

基于四方邻域路径映射的二维元胞自动机 高质量伪随机数发生方法

刘 星

北京邮电大学数学与科学学院, 北京

收稿日期: 2025 年 12 月 22 日; 录用日期: 2026 年 2 月 2 日; 发布日期: 2026 年 2 月 12 日

摘 要

针对硬件伪随机数发生器在蒙特卡洛仿真、统计抽样及片上系统测试等非对抗性应用场景中的应用需求, 研究一种兼顾长周期、统计随机性、多路输出低相关性 with 实现复杂度的二维元胞自动机伪随机数发生方法。基于四方邻域 (半径 1, 含中心) 的二维元胞自动机模型, 提出一种路径映射构造框架, 将 $R \times C$ 阵列沿行映射、列映射及其蛇形映射线性化为长度 $N=RC$ 的一维序列, 并在一维空间中利用 Cattell-Muzio 方法合成与给定本原多项式对应的混合元胞自动机 (规则 90/150), 再回映射至二维拓扑, 从而在二维结构上显式继承最大周期与线性复杂度等可分析性质。在 64×64 阵列、周期边界及单流 10^6 bit 的统一仿真平台下, 所提出的路径型二维元胞自动机在 NIST SP 800-22 随机性测试套件的多项核心子测试中均通过; 在 $K=64$ 路并行输出场景下, 蛇形路径映射在零时延多流相关矩阵的非对角相关系数上显著低于多种典型二维更新核。结果表明, 该方法在随机性质量、多流去相关能力与逻辑复杂度之间实现了较为均衡的折中, 适用于通用硬件伪随机激励与片上系统测试等非对抗性应用场景。

关键词

元胞自动机, 伪随机数发生器, 路径映射, 多流伪随机序列, NIST SP 800-22

A Four-Neighborhood Path-Mapping-Based Two-Dimensional Cellular Automaton Method for High-Quality Pseudorandom Number Generation

Xing Liu

School of Mathematics and Statistics, Beijing University of Posts and Telecommunications, Beijing

Received: December 22, 2025; accepted: February 2, 2026; published: February 12, 2026

Abstract

High-quality pseudorandom number generators are fundamental to Monte Carlo simulation, statistical sampling, and non-adversarial on-chip testing applications. To address the limitations of one-dimensional structures in multi-stream and two-dimensional array scenarios, a path-mapping-based two-dimensional cellular automaton pseudorandom number generation method with a four-neighbor neighborhood is presented. The proposed approach linearizes an $R \times C$ array into a one-dimensional sequence of length $N=RC$ through reversible row/column and snake-path mappings, synthesizes a hybrid cellular automaton based on rules 90/150 using the Cattell-Muzio method, and maps it back to the two-dimensional topology, thereby explicitly inheriting the maximal period and linear complexity associated with primitive polynomials. Simulation results obtained on a 64×64 array with periodic boundaries and single-stream outputs of 10^6 bits demonstrate that the proposed method passes all selected core subtests of the NIST SP 800-22 test suite. In multi-stream evaluations with $K=64$ parallel outputs, snake-path mappings exhibit significantly reduced inter-stream correlation compared with several representative two-dimensional cellular automaton kernels. These results indicate that the proposed method achieves a favorable trade-off among theoretical analyzability, statistical randomness quality, multi-stream decorrelation capability, and logic complexity, making it suitable for general-purpose hardware pseudorandom excitation and non-adversarial multi-stream applications.

Keywords

Cellular Automata, Pseudorandom Number Generator, Path Mapping, Multistream Pseudorandom Sequence, NIST SP 800-22

Copyright © 2026 by author(s) and Hans Publishers Inc.

This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

1. 研究现状与背景

1.1. 高质量伪随机序列的需求与评测方法

高质量伪随机序列是现代信息系统中的基础资源，广泛服务于蒙特卡洛仿真、统计抽样以及硬件伪随机数发生器等场景。不同应用的最终指标各不相同，但对序列本身的核心要求高度一致：一是具有足够长的周期与状态空间，以避免短周期导致的模式重复和统计偏差；二是满足近似独立同分布特性，即在单比特频数、局部块频数、游程结构、谱特性、线性复杂度等方面均接近真正随机序列；三是能够在多路并行输出时保持序列之间的低相关性，避免多条输出相互“预测”，从而保证有效样本维度。为定量评估伪随机序列的“随机性质量”，已有大量标准化测试工具被提出。典型如 NIST SP 800-22 随机性测试套件，通过单比特频数 (Frequency)、区块频数 (Block Frequency)、游程 (Runs)、前/后向累加和 (Cumulative Sums, Forward/Backward)、近似熵 (Approximate Entropy)、矩阵秩 (Rank) 与频谱 (FFT) 等十余项统计检验，从不同尺度刻画序列的均匀性、独立性和线性依赖结构；Diehard、Dieharder 与 TestU01 等测试集则从更细粒度的统计角度对伪随机序列施加更高强度的压力测试。对于以硬件伪随机数发生器为代表的工程应用而言，现有设计流程普遍遵循“先保证序列的统计随机性质量，再在此基础上优化结构复杂度和能耗”的路径：只有在通过足够严格的随机性测试前提下，后续关于实现代价和并行伸缩性的分析才具有意义。

