

Bent函数的构造

董军武

广州大学数学与信息科学学院, 广东 广州

收稿日期: 2026年8月25日; 录用日期: 2026年9月27日; 发布日期: 2026年10月14日

摘 要

Bent函数是非线性度达到最高的一类具有偶数个变量的布尔函数。一个熟知的结果是: f 是 $n = 2k$ 元 Bent 函数的充分必要条件是 f 由两个谱支撑互不相交的 $2k - 1$ 元半 Bent 函数的级联而成。提出一个方法: 用 2^{k-1} 个标号互不相同的仿射函数, 沿子空间级联, 可得到 $2k - 1$ 元半 Bent 函数, 从而可以构造 $2k$ 元 Bent 函数。并证明: 当 $k = 1, 2$ 时, 用这种方法可以得到所有的 $n = 2, 4$ 元 Bent 函数。

关键词

Bent函数, 半Bent函数, 仿射函数, 沿子空间级联, 谱支撑

The Construction of Bent Functions

Junwu Dong

School of Mathematics and Information Sciences, Guangzhou University, Guangzhou Guangdong

Received: August 25, 2026; accepted: September 27, 2026; published: October 14, 2026

Abstract

Bent functions are a class of Boolean functions with even number of variables that have the highest degree of nonlinearity. A well-known result is that the sufficient and necessary condition for f to be a Bent function with $n = 2k$ variables is that f is a concatenation of two semi Bent functions with $2k - 1$ variables whose spectral support are disjoint. A method is proposed: by concatenating 2^{k-1} affine functions with different labels along a given subspace, we can construct a semi Bent function with $2k - 1$ variables, and Bent functions with $2k$ variables can be obtained accordingly. We prove that: when $k = 1, 2$, all the Bent functions with 2 or 4 variables can be obtained in this way.

Keywords

Bent Function, Semi Bent Function, Affine Function, Concatenation along Subspace, Spectral Support



1. 引言

Bent 函数是非线性度达到最高的一类具有偶数个变量的布尔函数, 具有非常优良的密码学性质, 从而在密码模块中有着重要的应用。Bent 函数的性质、构造与计数一直吸引着无数的专家学者。

很多学者对 Bent 函数的构造和性质做了研究[1]-[10], 其中[1]给出 $2k$ 元 Bent 函数的代数次数不超过 k , 并给出了计算所有 6 元 Bent 函数的方法, 但是文中并没有给出明确的结果。文献[9]中, 利用布尔函数谱值在子空间的上分布规律, 通过计算机搜索计算出 6 元 Bent 函数的个数为 $5\,425\,430\,528$ 。文献[10]通过 50 台计算机历时三个月, 终于计算出 8 元 Bent 函数的个数为 $9927\,0589\,2659\,3437\,0305\,7858\,6124\,2880$ 。这是目前最好的结果, 对于 10 元以上的 Bent 函数, 人们不知道到底有多少。

文献[8]中证明了一个定理: f 是 $2k$ 元 Bent 函数当且仅当 f 是由两个谱支撑互不相交的 $2k-1$ 元半 Bent 函数的级联。基于这个结果, 本文考虑将 2^{k-1} 个 k 元仿射函数沿 F_2^{2k-1} 的任一 k 维线性子空间级联。如果选择的仿射函数的标号互不相同, 则可以构造一批 $2k-1$ 元半 Bent 函数, 并能方便地计算出它们的谱支撑, 从而可以构造出一批 $2k$ 元 Bent 函数。进一步证明: 用这种方式可以构造出全部的 $n=2$ 或者 4 元 Bent 函数。

2. 半 Bent 函数

先引入 Bent 函数的定义:

定义 1. 假定 f 是一个 n 元布尔函数, 如果对任意的 $\lambda \in F_2^n$, f 在 λ 处的 Walsh 谱值都满足 $|\hat{f}(\lambda)| = 2^{\frac{n}{2}}$, 则称 f 是 Bent 函数。

熟知的事实是: n 元 Bent 函数存在的充分条件是 n 为偶数。

假定 f 是 $n=2k$ 元布尔函数, 总可以把 f 看作两个 $n-1$ 元布尔函数 g_1 与 g_2 的级联, 即 $f = g_1 \parallel g_2$ 。这时对任意的 $u \in F_2^{n-1}$, 有

$$g_1(u) = f(u, 0), \quad g_2(u) = f(u, 1).$$

由蝶形算法可知

$$\hat{f}(u, 0) = \hat{g}_1(u) + \hat{g}_2(u), \quad \hat{f}(u, 1) = \hat{g}_1(u) - \hat{g}_2(u) \quad (1)$$

从而有

$$\hat{g}_1(u) = \frac{1}{2}(\hat{f}(u, 0) + \hat{f}(u, 1)), \quad \hat{g}_2(u) = \frac{1}{2}(\hat{f}(u, 0) - \hat{f}(u, 1)) \quad (2)$$

如果 f 是 Bent 函数, 对任意的 $u \in F_2^{n-1}$ 都有 $\hat{f}(u, 0), \hat{f}(u, 1) \in \{2^k, -2^k\}$, 因此对任意的 $u \in F_2^{n-1}$, 都有 $\hat{g}_1(u), \hat{g}_2(u) \in \{2^k, 0, -2^k\}$ 。为此引入半 Bent 函数的定义:

定义 2. 假定 $m=2k-1$ 为奇数, g 是 m 元布尔函数, 如果对任意的 $u \in F_2^m$, g 在 u 处的 Walsh 谱值都满足 $\hat{g}(u) = 2^{\frac{n}{2}}, 0, -2^{\frac{n}{2}}$, 则称 g 是半 Bent 函数。

定义 3. 假定 n 是任一正整数, f 是 n 元布尔函数, 定义 f 的 Walsh 谱支撑集合(简称为谱支撑)为

$$\text{supp}(\hat{f}) = \{\lambda \in F_2^n \mid \hat{f}(\lambda) \neq 0\}.$$

假定 g 是 $m = 2k - 1$ 元半 Bent 函数, 利用 Parseval 恒等式可知

$$\sum_{u \in F_2^m} \hat{g}^2(u) = 2^{2m} = 2^{4k-2} = |\text{supp}(\hat{f})| \cdot 2^{2k}$$

因此 $|\text{supp}(\hat{g})| = 2^{2k-2} = 2^{m-1}$ 。也就是说每一个 $m = 2k - 1$ 元半 Bent 函数 g , 它的谱支撑集合恰好包含地址空间一半的向量。

