一种计算旋转对称布尔函数的汉明重量和非线性度的新方法

张习勇[①②④] 祁应红[*①] 高光普[③] 李玉娟[④]
[①](信息工程大学 郑州 450002)
[②](数学工程与先进计算国家重点实验室 无锡 214215)
[③](洛阳外国语学校 洛阳 471003)
[④](信息保障技术重点实验室 北京 100072)

摘 要：旋转对称布尔函数是一类重要的密码学函数，研究其重量和非线性度等密码学性质具有很好的理论价值。区别于已有的计算方法，该文利用特定的正规基把这些布尔函数的问题转化为有限域上的指数和问题，得到了$4\nmid n$和$n=2^s$时一些二次旋转对称布尔函数的重量和非线性度的新结果。使用所提的方法，可以计算几乎全部的二次旋转对称布尔函数的重量和非线性度。所提的新方法对于研究一般的旋转对称布尔函数具有一定的参考意义。

关键词：密码学；旋转对称布尔函数；非线性度；汉明重量；正规基
中图分类号： TN918 **文献标识码**： A **文章编号**：1009-5896(2015)11-2691-06
DOI: 10.11999/JEIT 150164

A New Method for Evaluation of Hamming Weight and Nonlinearity of Rotation-symmetric Boolean Functions

Zhang Xi-yong[①②④] Qi Ying-hong[①] Gao Guang-pu[③] Li Yu-juan[④]
[①](*Information Engineering University*, *Zhengzhou* 450002, *China*)
[②](*State Key Laboratory of Mathematical Engineering and Advanced Computing*, *Wuxi* 214215, *China*)
[③](*Luoyang University of Foreign Languages*, *Luoyang* 471003, *China*)
[④](*Science and Technology on Information Assurance Laboratory*, *Beijing* 100072, *China*)

Abstract: Rotation-symmetric Boolean function is a class of Boolean functions with good cryptographic properties, and researches on its weight and nonlinearity cryptographic properties have good theoretical value. Different from the conventional calculation method, in this paper, these problems are converted to the evaluation of exponential sum on finite fields with a specific normal basis. Some new results about the weight and nonlinearity of some rotation-symmetric Boolean functions of degree 2 with $4\nmid n$ and $n=2^s$ are obtained. Using the proposed method, the weight and nonlinearity of almost all Rotation-symmetric Boolean functions of degree 2 can be evaluated. This new method is also interesting for studies on the other Boolean functions.

Key words: Cryptography; Rotation-symmetric Boolean functions; Nonlinearity; Hamming weight; Normal bases

1 引言

布尔函数在现代密码学中有着广泛的应用，很多学者致力于其性质和应用的研究。1999 年，Pieprzyk 等人[1]提出了旋转对称布尔函数的概念，这类布尔函数在输入变量旋转变化时，其函数值保持不变。人们在研究中发现这种类型的布尔函数具有良好的密码学性质，并将其应用于如 MD4, MD5, HAVAL 等一些摘要算法中。对这种类型的布尔函数的非线性度和汉明重量的研究取得了很好的结果。例如在 2002 年，Cusick 等人[2]研究了一类二次旋转对称布尔函数的快速求值，得到了该类布尔函数的重量，并且给出了当变元个数为偶数时此类函数的非线性度。同时他们通过分析实验数据，提出了一个猜想：旋转对称布尔函数$f(x_0,x_1,\cdots,x_{n-1})=\sum_{i=0}^{n-1}x_ix_{i+1}x_{i+2}$的非线性度和其汉明重量相等。2010 年，Ciungu[3]证明了该猜想在变元个数为 3 的倍数时是成立的，2011 年，Zhang 等人[4]证明了上述猜想。2012 年，Wang 等人[5]将此猜想推广到了次数为 4 的旋转对称布尔函数，证明了$f(x_0,x_1,\cdots,x_{n-1})=\sum_{i=0}^{n-1}x_ix_{i+1}x_{i+2}x_{i+3}$的非线性度与其汉明重量相等。

近来，人们分别研究了旋转对称布尔函数的非

收稿日期：2015-01-29；改回日期：2015-06-11；网络出版：2015-07-27
*通信作者：祁应红 yinghong_qi@163.com
基金项目：国家自然科学基金(61402522, 60803154, 61572027)；数学工程与先进计算国家重点实验室课题；信息保障技术重点实验室开放基金(KJ-13-108)
Foundation Items: The National Natural Science Foundation of China (61402522, 60803154, 61572027); Project of State Key Lab of Mathematical Engineering and Advanced Computing; Open Foundation of Science and Technology on Information Assurance Laboratory (KJ-13-108)

线性度、重量和其它性质[6−12]，有些结论可用公式直接表示这两个参数。文献[11]刻画了二次单轨道旋转对称布尔函数的汉明重量和非线性度，文献[12]中给出了一类特殊的二次双轨道旋转对称布尔函数的汉明重量和非线性度，这些结果只能计算极少几类旋转对称布尔函数的情况，而对于一般的情况，这两篇文章中的方法不再适用。本文利用正规基，将布尔函数的问题转化为有限域上的指数和问题，这种新方法可能更适合研究一般的旋转对称布尔函数。

