一份关于“大”布尔方程近期发展的综述

Ali Muhammad Ali Rushdi

电气与计算机工程系，工程学院，阿卜杜勒阿齐兹国王大学，沙特阿拉伯吉达 21589，邮政信箱 80200{arushdi@ieee.org; arushdi@kau.edu.sa}

摘要。数字电路设计中经常遇到的一项任务，是求解形如 $\mathrm{h}(\boldsymbol{X},\boldsymbol{Y},\boldsymbol{Z})=1$ 的二值布尔方程，其中 $\mathrm{h}: B_2^{k+m+n} \rightarrow B_2$，而 $\boldsymbol{X}$、$\boldsymbol{Y}$ 和 $\boldsymbol{Z}$ 分别是长度为 k、m 和 n 的二进制向量，分别表示输入、中间值和输出。从该方程中消去变量 $\boldsymbol{Y}$ 所得到的消元结果式可写成 $g(\boldsymbol{X},\boldsymbol{Z})=1$，其中$g$: $B_2^{k+n} \rightarrow B_2$。通常，需要根据 $\boldsymbol{X}$ 求解 $\boldsymbol{Z}$，因此不可避免地要采用“ 大”布尔代数，即大于二值布尔代数的有限（原子）布尔代数。另一类必须求解“大”布尔方程的情形，是所谓的“数字电路设计基本问题”。这类问题涉及五个向量布尔量 $\boldsymbol{X}$、$\boldsymbol{Y}$、$\boldsymbol{Z}$、$\boldsymbol{s}$ 和 $\boldsymbol{t}$，它们分别属于 B_2^k、B_2^m、B_2^n、B_2^l 和 B_2^l。考虑一个具有两个（向量）输入 $\boldsymbol{X}$ 和 $\boldsymbol{Y}$ 以及一个向量输出 $\boldsymbol{t}(\boldsymbol{X},\boldsymbol{Y})$ 的“父”组合网络 C，并假设网络 C 由两个子网络 A 和 B 组成，其中子网络 A 具有单个（向量）输入 $\boldsymbol{X}$ 和向量输出 $\boldsymbol{Z}(\boldsymbol{X})$；而网络 B 具有两个向量输入 $\boldsymbol{Z}(\boldsymbol{X})$ 和 $\boldsymbol{Y}$，以及向量输出 $\boldsymbol{s}(\boldsymbol{Z},\boldsymbol{Y})$，该输出与网络 C 的向量输出 $\boldsymbol{t}(\boldsymbol{X},\boldsymbol{Y})$ 完全相同。上述结构涉及三个向量布尔函数，即 $\boldsymbol{Z}(\boldsymbol{X})$、$\boldsymbol{s}(\boldsymbol{Z},\boldsymbol{Y})$ 和 $\boldsymbol{t}(\boldsymbol{X},\boldsymbol{Y})$。当利用 $\boldsymbol{s}(\boldsymbol{Z}(\boldsymbol{X}),\boldsymbol{Y})$ 与 $\boldsymbol{t}(\boldsymbol{X},\boldsymbol{Y})$ 相等这一信息，并结合已知的三个函数 $\boldsymbol{Z}(\boldsymbol{X})$、$\boldsymbol{s}(\boldsymbol{Z},\boldsymbol{Y})$ 和 $\boldsymbol{t}(\boldsymbol{X},\boldsymbol{Y})$ 中的两个来推导第三个函数时，会出现三个问题。其中两个问题是必须求解“大”布尔方程的自然实例。求解“大”布尔方程的方法大致可分为代数法、表格法、数值法和图方法。其中最突出的是代数法和图方法。本文针对方法的简易性、效率和可用性，对这两类方法进行了综述和比较。本文将布尔方程的解主要分为包含式通解、参数化通解和特解。在包含式通解中，每个变量都表示为一个区间，该区间基于原函数连续的合取或析取消元式构成。在参数化通解中，每个变量都通过任意参数表示，这些参数是从底层布尔代数中自由选取的元素。特解是从底层布尔代数到每个相关变量的赋值，该赋值使布尔方程成为恒等式。本文通过一个示例，对这三类解进行了教程式阐述、回顾和比较。该示例还从一种近期发展起来的、依赖原子分解的技术角度进行了考察。事实表明，图技术至少可以与代数技术相竞争（并且有时优于代数技术），因为图技术能够更好地控制相关函数表示的最小性，因此更有能力生成更紧凑的解。

关键词：布尔方程的解、包含式通解、参数化通解、特解、原子分解、数字设计。

1. 引言

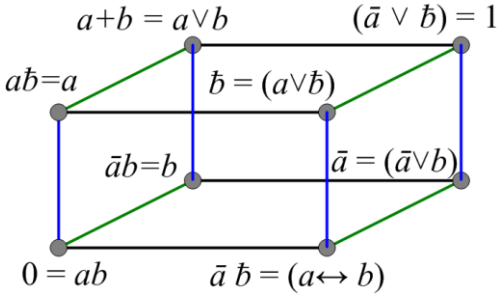
数学界和工程界中一个突出的“误称”是“布尔代数”这一术语。该术语被广泛用于指代开关代数，而开关代数只是有限“布尔代数”的一个特例，它具有 0 个生成元、1 个原子，以及属于 $\mathrm{B}_2 = \{0, 1\}$ 的两个元素。“布尔代数”一词指的是基数有限或无限的代数（Halmos 和 Givant，2009）。事实上，“有限布尔代数”涵盖了由自然数 $n\,(n \geq 0)$ 描述的可数无限多个原子代数，其中一个代数具有 n 个生成元、N 个原子（$2^{n-1} < \mathrm{N} \leq 2^n$）和 2^{N} 个元素。无意中使用一般术语“布尔代数”来指代其开关代数这一特例 B_2，会导致许多问题、谬误和误解，因为开关代数比广义有限（原子）布尔代数简单得多。因此，许多作者（Ahmad 和 Rushdi，2018年；Brown，1990年；Rushdi 和 Ahmad，2017年；2018年；Rushdi和Amashah，2012年；Rushdi 和 Zagzoog，2019年）开始将除 B_2 之外的有限布尔代数（即具有 n 个生成元（$n > 0$）的代数）称为“大”布尔代数。图 1 将两个“大”布尔代数 B_8 和 B_{16}, 的载体（有补分配格）可视化，展示了其元素之间的“偏序”。在此，超立方体 B_{16} 是自由布尔代数 $FB(a, b)$。当其四个原子中的一个（此处为 ab）被置零时，它会收缩为立方体 B_8。两个代数都需要（至少）两个生成元 a 和 b。

“大”布尔代数中的布尔方程研究贯穿了过去两个世纪，Boole、Schröder、Whitehead、Poretski、Löwenheim、Rudeanu 和 Brown 等杰出学者为此作出了奠基性贡献。这一事实表明，我们确实是站在巨人的肩膀上。“大”布尔方程求解的重要性怎么强调都不为过。它渗透到数字或逻辑设计的许多子领域，例如布尔函数分解、数字电路的故障诊断与无冒险综合、二进制码构造、触发器激励以及时序电路设计。“大”布尔方程求解还被应用于现代科学的其他领域，包括生物学、文法、化学、法学、医学、光谱学和图论（Brown，1990年）。

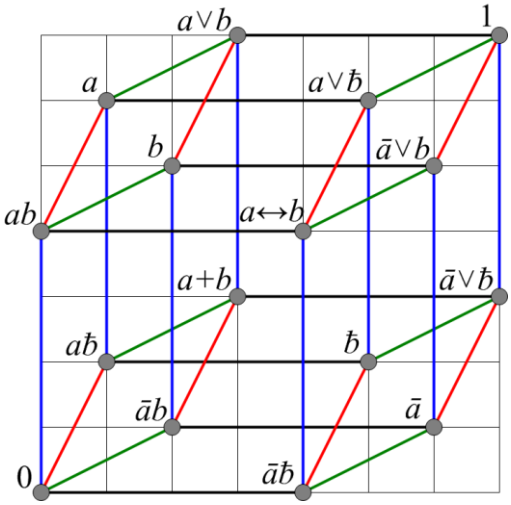
“大”布尔方程的求解方法大致可分为代数方法、表格法、数值方法和图方法。其中最重要的是代数方法和图方法。本文围绕简洁性、效率和可用性，对这两类方法进行综述和比较。本文将“大”布尔方程的主要解类型（Rudeanu，1974年；2010年；Brown；1970年；1974年；1990年；Rushdi，2001年；2004年；Baneres 等，2009年；Rushdi 和 Ba-Rukab，2003年）确定为包含式通解、参数化通解和特解。在包含式通解中，每个变量都表示为一个区间，该区间基于原函数 successive 与运算或析取消元式构成。在参数化通解中，每个变量都通过任意参数表示，而这些参数通常可以自由选取为底层布尔代数中的元素。特解是从底层布尔代数到每个相关变量的一个赋值，使布尔方程成为恒等式。本文通过一个说明性示例，对这三类解进行教程式阐述、综述和比较。该示例还将从一种最近发展起来的技术角度加以考察，这种技术依赖于相关函数和变量的原子分解。事实证明，图技术至少可以与代数技术相媲美（有时甚至优于代数技术），因为图技术能够更好地控制相关函数表示的最小性，因此更有能力生成更紧凑的解。

本文其余部分的组织如下。第 2 节介绍若干无法避免进行“大”布尔方程求解的具体情形。第 3 节讲述各种求解方法的数学细节，以及相关问题，例如如何将给定的数字规格（如 $\boldsymbol{s} = \boldsymbol{t}$ 所示形式）统一为单个布尔方程，以及变量消去的方法。特别是，第 3 节推导任意布尔方程的参数解和包含式通解，并说明如何将它们改写为所有特解的极为紧致的列表，从而能够轻松找出具有某些理想特征的特解。第 4 节比较代数方法和图方法在求解布尔方程方面的异同。第 5 节给出一个详细的

示例，其中通过三种方法获得一般参数解，分别是：(a) 直接紧致解；(b) 通过包含解间接获得的紧致解；以及 (c) 直接置换加性解，并由此得到所有特解的紧致列表。这种置换加性解是通过对相关函数和变量进行原子分解而获得的解的先驱。第 6 节总结全文。



