

关于《Barker 码的一些结论和二元码的优选问题》 一文的商榷¹

赵晓群 王仲文*

(燕山大学计算机与信息工程系 秦皇岛 066004)

*(北京电子科技学院 北京 100039)

摘 要 指出杨光正(1995)关于证明 $n > 13$ 的 Barker 不存在的证明过程有误, 因此, $n > 13$ 的 Barker 码是否存在仍然是一个猜想。

关键词 Barker 码, 二元码

中图分类号 TN911.22

1 引言

Barker 码是最佳二相码, 在雷达、通信和遥测遥控领域中有广泛应用。然而自 Barker 码问世近半个世纪以来, 仅找到码长 $n \leq 13$ 的几个 Barker 码^[1], 已证明当 $n > 13$ 时, 若存在 Barker 码, 则码长必为 $n = 4t^2$ ^[2], 并已证明当 $16 \leq n < 12100$ 时, 不存在 Barker 码^[1,2], 进而猜测 $n > 13$ 时很可能不存在 Barker 码, 但至今未能证明。理论分析还表明, 长为 $n = 4t^2$ 的 Barker 码的存在问题与 $n = 4t^2$ 阶的循环 Hadamard 矩阵及长为 $n = 4t^2$ 的一维最佳二进阵列的存在问题密切相关^[3]。1995 年, 文献 [4] 称证明 $n > 13$ 时不存在 Barker 码, 但证明过程有误。

2 文献 [4] 关于 Barker 问题证明的失误之处

为简练起见, 文中有关符号的定义参见文献 [4]。文献 [4] 中关于证明“ $n > 13$ 的 Barker 码不存在”的过程是(文献 [4] 第 4 节):

Y_n 变成 R_n 时, 要求 Y_n 中每列应增加的 -1 个数 Δ^- 为

$$\Delta^- = \sqrt{n}/2. \quad (1)$$

另一方面与 Y_n 对应的 Y'_n (Y'_n 为 Y_n 中第一列元素为 -1 的 w 行组成的 $w \times n$ 阶新矩阵) 中, 第一列与任一系列 j 的 $d_D^N(1, j) = L_s = n/4$, $d_D^S(1, j) = w - L_s$, 它们分别等于第 j 列的正元和负元数。当用 -1 乘 Y'_n 后, 各列的正元、负元全部易号, 任一系列 j 的负元个数与正元个数之差是 $d_D^N(1, j) - d_D^S(1, j)$, 因易号前原有的负元数 $d_D^S(1, j)$ 应扣除, 故净增加的负元数 Δ^- 应为

$$\Delta^- = d_D^N(1, j) - 2d_D^S(1, j) = \sqrt{n} - \sqrt{n}/4 \quad (2)$$

由 (1) 式和 (2) 式解得 $n=0, n=4$, 故得 $n = 4t^2$ 时, 仅存在 $n=4$ 长的 Barker 码, 即不存在 $n > 13$ 的 Barker 码。

在上述证明过程中, (2) 式是错误的。计算 Y'_n 中每个元素易号后, 第 j 列 ($j \neq 1$) 元素中负元的个数与 Y'_n 中相应列负元的个数之差 Δ^- 应为

¹ 1996-04-10 收到, 1996-06-19 定稿

$$\begin{aligned}\Delta^- &= (-Y'_n) \text{中第} j \text{列元素负号的个数} - Y'_n \text{中第} j \text{列元素负号的个数} \\ &= d_D^N(1, j) - d_D^S(1, j) = \sqrt{n}/2\end{aligned}\quad (3)$$

因为 (3) 式与 (1) 式相同, 故解不出 $n=0$ 和 $n=4$, 从而文献 [4] 关于 $n > 13$ 时不存在 Barker 码结论是得不出来的。

3 结 论

关于 $n > 13$ 的 Barker 码是否存在还没有明确结论, 有待进一步研究。

参 考 文 献

- [1] 钟义信. 伪噪声编码通信. 北京: 人民邮电出版社, 1979, 153-155.
- [2] 肖国镇, 梁传甲, 王育民. 伪随机序列及其应用. 北京: 国防工业出版社, 1985, 187-189.
- [3] 杨义先, 林须端. 编码密码学. 北京: 人民邮电出版社, 1992, 125-126.
- [4] 杨光正. Barker 码的一些结论和二元码的优选问题. 电子科学学报, 1995; 17(1): 35-41.

COMMENT ON "SOME CONCLUSIONS ON BARKER CODES AND THE PROBLEM OF SEEKING BEST BINARY CODE"

Zhao Xiaoqun

(Yanshan University, Dep. of Computer and Inform. Eng., Qinhuangdao 066004)

Wang Zhongwen

(Beijing Electronic Technology Institute, Beijing 100039)

Abstract This paper point out that there is no $n > 13$ Barker code concluded by Yang Guangzheng(1995) is not correct. So it is still a conjecture that there is no $n > 13$ Barker codes.

Key words Barker codes, Binary codes

赵晓群: 男, 1962年生, 副教授, 哈尔滨工业大学在职博士生, 主要从事通信理论、编码理论、计算机应用等方面的研究。

王仲文: 男, 1940年生, 教授, 主要从事通信理论、编码理论、密码学、遥测遥控等方面的研究。