DOI: 10.13656/j.cnki.gxkx.2008.03.001
广西科学 Guangxi Sciences 2008, 15(3): 218~220

不相交差族 $(p^n, 4, 1)$-DDF的存在性*

The Existence of $(p^n, 4, 1)$ Disjoint Difference Families

杨建效
YANG Jian-xiao

(陕西铁路工程职业技术学院,陕西渭南 714000)
(Shaanxi Railway Engineering Professional Technology Institute, Weinan, Shaanxi, 714000, China)

摘要:利用乘法特征和的 Weil定理,结合计算机搜索来构造不相交差族,证明不相交差族 $(p^n, 4, 1)$-DDF的存在性,其中 $p \equiv 1 \pmod{12}$ 为质数且 $n \geq 1$.

关键词:差族 不相交差族 特征和
中图法分类号: O157.2 文献标识码: A 文章编号: 1005-9164(2008)03-0218-03

Abstract By using Weil's theorem on character sum estimates and constructing disjoint difference families with computer, it is proved that there exists a $(p^n, 4, 1)$-DDF, where $p \equiv 1 \pmod{12}$ is a prime number and $n \geq 1$.

Key words difference family, disjoint difference family, character sum

区组设计的研究是组合设计理论的核心内容.差族是区组设计的主要研究对象之一,它可以用来构造多种区组设计.很多学者对差族的存在性进行研究[1-4].本文利用乘法特征和的 Weil定理,结合计算机搜索来构造不相交差族,证明 $(p^n, 4, 1)$-DDF的存在性,其中 $p \equiv 1 \pmod{12}$ 为质数且 $n \geq 1$.

1 预备知识

设 G是一个 v阶的 Abel群, $B = \{B_i \mid i \in I\}$,其中 B_i 是 G的某些 k元集合, $\Delta B_i = \{a - b \mid a, b \in B_i, a \neq b\}$, $\Delta B = \bigcup \Delta B_i$.如果 ΔB 使得 G的每一个非零元恰好在其出现 λ次,则称 B是一个 (v, k, λ)差族,记为 (v, k, λ)-DF,其中 B_i 称为基区组.如果一个 (v, k, λ)-DF的基区组是不相交的,则称 (v, k, λ)-DF是一个不相交差族,记为 (v, k, λ)-DDF.显然, (v, k, λ)-DDF存在的必要条件为 $\lambda(v-1) \equiv 0 \pmod{k(k-1)}$且 $\lambda \leq k - 1$.设 $\mathscr{F} = \{F_0, F_2, \cdots, F_{s-1}\}$,其中每一个 F_i 是一个 (v, k, λ)-DDF,如果 $\bigcup_{i=0}^{s-1} \bigcup_{B \in F_i} B$ 恰好是 $G \setminus \{0\}$的一个划分,则称 $\mathscr{F}$ 是一个 (v, k, λ)-CDDF.从而,由 (v, k, λ)-CDDF的存在性可知 (v, k, λ)-DDF的存在性.

引理 **1.1**[2] 如果 $v \equiv 1 \pmod 6$,则存在 $(v, 3, 1)$-DDF.

引理 **1.2**[3] 设 $q - 1 = el$是一个奇质数幂,则存在 $(v, (q-1)/e, (q-1-e)/e)$-DDF.

当 $l = 3, 4$时,有

引理 **1.3** 设 $q - 1 = 3e$是一个奇质数幂,则存在 $(v, 3, 2)$-DDF.

引理 **1.4** 设 $q - 1 = 4e$是一个奇质数幂,则存在 $(v, 4, 3)$-DDF.

引理 **1.5**[4] 设 $v = 12t + 1$是一个质数, t为奇数且 $v \neq 13$,则存在 $(v, 4, 1)$-CDDF.

令 $G = Z_{13}$, $F = \{0, 1, 3, 9\}$.显然 F是一个 $(13, 4, 1)$-DDF,从而有

引理 **1.6** 设 $v = 12t + 1$是一个质数, t为奇数,则存在 $(v, 4, 1)$-DDF.

设 $T_1 = \{a_i \mid i \in I\}$, $T_2 = \{b_j \mid j \in J\}$,记 $T_1 \cdot T_2 = \{a_i b_j \mid i \in I, j \in J\}$.如果 $T_1 = \{a\}$,则 $T_1 \cdot T_2 = aT_2 = \{ab_j \mid j \in J\}$.

由文献[3]中的定理 1,可得

引理 **1.7** 如果在 $GF(q)$中存在 (q, k, λ)-DDF,则在 $GF(q^n)$中存在 (q^n, k, λ)-DDF.

