Some Basic Results Concerning Permutation Polynomials over Finite Fields

Gary L. Mullen

Penn State University

mullen@math.psu.edu

July 23, 2010

F_q finite field order $q = p^e$

value set of $f \in F_q[x]$, $V_f = \{f(a) | a \in F_q\}$

f is Perm. Poly. (PP) if $|V_f| = q$

Some Basic Properties of PPs over F_q

1. If $f(x)$ is PP, so is $af(x+b)+c$ for $a \neq 0, b, c \in F_q$

Some Basic Properties of PPs over F_q

1. If $f(x)$ is PP, so is $af(x+b)+c$ for $a \neq 0, b, c \in F_q$
2. $q!$ total; group under comp. mod $x^q - x$ iso. S_q, sym. group

Some Basic Properties of PPs over F_q

1. If $f(x)$ is PP, so is $af(x+b)+c$ for $a \neq 0, b, c \in F_q$
2. $q!$ total; group under comp. mod $x^q - x$ iso. S_q, sym. group
3. Normalized if monic, $f(0) = 0$, and coeff. of x^{n-1} is 0 if deg. n not divisible by p

Some Basic Properties of PPs over F_q

1. If $f(x)$ is PP, so is $af(x+b)+c$ for $a \neq 0, b, c \in F_q$
2. $q!$ total; group under comp. mod $x^q - x$ iso. S_q, sym. group
3. Normalized if monic, $f(0) = 0$, and coeff. of x^{n-1} is 0 if deg. n not divisible by p
4. L/N p 352 list of all nor. PPs of deg. < 6

Some Basic Properties of PPs over F_q

1. If $f(x)$ is PP, so is $af(x+b)+c$ for $a \neq 0, b, c \in F_q$
2. $q!$ total; group under comp. mod $x^q - x$ iso. S_q, sym. group
3. Normalized if monic, $f(0) = 0$, and coeff. of x^{n-1} is 0 if deg. n not divisible by p
4. L/N p 352 list of all nor. PPs of deg. < 6
5. x^n PP on F_q iff $(n, q-1) = 1$

Some Basic Properties of PPs over F_q

1. If $f(x)$ is PP, so is $af(x+b)+c$ for $a \neq 0, b, c \in F_q$
2. $q!$ total; group under comp. mod $x^q - x$ iso. S_q, sym. group
3. Normalized if monic, $f(0)=0$, and coeff. of x^{n-1} is 0 if deg. n not divisible by p
4. L/N p 352 list of all nor. PPs of deg. < 6
5. x^n PP on F_q iff $(n, q-1) = 1$
6. Linearized polys. $f(x) = \sum a_i x^{p^i}$ PP iff $det(A_f) \neq 0$

Some Basic Properties of PPs over F_q

1. If $f(x)$ is PP, so is $af(x+b)+c$ for $a \neq 0, b, c \in F_q$
2. $q!$ total; group under comp. mod $x^q - x$ iso. S_q, sym. group
3. Normalized if monic, $f(0)=0$, and coeff. of x^{n-1} is 0 if deg. n not divisible by p
4. L/N p 352 list of all nor. PPs of deg. < 6
5. x^n PP on F_q iff $(n, q-1) = 1$
6. Linearized polys. $f(x) = \sum a_i x^{p^i}$ PP iff $det(A_f) \neq 0$
7. If q odd, $x^{(q+1)/2} + ax$ contains $(q-3)/2$ PPs

Some Basic Properties of PPs over F_q

1. If $f(x)$ is PP, so is $af(x+b)+c$ for $a \neq 0, b, c \in F_q$
2. $q!$ total; group under comp. mod $x^q - x$ iso. S_q, sym. group
3. Normalized if monic, $f(0) = 0$, and coeff. of x^{n-1} is 0 if deg. n not divisible by p
4. L/N p 352 list of all nor. PPs of deg. < 6
5. x^n PP on F_q iff $(n, q-1) = 1$
6. Linearized polys. $f(x) = \sum a_i x^{p^i}$ PP iff $det(A_f) \neq 0$
7. If q odd, $x^{(q+1)/2} + ax$ contains $(q-3)/2$ PPs
8. $x^r(f(x^s))^{(q-1)/s}$ PPs and group structure

