面向位向量理论的量子 SMT 求解器

Shang-Wei Lin南洋理工大学，新加坡shang-wei.lin@ntu.edu.sg

Si-Han Chen、Tzu-Fan Wang 和 Yean-Ru Chen国立成功大学，台湾chenyr@mail.ncku.edu.tw

arXiv:2303.09353v1 [cs.LO] 16 Mar 2023

摘要—给定一个可满足性模理论（SMT）公式 F，经典 SMT 求解器会尝试：(1) 将 F 抽象为布尔公式 F_B；(2) 找到 F_B的布尔解；(3) 检查该布尔解是否与理论一致。步骤（2）和（3）可能需要反复交替执行，直到找到一致的解。在这项工作中，我们开发了一种用于位向量理论的量子 SMT 求解器。借助量子系统中叠加的特性，我们的求解器能够同时考察所有输入，并一次性检查布尔域与理论域之间的一致性。

索引词 汇—**量子计算、SMT 求解器、Grover 算法** **法器**

一、引言

可满足性模理论（SMT）是指判断一阶公式相对于某个可判定一阶理论是否可满足的问题。与布尔可满足性问题（SAT）相比，SMT 中的原子可以根据其所基于的理论而呈现不同形式。凭借更丰富的表达能力，SMT 广泛应用于众多领域，尤其是形式化验证，应用范围涵盖神经网络 [13] [5] 和智能合约[4] [2]等新兴主题，以及硬件电路设计 [9] [1]。考虑以下公式 F：该公式基于定宽位向量理论，包含三个整数变量 a、 b 和 c，每个变量的长度均为 2 位。

$$F : [(a > b) \vee (a < b) \vee (a = b)] \wedge [\neg(a > b) \vee \neg(a < b) \vee \neg(a = b)]$$

公式 F 可满足，因为存在赋值 $a = 2$ 和$b = 2$，其二进制表示分别为 10 和 10，使得F 的求值结果为 True。这样的赋值称为解。如果不存在任何解，该公式就称为不可满足。

为了解决可满足性模理论问题，大多数先进的 SMT 求解器都采用经典的 惰性方法 [19], ，该方法包含三个步骤：(1) 将原始公式抽象为布尔公式，即从原始理论域抽象到布尔域；(2) 为抽象后的布尔公式寻找一个解；(3) 检查布尔域与原始理论域之间的一致性。如果第 (2) 步找到的解在两个域中并不一致，就会将其舍弃，并继续执行第 (2) 步，直到找到一个一致的解

找到后，或者判定该公式不可满足。

例如，若使用布尔变量 x、 y 和 z 分别表示谓词 $(a > b)$、$(a < b)$ 和 $(a = b)$，则公式 F可抽象为如下布尔公式 F_B:

$$F_B : (x \vee y \vee z) \wedge (\neg x \vee \neg y \vee \neg z)$$

SAT 求解器可用于寻找布尔公式F_B的解，而位向量理论求解器则可帮助检查一致性。图 1 展示了惰性方法如何求解公式 F。在前 3 次迭代中，SAT 求解器找到了赋值，但这些赋值立即被理论求解器拒绝。例如，在第1次迭代中，SAT 求解器为公式 F_B 找到了一个解 $x = 0 \wedge y = 1 \wedge z = 1$，但理论求解器拒绝了它，因为 $(a < b)$ 和 $(a = b)$ 无法同时成立。这种来回过程又持续了两次迭代，最终在第4次迭代中找到了一个一致的解。

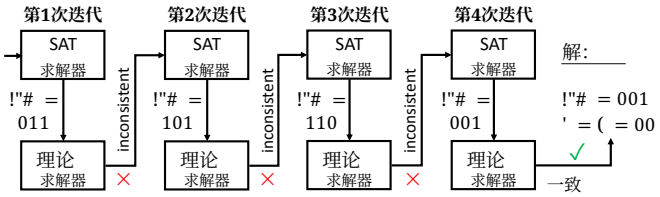


图 1. 通过经典惰性方法进行 SMT 求解

可以看到，这种来回过程的每次迭代都只会检查一个布尔解与理论是否一致。如果搜索空间很大，这种方法就难以扩展。事实上，惰性方法有一个在线 版本，该版本采用启发式方法，从而提高效率。不过，在线版本并未降低理论时间复杂度。

近年来，量子技术被广泛应用于许多领域，利用量子系统中叠加和纠缠的特性来解决传统上难以处理的问题。Grover 算法 [12], 是著名的量子算法之一，可在庞大的搜索空间中搜索目标对象。Grover 算法包含两个基本组成部分：(1) 预言机，以及 (2) 扩散算子。简而言之，预言机回答搜索空间中的某个对象是否为目标对象这一“是/否”问题，而扩散算子则试图提高或最大化测量到目标对象的概率。第 II 节简要介绍了 Grover 算法的细节。

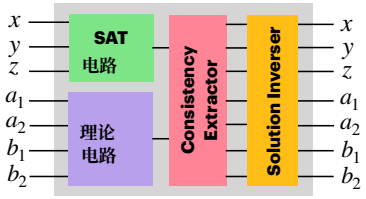
要将 Grover 算法用于搜索问题，关键是提供预言机。只要预言机能够在搜索空间中正确识别目标，标准且独立于搜索问题的扩散算子就能帮助“提取”这些目标。在本研究中，我们开发了一种基于 Grover 算法的量子 SMT 求解器。具体而言，给定一个 SMT 公式，我们开发了一种方法来生成 Grover 算法搜索该 SMT 公式的解所需的预言机。

