J. Korean Math. Soc. 30(1993), No. 1, pp. 41–49

POLYNOMIAL ISOMORPHISMS OF CAYLEY OBJECTS OVER THE FIELDS OF ORDER p^2

HONG GOO PARK

1. Introduction

We define a combinatorial object with a vertex set V to be a pair $\mathcal{C} = [V, S]$ where V is a set, and S is a subset of $V \cup 2^V \cup 2^{2^V} \cup \cdots$, called the structure. If $\mathcal{C}$ and $\mathcal{C}'$ are both combinatorial objects, then an isomorphism between $\mathcal{C}$ and $\mathcal{C}'$ is a bijective function from the vertex set of $\mathcal{C}$ to the vertex set of $\mathcal{C}'$ which also preserves the structures. An isomorphism from $\mathcal{C}$ to itself is called an automorphism of $\mathcal{C}$. It is clear that the set $\mathrm{Aut}(\mathcal{C})$ of all automorphisms of $\mathcal{C}$ constitues a group under the operation of composition and is a subgroup of the symmetric group S_V on the vertex set V.

Let V be a finite group and T the group of all translations $t_\alpha : V \longrightarrow V$ defined by $t_\alpha(x) = x + \alpha$ for $\alpha \in V$ and all $x \in V$. Then a combinatorial object $\mathcal{C}$ of V is called a Cayley object of V if $\mathrm{Aut}(\mathcal{C}) \supseteq T$ (see [2] for a similar definition).

ISOMORPHISM PROBLEM. Let $GF(q)$ denote a finite field of order $q = p^n$, where p is a prime number and n a positive integer. In 1930-1931, the first polynomial representation of isomorphisms between two combinatorial objects was found by Bays [4] and Lambossy [11]. They showed that if two Cayley objects of $GF(p)$ are isomorphic, then they are isomorphic by multiplier maps; that is, maps $f : GF(p) \longrightarrow GF(p)$ of the form $f(x) = ax$ for $a \in GF(p)\backslash\{0\}$.

To generalize this result, it is natural to drop the condition that $|V|$ is a prime in the theorem. In [1], Alspach and Parsons extend the theorem in the case of graphs and digraphs to the vertex set $\mathbf{Z}_{rs}$ for distinct primes r and s. There are many papers verifying that the

Received November 12, 1991. Revised August 19, 1992.
The research in this paper is partially supported by 1989-Faculty Reseach Grant of University of North Texas, Denton, TX, U.S.A. .

Bays-Lambossy theorem is still true for certain non-prime numbers [2,9,10,13]. From [1,3,5,9], we can see many examples of specific combinatorial objects (or Cayley objects) in which some assumption on $|V|$ is necessary. Pálfy [13] in 1987 solved the problem of determining when the Bays-Lambossy theorem generalizes to arbitrary Cayley objects.

He showed in [13] that the condition 'two Cayley objects of a finite group V are isomorphic if and only if they are isomorphic by a group automorphism', is satisfied exactly when the vertex set V is a group of order 4 or cyclic of order m with $\gcd(m, \phi(m)) = 1$, where ϕ is Euler's phi-function.

When does the Bays-Lambossy theorem generalize to a specific Cayley object such as graphs, digraphs, or designs? The aim of this paper is to investigate the polynomial representation of isomorphisms between two Cayley objects of a finite field $GF(p^2)$ in the case that Pálfy's conditions are not satisfied; that is $\gcd(m, \phi(m)) \neq 1$.

DEFINITION AND TERMINOLOGY. Let $\mathrm{Sym}(q)$ denote the symmetric group on $GF(q)$. Consider the ring $GF[q,x]$ of polynomials over $GF(q)$. A polynomial $f(x) \in GF[q,x]$ is called a permutation polynomial of $GF(q)$ if f, as a function, permutes elements of $GF(q)$. If $S[q,x]$ is the set of all functions induced by permutation polynomials $f(x) \in GF[q,x]$, then $S[q,x] \simeq \mathrm{Sym}(q)$. If $q > 2$, then we can normalize so that $\deg(f) < q-1$. By A, we mean the group of all invertible affine linear transformations of $GF(q)$ viewed as a vector space over $GF(p)$. Let $B[q,x]$ denote the Betti-Mathieu group (ref. [12, pp. 361–362]) whose elements are permutation polynomials over $GF(q)$ of the form

