Article ID: 1000-341X(2006)02-0219-08 **Document code**: A

On Dickson Polynomials and Difference Sets

CAO Xi-wang[1], *QIU Wei-sheng*[2]

(1. School of Math. Sci., Nanjing University of Aeronautics and Astronautics, Jiangsu 210016, China;
2. School of Mathematical Sciences, Peking University, Beijing 100871, China)
(E-mail: xwcao@nuaa.edu.cn)

Abstract: In 1998, Maschietti constructed several cyclic difference sets from monomial hyperovals. R. Evans, H.D.L. Holloman, C. Krattnthaler and Qing Xiang gave an algebraic proof of the two autocorrelation property of the related binary sequence. In this paper, we show that hyperovals are very closely related to two-to-one maps, and then we proceed to generalize Maschietti's result.

Key words: cyclic difference sets; permutation polynomials; hyperovals; two-to-one maps; binary sequences.
MSC(2000): 05B10, 51E20, 05B25, 94B27
CLC number: O152.6, O157.2, O157.4

1. Introduction

The correlation properties of binary sequences are important in code-division multiple access (CDMA) spread spectrum communications[1,2]. It is well-known that the existence of a balance binary sequence of period 2^m-1 for some integer m having a two level autocorrelation function is equivalent to that of a cyclic difference set with parameters $(2^m-1, 2^{m-1}-1, 2^{m-2}-1)$. For the definition and properties of difference sets, we refer the reader to D. Jungnickel[3], A. Pott[4].

In [5], Maschietti constructed a family of cyclic difference sets with Singer parameters using hyperovals in certain projective geometries. This is a remarkable result, since it can be proved that the difference sets constructed from Maschietti's method may be new! Evans R., Holloman H.D.L., Krattnthaler C. and Qing Xiang[6] gave a simple algebraic proof of Maschietti's results immediately after maschietti's paper published. In this paper, we show that hyperovals are very closely related to the so called two-to-one maps, then we proceed to generalize Maschietti's result.

The paper is organized in 4 sections. In Section 2, we give some preliminary results; In Section 3, we show that the existence of hyperovals is equivalent to the existence of some two-to-one maps; In Section 4, we give a family of cyclic difference sets which is a generalization of Maschiettii's result.

2. Basic definition and preliminary results

If G is a group of order v, a (v,k,λ) difference set in G is a k-subset D of G such that the list of differences gh^{-1} $(g,h\in G)$ contains each element $g(\neq e)$ of G exactly λ times. We

Received date: 2004-05-09

identify any subset S of G with the group ring element $\sum_{g\in S} g$ in the group ring $\mathbf{Z}[G]$, and denote $\sum_{g\in G} a_g g^t$ by $A^{(t)}$ when $A=\sum_{g\in G} a_g g$. With these notations, it is obvious that D is a (v,k,λ) difference set in G if and only if the following equation holds in $\mathbf{Z}[G]$:

$$DD^{(-1)} = n + \lambda G, \tag{2.1}$$

where $n=k-\lambda$. If D is (v,k,λ) difference set in G, then $\overline{D}$, the complement of D in G, is also a difference set in G with parameters $(v, v-k, v-2k+\lambda)$. D is called a cyclic difference set in G if G is a cyclic group.

By $PG(2,q)$ we denote the projective plane of order q, a k-arc of $PG(2,q)$ is a set of k distinct points in $PG(2,q)$ such that no three of them are collinear. It is well-known that the maximum of k is $q+1$ or $q+2$ according as q is odd or even. When q is odd, a $(q+1)$- arc is called an oval, and when q is even, a $(q+2)$- arc is called an hyperoval of $PG(2,q)$. In $PG(2,q)$, the Desarguesian plane over the Galois field F_q, every nonsigular conic is a $(q+1)$-arc, the converse is true when q is odd[7]. If q is even, the $(q+1)$-unisecants to a $(q+1)$-arc $\mathcal{K}$ in $PG(2,q)$ are concurrent, the point of the concurrence is called a nuclear, so a $(q+1)$-arc can be uniquely completed to a hyperoval by adding the nuclear[7,8,9].

