高非线性度多输出布尔函数的构造

常祖领[1], 柯品惠[2], 张 [3], 温巧燕[3]
(1. 郑州大学数学系, 河南郑州 450052; 2. 福建师范大学数学与计算机科学学院, 福建福州 350007;
3. 北京邮电大学理学院, 北京 100876)

摘 要: 本文主要讨论了构造具有高非线性度多输出布尔函数的方法. 对于输入变量个数少于输出变量个数的多输出布尔函数, 我们给出了存在非零非线性度的充分必要条件及具体的构造方法. 我们还利用一类特殊的多输出 bent 函数构造出具有非常高非线性度的无偏多输出函数.

关键词: 布尔函数; 非线性度; bent 函数; Reed-Muller 码
中图分类号: TN918.1 文献标识码: A 文章编号: 0372-2112 (2008) 01-0141-05

Constructions of Multi-Output Boolean Functions with High Nonlinearity

CHANG Zu-ling[1], KE Pin-hui[2], ZHANG Jie[3], WEN Qiao-yan[3]
(1. *Department of Mathematics, Zhengzhou University, Zhengzhou, Henan 450052, China;*
2. *School of Mathematics and Computer Science, Fujian Normal University, Fuzhou, Fujian 350007, China;*
3. *School of Sciences, Beijing University of Posts and Telecommunications, Beijing 100876, China*)

Abstract: This paper mainly study the methods to construct multi-output Boolean functions with high nonlinearity. For multi-output Boolean functions satisfying the number of input variables smaller than the number of output variables, we provide one sufficient and necessary condition for existing nonzero nonlinearity and the corresponding constructing method. We also use one special class multi-output bent functions to construct unbiased multi-output Boolean functions with very high nonlinearity.

Key words: Boolean functions; nonlinearity; bent functions; Reed-Muller codes

1 引言

非线性度[1]是衡量密码体制安全性的一个重要指标. 具有高非线性度的函数在很多领域如密码、序列和编码中都有重要的应用. 在密码领域中, 高非线性度的函数可以在流密码中用来构造密钥流生成器, 在分组密码中可以用来构造 S-盒, 在 Hash 运算中来构造分块, 还可以来构造认证码. 在编码理论中, 高非线性度的函数可以用来构造纠错性能优越的码. 在序列理论中, 它们可以在 CDMA 通信系统中用来构造相关性质良好的序列. 因此高非线性度是我们构造布尔函数时最基本和最重要的目标之一.

由于多输出布尔函数在应用中的效率更高, 所以在实际中多输出函数的应用更多. 具有高非线性度的多输出函数的构造一直受到注意, 并取得了很多成果. 但对于其中的特殊部分, 当输入变量个数少于输出变量个数时, 多输出布尔函数是否存在非零的非线性度, 以及如何构造具有高非线性度多输出布尔函数这两个问题一直没有得到解决. 本文将考虑这两个问题, 根据 Reed-Muller 码的结果和方法, 首先得到存在非零非线性度的充分必要条件, 然后给出具体的构造方法, 从而解决了这两个问题.

多输出布尔函数的无偏性也是衡量函数的密码性质的标准之一. 本文还讨论了同时具有无偏性和高非线性性的多输出布尔函数的构造问题. 我们利用具有某些性质的多输出 bent 函数和具有高非线性度的置换函数, 把它们组合, 从而得到了非线性度非常高的无偏的多输出布尔函数.