2 预备知识

用 $\mathbb{F}_2^n$ 表示二元域 $\mathbb{F}_2$ 上的 n 维向量空间，$\mathbb{F}_2^n$ 到 $\mathbb{F}_2$ 上的任一映射称为 $\mathbb{F}_2^n$ 上的 n 元布尔函数，简称为布尔函数。本文用 $\boldsymbol{x}=(x_0,x_1,\cdots,x_{n-1})$ 表示 $\mathbb{F}_2^n$ 中的元素，其任意两个元素 $\boldsymbol{x}$ 与 $\boldsymbol{y}$ 的内积用 $\boldsymbol{x}\cdot\boldsymbol{y}=\sum_{i=0}^{n-1}x_iy_i$ (和运算为二元域上的运算，下同)表示。用 $\mathrm{wt}(\cdot)$ 表示向量或布尔函数的汉明重量，简称重量，其中 $\mathrm{wt}(\boldsymbol{x})=\sum_{i=0}^{n-1}x_i$。而对布尔函数 f 来说，$\mathrm{wt}(f)=|\{\boldsymbol{x}\in\mathbb{F}_2^n\mid f(\boldsymbol{x})=1\}|$ ($|\cdot|$ 表示集合的元素个数)。布尔函数 f 与 g 的距离用 $d(f,g)=\mathrm{wt}(f+g)$ 表示。

定义 1 如果一个 n 元布尔函数 $f(\boldsymbol{x})$ 对任意的 $\boldsymbol{x}=(x_0,x_1,\cdots,x_{n-1})\in\mathbb{F}_2^n$ 满足：$f(x_0,x_1,\cdots,x_{n-1})=f(x_{n-1},x_0,\cdots,x_{n-2})$，则称该函数为旋转对称布尔函数。

定义 2[13] n 元旋转对称布尔函数 $f(\boldsymbol{x})$ 可以用形式 $a+a_0x_0+\sum a_{0i}x_0x_i+\cdots+a_{012\cdots n-1}x_0x_1\cdots x_{n-1}$ 表示，其中 $a,a_0,a_{0i},\cdots,a_{012\cdots n-1}\in\{0,1\}$，称这种表示方法为 $f(\boldsymbol{x})$ 的简代数正规型。

定义 3 n 元布尔函数 $f(\boldsymbol{x})$ 在 $\boldsymbol{c}$ 点的傅里叶变换为 $\hat{f}(\boldsymbol{c})=\sum_{\boldsymbol{x}\in\mathbb{F}_2^n}(-1)^{f(\boldsymbol{x})+\boldsymbol{c}\cdot\boldsymbol{x}}$。

定义 4 n 元布尔函数 $f(\boldsymbol{x})$ 的非线性度为 $N_f=\min\{d(f(\boldsymbol{x}),\boldsymbol{c}\cdot\boldsymbol{x}):\boldsymbol{c}\in\mathbb{F}_2^n\}$。

由定义 3 与定义 4 以及线性函数的性质可知：

$$\mathrm{wt}(f)=\frac{2^n-\hat{f}(\boldsymbol{0})}{2} \tag{1}$$

$$N_f=\frac{2^n-\max\{|\hat{f}(\boldsymbol{c})|:\boldsymbol{c}\in\mathbb{F}_2^n\}}{2} \tag{2}$$

用 $\mathbb{F}_{2^n}$ 表示含有 2^n 个元素的有限域，它是 $\mathbb{F}_2$ 上的 n 次扩域，这可以通过选取 $\mathbb{F}_2$ 上的 n 次不可约多项式 $f(x)$ 来构造得到，即取 $\mathbb{F}_{2^n}=\mathbb{F}_2[x]/(f(x))$。$\mathbb{F}_{2^n}$ 到 $\mathbb{F}_2$ 上的全部线性变换可以通过迹函数得到，迹函数是一类重要的函数，例如很多密码函数的构造和分析都离不开这类最基本的线性函数。用 $\mathrm{Tr}(\cdot)$ 表示 $\mathbb{F}_{2^n}$ 到 $\mathbb{F}_2$ 上的绝对迹函数，定义为：对任意的 $\alpha\in\mathbb{F}_{2^n}$，$\mathrm{Tr}(\alpha)=\sum_{i=0}^{n-1}\alpha^{2^i}$。不难验证这是一个线性函数，且 $\mathrm{Tr}(\alpha)\in\mathbb{F}_2$。对 $x\in\mathbb{F}_{2^n}$，定义 $e(x)=(-1)^{\mathrm{Tr}(x)}$。在多值密码函数的研究中，构造和分析一些密码函数时，需要计算其 Walsh 谱等谱值，这其实就是一类指数和的计算问题。本文在有限域中描述这类指数和，即对任意的 $g(x)\in\mathbb{F}_2[x]$，定义指数和为 $S(g,n)=\sum_{x\in\mathbb{F}_{2^n}}e(g(x))$。

有限域可以看成其子域上的向量空间，针对不同的用途，人们选用不同的向量空间上的基，如正规基，多项式基等。$\mathbb{F}_{2^n}$ 在 $\mathbb{F}_2$ 上的正规基是形式如 $\alpha,\alpha^2,\cdots,\alpha^{2^{n-1}}$ 的一组元素，选用这样正规基的优点之一是做平方运算不费计算资源(可以忽略不计)。由正规基定理知，对任意的 $n\geq1$，在 $\mathbb{F}_{2^n}$ 中存在一组 $\mathbb{F}_2$ 上的正规基。假设正规元为 $\alpha\in\mathbb{F}_{2^n}$，则对任意的 $x\in\mathbb{F}_{2^n}$，存在 $\boldsymbol{x}=(x_0,x_1,\cdots,x_{n-1})\in\mathbb{F}_2^n$ 使得 $x=\sum_{i=0}^{n-1}x_i\alpha^{2^i}$，称 $\boldsymbol{x}$ 为 x 在此基下的坐标。

