arXiv:2601.02518v1 [math.SP] 5 Jan 2026

# 扩散计算与量子计算：用于阶寻找和因数分解的比较模型

CarlosA. Cadavid
Paulina Hoyos Jay
Jorgenson Lejla
Smajlović J. D.
Vélez

2026年1月7日

**摘要**

我们研究一种用于整数因数分解的混合计算模型：在标准数字算术的基础上，增加对有限图上迭代扩散过程 的访问能力。一次扩散步 包括：对一个经 $\ell^1$ 归一化的状态向量应用固定的局部平均算子（半惰性随机游走矩阵），并按照规定读出少量坐标。我们的目标并非在通常的电路模型内改进 Shor 算法，而是理解这样一种情形下能够实现什么：将扩散视为真正的硬件原语，其实际更新时间成本不随底层状态空间的大小而增加。

设 $N \geq 3$ 为一个具有 $m \geq 2$ 个不同素因子的奇合数，并设 $b \in (\mathbb{Z}/N\mathbb{Z})^*$ 的乘法阶为 $r = \mathrm{ord}_N(b)$。我们为循环子群 $\langle b \rangle$ 关联一个使用二进制幂生成元 $b^{\pm 2^t}$、其中 $0 \leq t \leq M = \lfloor \log_2 N \rfloor + 1$ 的加权凯莱图，并分析相应的半惰性游走算子 $W$。利用显式的特征展开以及关于模 $r$ 的疏分序列 $2^t$ 的倍增引理，我们证明，经过 $n = O\big((\log_2 N)^2\big)$ 次扩散步后，单位元处的单个热核值满足

$$\left| p_n(e) - \frac{1}{r} \right| \leq \frac{1}{4N^2},$$

因此，通过对 $1/p_n(e)$ 进行舍入，可以唯一地恢复 $r$。将这一扩散阶寻找原语与从因数分解到阶寻找的经典归约相结合，可得出一种扩散辅助因数分解程序，其成功概率为 $p(m) = 1 - (m+1)/2^m$，仅取决于不同素因子的个数 $m$ $N$。

与此同时，我们还开发了一种互补的关系寻找机制：探索凯莱图时遇到的二进制词之间的碰撞会产生环关系 $D = qr$，反复进行最大公因数更新通常会稳定在 $r$ （或其较小倍数）。我们给出了数值示例和实现，其中包括基于环的因数分解案例：费马数 $F_5 = 2^{32} + 1$、$N = 8,219,999$（用于与近期量子退火实验进行比较），以及 $N = 1,099,551,473,989$（用于与当前量子计算记录进行比较）。

## 1 引言

### 1.1 动机与范围

对合数进行因数分解 $N$ 是计算数论和密码学中的一个基石问题，与$(\mathbb{Z}/N\mathbb{Z})^*$的结构密切相关；例如参见 [HW08、CP05、Me96、BS96]。

经典方法非常复杂，通常需要亚指数时间，但在$\log_2 N$ 中，标准数字模型 [CP05]下尚无已知的多项式时间算法。
Shor 算法表明，在量子电路模型中，因数分解可归约为阶寻找，而阶寻找可通过量子周期查找／傅里叶采样在多项式时间内求解[Sh94、Sh97、NC10、EJ96]。有关近期进展和推广，参见 [CBK22、Hh25、Ra24、Re25、XQLM23]及其中的参考文献。概括而言：将模幂运算编码为相干线性演化，通过干涉提取周期性，并以经典后处理（连分数和验证）完成计算 [Sh94、Sh97、KSV99、NC10]。

本文研究一种不同的计算原语：将有限图上的扩散作为阶寻找的模拟机制。具体而言，我们分析定义在与 $(\mathbb{Z}/N\mathbb{Z})^*$ 的循环子群关联的加权凯莱图上的迭代半惰性随机游走（离散时间热流）。我们的目标并非在通常的数字／RAM 模型或量子电路模型中改进 Shor 算法。相反，我们提出一种混合模型，在该模型中，标准数字算术由可迭代和查询的扩散过程加以增强。按此计算方式，在明确的接口假设下，阶恢复只需 $\mathrm{poly}(\log_2 N)$ 数字运算，以及 $O((\log_2 N)^2)$ 次扩散迭代。

## 1.2 量子层与扩散迭代

为清晰地核算资源，我们将两种非数字范式都示意为线性算子的交替应用，并在其后进行：(i) 量子情形下的观测/投影；(ii) 扩散情形下的经典读出，随后进行条件化（后处理）：

$$\begin{aligned}\text{quantum:}\quad &\cdots \xrightarrow{U} \xrightarrow{\text{measure/proj}} \xrightarrow{U} \xrightarrow{\text{measure/proj}} \cdots,\\ \text{diffusion:}\quad &\cdots \xrightarrow{W} \xrightarrow{\text{read/cond}} \xrightarrow{W} \xrightarrow{\text{read/cond}} \cdots.\end{aligned}$$

这仅是记账： $U$ 是酉算子（能够产生干涉），而 $W$ 是马尔可夫的、耗散的 [NC10，LPW09]。这样做是为了明确混合模型中假定工作发生的位置：定理将扩散原语的调用次数界定为 $O((\log_2 N)^2)$，其余处理则采用标准数字算术。

## 1.3 物理扩散原语、资源扩展与局部性

我们的复杂度界分别追踪两种资源：数字步骤和扩散步数。

**数字步骤**。对 $O(\log_2 N)$ 位整数执行确定性运算（模运算、最大公约数、验证、记账），这些运算的复杂度均为 $\log_2 N$ 阶，符合标准算术/RAM意义[Kn97，BS96]。

**扩散步数**。 对固定的局部平均算子（即图 $X$上的半惰性游走算子 $W$）应用一次，并按照预先规定的方式读出 $\ell^1$归一化态向量中少数几个“温度”坐标。

扩散步的预期解释是基于硬件的。事实上，只有将扩散视为真正的硬件原语时，才会产生加速：单次硬件级更新 可在每个顶点同时执行局部平均，其实际耗时（即用时钟测量的真实经过时间）不会随顶点数量增加而增长，而且所需的读出精度可通过 $\mathrm{poly}(\log_2 N)$ 开销实现。在此模型中，一次扩散步的实际耗时被视为与所表示的顶点数量无关，因为所有顶点都会并行更新。如果通过显式更新一个

长度为-$r$的状态向量（其中 $r = \mathrm{ord}_N(b)$ 可能高达 $\varphi(N)$，即欧拉函数）来进行数字模拟扩散，那么这种优势便会消失，该过程相对于 $\log_2 N$ 将变为指数级。
这一假设将成本从时间转移到了物理资源上。任何字面意义上的扩散器都必须表示一个定义在大小为 $\Omega(|X|)$ 的顶点集上的状态，因此设备面积/能耗至少随 $|X|$ 线性增长。因此，我们的结果是概念性的、基于模型的：它们表明，给定这样一种具有足够读出精度的扩散原语，在经过 $O((\log_2 N)^2)$ 次扩散迭代后，仅凭一个热核值即可确定阶 $r$ 。

另一个运作层面的要点是局部性。尽管底层凯莱图具有 $r$ 个顶点，但其动力学由一个简短的生成集规定，并且是局部的；因此，实现无需预先构造完整的图。相反，扩散机制可以通过反复进行局部平均来演化状态，并且（从概念上说）只“扩展”在规定的迭代次数内实际到达的那部分图，这与凯莱图的标准随机游走视角相一致 [LPW09、第97]。

## 1.4 主要结果

固定一个奇合数

$$N = \prod_{i=1}^{m} p_i^{e_i} \qquad (m \geq 2,\ p_i \text{ distinct odd primes}). \tag{1.1}$$

令 $b \in (\mathbb{Z}/N\mathbb{Z})^*$ 的奇数 阶为 $r = \mathrm{ord}_N(b)$。在事先不知道 $r$ 的情况下，我们考虑由 $b^{\pm 2^t}$（对应于 $0 \leq t \leq M = \lfloor \log_2 N \rfloor + 1$）这些移动生成的 $\langle b \rangle$ 上的加权凯莱图。我们分析相应的半惰性游走算子 $W$ 及其离散时间热核。我们证明，对于

$$n_0 = 4(M+1)(\log_2 N + 2) = O((\log_2 N)^2),$$

单个 单位元处的热核值 $p_{n_0}(e)$，可通过对 $1/p_{n_0}(e$ 舍入而唯一确定 $r$ ).
存在确定性算法可以判定 $N$ 是素数还是素数幂；例如，参见 [AKS04], [Be07], 或 [Ra80]。对于这两个问题，即判定 $N$ 是素数还是素数幂，目前已知的最佳算法具有（经典）复杂度，阶为 $O((\log N)^a)$，其中 $a$为某个常数。因此，至少从理论可计算性的角度来看，我们不认为假设 $N$ 既不是素数也不是素数幂具有任何限制性。

## 1.5 结构安排

本文结构如下。第2 节构建加权图和凯莱图上的扩散／热核框架。第3 节汇集了将因数分解约化为阶寻找时所用的数论预备知识。第4 节证明主要的扩散阶寻找定理。第5 节给出扩散辅助因数分解算法的伪代码，以及扩散原语的数值模拟代码（例如使用 Python）。第6 节介绍一种加速的、基于碰撞的关系寻找机制，该机制通过检测闭合环，并利用所得环长的最大公因数稳定化来实现。第7 节分析在 $G$上的游走的碰撞统计，包括尺度估计。最后，第8节给出说明性数值示例。

# 2 扩散预备知识

## 2.1 加权图

全文中，图均为有限、无向、连通且不含自环。加权图$X = (V, E, w)$由有限顶点集 $V$、由 $V$ 的二元子集构成的边集 $E$，以及权重函数 $w\colon V \times V \to \mathbb{R}$ 组成，并满足以下性质。

- **对称性：** $w(x, y) = w(y, x)$ 对所有 $x, y \in V$。
- **非负性：** $w(x, y) \geq 0$ 对所有 $x, y \in V$。
- **边上的支撑：** $w(x, y) > 0$ 当且仅当$\{x, y\} \in E$。

固定 $V$ 的一个排序，其中包含 $|V| = k$。邻接算子 $A_X$ 是定义在 $V$ 上函数空间 $f$ 上的算子，满足 $(A_X f)(x) = \sum_{y \in V} w(x, y) f(y)$。
顶点 $x \in V$的度为

$$d(x) = \sum_{y \in V} w(x, y).$$

我们称 $X$ 为度 $d$ 正则，如果对于所有 $x \in V$，都有 $d(x) = d$。

## 2.2 半惰性游走与离散时间热核

假设 $X$ 是 $d$-正则的。半惰性游走矩阵 为

$$W = \frac{1}{2}\left(I + \frac{1}{d}A_X\right). \tag{2.1}$$

从初始概率分布 $p_0 \in \mathbb{R}^k$ $(p_0 \geq 0, \|p_0\|_1 = 1)$ 出发，定义 e

$$p_n = W^n p_0.$$

将 $w_n(x, y)$ 记为 $W^n$ 的 $(x, y)$ 项。这表示从 $y$ 出发的游走经过 $n$ 步后位于 $x$ 的概率。我们将 $p_n$ 称为离散时间热核。
也就是说，离散时间导数 $\partial_n p_n = p_{n+1} - p_n$ 和离散（概率）拉普拉斯算子$\Delta = W - I$ 满足

$$\partial_n p_n = \Delta p_n, \tag{2.2}$$

定义在 $X$上的离散热方程。正则图 $p_n$ 上的离散时间热核的显式表达式见 [CHJSV23]。

## 2.3 谱展开与一致界

由于该图是 $d$-正则图，随机游走矩阵是 $P = \frac{1}{d}A_X$。于是， $P$是实对称矩阵，且

$$\operatorname{spec}(P) \subset [-1, 1] \qquad (\text{see e.g. [Ni18, Thm. 7.5]}).$$