定义 4. 假定 g_1 与 g_2 是两个半 Bent 函数, 如果它们的谱支撑集合不相交, 即

$$\text{supp}(\hat{g}_1) \cap \text{supp}(\hat{g}_2) = \emptyset,$$

则称这两个半 Bent 函数不相交。

下面的定理 1 给出 $2k$ 元 Bent 函数与 $2k - 1$ 元半 Bent 函数的关系:

定理 1. 假定 $n = 2k$ 元布尔函数 f 是两个 $n - 1$ 元布尔函数 g_1 与 g_2 的级联, 则 f 是 Bent 函数的充分必要条件是 g_1 与 g_2 是不相交的 $2k - 1$ 元半 Bent 函数。

定理 1 的证明可参阅文献[8]。

根据定理 1, 为了计算 $n = 2k$ 元 Bent 函数的个数, 需要做两步: 第一步, 计算出所有的 $2k - 1$ 元半 Bent 函数。第二步, 对每一个 $2k - 1$ 元半 Bent 函数, 统计有多少个 $2k - 1$ 元半 Bent 函数与之不相交。将这些个数加起来, 就是 $n = 2k$ 元 Bent 函数的个数。

假定 g 是 $m = 2k - 1$ 元半 Bent 函数, 则 g 的谱支撑中包含 2^{m-1} 个元素。如果 g 的谱支撑集合恰好是 F_2^m 的一个 $m - 1$ 维向量空间或者是 F_2^m 的某个 $m - 1$ 维向量空间的补集, 则称 g 是第一类半 Bent 函数。否则称 g 为第二类半 Bent 函数。

3. 第一类半 Bent 函数的构造

本节约定 $m = 2k - 1$ 为奇数, $k \geq 1$ 是正整数。下面的定理 2 表明, 可以通过两个 $2k - 2$ 元 Bent 函数级联, 来构造 m 元半 Bent 函数:

定理 2. 如果 g_1, g_2 是两个 $m - 1 = 2k - 2$ 元 Bent 函数, 则它们的级联 $f = g_1 \parallel g_2$ 就是一个 m 元半 Bent 函数。

证明: 由于 g_1, g_2 是 $2k - 2$ 元 Bent 函数, 因此对任意的 $v \in F_2^{2k-2}$, 都有

$$\hat{g}_1(v) = \pm 2^{k-1}, \hat{g}_2(v) = \pm 2^{k-1}.$$

利用公式(1)可知, 对任意的 $v \in F_2^{2k-2}$ 有

$$\hat{f}(v, 0) = 0, \pm 2^k, \hat{f}(v, 1) = 0, \pm 2^k.$$

即 f 是 m 元半 Bent 函数。

下面构造第一类 m 元半 Bent 函数: 假定 g_1 是任意一个 $m - 1$ 元 Bent 函数, 取 $g_2 = g_1 + 1$, 即 g_2 的真值表为 g_1 真值表的取反(0 变为 1, 1 变为 0), 则 g_2 也是 $m - 1$ 元 Bent 函数。利用定理 2 可知 $f = g_1 \parallel g_2$ 是 m 元半 Bent 函数。容易验证, 对任意的 $v \in F_2^{m-1}$, 有 $\hat{g}_2(v) = -\hat{g}_1(v)$ 。由公式(1)可知 m 元半 Bent 函数 f 的谱支撑集合恰好为地址空间 F_2^m 的 $m - 1$ 维向量空间 F_2^{m-1} 的补集, 这样构造的半 Bent 函数是第一类半 Bent 函数。

假定共有 N_{k-1} 个 $2k - 2$ 元 Bent 函数, 那么按照上面的方法可以构造出 N_{k-1} 个第一类 m 元半 Bent 函数, 并且它们的谱支撑集合都恰好为向量空间 F_2^{m-1} 的补集。

另一方面, 如果 f 是一个 m 元半 Bent 函数, 而且它的谱支撑集合 $\text{supp}(\hat{f})$ 为 F_2^{m-1} 的补集。将 f 看成两个 $m-1$ 元布尔函数的级联 $f = g_1 \parallel g_2$, 利用公式(2)可知对任意的 $v \in F_2^{m-1}$ 都有

$$\hat{g}_2(v) = -\hat{g}_1(v)$$

成立, 即 $g_2 = g_1 + 1$, 也就是说 f 一定由上面的方式得到。

类似地, 取 g_1 为任一 $m-1=2k-2$ 元 Bent 函数, 取 $g_2 = g_1$, 再令 $f = g_1 \parallel g_2$, 则 f 是 m 元半 Bent 函数, 而且它的谱支撑集合恰好为 F_2^{m-1} , 即这样构造的布尔函数也是第一类 m 元半 Bent 函数。

假定 B 为 F_2^m 的任一 $m-1$ 维向量空间, 取线性变换 A (即 $m-1$ 阶可逆 0-1 矩阵), 该线性变换将子空间 F_2^{m-1} 变为 B 。假定这个线性变换的定义如下:

$$\begin{aligned} \varphi: F_2^m &\rightarrow F_2^m \\ u &\mapsto u^T A \end{aligned}$$

其中 $u^T = (u_1, u_2, \dots, u_m)$ 表示行向量。由于 A 是可逆矩阵, 因此该线性变换把 F_2^{m-1} 的补集变为 B 的补集。

假定 f 是一个 m 元布尔函数, 利用矩阵 A 定义另外一个布尔函数 $h(x) = f(Ax)$ 。利用 Walsh 谱的定义容易验证: 对任意的 $u \in F_2^m$ 都有

$$\hat{h}(u^T A) = \hat{f}(u). \quad (3)$$

如果 f 是 m 元第一类半 Bent 函数, 并且谱支撑集合 $\text{supp}(\hat{f}) = F_2^{m-1}$ 。 B 是 F_2^m 的任一 $m-1$ 维向量空间, A 的定义如上, 利用公式(3)可知由 $h(x) = f(Ax)$ 定义的布尔函数, 其谱支撑集合恰好为 B , 即 h 也是第一类半 Bent 函数。反之亦然, 即如果 h 是 m 元第一类半 Bent 函数, 并且 $\text{supp}(\hat{h}) = B$, 利用 $h(x) = f(Ax)$ 构造布尔函数 f , 则 f 是 m 元第一类半 Bent 函数, 而且其谱支撑集合 $\text{WZ}(\hat{f}) = F_2^{m-1}$ 。

如果 f 是 m 元第一类半 Bent 函数, 并且它的谱支撑集合 $\text{supp}(\hat{f})$ 是 F_2^{m-1} 的补集, 则由 $h(x) = f(Ax)$ 定义的布尔函数也是 m 元第一类半 Bent 函数, 并且其谱支撑集合恰好为子空间 B 的补集。

熟知, m 维向量空间共有 $2^m - 1$ 个 $m-1$ 维向量空间。因此得到下面的结果: 为了方便, 我们约定, 把谱支撑集合相同的 m 元半 Bent 函数看作一类。