引理 1 对任意的 $\boldsymbol{c}=(c_0,c_1,\cdots,c_{n-1})\in\mathbb{F}_2^n$，存在唯一的 $b\in\mathbb{F}_{2^n}$，使得 $\mathrm{Tr}(bx)=\boldsymbol{c}\cdot\boldsymbol{x}$，其中 $\boldsymbol{x}$ 为 x 在给定正规基下的坐标。

证明 假设 $\mathbb{F}_{2^n}$ 在 $\mathbb{F}_2$ 上的正规元为 α，任取 $b\in\mathbb{F}_{2^n}$，b 在 α 对应正规基下的坐标为 $(b_0,b_1,\cdots,b_{n-1})\in\mathbb{F}_2^n$，则有 $\mathrm{Tr}(bx)=\mathrm{Tr}\left(\left(\sum_{i=0}^{n-1}b_i\alpha^{2^i}\right)\left(\sum_{j=0}^{n-1}x_j\alpha^{2^j}\right)\right)=\sum_{i=0}^{n-1}\left(\sum_{j=0}^{n-1}\mathrm{Tr}\left(\alpha^{2^i}\alpha^{2^j}\right)b_j\right)x_i$。

令 $\sum_{j=0}^{n-1}\mathrm{Tr}(\alpha^{2^i}\alpha^{2^j})b_j=c_i,i=0,1,\cdots,n-1$，则此方程组的系数矩阵为 $\boldsymbol{A}=(\mathrm{Tr}(\alpha^{2^i}\alpha^{2^j}))_{n\times n}$ ($0\leq i,j\leq n-1$)。因 α 为正规元，故 $|\boldsymbol{A}|\neq0$，从而此方程组有唯一解 $(b_0,b_1,\cdots,b_{n-1})^{\mathrm{T}}=A^{-1}(c_0,c_1,\cdots,c_{n-1})^{\mathrm{T}}$，且有 $\mathrm{Tr}(bx)=\boldsymbol{c}\cdot\boldsymbol{x}$。 证毕

假设存在 n 元布尔函数 $f(\boldsymbol{x})$ 以及单变元函数 $g(x)\in\mathbb{F}_2[x]$，满足 $f(\boldsymbol{x})=\mathrm{Tr}(g(x))$，其中 $\boldsymbol{x}=(x_0,x_1,\cdots,x_{n-1})$ 为 x 在给定正规基下的坐标。由引理 1 知对任意的 $\boldsymbol{c}\in\mathbb{F}_2^n$ 存在唯一的 $b\in\mathbb{F}_{2^n}$，使得 $\mathrm{Tr}(bx)=\boldsymbol{c}\cdot\boldsymbol{x}$，从而可得 $f(\boldsymbol{x})$ 在 $\boldsymbol{c}$ 点的傅里叶变换为

$$\begin{aligned}\hat{f}(\boldsymbol{c})&=\sum_{\boldsymbol{x}\in\mathbb{F}_2^n}(-1)^{f(\boldsymbol{x})+\boldsymbol{c}\cdot\boldsymbol{x}}=\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(g(x))+\mathrm{Tr}(bx)}\\&=S(g(x)+bx,n)\end{aligned} \tag{3}$$

综合式(1)～式(3)可知，求取 $f(\boldsymbol{x})$ 的重量和非线性度可以转化为求取对应 $g(x)$ 的指数和，这是本文研究的出发点。而对于旋转对称布尔函数有特殊类型的单变元函数与其对应，例如：

$$\begin{aligned}\mathrm{Tr}\left(x^{1+2^i}\right)&=\mathrm{Tr}\left(\left(\sum_{j=0}^{n-1}x_j\alpha^{2^j}\right)\left(\sum_{j=0}^{n-1}x_j\alpha^{2^j}\right)^{2^i}\right)\\&=\sum_{1\le j<\lceil n/2\rceil}\mathrm{Tr}\left(\alpha\alpha^{2^{i+j}}+\alpha\alpha^{2^{i-j}}\right)\\&\quad\cdot\left(x_0x_j+x_1x_{j+1}+\cdots+x_{n-1}x_{j-1}\right)\\&\quad+\mathrm{Tr}\left(\alpha\alpha^{2^i}\right)(x_0+x_1+\cdots x_{n-1})\end{aligned}\tag{4}$$

对不同的正规基，$\mathrm{Tr}\left(x^{1+2^i}\right)$对应不同的旋转对称布尔函数。在文献[14]中，对形如$g(x)=\sum_{i=0}^{k}a_ix^{1+2^i}$（$a_i\in\mathbb{F}_2$）的指数和做了较深入的研究，由式(4)知该类型函数的绝对迹函数正好对应于特殊类型的二次旋转对称布尔函数。在本文中定义$\Delta g(x)=\sum_{i=0}^{k}\left(a_i^{2^k}x^{2^{k+i}}+a_i^{2^{k-i}}x^{2^{k-i}}\right)$，其中$a_k=1$。由文献[14]中命题 3.1 知

$$S(g+bx,n)=\epsilon_n(g+bx)2^{(n+l_n(g))/2}\tag{5}$$

其中$l_n(g)=\log_2\left[\deg\left(\Delta g,x^{2^n}-x\right)\right]$,$\epsilon_n(g+bx)\in\{0,\pm1\}$。

