软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software, 2022,33(2):717−724 [doi: 10.13328/j.cnki.jos.006158]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

一种密码函数存在性证明的新方法*

尤启迪[1,2], 张习勇[2], 周 旋[2], 吴兆阳[2], 袁 野[2]

[1](清华大学 计算机科学与技术系, 北京 100084)

[2](天地一体化信息技术国家重点实验室, 北京 100086)

通信作者: 张习勇, E-mail: xiyong.zhang@hotmail.com

摘 要: 密码函数在密码学中具有重要的研究价值. 从组合的角度, 给出了一种密码函数不存在性证明的新方法, 并且得到了一些新结果, 部分结果优于已有结论, 这些结果可以部分证明不存在次数大于 2 的齐次旋转对称 bent 函数这一公开猜想. 同时, 利用多项式的最大公因子算法刻画了 2 次齐次旋转对称 bent 函数. 该方法也可以用于刻画其他形式的 bent 函数的存在性.

关键词: 旋转对称布尔函数; bent 函数; 傅里叶变换

中图法分类号: TP309

中文引用格式: 尤启迪, 张习勇, 周旋, 吴兆阳, 袁野. 一种密码函数存在性证明的新方法. 软件学报, 2022, 33(2): 717–724. http://www.jos.org.cn/1000-9825/6158.htm

英文引用格式: You QD, Zhang XY, Zhou X, Wu ZY, Yuan Y. New Method for Existence Proof of Some Cryptographic Functions. Ruan Jian Xue Bao/Journal of Software, 2022, 33(2): 717−724 (in Chinese). http://www.jos.org.cn/1000-9825/6158.htm

New Method for Existence Proof of Some Cryptographic Functions

YOU Qi-Di[1,2], ZHANG Xi-Yong[2], ZHOU Xuan[2], WU Zhao-Yang[2], YUAN Ye[2]

[1](Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China)

[2](State Key Laboratory of Space-Ground Integrated Information Technology, Beijing 100086, China)

Abstract: Cryptographic functions have important applications in the research of cryptography. This paper describes a more suitable approach to prove the nonexistence of some cryptographic functions, and obtain some new results, which support the conjecture that there are no homogeneous rotation symmetric bent functions of algebraic degree>2. Also, homogeneous degree 2 rotation symmetric bent functions are characterizedby using GCD of polynomials. The method presented in this paper can also be used to characterize the existence of other forms of bent functions.

Key words: rotation-symmetric Boolean functions; bent functions; Fourier transform

现代密码学的研究离不开密码函数, 密码函数一般用于构造密码算法的中心部件. 自从 Rothus[1]在 20 世纪 70 年代提出了 bent 函数后, bent 函数在过去的 40 多年有了深入的研究, 并且因其良好的密码学和组合学属性, 在加密算法和纠错编码中有了广泛的应用. 例如在对称密码中, bent 函数由于具有最大非线性度和差分平衡一致性, 可抵抗线性攻击和差分攻击, 用来构造密码算法的非线性部件.

近些年来, 齐次旋转对称(简记为 RotS)布尔函数因其理想的性质引起了人们的广泛关注[2−4]. 如: 这种函数可利用前面循环迭代来快速求值, 所以当密码算法对函数求值的效率要求较高时, 这类旋转对称形式的函数可以作为密码函数使用, 如 MD4 和 MD5 等消息摘要算法.

由于 bent 函数和旋转对称布尔函数都具有优良的密码学性质, 人们自然会问哪种类型的齐次旋转对称 bent 函数存在. 事实上, 文献[5−10]对齐次 bent 函数都有研究. 特别重要的是, 最近几年, 文献[11−13]给出了

* 基金项目: 国家自然科学基金(61572027)

收稿时间: 2020-02-17; 修改时间: 2020-04-29; 采用时间: 2020-09-07; jos 在线出版时间: 2021-08-03

旋转对称布尔 bent 函数的几种新构造. Stănică 和 Maitra[6,7]对变元个数在 10 以内的旋转对称 bent 函数进行了研究, 他们列举了变元个数为 8 时所有的旋转对称 bent 函数, 发现了 4·3776 个次数为 2 的函数. 但当变元个数为 10 时, 并没有发现次数为 3、4 和 5 的齐次旋转对称 bent 函数, 于是他们提出了如下猜想.

猜想 1.1. 不存在次数大于 2 的齐次旋转对称 bent 函数.

我们简要综述与该猜想证明相关的一些已有结果和证明方法. 注意到布尔 bent 函数本质上是 Hadamard 差集, Xia 等人[8]证明了对任意的 $n>3$, 不存在变元个数为 $2n$ 的次数为 n 的齐次 bent 函数. 通过利用一个布尔函数部分点的傅里叶谱值与其子函数的傅里叶谱值之间的关系, Meng 等人[9]得到了关于齐次 bent 函数次数的一个较低的上界. 在文献[14]中, Carsto 和 Medina 等人利用函数的傅里叶变换的线性递归关系, 给出了特殊的一类旋转对称布尔函数不是 bent 函数的证明.

定理 1.2. 假设 n 元旋转对称布尔函数 f 的简代数正规型为 $x_1\ldots x_d+x_1\ldots x_{d-1}$, $d\geqslant 5$, 则对于充分大的 n, f 不是 bent 函数.

在文献[10]中, Stănică 等人从具有缺项的函数的非线性度出发, 得到了如下的不存在性结论(见第 1 节布尔函数的简代数正规型表示).

定理 1.3. 假设 n 元齐次旋转对称布尔函数 f 的次数大于 3, 则以下结论成立.

