文章编号:1671-4229(2024)04-0056-11

WDC 算法与 6 元 Bent 函数计数

董军武, 王殊懿, 曹 磊
(广州大学 数学与信息科学学院, 广东 广州 510006)

摘 要: 一般情况下,在布尔函数的研究中,给定一部分地址处 Walsh 谱值的集合 $A=\{(\boldsymbol{\lambda}_i,a_i)\mid\boldsymbol{\lambda}_i\in F_2^n,a_i\in Z,i=0,1,2,\cdots,m-1\}$,寻找满足在这些地址具有给定谱值的所有 n 元布尔函数是很困难的。但是如果给定的地址集合是一个向量子空间,则有简单的求解方法。文章给出一种 WDC 算法,求解具有子空间结构地址的 Walsh 谱值的所有 n 元布尔函数以及个数。该算法包括 3 方面的内容:①如何构造满足这些条件的 n 元布尔函数;②满足这些条件的 n 元布尔函数有多少个? ③子空间地址上的谱值满足什么条件时,才能保证满足这些条件的 n 元布尔函数存在。另外,Bent 函数是非线性度最高的布尔函数,具有非常好的密码学性质。文章利用 WDC 算法并借助计算机搜索,求解出所有的 6 元 Bent 函数,共有 5 425 430 528 个。

关键词: WDC 算法; Walsh 谱; Bent 函数; 哈德玛矩阵
中图分类号: O236.2; TN918.1 **文献标志码**: A

WDC algorithm and enumeration of Bent functions with 6 variables

DONG Jun-wu, Wang Shu-yi, CAO Lei
(School of Mathematics and Information Sciences, Guangzhou University, Guangzhou 510006, China)

Abstract: In the research of Boolean functions, there is an important problem: given a subset $A=\{(\boldsymbol{\lambda}_i,a_i)\mid\boldsymbol{\lambda}_i\in F_2^n,a_i\in\mathbf{Z},i=0,1,2,\cdots,m-1\}$, find all the Boolean functions f in n variables, such that $\hat{f}(\boldsymbol{\lambda}_i)=a_i$ for all $i=0,1,2,\cdots,m-1$, where $\hat{f}(\boldsymbol{\lambda}_i)$ is the Walsh spectral value of the Boolean function f at the address $\boldsymbol{\lambda}_i$. In general, this problem is quite difficult. But if the given set of addresses is a vector subspace of F_2^n, there is a simple solution. This paper, gives an algorithm called WDC Algorithm, that can solve this problem efficiently in this special case. The WDC Algorithm contains the following three parts: ① constructs all the Boolean functions that satisfying all these conditions; ② finds the number of such Boolean functions; and ③ gives a necessary and sufficient condition of the spectral distribution on the subspace to ensure the existence of such Boolean functions. On the other hand, the Bent function is the Boolean function that has the maximal nonlinearity, thus possessing excellent cryptographic properties. This paper uses WDC algorithm to find all 6 - variable Bent functions by means of computer searching, the total number of such functions is 5 425 430 528.

Key words: WDC algorighm; Walsh spectral; Bent function; Hadamard matrix

布尔函数是密码学中一个很重要而且非常有趣的研究课题,在流密码与分组密码的领域中有广泛的应用。人们根据特殊的密码场景提出相应的密码性质,然后研究满足这些性质的布尔函数的构造与计数。布尔函数最常用的密码学性质有:非线性度、相关免疫度、代数免疫度等,文献[1]是一本非常好的关于布尔函数的专著。

Walsh 变换是研究布尔函数的非常重要的工

收稿日期: 2024-01-22; **修回日期**: 2024-03-04
作者简介: 董军武(1971—),男,副教授. E-mail:djunwu@163.com
引文格式: 董军武, 王殊懿, 曹磊. WDC 算法与 6 元 Bent 函数计数[J]. 广州大学学报(自然科学版),2024,23(4):56-66.

具。在布尔函数的理论研究中有一个问题,即给定一个谱值的集合 A
$A=\{(\boldsymbol{\lambda}_i,a_i)\mid\boldsymbol{\lambda}_i\in F_2^n,a_i\in\mathbf{Z},i=0,1,2,\cdots,m-1\}$,求满足条件:对任意的 $i=0,1,2,\cdots,m-1$ 都有 $\hat{f}(\boldsymbol{\lambda}_i)=a_i$ 的所有 n 元布尔函数。对于随机给定的地址集合 A,求解这样的问题是困难的,早在二十世纪九十年代,有很多学者用机器学习的方法研究这个问题[2-4]。

2023 年第八届全国数学密码挑战赛的第三题就是这样的实例。在比赛过程中,笔者找到一种方法:如果给定部分谱值的地址集合是一个向量子空间,则有好的算法解决这个问题。该算法用参赛的 3 名成员也是本文作者姓的第一个字母命名,称为 WDC 算法。

非线性度是衡量布尔函数的重要密码学指标,非线性度达到最大的布尔函数称为 Bent 函数。当 n 为偶数时,n 元 Bent 函数是存在的,它在每一个地址处的 Walsh 谱值的绝对值均为 $2^{\frac{n}{2}}$。

很多学者对 Bent 函数的构造和性质做了研究[5-12],其中,文献[5]指出 $2m$ 元 Bent 函数的代数次数不超过 m,并提出了计算所有 6 元 Bent 函数的方法,但是并没有给出明确的结果。

本文利用 WDC 算法研究 6 元 Bent 函数的计数问题,计算出所有 6 元 Bent 函数共 5 425 430 528 个。

1　预备知识

这里仅介绍本文所需要的有关布尔函数的内容,关于这方面的完整知识,可参阅文献[1]的第二章或者文献[13]的第十章。

以 F_2 表示只有两个元素$\{0,1\}$的二元域。F_2 上的 n 维向量空间记为 $F_2^n=\{(a_1,a_2,\cdots,a_n)\mid a_i\in F_2\}$。$F_2^n$ 中有 2^n 个向量。当需要把向量空间 F_2^n 中的向量全部列出来时,一般按照坐标的字典顺序,即把每一个向量长为 n 的 0 - 1 串看成一个整数的二进制,这些整数之间的大小关系就字典顺序。通常把 F_2^n 中的元素称为地址。

定义在 F_2^n 上,取值为 0 或 1 的函数称为 n 元布尔函数。将 n 元布尔函数 f 的函数值按照地址的字典顺序从小到大全部排列出来,构成一个长度为 2^n 的 0 - 1 串,称之为 n 元布尔函数 f 的真值表。反之,任一长度为 2^n 的 0 - 1 串均可看作某个 n 元布尔函数的真值表,由此可知,共有 2^{2^n} 个 n 元布尔函数。

假定 f 是一个 n 元布尔函数,将 $(-1)^{f(\boldsymbol{x})}$ 按照地址 $\boldsymbol{x}$ 的字典顺序排列构成一个长度为 2^n 的向量,称为布尔函数 f 的极化向量,简记为 $(-1)^f$。

假设 $\boldsymbol{\lambda}=(\lambda_1,\lambda_2,\cdots,\lambda_n)\in F_2^n$,以及 $\boldsymbol{x}=(x_1,x_2,\cdots,x_n)\in F_2^n$,定义 $\boldsymbol{\lambda}$与 $\boldsymbol{x}$ 的内积为它们的对应坐标相乘之后再相加,记为 $\boldsymbol{\lambda}\cdot\boldsymbol{x}$,即

$$\boldsymbol{\lambda}\cdot\boldsymbol{x}=\lambda_1x_1+\lambda_2x_2+\cdots+\lambda_nx_n。$$

这里的加法与乘法,指的是把 0 与 1 看作整数时的加法和乘法。

给定一个 n 元布尔函数 f,对任意的地址 $\boldsymbol{\lambda}\in F_2^n$,定义 f 在 $\boldsymbol{\lambda}$处的 Walsh 谱值为

$$\hat{f}(\boldsymbol{\lambda})=\sum_{\boldsymbol{x}\in F_2^n}(-1)^{\lambda\cdot\boldsymbol{x}+f(\boldsymbol{x})}。$$

