基于固定极 Reed-Muller 展开式的 3 阶可逆逻辑函数 NP-NP 等价判定

罗庆斌[1] 杨国武[2] 邵院华[2] 樊富有[2]
(电子科技大学数学科学学院 成都 611731)[1] (电子科技大学计算机科学与工程学院 成都 611731)[2]

摘 要 在可逆逻辑函数综合中,分类可以使模块重复使用。把布尔函数 NP-N 等价的概念推广到可逆逻辑函数中,得到了可逆逻辑函数 NP-NP 等价的概念;把最小项数为 4 的 3 元布尔函数根据辅因子的码值向量分成 5 类,并计算出了这 5 类布尔函数的固定极 Reed-Muller(FPRM)展开式;把可逆逻辑函数的辅因子码值向量排序后是否相同作为可逆逻辑函数是否 NP-NP 等价的初步判定,当它们相同时,两个可逆逻辑函数 NP-NP 等价当且仅当它们的各个对应的输出分量有相同的变量映射,否则它们不是 NP-NP 等价的。运用这个方法可以判定任意的两个 3 阶可逆逻辑函数是否 NP-NP 等价。

关键词 量子电路综合,FPRM 展开式,可逆逻辑函数,NP-NP 等价,等价判定
中图法分类号 TP387 **文献标识码** A

Judgment of NP-NP Equivalence for 3-bit Reversible Logic Functions via Fixed Polarity Reed-muller Forms

LUO Qing-bin[1] YANG Guo-wu[2] SHAO Yuan-hua[2] FAN Fu-you[2]
(School of Mathematical Sciences, University of Electronic Science and Technology of China, Chengdu 611731, China)[1]
(School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China)[2]

Abstract In reversible logic synthesis, the templates can be used repeatedly through classification. Extending the definition of NP-N equivalence for Boolean functions to the reversible logic functions, the definition of NP-NP equivalence for reversible logic functions can be given. Divide all 3-varible Boolean functions in which everyone of them has exactly four minterms into five classes by their cofactor weight vectors, and calculate the fixed polarity Reed-Muller Form of each class. By comparing the sorted cofactor weight vectors, whether the reversible logic functions are NP-NP equivalent can be judged preliminarily. When the sorted cofactor weight vectors are identical, the reversible logic functions should be judged as NP-NP equivalence if and only if their every corresponding output which is Boolean function has the same variable mappings. Otherwise, the reversible logic functions are not NP-NP equivalent. Thus, whether two 3-bit reversible logic functions are NP-NP equivalent can be judged by this method.

Keywords Synthesis of quantum circuit, Fixed polarity reed-muller form, Reversible logic function, NP-NP equivalence, Equivalence judgment

1 引言

Landauer 准则[1]告诉我们,在不可逆逻辑计算中,每有一单位信息的丢失,将会产生 KTln2 焦耳的热量。1973 年,Bennett[2]证明了用可逆逻辑门构造的电路不会有能量的耗散。因此可逆逻辑综合成为近 40 年来研究的热点,也取得了许多成果:D. Maslov[3]提出先用真值表构造可逆逻辑电路,再用模板技术优化;K. Fazel[4]提出了基于积和范式的综合方法;Gupta[5]给出了基于 Reed-Muller 的启发式规则;Song 等人[6]给出了可逆逻辑门的代数特征;Shende[7]将可逆逻辑电路综合简化为置换问题,并提出了性能较好的递归算法;Yang[8]在此基础上将可逆逻辑电路综合进一步抽象为群论问题,算法性能远远超过其他算法。但这些算法最多只能完全综合 3 阶的可逆逻辑函数,对于更高阶的可逆逻辑函数就会出现各种困难。于是 J. E. Rice[9]提出通过分类的方式来综合可逆逻辑函数,D. Maslov[3]指出在用模板技术综合可逆逻辑函数时,分类可以减少模板的数量,并找出所需的类,M. Perkowki 等在文献[14]中提出了可逆逻辑函数的"NP-N 等价类"。