Some Basic Properties of PPs over F_q

1. If $f(x)$ is PP, so is $af(x+b)+c$ for $a \neq 0, b, c \in F_q$
2. $q!$ total; group under comp. mod $x^q - x$ iso. S_q, sym. group
3. Normalized if monic, $f(0) = 0$, and coeff. of x^{n-1} is 0 if deg. n not divisible by p
4. L/N p 352 list of all nor. PPs of deg. < 6
5. x^n PP on F_q iff $(n, q-1) = 1$
6. Linearized polys. $f(x) = \sum a_i x^{p^i}$ PP iff $det(A_f) \neq 0$
7. If q odd, $x^{(q+1)/2} + ax$ contains $(q-3)/2$ PPs
8. $x^r(f(x^s))^{(q-1)/s}$ PPs and group structure
9. M, Handbook Combin. Designs, Sec. Ed., (CRC 07), 572-574

1. $|V_{x^n}| = 1 + \frac{q-1}{(n,q-1)}$

1. $|V_{x^n}| = 1 + \frac{q-1}{(n,q-1)}$
2. **Das/M** (Fq 6, Springer, 02) $|V_f| \geq L_f + 2$ where L_f is max # 0s in any col. of matrix A_f

1. $|V_{x^n}| = 1 + \frac{q-1}{(n,q-1)}$
2. **Das/M** (Fq 6, Springer, 02) $|V_f| \geq L_f + 2$ where L_f is max # 0s in any col. of matrix A_f
3. **Mills** (Pac. J. Math. 64) If f monic deg. $n < \sqrt{q}$ with $(n,q) = 1$ and $|V_f| = \lfloor (q-1)/n \rfloor + 1$, then $n|(q-1)$ and $f(x) = (x+b)^n + c$

Dickson Polynomials

Dickson poly. deg. n, parameter $a \in F_q$

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

(i) Let $T_n(x) = \cos\,(n \arccos x)$ be Chebyshev poly. first kind.

Then over C, $D_n(2x,1) = 2T_n(x)$.

(ii) Recurrence: $D_n(x,0) = x^n$

$D_{n+2}(x,a) = xD_{n+1}(x,a) - aD_n(x,a), n \geq 0$ with
$D_0(x,a) = 2, D_1(x,a) = x$

Theorem

(Funct. eq.) $D_n(x,a) = y^n + \frac{a^n}{y^n}$ *with* $x = y + a/y$, $y \in F_{q^2}$

Theorem

(Funct. eq.) $D_n(x,a) = y^n + \frac{a^n}{y^n}$ *with* $x = y + a/y$, $y \in F_{q^2}$

Theorem

Dickson *(Ann Math 1897) If* $a \neq 0 \in F_q$, $D_n(x,a)$ *PP on* F_q *iff* $(n, q^2 - 1) = 1$.

Theorem

(Funct. eq.) $D_n(x,a) = y^n + \frac{a^n}{y^n}$ *with* $x = y + a/y$, $y \in F_{q^2}$

Theorem

Dickson *(Ann Math 1897) If* $a \neq 0 \in F_q$, $D_n(x,a)$ *PP on* F_q *iff* $(n, q^2-1) = 1$.

Theorem

Chou/Gomez-Calderon/M *(JNT 88) For* $a \neq 0 \in F_q$

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

$\alpha = 0, 1/2, 1$

Theorem

(i) x^n *PP on* F_p *for* ∞ *ly many primes* p *iff* $(n, 2) = 1$
(ii) If $a \neq 0$, $D_n(x, a)$ *PP on* F_p *for* ∞ *ly many primes* p *iff* $(n, 6) = 1$.

Theorem

(i) x^n *PP on* F_p *for* ∞ *ly many primes* p *iff* $(n, 2) = 1$
(ii) If $a \neq 0$, $D_n(x, a)$ *PP on* F_p *for* ∞ *ly many primes* p *iff* $(n, 6) = 1$.

