

长为 $\{4, 5, 6\}$ 的完备删位纠错码的存在性*

蒲利群¹, 柴艳玲²

(1. 郑州大学数学与统计学院, 河南 郑州 450001;

2. 郑州城市职业学院, 河南 郑州 452370)

摘要: 研究具有混合长度的删位纠错码的存在性问题。利用有向平衡设计, 证明了当 $v \geq 4$ 时, $v \notin \{8, 9\}$ 和可能的 $v \neq 14$, $T(2, \{4, 5, 6\}, v)$ -码都存在, 且给出了码字总数的一个上界。

关键词: 删位纠错码; 完备删位纠错码; 混合长度; 有向成对平衡设计

中图分类号: O157.2 **文献标志码:** A **文章编号:** 0529-6579 (2013) 06-0133-03

The Existence of Perfect Deletion-Correcting Codes of Length $\{4, 5, 6\}$

PU Liqun¹, CHAI Yanling²

(1. School of Mathematics and Statistics, Zhengzhou University, Zhengzhou 450001, China;

2. Department of Mathematics, City University of Zhengzhou, Zhengzhou 452370, China)

Abstract: Deletion-correcting codes of mixed length are considered. By applying directed pairwise balanced design, it is proved that for all positive integers v , $v \geq 4$ and $v \notin \{8, 9\}$ and possibly $v \neq 14$, there exists $T(2, \{4, 5, 6\}, v)$ -codes. The bound of $T(2, \{4, 5, 6\}, v)$ -codes is also investigated.

Key words: deletion-correcting code; perfect deletion-correcting code; mixed length; directed pairwise balanced design

设 Z_v 上所有 k 维向量的集合为 Z_v^k , 任意非空子集 C 称为 Z_v 上长为 k 的码, C 中的元素称为码字。设向量 $x \in Z_v^k$, $y \in Z_v^t$, 其中 $0 < t < k$ 。如果由向量 x 删去 $(k-t)$ 个分量可以得到向量 y , 则称向量 y 为向量 x 的子向量。如果任意向量 $y \in Z_v^t$ 至多出现在 C 的一个码字中, 则称 C 为 Z_v 上的一个 $(k-t)$ -删位纠错码。若任意向量 $y \in Z_v^t$ 恰好出现在 C 的一个码字中, 则称 C 是完备的。如果 C 中任意一个码字都不含有重复字符, 称 C 为一个 $T(t, k, v)$ -码。

卫星通讯中, 常常会出现信号衰减和数据丢失, 删位纠错码为了解决此问题而产生。1992年 Levenshtein^[1]首次提出完备删位纠错码的概念, 现已有大量文献对 $T(2, k, v)$ -码做了研究^[2-6], 这些码中码字长度都是一个固定值。文 [7] 提出了

具有混合长度的删位纠错码 $T(2, K, v)$ 的概念, 其中的码字长度取自一个给定的正整数集 K ; 且对 $v \geq 3, v \neq 8$, 利用组合设计方法, 在 Z_v 上构造了具有混合长度 $\{3, 4, 5\}$ 的 $T(2, \{3, 4, 5\}, v)$ -码, 并给出了码字总数的一个上界。本文研究 $K = \{4, 5, 6\}$ 时, $T(2, \{4, 5, 6\}, v)$ -码的存在性。

1 $T(2, \{4, 5, 6\}, v)$ -码的存在性

设 K 是给定的正整数集合, X 是 v 个点的集合, B 是 k 元有序组的集合, 其中 $k \in K$ 。若 X 的任意一个有序点对都恰好出现在 B 中的一个 k 元有序组中, 则称 (X, B) 为一个有向成对平衡设计, 简记 $DB(K, 1; v)$ 。其中, B 中的任何一个 k 元有序组称为一个区组。

如果将 $DB(K, 1; v)$ 的所有区组看成码字, 所

* 收稿日期: 2013-03-19

基金项目: 国家自然科学基金面上资助项目 (11071163)

