diagonal kinds of polynomials in several variables where the preimage points come from subsets of the field rather than the entire field.

See Also

§8.1	Discusses permutation polynomials in one variable.
§8.2	Discusses permutation polynomials in several variables.
§8.4	Considers exceptional polynomials.
[624]	Considers polynomials whose value sets lie in a subfield.
[729]	Studies value sets as they relate to Dembowski-Ostrom and planar polynomials.

References Cited: [57, 284, 288, 349, 350, 546, 623, 624, 625, 662, 729, 752, 753, 755, 767, 768, 769, 1083, 1219, 1307, 1308, 1363, 1364, 1454, 1934, 2038, 2100, 2743, 2823, 2908, 2916, 2978, 2979]

8.4 Exceptional polynomials

Michael E. Zieve, *University of Michigan*

8.4.1 Fundamental properties

8.4.1 Definition An *exceptional polynomial* over $\mathbb{F}_q$ is a polynomial $f \in \mathbb{F}_q[x]$ which is a permutation polynomial on $\mathbb{F}_{q^m}$ for infinitely many m.

8.4.2 Remark If $f \in \mathbb{F}_q[x]$ is exceptional over $\mathbb{F}_{q^k}$ for some k, then f is exceptional over $\mathbb{F}_q$.

8.4.3 Definition A polynomial $F(x, y) \in \mathbb{F}_q[x, y]$ is *absolutely irreducible* if it is irreducible in $\bar{\mathbb{F}}_q[x, y]$, where $\bar{\mathbb{F}}_q$ is an algebraic closure of $\mathbb{F}_q$.

8.4.4 Theorem [662] A polynomial $f \in \mathbb{F}_q[x]$ is exceptional over $\mathbb{F}_q$ if and only if every absolutely irreducible factor of $f(x) - f(y)$ in $\mathbb{F}_q[x, y]$ is a constant times $x - y$.

8.4.5 Corollary If $f \in \mathbb{F}_q[x]$ is exceptional, then there are integers $1 < e_1 < e_2 < \cdots < e_k$ such that: f is exceptional over $\mathbb{F}_{q^n}$ if and only if n is not divisible by any e_i.

8.4.6 Corollary If $f \in \mathbb{F}_q[x]$ is exceptional, then there is an integer $M > 1$ such that f permutes each field $\mathbb{F}_{q^m}$ for which m is coprime to M.

8.4.7 Corollary For $g, h \in \mathbb{F}_q[x]$, the composition $g \circ h$ is exceptional if and only if both g and h are exceptional.

8.4.8 Definition A polynomial $f \in \mathbb{F}_q[x]$ is *indecomposable* if it cannot be written as the composition $f = g \circ h$ of two nonlinear polynomials $g, h \in \mathbb{F}_q[x]$.

8.4.9 Corollary A polynomial $f \in \mathbb{F}_q[x]$ is exceptional if and only if it is the composition of indecomposable exceptional polynomials.

8.4.2 Indecomposable exceptional polynomials

8.4.10 Theorem [1117] Let f be an indecomposable exceptional polynomial over $\mathbb{F}_q$ of degree n, and let p be the characteristic of $\mathbb{F}_q$. Then either

1. n is coprime to p, or
2. n is a power of p, or
3. $n = \frac{p^r(p^r-1)}{2}$ where $r > 1$ is odd and $p \in \{2, 3\}$.

8.4.11 Theorem [1750, 2187] The indecomposable exceptional polynomials over $\mathbb{F}_q$ of degree coprime to q are precisely the polynomials of the form $\ell_1 \circ f \circ \ell_2$ where $\ell_1, \ell_2 \in \mathbb{F}_q[x]$ are linear and either

1. $f(x) = ax + b$ with $a \in \mathbb{F}_q^*$ and $b \in \mathbb{F}_q$, or
2. $f(x) = x^n$ where n is a prime which does not divide $q - 1$, or
3. $f(x) = D_n(x, a)$ (a Dickson polynomial) where $a \in \mathbb{F}_q^*$ and n is a prime which does not divide $q^2 - 1$.

8.4.12 Theorem [1368, 1370] The indecomposable exceptional polynomials over $\mathbb{F}_q$ of degree $s(s-1)/2$, where $s = p^r > 3$ and $q = p^m$ with p prime, are precisely the polynomials of the form $\ell_1 \circ f \circ \ell_2$ where $\ell_1, \ell_2 \in \mathbb{F}_q[x]$ are linear, $r > 1$ is coprime to $2m$, and f is one of the following polynomials:

1. $x^{-s}\, T(ax^e)^{(s+1)/e}$ where $p = 2,\ T(x) = x^{s/2} + x^{s/4} + \cdots + x,\ e \mid (s+1),$ and $a \in \mathbb{F}_q^*$,
2. $\left(\dfrac{T(x)+a}{x}\right)^s \cdot \left(T(x) + \dfrac{T(x)+a}{a+1} \cdot T\!\left(\dfrac{x(a^2+a)}{(T(x)+a)^2}\right)\right)$ where $p = 2,\ a \in \mathbb{F}_q \setminus \mathbb{F}_2$, and $T(x) = x^{s/2} + x^{s/4} + \cdots + x$,
3. $x(x^{2e} - a)^{(s+1)/(4e)} \left(\dfrac{(x^{2e} - a)^{(s-1)/2} + a^{(s-1)/2}}{x^{2e}}\right)^{(s+1)/(2e)}$ where $p = 3,\ e \,\big|\, \frac{s+1}{4}$, and $a \in \mathbb{F}_q^*$ is an element whose image in $\mathbb{F}_q^*/(\mathbb{F}_q^*)^{2e}$ has even order.

8.4.13 Remark The proofs of Theorems 8.4.10 and 8.4.12 rely on the classification of finite simple groups.

8.4.14 Theorem [1117, 1750] For prime p, the degree-p exceptional polynomials over $\mathbb{F}_{p^m}$ are precisely the polynomials $\ell_1 \circ f \circ \ell_2$ where $\ell_1, \ell_2 \in \mathbb{F}_{p^m}[x]$ are linear and $f(x) = x(x^{(p-1)/r} - a)^r$ with $r \mid (p-1)$ and $a \in \mathbb{F}_{p^m}$ such that $a^{r(p^m-1)/(p-1)} \neq 1$.

8.4.15 Proposition [669, 835] Let L be a *linearized polynomial* (i.e., $L(x) = \sum_{i=0}^d a_i x^{p^i}$ with $a_i \in \mathbb{F}_{p^m}$), and let $S(x) = x^j H(x)^k$ where $H \in \mathbb{F}_{p^m}[x]$ satisfies $L(x) = x^j H(x^k)$. Then S is exceptional over $\mathbb{F}_{p^m}$ if and only if S has no nonzero roots in $\mathbb{F}_{p^m}$.

8.4.16 Proposition [1365] Let $s = p^r$ where p is an odd prime. If $a \in \mathbb{F}_{p^m}$ is not an $(s-1)$-th power, then

$$\frac{(x^s - ax - a)\cdot(x^s - ax + a)^s + \left((x^s - ax + a)^2 + 4a^2x\right)^{(s+1)/2}}{2x^s}$$

is an indecomposable exceptional polynomial over $\mathbb{F}_{p^m}$.

8.4.17 Proposition [1367] Let $s = 2^r$. If $a \in \mathbb{F}_{2^m}$ is not an $(s-1)$-th power, then

$$\frac{(x^s + ax + a)^{s+1}}{x^s} \cdot \left(\frac{x^s + ax}{x^s + ax + a} + T\left(\frac{a^2 x}{(x^s + ax + a)^2} \right) \right)$$

is an indecomposable exceptional polynomial over $\mathbb{F}_{2^m}$, where $T(x) = x^{s/2} + x^{s/4} + \cdots + x$.

8.4.18 Remark The previous three Propositions describe all known indecomposable exceptional polynomials over $\mathbb{F}_{p^m}$ of degree p^r with $r > 0$, up to composing on both sides with linear polynomials. It is expected that there are no further examples. Theorem 8.4.14 shows this when $r = 1$, and [1367, 2121] show it under different hypotheses.

8.4.3 Exceptional polynomials and permutation polynomials

8.4.19 Theorem A permutation polynomial over $\mathbb{F}_q$ of degree at most $q^{1/4}$ is exceptional over $\mathbb{F}_q$.

8.4.20 Remark A weaker version of Theorem 8.4.19 was proved in [772]; the stated result is obtained from the same proof by using the fact that an absolutely irreducible degree-d bivariate polynomial over $\mathbb{F}_q$ has at least $q + 1 - (d-1)(d-2)\sqrt{q}$ roots in $\mathbb{F}_q \times \mathbb{F}_q$. For proofs of this estimate, see [145, 1119, 1881]. A stronger (but false) version of this estimate was stated in [1934], and [1219] deduced Theorem 8.4.19 from this false estimate. Finally, [145] states a stronger version of Theorem 8.4.19, but the proof is flawed and when fixed it yields Theorem 8.4.19.

8.4.21 Remark Up to composing with linears on both sides, the only known non-exceptional permutation polynomials over $\mathbb{F}_q$ of degree less than $\sqrt{q}$ are $x^{10} + 3x$ over $\mathbb{F}_{343}$ and $\frac{(x+1)^N + 1}{x}$ over $\mathbb{F}_{2^{4r-1}}$, where $r \geq 3$ and $N = (4^r + 2)/3$.

8.4.22 Remark Heuristics predict that "at random" there would be no permutation polynomials over $\mathbb{F}_q$ of degree less than $\frac{q}{2 \log q}$.

8.4.23 Remark There are no known examples of non-exceptional permutation polynomials over $\mathbb{F}_q$ of degree less than $\frac{q}{2 \log q}$ when q is prime.

8.4.24 Remark Nearly all known examples of permutation polynomials over $\mathbb{F}_q$ of degree less than $\frac{q}{2 \log q}$ can be written as the restriction to $\mathbb{F}_q$ of a permutation π of an infinite algebraic extension K of $\mathbb{F}_q$, where π is induced by a rational function in the symbols $\sigma^i(x)$, with σ being a fixed automorphism of K. Such a permutation π may be viewed as an exceptional rational function over the *difference field* (K, σ); see [698, 1907, 1908].

8.4.4 Miscellany

8.4.25 Theorem [540, 3068] Every permutation of $\mathbb{F}_q$ is induced by an exceptional polynomial.

8.4.26 Theorem [683, 1365, 1893] Exceptional polynomials over $\mathbb{F}_q$ have degree coprime to $q - 1$.

8.4.27 Remark Theorem 8.4.26 is called the Carlitz–Wan conjecture. It follows from Theorems 8.4.10, 8.4.11, and 8.4.12. However, the known proofs of Theorems 8.4.10 and 8.4.12 rely on the classification of finite simple groups, whereas [683, 1365, 1893] present short self-contained proofs of Theorem 8.4.26.

8.4.28 Theorem If $f \in \mathbb{Z}[x]$ is a permutation polynomial over $\mathbb{F}_p$ for infinitely many primes p, then f is the composition of linear and Dickson polynomials.

8.4.29 Remark Theorem 8.4.28 was proved in [2558] when f has prime degree. It was shown in [2187] (confirming an assertion in [2558]) that the full Theorem 8.4.28 follows quickly from the main lemma in [2558] together with a group-theoretic result from [2559]. A different proof of Theorem 8.4.28 appears in [1106, 1931, 2824], which combines this group-theoretic result with Weil's bound on the number of $\mathbb{F}_q$-rational points on a genus-g curve over $\mathbb{F}_q$.

8.4.30 Remark Theorem 8.4.28 is called the Schur conjecture, although Schur did not pose this conjecture. The paper [1106] made the incorrect assertion that Schur had conjectured Theorem 8.4.28 in [2558], and this assertion has become widely accepted despite its falsehood.

8.4.31 Remark The concept of exceptionality can be extended to rational functions or more general maps between varieties [1369]. In particular, many exceptional rational functions arise as coordinate projections of isogenies of elliptic curves [1112, 1366, 2188].

8.4.5 Applications

8.4.32 Remark Exceptional polynomials were used in [2782] to produce families of hyperelliptic curves whose Jacobians have an unusually large endomorphism ring. These curves were used in [765] to realize certain groups $\mathrm{PSL}_2(q)$ as Galois groups of extensions of certain cyclotomic fields.

8.4.33 Remark Exceptional polynomials were used in [513, 2336] to produce curves whose Jacobian is isogenous to a power of an elliptic curve, and in particular to produce maximal curves (see Section 12.5).

8.4.34 Lemma [857] We have $(x+1)^N + x^N + 1 = f(x^2+x)$ in $\mathbb{F}_2[x]$, where $N = 4^r - 2^r + 1$ and $f(x) = T(x)^{2^r+1}/x^{2^r}$ with $T(x) = x^{2^{r-1}} + x^{2^{r-2}} + \cdots + x$. This polynomial $f(x)$ is obtained from case 1 of Theorem 8.4.12 by putting $a = 1$ and $e = 1$.

8.4.35 Remark This result (together with exceptionality of f) has been used to produce new examples of binary sequences with ideal autocorrelation [857], cyclic difference sets with Singer parameters [859], almost perfect nonlinear functions [858], and bent functions [859, 3009]. See Sections 10.3, 14.6, 9.2, and 9.3, respectively.

8.4.36 Remark For further results about the polynomials f from Lemma 8.4.34, including formulas for a polynomial inducing the inverse of the permutation induced by f on $\mathbb{F}_{2^m}$, see [901]. These polynomials are shown to be exceptional in [691, 692, 859, 901, 3067].

8.4.37 Remark The polynomials in cases 1 and 3 of Theorem 8.4.12 have been used to produce branched coverings of the projective line in positive characteristic whose Galois group is either symplectic [9] or orthogonal [8].

See Also

§8.1	For discussion of permutation polynomials in one variable.
§8.3	For value sets of polynomials.
[58], [1364]	For *Davenport pairs*, which are pairs (f, g) of polynomials in $\mathbb{F}_q[x]$ such that $f(\mathbb{F}_{q^m}) = g(\mathbb{F}_{q^m})$ for infinitely many m. This notion generalizes exceptionality, since $f \in \mathbb{F}_q[x]$ is exceptional if and only if (f, x) is a Davenport pair.
[691], [692], [3067]	For the factorization of $f(x) - f(y)$ where $f(x)$ is a polynomial from case 1 or 3 of Theorem 8.4.12.
[691], [1895], [2185]	For the discovery of some of the polynomials in Theorem 8.4.12.
[835]	For a thorough study of exceptional polynomials using only the Hermite–Dickson criterion, and the discovery of the polynomials in Theorem 8.4.11 and Proposition 8.4.15.

