第 22 卷 第 1 期 电 子 科 学 学 刊 Vol.22 No.1
2000 年 1 月 JOURNAL OF ELECTRONICS Jan. 2000

有限域上的 n 元正交多项式组 [1]

亢保元 王育民

(西安电子科技大学 ISN 国家重点实验室 西安 710071)

摘 要 置换多项式在通信领域有重要的应用，作为置换多项式的推广，R.Lidl 等人 (1983) 引入了正交多项式组的概念，并给出它的一些基本性质．本文就这一问题做了进一步的研究，得到了有意义的结果．

关键词 有限域，置换多项式，正交多项式组

中图号 TN918.1

1 引 言

置换在通信领域有重要的应用，例如，没有信息扩张的密码体制实际上可以看作置换的结果，著名的 RSA[1] 公钥体制也只不过是一种多项式置换．所以，研究置换多项式是非常必要的．作为置换多项式的推广，文献 [2] 引入了正交多项式组的概念，这一概念也可看作是布尔置换 [3] 概念的推广，并且它还等价于文献 [4] 中的多输出函数的正交性．所以，正交多项式组有广阔的应用前景．本文在文献 [2] 的基础上进一步给出了这方面的一些结果．

2 有关的概念及基本性质

以 $F_q[x_1,\cdots,x_n]$ 表示有限域 F_q 上的 n 元多项式环，$n\geq 1$．

定义 1[2] 设 $f\in F_q[x_1,\cdots,x_n]$, 若对任意的 $a\in F_q$, $f(x_1,\cdots,x_n)=a$ 在 F_q^n 上有 q^{n-1} 个解，则称 f 为 F_q 上的 n 元置换多项式．

定义 2[2] 设 $f_1\cdots,f_m\in F_q[x_1,\cdots,x_n]$, $1\leq m\leq n$．如果对任意的 $(a_1,\cdots,a_m)\in F_q^m$, 方程组：

$$f_1(x_1,\cdots,x_n)=a_1,\quad\cdots,\quad f_m(x_1,\cdots,x_n)=a_m.$$

在 F_q^n 上有 q^{n-m} 个解，则称 $f_1,\cdots,f_m$ 在 F_q 上正交．或者说，$f_1,\cdots,f_m$ 为 F_q 上的 n 元正交多项式组．

性质 1[2] 当 $m=n$ 时，正交多项式组 $f_1,\cdots,f_m$ 导出 F_q^n 上的一个置换 $[f_1,\cdots,f_n]$．

性质 2 任一正交多项式组的非空子集仍成正交多项式组．

证明 设 $f_1\cdots,f_m\in F_q[x_1,\cdots,x_n]$ 为正交多项式组，$1\leq s<m$, 下证 $f_1\cdots,f_s$ 为正交多项式组．对任意的 $(a_1,\cdots,a_s)\in F_q^s$ 添加 $m-s$ 个分量 $a_{s+1},\cdots,a_m$, 可得到 q^{m-s} 个 F_q^m 中的向量，而每一方程组：

$$f_1(x_1,\cdots,x_n)=a_1,\quad\cdots,\quad f_s(x_1,\cdots,x_n)=a_s,$$
$$f_{s+1}(x_1,\cdots,x_n)=a_{s+1},\quad\cdots,\quad f_m(x_1,\cdots,x_n)=a_m.$$

有 q^{n-m} 个解，且这样的方程组的解集互不相交，故

$$f_1(x_1,\cdots,x_n)=a_1,\quad\cdots,\quad f_s(x_1,\cdots,x_n)=a_s.$$

有 $q^{m-s}q^{n-m}=q^{n-s}$ 个解，即 $f_1,\cdots,f_s$ 为正交多项式组．

[1] 1998-04-14 收到，1998-11-16 定稿

由性质 2, 若 $f_1,\cdots,f_m$ 为正交多项式组. 则 $f_1,\cdots,f_m$ 均为置换多项式.

