Advances in Applied Mathematics 应用数学进展, 2014, 3, 62-69
Published Online May 2014 in Hans. http://www.hanspub.org/journal/aam
http://dx.doi.org/10.12677/aam.2014.32010

Hans汉斯

Construction of Vectorial Boolean Function Based on T-D Conjecture

Yiran Chen, Meng Zhou

Key Laboratory of Mathematics, Information and Behaviour of the Ministry of Education, School of Mathematics and System Science, Beihang University, Beijing
Email: 13352225@qq.com, zm1613@sina.com

Received: Feb. 18th, 2014; revised: Mar. 20th, 2014; accepted: Mar. 28th, 2014

Copyright © 2014 by authors and Hans Publishers Inc.
This work is licensed under the Creative Commons Attribution International License (CC BY).
http://creativecommons.org/licenses/by/4.0/
Open Access

Abstract

An improvement has been made on the construction method of Boolean Functions and the relevant conclusions of combinatorial conjecture proposed by Ziran Tu. We generalized their results and extended to the vectorial case. A class of bent Boolean functions *F* with the maximum algebraic immunity is presented by a more general construction method. Then by modifying *F*, we get new vectorial balanced functions with optimum algebraic degree, good nonlinearity and good algebraic immunity even maximum algebraic immunity for some cases.

Keywords

Vectorial Boolean Functions, Algebraic Immunity, Bent Function, Balancedness, Nonlinearity

T-D猜想上多输出布尔函数构造

陈怡然，周　梦

北京航空航天大学数学与系统科学学院，数学、信息与行为教育部重点实验室，北京
Email: 13352225@qq.com, zm1613@sina.com

收稿日期：2014年2月18日；修回日期：2014年3月20日；录用日期：2014年3月28日

摘　要

本文针对基于涂自然等人提出的组合猜想上布尔函数的构造方法和有关结论，将组合猜想和构造方法一

般化，并将其推广到多输出布尔函数上去，构造出具有最优代数免疫度的多输出bent函数*F*，同时通过修改*F*构造出具有好的非线性度、最优代数度和最优代数免疫度兼具的多输出平衡布尔函数函数。

关键词

多输出布尔函数，代数免疫度，Bent函数，平衡性，非线性度

1. 引言

布尔函数作为密码学的重要组成部分，随着信息时代的到来，其研究得到了快速发展。布尔函数按构造可分为单输出布尔函数和多输出布尔函数两种，单输出布尔函数一般用于流密码，而用于构成 S-盒的向量布尔函数也叫做多输出布尔函数在分组密码和流密码都有着重要作用。2009 年涂自然和邓映蒲提出了 T-D 猜想，构造出能抵抗代数攻击[1]-[4]等多种攻击，具有最佳非线性性和代数免疫度[5]的单输出布尔函数。2011 年冯克勤等将其猜想和构造方法推广到多输出布尔函数中，构造出了在一定条件下非线性和代数免疫度很好的多输出布尔函数。后来又出现了基于 T-D 猜想的各种组合猜想，构造出了更多的密码学性质优异的单输出布尔函数，由此我们基于 T-D 猜想和其他组合猜想大胆构造出一个一般的组合猜想，并假设这个猜想也可以推广到多输出布尔函数中，从而同样可以构造出更多的密码学性质优异的多输出布尔函数，我们将系统的对这个假设进行验证。

本文主要有这几个部分：第 2 节介绍相关知识；第 3 节给出 T-D 猜想和相关新组合猜想；第 4 节给出了一类具有最优代数免疫度的偶数元多输出布尔函数的构造；第 5 节对此多输出布尔函数进行修改，并讨论它的平衡性和非线性度；第 6 节进行总结和展望。

2. 布尔函数基本知识

2.1. 单输出布尔函数

单输出 n 元布尔函数定义为：设 $\mathbb{F}_2$ 是二元有限域，$\mathbb{F}_2^n$ 是 $\mathbb{F}_2$ 上的 n 维向量空间，一个 n 元布尔函数 f 是从 $\mathbb{F}_2^n$ 到 $\mathbb{F}_2$ 上的一个映射。n 元布尔函数的全体记作 B_n。一个 n 元布尔函数 f 的基本表示方法是真值表表示，即 $\mathbb{F}_2$ 上的一个长为 2^n 的向量：$\left(f(0,\cdots,0,0), f(0,\cdots,0,1), f(0,\cdots,1,0),\cdots, f(1,\cdots,1,1)\right)$。每一个 n 元布尔函数 f 还可以唯一表示为 $\mathbb{F}_2$ 上的含 n 个变元的多项式，称之为 f 的代数正规型(Algebraic Normal Form, ANF)：$f(x_1,\cdots,x_n)=\sum_{I\subset\{1,2,\cdots,n\}} a_I \prod_{i\in I} x_i \ (a_I \in F_2)$。非零布尔函数 f 的代数次数 $\deg(f)$ 定义为代数正规型中系数非零项所含有最多的变元的个数，规定代数系数不超过 1 的布尔函数为仿射函数，全体 n 元仿射函数的集合记为 A_n。设 $\mathbb{F}_{2^n}$ 为 2^n 元有限域，则它可以看成 $\mathbb{F}_2$ 上的 n 维向量空间。$\mathbb{F}_{2^n}$ 上的任意布尔函数也可以表示成唯一的单变元多项式：$f(x)=\sum_{i=0}^{2^n-1} a_i x^i$ 其中 $a_0, a_{2^n-1}\in\mathbb{F}_2, a_i\in\mathbb{F}_{2^n}$ 对 $1\le i<2^n-1$，且满足 $a_i^2=a_{2i\left(\mathrm{mod}\,2^n-1\right)}$。此时 f 的代数次数 $\deg(f)$ 为 $\max\left\{\omega t(\bar{i}) \mid a_i\neq 0, 0\le i<2^n\right\}$，这里 $\bar{i}$ 为 i 的二进制展开。

