Bull. Korean Math. Soc. **29** (1992), No. 2, pp. 277–283

POLYNOMIALS SATISFYING $f(x+a) = f(x) + c$ OVER FINITE FIELDS

Hong Goo Park

1. Introduction

Let $GF(q)$ be a finite field with q elements where $q = p^n$ for a prime number p and a positive integer n. Consider an arbitrary function φ from $GF(q)$ into $GF(q)$. By using the Lagrange's Interpolation formula for the given function φ, φ can be represented by a polynomial which is congruent $\pmod{x^q - x}$ to a unique polynomial over $GF(q)$ with the degree $< q$. In [3], Wells characterized all polynomials over a finite field which commute with translations. Mullen [2] generalized the characterization to linear polynomials over the finite fields, i.e., he characterized all polynomials $f(x)$ over $GF(q)$ for which $\deg(f) < q$ and $f(bx+a) = b \cdot f(x) + a$ for fixed elements a and b of $GF(q)$ with $a \neq 0$. From those papers, a natural question (though difficult to answer) to ask is: what are the explicit form of $f(x)$ with zero terms?

In this paper we obtain the exact form (together with zero terms) of a polynomial $f(x)$ over $GF(q)$ for which satisfies $\deg(f) < p^2$ and

$$f(x+a) = f(x) + c \tag{1}$$

for the fixed nonzero elements a and c in $GF(q)$.

The characterization will be obtained by equating coefficients in (1) and using a result from Pólya's theory of enumeration (ref. [1] and [2]).

We will use the standard convention for binomial coefficients, i.e., $\binom{s}{t} = 0$ if $s < t$. We will require the following known property of binomial coefficients (E. Lucas 1887).

Received November 12, 1991.

If $s = \sum_{i=0}^{k} s_i p^i$ and $t = \sum_{i=0}^{k} t_i p^i$ $(0 \leq s_i,\ t_i \leq p-1)$ are the base p representations for s and t, then

$$(2) \qquad \binom{s}{t} \equiv \binom{s_1}{t_1}\binom{s_2}{t_2}\cdots\binom{s_k}{t_k} \pmod{p},$$

where p is a prime. It is well known that

$$(3) \qquad \binom{s}{t} = \binom{s-1}{t} + \binom{s-1}{t-1}.$$

Let $E_p(m)$ denote the largest exponent k such that p^k divides $m \in \mathbb{N}$, and d_s the sum of the digits in the representation of s written in base p.

Let $s = a_0 + a_1 p + \cdots + a_e p^e$ for some $e \in \mathbb{N}$. Then it is not hard to show that $s - d_s = \sum_{j=0}^{e} a_j(p^j - 1)$, and so $(s-d_s)/(p-1) = \sum_{j=1}^{e}[s/p^j] = E_p(s!)$. Thus,

$$(4) \qquad \begin{aligned} E_p\left(\binom{s}{t}\right) &= E_p(s!) - E_p((s-t)!) - E_p(t!) \\ &= (d_t + d_{s-t} - d_s)/(p-1). \end{aligned}$$

Consider a polynomial $f(x)$ of $GF(q)$. Then $\deg(f) = 1$ and $f(x)$ satisfies (1) if and only if $f(x) = a^{-1}cx + u$ for $u \in GF(q)$. So, assuming that $\deg(f) > 1$, we have the following result that represents the desired form of $f(x)$ satisfying (1).

THEOREM. *Let $f(x) = \sum_{i=0}^{d} b_i x^i$ be a polynomial of $GF(q)$ with $d < p^2$. Then $f(x)$ satisfies (1) if and only if the following conditions hold*

(a) *$d = rp$ for $0 < r < p$, and for each fixed m and k with $0 \leq k < m \leq r$,*

$$(m-k)b_{\delta_{mk}}a^p + (k+1)b_{\delta_{m,k+1}}a = \begin{cases} c, & \text{if } m = 1 \\ 0, & \text{otherwise}, \end{cases}$$

where $\delta_{mk} = mp - k(p-1)$.