Conjecture

Schur *(1922) If* $f \in Z[x]$ *and* f *PP on* F_p *for* ∞ *ly primes* p, *then* f *is a composition of* $ax^k + b$ *and DPs* $D_n(x, a)$

Theorem

Fried *(Mich. Math. J. 70) Schur conj. true*

Theorem

Fried *(Mich. Math. J. 70) Schur conj. true*

Theorem

Turnwald *(J. Austral. Math. Soc., 95) Schur conj. true, no complex. anal.*

Theorem

Fried *(Mich. Math. J. 70) Schur conj. true*

Theorem

Turnwald *(J. Austral. Math. Soc., 95) Schur conj. true, no complex. anal.*

See **Lidl/M/Turnwald**, "Dickson Polys.," 1993

A DIFFERENT PERSPECTIVE

Xiang-dong Hou/M/James Sellers/Joe Yucas (FFA 09)

A DIFFERENT PERSPECTIVE

Xiang-dong Hou/M/James Sellers/Joe Yucas (FFA 09)

Consider $D_n(x, a)$ but now fix x, and let a be the variable.

$D_n(x, a)$ is a reversed Dickson poly. (RDP)

A DIFFERENT PERSPECTIVE

Xiang-dong Hou/M/James Sellers/Joe Yucas (FFA 09)

Consider $D_n(x, a)$ but now fix x, and let a be the variable.

$D_n(x, a)$ is a reversed Dickson poly. (RDP)

Problem

When do RDPs yield PPs?

A DIFFERENT PERSPECTIVE

Xiang-dong Hou/M/James Sellers/Joe Yucas (FFA 09)

Consider $D_n(x, a)$ but now fix x, and let a be the variable.

$D_n(x, a)$ is a reversed Dickson poly. (RDP)

Problem

When do RDPs yield PPs?

Hereafter, we consider RDPs as functions of x

Consider $D_n(a, x)$ with $a \in F_q$ fixed

$a = 0$**:** If n is odd, $D_n(0, x) = 0$ is not PP

If $n = 2k$ is even, q odd, $D_{2k}(0, x) = 2(-1)^k x^k$ is a PP on F_q iff $(k, q-1) = 1$.

Funct. eq. implies

$$D_n(a, x) = a^n D_n\Big(1, \frac{x}{a^2}\Big).$$

Hence for $a \neq 0$, $D_n(a, x)$ is a PP on $\mathbb{F}_q$ if and only if $D_n(1, x)$ is a PP on $\mathbb{F}_q$.

Suffices to consider the RDP $D_n(1, x)$. The ultimate question is for which n the poly. $D_n(1, x)$ is a PP on $\mathbb{F}_q$. This question, unlike the same question for Dickson polys. $D_n(x, a)$, does not seem to have an easy answer.

When are $D_{n_1}(1, x)$ and $D_{n_2}(1, x)$ equal as functions on F_{p^e}?

When are $D_{n_1}(1,x)$ and $D_{n_2}(1,x)$ equal as functions on F_{p^e}?

(i) If $n_1, n_2 > 0$ are integers such that $n_1 \equiv n_2 \pmod{p^{2e}-1}$, then $D_{n_1}(1,x) = D_{n_2}(1,x)$ for all $x \in \mathbb{F}_q$.

(ii) If two positive integers n_1 and n_2 belong to the same p-cyclotomic coset modulo $p^{2e}-1$, then $D_{n_1}(1,x)$ is a PP on $\mathbb{F}_q$ if and only if $D_{n_2}(1,x)$ is a PP on $\mathbb{F}_q$.

