严格平衡雪崩布尔函数的研究*

陈 勤**

(杭州电子工业学院计算机科学与技术系 杭州 310037)

【摘要】 通过对三维严格平衡雪崩布尔函数的实验和分析，给出了一种布尔函数从低维向高维扩张的方法，得到了一些有价值的结果，并提出了高维严格平衡雪崩布尔函数的一种生成方法.

关 键 词 布尔函数； 平衡性； 严格雪崩； 生成树； 扩张

中图分类号 TP309

从$Z_2^n \sim Z_2$的n维布尔函数$f(x_1, x_2, \cdots, x_n)$广泛应用于流密码及分组密码中，这些函数是密码体系中的一个重要组成部分。在理论和实际的研究中都指出了函数f应满足一些设计准则[1]，其中主要准则是平衡性、严格雪崩和高非线性度。

平衡性 指f的输出中有一半为1、一半为0。令

$$A=\{(x_1,x_2,\cdots,x_n)\mid f(x_1,x_2,\cdots,x_n)=1,(x_1,x_2,\cdots,x_n)\in Z_2^n\}$$

$$B=\{(x_1,x_2,\cdots,x_n)\mid f(x_1,x_2,\cdots,x_n)=0,(x_1,x_2,\cdots,x_n)\in Z_2^n\}$$

若集合A与B中元素个数相等，则称f是平衡的。

严格雪崩 指f的任意一个输入变量取补，f的输出中有一半改变。令

$$B_j=\{(x_1,x_2,\cdots,\overline{x_j},\cdots,x_n)\mid f(x_1,x_2,\cdots,\overline{x_j},\cdots,x_n)=0,(x_1,x_2,\cdots,\overline{x_j},\cdots,x_n)\in Z_2^n\}$$

$$A_j=\{(x_1,x_2,\cdots,x_j,\cdots,x_n)\mid f(x_1,x_2,\cdots,x_j,\cdots,x_n)=1,(x_1,x_2,\cdots,x_j,\cdots,x_n)\in Z_2^n\}$$

当$1\leqslant j\leqslant n$时集合A_j与B_j中元素个数均相等，则称f满足严格雪崩。

非线性度 指f与所有$Z_2^n\to Z_2$仿射函数的距离的最小值。令$N_f=\min\{d(f,y_i)\}$，其中y_i为$Z_2^n\to Z_2$的仿射函数，$d(f,y_i)=\sum(f\oplus y_i)$，则称$N_f$为$f$的拓扑非线性度。

本文研究了严格平衡雪崩布尔函数的生成及相关性质。

1 三维严格平衡雪崩布尔函数的生成

记X_1=(0,0,0)，X_2=(0,0,1)，X_3=(0,1,0)，X_4=(0,1,1)，X_5=(1,0,0)，X_6=(1,0,1)，X_7=(1,1,0)，X_8=(1,1,1)。

设三维布尔函数$y=f(X)=f(x_1,x_2,x_3)$是平衡的，令

$$y_i=f(X_i)=f(x_1,x_2,x_3)\qquad 1\leqslant i\leqslant 8\qquad y_i、x_1、x_2、x_3\in Z_2$$

根据平衡性定义，$\sum y_i=4$。在$y=f(X)$满足平衡性的前提下，要使其满足严格雪崩，则定义以下三组数对

$$(y_1,y_2)\quad(y_3,y_4)\quad(y_5,y_6)\quad(y_7,y_8)$$
$$(y_1,y_3)\quad(y_2,y_4)\quad(y_5,y_7)\quad(y_6,y_8)$$
$$(y_1,y_5)\quad(y_2,y_6)\quad(y_3,y_7)\quad(y_4,y_8)$$