定义 5　设$\alpha\in\mathbb{F}_{2^n}$，$a_i=\mathrm{Tr}\left(\alpha^{1+2^i}\right)$（$0\le i\le n-1$），称$\boldsymbol{a}=(a_0,a_1,\cdots,a_{n-1})\in\mathbb{F}_2^n$为元素$\alpha$的关联向量。

定义 6　若多项式$f(x)=a_0+a_1x+a_2x^2+\cdots+a_{n-1}x^{n-1}\in\mathbb{F}_2[x]/(x^n-1)$的系数满足$a_i=a_{n-1}$（$1\le i\le n-1$），则称该多项式为对称多项式。

本文需要关于有限域上具有良好迹正交关系的正规基的一些结果，下面的结论另文给出，也可参见文献[15]。

定理 1　已知$\boldsymbol{a}=(a_0,a_1,\cdots,a_{n-1})\in\mathbb{F}_2^n$，$f_{\boldsymbol{a}}(x)=\sum_{i=0}^{n-1}a_ix^i\in\mathbb{F}_2[x]$，则存在$\mathbb{F}_{2^n}$在$\mathbb{F}_2$上的正规元$\alpha$，满足其关联向量为给定$\boldsymbol{a}$充分必要条件为：

(1) $f_{\boldsymbol{a}}(x)$为对称多项式且与x^n+1互素；

(2) 若n是偶数，则$a_{n/2}=0$且当$4\mid n$时有$\sum_{i=0}^{n/4-1}a_{2i+1}=1$。

设正整数$n=2^en^*$（$\gcd(n^*,2)=1$），记$v_2(n)=e$。

定理 2[14]　假设正整数m,n满足$m\mid n$，奇素数$p_1,p_2,\cdots,p_t$（可相同）满足$2^{\frac{1}{2}(l_{p_1p_2\cdots p_in}(g)-l_{p_1p_2\cdots p_{i-1}n}(g))}\equiv(-1)^{\delta_i}(\bmod p_i),\ (1\le i\le t)$则有$\epsilon_{p_1p_2\cdots p_tn}(g)=(-1)^{\delta_1+\delta_2+\cdots+\delta_t}\left(\frac{2}{p_1p_2\cdots p_t}\right)^n\epsilon_n(g)$，其中$\left(\frac{2}{p_1p_2\cdots p_t}\right)$为雅可比符号。

定理 3[14]　令$g(x)=ax^{1+2^\alpha}\in\mathbb{F}_{2^m}[x],a\in\mathbb{F}_{2^m}^*$，记$o(a)$为$a$在$\mathbb{F}_{2^m}^*$中的阶，令$t=o(a)/(o(a),2^\alpha-1)$。正整数$m,n$满足$m\mid n$，$c\in\mathbb{F}_{2^n}$，则

$$(1)\ l_n(g+cx)=\begin{cases}(2\alpha,n), & (2^{2\alpha}-1,2^n-1/t)\\ & =2^{(2\alpha,n)}-1\\ 0, & \text{其它}\end{cases}$$

(2) 若$v_2(n)>v_2(\alpha)$，若$\Delta g(x)=c^{2^\alpha}$有解$x^*\in\mathbb{F}_{2^n}$，则

$$\epsilon_n(g+cx)=\begin{cases}e(g(x^*)), & v_2(n)=v_2(\alpha)+1\text{且}\\ & (2^{2\alpha}-1,(2^n-1)/t)\\ & =2^{(2\alpha,n)}-1\text{或}v_2(n)\\ & >v_2(\alpha)+1\text{且}(2^{2\alpha}-1,\\ & (2^n-1)/t)\ne2^{(2\alpha,n)}-1\\ -e(g(x^*)), & v_2(n)=v_2(\alpha)+1\text{且}\\ & (2^{2\alpha}-1,(2^n-1)/t)\\ & \ne2^{(2\alpha,n)}-1\text{或}v_2(n)\\ & >v_2(\alpha)+1\text{且}(2^{2\alpha}-1,\\ & (2^n-1)/t)=2^{(2\alpha,n)}-1\end{cases}$$

若$\Delta g(x)=c^{2^\alpha}$在$\mathbb{F}_{2^n}$上无解，则$\epsilon_n(g+cx)=0$。

3　$4\nmid n$时二次旋转对称布尔函数的重量与非线性度的计算

本节假设正整数$n=2^ep_1p_2\cdots p_t$，其中$p_i(1\le i\le t)$为奇素数，$e\le1$，即$4\nmid n$。

定理 4　假设n元旋转对称布尔函数$f(\boldsymbol{x})$的简代数正规型为$f(\boldsymbol{x})=\sum_{i=1}^{k}a_ix_0x_i$，$k<\lceil n/2\rceil$，用$u_f$表示$f$中下标$i$为偶数的个数，$v_f=\sum_{i=1}^{k}a_i$。设$g(x)=\sum_{i=1}^{k}a_ix^{1+2^i}\in\mathbb{F}_2[x]$，则

(1) $N_f=2^{n-1}-2^{(n+l_n(g))/2-1}$。

(2)

$$\mathrm{wt}(f)=\begin{cases}2^{n-1}-(-1)^{\delta_1+\delta_2+\cdots+\delta_t}\left(\frac{2}{p_1p_2\cdots p_t}\right)2^{(n+l_n(g))/2-1}, & e=0\text{且}v_f=0\\ 2^{n-1}-(-1)^{\delta_1+\delta_2+\cdots+\delta_t}2^{(n+l_n(g))/2-1}, & e=1\text{且}u_f\equiv0(\bmod2)\\ 2^{n-1}, & e=0\text{且}v_f=1\text{或}e=1\text{且}u_f\equiv1(\bmod2)\end{cases}$$