单输出 n 元布尔函数 f 的支撑集定义为：$supp(f)=\left\{x\in\mathbb{F}_2^n \mid f(x)=1\right\}$。支撑集 $supp(f)=$ 所含元素的个数称为 f 的 Hamming 重量，记为 $\omega t(f)$。若 $\omega t(f)=2^{n-1}$，则称 n 元布尔函数是平衡的。两个 n 元布尔函数 f 和 g 的 Hamming 距离 $d_H(f,g)$ 定义为 $\omega t(f+g)$。

单输出布尔函数 f 的非线性度定义为：$nl(f)=\min_{g\in A_n}\left(d_H(f,g)\right)$。

单输出布尔函数的 Walsh 谱定义为：令 $x=(x_1,x_2,\cdots,x_n)$，$a=(a_1,a_2,\cdots,a_n)$ 都属于 $\mathbb{F}_2^n$。记

$a\cdot x=a_1x_1+a_2x_2+\cdots+a_nx_n$，则 Walsh 谱 $W_f(a)=\sum_{x\in F_2^n}(-1)^{f(x)+a\cdot x}$。对于 $f:\mathbb{F}_{2^n}\to\mathbb{F}_2$，其 f 在 a 点的 Walsh 谱定义为：$W_f(a)=\sum_{x\in F_{2^n}}(-1)^{f(x)+tr(ax)}$，$a\in\mathbb{F}_{2^n}$ 其中 tr 是从 $\mathbb{F}_2^n$ 到 $\mathbb{F}_2$ 上的迹函数：$tr(x)=x+x^2+x^{2^2}+\cdots+x^{2^{n-1}}$。对于 $f:\mathbb{F}_{2^k}\times\mathbb{F}_{2^k}\to\mathbb{F}_2$，其 f 在 (a,b) 点的 Walsh 谱定义为：$W_f(a,b)=\sum_{(x,y)\in\mathbb{F}_{2^k}\times\mathbb{F}_{2^k}}(-1)^{f(x,y)+tr(ax+by)},(a,b)\in\mathbb{F}_{2^k}\times\mathbb{F}_{2^k}$。一个布尔函数 f 是平衡函数当且仅 $W_f(0)=0$。f 的非线性度也可以由 Walsh 谱给出：$nl(f)=2^{n-1}-\frac{1}{2}\max_{\omega\in\mathbb{F}_2^n}|W_f(\omega)|$。对任意 n 元布尔函数 f，有 $nl(f)\le 2^{n-1}-2^{\frac{n}{2}-1}$。达到这个上界的布尔函数称为 Bent 函数[6]。

单输出布尔函数代数免疫度的定义：对 $f\in B_n(x)$，f 的零化子的集合记作：$Ann(f)=\{g\in B_n(x)\mid fg=0\}$。布尔函数 f 的代数免疫度（Algebraic Immunity）$AI(f)$ 指的是：f 与 $f+1$ 的非零零化子的最低次数，即 $AI(f)=\min\{\deg(g)\mid 0\ne g\in Ann(f)\cup Ann(f+1)\}$，可以证明，$n$ 元布尔函数的代数免疫度不超过 $\left\lceil\frac{n}{2}\right\rceil$ [3] [5]。如果一个 n 元布尔函数的代数免疫度恰好等于 $\left\lceil\frac{n}{2}\right\rceil$，则称该函数具有最优代数免疫度或最大代数免疫度(Maximum Algebraic Immunity)，简称 MAI 函数。

2.2. 多输出(向量)布尔函数

假设 $1\le m\le n$，多输出布尔函数定义为：$F=(f_1,\cdots,f_m):\mathbb{F}_2^n\to\mathbb{F}_2^m\ (f_i\in B_n,1\le i\le m)$。

如果对所有 $b\in\mathbb{F}_2^m$，$|F^{-1}(b)|=2^{n-m}$ 称布尔函数 F 是平衡的，其中 $b=(b_1,\cdots,b_m)\in\mathbb{F}_2^m$，$F^{-1}(b)=\{a=(a_1,\cdots,a_n)\in\mathbb{F}_2^n\mid F(a)=b\}=\{a\in\mathbb{F}_2^n\mid f_i(a)=b_i\ (1\le i\le m)\}$，我们知道布尔函数 F 是平衡的当且仅当布尔函数 $vF=v_1f_i+\cdots v_mf_m:\mathbb{F}_2^n\to\mathbb{F}_2$ 是平衡的，对每个 $0\ne v=(v_1,\cdots,v_m)$。