2 基本概念

令 $f(x)$ 是从向量空间 F_2^n 到 F_2 上的布尔函数. 我们把布尔函数 $f(x)$ 表示成一个具有 n 个变量的多项式

$$f(x_1, x_2, \cdots, x_n) = a_0 \oplus \left(\bigoplus_{i=1}^{n} a_i x_i\right) \oplus \left(\bigoplus_{1 \leqslant i \neq j \leqslant n}^{n} a_{ij} x_i x_j\right) \oplus \cdots \oplus a_{12\cdots n} x_1 x_2 \cdots x_n$$

收稿日期: 2006-01-10; 修回日期: 2007-12-19
基金项目: 国家自然科学基金(No. 60373059); 国家自然科学基金重大研究计划(No. 90604023); 河南省教育厅自然科学研究项目(No. 2007110034)

其中的系数 $a_0, a_i, a_{ij}, \cdots, a_{12\cdots n} \in F_2$. 函数 $f(x)$ 的这种表示称为 $f(x)$ 的代数范式(algebraic normal form, 简记为 ANF). 在 $f(x)$ 的代数范式中, 每一个单项 $x_{i_1}\cdots x_{i_s}$ 称为一个 $f(x)$ 的单项式(monomial). 单项式的次数就是其中不同变量 x_i 的个数, $f(x)$ 的代数范式的次数就是它的所有单项式的次数中的最大值, 而布尔函数的次数就是它的代数范式的次数.

F_2^n 上的仿射函数就是次数不大于 1 的布尔函数, 一般有如下形式:

$$f(x) = a_0 \oplus a_1x_1 \oplus \cdots \oplus a_nx_n$$

其中 $a_i \in F_2$, $i = 0, 1, \cdots, n$. 如果 $a_0 = 0$, 我们就称这个函数是线性函数. 我们以后用 $A(n)$ 来表示 F_2^n 上所有仿射函数的集合.

布尔函数 $f(x)$ 的汉明(Hamming) 重量, $wt(f)$, 定义为函数 $f(x)$ 的真值表中 1 的个数. 如果 $f(x)$ 的真值表中 0 和 1 各占一半, 即 $wt(f) = 2^{n-1}$, 我们就称这个函数是平衡的. 两个具有相同输入的函数 $f(x)$, $g(x)$ 之间的汉明距离定义为两个函数的和的重量, 即 $d(f, g) = wt(f \oplus g)$.

具有 n 个输入 m 个输出的多输出布尔函数, 简记为 (n, m)-函数, 是一个从 F_2^n 到 F_2^m 的函数. (n, m)-函数一般表示为 $F(x) = (f_1(x), \cdots, f_m(x))$, 其中的 $f_i(x)$ 被称为 $F(x)$ 的分量函数, 是 F_2^n 上的单输出布尔函数. 对于 (n, m)-函数, 如果它的每个输出对应的输入的个数是一样多的, 就称这个 (n, m)-函数是无偏的. 显然, 当 $n = 1$ 时, 无偏的概念等价于前面定义的平衡. 容易证明, (n, m)-函数是无偏的当且仅当它的分量函数的非零线性组合 $c_1f_1(x) \oplus \cdots \oplus c_mf_m(x)$, $c_1, \cdots, c_m \in F_2$, 且不全为 0, 是平衡的单输出函数. 因为 (n, m)-函数的输出个数是 2^m, 所以无偏函数每个输出对应的输入的个数是 2^{n-m}. 显然, 只有当 $m \leqslant n$ 时才会存在无偏函数. 我们称无偏的 (n, n)-函数为置换函数.

布尔函数 $f(x)$ 的非线性度, 记为 N_f, 等于它与所有仿射函数的汉明距离的最小值, 即:

$$N_f = \min_{l \in A(n)} d(f, l) = \min_{l \in A(n)} wt(f \oplus l)$$

对于多输出的 (n, m)-函数 $F(x) = (f_1(x), \cdots, f_m(x))$, 它的非线性度 N_F, 满足 $N_F = \min N_g$, 其中 N_g 是 $F(x)$ 的分量函数的任意一个非零线性组合得到的单输出函数 $g(x)$ 的非线性度, 即, $g(x) = a_1f_1(x) \oplus \cdots \oplus a_mf_m(x)$, 其中 $a_1, \cdots, a_m \in F_2$ 并且它们不全为零.

