n 元 H-布尔函数 (II) [1]

杨义先 邢育森

(北京邮电大学信息工程系 北京 100088)

摘 要 本文是杨义先以前工作 (1988) 的继续，利用特征矩阵分析 n 元 H- 布尔函数的结构性质，求出了目前为止最好的计数下界。

关键词 H-布尔函数，密码特性，构造和计数

中图号 TN918.1, O153.2

1 引 言

本文是文献 [1] 的继续。

n 元 H-布尔函数在阵列编码、纠错编码和现代密码研究和应用中都起着很重要的作用：(1)n 维 2 阶 Hadamard 矩阵与 n 元 H-布尔函数密切相关；(2) 满足严格雪崩准则的布尔函数与 n 元 H-布尔函数定义等价；(3) 满足 1 次扩散准则的布尔函数与 n 元 H-布尔函数定义等价；(4) 重要而常用的 Bent 函数是 n 元 H-布尔函数的一部分 (特例)；(5)n 元 H-布尔函数在 Reed-Muller 码研究中有重要应用。

n 元 H-布尔函数的个数 $H(n)$ 的求解是一个难度很大且至今尚未解决的问题。文献 [2-5] 分别求出了 $H(2)$、$H(3)$、$H(4)$ 和 $H(5)$。文献 [1, 6-8] 对一些特殊情况的 $H(n)$ 进行了讨论。我们首次利用布尔函数的特征矩阵方法研究 n 元 H-布尔函数的结构特征并由此得到了目前最好的 $H(n)$ 的下界公式。

2 结构特征

定义 1 n 元布尔函数 $f(x_1,\cdots,x_n)$ 称为 n 元 H-布尔函数，当且仅当对任意的单位向量 $\varepsilon_i=(0,\cdots,1,\cdots,0)$, $1\le i\le n$ 成立 $W(f(x+\varepsilon_i)+f(x))=2^{n-1}$。

引理 1 n 元 H-布尔函数的重量 $W(f)$ 一定为偶数 (设为 $2k$), 其取值范围为 $2^{n/2-1}\le|W(f)-2^{n-1}|\le 2^{n-2}$。

记 $H(n)$ 为 n 元 H-布尔函数的个数。目前求得的 $H(n)$ 有：$H(2)=8$, $H(3)=16$, $H(4)=4128$, $H(5)=12,086,336$. 为了研究 $H(n)$ 的取值，先对 n 元 H-布尔函数的结构进行分析。

记 n 元 H-布尔函数重量为 $W(f)=2k(2^{n-3}\le k\le 2^{n-2}-2^{n/2-2}$ 或者 $2^{n-2}+2^{n/2-2}\le k\le 3\times 2^{n-3})$。设重量为 $2k$ 的 n 元 H-布尔函数的个数为 $H(n,2k)$, 则 $H(n)=\sum_k H(n,2k)$。将 $H(n,2k)=H(n,2^n-2k)$ 代入，得

[1] 1995-06-24 收到，1995-06-24 定稿
国家杰出青年基金和国家教委跨世纪优秀人才专项基金资助课题

定理 1　$H(n)=2\sum_{k=2^{n-3}}^{2^{n-2}-2^{n/2-2}}H(n,2k)$ 。

下面分析 n 元 H-尔函数的定序特征矩阵。

定义 2　使 $f(X)=1$ 成立的 n 元向量称为 $f(X)$ 的特征向量。把 $f(X)$ 的所有特征向量按字典顺序排列所得的矩阵称为 $f(X)$ 的定序特征矩阵。显然，布尔函数与其定序特征矩阵是一一对应的。

定义 3　设各行互异矩阵 $A=(a_{ij})_{2k\times n}, a_{ij}=0,1$，若 A 的任意 $n-1$ 列组成的子矩阵中有 r 组 (共 $2r$) 行相同，其它各行互异，称 A 为 A_r 型矩阵。特别的，$r=0$ 时，A_0 的任意 $n-1$ 列组成的子矩阵的各行互异。

定理 2　设 n 元布尔函数 $f(X)$ 的重量为 $2k$, $f(X)$ 为 n 元 H-布尔函数的充要条件为 $f(X)$ 的定序特征矩阵是 $A_{k-2^{n-3}}$ 型矩阵。

证明　由定义 1，$W(f(x_1,\cdots,x_{i-1},0,\cdots,x_n)f(x_1,\cdots,x_{i-1},1,\cdots,x_n))=k-2^{n-3}$，即 $f(X)$ 的定序特征矩阵中去掉第 i 列后所得的子矩阵中有且只有 $k-2^{n-3}$ 组 (共 $2k-2^{n-3}$ 行) 是相同的。由 i 的任意性，可得结论。　　证毕

此定理说明了 n 元 H-布尔函数的构造结构。

3　计数下界

下面考虑 $A_r(0\le r\le 2^{n-3}-2^{n/2-2})$ 型矩阵的构造和计数。

4·1　A_0 型矩阵

引理 2　各行互异的二进制矩阵 A 是 A_0 型矩阵的充要条件是 A 的各行向量之间的 Hamming 距离大于 1 。(此时 A_0 有 2^{n-2} 行)