布尔函数 F 的非线性度定义为：

$$nl(F)=\min\{nl(v\cdot F):0\ne v\in\mathbb{F}_2^m\}=2^{n-1}-\frac{1}{2}\max\left\{\left|\sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot F(x)+u\cdot x}\right|:0\ne v\in\mathbb{F}_2^m,u\in\mathbb{F}_2^n\right\}$$

已经证明出对每个 m,n，$nl(F)\le 2^{n-1}-2^{\frac{n}{2}-1}$。如果 $nl(F)=2^{n-1}-2^{\frac{n}{2}-1}$，称布尔函数 F 为 bent 函数，只有可能当且仅当 n 是偶数且 $m\le\frac{n}{2}$ 时得到。从定义可以很容易得到布尔函数 F 为 bent 函数当且仅当对每个 $0\ne v\in\mathbb{F}_2^m$，函数 $vF:\mathbb{F}_2^n\to\mathbb{F}_2$ 是 bent 函数。

布尔函数 F 的代数度定义为：$Deg(F)=\max\{\deg(f_i):1\le i\le m\}=\max\{\deg(v\cdot F):0\ne v\in\mathbb{F}_2^m\}$，如果 F 是平衡的，那么所有 $f_i\ (1\le i\le m)$ 都是平衡的，所以 $Deg(F)\le n-1$。

布尔函数 F 的代数免疫度定义为 $AI(F)=\min\{\deg(g):0\ne g\in B_n,\exists b\in\mathbb{F}_2^m\text{满足}g|_{F^{-1}(b)}=0\}$。令 $d=d(n,m)$ 是满足 $\sum_{i=0}^{d}\binom{n}{i}>2^{n-m}$ 的最小整数，那么已经证明 $AI(F)\le d(n,m)$，取等号时布尔函数 F 取得最优代数免疫度。

3. 一些组合猜想

猜想 1[7](T-D 猜想) 设 $k\in Z$，$k>1$，对任意 $x\in\mathbb{Z}_{2^k-1}$，把 x 展开成 k 位二进制数，用 $\omega t(\bar{x})$ 表示 x 的展开式中 1 的个数，对任意 $t\in\mathbb{Z}$，$0<t<2^k-1$，令

$$S_t=\{(a,b)\mid a,b\in Z_{2^k-1},a+b\equiv t\bmod 2^k-1,\omega t(\bar{a})+\omega t(\bar{b})\le k-1\}$$ 则 $|S_t|\le 2^{k-1}$。

[7]中涂自然和邓映蒲说明了虽然至今无法精确证明此猜想，但已经可以证明当 $k \le 29$ 时猜想成立。D.Tang 等人在文献[8]又给出了一个类似的新组合猜想：

猜想 2[8]设 $k \in \mathbb{Z}$， $k>1$。对任意 $0<t<2^k-1$，定义

$$S_{t,-}=\left\{(a,b)\mid a,b\in Z_{2^k-1}, a-b\equiv t \bmod 2^k-1, \omega t(\bar{a})+\omega t(\bar{b})\le k-1\right\}$$ 则 $\left|S_{t,-}\right|\le 2^{k-1}$。

这个猜想已经被证明[9]，同时也提出了下面的猜想：

猜想 3[8]设 $k \in \mathbb{Z}$， $k>1$， $u \in \mathbb{Z}_{2^k-1}^*$。对任意 $0<t<2^k-1$，定义：

$$S_{t,u,-}=\left\{(a,b)\mid 0\le a,b<2^k-1, ua-b\equiv t \bmod 2^k-1, \omega t(\bar{a})+\omega t(\bar{b})\le k-1\right\}$$，则 $\left|S_{t,u,-}\right|\le 2^{k-1}$。

并且，当 $2\le k\le 15$ 时，文献[8]对 $ua\pm b$ 的情况给出了验证。可见猜想 3 包括了猜想 2 这种特殊情况，下面我们在这里将给出一个更一般化的组合猜想：

猜想 4 设 $k \in \mathbb{Z}$， $k>1$， $u,v \in \mathbb{Z}_{2^k-1}^*$。对任意 $0<t<2^k-1$，定义：

$$S_{t,u,-v}=\left\{(a,b)\mid 0\le a,b<2^k-1, ua-vb\equiv t \bmod \left(2^k-1\right), \omega t(\bar{a})+\omega t(\bar{b})\le k-1\right\}$$，则 $\left|S_{t,u,-v}\right|\le 2^{k-1}$。

证明文献[10]中已证明了 $ua+vb$ 的情况等同于 $ua+b$ 的情况，这里也可以用同样的手段得出猜想 4 等同于猜想 3。

在文献[11]中冯克勤等将组合猜想 1 推广到了多输出布尔函数上，于是大胆假设这几种猜想都同样可以推广到多输出布尔函数中，这里对猜想 4 进行推广：

猜想 5 令 $1\le m\le k, 1\le t\le 2^k-2, 1\le D\le k-1$，定义：

$$S_{t,u,-w}(k,D)=\left\{(a,b)\mid 0\le a,b<2^k-1, ua-wb\equiv t\left(\bmod 2^k-1\right), s(a)+s(b)\le D-1\right\};$$

$$N(k,D)=\max\left\{\left|S_{t,u,-w}(k,D)\right|: 1\le t\le 2^k-2\right\},$$

其中对于 $a \in \mathbb{Z}_{2^k-1}$， $0\le a\le 2^k-2$， $a=a_0+a_1 2+\cdots+a_{k-1}2^{k-1}\left(a_i\in\{0,1\}\right)$， $s(a)=a_0+\cdots+a_{k-1}$。令 $D(k,m)$ 是最大的整数 D 那么 $N(k,D)\le 2^{k-m}$。