References Cited: [8, 9, 58, 145, 513, 540, 662, 669, 683, 691, 692, 698, 765, 772, 835, 857, 858, 859, 901, 1106, 1112, 1117, 1119, 1219, 1364, 1365, 1366, 1367, 1368, 1369, 1370, 1750, 1881, 1893, 1895, 1907, 1908, 1931, 1934, 2121, 2185, 2187, 2188, 2336, 2558, 2559, 2782, 2824, 3009, 3067, 3068]

Bibliography

[1] R. Abarzúa, N. Thériault, R. Avanzi, I. Soto, and M. Alfaro, Optimization of the arithmetic of the ideal class group for genus 4 hyperelliptic curves over projective coordinates, *Advances in Mathematics of Communications* 4 (2010) 115–139. <795>

[2] E. Abbe, Randomness and dependencies extraction via polarization, In *Proc. Information Theory and Applications Workshop (ITA)*, 1–7, 2011. <731>

[3] M. Abdón and F. Torres, On maximal curves in characteristic two, *Manuscripta Math.* 99 (1999) 39–53. <455, 457>

[4] R. J. R. Abel, Some new BIBDs with block size 7, *J. Combin. Des.* 8 (2000) 146–150. <589, 591>

[5] R. J. R. Abel and M. Buratti, Some progress on $(v, 4, 1)$ difference families and optical orthogonal codes, *J. Combin. Theory, Ser. A* 106 (2004) 59–75. <586, 591>

[6] R. J. R. Abel, N. J. Finizio, G. Ge, and M. Greig, New Z-cyclic triplewhist frames and triplewhist tournament designs, *Discrete Appl. Math.* 154 (2006) 1649–1673. <611>

[7] R. J. R. Abel and G. Ge, Some difference matrix constructions and an almost completion for the existence of triplewhist tournaments TWh(v), *European J. Combin.* 26 (2005) 1094–1104. <610, 611>

[8] S. S. Abhyankar, Resolution of singularities and modular Galois theory, *Bull. Amer. Math. Soc. (New Ser.)* 38 (2001) 131–169. <232, 233>

[9] S. S. Abhyankar, Symplectic groups and permutation polynomials. II, *Finite Fields Appl.* 8 (2002) 233–255. <232, 233>

[10] F. Abu Salem, S. Gao, and A. G. B. Lauder, Factoring polynomials via polytopes, In *ISSAC '04: Proceedings of the 2004 International Symposium on Symbolic and Algebraic Computation*, 4–11, New York, 2004, ACM. <383, 386>

[11] F. K. Abu Salem, An efficient sparse adaptation of the polytope method over $\mathbb{F}_p$ and a record-high binary bivariate factorisation, *J. Symbolic Comput.* 43 (2008) 311–341. <383, 386>

[12] J.-K. Accetta, Z. Mejías, and A. Santos, Número de waring en cuerpos finitos, Preprint, 2011. <205, 207>

[13] W. W. Adams and P. Loustaunau, *An Introduction to Gröbner Bases*, American Mathematical Society, Providence, RI, first edition, 1994. <80, 81, 694, 695>

[14] L. Adleman and H. Lenstra, Finding irreducible polynomials over finite fields, In *Proceedings of the Eighteenth Annual ACM Symposium on Theory of Computing*, 350–355, ACM, New York, NY, USA, 1986. <114, 122, 372, 373, 374, 398>

[15] L. Adleman, K. Manders, and G. Miller, On taking roots in finite fields, In *Proceedings of the Eighteenth Annual Symposium on Foundations of Computer Science*, 175–178, IEEE Computer Society, Washington, DC, USA, 1977. <375, 376>

[16] L. M. Adleman, The function field sieve, In *Algorithmic Number Theory*, volume 877 of *Lecture Notes in Comput. Sci.*, 108–121, Springer, Berlin, 1994. <392, 394>

[57] W. Aitken, On value sets of polynomials over a finite field, *Finite Fields Appl.* 4 (1998) 441–449. <228, 229>

[58] W. Aitken, M. D. Fried, and L. M. Holt, Davenport pairs over finite fields, *Pacific J. Math.* 216 (2004) 1–38. <233>

[59] M. Ajtai, H. Iwaniec, J. Komlós, J. Pintz, and E. Szemerédi, Construction of a thin set with small Fourier coefficients, *Bull. London Math. Soc.* 22 (1990) 583–590. <178, 179>

[60] A. Akbary, S. Alaric, and Q. Wang, On some classes of permutation polynomials, *Int. J. Number Theory* 4 (2008) 121–133. <216, 217, 222>

[61] A. Akbary, D. Ghioca, and Q. Wang, On permutation polynomials of prescribed shape, *Finite Fields Appl.* 15 (2009) 195–206. <211, 212, 222>

[62] A. Akbary, D. Ghioca, and Q. Wang, On constructing permutations of finite fields, *Finite Fields Appl.* 17 (2010) 1–17. <213, 214, 217, 218, 222>

[63] A. Akbary and Q. Wang, On some permutation polynomials over finite fields, *Int. J. Math. Math. Sci.* 16 (2005) 2631–2640. <215, 222>

[64] A. Akbary and Q. Wang, A generalized Lucas sequence and permutation binomials, *Proc. Amer. Math. Soc.* 134 (2006) 15–22. <211, 215, 216, 222>

[65] A. Akbary and Q. Wang, On polynomials of the form $x^r f(x^{(q-1)/l})$, *Int. J. Math. Math. Sci.* (2007) Art. ID 23408, 7. <214, 215, 216, 222>

[66] S. Akiyama, On the pure Jacobi sums, *Acta Arith.* 75 (1996) 97–104. <140, 155>

[67] M.-L. Akkar, N. T. Courtois, R. Duteuil, and L. Goubin, A fast and secure implementation of Sflash, In *Public Key Cryptography—PKC 2003*, volume 2567 of *Lecture Notes in Comput. Sci.*, 267–278, Springer, Berlin, 2002. <764, 775>

[68] E. Aksoy, A. Çeşmelioğlu, W. Meidl, and A. Topuzoğlu, On the Carlitz rank of permutation polynomials, *Finite Fields Appl.* 15 (2009) 428–440. <222>

[69] A. A. Albert, Symmetric and alternate matrices in an arbitrary field. I, *Trans. Amer. Math. Soc.* 43 (1938) 386–436. <500, 503>

[70] A. A. Albert, *Fundamental Concepts of Higher Algebra*, University of Chicago Press, Chicago, IL, 1958. <57, 58, 59, 61>

[71] A. A. Albert, Finite division algebras and finite planes, In *Proc. Sympos. Appl. Math., Vol. 10*, 53–70, American Mathematical Society, Providence, RI, 1960. <268, 271>

[72] A. A. Albert, Generalized twisted fields, *Pacific J. Math.* 11 (1961) 1–8. <269>

[73] A. A. Albert, Isotopy for generalized twisted fields, *An. Acad. Brasil. Ci.* 33 (1961) 265–275. <269>

[74] R. Albert and H. G. Othmer, The topology of the regulatory interactions predicts the expression pattern of the segment polarity genes in *drosophila melanogaster*, *J. Theoret. Biol.* 223 (2003) 1–18. <816, 825>

[75] W. R. Alford, A. Granville, and C. Pomerance, There are infinitely many Carmichael numbers, *Ann. of Math., 2nd Ser.* 139 (1994) 703–722. <128, 132>

[76] N. Ali, Stabilité des polynômes, *Acta Arith.* 119 (2005) 53–63. <336, 338>

[77] B. Allombert, Explicit computation of isomorphisms between finite fields, *Finite Fields Appl.* 8 (2002) 332–342. <341, 357>

[78] J.-P. Allouche and J. Shallit, *Automatic Sequences: Theory, Applications, Generalizations*, Cambridge University Press, Cambridge, 2003. <539>

[79] J.-P. Allouche and D. S. Thakur, Automata and transcendence of the Tate period in finite characteristic, *Proc. Amer. Math. Soc.* 127 (1999) 1309–1312. <539>

[137] A. Arwin, Über Kongruenzen von dem fünften und höheren Graden nach einem Primzahlmodulus, *Ark. Mat. Astr. Fys.* 14 (1918) 1–46. <375, 376>

[138] M. Aschbacher, Isotopy and geotopy for ternary rings of projective planes, *J. Algebra* 319 (2008) 868–892. <271>

[139] D. W. Ash, I. F. Blake, and S. A. Vanstone, Low complexity normal bases, *Discrete Appl. Math.* 25 (1989) 191–210. <111, 113, 114, 122>

[140] A. Ashikhmin and E. Knill, Nonbinary quantum stabilizer codes, *IEEE Transactions on Information Theory* 47 (2001) 3065–3072. <828, 832>

[141] E. F. Assmus, Jr. and J. D. Key, *Designs and Their Codes*, volume 103 of *Cambridge Tracts in Mathematics*, Cambridge University Press, Cambridge, 1992. <29, 30, 302, 304>

[142] E. F. Assmus, Jr. and H. F. Mattson, Jr., New 5-designs, *J. Combinatorial Theory* 6 (1969) 122–151. <682, 695>

[143] A. O. L. Atkin and F. Morain, Elliptic curves and primality proving, *Math. Comp.* 61 (1993) 29–68. <341, 357>

[144] Y. Aubry and P. Langevin, On the weights of binary irreducible cyclic codes, In *Coding and Cryptography*, volume 3969 of *Lecture Notes in Comput. Sci.*, 46–54, Springer, Berlin, 2006. <146, 155>

[145] Y. Aubry and M. Perret, A Weil theorem for singular curves, In *Arithmetic, Geometry and Coding Theory*, 1–7, de Gruyter, Berlin, 1996. <231, 233>

[146] J.-P. Aumasson, M. Finiasz, W. Meier, and S. Vaudenay, A hardware-oriented trapdoor cipher, In J. Pieprzyk, H. Ghodosi, and E. Dawson, editors, *Information Security and Privacy*, volume 4586 of *Lecture Notes in Computer Science*, 184–199, Springer Berlin / Heidelberg, 2007. <622, 634>

[147] R. Avanzi, Aspects of hyperelliptic curves over large prime fields in software implementations, In *Proceedings of the Sixth International Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, volume 3156 of *Lecture Notes in Comput. Sci.*, 148–162, Springer, Berlin, 2004. <789, 795>

[148] R. Avanzi, N. Thériault, and Z. Wang, Rethinking low genus hyperelliptic Jacobian arithmetic over binary fields: interplay of field arithmetic and explicit formulae, *Journal Mathematical Cryptology* 2 (2008) 227–255. <791, 795>

[149] J. Ax, Zeroes of polynomials over finite fields, *Amer. J. Math.* 86 (1964) 255–261. <193, 195, 207, 474, 481>

[150] N. Axvig, D. Dreher, K. Morrison, E. Psota, L. C. Pérez, and J. L. Walker, Analysis of connections between pseudocodewords, *IEEE Trans. Inform. Theory* 55 (2009) 4099–4107. <710, 711>

[151] M. Ayad and D. L. McQuillan, Irreducibility of the iterates of a quadratic polynomial over a field, *Acta Arith.* 93 (2000) 87–97. <336, 338>

[152] M. Ayad and D. L. McQuillan, Corrections to: "Irreducibility of the iterates of a quadratic polynomial over a field" [Acta Arith. **93** (2000), 87–97; MR1760091 (2001c:11031)], *Acta Arith.* 99 (2001) 97. <336, 338>

[153] M. Baake, J. A. G. Roberts, and A. Weiss, Periodic orbits of linear endomorphisms on the 2-torus and its lattices, *Nonlinearity* 21 (2008) 2427–2446. <331, 338>

[154] L. Babai, The Fourier transform and equations over finite abelian groups, Private Communication. <304>

[155] L. Babai, Spectra of Cayley graphs, *J. Combin. Theory, Ser. B* 27 (1979) 180–189. <644, 650>

[156] L. Babai, W. M. Kantor, and A. Lubotsky, Small-diameter Cayley graphs for finite

[511] M. Car and L. Gallardo, Sums of cubes of polynomials, *Acta Arith.* 112 (2004) 41–50. <492, 493>

[512] M. Car and L. Gallardo, Waring's problem for polynomial biquadrates over a finite field of odd characteristic, *Funct. Approx. Comment. Math.* 37 (2007) 39–50. <207, 492, 493>

[513] P. Carbonne and T. Henocq, Décomposition de la jacobienne sur les corps finis, *Bull. Polish Acad. Sci. Math.* 42 (1994) 207–215. <232, 233>

[514] J.-P. Cardinal, On a property of Cauchy-like matrices, *C. R. Acad. Sci. Paris, Sér. I, Math.* 328 (1999) 1089–1093. <527, 528>

[515] I. Cardinali, O. Polverino, and R. Trombetti, Semifield planes of order q^4 with kernel F_{q^2} and center F_q, *European J. Combin.* 27 (2006) 940–961. <269, 271>

[516] C. Carlet, A larger class of cryptographic Boolean functions via a study of the Maiorana-McFarland construction, In *Advances in Cryptology—CRYPTO 2002*, volume 2442 of *Lecture Notes in Comput. Sci.*, 549–564, Springer, Berlin, 2002. <242, 245>

[517] C. Carlet, On the coset weight divisibility and nonlinearity of resilient and correlation-immune functions, In *Sequences and Their Applications*, Discrete Math. Theor. Comput. Sci. (Lond.), 131–144, Springer, London, 2002. <240, 245>

[518] C. Carlet, On the secondary constructions of resilient and bent functions, In *Coding, Cryptography and Combinatorics*, volume 23 of *Progr. Comput. Sci. Appl. Logic*, 3–28, Birkhäuser, Basel, 2004. <242, 245>

[519] C. Carlet, Recursive lower bounds on the nonlinearity profile of Boolean functions and their applications, *IEEE Trans. Inform. Theory* 54 (2008) 1262–1272. <239, 245>

[520] C. Carlet, Boolean Functions for Cryptography and Error Correcting Codes (Chapter 8), In Y. Crama and P. L. Hammer, editors, *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, 257–397, Cambridge University Press, 2010. <174, 179, 236, 237, 238, 240, 241, 242, 243, 245, 255, 260, 261, 266>

[521] C. Carlet, Vectorial Boolean functions for cryptography, In Y. Crama and P. L. Hammer, editors, *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, 398–469, Cambridge University Press, 2010. <246, 247, 254, 266>

[522] C. Carlet, P. Charpin, and V. Zinoviev, Codes, bent functions and permutations suitable for DES-like cryptosystems, *Des. Codes Cryptogr.* 15 (1998) 125–156. <248, 250, 251, 252, 253, 254>

[523] C. Carlet, L. E. Danielsen, M. G. Parker, and P. Solé, Self-dual bent functions, *Int. J. Inf. Coding Theory* 1 (2010) 384–399. <256, 266>

[524] C. Carlet and S. Dubuc, On generalized bent and q-ary perfect nonlinear functions, In *Finite Fields and Applications*, 81–94, Springer, Berlin, 2001. <264, 266>

[525] C. Carlet and K. Feng, An infinite class of balanced functions with optimal algebraic immunity, good immunity to fast algebraic attacks and good nonlinearity, In *Advances in Cryptology—ASIACRYPT 2008*, volume 5350 of *Lecture Notes in Comput. Sci.*, 425–440, Springer, Berlin, 2008. <243, 245>

[526] C. Carlet and P. Gaborit, Hyper-bent functions and cyclic codes, *J. Combin. Theory, Ser. A* 113 (2006) 466–482. <257, 266>

[527] C. Carlet and P. Guillot, A new representation of Boolean functions, In *Ap-*

plied Algebra, Algebraic Algorithms and Error-Correcting Codes, volume 1719 of *Lecture Notes in Comput. Sci.*, 94–103, Springer, Berlin, 1999. <236, 245>

[528] C. Carlet, T. Helleseth, A. Kholosha, and S. Mesnager, On the dual of bent functions with 2^r Niho exponents, In *Proceedings of the 2011 IEEE International Symposium on Information Theory*, 657–661. IEEE, 2011. <261, 262, 266>

[529] C. Carlet and S. Mesnager, On Dillon's class H of bent functions, Niho bent functions and o-polynomials, *J. Combin. Theory, Ser. A* 118 (2011) 2392–2410. <261, 262, 266>

[530] C. Carlet and A. Pott, editors, *Sequences and Their Applications*, volume 6338 of *Lecture Notes in Computer Science*, Springer, Berlin, 2010. <30>

[531] C. Carlet and P. Sarkar, Spectral domain analysis of correlation immune and resilient Boolean functions, *Finite Fields Appl.* 8 (2002) 120–130. <240, 245>

[532] C. Carlet and B. Sunar, editors, *Arithmetic of Finite Fields*, volume 4547 of *Lecture Notes in Computer Science*, Springer, Berlin, 2007. <30>

[533] C. Carlet and J. L. Yucas, Piecewise constructions of bent and almost optimal Boolean functions, *Des. Codes Cryptogr.* 37 (2005) 449–464. <200>

[534] L. Carlitz, The arithmetic of polynomials in a Galois field, *Amer. J. Math.* 54 (1932) 39–50. <76, 81, 358, 360, 368>

[535] L. Carlitz, Some applications of a theorem of Chevalley, *Duke Math. J.* 18 (1951) 811–819. <207>

[536] L. Carlitz, Primitive roots in a finite field, *Trans. Amer. Math. Soc.* 73 (1952) 373–382. <130, 132>

[537] L. Carlitz, Some problems involving primitive roots in a finite field, *Proc. Nat. Acad. Sci. U.S.A.* 38 (1952) 314–318; errata, 618. <109, 110>