在将 B_{16} 置于四个原子之一（ab = 0）为零的条件下折叠后得到的 B_8，格。



表示16个元素之间偏序关系的超立方体格B_{16},，其中一个例子是 $0 \le \bar{a}\bar{b} \le \bar{a} \le \bar{a} \vee \bar{b} \le 1$。

图1。两个“大”布尔代数 B_8 和 B_{16}的可视化。这里，当其四个原子之一（此处为 ab）被置零时，超立方体 $B_{16} = FB(a, b)$会塌缩为立方体 B_8。两个代数都需要（至少）两个生成元 a 和 b。

2. “大”布尔方程求解的**必要性**

现在，我们将展示若干无法避免“大”布尔方程求解的具体情形。最简单的情形涉及求解一个“逻辑逆问题”：利用对向量函数 $\boldsymbol{Z}(\boldsymbol{X})$ 的知识，求出其逆向量函数 $\boldsymbol{X}(\boldsymbol{Z})$（Jevons，1872年；1974年；Pratt，1974年；1975年b）。当 $\boldsymbol{X}$ 和 $\boldsymbol{Z}$ 分别是长度为 k 和 n的二进制向量，表示数字电路的输入和输出时，上述问题就等价于：通过了解正向函数 $\boldsymbol{Z}(\boldsymbol{X})$，推导逆电路函数 $\boldsymbol{X}(\boldsymbol{Z})$。对函数 $\boldsymbol{Z}(\boldsymbol{X})$ 的了解，可以改写为如下形式的方程：$g(\boldsymbol{X}, \boldsymbol{Z}) = 1$，其中 g：$B_2^{k+n} \rightarrow B_2$。然后对 $\boldsymbol{X}$ 求解，其元素属于自由布尔代数 $FB(\boldsymbol{Z})$，即其元素构成关于 n 个变量 Z_1、Z_2、.....和 Z_n的全部 2^{2^n} 开关函数。

一种更复杂的情形涉及数字电路设计中经常遇到的一项任务：电路规范可以（通常也确实会）归约为一个形式为 $\mathrm{h}(\boldsymbol{X}, \boldsymbol{Y}, \boldsymbol{Z}) = 1$ 的单个二值布尔方程，其中 h: $B_2^{k+m+n} \rightarrow B_2$ 与 $\boldsymbol{X}$ 与 $\boldsymbol{Z}$ 与以往相同，而 $\boldsymbol{Y}$ 是一个长度为 m 的二进制向量，表示中间值（通常无法访问，因此也无法控制，并且

不可观测）。上述方程可用于求出 $\boldsymbol{Z}$ 在 $FB(\boldsymbol{X},\boldsymbol{Y})$ 上的所有解，然后仅保留只依赖于 $\boldsymbol{X}$ 的 $\boldsymbol{Z}$ 的解。这些与 $\boldsymbol{Y}$ 无关的解，可以通过从原方程中消去变量 $\boldsymbol{Y}$ 所得的消元结果式的推导直接获得，该结果式可写成 $g(\boldsymbol{X},\boldsymbol{Z})=1$，其中 $g\colon B_2^{k+n}\to B_2$。所需的解只需对 $g(\boldsymbol{X},\boldsymbol{Z})=1$ 关于 $FB(\boldsymbol{X})$ 求解 $\boldsymbol{Z}$ 即可得到（Brown，2011年）。

更为复杂的数字电路设计情形可以用图 2 所示的总体布局来描述。该布局最初由 Ledley（1959；1960）提出，但不包含那条隐蔽的迂回路径，后来被 Bell（1968）和 Brown（1975年a）采用。Ledley 的布局包含一个由两个子网络 A 和 B 构成的组合逻辑电路 C。最终输出既可以看作子网络 B 的输出 $\boldsymbol{s}(\boldsymbol{Y},\boldsymbol{Z})$，也可以看作父网络 C 的输出 $\boldsymbol{t}(\boldsymbol{X},\boldsymbol{Y})$。其中，五个量 $\boldsymbol{X}$、$\boldsymbol{Y}$、$\boldsymbol{Z}$、$\boldsymbol{s}$ 和 $\boldsymbol{t}$ 是长度分别为 k、m、n、l 和 l 的二进制或布尔向量，分别表示基本输入、侧输入、中间值、子网络 B 的输出以及整个网络 C 的输出。这意味着，量 $\boldsymbol{X}$、$\boldsymbol{Y}$、$\boldsymbol{Z}$、$\boldsymbol{s}$ 和 $\boldsymbol{t}$ 分别属于 B_2^k、B_2^m、B_2^n、B_2^l 和 B_2^l，其中 B_2 表示二值布尔代数 B_2。因此，产生了三个“数字电路设计基本问题”（Ledley，1959；1960；Rushdi 与 Ahmad，2017），即

第一类问题：给定 $\boldsymbol{Z}(\boldsymbol{X})$ 和 $\boldsymbol{s}(\boldsymbol{Y},\boldsymbol{Z})$，求 $\boldsymbol{t}(\boldsymbol{X},\boldsymbol{Y})$。第二类问题：给定 $\boldsymbol{Z}(\boldsymbol{X})$ 和 $\boldsymbol{t}(\boldsymbol{X},\boldsymbol{Y})$，求 $\boldsymbol{s}(\boldsymbol{Y},\boldsymbol{Z})$。三型问题：给定 $\boldsymbol{s}(\boldsymbol{Y},\boldsymbol{Z})$ 以及 $\boldsymbol{t}(\boldsymbol{X},\boldsymbol{Y})$，求 $\boldsymbol{Z}(\boldsymbol{X})$。

Brown（1975年a）通过在图2中添加阴影隐蔽路径，略微改变了 Ledley 的网络结构，因此将 $\boldsymbol{s}(\boldsymbol{Y},\boldsymbol{Z})$ 替换为 $\boldsymbol{s}(\boldsymbol{X},\boldsymbol{Y},\boldsymbol{Z})$。根据图1中的阴影路径是否可以省略，或是否需要（或使用）该路径，子网络 B 被称为“诚实转换器”或“隐蔽转换器”。

第一类问题可以通过直接代入轻松求解，而第二类和三型问题则可以通过“大”布尔方程求解来处理。解决三型问题完全依赖于“大”布尔代数中的方程求解方法（Rushdi 和 Ahmad，2017年），但处理广义第二类问题则通过其他技术更为有效（Brown，1975年a；Rushdi，2018年：2019年）。

“大”布尔代数一个重要的潜在应用领域是密码学。Ahmad 和 Rushdi（2018年）最近提出了一种利用“大”布尔函数对消息进行加密的方案。该函数生成的方程无法由传统的可满足性（SAT）求解器求解，并会导致最坏情况下的 搜索空间大幅增加。逻辑密码分析表明，该方案确实非常难以破解。对手似乎无法缩减或剪枝搜索空间（除了缩短每个节点所需完成的任务），因而被迫遍历整个搜索空间。事实上，对手可能会得到多个候选解，随后必须寻找线索，以确定其中哪个才是正确的解。对手不仅要面对寻找“大”布尔方程解的过高难度，还要面对该解不唯一所带来的歧义。上述方案使布尔曲线拟合（BCF）或布尔插值问题重新受到关注；在整整一个世纪里，这一问题一直被视为纯粹的数学趣题。通过求解“大”布尔代数上的“大”布尔方程组，可以得到 BCF 问题的统一解（Rudeanu，1974年；Rushdi 和 Balamesh，2019年；Balamesh 和 Rushdi，2022年）。

