5 元饱和最优布尔函数的计数问题*

谢 敏[1,2+], 裴定一[1]

[1](信息安全国家重点实验室(中国科学院研究生院),北京 100049)

[2](计算机网络与信息安全教育部重点实验室(西安电子科技大学),陕西 西安 710071)

On the Number of 5-Variable Best Boolean Functions

XIE Min[1,2+], PEI Ding-Yi[1]

[1](State Key Laboratory of Information Security (Graduate School of Chinese Academy of Sciences), Beijing 100049, China)

[2](Key Laboratory of Computer Networks and Information Security (Xidian University), Ministry of Education, Xi'an 710071, China)

+ Corresponding author: E-mail: xiekemin@163.com

Received 2003-11-17; Accepted 2004-03-02

Xie M, Pei DY. On the number of 5-variable best boolean functions. *Journal of Software*, 2005,16(4):595−600.
DOI: 10.1360/jos160595

Abstract: The n-variable and m-resilient ($m>n/2-2$) Boolean functions achieving both the upper bound on nonlinearity $2^{n-1}-2^{m+1}$ and the upper bound on algebraic degree $n-m-1$ must have three valued Walsh spectra: $0,\pm 2^{m+2}$, which are called saturated best (SB in short). Using the known results of weight distributions of the cosets of the (32,6) Reed-Muller code and a new construction method for SB functions gives the number of the 5-variable SB functions.

Key words: nonlinearity; correlation immunity; Walsh transform; best function

摘 要: 同时达到代数次数上界 $n-m-1$ 和非线性度上界 $2^{n-1}-2^{m+1}$ 的 n 元 m 阶弹性布尔函数($m>n/2-2$)具有 3 个 Walsh 谱值:$0,\pm 2^{m+2}$,这样的函数被称为饱和最优函数(saturated best,简称 SB).将利用(32,6)Reed-Muller 码陪集重量的分布,从一种全新的构造角度出发,给出 $n=5$ 的饱和最优函数的个数.

关键词: 非线性度;相关免疫;Walsh 谱;最优函数

中图法分类号: TP309 **文献标识码**: A

布尔函数在信息安全领域有着很好的应用,具有良好密码性质的函数在密码体制中发挥着重要作用.具有 3 个 Walsh 谱值的布尔函数受到了广大学者的关注(如 Sarkar[5],Tarannikov[9]).众所周知,n 元 m 阶弹性函数($m>n/2-2$)最大可能的非线性度为 $2^{n-1}-2^{m+1}$,最大的代数次数为 $n-m-1$,同时达到这两个上界的函数具有 3 个 Walsh 谱值:$0,\pm 2^{m+2}$.这类平衡布尔函数被称为饱和最优函数(saturated best,简称 SB),在流密码领域具有很好的

* Supported by the National Natural Science Foundation of China under Grant No.19931010 (国家自然科学基金); the National Grand Fundamental Research 973 Program of China under Grant No.G1999035804 (国家重点基础研究发展规划(973))

作者简介: 谢敏(1976−),女,湖南桃源人,博士,主要研究领域为密码学,信息安全;裴定一(1941−),男,教授,主要研究领域为密码学,信息安全.

应用价值.对一个三谱值 n 元 m 阶弹性函数($m>n/2-2$),只要代数次数和非线性度之一达到其上界,则另一个亦达到其上界.

我们用(n,m,d,x)记非线性度为 x 代数次数为 d 的 n 元 m 阶弹性布尔函数.具有相同参数的函数(n,m,d,x)若存在,将是不唯一的.设整数 $i\geq 0, j\geq 1$,令 $f_{i,0}$ 表示$(3+2i,i,2+i,2^{2+2i}-2^{i+1})$SB 函数(注意条件 $m>n/2-2$),$f_{i,j}$ 表示$(n_j,m_j,2+i,x_j)$SB 函数,其中 $n_j=n_{j-1}+1, m_j=m_{j-1}+1, x_j=2x_{j-1}$.这样,我们得到了饱和最优函数序列 SBS($i$).可以证明任意 SB 函数一定属于某一序列 SBS(i)($i\geq 0$)[5].易证,若 $f_{i,j}$ 为函数序列 SBS(i)中的第 j 个函数,则 $g=Y\oplus f_{i,j}$(Y 不出现在 $f_{i,j}$ 中)是序列 SBS(i)中的函数 $f_{i,j+1}$.利用类似 Maiorana-McFarland 函数构造方法,对所有 $t\geq t_0$ 可以构造 $f_{i,t}$,其中 $2^{1+i}=3+i+t_0$[5].

