第17卷 第1期 电子科学学刊 Vol. 17 No. 1
1995年1月 JOURNAL OF ELECTRONICS Jan. 1995

Barker 码的一些结论和二元码的优选问题

杨 光 正
(中国西南电子技术研究所 成都 610036)

摘要 本文最终证明了不存在 $n>13$ 位的 Barker 码，并探索了二相码的解析优选法. 文中定义了一个 Y_n 矩阵，并由 Y_n 导出了二相码的重量 w, Hamming 距离 d, 游程数 l 和码长 n 之间的关系式，所得关系不仅揭示出二相码各参数之间的内在联系，而且可用它来解决 Barker 码的存在性问题，从而将二相码的优选问题建立在解析的基础上. 文中还举出了应用实例.

关键词 Barker 码，二元码，选码方法.

1 引 言

优选二相码是一件十分艰巨的工作，Lindner[1]和 Cohn[2] 的计算机优选法不仅耗资耗时惊人，而且只能用于码长不长的情况. 分数维树选码法[3]虽然在搜索时间上改善了几个数量级，但可惜得到的不是最优码. 对二相码的优选问题迄今为止尚无良策.

Barker 码是最佳二相码，然而自 1953 年 Barker[4] 码问世近半个世纪以来仅找到了几个 Barker 码，是否存在 $n>13$ 位的 Barker 码? 这个难题一直困扰着学术界，到目前为止，仅得到如下结论: Storer[5] 证明了当 n 为奇数时肯定不存在 $n>13$ 位的 Barker 码. Luenburger[6] 进一步证明了倘若存在 $n>13$ 位的 Barker 码，则 n 必为完全平方数，最后 Turyn[7] 指出这个完全平方数的形式应该是 $n=4t^2$，并猜测很可能不存在 $n>13$ 位的 Barker 码.

由于二相码在现代雷达、通讯、遥控遥测等领域中的广泛应用，所以无论从理论或应用的角度来看，解决这两大难题都有十分重要的意义.

2 Y_n 矩阵和定义

设 n 阶方阵

$$M_n=[a_{ij}]_n,\ a_{ij}\in(0,1),\ i,j=1,2,\cdots,n$$

满足条件:

(1) $a_{i(j+1)}=a_{(i+1)j}\ (\mathrm{mod}\,n)$,

1993-06-15 收到，1994-01-04 定稿

杨光正 男，1937 年生，高级工程师，从事雷达专业，主要研究兴趣是信号处理，通信理论，智能理论.

(2) $\sum_{k=1}^{n}(a_{ik}\oplus a_{jk})=d=\text{const},\ i\neq j,$

其中$\oplus$是异或运算.

对域 $f=(0,1)$, $F=(1,-1)$,

作映射 $\mu:\ \mu(f)\to F,\ \mu^{-1}(F)\to f,$

$\mu(a_{ij})=\{c_{ij},\ 1\leqslant i,j\leqslant n: c_{ij}\in F\}.$

记 $\mu(M_n)=[c_{ij}]_n=Y_n.$

不难看出 Y_n 是对称方阵,且其任一行是由前一行循环左移一位而得.

由 Y_n 的行向量构成的序集记为

$$C=(C_i),\ i=1,2,\cdots,n.$$

若向量 $C_i=(c_{ij})$, $C_i\subset C$, $c_{ij}\in F$, $j=1,2,\cdots,n$. 是码字,则 Y_n 的逆象 M_n 是等重等距码矩阵. 文中我们不加区分地将 Y_n 也称为等重等距码矩阵.

由于映射: $0\to1,1\to-1$, 故 $C_i(\subset C)$的重量w就是 C_i 中-1 的个数. $C_i(\subset C)$ 与 $C_j(\subset C)$ 之间的 Hamming 距离 d 等于 C_i 与 C_j 逐位相比所得的异号元素(文中简称异元)的个数.

容易证明(从略) Y_n 有以下性质:

(1) $\sum_{i=1}^{n}c_{ij}=\sum_{j=1}^{n}c_{ij},\quad \sum_{k=1}^{n}c_{ik}=\sum_{k=1}^{n}c_{jk};$

(2) $\frac{1}{2}\left(\sum_{k=1}^{n}|c_{ik}+c_{jk}|\right)=n-d,\ i\neq j;$

(3) $c_{ij}=c_{(\frac{n}{2}+i)(\frac{n}{2}+j)},\quad c_{i(\frac{n}{2}+i)}=c_{(\frac{n}{2}+i)j},\quad i,j\leqslant\frac{n}{2}$, 当 n 为偶数时;

$$\left.\begin{aligned}&c_{ij}=c_{(\frac{n+1}{2}+i)(\frac{n-1}{2}+j)},\quad i\leqslant\frac{n-1}{2},\quad j\leqslant\frac{n+1}{2},\\&c_{i(\frac{n+1}{2}+j)}=c_{(\frac{n+1}{2}+i)j},\quad i,j\leqslant\frac{n-1}{2},\end{aligned}\right\}\text{当 } n \text{ 为奇数时.}$$

定义 1 若 l 是 $C_i(\subset C)$ 的游程数,定义 $L_t=[l/2]$为码 C_i 的码节数. $[*]$表示不超过$*$的最大整数.

