$(q, 3\ \ 2, 1)$-外差族的存在性

王金华, 王 新, 高 华

(南通大学理学院, 江苏 南通 226007)

[摘要] 应用有限域和差矩阵给出了外差族的两个递推构作, 并且证明了当 $q \equiv 1 \pmod{24}$是质数幂时存在 $(q, 3\ \ 2, 1)$-外差族.

[关键词] 外差族, 差矩阵, 有限域

[中图分类号] O157.2 [文献标识码] A [文章编号] 1001-4616(2009)01-0012-04

Existence of $(q, 3\ \ 2, 1)$-External Difference Families

Wang Jinhua, Wang Xin, Gao Hua

(School of Sciences, Nantong University, Nantong 226007, China)

Abstract From finite field and difference matrix, two recursive constructions for external difference families are given and it is proved that there exists a $(q, 3\ \ 2, 1)$-external difference family for any prime power $q \equiv 1 \pmod{24}$.

Key words external difference family, difference matrix, finite field

设$(G, +)$为一个 v阶 Abel群, t, u, c为正整数, D为 G上的 t个 $u \times c$阶矩阵 $\boldsymbol{B}_r$(称为基区组)所组成的族, 其中 $\boldsymbol{B}_r = (b_{ij}^r)_{u \times c}$, $1 \leqslant r \leqslant t$定义重集 $B_r = \{(b_{i_1 j_1}^r - b_{i_2 j_2}^r) \mid 1 \leqslant i_1 < i_2 \leqslant u, 1 \leqslant j_1, j_2 \leqslant c\}$, $D = \sum_{r=1}^{t} B_r$. 如果 $D = \lambda(G \setminus \{0\})$, 则称 D为 G上一个 $(v, u \times c, \lambda)$-外差族, 简记为 $(v, u \times c, \lambda)$-EDF, 其中 $\lambda(G \setminus \{0\})$表示 G中每个非零元恰出现 λ次的重集.

由外差族的定义有下面引理.

引理 **1** $(v, u \times c, \lambda)$-EDF存在的必要条件是 $\lambda(v-1) \equiv 0 \pmod{c^2 u(u-1)}$.

外差族的概念是 Ogata, Kurosawa, Stinson和 Saido[1] 于 2004年在研究认证码时首次介绍的一类新的组合设计, 它是差族概念的推广, 在编码密码学中有很好的应用. 文献[1]已经详细阐述了它与分裂平衡区组设计、c-分裂认证码、密码共享方案之间的关系, 这些事实说明外差族(EDF)存在性问题值得深入研究. 最近 Chang和 Ding[2] 给出了一些外差族的构造方法, 得到了一些指数 $\lambda > 1$的外差族类, 详细结果见文献[2]. 对指数 $\lambda = 1$时的外差族仅有下面一个无穷类.

定理 **1**[3] 对任意正整数 t, c存在 $(2c^2 t + 1, 2\ \ c, 1)$-EDF.

本文将进一步研究外差族的存在性.

1 外差族的构作

在本节中, 我们利用有限域和差矩阵给出外差族的两个递推构作.

定理 **2** 设 n是任意正整数. 如果在 $GF(q)$上存在 $(q, u \times c, \lambda)$-EDF, 则在 $GF(q^n)$上存在 $(q^n, u \times c, \lambda)$-EDF.

证明 设 D是 $GF(q)$上的 $(q, u \times c, \lambda)$-EDF. 由有限域知 $GF(q)^* = GF(q) \setminus \{0\}$是 $GF(q^n)^* =$

收稿日期: 2008-06-12

基金项目: 国家自然科学基金(10771193)、江苏省高校自然科学基金(07KJB110090)、南通大学博士启动基金(07B12)、南通大学创新人才基金资助项目.

