arXiv:2602.14037v1 [cs.CC] 15 Feb 2026

仿射秩最小化是 ER-完全的

Angshul Majumdar[a]

[a]因陀罗普拉斯塔信息技术学院，德里，新德里，*110020*，印度 a

摘要

我们研究判定问题 仿射秩最小化，记作 ARM(k)：给定有理矩阵 $A_1, \dots, A_q \in \mathbb{Q}^{m\times n}$ 和标量 $b_1, \dots, b_q \in \mathbb{Q}$，判断是否存在 $X \in \mathbb{R}^{m\times n}$，使得对所有 $\ell \in [q]$，均有 $\langle A_\ell, X\rangle = b_\ell$，且秩($X$) $\le k$。我们首先证明成员资格：对于每个固定的 $k \ge 1$，通过给出一个利用常数大小分解见证对秩约束进行显式存在性编码的方法，证明 ARM(k) $\in \exists\mathbb{R}$。随后，我们通过从 ETR 到 ARM(k) 的多项式时间多对一归约证明 $\exists\mathbb{R}$-困难，其中输入被限制为仿射等式加一个全局约束秩(X) $\le k$。该归约将 ETR 公式编译为门等式标准形式的算术电路，并将每个电路量赋给 X 的一个指定元素；仿射语义（常数、复制、加法/取负）通过线性约束直接强制实现，而乘法语义则通过常数大小的强制秩构件实现，其可靠性由一个固定秩的“规范”子矩阵保证，从而消除因子分解歧义。我们证明了一个组合引理，表明这些构件可以嵌入而不会产生意外交互，由此保证编码的整体可靠性和完备性，并保持维数和位长的多项式界。因此，ARM(k) 是 $\exists\mathbb{R}$-完全的（特别地，ARM(3) 是 $\exists\mathbb{R}$-完全的），这表明在固定常数秩上界下，纯仿射约束的可行性足以刻画实代数可行性的全部表达能力。

关键词：仿射秩最小化；低秩可行性；实数存在性理论；ER-完备性；代数复杂性；多项式时间归约；算术电路；秩约束矩阵补全

1. 引言

1.1. 动机

低秩结构是贯穿矩阵补全、逆问题与系统辨识的统一建模原则：人们假定未知对象位于（或接近）一个低维代数簇，而观测则施加线性约束。在矩阵补全及相关恢复问题中，低秩同时支撑统计保证与算法设计；核范数最小化等凸替代方法如今已成为标准，并在非相干性与采样假设下给出精确的恢复结果 [1, 2, 3, 4, 5]。在控制与系统理论中，秩最小化表述经由汉克尔结构模型、实现理论与模型降阶自然出现；早期表述与松弛方法可见于，例如 [6, 7, 8]。在这些领域中，秩约束是唯一的非线性来源，而测量模型是仿射的。

本文旨在以最简洁的判定形式，确定相应可行性问题的精确最坏情况复杂度。这样的分类有两个重要意义。首先，它解释了为什么几乎所有已知的实用方法都必须选择放宽问题（例如使用核范数），或接受非凸性（例如采用分解、交替最小化） [6, 4]。其次，它明确了实数域上代数可行性所对应的正确复杂度类，从而排除“NP 困难，但或许仍是离散问题”这类误解：这里的障碍本质上是半代数的。

1.2. 复杂度背景

实数域$\mathbb{R}$ 上多项式约束可行性的自然参照是实数存在理论（ETR）及其对应的复杂度类 $\exists\mathbb{R}$。对 $\exists\mathbb{R}$ 而言的完备问题涵盖了广泛的几何与代数可行性问题；尤其是， $\exists\mathbb{R}$ 在标准位模型下介于 NP 与多项式空间之间，而多项式空间上界则来自实数一阶理论的量词消去与判定过程 [9]。Blum–Shub–Smale 框架与位模型视角阐明了实数计算和代数编码之间的相互作用 [10], [11]。

我们的目标是准确定位这一类矩阵可行性问题在整个图景中的位置：输入是纯仿射形式（带有有理系数的线性等式），所有非线性都局限于单个全局秩约束。这是一种特别规范的目标形式：它避免了显式列出

实例的子式、行列式谓词，或“秩$(X) \le k$”之外的任何其他多项式约束。

1.3. 主要贡献

我们在标准有理数输入模型下研究判定问题仿射秩最小化 ARM(k)：给定

$$A_1, \dots, A_q \in \mathbb{Q}^{m\times n}, \qquad b_1, \dots, b_q \in \mathbb{Q}, \tag{1.1}$$

判断是否存在 $X \in \mathbb{R}^{m\times n}$ 使得

$$\langle A_\ell, X\rangle = b_\ell \ \ (\ell \in [q]), \qquad \operatorname{rank}(X) \le k. \tag{1.2}$$

本文证明的主要结果如下：

- **成员资格**。 对于每个固定的 $k \ge 1$，ARM(k) $\in \exists\mathbb{R}$。
- $\exists\mathbb{R}$**-困难性**。 在来自实数存在理论的多项式时间多对一归约下，ARM 是 $\exists\mathbb{R}$-困难的。
- **固定常数秩**。 即使秩固定为常数 $k = 3$，困难性仍然成立，因此 ARM(3) 是 $\exists\mathbb{R}$-完备的。
- **多项式规模与位长控制**。 归约输出的实例，其维度和有理数编码总长度均为源实数存在理论实例规模的多项式。

一个关键的概念要点（本项目中称为“选项 B”准则）是，归约生成的实例严格遵循输入格式 (1.2)：仅包含对单个矩阵变量元素的仿射等式 X 以及一个全局约束$\operatorname{rank}(X) \le 3$。生成的 ARM 实例中不包含显式的子式约束、行列式约束或其他多项式附加条件。

1.4. 技术概述

从整体上看，我们通过将算术推理编译为对单个矩阵的指定元素 施加的仿射约束，并将全局秩上界作为实施非线性语义的唯一机制，从而将实数存在理论归约为 ARM(3)。

（i）从实数存在理论到算术电路约束。 一种标准归约将一般的实数存在理论公式转换为一个等可满足的多项式合取式

等式，再将其转换为算术电路的逐门约束系统（每个门对应一个等式）。这种电路标准形在代数归约中无处不在，并能直接控制位大小 [10, 9, 12]。

（ii）将门编译为单个矩阵上的仿射约束。每个门值都分配到一个承载变量位置（r_i， c_i），并由指定的条目$X_{r_i,\ c_i}$表示。线性关系（常数、复制、加法、取负）可直接转化为承载变量之间的仿射等式。唯一真正的非线性门是乘法（以及在需要时的求逆/非零），它通过由新引入的一组辅助行/列上的仿射约束构成的常数规模强制秩构件来实现。

（iii）秩是唯一的非线性：通过行列式障碍强制实现。这些构件经过专门设计，使得任何对预期恒等式（例如 $z = xy$）的违反都会导致一个 4×4 子矩阵达到满秩，这与秩$(X) \leq 3$相矛盾。从概念上说，这与行列式簇的几何性质相符（秩受限集合是扎里斯基闭的，且由子式刻画） [13]。反过来，当恒等式成立时，该构件存在一个显式的秩 3 补全。

(iv) 规范固定与定义良好的解码。 由于秩 3 分解在可逆基变换下并不唯一，我们固定一个常数满秩3×3 子矩阵（即“规范块”），使所有解码得到的承载变量值在可行的秩 3 实现中保持不变。这样便消除了唯一微妙的全局歧义，使归约能够组合各个构件，而不会产生隐藏的耦合。

1.5. 相关工作

秩最小化与松弛方法。 秩的凸松弛（尤其是核范数）构成了现代低秩恢复理论的基石[1, 2, 3, 4]。基于分解的非凸替代方法也得到了广泛应用，并且在实践中往往效果显著，尽管它们不会改变最坏情形可行性复杂度。在系统辨识与控制中，秩最小化通过结构化低秩近似和基于汉克尔矩阵的表述自然出现 [6, 7, 8]。

离散情形下秩问题的困难性。若干密切相关的秩问题已知在离散模型中具有计算困难性。例如，低秩近似和仿射空间上的秩最小化的变体都呈现出 NP 困难现象 [14]。然而，这些结果并未确定 $\exists\mathbb{R}$ 所刻画的精确的实数可行性复杂度。

$\exists\mathbb{R}$完备性是恰当的视角。大量计算几何和实代数复杂性领域的研究指出，$\exists\mathbb{R}$ 是连续可行性问题的恰当复杂性类，而归约通常通过代数编码和电路标准形式 [10, 9]进行。我们的贡献在于证明，即使在高度受限的仿射 $+$ 单一秩约束输入规范下，ARM(3) 也已能充分表达 $\exists\mathbb{R}$的全部表达能力。

2. 预备知识

本节将确定全文使用的形式模型和记号：实数存在理论（ETR）及其标准归约形式；将算术电路视为多项式系统的紧凑表示；在有理数输入编码下的仿射秩最小化判定问题 ARM(k)；用作存在性见证工具的秩分解引理；以及分块矩阵和索引约定。关于 ETR 和 $\exists\mathbb{R}$ 的背景知识可参见 [15, 9]；实数代数编码和多项式系统见 [16]；而基于 $\mathbb{R}$ 的计算以及电路式表示，则是 Blum–Shub–Smale 框架中的经典内容 [17]。

2.1. 实数存在理论（*ETR*）

语法与编码。。设 $x = (x_1, \ldots, x_n)$ 为实变量。原子谓词是以下形式之一

$$p(x) = 0, \qquad p(x) \neq 0, \qquad p(x) \geq 0, \qquad p(x) > 0, \tag{2.1}$$

其中 $p \in \mathbb{Z}[x_1, \ldots, x_n]$。无量词公式 *()*是由原子谓词通过布尔组合并使用 $\wedge$， $\vee$， $\neg$构成的任意公式。实数存在理论实例是一条形如以下形式的语句

$$\exists x \in \mathbb{R}^n : \ \varphi(x), \tag{2.2}$$

而判定问题是判断是否存在这样的一个 x 。

输入规模按照标准位模型衡量：系数以二进制给出，多项式以稀疏形式给出，即列出单项式和指数向量； φ 的规模计算所有系数的总位长以及布尔表达式的语法规模。若出现有理系数，则将其编码为既约形式；清除分母后，可得到一个等价的整数系数实例，其位大小与原实例的位大小 [16] 呈多项式关系。

类 $\exists\mathbb{R}$.. 语言 L 属于 $\exists\mathbb{R}$，当且仅当它可在多项式时间内多对一归约到实数存在理论（ETR）。许多几何可行性问题在此类归约下是完全的 $\exists\mathbb{R}$ [15]。由实数一阶理论的判定过程以及存在片段的 $\exists\mathbb{R} \subseteq$ 多项式空间复杂度可得其经典上界多项式空间 [9]。

标准标准形式。 对于归约，使用受限的句法形式会更方便。我们记录后续将用到的特定标准形式：一组用于编码算术电路的多项式等式的合取式。

定义 2.1（实数存在理论等式形式）。 如果一个实数存在理论实例是如下语句，则称其处于等式形式

$$\exists y \in \mathbb{R}^N : \bigwedge_{t=1}^{T} f_t(y) = 0 \tag{2.3}$$

其中每个 $f_t \in \mathbb{Z}[y_1, \ldots, y_N]$。

引理 2.2（消除不等式和布尔结构）。 给定任意实数存在理论实例 $\exists x : \varphi(x)$，可以在多项式时间内构造一个与之等可满足的等式形式实例（定义 2.1），其位大小仅呈多项式级增长。

证明。 将 φ 转换为析取范式 $\bigvee_{j=1}^{M} \bigwedge_{i=1}^{T_j} \alpha_{ij}$，公式大小（以布尔电路衡量）仅呈多项式级增长（若坚持显式写出析取范式，最坏情况下增长可能是指数级，因此我们采用下文的标准选择变量编码）。引入选择变量s_1，. . . ，s_M，并利用多项式等式强制恰有一个选择变量处于激活状态，例如，

$$\sum_{j=1}^{M} s_j - 1 = 0, \qquad s_j(1 - s_j) = 0 \quad (j \in [M]). \tag{2.4}$$

对于子句 j 中的每个原子谓词 α_{ij}，仅当 $s_j = 1$ 时才通过将相应的相等约束乘以 s_j 来强制其成立。因此，只需将每个原子谓词转换为含辅助变量的多项式等式。

