第16卷第3期 数学研究与评论 Vol. 16 No. 3
1996年8月 JOURNAL OF MATHEMATICAL RESEARCH AND EXPOSITION Aug. 1996

有限域上具有交换图表性质的多项式*

邵嘉裕 郭镜明
(同济大学应用数学系, 上海200092)

摘 要 本文给出了有限域 F_q 上满足条件 $f(g(x)) \equiv h(f(x))$ 的多项式 $f(x)$ 的通解表示公式及在 $\deg f < q$ 条件下的 $f(x)$ 的个数计算公式, 此地 $g(x)$ 和 $h(x)$ 是 F_q 上给定的两个多项式, 其中之一是置换多项式. 这一结果推广了文献[3]的主要结果, 而在 $g(x)$ 和 $h(x)$ 均为线性多项式的特殊情况, 则分别推广了文献[1]和[2]中的主要结果.

关键词 有限域, 多项式, 有向图
分类号 AMS(1991) 12E05/CCL O153.4

§1 引 言

设 p 为素数, n 为正整数, $q = p^n$, 记 F_q 为含有 q 个元素的有限域, $F_q[x]$ 为域 F_q 上以 x 为不定元的一元多项式的集合. 对 F_q 上的两个多项式 $f_1(x)$ 和 $f_2(x)$, 若它们作为多项式函数相等, 即若 $f_1(a) = f_2(a)$, $\forall a \in F_q$, 则称此两多项式恒等, 记作 $f_1(x) \equiv f_2(x)$. 易知 $f_1(x) \equiv f_2(x)$ 的充要条件是 $f_1(x) \equiv f_2(x) \pmod{(x^q - x)}$. F_q 上一个多项式 $g(x)$ 称为是置换多项式, 若 $g(x)$ 作为 F_q 到自身的映射是一个一一对应.

Wells 在[1]中给出了 F_q 上满足如下条件

$$f(x + a) \equiv f(x) + a \tag{1.1}$$

的多项式 $f(x)$ 的特征刻画, 此地 $a \in F_q$, 且 $a \neq 0$. 他并用 Pólya 计数定理确定了满足(1.1)且次数 $\deg f < q$ 的多项式 $f(x)$ 的个数为 $q^{p^{n-1}}$. Mullen 在[2]中推广了Wells 的结论, 并给出了 F_q 上满足条件

$$f(bx + a) \equiv bf(x) + a \tag{1.2}$$

的多项式 $f(x)$ 的特征刻画(此地 $a, b \in F_q$, 且 $b \neq 0$), 并且确定了: 若 b 在 F_q 的非零元乘法群 F_q^* 中的阶是 $k > 1$, 则满足(1.2)且次数 $\deg f < q$ 的多项式 $f(x)$ 的个数为 $q^{\frac{q-1}{k}}$. C. Y. Chao 在[3]中进一步把Wells 和Mullen 的结论推广到了更一般的情形, 他利用 Schur 的关于置换群的中心化环的思想方法, 用矩阵的形式给出了 F_q 上满足条件

$$f(g(x)) \equiv g(f(x)) \tag{1.3}$$

的多项式 $f(x)$ 的特征刻画. 此地 $g(x)$ 是 F_q 上给定的一个置换多项式. 他还用 Pólya 计数定理给出了计算满足条件(1.3)且次数 $\deg f < q$ 的多项式 $f(x)$ 的个数的一个公式, 并给出了找出

* 1994年6月21日收到. 96年4月18日收到修改稿. 国家自然科学基金资助项目.

全部 $f(x)$ 的通解的一个算法. 易见文[1]、[2]中的结果分别是[3]中当 $g(x)=x+a$ 和 $g(x)=bx+a$ 时的特殊情形. 但是, 文[1]、[2]和[3]都未能给出满足条件的 $f(x)$ 的通解的表达式.

在本文中将运用与文[1]、[2]、[3]不同的方法(主要是代数方法与图论方法相结合的方法), 讨论形式更为一般的问题: 设 $g(x), h(x)$ 是域 F_q 上给定的两个多项式, 称 F_q 上多项式 $f(x)$ (对 $g(x)$ 和 $h(x)$ 而言) 是满足"交换图表"性质的, 如果 $f(x)$ 满足

$$f(g(x)) \equiv h(f(x)), \tag{1.4}$$

将给出当 $g(x)$ 和 $h(x)$ 中只需有一个是置换多项式时, 满足(1.4)的多项式 $f(x)$ 的通解表示式及在条件 $\deg f < q$ 下 $f(x)$ 的个数计算公式. 显然, 文[3]中研究的问题是此地 $g(x)=h(x)$ 时的特殊情形. 这样, 本文不仅所讨论的问题比文[1], [2], [3]更为一般, 而且得到了比文[1], [2], [3]更进一步的结论 —— 即给出了满足条件(1.4)的多项式 $f(x)$ 的通解表示式.