本文主要研究 3 阶可逆逻辑函数的 NP-NP 等价判定问题。先计算出可逆逻辑函数辅因子码值向量,并把码值向量排序后是否相同作为可逆逻辑函数是否 NP-NP 等价的初步判定,当排序后的辅因子的码值向量相同时,再建立各个输出分量之间的对应关系,然后找出各个输出分量 NP-N 等价时的变量映射集合,通过判断这些集合的交集是否为空来判断给定的可逆逻辑函数是否 NP-NP 等价。

到稿日期:2012-12-09 返修日期:2013-03-12 本文受国家自然科学基金项目(61272175),高等学校博士学科点专项科研基金(20090185110006),四川省教育厅重点项目(2011ZA173)资助。
罗庆斌(1987—),男,硕士生,CCF 学生会员,主要研究方向为量子计算、可逆逻辑综合,E-mail:qingbinluo@126.com。

本文第2节对FPRM展开式和可逆逻辑函数的相关知识作一简单的介绍；第3节引进由布尔函数的积和范式得到FPRM展开式的算法；第4节提出判定3阶可逆逻辑函数是否NP-NP等价的具体方法；最后对全文做一个简单的总结。

2 基本定义和相关结论

在这一部分里，我们将引进FPRM展开式和可逆逻辑函数相关的定义和结论。

在含有n个变量的完全布尔函数$f(x_1,x_2,\cdots,x_n)$(简写为f)中，$\hat{x}_{i_1}\hat{x}_{i_2}\cdots\hat{x}_{i_j}$为$f$的一个积项($1\leqslant j\leqslant n$)，其中$\hat{x}_{i_k}$($1\leqslant k\leqslant n$)既可以是$x_{i_k}$，也可以是$\bar{x}_{i_k}$，称为变量$x_{i_k}$的文字。

定义1[10,12](积和范式) 当n元布尔函数f中的某个积项$\hat{x}_{i_1}\hat{x}_{i_2}\cdots\hat{x}_{i_n}$使$f=1$时，称该积项为$f$的一个最小项，且记$m_j=\prod_{k=1}^{n}\hat{x}_{i_k}=\hat{x}_{i_1}\hat{x}_{i_2}\cdots\hat{x}_{i_n}$为$f$的第$j$个最小项。$f$中各最小项之并称为$f$的积和范式。

在布尔函数f中，若存在l个最小项，那么可将$|f|$记为f中最小项的数目，且令$|f|=l$。f中的x_i均以1代替后，所得到的布尔表达式记为f_{x_i}，称为f关于x_i的辅因子；相反地，f中的x_i均以0代替后，所得到的布尔表达式记为$f_{\bar{x}_i}$，称为f关于$\bar{x}_i$的辅因子。若$|f_{x_i}|=|f_{\bar{x}_i}|$，则称布尔函数$f$关于变量$x_i$是平衡的。

对布尔函数$f(x_1,x_2,\cdots,x_n)$做一系列的Davio展开，便可得到FPRM展开式。于是，我们首先引入：

正Davio展式(pD)：$f(x_1,x_2,\cdots,x_n)=f_{\bar{x}_i}\oplus x_i f^B_{x_i}$；

负Davio展式(nD)：$f(x_1,x_2,\cdots,x_n)=f_{x_i}\oplus\bar{x}_i f^B_{x_i}$，其中$f^B_{x_i}=f_{x_i}\oplus f_{\bar{x}_i}$。

若对布尔函数$f(x_1,x_2,\cdots,x_n)$关于文字$\hat{x}_i$做pD展开，得到的展开式中将不会有$\bar{x}_i$(极性为1)；若做nD展开，得到的展开式中将不会有x_i(极性为0)。