证明 设 $B = \{B_i \mid i \in I\}$是在 $GF(q)$上的一个 (q, k, λ)-DDF,则 $\Delta B = \lambda(GF(q) \setminus \{0\})$.如果将 $GF(q)$看作是 $GF(q^n)$的一个子域,则 $GF(q) \setminus \{0\}$就是 $GF(q^n) \setminus \{0\}$的一个子群,记为 H^e,其中 $e = (q^n - 1)/(q - 1)$.

设 S是 H^e在 $GF(q^n) \setminus \{0\}$中的一个陪集代表系,

收稿日期: 2007-03-14

作者简介:杨建效(1977-),男,助教,硕士,主要从事组合数学的研究工作。

* 国家自然科学基金项目(10561002)资助。

$B^* = \{sB_i \mid s \in I, s \in S\}$,则 $\Delta B^* = \sum_{s\in S}\sum_{s\in I}\{s\}\circ B_i = S\circ \Delta B = \{s\}\circ \lambda(H^e) = \lambda(G(q^n)\setminus\{0\})$. 从而,$B^*$ 是一个 (q^n, k, λ)-DF.

设 s_iB_k, s_jB_h 是 B^* 中的两个不同的区组,若 $i = j$,则有 $k \neq h$. 由于 B_k, B_h 不相交,从而 s_iB_k, s_jB_h 不相交;若 $i \neq j$,则 s_i 和 s_j 位于 H^e 的不同陪集中. 由于 $B_k, B_h \subseteq H^e$,从而 s_iB_k, s_jB_h 不相交. 综上所述证明完毕.

2 主要结果

设 v 是一个质数幂,$F_v = GF(v)$,a 是 F_v 的本原元,$e \mid v-1$. H 是 $F_v^* = F_v\setminus\{0\}$ 的 $(v-1)/e$ 阶乘法子群,$H^i = a^iH, 0 \leqslant i \leqslant e-1$.

引理 **2.1**[3] 设 $e \mid v-1$,B 是 F_v 的一个 k 元子集. 如果 $\Delta B = \{a-b \mid a, b \in B, a \neq b\}$ 中的元素恰好在 H^0 的每一个陪集中分配 λ 个,则存在 (v, k, w)-DF;若 $2e \mid (v-1)$,则存在 $(v, k, w/2)$-DF.

引理 **2.2** 设 $v = 12t+1$ 是一个质数幂,$B = \{1, x, x^2, x^3\}$. 若 $x \in H^1$,$x+1 \in H^3$,$x^2+x+1 \in H^5$,则存在 $(v, 4, 1)$-DDF.

证明 $\Delta B = \pm(x-1)\{1, x, x^2, x+1, x(x+1), x^2+x+1\}$. 在引理 2.1 中取 $e = 6$,设 H^0 是 F_v^* 的 $(v-1)/6 = 2t$ 阶乘法子群. 显然,ΔB 中的元素恰好在 H^0 的每个陪集中出现 2 个. 令 $B = \{B, a^6B, \cdots, a^{6(t-1)}B\}$,不难验证 B 是一个 $(v, 4, 1)$-DDF,证毕.

引理 **2.3**[5] 令 χ 为 $GF(q)$ 的 m 阶乘法特征,$m > 1$,$f(x) \in GF(q)[x]$ 为首 1 正次数多项式,且不是某多项式的 m 次幂,d 为 $f(x)$ 在扩域中相异根的个数,则对任意的 $T \in GF(q)$,有

$$\left|\sum_{c\in GF(q)}\chi(Tf(c))\right| \leqslant (d-1)\sqrt{q}.$$

引理 **2.4** 若 $v \equiv 1 \pmod{12}$ 为质数幂,且 $v \geqslant 256036$,则存在 $(v, 4, 1)$-DDF.

证明 利用引理 2.2 和 Weil 定理来构造 $(v, 4, 1)$-DDF.