1. 如果 f 的简代数正规型为 $x_1\ldots x_d$, 则 f 不是 bent 函数;
2. 如果 f 的简代数正规型为 $x_1\ldots x_d+x_1\ldots x_{d-1}x_{d+1}$, 且此时 n、d 满足: 当 $n\neq 1 (\mathrm{mod}\ d)$时, $\dfrac{n-2}{4}>\left\lfloor\dfrac{n}{d}\right\rfloor$; 当 $n=1 (\mathrm{mod}\ d)$时, $\dfrac{n}{4}>\left\lfloor\dfrac{n}{d}\right\rfloor$, 则 f 不是 bent 函数;
3. 如果 f 的简代数正规型为 $\boldsymbol{x}^{\boldsymbol{u}_1}+\boldsymbol{x}^{\boldsymbol{u}_2}+\ldots+\boldsymbol{x}^{\boldsymbol{u}_m}$, 则当 $d_f<\dfrac{n/2-1}{\lfloor n/d\rfloor}$时, f 不是 bent 函数, 其中,

$$d_f=\mathrm{Max}_i\{i_2-i_1,n+1-i_d\mid u_{i_1}^{(i)}=u_{i_2}^{(i)}=u_{i_d}^{(i)}=1,\text{满足}u_j^{(i)}=0,1\leqslant i_1<j<i_2\leqslant n,1\leqslant i\leqslant m\}.$$

利用更精细的计算取定变元后的子函数的谱值, Meng 等人[15]得到了更优的不存在性证明结果.

定理 1.4. 假设 n 元齐次旋转对称布尔函数 f 的次数大于 3, 则以下结论成立.

1. 如果 f 的简代数正规型为单项式 $\boldsymbol{x}^{\boldsymbol{u}}$, 则 f 不是 bent 函数;
2. 如果 f 的简代数正规型为 $\boldsymbol{x}^{\boldsymbol{u}_1}+\boldsymbol{x}^{\boldsymbol{u}_2}+\ldots+\boldsymbol{x}^{\boldsymbol{u}_m}$, 则当 $d_f\leqslant\dfrac{n}{2}$时, f 不是 bent 函数, 其中,

$$d_f=\mathrm{Max}_i\{i_2-i_1,n+1-i_d\mid u_{i_1}^{(i)}=u_{i_2}^{(i)}=u_{i_d}^{(i)}=1,u_j^{(i)}=0,1\leqslant i_1<j<i_2\leqslant n,1\leqslant i\leqslant m\}.$$

由此可见, 目前不存在性的证明结果离上述猜想的完全证明还有较大的差距. 其实, 利用较深刻的数论结果, 可以将 bent 函数的问题转化为组合的问题. 本文将从组合的角度出发, 给出一种不同的较适用于研究齐次旋转对称 bent 函数存在性的方法. 通过利用旋转对称布尔函数的旋转对称形式, 本文的方法可以证明更多无法通过定理 1.2–定理 1.4 得到的不存在性结果. 例如, 我们的结果表明: 其简代数正规型包含 $x_1\ldots x_d$ 的大多次数大于等于 3 的齐次旋转对称 bent 函数是不存在的; 当简代正规型满足一定条件时, 其次数具有上界 $d\leqslant\dfrac{3n}{8}$. 最后, 利用多项式的 GCD 算法, 本文给出了次数为 2 的齐次旋转对称 bent 函数的一个等价刻画. 本文的方法也可用于其他形式的 bent 函数的存在性证明.

1 预备知识

本节给出一些有关齐次旋转对称布尔函数和 bent 函数的预备知识和符号.

假设 $\mathbb{F}_2^n$ 为二元域$\mathbb{F}_2$上的 n 维向量空间, n 元布尔函数 $f(x_1,x_2,\ldots,x_n)$是 $\mathbb{F}_2^n$ 到$\mathbb{F}_2$的映射. 对 $\boldsymbol{x}=(x_1,x_2,\ldots,x_n)$, $\boldsymbol{u}=(u_1,u_2,\ldots,u_n)\in\mathbb{F}_2^n$, 记 $\boldsymbol{x}^{\boldsymbol{u}}=x_1^{u_1}x_2^{u_2}\ldots x_n^{u_n}$, 则任意的布尔函数 f 都有唯一的形式: $f(\boldsymbol{x})=\sum\limits_{\boldsymbol{u}\in U_f}\boldsymbol{x}^{\boldsymbol{u}}$, 其中, $U_f\subseteq\mathbb{F}_2^n$.

用$|\boldsymbol{u}|$表示$\boldsymbol{u}\in\mathbb{F}_2^n$的汉明重量, 则$f$的代数次数定义为$\mathrm{Max}\{|\boldsymbol{u}||\boldsymbol{u}\in U_f\}$. 下文中, 也将$\boldsymbol{u}$看成$\mathbb{F}_2^n$的一个子集合.

用$A||B$表示两组比特串A、B的串联, 用$\underbrace{1\ldots1}_{l}$(或$\underbrace{0\ldots0}_{l}$)表示长度为$l$的一串1(或0), 用$\underbrace{1*\ldots*1}_{l}$表示第1个和最后一个比特为1的长度为$l$的串.