(b) *The other coefficients which do not occur in (a) are all zero, except that b_0 is unrestricted.*

2. Proof of the Theorem

Let A_i denote the coefficient of x^i in the polynomial $f(x+a)$ in (1). Then

$$A_{d-i}=\sum_{j=0}^{i}\binom{d-j}{i-j}b_{d-j}a^{i-j}, \qquad (0\le i<d). \tag{5}$$

Suppose that the polynomial $f(x)$ satisfies the condition (1). Clearly $d=rp$ for $0<r<p$.

First, we will show part (b) in the theorem. To do this, we need to find all zero coefficients in $f(x)$ satisfying the given condition. By using (2) and induction on i with $1<r<p$,

$$\begin{aligned} A_{d-2} &= \binom{d}{2}b_d a^2+\binom{d-1}{1}b_{d-1}a+\binom{d-2}{0}b_{d-2}\\ &=(d-1)b_{d-1}a+b_{d-2}\\ &=-b_{d-1}a+b_{d-2}. \end{aligned}$$

Since $a\neq 0$, (1) implies $b_{d-1}=0$. Assuming $b_{d-i}=0$ for $1<i<p-2$, we can see easily that

$$A_{d-i-2}=-(i+1)b_{d-i-1}a+b_{d-i-2}.$$

So $b_{d-i-1}=0$. Thus $b_{d-i}=0$ for all $i=1,\cdots,p-2$.

In general we will prove that $b_{d-sp-t}=0$ for each fixed s with $0<s<r$ and t, $0<t<p-s-1$. Fix s and t. Assume that $b_{d-up-v}=0$ for all u and v satisfying either

(i) $0\le u<s\le r-1$ and $0<v<p-u-1$, or
(ii) $0<v<t<p-s-1$ if $u=s$.

With this assumption we will compute $A_{d-sp-t-1}$.

Let $z=z(s,t)=sp+t+1$ for each fixed s and t.
Then, by (5) and the induction hypothesis,

$$\begin{aligned} A_{d-z} &= \sum_{j=0}^{z}\binom{d-j}{z-j}b_{d-j}a^{z-j} \\ &= -tab_{rp-sp-t}+b_{rp-z}+\sum_{i=0}^{s}\sum_{j=0}^{i}\Delta_z(i,j)\cdot b_e a^y \end{aligned} \tag{6}$$

where $\triangle_z(i,j) = \binom{e}{y} = \binom{(r-i)p+i-j}{(s-i)p+i-j+t+1} = \binom{rp-i(p-1)-j}{z-i(p-1)-j}$.

So, if $0 < r-i < p$ and $0 \le s-i < p$ then $d_y + d_{e-y} - d_e = p-1$ implies $E_p[\triangle_z(i,j)] = 1$ by (5). This says $\triangle_z(i,j) \equiv 0 \pmod p$ for the fixed z and each given i and j. Hence, $A_{d-z} = -tab_{d-z-1} + b_{d-z}$. From (1) and the induction hypothesis, $b_{d-sp-t} = 0$ for every s and t such that $0 \le s \le r-1$ and $0 < t < p-s-1$. Note that b_0 is unrestricted. It is not hard to check that those coefficients in (b) run through all coefficients in $f(x)$ except the ones occurring in (a). This completes the proof of (b) in the theorem.

To obtain the first part, we first denote by $\mathcal{R}_{mk}$ the condition given in part (a) for each m and all k's such that $0 < k < m \le r$; that is,

$$\begin{aligned} &\mathcal{R}_{10} : b_p a^p + b_1 a = c, \\ &\mathcal{R}_{mk} : (m-k) b_{\delta_{mk}} a^p + (k+1) b_{\delta_{m,k+1}} a = 0 \end{aligned} \tag{7}$$

for $m \ne 1$.

For each fixed m and all k's with $0 < k < m \le r$, the condition $\mathcal{R}_{mk}$ will be obtained recursively by using (3-5) and finding a certain pattern of the binomial coefficents given by $f(x+a)$ in (1). We will see that each condition $\mathcal{R}_{mk}$ can be derived recursively by computing $A_{mp-kp-p+k}$ for each fixed m and all k's such that $0 < k < m \le r$.