回顾 $W = \frac{1}{2}(I + P)$。若 $\theta \in \operatorname{spec}(P)$，则 $\frac{1}{2}(1 + \theta) \in \operatorname{spec}(W)$。因此

$$\operatorname{spec}(W) = \left\{\tfrac{1}{2}(1 + \theta) : \theta \in \operatorname{spec}(P)\right\} \subset [0, 1].$$

特别地， $W$ 是对称的，且其所有特征值均为实数且非负。令

$$1 = \lambda_0 > \lambda_1 \geq \cdots \geq \lambda_{k-1} \geq 0 \tag{2.3}$$

为 $W$的特征值，其正交归一特征基$\{\psi_0$、 $\psi_1$、.....、 $\psi_{k-1}\}$ 满足 $W\psi_j$ =$\lambda_j\psi_j$。

此外， $P\mathbf{1} = \mathbf{1}$（因此 $W\mathbf{1} = \mathbf{1}$），所以我们可以取 $\psi_0 = \frac{1}{\sqrt{k}}\mathbf{1}$.因此，对于任意初始分布 $p_0$，我们有谱展开

$$p_n = W^n p_0 = \sum_{j=0}^{k-1} \langle \psi_j, p_0 \rangle \, \lambda_j^n \, \psi_j,$$

其中 $\langle \psi, \phi \rangle$ 表示向量 $\psi, \phi \in \mathbb{R}^k$ 的通常内积。

**命题 2.1**。 设 $\lambda_1$ 是 $W$ 中严格小于 1 的最大特征值。若 $p_0$ 是一个概率分布，则对于每个顶点 $x \in V$ 以及任意 $n \geq 0$,

$$\left| p_n(x) - \frac{1}{k} \right| \leq \lambda_1^n.$$

证明。 设 $\psi_0 = \frac{1}{\sqrt{k}}\mathbf{1}$，并将该向量扩展为 $W$ 的正交归一特征基 $\{\psi_0, \psi_1, \ldots, \psi_{k-1}\}$：$W\psi_j = \lambda_j\psi_j$, 其中 $1 = \lambda_0 > \lambda_1 \geq \lambda_2 \geq \cdots$。 由于 $p_0$ 是一个概率分布,

$$\langle \psi_0, p_0 \rangle = \frac{1}{\sqrt{k}} \sum_{x \in V} p_0(x) = \frac{1}{\sqrt{k}}.$$

因此

$$p_n = W^n p_0 = \sum_{j=0}^{k-1} \langle \psi_j, p_0 \rangle \, \lambda_j^n \, \psi_j = \frac{1}{k}\mathbf{1} + \sum_{j=1}^{k-1} \langle \psi_j, p_0 \rangle \, \lambda_j^n \, \psi_j.$$

设 $u_n = \sum_{j=1}^{k-1} \langle \psi_j, p_0 \rangle \, \lambda_j^n \, \psi_j$, 于是 $p_n = \frac{1}{k}\mathbf{1} + u_n$，且 $u_n$ 与 $\mathbf{1}$ 正交。

固定 $x \in V$并设 $a_j = \langle \psi_j, p_0 \rangle$ 以及 $b_j = \lambda_j^n \psi_j(x)$ 对于 $1 \leq j \leq k-1$。 则 $u_n(x) = \sum_{j=1}^{k-1} a_j b_j$, 根据柯西–施瓦茨不等式,

$$|u_n(x)| \leq \Big( \sum_{j=1}^{k-1} |a_j|^2 \Big)^{1/2} \Big( \sum_{j=1}^{k-1} |b_j|^2 \Big)^{1/2} = \Big( \sum_{j=1}^{k-1} |\langle \psi_j, p_0 \rangle|^2 \Big)^{1/2} \Big( \sum_{j=1}^{k-1} \lambda_j^{2n} \psi_j(x)^2 \Big)^{1/2}.$$

根据帕塞瓦尔恒等式,

$$\|p_0\|_2^2 = \sum_{j=0}^{k-1} |\langle \psi_j, p_0 \rangle|^2, \qquad \text{hence} \qquad \sum_{j=1}^{k-1} |\langle \psi_j, p_0 \rangle|^2 \leq \|p_0\|_2^2.$$

由于对于 $j \geq 1$, $\lambda_j \in [0, \lambda_1]$ ,

$$\sum_{j=1}^{k-1} \lambda_j^{2n} \psi_j(x)^2 \leq \lambda_1^{2n} \sum_{j=1}^{k-1} \psi_j(x)^2 \leq \lambda_1^{2n} \sum_{j=0}^{k-1} \psi_j(x)^2.$$

最后，利用 $\langle \psi_j, \delta_x \rangle = \psi_j(x)$ 以及关于 $\delta_x$ 的帕塞瓦尔恒等式，我们得到

$$\sum_{j=0}^{k-1} \psi_j(x)^2 = \sum_{j=0}^{k-1} |\langle \psi_j, \delta_x \rangle|^2 = \|\delta_x\|_2^2 = 1.$$

结合这些界可得 $|u_n(x)| \leq \lambda_1^n \|p_0\|_2$。 由于 $p_0 \geq 0$ 和 $\|p_0\|_1 = 1$，我们有$\|p_0\|_2 \leq \|p_0\|_1 = 1$, 因此 $|p_n(x) - \frac{1}{k}| = |u_n(x)| \leq \lambda_1^n$。 □

### 2.4 有限阿贝尔群的加权凯莱图

设 $G$ 是一个采用加法记号的有限阿贝尔群，$S \subseteq G$ 是一个对称生成集（因此$s \in S \Rightarrow -s \in S$），并且 $\alpha\colon S \to \mathbb{R}_{>0}$，其中 $\alpha(s) = \alpha(-s)$。加权凯莱图$X = \mathsf{Cay}(G, S, \alpha)$ 的顶点集为 $G$，边权重为

$$w(x,y) = \alpha(x-y) \quad \text{if } x-y \in S, \qquad w(x,y) = 0 \text{ otherwise.}$$

它是度为

$$d = \sum_{s \in S} \alpha(s).$$

特征标可将邻接算子对角化 $A_X$；背景介绍见 [CR62]，以及 [Ba79，推论 3。2] 凯莱图的谱公式见此处。若 $\chi$ 是 $G$的一个特征标，则它是 $A_X$ 的特征向量，其特征值为

$$\eta(\chi) = \sum_{s \in S} \alpha(s)\chi(s),$$

因此是 $W$ 的特征向量，特征值为 $\lambda(\chi) = \frac{1}{2}\,(1 + \eta(\chi)/d)$。

## 3 数论预备知识

本节介绍因数分解归约中用到的初等数论知识。以下所有结论都是标准结果；我们按照后文所需的形式和一般性，给出简短证明。一般参考资料包括 [HW08，第 1–3], [CP05，第 2–4], 以及 [BS96，第 2–4]；另见[Me96，§2–5] 关于从阶查找归约到因数分解的标准密码学表述。

设 $N$ 为一个正奇整数，将其写成乘积

$$N = \prod_{i=1}^{m} p_i^{e_i}, \tag{3.1}$$

其中 $m \geq 2$，素数 $p_1$、……、$p_m$ 互不相同且均为奇数，指数满足 $e_i > 0$。特别地，$N$ 既不是素数，也不是素数幂。

令 $\mathbb{Z}_N = \mathbb{Z}/N\mathbb{Z}$表示模 $N$的剩余环，令 $\mathbb{Z}_N^*$表示其单位群。存在一个自然映射

$$\mathbb{Z}_N \longrightarrow \mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_m^{e_m}}, \qquad a \longmapsto (a \bmod p_1^{e_1}, \ldots, a \bmod p_m^{e_m}). \tag{3.2}$$

根据中国剩余定理（中国剩余定理），(3.2)是环同构。将其限制到单位群，可得群同构

$$g_N : \mathbb{Z}_N^* \xrightarrow{\sim} \mathbb{Z}_{p_1^{e_1}}^* \times \cdots \times \mathbb{Z}_{p_m^{e_m}}^*. \tag{3.3}$$

略微滥用记号时，我们有时用 $x$ 表示 $\mathbb{Z}_N^*$ 的一个元素，或其像 $g_N(x)$。

For 对于每个 $i$，群 $\mathbb{Z}_{p_i^{e_i}}^*$在乘法下是循环群。固定一个生成元 $u_i$。其阶为 i s

$$\operatorname{ord}_{p_i^{e_i}}(u_i) = \varphi(p_i^{e_i}) = p_i^{e_i-1}(p_i - 1) = 2^{c_i} p_i',$$

其中 $c_i > 0$ 和 $p_i'$ 均为奇数。

不失一般性，我们假设素数按如下顺序排列：

$$c_1 \geq c_2 \geq \cdots \geq c_m. \tag{3.4}$$

下面的命题表明，假设中国剩余定理分解中的指数满足奇偶性条件，就可以生成模 $N$. 下非平凡的 1 的平方根

**命题 3.1**。 设 $a \in \mathbb{Z}_N^*$。设 $s \geq 0$ 为满足以下条件的最小整数

$$a^{2^s q} \equiv 1 \pmod{N}$$

对于某个奇整数 $q$。设

$$g_N(a) = (u_1^{d_1}, \ldots, u_m^{d_m}).$$

如果 存在指标 $i < j$，使得 $d_i$ 为奇数且 $d_j$ 为偶数，那么 $s > 0$。此外，令 $g$

$$x = a^{2^{s-1} q},$$

可得

$$x^2 \equiv 1 \pmod{N} \qquad and \qquad x \not\equiv \pm 1 \pmod{N}. \tag{3.5}$$

证明。 假设 $d_i$ 为奇数且 $d_j$ 为偶数。设 $d_j = 2^v d_j'$，其中 $v > 0$ 和 $d_j'$ 均为奇数。
由于 $a^{2^s q} \equiv 1$（模 $N$），可得

$$u_i^{2^s q d_i} \equiv 1 \pmod{p_i^{e_i}}.$$

因此，阶 $\mathrm{ord}^{p_i^{e_i}}(u_i) := 2^{c_i} p_i'$ 整除 $2^s q d_i$。由于 $q$ 和 $d_i$ 都是奇数，2-部分迫使 $2^{c_i} \mid 2^s$，于是 $s \geq c_i \geq 1$。
Set

$$x = a^{2^{s-1} q} = (u_1^{2^{s-1} q d_1}, \ldots, u_m^{2^{s-1} q d_m}).$$

Then

$$x^2 = a^{2^s q} \equiv 1 \pmod{N}.$$

由 $s$ 的最小性可知， $x \not\equiv 1$（模 $N$）。
剩下要证明 $x \not\equiv -1$（模 $N$）。现在

$$x \equiv u_j^{2^{s-1} q d_j} = u_j^{2^{s-1} q \cdot 2^v d_j'} = u_j^{2^{s+v-1} q d_j'} \pmod{p_j^{e_j}}.$$