将 f 的 Walsh 谱值按照地址 λ 的字典顺序排列出来,称为 f 的 Walsh 谱,简记为 $\hat{f}$。

对于 $\boldsymbol{\lambda}=(\lambda_1,\lambda_2,\cdots,\lambda_n)\in F_2^n$,可以构造一个线性函数,记为 $\boldsymbol{\lambda}\cdot\boldsymbol{x}$ 如下:

$$\lambda_1x_1+\lambda_2x_2+\cdots+\lambda_nx_n,$$

该线性函数的极化向量记为 $(-1)^{\boldsymbol{\lambda}\cdot\boldsymbol{x}}$。于是布尔函数 f 在 λ 处的 Walsh 谱值可以看作线性函数 $\boldsymbol{\lambda}\cdot\boldsymbol{x}$ 的极化向量与 f 的极化向量的内积。向量的内积可看作矩阵的乘法,把 2^n 个线性函数的极化向量当作行,按照线性函数参数 $\boldsymbol{\lambda}$的字典顺序排成一个 2^n 阶方阵,这个方阵称为 n 阶哈德玛矩阵记为 $\boldsymbol{H}_n$。由此可知,n 阶哈德玛矩阵的元素表达式为

$$\boldsymbol{H}_n=((-1)^{i\cdot j})_{2^n\times2^n},$$

其中,$0\leqslant i,j<2^n$,$i\cdot j$ 表示内积。关于哈德玛矩阵,定理 1 列出一些常用而重要的结论,略去证明。

定理 1　n 阶哈德玛矩阵有如下的性质:

(1)可用矩阵运算计算布尔函数 f 的 Walsh 谱

$$\hat{f}=\boldsymbol{H}_n(-1)^f;$$

(2)n 阶哈德玛矩阵满足下面的递推关系:

$$\boldsymbol{H}_n=\begin{pmatrix}\boldsymbol{H}_{n-1}&\boldsymbol{H}_{n-1}\\\boldsymbol{H}_{n-1}&-\boldsymbol{H}_{n-1}\end{pmatrix},\ \boldsymbol{H}_1=\begin{pmatrix}1&1\\1&-1\end{pmatrix};$$

(3)n 阶哈德玛矩阵是可逆的并且

$$\boldsymbol{H}_n\boldsymbol{H}_n=2^n\boldsymbol{I}_{2^n},$$

其中,$\boldsymbol{I}_{2^n}$ 为 2^n 阶单位矩阵。

蝶化算法。假定 F 是一个 n 元布尔函数,F 的真值表是一个长为 2^n 的 0 - 1 串,可将这个 0 - 1 串从中间分开得到两个长为 2^{n-1} 的 0 - 1 串,这两个长为 2^{n-1} 的 0 - 1 串,可以看作两个 $n-1$ 元布尔函数的真值表,假定左边的记为 f_1,右边的记为 f_2。也就是说,任何一个 n 元布尔函数 F 的真值表都可以看作某两个 $n-1$ 元布尔函数 f_1 与 f_2 的真值表级联而成。它们的 Walsh 谱分别记为 $\hat{f}$、$\hat{f}_1$ 与 $\hat{f}_2$。令 $\boldsymbol{H}_n$、$\boldsymbol{H}_{n-1}$ 分别表示 n 与 $n-1$ 阶哈德玛矩阵,则有

$$\hat{f}_1 = \boldsymbol{H}_{n-1}(-1)^{f_1},$$
$$\hat{f}_2 = \boldsymbol{H}_{n-1}(-1)^{f_2},$$
$$\hat{f} = \boldsymbol{H}_n(-1)^F。$$

由于

$$\boldsymbol{H}_n = \begin{pmatrix} \boldsymbol{H}_{n-1} & \boldsymbol{H}_{n-1} \\ \boldsymbol{H}_{n-1} & -\boldsymbol{H}_{n-1} \end{pmatrix}, (-1)^F = \begin{pmatrix} (-1)^{f_1} \\ (-1)^{f_2} \end{pmatrix},$$

利用分块矩阵的乘法运算有

$$\hat{f} = \boldsymbol{H}_n(-1)^F = \begin{pmatrix} \boldsymbol{H}_{n-1} & \boldsymbol{H}_{n-1} \\ \boldsymbol{H}_{n-1} & -\boldsymbol{H}_{n-1} \end{pmatrix} \begin{pmatrix} (-1)^{f_1} \\ (-1)^{f_2} \end{pmatrix} =$$
$$\begin{pmatrix} \boldsymbol{H}_{n-1}(-1)^{f_1} + \boldsymbol{H}_{n-1}(-1)^{f_2} \\ \boldsymbol{H}_{n-1}(-1)^{f_1} - \boldsymbol{H}_{n-1}(-1)^{f_2} \end{pmatrix} = \begin{pmatrix} \hat{f}_1 + \hat{f}_2 \\ \hat{f}_1 - \hat{f}_2 \end{pmatrix}。$$

由此可知,如果知道了两个 $n-1$ 元布尔函数 f_1 和 f_2 的 Walsh 谱,将它们对应位置相加就是由它们级联而成的 n 元布尔函数 F 的前一半位置的 Walsh 谱值;将它们对应的位置相减就是由它们级联而成的 n 元布尔函数 F 的后一半位置的 Walsh 谱值。这个方法一直往前推,把 n 元布尔函数 F 的真值表看成 2^{n-1} 个一元布尔函数的真值表依次拼接而成,然后一步一步地利用递推关系可以计算出 n 元布尔函数 F 的 Walsh 谱。

简单的分析可知,用蝶化算法计算 n 元布尔函数的 Walsh 谱的计算复杂度为 $O(n2^n)$,比用哈德玛矩阵计算的复杂度低。

非线性度。形如

$$\lambda_1 x_1 + \lambda_2 x_2 + \cdots + \lambda_n x_n + \mu$$

的函数称为仿射函数(其中,$\lambda_i, \mu \in F_2$)。两个布尔函数 f 及 g 的汉明距离定义为它们真值表中取值不同的分量个数,记为 $d(f,g)$。n 元布尔函数 f 的非线性度定义为 f 与所有仿射函数的最小距离,记为 N_f。则有

定理 2 假设 f 是 n 元布尔函数,则

$$N_f = 2^{n-1} - \frac{1}{2}\max_{\boldsymbol{\lambda} \in F_2^n} \{ |\hat{f}(\boldsymbol{\lambda})| \}。$$

对任意的 n 元布尔函数 f,有下面的结论成立:

定理 3 $\sum_{\boldsymbol{\lambda} \in F_2^n} (\hat{f}(\boldsymbol{\lambda}))^2 = 4^n$。

由此可知,当 $n=2m$ 为偶数,并且 n 元布尔函数 f 在每一地址处的 Walsh 谱值的绝对值均为 $2^{\frac{n}{2}}$ 时,其非线性度达到最大值 $2^{n-1} - 2^{\frac{n}{2}-1}$。非线性度达到这个最大值的 n 元布尔函数称为 Bent 函数。下面介绍一种常用的构造 Bent 函数的方法:

定理 4 假定 $n=2m$ 是偶数,而 $h(x_1, \cdots, x_m)$ 是一个 m 元布尔函数,则函数 $f = h + x_1 x_{m+1} + x_2 x_{m+2} + \cdots + x_m x_{2m}$ 是一个 n 元 Bent 函数。

当 $n=2m$ 是偶数时,有多少个 n 元 Bent 函数?这是一个目前尚未解决的问题。本文利用 WDC 算法,借助计算机的计算,得到所有 6 元 Bent 函数的总数为 5 425 430 528。下面将详细给出所需要的理论和计算过程。

