arXiv:2512.21764v1 [cs.CC] 25 Dec 2025

关于 Avoid 与 MCSP 的注记

Edward A. Hirsch* Ilya Volkovich†

摘要

Ghentiyala、Li 和 Stephens-Davidowitz 最近的一项结果（ECCC TR 25-210）表明，任何可通过确定性或随机化图灵归约归约到值域回避问题（Avoid）的语言，都属于 AM ∩ coAM。本文介绍了另一种可能的途径，即通过最小电路规模问题（MCSP）获得同一结果。

1 引言

该值域回避（Avoid）问题定义如下：给定一个布尔电路 C： $\{0,1\}^n \to \{0,1\}^m$ 满足 $m > n$，输出一个字符串 $y \in \{0,1\}^m$ 使得 $y \notin$ 像（C），也就是说， y 在 C 下没有原像。自 20 世纪 80 年代以来，数理逻辑领域的文献一直在研究这个问题 [PWW88], ，并将其称为“对偶弱鸽巢原理”（dWPHP）。它在计算复杂性理论中的“新生”始于 Kleinberg、Korten、Mitropolsky 和 Papadimitriou 的研究 [KKMP21]。此后，这个问题引起了广泛关注（例如，参见 [GLSD25] 及其中的参考文献，了解复杂性理论视角下的综述；关于有界算术领域的研究，则参见 [Kra25] ）。

Avoid 是全搜索问题的一个自然例子，也就是说，这是一类始终存在解的搜索问题。此外，从 $\{0,1\}^m$ 中随机选取的元素以至少 $1-2^{-(m-n)}$ 的概率成为一个解。因此，最困难的实例[1] 出现在 $m = n+1$ 时；在这种情况下，平凡的随机化算法成功的概率可能接近 $\frac{1}{2}$。为了提高成功概率，自然可以抽取若干个随机样本并对其进行检查。这将得到一个“零误差”的 $\mathrm{ZPP}^{\mathrm{NP}}$ 算法。然而，NP 预言机似乎是必需的，因为即使有人给出了一个正确解，也不清楚如何高效地 验证或选出该解。这引出了下面这个自然的问题：

> “我们能否在不使用NP 预言机的情况下，提高求解Avoid 的成功概率；或者至少使用一个针对更简单问题的预言机来实现这一点？”

在最小电路规模问题（MCSP）中，我们给定一个 n元布尔函数 f 的真值表 $tt \in \{0,1\}^{2^n}$ ： $\{0,1\}^n \to \{0,1\}$ 以及一个参数 $0 \le s \le 2^n$，目标是

*计算机科学系，阿里埃勒大学，以色列。本研究得到了以色列国、移民吸收部和科学家吸收中心的支持。电子邮箱：edwardh@ariel.ac.il

†波士顿学院计算机科学系，马萨诸塞州栗树山。电子邮箱：ilya.volkovich@bc.edu[1]还有一个更强的版本，对应于经典鸽巢问题的对偶版本，其中定义域仅比像小一个元素。该版本也曾在相关文献中得到研究，但其复杂性特征却大不相同。

确定 f 是否可以由规模至多为 s的布尔电路计算。该问题与 Avoid 有着相似的命运：尽管其起源可以追溯到20世纪60年代（例如见 [Tra84]），但在 Kabanets 和 Cai 于 [KC00]重新提出该问题后，人们对它的兴趣再次高涨。在那项工作中，人们还注意到 MCSP $\in$ NP。然而，该问题的真正复杂性仍然未知。特别是，在标准的（确定性的）多对一归约下，人们既不知道、也不相信它是 NP 困难的 [MW15, HP15]。尽管如此，近期的一些结果在更一般的归约概念下，为 MCSP 的 NP 困难性提供了证据 [ILO20, Ila20, Ila23]。更准确地说， [ILO20, Ila20] 证明了 MCSP 的一些变体（例如“多输出”版本和部分版本）在随机化多对一归约下是 NP 困难的；而近期的工作 [Ila23]表明，MCSP 在随机化预言机模型中是 NP 困难的，并且 MCSP^O ——MCSP 的相对化版本——对于随机预言机 O在 P/poly 归约下是 NP 困难的。最后，对于任意预言机 B，MCSP，事实上 MCSP^B ，都可以被视为自然性质 [RR97, KC00] 的特例。

