,11,6,2 | 529,42 |
| 530,10,7,3 | 531,12,6,2 | 532,1 | 533,4,3,2 | 534,7,5,1 | 535,8,6,2 | 536,7,5,3 | 537,94 |
| 538,5,2,1 | 539,10,5,4 | 540,179 | 541,13,10,4 | 542,9,3,2 | 543,16 | 544,13,9,6 | 545,122 |
| 546,8,2,1 | 547,13,7,4 | 548,10,5,3 | 549,16,4,3 | 550,193 | 551,135 | 552,20,5,2 | 553,39 |
| 554,11,8,3 | 555,10,9,4 | 556,153 | 557,7,6,5 | 558,14,9,5 | 559,34 | 560,11,9,6 | 561,71 |
| 562,11,4,2 | 563,14,7,3 | 564,163 | 565,11,6,1 | 566,153 | 567,143 | 568,17,11,10 | 569,77 |
| 570,67 | 571,10,5,2 | 572,12,8,1 | 573,10,6,4 | 574,13 | 575,146 | 576,13,4,3 | 577,25 |

**Table 2.2.2** Lowest weight lowest-lexicographical order primitive polynomial of degree $n \leq 577$ over $\mathbb{F}_2$. Output: $n, k$ (for trinomials $x^n + x^k + 1$) or $n, k_1, k_2, k_3$ (for pentanomials $x^n + x^{k_1} + x^{k_2} + x^{k_3} + 1$).

**2.2.7 Remark** Table 2.2.3 is the analogous table to Table 2.2.1, giving the lowest-weight, lowest-lexicographical order irreducible polynomial of degree $n \leq 516$ over $\mathbb{F}_3$.

| | | | | |
|---|---|---|---|---|
| 2,(1) | 3,1(2),(1) | 4,1(1),(2) | 5,1(2),(1) | 6,1(1),(2) |
| 7,2(1),(2) | 8,2(1),(2) | 9,4(1),(2) | 10,2(2),(1) | 11,2(1),(2) |
| 12,2(1),(2) | 13,1(2),(1) | 14,1(1),(2) | 15,2(1),(2) | 16,4(1),(2) |
| 17,1(2),(1) | 18,7(1),(2) | 19,2(1),(2) | 20,5(1),(2) | 21,5(2),(1) |
| 22,4(2),(1) | 23,3(2),(1) | 24,4(1),(2) | 25,3(2),(1) | 26,2(2),(1) |
| 27,7(2),(1) | 28,2(1),(2) | 29,4(1),(2) | 30,1(1),(2) | 31,5(2),(1) |
| 32,5(1),(2) | 33,5(2),(1) | 34,2(2),(1) | 35,2(1),(2) | 36,14(1),(2) |
| 37,6(1),(2) | 38,4(2),(1) | 39,7(2),(1) | 40,1(1),(2) | 41,1(2),(1) |
| 42,7(1),(2) | 43,17(2),(1) | 44,3(1),(2) | 45,17(2),(1) | 46,5(1),(2) |
| 47,15(2),(1) | 48,8(1),(2) | 49,3(2),2(1),(1) | 50,6(2),(1) | 51,1(2),(1) |
| 52,7(1),(2) | 53,13(2),(1) | 54,1(1),(2) | 55,11(2),(1) | 56,3(1),(2) |
| 57,7(1),2(1),(2) | 58,8(2),(1) | 59,17(2),(1) | 60,2(1),(2) | 61,7(2),(1) |
| 62,10(2),(1) | 63,26(1),(2) | 64,3(1),(2) | 65,5(1),3(1),(1) | 66,10(2),(1) |
| 67,2(1),(2) | 68,3(1),2(1),(1) | 69,17(2),(1) | 70,4(2),(1) | 71,20(1),(2) |
| 72,28(1),(2) | 73,1(2),(1) | 74,12(2),(1) | 75,5(2),4(1),(1) | 76,9(1),(2) |
| 77,16(1),(2) | 78,13(1),(2) | 79,26(1),(2) | 80,2(1),(2) | 81,40(1),(2) |
| 82,2(2),(1) | 83,27(2),(1) | 84,14(1),(2) | 85,16(1),(2) | 86,13(1),(2) |
| 87,26(1),(2) | 88,6(1),(2) | 89,13(2),(1) | 90,19(1),(2) | 91,17(2),(1) |
| 92,10(1),(2) | 93,23(2),(1) | 94,30(2),(1) | 95,47(2),(1) | 96,16(1),(2) |
| 97,12(1),(2) | 98,4(1),3(1),(1) | 99,19(2),(1) | 100,25(1),(2) | 101,31(2),(1) |
| 102,2(2),(1) | 103,47(2),(1) | 104,5(1),(2) | 105,6(1),2(1),(1) | 106,26(2),(1) |
| 107,3(2),(1) | 108,2(1),(2) | 109,9(2),(1) | 110,22(2),(1) | 111,2(1),(2) |
| 112,6(1),(2) | 113,19(2),(1) | 114,7(1),(2) | 115,32(1),(2) | 116,15(1),(2) |
| 117,52(1),(2) | 118,34(2),(1) | 119,2(1),(2) | 120,4(1),(2) | 121,1(2),(1) |
| 122,14(2),(1) | 123,7(1),4(1),(2) | 124,25(1),(2) | 125,52(1),(2) | 126,49(1),(2) |
| 127,8(1),(2) | 128,6(1),(2) | 129,3(2),2(1),(1) | 130,10(1),6(1),(1) | 131,27(2),(1) |
| 132,19(1),14(1),(1) | 133,15(2),(1) | 134,4(2),(1) | 135,44(1),(2) | 136,57(1),(2) |
| 137,1(2),(1) | 138,34(2),(1) | 139,59(2),(1) | 140,59(1),(2) | 141,5(2),(1) |
| 142,40(2),(1) | 143,35(2),(1) | 144,56(1),(2) | 145,24(1),(2) | 146,2(2),(1) |
| 147,8(1),(2) | 148,3(1),(2) | 149,11(2),10(1),(1) | 150,73(1),(2) | 151,2(1),(2) |
| 152,18(1),(2) | 153,59(2),(1) | 154,32(2),(1) | 155,12(1),(2) | 156,26(1),(2) |
| 157,22(1),(2) | 158,52(2),(1) | 159,32(1),(2) | 160,4(1),(2) | 161,9(1),5(1),(1) |
| 162,19(1),(2) | 163,59(2),(1) | 164,15(1),(2) | 165,22(1),(2) | 166,54(2),(1) |
| 167,71(2),(1) | 168,28(1),(2) | 169,24(1),(2) | 170,32(2),(1) | 171,20(1),(2) |
| 172,19(1),(2) | 173,7(2),(1) | 174,52(2),(1) | 175,10(1),8(1),(1) | 176,12(1),(2) |
| 177,52(1),(2) | 178,11(1),(2) | 179,59(2),(1) | 180,38(1),(2) | 181,37(2),(1) |
| 182,25(1),(2) | 183,2(1),(2) | 184,20(1),(2) | 185,64(1),(2) | 186,46(2),(1) |
| 187,8(1),(2) | 188,11(1),(2) | 189,9(1),7(1),(1) | 190,94(2),(1) | 191,71(2),(1) |
| 192,32(1),(2) | 193,12(1),(2) | 194,24(2),(1) | 195,26(1),(2) | 196,79(1),(2) |
| 197,9(1),7(1),(1) | 198,29(1),(2) | 199,35(2),(1) | 200,3(1),(2) | 201,88(1),(2) |
| 202,62(2),(1) | 203,3(2),(1) | 204,50(1),(2) | 205,9(2),(1) | 206,61(1),(2) |
| 207,11(2),8(1),(1) | 208,10(1),(2) | 209,40(1),(2) | 210,7(1),(2) | 211,89(2),(1) |
| 212,14(1),3(1),(1) | 213,17(2),4(1),(1) | 214,6(2),(1) | 215,36(1),(2) | 216,4(1),(2) |
| 217,85(2),(1) | 218,18(2),(1) | 219,25(2),(1) | 220,15(1),(2) | 221,12(1),2(1),(1) |
| 222,4(2),(1) | 223,8(1),5(2),(1) | 224,12(1),(2) | 225,16(1),(2) | 226,38(2),(1) |
| 227,11(2),(1) | 228,14(1),(2) | 229,72(1),(2) | 230,64(2),(1) | 231,8(1),7(1),(2) |
| 232,30(1),(2) | 233,6(1),2(1),(1) | 234,91(1),(2) | 235,26(1),(2) | 236,9(1),(2) |
| 237,70(1),(2) | 238,4(2),(1) | 239,5(2),(1) | 240,8(1),(2) | 241,88(1),(2) |
| 242,2(2),(1) | 243,121(2),(1) | 244,31(1),(2) | 245,97(2),(1) | 246,13(1),(2) |
| 247,122(1),(2) | 248,50(1),(2) | 249,59(2),(1) | 250,104(2),(1) | 251,9(2),(1) |
| 252,98(1),(2) | 253,7(2),(1) | 254,16(2),(1) | 255,26(1),(2) | 256,12(1),(2) |