Suppose that $m = r$. If $k = 0$, then

$$\begin{aligned} A_{d-p} &= \binom{\delta_{rk}}{p} b_{\delta_{rk}} a^p + \binom{\delta_{r,k+1}}{1} b_{\delta_{r,k+1}} a + b_{\delta_{r-1,k}} \\ &= r b_{\delta_{r0}} a^p + b_{\delta_{r1}} a + b_{d-p}. \end{aligned} \tag{8}$$

So the condition $\mathcal{R}_{r0}$ is obtained from (1).

In general, let $z = z(k) = kp + (p-k)$ and

$$\bar{\triangle}_k(i,j) = \triangle_k(i,j) \cdot b_e a^y = \binom{d - i(p-1) - j}{z - i(p-1) - j} b_e a^y,$$

where $e = d - i(p-1) - j$ and $y = z - i(p-1) - j$ for each fixed

$k=0,1,\cdots,r-1$ and some integers $i,\ j\geq 0$. Then one can see

$$\begin{aligned} A_{\delta_{r-1,k}} &= \bar{\triangle}_k(k,p-1)+\bar{\triangle}_k(k,p)+\sum_{i=0}^{k}\sum_{j=0}^{i}\bar{\triangle}_k(i,j) \\ &= \bar{\triangle}_k(k,0)+\bar{\triangle}_k(k,p-1)+\bar{\triangle}_k(k,p) \\ &\quad + \sum_{0\leq j\leq i\leq k-1}\bar{\triangle}_k(i,j)+\sum_{j=1}^{k}\bar{\triangle}_k(k,j). \end{aligned} \tag{9}$$

Note that $i-j-k$ is not divisible by p. Since $-k\leq i-j-k<0$ and $k<p$, $0<p+i-j-k<p$ implies that $E_p[\triangle_k(i,j)]=\{(k+p-j-k)+(r-1)-(r-j)\}/(p-1)=1$.
Thus $\triangle_k(i,j)\equiv 0 \pmod p$ for each $i,j<k$. By the same way, we can see $\triangle_k(k,j)\equiv 0 \pmod p$ for $j=1,2,\cdots,k$. Hence

$$A_{\delta_{r-1,k}}=(r-k)b_{\delta_{rk}}a^p+(k+1)b_{\delta_{r,k+1}}a+b_{\delta_{r-1,k}} \tag{10}$$

for each $k=1,2,\cdots,r-1$. By equating the coefficients in (1), we get the conditions $\mathcal{R}_{rk}$ for $0\leq k<r$.

To obtain the conditions $\mathcal{R}_{mk}$ for $0\leq k<m<r$, fix m and k. Suppose that $\mathcal{R}_{uk}$ is true for each u such that $m<u<r$. Then consider the coefficient of x^σ in $f(x+b)$ where $\sigma=\delta_{m-1,k}$. If $m-1\leq u<r$ and $0\leq v\leq r-1$ then the binomial coefficient in front of $b_{\delta_{uv}}$ in $A_{\delta_{m-1,k}}$ can be written by

$$\triangle_{mk}(u,v)=\binom{(u-v)p+v}{(u-v+k-m)p+(p-k+v)}. \tag{10'}$$

Let $u'=u-v+k-m$. Since $m-k\leq u-v<r$ and $0\leq k<m<r$, $0\leq u'\leq r-(m-k)<p$ for the fixed m and k. Thus $\triangle_{uv}\equiv 0 \pmod p$ by (4). Also, by (12), if $m-1<u\leq m-k$ and $k\leq v\leq k+u-m+1$, then $E_p[\triangle_{uv}(u,v)]=1$ implies $\triangle_{uv}(u,v)\equiv 0 \pmod p$.

