Lucas Sequences, Permutation Polynomials, and Inverse Polynomials

Qiang (Steven) Wang

School of Mathematics and Statistics
Carleton University

IPM 20 - Combinatorics 2009,
Tehran, May 16-21, 2009.

Outline

Outline

1. **Lucas Sequences**
   - Fibonacci numbers, Lucas numbers
   - Lucas sequences
   - Dickson polynomials
   - Generalized Lucas Sequences
2. **Permutation polynomials (PP) over finite fields**
   - Introduction of permutation polynomials
   - Permutation binomials and sequences
3. **Inverse Polynomials**
   - Compositional inverse polynomial of a PP
   - Inverse polynomials of permutation binomials
4. **Summary**

Fibonacci numbers

Origin

- Ancient India: Pingala (200 BC).
- West: Leonardo of Pisa, known as Fibonacci (1170-1250), in his Liber Abaci (1202). He considered the growth of an idealised (biologically unrealistic) rabbit population.

Liber Abaci, 1202

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, \cdots$$

$$F_0 = 0,\ F_1 = 1,\ F_n = F_{n-1} + F_{n-2} \text{ for } n \geq 2.$$

Leonardo of Pisa, Fibonacci (1170-1250)

Figure: Fibonacci (1170-1250)

Fibonacci (1170-1250)

Figure: A statue of Fibonacci in Pisa

Lucas numbers

Lucas numbers (Edouard Lucas)

$$2, 1, 3, 4, 7, 11, 18, 29, 47, 76, \cdots$$

$$L_0 = 2,\ L_1 = 1,\ L_n = L_{n-1} + L_{n-2} \text{ for } n \geq 2.$$

Edouard Lucas (1842-1891)

Figure: Edouard Lucas (1842-1891)

Lucas sequences

Let P, Q be integers and $\triangle = P^2 - 4Q$ be a nonsquare.

Fibonacci type

$U_0(P,Q) = 0,$
$U_1(P,Q) = 1,$
$U_n(P,Q) = PU_{n-1}(P,Q) - QU_{n-2}(P,Q)$ for $n \geq 2$.

Lucas type

$V_0(P,Q) = 2,$
$V_1(P,Q) = P,$
$V_n(P,Q) = PV_{n-1}(P,Q) - QV_{n-2}(P,Q)$ for $n \geq 2$.

$U_n(1,-1)$ - Fibonacci numbers
$U_n(2,-1)$ - Pell numbers
$U_n(1,-2)$ - Jacobsthal numbers

$V_n(1,-1)$ - Lucas numbers
$V_n(2,-1)$ - Pell-Lucas numbers

basic properties

- characteristic equation: $x^2 - Px + Q = 0$.
- $a = \frac{P+\sqrt{\triangle}}{2}$ and $b = \frac{P-\sqrt{\triangle}}{2} \in \mathbb{Q}[\sqrt{\triangle}]$
- $U_n(P, Q) = \frac{a^n - b^n}{a-b}$.
- $V_n(P, Q) = a^n + b^n$.

Applications

RSA

- $n = pq$, p and q are distinct primes.
- $k = (p-1)(q-1)$.
- $\gcd(e,k) = 1$ and $ed \equiv 1 \pmod{k}$. Here e is called a public key and d a private key. Each party has a pair of keys, i.e., (e_A, d_A) and (e_B, d_B).

$$\text{Alice} \quad \xrightarrow{c \equiv m^{e_B} \pmod{n}} \quad \text{Bob}$$

$$c^{d_B} \equiv (m^{e_B})^{d_B} \equiv m^{e_B d_B} \equiv m \pmod{n}.$$

Applications

LUC

- $n = pq$, p and q are distinct primes.
- $k = (p^2 - 1)(q^2 - 1)$.
- $\gcd(e, k) = 1$ and $ed \equiv 1 \pmod{k}$.

$$\text{Alice} \xrightarrow{V_{e_B}(m,1)} \text{Bob}$$

$$V_d(V_e(m,1),1) \equiv V_{de}(m,1) \equiv m \pmod{n}.$$

Dickson polynomials

Dickson polynomials of the first kind of degree n

- $$S_n = \alpha^n + \beta^n = \sum_{j=0}^{\lfloor n/2 \rfloor} (-1)^j \frac{n}{n-j} \binom{n-j}{j} (\alpha\beta)^j (\alpha+\beta)^{n-2j}.$$