其中$\delta_i(1\le i\le t)$为定理 3 中所定义。

证明　设$\boldsymbol{a}=(1,0,\cdots,0)\in\mathbb{F}_2^n$，由定理 1 知，存在$\mathbb{F}_{2^n}$在$\mathbb{F}_2$上的正规元$\alpha$，使得$\alpha$的关联向量为

$\boldsymbol{a}$ (实际为自对偶正规基)。假设 $x\in\mathbb{F}_{2^n}$ 在 α 对应正规基下的坐标为 $\boldsymbol{x}=(x_0,x_1,\cdots,x_{n-1})\in\mathbb{F}_2^n$。由式(4)知 $\mathrm{Tr}(x^{1+2^i})=x_0x_i+x_1x_{i+1}+\cdots+x_{n-1}x_{i-1}$ ($i\neq 0$),于是有

$$\begin{aligned}\mathrm{Tr}(g(x))&=\mathrm{Tr}\left(\sum_{i=0}^{k}a_ix^{1+2^i}\right)\\&=\sum_{i=0}^{k}a_i(x_0x_i+x_1x_{i+1}+\cdots+x_{n-1}x_{i-1})\\&=f(\boldsymbol{x})\end{aligned}$$

由式(3)知 $\hat{f}(\boldsymbol{c})=S(g(x)+bx,n)$,其中 $b\in\mathbb{F}_{2^n}$ 满足 $\mathrm{Tr}(bx)=\boldsymbol{c}\cdot\boldsymbol{x}$。而由式(5)知 $S(g+bx,n)=\epsilon_n(g)2^{(n+l_n(g))/2}$,从而由式(2)可得

$$\begin{aligned}N_f&=\frac{2^n-\max\{|\,\hat{f}(\boldsymbol{c})\,|:\boldsymbol{c}\in\mathbb{F}_2^n\}}{2}\\&=\frac{2^n-\max\{|\,S(g(x)+bx,n)\,|:b\in\mathbb{F}_{2^n}\}}{2}\\&=2^{n-1}-2^{(n+l_n(g))/2-1}。\end{aligned}$$

由定理 2 知

$$\epsilon_n(g)=\begin{cases}(-1)^{\delta_1+\delta_2+\cdots+\delta_t}\left(\dfrac{2}{p_1p_2\cdots p_t}\right)\epsilon_1(g), & e=0\\(-1)^{\delta_1+\delta_2+\cdots+\delta_t}\epsilon_2(g), & e=1\end{cases}$$

另一方面

$$S(g,1)=\sum_{x\in\mathbb{F}_2}e\left(\sum_{i=1}^{k}a_ix^{1+2^i}\right)=\begin{cases}2, & \sum_{i=1}^{k}a_i=0\\0, & \sum_{i=1}^{k}a_i=1\end{cases}$$

从而

$$\epsilon_1(g)=\begin{cases}1, & v_f=0\\0, & v_f=1\end{cases}$$

对正整数 a,易得

$$1+2^a\equiv\begin{cases}0(\mathrm{mod}\ 3), & a\text{为奇数}\\2(\mathrm{mod}\ 3), & a\text{为偶数}\end{cases}$$

于是对任意的 $x\in\mathbb{F}_{2^2}$,当 a 为奇数时 $x^{1+2^a}\in\mathbb{F}_2$,当 a 为偶数时 $x^{1+2^a}=x^2$,从而有

$$\begin{aligned}S(g,2)&=\sum_{x\in\mathbb{F}_{2^2}}e\left(\sum_{i=1}^{k}a_ix^{1+2^i}\right)=\sum_{x\in\mathbb{F}_{2^2}}e(u_fx^2)\\&=\begin{cases}\sum\limits_{x\in\mathbb{F}_{2^2}}e(x^2), & u_f\equiv 1(\mathrm{mod}\,2)\\\sum\limits_{x\in\mathbb{F}_{2^2}}e(0), & u_f\equiv 0(\mathrm{mod}\,2)\end{cases}\\&=\begin{cases}0\,, & u_f\equiv 1(\mathrm{mod}\,2)\\2^2, & u_f\equiv 0(\mathrm{mod}\,2)\end{cases}\end{aligned}$$

故此时

$$\epsilon_2(g)=\begin{cases}0, & u_f\equiv 1(\mathrm{mod}\,2)\\1, & u_f\equiv 0(\mathrm{mod}\,2)\end{cases}$$

综上可得

$$\epsilon_n(g)=\begin{cases}(-1)^{\delta_1+\delta_2+\cdots+\delta_t}\left(\dfrac{2}{p_1p_2\cdots p_t}\right),\\\quad e=0\text{且}v_f=0\\(-1)^{\delta_1+\delta_2+\cdots+\delta_t},\\\quad e=1\text{且}u_f\equiv 0(\mathrm{mod}\,2)\\0,\ \ e=0\text{且}v_f=1\text{或}e=1\text{且}u_f\equiv 1(\mathrm{mod}\,2)\end{cases}$$

于是由 $\hat{f}(\boldsymbol{0})=S(g(x),n)=\epsilon_n(g)2^{(n+l_n(g))/2}$ 及式(1)可得结论(2)。 证毕