[538] L. Carlitz, A theorem of Dickson on irreducible polynomials, *Proc. Amer. Math. Soc.* 3 (1952) 693–700. <50, 51, 55, 69, 75>

[539] L. Carlitz, Invariantive theory of equations in a finite field, *Trans. Amer. Math. Soc.* 75 (1953) 405–427. <223, 225>

[540] L. Carlitz, Permutations in a finite field, *Proc. Amer. Math. Soc.* 4 (1953) 538. <231, 233>

[541] L. Carlitz, Representations by quadratic forms in a finite field, *Duke Math. J.* 21 (1954) 123–137. <500, 503>

[542] L. Carlitz, Representations by skew forms in a finite field, *Arch. Math. (Basel)* 5 (1954) 19–31. <500, 503>

[543] L. Carlitz, Solvability of certain equations in a finite field, *Quart. J. Math. Oxford, 2nd Ser.* 7 (1956) 3–4. <204, 207>

[544] L. Carlitz, Some theorems on irreducible reciprocal polynomials over a finite field, *J. Reine Angew. Math.* 227 (1967) 212–220. <53, 55, 279, 283>

[545] L. Carlitz, Kloosterman sums and finite field extensions, *Acta Arith.* 16 (1969/1970) 179–193. <150, 155>

[546] L. Carlitz, D. J. Lewis, W. H. Mills, and E. G. Straus, Polynomials over finite fields with minimal value sets, *Mathematika* 8 (1961) 121–130. <207, 226, 229>

[547] L. Carlitz and S. Uchiyama, Bounds for exponential sums, *Duke Math. J.* 24 (1957) 37–41. <315, 318>

[548] L. Carlitz and C. Wells, The number of solutions of a special system of equations in a finite field, *Acta Arith* 12 (1966/1967) 77–84. <211, 223>

[549] R. Carls and D. Lubicz, A p-adic quasi-quadratic time point counting algorithm,

<169, 179, 206, 207>

[646] J. A. Cipra, T. Cochrane, and C. Pinner, Heilbronn's conjecture on Waring's number (mod p), *J. Number Theory* 125 (2007) 289–297. <206, 207>

[647] M. Cipu, Dickson polynomials that are permutations, *Serdica Math. J.* 30 (2004) 177–194. <219, 223>

[648] M. Cipu and S. D. Cohen, Dickson polynomial permutations, In *Finite Fields and Applications*, volume 461 of *Contemp. Math.*, 79–90, Amer. Math. Soc., Providence, RI, 2008. <219, 223>

[649] T. Cochrane, J. Coffelt, and C. Pinner, A further refinement of Mordell's bound on exponential sums, *Acta Arith.* 116 (2005) 35–41. <184, 186>

[650] T. Cochrane, M.-C. Liu, and Z. Zheng, Upper bounds on n-dimensional Kloosterman sums, *J. Number Theory* 106 (2004) 259–274. <154, 155>

[651] T. Cochrane and C. Pinner, Sum-product estimates applied to Waring's problem mod p, *Integers* 8 (2008) A46, 18. <186, 206, 207>

[652] T. Cochrane and C. Pinner, Explicit bounds on monomial and binomial exponential sums, *Q. J. Math.* 62 (2011) 323–349. <334, 338>

[653] T. Cochrane, C. Pinner, and J. Rosenhouse, Bounds on exponential sums and the polynomial Waring problem mod p, *J. London Math. Soc., 2nd Ser.* 67 (2003) 319–336. <207>

[654] T. Cochrane and Z. Zheng, A survey on pure and mixed exponential sums modulo prime powers, In *Number Theory for the Millennium I*, 273–300, A. K. Peters, Natick, MA, 2002. <154, 155>

[655] H. Cohen, *A Course in Computational Algebraic Number Theory*, volume 138 of *Graduate Texts in Mathematics*, Springer-Verlag, Berlin, 1993. <340, 341, 353, 356, 357, 398, 788>

[656] H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, and F. Vercauteren, editors, *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, Discrete Mathematics and Its Applications. Chapman & Hall/CRC, Boca Raton, FL, 2006. <29, 30, 340, 348, 350, 352, 353, 354, 357, 387, 394, 444, 446, 447, 448, 449, 450, 779, 780, 788, 789, 790, 795>

[657] H. Cohen and H. W. Lenstra, Jr., Primality testing and Jacobi sums, *Math. Comp.* 42 (1984) 297–330. <341, 357>

[658] S. Cohen and H. Niederreiter, editors, *Finite Fields and Applications*, volume 233 of *London Mathematical Society Lecture Note Series*, Cambridge, 1996. Cambridge University Press. <30>

[659] S. D. Cohen, The distribution of irreducible polynomials in several indeterminates over a finite field, *Proc. Edinburgh Math. Soc., Ser. II* 16 (1968/1969) 1–17. <77, 78, 81>

[660] S. D. Cohen, Further arithmetical functions in finite fields, *Proc. Edinburgh Math. Soc., Ser. II* 16 (1968/1969) 349–363. <362, 368>

[661] S. D. Cohen, On irreducible polynomials of certain types in finite fields, *Proc. Cambridge Philos. Soc.* 66 (1969) 335–344. <53, 54, 55, 56, 61>

[662] S. D. Cohen, The distribution of polynomials over finite fields, *Acta Arith.* 17 (1970) 255–271. <67, 69, 210, 223, 227, 229, 233>

[663] S. D. Cohen, Some arithmetical functions in finite fields, *Glasgow Math. J.* 11 (1970) 21–36. <76, 78, 81>

[664] S. D. Cohen, Uniform distribution of polynomials over finite fields, *J. London Math. Soc., 2nd Ser.* 6 (1972) 93–102. <73, 75>

[665] S. D. Cohen, The values of a polynomial over a finite field, *Glasgow Math. J.* 14 (1973) 205–208. <362, 368>

[666] S. D. Cohen, The irreducibility of compositions of linear polynomials over a finite field, *Compos. Math.* 47 (1982) 149–152. <56, 59, 61, 62, 66>

[667] S. D. Cohen, The reducibility theorem for linearised polynomials over finite fields, *Bull. Austral. Math. Soc.* 40 (1989) 407–412. <62, 66>

[668] S. D. Cohen, Windmill polynomials over fields of characteristic two, *Monatsh. Math.* 107 (1989) 291–301. <65, 66, 84, 85>

[669] S. D. Cohen, Exceptional polynomials and the reducibility of substitution polynomials, *Enseign. Math., IIe Ser.* 36 (1990) 53–65. <230, 233>

[670] S. D. Cohen, Primitive elements and polynomials with arbitrary trace, *Discrete Math.* 83 (1990) 1–7. <87, 90>

[671] S. D. Cohen, Proof of a conjecture of Chowla and Zassenhaus on permutation polynomials, *Canad. Math. Bull.* 33 (1990) 230–234. <221, 223>

[672] S. D. Cohen, Permutation polynomials and primitive permutation groups, *Arch. Math. (Basel)* 57 (1991) 417–423. <211, 223>

[673] S. D. Cohen, The explicit construction of irreducible polynomials over finite fields, *Des. Codes Cryptogr.* 2 (1992) 169–174. <56, 60, 61, 279, 283>

[674] S. D. Cohen, Dickson polynomials of the second kind that are permutations, *Canad. J. Math.* 46 (1994) 225–238. <219, 223>

[675] S. D. Cohen, Dickson permutations, In *Number-Theoretic and Algebraic Methods in Computer Science*, 29–51, World Sci. Publ., River Edge, NJ, 1995. <219, 223>

[676] S. D. Cohen, Permutation group theory and permutation polynomials, In *Algebras and Combinatorics*, 133–146, Springer, Singapore, 1999. <209, 223>

[677] S. D. Cohen, Gauss sums and a sieve for generators of Galois fields, *Publ. Math. Debrecen* 56 (2000) 293–312. <84, 85, 87, 89, 90>

[678] S. D. Cohen, Kloosterman sums and primitive elements in Galois fields, *Acta Arith.* 94 (2000) 173–201. <88, 90>

[679] S. D. Cohen, Primitive polynomials over small fields, In *Finite Fields and Applications*, volume 2948 of *Lecture Notes in Comput. Sci.*, 197–214, Springer, Berlin, 2004. <88, 90>

[680] S. D. Cohen, Explicit theorems on generator polynomials, *Finite Fields Appl.* 11 (2005) 337–357. <56, 60, 61, 72, 75>

[681] S. D. Cohen, Primitive polynomials with a prescribed coefficient, *Finite Fields Appl.* 12 (2006) 425–491. <87, 90>

[682] S. D. Cohen, Primitive cubics and quartics with zero trace and prescribed norm, *Finite Fields Appl.* 18 (2012) 1156–1168. <87>

[683] S. D. Cohen and M. D. Fried, Lenstra's proof of the Carlitz-Wan conjecture on exceptional polynomials: an elementary version, *Finite Fields Appl.* 1 (1995) 372–375. <211, 223, 231, 233>

[684] S. D. Cohen and M. J. Ganley, Commutative semifields, two-dimensional over their middle nuclei, *J. Algebra* 75 (1982) 373–385. <269, 270, 271, 275>

[685] S. D. Cohen and D. Hachenberger, Primitive normal bases with prescribed trace, *Appl. Algebra Engrg. Comm. Comput.* 9 (1999) 383–403. <84, 85, 110>

[686] S. D. Cohen and D. Hachenberger, Primitivity, freeness, norm and trace, *Discrete Math.* 214 (2000) 135–144. <87, 89, 90>

[687] S. D. Cohen and S. Huczynska, Primitive free quartics with specified norm and trace, *Acta Arith.* 109 (2003) 359–385. <84, 85, 87, 89, 90, 110>

[688] S. D. Cohen and S. Huczynska, The primitive normal basis theorem—without a computer, *J. London Math. Soc., 2nd Ser.* 67 (2003) 41–56. <88, 90>

[689] S. D. Cohen and S. Huczynska, The strong primitive normal basis theorem, *Acta Arith.* 143 (2010) 299–332. <90, 110>

[690] S. D. Cohen and C. King, The three fixed coefficient primitive polynomial theorem, *JP J. Algebra Number Theory Appl.* 4 (2004) 79–87. <88, 90>

[691] S. D. Cohen and R. W. Matthews, A class of exceptional polynomials, *Trans. Amer. Math. Soc.* 345 (1994) 897–909. <232, 233, 294, 296>

[692] S. D. Cohen and R. W. Matthews, Exceptional polynomials over finite fields, *Finite Fields Appl.* 1 (1995) 261–277. <232, 233>

[693] S. D. Cohen and D. Mills, Primitive polynomials with first and second coefficients prescribed, *Finite Fields Appl.* 9 (2003) 334–350. <88, 90>

[694] S. D. Cohen, G. L. Mullen, and P. J.-S. Shiue, The difference between permutation polynomials over finite fields, *Proc. Amer. Math. Soc.* 123 (1995) 2011–2015. <221, 223>

[695] S. D. Cohen and M. Prešern, Primitive finite field elements with prescribed trace, *Southeast Asian Bull. Math.* 29 (2005) 283–300. <87, 90>

[696] S. D. Cohen and M. Prešern, Primitive polynomials with prescribed second coefficient, *Glasgow Math. J.* 48 (2006) 281–307. <87, 90>

[697] S. D. Cohen and M. Prešern, The Hansen-Mullen primitive conjecture: completion of proof, In *Number Theory and Polynomials*, volume 352 of *London Math. Soc. Lecture Note Ser.*, 89–120, Cambridge Univ. Press, Cambridge, 2008. <87, 90>

[698] R. M. Cohn, *Difference Algebra*, Interscience Publishers John Wiley & Sons, New York-London-Sydeny, 1965. <231, 233>

[699] C. J. Colbourn, Covering arrays from cyclotomy, *Des. Codes Cryptogr.* 55 (2010) 201–219. <603, 611>

[700] C. J. Colbourn, Covering arrays and hash families, In *Information Security and Related Combinatorics*, NATO Peace and Information Security, 99–136, IOS Press, 2011. <602, 611>

[701] C. J. Colbourn and J. H. Dinitz, editors, *Handbook of Combinatorial Designs*, Discrete Mathematics and its Applications. Chapman & Hall/CRC, Boca Raton, FL, second edition, 2007. <29, 30, 311, 318, 543, 547, 548, 556, 564, 566, 588, 591, 592, 599, 608, 609, 611>

[702] C. J. Colbourn and A. C. H. Ling, Linear hash families and forbidden configurations, *Des. Codes Cryptogr.* 52 (2009) 25–55. <605, 611>

[703] C. J. Colbourn and A. Rosa, *Triple Systems*, Oxford Mathematical Monographs. The Clarendon Press, Oxford University Press, New York, 1999. <583, 587, 591>

[704] G. E. Collins, Computing multiplicative inverses in GF(p), *Math. Comp.* 23 (1969) 197–200. <353, 357>

[705] G. E. Collins, Lecture notes on arithmetic algorithms, 1980, University of Wisconsin. <353, 357>

[706] A. Commeine and I. Semaev, An algorithm to solve the discrete logarithm problem with the number field sieve, In *Public Key Cryptography—PKC 2006*, volume 3958 of *Lecture Notes in Comput. Sci.*, 174–190, Springer, Berlin, 2006. <393,

[762] F. Daneshgaran and M. Mondin, Design of interleavers for turbo codes: iterative interleaver growth algorithms of polynomial complexity, *IEEE Trans. Inform. Theory* 45 (1999) 1845–1859. <718, 719>

[763] A. Danilevsky, The numerical solution of the secular equation, *Matem. Sbornik* 44 (1937) 169–171, In Russian. <369, 374>

[764] G. Darbi, Sulla riducibilità delle equazioni aldebriche, *Ann. Mat. Pura Appl.* 4 (1927) 185–208. <58, 61>

[765] H. Darmon and J.-F. Mestre, Courbes hyperelliptiques à multiplications réelles et une construction de Shih, *Canad. Math. Bull.* 43 (2000) 304–311. <232, 233>

[766] P. Das, The number of permutation polynomials of a given degree over a finite field, *Finite Fields Appl.* 8 (2002) 478–490. <212, 223>

[767] P. Das, The number of polynomials of a given degree over a finite field with value sets of a given cardinality, *Finite Fields Appl.* 9 (2003) 168–174. <228, 229>

[768] P. Das, Value sets of polynomials and the Cauchy Davenport theorem, *Finite Fields Appl.* 10 (2004) 113–122. <228, 229>

[769] P. Das and G. L. Mullen, Value sets of polynomials over finite fields, In *Finite Fields with Applications to Coding Theory, Cryptography and Related Areas*, 80–85, Springer, Berlin, 2002. <227, 229>

[770] H. Davenport, Bases for finite fields, *J. London Math. Soc., 2nd Ser.* 43 (1968) 21–39. <109, 110, 130, 132>

[771] H. Davenport and D. J. Lewis, Character sums and primitive roots in finite fields, *Rend. Circ. Mat. Palermo, 2nd Ser.* 12 (1963) 129–136. <175, 179>

[772] H. Davenport and D. J. Lewis, Notes on congruences. I, *Quart. J. Math. Oxford, 2nd Ser.* 14 (1963) 51–60. <231, 233, 286, 296>

[773] J. H. Davenport, Y. Siret, and É. Tournier, *Calcul Formel : Systèmes et Algorithmes de Manipulations Algébriques.*, Masson, Paris, France, 1987. <376, 386>

[774] J. H. Davenport and B. M. Trager, Factorization over finitely generated fields, In *SYMSAC'81: Proceedings of the Fourth ACM Symposium on Symbolic and Algebraic Computation*, 200–205. ACM, 1981. <381, 386>

[775] G. Davidoff, P. Sarnak, and A. Valette, *Elementary Number Theory, Group Theory, and Ramanujan Graphs*, volume 55 of *London Mathematical Society Student Texts*, Cambridge University Press, Cambridge, 2003. <644, 645, 650>

[776] J. A. Davis, Difference sets in abelian 2-groups, *J. Combin. Theory, Ser. A* 57 (1991) 262–286. <597, 599>

[777] J. A. Davis and J. Jedwab, A unifying construction for difference sets, *J. Combin. Theory, Ser. A* 80 (1997) 13–78. <597, 599>

