Advances in Applied Mathematics 应用数学进展, 2021, 10(1), 343-350
Published Online January 2021 in Hans. http://www.hanspub.org/journal/aam
https://doi.org/10.12677/aam.2021.101039

Hans汉斯

基于Gröbner基方法的乘法器等价性验证

张璇思，刘佳姝，江建国*

辽宁师范大学数学学院，辽宁 大连
Email: *jjgbox@sina.com

收稿日期：2020年12月25日；录用日期：2021年1月19日；发布日期：2021年1月28日

摘　要

乘法器的等价性验证目前仍是大规模算术集成电路设计领域内的一大难题。本文利用逻辑门与多项式之间的对应关系，构建了乘法器的代数模型，将乘法器等价性验证问题转化成理想成员判定问题，然后再用计算机代数系统中的Gröbner基方法进行求解。提出了一种对乘法器结构进行切片后再采用增量式验证的新方法。在Linux平台上的计算机代数系统Mathematica上所做的实验结果也表明了该方法的有效性。

关键词

Gröbner基，等价性验证，整数乘法器，增量式验证，切片

Equivalence Verification of Multipliers Based on Gröbner Basis Method

Xuansi Zhang, Jiashu Liu, Jianguo Jiang*

School of Mathematics, Liaoning Normal University, Dalian Liaoning
Email: *jjgbox@sina.com

Received: Dec. 25th, 2020; accepted: Jan. 19th, 2021; published: Jan. 28th, 2021

Abstract

The equivalence verification of multipliers is still a difficult problem in the field of LSI design. In this paper, the algebraic model of multipliers is constructed by using the corresponding relationship between logic gates and polynomials. The problem of equivalence verification of multipliers is transformed into the problem of determining ideal members. Then, the problem is solved by the Gröbner basis method in computer algebra system. This paper presents a new method of incremental

*通讯作者。

文章引用: 张璇思, 刘佳姝, 江建国. 基于 Gröbner 基方法的乘法器等价性验证[J]. 应用数学进展, 2021, 10(1): 343-350. DOI: 10.12677/aam.2021.101039

verification after slicing the multiplier structure. The experimental results on Mathematica, a computer algebra system on Linux platform, also show the effectiveness of the method.

Keywords

Gröbner Basis, Equivalence Verification, Integer Multiplier, Incremental Validation, Slicing

1. 引言

随着科学技术的发展，集成电路的结构日益复杂，步入 SoC 时代，在门级抽象层次上已经达到数以百万和千万门系统的设计和验证[1]。为了保证设计的错误能及时发现，杜绝因重新设计和流片浪费开发成本和设计周期，就需要对电路进行正确性的验证。传统的模拟验证因其不完备性，已经不能适用于现时的较高抽象层次上的集成电路的验证，为了避免“20 世纪 60 年代的软件危机”和“著名的奔腾 FDIV 错误”此类情况发生，促使人们去研究更完善的验证方法[2] [3] [4]。

等价性验证是目前在实际的芯片设计中应用最广泛的形式化验证技术，如 Synopsys 公司的 Formality，Mentor Graphics 公司的 FormalProTM，Cadence 公司的 Affirma 等，并且能处理较大规模的设计[5]。等价性验证一般采用图表示法和代数表示方法[6]。图表示法主要使用二叉判定图(BDD)，Brand 利用 BDD 将电路建模为 miter，计算所有可达状态这就是典型的基于有限状态机遍历算法[7]。尽管最近十多年里，由于 BDD 方法的研究进展使得基于有限状态机遍历算法有了很大进步，但 BDD 需要大量储存和操作空间的问题仍无法避免，而且用布尔函数表示的状态集会成指数增长，存在状态空间爆炸问题。并且在抽象层较高的等价性验证中，受图形表示能力和图形构造上的制约，BDD 无法胜任验证任务。相比而言，基于代数方法的等价性验证则更适合高层次验证。

代数学是数学的一个基本分支，它所处理和研究的数学对象是抽象的代数符号与概念，如整数、有理数、多项式、环、理想等[8] [9]。其中多项式由于其描述电路时抽象建模能力强，表示具有规范性、无歧义性，使其成为理想的电路建模工具。Buchberger 在 1915 年提出了多项式环上的 Gröbner 基，因其良序性方面的优势适用于计算机代数领域[10] [11]。本文运用 Gröbner 基与乘法器电路结合的思想，在 Galois 域上采用迭代算法验证整数乘法器电路[11] [12] [13] [14]。通过实验对比不同方法所需运行时间，易见各方法对乘法器等价性验证的效率影响。