1.2. 元胞自动机伪随机序列研究进展

元胞自动机 (Cellular Automata, CA) 以时间、空间和状态的离散性为特征，通过局部规则并行更新全局状态，在硬件层面天然具备互连局部、结构规整和高并行度等优势。早期研究表明，一维线性混合元胞自动机在适当规则配置下可以获得与 LFSR 等价的周期性质，并可作为 LFSR 的替代结构用于伪随机数与伪随机测试图样的生成 [1] [2]。从随机性质量角度看，一维混合 CA 通过合理选择规则组合，同样能够通过 NIST、Diehard 等统计测试，其生成序列在频数、游程、线性复杂度等方面接近真正随机 [3]。

在此基础上,研究者进一步将 CA 拓展到二维网格:直接在 $R \times C$ 阵列上定义邻域和更新规则,以期利用平面扩散获得更高的“混合效率”和并行输出能力。Serra 等人提出了基于二维线性元胞自动机的随机模式生成框架, Tomassini 等系统考察了二维 CA 生成的随机数在多种统计测试下的表现,表明合适规则配置下的二维 CA 可以产生质量可比甚至优于一维结构的伪随机序列 [4]。在这一类工作中,随机性测试结果(例如通过/未通过的 NIST 子项、p-value 分布、Diehard/TestU01 统计量)是度量结构优劣的首要指标。

在二维线性元胞自动机更新核方面,已有工作给出了多种具有代表性的结构。Torres-Huitzil 等在文献中系统比较了一系列二维 CA 伪随机数发生器 [5]。其中两种被广泛采用的基线结构分别是:

(1) Moore 八邻域线性更新核 (moore9): 采用 Moore 八邻域(不含中心),每个元胞从上下左右及四个对角共 8 个邻居收集状态并统一异或。该结构连通度高、扩散速度快,能够在较少步数内打散初始模式,对 NIST SP 800-22 随机性测试套件表现良好(包括单比特频数、区块频数、游程、累加和、近似熵、矩阵秩等子项),因而被视为二维 CA 伪随机数发生器的“强基线”。但在硬件层面,每比特需要约 7 个两输入异或门,逻辑复杂度和连线复杂度都较高 [5]。

(2) 去中心非对称四邻域更新核 (npca4): 仅取 SW, W, NE, E 四个方向的邻居做线性异或,相较于 Moore 八邻域核刻意降低了垂直耦合度和异或门个数,在扩散能力与硬件代价之间取得一定折中。已有实验表明,在合适的阵列规模和初值选择下,该结构同样可以顺利通过 NIST SP 800-22 中的多数甚至全部子测试,显示出良好的随机性质量 [5]。

Guan 等人在文献中提出的水平-对角非对称二维更新核 (asym2d) 则代表了另一类思路:在水平方向采用类似 rule-150 的核 $L \oplus C \oplus R$,并额外引入对角 UR, DL 两个方向的输入,形成具有明显方向偏置的非对称二维线性更新核 [6]。相关实验表明,asym2d 在多项 NIST 子测试中表现良好,但在矩阵秩测试上存在一定劣势,提示其内部仍存在较强的线性依赖结构 [5] [6]。

国内研究方面,朱保平等提出了二维可控元胞自动机伪随机序列发生方法,通过可控参数调节更新规则以改善序列周期性与统计性质,并利用 NIST / Diehard 等工具验证随机性 [7]。杨勇等构造了基于 $2 \times n$ 元胞自动机结构的高质量伪随机数发生器,从结构约束角度折中二维扩散能力与实现复杂度 [8]。孙凌宇等系统比较了基本与混合元胞自动机伪随机数发生特性,同样以随机性测试结果作为结构选择的重要依据 [9]。近年来,围绕多流并行输出和高通量伪随机数发生,亦有一系列基于规则阵列、支持多路独立输出的二维元胞自动机结构被提出,在 NIST / TestU01 等测试套件下展示出良好的随机性与并行性 [10] [11] [12]。

总体来看,已有一维与二维元胞自动机研究的评价核心,仍然是生成序列在标准测试套件下的随机性质量:通过多少子测试、p-value 是否均匀、是否存在明显的线性依赖或周期缺陷。在这一点上,二维 CA 已经给出了大量有力验证,但在多流相关性定量分析与结构复杂度系统比较方面仍有进一步改进空间。

1.3. 现有二维 CA 伪随机数发生方法的不足与本文工作

尽管现有二维元胞自动机伪随机数发生器在 NIST / Diehard / TestU01 等统计测试套件下普遍表现出良好的随机性质量,但仍存在若干共性不足:

- 多邻域线性异或聚合导致每比特所需异或门数量偏高（典型值约为 3-7 个两输入异或门/比特），在硬件实现时逻辑复杂度较大；
- 邻域往往涉及对角和相对较远的连线，互连不够“局部”且方向性偏强，不利于在大规模二维阵列上规整布局；
- 相当一部分二维更新核更多基于经验结构设计，缺乏与一维本原多项式一一对应的合成理论，难以在设计阶段直接保证最大周期和线性复杂度，也不便于系统地控制周期与初始状态空间；
- 现有工作多以内生序列的单流随机性为主要评价指标，对多路并行输出流之间的相关性以及在给定状态位约束下的多流扩展能力关注相对不足。

基于上述观察，本文的目标是：在保持高随机性质量这一前提下，构造一类同时具备可分析周期性质、多流低相关性和较低结构复杂度的二维元胞自动机伪随机数发生方法。具体而言，本文在继承一维线性混合元胞自动机（规则 90/150）与本原多项式一一对应的可综合化优势 [1] [2]。在此基础上，引入四方邻域 + 受限垂直耦合 + 路径映射的二维结构设计框架：在二维拓扑上仅保留“四方邻域 + 单向垂直耦合”，以提高互连局部性并控制每比特逻辑复杂度（XOR/bit）；通过行映射、列映射以及行/列蛇形映射（分别对应 row、col、row_snake、col_snake）将 $R \times C$ 阵列线性化，应用 Cattell-Muzio 算法合成对应本原多项式的一维混合元胞自动机，从而在保持严格可分析周期性质的同时，获得多路并行输出结构。后文将从 NIST SP 800-22 随机性测试、多流零时延相关性以及每比特逻辑复杂度等指标出发，系统比较本文结构与典型二维更新核 moore9、npca4、asym2d 的综合表现。

2. 方法与原理

2.1. 邻域与线性规则

本文采用四方邻域（半径 1）：每个元胞的下一状态由其自身及其上/下/左/右四个邻居共同决定（共 5 元胞），如图 1 所示。为对比，moore9 基线使用 Moore 八邻域（不含中心）的线性 XOR 聚合 [5]。

在一维元胞自动机中，规则 90/150 是两种基本线性规则；以 0/1 表示规则 90/150 并形成混合元胞自动机。Bardell 等在伪随机测试图样生成背景下讨论了此类结构的别名与实现形态 [13]。Cattell-Muzio 给出从给定不可约多项式综合对应一维混合元胞自动机的算法 [1]。通过适当布置规则 150/90 的分布，可令元胞自动机的特征多项式为本原多项式、周期达 $2^n - 1$ 。

2.2. 二维到一维的路径映射思想

直接在 $R \times C$ 阵列上推导特征多项式往往规模庞大。为此，我们先将二维状态按特定可逆路径映射为长度 $N=RC$ 的一维序列，在该序列上用 Cattell-Muzio 合成得到匹配本原多项式的混合元胞自动机（规则 90/150），再将规则位置回映射至二维拓扑。设 $\pi(i, j) \in \{1, \dots, N\}$ 为路径双

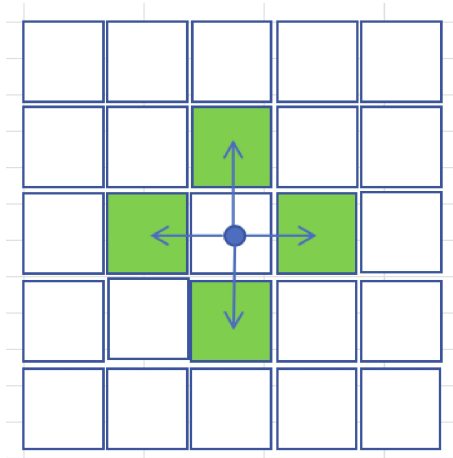


Figure 1. Illustration of the four-neighbor neighborhood (radius 1)

图 1. 四方邻域（半径 1）示意图

射 (i 为行、 j 为列), 四种路径定义如下:

$$\text{row} : k = \pi_{\text{row}}(i, j) = (i - 1)C + j; \quad (1)$$

$$\text{col} : k = \pi_{\text{col}}(i, j) = (j - 1)R + i; \quad (2)$$

$$\text{row_snake} : k = \pi_{\text{rs}}(i, j) = \begin{cases} (i - 1)C + j, & i \text{ 为奇数,} \\ (i - 1)C + (C - j + 1), & i \text{ 为偶数,} \end{cases} \quad (3)$$

$$\text{col_snake} : k = \pi_{\text{cs}}(i, j) = \begin{cases} (j - 1)R + i, & j \text{ 为奇数,} \\ jR - i + 1, & j \text{ 为偶数.} \end{cases} \quad (4)$$

上述四种 π 均为双射: 它们将二维阵列线性化为一维序列 $y \in \{0, 1\}^N$, 并保持逐元可逆回映射。直观地:

- row: 逐行、每行从左到右, 行与行之间顺序相接;
- col: 逐列、每列从上到下, 列与列之间顺序相接;
- row_snake: 奇数行左 \rightarrow 右, 偶数行右 \rightarrow 左 (行内反向);
- col_snake: 奇数列上 \downarrow 下, 偶数列下 \uparrow 上 (列内反向)。

在一维上, 混合元胞自动机的线性更新为

$$y^{(t+1)} = A(d)y^{(t)} \pmod{2}, \quad (5)$$

其中

$$A(d) = S_{-1} + \text{Diag}(d) + S_{+1}, \quad (6)$$

这里 $d \in \{0, 1\}^N$ 为 90/150 规则向量, $S_{\pm 1}$ 为左右移位矩阵; 周期边界时在角上补 1:

$$A_{1N} = A_{N1} = 1. \tag{7}$$

为便于复现, $S_{\pm 1}$ 的元素定义为

$$(S_{+1})_{k,k+1} = 1, \quad (S_{-1})_{k,k-1} = 1, \quad 2 \leq k \leq N - 1, \tag{8}$$

$$\text{周期边界: } (S_{+1})_{N,1} = 1, \quad (S_{-1})_{1,N} = 1. \tag{9}$$

用路径置换矩阵 Π 表示线性化, 二维全局更新矩阵可写为

$$G = \Pi^{-1}A(d)\Pi. \tag{10}$$

由于相似变换保持特征多项式不变, 只要 $A(d)$ 由 Cattell-Muzio 合成匹配本原多项式, 则回映射后的 G 也保持最大周期 (除全零态)。

蛇形路径的意义 蛇形路径 `row_snake` 和 `col_snake` 通过在相邻行 (或列) 内反向遍历, 引入交错的局部反转块, 使一维相邻索引映射到二维时既可能对应左右/上下, 也可能对应对角近邻, 从而在导出位流与多路输出分配时削弱单一方向的短程相关 (第 3.3 节的多流相关指标亦验证了这一点)。

受限垂直邻域 为降低耦合复杂度与布线代价, 我们采用受限垂直邻域: 每个元胞在垂直方向仅从“上”或“下”取一个输入 (而非上下同时取值)。以行作为块划分, 受限垂直邻域令二维更新矩阵在上下耦合项上仅保留一个块带, 从而呈现块上 (或下) 三角结构, 便于代数分析与实现 [14]。在门级上, 这使每比特平均约需 1.5 个两输入异或门 (规则 90/150 比例近半), 与表 2 的实现复杂度代理一致。需要说明的是, 本文的受限垂直邻域是对由相似变换得到的二维连线形态的几何刻画, 并不在代数上引入额外的线性项, 因此式 (10) 所对应的一维最大周期性质仍然保持。

2.3. 以列蛇形映射为例的完整构造流程

记号与设定 在二元域 $= \{0, 1\}$ 上工作, 所有运算取模 2。令 $R, C \in \mathbb{N}$, 总元胞数 $N=RC$ 。记时刻 t 的二维状态矩阵为 $X^{(t)} = (x_{i,j}^{(t)}) \in \{0, 1\}^{R \times C}$ 。离线合成长度为 N 的一维混合元胞自动机系数向量 $d = (d_1, \dots, d_N) \in \{0, 1\}^N$, 满足最大周期条件。

蛇形列向量化 定义双射 $\pi : (i, j) \mapsto k$, 按“奇列顺序、偶列倒序”的蛇形规则将二维展开为一维 $y^{(t)} \in \{0, 1\}^N$:

$$k = \pi(i, j) = \begin{cases} (i - 1) + R(j - 1) + 1, & j \text{ 为奇数,} \\ Rj - (i - 1), & j \text{ 为偶数,} \end{cases} \quad y_{\pi(i,j)}^{(t)} = x_{i,j}^{(t)}.$$

一维更新矩阵与演化 设三对角矩阵 $A(d) \in \{0, 1\}^{N \times N}$, 主对角为 d_1, \dots, d_N , 上下副对角为 1 (开边界)。周期边界时令 $A_{1N}=A_{N1}=1$ 。一步演化为

$$y^{(t+1)} = A(d) y^{(t)} \pmod{2}, \quad (11)$$

再由 π^{-1} 回写二维: $x_{i,j}^{(t+1)} = y_{\pi(i,j)}^{(t+1)}$ 。

逐元公式 对 $k=1, \dots, N$ 有

$$y_k^{(t+1)} \equiv d_k y_k^{(t)} \mathbf{1}_{[k>1]} y_{k-1}^{(t)} \mathbf{1}_{[k<N]} y_{k+1}^{(t)} \pmod{2}, \quad (12)$$