§2 主要结果

有限域 F_q 上任一多项式 $f(x)$ 显然可视为 F_q 上的一个函数, 因此它对应了 F_q 到自身的一个映射 f. 反之, 对 F_q 到自身的任一映射 φ, 并作如下多项式

$$f(x)=\sum_{a\in F_q}\varphi(a)[1-(x-a)^{q-1}], \tag{2.1}$$

则不难验证 $\deg f < q$, 且对任意 $b\in F_q$, 有 $f(b)=\varphi(b)$. 即此多项式 $f(x)$ 所对应的映射就是 φ. 这样就在 F_q 上所有次数小于 q 的多项式的集合和 F_q 到自身的所有映射的集合之间建立了一个一一对应. 在这个对应关系下, 多项式 $f(x)$ 满足 $f(g(x))\equiv h(f(x))$ 当且仅当其相应的映射 f 满足 $fg=hf$. 这样就可先把求多项式的问题转化为求映射的问题, 然后把所求出的满足条件的全部映射依(2.1)式写出相应的多项式, 即可得到满足(1.4)且 $\deg f < q$ 的全部多项式 $f(x)$ 的通解了. 把它们再加上 x^q-x 的任意倍式, 即得满足(1.4)且次数不限的全部 $f(x)$ 的通解表示式了.

为方便起见以下记

$$Q_a(x)=1-(x-a)^{q-1}, \tag{2.2}$$

显然 $Q_a(a)=1$ 而当 $b\neq a$ 时, 则有 $Q_a(b)=0$. 为简便计, 也常记 $Q_a(x)=Q_0(x-a)$.

要给出满足条件 $fg=hf$ 的全部映射 f 显然取决于给定映射 g 和 h 的特征. 一般说来, 当 g 或 h 不是置换(即不是一一对应)时, 它的结构可能是相当复杂的. 此时能够最清楚地描述此映射的就是下面将引进的"伴随有向图".

以下记 $\mathbf{F}_V$ 为有限集 V 到自身的全体映射所成的集合(并将 $\mathbf{F}_{F_q}$ 简记为 $\mathbf{F}_q$). V 到 V 的一个一一对应称为是 V 上的一个置换. V 上的全体置换所成的群称为 V 上的对称群, 记作 S_V.

定义 2.1 映射 $f\in\mathbf{F}_V$ 的伴随有向图 $D(f)$ 定义为以 V 为点集, 以 $E=\{(u,v)\in V\times V \mid f(u)=v\}$ 为弧集合的有向图.

注意有向图 $D(f)$ 中是允许有环(loop)的.

由定义易见 $D(f)$ 也完全确定了映射 f (f 在任一点 u 处的象就是 $D(f)$ 中从 u 点发出的唯一弧的终点). 任一映射 $f\in\mathbf{F}_V$ 的伴随有向图 $D(f)$ 都是一个每点出度均为1的有向图(简称

为 1- 出度有向图), 且反之亦然. 为了给出 1- 出度有向图的基本结构特征, 先引进"有向树形图"的概念.

引理 2.1 设 n 阶有向图 $D=(V,E)$ 中恰有一个点 v^* 的出度 $d^+(v^*)=0$, 而其余各点的出度均为 1, 则如下四条件等价:

(1) 从 D 中任一点 v 均有 v 到 v^* 的有向路.

(2) D 看作无向图(即若不计 D 中弧的方向) 时是连通的.

(3) D 不含无向圈.

(4) D 不含有向圈.

当这些条件满足时, 这样的 D 称为是一个以 v^* 为根的"有向树形图".

证明 (1)⇒(2) 对 D 中任意点 u 和 v, 由(1) 知它们均有路到 v^*, 故 u 和 v 之间可由无向路相连.

(2)⇒(3) D 的弧数等于 D 中各点出度之和, 故有 $|E|=\sum_{v\in V}d^+(v)=n-1$. 故 D 看作无向图时是含 $n-1$ 条边的 n 阶连通图, 从而是一个无向树[4]. 于是 D 不含无向圈.

(3)⇒(4) 显然.