- $$D_n(x,a) = \sum_{j=0}^{\lfloor n/2 \rfloor} \frac{n}{n-j} \binom{n-j}{j} (-a)^j x^{n-2j}, \ n \geq 1.$$

- $$D_n(\alpha + \frac{a}{\alpha}, a) = \alpha^n + \frac{a^n}{\alpha^n}.$$

Dickson polynomials

Dickson polynomials of the first kind of degree n

- $$S_n = \alpha^n + \beta^n = \sum_{j=0}^{\lfloor n/2 \rfloor} (-1)^j \frac{n}{n-j} \binom{n-j}{j} (\alpha\beta)^j (\alpha+\beta)^{n-2j}.$$

- $$D_n(x, a) = \sum_{j=0}^{\lfloor n/2 \rfloor} \frac{n}{n-j} \binom{n-j}{j} (-a)^j x^{n-2j}, \ n \geq 1.$$

- $$D_n(\alpha + \frac{a}{\alpha}, a) = \alpha^n + \frac{a^n}{\alpha^n}.$$

Dickson polynomials

Dickson polynomials of the first kind of degree n

- $$S_n = \alpha^n + \beta^n = \sum_{j=0}^{\lfloor n/2 \rfloor} (-1)^j \frac{n}{n-j} \binom{n-j}{j} (\alpha\beta)^j (\alpha+\beta)^{n-2j}.$$

- $$D_n(x, a) = \sum_{j=0}^{\lfloor n/2 \rfloor} \frac{n}{n-j} \binom{n-j}{j} (-a)^j x^{n-2j}, \ n \geq 1.$$

- $$D_n(\alpha + \frac{a}{\alpha}, a) = \alpha^n + \frac{a^n}{\alpha^n}.$$

Dickson polynomials

Dickson polynomials of the first kind of degree n

- $\alpha^n + \beta^n = (\alpha+\beta)(\alpha^{n-1} + \beta^{n-1}) - (\alpha\beta)(\alpha^{n-2} + \beta^{n-2})$.
- $D_n(x, a) = xD_{n-1}(x, a) - aD_{n-2}(x, a)$.
- $D_0(x, a) = 2, D_1(x, a) = x$.
- $D_n(P, a) = V_n(P, a)$.

Dickson polynomials

Dickson polynomials of the first kind of degree n

- $\alpha^n + \beta^n = (\alpha+\beta)(\alpha^{n-1}+\beta^{n-1}) - (\alpha\beta)(\alpha^{n-2}+\beta^{n-2})$.
- $D_n(x,a) = xD_{n-1}(x,a) - aD_{n-2}(x,a)$.
- $D_0(x,a) = 2, D_1(x,a) = x$.
- $D_n(P,a) = V_n(P,a)$.

Dickson polynomials

Dickson polynomials of the first kind of degree n

- $\alpha^n + \beta^n = (\alpha + \beta)(\alpha^{n-1} + \beta^{n-1}) - (\alpha\beta)(\alpha^{n-2} + \beta^{n-2}).$
- $D_n(x, a) = xD_{n-1}(x, a) - aD_{n-2}(x, a).$
- $D_0(x, a) = 2, D_1(x, a) = x.$
- $D_n(P, a) = V_n(P, a).$

Dickson polynomials

Dickson polynomials of the first kind of degree n

- $\alpha^n + \beta^n = (\alpha + \beta)(\alpha^{n-1} + \beta^{n-1}) - (\alpha\beta)(\alpha^{n-2} + \beta^{n-2})$.
- $D_n(x, a) = xD_{n-1}(x, a) - aD_{n-2}(x, a)$.
- $D_0(x, a) = 2, D_1(x, a) = x$.
- $D_n(P, a) = V_n(P, a)$.