周期边界时取 $k \pm 1$ 为模 N 的邻居。

算法 1 列蛇形映射 (col_snake): 二维阵列到一维元胞自动机构造与更新

- 1: **输入:** $R, C, \mathbf{X}^{(0)}, \mathbf{d} \in \{0, 1\}^N$
 - 2: **当** 需要产生序列
 - 3: 按 π 将 $\mathbf{X}^{(t)}$ 蛇形列向量化为 $\mathbf{y}^{(t)}$
 - 4: $\mathbf{y}^{(t+1)} \leftarrow A(\mathbf{d}) \mathbf{y}^{(t)} \pmod{2}$ 或按逐元公式更新
 - 5: 由 π^{-1} 回写 $\mathbf{X}^{(t+1)}$
 - 6: $t \leftarrow t + 1$
 - 7: **结束**
-

3. 实验与结果

3.1. 实验平台与参数设置

为客观比较不同二维元胞自动机伪随机数发生方法的随机性质量, 本文在统一的软件和参数设置下进行评测。实验平台为 Python 3 环境, 对于每种结构, 从不同初始状态生成 100 条伪随机比特序列, 每条序列长度为 10^6 bit, 作为 NIST 测试输入。

NIST SP 800-22 提供了 15 类统计子测试 [15]。本文完整运行该测试集, 并重点关注以下 8 个常用子测试: 单比特频数 (Frequency)、区块频数 (Block Frequency)、游程 (Runs)、前/后向累加和 (Cumulative Sums, Forward/Backward)、近似熵 (Approximate Entropy)、矩阵秩 (Rank) 与频谱 (FFT)。显著性水平统一取 $\alpha = 0.01$ 。按照 NIST 官方建议, 当样本数为 $N=100$ 时, 除随机游程类测试外, 各子测试的通过比例应落在约 $[0.96, 1.00]$ 的区间内; 同时还需检查每个子测试的“ p 值的 p 值”是否过于接近 0 或 1, 以避免出现明显的非均匀性 [15]。

在随机性测试之外, 本文还给出了两类与工程应用相关的指标: 一是多流输出场景下的跨序列相关性 (例如面向多流并行仿真或多链激励时的零时延相关矩阵的最大/平均非对角相关系数), 二是在统一逻辑建模下估算的每比特两输入异或门数 (XOR/bit) 以及状态位/输出流数目。这些指标不直接进入 NIST 统计判据, 但反映了伪随机数发生器在多流独立性和硬件实现代价上的差异。

3.2. 对比方法

本文在相同阵列规模 $R=C=64$ 、周期边界条件下，对比 7 种二维元胞自动机伪随机数发生方法：

- **Moore 八邻域线性核 (moore9)**：每个元胞从 Moore 八邻域（不含中心）的 8 个邻居收集状态并统一异或。该结构扩散速度快，是二维线性 CA 伪随机数发生器中的强基线之一 [5]。
- **去中心非对称四邻域核 (npca4)**：仅取 SW, W, NE, E 四个方向的邻居做线性异或，相较 moore9 降低了垂直耦合度和异或门数量，在扩散能力与硬件代价之间取得折中 [5]。
- **水平 - 对角非对称二维核 (asym2d)**：水平方向采用类似 rule-150 的 $L \oplus C \oplus R$ 核，并额外引入对角 UR, DL 输入，形成具有方向偏置的二维线性 CA 结构 [6]。
- **行/列路径型二维 CA (row/col)**：先将 $R \times C$ 阵列按行优先 (row) 或列优先 (col) 映射为长度 $N=RC$ 的一维序列，再基于 Cattell-Muzio 方法合成与给定本原多项式对应的一维混合 CA (规则 90/150)，最后回映射到二维拓扑。
- **蛇形路径型二维 CA (row_snake/col_snake)**：在行/列映射基础上，引入奇偶行（或列）反向遍历的蛇形路径，使一维相邻索引对应到二维时既可能是水平/垂直邻居，也可能是对角近邻，以削弱单一方向的短程相关。

对于四种路径型结构，更新矩阵通过 Cattell-Muzio 一维合成算法显式匹配给定本原多项式，其特征多项式与一维结构一致，从而保证除了全零态之外的最大周期 2^N-1 与可分析的线性复杂度。二维几何上仅保留四方邻域与受限垂直耦合，使得平均 XOR/bit 约为 1.5，状态位/输出流为 $R \times C$ ，便于在片上作为通用高质量伪随机数发生器平铺扩展。

3.3. 随机性测试结果与分析

表 1 汇总了 7 种方法在 NIST SP 800-22 中 8 个核心子测试上的 p 值统计结果（对应 NIST 报告中“ p 值的 p 值”），每个子测试的样本数均为 100。所有方法在这些子测试中的通过比例均不低于 96/100，且 p 值范围大致介于 0.04 到 0.98 之间。

Table 1. Comparison of p -values of different two-dimensional cellular automaton methods in NIST SP 800-22 subtests