定义2[12](FPRM展开式) 若对布尔函数$f(x_1,x_2,\cdots,x_n)$分别关于文字$\hat{x}_1,\hat{x}_2,\cdots,\hat{x}_n$做Davio展开，得到的式子称为$f$的FPRM展开式，它有下面的形式：

$$f=a_0\oplus a_1\hat{x}_1\oplus a_2\hat{x}_2\oplus\cdots\oplus a_n\hat{x}_n\oplus a_{n+1}\hat{x}_1\hat{x}_2\oplus\cdots\oplus a_{2^n-1}\hat{x}_1\hat{x}_2\cdots\hat{x}_n$$

其中，$a_i\in\{0,1\}$($1\leqslant i\leqslant 2^n-1$)为二进制系数。

例1 3元布尔函数$f=\sum(3,4,6,7)$按极(0,1,0)展开的RM展开式为$f=x_2\oplus\bar{x}_3\oplus\bar{x}_1\bar{x}_3\oplus x_2\bar{x}_3$。

定义3[6](可逆逻辑函数) 令$B=\{0,1\}$，一个有ω个输入变元$A_1,A_2,\cdots,A_\omega$、ω个输出变量的布尔逻辑函数$F:B^\omega\to B^\omega$是可逆的，当且仅当F是一个一一映射，其中，$(A_1,A_2,\cdots,A_\omega)\in B^\omega$是输入向量，$(B_1,B_2,\cdots,B_\omega)\in B^\omega$是输出向量。

事实上，ω阶的可逆逻辑函数就是对2^ω个ω维的二值(0和1)输入向量的置换。后面为了我们叙述的方便，并不把可逆逻辑函数写成置换的形式，而是写成各个输出分量的积和范式的形式。

由文献[10]可知，两个布尔函数NP-N等价是指，对其中的一个函数做变量否定、变量交换或者函数否定操作，可以使这两个函数相等。类似地，我们也可以定义可逆逻辑函数的NP-NP等价。

定义4(可逆逻辑函数NP-NP等价) 对于两个可逆逻辑函数$F(f_1(x_1,x_2,\cdots,x_\omega),f_2(x_1,x_2,\cdots,x_\omega),\cdots,f_\omega(x_1,x_2,\cdots,x_\omega))$和$G(g_1(x_1,x_2,\cdots,x_\omega),g_2(x_1,x_2,\cdots,x_\omega),\cdots,g_\omega(x_1,x_2,\cdots,x_\omega))$，若对$F$(或$G$)做以下一项或多项操作得到$F'$(或$G'$)，使得$F'=G$(或$F=G'$)，则称$F$和$G$是NP-NP等价的：①否定输入变元；②交换输入变元；③否定输出分量；④交换输出分量。

此定义是布尔函数NP-N等价的推广，这种推广是合理的：对于两个布尔函数，对其中一个做①②③中的某些变换，使得这两个布尔函数相等，这是布尔函数NP-N等价的定义。ω阶可逆逻辑函数可以看成是由ω个布尔函数(输出分量)构成的，变换①②③可以很自然地引入；又因为每个ω阶可逆逻辑函数都有ω个输出分量，让可逆逻辑函数F中的输出分量$f_i(1\leqslant i\leqslant\omega)$在变换①②③下和可逆逻辑函数$G$的输出分量$g_j(1\leqslant j\leqslant\omega)$相等是可行的，所以变换④也是合理的。

3 FPRM展开式

在这一部分里，将给出FPRM展开式的相关结论。

3.1 J. E. Savage算法

为了求得布尔函数$f(x_1,x_2,\cdots,x_n)$的某固定极RM展开式，若对$f(x_1,x_2,\cdots,x_n)$中的每个变元依次做Davio展开，这显然比较麻烦。文献[13]给出了由布尔函数的积和范式构造FPRM展开式的J. E. Savage算法。我们这里略微做了一些改进：

