Laigle-Chapuy, Yann

Permutation polynomials and applications to coding theory. (English) Zbl 1107.11048

Finite Fields Appl. 13, No. 1, 58-70 (2007).

Using the characterization of permutation polynomials over the finite field F_q of the form $X^r f(X^{(q-1)/d})$ given by *D. Wan* and *R. Lidl* [Monatsh. Math. 112, No. 2, 149–163 (1991; Zbl 0737.11040)] the author exhibits a new class of permutation binomials. Moreover, he estimates the number of permutation binomials of the form $X^r(X^{(q-1)/m}+a)$, $a \in F_q$, using the Weil bound.

Finally, he gives some applications to coding theory mainly related to a conjecture of *T. Helleseth* [Discrete Math. 16, 209–232 (1976; Zbl 0348.94017)] on the existence of balanced words of the form $Tr(x^k + ax)$, $a \in F_{2^n}^*$, if $\gcd(k, 2^n - 1) = 1$.

Reviewer: Arne Winterhof (Linz)

MSC:

11T06 Polynomials over finite fields

Cited in **67** Documents

Keywords:

finite fields; permutation; permutation binomial; complete permutation; Niho exponent; balanced codeword; cross-correlation function; Boolean function

Full Text: DOI

References:

[1] Carlitz, L., Some theorems on permutation polynomials, Bull. amer. math. soc., 68, 120-122, (1962) · Zbl 0217.33003

[2] Carlitz, L.; Wells, C., The number of solutions of a special system of equations in a finite field, Acta arith., 12, 77-84, (1966/1967) · Zbl 0147.04003

[3] Charpin, P., Cyclic codes with few weights and niho exponents, J. combin. theory ser. A, 108, 247-259, (2004) · Zbl 1072.94016

[4] Chou, W.S., Binomial permutations of finite fields, Bull. austral. math. soc., 38, 3, 325-327, (1988) · Zbl 0648.12013

[5] Dickson, L.E., 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, 1-6, 161-183, (1896/97) · Zbl 28.0135.03

[6] H. Dobbertin, Kasami power functions, permutation polynomials and cyclic difference sets, in: Difference Sets, Sequences and Their Correlation Properties, Bad Windsheim, 1998, NATO Advanced Sciences Institutes Series C Mathematical and Physical Sciences, vol. 542, Kluwer Academic Publishers, Dordrecht, 1999, pp. 133-158. · Zbl 0946.05010

[7] H. Dobbertin, P. Felke, T. Helleseth, P. Rocendalh, Niho type cross-correlation functions via dickson polynomials and kloosterman sums, preprint. · Zbl 1178.94220

[8] Helleseth, T., Some results about the cross-correlation function between two maximal linear sequences, Discrete math., 16, 3, 209-232, (1976) · Zbl 0348.94017

[9] Hermite, C., Sur LES fonctions de sept lettres, C. R. acad. sci. Paris, 57, 750-757, (1863)

[10] Janphaisaeng, S.; Laohakosol, V.; Harnchoowong, A., Some new classes of permutation polynomials, Sci. Asia, 28, 401-405, (2002)

[11] Levine, J.; Brawley, J.V., Some cryptographic applications of permutation polynomials, Cryptologia, 1, 76-92, (1977)

[12] Levine, J.; Chandler, R., Some further cryptographic applications of permutation polynomials, Cryptologia, 11, 4, 211-218, (1987)

[13] R. Lidl, On cryptosystems based on polynomials and finite fields, in: Advances in Cryptology, Paris, 1984, Lecture Notes in Computer Science, vol. 209, Springer, Berlin, 1985, pp. 10-15.

[14] Lidl, R.; Mullen, G.L., When does a polynomial over a finite field permute the elements of the field?, Amer. math. monthly, 95, 243-246, (1988) · Zbl 0653.12010

[15] Lidl, R.; Mullen, G.L., When does a polynomial over a finite field permute the elements of the field?, Amer. math. monthly, 100, 71-74, (1993) · Zbl 0777.11054

[16] Lidl, R.; Müller, W.B., A note on polynomials and functions in algebraic cryptography, Ars combin., 17, A, 223-229, (1984) · Zbl 0539.94018

[17] Lidl, R.; Müller, W.B., Permutation polynomials in RSA-cryptosystems, (), 293-301

[18] R. Lidl, H. Niederreiter, Finite fields, Encyclopedia of Mathematics and its Applications, vol. 20, second ed., Cambridge University Press, Cambridge, 1997 (With a foreword by P.M. Cohn).

[19] Mullen, G.L.; Niederreiter, H., Dickson polynomials over finite fields and complete mappings, Canad. math. bull., 30, 1, 19-27, (1987) · Zbl 0576.12020

[20] Müller, W.B.; Nöbauer, W., Some remarks on public-key cryptosystems, Studia sci. math. hungar., 16, 1-2, 71-76, (1981) · Zbl 0476.94016

[21] Niederreiter, H.; Robinson, K.H., Complete mappings of finite fields, J. austral. math. soc. ser. A, 33, 2, 197-212, (1982) · Zbl 0495.12018

[22] Y. Niho, Multi-valued cross-correlation function between two maximal linear recursive sequences, Ph.D. Thesis, University of Southern California, Los Angeles, CA, 1975.

[23] Small, C., Permutation binomials, Internat. J. math. math. sci., 13, 2, 337-342, (1990) · Zbl 0702.11085

[24] Turnwald, G., Permutation polynomials of binomial type, (), 281-286

[25] Wan, D.Q., On a problem of Niederreiter and Robinson about finite fields, J. austral. math. soc. ser. A, 41, 3, 336-338, (1986) · Zbl 0607.12009

[26] Wan, D.Q.; Lidl, R., Permutation polynomials of the form $x^r f(x^{(q - 1) / d})$ and their group structure, Monatsh. math., 112, 2, 149-163, (1991) · Zbl 0737.11040

[27] Wang, L., On permutation polynomials, Finite fields appl., 8, 3, 311-322, (2002) · Zbl 1044.11103