(4)⇒(1) 令 P 为 D 中以 v 为始点的最长有向路, 则 P 的终点 u 必定是那个出度为 0 的点 v^*. 因若不然, 设 u 还发出一条弧 (u,w). 则当 $w\notin V(P)$ 时, $P+(u,w)$ 将是以 v 为始点的一条比 P 更长的路, 这与 P 的取法矛盾; 而当 $w\in V(P)$ 时, P 中从 w 到 u 的子路加上弧 (u,w) 将构成一个有向圈, 这与条件(4) 矛盾. 于是 $u=v^*$, 而 P 就是 v 到 v^* 的一条有向路. □

由于 1- 出度有向图的每个无向连通分支也是 1- 出度有向图, 因此只需研究"无向连通"(即视为无向图时是连通) 的 1- 出度有向图即可.

引理 2.2 设 $D=(V,E)$ 是个 n 阶无向连通的 1- 出度有向图, 则有:

(1) D 含有唯一的一个无向圈 C, 且 C (在考虑其上弧的方向时) 也恰好是一个有向圈,

(2) 设 $T_1,\cdots,T_k$ 是 D 删去 C 中全部弧后的有向图 $D-E(C)$ 的所有无向连通分支(简称为 D 的"枝"), 则:

(i) 每个 T_i 恰含唯一的一个 C 上点(不妨设为 u_i),

(ii) T_i 是一个以 u_i 为根的有向树形图.

证明 (1) 取 T 为 D 的一个无向生成树, 则 T 恰含 $n-1$ 条边. 又因 $|E|=\sum_{v\in V}d^+(v)=|V|=n$, 即 D 恰含 n 条弧, 故 D 作为无向图时等于生成树 T 添加一条边, 从而恰含一个无向圈.

另一方面, D 中若无有向圈, 则与引理 2.1 中(4)⇒(1) 类似地可证 D 中一条最长路的终点必定是出度为 0, 这与每点出度为 1 的条件矛盾. 于是 D 中有有向圈. 但 D 中又只有唯一的一个无向圈 C, 故 C 也必是有向圈.

(2) (i) 若 $D-E(C)$ 的某个(无向) 分支 T_i 不含 C 上点, 则 T_i 和 C 在 $D=(D-E(C))+E(C)$ 中将属于两个不同的连通分支, 这与 D 无向连通相矛盾. 若某个 T_i 含有 C 上两个不同点, 设为 x 和 y, 则 x 和 y 在 T_i 中有(无向) 路相连, 且此路的任一边都是 C 外边, 由此将可知 D 中至少有三个(过点 x 和 y 的) 无向圈, 这与结论(1) 相矛盾.

(ii) 易见 u_i 在 T_i 中出度为 0(因 u_i 发出的唯一弧是 C 中弧, 在 $D-E(C)$ 中已被删去), 而

T_i 中其余各点的出度均为 1(因其余各点不在 C 上, 其发出的弧也不是 C 上弧, 故在 $D - E(C)$ 中), 又 T_i 作为无圈图 $D - E(C)$ 的子图也无圈 于是由引理 2 1 知 T_i 是一个以 u_i 为根的有向树形图 □

下面回过头来讨论满足条件 $fg = hf$ (其中 $g, h \in \mathbf{F}_V$ 为给定, 且至少有一个是置换) 的映射 f 的存在性、构造和特征刻画等问题 先引入如下概念:

定义 2 2 设 $g, h \in \mathbf{F}_V$ 的伴随有向图分别为 $D(g)$ 和 $D(h)$, A, B 分别为 $D(g)$ 和 $D(h)$ 中的一个有向圈, 其长分别记作 $l_g(A)$ 和 $l_h(B)$. 若 $l_h(B) \mid l_g(A)$, 则称圈 B 为圈 A 在 $D(h)$ 中的一个因子圈

为方便起见, 以下规定记号 $h^j(x)$ 表示 j 个多项式 $h(x)$ 的复合, 而 $(h(x))^j$ 表示 j 个 $h(x)$ 的乘积

引理 2 3 设 V 为有限集, $g, h \in \mathbf{F}_V$, g 和 h 中至少有一个是置换 g 和 h 的伴随有向图分别为 $D(g)$ 和 $D(h)$. 设 $A_1, \cdots, A_r$ 为 $D(g)$ 的全部有向圈, $a_i \in V(A_i)$ $(i = 1, \cdots, r)$. 则有

(1) 任一满足条件 $hf = fg$ 的映射 $f \in \mathbf{F}_V$ 由 f 在 $a_1, \cdots, a_r$ 处的象所唯一确定

(2) 设 $c_1, \cdots, c_r \in V$, 则存在 $f \in \mathbf{F}_V$ 满足

$$hf = fg \text{ 且 } f(a_i) = c_i \ (i = 1, \cdots, r) \tag{2 3}$$

的充要条件是 c_i 落在圈 A_i 在 $D(h)$ 中的某个因子圈上

(3) 满足(2) 中条件的 f 若存在, 则必唯一.