4. 最优代数免疫度的多输出布尔函数

根据上述猜想，和文献[11]中的构造，给出了一个一般的构造：

构造 1 令 $1\le m\le k$， $n=2k$， $0\le s\le 2^k-2$。α 为 $\mathbb{F}_{2^k}$ 的本原元，$\mathbb{F}_{2^k}$ 是下列 2^m 个不相交子列的并集：$A_0=\left\{\alpha^l \mid s\le l\le s+2^{k-m}-2\right\}\cup\{0\}$； $A_b=\left\{\alpha^l \mid s+2^{k-m}b-1\le l\le s+2^{k-m}(b+1)-2\right\}\left(1\le b\le 2^m-1\right)$。

每个整数 $b\left(1\le b\le 2^m-1\right)$ 有 2 进制展开 $b=b_0+b_1 2+\cdots+b_{m-1}2^{m-1}\left(b_i\in\{0,1\}\right)$，相当于向量 $\bar{b}=(b_0,b_1,\cdots,b_{m-1})\in\mathbb{F}_2^m$。对于每个 $i, 0\le i\le m-1$，我们定义对 $x,y\in\mathbb{F}_{2^k}$， $f_i=f_i(x,y):\mathbb{F}_{2^k}\times\mathbb{F}_{2^k}\to\mathbb{F}_2$，

$$f_i=f_i(x,y)=\begin{cases}1, & y\ne 0 \text{且} x^w y^u\in\bigcup\limits_{0\le b\le 2^m-1, b_i=1} A_b\\ 0, & \text{其他}\end{cases}$$ 那么构造布尔函数 $F=(f_0,\cdots,f_{m-1}):\mathbb{F}_{2^k}\times\mathbb{F}_{2^k}=\mathbb{F}_{2^n}\to\mathbb{F}_{2^m}$。

4.1. 代数免疫度

定理 1：设 F 是构造算法 1 中的多输出布尔函数，则 $AI(F)\ge D(k,m)$，特别的，当 $D(k,m)=d(n,m)$ 时 $AI(F)=d(n,m)$。

证明为了证明 $AI(F)\ge D=D(k,m)$，我们只需要证明如果 $h\in B_n$ 满足 $\deg(h)\le D-1$ 和至少有一个 $\bar{b}=(b_0,b_1,\cdots,b_{m-1})\in\mathbb{F}_2^m$ 满足 $h|_{F^{-1}(b)}=0$，那么 $h\equiv 0$。我们将 h 表示为 $h=h(x,y):\mathbb{F}_{2^n}=\mathbb{F}_{2^k}\times\mathbb{F}_{2^k}\to\mathbb{F}_2$，

$$h(x,y)=\sum_{i,j=0}^{2^k-1} h_{i,j}x^i y^j\left(h_{i,j}\in\mathbb{F}_{2^k}\right)$$。

由 $D-1\geq \deg(h)=\max\{s(i)+s(j)\,|\,h_{i,j}\neq 0\}$ 我们知道 $h(x,y)=\sum_{\substack{i,j=0\\ s(i)+s(j)\leq D-1}}^{2^k-1} h_{i,j}x^i y^j$。

因为 $F^{-1}(b)\supseteq\left\{\left(\gamma^{\frac{1}{w}}\beta^{-u},\beta^w\right)\,|\,\gamma\in A_b,\beta\in\mathbb{F}_{2^k}^*\right\}$，所以

$$0=h\left(\gamma^{\frac{1}{w}}\beta^u,\beta^{-w}\right)=\sum_{\substack{i,j=0\\ s(i)+s(j)\leq D-1}}^{2^k-1}h_{i,j}\gamma^{\frac{i}{w}}\beta^{ui-wj}=\sum_{t=0}^{2^k-1}\beta^t\sum_{\substack{0\leq i,j\leq 2^k-1\\ ui-wj=t\left(\mathrm{mod}\,2^k-1\right)\\ s(i)+s(j)\leq D-1}}h_{i,j}\gamma^{\frac{i}{w}}=h_{0,0}+\sum_{t=1}^{2^k-2}h_t(\gamma)\beta^t$$

其中 $h_t(\gamma)=\sum_{(i,j)\in S_{t,u,-w}(k,D)}h_{i,j}\gamma^{\frac{i}{w}}\left(1\leq t\leq 2^k-2\right)$，集合 $S_{t,u,-w}(k,D)$ 是猜想 5 中定义的。

考虑多项式 $H(y)=h_{0,0}+\sum_{t=1}^{2^k-2}h_t(\gamma)y^t\in\mathbb{F}_{2^k}[y]$，我们知道对所有的 $\beta\in\mathbb{F}_{2^k}^*$，$H(\beta)=0$。因此我们得到 $h_{0,0}=0$ 且 $0=h_t(\gamma)=\sum_{(i,j)\in S_{t,u,-w}(k,D)}h_{i,j}\gamma^{\frac{i}{w}}\left(1\leq t\leq 2^k-2,\gamma\in A_b\right)$。