| | | | | |
|---|---|---|---|---|
| 257,22(1),(2) | 258,7(1),(2) | 259,65(2),(1) | 260,35(1),(2) | 261,119(2),(1) |
| 262,54(2),(1) | 263,69(2),(1) | 264,23(1),16(1),(1) | 265,61(2),(1) | 266,30(2),(1) |
| 267,9(1),2(1),(2) | 268,15(1),(2) | 269,7(2),(1) | 270,88(2),(1) | 271,50(1),(2) |
| 272,114(1),(2) | 273,46(1),(2) | 274,2(2),(1) | 275,12(1),(2) | 276,10(1),2(1),(2) |
| 277,24(1),(2) | 278,118(2),(1) | 279,7(2),(1) | 280,15(1),(2) | 281,10(1),7(1),(2) |
| 282,10(2),(1) | 283,23(2),(1) | 284,5(1),(2) | 285,89(2),(1) | 286,70(2),(1) |
| 287,101(2),(1) | 288,112(1),(2) | 289,73(2),(1) | 290,43(1),(2) | 291,25(2),(1) |
| 292,13(1),12(1),(1) | 293,7(2),(1) | 294,16(2),(1) | 295,83(2),(1) | 296,6(1),(2) |
| 297,3(2),2(1),(1) | 298,13(1),3(1),(2) | 299,51(2),(1) | 300,146(1),(2) | 301,30(1),(2) |
| 302,4(2),(1) | 303,8(1),2(1),(1) | 304,36(1),(2) | 305,46(1),(2) | 306,118(2),(1) |
| 307,17(2),(1) | 308,53(1),(2) | 309,3(2),2(1),(1) | 310,24(2),(1) | 311,13(2),12(1),(1) |
| 312,52(1),(2) | 313,93(2),(1) | 314,44(2),(1) | 315,127(2),(1) | 316,87(1),(2) |
| 317,7(2),(1) | 318,64(2),(1) | 319,10(1),9(1),(2) | 320,3(1),(2) | 321,83(2),(1) |
| 322,71(1),(2) | 323,9(2),(1) | 324,38(1),(2) | 325,157(2),(1) | 326,118(2),(1) |
| 327,7(2),(1) | 328,3(1),(2) | 329,52(1),(2) | 330,11(1),(2) | 331,2(1),(2) |
| 332,13(1),6(1),(1) | 333,94(1),(2) | 334,142(2),(1) | 335,8(1),(2) | 336,56(1),(2) |
| 337,3(2),(1) | 338,48(2),(1) | 339,49(2),(1) | 340,86(1),(2) | 341,25(2),(1) |
| 342,40(2),(1) | 343,12(1),10(1),(1) | 344,38(1),(2) | 345,101(2),(1) | 346,14(2),(1) |
| 347,18(1),(2) | 348,146(1),(2) | 349,54(1),(2) | 350,157(1),(2) | 351,20(1),(2) |
| 352,7(1),(2) | 353,142(1),(2) | 354,104(2),(1) | 355,41(2),(1) | 356,15(1),(2) |
| 357,71(2),(1) | 358,77(1),(2) | 359,15(2),(1) | 360,76(1),(2) | 361,157(2),(1) |
| 362,74(2),(1) | 363,26(1),(2) | 364,1(1),(2) | 365,88(1),(2) | 366,4(2),(1) |
| 367,107(2),(1) | 368,27(1),(2) | 369,11(2),(1) | 370,11(1),(2) | 371,27(2),(1) |
| 372,94(1),(2) | 373,25(2),(1) | 374,16(2),(1) | 375,67(2),(1) | 376,9(1),(2) |
| 377,160(1),(2) | 378,7(1),(2) | 379,44(1),(2) | 380,9(1),(2) | 381,143(2),(1) |
| 382,137(1),(2) | 383,80(1),(2) | 384,64(1),(2) | 385,22(1),(2) | 386,24(2),(1) |
| 387,152(1),(2) | 388,87(1),(2) | 389,76(1),(2) | 390,13(1),(2) | 391,22(1),21(2),(1) |
| 392,158(1),(2) | 393,185(2),(1) | 394,14(1),9(1),(1) | 395,23(2),(1) | 396,58(1),(2) |
| 397,12(1),5(1),(2) | 398,70(2),(1) | 399,181(2),(1) | 400,3(1),(2) | 401,11(2),10(1),(1) |
| 402,176(2),(1) | 403,161(2),(1) | 404,9(1),2(1),(1) | 405,25(1),18(1),(2) | 406,6(2),(1) |
| 407,48(1),(2) | 408,100(1),(2) | 409,99(2),(1) | 410,18(2),(1) | 411,8(1),2(1),(1) |
| 412,79(1),(2) | 413,22(1),(2) | 414,37(1),(2) | 415,13(1),3(1),(1) | 416,20(1),(2) |
| 417,40(1),(2) | 418,80(2),(1) | 419,26(1),(2) | 420,14(1),(2) | 421,13(2),(1) |
| 422,178(2),(1) | 423,68(1),(2) | 424,45(1),(2) | 425,61(2),(1) | 426,9(1),7(1),(2) |
| 427,167(2),(1) | 428,71(1),(2) | 429,65(2),(1) | 430,72(2),(1) | 431,66(1),(2) |
| 432,8(1),(2) | 433,120(1),(2) | 434,67(1),(2) | 435,8(1),2(1),(1) | 436,13(1),2(1),(1) |
| 437,14(1),3(2),(1) | 438,17(1),(2) | 439,16(1),3(2),(1) | 440,11(1),(2) | 441,7(1),6(1),(2) |
| 442,11(1),3(1),(2) | 443,188(1),(2) | 444,178(1),(2) | 445,141(2),(1) | 446,1(1),(2) |
| 447,157(2),(1) | 448,24(1),(2) | 449,52(1),(2) | 450,32(2),(1) | 451,17(2),(1) |
| 452,17(1),(2) | 453,17(2),4(1),(1) | 454,22(2),(1) | 455,32(1),(2) | 456,28(1),(2) |
| 457,67(2),(1) | 458,144(2),(1) | 459,13(2),6(1),(1) | 460,57(1),(2) | 461,13(2),(1) |
| 462,73(1),(2) | 463,15(1),13(1),(1) | 464,60(1),(2) | 465,41(2),(1) | 466,167(1),(2) |
| 467,48(1),(2) | 468,182(1),(2) | 469,166(1),(2) | 470,52(2),(1) | 471,8(1),(2) |
| 472,18(1),(2) | 473,73(2),(1) | 474,83(1),(2) | 475,17(2),(1) | 476,10(1),(2) |
| 477,101(2),(1) | 478,10(2),(1) | 479,221(2),(1) | 480,16(1),(2) | 481,22(1),(2) |
| 482,127(1),(2) | 483,26(1),(2) | 484,39(1),(2) | 485,1(2),(1) | 486,125(1),(2) |
| 487,29(2),(1) | 488,62(1),(2) | 489,7(1),5(1),(1) | 490,194(2),(1) | 491,11(2),(1) |
| 492,26(1),(2) | 493,4(1),(2) | 494,244(2),(1) | 495,7(2),(1) | 496,85(1),(2) |
| 497,7(2),6(1),(1) | 498,118(2),(1) | 499,20(1),(2) | 500,39(1),(2) | 501,88(1),(2) |
| 502,18(2),(1) | 503,35(2),(1) | 504,196(1),(2) | 505,61(2),(1) | 506,14(2),(1) |
| 507,80(1),(2) | 508,91(1),(2) | 509,151(2),(1) | 510,52(2),(1) | 511,215(2),(1) |
| 512,24(1),(2) | 513,14(1),10(1),(1) | 514,44(2),(1) | 515,8(1),(2) | 516,14(1),(2) |

**Table 2.2.3** Lowest weight lowest lexicographical order irreducible polynomial of degree $n$ over $\mathbb{F}_3$. Output: $n$, {*degrees, (coefficients)*}, *(constant term).*

**2.2.8 Remark** Necessary and sufficient conditions for the existence of an irreducible binomial of degree $n$ over finite fields of odd characteristic are given in [1939, Theorem 3.75]. A constructive derivation of the degrees for which there exists an irreducible binomial over $\mathbb{F}_q$, $q$ odd, is given in [2356]. The following conjecture summarizes empirical observations of extending Tables 2.2.1 and 2.2.3 to higher characteristics.

**2.2.9 Conjecture** Let $q > 2$. For every $n$, there is an irreducible polynomial of degree $n$ over $\mathbb{F}_q$ of weight at most 4.

### 2.2.2 Low-complexity normal bases

**2.2.10 Remark** Normal bases are often required in hardware implementations of finite fields due to the efficiency of exponentiation when the finite field is represented using a normal basis.

The *complexity* of a normal basis $N$, $C_N$, is defined in Definition 5.3.1. Normal bases with low complexity are highly preferred. An *optimal* normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is a normal basis attaining the minimum complexity $C_N = 2n - 1$. See Sections 5.2 and 5.3 for more details on normal bases and their complexities.

#### 2.2.2.1 Exhaustive search for low complexity normal bases

**2.2.11 Remark** Table 2.2.4 is due to an exhaustive search for normal bases of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$, $n \leq 39$, originally given in [2015]. The table gives the number of normal bases, the smallest and largest complexities $(m_{C_N}, M_{C_N})$, the average and variance $(Avg_{C_N}, Var_{C_N})$ of complexities and the smallest and largest complexities for self-dual normal elements. In Table 2.2.4, we fix a typo on the minimum complexity of $n = 37$, originally noted in [130], and make some minor corrections to the calculations of the averages and variances. In the "Notes" column, "Optimal" indicates that the basis with minimal complexity is an optimal normal basis (Theorem 5.3.6), and "sd" indicates that the minimal complexity basis is self-dual.

| | | | | | | **self-dual** | | |
|---|---|---|---|---|---|---|---|---|
| $n$ | # Normal bases | $m_{C_N}$ | $M_{C_N}$ | $Avg_{C_N}$ | $Var_{C_N}$ | $m_{C_N}$ | $M_{C_N}$ | Notes |
| 2 | 1 | 3 | 3 | 3.00 | 0 | 3 | 3 | Optimal, sd |
| 3 | 1 | 5 | 5 | 5.00 | 0 | 5 | 5 | Optimal, sd |
| 4 | 2 | 7 | 9 | 8.00 | 1.00 | - | - | |
| 5 | 3 | 9 | 15 | 11.67 | 6.22 | 9 | 9 | Optimal, sd |
| 6 | 4 | 11 | 17 | 15.00 | 6.00 | 11 | 15 | Optimal, sd |
| 7 | 7 | 19 | 27 | 23.00 | 9.14 | 21 | 21 | $m_{C_N} = 3n - 2$ |
| 8 | 16 | 21 | 35 | 29.00 | 11 | - | - | $m_{C_N} = 3n - 3$ |
| 9 | 21 | 17 | 45 | 35.57 | 41.57 | 17 | 29 | Optimal, sd |
| 10 | 48 | 19 | 61 | 44.83 | 61.31 | 27 | 51 | |
| 11 | 93 | 21 | 71 | 55.82 | 57.65 | 21 | 57 | Optimal, sd |
| 12 | 128 | 23 | 83 | 64.13 | 107.23 | - | - | |
| 13 | 315 | 45 | 101 | 78.38 | 71.07 | 45 | 81 | sd |
| 14 | 448 | 27 | 135 | 91.07 | 108.42 | 27 | 135 | Optimal, sd |
| 15 | 675 | 45 | 137 | 105.89 | 127.36 | 45 | 105 | sd |
| 16 | 2048 | 85 | 157 | 115.82 | 114.59 | - | - | |
| 17 | 3825 | 81 | 177 | 136.83 | 136.67 | 81 | 171 | sd |
| 18 | 5376 | 35 | 243 | 153.51 | 185.12 | 35 | 243 | Optimal, sd |
| 19 | 13797 | 117 | 229 | 172.00 | 171.91 | 117 | 201 | sd |
| 20 | 24576 | 63 | 257 | 190.81 | 205.81 | - | - | |
| 21 | 27783 | 95 | 277 | 210.97 | 216.43 | 105 | 237 | |
| 22 | 95232 | 63 | 363 | 231.93 | 238.56 | 63 | 363 | $m_{C_N} = 3n - 3$ |
| 23 | 182183 | 45 | 325 | 254.02 | 254.60 | 45 | 309 | Optimal, sd |
| 24 | 262144 | 105 | 375 | 276.89 | 281.01 | - | - | |
| 25 | 629145 | 93 | 383 | 301.01 | 300.37 | 93 | 357 | sd |
| 26 | 1290240 | 51 | 555 | 325.96 | 328.59 | 51 | 555 | Optimal, sd |
| 27 | 1835001 | 141 | 443 | 351.99 | 351.38 | 141 | 413 | |
| 28 | 3670016 | 55 | 517 | 378.98 | 379.12 | - | - | Optimal |
| 29 | 9256395 | 57 | 521 | 407.00 | 406.21 | 57 | 465 | Optimal, sd |
| 30 | 11059200 | 59 | 759 | 435.95 | 438.52 | 59 | 759 | Optimal, sd |
| 31 | 28629151 | 237 | 587 | 466.00 | 465.21 | 237 | 537 | sd |
| 32 | 67108864 | 361 | 621 | 497.00 | 496.07 | - | - | |
| 33 | 97327197 | 65 | 693 | 529.00 | 528.44 | 65 | 693 | Optimal, sd |
| 34 | 250675200 | 243 | 819 | 562.00 | 561.52 | 243 | 819 | sd |
| 35 | 352149515 | 69 | 779 | 596.00 | 595.08 | 69 | 693 | Optimal, sd |
| 36 | 704643060 | 71 | 1017 | 630.99 | 630.51 | - | - | Optimal |
| 37 | 1857283155 | 141 | 823 | 667 | 666.04 | 141 | | sd |
| 38 | 3616800703 | 207 | 1131 | 704.00 | 703.18 | 207 | | |
| 39 | 5282242828 | 77 | 933 | 742.00 | 741.09 | 77 | | Optimal, sd |

**Table 2.2.4** Statistics for normal bases of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ obtained by exhaustive search, $n \leq 39$.

**2.2.12 Remark** Our first conjecture based on Table 2.2.4 appears in [3036] and elsewhere. We also summarize the conjectures found in [2015].

**2.2.13 Conjecture** When no optimal normal basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ exists, the minimum complexity of a normal basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ is $3n - 3$.

**2.2.14 Remark** Normal bases of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ achieving a complexity of $3n-3$ are given in Proposition 5.3.46 and this complexity is the minimal found when $n = 8$ and $n = 22$.

**2.2.15 Conjecture** The number of normal bases of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ are normally distributed with respect to their complexities. Furthermore, the average complexity of a normal basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ is $(n^2-n+3)/2$ and the variance is also $n^2/2-cn$, for a small positive constant $c$.

**2.2.16 Remark** We remark that the conspicuous wording in Conjecture 2.2.15, that normal bases are normally distributed, is mostly coincidental. Indeed, as $n$ grows, the number of normal bases grow like $2^n/\log(n)$, see Theorem 5.2.13, so the Central Limit Theorem supports this conjecture. The precise distribution of the complexities is still an open and interesting problem.