Next choose u and v so that $m+1\leq u\leq r$ and $k\leq v\leq u-m+k+1$. Then we denote

$$S_{ui}=\sum_{i=0}^{u-m+1}\binom{u-k-i}{u-m+1-i}\binom{k+i}{i}b_{\delta_{u,k+i}}a^{\delta_{u-m-1,i}}. \tag{11}$$

Note that each binomial coefficient in (11) is not a zero modulo p. Let $B_{u0} = \binom{u-k}{u-m+1}/(u-k)$. Then, by using induction on $i = 0, 1, \cdots, m' - m$, it is not hard to show that there exists a nonzero number $B_{ui} \in GF(p)$ such that

$$(12) \qquad S_{ui} = \sum_{i=0}^{u-m} B_{ui} \cdot \{(u-k-i) b_{\delta_{u,k+i}} \cdot a^p + (k+i+1) b_{\delta_{u,k+i+1}} \cdot a\} a^{\delta_{u-m,i}}$$

where $B_{ui} = \{(u-m-i+1)(k+1)/i(u-k-i)\}$ for $i = 1, \cdots, u-m$.

We denote $R_{mk} = (m-k) b_{\delta_{mk}} \cdot a^p + (k+1) b_{\delta_{m,k+1}} \cdot a$.

By our assumption, each summation $S_{ui} \equiv 0 \pmod p$ since

$$(13) \qquad S_{ui} = \sum_{i=0}^{u-m} B_{ui} \cdot R_{u,k+i} \cdot a^{\delta_{u-m,i}}$$

for each given u and i. From (b) in theorem,

(14)

$$\begin{aligned} A_{\delta_{m-1,k}} &= \binom{\delta_{mk}}{p} b_{\delta_{mk}} \cdot a^p + \binom{\delta_{1k}+1}{1} b_{\delta_{m,k+1}} \cdot a + b_{\delta_{m-1,k}} \\ &= (m-k) b_{\delta_{mk}} a^p + (k+1) b_{\delta_{m,k+1}} a + b_{\delta_{m-1,k}} \\ &\quad + \sum_{u=m+1}^{r} \sum_{i=0}^{u-m+1} S_{ui}. \end{aligned}$$

Equating the above coefficients for each fixed m and all k's with $0 \le k < m < r$ in (1), the conditions $\mathcal{R}_{mk}$ in (a) of the theorem can now be derived. Therefore (a) and (b) in the theorem are both necessary if (1) is to hold.

Suppose that $f(x)$ is a polynomial satisfying (a) and (b). Let $u = (m-1)p - k(p-1)$. By (14) and (a) in Theorem, $A_u = R_{mk} + b_u = b_u$ for $0 \le k < m \le r$ and $m \ne 1$. And if $m = 1$, then $A_0 = b_p a^p + b_1 a + b_0 = c + b_0$. Thus the polynomials given by (a) and (b) in the theorem satisfy (1) and the number of such polynomials is exactly p^{np} (see remark 1.).

REMARK 1. In general, the number of polynomials $f(x)$ with the property (1) is $q^{p^{n-1}}$ (ref. [1] and [2]).

REMARK 2. Suppose that a polynomial $f(x)$ over $GF(q)$ satisfies (1) with $\deg(f) < p^2$. If $A_{mp-kp+k}$ is a coefficient of $x^{mp-kp+k}$-term in $f(x+a)$ for $0 \le k \le m \le r$, then

$$A_{mp-kp+k} = \begin{cases} b_{mp-kp+k}, & \text{if } m = r \\ (m-k+1)b_u a^P + (k+1)b_v a + b_{mp-kp+k}, & \text{otherwise} \end{cases}$$

where $u = (m+1)p - k(p-1)$ and $v = (m+1)p - (k+1)(p-1)$.

References

1. N. G. deBruijn, *Pólya's Theory of Counting*, Applied Combinatorial Mathematics (ED., E. F. Beckenbach), Wiley, New York, (1964), 164–166.
2. G. Mullen, *Polynomials over Finite Fields which commute with Linear Permutations*, Proc. Amer. Math. Soc. **84**(1982), 315–317.
3. C. Wells, *Polynomials over Finite Fields which commute with Translations*, Proc. Amer. Math. Soc. **46**(1974), 347–350.

DEPARTMENT OF MATHEMATICS, JEONJU UNIVERSITY, JEONJU, 560-759, KOREA