3 $n < m$ 时非线性 (n, m)-函数的构造

在这一节中我们主要利用 Reed-Muller 码的知识来构造 $n < m$ 时的非线性多输出布尔函数. 令 $0 \leqslant r \leqslant n$, r 阶 Reed-Muller 码 $RM(r, n)$ 是由所有对应代数范式 $f(x_1, \cdots, x_n)$ 次数不大于 r 的长度为 2^n 的二元串组成的集合. 因为仿射函数的次数不大于 1, 因此所有仿射函数组成的集合 $A(n)$, 就是 1 阶 Reed-Muller 码 $RM(1, n)$. Reed-Muller 码在编码理论中有着重要的位置, 同时, 任意一个布尔函数都可以看作一个 Reed-Muller 码的码字, 所以它在密码中也有很多应用. 关于 Reed-Muller 码的更多的性质和结论, 可以参考文献[2], 我们只在这里列出主要用到的结果.

定理 1 Reed-Muller 码 $RM(r, n)$ 的最小距离是 2^{n-r}, 且它的参数为 $\left[2^n, 1+\binom{n}{1}+\cdots+\binom{n}{r}, 2^{n-r}\right]$.

令 $f(x)$ 是代数范式次数为 $r > 1$ 的布尔函数, 则它包含于 $RM(r, n)$. 显然 $A(n) = RM(1, n) \subseteq RM(r, n)$, 所以对任意仿射函数 $a(x) \in A(n)$, $f(x) \oplus a(x)$ 的代数次数仍为 r. 由于 $RM(r, n)$ 的最小距离是 2^{n-r}, 则 $f(x)$ 和 $a(x)$ 的距离不小于 2^{n-r}. 由这个事实我们可以推出如果 $f(x)$ 的代数次数为 $r > 1$, 则 $f(x)$ 的非线性度至少为 2^{n-r}.

对于多输出布尔函数, 情况比较复杂. 并不是所有的 (n, m)-函数都有非零非线性度. 例如, 当 $n = 1$ 时, 非线性度肯定为 0; 当 $n = 2$ 且 $m \geqslant 2$ 时, 唯一的非线性项只有 x_1x_2, 不可能构造出两个非线性项不同的分量函数, 所以非线性度也是 0. 因此在构造高非线性度多输出函数之前, 我们必须首先来判断是否存在这样的函数. 所以我们来讨论存在具有非零非线性度的 (n, m)-函数的条件.

定理 2 对于两个整数 n, m, 存在非线性度非 0 的 (n, m)-函数的充要条件是 $2^n - n - 1 \geqslant m$.

证明 首先我们来证明本定理的充分性. 易知代数次数至少为 2 的单项式 $x_{i_1}x_{i_2}\cdots x_{i_s}$ 的个数为 $2^n - n - 1$. 因为 $2^n - n - 1 \geqslant m$, 根据 Reed-Muller 的知识, 我们可以以下面方法来构造一个 (n, m)-函数 $F(x) = (f_1(x), \cdots, f_m(x))$: 从 $2^n - n - 1$ 个次数至少为 2 的单项式中任意选 m 个来作为 $F(x)$ 的 m 个分量函数. 对于这个函数, 它的分量函数的任意非零线性组合的次数最多为 n 且最小为 2, 所以它的任意非零线性组合都属于 $RM(n, n)$. 根据非线性度的定义和定理 1, 我们得出 $F(x)$ 的非线性度至少为 1.