令 $f_1(x) = a^{-1}x$,$f_2(x) = a^{-3}(x+1)$,$f_3(x) = a^{-5}(x^2+x+1)$,则引理 2.2 中的条件可以转化为是否存在元素 $x \in F_v^*$ 满足:

$$f_i(x) \in H^0, 1 \leqslant i \leqslant 3. \quad (1)$$

在 $GF(v)$ 中,令 χ 为 6 阶的非平凡乘法特征,也就是说,当 $x \in H^j$ 时 $\chi(x) = \theta^j$,$0 \leqslant j \leqslant 5$,其中 $\theta = \exp(\frac{\pi i}{3})$ 为 6 次单位根. 令 $B_i = \chi(f_i(x))$ 且 $D_i = 1 + B_i + \cdots + B_i^5$,$1 \leqslant i \leqslant 3$. 则

$$D_i = \begin{cases} 6, \text{if } f_i(x) \in H^0, \\ 1, \text{if } f_i(x) = 0, \\ 0, \text{if } f_i(x) \notin H^0 \cup \{0\}. \end{cases}$$

令

$$S = \sum_{x\in GF(v)}\prod_{i=1}^{3}(1 + B_i + \cdots + B_i^5). \quad (2)$$

则 S 等于 $6^3n + d$,其中 n 为 $GF(v)$ 中满足条件 (1) 的元素 x 的个数,d 为 $f_i(x)$,$1 \leqslant i \leqslant 3$ 为 0 时对和 S 的贡献. 对任意的 $1 \leqslant i \leqslant 3$,如果 $f_i(x) = 0$,则对 S 的贡献最多为 6^2. 因此,如果 $|S| > 6^3 + 3\times 6^2 = 324$,则在 F_v^* 中至少有一个元素 x 满足条件 (1).

将 S 展开有:

$$S = \sum_{x\in GF(v)}1 + \sum_{i=1}^{3}\sum_{k=1}^{5}\sum_{x\in GF(v)}B_i^k + \sum_{1\leqslant i_1\leqslant i_2\leqslant 3}\sum_{1\leqslant k_1,k_2\leqslant 5}\sum_{x\in GF(v)}B_{i_1}^{k_1}B_{i_2}^{k_2} + \sum_{1\leqslant k_1,k_2,k_3\leqslant 5}\sum_{x\in GF(v)}B_1^{k_1}B_2^{k_2}B_3^{k_3}. \quad (3)$$

由引理 2.3,显然有 $f_1(x), f_2(x), f_3(x)$ 两两互素. 设 $G(x) = f_1(x)^{T_1}f_2(x)^{T_2}f_3(x)^{T_3}$ 为正次数多项式,可以证明当 $T_i \leqslant 5$,$1 \leqslant i \leqslant 3$ 时,$G(x)$ 不可能为 $GF(v)[x]$ 中的一个多项式的 6 次幂. 事实上,如果 $G(x) = p(x)^6$,由于 $f_1(x), f_2(x), f_3(x)$ 是两两互素的,所以 $T_1 \equiv T_2 \equiv T_3 \equiv 0 \pmod 6$,又因为 $T_i \leqslant 5$,$1 \leqslant j \leqslant 3$,所以有 $T_1 = T_2 = T_3 = 0$,与假设矛盾. 注意到可以找到相应的 c 使得 (3) 式中的每 1 项乘积都表示成 $\chi(cf(x))$ 的形式,其中 $f(x)$ 是首一多项式. 易见,$\deg(f_1(x)) = 1$,$\deg(f_2(x)) = 1$,$\deg(f_3(x)) = 2$. 所以,由引理 2.3,有

$$\left|\sum_{i=1}^{3}\sum_{k=1}^{5}\sum_{x\in G(F)(v)}B_i^k\right| \leqslant 5(2-1)\sqrt{v} = 5\sqrt{v},$$

$$\left|\sum_{1\leqslant i_1<i_2\leqslant 3}\sum_{1\leqslant k_1,k_2\leqslant 5}\sum_{x\in GF(v)}B_{i_1}^{k_1}B_{i_2}^{k_2}\right| \leqslant 5^2(1+1-1+2+1-1+2+1-1)\sqrt{v} = 125\sqrt{v},$$

$$\left|\sum_{1\leqslant k_1,k_2,k_3\leqslant 5}\sum_{x\in GF(v)}B_1^{k_1}B_2^{k_2}B_3^{k_3}\right| \leqslant 5^3(2+1+1-1)\sqrt{v} = 375\sqrt{v}.$$

从而有 $|S| \geqslant v - (5+125+375)\sqrt{v} = v - 505\sqrt{v}$.

如果 $v - 505\sqrt{v} > 324$,即 $v \geqslant 256036$,则 $n \geqslant 1$. 从而引理得证.

引理 **2.5** 设 $v \equiv 1 \pmod{12}$ 为质数,$v \in [13, 256036)$. 如果 $v \notin E = \{73, 241, 313\}$,则存在 $(v, 4, 1)$-DDF.

