arXiv:2611.30887v1 [cs.CC] 23 Nov 2026

一个（17/7 − o(1)）n 二进制编码 3-SAT 的电路下界

Theodoros Yianni伦敦大学皇家霍洛威学院计算机科学系

Sahibzada Allahyar
smaa4@cantab.ac.uk

摘要

我们将针对一种特定的 3-SAT 二进制编码，在完整的双输入布尔基、深度和共享均不受限的情况下，将基本的 $n-1$ 电路下界加强到（17/7）$n - O$（$n \log\log n/\log n$）个门。对于每个整数 $w \geq 5$，我们使用 $n = 3m(w+1)$ 个比特，对含有恰好 $m = 2^w - 1$ 个子句、使用 m 个可用变量的 3-CNF公式进行编码。证明将布尔测试嵌入变量标识符中，同时保留 $n - o(n)$ 个自由位，并结合加权门消去与一个基于这些测试相对于 $\mathbb{F}_2$的完整代数次数所得的非线性门下界。我们为任意无环二输入电路提供有限不等式和渐近下界的 Lean 证明。

1 引言

我们以完整二进制公式描述的长度为基准，衡量 3-SAT 的电路复杂度。3-SAT 的 NP完全性 [1] 促使我们寻求此类下界，但若要保留首项常数，就必须控制编码长度。若一个 t位输入被归约为一个 t^2位公式描述，那么关于 t 的线性下界，相对于描述长度而言仅为平方根阶。我们将困难的布尔测试直接嵌入变量标识符中，从而保留 $n - o(n)$ 描述位的 n，并在完整二进制基下得到首项系数为 17/7 的下界。

主要结果。 对于整数 $w \geq 5$，令 $m = 2^w - 1$，并令 F_w 为如下 3-SAT 判定函数：公式恰含 m 个三文字子句，且至多有 m 个可用变量。我们使用一个 w位变量标识符和一个符号位来编码每个文字，因此得到 $n = 3m(w+1)$ 个输入位。在第 2节的编码中，标识符零会被拒绝；但允许出现未使用变量、重复文字、重复子句和永真式。记 $C_{B_2}(f)$ 为计算 f的无环电路所需的最少内部门数，其中门可实现至多有两个输入的任意布尔函数，且深度和共享均不受限制。

The定理 1.1 (主要结果)。 当输入长度为 $n = 3(2^w - 1)(w+1)$ 时，$w \to \infty$，

$$C_{B_2}(F_w) \geq \frac{17}{7} n - O\left(\frac{n \log\log n}{\log n}\right),$$

基于模素数加权和的限制给出 $C_{B_2}(F_w) \geq (17/7)n - O(n/\sqrt{\text{对数 } n})$。

定理 8.2 给出了有限不等式，并证明了这两个估计。该下界是相对于所有描述位衡量的，包括标识符和符号，并强化了这种编码下的初等 $n-1$下界。

相关工作。 门消除可追溯至 Schnorr [2] ，并构成了一系列针对特定布尔函数的线性下界的基础，其中包括 Stockmeyer 和 Paul 提出的 $5/2$系数 [3, 4]以及 3 （由 Blum 提出） [5]。在 Blum 的结果发表三十多年后，Find、Golovnev、Hirsch 和 Kulikov 超越了系数 3 [6]；随后 Li 和 Yang 得到了 $3.1n - o(n)$ [7]。Mishra 和 Santhanam 对某个属于 $4n - O(\log n)$ 的函数给出了 P [8],，但要将这样的下界转移到 F_w ，就必须同时控制归约规模和输出长度。

Lachish and Raz 引入了强二依赖性：在固定了许多其他输入后，通过固定一对输入得到的四个函数仍保持彼此不同；他们利用这一性质证明了在排除异或及其取反的基上的下界 [9]。Zwick 的工作研究了受限基上的扇出 [10], ，而加权门消去则分别计算不同门类型的成本 [11]。Kojevnikov 和 Kulikov 将加权消元与非线性门的代数次数界相结合 [12,第 3]节；我们的门数计算采用了这一组合，并使用了两级输入抵扣。

证明策略。 该嵌入使用包含同一负文字三个副本的子句，迫使选定的变量为假。由于其余子句只包含正文字，将每个未受约束变量设为真，当且仅当每个子句都包含一个未被强制设为假的变量时，才能满足这些子句。因而，自由标识符位分别输入布尔测试，以判断该标识符是否命名了一个未受约束变量。适当选择每个标识符所用自由位的数量，可以保留$n - o(n)$ 比特；传递引理还会计算随固定比特一同移除的门（第 3–4节）。

我们选取满足两个性质的布尔测试来支撑门数下界。只要仍有足够多的自由比特，任意一对自由比特的四种赋值都会给出关于其余自由比特的四个不同函数，因此在固定更多输入时，门消除仍可继续。这些测试还具有满代数次数，即输入数量所允许的最大次数，从而迫使电路使用额外的非线性门。我们通过计数论证和加权模构造（第 5 节）得到这些测试。

门数计算为奇偶门（异或及其取反）赋予权重 7，为非线性门赋予权重 4，然后为每个输入最多减去两点信用。若某个输入唯一的后继是非线性门，该输入便获得一点信用；若该门唯一的后继也为非线性门，则再获得一点信用。在每个消去步骤中，都可以固定一个输入，使这一量至少减少 14；在紧确情形下，被移除的门贡献 12 个单位，新增的两点信用则贡献另外 2 个单位。消去之前，嵌入的函数在其 L 个自由输入上具有满次数，因此 Schnorr 的次数界迫使其至少包含 $L - 1$ 个非线性门 [13]。将这些门的权重从 4 提高到 7，可额外增加 $3L - 3$ 个单位，同时使每个门的权重都达到 7。将每次减少的 14 个单位相加，并加入这一次数界，便得到系数 $17/7$；消去停止时，每个块中剩余输入带来的低阶损失也计入其中。第 6–7 节确立局部记账方法，第 8 节将其求和，并把此下界转移到完整的 SAT 描述上。

形式化验证。 归档于 Zenodo 的 Lean 形式化 [14], 验证了任意无环二输入电路的有限界和两个渐近估计。它将带有共享前驱的无环电路图与用于消元的有序表示联系起来。第8.1节介绍论文与代码的对应关系、参数假设和可复现性检查。

2 编码与电路模型

全文中，$\{0,1\} = \{0,1\}$ 以及所有对数均以 2 为底。

定义 2.1 （3-SAT 的二进制编码）。 固定一个整数 $w \geq 5$ 并设 $m = 2^w - 1$。一个公式恰好包含 m 个关于可用变量 $X_1, \ldots, X_m$的有序子句。每个子句按文字顺序编码为三个连续的文字字段。一个字段由标识符位$b_0, \ldots, b_{w-1}$后接一个符号位 s组成，标识符为 $v = \sum_{j=0}^{w-1} 2^j b_j$。对于 $1 \leq v \leq m$，该字段

表示当 $s=0$ 时为 X_v，当 $s=1$时为 $\neg X_v$；标识符零无效。将子句记录串接起来后得到 $n=3m(w+1)$ 比特。变量可以缺省，重复文字、重复子句和永真式均允许。

总布尔函数 $F_w:\{0,1\}^n\to\{0,1\}$ 若任一标识符无效，则函数值为零；否则，当且仅当编码公式可满足时，函数值为一。

定义 2.2（电路模型与复杂度）。 A B_2 电路是一个有限的无环网络，具有带标签的主输入和一个指定输出。每个门计算至多两个前驱值的任意布尔函数；一个前驱可以同时提供两个参数。深度和共享均不受限制，不同输入长度下的电路可以独立选取。大小 $|C|$ 是内部门的数量，包括一元门和常量门；输入和连线不计入大小。电路复杂度 $C_{B_2}(f)$是计算 f并在每个输入上都正确的 B_2 电路的最小大小。

无环性使我们能够按照前驱在前的顺序排列各门；我们利用这一顺序在限制下简化电路。

定义 2.3（依赖与限制）。 若存在两个仅在该输入上不同的赋值使输出不同，则该输入是本质的 。常值限制 ρ 将指定输入位固定为指定值。在其余输入上得到的函数称为余因子 $f|_\rho$。固定一对比特可得到四个余因子，其中一些可能相同。

引理 2.4（基本大小界）： 一个具有 $N\geq 1$ 个关键输入的 B_2 电路至少有 $N-1$ 个门。

证明。 删除所有没有通向输出的顶点，但保留每个关键输入。若剩余电路具有 $a\geq N$ 个输入顶点和 s 个门，则其底层无向图是连通的，并且至少有 $a+s-1$ 条边。进入各门的连线至多有 $2s$ 条，因此 $a+s-1\leq 2s$，从而 $s\geq N-1$。删除操作不会增加门数。 □

3 将布尔测试嵌入公式

为了使自由标识符位计算出布尔测试的相互独立副本，我们使用固定的辅助子句强制选定变量为假。这样，仅当每个剩余的正子句都包含一个强制集合之外的变量时，该子句才恰好可以满足。对于 $a\in\{0,1\}^r$，我们还按照定义 a 中的比特顺序，将其无符号整数值记作 2.1。

引理 3.1（任意块的稀疏辅助限制）。 设 $1\leq r\leq w-1$，且令$g:\{0,1\}^r\to\{0,1\}$ 为任意布尔函数。令 $M=m-|g^{-1}(0)|$，并假设 $M\geq 1$。存在一个限制，恰好固定 $n-3Mr$ 个 F_w 的比特，其余因子为

$$G=\bigwedge_{c=1}^{M}\left(g(x_{c,1})\vee g(x_{c,2})\vee g(x_{c,3})\right).$$

这里，每个 $x_{c,\,j}\in\{0,1\}^r$ 都是一个独立块的自由输入位，它们的总数为 $L=3Mr$。

证明。 当 $g(a)=0$ 时，称标识符 $v=2^{w-1}+a$ 为禁用标识符。对于每个禁用的 v，插入固定子句 $(\neg X_v\vee\neg X_v\vee\neg X_v)$。这将强制 $X_v=0$，每个 $|g^{-1}(0)|$ 禁用标识符各使用一条记录。

将剩余的 M 条记录用作正子句，并将每个符号位设为零。在每个字段中，将最高位标识符位设为一，并将位置 $r,\dots,w-2$ 设为零，同时保留最低的 r 位自由。范围 $r\leq w-1$ 保证这些选择彼此一致。自由位恰好有 $3Mr$ 个，因此恰好固定了 $n-3Mr$ 个比特。

每个自由标识符都介于 2^{w-1} 和 $2^{w-1}+2^r-1\leq m$ 之间，因此都不为零，也没有超出范围。如果某个正子句含有三个禁用标识符，那么固定子句会迫使它为假。如果每个