定义 2 $C_i(\subset C)$ 的前 l_h 个游程称为码首 C_h, 最后 l_t 个游程称为码尾 C_t, 中间 $l_b=l-(l_h+l_t)$ 个游程称为码身 C_b.

定义 3 $C_i(\subset C)$ 与 $C_j(\subset C)$ 逐位比较, C_i 中的负元与 C_j 中对应元异号的个数称为负元距离,记为 $d_D^N(i,j)$, 同号的个数称为负元零距,记为 $d_D^L(i,j)$.

定义 4 最优码采用 Lindner[1] 的定义, 对最大旁瓣不超过±1的最优码称为最佳码.

定义 5 周期性自相关函数的旁瓣恒为常数的码称为匀值旁瓣码.

3 匀值旁瓣码的几个定理

引理 1 若 d 和 L_t 分别是 Y_n 中码字间的 Hamming 距离和码字的码节数, 则必

有

$$L_t = d/2. \tag{1}$$

证　因 $C_{i+1}(\subset C)$ 是 $C_i(\subset C)$ 左循环位移一位的结果，因此一个游程仅能提供一对异元。现将 C_{i+1} 与 C_i 逐位比较，当游程总数 l 为偶数时，异元数 $d = l$，当 l 为奇数时，必有 $c_1 = c_n(\in C_i)$，因此左循环位移一位后，l 个游程只能提供 $l-1$ 对异元，亦即 $d = l-1$，又因在 l 为奇数的情况下，等式 $[l/2] = (l-1)/2$ 成立。综合两种情况即得

$$L_t = d/2.$$

证毕

定理 1　在 Y_n 中，若 w 是码字 C_i 的重量，d 是码字之间的 Hamming 距离，则必有

$$d = 2w(n-w)/(n-1). \tag{2}$$

证　$C_i(\subset C)$ 和 $C_j(\subset C)$ 共有负元 $2w$ 个，C_i 与 $C_j(i \neq j)$ 之间的 Hamming 距离 $d = d_D^N(i,j) + d_D^N(j,i)$，此外由定义 3 可知，重量与负元距离和负元零距之间有下列关系

$$w_i = d_D^N(i,j) + d_D^t(i,j),$$
$$w_j = d_D^N(j,i) + d_D^t(j,i),$$

由于 $d_D^t(i,j) = d_D^t(j,i)$，$w_i = w_j = w$，故将上面两式相加后可解出

$$d_D^t(i,j) = w - L_t.$$

现将 Y_n 中第一列元素为 -1 的 w 行抽出来依序排成一个 $w \times n$ 阶新矩阵 Y'_n。在 Y'_n 中，除第一列外，每列都有 $w - L_t$ 个 -1。

另一方面，在 Y'_n 矩阵中，每行有 w 个负元，若不计 Y'_n 的第一列，则 Y'_n 中总共有 $w(w-1)$ 个负元，于是每列的负元数是 $w(w-1)/(n-1)$，二者应相等，

$$w - L_t = w(w-1)/(n-1).$$

解得

$$L_t = w(n-w)/(n-1), \tag{3}$$

或

$$d = 2w(n-w)/(n-1).$$

证毕

将 Y_n 第一列中负元所在的行乘以 -1，这样得到的矩阵记为 R_n。

定理 2　若 S 是 R_n 中除第一列外任一列的算术和，w 是 Y_n 中码字的重量，则必有

$$w = (n \pm \sqrt{(n-1)S+n})/2. \tag{4}$$

证　因与 Y_n 对应的 Y'_n 中，除第一列外，每列中有 $w - L_t$ 个负元，L_t 个正元，将 Y'_n 乘 -1 后每列变成有 $w - L_t$ 个正元，L_t 个负元，故除第一列外，任一列 j 的算术和 σ_j 应为

$$\sigma_j = w - 2L_t = w - d = \sigma$$

是一常数。

R_n 与 Y_n 不同之处仅在于 R_n 中每列正元增加了 σ 个，负元减少了 σ 个，故而除第一列外，R_n 中任一列 j 的算术和 S_j 应为

$$S_j = (n-2w) + 2\sigma_j = n - 2d = S, \tag{5}$$

也是常数，再结合定理 1 即得

$$w = (n \pm \sqrt{(n-1)S+n})/2.$$

证毕

推理1 $C_i(\subset C)$ 的码节数 L_i 必满足关系

$$L_i=(n-S)/4. \tag{6}$$

只要将(5)式代入(1)式化简即得.

