一种通过有界宽度电路研究电路下界的方法

Hiroki Morizumi日本岛根大学
morizumi@cis.shimane-u.ac.jp

arXiv:2305.00794v1 [cs.CC] 1 May 2023

摘要

本文研究一种通过有界宽度电路研究电路下界的方法。该方法包括两个步骤：(i) 将电路转换为（确定性或非确定性）有界宽度电路。(ii) 证明有界宽度电路的下界。

对于第二步，我们证明存在一个显式布尔函数 f，满足如下性质：如果一个规模为 s、宽度为 w 的非确定性电路计算 f，那么 $w = \Omega(\frac{n^4}{4^{\frac{s}{n}}s^3}) - \log_2 s$。对于第一步，我们给出了一些观察结果，其中包括转换为有界宽度电路与标准卵石游戏之间的关系。

1 引言

证明电路下界是计算复杂性理论的核心课题之一。本文提出并研究一种通过有界宽度电路证明电路下界的方法。该方法分为两个步骤。

1. 将电路转换为（确定性或非确定性）有界宽度电路。
2. 证明有界宽度电路的下界。

本文针对每个步骤都给出了一些结果。

注：电路中宽度的定义见第 2.1 节。我们也考虑非确定性情形下的有界宽度电路。据我们所知，尚无论文研究过非确定性有界宽度电路，敬请注意我们对非确定性有界宽度电路的定义。详情见第 2.2 节。

1.1 有界宽度电路的下界

我们首先证明有界宽度电路的下界，这与该方法的第二步相关。关于下界，我们的结果如下述定理所示。

定理 1。存在一个显式布尔函数 f，如下所示：如果一个规模为 s、宽度为 w 的非确定性电路计算 f，那么

$$w = \Omega(\frac{n^4}{4^{\frac{s}{n}}s^3}) - \frac{\log_2 s}{2}.$$

根据该定理，我们可以如下得到有界宽度电路的下界，例如。

推论 2. 存在一个显式布尔函数 f，任何规模为 $O(n)$、宽度为 $o(n)$ 的非确定性电路都无法计算它。

推论 3. 存在一个显式布尔函数 f，任何规模为 $O(n \log\log n)$、宽度为 $n^{\log^{\omega(1)} n}$ 的非确定性电路都无法计算它。

我们的下界证明基于分支程序下界的一项已知结果，该结果见第 3.1 节。

有界宽度电路。尽管有界宽度电路是本文主要目标（即研究电路下界的方法）中的一个中间模型，但有界宽度电路的下界本身也可能具有独立的研究价值。电路的宽度对应于图灵机所用的空间，而非一致 SC 是一类判定问题：这些问题可由规模为多项式、宽度为多对数且扇入为 2 的布尔电路求解。（SC 是一类判定问题：这些问题可由同时使用多项式时间和多对数空间的图灵机求解。）然而，据我们所知，此前尚未有人讨论有界宽度电路的下界。

相关问题。证明存在一个显式布尔函数 f，它无法由任何规模为 $O(n)$、深度为 $O(\log n)$ 的（确定性）电路计算，是电路复杂性领域一个切实可行的目标。推论 2 以更强的形式解决了这一公开问题的宽度变体。证明一般电路的超线性规模下界是电路复杂性领域的核心问题。推论 2 表明，如果宽度受到稍微严格的限制，我们就能证明超线性下界。

1.2 转换为有界宽度电路

我们在上一小节中证明了有界宽度电路的下界。定理 1 展示了该方法第一步中转换的目标。（该目标是当前目标，我们希望得到更强的下界。）根据定理 1，我们得到以下推论。