1)写出f的积和范式；

2)将积和范式中的“∪”换成“⊕”；

3)若f中文字$\hat{x}_i$的极性是1，则将积和范式中所有的$\bar{x}_i$换成$1\oplus x_i$，若$\hat{x}_i$的极性是0，则将积和范式中所有的x_i换成$1\oplus\bar{x}_i$；

4)运用“·”对“⊕”进行分配律展开；

5)合并同类项得到f的RM展开式。

在例1中，我们运用这个算法可以得到相同的结果。

3.2 布尔函数固定极RM展开式极性的确定[10]

f中所有不平衡变量x_i，其极性可以唯一确定：当$|f_{x_i}|>|f_{\bar{x}_i}|$时，$x_i$的极性为1；当$|f_{x_i}|<|f_{\bar{x}_i}|$时，$x_i$的极性为0。当$f$中所有不平衡变量$x_i$的极性确定后，将$f$按照这些变量的极性展开(原来$f$中的平衡变量不动)，得到一个新的展开式$f'$，在这个新的展开式中，找出在原$f$中平衡的，在$f'$中部不平衡的变量，再由上面的方法确定其极性，继续展开，直到所有的变量的极性确定为止。如果在确定f各变量的极性过程中，某些变量始终是平衡的，则其极性无法确定，这时函数须分别按该变元的0,1极性展开。

例2 对4元布尔函数$f(x_1,x_2,x_3,x_4)=\sum(0,2,5,6,7,9,13,14)$，确定其FPRM展式的极性。

解：在f中，$|f_{\bar{x}_1}|=5>|f_{x_1}|=3$，$|f_{x_2}|=5>|f_{\bar{x}_2}|=3$，所以$x_1$的极性为0，$x_2$的极性为1，$|f_{x_3}|=|f_{\bar{x}_3}|=4$，$|f_{x_4}|=|f_{\bar{x}_4}|=4$，$x_3,x_4$的极性不确定。将$f$按照$x_1,x_2$的极性展开有：

$$f=f'=\bar{x}_1(\bar{x}_3\bar{x}_4\oplus\bar{x}_3x_4\oplus x_3\bar{x}_4)\oplus\bar{x}_1x_2(\bar{x}_3\bar{x}_4\oplus\bar{x}_3x_4\oplus x_3\bar{x}_4\oplus x_3x_4)\oplus\bar{x}_3x_4\oplus x_2x_3\bar{x}_4$$

式中，$|f_{\bar{x}_3}'|=5>|f_{x_3}'|=3$，$|f_{\bar{x}_4}'|=5>|f_{x_4}'|=3$，所以，

x_3, x_4 的极性均为 0。于是函数 f 的极性 $v=(0,1,0,0)$，再将 f 按极性 v 展开，得其 FPRM 展开式为：

$$f_v=\bar{x}_1\bar{x}_3\bar{x}_4 \oplus \bar{x}_1\bar{x}_3 \oplus \bar{x}_1\bar{x}_4 \oplus \bar{x}_1 x_2 \oplus \bar{x}_3\bar{x}_4 \oplus \bar{x}_3 \oplus x_2\bar{x}_3\bar{x}_4 \oplus x_2\bar{x}_4$$

对于给定的布尔函数，当它的极性唯一确定后，其 FPRM 展开式也就唯一确定了。下面这个引理，给出了两个布尔函数 NP 等价与 FPRM 展开式之间的关系。

引理 1[10] 假设布尔函数 $f(x_1,x_2,\cdots,x_n)$ 和 $g(y_1,y_2,\cdots,y_n)$ 变元的极性由极性确定规则确定，那么 f 和 g NP 等价，当且仅当它们的 FPRM 展开式 NP 等价。

推论 假设布尔函数 $f(x_1,x_2,\cdots,x_n)$ 和 $g(y_1,y_2,\cdots,y_n)$ 变元的极性由极性确定规则确定，那么 f 和 g NP-N 等价，当且仅当它们的 FPRM 展开式 NP-N 等价。