序列 SBS(0)和 SBS(1)中的所有函数都已知,而构造初始函数 $f_{i,0}, i\geq 2$ 还相当困难.Pasalic,Johansson,Maitra 和 Sarkar[3]构造出了(7,2,4,56)函数,即 $f_{2,0}$.但构造初始函数 $f_{i,0}, i\geq 3$ 还是一个未解决的问题.在(7,2,4,56)函数已有的构造方法中[3,11],都用到了 5 个变元的饱和最优函数,即(5,1,3,12)函数.如果能搞清楚所有(5,1,3,12)函数的分布性质,就能很好地控制(7,2,4,56)函数的构造,进而推动变元个数更大的饱和最优函数的构造.本文将研究(5,1,3,12)函数的计数问题,利用已有关于(32,6)Reed-Muller 码陪集重量分布的结果,确切地给出所有(5,1,3,12)函数的总数.同时,我们也找到了(5,1,3,12)函数的一些有价值的分布特征.

$\{0,1\}^n$ 上函数 f 的 Walsh 变换定义为

$$W_f(\lambda)=\sum_x (-1)^{f(x)+\lambda\cdot x}, \lambda\in\{0,1\}^n \tag{1}$$

其中,x 遍历$\{0,1\}^n$.它的逆变换定义为

$$(-1)^{f(x)}=2^{-n}\sum_\lambda W_f(\lambda)(-1)^{\lambda\cdot x} \tag{2}$$

其中,λ遍历$\{0,1\}^n$.我们有 Parseval 等式 $\sum_\lambda W_f^2(\lambda)=4^n$.

1 关于三 Walsh 谱函数的构造

设 f 为具有三 Walsh 谱值:$0,\pm d$ 的 n 元函数,k 为使得 $W_f(\lambda)\neq 0$ 的$\lambda\in\{0,1\}^n$ 的个数.由 Parseval 等式可知 $k\cdot d^2=2^{2n}$,可见 k 为一个平方数,记 $k=s^2$,则有 $d^2=(2^n/s)^2$,因而 $s|2^n$,记 $s=2^r$,则 $k=2^{2r}=4^r$.

设 $NZ(f)=\{\lambda|W_f(\lambda)\neq 0\}=\{\lambda_i=(\lambda_{1,i},\ldots,\lambda_{n,i})^t, 1\leq i\leq k\}$(这里视$\lambda_i$为列向量)是函数 f 具有非零 Walsh 谱值的位置的集合.下文中,$NZ(f)$亦表示其相应的$\{0,1\}$上的 $n\times k$ 阶矩阵.

为方便起见,我们引入 k 维向量 $h=(h_1,h_2,\ldots,h_k)$来表示 f 非零 Walsh 谱值相应的符号,其中

$$h_i=\begin{cases}0, & W_f(\lambda_i)>0\\ 1, & W_f(\lambda_i)<0\end{cases}.$$

关于三谱值函数 f 的 $NZ(f)$,我们有如下定理.不失一般性,我们假设 $f(0)=0$.Walsh 谱值为正值的个数 $a=2^{2r-1}+2^{r-1}$.

定理 1[11]. $NZ(f)$矩阵的 n 个行向量生成的线性子空间$\{\lambda^j=(\lambda_{j,1},\lambda_{j,2},\ldots,\lambda_{j,k}), 1\leq j\leq 2^n\}$满足如下性质:对任意 j, $1\leq j\leq 2^n$,记 $\lambda^{j+}=(\lambda_{j,i_1},\lambda_{j,i_2},\ldots,\lambda_{j,i_a})$, $\lambda^{j-}=(\lambda_{j,\gamma_1},\lambda_{j,\gamma_2},\ldots,\lambda_{j,\gamma_{k-a}})$,其中,$a=2^{2r-1}+2^{r-1}$, $h_{i_l}=0 (1\leq l\leq a)$, $h_{\gamma_l}=0 (1\leq l\leq k-a)$,则 λ^{j+} 与 λ^{j-} 两部分具有相同个数的 1,或相同个数的 0.