本文旨在一个自然的框架下，将 Avoid 与 MCSP联系起来：即在随机化图灵归约下。近期，Ghentiyala、Li 和 Stephens-Davidowitch [GLSD25] 将其与 Arthur–Merlin协议联系起来，并证明 $\mathsf{BPP}^{\mathsf{Avoid}} \subseteq \mathsf{AM} \cap \mathsf{coAM}$ （对于这些复杂性类的承诺版本，也有相应结论）。他们还指出，当伸展量适度大时$m = n+\omega(\log n)$，该结论就变得平凡，因为这个 Avoid$_m$ 预言机不会为 BPP带来更强的能力，也就是说，$\mathsf{BPP}^{\mathsf{Avoid}_m}$ =BPP。我们要探究，对于其他取值的 Avoid ， m的复杂度如何；具体而言，当 $m = n + 1$时，这个问题的最难实例又如何？我们证明，即使在这种情况下，也可以用 Avoid预言机替换为 MCSP预言机。

乍看之下，$\mathsf{BPP}^{\mathsf{MCSP}}$ 与 AM ∩coAM 在目前的认知下似乎不可比，但 Hirahara 和 Watanabe 关于 与预言机无关的 归约到MCSP[HW16] 的观察表明，$\mathsf{BPP}^{\mathsf{MCSP}}$ “终究”可能包含于 AM ∩coAM之中。关于此问题的进一步讨论，请参见第 4 节。

1.1 结果

我们的主要结果展示了：在拥有 MCSP 预言机访问的情况下，如何提高求解 Avoid 的成功概率。

定理 1. 存在一种随机化算法，给定 $\varepsilon > 0$、一个布尔电路 C： $\{0,1\}^n \to \{0,1\}^m$ （针对 $m > n$），以及对 MCSP 的预言机访问，输出一个字符串 $y \in \{0,1\}^m$，使得 $y \notin$ 像 (C)，其概率至少为 $1-\varepsilon$，且运行时间关于 $1/\varepsilon$ 和 C 的大小为多项式。

作为一个直接推论，我们得到了所有通过随机化图灵归约归约到 Avoid 的语言（以及承诺问题）集合的一个上界。

推论 2. $(\mathsf{pr})\mathsf{BPP}^{\mathsf{Avoid}} \subseteq (\mathsf{pr})\mathsf{BPP}^{\mathsf{MCSP}}$。

2 预备知识

我们首先正式定义并回顾相关问题。

定义 2.1 (Avoid)。 给定一个布尔电路 C： $\{0,1\}^n \to \{0,1\}^m$，其中 $m > n$，求一个字符串 $y \in \{0,1\}^m$，使得 $y \notin$ 像 (C)。

定义 2.2 (MCSP，MCSP^B)。 给定一个 n 变量布尔函数 f： $\{0,1\}^n \to \{0,1\}$ 的真值表 $tt \in \{0,1\}^{2^n}$ 以及参数 $0 \le s \le 2^n$，判断 f 是否可以由规模至多为 s 的布尔电路计算。在该问题的相对化版本中，MCSP^B，布尔电路还允许使用 B-预言机门。

2.1 多项式时间可计算函数的求逆

Allender 等人 [ABK+06] 证明，具有足够高的时间有界 Kolmogorov 复杂度（按适当意义定义）的足够稠密的字符串集合[2] 可用于破解（即求逆）任意多项式时间可计算函数。他们进一步指出，此类集合可以在$\mathsf{P}^{\mathsf{MCSP}}$中构造，因此 MCSP 预言机足以实现这一目的：

引理 2.3 ([ABK+06，定理45及其后的讨论])。 设 $f_z(x) = f(z,\ x)$ 是一个可在关于 $|x|$的多项式时间内一致计算的函数。存在一个概率预言机图灵机$A^{\bullet}$ 和 $k \in \mathbb{N}$，使得对于任意 n 和 z：

$$\Pr_{|x|=n,\,\tau}\left[f_z\left(A^{\mathsf{MCSP}}(z, f_z(x), \tau)\right) = f_z(x)\right] \geq 1/n^k,$$

其中 x 是均匀随机选取的，τ 表示 A的随机性；该过程的运行时间关于 $|x|$ (以及 $|z|$ 和 $|f_z(x)|$) 是多项式时间，但由于一致性条件，这一点并不重要。