Dickson polynomials

Dickson polynomials of second kind of degree n

- $$E_n(x,a) = \sum_{j=0}^{\lfloor n/2 \rfloor} \binom{n-j}{j} (-a)^j x^{n-2j}.$$
- $E_0(x,a) = 1$, $E_1(x,a) = x$,
  $E_n(x,a) = xE_{n-1}(x,a) - aE_{n-2}(x,a)$
- $E_n(x,a) = \frac{\alpha^{n+1}-\beta^{n+1}}{\alpha-\beta}$ for $x = \alpha+\beta$ and $\beta = \frac{a}{\alpha}$ and $\alpha^2 \neq a$.
  Moreover, $E_n(\pm 2\sqrt{a}, a) = (n+1)(\pm\sqrt{a})^n$.
- $E_n(P,Q) = U_{n+1}(P,Q)$.

Dickson polynomials

Dickson polynomials of second kind of degree n

- $$E_n(x,a) = \sum_{j=0}^{\lfloor n/2 \rfloor} \binom{n-j}{j} (-a)^j x^{n-2j}.$$
- $E_0(x,a) = 1$, $E_1(x,a) = x$,
  $E_n(x,a) = xE_{n-1}(x,a) - aE_{n-2}(x,a)$
- $E_n(x,a) = \frac{\alpha^{n+1}-\beta^{n+1}}{\alpha-\beta}$ for $x = \alpha+\beta$ and $\beta = \frac{a}{\alpha}$ and $\alpha^2 \neq a$.
  Moreover, $E_n(\pm 2\sqrt{a}, a) = (n+1)(\pm\sqrt{a})^n$.
- $E_n(P,Q) = U_{n+1}(P,Q)$.

Dickson polynomials

Dickson polynomials of second kind of degree n

- $$E_n(x,a) = \sum_{j=0}^{\lfloor n/2 \rfloor} \binom{n-j}{j} (-a)^j x^{n-2j}.$$
- $E_0(x,a) = 1$, $E_1(x,a) = x$,
  $E_n(x,a) = xE_{n-1}(x,a) - aE_{n-2}(x,a)$
- $E_n(x,a) = \frac{\alpha^{n+1}-\beta^{n+1}}{\alpha-\beta}$ for $x = \alpha+\beta$ and $\beta = \frac{a}{\alpha}$ and $\alpha^2 \neq a$.
  Moreover, $E_n(\pm 2\sqrt{a}, a) = (n+1)(\pm\sqrt{a})^n$.
- $E_n(P,Q) = U_{n+1}(P,Q)$.

Dickson polynomials

Dickson polynomials of second kind of degree n

- $$E_n(x,a) = \sum_{j=0}^{\lfloor n/2 \rfloor} \binom{n-j}{j} (-a)^j x^{n-2j}.$$
- $E_0(x,a) = 1$, $E_1(x,a) = x$,
  $E_n(x,a) = xE_{n-1}(x,a) - aE_{n-2}(x,a)$
- $E_n(x,a) = \frac{\alpha^{n+1}-\beta^{n+1}}{\alpha-\beta}$ for $x = \alpha+\beta$ and $\beta = \frac{a}{\alpha}$ and $\alpha^2 \neq a$.
  Moreover, $E_n(\pm 2\sqrt{a}, a) = (n+1)(\pm\sqrt{a})^n$.
- $E_n(P,Q) = U_{n+1}(P,Q)$.

$V_n(1,-1)$

Lucas numbers $V_n(1,-1)$

$2, 1, 3, 4, 7, \cdots \implies V_n(1,-1) = (\frac{1+\sqrt{5}}{2})^n + (\frac{1-\sqrt{5}}{2})^n$.

$$a = \frac{1+\sqrt{5}}{2} = 2\cos(\frac{\pi}{5}) = e^{-\frac{\pi}{5}} + e^{\frac{\pi}{5}}.$$

$$b = \frac{1-\sqrt{5}}{2} = 2\cos(\frac{3\pi}{5}) = e^{-\frac{3\pi}{5}} + e^{\frac{3\pi}{5}}.$$

Let η be a primitive 10th root of unity. Then

$$a = \eta + \eta^{-1} \textit{ and } b = \eta^3 + \eta^{-3}.$$

Hence

$$V_n(1,-1) = (\eta + \eta^{-1})^n + (\eta^3 + \eta^{-3})^n.$$

Definition

Generalized Lucas sequence (Akbary, W., 2006)