基于定理 1,我们可以利用下面的方法来构造三谱值布尔函数.

寻找$(n+1)\times k$ 阶矩阵 $\begin{pmatrix}NZ(f)\\ h\end{pmatrix}$使 $NZ(f)$满足定理 1 中的条件,且其各列向量两两不同.其中,$\begin{pmatrix}NZ(f)\\ h\end{pmatrix}$表示将符号向量 h 添加在 $NZ(f)$后.

易知在不考虑$\begin{pmatrix}NZ(f)\\ h\end{pmatrix}$各列的顺序下,不同的$\begin{pmatrix}NZ(f)\\ h\end{pmatrix}$对应不同的函数.这样构造函数 f 的问题,就转为构造相应的矩阵$\begin{pmatrix}NZ(f)\\ h\end{pmatrix}$了.如果能找到该相应的矩阵,我们就可以利用 Walsh 逆变换(2)得到函数 f.

具体来说,对(5,1,3,12)函数,有 $d=2^{m+2}=2^{1+2}=8$,则 $k=4^{5-1-2}=16$,构造(5,1,3,12)函数就等于构造满足以下条件的矩阵 $\begin{pmatrix} NZ(f) \\ h \end{pmatrix}_{6\times 16}$:$NZ(f)$满足定理 1 中条件;$NZ(f)$各列向量(16 个)两两不同;16 个列向量的重量均大于等于 2.(☆)

2 (5,1,3,12)函数的计数

文献[1]给出了(32,6)Reed-Muller 码陪集重量分布的结果,为我们提供了寻找(5,1,3,12)函数的范围.

定义等价关系[1]:5 元函数 f 和 g 是等价的当且仅当存在 5 阶二元可逆矩阵 $\mu,a,b\in\{0,1\}^5$ 及 $c\in\{0,1\}$,使

$$g(x)=f(x\cdot\mu+a)+x\cdot b+c \tag{3}$$

这里,我们视 x,a 为行向量,b 为列向量.

定理 2[1]. 按以上等价关系,5 个变量的布尔函数可分为 48 个等价类,其中次数为 3,非线性度为 12 的等价类仅有如下两个:(1) $x_1x_2x_3+x_1x_4+x_2x_5+A_5(x)$;(2) $x_1x_2x_3+x_1x_4x_5+x_2x_3+x_2x_4+x_3x_5+A_5(x)$.其中,$A_5(x)$为 5 元仿射函数的集合.

下文中所说的"函数陪集"是指关于仿射函数 $A_5(x)$的陪集.

引理 1. 在等价类(1),(2)中,每一函数陪集内的平衡函数占陪集内函数总数的一半.

证明:由文献[1]可知,两个等价类中每一函数 Walsh 谱值非零的个数均为 16 个.注意到,函数的非零 Walsh 谱值个数即为函数陪集中不平衡函数个数的一半.因而,每一函数陪集中有 32 个平衡函数,32 个非平衡函数.由此得证. □

引理 2[7]. 在变量的仿射变换作用下,函数的代数次数、非线性度及平衡性是不变的.

由此得知,要寻找(5,1,3,12)函数,只需考虑定理 2 中的两个等价类.

下面我们来考察一下确定等价关系的变换(3)对函数 f 所对应的矩阵 $\begin{pmatrix} NZ(f) \\ h \end{pmatrix}$ 有什么作用.

引理 3. f,g 为 5 元布尔函数,$g(x)=f(xM+a)+x\cdot b+c$,其中 M 为 5 阶二元可逆矩阵,$a,b\in\{0,1\}^5$,$c\in\{0,1\}$,令 f,g 对应的符号向量为 h_f,h_g,则

(1) $NZ(g)=M\cdot NZ(f)+B, B=\overbrace{(b,b,...,b)}^{16}$, (2) $h_g=h_f+h$, 其中 $h=a\cdot NZ(f)+C, C=\overbrace{(c,c,...,c)}^{16}$.