通讯联系人: 王金华, 博士, 副教授, 研究方向: 组合设计及其应用. E-mail: jhwang@ntu.edu.cn

$GF(q^n)\setminus\{0\}$的指数 $e=(q^n-1)/(q-1)$的惟一乘法子群. 令 $H_j^e(0\le j\le e-1)$为群 $GF(q^n)^*$ 关于子群 $GF(q)^*$ 的 e个陪集, 其中$H_0^e=GF(q)^*$. 任取 e个陪集的一个代表系 R, 令 $F=\{r+\boldsymbol{B}: \boldsymbol{B}\in D, r\in R\}$, 则 F 为 $GF(q^n)$ 上的 $(q^n, u, c,)$-EDF. 事实上,

$$F=\bigcup_{r\in R,\boldsymbol{B}\in D}(r+\boldsymbol{B})=\bigcup_{r\in R,\boldsymbol{B}\in D}r+B=\bigcup_{r\in R}r+GF(q)^*=\left(\bigcup_{0\le j\le e-1}H_j^e\right)^*=(GF(q^n)^*).$$

证毕.

设 $(G, +)$是 m 阶 Abel群, $\boldsymbol{M}=(d_{ij})(0\le i\le k-1, 0\le j\le m-1)$为 G上 $k\times m$ 阶矩阵. 如果$\boldsymbol{M}$中任意两行 i_1、$i_2(0\le i_1<i_2\le k-1)$的差 $_{i_1i_2}=\{d_{i_2j}-d_{i_1j}: j=0, 1, \cdots, m-1\}$满足 $_{i_1i_2}=G$, 则称$\boldsymbol{M}$为 G 上的一个 $(m, k, 1)$-差矩阵, 记为 $(m, k, 1)$-DM. 关于差矩阵存在性结果及相关信息可参考文献 [4]. 由差矩阵的定义知, 对任意质数幂 q, 有限域 $GF(q)$ 的乘法表构成一个 $(q, q, 1)$-DM. 在一个 $(q, q, 1)$-DM 中删去任意 $q-k$行得到一个 $(q, k, 1)$-DM. 一般地, 我们有下面的结论.

定理 **3**[4] 设 $q=q_1q_2\cdots q_r$, 其中 q_j是不小于 k的质数幂, 则在 $(\bigcup_{j}^{r}GF(q_j), +)$ 上存在 $(q, k, 1)$-DM.

定理 **4** 设 $(G_1, +)$和 $(G_2, +)$分别为 v和 m 阶 Abel群. 如果 G_1上存在 $(v, u, c,)$-EDF, G_2上存在 $(m, u, c,)$-EDF和 $(m, u, 1)$-DM, 则群 $(G_1\times G_2, +)$ 上存在 $(mv, u, c,)$-EDF.

证明 设 D 为 G_1上的 $(v, u, c,)$-EDF, 设 E和$\boldsymbol{M}=(d_{ij})(1\le i\le u, 0\le j\le m-1)$分别为 G_2上的 $(m, u, c,)$-EDF和 $(m, u, 1)$-DM. 对每个基区组 $\boldsymbol{B}=(b_{ij})_{u\times c}\in D$, 构作 $G_1\times G_2$上的m 个 $u\times c$ 阶矩阵 $\boldsymbol{B}_j(0\le j\le m-1)$:

$$\boldsymbol{B}_j=\begin{pmatrix}(b_{11}, d_{1j}) & (b_{12}, d_{1j}) & \cdots & (b_{1c}, d_{1j})\\ (b_{21}, d_{2j}) & (b_{22}, d_{2j}) & \cdots & (b_{2c}, d_{2j})\\ \vdots & \vdots & & \vdots\\ (b_{u1}, d_{uj}) & (b_{u2}, d_{uj}) & \cdots & (b_{uc}, d_{uj})\end{pmatrix}.$$

而每个基区组$\boldsymbol{A}=(a_{ij})_{u\times c}\in E$, 构作 $G_1\times G_2$上的 1个 $u\times c$阶矩阵 $\boldsymbol{A}_0=((0, a_{ij}))$. 令 $A(\boldsymbol{B})=\bigcup_{j=0}^{m-1}\{\boldsymbol{B}_j\}$, $F=\left(\bigcup_{\boldsymbol{A}\in E}\{\boldsymbol{A}_0\}\right)\cup\left(\bigcup_{\boldsymbol{B}\in D}A(\boldsymbol{B})\right)$, 由外差族和差矩阵的定义直接验证知 F 为 $G_1\times G_2$上的 $(mv, u, c,)$-EDF. 证毕.