正子句都包含一个非禁用标识符，那么将每个未受约束变量设为真、每个禁用变量设为假，就能得到一个满足所有子句的赋值。在自由域中，当且仅当某个标识符的低位使 g 等于一时，该标识符才不是禁用标识符。因此，可满足性条件就是所显示的函数 G。 □

一个小例子。 取 $w = 5$， $r = 2$ 和 $g(a_0, a_1) = a_0 \vee a_1$。四个可能的标识符16、17、18、19中，只有 16 是禁用的，因此一个子句便能强制 $X_{16} = 0$。其余 30 个子句都使用各含两个自由标识符位的正文字。当且仅当每个子句都包含一个不等于 16的标识符时，它们才同时可满足。第 5 节构造了在施加限制后仍保留输入依赖性的测试，以满足下界所需条件。

为了统计固定这些比特后移除的门数，我们首先证明每个描述位都会影响答案。

引理 3.2 （每个编码位的本质性）。 定义 *2.1* 中的每一位对于 F_w都是本质的。

证明。 任取一条子句记录及其任意一个字段。将所有其他未使用的记录都填为重言式 ($X_1 \vee \neg X_1 \vee X_1$)。假设 $w \geq 5$ 给出 $m \geq 31$，因此下面的附加记录可用。

对于符号位，令选定的文字最初为 X_2 ，其两个伴随文字为 X_1。在另外两条记录中，使用负重复文字子句强制设为 $X_1 = X_2 = 0$ 。此时选定子句为假，因此公式不可满足。仅翻转选定的符号位会将 X_2 变为 $\neg X_2$，从而使公式可满足。

对于标识符位位置 $j \in \{0, \ldots, w-1\}$，将选定记录的三个文字最初全部设为正 X_m。在另一条记录中，强制设为 $X_m = 0$，使公式不可满足。 $m = 2^w - 1$ 的所有位均为 1，因此翻转选定位后得到标识符 $m - 2^j$，该标识符位于$\{1, \ldots, m-1\}$中。现在设置 $X_m = 0$ 和 $X_{m-2^j} = 1$ 即可满足公式。每个见证仅改变选定的编码位，从而证明其本质性。 □

引理 2.4 和 3.2 给出了下界 $n - 1$。接下来，我们统计通过固定关键输入而移除的门，以及剩余函数所需的门。

4 通过限制转移下界

我们首先通过简化电路的门和连线来规范化电路，同时不增加其规模；随后界定固定关键输入时移除的门数。

定义 4.1 (门类型)。 一个本质二元真值表依赖于两个形式参数。存在两个奇偶真值表，$x \oplus y \oplus c$，其中 $\oplus$ 是异或，而 $c \in \{0,1\}$。其余八个本质真值表是非线性的，形式为 $((x \oplus a) \wedge (y \oplus b)) \oplus c$，其中 $a, b, c \in \{0, 1\}$。退化真值表是常量，或仅依赖一个形式参数。用 $X(C)$ 和 $A(C)$ 分别表示 C中的奇偶门数和非线性门数。

八个非线性真值表在一行或三行上的输出为 1；即使实际的前驱信号彼此相关，这种分类仍取决于门的真值表。

非线性门有一个输入值，可以使其另一个输入无关紧要 .

定义 4.2 (阻塞值)。 非线性门的某个操作数取阻塞值时，无论另一个操作数取何值，输出都是常量。在定义 4.1 的非线性形式中，阻塞值为 a 和 b，常量输出为 c。

因此，将一个操作数固定为其阻塞值，就可以移除该门，并将一个常量传播到其后继节点。

定义 4.3（规范化电路）。如果电路中的每个门都有本质二元真值表、其两个前驱互不相同，且每个门都能到达输出，则称该电路为规范化电路。此外，它不能包含输入三角形。输入三角形由门 $P = p(x,\ u)$ 和 $Q = q(x,\ P)$ 组成，其中 x 是一个主输入，u 是另一个前驱。

移除输入三角形后，Q 即可直接从$(x、\ u)$ 使用一个二元真值表进行计算。这些化简在门消除中很常见，[10, 11]此处给出所需的细节。

引理 4.4 (规范化)。如果输出函数至少有两个本质输入，则它存在一个大小不超过原电路的规范化电路。

证明。这里，信号的一个文字是指该信号或其补。

1. 移除不计算任何本质二元运算的门。删除所有没有通向输出的路径的门。常量操作数、重复操作数或退化真值表会产生一个常量或某个前驱的文字，因此将其替换为该常量，或绕过该门。在后一种情况下，将所有取反并入接收该信号的门的真值表中。由于输出至少有两个本质输入，其保留下来的信号是一个二元门的文字。选择该门作为输出，剪除其后继节点，并将任何最终取反吸收到其真值表中。

2. 替换输入三角形。对于 $P = p(x、\ u)$ 和 $Q = q(x、\ P)$，将 Q 处的真值表替换为$\psi(x、\ u) = q(x、\ p(x、\ u))$。如果其他门使用 P的输出，则保留 P。如果 q是非线性的，则在 x 处阻塞它会得到 ψ的一个常量余因子。如果 q 是奇偶函数且 p 是非线性的，则在 x 处阻塞 p 会得到一个常量余因子。如果二者都是奇偶函数，则 x 的两次出现会相互抵消。因此，ψ 是非线性或退化的；它绝不是真正的本质奇偶真值表。再次应用步骤 1。

3. 检查终止性。所有删除和旁路操作都保留原有的前驱次序，且每一步都不会增加门的数量。在删除操作之间，三角形替换会将 Q 的前驱从 P 改为更早的顶点 u。这会严格减小所有连线的前驱索引之和，因此替换和删除操作只能进行有限次。

终止时，电路已规范化，函数保持不变，且没有新增任何门。

□

因此，我们可以在施加限制之前，将一个大小最小的电路规范化 n.

引理 4.5 (限制所移除的门)。在一个规范化电路中，固定 t 个限制前为本质输入的输入。假设余因子至少有两个本质输入。化简至少移除 t 个门。

证明。令 d 表示从这些固定输入引出的连线数；根据其本质性，有 $d \geq t$。令 S 包含这些输入以及通过传播常量而变为常量的所有 h 门。输出位于 S之外，因为余因子仍有两个本质输入。

令 e 表示两个端点都在 S中的连线数，并令 b 表示从 S引出的连线数。每个常值门至多接收来自 S的两条连线，因此 $e \leq 2h$。S 中的每个门都有一条出连线，因为原电路已规范化，且其输出位于 S之外。因此 $e + b \geq d + h$，进而$h + b \geq d$。

这些 b 离开 S 的连线进入不同的门：如果有两条连线进入同一个门，那么它的两个操作数都会是常量，并且该门将属于 S。每个接收门都有一个常量操作数，根据引理4.4，可以将其旁路或替换为常量。这些 b 门不同于 h常量门，因此至少有 $h + b \geq d \geq t$ 个门被移除。

□

将这一计数应用于 SAT 限制，可得到如下转移不等式。

引理 4.6（转移）。若将 F_w 限制为固定的 $n - L$ 个比特后，得到一个依赖所有 $L \geq 2$ 个自由位的函数 G，则 $C_{B_2}(F_w) \geq n - L + C_{B_2}(G)$。

证明。利用引理 4.4规范化一个最小电路。根据引理 3.2，每个固定的编码位在施加限制之前都是必不可少的，因此引理 4.5 至少移除了 $n - L$ 个门。剩余电路计算 G，因此至少有 $C_{B_2}(G)$ 个门；加上移除的门即可得到该不等式。两项开销都是在同一个原始电路中衡量的，因此无需假设其计算彼此不相交。 □

5 能在限制下存活的布尔测试

传递引理将 SAT 问题归约为自由标识符字段的电路下界，因此我们为每个字段选择布尔测试，使其同时支持门数的两个部分。高代数次数意味着需要大量非线性门，而不同的余因子则确保输入设置在门消除固定其他比特时仍可区分。

定义 5.1（代数次数）。 将布尔函数表示为二元素字段 $\mathbb{F}_2$上的唯一多线性多项式。这里，加法是异或，乘法是与；多线性是指每个变量的指数至多为一。代数次数 $\deg_{\mathbb{F}_2} f$ 是非零系数单项式中变量数的最大值。常量的次数定义为零。一个 r 变量函数若其次数为 r [15, Section 2.2.1]，则称其具有满次数。

对接受赋值的数量取模二进行计数，无需构造多项式即可检测满次数。

引理 5.2（满次数测试）。 对于 $r \geq 1$，一个 r 变量函数具有满次数，当且仅当它有奇数个接受赋值。

证明。 对布尔立方体上的多项式值求和。一个含有 j 个变量的单项式恰好在 2^{r-j} 个赋值上取值为 1；如果 $j < r$，这个数就是偶数，因此它在 $\mathbb{F}_2$中的贡献为零。对于 $j = r$，其贡献恰好等于所有 r 变量乘积的系数。这个和统计了模 2 意义下的接受赋值数，因此，当且仅当满次数项的系数为 1 时，接受赋值的数量为奇数。 □

恰好一半的布尔真值表具有满次数。
SAT 嵌入通过与和或组合针对互不相交的标识符字段进行的测试。

定义 5.3（只读一次复合）。 块是在其自身输入位集合上定义的布尔函数。只读一次的与/或复合是由与和或运算构成的有根二叉树。其叶子是定义在两两不相交的输入集合上的块，并且每个块只出现一次。用 B 表示叶子的数量，用 L 表示输入位的总数。

这里的“只读一次”描述的是定义该函数的树；计算该函数的电路仍可任意共享门。

Schnorr 的界将多项式次数与非线性门的数量联系起来 [13]；我们采用 Kojevnikov 和 Kulikov 的二进制电路表述 [12,引理 1]。

引理 5.4（次数需要非线性门）。 如果 f 的代数次数为 $D \geq 1$，那么任何计算 f 的 B_2 电路都至少包含 $D - 1$ 个非线性门。

证明。 按前驱顺序将非线性门列为 z_1、……、 z_A。将它们的输出视为相互独立的形式布尔变量。其他所有门在 $\mathbb{F}_2$上都是仿射的，也就是说，它们是一个常量加上若干单个变量之和。因此，在z_j 之前的每个信号都是原始输入和z_1、……、 z_{j-1}的仿射函数。定义z_j 的多项式p_j 关于这些符号的总次数至多为二。最终输出是原始输入和所有z_j的仿射函数。