证明:考虑两函数的 Walsh 变换,我们有

$$W_f(\lambda)=(-1)^{a\lambda+c}W_g(M\cdot\lambda+b) \tag{*}$$

事实上,

$$(-1)^{a\lambda+c}W_g(M\cdot\lambda+b)=(-1)^{a\lambda+c}\sum_{x\in\{0,1\}^5}(-1)^{g(x)+x(M\cdot\lambda+b)}=\sum_{x\in\{0,1\}^5}(-1)^{f(xM+a)+x\cdot b+c+x(M\cdot\lambda+b)+a\lambda+c}$$

$$=\sum_{x\in\{0,1\}^5}(-1)^{f(xM+a)+(xM+a)\lambda}=W_f(\lambda).$$

由(*)可知,M,b 改变函数非零 Walsh 谱位置,a,c 改变函数非零 Walsh 谱值的符号.由此即得引理结论. □

由我们的构造方法及引理 3 易得下面的推论.

推论 1. 若 $f(xM)$为(5,1,3,12)函数,M 为 5 阶二元可逆矩阵,则对 M 进行行间置换得到 M',亦有 $f(xM')$为(5,1,3,12)函数.

我们可以验证以下结果.

引理 4. 在等价类(1)(2)中,每一函数陪集中的平衡函数,可由其中任一平衡函数 $f(x)$经变换 $f(xM+a)+c$ 得到,其中,M 为 5 阶二元可逆矩阵,$a\in\{0,1\}^5$,$c\in\{0,1\}$.

将全体形如 $\varphi: f\mapsto\varphi(f)=f(xM+a)+c$ (其中 M 为 5 阶二元可逆矩阵,$a\in\{0,1\}^5$,$c\in\{0,1\}$)的变换组成的群记为 ρ.

引理 5. 在等价类(1)中任取平衡函数 $f(x)$,该等价类中平衡函数可由 $f(x)$经 ρ 中的变换得到.同样结论对等价类(2)也成立.

证明:设 $g(x)$为等价类(1)中的任意一个平衡函数,因它与 $f(x)$等价,故有 $g(xM+a)+x\cdot b+c=f(x)$,即

$$g(xM+a)+c=f(x)+x\cdot b,$$

上式左端为平衡函数,所以由引理 2 右端也为平衡函数,且与 $f(x)$属于同一函数陪集,由引理 4,存在$\phi\in\rho$,使

$$g(xM+a)+c=\phi(f),$$

左端也可表示为$\phi'(g)(\phi'\in\|)$,故 $g=(\phi')^{-1}\phi(f)$. □

在等价类(1),(2)中,分别取平衡函数 $f_1(x)$,$f_2(x)$.(5,1,3,12)函数一定是平衡的,故

$$G_i=\{\phi(f_i)|\phi\in\rho,\phi(f_i)\text{为(5,1,3,12)函数}\},i=1,2.$$

即分别为等价类(1)与(2)中的所有(5,1,3,12)函数.以 G 表示全体(5,1,3,12)函数,我们有 $G=G_1\cup G_2$.由引理 2,等价类(1)、(2)中的函数为(5,1,3,12)函数,当且仅当它为 1 阶相关免疫函数.

考虑 G_i 中的函数个数.对一个固定好的可逆矩阵 M,若 $f_i(xM)$是 1 阶相关免疫函数,则对任意 a 和 c,$f_i(xM+a)+c$ 也是 1 阶相关免疫函数,因它与 $f_i(xM)$具有相同的 NZ 集合(引理 3).反之,若对某一 a 和 c,$f_i(xM+a)+c$ 是 1 阶相关免疫函数,同样由引理 3 可知,$f_i(xM)$也是 1 阶相关免疫函数.

令$\mu_i=\{M|f_i(xM)\text{为(5,1,3,12)函数},M\text{为可逆矩阵}\},i=1,2$.可见$|G_i|=64|\mu_i|$.

在 G_i 中,同一函数会重复出现.若$\phi_1(f_i)=\phi_2(f_i),\phi_1,\phi_2\in\rho$,则 $f_i=\phi_1^{-1}\phi_2(f_i)$.定义$\rho$的子群

$$\rho_i=\{\phi\in\rho|f_i=\phi(f_i)\},i=1,2.$$

ρ中关于ρ_i的同一陪集中的变换将f_i变为同一个函数,可见 G_i 中同一函数重复出现的次数为$|\rho_i|$.上述推论即证明了下面的定理.