2 WDC 算法

在布尔函数的理论和应用中,有如下问题,即定一个子集

$$A = \{ (\boldsymbol{\lambda}_i, a_i) \mid i = 0, 1, \cdots, m-1 \},$$

计算所有的 n 元布尔函数 f,使得对任意的 $i = 0, 1, 2, \cdots, m-1$,都有 $\hat{f}(\boldsymbol{\lambda}_i) = a_i$。为了方便,称满足这些条件的布尔函数为目标布尔函数。

利用哈德玛矩阵可以计算布尔函数的 Walsh 谱,即 $\boldsymbol{H}_n(-1)^f = \hat{f}$。依据集合 A 中的每一个地址 $\boldsymbol{\lambda}_i$ 选择 n 阶哈德玛矩阵 $\boldsymbol{H}_n$ 的第 $\boldsymbol{\lambda}_i$ 行,构造一个线性方程,增广常数为 a_i,这样就得到一个线性方程组,该线性方程组有 m 个方程,有 2^n 个未知量。利用高斯消元法求解该线性方程组,所有取值为 ± 1 的解就是全体目标布尔函数的极化向量。

一般情况下,当自由未知量比较多的时候(例如有 64 个自由未知量),想找出目标布尔函数并不容易。

但是,如果给定的 Walsh 谱地址构成一个向量子空间,则有一个算法能彻底解决这个问题,称为 WDC 算法,该算法包含 3 方面的内容:①目标函数的存在性,即子空间上给定的谱值满足什么

条件时,目标布尔函数是存在的;②在目标布尔函数存在的条件下,共有多少个目标布尔函数;③求出所有的目标布尔函数。

假定 B 是 F_2^n 的 r 维向量子空间,其中,$1\leqslant r<n$。为了方便,记 $s=n-r$。定义 B 的正交补空间为

$$B^{\perp}=\{\boldsymbol{\alpha}\in F_2^n \mid \boldsymbol{\alpha}\cdot\boldsymbol{\beta}=0,\boldsymbol{\beta}\in B\},$$

B 的正交补空间的维数恰好为 s。利用内积的双线性特点,为了计算 B 的正交补空间只需要让 $\boldsymbol{\alpha}$ 与 B 的一组基都正交即可。

定理 5 是 WDC 算法的理论基础,证明见附录中。

定理 5　假定 B 是向量空间 F_2^n 的 r 维子空间,以 B 中的元素为行号,从 n 阶哈德玛矩阵 $\boldsymbol{H}_n$ 中选择 2^r 行,得到子矩阵 $\boldsymbol{M}$。则通过有限次交换 $\boldsymbol{M}$ 某两列的操作,可将矩阵 $\boldsymbol{M}$ 化为如下的形状:$(\boldsymbol{H}_r\mid\boldsymbol{H}_r\mid\cdots\mid\boldsymbol{H}_r)$,共 2^s 个 r 阶哈德玛矩阵。

假定给定部分 Walsh 谱值的集合为 $A=\{(\boldsymbol{\lambda}_i,a_i)\mid\boldsymbol{\lambda}_i\in B\}$,其中,$B$ 为 r 维子空间,将 B 中的向量按照字典顺序写出来如下:$B=\{\boldsymbol{\lambda}_0,\boldsymbol{\lambda}_1,\boldsymbol{\lambda}_2,\cdots,\boldsymbol{\lambda}_{2^r-1}\}$。将谱值信息写成向量的形式 $\boldsymbol{\alpha}=(a_0,a_1,\cdots,a_{2^r-1})^{\mathrm{T}}$,则线性方程组

$$\boldsymbol{M}\boldsymbol{y}=\boldsymbol{\alpha}\qquad(1)$$

的所有取值为 ±1 的解就是所有目标布尔函数的极化向量。由于 $\boldsymbol{H}_r\boldsymbol{H}_r=2^r\boldsymbol{I}_r$,用 $\frac{1}{2^r}\boldsymbol{H}_r$ 乘以式(1)的两边,记 $\boldsymbol{\beta}=\frac{1}{2^r}\boldsymbol{H}_r\boldsymbol{\alpha}$,则通过有限次交换某两列的操作之后,可将线性方程组(1)转化为

$$(\boldsymbol{I}_{2^r}\mid\boldsymbol{I}_{2^r}\mid\cdots\mid\boldsymbol{I}_{2^r})\boldsymbol{y}=\boldsymbol{\beta},$$

即 2^r 个具有如下特殊形式的线性方程

$$y_{j_0}+y_{j_1}+\cdots+y_{j_{2^s-1}}=b_j。\qquad(2)$$

由此可知,不同的线性方程,它们未知量的交集为空。因此,只要求出每一个形如式(2)的线性方程的解,就可以求出所有目标布尔函数的极化向量。

如果给 r 维子空间 B 中的地址随机赋 Walsh 谱值的话,则目标布尔函数很可能不存在。为此引入定义 1。

定义 1　称 r 维子空间 B 上的一个谱分布是相容的,指对于这个谱分布,一定存在目标布尔函数。

引入一个符号:对任意的正整数 s,$1\leqslant s<n$,记 $\Gamma(s)=\{0,\pm2,\pm4,\pm6,\cdots,\pm2^s\}$。容易验证 $\Gamma(s)=\{2^s-2z\mid0\leqslant z\leqslant2^s\}$,由此可知,集合 $\Gamma(s)$ 中共有 2^s+1 个数。

定理 6　假定 B 是 r 维向量子空间,$\boldsymbol{\alpha}$ 为子空间 B 上的一个谱分布,记 $\boldsymbol{\beta}=\frac{1}{2^r}\boldsymbol{H}_r\boldsymbol{\alpha}$。则谱分布 $\boldsymbol{\alpha}$ 是相容的充分必要条件是向量 $\boldsymbol{\beta}$ 的每一个分量都落在集合 $\Gamma(s)$ 中。

证明　如果目标布尔函数存在,假定 f 是其中一个目标布尔函数,则 f 的极化向量就是线性方程(1)的解,从而也是线性方程组(2)的解。对每一个 $j=0,1,2,\cdots,2^r-1$,令 z_j 表示 2^s 个变量 $y_{j_0},y_{j_1},\cdots,y_{j_{2^s-1}}$ 中取值为 -1 的变量个数,则这 2^s 个变量中取值为 1 的变量个数为 2^s-z_j,于是方程(2)就变为

$$(2^s-z_j)-z_j=b_j,$$

即 $b_j=2^s-2z_j\in\Gamma(s)$。

另外,如果谱值向量 $\boldsymbol{\alpha}$ 满足定理中的条件,对每一个 j,取 z_j 满足条件 $b_j=2^s-2z_j$。在由线性方程(2)所决定的 2^s 个变量中,任意选择 z_j 个变量,赋值为 -1,将其余的 2^s-z_j 个变量赋值 1,则这些变量满足方程(2),从而它们是线性方程组(1)的解,即它们是某个目标布尔函数的极化向量,这就证明谱向量 $\boldsymbol{\alpha}$ 是相容的。

定理 7 给出了所有目标布尔函数的个数。

定理 7　如果 r 维向量子空间 B 上的谱分布 $\boldsymbol{\alpha}$ 是相容的,令 $\boldsymbol{\beta}=\frac{1}{2^r}\boldsymbol{H}_r\boldsymbol{\alpha}$。记 $\boldsymbol{\beta}=(b_0,b_1,\cdots,b_{2^r-1})$,对每一个 $j=0,1,2,\cdots,2^r-1$,令 $z_j=\frac{1}{2}(2^s-b_j)$,则所有目标布尔函数的个数为

$$N=\prod_{j=0}^{2^r-1}C_{2^s}^{z_j}。$$

证明　由于向量 $\boldsymbol{\alpha}$ 是相容的,因此所有的目标布尔函数恰好是线性方程组(1)的取值为 ±1 的解。线性方程组(1)可以化简成 2^r 个形如(2)的方程,这些方程中的未知量没有交集。因此,所有目标函数的个数等于每一个形如(2)的解数之积。形如(2)的方程的解就是从 2^s 个未知量中,任意选择 z_j 个未知量,赋值为 -1,其余的 2^s-z_j 个未知量赋值为 1,即每一个形如(2)的方程的解数为组合数 $C_{2^s}^{z_j}$,因此,所有的目标布尔函数的个数为 $N=\prod_{j=0}^{2^r-1}C_{2^s}^{z_j}$。