我们再次以公式 F 为例。假设两个变量 a 和 b各为 2 位长，分别用二进制字符串 a_1a_2 和 b_1b_2表示。结合抽象的布尔公式 F_B，我们可以用七位来表示搜索空间中的每个元素$|v\rangle$，表示为列向量 $|x,\ y,\ z,\ a_1,\ a_2,\ b_1,\ b_2\rangle$。要使 $|v\rangle$ 成为公式 F的解，必须满足一些要求。首先，在布尔域中，x、 y、 z 必须满足以下条件:

$$F_B(x, y, z) = (x \vee y \vee z) \wedge (\neg x \vee \neg y \vee \neg z) = 1 \qquad (1)$$

其次，在位向量理论域中，a_1、 a_2、 b_1、 b_2 需要与它们的布尔抽象 x、 y、 z保持一致。因此，它们必须满足以下三个条件:

$$(x = 1 \iff a_1a_2 > b_1b_2) \vee (x = 0 \iff a_1a_2 \not> b_1b_2) \qquad (2)$$
$$(y = 1 \iff a_1a_2 < b_1b_2) \vee (y = 0 \iff a_1a_2 \not< b_1b_2) \qquad (3)$$
$$(z = 1 \iff a_1a_2 = b_1b_2) \vee (z = 0 \iff a_1a_2 \neq b_1b_2) \qquad (4)$$



(a) 我们的预言机 Ψ

可满足性模理论结果：16 个解

xyz	a_1a_2	b_1b_2
001	00	00
	01	01
	10	10
	11	11
010	00	01
	00,01	10
	00,01,10	11
100	01	00
	10	00,01
	11	00,01,10

(b) 解

图 2. 我们的预言机结构 Ψ

接下来是有趣且关键的部分。如果我们能够构造一个预言机 Ψ，帮助我们同时处理这四个条件，那么扩散算子就可以继续为我们提取解。也就是说，我们的预言机 Ψ 会执行以下操作：

$$\Psi(|v\rangle) = \begin{cases} -1 \cdot |v\rangle & \text{if} \quad (1) \wedge (2) \wedge (3) \wedge (4) \\ |v\rangle & \text{otherwise} \end{cases}$$

如果输入 $|v\rangle$ 是 F的一个解，我们的预言机就会为它添加一个“-1”相位；否则， $|v\rangle$ 保持不变。由于输入 $|v\rangle$ 可以处于叠加态，表示每一种可能的输入，我们的预言机能够一次性找出 F 的所有解。随后，扩散算子会识别带有“-1”相位的输入，并尝试提高／最大化测量到这些输入的概率。图 2 (b) 显示了公式 F的全部 16 个解，我们的预言机能够一次性从 128 个输入中找出所有解。

图 2 (a) 展示了我们的预言机设计结构，并概述了我们的贡献。我们的预言机包含四个组件：

1) **SAT 电路** （参见第 III-A 节）确定布尔域中的解，即本例中的方程 (1)。2) **理论电路** （参见第 III-B 节）根据不同输入，确定理论域中各谓词（例如本例中的 $a < b$、 $a > b$、 $a = b$ ）的真值。3) **一致性提取器** （参见第 III-C 节）找出在布尔域和理论域中都一致的解，即本例中的 (1) $\wedge$ (2) $\wedge$ (3) $\wedge$ (4)。4) **解反转器** （参见第 III-D 节）通过为这些解添加“-1”相位，将 SMT 公式的解反转，以供扩散算子进一步处理。

我们还证明了各组件设计的正确性。本文其余部分安排如下。第 II 节回顾量子计算的预备概念。第 III 节介绍我们提出的、基于 Grover 算法的量子 SMT 求解器，用于求解位向量理论公式。第 IV 节给出我们方法的评估结果。第 V 节讨论相关工作。第 VI 节讨论结论及未来工作。

II. 预备知识

我们假设读者具备量子计算的基本概念，例如张量积运算、内积运算、外积运算，以及 X、Z、H、CCNOT 等基本量子门。我们使用右矢记号 $|\cdot\rangle$ 表示代表量子系统状态的（列）向量，并使用左矢记号 $\langle\cdot|$ 表示其共轭转置。给定两个向量 $|v_1\rangle$ 和 $|v_2\rangle$，我们用 $\langle v_1|v_2\rangle$ 表示它们的内积，用 $|v_1\rangle\langle v_2|$ 表示它们的外积，用 $|v_1\rangle \otimes |v_2\rangle$ 表示它们的张量积。为简单起见，我们可以将 $|v_1\rangle \otimes |v_2\rangle$ 写作 $|v_1,\ v_2\rangle$，甚至写作 $|v_1 v_2\rangle$。

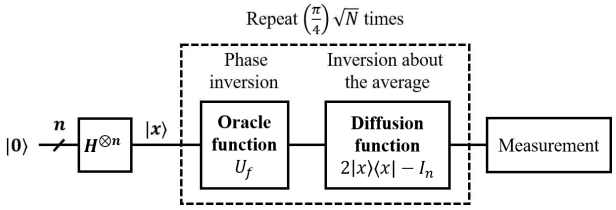


图 3. Grover 算法

A. Grover 算法

Grover 算法 [12] 是最著名的量子算法之一。它用于解决搜索问题，即从含有 N 个元素的无序数据库中找出一个目标元素。得益于量子系统并行计算的特性，Grover 算法只需执行 $O(\sqrt{N})$ 次操作即可找到目标元素，相较于需要执行 $O(N)$ 次操作的经典方法，速度提升了二次方。Grover 算法广泛应用于许多领域，例如密码学、模式匹配等。