For $n_1, n_2 \in \{0, 1, \ldots, p^{2e} - 1\}$, we say that $n_1 \sim n_2$ if $D_{n_1}(1, x) \equiv D_{n_2}(1, x) \pmod{x^{p^e} - x}$. The relation $\sim$ is an eq. rel. whose eq. classes can be described:

Theorem

Let $p = 2$. Then the $\sim$-eq. classes of $\{0, 1, \ldots, 2^{2e} - 1\}$ are

$$\{0\},$$

$$\{2^k : 0 \le k \le 2e - 1\},$$

$$\{(2^e + 1)2^k : 0 \le k \le e - 1\},$$

$$\{\alpha + \beta 2^e, \beta + \alpha 2^e\}, \qquad \begin{array}{l} 0 \le \alpha, \beta \le 2^e - 1, \\ \alpha + \beta 2^e \ne 0,\ 2^k\ (0 \le k \le 2e - 1), \\ (2^e + 1)2^k\ (0 \le k \le e - 1). \end{array}$$

Theorem

Let p be an odd prime. Then the $\sim$-eq. classes of $\{0, 1, \ldots, p^{2e} - 1\}$ are

$$\begin{array}{ll}
\{0\}, & \\
\{p^k : 0 \leq k \leq 2e - 1\}, & \\
\{\frac{p^{2e}-1}{2} + p^k : 0 \leq k \leq 2e - 1\}, & \\
\{\alpha + \beta p^e, \beta + \alpha p^e\}, & 0 \leq \alpha, \beta \leq p^e - 1,\ \alpha + \beta p^e \neq 0, \\
& p^k, \frac{p^{2e}-1}{2} + p^k,\ 0 \leq k \leq 2e - 1.
\end{array}$$

$f : F_q \to F_q$ is called almost perfect nonlinear (APN) if for each $a \in F_q^*$ and $b \in F_q$, the equation $f(x+a) - f(x) = b$ has at most two sols. in F_q.

$f : F_q \rightarrow F_q$ is called almost perfect nonlinear (APN) if for each $a \in F_q^*$ and $b \in F_q$, the equation $f(x+a) - f(x) = b$ has at most two sols. in F_q.

x^n is an APN fcn. on F_q iff for each $b \in F_q$, the eq. $(x+1)^n - x^n = b$ has at most two sols. in F_q.

$f : F_q \to F_q$ is called almost perfect nonlinear (APN) if for each $a \in F_q^*$ and $b \in F_q$, the equation $f(x+a) - f(x) = b$ has at most two sols. in F_q.

x^n is an APN fcn. on F_q iff for each $b \in F_q$, the eq. $(x+1)^n - x^n = b$ has at most two sols. in F_q.

Theorem

(i) x^n is an APN func. on $F_{2^{2e}} \Rightarrow D_n(1,x)$ is a PP on $F_{2^e} \Rightarrow x^n$ is an APN function on F_{2^e}.

$f : F_q \to F_q$ is called almost perfect nonlinear (APN) if for each $a \in F_q^*$ and $b \in F_q$, the equation $f(x+a) - f(x) = b$ has at most two sols. in F_q.

x^n is an APN fcn. on F_q iff for each $b \in F_q$, the eq. $(x+1)^n - x^n = b$ has at most two sols. in F_q.

Theorem

(i) x^n is an APN func. on $F_{2^{2e}} \Rightarrow D_n(1,x)$ is a PP on $F_{2^e} \Rightarrow x^n$ is an APN function on F_{2^e}.
(ii) Let p be an odd prime and n an odd pos. integer. Then x^n is an APN func. on $F_{p^{2e}} \Rightarrow D_n(1,x)$ is a PP on $F_{p^e} \Rightarrow x^n$ is an APN func. on F_{p^e}

Theorem

The RDP $D_n(1,x)$ is a PP on F_{p^e} in each of the following cases:

I. $p = 2$.

(i) $n = 2^k + 1, \quad (k, 2e) = 1.$ *(Gold)*

(ii) $n = 2^{2k} - 2^k + 1, \quad (k, 2e) = 1.$ *(Kasami)*

(iii) $n = 2^{8k} + 2^{6k} + 2^{4k} + 2^{2k} - 1, \quad e = 5k.$ *(Dobbertin)*

Theorem

The RDP $D_n(1,x)$ is a PP on F_{p^e} in each of the following cases:

I. $p = 2$.

(i) $n = 2^k + 1, \quad (k, 2e) = 1.$ *(Gold)*

(ii) $n = 2^{2k} - 2^k + 1, \quad (k, 2e) = 1.$ *(Kasami)*

(iii) $n = 2^{8k} + 2^{6k} + 2^{4k} + 2^{2k} - 1, \quad e = 5k.$ *(Dobbertin)*

Theorem

The RDP $D_n(1,x)$ is a PP on F_{p^e} in each of the following cases:

II. $p > 2$.

(i) $n = 3, \quad p > 3.$ *($D_3(1,x) = -3x + 1$, trivial)*

(ii) $n = p^e + 2, \quad p^e \equiv 1 \pmod 3$.