由 $D=D(k,m)$ 的定义，我们知道 $\left|S_{t,u,-w}(k,D)\right|\leq 2^{k-m}$，令 $h_t(z)=\sum_{(i,j)\in S_{t,u,-w}(k,D)}h_{i,j}z^{\frac{i}{w}}\in\mathbb{F}_{2^k}[z]$，$h_t(z)$ 中非零系数 $h_{i,j}$ 的个数最多为 2^{k-m}，又对所有 $\gamma\in A_b$，$h_t(\gamma)=0$。如果 $1\leq b\leq 2^m-1$，$A_b=\left\{\alpha^l\,|\,s+2^{k-m}b-1\leq l\leq s+2^{k-m}(b+1)-2\right\}$，由 BCH 码[12]中 BCH 界知 $h_t(z)$ 的所有系数都是 0。当 $b=0$ 时，$A_0=\left\{\alpha^l\,|\,s\leq l\leq s+2^{k-m}-2\right\}\cup\{0\}$，如果 $s(t)\geq D$，那么 $ui-wj\equiv t\left(\mathrm{mod}\,2^k-1\right)$ 相当于 $s(i)+s(j)\geq s(t)>D-1$ 此时 $S_{t,u,-w}(k,D)$ 是空集。如果 $s(t)\leq D-1$ 不妨设 $(i,j)=(0,t)\in S_{t,u,-w}(k,D)$，容易知道 $0=h_t(0)=h_{0,t}$，所以 $h_t(z)$ 中非零系数的个数最多为 $2^{k-m}-1$，而 $h_t\left(\alpha^l\right)=0\left(s\leq l\leq s+2^{k-m}-2\right)$，得到 $h_t(z)\equiv 0$。综上，$h(x,y)$ 的所有系数 $h_{i,j}$ 都等于 0，即 $h\equiv 0$。

注：证明 $AI(F)\geq D(k,m)$ 的过程中没有用到 $F(a,0),a\in\mathbb{F}_{2^k}$，因此对任意 $F'(x,y):\mathbb{F}_{2^k}\times\mathbb{F}_{2^k}\to\mathbb{F}_2$ 满足 $F'(a,b)=F(a,b),b\in\mathbb{F}_q^*$，我们有不论 $F'(a,0)\left(a\in\mathbb{F}_q\right)$ 的值是多少 $AI(F')\geq D(k,m)$。

4.2. 一类具有最优代数免疫度的 Bent 函数

我们可以看出构造 1 中定义的布尔函数的非线性度随着 u,v 取值的变化而变化，我们考虑它可否成为非线性度达到最高的 bent 函数。

引理 1： 设 $n=2k\geq 4$，$\left(u,2^k-1\right)=1$。α 为 F_{2^k} 的本原元，设 $\Delta_s=\left\{\alpha^s,\alpha^{s+1},\cdots,\alpha^{s+2^{k-1}-1}\right\}$。其中 $0\leq s<2^k-1$，$s\in\mathbb{Z}$。定义 $f\in B_n$ 如下：$f(x,y)=g\left(x^w y^u\right),\left(w,2^k-1\right)=1$ 其中 g 是定义在 F_{2^k} 上满足 $supp(g)=\Delta_s$ 的布尔函数。当 $\frac{2^k-1-u}{w}=2^l$，$0\leq l<k$ 时，$f(x,y)$ 是 bent 函数。

证明： 我们仅需计算 $W_f(a,b)$。因为 $\omega t(f)=\left(2^k-1\right)\cdot 2^{k-1}=2^{2k-1}-2^{k-1}$，显然 $W_f(0,0)=2^k$。$(a,b)\in\mathbb{F}_{2^k}\times\mathbb{F}_{2^k}$ 且 $ab=0$ 时 $W_f(a,b)=2^k$。

对 $\forall(a,b)\in\mathbb{F}_{2^k}\times\mathbb{F}_{2^k}\setminus\{(0,0)\}$，有

$$W_f(a,b)=\sum_{(x,y)\in\mathbb{F}_{2^k}\times\mathbb{F}_{2^k}}(-1)^{f(x,y)+tr(ax+by)}=-2\sum_{(x,y)\in supp(f)}(-1)^{tr(ax+by)}$$

$$=-2\sum_{\gamma\in\Delta_s}\sum_{y\in\mathbb{F}_{2^k}^*}(-1)^{tr\left(a\gamma^{\frac{1}{w}}y^{\frac{2^k-1-u}{w}}+by\right)}=-2\sum_{\gamma\in\Delta_s}\sum_{y\in\mathbb{F}_{2^k}^*}(-1)^{tr\left(a\lambda^{\frac{1}{2^k-1-v}}y^{\frac{u}{2^k-1-v}}\right)+tr(by)}$$

。

令 $\frac{2^k-1-u}{w}=z$ 易知 $(z,2^k-1)=1$，那么一定存在唯一的 $\beta_\gamma\in\mathbb{F}_{2^k}^*$，使得 $\beta_\gamma{}^z=a\gamma^{\frac{1}{w}}$，而 $z=2^l$，所以 $tr\left(a\gamma^{\frac{1}{w}}y^z\right)=tr(\beta_\gamma y)$，于是我们有：$W_f(a,b)=-2\sum_{\lambda\in\Delta_s}\sum_{y\in\mathbb{F}_{2^k}^*}(-1)^{tr(\beta_\gamma y)+tr(by)}=-2\sum_{\lambda\in\Delta_s}\sum_{y\in\mathbb{F}_{2^k}^*}(-1)^{tr((\beta_\gamma+b)y)}$。