注意到，对给定布尔电路在输入 x 上求值，可以在关于电路规模的多项式时间内一致完成；再利用强、弱单向函数之间的标准变换，我们得到：

引理 2.4. 存在一个概率预言机图灵机 $M^{\bullet}$，给定 $\varepsilon > 0$ 和一个以 n 个输入、$m = n + 1$ 个输出的布尔电路 C，其运行时间为 $\mathrm{poly}(|C|, 1/\varepsilon)$，并满足：

$$\Pr_{|x|=n,\,\tau}\left[C\left(M^{\mathsf{MCSP}}(1/\varepsilon, C, C(x), \tau)\right) = C(x)\right] \geq 1 - \varepsilon,$$

其中，x 是均匀随机选取的，τ 表示 M的随机性 .

尽管 [ABK+06] 的结果此前曾以这种形式使用过（例如参见 [AGvM+18]），为求完整起见，我们在附录 A 节中从其原始形式（引理 2.3）正式推导出该结果。

注释 2.5。 还可以进一步观察到，引理 *2.3* 和 *2.4* 中的 MCSP 预言机可以替换为任意语言 MCSP^B，B 事实上，还可以替换为 [*RR97*]意义下任何具有指数级效用的“自然性质”。这包括 MKTP 及其他度量。更多讨论见第 *4* 节。

为方便记号，我们将以下事件称为“成功求逆”：

定义 2.6。 $I_{C,\ y,\ \tau}$表示事件 $C\left(M^{\mathsf{MCSP}}(1/\varepsilon、\ C、\ y、\ \tau)\right) = y$。也就是说，该事件表示：在能够访问 MCSP 预言机且具有随机性 τ的情况下，机器 M 输出 y 在 C 下的一个原像。

特别要注意，对于任意 $y \notin$像 (C) 和任意 τ，我们都有 $\mathbf{Pr}_{\tau}\left[I_{C,y,\tau}\right] = 0$。此外，利用上述记号，我们可以将引理 2.4 简洁地改写为

$$\Pr_{|x|=n,\,\tau}\left[I_{C,C(x),\tau}\right] \geq 1 - \varepsilon.$$

固定一个布尔电路 C：$\{0,1\}^n \to \{0,1\}^m$。以下引理将随机输入 C 的求逆概率与在 C 的陪域中随机元素 的求逆概率联系起来，即 $\{0,1\}^m$。为确保论述自成一体，我们给出这个（非常标准的）证明：

[2]也就是说，需要一个语言 L，其中每种长度 n 的比特串至少有 $2^n/n^k$ 个，并且对于每个 $x \in L$，KT(x) $\geq |x|^{1/k}$；这里 KT 表示他们所定义的时间受限柯尔莫哥洛夫复杂度。

引理 2.7. $\Pr_{|y|=m,\ \tau}[I_{C,y,\tau}] \leq \frac{1}{2^{m-n}} \cdot \Pr_{|x|=n,\ \tau}\left[I_{C,C(x),\tau}\right]$.

证明。

$$\Pr_{x,\tau}\left[I_{C,C(x),\tau}\right] = \sum_{y\in\{0,1\}^m} \Pr_{\tau}[I_{C,y,\tau}] \cdot \Pr_{x}[C(x)=y] = \sum_{y\in \mathrm{Im}(C)} \Pr_{\tau}[I_{C,y,\tau}] \cdot \Pr_{x}[C(x)=y] \geq$$

$$\sum_{y\in \mathrm{Im}(C)} \Pr_{\tau}[I_{C,y,\tau}] \cdot \frac{1}{2^n} = \frac{2^m}{2^n} \cdot \frac{1}{2^m} \cdot \sum_{y\in\{0,1\}^m} \Pr_{\tau}[I_{C,y,\tau}] = \frac{2^m}{2^n} \cdot \Pr_{y,\tau}[I_{C,y,\tau}]. \qquad \square$$

下一个引理表明，如果引理 2.4 中的求逆器无法为随机元素 y 找到原像，那么该元素 y 很可能没有这样的原像。也就是说，y 位于 C 的值域之外。

引理 2.8. 概率$_{|y|=m,\tau}[y \notin$ 像 $(C) | \bar{I}_{C,y,\tau}] \geq$ 概率$_{|x|=n,\tau}\left[I_{C,C(x),\tau}\right]$。