对布尔多项式进行操作：对每个当前变量 u（包括每个形式门变量），将 u^2 替换为 u 。这样，每次替换后多项式都会变为多线性多项式。若其当前次数至多为 $d \geq 1$，则将含有z_j的项分离出来：

$$P = z_j U + V, \qquad z_j \notin \mathrm{Var}(U) \cup \mathrm{Var}(V), \qquad \deg U \leq d - 1, \quad \deg V \leq d.$$

这里，Var(U)是出现在 U中的变量集合。将z_j 替换为p_j 后得到 $p_jU + V$，其次数至多为 $d + 1$。将结果化为多线性形式不会增加其次数。

按该顺序代入 z_A、z_{A-1}、……、z_1。每个 p_j 只使用更早的门符号，因此代入后只剩下原始输入。从次数至多为一开始， A 代入后次数至多为 $A + 1$。所得多项式表示 f，因此 $D \le A + 1$，等价地，$A \ge D - 1$。 □

该界在任意共享的情况下仍然成立；逆向代入会将每个非线性门计数一次。

不相交性使得块通过与或组合时，其次数相加。

命题 5.5 （只读一次复合的次数）。 在不相交输入上，对次数为 d_1、……、$d_B \ge 1$ 的函数进行复合，其次数为 $d_1 + \cdots + d_B$。特别地，在 L 个输入上对满次数块进行复合，其次数为 L。表示该复合的每个电路至少包含 $L - 1$个非线性门。

证明。 设 f 和 g 使用不相交变量，并且次数分别为 d、$e \ge 1$。 f中的一个次数为 d的单项式与 g 中的一个次数为 e 的单项式的乘积，其次数为 $d + e$。不相交变量集唯一确定该单项式的两个因子，因此这些项不可能相互抵消。于是， fg 的次数为$d + e$。或对应的多项式为 $f + g + fg$。由于 $d + e$ 超过 d 和 e，其最高次部分再次与 fg的最高次部分相同。

在每个父节点处，两个子树仍使用互不相交的输入集，因此它们的次数相加。由归纳法可得 $d_1 + \cdots + d_B$ 在根节点处成立。对于满次数块，其总和为 L，因此引理 5.4表明，任何实现该复合函数的电路至少需要 $L - 1$ 个非线性门。 □

门消除还要求输入依赖性在限制之后仍然保持。

定义 5.6 (余因子条件)。 对于一个布尔函数，采用以下三个条件 s.

- (E1)：固定任意一个比特后，每个剩余比特都是本质变量。
- (E2)：固定任意至多两个比特后，每个剩余比特都是本质变量。
- (S4)：对于任意两个不同的比特，固定它们后得到的四个余因子两两不同。

我们在单比特限制之前使用 (E2)，之后使用 (E1)。

定义 5.7 (鲁棒块)。 对于整数 $3 \le k \le r$，若一个定义在 r 个输入上的块满足：每个至少保留 k 个输入的限制都满足 (S4)，则称其为 k-鲁棒的。

按照 Lachish and Raz [9, 定义 3.1–3.2] 的术语，这就是强二依赖。只需检查恰好保留 k 个输入的限制，因为两个余因子相等这一性质在任何共同的进一步限制下都会保留。因此，在多于 k 个输入时出现的失败，也会导致恰好保留 k 个输入时出现失败：保留选定比特对不变，并固定其他输入，直到恰好剩下 k 个输入，正如 $k \ge 3$ 所允许的那样。

引理 5.8 (跨块的余因子)。 假设只读一次复合中的每个叶节点都是一个 k-鲁棒块的限制。若每个叶节点都至少保留 $k + 2$ 个比特，则该复合满足 *(E1)*、*(E2)* 和 *(S4)*。若每个叶节点都至少保留 $k + 1$ 个比特，则该复合仍满足 *(E1)*。

证明。 1. 证明每个相关叶节点都能取到两个值。 一个至少剩余 k个比特的鲁棒叶节点对每个比特都具有本质性。否则，某个包含非本质比特的比特对会有两个相同的余因子，这与 (S4) 矛盾。因此，每个叶节点都不是常量。每棵子树也都不是常量：令其两个子节点都为零或都为一，即可得到所需的父节点值。它们的输入互不相交，因此可以同时作出这些选择。

2. 显露一个叶节点，并证明本质性断言。 沿着选定叶节点到根节点的路径，在 AND 父节点处将每个兄弟节点设为一，在 OR 父节点处将其设为零。这样，根节点的值就等于选定叶节点的值。在每个叶节点都至少剩余 k 个比特的限制下，这仍然可行。以 $k+2$ 个比特为起点，允许固定任意两个比特，从而证明 (E2)，进而证明 (E1)。以 $k+1$ 为起点，允许固定一个比特，从而证明最后一个断言。

3. 分离一个叶子中比特的四个余因子。 使用步骤 2 暴露该叶子。根据鲁棒性，它的四个余因子各不相同。如果完整组合中的两个余因子相等，那么暴露该叶子将保留这种相等关系，从而产生矛盾。

4. 分离两个叶子中比特的四个余因子。 将从这两条路径分出的每个子树设为步骤 2 中的中性值。保留下来的运算是两条路径最近公共祖先处的与或或。根据本质性，每个选定的比特都会产生其叶子的两个不同余因子。根据该比特固定后的本质性，这些余因子均非常量。对于与运算，接受赋值是从两个非空接受集合中分别取元素组成的数对。通过取这些数对的相应坐标，可以恢复出每个集合。因此，每个集合有两种选择，从而得到四个不同的接受赋值集合。对于或运算，对非空拒绝集合应用相同的推理 [16,第 1 节。2]。

□

5.1 构造满次数鲁棒块

计数论证给出了满次数测试，其鲁棒性阈值 k 随块长度呈对数增长；而采用模素数加权和的构造，其阈值则按平方根级增长。对于 SAT 限制，只需证明这类测试存在即可。计数证明使用随机真值表和并合界来区分余因子，与 Kabanets [17,第 3], 节中的做法相同，并且也要求满次数。

命题 5.9 (计数构造)。 设 $r \geq k+2$ 且 $k \geq 3$。若 $2^{k-2} > \log_2(6r(r-1)) + r\log_2 3,$ ，则存在一个定义在 r 个输入上的 k-鲁棒函数，其次数为满 $\mathbb{F}_2$ 次 r。

证明。 从所有定义在 r 比特上的真值表中均匀随机选择 g 。施加限制后，若有 $j \geq k$ 个自由位，则选定比特对的四种取值会留下四组互不相交的赋值。对应的真值表是定义在 $j-2$ 比特上的相互独立的均匀函数。这些函数共有 $\binom{4}{2} = 6$ 对。每对相同的概率为 $2^{-2^{j-2}}$，因此发生任何相同情况的概率至多为 $6 \cdot 2^{-2^{k-2}}$。

最多有 3^r 个限制，因为每个比特都可以是自由的、固定为零或固定为一；对于每个限制，最多有 $\binom{r}{2}$ 个选定比特对。因此，根据并合界，失败概率至多为

$$3^r \cdot 3r(r-1) \cdot 2^{-2^{k-2}} < \frac{1}{2}.$$

严格的 不等式在以 tw 为底取幂后，恰好就是所述的对数假设 o.

恰好一半的真值表包含奇数个一：翻转任意一个表项即可将奇表与偶表配对。根据引理 5.2，因此满次数的概率为 $1/2$。因此，失败界意味着满次数与鲁棒性同时成立的概率为正。

□

对于较大的 r，取 $k = \log_2 r + O(1)$ 即可使不等式成立。

Savický 和 Žák 利用模素数加权和结合子集和覆盖，在限制 [18, 定理 2.5 和第 3] 节之后区分余因子。这里我们测试其是否等于单个剩余类：选择一个模数来区分所有四种成对设置，并选择一个剩余类以得到满次数。

命题 5.10 (加权模分块)。 设 $r \geq 4$，并设 p 为大于 $2r$ 的最小素数。设 m_p 为满足 $1 + m_p(m_p + 1)/2 \geq p$ 的最小非负整数。令$k = m_p + 2 \leq \lceil\sqrt{8r}\rceil + 2$。对于 $r \geq k + 2$ 以及模 p 的任意剩余类 t，函数

$$g_{r,t}(a_1, \ldots, a_r) = \left[\sum_{i=1}^{r} i\, a_i \equiv t \pmod{p}\right]$$

是 k-稳健的。至少存在一个剩余类 t，使其具有满次数 r。这里，$[P]$ 在陈述P 成立时等于一，否则等于零。

权重 1，……，r 能够区分任意两个比特的四种取值，而足够多的其余权重则保证每个对应的剩余类都可达。

证明。 1. 确定四个目标剩余类。 固定一些比特后，令 F 为自由指标集，并令 τ 为模 p 下 t 减去固定比特的贡献。假设 $|F| \geq k$。对于不同的i，$j \in F$，四个余因子具有形式 $[S \equiv \tau - \sigma \pmod{p}]$。这里 $\sigma \in \{0,\ i,\ j,\ i + j\}$，而 S是对 $F \setminus \{i,\ j\}$上的加权和。四个目标彼此不同：i，j 是不同的正整数，并且 $i + j \leq 2r < p$。

2. 证明四个目标都能取到。 令 $H = F \setminus \{i,\ j\}$，将其视为模 p 的剩余类集合。于是 $|H| \geq m_p$ 和 $H \cap (-H) = \varnothing$，因为所有权重都属于 $[1, r]$，且 $2r < p$。Balandraud 子集和定理指出，对于奇素数 p 和这样的集合 H，

$$|\Sigma(H)| \geq \min\{p,\ 1 + |H|(|H| + 1)/2\}.$$

这里 $\Sigma(H)$ 包含 H的所有子集之和，包括空子集 [19, 定理 3]。定义 m_p 使右侧为 p，因此每个目标剩余类都能由剩余自由位的一种赋值取得。每个余因子在一个非空赋值集合上取值为 1，且这四个集合两两不相交，因此这些余因子各不相同。这证明了鲁棒性。

3. 界定阈值。 Bertrand 假设保证在 $2r$ 和 $4r$ [20]之间存在一个素数。由于p是大于 $2r$的最小素数，因此有 $p < 4r$。令 $q = \lceil\sqrt{8r}\rceil$，得到 $q(q+1)/2 > 4r > p - 1$，于是 $m_p \leq q$ 和 $k \leq q + 2$。

4. 求奇数剩余类计数。 设 N_t 统计满足 $\sum_i i a_i \equiv t \pmod{p}$的赋值。在 $\mathbb{F}_2[z]/(z^p - 1)$ 中，这些计数的奇偶性由下式记录：

$$\sum_{t=0}^{p-1} (N_t \bmod 2) z^t \equiv \prod_{i=1}^{r} (1 + z^i) \pmod{z^p - 1}.$$

