Bent 函数和弹性函数的最小距离

李 超[1,2], 屈龙江[1]
(1. 国防科技大学数学与系统科学系, 湖南长沙 410073; 2. 福建师范大学网络安全与密码技术重点实验室, 福建福州 350007)

摘 要: 研究了 Bent 函数和弹性函数的最小距离, 给出了求 Bent 函数和弹性函数的最小距离的一个新算法, 得到了 Bent 函数和弹性函数最小距离新的下限, 新的下限在一阶情形优于 S. Maity 等人在 2004 年给出的结果, 同时证实了他们所提出的猜想, 并且得到了 12 元、14 元 Bent 函数和一阶弹性函数的最小距离.

关键词: Bent 函数; 弹性函数; 最小距离
中图分类号: TN918 文献标识码: A 文章编号: 0372-2112 (2008) 01-0136-05

Minimum Distance Between Bent and Resilient Boolean Functions

LI Chao[1,2], QU Long-jiang[1]
(1. *Department of Mathematic and System Science, NUDT, Changsha, Hunan 410073, China;*
2. *Key Laboratory of Network Security and Cryptology, Fujian Normal University, Fuzhou, Fujian 350007, China*)

Abstract: The minimum distance between Bent functions and Resilient functions is studied. An algorithm for calculating the minimum distance between Bent functions and resilient functions is given. We give a new lower bound for the minimum distance between Bent functions and 1-resilient functions. This new lower bound is better than that presented by S. Maity etc in 2004, and their conjectures are proven to be true. The minimum distances between Bent functions and 1-resilient functions on 12 and 14 variables are also given.

Key words: Bent function; resilient function; minimum distance

1 引言

Bent 函数和弹性函数在密码设计与分析中具有十分重要的作用. Bent 函数是 Rothaus 在 1976 年提出的[7], 它是一类结构最简单的完全非线性函数, 具有最优的非线性性, 能够有效地抵抗线性密码攻击. 弹性函数是 Chor. B 在 1985 年提出的, 它具有平衡性和较强的相关免疫性, 它可以有效抵抗相关攻击[1]. 近年来, 具有高非线性度和高代数次数的弹性函数的构造引起了密码学界的关注[2,5,8,9]. 文献[6]提出了一种通过修改 Bent 函数的部分输出点来构造高非线性度的 1 阶弹性函数的方法, 因此, Bent 函数和弹性函数的最小距离问题引起了密码学者的关注. 最先研究这个问题的是 S. Maity 和 S. Maitra[4], 他们研究了 Bent 函数和 1 阶弹性函数的最小距离, 得到了最小距离的一个下限, 并且对于 $4 \leqslant n \leqslant 10$ 的 n 元(n 偶)布尔函数的情形给出了最小距离的具体值, 而当 $n=12$ 时, 他们通过具体构造给出了一个上限, 并且猜想"该上限就是 12 元 Bent 函数和 12 元 1 阶弹性函数的最小距离", 并把该猜想作为文章的一个 open problem. 本文在 S. Maity 和 S. Maitra[4] 工作的基础上, 更一般地, 对于 Bent 函数和 t 阶弹性函数的最小距离进行了研究, 将该问题转化为一个构造满足一定条件的矩阵的组合问题和一种特定形式的 Bent 函数是否存在的问题, 提出了一个计算最小距离的算法. 应用该算法, 得到了 Bent 函数和弹性函数最小距离新的下限, 新的下限在一阶情形优于文献[4]中的结果, 证实了文献[4]中的猜想, 得到了 12 元和 14 元 Bent 函数和一阶弹性函数的最小距离.

2 基本概念与算法

设 $f(x)$ 为一个 n 元布尔函数, 则 $f(x)$ 的 Walsh 谱是 $\{0,1\}^n$ 上的一个实值函数, 其定义为:

$$W_f(\omega)=\sum_{x\in\{0,1\}^n}(-1)^{f(x)\oplus x\cdot\omega}$$

Bent 函数和弹性函数均有多种等价定义, 为方便起见, 我们采用 Walsh 谱的方式来给出它们的定义.