作者简介: 蒲利群 (1966年生), 女; 研究方向: 组合设计与编码理论; E-mail: liqunpu@zzu.edu.cn

有码字的集合就是一个 $T(2, K, v)$ - 码。

在 Z_v 上存在一个 $T(2, K, v)$ - 码, 等价于存在一个 $DB(K, 1; v)$ 。若 $K_1 \subseteq K_2$, $T(2, K_1, v)$ - 码必为 $T(2, K_2, v)$ - 码。[8] 利用组合方法构造, 并给出了 $K = \{4, 5\}$ 和 $K = \{5, 6\}$ 时, $DB(\{4, 5\}, 1; v)$ 和 $DB(\{4, 6\}, 1; v)$ 的存在性结论。

引理 1^[8] 当 $v \geq 4$, 且 $v \notin \{6, 8, 9, 12, 14\}$ 时, $DB(\{4, 5\}, 1; v)$ 存在。

引理 2^[8] 当 $v \equiv 0, 1 \pmod{3}$, $v \geq 4$, 且 $v \notin \{9, 15\}$ 时, $DB(\{5, 6\}, 1; v)$ 存在。

综合引理 1 和引理 2, 可以得到, 当 $v \geq 4$ 和可能的 $v \notin \{8, 9, 14\}$, 存在一个 $T(2, \{4, 5, 6\}, v)$ - 码。于是, 我们可以得到以下定理。

定理 1 当 $v \geq 4$, 且 $v \notin \{8, 9\}$ 和可能的 $v \neq 14$ 时, 存在一个 $T(2, \{4, 5, 6\}, v)$ - 码。

下面我们将在定理 2 和定理 3 中证明 $v \in \{8, 9\}$ 时, $T(2, \{4, 5, 6\}, v)$ - 码不存在。

2 $v \in \{8, 9\}$ 时, $T(2, \{4, 5, 6\}, v)$ - 码的不存在性

设 C 是定义在 Z_v 上的一个 $T(2, \{4, 5, 6\}, v)$ - 码, 为叙述方便引入以下记号。

$r_j(x)$: 字符 x 在长为 j 的码字中出现的次数, $\forall x \in Z_v$;

b_j : C 中长度为 j 的码字个数。其中, $j = 4, 5, 6$

引理 3 设 C 是一个 $T(2, \{4, 5, 6\}, v)$ - 码, 则有

(i) $3r_4(x) + 4r_5(x) + 5r_6(x) = 2(v-1)$, $\forall x \in Z_v$;

(ii) $b_4 = \frac{\sum_{x \in Z_v} r_4(x)}{4}$, $b_5 = \frac{\sum_{x \in Z_v} r_5(x)}{5}$, $b_6 =$

$$\frac{\sum_{x \in Z_v} r_6(x)}{6}。$$

证明 Z_v 中的任意点对都恰好出现在 C 的一个码字中, 任意一点 x 与其他的 $(v-1)$ 个点构成 $2(v-1)$ 个序对。由于 x 出现在 $r_4(x)$ 个长为 4 的码字中, 且每个码字都有 3 个含 x 的序对, 因此, 所有长为 4 的码字中共有 $3r_4(x)$ 个含 x 的序对。同理, 所有长为 5 的码字中共有 $4r_5(x)$ 个含 x 的序对, 所有长为 6 的码字中共有 $5r_6(x)$ 个含 x 的序对。从而, (i) 式成立。

Z_v 中的任意一点 x 都出现在 $r_4(x)$ 个长为 4 的

码字中, 于是长为 4 的码字中共有 $\sum_{x \in Z_v} r_4(x)$ 个点。

$$\text{故 } b_4 = \frac{\sum_{x \in Z_v} r_4(x)}{4}。$$

$$\text{同理, } b_5 = \frac{\sum_{x \in Z_v} r_5(x)}{5}, b_6 = \frac{\sum_{x \in Z_v} r_6(x)}{6}。$$

