arbitrary subfields of the finite field. The results developed in this paper are used to construct additional complete sets of frequency squares, rectangles and hyperrectangles, and orthogonal arrays. Some of the theorems present a relationship between permutation polynomials of a finite field and field permutation functions, an implicit bound on the possible number of functions in an orthogonal field system, and results related to the generation of orthogonal field systems.

8.2.21 Remark For finite rings there are two concepts to distinguish: permutation polynomials (as above) and strong permutation polynomials. The latter are defined via the cardinality of the inverse image. Polynomials are *strong permutation polynomials* (or *strong orthogonal systems*) in n variables if they can be completed to an orthogonal system of n polynomials in n variables.

8.2.22 Theorem [1129] If R is a local ring whose maximal ideal has a minimal number m of generators, then for every $n > m$ there exists a permutation polynomial in n variables that is not a strong permutation polynomial.

8.2.23 Corollary [1129] Every permutation polynomial in any number of variables over a local ring R is strong if and only if R is a finite field.

8.2.24 Remark Wei and Zhang showed [2954] that if $n \leq m$ in the setting of Theorem 8.2.22, then every orthogonal system of k polynomials in n variables can be completed to an orthogonal system of n polynomials (and in particular, every permutation polynomial is strong).

See Also

§9.4	Considers κ-polynomials used for constructions of semifields.
§14.1	Discusses orthogonal latin squares and hypercubes.
[1934]	Section 7.5 discusses permutations and orthogonal systems in several variables.
[2183]	Considers bounds for value sets of polynomial vectors in several variables.
[2321]	Considers an application of permutation polynomials and orthogonal systems to pseudorandom number generation.
[3056]	Considers permutation polynomials over finite commutative rings.

References Cited: [539, 1129, 1932, 1934, 1935, 2027, 2167, 2169, 2222, 2223, 2224, 2321, 2733, 2954, 3056]

8.3 Value sets of polynomials

Gary L. Mullen, *The Pennsylvania State University*
Michael E. Zieve, *University of Michigan*

8.3.1 Definition For $f \in \mathbb{F}_q[x]$, the *value set of* f is the set $V_f = \{f(a) | a \in \mathbb{F}_q\}$; the cardinality of V_f is denoted by $\#V_f$.

8.3.2 Remark Every subset of $\mathbb{F}_q$ occurs as V_f for some $f \in \mathbb{F}_q[x]$ of degree at most $q-1$ (by the Lagrange Interpolation Formula); see Theorem 2.1.131.

8.3.1 Large value sets

8.3.3 Remark Any $f \in \mathbb{F}_q[x]$ satisfies $\#V_f \leq q$; equality occurs precisely when f is a permutation polynomial; see Section 8.1.

8.3.4 Theorem Suppose $f \in \mathbb{F}_q[x]$ of degree n is not a permutation polynomial. Then:

1. [2823, 2908, 2979] $\#V_f \leq q - \lceil (q-1)/n \rceil$.
2. [1083, 1363, 1364] If $\#V_f \neq (1-1/n)q$ and $n > 5$ then $\#V_f \leq (1-2/n)q + O_n(\sqrt{q})$.
3. [1363] If $\gcd(n, q) = 1$ then $\#V_f \leq (5/6)q + O_n(\sqrt{q})$.

8.3.5 Example [755] Let $q = r^k$ where r is a prime power and k is a positive integer. Then $f(x) := x^r + x^{r-1}$ satisfies $\#V_f = q - q/r$, and hence achieves equality in (1).

8.3.2 Small value sets

8.3.6 Remark If $f \in \mathbb{F}_q[x]$ has degree n, then $\#V_f \geq \lceil q/n \rceil$ (since each $\alpha \in \mathbb{F}_q$ has at most n preimages under f).

8.3.7 Definition A polynomial $f \in \mathbb{F}_q[x]$ of degree n is a *minimal value set polynomial* if $\#V_f = \lceil q/n \rceil$.

8.3.8 Theorem [546] Let $f \in \mathbb{F}_p[x]$ have degree n, where p is prime. If $n < p$ and $\#V_f = \lceil p/n \rceil \geq 3$, then n divides $p-1$ and $f(x) = a(x+b)^n + c$ with $a, b, c \in \mathbb{F}_p$.

8.3.9 Theorem [2100] Let $f \in \mathbb{F}_q[x]$ be monic of degree n, where $\gcd(n, q) = 1$ and $n \leq \sqrt{q}$. If $\#V_f = \lceil q/n \rceil$, then n divides $q-1$ and $f(x) = (x+b)^n + c$ with $b, c \in \mathbb{F}_q$.

8.3.10 Problem Determine all minimal value set polynomials over $\mathbb{F}_{p^k}$. This is done for $k \leq 2$ in [2100].

8.3.11 Remark Minimal value set polynomials whose values form a subfield are characterized in [350]. A connection between minimal value set polynomials and Frobenius non-classical curves is given in [349].

8.3.12 Theorem [623, 1308] If $f(x) \in \mathbb{F}_q[x]$ is monic of degree $n > 15$, where $n^4 < q$ and $\#V_f < 2q/n$, then $f(x)$ has one of the forms:

1. $(x+a)^n + b$, where $n \mid (q-1)$;
2. $((x+a)^{n/2} + b)^2 + c$, where $n \mid (q^2-1)$;
3. $((x+a)^2 + b)^{n/2} + c$, where $n \mid (q^2-1)$.

8.3.13 Theorem [288] Let $f \in \mathbb{F}_p[x]$ have degree less than $\frac{3}{4}(p-1)$, where p is prime. If $\#f(\mathbb{F}_p^*) = 2$ then f is a polynomial in $x^{(p-1)/d}$ for some $d \in \{2, 3\}$.

8.3.14 Remark This result indicates that some phenomena become apparent only when ones considers $\#f(\mathbb{F}_p^*)$ rather than $\#V_f$.

8.3.3 General polynomials

8.3.15 Theorem [284, 2978] Fix n, and let $e_n := \sum_{j=1}^{n}(-1)^{j-1}/j!$. There is a constant a_n such that, for each q, there are $q^n + O_n(q^{n-1})$ monic polynomials $f \in \mathbb{F}_q[x]$ of degree n satisfying $|\#V_f - e_n q| \leq a_n\sqrt{q}$.

8.3.16 Remark The previous result says that if q is large compared to n then most polynomials over $\mathbb{F}_q$ of degree n take approximately $e_n q$ values. Note that $e_n \to 1 - 1/e$ as $n \to \infty$.

8.3.17 Theorem [662] For fixed n, there is a finite set T_n of rational numbers such that: for any q, and any $f \in \mathbb{F}_q[x]$ of degree n, there is an element $c_f \in T_n$ such that $\#V_f = c_f q + O_n(\sqrt{q})$.

8.3.18 Remark The set T_n may be chosen to be $\{a/n!\colon (n-1)! \leq a \leq n!\}$.

8.3.19 Remark For fixed n, if q is large and $f \in \mathbb{F}_q[x]$ has degree n, then $\#V_f/q$ lies in a tiny interval around a member of a finite set; crucially, this finite set depends only on n, and not on q.

8.3.20 Theorem [662] Let $f \in \mathbb{F}_q[x]$ have degree n, and write $f = g(x^{p^j})$ where $j \geq 0$ and $g \in \mathbb{F}_q[x] \setminus \mathbb{F}_q[x^p]$; here p is the characteristic of $\mathbb{F}_q$. Let t be transcendental over $\mathbb{F}_q$, and let A and G be the Galois groups of $g(x) - t$ over $\mathbb{F}_q(t)$ and $\bar{\mathbb{F}}_q(t)$, respectively, where $\bar{\mathbb{F}}_q$ denotes an algebraic closure of $\mathbb{F}_q$. Then G is a normal subgroup of A, and A/G is cyclic. The quantity c_f in Theorem 8.3.17 may be taken to be the proportion of elements in a generating coset of A/G which fix at least one of the roots of $g(x) - t$.

8.3.21 Example Let $f \in \mathbb{F}_q[x]$ have degree n.

1. If $n = 2$ then $\#V_f \in \{q/2, (q+1)/2, q\}$.
2. If $n = 3$ then $\#V_f \in \{q/3, (q+2)/3, (2q-1)/3, 2q/3, (2q+1)/3, q\}$.
3. [2038] If $n = 4$ and q is an odd prime then $\#V_f$ is either $(q+3)/4$, $(q+1)/2$, $(3q+4+i)/8$ with $\pm i \in \{1, 3, 5\}$, or $5q/8 + O(\sqrt{q})$.

8.3.4 Lower bounds

8.3.22 Theorem [2916] If $\mu_q(f)$ is the smallest positive integer i so that $\sum_{a \in F_q}(f(a))^i \neq 0$, then $\#V_f \geq \mu_q(f) + 1$.