例 1 假设 n 元旋转对称布尔函数 $f(\boldsymbol{x})$ 的简代数正规型为 $f(\boldsymbol{x})=x_0x_1+x_0x_2$,则 $u_f=1$,$v_f=0$。构造函数 $g(x)=x^{1+2^1}+x^{1+2^2}\in\mathbb{F}_2[x]$,$\Delta g(x)=x^{2^{2+1}}+x^{2^{2-1}}+x^{2^{2+2}}+x^{2^{2-2}}=x^{16}+x^8+x^2+x$,利用 maple 分解 $\Delta g(x)$,可计算得 $\deg(\Delta g(x),x^{2^n}-x)$,进而若 n 形如 $n=2^e3^hp_1p_2\cdots p_t$,其中 $(2\cdot 3,p_i)=1$,$i=1,2,\cdots,t$。则

$$l_n(g)=\begin{cases}1, & e=0,\ h=0\\2, & e=1,\ h=0\\3, & e=0,\ h\geq 1\\4, & e=1,\ h\geq 1\end{cases}$$

从而可得

$$N_f=\begin{cases}2^{n-1}-2^{(n-1)/2}, & e=0,\ h=0\\2^{n-1}-2^{n/2}, & e=1,\ h=0\\2^{n-1}-2^{(n+1)/2}, & e=0,\ h\geq 1\\2^{n-1}-2^{(n+2)/2}, & e=1,\ h\geq 1\end{cases}$$

当 $e=1$ 时,因 $u_f=1\equiv 1\,(\mathrm{mod}\ 2)$,故由定理 4 知 $\mathrm{wt}(f)=2^{n-1}$。

当 $e=0$ 时,因 $v_f=0$,故 $\mathrm{wt}(f)=2^{n-1}-(-1)^{\delta_1+\delta_2+\cdots+\delta_t}\left(\dfrac{2}{p_1p_2\cdots p_t}\right)2^{(n+l_n(g))/2-1}$。若此时 $h\geq 1$,则对任意的 $i>1$,有

$$2^{\frac{1}{2}(l_{3^ip_1p_2\cdots p_t}(g)-l_{3^{i-1}p_1p_2\cdots p_t}(g))}=2^{\frac{1}{2}(3-3)}=1\equiv 1(\mathrm{mod}\ 3)$$

$$2^{\frac{1}{2}(l_{3p_1p_2\cdots p_t}(g)-l_{p_1p_2\cdots p_t}(g))}=2^{\frac{1}{2}(3-1)}=2\equiv -1(\mathrm{mod}\ 3)$$

$$2^{\frac{1}{2}(l_{p_1p_2\cdots p_i}(g)-l_{p_1p_2\cdots p_{i-1}}(g))}=2^{\frac{1}{2}(1-1)}=1\equiv 1(\mathrm{mod}\ p_i)$$

$$(1\leq i\leq t)$$

故 $\mathrm{wt}(f)=2^{n-1}-\left(\dfrac{2}{3}\right)^{h-1}(-1)\left(\dfrac{2}{3}\right)\left(\dfrac{2}{p_1p_2\cdots p_t}\right)2^{(n+l_n(g))/2-1}$

$=2^{n-1}-(-1)^{h+1}\left(\dfrac{2}{p_1p_2\cdots p_t}\right)2^{(n+l_n(g))/2-1}$。综上可得

$$\mathrm{wt}(f)=\begin{cases}2^{n-1}-\left(\dfrac{2}{p_1p_2\cdots p_t}\right)2^{(n-1)/2}, \\ \qquad e=0,\quad h=0\\ 2^{n-1}-(-1)^{h+1}\left(\dfrac{2}{p_1p_2\cdots p_t}\right)2^{(n+1)/2}, \\ \qquad e=0,\quad h\geq 1\\ 2^{n-1},\quad e=1\end{cases}$$

表 1 是利用计算机编程得到的该函数的汉明重量和非线性度，可用例子中得出的公式进行验证。

沿用定理 4 中的符号 u_f 及 v_f。当 $e=1$ 即 $v_2(n)=1$，且对定理 4 中给出的 $f(\boldsymbol{x})$，$u_f=0$ 时，该函数的重量和非线性度的计算有更简单的公式。证明的方法与定理 4 的证明类似，只需结合文献[14]中定理 5.1，在此只给出结论。

定理 5　假设 $v_2(n)=1$，n 元旋转对称布尔函数 $f(\boldsymbol{x})$ 的简代数正规型为 $f(\boldsymbol{x})=\sum_{i=0}^{k}a_ix_0x_{2i+1}$，其中 k 满足 $2k+1<n/2$。令 $g(x)=\sum_{i=0}^{k}a_ix^{1+2^{2i+1}}\in\mathbb{F}_2[x]$，则

(1) $N_f=2^{n-1}-2^{(n+l_n(g))/2-1}$。

(2) $\mathrm{wt}(f)=2^{n-1}-(-1)^{(n+l_n(g))/2}2^{(n+l_n(g))/2-1}$。

表 1 计算机编程得到的例 1 的部分结果

n	9	10	11	13	14	15	17	18
N_f	224	480	992	4032	8064	16128	65280	130048
$\mathrm{wt}(f)$	288	512	1056	4160	8192	16640	65280	131072

例 2　假设 $v_2(n)=1$，n 元旋转对称布尔函数 $f(\boldsymbol{x})$ 的简代数正规型为 $f(\boldsymbol{x})=x_0x_1+x_0x_3$，令 $g(x)=x^{1+2}+x^{1+2^3}$，则 $\Delta g(x)=x^{2^6}+x^{2^4}+x^{2^2}+x$，$\deg(\Delta g(x),x^{2^n}-x)=4$，故 $l_n(g)=2$，进而可得 $N_f=2^{n-1}-2^{n/2}$，$\mathrm{wt}(f)=2^{n-1}-2^{n/2}$。给出部分计算机得出的结果如表 2 所示。