2 $(q, 3, 2, 1)$-*EDF* 的存在性

由引理 1知 $(q, 3, 2, 1)$-EDF存在的必要条件就是 $q\equiv 1(\mathrm{mod}\ 24)$. 在本节中, 我们将证明当 $q\equiv 1(\mathrm{mod}\ 24)$ 是质数幂时 $(q, 3, 2, 1)$-EDF是存在的. 为此需要一些关于有限域的概念.

设质数幂 $q\equiv 1(\mathrm{mod}\ n)$, $\in GF(q)^*$ 的生成元. 令 $C_0^n=\{^{in}: 1\le i\le (q-1)/n\}$为乘法群 $GF(q)^*$ 的 $(q-1)/n$阶子群, $C_j^n=^{j}C_0^n, 0\le j\le n-1$, 则称 $C^n=\{C_0^n, C_1^n, \cdots, C_{n-1}^n\}$为 $GF(q)^*$ 的指数为 n的分圆类. 从 $C_j^n, 0\le j\le n-1$中各取一个代表组成的集合称为分圆类 C^n的相异代表系, 记为 SDRC(C^n).

引理 **2** 设 $q=24t+1$是一个质数幂, 是 $GF(q)$的一个本原根, x是 $GF(q)$中的某个元素. 如果$\{1-^{8t}, x-^{8t}, 1-x^{8t}, x-x^{8t}\}$是一个 SDRC$(C^4)$, 则 $GF(q)$ 上存在 $(q, 3, 2, 1)$-EDF.

证明 设

$$\boldsymbol{B}=\begin{pmatrix}1 & & x & \\ & ^{8t} & & x^{8t}\\ & ^{16t} & & x^{16t}\end{pmatrix},$$

则

$$B=\{1, ^{4t}, ^{8t}, ^{12t}, ^{16t}, ^{20t}\}\cup\{1-^{8t}, x-^{8t}, 1-x^{8t}, x-x^{8t}\}.$$

令 $D=\{\boldsymbol{B}_i: 0\le i\le t-1\}$, 其中

$$\boldsymbol{B}_i=^{4i}\boldsymbol{B}=\begin{pmatrix}^{4i} & & x & ^{4i}\\ & ^{8t+4i} & & x^{8t+4i}\\ & ^{16t+4i} & & x^{16t+4i}\end{pmatrix},$$

则

$$D = \bigcup_{0 \le i \le t-1} B_i = \{1, \alpha^4, \cdots, \alpha^{4(t-1)}\} \cup \{1, \alpha^{4t}, \cdots, \alpha^{20t}\} \cup \{1-\alpha^{8t}, x-\alpha^{8t}, 1-x\alpha^{8t}, x-x\alpha^{8t}\}.$$

显然,

$$C_0^4 = \{1, \alpha^4, \cdots, \alpha^{4(t-1)}\} \cup \{1, \alpha^{4t}, \cdots, \alpha^{20t}\}.$$

因为 $\{1-\alpha^{8t}, x-\alpha^{8t}, x-\alpha^{16t}, x(1-\alpha^{8t})\}$ 是一个 SDRC(C^4), 所以

$$D = C_0^4 \cup \{1-\alpha^{8t}, x-\alpha^{8t}, 1-x\alpha^{8t}, x-x\alpha^{8t}\} = GF(q)^*,$$

即 D 是 $GF(q)$ 上的 $(q, 3, 2, 1)$-EDF. 证毕.

为了应用引理 2去构作 $(q, 3, 2, 1)$-EDF, 我们需要下面的定理和推论.

定理 **5**[5]　设 $q \equiv 1 \pmod n$ 是一个质数幂且满足不等式

$$q - \left[\sum_{i=0}^{s-2} \binom{s}{i} (s-i-1)(n-1)^{s-i}\right]\sqrt{q} - sn^{s-1} > 0,$$

那么对于任意给定的 s-元数组 $(j_1, j_2, \cdots, j_s) \in \{0, 1, \cdots, n-1\}^s$ 和任意给定的 $GF(q)$ 中两两不同的元素组成的 s-元数组 $(c_1, c_2, \cdots, c_s)$, 存在一个元素 $x \in GF(q)$, 使得 $x + c_i \in C_{j_i}^n$, $i = 1, 2, \cdots, s$.