证明 (1) 情形 1: 若 g 是置换, 则 V 中任一点都落在 $D(g)$ 的某一圈上 任取 $a \in V$, 不妨设 a 落在 $D(g)$ 中的圈 A_i 上, 则必存在正整数 j, 使 $a = g^j(a_i)$. 于是当 $hf = fg$ 时有

$$f(a) = f(g^j(a_i)) = h^j(f(a_i)),$$

即 $f(a)$ 由诸 $f(a_i)$ 之值所确定

情形 2: 若 h 是置换 任取 $a \in V$, 不妨设 a 属于 $D(g)$ 中含有有向圈 A_i 的那个无向连通分支 $D_i(g)$. 则由引理 2 1 及引理 2 2 知 $D(g)$ 中存在从点 a 到点 a_i 的有向路, 于是存在 j (事实上可取 j 为 $D(g)$ 中从点 a 到点 a_i 的距离 $d_g(a, a_i)$) 使 $a_i = g^j(a)$. 因此当 $hf = fg$ 时有

$$h^j(f(a)) = f(g^j(a)) = f(a_i).$$

但 h 是置换, 存在逆映射 h^{-1}. 故由上式得

$$f(a) = h^{-j}(f(a_i)),$$

此时 $f(a)$ 同样可由 $f(a_i)$ 之值所确定

(2) 以下用记号 $l_h(c_i)$ 和 $l_g(a_i)$ 分别表示 $D(h)$ 中含点 c_i 的圈之长及 $D(g)$ 中含点 a_i 的圈之长

必要性 若存在 f 满足(2 3), 则由 $g^{l_g(a_i)}(a_i) = a_i$ 可得

$$h^{l_g(a_i)}(c_i) = h^{l_g(a_i)}(f(a_i)) = f(g^{l_g(a_i)}(a_i)) = f(a_i) = c_i \ (i = 1, \cdots, r),$$

于是 c_i 必落在有向图 $D(h)$ 的某个有向圈上, 且满足 $l_h(c_i) \mid l_g(a_i)$, 即 c_i 落在圈 A_i 在 $D(h)$ 中的某个因子圈上

充分性 情形 1: 若 g 是置换 对任一 $a \in V$, 与 (1) 中同样地论证知 a 可表为 $a = g^j(a_i)$. 构作映射 $f \in \mathbf{F}_V$, 使

$$f(a) = h^j(c_i) \quad (\text{若 } a = g^j(a_i)), \tag{2 4}$$

则可验证这样构作的映射 f 是合理定义的. 因若有 $g^j(a_i) = g^{j_1}(a_{j_1})$, 则 a_i 和 a_{i_1} 属于有向图 $D(g)$ 的同一个无向连通分支, 故属于 $D(g)$ 的同一圈(因由引理 2.2 知该无向分支中只有唯一圈), 从而 $i = i_1$. 又由 $l_h(c_i) \mid l_g(a_i)$ 得: $g^j(a_i) = g^{j_1}(a_i) \Rightarrow j \equiv j_1 (\mathrm{mod}\, l_g(a_i)) \Rightarrow j \equiv j_1 (\mathrm{mod}\, l_h(c_i)) \Rightarrow h^j(c_i) = h^{j_1}(c_i) = h^{j_1}(c_{i_1})$, 故知 f 是合理定义的.

又当 $a = g^j(a_i)$ 时, 有

$$h(f(a)) = h^{j+1}(c_i) = f(g^{j+1}(a_i)) = f(g(a)) \tag{2.5}$$

及 $f(a_i) = f(g^0(a_i)) = h^0(c_i) = c_i$, 故 f 满足(2.3).