我们断言 $x$ 模 $p_j^{e_j}$ 同余于 1。事实上，由于 $a^{2^s q} \equiv 1$（模 $p_j^{e_j}$），我们有

$$u_j^{2^s q d_j} = u_j^{2^{s+v} q d_j'} \equiv 1 \pmod{p_j^{e_j}}.$$

因此，阶 $2^{c_j} p_j'$ 整除 $2^{s+v} q d_j'$。由于 $q d_j'$ 是奇数，这意味着

$$s + v \geq c_j \quad \text{and} \quad p_j' \mid q d_j'.$$

由于 $s \geq c_i \geq c_j$（根据（3.4））且 $v > 0$，我们有 $s + v - 1 \geq c_j$，因此 $2^{c_j} p_j'$ 整除 $2^{s+v-1} q d_j'$，这恰好是

$$u_j^{2^{s+v-1} q d_j'} \equiv 1 \pmod{p_j^{e_j}}.$$

因此， $x \equiv 1$（模 $p_j^{e_j}$）。
但这意味着 $x \not\equiv -1$ (模 $N$)，否则 $x \equiv -1$ (模 $p_j^{e_j}$) 也成立。将这两个同余式相减，会得到 $2 \equiv 0$ (模 $p_j^{e_j}$)，这与 $p_j$ 为奇数矛盾。

□

**引理 3.2**。 设 $N$如 (3.1)所示，并设 $M = \lfloor 对数_2\, N \rfloor + 1$。对于任意 $a \in \mathbb{Z}_N^*$，定义元素列表

$$S(a) = \{\, a^{2^t} \bmod N :\ t = 0, \ldots, M \,\} \cup \{\, a^{-2^t} \bmod N :\ t = 0, \ldots, M \,\} \subset \mathbb{Z}_N^*.$$

如果 $S$（$a$）中出现重复，那么（根据该重复）可以在至多 $O$（$\log_2 N$）个确定性步骤内求出一个奇整数 $q$以及满足 $a^{2^s q} \equiv 1$ （mod $N$）的最小 $s \geq 0$。
此外，如果从 $\mathbb{Z}_N^*$ 中均匀随机选取 $a$，那么其概率为

$$p(m) = 1 - \frac{m+1}{2^m},$$

元素 $x = a^{2^{s-1}q}$ （当 $s > 0$时）满足 （3.5）。

证明。 $S(a)$ 中出现重复意味着，对于某个 $0 \leq t' < t \leq M$ 以及某种符号选择，

$$a^{2^t} \equiv a^{\pm 2^{t'}} \pmod{N},$$

因此

$$a^{2^t \pm 2^{t'}} \equiv 1 \pmod{N}.$$

将指数分解为

$$2^t \pm 2^{t'} = 2^{t'}(2^{t-t'} \pm 1) = 2^{t'} q,$$

其中 $q = 2^{t-t'} \pm 1$ 为奇数。由 $q$ 可以通过反复除以 2（如果可以），确定满足 $a^{2^s q} \equiv 1$ (mod $N$) 的最小 $s$，这需要进行 $O(\log_2 N)$ 次检查。
对于概率界，写作 $g_N(a) = (u_1^{d_1}, \ldots\ldots, u_m^{d_m})$。对于每个 $i$，指数 $d_i$ 模 2 均匀分布（一半为偶数，一半为奇数）；中国剩余定理使奇偶向量 $(d_1 \bmod 2, \ldots\ldots, d_m \bmod 2)$ 在 $\{0, 1\}^m$ 上均匀分布。

根据命题 3.1，若存在 $i < j$ 使得 $d_i$ 为奇数且 $d_j$ 为偶数，则成功。失败意味着不存在 这样的数对，即不存在指标 $i < j$ 使得 $d_i$ 为奇数且 $d_j$ 为偶数。等价地，奇偶向量

$$(d_1 \bmod 2, \ldots, d_m \bmod 2) \in \{0, 1\}^m$$

是非递减的 （一旦出现 1，后续所有项都是 1）。因此，它必定具有以下形式

$$(\underbrace{0, \ldots, 0}_{t \text{ zeros}}, \underbrace{1, \ldots, 1}_{m-t \text{ ones}}) \qquad \text{for some } t \in \{0, 1, \ldots, m\},$$

恰好给出 $m+1$ 种可能性。每种可能性的概率为 $2^{-m}$，因此失败概率为 $(m+1)/2^m$，成功概率为 $1 - (m+1)/2^m$。 □

注 3.3。由于 $N$ 既不是素数，也不是素数幂，因此有 $m \geq 2$。于是 $p(2) = 1 - \frac{3}{4} = \frac{1}{4}$，并且函数 $p(m) = 1 - \frac{m+1}{2^m}$ 对于 $m \geq 2$ 严格递增，且 $p(m) \to 1$ 随着 $m \to \infty$。特别地，即使事先不知道 $m$，随机选择一次 $a \in \mathbb{Z}_N^*$，也会以至少 $p(2) = \frac{1}{4}$ 的概率，得到一个$x = a^{2^{s-1}q}$ （当 $s > 0$ 时）满足所需性质 (3.5) 的元素。等价地，失败概率满足

$$\Pr[\text{failure in one trial}] = 1 - p(m) = \frac{m+1}{2^m} \leq \frac{3}{4}.$$

如果我们独立地重复该构造 $k$ 次（每次都重新随机选择 $a$），那么所有得到的值 $x$ 都不满足这两个条件的概率为

$$(1 - p(m))^k \leq \left(\frac{3}{4}\right)^k.$$

对于高度合成的 $N$（较大的 $m$），量 $1 - p(m) = (m+1)2^{-m}$ 远小于$3/4$，因此失败概率的衰减速度明显快于 $(3/4)^k$。

**引理 3.4**。 设 $G$ 为一个阶为偶数 $n = 2^c m$ 的有限循环群，其中 $c > 0$ 和 $m$ 为奇数，并设 $u$ 为一个生成元。则对于 $1 \le d \le n$ ，有

$$\mathrm{ord}_G(u^d) = \frac{n}{\gcd(n, d)}.$$

证明。 这是显然的，因为 $u^d$ 生成了指数为最大公约数$(n, d)$ 的子群。 □

**引理 3.5**。 对于任意 $a \in \mathbb{Z}_N^*$，整除 2 的最高次幂若整除 $\mathrm{ord}_N(a)$ ，则该幂严格小于$\log_2 N$。特别地，若 $M = \lfloor \log_2 N \rfloor + 1$ 且 $b = a^{2^M}$，则$\mathrm{ord}_N(b)$ 为奇数。

证明。 写作 $g_N(a) = (a_1, \ldots, a_m)$，其中 $a_i \in \mathbb{Z}^*_{p_i^{e_i}}$ 于是

$$\mathrm{ord}_N(a) = \mathrm{lcm}\big(\mathrm{ord}_{p_1^{e_1}}(a_1), \ldots, \mathrm{ord}_{p_m^{e_m}}(a_m)\big).$$

每个 $\mathrm{ord}_{p_i^{e_i}}(a_i)$ 都整除 $\varphi(p_i^{e_i}) = 2^{c_i} p_i'$，因此 $\mathrm{ord}_N(a)$ 的 2进赋值至多为 $\max_i c_i$。最后，$2^{c_i} \mid \varphi(p_i^{e_i}) < p_i^{e_i} \le N$，所以对所有 $i$，$c_i < \log_2 N$，从而 $\max_i c_i < \log_2 N$。取$M = \lfloor \log_2 N \rfloor + 1$后，$2^M$可被 $\mathrm{ord}_N(a)$ 的整个 2-部分整除，因此 $b = a^{2^M}$的阶为奇数。

□

**命题 3.6**。 集合 $M = \lfloor \log_2 N \rfloor + 1$。对于任意 $a \in \mathbb{Z}_N^*$，令 $b = a^{2^M}$并记作

$$r_b = \mathrm{ord}_N(b),$$

根据引理 *3.5*，该数为奇数。若已知 $r_b$，则 $\mathrm{ord}_N(a)$ 至多可用 $O(\log_2 N)$个确定性步骤计算得到。

此外，若 $a$ 从 $\mathbb{Z}_N^*$中均匀随机选取，则以至少 $p(m) = 1 - (m+1)/2^m$ 的概率，阶 $r_a = \mathrm{ord}_N(a)$ 为偶数，且元素 $x = a^{r_a/2}$ 满足 (3.5)。

证明。 由于 $b = a^{2^M}$且 $r_b$为奇数， $a$的阶具有 $r_a = 2^k r_b$的形式，其中 $0 \le k \le M$为某个数。通过测试 $a^{2^k r_b} \equiv 1 \pmod N$（其中 $k = 0$、1、.....、$M$），可以找到最小的 $k$，这需要$O(\log_2 N)$个确定性步骤（重复平方/模幂运算）。
对于该概率结论，应用引理3.2 和命题3.1。 □

# 4 扩散阶数求解

本节介绍分析的核心：一种通过在由 $b$生成的循环子群的凯莱图上迭代半惰性随机游走算子来实现的阶寻找原语。该方法具有局部性：无需构造完整的凯莱图。在点$x \in \langle b \rangle$ 处对随机游走算子应用一次，只需计算其邻居

$$x \longmapsto x\, b^{\pm 2^t} \pmod N \qquad (0 \le t \le M),$$

这可以通过模乘（以及模逆）来执行。

**底层的凯莱图和随机游走矩阵**。设

$$M = \lfloor \log_2 N \rfloor + 1, \qquad G = \langle b \rangle \subseteq (\mathbb{Z}/N\mathbb{Z})^*.$$

考虑具有生成多重集的（无权）凯莱图 $X = X_{N,\,b} = \mathrm{Cay}(G,\ S)$

$$S = \{\, b^{\pm 2^t} : 0 \le t \le M \,\}.$$

等价地， $X$ 这是一个顶点集为 $G$ 且权重为

$$w(x,y) = \#\{\, t \in \{0,\dots,M\} : y = x\,b^{2^t} \text{ or } y = x\,b^{-2^t} \,\}.$$

那么， $X$ 是 $d$正则的，度为 $d = 2(M+1)$ ，其邻接矩阵 $A_X$ 定义如下

$$(A_X p)(x) = \sum_{y \in G} w(x,y)\, p(y).$$

与第2.2节一样， $X$ 上的（简单）随机游走矩阵为

$$P = \frac{1}{d} A_X.$$

特别地，对于函数 $p$: $G \to \mathbb{R}$ ，我们有如下具体公式

$$(Pp)(x) = \frac{1}{2(M+1)} \sum_{t=0}^{M} \Big( p(x\,b^{2^t}) + p(x\,b^{-2^t}) \Big), \qquad x \in G. \tag{4.1}$$

固定一个排序 $G = \{x_1, \text{.....}, {}^{x_{|G|}}\}$ ，并将 $p$: $G \to \mathbb{R}$ 视为列向量

$$(p(x_1), \dots, p(x_{|G|}))^{\mathsf{T}} \in \mathbb{R}^{|G|}.$$

与之前一样，定义相应的半惰性游走算子

$$W = W_{N,b} = \frac{1}{2}(I + P).$$

## 4.1 扩散定理

**定理 4.1 (**扩散阶数求解**)**。 设 $N > 1$ 为一个整数。设 $b \in (\mathbb{Z}/N\mathbb{Z})^*$ 的乘法阶为 $r = \mathrm{ord}_N(b)$ 。令

$$M = \lfloor \log_2 N \rfloor + 1, \qquad G = \langle b \rangle \subseteq (\mathbb{Z}/N\mathbb{Z})^*, \qquad |G| = r.$$

设 $\{p_n\}_{n \ge 0}$ 是定义在 $G$ 上的半惰性游走，其转移矩阵为 $W$ ，初始状态为单位元处的狄拉克函数，即

$$p_0 = \delta_e, \qquad p_n = W^n p_0, \qquad (n \ge 0).$$

那么，对于每一个

$$n \;\ge\; 4(M+1)\big(\log_2 N + 2\big), \tag{4.2}$$

单个读出值 $p_n(e)$ 可唯一确定 $r$，即它是 $(0, N]$ 中唯一一个其倒数位于 $1/(4N^2)$ 内的整数。

定理4.1 将在第 4.2小节中证明。

**推论 4.2**。 在定理 *4.1*的假设下，如果 $|p_n(e) - 1/r| \le 1/(4N^2)$ $t$ *hen*

$$\mathrm{round}\big(1/p_n(e)\big) = r.$$

证明。 由于 $r \le N$，我们有

$$p_n(e) \ge \frac{1}{r} - \frac{1}{4N^2} \ge \frac{1}{N} - \frac{1}{4N^2} = \frac{4N-1}{4N^2} > \frac{3}{4N}.$$