由定理 5有下面的推论.

推论 **1**　设 $q \equiv 1 \pmod n$ 是一个质数幂且 $q \ge A(n, s)^2$, 其中

$$A(n, s) = [B(n, s) + \sqrt{B(n, s)^2 + 4sn^{s-1}}]/2,$$

$$B(n, s) = \sum_{i=0}^{s-2} \binom{s}{i} (s-i-1)(n-1)^{s-i},$$

那么对于任意给定的 s-元数组 $(j_1, j_2, \cdots, j_s) \in \{0, 1, \cdots, n-1\}^s$ 和任意给定的 $GF(q)$ 中两两不同的元素组成的 s-元数组 $(c_1, c_2, \cdots, c_s)$, 存在一个元素 $x \in GF(q)$, 使得 $x + c_i \in C_{j_i}^n$, $i = 1, 2, \cdots, s$.

引理 **3**　设 $q \equiv 1 \pmod{24}$ 是一个质数幂且 $q \ge 6\,657$, 则存在 $(q, 3, 2, 1)$-EDF.

证明　设 α 是 $GF(q)^*$ 的一个生成元, 不妨设 $1-\alpha^{8t} \in C_a^4$, 取 $b, c, d \in \{0, 1, 2, 3\} \setminus \{a\}$, 且 $d \ne 0$ 使得 $\{a, b, c, a+d\}$ 是模 4的完全剩余系. 应用推论 1, 其中 $n = 4$, $s = 3$知, 当 $q \ge 6\,657$存在 $x \in GF(q)$ 使得 $x - \alpha^{8t} \in C_b^4$, $1 - x\alpha^{8t} \in C_c^4$, $x \in C_d^4$. 由 $\{a, b, c, a+d\}$ 是模 4的完全剩余系知 $\{1-\alpha^{8t}, x-\alpha^{8t}, 1-x\alpha^{8t}, x-x\alpha^{8t}\}$ 是一个 SDRC(C^4), 再由引理 2知 $GF(q)$ 上存在 $(q, 3, 2, 1)$-EDF.

当 $q < 6\,657$时, 我们将通过计算机搜索寻找 $GF(q)$ 中满足引理 2条件的元 α 和 x, 从而证明 $(q, 3, 2, 1)$-EDF的存在性.

引理 **4**　设 $p \equiv 1 \pmod{24}$ 是一个质数且 $p < 6\,657$, 则存在 $(p, 3, 2, 1)$-EDF.

证明　应用引理 2, 相应的质数 p、α 和 x 见表 1.

引理 **5**　设 $q = p^2 \equiv 1 \pmod{24}$, 其中 p 是一个质数且 $q < 6\,657$, 则存在 $(q, 3, 2, 1)$-EDF.

证明　由 $q < 6\,657$知, $5 \le p \le 79$. 设 $f(x)$ 为 $Z_p[x]$ 上的二次本原多项式, α 满足 $f(\alpha) = 0$, 则 $GF(q) = Z_p[x]/(f(x)) = Z_p[\alpha]$. 应用引理 2, 相应的质数 p、$f(x)$ 和 x 见表 2.

引理 **6**　设 $q \equiv 1 \pmod{24}$ 是一个质数幂且 $q < 6\,657$, 则存在 $(q, 3, 2, 1)$-EDF.

证明　设 $q = p^n$, 其中 p 是质数. 当 $n = 1$, 2时结论由引理 4和引理 5得到; 当 $n \ge 3$时结论由引理 4, 引理 5和定理 2得到.

现在给出本文的主要结果.

定理 **6**　设 $q \equiv 1 \pmod{24}$ 是一个质数幂, 则存在 $(q, 3, 2, 1)$-EDF.

证明　结论由引理 3和引理 6得到.

定理 **7**　设 $v = q_1 q_2 \cdots q_t$, 其中 $q_i \equiv 1 \pmod{24}$ 是一个质数幂, 则存在 $(v, 3, 2, 1)$-EDF.

证明　对 t 归纳证明.

当 $t = 1$时, 由定理 6结论成立.