$$f(x) = \sum_{s=0}^{n-1} a_s x^{p^s} \in GF[q,x].$$

It is well-known that $B[q,x] \simeq GL(n,p)$, the general linear group of non-singular $n \times n$ matrices over $GF(p)$ under matrix multiplication. It follows from this that $A \simeq T \circ B[q,x] < S[q,x]$. Denote $\mathcal{A} = T \circ B[q,x]$. Each element in $\mathcal{A}$ is called an affine permutation p-polynomial of $GF(q)$.

Let $K = GF(q)$ and $F = GF(p)$. Then we define an absolute trace function $\mathrm{Tr} = \mathrm{Tr}_{K/F}$ of $\alpha \in K$ over F by

$$\mathrm{Tr}(\alpha) = \sum_{j=0}^{n-1} \alpha^{p^j}.$$

BRIEF DESCRIPTION OF MAIN RESULT. Let p be an odd prime. In [14], we characterized all polynomials $f(x)$ over $GF(q)$ for which $\deg(f) < p^2$ and $f(x+\beta) = f(x) + \alpha$ for the fixed nonzero elements α and β in $GF(q)$. By using this characterization, we will see in section 3 that two Cayley objects over $GF(p^2)$ satisfying certain conditions are isomorphic by a quadratic type permutation polynomial over $GF(p^2)$.

The statement and proof of the above main result is given in section 3. In section 2 and 3, we assume that p is an odd prime.

2. Preliminaries

By $a(f)$, we mean the cycle type of a permutation polynomial $f(x)$ of $GF(q)$. Let $f^{(m)}(x)$ be the m'th iterate of $f(x)$. For a polynomial $f(x) \in GF[q,x]$, the order $|f|$ of $f(x)$ is the least positive integer m such that $f^{(m)}(x) = x(\mathrm{mod} x^q - x)$. First we will prove

PROPOSITION 1. *Let $q = p^n$ with $n \geq 2$. Let $w(x) = \beta + x + L_\gamma(x) \in \mathcal{A}\backslash\{x\}$ for $\beta \in GF(q)$ and $\gamma \in \mathrm{Ker}(\mathrm{Tr})$, where $L_\gamma(x)$ denotes $\mathrm{Tr}(\gamma x)$. Then,*

(a) $\beta \in GF(p)$ and $\gamma \neq 0$ if and only if $w(x)$ is composed of $p^{n-1} - p^{n-2}$ disjoint cycles of length p.

(b) Either $\beta \in GF(q)\backslash\{0\}$ and $\gamma = 0$, or $\beta \notin GF(p)$ and $\gamma \neq 0$ if and only if $w(x)$ is composed of p^{n-1} disjoint cycles of length p.

Proof. (a) Suppose that $\beta \in GF(p)$ and $\gamma \in \mathrm{Ker}(\mathrm{Tr})\backslash\{0\}$. Clearly $w(x)$ is a permutation polynomial of $GF(q)$. If $w(\alpha) = \alpha$ for an element $\alpha \in GF(q)$, then $\beta + L_\gamma(\alpha) = 0$. Since L_γ is a linear transformation of $GF(q)$ over $GF(p)$, we can choose an element $c \in GF(q)$ such that $L_\gamma(c+\alpha) = 0$. Then $\gamma(c+\alpha) \in \mathrm{Ker}(\mathrm{Tr})$ if and only if $\alpha = \gamma^{-1}\eta - c$ for $\eta \in \mathrm{Ker}(\mathrm{Tr})$ for $\eta \in \mathrm{Ker}(\mathrm{Tr})$ and some $c \in GF(q)$ with $L_\gamma(c) = \beta$. So $w(x)$ fixes p^{n-1} elements of $GF(q)$ and is composed of $p^{n-1} - p^{n-2}$ disjoint cycles of length p since $|w| = p$.

Conversely, if $w(x)$ is composed of $p^{n-1} - p^{n-2}$ disjoint cycles of length p, then $\gamma \neq 0$ and there is an element $\alpha \in GF(q)$ such that $w(\alpha) = \alpha$. This implies $\beta = -L_\gamma(\alpha) \in GF(p)$.