因此

$$\left| \frac{1}{p_n(e)} - r \right| = \left| \frac{r(1/r - p_n(e))}{p_n(e)} \right| \le \frac{N \cdot (1/(4N^2))}{3/(4N)} = \frac{1}{3} < \frac{1}{2},$$

这迫使舍入结果等于 $r$。 □

备注4.3。定理4.1 是在完全一般的情形下陈述的。它只涉及在阶为 $G = \langle b \rangle$ 的循环子群上进行扩散，其中 $r = 阶_N(b)$，其证明不依赖于 $N$ 的任何特殊算术假设，只要求满足明确列出的不等式。然而，在本文其余部分，我们只会在因数分解情形下使用定理4.1 ，此时假设 $N$ 是既非素数也非素数幂的奇整数，并选择 $b$ 使得 $r = 阶_N(b)$ 为奇数。

接下来，我们将陈述并证明一个倍增引理，我们将在下一节4.1 的定理证明中用到它。从概念上讲，这是一个稀疏级数现象：倍增序列$2^t$ 以足够快的速度扩散剩余类，因此必然会遇到一个区间，使得其中的相位具有非正的余弦值；这让人联想到 Korobov型界在稀疏指数和中所利用的机制，参见例如 [KM12]或 [Va19]。

**引理 4.4**（倍增引理）。设 $r$ 为整数，并设 $M \geq 0$ 满足 $2^M > r$。对于满足 $1 \leq k \leq r-1$的每个整数 $k$，存在 $t \in \{0、1、\ldots\ldots、M\}$，使得

$$k2^t \bmod r \in \left[\frac{r}{4}, \frac{3r}{4}\right].$$

证明。对于每个 $t \geq 0$，令 $a_t \in \{0、1、\ldots\ldots、r-1\}$ 为 $k2^t$ 模 $r$的最小剩余。反设对于所有 $t \in \{0、\ldots\ldots、M\}$，

$$a_t \in \left[0, \frac{r}{4}\right) \cup \left(\frac{3r}{4}, r\right).$$

Set

$$b_t := \min(a_t,\ r - a_t).$$

于是，对所有 $t \in \{0, \ldots, M\}$，都有 $0 < b_t < r/4$。

我们断言，对于 $t = 0, \ldots, M-1$，有 $b_{t+1} = 2b_t$。若 $a_t < r/4$，则 $2a_t < r/2 < r$，因此 $a_{t+1} = 2a_t$，进而 $b_{t+1} = 2b_t$。若 $a_t > 3r/4$，则 $2a_t \in (3r/2, 2r)$，所以 $a_{t+1} = 2a_t - r \in (r/2, r)$，因此

$$b_{t+1} = r - a_{t+1} = r - (2a_t - r) = 2(r - a_t) = 2b_t.$$

因此，对所有 $t \leq M$，都有 $b_t = 2^t b_0$。由于 $b_0 = \min(k, r-k) \geq 1$，我们有 $b_M \geq 2^M$。

根据假设， $2^M > r$，因此 $b_M \geq 2^M > r/4$，这与 $b_M < r/4$ 矛盾。这个矛盾证明了该引理。□

回忆一下，对于 $k \in \{0, 1, \ldots\ldots, r-1\}$，如果

$$\chi_k(j) = \exp\left(\frac{2\pi i k j}{r}\right), \qquad j \in \mathbb{Z}/r\mathbb{Z},$$

then

$$\frac{1}{r}\sum_{k=0}^{r-1} \chi_k(j) = \begin{cases} 1, & j \equiv 0 \pmod r, \\ 0, & j \not\equiv 0 \pmod r. \end{cases}$$

## 4.2 定理 4.1 的证明

*Pro*的。我们改用加法记号。子群 $G = \langle b \rangle$ 是一个阶为 $r$ 的循环群。因此 e,

$$\phi : \mathbb{Z}/r\mathbb{Z} \longrightarrow G, \qquad \phi(j) = b^j$$

是一个同构。利用 $\phi$ ，我们通过 $\tilde{p}(j) = p(b^j)$ 将函数 $p : G \to \mathbb{R}$ 变换为函数 $\tilde{p} : \mathbb{Z}/r\mathbb{Z} \to \mathbb{R}$。特别地， $\tilde{p}(0) = p(e)$。在此识别下，右乘

$b^{\pm 2^t}$ 变为模 $r$ 的平移 $\pm 2^t$。因此，随机游走算子 $P$ 变为平移不变随机游走

$$(P\widetilde{p})(j) = \frac{1}{2(M+1)} \sum_{t=0}^{M} \Big( \widetilde{p}(j+2^t) + \widetilde{p}(j-2^t) \Big), \qquad j \in \mathbb{Z}/r\mathbb{Z}.$$

现在，特征标是 $P$ 的特征函数。由于 $\chi_k(j \pm a) = \chi_k(j)\chi_k(\pm a)$, has

$$(P\chi_k)(j) = \chi_k(j) \cdot \frac{1}{2(M+1)} \sum_{t=0}^{M} \left( e^{2\pi i k 2^t / r} + e^{-2\pi i k 2^t / r} \right) = \chi_k(j) \cdot \frac{1}{M+1} \sum_{t=0}^{M} \cos\left( \frac{2\pi k 2^t}{r} \right).$$

因此， $P\chi_k = \mu_k \chi_k$ 满足

$$\mu_k = \frac{1}{M+1} \sum_{t=0}^{M} \cos\left( \frac{2\pi k 2^t}{r} \right),$$

因此 $W\chi_k = \lambda_k \chi_k$ 其中 $\lambda_k = (1+\mu_k)/2$。如前所述（2.3）， $\lambda_0 = 1$ 且 $0 \le \lambda_k \le 1$对所有 $k$。

设 $\delta_0$ 为 $0 \in \mathbb{Z}/r\mathbb{Z}$ 处的狄拉克函数。根据正交性，

$$\delta_0(j) = \frac{1}{r} \sum_{k=0}^{r-1} \chi_k(j).$$

应用 $W^n$ 并在 0 处求值，得到

$$(W^n \delta_0)(0) = \frac{1}{r} \sum_{k=0}^{r-1} \lambda_k^n = \frac{1}{r} + \frac{1}{r} \sum_{k=1}^{r-1} \lambda_k^n.$$

映射回 $G$ 后，左侧恰好是 $p_n(e)$，因此

$$\left| p_n(e) - \frac{1}{r} \right| \le \max_{1 \le k \le r-1} \lambda_k^n. \tag{4.3}$$

固定 $k \in \{1, \dots, r-1\}$。由引理 4.4 可知存在 $t \in \{0, \dots, M\}$ 使得

$$k 2^t \bmod r \in \left[ \frac{r}{4}, \frac{3r}{4} \right], \qquad \text{hence} \qquad \cos\left( \frac{2\pi k 2^t}{r} \right) \le 0.$$

所有其他余弦项均为 $\le 1$，因此

$$\mu_k \le \frac{M}{M+1} = 1 - \frac{1}{M+1}, \qquad \text{and therefore} \qquad \lambda_k = \frac{1+\mu_k}{2} \le 1 - \frac{1}{2(M+1)}.$$

结合式（4.3），并利用 $1 - x \le \mathrm{e}^{-x}$,

$$\left| p_n(e) - \frac{1}{r} \right| \le \left( 1 - \frac{1}{2(M+1)} \right)^n \le \exp\left( -\frac{n}{2(M+1)} \right).$$

若 $n \ge 4(M+1)(\log_2 N + 2)$，则

$$\exp\left( -\frac{n}{2(M+1)} \right) \le \exp(-2(\log_2 N + 2)) = \mathrm{e}^{-4}\, \mathrm{e}^{-2\log_2 N}.$$

由于 $\log_2 N = \ln N / \ln 2 \ge \ln N$，我们有 $\mathrm{e}^{-2\log_2 N} \le \mathrm{e}^{-2\ln N} = N^{-2}$，因此右侧为$\le \mathrm{e}^{-4} N^{-2} < \frac{1}{4N^2}$。于是

$$\left| p_n(e) - \frac{1}{r} \right| \le \frac{1}{4N^2}.$$

**唯一性** $r$。 由于 $r = \mathrm{ord}_N(b)$ 整除 $|\mathbb{Z}_N^*| = \varphi(N)$ 和 $N > 1$，我们有 $\varphi(N) < N$，因此 $r < N$。（特别是 $2^M > N > r$， 对于 $M = \lfloor \log_2 N \rfloor + 1$.）对于互不相同的整数 $a \neq b \mathrm{in} \{1, \ldots, N\}$，

$$\left| \frac{1}{a} - \frac{1}{b} \right| = \frac{|a-b|}{ab} \geq \frac{1}{N^2}.$$

因此，至多存在一个整数 $r' \in (0, N]$ 使得 $\left| p_n(e) - \frac{1}{r'} \right| \leq \frac{1}{4N^2}$。前述估计表明， $r$ 满足该不等式，因此由 $p_n(e)$可唯一确定 $r$ 。 □

## 5 扩散辅助因数分解算法

本节介绍扩散辅助因数分解算法。该算法以具有 $m \geq 2$ 个奇素因子的正整数 $N$ 为输入。对于随机整数$a \in \{1, 2, \ldots\ldots, N-1\}$的每一种取值，算法以至少 $p(m) = 1 - 2^{-m}(m+1)$ 的概率返回$N$的一个因子 $d$ 。

在我们 继续介绍该算法的伪代码之前，先陈述以下两条备注 s.

备注 5.1. 算法 1 与 Shor 因数分解算法一样，具有概率性：一次试验 (即选取一个 $a$ 并执行后续步骤)可能会以重新开始（`continue` 在算法 1中；等价地，针对特定的 $a$返回 $x \equiv \pm 1$ (模 $N$) ，因此只会得到平凡的最大公约数。

然而，对于至少有两个不同素因子的合数 $N$ ，每次独立试验都有非零的成功概率，该概率仅取决于中国剩余定理奇偶模式（参见命题 3.6和引理3.2）。因此，独立重复该过程会使总体失败概率非常接近于 0。

概率优化问题 $p(m)$ 我们将留待以后探讨其成功概率。就此而言， [Za13]的方法似乎适用。

备注5.2。 实际应用中，在调用算法 之前，可以高效地排除“$N$ 是素数”和“$N$ 是素数幂”这两种情况。对于素性测试，有快速随机测试（例如 Miller–Rabin）、确定性多项式时间算法（ AKS）以及实用的基于证书的方法（例如 ECPP）。要测试 $N$ 是否为素数幂，可以先执行完全幂测试（判断是否存在 $N = u^k$ 且 $k \geq 2$），如果存在，再对底数 $u$进行素性测试。参见例如 [ CP05]。