定理 3. 假定 $m = 2k-1$ 是奇数。如果所有 $m-1 = 2k-2$ 元 Bent 函数的个数为 N_{k-1} 。则所有的 m 元第一类半 Bent 函数共有 $2(2^m - 1)$ 类, 每类中恰好有 N_{k-1} 个函数, 共计 $2(2^m - 1)N_{k-1}$ 个 m 元第一类半 Bent 函数。

利用定理 1, 可以得到如下的构造 $2k$ 元 Bent 函数的结果:

定理 4. 假定能构造出 N_{k-1} 个 $2k-2$ 元 Bent 函数, 则可以构造出

$$N_k = 2(2^{2k-1} - 1)N_{k-1}^2 \quad (4)$$

个 $2k$ 元 Bent 函数。

证明: 如果能构造出 N_{k-1} 个 $2k-2$ 元 Bent 函数。由定理 4, 利用这些 Bent 函数可以构造出 $2(2^{2k-1} - 1)N_{k-1}$ 个 $2k-1$ 元半 Bent 函数, 这些半 Bent 函数, 按照谱支撑集合是否相等可分成若干类, 每类中恰好有 N_{k-1} 个函数。从而每个半 Bent 函数都有 N_{k-1} 个半 Bent 函数与之不相交, 由定理 1 可知, 可以构造出 $N_k = 2(2^{2k-1} - 1)N_{k-1}^2$ 个 $2k$ 元 Bent 函数。

4. 仿射函数沿子空间的级联

本节假定 $m = 2k+1$ 为奇数, 介绍一种构造 $m = 2k+1$ 元半 Bent 函数的方法: 仿射函数沿向量空间

级联。先介绍典范级联。共有 2^{k+2} 个 $k+1$ 元仿射函数。对于仿射

$$a_1x_1 + a_2x_2 + \cdots + a_{k+1}x_{k+1} + b$$

定义其标号为由诸变量的系数(不包含常数项 b)所构成的长为 $k+1$ 的 0-1 向量, 所有 $k+1$ 元仿射函数按照标号是否相同, 可以分成 2^{k+1} 组, 每组中恰好有两个仿射函数。所有这些标号恰好构成向量空间 F_2^{k+1} 。

任选 2^k 个 $k+1$ 元仿射函数 $l_1, l_2, \dots, l_{2^k}$, 使得它们的标号两两不同。将它们的真值表从左到右依次级联, 得到一个长为 $2^{2k+1} = 2^m$ 的 0-1 串, 即得到一个 m 元布尔函数的真值表。称这个 m 元布尔函数 f 为 $l_1, l_2, \dots, l_{2^k}$ 的典范级联, 记为 $f = l_1 \parallel l_2 \parallel \cdots \parallel l_{2^k}$ 。

下面计算 f 的 Walsh 谱, 并证明 f 是一个 $m = 2k+1$ 元半 Bent 函数。

$k+1$ 元仿射函数 l 的 Walsh 谱中只有地址等于 l 的标号处谱值为 $\pm 2^{k+1}$, 其余地址处的谱值全为零。用蝶化算法计算 f 的 Walsh 谱, 就是从 f 的极化向量出发, 做 $m = 2k+1$ 轮蝶化算法。当做到 $k+1$ 轮时, 中间结果恰好为所选择的 2^k 个 $k+1$ 元仿射函数的 Walsh 谱, 即每一段中只有一个地址处的谱值为 $\pm 2^{k+1}$, 其余地址处的谱值全为零。由于这些仿射函数的标号互不相同, 所以每一段中, 非零谱值的地址所处的相对位置也是两两不同的。在后面的每一轮蝶化过程中, Walsh 谱值的中间结果全为零或者 $\pm 2^{k+1}$, 并且每一轮过后, 非零的 Walsh 谱值刚好增加一半。当做完 $m = 2k+1$ 轮蝶化算法之后, 得到 f 的 Walsh 谱中, 恰好 2^{m-1} 个地址具有谱值 $\pm 2^{k+1}$, 其余 2^{m-1} 个地址处的谱值均为零。这就证明 f 是一个 $m = 2k+1$ 元半 Bent 函数。

接着计算 f 的谱支撑集合: 令 S 表示所选择的 2^k 个仿射函数标号所构成的集合, 即

$$S = \{\lambda_1, \lambda_2, \dots, \lambda_{2^k}\}$$

再考虑向量的集合

$$T = \{t_{k+2}e_{k+2} + \cdots + t_me_m \mid t_j = 0, 1\},$$

其中 e_j 第 j 个分量为 1, 其余分量全为 0 的单位向量。根据蝶化算法的过程可知

$$\sup(\hat{f}) = \{\alpha + \beta \mid \alpha \in S, \beta \in T\}. \quad (5)$$

例 1. 取 $k = 2$, 则 $m = 2k+1 = 5$ 。共有 16 个 $k+1 = 3$ 元仿射函数, 它们的标号共有 8 个, 构成向量空间 $F_2^3 = \{0, 1, 2, 3, 4, 5, 6, 7\}$ (本例中用 0-1 向量代表的十进制表示向量, 例如 $(0, 0, 0, 1, 0)$ 用 8 表示等)。取 4 个互不相同的标号: 0, 2, 6, 7。对应的线性函数真值表分别为 $l_0: 00000000$, $l_2: 00110011$, $l_6: 00111100$, $l_7: 01101001$ 。这四个线性函数典范级联得到的 $m = 5$ 元布尔函数 f 的真值表为: 00000000 00110011 00111100 01101001。于是集合 $S = \{0, 2, 6, 7\}$, $T = \{0, 8, 16, 24\}$ 。布尔函数 f 的 Walsh 谱支撑为

$$\text{supp}(\hat{f}) = S + T = \{0, 2, 6, 7, 8, 10, 14, 15, 16, 18, 22, 23, 24, 26, 30, 31\}。$$

事实上, 用蝶化算法计算 f 的 Walsh 谱时第 3 步的中间结果为: 80000000 00800000 00000080 00000008, 支撑集合为 $\{0, 10, 23, 31\}$ 。

蝶化算法第 4 步的中间结果为: 80800000 80-800000 00000088 0000008-8, 支撑集合为 $\{0, 10, 23, 31, 2, 8, 22, 30\}$ 。

蝶化算法第 5 步的中间结果为: 80800088 80-80008-8 808000-8-8 80-8000-88, 支撑集合为 $\{0, 10, 23, 2, 8, 22, 30, 6, 7, 14, 15, 16, 18, 24, 26\}$ 。排序后就是集合 $S + T$ 。