(b) It is noted that either $\beta \in GF(q)\backslash\{0\}$ and $\gamma = 0$, or $\beta \neq GF(p)$ and $\gamma \neq 0$ if and only if there is no fixed element under $w(x)$. Since $|w| = p$, the above sufficient condition is true if and only if $w(x)$ is composed of p^{n-1} disjoint cycles of length p; that is, $a(w) = a(x+\beta)$.□

We will usually write our operators on the right. Let Y be a subset of a group G and $y \in Y$, $g \in G$. Then we will use the exponential notations Y^g for $g^{-1}Yg$, and y^g for $g^{-1}yg$.

Let G_1 and G_2 be contained in the symmetric group S_V on a set V. We set $H_{G_1}(G_2) = \{\pi \in S_V | G_1^\pi < G_2\}$. From the following Lemma 2, we obtain the existence of special kinds of isomorphisms between two isomorphic combinatorial objects of $GF(q)$. The proof can be found in [6, pp. 159–160].

LEMMA 2. *Suppose that $\mathcal{C}$ and $\mathcal{C}'$ are isomorphic combinatorial objects of a vertex set V. Let P be any Sylow p-subgroup of $Aut(\mathcal{C})$ and Q a p-group in $Aut(\mathcal{C}')$. Then $\mathcal{C}$ and $\mathcal{C}'$ are isomorphic by an element in $H_Q(P)$.*

Let $V = GF(q)$ and $S[q,x]$ the group of all permutation polynomial of $GF(q)$. If two combinatorial objects of $GF(q)$ are isomorphic, then the above lemma says that they are isomorphic by a function in $H_Q(P)$. By Lagrange's Interpolation Formula [8, pp.55], the function can be represented by a unique polynomial $f(x)$ of $GF(q)$ with $\deg(f) < q$ and

$$f(x) \in H_{\mathcal{L}}(\mathcal{P}) = \{h(x) \in S[q,x] | \mathcal{L}^h < \mathcal{P}\}$$

where $\mathcal{P}$ and $\mathcal{L}$ are the polynomial representations over $GF(q)$ of P and Q. Respectively, this is quite natural because $\mathrm{Aut}(\mathcal{C}) < \mathrm{Sym}(q) \simeq S[q,x]$.

Consider the group $\mathcal{W} = \{w(x) = \beta + x + L_\gamma(x) \in \mathcal{A} | \beta \in GF(q), \gamma \in \mathrm{Ker(Tr)}\}$.

LEMMA 3. *If $f(x) \in H_T(\mathcal{W})$, then $f(x+c) = f(x) + f(c) - f(0)$ for every $c \in GF(p)$.*

Proof. Suppose that $f(x) \in H_T(\mathcal{W})$. Then, for each $\alpha \in GF(q)$, we can choose a unique $w(x) = \beta + x + L_\gamma(x) \in \mathcal{W}$ such that

$$f(x) + \alpha = f(\beta + x + L_\gamma(x)). \tag{1}$$

It follows from (1) that $f(c) + \alpha = f(\beta + c)$ for $c \in GF(p)$. Also (1) implies that $f(c) + f(\beta) - f(0) = f(\beta + c)$. Since β is uniquely determined by α and runs through all elements of $GF(q)$, $f(c)+f(x)-f(0) = f(x + c)$ for every $c \in GF(p) \cdot \square$

Next, for an arbitrary prime p, we characterize all polynomials $f(x)$ over $GF(q)$ for which $\deg(f) < p^2$ and

$$f(x + \beta) = f(x) + \alpha \tag{2}$$

for fixed $\alpha, \beta \in GF(q)\backslash\{0\}$. If $\deg(f) = 1$, then $f(x) \in GF[q, x]$ satisfies (2) if and only if $f(x) = \alpha\beta^{-1}x + u$ for $u \in GF(q)$. So we assume now that $\deg(f) \neq 1$ in (2). By equating the coefficients in (2) we can obtain the following Theorem 4. The proof is given in [14].

THEOREM 4. *Let $f(x) = \sum_{i=0}^{d} b_i x^i \in GF[q, x]$ with $d < p^2$. Then $f(x)$ satisfies (2) if and only if the following conditions hold:*

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

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

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.