8.3.23 Remark Assume that for a polynomial f the degree n of f satisfies $n < q - 1$. Write $(f(x))^i = \sum_{j=0}^{q-1} a_{ij} \bmod (x^q - x)$. Let A_f be the matrix $A_f = (a_{ij}^{q-1})$, for $1 \leq i, j \leq q-1$ so that the (i,j)-th entry of A_f is 1 if the coefficient of x^j in $(f(x))^i \bmod (x^q - x)$ is nonzero. If f is not the zero polynomial, then A_f has at least one nonzero column. If the j-th column of A_f consists entirely of 0's or entirely of 1s, set $l_j = 0$. Otherwise, for a nonzero j-th column of A_f, arrange the entries in a circle and define l_j to be the maximum number of consecutive zeros appearing in this circular arrangement. Let L_f be the maximum of the values of l_j, where the maximum is taken over all of the $q-1$ columns of the matrix A_f.

8.3.24 Theorem [769] With notation as above, $|V_f| \geq L_f + 2$.

8.3.25 Remark [625] If f is a polynomial over $\mathbb{F}_q$ and A_f' is the matrix from Remark 8.3.23 without the $(q-1)$-st powers, i.e., the matrix $A_f' = (a_{ij})$, then $\#V_f = 1 + \operatorname{rank}(A_f')$.

8.3.26 Corollary Since $|V_f| \geq l_{q-1} + 2$, we have the result of Theorem 2.1 of [2916].

8.3.27 Remark The Hermite/Dickson criterion from Section 8.1 is essentially equivalent to the first $q-2$ consecutive elements of the last column of the matrix A_f being 0, with the last

element being 1. Thus f is a permutation polynomial if and only if $L_f = q - 2$.

8.3.28 Remark See [2823] for further inequalities.

8.3.5 Examples

8.3.29 Theorem $\#V_{x^n} = 1 + (q-1)/(n, q-1)$.

8.3.30 Definition The *Dickson polynomial* of degree n and parameter $a \in \mathbb{F}_q$ is defined by

$$D_n(x,a) = \sum_{i=0}^{\lfloor n/2 \rfloor} \frac{n}{n-i} \binom{n-i}{i} (-a)^i x^{n-2i}.$$

8.3.31 Remark See Section 9.6 for a discussion of Dickson polynomials over $\mathbb{F}_q$.

8.3.32 Theorem [623] Suppose q is odd with $2^r \mid\mid (q^2-1)$. Then for each $n \geq 1$, and each $a \in \mathbb{F}_q^*$,

$$\#V_{D_n(x,a)} = \frac{q-1}{2(n,q-1)} + \frac{q+1}{2(n,q+1)} + \alpha,$$

where $\alpha = 1$ if $2^{r-1} \mid\mid n$; $\alpha = 1/2$ if $2^t \mid\mid n$ and $1 \leq t \leq r-2$; $\alpha = 0$ otherwise. Here η denotes the quadratic character defined by $\eta(0) = 0$, $\eta(a) = 1$ if a is a square in $\mathbb{F}_q$ and $\eta(a) = -1$ if a is a nonsquare in $\mathbb{F}_q$.

8.3.33 Remark If $(n_1, q^2-1) = (n_2, q^2-1)$, then $\#V_{D_{n_1}(x,a)} = \#V_{D_{n_2}(x,a)}$.

8.3.34 Theorem [623] Suppose q is even. Then for each $n \geq 1$, and each $a \in \mathbb{F}_q^*$,

$$\#V_{D_n(x,a)} = \frac{q-1}{2(n,q-1)} + \frac{q+1}{2(n,q+1)}$$

8.3.35 Remark For further examples, see for instance [752, 753].

8.3.6 Further value set papers

8.3.36 Remark There are many other papers describing results concerning value sets of polynomials over finite fields; however for lack of space, we are unable to precisely state them. Pages 379-381 of [1934] provide a wealth of descriptions of older papers dealing with value sets; pages 388-389 of [1934] provide summaries of value set results for polynomials in several variables. The paper [2823] presents the state of knowledge about value sets as of 1995.

8.3.37 Remark Since the publication of [1934], in [767] are given formulas for the number of polynomials of degree $q-1$ with a value set of cardinality k. Paper [768] describes values sets of diagonal equations over finite fields by giving a new proof of the Cauchy-Davenport theorem. See [752] and [753] for a discussion of polynomials over $\mathbb{F}_{2^n}$ which take on each nonzero value only a small number of times (at most six).

8.3.38 Remark Paper [1219] shows that if f is not a permutation polynomial over $\mathbb{F}_q$ and $q \geq n^4$, then $\#V_f < q - q/(2n)$, while [755] shows that by using the polynomial $(x+1)x^{q-1}$, Wan's bound is sharp for every extension of the base field. The paper [57] discusses results concerning the size of the intersection of the value sets of two nonconstant polynomials and [1454] discusses lower bounds for the size of the value set for the polynomial $(x^m + b)^n$ improving the bound given in [1307]. Paper [2743] discusses cardinalities of value sets for

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 $g, h \in \mathbb{F}_q[x]$.

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>

[267] K. Bibak, Additive combinatorics with a view towards computer science and cryptography: An exposition, *arXiv:1108.3790.* <183, 185, 186>

[268] F. Bien, Constructions of telephone networks by group representations, *Notices Amer. Math. Soc.* 36 (1989) 5–22. <634, 641, 650>

[269] J. Bierbrauer, *Introduction to Coding Theory*, Discrete Mathematics and its Applications. Chapman & Hall/CRC, Boca Raton, FL, 2005. <29, 30>

[270] J. Bierbrauer, A direct approach to linear programming bounds for codes and (t, m, s)-nets, *Des. Codes Cryptogr.* 42 (2007) 127–143. <613, 622>

[271] J. Bierbrauer, A family of crooked functions, *Des. Codes Cryptogr.* 50 (2009) 235–241. <252, 254>

[272] J. Bierbrauer, New commutative semifields and their nuclei, In *Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes*, volume 5527 of *Lecture Notes in Comput. Sci.*, 179–185, Springer, Berlin, 2009. <275>

[273] J. Bierbrauer, New semifields, PN and APN functions, *Des. Codes Cryptogr.* 54 (2010) 189–200. <275>

[274] J. Bierbrauer and Y. Edel, Theory of perpendicular arrays, *J. Combin. Des.* 2 (1994) 375–406. <604, 611>

[275] J. Bierbrauer, Y. Edel, and W. C. Schmid, Coding-theoretic constructions for (t, m, s)-nets and ordered orthogonal arrays, *J. Combin. Des.* 10 (2002) 403–418. <614, 617, 622>

[276] J. Bierbrauer and G. M. Kyureghyan, Crooked binomials, *Des. Codes Cryptogr.* 46 (2008) 269–301. <252, 254>

[277] E. Biham and A. Shamir, Differential cryptanalysis of DES-like cryptosystems, *J. Cryptology* 4 (1991) 3–72. <246, 254>

[278] M. Biliotti, V. Jha, and N. L. Johnson, *Foundations of Translation Planes*, volume 243 of *Monographs and Textbooks in Pure and Applied Mathematics*, Marcel Dekker Inc., New York, 2001. <558, 566>

[279] O. Billet and H. Gilbert, Cryptanalysis of Rainbow, In *Security and Cryptography for Networks*, volume 4116 of *Lecture Notes in Comput. Sci.*, 336–347. Springer, 2006. <764, 765, 775>

[280] O. Billet, M. J. B. Robshaw, and T. Peyrin, On building hash functions from multivariate quadratic equations, In J. Pieprzyk, H. Ghodosi, and E. Dawson, editors, *ACISP*, volume 4586 of *Lecture Notes in Computer Science*, 82–95. Springer, 2007. <774, 775>

[281] Y. Bilu and N. Linial, Lifts, discrepancy and nearly optimal spectral gap, *Combinatorica* 26 (2006) 495–519. <638, 648, 649, 650>

[282] G. Bini and F. Flamini, *Finite Commutative Rings and their Applications*, The Kluwer International Series in Engineering and Computer Science, 680. Kluwer Academic Publishers, Boston, MA, 2002. <26, 27, 29>

[283] B. J. Birch, How the number of points of an elliptic curve over a fixed prime field varies, *J. London Math. Soc., 2nd Ser.* 43 (1968) 57–60. <424, 434>

[284] B. J. Birch and H. P. F. Swinnerton-Dyer, Note on a problem of Chowla, *Acta Arith.* 5 (1959) 417–423 (1959). <227, 229>

[285] P. Birkner, Efficient divisor class halving on genus two curves, In *Thirteenth International Workshop on Selected Areas in Cryptography*, volume 4356 of *Lecture Notes in Comput. Sci.*, 317–326, Springer, Berlin, 2007. <789, 795>

[286] P. Birkner and N. Thériault, Faster halvings in genus 2, In *Fifteenth International Workshop on Selected Areas in Cryptography*, volume 5381 of *Lecture Notes in*

Comput. Sci., 1–17, Springer, Berlin, 2009. <789, 795>

[287] P. Birkner and N. Thériault, Efficient halving for genus 3 curves over binary fields, *Advances in Mathematics of Communications* 4 (2010) 23–47. <791, 795>