每个因子都会选择是否包含权重 i，而模 $z^p - 1$ 约简会汇总具有相同剩余类的和。写作 $\Phi_p(z) = 1 + z + \cdots + z^{p-1}$，则 $z^p - 1 = (z + 1)\Phi_p(z)$ 在 $\mathbb{F}_2$ 上成立。由于 p 是奇数，$z^p - 1$ 在特征二下的导数为 z^{p-1}。它与 $z^p - 1$ 互素，因此后一个多项式没有重因子。在 $\mathbb{F}_2$ 上的 $z^p - 1$ 的分裂域中运算，此时该多项式可分解为线性因子。由于 $\Phi_p(1) = 1$，其根是除 1 以外的 p 次单位根。因为 p 是素数，每个根的乘法阶为 p。这样的根不可能满足 $1 + z^i = 0$，其中 $1 \leq i \leq r < p$。因此，Φ_p 的任何不可约因子都不整除乘积中的任何因子。特别地，Φ_p 不整除该乘积，而该乘积模 $z^p - 1$ 的余数非零。因此，至少有一个 N_t 为奇数，而引理 5.2 说明该 $g_{r,t}$ 具有满次数。

5. 有效地指定剩余类。从一个长度为 p 的奇偶函数向量开始，该向量在剩余类零处为 1，其余位置均为 0。对于 $i = 1, \ldots, r$，将它循环移位 i 后的结果与自身相加，运算在 $\mathbb{F}_2^p$ 中进行。等价地，将多项式向量更新为 $v \leftarrow v + z^i v$ 模 $z^p - 1$。经过 r 次更新后，其各项即为所有 N_t 的奇偶函数，因此选择取值为 1 的最小剩余类。一旦固定 p，此递推的代价为 $O(rp) = O(r^2)$ 次位运算。

□

这个二次界假设已提供素数；第 8.1 节介绍了寻找素数以及构造块的形式化成本。

6 限制下的门计数

我们用加权门数衡量限制的影响：对主输入所附带的两种信用，各减去一个单位。当某个输入的唯一后继是非线性门时，它获得第一份信用；当该门的唯一后继也为非线性门时，它获得第二份信用。为了追踪这些信用在限制下如何变化，我们会在化简过程中记录哪些门使用了每个信号。

我们首先区分后继门的数量与它们使用的操作数位置数量。

定义 6.1（后继集合与扇出）。对于定义 v 2.2 中的一个顶点，令 $\mathrm{succ}(v)$ 表示以 v 为操作数的门的集合。其扇出为 $d(v) = |\mathrm{succ}(v)|$。对于顶点集合 Y，定义 $\mathrm{succ}(Y) = \bigcup_{v \in Y} \mathrm{succ}(v)$。这些集合指的是当前电路。它们包含暂时存在但没有路径通向输出的任何门。

一个门若两次使用同一信号，仍只计作一个后继，不过下文化简的电路中，每个门都有两个不同的前驱。

定义 6.2（限制下的消解）。设 C 计算 f。假设其门都有不同的前驱，且其输出门没有后继。中间门可以具有退化真值表，如定义 4.1所述。设 ρ 固定输入集 I，并假设 $f|_\rho$ 至少有两个本质输入。

按拓扑序处理节点，确保每个前驱都先处理。为每个节点v 赋予一个已消解信号 $\sigma(v)$。它是一个常量或某个节点的文字，表示该节点的值或其补。固定输入消解为其指定的常量；自由输入 z 消解为 z。对于 $G = g(a, b)$，将已消解操作数代入 g。将不同的底层节点名称视为相互独立的形式布尔变量，不论它们计算出的信号之间有何关系，并据此检验所得真值表。以下规则中的变为常量和依赖均指这一局部真值表检验。

- 如果 $g(\sigma(a)\ \sigma(b))$ 是常量，那么 G 变为常量，且 $\sigma(G)$ 就是该常量。
- 如果它恰好依赖一个底层节点 N，那么 $\sigma(G)$ 就是 N 对应的文字。我们称 G 被旁路，并传递 N。
- 如果它依赖两个不同的底层节点，G 在消解后保留，且 $\sigma(G) = G$。将其操作数替换为这些节点，并将任何补吸收到其真值表中。

该规则涵盖常量操作数、退化真值表以及塌缩：两个操作数都解析为同一节点的文字，且所得真值表给出常量或文字。

消解确定输出信号；随后进行剪枝，移除不再对其产生贡献的门。

定义 6.3（简化电路）。根据定义 6.2，设 $f|_\rho$ 至少依赖两个输入。原始输出解析为某个门的文字 N，且该门在消解后仍然保留。将 N 指定为新输出。如果该文字带补，则对 N处的真值表取补。剪除所有不存在通往 N路径的门。特别地，N 的任何后继都不会保留，因此更改其真值表不会影响其他保留的门。

将所得电路 C^ρ 称为 简化电路。如果某个原始门不在 C^ρ中，则称其已被消除。这包括变为常量、被旁路，或在消解后保留但被剪枝的门。根据引理 $N(C^\rho)$，将 C^ρ 规范化为 4.4。

在本节余下部分中，电路遵循定义 6.2中的前驱互异与输出约定，并且每次应用消解时，都假设该余因子至少有两个本质输入。

引理 6.4 （消解与依赖）。 定义 *6.3* 中的简化电路计算 $f|_\rho$，并保留每个未删除门的类型。如果从某个自由输入到输出的每条路径都经过一个在 ρ 下取常量值的门，那么 $f|_\rho$ 与该输入无关。

路径判据适用于任意电路和限制，无需双本质输入假设。当某个门计算自由输入的常值函数，而局部消解检验未能检测到这一点时，该判据同样适用。

证明。 在 ρ下，每个已消解操作数的值都与其原始值完全相同，因此按照拓扑序进行归纳，可保持每个门值和输出不变。随后，剪枝只会移除没有通向该输出的路径的门。

保留的门有两个不同的已消解操作数，其真值表的变化仅限于对输入取补，或对指定输出取补。这两种操作都保持定义4.1.中的奇偶函数类型和非线性类型不变。

将 ρ 下取常量值的每个门替换为其值。如果自由输入到输出的每条路径都经过这样的门，那么剩余路径中就没有任何一条能将该输入传递到输出。因此，余因子与该输入无关。

□

以下引理追踪信号经过传递该信号的门时的情况。

引理 6.5 (传递)**.** 使用定义 *6.1–6.3.* 设 N 是一个自由输入或一个在消解后保留下来的门。设 S_N 为这样一组节点：它们的已消解信号是 N的文字；特别地，$N \in S_N$。

(a) $S_N \setminus \{N\}$ 中的每个节点都是一个在 S_N 中有操作数的门。

(b) N 在 C^ρ 中的后继节点恰好是 C^ρ 中具有位于 S_N 的原始操作数的门。

(c) 如果 $N \in Y \subseteq S_N$，并且 $\mathrm{succ}(Y) \setminus Y$ 中没有门位于 S_N 中，那么 $S_N = Y$。

(c) 部分让我们能够证明，某个集合包含所有传递 N 的节点：只需检查没有离开该集合的边会指向另一个这样的节点。

证明。 对于 (a)， $S_N \setminus \{N\}$ 中的节点不可能是主输入。将其写作 $G = g(a, b)$。要使 N 出现在代入后的真值表 $g(\sigma(a)\ \sigma(b))$ 中，至少一个已消解操作数必须是 N 的文字。

对于 (b)， C^ρ 中保留的门的每个操作数都是某个原始操作数的已消解信号所对应的底层节点。仅当该原始操作数位于 S_N 中时，它才是 N。

对于 (c)，如果 $S_N \setminus Y$ 非空，设 G 是其拓扑序中最靠前的节点。根据 (a)， G 在 S_N 中有一个前驱。该前驱出现得更早，因此它属于 Y。于是 $G \in \mathrm{succ}(Y) \setminus Y$，这与假设矛盾。

□

定义 6.6 (第一份信用)。 如果主输入 z 的后继集合 succ(z) 只包含一个非线性门 W_z，则该主输入可获得一份信用。将 z 称为 *D* 变量，将 W_z 称为它的 *D* 门。用$\mathcal{D}(C)$ 表示 D 变量的集合，用 $D(C) = |\mathcal{D}(C)|$ 表示其基数。

信用取决于当前的后继集合，因此在施加限制后可能出现或消失。

依赖条件可防止固定其他一两个输入后，某个获信用输入对输出的影响被切断。

引理 6.7 (禁构形)。 设 C 计算 f，其信用如定义 *6.6* 所述，条件如定义 *5.6*所述。

(a) 在 *(E1)* 条件下，没有具有两个主操作数的门是 *D* 门。因此，不同的 *D* 变量对应不同的 *D* 门，且 $D(C) \le A(C)$。

(b) 在 *(E2)* 条件下，具有两个主操作数的本质门 T 的后继都不是 *D* 门。

这些 排除条件将限制可分配给单个被消去的门的损失信用数量 .

证明。对于 (a)，假设 $W = W_z$ 的操作数为 z 和一个不同的主输入 v。将 v 固定为针对 W 的阻塞值，会使该门变为常量。从 z 出发的每条路径都以 $z \to W$开头，因此引理 6.4 说明余因子与 z无关。这与 (E1) 矛盾。如果两个 D 变量共用一个 D 门，那么它的操作数就是这两个主输入。因此 $z \mapsto W_z$ 是单射。由于每个W_z 都是非线性的，$D(C) \le A(C)$。

对于 (b)，假设 T 的主操作数是 x、y，其后继 W 是 z的 D 门。W的操作数是 T、z。此外，$z \notin \{x, y\}$：它唯一的后继是 W，而 x和 y都连接到 T。由于 T处的本质真值表取两个值，选择 (x, y)，使得 T阻断 W。因此，从 z 出发的每条路径都会经过常值门 W，这与引理 6.4 矛盾，违反了 (E2)。

□

第二份信用记录了同一单后继链上的另一个非线性门 n.

定义 6.8（第二份信用）。输入 $z \in \mathcal{D}(C)$ 在 $\mathrm{succ}(W_z) = \{W_z^2\}$且 W_z^2是非线性门时，可获得第二份信用。称 z 为 D^*-变量。用 $\mathcal{D}^*(C)$ 表示它们构成的集合，用 $D^*(C)$ 表示其基数。若一个门是 z的 W_z，则它在 z中扮演第一角色；若它是 W_z^2，则扮演第二角色。

W_z^2中的上标表示第二门，而不是平方；D^*变量会获得两份信用。

定义 6.9 (两层势函数)。使用定义 4.1中的门数以及定义6.6 和 6.8中的信用，令

$$\Psi_2(C) = 7X(C) + 4A(C) - D(C) - D^*(C). \tag{1}$$

Eli消去门或创建信用会降低 Ψ_2；损失的信用会抵消这一下降的一部分。

引理 6.10 (角色)。设 C 计算 f，角色定义同定义 *6.8*。

(a) 在 *(E1)* 条件下，具有主操作数的门不能具有第二角色。主输入 x 的直接后继 $d(x) \ge 2$ 不具有任何一种角色。

(b) 在 （*E2*）中，具有两个主操作数的本质门的后继不具有任何角色 .