等式 $p(x) = 0$ 已经符合所需形式。对于非严格不等式，使用标准松弛变量编码：

$$p(x) \geq 0 \iff \exists u \in \mathbb{R} : \; p(x) - u^2 = 0. \tag{2.5}$$

对于严格不等式，

$$p(x) > 0 \iff \exists u, v \in \mathbb{R} : \ p(x) - u^2 = 0 \ \wedge \ uv - 1 = 0, \tag{2.6}$$

这强制要求 $u \neq 0$，从而得到 $u^2 > 0$。不等式约束 p（x）$\neq 0$ 可以编码为

$$p(x) \neq 0 \iff \exists v \in \mathbb{R} : \ p(x)v - 1 = 0. \tag{2.7}$$

所有新增多项式的次数至多为 2，且引入的约束和变量的数量及位大小均以多项式为界 [16]。 □

电路标准形式。 在后续的归约中，我们实际上将使用一种结构更明确的等式形式，其中每个约束都表示单个算术门的语义。算术电路对此进行了概括（第 2.2 节）。

2.2. 实数域上的算术电路

算术电路为多项式系统提供了紧凑的表示形式，也是 $\exists\mathbb{R}$ 归约的一种便捷标准形式。

定义 2.3（算术电路）。 一个**算术电路** 定义在 $\mathbb{R}$ 上，具有输入变量 x_1，……，x_n，是一个有限的有向无环图，其门具有以下类型：

1. 由变量 x_i 标记的输入门；
2. 由有理常数 $c \in \mathbb{Q}$ 标记的常数门；
3. 由 $+$ 或 $\times$ 标记的二元门（扇入为 2）；
4. 由 $-$ 标记的一元取反门（扇入为 1）。

每个门都以自然的方式计算关于 $\mathbb{Q}[x_1, \ldots, x_n]$ 的一个多项式。

定义 2.4（电路大小与位大小）。 电路的**大小** 是门的数量。**位大小** 还会统计所有有理常数的总位长（既约形式下的分子和分母）。不失一般性，可令扇入为二：任何扇入更高的加法或乘法都可以展开为由门组成的二叉树，且仅造成线性膨胀。

门变量编码。 给定一个门集合为 G的电路$\mathcal{C}$ ，为每个门 $g \in G$引入一个实变量 z_g 。定义约束集 GateEq($\mathcal{C}$)，其中每个门对应一个多项式等式：

- 如果 g 是一个输入 x_i，则施加 $z_g - x_i = 0$;
- 如果 g 是一个常数 $c \in \mathbb{Q}$，则施加 $z_g - c = 0$;
- 如果 $g = g_1 + g_2$，则施加 $z_g - z_{g_1} - z_{g_2} = 0$;
- 如果 $g = g_1 \times g_2$，则施加 $z_g - z_{g_1} z_{g_2} = 0$;
- 如果 $g = -g_1$，则施加 $z_g + z_{g_1} = 0$。

引理 2.5 （电路约束是精确的）。 设 C 是一个算术电路，其指定输出门为 g_{out} ，并令 $p_{\mathcal{C}}(x)$ 表示在 g_{out}处计算得到的多项式。那么对于每个 $x \in \mathbb{R}^n$,

$$p_{\mathcal{C}}(x) = 0 \quad \Longleftrightarrow \quad \exists (z_g)_{g \in G} \in \mathbb{R}^{|G|} : \ \text{GateEq}(\mathcal{C}) \ \wedge \ z_{g_{\text{out}}} = 0. \tag{2.8}$$

此外，约束的数量为 $|G| + 1$ ，位大小关于 C 的位大小是多项式级的。

证明。 正向做法是将 z_g 赋值为门 g在输入 x下计算出的值。根据定义，这满足每个门方程，并得到$z_{g_{\text{out}}} = p_{\mathcal{C}}(x) = 0$。反过来，任何满足 GateEq($\mathcal{C}$) 的赋值，都必须通过对有向无环图拓扑序进行归纳，证明其在每个门上的取值与电路求值一致；因此 $z_{g_{\text{out}}} = p_{\mathcal{C}}(x)$，所以 $z_{g_{\text{out}}} = 0$ 蕴含 $p_{\mathcal{C}}(x) = 0$。大小界显然成立。 □

在归约中的应用。 引理 2.5 是后续使用的精确标准形式：我们不会使用任意多项式，而是逐门编码计算，再将这些门方程转换为矩阵约束。

2.3. 仿射秩最小化$\text{ARM}(k)$

现在，我们来定义本文研究的矩阵可行性问题。

仿射约束.. 固定维数 $m \times n$。对于 $A, X \in \mathbb{R}^{m\times n}$，记作

$$\langle A, X\rangle := \sum_{i=1}^{m}\sum_{j=1}^{n} A_{ij}X_{ij} \tag{2.9}$$

对于弗罗贝尼乌斯内积。

定义 2.6 (ARM(k))。固定一个整数 $k \geq 1$。判定问题 ARM(k) 定义如下：

Input: matrices $A_1, \ldots, A_q \in \mathbb{Q}^{m\times n}$ and scalars $b_1, \ldots, b_q \in \mathbb{Q}$.
问题：是否存在 $X \in \mathbb{R}^{m\times n}$ 使得

$$\langle A_\ell, X\rangle = b_\ell \quad (\ell \in [q]) \qquad \text{and} \qquad \operatorname{rank}(X) \leq k \ ? \tag{2.10}$$

编码模型和大小度量。。所有输入有理数均以既约形式编码；实例长度是所有 A_ℓ 和所有 b_ℓ 的所有条目中分子/分母的总位长，再加上 $(m,\ n,\ q)$ 的编码长度。消去分母可得到一个具有整数数据且位大小多项式相关的等价实例。

固定秩关注点。。我们的主要完备性陈述针对固定常数 $k = 3$；强调这一限制时，我们记作 ARM(3)。

2.4. 秩分解作为见证工具

低秩可以通过双线性分解以存在量化的方式表示。这一观察将用于证明成员资格属于 $\exists\mathbb{R}$，并简化正确性论证。

引理 2.7（秩分解等价性）。设 $X \in \mathbb{R}^{m\times n}$ 和 $k \geq 1$。那么 $\operatorname{秩}(X) \leq k$ 当且仅当存在 $U \in \mathbb{R}^{m\times k}$ 和 $V \in \mathbb{R}^{k\times n}$，使得

$$X = UV. \tag{2.11}$$

证明。若 $X = UV$，其中 $U \in \mathbb{R}^{m\times k}$ 且 $V \in \mathbb{R}^{k\times n}$，则 $\operatorname{rank}(X) \leq k$。

反过来，如果 $\operatorname{rank}(X) = r \leq k$，将 $X = \sum_{t=1}^{r} a_t b_t^{\top}$ 写成向量 $a_t \in \mathbb{R}^m$ 和 $b_t \in \mathbb{R}^n$。令 $U \in \mathbb{R}^{m\times k}$ 的前 r 列为 a_1、……、a_r，其余列为零；令 $V \in \mathbb{R}^{k\times n}$ 的前 r 行为 $b_1^{\top}$、……、$b_r^{\top}$，其余行为零。于是 $UV = X$。 □

定理 2.8 ($\mathrm{ARM}(k) \in \exists\mathbb{R}$ 对于固定的 k)。 对于每个固定的 $k \geq 1$，判定问题 $\mathrm{ARM}(k)$ 属于 $\exists\mathbb{R}$。

证明。 给定一个实例 $(A_\ell, b_\ell)_{\ell=1}^{q}$，引入表示 $U \in \mathbb{R}^{m\times k}$ 和$V \in \mathbb{R}^{n\times k}$ 的变量，并对它们进行存在量化。定义 $X := UV$，使得每个元素都满足

$$X_{ij} = \sum_{t=1}^{k} U_{it} V_{jt}, \tag{2.12}$$

一个关于变量 2 的二次多项式 (U, V)。每个仿射约束$\langle A_\ell, X\rangle = b_\ell$ 在代入 2 后，(U, V) 中变为一个二次多项式等式 $X = UV$。根据引理 2.7，所得存在型系统可满足，当且仅当原始 $\mathrm{ARM}(k)$ 实例可满足。该转换可在多项式时间内完成，并使位大小呈多项式增长。 □

备注 2.9（非算法性用途）。 引理 2.7 和定理2.8 仅用于在正确性证明中将低秩表述为存在见证条件。它们并未给出求解 $\mathrm{ARM}(k)$的算法；由此得到的可行性约束是双线性且非凸的。

2.5. 分块矩阵记法与指定元素

我们将通过固定元素并令较大分块矩阵中的子块相等来施加关系。本小节明确索引方式，并展示如何将这些关系编译为定义2.6中的仿射形式。

下标集与子矩阵。 对于 $n \in \mathbb{N}$，令 $[n] := \{1, \ldots, n\}$。对于 $I \subseteq [m]$和 $J \subseteq [n]$，用 $X[I, J]$ 表示将 $X \in \mathbb{R}^{m\times n}$ 限制到行下标属于 I 且列下标属于 J 所得的子矩阵。

选择矩阵。 给定 $I = \{i_1 < \cdots < i_p\} \subseteq [m]$，定义行选择矩阵 $S_I \in \{0, 1\}^{p\times m}$，使其满足 $(S_I)_{a,i_a} = 1$，其余位置均为零，因此$S_I X = X[I, :]$。给定 $J = \{j_1 < \cdots < j_q\} \subseteq [n]$，定义列选择矩阵 $T_J \in \{0, 1\}^{n\times q}$，使其满足 $(T_J)_{j_b,b} = 1$，因此 $XT_J = X[:, J]$。于是

$$X[I, J] = S_I X T_J. \tag{2.13}$$

初等矩阵和元素约束.....对于 $(i,\ j) \in [m] \times [n]$，令 $E^{(i,j)} \in \mathbb{R}^{m\times n}$ 为一个在 $(i,\ j)$ 处元素为 1、其余元素均为 0 的矩阵。于是，$X_{ij} = c$ 等价于仿射约束 $\langle E^{(i,j)},\ X\rangle = c$。

引理2.10（编译指定元素约束和块相等约束）。设 $X \in \mathbb{R}^{m\times n}$。

1. 将一组指定元素 $\{(i_t, j_t)\}_{t=1}^{T}$ 固定为常数 $\{c_t\}_{t=1}^{T}$，可表示为 T 个形如 $\langle A_\ell, X\rangle = b_\ell$ *with* $A_\ell \in \{0,1\}^{m\times n}$ 的仿射约束。*2.* 强制两个子矩阵 $X[I,J] = X[I',J']$ 与 $|I| = |I'|$ 和 $|J| = |J'|$ 相等，可表示为 $|I||J|$ 个仿射约束。

所有此类约束的有理系数位大小为 $O(1)$（索引编码除外），且编译可在关于$m+n+T$的多项式时间内计算。

证明。 **(1)** 使用 $A_\ell = E^{(i_\ell, j_\ell)}$ 和 $b_\ell = c_\ell$。

(2) 对块中的每个位置 (a,b)，强制 $X_{i_a,j_b} - X_{i'_a,j'_b} = 0$，其等于

$$\langle E^{(i_a,j_b)} - E^{(i'_a,j'_b)}, X\rangle = 0. \tag{2.14}$$

□

分块矩阵表示.. 书写时

$$X = \begin{bmatrix} X_{11} & X_{12} \\ X_{21} & X_{22} \end{bmatrix},$$

我们默认将行列下标划分为连续段；需要非连续块时，我们会明确指定下标集并使用 $X[I,J]$ 记法。

目的.. 引理2.10 确保所有以指定元素和子块相等表示的构件约束对于 $\mathrm{ARM}(k)$ 实例均有效，无需反复重新推导仿射编码。

3. 问题标准形与归约概述

本节明确归约中始终采用的源标准形和目标编码，并陈述后续各节证明的主要复杂性结论。此处不引入新的技术论证；所有非平凡的构造和正确性证明均留待第5–8节展开。本节旨在明确归约的逻辑结构，并分离出在固定秩界下必须模拟的最小代数原语。

3.1. 源标准形：算术电路等式形式的实数存在理论

如第2.1节所述，我们在标准位模型下处理实数存在理论（实数存在理论）。根据引理2.2，每个实数存在理论实例都可以在多项式时间内转换为仅由多项式等式组成的等可满足实例。

