arXiv:2603.09379v1 [cs.CC] 10 Mar 2026

真值表扰动下电路规模变化的一个简单构造性界

Kirill Krinkin 帕福斯尼亚
波利斯大学
kirill@krinkin.com

摘要

已有关于最小电路规模问题的研究隐含指出，在单点真值表扰动下，最优电路规模的变化至多为 $O(n)$。本文针对任意固定的有限完备基（其中门的代价均为单位代价），明确给出这一界；通过望远镜求和论证将其推广至一般汉明距离，并利用 SAT 推导的精确电路规模，在 AIG 基中对 222 个 NPN 等价类中的 220 个进行穷举验证。在 987 条变异边中，观察到的最大差值为 $4 = n$，证实该界对 AIG 是紧的（ $n = 4$ ）。

1 引言

已有关于最小电路规模问题（MCSP）的研究隐含指出，在单点扰动下，最优电路规模的变化至多为 $O(n)$；这一结果被用作集中性论证中的有界差分要素 [4]。本文将这一现象提炼为针对任意固定有限完备基的独立结论，明确表述相应的汉明距离界，并以 AIG 模型中的精确小规模证据作为补充。

布尔函数 f 在完备门基 B 上的最优电路规模 opt(f, B) 是衡量计算复杂性的基本指标。一个自然的问题是：该指标对函数的小幅变化有多敏感?

我们注意到，改变布尔函数真值表中的单个位，最优电路规模至多改变 $O(n)$ 个门，其中 n 是变量的数量。该界是构造性的：我们明确给出了修改后的电路。我们使用 SAT 验证的精确电路规模，对 AIG 基中的 $n = 4$ 进行了穷举验证，并表明在 AIG 基中，该界在 $n = 4$ 处是紧的。穷举验证仅限于 $n = 4$ 和一种电路模型；因此，应将其视为对该构造及局部紧性的验证，而非渐近性证据。

2 预备知识

n 个变量的 布尔函数 是一个映射 f: $\{0,1\}^n \to \{0,1\}$。其 真值表 tt(f) 是一个长度为 2^n 的二进制字符串，按输入的字典序列出输出值。

两个真值表之间的汉明距离 d_H(tt(f), tt(f'))是它们取值不同的位置数量。

在门基 B 上的电路是一个有向无环图，其内部节点由来自 B的门标记，其源是输入变量 $x_0, \ldots, x_{n-1}$。电路的规模是

内部节点（门）的数量。最优电路规模$\mathrm{opt}(f, B)$是基 B 中所有计算 f [5]的电路的最小规模。

若每个布尔函数都能由基 B 上的电路计算，则称该基为完备的。在本文中，我们假设 B 是有限的，且每个门的代价均为单位代价。我们考虑两个具体的基：

- **AIG基：** $\{$与(x, y) $\neg x\}$，并允许免费反相——每个门的输出都可免费以两种极性使用。电路规模仅计与门。
- **AON基：** $\{$与(x, y)，或(x, y) $\neg x\}$。电路规模计与门、或门和非门。

3 主要结果

定理1。对于任意固定的有限完备门基 B，其门均为单位代价；对于任意两个以 n 个变量为自变量的布尔函数 f、f'，

$$|\mathrm{opt}(f, B) - \mathrm{opt}(f', B)| \;\le\; c_B \cdot n \cdot d_H(\mathrm{tt}(f), \mathrm{tt}(f')),$$

其中 c_B 是仅取决于 B的常数。

证明。只需证明 $d_H = 1$ 的情形。对于一般的 d_H，设 $f = f_0$，f_1，……，$f_{d_H} = f'$ 是一列函数，其中每一对相邻函数恰有一个真值表位不同。在每一步应用 $d_H = 1$ 界并求和，得到：

$$|\mathrm{opt}(f, B) - \mathrm{opt}(f', B)| \;\le\; \sum_{i=1}^{d_H} |\mathrm{opt}(f_{i-1}, B) - \mathrm{opt}(f_i, B)| \;\le\; c_B \cdot n \cdot d_H.$$