3. Main Result

The main result can now be stated as follows and the result can be improved if more is known about the automorphism group of C.

THEOREM 5. *Let $\mathcal{C}$ and $\mathcal{C}'$ be any two Cayley objects of $GF(p^2)$ for an odd prime p. Define a linear operator $\phi : GF(p^2) \longrightarrow GF(p^2)$ by $\phi(x) = x^p - x$ for all $x \in GF(p^2)$. Suppose that there is a Sylow p-subgroup P of $Aut(\mathcal{C})$ with $T \subseteq P \subseteq A$. Then $\mathcal{C}$ and $\mathcal{C}'$ are isomorphic by a permutation polynomial over $GF(p^2)$ of the form*

$$f(x) = a[\phi(\lambda x)]^2 + w(x),$$

where both a and λ are some elements of $GF(p^2)$ and $w(x) \in \mathcal{A}$.

Proof. Let $q = p^2$ for an odd prime p. Suppose that P is a Sylow p-subgroup of $\mathrm{Aut}(\mathcal{C})$ such that $T \subseteq P \subseteq A$. Let $\mathcal{P}$ denote the polynomial representation over $GF(q)$ of P. By Lemma 2, an isomorphism of $\mathcal{C}$ and $\mathcal{C}'$ can be expressed by a permutation polynomial $f(x)$ in $H_T(\mathcal{P})$ with $\deg(f) \leq q-1$ since $\mathcal{C}'$ is a Cayley object of $GF(q)$.

Consider the group $\mathcal{W}$ as mentioned earlier for $n = 2$. Since $|\mathcal{W}| = p^3$, it is clear that $\mathcal{W}$ is a Sylow p-subgroup of $\mathcal{A}$. Since $\mathcal{P}$ is a p-subgroup of $\mathcal{A}$, there exists a Sylow p-subgroup $\mathcal{H}$ of $\mathcal{A}$ such that $T < \mathcal{P} < \mathcal{H}$. By the Sylow theorems we can choose a polynomial $\psi(x) \in \mathcal{A}$ so that $T^{f\psi^{-1}} < \mathcal{P}^{\psi^{-1}} < \mathcal{H}^{\psi^{-1}} = \mathcal{W}$. Since $\psi(x) = l(x) + c$ for some $c \in GF(q)$ and some permutation polynomial $l(x) \in B[q, x]$, $f(x)$ can be written as $g(l(x))$ for $g(x) \in H_T(\mathcal{W})$.

If $h(x) = g(x) - g(0)$, then $h(x) = t_c^{-1}g(x)$ for $c = g(0)$ and $T^h = [T^{t_c^{-1}}]^g = T^g < \mathcal{W}$ since T is commutative. Thus it is sufficient to find all polynomials $h(x)$ of $GF(q)$ for which $h(0) = 0$ and $T^h < \mathcal{W}$. If $\mathcal{W}' = \{w(x) = \beta + x + L_\gamma(x) \in \mathcal{W} | \beta \in GF(p) \text{ and } \gamma \in \mathrm{Ker(Tr)} \setminus \{0\}\}$, then $T^h \subset \{\mathcal{W} \setminus \mathcal{W}'\} = W_*$ by Proposition 1. So $H_T(\mathcal{W}) = H_T(\mathcal{W}_*)$. Then, for each $\alpha \in GF(q)$, there exists a unique polynomial $w(x) = \beta + x + L_\gamma(x) \in \mathcal{W}_*$ such that $t_\alpha^h(x) = w(x)$.

Since $h(x)$ is a permutation polynomial of $GF(q)$ with $h(0) = 0$, we have an element $z \in GF(q)$ such that $t_\alpha^h(z) = 0 = h^{-1}(\alpha) + z + L_\gamma(z)$ for each $\alpha \in GF(q)$. Then $t_\alpha^h(z) = 0$ if and only if $z = h^{-1}(-\alpha)$, and so

$$h^{-1}(\alpha) + h^{-1}(-\alpha) = (z^p - z)\gamma \tag{3}$$

for every $\alpha \in GF(q)$ and the corresponding $\gamma \in \mathrm{Ker(Tr)}$.