我们不直接处理显式的多项式方程，而是采用第2.2节形式化的算术电路标准形式。这种表示在 $\exists\mathbb{R}$归约中是标准做法，并允许使用局部代数约束进行逐门模拟；例如参见 [9, 15, 16]。

具体而言，每个实例都归约为一个算术电路 C，其定义在 $\mathbb{R}$上，门集合为 G，并具有指定输出门 g_{out}，使得

$$\exists x \in \mathbb{R}^n : p_C(x) = 0 \quad \Longleftrightarrow \quad \exists (z_g)_{g \in G} : \mathrm{GateEq}(C) \ \wedge \ z_{g_{\text{out}}} = 0, \tag{3.1}$$

如引理2.5所述。

每个门方程均属于以下基本类型之一：

$$\begin{aligned} &\text{(i)} \ z = x + y, \\ &\text{(ii)} \ z = x \cdot y, \\ &\text{(iii)} \ z = -x, \\ &\text{(iv)} \ z = c \quad (c \in \mathbb{Q}), \\ &\text{(v)} \ x \geq 0 \text{ or } x > 0, \end{aligned} \tag{3.2}$$

其中，不等式通过标准的基于平方与逆的编码予以消除（引理2.2）。这一受限门集合足以模拟任意实代数约束，并通常用于 $\exists\mathbb{R}$完备性构造。

3.2. 目标问题：固定秩仿射秩最小化

目标判定问题是具有固定秩界的仿射秩最小化 $k = 3$，定义见第 2.3 节。一个实例由有理仿射约束组成

$$\langle A_\ell, X \rangle = b_\ell, \qquad \ell \in [q], \tag{3.3}$$

以及全局约束

$$\mathrm{rank}(X) \leq 3. \tag{3.4}$$

该归约构造了一个全局矩阵变量 $X \in \mathbb{R}^{m \times n}$，其秩3结构作为所有电路标量的统一承载变量。每个电路

变量都由 X 中指定的一个元素表示，而变量之间的所有语义关系都通过仿射约束与秩上界共同施加。

微妙之处在于，即使将秩固定为一个较小的常数，困难性依然存在。已知固定秩代数可行性问题会表现出$\exists\mathbb{R}$-困难性，见于多种几何与矩阵实现情境；例如，参见源自 Mnëv 定理及其改进的普适性结果 [18,19]。

3.3. 秩–*3* 作为非线性强制媒介

该归约的一个核心原则是：全局秩约束与精心布置的仿射等式相结合时，可以强制实现非线性代数关系。关键观察虽初等却十分有力：若秩(X) $\leq$3，则 X 的每个 4×4 子式都必须为零。

因此，任何迫使存在一个具有非零行列式的 4×4 子矩阵的仿射约束集合，都必然违反秩上界。该机制使得形如 $z = xy$的乘法约束能够被间接强制实现：只需构造一个常数规模仿射模式，使得任何违反 $z \neq xy$ 都会在某个 4×4 子式中诱导出非零行列式。

此类基于行列式的秩障碍，是实现空间及相关秩约束模型中普适性现象的基础 [18, 19]。在本研究中，这一思想被提炼为一个具体的秩–3 强制构件，并在第5节中得到严格构造与分析。

3.4. 归约映射

现在，我们从陈述层面概述这一归约。

输入.....一个算术电路 C，其规模为 s，且处于门等式标准形式（3.1）。

输出.....一个 ARM 实例（$\mathcal{M}$ b, $k = 3$），满足：

- 矩阵维数 m, n 关于 s 呈多项式关系；
- 仿射约束的数量为 $O(s)$；
- 所有系数均为有理数，且具有多项式位长。

构造概要。

1. 引入一个矩阵变量 X，使其秩为$X \le 3$。2. 为每个电路导线出现项指定 X 中的一个指定项。3. 通过仿射等式强制满足常数、复制、加法和取负。4. 通过行列式强制构造强制满足乘法和逆关系。5. 使用基于平方与逆的编码消除不等式。6. 固定 X 的一个满秩 3×3 子矩阵，以消除规范自由度。7. 将指定输出项固定为零，以强制满足电路输出约束。

所有步骤都可在多项式时间内计算，并保持可满足性。

3.5. 主要复杂性结论

现在我们陈述并证明该构造带来的主要复杂性结论。

定理3.1. *ARM*$(k = 3)$ 在多项式时间多对一归约下是 $\exists\mathbb{R}$-困难的。

证明。 我们给出一个从某个固定的 $\exists\mathbb{R}$-困难问题出发的多项式时间多对一归约。设源实例是实数域上的一个多项式方程存在系统

$$\exists y \in \mathbb{R}^d : \quad f_1(y) = 0,\ \ldots,\ f_q(y) = 0, \tag{3.5}$$

其中每个 f_ℓ 都是具有有理系数的多项式（可以采用基于此类输入的 $\exists\mathbb{R}$标准定义）。

该归约在（3.5）的输入规模所对应的多项式时间内，构造出一个由仿射约束 ARM(3) 所指定的实例

$$\langle A_\ell, X \rangle = b_\ell, \qquad \ell = 1, \ldots, Q, \tag{3.6}$$

对于矩阵变量 $X \in \mathbb{R}^{m \times n}$，以及秩承诺

$$\operatorname{rank}(X) \le 3, \tag{3.7}$$

使得 (3.5) 可满足，当且仅当存在一个满足 (X 的 3.6)–(3.7)。

我们证明这两个方向。

可靠性。 假设（3.5）可满足，并固定一个见证 $y^\star \in \mathbb{R}^d$ ，使得对所有 $\ell \in [q]$有$f_\ell(y^\star) = 0$ 。由 $y^\star$ 我们得到对构造所用全部载体的一致实数值赋值（特别地，对每一个表示源变量或中间量的承载变量条目$X_{r,\ c}$，我们将该承载变量设为预期的实数值）。对于归约引入的每一个常数规模构件，构件层面的正确性保证提供局部因子

$$U^{(t)} \in \mathbb{R}^{m\times 3}, \qquad V^{(t)} \in \mathbb{R}^{3\times n}, \tag{3.8}$$

处于规范规范中，使得局部矩阵

$$X^{(t)} := U^{(t)}V^{(t)} \tag{3.9}$$

满足该构件的全部仿射约束，并与该构件所用的规定载体值相匹配。

该构造强制执行不相交支撑规则：除一个共享的钉住 3×3 规范块外，不同构件使用互不相交的新行与互不相交的新列。在此规则下，我们可通过逐个构件地将 $U^{(t)}$ 的行以及 $V\ ^{(t)}$ 的列复制到相应的全局指标上，并任意设定其余未定义的行/列，来定义全局因子 U， V。设

$$X := UV. \tag{3.10}$$

根据构造，在构件 t涉及的下标集上，全局因子与局部因子相同，因此 X 在每个元素上都与 $X^{(t)}$ 在构件 t中出现的每个元素上相一致。因此，每个构件中的每个仿射约束对 X都成立。由于 X 是一个 $m \times 3$ 与一个 $3 \times n$矩阵的乘积，我们还有 $\mathrm{rank}(X) \le 3$。因此，(3.6)–(3.7) 是可满足的。

完备性。 假设所构造的 ARM(3) 实例（3.6）–（3.7）是可满足的，并令 $X^\star$ 为一个可行解。根据该实例中的固定规范约束，一个固定的 3×3 子矩阵 $X^\star$ 等于一个满秩常数矩阵 B。由于 $\mathrm{rank}(X^\star) \le 3$，我们可以写成 $X^\star = UV$ 其中某个 $U \in \mathbb{R}^{m\times 3}$，$V \in \mathbb{R}^{3\times n}$。利用固定块的可逆性，我们可以在 $\mathbb{R}^3$ 中应用基变换，将 （U， V）置于规范规范下，使得固定的

行/列保持固定；在此规范下，参与约束的任何行/列都不存在剩余歧义。

现在从 $X^\star$ 中读出所有指定载体的值（即将指定元素解释为归约所预期的实数）。由于 $X^\star$满足每个构件的仿射约束，小工具级解码保证这些载体值满足预期的代数关系（复制约束、常数、加法、乘法，以及构造所编码的最终输出条件）。因此，解码后的赋值给出了一个实数见证 $y^\star$，满足（3.5）。所以源实例可满足。

映射的复杂度。对于每个源方程和每个构件，该归约仅引入常数个新的承载变量和仿射约束，并且所有系数都是有理数，其位长相对于输入描述为多项式级。因此，从（3.5）到（3.6）的映射可在多项式时间内计算，且是多对一归约。

因此 ARM(3) 是 $\exists\mathbb{R}$-难的。 □

定理 3.2。对于每个固定的 $k \geq 1$，$\mathit{ARM}(k) \in \exists\mathbb{R}$。

证明。固定 $k \geq 1$。ARM(k) 的一个实例由有理矩阵A_1、……、$A_q \in \mathbb{Q}^{m\times n}$和有理数 b_1、……、$b_q \in \mathbb{Q}$组成，并询问是否存在 $X \in \mathbb{R}^{m\times n}$ 使得

$$\langle A_\ell, X\rangle = b_\ell, \qquad \ell = 1, \ldots, q, \tag{3.11}$$

and

$$\operatorname{rank}(X) \leq k. \tag{3.12}$$

我们给出一个具有多项式方程的等价的实数域上的存在句。

为矩阵 $U \in \mathbb{R}^{m\times k}$ 和 $V \in \mathbb{R}^{k\times n}$ 引入变量，并定义

$$X := UV. \tag{3.13}$$

那么，对于任意这样的 X，(3.12) 会自动成立，因为 $\operatorname{rank}(UV) \leq k$。将 (3.13) 代入 (3.11)，对于每个 ℓ，得到

$$\langle A_\ell, UV\rangle = b_\ell. \tag{3.14}$$

（3.14）的每个左端都是次数为2的多项式，其变元为 U的各个元素

以及 V：事实上，

$$\langle A_\ell, UV\rangle = \sum_{i=1}^{m}\sum_{j=1}^{n}(A_\ell)_{ij}(UV)_{ij} = \sum_{i=1}^{m}\sum_{j=1}^{n}(A_\ell)_{ij}\sum_{t=1}^{k}U_{it}V_{tj}. \tag{3.15}$$

因此，ARM(k) 等价于存在句

$$\exists U \in \mathbb{R}^{m\times k}\ \exists V \in \mathbb{R}^{k\times n}:\ \bigwedge_{\ell=1}^{q}\Big(\langle A_\ell, UV\rangle - b_\ell = 0\Big), \tag{3.16}$$

这是一个实例 $\exists\mathbb{R}$ （对实数进行存在量化，并附有多项式等式）。因此，ARM(k) $\in \exists\mathbb{R}$。 □

推论 3.3. *ARM*($k = 3$) 是 $\exists\mathbb{R}$完全的。

证明。 由定理 3.1，ARM(3) 是 $\exists\mathbb{R}$困难的。由定理 3.2，ARM(3) $\in \exists\mathbb{R}$。因此，ARM(3)是 $\exists\mathbb{R}$完全的。 □

4. 秩–3 模板与规范固定

本节定义一个全局矩阵变量 $X \in \mathbb{R}^{m\times n}$，其秩3结构作为统一的承载变量，用于表示算术电路编码中出现的所有标量。每个电路变量都由 X 的一个指定元素表示，而所有语义关系均通过仿射约束来强制实现。由于低秩分解并非唯一，因此需要特别谨慎，确保指定元素所编码的标量值定义明确。我们通过显式规范固定来解决这一问题。

4.1. 指定值承载变量

令 $\{z_1, \ldots\ldots, z_N\}$ 表示算术电路编码（第 2 节）中引入的门变量所对应的实值变量。我们用矩阵 X 的指定元素表示每个这样的标量。

引理 4.1 （指定元素的仿射约束）。 设 $X \in \mathbb{R}^{m\times n}$。

1. 固定一个元素：对于任意 $(r, c) \in [m]\times[n]$ 和任意 $a \in \mathbb{Q}$，约束

$$X_{r,c} = a \tag{4.1}$$

可写成一个单一的仿射约束 $\langle A, X\rangle = b$。

2. 两个元素相等：对于任意 (r, c) 、 $(r', c') \in [m] \times [n]$，约束

$$X_{r,c} = X_{r',c'} \tag{4.2}$$

可写成单个仿射约束 $\langle A, X \rangle = b$。

证明。 对于（4.1），令 $A \in \mathbb{R}^{m \times n}$ 具有 $A_{r,\ c} = 1$，其余所有元素均为 0，并令$b = a$。于是 $\langle A,\ X \rangle = X_{r,\ c} = b$。