[288] A. Biró, On polynomials over prime fields taking only two values on the multiplicative group, *Finite Fields Appl.* 6 (2000) 302–308. <226, 229>

[289] R. R. Bitmead and B. D. O. Anderson, Asymptotically fast solution of Toeplitz and related systems of linear equations, *Linear Algebra Appl.* 34 (1980) 103–116. <527, 528>

[290] R. Blache, p-Density, exponential sums and Artin-Schreier curves, preprint available, `http://arxiv.org/abs/0812.3382`, 2008. <474, 478, 481>

[291] R. Blache, First vertices for generic Newton polygons, and p-cyclic coverings of the projective line, preprint available, `http://arxiv.org/abs/0912.2051`, 2009. <478, 481>

[292] R. Blache, Newton polygons for character sums and Poincaré series, *Int. J. Number Theory* 7 (2011) 1519–1542. <479, 481>

[293] R. Blache, J.-P. Cherdieu, and J. Estrada Sarlabous, Some computational aspects of Jacobians of curves in the family $y^3 = \gamma x^5 + \delta$ over $\mathbb{F}_p$, *Finite Fields Appl.* 13 (2007) 348–365. <799, 803>

[294] R. Blache and É. Férard, Newton stratification for polynomials: the open stratum, *J. Number Theory* 123 (2007) 456–472. <478, 481>

[295] R. Blache, É. Férard, and H. J. Zhu, Hodge-Stickelberger polygons for L-functions of exponential sums of $P(x^s)$, *Math. Res. Lett.* 15 (2008) 1053–1071. <478, 479, 481>

[296] S. R. Blackburn, A generalisation of the discrete Fourier transform: determining the minimal polynomial of a periodic sequence, *IEEE Trans. Inform. Theory* 40 (1994) 1702–1704. <322, 330>

[297] S. R. Blackburn, T. Etzion, and K. G. Paterson, Permutation polynomials, de Bruijn sequences, and linear complexity, *J. Combin. Theory, Ser. A* 76 (1996) 55–82. <323, 330>

[298] S. R. Blackburn, D. Gómez-Pérez, J. Gutierrez, and I. E. Shparlinski, Predicting the inversive generator, In *Cryptography and Coding*, volume 2898 of *Lecture Notes in Comput. Sci.*, 264–275, Springer, Berlin, 2003. <332, 338>

[299] S. R. Blackburn, D. Gómez-Pérez, J. Gutierrez, and I. E. Shparlinski, Predicting nonlinear pseudorandom number generators, *Math. Comp.* 74 (2005) 1471–1494. <332, 338>

[300] S. R. Blackburn, D. Gómez-Pérez, J. Gutierrez, and I. E. Shparlinski, Reconstructing noisy polynomial evaluation in residue rings, *J. Algorithms* 61 (2006) 47–59. <332, 338>

[301] S. R. Blackburn and P. R. Wild, Optimal linear perfect hash families, *J. Combin. Theory, Ser. A* 83 (1998) 233–250. <605, 611>

[302] R. E. Blahut, Transform techniques for error control codes, *IBM J. Res. Develop.* 23 (1979) 299–315. <322, 330>

[303] R. E. Blahut, *Theory and Practice of Error Control Codes*, Addison-Wesley Publishing Company Advanced Book Program, Reading, MA, 1983. <29, 30, 653, 655, 672, 680, 682, 684, 685, 695>

[304] I. F. Blake, editor, *Algebraic Coding Theory: History and Development*, Dowden Hutchinson & Ross Inc., Stroudsburg, Pa., 1973, Benchmark Papers in Electrical Engineering and Computer Science. <694, 695>

[343] D. Boneh and M. Franklin, Identity-based encryption from the Weil pairing, *SIAM J. Comput.* 32 (2003) 586–615. <739, 741>

[344] D. Boneh, E.-J. Goh, and K. Nissim, Evaluating 2-DNF formulas on ciphertexts, In J. Kilian, editor, *Theory of Cryptography—TCC 2005*, volume 3378 of *Lecture Notes in Computer Science*, 325–341, Berlin, 2005, Springer-Verlag. <784, 788>

[345] D. Boneh, B. Lynn, and H. Shacham, Short signatures from the Weil pairing, *J. Cryptology* 17 (2004) 297–319. <739, 741>

[346] D. Boneh and R. Venkatesan, Rounding in lattices and its cryptographic applications, In *Proceedings of the Eighth Annual ACM-SIAM Symposium on Discrete Algorithms*, 675–681, New York, 1997, ACM. <170, 179>

[347] D. Boneh and R. Venkatesan, Breaking RSA may not be equivalent to factoring (extended abstract), In *Advances in Cryptology—EUROCRYPT '98*, volume 1403 of *Lecture Notes in Comput. Sci.*, 59–71, Springer, Berlin, 1998. <170, 179>

[348] T. J. Boothby and R. W. Bradshaw, Bitslicing and the method of four Russians over larger finite fields, preprint available, `http://arxiv.org/abs/0901.1413`, 2009. <515, 528>

[349] H. Borges, Frobenius non-classical curves of type $g(y) = f(x)$, preprint, 2012. <226, 229>

[350] H. Borges and F. Conceição, On the characterization of minimal value set polynomials, preprint, 2012. <226, 229>

[351] P. Borwein, K.-K. S. Choi, and J. Jedwab, Binary sequences with merit factor greater than 6.34, *IEEE Trans. Inform. Theory* 50 (2004) 3234–3249. <317, 318>

[352] J. Bos and M. E. Kaihara, Playstation 3 computing breaks 2^{60} barrier: 112-bit prime ECDLP solved, online annoucement, http://lacal.epfl.ch/112bit_prime, 2009. <394>

[353] S. Bosch, U. Güntzer, and R. Remmert, *Non-Archimedean Analysis: A Systematic Approach to Rigid Analytic Geometry*, volume 261 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*, Springer-Verlag, Berlin, 1984. <530, 539>

[354] R. C. Bose, On the application of the properties of Galois fields to the construction of hyper-graeco-latin squares, *Sankhyā* 3 (1938) 323–338. <544, 547, 548>

[355] R. C. Bose, On the construction of balanced incomplete block designs, *Ann. Eugenics* 9 (1939) 353–399. <584, 591>

[356] R. C. Bose, On some connections between the design of experiments and information theory, *Bull. Inst. Internat. Statist.* 38 (1961) 257–271. <623, 634>

[357] R. C. Bose and R. C. Burton, A characterization of flat spaces in a finite geometry and the uniqueness of the Hamming and the MacDonald codes, *J. Combinatorial Theory* 1 (1966) 96–104. <552, 556>

[358] R. C. Bose and D. K. Ray-Chaudhuri, On a class of error correcting binary group codes, *Information and Control* 3 (1960) 68–79. <670, 694, 695>

[359] W. Bosma, J. Cannon, and C. Playoust, The Magma algebra system I: The user language, *J. Symbolic Comput.* 24 (1997) 235–265. <381, 386>

[360] W. Bosma, J. Cannon, and A. Steel, Lattices of compatibly embedded finite fields, *J. Symbolic Comput.* 24 (1997) 351–369. <395, 398>

[361] W. Bosma and H. W. Lenstra, Jr., Complete systems of two addition laws for

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,

Symposium on Discrete Algorithms, 1457–1463, 2012. <94>

[608] J. H. Cheon, J. Hong, and M. Kim, Accelerating Pollard's rho algorithm in finite fields, *Journal of Cryptology* 25 (2012) 185–242. <391, 394>

[609] R. C. C. Cheung, S. Duquesne, J. Fan, N. Guillermin, I. Verbauwhede, and G. X. Yao, FPGA implementation of pairings using residue number system and lazy reduction, In *Proceedings of the 2011 Workshop on Cryptographic Hardware and Embedded Systems*, 421–441, 2011. <814>

[610] C. Chevalley, Démonstration d'une hypothèse de m. artin, *Abhand. Math. Sem. Hamburg* 11 (1936) 73–75. <201, 207>

[611] G. Chèze, *Des méthodes symboliques-numériques et exactes pour la factorisation absolue des polynômes en deux variables*, PhD thesis, Université de Nice-Sophia Antipolis (France), 2004. <380, 386>

[612] G. Chèze and G. Lecerf, Lifting and recombination techniques for absolute factorization, *J. Complexity* 23 (2007) 380–420. <378, 386>

[613] A. M. Childs, L. J. Schulman, and U. V. Vazirani, Quantum algorithms for hidden nonlinear structures, In *Forty Eighth Annual IEEE Symposium on Foundations of Computer Science*, 395–404, 2007. <831, 832>

[614] A. M. Childs and W. van Dam, Quantum algorithms for algebraic problems, *Rev. Modern Phys.* 82 (2010) 1–52. <825, 832>

[615] K. Chinen and T. Hiramatsu, Hyper-Kloosterman sums and their applications to the coding theory, *Appl. Algebra Engrg. Comm. Comput.* 12 (2001) 381–390. <148, 155>