推理2 $C_1(\subset C)$ 是匀值旁瓣码,且其旁瓣电平等于 $(n-2d)$.

证 因实域上的自相关函数具有对称性,故只需考察周期性自相关函数的半个周期即可(下文不再说明).

$C_1(\subset C)$ 的周期性自相关函数的右半周期是

$$Y_n\cdot[c_{i1}]_{n\times1}=Y_n\cdot[c_{1i}]^T_{1\times n}=\left[\sum_{j=1}^{n}c_{1j}\cdot c_{ij}\right]_{n\times1},\quad i=1,2,\cdots,n.$$

考虑 Y_n 的性质后,立即得出:由 R_n 每列之算术和构成的行矩阵的转置与上式相等.

R_n 第一列之和等于 n,它是 C_1 的自相关峰.又由(5)式可知,除第一列外,任一列之和 S 恒等于常数 $(n-2d)$,即 C_1 是匀值旁瓣码. 证毕

定理3 $C_1(\subset C)$ 是最佳码字的必要条件是其码首长度 n_h 等于码尾长度 n_t,且其码尾至少由 $l_t=n_h-1$ 个长度为1的游程组成.

证 将 $C_1(\subset C)$ 和它的非周期性自相关函数写成便于分析的形式

$$[C_1]_{1\times n}\cdot{}^rY_n=[\rho_i]_{1\times n},\quad i=1,2,\cdots,n.$$

式中

$$\rho_i=\sum_{j=1}^{n-i+1}c_{1j}\cdot c_{ji},\quad i=1,2,\cdots,n.$$

$$[C_1]_{1\times n}=[c_{11}c_{12}\cdots c_{1k}\cdots c_{1n_h}\cdots c_{1(n-n_h+1)}c_{1(n-n_h+2)}\cdots c_{1n}],$$
$$k=1,2,\cdots,n_h,\quad n_h<n.$$

$$^rY_n=\begin{bmatrix}c_{11} & c_{12}\cdots c_{1j}\cdots c_{1(n-1)} & c_{1n}\\ c_{21} & c_{22} \qquad\qquad c_{2n} & 0\\ \vdots & \vdots \qquad\qquad \vdots & \vdots\\ c_{j1} & \vdots \qquad\qquad \vdots & \vdots\\ \vdots & \vdots \qquad\qquad \vdots & \vdots\\ c_{(n-1)1} & \vdots \qquad\qquad \vdots & \vdots\\ c_{n1} & 0\cdots\cdots\cdots\cdots\cdots & 0\end{bmatrix},\quad j=1,2,\cdots,n.$$

${}^rY_n$ 是 Y_n 的左上三角矩阵.

若 C_1 是最佳码字,根据 Luenburger[6] 的定义,其非周期自相关函数的旁瓣应为

$$\rho_i=\begin{cases}0, & i\text{ 是偶数}\\ 1(\text{或}-1), & i\text{ 是}>1\text{ 的奇数},\end{cases}\Bigg\}\ n\text{ 为奇数;}$$

$$|\rho_i|=\begin{cases}0, & i\text{ 是}>1\text{ 的奇数},\\ 1, & i\text{ 是偶数},\end{cases}\Bigg\}\ n\text{ 为偶数.}$$

由于任何码 C_x 与它的 $C_x^*,\bar{C}_x,\bar{C}_x^*$ 都有相同的自相关函数,因而只需研究其中之一.在四种情况中,我们择码首是正元的那个码来研究,为此不失一般地指定 $c_{1k}=1$, $k=1,2,\cdots,n_h$, 对此

$$\rho_i = \sum_{j=1}^{n-i+1} c_{ji}, \quad i \geqslant n-(n_h-1).$$

现作下标变换，令 $i = n - n_h + k$，则有

$$\rho_{n-n_h+k} = \sum_{j=1}^{n-n_h-k+1} c_{j(n-n_h+k)}, \quad k = 1, 2, \cdots, n_h.$$