下面来证明必要性. 为了使得一个 (n, m)-函数 $F(x) = (f_1(x), \cdots, f_m(x))$ 的非线性度不为 0, 根据非线性度的定义, $F(x)$ 的分量函数的 $2^m - 1$ 个非零线性组合都必须是非线性函数, 且在每个函数中次数至少为 2 的单项式必须和另外一个函数的不完全一样, 所以我们需要次数至少为 2 的单项式的 $2^m - 1$ 个不同的非零线性组合. 对于某个数 n, 次数至少为 2 的单项式的个数为

2^n-n-1, 而这些单项式的非零线性组合的个数为 $2^{2^n-n-1}-1$ 个. 如果 $2^n-n-1<m$, 则 $2^{2^n-n-1}-1<2^m-1$, 这时 $F(x)$ 的分量函数的非零线性组合中, 至少有两个组合的次数至少为 2 的单项式是一样的, 则 $F(x)$ 的分量函数的非零线性组合中至少有一个是仿射函数, 则 $F(x)$ 的非线性度为 0. 所以如果 $F(x)$ 的非线性度不为 0, 则我们一定有 $2^n-n-1\geqslant m$.　　证毕.

根据定理 1 及定理 2 的证明过程, 我们可以推出构造 $n<m$ 时的高非线性度 (n, m)-函数的方法如下: 我们取不同的次数至少为 2 至多为 r 的单项式作为 $F(x)$ 的分量函数. 如果这样的单项式的个数不少于 m, 则我们总可以构造出一个 (n, m)-函数 $F(x)$ 满足其分量函数的 2^m-1 个非零线性组合都是非线性函数, 且其中次数至少为 2 至多为 r 的单项式与另外一个的不完全相同, 而对应函数的次数至多为 r. 根据非线性度的定义和 Reed-Muller 码的性质, $F(x)$ 的非线性度至少为 2^{n-r}.

对于上面这种构造方法, n 越大, 构造出的函数的非线性度就越大. 特别地, 次数至少为 2 至多为 $n-1$ 的单项式的个数为 2^n-n-2. 如果 $2^n-n-2\geqslant m$, 我们就可构造出非线性度至少为 2 的 (n, m)-函数, 而如果 2^n-2n-2, 即次数至少为 2 至多为 $n-2$ 的单项式的个数, 大于等于 m, 则我们就可以构造出非线性度至少为 4 的 (n, m)-函数. 当 $\binom{n}{2}\geqslant m$, 则我们可以得到下面推论.

推论 1　对于两个整数 n, m, 如果 $\binom{n}{2}\geqslant m$, 则存在非线性度至少为 2^{n-2} 的 (n, m)-函数.

证明　如果 $\binom{n}{2}\geqslant m$, 则至少存在 m 个不同的次数为 2 的单项式. 用这些单项式来做 (n, m)-函数 $F(x)$ 的分量函数, 则分量函数的非零线性组合的次数都是 2, 所以根据定理 1, $F(x)$ 的非线性度是 2^{n-2}.　　证毕.

例　当 $n=4$, $m=6$ 时, 代数次数为 2 的单项式为

$$x_1x_2,\ x_1x_3,\ x_1x_4,\ x_2x_3,\ x_2x_4,\ x_3x_4.$$

我们来构造 $(4, 6)$-函数

$$F(x)=(f_1(x), f_2(x), f_3(x), f_4(x), f_5(x), f_6(x))$$

使之满足

$$f_1(x)=x_1x_2, f_2(x)=x_1x_3, f_3(x)=x_1x_4$$
$$f_4(x)=x_2x_3, f_5(x)=x_2x_4, f_6(x)=x_3x_4$$

可验证, 这个函数的非线性度是 $2^{4-2}=4$, 而这也是 $(4, 6)$-函数的最大的非线性度.

推论 2　对于两个整数 n, m, 如果 $\binom{n}{2}\geqslant 2m$, 则存在非线性度至少为 $2^{n-1}-2^{n-3}$ 的 (n, m)-函数.