选定 2^k 个标号之后(注意这些标号两两不同), 每个仿射函数有两种选择方法, 不同的仿射函数只影响到非零 Walsh 谱值的符号, 并不影响非零 Walsh 谱值的地址。将这 2^k 个仿射函数典范级联时, 它们不同的排列顺序有 $2^k!$ 个, 不同的排列顺序, 经过 m 轮蝶化算法之后, 谱支撑集合完全相同。这样构造的 m

元半 Bent 函数具有相同的谱支撑集合, 称为仿射级联类, 每类中有 $2^{2^k} \cdot (2^k)!$ 个函数。

下面介绍沿子空间级联的方法: 假定 B 是 F_2^{2k+1} 的 $k+1$ 维向量量子空间, 考虑商空间 $V = F_2^{2k+1} / B$ 。给定商集中, 每个陪集的代表元素选为该陪集中字典排序最小的元素。每个陪集中均包含 2^{k+1} 个向量, 将陪集中的向量按照字典顺序排列。将 2^k 个陪集按照代表元的字典顺序排列。然后将所选择的 2^k 个仿射函数的真值表, 按照陪集代表元的字典顺序, 依次赋给每个陪集中的地址向量, 得到一个 $m = 2k+1$ 元布尔函数 h , 称这个布尔函数 h 为仿射函数 $\{l_1, l_2, \dots, l_{2^k}\}$ 沿子空间 B 的级联。前面讲的典范级联, 就是沿特殊的子空间 $B = F_2^{k+1}$ 的级联。

例 2. (仿射函数沿子空间级联的例子) 取 $k=1$, 则 $m=3$ 。则 $F_2^m = \{0, 1, 2, 3, 4, 5, 6, 7\}$ 。取 $k+1=2$ 维子空间 $B = \{0, 2, 5, 7\}$, 则 F_2^m 共有两个关于 B 的陪集: $B_0 = \{0, 2, 5, 7\}$, $B_1 = \{1, 3, 4, 6\}$ 。假定两个编号分别为 1 与 2 的 2 元线性函数的真值表为: $l_1: 0101$, $l_2: 0011$ 。而 3 元布尔函数 f 是 l_1, l_2 沿子空间 B 的级联, 则当 $x \in B_0$ 时, $f(x)$ 取 l_1 的相应函数值。当 $x \in B_1$ 时, $f(x)$ 取 l_2 的相应函数值。于是 f 的真值表为: 00101011 (见表 1)。

Table 1. The concatenation of affine functions along with subspace

表 1. 仿射函数沿子空间的级联

地址	0	1	2	3	4	5	6	7
l_1	0		1			0		1
l_2		0		0	1		1	
f	0	0	1	0	1	0	1	1

令 $f = l_1 \parallel l_2 \parallel \dots \parallel l_{2^k}$ 为典范级联。假定子空间 B 中的地址如下:

$$B = \{0, \beta_1, \beta_2, \dots, \beta_{2^{k+1}-1}\},$$

假定商集的代表元(取陪集中字典顺序最小者作为代表元)按照字典顺序排列如下:

$$F_2^{2k+1} / B = \{0 + B, \gamma_1 + B, \gamma_2 + B, \dots, \gamma_{2^k-1} + B\}.$$

选择 B 的一组特殊基 $\{\beta_{2^0}, \beta_{2^1}, \dots, \beta_{2^k}\}$, 选择商集的一组特殊基 $\{\gamma_{2^0}, \gamma_{2^1}, \dots, \gamma_{2^k-1}\}$, 以这些向量为列向量, 构造一个 $m = 2k+1$ 阶矩阵 A 如下:

$$A = (\beta_{2^0}, \beta_{2^1}, \dots, \beta_{2^k}, \gamma_{2^0}, \gamma_{2^1}, \dots, \gamma_{2^k-1}).$$

由于这些向量恰好构造向量空间 F_2^m 的一组基, 因此 A 是一个可逆矩阵。假定由仿射函数 $\{l_1, l_2, \dots, l_{2^k}\}$ 沿子空间 B 的级联得到的布尔函数为 h , 则有

$$h(Ax) = f(x). \quad (6)$$

因此 h 的谱支撑集合 $\text{supp}(\hat{h})$ 与 f 的谱支撑集合 $\text{supp}(\hat{f})$ 满足如下关系

$$\text{supp}(\hat{f}) = \{u^T A \mid u \in \text{supp}(\hat{h})\}.$$

由于 f 是 m 元半 Bent 函数, 故 h 也是 m 元半 Bent 函数。当选择不同标号的仿射函数与不同的向量量子空间做级联时, 产生的布尔函数会不会重合? 当 $k=1$ 时, 有下面的结果, 在附录中证明:

定理 5. 假定 l_1, l_2 是两个具有不同标号的 r 元仿射函数, B 是向量空间 F_2^{r+1} 的任一 r 维向量量子空间, f 是 l_1, l_2 沿子空间 B 级联产生的布尔函数。则存在另外两组具有不同标号的仿射函数, 以及 F_2^{r+1} 的另外

两个不同的子空间, 级联之后仍得到布尔函数 f 。

证明了 $k=2$ 的形, 即下面的定理 6:

定理 6. 假定 m 是大于 3 的正整数, 任取 4 具有不同标号的 $m-2$ 元仿射函数, 沿 F_2^m 的任一 $m-2$ 维子空间级联, 得到布尔函数 $F(x)$ 。

(1) 如果这 4 个标号构成二维向量空间, 或者某个二维向量空间的陪集, 则存在 15 个子空间, 使得 $F(x)$ 沿这些子空间的四个陪集析取出来的函数全是仿射函数。

(2) 如果这 4 个标号不构成二维向量空间, 也不构成某个二维向量空间的陪集, 则 $F(x)$ 只能沿这个子空间析取出 4 个仿射函数。

最后要说明一点: 由于仿射函数沿子空间 B 级联, 相当于从仿射函数的典范级联出发, 通过构造合适的 m 阶 0-1 可逆矩阵 A , 再由 $h(Ax) = f(x)$ 得到。要说明的是, 当 A 取遍所有的 m 阶 0-1 可逆矩阵时, 由 $h(Ax) = f(x)$ 构造不出新的布尔函数, 即构造出来的函数仍然由某些仿射函数沿合适的子空间级联。原因如下: 考虑矩阵 A 的列向量组, 它的前 $k+1$ 个向量生成一个 $k+1$ 维向量量子空间 B (顺序不一定是字典排序, 需要一个线性变换, 就可以变成字典顺序)。 A 的后 k 个向量生成的 k 维子空间, 与商集 F_2^{k+1} / B 中的陪集一一对应 (商集中的向量不一定是字典排序, 商空间也不一定是按照前面给定的顺序排序, 但是前者相当于把仿射函数用其它的仿射函数代替, 后者相当于把仿射函数做一个重新排序)。不管怎么说, 最后的结果相当于另外 2^k 个仿射函数沿子空间 B 的级联。