最后,给出目标布尔函数的构造方法。给定 r 维向量子空间 B,以及相容的谱分布 $\boldsymbol{\alpha}$。令 V 为 B 的正交补空间。对任意的 $\boldsymbol{\gamma}\in F_2^n$,称集合

$$\boldsymbol{\gamma}+V=\{\boldsymbol{\gamma}+\boldsymbol{\xi}\mid\boldsymbol{\xi}\in V\}$$

为 V 的陪集。则向量空间 F_2^n 可以分解成 2^r 个两两不相交的陪集的并。定理8表明,每一个形如(2)的方程中,未知量的下标恰好取自 V 的某个陪集。

定理8 每一个形如(2)的方程,它的未知量的下标恰好取自 V 的某个陪集。

证明 由定理5可知,系数矩阵 $\boldsymbol{M}$ 的每一列都是 r 维向量空间 F_2^r 上的一个线性函数,F_2^r 上共有 2^r 个线性函数,每一个线性函数都恰好在矩阵 $\boldsymbol{M}$ 中出现 2^s 次,即可将 2^n 个未知量分成互不相交的 2^r 个组,每组中有 2^s 个未知量,每个未知量对应矩阵 $\boldsymbol{M}$ 的一列。未知量出现在形如(2)的同一个方程中的充分必要条件是,矩阵 $\boldsymbol{M}$ 中与这些未知量相对应的列完全相同(这样的话,用 r 阶哈德玛矩阵作用再除以 2^r 之后,这些列就是相同的单位向量,即只有一个分量取值为1,其余分量取值全为0的向量)。注意到矩阵 $\boldsymbol{M}$ 的元素是由 B 中的向量与列标的内积决定,而向量子空间 B 上的内积,可以由 B 的任意一组基决定。令

$$\{\boldsymbol{\beta}_{2^0},\boldsymbol{\beta}_{2^1},\cdots,\boldsymbol{\beta}_{2^{r-1}}\}\tag{3}$$

为 B 的一组基,任选一个列标 J_0,构造 r 维向量

$$\boldsymbol{\eta}=(\boldsymbol{J}_0\cdot\boldsymbol{\beta}_{2^0},\boldsymbol{J}_0\cdot\boldsymbol{\beta}_{2^1},\cdots,\boldsymbol{J}_0\cdot\boldsymbol{\beta}_{2^{r-1}})^{\mathrm{T}},$$

再令矩阵

$$\boldsymbol{C}=(\boldsymbol{\beta}_{2^0},\boldsymbol{\beta}_{2^1},\cdots,\boldsymbol{\beta}_{2^{r-1}}),$$

则有 $\boldsymbol{\eta}=\boldsymbol{C}\boldsymbol{J}_0$。

于是在矩阵 $\boldsymbol{M}$ 中,与列标 $\boldsymbol{J}_0$ 完全相同的列标 $\boldsymbol{J}$ 恰好是线性方程组

$$\boldsymbol{\eta}=\boldsymbol{C}\boldsymbol{X}\tag{4}$$

的解。由线性方程组解的理论,线性方程组(4)的所有解均形如

$$\boldsymbol{J}_0+\boldsymbol{J},\tag{5}$$

其中,$\boldsymbol{J}$ 是齐次线性方程组 $\boldsymbol{C}\boldsymbol{X}=0$ 的解。由正交补空间的定义知,齐次线性方程组 $\boldsymbol{C}\boldsymbol{X}=0$ 的解恰好是 B 的正交补空间 V。因此,线性方程组(4)的解恰好是 V 的一个陪集。

最后一个问题是如何选择线性方程组的增广系数 b_j。

解线性方程组(1)的时候,可以利用陪集分解,将未知量分组,但是选择哪一个增广系数呢?将系数矩阵化简后,每一列都是 2^r 维单位向量,定理8就是把具有相同单位向量的列分成一组,该组中决定的形如(2)的方程,其增广系数 b_j 的下标 j 就是单位向量中唯一的1出现的位置。如果 r 元线性函数的表达式为

$$l_0x_0+l_1x_1+\cdots+l_{l-1}x_{r-1},$$

那么,这个线性函数的极化向量经过 r 阶哈德玛矩阵作用并除以 2^r 之后,所得到的单位向量中,唯一的取值为1的分量位置就是 $\boldsymbol{l}=l_0+2l_1+2^2l_2+\cdots+2^{r-1}l_{r-1}$。因此,为了选择增广系数,需要计算出形如(2)的方程中任一未知量所在的列,经哈德玛矩阵化成单位向量时,1出现的位置,并计算出该列所对应的线性函数的表达式。由于选择了一组特殊的基(3),只要让任一未知量所对应的列与该基中的每个基向量做内积即可,而这一步运算恰好是前面计算的 $\boldsymbol{\eta}$。WDC算法步骤如下:

WDC 算法

输入:r 维子空间 B, 2^r 维向量 $\boldsymbol{\alpha}$ 以及向量空间的维数 n。

输出:一个目标布尔函数或者无解

Step 1: 令 $s=n-r$;

Step 2: 计算 $\boldsymbol{\beta}=\frac{1}{2^r}\boldsymbol{H}_r\boldsymbol{\alpha}$;

Step 3: 如果 $\boldsymbol{\beta}$ 的某个分量不在集合 $\Gamma(s)$ 中,则返回"无解",算法结束;

Step 4: 对每一个 $i=0,1,2,\cdots,2^r-1$,计算 $z_i=\frac{1}{2}(2^s-b_i)$;

Step 5: 令 $\boldsymbol{C}=(\boldsymbol{\beta}_{2^0},\boldsymbol{\beta}_{2^1},\cdots,\boldsymbol{\beta}_{2^{r-1}})$ 为子空间 B 的一组特殊基;

Step 6: 计算 B 的正交补空间 V;

Step 7: 令 D 为整个向量空间 F_2^n;

Step 8: for i from 0 to 2^r-1 do

(1) 从 D 中任取一个向量 $\boldsymbol{\xi}$,计算 $\boldsymbol{\eta}=\boldsymbol{C}\boldsymbol{\xi}$;

(2) 计算陪集 $\boldsymbol{\xi}+V$;

(3) 从下标在 $\boldsymbol{\xi}+V$ 中的 2^s 个未知量中,任意选择 z_η 未知量赋值为1,其余的 2^s-z_η 个未知量赋值为0;

(4) 从 D 中去掉陪集 $\boldsymbol{\xi}+V$ 中的所有向量;

Step 9: 输出布尔函数 f。

注:在 WDC 算法中,计算量最大的是第 2 步的矩阵计算,计算复杂度为 $O(2^{2n})$。如果用蝶化算法,计算复杂度为 $O(n2^n)$。

约定,用向量的十进制标号表示向量。

例 1　假定 $n=4, B=\{0,1,2,3\}$ 为 F_2^4 中的二维向量子空间。令 $\boldsymbol{\alpha}=(6,-2,-2,-2)^{\mathrm{T}}$。$s=n-r=2$。