**2.2.17 Remark** Self-dual normal bases are often preferred in normal basis implementations due to their highly symmetric properties; see Sections 5.1, 5.2, 5.3, 16.7 as well as [1264, 2925], for more information on self-dual normal bases and their implementations. Exhaustive searches of self-dual normal bases of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ appear in [130, 1263, 1631, 2015] and [130] gives an exhastive search of self-dual normal bases of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ for larger $q$ and odd $n$. Tables 2.2.5, 2.2.6 and 2.2.7 are directly from [130]; we note that we did not implement their algorithm. Table 2.2.5 gives the minimum complexity $C_n$ of a self-dual normal basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ for odd $n \leq 45$, Table 2.2.6 for $q$ a power of 2 and small $n$, and Table 2.2.7 for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ for odd $q \leq 19$ and small $n$.

| $n$ | 3 | 5 | 7 | 9 | 11 | 13 | 15 | 17 | 19 | 21 | 23 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $C_n$ | 5 | 9 | 21 | 17 | 21 | 45 | 45 | 81 | 117 | 105 | 45 |

| $n$ | 25 | 27 | 29 | 31 | 33 | 35 | 37 | 39 | 41 | 43 | 45 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $C_n$ | 93 | 141 | 57 | 237 | 65 | 69 | 141 | 77 | 81 | 165 | 153 |

**Table 2.2.5** The lowest complexity for self-dual normal bases of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ for odd $n$, $n \leq 45$.

| $q/n$ | 3 | 5 | 7 | 9 | 11 | 13 | 15 | 17 | 19 | 21 | 23 | 25 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2 | 5 | 9 | 21 | 17 | 21 | 45 | 45 | 81 | 117 | 105 | 45 | 93 |
| 4 | 5 | 9 | 21 | 17 | 21 | 45 | 45 | 81 | 117 | 105 | 45 | 93 |
| 8 | 9 | 9 | 21 | 45 | 21 | 45 | 81 | 81 | | | | |
| 16 | 5 | 9 | 21 | 17 | 21 | 45 | | | | | | |
| 32 | 5 | 19 | 21 | 17 | 21 | | | | | | | |
| 64 | 9 | 9 | 21 | 45 | | | | | | | | |
| 128 | 5 | 9 | 37 | | | | | | | | | |
| 256 | 5 | 9 | | | | | | | | | | |

**Table 2.2.6** Lowest complexity for self-dual normal bases of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ where $q$ is a power of 2 for small odd values of $n$.

| $q/n$ | 3 | 5 | 7 | 9 | 11 | 13 | 15 | 17 | 19 | 21 | 23 | 25 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 3 | 7 | 13 | 25 | 37 | 55 | 67 | – | 91 | 172 | – | 127 | 135 |
| 5 | 6 | 13 | 25 | 46 | 64 | 85 | – | 157 | 153 | 150 | | |
| 7 | 6 | 16 | 19 | 41 | 61 | 96 | 87 | | | – | | |
| 11 | 6 | 13 | 25 | 52 | 31 | 100 | 78 | | | | | |
| 13 | 6 | 13 | 25 | 51 | 64 | 37 | | | | | | |
| 17 | 8 | 13 | 25 | 51 | 64 | 100 | | – | | | | |
| 19 | 8 | 13 | 31 | 51 | 67 | | | | – | | | |

**Table 2.2.7** Lowest complexity for self-dual normal bases of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ for odd primes $q \leq 19$ and small odd values of $n$.

#### 2.2.2.2 Minimum type of a Gauss period admitting a normal basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$

**2.2.18 Remark** We briefly recall the definition of a Gauss period (Definition 5.3.16). Let $r = nk+1$ be a prime not dividing $q$ and let $\gamma$ be a primitive $r$-th root of unity in $\mathbb{F}_{q^{nk}}$. Furthermore, let $K$ be the unique subgroup of order $k$ in $\mathbb{Z}_r^*$ and $K_i = \{a \cdot q^i : a \in K\} \subseteq \mathbb{Z}_r^*$ be cosets of $K$, $0 \leq i \leq n-1$. The elements

$$\alpha_i = \sum_{a \in K_i} \gamma^a \in \mathbb{F}_{q^n}, \quad 0 \leq i \leq n-1,$$

are *Gauss periods* of type $(n,k)$ over $\mathbb{F}_q$. Gauss periods over finite fields are highly desirable as normal bases since, when they exist, they have low complexity; see Theorem 5.3.23. Normal bases due to Gauss periods of type $(n,1)$, for all $q$, and of type $(n,2)$, for $q = 2$, characterize the *optimal normal bases* (Theorem 5.3.6) and have complexity $2n-1$. Gauss periods also often have high order, see Remark 5.3.49. For conditions on when Gauss periods of type $(n,k)$ admit normal bases of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, see Theorem 5.3.17. In particular, we note that there is no Gauss period of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ which admits a normal basis when 8 divides $n$.

Table 2.2.8 gives the lowest $k$ for which a *Gauss period* of type $(n,k)$ admits a normal basis of $\mathbb{F}_{2^n}$ pver $\mathbb{F}_2$ for $n \leq 577$. We give a similar table over $\mathbb{F}_3$ in Table 2.2.9. This range was chosen to cover degrees for common implementations of finite field arithmetic. The output of the table is in the format "$n,k''$ where $k$ is the minimum number admitting a type $(n,k)$ Gauss period over $\mathbb{F}_{q^n}$, where $q = 2,3$.

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 2,1 | 3,2 | 4,1 | 5,2 | 6,2 | 7,4 | 9,2 | 10,1 | 11,2 | 12,1 | 13,4 | 14,2 |
| 15,4 | 17,6 | 18,1 | 19,10 | 20,3 | 21,10 | 22,3 | 23,2 | 25,4 | 26,2 | 27,6 | 28,1 |
| 29,2 | 30,2 | 31,10 | 33,2 | 34,9 | 35,2 | 36,1 | 37,4 | 38,6 | 39,2 | 41,2 | 42,5 |
| 43,4 | 44,9 | 45,4 | 46,3 | 47,6 | 49,4 | 50,2 | 51,2 | 52,1 | 53,2 | 54,3 | 55,12 |
| 57,10 | 58,1 | 59,12 | 60,1 | 61,6 | 62,6 | 63,6 | 65,2 | 66,1 | 67,4 | 68,9 | 69,2 |
| 70,3 | 71,8 | 73,4 | 74,2 | 75,10 | 76,3 | 77,6 | 78,7 | 79,4 | 81,2 | 82,1 | 83,2 |
| 84,5 | 85,12 | 86,2 | 87,4 | 89,2 | 90,2 | 91,6 | 92,3 | 93,4 | 94,3 | 95,2 | 97,4 |
| 98,2 | 99,2 | 100,1 | 101,6 | 102,6 | 103,6 | 105,2 | 106,1 | 107,6 | 108,5 | 109,10 | 110,6 |
| 111,20 | 113,2 | 114,5 | 115,4 | 116,3 | 117,8 | 118,6 | 119,2 | 121,6 | 122,6 | 123,10 | 124,3 |
| 125,6 | 126,3 | 127,4 | 129,8 | 130,1 | 131,2 | 132,5 | 133,12 | 134,2 | 135,2 | 137,6 | 138,1 |
| 139,4 | 140,3 | 141,8 | 142,6 | 143,6 | 145,10 | 146,2 | 147,6 | 148,1 | 149,8 | 150,19 | 151,6 |
| 153,4 | 154,25 | 155,2 | 156,13 | 157,10 | 158,2 | 159,22 | 161,6 | 162,1 | 163,4 | 164,5 | 165,4 |
| 166,3 | 167,14 | 169,4 | 170,6 | 171,12 | 172,1 | 173,2 | 174,2 | 175,4 | 177,4 | 178,1 | 179,2 |
| 180,1 | 181,6 | 182,3 | 183,2 | 185,8 | 186,2 | 187,6 | 188,5 | 189,2 | 190,10 | 191,2 | 193,4 |
| 194,2 | 195,6 | 196,1 | 197,18 | 198,22 | 199,4 | 201,8 | 202,6 | 203,12 | 204,3 | 205,4 | 206,3 |
| 207,4 | 209,2 | 210,1 | 211,10 | 212,5 | 213,4 | 214,3 | 215,6 | 217,6 | 218,5 | 219,4 | 220,3 |
| 221,2 | 222,10 | 223,12 | 225,22 | 226,1 | 227,24 | 228,9 | 229,12 | 230,2 | 231,2 | 233,2 | 234,5 |
| 235,4 | 236,3 | 237,10 | 238,7 | 239,2 | 241,6 | 242,6 | 243,2 | 244,3 | 245,2 | 246,11 | 247,6 |
| 249,8 | 250,9 | 251,2 | 252,3 | 253,10 | 254,2 | 255,6 | 257,6 | 258,5 | 259,10 | 260,5 | 261,2 |
| 262,3 | 263,6 | 265,4 | 266,6 | 267,8 | 268,1 | 269,8 | 270,2 | 271,6 | 273,2 | 274,9 | 275,14 |
| 276,3 | 277,4 | 278,2 | 279,4 | 281,2 | 282,6 | 283,6 | 284,3 | 285,10 | 286,3 | 287,6 | 289,12 |
| 290,5 | 291,6 | 292,1 | 293,2 | 294,3 | 295,16 | 297,6 | 298,6 | 299,2 | 300,19 | 301,10 | 302,3 |
| 303,2 | 305,6 | 306,2 | 307,4 | 308,15 | 309,2 | 310,6 | 311,6 | 313,6 | 314,5 | 315,8 | 316,1 |
| 317,26 | 318,11 | 319,4 | 321,12 | 322,6 | 323,2 | 324,5 | 325,4 | 326,2 | 327,8 | 329,2 | 330,2 |
| 331,6 | 332,3 | 333,24 | 334,7 | 335,12 | 337,10 | 338,2 | 339,8 | 340,3 | 341,8 | 342,6 | 343,4 |
| 345,4 | 346,1 | 347,6 | 348,1 | 349,10 | 350,2 | 351,10 | 353,14 | 354,2 | 355,6 | 356,3 | 357,10 |
| 358,10 | 359,2 | 361,30 | 362,5 | 363,4 | 364,3 | 365,24 | 366,22 | 367,6 | 369,10 | 370,6 | 371,2 |
| 372,1 | 373,4 | 374,3 | 375,2 | 377,14 | 378,1 | 379,12 | 380,5 | 381,8 | 382,6 | 383,12 | 385,6 |
| 386,2 | 387,4 | 388,1 | 389,24 | 390,3 | 391,6 | 393,2 | 394,9 | 395,6 | 396,11 | 397,6 | 398,2 |
| 399,12 | 401,8 | 402,5 | 403,16 | 404,3 | 405,4 | 406,6 | 407,8 | 409,4 | 410,2 | 411,2 | 412,3 |
| 413,2 | 414,2 | 415,28 | 417,4 | 418,1 | 419,2 | 420,1 | 421,10 | 422,11 | 423,4 | 425,6 | 426,2 |
| 427,16 | 428,5 | 429,2 | 430,3 | 431,2 | 433,4 | 434,9 | 435,4 | 436,13 | 437,18 | 438,2 | 439,10 |
| 441,2 | 442,1 | 443,2 | 444,5 | 445,6 | 446,6 | 447,6 | 449,8 | 450,13 | 451,6 | 452,11 | 453,2 |
| 454,19 | 455,26 | 457,30 | 458,6 | 459,8 | 460,1 | 461,6 | 462,10 | 463,12 | 465,4 | 466,1 | 467,6 |
| 468,21 | 469,4 | 470,2 | 471,8 | 473,2 | 474,5 | 475,4 | 476,5 | 477,46 | 478,7 | 479,8 | 481,6 |
| 482,5 | 483,2 | 484,3 | 485,18 | 486,10 | 487,4 | 489,12 | 490,1 | 491,2 | 492,13 | 493,4 | 494,3 |
| 495,2 | 497,20 | 498,9 | 499,4 | 500,11 | 501,10 | 502,10 | 503,6 | 505,10 | 506,5 | 507,4 | 508,1 |
| 509,2 | 510,3 | 511,6 | 513,4 | 514,33 | 515,2 | 516,3 | 517,4 | 518,14 | 519,2 | 521,32 | 522,1 |
| 523,10 | 524,5 | 525,8 | 526,3 | 527,6 | 529,24 | 530,2 | 531,2 | 532,3 | 533,12 | 534,7 | 535,4 |
| 537,8 | 538,6 | 539,12 | 540,1 | 541,18 | 542,3 | 543,2 | 545,2 | 546,1 | 547,10 | 548,5 | 549,14 |
| 550,7 | 551,6 | 553,4 | 554,2 | 555,4 | 556,1 | 557,6 | 558,2 | 559,4 | 561,2 | 562,1 | 563,14 |
| 564,3 | 565,10 | 566,3 | 567,4 | 569,12 | 570,5 | 571,10 | 572,5 | 573,4 | 574,3 | 575,2 | 577,4 |