Grover 算法的整体结构如图 3 所示。它的两个主要操作是相位反转 和关于平均值的反演，分别由预言机和扩散算子执行。首先，将输入置于叠加态（$|x\rangle$），以便一次评估数据库中的所有元素。接下来，预言机函数 U_f 考虑所有可能的输入，并通过应用相位反转来标记目标元素，即 $U_f|x\rangle = (-1)^{f(x)}|x\rangle$，其中目标元素满足 $f(x) = 1$，其他元素则满足 $f(x) = 0$。预言机与具体问题相关，而扩散算子则不然。因此，设计正确的预言机是应用 Grover 算法的关键。目标元素被标记后，扩散算子会执行关于平均值的反演 操作，以提高目标元素的概率，从而可以通过测量获得结果。为了使测得目标元素的概率达到最优，这两个操作（称为一次 Grover 迭代）需要重复执行（$\pi/4$）$\sqrt{N}$ 次。

—

Grover 算法也可用于存在多个目标元素的问题。在这种情况下，所需的迭代次数变为 $(\pi/4)\sqrt{N/M}$，其中 M 是目标元素的数量。此外，由于该算法的固有特性 [23]，只有当目标元素的数量少于非目标元素的数量（即 $M/N < 50\%$）时，才能测得正确结果。由于搜索前通常不知道目标元素的数量，因此有几种方法可以解决这个问题。最常见的方法是在使用 Grover 算法之前，先应用量子计数 [7] 来获得目标元素的（近似）数量。得知 M/N的比例后，如果该比例超过 50%，可以通过添加 N 个非目标元素将搜索空间扩大一倍，这样目标元素的数量就始终少于搜索空间的一半。另一种方法是应用 Boyer 等人提出的高级算法 [6]。

B. SAT、SMT 与定宽位向量理论

布尔公式由布尔变量之间的逻辑运算符构成，例如否定（¬）、合取（∧）和析取（∨）。给定一个布尔公式，布尔可满足性（SAT）问题要判断是否存在一种布尔变量的赋值，使该公式成立。

可满足性模理论（SMT）是 SAT 的扩展，旨在判断一个数学公式是否可满足。数学公式由原子（谓词）构成，并通过

$$E \simeq \tilde{a} \mid \mathcal{C} \mid E_1 \odot E_2 \text{ 其中} \odot \text{ 是算术运算符}$$
$$atom \simeq E_1 \rhd E_2 \text{ 其中} \rhd \in \{<, >, =, \geq, \leq, \neq\}$$

图4. $\mathcal{BV}$ 原子的语法

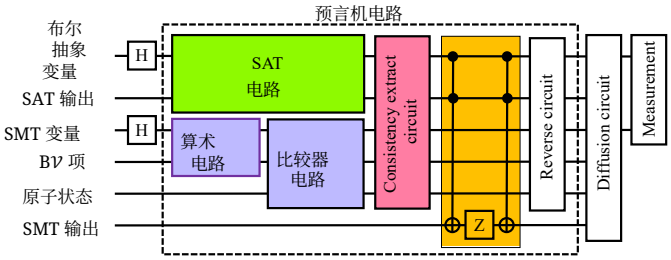


图5. 我们的 $\mathcal{BV}$ SMT 求解器的量子电路

由布尔逻辑运算符组成（例如，第 I 节中的公式 F）。原子的类型取决于数学公式中使用的理论。

本文关注无量词定宽位向量理论（参见 [19]第 4.2.5 节），简称为 $\mathcal{BV}$。$\mathcal{BV}$ 原子的语法见图4。表达式E 可以是一个具有 n 位的变量 $\tilde{a}$、一个常数 $\mathcal{C}$，或两个表达式 E_1 和 E_2之间进行算术运算的结果。请注意，一旦确定了数据宽度（n 位），所有表达式的宽度便固定不变。一个原子由两个表达式和一个比较运算符 $\rhd$构成，其中 $\rhd \in \{<, >, =, \geq, \leq, \neq\}$。算术运算符包括字拼接、模加、模乘、按位运算、移位运算等。

III. 方法论

本节介绍一种基于 Grover 算法、用于 $\mathcal{BV}$ 理论的量子 SMT 求解器。图 5 展示了其框图，与图 2 (a) 中的整体结构相呼应。如第一节所述，预言机是标记解的关键组件，使扩散算子能够确定应提高哪些元素的概率，以便测量时更容易得到它们。由于扩散算子是标准组件，且与搜索问题无关，因此不再赘述。下文将重点介绍如何构造预言机。

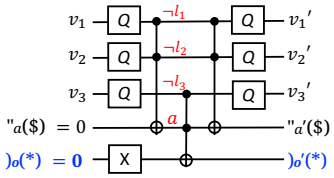
A. SAT 电路

Fernandes 等人 [10] 展示了一个为 3-SAT 问题构造预言机电路的示例，并基于 Grover 算法求解了该问题。然而，他们并未提供构造预言机电路的系统方法。本节提出一种方法，可为任意 3-SAT 公式以构造性方式生成预言机电路，并证明其正确性。考虑以下用于合取范式（CNF）3-SAT 公式的语法：

$$\begin{aligned} F &\simeq C \mid F_1 \wedge F_2 \\ C &\simeq l_1 \vee l_2 \vee l_3 \\ l &\simeq v \mid \neg v \mid 0 \end{aligned}$$

图 6 展示了如何为子句 $C: l_1 \vee l_2 \vee l_3$ 构造量子电路。请注意，Q 门取决于每个文字 l_i。如果 l_i 是负文字 $\neg v_i$，Q 将是 I 门，也就是恒等门；否则，Q 将是 X 门，也称为非门。量子比特 $q_a(C)$ 是用于内部计算的辅助位[1]，而 $q_o(C)$ 是