再结合 Y_n 的性质可得

$$\rho_{n-n_h+k} = \sum_{j=1}^{n_h-k+1} c_{(1+j-1)(n-n_h+k)}$$

$$= \sum_{j=1}^{n_h+1-k} c_{1(n-n_h+k+j-1)}, \quad k = 1, 2, \cdots, n_h.$$

可由此 n_h 个线性方程解出码尾，当 ρ_{n-n_h+k} 给定后，解是唯一的，它是由长度为 1 的 n_h 个游程组成，由于不能肯定 $c_{1(n-n_h+1)}$ 是否是独立的游程，因此至少

$$l_t = n_h - 1 \tag{7}$$

命题成立。　　证毕

定理 4　长度为 n 的双值旁瓣码[*] C_1，其码首长度 n_h 必满足不等式

$$n_h \leqslant (n + 6 \pm b)/4, \tag{8}$$

b 是某个正整数。

证　因 $C_1 = (C_h C_b C_t) = (c_1 c_2 \cdots c_n)$，其非周期自相关函数 $\rho(j)$ 是

$$\rho(j) = C_h \cdot C_h^* + C_b \cdot C_b^* + C_t \cdot C_t^* + C_b \cdot C_h^* + C_t \cdot C_h^* + C_t \cdot C_b^*$$

$$= \rho_{hh}(j) + \rho_{bb}(j) + \rho_{tt}(j) + \rho_{bh}(j) + \rho_{th}(j) + \rho_{tb}(j).$$

现考察 $j = 3$ 处的旁瓣，不失一般地设 $\rho(3) = \pm b$，对于 $n_b > 1$，$n_h > 2$ 的情况，只剩下五项，

$$\rho(3) = \sum_{i=1}^{n-2} c_i \cdot c_{i+2} = [\rho_{hh}(3) + \rho_{tt}(3)] + [\rho_{bb}(3) + \rho_{bh}(3) + \rho_{tb}(3)].$$

考虑到定理 3，可设 $C_h = (1^j)_{n_h}$，$C_t = ((-1)^{j+1})_{n_h}$。由此不难算出 $\rho_{hh}(3) + \rho_{tt}(3) = 2(n_h - 2)$，于是有

$$2(n_h - 2) + [\rho_{bb}(3) + \rho_{bh}(3) + \rho_{tb}(3)] = \pm b.$$

$\rho(3)$ 共有 $(n-2)$ 项，其中 $\rho_{bb}(3)$ 贡献 $(n_b - 2)$ 项，$\rho_{tb}(3) + \rho_{bh}(3)$ 贡献 4 项，共计 $(n_b + 2)$ 项，欲使 C_b 最短，须要这 $(n_b + 2)$ 项全为 -1，于是有

$$2(n_h - 2) - (n_b + 2) = \pm b,$$

$$n_b = 2n_h - 6 \mp b.$$

多数情况下不能保证 C_b 最短，故而上式应改成不等式：$n_b \geqslant 2n_h - 6 \mp b$。

再考虑 $n = n_b + n_h + n_t = 2n_h + n_b$。最后得到

$$n_h \leqslant (n + 6 \pm b)/4.$$

证毕

对于最佳码，当 n 为偶数时，$b = 0$；当 n 为奇数时，$b = 1$。

---

[*] 本文所说的双值旁瓣码是指非周期自相关函数旁瓣仅有两个取值，注意：切勿与双值自相关码混淆。

4 Barker 码存在性问题

将 R_n 满足 $S=0$ 的 Y_n 记作 H_n，不难证明(从略)

$$H_n \cdot H_n^T = nI_n,$$

即 Y_n 退化成 n 阶 Hadamard 矩阵，对此(4)式简化成

$$w = (n \pm \sqrt{n})/2. \tag{9}$$

因已约定四种情况中只研究一种，故只取式中的负号，同理(3)式简化成

$$L_t = n/4, \quad d = n/2.$$

因 w 必需是正整数，故由(9)式可知，n 必为完全平方数，又由 Hadamard 矩阵的基本性质[6]可知 n 必为 4 的倍数，由此可知必有 $n=4t^2$ (t 是自然数)．此结论早由 Turvn[7] 从其它途径获得过．