2. Gröbner 基理论

对于环 R 中给定的理想 I，其 Gröbner 基一般并不唯一。这些 Gröbner 基与项序的选择密切相关，下面给出相关定义[8] [9] [10]。

定义 2.1 设k为任意一个域，变量序列 $x_1,\cdots,x_n$ 记为 X，将含有 n 个变量的多项式环记为$k[X]$或 $k[x_1,\cdots,x_n]$。

多项式环中最重要的结构为理想，理想为多项式环中的一种子集，其中的元素对加法和乘法封闭。

定义 2.2 多项式集合 I 是环 $k[X]$的子集，如果满足

(1) $0 \in I$，

(2) 如果 $f,g \in I$，则 $f+g \in I$，

(3) 如果 $f \in I, h \in K[X]$，则 $hf \in I$，

上述条件，则称 I 为多项式理想。

对于 Gröbner 基来说，多项式环 $k[x_1,\cdots,x_n]$ 中单项式序的概念是一个基本概念，他可以定义出任意多项式的首项，从而保证多项式除法操作下余式唯一。

定义 2.3 设 $\alpha=(\alpha_1,\cdots,\alpha_n),\beta=(\beta_1,\cdots,\beta_n)\in Z_{\geq 0}^n$，集合 T 上的关系 $\prec$ 称为一个单项式序，如果 $\prec$ 满足下面条件：

(1) $\prec$ 为 T 上的一个全序；

(2) $x^\alpha \prec x^\beta, x^\gamma \in T$，那么，$x^{\alpha+\gamma} \prec x^{\beta+\gamma}$；

(3) $\prec$ 为 T 上的良序，即 T 上每一个非空子集有极小元。

其中 $T=\left\{X^\alpha = x_1^{\alpha_1}x_2^{\alpha_2}\cdots x_n^{\alpha_n} \mid \alpha=(\alpha_1,\alpha_2,\cdots,\alpha_n)\in Z_{\geq 0}^n\right\}$ 是所有单项的集合。

单项式序常见的有三种，字典序，分次字典序，分次逆字典序。

定义 2.4 设 $\alpha=(\alpha_1,\cdots,\alpha_n),\beta=(\beta_1,\cdots,\beta_n)\in Z_{\geq 0}^n$，如果 $\alpha-\beta \in Z^n$ 的最左边非空元素为正数，则称单项式 $x^\alpha \prec_{lex} x^\beta$ 为字典序排序。

定义 2.5 非零多项式 $f \in k[x_1,\cdots,x_n]$ 在给定的单项式序下，可唯一表示为 $f=c_1x^{\alpha_1}+\cdots+c_nx^{\alpha_n}$

则称 $LC(f)=c_1$ 为多项式 f 的首项系数，$Mulidegree(f)=\alpha_1$ 为多项式 f 的次数，$LM(f)=x^{\alpha_1}$ 为多项式 f 的首单项式，$Lt(f)=LC(f)LM(f)=c_1x^{\alpha_1}$ 为多项式 f 的首项。

定义 2.6 在多项式环 $k[x_1,\cdots,x_n]$ 上给定一个单项式序，非零理想 I 的有限子集 $G=\{g_1,\cdots,g_t\}$，如果满足

$$\langle LT(g_1),\cdots,LT(g_t)\rangle = \langle LT(I)\rangle$$

称 G 为理想 I 的 Gröbner 基。

结合多元多项式除法，Gröbner 基理论为理想成员问题提供了一个判定过程：给定一个多项式 $q \in k[X]$ 和理想 $I=\langle G\rangle=\langle g_0,\cdots,g_m\rangle \subseteq k[X]$。通过计算余数是否等于零，则可判定 q 是否为 I 中的元素。

3. 代数模型

Buchberger 算法利用 S-多项式去求多项式的 Gröbner 基，该算法的时间和空间复杂度是指数级的，在实际应用中是不可行的。因此本文直接将电路建模为 Gröbner 基多项式。

考虑一个具有 l 个布尔输入 $a_0,\cdots,a_{l-1}$ 和 m 个输出 $s_0,\cdots,s_{m-1}$ 的电路 C。它的每个内部门由一个门变量 $g_0,\cdots,g_j$ 表示。接下来在相同的布尔输入 $a_0,\cdots,a_{l-1}$ 下，设电路 C'有 m 个不同的输出 $s_0',\cdots,s_{m-1}'$。与电路 C 中每个门(输出)类似，在电路 C'中由门变量 $g_0',\cdots,g_k'$ 表示。