Now we recall some basic results which will be used later.

Lemma 2.1[7] *By $\mathcal{K}$ we denote a k-arc in $PG(2,q)$, then for any point Q in $PG(2,q)$, one has*

$$\sigma_1(Q) + 2\sigma_2(Q) = k,$$

where $\sigma_i(Q)$ is the number of i-secants through Q. A 2-secant is called a bisecant and a 1-secant is called a unisecant, a 0-secant is an external line.

Two hyperovals are called equivalent if one hyperoval can be transformed to the other by a projective linear transformation, i.e., an element of $PGL(3,q)$. By the fundamental theorem of projective geometry, the group $PGL(3,q)$ is transitive on the quadrangles ([8], Theorem 2.12), thus every hyperoval can be mapped to a hyperoval containing the fundamental quadrangle $(1,0,0),(0,1,0),(0,0,1),(1,1,1)$.

Lemma 2.2 (Seger's Theorem, see for example, [7], Theorem 8.22, Page 184, or [9]) *Every hyperoval can be written in the form*

$$D(f) = \{(1,t,f(t)) | t\in F_q\} \cup \{(0,1,0),(0,0,1)\},$$

where f is a permutation polynomial of degree at most $q-2$, satisfying $f(0)=0, f(1)=1$, and for each $s\in F_q$, the polynomial

$$f_s(x) = \begin{cases} \frac{f(x+s)+f(s)}{x} & x\neq 0, \\ 0 & otherwise \end{cases}$$

is also a permutation on F_q.

Let $\tau: F_{2^m} \to F_{2^m}$ be defined by

$$\tau(x) = x + x^h,$$

and Im(τ) be the image of the map τ, the following two lemmas are due to Maschiettii[5].

Lemma 2.3 *Let $q = 2^m$, the $(q+2)$-set*

$$D(f) = \{(1, t, t^h)|t \in F_q\} \cup \{(0, 1, 0), (0, 0, 1)\}$$

in $PG(2, q)$ is a hyperoval if and only if $\gcd(h, q-1) = 1$, *and τ is a two-to-one map from F_q to itself. Where a two-to-one map τ means that every image of τ has exactly 2 pre-images.*

Lemma 2.4 *Let $q = 2^m$, if the $(q+2)$-set*

$$D(f) = \{(1, t, t^h)|t \in F_q\} \cup \{(0, 1, 0), (0, 0, 1)\}$$

is a hyperoval in $PG(2, q)$, then $D_{h,m} = \mathrm{Im}(\tau)\backslash\{0\}$ is a $(q-1, q/2-1, q/4-1)$ cyclic difference set in F_q^*.

The following two lemmas are well-known.

Lemma 2.5[10] *If χ_1 and χ_2 are two multiplicative characters of F_q^*, the Jacobi sum is defined by*

$$J(\chi_1, \chi_2) = \Sigma_{x \in F_q} \chi_1(x)\chi_2(1-x),$$

then

$$J(\chi_1, \chi_2)\overline{J(\chi_1, \chi_2)} = q.$$

Lemma 2.6[11] *Let G be an abelian group of order v, then a k-subset D of G is a difference set if and only if*

$$\chi(D)\overline{\chi(D)} = k - \lambda,$$

for every nontrivial multiplicative character χ of G, where $\chi(D)$ stands for $\Sigma_{d \in D}\chi(d)$.

3. Hyperovals and two-to-one maps

Firstly, we have the following simple proposition.

Proposition 3.1 *Let $\mathcal{K}$ be a k-arc in a projective plane $PG(2, q)$, if every line has 0 or 2 points in common with $\mathcal{K}$, i.e., every line is either a bisecant or an external line with regard to $\mathcal{K}$, then $\mathcal{K}$ is a hyperoval.*

Proof [1]This proposition is well-known, but we have not seen a proof in literature, so we give a short proof here based on Lemma 2.1.