若一个门不具有任何信用角色，我们称其为无作用 门；在下文的记账中，这种门无法被分配损失信用。

证明。对于 (a)，假设 $G = g(x, W_z) = W_z^2$有主操作数 x。输入 z与 x不同，因为 z 只连接到 W_z，而 x 连接到 G。将 x 固定为 G的阻塞值。所有从 z出发的路径都经过 W_z，随后经过现在为常量的 G。该余因子与 z无关，这与 (E1) 矛盾。

设 G 是 x 的后继，且具有 $d(x) \ge 2$。前面的论证排除了第二角色。若$G = W_z$，则 $z \ne x$，因为 z 只有一个后继。G 的操作数将是主输入 x，z，这与引理 6.7(a) 矛盾。

对于 (b)，设 T 的主操作数为 x、y，且 S 是其后继。引理 6.7(b) 排除了第一角色。若 $S = W_z^2$，其操作数为 T、W_z。由引理 6.7(a) 可得 $W_z \ne T$。此外，$z \notin \{x, y\}$，因为 z 只连接到 W_z。选取 (x, y)，使得 T 阻塞 S。于是，从 z 出发的所有路径都会经过常值门 S，这与 (E2) 矛盾。

□

我们通过从被消去的门的贡献中扣除每一份损失信用来进行核算，并将分配给该门的总量称为其收费。

引理 6.11（为 Ψ_2）**收费**。采用定义 *6.9* 中的势以及定义 *6.2*中的消解。设 C 计算满足 *(E1)* 的函数 f。设 ρ 固定输入集 I。假设 $f|_\rho$依赖于每个自由输入，且至少有两个输入保留。

当语句 P成立时写作 $[P] = 1$，否则写作 $[P] = 0$。输入 z的旧信用为 $\lambda(z) = [z \in D(C)] + [z \in D^*(C)]$。对于 $z \notin I$，令 $\lambda'(z)$ 表示其在 C^ρ中的相应信用。对于$z \in I$，设 $\lambda'(z) = 0$。获得的信用总量为 $\Gamma = \sum_z \max(\lambda'(z) - \lambda(z), 0)$。

为原始门赋予权重 G $w_2(G)$，若其为奇偶函数、非线性或退化门，则权重分别为 7、4 或 0 。在被消去的门上存在非负整数电荷 $\chi_2(G)$，使得

$$\Psi_2(C) - \Psi_2(C^\rho) = \sum_{G\ eliminated} \big(w_2(G) - \chi_2(G)\big) + \Gamma. \tag{1a}$$

只有具有第一或第二角色的非线性门才会被收费，且每次收费最多为两单位。如果$I \cap D(C) = \varnothing$，每次收费最多为一单位，并且没有被收费的门会变成常量。

公式（1a）将下降量分解为门权重、损失的信用和获得的信用。如果没有 D 变量被固定，每个被消去的非线性门至少贡献三单位。无角色非线性门或变成常量的门，则贡献全部四单位。

证明。 将每个输入损失的信用分配给其原始信用链上被消去的门，然后界定每个门的收费。

1. 将信用损失与获得的信用分开。令 $\Lambda = \sum_z \max(\lambda(z) - \lambda'(z), 0)$ 为信用损失总量。 $D + D^*$ 的原始值减去其限制后的值为 $\Lambda - \Gamma$。根据引理 6.4， $7X + 4A$ 的下降量等于对所有被消去的门求和得到的 $w_2(G)$。只需恰好向这些门分配Λ 单位。任何满足 $\lambda(z) > \lambda'(z)$ 的输入都属于 D(C)。

2. 当 z 是自由的，且 W_z 仍然存在时，分配一份损失。 由于 W_z 在消解后仍然存在， $\sigma(W_z) = W_z$，并且引理 6.5(c) 在 $Y = \{z\}$的条件下给出 $S_z = \{z\}$。(b) 部分使 W_z 成为 z在 C^ρ中的唯一后继；它仍是非线性门，因此第一份信用得以保留。因此，这一损失为一，源于 z 失去第二份信用。

门 W_z^2必须被消去：如果它仍然存在，引理 6.5(c) 将给出 $S_{W_z} = \{W_z\}$。(b) 部分随后会使非线性门 W_z^2成为 W_z 在 C^ρ中的唯一后继，从而保留第二份信用。因此，我们将损失的这一单位记在 W_z^2上。

3. 当 z 是自由的，且 W_z 被消去时，分配一份损失。 如果 z 在 C^ρ中仍有第一份信用，则正损失为一；将其记在 W_z上。否则， z 会失去全部 $\lambda(z)$ 份信用。对 W_z 收费一次；当 $z \in \mathcal{D}^*(C)$ 时，对 W_z^2收费一次。

为说明为何对 W_z^2 收费，假设它仍然存在。若 $W_z \notin S_z$，引理 6.5(c) 得出 $S_z = \{z\}$。(b) 部分随后会使 z 在 C^ρ 中没有后继，这与本质性矛盾。因此， $W_z \in S_z$。将 (c) 部分应用于 $Y = \{z, W_z\}$。它唯一的出边后继是 W_z^2，该后继在消解后仍然存在，且不会经过 z。因此， $S_z = \{z, W_z\}$。根据 (b) 部分， z 在 C^ρ 中唯一的后继是非线性门 W_z^2。这会使 z 获得第一份信用，与假设矛盾。因此， W_z^2 被消除。

4. 当 z 被固定时，分配一份损失。这里 $\lambda'(z) = 0$，因此损失为 $\lambda(z)$。门 W_z 有一个常量操作数，因此会被消除；对它收费一次。如果 z 获得了第二份信用，则在该门被消除时对 W_z^2 收费。如果 W_z^2 仍然存在，则将第二个单位分配给 W_z 。

5. 恢复势恒等式。 步骤 2–4 为每个失去信用的输入恰好分配 $\lambda(z) - \lambda'(z)$ 个单位。每次分配都指向一个已消去的非线性门，且该门具有与该输入对应的角色。定义 $\chi_2(G)$ 为分配给 G 的单位数。于是 $\sum_G \chi_2(G) = \Lambda$。代入步骤 1 即可证明公式（1a）。

6. 将每个门的收费限定为至多两次。 如果 $G = W_z$，则它具有一个主操作数，因此引理 6.10（a）排除了 G处的每个第二角色。引理 6.7（a）使 z 唯一。只有 z 会向 G收费：自由时至多一次，固定时至多两次。

否则 G 只能通过第二角色收费。对于每个这样的角色，一个操作数是第一门 W_z。根据引理，这些门确定了互不相同的输入6.7(a)。二元门有两个操作数，而每个相关输入至多赋予一个单位。因此 $\chi_2(G) \le 2$。

7. 在没有固定 D 变量时，找出唯一可能被重复收费的情况。假设 $I \cap \mathcal{D}(C) = \varnothing$。步骤 4 从不适用，因此第一门至多接收一个单位。重复收费需要某个第二门 $G = g(W_{z_1}, W_{z_2})$ $= W_{z_1}^2 = W_{z_2}^2$ 对应不同的自由输入 z_1, z_2。只需证明该门仍然属于 C^ρ。

8. 证明共同的第二门在消解后仍然保留。对于 $i = 1, 2$，门 W_{z_i} 不可能变成常量。从 z_i 出发的每条路径都会经过它，而且 $f|_\rho$ 依赖于 z_i。同样，W_{z_i}也不可能经过 z_i以外的节点。否则会得到 $S_{z_i} = \{z_i\}$ 根据引理 6.5(c)，(b) 部分便会使 z_i 没有保留后继，这与其本质性矛盾。因此 $\sigma(W_{z_i})$ 要么是 W_{z_i}，要么是 z_i的一个文字。

四个节点 z_1、z_2、W_{z_1}、W_{z_2} 互不相同。前两个是不同的输入；根据引理 6.7(a)，后两个是不同的门。因此，G 的操作数消解为不同节点的文字，所以 G在消解后仍然保留。

9. 证明共同的第二门不会被剪除。引理 6.5(c) 给出 $S_{z_1} \subseteq \{z_1, W_{z_1}\}$。当 $W_{z_1} \notin S_{z_1}$ 时使用$Y = \{z_1\}$，否则使用 $Y = \{z_1, W_{z_1}\}$。在后一种情况下，唯一的出边门是 G，它在消解后仍然保留，且不会经过 z_1。如果 W_{z_1} 在消解后仍然保留，(c) 部分还给出 $S_{W_{z_1}} = \{W_{z_1}\}$。(b) 部分将 z_1 的新后继限制在 $\{W_{z_1}, G\}$ 内，而 W_{z_1} 的新后继则在 $\{G\}$ 内。

一个幸存的 W_{z_1} 不可能是新输出。否则，原始输出就会位于 $S_{W_{z_1}} = \{W_{z_1}\}$ 中。但 W_{z_1} 有后继 G，而原始输出没有后继。本质性保证存在一条从 z_1 到新输出的路径。根据后继的描述，这条路径必经 G，因此 G 不会被剪枝。所以，步骤 7 中可能出现的重复收费可以排除。

10. 排除对变为常量的门进行收费。现在，每个被收费的门都在某个自由输入 z 中扮演一个角色。将 W_z 或 W_z^2 设为常量，会切断从 z 到输出的所有路径。这与 $f|_\rho$ 中 z 的本质性矛盾。

□

消元可能会产生输入三角形；下一个引理表明，规范化会保留势能下降。

引理 6.12 (规范化保留势函数界)。假设 C' 的每个门都是本质的二元门，具有不同的前驱，且都能到达输出。如果其函数至少有两个输入并满足 *(E1)*，那么 $\Psi_2(N(C')) \le \Psi_2(C')$。

证明。对于 $P = p(x, u)$ 和 $Q = q(x, P)$，按照引理 4.4，将 Q 替换为 $\psi(x, u) = q(x, p(x, u))$。暂时保留 P，并将边 $P \to Q$ 替换为 $u \to Q$。由于真值表 ψ 是非线性的或为退化门，$7X + 4A$ 不会增加。

一个 D 变量 z 不可能等于 u。它的唯一后继将是 P，且有两个主操作数，这与引理 6.7(a) 矛盾。$Q = W_z$ 也不可能：它的主操作数 x 同时输入到 P和 Q中。因此，改变边和真值表不会破坏任何第一份信用。