[778] J. A. Davis and J. Jedwab, Peak-to-mean power control in OFDM, Golay complementary sequences, and Reed-Muller codes, *IEEE Trans. Inform. Theory* 45 (1999) 2397–2417. <834, 835, 840>

[779] E. Dawson and L. Simpson, Analysis and design issues for synchronous stream ciphers, In *Coding Theory and Cryptology*, volume 1 of *Lect. Notes Ser. Inst. Math. Sci. Natl. Univ. Singap.*, 49–90, World Sci. Publ., River Edge, NJ, 2002. <320, 330>

[780] J. De Beule and L. Storme, *Current Research Topics in Galois Geometry*, Nova Academic Publishers, Inc., New York, 2012. <29, 30, 565, 566>

[781] P. de la Harpe and A. Musitelli, Expanding graphs, Ramanujan graphs, and 1-factor perturbations, *Bull. Belg. Math. Soc. Simon Stevin* 13 (2006) 673–680. <649, 650>

Abh. Math. Sem. Hansischen Univ. 14 (1941) 197–272. <425, 434>

[821] M. Dewar, L. Moura, D. Panario, B. Stevens, and Q. Wang, Division of trinomials by pentanomials and orthogonal arrays, *Des. Codes Cryptogr.* 45 (2007) 1–17. <632, 633, 634>

[822] M. Dewar and D. Panario, Linear transformation shift registers, *IEEE Trans. Inform. Theory* 49 (2003) 2047–2052. <65, 66>

[823] M. Dewar and D. Panario, Mutual irreducibility of certain polynomials, In *Finite Fields and Applications*, volume 2948 of *Lecture Notes in Comput. Sci.*, 59–68, Springer, Berlin, 2004. <65, 66>

[824] J.-F. Dhem, *Design of an Efficient Public Key Cryptographic Library for RISC-Based Smart Cards*, PhD thesis, Faculté des sciences appliquées, Laboratoire de microélectronique, Université catholique de Louvain-la-Neuve, Belgique, 1998, available at `http://users.belgacom.net/dhem/these/index.html`. <348, 357>

[825] A. Díaz and E. Kaltofen, FoxBox a system for manipulating symbolic objects in black box representation, In *ISSAC '98: Proceedings of the 1998 International Symposium on Symbolic and Algebraic Computation*, 30–37, 1998. <386>

[826] J. W. Di Paola, On minimum blocking coalitions in small projective plane games, *SIAM J. Appl. Math.* 17 (1969) 378–392. <553, 556>

[827] P. Diaconis and R. Graham, Products of universal cycles, In E. D. Demaine, M. L. Demaine, and T. Rodgers, editors, *A Lifetime of Puzzles*, 35–55, A. K. Peters Ltd., Wellesley, MA, 2008. <624, 634>

[828] P. Diaconis and R. Graham, *Magical Mathematics: The Mathematical Ideas that Animate Great Magic Tricks*, Princeton University Press, 2011. <624, 634>

[829] P. Diaconis and M. Shahshahani, Generating a random permutation with random transpositions, *Z. Wahrsch. Verw. Gebiete* 57 (1981) 159–179. <643, 644, 650>

[830] J. Dick, Walsh spaces containing smooth functions and quasi-Monte Carlo rules of arbitrary high order, *SIAM J. Numer. Anal.* 46 (2008) 1519–1553. <615, 620, 622>

[831] J. Dick, P. Kritzer, G. Leobacher, and F. Pillichshammer, Constructions of general polynomial lattice rules based on the weighted star discrepancy, *Finite Fields Appl.* 13 (2007) 1045–1070. <616, 622>

[832] J. Dick and H. Niederreiter, On the exact t-value of Niederreiter and Sobol' sequences, *J. Complexity* 24 (2008) 572–581. <620, 622>

[833] J. Dick and H. Niederreiter, Duality for digital sequences, *J. Complexity* 25 (2009) 406–414. <620, 622>

[834] J. Dick and F. Pillichshammer, *Digital Nets and Sequences: Discrepancy Theory and Quasi-Monte Carlo Integration*, Cambridge University Press, Cambridge, 2010. <612, 615, 616, 617, 620, 622>

[835] L. E. Dickson, The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group, *Ann. of Math.* 11 (1896/97) 65–120. <209, 223, 230, 233>

[836] L. E. Dickson, Higher irreducible congruences, *Bull. Amer. Math. Soc.* 3 (1897) 381–389. <58, 61>

[837] L. E. Dickson, A class of groups in an arbitrary realm connected with the configuration of the 27 lines on a cubic surface, *Quart. J. Pure Appl. Math.* 33 (1901) 145–173. <10>

[838] L. E. Dickson, Theory of linear groups in an arbitrary field, *Trans. Amer. Math. Soc.* 2 (1901) 363–394. <10>

[839] L. E. Dickson, A new system of simple groups, *Math. Ann.* 60 (1905) 137–150. <10>

[840] L. E. Dickson, On finite algebras, In *Gesellschaften der Wissenschaften zu Göttingen*, 358–393, 1905. <269, 271>

[841] L. E. Dickson, Criteria for the irreducibility of functions in a finite field, *Bull. Amer. Math. Soc.* 13 (1906) 1–8. <63, 66>

[842] L. E. Dickson, On commutative linear algebras in which division is always uniquely possible, *Trans. Amer. Math. Soc.* 7 (1906) 514–522. <269, 271, 275>

[843] L. E. Dickson, A class of groups in an arbitrary realm connected with the configuration of the 27 lines on a cubic surface (second paper), *Quart. J. Pure Appl. Math.* 39 (1908) 205–209. <10>

[844] L. E. Dickson, A fundamental system of invariants of the general modular linear group with a solution of the form problem, *Trans. Amer. Math. Soc.* 12 (1911) 75–98. <58, 59, 61>

[845] L. E. Dickson, *Linear Groups: With an Exposition of the Galois Field Theory*, with an introduction by W. Magnus. Dover Publications Inc., New York, 1958. <2, 10, 29, 30, 57, 58, 59, 61, 66, 68, 69>

[846] L. E. Dickson, *History of the Theory of Numbers. Vol. I: Divisibility and Primality*, Chelsea Publishing Co., New York, 1966. <2, 10>

[847] C. Diem, The GHS attack in odd characteristic, *Journal of the Ramanujan Mathematical Society* 18 (2003) 1–32. <778, 788, 802, 803>

[848] C. Diem, The XL-algorithm and a conjecture from commutative algebra, In *Advances in Cryptology—ASIACRYPT 2004*, volume 3329 of *Lecture Notes in Comput. Sci.*, 323–337, Springer, Berlin, 2004. <774, 775>

[849] C. Diem, An index calculus algorithm for plane curves of small degree, In *Algorithmic Number Theory*, volume 4076 of *Lecture Notes in Comput. Sci.*, 543–557, Springer, Berlin, 2006. <790, 795, 800, 803>

[850] C. Diem and J. Scholten, Cover Attacks – A report for the AREHCC project, 2003. <794, 795>

[851] C. Diem and E. Thomé, Index calculus in class groups of non-hyperelliptic curves of genus three, *J. Cryptology* 21 (2008) 593–611. <790, 795, 801, 803>

[852] J. Dieudonné, *Sur les Groupes Classiques*, Actualités Sci. Ind., 1040 (Publ. Inst. Math. Univ. Strasbourg Nou. Sér. 1 (1945)). Hermann et Cie., Paris, 1948. <506, 508, 509, 511, 512, 513, 514>

[853] J. A. Dieudonné, *La Géométrie des Groupes Classiques*, Springer-Verlag, Berlin, 1971, IIe ed. <505, 509, 513, 514>

[854] W. Diffie and M. E. Hellman, New directions in cryptography, *IEEE Trans. Information Theory* IT-22 (1976) 644–654. <177, 179, 737>

[855] W. Diffie and M. E. Hellman, New directions in cryptography, In *Secure Communications and Asymmetric Cryptosystems*, volume 69 of *AAAS Sel. Sympos. Ser.*, 143–180, Westview, Boulder, CO, 1982. <756, 775>

[856] J. F. Dillon, *Elementary Hadamard Difference-Sets*, ProQuest LLC, Ann Arbor, MI, 1974, Thesis (Ph.D.)–University of Maryland, College Park. <258, 259, 260, 262, 263, 266>

[857] J. F. Dillon, Multiplicative difference sets via additive characters, *Des. Codes Cryptogr.* 17 (1999) 225–235. <232, 233, 253, 254, 595, 599>

[858] J. F. Dillon, Geometry, codes and difference sets: exceptional connections, In *Codes and Designs*, volume 10 of *Ohio State Univ. Math. Res. Inst. Publ.*, 73–85, de Gruyter, Berlin, 2002. <232, 233, 253, 254>

[859] J. F. Dillon and H. Dobbertin, New cyclic difference sets with Singer parameters, *Finite Fields Appl.* 10 (2004) 342–389. <232, 233, 253, 254, 261, 266, 313, 318, 595, 599, 746, 747, 755>

[860] J. F. Dillon and G. McGuire, Near bent functions on a hyperplane, *Finite Fields Appl.* 14 (2008) 715–720. <304>

[861] E. Dimitrova, L. D. García-Puente, F. Hinkelmann, A. S. Jarrah, R. Laubenbacher, B. Stigler, M. Stillman, and P. Vera-Licona, Polynome, Available at `http://polymath.vbi.vt.edu/polynome/`, 2010. <823, 825>

[862] E. Dimitrova, L. D. García-Puente, F. Hinkelmann, A. S. Jarrah, R. Laubenbacher, B. Stigler, M. Stillman, and P. Vera-Licona, Parameter estimation for Boolean models of biological networks, *Theoret. Comput. Sci.* 412 (2011) 2816–2826. <822, 825>

[863] E. S. Dimitrova, A. S. Jarrah, R. Laubenbacher, and B. Stigler, A Gröbner fan method for biochemical network modeling, In *ISSAC 2007*, 122–126, ACM, New York, 2007. <822, 825>

[864] C. Ding, T. Helleseth, and H. Niederreiter, editors, *Sequences and Their Applications*, Springer Series in Discrete Mathematics and Theoretical Computer Science, London, 1999. Springer-Verlag London Ltd. <30>

[865] C. Ding, D. Pei, and A. Salomaa, *Chinese Remainder Theorem: Applications in Computing, Coding, Cryptography*, World Scientific Publishing Co. Inc., River Edge, NJ, 1996. <222, 223>

[866] C. Ding, Z. Wang, and Q. Xiang, Skew Hadamard difference sets from the Ree-Tits slice symplectic spreads in $\mathrm{PG}(3, 3^{2h+1})$, *J. Combin. Theory, Ser. A* 114 (2007) 867–887. <222, 223, 274, 275, 596, 599>

[867] C. Ding, Q. Xiang, J. Yuan, and P. Yuan, Explicit classes of permutation polynomials of $\mathbb{F}_{3^{3m}}$, *Sci. China, Ser. A* 52 (2009) 639–647. <219, 223>

[868] C. Ding, G. Xiao, and W. Shan, *The Stability Theory of Stream Ciphers*, volume 561 of *Lecture Notes in Computer Science*, Springer-Verlag, Berlin, 1991. <320, 323, 330>

[869] C. Ding and J. Yuan, A family of skew Hadamard difference sets, *J. Combin. Theory, Ser. A* 113 (2006) 1526–1535. <222, 223, 272, 275, 596, 599>

[870] C. Ding and P. Yuan, Permutation polynomials over finite fields from a powerful lemma, *Finite Fields Appl.* 17 (2011) 560–574. <214, 217, 219, 223>

[871] C. S. Ding, H. Niederreiter, and C. P. Xing, Some new codes from algebraic curves, *IEEE Trans. Inform. Theory* 46 (2000) 2638–2642. <699, 704>

[872] J. Ding, A new variant of the Matsumoto-Imai cryptosystem through perturbation, In *Public Key Cryptography—PKC 2004*, volume 2947 of *Lecture Notes in Comput. Sci.*, 305–318, Springer, Berlin, 2004. <765, 775>

[873] J. Ding, Mutants and its impact on polynomial solving strategies and algorithms, Privately distributed research note, University of Cincinnati and Technical University of Darmstadt, 2006. <773, 775>

[874] J. Ding, Inverting square systems algebraically is exponential, Cryptology ePrint Archive, Report 2011/275, 2011, `http://eprint.iacr.org/`. <762, 767, 774, 775>

[875] J. Ding, J. Buchmann, M. S. E. Mohamed, W. S. A. M. Mohamed, and R.-P.

Cryptography, Springer, Berlin, 2009. <755, 775>

[890] J. Ding and B.-Y. Yang, Multivariate polynomials for hashing, In *Inscrypt*, LNCS. Springer, 2007, to appear, cf. `http://eprint.iacr.org/2007/137`. <774, 775>

[891] J. Ding, B.-Y. Yang, C.-H. O. Chen, M.-S. Chen, and C.-M. Cheng, New differential-algebraic attacks and reparametrization of rainbow, In *Applied Cryptography and Network Security*, volume 5037 of *LNCS*, 242–257. Springer, 2008, cf. `http://eprint.iacr.org/2008/108`. <764, 765, 771, 772, 773, 775>

[892] J. Ding and Z. Yin, Cryptanalysis of TTS and Tame–like signature schemes, In *Third International Workshop on Applied Public Key Infrastructures*, 2004. <766, 775>

[893] J. H. Dinitz, New lower bounds for the number of pairwise orthogonal symmetric Latin squares, In *Proceedings of the Tenth Southeastern Conference on Combinatorics, Graph Theory and Computing*, Congress. Numer., XXIII–XXIV, 393–398, Winnipeg, Man., 1979. <606, 611>

[894] J. H. Dinitz and D. R. Stinson, The construction and uses of frames, *Ars Combin.* 10 (1980) 31–53. <607, 608, 611>

[895] J. H. Dinitz and D. R. Stinson, Room squares and related designs, In *Contemporary Design Theory*, Wiley-Intersci. Ser. Discrete Math. Optim., 137–204, Wiley, New York, 1992. <608, 611>

[896] J. H. Dinitz and G. S. Warrington, The spectra of certain classes of Room frames: the last cases, *Electron. J. Combin.* 17 (2010) Research Paper 74, 13 pages. <608, 611>

[897] J. D. Dixon and D. Panario, The degree of the splitting field of a random polynomial over a finite field, *Electron. J. Combin.* 11 (2004) Research Paper 70, 10 pp. <367, 368>

[898] V. Dmytrenko, F. Lazebnik, and J. Williford, On monomial graphs of girth eight, *Finite Fields Appl.* 13 (2007) 828–842. <222, 223>

[899] H. Dobbertin, Almost perfect nonlinear power functions on GF(2^n): the Niho case, *Inform. and Comput.* 151 (1999) 57–72. <222, 223, 254, 255>

[900] H. Dobbertin, Almost perfect nonlinear power functions on GF(2^n): the Welch case, *IEEE Trans. Inform. Theory* 45 (1999) 1271–1275. <222, 223, 254, 255>

[901] H. Dobbertin, Kasami power functions, permutation polynomials and cyclic difference sets, In *Difference Sets, Sequences and Their Correlation Properties*, volume 542 of *NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci.*, 133–158, Kluwer Acad. Publ., Dordrecht, 1999. <232, 233, 595, 599>

[902] H. Dobbertin, Almost perfect nonlinear power functions on GF(2^n): a new case for n divisible by 5, In *Finite Fields and Applications*, 113–121, Springer, Berlin, 2001. <220, 223, 254, 255>

[903] H. Dobbertin, G. Leander, A. Canteaut, C. Carlet, P. Felke, and P. Gaborit, Construction of bent functions via Niho power functions, *J. Combin. Theory, Ser. A* 113 (2006) 779–798. <261, 266>

[904] H. Dobbertin, D. Mills, E. N. Müller, A. Pott, and W. Willems, APN functions in odd characteristic, *Discrete Math.* 267 (2003) 95–112. <249, 254, 255>