3. 各种解的类型的数学推导 3.1. 将规格统一为单个布尔方程

任何布尔代数的一个显著特征是，多个方程组成的方程组等价于单个方程。例如，考虑图 2 所示的数字系统，该系统由以下 l 标量形式的向量布尔方程表示

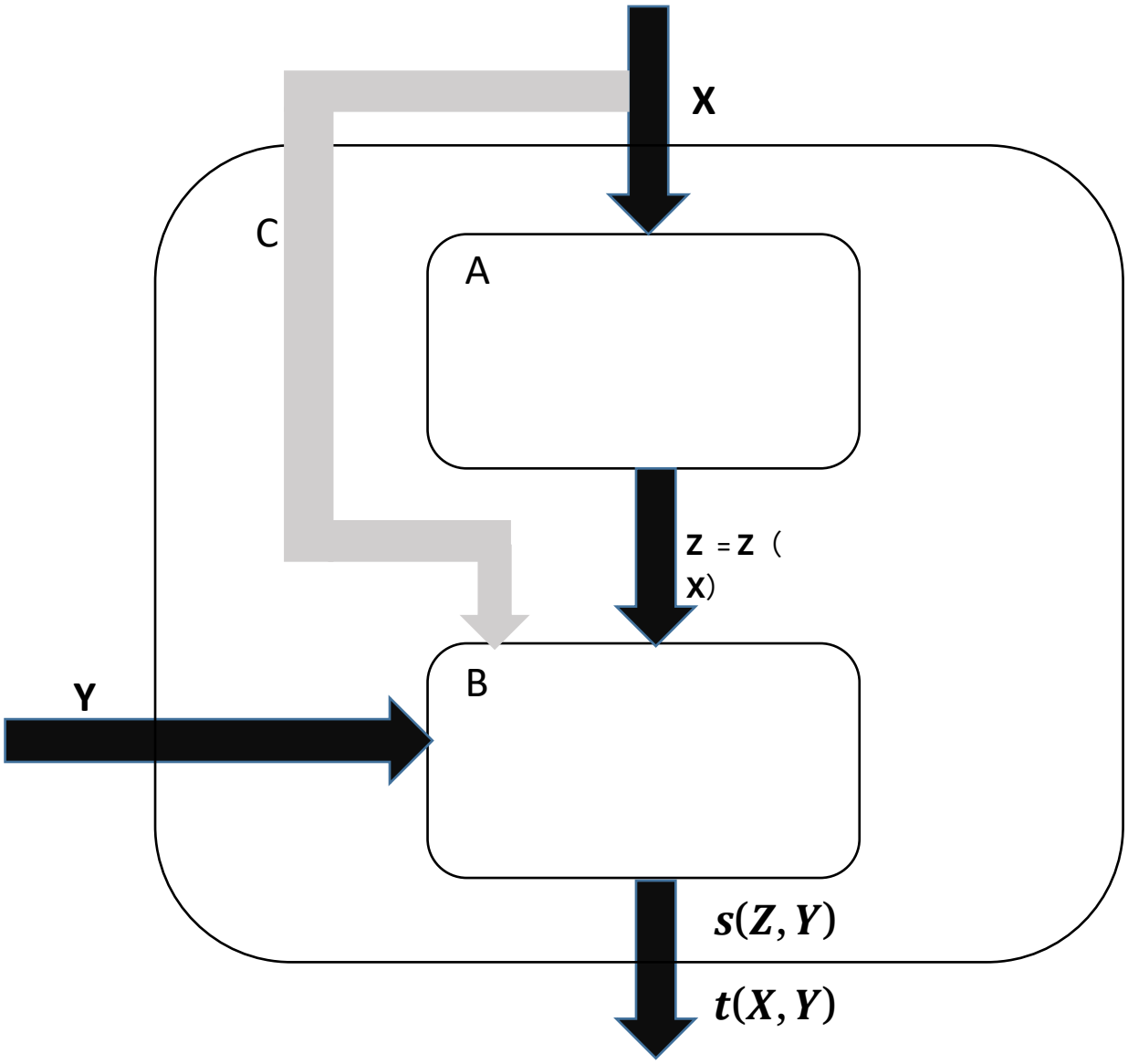


图 2. 数字电路设计广义问题的布局（如果需要隐蔽的（点状）路径，则将函数 $s(Z.\ Y)$ 替换为 $s(X, Z, Y)$）。

$$\boldsymbol{s} = \boldsymbol{t}, \tag{1a}$$

或等价的标量形式

$$s_i = t_i\,, \qquad 1 \leq i \leq l, \tag{1b}$$

其中 $s_i = s_i(\mathbf{X}, \mathbf{Y}, \mathbf{Z})$ 与 $t_i = t_i(\mathbf{X}, \mathbf{Y}, \mathbf{Z})$。由 l 个标量方程组成的系统 **(1)** 化简为如下形式的单个布尔方程

$$h(\boldsymbol{X}, \boldsymbol{Y}, \boldsymbol{Z}) = 1\,, \tag{2a}$$

其中

$$h(\boldsymbol{X},\boldsymbol{Y},\boldsymbol{Z}) \equiv \wedge_{i=1}^{l}(s_i \odot t_i), \tag{2b}$$

或具有以下形式

$$r(\boldsymbol{X},\boldsymbol{Y},\boldsymbol{Z}) = 0\,, \tag{3a}$$

其中

$$r(\boldsymbol{X},\boldsymbol{Y},\boldsymbol{Z}) = \bar{h}(\boldsymbol{X},\boldsymbol{Y},\boldsymbol{Z}) \equiv \vee_{i=1}^{l}(s_i \oplus t_i). \tag{3b}$$

方程（2b）和（3b）中的符号 $\wedge$、 $\vee$、 $\oplus$ 和 $\odot$ 分别表示与运算符、或运算符、异或（Exclusive-OR）运算符以及同或（符合或等价）运算符。（2b）与（3b）之间的关系只是两个德摩根定律的表达。请注意，与运算符和或运算符是对偶的，而同或和异或运算符既互补又对偶。

3.2. 变量消去

Brown（2011年）证明，从布尔方程（3a）（称为母方程）中消去变量 $\boldsymbol{Y}$ 所得到的消元结果式为导出布尔方程

$$f(\boldsymbol{X},\boldsymbol{Z}) = 0\,, \tag{4a}$$

其中

$$f(\boldsymbol{X},\boldsymbol{Z}) \equiv \vee_{\mathbf{A}\in\{0,1\}^m}\ r(\boldsymbol{X},\boldsymbol{A},\boldsymbol{Z})\,. \tag{4b}$$

并且，导出方程的解恰好是母方程 (3a) 中不涉及被消去变量 $\boldsymbol{Y}$ 的那些解。

在此我们将使用上述结果的对偶形式，即如果我们用 (2a) 而不是 (3a) 作为母方程，那么消去变量 $\boldsymbol{Y}$ 后得到的消元结果式就是互补导出布尔方程

$$g(\boldsymbol{X},\boldsymbol{Z}) = 1\,, \tag{5a}$$

其中

$$g(\boldsymbol{X},\boldsymbol{Z}) \equiv \wedge_{\mathbf{A}\in\{0,1\}^m}\ h(\boldsymbol{X},\boldsymbol{A},\boldsymbol{Z})\,. \tag{5b}$$

并且，导出方程 (5a) 的解恰好是母方程 (2a) 中不涉及被消去变量 $\boldsymbol{Y}$ 的那些解。

3.3. 参数解的推导

我们寻求形如（5a）的布尔方程的解，其中 $g(\boldsymbol{X},\boldsymbol{Z})$: $B_2^{k+n} \to B_2$ 是由 k 个二值变量 $\boldsymbol{X} = [\,X_1\ X_2\ \ldots\ldots X_k\,]^T$ 和 n 个二值变量 $[\,Z_1\ Z_2\quad Z_n\,]^T$ $\boldsymbol{X}$ $\boldsymbol{Z}$ .....

构成的二值布尔函数。然而，我们不需要列出 和 的二进制解，而是希望用 $\boldsymbol{X}$ 表示 $\boldsymbol{Z}$ 。这意味着我们正在寻求一个“大型”布尔方程的解。我们将 $g(\boldsymbol{X},\boldsymbol{Z})$ 视为 $g(\boldsymbol{X};\ \boldsymbol{Z})$，或简单地视为 $g(\boldsymbol{Z})$，并将（5a）改写为

$$g(\boldsymbol{Z}) = 1, \tag{6}$$

其中 $g(\boldsymbol{Z})$：$B_{2^K}^n \rightarrow B_{2^K}$，且 B_{2^K} 是自由布尔代数 $FB(X_1, X_2 \ldots\ldots X_k)$，具有 $K = 2^k$ 个原子和 $2^K = 2^{2^k}$ 个元素。现在，我们用其最小项标准形（MCF）（Brown，1990）表示 $g(\boldsymbol{Z})$

$$g(\boldsymbol{Z}) \equiv \vee_{\mathbf{A} \in \{0,1\}^n} \; g(\boldsymbol{A})\, \boldsymbol{Z}^{\boldsymbol{A}}\,. \tag{7}$$

对于 $\boldsymbol{Z} = [\, Z_1\, Z_2\, .\, .\, Z_n\,]^{\,T} \in \; B_{2^K}^n$，$\boldsymbol{A} = [\, a_1\, a_2\, .\, .\, a_n\,]^{\boldsymbol{T}} \in \{0,1\}^n$，符号 $\boldsymbol{Z}^{\boldsymbol{A}}$ 定义为

$$\boldsymbol{Z}^{\boldsymbol{A}} = \; {Z_1}^{a_1}\; {Z_2}^{a_2} \ldots\; {Z_n}^{a_n}, \tag{8}$$

其中，如果 $a_i = 0$，${Z_i}^{a_i}$ 取值为 $\bar{Z}_i$（取补文字）；如果 $a_i = 1$，则取值为 Z_i（未取补文字）。对于 $\mathbf{A} \in \{0, 1\}^n$，符号 $\boldsymbol{Z}^{\boldsymbol{A}}$ 涵盖 $\boldsymbol{Z}$的最小项，即 2^n 基本乘积或原始乘积

$$\overline{Z_1}\,\overline{Z_2} \ldots \overline{Z_{n-1}}\,\overline{Z_n},\;\; \overline{Z_1}\,\overline{Z_2} \ldots \overline{Z_{n-1}}\,Z_n,\;\; \ldots.,\; Z_1\, Z_2 \ldots Z_{n-1}\, Z_n. \tag{9}$$

方程（7）中的常量值 g（$\boldsymbol{A}$）是 B_{2^K} 的元素，称为 g（$\boldsymbol{Z}$）的判别式。这些判别式是 g（$\boldsymbol{Z}$）的自然映射的条目，其输入域为 $\{0, 1\}^n \subseteq B_{2^K}^n$。布尔代数 $B_{2^K} = FB$（$X_1, X_2 \ldots\ldots .\, X_k$）具有生成元 X_i（$1 \leq \; i \; \leq \; k$），它们看起来像变量（事实上，在我们将其角色改为生成元之前，它们原本就是输入变量）。因此，我们可以接受出于历史原因赋予 g（$\boldsymbol{Z}$）的自然映射的名称，即变量输入卡诺图（VEKM）。现在我们注意到，$\boldsymbol{X}$ 的最小项，即 $2^k = K$ 基本乘积或原始乘积

$$\overline{X_1}\,\overline{X_2} \ldots \overline{X_{k-1}}\,\overline{X_k},\;\; \overline{X_1}\,\overline{X_2} \ldots \overline{X_{k-1}}\,X_k,\;\; \ldots,\;\; X_1\, X_2 \ldots X_{k-1}\, X_k, \tag{10}$$

正是底层布尔代数的所有原子。为方便起见，我们将这些原子称为 T_i $(0 \leq \; i \; \leq \; (K-1))$，因此 $g(\boldsymbol{A})$ 可以写成

$$g(\boldsymbol{A}) \; = \vee_{i=0}^{K-1} \; (e_i(\boldsymbol{A}) \wedge \; T_i\,), \tag{11}$$

其中，我们使用符号 $e_i(\boldsymbol{A})$ 表示事件的指示函数，即原子 T_i 出现在 $g(\boldsymbol{A})$ 的表达式中，即

$$e_i(\boldsymbol{A}) = \begin{Bmatrix} 1,\; if\; T_i \;\rightarrow\; g(\boldsymbol{A}) \\ 0,\; otherwise \end{Bmatrix} = \; g(\boldsymbol{A})/T_i, \tag{12}$$