收稿日期: 2006-10-09; 修回日期: 2007-12-18
基金项目: 国家自然科学基金(No. 60573028); 国防科大校预研基金(No. JC07-02-03); 福建师范大学网络安全与密码技术重点实验室开放课题(No. 07A0003)

定义 **1**[7]　对于 n 元布尔函数 $f(x)$, 如果对所有的 $\omega\in F_2^n$, 均有 $W_f(\omega)=\pm 2^{n/2}$ 成立, 则称 $f(x)$ 为 n 元 Bent 函数.

定义 **2**[3]　n 元布尔函数 $f(x)$ 为 t 阶弹性函数当且仅当其 Walsh 谱满足:

$$W_f(\omega)=0,\ \forall 0\leqslant wt(\omega)\leqslant t$$

由 Bent 函数的定义, 仅当 n 为偶数的时候, Bent 函数才可能存在. 所以, 下文中 n 总是表示偶数.

定义 **3**[4]　$f(x)$ 在 $\{0,1\}^n$ 的一个子集 S 上的限制 Walsh 谱定义为

$$W_f(\omega)\mid_S=\sum_{x\in S}(-1)^{f(x)\oplus x\cdot\omega}$$

引理 **1**[4]　设 $S\subset\{0,1\}^n$, $b(x), f(x)$ 为两个 n 元布尔函数, 并且

$$f(x)=\begin{cases} b(x)\oplus 1, & x\in S\\ b(x), & x\notin S\end{cases}$$

则 $W_f(\omega)=W_b(\omega)-2W_b(\omega)\mid_S$.

记 A 为全体 n 元 Bent 函数的集合, B 为全体 n 元 t 阶弹性函数的集合, 则 Bent 函数和弹性函数的最小距离 $dBR_n(t)$ 定义为:

$$dBR_n(t)=\min_{b\in A,f\in B}d(b,f)$$

其中 $d(b,f)$ 表示布尔函数 b,f 的 Hamming 距离.

关于 $dBR_n(1)$, 文献[4]中有如下结论:

引理 **2**[4]

$$dBR_n(1)\geqslant 2^{(n/2)-1}+2\left\lceil\frac{(r+1)\left(2^{(n/2)-1}-\sum_{i=0}^{r}\binom{n}{i}\right)+\sum_{i=0}^{r}i\binom{n}{i}}{n-r-1}\right\rceil$$

, 其中 r 为满足 $\sum_{i=0}^{r}\binom{n}{i}\leqslant 2^{(n/2)-1}+1<\sum_{i=0}^{r+1}\binom{n}{i}$ 的整数.

推论 **1**[4]　设 n 是满足 $8\leqslant n\leqslant 16$ 的偶数, 则

$$dBR_n(1)\geqslant 2^{(n/2)-1}+2\left\lceil\frac{2^{n/2}-n-2}{n-2}\right\rceil.$$

文献[4]在得到上述下限的同时, 对 $n=8,10$ 的情形都构造出了距离达到该下限的 Bent 函数和 1 阶弹性函数, 从而求出了 $dBR_8(1)=10$, $dBR_{10}(1)=22$. 当 $n=12$ 时, 由推论 1 可知 $dBR_{12}(1)\geqslant 42$. S. Maity 等人无法修改某个 Bent 函数的 42 个点来构造 1 阶弹性函数, 但他们成功地从 1 个 Bent 函数出发, 修改了 44 个点得到了一个 1 阶弹性函数, 从而得到 $dBR_{12}(1)\leqslant 44$. 在文献[4]的最后, 他们给出了如下猜想: $dBR_{12}(1)=44$, 并把推论 1 中的下限是否是紧的做为公开问题. 本文证实了 $dBR_{12}(1)=44$, 且推论中的下限不是紧的.

设 k, n 均为偶数, $k>2^{(n/2)-1}$, 对于任意矩阵 $S_{k\times n}=(S_{ij})_{k\times n}$, 令

$$S_{k\times n}=(S_{ij})_{k\times n}\triangleq(\alpha_1,\cdots,\alpha_n)\triangleq\begin{pmatrix}x_1\\ \vdots\\ x_k\end{pmatrix}$$

其中 $\alpha_i\in F_2^k(1\leqslant i\leqslant n)$, $x_i\in F_2^n$ 且 $x_i\neq x_j(\forall 1\leqslant i\neq j\leqslant k)$.