[905] C. Doche, Redundant trinomials for finite fields of characteristic 2, In *Australasian Conference on Information Security and Privacy – ACISP 2005*, volume 3574 of *Lecture Notes in Comput. Sci.*, 122–133, Springer, Berlin, 2005. <345, 347, 357>

groups to prime-order groups, In *Advances in Cryptology—EUROCRYPT 2010*, volume 6110 of *Lecture Notes in Computer Science*, 44–61, Springer-Verlag, Berlin, 2010. <784, 788>

[1096] J. W. Freeman, Reguli and pseudoreguli in PG(3, s^2), *Geom. Dedicata* 9 (1980) 267–280. <563, 566>

[1097] T. S. Freeman, G. Imirzian, E. Kaltofen, and Lakshman Yagati, DAGWOOD: A system for manipulating polynomials given by straight-line programs, *ACM Trans. Math. Software* 14 (1988) 218–240. <385, 386>

[1098] D. Freemann, M. Scott, and E. Teske, A taxonomy of pairing-friendly elliptic curves, *Journal of Cryptology* 23 (2010) 224–280. <785, 786, 788>

[1099] Free Software Foundation, GNU Multiple Precision library, version 5.0.4, 2012, available at `http://gmplib.org/`. <340, 349, 357>

[1100] G. Frei, The unpublished section eight: on the way to function fields over a finite field, In *The Shaping of Arithmetic After C. F. Gauss's Disquisitiones Arithmeticae*, 159–198, Berlin: Springer, 2007. <5>

[1101] G. Frey, Applications of arithmetical geometry to cryptographic constructions, In D. Jungnickel and H. Niederreiter, editors, *Finite Fields and Applications*, 128–161, Springer-Verlag, Berlin, 2001. <777, 788, 801, 803>

[1102] G. Frey and T. Lange, Varieties over special fields, In *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, Discrete Math. Appl., 87–113, Chapman & Hall/CRC, Boca Raton, FL, 2006. <29, 30, 450>

[1103] G. Frey, M. Müller, and H.-G. Rück, The Tate pairing and the discrete logarithm applied to elliptic curve cryptosystems, *IEEE Trans. Inform. Theory* 45 (1999) 1717–1719. <450>

[1104] G. Frey, M. Perret, and H. Stichtenoth, On the different of abelian extensions of global fields, In *Coding Theory and Algebraic Geometry*, volume 1518 of *Lecture Notes in Math.*, 26–32, Springer, Berlin, 1992. <462, 463>

[1105] G. Frey and H.-G. Rück, A remark concerning m-divisibility and the discrete logarithm problem in the divisor class group of curves, *Math. Comp.* 62 (1994) 865–874. <784, 788, 802, 803>

[1106] M. Fried, On a conjecture of Schur, *Michigan Math. J.* 17 (1970) 41–55. <221, 223, 232, 233, 277, 283, 286, 287, 296>

[1107] M. Fried, The field of definition of function fields and a problem in the reducibility of polynomials in two variables, *Illinois J. Math.* 17 (1973) 128–146. <294, 296>

[1108] M. Fried, On a theorem of Ritt and related Diophantine problems, *J. Reine Angew. Math.* 264 (1973) 40–55. <288, 296>

[1109] M. Fried, On a theorem of MacCluer, *Acta Arith.* 25 (1973/74) 121–126. <285, 286, 296>

[1110] M. Fried, On Hilbert's irreducibility theorem, *J. Number Theory* 6 (1974) 211–231. <287, 289, 293, 296>

[1111] M. Fried, Fields of definition of function fields and Hurwitz families—groups as Galois groups, *Comm. Algebra* 5 (1977) 17–82. <285, 296>

[1112] M. Fried, Galois groups and complex multiplication, *Trans. Amer. Math. Soc.* 235 (1978) 141–163. <232, 233, 292, 293, 296>

[1113] M. Fried and R. Lidl, On Dickson polynomials and Rédei functions, In *Contributions to General Algebra, 5*, 139–149, Hölder-Pichler-Tempsky, Vienna, 1987. <277, 283>

[1114] M. Fried and G. Sacerdote, Solving Diophantine problems over all residue class fields of a number field and all finite fields, *Ann. of Math., 2nd Ser.* 104 (1976) 203–233. <294, 295, 296>

[1115] M. D. Fried, The place of exceptional covers among all Diophantine relations, *Finite Fields Appl.* 11 (2005) 367–433. <285, 286, 287, 289, 290, 291, 292, 293, 294, 295, 296>

[1116] M. D. Fried, Variables separated equations: Strikingly different roles for the branch cycle lemma and the finite simple group classification, *Science China Mathematics* 55 (2012) 1–69. <286, 291, 294, 295, 296>

[1117] M. D. Fried, R. Guralnick, and J. Saxl, Schur covers and Carlitz's conjecture, *Israel J. Math.* 82 (1993) 157–225. <211, 223, 230, 233, 287, 294, 296>

[1118] M. D. Fried and M. Jarden, *Field Arithmetic*, volume 11 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*, Springer-Verlag, Berlin, 1986. <29, 30, 288, 293, 294, 295, 296>

[1119] M. D. Fried and M. Jarden, *Field Arithmetic*, volume 11 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas, 3rd Series. A Series of Modern Surveys in Mathematics]*, Springer-Verlag, Berlin, third edition, 2008, Revised by Jarden. <29, 30, 231, 233>

[1120] M. D. Fried and R. E. MacRae, On curves with separated variables, *Math. Ann.* 180 (1969) 220–226. <293, 296>

[1121] M. D. Fried and R. E. MacRae, On the invariance of chains of fields, *Illinois J. Math.* 13 (1969) 165–171. <287, 296>

[1122] E. Friedman and L. C. Washington, On the distribution of divisor class groups of curves over a finite field, In *Théorie des Nombres*, 227–239, de Gruyter, Berlin, 1989. <444, 450>

[1123] J. Friedman, Some geometric aspects of graphs and their eigenfunctions, *Duke Math. J.* 69 (1993) 487–525. <638, 639, 648, 650>

[1124] J. Friedman, A Proof of Alon's Second Eigenvalue Conjecture and Related Problems, *Mem. Amer. Math. Soc.* 195 (2008). <649, 650>

[1125] J. Friedman, R. Murty, and J.-P. Tillich, Spectral estimates for abelian Cayley graphs, *J. Combin. Theory, Ser. B* 96 (2006) 111–121. <643, 650>

[1126] C. Friesen, A special case of Cohen-Lenstra heuristics in function fields, In *Number Theory*, volume 19 of *CRM Proc. Lecture Notes*, 99–105, Amer. Math. Soc., Providence, RI, 1999. <444, 450>

[1127] C. Friesen, Class group frequencies of real quadratic function fields: the degree 4 case, *Math. Comp.* 69 (2000) 1213–1228. <444, 450>

[1128] C. Friesen, Bounds for frequencies of class groups of real quadratic genus 1 function fields, *Acta Arith.* 96 (2001) 313–331. <444, 450>

[1129] S. Frisch, When are weak permutation polynomials strong?, *Finite Fields Appl.* 1 (1995) 437–439. <225>

[1130] D. Fu and J. Solinas, IKE and IKEv2 authentication using the elliptic curve digital signature algorithm (ECDSA), RFC 4754, Internet Engineering Task Force, 2007, `http://www.ietf.org/rfc/rfc4754.txt`. <777, 788>

[1131] F.-W. Fu, H. Niederreiter, and F. Özbudak, On the joint linear complexity of linear recurring multisequences, In *Coding and Cryptology*, volume 4 of *Ser. Coding Theory Cryptol.*, 125–142, World Sci. Publ., Hackensack, NJ, 2008. <319, 325, 330>

[1209] T. Garefalakis and D. Panario, The index calculus method using non-smooth polynomials, *Math. Comp.* 70 (2001) 1253–1264. <364, 368>

[1210] T. Garefalakis and D. Panario, Polynomials over finite fields free from large and small degree irreducible factors, *J. Algorithms* 44 (2002) 98–120. <364, 368>

[1211] M. R. Garey and D. S. Johnson, *Computers and Intractability: A Guide to the Theory of NP-completeness*, W. H. Freeman and Co., San Francisco, Calif., 1979. <773, 775>

[1212] G. Garg, T. Helleseth, and P. V. Kumar, Recent advances in low-correlation sequences, In V. Tarokh, editor, *New Directions in Wireless Communications Research*, chapter 3, 63–92, Springer-Verlag, Berlin, 2009. <311, 317, 318>

[1213] J. von zur Gathen, Factoring sparse multivariate polynomials, In *Twenty Fourth Annual IEEE Symposium on Foundations of Computer Science*, 172–179, Los Alamitos, CA, USA, 1983. <385, 386>

[1214] J. von zur Gathen, Hensel and Newton methods in valuation rings, *Math. Comp.* 42 (1984) 637–661. <379, 386>

[1215] J. von zur Gathen, Irreducibility of multivariate polynomials, *J. Comput. System Sci.* 31 (1985) 225–264. <380, 384, 386>

[1216] J. von zur Gathen, Irreducible polynomials over finite fields, In *Proc. Sixth Conf. Foundations of Software Technology and Theoretical Computer Science*, volume 241 of *Springer Lecture Notes in Computer Science*, 252–262, Delhi, India, 1986. <373, 374>

[1217] J. von zur Gathen, Factoring polynomials and primitive elements for special primes, *Theoretical Computer Science* 52 (1987) 77–89. <375, 376>

[1218] J. von zur Gathen, Tests for permutation polynomials, *SIAM J. Comput.* 20 (1991) 591–602. <210, 223>

[1219] J. von zur Gathen, Values of polynomials over finite fields, *Bull. Austral. Math. Soc.* 43 (1991) 141–146. <228, 229, 231, 233>

[1220] J. von zur Gathen, Irreducible trinomials over finite fields, *Math. Comp.* 72 (2003) 1987–2000. <65, 66, 342, 357>

[1221] J. von zur Gathen, Counting decomposable multivariate polynomials, *Appl. Algebra Engrg. Comm. Comput.* 22 (2011) 165–185. <79, 80, 81>

[1222] J. von zur Gathen and J. Gerhard, Arithmetic and factorization of polynomials over $\mathbb{F}_2$, Technical Report tr-rsfb-96-018, University of Paderborn, Germany, 1996, 43 pages. <376>

[1223] J. von zur Gathen and J. Gerhard, Polynomial factorization over $\mathbb{F}_2$, *Math. Comp.* 71 (2002) 1677–1698. <362, 368, 375, 376>

[1224] J. von zur Gathen and J. Gerhard, *Modern Computer Algebra*, Cambridge University Press, Cambridge, New York, Melbourne, second edition, 2003. <29, 30, 80, 81, 119, 120, 122, 340, 357, 370, 371, 374, 375, 376, 379, 381, 386>

[1225] J. von zur Gathen, J. L. Imaña, and Ç. K. Koç, editors, *Arithmetic of Finite Fields*, volume 5130 of *Lecture Notes in Computer Science*, Berlin, 2008. Springer, Available electronically at `http://www.springerlink.com/content/978-3-540-69498-4`. <30>

[1226] J. von zur Gathen and E. Kaltofen, Factoring multivariate polynomials over finite fields, *Math. Comp.* 45 (1985) 251–261. <380, 386>

[1227] J. von zur Gathen and E. Kaltofen, Factoring sparse multivariate polynomials, *J. Comput. System Sci.* 31 (1985) 265–287. <384, 385, 386>

[1228] J. von zur Gathen, M. Karpinski, and I. E. Shparlinski, Counting curves and their

814>

[1358] K. C. Gupta and S. Maitra, Multiples of primitive polynomials over GF(2), In *Progress in Cryptology—INDOCRYPT 2001*, volume 2247 of *Lecture Notes in Comput. Sci.*, 62–72, Springer, Berlin, 2001. <627, 634>

[1359] S. Gurak, Gauss and Eisenstein sums of order twelve, *Canad. Math. Bull.* 46 (2003) 344–355. <145, 155>

[1360] S. Gurak, Gauss sums for prime powers in p-adic fields, *Acta Arith.* 142 (2010) 11–39. <154, 155>

[1361] S. Gurak, Jacobi sums and irreducible polynomials with prescribed trace and restricted norm, In *Finite Fields: Theory and Applications*, volume 518 of *Contemp. Math.*, 193–208, Amer. Math. Soc., Providence, RI, 2010. <137, 155>

[1362] S. J. Gurak, Kloosterman sums for prime powers in p-adic fields, *J. Théor. Nombres Bordeaux* 21 (2009) 175–201. <154, 155>

[1363] R. Guralnick and D. Wan, Bounds for fixed point free elements in a transitive group and applications to curves over finite fields, *Israel J. Math.* 101 (1997) 255–287. <226, 229>

[1364] R. M. Guralnick, Rational maps and images of rational points of curves over finite fields, *Irish Math. Soc. Bull.* (2003) 71–95. <226, 229, 233>

[1365] R. M. Guralnick and P. Müller, Exceptional polynomials of affine type, *J. Algebra* 194 (1997) 429–454. <230, 231, 233>

[1366] R. M. Guralnick, P. Müller, and J. Saxl, The rational function analogue of a question of Schur and exceptionality of permutation representations, *Mem. Amer. Math. Soc.* 162 (2003) viii+79. <232, 233, 292, 293, 296>

[1367] R. M. Guralnick, P. Müller, and M. E. Zieve, Exceptional polynomials of affine type, revisited, Preprint, 1999. <231, 233>

[1368] R. M. Guralnick, J. Rosenberg, and M. E. Zieve, A new family of exceptional polynomials in characteristic two, *Ann. of Math., 2nd Ser.* 172 (2010) 1361–1390. <230, 233>

[1369] R. M. Guralnick, T. J. Tucker, and M. E. Zieve, Exceptional covers and bijections on rational points, *Int. Math. Res. Not. IMRN* (2007) Art. ID rnm004, 20. <232, 233>

[1370] R. M. Guralnick and M. E. Zieve, Polynomials with PSL(2) monodromy, *Ann. of Math., 2nd Ser.* 172 (2010) 1315–1359. <230, 233>

[1371] V. Guruswami and A. C. Patthak, Correlated algebraic-geometric codes: improved list decoding over bounded alphabets, *Math. Comp.* 77 (2008) 447–473. <697, 704>

[1372] V. Guruswami and A. Rudra, Limits to list decoding Reed-Solomon codes, *IEEE Trans. Inform. Theory* 52 (2006) 3642–3649. <691, 695>

[1373] V. Guruswami and M. Sudan, Improved decoding of Reed-Solomon and algebraic-geometry codes, *IEEE Trans. Inform. Theory* 45 (1999) 1757–1767. <691, 695>

[1374] F. G. Gustavson, Analysis of the Berlekamp-Massey linear feedback shift-register synthesis algorithm, *IBM J. Res. Develop.* 20 (1976) 204–212. <324, 330>

[1375] J. Gutierrez and D. Gómez-Pérez, Iterations of multivariate polynomials and discrepancy of pseudorandom numbers, In *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, volume 2227 of *Lecture Notes in Comput. Sci.*, 192–199, Springer, Berlin, 2001. <332, 334, 338>

[1376] J. Gutierrez and Á. Ibeas, Inferring sequences produced by a linear congruential

[1749] R. Kloosterman, The zeta function of monomial deformations of Fermat hypersurfaces, *Algebra Number Theory* 1 (2007) 421–450. <473, 481>

[1750] A. A. Klyachko, Monodromy groups of polynomial mappings, In *Studies in Number Theory*, volume 6, 82–91, Izdat. Saratov. Univ., Saratov, 1975. <230, 233>

[1751] A. W. Knapp, *Elliptic Curves*, volume 40 of *Mathematical Notes*, Princeton University Press, Princeton, NJ, 1992. <29, 30, 417, 434>

[1752] M. P. Knapp, Diagonal equations of different degrees over p-adic fields, *Acta Arith.* 126 (2007) 139–154. <207>

[1753] N. Knarr and M. Stroppel, Polarities and unitals in the Coulter-Matthews planes, *Des. Codes Cryptogr.* 55 (2010) 9–18. <273, 275>

[1754] E. Knill and R. Laflamme, Theory of quantum error-correcting codes, *Phys. Rev. A* 55 (1997) 900–911. <828, 832>

[1755] A. Knopfmacher and J. Knopfmacher, Counting polynomials with a given number of zeros in a finite field, *Linear and Multilinear Algebra* 26 (1990) 287–292. <362, 368>