其中，符号 $(r \,/\, s) = (r)_{s=1}$ 表示 r 关于 s 的布尔商（Brown，1990）。方程 (12) 表示，$e_i(\boldsymbol{A})$ 指示原子 T_i 是否出现在自然映射中 $g(\boldsymbol{Z})$ 的单元 $\boldsymbol{A}$ 内。现在，我们将 n_i $(0 \leq \; n_i \; \leq \; 2^n)$ 定义为 T_i 在 $g(\boldsymbol{A})$ 的表达式 (11) 中实际出现的总次数，即

$$n_i = \; \sum_{\mathbf{A} \in \{0,1\}^n} \; e_i(\boldsymbol{A})\,. \tag{13}$$

(1a) 在B_{2^K}（原样）上的无条件特解总数$N_{unconditional}$ 为

$$N_{unconditional} = \; \prod_{i=0}^{K-1} \; n_i. \tag{14}$$

如果某个$n_i = 0$，即如果某个原子T_i永远不会出现在任何表达式$g(\boldsymbol{A})$中，而其中$\boldsymbol{A} \in \{0,1\}^n$（也就是说，如果$T_i$不出现在$g(\boldsymbol{Z})$的映射表的任何单元格中），则该数为零。为避免这种情况，必须坚持以下一致性条件：任何满足T_i且$n_i = 0$的原子都必须被禁止或置零。这意味着底层布尔代数会失去这些原子，从而退化为一个更小的代数，即其某个真子代数。在这个新的布尔代数上，解的数量为

$$N_{conditional} = \prod_{\substack{i=0 \\ n_i \neq 0}}^{K-1} n_i. \tag{15}$$

请注意，当$n_i = 1$对于$0 \leq i \leq (K-1)$时，这个数可以是1（即唯一解），但实际上也可能增长到极大的值。现在，我们引入一组参数$\boldsymbol{p}_i$ $(0 \leq i \leq (K-1),\ n_i \neq 0)$，以构造一个正交归一标签集，并将其附加到判别式$g(\boldsymbol{A})$中断言原子$T_i$的各个出现实例上（即附加到$g(\boldsymbol{Z})$的自然映射中的单元格$\boldsymbol{A} \in \{0,1\}^n$上）。原子$T_i$所需参数的最小数量（向量$\boldsymbol{p}_i$的长度）为

$$l(\boldsymbol{p}_i) = \lceil \log_2 n_i \rceil, \qquad 0 \leq i \leq (K-1), n_i \neq 0. \tag{16}$$

这里，$\lceil x \rceil$表示实数x向上取整，即大于或等于x的最小整数。参数$\boldsymbol{p}_i$可用于生成一组$n_i \leq 2^{l(\boldsymbol{p}_i)}$正交归一标签$\{t_1, t_2 \ldots t_{n_i}\}$，使得

$$t_1 \vee t_2 \vee \ldots \vee t_{n_i} = 1, \tag{17a}$$

$$t_{j_1} \wedge t_{j_2} = 0 \qquad \forall\ j_1, j_2 \in \{1, 2, \ldots, n_i\}. \tag{17b}$$

当$n_i = 2^{l(\boldsymbol{p}_i)}$正交归一标签集可以被可视化为卡诺图中单元格的乘积时，其图变量就是基础参数。如果$2^{l(\boldsymbol{p}_i)-1} < n_i < 2^{l(\boldsymbol{p}_i)}$，此类图中的某些单元格会被合并，并且该图会简化为一种类似图的结构。

当原子T_i的每次出现都由其正交归一标签集中的某个特定成员进行标记时，会得到辅助函数$G(\boldsymbol{Z}, \boldsymbol{p}_i)$ $(0 \leq i \leq (K-1),\ n_i \neq 0)$。此时，参数解由下式给出（Brown，1970年；Rushdi 和 Amashah，2011年；Rushdi 和 Ahmad，2018年；Rushdi 和 Zagzoog，2019年）。

$$Z_u = \vee_{\{\mathbf{A} \in \{0,1\}^n | A_u = 1\}} G(\boldsymbol{A}, \boldsymbol{p}_i).\ 1 \leq u \leq n, (0 \leq i \leq (K-1),\ n_i \neq 0). \tag{18}$$

在（18）中用于为所有原子构造标签的参数总数为

$$E = \sum_{i=1}^{k} l(\boldsymbol{p}_i) = \sum_{i=1}^{k} \lceil \log_2(n_i) \rceil. \tag{19}$$

传统方法是从共享的参数池中选择参数向量，以尽量减少所使用的参数数量，此时其变为

$$E' = \max_i\ l(\boldsymbol{p}_i) = \max_i \lceil \log_2 n_i \rceil = \lceil \log_2 (\max_i n_i) \rceil. \tag{20}$$

然而，所使用的参数必须属于底层布尔代数（可能会因一致性条件而退化）。现在，我们提议为每个原子T_i（$0 \leq i \leq K-1$ $n_i \neq 0$ 18 ，）使用独立参数$\boldsymbol{p}_i$。表达式（）不会像传统情形那样紧凑，但独立参数$\boldsymbol{p}_i$现在属于二值布尔代数B_2（Brown，2003年；Rushdi和Amashah，2011年），这一事实有助于生成所有特解，正如下一小节中即将看到的那样。

3.4.包含性通解

函数 g（$\boldsymbol{Z}$） 关于其前 k 个变量的集合（k = *0*，1，...，n）的析取消元式（Brown，1990年）或连接导数（Thayse，1975年）g_{k+1}（Z_{k+1}，Z_{k+2}，...，Z_n）定义为

$$g_1(Z_1, Z_2, \ldots, Z_n) = g(Z_1, Z_2, \ldots, Z_n), \tag{21a}$$

$$g_k(Z_k, Z_{k+1}, \ldots, Z_n) = g_{k-1}(1, Z_k, Z_{k+1}, \ldots, Z_n) \vee g_{k-1}(0, Z_k, Z_{k+1}, \ldots, Z_n), \ (k = 2, 3, \ldots, n), \tag{21b}$$

$$g_{n+1} = g_n(1) \vee g_n(0). \tag{21c}$$

方程 (5a) 在满足一致性条件时有解 $\boldsymbol{Z} \in B_2^n$。当由 (21c) 给出的 g_{n+1} 为 1 时，即满足这一条件；此时，方程组 $\{g_n = 1, g_{n-1} = 1, ..., g_1 = 1\}$ 可按逆序求解，得到

$$\overline{g_n}(0) \leq Z_n \leq g_n(1), \tag{22a}$$

$$\overline{g_j}(0, Z_{j+1}, \ldots, Z_n) \leq Z_j \leq g_j(1, Z_{j+1}, \ldots, Z_n), \ (j = n-1, \ldots, 1). \tag{22b}$$

注意，上述每个方程都是前一个方程的一致性条件（即 $g_{k+1} = 1$ 是 $g_k = 1$ 的一致性条件，k = n, (n-1), ..., 1）。应用这些一致性条件后，解 (22a) 修改为

$$s_n \leq Z_n \leq t_n, \tag{23a}$$

$$s_k(Z_{k+1}, Z_{k+2}, \ldots, Z_n) \leq Z_k \leq t_k(Z_{k+1}, Z_{k+2}, \ldots, Z_n) \quad (k = n-1, n-2, ..., 1), \tag{23b}$$

其中

$$\overline{g_n}(0)\, g_n(1) \leq s_n \leq \overline{g_n}(0), \tag{24a}$$

$$g_n(1) \leq t_n \leq \overline{g_n}(0) \vee g_n(1), \tag{24b}$$

$$\overline{g_k}(0, Z_{k+1}, Z_{k+2}, ..., Z_n)\, g_k(1, Z_{k+1}, Z_{k+2}, ..., Z_n) \leq s_k \leq \overline{g_k}(0, Z_{k+1}, Z_{k+2}, ..., Z_n), \ (k = n-1, n-2, ..., 1), \tag{24c}$$

$$g_k(1, Z_{k+1}, Z_{k+2}, \ldots, Z_n) \leq t_k \leq \overline{g_k}(0, Z_{k+1}, Z_{k+2}, \ldots, Z_n) \vee g_k(1, Z_{k+1}, Z_{k+2}, \ldots, Z_n), \ (k = n-1, n-2, \ldots, 1), \tag{24d}$$

该解称为双不等式包含式解。Rushdi（2001；2004）将其改写为以下等价形式，称为双不等式包含式解的不完全指定的变体

$$s_n = \overline{g_n}(0)\, g_n(1) \vee d(\overline{g_n}(0)), \tag{25a}$$

$$t_n = g_n(1) \vee d(\overline{g_n}(0)), \tag{25b}$$

$$s_k = \overline{g_k}(0, Z_{k+1}, Z_{k+2}, ..., Z_n)\, g_k(1, Z_{k+1}, Z_{k+2}, ..., Z_n) \vee d(\overline{g_k}(0, Z_{k+1}, Z_{k+2}, ..., Z_n)), \quad (k = n-1, n-2, \ldots, 1), \tag{25c}$$

$$t_k = g_k(1, Z_{k+1}, Z_{k+2}, ..., Z_n) \vee d(\overline{g_k}\,(0, Z_{k+1}, Z_{k+2}, ..., Z_n)), (k = n\text{-}1, n\text{-}2, ..., 1), \quad (25d)$$

为方便起见，我们将 $g_n(0)$ 记为 $g_n(0_n)$，将 $g_n(1)$ 记为 $g_n(1_n)$，将 $(0, Z_{k+1}, Z_{k+2}, ..., Z_n)$ 记为 $g_k(0_k)$，并将 $g_k(1, Z_{k+1}, Z_{k+2}, ..., Z_n)$ 记为 $g_k(1_k)$。因此，方程 (21) 和 (25) 可以改写为以下形式

$$g_1 = g \quad (26a)$$

$$g_k = g_{k-1}\,(0_{k\text{-}1}) \vee g_{k-1}\,(1_{k\text{-}1}), (k = 2, 3, \ldots, n+1) \quad (26b)$$

$$s_k = \overline{g_k}\,(0_k)\, g_k(1_k) \vee d(\overline{g_k}\,(0_k)), \quad (k = n, n\text{-}1, \ldots, 1), \quad (26c)$$

$$t_k = g_k(1_k) \vee d(\overline{g_k}\,(0_k)), \quad (k = n, n\text{-}1, \ldots, 1). \quad (26d)$$

