·学术论文与技术报告·

Bent函数估计的可计算达到上界

王 玲，张建州

(1.电子科技大学电子工程学院 成都 610054; 2. 四川大学计算机学院 成都 610065)

【摘要】Bent函数的计数和数目估计问题与依据其设计的流密码的安全性有密切联系。通过将Bent函数表示为定序特征矩阵，引入Bent矩阵的概念；根据Bent函数的定义，得到Bent矩阵的一些性质；利用解决一阶相关免疫布尔函数计数问题的方法，给出Bent函数个数估计的一个基于整数分拆表示的可计算上界，计算实例说明该上界是可达到的上界。

关 键 词 Bent函数; 定序特征矩阵; 上界; 分拆

中图分类号 TN918.1; O157.1 文献标识码 A

A Best Possible Computable Upper Bound on Bent Functions

Wang Ling，Zhang Jianzhou

(1. School of Electrical Engineering, UEST of China Chengdu 610054; 2. College of Computer, Sichuan University Chengdu 610065)

Abstract Enumeration and estimation of bent functions are closely related to the security of stream ciphers designed by them. In this paper, bent matrix is introduced when bent function is denoted by the ordered characteristic matrix. With help of the definition of bent function, some properties of bent matrix are obtained. On the basis of the author's approach to solving the enumeration of the first order correlation-immune Boolean functions, a computable upper bound on the number of bent functions, which is represented by the summation over the integer partition, is given. Examples show that the upper bound is a best possible upper bound.

Key words Bent function; ordered characteristic matrix; upper bound; partition

Bent函数的概念提出后[1]，人们发现它在密码学中有重要应用[2]，其结构、构造和计数问题的研究受到广泛关注[2~5]。文献[3]系统总结了Bent函数研究的结果和问题，但Bent函数的计数问题始终未解决，甚至一个好的上界估计也不知道。本文根据Bent函数的定义，研究了Bent函数定序特征矩阵的性质，利用文献[6, 7]的思想，给出Bent函数数目估计的一个可计算上界，计算实例说明该上界是可以达到的上界。

1 Bent函数和Bent矩阵

设 $f(x_1, x_2, \Lambda\ , x_n)$ 是n元布尔函数，可看作从 $GF^n(2)$ 到 $GF(2)$ 的映射，其中 $GF(2)$ 是二元有限域。文献[1]引入 $f(x_1, x_2, \Lambda\ , x_n)$ 的下列变换

$$c(l) = \frac{1}{2^{n/2}} \sum_{x \in GF^n(2)} (-1)^{f(x)+<l,x>} \tag{1}$$

收稿日期：2002 – 07 – 04
基金项目：国家自然科学基金资助项目(60371024)
作者简介：王玲(1962 –)，女，大学，高级工程师，主要从事微波电路与通信方面的研究.

式中 $l \in GF^n(2)$，$<\ddot{e}, x>$为内积。并定义：若 $c(l)=\pm 1$(对每一个 $l \in GF^n(2)$)，则称 $f(x_1, x_2, \Lambda\ , x_n)$ 是Bent函数，n显然是偶数。

记$w=W(f)$，其中 $W(f)=\sum_x f(x)$ 是 $f(x_1, x_2, \Lambda\ , x_n)$ 的Hamming重量。由式(1)，令 $l=0$，可得 $w=2^{n-1}+2^{\frac{n}{2}-1}c(0)$，即$n$元Bent函数 $f(x_1, x_2, \Lambda\ , x_n)$ 的Hamming重量等于 $2^{n-1}+2^{\frac{n}{2}-1}$ 或 $2^{n-1}-2^{\frac{n}{2}-1}$，于是，$n$元Bent函数按Hamming重量分类只有两类。用式(1)可验证若 $f(x_1, x_2, \Lambda\ , x_n)$ 是Bent函数，则 $f(x_1, x_2, \Lambda\ , x_n)+1$ 也是Bent函数。另一方面，当 $f(x_1, x_2, \Lambda\ , x_n)$ 的Hamming重量等于 $2^{n-1}+2^{\frac{n}{2}-1}$ (或 $2^{n-1}-2^{\frac{n}{2}-1}$)时，$f(x_1, x_2, \Lambda\ , x_n)+1$的Hamming重量等于 $2^{n-1}-2^{\frac{n}{2}-1}$(或 $2^{n-1}+2^{\frac{n}{2}-1}$)。这说明：$n$元Bent函数按Hamming重量分成的两类其数目相等。称向量集合

$$D=\{(d_1, d_2, \Lambda\ , d_n) \mid\ f(d_1, d_2, \Lambda\ , d_n)=1\}$$

为 $f(x_1, x_2, \Lambda\ , x_n)$ 的特征集合。又记 $\boldsymbol{c}_1=(c_{11}, c_{12}\mathrm{L}\ , c_{1n})$,…, $\boldsymbol{c}_w=(c_{w1}, c_{w2}, \Lambda\ , c_{wn})$ 为集合D中按字典序排列的 $f(x_1, x_2, \Lambda\ , x_n)$ 的一切特征向量，$w\times n$ 阶0、1矩阵

