第17卷 第3期 电子科学学刊 Vol. 17 No. 3
1995 年 5 月 JOURNAL OF ELECTRONICS May 1995

布尔函数的线性结构的特征

冯登国 肖国镇
(西安电子科技大学信息保密所，西安 710071)

摘要 本文首先利用布尔函数的特征集合对布尔函数的线性结构进行了刻划，给出了寻找布尔函数的线性结构的一种方法. 其次引入了布尔函数的 r 型线性结构的概念，并对其进行了研究，同时还指出了布尔函数的 r 型线性结构的密码学意义.

关键词 布尔函数，线性结构，特征集合

1 引言

在密码学中，一个好的函数必须具有较高的非线性度，亦即它与所有线性和仿射函数的集合之间的汉明距离较大. 而在文献[1]中指出，函数的非线性程度亦可用所谓的函数的线性结构来衡量，因此研究函数的线性结构有着重要意义. 本文主要讨论 n 元布尔函数 $f:F_2^n \to F_2$.

2 线性结构的特征

定义 1 一个向量 $\omega \in F_2^n$ 称为布尔函数 $f:F_2^n \to F_2$ 的一个线性结构，如果对任意的向量 $x \in F_2^n$ 有 $f(x+\omega)-f(x)=$ 常值 $(=f(\omega)-f(0))$.

显然一个布尔函数的全体线性结构 U_f 构成 F_2^n 的一个线性子空间.

定义 2 设布尔函数 $f:F_2^n \to F_2$，令 $V_f=\{x \in F_2^n | f(x)=1\}$，称 V_f 为 f 的特征集合.

为研究问题方便，将布尔函数 f 的线性结构分类，记 $U_0=\{\omega \in F_2^n | f(x+\omega)-f(x)=0, \forall x \in F_2^n\}$，$U_1=\{\omega \in F_2^n | f(x+\omega)-f(x)=1, \forall x \in F_2^n\}$，则 $U_f=U_0 \cup U_1$.

易验证，U_0 是 U_f 的一个线性子空间，而且若 $\alpha,\beta \in U_1$，则 $\alpha-\beta \in U_0$，因而由代数知识易推出 $U_1=b+U_0$，$b \in U_1$，故 $U_f=U_0 \cup (b+U_0)$，由此可见只要讨论清楚 U_0 的结构即可.

定理 1 $\alpha \in U_0$，当且仅当 $\alpha+V_f=V_f$.

证明 "$\Longrightarrow$"设 $\alpha \in U_0$，则对任意的 $x \in F_2^n$ 有 $f(x+\alpha)=f(x)$. 对任意的 $x' \in V_f$，因为 $f(x')=1$，所以 $f(x'+\alpha)=f(x')=1$，即 $x'+\alpha \in V_f$，$x' \in \alpha+V_f$，说明 $V_f \subseteq \alpha+V_f$，但 $|V_f|=|\alpha+V_f|$，所以 $V_f=\alpha+V_f$. 其中 $|V|$ 表示集 V 中元素的个数.

1993-11-25 收到，1994-05-06 定稿
冯登国 男，1965 年生，博士生，现从事密码学、编码学、信息论的研究.
肖国镇 男，1935 年生，教授，博士生导师，现从事密码学、编码学、信息论、应用数学等方面的教学和研究.

"$\Leftarrow$"设 $\alpha+V_f=V_f$，对任意的 $x\in F_2^n$，若 $x\in V_f$，则 $x+\alpha\in V_f$，所以 $f(x)=f(x+\alpha)=1$. 若 $x\notin V_f$，则 $f(x)=0$. 下面说明 $x+\alpha\notin V_f$，否则 $x+\alpha\in V_f$，$x\in\alpha+V_f=V_f$，矛盾. 所以 $x+\alpha\notin V_f$，即 $f(x+\alpha)=0=f(x)$. 由定义 1 知 $\alpha\in U_0$.

推论 1　若 $U_0\neq\{0\}$，则 $|V_f|$ 必为偶数.

证明　由定理 1 知，x 和 $x+\alpha$ 同属于 V_f 或同不属于 V_f. 当 $\alpha\neq 0$ 时，$|V_f|$ 为偶数.

推论 2　$\alpha\neq 0$，$\alpha\in U_0$，当且仅当对任何 $V\subset V_f$，$|V|=|V_f|/2$ 有 $\alpha+V=V_f\backslash V$.

类似于定理 1 的证明可得出：

定理 2　$\alpha\in U_1$，当且仅当 $\alpha+V_f=F_2^n\backslash V_f$.

推论 3　若 $U_1\neq\phi$，则 $|V_f|=2^{n-1}$，即 f 为平衡布尔函数.