表 2 计算机编程得到的例 2 的部分结果

n	10	14	18	22	26
N_f/$\mathrm{wt}(f)$	480	8064	130560	2095104	33546240

4　$n=2^s$ 时特殊二次旋转对称布尔函数的重量与非线性度的计算

本节假设 $n=2^s,s\geq 2$，此时不存在 $\mathbb{F}_{2^n}$ 在 $\mathbb{F}_2$ 上的自对偶正规基，但由定理 1 知，可以找到特殊的正规元 $\alpha\in\mathbb{F}_{2^n}$ 使其关联向量满足一定条件，再利用式(4)可以确立旋转对称布尔函数与单变元函数之间的对应关系。

定理 6　假设 n 元旋转对称布尔函数的简代数正规型为 $f(\boldsymbol{x})=x_0x_{a-t}+x_0x_a+x_0x_{a+t}$，其中 a 满足 $1\leq a-t<a<a+t<[n/2]$，$1\leq t<a$ 为奇数。则有

(1) $N_f=2^{n-1}-2^{(n+(2a,n))/2-1}$。

(2) $\mathrm{wt}(f)=2^{n-1}+2^{(n+(2a,n))/2-1}$。

证明　令向量 $\boldsymbol{a}=(1,0,\cdots,0,1,0,\cdots,0,1,0,\cdots,0)\in\mathbb{F}_2^n$，其中分量 $a_0=a_t=a_{n-t}=1$，其余为 0，则 $\boldsymbol{a}$ 对应的对称多项式为 $f_{\boldsymbol{a}}(x)=x^{n-t}+x^t+1\in\mathbb{F}_2[x]$。而此时 $x^n+1=x^{2^s}+1=(x+1)^{2^s}$，故 $\gcd(f_{\boldsymbol{a}}(x),x^n+1)=1$，另外定理 1 条件(2)显然满足，于是存在 $\mathbb{F}_{2^n}$ 在 $\mathbb{F}_2$ 上的正规元 α 使得其关联向量为 $\boldsymbol{a}$。亦即

$$\mathrm{Tr}(\alpha\alpha^{2^i})=\begin{cases}1, & i=0,t,n-t\\ 0, & \text{其它}\end{cases}$$

假设 $x\in\mathbb{F}_{2^n}$ 在此基下的坐标为 $\boldsymbol{x}=(x_0,x_1,\cdots,x_{n-1})\in\mathbb{F}_2^n$。令 $g(x)=x^{1+2^a}\in\mathbb{F}_2[x]$，则由式(4)知

$$\begin{aligned}\mathrm{Tr}(g(x))&=\mathrm{Tr}\left(x^{1+2^a}\right)\\ &=x_0x_{a-t}+x_1x_{a-t+1}+\cdots+x_{n-1}x_{a-t-1}\\ &\quad+x_0x_a+x_1x_{a+1}+\cdots+x_{n-1}x_{a-1}\\ &\quad+x_0x_{a+t}+x_1x_{a+t+1}+\cdots+x_{n-1}x_{a+t-1}\\ &=f(\boldsymbol{x})\end{aligned}$$

由式(3)知对任意的 $\boldsymbol{c}\in\mathbb{F}_2^n$，$\hat{f}(\boldsymbol{c})=S(g(x)+bx,n)$，其中 $b\in\mathbb{F}_{2^n}$ 满足 $\mathrm{Tr}(bx)=\boldsymbol{c}\cdot\boldsymbol{x}$，利用定理 3(1)的结果可得

$$\begin{aligned}N_f&=\frac{2^n-\max\{|\,\hat{f}(\boldsymbol{c})\,|:\boldsymbol{c}\in\mathbb{F}_2^n\}}{2}\\ &=\frac{2^n-\max\{|\,S(g(x)+bx,n)\,|:b\in\mathbb{F}_{2^n}\}}{2}\\ &=2^{n-1}-2^{(n+(2a,n))/2-1}\end{aligned}$$

而对任意的 $1<a<[n/2]-t$，$v_2(n)=s>v_2(a)+1$，且 $\Delta g(x)=x^{2^{2a+2}}+x=0$ 有解 $x^*=0$，由定理 3(2)知 $\epsilon_n(g)=-e(g(0))=-1$。再由 $\hat{f}(\boldsymbol{0})=S(g(x),n)=\epsilon_n(g)2^{(n+l_n(g))/2}$ 及式(1)得 $\mathrm{wt}(f)=2^{n-1}+2^{(n+(2a,n))/2-1}$。证毕

例 3 假设 $n=16$，

(1)若 $f(\boldsymbol{x})=x_0x_1+x_0x_2+x_0x_3$，则 $s=4$，a=2，$t=1$。故 $N_f=2^{n-1}-2^{(n+(2a,n))/2-1}=2^{16-1}-2^{(16+4)/2-1}=32256$，$\mathrm{wt}(f)$=$2^{n-1}$+$2^{(n+(2a,n))/2-1}$=$2^{16-1}$+$2^{(16+4)/2-1}=33280$。

(2) 若 $f(\boldsymbol{x})=x_0x_1+x_0x_4+x_0x_7$，则 $s=4$，$a=4$，$t=3$，故 $N_f=2^{n-1}-2^{(n+(2a,n))/2-1}=2^{16-1}-2^{(16+8)/2-1}=30720$，$\mathrm{wt}(f)=2^{n-1}+2^{(n+(2a,n))/2-1}=2^{16-1}+2^{(16+8)/2-1}=34816$。这两个结果都可以用计算机进行验证。