定理 2 不存在 $T(2, \{4, 5, 6\}, 8)$ - 码。

证明 假设存在一个 $T(2, \{4, 5, 6\}, 8)$ - 码 C , 由引理 3 得,

$$3r_4(x) + 4r_5(x) + 5r_6(x) = 14$$

于是, $(r_4(x), r_5(x), r_6(x)) = (0, 1, 2), (3, 0, 1)$, 或 $(2, 2, 0)$ 。将 Z_8 中的点划分成三类:

$$V_1 = \{x \in Z_8 \mid (r_4(x), r_5(x), r_6(x)) = (0, 1, 2)\},$$

$$V_2 = \{x \in Z_8 \mid (r_4(x), r_5(x), r_6(x)) = (3, 0, 1)\},$$

$$V_3 = \{x \in Z_8 \mid (r_4(x), r_5(x), r_6(x)) = (2, 2, 0)\}$$

其中, $|V_i| = v_i, i = 1, 2, 3$ 。

显然, $v_1 + v_2 + v_3 = 8$, 且 $0 \leq v_1, v_2, v_3 \leq 8$ 。

又 $b_4 = \frac{3v_2 + 2v_3}{4}, b_5 = \frac{v_1 + 2v_3}{5}, b_6 = \frac{2v_1 + v_2}{6}$ 。于是,

$$2v_1 + v_2 = 0, 6, 12。$$

情形① $2v_1 + v_2 = 0$, 此时 $v_1 = v_2 = 0, v_3 = 8$, 则 $b_5 = \frac{16}{5}$, 不成立。

情形② $2v_1 + v_2 = 6$, 此时 $v_2 = 6 - 2v_1, v_3 = 2 + v_1$, 则 $b_4 = \frac{22 - 4v_1}{4}$, 不成立。

情形③ $2v_1 + v_2 = 12$, 此时 $v_2 = 12 - 2v_1, v_3 = v_1 - 4$, 则 $b_5 = \frac{3v_1 - 8}{5}$ 。必有 $v_1 \equiv 1 \pmod{5}, 4 \leq v_1 \leq 6$ 。于是有, $v_1 = 6, v_2 = 0, v_3 = 2, b_4 = 1$, 而 V_3 中的每个点 x 都出现在 $2(>1)$ 个长为 4 的码字中, 矛盾。

综上, 不存在 $T(2, \{4, 5, 6\}, 8)$ - 码。

定理 3 不存在 $T(2, \{4, 5, 6\}, 9)$ - 码。

证明 假设存在一个 $T(2, \{4, 5, 6\}, 9)$ - 码, 由引理 3 得,

$$3r_4(x) + 4r_5(x) + 5r_6(x) = 16$$

于是, $(r_4(x), r_5(x), r_6(x)) = (2, 0, 2), (1, 2, 1), (0, 4, 0)$ 或 $(4, 1, 0)$ 。将 Z_9 中的点划分成四类:

$$V_1 = \{x \in Z_9 \mid (r_4(x), r_5(x), r_6(x)) = (2, 0, 2)\},$$

$$V_2 = \{x \in Z_9 \mid (r_4(x), r_5(x), r_6(x)) = (1, 2, 1)\},$$

$$V_3 = \{x \in Z_9 \mid (r_4(x), r_5(x), r_6(x)) = (0, 4, 0)\},$$

$$V_4 = \{x \in Z_9 \mid (r_4(x), r_5(x), r_6(x)) = (4, 1, 0)\}$$

其中, $|V_i| = v_i, i = 1, 2, 3, 4$ 。

显然, $v_1 + v_2 + v_3 + v_4 = 9$, 且 $0 \leq v_1, v_2, v_3, v_4 \leq 9$ 。又 $b_4 = \frac{2v_1 + v_2 + 4v_4}{4}$, $b_5 = \frac{2v_2 + 4v_3 + v_4}{5}$, $b_6 = \frac{2v_1 + v_2}{6}$ 。于是, $2v_1 + v_2 = 0, 6, 12, 18$ 。

情形① $2v_1 + v_2 = 0$, 此时 $v_1 = v_2 = 0$, $v_4 = 9 - v_3$, 则 $b_5 = \frac{9 + 3v_3}{5}$, 必有 $v_3 \equiv 2 \pmod{5}$ 。若 $v_3 = 2$, 则 $v_4 = 7$, $b_5 = 3$, 而 V_3 中的每个点 x 都出现在 $4 (> 3)$ 个长为 5 的码字中, 矛盾。若 $v_3 = 7$, 则 $v_4 = 2$, $b_4 = 2$, 而 V_4 中的每个点 x 都出现在 $4 (> 2)$ 个长为 4 的码字中, 矛盾。