设 z 有第二份信用。只有在 $\mathrm{succ}(W_z)$ 时，添加的边才可能改变 $u = W_z$。此时，$P = W_z^2$会有主操作数 x，这与引理 6.10(a) 矛盾。只有在 $P = W_z$时，删除的边才可能改变该后继集合。这不可能：x 有两个后继，并且如上所示，u 不可能是 D 变量。最后，Q 不可能具有第二角色，因为它有主操作数 x。每一份第二信用都得以保留。

应用定义6.2 ，并保持函数不变。$I = \varnothing$。要看出 (E1) 在至少有两个输入时能确保每个输入都相关，选取一个输入并固定另一个不同的输入。根据 (E1)，只改变所选输入，就会在某个赋值下改变所得函数的输出。引理6.11 至多将一个损失单位分配给每个被消去的非线性门，而不会分配给退化门。式（1a）中的每项门的贡献均非负，Γ亦然。

引理4.4 中的终止论证适用于重复进行三角形替换和化简。由于这些操作都不会增加 Ψ_2，最终规范化电路的势至多为Ψ_2（C'）。

□

7 每个输入十四个单位

我们证明，将某个输入固定后，势至少会减少十四，从而细化了 Zwick 关于每个输入被多少个门使用的分析 [10, 引理 3。2] 适用于定义 4.1 中的门类型。在紧致情形下，被消去的门贡献十二个单位，而两个仍然存在的非线性门构成一条单后继链，为某个输入带来两份新信用（图 1）。这种记账适用于整个电路，并允许任意共享。

引理 7.1 (一步消去)。 设 C 按照定义 *4.3* 的含义已规范化。假设它计算一个函数 f，该函数至少有两个输入，且满足 *(E2)* 和 *(S4)*。则存在某个主输入 x，满足 $d(x) \geq 2$，以及某个 $c \in \{0,1\}$，使得

$$\Psi_2(C) - \Psi_2\big(N(C^{x=c})\big) \geq 14. \tag{1b}$$

所选输入至少有两个后继，因此在施加限制之前，它没有第一份信用。于是，引理 6.11 将至多一份损失信用分配给每个被消去的门。

证明。 检查第一门及其直接后继。如果被消去的门尚未提供十四个单位，我们就利用 (S4) 分离后继链，并考察可能获得的信用。

1. 确定每个门的贡献。 (S4) 条件要求至少有三个输入：若只有两个输入，四个输入对余因子都会是布尔常量，不可能各不相同。根据 (E2)，对任意一个输入施加限制后，仍至少有两个本质输入，并满足 (E1)。因此，引理6.12使我们能够在最终归一化之前计算减少量。

我们只会固定一个扇出至少为二的输入，而它不可能是 D 变量。因此，引理6.11为每个被消去的奇偶门分配七个单位，为每个被消去的非线性门至少分配三个单位。若非线性门不再发挥任何作用或变为常量，则贡献为四。每获得一份新的信用，就增加一个单位。

2. 找到第一门和一个至少使用两次的输入。 令 T 为拓扑序中的第一门，其主操作数为不同的 x、y。如果两者都只输入到 T，那么 (x、y) 的所有依赖关系都会经过单个比特 T。这对输入至多产生两个余因子，与 (S4) 矛盾。对操作数命名，使得 $d(x) \geq 2$。

以下两个结构性事实可以避免重复计数。由主输入 v 驱动的门的后继不能同时由 v 直接驱动，否则就会形成输入三角形。此外，被化为常量的门不可能是输出，因为余因子至少有两个本质输入。它在原规范化电路中有一个后继，而每个这样的后继都会被消去。

引理 6.10 使 x 的每个直接后继以及 T 的每个后继都无作用。因此，任一集合中被消去的非线性门均贡献四个单位。

3. 完成 T 是奇偶函数的情形。 如果 x 的所有后继节点都是奇偶门，那么对 x 的任一赋值都会消去至少两个门，得到十四个单位。否则，选择一个非线性后继P，并通过 x将其阻塞。不同的门 T、P贡献 $7 + 4$，而现在已成为常量的 P 的一个后继会被消去，并贡献至少三个单位。由于无环性，该后继不同于 P；又由于 T 排在首位，它也不同于 T，因此总计至少为十四。剩下的情形是非线性 T。

4. 将非线性情形化简为每个输入有两个后继节点。 输入 y 的扇出也至少为二，因为否则，通过 T 将 x 阻塞会使 y 断开，这与 (E1) 和引理 6.4 矛盾。

令 c_T 为 T 被阻塞时的常量输出。分别将 ε, δ 记为 x, y在 T处的阻塞值。对于 $v = x$ 或 $v = y$，称将 v 固定为其阻塞值以处理 T 为 v步。如果$d(v) \geq 3$，这一步会消去 T、 v的另外两个后继节点，以及 T的一个后继节点。这四个门彼此不同： T 的后继节点不可能同时是 v的直接后继节点。每个门至少贡献四，总计至少十六。

因此，我们可以假设 $d(x) = d(y) = 2$，并记 $\mathrm{succ}(x) = \{T, U\}$ 以及 $\mathrm{succ}(y) = \{T, V\}$，其中 U, V 根据引理 6.10(a) 无作用。

5. 排除 U 或 V处的奇偶函数和匹配阻塞值。 如果 U 是奇偶函数， x步会消去T, U 以及 T的一个后继节点，至少贡献 $4 + 7 + 4$。这些门彼此不同，因为不存在输入三角形，因此 T 的后继节点不可能是 U。如果 V 是奇偶函数，y步可得相应的估计。

假设相反， x 在 T， U 处的阻塞值相同。将 x 固定为该值，使两个门都变为常量。两个门都以 x 为主操作数，且不存在输入三角形，因此彼此都不是对方的输入。如果它们的后继集合总共至少包含两个不同的门，就选择 T 的一个后继，以及它们后继集合并集中的另一个门。它们都不同于 T， U ，分别至少贡献四个和三个单位。再加上 T， U，总数至少为十五。如果只有一个共同后继，那么它的两个操作数都是常量，因此贡献四个单位，并且它有一个被消除的后继，至少贡献三个单位。总数同样达到这一数值。在 T， V 处阻塞值相同的情形，则改为固定 y 处理。

剩下 非线性 U， V，其阻塞值与 T 在 x， y处的阻塞值相反，分别 ly.

6. 化简为 T 的唯一非线性后继。 x步消除了 T， U，贡献八个单位。如果 T 有两个不同的后继，它们都会被消除，且各自至少贡献四个单位。由于不存在输入三角形，它们都不等于 U，因此总数至少为十六。

否则，令 R 为 T 的唯一后继；它不同于 U 和 V，因为这些门的主操作数为 x， y。如果 R 是奇偶函数，则贡献七个单位，总数达到十五。如果 R 是非线性的，且 c_T 阻塞它，那么它会变成常量并贡献四个单位。 R 的任何不同于 U 的后继至少增加三个单位。如果它唯一的后继是 U，那么 $U = u(x, R)$ 的两个操作数都是常量。 U 的一个被消除的后继会增加所需的三个单位。根据拓扑序，这些额外的门与已计数的门互不相同。

唯一剩下的情况是：有一个未被 c_T 阻塞的唯一非线性后继 R。 x 步骤消除了三个互不相同且无作用的门 T， U， R，贡献十二个单位。 y 步骤同样消除 T， V， R，并贡献十二个单位。

7. 使用 *(S4)* 证明 $U \neq V$。 我们使用 Lachish and Raz 的双后继障碍 [9,引理 3.8]；由于相关门是非线性的，其局部论证适用。令 c_U， c_V 为 U， V 在被阻塞时的输出。如果 $U = V$，它的两个前驱是 x， y，并且对这一对的所有依赖都经过 (T， U)。在 T 对应的 x 阻塞值下，第一个分量为 c_T，而第二个分量可取两个比特中的任意一个。在 x 的另一个取值下，第二个分量为 c_U，而第一个分量可取两个比特中的任意一个。这两个集合共有 (c_T， c_U)，因此它们的并集只有三个值。因此，(x, y) 至多有三个不同的余因子，这与 (S4) 矛盾。因此 T， U， V 互不相同。

8. 将 U和 V 的后继节点分类。 U和 V都不是输出：如果输出是 V，通过 y 将其阻塞会使整个余因子成为常量，这与 (E1) 矛盾。对 U 的论证使用 x，而对 C 进行规范化可确保两个门都有后继节点。

当 V好节点至少有两个后继节点、其唯一后继是奇偶函数，或其唯一后继是被 c_V 阻塞的非线性节点时，称其为好。否则称其为坏。一个坏的 V 有一个

非线性后继 V_2，且 c_V 不阻塞该后继。对 U 使用相同的定义；当其为坏时，U_2 是其唯一后继。这种分类区分了可通过门移除解决的情况，以及可能需要新的输入积分的情况。

9. 当 V 良好时结束。将 y 固定为对于 V 的阻塞值，而该值对于 T 是非阻塞的。门 V 变为常量，T 被旁路；二者各贡献四个单位。若 V 至少有两个后继节点，则其中两个至少贡献 $3+3$。如果它唯一的后继节点是奇偶函数，则该门贡献七个单位。在剩余的良好情形中，其唯一的后继节点是非线性的，并被 c_V 阻塞；它变为常量并贡献四个单位，而该门的一个被消除的后继节点至少贡献三个单位。加上来自 T、V 的八个单位，每种情形都至少得到十四个单位。所计数的后代与 T、V 不同，区别在于拓扑序。

10. 当 U 良好时结束。将 x 固定为对于 U 的阻塞值。门 U 变为常量，T 被旁路，从而贡献八个单位。第 9 步中的三个替代情况（以 U 替代 V）至少再贡献六个单位。现在可以假设 U、V 均为坏的。

11. 当 $V_2 \notin \{R, U\}$ 时获得两个信用。在 x 步中，门 T, U, R 贡献十二个信用。如果另一个门被消去，它至少贡献三个信用，因此估算成立。

否则，其他每个门都仍留在 $C^{x=\varepsilon}$ 中。特别是，V 仍然存在：它与 U 在第 7 步不同，并且由于它们的位置以及缺少输入三角形，它也与 T, R 不同。门 V_2 也仍然存在，因为它不是 T（它是第一个），而且根据当前假设，它与 U, R 不同。

succ(y) 的两个门都没有通过 y：T 是常量，而 V 在消解后仍然存在。引理 6.5(c) 给出 $S_y = \{y\}$。由于 V_2 在消解后仍然存在，且是 V 的唯一后继，它也给出 $S_V = \{V\}$。(b) 部分现在表明，新的后继集合恰好是 y 对应的 $\{V\}$，以及 V 对应的 $\{V_2\}$。