For any odd integer $\ell = 2k+1 \geq 3$ and η be a fixed primitive 2ℓth root of unity. The generalized Lucas sequence of order $k = \frac{\ell-1}{2}$ is defined as

$$a_n = \sum_{\substack{t=1 \\ t \text{ odd}}}^{\ell-1} (\eta^t + \eta^{-t})^n = \sum_{t=1}^{\frac{\ell-1}{2}} ((-1)^{t+1}(\eta^t + \eta^{-t}))^n.$$

Characteristic polynomials

Characteristic polynomials

$$g_k(x) = \prod_{\substack{t=1 \\ t \ \text{odd}}}^{\ell-1} (x - (\eta^t + \eta^{-t})).$$

ℓ	initial values	$g_k(x)$
$\ell = 3$	1	$x - 1$
$\ell = 5$	$2, 1$	$x^2 - x - 1$
$\ell = 7$	$3, 1, 5$	$x^3 - x^2 - 2x + 1$
$\ell = 9$	$4, 1, 7, 4$	$x^4 - x^3 - 3x^2 + 2x + 1$
$\ell = 11$	$5, 1, 9, 4, 25$	$x^5 - x^4 - 4x^3 + 3x^2 + 3x - 1$

Recurrence relation of characteristic polynomials

Theorem (W. 2009)

Let $\ell = 2k+1$, $g_0(x) = 1$, *and* $g_k(x) = \prod_{\substack{t=1 \\ t \text{ odd}}}^{\ell-1} (x - (\eta^t + \eta^{-t}))$.

Then

- $g_k(x) = E_k(x,1) - E_{k-1}(x,1)$ *for* $k \geq 1$.
- $g_k(x) = \sum_{i=0}^{k} (-1)^{\lceil \frac{i}{2} \rceil} \binom{k - i + \lfloor \frac{i}{2} \rfloor}{\lfloor \frac{i}{2} \rfloor} x^{k-i}$.
- $g_k(x)$ *satisfies the following recurrence relation:*
  $g_0(x) = 1$, $g_1(x) = x - 1$,
  $g_k(x) = x g_{k-1}(x) - g_{k-2}(x)$ *for* $k \geq 2$.
- *The generating function of the above recurrence is* $G(x;t) = \frac{1-t}{1-xt+t^2}$.

Sketch of the proof

- $$\begin{aligned} E_k(x,1) - E_{k-1}(x,1) &= E_k(u+1/u) - E_{k-1}(u+1/u) \\ &= \frac{u^{k+1}-u^{-(k+1)}}{u-u^{-1}} - \frac{u^k-u^{-k}}{u-u^{-1}} \\ &= (u^{2k+1}+1)/(u^n(u+1)) \end{aligned}$$
- η is a primitive $2\ell = 4k+2$ root of unity implies that $\eta^{2k+1} = -1$.
- $\eta^t + \eta^{-t}$ is a root of $E_k(u+1/u) - E_{k-1}(u+1/u)$ for any odd t.

Sketch of the proof

- $$\begin{aligned} E_k(x,1) - E_{k-1}(x,1) &= E_k(u+1/u) - E_{k-1}(u+1/u) \\ &= \frac{u^{k+1}-u^{-(k+1)}}{u-u^{-1}} - \frac{u^k-u^{-k}}{u-u^{-1}} \\ &= (u^{2k+1}+1)/(u^n(u+1)) \end{aligned}$$
- η is a primitive $2\ell = 4k+2$ root of unity implies that $\eta^{2k+1} = -1$.
- $\eta^t + \eta^{-t}$ is a root of $E_k(u+1/u) - E_{k-1}(u+1/u)$ for any odd t.

Sketch of the proof

- $$\begin{aligned} E_k(x,1) - E_{k-1}(x,1) &= E_k(u+1/u) - E_{k-1}(u+1/u) \\ &= \frac{u^{k+1}-u^{-(k+1)}}{u-u^{-1}} - \frac{u^k-u^{-k}}{u-u^{-1}} \\ &= (u^{2k+1}+1)/(u^n(u+1)) \end{aligned}$$
- η is a primitive $2\ell = 4k+2$ root of unity implies that $\eta^{2k+1} = -1$.
- $\eta^t + \eta^{-t}$ is a root of $E_k(u+1/u) - E_{k-1}(u+1/u)$ for any odd t.