在$\mathbb{F}_2$上定义一个运算$\oplus$为$x,y\in\mathbb{F}_2$, $x\oplus y=0$当且仅当$x=0$且$y=0$. $\oplus$可以用如下方式扩展至$\mathbb{F}_2^n$上: 对任意的$\boldsymbol{x},\boldsymbol{y}\in\mathbb{F}_2^n$, $\boldsymbol{x}\oplus\boldsymbol{y}=(x_1\oplus y_1,x_2\oplus y_2,\ldots,x_n\oplus y_n)$, 这样, 可在$\mathbb{F}_2^n$上定义乘法运算$\otimes$为

$$\boldsymbol{x}^{\boldsymbol{u}_1}\otimes\boldsymbol{x}^{\boldsymbol{u}_2}=\boldsymbol{x}^{\boldsymbol{u}_1\oplus\boldsymbol{u}_2},\quad \boldsymbol{x},\boldsymbol{u}_1,\boldsymbol{u}_2\in\mathbb{F}_2^n.$$

设$1\leqslant l\leqslant n$, 定义$\mathbb{F}_2^n$上的变换$\rho^l(\cdot)$为

$$\rho^l(x_1,x_2,\ldots,x_n)=(x_{n-l+1},x_{n-l+2},\ldots,x_n,x_1,\ldots x_{n-l}),$$

其中, 下标的运算按模n的意义进行. $\boldsymbol{x}\in\mathbb{F}_2^n$的周期$l_{\boldsymbol{x}}$定义为满足$\rho^l(\boldsymbol{x})=\boldsymbol{x}$的最小的$l$, 显然, $l_{\boldsymbol{x}}|n$且$l_{\boldsymbol{x}}=l_{\rho(\boldsymbol{x})}$.

定义 2.1. 一个布尔函数$f(\boldsymbol{x})$称为旋转对称的, 如果对所有的$\boldsymbol{x}\in\mathbb{F}_2^n$和$l\in[1,n]$, 下式都成立:

$$f(\boldsymbol{x})=f(\rho^l(\boldsymbol{x})).$$

显然, 一个旋转对称布尔函数具有如下形式:

$$f(\boldsymbol{x})=\sum_{1\leqslant i\leqslant m}\sum_{0\leqslant l\leqslant l_{\boldsymbol{u}_i}-1}\boldsymbol{x}^{\rho^l(\boldsymbol{u}_i)},$$

其中, $m\geqslant 1$, $\boldsymbol{u}_i\in\mathbb{F}_2^n(1\leqslant i\leqslant m)$. 因为$\boldsymbol{x}^{\boldsymbol{u}_i}$与$\boldsymbol{x}^{\rho(\boldsymbol{u}_i)}$是同时出现的, 所以我们可以用更加简洁的形式$\boldsymbol{x}^{\boldsymbol{u}_1}+\boldsymbol{x}^{\boldsymbol{u}_2}+\ldots+\boldsymbol{x}^{\boldsymbol{u}_m}$来表示旋转对称布尔函数, 这种形式称为$f$的简代数正规型.

定义 2.2. 布尔函数$f(\boldsymbol{x})$在点$\boldsymbol{c}\in\mathbb{F}_2^n$的傅里叶变换为

$$\hat{f}(\boldsymbol{c})=\sum_{\boldsymbol{x}\in\mathbb{F}_2^n}(-1)^{f(\boldsymbol{x})+\boldsymbol{c}\cdot\boldsymbol{x}},$$

其中, $\cdot$为空间$\mathbb{F}_2^n$上任两个向量的点积.

定义 2.3. 布尔函数$f(\boldsymbol{x})$称为bent函数, 如果对所有的$\boldsymbol{c}\in\mathbb{F}_2^n$, 都有$|\hat{f}(\boldsymbol{c})|=2^{n/2}$.

周知: 如果$f(x_1,x_2,\ldots,x_n)$是bent函数, 则n是偶数, 且其代数次数有上界$n/2(n\geqslant 4)$.

假设$f(\boldsymbol{x})=\boldsymbol{x}^{\boldsymbol{u}_1}+\boldsymbol{x}^{\boldsymbol{u}_2}+\ldots+\boldsymbol{x}^{\boldsymbol{u}_m}$, 定义:

$$h_f(\boldsymbol{u})=\sum_{\substack{0\leqslant t_1,\ldots,t_m\leqslant 1\\ t_1\boldsymbol{u}_1\oplus t_2\boldsymbol{u}_2\oplus\ldots\oplus t_m\boldsymbol{u}_m=\boldsymbol{u}}}(-2)^{t_1+t_2+\ldots+t_m},$$

可得出:

$$\hat{f}(\boldsymbol{c})=(-1)^{|\boldsymbol{c}|}\sum_{\boldsymbol{u}\succ\boldsymbol{c}}2^{n-|\boldsymbol{u}|}h_f(\boldsymbol{u}),$$

其中, $\succ$是$\mathbb{F}_2^n$上的偏序: $(u_1,u_2,\ldots,u_n)\succ(v_1,v_2,\ldots,v_n)$当且仅当$u_i=v_i$或$(u_i,v_i)=(1,0)$. 由于$\succ$是偏序, 可以算出上式的反演变换为

$$h_f(\boldsymbol{u})=(-1)^{|\boldsymbol{u}|}2^{|\boldsymbol{u}|-n}\cdot\sum_{\boldsymbol{c}\succ\boldsymbol{u}}\hat{f}(\boldsymbol{c}).$$

在文献[16,17]中, 根据上述公式和定义2.3, 得到:

引理 2.4. 假设n是偶数, $f(\boldsymbol{x})=\boldsymbol{x}^{\boldsymbol{u}_1}+\boldsymbol{x}^{\boldsymbol{u}_2}+\ldots+\boldsymbol{x}^{\boldsymbol{u}_m}$, 则$f$是bent函数当且仅当:

$$v_2(h_f(\boldsymbol{u}))\begin{cases}=n/2, & 若\boldsymbol{u}=\boldsymbol{1}\\ >|\boldsymbol{u}|-n/2, & 若\boldsymbol{u}\neq\boldsymbol{1}\end{cases},$$

其中, $v_2(\cdot)$是2-adic阶函数, $\boldsymbol{1}$表示向量$(1,1,\ldots,1)\in\mathbb{F}_2^n$.