表 1. 不同二维元胞自动机方法在 NIST SP 800-22 子测试上的 p 值比较

方法	单比特频数	区块频数	游程	累加和 (前向)	累加和 (后向)	近似熵	矩阵秩	FFT
Moore 八邻域核 (moore9)	0.1373	0.9241	0.7792	0.9241	0.8832	0.3505	0.4012	0.4750
去中心非对称四邻域核 (npca4)	0.7598	0.8165	0.4750	0.2023	0.9357	0.9357	0.1917	0.2023
水平 - 对角非对称二维核 (asym2d)	0.1373	0.2757	0.9717	0.7598	0.2133	0.0401	0.1538	0.5749
行映射 (row)	0.4012	0.4012	0.5341	0.9879	0.2133	0.6163	0.3041	0.1538
列映射 (col)	0.4559	0.3505	0.2368	0.2023	0.6371	0.8677	0.3345	0.6371
行蛇形映射 (row_snake)	0.5749	0.4750	0.1626	0.5544	0.4944	0.4373	0.8677	0.4190
列蛇形映射 (col_snake)	0.4559	0.9463	0.1453	0.7598	0.7792	0.4373	0.1719	0.5544

从表 1 可以看出，三种二维 CA 基线 (moore9、npca4、asym2d) 和本文提出的四种路径型二维 CA 在 8 个核心子测试上的表现总体相近：

- 对于 npca4, 各子测试的通过比例均不低于 98/100, p 值分布较为均匀;
- asym2d 在近似熵子测试上的 p 值约为 0.0401, 对应通过比例为 96/100, 是 8 个子测试中最接近显著性边界的一项, 但仍满足 NIST 建议的接受区间;
- 四种路径型结构中, row 在 8 个子测试中的最小通过比例达到 99/100, col、row_snake 和 col_snake 的最小通过比例也都在 97/100 左右, 且未出现 p 值过于贴近 0 或 1 的异常情况。

总体而言, 在核心子测试上, 本文方法与文献中的典型二维 CA 基线处于同一随机性水平, 没有观察到系统性劣化。

在模板及其他子测试方面, 每种方法都运行了包括 NonOverlappingTemplate、OverlappingTemplate、Serial、线性复杂度 (Linear Complexity) 等在内的完整 NIST 子测试。以 NonOverlappingTemplate 为例, 每个发生器接受了 148 个模板的检验:

- npca4、asym2d 与 col_snake 在全部 148 个模板上的通过比例均不低于 96/100;
- moore9、row、col 和 row_snake 各有 1 个模板的通过比例为 95/100, 略低于 NIST 建议区间下界并被工具标记为 “*”, 其余模板均在 96/100 以上;

考虑到 7 种方法共执行了上千个模板子测试, 出现极少数 95/100 的情况可以视作统计波动, 而非结构性的随机性缺陷。其它如 OverlappingTemplate、Universal、Serial、Linear Complexity 等子测试的 p 值也都落在合理区间内, 未出现集中失效现象。

综合以上结果可以得出结论: 在 NIST SP 800-22 完整测试集中, 本文提出的四种路径型二维元胞自动机伪随机数发生方法在各项统计随机性指标上均与文献中的二维 CA 基线 (moore9、npca4、asym2d) 相当, 未观察到显著劣化或系统性薄弱项。这为后续讨论其在多流输出和硬件代价方面的优势奠定了前提, 即在保持 “高质量伪随机数” 这一基础要求的前提下, 再比较多流相关性和 XOR/bit 等工程指标的优劣。

3.4. 多流相关性与实现复杂度

多流相关性 (并行输出场景)。 在 $K=64$ 路并行输出、激励长度 $T \approx 3 \times 10^3$ 的设置下, 我们计算了不同方法的零时延多流相关矩阵, 并从中提取非对角元素的最大/平均 $|\rho|$ 。图 2 显示: 路径型二维元胞自动机整体上具有更低的多流相关性, 其中蛇形路径 (行蛇形映射、列蛇形映射) 的非对角 $\max |\rho|$ 最低, 接近理想独立序列水平; 几种真·二维核 (Moore 八邻域、去中心非对称四邻域、水平-对角非对称二维) 的非对角 $\max |\rho|$ 明显偏高, 多路输出之间耦合更强。

实现复杂度代理 (XOR/bit 与状态位/输出流)。 表 2 给出了不同方法在统一建模下的状态位/输出流与每比特两输入异或门数量。可以看到, 所有方法的状态位/输出流均为 $R \times C$, 即在阵列规模相同的前提下, 路径型方法与真·二维核具有可比的 “比特并行度”。在异或门开销方面, 路径型二维元胞自动机更新核约为 1.5 个两输入 XOR/bit, 而去中心非对称四邻域核、水平-对角非对称二维核和 Moore 八邻域核的 XOR/bit 则依次增加。路径型方案在保持统计随机性的同时显著降低了每比特所需的线性逻辑资源。