5. 第二类半 Bent 函数的构造

当 $k=1, 2$ 时, 从 2^{k+1} 个标号中任选 2^k 个两两不同的标号, 共有 $C_{2^{k+1}}^{2^k}$ 种方法, 因此利用仿射函数典范级联的方法可以构造出 $C_{2^{k+1}}^{2^k} \cdot 2^{2^k} \cdot (2^k)!$ 个 m 元半 Bent 函数。标号的每一种取法, 对于固定的 $k+1$ 维向量子空间, 能产生一类 m 元半 Bent 函数, 每类中有 $2^{2^k} \cdot (2^k)!$ 个函数。而向量空间 F_2^{k+1} 中 k 维向量量子空间的个数, 以及 k 维向量量子空间的补集的个数, 均为 $2^{k+1} - 1$ 。因此选定子空间 B 之后沿子空间 B 级联可得到

$$\left(C_{2^{k+1}}^{2^k} - 2(2^{k+1} - 1)\right) 2^{2^k} \cdot (2^k)!$$

个第二类 $m = 2k+1$ 元半 Bent 函数。一个熟知的事实: 向量空间 F_2^{2k+1} 中 $k+1$ 维向量量子空间的个数为:

$$\frac{(2^m - 2^0)(2^m - 2^1)(2^m - 2^2) \cdots (2^m - 2^k)}{(2^{k+1} - 2^0)(2^{k+1} - 2^1)(2^{k+1} - 2^2) \cdots (2^{k+1} - 2^k)} = \frac{\prod_{i=0}^k (2^{m-i} - 1)}{\prod_{i=0}^k (2^{k+1-i} - 1)}.$$

于是沿不同的 $k+1$ 维向量量子空间级联时, 产生的第二类 m 元半 Bent 函数的个数为

$$\frac{\prod_{i=0}^k (2^{m-i} - 1)}{\prod_{i=0}^k (2^{k+1-i} - 1)} \left(C_{2^{k+1}}^{2^k} - 2(2^{k+1} - 1)\right) 2^{2^k} \cdot (2^k)!.$$

6. 若干例子

例 3. 当 $k=1$ 时, 计算所有的 1 元半 Bent 函数。共有 4 个 1 元布尔函数, 利用 1 阶哈德玛矩阵计算它们的 Walsh 谱如下:

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 \\ 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \begin{pmatrix} 0 \\ 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} -1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ -2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} -1 \\ -1 \end{pmatrix} = \begin{pmatrix} -2 \\ 0 \end{pmatrix}.$$

由此可知，它们都是第一类的 1 元半 Bent 函数。由上面的计算可知，每一个 1 元半 Bent 函数都恰好有 2 两个不相交的 1 元半 Bent 函数，即如果将具有相同谱支撑或者谱零集合的 1 元半 Bent 函数看作一类，则每类中有 2 个 1 元半 Bent 函数，见表 2。

Table 2. All the semi bent functions with one variable

表 2. 所有 1 元半 Bent 函数信息

序号	半 Bent 函数	互补的半 Bent 函数
1	00	01, 10
2	01	00, 11
3	10	00, 11
4	11	01, 10

根据定理 1，可得到 $N_1 = 8$ 个 2 元 Bent 函数，这也是全部 2 元 Bent 函数，列举真值表如下：

0001 0010 0100 0111 1000 1011 1101 1110.

例 4. 当 $k=2$ 时，计算所有的 3 元半 Bent 函数与所有的 4 元 Bent 函数。

由于 2 元 Bent 函数共有 $N_1 = 8$ 个，由定理 3 知，第一类 3 元半 Bent 函数的个数为

$$2(2^3 - 1)N_1 = 112.$$

再由定理 4，可构造出 $112 \times 8 = 896$ 个 4 元 Bent 函数。下面证明，这些就是所有的 4 元 Bent 函数。先介绍一个引理(证明可参阅文献[9]):

引理. 假定 B 是 F_2^n 的 r 维向量子空间，令 V 是 B 的正交补空间，即

$$V = \{x \in F_2^n \mid \text{对任意的 } y \in F_2^n \text{ 都有 } x \cdot y = 0\}.$$

对任意的 n 元布尔函数 f ，记 $b = \sum_{x \in V} (-1)^{f(x)}$ ，则有

$$\sum_{\lambda \in B} \hat{f}(\lambda) = 2^r b.$$

其中 $b \in \{0, \pm 2, \pm 4, \pm 6, \dots, \pm 2^{n-r}\}$ 。

证明下面的结果：

定理 7. 不存在第二类 3 元半 Bent 函数。

证明：假定 f 是 3 元半 Bent 函数，为了讨论上的方便，考虑谱值为 0 的地址集合 $\{\lambda_0, \lambda_1, \lambda_2, \lambda_3\}$ 。注意到非退化的线性变换把向量子空间变为向量子空间，对任意的 3 阶可逆 0-1 矩阵 A ，令 $g(x) = f(Ax)$ ，则 f 是第一类的 3 元半 Bent 函数，当且仅当 g 是第一类的 3 元半 Bent 函数。总可以取合适的矩阵 A ，使得 $\hat{g}(0) = 0$ ，因此不妨设 $\lambda_0 = 0$ 。

集合 $B = \{0, \lambda_1, \lambda_2, \lambda_1 + \lambda_2\}$ 为 3 维向量空间 F_2^3 的一个 $r = 2$ 维子空间。在引理中取 $n = 3$ ， $r = 2$ 可得

$$\sum_{\lambda \in B} \hat{f}(\lambda) = 2^2 b, \quad b \in \{0, \pm 2\}.$$

即

$$\hat{f}(0) + \hat{f}(\lambda_1) + \hat{f}(\lambda_2) + \hat{f}(\lambda_1 + \lambda_2) = \hat{f}(\lambda_1 + \lambda_2) \in \{0, \pm 8\}.$$

而 f 是 3 元半 Bent 函数， $\hat{f}(\lambda_1 + \lambda_2)$ 只能是 0, ± 4 ，因此 $\hat{f}(\lambda_1 + \lambda_2) = 0$ ，即 f 的谱值为 0 的地址集合恰好为 2 维向量子空间，因此 f 是第一类 3 元半 Bent 函数，证毕。