Outline

Introduction of PPs

Definition

A polynomial $f(x) \in \mathbb{F}_q[x]$ is a permutation polynomial (PP) of $\mathbb{F}_q$ if f permutes the elements of $\mathbb{F}_q$.
Equivalently,

- the function $f : c \mapsto f(c)$ is onto;
- the function $f : c \mapsto f(c)$ is one-to-one;
- $f(x) = a$ has a (unique) solution in $\mathbb{F}_q$ for each $a \in \mathbb{F}_q$.
- the plane curve $f(x) - f(y) = 0$ has no $\mathbb{F}_q$-rational point other than points on the diagonal $x = y$.

Introduction of PPs

Some classical examples

- $P(x) = ax + b, a \neq 0$
- $P(x) = x^n$ is a PP of $\mathbb{F}_q$ iff $(n, q-1) = 1$. (RSA)
- Dickson polynomial of the first kind $D_n(x, \pm 1)$ of degree n over $\mathbb{F}_q$ is PP iff $(n, q^2 - 1) = 1$. (LUC)
- $P_1 \circ P_2$ is a PP iff P_1 and P_2 are PPs.
- x^m is the inverse of x^n iff $mn \equiv 1 \pmod{q-1}$.
- $D_n(D_m(x, 1), 1) = D_{mn}(x, 1) = x$ iff $mn \equiv 1 \pmod{q^2 - 1}$.

Introduction of PPs

Fundamental Questions

Classification, enumeration, and applications of PPs.

Problem 13, R. Lidl and G. Mullen, 1993

Determine conditions on k, r, and q so that $P(x) = x^k + ax^r$ permutes $\mathbb{F}_q$ with $a \in \mathbb{F}_q^*$.

Introduction of PPs

Fundamental Questions

Classification, enumeration, and applications of PPs.

Problem 13, R. Lidl and G. Mullen, 1993

Determine conditions on k, r, and q so that $P(x) = x^k + ax^r$ permutes $\mathbb{F}_q$ with $a \in \mathbb{F}_q^*$.

$P(x) = x^k + ax^r$

Set up

$P(x) = x^r f(x^s) = x^r(x^{es} + a)$, $s = (k-r, q-1)$, $\ell = \frac{q-1}{s}$.

Some necessary conditions

If $a = b^s$, then $x^r(x^{es} + a)$ is PP iff $x^r(x^{es} + 1)$ is PP.

- $(r, s) = 1$,
- $1 + \zeta^{ei} \neq 0$ for $i = 0, 1, \ldots, \ell - 1$ implies that $(2e, \ell) = 1$ where ζ is a primitive ℓ-th root of unity. Hence ℓ is odd.
- $2^s = 1$ in $\mathbb{F}_q$.
- $2r + es \not\equiv 0 \pmod{\ell}$.

$P(x) = x^k + x^r$

Theorem (L. Wang, 2002)

1. *For* $\ell = 3$, $P(x)$ *is a PP of* $\mathbb{F}_q$ *if and only if*
   (i) $(r, s) = 1$.
   (ii) $2r + es \not\equiv 0 \pmod 3$.
   (iii) $2^s \equiv 1 \pmod p$.

Theorem (L. Wang, 2002)

2. *For* $\ell = 5$, $P(x)$ *is a PP of* $\mathbb{F}_q$ *if and only if*
   (i) $(r, s) = 1$.
   (ii) $2r + es \not\equiv 0 \pmod 5$.
   (iii) $2^s \equiv 1 \pmod p$.
   (iv) $(\frac{1+\sqrt{5}}{2})^s + (\frac{1-\sqrt{5}}{2})^s \equiv 2 \pmod p$.

$P(x) = x^k + x^r$

Theorem (L. Wang, 2002)

1. For $\ell = 3$, $P(x)$ is a PP of $\mathbb{F}_q$ if and only if

(i) $(r, s) = 1$.

(ii) $2r + es \not\equiv 0 \pmod 3$.

(iii) $2^s \equiv 1 \pmod p$.

Theorem (L. Wang, 2002)

2. For $\ell = 5$, $P(x)$ is a PP of $\mathbb{F}_q$ if and only if

(i) $(r, s) = 1$.