[1756] A. Knopfmacher and J. Knopfmacher, Counting irreducible factors of polynomials over a finite field, *Discrete Math.* 112 (1993) 103–118. <362, 368>

[1757] A. Knopfmacher, J. Knopfmacher, and R. Warlimont, Lengths of factorizations for polynomials over a finite field, In *Finite Fields: Theory, Applications, and Algorithms*, volume 168 of *Contemp. Math.*, 185–206, Amer. Math. Soc., Providence, RI, 1994. <362, 368>

[1758] A. Knopfmacher and R. Warlimont, Distinct degree factorizations for polynomials over a finite field, *Trans. Amer. Math. Soc.* 347 (1995) 2235–2243. <362, 368>

[1759] D. E. Knuth, Finite semifields and projective planes, *J. Algebra* 2 (1965) 182–217. <267, 269, 271>

[1760] D. E. Knuth, *The Art of Computer Programming. Vol. 2: Seminumerical Algorithms*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont, 1969. <359, 361, 368, 391, 394>

[1761] D. E. Knuth, The analysis of algorithms, In *Actes du Congrès International des Mathématiciens (Nice, 1970), Tome 3*, 269–274, Gauthier-Villars, Paris, 1971. <353, 357>

[1762] D. E. Knuth, *The Art of Computer Programming. Vol. 2, Seminumerical Algorithms*, Addison-Wesley Publishing Company, Reading, MA, second edition, 1981, Addison-Wesley Series in Computer Science and Information Processing. <350, 357>

[1763] D. E. Knuth, *The Art of Computer Programming. Vol. 2, Seminumerical algorithms*, Addison-Wesley Publishing Company, Reading, MA, third edition, 1997, Addison-Wesley Series in Computer Science and Information Processing. <340, 348, 349, 357>

[1764] N. Koblitz, p-adic variation of the zeta-function over families of varieties defined over finite fields, *Compositio Math.* 31 (1975) 119–218. <480, 481>

[1765] N. Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, Graduate Texts in Mathematics, Vol. 58, Springer-Verlag, New York, 1977. <474, 481>

[1766] N. Koblitz, Elliptic curve cryptosystems, *Math. Comp.* 48 (1987) 203–209. <737, 741, 775, 788>

[1767] N. Koblitz, Hyperelliptic cryptosystems, *J. Cryptology* 1 (1989) 139–150. <737, 741, 789, 795>

[1768] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, volume 97 of *Grad-*

<472, 473>

[1864] G. Laumon, Exponential sums and l-adic cohomology: a survey, *Israel J. Math.* 120 (2000) 225–257. <163>

[1865] M. Lavrauw, G. L. Mullen, S. Nikova, D. Panario, and L. Storme, editors, *Proc. Tenth International Conference on Finite Fields and Applications*, volume 579, Amer. Math. Soc., Providence, RI, 2012. <30>

[1866] M. Lavrauw and O. Polverino, Finite semifields, In L. Storme and J. D. Buele, editors, *Current Research Topics in Galois Geometry*, chapter 6, Nova Publishers, 2011. <267, 271>

[1867] M. Lavrauw, L. Storme, and G. Van de Voorde, A proof of the linearity conjecture for k-blocking sets in $\mathrm{PG}(n, p^3)$, p prime, *J. Combin. Theory, Ser. A* 118 (2011) 808–818. <553, 556>

[1868] K. M. Lawrence, A combinatorial characterization of (t, m, s)-nets in base b, *J. Combin. Des.* 4 (1996) 275–293. <613, 622>

[1869] K. M. Lawrence, A. Mahalanabis, G. L. Mullen, and W. C. Schmid, Construction of digital (t, m, s)-nets from linear codes, In *Finite Fields and Applications*, volume 233 of *London Math. Soc. Lecture Note Ser.*, 189–208, Cambridge University Press, Cambridge, 1996. <617, 622>

[1870] C. F. Laywine and G. L. Mullen, *Discrete Mathematics using Latin Squares*, Wiley-Interscience Series in Discrete Mathematics and Optimization. John Wiley & Sons Inc., New York, 1998. <29, 30, 544, 548>

[1871] C. F. Laywine, G. L. Mullen, and G. Whittle, d-dimensional hypercubes and the Euler and MacNeish conjectures, *Monatsh. Math.* 119 (1995) 223–238. <545, 546, 548>

[1872] D. Lazard, Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations, In *Computer Algebra*, volume 162 of *Lecture Notes in Comput. Sci.*, 146–156, Springer, Berlin, 1983. <773, 775>

[1873] G. Leander and A. Kholosha, Bent functions with 2^r Niho exponents, *IEEE Trans. Inform. Theory* 52 (2006) 5529–5532. <261, 266>

[1874] N. G. Leander, Monomial bent functions, *IEEE Trans. Inform. Theory* 52 (2006) 738–743. <261, 263, 266>

[1875] G. Lecerf, Sharp precision in Hensel lifting for bivariate polynomial factorization, *Math. Comp.* 75 (2006) 921–933. <379, 386>

[1876] G. Lecerf, Improved dense multivariate polynomial factorization algorithms, *J. Symbolic Comput.* 42 (2007) 477–494. <380, 386>

[1877] G. Lecerf, Fast separable factorization and applications, *Appl. Alg. Eng. Comm. Comp.* 19 (2008) 135–160. <377, 378, 386>

[1878] G. Lecerf, New recombination algorithms for bivariate polynomial factorization based on Hensel lifting, *Appl. Alg. Eng. Comm. Comp.* 21 (2010) 151–176. <378, 386>

[1879] C. Lee and C. Chang, Low-complexity linear array multiplier for normal basis of type-II, In *Proc. IEEE International Conf. Multimedia and Expo*, 1515–1518, 2004. <813, 815>

[1880] C. Lee and C. W. Chiou, Scalable Gaussian normal basis multipliers over $GF(2^m)$ using Hankel matrix-vector representation, *Journal of Signal Processing Systems* 69 (2012) 197–211. <814, 815>

[1881] D. B. Leep and C. C. Yeomans, The number of points on a singular curve over a finite field, *Arch. Math. (Basel)* 63 (1994) 420–426. <231, 233>

[1882] A. M. Legendre, Recherches d'analyse indeterminee, *Memoires Acad. Sci. Paris* (1785) 465–559. <175, 179>

[1883] D. H. Lehmer, Euclid's Algorithm for Large Numbers, *Amer. Math. Monthly* 45 (1938) 227–233. <353, 357>

[1884] A. Lempel and H. Greenberger, Families of sequences with optimal Hamming correlation properties, *IEEE Trans. Information Theory* IT-20 (1974) 90–94. <836, 837, 840>

[1885] A. Lempel and M. J. Weinberger, Self-complementary normal bases in finite fields, *SIAM J. Discrete Math.* 1 (1988) 193–198. <108, 110>

[1886] D. Lenskoi, On the arithmetic of polynomials over a finite field (Russian), *Volz. Mat. Sb.* 4 (1966) 155–159. <487, 493>

[1887] A. K. Lenstra, Factorization of polynomials, In *Computational Methods in Number Theory, Part I*, volume 154 of *Math. Centre Tracts*, 169–198, Math. Centrum, Amsterdam, 1982. <398>

[1888] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász, Factoring polynomials with rational coefficients, *Math. Ann.* 261 (1982) 515–534. <381, 386>

[1889] A. K. Lenstra and E. R. Verheul, Selecting cryptographic key sizes, In H. Imai and Y. Zheng, editors, *Public Key Cryptography—Third International Workshop on Practice and Theory in Public Key Cryptosystems PKC 2000*, volume 1751 of *Lecture Notes in Comput. Sci.*, 446–465, Springer-Verlag, Berlin, 2000. <776, 788>

[1890] H. W. Lenstra, Finding isomorphisms between finite fields, *Math. Comp.* 56 (1991) 329–347. <341, 357, 395, 398>

[1891] H. W. Lenstra, Jr., A normal basis theorem for infinite Galois extensions, *Nederl. Akad. Wetensch. Indag. Math.* 47 (1985) 221–228. <124, 132>

[1892] H. W. Lenstra, Jr., Finding small degree factors of lacunary polynomials, In K. Győry, H. Iwaniec, and J. Urbanowicz, editors, *Number Theory in Progress: Proc. Internat. Conf. Number Theory*, 267–276, Berlin, 1999, de Gruyter. <384, 386>

[1893] H. W. Lenstra, Jr., Exceptional covers, October 1999, MSRI lecture, available at `http://www.msri.org/realvideo/ln/msri/1999/cgt/lenstra/1/index.html`. Accessed April 12, 2012. <231, 233>

[1894] H. W. Lenstra, Jr. and R. J. Schoof, Primitive normal bases for finite fields, *Math. Comp.* 48 (1987) 217–231. <88, 90, 109, 110, 130, 132>

[1895] H. W. Lenstra, Jr. and M. Zieve, A family of exceptional polynomials in characteristic three, In *Finite Fields and Applications*, volume 233 of *London Math. Soc. Lecture Note Ser.*, 209–218, Cambridge Univ. Press, Cambridge, 1996. <233>

[1896] J. S. Leon, J. M. Masley, and V. Pless, Duadic codes, *IEEE Trans. Inform. Theory* 30 (1984) 709–714. <674, 695>

[1897] M. Leone, A new low complexity parallel multiplier for a class of finite fields, In *Proc. Cryptographic Hardware and Embedded Systems (CHES)*, volume 2162 of *Lecture Notes Comput. Sci.*, 160–170. Springer, 2001. <813, 815>

[1898] R. Lercier, *Algorithmique des Courbes Elliptiques dans les Corps Finis*, PhD thesis, École Polytechnique, 1997, In French, available at `http://perso.univ-rennes1.fr/reynald.lercier/file/Ler97a.pdf`. <353, 357>

[1899] R. Lercier and D. Lubicz, Counting points on elliptic curves over finite fields of small characteristic in quasi quadratic time, In E. Biham, editor, *Advances in Cryptology—EUROCRYPT 2003*, volume 2656 of *Lecture Notes in Comput.*

Sci., 360–373, Springer-Verlag, Berlin, 2003. <780, 788>

[1900] R. Lercier and D. Lubicz, A quasi quadratic time algorithm for hyperelliptic curve point counting, *Ramanujan J.* 12 (2006) 399–423. <448, 450, 485>

[1901] C. Leroux, I. Tal, A. Vardy, and W. J. Gross, Hardware architectures for successive cancellation decoding of polar codes, In *2011 IEEE International Conference on Acoustics, Speech and Signal Processing—ICASSP*, 1665–1668, 2011. <731>

[1902] K. H. Leung, S. L. Ma, and B. Schmidt, Nonexistence of abelian difference sets: Lander's conjecture for prime power orders, *Trans. Amer. Math. Soc.* 356 (2004) 4343–4358. <595, 599>

[1903] K. H. Leung, S. L. Ma, and B. Schmidt, New Hadamard matrices of order $4p^2$ obtained from Jacobi sums of order 16, *J. Combin. Theory, Ser. A* 113 (2006) 822–838. <143, 155>

[1904] K. H. Leung, S. L. Ma, and B. Schmidt, On Lander's conjecture for difference sets whose order is a power of 2 or 3, *Des. Codes Cryptogr.* 56 (2010) 79–84. <595, 599>

[1905] K. H. Leung and B. Schmidt, The field descent method, *Des. Codes Cryptogr.* 36 (2005) 171–188. <596, 599>

[1906] V. Levenshtein, Application of Hadamard matrices to a problem of coding theorey, *Problemy Kibernetiki* 5 (1961) 123–136. <164, 179>

[1907] A. Levin, *Difference Algebra*, volume 8 of *Algebra and Applications*, Springer, New York, 2008. <231, 233>

[1908] A. B. Levin, Difference algebra, In *Handbook of Algebra*, volume 4, 241–334, Elsevier/North-Holland, Amsterdam, 2006. <231, 233>

[1909] F. Levy-dit Vehel and L. Perret, Polynomial equivalence problems and applications to multivariate cryptosystems, In *Progress in Cryptology—INDOCRYPT 2003*, volume 2904 of *Lecture Notes in Comput. Sci.*, 235–251, Springer, Berlin, 2003. <759, 775>

[1910] H. Li and H. J. Zhu, Zeta functions of totally ramified p-covers of the projective line, *Rend. Sem. Mat. Univ. Padova* 113 (2005) 203–225. <479, 481>

[1911] J. Li, D. B. Chandler, and Q. Xiang, Permutation polynomials of degree 6 or 7 over finite fields of characteristic 2, *Finite Fields Appl.* 16 (2010) 406–419. <209, 223>

[1912] J. Li and D. Wan, On the subset sum problem over finite fields, *Finite Fields Appl.* 14 (2008) 911–929. <207>

[1913] J. Li and D. Wan, Counting subset sums of finite abelian groups, *J. Combin. Theory, Ser. A* 119 (2012) 170–182. <207>

[1914] K.-Z. Li and F. Oort, *Moduli of Supersingular Abelian Varieties*, volume 1680 of *Lecture Notes in Mathematics*, Springer-Verlag, Berlin, 1998. <480, 481>

[1915] L. Li and O. Roche-Newton, An improved sum-product estimate for general finite fields, *SIAM J. Discrete Math.* 25 (2011) 1285–1296. <182>

[1916] W.-C. Li, Character sums and abelian Ramanujan graphs, *J. Number Theory* 41 (1992) 199–217. <642, 650>

[1917] W.-C. Li, *Number Theory with Applications*, volume 7 of *Series on University Mathematics*, World Scientific Publishing Co. Inc., River Edge, NJ, 1996. <29, 30, 635, 642, 643, 650>

[1918] W.-C. Li, On negative eigenvalues of regular graphs, *C. R. Acad. Sci. Paris, Sér. I, Math.* 333 (2001) 907–912. <639, 650>

[1919] W.-C. Li, Recent developments in automorphic forms and applications, In *Number Theory for the Millennium II*, 331–354, A. K. Peters, Natick, MA, 2002. <635, 650>

[1920] W.-C. Li, Ramanujan hypergraphs, *Geom. Funct. Anal.* 14 (2004) 380–399. <640, 650>

[1921] W.-C. Li, Zeta functions in combinatorics and number theory, In *Fourth International Congress of Chinese Mathematicians*, volume 48 of *AMS/IP Stud. Adv. Math.*, 351–366, Amer. Math. Soc., Providence, RI, 2010. <650>

[1922] W.-C. Li and P. Solé, Spectra of regular graphs and hypergraphs and orthogonal polynomials, *European J. Combin.* 17 (1996) 461–477. <640, 650>

[1923] Y. Li, S. Ling, H. Niederreiter, H. Wang, C. Xing, and S. Zhang, editors, *Coding and Cryptology*, volume 4 of *Series on Coding Theory and Cryptology*. World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2008. <30>

[1924] Y. Li and M. Wang, On EA-equivalence of certain permutations to power mappings, *Des. Codes Cryptogr.* 58 (2011) 259–269. <219, 223>

[1925] Q. Liao and K. Feng, On the complexity of the normal bases via prime Gauss period over finite fields, *J. Syst. Sci. Complex.* 22 (2009) 395–406. <118, 122>

[1926] Q. Liao and L. You, Low complexity of a class of normal bases over finite fields, *Finite Fields Appl.* 17 (2011) 1–14. <113, 122>

[1927] Y. S. Liaw, More Z-cyclic Room squares, *Ars Combin.* 52 (1999) 228–238. <608, 611>

[1928] R. Lidl and G. L. Mullen, When does a polynomial over a finite field permute the elements of the field?, *Amer. Math. Monthly* 95 (1988) 243–246. <209, 223>

[1929] R. Lidl and G. L. Mullen, Cycle structure of Dickson permutation polynomials, *Math. J. Okayama Univ.* 33 (1991) 1–11. <221, 223>

[1930] R. Lidl and G. L. Mullen, When does a polynomial over a finite field permute the elements of the field?, II, *Amer. Math. Monthly* 100 (1993) 71–74. <209, 210, 223>