对于（4.2），令 A 具有 $A_{r,\ c} = 1$, $A_{r',\ c'} = -1$，其余所有元素均为 0，并令 $b = 0$。于是 $\langle A,\ X \rangle = X_{r,\ c} - X_{r',\ c'} = 0$。 □

定义 4.2（指定元素）。 对于每个电路变量 z_i，固定一个索引对（r_i，c_i）$\in [m] \times [n]$ 并定义

$$x_i := X_{r_i, c_i}. \tag{4.3}$$

我们将（r_i，c_i）称为承载 z_i 值的指定位置。

将指定元素固定为某个常数，或强制两个指定元素相等，都可以通过如下形式的仿射约束表示：$\langle A,\ X \rangle = b$根据引理 4.2 引理 4.1。因此，本节引入的所有约束都是 ARM(3) 的有效实例。

关键要求是映射

$$X \longmapsto (x_1, \ldots, x_N) \tag{4.4}$$

在满足秩$(X) \leq 3$ 及所有既定仿射约束的矩阵可行集上定义良好。

4.2. 秩 *3* 分解的规范自由度

根据引理 2.7，约束 $\operatorname{rank}(X) \leq 3$ 等价于存在矩阵 $U \in \mathbb{R}^{m \times 3}$ 和 $V \in \mathbb{R}^{3 \times n}$ 使得

$$X = UV. \tag{4.5}$$

这种分解并不唯一：对于任意可逆的 $G \in GL(3)$,

$$UV = (UG)(G^{-1}V). \tag{4.6}$$

这意味着规范自由度使矩阵 U 和 V 并非唯一规范。虽然乘积 X 在（4.6）下保持不变，但多个

分解引出了一个问题：解码（4.4）是否与所选分解无关。因此，必须显式进行规范固定。

4.3. 通过固定子矩阵进行规范固定

通过固定 X 的一个常数子矩阵，我们消除了所有非平凡的规范自由度。

引理 4.3（规范固定引理）。设 $I_0 \subseteq [m]$ 和 $J_0 \subseteq [n]$ 满足 $|I_0| = |J_0| = 3$。固定一个常数满秩矩阵 $B \in \mathbb{R}^{3\times 3}$（例如 $B = I_3$），并施加仿射约束

$$X[I_0, J_0] = B. \tag{4.7}$$

那么，对于满足 $\operatorname{rank}(X) \le 3$ 及所有仿射约束的任意矩阵 X，解码值 $x_i = X_{r_i,\ c_i}$ 均可被唯一确定。

证明。令 $X = UV$ 为满足（4.5）的任意一个分解。限制到固定索引后可得

$$U[I_0, :]\, V[:, J_0] = B. \tag{4.8}$$

由于 B 的秩为 3，矩阵 $U[I_0, :]$ 和 $V[:\ J_0]$ 的秩都至少为 3。由于它们是 3×3 矩阵，因此都可逆。

现在考虑两个秩 3 分解 $X = UV = U\prime V\prime$。根据（4.5），存在 $G \in GL(3)$，使得 $U\prime = UG$ 且 $V\prime = G^{-1}V$。

限制到固定索引并使用（4.6），可得

$$U[I_0, :]\, V[:, J_0] = U[I_0, :]\, G\, \left(G^{-1}V\right)[:, J_0]. \tag{4.9}$$

由于 $U[I_0, :]$ 和 $V[:\ J_0]$ 可逆，因此可推出 $G = I_3$。因此，该分解在平凡规范变换意义下是唯一的，所以 X 的每个元素，尤其是每个指定元素 $X_{r_i,\ c_i}$，在所有可容许的秩 3 分解中均保持不变。 □

注 4.4（仿射可实现性）。（4.7）中的每个等式都对应于如下形式的仿射约束 $\langle E^{(i,j)}, X\rangle = B_{ab}$。规范固定约束的数量是常数，与输入规模无关。

4.4. 一致性约束与扇出

算术电路允许不受限制的扇出：一个门的输出可以馈入多个后续门。这通过对指定元素施加相等约束来实现。

定义 4.5（一致性约束）。 如果两个电路变量 z_i 和 z_j表示同一个逻辑量，我们施加

$$X_{r_i,c_i} = X_{r_j,c_j}. \tag{4.10}$$

根据引理 4.2，每个约束（4.10）都可表示为单个仿射约束。这些约束确保导线的所有复制都携带相同的解码后标量值。

4.5. 良定义性与可靠性

现在，我们将秩–3 模板所提供的正确性保证分别讨论。

引理 4.6（解码的良定义性）。 对于任意满足 X 秩条件 $\mathrm{rank}(X) \le 3$以及第 *4.1–4.4*节所有约束的 （x_1，……， x_N），其解码值均唯一确定。

证明。 这可直接由引理 4.3 以及指定条目的定义得出。 □

引理 4.7（语义正确性）。 编码电路门和导线相等关系的所有仿射约束，均由解码值（x_1，……， x_N）精确满足。

证明。 每个门约束都通过指定元素之间的仿射等式直接施加。根据引理 4.6，解码值唯一地满足这些等式。 □

定理 4.8（秩–3 编码的可靠性）。 由该电路构造的秩–3 *ARM* 实例可满足，当且仅当原算术电路可满足。

证明。 （若）给定电路变量的一个满足赋值，通过固定规范块（X 4.9），根据电路值为每个指定元素赋值，并补全其余元素以得到一个秩–3矩阵。

（仅当）给定一个可行的 X，通过（4.3）解码电路值。根据引理4.6 和 4.7，这些值满足所有电路约束。 □

5. 秩强制原语

本节构建归约的核心技术工具：秩强制原语，它们仅使用仿射约束和全局秩上界$\mathrm{rank}(X) \leq 3$来强制非线性代数关系。此处引入的所有约束均为有效的 ARM(3) 实例（定义2.6），且与第3节的秩模板及规范固定约束兼容4。

核心结果是一个基于行列式的强制构件，用于强制指定标量变量之间满足形如 $c = ab$ 的乘法关系。该构件取代了早期归约中使用的所有基于子式的约束，是整个构造的技术核心。

5.1. 全局秩约束下的强制

我们先介绍两个基本但至关重要的线性代数事实。

引理 5.1 (秩的单调性**)。** 设 $X \in \mathbb{R}^{m\times n}$，且令 Y 为 X 的任意子矩阵。那么

$$\mathrm{rank}(X) \;\geq\; \mathrm{rank}(Y).$$

证明。 在将 Y的任意一组线性无关的行（或列）视为 X的行（或列）时，它们仍然线性无关。 □

引理 5.2 （ 4×4 子式的消失）。 若秩$(X) \leq 3$，则 X 的每个 4×4子式的行列式都为零。

证明。 X 的一个 4×4 子矩阵的秩至多为秩$(X) \leq 3$，因此其行列式为零。 □

引理 5.1 和5.2 形式化了本节中使用的强制原理：任何对双线性恒等式的违反，只要会产生一个满秩的 4×4 子矩阵，就必然与全局秩上界矛盾。

5.2. 行列式强制构造

现在我们介绍关键的强制原语。

引理 5.3 （行列式强制构造）。 存在一个常数规模的仿射约束系统，作用于矩阵 $X \in \mathbb{R}^{m\times n}$，其指定元素为$a$、$b$、$c$，满足：

(可靠性**)** 如果 X 满足所有约束且 秩$(X) \leq 3$，那么

$$c = ab. \tag{5.1}$$

(完备性) 对于满足 $c = ab$ 的任意实数 (a, b, c)，存在一个可行矩阵，其秩$(X) \le 3$，并且满足所有约束。

构造。固定两个行索引 r_1，r_2 和两个列索引 c_1，c_2。施加仿射约束

$$X[\{r_1, r_2\}, \{c_1, c_2\}] = \begin{pmatrix} 1 & a \\ b & c \end{pmatrix}. \tag{5.2}$$

的所有其他元素均不受约束，但须满足第4节的规范固定约束。约束（5.2）通过四个指定元素约束（引理 4.1）实现。

5.3. 代数秩障碍

该构件的强制作用由以下明确的秩障碍刻画。

引理 5.4（通过 4×4 行列式的秩障碍）。假设施加了第 *4* 节的规范固定约束，从而固定了一个满秩 3×3 子矩阵$X[I_0, J_0] = B$。若指定元素满足 $c \neq ab$，则

$$\operatorname{rank}(X) \ \ge \ 4.$$

证明。令 i_1，$i_2 \in I_0$和 j_1，$j_2 \in J_0$为任意两个索引。考虑 4×4子矩阵

$$Y = \begin{pmatrix} B[i_1, i_1] & B[i_1, i_2] & 0 & 0 \\ B[i_2, i_1] & B[i_2, i_2] & 0 & 0 \\ 0 & 0 & 1 & a \\ 0 & 0 & b & c \end{pmatrix}.$$

由于 B 可逆，左上角的 2×2 块具有非零行列式。Y 的行列式可分解为

$$\det(Y) = \det(B[i_1, i_2; i_1, i_2]) \cdot (c - ab).$$

若 $c \neq ab$，则 $\det(Y) \neq 0$，因此 $\operatorname{rank}(Y) = 4$。根据引理 5.1，$\operatorname{rank}(X) \ge \operatorname{rank}(Y) = 4$。 □

5.4. 构造元的可靠性

引理的证明 *5.3*(可靠性)。假设 X 满足所有约束，并且秩$(X) \le 3$。若 $c \neq ab$，引理5.4则推出 秩$(X) \ge 4$，矛盾。因此 $c = ab$。 □

5.5. 构造性完备性

引理的证明 *5.3*(完备性)。 假设 $c = ab$。按照第 $X[I_0, J_0] = B$ 4 节中的设定固定规范块。定义三个向量 u_1、u_2、$u_3 \in \mathbb{R}^n$，分别对应三个规范行。将两个构件行明确写为

$$(1, a) = \alpha_1 u_1 + \alpha_2 u_2 + \alpha_3 u_3, \qquad (b, c) = b(1, a),$$

这些系数 α_i 存在，因为规范行张成了 $\mathbb{R}^3$。 X 的所有其余行均定义为 u_1、u_2、u_3 的任意线性组合。因此， X 的每一行都位于一个 3 维子空间中，所以 $\mathrm{rank}(X) \leq 3$。根据构造，所有仿射约束均得到满足。 □

5.6. 非退化性与唯一性

引理 5.5 (无伪解)。 在规范固定约束下，行列式强制构件不存在满足 $\mathrm{rank}(X) \leq 3$ 且$c \neq ab$的可行解。

证明。 由引理5.4可直接得出。 □

5.7. 复杂度核算

引理 5.6 （原语复杂度）。 每个行列式强制构造使用：

- $O(1)$行和列，
- 恰好四个指定元素约束，
- $O(1)$ 个仿射约束，系数取自$\{0, \pm 1\}$。

5.8. 在归约中的作用

引理 5.3 是该归约的基本非线性强制原语。它使算术电路编码（第2.2节）中的乘法门能够通过仿射约束和全局秩上界得到精确模拟。结合等式约束和规范固定约束，它完成了在 ARM(3)中对任意算术电路的模拟。

6. 编译为仿射约束的门小工具

本节通过将算术电路（第2.2节）的每个门编译为全局矩阵变量 $X \in \mathbb{R}^{m\times n}$上的一个常数规模仿射约束集合，并加上唯一的全局约束 $\operatorname{rank}(X) \leq 3$，从而完成该归约。所有非线性语义都仅通过秩障碍来强制实现，所用的是第5节提出的行列式强制原语。