Let Q be a point not on $\mathcal{K}$, by Lemma 2.1, we have

$$\sigma_1(Q) + 2\sigma_2(Q) = k. \tag{3.1}$$

[1] The authors would like to express their gratefulness to Professor Huiling Li for giving them a simple proof of this Proposition.

Since every line is either a bisecant or an external line with regard to $\mathcal{K}$ by the hypothesis, we have $\sigma_1(Q)=0$, so by (3.1), we have $\sigma_2(Q)=k/2$. Counting the pairs of points and lines in the set

$$E=\{(Q,l)|Q\in PG(2,q)\backslash\mathcal{K},\ l\ \textit{ is a bisecant passing through }\ Q\}$$

in two difference ways: Firstly, for a fixed line l, l has $q+1$ points, but l is a bisecant which means that l meets $\mathcal{K}$ in two points, so there are $q-1$ choices of the point Q, we note that $Q\in PG(2,q)\backslash\ \mathcal{K}$. Now, let l run, since it meets $\mathcal{K}$ in two points, in other words, each pair of points on $\mathcal{K}$ determines such a line, and vice versa. Therefore, the total number of l is $\binom{k}{2}=\frac{k(k-1)}{2}$. So we have

$$|E|=(q-1)\frac{k(k-1)}{2}.$$

Secondly, for a fixed point Q, we proved that $\sigma_2(Q)=k/2$ as before going, and there are $(q^2+q+1-k)$ choices of Q, hence we obtain that

$$|E|=\frac{k}{2}(q^2+q+1-k).$$

As a consequence,

$$(q-1)\frac{k(k-1)}{2}=\frac{k}{2}(q^2+q+1-k),$$

which implies $k=q+2$.

Since every line meets $\mathcal{K}$ in 0 or 2 points, no three points on $\mathcal{K}$ are collinear, therefore, $\mathcal{K}$ is a hyperoval.

The proof of the necessity is trivial, and the result follows. This completes the proof. □

Now we show that the existence of hyperovals is equivalent to that of certain two-to-one maps.

Proposition 3.2 *Suppose that $f(x)$ is a permutation polynomial, then*

$$D(f)=\{(1,t,f(t))|t\in F_q\}\cup\{(0,1,0),(0,0,1)\}$$

is a hyperoval if and only if for each $a\in F_q^*$, $\tau(x)=ax+f(x)$ is a two-to-one map.

Proof If $D(f)$ is a hyperoval, then any line of the affine equation $y=-ax+b$ meets $D(f)$ at either 0 or 2 points, which implies that the equation $ax+f(x)=b$ has either 0 or 2 solutions in F_q, and $\tau(x)=ax+f(x)$ is a two-to-one map.

Conversely, if $\tau(x)=ax+f(x)$ is a two-to-one map, it is straightforward to show that a line of $PG(2,q)$ with homogeneous equation $cy=ax+bz$ with $b=0$ intersects $D(f)$ at 0 or 2 points. It remains to show that the line $z=-ax+b$ meets $D(f)$ at 0 or 2 points.

Since

$$\left\{\begin{array}{ll} z= & -ax+b \\ z= & f(x)\end{array}\right. \Leftrightarrow ax+f(x)=b,$$

so each line intersects $D(f)$ in 0 or 2 points. By Proposition 3.1, $\mathcal{K}$ is a hyperoval. □

Corollary 3.3 *If $f(x)$ is a permutation polynomial, then $\tau(x)=ax+f(x)$ is a two-to-one map* *if and only if $f_s(x)$ is a permutation polynomial for each $s \in F_q$, where $f_s(x)$ is defined as before.*

Proof If $f_s(x)$ is a permutation polynomial, then by Seger's theorem (Lemma 2.2), $D(f)$ is a hyperoval, so $\tau(x) = ax + f(x)$ is a two-to-one map by Proposition 3.2.