2 主要结果

设f的简代数正规型为$\sum_{1\leqslant i\leqslant m}\boldsymbol{x}^{\boldsymbol{u}_i}$, 其中, $\boldsymbol{u}_i=(u_1^{(i)},u_2^{(i)},\ldots,u_n^{(i)})$. 对于任意的$i$, 设$|\boldsymbol{u}_i|=v_i$. 记$u_{i_j}^{(i)}=1$, $1\leqslant j\leqslant v_i$,

且 i_1=1. 令:

$$d_j^{(i)}=\begin{cases} i_{j+1}-i_j, & 1\leqslant j\leqslant v_i-1 \\ n+1-i_{v_i}, & j=v_i \end{cases}.$$

当函数为齐次旋转对称 bent 函数 f 时, 若 f 的次数为 d 齐次的, 则对于每个 $1\leqslant i\leqslant m$, $|\boldsymbol{u}_i|=d$. 由于函数的代数形式为旋转对称形式的, 因此不妨设 $d_{v_i}^{(i)}=\mathrm{Max}\{d_j^{(i)}\,|\,1\leqslant j\leqslant v_i\}$, $1\leqslant i\leqslant m$.

假设:

$$D_i=\mathrm{Max}\{k\,|\,u_k^{(i)}=1,1\leqslant k\leqslant n\},1\leqslant i\leqslant m,$$
$$D_1=\mathrm{Min}\{D_i\,|\,1\leqslant i\leqslant m\},$$

令 $\boldsymbol{u_0}=\boldsymbol{u}_1\oplus\rho^{D_1}(\boldsymbol{u}_1)\oplus\ldots\oplus\rho^{(k-1)D_1}(\boldsymbol{u}_1)$, 其中, k 满足 $kD_1<n$, 且$(k+1)D_1\geqslant n$.

定理 3.1. 假设齐次旋转对称 bent 函数 f 的次数 $d\geqslant 3$, f 的简代数正规型为 $\sum_{1\leqslant i\leqslant m}\boldsymbol{x}^{\boldsymbol{u}_i}$. 设$|\boldsymbol{u}_0|=kd$. 若关于 e_{ij} $(1\leqslant i\leqslant m,1\leqslant j\leqslant n)$的方程 $\mathop{\oplus}_{1\leqslant i\leqslant m}\mathop{\oplus}_{1\leqslant j\leqslant n}e_{ij}\rho^j(\boldsymbol{u}_i)=\boldsymbol{u_0},e_{ij}=0,1$ 满足 $\sum_{1\leqslant i\leqslant m,1\leqslant j\leqslant n}e_{ij}=k$ 的解唯一, 则 $k\cdot(d-1)<\dfrac{n}{2}$.

证明: 因为$|\boldsymbol{u}_i|=d$, $1\leqslant i\leqslant m$, $|\boldsymbol{u}_0|=kd$, 可推出:

$$\mathrm{Min}\left\{\sum_{1\leqslant i\leqslant m,1\leqslant j\leqslant n}e_{ij}\,\middle|\,\mathop{\oplus}_{1\leqslant i\leqslant m}\mathop{\oplus}_{1\leqslant j\leqslant n}e_{ij}\rho^j(\boldsymbol{u}_i)=\boldsymbol{u_0},e_{ij}=0,1\right\}=k.$$

根据假设可知, 方程 $\mathop{\oplus}_{1\leqslant i\leqslant m}\mathop{\oplus}_{1\leqslant j\leqslant n}e_{ij}\rho^j(\boldsymbol{u}_i)=\boldsymbol{u_0},e_{ij}=0,1$ 满足 $\mathrm{Min}\left\{\sum_{1\leqslant i\leqslant m,1\leqslant j\leqslant n}e_{ij}\right\}=k$ 的唯一解为

$$\boldsymbol{u_0}=\boldsymbol{u}_1\oplus\rho^{D_1}(\boldsymbol{u}_1)\oplus\ldots\oplus\rho^{(k-1)D_1}(\boldsymbol{u}_1).$$

因此可得 $v_2(h_f(\boldsymbol{u}_0))=k$. 而 $kD_1<n$, $\boldsymbol{u}_0\neq\boldsymbol{1}$, 由引理 2.4 可知: $v_2(h_f(\boldsymbol{u}_0))=k>|\boldsymbol{u}_0|-\dfrac{n}{2}=kd-\dfrac{n}{2}$, 故 $k\cdot(d-1)<\dfrac{n}{2}$. 证毕. □

由上定理, 可得:

推论 3.2. 如果 f 为 bent 函数, 其简代数正规型为 $\sum_{1\leqslant i\leqslant m}\boldsymbol{x}^{\boldsymbol{u}_i},\boldsymbol{u}_l=A_l\,\|\,B_{D_1-l}\,\|\,\underbrace{0\ldots0}_{n-D_1}$, $1\leqslant l\leqslant D_1$, 其中, $A_l=\underbrace{1*\ldots*1}_{l},B_{D_1-l}=\underbrace{1*\ldots*1}_{D_1-l}$, 满足$\forall i_1,i_2,j(1\leqslant i_1,i_2\leqslant m)$, $(1<j<D_{i_1}),\boldsymbol{u}_{i_1}\cap\rho^j(\boldsymbol{u}_{i_2})\neq\varnothing$; 且对所有的 $1\leqslant i\leqslant m$, 有 $\boldsymbol{u}_i\neq A_l\,\|\,\underbrace{0\ldots0}_{D_i-D_1}\|\,B_{D_1-l}\,\|\,\underbrace{0\ldots0}_{n-D_i}$, 且 $\boldsymbol{u}_i\neq B_{D_1-l}\,\|\,\underbrace{0\ldots0}_{n-kD_1}\|\,A_l\,\|\,\underbrace{0\ldots0}_{kD_1-D_1}$, 则当 $kD_1<n$ 时, $k\cdot(d-1)<\dfrac{n}{2}$.