(ii) $2r + es \not\equiv 0 \pmod 5$.

(iii) $2^s \equiv 1 \pmod p$.

(iv) $L_s \equiv 2 \pmod p$, *where L_n is the n-th element of the Lucas sequence defined by the recursion $L_{n+2} = L_n + L_{n+1}$, $L_0 = 2$ and $L_1 = 1$.*

Connection between PPs and sequences

Theorem (W. 2006)

Let $q = p^m$ be a odd prime power and $q - 1 = \ell s$. Assume that

$$(2e, \ell) = 1,\ (r, s) = 1,\ 2^s \equiv 1 \pmod p,\ 2r + es \not\equiv 0 \pmod \ell.$$

Then $P(x) = x^r(x^{es} + 1)$ is a PP of $\mathbb{F}_q$ iff

$$\sum_{j=0}^{u_c} t_j^{(j_c)} a_{cs+j} = -1, \tag{1}$$

for all $c = 1, \ldots, \ell - 1$, where $\{a_n\}$ is the generalized Lucas sequence of order $\frac{\ell-1}{2}$ over $\mathbb{F}_p$, $j_c = c(2e^{\phi(\ell)-1}r + s) \bmod 2\ell$, $t_j^{(j_c)} = [x^j]D_{j_c}(x, 1)$ is the coefficient of x^j in $D_{j_c}(x, 1)$.

Idea

Theorem 1 (Akbary, W. 07)

Let $q-1=\ell s$ for some positive integers l and s. Let ζ be a primitive ℓ-th root of unity in $\mathbb{F}_q$ and $f(x)$ be a polynomial over $\mathbb{F}_q$. Then the polynomial $P(x)=x^r f(x^s)$ is a PP of $\mathbb{F}_q$ if and only if

(i) $(r,s)=1$.

(ii) $f(\zeta^t)\neq 0$, for each $t=0,\cdots,\ell-1$.

(iii) $\sum_{t=0}^{\ell-1}\zeta^{crt}f(\zeta^t)^{cs}=0$ for each $c=1,\cdots,\ell-1$.

Remark: cyclotomic permutation

Remark

- Equation (1) can be written as $D_{j_c}(\{a_{cs}\}) = -1$ for all $c = 1, \ldots, \ell - 1$.
- The degree j_c is even for any c.
- Since $g_k(\{a_{n_c}\}) = 0$, we have $R_m(\{a_{n_c}\}) = D_m(\{a_{n_c}\})$ where $R_m(x)$ is the remainder of $D_m(x)$ divided by $g_k(x)$.

permutation binomials

Theorem (Akbary, W., 06)

Under the following conditions on ℓ, r, e and s,

$$(r, s) = 1,\ (e, \ell) = 1, \text{ and } \ell \text{ is odd.} \qquad (*)$$

the binomial $P(x) = x^r(x^{es} + 1)$ is a permutation binomial of $\mathbb{F}_q$ if $(2r + es, \ell) = 1$, $2^s \equiv 1 \pmod{p}$ and $\{a_n\}$ is s-periodic over $\mathbb{F}_p$.

Permutation binomials

Theorem (Akbary, W., 06)

Let p be an odd prime and $q = p^m$. Let ℓ be an odd positive integer. Let $p \equiv -1 \pmod{\ell}$ or $p \equiv 1 \pmod{\ell}$ and $\ell \mid m$. Under the conditions $(*)$ on r, e and s, the binomial $P(x) = x^r(x^{es} + 1)$ is a permutation binomial of $\mathbb{F}_q$ if and only if $(2r + es, \ell) = 1$.

Why? $g_{\frac{\ell-1}{2}}(x)$ splits over $\mathbb{F}_p[x]$.

Let γ_j $(1 \le j \le \frac{l-1}{2})$ be roots of $g_{\frac{\ell-1}{2}}(x)$ in $\mathbb{F}_p$, we have $\gamma_j^s \equiv 1 \pmod{p}$ for $j = 1, \cdots, \frac{\ell-1}{2}$.

The sequence $\{a_n\}$ is always s-periodic.