**算法 1：** 扩散辅助因式分解($N$)

**输入：** 既非素数也非素数幂的奇合数 $N \geq 3$ 。

**输出：** $N$的一个非平凡因子 $d$ 。

**当**$true$ **时执行**

**(1) 随机选择和最大公因数测试。**

选择 $a \leftarrow$ 在$\{1, 2, \ldots, N-1\}$中均匀分布。

$d \leftarrow$ 最大公约数$(a, N)$。

**如果** $1 < d < N$**，则**

  **返回** $d$

**(2) 计算加倍多重集。**

$M \leftarrow \lfloor$对数$_2\, N \rfloor + 1$。

计算

$$S\ (a)\ \ = \{a^{\pm 2^t} \text{ 模 } N\colon \quad t = 0, 1, \ldots, M\}$$

通过重复平方（和求逆）。

**(3) 早期碰撞分支。**

**如果** $S(a)$ 包含重复项**则**

  从该重复项中确定性地提取一个奇数 $q$ 和最小的 $s \geq 0$ ，使得 $a^{2^s q} \equiv 1$ (模 $N$) (引理 3.2)。

  **如果** $s > 0$ **则**

    $x \leftarrow a^{2^{s-1} q}$ 模 $N$。

    $d \leftarrow$ 最大公约数$(x - 1,\ N)$。

    **如果** $1 < d < N$**，则**

      **返回** $d$

**(4) 将阶奇化。**

$b \leftarrow a^{2^M}$ 模 $N$。

`// then` 阶$_N(b)$ `is odd (Lemma 3.5)`

**(5) 扩散阶数求解。**

使用扩散原语（定理 4.1）来恢复 $r_b \leftarrow$ 阶$_N(b)$。

**(6) 提升阶数并提取因子。**

求最小的 $k \in \{0$、$1$、.....、$M\}$ 使得 $a^{2^k r_b} \equiv 1 \pmod{N}$。

$r_a \leftarrow 2^k r_b$。

**if** $r_a$ 为偶数**则**

  $x \leftarrow a^{r_a/2}$ 模 $N$。

  $d \leftarrow$ 最大公约数$(x - 1,\ N)$。

  **若** $1 < d < N$ **则**

    **返回** $d$

**继续** `// 失败 for this` $a$`; restart with new` $a$

## 6 通过碰撞与最大公约数稳定化进行关系查找

本节讨论一种互补的（更快的）机制，用于从探索凯莱图时碰撞产生的显式关系中恢复阶 $r = \mathrm{ord}_N(b)$

$$G = \langle b \rangle \subseteq (\mathbb{Z}/N\mathbb{Z})^*.$$

我们将凯莱图视为从单位元出发，通过沿着二进生成多重集中的短词进行探索。

$$S = \{\, b^{\pm 2^t} : \ 0 \le t \le M \,\}, \qquad M = \lfloor \log_2 N \rfloor + 1.$$

每当两个不同的抽样词落在同一个顶点上时，我们就得到群中的一个算术关系。反复发生碰撞会产生许多这样的关系；对相应的指数取最大公约数，往往会稳定到 $r$ （或 $r$的一个小倍数）。

我们注意到，这样的两个词结合起来会在图上形成一条闭测地线，因此当前的问题与测量图的围长、检测其最短非平凡闭路密切相关。因此，我们展示了另一种方式，说明所考虑图的几何性质与和 $\mathrm{ord}_N(b)$相关的算术之间存在联系。

## 6.1 指数词与环关系

与定理的证明4.1 （以及全文）一样，我们使用指数坐标。假设 $r$ 为奇数，并将

$$G = \langle b \rangle \simeq \mathbb{Z}/r\mathbb{Z}, \qquad j \longmapsto b^j.$$

长度为 $L$的（非惰性）词是一个序列

$$w = [(\varepsilon_1, t_1), \dots, (\varepsilon_L, t_L)], \qquad \varepsilon_i \in \{\pm 1\}, \ \ t_i \in \{0, \dots, M\}.$$

其整数指数和终点为

$$E(w) = \sum_{i=1}^{L} \varepsilon_i 2^{t_i} \in \mathbb{Z}, \qquad x(w) = b^{E(w)} \in G.$$

显然,

$$|E(w)| \le L\, 2^M. \tag{6.1}$$

**定义 6.1 (**词碰撞与循环关系**).** 设 $w, w'$ 是长度至多为 $L$ 的词。若 $(w, w')$ 满足词碰撞，则称其为词碰撞。

$$x(w) = x(w') \quad \text{in } G.$$

相关的 环差 (或环指数)是

$$D(w, w') = E(w) - E(w').$$

如果 $E(w) \neq E(w')$，则称词碰撞为非平凡的；等价地，如果 $D(w, w') \neq 0$，也成立。.

**命题 6.2.** 设 $w$， $w'$ 是长度至多为 $L$ 的词，构成一个 非平凡的 词碰撞（定义*6.1*）。那么

$$D(w, w') \neq 0, \qquad r \mid D(w, w'), \qquad \textit{and} \qquad 0 < |D(w, w')| \le 2L\, 2^M.$$

等价地，存在 $q \in \mathbb{Z} \setminus \{0\}$，使得

$$D(w, w') = q\, r \qquad \textit{and} \qquad |q\, r| \le 2L\, 2^M.$$

证明。 碰撞 $x(w) = x(w')$ 意味着

$$b^{E(w)} \equiv b^{E(w')} \pmod{N},$$

因此

$$b^{E(w)-E(w')} \equiv 1 \pmod{N}.$$

根据 $r = \mathrm{ord}_N(b)$ 的定义，这意味着 $r \mid D(w, w')$。
如果 $E(w) = E(w')$，那么 $D(w, w') = 0$，且该碰撞不会产生关系；根据假设，我们讨论的是非平凡情形，因此 $D(w, w') \neq 0$。
最后，根据（6.1），

$$|D(w, w')| \leq |E(w)| + |E(w')| \leq 2L\, 2^M. \qquad \square$$

备注 6.3（运行中的最大公约数始终是 $r$ 的倍数）。如果 $D_1, \ldots, D_s$ 是来自非平凡词碰撞的非零环路差，那么每个 $D_i$ 都能被 $r$ 整除，因此

$$r \mid g_s = \gcd(|D_1|, \ldots, |D_s|).$$

因此，随着收集到更多关系，运行中的最大公约数只会减小，并且始终是真实阶的倍数。

## 6.2 最大公因数稳定化与 ζ 函数

根据命题 6.2，每次碰撞都会产生一个非零关系 $D_i = q_i r \neq 0$，$i = 1, \ldots, s$ 并且我们取最大公约数 $g_s = \gcd(|D_1|, \ldots, |D_s|)$。显然，

$$g_s = r \cdot \gcd(|q_1|, \ldots, |q_s|).$$

特别地，$g_s = r$ 当且仅当 $\gcd(q_1, \ldots, q_s) = 1$。
因此，阶恢复归结为弄清 $\gcd(q_1, \ldots, q_s)$ 多快会降至 1。
注 6.4。在有利的长游走中，不同的碰撞来自本质上互不相关的词对，乘数 $q_i = D_i/r$ 的行为近似于一组大小相近、彼此近似独立的非零整数。

以下定理在文献中广为人知（参见 [Nym72] 和 [Leh00]）。

**定理 6.5** (最大公因数的黎曼ζ定律)。固定 $s \geq 2$。设 $U_1, \ldots, U_s$ 是独立随机整数，且每个都在 $\{1, 2, \ldots, Q\}$ 上均匀分布。当 $Q \to \infty$ 时，

$$\Pr(\gcd(U_1, \ldots, U_s) = 1) = \frac{1}{\zeta(s)} + O\left(\frac{\delta_{s=2} \log Q + 1}{Q}\right),$$

其中，当 $s = 2$ 时为 $\delta_{s=2} = 1$，否则为零。

注 6.6。

$$\frac{1}{\zeta(2)} = \frac{6}{\pi^2} \approx 0.608, \qquad \frac{1}{\zeta(3)} \approx 0.832, \qquad \frac{1}{\zeta(4)} = \frac{90}{\pi^4} \approx 0.924.$$

这解释了为什么通常只需少数独立关系，运行中的最大公约数就足以降至真实阶。

## 7 随机游走在 $G$ 上的碰撞界

We 将碰撞的讨论具体应用于我们在循环群上的（半惰性）随机游走 p

$$G = \langle b \rangle, \qquad |G| = r,$$

其转移算子为 $W$，如前几节所述。对于 $x$，$y \in G$ 和 $t \geq 0$，定义 $t$ 步转移概率为

$$p(y, x; t) = (W^t \delta_y)(x).$$

因此，$p(y,\ x;\ t)$ 表示从 $y$ 开始的随机游走在经过 $t$ 步后位于 $x$ 的概率。特别地，从单位元 $e$ 开始的随机游走在时间 $t$ 时的端点分布为

$$p_t(x) = p(e, x; t) = (W^t \delta_e)(x), \qquad x \in G.$$

为避免单条轨迹上所取样本之间的依赖关系，我们通过独立随机游走生成端点：从 $e$ 出发运行 $t$ 步，记录端点，在 $e$ 处重新开始，并将这一过程重复 $T$ 次。

**定义 7.1**。 固定 $t \geq 0$ 和一个整数 $T \geq 1$。令 $\Omega = G^T$。对于 $\mathbf{x} = (x_1、\ldots\ldots、x_T) \in \Omega$，定义坐标映射

$$X_i : \Omega \to G, \qquad X_i(\mathbf{x}) = x_i \qquad (i = 1, \ldots, T).$$

**定义 7.2**。 假设定义 7.1。我们称 $X_1、\ldots\ldots、X_T$是在时间 $t$通过独立重启进行采样的，**如果对每个** $\mathbf{x} = (x_1、\ldots\ldots、x_T) \in \Omega$，

$$\Pr\big((X_1, \ldots, X_T) = (x_1, \ldots, x_T)\big) = \prod_{i=1}^{T} p(e, x_i; t).$$

**定义 7.3**。 假设定义 7.2。我们称样本 $X_1，\ldots\ldots，X_T$中发生了 $1 \leq i < j \leq T$与 $x \in G$的 $X_i（x）= X_j（x）$。

**定义 7.4**。 将时刻 $t$ 的碰撞参数定义为

$$s_2(t) = \sum_{x \in G} p(e, x; t)^2 = \sum_{x \in G} p_t(x)^2.$$

**定理 7.5**。 设 $X_1，\ldots\ldots，X_T$是在时刻 $t$（定义 7.2）通过独立重启获得的。令 $Z$ 表示 $T$ 个样本中碰撞对的数量，即

$$Z = \#\{(i, j) : 1 \leq i < j \leq T,\ X_i(x) = X_j(x) \text{ for some } x \in G\}.$$

在时刻 $t$，$T$ 条独立随机游走中首次碰撞的期望值为

$$\mathrm{E}[Z] = \binom{T}{2} s_2(t).$$

特别地，当 $t \to \infty$，从而 $x \mapsto p（e，\ x；\ t）$接近 $G$ 上的均匀分布时，我们有

$$\mathrm{E}[Z] \sim \frac{T(T-1)}{2r}. \tag{7.1}$$

证明。 随机变量 $X_1, \ldots, X_T$ 相互独立，且

$$\Pr(X_i = x) = p_t(x) = p(e, x; t), \qquad (x \in G,\ i = 1, \ldots, T).$$

因此，期望值 $\mathrm{E}[Z]$ 为

$$\mathrm{E}[Z] = \sum_{1 \le i < j \le T} \Pr(X_i(x) = X_j(x) \text{ for some } x \in G).$$

固定 $i < j$。利用独立性和共同分布 $p_t$，我们有

$$\Pr(X_i = X_j) = \sum_{x \in G} \Pr(X_i = x,\ X_j = x) = \sum_{x \in G} \Pr(X_i = x) \Pr(X_j = x) = \sum_{x \in G} p_t(x)^2 = s_2(t).$$

共有 $\binom{T}{2}$ 种选择 $(i,\ j)$，因此（7.1）成立。

最后，如果 $t$ 足够大，使得 $p_t$ 在 $G$ 上接近均匀分布（因此，对所有 $x \in G$，$p_t(x) \approx 1/r$），则 n

$$s_2(t) = \sum_{x \in G} p_t(x)^2 \approx \sum_{x \in G} \frac{1}{r^2} = \frac{1}{r},$$