其中，d(.) 表示无关算子（Reusch，1975年；Rushdi 和 Albarakati，2012年；2014）。请注意，该记法

$$f = g \vee d(h), \quad (27)$$

表示

$$\{g = 1\} \rightarrow \{f = 1\}, \quad (28a)$$

$$\{g = 0\} \wedge \{h = 0\} \rightarrow \{f = 0\} \quad (28b)$$

请注意，当 ({g = *0*} ⋀ {h = *1*}) 时，(28) 并未说明 f 的取值。记法 (27)（在有多个变量 X 的情况下）应理解为

$$f(\boldsymbol{X}) = g(\boldsymbol{X}) \vee (d(\boldsymbol{X}) \wedge h(\boldsymbol{X})), \quad (29)$$

但是，尽管显然可以理解任意函数 d(X) 取决于 X，为便于运算，这种依赖关系被隐藏或隐含起来。在逻辑设计领域，隐藏无关符号 d 对相关变量的依赖关系是一种常见做法。

3.5. 所有特解的列举

参数解 (18) 可通过展开树生成所有特解。通常，在传统方法中，这种展开树是一棵完全树，需要将$2^{K'}$ 值赋给每个E' 参数，其中$K' \leq K$ 是底层布尔代数中原子的最终数量（可能因一致性条件而发生某些合并）。每个父节点有$2^{K'}$ 个子节点，树的根节点以下有E' 层。因此，树有 $(2^{K'})^{E'} = 2^{K'E}$ 个叶节点。这些叶节点构成全部特解集合，但可能存在重复。为避免重复，我们从第一个展开层级开始，便确保合并解值相同的兄弟节点。经过这种合并后，树不再是完全树，其叶节点恰好就是特解，即没有重复。如果进一步允许合并同层的表亲节点，树就会被一个紧凑列出特解的无环图取代（Rushdi，2012年）。

在另一种方法中（Rushdi 和 Ahmad，2018年），要构造完全形式的展开树，需为每个E 独立参数赋予二进制值 {0,1}。由于完全二叉树的根节点以下有E 层，因此它有2^E 个叶节点。合并解值相同的兄弟节点后，树不再是完全树，其叶节点就是不重复的特解。由于通常$E < K'E'$（尽管$E > E'$），这种方法中的展开树规模通常小于传统方法。不过，这种替代方法的真正优势在于，它可以完全避免使用展开树（或展开无环图）。关键在于注意到，参数解 (18) 可以改写为原子的加权和：这些原子T_i 出现在函数$g(\boldsymbol{Z})$的判别式$g(\boldsymbol{A})$（如式 (11) 所示）中，即：

$$\boldsymbol{Z} = \vee_{\substack{i=0 \\ n_i \neq 0}}^{K-1} (\boldsymbol{Co}(T_i) \wedge T_i), \tag{30}$$

其中，我们将向量 $\boldsymbol{Co}(T_i)$ 称为断言原子 T_i 的“贡献”，并将合取式 $(\boldsymbol{Co}(T_i) \wedge T_i)$ 称为该原子的“总贡献”。现在注意到，$\boldsymbol{Co}(T_i)$ {or $\boldsymbol{Co}(T_i) \wedge T_i$} 恰好有 n_i 种可能取值，这些取值可以通过表示相关标签时所使用的相同类似卡诺图的结构方便地列出。因此，我们将式（30）解释为一种方便列出所有特解的方法：将断言原子 T_i 的总贡献进行析取，其中总贡献以其全部 n_i 种可能形式给出。要获得一个具体的特解，只需对每个原子的总贡献任意选取其中一种可能形式，然后将所选的总贡献相加即可。以这种方式得到的特解总数与式（15）给出的总数一致。式（30）中的解也可以通过相关函数和变量的原子分解获得（Balamesh 和 Rushdi，2019年；2022年）。

3.6. 选取具有特定特征的特解

方程（30）至关重要，因为它在紧凑的空间内列出了数量（可能非常庞大）的所有特解。因此，只需快速查看上述列表，就可以选取具有某些特定理想特征的解。

4. 关于代数方法和图方法

代数方法构成了其他方法赖以建立的支柱，并且在每个实现细节中都不可或缺。图过程除了作为一种实用的方式来组织代数方法之外，并未增添任何超越代数方法的内容（Rudeanu，2003年）。然而，这种实用性不应被低估，因为它增添了图示直观和分治策略，从而促进运算，使其更快且不易出错，并且可能产生更加紧凑的结果（Rushdi和Amashah，2012年）。图方法能够方便地处理布尔函数的繁琐运算，其中包括：（a）否定或求补这一元运算，它可以在图形式的函数上逐单元应用；以及（b）任意二元运算（例如与、或、异或），它可以逐单元地作用于两个均采用图形式的函数。此外，图折叠（Rushdi，1986年；Rushdi 和 Rushdi，2018年）能够直接实现关于布尔函数的一个或多个变量的并微分和交微分运算（也称为对这些变量进行合取消去或析取消去）。

图方法并不局限于使用经典卡诺图（CKM），还通过使用变量输入卡诺图（VEKM）与代数方法相互衔接；变量输入卡诺图在本质上属于半代数方法（Rushdi和Amashah，2011年）。含有 n 个变量的布尔函数具有 2^n 种 VEKM 表示（取决于图变量和输入变量的选择），其范围从 CKM（含 n 个图变量和 0 个输入变量）到纯代数表达式（含 0 个图变量和 n 个输入变量）。这清楚地表明，纯代数表达式是 VEKM 表示的一种特殊情况。当然，VEKM 无法处理无限布尔代数，但它可作为有限“大型”布尔代数的自然映射（Brown，1990年）。因此，没有理由声称代数方法

优于 VEKM方法，因为后者将前者包含为特殊情况。恰恰相反，VEKM方法在本质上属于半代数方法，因此始终能够充分利用代数理论所提供的结果。它们能够更好地控制相关函数表示的最小性。

具体而言，Rushdi和Amashah（2012年）研究了Rudeanu（2003年）的纯代数方法，并指出该方法之所以简洁，是因为牺牲了双不等式包含式解所提供的一个自由度；因此，它采用了该解的一个特殊的完全指定实例。由此，它只能在一组选定系数上实现局部最小性，而不是在更基本的相关变量和生成元集合上实现局部最小性。因此，这种纯代数方法并不总是像一般的VEKM方法那样高效，后者寻求基于双不等式包含式解的不完全指定的变体来实现全局最小性。这意味着，VEKM解至少不劣于纯代数解，但有时会更优。

5. 一个说明性示例

本节研究的问题取自一本关于布尔代数的旧著（Goodstein，1963年），该书通过一种非构造性定理证明方法给出了一个一般的参数化“解”。然而，这个所谓的解通常无法满足其 intended 求解的方程，因为它没有认识到一致性条件的必要性。考虑布尔函数

$$f(\mathrm{X},\mathrm{Y}) = \mathrm{c}\,(\mathrm{a}\vee\mathrm{X})\,(\mathrm{b}\vee\mathrm{Y}), \tag{31}$$

其中 $f\colon \mathrm{B}_{256}^{2}\to\mathrm{B}_{256}$，与 $\mathrm{B}_{256}=\mathrm{FB}(\mathrm{a},\mathrm{b},\mathrm{c})$。方程 $\{f=0\}$ 的解用独立“变量”a、b 和 c 表示因变量 X 和 Y；本文将这些独立变量视为底层布尔代数的生成元。我们对函数 f 取补，得到 $g=\bar{f}$，从而求解等价方程

$$g(\mathrm{X},\mathrm{Y}) = \bar{\mathrm{c}}\vee\bar{\mathrm{a}}\bar{\mathrm{X}}\vee\bar{\mathrm{b}}\bar{\mathrm{Y}} = 1, \tag{32}$$

其中 $g\colon \mathrm{B}_{256}^{2}\to\mathrm{B}_{256}$。在接下来的三个小节中，我们给出方程（32）的三个解。这些解分别是直接得到的常规参数解、通过一个次和得到的常规参数解，以及一个置换加性参数解。

5.1. 直接得到的常规参数解

g 关于其两个自变量 X 和 Y 的布尔-香农展开为

$$\begin{aligned} g(\mathrm{X},\mathrm{Y}) &= \left(\bar{\mathrm{a}}\vee\bar{\mathrm{b}}\vee\bar{\mathrm{c}}\right)\bar{\mathrm{X}}\,\bar{\mathrm{Y}}\vee\left(\bar{\mathrm{a}}\vee\bar{\mathrm{c}}\right)\bar{\mathrm{X}}\,\mathrm{Y}\vee\left(\bar{\mathrm{b}}\vee\bar{\mathrm{c}}\right)\mathrm{X}\,\bar{\mathrm{Y}}\vee\left(\bar{\mathrm{c}}\right)\mathrm{X}\,\mathrm{Y} \\ &= \left(\bar{\mathrm{a}}\mathrm{bc}\vee\bar{\mathrm{a}}\bar{\mathrm{b}}\mathrm{c}\vee a\bar{\mathrm{b}}\mathrm{c}\vee\bar{\mathrm{c}}\right)\bar{\mathrm{X}}\,\bar{\mathrm{Y}}\vee\left(\bar{\mathrm{a}}\mathrm{bc}\vee\bar{\mathrm{a}}\bar{\mathrm{b}}\mathrm{c}\vee\bar{\mathrm{c}}\right)\bar{\mathrm{X}}\,\mathrm{Y}\vee\left(a\bar{\mathrm{b}}\mathrm{c}\vee\bar{\mathrm{a}}\bar{\mathrm{b}}\mathrm{c}\vee\bar{\mathrm{c}}\right)\mathrm{X}\,\bar{\mathrm{Y}}\vee\left(\bar{\mathrm{c}}\right)\mathrm{X}\,\mathrm{Y}, \end{aligned} \tag{33}$$

因此，其自然映射（变量输入卡诺图（VEKM））如图3所示。该映射中的每个条目都是“输入变量”或生成元 a、b 和 c 的函数，并且是 FB(a, b, c) 的八个原子中的若干个的析取。图3映射各单元格中这八个原子的出现次数分别为 4、3、4、2、4、0、4 和 2，这立即表明：