所以，当要判定两个可逆逻辑函数是否 NP 等价或者 NP-N 等价时，只需判定它们的 RM 展开式是否 NP 等价或者 NP-N 等价即可。

4 可逆逻辑函数 NP-NP 等价的判定

4.1 辅因子的码值向量

我们知道两个布尔函数 f 和 g NP-N 等价的必要条件是它们的最小项数相等，即：$|f|=|g|$，而当 $|f|=|g|$ 时，f 中的变元 x_i 与 g 中的变元 y_j 相对应的必要条件是 $\max\{|f_{x_i}|,|f_{\bar{x}_i}|\}=\max\{|g_{y_j}|,|g_{\bar{y}_j}|\}$。为了后面我们叙述的方便，在布尔函数 f 中，把 $\max\{|f_{x_1}|,|f_{\bar{x}_1}|\}$，$\max\{|f_{x_2}|,|f_{\bar{x}_2}|\}$，$\cdots$，$\max\{|f_{x_n}|,|f_{\bar{x}_n}|\}$ 按从大到小的顺序排列的数组称为 f 的辅因子码值向量，记为 $V_w(f)$。把可逆逻辑函数的每个输出分量的辅因子码值向量按输出分量的顺序排列的二维数组称为可逆逻辑函数的辅因子码值向量。

例 3 布尔函数 $f(x_1,x_2,x_3,x_4)=\sum(0,2,5,6,7,9,13,14)$ 的辅因子码值向量 $V_w(f)=(5,5,4,4)$；可逆逻辑函数 $F=(\sum(3,5,6,7),\sum(2,4,5,7),\sum(1,4,5,6))$ 的辅因子码值向量为 $V_w(F)=[(3,3,3),(3,2,2),(3,3,2)]$。

由于可逆逻辑函数的每个输出分量也是一个布尔函数，且 ω 阶可逆逻辑函数的每个输出分量的最小项数为 $2^{\omega-1}$，因此，在研究 ω 阶的可逆逻辑函数之前，我们可以先研究最小项数为 $2^{\omega-1}$ 的布尔函数的性质。

定理 1 最小项数为 4 的 3 变元布尔函数 $f(x_1,x_2,x_3)$ 只有 5 种不同的辅因子码值向量，它们分别是(4,2,2)，(3,3,3)，(3,3,2)，(3,2,2)和(2,2,2)。

证明：对于最小项数为 4 的布尔函数，单个变量的辅因子码值必须小于或等于 4。当有变元的辅因子码值为 4 时(不妨设 $|f_{x_1}|=4$)，下面我们来证明其余的两个变量都必须是平衡的。若不然，则存在某文字的辅因子码值(不妨设 $|f_{x_2}|$)为 4 或 3，在这两种情况下，不管剩下的变量(假设后，只剩 x_3)怎样取，都会出现重复的最小项，这与布尔函数的最小项数为 4 矛盾。即当某变元的辅因子码值为 4 时，其它两个变元都是平衡的。最后，可以验证，剩下的 4 种辅因子码值向量都是存在的。

根据极性确定规则，码值向量为(3,3,3)，(3,2,2)的布尔函数的极性是唯一的，虽然码值向量为(4,2,2)，(3,3,2)，(2,2,2)的布尔函数的极性不唯一，但是它们的 RM 展开式都可以写成“表 1”的形式。

表 1 最小项数为 4 的 3 元布尔函数辅因子码值向量对应的 FPRM 展开式

码值向量	对应的 FPRM 展开式
(4,2,2)	$\hat{x}_i(i=1,2,3)$
(3,3,3)	$\hat{x}_1\hat{x}_2 \oplus \hat{x}_1\hat{x}_3 \oplus \hat{x}_2\hat{x}_3$
(3,3,2)	$\hat{x}_i \oplus \hat{x}_i\hat{x}_k \oplus \hat{x}_j\hat{x}_k(i,j,k=1,2,3)$
(3,2,2)	$\hat{x}_i \oplus \hat{x}_j\hat{x}_k(i,j,k=1,2,3)$
(2,2,2)	$\hat{x}_i \oplus \hat{x}_j(i,j=1,2,3)$