情形② $2v_1 + v_2 = 6$, 则 $b_4 = \frac{6 + 4v_4}{4}$, 不成立。

情形③ $2v_1 + v_2 = 12$, 此时 $v_2 = 12 - 2v_1$, $v_4 = 9 - v_1 - (12 - 2v_1) - v_3 = v_1 - v_3 - 3$, 从而, $v_1 \leq 6$, 且 $v_1 - v_3 \geq 3$ 。又 $b_5 = \frac{2(12 - 2v_1) + 4v_3 + (v_1 - v_3 - 3)}{5} = \frac{21 - 3v_1 - 3v_3}{5}$, 必有 $v_1 - v_3 \equiv 2 \pmod{5}$, 故 $v_1 - v_3 = 7$, $v_1 \geq 7$, 矛盾。

情形④ $2v_1 + v_2 = 18$, 此时 $v_1 = 9$, $v_2 = v_3 = v_4 = 0$, $b_4 = \frac{18}{4}$, 不成立。

综上, 不存在 $T(2, \{4,5,6\}, 9)$ - 码。

3 码字总数的上界

一个 $T(2, \{4,5,6\}, v)$ - 码包含了 $v(v-1)$ 个有序对, 而每个长为 k 的码字中, 包含了 $\frac{k(k-1)}{2}$

个这样的有序对。从而 $\sum_{k \in K} \frac{k(k-1)}{2} = v(v-1)$ 。

设 $T(2, \{4,5,6\}, v)$ - 码中, 长为 4, 5, 6 的码字个数分别为 b_4, b_5, b_6 , 则 $6b_4 + 10b_5 + 15b_6 = v(v-1)$ 。

1)。显然, 码字总数 $\leq \max\{b_4 + b_5 + b_6\}$, 从而不超过 $\left\lfloor \frac{v(v-1)}{6} \right\rfloor$ 。

4 小结

本文证明了当 $v \geq 4$ 时, $v \notin \{8, 9\}$ 和可能 $v \neq 14$, $T(2, \{4,5,6\}, v)$ - 码都存在, 且给出了码字个数的一个上界。对 $v = 14$, 如何构造出一个 $T(2, \{4,5,6\}, 14)$ - 码, 或者证明它不存在?

参考文献:

- [1] LEVENSHTAIN V I. On perfect codes in deletion and insertion metric [J]. Discrete Math Appl, 1992, 2(3): 241 - 258.
- [2] BOURS P A H. On the construction of perfect deletion-correcting codes using design theory [J]. Designs, Codes and Cryptography, 1995, 6(2): 5 - 20.
- [3] MAHMOUDI A. Existence of perfect 3-deletion-correcting codes [J]. Designs, Codes and Cryptography, 1998, 14(1): 81 - 87.
- [4] YIN J X. A combinatorial construction for perfect deletion-correcting codes [J]. Designs, Codes and Cryptography, 2001, 23(2): 99 - 110.
- [5] SHALABY N, WANG J M, YIN J X. Existence of 4-deletion-correcting codes with length six [J]. Designs, Codes and Cryptography, 2002, 27(3): 145 - 156.
- [6] WANG J M, YIN J X. Constructions for perfect 5-deletion-correcting codes of length 7 [J]. IEEE Transaction on Information Theory, 2006, 52(8): 3676 - 3685.
- [7] 蒲利群, 柴艳玲. 长为 $\{3,4,5\}$ 的完备删位纠错码的组合构造 [J]. Journal of Mathematics, 2013, 33(1): 163 - 166.
- [8] FUJI-HARA R, MIAO Y, WANG J M, et al. Directed $B(K, 1; v)$ with $K = \{4, 5\}$ and $\{5, 6\}$ related to deletion/insertion-correcting codes [J]. Combinatorial Designs, 2001, 9(12): 147 - 156.