1. 原子 abc 完全没有出现在图3中映射的任何单元格里。这意味着该原子必须被置零，即方程（32）的一致性条件为

$$\mathrm{abc} = 0. \tag{34}$$

当布尔代数 $\mathrm{B}_{256}=\mathrm{FB}(\mathrm{a},\mathrm{b},\mathrm{c})$ 失去其 abc 原子后，便塌缩为一个仅含 7 个原子的子代数，即塌缩为 B_{128}。B_{256} 和 B_{128} 的规模过大，无法在此进行可视化。

不过，为了让读者一窥代数塌缩的含义，我们已经在图1中展示了表示 B_{16}，的超立方体格，并进一步表示了它在失去 ab 原子后塌缩为 B_8 的过程。

2. 式（32）的特解数量等于图3中断言原子出现次数的乘积，即

$$N_{particular} = 2^2 * 3^1 * 4^4 = 3072. \tag{35}$$

式（32）的参数解所需的最少参数数量为

$$k = \lceil \log_2 4 \rceil = 2\,. \tag{36}$$

事实上，预计这一数量小于或等于所涉及的变量数量（Brown，1990），此处为$n = 2$。

为便于获得参数数量最少的参数解，我们注意到，四个原子 $a\bar{b}\bar{c}$、$a\bar{b}c$、$ab\bar{c}$ 和 abc 均普遍存在于图3的图中，因此我们将它们合并为 $\bar{c}$。注意，这种合并是允许的，因为它等价于对这些原子的每个实例分别以相同方式使用同一组正交归一标签，或对它们的总析取 $\bar{c}$ 集体使用同一组正交归一标签。在图4中，我们构造辅助函数 $G_1(X, Y; a, b, c; u, v)$：将正交归一集 $\{\bar{u}\bar{v}, \bar{u}v, u\bar{v}, uv\}$ 中的标签附加到项 $\bar{c}$（该项出现4次），将正交归一集 $\{(\bar{u}\bar{v} \vee uv),\ \bar{u}v, u\bar{v}\}$ 中的标签附加到原子 $a\bar{b}c$（该原子出现3次），并将正交归一集 $\{(\bar{u} \vee v),\ u\bar{v}\}$ 中的标签附加到原子 $ab\bar{c}$（该原子出现2次）。我们选择上述正交归一集，是为了获得最紧凑的解。事实上，我们并不在意 $X\bar{Y}$-单元格中的条目有多繁琐，因为它们不会影响最终解。然而，其他三个单元格中每个单元格都只有一个标签，即 $X\bar{Y}$-单元格中的标签 $\bar{u}v$、$XY\bar{}$-单元格中的标签 $u\bar{v}$，以及 XY-单元格中的标签 uv。我们可以在图4的每个单元格中加入归零原子 abc 无关项。我们的最终解为

$$X = \left(\bar{a}\bar{b}c \vee a\bar{b}c \vee \bar{c}\right)u\bar{v} \vee \bar{c}uv \vee d(abc) \tag{37a}$$
$$Y = \left(\bar{a}\bar{b}c \vee \bar{a}bc \vee \bar{c}\right)\bar{u}v \vee \bar{c}uv \vee d(abc). \tag{37b}$$

通过忽略无关项并应用反射律，可以简化这些公式，得到

$$X = u(\bar{b}c\bar{v} \vee \bar{c}(\bar{v} \vee v)) = u(\bar{b}\bar{v} \vee \bar{c}) \tag{38a}$$
$$Y = v(\bar{b}c\bar{u} \vee \bar{c}(\bar{u} \vee u)) = v(\bar{a}\bar{u} \vee \bar{c}) \tag{38b}$$

将解（38）代入（32）得到

$$f(X, Y) = c\left(a \vee u\bar{b}\bar{v} \vee u\bar{c}\right)(b \vee v\bar{a}\bar{u} \vee v\bar{c}) = abc = 0, \tag{39}$$

而将其代入（33）得到

$$\begin{aligned} g(X, Y) &= \bar{c} \vee \bar{a}(\bar{u} \vee (b \vee v)c) \vee \bar{b}(\bar{v} \vee (a \vee u)c) \\ &= \bar{c} \vee \bar{a}\bar{u} \vee \bar{a}b \vee \bar{a}v \vee \bar{b}\bar{v} \vee a\bar{b} \vee \bar{b}u(\bar{u} \vee (b \vee v)c) = \bar{a} \vee \bar{b} \vee \bar{c} = 1, \end{aligned} \tag{40}$$

其中，将 $a\bar{b}\bar{}$ 的共识项添加到式（40）的第二行，然后与 $(a\bar{b} \vee ab\bar{})$ 合并，得到 $(a\bar{} \vee b\bar{})$，后者随后吸收 $(a\bar{u} \vee a\bar{}v \vee b\bar{}\bar{v} \vee b\bar{}u)$。上述替换的结果验证了解，并部分解释了一致性条件存在的原因。由于一致性条件（34），我们进一步采用了 $(a\bar{} \vee b\bar{} \vee \bar{c}) = 1$，因为这是通过对（34）两边取补得到的。如果采用图最小化技术（Rushdi，1987），上述代数运算本可以大大简化。

5.2. 通过包含解得到的常规参数解

在本小节中，我们利用变量输入卡诺图（VEKM）以最紧凑的形式推导出式（29）的一般包含解。图 5 展示了根据 Rushdi（2001；2004）的方法用于获得该解的变量输入卡诺图。最终得到的结果为

$$0 \le Y \le \bar{c} \vee \bar{a}\,\bar{X} \tag{41a}$$
$$0 \le X \le \bar{b} \vee \bar{c}\,, \tag{41b}$$

受一致性解约束

$$\bar{a} \vee \bar{b} \vee \bar{c} = 1. \tag{41c}$$

我们可以将包含解 (41) 转换为一个参数解，即

$$X = u(\bar{b} \vee \bar{c}) \tag{42a}$$
$$Y = v(\bar{c} \vee \bar{a}\bar{X}) = v(\bar{c} \vee \bar{a}\bar{u} \vee \bar{a}bc) = v(\bar{c} \vee \bar{a}\bar{u} \vee \bar{a}b). \tag{42b}$$

将此解代入 (31)，可得

$$f(X,Y) = c\big(a \vee u\bar{b} \vee u\bar{c}\big)(b \vee v\bar{c} \vee v\bar{a}\bar{u} \vee v\bar{a}b) = abc = 0. \tag{43}$$

该解并不像 (38) 中的解那样对称。因此，它可用于生成第三个解，即：

$$Y = v(\bar{a} \vee \bar{c}) \tag{44a}$$
$$X = u(\bar{c} \vee \bar{b}\bar{Y}) = u(\bar{c} \vee \bar{b}\bar{v} \vee a\bar{b}) = v(\bar{c} \vee \bar{a}\bar{u} \vee \bar{a}b). \tag{44b}$$

尽管解（42）和（44）不像（38）中的解那样具有对称性，但它们的优点在于，在每个解中，一个变量只依赖于单个参数，而不是两个参数。

5.3. 置换加性参数解

尽管（38）、（42）或（44）中的解优雅、紧凑且具有对称性，但它们并不便于用来列出所有特解，因为两个参数u 和v 都应被赋予一个独立的值，该值等于 B_{128} 中的某个特定元素。为此所使用的展开树应探索（u，v）值的全部$128 \times 128 = 16384$ 种组合，最终将得到 3072 个解。为避免使用这种展开树，我们采用另一种方法：为每个单个原子使用独立参数，如图6所示。所使用的参数数量从2个大幅增加到12个；尽管与之前的（38）、（42）或（44）中的解相比，详细的代数解会更加繁琐，但它仍然是一个具有原子分解性质的置换加性公式，并且以紧凑的形式列出了方程（32）的全部3072个特解。该公式简洁地给于图7中。要获得向量$[X\ Y]^T$的值，只需为每个原子选择其关联的任意可能值即可。满足条件 $abc = 0$的特解示例有两个：

$$\begin{bmatrix} X \\ Y \end{bmatrix} = \bar{a}\bar{b}\bar{c}\begin{bmatrix} 0 \\ 0 \end{bmatrix} \vee \bar{a}\bar{b}c\begin{bmatrix} 0 \\ 0 \end{bmatrix} \vee \bar{a}b\bar{c}\begin{bmatrix} 0 \\ 0 \end{bmatrix} \vee \bar{a}bc\begin{bmatrix} 0 \\ 0 \end{bmatrix} \vee a\bar{b}\bar{c}\begin{bmatrix} 0 \\ 0 \end{bmatrix} \vee a\bar{b}c\begin{bmatrix} 0 \\ 0 \end{bmatrix} \vee ab\bar{c}\begin{bmatrix} 0 \\ 0 \end{bmatrix} \vee abc\begin{bmatrix} 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix} \tag{45}$$

$$\begin{bmatrix} X \\ Y \end{bmatrix} = \bar{a}\bar{b}\bar{c}\begin{bmatrix} 0 \\ 1 \end{bmatrix} \vee \bar{a}\bar{b}c\begin{bmatrix} 0 \\ 1 \end{bmatrix} \vee \bar{a}b\bar{c}\begin{bmatrix} 0 \\ 1 \end{bmatrix} \vee \bar{a}bc\begin{bmatrix} 0 \\ 1 \end{bmatrix} \vee a\bar{b}\bar{c}\begin{bmatrix} 1 \\ 0 \end{bmatrix} \vee a\bar{b}c\begin{bmatrix} 1 \\ 0 \end{bmatrix} \vee ab\bar{c}\begin{bmatrix} 1 \\ 0 \end{bmatrix} \vee abc\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} a \\ \bar{a} \end{bmatrix}. \tag{46}$$

请注意，将任一特解代入（31）后，方程可化为 $\{abc = 0\}$；代入（32）后，则可化为 $\{a^- \vee b^- \vee \bar{c} = 1\}$。