1) $\beta_\gamma+b\neq 0$，即对任意 $\gamma\in\Delta_s$，$a\gamma^{\frac{1}{w}}\neq b^z$，

$$W_f(a,b)=-2\sum_{\lambda\in\Delta_s}\left(\sum_{x\in\mathbb{F}_{2^k}}(-1)^{tr(x)}-(-1)^{tr(0)}\right)=2^k\ (\text{因为}\sum_{x\in\mathbb{F}_{2^k}}(-1)^{tr(x)}=0)$$

2) $\beta_\gamma+b=0$，即对一些 $\gamma_1\in\Delta_s$，$a\gamma_1^{\frac{1}{w}}=b^z$，

$$W_f(a,b)=-2\sum_{\gamma\in\Delta_s\setminus\{\gamma_1\}}\left(\sum_{x\in\mathbb{F}_{2^k}}(-1)^{tr(x)}-(-1)^{tr(0)}\right)-2\sum_{y\in\mathbb{F}_{2^k}^*}(-1)^0=-2\left(2^{k-1}-1\right)(-1)-2\left(2^k-1\right)=-2^k$$

注意到最多只存在一个 $\gamma\in\Delta_s$ 满足 $a\gamma^{\frac{1}{w}}=b^z$，对 $(a,b)\in\mathbb{F}_{2^k}^*\times\mathbb{F}_{2^k}^*$。

综上，对任意 $(a,b)\in\mathbb{F}_{2^k}\times\mathbb{F}_{2^k}$，$W_f(a,b)=\pm 2^k$ 所以 f 是 bent 函数。

注：事实上，这类 bent 函数是 Dillon 提出的 PS 类函数[13]。因为 $E_\lambda=\left\{\left(\lambda^{\frac{1}{2^k-1-v}}y^{2^l},y\right)\mid y\in\mathbb{F}_{2^k}\right\},\lambda\in\Delta_s$ 是 2^{k-1} 个 $\mathbb{F}_{2^{2k}}$ 的 k 维线性子空间且对于 $\lambda_1\neq\lambda_2$，$\lambda_1,\lambda_2\in\Delta_s$ 有 $E_{\lambda_1}\cap E_{\lambda_2}\neq\Phi$。

定理 2 令 F 是构造 1 中定义的多输出布尔函数，若 $\frac{2^k-1-u}{w}=2^l$，$0\le l<k$，那么 F 是具有最优代数免疫度的 bent 函数，

证明：要证明 F 是 bent 函数，我们需要证明 $F_v=F_v(x,y)=v_0f_0+\cdots+v_{m-1}f_{m-1}:\mathbb{F}_{2^n}=\mathbb{F}_{2^k}\times\mathbb{F}_{2^k}\to\mathbb{F}_2$ 对每个 $0\neq v=(v_0,v_1,\cdots,v_{m-1})\in\mathbb{F}_2^m$ 是 bent 函数。由 F 的定义知对于每个 $x\in\mathbb{F}_{2^k}$，$F_v(x,0)=0$。假设 $y\in\mathbb{F}_{2^k}^*$，那么对于每个 $c\in\mathbb{F}_2$ 都存在 $x,y\in\mathbb{F}_{2^k}$ 满足：$f_i(x,y)=c\Leftrightarrow x^wy^u\in\bigcup_{0\le b\le 2^m-1,b_i=c}A_b$，从而对每个 $\bar{b}=(b_0,b_1,\cdots,b_{m-1})\in\mathbb{F}_2^m$，$(f_0(x,y),\cdots,f_{m-1}(x,y))=\bar{b}\Leftrightarrow x^wy^u\in A_b$，$b=b_0+b_12+\cdots+b_{m-1}2^{m-1}$。

因此，$F_v(x,y)=1\Leftrightarrow x^wy^u\in A_b$ 对每个 $0\le b\le 2^m-1$ 满足 $v\cdot\bar{b}=v_0b_0+\cdots+v_{m-1}b_{m-1}=1\Leftrightarrow x^wy^u\in\bigcup_{0\le b\le 2^m-1,b_i=c}A_b$。

我们定义 $g_v=g_v(x):\mathbb{F}_{2^k}\to\mathbb{F}_2$ 为 $g_v=g_v(x)=\begin{cases}1, & \text{如果}x\in\bigcup_{0\le b\le 2^m-1,v\cdot b=1}A_b\\ 0, & \text{其他}\end{cases}$ 那么对于 $x,y\in\mathbb{F}_{2^k}$ $F_v(x,y)=g_v(x^wy^u)$。

对每个非零向量 $v=(v_0,v_1,\cdots,v_{m-1})\in\mathbb{F}_2^m$，方程 $v\cdot\bar{b}=1$ 的解 $\bar{b}\in\mathbb{F}_2^m$ 的个数是 2^{m-1} 因此 $\left|g_v^{-1}(1)\right|=\sum_{0\le b\le 2^m-1,v\cdot b=1}|A_b|=2^{m-1}\cdot 2^{k-m}=2^{k-1}$，即 g_v 是平衡的，由引理 1 知对每个 $0\neq v\in\mathbb{F}_2^m$，F_v 是 bent 函数，因此 F 是 bent 函数。