计算 $\boldsymbol{\beta}=\frac{1}{2^2}\boldsymbol{H}_2\boldsymbol{\alpha}=(0,2,2,2)^{\mathrm{T}}$,由于 $\boldsymbol{\beta}$ 的每个分量都在集合 $\Gamma(s)=\{0,\pm2,\pm4\}$ 中,因此,目标布尔函数存在。计算

$$z_0=\frac{1}{2}(2^2-b_0)=2,$$

$$z_1=\frac{1}{2}(2^2-b_1)=1,$$

$$z_2=\frac{1}{2}(2^2-b_2)=1,$$

$$z_3=\frac{1}{2}(2^2-b_3)=1。$$

由定理 6 可知,所有的目标布尔函数的个数为

$$N=C_4^2C_4^1C_4^1C_4^1=384。$$

下面利用 WDC 算法计算出一个目标布尔函数。B 的正交补空间为

$$V=\{0,4,8,12\}。$$

B 的一组特殊基为 $\{1,2\}$,可得矩阵

$$\boldsymbol{C}=\begin{pmatrix}1&0&0&0\\0&1&0&0\end{pmatrix}。$$

下面构造 V 的 4 个陪集:

取 $\boldsymbol{\xi}_0=0$ 得 $\boldsymbol{\xi}_0+V=\{0,4,8,12\}$。计算

$$\boldsymbol{\eta}_0=\boldsymbol{C}\boldsymbol{\xi}_0=(0,0)^{\mathrm{T}},$$

因 $z_0=2$,从 $\{y_0,y_4,y_8,y_{12}\}$ 中选择两个变量取值为 1,其余两个变量取值为 0,不妨令 $y_0=y_4=1$, $y_8=y_{12}=0$。

取 $\boldsymbol{\xi}_1=1$ 得 $\boldsymbol{\xi}_1+V=\{1,5,9,13\}$。计算

$$\boldsymbol{\eta}_1=\boldsymbol{C}\boldsymbol{\xi}_1=(1,0)^{\mathrm{T}}$$

编号为 1。因 $z_1=1$,从 $\{y_1,y_5,y_9,y_{13}\}$ 中选择一个变量取值为 1,其余 3 个变量取值为 0,不妨令 $y_1=1$, $y_5=y_9=y_{13}=0$。

取 $\boldsymbol{\xi}_1=2$ 得 $\boldsymbol{\xi}_2+V=\{2,6,10,14\}$。计算

$$\boldsymbol{\eta}_2=\boldsymbol{C}\boldsymbol{\xi}_2=(0,1)^{\mathrm{T}}$$

编号为 2。因 $z_2=1$,从 $\{y_2,y_6,y_{10},y_{14}\}$ 中选择一个变量取值为 1,其余 3 个变量取值为 0,不妨令 $y_2=1$, $y_6=y_{10}=y_{14}=0$。

取 $\boldsymbol{\xi}_3=3$ 得 $\boldsymbol{\xi}_3+V=\{3,7,11,15\}$。计算

$$\boldsymbol{\eta}_3=\boldsymbol{C}\boldsymbol{\xi}_3=(1,1)^{\mathrm{T}}$$

编号为 3。因 $z_3=1$,从 $\{y_3,y_7,y_{11},y_{15}\}$ 中选择一个变量取值为 1,其余 3 个变量取值为 0,不妨令 $y_3=1$, $y_7=y_{11}=y_{15}=0$。

于是得到一个目标布尔函数,其真值表为 1111 1000 0000 0000,即它满足条件:

$\hat{f}(0)=6, \hat{f}(1)=-2, \hat{f}(2)=-2, \hat{f}(3)=-2$。

事实上,该布尔函数的 Walsh 谱为

$$6,-2,-2,-2,-6,2,2,2,$$
$$-10,-2,-2,-2,-6,2,2,2。$$

3　6 元 Bent 函数的计数

本节利用 WDC 算法,计算 6 元 Bent 函数的个数。在下面的讨论中,需要用到定理 9:

定理 9　假定 B 是 F_2^n 的 r 维向量子空间,令 V 为 B 的正交补空间。对任意的 n 元布尔函数 f,记 $b=\sum_{\boldsymbol{x}\in V}(-1)^{f(\boldsymbol{x})}$。则有

$$\sum_{\boldsymbol{\lambda}\in B}\hat{f}(\boldsymbol{\lambda})=2^r b,\tag{6}$$

其中,$b\in\Gamma(s)$ 有 2^s+1 种可能。

证明　按照 Walsh 谱的定义,并交换求和的顺序可得

$$\sum_{\boldsymbol{\lambda}\in B}\hat{f}(\boldsymbol{\lambda})=\sum_{\boldsymbol{\lambda}\in B}\sum_{\boldsymbol{x}\in F_2^n}(-1)^{\boldsymbol{\lambda}\cdot\boldsymbol{x}+f(\boldsymbol{x})}=$$
$$\sum_{\boldsymbol{x}\in F_2^n}\Big(\sum_{\boldsymbol{\lambda}\in B}(-1)^{\boldsymbol{\lambda}\cdot\boldsymbol{x}}\Big)(-1)^{f(\boldsymbol{x})}。$$

考虑内和

$$\sum_{\boldsymbol{\lambda}\in B}(-1)^{\boldsymbol{\lambda}\cdot\boldsymbol{x}}\tag{7}$$

表示在 n 阶哈德玛矩阵中,选择 $\boldsymbol{x}$ 所在的列,将行标号 $\boldsymbol{\lambda}\in B$ 的元素全部加起来。定理 5 中,矩阵 $\boldsymbol{M}$ 就是从 n 阶哈德玛矩阵中按照标号 $\boldsymbol{\lambda}\in B$ 选择行构成的矩阵。因此,内和(7)就是矩阵 $\boldsymbol{M}$ 的第 $\boldsymbol{x}$ 列中所有元素相加。定理 5 表明矩阵 $\boldsymbol{M}$ 的每一列都是 r 元线性函数的极化向量并且每一个 r 元线性函数都恰好出现 2^s 次。

由于非零的线性函数是平衡的,它的极化向量中 1 与 −1 各占一半,因此,对应的内和(7)等于 0。而 r 元零函数的极化向量全为 1,因此,对应的内和(7)等于 2^r。V 是 B 的正交补空间,因此,矩阵 $\boldsymbol{M}$ 的第 $\boldsymbol{x}$ 列对应零函数,当且仅当 $\boldsymbol{x}\in V$,即

$$\sum_{\boldsymbol{\lambda}\in B}(-1)^{\boldsymbol{\lambda}\cdot x}=\begin{cases}0, & \boldsymbol{x}\notin V,\\ 2^r, & \boldsymbol{x}\in V。\end{cases}$$

于是有

$$\begin{aligned}\sum_{\boldsymbol{\lambda}\in B}\hat{f}(\boldsymbol{\lambda}) &= \sum_{x\in F_2^n}\Big(\sum_{\boldsymbol{\lambda}\in B}(-1)^{\boldsymbol{\lambda}\cdot x}\Big)(-1)^{f(x)} = \\ &\sum_{x\in V}\Big(\sum_{\boldsymbol{\lambda}\in B}(-1)^{\boldsymbol{\lambda}\cdot x}\Big)(-1)^{f(x)}+\\ &\sum_{x\notin V}\Big(\sum_{\boldsymbol{\lambda}\in B}(-1)^{\boldsymbol{\lambda}\cdot x}\Big)(-1)^{f(x)} = \\ &\sum_{x\in V}\Big(\sum_{\boldsymbol{\lambda}\in B}(-1)^{\boldsymbol{\lambda}\cdot x}\Big)(-1)^{f(x)} = \\ &2^r\sum_{x\in V}(-1)^{f(x)} = b\cdot 2^r,\end{aligned}$$

结论得证。

假定f是一个6元Bent函数,则对任意的$\boldsymbol{\lambda}\in F_2^6$,都有$\hat{f}(\boldsymbol{\lambda})=8$或者$\hat{f}(\boldsymbol{\lambda})=-8$。取一个固定的五维子空间$B=\{0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31\}$。$B$的正交补空间为$V=\{0,32\}$。