(iii) $n = \frac{5^k+1}{2} \qquad p = 5,\ (k, 2e) = 1.$

Some examples of RDPPs not coming from APN fcns.

Example

(i) $p = 2$, $e = 2$, $n = 2^4 + 2^2 + 1 = 21$. *Then* $D_{21}(1, x)$ *is a PP on* F_{2^4} *but* x^{21} *is not an APN function on* F_{2^8}.
(ii) Let $p = 2$, $e = 3$, $n = 2^2 + 1 = 5$. *Then* x^5 *is an APN function on* F_{2^3} *(the Gold case) but* $D_5(1, x) = x^2 + x + 1$ *is not a PP on* F_{2^3}.
(iii) Let $p > 3$ *be a prime such that* $p \equiv -1 \pmod 3$ *and let* $e = 1$, $n = p + 2$. *Then* $x^{p+2} (= x^3)$ *is an APN function on* F_p *but* $D_{p+2}(1, x)$ *is not a PP on* F_p.

Theorem

Let p be an odd prime and $k \geq 0$. Then in $F_p[x]$,

$$D_{p^k+1}(1, x) = 2\left(-x + \frac{1}{4}\right)^{\frac{p^k+1}{2}} + \frac{1}{2}$$

$$D_{p^k+2}(1, x) = 2\left(-x + \frac{1}{4}\right)^{\frac{p^k+1}{2}} + \frac{1}{2} - x.$$

Theorem

Let p be an odd prime and $k \geq 0$. Then in $F_p[x]$,

$$D_{p^k+1}(1,x) = 2\Big(-x + \frac{1}{4}\Big)^{\frac{p^k+1}{2}} + \frac{1}{2}$$

$$D_{p^k+2}(1,x) = 2\Big(-x + \frac{1}{4}\Big)^{\frac{p^k+1}{2}} + \frac{1}{2} - x.$$

Theorem

Let e be a positive even integer and let $n = 2^e + 2^k + 1$, where k is a positive integer such that $(k-1, e) = 1$. Then $D_n(1,x)$ is a PP on F_{2^e}.

Theorem

Let p be an odd prime and $k \geq 0$. Then in $F_p[x]$,

$$D_{p^k+1}(1,x) = 2\Big(-x + \frac{1}{4}\Big)^{\frac{p^k+1}{2}} + \frac{1}{2}$$

$$D_{p^k+2}(1,x) = 2\Big(-x + \frac{1}{4}\Big)^{\frac{p^k+1}{2}} + \frac{1}{2} - x.$$

Theorem

Let e be a positive even integer and let $n = 2^e + 2^k + 1$, where k is a positive integer such that $(k-1, e) = 1$. Then $D_n(1,x)$ is a PP on F_{2^e}.

Theorem

Let $k > 0$ be an integer such that $(k, 2e) = 1$ and let $n = \frac{3^k+1}{2}$. Then $D_n(1,x)$ is a PP on F_{3^e}.