[616] A. Chistov, Polynomial time construction of a finite field, In *Abstracts of Lectures at Seventh All-Union Conference in Mathematical Logic*, 196, Novosibirsk, USSR, 1984, In Russian. <372, 374>

[617] H. T. Choi and R. Evans, Congruences for sums of powers of Kloosterman sums, *Int. J. Number Theory* 3 (2007) 105–117. <151, 152, 155>

[618] B. C. Chong and K. M. Chan, On the existence of normalized room squares, *Nanta Math.* 7 (1974) 8–17. <606, 611>

[619] W. S. Chou, *Permutation Polynomials on Finite Fields and their Combinatorial Applications*, PhD thesis, Penn. State Univ., University Park, PA, 1990. <221, 223>

[620] W. S. Chou, The period lengths of inversive pseudorandom vector generations, *Finite Fields Appl.* 1 (1995) 126–132. <222, 223>

[621] W.-S. Chou, The factorization of Dickson polynomials over finite fields, *Finite Fields Appl.* 3 (1997) 84–96. <277, 283>

[622] W.-S. Chou and S. D. Cohen, Primitive elements with zero traces, *Finite Fields Appl.* 7 (2001) 125–141. <87, 90>

[623] W. S. Chou, J. Gómez-Calderón, and G. L. Mullen, Value sets of Dickson polynomials over finite fields, *J. Number Theory* 30 (1988) 334–344. <226, 228, 229>

[624] W.-S. Chou, J. Gómez-Calderón, G. L. Mullen, D. Panario, and D. Thomson, Subfield value sets of polynomials over finite fields, *Funct. Approx. Comment. Math.* (In press, 2012) 21 pages. <229>

[625] W.-S. Chou and G. L. Mullen, A note on value sets of polynomials over finite fields, preprint, 2012. <227, 229>

[626] S. Chowla and H. J. Ryser, Combinatorial problems, *Canadian J. Math.* 2 (1950) 93–99. <593, 599>

<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>

of square order, *Finite Fields Appl.* 18 (2012) 316–336. <274, 275>

[727] R. S. Coulter and R. W. Matthews, Planar functions and planes of Lenz-Barlotti class II, *Des. Codes Cryptogr.* 10 (1997) 167–184. <264, 266, 272, 273, 275>

[728] R. S. Coulter and R. W. Matthews, On the permutation behaviour of Dickson polynomials of the second kind, *Finite Fields Appl.* 8 (2002) 519–530. <219, 223>

[729] R. S. Coulter and R. W. Matthews, On the number of distinct values of a class of functions over a finite field, *Finite Fields Appl.* 17 (2011) 220–224. <229, 274, 275>

[730] N. T. Courtois, Fast algebraic attacks on stream ciphers with linear feedback, In *Advances in Cryptology—CRYPTO 2003*, volume 2729 of *Lecture Notes in Comput. Sci.*, 176–194, Springer, Berlin, 2003. <241, 245>

[731] N. T. Courtois, Algebraic attacks over GF(2^k), application to HFE Challenge 2 and Sflash-v2, In *Public Key Cryptography—PKC 2004*, volume 2947 of *Lecture Notes in Comput. Sci.*, 201–217, Springer, Berlin, 2004. <773, 775>

[732] N. T. Courtois, M. Daum, and P. Felke, On the security of HFE, HFEv- and Quartz, In *Public Key Cryptography—PKC 2003*, volume 2567 of *Lecture Notes in Comput. Sci.*, 337–350, Springer, Berlin, 2002. <762, 772, 775>

[733] N. T. Courtois, L. Goubin, W. Meier, and J.-D. Tacier, Solving underdefined systems of multivariate quadratic equations, In *PubKeyCrypt 2002*, volume 2274 of *Lecture Notes in Computer Science*, 211–227. David Naccache and Pascal Paillier, editors, 2002. <773, 775>

[734] N. T. Courtois, L. Goubin, and J. Patarin, *SFLASH: Primitive specification (second revised version)*, 2002, `https://www.cosic.esat.kuleuven.be/nessie`, Submissions, Sflash, 11 pages. <764, 775>

[735] N. T. Courtois, A. Klimov, J. Patarin, and A. Shamir, Efficient algorithms for solving overdefined systems of multivariate polynomial equations, In *Advances in Cryptology—EUROCRYPT 2000*, volume 1807 of *Lecture Notes in Comput. Sci.*, 392–407, Springer, Berlin, 2000. <772, 773, 775>

[736] N. T. Courtois and W. Meier, Algebraic attacks on stream ciphers with linear feedback, In *Advances in Cryptology—EUROCRYPT 2003*, volume 2656 of *Lecture Notes in Comput. Sci.*, 345–359, Springer, Berlin, 2003. <241, 245>

[737] N. T. Courtois and J. Patarin, About the XL algorithm over GF(2), In *Topics in Cryptology—CT-RSA 2003*, volume 2612 of *Lecture Notes in Comput. Sci.*, 141–157, Springer, Berlin, 2003. <773, 775>

[738] N. T. Courtois and J. Pieprzyk, Cryptanalysis of block ciphers with overdefined systems of equations, In *Advances in Cryptology—ASIACRYPT 2002*, volume 2501 of *Lecture Notes in Comput. Sci.*, 267–287, Springer, Berlin, 2002. <773, 774, 775>

[739] J.-M. Couveignes and T. Henocq, Action of modular correspondences around CM points, In C. Fieker and D. R. Kohel, editors, *Algorithmic Number Theory—ANTS-V*, volume 2369 of *Lecture Notes in Computer Science*, 234–243, Berlin, 2002, Springer-Verlag. <778, 788>

[740] J.-M. Couveignes and J.-G. Kammerer, The geometry of flex tangents to a cubic curve and its parameterizations, *Journal of Symbolic Computation* 47 (2012) 266–281. <788>

[741] J.-M. Couveignes and R. Lercier, Elliptic periods for finite fields, *Finite Fields Appl.* 15 (2009) 1–22. <115, 116, 122>

[742] J.-M. Couveignes and R. Lercier, Fast construction of irreducible polynomials over finite fields, *Israel Journal of Mathematics* (2011), To appear. ArXiv:0905.1642v2. <372, 374>

[743] D. Cox, J. Little, and D. O'Shea, *Ideals, Varieties, and Algorithms*, Undergraduate Texts in Mathematics. Springer, New York, third edition, 2007. <775, 817, 825>

[744] D. A. Cox, *Galois Theory*, Pure and Applied Mathematics (New York). Wiley-Interscience, John Wiley & Sons, Hoboken, NJ, 2004. <2, 8, 10>

[745] R. Crandall, Method and apparatus for public key exchange in a cryptographic system, United States Patent 5,159,632, Date: Oct. 27th 1992. <346, 357>

[746] R. Crandall and C. Pomerance, *Prime Numbers*, Springer, New York, second edition, 2005, A computational perspective. <340, 348, 349, 356, 357, 489, 493>

[747] R. M. Crew, Etale p-covers in characteristic p, *Compositio Math.* 52 (1984) 31–45. <480, 481>

[748] H. S. Cronie and S. B. Korada, Lossless source coding with polar codes, In *Proc. (ISIT) Symp. IEEE Int Information Theory*, 904–908, 2010. <731>

[749] E. Croot, Sums of the form $1/x_1^k + \cdots + 1/x_n^k$ modulo a prime, *Integers* 4 (2004) A20, 6. <207>

[750] S. Crozier, J. Lodge, P. Guinand, and A. Hunt, Performance of turbo codes with relative prime and golden interleaving strategies, In *Proc. of the Sixth International Mobile Satellite Conference (IMSC '99)*, 268–275, Ottawa, Ontario, Canda, 1999. <718, 719>

[751] C. Culbert and G. L. Ebert, Circle geometry and three-dimensional subregular translation planes, *Innov. Incidence Geom.* 1 (2005) 3–18. <560, 566>

[752] T. W. Cusick, Value sets of some polynomials over finite fields GF(2^{2m}), *SIAM J. Comput.* 27 (1998) 120–131 (electronic). <228, 229>

[753] T. W. Cusick, Polynomials over base 2 finite fields with evenly distributed values, *Finite Fields Appl.* 11 (2005) 278–291. <228, 229>

[754] T. W. Cusick, C. Ding, and A. Renvall, *Stream Ciphers and Number Theory*, volume 66 of *North-Holland Mathematical Library*, Elsevier Science B.V., Amsterdam, revised edition, 2004. <29, 30, 321, 322, 327, 328, 330>

[755] T. W. Cusick and P. Müller, Wan's bound for value sets of polynomials, In *Finite Fields and Applications*, volume 233 of *London Math. Soc. Lecture Note Ser.*, 69–72, Cambridge Univ. Press, Cambridge, 1996. <226, 228, 229>

[756] S. Czapor, K. Geddes, and G. Labahn, *Algorithms for Computer Algebra*, Kluwer Academic Publishers, 1992. <29, 30, 376, 386>