Let Γ be the set of elements $\gamma \in \mathrm{Ker}(\mathrm{Tr})$ satisfying (3) for each $\alpha \in GF(q)$. Then we define a mapping $\xi : GF(q) \longrightarrow GF(q) \times \Gamma$ by

$$\xi(\alpha) = \begin{cases} (h^{-1}(\alpha), 0), & \text{if } \alpha \in h(GF(p)) \\ (h^{-1}(\alpha), [h^{-1}(\alpha) + z]/[z^p - z]), & \text{otherwise} \end{cases}.$$

Clearly the mapping ξ is well-defined and injective. Thus $h(x)$ satisfies (2) if and only if there exists a unique $\xi(\alpha) = (h^{-1}(\alpha), \gamma) \in GF(q) \times \Gamma$ such that, for all $\alpha \in GF(q)$,

$$h(h^{-1}(\alpha) + x + L_\gamma(x)) = h(x) + \alpha. \tag{4}$$

Since $L_\gamma(c) = 0$ for $c \in GF(p)$, Lemma 3 and (4) imply that $h(x) \in H_T(\mathcal{W})$ also satisfies, for $c \in GF(p)$,

$$h(x + c) = h(x) + h(c). \tag{5}$$

Let $h(x) = \sum_{s=1}^{d} b_s x^s \in GF[q, x]$ with $d < q$. If $d = 1$, then $h(x)$ represents a multiplier mapping on $GF(q)$. So we assume that $d \neq 1$. By Theorem 4 and (5), $d = rp$ for $0 < r < p$ and $(m-k)b_{mp-kp+k} + (k+1)b_{mp-kp-p+k+1} = 0$ for $2 \leq m \leq r, 0 \leq k \leq m-1$. It follows from this that if we let $A_i = b_{ip} + b_{ip-p+1} + b_{ip-2p+2} + \cdots + b_i$ for $i = 1, 2, \cdots, r$, then all $A_i = 0$ except $i = 1$. Thus, by Theorem 4,

$$\begin{aligned} h(L_\gamma(x)) &= \sum_{i=1}^{r} \sum_{k=0}^{i} b_{ip-kp+1} (\gamma x + \gamma^p x^p)^{ip-kp+k} \\ &= \sum_{i=1}^{r} \sum_{j=0}^{i} \binom{i}{j} A_i (\gamma x)^{i+jp-j} \\ &= \sum_{j=0}^{1} \binom{1}{j} A_1 (\gamma x)^{1+jp-j} \\ &= (b_1 + b_p) \cdot L_\gamma(x). \end{aligned} \tag{6}$$

From (6), for all $\alpha \in GF(q)$ with $\beta = h^{-1}(\alpha)$, $h(\beta + x) + h(L_\gamma(x)) = h(x) + \alpha$, and so every term in the right hand side will vanish except x^p, x, and the constant term. By equating those three terms, we can have the following two conditions for $h(x) \in H_T(\mathcal{W}_*)$:

(I) $2b_{2p}(\beta^p - \beta) = (b_1 + b_p)\gamma$, and

(II) $b_p\beta^p + b_1\beta = \alpha$,

for all $\alpha \in GF(q)$ with $\xi(\alpha) = (\beta, \gamma) \in GF(q) \times \Gamma$.

Since $\beta = h^{-1}(\alpha)$ runs through all elements of $GF(q)$, $b_1 + b_p \neq 0$ from (II). Hence, (I) and (II) imply that if $h(x) \in H_T(\mathcal{W})$ with $h(0) = 0$, then the polynomial is of the form $h(x) = a(x^p - x)^2 + bx^p + cx$ for some a, b and $c \in GF(q)$. Futhermore, $bx^p + cx \in B[p^2, x]$ and $a(\beta^p - \beta) = (b + c)\gamma$ for $(\beta, \gamma) = \xi(\alpha) = (h^{-1}(\alpha), \gamma) \in GF(q) \times \Gamma$.