证明　如果 $\binom{n}{2}\geqslant 2m$, 则至少存在 $2m$ 个不同的次数为 2 的单项式. 我们用下面方法来构造一个 (n, m)-函数 $F(x)=(f_1(x), \cdots, f_m(x))$: 对于 $1\leqslant i\leqslant m$, 我们令 $f_1(x)=x_{i_1}x_{i_2}\oplus x_{i_3}x_{i_4}$, 并且 $i_1, i_2, i_3, i_4\in\{1, 2, \cdots, n\}$ 是四个不同的数. 另外, 每个次数为 2 的单项式最多出现在一个分量函数中, 而分量函数的非零线性组合不能写成下面形式:

$$(x_{i_1}\oplus\cdots\oplus x_{i_s})(x_{j_1}\oplus\cdots\oplus x_{j_t})$$

其中 $i_1, \cdots i_s, j_1, \cdots j_t$ 是不同的数. 上面条件是可以满足的, 只要对任意两个分量函数

$$f_i(x)=x_{i_1}x_{i_2}\oplus x_{i_3}x_{i_4}, f_j(x)=x_{j_1}x_{j_2}\oplus x_{j_3}x_{j_4}$$

中, 集合 $\{i_1, i_2, i_3, i_4\}$ 与 $\{j_1, j_2, j_3, j_4\}$ 不相同即可. 证毕.

根据文献[3], 代数次数为 2 的布尔函数都是部分 bent 函数. 根据部分 bent 函数的性质, 我们构造出的 (n, m)-函数 $F(x)$ 的分量函数的非零线性组合, 必要时经过线性变换, 都具有下面形式:

$$g(x)=x_1x_2\oplus x_3x_4\oplus h(x_5, \cdots, x_n)$$

显然 $b(x)=x_1x_2\oplus x_3x_4$ 是 F_2^4 上的 bent 函数, 所以它的非线性度 $N_b=2^{4-1}-2^{2-1}=6$. 则 $g(x)$ 的非线性度是

$$N_g=2^{n-4}N_b+2^4N_h-2N_gN_h=2^{n-4}6+(2^4-2\times 6)N_h$$
$$=2^{n-1}-2^{n-3}+4N_h\geqslant 2^{n-1}-2^{n-3}$$

所以我们推出 $F(x)$ 的非线性度至少为 $2^{n-1}-2^{n-3}$.

例　当 $n=6$, $m=7$ 时, 我们来构造一个 $(6, 7)$-函数 $F(x)$, 其分量函数如下:

$$f_1(x)=x_1x_2\oplus x_3x_6,\quad f_2(x)=x_1x_3\oplus x_2x_5,$$
$$f_3(x)=x_1x_4\oplus x_2x_6,\quad f_4(x)=x_1x_5\oplus x_3x_4,$$
$$f_5(x)=x_1x_6\oplus x_3x_5,\quad f_6(x)=x_2x_3\oplus x_4x_5,$$
$$f_7(x)=x_2x_4\oplus x_5x_6,$$

则 $(6, 7)$-函数 $F(x)=(f_1(x), f_2(x), \cdots, f_7(x))$ 的非线性度为 $2^{6-1}-2^{6-3}=24$

利用相同的思想, 我们可以构造出更多的具有高非线性度的 (n, m)-函数. 事实上, 对于 $3\leqslant n\leqslant 8$, $1\leqslant m\leqslant 8$ 时的 (n, m)-函数的最大非线性度已经在文献[4]中给出, 但是文献[4]中并没有更深入的研究该问题, 也没有给出一般的构造方法. 本文中的定理 2 及两个推论可以看作是关于 $n<m$ 时构造具有高非线性度 (n, m)-函数的一般性的结果.

在文献[5, 6]中, 作者主要讨论了利用线性码来构造具有高非线性度的 resilient 函数. 他们也是按照输入和输出变量的个数的关系, 分成了三部分讨论, 其中当然就用到了 $n<m$ 时的高非线性度的 (n, m)-函数的结果. 但遗憾的是文献[5, 6]中并没有解决这个问题, 因而该文中的部分结果并不完整, 或者直接令 $n<m$ 时的

(n, m) -函数的非线性度为 0, 使得构造出的函数的非线性度没有达到最高. 因此我们这一部分的结果可以用来改进文献[5, 6]中的一些结果, 使得对应函数的非线性度更高.