在全文中，标量变量 x、y、z表示 X （定义 4.2）中指定元素的解码值。

6.1. 常数与复制约束

构造约定（新索引与出现位置载体）。在下文的编译过程中，每个门小工具 $\mathcal{G}$ 都分配有自己独立的新辅助行索引 $\mathcal{I}(\mathcal{G}) \subseteq [m]$ 和辅助列索引 $\mathcal{J}(\mathcal{G}) \subseteq [n]$，且与其他所有构件的辅助索引互不相交。此外，我们采用基于出现位置的承载变量：电路值的每个出现位置（例如，作为其他地方输入的门输出、扇出等）都有自己的指定位置 (r, c)；当两个出现位置必须表示同一个标量时，我们仅通过显式仿射复制约束（形式为 (6.2)）来强制它们相等。因此，构件可以通过复制约束共享值，但绝不会重复使用相同的辅助索引，也不会依赖于在不同构件之间重复使用相同的承载位置。

常数构件.. 要强制 $x = c$ 对 $c \in \mathbb{Q}$成立，施加

$$X_{r_x,c_x} = c. \tag{6.1}$$

复制构件.. 要强制 $x = y$，施加

$$X_{r_x,c_x} - X_{r_y,c_y} = 0. \tag{6.2}$$

扇出与线路出现位置。当电路中某处产生的标量被多次使用时（例如，某个门的输出馈入后续多个门），我们不会在这些用途中重复使用同一个指定位置（r，c）。相反，每次使用都会分配一个新的指定载体项，并且仅通过一组形如（6.2）的复制约束来强制所有此类出现项相等。整个编译过程中均采用这一约定，这对第3 节中的全局秩–8嵌入论证至关重要。

引理 6.1（常数与复制正确性）。约束（6.1）和（6.2）分别强制满足 $x = c$ 和 $x = y$，且与秩约束无关。

证明。 等式 (6.1) 通过仿射等式将指定条目X_{r_x,c_x} 设为有理常数 c，因此无论秩(X)如何，任何可行解中的解码值都满足 $x = c$。同理，(6.2) 是仿射等式 $X_{r_x,c_x} = X_{r_y,c_y}$，因此任何可行解中的解码值都满足 $x = y$，同样与秩(X)无关。 □

6.2 加法与取反构造

引理 6.2 (加法构造)。 存在一个常数规模仿射系统，可强制满足

$$z = x + y. \tag{6.3}$$

证明。 设 $(r_x, c_x), (r_y, c_y), (r_z, c_z)$ 分别是 x, y, z 的指定载体。施加以下单个仿射约束

$$X_{r_z,c_z} - X_{r_x,c_x} - X_{r_y,c_y} = 0,$$

它关于 X 的各个条目是线性的。解码得到 $z - x - y = 0$，即 $z = x + y$。该系统规模为常数（一个方程）。 □

引理 6.3 (取反构造)。 存在一个常数规模仿射系统，可强制满足

$$z = -x. \tag{6.4}$$

证明。 施加仿射约束

$$X_{r_z,c_z} + X_{r_x,c_x} = 0.$$

解码得到 $z + x = 0$，因此得到 $z = -x$。同样，该系统具有常数规模。 □

6.3 乘法构造

使用引理 5.3 的行列式强制原语来强制实现乘法。

引理 6.4（乘法正确性）。 存在一个常数规模仿射系统，使得在 $\mathrm{rank}(X) \le 3$ 的条件下，

$$z = xy. \tag{6.5}$$

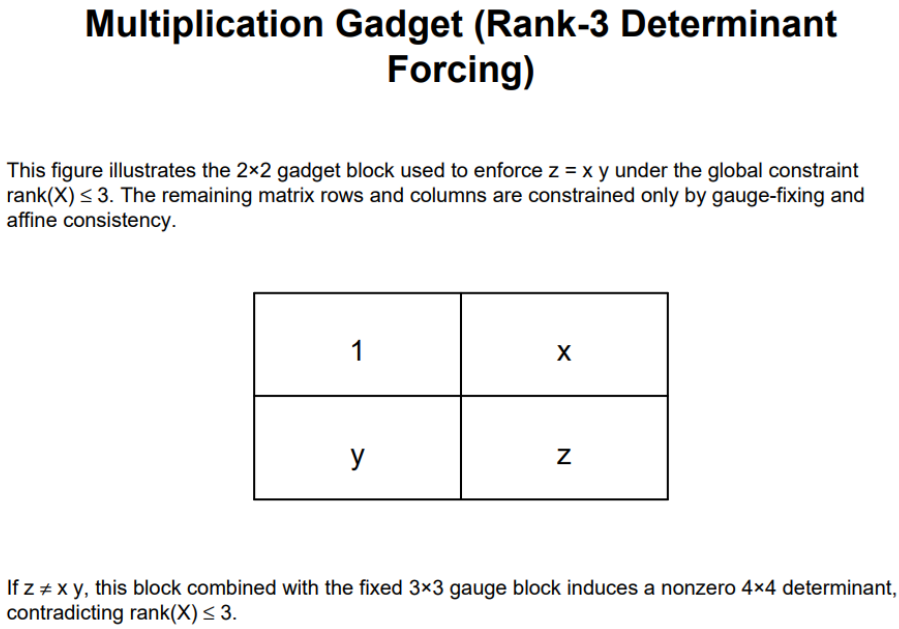

图 1：行列式强制乘法组件。 2×2 块与固定的 3×3 规范块组合；对 $z = xy$ 的任何违反都会导致非零的 4×4 行列式。

证明。对承载 x、 y、 z 的指定元素应用引理 5.3 中的行列式强制构造。根据该引理，此构件仅引入$O(1)$个辅助项（因此有 $O(1)$个仿射约束），并具有以下两个性质。

可靠性。 若 $z \neq xy$，则引理 5.4 保证存在一个 4×4 子式，其对应的受约束矩阵的行列式非零。因此，任何满足构件约束的矩阵，其秩都至少为4，这与全局约束$\text{rank}(X) \leq 3$矛盾。因此，在$\text{rank}(X) \leq 3$的条件下，可行性要求 $z = xy$。

完备性。 若 $z = xy$，则引理 5.3 明确构造出一个矩阵，满足所有构件仿射约束，且秩至多为3。将这个常数规模的补全嵌入全局矩阵（使用新索引），可保持可行性和秩 ≤ 3。

因此该构件强制执行（6.5）恰好在秩$(X) \leq 3$下。 □

6.4. 逆运算与非零约束

引理 6.5 （逆运算小工具）。 在秩$(X) \leq 3$下，用于强制执行的仿射约束

$$xy = 1 \tag{6.6}$$

蕴含 $x \neq 0$ 和 $y = 1/x$。

证明。约束 (6.6) 由乘法小工具（引理 6.4）实现，并使用引理 6.1将指定输出固定为常数 1。因此，在 秩$(X) \leq 3$ 的条件下，可行性意味着 $xy = 1$ 在实数域上成立。

如果 $x = 0$，那么对于所有 y， $xy = 0$ ，这与 $xy = 1$ 矛盾。因此 $x \neq 0$。由于 $x \neq 0$，将 $xy = 1$ 两边除以 x ，得到 $y = 1/x$。 □

6.5. 通过平方表示不等式

引理 6.6 (非负性)。 标量 x 满足 $x \geq 0$ 当且仅当存在 s 使得

$$x = s^2. \tag{6.7}$$

证明。 (⇒) 若 $x \geq 0$，令 $s := \sqrt{x} \in \mathbb{R}$。则 $s^2 = x$。

(⇐) 若存在实数 s使得 $x = s^2$ ，则 $x \geq 0$ ，因为实数的平方非负。 □

引理 6.7 (严格正性)。 标量 x 满足 $x > 0$ 当且仅当存在 s、t使得

$$x = s^2, \qquad st = 1. \tag{6.8}$$

证明。 (⇒) 若 $x > 0$，令 $s := \sqrt{x} > 0$ ，并设 $t := 1/s$。则 $x = s^2$ 且$st = 1$。

(⇐) 若实数 s, t满足 $x = s^2$ 和 $st = 1$ ，则 $st = 1$ 意味着 $s \neq 0$。因此 $x = s^2 > 0$。 □

实现.....约束（6.7）和（6.8）通过以下方式实现：为 s （以及在需要时为 t ）引入新的指定载体，使用引理 $x = s^2$6.4 （两个输入均为 s ）来施加 $st = 1$ ，并结合引理 6.4 和引理 6.1 来施加 逆运算结论由引理 6.5 证明。

6.6. 门级与电路级完备性

电路编译的索引约定.....在电路级编译中，每个门实例都会被转换为独立的常数规模构件，并使用新的辅助行/列，且这些辅助行/列不会在不同门之间重复使用。此外，我们将每个出现位置的线路值视为 X中的一个独立指定条目：如果某个输出连接到多个后续门，则为每次使用分配一个独立的载体位置，并通过形式为（6.2）的复制约束显式保证各次出现的值相等。这一约定确保所有构件都在不相交的辅助支撑集上组合，并且电路中值的共享仅通过显式的仿射一致性约束实现。

定理 6.8（门完备性）。 电路模型 $\mathbb{R}$ 中使用的每个算术门（见第 *2.2* 节）都可以编译为 $O(1)$ 个仿射约束，使得在 $\operatorname{rank}(X) \leq 3$ 的条件下，解码值满足精确的门语义。

证明。 根据构造，第 2.2 节使用的门集合仅通过上述构件进行编译：常数和复制（引理 6.1）、加法和取负（引理 6.2–6.3）、乘法（引理 6.4）、求逆/非零（引理 6.5），以及（必要时）化归为平方约束和求逆约束的不等式（引理 6.6–6.7 以及实现段落）。

这些构件均仅使用 $O(1)$ 个仿射约束，且都是正确的：对于线性门，其正确性与秩无关（引理 6.1、6.2、6.3）；对于非线性基本操作，在$\operatorname{rank}(X) \leq 3$ 的条件下，其正确性由秩障碍（引理 6.4、6.5）以及不等式的实代数等价关系（引理 6.6、6.7）保证。因此，任何单个门实例都可以编译为 $O(1)$ 个仿射约束，其在 $\operatorname{rank}(X) \leq 3$ 条件下的可行性会确保精确的门语义。

□

注记 6.9（所有构造组件补全的统一规范）。 所有门构件均在相同的固定块约束 $X[I_0, J_0] = B$ （引理4.3）下完成。特别是，每当我们调用门级完备性来声称某个构件存在一个秩为3 的见证矩阵时，我们都可以（也将会）将该见证表示为由固定块诱导的规范规范，即选择一个分解 $X = UV$，其中 $U[I_0, :\ ] = I_3$且$V[J_0, :\ ] = B^\top$。采用这一统一规范，便可在第8节将所有构件见证嵌入单个全局分解中，而不会出现因子层面的不一致。

推论 6.10（线性规模的电路编译）。 大小为 s 的算术电路可以编译为一个包含 $O(s)$ 个仿射约束和变量的 *ARM(3)* 实例。

证明。 电路中的每个门都被编译为一个常数规模构件，其中包含$O(1)$个仿射约束和 $O(1)$个新的辅助索引（行/列和指定载体）。根据上述索引约定，构件不会重复使用辅助索引，并且每个导线出现项至多引入一个额外载体以及 $O(1)$个复制约束。因此，仿射约束和辅助变量的总数随门实例和导线出现项的数量线性增长；对于大小为 s的电路，两者均为 $O(s)$。因此，所得 ARM(3) 实例的大小为 $O(s)$。

□

6.7. 归约的全局正确性

定理 6.11（ARM(3) 编码的正确性）。 构造出的 *ARM(3)* 实例可行，当且仅当原算术电路可满足。

证明。 （⇒）假设 ARM(3) 实例可行：存在 $X \in \mathbb{R}^{m\times n}$满足所有编译后的仿射约束，且 秩$(X) \leq 3$。读取指定载体的值，对每个电路导线出现项进行解码（定义4.2）。复制约束（6.2）确保所有应当相等的出现项都解码为相同的实数值（引理 6.1）。对于每个门实例，相应的构件约束在 X 中成立；根据定理 6.8 （秩(下编译后构件的可靠性 $X) \leq 3$），解码值满足精确的门语义。因此，通过对电路有向无环图进行拓扑求值，解码后的赋值满足每个门方程，从而电路在 $\mathbb{R}$ 上可满足。

(⇐) 假设该算术电路可满足。固定一个满足赋值，为每个导线出现项赋予实数值，并确保这些值符合扇出关系。对于每个门实例，根据定理 6.8 （相应构件的完备性），存在一个秩为 3 的补全，在固定块条件下满足该门的仿射约束。采用新索引约定，将每个常数大小构件的补全嵌入全局矩阵中互不相交的辅助支撑集上，并通过复制约束强制导线出现项之间相等。由于这些构件仅共享指定值（以及公共固定块），它们可以组合而互不干扰，从而得到一个全局可行矩阵 X，其秩$(X) \leq 3$ 满足所有仿射约束。因此，该 ARM(3) 实例可行。