[1931] R. Lidl, G. L. Mullen, and G. Turnwald, *Dickson Polynomials*, volume 65 of *Pitman Monographs and Surveys in Pure and Applied Mathematics*, Longman Scientific & Technical, Harlow, 1993. <29, 30, 223, 232, 233, 276, 282, 283, 287, 291, 296, 327, 330>

[1932] R. Lidl and H. Niederreiter, On orthogonal systems and permutation polynomials in several variables, *Acta Arith.* 22 (1972/73) 257–265. <224, 225>

[1933] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and Their Applications*, Cambridge University Press, Cambridge, revised edition, 1994. <11, 29, 30, 66, 69, 306, 311, 387, 394>

[1934] R. Lidl and H. Niederreiter, *Finite Fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*, Cambridge University Press, Cambridge, second edition, 1997. <2, 10, 11, 22, 25, 29, 30, 35, 46, 56, 57, 58, 61, 62, 66, 69, 82, 85, 165, 167, 169, 173, 177, 179, 196, 200, 201, 203, 207, 208, 209, 210, 221, 223, 225, 228, 229, 231, 233, 246, 255, 276, 280, 283, 312, 318, 319, 321, 330, 343, 357, 359, 368, 371, 374, 387, 388, 394, 503>

[1935] R. Lidl and C. Wells, Chebyshev polynomials in several variables, *J. Reine Angew. Math.* 255 (1972) 104–111. <224, 225>

[1936] C. H. Lim and P. J. Lee, More flexible exponentiation with precomputation, In *Advances in Cryptology—CRYPTO '94*, volume 839 of *Lecture Notes in Comput. Sci.*, 95–107, Springer, Berlin, 1994. <350, 357>

[2107] R. T. Moenck, On the efficiency of algorithms for polynomial factoring, *Mathematics of Computation* 31 (1977) 235–250. <375, 376>

[2108] T. Moh, A public key system with signature and master key functions, *Comm. Algebra* 27 (1999) 2207–2222. <766, 774, 775>

[2109] M. S. E. Mohamed, D. Cabarcas, J. Ding, J. Buchmann, and S. Bulygin, MXL_3: an efficient algorithm for computing Gröbner bases of zero-dimensional ideals, In *Information Security and Cryptology—ICISC 2009*, volume 5984 of *Lecture Notes in Comput. Sci.*, 87–100, Springer, Berlin, 2010. <773, 775>

[2110] M. S. E. Mohamed, J. Ding, J. Buchmann, and F. Werner, Algebraic attack on the MQQ public key cryptosystem, In *Eighth International Conference on Cryptology and Network Security*, volume 5888 of *Lecture Notes in Comput. Sci.*, 392–401, 2009. <767, 775>

[2111] M. S. E. Mohamed, W. S. A. E. Mohamed, J. Ding, and J. Buchmann, MXL2: Solving polynomial equations over GF(2) using an improved mutant strategy, In J. Buchmann and J. Ding, editors, *PQCrypto*, volume 5299 of *Lecture Notes in Comput. Sci.*, 203–215. Springer, 2008. <773, 775>

[2112] B. Mohar, Isoperimetric numbers of graphs, *J. Combin. Theory, Ser. B* 47 (1989) 274–291. <641, 650>

[2113] B. Mohar, A strengthening and a multipartite generalization of the Alon-Boppana-Serre theorem, *Proc. Amer. Math. Soc.* 138 (2010) 3899–3909. <639, 640, 650>

[2114] M. Moisio, The moments of a Kloosterman sum and the weight distribution of a Zetterberg-type binary cyclic code, *IEEE Trans. Inform. Theory* 53 (2007) 843–847. <151, 155>

[2115] M. Moisio, On the number of rational points on some families of Fermat curves over finite fields, *Finite Fields Appl.* 13 (2007) 546–562. <202, 207>

[2116] M. Moisio, Kloosterman sums, elliptic curves, and irreducible polynomials with prescribed trace and norm, *Acta Arith.* 132 (2008) 329–350. <71, 75, 263, 266>

[2117] M. Moisio, On the moments of Kloosterman sums and fibre products of Kloosterman curves, *Finite Fields Appl.* 14 (2008) 515–531. <151, 155>

[2118] M. Moisio and K. Ranto, Elliptic curves and explicit enumeration of irreducible polynomials with two coefficients prescribed, *Finite Fields Appl.* 14 (2008) 798–815. <75>

[2119] M. Moisio, K. Ranto, M. Rinta-Aho, and K. Väänänen, On the weight distribution of cyclic codes with one or two zeros, *Adv. Appl. Discrete Math.* 3 (2009) 125–150. <148, 155>

[2120] M. Moisio and D. Wan, On Katz's bound for the number of elements with given trace and norm, *J. Reine Angew. Math.* 638 (2010) 69–74. <190, 195>

[2121] F. Möller, Exceptional polynomials with 2-transitive affine monodromy groups, *Finite Fields Appl.* 18 (2012) 445–457. <231, 233>

[2122] R. A. Mollin and C. Small, On permutation polynomials over finite fields, *Internat. J. Math. Math. Sci.* 10 (1987) 535–543. <216, 223>

[2123] R. Moloney, *Divisibility Properties of Kloosterman Sums and Division Polynomials for Edwards Curves*, PhD dissertation, University College Dublin, College of Engineering, Mathematical and Physical Sciences, 2011. <148, 155>

[2124] M. Monagan and R. Pearce, Polynomial division using dynamic arrays, heaps, and packed exponent vectors, In *Proc. of CASC 2007*, 295–315. Springer-Verlag,

[2181] G. L. Mullen and I. E. Shparlinski, Open problems and conjectures in finite fields, In *Finite Fields and Applications*, volume 233 of *London Math. Soc. Lecture Note Ser.*, 243–268, Cambridge Univ. Press, Cambridge, 1996. <68, 69, 83, 84, 85, 91, 93>

[2182] G. L. Mullen, H. Stichtenoth, and H. Tapia-Recillas, editors, *Finite Fields with Applications to Coding Theory, Cryptography and Related Areas*, Springer-Verlag, Berlin, 2002. <30>

[2183] G. L. Mullen, D. Wan, and Q. Wang, Value sets of polynomials maps over finite fields, Quarterly J. of Math., to appear, 2012. <225>

[2184] G. L. Mullen and D. White, A polynomial representation for logarithms in GF(q), *Acta Arith.* 47 (1986) 255–261. <390, 394>

[2185] P. Müller, New examples of exceptional polynomials, In *Finite Fields: Theory, Applications, and Algorithms*, volume 168 of *Contemp. Math.*, 245–249, Amer. Math. Soc., Providence, RI, 1994. <233>

[2186] P. Müller, Primitive monodromy groups of polynomials, In *Recent Developments in the Inverse Galois Problem*, volume 186 of *Contemp. Math.*, 385–401, Amer. Math. Soc., Providence, RI, 1995. <294, 296>

[2187] P. Müller, A Weil-bound free proof of Schur's conjecture, *Finite Fields Appl.* 3 (1997) 25–32. <221, 223, 230, 232, 233>

[2188] P. Müller, Arithmetically exceptional functions and elliptic curves, In *Aspects of Galois Theory*, volume 256 of *London Math. Soc. Lecture Note Ser.*, 180–201, Cambridge Univ. Press, Cambridge, 1999. <232, 233>

[2189] S. Müller, On the computation of square roots in finite fields, *Des. Codes Cryptogr.* 31 (2004) 301–312. <354, 357>

[2190] V. Müller, Fast multiplication on elliptic curves over small fields of characteristic two, *Journal of Cryptology* 11 (1998) 219–234. <793, 795>

[2191] R. Mullin, I. Onyszchuk, S. Vanstone, and R. Wilson, Optimal normal bases in $GF(p^n)$, *Discrete Appl. Math.* 22 (1988/89) 149–161. <810, 811, 815>

[2192] R. C. Mullin and G. L. Mullen, editors, *Finite Fields: Theory, Applications, and Algorithms*, volume 225 of *Contemporary Mathematics*, American Mathematical Society, Providence, RI, 1999. <30>

[2193] R. C. Mullin and E. Nemeth, An existence theorem for room squares, *Canad. Math. Bull.* 12 (1969) 493–497. <606, 611>

[2194] R. C. Mullin, I. M. Onyszchuk, S. A. Vanstone, and R. M. Wilson, Optimal normal bases in GF(p^n), *Discrete Appl. Math.* 22 (1988/89) 149–161. <111, 122>

[2195] R. C. Mullin, J. L. Yucas, and G. L. Mullen, A generalized counting and factoring method for polynomials over finite fields, *J. Combin. Math. Combin. Comput.* 72 (2010) 121–143. <53, 54, 55>

[2196] D. Mumford, An algebro-geometric construction of commuting operators and of solutions to the Toda lattice equation, Korteweg deVries equation and related nonlinear equation, In *Proceedings of the International Symposium on Algebraic Geometry*, 115–153, Kinokuniya Book Store, Tokyo, 1978. <538, 539>

[2197] D. Mumford, *Algebraic Geometry. I,* Classics in Mathematics. Springer-Verlag, Berlin, 1995. <380, 386>

[2198] D. Mumford, *The Red Book of Varieties and Schemes*, volume 1358 of *Lecture Notes in Mathematics*, Springer-Verlag, Berlin, expanded edition, 1999. <284, 285, 290, 291, 296>

[2199] A. Munemasa, Orthogonal arrays, primitive trinomials, and shift-register sequences,

<333, 335, 336, 338>

[2328] A. Ostafe and I. E. Shparlinski, On the Waring problem with Dickson polynomials in finite fields, *Proc. Amer. Math. Soc.* 139 (2011) 3815–3820. <186, 207>

[2329] A. Ostafe and I. E. Shparlinski, Degree growth, linear independence and periods of a class of rational dynamical systems, In *Proc. Conf. on Arithmetic, Geometry, Cryptography and Coding Theory*, volume 574 of *Contemp. Math.*, 131–144, Amer. Math. Soc., Providence, RI, 2012. <333, 335, 336, 338>

[2330] A. Ostafe and I. E. Shparlinski, On the power generator and its multivariate analogue, *J. Complexity* 28 (2012) 238–249. <333, 334, 338>

[2331] A. Ostafe, I. E. Shparlinski, and A. Winterhof, On the generalized joint linear complexity profile of a class of nonlinear pseudorandom multisequences, *Adv. Math. Commun.* 4 (2010) 369–379. <335, 336, 338>

[2332] A. Ostafe, I. E. Shparlinski, and A. Winterhof, Multiplicative character sums of a class of nonlinear recurrence vector sequences, *Int. J. Number Theory* 7 (2011) 1557–1571. <335, 336, 338>

[2333] A. M. Ostrowski, Über die Bedeutung der Theorie der konvexen Polyeder für die formale Algebra, *Jahresber. Deutsch. Math.-Verein.* 30 (1921) 98–99. <382, 386, 965>

[2334] A. M. Ostrowski, On the significance of the theory of convex polyhedra for formal algebra, *ACM SIGSAM Bull.* 33 (1999) 5, Translated from [2333]. <382, 386>

[2335] P. Oswald and A. Shokrollahi, Capacity-achieving sequences for the erasure channel, *IEEE Trans. Inform. Theory* 48 (2002) 3017–3028. <721, 726>

[2336] F. Özbudak, On maximal curves and linearized permutation polynomials over finite fields, *J. Pure Appl. Algebra* 162 (2001) 87–102. <232, 233>

[2337] C. Paar, A new architecture for a parallel finite field multiplier with low complexity based on composite fields, *IEEE Trans. Comput.* 45 (1996) 856–861. <805, 806, 815>

[2338] L. J. Paige, Neofields, *Duke Math. J.* 16 (1949) 39–60. <26, 30>

[2339] R. Paley, On orthogonal matrices., *J. Math. Phys., Mass. Inst. Techn.* 12 (1933) 311–320. <164, 179>

[2340] R. E. A. C. Paley, On orthogonal matrices, *J. Math. Phys* 12 (1933) 311–320. <601, 611>

[2341] V. Y. Pan, *Structured Matrices and Polynomials: Unified Superfast Algorithms*, Birkhäuser Boston Inc., Boston, MA, 2001. <526, 528>

[2342] D. Panario, What do random polynomials over finite fields look like?, In *Finite Fields and Applications*, volume 2948 of *Lecture Notes in Comput. Sci.*, 89–108, Springer, Berlin, 2004. <359, 368>

[2343] D. Panario, X. Gourdon, and P. Flajolet, An analytic approach to smooth polynomials over finite fields, In *Algorithmic Number Theory*, volume 1423 of *Lecture Notes in Comput. Sci.*, 226–236, Springer, Berlin, 1998. <393, 394>

[2344] D. Panario, B. Pittel, B. Richmond, and A. Viola, Analysis of Rabin's irreducibility test for polynomials over finite fields, *Random Structures Algorithms* 19 (2001) 525–551. <363, 368, 370, 374>

[2345] D. Panario and B. Richmond, Analysis of Ben-Or's polynomial irreducibility test, *Random Structures Algorithms* 13 (1998) 439–456. <363, 368, 371, 374>

[2346] D. Panario and B. Richmond, Exact largest and smallest size of components, *Algorithmica* 31 (2001) 413–432. <365, 367, 368>

lem in finite fields, In *Algorithmic Number Theory: Lattices, Number Fields, Curves and Cryptography*, volume 44 of *Math. Sci. Res. Inst. Publ.*, 397–420, Cambridge Univ. Press, Cambridge, 2008. <393, 394>

[2540] O. Schirokauer, The number field sieve for integers of low weight, *Math. Comp.* 79 (2010) 583–602. <393, 394>

[2541] B. Schmidt, *Characters and Cyclotomic Fields in Finite Geometry*, volume 1797 of *Lecture Notes in Mathematics*, Springer-Verlag, Berlin, 2002. <592, 593, 599>

[2542] K. Schmidt, *Dynamical Systems of Algebraic Origin*, volume 128 of *Progress in Mathematics*, Birkhäuser Verlag, Basel, 1995. <331, 338>

[2543] W. M. Schmidt, *Equations over Finite Fields. An Elementary Approach*, Lecture Notes in Mathematics, Vol. 536. Springer-Verlag, Berlin, 1976. <29, 30, 170, 179, 187, 188, 193, 195>

[2544] W. M. Schmidt, Construction and estimation of bases in function fields, *J. Number Theory* 39 (1991) 181–224. <324, 331>

[2545] T. Schoen and I. Shkredov, Additive properties of multiplicative subgroups of $\mathbb{F}_p$, *Quart. J. Math.* 63 (2012) 713–822. <206, 207>

[2546] J. Scholten and H. J. Zhu, Families of supersingular curves in characteristic 2, *Math. Res. Lett.* 9 (2002) 639–650. <481>

[2547] J. Scholten and H. J. Zhu, Hyperelliptic curves in characteristic 2, *Int. Math. Res. Not.* (2002) 905–917. <478, 481, 791, 795>

[2548] J. Scholten and H. J. Zhu, Slope estimates of Artin-Schreier curves, *Compositio Math.* 137 (2003) 275–292. <478, 481>

[2549] R. A. Scholtz, The spread spectrum concept, *IEEE Trans. Commun.* COM-25 (1977) 748–755. <833, 836, 840>

[2550] R. A. Scholtz and L. R. Welch, GMW sequences, *IEEE Trans. Inform. Theory* 30 (1984) 548–553. <312, 318>

[2551] T. Schönemann, Grundzüge einer allgemeinen theorie der höheren congruenzen, deren modul eine reele primzahl ist, *J. Reine Agnew. Math.* 31 (1845) 269–325. <8, 10>

[2552] A. Schönhage, Schnelle berechnung von kettenbruchentwicklungen, *Acta Inf.* 1 (1971) 139–144. <353, 357>

[2553] A. Schönhage, Schnelle Multiplikation von Polynomen über Körpern der Charakteristik 2, *Acta Informatica* 7 (1977) 395–398. <376>

[2554] A. Schönhage and V. Strassen, Schnelle Multiplikation grosser Zahlen, *Computing (Arch. Elektron. Rechnen)* 7 (1971) 281–292. <349, 352, 357, 376>

[2555] R. Schoof, Elliptic curves over finite fields and the computation of square roots mod p, *Math. Comp.* 44 (1985) 483–494. <484, 485, 779, 788>