5 与已有结论及方法的比较

文献[11]研究了简代数正规型为 $f_{n,s}=x_0x_{s-1}$ $(1<s\le\lceil n/2\rceil)$ 的二次旋转对称布尔函数的重量和非线性度。通过等价变换将 $f_{n,s}$ 转化为若干个已知其重量和非线性度的子布尔函数的组合，而这些子布尔函数的个数可由 $\mathbb{Z}_n$ 的子群 $\langle s-1\rangle$ 的阶来刻画，再利用文献中给出的引理 5 求出了 $f_{n,s}$ 的重量和非线性度计算公式。文献[12]研究了一类双轨道旋转对称布尔函数，其简代数正规型为 $f=x_0x_1+x_0x_2$，构造了一个仿射变换，将 f 仿射等价为一个已知其重量和非线性度的布尔函数，同样求出了 f 的重量和非线性度计算公式。

目前对于二次旋转对称布尔函数的重量和非线性度的研究结果有限，原因之一是没有一般性的办法来解决这类二次函数的指数和的计算问题，如上述两文中的方法只能适用于上述两文中的特殊的二次旋转对称布尔函数。本文使用的方法与上述两个文献中使用的方法不同，将二次旋转对称布尔函数的重量和非线性度的问题转化为有限域上单变元函数的指数和计算问题，最终求取了 $4\nmid n$ 时任意的二次旋转对称布尔函数的重量和非线性度，同时对 $n=2^s,s\ge2$ 时的特殊类型的旋转对称布尔函数重量和非线性度进行了刻画。当 $4\nmid n$ 时，文献[11]的结论是本文定理 4 的特殊情形，而文献[12]的结论是本文例 1 的特殊情形。相比于已有的方法，本文的这种利用特殊的正规基的方法更有一般性，能计算大部分二次旋转对称布尔函数的非线性度，且计算非线性度时，主要运算之一是求取特殊的具有指定正交关系的正规基(参见文献[16]等，可知有时(如 $n=2^s,s\ge2$)是线性运算)。本文方法对研究一般的高次旋转对称布尔函数也有一定的参考意义。

参 考 文 献

[1] Pieprzyk J and Qu C X. Fast hashing and rotation-symmetric functions[J]. *Journal of Universal Computer Science*, 1999, 5(1): 20–31.

[2] Cusick T W and Stănică P. Fast evaluation, weights and nonlinearity of rotation-symmetric functions[J]. *Discrete Mathematics*, 2002, 258(1): 289–301.

[3] Ciungu L C. Cryptographic Boolean functions: Thus-Morse sequences, weight and nonlinearity[D]. [Ph.D. dissertation], University at Buffalo, 2010.

[4] Zhang X, Guo H, Feng R, *et al*.. Proof of a conjecture about rotation symmetric functions[J]. *Discrete Mathematics*, 2011, 311(14): 1281–1289.

[5] Wang B, Zhang X, and Chen W. The hamming weight and nonlinearity of a type of rotation symmetric Boolean function [J]. *Acta Mathematica Sinica, Chinese Series*, 2012, 55(4): 613–626.

[6] Cusick T W. Finding Hamming weights without looking at truth tables[J]. *Cryptography and Communications*, 2013, 5(1): 7–18.

[7] Brown A and Cusick T W. Equivalence classes for cubic rotation symmetric functions[J]. *Cryptography and Communications*, 2013, 5(2): 85–118.

[8] KV L, Sethumadhavan M, and Cusick T W. Counting rotation symmetric functions using Polya's theorem[J]. *Discrete Applied Mathematics*, 2014, 169: 162–167.

[9] Cusick T W and Cheon Y. Affine equivalence for cubic rotation symmetric Boolean functions with n=pq variables[J]. *Discrete Mathematics*, 2014, 327: 51–61.

[10] Cusick T W and Cheon Y. Affine equivalence of quartic homogeneous rotation symmetric Boolean functions[J]. *Information Sciences*, 2014, 259: 192–211.

[11] Kim H, Park S M, and Hahn S G. On the weight and nonlinearity of homogeneous rotation symmetric Boolean functions of degree 2[J]. *Discrete Applied Mathematics*, 2009, 157(2): 428–432.

[12] Liu H. On the weight and nonlinearity of quadratic rotation symmetric function with two MRS functions[J]. *General Mathematics Notes*, 2013, 16(1): 12–19.

[13] Stănică P and Maitra S. Rotation symmetric Boolean functions-count and cryptographic properties[J]. *Discrete Applied Mathematics*, 2008, 156(10): 1567–1580.

[14] Hou X D. Explicit evaluation of certain exponential sums of binary quadratic functions[J]. *Finite Fields and Their Applications*, 2007, 13(4): 843–868.

[15] Weinberger M J and Lempel A. Factorization of symmetric circulant matrices in finite fields[J]. *Discrete Applied Mathematics*, 1990, 28(3): 271–285.

[16] Zhang X, Cao X, and Feng R. A method of evaluation of exponential sum of binary quadratic functions[J]. *Finite Fields and Their Applications*, 2012, 18(6): 1089–1103.

张习勇：男，1975 年生，副教授，研究方向为编码密码学.

祁应红：男，1986 年生，硕士生，研究方向为编码密码学.

高光普：男，1984 年生，讲师，研究方向为对称密码设计与分析.