推论 4. 如果电路类 $\mathcal{C}$ 中的任意电路都可以转换为一个不满足

$$w = \Omega(\frac{n^4}{4^{\frac{s}{n}} s^3}) - \frac{\log_2 s}{2},$$

那么就存在一个显式布尔函数 f，它无法由 $\mathcal{C}$ 中的任何电路计算。

以下推论给出了更明确的表述。

推论 5. 如果电路类 $\mathcal{C}$ 中的任意电路都可以转换为一个满足规模 $O(n \log\log n)$ 和宽度 $n^{\log^{\omega(1)} n}$ 的非确定性电路，那么就存在一个显式布尔函数 f，它无法由 $\mathcal{C}$ 中的任何电路计算。

在第 4 节中，我们给出一些观察结果，其中包括将电路转换为有界宽度电路与标准卵石游戏之间的关系。

1.3 论文结构

第 3 节和第 4 节分别对应第 1.1 节和第 1.2 节。我们关于下界的证明概要还提供了一种用于非确定性有界宽度电路的可满足性算法。我们将在第 5 节提及该算法。

2 预备知识

2.1 电路

电路在形式上定义为有向无环图。入度为 0 的节点称为输入端，每个输入端都标记一个变量或常量 0 或 1。其他节点

称为门，每个门都标记一个布尔函数。节点的扇入是该节点的入度，节点的扇出是该节点的出度。本文中的门包括扇入为 2 的与门、扇入为 2 的或门，以及非门。图中有一个特定节点称为输出。电路的规模是电路中门的数量。

当我们考虑电路的宽度时，会临时在电路中插入复制门。复制门是一种虚拟门，只会输出其输入。若电路中的门集可以划分为若干称为层的子集，并且电路中的每条边都连接相邻的层，则称该电路为分层电路。注意，通过在跨越若干层的每条边上插入复制门，任何电路都可以自然地转换为分层电路。一层的宽度是该层中的门数。电路的宽度是电路所有层的最大宽度。

非确定性电路是一个具有实际输入（$x_1, \ldots, x_n$） $\in \{0,1\}^n$ 以及一些额外输入（$y_1, \ldots, y_m$） $\in \{0,1\}^m$ （称为猜测输入）的电路。非确定性电路按如下方式计算布尔函数 f：对于 $x \in \{0,1\}^n$, $f(x) = 1$，当且仅当存在一种猜测输入 $\{y_1, \ldots, y_m\}$ 的赋值使得电路输出 1。我们将不含猜测输入的电路称为确定性电路，以便与非确定性电路区分。

2.2 非确定性有界宽度电路的定义

据我们所知，尚无论文研究非确定性有界宽度电路。我们还需要注意，猜测输入的出现会敏感地影响电路的计算能力。我们将标记为猜测输入的节点数限制为至多一个，而不限制标记为实际输入的节点数。（若宽度无界，这一限制便毫无意义。）此外，在非确定性图灵机中，每个非确定性选择都不能重复；如果图灵机的空间受限，图灵机也无法存储所有非确定性选择。

2.3 分支程序

非确定性分支程序是一个有向无环图。出度非零的节点称为内部节点，并标记为一个变量。出度为 0 的节点称为汇点，并标记为 0 或 1。每个内部节点的出边都标记为 0 或 1。图中有一个特定节点，称为起始节点。当且仅当至少存在一条路径通向标记为 1 的汇点时，非确定性分支程序的输出为 1。分支程序的规模是其节点数。若每条路径上每个变量出现至多 k 次，则称该分支程序为语法读入-k-次。

3 有界宽度电路的下界

3.1 分支程序的下界

为了证明定理 1，我们使用以下定理。

定理 6（[2]）。存在一个显式布尔函数 f，使得每个用于计算 f 的非确定性语法读-k-次分支程序的规模均为 $\exp(\Omega(\frac{n}{4^k k^3}))$。

在本文中，我们用 f_{BRS} 表示该定理中的布尔函数。

3.2 定理 1 的证明

在本小节中，我们证明定理 1。首先，我们定义电路的读-k次概念。如果一个变量标记的节点数至多为 k，则称该变量在电路中被读-k次。如果电路中的每个实际输入都被读-k次，则称该电路为读-k次电路。（注意，由于电路的宽度有界，“读-k次”这一说法是有意义的。）