Conjecture

Let $p > 3$ *be a prime and let* $1 \leq n \leq p^2 - 1$. *Then* $D_n(1, x)$ *is a PP on* F_p *if and only if*

$$n = \begin{cases} 2,\ 2p,\ 3,\ 3p,\ p+1,\ p+2,\ 2p+1 & \textit{if } p \equiv 1 \pmod{12}, \\ 2,\ 2p,\ 3,\ 3p,\ p+1 & \textit{if } p \equiv 5 \pmod{12}, \\ 2,\ 2p,\ 3,\ 3p,\ p+2,\ 2p+1 & \textit{if } p \equiv 7 \pmod{12}, \\ 2,\ 2p,\ 3,\ 3p & \textit{if } p \equiv 11 \pmod{12}. \end{cases}$$

p^e	n	cyclotomic coset mod $p^{2e}-1$	reference
2	3	3	**T??** I(i)
2^2	3	3, 6, 12, 9	**T??** I(i)
2^3	3	3, 6, 12, 24, 48, 33	**T??** I(i)
2^4	3	3, 6, 12, 24, 48, 96, 192, 129	**T??** I(i)
	9	9, 18, 36, 72, 144, 33, 66, 132	**T??** I(i)
	21	21, 42, 84, 168, 81, 162, 69, 138	**T??**
	39	39, 78, 156, 57, 114, 228, 201, 147	**T??** I(ii)
2^5	3	3, 6, 12, 24, 48, 96, 192, 384, 768, 513	**T??** I(i)
	9	9, 18, 36, 72, 144, 288, 576, 129, 258, 516	**T??** I(i)
	57	57, 114, 228, 456, 912, 801, 579, 135, 270, 540	**T??** I(ii)
	213	213, 426, 825, 681, 339, 678, 333, 666, 309, 618	**T??** I(iii)
2^6	3	3, 6, 12, 24, 48, 96, 192, 384, 768, 1536, 3072, 2049	**T??** I(i)
	33	33, 66, 132, 264, 528, 1056, 2112, 129, 258, 516, 1032, 2064	**T??** I(i)
	69	69, 138, 276, 552, 1104, 2208, 321, 642, 1284, 2568, 1041, 2082	**T??**
	159	159, 318, 636, 1272, 2544, 993, 1986, 3972, 3849, 3603, 3111, 2127	**T??** I(ii)

Table: Reversed Dickson PPs $D_n(1,x)$ on $\mathbb{F}_{p^e}$, $p^e < 200$

p^e	n	cyclotomic coset mod $p^{2e}-1$	reference
2^7	3	3, 6, 12, 24, 48, 96, 192, 384, 768, 1536, 3072, 6144, 12288, 8193	T?? I(i)
	9	9, 18, 36, 72, 144, 288, 576, 1152, 2304, 4608, 9216, 2049, 4098, 8196	T?? I(i)
	33	33, 66, 132, 264, 528, 1056, 2112, 4224, 8448, 513, 1026, 2052, 4104, 8208	T?? I(i)
	57	57, 114, 228, 456, 912, 1824, 3648, 7296, 14592, 12801, 9219, 2055, 4110, 8220	T?? I(ii)
	543	543, 1086, 2172, 4344, 8688, 993, 1986, 3972, 7944, 15888, 15393, 14403, 12423, 8463	T?? I(ii)
3	2	2, 6	C?? (i)
3^2	2	2, 6, 18, 54	C?? (i)
	10	10, 30	C?? (i)
	14	14, 42, 46, 58	T??
3^3	2	2, 6, 18, 54, 162, 486	C?? (i)
	10	10, 30, 90, 270, 82, 246	C?? (i)
	122	122, 366, 370, 382, 418, 526	T??
3^4	2	2, 6, 18, 54, 162, 486, 1458, 4374	C?? (i)
	14	14, 42, 126, 378, 1134, 3402, 3646, 4378	T??
	82	82, 246, 738, 2214	C?? (i)
	86	86, 258, 774, 2322, 406, 1218, 3654, 4402	?
	122	122, 366, 1098, 3294, 3322, 3406, 3658, 4414	T??
	1094	1094, 3282, 3286, 3298, 3334, 3442, 3766, 4738	T??