这就证明了第二个结论。 □

注 7.6。 从启发式角度来说，定理 7.5 告诉我们，$T$个独立随机游走在时刻 $t$ 发生首次碰撞是合理的（即碰撞期望接近 1），只要

$$\binom{T}{2} s_2(t) \approx 1, \qquad \text{equivalently} \qquad T \approx \frac{1}{\sqrt{s_2(t)}}.$$

特别是，如果 $t$ 足够大，使得 $x \mapsto p(e,\ x; t)$ 在 $G$ 上接近均匀分布，那么

$$s_2(t) \approx \frac{1}{r}, \qquad \text{and hence} \qquad T \approx \sqrt{r}.$$

注 7.7。 上述启发式论证立即区分了纯数字碰撞搜索的两种情形（即对行走过程进行模拟，并通过普通算术而非扩散原语生成端点）。在一般情况下，预期有

$$r = \mathrm{ord}_N(b) \text{ to be large, typically comparable to } \varphi(N) \text{ (and often of order } N).$$

于是碰撞尺度变为

$$T \approx \sqrt{r} \ \approx \ \sqrt{\varphi(N)},$$

因此，要看到第一次碰撞，所需的重新开始次数本身约为环境群大小的平方根。这正是人们对经典数字算法的预期：其生成关系的唯一机制是碰撞检测；它受统计规律支配，无法在 $\log\ N$ 中得到多项式时间的阶查找过程。

另一方面，如果所选底数恰好具有较小的阶

$$r = \mathrm{ord}_N(b) \ll \varphi(N),$$

那么同一估计预示着显著的数字加速：

$$T \approx \sqrt{r} \ \ll \ \sqrt{\varphi(N)}.$$

在这种情况下，该方法在普通数字计算机上相当实用，因为采样负担从 $\varphi$（$N$）的平方根降至 $r$ 的平方根，而后续的最大公约数稳定化步骤通常只需要少量实质上相互独立的关系。数值实验中可以观察到这一现象；参见示例8.3，其中 $r$ 足够小，因此经过数量适中的独立重启后便会出现碰撞，并且通过标准数字处理即可快速求得该阶。

值得将这种数字加速与基于扩散的模型中发生变化（以及不变）的部分区分开来。当第4节中的扩散原语可用时，求得该阶并不是靠等待随机游走端点发生碰撞。相反，只需在经过可控次数的扩散迭代后读取一个热核值：分析表明，经过$t = O((\log_2 N)^2)$次更新后，分布已足够平坦，使得 $p_t$（$e$） $\approx 1/r$，而这个单一标量已可通过舍入确定 $r$ 。因此，尺度 $T \approx \sqrt{r}$ 并不是决定基于扩散的阶查找过程性能的量。

相比之下，如果试图在扩散设备中实现碰撞方法本身，那么数字估算 $T \approx \sqrt{r}$ 仍然描述了要生成多少基本独立的样本才能观察到碰撞。将 $\sqrt{\varphi(N)}$ 替换为 $\sqrt{r}$ 在软件中可能带来显著改进，但对物理扩散器的影响可能有限，因为主要成本往往取决于表示和演化某种状态所需的规模、能量与精度，而该状态所依托的顶点集大小约为 $r$ 个元素。

最后，我们可以设想一些混合变体，更直接地利用扩散硬件进行基于碰撞的关系查找。我们不必只从单位元 $e$重新开始，而可以同时从许多起始点启动扩散，让质量从多个源向外扩散，从而并行探索凯莱图。在这种图景中，“碰撞”将表现为不断扩展的分布（热前沿）相互重叠，而不是两个采样终点字面上的重合。本文不探讨这类多源增长策略，但它们为如何在上述分析的单源设置之外利用扩散并行性，指明了一个自然方向。

# 8 示例

本节通过不同的合数示例，说明基于扩散的阶恢复，并展示采用数字碰撞策略的示例。

## 8.1 示例 1： $N = 299$

取 $N = 299 = 13 \cdot 23$ 和 $b = 3 \in (\mathbb{Z}/N\mathbb{Z})^*$.。检查可知，$\gcd(b, N) = 1$。元素 $b$ 在模 $N$ 下的乘法阶为奇数：

$$r = \mathrm{ord}_{299}(3) = 33.$$

如第 4 节所述，我们在循环子群 $\langle b \rangle \subset (\mathbb{Z}/N\mathbb{Z})^*$ 上构造凯莱图，使用生成元 $b^{\pm 2^t}$，其中 $0 \le t \le M$ 具有 $M = \lfloor \text{对数}_2\, N \rfloor + 1$。见图 1。然后，我们从单位元开始运行半懒随机游走。

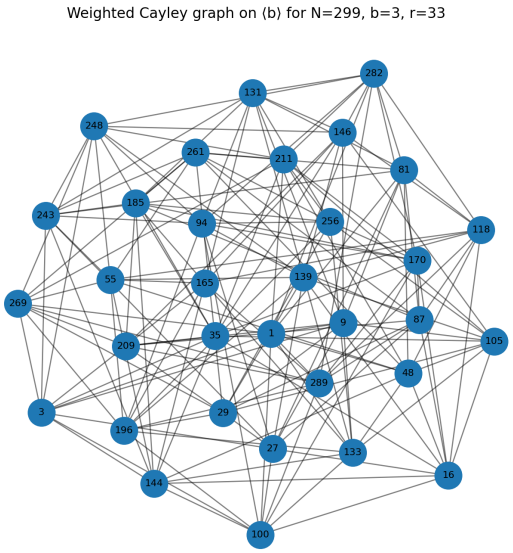


图 1：以生成元 $b^{\pm 2^t}$ 构成的 $\langle 3\rangle \subset (\mathbb{Z}/299\mathbb{Z})^*$ 上的凯莱图。这里 $N = 299$、$b = 3$，且 $\mathrm{ord}_{299}(3) = 33$。

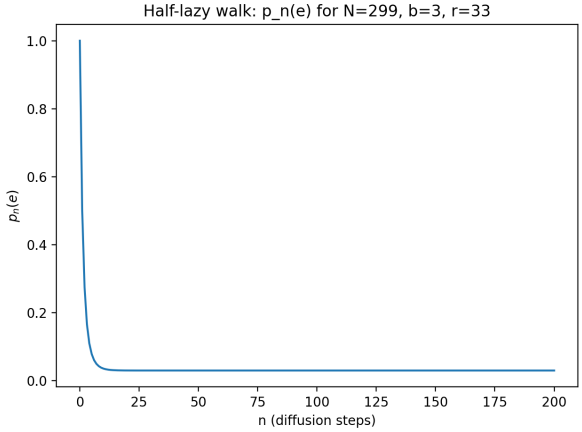


图 2：在 $\langle 3\rangle$ 上的半惰性随机游走的单位元处的取值 $p_n(e)$（其中 $N = 299$）。

**通过舍入恢复阶。** 如图 2所示，$p_n(e)$ 迅速趋近于 $1/r$，因此 $1/p_n(e)$ 趋近于 $r = 33$。图 3 绘制了 $1/p_n(e)$ 以及目标水平 $r$。从数值上看，舍入很快就稳定下来：从 $n = 17$ 开始，有

$$\mathrm{round}\big(1/p_n(e)\big) = 33.$$

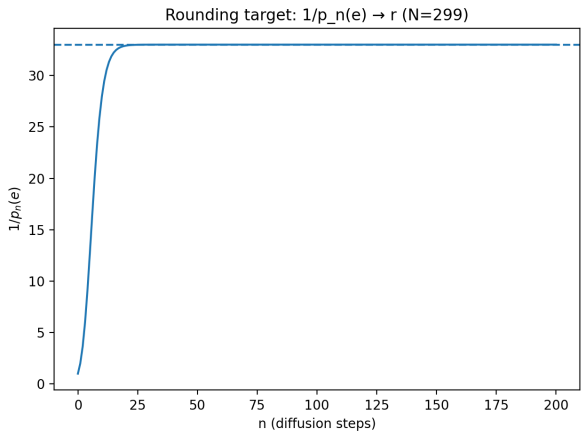


图3：序列 $1/p_n(e)$ 收敛到 $r = \mathrm{ord}_{299}(3) = 33$；舍入可恢复 $r$。（虚线表示 $r = 33$。）

这为扩散模型提供了一个具体的"小-$N$"可视化：动力学逐渐混合，趋向$\langle b\rangle$ 上的均匀分布（大小为 $r$），而当它足够接近 $1/r$时，单个标量读出 $p_n(e)$即可确定 $r$。

## 8.2 例2： $N = 1022117$

现在，我们取 $N = 1009{\cdot}1013 = 1022117$，以及 $b = 576 \in (\mathbb{Z}/N\mathbb{Z})^*$。检查可得 $\gcd(b, N) = 1$，且 $b$ 模 $N$ 的阶为奇数：

$$r = \mathrm{ord}_N(b) = 5313.$$

我们在循环子群 $\langle b\rangle$ 的加权凯莱图上运行半惰性扩散，使用生成元 $b^{\pm 2^t}$，针对 $0 \le t \le M$，其中 $M = \lfloor \log_2 N \rfloor + 1$。理论预测，经过$n = O((\log_2 N)^2)$ 个扩散步后，单位元处的单个热核值通过舍入即可确定 $r$ $1/p_n(e)$。参见图 5和 6。

注释 8.1. 扩散更新具有局部性，因此实现不 需要预先构建整个凯莱图。不过，为了便于可视化，我们只绘制单位元附近的一小片区域（局部视图），因为完整的图有 $r = 5313$ 个顶点。参见图 4。