证明　由定理 2 知，若 $\alpha\in U_1$，则 $\alpha+V_f=F_2^n\backslash V_f$，$|\alpha+V_f|=|F_2^n\backslash V_f|$；又 $|\alpha+V_f|=|V_f|$，$|F_2^n\backslash V_f|=2^n-|V_f|$；故 $|V_f|=2^{n-1}$.

推论 4　$\alpha\in U_1$，当且仅当对任何 $V\subset V_f$，$|V|=|V_f|/2$ 有 $\alpha+V=F_2^n\backslash(V_f\cup(\alpha+V))$.

由定理 1 和定理 2 可得：

定理 3　(1) 若 $(0,0,\cdots,0)\in V_f$，则 $U_0\subseteq V_f$，$U_1\subseteq F_2^n\backslash V_f$. (2) 若 $(0,0,\cdots,0)\in F_2^n\backslash V_f$，则 $U_0\subseteq F_2^n\backslash V_f$，$U_1\subseteq V_f$.

由推论 3 知，当 $U_1\neq\phi$ 时，$|V_f|=2^{n-1}$. 那么当 $|V_f|\neq 2^{n-1}$ 时，$U_1=\phi$，此时 $U_f=U_0$.

定理 4　设 U_0 的维数为 r，则 $|V_f|=2^r\cdot s$.

证明　当 $(0,0,\cdots,0)\in V_f$ 时，由定理 3 的(1)知 $U_0\subseteq V_f$. 若 $U_0=V_f$，显然 $|V_f|=|U_0|=2^r$；否则取 $b_1\in V_f$，$b_1\notin U_0$，由定理 1 知，$(b_1+U_0)\subseteq V_f$. 因此 $U_0\cup(b_1+U_0)\subseteq V_f$，若 $U_0\cup(b_1+U_0)=V_f$，易知 $U_0\cap(b_1+U_0)=\phi$. $|U_0|=|(b_1+U_0)|=2^r$，所以 $|V_f|=2^r\cdot 2$；否则取 $b_2\notin U_0\cup(b_1+U_0)$，$b_2\in V_f$，由定理 1 知，$(b_2+U_0)\subseteq V_f$. 按这种方法取下去，因为 V_f 中的元素有限，所以总可以做到 $V_f=U_0\cup(b_1+U_0)\cup\cdots\cup(b_{s-1}+U_0)$ 且 $(b_i+U_0)\cap(b_j+U_0)=\phi(i\neq j)$，$|U_0|=|(b_1+U_0)|=\cdots=|(b_{s-1}+U_0)|=2^r$，故 $|V_f|=2^r\cdot s$.

当 $(0,0,\cdots,0)\in F_2^n\backslash V_f$ 时，由定理 3 的(2)知，$U_0\subseteq F_2^n\backslash V_f$. 按上述方法可得 $|F_2^n\backslash V_f|=2^r\cdot s$. 因此 $|V_f|=2^n-2^r\cdot s=2^r(2^{n-r}-s)$.

定理 5　$U_f=F_2^n$，当且仅当 f 为线性或仿射函数.

证明　"$\Leftarrow$"直接按定义可验证当 f 为线性或仿射函数时，$U_f=F_2^n$.

"$\Rightarrow$"设 $U_f=F_2^n$，若 $U_1=\phi$，由定理 4 知，$|V_f|=2^r\cdot s$，不妨设 $(0,0,\cdots,0)\in V_f$，这里 $r=n$，即 $|V_f|=2^n\cdot s$. 又 $V_f\neq\phi$，所以 s 只能等于 1. 这样 $V_f=F_2^n$. f 是常值函数 1，即为仿射函数. 若 $U_1\neq\phi$，则 $|U_1|=|U_0|=2^{n-1}$. 不妨设 $(0,0,\cdots,0)\in V_f$，则 $U_0\subseteq V_f$. 由推论 3 知，$|V_f|=2^{n-1}$，故 $V_f=U_0$，即 V_f 是一个 $n-1$ 维的线性子空间. 因此由代数知识可知，V_f 是某个一元齐次线性方程 $\omega\cdot x=0$ 的正交子空

间，令 $g(x)=\omega\cdot x+1$，则 $g(x)$ 以 V_f 为特征集合．因此 $f(x)=g(x)=\omega\cdot x+1$ 为仿射函数．