性质 3[2,定理7.36]　设 $f_1,\cdots,f_m\in F_q[x_1,\cdots,x_n]$ 为正交多项式组, 则对任意的 r, $1\le r\le n-m$, 存在多项式 $f_{m+1},\cdots,f_{m+r}\in F_q[x_1,\cdots,x_n]$ 使 $f_1,\cdots f_m,f_{m+1},\cdots f_{m+r}$ 为正交多项式组.

3 主要结果

定理 1　$f_1\cdots,f_m\in F_q[x_1,\cdots,x_n]$ 为正交多项式组, 当且仅当存在 F_q^n 上的置换 $[f_1,\cdots,f_m,f_{m+1},\cdots,f_n]$, $f_{m+1},\cdots,f_n\in F_q[x_1,\cdots,x_n]$.

证明　由性质 1 和性质 3 可知必要性成立, 由性质 2 可知充分性成立.

定理 2　$f_1\cdots,f_m,g_1,\cdots,g_n\in F_q[x_1,\cdots,x_n]$, 若 $f_1\cdots,f_m$ 为正交多项式组, 而 $[g_1,\cdots,g_n]$ 为 F_q^n 上的置换, 则 $f_1(g_1,\cdots,g_n),\cdots,f_m(g_1,\cdots,g_m)$ 为 F_q 上正交多项式组.

证明　任意的 $(a_1,\cdots,a_m)\in F_q^m$, 因 $[g_1,\cdots,g_n]$ 为 F_q^n 上的置换, 所以方程组:

$$f_1(x_1,\cdots,x_n)=a_1,\quad\cdots,\quad f_m(x_1,\cdots,x_n)=a_m$$

与方程组:

$$f_1(g_1(x_1,\cdots,x_n),\cdots g_n(x_1,\cdots,x_n))=a_1,\quad\cdots,\quad f_m(g_1(x_1,\cdots,x_n),\cdots,g_n(x_1,\cdots,x_n))=a_m$$

的解有一一对应关系. 故当 $f_1\cdots,f_m$ 正交时, $f_1(g_1,\cdots,g_n),\cdots,f_m(g_1,\cdots,g_m)$ 亦正交.

推论　设 $f_1\cdots,f_m\in F_q[x_1,\cdots,x_n]$ 为正交多项式组, D 为 F_q 上的 n 阶非奇异方阵, 则

$$f_1(XD+C),\cdots,f_m(XD+C)$$

为正交多项式组, 其中 $X=(x_1,\cdots,x_n)$, $C=(c_1,\cdots,c_n)$ 为 F_q^n 中的任一向量.

证明　因 D 非奇异, 故

$$X\to XD+C$$

为 F_q^n 上的置换, 由定理 2 知结论成立.

定理 3　设 $f_1(x_1,\cdots,x_m),\cdots,f_s(x_1,\cdots,x_m)$ 为 m 元正交多项式组, 而 $g_1(x_{m+1},\cdots,x_n),\cdots,g_s(x_{m+1},\cdots x_n)$ 为任一组多项式, 则

$$f_1(x_1,\cdots,x_m)+g_1(x_{m+1},\cdots,x_n),\cdots,f_s(x_1,\cdots,x_m)+g_s(x_{m+1},\cdots,x_n)$$

为 n 元正交多项式组.

证明　设 $(t_1,\cdots,t_s)\in F_q^s$, 且 $(t_1,\cdots,t_s)\ne(0,\cdots,0)$, 这时

$$t_1(f_1+g_1)+\cdots+t_s(f_s+g_s)=(t_1f_1+\cdots+t_sf_s)+(t_1g_1+\cdots+t_sg_s)$$

因 $f_1,\cdots,f_s$ 为正交多项式组, 由文献 [2 , 定理 7.39] 知 $t_1f_1+\cdots+t_sf_s$ 为 m 元置换多项式. 再由文献 [2, 定理 7.42] 知 $(t_1f_1+\cdots+t_sf_s)+(t_1g_1+\cdots t_sg_s)=t_1(f_1+g_1)+\cdots+t_s(f_s+g_s)$ 为 n 元置换多项式, 于是据文献 [2, 定理 7.39] 得 $f_1(x_1,\cdots,x_m)+g_1(x_{m+1},\cdots,x_n),\cdots,f_s(x_1,\cdots,x_m)+g_s(x_{m+1},\cdots,x_n)$ 为 n 元正交多项式组.