5. 具有最优代数免疫度的平衡布尔函数

平衡性是布尔函数又一个重要的密码学性质，一个非平衡的布尔函数其输出序列的随机性是最不理想的吗，易受区分攻击，bent 函数有最大的非线性度，但不是平衡的。这个部分我们将把构造 1 中布尔函数改造为平衡函数，同时也兼具好的代数免疫度和非线性度。

构造 2 令$1\le m\le k$， $n=2k\ge 4$， $0\le s,r\le 2^k-2$， α,β是$\mathbb{F}_{2^k}$的两个本原元。令$F'(x,y)=F(x,y)+G(x,y):\mathbb{F}_{2^n}=\mathbb{F}_{2^k}\times\mathbb{F}_{2^k}\to\mathbb{F}_2^m$其中$F(x,y)$是构造 1 中定义的布尔函数，$G(x,y)=(g_0(x,y),\cdots,g_{m-1}(x,y)):\mathbb{F}_{2^k}\times\mathbb{F}_{2^k}\to\mathbb{F}_2^m$定义为：

$$g_i(x,y)=\begin{cases}1, & y=0\text{且}x\in\bigcup\limits_{\substack{0\le b\le 2^m-1\\ b_i=1}}C_b\\ 0, & \text{其他}\end{cases},(0\le i\le m-1)$$

其中

$C_0=\{0\}\cup\{\beta^l\mid r\le l\le r+2^{k-m}-2\}$， $C_b=\{\beta^l\mid r+2^{k-m}b-1\le l\le r+2^{k-m}(b+1)-2\}(1\le b\le 2^m-1)$。

那么F'是平衡的，且$AI(F')\ge D(k,s)$， $nl(F')\ge 2^{n-1}-2^{k-1}-\frac{2^{\frac{k}{2}+m}}{\pi}\ln\left(\frac{4(2^k-1)}{\pi}\right)-1$。

证明：因为$F'^{-1}(b)$和$G^{-1}(b)$对任意$b\in\mathbb{F}_{2^k}$是不相交的所以$|F'^{-1}(b)|=|F^{-1}(b)|+|G^{-1}(b)|=(2^{n-m}-2^{k-m})+2^{k-m}=2^{n-m}$故$F'$是平衡的。$AI(F')\ge D(k,s)$的证明参照定理 1 后的注。现在只需证明$nl(F')\ge 2^{n-1}-2^{k-1}-\frac{2^{\frac{k}{2}+m}}{\pi}\ln\left(\frac{4(2^k-1)}{\pi}\right)-1$。

注意到$nl(F')=2^{n-1}-\frac{1}{2}\max\{|W_{v\cdot F'}(a,b)|:0\ne v\in\mathbb{F}_2^m,a,b\in\mathbb{F}_{2^k}\}$，其中：

$$v\cdot F'=\sum_{i=0}^{m-1}v_i f'=\sum_{i=0}^{m-1}v_i(f_i+g_i)=v\cdot F+v\cdot G,$$

$$\begin{aligned}W_{v\cdot F'}(a,b)&=\sum_{x,y\in\mathbb{F}_{2^k}}(-1)^{v\cdot F'(x,y)+Tr(ax+by)}\\&=\sum_{v\cdot G(x,y)=0}(-1)^{v\cdot F(x,y)+Tr(ax+by)}-\sum_{v\cdot G(x,y)=1}(-1)^{v\cdot F(x,y)+Tr(ax+by)}\\&=\sum_{x,y\in\mathbb{F}_{2^k}}(-1)^{v\cdot F(x,y)+Tr(ax+by)}-2\sum_{v\cdot G(x,y)=1}(-1)^{v\cdot F(x,y)+Tr(ax+by)}\\&=W_{v\cdot F}(a,b)-2\sum_{\substack{x\in\mathbb{F}_{2^k}\\ v\cdot G(x,0)=1}}(-1)^{Tr(ax)}\quad\left(Tr:\mathbb{F}_{2^k}\to\mathbb{F}_2\text{是迹映射}\right)\end{aligned}$$

因为$v\cdot G(x,y)=1$相当于$y=0$且$v\cdot F(x,0)=0$。

如果$a=0$，那么$W_{v\cdot F'}(0,b)=W_{v\cdot F}(0,b)-2\#\{x\in\mathbb{F}_{2^k}\mid v\cdot G(x,0)=1\}$。

而$W_{v\cdot F}(0,b)=\sum_{x,y\in\mathbb{F}_{2^k}}(-1)^{F_v(x,y)+Tr(by)}=\sum_{x\in\mathbb{F}_{2^k}}1+\sum_{\substack{x\in\mathbb{F}_{2^k}^*\\ y\in\mathbb{F}_{2^k}}}(-1)^{g_v(x^wy^u)+Tr(by)}=2^k+\sum_{y\ne 0}(-1)^{Tr(by)}\sum_{x\in\mathbb{F}_{2^k}}(-1)^{g_v(x^wy^u)}=2^k$