**Table 2.2.8** Lowest type of a Gauss period forming a normal basis for $q = 2$ and $n \leq 577$.

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 2,2 | 3,2 | 4,1 | 5,2 | 6,1 | 7,4 | 8,2 | 9,2 | 10,3 | 11,2 | 13,4 | 14,2 |
| 15,2 | 16,1 | 17,6 | 18,1 | 19,10 | 20,5 | 21,2 | 22,3 | 23,2 | 25,4 | 26,2 | 27,4 |
| 28,1 | 29,2 | 30,1 | 31,10 | 32,8 | 33,6 | 34,3 | 35,2 | 37,4 | 38,15 | 39,2 | 40,7 |
| 41,2 | 42,1 | 43,4 | 44,2 | 45,4 | 46,3 | 47,6 | 49,4 | 50,2 | 51,8 | 52,1 | 53,2 |
| 54,3 | 55,6 | 56,2 | 57,4 | 58,4 | 59,12 | 61,6 | 62,21 | 63,2 | 64,4 | 65,2 | 66,3 |
| 67,4 | 68,2 | 69,2 | 70,3 | 71,8 | 73,4 | 74,2 | 75,8 | 76,10 | 77,6 | 78,1 | 79,4 |
| 80,5 | 81,2 | 82,9 | 83,2 | 85,16 | 86,2 | 87,4 | 88,1 | 89,2 | 90,7 | 91,10 | 92,5 |
| 93,4 | 94,3 | 95,2 | 97,4 | 98,2 | 99,2 | 100,1 | 101,6 | 102,11 | 103,6 | 104,5 | 105,2 |
| 106,10 | 107,6 | 109,10 | 110,3 | 111,2 | 112,1 | 113,2 | 114,5 | 115,4 | 116,2 | 117,8 | 118,9 |
| 119,2 | 121,6 | 122,3 | 123,6 | 124,13 | 125,2 | 126,1 | 127,4 | 128,2 | 129,8 | 130,4 | 131,2 |
| 133,16 | 134,2 | 135,4 | 136,1 | 137,6 | 138,1 | 139,4 | 140,2 | 141,2 | 142,4 | 143,6 | 145,10 |
| 146,2 | 147,10 | 148,1 | 149,8 | 150,5 | 151,6 | 152,5 | 153,14 | 154,3 | 155,2 | 157,10 | 158,2 |
| 159,34 | 160,4 | 161,6 | 162,1 | 163,4 | 164,5 | 165,2 | 166,3 | 167,14 | 169,4 | 170,8 | 171,12 |
| 172,1 | 173,2 | 174,9 | 175,4 | 176,2 | 177,4 | 178,15 | 179,2 | 181,6 | 182,14 | 183,4 | 184,7 |
| 185,8 | 186,15 | 187,6 | 188,5 | 189,2 | 190,3 | 191,2 | 193,4 | 194,2 | 195,10 | 196,1 | 197,18 |
| 198,1 | 199,4 | 200,2 | 201,10 | 202,3 | 203,12 | 205,4 | 206,3 | 207,4 | 208,10 | 209,2 | 210,1 |
| 211,10 | 212,5 | 213,6 | 214,3 | 215,6 | 217,6 | 218,15 | 219,4 | 220,4 | 221,2 | 222,1 | 223,12 |
| 224,2 | 225,8 | 226,15 | 227,24 | 229,12 | 230,2 | 231,2 | 232,1 | 233,2 | 234,5 | 235,4 | 236,8 |
| 237,6 | 238,4 | 239,2 | 241,6 | 242,3 | 243,2 | 244,4 | 245,24 | 246,3 | 247,6 | 248,11 | 249,8 |
| 250,3 | 251,2 | 253,4 | 254,2 | 255,12 | 256,1 | 257,6 | 258,5 | 259,10 | 260,2 | 261,6 | 262,3 |
| 263,6 | 265,4 | 266,8 | 267,4 | 268,1 | 269,8 | 270,3 | 271,6 | 272,5 | 273,10 | 274,3 | 275,12 |
| 277,4 | 278,2 | 279,10 | 280,1 | 281,2 | 282,1 | 283,6 | 284,2 | 285,2 | 286,3 | 287,6 | 289,12 |
| 290,20 | 291,6 | 292,1 | 293,2 | 294,5 | 295,12 | 296,2 | 297,8 | 298,4 | 299,2 | 301,10 | 302,3 |
| 303,2 | 304,4 | 305,6 | 306,7 | 307,4 | 308,2 | 309,4 | 310,15 | 311,6 | 313,6 | 314,14 | 315,2 |
| 316,1 | 317,26 | 318,17 | 319,4 | 320,2 | 321,18 | 322,3 | 323,2 | 325,4 | 326,2 | 327,10 | 328,7 |
| 329,2 | 330,1 | 331,6 | 332,8 | 333,6 | 334,15 | 335,6 | 337,10 | 338,2 | 339,10 | 340,4 | 341,8 |
| 342,13 | 343,4 | 344,5 | 345,2 | 346,3 | 347,6 | 349,10 | 350,2 | 351,22 | 352,1 | 353,14 | 354,3 |
| 355,12 | 356,11 | 357,4 | 358,4 | 359,2 | 361,30 | 362,3 | 363,4 | 364,7 | 365,18 | 366,5 | 367,6 |
| 368,11 | 369,2 | 370,4 | 371,2 | 373,4 | 374,3 | 375,2 | 376,7 | 377,14 | 378,1 | 379,12 | 380,5 |
| 381,20 | 382,10 | 383,12 | 385,6 | 386,2 | 387,14 | 388,1 | 389,24 | 390,5 | 391,6 | 392,8 | 393,10 |
| 394,9 | 395,6 | 397,6 | 398,2 | 399,12 | 400,1 | 401,8 | 402,5 | 403,4 | 404,2 | 405,2 | 406,21 |
| 407,8 | 409,4 | 410,2 | 411,2 | 412,19 | 413,2 | 414,9 | 415,30 | 416,5 | 417,6 | 418,15 | 419,2 |
| 421,10 | 422,21 | 423,4 | 424,4 | 425,12 | 426,3 | 427,4 | 428,2 | 429,2 | 430,3 | 431,2 | 433,4 |
| 434,3 | 435,4 | 436,13 | 437,18 | 438,9 | 439,10 | 440,2 | 441,6 | 442,3 | 443,2 | 445,6 | 446,15 |
| 447,4 | 448,1 | 449,8 | 450,33 | 451,6 | 452,8 | 453,2 | 454,28 | 455,2 | 457,30 | 458,15 | 459,8 |
| 460,1 | 461,6 | 462,1 | 463,12 | 464,2 | 465,10 | 466,3 | 467,6 | 469,10 | 470,2 | 471,8 | 472,4 |
| 473,2 | 474,3 | 475,4 | 476,2 | 477,14 | 478,4 | 479,8 | 481,28 | 482,3 | 483,10 | 484,7 | 485,2 |
| 486,1 | 487,4 | 488,2 | 489,12 | 490,15 | 491,2 | 493,4 | 494,3 | 495,30 | 496,13 | 497,14 | 498,11 |
| 499,4 | 500,8 | 501,16 | 502,9 | 503,6 | 505,10 | 506,2 | 507,18 | 508,1 | 509,2 | 510,7 | 511,6 |
| 512,23 | 513,4 | 514,3 | 515,2 | 517,4 | 518,9 | 519,2 | 520,1 | 521,32 | 522,3 | 523,10 | 524,2 |
| 525,20 | 526,3 | 527,6 | 529,24 | 530,2 | 531,2 | 532,4 | 533,12 | 534,27 | 535,4 | 536,8 | 537,8 |
| 538,4 | 539,12 | 541,18 | 542,3 | 543,2 | 544,10 | 545,6 | 546,5 | 547,10 | 548,2 | 549,18 | 550,21 |
| 551,2 | 553,4 | 554,2 | 555,6 | 556,1 | 557,6 | 558,5 | 559,4 | 560,5 | 561,2 | 562,9 | 563,14 |
| 565,6 | 566,3 | 567,28 | 568,1 | 569,12 | 570,1 | 571,10 | 572,5 | 573,4 | 574,3 | 575,2 | 577,4 |

**Table 2.2.9** Lowest type of a Gauss period forming a normal basis for $q = 3$ and $n \leq 577$.

#### 2.2.2.3 Minimum-known complexity of a normal basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$, $n \geq 40$

**2.2.19 Remark** Table 2.2.10 gives the minimum complexity of a normal basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ for $40 \leq n \leq 721$ by using a combination of the exhaustive search data of Table 2.2.4 and theorems from Section 5.3. In each row, we give the degree $n$, the minimum complexity $C_n$ of a normal basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$, the method by which the normal basis was obtained and what property or parameters were used. In the "Method" column, "Optimal" indicates existence of an optimal normal basis, "GNB" indicates the basis arises as a Gauss period and their type is given in the "Property" column. Proposition 5.3.38 constructs normal bases of $\mathbb{F}_{q^n}$ using normal bases of subfields of coprime degree. When this method wins, the values of these coprime factors are indicated in the "Property" column. Corollary 5.3.15 requires an optimal normal basis of $\mathbb{F}_{2^{kn}}$ and the type of the optimal normal basis and the value of $k$ are indicated in the "Property" column. Finally, "sd" indicates that the basis is self-dual.

When $n$ is a power of 2, the best result, when available, is by random search since known methods do not apply. Gauss periods cannot form normal bases when 8 divides $n$, see Proposition 5.3.20, and $n$ contains no coprime factors with which to apply Proposition 5.3.38. By Conjecture 2.2.15, the complexity of these bases is likely to approach $n^2/2$.

**2.2.20 Problem** Find constructions of low complexity normal bases of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ when $n$ is a prime power, specifically a power of 2.