考虑B上的谱值分布。由定理9可知,$\sum_{\boldsymbol{\lambda}\in B}\hat{f}(\boldsymbol{\lambda})=2^5b$,其中,$b\in\Gamma(1)=\{\pm 2,0\}$,即$\sum_{\boldsymbol{\lambda}\in B}\hat{f}(\boldsymbol{\lambda})=64,0$或$-64$。假定$f$在$B$中有$u$个8,由于$B$中有32个向量,因此,$B$中有$32-u$个$-8$。于是

$$\sum_{\boldsymbol{\lambda}\in B}\hat{f}(\boldsymbol{\lambda})=8u-8(32-u)\in\{0,64,-64\},$$

可得$u=20$, 16或者12,即五维子空间B上的谱值分布有

$$C_{32}^{12}+C_{32}^{20}+C_{32}^{16}=1\ 052\ 666\ 070$$

种可能。这个数量在普通计算机的搜索范围之内,笔者对每一种可能的谱值分布,先利用定理6判断该分布是否相容。如果相容,进一步利用WDC算法求出所有目标布尔函数,对每一个目标布尔函数,计算其Walsh谱,判断是否为Bent函数,从而可以计算出所有6元Bent函数的数目。

经过4天多的计算,发现共有5 425 430 528个6元Bent函数。在计算过程中,还发现一些规律如下:

当$u=12$和$u=20$时,即B上的谱值分布分别有12和20个8时,B相容的向量个数是相同的,均有3 513 664个。

对于二者个数相等,可以证明:如果$\boldsymbol{\alpha}$是B相容的向量,并且在B上的谱值有12个8,则存在布尔函数f,使得f在B上地址的Walsh谱值恰好为向量$\boldsymbol{\alpha}$。令$g=f+1$,则对任意的$\boldsymbol{\lambda}\in F_2^6$,均有$\hat{g}(\boldsymbol{\lambda})=-\hat{f}(\boldsymbol{\lambda})$。即$-\boldsymbol{\alpha}$也是$B$相容的向量,而向量$-\boldsymbol{\alpha}$中有$u=20$个8。反之亦然,即如果$\boldsymbol{\alpha}'$是具有20个8的$B$相容向量,则$-\boldsymbol{\alpha}'$就是具有12个8的$B$相容向量,这就证明具有12个8的$B$相容向量个数等于具有20个8的$B$相容向量个数。

当$u=16$时,即B上的谱值分布有16个8时,满足这个条件的B相容向量有7 027 328个。这个数目恰好等于$u=12$与$u=20$的个数之和。

对每一个B相容的向量$\boldsymbol{\alpha}$,利用WDC算法,即计算$\boldsymbol{\beta}=\frac{1}{2^5}\boldsymbol{H}_5\boldsymbol{\alpha}$,$\boldsymbol{\beta}$是均有16个分量取值为0,从而有$2^{16}=65\ 536$个目标布尔函数。进一步计算每一个目标布尔函数的Walsh谱,发现有两种可能:这65 536个目标布尔函数中要么有384个Bent函数,要么有896个Bent函数。更详细的信息见表1。

表1 6元Bent函数个数信息

Table 1 Enumeration information of 6-variable Bent functions

函数个数	$u=12$	$u=20$	$u=16$	总数
384	3 499 776	3 499 776	6 999 552	13 999 104
896	13 888	13 888	27 776	55 552

因此,6元Bent函数的总数为

$$N=13\ 999\ 104*384+55\ 552*896=$$
$$5\ 425\ 430\ 528。$$

4 结 语

本文提出了WDC算法,完整解决了具有子空间谱值分布的目标布尔函数的问题。给定r维子空间B,以及B上的一个谱值分布向量$\boldsymbol{\alpha}$,给出了$\boldsymbol{\alpha}$为B相容的充分必要条件,给出了目标布尔函数的计数公式,并给出了求解目标布尔函数的方法。用WDC算法求解目标布尔函数时,算法复杂度远远低于高斯消元法的复杂度。

作为WDC算法的一个应用,借助计算机的计算能力,笔者计算出所有6元Bent函数的数目。在解决6元Bent函数的计数过程中,并没有充分利用WDC算法提供的信息,而是过多地依赖计算机的搜索能力。例如只选择一个五维子空间使用WDC算法。事实上在五维子空间B中还有更多

的维数更小的子空间,如果充分利用定理 8,或许会减少计算机的搜索工作量,或者说可以尝试计算 8 元 Bent 函数的计数问题。

展望未来,有以下 3 个方向可以进一步研究:

(1)深入研究 n 元 Bent 函数在 $n-1$ 维子空间 B 上的分布规律,即研究 B 相容向量的个数;

(2)猜想:假定 B 是 n 维向量空间 F_2^n 的 $n-1$ 维子空间,给定 B 上的一个取值为 $\pm 2^{n/2}$ 的谱分布 $\boldsymbol{\alpha}$。如果 $\boldsymbol{\alpha}$ 是相容的,则目标布尔函数的个数一定是 2^{2^n-2};

(3)如果上述的猜想正确,那么就需要进一步研究每一个 B 相容向量的目标布尔函数中,到底有多少个 n 元 Bent 函数。

今后将继续挖掘 WDC 算法的潜力,用更多的理论结果代替计算的搜索,以期计算出 8 元甚至 10 元 Bent 函数的个数。

参考文献:

[1] 温巧燕, 钮心忻, 杨义先. 现代密码学中的布尔函数[M]. 北京:科学出版社, 2000.

[2] Mansour Y. Learning Boolean functions via the Fourier transform[J]. Theoretical Advances in Neural Computation & Learning, 1994, 282(2):391-424.

[3] Kharitonov M. Proceedings of the Twenty-Fifth Annual ACM Symposium on Theory of Computing, May 16-18, 1993[C]. New York:ACM,1993.

[4] Johannes K, Lindner W. Learning Boolean functions under the uniform distribution via the Fourier transform[J]. Bulletin of the European Association for Theoretical Computer Science, 2006, 42(89):48-78.

[5] Rothaus O S. On "Bent" functions[J]. Journal of Combinatorial Theory, Series A, 1976, 20(3): 300-305.

[6] Carlet C. Eurocode '90, Lecture Notes in Computer Science, November 05-09,1990[C]. Berlin: Springer-Verlag,1990.

[7] Carlet C. Partially-Bent functions[J]. Design Codes and Cryptography, 1993, 3(2):135-145.

[8] Carlet C, Guillot P. A characterization of binary Bent functions[J]. Journal of Combinatorial Theory Series A, 1996, 76(2): 328-335.

[9] Carlet C. Lecture Notes in Computr Science, Advance in Cryptoloty-EUROCRYPT'93 May 23-27,1993[C]. Berlin:Springer-Verlag, 1993.

[10] Dillon J F. Elementary Hadamard difference sets[D]. College Park: University of Maryland, 1974.

[11] Hou X D. Results on Bent functions[J]. Journal of Combinatorial Theory, Series A, 1997, 80(2):232-246.

[12] 胡磊, 裴定一,冯登国. 一类 Bent 函数的构造[J]. 中国科学院研究生院学报, 2002, 19(2): 103-106.

[13] 裴定一, 徐祥,等. 信息安全数学基础[M]. 第二版. 北京:人民邮电出版社, 2016.

[14] Langevin P, Leander G. Counting all bent functions in dimension eight 99270589265934 370305785861242880[J]. Design Codes and Cryptography, 2011, 59:193-205.