证明 通过计算机搜索,对于 $v \equiv 1 \pmod{12}$ 为质数,$v \in [13, 256036)$ 且 $v \notin E$,满足引理 2.2 条件的元素 $x \in F_v^*$ 全部找到. 在表 1 中列出了 $v \leqslant 1801$ 的数组 (v, a, x),其中 a 为 F_v 的本原元,x 为满足条件的元素. 而对其它的质数,由于篇幅关系在这里不一一列出.

表 1 数组 (v,ξ,x) $(x\leqslant 1801)$

Table 1 Array (v,ξ,x) $(x\leqslant 1801)$

v	a	x	v	a	x	v	a	x
97	5	41	193	5	70	337	10	65
409	21	62	433	5	267	457	13	339
577	5	562	601	7	498	673	5	596
769	11	629	937	5	166	1009	11	38
1033	5	945	1129	11	20	1153	5	186
1201	11	659	1249	7	1143	1297	10	393
1321	13	832	1489	14	1229	1609	7	1551
1657	11	159	1753	7	452	1777	5	1513
1801	11	782						

引理 **2.6** 设 $v=12t+1$是一个质数幂,$B=\{1, x, x^2, x^3\}$.若 $x\in H^5$, $x+1\in H^3$, $x^2+x+1\in H^1$,则存在 $(v,4,1)$-DDF.

证明 证明同理引理 2.2.

引理 **2.7** 设 $v\in E=\{73, 241, 313\}$,则存在 $(v,4,1)$-DDF.

证明 通过计算机搜索,找到满足引理 2.6条件的元素 $x\in F_v^*$,其中 a为 F_v 的本原元,x 为满足条件的元素.在表 2中列出了相应的结果.

定理 **2.1** 设 $v=12t+1$是一个质数,t 为偶数,则存在 $(v,4,1)$-DDF.

表 2 数组 (v,ξ,x)

Table 2 Array (v,ξ,x)

v	a	x	v	a	x	v	a	x
73	5	29	241	7	84	313	10	92

证明 引理 2.4给出当 $v\geqslant 256036$时,$(v,4,1)$-DDF的存在性;引理 2.5和引理 2.7给出当 $v\in[13, 256036)$时,$(v,4,1)$-DDF的存在性.证明完毕.

由引理 1.6引理 1.7和定理 2.1,有结果:

定理 **2.2** 设 $p\equiv 1(\mathrm{mod}12)$是一个质数,$n\geqslant 1$,则存在 $(p^n,4,1)$-DDF.

参考文献:

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

[2] Dinitz J H, Rodency P. Disjoint difference families with block size 3[J]. Util Math, 1997, 52: 153-160.

[3] Wilson R M. Cyclotomy and difference families in elementary abelian groups[J]. J Number Theory, 1972, 4: 17-47.

[4] Fuji-Hara R, Miao Y. Complete sets of disjoint difference families and their applications[J]. J Statistical Planning and Inference, 2002, 106: 87-103.

[5] Lidl R, Niederreiter H. Finite fields, Encyclopedia of mathematics and its applications [M]. Cambridge: Cambridge University Press, 1983: 20.

(责任编辑: 尹 闯)

(上接第 217页 Continue from page 217)

由定理 3可知 $k+(|E(G)|-1)d\geqslant f^*(u_1u_3)\geqslant 2k+1$,即 $k\leqslant(|E(G)|-1)d-1$.

推论 **5**[8] 若图 G是 k-优美的且 G包含三角形 K_3,则 $k\leqslant|E(G)|-2$.

参考文献:

[1] Joseph A Gallian. A dynamic survey of graph labeling [J]. The Electronic Journal of Combinatorics, 2007, # DS6(14): 1-180.

[2] Joseph A Gallian. A dynamic survey of graph labeling [J]. The Electronic Journal of Combinatics, 2005, # DS6 (5): 1-148.

[3] 梁志和. 关于图标号问题 [J]. 河北师范大学学报: 自然科学版, 2000, 24(3): 300-303.

[4] 程恩魁. 图的强协调性的两个充分条件 [J]. 辽宁工学院学报, 2005, 21(5): 8-9.

[5] 哈拉里 F. 图论 [M]. 李慰萱, 译. 上海: 上海科学技术出版社, 1980.

[6] 邦迪 J A, 默蒂 U S R. 图论及其应用 [M]. 吴望名, 李念祖, 吴兰芳, 等译. 北京: 科学出版社, 1984.

[7] 朱洪, 陈增武, 段振华, 等. 算法设计和分析 [M]. 上海: 上海科学技术文献出版社, 1989.

[8] 梁怀学, 刘春峰. 关于图的 k-优美性 [J]. 东北师大学报: 自然科学版, 1991(1): 41-44.

(责任编辑: 尹 闯)