另外, 我们所给出的构造方法也有缺点. 因为 $n<m$ 时函数有可能不存在非零非线性度, 我们并没有给出一个对所有 n, m 都适用的一般性的公式, 而是根据 m 的不同而给出对应的非线性度的公式. 而且当 n 比较小时根据我们给出的公式求得的非线性度非常接近最大值, 但当 n 越来越大, 根据我们给出的公式求得的非线性度就和最大值差得越来越多. 在今后的工作中, 我们将继续这方面的研究来克服这些缺点.

4 高非线性度无偏-(n, m) 函数的构造

在这一部分内容中, 我们将讨论如何利用一类特殊的多输出 bent 函数来构造具有高非线性度的无偏的多输出函数.

在文献[7]中作者 H. Dobbertin 给出了一种利用 bent 函数来构造单输出的高非线性度的平衡函数的方法. 作者证明, 只要一个 bent 函数 F_2^n 在的某个 p 维子空间上是常值的, 就可以根据它来构造出高非线性度的平衡函数. 事实上, 如果 bent 函数存在某个 p 维子空间使得在其上是常值, 则我们就称这个 bent 函数是 normal 的[8~10], 如果在其上是仿射的, 就称它是弱 normal 的. Bent 函数的 normal 性是一个比较重要的概念. 以前人们认为 bent 函数基本上都是 normal 或弱 normal 的, 直到文献[11]构造出了一种 bent 函数, 非 normal 也非弱 normal, 并且这种 bent 函数还很多, 这样才改变了人们对 bent 函数的看法, 吸引了许多学者来探讨 bent 函数的本质和特性. 关于 bent 函数的 normal 性的详细知识可在文献[8~10]中找到. 我们这里要求我们选的 bent 函数都是 normal 的.

文献[7]给出构造方法如下: 令 $f(x)$ 是 F_2^n 上的一个 normal 的 bent 函数. 如果 $wt(f)=2^{n-1}-2^{n/2-1}$, 则我们就选一 $p=n/2$ 维子空间 E 使得 $f(x)$ 满足当 $x\in E$ 时 $f(x)=0$, 如果 $wt(f)=2^{n-1}+2^{n/2-1}$, 则我们就选一个 p 维子空间 E 使得 $f(x)$ 满足当 $x\in E$ 时 $f(x)=1$. 令 g 是子空间 E 上任意一个平衡函数. 则布尔函数 $f'=f+g$, 它在子空间 E 上的取值等于 g 或 $\bar{g}$ 的取值, 在除去 E 的其它处的取值等于 f 的取值, 则 f' 是一个平衡函数.

我们用 $N_n(f')$ 来表示 f' 的非线性度, 用 $N_p(g)$ 来表示 g 的非线性度, 则可以证明新函数的非线性度满足

$$N_n(f')\geqslant 2^{n-1}-2^{n/2}+N_p(g)$$

采用同样的思想, 我们可以借助这种思想和对应的多输出 bent 函数来构造高非线性度的多输出无偏函数.

令 $F(x)=(f_1, \cdots, f_m)$ 是一个 (n, m)-bent 函数, 且它的分量函数都在某个 p 维子空间 E 上是常值. (取法与上面相同) 令 $H=(h_1, \cdots, h_m)$ 是 E 上的无偏 (p, m)-函数, 其非线性度为 N_H. 对于新的 (n, m)-函数, $F'=F+H$ 它的取值与上面单输出情形相同. 则它的分量函数的任意非零线性组合都是和的对应的分量的非零线性组合. 易证 $F'=F+H$ 是无偏的. 类似于单输出情形的讨论, 它的非线性度应满足

$$N_n(F')\geqslant 2^{n-1}-2^{n/2}+N_H$$

根据上面的方法, 只要我们选取适当的 bent 函数和无偏 (p, m)-函数, 我们就可以构造出非线性度非常高的函数. 常见的 (n, m)-bent 函数包括 M-M 类和 PS 类, 其详细的构造过程可在文献[12~14]中找到, 这里就不一一列出. 我们可以得到下面的两个推论. 推论的证明和上面的分析相似, 其中主要是理解 M-M 类和 PS 类 bent 的构造. 我们在这里略去了详细的证明, 只把结果列出来.