证明。

$$\Pr_{y,\tau}[y \notin \mathrm{Im}(C) \mid \bar{I}_{C,y,\tau}] = \frac{\Pr_{y,\tau}[y \notin \mathrm{Im}(C) \wedge \bar{I}_{C,y,\tau}]}{\Pr_{y,\tau}[\bar{I}_{C,y,\tau}]} = \frac{\Pr_{y,\tau}[y \notin \mathrm{Im}(C)]}{\Pr_{y,\tau}[\bar{I}_{C,y,\tau}]} \geq \frac{1-\frac{1}{2^{m-n}}}{1-\frac{1}{2^{m-n}} \cdot \Pr_{|x|=n,\tau}\left[I_{C,C(x),\tau}\right]} =$$

$$\frac{2^{m-n}-1}{2^{m-n}-\Pr_{|x|=n,\tau}\left[I_{C,C(x),\tau}\right]} \geq \Pr_{|x|=n,\tau}\left[I_{C,C(x),\tau}\right]. \qquad \square$$

3 将Avoid归约为 MCSP：主要结果的证明 lt

现在我们可以证明主要结果了。

定理 *1* 的证明。令 $M^{\bullet}$ 为引理 2.4 中的机器。以下过程以高概率解决输入为 C的问题 Avoid: $\{0,1\}^n \to \{0,1\}^m$

1. 重复以下步骤 t 次:

   (a) 均匀随机地选取 $y \in \{0,1\}^m$。(b) 如果 $C\left(M^{\mathsf{MCSP}}(1/\varepsilon,\ C,\ y,\ \tau)\right) \neq y$，则输出 y；否则继续。

2. 输出 $\perp$。

此过程有两个误差来源:

1. 此过程输出 Im (C) 中的一个元素。根据引理 2.4 和 2.8，该概率至多为 εt。

2. 该过程输出 $\perp$。只有当所有随机选取都落在像 (C) 内时才会发生（并且 M^{MCSP} 的所有执行都成功，但这其实并不重要）。即使 $m = n+1$，该概率也至多为 $(2^{n-m})^t \leq 1/2^t$。

因此，总误差至多为 $\varepsilon t + 2^{-t}$；通过选择 $t = n$ 和 $\varepsilon = \varepsilon'/(2n)$，可以使其小于任意 $\varepsilon' > 0$。 $\square$

推论 *2* 的证明。假设 $\mathrm{BPP}^{\mathsf{Avoid}}$ 机器运行时间为 $p(n)$，其中$p(n)$是某个多项式。通过在定理 1 中选择 $\varepsilon = \frac{1}{8p(n)}$，所有查询都将以至少 $7/8$ 的概率得到正确回答，并且机器的误差仍将保持有界。 $\square$

4 与预言机无关的归约及与先前结果的比较

我们指出，在上述求解 Avoid 的过程中，机器 M 不仅在获得对 MCSP 本身的预言机访问时能够正确运行，而且当MCSP被替换为 MCSP^B 以及任何 任意的 预言机 B时也能正确运行。这种 预言机无关的 归约到 MCSP 的概念由 Hirahara 和 Watanabe [HW16], 提出；他们指出，大多数已知的归约到 MCSP（包括 [ABK+06]的归约）都是以这种方式运行的（见 [HW16，第 3]节）。在那项工作中，他们还研究了此类归约的能力。特别是，他们证明了以下结论：

定理 ([HW16，定理 2])。 如果语言 L 可通过一个与预言机无关的随机化归约归约到 MCSP ，且该归约的误差可忽略并且至多进行一次查询，那么 $L \in \mathsf{AM} \cap \mathsf{coAM}$。换言之，

$$\bigcap_B \mathsf{BPP}^{\mathsf{MCSP}^B[1]} \subseteq \mathsf{AM} \cap \mathsf{coAM}.$$

他们还证明了，无论查询次数多少，确定性的、与预言机无关的多项式时间图灵归约都不会带来额外的能力：无论 查询次数多少：

定理 ([HW16，定理 1])。 $\bigcap_B \mathsf{P}^{\mathsf{MCSP}^B} = \mathsf{P}$。

由于我们用于求解 Avoid 的过程与预言机无关（另见注释 2.5），我们得到推论 2 的以下“与预言机无关”扩展：

推论3. $\mathsf{BPP}^{\mathsf{Avoid}} \subseteq \bigcap_B \mathsf{BPP}^{\mathsf{MCSP}^B}$。