4.2 3 阶可逆逻辑函数 NP-NP 等价判定

由这 5 个辅因子码值向量所对应函数的 RM 展开式，我们知道对于 3 元最小项数为 4 的布尔函数，辅因子码值向量相同也是两个布尔函数 NP-N 等价的充分条件，而且不只一个变量映射。但这扩展到可逆逻辑函数中就不成立了，因为两个可逆逻辑函数 NP-NP 等价，除了对应的输出分量 NP-N 等价外，还必须要求这 3 对输出分量所做的变量映射是一样的。因此，当两个可逆逻辑函数的辅因子码值向量相同时，是否存在相同的变量映射使具有相同辅因子码值向量的输出分量 NP-N 等价，就成为判定两个可逆逻辑函数是否 NP-NP 等价的关键。基于这一思想，我们提出了判断两个可逆逻辑函数是否 NP-NP 等价的方法。

判断两个 3 阶可逆逻辑函数是否 NP-NP 等价的一般方法：

①分别计算出这两个可逆逻辑函数的二维辅因子码值向量，并将它们排序，若排序后它们的码值向量不同，则这两个可逆逻辑函数不是 NP-NP 等价的，否则转②；

②根据极性确定规则，求出这两个可逆逻辑函数各个输出分量的 RM 展开式，其中一个可逆逻辑函数须求出它的各个输出分量求非后的 RM 展开式，并把它们写成“表 1”中的形式；

③根据输出分量的辅因子码值向量是否相同，建立两可逆逻辑函数 3 个输出分量 RM 展开式之间的一一映射；

④取出③中的一个映射，分别求出它们对应分量 RM 展开式 NP-N 等价下变量映射的集合 S_1,S_2,S_3；

⑤若 $S_1\cap S_2\cap S_3\neq\varnothing$，则这两个可逆逻辑函数 NP-NP 等价，若 $S_1\cap S_2\cap S_3=\varnothing$，取③中剩下的一个输出分量映射重复④，若取完③中的映射，仍然是 $S_1\cap S_2\cap S_3=\varnothing$，则这两个可逆逻辑函数不是 NP-NP 等价的。

下面先对这个算法做一个简单的说明，并用一个例子具体阐述算法的执行过程：显然，两个可逆逻辑函数的辅因子向量相等是它们 NP-NP 等价的必要条件，所以步骤①可以排除部分不等价的情况；在辅因子向量相等时，便可以建立输出分量之间的一一映射，这种映射可能不只一个，因此可能需要逐一考察，而由可逆逻辑函数 NP-NP 等价的定义可知，两个可逆逻辑函数 NP-NP 等价的充要条件是，存在某个一一映射，使得在该映射下对应的输出分量 NP-N 等价，并且它们有相同的变量映射，步骤③④⑤正是运用了该充要条件；而定理 1 是步骤②的理论基础。又因为可逆逻辑函数是 3 阶(有限阶)的，所以算法将终止。

例 4 判断可逆逻辑函数 $F=(\sum(3,5,6,7),\sum(2,4,5,7),\sum(1,4,5,6))$ 和 $G=(\sum(0,1,2,6),\sum(1,2,3,4),\sum(2,4,6,7))$ 是否 NP-NP 等价。

(下转第 256 页)

[4] J Xian, L Pei-yu, G Wei, et al. An algorithm application in intrusion forensics based on improved information gain [C] // 3rd Symposium on Web Society(SWS)2011. 2011

[5] Wang Zi-qiang, Zhang De-xian. Feature Selection in Text Classification Via SVM and LSI[J]. Lecture Notes in Computer Science, 2006, 3971: 1381-1386