门电路的逻辑门用多项式和信号作为布尔变量建模。其布尔变量之间的多项式关系是

$$\begin{aligned} &u=\neg v \Leftrightarrow -u+1-v=0\\ &u=v\wedge w \Leftrightarrow -u+vw=0\\ &u=v\vee w \Leftrightarrow -u+v+w-vw=0\\ &u=v\oplus w \Leftrightarrow -u+v+w-2vw=0 \end{aligned} \tag{1}$$

每个逻辑门都是以门输入变量来描述门输出变量的方式来建模的。

每个多项式的一般形式是：

$$p_i = \text{首项}(x_i)+\text{尾部}(p_i)$$

其中首项 x_i 是门的输出变量，尾部 p_i 是由门的输入变量组成的术语。根据这个多项式形式，模型的所有

首项都是相对素的。电路是在布尔值范围内操作，因此，对于变量 u，可得到关系式 $u(u-1)=0$。满足等式左侧的多项式编码形式称为域多项式 F。

定义 3.1 设 $G\in k[X]$ 是满足(1)的对应多项式的电路 C 每个门的集合，并且多项式 $a_i(a_i-1)$ 和 $b_i(b_i-1)$ 称为输入域多项式，$0\le i<n$。则 $G\in k[X]$ 中生成的理想用 $J(C)$ 表示。

定义 3.2 设 C 是一个电路。一个多项式 $p\in k[X]$ 被称为电路 C 的多项式电路约束(*PCC*)，如果把 $(a_0,\cdots,a_{n-1},b_0,\cdots,b_{n-1})\in\{0,1\}^{2n}$ 和结果值 $g_0,\cdots,g_k,s_0,\cdots,s_{2n-1}$ 带入多形式 p 得 0。

定义 3.3 电路 C 被称为乘法器，如果满足 $\sum_{i=0}^{2n-1}2^i s_i-\left(\sum_{i=0}^{n-1}2^i a_i\right)\left(\sum_{i=0}^{n-1}2^i b_i\right)$ 是 *PCC*。

本文针对于简单部分积生成的乘法器，其中部分积是指由两个电路输入通过与门产生的输出。为了从 Gröbner 基中消除带有部分积的这些多项式，把定义 3.3 中乘法器的规范改为推论 3.1 中规定的规范。

推论 3.1 电路 C 是乘法器，如果满足 $\sum_{i=0}^{2n-1}2^i s_i-\sum_{i,j=0}^{n-1}p_{i,j}\in J(C)$，其中 $p_{i,j}=a_i b_i$。

通过展开定义 3.3 中的和式，并在推论 3.1 中用 $a_i b_i$ 替代 $p_{i,j}$，很容易地验证推论 3.1 的正确性。

乘法器的结构包括多个全加器及半加器，下面就以简单的全加器为例，给出理想成员问题判定过程：

例 1：实现图 1 所示功能 $s_i+2c_i=a_i+b_i+c_{i-1}$ 的全加器电路。

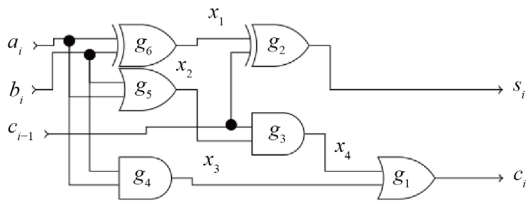

Figure 1. Full-add circuit
图 1. 全加器电路

根据(1)，得图 1 的代数模型是

$$g_1:=-c_i-x_4x_3+x_4x_3,\ g_2:=-s_i-2x_1c_{i-1}+x_1+c_{i-1}$$

$$g_3:=-x_4+x_2c_{i-1},\ \ g_4:=-x_3+a_ib_i,$$

$$g_5:=-x_2-a_ib_i+a_i+b_i,\ \ g_6:=-x_1-2a_ib_i+a_i+b_i$$

其中规范多项式为 $p_{spec}=-2c_i-s_i+c_{i-1}+b_i+a_i$，将多项式变量按电路的逆拓扑顺序 $a_i\prec b_i\prec c_{i-1}\prec x_1\prec x_2\prec x_3\prec x_4\prec s_i\prec c_i$ 排序，在此序下，用规范多项式 p_{spec} 归约代数模型 g_i：