6. 结论

本文综述了历经两个世纪的“大”布尔方程求解这一主题的当代发展状况。文章强调，该主题已经足够成熟，能够在许多重要、多样且有益的领域得到应用，尤其是在数字设计和密码学领域。本文完整地介绍并演示了构造参数化通解或包含式通解的方法，以及如何简洁地列出“大”布尔方程的特解。作为延伸内容，本文解释了施加一致性条件的必要性，以及此类条件可能产生的影响：使底层布尔代数坍缩为严格更小的子代数。因此，本文为未来充分利用“大”布尔代数和“大”布尔方程求解的数学理论奠定了基础。

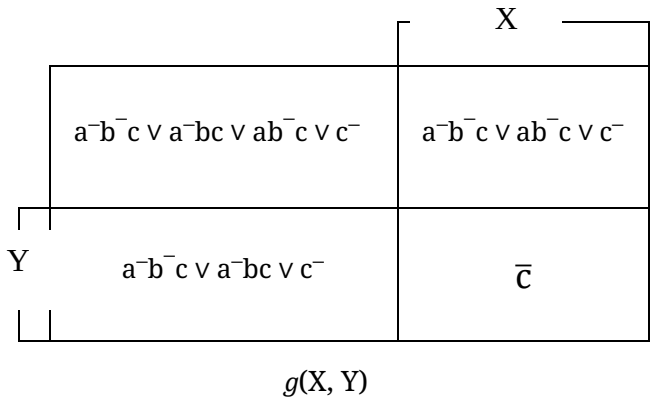


图3. g(X, Y) 的自然映射，其中四个原子 a⁻b⁻c̄、a⁻bc̄、ab⁻c̄ 和 abc̄ 组合为 c̄。这种组合等价于以相同方式，将同一组正交归一标签 $\{\bar{u}\bar{v}, \bar{u}v, u\bar{v}, uv\}$ 分别用于这些原子的实例，或将其整体用于它们的总析取 c̄。

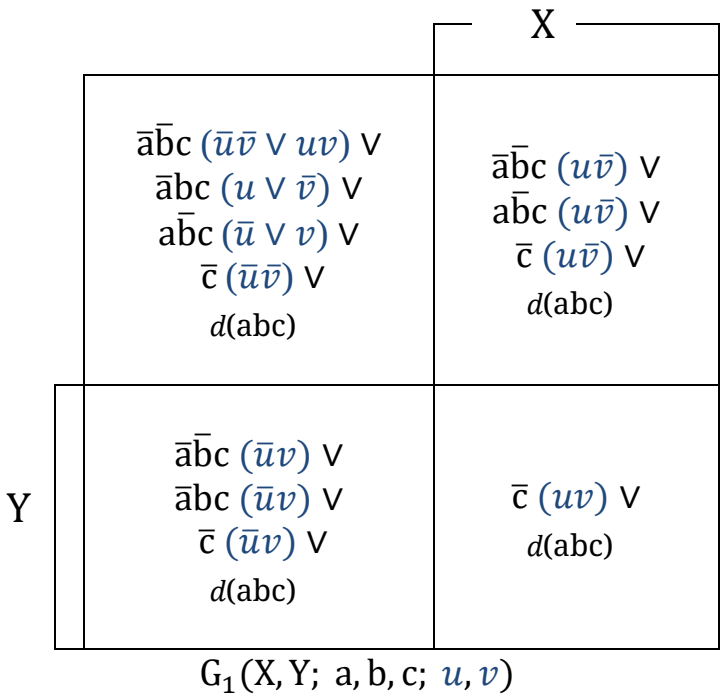
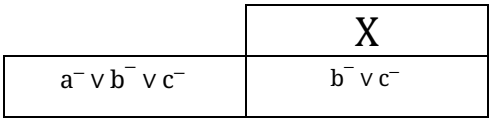
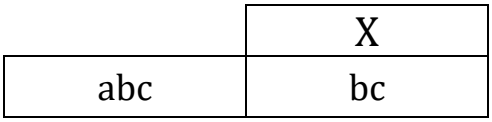


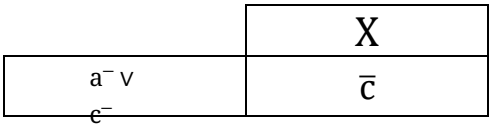
图4. 辅助函数 G_1，其每个原子实例都由正交归一集的成员标记。不同原子使用公共参数。



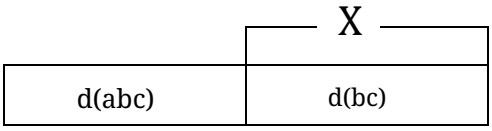
$g(X, 0)$



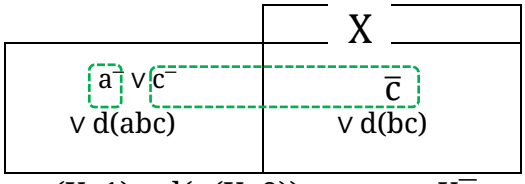
$\bar{g}(X, 0)$



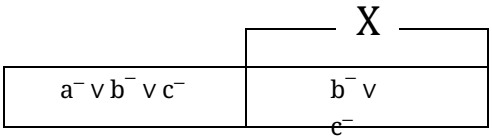
$g(X, 1)$



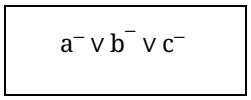
$$s_Y = \bar{g}(X, 0)g(X, 1) \vee d(\bar{g}(X, 0)) = 0$$



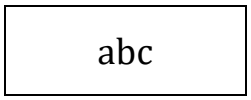
$$t_Y = g(X, 1) \vee d(\bar{g}(X, 0)) = c^- \vee a^- X^-$$



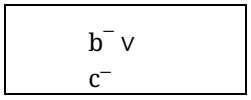
$$g_1(X) = g(X, 0) \vee g(X, 1) = 0$$



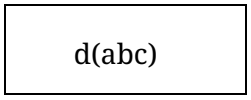
$g_1(0)$



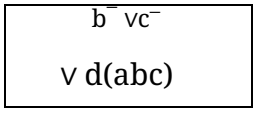
$\overline{g_1}(0)$



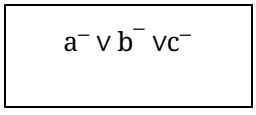
$g_1(1)$



$$s_{\mathrm{X}} = \overline{g_1}(0)\ g_1(1) \vee \mathrm{d}(\overline{g_1}(0)) = 0$$

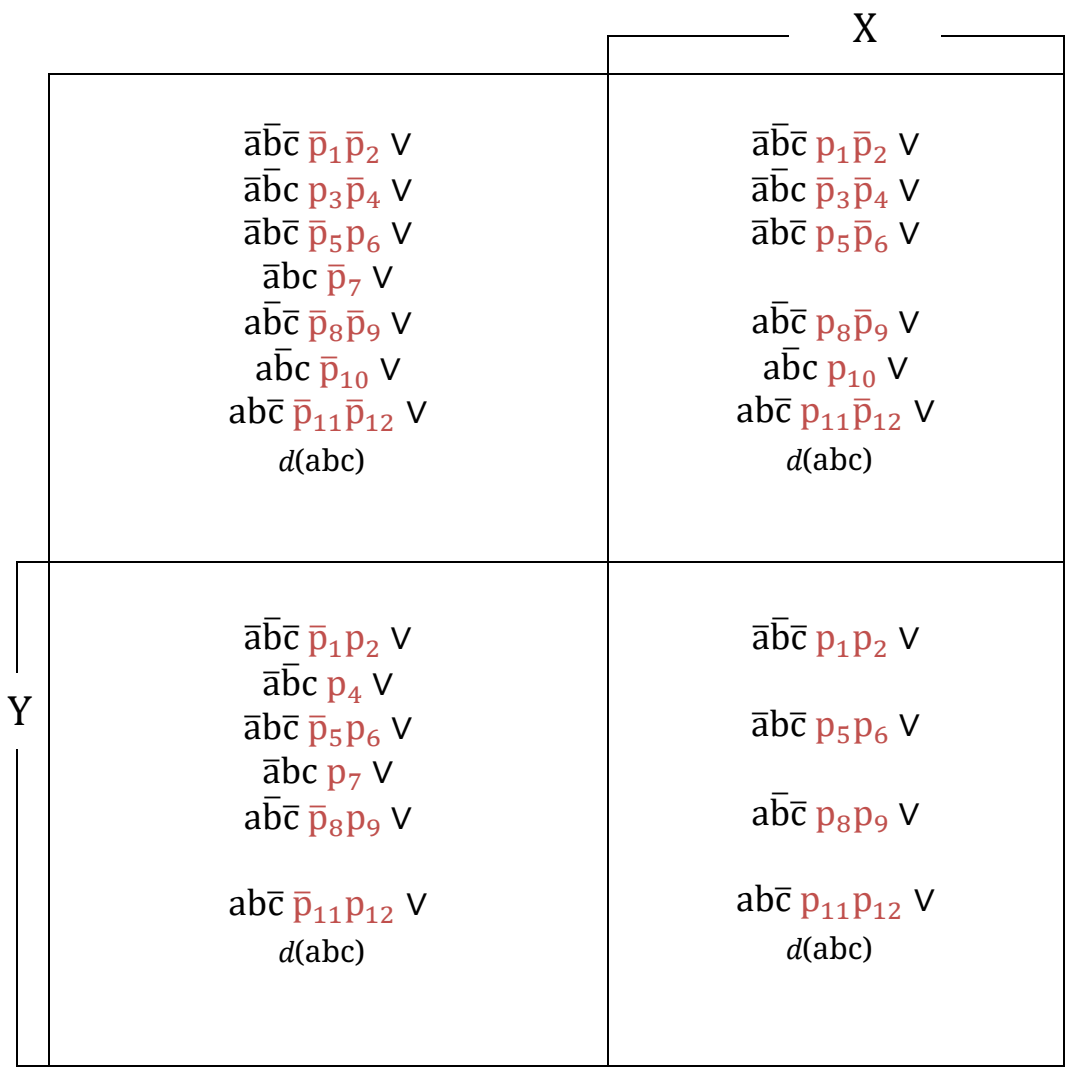


$$t_{\mathrm{X}} = g_1(1) \vee \mathrm{d}(\overline{g_1}(0)) = \mathrm{b}^- \vee \mathrm{c}^-$$



$$g_0 = g_1(0) \vee g_1(1) = 1$$

图 5. 推导式（32）最紧凑包含解时所使用的各种 VEKM。



G_2(X, Y; a、b、c; p)