每组4个元素对中，必须含有2对(0,0)或(1,1)，也含有2对(0,1)或(1,0)。

不同的三变元布尔函数有2^{2^3}个，不同的n变元布尔函数有2^{2^n}个。在2^{2^n}个不同的n变元布尔函数中，采用完全搜索的方法来寻找严格平衡雪崩布尔函数，其搜索量为2^{2^n}。在平衡约束下，严格雪崩三变元布尔函数的搜索量为$C(2^3,2^2)$，n变元时搜索量为$C(2^n,2^{n-1})$。由此可见，若不利用某

2000年5月6日收稿
* 国防科技重点实验室基金资助项目
** 男 38岁 硕士 副教授

些特殊的性质，要寻找严格平衡雪崩布尔函数难度很大。因此，有必要对低维严格平衡雪崩布尔函数的性质进行研究。为此，本文采用平衡约束方法，搜索出所有三变元严格平衡雪崩布尔函数，共计32个，如表1所示。

表1　三变元严格平衡雪崩布尔函数

x_1	x_2	x_3	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{15}	f_{16}
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	1	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0	1	0	0	0	0	1	1	1	1	1	0	0	0	0	0	1	1	1
0	1	1	1	1	1	0	0	0	1	1	0	0	0	1	1	1	1	1
1	0	0	0	1	1	0	1	1	0	1	0	1	1	0	1	0	0	0
1	0	1	1	0	1	1	0	1	1	0	1	1	1	0	1	0	0	1
1	1	0	1	1	0	1	1	1	0	1	1	0	1	1	0	0	1	0
1	1	1	1	1	1	1	1	0	1	0	1	1	0	1	0	1	0	0

x_1	x_2	x_3	f_{17}	f_{18}	f_{19}	f_{20}	f_{21}	f_{22}	f_{23}	f_{24}	f_{25}	f_{26}	f_{27}	f_{28}	f_{29}	f_{30}	f_{31}	f_{32}
0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
0	0	1	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0	1	0	0	0	0	1	1	1	1	1	0	0	0	0	0	1	1	1
0	1	1	0	0	0	0	0	1	1	1	0	0	1	1	1	0	0	0
1	0	0	1	1	1	0	1	0	0	1	0	1	0	0	1	0	0	1
1	0	1	0	1	1	0	1	0	0	0	1	0	0	1	0	0	1	0
1	1	0	1	0	1	1	0	0	1	0	0	1	0	0	0	1	0	0
1	1	1	1	1	0	1	0	1	0	0	1	0	1	0	0	0	0	0

从表1可见 f_i 与 $f_{32-i+1}(1\leqslant i\leqslant 16)$ 具有输出对称性，即 f_i 与 $f_{32-i+1}(1\leqslant i\leqslant 16)$ 之间具有输入不变、输出取反的对称关系，f_2 可由 f_1 中 X_5 与 X_6 的输出换位得到，f_3 可由 f_2 中 X_6 与 X_7 的输出换位得到。

若不考虑对称部分，即仅考虑 $f_1, f_2,\cdots, f_{16}$，三变元严格平衡雪崩布尔函数可由其中某个 f，通过输出换位生成所有三变元严格平衡雪崩布尔函数。f_1 作为生元时，生成树如图1所示。

一般地，在找到某个 n 变元严格平衡雪崩布尔函数 f_1 的前提下，因为输出值中总是含 2^{n-1} 个1，因此理论上总可在严格雪崩约束下经过有限次输出换位，得到所有 n 变元严格平衡雪崩布尔函数。因此，问题的关键是如何由低维通过某种方式扩张成某个高维的 n 变元严格平衡雪崩布尔函数。

2　严格平衡雪崩布尔函数的扩张

定义　n 变元布尔函数 f、g 记为

$$f=(f_1, f_2,\cdots, f_{2^n}) \qquad f_i\leftrightarrow(x_1,x_2,\cdots,x_n)\in Z_2^n$$

$$g=(g_1, g_2,\cdots, g_{2^n}) \qquad g_i\leftrightarrow(x_1,x_2,\cdots,x_n)\in Z_2^n$$