[1]符号 $q_a(C)$ 并不表示函数应用，只是表示 q_a 是子句 C 的辅助位。同样，$q_o(C)$ 表示输出位
子句 C 的，$q_o(F)$ 表示公式 F 的输出位。



Q: { X, 如果 l_i 是 v_i 或0；I, 如果 l_i 是 $\neg v_i$

图 6. 子句的量子电路 $C: l_1 \vee l_2 \vee l_3$

C 真值的输出位。定理 1 证明，子句 C 的量子电路构造是正确的。

定理 *1*：**[子句正确性]** (1) $q_o'(C) = 1 \iff$ 子句 C 为真，(2) $q_a'(C) = 0$，且 (3) $v_i' = v_i$ 对所有 $i \in \{1, 2, 3\}$均成立。

证明 *1*：给定子句 $C: l_1 \vee l_2 \vee l_3$，由于若 l_i 是负文字 $\neg v_i$，Q 将是 I 门；否则，Q 将是 X 门，因此我们有 $Q(v_i) = \neg l_i$，如图 6 中红色标记所示。令 a 为对其应用第一个 CCNOT门后 $q_a(C)$ 的值。

证明条件 (1)：$q_o'(C) = 0 \Leftrightarrow (\neg l_3 = 1) \wedge (a = 1) \iff (\neg l_3 = 1) \wedge (\neg l_1 = 1) \wedge (\neg l_2 = 1)$。如果对两边取否定，则有 $\neg(q_o'(C) = 0) \Leftrightarrow \neg((\neg l_1 = 1) \wedge (\neg l_2 = 1) \wedge (\neg l_3 = 1))$。因此，$q_o'(C) = 1 \Leftrightarrow \neg(\neg l_1 = 1) \vee \neg(\neg l_2 = 1) \vee \neg(\neg l_3 = 1)$。也就是说，$q_o'(C) = 1 \Leftrightarrow (l_1 = 1) \vee (l_2 = 1) \vee (l_3 = 1)$。

证明条件 (2)：$q_a'(C) = (\neg l_1 \wedge \neg l_2) \oplus a$。由于 a 是在 $q_a(C)$ 上应用 CCNOT门得到的，其中 $\neg l_1$ 和 $\neg l_2$ 是控制位，因此我们有 $q_a'(C) = (\neg l_1 \wedge \neg l_2) \oplus ((\neg l_1 \wedge \neg l_2) \oplus 0) = (\neg l_1 \wedge \neg l_2) \oplus (\neg l_1 \wedge \neg l_2) = 0$。

证明条件 (3)：$v_i' = Q(\neg l_i) = Q(Q(v_i)) = v_i$，因为 $QQ = I$，而 Q 要么是 X 门，要么是 I 门。■

图7展示了如何为公式 F 构造量子电路：$F_1 \wedge F_2$。需要先构造 F_1 和 F_2 的量子电路，然后用 CCNOT门将它们合取。量子比特 $q_o(F)$ 是公式 F 的真值输出位。定理2证明了公式 F 的量子电路构造是正确的。

定理*2*：**[公式正确性]** (1) $q_o'(F) = 1 \iff$ 公式 F 为真，(2) $q_a'(F) = 0$，以及 (3) $v_i' = v_i$ 对所有 $i \in \{1, 2, \ldots, n\}$。

证明 *2*：我们通过对生成任意公式 F 的语法进行结构归纳法来证明此定理。基本情形，即 F 为一个子句 C 时，已在定理 1 中得到证明。

归纳假设：设 F_1 和 F_2 是两个满足以下三个条件的公式：(a) $q_o'(F_1) = 1 \iff$ 公式 F_1 为真，且 $q_o'(F_2) = 1 \iff$ 公式 F_2 为真。(b) $q_a'(F_1) = 0$ 且 $q_a'(F_2) = 0$。(c) $v_i' = v_i$ 对 $i \in \{1, 2, \ldots, n\}$。

考虑归纳步骤，F 的电路：$F_1 \wedge F_2$ 是基于 F_1 和 F_2构造的，如图7所示。

证明条件 (1)：由于 CCNOT门，$q_o'(F) = 1 \Leftrightarrow ((q_o'(F_1) = 1) \wedge (q_o'(F_2) = 1)) \oplus 0 \Leftrightarrow (q_o'(F_1) = 1) \wedge (q_o'(F_2) = 1)$。根据归纳假设 (b)，我们可以得出

q_o' F $= 1$ 0)为真，且为真为真。
$\iff$ F_1 F_2 $\iff$ F

证明条件 (2)：根据归纳假设 (b)，$q_a'(F) = q_a'(F_2) = 0$。

证明条件 (3)：由于 F的 v_i'等于 F_2的 v_i'，根据归纳假设 (c)，对于所有 $i \in \{1, 2, \ldots, n\}$，$v_i' = v_i$。■

B. 理论电路

现在，我们说明如何为由算术运算和比较运算组成的原子构造理论电路。考虑图4所示的任意原子的语法规则。表达式可以是变量 $\tilde{a}$、常数 $\mathcal{C}$，也可以是两个表达式 E_1 和 E_2 之间进行算术运算的结果。构造变量 $\tilde{a}$ 或常数 $\mathcal{C}$ 的电路很简单，因此此处略去。其余情况是 $\tilde{a} \odot \tilde{b}$。这里，我们不列出