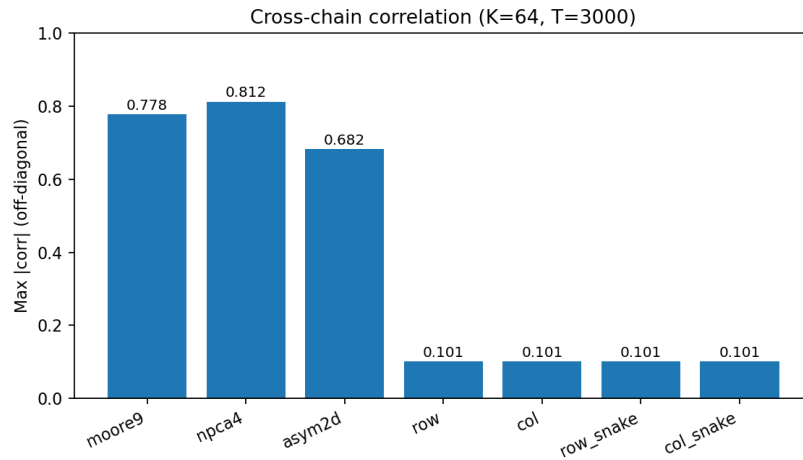


Figure 2. Comparison of inter-chain correlation for different two-dimensional cellular automaton methods (off-diagonal max $|\rho|$)

图 2. 不同二维元胞自动机方法的跨链相关性比较 (非对角 max $|\rho|$)

Table 2. Comparison of engineering proxy metrics for different two-dimensional cellular automaton structures

表 2. 不同二维元胞自动机方法在 NIST SP 800-22 子测试上的 p 值比较

方法 Method	Moore 八邻域核 Moore	水平 - 对角非对称二维核 Asym2D	去中心非对称四邻域核 NPCA4	行映射 Row	列映射 Col	行蛇形映射 Row-Snake	列蛇形映射 Col-Snake
状态位/链 (State bits per chain)	$R \times C$	$R \times C$	$R \times C$	$R \times C$	$R \times C$	$R \times C$	$R \times C$
两输入 XOR/bit (2-input XOR per bit)	7.0	4.0	3.0	1.5	1.5	1.5	1.5

3.5. 应用场景界定与安全性讨论

需要指出的是，本文所研究的二维元胞自动机伪随机数发生器本质上属于线性系统。其状态演化可由模 2 线性递推关系完全刻画，在代数结构上与一维混合规则 90/150 元胞自动机及线性反馈移位寄存器具有一致的线性特征。本文通过路径映射与四方邻域结构设计，在保持线性可分析性的前提下改善了链间相关性和硬件复杂度，但并未引入非线性更新机制。在此背景下，有必要对本文方法的适用应用场景与安全性含义作出明确界定。本文采用的 NIST SP 800-22 随机性测试主要用于检验序列在统计意义上是否存在显著偏差，其通过结果仅表明生成序列在频数分布、游程结构、累积和等统计特征上表现良好，并不构成对抗性安全性的证明。特别地，对于线性系统而言，通过统计测试并不能排除其在已知结构或已知输出条件下被预测或重构的可能性。

因此，本文提出的二维元胞自动机伪随机数发生器主要面向非对抗性应用场景，包括但不限于：

- 蒙特卡洛仿真与统计抽样中的随机激励源；
- 数值实验、优化算法和仿真系统中的随机扰动生成；
- 芯片逻辑内建自测试（BIST）中用于扫描链激励的伪随机模式发生器 [16]。

在上述应用中，伪随机源的核心需求在于良好的统计性质、低相关性、高吞吐率以及可控的

硬件复杂度，而非密码学意义上的不可预测性。本文提出的路径型二维元胞自动机结构正是围绕这些工程约束展开设计与评估。

若将该类结构用于密码学相关应用或对抗性安全场景，则必须在输出端进一步引入非线性后处理机制，例如非线性布尔函数组合、S-box 映射或其他非线性滤波结构，以破坏其线性可预测性。关于非线性扩展方案的系统设计、安全性分析及其对硬件复杂度的影响，已超出本文讨论范围，将作为后续研究方向展开。

4. 结论与展望

本文围绕四方邻域路径型二维元胞自动机伪随机数发生方法，搭建了统一的仿真与评估平台，并与若干典型二维更新核进行了系统对比。结合前文结果，可以得到如下三个方面的结论。

(1) 理论上：一维本原多项式合成支撑二维结构的最大周期与可分析性。通过路径映射将二维阵列线性化，在一维空间内应用 Cattell-Muzio 混合元胞自动机合成方法，可与给定本原多项式建立一一对应关系，在设计阶段显式保证一维结构具有特征多项式为本原多项式、周期为 $2^N - 1$ （除全零态外全部状态都在同一轨道中）以及线性复杂度可解析等性质；再通过可逆路径映射回到二维，二维更新矩阵与一维矩阵相似，从而在二维结构上继承同一个本原特征多项式和最大周期。这使得本文给出的二维 CA 伪随机数发生器不仅在几何上契合二维阵列，而且在周期长度和状态空间利用率上具有严格的一维理论保证，这一点与许多经验构造的二维 CA 形成了区分。