[757] J. Daemen and V. Rijmen, *The Design of Rijndael: AES – the Advanced Encryption Standard*, Springer-Verlag, 2002. <29, 30, 742, 751, 752, 755>

[758] Z. Dai, Multi-continued fraction algorithms and their applications to sequences, In *Sequences and Their Applications—SETA 2006*, volume 4086 of *Lecture Notes in Comput. Sci.*, 17–33, Springer, Berlin, 2006. <323, 330>

[759] Z. Dai and X. Feng, Classification and counting on multi-continued fractions and its application to multi-sequences, *Sci. China, Ser. F* 50 (2007) 351–358. <323, 330>

[760] Z. Dai, K. Wang, and D. Ye, Multi-continued fraction algorithm on multi-formal Laurent series, *Acta Arith.* 122 (2006) 1–16. <323, 330>

[761] Z. Dai and J. Yang, Multi-continued fraction algorithm and generalized B-M algorithm over $\mathbb{F}_q$, *Finite Fields Appl.* 12 (2006) 379–402. <323, 330>

[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>

nomials and generalized cyclotomic polynomials over finite fields, *Finite Fields Appl.* 13 (2007) 492–515. <278, 279, 280, 283>

[1077] P. Flajolet, X. Gourdon, and D. Panario, The complete analysis of a polynomial factorization algorithm over finite fields, *J. Algorithms* 40 (2001) 37–81. <359, 362, 363, 367, 368, 375, 376>

[1078] P. Flajolet and A. Odlyzko, Singularity analysis of generating functions, *SIAM J. Discrete Math.* 3 (1990) 216–240. <360, 368>

[1079] P. Flajolet and A. M. Odlyzko, Random mapping statistics, In *EUROCRYPT*, 329–354, 1989. <745, 755>

[1080] P. Flajolet and R. Sedgewick, *Analytic Combinatorics*, Cambridge University Press, Cambridge, 2009. <359, 361, 368>

[1081] P. Flajolet and M. Soria, Gaussian limiting distributions for the number of components in combinatorial structures, *J. Combin. Theory, Ser. A* 53 (1990) 165–182. <361, 367, 368>

[1082] P. Flajolet and M. Soria, General combinatorial schemas: Gaussian limit distributions and exponential tails, *Discrete Math.* 114 (1993) 159–180. <361, 367, 368>

[1083] J. J. Flynn, *Near-Exceptionality over Finite Fields*, PhD dissertation, University of California, Berkeley, Department of Mathematics, 2001. <226, 229>

[1084] S. Fomin and A. Zelevinsky, The Laurent phenomenon, *Adv. in Appl. Math.* 28 (2002) 119–144. <331, 338>

[1085] K. Fong, D. Hankerson, J. López, and A. Menezes, Field inversion and point halving revisited, *IEEE Trans. Comput.* 53 (2003) 1047–1059. <357>

[1086] F. Fontein, Groups from cyclic infrastructures and Pohlig-Hellman in certain infrastructures, *Adv. Math. Commun.* 2 (2008) 293–307. <450>

[1087] G. D. Forney, Jr., On decoding BCH codes, *IEEE Trans. Information Theory* IT-11 (1965) 549–557. <686, 694, 695>

[1088] G. D. Forney, Jr., *Concatenated Codes*, M.I.T. Press, Cambridge, MA, 1966. <712, 719>

[1089] G. D. Forney, Jr., Generalized minimum distance decoding, *IEEE Trans. Information Theory* IT-12 (1966) 125–131. <689, 694, 695>

[1090] G. D. Forney, Jr., N. J. A. Sloane, and M. D. Trott, The Nordstrom-Robinson code is the binary image of the octacode, In *Coding and Quantization*, volume 14 of *DIMACS Ser. Discrete Math. Theoret. Comput. Sci.*, 19–26, Amer. Math. Soc., Providence, RI, 1993. <693, 695>

[1091] P.-A. Fouque, L. Granboulan, and J. Stern, Differential cryptanalysis for multivariate schemes, In *Advances in Cryptology—EUROCRYPT 2005*, volume 3494 of *Lecture Notes in Comput. Sci.*, 341–353, Springer, Berlin, 2005. <765, 769, 770, 775>

[1092] P.-A. Fouque, G. Macario-Rat, L. Perret, and J. Stern, Total break of the l-IC signature scheme, In *Public Key Cryptography—PKC 2008*, volume 4939 of *Lecture Notes in Comput. Sci.*, 1–17, Springer, Berlin, 2008. <765, 775>

[1093] H. M. Fredricksen, A. W. Hales, and M. M. Sweet, A generalization of Swan's theorem, *Math. Comp.* 46 (1986) 321–331. <64, 66>

[1094] D. Freeman, P. Stevenhagen, and M. Streng, Abelian varieties with prescribed embedding degree, In *Algorithmic Number Theory*, volume 5011 of *Lecture Notes in Comput. Sci.*, 60–73, Springer, Berlin, 2008. <803>

[1095] D. M. Freeman, Converting pairing-based cryptosystems from composite-order

[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

Berlin, 2008. <30>

[1303] D. Gómez, J. Gutierrez, and Á. Ibeas, Attacking the Pollard generator, *IEEE Trans. Inform. Theory* 52 (2006) 5518–5523. <332, 338>

[1304] D. Gómez and A. P. Nicolás, An estimate on the number of stable quadratic polynomials, *Finite Fields Appl.* 16 (2010) 401–405. <172, 179, 336, 337, 338>

[1305] D. Gómez, A. P. Nicolás, A. Ostafe, and D. Sadornil, Stable polynomials over finite fields, preprint available, `http://arxiv.org/abs/1206.4979`, 2011. <337, 338>

[1306] D. Gómez and A. Winterhof, Waring's problem in finite fields with Dickson polynomials, In *Finite Fields: Theory and Applications*, volume 518 of *Contemp. Math.*, 185–192, Amer. Math. Soc., Providence, RI, 2010. <207>

[1307] J. Gómez-Calderón, On the cardinality of value set of polynomials with coefficients in a finite field, *Proc. Japan Acad., Ser. A Math. Sci.* 68 (1992) 338–340. <228, 229>

[1308] J. Gómez-Calderón and D. J. Madden, Polynomials with small value set over finite fields, *J. Number Theory* 28 (1988) 167–188. <226, 229>

[1309] D. Gómez-Pérez, A. Ostafe, and I. E. Shparlinski, Algebraic entropy, automorphisms and sparsity of algebraic dynamical systems and pseudorandom number generator, Preprint, 2012. <333, 334, 338>

[1310] D. Gómez-Pérez, A. Ostafe, and I. E. Shparlinski, On irreducible divisors of iterated polynomials, *Revista Matem. Iberoamer.* (2012), to appear. <331, 336, 337, 338>

[1311] G. Gong, T. Helleseth, H. Hu, and A. Kholosha, On the dual of certain ternary weakly regular bent functions, *IEEE Trans. Inform. Theory* 58 (2012) 2237–2243. <263, 266>

[1312] G. Gong, T. Helleseth, H.-Y. Song, and K. Yang, editors, *Sequences and Their Applications*, volume 4086 of *Lecture Notes in Comput. Sci.*, Springer, Berlin, 2006. <30>

[1313] G. Gong and A. M. Youssef, Cryptographic properties of the Welch-Gong transformation sequence generators, *IEEE Transactions on Information Theory* 48 (2002) 2837–2846. <747, 755>

[1314] P. Gopalan, V. Guruswami, and R. J. Lipton, Algorithms for modular counting of roots of multivariate polynomials, In *LATIN 2006: Theoretical Informatics*, volume 3887 of *Lecture Notes in Comput. Sci.*, 544–555, Springer, Berlin, 2006. <483, 485>

[1315] V. D. Goppa, A new class of linear correcting codes, *Problemy Peredači Informacii* 6 (1970) 24–30. <676, 694, 695>

[1316] V. D. Goppa, Rational representation of codes and (L, g)-codes, *Problemy Peredači Informacii* 7 (1971) 41–49. <676, 694, 695>

[1317] V. D. Goppa, Codes that are associated with divisors (Russian), *Problemy Peredači Informacii* 13 (1977) 33–39. <695, 704>

[1318] V. D. Goppa, Codes on algebraic curves (Russian), *Dokl. Akad. Nauk SSSR* 259 (1981) 1289–1290. <695, 704>

[1319] V. D. Goppa, Algebraic-geometric codes (Russian), *Izv. Akad. Nauk SSSR Ser. Mat.* 46 (1982) 762–781. <695, 704>

[1320] B. Gordon, W. H. Mills, and L. R. Welch, Some new difference sets, *Canad. J. Math.* 14 (1962) 614–625. <312, 318, 594, 595, 599>

[1321] D. M. Gordon, Discrete logarithms in GF(p) using the number field sieve, *SIAM*

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

[1453] A. S. Hedayat, N. J. A. Sloane, and J. Stufken, *Orthogonal Arrays, Theory and Applications*, Springer Series in Statistics. Springer-Verlag, New York, 1999. <602, 611, 623, 634>