□

6.8. 秩*3*极小性

引理 6.12 （秩–3 行列式强制的极小性）。 秩–2 矩阵无法支持引理 *5.3*中所用形式的基于行列式的乘法强制：每个 3×3 子式都恒等于零。因此，任何依赖非零 3×3 或 4×4 子式作为障碍的构造，都无法在全局秩上界 秩$(X) \leq 2$ 下强制 $z = xy$ 。

证明。 若 秩$(X) \leq 2$，则 X 的任意三行集合都线性相关，因此每个 3×3 子式的行列式都等于 0。特别地，任何 4×4 子式的行列式也等于 0 ，因为秩 ≤ 2 意味着 $k \times k$ 的所有 $k \geq 3$子式都为零。行列式强制原语（第 5 节）通过构造一个大小至少为 3且行列式非零的子式来导出矛盾，当 $z \neq xy$时便会出现这种情况。在 秩$(X) \leq 2$的条件下，这种障碍不可能存在。因此，秩 3 是这种基于行列式的强制机制能够发挥作用的最低秩。 □

备注 6.13。 引理6.12 形式化说明了为什么秩–3 是与我们的乘法小工具相容的最小全局秩上界，并且进而也是在本框架中实现非线性算术精确模拟的最小上界。

7. 归约接口：从实数存在理论/电路到 ARM(3)

本节结束构造层，并开启正确性层。前面的构造已经说明，如何在全局约束秩$(X) \leq 3$ (定理 4.8) 下，将每个算术门编译为常数大小的仿射构件；这意味着，大小为 s 的电路可得到一个ARM(3)实例，其中有 $O(s)$个指定载体和 $O(s)$个仿射约束。这里我们给出归约映射，并记录精确的等价性陈述，以供可靠性与完备性证明使用；这两个证明将通过全局复合进行（引理 8.4）。

7.1. 回顾源标准形：电路/门形式的实数存在理论

我们将标准位模型下的实数存在理论（ETR）作为源语言，即形如以下形式的语句

$$\exists x \in \mathbb{R}^n : \ \varphi(x), \tag{7.1}$$

其中 φ 是多项式谓词的无量词布尔组合。按照本文中的约定，我们采用以下标准编译流水线。

实数存在理论实例可在多项式时间内转换为一个算术电路C 以及单个输出约束 $p_C(x) = 0$，随后再转换为相应的门变量约束系统 GateEq(C)，以编码电路语义。

具体而言，给定一个电路 C，其门集合为 G，指定输出门为g_{out}，我们为每个门 $g \in G$ 引入一个实变量 z_g，并针对每个门施加一个等式，以定义 GateEq(C)（第 1.2 节）。其关键的精确性保证是：

$$p_C(x) = 0 \quad \Longleftrightarrow \quad \exists (z_g)_{g\in G} \in \mathbb{R}^{|G|} : \ \mathrm{GateEq}(C) \ \wedge \ z_{g_{\text{out}}} = 0, \tag{7.2}$$

这就是标准的电路语义等价性。

7.2. 目标格式回顾：带有指定载体的 ARM(3)

一个 ARM(3) 实例由有理仿射约束组成

$$\langle A_\ell, X\rangle = b_\ell, \qquad \ell \in [q], \tag{7.3}$$

以及秩上界

$$\mathrm{rank}(X) \le 3, \tag{7.4}$$

其中 $\langle A, \ X\rangle$ 是弗罗贝尼乌斯内积。

为了将电路标量编码到单个矩阵变量 $X \in \mathbb{R}^{m\times n}$中，我们使用指定元素(定义4.2)：对于每个电路门变量（按照电路编译约定，也就是每个导线出现项），我们固定一个载体位置(r_i, c_i) 并解码

$$x_i := X_{r_i,c_i}. \tag{7.5}$$

扇出通过显式的仿射一致性约束来处理，这些约束使各载体相等（定义2.4），即形如 $X_{r_ic_i} = X_{r_jc_j}$ 的约束。

最后，所有构件均在同一固定块约束（引理4.3）下完成，该约束固定一个满秩 3×3 子矩阵 $X[I_0, J_0] = B$；这消除了非平凡的规范自由度，并确保解码（7.5）在可行集上定义良好。

7.3. 归约映射（陈述层面）

给定一个采用门变量形式的电路实例 $\mathrm{GateEq}(C) \wedge z_{g_{\text{out}}} = 0$ 2.2，我们按如下方式构造一个 ARM(3)实例。

1. 为每个导线出现项和每个门输出指定一个载体 $(r_i,\ c_i)$ （定义4.2和定义8.1–8.2）。2. 对于扇出所要求的每个等式，添加相应的一致性约束，使两个指定载体相等（定义 2.4）。3. 对于 GateEq(C)中的每个门方程，添加第 4节构造的常数规模仿射构件约束：常数/复制（引理 4.1）、加法/取负（引理 4.3）、通过行列式强制实现乘法（ 3），以及（当电路模型中存在时）求逆/非零和不等式编码（ 4.4）。

4. 为 $z_{g_{\text{out}}}$ 的承载变量添加输出约束 $X_{r_{\text{out}},\ c_{\text{out}}} = 0$ 。

根据构造，上述每个约束都是仿射的，并且可以用7.3输入格式（引理 4.1）表示。

7.4. 规模与编码保证

我们将复杂度归约所需的记账事实单独列出。

引理 7.1 （线性规模编译）。 设 C 是一个含有 s个门的算术电路。第 *6*、 *7*节所述的编译会生成一个含有 ARM(3)实例，其中包含O（s）个指定载体，以及 O（s）个仿射约束。

证明。 C 中的每个门都会被转换为一个常数规模构件：该构造为每个门构件引入 O(1) 个新的辅助行/列和 O(1) 个仿射约束，并且每个门只引入 O(1) 个指定载体（用于该构件的输入/输出载体）。构件之间唯一共享的对象是固定的规范块索引 I_0， J_0 及其对应的固定约束，这些约束额外贡献 O(1) 个约束。因此，对 s个门求和可得 O(s) 个指定载体和 O(s) 个仿射约束。 □

引理 7.2 （多项式位长复杂度）。该归约生成的有理数约束数据，其总位长关于输入电路的位长为多项式。

证明。 除将指定元素固定为电路常数的约束外，所有构件约束都使用常数数量的仿射等式，其系数矩阵的元素属于$\{0, \pm 1\}$。这些常数直接从电路描述中复制。规范固定约束将一个常数规模的

3×3 块固定为有理数数据。由引理 $O(s)$ 7.1可知，约束总数为 s，且每个约束的有理数编码长度均为多项式级，因此总编码长度是输入规模的多项式（实际上，除输入常数的位长外，它关于 s 呈线性）。

□

7.5. 正确性接口定理（已在 *5* 中证明）

引理 7.3（电路语义等价性）。设 C 是定义在 $\mathbb{R}$ 上、门集合为 G、输出门为 g_{out} 的算术电路，并设指定的输入元组为 x（赋给输入门）。令 $z_g \in \mathbb{R}$ 表示门 g 上携带的值。令$\mathrm{GateEq}(C)$ 表示所有门方程的合取，这些门方程用于约束 C 中每个门（输入、常数、加法、乘法）的局部语义。令 $p_C(x)$ 表示在输入 x 上求值该电路所得到的实数（即在 C 的唯一语义下，输出门上的值）。那么

$$p_C(x) = 0 \quad \Longleftrightarrow \quad \exists (z_g)_{g \in G} \in \mathbb{R}^{|G|} : \ \mathrm{GateEq}(C) \ \wedge \ z_{g_{\text{out}}} = 0. \tag{7.6}$$

证明。（$\Rightarrow$）假设 $p_C(x) = 0$。按照拓扑序，逐门计算电路 C 在输入 x 上的值。由此为每个门 $g \in G$ 生成一个值 $z_g \in \mathbb{R}$，满足：（i）对于每个输入门或常数门，z_g 等于其指定值；（ii）对于每个加法门 g，若其子节点为 g_1、g_2，则有 $z_g = z_{g_1} + z_{g_2}$；（iii）对于每个乘法门 g，若其子节点为 g_1、g_2，则有 $z_g = z_{g_1} z_{g_2}$。因此，对于此赋值 $(z_g)_{g \in G}$，GateEq(C) 成立。此外，根据 $p_C(x)$ 的定义，它是输出值，因此 $z_{g_{\text{out}}} = p_C(x) = 0$。所以，式 (7.6) 的右侧成立。

($\Leftarrow$) 假设存在一个赋值 $(z_g)_{g \in G}$，满足 GateEq(C) 和 $z_{g_{\text{out}}} = 0$。约束 GateEq(C) 确保每个门值都与其局部运算及其子门一致。由于电路无环，这些方程通过沿任意拓扑序进行归纳，唯一确定了每个门值。特别地，输出门处所规定的值等于电路求值 $p_C(x)$。因此 $p_C(x) = z_{g_{\text{out}}} = 0$，从而证明了左侧。

□

现在我们陈述完成 $\exists\mathbb{R}$-困难性证明流程所需的等价关系。

定理 7.4 (电路可满足当且仅当编译后的 $\mathrm{ARM}(3)$ 实例可行**)**。令C 为算术电路实例，并令 p_C 表示输出多项式。令 $\boldsymbol{I}(C)$ 为通过应用构件构造以及接口映射（指定载体、一致性）得到的 $\mathrm{ARM}(3)$ 实例

约束，以及固定块）。然后

$$\exists x \in \mathbb{R}^n : \; p_C(x) = 0 \quad \Longleftrightarrow \quad \exists X \in \mathbb{R}^{m \times n} : \; \operatorname{rank}(X) \le 3 \; \wedge \; X \models \mathcal{I}(C). \tag{7.7}$$

证明。 我们证明两个方向。

可靠性（⇒）.. 假设 $\exists x \in \mathbb{R}^n$ 使得 p_C（x） $= 0$。根据引理 7.3，存在门值赋值 （z_g）$_{g \in G}$ 满足门方程GateEq(C) 与 $z_{g_{\text{out}}} = 0$。利用这些值，为归约中使用的所有指定载体赋予一致的实数（输入、中间门输出以及任何复制项），并且根据构造遵守每一条仿射复制/常数约束。

对于由编译产生的每个构件$\mathcal{G}_t$ ，构件级完备性性质给出局部因子

$$U^{(t)} \in \mathbb{R}^{m \times 3}, \qquad V^{(t)} \in \mathbb{R}^{3 \times n}$$

在规范规范下，使得 $X^{(t)} : = U^{(t)} V^{(t)}$ 满足 $\mathcal{G}_t$ 的所有仿射约束，并且匹配$\mathcal{G}_t$所使用的指定载体值。将引理 8.4 应用于所有构件的族，我们得到全局因子 U， V 处于同一规范规范下，使得全局矩阵

$$X := UV \tag{7.8}$$

同时满足所有构件约束，并匹配所有指定载体值。由于 X 是一个 $m \times 3$ 与一个 $3 \times n$ 矩阵的乘积，秩$(X) \le 3$ 成立。因此 $X \models \mathcal{I}(C)$，从而确立正向。

完备性（⇐）.....假设存在 $X \in \mathbb{R}^{m \times n}$ 使得 秩$(X) \le 3$且 $X \models \mathcal{I}(C)$。根据引理 8.3，我们可以固定一个处于规范规范下的秩–3 分解 $X = UV$。从 X中读出所有指定载体的值（即编码电路输入、门输出和复制项的指定元素）。由于 X 在 秩$(X) \le 3$条件下满足每个构件的仿射约束，构件级可靠性意味着这些解码后的载体值逐门满足预期的代数关系；特别是，解码后的门值满足 GateEq(C)，而编译后的输出条件则强制解码后的输出值等于 0。