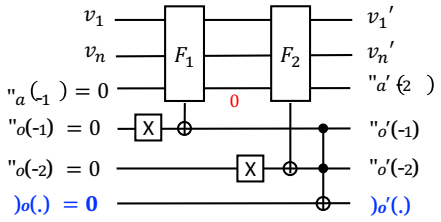


图7. 公式的量子电路构造 F



(a) 算术电路　　(b) 比较器电路

图 8. 理论电路

所有算术运算，因为种类繁多。它们既可以基于基本量子门构造，也可以采用相关工作中提出的方法（参见第 V 节）。相反，为便于说明，我们将算术运算的电路抽象为图 8 (a) 所示的一般形式。针对不同的算术运算，可以自底向上地构造出相应的最终电路。

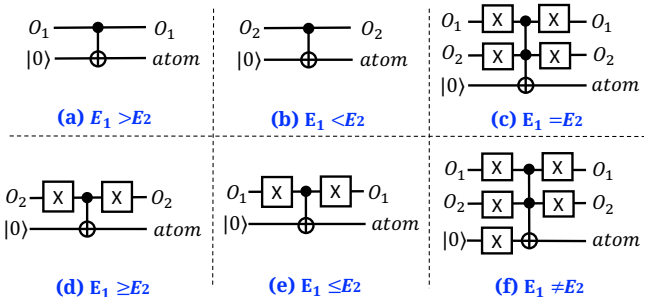
对于形如 $E_1 \triangleright E_2$ 的每个原子式，我们采用比较器 [18] 来比较 E_1 和 E_2。比较器的整体结构如图 8 (b) 所示。当然，算术电路的输出位 $E_1 \odot E_2$ 将作为比较器电路的输入。比较器的两个输出位 O_1 和 O_2 表示 E_1 和 E_2 之间的关系，如下所示。注意，在比较器设计 [18] 中，不存在 (1，1) 这种情况。

$$(O_1, O_2) = \begin{cases} (0,1) & \text{if} \quad E_1 < E_2 \\ (1,0) & \text{if} \quad E_1 > E_2 \\ (0,0) & \text{if} \quad E_1 = E_2 \end{cases}$$

根据两个输出位 O_1 和 O_2，可以为六种不同情况中的每一种构造相应的原子，如图 9 (a)–(f) 所示。定理 3 证明了我们为原子构造电路的正确性。

定理 *3*： **[原子正确性]** 对于每个原子 $E_1 \triangleright E_2$ 及其对应的 $atom$ 位，我们有 $atom = 1 \iff (E_1 \triangleright E_2) = 1$。

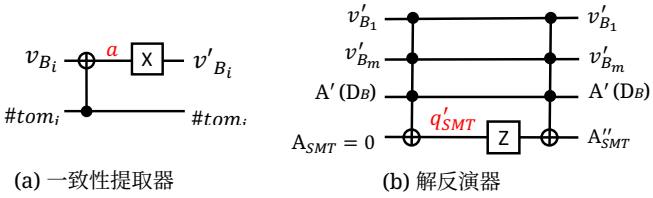
证明 *3*： 根据基本量子门的真值表，逐一检查每种情况下的 $atom$输出，即可轻松证明。由于篇幅所限，此处省略证明。■



(a) $E_1 > E_2$　(b) $E_1 < E_2$　(c) $E_1 = E_2$

(d) $E_1 \geq E_2$　(e) $E_1 \leq E_2$　(f) $E_1 \neq E_2$

图 9. 原子的量子电路构造



(a) 一致性提取器　　(b) 解反演器

图 10. 一致性提取器和解反演器

C. 一致性提取器

一致性提取器 的任务是提取在布尔域和位向量域中都一致的赋值。也就是说，给定一个 $atom_i$ 及其布尔抽象变量 v_{B_i}，我们希望确保 $v'_{B_i} = 1$ 当且仅当 $atom_i$ 和 v_{B_i} 在逻辑上等价。

如图 10 (a) 所示，一致性提取器由一个 CNOT 门和一个 X 门组成。输入 $atom_i$ 作为 CNOT 门的控制位，而另一个输入 v_{B_i} 作为目标位，随后通过一个 X 门翻转其结果。通过这一设计，当且仅当 $atom_i$ 和 v_{B_i} 具有相同的真值时，输出量子比特 v'_{B_i} 才为 1。定理 4 证明了我们用于一致性提取器的量子电路的正确性。

定理 *4*： **[一致性提取器的正确性]** $(v'_{Bi} = 1) \iff (v_{B_i} \equiv atom_i)$.

证明 *4*： 令 a 为应用 CNOT 门后得到的 v_{Bi} 结果，如图 10 中红色标记所示。

$$\begin{aligned} v'_{Bi} = 1 \quad &\Leftrightarrow \quad a = 0 \quad \Leftrightarrow \quad (v_{Bi} \oplus atom_i) = 0 \\ &\Leftrightarrow \quad (v_{Bi} = 0 \wedge atom_i = 0) \vee (v_{Bi} = 1 \wedge atom_i = 1) \\ &\Leftrightarrow \quad v_{B_i} \equiv atom_i \end{aligned}$$ ■

D. 解反演器

解反演器 是预言机的关键组件。它通过反演解来标记 SMT 公式的解，即为其赋予“−1”相位，使扩散算子能够识别哪些元素需要提高/最大化其被测得的概率。

如图 10 (b) 所示，解反演器的电路由两个 $(m+1)$-CNOT 门和一个 Z 门组成，其中 m 是布尔抽象变量的数量。定理 5 证明了解反演器的正确性。