图 6. 辅助函数 G_2，其中每个原子的实例均由正交归一集中的成员标记。不同原子使用独立参数，因此组合四个 $\bar{c}$ 原子不再起作用。

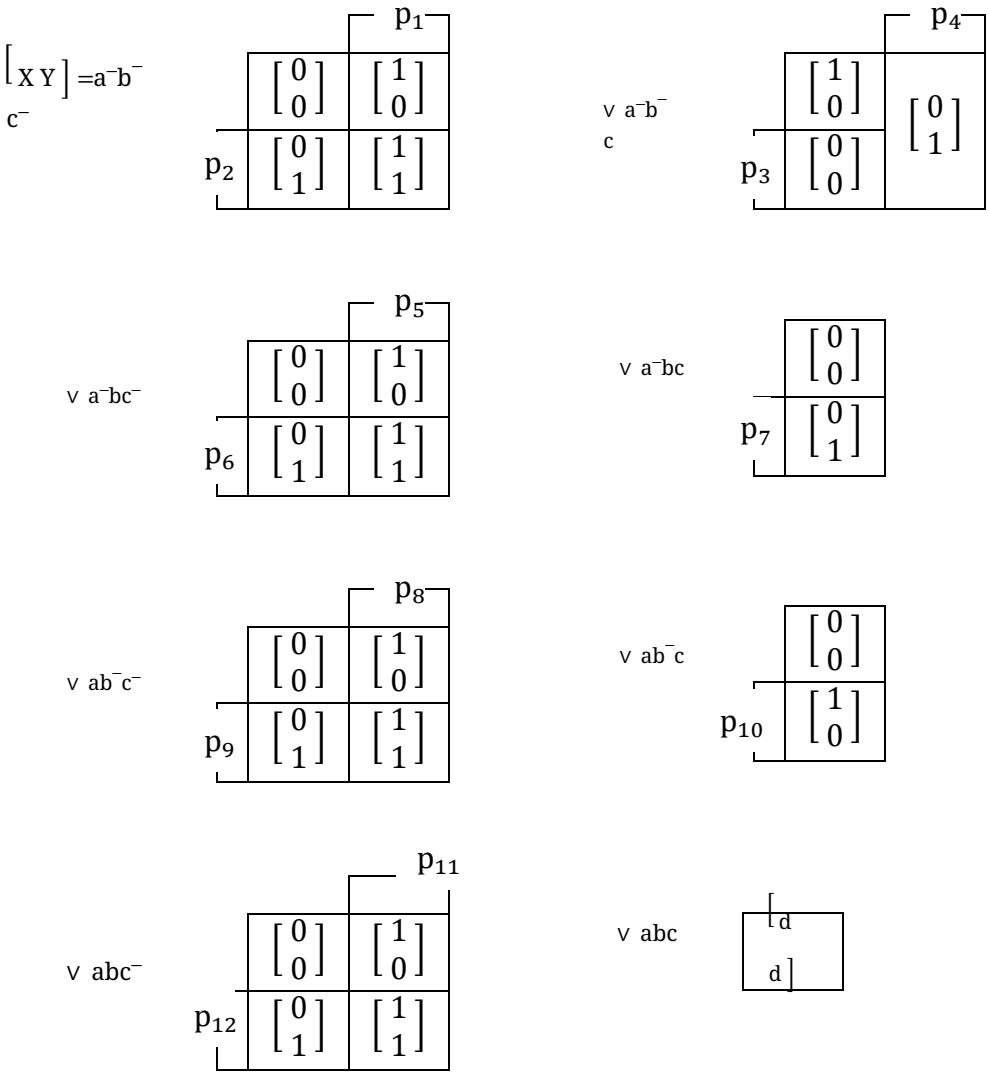


图7. 列出方程（32）全部3072个特解的置换加性公式。

致谢

本文的简短版本曾作为特邀主题演讲，在第一届工程与科学数学方法和技术国际会议（ICMMTES 2022）的全体会议上进行报告。该会议于2022年12月9日至10日在印度北阿坎德邦德拉敦的 Graphic Era Deemed to be University | Graphic Era Hill University 举行。

参考文献

Ahmad, W. & Rushdi, A. M. A.,（2018年）。利用大规模布尔可满足性难题的新型密码方案，《国际数学、工程与管理科学杂志》，3（1），47-61。

Balamesh, A. S., & Rushdi, A. M.（2019年）。通过原子分解为独立开关方程求解布尔方程。《国际计算机数学杂志：计算机系统理论》，4（3-4），185-203。

Balamesh, A. S., & Rushdi, A. M.（2022年）。布尔曲线拟合问题的原子化表述。《国际数学、工程与管理科学杂

Baneres, D., Cortadella, J., & Kishinevsky, M.（2009年）。一种求解布尔关系的递归范式。IEEE《计算机汇刊》，58(4)，512-527。Bell, N. R.（1968年）。用于教授复合输入逻辑电路基本概念的图表法。IEEE《教育汇刊》，E-11(3)，173-177。Brown, F. M.（1970年）。布尔方程的约简解，IEEE《计算机汇刊》，C-19 (10)，976-981。Brown, F. M.（1974年）。方程逻辑，IEEE《计算机汇刊》，C-23 (12)，1228-1237。Brown, F. M.（1975a）。受限输入问题，IEEE《计算机汇刊》，C-24 (1)，102-106。Brown, F. M.（1975b）。开关函数的方程实现，IEEE《计算机汇刊》，C-24 (11)：1054-1066。Brown, F. M.（1990年）。《布尔推理：布尔方程的逻辑》，Kluwer Academic Publishers，波士顿，美国。Brown, F. M.（2011年）。论布尔方程中的变量消去，《离散应用数学》，

Halmos, P., & Givant, S.（2009年）。《布尔代数导论》。Springer New York。Jevons, W. S.（

W. S.（1874年）。《科学原理：逻辑与科学方法论述》，英格兰，伦敦：MacMillan。Ledley, R. S.（1959年）。数字电路设计中的布尔矩阵方程，IRE《电子计算机汇刊》，EC-8 (6)，131-139。Ledley, R. S.（1960年）。《数字计算机与控制工程》。McGraw-Hill，纽约，NY，美国。Reusch, B.（1975年）。从子函数生成质蕴含项及覆盖问题的统一处理方法，IEEE《计算机汇刊》，C-24(9)。924-930。Rudeanu, S.（1974年）。《布尔函数与方程》，North-Holland Publishing Company & American Elsevier，阿姆斯特丹，荷兰。Rudeanu, S.（2003年）。求解布尔方程的代数方法与图方法之比较。《国际计算机数学杂志》，80(7)，815-817。Rudeanu, S.（2010年）。布尔集合与布尔方程的最一般解。《信息科学》，180(12)，2440-2447。Rushdi, A. M.（1986年）。开关函数的图表微分。《微电子学与可靠性》，26(5)，891-907。

Rushdi, A. M.（1987）。改进的变量输入卡诺图过程，《计算机与电气工程》，13(1)，41-52。Rushdi, A. M.，（2001）。使用变量输入卡诺图求解布尔方程，《国际计算机数学杂志》，78（1），23-38。Rushdi, A. M.，（2004）。使用变量输入卡诺图高效求解布尔方程，《阿卜杜勒阿齐兹国王大学学报：工程科学》，15（1），105-121。Rushdi, A. M.，（2012）。求解一般布尔方程的代数方法与图方法比较，《卡西姆大学学报：工程与计算机科学》，5（2），147-173。Rushdi, A. M. A.，（2018）。通过变量输入卡诺图处理数字电路设计中的广义第二类问题，《国际数学、工程与管理科学杂志》，3(4)，392-403。Rushdi, A. M. A.（2019）。数字电路设计中处理第二类和三型问题的基于图的方法比较。《应用科学与技术进展》第3卷第7章，国际图书出版社，胡格利，西孟加拉邦，印度，80-100。Rushdi, A. M. A. & Ahmad, W.，（2017）。通过布尔方程求解实现大布尔代数中的可满足性，《阿卜杜勒阿齐兹国王大学学报：工程科学》，28（1），3-18。Rushdi, A. M. A.，& Ahmad, W.（2018）。利用方程求解在“大”布尔代数上进行数字电路设计。《国际数学、工程与管理科学杂志》，3(4)，404-428。Rushdi, A. M. A.，& Albarakati, H. M.（2012）。布尔方程的逆问题，《计算机科学杂志》，8(12)，2098-2105。Rushdi, A. M. A. & Albarakati, H. M.（2014）。布尔方程最一般包含式解的主要类别，《信息科学》，281，53-65。Rushdi, A. M. & Amashah, M. H.（2011）。使用变量输入卡诺图生成紧凑的参数化通解，《国际计算机数学杂志》，88（15），3136-3149。Rushdi, A. M. & Amashah, M. H.（2012）。纯代数方法与VEKM方法求解大布尔方程的比较，《阿卜杜勒阿齐兹国王大学学报：工程科学》，23（2），75-85。Rushdi, A. M. A.，& Balamesh, A. S.（2019）。借助变量输入卡诺图进行布尔曲线拟合。《国际数学、工程与管理科学杂志》，4(6)，1287-1306。Rushdi, A. M.，& Ba-Rukab, O. M.（2003）。利用布尔方程的图解求解设计低成本多输出开关电路，《乌姆·阿尔古拉大学科学—医学—工程学报》，15（2），59-79。Rushdi, A. M.，& Zagzoog, S. S.（2019）。论“大”布尔方程求解及其在组合数字设计中的效用。《应用科学与技术进展》第2卷第3章，国际图书出版社，胡格利，西孟加拉邦，印度，25-48。

Rushdi, R. A.， & Rushdi, A. M.（2018）。卡诺图在医学研究中的效用：胎儿营养不良病例。《国际数学、工程与

Thayse, A.（1975年）。交与并导数及其在开关理论中的应用，《IEEE计算机汇刊》C-27(8)，713-720。