假设 f 和 f' 仅在输入 $x^* \in \{0,1\}^n$ 处不同，其中 $f(x^*) = 0$，且 $f'(x^*) = 1$。（情形 $f(x^*) = 1$ 可通过交换 f 和 f' 对称地得到。）

的上界$\mathrm{opt}(f')$。给定一个计算 f 的最优电路 S，其规模为 $\mathrm{opt}(f)$，按如下方式构造一个计算 f' 的电路。

步骤 *1*：相等检测器。构造一个子电路 $\mathrm{eq}(x, x^*)$，当且仅当 $x = x^*$ 时输出 1。这需要对每个 $i \in \{0, \ldots, n-1\}$ 检查 $x_i = x_i^*$，并将结果相与。在 AIG 基中，每次比较都对应一个文字（若 $x_i^* = 0$，取反免费），因此与链需要 $n-1$ 个门。在一般完备基 B 中，实现与和非各需要 c_B 个门，因此检测器的规模至多为 $c_B \cdot (n-1)$。（对于任意固定的有限完备基 B，存在常数 a_B，$b_B > 0$，使得修复构件——检测器加输出校正——的规模至多为 $a_B n + b_B$ 个门。对于 $n \ge 1$，这至多为 $c_B \cdot n$，其中 $c_B := a_B + b_B$。）

步骤 *2*：输出校正。计算

$$f'(x) = f(x) \vee \mathrm{eq}(x, x^*).$$

在 AIG 基中：$f'(x) = \neg(\neg f(x) \wedge \neg \mathrm{eq}(x, x^*))$，成本为 1 个与门（取反免费）。在一般基中，或门的成本最多为 c_B 个门。

总计：$\mathrm{opt}(f') \le \mathrm{opt}(f) + c_B \cdot n$。

上界：$\mathrm{opt}(f)$。给定一个用于 f' 的最优电路 S'，构造：

$$f(x) = f'(x) \wedge \neg \mathrm{eq}(x, x^*).$$

这是正确的：当 $x \neq x^*$ 时，eq $= 0$ 与 $f(x) = f'(x)$；当 $x = x^*$ 时，$f(x) = f'(x^*) \wedge 0 = 0 = f(x^*)$。检测器会重复使用；在 AIG 中，与门的成本为 1 个门（eq 的取反不产生额外成本），在一般情况下则为 c_B 个门。

总计：$\text{opt}(f) \leq \text{opt}(f') + c_B \cdot n$。

结合两个不等式：$|\text{opt}(f) - \text{opt}(f')| \leq c_B \cdot n$。 □

备注。对于 AIG 基，检测器需要 $n - 1$ 个与门（取反免费），输出校正需要 1 个门，因此得到 $c_B = 1$，界为 $n \cdot d_H$。对于一般基 B，常数 c_B 取决于在 B 中模拟与和非的代价。

4 紧性

在 AIG 基中，定理1的界在 $n = 4$ 处达到。NPN类 0x0001（单最小项函数，即对所有输入求与）满足 $\text{opt}_{\text{AIG}} = 3$，而 NPN类 0x0180 满足 $\text{opt}_{\text{AIG}} = 7$。这两个类通过一次单比特真值表变异相连，因此 $|\text{opt}(f) - \text{opt}(f')| = 4 = n$。

一个开放问题是，是否存在一个与 n 无关的常数 C，使得对于 $d_H = 1$，$|\text{opt}(f) - \text{opt}(f')| \leq C$。在 $n = 4$ 的实证证据表明，典型扰动远小于最坏情况：94.7% 的变异边具有 $|\Delta\text{opt}| \leq 2$，平均绝对差为 1.03。目前尚无已知的渐近下界族；对于无穷多个 n，是否存在 $\Omega(n)$ 的单比特间隙仍是开放问题。