【责任编辑: 卓祯雨】

附录一. 4 元 Bent 函数

如果 f 是一个 4 元 Bent 函数,则对任意的 $\boldsymbol{\lambda} \in F_2^4$ 都有 $\hat{f}(\boldsymbol{\lambda}) = 4$ 或者 $\hat{f}(\boldsymbol{\lambda}) = -4$。令 B 是 F_2^4 中的任一三维子空间,u 是 B 中谱值为 4 的个数。利用定理 9 可知 $u = 2, 6, 4$。

当 $u = 2$ 或者 6 时,共有 28 个维数为 8 的 B 相容向量;当 $u = 4$ 时,共有 56 个维数为 8 的 B 相容向量。

对于每一个 B 相容的向量 $\boldsymbol{\alpha}$,用 WDC 算法均可计算出 $2^4 = 16$ 个目标布尔函数,其中,有 8 个目标布尔函数为 Bent 函数,因此,4 元 Bent 函数共 896 个。表 2 列出了 4 元布尔函数的个数信息。

表 2　4 元 Bent 函数个数信息

Table 2　Enumeration information of 4-variable Bent functions

函数个数	$u=2$	$u=6$	$u=4$	总数
8	28	28	56	112
函数总数	224	224	448	896

附录二. 定理5的证明

由于 r 阶哈德玛矩阵是将 F_2^r 上的所有线性函数的极化向量作为行(或者列)按照线性函数的字典排序而得到的。矩阵 $\boldsymbol{M}$ 是从 n 阶哈德玛矩阵中根据 r 维子空间 B 中向量的字典顺序选择行而得到的。因此,定理5的证明分两大步:第一步,建立从 B 到 F_2^r 的一个同构映射,从而将矩阵 $\boldsymbol{M}$ 的每一列看作 F_2^r 上的线性函数;第二步,证明定理5的结论,即证明 F_2^r 上的每一个线性函数作为矩阵 $\boldsymbol{M}$ 的列,都恰好出现 2^s 次。

为了讨论上的方便,引入定义2。

定义2 对于向量空间 F_2^n 中的任一非零向量 $\boldsymbol{\alpha}=(a_0,a_1,\cdots,a_{n-1})$,称满足 $a_i\neq 0$ 的最大非负整数 i 为 $\boldsymbol{\alpha}$ 的最高权位,记为 $l(\boldsymbol{\alpha})$。

注:零向量不定义最高权位,每一个非零向量都有唯一的最高权位。

对于给定的 r 维向量子空间 B,令 $V_0=\{0\}$。下面通过 r 步将 B 中的向量进行字典排序:

第0步,假定集合 $B\backslash V_0$ 中最高权位的最小值为 l_0,满足 $l(\boldsymbol{\alpha})=l_0$ 的向量只有一个,如果满足这个条件的向量有多个,假定 $\boldsymbol{\alpha}_1$ 及 $\boldsymbol{\alpha}_2$ 的最高权位均为 l_0,那么 $\boldsymbol{\alpha}_1+\boldsymbol{\alpha}_2$ 的最高权位就小于 l_0,而且 $\boldsymbol{\alpha}_1+\boldsymbol{\alpha}_2\in B$,与 l_0 的最小性矛盾。把这个向量记为 $\boldsymbol{\beta}_{2^0}$。构造集合 $U_1=\{\boldsymbol{\beta}_{2^0}+\boldsymbol{\beta}\mid\boldsymbol{\beta}\in V_0\}$,并令集合 $V_1=V_0\cup U_1$。则集合 U_1 中只有一个元素,集合 V_1 中有两个元素。

第1步,假定集合 $B\backslash V_1$ 中最高权位的最小值为 l_1,构造集合

$$U_2=\{\boldsymbol{\beta}\in B\mid l(\boldsymbol{\beta})=l_1\}。$$

令集合 U_2 中字典顺序最小的向量为 $\boldsymbol{\beta}_{2^1}$,则有 $U_2=\{\boldsymbol{\beta}_{2^1}+\boldsymbol{\beta}\mid\boldsymbol{\beta}\in V_1\}$。由此可知,$U_2$ 中有2个元素。再令集合 $V_2=V_1\cup U_2$,则集合 V_2 中有4个元素。

一般地,在第 i 步中,假定集合 $B\backslash V_i$ 中最高权位的最小值为 l_i,构造集合

$$U_{i+1}=\{\boldsymbol{\beta}\in B\mid l(\boldsymbol{\beta})=l_i\}。$$

令集合 U_{i+1} 中字典顺序最小的向量为 $\boldsymbol{\beta}_{2^i}$,则有 $U_{i+1}=\{\boldsymbol{\beta}_{2^i}+\boldsymbol{\beta}\mid\boldsymbol{\beta}\in V_i\}$。由此可知,$U_{i+1}$ 中有 2^{i-1} 个元素。再令集合 $V_{i+1}=V_i\cup U_{i+1}$,则集合 V_{i+1} 中有 2^i 个元素。

当 $i=r-1$ 时,得到 V_r 中有 2^r 个元素,即 $V_r=B$。

在上述过程中,得到一组向量

$$\{\boldsymbol{\beta}_{2^0},\boldsymbol{\beta}_{2^1},\cdots,\boldsymbol{\beta}_{2^{r-1}}\}。\tag{8}$$

满足条件 $l(\beta_{2^i})=l_i$,而且

$$l_0<l_1<\cdots<l_{r-1}。$$

由此可知,向量组(8)是线性无关的,从而构成子空间 B 的一组基。

这组基还满足如下的性质:

引理1 对任意的 $k<i$,向量 $\boldsymbol{\beta}_{2^i}$ 的第 l_k 个坐标一定是0。

证明 用反证法,如果存在某个整数 $k<i$,使得向量 $\boldsymbol{\beta}_{2^i}$ 的第 l_k 个坐标为1,则向量 $\boldsymbol{\beta}_{2^i}+\boldsymbol{\beta}_{2^k}\in B$,但是这个向量的字典顺序大小于 $\boldsymbol{\beta}_{2^i}$,这个向量也在集合 U_{i+1} 中,这与 $\boldsymbol{\beta}_{2^i}$ 的字典序最小矛盾,引理1得证。

将 B 中的所有向量按照基(8)下的坐标的字典顺序排列,得到

$$B=\{\boldsymbol{\beta}_0,\boldsymbol{\beta}_1,\boldsymbol{\beta}_2,\cdots,\boldsymbol{\beta}_{2^r-1}\},$$

即对于每个非负整数 s,$0\leqslant s<2^r$,如果 s 的二进制表示为 $s=(s_0,s_1,\cdots,s_{r-1})$,则有

$$\boldsymbol{\beta}_s=s_0\boldsymbol{\beta}_{2^0}+s_1\boldsymbol{\beta}_{2^1}+\cdots+s_{r-1}\boldsymbol{\beta}_{2^{r-1}}。$$

下面证明,如果标号 $s<t$,则在字典顺序的意义下必定有 $\boldsymbol{\beta}_s<\boldsymbol{\beta}_t$。

假定标号 s 与 t 的二进制表示分别为

$$s=(s_0,s_1,\cdots,s_{r-1}),$$
$$t=(t_0,t_1,\cdots,t_{r-1}),$$

由于 $s<t$,则存在正整数 k,使得 $t_k=1$,$s_k=0$,并且 $s_{k+j}=t_{k+j}$,$j=1,2,\cdots,r-1-k$。为了方便,记 $l_k=$

$l(\boldsymbol{\beta}_{2^k})$为基向量的最高有效位。

将向量 $s_{k+1}\boldsymbol{\beta}_{2^{l_k+1}}+\cdots+s_{r-1}\boldsymbol{\beta}_{2^{l_r-1}}$的最低 l_k 个坐标全部置为 0,所得到的向量记为 $\boldsymbol{M}$。向量 $\boldsymbol{\beta}_s$ 与 $\boldsymbol{\beta}_t$ 的第 $l_k+1,l_k+2,\cdots,n-1$ 位的坐标与 $\boldsymbol{M}$ 在这些位的坐标完全相同。令

$$\boldsymbol{\eta}=\boldsymbol{\beta}_s+\boldsymbol{M},\ \boldsymbol{\xi}=\boldsymbol{\beta}_t+\boldsymbol{M}。$$