证明: 对于 $\boldsymbol{u_0}=\boldsymbol{u}_1\oplus\rho^{D_1}(\boldsymbol{u}_1)\oplus\ldots\oplus\rho^{(k-1)D_1}(\boldsymbol{u}_1)$, 由于$|\boldsymbol{u}_0|=k|\boldsymbol{u}_1|$, 且函数 f 是齐次的 RSBF, 故:

$$\mathrm{Min}\left\{\sum_{1\leqslant i\leqslant m,1\leqslant j\leqslant n}e_{ij}\,\middle|\,\mathop{\oplus}_{1\leqslant i\leqslant m}\mathop{\oplus}_{1\leqslant j\leqslant n}e_{ij}\rho^j(\boldsymbol{u}_i)=\boldsymbol{u}_0,e_{ij}=0,1\right\}=k.$$

由于$\forall i_1,i_2,j(1\leqslant i_1,i_2\leqslant m)$, $(1<j<D_{i_1}),\boldsymbol{u}_{i_1}\cap\rho^j(\boldsymbol{u}_{i_2})\neq\varnothing$, 可知满足上式的一组$\rho^j(\boldsymbol{u}_1)$只能由$\rho^j(\boldsymbol{u}_1)$通过级联的方式来拼接成 $\boldsymbol{u}_0$(否则, 由 $\boldsymbol{u}_{i_1}\cap\rho^j(\boldsymbol{u}_{i_2})\neq\varnothing$, 若通过非级联的方式得到 $\boldsymbol{u}_0$, 则会出现重复的 1, 而使得 k 个 $\rho^j(\boldsymbol{u}_1)$的组合后的向量的 Hamming 重量小于 $k\cdot d$).

又由于对所有的 $1\leqslant i\leqslant m$, 有 $\boldsymbol{u}_i\neq A_l\,\|\,\underbrace{0\ldots0}_{D_i-D_1}\|\,B_{D_1-l}\,\|\,\underbrace{0\ldots0}_{n-D_i}$, 且 $\boldsymbol{u}_i\neq B_{D_1-l}\,\|\,\underbrace{0\ldots0}_{n-kD_1}\|\,A_l\,\|\,\underbrace{0\ldots0}_{kD_1-D_1}$, 可知 $\boldsymbol{u}_0$ 不可通过 $\boldsymbol{u}_i$ $(1\leqslant i\leqslant m)$的其他级联方式得到.

因此, 满足 $\sum_{1\leqslant i\leqslant m,1\leqslant j\leqslant n}e_{ij}=k$ 的解唯一.

由定理 3.1 可知: 当 f 是 d 次 bent 函数, 且 $kD_1<n$ 时, 有 $k\cdot(d-1)<\dfrac{n}{2}$. □

上述定理以及推论表明很多旋转对称 bent 函数的不存在性. 例如, 可得如下结论.

命题 3.3. 齐次旋转对称布尔函数 f 的次数 $d\geqslant 3$, 则以下不存在性结论成立.

(1) 如果 f 的简代数正规型 $\sum_{1\leqslant i\leqslant m}\boldsymbol{x}^{\boldsymbol{u}_i}$ 包含 $\boldsymbol{x}^{\boldsymbol{u}_1}=x_1x_2...x_d$, 且 $\boldsymbol{u}_i(2\leqslant i\leqslant m)$的形式不是 $\underbrace{1...1}_{l}\underbrace{0...0}_{D_1-d}\underbrace{1...1}_{d-l}\underbrace{0...0}_{n-D_1}$, 则 f 不是 bent 函数;

(2) 如果 f 的简代数正规型为 $x_1\ldots x_d+x_1\ldots x_{d-1}x_{d+1}$, 则 f 不是 bent 函数;

(3) 设 n 元旋转对称函数 f 的简代数正规型为 $\sum_{1\leqslant i\leqslant m}\boldsymbol{x}^{\boldsymbol{u}_i}$, 其中, $\boldsymbol{u}_i(1\leqslant i\leqslant m)$满足定理 3.1 的条件, 且 $n=kD_1+r$, $0<r\leqslant D_1$, 则当 f 为 bent 函数时, $D_1>\dfrac{2k(d-1)}{k+1}$. 进一步有, $d\leqslant\dfrac{n}{4}\left(1+\dfrac{1}{k}\right)$.

证明:

(1) 如果 $d\nmid n$, 令 $n=qd+r$, $0<r<d$, $q\geqslant 2$. 因为 $\boldsymbol{x}^{\boldsymbol{u}_1}=x_1x_2...x_d$, 且 $\boldsymbol{u}_i(2\leqslant i\leqslant m)$的形式不是 $\underbrace{1...1}_{l}\underbrace{0...0}_{D_1-d}\underbrace{1...1}_{d-l}\underbrace{0...0}_{n-D_1}$, 利用推论 3.2 可知, $k\cdot(d-1)<\dfrac{n}{2},1\leqslant k\leqslant\left\lfloor\dfrac{n}{d}\right\rfloor$.

令 $k=\left\lfloor\dfrac{n}{d}\right\rfloor=q$, 则 $qd<2q+r<2q+d$, 可得 $d<2+\dfrac{2}{q-1}$.