Conversely, if $\tau(x) = ax + f(x)$ is a two-to-one map, by Proposition 3.2 again, we know $D(f)$ is a hyperoval. Suppose that $f_s(T) = f_s(T')$ for some $T \neq T'$, let $a = T + s, b = T' + s$, then

$$f_s(T) = f_s(T') \Leftrightarrow \frac{f(T+s)+f(s)}{T} = \frac{f(T'+s)+f(s)}{T'}$$

$$\Leftrightarrow \frac{f(a)+f(s)}{a+s} = \frac{f(b)+f(s)}{b+s} \Leftrightarrow \begin{vmatrix} 1 & a & f(a) \\ 1 & b & f(b) \\ 1 & s & f(s) \end{vmatrix} = 0$$

$\Leftrightarrow$ the points $(1, a, f(a)), (1, b, f(b)), (1, s, f(s))$ are collinear, which is a contradiction with that $D(f)$ is a hyperoval. □

Corollary 3.4 *If $f(x)$ is a permutation polynomial, then $\tau(x) = ax + f(x)$ is a two-to-one map for each $a \in F_q^*$ if and only if*

$$\tau_s(x) = \begin{cases} \frac{\tau(x+s)+\tau(s)}{x} & x \neq 0, \\ 0 & otherwise \end{cases}$$

is a permutation polynomial.

The proof is similar to that of Corollary 3.3, omitted. □

4. Two-to-one maps and difference sets

In this section, we proceed to generalize Maschietti's result. Generally speaking, we have the following

Proposition 4.1 *Let $q = 2^m$, $\tau(x) = x^t + x^{t+k}$, with $\gcd(k, q-1) = 1$, and $\gcd(tk^{-1}+1, q-1) = 1$, where k^{-1} is the inverse of $k \in \mathbf{Z}_{q-1}$, then $D_{t,k,m} = \mathrm{Im}(\tau)\backslash\{0\}$ is a $(q-1, q/2-1, q/4-1)$ difference set provided that τ is a two-to-one map.*

Proof Let χ be a nontrivial multiplicative character of F_q^*. Since τ is a two-to-one map, we have

$$\chi(D_{t,k,m}) = \frac{1}{2}\Sigma_{x\in F_q}\chi(x^t + x^{t+k}) = \frac{1}{2}\Sigma_{x\in F_q}\chi(x^t)\chi(1 + x^k).$$

Since $\gcd(k, q-1) = 1$, $y = x^k$ is a permutation polynomial of F_q. If we denote $\varphi(y) = \chi(x^t) = \chi(y^{tk^{-1}})$, then direct calculation shows that φ is a multiplicative character of F_q^*, and $\varphi\chi$ is not trivial.

Hence

$$\chi(D_{t,k,m}) = \frac{1}{2}\Sigma_{y\in F_q}\varphi(y)\chi(1 + y) = \frac{1}{2}J(\varphi, \chi),$$

where $J(\varphi, \chi)$ is the Jacobi sum of φ and χ.

It is well-known that (Lemma 2.5): $J(\varphi, \chi)\overline{J(\varphi, \chi)} = q$. Hence

$$\chi(D_{t,k,m})\overline{\chi(D_{t,k,m})} = 2^{m-2}.$$

By the result of Turyn (Lemma 2.6), we obtain that $D_{t,k,m}$ is a difference set in F_q^*. □

Obviously, when $t=1$, the above proposition is precisely the Maschietti's result.

The following theorem is a generalization of Proposition 4.1.

Theorem 4.2 *Suppose that $g(x)$ is a permutation polynomial on $F_q, q=2^m$, t is even, $\sum_{i=1}^t a_i \neq 0, \sum_{i=1}^t k_i \neq 0$, $\gcd(k_i, q-1)=1, i=1,2,\cdots,t$. Let $f(x)=\prod_{i=1}^t (g(x)+a_i)^{k_i}$, if $f(x)$ is a 2^u to one map, i.e. each image of $f(x)$ has precisely 2^u pre-images. Then $D_f=\mathrm{Im}(f(x))\backslash\{0\}$ is difference sets in F_q^*.*