则 f 与 g 的扩张 $f\ \ g$ 记为 $h=(h_1,h_2,\cdots,h_{2^{n+1}})$，满足

$$h=(f_1, f_2,\cdots, f_{2^n}, g_1, g_2,\cdots, g_{2^n})$$

$$f_i\leftrightarrow(0,x_1,x_2,\cdots,x_n)=(x_1^*,x_2^*,\cdots,x_{n+1}^*)\in Z_2^{n+1} \qquad i=1,2,\cdots,2^n$$

$$g_i\leftrightarrow(1,x_1,x_2,\cdots,x_n)=(x_1^*,x_2^*,\cdots,x_{n+1}^*)\in Z_2^{n+1} \qquad i=1,2,\cdots,2^n$$

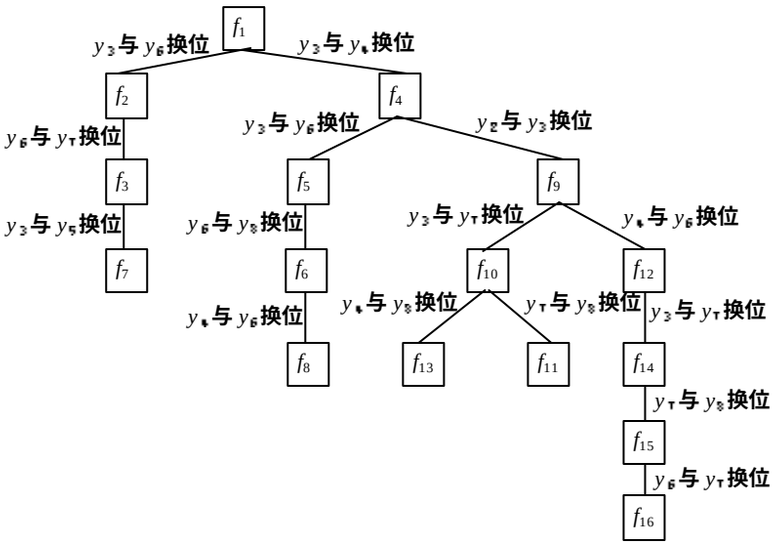

图 1　三变元严格平衡雪崩布尔函数的生成树

定理 1　若 f、g 均为 n 维平衡布尔函数，则 $f\ \ g$ 为 n+1维平衡布尔函数。

证明　因为 f、g 均为 n 维平衡布尔函数，所以 $\sum_{i=1}^{2^n} f_i = 2^{n-1}$, $\sum_{i=1}^{2^n} f_i = 2^{n-1}$。根据扩张定义，$\sum_{i=1}^{2^{n+1}} h_i = \sum_{i=1}^{2^n} f_i + \sum_{i=1}^{2^n} g_i = 2^{n-1} + 2^{n-1} = 2^n$，$f$ 与 g 的扩张 $f\ \ g$ 为 n+1维平衡布尔函数。

定理 2　若 f、g 均为 n 维严格平衡雪崩布尔函数，且 f 与 g 真值表中输出元组成的向量 $\boldsymbol{f}$、$\boldsymbol{g}$ 之间的 Hamming 距离 $d(\boldsymbol{f},\boldsymbol{g}) = 2^{n-1}$[2]，则 f 与 g 的扩张 $f\ \ g$ 为 n+1维严格平衡雪崩布尔函数。

证明　由定理1可知 $f\ \ g$ 为 n+1维平衡布尔函数。因 f、g 严格雪崩，则

$$\sum (f(x_1,x_2,\cdots,x_j,\cdots,x_n) \oplus f(x_1,x_2,\cdots,\overline{x_j},\cdots,x_n)) = 2^{n-2} \qquad 1 \leqslant j \leqslant n$$

$$\sum (g(x_1,x_2,\cdots,x_j,\cdots,x_n) \oplus g(x_1,x_2,\cdots,\overline{x_j},\cdots,x_n)) = 2^{n-2} \qquad 1 \leqslant j \leqslant n$$