$$p_{spec}\xrightarrow{g_1}-s_i+2x_4x_3-2x_4-2x_3+c_{i-1}+b_i+a_i$$

$$\xrightarrow{g_2}2x_4x_3-2x_4-2x_3+2x_1c_{i-1}-x_1+b_i+a_i$$

$$\xrightarrow{g_3}2x_3x_2c_{i-1}-2x_3-2x_2c_{i-1}+2x_1c_{i-1}-x_1+b_i+a_i$$

$$\xrightarrow{g_4}2x_2c_{i-1}b_ia_i-2x_2c_{i-1}+2x_1c_{i-1}-x_1-2b_ia_i+b_i+a_i$$

$$\xrightarrow{g_5}2x_1c_{i-1}-x_1+4c_{i-1}b_ia_i-2c_{i-1}a_i-2c_{i-1}b_i-2b_ia_i+b_i+a_i$$

$$\xrightarrow{g_6}0$$

通过计算得余数为 0，因此提取的代数模型为 Gröbner 基。为了更好的加快验证效率，下节将介绍 Gröbner 基的约化。

4. 加法器重写

通常情况，关于生成的 Gröbner 基归约规范，会导致中间约化结果中单项式的数量急剧增加，而影响验证效率[9] [15]。因此我们利用加法器重写，以便更有效约化 Gröbner 基[12]。

首先在乘法器的门级表示中识别全加器和半加法器，并将它们视为独立电路。然后应用变量消去，即用相应的加法器规范来代替全加器和半加法器内部门的所有多项式。这会使表示整个乘法器的 Gröbner 基更小、更紧凑，从而加快了归约过程。

定义 4.1 一个电路 C 被称为全加器，如果满足 $-2c-s+a+b+i$ 是 PCC；相应地，一个电路C被称为半加器，如果满足 $-2c-s+a+b$ 是 PCC。其中 c,s 表示输出， a,b,i 表示输入。

例 2 给出简单全加器电路A相应的规范多项式：

$$H=\left\{-c+g_1+g_2-g_1g_2,-s+g_0+i-2g_0i,-g_2+ab,-g_1+g_0i,-g_0+a+b-2ab\right\}$$

那么 H 是 $J(A)=\langle H\rangle$ 关于序 $a<b<i<g_0<g_1<g_2<s<c$ 的 Gröbner 基。

为了消除内部变量 g_0,g_1,g_2，直接将输出 s,c 表示为加法器输入 a,b,i 的多项式。下面就给出相关定义和定理，其中 R 表示环 $k[a,b,i,s,c,g_0,g_1,g_2]$ 和 R_{elim} 表示环 $k[a,b,i,s,c]$ [9]。

定义 4.2 给定 $J\subset R$，消去理想 J_{elim} 是 R_{elim} 的理想，定义 $J_{elim}=J\cap R_{elim}$ [9]。

定理 4.1 设 $J\subset R$ 为理想， H' 是 J 关于序 $a<b<i<s<c<g_0<g_1<g_2$ 的 Gröbner 基。那么集合 $H_{elim}=H'\cap R_{elim}$ 是消去理想 J_{elim} 的 Gröbner 基[9]。

例 1 (续) 为了消除变量 g_0,g_1,g_2，从 H 中删除涉及这些变量的多项式是不可行的。因此我们根据定理 4.1 中给定的序，去计算第二个 Gröbner 基 H'。再从 H' 中删除涉及 g_0,g_1,g_2 的多项式，得

$$H_{elim}=\left\{-2c-s+a+b+i,-s+a+b+i-2ab-2ai-2bi+4abi\right\}.$$

由定理 4.1， H_{elim} 是 $J_{elim}(A)$ 的 Gröbner 基，则 Gröbner 基就通过加法器重写得以化简。值得一提的是，对于本文研究的能完全分为全加器和半加法器的乘法器，可以约化首项是全加器或半加法器的和输出多项式，如 H_{elim} 中多项式 $-2c-s+a+b+i$ 就可以被首项是 $-s$ 的多项式约化。将其从 Gröbner 基中消除会带来进一步的改进，但 Gröbner 基消除该方法有失完备性。

