$(n,6,m)$ 等重等距码的一种构造方法 [1]

林柏钢 邱宏端 *

(福州大学计算机系 福州 350002)
*(福州大学侨兴轻工学院 福州 350002)

摘 要 本文给出 $(n,6,m)(m \geq 6)$ 等重等距码的一种构造方法，侧重讨论了 $(n,6,m)$ 等重等距码的基本结构形式，设计了几类可以用来构造 $(n,6,m)$ 等重等距码的基本单元子块，并分析了构造原则和实现结果，以及置换个数和性能分析。

关键词 等重等距码，窗口码矩阵，子块阵列，置换组合，检错码
中图号 TN911.31

1 引 言

一般线性等重码的结构分析已基本得到解决[1]。而对于一般非线性等重等距码 $(n,2u,m)$ 的研究，由于其结构形式远比线性情形复杂得多，所以分析起来有较大难度。但对于这类既有理论价值又有实用意义的非线性等重等距码的研究，国内外的学者仍然取得不少新成果[2-5]。本文将从构造的角度，对 $(n,6,m)$ $(m \geq 6)$ 等重等距码的结构进行初步分析，并给出一种组合构造的实现方法。最后讨论置换个数和检错性能。

2 $(n,6,m)$ 等重等距码基本结构分析

我们知道，由于码距 $d=2u$ 恒定，研究 $(n,2u,m)$ 等重等距码，最终都可归结为研究 A' 窗口等重等距码矩阵问题。因为矩阵：

$$A=\left[\begin{array}{c|c} \overbrace{\begin{array}{c}1010\cdots011\\ \cdots\cdots\cdots\\ 1010\cdots011\end{array}}^{k\ (R)} & \overbrace{\begin{array}{c}A'\\ (A'_s+A''_s)\end{array}}^{n-k=n'\ (d\equiv 6,\ m'=6)} \end{array}\right]_{l\times n}$$

因此，研究 $(n,6,m)(m \geq 6)$ 等重等距码，只要它可用 $A=(n,6,m)=[R|A']_{l\times n}$ 来表达，同样可称 $A'=(n',6,m')$ 为 A 矩阵的窗口等重等距码矩阵。同理，$A'=A'_s+A''_s$ 则称为 A 矩阵的对称等重等距码窗口矩阵。

引理 1 若 $A=(n,6,m)$ 可用 R、A'，或 $R=R'+R''$，$A'=A'_s+A''_s$ 表示，则下列基本结构等价。

(1) $A=(n,6,m)=[R|A']_{l\times n}$，

(2) $A=(n,6,m)=[R'|R''|A']_{l\times n}$，

[1] 1998-08-26 收到，1999-08-01 定稿

(3) $A=(n,6,m)=[R|A'_s|A''s]_{l\times n}$，

(4) $A=(n,6,m)=[R'|R''|A'_s|A''_s]_{l\times n}$，

其中 $R=R'+R''(R'=R''=R/2)$ 为任意给定排列的 l 行 k 列完全相同的 (0,1) 组合阵列，$A'_s=A''_s=A'/2$ 分别为对应 l 行 n'' 列的码矩阵，$n''=n'/2$。

推论 1　R，A' 及 R'，R''，A'_s，A''_s 经任何左右列向置换后，其基本结构保持不变。

因为 $R=R'+R''$ 的长度可任意组合，所以只要研究 A' 窗口矩阵就行了。这里我们仍然约定，$A'=A'_s+A''_s$ 为两个对称的窗口矩阵。分析 $A'=(n',6,m')$ 可以看出，组成 $A'=(n',6,m')$ 窗口矩阵的典型基本结构是：码长为 12，码重为 6 和码距为 6 的形式。所以，研究 $A'=(n',6,m')$ 可直接以 $A'=(12,6,6)$ 为背景，来分析其码字矩阵结构。