当 Y_n 是 H_n 时，每列之和

$$\sum_{k=1}^{n} c_{ik} = 2(d-w) = \sqrt{n}.$$

与 Y_n 对应的 R_n 每列之和(除第一列外)是 $S=0$．由此可知，在 $Y_n \to R_n$ 时，要求 Y_n 中每列应增加的 -1 个数 Δ^- 为

$$\Delta^- = \sqrt{n}/2. \tag{10}$$

另一方面与 Y_n 对应的 Y'_n 中，第一列与任一列 j 的 $d_D^N(1,j) = L_t = n/4$，$d_D^t(1,j) = w - L_t$，它们分别等于第 j 列的正元和负元数．当用 -1 乘 Y'_n 后，各列的正负元全部易号，任一列 j 的负元个数与正元个数之差是 $d_D^N(1,j) - d_D^t(1,j)$，因易号前原有的负元数 $d_D^t(1,j)$ 应扣除，故净增加的负元数 Δ^- 应为

$$\Delta^- = d_D^N(1,j) - 2d_D^t(1,j) = \sqrt{n} - n/4. \tag{11}$$

(10)式与(11)式应相等

$$\sqrt{n} - n/4 = \sqrt{n}/2,$$

由此得

$$n(n-4) = 0,$$

解为

$$n = 0 \quad 和 \quad n = 4.$$

即在 $n=4t^2$ 的值域内，只存在唯一的一个 4 位的 Barker 码．到此为止，我们可对近半个世纪悬而未决的问题下结论了：不存在 $n>13$ 的 Barker 码．

5 最优码的解析搜索法

本节拟用实例说明解析搜索法的可行性和有效性．在举例之前还需补充二条推理．

推理 3 长度为 n 的双值旁瓣码，其码元 c_n 必与旁瓣电平同号．

证 因 $\rho_n = c_1 \cdot c_n$，前面已指定 $c_1 = 1$，故必有 $\rho_n = c_n$，

推理 4 当 $S=1$ 时，l 必为奇数．

证 按码节的定义，每一码节中必是一个正游程后接一个负游程，若 l 是偶数，则

c_n 必是 -1，这与推理 3 矛盾，所以当 $S=1$ 时，j 一定是奇数。

例 1　试在 $S=1$ 的码集中搜索最优码。

将 $S=1$ 代入(4)式得

$$w=(n\pm\sqrt{2n-1})/2, \tag{12}$$

只有在 $n=5,13,\cdots\cdots$ 的情况下才能保证 w 是正整数。

(1) 当 $n=5$ 时，可算出 $w=1$，$L_t=1$，$l=3$，$c_5=1$，考虑定理 3 后可得 $C_1=(111-11)$，这是 5 位 Barker 码。

(2) 当 $n=13$ 时，可算出 $w=4$，$L_t=3$，$l=7$，$c_{13}=1$，$n_k\leqslant 5$，根据定理 3，先写出码首、码尾 $C_1=(11111C_b1-11-11)$，还剩一个正元，二个负元，一个码节，二个游程，仅当 $C_b=(-1-11)$ 时，才能满足上述全部关系。于是 $C_1=(11111-1-111-11-11)$，这是 13 位 Barker 码。

例 2　试在 $S=-1$ 的码集中搜索最优码。

将 $S=-1$ 代入(4)式得

$$w=(n\pm 1)/2.$$

此式表明，正元与负元之差是 1，且 n 必为奇数，这恰好是 m 序列应满足的条件之一。

若我们希望在 $n=7$ 的码集中选出最优码，不难算出 $w=3$，$L_t=2$，$l=4$，$c_7=-1$，$n_k\leqslant 3$，于是可直接写出 $C_1=(111-1-11-1)$，这正是 7 位 Barker 码。

仿此可从 11 位码集中搜索到 11 位 Barker 码。

致谢　本课题曾得到游荣华、陆逸平同志的鼎力支持，谨在此表示诚挚的谢意。

参　考　文　献

[1] Lindner J. Electron. Lett., 1975, 11(2):507—508.
[2] Cohn M N, Fox M, Baden J M. Minimum Peak Sidelobe Pulse Compression Codes. The Record of the IEEE 1990 International Radar Conference. New York: 1990, 633—638.
[3] 李炳成，朱耀庭，朱光熹，等. 基于分维的二相码选码方法. 中国电子学会雷达专业学会，第五届学术年会论文集，武汉: 1989，669—674.
[4] Barker R H. Group Synchonizing of Binary Digital Systems. in Communication Theory, Jackson W, ed. New York: Academic Press, Inc., 1953, 273—287.
[5] Turyn R, Storer J E. Proc. Am. Math. Soc., 1961, 12(1): 394—399.
[6] Luenburger D G. Proc. IEEE, 1963, 51(1): 230—231.
[7] Turyn R. Proc. IEEE (Correspondence), 1963, 51(9): 1256.
[8] 胡正名，陈启浩. 矩阵方法. 北京: 人民邮电出版社，1984，134—137.

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

Yang Guanzheng
(Southwest China Research Institute of Electronic Technology, Chengdu 610036)

Abstract　A new method that seek out best binary code by means of analytics is proposed in this paper, and it was proved that there is no $n>13$ Barker code as well.

Key words　Barker code, Binary code, Selecting code