记 $u=\frac{k}{2}-2^{(n/2)-2}$, 对任意 $C=(c_1,\cdots,c_n)\in F_2^n$, 记 $\gamma_C=\sum_{i=1}^{N}c_i\alpha_i\triangleq(\gamma_1,\gamma_2)$, $\gamma_1\in F_2^u$, $\gamma_2\in F_2^{u+2^{(n/2)-1}}$. 设 γ_1 中 1 的个数为 a_γ, γ_2 中 1 的个数为 b_γ.

定义 **4**　若对某一整数 t, $1\leqslant t\leqslant n$, 矩阵 $\boldsymbol{S}_{k\times n}$ 满足: 对 $\forall C\in F_2^n$, $wt(C)\leqslant t$, 生成的 γ_C 具有性质: $b_\gamma-a_\gamma=0$ 或 $b_\gamma-a_\gamma=2^{(n/2)-1}$, 则称 $\boldsymbol{S}_{k\times n}$ 为一个 n 元 t 阶弹性矩阵. 特别地, 对一给定的 n, t, 记使得 $\boldsymbol{S}_{k\times n}$ 存在的最小偶数 k 为 $M_n(t)$, 则有:

定理 **1**　$dBR_n(t)\geqslant M_n(t)$

证明　设 $b(x)$ 和 $f(x)$ 是一对满足 $d(b(x),f(x))=dBR_n(t)$ 的 n 元布尔函数, 其中 $b(x)$ 为 bent 函数, $f(x)$ 为 t 阶弹性函数. 不妨设 $W_b(0)=2^{n/2}$, 记 $S=\{x\in F_2^n\mid b(x)\neq f(x)\}$, 则 $|S|=dBR_n(t)$.

设 $S_1=\{x\in F_2^n\mid b(x)=1, f(x)=0\}$, $S_2=\{x\in F_2^n\mid b(x)=0, f(x)=1\}$, 则 $S=S_1\cup S_2$, 按先 S_1 中元素后 S_2 中元素的顺序把 S 中元素填入一个 $dBR_n(t)\times 1$ 的矩阵中, 再将每个元素都按行向量方式展开, 则可以得到一个 $dBR_n(t)\times n$ 的 0, 1 矩阵, 记该矩阵为 $\boldsymbol{M}$. 现在证明 $\boldsymbol{M}$ 是一个 n 元 t 阶弹性矩阵.

事实上, 由于 $f(x)$ 是 t 阶弹性函数, $b(x)$ 是 Bent 函数知, 对 $\forall\omega$, $wt(\omega)\leqslant t$, 有:

$$W_f(\omega)=W_b(\omega)-2\sum W_b(\omega)\mid_S=W_b(\omega)-2\sum_{x\in s_1}(-1)^{\omega\cdot x+1}-2\sum_{x\in s_2}(-1)^{\omega\cdot x}=0$$

特别的, 对 $\omega=0$, 由 $W_b(0)=2^{n/2}$ 知 $|S_2|-|S_1|=2^{(n/2)-1}$; 又由于 $|S_2|+|S_1|=|S|=dBR_n(t)$, 从而有 $|S_1|=\frac{1}{2}dBR_n(t)-2^{(n/2)-2}$, $|S_2|=\frac{1}{2}dBR_n(t)+2^{(n/2)-2}$. 记 $u=|S_1|=\frac{1}{2}dBR_n(t)-2^{(n/2)-2}$, 则 $|S_2|=\frac{1}{2}dBR_n(t)+2^{(n/2)-2}=u+2^{(n/2)-1}$. 记 $\boldsymbol{M}$ 的列向量为 $(\alpha_1,\cdots,\alpha_n)$. $\forall\omega$, $wt(\omega)\leqslant t$, 记 $\gamma_\omega=\sum_{i=1}^{n}\omega_i\alpha_i\triangleq(\gamma_1,\gamma_2)$, $\gamma_1\in F_2^u$, $\gamma_2\in F_2^{u+2^{(n/2)-1}}$. 设 γ_1、γ_2 中 1 的个数分别为 a_γ、b_γ, 则有 $W_b(\omega)-2(a_\gamma-(|S_1|-a_\gamma))-2(|S_2|-2b_\gamma)=0$. 代入 $|S_1|$ 和 $|S_2|$ 的值, 即有 $b_\gamma-a_\gamma=\frac{1}{4}(2^{(n/2)}-W_b(\omega))$. 由于 $b(x)$ 是 Bent 函数, 对 $\forall\omega$, $W_b(\omega)=\pm 2^{n/2}$, 从而有 $b_\gamma-a_\gamma=0$ 或 $b_\gamma-a_\gamma=2^{(n/2)-1}$, 故 $\boldsymbol{M}$ 为一个 n