[6] Yang Yu-zhen, Liu Pei-yu, Zhu Zhen-fang, et al. The Research of an Improved Information Gain Method Using Distribution Information of Terms[C]// IEEE International Symposium. 2009: 938-941

[7] 崔自峰,徐宝文,张卫峰. 一种近似 Markov Blanket 最优特征选择算法[J]. 计算机学报,2007,30(12):2074-2081

[8] Hu Qing-hua, Yu Da-ren, Xie Zong-xia. Neighborhood classifiers [J]. Expert Systems with Applications, 2008, 34(2): 866-876

[9] 刘海峰,王元元,姚泽清. 文本分类中一种基于选择的二次特征降维方法[J]. 情报学报,2009,28(1):23-27

[10] 徐燕,李锦涛,王斌,等. 基于区分类别能力的高性能特征选择方法 [J]. 软件学报,2008,19(1):82-89

[11] 周城,葛斌,唐九阳,等. 基于相关性和冗余度的联合特征选择方法[J]. 计算机科学,2012,39(4):181-184

[12] 刘庆和,梁正友. 一种基于信息增益的特征优化选择方法[J]. 计算机工程与应用,2011,47(12):130-136

(上接第 220 页)

解:①分别求出两个可逆逻辑函数的二维辅因子码值向量,分别为:$V_w(F)=[(3,3,3),(3,2,2),(3,3,2)]$,$V_w(G)=[(3,3,2),(3,2,2),(3,3,3)]$,排序后有:$V_w(F)=V_w(G)=[(3,3,3),(3,3,2),(3,2,2)]$。

②求出各个输出分量的 RM 展开式有:F 的输出分量为 $f_3=x_1x_2\oplus x_1x_3\oplus x_2x_3$,$f_2=x_1\oplus x_2\bar{x}_3$,$f_1=x_1\oplus x_1x_3\oplus\bar{x}_2x_3$;$G$ 的输出分量为 $g_3=\bar{x}_1\oplus\bar{x}_1x_2\oplus x_2\bar{x}_3=1\oplus x_1\oplus x_1x_2\oplus x_2x_3=\bar{x}_3\oplus\bar{x}_2\bar{x}_3\oplus\bar{x}_1\bar{x}_2=1\oplus x_3\oplus\bar{x}_2x_3\oplus x_1\bar{x}_2$,$g_2=\bar{x}_1\oplus\bar{x}_2\bar{x}_3=1\oplus x_1\oplus\bar{x}_2\bar{x}_3$,$g_1=x_1x_2\oplus x_1\bar{x}_3\oplus x_2\bar{x}_3=1\oplus\bar{x}_1\bar{x}_2\oplus\bar{x}_1x_3\oplus\bar{x}_2x_3$。

③根据可逆逻辑函数输出分量的码值向量,建立输出分量之间的对应关系仅有:$\varphi:(f_3,f_2,f_1)\leftrightarrow(g_1,g_2,g_3)$。

④求对应输出分量 NP-N 等价时,所有变量映射的集合。当 f_3 和 g_1 NP-N 等价时,变量映射的集合 S_1 共有 12 个元素,分别是 (x_1,x_2,x_3) 与 $(x_1,x_2,\bar{x}_3)$ 的所有置换的对应和 (x_1,x_2,x_3) 与 $(\bar{x}_1,\bar{x}_2,x_3)$ 所有置换的对应,当 f_2 与 g_2 NP-N 等价时,变量映射的集合 S_2 为 (x_1,x_2,x_3) 分别与 $(\bar{x}_1,\bar{x}_2,x_3)$,$(\bar{x}_1,\bar{x}_3,x_2)$,$(x_1,\bar{x}_2,x_3)$,$(x_1,\bar{x}_3,x_2)$ 的对应,当 f_1 与 g_3 NP-N 等价时,变量映射的集合 S_3 为 (x_1,x_2,x_3) 分别与 $(\bar{x}_1,x_3,x_2)$,$(x_1,\bar{x}_3,x_2)$,$(x_3,x_1,\bar{x}_2)$,$(x_3,\bar{x}_1,\bar{x}_2)$ 的对应。