定理 3. $|G|=|G_1|+|G_2|=64\left(\dfrac{|\mu_1|}{|\rho_1|}+\dfrac{|\mu_2|}{|\rho_2|}\right)$.

3 计算结果

我们取等价类(1)中函数 $f_1(x)=x_1x_2x_3+x_1x_4+x_2x_5+x_3$,取等价类(2)中函数 $f_2(x)=x_1x_2x_3+x_1x_4x_5+x_2x_3+x_2x_4+x_3x_5+x_4+x_5$.

以下分别来确定$|\mu_i|$及$|\rho_i|$,$i=1,2$,算法如下.

关于$|\mu_i|$.

输入:NZ_i,h_i.

输出:使 $M\cdot NZ_i$ 满足条件(☆)的 M 的个数(不考虑 M 的行间变换).

开始

第 1 步:计算 NZ_i 的 32 种行间组合构成的矩阵 N,将组合系数作为相应行的编号.

第 2 步:从 N 中任选 5 行构成 NZ_i',5 行在 N 中的行号构成矩阵 M,行号严格递增.

第 3 步:检查 M 是否可逆:若 M 不可逆,转至第 2 步;若 M 可逆,转至第 4 步.

第 4 步:检查 NZ_i'是否符合条件(☆):若不符合,转至第 2 步;若符合,计数器加 1.

重复第 2~4 步,直至第 2 步达到循环条件,输出计数器值.

结束

由推论 1,此程序中不考虑 M 的行间置换,这样大大提高了效率.事实上,我们是从一个三谱值函数的 NZ 集出发,故而在上面第 4 步中,只需检查 NZ_i'是否符合条件(☆)中的最后一条即可,这也大大提高了程序的效率.

我们输入:

$$NZ_1=\begin{pmatrix}0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1\\0&0&0&0&1&1&1&1&0&0&0&0&1&1&1&1\\0&1&1&1&0&1&1&1&0&1&1&1&0&1&1&1\\1&0&0&1&1&0&0&1&1&0&0&1&1&0&0&1\\1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0\end{pmatrix},$$

$$h_1=(0,\ 0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 1,\ 1,\ 0,\ 0,\ 1,\ 1,\ 1,\ 0,\ 0);$$

$$NZ_2=\begin{pmatrix}0&0&0&0&0&0&0&0&0&0&1&1&1&1&1&1\\0&0&0&0&0&0&1&1&1&1&0&0&1&1&1&1\\0&0&0&1&1&1&0&0&0&1&0&1&0&1&1&1\\0&1&1&0&1&1&0&1&1&0&0&0&0&0&1&1\\1&0&1&1&0&1&1&0&1&0&0&0&0&1&0&1\end{pmatrix},$$

$$h_2=(0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 1,\ 0,\ 0,\ 1,\ 1,\ 0,\ 0,\ 1,\ 1,\ 0).$$

可以得到$|\mu_1|=1248\times120$,$|\mu_2|=1512\times120$.

关于$|\rho_i|$.

输入: NZ_i, h_i.

输出:使 $f(x)=f(xM+a)+c$(c=0 或 1)的(M,a,c)的个数,即$|\rho_i|$.

开始

第 1 步:计算 NZ_i 的 32 种行间组合构成的矩阵 N,将组合系数作为相应行的编号.

第 2 步:计算变换 a,c 所能得到的符号向量的集合 $FH=(h_i+N)\cup(h_i+N+\mathbf{1}),h_i+N=\{h_i+n\}_{n\in N},\mathbf{1}$ 为 16 维全 1 向量(因为 NZ_i 的 5 个行向量是线性独立的,所以 FH 中的 64 个向量是互不相同的).

第 3 步:从 N 中任选 5 行构成 NZ_i',5 行在 N 中的行号构成矩阵 M.

第 4 步:检查 M 是否可逆:若 M 不可逆,转至第 2 步;若 M 可逆,且相应的 NZ_i'作为列向量集合与 NZ_i 相同,转至第 5 步.

第 5 步:求 NZ_i'的符号向量 h_i'.

第 6 步:检查 $h_i'+h_i$ 是否属于 FH:若 $h_i'+h_i\in FH$,计数器加 1;若 $h_i'+h_i\notin FH$,转至第 3 步.

重复第 3~6 步,直至第 3 步达到循环条件,输出计数器值.

结束.