$$\boldsymbol{C}=\begin{pmatrix}\boldsymbol{c}_1\\ \boldsymbol{c}_2\\ \mathrm{M}\\ \boldsymbol{c}_w\end{pmatrix}=\begin{pmatrix}c_{11}\ c_{12}\ \mathrm{K}\ c_{1n}\\ c_{21}\ c_{22}\ \mathrm{K}\ c_{2n}\\ \mathrm{M}\ \ \mathrm{M}\ \mathrm{K}\ \ \mathrm{M}\\ c_{w1}\ c_{w2}\ \mathrm{K}\ c_{wn}\end{pmatrix}$$

称为 $f(x_1, x_2, \Lambda\ , x_n)$ 的定序特征矩阵。显然布尔函数和其定序特征矩阵是相互唯一确定的。

当 $l\neq 0$时，由式(1)可得

$$\begin{aligned}c(l)&=\frac{1}{2^{n/2}}\sum_{x\in GF^n(2)}(-1)^{f(x)+<l,x>}=\frac{1}{2^{n/2}}\left(\sum_{f(x)=0}(-1)^{<l,x>}+\sum_{f(x)=1}(-1)^{1+<l,x>}\right)=\\ &\frac{1}{2^{n/2}}\left(\sum_{x\in GF^n(2)}(-1)^{<l,x>}-\sum_{f(x)=1}(-1)^{<l,x>}-\sum_{f(x)=1}(-1)^{<l,x>}\right)=-\frac{1}{2^{n/2-1}}\sum_{f(x)=1}(-1)^{<l,x>}\end{aligned}\tag{2}$$

式(2)推导中，利用了当 $l\neq 0$时，$\sum_{x\in GF^n(2)}(-1)^{<l,x>}=0$。式(2)说明：通过取适当的$l$值，定序特征矩阵任意列向量中0和1的数目差是 $2^{\frac{n}{2}-1}$ 或 $-2^{\frac{n}{2}-1}$，定序特征矩阵中不同列的布尔和向量中0和1的数目差也是 $2^{\frac{n}{2}-1}$ 或 $-2^{\frac{n}{2}-1}$。由此定义$w\times n$ 阶矩阵$\boldsymbol{A}$各行互异且任意不同列的布尔和向量中0和1的数目差是 $2^{\frac{n}{2}-1}$ 或 $-2^{\frac{n}{2}-1}$，0、1矩阵 $\boldsymbol{A}=(a_{ij})$ 为Bent矩阵[4]，这里w等于 $2^{n-1}+2^{\frac{n}{2}-1}$ 或 $2^{n-1}-2^{\frac{n}{2}-1}$。一个$n$元Bent函数 $f(x_1, x_2, \Lambda\ , x_n)$ 对应于$w!$个Bent矩阵，其中 $w!=w(w-1)\Lambda\ 2\cdot 1$。由式(2)看出：若$\boldsymbol{A}$是Bent矩阵，则对$\boldsymbol{A}$的任意几列的分量作布尔补运算后得到的矩阵仍然是Bent矩阵。

2 Bent函数数目估计的可计算上界

要估计n元Bent函数 $f(x_1, x_2, \Lambda\ , x_n)$ 的数目上界，只需估计$W(f)=2^{n-1}-2^{\frac{n}{2}-1}$的Bent函数数目的上界。记 $W(f)=2^{n-1}-2^{\frac{n}{2}-1}$ 的Bent函数数目为 $B(n)$，则由Bent函数的定序特征矩阵与Bent矩阵的关系可知Bent矩阵的数目等于 $(2^{n-1}-2^{\frac{n}{2}-1})!B(n)$。因此，估计 $W(f)=2^{n-1}-2^{\frac{n}{2}-1}$ 的Bent函数数目的上界关键是估计Bent矩阵数目的上界。由分析可知：估计 $(2^{n-1}-2^{\frac{n}{2}-1})!B(n)$ 的上界可以通过计数每列有 $2^{n-2}-2^{\frac{n}{2}-1}$ 个0和 2^{n-2} 个1的0、1矩阵获得，记这种矩阵的数目为$T(n)$。若求得$T(n)$，则 $(2^{n-1}-2^{\frac{n}{2}-1})!B(n)\leq 2^n T(n)$。

利用文献[6]的方法，可以给出

$$T(n)=(2^{n-1}-2^{\frac{n}{2}-1})\sum_{<j>}(-1)^{a(<j>)}h(<j>)\quad\left(\sum_{a\in\{0,1\}^{r(<j>)}}\binom{j_1}{2^{n-2}-2^{\frac{n}{2}-1}-(a, \boldsymbol{q}(<j>))}\right)^n\tag{3}$$