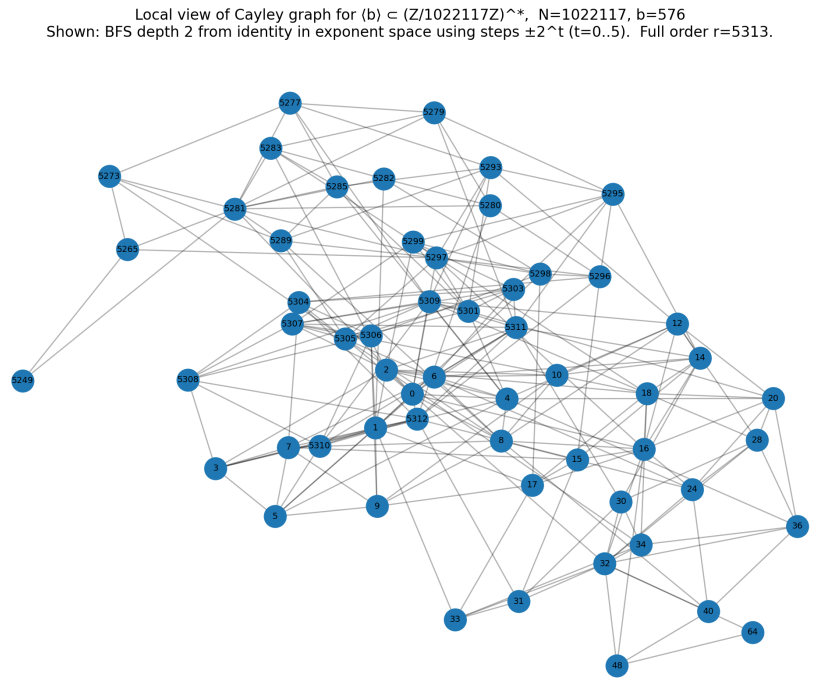


图 4：单位元附近凯莱图的局部视图（以指数坐标表示）。这仅用于示意；完整的凯莱图有 $r = 5313$ 个顶点。

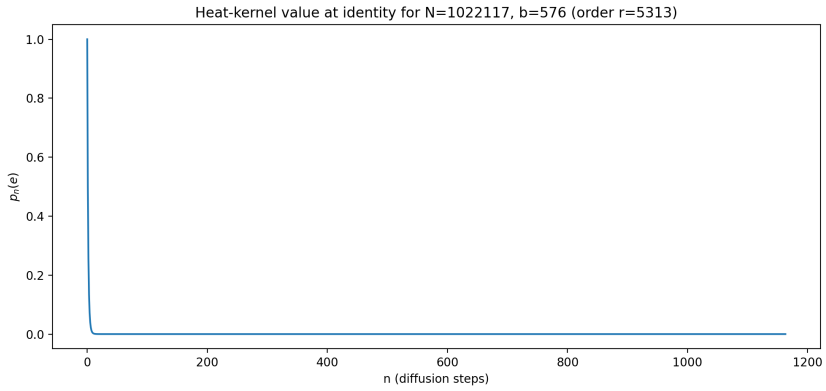


图 5：单位元处的热核值 $p_n(e)$随扩散步数 $n$ 变化的情况。当 $n \to \infty$ 时，有 $p_n(e) \to 1/r$。

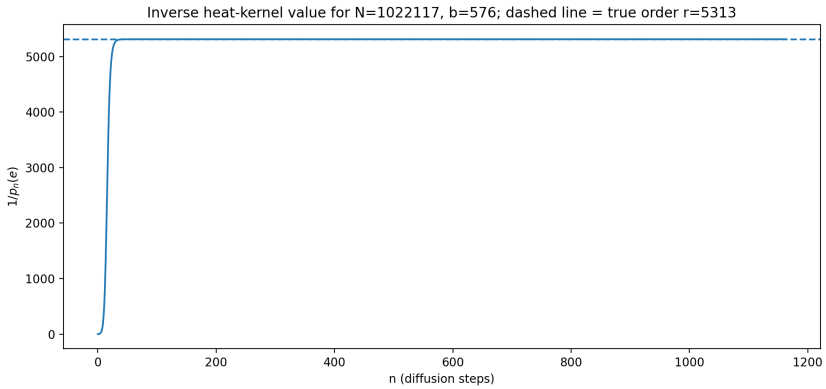


图6：逆值 $1/p_n(e)$ 收敛至真实阶 $r = 5313$ （虚线）。本次运行中，舍入 $1/p_n(e)$ 在经过相对较少的扩散步数后恢复了 $r$ 。

### 8.3 例3： $F_5 = 2^{2^5} + 1$

我们在费马数上展示循环搜索实现

$$F_5 = 2^{2^5} + 1 = 2^{32} + 1 = 4294967297.$$

$$\langle a \rangle \subset (\mathbb{Z}/N\mathbb{Z})^*$$

不同的词落在同一个终点，

$$a^{E_{\text{new}}} \equiv a^{E_{\text{prev}}} \pmod{N},$$

我们记录一份循环证书。这会产生一个指数差

$$D = E_{\text{new}} - E_{\text{prev}} \qquad \text{with} \qquad a^D \equiv 1 \pmod{N},$$

因此 $D$ 是阶 $r = \text{ord}_N(a)$ 的倍数。随后，我们应用标准的“尽可能减半”约简，得到一个更小的倍数 $D_{\min}$，并持续维护运行中的最大公约数

$$g \leftarrow \gcd(g, D_{\min}).$$

实际应用中，经过适量的碰撞后，这个最大公约数通常会稳定为阶的倍数，随后可将其约化为真实阶，并用于常规的阶到因数步骤。
对于 $N = F_5$，使用词长 $L = 2000$、最多 120000 个样本和 8 的稳定性阈值时，算法首次尝试便成功，随机底数为

$$a = 3945765912.$$

连续的循环结果以及运行中的最大公约数的变化如下：

```
[attempt 1] trying a = 3945765912
    sampling words of length L = 2000, max_samples = 120000, stable_hits = 8
[collision #  1]  D_min = 314919552   running_gcd = 314919552
[collision #  2]  D_min = 32543920512   running_gcd = 6700416
[collision #  3]  D_min = 52336949376   running_gcd = 6700416
[collision #  4]  D_min = 22975726464   running_gcd = 6700416
[collision #  5]  D_min = 40839035520   running_gcd = 6700416
[collision #  6]  D_min = 25012652928   running_gcd = 6700416
[collision #  7]  D_min = 4187760000   running_gcd = 6700416
```

```
[collision #  8]  D_min = 3986747520   running_gcd = 6700416
[collision #  9]  D_min = 18097823616   running_gcd = 6700416
[collision # 10]  D_min = 9749105280   running_gcd = 6700416
  stabilized gcd = 6700416
  reduced order r = 6700416
```

第二次碰撞后，运行中的最大公约数降至 $g = 6700416$ 并保持不变；再经过几次碰撞后，便满足稳定化判据。随后进行的确定性约简证实

$$r = \mathrm{ord}_N(a) = 6700416.$$

最后，由于 $r$ 为偶数且 $a^{r/2} \not\equiv \pm 1 \pmod{N}$，标准的阶到因数步骤可得非平凡因数：

$$\gcd(a^{r/2} - 1,\, N) = 6700417, \qquad \gcd(a^{r/2} + 1,\, N) = 641,$$

因此

$$F_5 \;=\; 4294967297 \;=\; 641 \cdot 6700417.$$

本次运行中，观测到的运行时间为 **11.734** 秒。

### 8.4 示例 4： $N = 8219999$

一种近期开发的量子退火方法将紧凑二进制乘法器电路嵌入 Pegasus 拓扑，并报告了因数分解

$$N = 8219999 = 251 \cdot 32749$$

在 D-Wave Advantage 4.1 退火机上进行；参见 [DSS24]。

我们对同一个整数 $N$应用带环扩散实现。该算法探索循环子群的凯莱图

$$\langle a \rangle \subset (\mathbb{Z}/N\mathbb{Z})^{\times}$$

u使用二进制幂生成元 $a^{\pm 2^t}$。每当两个不同的词落在同一个终点 nt,

$$a^{E_{\mathrm{new}}} \equiv a^{E_{\mathrm{prev}}} \pmod{N},$$

我们就得到一个指数差为 $D = E_{\mathrm{new}} - E_{\mathrm{prev}}$ 的循环证书，因此 $a^D \equiv 1 \pmod{N}$。在“尽可能折半”以得到 $D_{\min}$后，我们更新运行中的最大公约数 $g \leftarrow \gcd(g,\ D_{\min})$；一旦 $g$ 稳定下来，就将其约化为真实阶 $r = \mathrm{ord}_N(a)$，并用于标准的从阶到因数分解步骤。

这次运行中，我们使用了词长 $L = 2000$，样本数最多为 **120000**，稳定性阈值为 **8**。算法首次尝试便成功，使用的底数为 $a = 7081686$：

```
[attempt 1] trying a = 7081686
    sampling words of length L = 2000, max_samples = 120000, stable_hits = 8
[collision #  1]  D_min = 12962750   running_gcd = 12962750
[collision #  2]  D_min = 111206750   running_gcd = 682250
[collision #  3]  D_min = 119393750   running_gcd = 682250
[collision #  4]  D_min = 42981750   running_gcd = 682250
[collision #  5]  D_min = 3411250   running_gcd = 682250
[collision #  6]  D_min = 3411250   running_gcd = 682250
```

```
[collision #  7]  D_min = 130309750   running_gcd = 682250
[collision #  8]  D_min = 68907250   running_gcd = 682250
[collision #  9]  D_min = 104384250   running_gcd = 682250
[collision # 10]  D_min = 55262250   running_gcd = 682250
  stabilized gcd = 682250
  reduced order r = 682250

SUCCESS: N = 32749 * 251

FINAL: 8219999 = 251 * 32749
TOTAL TIME: 3.120 s  (0:00:03)
```

因此，在这个实例中，循环方法恢复了因数分解结果

$$8219999 = 251 \cdot 32749$$

在报告的运行中，运行时间约为 3.12 秒。

### 8.5 示例 5： $N = 1099551473989$

在 Zapata Computing 及其合作者开展的研究中，整数 $N = 1{,}099{,}551{,}473{,}989$ 使用超导量子处理器上的变分量子因式分解（VQF）工作流程进行了因数分解；参见 [KSK21]。以下是碰撞策略的结果。

```
Enter N (odd, >3, not prime, not prime power), up to ~10 digits recommended: 1099551473989
Choose word length L (e.g. 800-2000): 2000
Choose max_samples per attempt (e.g. 30000-120000): 120000Choose max_attempts (e.g. 20-80): 80


[attempt 1] trying a = 28213600916sampling words of length L = 2000,
 max_samples = 120000, stable_hits = 8
no stabilized gcd from loops in this attempt (try another a).

[attempt 2] trying a = 1010844181454sampling words of length L = 2000,
 max_samples = 120000, stable_hits = 8
no stabilized gcd from loops in this attempt (try another a).

[attempt 3] trying a = 45342608514sampling words of length L = 2000,
 max_samples = 120000, stable_hits = 8
[collision #  1]  D_min = 33192646812150   running_gcd = 33192646812150
no stabilized gcd from loops in this attempt (try another a).

[attempt 4] trying a = 528571176770sampling words of length L = 2000,
 max_samples = 120000, stable_hits = 8
no stabilized gcd from loops in this attempt (try another a).

[attempt 5] trying a = 591840418317sampling words of length L = 2000,
 max_samples = 120000, stable_hits = 8
no stabilized gcd from loops in this attempt (try another a).

[attempt 6] trying a = 327685619692
  sampling words of length L = 2000,  max_samples = 120000,  stable_hits =
```

```
  no stabilized gcd from loops in this attempt (try another a).

[attempt 7] trying a = 1046655708948sampling words of length L = 2000,
 max_samples = 120000,  stable_hits = 8
no stabilized gcd from loops in this attempt (try another a).

[attempt 8] trying a = 477422510912sampling words of length L = 2000,
 max_samples = 120000,  stable_hits = 8
no stabilized gcd from loops in this attempt (try another a).

[attempt 9] trying a = 378381310618sampling words of length L = 2000,
 max_samples = 120000,  stable_hits = 8
no stabilized gcd from loops in this attempt (try another a).

[attempt 10] trying a = 747483761123sampling words of length L = 2000,
 max_samples = 120000,  stable_hits = 8
no stabilized gcd from loops in this attempt (try another a).

[attempt 11] trying a = 1001492753655sampling words of length L = 2000,
 max_samples = 120000,  stable_hits = 8
no stabilized gcd from loops in this attempt (try another a).

[attempt 12] trying a = 394688788349sampling words of length L = 2000,
 max_samples = 120000, stable_hits = 8
no stabilized gcd from loops in this attempt (try another a).

[attempt 13] trying a = 478211699347sampling words of length L = 2000,
 max_samples = 120000, stable_hits = 8
no stabilized gcd from loops in this attempt (try another a).

[attempt 14] trying a = 365250373964sampling words of length L = 2000,
 max_samples = 120000, stable_hits = 8
no stabilized gcd from loops in this attempt (try another a).

[attempt 15] trying a = 893381186972sampling words of length L = 2000,
 max_samples = 120000, stable_hits = 8
no stabilized gcd from loops in this attempt (try another a).

[attempt 16] trying a = 750796458253sampling words of length L = 2000, max_samples = 120000,
 stable_hits = 8
[collision #  1]  D_min = 3966231680600   AGGRESSIVE ONE-COLLISION FACTOR: 1048589 * 1048601

FINAL: 1099551473989 = 1048589 * 1048601
TOTAL TIME: 3132.641 s  (0:52:13)
```