| $n$ | $C_n$ | Method | Property |
|---|---|---|---|
| 40 | 189 | Prop. 5.3.38 | 5, 8 |
| 41 | 81 | Optimal | Type 2, sd |
| 42 | 135 | Prop. 5.3.38 | 3, 14 |
| 43 | 165 | GNB | $k = 4$, sd |
| 44 | 147 | Prop. 5.3.38 | 4, 11 |
| 45 | 153 | Search | [130], sd |
| 46 | 135 | Prop. 5.3.38 | 2, 23 |
| 47 | 261 | GNB | $k = 6$, sd |
| 48 | 425 | Prop. 5.3.38 | 3, 16 |
| 49 | 189 | GNB | $k = 4$, sd |
| 50 | 99 | Optimal | Type 2, sd |
| 51 | 101 | Optimal | Type 2, sd |
| 52 | 103 | Optimal | Type 1 |
| 53 | 105 | Optimal | Type 2, sd |
| 54 | 209 | GNB | $k = 3$ |
| 55 | 189 | Prop. 5.3.38 | 5, 11 |
| 56 | 399 | Prop. 5.3.38 | 7, 8 |
| 57 | 497 | Search | [1263], sd |
| 58 | 115 | Optimal | Type 1 |
| 59 | 597 | Search | [1263], sd |
| 60 | 119 | Optimal | Type 1 |
| 61 | 345 | GNB | $k = 6$, sd |
| 62 | 351 | GNB | $k = 6$, sd |
| 63 | 323 | Prop. 5.3.38 | 7, 9 |
| 64 | 1829 | Random | |
| 65 | 129 | Optimal | Type 2, sd |
| 66 | 131 | Optimal | Type 1 |
| 67 | 261 | GNB | $k = 4$, sd |
| 68 | 567 | Prop. 5.3.38 | 4, 17 |
| 69 | 137 | Optimal | Type 2, sd |
| 70 | 207 | Prop. 5.3.38 | 2, 35 |
| 71 | 567 | GNB | $k = 8$, sd |
| 72 | 357 | Prop. 5.3.38 | 8, 9 |
| 73 | 285 | GNB | $k = 4$, sd |
| 74 | 147 | Optimal | Type 2, sd |
| 75 | 465 | Prop. 5.3.38 | 3, 25 |
| 76 | 297 | GNB | $k = 3$ |
| 77 | 399 | Prop. 5.3.38 | 7, 11 |
| 78 | 231 | Prop. 5.3.38 | 2, 39 |
| 79 | 309 | GNB | $k = 4$, sd |
| 80 | 765 | Prop. 5.3.38 | 5, 16 |
| 81 | 161 | Optimal | Type 2, sd |
| 82 | 163 | Optimal | Type 1 |
| 83 | 165 | Optimal | Type 2, sd |
| 84 | 275 | Prop. 5.3.38 | 3, 28 |
| 85 | 729 | Prop. 5.3.38 | 5, 17 |
| 86 | 171 | Optimal | Type 2, sd |
| 87 | 285 | Prop. 5.3.38 | 3, 29 |
| 88 | 441 | Prop. 5.3.38 | 8, 11 |
| 89 | 177 | Optimal | Type 2, sd |
| 90 | 179 | Optimal | Type 2, sd |
| 91 | 525 | GNB | $k = 6$, sd |
| 92 | 315 | Prop. 5.3.38 | 4, 23 |
| 93 | 365 | GNB | $k = 4$, sd |
| 94 | 369 | GNB | $k = 3$ |
| 95 | 189 | Optimal | Type 2, sd |
| 96 | 1805 | Prop. 5.3.38 | 3, 32 |
| 97 | 381 | GNB | $k = 4$, sd |
| 98 | 195 | Optimal | Type 2, sd |
| 99 | 197 | Optimal | Type 2, sd |
| 100 | 199 | Optimal | Type 1 |
| 101 | 585 | GNB | $k = 6$, sd |
| 102 | 303 | Prop. 5.3.38 | 2, 51 |
| 103 | 597 | GNB | $k = 6$, sd |
| 104 | 945 | Prop. 5.3.38 | 8, 13 |
| 105 | 209 | Optimal | Type 2, sd |
| 106 | 211 | Optimal | Type 1 |
| 107 | 621 | GNB | $k = 6$, sd |
| 108 | 627 | GNB | $k = 5$ |
| 109 | 1081 | Cor. 5.3.15 | Type 2, $k = 5$, sd |
| 110 | 399 | Prop. 5.3.38 | 10, 11 |
| 111 | 705 | Prop. 5.3.38 | 3, 37 |
| 112 | 1615 | Prop. 5.3.38 | 7, 16 |
| 113 | 225 | Optimal | Type 2, sd |
| 114 | 663 | GNB | $k = 5$ |
| 115 | 405 | Prop. 5.3.38 | 5, 23 |
| 116 | 399 | Prop. 5.3.38 | 4, 29 |
| 117 | 765 | Prop. 5.3.38 | 9, 13 |
| 118 | 687 | GNB | $k = 6$, sd |
| 119 | 237 | Optimal | Type 2, sd |
| 120 | 945 | Prop. 5.3.38 | 3, 40 |
| 121 | 705 | GNB | $k = 6$, sd |
| 122 | 711 | GNB | $k = 6$, sd |
| 123 | 405 | Prop. 5.3.38 | 3, 41 |
| 124 | 489 | GNB | $k = 3$ |
| 125 | 729 | GNB | $k = 6$, sd |
| 126 | 459 | Prop. 5.3.38 | 9, 14 |
| 127 | 501 | GNB | $k = 4$, sd |
| 128 | 7821 | Random | |
| 129 | 825 | Prop. 5.3.38 | 3, 43 |
| 130 | 259 | Optimal | Type 1 |
| 131 | 261 | Optimal | Type 2, sd |
| 132 | 455 | Prop. 5.3.38 | 4, 33 |
| 133 | 1595 | GNB | $k = 12$, sd |
| 134 | 267 | Optimal | Type 2, sd |
| 135 | 269 | Optimal | Type 2, sd |
| 136 | 1701 | Prop. 5.3.38 | 8, 17 |
| 137 | 801 | GNB | $k = 6$, sd |
| 138 | 275 | Optimal | Type 1 |
| 139 | 549 | GNB | $k = 4$, sd |
| 140 | 483 | Prop. 5.3.38 | 4, 35 |
| 141 | 1127 | GNB | $k = 8$, sd |
| 142 | 831 | GNB | $k = 6$, sd |
| 143 | 837 | GNB | $k = 6$, sd |
| 144 | 1445 | Prop. 5.3.38 | 9, 16 |
| 145 | 513 | Prop. 5.3.38 | 5, 29 |
| 146 | 291 | Optimal | Type 2, sd |
| 147 | 861 | GNB | $k = 6$, sd |
| 148 | 295 | Optimal | Type 1 |
| 149 | 1191 | GNB | $k = 8$, sd |
| 150 | 495 | Prop. 5.3.38 | 3, 50 |
| 151 | 885 | GNB | $k = 6$, sd |
| 152 | 2457 | Prop. 5.3.38 | 8, 19 |
| 153 | 605 | GNB | $k = 4$, sd |
| 154 | 567 | Prop. 5.3.38 | 11, 14 |
| 155 | 309 | Optimal | Type 2, sd |
| 156 | 515 | Prop. 5.3.38 | 3, 52 |
| 157 | 1561 | Cor. 5.3.15 | Type 2, $k = 5$, sd |
| 158 | 315 | Optimal | Type 2, sd |
| 159 | 525 | Prop. 5.3.38 | 3, 53 |
| 160 | 3249 | Prop. 5.3.38 | 5, 32 |
| 161 | 855 | Prop. 5.3.38 | 7, 23 |
| 162 | 323 | Optimal | Type 1 |
| 163 | 645 | GNB | $k = 4$, sd |
| 164 | 567 | Prop. 5.3.38 | 4, 41 |
| 165 | 585 | Prop. 5.3.38 | 5, 33 |
| 166 | 495 | Prop. 5.3.38 | 2, 83 |
| 167 | 2325 | Cor. 5.3.15 | Type 2, $k = 7$, sd |
| 168 | 1995 | Prop. 5.3.38 | 3, 56 |
| 169 | 669 | GNB | $k = 4$, sd |
| 170 | 999 | GNB | $k = 6$, sd |
| 171 | 1989 | Prop. 5.3.38 | 9, 19 |
| 172 | 343 | Optimal | Type 1 |
| 173 | 345 | Optimal | Type 2, sd |
| 174 | 347 | Optimal | Type 2, sd |
| 175 | 693 | GNB | $k = 4$, sd |
| 176 | 1785 | Prop. 5.3.38 | 11, 16 |
| 177 | 701 | GNB | $k = 4$, sd |
| 178 | 355 | Optimal | Type 1 |
| 179 | 357 | Optimal | Type 2, sd |
| 180 | 359 | Optimal | Type 1 |
| 181 | 1065 | GNB | $k = 6$, sd |
| 182 | 721 | GNB | $k = 3$ |
| 183 | 365 | Optimal | Type 2, sd |
| 184 | 945 | Prop. 5.3.38 | 8, 23 |
| 185 | 1269 | Prop. 5.3.38 | 5, 37 |
| 186 | 371 | Optimal | Type 2, sd |
| 187 | 1101 | GNB | $k = 6$, sd |
| 188 | 1107 | GNB | $k = 5$ |
| 189 | 377 | Optimal | Type 2, sd |
| 190 | 567 | Prop. 5.3.38 | 2, 95 |
| 191 | 381 | Optimal | Type 2, sd |
| 192 | 9145 | Prop. 5.3.38 | 3, 64 |
| 193 | 765 | GNB | $k = 4$, sd |
| 194 | 387 | Optimal | Type 2, sd |
| 195 | 645 | Prop. 5.3.38 | 3, 65 |
| 196 | 391 | Optimal | Type 1 |
| 197 | 3529 | Cor. 5.3.15 | Type 2, $k = 9$, sd |
| 198 | 591 | Prop. 5.3.38 | 2, 99 |
| 199 | 789 | GNB | $k = 4$, sd |
| 200 | 1953 | Prop. 5.3.38 | 8, 25 |
| 201 | 1305 | Prop. 5.3.38 | 3, 67 |
| 202 | 1191 | GNB | $k = 6$, sd |
| 203 | 1083 | Prop. 5.3.38 | 7, 29 |
| 204 | 707 | Prop. 5.3.38 | 4, 51 |
| 205 | 729 | Prop. 5.3.38 | 5, 41 |
| 206 | 817 | GNB | $k = 3$ |
| 207 | 765 | Prop. 5.3.38 | 9, 23 |
| 208 | 3825 | Prop. 5.3.38 | 13, 16 |
| 209 | 417 | Optimal | Type 2, sd |
| 210 | 419 | Optimal | Type 1 |
| 211 | 2101 | Cor. 5.3.15 | Type 2, $k = 5$, sd |
| 212 | 735 | Prop. 5.3.38 | 4, 53 |
| 213 | 845 | GNB | $k = 4$, sd |
| 214 | 849 | GNB | $k = 3$ |
| 215 | 1269 | GNB | $k = 6$, sd |

| $n$ | $C_n$ | Method | Property |
|---|---|---|---|
| 216 | 2961 | Prop. 5.3.38 | $8, 27$ |
| 217 | 1281 | GNB | $k = 6$, sd |
| 218 | 1287 | GNB | $k = 5$ |
| 219 | 869 | GNB | $k = 4$, sd |
| 220 | 873 | GNB | $k = 3$ |
| 221 | 441 | Optimal | Type 2, sd |
| 222 | 735 | Prop. 5.3.38 | $3, 74$ |
| 223 | 2665 | Cor. 5.3.15 | Type 2, $k = 6$, sd |
| 224 | 6859 | Prop. 5.3.38 | $7, 32$ |
| 225 | 1581 | Prop. 5.3.38 | $9, 25$ |
| 226 | 451 | Optimal | Type 1 |
| 227 | 5447 | GNB | $k = 24$, sd |
| 228 | 1485 | Prop. 5.3.38 | $3, 76$ |
| 229 | 2747 | GNB | $k = 12$, sd |
| 230 | 459 | Optimal | Type 2, sd |
| 231 | 461 | Optimal | Type 2, sd |
| 232 | 1197 | Prop. 5.3.38 | $8, 29$ |
| 233 | 465 | Optimal | Type 2, sd |
| 234 | 867 | Prop. 5.3.38 | $9, 26$ |
| 235 | 933 | GNB | $k = 4$, sd |
| 236 | 937 | GNB | $k = 3$ |
| 237 | 1545 | Prop. 5.3.38 | $3, 79$ |
| 238 | 711 | Prop. 5.3.38 | $2, 119$ |
| 239 | 477 | Optimal | Type 2, sd |
| 240 | 3825 | Prop. 5.3.38 | $3, 80$ |
| 241 | 1425 | GNB | $k = 6$, sd |
| 242 | 1431 | GNB | $k = 6$, sd |
| 243 | 485 | Optimal | Type 2, sd |
| 244 | 969 | GNB | $k = 3$ |
| 245 | 489 | Optimal | Type 2, sd |
| 246 | 815 | Prop. 5.3.38 | $3, 82$ |
| 247 | 1461 | GNB | $k = 6$, sd |
| 248 | 4977 | Prop. 5.3.38 | $8, 31$ |
| 249 | 825 | Prop. 5.3.38 | $3, 83$ |
| 250 | 2187 | Prop. 5.3.38 | $2, 125$ |
| 251 | 501 | Optimal | Type 2, sd |
| 252 | 935 | Prop. 5.3.38 | $9, 28$ |
| 253 | 945 | Prop. 5.3.38 | $11, 23$ |
| 254 | 507 | Optimal | Type 2, sd |
| 255 | 909 | Prop. 5.3.38 | $5, 51$ |
| 256 | | No data | Prime power |
| 257 | 1521 | GNB | $k = 6$, sd |
| 258 | 855 | Prop. 5.3.38 | $3, 86$ |
| 259 | 2581 | Cor. 5.3.15 | Type 2, $k = 5$, sd |
| 260 | 903 | Prop. 5.3.38 | $4, 65$ |
| 261 | 521 | Optimal | Type 2, sd |
| 262 | 783 | Prop. 5.3.38 | $2, 131$ |
| 263 | 1557 | GNB | $k = 6$, sd |
| 264 | 1365 | Prop. 5.3.38 | $8, 33$ |
| 265 | 945 | Prop. 5.3.38 | $5, 53$ |
| 266 | 1575 | GNB | $k = 6$, sd |
| 267 | 885 | Prop. 5.3.38 | $3, 89$ |
| 268 | 535 | Optimal | Type 1 |
| 269 | 2151 | GNB | $k = 8$, sd |
| 270 | 539 | Optimal | Type 2, sd |
| 271 | 1605 | GNB | $k = 6$, sd |
| 272 | 6885 | Prop. 5.3.38 | $16, 17$ |
| 273 | 545 | Optimal | Type 2, sd |
| 274 | 2403 | Prop. 5.3.38 | $2, 137$ |
| 275 | 1953 | Prop. 5.3.38 | $11, 25$ |
| 276 | 959 | Prop. 5.3.38 | $4, 69$ |
| 277 | 1101 | GNB | $k = 4$, sd |
| 278 | 555 | Optimal | Type 2, sd |
| 279 | 1109 | GNB | $k = 4$, sd |
| 280 | 1449 | Prop. 5.3.38 | $8, 35$ |
| 281 | 561 | Optimal | Type 2, sd |
| 282 | 1671 | GNB | $k = 6$, sd |
| 283 | 1677 | GNB | $k = 6$, sd |
| 284 | 1129 | GNB | $k = 3$ |
| 285 | 945 | Prop. 5.3.38 | $3, 95$ |
| 286 | 1071 | Prop. 5.3.38 | $11, 26$ |
| 287 | 1539 | Prop. 5.3.38 | $7, 41$ |
| 288 | 6137 | Prop. 5.3.38 | $9, 32$ |
| 289 | 3457 | Cor. 5.3.15 | Type 2, $k = 6$, sd |
| 290 | 1035 | Prop. 5.3.38 | $5, 58$ |
| 291 | 1725 | GNB | $k = 6$, sd |
| 292 | 583 | Optimal | Type 1 |
| 293 | 585 | Optimal | Type 2, sd |
| 294 | 975 | Prop. 5.3.38 | $3, 98$ |
| 295 | 4719 | GNB | $k = 16$, sd |
| 296 | 2961 | Prop. 5.3.38 | $8, 37$ |
| 297 | 1761 | GNB | $k = 6$, sd |
| 298 | 1767 | GNB | $k = 6$, sd |
| 299 | 597 | Optimal | Type 2, sd |
| 300 | 995 | Prop. 5.3.38 | $3, 100$ |
| 301 | 3001 | Cor. 5.3.15 | Type 2, $k = 5$, sd |
| 302 | 1201 | GNB | $k = 3$ |
| 303 | 605 | Optimal | Type 2, sd |