两个门都是非线性的，并且限制之前，输入 y 有两个后继节点，因此获得第一份信用和第二份信用。因此，势能下降至少为 $12 + 2 = 14$。

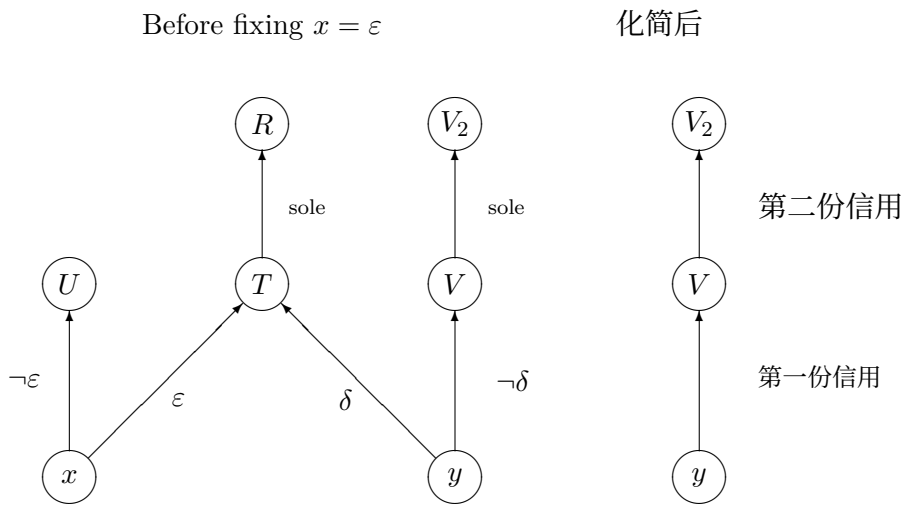


图 1：引理 7.1 的步骤 11 的紧致情形，此时仅消除了 T、U、R，并且 $V_2 \notin \{R, U\}$。边标签给出了接收门处的阻塞值；其他操作数和边均省略。T 和 V 的标记后继节点是唯一的。限制之后，y 和 V 各自只有图中所示的单个后继节点，并且二者 V、V_2 都是非线性的。移除的门贡献十二个单位；新增的两份信用贡献剩余的两个单位。

12. 当.....时，剪除未使用的门 $V_2 = U$。将 x 固定为 U 的阻塞值。然后 U 变为常量，T 被旁路，计数加八。如果 V 在消解后仍然存在，它唯一的后继是

常值门 U。引理 6.5(c) 给出 $S_V = \{V\}$，而 (b) 部分使它在简化电路中没有后继。

它不可能是新输出：原始输出不是 V，因为 V有后继 U，且没有其他节点属于 S_V。因此，V 被剪枝。无论是通过消解还是剪枝移除，它都贡献四个单位，因为它无作用。最后，U_2 被消除，贡献至少三个单位。它不同于先于 U 的 V，也不同于按拓扑序排列的 T，U。总计至少为十五。

13. 在反向配置中获得两个信用。假设 $V_2 = R$ 和 $U_2 \notin \{R, V\}$。在y步骤中，无作用的门 T、V、R 贡献十二个单位。如果还有其他门被消除，总计至少为十五。否则，U、U_2 仍然保留。引理 6.5 给出 $S_x = \{x\}$ 和 $S_U = \{U\}$，与步骤 11 中完全相同。新的后继集合分别为 x 的 $\{U\}$ 和 U的 $\{U_2\}$。输入 x 获得两个信用，共计十四个单位。

14. 排除 $V_2 = R$ 和 $U_2 = V$。 </style>令 ε 为 x 相对于 T的阻塞值，δ 为 y的阻塞值。固定$x = \neg\varepsilon$，它会阻塞 U。由于 U 是坏的，其常量值 c_U 不会阻塞 $V = U_2$。因此，门 V 变为 y的一个文字。当且仅当 $y = \neg\delta$时，它恰好等于 c_V；$y = \neg\delta$是 V的阻塞值。门 T 也变为 y的一个文字，当且仅当 $y = \delta$时，它恰好等于 c_T。

门 R 的操作数为 T、V。c_T和 c_V都不会阻塞它。因此，它在 T处的阻塞值为$\neg c_T$，在 V 处的阻塞值为 $\neg c_V$。当 $y = \delta$时，它的 V操作数为 $\neg c_V$，并会阻塞它。当 $y = \neg\delta$时，它的T操作数为 $\neg c_T$，并会阻塞它。这两种阻塞赋值都会使非线性门 R输出相同的常量。

从 y 出发的每条路径都经过 T 或 V，而这两者都只连接到 R。因此，该余因子与 y无关，这与 (E1) 矛盾。

15. 处理剩余情况。 前面的步骤涵盖了除 $V_2 = R$ 和 $U_2 = R$ 以外的所有情况。在这种情况下，R 会有三个不同的操作数 T、U、V，这对于二元门来说是不可能的。

在每种情况下，选中的输入的扇出至少为二，且势能下降至少为十四。最终归一化无法使势增加到步骤 1，由此证明等式 (1b)。 □

真值表 1汇总了最终的替代情况及其估算。

条件	限制	势能下降或排除
$V_2 \notin \{R, U\}$	$x = \varepsilon$	至少 $12 + 2$；步骤 11
$V_2 = U$	$x = \neg\varepsilon$	至少 15；步骤12
$V_2 = R$, $U_2 \notin \{R, V\}$	$y = \delta$	至少 $12 + 2$；步骤 13
$V_2 = R$, $U_2 = V$	$x = \neg\varepsilon$	与 (E1) 矛盾；步骤 14
$V_2 = R$, $U_2 = R$	None	三个操作数位于 R；步骤 15

表 1：当 U、V 在引理 7.1 中均为坏时的最终替代情况。阻塞值 ε、δ在 T 处的定义见步骤 4。在任一 $12 + 2$ 行中，如果只有三个门消失，则两个信用提供最后两个单位；每增加一个被消去的门，至少提供三个单位。

8 3-SAT 的门数

为了界定组合函数的电路规模，我们在对整个电路施加限制时，将势能下降量相加：对每个块计算单比特步骤，直到其达到 $k + 1$ 自由输入。然后加上由满次数给出的非线性门数量。

定理 8.1（鲁棒块的组合）。 设 G 是一个只读一次复合，其 B 个不相交块是 k-鲁棒函数的限制。每个块至少保留 $k+2$ 个自由输入。记 L 为它们的总数，并将 G 的电路视为恰好具有这些 L 个主输入。每个计算 G 的规范化电路都满足

$$\Psi_2(C) \geq 14\big(L-(k+1)B\big). \tag{2}$$

如果所有块都具有满次数，那么它们的复合满足

$$C_{B_2}(G) \geq \left\lceil \frac{17L-14(k+1)B-3}{7} \right\rceil. \tag{3}$$

第二个断言中的满次数要求是指：在施加所述限制后，块在仍然自由的输入上具有满次数。项 $L-(k+1)B$ 在 (2) 中统计引理 7.1 所适用的单比特消去次数，而 ($3L-3$ 在 (3) 中的额外项则来自满次数所迫使出现的非线性门。

证明。 我们交替进行单比特消去与移除任何达到阈值的块。后一操作不会增加势，因此我们只统计单比特步骤。

1. 在所有块都足够长时消去一个比特。 如果每个块至少有 $k+2$ 个比特，引理 5.8 便给出复合满足 (E2) 和 (S4)。应用引理7.1，并在施加其限制后进行规范化。势至少下降十四，且恰有一个块失去一个自由输入。

2. 移除达到阈值的块。 当某个块首次达到 $k+1$ 个比特时，根据鲁棒性，它仍然是非常量的。如果还有另一个块，就给短块的所有比特赋值，使其在 AND 父节点处取值为一，或在 OR 父节点处取值为零。然后，它的兄弟节点便会在定义树中取代该父节点。在施加这一限制之前，每个叶节点至少有 $k+1$ 个比特，因此引理 5.8 给出 (E1)。此后，剩余的复合依赖于每个自由输入，并且仍满足 (E1)。引理 6.11的收费恒等式具有非负贡献：即使一个非线性门被收费两次，其贡献也为 $4-2=2$。因此，消解不会增加 Ψ_2。引理 6.12表明后续的规范化也同样不会增加它。如果只剩下一个块，则在它达到$k+1$ 个比特时停止。

3. 将各项下降量相加。 一个初始长度为 ℓ 的块在移除或最终停止前，恰好经历 $\ell-(k+1)$ 个单比特步骤。因此，此类步骤的总数为 $L-(k+1)B$。在终端电路中， $D^* \leq D \leq 2A$，其中第二个不等式成立，是因为每一份第一份信用都使用一个非线性门的两个操作数之一。因此 $D+D^* \leq 4A$，而方程（1）给出$\Psi_2 \geq 0$。每个计入的步骤都会使势至少下降十四，而其他所有操作的下降量均非负。这就证明了（2）。

4. 将势转换为电路规模。 根据引理 G，对 4.4 的一个最小电路进行规范化。每个门都是奇偶函数或非线性门，因此将方程（1）重新排列可得

$$7|C| = \Psi_2(C) + 3A(C) + D(C) + D^*(C).$$

满次数和命题 5.5 给出 $A(C) \geq L-1$；代入此上界，并利用两种信用计数均非负，可得

$$7|C| \geq 14\big(L-(k+1)B\big) + 3(L-1) = 17L - 14(k+1)B - 3.$$

由于 $|C|$是整数，除以七并取上取整即可证明（3）。

□

现在，通过将这些块嵌入变量标识符中并应用传递引理，我们得到定理 1.1及其有限形式。

定理 8.2（二进制编码的 3-SAT 的门复杂度）。 设 F_w 为定义 *2.1* 中的判定函数，该函数针对恰好 $m = 2^w - 1$ 个子句，且有 m 个可用变量。其编码有$n = 3m(w + 1)$ 比特。对于不受限制的二进制电路复杂度，沿着这些输入长度，当$w \to \infty$，

$$C_{B_2}(F_w) \geq \frac{17}{7}n - O\left(\frac{n \log\log n}{\log n}\right). \tag{4}$$

更精确地，设整数 r, k 满足 $4 \leq r \leq w - 1$, $3 \leq k \leq r - 2$，且 $2^{k-2} > \log_2(6r(r-1)) + r \log_2 3$。那么

$$C_{B_2}(F_w) \geq n + \left\lceil \frac{(30r - 42(k+1))(m - 2^r) - 3}{7} \right\rceil. \tag{5}$$