元 t 阶弹性矩阵, 由 $M_n(t)$ 的定义知: $dBR_n(t) \geqslant M_n(t)$. 证毕

由上面的证明过程, 我们看到对于任何一个 Bent 函数 $b(x)$ 和一个 t 阶弹性函数 $f(x)$, 都可以构造出一个 t 阶弹性矩阵 $\boldsymbol{M}_{k\times n}$, 所以为了构造距离尽可能小的 $b(x)$ 和 $f(x)$, 我们可以先构造使 k 尽可能小的 $\boldsymbol{M}_{k\times n}$, 然后再从 $\boldsymbol{M}_{k\times n}$ 分析对应的 $b(x)$ 函数是否存在, 如果存在, 则我们求出了 $dBR_n(t)$. 由此, 可以得到一个计算 n 元 Bent 函数和 t 阶弹性函数最小距离 $dBR_n(t)$ 的方法, 算法流程如下:

Step1 构造使 k 尽可能小的 $\boldsymbol{M}_{k\times n}$;

Step2 寻找满足下列条件的 Bent 函数 $b(x)$:

(1) $b(x)=1,\ \forall x\in S_1;\ b(x)=0,\ \forall x\in S_2$;

(2) $W_b(0)=2^{n/2},\ \forall \omega\in F_2^n,\ 1\leqslant wt(\omega)\leqslant t$,

如果 $b_\gamma - a_\gamma = 0$, 则 $W_b(\omega)=2^{n/2}$; 如果 $b_\gamma - a_\gamma = 2^{(n/2)-1}$, 则 $W_b(\omega)=-2^{n/2}$;

Step3 如果 step2 可以找到满足条件的 $b(x)$, 则 $dBR_n(t)=k$; 如果失败, 尝试别的 $M_{k\times n}$, 对新的 $M_{k\times n}$, 执行 step2; 如果对于对应该 k 值的所有 $M_{k\times n}$ 都无法找到满足条件的 $b(x)$ 的话, 则把 k 值加 2, 构造新的 $M_{k\times n}$, 执行 step2.

3 Bent 函数和 1 阶弹性函数的最小距离

定理 **2** Bent 函数和 1 阶弹性函数的最小距离满足:

$$dBR_n(1) \geqslant 2^{\frac{n}{2}-1}+2\left\lceil \frac{A}{n-r_1-r_2-2}\right\rceil$$

其中,

$$A=(n-r_1-1)\sum_{i=0}^{r_1}\binom{n}{i}+\sum_{i=0}^{r_2}i\binom{n}{i}+(r_2+1)\left(2^{\frac{n}{2}-1}-\sum_{i=0}^{r_2}\binom{n}{i}\right)-\sum_{i=0}^{r_1}(n-i)\binom{n}{i}$$

其中记 $u=\frac{1}{2}dBR_n(1)-2^{(n/2)-2}$, r_1 为满足 $\sum_{i=0}^{r_1}\binom{n}{r}\leqslant u<\sum_{i=0}^{r_1+1}\binom{n}{i}$ 的整数, r_2 为满足 $\sum_{i=0}^{r_2}\binom{n}{i}\leqslant u+2^{(n/2)-1}<\sum_{i=0}^{r_2+1}\binom{n}{i}$ 的整数.