由引理 1 基(8)的性质可知,向量 $\boldsymbol{\beta}_s$ 和 $\boldsymbol{\beta}_t$ 的标号分别等于向量 $\boldsymbol{\eta}$ 和 $\boldsymbol{\xi}$ 的标号加上整数 M。

向量 $\boldsymbol{\eta}$ 的第 $l_k,l_k+1,\cdots,n-1$ 位的坐标全为 0,因此,向量 $\boldsymbol{\eta}$ 的字典序号为 $<2^{l_k}$。而向量 $\boldsymbol{\xi}$ 的第 l_k 位坐标等于 1,因此,$\boldsymbol{\xi}$ 的字典序号 $\geqslant 2^{l_k}$,从而 $\boldsymbol{\beta}_s$ 的字典编号小于 $\boldsymbol{\beta}_t$ 的字典编号,结论得证。

下面的例子解释了整个证明的过程,在例 3 中,用不带前缀 $0x$ 的十六进制表达式表示向量空间中的向量,例如 27 的二进制表示为 $1+2^1+2^2+0\cdot 2^3+0\cdot 2^4+2^5$,因此,27 表示向量(1,1,1,0,0,1)。

例 3　假定向量空间的维数 $n=6$,令 B 为由 $\boldsymbol{\alpha}_1=3$, $\boldsymbol{\alpha}_2=0e$, $\boldsymbol{\alpha}_3=27$ 生成的子空间。按照向量的字典顺序列出 B 中的 8 个向量如下:

$$B=\{00,\ 03,\ 0d,\ 0e,\ 24,\ 27,\ 29,\ 2a\}。\tag{9}$$

取 $V_0=\{00\}$。

第 0 步:集合 $B\backslash V_0$ 中,向量 03 的最高权位最小,即 $l_0=l(03)=1$。则令 $\boldsymbol{\beta}_{2^0}=03$ 并构造集合

$$U_1=\{\boldsymbol{\beta}_{2^0}+\boldsymbol{\beta}\mid\boldsymbol{\beta}\in V_0\}=\{03\},$$

再构造集合 $V_1=V_0\cup U_1=\{00,03\}$。

第 1 步:集合 $B\backslash V_1=\{0d,\ 0e,\ 24,\ 27,\ 29,\ 2a\}$。在这个集合中,向量 $0d$ 的最大权位 $l(0d)=3$ 是最小的,即 $l_1=3$。令 $\boldsymbol{\beta}_{2^1}=0d$ 并构造集合

$$U_2=\{\boldsymbol{\beta}_{2^1}+\boldsymbol{\beta}\mid\boldsymbol{\beta}\in V_1\}=\{0d,0e\},$$

再构造集合 $V_2=V_1\cup U_2=\{00,03,0d,0e\}$。

第 2 步:集合 $B\backslash V_2=\{24,\ 27,\ 29,\ 2a\}$。在这个集合中,向量 24 的最大权位 $l(24)=5$ 是最小的,即 $l_2=5$。令 $\boldsymbol{\beta}_{2^2}=24$,并构造集合

$$U_3=\{\boldsymbol{\beta}_{2^2}+\boldsymbol{\beta}\mid\boldsymbol{\beta}\in V_2\}=\{24,27,29,2a\},$$

再构造集合 $V_3=V_2\cup U_3=B$。

上面的过程,构造出子空间 B 的一组特殊基$\{\boldsymbol{\beta}_{2^0}=03,\boldsymbol{\beta}_{2^1}=0d,\boldsymbol{\beta}_{2^2}=24\}$,用坐标的形式写出这组基如下:

$$\boldsymbol{\beta}_{2^0}=(1,1,0,0,0,0),$$
$$\boldsymbol{\beta}_{2^1}=(1,0,1,1,0,0),$$
$$\boldsymbol{\beta}_{2^2}=(0,0,1,0,0,1)。$$

由此可以明显地看出,引理 1 的结论是成立的,即向量 $\boldsymbol{\beta}_{2^2}$的第 $l_0=1$、第 $l_2=3$ 处的坐标全为 0;向量 $\boldsymbol{\beta}_{2^1}$的第 $l_0=1$ 处的坐标为 0。

综上所述,建立从子空间 B 到向量空间 F_2^r 上的同构映射:

$$\varphi:F_2^r\to B,$$
$$\boldsymbol{i}=(i_0,i_1,\cdots,i_{r-1})\mapsto\boldsymbol{\beta}_i。$$

假定矩阵 $\boldsymbol{M}$ 是从 n 阶哈德玛矩阵 $\boldsymbol{H}_n$ 中依据子空间 B 中的地址选择 2^r 行所得到的子矩阵,则矩阵 $\boldsymbol{M}$ 的第 i 行第 j 列处的元素定义为 $m_{i,j}=(-1)^{\boldsymbol{\beta}_i\cdot j}$。由此定义向量空间 F_2^r 上的函数如下:对任意固定的 $\boldsymbol{j}\in F_2^n$ 以及任意的 $\boldsymbol{i}\in F_2^r$,函数

$$f_j(i)=m_{ij}=(-1)^{\boldsymbol{\beta}_i\cdot j}=(-1)^{\varphi(i)\cdot j}。\tag{10}$$

由于 φ 是同构映射,保持向量空间中的加法运算,而内积是双线性映射,也保持向量空间中的加法运算,因此,公式(10)定义了向量空间 F_2^r 上的线性函数,即矩阵 $\boldsymbol{M}$ 的每一列都是向量空间 F_2^r 上的线性函数,r 维向量空间 F_2^r 上共有 2^r 个线性函数。

最后证明 F_2^r 上每一个线性函数都在矩阵 $\boldsymbol{M}$ 中某一列中出现,而且恰好出现 2^{n-r}次。

将基(8)的向量当作行,构造一个秩为 r 的 $r\times n$ 矩阵 $\boldsymbol{C}$。利用矩阵 $\boldsymbol{C}$ 构造一个从向量空间 F_2^n 到向量空间 F_2^r 的映射如下:

$$\psi:\ F_2^n\rightarrow F_2^r,$$
$$\boldsymbol{j}\mapsto \boldsymbol{Cj},$$

其中,$\boldsymbol{Cj}$ 为矩阵与向量的普通乘法。矩阵 $\boldsymbol{C}$ 的秩为 r,因此,ψ 是满同态,它的核

$$Ker(\psi)=\{\boldsymbol{j}\in F_2^n \mid \boldsymbol{Cj}=0\}$$

是 $s=n-r$ 维的向量子空间,即向量空间 B 的零化子空间,记为 V。于是向量空间 F_2^n 可以分解成 2^r 个互不相交的陪集的并:

$$\boldsymbol{j}_k+V,\ k=0,1,2,\cdots,2^r-1。$$

当 $\boldsymbol{j}$ 取自某个陪集 $\boldsymbol{j}_k+V$, 如果令

$$\boldsymbol{Cj}_k=(a_0,a_1,\cdots,a_{r-1})^{\mathrm{T}},$$

则有 $\boldsymbol{Cj}=(a_0,a_1,\cdots,a_{r-1})^{\mathrm{T}}$。假定由第 $\boldsymbol{j}$ 列诱导的 $f_j(\boldsymbol{x})=l_0x_0+l_1x_1+\cdots+l_{r-1}x_{r-1}$,由基(8)的选择,以及内积的定义可知,对每一个 $k=0,1,2,\cdots,r-1$ 都有

$$\boldsymbol{l}_k=\boldsymbol{\beta}_{2^k}\cdot\boldsymbol{j}=a_k,$$

即在矩阵 $\boldsymbol{M}$ 中,由陪集 $\boldsymbol{j}_k+V$ 中的向量 $\boldsymbol{j}$ 所决定的列,对应于同一个线性函数

$$a_0x_0+a_1x_1+\cdots+a_{r-1}x_{r-1},$$

因此,所有的 r 元线性函数作为矩阵 $\boldsymbol{M}$ 的列全部出现,而且每一个线性函数都恰好重复出现 2^s 次。定理得证。