情形 2: 若 h 是置换. 对任一 $a \in V$, 与(1)同样地论证知有 i, j, 使 $a_i = g^j(a)$. 此时构作映射 $f \in \mathbf{F}_V$, 使

$$f(a) = h^{-j}(c_i) \quad (\text{若 } a_i = g^j(a)). \tag{2.6}$$

则当有 $a_i = g^j(a)$, $a_{i_1} = g^{j_1}(a)$ 时, a_i 和 a_{i_1} 属于 $D(g)$ 的同一无向分支, 故属 $D(g)$ 的同一圈, 从而 $i = i_1$. 又由 $a_i = g^j(a) = g^{j_1}(a)$ 及 $l_h(c_i) \mid l_g(a_i)$ 也容易推出 $h^{-j}(c_i) = h^{-j_1}(c_i)$. 故这样构作的 f 也是合理定义的. 类似地又可验证 f 也满足(2.3). 充分性得证.

(3) 由(1)即知当 $f(a_i) = c_i$ ($i = 1, \cdots, r$) 确定后, 满足条件 $hf = fg$ 的映射 f 若存在, 则只有一个. □

下面再利用插值多项式公式(2.1)将上述关于映射的结论转化到 F_q 上的多项式上去.

定理 2.1 设 $h(x), g(x) \in F_q[x]$, 其中 $g(x)$ 是置换多项式. 设 $A_1, \cdots, A_r$ 是 $g(x)$ 所相应的映射 $g \in \mathbf{F}_{qq}$ 的伴随有向图 $D(g)$ 的全部有向圈, $a_i \in V(A_i)$, $l_g(a_i)$ 为 $D(g)$ 中含点 a_i 的圈之长 ($i = 1, \cdots, r$). 则满足条件 $f(g(x)) \equiv h(f(x))$ 且次数 $\deg f < q$ 的全体多项式 $f(x)$ 的通解可表示为

$$f(x) = \sum_{i=1}^{r} \sum_{j=0}^{l_g(a_i)-1} h^j(c_i) Q_0(x - g^j(a_i)), \tag{2.7}$$

其中 c_i 取遍 F_q 中落在有向图 $D(h)$ 的圈上且满足 $l_h(c_i) \mid l_g(a_i)$ 的全部点 ($i = 1, \cdots, r$) (换言之, 即 c_i 取遍圈 A_i 在 $D(h)$ 中的全部因子圈上的点).

证明 $h(x), g(x)$ 所相应的映射 $h, g \in \mathbf{F}_{qq}$, 此时有向图 $D(h), D(g)$ 的顶点集就是有限域 F_q. 而由 $g(x)$ 是置换多项式知

$$F_q = \bigcup_{i=1}^{r} V(A_i) = \bigcup_{i=1}^{r} \{a_i, g(a_i), \cdots, g^{l_g(a_i)-1}(a_i)\} = \bigcup_{i=1}^{r} \bigcup_{j=0}^{l_g(a_i)-1} \{g^j(a_i)\}. \tag{2.8}$$

因 $f(x)$ 满足 $f(g(x)) \equiv h(f(x))$ 的充要条件是它们所相应的映射满足 $fg = hf$. 而引理 2.3 又指出了满足 $fg = hf$ 的全部映射 f 可表为如下之形式(用 f 在 F_q 中由(2.8)式表示的全部元素的象来描述):

$$f(g^j(a_i)) = h^j(c_i) \quad (i = 1, \cdots, r;\ j = 0, 1, \cdots, l_g(a_i) - 1),$$

只要其中 c_i 落在 A_i 在 $D(h)$ 中的因子圈上. 然后再利用插值多项式公式(2.1)将这样得到的全部映射所对应的次数小于 q 的多项式写出, 即得满足 $f(g(x)) = h(f(x))$ 且次数 $\deg f < q$ 的 $f(x)$ 的通解公式(2.7). □

注 若将 $\deg f < q$ 的限制条件去掉, 则 $f(x)$ 的通解可表为

$$f(x) = \sum_{i=1}^{r} \sum_{j=0}^{l_g(a_i)-1} h^j(c_i) Q_0(x - g^j(a_i)) + b(x)(x^q - x), \tag{2.9}$$

其中 c_i 的意义同(2 7) 式, 而 $b(x)$ 则可取遍 F_q 上的任意多项式. 这一说明也同样适用于后面定理 2 2 及定理 2 4 中所得的各种通解公式.

与定理 2 1 类似地可以得到当 $h(x)$ 为置换多项式时, 满足条件 $f(g(x)) \equiv h(f(x))$ 的 F_q 上多项式 $f(x)$ 的通解表示式如下.