引理 2　若 $A'=(n',6,m')=(12,6,6)$ 存在，则其基本阵列结构为 $A'=[A'_s|A'_s]_{9\times 12}$。其中对称窗口阵列

$$A'_s=\begin{bmatrix}a'_{11} & a'_{12}\\ a'_{21} & a'_{22}\\ a'_{31} & a'_{32}\end{bmatrix}_{9\times 6},\quad A''_s=\begin{bmatrix}a''_{11} & a''_{12}\\ a''_{21} & a''_{22}\\ a''_{31} & a''_{32}\end{bmatrix}_{9\times 6}$$

的码字阵列子集块：(a'_{ij})，(a''_{ij}) 分别为 $(0,1)_{3\times 3}$ 组合阵列。且 $1\le i\le 3$，$1\le j\le 2$。给定 i，可遍取 j。

定义 1　若 $(a'_{ij})_{3\times 3}$，$(a''_{ij})_{3\times 3}$ $(1\le i\le 3,1\le j\le 2)$ 码字阵列子集块中的每行码重个数均一样，则可用 $w=1,2,3\cdots$ 表示，并可分别记为 $w(1)$, $w(2)$, $w(3)\cdots$；若对应每一列向子集块的同码重组合，可用下列几种类型表示：

$$W(1)=\begin{bmatrix}w(1)\\ w(1)\\ w(1)\end{bmatrix},\quad W(2)=\begin{bmatrix}w(2)\\ w(2)\\ w(2)\end{bmatrix},\quad W(3)=\begin{bmatrix}w(3)\\ w(3)\\ w(3)\end{bmatrix},\quad W(4)=\begin{bmatrix}w(4)\\ w(4)\\ w(4)\end{bmatrix},$$

则称 $W(\sigma)(\sigma=1,2,3,\cdots)$ 为同类码重表示法。

下面讨论 (12,6,6) 等重等距码的几个简单性质。

引理 3　若 $A'=(12,6,6)$ 等重等距码成立，则对称码重结构必等价于下列四组组合码矩阵的同类码重结构形式：

$$A'=(12,6,6)=[\overbrace{W(1)W(2)}^{W(3)}\mid\overbrace{W(1)W(2)}^{W(3)}]_{9\times 12},$$

$$A'=(12,6,6)=[W(2)W(1)\mid W(1)w(2)]_{9\times 12},$$

$$A'=(12,6,6)=[W(1)W(2)\mid W(2)w(1)]_{9\times 12},$$

$$A'=(12,6,6)=[W(2)W(1)\mid W(2)w(1)]_{9\times 12},$$

引理 4　若 $A'=(12,6,6)$ 等重等距码成立，则其非对称码重结构必等价于下列两组组合码矩阵的同类码重结构形式：

$$A' = (12,6,6) = [\overbrace{W(2)W(2)}^{W(4)} \mid \overbrace{W(1)W(1)}^{W(2)}]_{9\times 12},$$

$$A' = (12,6,6) = [\overbrace{W(1)W(1)}^{W(2)} \mid \overbrace{W(2)W(2)}^{W(4)}]_{9\times 12},$$

推论 2 在同类码重等价类组合结构中，任一列块对应的码重相等。

推论 3 在同类码重等价类组合结构中，任一列块不存在非相等码重。

推论 4 任一同类码重的等价类结构的码字个数都相等。

依据上述这些基本性质，构造过程主要依据对称和相等码重来构造 (12,6,6) 等重等距码。非相等和非对称情形暂不考虑。因为后者可以通过前者的置换组合很容易得到。

3 (12,6,6) 等重等距码构造方法

定义 2 称 I_1，I_1'、I_0、I_0' 为基本单位 3 阶 (0,1)-矩阵，是指 I_1 为正向 1-单位 (0,1) 方阵，I_1' 为反向 1-单位 (0,1) 方阵，I_0 为正向 0-单位 (0,1) 方阵，I_0' 为反向 0-单位 (0,1) 方阵。其各自结构形式分别为

$$I_1 = \begin{bmatrix}100\\010\\001\end{bmatrix}_{3\times 3},\quad I_1' = \begin{bmatrix}001\\010\\100\end{bmatrix}_{3\times 3},\quad I_0 = \begin{bmatrix}011\\101\\110\end{bmatrix}_{3\times 3},\quad I_0' = \begin{bmatrix}110\\101\\011\end{bmatrix}_{3\times 3}.$$