| $n$ | $C_n$ | Method | Property |
|---|---|---|---|
| 304 | 9945 | Prop. 5.3.38 | $16, 19$ |
| 305 | 1809 | GNB | $k = 6$, sd |
| 306 | 611 | Optimal | Type 2, sd |
| 307 | 1221 | GNB | $k = 4$, sd |
| 308 | 1155 | Prop. 5.3.38 | $11, 28$ |
| 309 | 617 | Optimal | Type 2, sd |
| 310 | 927 | Prop. 5.3.38 | $2, 155$ |
| 311 | 1845 | GNB | $k = 6$, sd |
| 312 | 1617 | Prop. 5.3.38 | $8, 39$ |
| 313 | 1857 | GNB | $k = 6$, sd |
| 314 | 1863 | GNB | $k = 5$ |
| 315 | 1173 | Prop. 5.3.38 | $9, 35$ |
| 316 | 631 | Optimal | Type 1 |
| 317 | 8217 | Cor. 5.3.15 | Type 2, $k = 13$, sd |
| 318 | 1055 | Prop. 5.3.38 | $3, 106$ |
| 319 | 1197 | Prop. 5.3.38 | $11, 29$ |
| 320 | 16461 | Prop. 5.3.38 | $5, 64$ |
| 321 | 3105 | Prop. 5.3.38 | $3, 107$ |
| 322 | 1215 | Prop. 5.3.38 | $14, 23$ |
| 323 | 645 | Optimal | Type 2, sd |
| 324 | 1127 | Prop. 5.3.38 | $4, 81$ |
| 325 | 1293 | GNB | $k = 4$, sd |
| 326 | 651 | Optimal | Type 2, sd |
| 327 | 2615 | GNB | $k = 8$, sd |
| 328 | 1701 | Prop. 5.3.38 | $8, 41$ |
| 329 | 657 | Optimal | Type 2, sd |
| 330 | 659 | Optimal | Type 2, sd |
| 331 | 1965 | GNB | $k = 6$, sd |
| 332 | 1155 | Prop. 5.3.38 | $4, 83$ |
| 333 | 2397 | Prop. 5.3.38 | $9, 37$ |
| 334 | 2629 | GNB | $k = 7$ |
| 335 | 2349 | Prop. 5.3.38 | $5, 67$ |
| 336 | 8075 | Prop. 5.3.38 | $3, 112$ |
| 337 | 3361 | Cor. 5.3.15 | Type 2, $k = 5$, sd |
| 338 | 675 | Optimal | Type 2, sd |
| 339 | 1125 | Prop. 5.3.38 | $3, 113$ |
| 340 | 1353 | GNB | $k = 3$ |
| 341 | 2727 | GNB | $k = 8$, sd |
| 342 | 2031 | GNB | $k = 6$, sd |
| 343 | 1365 | GNB | $k = 4$, sd |
| 344 | 3465 | Prop. 5.3.38 | $8, 43$ |
| 345 | 1233 | Prop. 5.3.38 | $5, 69$ |
| 346 | 691 | Optimal | Type 1 |
| 347 | 2061 | GNB | $k = 6$, sd |
| 348 | 695 | Optimal | Type 1 |
| 349 | 3481 | Cor. 5.3.15 | Type 2, $k = 5$, sd |
| 350 | 699 | Optimal | Type 2, sd |
| 351 | 3501 | Cor. 5.3.15 | Type 2, $k = 5$, sd |
| 352 | 7581 | Prop. 5.3.38 | $11, 32$ |
| 353 | 4929 | Cor. 5.3.15 | Type 2, $k = 7$, sd |
| 354 | 707 | Optimal | Type 2, sd |
| 355 | 2109 | GNB | $k = 6$, sd |
| 356 | 1239 | Prop. 5.3.38 | $4, 89$ |
| 357 | 1185 | Prop. 5.3.38 | $3, 119$ |
| 358 | 1071 | Prop. 5.3.38 | $2, 179$ |
| 359 | 717 | Optimal | Type 2, sd |
| 360 | 3213 | Prop. 5.3.38 | $5, 72$ |
| 361 | 10801 | Cor. 5.3.15 | Type 2, $k = 15$, sd |
| 362 | 2151 | GNB | $k = 5$ |
| 363 | 1445 | GNB | $k = 4$, sd |
| 364 | 1449 | GNB | $k = 3$ |
| 365 | 2565 | Prop. 5.3.38 | $5, 73$ |
| 366 | 1095 | Prop. 5.3.38 | $2, 183$ |
| 367 | 2181 | GNB | $k = 6$, sd |
| 368 | 3825 | Prop. 5.3.38 | $16, 23$ |
| 369 | 1377 | Prop. 5.3.38 | $9, 41$ |
| 370 | 1323 | Prop. 5.3.38 | $5, 74$ |
| 371 | 741 | Optimal | Type 2, sd |
| 372 | 743 | Optimal | Type 1 |
| 373 | 1485 | GNB | $k = 4$, sd |
| 374 | 1489 | GNB | $k = 3$ |
| 375 | 749 | Optimal | Type 2, sd |
| 376 | 5481 | Prop. 5.3.38 | $8, 47$ |
| 377 | 2565 | Prop. 5.3.38 | $13, 29$ |
| 378 | 755 | Optimal | Type 1 |
| 379 | 4547 | GNB | $k = 12$, sd |
| 380 | 1323 | Prop. 5.3.38 | $4, 95$ |
| 381 | 2505 | Prop. 5.3.38 | $3, 127$ |
| 382 | 1143 | Prop. 5.3.38 | $2, 191$ |
| 383 | 4595 | GNB | $k = 12$, sd |
| 384 | 39105 | Prop. 5.3.38 | $3, 128$ |
| 385 | 1449 | Prop. 5.3.38 | $11, 35$ |
| 386 | 771 | Optimal | Type 2, sd |
| 387 | 1541 | GNB | $k = 4$, sd |
| 388 | 775 | Optimal | Type 1 |
| 389 | 9335 | GNB | $k = 24$, sd |
| 390 | 1295 | Prop. 5.3.38 | $3, 130$ |
| 391 | 2325 | GNB | $k = 6$, sd |