引理 7. 任意规模为 s 、宽度为 w 的非确定性读-k次电路，都可以转换为规模为 $4^w s$的非确定性语法读-k次分支程序。

证明。从一层传递到下一层的取值（0 或 1）数量至多为 w。对于每种至多包含 2^w 个 0 和 1 的组合，我们在构造的分支程序中准备一个节点。从电路到分支程序的直接转换足以证明该引理。

□

如果电路的规模为 s，那么标记为实际输入的节点数量至多为 $s+1$。因此，平均而言，每个实际输入对应的节点数量至多为 $\frac{s+1}{n}$。然而，该电路不一定是读-$\frac{s+1}{n}$-次的。这是此证明中最困难的地方。我们通过布尔函数 f 的定义来解决这一难点。

我们将 $f(x_1, x_2, \ldots, x_{2n}, z_1, z_2, \ldots, z_{2n})$ 定义如下。如果 $\sum_{i=1}^{2n} z_i \neq n$，那么 $f = 0$。否则，$f = f_{BRS}$，且这 n 个输入变量是满足 $z_i = 1$ 的 x_i。

定理 1 的证明。设 C 是一个计算 $f(x_1, x_2, \ldots, x_{2n}, z_1, z_2, \ldots, z_{2n})$ 的非确定性电路，且 s 和 w 分别是 C 的规模和宽度。我们从 $x_1, \ldots, x_{2n}$ 中选取 n 个变量，使得每个被选中的变量在 C 中恰好被读取 $\frac{s}{n}$ 次。如果 x_i 被选作 $1 \leq i \leq 2n$，我们就将 z_i 赋值为 1；否则赋值为 0。对于未被选作 $1 \leq i \leq 2n$ 的 x_i，我们任意赋值。设 C' 是得到的每个变量恰好被读取 $\frac{s}{n}$ 次的电路，且 s' 和 w' 分别是 C' 的规模和宽度。C' 计算 f_{BRS}，且 $s' \leq s$ 和 $w' \leq w$。由引理 7 和定理 6,

$$\begin{aligned}
4^{w'} s' &= \exp(\Omega(\frac{n}{4^{\frac{s}{n}}(\frac{s}{n})^3})) \\
4^w s &= \exp(\Omega(\frac{n}{4^{\frac{s}{n}}(\frac{s}{n})^3})) \\
2w + \log_2 s &= \Omega(\frac{n^4}{4^{\frac{s}{n}} s^3}) \\
w &= \Omega(\frac{n^4}{4^{\frac{s}{n}} s^3}) - \frac{\log_2 s}{2}.
\end{aligned}$$

□

4 转换为有界宽度电路

我们可以在推论 4 和推论 5 中选择各种电路作为电路类。本节首先展示一个从受限电路转换为有界宽度电路的例子，并证明转换为有界宽度电路与标准卵石游戏之间的关系。

4.1 从 $O(n)$ 规模、 $O(\log n)$ 深度电路进行转换

证明存在一个显式布尔函数 f，它无法由任何规模为 $O(n)$、深度为 $O(\log n)$ 的确定性电路计算，是电路复杂性领域一个切实可行的目标。下面的定理给出了从受限电路转换为有界宽度电路的一个例子。

定理 8. 任意规模为 $O(n)$、深度为 $O(\log n)$ 的确定性电路，都可以转换为规模为 $O(n^{1+\epsilon})$、宽度为 $O(n/\log\log n)$ 的确定性电路。

证明。设 C 是一个规模为 $O(n)$、深度为 $O(\log n)$ 的电路。众所周知，我们可以在 C 中找到 $O(n/\log\log n)$ 条边，移除这些边后，所得电路的深度至多为 $\epsilon \log n$（[5], 第 14.4.3 节）。我们构造一个电路，逐条计算 $O(n/\log\log n)$ 条边的值。