遗憾的是， [HW16] 给出的上述结果／刻画并不适用于我们的过程，因为我们的归约是随机化的，且会进行多次查询。与此同时，Ghentiyala、Li 和 Stephens-Davidowitz 最近的一项结果 [GLSD25] 表明$\mathsf{BPP}^{\mathsf{Avoid}} \subseteq \mathsf{AM} \cap \mathsf{coAM}$。综合这些结果，它们为以下猜想提供了支持证据，我们提出该猜想如下：

猜想4.1. $\bigcap_B \mathsf{BPP}^{\mathsf{MCSP}^B} \subseteq \mathsf{AM} \cap \mathsf{coAM}$。

也就是说，如果一种语言 L可通过与预言机无关的随机化归约归约到 MCSP，那么无论查询次数多少， $L \in \mathsf{AM} \cap \mathsf{coAM}$。

与此同时，Sdroievski、da Silva 和 Vignatti [SdSV19] 设计了一种随机算法，在获得对 MCSP 的预言机访问后，可以解决隐藏子群问题（HSP）。值得注意的是，HSP 是量子计算理论中的核心问题。顺便提一句，他们的归约也是预言机无关的[3]。因此，如果该猜想成立，它不仅意味着我们的结果为将 $\mathsf{BPP}^{\mathsf{Avoid}}$ 纳入 $\mathsf{AM} \cap \mathsf{coAM}$ 提供了另一种（且可能更强的）途径，还将 $\mathsf{BPP}^{\mathsf{HSP}}$ 纳入 $\mathsf{AM} \cap \mathsf{coAM}$，据我们所知，这一点目前尚未得到证明。

[3]尽管形式化表述是HSP 可以在$\mathsf{BPP}^{\mathsf{MTKP}}$中求解，但他们的归约实际上基于 [ABK+06] 的定理45（引理 2.4）。与我们的情况一样，这得出了一个与预言机无关的$\mathsf{BPP}^{\mathsf{MCSP}}$包含关系。

支持该猜想的另一项证据（正如 [HW16] 中所指出的）来自 Allender 和 Das 的结果 [AD14]，该结果表明$\mathsf{SZK} \subseteq \mathsf{BPP}^{\mathsf{MCSP}}$，且所用归约与预言机无关。这补充了此前已知的包含关系 $\mathsf{SZK} \subseteq \mathsf{AM} \cap \mathsf{coAM}$[For89、Oka00、SV03]。能否扩展 [GLSD25] 的技术来证明这一猜想？

参考资料

[ABK+06] E. Allender、H. Buhrman、M. Kouck´y、D. van Melkebeek 和 D. Ronneburger。随机串的力量。SIAM J. Comput., 35(6):1467–1493, 2006.[AD14] E. Allender 和 B. Das。零知识与电路最小化。载于《数学计算机科学基础》（MFCS），第 25–32 页，2014.[AGvM+18] E. Allender、J. A. Grochow、D. van Melkebeek、C. Moore 和 A. Morgan。最小电路规模、图同构及相关问题。SIAM J. Comput., 47(4):1339–1372, 2018.[For89] L. Fortnow。完美零知识的复杂性。《计算研究进展》，5:327–343，1989.[GLSD25] S. Ghentiyala、Z. Li 和 N. Stephens-Davidowitz。值域回避、Arthur–Merlin 与 TFNP。Electron. Colloquium Comput. Complex., TR25-210, 2025.[HP15] J. M. Hitchcock 和 A. Pavan。最小电路规模问题的 NP 完全性。载于第 35 届 IARCS 软件技术与理论计算机科学基础年会（FSTTCS），第 236–245 页，2015.[HW16] S. Hirahara 和 O. Watanabe。作为预言机的最小电路规模问题的局限。载于第 31 届计算复杂性会议（CCC），第 18:1–18:20 页，2016.[Ila20] R. Ilango。从上下两方面研究 MCSP：一种条件变体的困难性以及 AC0[p]。载于第 11 届理论计算机科学创新会议（ITCS），LIPIcs 第 151 卷，第 34:1–34:26 页。达格施图尔：Schloss Dagstuhl - Leibniz-Zentrum f¨ur Informatik，2020.[Ila23] R. Ilango。SAT 可归约到带随机预言机的最小电路规模问题。载于第 64 届 IEEE 计算机科学基础年会（FOCS 2023），美国加利福尼亚州圣克鲁斯，2023 年 11 月 6–9 日，第 733–742 页。IEEE，2023.[ILO20] R. Ilango、B. Loff 和 I. Carboni Oliveira。多输出函数电路最小化的 NP 困难性。载于第 35 届计算复杂性会议（CCC），LIPIcs 第 169 卷，第 22:1–22:36 页。Schloss Dagstuhl - Leibniz-Zentrum f¨ur Informatik，2020.[KC00] V. Kabanets 和 J. Cai。电路最小化问题。载于第 32 届 ACM 理论计算会议（STOC）论文集，第 73–79 页，2000.[KKMP21] R. Kleinberg、O. Korten、D. Mitropolsky 和 C. Papadimitriou。多项式层次中的全函数。载于 James R. Lee 编，第 12 届理论计算机科学创新