On the other hand, if a polynomial $h(x) = a(x^p - x) + bx^p + cx \in GF[q, x]$ with the condition (I) and (II), then it can be easily shown that $h(\beta + x + L_\gamma(x)) = h(x) + \alpha$. Thus the given polynomial $h(x) \in H_T(\mathcal{W})$. According to the above results, we prove that a polynomial $h(x) \in H_T(\mathcal{W})$ with $T \subseteq P \subseteq A$ and $h(0) = 0$ if and only if $h(x) = a(x^p - x)^2 + k(x)$ for $k(x) \in B[p^2, x]$ such that $2a(\beta^p - \beta) = k(1) \cdot \gamma$ for $(\beta, \gamma) = \xi(\alpha) \in GF(p^2) \times \Gamma$.

Therefore, two Cayley objects of $GF(p^2)$ with $T \subseteq P \subseteq A$ are isomorphic if and only if they are isomorphic by a function in $H_T(\mathcal{W})$ and the function on $GF(p^2)$ can be represented by a permutation polynomial of the form

$$\begin{aligned} f(x) = g(l(x)) &= h(l(x)) + g(0) \\ &= a[\phi(\lambda x)]^2 + \omega(x) \end{aligned}$$

where both a and λ are some elements of $GF(p^2)$ and $w(x)$ is an affine permutation p-polynomial of $\mathcal{A}$. □

REMARK. The affine group A in Theorem 5 is obviously a subgroup of $Sym(q)$, but not necessarily a subgroup of $\mathrm{Aut}(\mathcal{C})$. N.Brand [7] calculated the automorphism groups of a family of $2-(v, 3, 2)$ designs. In the same paper, he also found a block design whose automorphism group is isomorphic to the general linear groups with certain conditions. In fact, it is an complicated problem in this area to find the group structure of $\mathrm{Aut}(\mathcal{C})$ over an arbitrary Cayley object. It remains an

interesting unsolved problem to generalize the Bays-Lambossy theorem to an arbitrary Cayley object.

ACKNOWLEDGMENT. The author is indebted to Dr. Neal Brand for his encouragement and helpful comments.

References

1. B.Alspach and T.D. Parsons, *Isomorphism of circulant graphs and designs*, Discrete Math. **25** (1979), 97–108.
2. L.Babai, *Isomorphism problem for a class of point-symmetric structures*, Acta Math. Acad. Sci. Hungar. **29** (1977), 329–336.
3. L.Babai and P. Frankl, *Isomorphism of Cayley graphs I*, Colloq. Math. Soc. J. Bolyai, 18. Combinatorics, Keszthely, (1976), North-Holland, Amsterdam, (1978), 35–52.
4. S.Bays, *Sur les systèms cycliques de triples de Steiner différents pour N premier (ou puissance de nombre premier) de la forme* $6n+1$, *Comment. Math. Helv. 2 (1930), 294-305: II-VI, Comment. Math. Helv. 3 (1931), 22-41, 122-147, 307-325.*
5. N.Brand, *Isomorphic designs that are not multiplier equivalent*, Discrete Math. **57** (1985), 159–165.
6. ———, *Quadratic isomorphisms of* $\mathbf{Z}_p \oplus \mathbf{Z}_p$ *objects*, Congressus Numer. **58** (1987), 157–163.
7. ———, *Design isomorphisms and group isomorphisms*, Geometriae Dedicata **27** (1988), 281–294.
8. L.E. Dickson, *Linear groups: With an exposition of the Galois field theory*, Dover, New York (1958).
9. B. Elspas and J. Turner, *Graphs with circulant adjacency matrices*, J. Combin. Theory **9** (1970), 297–307.
10. C.D. Godsil, *On Cayley graph isomorphisms*, Ars Combin. **15** (1983), 231–246.
11. P. Lambossy, *Sur une manière de différencier les fonctions cycliques d'une forme donnée*, Comment. Math. Helv. **3** (1931), 69–102.
12. R. Lidl and H. Niedereiter, *Finite fields*, Encyclopedia Math., Appl. Vol 20, Addison-Wesley, Reading, Mass. (1983).
13. P.P. Pálfy, *Isomorphism problems for relational structures with a cyclic automorphism*, European J. Combin. **8** (1987), 35–43.
14. H.G. Park, *Polynomials satisfying* $f(x+a) = f(x) + c$ *over finite fields*, Bull. Korean Math. Soc. **29**(1992), No. 2,, 277–283.

Department of Mathematics
Jeonju University
Jeonju, 560-759, Korea