[2556] R. Schoof, Algebraic curves over $\mathbf{F}_2$ with many rational points, *J. Number Theory* 41 (1992) 6–14. <458, 463>

[2557] B. Schumacher and M. D. Westmoreland, Modal quantum theory, In *QPL 2010, 7th Workshop on Quantum Physics and Logic*, 145–149, 2010. <831, 832>

[2558] I. Schur, Über den Zusammenhang zwischen einem Problem der Zahlentheorie und einem Satz über algebraische Funktionen, *S.-B. Preuss. Akad. Wiss. Phys.-Math. Klasse* (1923) 123–134. <232, 233>

[2559] I. Schur, Zur theorie der einfach transitiven permutationgruppen, *S.-B. Preuss. Akad. Wiss. Phys.-Math. Klasse* (1933) 598–623. <232, 233>

[2560] R. Schürer, A new lower bound on the t-parameter of (t, s)-sequences, In *Monte*

[2777] T. Tao, *Structure and Randomness*, American Mathematical Society, Providence, RI, 2008. <304>

[2778] T. Tao and V. Vu, *Additive Combinatorics*, volume 105 of *Cambridge Studies in Advanced Mathematics*, Cambridge University Press, Cambridge, 2006. <29, 30, 182, 186>

[2779] V. Tarokh, N. Seshadri, and A. R. Calderbank, Space-time codes for high data rate wireless communication: performance criterion and code construction, *IEEE Trans. Inform. Theory* 44 (1998) 744–765. <838, 840>

[2780] J. Tate, Endomorphisms of abelian varieties over finite fields, *Invent. Math.* 2 (1966) 134–144. <425, 427, 434, 453, 457, 798, 803>

[2781] J. Tate, The arithmetic of elliptic curves, *Invent. Math.* 23 (1974) 179–206. <417, 434>

[2782] W. Tautz, J. Top, and A. Verberkmoes, Explicit hyperelliptic curves with real multiplication and permutation polynomials, *Canad. J. Math.* 43 (1991) 1055–1064. <232, 233>

[2783] D. E. Taylor, *The Geometry of the Classical Groups*, volume 9 of *Sigma Series in Pure Mathematics*, Heldermann Verlag, Berlin, 1992. <506, 507, 508, 511, 513, 514>

[2784] A. F. Tenca and Ç. K. Koç, A scalable architecture for Montgomery multiplication, In *Proc. Cryptographic Hardware and Embedded Systems (CHES)*, volume 1717 of *Lecture Notes Comput. Sci.*, 94–108, Springer, Berlin, 1999. <814, 815>

[2785] G. Tenenbaum, *Introduction to Analytic and Probabilistic Number Theory*, volume 46 of *Cambridge Studies in Advanced Mathematics*, Cambridge University Press, Cambridge, 1995. <363, 364, 368>

[2786] A. Terras, *Fourier Analysis on Finite Groups and Applications*, volume 43 of *London Mathematical Society Student Texts*, Cambridge University Press, Cambridge, 1999. <299, 301, 302, 304, 636, 650>

[2787] E. Teske, Square-root algorithms for the discrete logarithm problem (a survey), In *Public-Key Cryptography and Computational Number Theory*, 283–301, de Gruyter, Berlin, 2001. <391, 394>

[2788] F. Thaine, On Gaussian periods that are rational integers, *Michigan Math. J.* 50 (2002) 313–337. <135, 155>

[2789] D. Thakur, Multizeta in function field arithmetic, In *Proceedings of Banff Workshop*, European Mathematical Society (EMS), Zürich. <536, 537, 539>

[2790] D. S. Thakur, *Function Field Arithmetic*, World Scientific Publishing Co. Inc., River Edge, NJ, 2004. <29, 30, 529, 539>

[2791] J. A. Thas, Normal rational curves and k-arcs in Galois spaces, *Rend. Mat. (6)* 1 (1968) 331–334. <578, 581>

[2792] J. A. Thas, The affine plane $\mathrm{AG}(2, q)$, q odd, has a unique one point extension, *Invent. Math.* 118 (1994) 133–139. <581>

[2793] "The GAP Group", GAP system for computational discrete algebra, `http://www.gap-system.org`, as viewed in July, 2012. <45, 46>

[2794] "The GNU Project", The GNU MP Bignum library, `http://www.gmplib.org/`, as viewed in July, 2012. <30, 45, 46>

[2795] The Magma computational algebra system for algebra, number theory and geometry, version 2.18-3, 2012. <340, 357, 773, 775>

[2796] "The Mathworks Inc.", MATLAB - The Language of Technical Computing, `http://www.mathworks.com/products/matlab/`, as viewed in July 2012. <45, 46>

volume 139 of *Mathematical Surveys and Monographs*, American Mathematical Society, Providence, RI, 2007. <29, 30>

[2817] M. A. Tsfasman and S. G. Vlăduţ, *Algebraic-Geometric Codes*, volume 58 of *Mathematics and its Applications (Soviet Series)*, Kluwer Academic Publishers Group, Dordrecht, 1991. <29, 30, 702, 704>

[2818] M. A. Tsfasman, S. G. Vlăduţ, and T. Zink, Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound, *Math. Nachr.* 109 (1982) 21–28. <457, 458, 463, 703, 704>

[2819] S. Tsujii, A. Fujioka, and T. Itoh, Generalization of the public key cryptosystem based on the difficulty of solving a system of non-linear equations, In *Proc. Tenth Symposium on Information Theory and Its Applications*, JA5–3, 1987. <756, 760, 775>

[2820] S. Tsujii, K. Kurosawa, T. Itoh, A. Fujioka, and T. Matsumoto, A public key cryptosystem based on the difficulty of solving a system of nonlinear equations, *ICICE Transactions (D) J69-D* 12 (1986) 1963–1970. <756, 760, 775>

[2821] W. J. Turner, *Black Box Linear Algebra with the Linbox Library*, PhD thesis, 2002. <524, 528>

[2822] G. Turnwald, Permutation polynomials of binomial type, In *Contributions to General Algebra, 6*, 281–286, Hölder-Pichler-Tempsky, Vienna, 1988. <211, 216, 223>

[2823] G. Turnwald, A new criterion for permutation polynomials, *Finite Fields Appl.* 1 (1995) 64–82. <210, 221, 223, 226, 228, 229>

[2824] G. Turnwald, On Schur's conjecture, *J. Austral. Math. Soc., Ser. A* 58 (1995) 312–357. <221, 223, 232, 233>

[2825] R. Turyn and J. Storer, On binary sequences, *Proc. Amer. Math. Soc.* 12 (1961) 394–399. <317, 318>

[2826] R. J. Turyn, The linear generation of Legendre sequence, *J. Soc. Indust. Appl. Math.* 12 (1964) 115–116. <327, 331>

[2827] R. J. Turyn, Character sums and difference sets, *Pacific J. Math.* 15 (1965) 319–346. <597, 598, 599>

[2828] R. J. Turyn, An infinite class of Williamson matrices, *J. Combin. Theory, Ser. A* 12 (1972) 319–321. <602, 611>

[2829] R. J. Turyn, Hadamard matrices, Baumert-Hall units, four-symbol sequences, pulse compression, and surface wave encodings, *J. Combin. Theory, Ser. A* 16 (1974) 313–333. <834, 840>

[2830] S. Uchiyama, Note on the mean value of $V(f)$. II, *Proc. Japan Acad.* 31 (1955) 321–323. <362, 368>

[2831] S. Uchiyama, Sur les polynômes irréductibles dans un corps fini. II, *Proc. Japan Acad.* 31 (1955) 267–269. <69, 75>

[2832] D. Ulmer, Jacobi sums, Fermat Jacobians, and ranks of abelian varieties over towers of function fields, *Math. Res. Lett.* 14 (2007) 453–467, `http://people.math.gatech.edu/~ulmer/research/papers/2007c-correction.pdf`. <140, 155>

[2833] C. Umans, Fast polynomial factorization and modular composition in small characteristic, In *STOC'08*, 481–490, ACM, New York, 2008. <352, 357>

[2834] A. Valette, Graphes de Ramanujan et applications, *Astérisque* (1997) Exp. No. 829, 4, 247–276, Séminaire Bourbaki, Vol. 1996/97. <635, 650>

[2835] E. R. van Dam and D. Fon-Der-Flaass, Codes, graphs, and schemes from nonlinear functions, *European J. Combin.* 24 (2003) 85–98. <252, 253, 255>

<178, 179>

[2994] E. Witt, Über steinersche systeme, *Abh. Math. Sem. Univ. Hamburg* 12 (1938) 265–275. <581>

[2995] C. Wolf, A. Braeken, and B. Preneel, Efficient cryptanalysis of RSE(2)PKC and RSSE(2)PKC, In *2004*, volume 3352 of *Lecture Notes in Computer Science*, 294–309, Sept. 8–10 2004, Extended version: `http://eprint.iacr.org/2004/237`. <763, 775>

[2996] J. K. Wolf, Adding two information symbols to certain nonbinary BCH codes and some applications, *Bell System Tech. J.* 48 (1969) 2405–2424. <673, 695>

[2997] J. Wolfmann, Formes quadratiques et codes à deux poids, *C. R. Acad. Sci. Paris, Sér. A-B* 281 (1975) Aii, A533–A535. <199, 200>

[2998] J. Wolfmann, The number of solutions of certain diagonal equations over finite fields, *J. Number Theory* 42 (1992) 247–257. <202, 207>

[2999] J. Wolfmann, New results on diagonal equations over finite fields from cyclic codes, In *Finite Fields: Theory, Applications, and Algorithms*, volume 168 of *Contemp. Math.*, 387–395, Amer. Math. Soc., Providence, RI, 1994. <207>

[3000] J. Wolfmann, Some systems of diagonal equations over finite fields, *Finite Fields Appl.* 4 (1998) 29–37. <207>

[3001] "Wolfram Research", Wolfram Research: Mathematica, technical and scientific software, `http://www.wolfram.com/`, as viewed in July, 2012. <45, 46>

[3002] W. K. Wootters and B. D. Fields, Optimal state-determination by mutually unbiased measurements, *Ann. Physics* 191 (1989) 363–381. <826, 832>

[3003] H. Wu, Low complexity bit-parallel finite field arithmetic using polynomial basis, In *Proc. Cryptographic Hardware and Embedded Systems (CHES)*, volume 1717 of *Lecture Notes Comput. Sci.*, 280–291, Springer, Berlin, 1999. <806, 815>

[3004] H. Wu, Bit-parallel finite field multiplier and squarer using polynomial basis, *IEEE Trans. Comput.* 51 (2002) 750–758. <807, 815>

[3005] H. Wu, M. A. Hasan, and I. F. Blake, New low-complexity bit-parallel finite field multipliers using weakly dual bases, *IEEE Trans. Comput.* 47 (1998) 1223–1234. <814, 815>

[3006] H. Wu, M. A. Hasan, I. F. Blake, and S. Gao, Finite field multiplier using redundant representation, *IEEE Trans. Comput.* 51 (2002) 1306–1316. <345, 357, 814, 815>

[3007] M. Wu, X. Yang, and C. Chan, A dynamic analysis of irs-pkr signaling in liver cells: A discrete modeling approach, *PLoS ONE* 4 (2009) e8040. <816, 825>

[3008] P.-C. Wu, Random number generation with primitive pentanomials, *ACM Trans. Modeling and Computer Simulation* 11 (2001) 346–351. <91, 92, 93>

[3009] Q. Xiang, Maximally nonlinear functions and bent functions, *Des. Codes Cryptogr.* 17 (1999) 211–218. <232, 233>

[3010] G. Xiao and S. Wei, Fast algorithms for determining the linear complexity of period sequences., In *Progress in Cryptology—INDOCRYPT 2002*, volume 2551 of *Lecture Notes in Comput. Sci.*, 12–21, Springer, Berlin, 2002. <323, 331>

[3011] G. Xiao, S. Wei, K. Y. Lam, and K. Imamura, A fast algorithm for determining the linear complexity of a sequence with period p^n over GF(q), *IEEE Trans. Inform. Theory* 46 (2000) 2203–2206. <323, 331>

[3012] G. Z. Xiao and J. L. Massey, A spectral characterization of correlation-immune combining functions, *IEEE Trans. Inform. Theory* 34 (1988) 569–571. <240, 245>

semifields, *Finite Fields Appl.* 15 (2009) 125–133. <275>

[3054] Z. Zha and X. Wang, New families of perfect nonlinear polynomial functions, *J. Algebra* 322 (2009) 3912–3918. <275>

[3055] L. Zhang, Q. Huang, S. Lin, K. Abdel-Ghaffar, and I. Blake, Quasi-cyclic LDPC codes: an algebraic construction, rank analysis, and codes on Latin squares, *IEEE Trans. Communications* 58 (2010) 3126–3139. <710, 711>

[3056] Q. Zhang, Polynomial functions and permutation polynomials over some finite commutative rings, *J. Number Theory* 105 (2004) 192–202. <222, 223, 225>

[3057] Z. Zhao and X. Cao, A note on the reducibility of binary affine polynomials, *Des. Codes Cryptogr.* 57 (2010) 83–90. <65, 66>

[3058] G. Zhou and H. Michalik, Comments on 'A new architecture for a parallel finite field multiplier with low complexity based on composite field', *IEEE Trans. Comput.* 59 (2010) 1007–1008. <805, 806, 815>

[3059] K. Zhou, A remark on linear permutation polynomials, *Finite Fields Appl.* 14 (2008) 532–536. <209, 223>

[3060] G. Zhu and D. Wan, An asmptotic formula for counting subset sums over subgroups of finite fields, *Finite Fields Appl.* 18 (2012) 192–209. <207>

[3061] H. J. Zhu, p-adic variation of L functions of one variable exponential sums. I, *Amer. J. Math.* 125 (2003) 669–690. <478, 481>

[3062] H. J. Zhu, Asymptotic variation of L functions of one-variable exponential sums, *J. Reine Angew. Math.* 572 (2004) 219–233. <478, 481>

[3063] H. J. Zhu, L-functions of exponential sums over one-dimensional affinoids: Newton over Hodge, *Int. Math. Res. Not.* (2004) 1529–1550. <476, 478, 481>

[3064] N. Zierler, Linear recurring sequences, *J. Soc. Indust. Appl. Math.* 7 (1959) 31–48. <306, 311>

[3065] N. Zierler, Primitive trinomials whose degree is a Mersenne exponent, *Information and Control* 15 (1969) 67–69. <91, 93>

[3066] N. Zierler and W. H. Mills, Products of linear recurring sequences, *J. Algebra* 27 (1973) 147–157. <307, 311>

[3067] M. Zieve, Bivariate factorizations via Galois theory, with application to exceptional polynomials, *J. Algebra* 210 (1998) 670–689. <232, 233>

[3068] M. E. Zieve, On a theorem of Carlitz, arXiv:0810.2834, 2008. <231, 233>

[3069] M. E. Zieve, Some families of permutation polynomials over finite fields, *Int. J. Number Theory* 4 (2008) 851–857. <216, 217, 223>

[3070] M. E. Zieve, On some permutation polynomials over $\mathbb{F}_q$ of the form $x^r h(x^{(q-1)/d})$, *Proc. Amer. Math. Soc.* 137 (2009) 2209–2216. <214, 216, 223>

[3071] M. E. Zieve, Classes of permutation polynomials based on cyclotomy and an additive analogue, In *Additive Number Theory*, 355–361, Springer, 2010. <214, 217, 223>

[3072] P. Zimmermann, Avoiding adjustments in modular computations, 2012, preprint available at `http:www.loria.fr/~zimmerma/papers/norm.pdf`. <348, 357>

[3073] T. Zink, Degeneration of Shimura surfaces and a problem in coding theory, In *Fundamentals of Computation Theory*, volume 199 of *Lecture Notes in Comput. Sci.*, 503–511, Springer, Berlin, 1985. <457>

[3074] R. Zippel, Probabilistic algorithms for sparse polynomials, In *EUROSAM '79: Proceedings of the International Symposium on Symbolic and Algebraic Computation*, number 72 in Lecture Notes in Comput. Sci., 216–226. Springer-Verlag,