□

尽管我们可以通过定理 8 得到一个有界宽度电路，但对于我们当前的目标而言，该电路规模过大；这个目标已在第 1.2 节中提及。

4.2 卵石游戏与转换

本文考察的卵石游戏如下。（定义参见论文 [4]。）

定义 9（卵石游戏）。设 G 是一个具有唯一汇点 z 的有向无环图。在 G 上进行的黑白卵石游戏如下所述，是一个单人游戏。在任意时刻 t，我们在 G 的顶点上有一个配置 $\mathbb{P}_t = (B_t, W_t)$，其中包含黑色卵石 B_t 和白色卵石 W_t，每个顶点至多一个卵石。游戏规则如下：

1. 如果空顶点 v 的所有直接前驱上都有棋子，则可以在 v 上放置一个黑色棋子。特别地，始终可以在源点上放置一个黑色棋子。
2. 可以随时从任意顶点移除一个黑色卵石。
3. 白色卵石可以随时放置在任何空顶点上。
4. 如果一个带有白色卵石的顶点 v 的所有直接前驱上都放置了卵石，则可以移除顶点 v 上的白色卵石。特别地，始终可以从源点上移除白色卵石。

对 G 的黑白卵石摆放是一个卵石配置序列 $\mathcal{P} = \{\mathbb{P}_0, \ldots, \mathbb{P}_\tau\}$，满足 $\mathbb{P}_0 = (\emptyset, \emptyset)$、$\mathbb{P}_\tau = (\{z\}, \emptyset)$，并且对于所有 $t \in [\tau]$，$\mathbb{P}_t$ 都可以通过上述规则之一从 $\mathbb{P}_{t-1}$ 推出。卵石摆放 $\mathcal{P} = \{\mathbb{P}_0, \ldots, \mathbb{P}_\tau\}$ 的时间就是 $\mathsf{time}(\mathcal{P}) = \tau$，空间则是 $\mathsf{space}(\mathcal{P}) = \max_{0 \le t \le \tau} \{|B_t \cup W_t|\}$。黑色卵石摆放是仅使用黑色卵石的卵石摆放，也就是说，对所有 t，都有 $W_t = \emptyset$。

由于电路被定义为有向无环图，我们可以考虑用于电路的卵石游戏。（电路中的输入端和输出分别是图中的源顶点和唯一汇点。）以下两个定理展示了卵石游戏与转换为有界宽度电路之间的关系。

定理 10. 若确定性电路 C存在一个黑色卵石摆放 $\mathcal{P}$，则可将该电路 C转换为规模为 $\mathsf{time}(\mathcal{P})$、宽度为 $\mathsf{space}(\mathcal{P})$ 的确定性电路。

证明。对于黑色卵石的放置和移除，按如下方式构造电路 s:

1. 若放置一个黑色卵石，则添加一个输入节点或门节点，并适当地将其与其他节点连接。
2. 若移除一个黑色卵石，则不做任何操作。

所得电路与 C 显然计算相同的布尔函数。电路的规模至多等于黑色卵石的放置次数，而该次数至多为 $\mathsf{time}(\mathcal{P})$。对于时间 t，只有当放置的黑色卵石直到 t都未被移除时，添加的输入端和门才会一直使用到 t，并且仅从 $t+1$ 使用。因此，电路中时间 t 对应层的宽度至多等于当前黑色卵石的数量（即 $|B_t|$），电路的宽度至多为 $\mathsf{space}(\mathcal{P})$。 □

定理 11. 如果确定性电路 C存在黑白卵石摆放 $\mathcal{P}$，那么电路C 可以转换为规模为 $c \cdot \mathsf{time}(\mathcal{P})$、宽度为 $\mathsf{space}(\mathcal{P}) + 1$ 的非确定性电路，其中 c为常量。