[1454] A. Hefez, On the value sets of special polynomials over finite fields, *Finite Fields Appl.* 2 (1996) 337–347. <228, 229>

[1455] L. Heffter, Ueber Tripelsysteme, *Math. Ann.* 49 (1897) 101–112. <584, 591>

[1456] H. Heilbronn, Lecture Notes on Additive Number Theory mod p, *California Institute of Technology* (1964). <206, 207>

[1457] R. Heindl, *New Directions in Multivariate Public Key Cryptography*, PhD dissertation, Clemson University, 2009, `http://etd.lib.clemson.edu/documents/1247508584/`. <767, 775>

[1458] J. Heintz and M. Sieveking, Absolute primality of polynomials is decidable in random polynomial time in the number of variables, In *Automata, Languages and Programming*, volume 115 of *Lecture Notes in Comput. Sci.*, 16–28, Springer-Verlag, 1981. <380, 386>

[1459] H. A. Helfgott, Growth and generation in $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$, *Ann. of Math., 2nd Ser.* 167 (2008) 601–623. <185, 186>

[1460] H. A. Helfgott, Growth in $\mathrm{SL}_3(\mathbb{Z}/p\mathbb{Z})$, *J. Eur. Math. Soc. (JEMS)* 13 (2011) 761–851. <185, 186>

[1461] H. A. Helfgott and M. Rudnev, An explicit incidence theorem in $\mathbb{F}_p$, *Mathematika* 57 (2011) 135–145. <185, 186>

[1462] H. A. Helfgott and A. Seress, On the diameter of permutation groups, *arXiv:1109.3550*. <185, 186>

[1463] T. Helleseth, Some results about the cross-correlation function between two maximal linear sequences, *Discrete Math.* 16 (1976) 209–232. <253, 255, 314, 318>

[1464] T. Helleseth, On the covering radius of cyclic linear codes and arithmetic codes, *Discrete Appl. Math.* 11 (1985) 157–173. <170, 179>

[1465] T. Helleseth, H. D. L. Hollmann, A. Kholosha, Z. Wang, and Q. Xiang, Proofs of two conjectures on ternary weakly regular bent functions, *IEEE Trans. Inform. Theory* 55 (2009) 5272–5283. <263, 266>

[1466] T. Helleseth and A. Kholosha, Monomial and quadratic bent functions over the finite fields of odd characteristic, *IEEE Trans. Inform. Theory* 52 (2006) 2018–2032. <259, 263, 266>

[1467] T. Helleseth and A. Kholosha, On the dual of monomial quadratic p-ary bent functions, In *Sequences, Subsequences, and Consequences*, volume 4893 of *Lecture Notes in Comput. Sci.*, 50–61, Springer, Berlin, 2007. <263, 266>

[1468] T. Helleseth and A. Kholosha, New binomial bent functions over the finite fields of odd characteristic, *IEEE Trans. Inform. Theory* 56 (2010) 4646–4652. <264, 266>

[1469] T. Helleseth and A. Kholosha, Crosscorrelation of m-sequences, exponential sums, bent functions and Jacobsthal sums, *Cryptogr. Commun.* 3 (2011) 281–291. <264, 266>

[1470] T. Helleseth, A. Kholosha, and S. Mesnager, Niho bent functions and Subiaco hyperovals, In M. Lavrauw, G. L. Mullen, S. Nikova, D. Panario, and L. Storme, editors, *Theory and Applications of Finite Fields*, volume 579 of *Contemporary Mathematics*, 91–101, Providence, Rhode Island, 2012, American Mathematical Society. <261, 262, 266>

[1471] T. Helleseth and P. V. Kumar, Sequences with low correlation, In *Handbook of*

[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>

of pseudorandomness, the Legendre symbol, *Acta Arith.* 82 (1997) 365–377. <176, 179, 329, 330, 833, 840>

[2033] U. M. Maurer, Fast generation of prime numbers and secure public-key cryptographic parameters, *J. Cryptology* 8 (1995) 123–155. <341, 357>

[2034] U. M. Maurer and S. Wolf, The Diffie-Hellman protocol: towards a quarter-century of public key cryptography, *Des. Codes Cryptogr.* 19 (2000) 147–171. <737, 741>

[2035] J. P. May, D. Saunders, and Z. Wan, Efficient matrix rank computation with application to the study of strongly regular graphs, In *ISSAC 2007*, 277–284, ACM, New York, 2007. <527, 528>

[2036] B. Mazur, Frobenius and the Hodge filtration (estimates), *Ann. of Math., 2nd Ser.* 98 (1973) 58–95. <475, 481>

[2037] O. D. Mbodj, Quadratic Gauss sums, *Finite Fields Appl.* 4 (1998) 347–361. <144, 155>

[2038] K. McCann and K. S. Williams, The distribution of the residues of a quartic polynomial, *Glasgow Math. J.* 8 (1967) 67–88. <227, 229>

[2039] K. S. McCurley, Cryptographic key distribution and computation in class groups, In *Number Theory and Applications*, volume 265 of *NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci.*, 459–479, Kluwer Acad. Publ., Dordrecht, 1989. <388, 394>

[2040] B. R. McDonald, *Finite Rings with Identity*, Pure and Applied Mathematics, Vol. 28. Marcel Dekker Inc., New York, 1974. <26, 27, 29>

[2041] R. J. McEliece, Table of polynomials of period e over GF(p), *Math. Comp.* 23 (1969) C1–C6. <58, 61>

[2042] R. J. McEliece, *The Theory of Information and Coding*, Addison-Wesley Publishing Co., Reading, Mass.-London-Amsterdam, 1977. <653, 676, 677, 686, 695>

[2043] R. J. McEliece, A public-key cryptosystem based on algebraic coding theory, DSN progress report #42-44, Jet Propulsion Laboratory, Pasadena, California, 1978. <740, 741>

[2044] R. J. McEliece, *Finite Fields for Computer Scientists and Engineers*, The Kluwer International Series in Engineering and Computer Science, 23. Kluwer Academic Publishers, Boston, MA, 1987. <11, 29, 30>

[2045] R. J. McEliece, E. R. Rodemich, H. Rumsey, Jr., and L. R. Welch, New upper bounds on the rate of a code via the Delsarte-MacWilliams inequalities, *IEEE Trans. Information Theory* IT-23 (1977) 157–166. <665, 666, 695>

[2046] R. L. McFarland, A family of difference sets in non-cyclic groups, *J. Combin. Theory, Ser. A* 15 (1973) 1–10. <259, 266, 597, 599>

[2047] G. McGuire, G. L. Mullen, D. Panario, and I. E. Shparlinski, editors, *Finite Fields: Theory and Applications*, volume 518 of *Contemporary Mathematics*, American Mathematical Society, Providence, RI, 2010. <30>

[2048] B. D. McKay and I. M. Wanless, On the number of Latin squares, *Ann. Comb.* 9 (2005) 335–344. <543, 548>

[2049] H. McKean and V. Moll, *Elliptic Curves: Function Theory, Geometry, Arithmetic*, Cambridge University Press, Cambridge, 1997. <29, 30, 417, 434>

[2050] P. K. Meher, Systolic and super-systolic multipliers for finite field $GF(2^m)$ based on irreducible trinomials, *IEEE Transactions on Circuits and Systems I: Regular Papers* 55 (2008) 1031–1040. <807, 815>

[2051] W. Meidl, Linear complexity and k-error linear complexity for p^n-periodic se-

Theory, volume 10 of *IRMA Lect. Math. Theor. Phys.*, 225–251, Eur. Math. Soc., Zürich, 2006. <151, 155>

[2088] T. Migler, K. E. Morrison, and M. Ogle, How much does a matrix of rank k weigh?, *Math. Mag.* 79 (2006) 262–271. <494, 503>

[2089] M. Mignotte and C. Schnorr, Calcul des racines d-ièmes dans un corps fini, *Comptes Rendus de l'Académie des Sciences Paris* 290 (1988) 205–206. <375, 376>

[2090] P. Mihăilescu, Fast generation of provable primes using search in arithmetic progressions, In *Advances in Cryptology—CRYPTO '94*, volume 839 of *Lecture Notes in Comput. Sci.*, 282–293, Springer, Berlin, 1994. <341, 357>

[2091] P. Mihăilescu, Optimal Galois field bases which are not normal, 1997, Presented at the Workshop on Fast Software Encryption in Haifa. <347, 357>

[2092] P. Mihăilescu, Medium Galois Fields, their Bases and Arithmetic, 2000, `http://grouper.ieee.org/groups/1363/P1363a/NumThAlgs.html`. <352, 357>

[2093] P. Mihăilescu, F. Morain, and E. Schost, Computing the eigenvalue in the Schoof–Elkies–Atkin algorithm using abelian lifts, In C. W. Brown, editor, *Proceedings of the 2007 International Symposium on Symbolic and Algebraic Computation—ISSAC 2007*, 285–292, ACM, New York, 2007. <779, 788>

[2094] G. L. Miller, Riemann's hypothesis and tests for primality, *J. Comput. System Sci.* 13 (1976) 300–317. <340, 357>