Proof For any non-trivial character χ of F_q^*, since $f(x)$ is a 2^u to one map, we have

$$\begin{aligned}2^u\chi(D_f) &= \sum_{x\in F_q}\chi(f(x)) = \sum_{x\in F_q}\chi(\prod_{i=1}^t (g(x)+a_i)^{k_i})\\ &= \sum_{x\in F_q}\prod_{i=1}^t \chi^{k_i}(g(x)+a_i) = \sum_{x\in F_q}\chi^{\sum_{i=1}^t k_i}(\sum_{i=1}^t a_i)\prod_{i=1}^t \chi^{k_i}(\frac{g(x)+a_i}{\sum_{i=1}^t a_i})\\ &= \chi^{\sum_{i=1}^t k_i}(\sum_{i=1}^t a_i)J(\chi^{k_1},\cdots,\chi^{k_t}).\end{aligned}$$

Note that the last identity is based on the fact that t is even, so

$$\sum_{i=1}^t \frac{g(x)+a_i}{\sum_{i=1}^t a_i} = 1+\frac{tg(x)}{\sum_{i=1}^t a_i}=1.$$

By ([12], Theorem 4, page 101), one has that

$$|J(\chi^{k_1},\cdots,\chi^{k_t})| = q^{(t-1)/2}.$$

Hence, $\chi(D_f)\overline{\chi(D_f)} = 2^{m(t-1)-2u}$. By Lemma 2.6, $D(f)$ is a (v,k,λ) difference sets in F_q^*. □

Remark 4.3 (1) When $t=2$, the above theorem provides difference sets with Singer parameters. See Guohua Xiong[13].

(2) Using Theorem 4.2, one can construct binary sequences with ideal correlation functions.

Now we give an example which illustrating our construction works indeed.

Example The Dickson polynomial $D_n(x,a)$ of type I is

$$D_n(x,a)=\sum_{i=0}^{\lfloor n/2\rfloor}\frac{n}{n-i}\left(\begin{array}{c} n-i\\ i\end{array}\right)(-a)^i x^{n-2i},$$

where x is an indeterminate, $a\in R$, a communicative ring. $\lfloor n/2\rfloor$ stands for the biggest integer less than or equal to $n/2$. Whenever $n=0$, define $D_0(x,a)=2$. Denote $D_n(x,1)$ simply by $D_n(x)$. It is well know that $D_n(x,a)$ is a permutation on F_q if and only if $\gcd(n,q^2-1)=1$ (cf, [14], Theorem 3.2, page 38). Suppose that n is indeed that case, we define $f(x)$ as

$$f(x)=(D_n(x))^{5l}(D_n(x)+1)^l,$$

where l satisfying $\gcd(l, q-1) = 1, q = 2^d$, and $d \geq 5$ is odd. Since

$$f(x) = (D_n(x) + D_n(x)^6)^l = (y + y^6)^l,$$

and $g(y) = y^6$ correspond to the Seger hyperoval, so $f(x)$ is a two to one map. By Theorem 4.2, $D(f)$ is a difference set in F_q^*. Particularly, let $q = 2^7$, α be a primitive element in $GF(2^7)$ with $\alpha^7 + \alpha + 1 = 0$. Taking $n = 5, l_1 = 2$, we have

$$D_5(x) = x + x^3 + x^5,$$

$$f_1(x) = x^2 + x^6 + x^{10} + x^{12} + x^{20} + x^{36} + x^{52} + x^{60}.$$

Denote $C_j = \{\alpha^{j2^i}, i = 0, 1, 2, \cdots, 6\}$, direct calculation shows that

$$D_{f_1} = C_3 \cup C_7 \cup C_9 \cup C_{13} \cup C_{21} \cup C_{23} \cup C_{27} \cup C_{29} \cup C_{55}.$$