# 9 扩散原语的最简 RC 网络实现

最后，我们简要介绍一种在连续时间 下实现扩散原语的可能物理方式，并说明为何以较小的时间步长 $\Delta t$ 进行采样可以近似我们模型中使用的离散

算子。
固定一个顶点集为 $V=\{1,\dots,r\}$ 的有限无向加权图，并设其电导对称$g_{ij}=g_{ji}\geq 0$ （$g_{ij}=0$ 若不存在边）。将一个电容器 $C>0$ 连接到地，并连接到每个顶点 $i$；用一个电导为 $g_{ij}=1/R_{ij}$ 的电阻器连接顶点 $i$ 和 $j$。设 $V_i(t)$ 为节点 $i$ 在时间 $t$的电压，并令

$$V(t)=(V_1(t),\dots,V_r(t))^{\mathsf{T}}.$$

By 根据基尔霍夫电流定律，电容器电流等于电阻性净流出的相反数 :

$$C\,\frac{d}{dt}V_i(t)=-\sum_{j=1}^{r} g_{ij}(V_i(t)-V_j(t)).$$

令 $L$ 为相应的加权图拉普拉斯算子，即

$$L_{ii}=\sum_{j\neq i} g_{ij},\qquad L_{ij}=-g_{ij}\quad (i\neq j).$$

于是，网络动力学满足以下线性常微分方程

$$C\,\frac{d}{dt}V(t)=-L\,V(t),\qquad \text{hence}\qquad V(t)=\exp\!\left(-\frac{t}{C}L\right)V(0). \tag{9.1}$$

因此，该 $RC$ 网络实现了图上的连续时间热流。
在本文的抽象模型中，一次扩散步是一个固定的线性算子

$$W:\mathbb{R}^r\to\mathbb{R}^r$$

反复应用。连续时间实现产生的则是半群 $t\mapsto\exp(-(t/C)L)$，而一种自然的离散时间基本操作可通过按固定时间间隔 $\Delta t>0$ 采样得到：

$$V^{(n+1)}=V((n+1)\Delta t)=\exp\!\left(-\frac{\Delta t}{C}L\right)V(n\Delta t)=W_{\Delta t}\,V^{(n)}, \tag{9.2}$$

其中

$$W_{\Delta t}=\exp\!\left(-\frac{\Delta t}{C}L\right).$$

这是通过仅在时刻 0、 $\Delta t$、 $2\Delta t$、.....观察连续电路而得到的精确离散时间演化。

当 $\Delta t$ 足够小时，矩阵指数可作一阶展开：

$$\exp\!\left(-\frac{\Delta t}{C}L\right)=I-\frac{\Delta t}{C}L+O(\Delta t^2),\qquad \Delta t\to 0, \tag{9.3}$$

这里的误差是按元素或按算子范数理解的。因此，单个采样步满足

$$V^{(n+1)}-V^{(n)}=-\frac{\Delta t}{C}L\,V^{(n)}+O(\Delta t^2).$$

换言之：在极短的时间间隔内，每个节点电压都会发生微小变化，其变化量与拉普拉斯算子成正比（即该节点与其相邻节点之间的加权差分）；这正是扩散的局部平均机制。

等价地，如果指定一个形式如下的目标离散时间平均算子

$$P=I-\gamma L$$

其中尺度为 $\gamma > 0$，那么选择

$$\gamma = \frac{\Delta t}{C}$$

使电路的采样步满足

$$W_{\Delta t} = \exp\!\left(-\frac{\Delta t}{C} L\right) = P + O(\Delta t^2).$$

因此，通过取较小的 $\Delta t$ （并相应增加采样步数，以达到固定的物理混合时间），连续时间 $RC$ 扩散可近似我们分析中使用的离散扩散过程。

### 实现

在物理实现中，电路持续运行，而计算中所计的一个“扩散步”对应于以下任一操作：

- 每隔 $\Delta t$ 秒对节点电压进行采样（得到精确映射 $W_{\Delta t}$），或
- 在 $\Delta t$ 较小的工作状态下运行，使得每次采样都是一次小幅的局部平均更新，从而近似一个指定的离散算子。

这为扩散原语提供了一个具体的诠释，即硬件支持的局部弛豫步骤。

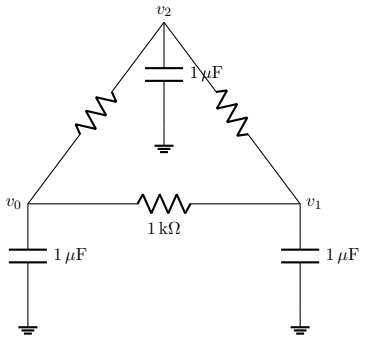


图 7：在 $N = 21$ 的凯莱图上实现扩散的 RC 网络。取 $N = 21$并选择 $a = 2$。令 $M = \lfloor \log_2 21 \rfloor + 1 = 5$，设 $b \equiv a^{2^M} \equiv 2^{32} \pmod{21}$。由于 $\mathrm{ord}_{21}(2) = 6$，我们有 $2^{32} \equiv 2^2 \equiv 4 \pmod{21}$，因此 $b = 4$ 且 $\mathrm{ord}_{21}(4) = 3$。因此 $G = \langle 4 \rangle = \{1, 4, 16\}$ 有三个顶点，生成元 $b^{\pm 2^t}$ 化简为 $\mathbb{Z}/3\mathbb{Z}$上的步骤 $\pm 1$，因此该凯莱图是一个 3-环。

## 致谢

Carlos A. Cadavid 衷心感谢 EAFIT大学（哥伦比亚）为项目《扩散过程在健康与计算领域的重要性研究及应用》（项目代码 11740052022）提供的经费支持。Jay Jorgenson 感谢 PSC-CUNY奖项68462-00 56 的资助，该奖项由专业人员大会和纽约市立大学共同资助。Juan D. Vélez 衷心感谢哥伦比亚国立大学在本研究期间给予的支持。

# 参考文献

[AKS04] M. Agrawal、N. Kayal 和 N. Saxena，PRIMES 属于 P，《数学年鉴》（第2辑）160（2004），781–793。[Ba79] L. Babai，《凯莱图的谱》，《组合理论杂志》B辑27（1979），第2期，180–189。[BS96] E. Bach 和 J. Shallit，《算法数论》第1卷：高效算法，麻省理工学院出版社，1996。[Be07] D. J. Bernstein、H. W. Lenstra 和 J. Pila，通过分解为互素数检测完全幂，《数学计算》76（2007），385–388。[CBK22] D. Chicayban Bastos 和 L. A. Kowada，Pollard rho 算法的一个量子版本，其中 Shor 算法是一个特例，载于：《计算与组合数学》，《计算机科学讲义》13595，施普林格，查姆，2022，212–219。[CHJSV23] C. A. Cadavid、P. Hoyos、Jay Jorgenson、L. Smajlović 和 J. D. Vélez，正则图上的离散扩散型方程及其应用，《差分方程应用》29（2023），第4期，455–488。[Ch97] F. R. K. Chung，《谱图论》，美国数学会，1997。[CP05] R. Crandall 和 C. Pomerance，《素数：计算视角》，第2版，施普林格，2005。[CR62] C. W. Curtis 和 I. Reiner，《有限群与结合代数表示论》，威利出版社，1962；重印本：威利经典丛书，1988。[DSS24] J. Ding、G. Spallitta 和 R. Sebastiani，通过模局部结构嵌入和量子退火实现有效的素因数分解，《科学报告》14（2024），文章编号3518。doi：10.1038/s41598-024-53708-7。[EJ96] A. K. Ekert 和 R. Jozsa，量子计算与 Shor 因数分解算法，《现代物理评论》68（1996），第3期，733–753。[HW08] G. H. Hardy 和 E. M. Wright，《数论导论》，第6版，牛津大学出版社，2008。[Hh25] M. Hhan，一种求一般下界的新方法：经典／量子最小描述长度、量子因数分解及其他，载于：密码学进展——EUROCRYPT 2025。第七部分，《计算机科学讲义》15607，施普林格，查姆，2025，345–374。[KM12] J. Kaczorowski 和 G. Molteni，和的极值 $\sum_{r=1}^{\tau} e(a2^r/q)$，《数论杂志》132（2012），2595–2603。[Kn97] D. E. Knuth，《计算机程序设计艺术》第2卷：半数值算法，第3版，艾迪生-韦斯利，1997。[KSK21] A. H. Karamlou、W. A. Simon、A. Katabarwa、T. L. Scholten、B. Peropadre、Y. Cao 等，分析超导量子处理器上变分量子因式分解的性能，《npj量子信息》7（2021），文章编号156。DOI：10.1038/s41534-021-00478-z。[KSV99] A. Yu. Kitaev、A. H. Shen 和 M. N. Vyalyi，《经典与量子计算》，《数学研究生教材》47，美国数学会，普罗维登斯，罗得岛州，2002年（由 L. J. Senechal 从1999年的俄文原版译出）。

[Leh00] D. N. Lehmer，《某些欧拉函数和的渐近求值》，美国数学杂志 22 (1900)，293–335。[LPW09] D. A. Levin、Y. Peres 和 E. L. Wilmer，《马尔可夫链与混合时间》，美国数学会，2009。[Me96] A. J. Menezes、P. C. van Oorschot 和 S. A. Vanstone，《应用密码学手册》，CRC出版社，1996。[NC10] M. A. Nielsen 和 I. L. Chuang，《量子计算与量子信息》（十周年纪念版），剑桥大学出版社，2010。[Ni18] B. Nica，《谱图论简明导论》，EMS数学教材，欧洲数学会，2018。[Nym72] J. E. Nymann，关于 $k$ 正整数互素的概率，《数论杂志》4 (1972)，469–473。[Ra80] M. O. Rabin，用于测试素数性的概率算法，《数论杂志》12 (1980)，第1期，128–138。[Ra24] S. Ragavan 和 V. Vaikuntanathan，空间高效且抗噪声的量子因数分解，载于：《密码学进展——CRYPTO 2024》第六部分，计算机科学讲义 14925，施普林格，查姆，2024，107–140。[Re25] O. Regev，一种高效的量子因数分解算法，《美国计算机学会杂志》72 (2025)，第1期，文章10，13页。doi: 10.1145/3708471。[Sh94] P. W. Shor，量子计算算法：离散对数与因数分解，载于：《第35届计算机科学基础年会论文集》（计算机科学基础年会），电气电子工程师学会，1994，124–134。[Sh97] P. W. Shor，在量子计算机上进行素因数分解和离散对数计算的多项式时间算法，《工业与应用数学学会计算杂志》26 (1997)，第5期，1484–1509。[Va19] J. Vandehey，Korobov型指数和的差分方法，《分析与数学杂志》138 (2019)，405–439。[XQLM23] L. Xiao、D. Qiu、L. Luo 和 P. Mateus，分布式Shor算法，《量子信息与计算》23 (2023)，第1–2期，27–44。[Za13] P. Zawadzki，量子因数分解效能的闭式公式，《量子信息处理》12 (2013)，97–108。

## 作者信息

Carlos A. Cadavid 数学系，EAFIT大学，麦德林，哥伦比亚
ccadavid@eafit.edu.co

Paulina Hoyos 数学系，德克萨斯大学奥斯汀分校，美国
paulinah@utexas.edu

Jay Jorgenson 纽约市立学院数学系，美国
jjorgenson@mindspring.com

Lejla Smajlović 萨拉热窝大学数学系，波斯尼亚和黑塞哥维那
lejlas@pmf.unsa.ba

Juan D. Vélez 哥伦比亚国立大学数学系，麦德林，哥伦比亚jdvelez@unal.edu.co