证明 记 $S_{k\times n}$ 为一个 n 元 1 阶弹性矩阵, $u=\frac{k}{2}-2^{(n/2)-2}$. 由 n 元 t 阶弹性矩阵的定义, S 的任意两行不相等, 且对于 S 中的任意一列 α_i, 令

$$\alpha_i=\begin{pmatrix}\alpha_i^1\\ \alpha_i^2\end{pmatrix},\ \alpha_i^1\in F_2^u,\ \alpha_i^2\in F_2^{u+2^{(n/2)-1}}$$

则 $wt(\alpha_i^1)=wt(\alpha_i^2)$ 或 $wt(\alpha_i^2)-wt(\alpha_i^1)=2^{(n/2)-1}$. 现将 S 的每一列 $\alpha_i(1\leqslant i\leqslant n)$ 做如下变换: 如果 $wt(\alpha_i^1)=wt(\alpha_i^2)$, 则该列不变; 如果 $wt(\alpha_i^2)-wt(\alpha_i^1)=2^{(n/2)-1}$, 则将该列所有元素加 1 模 2. 记生成的新矩阵为 S', 则易见 S' 的任意两行也不相等. 设 $S'=\begin{pmatrix}\boldsymbol{M}_1\\ \boldsymbol{M}_2\end{pmatrix}$, 其中 $\boldsymbol{M}_1$ 为 $u\times n$ 矩阵, $\boldsymbol{M}_2$ 为 $\left(u+2^{(n/2)-1}\right)\times n$ 矩阵, 则易见 $\boldsymbol{M}_1$ 和 $\boldsymbol{M}_2$ 的对应列的 1 的个数相等. 记 N_1, N_2 分别为 $\boldsymbol{M}_1$, $\boldsymbol{M}_2$ 中 1 的总数, 则 $N_1=N_2$. 设 r_1 为满足 $\sum_{i=0}^{r_1}\binom{n}{i}\leqslant u<\sum_{i=0}^{r_1+1}\binom{n}{i}$ 的整数, r_2 为满足 $\sum_{i=0}^{r_2}\binom{n}{i}\leqslant u+2^{(n/2)-1}<\sum_{i=0}^{r_2+1}\binom{n}{i}$ 的整数, 则:

$$N_1\leqslant\sum_{i=0}^{r_1}(n-i)\binom{n}{i}+(n-r_1-1)\left(u-\sum_{i=0}^{r_1+1}\binom{n}{i}\right)$$

$$N_2\geqslant\sum_{i=0}^{r_2}i\binom{n}{i}+(r_2+1)\left(u+2^{(n/2)-1}-\sum_{i=0}^{r_2}\binom{n}{i}\right)$$

而由 $N_1=N_2$ 知:

$$\sum_{i=0}^{r_1}(n-i)\binom{n}{i}+(n-r_1-1)\left(u-\sum_{i=0}^{r_1}\binom{n}{i}\right)\geqslant\sum_{i=0}^{r_2}i\binom{n}{i}+(r_2+1)\left(u+2^{(n/2)-1}-\sum_{i=0}^{r_2}\binom{n}{i}\right)$$

$$(n-r_1-r_2-2)u\geqslant(n-r_1-1)\sum_{i=0}^{r_1}\binom{n}{i}+\sum_{i=0}^{r_2}i\binom{n}{i}+(r_2+1)\left(2^{(n/2)-1}-\sum_{i=0}^{r_2}\binom{n}{i}\right)-\sum_{i=0}^{r_1}(n-i)\binom{n}{i} \quad (1)$$

当 $n-r_1-r_2-2>0$ 时, 进一步, 有

$$u\geqslant\left\lceil\frac{B}{n-r_1-r_2-2}\right\rceil$$

其中,

$$B=(n-r_1-1)\sum_{i=0}^{r_1}\binom{n}{i}+\sum_{i=0}^{r_2}i\binom{n}{i}+(r_2+1)\left(2^{\frac{n}{2}-1}-\sum_{i=0}^{r_2}\binom{n}{i}\right)-\sum_{i=0}^{r_1}(n-i)\binom{n}{i} \quad (2)$$

而由 $u=\frac{k}{2}-2^{(n/2)-2}$ 和 $M_n(1)$ 的定义有

$$dBR_n(1)\geqslant M_n(1)\geqslant 2^{\frac{n}{2}-1}+2\left\lceil\frac{C}{n-r_1-r_2-2}\right\rceil$$