推论 **3** (M-M 类) 令 $F(x, y)=(f_1(x, y), \cdots, f_m(x, y))$ 是 F_2^n 上的一个 M-M 类 (n, m)-bent 函数. 对于 $i=1, 2, \cdots, m$,

$$f_1(x, y)=x\cdot\pi_i(y)\oplus g_i(y),$$

其中 $\pi_i(y)$, $i=1, \cdots, m$ 是 F_2^p 上任意置换函数的 m 个分量函数且满足 $\pi_i(0)=0$, $g_i(y)$ 是 F_2^p 上任意函数. 令 $H(x)=(h_1(x), \cdots, h_m(x))$ 是一个无偏的 (p, m)-函数, 其非线性度为 N_H. 定义一个新的 (n, m)-函数 $F'(x, y)=(f'_1(x, y), \cdots, f'_m(x, y))$, 使得其满足对于 $i=1, 2, \cdots, m$,

$$f'(x, y)=\begin{cases} h_i(x) & y=0,\\ f_i(x, y) & y\neq 0.\end{cases}$$

则 $F'(x, y)$ 是一个无偏的 (n, m)-函数, 它的非线性度满足

$$N_{F'}\geqslant 2^{n-1}-2^{n/2}+N_H$$

推论 **4** (PS 类) 令 $E_0, E_1, \cdots, E_{2^p}$ 是 F_{2^n} 的一个分解, 且 $H=(h_1, \cdots, h_m)$ 是其中一个子空间 E_s, $s\in\{0, 1, \cdots, 2^p\}$ 上的一个无偏 (p, m)-函数, 它的非线性度是 N_H. 令 φ 为一个从 F_{2^p} 到 $\{0, 1, \cdots, 2^p\}\setminus\{s\}$ 上的一一映射, 且 $G=(g_1, \cdots, g_m)$ 为任意一个无偏 (p, m)-函数. 定义子集 s_i, $i=1, \cdots, m$ 如下:

$$S_i=\{\varphi(\alpha)\mid g_i(\alpha)=1, \alpha\in F_{2^p}\}$$

这时 (n, m)-函数 $F'(x)=(f'_1(x), \cdots, f'_m(x))$, 其中对于 $i=1, \cdots, m$,

$$f'_i(x)=\begin{cases} h_i(x) & x\in E_s\\ \sum_{j\in S_i} I_{E_j}(x) & \text{其他}\end{cases}$$

则 $F'(x)$ 是一个无偏的 (n, m)-函数, 它的非线性度满足

$$N_{F'} \geqslant 2^{n-1} - 2^{\frac{n}{2}} + N_H$$

利用上面的结果, 我们可以构造出具有非常高的非线性度的无偏(n, m)-函数. 例如, 当 $n=8$ 时, 我们可以先构造出一个 M-M 类或 PS 类的$(8, 4)$-bent 函数, 并且可以构造出一个$(4, 4)$-置换函数, 其非线性度为 4. 根据上面的推论, 我们就可以构造出一个无偏$(8, 4)$-函数, 非线性度为

$$2^7 - 2^4 + 4 = 116.$$

这个非线性度也是 8 个输入无偏函数的非线性度的最大值[15].