定理 *5*： **[解反演器的正确性]** (1) $q'_{\text{SMT}} = 1$ 当且仅当 $q'_o(F_B) = 1$ 且 $v_{B_i} \equiv atom_i$, $\forall i \in \{1, 2, \ldots, m\}$。(2) 所有解都加上一个“−1”相位。

证明 *5*： 令 q'_{SMT} 表示应用第一个 $(m+1)$-CNOT 门后该 q_{SMT} 位的值，如图 10 (b) 中红色标记所示。由于 q_{SMT}（初始化为 0）是 $(m+1)$-CNOT 门的目标位，且 v'_{B_i} 是受控位之一，因此我们知道 $q'_{SMT} = 1 \Leftrightarrow (v'_{B_1} \wedge v'_{B_2} \wedge \ldots \wedge v'_{B_m} \wedge q'_o(F_B)) = 1$。根据定理 4，我们可以得出条件 (1) 成立。

为了证明条件 (2)，我们来考察量子电路的状态。$|v'_{B_1}, \ldots, v'_{B_m}, \ldots, q'_o(F_B)\ q'_{\text{SMT}}\rangle$ 表示应用第一个 $(m+1)$-CNOT 门后的量子态。由于 q'_{SMT} 的值可能为 0 或 1，系统空间 S 可以划分为两个互不相交的集合 S_0 和 S_1。也就是说，$S = S_0 \cup S_1$，其中 $S_0 = \{|v'_{B_1}, \ldots, v'_{B_m}, \ldots, q'_o(F_B)\ 0\rangle\}$，而 $S_1 = \{|v'_{B_1}, \ldots, v'_{B_m}, \ldots, q'_o(F_B)\ 1\rangle\}$。根据我们刚刚证明的条件 (1)，$S_1$ 恰好是 SMT 问题所有解的集合。之后，在 q'_{SMT} 位上施加一个 Z 门。由于 $Z(|0\rangle) = |0\rangle$ 且 $Z(|1\rangle) = -1|1\rangle$，Z 门会为 S_1 中的每个元素赋予“−1”相位，也就是说，所有解都会被加上“−1”相位。■

表 I 求解电路中包含的量子比特列表 $\mathcal{F}$

模块	量子比特名称	数量
SMT	布尔抽象变量	3
	SMT 变量	2*2
	辅助量子比特	5
	SMT 输出	1
	加法量子比特	1
SAT	SAT 输出	1
	额外量子比特	2
加法器	加法器输出	3
按位异或	按位异或输出	2
比较器 1 和 2	比较器输出	2*2
	比较器内部输出	(2-1)*2*2
	比较器辅助量子比特	1*2

E. 逆向电路

对解进行反演后，预言机函数的最后一部分是逆电路，它由与上述四个组件相对应的逆电路构成。逆电路的目的是将量子比特恢复到其初始状态，这符合量子计算的可逆性。此外，Grover 算法可能需要经过多次迭代来放大解的概率。辅助比特需要恢复原状，以便在后续迭代中使用。

IV. 评估

在本节中，我们展示用于求解 $\mathcal{BV}$ 可满足性模理论公式 $\mathcal{F}$的量子电路设计，其布尔抽象公式为

$$\mathcal{F}_B : (x \vee y \vee z) \wedge (x \vee \neg y \vee z)$$

其中原子 x : $(a+b < a \oplus b)$、 y : $(a+b > a \oplus b)$ 和 z : $(a+b = 1)$，变量 a、 b、 c 均为 2 位长；‘+’表示模加运算，‘$\oplus$’表示异或运算。

图 11 (a) 展示了公式 $\mathcal{F}$ 的量子 SMT 求解器框图，其中仅显示了重要的量子比特。每个模块的内部量子比特均省略。尽管图中将 SAT 和理论（算术+ 比较器）电路按顺序绘制，但在实际实现中，由于二者之间没有依赖关系，它们可以并行运行。主要输入是三个布尔抽象变量 x、 y、 z 以及 SMT 变量 a、 b。初始时，Hadamard 门将它们置于叠加态。为求解公式 $\mathcal{F}$，需要两个比较器。比较器一负责比较 $(a + b)$ 和 $(a \oplus b)$ 之间的关系，而比较器二则负责比较 $(a + b)$ 与常数 1。

该电路在 Qiskit [3] 中实现并进行了模拟。整个电路需要 32 个量子比特，这已经达到 Qiskit 支持的量子比特数量上限。所需量子比特的具体构成列于表 I。图 11 (b) 所示的模拟结果，是通过将五次 Grover 迭代作为一次测量，并重复进行 1,024 次测量，获得 1,024 次测量结果得到的。有人可能会想知道，我们如何得出执行 Grover 算法所需的迭代次数（即 $\frac{\pi}{4}\sqrt{N/M}$，参见第 II 节）。实际上，可以通过量子计数 [7] 得到这个数值。然而，Qiskit 支持的 32 个量子比特不足以对此电路执行量子计数。因此，我们从一次迭代开始逐步增加次数，直到测量的概率分布开始变差。在本实验中，我们得到的转折点是五次迭代。实际上，我们通过枚举搜索空间和解，手动计算了 $\frac{\pi}{4}\sqrt{N/M}$ 的值。我们发现该值与五这个次数一致。

表 II 通过量子电路得到的解

输出位串	计数	赋值		
		(x, y, z)	a	b
0010100	174	(0, 0, 1)	01	00
0011110	158	(0, 0, 1)	11	10
0010001	183	(0, 0, 1)	00	01
1001101	156	(1, 0, 0)	11	01
0011011	164	(0, 0, 1)	10	11
1000111	182	(1, 0, 0)	01	11