5. 增量式等价性验证

本节引入了一种基于电路列式切片的增量验证将乘法器电路的整体 Gröbner 基划分为 $2n$ 个更小的切片 Gröbner 基。将问题分解为更小的 $2n$ 个子问题，逐个解决[15] [16]。

定义 5.1 设 C 和 C'是两个电路，如果 s_i-s_i' 是一个 PCC $(i=0,1,\cdots,m-1)$，那么电路 C 和 C'是等价的，记为 $C\equiv C'$。

引理 5.1 $C\equiv C'$ 当且仅当 $\sum_{i=0}^{m-1}2^i(s_i-s_i')\in J(C\cup C')$。

引理 5.2 设 C 和 C'是 两个电路，G 和 G' 是理想 $J(C)$ 和 $J(C')$ 关于序 $\prec,\prec'$ 的 Gröbner 基。设 $\prec_{\cup}$ 是一个反向拓扑序，使得 $\prec,\prec'$ 属于 $\prec_{\cup}$ 中。那么 $G\cup G'$ 是理想 $J(C\cup C')$ 关于 $\prec_{\cup}$ 的 Gröbner 基。

本文中的增量式等价性验证技术，使用切片和切片 Gröbner 基的定义[15]。对电路进行切片，进而进行增量式的等价性验证，由于电路 $C\cup C'$ 的和的规范可能是未知的，或者无法在 Z 上以规范和抽象形式表示，不能使用对给定规范执行理想成员的资格测试。因此将 $C\cup C'$ 和表示为多项式集，并将它们的 Gröbner基组合成一个模型 $G_{\cup}=G\cup G'$。然后将问题转化为测试 G_1 和 G_2 关于 $G_{\cup}$ 中变量之间的成员关系。

定义 5.2 设是 C 和 C'上述的两个电路

1) 对于每对输出位 s 和 s'，我们确定其输入锥，即与门，其依赖于：

$$I_i = \{门g \mid g在输出s或s'的输入锥\}$$

2) 切片 S_i 定义为连续锥 I_i 的差：

$$S_0 \coloneqq I_0$$

$$S_{i+1} \coloneqq I_{i+1} \setminus \bigcup_{j=0}^{i} S_j$$

若 G_i 是切片 S_i 中电路 C 和 C'的门 的多项式集，则易证 G_i 是切片 S_i 的 Gröbner 基。

定义 5.3 设 C 和 C'是上述两个电路，在其变量上 m 个 $\Delta_0,\cdots,\Delta_m$ 的多项式序列称为切片多项式序列，如果

$$-\Delta_i + 2\Delta_{i+1} + (s_i - s_i') \in J(C \cup C'),\ (0 \le i \le m)$$

那么多项式 $E_i = -\Delta_i + 2\Delta_{i+1} + (s_i - s_i')$ 就称为 $\Delta_0,\cdots,\Delta_m$ 序列的切片关系。

定理 5.4 设 C 和 C'是上述两个电路，$\Delta_0,\cdots,\Delta_m$ 是定义 4.3 中定义的切片多项式序列。那么根据引理 5.1，C 和 C'是等价的($C \equiv C'$)当且仅当 $2^m\Delta_m - \Delta_0 \in J(C \cup C')$。

证明：

根据定义 5.3，得 $J(C \cup C')$

$$\sum_{i=0}^{m-1} 2^i (s_i - s_i') = \sum_{i=0}^{m-1} 2^i (2\Delta_{i+1} - \Delta_i) = 2^m\Delta_m - \Delta_0$$

设边界 $2^m\Delta_m = 0$

$$\Delta_{m-1} = [2\Delta_m + (s_m - s_m')]\%G_{m-1}$$

$$\Delta_{m-2} = [2\Delta_{m-1} + (s_{m-1} - s_{m-1}')]\%G_{m-2}$$

$$\vdots$$

$$\Delta_0 = 0$$

这确保了所有的 E_i 都在 $J(C \cup C')$ 中。$J(C \cup C')$ 包含所有的域多项式 F，因此将它们添加到 $G \cup G'$ 中。最后，计算是否 $\Delta_0 = 0$。下面给出算法：

算法 1：**等价性验证**

输入：电路 *C* 和 *C'*的切片 Gröbner 基 G_i

输出：确定电路 *C* 和 *C'*是否等价($C \equiv C'$ **)**

1 $\Delta_m \leftarrow 0$;