命题 *5.10* 中的加权模检验给出的限制 $C_{B_2}(F_w) \geq (17/7)n - O(n/\sqrt{\log n})$。

证明。 我们根据嵌入后剩余的正子句数量得到一个有限界；该数量的上界与所选检验无关；再选择参数，使误差为次线性。

1.构造受限 *SAT* 函数。 使用命题 k给出的 g 对 r 比特的全次数鲁棒检验，5.9。引理 3.1 产生 $M = m - |g^{-1}(0)|$ 个正子句，从而得到 $B = 3M$ 个不相交块和 $L = 3Mr$ 个自由位。用两个二元或门连接每个子句中的三个项，再用一棵二元与树合并这些子句。条件 $r \geq k + 2$ 使引理 5.8能够验证每个自由位都是必要的。

2. 转移复合下界。 引理 4.6 将 $n - L$ 个被移除的门添加到（3）中。代入$L = 3Mr$ 和 $B = 3M$ 可得

$$\begin{aligned} C_{B_2}(F_w) &\geq n - L + \left\lceil \frac{17L - 14(k+1)B - 3}{7} \right\rceil \\ &= n + \left\lceil \frac{(30r - 42(k+1))M - 3}{7} \right\rceil. \end{aligned} \tag{6}$$

3. 推导一致有限不等式。由于 $|g^{-1}(0)| \leq 2^r$，我们有 $M \geq m - 2^r$。如果 $30r - 42(k+1) \geq 0$, 则将该下界代入（6）中的 M，得到（5）。如果该系数为负，则它至多为 -6，因为它是六的倍数。此外， $r \leq w - 1$ 意味着 $m - 2^r \geq 1$。（5）中上取整内的分数随后至多为 $-9/7$, 其上取整为 -1。在这种情况下，引理 2.4 和 3.2 中的初等下界 $C_{B_2}(F_w) \geq n - 1$ 已足够。

4. 保留几乎所有描述位。取 $r = w - \lceil \text{对数}_2\, w \rceil - 1$。则

$$2^r \leq \frac{2^w}{2w} = \frac{m+1}{2w} \leq \frac{m}{w}, \qquad M = m - O(m/w).$$

使用 $n = 3m(w + 1)$ 和 $L = 3Mr$，固定比特的数量为

$$n - L = 3m(w + 1 - r) + 3(m - M)r = O(m \log w) = O(n \log w/w).$$

第一项统计每个文字字段中固定的高位标识符位和符号位；第二项统计辅助子句中额外固定的低位标识符位。

5. 选择对数阈值并估计损失。 命题 5.9 中计数假设右侧的数量级为 r。因此，最小的可接受整数 k 为 $\log_2 r + O(1)$。对于足够大的 w，有 $r \geq k + 2$，且所有有限假设均成立。由于上取整不小于其参数，式（6）的第一行给出

$$C_{B_2}(F_w) \geq \frac{17}{7}n - \frac{10}{7}(n - L) - 2(k+1)B - \frac{3}{7}.$$

现在 $B = 3M \le 3m = n/(w+1)$。步骤 4 和 $k = O(\log w)$ 使总损失为 $O(n\log w/w)$。最后 $\log_2 n = w + O(\log w)$，因此这是 $O(n \log\log n/\log n)$。这就证明了式（4）。

6.使用加权模检验。保持 r 的选择不变，但使用命题 5.10，其阈值为 $k = O(\sqrt{r})$。对于足够大的 w，要求 $r \ge k+2$ 再次成立。式（6）的推导仅使用了鲁棒性和满次数，因此同样适用于此检验。现在损失为

$$O(n \log w/w + nk/w) = O(n/\sqrt{\log n}).$$

命题5.10 中选定的剩余类规定了引理3.1中的禁用标识符。

□

8.1 形式化与可复现性

Lean 证明可在 Zenodo [14] 上获取。随附的补充材料提供了复现验证的说明，以及手稿中的结果与形式化定理之间的对应关系。

Lean 求值器实现了定义2.1，包括拒绝标识符零。电路既表示为有序门列表（每个门仅引用较早的信号），也表示为具有任意顶点标签、共享前驱和指定输出的无环图。单目门和常量门使用忽略未使用参数的真值表；这些参数可以用任意主输入填充，而无需增加门或产生环。两种表示计算出相同的函数，并且图模型的定理在定理8.2的假设下给出了有限界（5）以及两个渐近估计。

门消除证明会记录哪些输入仍然自由，并要求电路在应用势函数界时不得使用该集合以外的输入，参见定理 8.1。实现会统计信号作为门参数或输出出现的次数；另有引理证明，对于规范化电路，其信用计数与定义 6.6 和 6.8 一致。

加权模构造通过布尔值列表和一元计数器实现，每个计数单位对应一个符号。对于这种表示，形式化证明给出了选取素数和求出剩余类所需基本操作次数的多项式界。命题 $O(rp)$ 中的界5.10 则只计算给定素数后求出剩余类所需的操作。

本开发使用 Lean 4.35.0 和 mathlib 库的一个固定修订版本，审计确认这些证明仅使用标准 Lean 公理 `propext`、 `Classical.choice` 和`Quot.sound`。

9 结论

定理 8.2 为定义 $(17/7)n - O(n \log\log n/\log n)$ 中的二进制 SAT 族给出了下界，门数为2.1，其中对公式描述的每一位都计数，并允许任意二元门、深度和共享。

该嵌入将布尔测试放入变量标识符中，并保留 $n - o(n)$ 个描述位；即使不同测试之间共享电路中的门，加权门数仍然适用。仅靠门移除只能得到十二单位的势，因此需要新增信用来补足达到十四所需的两个单位。随后，满次数所需的非线性门便给出系数 $17/7$。

后续工作可以寻找显式测试，使其在固定更多输入后仍适用于门消除，从而降低 $O(n/\sqrt{\log n})$ 损失。改变子句与可用变量的比例，或许能找到既保留标识符测试、又几乎保留全部描述位的嵌入。重复变量出现带来的约束也可能进一步提高门数。形式化有限不等式为评估这些改进提供了基准。

A作者贡献。作者贡献相同，并列第一作者 p.

AI 使用披露。 AI 工具（Claude Code、Codex）协助完成了稿件结构安排、文献检索、Lean 验证、参考文献核查，以及 LaTeX 和证明的格式整理。证明思路由作者提出，作者对稿件内容、数学论证和研究结果承担全部责任。

参考文献

[1] L. Trevisan。《第3讲》讲义。CS254：计算复杂性，斯坦福大学，2014年。2014年1月14日。 https://theory.stanford.edu/~trevisan/cs254-14/lecture03.pdf。[2] C. P. Schnorr。《布尔函数复杂度的两个线性下界》。《计算》，13(2):155–171，1974年。 https://doi.org/10.1007/BF02246615。[3] L. J. Stockmeyer。关于某些对称布尔函数的组合复杂度。《数学系统理论》，10:323–336，1977年。 https://doi.org/10.1007/BF01683282。[4] W. J. Paul。布尔函数组合复杂度的一个 $2.5n$下界。《SIAM计算杂志》，6(3):427–443，1977年。 https://doi.org/10.1137/0206030。[5] N. Blum。需要 $3n$ 网络规模的布尔函数。《理论计算机科学》，28:337–345，1984年。 https://doi.org/10.1016/0304-3975(83)90029-4。[6] M. G. Find、A. Golovnev、E. A. Hirsch和A. S. Kulikov。改进 $3n$ 电路复杂度下界。《计算复杂性》，32，2023年。文章13。 https://doi.org/10.1007/s00037-023-00246-9。[7] J. Li和T. Yang。显式函数的 $3.1n - o$（n）电路复杂度下界。载于第54届ACM SIGACT计算理论年会论文集（STOC 2022），第1180–1193页，2022年。 https://doi.org/10.1145/3519935.3519976。[8] O. S. Mishra和R. Santhanam。针对一般布尔电路的一个显式 $4n - O$（$\log n$）规模下界。报告TR26-260，电子计算复杂性研讨会，2026。修订版 1，2026年11月3日。 https://eccc.weizmann.ac.il/report/2026/260/revision/1/。[9] O. Lachish和R. Raz。布尔电路的显式 $4.5n - o$（n）下界。载于第33届ACM计算理论年会论文集（STOC 2001），第399–408页，2001年。 https://doi.org/10.1145/380752.380832。[10] U. Zwick。在单调二元布尔函数基上，某些对称布尔函数组合复杂度的一个 $4n$ 下界。《SIAM计算杂志》，20(3):499–505，1991年。 https://doi.org/10.1137/0220032。[11] A. Golovnev、A. S. Kulikov、A. V. Smal和S. Tamaki。门消除：电路规模下界与#SAT上界。《理论计算机科学》，719:46–63，2018年。 https://doi.org/10.1016/j.tcs.2017.11.008。[12] A. Kojevnikov和A. S. Kulikov。布尔函数的电路复杂度与乘法复杂度。载于《程序、证明与过程》（CiE 2010），《计算机科学讲义》第6158卷，第239–245页，2010年。 https://doi.org/10.1007/978-3-642-13962-8_27。

[13] C. P. Schnorr。布尔函数的乘法复杂度。载于《应用代数、代数算法与纠错码》（AAECC-6），《计算机科学讲义》第357卷，第45–58页，1989年。 https://doi.org/10.1007/3-540-51083-4_47。[14] T. Yianni和S. Allahyar。3-SAT无约束电路复杂度的首次下界改进。迈向P $\neq$ NP。版本 v5，Zenodo，2026。2026年11月3日。预印本及随附的Lean 源代码，包括 17/7 证明软件包。 https://doi.org/10.5281/zenodo.23925452。[15] C. Carlet。《密码学与编码理论中的布尔函数》。剑桥大学出版社，2021年。 https://doi.org/10.1017/9781108606806。[16] E. Kushilevitz和N. Nisan。《通信复杂度》。剑桥大学出版社，1997年。 https://doi.org/10.1017/CBO9780511574948。[17] V. Kabanets。近似 k-wise独立性与困难布尔函数。载于LATIN 2000：理论信息学，《计算机科学讲义》第1776卷，第197–206页，2000年。 https://doi.org/10.1007/10719839_20。[18] P. Savický和S. Žák。1-分支程序的一个大下界。报告TR96-036，电子计算复杂性研讨会，1996年。修订版 1，1996年6月26日。https://eccc.weizmann.ac.il/report/1996/036/revision/1/。[19] É. Balandraud。通过多项式方法的 $\mathbb{F}_p$ 加法定理。arXiv:1702.06419，2017年。 https://doi.org/10.48550/arXiv.1702.06419。[20] P. L. Tchebichef。《关于素数的回忆录》。《纯粹与应用数学杂志》，17:366–390，1852年。第一辑。 https://www.numdam.org/item/JMPA_1852_1_17__366_0/。