If we take $l_2 = 3$, and the left parameters remains unchanged. Then

$$\begin{aligned} f_2(x) =& x^3 + x^5 + x^8 + x^9 + x^{17} + x^{18} + x^{21} + x^{22} + x^{23} + x^{24} + x^{54} + \\ & x^{25} + x^{26} + x^{37} + x^{39} + x^{40} + x^{41} + x^{50} + x^{53} + x^{55} + x^{57} + \\ & x^{58} + x^{61} + x^{63} + x^{65} + x^{82} + x^{86} + x^{90}, \\ D_{f_2} =& C_9 \cup C_{11} \cup C_{13} \cup C_{19} \cup C_{21} \cup C_{27} \cup C_{29} \cup C_{47} \cup C_{63}. \end{aligned}$$

Utilizing Hall polynomials or the basic Equation (2.1), one can check that $D(f_i), i = 1, 2$ are difference sets in $F_{2^7}^*$. We verified these facts by my computer (IBM R50e) using the software Mathematica 4.0, the machine time is less than one second.

Acknowledgment The authors would like to express their gratefulness to the referees for valuable comments and suggestions.

References:

[1] GOLOMB S W. *The Use of Combinatorial Structures in Communication Signal Design* [M]. Applications of Combinatorial Mathematics (Oxford, 1994), 59–78, Inst. Math. Appl. Conf. Ser. New Ser., 60, Oxford Univ. Press, New York, 1997.

[2] SIMON M K, OMURA J K, SCHOLTZ R A. et al. *Spectrum Communications (1)* [M]. New York: MA Computer Science Press, 1985.

[3] JUNGNICKEL D. *Difference Sets* [M]. Contemporary Design Theory, A Collection of Surveys, J. Dinitz, D.R. Stinson, eds., Wiley-interscience Series in Discrete Mathematics and optimization, New York: Wiley, 1999, 241-324

[4] POTT A. *Finite Geometry and Character Theory* [M]. Springer-Verlag, Berlin, 1995.

[5] MASCHIETTI A. *Difference sets and hyperovals* [J]. Des. Codes Cryptogr., 1998, **14**: 89–98.

[6] EVANS R, HOLLMANN H D L, KRATTENTHALER C. et al. *Gauss sums, Jacobi sums, and p-ranks of cyclic difference sets* [J]. J. Combin. Theory Ser. A, 1999, **87**: 74–119.

[7] HIRSCHFELD J W P. *Projective Geometries over Finite Fields* [M], 2nd edition, Oxford: Oxford University Press, 1998, 176–200

[8] HUGHES D R, PIPER F C. *Projective Plane* [M]. New York: Springer-Verlag, 1993.

[9] SEGER B. *Ovals in a finite projective plane* [J]. Canad. J. Math., 1955, **7**: 414–416.

[10] LANG S. *Cyclotomic Fields* [M]. Combined 2nd edition, New York: Spring-Verlag, 1990.

[11] TURYN R J. *Character sums and difference sets* [J]. Pacific J. Math., 1965, **15**: 319–346.

[12] IRELAND K, ROSEN M. *A Classical Introduction to Modern Number Theory* [M]. Second Edition, New York: Springer-Verlag, 1990.

[13] XIONG Guo-hua. *Constructing abelian difference sets, sequences, and crypoto-functions* [D]. Ph D Thesis, Beijing: Peking University, 2002.

[14] LIDL R, MULLEN G L, TURNWARD G. *Dickson Polynomials* [M]. Pitman Monographs and Surveys in Pure and Applied Mathematics, 65. Longman Scientific & Technical, Harlow; Copublished in the United States with John Wiley & Sons, Inc., New York, 1993.

Dickson 多项式与差集

曹喜望[1]，丘维声[2]

(1. 南京航空航天大学理学院数学系，江苏 南京 210016; 2. 北京大学数学科学学院，北京 100871)

摘要: 1998 年，Maschietti 用超卵形线构造了几个循环差集. R.Evans, H.D.L. Holloman, C.Krattnthaler 与 Qing Xiang 等给出了其对应的二元序列具有良好自相关函数的简单代数证明. 在本文中，证明了超卵形线与二对一映射有着紧密的联系，并且推广了 Maschietti 的结果.

关键词: 循环差集；置换多项式；超卵形线；二对一映射；二元序列.