定义 3 令 $a = [a_1a_2a_3]^{-1}$，$a_i(i = 1,2,3) \in [0,1]$ 为 A' 码矩阵中的二进制元素单元排列，则称 a 为子阵列块的子集码字。

定义 4 令 $I_u(\lambda) = [a]_{3\times 3}(u = 1,2,\cdots,v;\lambda = 1,2,3)$ 是一组基于正向基本单位方阵通过左右移动方式得到的 (0,1) 二进阵列；$I_u'(\lambda) = [a']_{3\times 3}(u = 1,2,\cdots,v,\lambda = 1,2,3)$ 是另一组基于反向基本单位方阵通过左右移动方式得到的 (0,1) 二进阵列，则 $I_u(\lambda)$，$I_u'(\lambda)$ 统称为 A' 码矩阵的基本单元子阵列块。

引理 5 若 A' 码矩阵可由基本单元子阵列块组成，则满足 $I_u(\lambda)$ 与 $I'u(\lambda)$ 定义的第一类组合阵列如下：

$$I_1(1) = \begin{bmatrix}100\\010\\001\end{bmatrix},\quad I_1'(1) = \begin{bmatrix}001\\010\\100\end{bmatrix},\quad I_0(1) = \begin{bmatrix}011\\101\\110\end{bmatrix},\quad I_0'(1) = \begin{bmatrix}110\\101\\011\end{bmatrix};$$

$$I_1(2) = \begin{bmatrix}010\\001\\100\end{bmatrix},\quad I_1'(2) = \begin{bmatrix}010\\100\\001\end{bmatrix},\quad I_0(2) = \begin{bmatrix}101\\110\\011\end{bmatrix},\quad I_0'(2) = \begin{bmatrix}101\\011\\110\end{bmatrix};$$

$$I_1(3) = \begin{bmatrix}001\\100\\010\end{bmatrix},\quad I_1'(3) = \begin{bmatrix}100\\001\\010\end{bmatrix},\quad I_0(3) = \begin{bmatrix}110\\011\\101\end{bmatrix},\quad I_0'(3) = \begin{bmatrix}011\\110\\101\end{bmatrix}.$$

定义 5 若 $a = [a_1a_2a_3]^{-1}$，且 $|a_i|(i = 1,2,3)$ 值相等，则 $I_u(\lambda) = [|a_i|]_{3\times 3}$ 称为给定选取方式等值单元子阵列块的子集码字。

引理 6　若 A' 阵列可由基本给定选取方式等值子块组成，则满足 $I_u(\lambda)$ 子阵列的第二类组合阵列如下：

$$I_2(1)=\begin{bmatrix}110\\110\\110\end{bmatrix},\quad I_2(2)=\begin{bmatrix}011\\011\\011\end{bmatrix},\quad I_2(3)=\begin{bmatrix}101\\101\\101\end{bmatrix};$$

$$I_3(1)=\begin{bmatrix}100\\100\\100\end{bmatrix},\quad I_3(2)=\begin{bmatrix}010\\010\\010\end{bmatrix},\quad I_3(3)=\begin{bmatrix}001\\001\\001\end{bmatrix}.$$

推论 5　(1) 在第一类基本子阵列块中，$d(a_i,a_j)(1\le i,j\le 3)\equiv 2$．(2) 在第二类基本子阵列块中，各子块间 $d(I_u(i)),(I_u(j))\equiv 2,(2\le u\le 3,\ 1\le i,j\le 3,\ i\ne j)$．