[2095] R. L. Miller, Necklaces, symmetries and self-reciprocal polynomials, *Discrete Math.* 22 (1978) 25–33. <279, 283>

[2096] S. J. Miller and M. R. Murty, Effective equidistribution and the Sato-Tate law for families of elliptic curves, *J. Number Theory* 131 (2011) 25–44. <424, 434>

[2097] V. S. Miller, Use of elliptic curves in cryptography, In *Advances in Cryptology—CRYPTO '85*, volume 218 of *Lecture Notes in Comput. Sci.*, 417–426, Springer, Berlin, 1986. <737, 741, 775, 788>

[2098] D. Mills, Factorizations of root-based polynomial compositions, *Discrete Math.* 240 (2001) 161–173. <63, 66>

[2099] D. Mills, Existence of primitive polynomials with three coefficients prescribed, *JP J. Algebra Number Theory Appl.* 4 (2004) 1–22. <88, 90>

[2100] W. H. Mills, Polynomials with minimal value sets, *Pacific J. Math.* 14 (1964) 225–241. <226, 229>

[2101] W. H. Mills and R. C. Mullin, Coverings and packings, In *Contemporary Design Theory*, Wiley-Intersci. Ser. Discrete Math. Optim., 371–399, Wiley, New York, 1992. <590, 591>

[2102] J. S. Milne, *Elliptic Curves*, BookSurge Publishers, Charleston, SC, 2006. <29, 30, 417, 434>

[2103] R. Mines, F. Richman, and W. Ruitenburg, *A Course in Constructive Algebra*, Universitext. Springer-Verlag, 1988. <377, 386>

[2104] M. Minzlaff, Computing zeta functions of superelliptic curves in larger characteristic, *Math. Comput. Sci.* 3 (2010) 209–224. <483, 485>

[2105] Y. Miyamoto, H. Doi, K. Matsuo, J. Chao, and S. Tsuji, A fast addition algorithm of genus two hyperelliptic curve, In *Proc. of SCIS2002, IEICE Japan*, 497–502, 2002, in Japanese. <790, 795>

[2106] R. T. Moenck, Another polynomial homomorphism, *Acta Informat.* 6 (1976) 153–169. <345, 357>

[2736] M. Sudan, Decoding of Reed Solomon codes beyond the error-correction bound, *J. Complexity* 13 (1997) 180–193. <690, 691, 695>

[2737] M. Sugita, M. Kawazoe, and H. Imai, Gröbner basis based cryptanalysis of sha-1, Cryptology ePrint Archive, Report 2006/098, 2006, `http://eprint.iacr.org/`. <774, 775>

[2738] Y. Sugiyama, M. Kasahara, S. Hirasawa, and T. Namekawa, A method for solving key equation for decoding Goppa codes, *Information and Control* 27 (1975) 87–99. <686, 695>

[2739] J. Sun and O. Y. Takeshita, Interleavers for turbo codes using permutation polynomials over integer rings, *IEEE Trans. Inform. Theory* 51 (2005) 101–119. <222, 223, 717, 718, 719>

[2740] Q. Sun, The number of solutions of certain diagonal equations over finite fields, *Sichuan Daxue Xuebao* 34 (1997) 395–398. <203, 207>

[2741] Q. Sun and D. Q. Wan, On the solvability of the equation $\sum_{i=1}^{n} x_i/d_i \equiv 0 \pmod 1$ and its application, *Proc. Amer. Math. Soc.* 100 (1987) 220–224. <202, 203, 207>

[2742] Q. Sun and D. Q. Wan, On the Diophantine equation $\sum_{i=1}^{n} x_i/d_i \equiv 0 \pmod 1$, *Proc. Amer. Math. Soc.* 112 (1991) 25–29. <203, 207>

[2743] Z.-W. Sun, On value sets of polynomials over a field, *Finite Fields Appl.* 14 (2008) 470–481. <204, 207, 228, 229>

[2744] B. Sunar, A generalized method for constructing subquadratic complexity $GF(2^k)$ multipliers, *IEEE Trans. Comput.* 53 (2004) 1097–1105. <806, 815>

[2745] B. Sunar, A Euclidean algorithm for normal bases, *Acta Appl. Math.* 93 (2006) 57–74. <354, 357>

[2746] B. Sunar and Ç. K. Koç, Mastrovito multiplier for all trinomials, *IEEE Trans. Comput.* 48 (1999) 522–527. <814, 815>

[2747] B. Sunar and Ç. K. Koç, An efficient optimal normal basis type II multiplier, *IEEE Trans. Comput.* 50 (2001) 83–87. <813, 815>

[2748] A. V. Sutherland, Genus 1 point-counting record modulo a 5000+ digit prime, 2010, Posting to the Number Theory List, `http://listserv.nodak.edu/cgi-bin/wa.exe?A2=ind1007&amp;L=nmbrthry&amp;T=0&amp;F=&amp;S=&amp;P=287`. <779, 788>

[2749] A. V. Sutherland, On the evaluation of modular polynomials, ArXiv 1202.3985v3, to appear in the proceedings of the Tenth Algorithmic Number Theory Symposium ANTS-X, 2012. <779, 788>

[2750] R. G. Swan, Factorization of polynomials over finite fields, *Pacific J. Math.* 12 (1962) 1099–1106. <33, 46, 63, 64, 66, 91, 93>

[2751] N. Szabo and R. I. Tanaka, *Residue Arithmetic and its Application to Computer Technology*, McGraw-Hill, 1967. <346, 357>

[2752] P. Sziklai, On small blocking sets and their linearity, *J. Combin. Theory, Ser. A* 115 (2008) 1167–1182. <553, 556>

[2753] T. Szőnyi, On the number of directions determined by a set of points in an affine Galois plane, *J. Combin. Theory, Ser. A* 74 (1996) 141–146. <550, 556>

[2754] T. Szőnyi, Blocking sets in Desarguesian affine and projective planes, *Finite Fields Appl.* 3 (1997) 187–202. <553, 556>

[2755] T. Szőnyi, Around Rédei's theorem, *Discrete Math.* 208/209 (1999) 557–575. <555, 556>

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>

[2895] D. Wan, Rationality of partial zeta functions, *Indag. Math. (New Ser.)* 14 (2003) 285–292. <192, 195>

[2896] D. Wan, Variation of p-adic Newton polygons for L-functions of exponential sums, *Asian J. Math.* 8 (2004) 427–471. <477, 479, 481>

[2897] D. Wan, Mirror symmetry for zeta functions, In *Mirror Symmetry V*, volume 38 of *AMS/IP Stud. Adv. Math.*, 159–184, Amer. Math. Soc., Providence, RI, 2006. <190, 194, 195>

[2898] D. Wan, Algorithmic theory of zeta functions over finite fields, In *Algorithmic Number Theory: Lattices, Number Fields, Curves and Cryptography*, volume 44 of *Math. Sci. Res. Inst. Publ.*, 551–578, Cambridge Univ. Press, Cambridge, 2008. <485>

[2899] D. Wan, Lectures on zeta functions over finite fields, In *Higher-Dimensional Geometry over Finite Fields*, volume 16 of *NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur.*, 244–268, IOS, Amsterdam, 2008. <187, 190, 195>

[2900] D. Wan, Modular counting of rational points over finite fields, *Found. Comput. Math.* 8 (2008) 597–605. <483, 485>

[2901] D. Q. Wan, On a problem of Niederreiter and Robinson about finite fields, *J. Austral. Math. Soc., Ser. A* 41 (1986) 336–338. <221, 223>

[2902] D. Q. Wan, Permutation polynomials over finite fields, *Acta Math. Sinica (New Ser.)* 3 (1987) 1–5. <211, 216, 223>

[2903] D. Q. Wan, Zeros of diagonal equations over finite fields, *Proc. Amer. Math. Soc.* 103 (1988) 1049–1052. <203, 204, 207>

[2904] D. Q. Wan, An elementary proof of a theorem of Katz, *Amer. J. Math.* 111 (1989) 1–8. <193, 195>

[2905] D. Q. Wan, Permutation polynomials and resolution of singularities over finite fields, *Proc. Amer. Math. Soc.* 110 (1990) 303–309. <211, 223>

[2906] D. Q. Wan, A generalization of the Carlitz conjecture, In *Finite Fields, Coding Theory, and Advances in Communications and Computing*, volume 141 of *Lecture Notes in Pure and Appl. Math.*, 431–432, Dekker, New York, 1993. <211, 223>

[2907] D. Q. Wan, Newton polygons of zeta functions and L functions, *Ann. of Math., 2nd Ser.* 137 (1993) 249–293. <477, 481>

[2908] D. Q. Wan, A p-adic lifting lemma and its applications to permutation polynomials, In *Finite Fields, Coding Theory, and Advances in Communications and Computing*, volume 141 of *Lecture Notes in Pure and Appl. Math.*, 209–216, Dekker, New York, 1993. <210, 223, 226, 229>