定理 2 2 设 $h(x), g(x) \in F_q[x]$, 其中 $h(x)$ 是置换多项式. 设 $D_1(g), \cdots, D_r(g)$ 为 $g(x)$ 所相应的映射 $g \in \mathbf{F}_{qq}$ 的伴随有向图 $D(g)$ 的全部无向连通分支, A_i 为 $D_i(g)$ 中的(唯一) 有向圈, $a_i \in V(A_i)$ $(i = 1, \cdots, r)$. 又对任一 $a \in D_i(g)$, 记 $d_g(a, a_i)$ 为 $D(g)$ 中从点 a 到 a_i 的距离. 则满足条件 $f(g(x)) \equiv h(f(x))$ 且次数 $\deg f < q$ 的 $f(x)$ 的通解可表为

$$f(x) = \sum_{i=1}^{r} \sum_{a \in D_i(g)} h^{-d_g(a, a_i)}(c_i) Q_0(x - a) \tag{2 10}$$

其中 c_i 取遍 F_q 中满足条件 $l_h(c_i) \mid l_g(a_i)$ 的全部点(即取遍圈 A_i 在 $D(h)$ 中的全部因子圈上的点 c_i), 而 $h^{-j}(x)$ 表示 j 个 $h^{-1}(x)$ 的复合.

定理 2 2 的证明与定理 2 1 类似, 从略.

利用上述结论可以进一步给出满足 $f(g(x)) \equiv h(f(x))$ 且 $\deg f < q$ 的多项式 $f(x)$ 的个数的如下计算公式.

定理 2 3 设 $h(x), g(x)$ 及其他记号的意义同定理 2 1 或定理 2 2. 对 $1 \leq j \leq q$, 设映射 g 和 h 的伴随有向图 $D(g)$ 和 $D(h)$ 中长为 j 的有向圈的个数分别为 $b_j(g)$ 和 $b_j(h)$. 又对 $1 \leq i \leq r$, 令 $N_i(h)$ 为 A_i 在 $D(h)$ 中全部因子圈的长度之和, 记 $N_{g,h}$ 为满足 $f(g(x)) \equiv h(f(x))$ 且 $\deg f < q$ 的 F_q 上多项式 $f(x)$ 的个数, 则有

(1) $$N_{g,h} = \prod_{i=1}^{r} N_i(h). \tag{2 11}$$

(2) $$N_{g,h} = \prod_{k=1}^{q} \Big(\sum_{j \mid k} j b_j(h) \Big)^{b_k(g)}. \tag{2 12}$$

证明 (1) 由公式(2 7) 或(2 10) 立得.

(2) 以 $N_i(h) = \sum_{j \mid l_g(a_i)} j b_j(h)$ 代入(2 11) 式并利用恒等式

$$\prod_{i=1}^{r} w(l_g(a_i)) = \prod_{k=1}^{q} w(k)^{b_k(g)}$$

对所有函数 $w(y)$ 均成立即可推得(2 12) 式. □

在 g 和 h 都是置换的特殊情形, (2 12) 的形式与 de-Bruijn 的公式一样[5]; 而在 $g = h$ 的特殊情形, 也与[3] 中用中心化环方法得到的公式一样. 但在具体计算时, 应用(2 11) 式比(2 12) 式更为简捷、方便.

参 考 文 献

[1] C. Wells, *Polynomials over finite fields which commute with translation*, Proc. Amer. Math. Soc., 46(1974), 347-350.

[2] G. L. Mullen, *Polynomials over finite fields which commute with linear permutations*, Proc. Amer. Math. Soc., 84(1982), 315-317.

[3] C. Y. Chao, *Polynomials over finite fields which commute with a permutation polynomial*, J. of Algebra, 163(1994), 295-311.

[4] J. A. Bondy and U. S. R. Murty, *Graph Theory with Applications*, The Macmillon Press, 1976.

[5] N. G. deBruijn, *Pólya's theory of counting*, in "*Applied Combinatorial Mathematics*"(*E. F. Beckenback, Ed.*), Wiley, New York, 1964, 148-184.

Polynomials over Finite Fields with the Commuting Diagram Properties

Shao Jiayu *Guo Jingming*

(Dept. of Appl. Math., Tongji University, 200092)

Abstract

We give explicit expressions for the general solutions of the polynomials $f(x)$ over finite field F_q satisfying the condition $f(g(x)) \equiv h(f(x))$ and give the counting formula for the number of such $f(x)$ with $\deg f < q$, where $g(x)$ and $h(x)$ are two given polynomials over F_q and one of them is a permutation polynomial. This generalizes the main results in [3] and also generalizes the main results in [1] and [2] in the special cases where $g(x)$ and $h(x)$ are both linear polynomials.

Keywords finite field, polynomial, digraph.