有了上述这些基本性质，下面就可以讨论 $A'=(n',6,m')$ 等重等距码构造问题．归结起来，必须遵守几个原则：

引理 7　在对称 (或非对称) 码重中，A' 中的任一列向不能存在全 1 元素．

证明　若任一 j 列为全 1 元素，则任一行有效码重 $m'=5$，使得任两行的码距 $d(C_k,C_l)\le 5$，$(1\le k,l\le 9)$．这与 $d(C_k,C_l)\equiv 6$ 矛盾．

引理 8　任一行向子块组中，不允许存在两个等值子块码字．

证明　由于等值子块 $d(a_i,a_j)(1\le i,j\le 3)=0$，若存在两个等值子块，必使该行向子块组中，任一码字距离 $d(C_k,C_l)\le 4$，结果与 $d(C_k,C_l)\equiv 6$ 矛盾．

例 1

$$\left[\begin{array}{c}\overbrace{110\ 100\ 110\ 010}^{d=4}\\110\ 010\ 110\ 100\\\underbrace{110\ 001\ 110}_{\text{等值子块}}\ 001\end{array}\right]\Rightarrow\left[\begin{array}{c}\overbrace{110\ 100\ 110\ 010}^{d=6}\\110\ 010\ 011\ 100\\\underbrace{110\ 001\ 101}_{\text{非等值子块}}\ 001\end{array}\right].$$

引理 9　任两行对应不同列向子块中，不允许存在两个等值元素码字．

例 2

$$\left|\begin{array}{c}110\ 110\ 010\ 001\\---------\\011\ \underbrace{110\ 001\ 001}_{\text{等值元素}}\end{array}\right|\Rightarrow\left|\begin{array}{c}110\ 110\ 010\ 001\\---------\\011\ \underbrace{110\ 001\ 010}_{\text{非等值元素}}\end{array}\right|.$$

定理 1　正确选取第一类或第二类子块阵列，必可构成引理 3、4 中要求的基本给定组合码字．

该定理表明，只要满足给定要求，并遵守有关构成规则，$A'(12,6,6)$ 等重等距码一定可以构成．下面分别就码重相等和非相等情形举例说明．

例 3　(1) $A'=(12,6,6)=[W(3)|W(3)]_{9\times 12}$ 结构情形：

$$A'=(12,6,6)=\left[\begin{array}{cc} \overbrace{100\ 011}^{W(3)} & \overbrace{100\ 101}^{W(3)} \\ 100\ 101 & 010\ 110 \\ 100\ 110 & 001\ 011 \\ 010\ 101 & 100\ 011 \\ 010\ 110 & 010\ 101 \\ 010\ 011 & 001\ 110 \\ 001\ 110 & 100\ 110 \\ 001\ 011 & 010\ 011 \\ 001\ 101 & 001\ 101 \end{array}\right] \text{或} = \left[\begin{array}{cc} \overbrace{110\ 100}^{W(3)} & \overbrace{100\ 110}^{W(3)} \\ 110\ 010 & 010\ 011 \\ 110\ 001 & 001\ 101 \\ 011\ 100 & 010\ 101 \\ 011\ 010 & 001\ 110 \\ 011\ 001 & 100\ 011 \\ 101\ 100 & 001\ 011 \\ 101\ 010 & 100\ 101 \\ 101\ 001 & 010\ 110 \end{array}\right].$$

(2) $A'(12,6,6)=[W(4)|W(2)]_{9\times 12}$ 或 $[W(2)|W(4)]_{9\times 12}$ 情形：

$$A'=(12,6,6)=\left[\begin{array}{cc} \overbrace{110\ 110}^{W(4)} & \overbrace{100\ 100}^{W(2)} \\ 110\ 011 & 010\ 010 \\ 110\ 101 & 001\ 001 \\ 011\ 011 & 100\ 001 \\ 011\ 101 & 010\ 100 \\ 011\ 110 & 001\ 010 \\ 101\ 101 & 100\ 010 \\ 101\ 110 & 010\ 001 \\ 101\ 011 & 001\ 100 \end{array}\right] \text{或} = \left[\begin{array}{cc} \overbrace{100\ 100}^{W(2)} & \overbrace{101\ 101}^{W(4)} \\ 010\ 100 & 110\ 110 \\ 001\ 100 & 011\ 011 \\ 001\ 001 & 101\ 110 \\ 100\ 001 & 110\ 011 \\ 010\ 001 & 011\ 101 \\ 010\ 010 & 101\ 011 \\ 001\ 010 & 110\ 101 \\ 100\ 010 & 011\ 110 \end{array}\right].$$