| $n$ | $C_n$ | Method | Property |
|---|---|---|---|
| 392 | 3969 | Prop. 5.3.38 | $8, 49$ |
| 393 | 785 | Optimal | Type 2, sd |
| 394 | 3915 | Cor. 5.3.15 | Type 1, $k = 9$ |
| 395 | 2349 | GNB | $k = 6$, sd |
| 396 | 1379 | Prop. 5.3.38 | $4, 99$ |
| 397 | 2361 | GNB | $k = 6$, sd |
| 398 | 795 | Optimal | Type 2, sd |
| 399 | 4777 | Cor. 5.3.15 | Type 2, $k = 6$, sd |
| 400 | 7905 | Prop. 5.3.38 | $16, 25$ |
| 401 | 3207 | GNB | $k = 8$, sd |
| 402 | 1335 | Prop. 5.3.38 | $3, 134$ |
| 403 | 6447 | GNB | $k = 16$, sd |
| 404 | 1609 | GNB | $k = 3$ |
| 405 | 1449 | Prop. 5.3.38 | $5, 81$ |
| 406 | 1539 | Prop. 5.3.38 | $14, 29$ |
| 407 | 2961 | Prop. 5.3.38 | $11, 37$ |
| 408 | 2121 | Prop. 5.3.38 | $8, 51$ |
| 409 | 1629 | GNB | $k = 4$, sd |
| 410 | 819 | Optimal | Type 2, sd |
| 411 | 821 | Optimal | Type 2, sd |
| 412 | 1641 | GNB | $k = 3$ |
| 413 | 825 | Optimal | Type 2, sd |
| 414 | 827 | Optimal | Type 2, sd |
| 415 | 1485 | Prop. 5.3.38 | $5, 83$ |
| 416 | 16245 | Prop. 5.3.38 | $13, 32$ |
| 417 | 1661 | GNB | $k = 4$, sd |
| 418 | 835 | Optimal | Type 1 |
| 419 | 837 | Optimal | Type 2, sd |
| 420 | 839 | Optimal | Type 1 |
| 421 | 4209 | GNB | $k = 10$, sd |
| 422 | 5053 | GNB | $k = 11$ |
| 423 | 1685 | GNB | $k = 4$, sd |
| 424 | 2205 | Prop. 5.3.38 | $8, 53$ |
| 425 | 2529 | GNB | $k = 6$, sd |
| 426 | 851 | Optimal | Type 2, sd |
| 427 | 6555 | Prop. 5.3.38 | $7, 61$ |
| 428 | 2547 | GNB | $k = 5$ |
| 429 | 857 | Optimal | Type 2, sd |
| 430 | 1539 | Prop. 5.3.38 | $5, 86$ |
| 431 | 861 | Optimal | Type 2, sd |
| 432 | 11985 | Prop. 5.3.38 | $16, 27$ |
| 433 | 1725 | GNB | $k = 4$, sd |
| 434 | 3843 | Prop. 5.3.38 | $2, 217$ |
| 435 | 1733 | GNB | $k = 4$, sd |
| 436 | 6091 | GNB | $k = 13$ |
| 437 | 5265 | Prop. 5.3.38 | $19, 23$ |
| 438 | 875 | Optimal | Type 2, sd |
| 439 | 4381 | Cor. 5.3.15 | Type 2, $k = 5$, sd |
| 440 | 3969 | Prop. 5.3.38 | $5, 88$ |
| 441 | 881 | Optimal | Type 2, sd |
| 442 | 883 | Optimal | Type 1 |
| 443 | 885 | Optimal | Type 2, sd |
| 444 | 1475 | Prop. 5.3.38 | $3, 148$ |
| 445 | 1593 | Prop. 5.3.38 | $5, 89$ |
| 446 | 2655 | GNB | $k = 6$, sd |
| 447 | 2661 | GNB | $k = 6$, sd |
| 448 | 34751 | Prop. 5.3.38 | $7, 64$ |
| 449 | 3591 | GNB | $k = 8$, sd |
| 450 | 1683 | Prop. 5.3.38 | $9, 50$ |
| 451 | 1701 | Prop. 5.3.38 | $11, 41$ |
| 452 | 1575 | Prop. 5.3.38 | $4, 113$ |
| 453 | 905 | Optimal | Type 2, sd |
| 454 | 9025 | Cor. 5.3.15 | Type 1, $k = 19$ |
| 455 | 2451 | Prop. 5.3.38 | $7, 65$ |
| 456 | 10437 | Prop. 5.3.38 | $8, 57$ |
| 457 | 13681 | Cor. 5.3.15 | Type 2, $k = 15$, sd |
| 458 | 2727 | GNB | $k = 6$, sd |
| 459 | 3671 | GNB | $k = 8$, sd |
| 460 | 919 | Optimal | Type 1 |
| 461 | 2745 | GNB | $k = 6$, sd |
| 462 | 1383 | Prop. 5.3.38 | $2, 231$ |
| 463 | 5545 | Cor. 5.3.15 | Type 2, $k = 6$, sd |
| 464 | 4845 | Prop. 5.3.38 | $16, 29$ |
| 465 | 1545 | Prop. 5.3.38 | $3, 155$ |
| 466 | 931 | Optimal | Type 1 |
| 467 | 2781 | GNB | $k = 6$, sd |
| 468 | 1751 | Prop. 5.3.38 | $9, 52$ |
| 469 | 1869 | GNB | $k = 4$, sd |
| 470 | 939 | Optimal | Type 2, sd |
| 471 | 3767 | GNB | $k = 8$, sd |
| 472 | 12537 | Prop. 5.3.38 | $8, 59$ |
| 473 | 945 | Optimal | Type 2, sd |
| 474 | 1575 | Prop. 5.3.38 | $3, 158$ |
| 475 | 1893 | GNB | $k = 4$, sd |
| 476 | 1659 | Prop. 5.3.38 | $4, 119$ |
| 477 | 1785 | Prop. 5.3.38 | $9, 53$ |
| 478 | 1431 | Prop. 5.3.38 | $2, 239$ |
| 479 | 3831 | GNB | $k = 8$, sd |
| 480 | 16245 | Prop. 5.3.38 | $3, 160$ |
| 481 | 2865 | GNB | $k = 6$, sd |
| 482 | 2871 | GNB | $k = 5$ |
| 483 | 965 | Optimal | Type 2, sd |
| 484 | 1929 | GNB | $k = 3$ |
| 485 | 3429 | Prop. 5.3.38 | $5, 97$ |
| 486 | 1455 | Prop. 5.3.38 | $2, 243$ |
| 487 | 1941 | GNB | $k = 4$, sd |
| 488 | 7245 | Prop. 5.3.38 | $8, 61$ |
| 489 | 3225 | Prop. 5.3.38 | $3, 163$ |
| 490 | 979 | Optimal | Type 1 |
| 491 | 981 | Optimal | Type 2, sd |
| 492 | 1863 | Prop. 5.3.38 | $12, 41$ |
| 493 | 1965 | GNB | $k = 4$, sd |
| 494 | 1969 | GNB | $k = 3$ |
| 495 | 989 | Optimal | Type 2, sd |
| 496 | 20145 | Prop. 5.3.38 | $16, 31$ |
| 497 | 9921 | Cor. 5.3.15 | Type 2, $k = 10$, sd |
| 498 | 1815 | Prop. 5.3.38 | $6, 83$ |
| 499 | 1989 | GNB | $k = 4$, sd |
| 500 | 5103 | Prop. 5.3.38 | $4, 125$ |
| 501 | 5001 | Cor. 5.3.15 | Type 2, $k = 5$, sd |
| 502 | 1503 | Prop. 5.3.38 | $2, 251$ |
| 503 | 2997 | GNB | $k = 6$, sd |
| 504 | 6783 | Prop. 5.3.38 | $7, 72$ |
| 505 | 5041 | Cor. 5.3.15 | Type 2, $k = 5$, sd |
| 506 | 2835 | Prop. 5.3.38 | $2, 253$ |
| 507 | 2021 | GNB | $k = 4$, sd |
| 508 | 1015 | Optimal | Type 1 |
| 509 | 1017 | Optimal | Type 2, sd |
| 510 | 1919 | Prop. 5.3.38 | $10, 51$ |
| 511 | 3045 | GNB | $k = 6$, sd |
| 512 | | No data | Prime power |
| 513 | 2045 | GNB | $k = 4$, sd |
| 514 | 4563 | Prop. 5.3.38 | $2, 257$ |
| 515 | 1029 | Optimal | Type 2, sd |
| 516 | 1715 | Prop. 5.3.38 | $3, 172$ |
| 517 | 2061 | GNB | $k = 4$, sd |
| 518 | 2793 | Prop. 5.3.38 | $7, 74$ |
| 519 | 1037 | Optimal | Type 2, sd |
| 520 | 2709 | Prop. 5.3.38 | $8, 65$ |
| 521 | 16671 | GNB | $k = 32$, sd |
| 522 | 1043 | Optimal | Type 1 |
| 523 | 5221 | Cor. 5.3.15 | Type 2, $k = 5$, sd |
| 524 | 1827 | Prop. 5.3.38 | $4, 131$ |
| 525 | 3465 | Prop. 5.3.38 | $3, 175$ |
| 526 | 2097 | GNB | $k = 3$ |
| 527 | 3141 | GNB | $k = 6$, sd |
| 528 | 5525 | Prop. 5.3.38 | $16, 33$ |
| 529 | 12695 | GNB | $k = 24$, sd |
| 530 | 1059 | Optimal | Type 2, sd |
| 531 | 1061 | Optimal | Type 2, sd |
| 532 | 2121 | GNB | $k = 3$ |
| 533 | 3645 | Prop. 5.3.38 | $13, 41$ |
| 534 | 1775 | Prop. 5.3.38 | $3, 178$ |
| 535 | 2133 | GNB | $k = 4$, sd |
| 536 | 5481 | Prop. 5.3.38 | $8, 67$ |
| 537 | 1785 | Prop. 5.3.38 | $3, 179$ |
| 538 | 3207 | GNB | $k = 6$, sd |
| 539 | 3969 | Prop. 5.3.38 | $11, 49$ |
| 540 | 1079 | Optimal | Type 1 |
| 541 | 9737 | GNB | $k = 18$, sd |
| 542 | 2161 | GNB | $k = 3$ |
| 543 | 1085 | Optimal | Type 2, sd |
| 544 | 29241 | Prop. 5.3.38 | $17, 32$ |
| 545 | 1089 | Optimal | Type 2, sd |
| 546 | 1091 | Optimal | Type 1 |
| 547 | 5469 | GNB | $k = 10$, sd |
| 548 | 3267 | GNB | $k = 5$ |
| 549 | 5865 | Prop. 5.3.38 | $9, 61$ |
| 550 | 2079 | Prop. 5.3.38 | $11, 50$ |
| 551 | 3285 | GNB | $k = 6$, sd |
| 552 | 2877 | Prop. 5.3.38 | $8, 69$ |
| 553 | 2205 | GNB | $k = 4$, sd |
| 554 | 1107 | Optimal | Type 2, sd |
| 555 | 2213 | GNB | $k = 4$, sd |
| 556 | 1111 | Optimal | Type 1 |
| 557 | 3321 | GNB | $k = 6$, sd |
| 558 | 1115 | Optimal | Type 2, sd |
| 559 | 2229 | GNB | $k = 4$, sd |
| 560 | 5865 | Prop. 5.3.38 | $16, 35$ |
| 561 | 1121 | Optimal | Type 2, sd |
| 562 | 1123 | Optimal | Type 1 |
| 563 | 7869 | Cor. 5.3.15 | Type 2, $k = 7$, sd |
| 564 | 2249 | GNB | $k = 3$ |
| 565 | 2025 | Prop. 5.3.38 | $5, 113$ |
| 566 | 2257 | GNB | $k = 3$ |
| 567 | 2261 | GNB | $k = 4$, sd |

| $n$ | $C_n$ | Method | Property |
|---|---|---|---|
| 568 | 11907 | Prop. 5.3.38 | $8, 71$ |
| 569 | 6817 | Cor. 5.3.15 | Type 2, $k = 6$, sd |
| 570 | 2079 | Prop. 5.3.38 | $6, 95$ |
| 571 | 5709 | GNB | $k = 10$, sd |
| 572 | 2163 | Prop. 5.3.38 | $11, 52$ |
| 573 | 1905 | Prop. 5.3.38 | $3, 191$ |
| 574 | 2187 | Prop. 5.3.38 | $14, 41$ |
| 575 | 1149 | Optimal | Type 2, sd |
| 576 | 31093 | Prop. 5.3.38 | $9, 64$ |
| 577 | 2301 | GNB | $k = 4$, sd |
| 578 | 3447 | GNB | $k = 6$, sd |
| 579 | 3825 | Prop. 5.3.38 | $3, 193$ |
| 580 | 2313 | GNB | $k = 3$ |
| 581 | 3135 | Prop. 5.3.38 | $7, 83$ |
| 582 | 1935 | Prop. 5.3.38 | $3, 194$ |
| 583 | 2205 | Prop. 5.3.38 | $11, 53$ |
| 584 | 5985 | Prop. 5.3.38 | $8, 73$ |
| 585 | 1169 | Optimal | Type 2, sd |
| 586 | 1171 | Optimal | Type 1 |
| 587 | 8205 | Cor. 5.3.15 | Type 2, $k = 7$, sd |
| 588 | 1955 | Prop. 5.3.38 | $3, 196$ |
| 589 | 2349 | GNB | $k = 4$, sd |
| 590 | 6183 | Prop. 5.3.38 | $5, 118$ |
| 591 | 3525 | GNB | $k = 6$, sd |
| 592 | 11985 | Prop. 5.3.38 | $16, 37$ |
| 593 | 1185 | Optimal | Type 2, sd |
| 594 | 4389 | Prop. 5.3.38 | $11, 54$ |
| 595 | 2133 | Prop. 5.3.38 | $5, 119$ |
| 596 | 2377 | GNB | $k = 3$ |
| 597 | 2381 | GNB | $k = 4$, sd |
| 598 | 1791 | Prop. 5.3.38 | $2, 299$ |
| 599 | 4791 | GNB | $k = 8$, sd |
| 600 | 9765 | Prop. 5.3.38 | $3, 200$ |
| 601 | 3585 | GNB | $k = 6$, sd |
| 602 | 3249 | Prop. 5.3.38 | $7, 86$ |
| 603 | 4437 | Prop. 5.3.38 | $9, 67$ |
| 604 | 4789 | GNB | $k = 7$ |
| 605 | 3609 | GNB | $k = 6$, sd |
| 606 | 1211 | Optimal | Type 2, sd |
| 607 | 3621 | GNB | $k = 6$, sd |
| 608 | 42237 | Prop. 5.3.38 | $19, 32$ |
| 609 | 2429 | GNB | $k = 4$, sd |
| 610 | 5427 | Prop. 5.3.38 | $2, 305$ |
| 611 | 1221 | Optimal | Type 2, sd |
| 612 | 1223 | Optimal | Type 1 |
| 613 | 6121 | Cor. 5.3.15 | Type 2, $k = 5$, sd |
| 614 | 1227 | Optimal | Type 2, sd |
| 615 | 1229 | Optimal | Type 2, sd |
| 616 | 8379 | Prop. 5.3.38 | $7, 88$ |
| 617 | 4935 | GNB | $k = 8$, sd |
| 618 | 1235 | Optimal | Type 1 |
| 619 | 2469 | GNB | $k = 4$, sd |
| 620 | 2163 | Prop. 5.3.38 | $4, 155$ |
| 621 | 3705 | GNB | $k = 6$, sd |
| 622 | 2481 | GNB | $k = 3$ |
| 623 | 3363 | Prop. 5.3.38 | $7, 89$ |
| 624 | 6545 | Prop. 5.3.38 | $16, 39$ |
| 625 | 22465 | Cor. 5.3.15 | Type 2, $k = 18$, sd |
| 626 | 5571 | Prop. 5.3.38 | $2, 313$ |
| 627 | 2085 | Prop. 5.3.38 | $3, 209$ |
| 628 | 4981 | GNB | $k = 7$ |
| 629 | 1257 | Optimal | Type 2, sd |
| 630 | 2415 | Prop. 5.3.38 | $18, 35$ |
| 631 | 6301 | Cor. 5.3.15 | Type 2, $k = 5$, sd |
| 632 | 6489 | Prop. 5.3.38 | $8, 79$ |
| 633 | 10505 | Prop. 5.3.38 | $3, 211$ |
| 634 | 8839 | Cor. 5.3.15 | Type 1, $k = 13$ |
| 635 | 4509 | Prop. 5.3.38 | $5, 127$ |
| 636 | 2415 | Prop. 5.3.38 | $12, 53$ |
| 637 | 2541 | GNB | $k = 4$, sd |
| 638 | 1275 | Optimal | Type 2, sd |
| 639 | 1277 | Optimal | Type 2, sd |
| 640 | 70389 | Prop. 5.3.38 | $5, 128$ |
| 641 | 1281 | Optimal | Type 2, sd |
| 642 | 3831 | GNB | $k = 6$, sd |
| 643 | 7705 | Cor. 5.3.15 | Type 2, $k = 6$, sd |
| 644 | 2475 | Prop. 5.3.38 | $23, 28$ |
| 645 | 1289 | Optimal | Type 2, sd |
| 646 | 1935 | Prop. 5.3.38 | $2, 323$ |
| 647 | 9045 | Cor. 5.3.15 | Type 2, $k = 7$, sd |
| 648 | 3381 | Prop. 5.3.38 | $8, 81$ |
| 649 | 6481 | Cor. 5.3.15 | Type 2, $k = 5$, sd |
| 650 | 1299 | Optimal | Type 2, sd |
| 651 | 1301 | Optimal | Type 2, sd |
| 652 | 1303 | Optimal | Type 1 |
| 653 | 1305 | Optimal | Type 2, sd |
| 654 | 6435 | Prop. 5.3.38 | $3, 218$ |
| 655 | 2349 | Prop. 5.3.38 | $5, 131$ |
| 656 | 6885 | Prop. 5.3.38 | $16, 41$ |
| 657 | 4845 | Prop. 5.3.38 | $9, 73$ |
| 658 | 1315 | Optimal | Type 1 |
| 659 | 1317 | Optimal | Type 2, sd |
| 660 | 1319 | Optimal | Type 1 |
| 661 | 3945 | GNB | $k = 6$, sd |
| 662 | 2641 | GNB | $k = 3$ |
| 663 | 2205 | Prop. 5.3.38 | $3, 221$ |
| 664 | 3465 | Prop. 5.3.38 | $8, 83$ |
| 665 | 3591 | Prop. 5.3.38 | $7, 95$ |
| 666 | 2499 | Prop. 5.3.38 | $9, 74$ |
| 667 | 2565 | Prop. 5.3.38 | $23, 29$ |
| 668 | 7985 | Cor. 5.3.15 | Type 1, $k = 11$ |
| 669 | 2669 | GNB | $k = 4$, sd |
| 670 | 2403 | Prop. 5.3.38 | $5, 134$ |
| 671 | 4005 | GNB | $k = 6$, sd |
| 672 | 34295 | Prop. 5.3.38 | $3, 224$ |
| 673 | 2685 | GNB | $k = 4$, sd |
| 674 | 4023 | GNB | $k = 5$ |
| 675 | 13113 | Prop. 5.3.38 | $25, 27$ |
| 676 | 1351 | Optimal | Type 1 |
| 677 | 5415 | GNB | $k = 8$, sd |
| 678 | 2255 | Prop. 5.3.38 | $3, 226$ |
| 679 | 6789 | GNB | $k = 10$, sd |
| 680 | 15309 | Prop. 5.3.38 | $5, 136$ |
| 681 | 14961 | Cor. 5.3.15 | Type 2, $k = 11$, sd |
| 682 | 4071 | GNB | $k = 6$, sd |
| 683 | 1365 | Optimal | Type 2, sd |
| 684 | 2729 | GNB | $k = 3$ |
| 685 | 2733 | GNB | $k = 4$, sd |
| 686 | 1371 | Optimal | Type 2, sd |
| 687 | 6869 | GNB | $k = 10$, sd |
| 688 | 14025 | Prop. 5.3.38 | $16, 43$ |
| 689 | 4725 | Prop. 5.3.38 | $13, 53$ |
| 690 | 1379 | Optimal | Type 2, sd |
| 691 | 6901 | Cor. 5.3.15 | Type 2, $k = 5$, sd |
| 692 | 2415 | Prop. 5.3.38 | $4, 173$ |
| 693 | 3743 | Prop. 5.3.38 | $7, 99$ |
| 694 | 2769 | GNB | $k = 3$ |
| 695 | 4941 | Prop. 5.3.38 | $5, 139$ |
| 696 | 5985 | Prop. 5.3.38 | $3, 232$ |
| 697 | 2781 | GNB | $k = 4$, sd |
| 698 | 4167 | GNB | $k = 5$ |
| 699 | 2325 | Prop. 5.3.38 | $3, 233$ |
| 700 | 1399 | Optimal | Type 1 |
| 701 | 12601 | Cor. 5.3.15 | Type 2, $k = 9$, sd |
| 702 | 7191 | Prop. 5.3.38 | $26, 27$ |
| 703 | 4197 | GNB | $k = 6$, sd |
| 704 | 38409 | Prop. 5.3.38 | $11, 64$ |
| 705 | 4209 | GNB | $k = 6$, sd |
| 706 | 14787 | Prop. 5.3.38 | $2, 353$ |
| 707 | 4221 | GNB | $k = 6$, sd |
| 708 | 1415 | Optimal | Type 1 |
| 709 | 2829 | GNB | $k = 4$, sd |
| 710 | 2833 | GNB | $k = 3$ |
| 711 | 5253 | Prop. 5.3.38 | $9, 79$ |
| 712 | 3717 | Prop. 5.3.38 | $8, 89$ |
| 713 | 1425 | Optimal | Type 2, sd |
| 714 | 2607 | Prop. 5.3.38 | $6, 119$ |
| 715 | 2709 | Prop. 5.3.38 | $11, 65$ |
| 716 | 2499 | Prop. 5.3.38 | $4, 179$ |
| 717 | 2385 | Prop. 5.3.38 | $3, 239$ |
| 718 | 2151 | Prop. 5.3.38 | $2, 359$ |
| 719 | 1437 | Optimal | Type 2, sd |
| 720 | 13005 | Prop. 5.3.38 | $5, 144$ |
| 721 | 4305 | GNB | $k = 6$, sd |