(1.1) 若 $q=2$, 则 $d<2+\dfrac{2}{q-1}=4$, 于是 d 只能为 3, 再次由 $qd<2q+r$ 得 $r>3$, 与 $r<d=3$ 矛盾.

(1.2) 若 $q=3$, 则 $d<2+\dfrac{2}{q-1}=3$, 与 $d\geqslant 3$ 矛盾.

(1.3) 若 $q\geqslant 4$, 则 $d<2+\dfrac{2}{q-2}<3$, 与 $d\geqslant 3$ 矛盾.

如果 $d|n$, 令 $n=qd$, $q\geqslant 2$. 取 $k=\left\lfloor\dfrac{n}{d}\right\rfloor-1=q-1$. 类似地, 利用推论 3.2 可得 $(q-1)(d-1)<\dfrac{n}{2}=\dfrac{qd}{2}$, 于是 $d<2+\dfrac{2}{q-2}$.

(1.4) 若 $q=2$, 则 $n=2d$. 取 $\boldsymbol{u}_0=\boldsymbol{u}_1\oplus\rho^{d-1}(\boldsymbol{u}_1)=\underbrace{1...1}_{n-1}\|0$.

同理可得 $v_2(h_f(\boldsymbol{u}_0))=2$. 由引理 2.4 知 $v_2(h_f(\boldsymbol{u}_0))=2>|\boldsymbol{u}_0|-\dfrac{n}{2}=n-1-\dfrac{n}{2}$, 故 $n<6$, 故 $d=n/2<3$, 与 $d\geqslant 3$ 矛盾.

(1.5) 若 $q=3$, 则 $d<2+\dfrac{2}{q-2}=4$. 故 $d=3$ 且 $n=qd=9$. 显然这是不可能的, 因 bent 函数的变元个数为偶数.

(1.6) 若 $q\geqslant 4$, 则 $d<2+\dfrac{2}{q-2}<3$, 与 $d\geqslant 3$ 矛盾.

(2) 记 $\boldsymbol{u}_1=\underbrace{1...1}_{d}\|\underbrace{0...0}_{n-d},\boldsymbol{u}_2=\underbrace{1...1}_{d-1}\|0\|1\|\underbrace{0...0}_{n-d-1}$, 则 f 的简代数正规型为 $\boldsymbol{x}^{\boldsymbol{u}_1}+\boldsymbol{x}^{\boldsymbol{u}_2}$. 若 $n\neq 0,1(\mathrm{mod}\ d)$, 令 $n=qd+r$, $1<r<d$, $q\geqslant 2$, 取 $\boldsymbol{u}_0=\boldsymbol{u}_1\oplus\rho^{D_1}(\boldsymbol{u}_1)\oplus...\oplus\rho^{(q-1)D_1}(\boldsymbol{u}_1)=\underbrace{1...1}_{qd}\|\underbrace{0...0}_{r}$, 则易得到 $v_2(h_f(\boldsymbol{u}_0))=q$.

由推论 3.2 可得 $q\cdot(d-1)<\dfrac{n}{2}$, 故 $qd<2q+r<2q+d$, 剩下的证明与步骤(1.1)–步骤(1.3)类似.

若 $n\equiv 0(\mathrm{mod}\ d)$, 令 $n=qd$, $q\geqslant 2$, 取 $\boldsymbol{u}_0=\boldsymbol{u}_1\oplus\rho^{D_1}(\boldsymbol{u}_1)\oplus...\oplus\rho^{(q-2)D_1}(\boldsymbol{u}_1)=\underbrace{1...1}_{(q-1)d}\|\underbrace{0...0}_{d}$, 类似由定理 3.1 可得 $d<2+\dfrac{2}{q-2}$, 分 $q=2$、$q=3$ 和 $q\geqslant 4$ 这 3 种情况讨论, 而 $q=3$ 和 $q\geqslant 4$ 和证明分别与步骤(1.5)、步骤(1.6)类似.

若 $q=2$, 令 $n=2d$. 取 $\boldsymbol{u}_0=\boldsymbol{u}_1\oplus\rho^{d-2}(\boldsymbol{u}_1)=\underbrace{1...1}_{2d-2}\|00$, 可得 $v_2(h_f(\boldsymbol{u}_0))=2$, 则根据引理 2.4 可得:

$$v_2(h_f(\boldsymbol{u}_0))=2>2d-2-n/2.$$

因此 $d<4$. 因 $d\geqslant 3$, 故 $d=3$, $n=6$. 然而可以验证, 简代数正规型为 $x_1x_2x_3+x_1x_2x_4$ 的 6 元旋转对称布尔函数不是 bent 函数.

还有一种情况为 $n\equiv 1(\bmod d)$. 假设 $n=qd+1$, 取 $\boldsymbol{u_0}=\boldsymbol{u}_1\oplus\rho^{D_1}(\boldsymbol{u}_1)\oplus\ldots\oplus\rho^{(q-2)D_1}(\boldsymbol{u}_1)=\underbrace{1\ldots1}_{(q-1)d}\|\underbrace{0\ldots0}_{d+1}$.

同理可得 $d<2+\dfrac{1}{q-2}$. 如果 $q>2$, 则 $d<3$ 与 $d\geqslant 3$ 矛盾. 如果 $q=2$, 则 $n=2d+1$, 而变元个数为奇数的 bent 函数是不存在的.