引理 10 令独立子阵列块 g_j 分别为 $g_1=\begin{bmatrix}000\\000\end{bmatrix}$, $g_2=\begin{bmatrix}000\\111\end{bmatrix}$, $g_3=\begin{bmatrix}111\\000\end{bmatrix}$, $g_4=\begin{bmatrix}111\\111\end{bmatrix}$, 则码字 C_0 可分别由 $g_j(1\le j\le 4)$ 不同排列组成，并对应行向的两个码字。

很显然，C_0 码字很容易由 g_j 组成，如果选用 g_1-g_4 顺序，则 $C_0=\begin{bmatrix}000 & 000 & 111 & 111\\ 000 & 111 & 000 & 111\end{bmatrix}$. 其它依此类推。

定理 2 若 $A'=(12,6,6)$ 达到尽可能大的码字，则 C_0 应正确选取，即 g_j 中的 $g_{1,4}$，$g_{2,3}$ 应与 A' 码矩阵结构中的 $W(1)$-$W(1)$ 与 $W(2)$-$W(2)$ 配对形式相互列向对应组合结构为：

$$C=\left[\begin{array}{cc} W(1)\text{-}W(1) & W(2)\text{-}W(2) \\ \hline g_1(\text{or}:g_4)\text{-}g_4(\text{or}:g_1) & g_2(\text{or}:g_3)\text{-}g_3(\text{or}:g_2) \\ (\text{或}:g_2(\text{or}:g_3)-g_3(or:g_2) & g_1(\text{or}:g_4)-g_4(\text{or}:g_1)) \end{array}\right]_{11\times 12}$$

其中 $W(1)$ 、 $W(2)$ 排列结构如引理 3,4 。

证明 根据引理 3,4 知，若添加 $g_j(1\le j\le 4)$ 组合后，在对应 $W(1)$-$W(1)$ 配对列向中，恒有 $d_1(W(1)),g_1(\text{or}:g_4))\equiv 3$, $d_1'(W(1),g_2(\text{or}:g_3))\equiv 3$; 而对应 $W(2)$-$W(2)$ 配对列向中，亦恒有 $d_2(W(2),g_2(\text{or}:g_3))\equiv 3$， $d_2'(W(2),g_1(\text{or}:g_4))\equiv 3$ 。综合考虑结果就有 $d(d_1,d_2)\equiv 6$, $d'(d_1',d_2')\equiv 6$ 。 证毕

例如：下列组合形式构成 C 码字成立：

$$C=\left[\begin{array}{cccc} W(1)W(2) & W(1)W(2) \\ \hline g_1 & g_2 & g_4 & g_3 \end{array}\right]_{11\times 12},\quad C=\left[\begin{array}{cccc} W(2)W(2) & W(1)W(1) \\ \hline g_1 & g_4 & g_2 & g_3 \end{array}\right]_{11\times 12}.$$

当然，这种构造方法并不唯一，还可以采用其它方法来实现，这里暂不赘述。

4 码字置换计数与性能讨论

如果我们把码字 C 到自身一个一一映射都看成是一个置换的话，那么，只要 $C=\{C_1,C_2,\cdots,C_{11}\}$ 给定，对应的码长 $n'=\{n_1,n_2,\cdots,n_{12}\}$ 确定，则 C 上的列向码字置换 ψ 可表示为

$$\psi=\begin{bmatrix} n_1 & n_2 & \cdots & n_{11} & n_{12} \\ \psi(n_1) & \psi(n_2) & \cdots & \psi(n_{11}) & \psi(n_{12}) \end{bmatrix}.$$