计算机科学会议（*ITCS 2021*），理论计算机科学信息学论文集（LIPIcs）第 185 卷，第 44:1–44:18 页，德国达格施图尔，2021 年。Schloss Dagstuhl–Leibniz-Zentrum f¨ur Informatik。[Kra25] Jan Kraj´ıˇcek。《证明复杂性生成器》。伦敦数学学会讲义系列。剑桥大学出版社，2025 年。[MW15] C. D. Murray 和 R. R. Williams。计算电路复杂性的（非）NP 困难性。载于第 *30* 届计算复杂性会议（*CCC*），第 365–380 页，2015 年。[Oka00] T. Okamoto。统计零知识证明之间的关系。*J. Comput.Syst. Sci.*，60(1):47–108，2000 年。[PWW88] J. Paris、A. Wilkie 和 A. R. Woods。鸽巢原理的可证明性与无限多个素数的存在。*J. Symb. Log.*，(53):1235–1244，1988 年。[RR97] A. A. Razborov 和 S. Rudich。自然证明。计算机与系统科学杂志，55(1):24–35，1997 年。[SdSV19] N. M. Sdroievski、M. V. G. da Silva 和 A. L. Vignatti。隐藏子群问题与 MKTP。理论计算机科学，795:204–212，2019 年。[SV03] A. Sahai 和 S. P. Vadhan。统计零知识的一个完全问题。*ACM*杂志，50(2):196–249，2003 年。[Tra84] B. A. Trakhtenbrot。俄罗斯穷举搜索算法方法综述。*IEEE*计算史年刊，6(4):384–400，1984 年。[Yao82] A. Chi-Chih Yao。陷门函数的理论与应用（扩展摘要）。载于第 *23* 届计算机科学基础年会，美国伊利诺伊州芝加哥，*1982* 年 *11* 月 *3–5* 日，第 80–91 页。IEEE计算机学会，1982 年。

引理 2.4 的证明概要

引理 *2.4* 的证明概要。 我们基本上需要应用一种将弱单向函数转换为强单向函数的标准构造，并处理“统一”设置。

根据引理 2.3，我们将定义如下函数 $f_z(x)$：

$$f_C(x) = (C(x_1), C(x_2), \ldots, C(x_t)),$$

对于 $x_i \in \{0,1\}^n$，以及对于足够大的 $t = O\left(\frac{n}{\varepsilon}\right)$。然后，类似于 [Yao82]，下面的算法 M^{MCSP} 以如下概率成功 $1-1/\varepsilon$：它将以下过程重复一个更大的多项式次数：随机选取 $j \in \{1,\ldots,t\}$，随机选取所有 x_i，在（x_1，……，x_t）上使用 A^{MCSP}，其中 x_j 替换为 y；如果结果正确，则输出该结果。

现在，为了使我们的函数在 C 中统一（即，使其运行时间仅关于 $|x|$ 为多项式），假设 C 至少有 $\sqrt{|C|}$ 个输入。如果输入少于此数量，则向其中添加足够的虚假输入（及输出），并考虑一个新的电路 D'，使其在这些输入上计算恒等函数。这不会改变对该电路求逆的概率（因为 ε 是常数），而且 $M^{\bullet}$ 的运行时间将变为关于 $|C|$ 的多项式（而不只是关于 n 的多项式）。 □