其中,

$$C=(n-r_1-1)\sum_{i=0}^{r_1}\binom{n}{i}+\sum_{i=0}^{r_2}i\binom{n}{i}+(r_2+1)\left(2^{\frac{n}{2}-1}-\sum_{i=0}^{r_2}\binom{n}{i}\right)-\sum_{i=0}^{r_1}(n-i)\binom{n}{i}$$

证毕

由定理 1 得到了 $M_n(1)$ 和 $dBR_n(1)$ 的一个下限. 由上一节的分析, 我们知道如果对于定理 1 中的一个下限

可以构造出相应的 n 元 1 阶弹性矩阵和相应的满足特定性质的 n 元 Bent 函数的话, 就可以求出了 n 元 Bent 函数和 1 阶弹性函数的最小距离 $dBR_n(1)$. 注意到式(1)中 r_1, r_2 是和 u 有一定关系的, 所以下面我们来分析一下式(1).

首先考虑 $u=1$ 在什么情况下成立.

显然此时有 $r_1=0$, 将 $u=1$ 和 $r_1=0$ 代入式(1)中, 有 $n-r_2-1\geqslant\sum_{i=0}^{r_2} i\binom{n}{i}+(r_2+1)\left(2^{(n/2)-1}-\sum_{i=0}^{r_2}\binom{n}{i}\right)$, 由 r_2 定义, $\sum_{i=0}^{r_2}\binom{n}{i}\leqslant u+2^{(n/2)-1}<\sum_{i=0}^{r_2+1}\binom{n}{i}$ 和 $u=1$ 有 $n-r_2-1\geqslant\sum_{i=0}^{r_2} i\binom{n}{i}-(r_2+1)$, 即 $n\geqslant\sum_{i=0}^{r_2} i\binom{n}{i}$, 从而有 $r_2\leqslant 1$. 如果 $r_2=0$, 则 $1+2^{(n/2)-1}<\sum_{i=0}^{r_2+1}\binom{n}{i}=1+n$, 从而 $n\leqslant 6$. 如果 $r_2=1$, 则 $1+2^{(n/2)-1}<\sum_{i=0}^{r_2+1}\binom{n}{i}=1+n+\frac{n(n-1)}{2}$, 从而 $n\leqslant 16$. 但是当 $8\leqslant n\leqslant 16$ 时, 把 $r_1=0$, $r_2=1$ 代入(1)中, 可以得到

$$u\geqslant\left\lceil\frac{2^{n/2}-n-3}{n-3}\right\rceil \tag{3}$$

由式(3), 有表 1:

表 1　$8\leqslant n\leqslant 16$ 时 u 的下限

n	8	10	12	14	16
u 的下限	1	3	6	11	19

注意到当 $n=16$ 时, 有 $u\geqslant 19>1+n=17$, $u+2^{(n/2)-1}\geqslant 19+128=147>1+n+\frac{n(n-1)}{2}=137$, 故此时应该取 $r_1=1$, $r_2=2$, 把该值和 $n=16$ 代入式(1)中重新计算得 $u\geqslant 20$. 再由 $dBR_n(1)\geqslant M_n(1)=2^{(n/2)-1}+2u$, 可以得到 $dBR_n(1)$ 的一个下限, 与文献[4]中的下限放在一起比较可以得到表 2:

表 2　$8\leqslant n\leqslant 16$ 时, 本文和文献[4]中 $dBR_n(1)$ 的下限的比较

n	8	10	12	14	16
文献[4]中 $dBR_n(1)$ 的下限	10	22	42	84	162
本文 $dBR_n(1)$ 的下限	10	22	44	86	168

对于 $8\leqslant n\leqslant 12$ 的情形, 文献[4]中构造了距离达到了我们的下限的 Bent 函数和相应的 1 阶弹性函数对. 因此我们的限对于这些情形都是紧的, 从而我们证实了文献[4]中的猜想, 即"12 元 Bent 函数和 12 元 1 阶弹性函数的最小距离是 44"和"引理 2 中的下限非紧".