这样 C 中的全体 $|C|!$ 个置换都可以构成一个码字群。

定理 3　任一确定的码字 $C=(C_{b1},C_{b2},C_{b3},C_{b4})_{11\times 12}$(其中 $C_{bi}(1\le i\le 4)$ 为列向码字子块)，则对应的块排列及块内元素排列共有：$4\times P(3,3)\times P(4,4)=576$ 种码字集合。

由于这种划分只限在四个子块及块内元素排列，并未考虑块与块间的置换形式排列，所以定理证明是显然的。

定理 4　任一确定的码字 $C=[C_{n1},C_{n2},\cdots C_{n11},C_{n12}]_{11\times 12}$，若对应任一列置换排列，则有 $P(12,12)=12!$ 种码字集合。

定理 4 适合于所有等重等距码。同时也说明等重等距码是利用码字率最高的一种编码形式。最后，我们来讨论 $A'=(12,6,6)$ 等重等距码的检错性能。

定理 5　$A'=(12,6,6)$ 等重等距码是检错好码。

证明　据文献 [6] 中定理 4 知，当 $4u\ge n$ 时，二进制 $(n,2u,w)$ 非线性等重码是最佳等重检错码。故有 $4u=n\to 4\times 3=12$ 成立。

可以看出，$A'=(12,6,6)$ 也是一类理想的平衡纠错码。　　证毕

5 结 束 语

本文在等重等距码的窗口矩阵的框架下，通过组合设计的方法来构造 (12,6 ,6) 非线性等重等距码，进而实现 $A'=(n',6,m')(m\ge n'/2)$ 的设计，最终完成给定的 $A=[R|A']$ 的非线性等重等距码的构造。这种组合设计方法，可以类似地推广到 $(n',n'/2,n'/2)$ 的结构形式作参考，但还不能完全系统地去替代，有许多不同的结构特点还需要进一步深入研究。

参 考 文 献

[1]　杨义先，胡正名．线性等重码的结构分析，电子学报，1990, 18(6): 1–8.

[2]　杨义先．极大等重等距码的结构分析．电子学报，1993, 21(7): 97–100.

[3]　胡正名．达到上界的一类等重码，通信学报，1985, 6(4): 44–48.

[4]　符方伟，沈世镒．等距码的几点注记．电子科学学刊，1995, 17(5): 535–538.

[5]　符方伟，沈世镒．等重码的一些新结果．通信学报，1997, 18(1): 17–21.

[6] Wang Xinmei. On the probability of undetected error for binary constant weight codes, BIWIT'88, Beijing: 1988, BI-4.1–4.2.

A CONSTITUTING METHOD OF BINARY CODES OF CONSTANT WEIGHT AND DISTANCE WITH PARAMETERS $(n, 6, m)$

Lin Baigang Qiu Hongduan*

(*Department of Computer Science and Technology, Fuzhou University, Fuzhou* 350002)

*(*Qiaoxin Light Industry College, Fuzhou University, Fuzhou* 350002)

Abstract In this paper, a constituting method of binary codes of constant weight and distance with parameters $(n, 6, m)(m \geq 6)$ is given. The basic structure form of this kind of codes is discussed and the subset block of basic unit which can be used to constitute this kind of codes is designed. The constituting rule and realization result are analysed. Finally, the numbers of permutations and the properties of error-detecting codes are discussed.

Key words Binary codes of constant weight and distance, Window codes matrix, Subset block array, Permutations combination, Error-detecting codes

林柏钢： 男，1953 年生，副教授，主要研究领域为：图论并行算法，组合编码与现代密码，计算机网络安全，AI 技术与工业自动化技术应用.

邱宏端： 女，1955 年生，副教授，主要研究领域为：信息编码与生物技术应用等.