定理 6 不存在布尔函数 f 使其线性结构空间 U_f 的维数为 $n-1$．

证明 反设布尔函数 f 的线性结构空间 U_f 的维数为 $n-1$．不妨设 $(0,0,\cdots,0)\in V_f$，若 $U_1=\phi$，则 $U_0=U_f$，$|V_f|=2^{n-1}\cdot s$．先证 $s\neq 2$，否则 $|V_f|=2^n$，此时 $f(x)=1$，从而 $U_0=U_f=F_2^n$．$U_f=U_0$ 的维数为 n，矛盾．再证 $s\neq 1$，否则 $V_f=U_0$，则 V_f 为 $n-1$ 维线性子空间．由代数知识知，$f(x)$ 是一个仿射函数，而仿射函数的线性结构空间的维数为 n，矛盾．说明 $U_1\neq\phi$，此时 $|V_f|=2^{n-1}$，$|U_0|=2^{n-2}$，$U_0\subseteq V_f$．下证 V_f 是一个线性子空间．对任何 $\alpha,\beta\in V_f$，由前面的讨论知，$V_f=U_0\cup(b+U_0)$．若 α,β 中之一属于 U_0，则 $\alpha+\beta\in V_f$．若 α,β 都不属于 U_0，则 $\alpha,\beta\in b+U_0$，从而 $\alpha=b+x$，$\beta=b+y$，$x,y\in U_0$，$\alpha+\beta=(b+x)+(b+y)=x+y\in U_0$，故 V_f 是一个 $n-1$ 维的线性子空间．由代数知识知，f 是一个仿射函数，而仿射函数的线性结构空间的维数为 n，矛盾．至此我们证明了不存在线性结构空间的维数为 $n-1$ 的布尔函数．

由上述讨论知，给定某个线性子空间 $U\subseteq F_2^n$，我们可以构造出布尔函数 f 使得 $U_0=U$．对于给定的布尔函数 f，$|V_f|$ 是一个定值，由定理 4 知 U_0 的维数和 $|V_f|$ 之间必须满足一定的关系．若 $|V_f|=2^r\cdot s$，s 是一个奇数，则 U_0 的维数小于、等于 r．

给定布尔函数 $f:F_2^n\to F_2$，下面介绍找 f 的线性结构的一种方法．

2.1 找第一类线性结构之集 U_0

(1) 计算 $f(0,0,\cdots,0)$，判断 $(0,0,\cdots,0)$ 是否属于 V_f，结合定理 3 便可知 U_0 包含在哪个集中．不妨设 $(0,0,\cdots,0)\in V_f$，则 $U_0\subseteq V_f$．

(2) 任取 $\alpha\in V_f$，下面验证 α 是否属于 U_0．把 V_f 任意分成两半，设为 V 和 $V_f\backslash V$，$|V|=|V_f\backslash V|$．若 $\alpha+V=V_f\backslash V$，则 $\alpha\in U_0$，否则 $\alpha\notin U_0$．当 $|V_f|$ 比 $|F_2^n\backslash V_f|$ 大得多时，利用集 $F_2^n\backslash V_f$．把 $F_2^n\backslash V_f$ 分成两半，设为 V 和 $(F_2^n\backslash V_f)\backslash V$，$|V|=|(F_2^n\backslash V_f)\backslash V|$．若 $\alpha+(F_2^n\backslash V_f)\backslash V=V$，则 $\alpha\in U_0$，否则 $\alpha\notin U_0$．

2.2 找第二类线性结构之集 U_1

(1) 若 $|V_f|\neq 2^{n-1}$ 或 $|U_0|=2^{n-2}$，由推论 3 和定理 6 知，$U_1=\phi$．

(2) 若 $|V_f|=2^{n-1}$，$|U_0|\neq 2^{n-2}$，不妨设 $(0,0,\cdots,0)\in V_f$．由定理 3 的(1)知，$U_1\subseteq F_2^n\backslash V_f$．任取 $\alpha\in F_2^n\backslash V_f$，由定理 2 验证 α 是否属于 U_1．只要找到一个 $\alpha\in U_1$，则 $U_1=\alpha+U_0$．

3 r 型线性结构

一个布尔函数 f 在点 $\alpha\neq 0$ 的非线性是由局部非线性[2] $P_{f(\alpha)}=\max\limits_{\beta=0,1}P(f(x+\alpha)-f(x)=\beta)$ 来度量的．从密码学角度来讲，不希望出现高概率的非零点．对于 f 的线性结构 α：$P_{f(\alpha)}=1$．从实用角度来考虑，不能只注意到使 $P_{f(\alpha)}=1$ 的点，我们也应该注意到使 $P_{f(\alpha)}$ 接近于 1 的点．有的点虽然不是线性结构点，但它与线性结构点差不多．

例如，令布尔函数 $f:F_2^3\to F_2$ 的特征集合为 $V_f=\{(0,0,0),(1,1,1),(0,1,0),(1,0,1),(0,0,1)\}$，考察点 $\alpha=(1,1,1)$．$\alpha+V_f=\{(1,1,1),(0,0,0),(1,0,1),(0,$

1,0),(1,1,0)}. $\alpha+V_f$ 与 V_f 有四个点一样，只有一个点不一样. 将点(0,0,1)和 $\alpha+(0,0,1)=(1,1,0)$ 去掉，我们发现 α 满足条件：对任何 $x\in F_2^n\backslash V$，$V=\{(0,0,1),(1,1,0)\}$，有 $f(x+\alpha)-f(x)=0$. 对于这种点 α，有 $P_{f(\alpha)}=(2^n-2)/2^n=1-|V|/2^n$. 可见当 $|V|\ll 2^n$ 时，$P_{f(\alpha)}\approx 1$. 由此可见，研究这种点很有必要.