假设 $t-1$时结论成立, 即存在 $(q_1 q_2 \cdots q_{t-1}, 3, 2, 1)$-EDF. 由定理 3知存在 $(q_t, 3, 1)$-DM, 应用定理 4得到 $(q_1 q_2 \cdots q_t, 3, 2, 1)$-EDF. 定理得证.

表 1 引理 4中质数 p 及相应的 和 x

Table 1 Elements and x corresponding to prime p in Lemma 4

p		x	p		x	p		x	p		x
73	5	17	3 169	7	11	1 753	7	5	4 969	11	14
97	5	30	3 217	5	21	1 777	5	6	4 993	5	10
193	5	2	3 313	10	10	1 801	11	29	5 113	19	7
241	7	7	3 361	22	13	1 873	10	10	5 209	17	37
313	10	5	3 433	5	20	1 993	5	13	5 233	10	11
337	10	19	3 457	7	3	2 017	5	2	5 281	7	7
409	21	14	3 529	17	39	2 089	7	6	5 449	7	14
433	5	7	3 673	5	11	2 113	5	20	5 521	11	6
457	13	5	3 697	5	2	2 137	10	11	5 569	13	27
577	5	10	3 769	7	17	2 161	23	50	5 641	14	3
601	7	7	3 793	5	8	2 281	7	20	5 689	11	44
673	5	8	3 889	11	21	2 377	5	14	5 737	5	21
769	11	6	4 057	5	40	2 473	5	15	5 857	7	14
937	5	17	4 129	13	30	2 521	17	2	5 881	31	11
1 009	11	33	4 153	5	7	2 593	7	11	5 953	7	33
1 033	5	6	4 177	5	3	2 617	5	7	6 073	10	2
1 129	11	12	4 201	11	35	2 689	19	6	6 121	7	13
1 153	5	3	4 273	5	15	2 713	5	2	6 217	5	3
1 201	11	29	4 297	5	19	2 833	5	13	6 337	10	6
1 249	7	3	4 441	21	24	2 857	11	3	6 361	19	7
1 297	10	5	4 513	7	7	2 953	13	21	6 481	7	7
1 321	13	5	4 561	11	7	3 001	14	21	6 529	7	7
1 489	14	12	4 657	15	10	3 049	11	26	6 553	10	5
1 609	7	12	4 729	17	7	3 121	7	3	6 577	5	2
1 657	11	37	4 801	7	33						

表 2 引理 5中质数 p 及相应的 $f(x)$ 和 x

Table 2 $f(x)$ and x corresponding to prime p in Lemma 5

p	$f(x)$	x	p	$f(x)$	x	p	$f(x)$	x	p	$f(x)$	x
5	x^2+x+2	3	7	x^2+x+3	10	11	x^2+x+7	5	13	x^2+x+2	7
17	x^2+x+3	3	19	x^2+x+2	3	23	x^2+x+7	3	29	x^2+x+3	10
31	x^2+x+12	3	37	x^2+x+5	7	41	x^2+x+12	10	43	x^2+x+3	18
47	x^2+x+13	5	53	x^2+x+5	13	59	x^2+x+2	5	61	x^2+x+2	9
67	x^2+x+12	3	71	x^2+x+11	6	73	x^2+x+3	5	79	x^2+x+3	3

[参考文献]

[1] Ogata W, Kurosawa K, Stinson D R, et al. New combinatorial designs and their applications to authentication codes and secret sharing schemes[J]. Discrte Math, 2004, 279(1/3): 383-405.

[2] Chang Y, Ding C. Constructions of external difference families and disjoint difference families[J]. Des Codes Crypt, 2006, 40(2): 167-185.

[3] Ge G, Miao Y, Wang L. Combinatorial constructions for optimal splitting authentication codes[J]. SIAM J Discrete Math, 2005, 18(4): 663-678.

[4] Colbourn C J, Dinitz J H. Handbook of Combinatorial Designs[M]. 2nd ed. Boca Raton: Chapman & Hall/CRC, 2007.

[5] Chang Y, Ji L. Optimal $(4up, 5, 1)$ optical orthogonal codes[J]. J Combin Des, 2004, 12(5): 346-361.

[责任编辑: 丁 蓉]