⑤于是,可求得:$S_1\cap S_2\cap S_3=\{(x_1,x_2,x_3)\leftrightarrow(x_1,\bar{x}_3,x_2)\}\neq\varnothing$,所以,可逆逻辑函数 F 和 G 是 NP-NP 等价的。

结束语 在可逆逻辑函数的综合中,分类可以使模块重复使用。因此,对可逆逻辑函数分类的研究是必要的,而判断两个可逆逻辑函数是否属于同一类又是研究可逆逻辑函数分类的重要部分。先计算出可逆逻辑函数辅因子码值向量,并把码值向量排序后是否相同作为可逆逻辑函数是否 NP-NP 等价的初步判定,当排序后的辅因子的码值向量相同时,再建立各个输出分量之间的对应关系,然后找出各个输出分量 NP-N 等价时的变量映射集合,通过判断这些集合的交集是否为空来判断给定的可逆逻辑函数是否 NP-NP 等价。我们把 3 阶可逆逻辑函数作为研究对象,并成功解决了 3 阶可逆逻辑函数 NP-NP 等价的判定问题。

参 考 文 献

[1] Landauer R. Irreversibility and Heat Generation in the Computing Process [J]. IBM Journal of Research and Development, 1961(5): 183-191

[2] Bennett C H. Logical reversibility of computation [J]. IBM Journal of Research and Development, 1973, 17(6): 525-532

[3] Maslov D, Dueck G W, Miller D M. Synthesis of Fredkin-Toffoli Reversible Networks [J]. IEEE Transactions on Very Large Scale Integration(VLSI)Systems, 2005, 13(6): 765-769

[4] Fazel K, Thornton M, Rice J E. ESOP-based Toffoli Gate Cascade Generation[C]// IEEE Pacific Rim Conference on Communications, Computers and Signal Processing. Aug. 2007: 206-209

[5] Li W Q, Chen H W, Li Z Q. Application of semi-template in reversible logic circuit [C]// Proceedings of the 11th International Conference on CSCWD. Melbourne, Australia, 2007: 155-161

[6] Song Xiao-yu, Yang Guo-wu, Perkowski M, et al. Algebraic Characterization of Reversible Logic Gates [J]. Theory of Computing Systems, 2006, 39(2): 311-319

[7] Shende V V, Prasad A K, Markov I L, et al. Synthesis of reversible logic circuits [J]. IEEE Trans on Circuits and Systems I, 2003, 22(6): 723-729

[8] Yang G W, Song X Y, Perkowski M, et al. Fast synthesis of exact minimal reversible circuits using group theory [J]. Proceedings of IEEE ASP-DAC, 2005(2): 18-21

[9] Rice J E. Considerations for Determining a Classification Scheme for Reversible Boolean Function [R]. TR-CSJR2-2007

[10] Tsai C C, Marek-Sadowska M. Boolean Functions Classification via Fixed Polarity Reed-Muller Forms [J]. IEEE Trans. Computers, 1997, 46(2): 173-186

[11] Mozammel H A, Khan A. Quantum Logic Circuit For Generating Fixed-Polarity Reed-Muller Coefficients [C]// 4th International Conference on Electrical and Computer Engineering. December 2006: 141-144

[12] Hirayama T, Takahashi M, Nishitani Y. Simplification of Exclusive-or Sum-of-Products Expressions Through Function Transformation [C]// Circuits and Systems, IEEE Asia Pacific Conference. Dec. 2006: 1480-1483

[13] 刘永才,张卫. 布尔方法论 [M]. 上海:上海科学技术文献出版社,1993

[14] Perkowski M, Joziwak L, Mixhchenko A, et al. A General Decomposition for Reversible Logic[C]// Proceedings of the International Workshop on Methods and Representations(RM). August 2001: 119-138