式中 $<j>$表示数 $l=2^{n-1}-2^{\frac{n}{2}-1}$ 的分拆，即 $<j>=1^{j_1}2^{j_2}\Lambda\ l^{j_l}$，满足 $\sum_{i=1}^{l} ij_i=l$；式(3)的求和是对 l 的所有分拆进行的；$a(<j>)=\sum_i j_{2i}$；$h(<j>)=\left(\prod_{i=1}^{l} j_i!i^{j_i}\right)^{-1}$；$r(<j>)=\sum_{i=2}^{l} j_i$；$r(<j>)$ 维向量 $\boldsymbol{q}(<j>)=(\underbrace{2,\Lambda,2}_{j_2},\underbrace{3,\Lambda,3}_{j_3},\Lambda,\underbrace{l,\Lambda,l}_{j_l})$ 由 j_2 个2、j_3 个3、…、j_l 个 l 构成；$\{0,1\}^{r(<j>)}$ 表示 $r(<j>)$ 维0、1向量的全体；$\boldsymbol{I}=(1,1,\Lambda,1)$ 是 $r(<j>)$ 维向量；$(\boldsymbol{I},\boldsymbol{q}(<j>))$ 和 $(a,\boldsymbol{q}(<j>))$ 都是向量内积运算；这里约定：当 $2^{n-2}-2^{\frac{n}{2}-1}-(a,\boldsymbol{q}(<j>))<0$ 或 $j_1<2^{n-2}-2^{\frac{n}{2}-1}-(a,\boldsymbol{q}(<j>))$ 时，$\binom{j_1}{2^{n-2}-2^{\frac{n}{2}-1}-(a,\boldsymbol{q}(<j.>))}=0$；当 $j_1\geq 0$ 时，$\binom{j_1}{0}=1$。

于是，得 n 元Bent函数个数估计的一个上界为

$$2^{n+1}\sum_{<j>}(-1)^{a(<j>)}h(<j>)\quad\left(\sum_{a\in\{0,1\}^{r(<j>)}}\binom{j_1}{2^{n-2}-2^{\frac{n}{2}-1}-(a,\boldsymbol{q}(<j>))}\right)^n$$

3　计算实例

本节给出利用得到的上界估计 n 元Bent函数数目的实例。

当 $n=2$ 时，$W(f)=2^{n-1}-2^{\frac{n}{2}-1}=1$，所以，2元Bent函数至多有8个。这与文献[4]通过计算机搜索得到的2元Bent函数数目相同。当 $n=4$ 时，$W(f)=2^{n-1}-2^{\frac{n}{2}-1}=6$，确定上界所需的值如表1所示。

表1　$n=4$ 时上界计算中所需的值

$<j>$	6^1	1^15^1	2^14^1	3^2	$1^12^13^1$	1^24^1	2^3	1^33^1	1^22^2	1^42^1	1^6
a	1	0	2	0	1	1	3	0	2	1	0
h	6^{-1}	5^{-1}	8^{-1}	18^{-1}	6^{-1}	8^{-1}	48^{-1}	18^{-1}	16^{-1}	48^{-1}	720^{-1}
c	0	0	1	0	1	1	3	3	3	7	15

将表1的值代入上界求得等于896，所以，4元Bent函数至多有896个，结果与文献[4]用计算机搜索得到的4元Bent函数数目相同。以上两例说明本文得到的上界是可以达到的。

4　结 束 语

本文利用Bent函数的Bent矩阵给出基于整数分拆表示的Bent函数的一个可计算上界，计算实例说明该上界是最好可能的上界，这为进一步研究Bent函数的计数问题提供了思路。

参 考 文 献

[1] Rothaus O S. On “Bent” functions[J]. J. of Combinatorial Theory, Ser.A, 1976, 20: 300-305

[2] 冯登国. 频谱理论及其在密码学中的应用[M]. 北京: 科学出版社, 2000

[3] Carlet C. Recent results on binary bent functions[J]. J. of Combinatorics, Information & System Sciences, 2000, 25(1-4): 133-149

[4] 王　隽, 李世取. Bent函数的一般构造法[J]. 高校应用数学学报(A辑), 1999, 14(4): 473-479

[5] Adams C M, Tavares S E. Generating and counting binary bent sequences[J]. IEEE Trans. on Information Theory, 1990, 36(5): 1 170-1 173

[6] 张建州. 计数一阶相关免疫布尔函数的可计算公式[J]. 通信学报, 2003, 24(6): 151-154

[7] 张建州. 非相关布尔函数个数的精确值[J]. 电子科技大学学报, 1994, 23(1): 89-94

编　辑　漆　蓉