($g_v:\mathbb{F}_{2^k}\to\mathbb{F}_2$是证明定理 1 中构造的平衡函数)。

又$-2\#\{x\in\mathbb{F}_{2^k}\mid v\cdot G(x,0)=1\}=-2\sum_{\substack{0\le b\le 2^m-1\\ v\cdot b=1}}\#\{x\in\mathbb{F}_{2^k}\mid x\in C_b\}=-2\cdot 2^{m-1}\cdot 2^{k-m}=-2^k$所以$W_{v\cdot F}(0,b)=0$。

我们已经知道对于$a\in\mathbb{F}_{2^k}^*$， $|W_{v\cdot F}(a,b)|\le 2^k$且$-2\sum_{x\in\mathbb{F}_{2^k}}(-1)^{Tr(ax)}=\sum_{x\in\mathbb{F}_{2^k}}(-1)^{v\cdot G(x,0)+Tr(ax)}$，由文献[14]中定理 3 的证明我们知道$\sum_{x\in\mathbb{F}_{2^k}}(-1)^{v\cdot G(x,0)+Tr(ax)}\ge\frac{2^{\frac{k}{2}+m+1}}{\pi}\ln\left(\frac{4(2^k-1)}{\pi}\right)+1$。因此

$$nl(F') \geq 2^{n-1} - 2^{k-1} - \frac{2^{\frac{k}{2}+m}}{\pi} \ln\left(\frac{4\left(2^k-1\right)}{\pi}\right) - 1$$ 。

6. 总结与展望

我们发现当 $w=1, v=-1$ 时，所构造的多输出布尔函数就是文献[11]中的函数，也就是冯克勤教授等通过对 T-D 猜想的推广构造出的多输出布尔函数。这里本文的推广给出了可能的更一般的多输出布尔函数构造方法，能提供更多的布尔函数供研究所用，在本文中，我们基于 T-D 猜想构造出一般化的组合猜想，并将构造方法推广到多输出布尔函数中，构造出具有最优代数免疫度的多输出布尔函数，这时可以通过确定 v,u 的取值来讨论布尔函数的各种密码学性质，这样更多的布尔函数可被发现并应用。本文还存在一些待解决的问题，如这种构造方法是否比已有方法更优还待考证，不同 v,u 取值时构造出的布尔函数性质的比较，这类构造方法构造出的布尔函数与已有的多输出布尔函数的比较等等，都是以后的研究重点。

致　谢

本文工作受国家自然科学基金资助，涂自然等的研究成果给予了深厚的研究基础和启发，同时张喆琳硕士提供了重要的参考文献，在此一并致以衷心的感谢。

项目基金

国家自然科学基金 NSFC 11271040 资助项目。

参考文献 (References)

[1] Armknecht, F. (2004) Improving fast algebraic attacks: FSE 2004. Springer Verlag, 65-82.

[2] Batten, L.M. (2004) Algebraic attacks over GF(q): Cryptology-INDOCRYPT 2004. Springer Verlag, 84-91.

[3] Courtois, N. and Meier, W. (2003) Algebraic attacks on stream ciphers with linear feedback: Cryptology-EUROCRYPT 2003. Springer Verlag, 345-359.

[4] Courtois, N. (2003) Fast algebraic attacks on stream ciphers with linear feedback: Advances in Cryptology-CRYPTO 2003. Springer Verlag, 176-194.

[5] Meier, W., Pasalic, E. and Carlet, C. (2004) Algebraic attacks and decomposition of Boolean functions: Cryptology-EUROCRYPT 2004. Springer Verlag, 474-491.

[6] Rothaus, O.S. (1976) On bent functions. *Journal of Combinatorial Theory A*, **20**,300-305.

[7] Tu, Z. and Deng, Y. (2010) A conjecture about binary strings and its applications on constructing Boolean functions with optimal algebraic immunity. *Designs, Codes and Cryptography*, 1-14.

[8] Tang, D., Carlet, C. and Tang, X. Highly nonlinear Boolean functions with optimum algebraic immunity and good behavior against fast algebraic attacks. Cryptology ePrint Archive. http://eprint.iacr.org/2011/366.pdf

[9] Cohen, G. and Flori, J.P. On a generalized combinatorial conjecture involving addition mod 2^k-1. Cryptology ePrint Archive. http://eprint.iacr.org/2011/400.pdf

[10] Jin, Q., Liu, Z., Wu, B. and Zhang, X. A general conjecture similar to T-D conjecture and its applications in constructing Boolean functions with optimal algebraic immunity. Cryptology ePrint Archive. http://eprint.iacr.org/2011/515.pdf

[11] Feng, K. and Yang, J. (2011) Vectorial Boolean functions with good cryptographic properties. *International Journal of Foundations of Computer Science*, **22**, 1271-1282.

[12] MacWilliams, F.J. and Sloane, N.J.A. (1977) The Theory of Error-Correcting Codes. North-Holland, Amsterdam.

[13] Dillon, J.F. (1974) Elementary hadamard difference sets. Ph.D. Thesis, University of Maryland, College Park.

[14] Carlet, C. and Feng, K. (2009) An infinite class of balanced vectorial Boolean functions with optimal algebraic immunity and good nonlinearity. In: Xing, C., *et al*., Eds., *Proceedings of the IWCC* 2009, 1-11.