**Table 2.2.10** Minimum found complexity of a normal basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$, $40 \leq n \leq 721$.

### 2.2.3 Resources and Standards

**2.2.21 Remark** The *Combinatorial Object Server* (COS) [2507] allows the user to specify a type of combinatorial object with specific parameter values and COS will return a list of the objects having the desired parameters. In many cases, the format of the output can be chosen to be more machine-readable or human-readable. COS does not rely on a list, rather it generates the objects requested on-the-fly; for this reason, the output is restricted to 200 objects. Examples of the objects generated are permutations, subsets and combinations, set and integer partitions, irreducible and primitive polynomials over small finite fields and spanning trees of a graph.

**2.2.22 Remark** The *Cunningham project* produces a set of tables to factor the numbers $b^n \pm 1$ for $b = 2, 3, 5, 6, 7, 10, 11, 12$ for $n$ as large as possible. The current factorization methods employed are the elliptic curve method, the multiple polynomial quadratic sieve and the number field sieve. For more information on factorization methods, see [2080, Chapter 3]. The Cunningham tables appear in published form [415] and as an electronic resource [2890].

**2.2.23 Remark** The *Great Internet Mersenne Prime Search* (GIMPS) [2084] is a distributed computing effort dedicated to finding and verifying Mersenne primes (that is, primes of the form $2^p - 1$, where $p$ is also a prime). GIMPS uses a combination of trial factoring using the Sieve of Eratosthenes, followed by the Pollard $P - 1$ method and ending with the Lucas-Lehmer primality test. For more information on primality testing, see [724, Chapter 31], for example. GIMPS provides the *Prime95* software, which automates all factoring and distributed computing processes. The (currently) largest known Mersenne prime is $2^{43112609} - 1$ containing 12978189 decimal digits [2084].

The search for Mersenne primes is of particular interest in searching for primitive trinomials of large degrees. Primitive polynomials of low-weight are useful in cryptographic applications and pseudo-random number generation; see Sections 14.9 and 16.2. If $p$ is a Mersenne prime, then any irreducible polynomial of degree $p$ over $\mathbb{F}_2$ is primitive. Since binomials of degree at least 2 cannot be irreducible over $\mathbb{F}_2$, we consider trinomials $x^p + x^r + 1$, for some $0 \leq r \leq p - 1$. Sieving trinomials for reducibles is possible by Swan's Theorem; see Section 3.3. For more details on the algorithms and methods used in the search for primitive trinomials, see [408]. An implementation of polynomial arithmetic over $\mathbb{F}_2$ which was motivated by the GIMPS project, entitled *gf2x*, is necessarily highly optimized and is preferred in some finite field software implementations; see Table 2.2.11 for more details.

**2.2.24 Remark** The *On-Line Encyclopedia of Integer Sequences*$^{TM}$ (OEIS$^{\text{TM}}$) [2800] is a constantly-updated, searchable database of integer sequences. Examples of famous sequences in the OEIS$^{\text{TM}}$ are the Catalan numbers (A000108), prime numbers (A000040) and the Fibonnacci numbers (A000045). Users can search by sequence, "word" (for example, "number of irreducible polynomials" yields sequence A001037) or sequence number. Sequences are sorted lexicographically, so the sequence references may have changed since the date of publication.

**2.2.25 Remark** In Table 2.2.11, we present a number of software packages which are useful for finite field implementations. We distinguish between packages which are open-source and commercial. We refer the reader to the citation, which provides a current (as of the date of publication) web URL to the most recent build of the software. We note that this is not an exhaustive list of software packages, simply a useful list of packages used or researched by the author.

**Open-source software packages for computations in discrete mathematics**

| Name | Ver. | Description | |
|---|---|---|---|
| *Fast Library for Number Theory* (FLINT) | 2.3 | A C library for performing computations in number theory. Routines include fast algorithms, on par with the other most efficient packages listed, for arbitrary precision integers, rational numbers, modular arithmetic and $p$-adic numbers. Most libraries also contain vector, polynomial and matrix methods. Multi-core support to come in future versions. | [1426] |
| *Groups, Algorithms, Programming* (GAP) | 4.4.x | A system for computational discrete algebra emphasizing computational group theory. Can do basic computations with arbitrary integers, rationals, finite fields, $p$-adic numbers, polynomials, rational functions and more. Contains a coding theory package, combinatorial functions and prime factorization routines. Provides its own programming language, libraries of algebraic algorithms written in the GAP language as well as data libraries of algebraic objects, particularly various types of groups. | [2796] |
| *gf2x* | 1.0 | Library for efficient arithmetic of single-variable polynomials over $\mathbb{F}_2$. Primarily introduces fast-fourier transform (FFT) for large-degree polynomial multiplication. | [399] |
| *The GNU Multiple Precision Arithmetic Library* (GMP) | 5.0.x | C/C++ library providing fast arbitrary precision arithmetic on integers, rational numbers and floating point numbers. | [2797] |
| *Macaulay2* | 1.4 | Software system focusing on algebraic geometry and commutative algebra. Contains core algorithms combined with a high-level interpreted language and debugger to support package creation. Uses elements of *PARI*, *NTL* and others in its routines. | [1355] |
| *Number Theory Library* (NTL) | 5.5.x | C++ library providing data structures and routines for arbitrary length integer arithmetic, arbitrary precision floating-point arithmetic and finite field arithmetic. Also contains lattice basis reduction algorithms and basic linear algebra packages. Interfaces with *gf2x* and *GMP* libraries for additional speed-ups. | [2633] |
| *PARI/GP* | 2.5.x | C library designed for fast computations in number theory including integer factorization and elliptic curve compututations. Also contains useful function for use with matrices, polynomials, power series and others. GP is a scripting language used by the gp interactive shell, which accesses the PARI functions. A subset of the GP language can be compiled as C code, resulting in a substantial speed-up. | [2801] |

**Open-source software packages for computations in discrete mathematics**

| Name | Ver. | Description | |
|---|---|---|---|
| *Singular* | 3.1.x | A computer algebra system focusing on polynomial computations. Specializes on commutative and non-commutative algebra, algebraic geometry and singularity theory. Provides a C-like programming language, extendable using libraries. Its core algorithms handle Gröbner bases, polynomial factorization, resultants and root finding. Advanced libraries and third-party software provide further functionality. | [792] |
| *SAGE* | 5.0 | Comprehensive Python-based open-source computer algebra package. Natively contains a finite field implementation as well as wrappers for other useful packages including Flint, GAP, NTL, PARI and Singular. Interpreted but contains the ability to compile, using Cython, as C code for a drastic improvement in speed. | [2709] |

**Commercial stand-alone packages containing finite field implementations**

| Name | Ver. | Description | |
|---|---|---|---|
| Magma | 2.18-x | Computational algebra system focusing on algebra, algebraic combinatorics, algebraic geometry and number theory. Language built to closely approximate the user's mode of thought and usual notation. Major algorithms are designed to give comparable performance to specialized programs. Also contains a number of large databases of elliptic curves, linear codes, irreducible polynomials over finite fields, graphs, Cunningham factorizations and others. | [712] |
| Maple | 16 | Comprehensive computer algebra suite, contains a full featured programming language to create scripts or full applications. A "smart" document environment allows embedding equations, visualizations or components in the document. Can take advantage of parallelism, multi-threading and multi-process programing. Finite field arithmetic natively given by the "GF" package. | [2002] |
| Mathematica | 8 | Development platform concetrating on integrating computation into workflows. Finite field computations are performed using the "FiniteFields" package and "GF" class. | [3004] |
| Matlab | R2012a | Programming environment for algorithm development and data analysis. Contains arithmetic over finite fields $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ for $n \leq 16$ within the "Communications System Toolbox". | [2799] |

**Table 2.2.11** Software packages useful for finite field implementations.

**See Also**

| | |
|---|---|
| §3.2, §3.3, §3.4 | For reducibility and irreducibility of low-weight polynomials. |
| §5.2, §5.3 | For normal bases and their complexities. |
| §11.1 | For computational techniques over finite fields. |
| [1413], [2080] | For patents and standards of elliptic curve cryptography, most of which contain guidelines for finite field implementations. |

**References Cited:** [130, 399, 408, 415, 712, 724, 792, 1263, 1264, 1355, 1413, 1426, 1631, 1777, 1939, 2002, 2015, 2080, 2084, 2180, 2356, 2507, 2573, 2582, 2633, 2709, 2753, 2796, 2797, 2799, 2800, 2801, 2890, 2925, 3004, 3036]