5 结论

本文主要讨论了高非线性多输出布尔函数的构造方面的问题. 当输入变量个数少于输出变量个数时, 我们给出了判断是否存在非零非线性度的函数的充分必要条件, 并根据该条件的证明过程给出了构造具有非零非线性度的这类多输出函数的通用方法, 并改进了有关结果. 我们还利用一类特殊的多输出 bent 函数构造出无偏的多输出函数. 这种多输出函数的非线性度非常高, 可以用于多个领域. 本文中的方法和结果有很高的应用价值, 并且对以后更深入地研究奠定了基础.

参考文献:

[1] W Meier, O Staffelbach. Nonlinearity criteria for Cryptographic functions[A]. In Advances in Cryptology-EUROCRYPT'89 (Lecture Notes in Computer Science, vol. 434)[C]. Berlin, Germay: Springer-Verlag, 1990. 549-562.

[2] F J MacWilliams, N J A Sloane. The Theory of Error Correcting Codes[M]. Amsterdam: North Holland, 1977.

[3] C Carlet. Partially-bent functions[J]. Designs, Codes and Cryptography, 1993, 3: 135-145.

[4] T Wadayama, T Hada, K Wakasugi, and M Kasahara. Upper and lower bounds on maximum nonlinearity of n-input m-output Boolean function[J]. Designs, Codes and Cryptography, 2001, 23: 23-33.

[5] E Pasalic, S Maitra. Linear codes in generalized construction of resilient functions with very high nonlinearity[J]. IEEE Transactions on Information Theory, 2002, 48(8): 2182-2191.

[6] K C Gupta, P Sarkar. Improved construction of nonlinear resilient S-boxes[J]. IEEE Transactions on Information Theory, 2005, 51(1): 339-348.

[7] H Dobbertin. Construction of bent functions and balanced Boolean functions with high nonlinearity[A]. Proceedings of the 1994 Leuven Workshop on Cryptographic Algorithms(Lecture Notes in Computer Science, vol. 1008)[C]. Berlin, Germay: Springer-Verlag, 1995. 61-74.

[8] A Canteaut, M Daum, H Dobbertin, and G Leander. Normal and nonnormal bent functions[A]. in Proc. Workshop on Coding and Cryptography (WCC 2003)[C]. Versailles, France, Mar. 2003. 91-100.

[9] C Carlet, H Dobbertin, and G Leander. Normal extensions of bent functions[J]. IEEE Transactions on Information Theory, 2004, 50(11): 2880-2885.

[10] M Daum, H Dobbertin, and G Leander. An algorithm for checking normality of Boolean functions[A]. in Proc. Workshop on Coding and Cryptography (WCC 2003)[C]. Versailles, France, Mar. 2003. 133-142.

[11] J F Dillon, H Dobbertin. New cyclic difference sets with Singer parameters[J]. Finite Fields their Applic., 2004, 342-389.

[12] C Carlet. Recent results on bent functions[A]. in Proceedings of the International Conference on Combinatorics, Information Theory and Statistics[C]. Portland, Maine, 1999. 275-291.

[13] 常祖领, 陈鲁生, 符方伟. PS 类 bent 函数的一种构造方法[J]. 电子学报, 2004, 32(10): 1649-1653.
Chang Zu-ling, Chen Lu-sheng, Fu Fang-wei. One method for constructing bent functions of class PS[J]. Acta Electronica Sinica, 2004, 32(10): 1649-1653.

[14] X Hou, P Langevin. Results on bent functions[J]. Journal of Combinatorics Theory, Series A, 1997, 80: 232-246.

[15] P Sarkar, S Maitra. Nonlinearity bounds and constructions of resilient Boolean functions[A]. in Proceedings of CRYPTO'2000 (Lecture Notes in Computer Science)[C]. Berlin: Springer-Verlag, vol. 1880, 2000. 515-532.

作者简介:

常祖领　男, 1976 年出生, 郑州大学副教授. 研究方向: 编码密码学. E-mail: zlchang@eyou.com