因此，根据引理 7.3，存在一个输入赋值 $x \in \mathbb{R}^n$ 使得 $p_C(x) = 0$，从而证明了反向。 □

对 $\exists\mathbb{R}$ 的推论。定义 $\exists\mathbb{R}$ 的标准归约，使我们能够从实数域上的多项式方程存在系统出发，并在多项式时间内将其编译为如下形式的算术电路可满足性实例 $\exists x \in \mathbb{R}^n : \; p_C(x) \; = 0$。因此，应用定理 7.4 可得$\exists\mathbb{R}$-难性，即 ARM(3) 的难性。此外，对于每个固定的 $k \geq 1$， $\mathrm{ARM}(k) \in \exists\mathbb{R}$ 可通过一个显式的秩 k 分解见证得到。因此，ARM(3)是 $\exists\mathbb{R}$-完全的。

8. 正确性证明

本节证明该归约具有双向正确性：**可靠性** (满足电路的赋值会产生一个可行的 ARM(3) 实例）以及**完备性** （一个可行的 ARM(3) 解可解码为满足电路的赋值）。唯一真正微妙之处在于全局一致性：许多常数规模构件叠加在同一个矩阵中，我们必须确保它们能够组合在一起，而不会产生任何隐含的代数耦合。我们通过以下方式使这一点严谨化：**(i)** 记录第 6 节构造所保证的索引规范属性；**(ii)** 利用引理 4.3 的固定块，为秩 3 分解固定一个规范规范；**(iii)** 证明所有构件见证都能嵌入同一个全局分解 $X = UV$ 中。

下面始终采用定义 4.2 中指定的载体约定：对于每个电路值 z_i ，记作

$$x_i \; := \; X_{r_i,c_i},$$

其中 $(r_i, \; c_i)$ 是归约所指定的载体位置。

8.1. 索引规范与规范规范

我们首先将由构造（第 6 节，第 6.1 小节和 5.5 小节）保证的两个性质形式化；下文的证明中将反复用到它们。

定义 8.1 （新辅助索引）。归约引入的每个构件 $\mathcal{G}$ 都附带一组辅助行索引 $\mathcal{I}(\mathcal{G}) \subseteq [m]$ 和一组辅助列索引 $\mathcal{J}(\mathcal{G}) \; \subseteq [n]$ ，满足

$$\mathcal{I}(\mathcal{G}) \cap \mathcal{I}(\mathcal{G}') = \emptyset, \qquad \mathcal{J}(\mathcal{G}) \cap \mathcal{J}(\mathcal{G}') = \emptyset \quad \text{for all } \mathcal{G} \neq \mathcal{G}'.$$

唯一可在各构件之间共享的索引，是全局规范集$I_0 \subseteq [m]$、 $J_0 \subseteq [n]$，以及由复制约束显式关联的指定载体索引。

定义 8.2（基于出现位置的载体）。 每一次出现的电路值（变量使用、扇出或门输入）都会被分配其自身的指定载体位置（r， c）。每当两处出现必须表示同一标量时，归约仅通过显式仿射复制约束（第6.1节）加以强制，而绝不会通过在两个不同构件中复用同一载体位置来实现。

定义 8.1–8.2 消除因子级冲突：构件可以共享取值（通过显式复制约束），但绝不会争用同一组辅助索引，也绝不会迫使不同的局部构造为同一因子行/列赋予不兼容的向量。

接下来，我们回顾固定规范块，并证明它为秩 3 分解导出一个典范规范。

引理 8.3 (规范固定与典范因子**)。** *ARM*(3) 实例包含仿射约束，用于固定一个 3×3 块

$$X[I_0, J_0] \;=\; B, \tag{8.1}$$

其中 $B \in \mathbb{R}^{3\times 3}$ 为固定值，且 $\det(B) \neq 0$ (如引理 *4.2*中构造）。若$\mathrm{rank}(X) \leq 3$ 且 (8.1) 成立，则存在因子

$$U \in \mathbb{R}^{m\times 3}, \qquad V \in \mathbb{R}^{3\times n} \quad \textit{such that} \quad X = UV$$

具有典范规范

$$U[I_0, :] = I_3, \qquad V[:, J_0] = B. \tag{8.2}$$

此外，一旦施加 (8.2)，就不存在剩余的 $GL(3)$ 规范自由度：任何其他满足条件的秩 3 分解 X 若满足 (8.2)，则必须在参与归约约束的所有行/列上与 (U, V)一致。

证明。 由于秩$(X) \leq 3$，对某些 $\widetilde{U} \in \mathbb{R}^{m\times 3}$ 和 $\widetilde{V} \in \mathbb{R}^{3\times n}$，记作 $X = \widetilde{U}\widetilde{V}$。限制到固定块可得

$$B = X[I_0, J_0] = \widetilde{U}[I_0, :]\, \widetilde{V}[:, J_0]. \tag{8.3}$$

由于 B可逆， $\widetilde{U}[I_0, :]$可逆。定义 $G := \widetilde{U}[I_0, :]^{-1}$并令$U := \widetilde{U}G$, $V := G^{-1}\widetilde{V}$。那么 $X = UV$仍然成立，且 $U[I_0, :] = I_3$。最后，

$$B = X[I_0, J_0] = U[I_0, :]\, V[:, J_0] = V[:, J_0], \tag{8.4}$$

因此 $V[:, J_0] = B$。这证明了规范规范下分解的存在性。

为了证明规范规范中的唯一性，假设 $X = U_1V_1 = U_2V_2$ 是两个满足 $U_k[I_0,:] = I_3$ 的分解以及 $V_k[:, J_0] = B$ 其中 $k = 1, 2$。由于 $U_1[I_0,:] = U_2[I_0,:] = I_3$，任何将这两个分解联系起来的换基矩阵 $H \in GL(3)$ 都必须满足 $I_3 = U_2[I_0,:] = U_1[I_0,:]H = H$，因此 $H = I_3$。所以，在通过构造受到约束的每一行/列上，$U_1 = U_2$ 和 $V_1 = V_2$ 均成立（特别是，任何出现在构件约束中的行/列，都会通过定义该构件的仿射等式与规范块相连）。因此，一旦在受约束的支撑集上施加（8.2），就不存在剩余的规范自由度。

□

8.2. 全局嵌入引理

现在，我们将以尽可能强的形式形式化构件组合：我们从不拼接分别计算出的矩阵，而只拼接单个全局因子对的行/列。

引理 8.4（构件见证的全局嵌入）。 固定规范规范（8.2）。考虑由归约生成的任意构件族 $\{\mathcal{G}_t\}_{t=1}^{T}$，以及对所有指定载体赋予实数值的相容赋值，该赋值满足每个仿射复制/常数约束。

假设对于每个构件 $\mathcal{G}_t$，都存在局部因子

$$U^{(t)} \in \mathbb{R}^{m\times 3}, \qquad V^{(t)} \in \mathbb{R}^{3\times n}$$

使得：

1. $U^{(t)}[I_0, :] = I_3$ 和 $V^{(t)}[:, J_0] = B$，
2. $X^{(t)} := U^{(t)}V^{(t)}$ 满足 $\mathcal{G}_t$ 的所有仿射约束，
3. $X^{(t)}$ 匹配 $\mathcal{G}_t$ 所使用的指定载体值。

那么，存在全局因子 U, V（具有相同的规范规范），使得 $X := UV$ 能够同时满足所有构件约束，并匹配所有指定载体值。

证明。 根据定义 8.1–8.2，每个构件 $\mathcal{G}_t$ 都与一组行索引和一组列索引相接。定义

$$\mathcal{R}_t \;:=\; I_0 \;\cup\; \mathcal{I}(\mathcal{G}_t) \;\cup\; \{r \text{ of carriers in } \mathcal{G}_t\}, \tag{8.5}$$

and

$$\mathcal{C}_t \;:=\; J_0 \;\cup\; \mathcal{J}(\mathcal{G}_t) \;\cup\; \{c \text{ of carriers in } \mathcal{G}_t\}. \tag{8.6}$$

此外，该构造确保了不相交性：对于 $t \neq t'$ ，

$$(\mathcal{R}_t \setminus I_0) \cap (\mathcal{R}_{t'} \setminus I_0) = \emptyset, \tag{8.7}$$

and

$$(\mathcal{C}_t \setminus J_0) \cap (\mathcal{C}_{t'} \setminus J_0) = \emptyset. \tag{8.8}$$

如下定义全局 $U \in \mathbb{R}^{m\times 3}$ 与 $V \in \mathbb{R}^{3\times n}$ 。首先施加规范规范：

$$U[I_0, :] = I_3, \qquad V[:, J_0] = B. \tag{8.9}$$

接下来，对每个构件 t 以及每个 $i \in$ 实数域$_t \setminus I_0$，令

$$U[i, :] \;:=\; U^{(t)}[i, :]. \tag{8.10}$$

类似地，对每个构件 t 以及每个 $j \in \mathcal{C}_t \setminus J_0$，令

$$V[:, j] \;:=\; V^{(t)}[:, j]. \tag{8.11}$$

最后，将 U 所有剩余未定义的行以及 V 的列任意设定（例如0）。该构造是良定义的：由（8.7），每个 $i \notin I_0$ 至多属于一个集合实数域$_t$，并且由（8.8），每个 $j \notin J_0$ 至多属于一个集合$\mathcal{C}_t$。

现在定义全局矩阵

$$X \;:=\; UV. \tag{8.12}$$

固定任意构件$\mathcal{G}_t$。出现在$\mathcal{G}_t$ 中的每条仿射约束仅提及元素 X_{ij}，其中（i, j）$\in$ 实数域$_t \times \mathcal{C}_t$。对任意这样的（i, j），由（8.10）和（8.11），我们有

$$U[i, :] = U^{(t)}[i, :] \quad \text{and} \quad V[:, j] = V^{(t)}[:, j], \tag{8.13}$$

因此

$$X_{ij} \;=\; U[i, :]\, V[:, j] \;=\; U^{(t)}[i, :]\, V^{(t)}[:, j] \;=\; X^{(t)}_{ij}. \tag{8.14}$$

因此，$\mathcal{G}_t$ 的每个仿射约束都对 X 成立，因为根据假设 $X^{(t)}$，它对 $X^{(t)}$ 成立2。同样，$\mathcal{G}_t$ 所用的指定载体值相匹配，因为 X 和 $X^{(t)}$ 在实数域$_t \times \mathcal{C}_t$ 上逐项一致（8.14），依据假设3。

由于$\mathcal{G}_t$ 是任意的， X 同时满足所有构件约束，并匹配所有指定载体值。

□

8.3. 正向（可靠性）

定理 8.5 （可靠性）。 如果算术电路实例可满足，那么构造出的 *ARM*(3)实例就有一个可行解 X ，秩$(X) \leq 3$，且满足所有仿射约束。

证明。 固定每个电路导线出现项和门输出的一个满足赋值，得到实数值 $\{z_i\}$。对于归约中的每个出现载体 (r, c) ，将该出现项指定的值设为 $x := z$ 根据定义 8.2 以及电路赋值的一致性，所有用于等同各出现项的复制约束均得到满足。

现在考虑任意构件 $\mathcal{G}_t$。由于电路赋值满足门语义，提供给 $\mathcal{G}_t$ 的指定输入/输出值满足该构件预期的关系。因此，第 *6* 节中确立的相应构件完备性陈述给出了该构件在固定块下的一个秩为 3 的见证，即局部因子 $U^{(t)}$, $V_{(t)}$ 满足规范规范 **(8.2)** 以及具有这些指定值的所有构件约束。（对于线性构件，无需使用秩上界即可成立；对于非线性构件，则由第 5 节的行列式强制完备性结果保证。）

应用引理 8.4 于所有构件组成的族，可得到全局因子 U、V，因此 $X = UV$ 满足所有 仿射约束。最后，$\mathrm{rank}(X) \leq 3$成立，因为 X 表示为一个 $m \times 3$ 因子与一个 $3 \times n$ 因子的乘积。

□

8.4. 反向推导（完备性）

定理 8.6 （完备性）。 如果所构造的 *ARM*(3) 实例存在一个可行矩阵 X ，满足所有仿射约束，且 $\mathrm{rank}(X) \leq 3$，那么解码值

$$z := X_{r,c}$$

指定出现位置载体上的值构成算术电路实例的一个满足赋值（因此，在通过复制约束识别各次出现后，也会在原始电路变量上诱导出一个满足赋值）。

证明。 设 X 是可行的，且 秩$(X) \leq 3$。由于该实例包含固定块约束 **(8.1)**，引理 8.3 适用；特别地，我们可以在

规范规范 (8.2) 下工作，且所有指定载体值都是定义良好的标量 $x = X_{r,\ c}$。

任取一个构件 $\mathcal{G}_t$。由于完整实例可行，矩阵 X 满足 $\mathcal{G}_t$ 的所有仿射约束。此外，X 的任何子矩阵限制的秩至多为 $\operatorname{rank}(X) \le 3$。因此，相应构件的 可靠性陈述（在第 6 节利用第 5节的秩障碍证明）适用：在秩 ≤ 3 和固定块的条件下，满足该构件的仿射约束会迫使其指定载体值在 $\mathbb{R}$中满足预期的门关系。