2 for←从 *m*-1 到 0

3 $\Delta_i \leftarrow remainder(2\Delta_{i+1} + s_i - s_i', G_i \cup F)$

4 end

5 return $\Delta_0 = 0$

根据定理 5.4，我们能推导出增量等价性验证算法。先固定边界 $2^m\Delta_m = 0$，并通过计算切片 Gröbner 基的 $2\Delta_{i+1} + s_i - s_i'$ 模的余数递归地导出 Δ_i，$E_i \in J(C \cup C')$。通过计算最后 Δ_0 的结果。如果 $\Delta_0 = 0$，则乘法器电路 C 和 C'是等价的。

6. 实验

本文对两类整数乘法器进行等价性验证，分别是 *btor* 乘法器和 *sp-ar-rc* 乘法器。这两个乘法器都是

根据推论 3.2 中的部分积作为两个输入位，然后由全加器和半加法器进行累加，如图 2 所示。

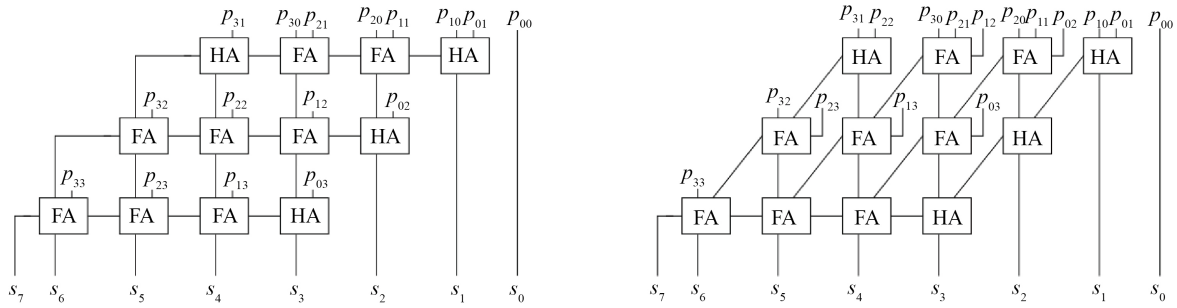

Figure 2. Structure of *btor* (left) and *sp-ar-rc* multipliers for $n=4$ with $p_{ij}=a_ib_j$

图 2. 具有 $p_{ij}=a_ib_j$ 的 $n=4$ 的 *btor* 乘法器(左)和 *sp-ar-rc* (右)乘法器的结构

图 2 是 $n=4$ 的 4 位两输入的实验验证的两类乘法器的结构。在 *btor* 乘法器中，全加法器和半加法器以网格状结构累积(图 2 左侧)；而在 *sp-ar-rc* 乘法器中，全加法器和半加法器是对角累积的(图 2 右侧)。我们使用工具 aigmultopoloy [15]，该工具以电路的 AIG 表示作为输入，并返回一个包含计算指令的文件。由于 Mathematica 输入语言更灵活，支持更多变量，被用作计算机代数系统，因而本文将这些指令传递给 Mathematica。

实验使用了一台带有 Ubuntu18.04 虚拟机的笔记本电脑，配备 Intel i5-8250 1.60 GHz CPU 和 4 GB 主内存。运行时间限制设置为 1200 秒，主内存使用限制为 4 GB。实验中的时间均以秒为单位列出。我们测量从 aigmultopoloy 开始到 Mathematica 完成的时间，包括该 aigmultopoloy 工具生成 Mathematica 文件所需的时间和计算机代数系统的启动时间。在实验数据中用 TO 表示达到时间限制、MO 表示达到内存限制、EE 表示状态错误。

如表 1 所示，无论是 Lingeling 还是 ABC 在 n 大于 8 位时，都超出实验设定的运行时间，而增量方法能验证达 32 位的这两类乘法器的等价性[16]。在此基础上添加加法器重写(第六列)，不仅能计算高达 128 位的等价性，同时 8~32 位乘法器的等价性验证也有着明显的加快。表中最后一列，不仅采用增量验证方法，还利用第四节中提到的 Gröbner 基消去，实验数据显示，与第六列相比对各位数乘法器的验证时间均略具优势。

Table 1. Equivalence checking

表 1. 等价性验证

乘法器	n	*Lingeling*	*ABC*	*增量方法*	*+加法器重写*	*+Gröbner 基消去*
btor vs. sp-ar-rc	8	13	18	2	0	0
btor vs. sp-ar-rc	16	TO	TO	8	1	1
btor vs. sp-ar-rc	32	TO	TO	82	4	3
btor vs. sp-ar-rc	64	TO	TO	TO	21	17
btor vs. sp-ar-rc	128	TO	TO	TO	188	175