如图 11 (b) 所示，我们可以观察到六种比其他比特串概率更高的比特串。表 II 将这六种比特串还原为五个主要变量 x, y, z, a, b 的赋值。它们恰好是公式 $\mathcal{F}$ 的解。“计数”列表示在 1,024 次测量中，该赋值被测得的次数。根据模拟结果，我们的电路测得解的概率为 99.32%（“计数”总和除以 1024）。此外，只需进行合理数量的测量，就有可能获得所有解。

V. 相关工作

A. SAT 电路

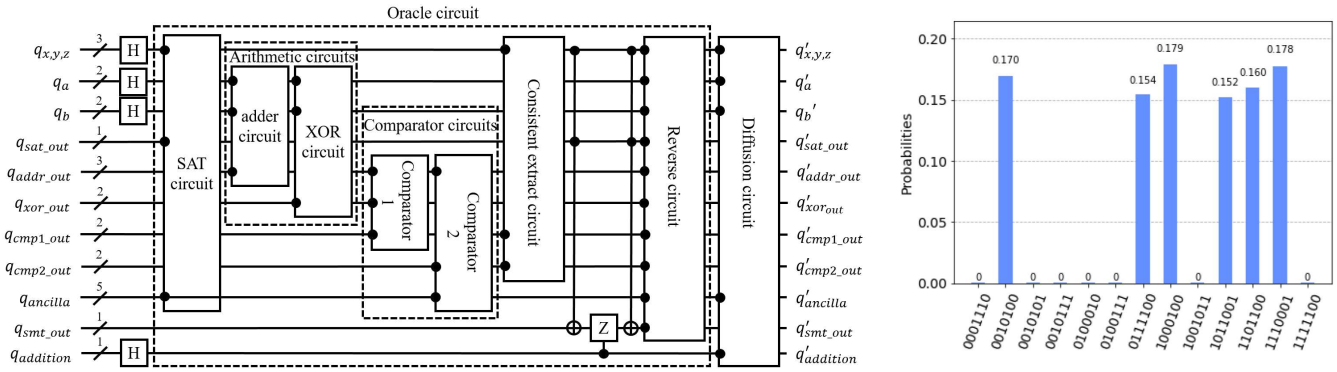
SAT 在广泛的应用领域中都很有用，但它也是一个著名的NP完全问题。许多研究都致力于提升求解SAT问题的性能，例如SAT求解器的硬件实现。借助量子系统中叠加的优势，可以利用量子电路加速SAT求解过程。Alberto等人 [16]提出了三种算法，包括量子Fredkin电路、量子寄存器机和量子P系统，用于求解SAT问题。通过将量子系统的叠加特性应用于输入，系统可以在一次评估中获得所有可能输入所对应的全部结果。然而，这些方法的共同问题在于SAT结果难以测量，因为当可满足赋值的数量远少于不可满足赋值的数量时，SAT结果出现的概率会非常低。尽管作者提出了非幺正算子，或采用混沌动力系统等其他方法 [17] 来提取SAT结果，但目前这些方法都难以实现。

解决测量问题的另一种方法是采用 Grover搜索算法。该算法通过放大目标元素的测量概率来查找数据库中的目标元素，因此，如果能在预言机函数中正确标记可满足赋值，它就适用于搜索这些赋值。Fernandes 等人 [10] 提出了基于 Grover 算法构建用于求解 3-SAT 的预言机电路的概念。

B. 量子算术与比较器电路

Chakrabarti 等人 [8] 提出了一种量子串行进位加法器，该加法器基于著名的 VBE加法器 [22] ，并减少了门级数量。他们提出的加法器重新组织了生成进位位的进位门，使部分门能够并行运算。另一方面，他们舍弃了 VBE加法器第二部分中的一系列求和门和进位门，并用 CNOT门替代这些门以生成求和结果。作者还提出了量子超前进位加法器的设计，但与串行进位加法器相比，它在量子比特用量和门级数量方面均无优势。我们的电路采用串行进位加法器执行模加运算。

Kotiyal 等人 [15] 提出了一种量子乘法器设计，重点在于减少辅助输入和垃圾输出，因为



(a) (b)

图 11. 求解公式 $\mathcal{F}$ 的量子电路及模拟结果

量子比特的使用量是量子电路设计的主要考量因素。他们提出的乘法器的优势在于，采用基于二叉树的设计并行处理部分积求和。此外，他们采用了 Takahashi 等人 [20] 提出的无需辅助量子比特和垃圾量子比特的加法器，以减少加法器所造成的开销。实现结果还表明，与此前的其他工作相比，他们的乘法器在辅助量子比特和垃圾量子比特的使用量方面分别提升了 60.34% 和 52.27%。

Kotiyal 等人 [14] 提出了一种量子双向桶形移位器，可执行四种移位运算，包括逻辑右移、逻辑左移、算术右移和算术左移。为了实现桶形移位器的主要组件——2选1多路复用器，他们采用 Fredkin 门（即受控交换门）进行实现，将控制量子比特设为选择信号，并将其中一个目标量子比特设为输出。他们还使用 CNOT 门处理信号扇出。与以往的工作相比，他们的移位器具有反转控制单元，可实现双向移位，尽管移位器的核心模块仅执行右移运算。

最后，一旦两个 $\mathcal{BV}$ 项准备就绪，就会使用量子比较器来确定原子的状态。Oliveira 等人 [18] 提出的量子比较器可以判断两个输入量子位串$\mathbf{a}$ 和$\mathbf{b}$之间的关系。与另一种基于减法的比较器 NKO 相比，他们的电路所需资源更少，且计算并行性更高。