我们输入与上相同的 $NZ_i,h_i,i=1,2$,可以得到$|\rho_1|=384$,$|\rho_2|=120$,由定理 3,有

$$|G_1|=\frac{|\mu_1|}{|\rho_1|}\times64=\frac{1248\times120}{384}\times64=24960,\ |G_2|=\frac{|\mu_2|}{|\rho_2|}\times64=\frac{1512\times120}{120}\times64=96768,$$

$$|G|=|G_1|+|G_2|=24960+96768=121728.$$

我们得到了所有(5,1,3,12)函数的总数.

在运行关于$|\mu_i|$的程序时,我们还可以得到(5,1,3,12)函数所有可能对应的 NZ 集合,稍做统计可以得到下面的结果:在不考虑 NZ 集行间置换的情况下,在等价类(1)中,有 5 种不同的 NZ 集;在等价类(2)中,有 44 种不同的 NZ 集.

有了这样的结果,我们就可以改进文献[11]中(7,2,4,56)函数的构造:在上述 49 种不同的 NZ 集中任取两种,各寻找与之对应的一对符号向量,使之满足文献[11]中命题 7 的条件,即可得到一个(7,2,4,56)函数.这一方法不适宜推广到(9,3,5,240)函数的构造.由此方法,要构造一个(9,3,5,240)函数,我们需要(7,2,4,56)函数对应的 2 个不同的 NZ 集,以及相应于每一个 NZ 的一对符号向量,它们满足类似于文献[11]命题 7 中条件的条件,其中一个条件是 2 个不同 NZ 集中所含有的重为 3 的向量必须不同,这等价于寻找(5,1,3,12)函数对应的 4 个不同 NZ 集,以及相应于每一 NZ 集的 4 个符号向量,它们满足类似于文献[11]命题 7 中条件的条件,其中一条要求 4 个不同 NZ 集含有的重为 2 的向量必须不同.而 49 种不同的 NZ 集中,每一种所含有重为 2 的向量的个数至少为 3,重为 2 的 5 元向量总共只有 10 个,这就意味着不可能找到满足要求的 4 个不同的 NZ 集.

References:

[1] Berlekamp R, Welch LR. Weight distributions of the cosets of the (32,6) Reed-Muller code. IEEE, 1972,IT-18(1):203−207.

[2] MacWillams FJ, Sloane NJA. The Theory of Error Correcting Codes. North Holland, 1977.

[3] Pasalic E, Johansson T, Maitra S, Sarkar P. New constructions of resilient and correlation immune Boolean functions achieving upper bounds on nonlinearity. In: Workshop on Coding and Cryptography 2001. 2001. 425−434.

[4] Sarkar P. Spectral domain analysis of correlation immune and resilient Boolean functions. Finite Fields and Their Applications, 2002,8(1):120−130.

[5] Sarkar P, Maitra S. Nonlinearity bounds and construction of resilient Boolean function. Advances in Cryptology- CRYPTO 2000, Lecture Notes in Computer Science 1880, Springer-Verlag, 2000. 515−532.

[6] Seberry J, Zhang XM, Zheng YL. On constructions and nonlinearity of correlation immune functions. In: Advances in Cryptology-EUROCRYPT'93. Springer-Verlag, 1994. 181−199.

[7] Seberry J, Zhang XM, Zheng YL. Nonlinearity and propagation characteristics of balanced Boolean functions. In: Advances in Cryptology-CRYPTO'93. Springer-Verlag, 1994. 49−60.

[8] Siegenthaler T. Correlation-Immunity of nonlinear combining functions for cryptographic applications. IEEE Trans. on Information Theory, 1984,IT-30:776−780.

[9] Tarannikov YV. On resilient Boolean functions with maximum possible nonlinearity. IndoCrypt2000, LNCS 1977, Springer-Verlag, 2000. 19−30.

[10] Xiao GZ, Massey J. A spectral characterization of correlation-immune combining functions. IEEE Trans. on Information Theory, 1988,34:569−571.

[11] Pei DY, Xie M. A property of the best Boolean functions. Journal of Systems Science and Mathematical Sciences, 2004,24(4): 479−487 (in Chinese with English abstract).

附中文参考文献:

[11] 裴定一,谢敏.最优布尔函数的一个性质.系统科学与数学,2004,24(4):479−487.