7. 结论

本文基于 Gröbner 基着眼于结构相似的乘法器，采用了增量式的等价性验证算法。在这个基础上，添加加法器重写和 Gröbner 基消去的算法相关实现，并已于 Linux 系统中成功编译。实验对比不同方法

进行等价性验证的运行时间，由实验数据易见，增量等价性验证能提高验证效率，并在此基础上进一步进行优化，其验证时间略具优势。未来如何将这些技术扩展到浮点运算，甚至更具挑战性的乘法器结构和其他算术电路还有待进一步研究。

参考文献

[1] 包日辉. SoC 设计平台中若干 IP 模块的设计[D]:[硕士学位论文]. 杭州: 杭州电子科技大学, 2019.

[2] Clarke, E.M., Grumberg, O. and Peled, D. (1999) Model Checking. The MIT Press, Cambridge.

[3] 韩俊刚, 杜敏慧. 数字硬件的形式化验证[M]. 北京: 北京大学出版社, 2001.

[4] 静思. 让科学之声以更强的力度震撼神州大地一从“奔腾芯片”的错误引发的联想[J]. 电子展望与决策, 1995(3): 23.

[5] Pruss, T., Kalla, P. and Enescu, F. (2014) Equivalence Verification of Large Galois Field Arithmetic Circuits Using Word-Level Abstraction via Gröbner Bases. *Proceedings of the* 51*st Annual Design Automation Conference*, San Francisco, June 2014. 1-6. https://doi.org/10.1145/2593069.2593134

[6] Fan, Q.R., Pan, F. and Duan, X.D. (2011) Using Logic Synthesis and Circuit Reasoning for Equivalence Checking. *Advanced Materials Research*, **201-203**, 836-840. https://doi.org/10.4028/www.scientific.net/AMR.201-203.836

[7] Vedhus, H. (2020) Deep Bayesian Neural Networks for Damage Quantification in Miter Gates of Navigation Locks. *Structural Health Monitoring*, **19**, 1391-1420. https://doi.org/10.1177/1475921719882086

[8] 周宁. 代数化符号模拟验证的应用研究[D]: [博士学位论文]. 北京: 北京交通大学, 2015.

[9] Cox, D., Little, J. and O'Shea, D. (1997) Ideals, Varieties, and Algorithms. Springer-Verlag, New York. https://doi.org/10.1007/978-1-4757-2693-0

[10] Huang, G.L. and Zhou, M. (2015) On The Termination of Algorithm for Computing Relative Gröbner Bases. *ACM Communications in Computer Algebra*, **49**, 28. https://doi.org/10.1145/2768577.2768632

[11] 李春红. 基于乘法器的振幅调制实验特性研究[J]. 2020, 33(2): 33-37.

[12] Sayed-Ahmed, A., Große, D., Kühne, U. Soeken, M. and Drechsler, R. (2016) Formal Verification of Integer Multipliers by Combining Gröbner Bases with Logic Reduction. 2016 *Design*, *Automation & Test in Europe Conference & Exhibition*, Dresden, 14-18 March 2016, 1048-1053. https://doi.org/10.3850/9783981537079_0248

[13] Chen, J. and Chen, Y. (2001) Equivalence Checking of Integer Multipliers. Proceedings of the 2001 Asia and South Pacific Design Automation Conference, Yokohama, 169-174. https://doi.org/10.1145/370155.370315

[14] Lv, J., Kalla, P. and Enescu, F. (2013) Efficient Gröbner Basis Reductions for Formal Verification of Galois Field Arithmetic Circuits. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, **32**, 1409-1420. https://doi.org/10.1109/TCAD.2013.2259540

[15] Ritirc, D., Biere, A. and Kauers, M. (2017) Column-Wise Verification of Multipliers Using Computer Algebra. 2017 Formal Methods in Computer Aided Design, Vienna, 2-6 October 2017, 23-30. https://doi.org/10.23919/FMCAD.2017.8102237

[16] Ritirc, D., Biere, A. and Kauers, M. (2018) Improving and Extending the Algebraic Approach for Verifying Gate-Level Multipliers. 2018 *Design*, *Automation & Test in Europe Conference & Exhibition*, Dresden, 19-23 March 2018, 1556-1561. https://doi.org/10.23919/DATE.2018.8342263