(3) 设 $n=kD_1+r$, $0<r\leqslant D_1$, 若 f 是 bent 函数, 且其简代数正规型满足定理 3.1 的条件, 则由定理 3.1 可知, $k\cdot(d-1)<\dfrac{n}{2}$. 若 $D_1\leqslant\dfrac{2k(d-1)}{k+1}$, 则:

$$2k\cdot(d-1)<n=k\cdot D_1+r\leqslant(k+1)\cdot D_1\leqslant(k+1)\cdot\frac{2k(d-1)}{k+1}=2k\cdot(d-1).$$

因此得到矛盾. 故 $D_1>\dfrac{2k(d-1)}{k+1}$.

进一步地, $D_1>n+1-d_d^1$, 由定理 1.3 可知, $d_d^1>n/2$, 得到 $D_1\leqslant n/2$, 故 $\dfrac{2k(d-1)}{k+1}<D_1\leqslant n/2$.

这样就有, $d\leqslant\dfrac{n}{4}\left(1+\dfrac{1}{k}\right)$. □

注 3.4. 可以看出, 上述的不存在性结论不能通过定理 1.3 得到, 例如, 简代数正规型为 $x_1x_2\ldots x_d+x_1x_2\ldots x_{d-1}x_{d+1}$ 的齐次旋转对称 bent 函数的不存在性不可通过定理 1.3 证明得到. 类似地, 利用推论 3.2, 也可证明简代数正规型为 $x_1x_2\ldots x_d+x_1x_2\ldots x_{d-1}$ 的旋转对称 bent 函数($d\geqslant 3$)是不存在的, 从而改进了定理 1.2 的结果.

注 3.5. 由上述第 3 条可知: 当 f 是 bent 函数时, 最短的 $\boldsymbol{u}_1$ 的长度 D_1 不能太小(如应约大于 $2d$). 当 $D_1<n/2$ 时, $k\geqslant 2$, 故其代数次数有上界 $d\leqslant\dfrac{n}{4}\left(1+\dfrac{1}{k}\right)\leqslant\dfrac{3n}{8}$.

注 3.6. 文献[18]中的叙述"次数大于等于 3 的单圈(即简代数正规型为 $\boldsymbol{x^u}$)齐次旋转对称 bent 函数不存在性证明"是不正确的. 作者证明的基础是假设所有的单圈旋转对称布尔函数仿射等价于简代数正规型为 $x_1x_2\ldots x_d$ 的旋转对称布尔函数. 事实上, 单圈旋转对称布尔函数并不等价于简代数正规型为 $x_1x_2\ldots x_d$ 的旋转对称布尔函数.

下面我们给出次数为 2 的齐次旋转对称 bent 函数的一个特征, 首先给出两个关于 bent 函数和循环矩阵的结论. $\mathbb{F}_2$ 上的循环矩阵的形式为

$$\begin{pmatrix}\boldsymbol{a}_1\\ \rho(\boldsymbol{a}_1)\\ \vdots\\ \rho^{n-1}(\boldsymbol{a}_1)\end{pmatrix},$$

其中, $\boldsymbol{a}_1=(a_{11},a_{12},\ldots,a_{1n})\in\mathbb{F}_2^n$. 因此, 我们可以用第 1 行的向量 $\boldsymbol{a}_1$ 来代表循环矩阵. 进一步, 可以用首行所对应的多项式 $\sum\limits_{1\leqslant j\leqslant n}a_{1j}x^{j-1}\in\mathbb{F}_2[x]$ 来代表一个循环矩阵. 下面是关于 bent 函数和循环矩阵的两个周知的结果.

引理 3.7. 二次布尔函数 $f(x_1,x_2,\ldots,x_n)=\sum\limits_{1\leqslant i\leqslant j\leqslant n}a_{ij}x_ix_j+\sum\limits_{1\leqslant i\leqslant n}b_ix_i$ 为 bent 函数当且仅当矩阵 $(a_{ij})_{n\times n}$ 是非奇异的, 其中, $a_{ij}=a_{ji}\in\mathbb{F}_2$, $a_{ii}=0$, $1\leqslant i,j\leqslant n$.

引理 3.8. $\mathbb{F}_2$ 上的循环矩阵 $(a_{ij})_{n\times n}$ 是非奇异的当且仅当多项式 $\sum\limits_{1\leqslant j\leqslant n}a_{1j}x^{j-1}$ 与 x^n+1 是互素的, 即:

$$GCD\left(\sum_{1\leqslant j\leqslant n}a_{1j}x^{j-1},x^n+1\right)=1.$$

可验证 $\sum_{1\leqslant i\leqslant n} x_i x_{e-1+i}(e>n/2)$ 与 $\sum_{1\leqslant i\leqslant n} x_i x_{n-e+1+i}(n-e+2\leqslant n/2+1)$ 是相等的, 因此我们可以假设2次齐次旋转对称布尔函数的简代数正规型为 $x_1x_{e_1}+x_1x_{e_2}+...+x_1x_{e_m}$, 其中, $2\leqslant e_1<e_2<\ldots<e_m\leqslant n/2+1$, $m\leqslant n/2$. 显然, f 的关联矩阵$(a_{ij})_{n\times n}$是循环的, 且其第 1 行向量$(a_{11},a_{12},\ldots,a_{1n})$满足:

$$a_{11}=0, a_{1e_i}=a_{1(n+2-e_i)}=1, 1\leqslant i\leqslant m,$$

$$a_{1j}=0, \text{如果} j\neq e_i \text{或} n+2-e_i.$$

故该循环矩阵用多项式表示为 $\sum_{1\leqslant i\leqslant m}(x^{e_i-1}+x^{n+1-e_i})$, 其中, 当 $e_i-1=n+1-e_i=n/2$ 时, 假设 $x^{e_i-1}+x^{n+1-e_i}$ 为 $x^{n/2}$. 由引理 3.7 与引理 3.8, 可得:

定理 3.9. 上述定义的 2 次齐次旋转对称布尔函数是 bent 函数当且仅当:

$$GCD\left(\sum_{1\leqslant i\leqslant m}(x^{e_i-1}+x^{n+1-e_i}), x^n+1\right)=1.$$

注 3.10. $GCD\left(\sum_{1\leqslant i\leqslant m}(x^{e_i-1}+x^{n+1-e_i}), x^n+1\right)=1$ 成立的一个必要条件为: 单项式 $x^{n/2}$ 包含在 $\sum_{1\leqslant i\leqslant m}(x^{e_i-1}+x^{n+1-e_i})$ 中, 即 f 的简代数正规型中包含 $x_1x_{n/2+1}$. 例如, 所有变元个数为 8 的 2 次齐次旋转对称 bent 函数如下(用简代数正规型表示[7]):

x_1x_5; $x_1x_2+x_1x_5$; $x_1x_3+x_1x_5$; $x_1x_4+x_1x_5$; $x_1x_2+x_1x_3+x_1x_5$; $x_1x_2+x_1x_4+x_1x_5$; $x_1x_3+x_1x_4+x_1x_5$; $x_1x_2+x_1x_3+x_1x_4+x_1x_5$.

3 结束语

密码学是信息安全的基石, 密码学的中心研究问题包括密码算法的设计与分析等, 而这需要进行函数的密码学性质的研究. 一般的密码学性质包括非线性度、相关免疫度、低差分一致性、代数免疫度等, 其中, 非线性度和相关免疫度的研究可归结为指数和的计算问题, 但一般函数的指数和的计算不是一件容易的事情. 将指数和转化为函数代数表达式的系数的计算, 这样可从组合的角度来计算函数的傅里叶系数. 本文的这种新方法可以从函数的代数表达式来直接判断函数是否为 bent 函数、弹性函数等, 因而较适合这类问题的研究.

References:

[1] Rothus OS. On bent functions. Journal of Combinatorial Theory Series A, 1976, 20: 300−305.

[2] Pieprzyk J, Qu CX. Fast hashing and rotation symmetric functions. Journal of Universal Computer Science, 1999, 5(1): 20−31.

[3] Cusik TW, Stănică P. Fast evaluation, weights and nonlinearity of rotation-symmetric functions. Discrete Mathematics, 2002, 258: 289−301.

[4] Kavut S, Maitra S, Yucel MD. Search for Boolean functions with excellent profiles in the rotation symmetric class. IEEE Trans. on Information Theory, 2007, 53(5): 1743−1751.

[5] Charnes C, Rötteler, Beth T. Homogeneous bent functions, invariants, and designs. Designs, Codes and Cryptography, 2002, 26(1-3): 139−154.

[6] Stănică P, Maitra S. Rotation symmetric Boolean functions-count and cryptographic properties. In: Bose RC, ed. Proc. of the Centenary Symp. on Discrete Mathematics and Applications. 2002. 15.

[7] Stănică P, Maitra S. Rotation symmetric Boolean functions-count and cryptographic properties. Discrete Applied Mathematics, 2008, 156: 1567−1580.

[8] Xia T, Seberry J, Pieprayk J, Charnes C. Homogeneous bent functions of degree n in $2n$ variables do not exist for $n>3$. Discrete Applied Mathematics, 2004, 142: 127−132.

[9] Meng Q, Zhang H, Yang M, Cui J. On the degree of homogeneous bent functions. Discrete Applied Mathematics, 2007, 155: 665−669.

[10] Stănică P. On the nonexistence of homogeneous rotation symmetric bent Boolean functions of degree greater than two. In: Proc. of the Cryptology and Information Security. 2008. 214−218.

[11] Gao GP, Zhang XY, Liu WF. Constructions of rotation symmetric Boolean bent functions. IEEE Trans. on Inform. Theory, 2012, 58(7): 4908−4913.

[12] Su S, Tang X. Systematic constructions of rotation symmetric Bent functions, 2-rotation symmetric Bent functions, and Bent idempotent functions. IEEE Trans. on Information Theory, 2017, 63(7): 4658−4667.

[13] Tang C, Qi Y, Zhou Z. Two infinite classes of rotation symmetric bent functions with simple representation. Applicable Algebra in Engineering, Communication and Computing, 2018, 29(3): 197−208.

[14] Castro FN, Medina LA, Stănică P. Generalized Walsh transforms of symmetric and rotation symmetric Boolean functions are linear recurrent. Applicable Algebra in Engineering Communication Computing, 2018, 29: 433−453.

[15] Meng Q, Chen L, Fu FW. On homogeneous rotation symmetric bent functions. Discrete Applied Mathematics, 2010, 158(10): 1111−1117.

[16] Hou XD. *p*-ary and *q*-ary versions of certain results about bent functions and resilient functions. Finite Fields and Their Applications, 2004, 10: 566−582.

[17] Carlet C, Guillot P. Bent resilient functions and the numerical normal form. In: Codes and Association Schemes, DIMACS Series in Discrete Mathematics and Theoretical Computer Science. American Mathematical Society, 2001, 56: 87−96.

[18] Stănică P, Maitra S, Clark JA. Results on rotation symmetric Bent and correlation immune Boolean functions. Fast Software Encryption, 2014, 3017: 161−177.

尤启迪(1982－), 男, 研究员, CCF 会员, 主要研究领域为密码学.

吴兆阳(1988－), 男, 高级工程师, 主要研究领域为网络与信息安全.

张习勇(1975－), 男, 博士, 副教授, 主要研究领域为密码学.

袁野(1988－), 男, 高级工程师, 主要研究领域为密码学.

周旋(1976－), 男, 研究员, 主要研究领域为密码学.