Case $\ell = 7$

Theorem (Akbary, W., 05)

Let $q - 1 = 7s$ and $1 \leq e \leq 6$. Then $P(x) = x^r(x^{es} + 1)$ is a permutation binomial of $\mathbb{F}_q$ if and only if $(r, s) = 1$, $2^s \equiv 1 \pmod{p}$, $2r + es \not\equiv 0 \pmod{7}$ and $\{a_n\}$ satisfies one of the following:

(a) $a_s = a_{-s} = 3$ *in* $\mathbb{F}_p$;

(b) $a_{-cs-1} = -1 + \alpha$, $a_{-cs} = -1 - \alpha$ *and* $a_{-cs+1} = 1$ *in* $\mathbb{F}_p$, *where c is the inverse of $s + 2e^5r$ modulo 7 and* $\alpha^2 + \alpha + 2 = 0$ *in* $\mathbb{F}_p$.

Case l=7

Corollary (Akbary, W., 05)

Let $q-1=7s$, $1 \le e \le 6$, and p be a prime with $\left(\frac{p}{7}\right)=-1$. Then $P(x)=x^r(1+x^{es})$ is a permutation binomial of $\mathbb{F}_q$ if and only if $(r,s)=1$, $2^s \equiv 1 \pmod{p}$ and $2r+es \not\equiv 0 \pmod{7}$.

Outline

Compositional inverse polynomial of a PP

Open problem

Let $P(x) = a_0 + a_1 + \ldots a_{q-2}x^{q-2}$ be a PP of $\mathbb{F}_q$ and $Q(x) = b_0 + b_1 x + \ldots b_{q-2}x^{q-2}$ be the compositional inverse of $P(x)$ modulo $x^q - x$.

Problem 10 (Mullen, 1993): Compute the coefficients of the inverse polynomial of a permutation polynomial efficiently.

Theorem (W. 2009)

Let p be odd prime and $q = p^m$, $\ell \geq 3$ is odd, $q - 1 = \ell s$, and $(e, \ell) = 1$. If $P(x) = x^r(x^{es} + 1)$ is a permutation polynomial of $\mathbb{F}_q$ and $Q(x) = b_0 + b_1 x + \cdots + b_{q-2}x^{q-2}$ is the inverse polynomial of $P(x)$ modulo $x^q - x$, then at most ℓ nonzero coefficients b_k corresponding to $k \equiv r^{-1} \pmod{s}$. Let $\bar{r} = r^{-1} \bmod s$ and $n_c = q - 1 - cs - \bar{r} = (\ell - c)s - \bar{r}$ with $c = 0, \cdots, \ell - 1$. Then

$$b_{q-1-n_c} = \frac{1}{\ell}(2^{n_c} + \sum_{j=0}^{u_c} t_j^{(u_c)} a_{n_c+j}), \tag{2}$$

where $u_c = 2(c + \frac{r\bar{r}-1}{s})e^{\phi(\ell)-1} + cs + \bar{r} \bmod 2\ell$, $t_j^{(u_c)}$ is the coefficient of x^j of Dickson polynomial $D_{u_c}(x)$ of the first kind, and $\{a_n\}_{n=0}^{\infty}$ is the generalized Lucas sequence of order $\frac{\ell-1}{2}$.

Idea

It is well known that

$$\sum_{y\in\mathbb{F}_q} y^{q-1-n}Q(s) = -b_n.$$

Since $P(x)$ is a PP of $\mathbb{F}_q$,

$$b_n = -\sum_{y\in\mathbb{F}_q} yP(y)^{q-1-n} = \frac{1}{\ell}\sum_{t=0}^{\ell-1}\zeta^*(\zeta^{-et}+1)^{q-1-n}.$$

Remark

- Equation (2) can be written as

$$b_{q-1-n_c} = \frac{1}{\ell}\left(2^{s-\bar{r}} + D_{u_c}(\{a_{n_c}\})\right).$$

- The degree u_n is odd for any c.
- Since $g_k(\{a_{n_c}\}) = 0$, we have $R_m(\{a_{n_c}\}) = D_m(\{a_{n_c}\})$ where $R_m(x)$ is the remainder of $D_m(x)$ divided by $g_k(x)$.