定理 4　$f_1,\cdots,f_m\in F_q[x_1,\cdots,x_n]$ 为正交多项式组, 当且仅当对 F_q 上任一 m 元置换多项式 $g(y_1,\cdots,y_m)$, 即有 $g(f_1(x_1,\cdots,x_n),\cdots,f_m(x_1,\cdots,x_n))$ 为 F_q 上 n 元置换多项式.

证明 *充分性* 设 $(t_1,\cdots,t_m)\in F_q^m$, 且 $(t_1,\cdots,t_m)\neq(0,\cdots,0)$, 因 $t_1y_1+\cdots,+t_my_m$ 为 F_q 上 m 元置换多项式. 于是, 由条件知 $t_1f_1+\cdots+t_mf_m$ 为 F_q 上 n 元置换多项式. 从而据文献 [2, 定理 7.39] 知 $f_1,\cdots,f_m$ 为正交多项式组.

必要性 对任意的 $a\in F_q$, 因 $g(y_1,\cdots,y_m)$ 为 m 元置换多项式, 故 $g(y_1,\cdots,y_m)=a$ 有 q^{m-1} 个解. 设 $(a_1,\cdots,a_m)$ 为其中的任一个解, 而 $f_1,\cdots,f_m$ 正交, 所以

$$f_1(x_1,\cdots,x_n)=a_1,\quad\cdots,\quad f_m(x_1,\cdots,x_n)=a_m.$$

有 q^{n-m} 个解. 这时 $g(f_1(x_1,\cdots,x_n),\cdots,f_m(x_1,\cdots,x_n))=a$ 就有 $q^{m-1}q^{n-m}=q^{n-1}$ 个解, 即 $g(f_1(x_1,\cdots,x_n),\cdots,f_m(x_1,\cdots,x_n))$ 为 F_q 上 n 元置换多项式.

4 结束语

正交多项式组有广阔的应用前景, 本文虽然给出了一些结果, 但关于它的研究还有待进一步深入.

参 考 文 献

[1] 王育民, 何大可. 保密学基础—应用. 西安: 西安电子科技大学出版社, 1990, 208-213.

[2] Lidl R, Niederriter H. Finite Fields, Encyclopedia of Mathematics and its Applications, Vol.20, Addison-Wesley Publishing Company, 1983, Chapter 7.

[3] 武传坤. 密码学中的布尔函数: [博士论文]. 西安: 西安电子科技大学, 1993 年 1 月.

[4] 冯登国. 频谱理论及其在通信保密技术中的应用: [博士论文]. 西安: 西安电子科技大学, 1995 年 4 月.

ORTHOGONAL SYSTEM OF POLYNOMIALS IN n INDETERMINATES OVER FINITE FIELDS

Kang Baoyuan Wang Yumin

(*National Key Lab. on ISN, Xidian University, Xi'an* 710071)

Abstract Permutation polynomials play an important role in communication field. As a generalization, the concept of orthogonal system of polynomials in n indeterminates over finite field was introduced by R.Lidl and H.Niederriter(1983). In this paper, this problem is discussed and several results are obtained.

Key words Finite fields, Permutation polynomials, Orthogonal system of polynomials

亢保元: 男, 1965 年生, 博士生, 讲师, 主要研究方向为保密学基础数学理论.
王育民: 男, 1936 年生, 教授, 博士生导师, 主要从事通信保密的教学与研究.