Table: continued

p^e	n	cyclotomic coset mod $p^{2e}-1$	reference
5	2	2, 10	C?? (i)
	3	3, 15	T?? II(i)
	6	6	C?? (i)
5^2	2	2, 10, 50, 250	C?? (i)
	3	3, 15, 75, 375	T?? II(i)
	26	26, 130	C?? (i)
	27	27, 135, 51, 255	T?? II(ii)
	63	63, 315, 327, 387	T?? II(iii)
5^3	2	2, 10, 50, 250, 1250, 6250	C?? (i)
	3	3, 15, 75, 375, 1875, 9375	T?? II(i)
	6	6, 30, 150, 750, 3750, 3126	C?? (i)
	26	26, 130, 650, 3250, 626, 3130	C?? (i)
	126	126, 630, 3150	C?? (i)
	1536	1563, 7815, 7827, 7887, 8187, 9687	T?? II(iii)
7	2	2, 14	C?? (i)
	3	3, 21	T?? II(i)
	9	9, 15	T?? II(ii)
7^2	2	2, 14, 98, 686	C?? (i)
	3	3, 21, 147, 1029	T?? II(i)
	50	50, 350	C?? (i)
	51	51, 357, 99, 693	T?? II(ii)

Table: Reversed Dickson PPs $D_n(1,x)$ on $\mathbb{F}_{p^e}$, $p^e < 200$

p^e	n	cyclotomic coset mod $p^{2e}-1$	reference
11	2	2, 22	C**??** (i)
	3	3, 33	T**??** II(i)
11^2	2	2, 22, 242, 2662	C**??** (i)
	3	3, 33, 363, 3993	T**??** II(i)
	122	122, 1342	C**??** (i)
	123	123,1353,243,2673	T**??** II(i)
13	2	2, 26	C**??** (i)
	3	3, 39	T**??** II(i)
	14	14	C**??** (i)
	15	15, 17	T**??** II(ii)
13^2	2	2, 26, 338, 4394	C**??** (i)
	3	3, 39, 507, 6591	T**??** II(i)
	170	170, 2210	C**??** (i)
	171	171, 2223, 339, 4407	T**??** II(ii)

Table: continued

$e = 1,\ 17 \leq p \leq 199$			
p	n	cyclotomic coset mod $p^2 - 1$	reference
$p \equiv 1 \pmod{12}$	2	$2,\ 2p$	C?? (i)
	3	$3,\ 3p$	T?? II(i)
	$p+1$	$p+1$	C?? (i)
	$p+2$	$p+2,\ 2p+1$	T?? II(ii)
$p \equiv 5 \pmod{12}$	2	$2,\ 2p$	C?? (i)
	3	$3,\ 3p$	T?? II(i)
	$p+1$	$p+1$	C?? (i)
$p \equiv 7 \pmod{12}$	2	$2,\ 2p$	C?? (i)
	3	$3,\ 3p$	T?? II(i)
	$p+2$	$p+2,\ 2p+1$	T?? II(ii)
$p \equiv 11 \pmod{12}$	2	$2,\ 2p$	C?? (i)
	3	$3,\ 3p$	T?? II(i)

Open Questions Related to RDPPs

1. If $D_n(1,x)$ is a PP on F_{2^e}, where e is odd, is x^n an APN function on $F_{2^{2e}}$?

Open Questions Related to RDPPs

1. If $D_n(1,x)$ is a PP on F_{2^e}, where e is odd, is x^n an APN function on $F_{2^{2e}}$?
2. If $D_n(1,x)$ is a PP on F_{p^e}, where $p > 3$ and n is odd, is x^n an APN function on $F_{p^{2e}}$?

Open Questions Related to RDPPs

1. If $D_n(1, x)$ is a PP on F_{2^e}, where e is odd, is x^n an APN function on $F_{2^{2e}}$?
2. If $D_n(1, x)$ is a PP on F_{p^e}, where $p > 3$ and n is odd, is x^n an APN function on $F_{p^{2e}}$?
3. Determine the value set of RDPs.

Problem

Why no other RDPPs over F_p other than those from conj.?

If $n \equiv 1, 5 \pmod 6$, then $D_n(1, 0) = D_n(1, 1) = 1$ so that $D_n(1, x)$ is not a PP on F_p.

Problem

Why no other RDPPs over F_p other than those from conj.?

If $n \equiv 1, 5 \pmod 6$, then $D_n(1, 0) = D_n(1, 1) = 1$ so that $D_n(1, x)$ is not a PP on F_p.