由定理 7, 以及前面的计算可知, 所有 4 元 Bent 函数的个数为 $N_2 = 896$ 。

这个例子的最后, 我们来说明所有的这些第一类 3 元半 Bent 函数均可由仿射函数沿子空间的级联得到: 用两个 2 元仿射函数沿子空间级联可以得到 3 元半 Bent 函数。2 元线性函数的标号共有 4 个, 任取两个标号不同的仿射函数, 共有 $C_4^2 = 6$ 种取法。选定 F_2^3 的一个 2 维向量空间后, 可产生一类 3 元半 Bent 函数, 这一类 3 元半 Bent 函数具有完全相同的谱支撑集合与谱零集合, 类中共有 $2 \times 2 \times 2 = 8$ 个函数。 F_2^3 中共有 7 个 2 维子空间, 已经证明 3 元半 Bent 函数一定是第一类的, 并将在附录中证明用两个仿射函数沿向量空间级联时, 所得到的每一个 3 元半 Bent 函数都恰好重复 3 次, 因此用仿射函数沿不同子空间级联共可以产生 $(6 \times 7 \times 8)/3 = 112$ 个 3 元半 Bent 函数, 即全部的 3 元半 Bent 函数都可由仿射函数沿子空间级联的方式产生。

7. 结束语

本文用仿射函数沿向量空间级联的方法构造出一批奇数元半 Bent 函数, 从而构造出一批偶数元 Bent 函数。当 $k=1,2$ 时, 用这种方法可以构造出所有的 2 元及 4 元 Bent 函数。用仿射函数沿子空间级联来构造 Bent 函数, 是本文的一个创新点, 这个方法到底能走多远还需要进一步探索。

基金项目

广东省基础与应用基础研究基金(2026A1515011401)。

参考文献

- [1] Rothaus, O.S. (1976) On “Bent” Functions. *Journal of Combinatorial Theory, Series A*, **20**, 300-305. [https://doi.org/10.1016/0097-3165\(76\)90024-8](https://doi.org/10.1016/0097-3165(76)90024-8)
- [2] Carlet, C. (1991) A Transformation on Boolean Functions, Its Consequences on Some Problems Related to Reed-Muller Codes. In: Cohen, G. and Charpin, P., Eds., *EUROCODE '90*, Springer, 42-50. https://doi.org/10.1007/3-540-54303-1_116
- [3] Carlet, C. (1993) Partially-Bent Functions. *Designs, Codes and Cryptography*, **3**, 135-145. <https://doi.org/10.1007/bf01388412>
- [4] Carlet, C. and Guillot, P. (1996) A Characterization of Binary Bent Functions. *Journal of Combinatorial Theory, Series A*, **76**, 328-335. <https://doi.org/10.1006/jcta.1996.0110>
- [5] Carlet, C. (1994) Two New Classes of Bent Functions. In: Helleseth, T., Ed., *Advances in Cryptology—EUROCRYPT '93*, Springer, 77-101. https://doi.org/10.1007/3-540-48285-7_8
- [6] Dillon, J.F. (1974) Elementary Hadamard Difference Sets. Ph.D. Thesis, University of Maryland.
- [7] Hou, X. and Langevin, P. (1997) Results on Bent Functions. *Journal of Combinatorial Theory, Series A*, **80**, 232-246. <https://doi.org/10.1006/jcta.1997.2804>
- [8] 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.
- [9] 董军武, 王殊懿, 等. 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.
- [10] Langevin, P. and Leander, G. (2011) Counting All Bent Functions in Dimension Eight 9927058926593437030-5785861242880. *Designs, Codes and Cryptography*, **59**, 193-205. <https://doi.org/10.1007/s10623-010-9455-z>

附录

本附录来证明下面的定理：

定理 5. 假定 l_1, l_2 是两个具有不同标号的 k 元仿射函数， B 是向量空间 F_2^{k+1} 的任一 k 维量子空间， f 是 l_1, l_2 沿子空间 B 级联产生的布尔函数。则存在另外两组具有不同标号的仿射函数，以及 F_2^{k+1} 的另外两个不同的子空间，级联之后得到布尔函数 f 。

在证明之前先做一点准备工作：给子空间标号。向量空间 F_2^{k+1} 共有 $2^{k+1}-1$ 个 k 维量子空间，每一个 k 维量子空间 B ，一定存在 $k+1$ 元线性函数 $l(x)$ 使得

$$B = \{x \in F_2^{k+1} \mid l(x) = 0\}.$$

将线性函数 $l(x)$ 的标号定义为子空间 B 的标号， k 维量子空间的标号即是向量空间 F_2^{k+1} 中的向量。给定 F_2^{k+1} 的 k 维量子空间 B ，令 $\bar{B}$ 表示 B 在 F_2^{k+1} 中的补集，假定集合中的向量按照字典排序，

$$B = \{0, \beta_1, \beta_2, \dots, \beta_{2^k-1}\}, \quad \bar{B} = \{\gamma_0, \gamma_1, \gamma_2, \dots, \gamma_{2^k-1}\}$$

而 f 是由 l_1, l_2 沿子空间 B 级联得到的布尔函数，则有

$$f(x) = \begin{cases} l_1(j), & \text{如果 } x = \beta_j \in B, \\ l_2(j), & \text{如果 } x = \gamma_j \in \bar{B}. \end{cases}$$

注：在上面的定义中 β_j 以及 γ_j 中的 j 不是整数，而是整数 j 的二进制表达式所代表的长为 k 的 0-1 向量，当作 F_2^k 中的向量来看待。

定理 5 的证明： 分三种情况来证明。第一种情况：假定子空间 $B = F_2^k$ ，即 B 的标号为 $\bar{\omega}_0 = (0, 0, \dots, 0, 1) \in F_2^{k+1}$ ； l_1 的标号为 0，并且假定是零函数，即真值表是长为 2^k 的全 0 串。而 l_2 的标号为非零向量 $\omega_1 \in F_2^k$ ，并假定 l_2 是线性函数。则的 l_2 的真值表中，0 与 1 各占一半。布尔函数 f 是由 l_1, l_2 沿子空间 B 级联得到的，即典范级联。则

$$f(x) = \begin{cases} 0, & \text{如果 } x \in B, \\ l_2(j), & \text{如果 } x = \gamma_j \in \bar{B}. \end{cases}$$

考虑标号为 $\bar{\omega}_1 = (\omega_1, 0)$ (仿射函数 l_2 的标号 ω_1 是 k 维向量，而 F_2^{k+1} 中 k 维子空间的标号是 $k+1$ 维向量) 的 k 维子空间 B_1 ，该子空间将向量空间 F_2^{k+1} 被分成互不相交的两部分 B_1 与 $\bar{B}_1$ 。考虑标号为 $\bar{\omega}_1 = (\omega_1, 0)$ 的 $k+1$ 元线性函数 L_1 ，它是两个 l_2 的典范级联。由于我们对量子空间 B 的特殊选择，当 $x = \gamma_j \in \bar{B}$ 时， $L_1(x) = l_2(j)$ 。由于 L_1 在 B_1 上取值为 0，在 $\bar{B}_1$ 上取值为 1，因此当 $\beta_j \in B_1$ 时 $l_2(j) = 0$ ，当 $\beta_j \in \bar{B}_1$ 时 $l_2(j) = 1$ 。