因此，当$2 \leqslant j \leqslant n$+1时

$$\sum (h(x_1^*,x_2^*,\cdots,x_j^*,\cdots,x_{n+1}^*) \oplus h(x_1^*,x_2^*,\cdots,\overline{x_j^*},\cdots,x_{n+1}^*)) =$$

$$\sum (f(x_1,x_2,\cdots,x_j,\cdots,x_n) \oplus f(x_1,x_2,\cdots,\overline{x_j},\cdots,x_n)) +$$

$$\sum (g(x_1,x_2,\cdots,x_j,\cdots,x_n) \oplus g(x_1,x_2,\cdots,\overline{x_j},\cdots,x_n)) = 2^{n-2} + 2^{n-2} = 2^{n-1}$$

又因 f 与 g 真值表中输出元组成的向量 $\boldsymbol{f}$、$\boldsymbol{g}$ 之间的 Hamming 距离 $d(\boldsymbol{f},\boldsymbol{g}) = 2^{n-1}$，所以

$$\sum (h(0,x_2^*,\cdots,x_j^*,\cdots,x_{n+1}^*) \oplus h(1,x_2^*,\cdots,x_j^*,\cdots,x_{n+1}^*)) = 2^{n-1}$$

因此 f 与 g 的扩张 $f\ \ g$ 为 n+1维严格雪崩布尔函数。

由此可见，通过低维向高维逐步扩张，然后再通过生成树的方法可以找到大量高维严格平衡雪崩布尔函数。在此基础上，结合其他设计要求(如高非线性度等)，可以从中选择满足各项设计准则的布尔函数。

3　结 束 语

本文通过对三维严格平衡雪崩布尔函数的实验和分析，得到了一些有价值的结果，并提出了寻找高维严格平衡雪崩布尔函数的一种生成方法。有关布尔函数非线性度的性质及其检测方法将另文阐述。

(下转第32页)

作进一步的改进，预测精度越高，则关联效果越好。本文同时解决了数据关联问题，再利用非线性估计方法即可实现多机动目标跟踪问题。

参 考 文 献

1 敬忠良. 神经网络跟踪理论及应用. 北京：国防工业出版社，1995

2 Kohonen T. The self-organizing map. Proceedings of the IEEE, 1990,(78):1 464~1 480

3 Shams S. Multiple elastic modules for visual pattern recognition. Neural Network, 1995,(8):1 439~1 456

Research on Fuzzy Neural Network for Data Fusion of Radar Net

Zhang Bing Qiu Zhiqiang

(Dept. of Electronics and Information, East China Shipbuilding Institute Jiangsu Zhenjiang 212003)

Abstract Based on the basic principle of data fusion, a fuzzy neural network model for data fusion of radar net is presented. The WTA competition for maximizing the fussy membership function in neuron′s receptive field and the problem of the repeated fusion about target data are analyzed. Simulation of data conjunction for three targets demonstrates the validity of the method.

Key words radar net; data fusion; data conjunction; fuzzy neural network

---

(上接第28页)

参 考 文 献

1 张文政. 布尔函数若干设计准则的研究. 通信保密，1994, (2):68~84

2 肖国镇，卿斯汉. 编码理论. 北京：科学出版社, 1993

Research on Boolean Functions of Balance and Strict Avalanche

Chen Qin

(Department of Computer Science and Technology，Hangzhou Institute of Electronic Engineering Hangzhou 310037)

Abstract Three variable Boolean functions with balance and strict avalanche are tested and analyzed, and an expansion method of Boolean functions from single-variable to multi-variable is given. Some valuable results are obtained. Finally, a generation method of constructing multi-variable Boolean functions with balance and strict avalanche is suggested.

Key words Boolean function； balance； strict avalanche； generation tree； expansion