定义 3　设布尔函数 $f:F_2^n\to F_2$，给定整数 r，$0\leqslant r\leqslant 2^n$，称 α 为布尔函数 f 的 r 型线性结构，如果存在一个集合 $V(\alpha):|V(\alpha)|\leqslant r$，使得对每个 $x\in F_2^n\backslash V(\alpha)$，有 $f(x+\alpha)-f(x)=$ 常值 $(=f(\alpha)-f(0))$. 特别地，当 $V(\alpha)$ 与 α 的选择无关时，此时 $|V(\alpha)|=$ 常值，不妨设等于 r，称 α 为一致 r 型线性结构. 显然，当 $r=0$ 时，$f(x)$的一致 0 型线性结构就是上节所说的线性结构.

对 r 型线性结构 α 来说，$P_f(\alpha)\geqslant(2^n-r)/2^n=1-r/2^n$. 当 $r\ll 2^n$ 时，$P_f(\alpha)\approx 1$.

由定义易知，当 $s\leqslant r$ 时，s 型线性结构一定是 r 型线性结构. 令布尔函数 $f:F_2^n\to F_2$ 的 r 型线性结构的集合为 $U_f^{(r)}$，将其分为两类：

第一类为 $U_0^{(r)}=\{\alpha\in F_2^n|$存在 $V(\alpha),|V(\alpha)|\leqslant r$，对任何 $x\in F_2^n\backslash V(\alpha),f(x+\alpha)=f(x)\}$.

第二类为 $U_1^{(r)}=\{\alpha\in F_2^n|$存在 $V(\alpha),|V(\alpha)|\leqslant r$，对任何 $x\in F_2^n\backslash V(\alpha),f(x+\alpha)=f(x)+1\}$.

$U_0^{(r)}$ 和 $U_1^{(r)}$ 都未必是线性子空间.

类似于定理 1 和定理 2 可证明

定理 7　$\alpha\in U_0^{(r)}$，当且仅当存在 $V(\alpha):|V(\alpha)|\leqslant r$，对任何 $x\in V_f\backslash V(\alpha)$有：$\alpha+V_f\backslash V(\alpha)=V_f\backslash V(\alpha)$.

定理 8　$\alpha\in U_1^{(r)}$，当且仅当存在 $V(\alpha):|V(\alpha)|\leqslant r$，对任何 $x\in V_f\backslash V(\alpha)$ 有：$\alpha+V_f\backslash V(\alpha)=F_2^n\backslash(V_f\backslash V(\alpha))$.

下面给出判断 α 是否是 r 型线性结构的一个方法. 判断方法与上节类似.

(1) 判断第一类 r 型线性结构的方法　先计算 $\alpha+V_f$，再与 V_f 相比较，如果至多只有 $r/2$ 个不同，那么 $\alpha\in U_0^{(r)}$，否则 $\alpha\notin U_0^{(r)}$.

(2) 判断第二类 r 型线性结构的方法　先计算 $\alpha+V_f$，再与 $F_2^n\backslash V_f$ 相比较，如果至多只有 $r/2$ 个不同，那么 $\alpha\in U_1^{(r)}$，否则 $\alpha\notin U_1^{(r)}$.

参　考　文　献

[1] Nyberg K. On the construction of highly nonlinear permutations. Advances in Cryptology, Proc. Eurocrypto' 92, Springer-Verlag, 1993, 92—98.

[2] Nyberg K, Knudsen L R. Provable Security against Differential Cryptanalysis. Advances in Cryptology, Proc. ,Eurocrypto'92, Springer-Verlag, 1993, 566—574.

CHARACTER OF LINEAR STRUCTURES OF BOOLEAN FUNCTIONS

Feng Dengguo Xiao Guozhen
(Institute of Information Security, Xidian University, Xi'an 710071)

Abstract The linear structures of Boolean functions are discussed using characteristic set of Boolean functions, and a way to find linear structures of Boolean functions is given. Then, the linear structures of Boolean functions are generalized, and r-type linear structures of Boolean functions are presented and studied, meanwhile the cryptological significance of r-type linear structures of Boolean functions is described.

Key words Boolean function, Linear structure, Characteristic set