假定 f 沿子空间提取出两个函数 B_1 ，分别为 f_1, f_2 。来证明 f_1, f_2 都是仿射函数，从而 f 是两个仿射函数 f_1, f_2 沿子空间级联而成。为了方便，定义四个集合

$$U_1 = B \cap B_1, \quad U_2 = \bar{B} \cap B_1, \quad U_3 = B \cap \bar{B}_1, \quad U_4 = \bar{B} \cap \bar{B}_1.$$

当 $x \in U_1$ 时，由于 $U_1 \subseteq B$ ，因此 $f_1(x) = l_1(x) = 0$ 。当 $x = \gamma_j \in U_2$ 时，由于 $U_2 \subseteq \bar{B}$ ，因此 $f_1(j) = l_2(j)$ ，另一方面， $U_2 \subseteq B_1$ ，而当 $\beta_j \in B_1$ 时 $l_2(j) = 0$ ，因此布尔函数 f_1 的真值表是长为 2^k 的全零串，是标号为零的仿射函数。

当 $x \in U_3$ 时，由于 $U_3 \subseteq B$ ，因此 $f_2(x) = l_1(x) = 0$ 。当 $x = \gamma_j \in U_4$ 时，由于 $U_4 \subseteq \bar{B}$ ，因此 $f_2(j) = l_2(j)$ 。另一方面， $U_4 \subseteq \bar{B}_1$ ，当 $\beta_j \in \bar{B}_1$ 时 $l_2(j) = 1$ ，即 $f_2(j) = 1$ 。因此布尔函数 f_1 的真值表是长为 2^{k-1} 的全 0 串

与长为 2^{k-1} 的全 1 串的级联, 当然是仿射函数, 标号为 $(0, 0, \dots, 0, 1)$ 。

考虑标号为 $\overline{\omega_2} = (\omega_1, 1) = \overline{\omega_1} + \overline{\omega_0}$ 的 k 维子空间 B_2 , 该子空间将向量空间 F_2^{k+1} 被分成互不相交的两部分 B_2 与 $\overline{B_2}$ 。考虑标号为 $\overline{\omega_2} = (\omega_1, 1)$ 的 $k+1$ 元线性函数 L_2 , 它是 l_2 与 l_2+1 典范级联。由于我们对向量量子空间 B 的特殊选择, 当 $x = \gamma_j \in \overline{B}$ 时, $L_2(x) = l_2(j) + 1$ 。因此 L_2 在 B_1 上取值为 0, 在 $\overline{B_2}$ 上取值为 1。从而当 $\beta_j \in B_2$ 时 $l_2(j) = 1$, 当 $\beta_j \in \overline{B_2}$ 时 $l_2(j) = 0$ 。

假定 f 沿子空间提取出两个函数 B_2 , 分别为 g_1, g_2 。来证明 g_1, g_2 都是仿射函数, 从而 f 是两个仿射函数 g_1, g_2 沿子空间级联而成。为了方便, 定义四个集合

$$V_1 = B \cap B_2, \quad V_2 = \overline{B} \cap B_2, \quad V_3 = B \cap \overline{B_2}, \quad V_4 = \overline{B} \cap \overline{B_2}.$$

当 $x \in V_1$ 时, 由于 $V_1 \subseteq B$, 因此 $g_1(x) = l_1(x) = 0$ 。当 $x = \gamma_j \in V_2$ 时, 由于 $V_2 \subseteq \overline{B}$, 因此 $g_1(j) = l_2(j)$, 另一方面, $V_2 \subseteq B_2$, 而且当 $\beta_j \in B_2$ 时 $l_2(j) = 1$, 因此 $g_1(j) = l_2(j) = 1$ 。因此布尔函数 f_1 的真值表是长为 2^{k-1} 的全 0 串与长为 2^{k-1} 的全 1 串的级联, 当然是仿射函数, 标号为 $(0, 0, \dots, 0, 1)$ 。

当 $x \in V_3$ 时, 由于 $V_3 \subseteq B$, 因此 $g_2(x) = l_1(x) = 0$ 。当 $x = \gamma_j \in V_4$ 时, 由于 $V_4 \subseteq \overline{B}$, 因此 $g_2(j) = l_2(j)$ 。另一方面, $V_4 \subseteq \overline{B_2}$, 而当 $\beta_j \in \overline{B_2}$ 时 $l_2(j) = 0$, 即 $g_2(j) = 0$ 。因此布尔函数 g_2 的真值表是长为 2^k 的全零串, 是标号为零的仿射函数。

对于 F_2^{k+1} 的其它 k 维子空间来说, 布尔函数 f 沿着这个子空间析取时, 得到的两个函数都不是零函数, 而且真值表中 1 的个数少于一半, 因此它们不可能是仿射函数。这就证明了 f 恰好由三组仿射函数沿合适的三个 k 维子空间级联而成。

同样的方法可以证明: 当子空间 $B = F_2^k$, l_1 的标号为 0, l_2 的标号为非零向量 $\omega_2 \in F_2^k$ 时, 结论成立 (根据 l_1, l_2 的四种情况, 逐一验证即可, 上面只验证了一种情况)。

第二种情况: 假定子空间 $B = F_2^k$, l_1 的标号不为零。构造辅助函数 $h(x) = l_1 \parallel l_2$, 考虑新的布尔函数 $g(x) = f(x) + h(x)$ 。则 $g(x)$ 满足第一种情况, 因此存在三组仿射函数沿合适的三个 k 维子空间级联可以得到 $g(x)$ 。由于仿射函数沿任意子空间析取出来的两个函数仍然是仿射函数, 因此对于这种情况定理的结论仍然成立。

第三种情况: 考虑一般的子 k 维子空间 B 。令 f 是两个标号不同的仿射函数 l_1, l_2 沿子空间 B 级联而成。先构造线性变换 φ 如下:

假定 $B = \{0, \beta_1, \beta_2, \dots, \beta_{2^k-1}\}$ 按照向量的字典顺序排列。假定补集 $\overline{B}$ 中字典顺序最小的向量为 γ 。选择子空间 B 的一组特殊基

$$\{\beta_{2^0}, \beta_{2^1}, \dots, \beta_{2^{k-1}}\}$$

构造 $k+1$ 阶 0-1 矩阵 $A = (\beta_{2^0}, \beta_{2^1}, \dots, \beta_{2^{k-1}}, \gamma)$ 。由于 $k+1$ 个列向量是线性无关的, 因此 A 是一个可逆矩阵。考虑线性变换

$$\begin{aligned} \varphi: F_2^{k+1} &\rightarrow F_2^{k+1} \\ x &\mapsto Ax \end{aligned}$$

线性变换 φ 把 k 维向量量子空间 $B_0^* = F_2^k$, 变为 B 。把 $\overline{B_0^*}$, 变为 $\overline{B}$ 。

利用矩阵 A , 以及布尔函数 f , 构造布尔函数 g 如下:

$$g(x) = f(Ax).$$

则布尔函数 g 是仿射函数 l_1, l_2 沿子空间 $B_0^* = F_2^k$ 的典范级联。由上面的第二种情况, 恰好存在三组仿射函

数, 以及三个 k 维向量空间 B_0^*, B_1^*, B_2^* , 使得 g 恰好等于这三种级联。由于线性变换把子空间变为子空间, 令 $B_1 = \varphi(B_1^*)$, $B_2 = \varphi(B_2^*)$, 而线性变换把仿射函数变为仿射函数, 此 f 恰好是三组仿射函数沿三个合适的子空间级联而成, 定理得证。

在这里强调一下: 三个合适的子空间的标号相加刚好为零向量!

例 5. 以 $k=3$ 为例, 举 3 个例子, 说明上述的证明过程:

(1) 假定仿射函数 l_1, l_2 的真值表分别为

$$l_1 = 00000000, \quad l_2 = 01100110.$$

即 l_1 的标号为 $0=(0,0,0)$, l_2 的标号为 $\omega_1=(1,1,0)$ 。 l_1, l_2 沿子空间 $B_0 = F_2^3$ 的典范级联为

$$f = 00000000 \parallel 01100110$$

由于 $B_0 = \{0,1,2,3,4,5,6,7\}$, $\overline{B_0} = \{8,9,a,b,c,d,e,f\}$ 。

考虑标号为 $\overline{\omega_1}=(\omega_1,0)=(1,1,0,0)$ 的 3 维子空间 B_1 , 则

$$B_1 = \{0,3,4,7,8,b,c,f\}, \quad \overline{B_1} = \{1,2,5,6,9,a,d,e\}.$$

则布尔函数 f 沿子空间 B_1 析出出来的两个布尔函数的真值表分别为:

$$l_1^* = 00000000, \quad l_2^* = 00001111$$

都是仿射函数, 标号分别为 $(0,0,0)$ 与 $(0,0,1)$ 。

考虑标号为 $\overline{\omega_2}=(\omega_1,1)=(1,1,0,1)$ 的 3 维子空间 B_2 , 则

$$B_2 = \{0,3,4,7,9,a,d,e\}, \quad \overline{B_2} = \{1,2,5,6,8,b,c,f\}.$$

则布尔函数 f 沿子空间 B_2 析出出来的两个布尔函数的真值表分别为:

$$l_1^{**} = 00001111, \quad l_2^* = 00000000$$

都是仿射函数, 标号分别为 $(0,0,1)$ 与 $(0,0,0)$ 。

当 f 沿其它子空间析取时, 得到的函数都不可能是仿射函数(因为, 不是全 0, 也不是全 1, 更不是平衡函数)。因此 f 可看作三组仿射函数沿三个合适的子空间级联而成。

(2) 假定仿射函数 l_1, l_2 的真值表分别为

$$l_1 = 01010101, \quad l_2 = 00110011.$$

即 l_1 的标号为 $\omega_1=(1,0,0)$, l_2 的标号为 $\omega_2=(0,1,0)$ 。 l_1, l_2 沿子空间 $B_0 = F_2^3$ 的典范级联为

$$f = 01010101 \parallel 00110011$$

构造辅助函数 $h = 0101 \ 0101 \ 0101 \ 0101$ 。考虑 $g(x) = f(x) + h(x)$, 则 g 的真值表为

$$g = 00000000 \parallel 01100110.$$

由刚计算的(1)知, g 由三组仿射函数沿三个子空间 B_0, B_1, B_2 级联而成。将布尔函数沿这三个子空间分别析取, 得到的三组函数分别为:

$$\begin{aligned} l_1 &= 01010101, \quad l_2 = 00110011, \\ l_1^* &= 01010101, \quad l_2^* = 10100101, \\ l_1^{**} &= 01010101, \quad l_2^* = 10100101. \end{aligned}$$

它们都是仿射函数。

(3) 假定选择的仿射函数仍然为

$$l_1 = 01010101, \quad l_2 = 00110011.$$

沿子空间 $B_0 = \{0, 3, 5, 6, 9, a, c, f\}$ 级联, 得到的布尔函数为

$$f = 00011011 \parallel 00100111.$$

B_0 的标号为 $\overline{\omega_0} = (1, 1, 1, 1)$ 。 $\overline{B_0}$ 字典排序最小的向量为 $\gamma = (1, 0, 0, 0)$ 。构造四阶 0-1 矩阵

$$A = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

为了方便, 列出由 A 构造的线性变换的一一对应关系如下(见表 S1):

Table S1. The true table of a linear transformation

表 S1. 线性变换的对应关系

x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
Ax	0	3	5	6	9	a	c	f	1	2	4	7	8	b	d	e

由布尔函数 f 及矩阵 A 构造布尔函数 g 如下: $g(x) = f(Ax)$ 。则 $g = l_1 \parallel l_2$ 为 l_1, l_2 沿子空间 $B_0^* = F_2^3$ 典范级联而成。由前面刚计算的(2)知, g 恰好是三组仿射函数沿三个子空间

$$B_0^* = \{0, 1, 2, 3, 4, 5, 6, 7\},$$

$$B_1^* = \{0, 3, 4, 7, 8, b, c, f\},$$

$$B_2^* = \{0, 3, 4, 7, 9, a, d, e\}.$$

利用表 S1 的对应关系, 我们写出线性变换把上面三个子空间分别变为:

$$B_0 = \{0, 3, 5, 6, 9, a, c, f\},$$

$$B_1 = \{0, 1, 6, 7, 8, 9, e, f\},$$

$$B_2 = \{0, 2, 4, 6, 9, b, d, f\}.$$

将布尔函数分别沿这三个子空间析取, 得到的三组布尔函数分别为:

$$l_1 = 01010101, \quad l_2 = 00110011,$$

$$l_1^* = 00110011, \quad l_2^* = 01101001,$$

$$l_1^{**} = 00110011, \quad l_2^{**} = 01010101.$$

它们均为仿射函数。