因此，编译电路的每个门关系都在解码后的指定值上成立。由于复制／扇出约束明确地将相同的出现位置识别为相等，解码值便沿电路有向无环图一致地传播；通过拓扑归纳，整个算术电路均得到满足。因此，原实例可满足。 □

备注 8.7（秩究竟在哪里发挥作用）。 仿射布线（常数、复制和线性约束）由 ARM 实例的仿射等式直接实施。秩上界 $\operatorname{rank}(X) \le 3$ 仅通过构件可靠性引理（在第 6 节利用第 5节的秩障碍证明）来调用，也就是说，它仅用于实施基于行列式的构件所编码的非线性语义。

9. 成员资格$\in \exists\mathbb{R}$

定理 9.1 (成员资格**)**。$\mathrm{ARM}(3) \in \exists\mathbb{R}$。

范围说明。本节仅论述复杂性类成员资格论证（将其编码为实数域上的存在句）。从逻辑上讲，本节内容独立于前几节中证明的困难性归约。

9.1. 秩$(X) \le 3$的行列式编码

我们使用通过子式消失来刻画秩有界矩阵的经典刻画。

引理 9.2 （通过消失子式确定秩）。 设 $X \in \mathbb{R}^{m\times n}$ 且设 $k \ge 1$。则

$$\operatorname{rank}(X) \le k \iff \det\Big(X[I,J]\Big) = 0 \ \textit{ for all } I \subseteq [m],\ J \subseteq [n] \ \textit{ with } |I| = |J| = k{+}1.$$

证明。 ($\Rightarrow$) 若秩$(X) \le k$，则每个 $(k+1) \times (k+1)$ 子矩阵 $X[I,J]$的秩至多为 k，因此 $\det(X[I,J]) = 0$。

($\Leftarrow$) 假设所有 $(k+1)\times(k+1)$ 子式都为零。若 $\operatorname{rank}(X) \ge k+1$，则根据标准的秩–子式等价，存在下标集 I, J，使得 $|I| = |J| = k+1$满足 $X[I,J]$满秩 $k+1$，这迫使 $\det(X[I,J]) \neq 0$，矛盾。因此 $\operatorname{rank}(X) \le k$。关于行列式簇和秩–子式刻画的背景介绍，参见例如 [20, 21] 。 □

将引理 9.2 应用于 $k = 3$，得到多项式系统

$$\det\Big(X[I,J]\Big) = 0 \qquad \forall\, I \subseteq [m],\ J \subseteq [n] \ \text{ with } \ |I| = |J| = 4. \tag{9.1}$$

9.2. 将一个ARM(3)实例编码为一个实数存在理论实例

回顾一下，ARM(3)的一个实例由有理数数据 $A_1, \dots, A_q \in \mathbb{Q}^{m\times n}$ 和 $b_1, \dots, b_q \in \mathbb{Q}$指定，并询问是否存在 $X \in \mathbb{R}^{m\times n}$ 使得

$$\langle A_\ell, X\rangle = b_\ell \quad (\ell \in [q]), \qquad \text{and} \qquad \operatorname{rank}(X) \le 3, \tag{9.2}$$

其中弗罗贝尼乌斯内积定义为

$$\langle A, X\rangle \ := \ \sum_{i=1}^{m}\sum_{j=1}^{n} A_{ij}X_{ij}. \tag{9.3}$$

定理证明*9.1*。 我们构造一个关于实变量 $\{X_{ij}\}_{i\in[m],\ j\in[n]}$ 的存在句，其形式为仅等式ETR范式：

$$\exists\, X \in \mathbb{R}^{m\times n} : \ \Big(\bigwedge_{\ell=1}^{q} \big(\langle A_\ell, X\rangle - b_\ell = 0\big) \Big) \ \wedge \ \Big(\bigwedge_{\substack{I\subseteq[m],\, J\subseteq[n]\\ |I|=|J|=4}} \det\Big(X[I,J]\Big) = 0 \Big). \tag{9.4}$$

（i）作为实数存在理论等式的语法有效性。每个约束$\langle A_\ell,\ X\rangle - b_\ell = 0$都是变量 X_{ij} 上的仿射多项式等式，且具有有理系数。每个约束 $\det(X[I,J]) = 0$ 都是一个四次整系数多项式等式。此外，每个行列式都可以利用莱布尼茨公式显式地写成 $X[I,J]$ 各项的多项式

$$\det(Y) = \sum_{\pi\in S_4} \operatorname{sgn}(\pi) \prod_{t=1}^{4} Y_{t,\pi(t)}, \tag{9.5}$$

因此，(9.4) 中的每个合取项都是关于 $(\mathbb{R},\ +,\ \times)$的真正多项式等式。

由于实数存在理论编码模型使用整数系数多项式，我们消去仿射约束中的分母：对每个 $\ell \in [q]$，将等式 $\langle A_\ell, X\rangle - b_\ell = 0$ 乘以出现在 A_ℓ 的各项以及 b_ℓ 中的分母的最小公倍数，从而得到一个等价的整数系数线性多项式等式。该规范化使位大小至多增加输入长度的一个多项式因子（参见例如 [22, 23]）。

(ii) 正确性（等可满足性）。 若 X 满足（9.2），则它满足（9.4）中的所有仿射等式，并且由引理 9.2 结合 $k = 3$ 可知它满足所有 4×4子式等式（9.1）。反之，若 X 满足（9.4），则所有仿射等式成立且所有 4×4 子式为零，因此引理 9.2 蕴含 秩$(X) \le 3$；故（9.2）成立。

(iii) 多项式时间构造与规模界。 实变量的数量为 mn。仿射等式的数量为 q。行列式等式的数量为

$$\binom{m}{4}\binom{n}{4} = O(m^4 n^4). \tag{9.6}$$

每个行列式等式展开后（通过（9.5））是由常数个 $4! = 24$ 个四次单项式组成的和4。因此，（9.4）中的无量词合取式的总编码长度关于输入规模呈多项式级（特别地，关于指定 A_ℓ 、 b_ℓ以及 m、 n、 q的有理数输入的位长呈多项式级）。因此，从（9.2）到（9.4）的映射可在多项式时间内计算，由此得到 $\mathrm{ARM}(3) \in \exists\mathbb{R}$。 □

注 9.3（与因子分解见证的关系）。 定理9.1 通过存在性分解见证证明了 $\mathrm{ARM}(k) \in \exists\mathbb{R}$ 对每个固定的 k 都成立$X = UV$。我们在此列出该定理，一方面是为了使用本文的记号，将成员资格方向完全明确地表述出来；另一方面是为了使其与整个归约（第 4–7 节）所采用的秩障碍视角保持一致。特别是对于 $k = 3$，记录尤其简单的行列式表述（9.1）很方便。

10. 结论

我们对固定常数秩上界下的仿射秩最小化 建立了精确的实代数复杂性分类。对于每个固定的 $k \ge 1$，ARM$(k) \in \exists\mathbb{R}$，其依据是对 rank$(X) \le k$ 的显式存在性编码。我们的主要

结果表明，这一上界在秩为 3 时已经是紧的：我们给出了从实数存在理论到 ARM(3) 的多项式时间多对一归约，且输出实例仅包含施加于单个矩阵变量 X 各元素上的有理仿射等式 ≤ 3，以及唯一的全局约束 $\mathrm{rank}(X) \leq 3$。

该归约将所有非线性都限制在秩上界中。线性电路语义（常数、复制/扇出、加法、取负）直接通过仿射约束强制实现，而乘法则通过一个常数规模的行列式强制原语来实现：结合一个固定的满秩 3×3 规范块，一个 2×2 构件会产生一个 4×4 子式，其行列式是 $(c - ab)$的非零常数倍，因此任何违反 $c = ab$ 的情况都会强制$\mathrm{秩}(X) \geq 4$。固定的规范块也消除了 GL(3) 歧义，并使全局组合论证成为可能，从而确保所有常数规模构件都嵌入同一个全局分解 $X = UV$，且不会产生意外耦合。这证明了该编码的可靠性和完备性，并保持了实例规模和比特复杂度的多项式界。

因此，ARM(3) 是 $\exists\mathbb{R}$-完全的。特别是，在秩$(X) \leq 3$ 的条件下判定纯仿射约束的可行性，其难度不低于实代数可行性；因此（除非发生通常所说的复杂性塌缩），尽管唯一的非线性来自秩约束，但仍不存在通用的多项式时间算法。

参考文献

[1] E. J. Candès, B. Recht，通过凸优化实现精确矩阵补全，《计算数学基础》9 (6) (2009) 717–772。[2] B. Recht，一种更简单的矩阵补全方法，《机器学习研究杂志》12 (2011) 3413–3430。[3] E. J. Candès, T. Tao，凸松弛的威力：近乎最优的矩阵补全，《IEEE 信息论汇刊》56 (5) (2010) 2053–2080。[4] B. Recht, M. Fazel, P. A. Parrilo，通过核范数最小化保证获得线性矩阵方程的最小秩解，《SIAM 评论》52 (3) (2010) 471–501。[5] M. Bachmayr, M. Faldum，一种用于高维抛物型偏微分方程的时空自适应低秩方法，《复杂性杂志》82 (2024) 101839。

[6] M. Fazel，具有应用的矩阵秩最小化，博士论文，斯坦福大学 (2002)。[7] M. Fazel, H. Hindi, S. P. Boyd，系统理论中的秩最小化及其应用，载于：美国控制会议 (ACC) 论文集，2004，第 3273–3278 页。[8] I. Markovsky，《低秩近似：算法、实现与应用》，施普林格，2012。[9] J. F. Canny，关于多项式空间中的某些代数与几何计算，载于：第 20 届 ACM计算理论研讨会 (STOC) 论文集，ACM，1988，第 460–467 页。[10] L. Blum, F. Cucker, M. Shub, S. Smale，《复杂性与实数域上的计算》，施普林格，1998。[11] F. Cucker， $p \neq nc$ 实数域上的，《复杂性杂志》8 (2) (1992) 230–238。[12] P. B"urgisser，代数复杂性理论中的时间—空间权衡，《复杂性杂志》16 (1) (2000) 2–49。[13] J. M. Landsberg，《张量：几何与应用》，美国数学学会，2012。[14] S. A. Vavasis，《非线性优化：复杂性问题》，计算机科学国际专著系列第 8 卷，牛津大学出版社，1991。[15] M. Schaefer，若干几何与拓扑问题的复杂度，《计算机与系统科学杂志》75 (2) (2009) 98–130。[16] S. Basu, R. Pollack, M.-F. Roy，《实代数几何中的算法》，《数学中的算法与计算》第 10 卷，施普林格，2006。[17] L. Blum, M. Shub, S. Smale，关于实数域上的计算与复杂性理论：NP完全性、递归函数与通用机器，《美国数学学会通报》21 (1) (1989) 1–46。

[18] N. E. Mnëv，《构形簇和凸多胞形簇分类问题的普遍性定理》，载于：O. Y. Viro（编），《拓扑与几何——罗赫林研讨班》，数学讲义第 1346 卷，施普林格，1988 年，第 527–544 页。[19] J. Richter-Gebert，《多胞形的实现空间》，数学讲义第 1643 卷，施普林格，1996 年。[20] W. Bruns、U. Vetter，《行列式环》，数学讲义第 1327 卷，施普林格，1988 年。[21] J. Harris，《代数几何：初级教程》，数学研究生教材第 133 卷，施普林格，1992 年。[22] J. Bochnak、M. Coste、M.-F. Roy，《实代数几何》，数学及其边缘领域成果第 36 卷，施普林格，1998 年。[23] J. Renegar，《关于实数一阶理论的计算复杂度与几何。I. 引言。预备知识。半代数集的几何。实数存在理论的判定问题》，《符号计算杂志》13（3）（1992）：255–299。