六、结论

本文提出了一种基于 Grover 算法的 $\mathcal{BV}$ 理论量子 SMT 求解器。与传统方法相比，我们提出的方法不仅在理论上可实现二次加速，还能够找到所有解。由于其他理论的 SMT 问题求解也由两部分组成（即 SAT 和理论求解），我们提出的预言机构造具有通用性，可扩展至其他理论；这也是我们未来的工作方向。

参考文献

[1] Alif Ahmed、Farimah Farahmandi 和 Prabhat Mishra。基于 RTL 模型的符号与具体相结合测试进行定向测试生成。载于*2018 Design,Automation & Test in Europe Conference & Exhibition (DATE)*，第 1538–1543 页，2018年。[2] Elvira Albert、Shelly Grossman、Noam Rinetzky、Clara Rodr´ıguez-N´u˜nez、Albert Rubio 和 Mooly Sagiv。为智能合约模块化驾驭回调。《*ACM* 程序设计语言汇刊》，4(OOPSLA)，2020年11月。[3] Gadi Aleksandrowicz、Thomas Alexander、Panagiotis Barkoutsos 等。Qiskit：一个用于量子计算的开源框架，2019年1月。

[4] Leonardo Alt 和 Christian Reitwiessner。基于可满足性模理论的 Solidity 智能合约验证。载于 Tiziana Margaria 和 Bernhard Steffen 编，形式化方法、验证与确认的应用：工业实践，第 376–388 页，沙姆，2018年。施普林格国际出版社。[5] Guy Amir、Haoze Wu、Clark Barrett 和 Guy Katz。基于可满足性模理论的二值化神经网络验证方法。载于 Jan Friso Groote 和 Kim Guldstrand Larsen 编，系统构造与分析工具及算法，第 203–222 页，沙姆，2021年。施普林格国际出版社。[6] Michel Boyer、Gilles Brassard、Peter Høyer 和 Alain Tapp。量子搜索的紧确界。物理学进展，46(4-5)：493– 505，1998年1月。[7] Gilles Brassard、Peter Hoyer 和 Alain Tapp。量子计数。*arXiv*预印本，第 quant–ph/9805082 页，1998年5月。[8] A mlan Chakrabarti 和 Susmita Sur-Kolay。量子加法器电路的设计及其误差性能评估。载于*2008*年国际电子设计会议，第 1–6 页，2008年。[9] Nicole Fern、Ismail San 和 Kwang-Ting Tim Cheng。通过求解可满足性问题检测功能未指定电路中的硬件木马。载于*2017*年第*22*届亚洲及南太平洋设计自动化会议（*ASP-DAC*），第 598–504 页，2017年。[10] Diogo Fernandes、Carla Silva 和 Inˆes Dutra。使用 Grover 量子搜索算法求解布尔可满足性问题，第 2 部分。*XRDS*，26(2)：68–71，2019年11月。[11] Markus Grassl、Brandon Langenberg、Martin Roetteler 和 Rainer Steinwandt。将 Grover 算法应用于高级加密标准：量子资源估算。载于 Tsuyoshi Takagi 编，后量子密码学，第 29–43 页，沙姆，2016年。施普林格国际出版社。[12] Lov K. Grover。一种用于数据库搜索的快速量子力学算法。*arXiv*预印本，第 quant–ph/9605043 页，1996年5月。[13] Guy Katz、Clark Barrett、David Dill、Kyle Julian 和 Mykel Kochen- derfer。Reluplex：一种用于验证深度神经网络的高效 SMT 求解器。*arXiv*预印本，第 arXiv:1702.01135 页，2017年2月。[14] Saurabh Kotiyal、Himanshu Thapliyal 和 Nagarajan Ranganathan。可逆双向桶形移位器的设计。载于*2011*年第*11*届 *IEEE* 国际纳米技术会议，第 463–468 页，2011年。[15] Saurabh Kotiyal、Himanshu Thapliyal 和 Nagarajan Ranganathan。基于二叉树、优化辅助比特和垃圾比特的可逆量子乘法器电路。载于*2014*年第*27*届国际超大规模集成电路设计会议和*2014*年第*13*届国际嵌入式系统会议，第 545–550 页，2014年。[16] Alberto Leporati 和 Sara Felloni。求解 3-SAT 的三种“量子”算法。理论计算机科学，372(2)：218–241，2007年。膜计算。[17] Masanori Ohya 和 Igor V. Volovich。用于研究 NP 完全问题的新量子算法。数学物理学报告，52(1)：25–33，2003年。[18] David Sena Oliveira 和 Rubens Viana Ramos。量子比特串比较器：电路及应用。量子计算与计算，7(1)：17–26，2007年。[19] Roberto Sebastiani。惰性理论模可满足性。可满足性、布尔建模与计算杂志，3，2007年12月。

[20] Yasuhiro Takahashi、Seiichiro Tani 和 Noboru Kunihiro。量子加法电路与无界扇出。*Quantum Info. Comput.*，10(9)：872–890，2010年9月。[21] Hiroyuki Tezuka、Kouhei Nakaji、Takahiko Satoh 和 Naoki Yamamoto。重新审视 Grover 搜索：在图像模式匹配中的应用。*Phys. Rev. A*，105：032440，2022年3月。[22] Vlatko Vedral、Adriano Barenco 和 Artur Ekert。用于基本算术运算的量子网络。*Phys. Rev. A*，54：147–153，1996年7月。[23] Ahmed Younes。Grover 量子搜索算法的优势与不足。*arXiv*预印本，第 arXiv:0811.4481 页，2008年11月。