[2909] D. Q. Wan, A classification conjecture about certain permutation polynomials, In *Finite Fields: Theory, Applications and Algorithms*, volume 168 of *Contemporary Math.*, 401–402, American Mathematical Society, Providence, RI, 1994. <221, 223>

[2910] D. Q. Wan, Permutation binomials over finite fields, *Acta Math. Sinica (New Ser.)* 10 (1994) 30–35. <211, 216, 223>

[2911] D. Q. Wan, A Chevalley-Warning approach to p-adic estimates of character sums, *Proc. Amer. Math. Soc.* 123 (1995) 45–54. <193, 195>

[2912] D. Q. Wan, Minimal polynomials and distinctness of Kloosterman sums, *Finite Fields Appl.* 1 (1995) 189–203. <149, 155>

[2913] D. Q. Wan and R. Lidl, Permutation polynomials of the form $x^r f(x^{(q-1)/d})$ and their group structure, *Monatsh. Math.* 112 (1991) 149–163. <214, 223>

[2914] D. Q. Wan, G. L. Mullen, and P. J.-S. Shiue, Erratum: "The number of permutation polynomials of the form $f(x) + cx$ over a finite field", *Proc. Edinburgh Math. Soc., Ser. II* 38 (1995) 133. <547, 548>

[2915] D. Q. Wan, G. L. Mullen, and P. J.-S. Shiue, The number of permutation polynomials of the form $f(x) + cx$ over a finite field, *Proc. Edinburgh Math. Soc., Ser. II* 38 (1995) 133–149. <221, 223, 547, 548>

[2916] D. Q. Wan, P. J.-S. Shiue, and C. S. Chen, Value sets of polynomials over finite fields, *Proc. Amer. Math. Soc.* 119 (1993) 711–717. <210, 223, 227, 229>

[2917] Z.-X. Wan, *Geometry of Classical Groups over Finite Fields*, Science Press, Beijing, second edition, 2002. <29, 30, 505, 507, 509, 512, 513, 514>

[2918] Z.-X. Wan, *Lectures on Finite Fields and Galois Rings*, World Scientific Publishing Co. Inc., River Edge, NJ, 2003. <11, 26, 27, 29, 30>

[2919] Z.-X. Wan, A shorter proof for an explicit formula for discrete logarithms in finite fields, *Discrete Math.* 308 (2008) 4914–4915. <390, 394>

[2920] Z.-X. Wan, *Finite Fields and Galois Rings*, World Scientific Publishing Co. Inc., Singapore, 2012. <29, 30>

[2921] Z.-X. Wan and K. Zhou, On the complexity of the dual basis of a type I optimal normal basis, *Finite Fields Appl.* 13 (2007) 411–417. <119, 122>

[2922] C. C. Wang, An algorithm to design finite field multipliers using a self-dual normal basis, *IEEE Trans. Comput.* 38 (1989) 1457–1460. <37, 46>

[2923] C. C. Wang, T. K. Truong, H. M. Shao, L. J. Deutsch, J. K. Omura, and I. S. Reed, VLSI architectures for computing multiplications and inverses in $GF(2^m)$, *IEEE Trans. Comput.* 34 (1985) 709–716. <811, 812, 815>

[2924] L. Wang, On permutation polynomials, *Finite Fields Appl.* 8 (2002) 311–322. <215, 223>

[2925] L. Wang and Y. Zhu, $F[x]$-lattice basis reduction algorithm and multisequence synthesis, *Sci. China, Ser. F* 44 (2001) 321–328. <324, 331>

[2926] L.-C. Wang and F.-H. Chang, Tractable rational map cryptosystem (version 2), `http://eprint.iacr.org/2004/046`, ver. 20040221:212731. <766, 775>

[2927] L.-C. Wang and F.-H. Chang, Tractable rational map cryptosystem (version 4), `http://eprint.iacr.org/2004/046`, ver. 20060203:065450. <766, 775>

[2928] L.-C. Wang, Y.-H. Hu, F. Lai, C.-Y. Chou, and B.-Y. Yang, Tractable rational map signature, In *Public Key Cryptography—PKC 2005*, volume 3386 of *Lecture Notes in Comput. Sci.*, 244–257, Springer, Berlin, 2005. <764, 775>

[2929] L.-C. Wang, B.-Y. Yang, Y.-H. Hu, and F. Lai, A "medium-field" multivariate public-key encryption scheme, In *Topics in Cryptology—CT-RSA 2006*, volume 3860 of *Lecture Notes in Comput. Sci.*, 132–149, Springer, Berlin, 2006. <766, 775>

[2930] L.-P. Wang and H. Niederreiter, Enumeration results on the joint linear complexity of multisequences, *Finite Fields Appl.* 12 (2006) 613–637. <324, 331>

[2931] L.-P. Wang, Y.-F. Zhu, and D.-Y. Pei, On the lattice basis reduction multisequence synthesis algorithm, *IEEE Trans. Inform. Theory* 50 (2004) 2905–2910. <324, 331>

[2932] M. Wang, Linear complexity profiles and continued fractions, In *Advances in Cryptology—EUROCRYPT '89*, volume 434 of *Lecture Notes in Comput. Sci.*, 571–585, Springer, Berlin, 1990. <323, 331>

[2933] M. Wang and I. F. Blake, Bit serial multiplication in finite fields, *SIAM J. Discrete Math.* 3 (1990) 140–148. <99, 103>

[2973] D. H. Wiedemann, Solving sparse linear equations over finite fields, *IEEE Trans. Inform. Theory* 32 (1986) 54–62. <344, 357, 393, 394, 523, 528>

[2974] D. Wiedermann, An iterated quadratic extension of GF(2), *Fibonacci Quart.* 26 (1988) 290–295. <60, 61>

[2975] M. J. Wiener and R. J. Zuccherato, Faster attacks on elliptic curve cryptosystems, In S. Tavares and H. Meijer, editors, *Selected Areas in Cryptography—SAC '98*, volume 1556 of *Lecture Notes in Computer Science*, 190–100, Springer-Verlag, Berlin, 1999. <777, 788>

[2976] M. L. H. Willems and J. A. Thas, A note on the existence of special Laguerre i-structures and optimal codes, *European J. Combin.* 4 (1983) 93–96. <579, 581>

[2977] M. Willett, Matrix fields over GF(q), *Duke Math. J.* 40 (1973) 701–704. <496, 503>

[2978] K. S. Williams, On general polynomials, *Canad. Math. Bull.* 10 (1967) 579–583. <227, 229>

[2979] K. S. Williams, On exceptional polynomials, *Canad. Math. Bull.* 11 (1968) 279–282. <226, 229>

[2980] K. S. Williams, Polynomials with irreducible factors of specified degree, *Canad. Math. Bull.* 12 (1969) 221–223. <362, 368>

[2981] V. V. Williams, Breaking the Coppersmith–Winograd barrier, 2011, preprint available at `http:cs.berkeley.edu/~virgi/matrixmult.pdf`. <352, 357, 376>

[2982] V. V. Williams, Multiplying matrices faster than Coppersmith-Winograd, In *Proceedings of the Forty Fourth Symposium on Theory of Computing*, STOC '12, 887–898, New York, NY, USA, 2012, ACM. <352, 357, 368, 374, 514, 528>

[2983] R. M. Wilson, Cyclotomy and difference families in elementary abelian groups, *J. Number Theory* 4 (1972) 17–47. <586, 591>

[2984] S. Winograd, On multiplication of 2×2 matrices, *Linear Algebra and Appl.* 4 (1971) 381–388. <517, 528>

[2985] S. Winograd, *Arithmetic Complexity of Computations*, SIAM, 1980. <806, 808, 809, 815>

[2986] A. Winterhof, On the distribution of powers in finite fields, *Finite Fields Appl.* 4 (1998) 43–54. <175, 179>

[2987] A. Winterhof, On Waring's problem in finite fields, *Acta Arith.* 87 (1998) 171–177. <169, 179, 206, 207>

[2988] A. Winterhof, Incomplete additive character sums and applications, In *Finite Fields and Applications*, 462–474, Springer, Berlin, 2001. <175, 179>

[2989] A. Winterhof, A note on Waring's problem in finite fields, *Acta Arith.* 96 (2001) 365–368. <206, 207>

[2990] A. Winterhof, Some estimates for character sums and applications, *Des. Codes Cryptogr.* 22 (2001) 123–131. <175, 179>

[2991] A. Winterhof, A note on the linear complexity profile of the discrete logarithm in finite fields, In *Coding, Cryptography and Combinatorics*, volume 23 of *Progr. Comput. Sci. Appl. Logic*, 359–367, Birkhäuser, Basel, 2004. <328, 331>

[2992] A. Winterhof and C. van de Woestijne, Exact solutions to Waring's problem for finite fields, *Acta Arith.* 141 (2010) 171–190. <206, 207>

[2993] E. Wirsing, Thin essential components, In *Topics in Number Theory*, 429–442. Colloq. Math. Soc. János Bolyai, Vol. 13, North-Holland, Amsterdam, 1976.