Problem

What happens over F_{p^e}, $e \geq 2$?

Theorem

Hou *(JCT,A, to appear) (i) If s even,* $D_{3^e+5}(1,x)$ *is PP on* F_{3^e}*.*

Theorem

Hou *(JCT,A, to appear) (i) If s even,* $D_{3^e+5}(1,x)$ *is PP on* F_{3^e}*.*
(ii) New func. $g_{n,q}(x)$ *defined by*

$$\sum_{a \in F_q} (x+a)^n = g_{n,q}(x^q - x)$$

If $p = 2$, $g_{n,2}(x) = D_n(1,x)$

Hou gives conds. when $g_{n,p}$ is PP on F_p

Theorem

Hou *(preprint) Nec. conds. for RDP to be PP*

$$\sum_{a \in F_q} D_n(1,a)^i, i = 1, 2$$

Dickson Polynomials Second Kind

Dickson poly. second kind deg. n, parameter $a \in F_q$

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

$E_n(x,0) = x^n$

$E_{n+2}(x,a) = xE_{n+1}(x,a) - aE_n(x,a), n \geq 0$ with
$D_0(x,a) = 1, D_1(x,a) = x$

See **Lidl/M/Turnwald** (93), "Dickson Polys." for some basic properties

Dickson Polynomials Second Kind

Dickson poly. second kind deg. n, parameter $a \in F_q$

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

$E_n(x,0) = x^n$

$E_{n+2}(x,a) = xE_{n+1}(x,a) - aE_n(x,a), n \geq 0$ with
$D_0(x,a) = 1, D_1(x,a) = x$

See **Lidl/M/Turnwald** (93), "Dickson Polys." for some basic properties

Problem

When does $E_n(x,a)$ induce PP on F_q?

Theorem

Matthews *(Thesis, 82) If* q *odd, and* $n+1 \equiv \pm 2 \pmod{p}, (q-1)/2, (q+1)/2$ *then* $E_n(x,1)$ *PP on* F_q

Theorem

Matthews *(Thesis, 82) If q odd, and $n+1 \equiv \pm 2 \pmod{p}, (q-1)/2, (q+1)/2$ then $E_n(x,1)$ PP on F_q*

Conjecture

Conditions also nec.

Theorem

Matthews *(Thesis, 82) If* q *odd, and* $n+1 \equiv \pm 2 \pmod{p}, (q-1)/2, (q+1)/2$ *then* $E_n(x,1)$ *PP on* F_q

Conjecture

Conditions also nec.

Theorem

Cipu/Cohen *(Fq 6, AMS 08) If* $p \geq 7$*, conj. true for* $q = p$ *and* $q = p^2$*.*

Problem

Determine value set for $E_n(x,1)$

PPs in Several Variables

Definition

A poly. $f \in F_q[x_1, \ldots, x_k]$ *is PP in* k *variables if the eq.* $f(x_1, \ldots, x_k) = \alpha$ *has* q^{k-1} *sols. in* F_q^k *for each* $\alpha \in F_q$

PPs in Several Variables

Definition

A poly. $f \in F_q[x_1, \ldots, x_k]$ *is PP in k variables if the eq.* $f(x_1, \ldots, x_k) = \alpha$ *has* q^{k-1} *sols. in* F_q^k *for each* $\alpha \in F_q$

Definition

Poly. $f_1, \ldots, f_r \in F_q[x_1, \ldots, x_k]$ *is orth. sys. in k variables if the sys. of eqs.* $f_i(x_1, \ldots, x_k) = \alpha_i$ *has* q^{k-r} *sols. in* F_q^k *for each* $(\alpha_1, \ldots, \alpha_r) \in F_q^r$

See L/N, Sec. 7.5

Appl. to Latin and Frequency Squares and Hypercubes

Theorem

M *(Disc. Math., 88) Complete sets of orth.* $F(q^i; q^{i-1}, \ldots, q^{i-1})$ *freq. squares.*

Also see **Laywine/M**, (Handbook Combin. Designs, 07, 465-471)