Example: $\ell = 3$

In this case, $k = 1$ and $g_1(x) = x - 1$. So $\{a_n\}$ is the constant sequence $1, 1, \ldots$. Moreover, $R_2(x) = -1$ and $R_4(x) = -1$ mean that $R_2(\{a_n\}) = R_4(\{a_n\}) = -a_n = -1$ is automatically satisfied.
Hence $x^r(x^{es} + 1)$ is PP of $\mathbb{F}_q$ iff $(r, s) = 1$, $2r + es \not\equiv 0 \pmod 3$, and $2^s \equiv 1 \pmod p$.
Furthermore, $R_1(x) = 1$, $R_3(x) = -2$, $R_5(x) = 1$. Hence $b_{q-1-n_c} = \frac{1}{3}(2^{-\bar{r}} + D_{u_c}(\{a_n\}))$.

$$D_{u_c}(\{a_{n_c}\}) = \begin{cases} a_{n_c} = 1 & \text{if } u_c \equiv 1, 5 \pmod 6 \\ -2a_{n_c} = -2 & \text{if } u_c \equiv 3 \pmod 6 \end{cases}$$

$$b_{q-1-n_c} = \begin{cases} \frac{1}{3}(2^{s-\bar{r}} + 1) & \text{if } u_c \equiv 1, 5 \pmod 6 \\ \frac{1}{3}(2^{s-\bar{r}} - 2) & \text{if } u_c \equiv 3 \pmod 6 \end{cases}$$

Example: $\ell = 5$

$k = 2$, $g_1(x) = x^2 - x - 1$ and $\{a_n\}$ is the Lucas sequence.
$R_2(x) = x - 1$, $R_4(x) = -x$, $R_6(x) = -x$, $R_8(x) = x - 1$.

$$D_{j_c}(\{a_{cs}\}) = \begin{cases} a_{cs+1} - a_{cs} & \text{if } j_c \equiv 2, 8 \pmod{10} \\ -a_{cs+1} & \text{if } j_c \equiv 4, 6 \pmod{10} \end{cases}$$

$R_1(x) = x$, $R_3(x) = 1 - x$, $R_5(x) = -2$, $R_7(x) = 1 - x$,
$R_9(x) = x$.

$$D_{u_c}(\{a_{n_c}\}) = \begin{cases} a_{n_c+1} & \text{if } u_c \equiv 1, 9 \pmod{10} \\ a_{n_c} - a_{n_c+1} & \text{if } u_c \equiv 3, 7 \pmod{10} \\ -2a_{n_c} & \text{if } u_c \equiv 5 \pmod{10} \end{cases}$$

$$b_{q-1-n_c} = \begin{cases} \frac{1}{5}(2^{n_c} + a_{n_c+1}) & \text{if } u_c \equiv 1, 9 \pmod{10} \\ \frac{1}{5}(2^{n_c} - a_{n_c+1}) & \text{if } u_c \equiv 3, 7 \pmod{10} \\ \frac{1}{5}(2^{n_c} - 2a_{n_c}) & \text{if } u_c \equiv 5 \pmod{10} \end{cases}$$

PPs of form $x^r(x^{\frac{e(q-1)}{5}}+1)$ and inverse PPs over $\mathbb{F}_{19^2}$

PP	Inverse of PP
$x+x^{73}$	$10x+10x^{73}+10x^{145}+9x^{217}+9x^{289}$
x^5+x^{77}	$3x^{29}+14x^{101}+3x^{173}+16x^{245}+16x^{317}$
x^7+x^{79}	$5x^{31}+5x^{103}+10x^{175}+2x^{247}+10x^{319}$
$x^{11}+x^{83}$	$16x^{59}+2x^{131}+5x^{203}+2x^{275}+16x^{347}$
$x^{13}+x^{85}$	$5x^{61}+18x^{133}+18x^{205}+5x^{277}+7x^{349}$
$x^{17}+x^{89}$	$x^{89}+x^{305}$
$x^{23}+x^{95}$	$3x^{47}+14x^{119}+3x^{191}+16x^{263}+16x^{335}$
$\cdots$	$\cdots$

Outline

Summary

Summary

- Some connections between generalized Lucas sequences and PPs (inverses)

Question

- When is the inverse of $x^r(x^{es}+1)$ still a binomial for $\ell > 3$?

Thank you for your attention.

Happy birthday, Reza and IPM!