5 计算验证

我们针对 AIG 基，在 $n = 4$ 处通过穷举枚举验证了该界。我们计算了所有 222 个四变量布尔函数 NPN 等价类的最优电路规模：其中 220 个类的精确值经 SAT 验证，其中 136 个通过穷举枚举 [3], 84 个通过基于 SAT 的精确综合 [1]，并采用立方与征服策略 [2]。剩余 2 个类获得了改进的上界（在 $k = 9$ 处 SAT 超时，在 $k = 10$ 处 SAT 得到确认）。

当一个类中的某个函数与另一个类中的某个函数仅有一位真值表位不同，变异图便在这两个 NPN 类之间连一条边。在两端的精确最优$_{\text{AIG}}$ 值均已知的 987 条变异边中，观察到的最大差值为 $4 = n$，这证实对于 AIG 基，该界在 $n = 4$ 处是紧的。

$\lvert\Delta$最优$_{\text{AIG}}\rvert$	边	%
0	300	30.4
1	414	41.9
2	221	22.4
3	45	4.6
4	7	0.7
总计	987	100.0

表1：具有精确最优规模的 NPN-4 类之间的变异边上，$|\Delta\text{最优}_{\text{AIG}}|$ 的分布。

达到 $|\Delta\text{opt}| = n = 4$ 的七条边，都连接着一个最优规模为 3 的函数和一个最优规模为 7 的函数。

6 讨论

该界说明，彼此接近的函数（按汉明距离衡量）具有可证明地接近的电路复杂度。

复杂度估计。 作为理论推论，该界给出一个最坏情况传递不等式：$\mathrm{opt}(f') \in [\mathrm{opt}(f) - c_B n,\ \mathrm{opt}(f) + c_B n]$，适用于 f 的任意汉明邻居 f'。

经验紧致性。 在 $n = 4$ 处，变异边上的平均绝对差为 1.03，远低于 $n = 4$ 的最坏情况界。这一差距在更大的 n 下是否仍然存在，是一个开放问题。具体而言：是否存在函数对 $(f_n,\ f_n')$ 的显式族，使得 $d_H(\mathrm{tt}(f_n),\ \mathrm{tt}(f_n')) = 1$且 $|\mathrm{opt}(f_n) - \mathrm{opt}(f_n')| = \Omega(n)$?

基依赖性。 常数 c_B 反映了在基 B 中实现相等检测器与输出校正的开销。对于具有免费反相的基（AIG），$c_B = 1$；对于没有免费反相的基，c_B 随实现与和非的代价而增长。对特定基而言，对 n 的线性依赖能否改进为次线性，仍是开放问题。

数据可用性

变异图、所有 222 个 NPN-4 类的最优电路规模以及验证脚本可在 https://github.com/krinkin/bounds 获取（提交时标记为 v1.0）。

参考文献

[1] A. Kojevnikov、A. S. Kulikov 和 G. Yaroslavtsev。使用 SAT 求解器寻找高效电路。载于 *SAT 2009*，LNCS 5584，第 32–44 页。Springer，2009 年。[2] M. J. H. Heule、O. Kull mann、S. Wieringa 和 A. Biere。立方体与征服：通过前瞻引导 CDCL SAT 求解器。载于*HVC 2011*，LNCS 7261，第 50–65 页。Springer，2012 年。[3]K. Krinkin。单位间隙：布尔电路中的共享如何运作。*arXiv* 预印本，arXiv:2603.08033，2026 年。[4] A. Golovnev、R. Ilango、R. Impagliazzo、V. Kabanets、A. Kolokolova 和 A. Tal。通过硬币问题证明针对 MCSP 的 $AC^0[p]$下界。载于第 *46* 届国际自动机、语言与编程研讨会（*ICALP*）论文集，LIPIcs 第 132 卷，第 66:1–66:15 页，2019 年。

[5] S.Jukna. 布尔函数复杂度：进展与前沿. Springer, 2012.