对 $n\leqslant 12$ 的情形, 我们求出了 $dBR_n(1)$ 的具体值. 现在来求解 $dBR_{14}(1)$. 由于 $dBR_{14}(1)\geqslant 86$, 我们尝试构造一个 14 元 Bent 函数和一个 1 阶弹性函数, 使其距离为 86. 按照我们给出的算法的思想, 首先构造一个 86×14 的一阶弹性矩阵 S. 由于 $k=86$, $n=14$, 故 $u=\frac{k}{2}-2^{(n/2)-2}=11$, 构造 11×14 的矩阵 $\boldsymbol{S}_1$ 如下:

$$\boldsymbol{S}_1=\begin{pmatrix}
1&1&1&1&1&1&1&1&1&1&1&1&1&1\\
0&0&1&1&1&1&1&1&1&1&1&1&1&1\\
1&1&0&0&1&1&1&1&1&1&1&1&1&1\\
1&1&1&1&0&0&1&1&1&1&1&1&1&1\\
1&1&1&1&1&1&0&0&1&1&1&1&1&1\\
1&1&1&1&1&1&1&1&0&0&1&1&1&1\\
1&1&1&1&1&1&1&1&1&1&0&0&1&1\\
1&1&1&1&1&1&1&1&1&1&1&1&0&0\\
0&1&1&0&1&1&1&1&1&1&1&1&1&1\\
1&0&1&1&0&1&1&1&1&1&1&1&1&1\\
1&1&0&1&1&0&1&1&1&1&1&1&1&1
\end{pmatrix}$$

由于 $u+2^{(n/2)-1}=75$, 现在来构造 75×14 的矩阵 $\boldsymbol{S}_2$, 而且满足 $\boldsymbol{S}_2$ 的前 6 列重为 9, 后 8 列重为 10. 这个构造主要是基于重为 2 的 14 元向量. 为了便于描述, 如果一个重为 2 的向量 $\alpha=(\alpha_1,\alpha_2,\cdots,\alpha_{14})$ 在 $i,j(1\leqslant i\neq j\leqslant 14)$ 处值为 1, 即 $\alpha_i=\alpha_j=1$, $\alpha_k=0$, $k\neq i,j$, 则我们把该向量简记为(i,j). 同理重为 1 的向量 e_j 可以简记为(j). 下面描述一个构造 $\boldsymbol{S}_2$ 的方法:

Step1　把所有重为 2 的 14 元向量一行行地填入一个矩阵 $\boldsymbol{S}_2^1$ 中, 则该矩阵为一个 $C_{14}^2\times 14=91\times 14$ 阵, 且每列重均为 $C_{13}^1=13$;

Step2　在 $\boldsymbol{S}_2^1$ 中除去向量$(i,i+7)$和$(i,14-i)$, $1\leqslant i\leqslant 7$, 记新矩阵为 $\boldsymbol{S}_2^2$, 则其为一个$(91-14)\times 14=77\times 14$ 阵, 且每列重均为 $13-2=11$;

Step3　在 $\boldsymbol{S}_2^2$ 中除去向量$(1,2)$, $(3,4)$和$(5,6)$, 并且添加全 0 向量, 记新矩阵为 $\boldsymbol{S}_2^3$, 则其为一个 75×14 阵, 且前 6 列重为 10, 后 8 列重为 11;

Step4　在 $\boldsymbol{S}_2^3$ 中挑选 14 个向量把它们变为重为 1 的向量, 使得 $\boldsymbol{S}_2^3$ 的每一列重量都减 1, 而且重为 1 的每个向量都恰出现一次. 比如, 一个可行的操作就是$(i,i+2)\rightarrow(i+2)$(定义 $13+2=1$, $14+2=2$), 记新矩阵为 $\boldsymbol{S}_2$. 则 $\boldsymbol{S}_2$ 满足的构造要求, 即其为一个 75×14 阵, 且前 6 列重为 9, 后 8 列重为 10.

记 $\boldsymbol{S}=\begin{pmatrix}\boldsymbol{S}_1\\ \boldsymbol{S}_2\end{pmatrix}$, 则我们得到了一个 86×14 的一阶弹性矩阵 $\boldsymbol{S}$. 下一步, 我们来构造一个 Bent 函数 $b(x)$ 使其满足:

(1) $W_b(\omega)=2^{n/2}=128$, $\forall\,\omega\in F_2^n$, $wt(\omega)\leqslant 1$;

(2) $b(x)=1$, $\forall x\in\boldsymbol{S}_1$; $b(x)=0$, $\forall x\in\boldsymbol{S}_2$.