下面通过构造得到 A_0 的计数下界：

引理 3　任意重量的 n 元向量，与其 Hamming 距离为 1 的 n 元向量有 n 个，且这些向量与原向量的重量奇偶性是相异的。

由此，从 2^{n-1} 个偶重量的 n 元向量中选出 s 个作为 A_0 的 s 行，则至少有 $2^{n-1}-ns$ 个奇重量的 n 元向量和选定的 s 行向量中的任一向量的 Hamming 距离均大于 1 。从这 $2^{n-1}-ns$ 个奇重量中选出 $2^{n-2}-ns$ 个与这 s 个偶重量向量一起构成 A_0 。

令 $A_0(n)$ 表示重量为 2^{n-2} 的 n 元 H-布尔函数的个数，则由 (1) 式和 (2) 式，得

定理 3　$A_0(n)\ge 2\sum_{s=0}^{2^{n-3}-1}\binom{2^{n-1}}{s}\binom{2^{n-1}-ns}{2^{n-2}-s}+\binom{2^{n-1}}{2^{n-3}}\binom{2^{n-1}-n2^{n-3}}{2^{n-3}}$ 。

注：上式中若某项的 $2^{n-1}-ns\le 0$, 则该项为 0 。

4·2　A_1 型矩阵

任取一个 n 元向量 P，与 P 的 Hamming 距离为 1 的 n 个向量为 $Q_1,\cdots,Q_n$ 和 P 作为 A_1 的 $n+1$ 行，又至少有 2^n-n^2 个向量与任意 Q_i 的 Hamming 距离大于 1，从其中选取 $2^{n-2}-n+1$ 个向量 (满足任两个向量之间 Hamming 距离大于 1) 和 $P, Q_1,\cdots,Q_n$ 一起构成 A_1 。选法有

定理 4　$A_1(n)\ge\binom{2^{n-1}}{1}\sum_{s=0}^{2^{n-3-\lfloor(n-1)/2\rfloor}}\binom{2^{n-1}-n^2-n}{s}\binom{2^{n-1}-n^2-n-ns}{2^{n-2}-n+1}$ 。

注：上式中若某项无意义，则该项为 0

4·3　A_r 型矩阵

选取 r 个 n 元向量 $P_1,\cdots,P_r$(其中任两个向量之间的 Hamming 距离大于 2) 和与 P_i 之间的 Hamming 距离为 1 的所有向量作为 A_r 的 $r(n+1)$ 行，至少有 2^n-rn^2 个向量与上述任意的向量之间的 Hamming 距离大于 1，从其中选取 $2^{n+2}+r(n-1)$ 个向量 (其中任两个向量之间 Hamming 距离大于 1) 与上述向量一起构成 A_r。此下界形式繁琐，略去。

由上所述，我们已得到了目前最好的 n 元 H-布尔函数的计数下界。

致谢 感谢北京邮电大学信息安全中心的全体人员的合作，特别感谢与田海建同学的有益讨论！

参 考 文 献

[1] 杨义先. N 元 H-布尔函数. 北京邮电学院学报, 1988, 11(3): 1–9.

[2] 杨义先，胡正名. 4 维 2 阶 Hadamard 矩阵的分类. 系统科学与数学, 1987, 7(1): 40–46.

[3] Shlichta P. Higher Dimensional Hadamard Matrices. IEEE Trans. on IT, 1979, IT-25(5): 825–826.

[4] 李世群，杨义先. 5 维 2 阶 Hadamard 矩阵计数问题的解决. 北京邮电学院学报, 1988, 11(2): 17–21.

[5] 潘新安，杨义先. 5 维 2 阶 Hadamard 矩阵的计数. 北京邮电学院学报, 1987, 10(4): 11–19.

[6] Hammer J, Seberry J. Higher dimensional orthogonal designs and applications. IEEE Trans. on IT, 1981, IT-27(6): 772–779.

[7] Launey W. A Note on N-dimensional Hadamard matrices of order 2^t and Reed-Muuler codes. IEEE Trans. on IT, 1991, IT-37(3): 664–666.

[8] 杨义先. n 维 2 阶 Hadamard 矩阵. 北京邮电学院学报, 1991, 11(4): 1–8.

[9] 杨义先，林须端，胡正名. 编码密码学. 北京：人民邮电出版社, 1992, 81–97; 225–229; 589–627.

ON THE H-BOOLEAN FUNCTIONS(II)

Yang Yixian Xing Yusen

(*Beijing University of Posts & Telecommunications, Beijing* 100088)

Abstract As the second part of author's serial research (1988), the cipher significant and structure properties of H-Boolean functions are investigated in further by the characteristic matrix. The best updated lower bounds are found for the enumeration of H-Boolean functions.

Key words H-Boolean functions, Cipher characteristic, Construction and enumeration

杨义先： 男，1961 年生，教授，博士生导师，主要从事现代密码、信号理论、纠错编码等领域的研究工作.

邢育森： 男，1972 年生，博士生，专业为信号与信息处理，研究方向为数字通信中的信号设计和密码安全.