证明。对于黑色卵石和白色卵石的每次放置与移除，按如下方式构造电路：

1. 如果放置一颗黑色卵石，则添加一个实际输入节点或门节点，并按适当方式与其他节点连接。

2. 如果移除一颗黑色卵石，则不做任何操作。 3. 如果放置一颗白色卵石，则添加一个猜测输入节点（标记为一个新的猜测变量）。 4. 如果移除一颗白色卵石，则添加若干门节点（特殊情况下也添加输入节点），以检查猜测输入是否正确。（详情如下。）

所得电路满足定理的条件，其证明方式与定理 10 类似。

在所得电路中，每个猜测输入都会猜测相应门（或特殊情况下的输入端）的输出。在情况 4 中，会检查猜测输入的正确性。如果猜测不正确，则强制将电路的输出设为 0。根据非确定性电路的定义，这保证了所得电路计算出正确的布尔函数。在情况 4 中，新增门的数量至多为常量，并且电路的宽度增加 1，以便强制将输出设为 0。

□

5 总结

本文探讨了一种通过有界宽度电路研究电路下界的方法。该方法目前尚未取得新的电路下界。尽管我们甚至还没有为受限图找到足够好的卵石游戏策略，但卵石游戏的已有结果或许会有所帮助。

第 3.2 节中用于证明下界的证明纲要，也给出了一个针对非确定性有界宽度电路的可满足性算法。最后，我们介绍该算法。

5.1 有界宽度电路的可满足性算法

电路可满足性问题定义如下。

输入：一个布尔电路 C

输出：是否存在某个输入使 C 输出 1?

自从 Ryan Williams 揭示该问题与电路复杂性下界之间的联系 [6] 以来，电路可满足性问题便得到了深入研究。

针对非确定性语法型读入 k 次的分支程序，可满足性算法如下。

定理 12（[3]）。存在一种确定性多项式空间算法，可在时间$O(\text{poly}(n, m^{k^2}) \cdot 2^{(1-4^{-k-1})n})$内求解含有 n 个变量和 m 条边的非确定性、语法型读-k次分支程序可满足性问题。

与下界证明的思路类似，我们给出了一个用于非确定性有界宽度电路的可满足性算法。

定理 13。存在一种确定性多项式空间算法，可在时间$O(\text{poly}(n, m^{k^2}) \cdot 2^{(1-4^{-k-\frac{3}{2}})n})$内求解含有 n 个实际输入端、规模为 s 且宽度为 w 的非确定性有界宽度电路可满足性问题，其中 $m = 4^w s$ 且 $k = \lceil \frac{2s}{n} \rceil$。

证明。设 C 是一个非确定性有界宽度电路。我们从 x_1、……、x_n 中选取 $n/2$ 个变量，使得每个选出的变量在 C 中恰好被读取 $\lceil \frac{2s}{n} \rceil$ 次。对于未选出的 $n/2$ 个变量，我们执行暴力搜索。然后，我们使用引理 7，并执行定理 12 中的算法。

□

参考文献

[1] Sanjeev Arora 和 Boaz Barak。《计算复杂性：现代方法》。剑桥大学出版社，2009 年。[2] Allan Borodin、Alexander A. Razborov 和 Roman Smolensky。关于读取 k 次的分支程序的下界。《计算复杂性》，3:1–18，1993 年。[3] Atsuki Nagao、Kazuhisa Seto 和 Junichi Teruyama。用于语法型读取 k 次分支程序的可满足性算法。载于 ISAAC 会议论文集，第 58:1–58:10 页，2017 年。[4] Jakob Nordstr¨om。卵石游戏、证明复杂性与时间-空间权衡。《逻辑方法与计算机科学》，9(3)，2013 年。[5] Leslie G. Valiant。计算复杂性中的图论性质。《计算机与系统科学杂志》，13(3):278–285，1976 年。[6] Ryan Williams。电路的算法与算法的电路。载于 CCC 会议论文集，第 248–261 页，2014 年。