通过分析, 我们发现取 $b(\boldsymbol{x})=b(\boldsymbol{X},\boldsymbol{Y})=\boldsymbol{X}\cdot\boldsymbol{Y}$ 即满足要求, 其中 $\boldsymbol{x}=(x_1,\cdots,x_{14})$, $\boldsymbol{X}=(x_1,\cdots,x_7)$, $\boldsymbol{Y}=(x_8,\cdots,x_{14})$.

令

$$f(\boldsymbol{x})=\begin{cases} b(\boldsymbol{x})\oplus 1, & \boldsymbol{x}\in \boldsymbol{S} \\ b(\boldsymbol{x}), & \boldsymbol{x}\notin \boldsymbol{S} \end{cases}$$

则由引理 1 的证明过程知,$f(\boldsymbol{x})$ 为 1 阶弹性函数,且 $d(b(\boldsymbol{x}),f(\boldsymbol{x}))=86$,从而 $dBR_{14}(1)\leqslant 86$,再由下限 $dBR_{14}(1)\geqslant 86$知,最终有 $dBR_{14}(1)=86$.

4 结束语

本文研究了 Bent 函数和弹性函数的最小距离,通过分析把该问题转化为一个构造满足一定条件的矩阵的组合问题和一个特定形式的 Bent 函数是否存在的问题,给出了一个求解该问题的算法,并给出了 Bent 函数和弹性函数的最小距离的一个下限公式. 具体到一阶情形,本文改进了 S. Maity 文献[4]中的下限,证实了他们提出的猜想,并且求出了 12、14 元 Bent 函数和一阶弹性函数的最小距离. 本文中得到的限对于 $n\leqslant 14$ 的情形都是紧的,对于 $n\geqslant 16$ 的情形如何,还需要对 1 阶弹性矩阵和 n 元 Bent 函数做深入研究才能确定. 我们估计,随着对 1 阶弹性矩阵和给定形式的 Bent 函数是否存在问题的进一步认识,提出更好的限是很有可能的.

参考文献:

[1] Chor B, Goldreich O, et al. Extraction problem or t-resilient functions[A]. 26th IEEE Symp Foundations of Computer Science[C]. 1985. 26. 396- 407.

[2] M Fedorova, Y V Tarannikov. On the constructing of highly nonlinear resilient Boolean functions by means of special matrices[A]. In Progress in Cryptology INDOCRYPT 2001[C]. volume 2247 in LNCS, Springer Verlag, 2001. 254- 266.

[3] X Gur-Zhen, J Massey. A spectral characterization of correlation immune combining functions[J]. IEEE Transactions on Information Theory, 1988, 34(3): 569- 571.

[4] S Maity, S Maitra, Minimum distance between bent and 1-resilient Boolean functions[A]. In Fast Software Encryption-FSE 2004[C]. volume 3017 in LNCS, Springer Verlag, 2004. 143- 160.

[5] S Maitra, E Pasalic. Further constructions of resilient Boolean functions with very high nonlinearity[J]. IEEE Transactions on Information Theory, 2002, 48(7): 1825- 1834.

[6] S Maity, T Johansson. Construction of cryptographically important boolean functions[A]. In INDOCRYPT 2002[C]. Volume 2551 in LNCS, Springer Verlag, 2002. 234- 245.

[7] O S Rothaus. On bent functions[J]. Journal of Combinatorial Theory, Series A, 1976, 20: 300- 305.

[8] P Sarkar, S Maitra. Nonlinearity bounds and constructions of resilient Boolean functions[A]. In Advances in Cryptology-CRYPTO 2000[C]. volume 1880 in LNCS, Springer Verlag, 2000. 515- 532.

[9] Y V Tarannikov. On resilient Boolean functions with maximum possible nonlinearity[A]. In Progress in Cryptology-INDOCRYPT 2000[C]. volume 1977 in LNCS, Springer Verlag, 2000. 19- 30.

作者简介:

李 超 男,1966 年 7 月生于湖南汨罗,国防科技大学理学院数学与系统科学系教授,博导. 主要研究兴趣:编码密码理论.

E-mail: lichao_nudt@sina.com