(2) 实验上：在 NIST 子测试与多流相关性上优于/不劣于典型二维核。在 64×64 、单流 10^6 bit 的统一平台下，本文提出的四类路径型二维 CA 在所选 NIST SP 800-22 子测试上全部通过，其 p 值表现与 moore9、npca4 等强基线相当或略优，而 asym2d 在矩阵秩或近似熵等对子结构敏感的子测试上存在明显压力；在 $K=64$ 路并行输出的多流相关性分析中，蛇形路径在零时延相关矩阵的非对角 $\max |\rho|$ 上显著低于若干真·二维核，多路伪随机序列之间更接近统计独立。

(3) 结构上：XOR/bit 更低、输出并行度高，适合作为通用硬件伪随机模式发生器。路径型二维 CA 仅依赖四方邻域与受限垂直耦合，互连局部、结构规整，对每比特所需的线性逻辑资源要求较低；与高连通的真·二维核相比，该类结构在 XOR/bit 指标上约节省一半以上的异或门，且保持与基线相同的状态位/输出流规模，有利于在大规模阵列上平铺扩展。因此，本文方法在“随机性质量-多流去相关-结构复杂度-并行伸缩性”之间提供了一种工程上可行的折中方案，适合作为通用伪随机数发生器。

在上述阶段性结论和已搭建的仿真/评测平台基础上，后续工作将主要沿着“随机性测试拓展—应用场景拓展—结构形式拓展”三条主线展开：

(1) 随机性测试的拓展。在现有 NIST SP 800-22 子测试基础上，引入 TestU01 等更大规模随机性测试框架，对不同阵列规模和路径映射进行更系统的稳健性验证，并考察周期、线性复杂度与统计测试结果之间的关系 [17]。

(2) 面向具体应用场景的联合建模。将二维元胞自动机伪随机数发生器与具体应用（如并行蒙特卡洛仿真、片上逻辑内建自测试、多通道安全协议）中的其他模块进行联合建模，在更大并行规模下评估多流相关性、实现代价与任务性能之间的折中关系。

(3) 结构形式的适度拓展。在保持局部互连与低异或门密度前提下, 尝试引入稀疏非线性或时变扰动, 探索更适合不同应用需求的二维元胞自动机结构族, 并考察其在不同工艺、不同版图约束下的可实现性。

总体而言, 本文基于“四方邻域 + 路径映射”的二维元胞自动机伪随机数发生方法, 在具有严格一维理论支撑的最大周期和线性复杂度、统计随机性质量、多流相关性与实现复杂度之间实现了较为均衡的折中, 为构造高质量硬件伪随机数发生器提供了一种可行方案, 也为其在芯片测试等多流伪随机激励场景中的应用探索奠定了基础。

参考文献

- [1] Cattell, K. and Muzio, J.C. (1996) Synthesis of One-Dimensional Linear Hybrid Cellular Automata. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, **15**, 325-335. <https://doi.org/10.1109/43.489103>
- [2] Serra, M., Slater, T., Muzio, J.C. and Miller, D.M. (1990) The Analysis of One-Dimensional Linear Cellular Automata and Their Aliasing Properties. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, **9**, 767-778. <https://doi.org/10.1109/43.55213>
- [3] Wolfram, S. (1986) Random Sequence Generation by Cellular Automata. *Advances in Applied Mathematics*, **7**, 123-169. [https://doi.org/10.1016/0196-8858\(86\)90028-x](https://doi.org/10.1016/0196-8858(86)90028-x)
- [4] Perrenoud, M., Sipper, M. and Tomassini, M. (2000) On the Generation of High-Quality Random Numbers by Two-Dimensional Cellular Automata. *IEEE Transactions on Computers*, **49**, 1146-1151. <https://doi.org/10.1109/12.888056>
- [5] Torres-Huitzil, C., Delgadillo-Escobar, M. and Nuno-Maganda, M. (2012) Comparison between 2D Cellular Automata Based Pseudorandom Number Generators. *IEICE Electronics Express*, **9**, 1391-1396. <https://doi.org/10.1587/elex.9.1391>
- [6] Guan, S.-U., Zhang, S. and Quieta, M.T. (2004) 2-D CA Variation with Asymmetric Neighborhood for Pseudorandom Number Generation. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, **23**, 378-388. <https://doi.org/10.1109/tcad.2004.823344>
- [7] 朱保平, 马骞, 刘凤玉. 二维可控细胞自动机伪随机序列发生方法研究 [J]. 中国工程科学, 2007, 9(6): 43-47.
- [8] 杨勇, 方勇, 夏天. 一种基于 2-by-n 元胞自动机的高质量伪随机数发生器 [J]. 四川大学学报, 2008, 40(5): 153-158.
- [9] 孙凌宇, 冷明, 王千峰, 郁松年. 基本和混合元胞自动机的伪随机数发生器研究 [J]. 计算机工程与应用, 2010, 46(27): 75-76.
- [10] Levina, A., Mukhamedjanov, D., Bogaevskiy, D., Lyakhov, P., Valueva, M. and Kaplun, D. (2022) High Performance Parallel Pseudorandom Number Generator on Cellular Automata. *Symmetry*, **14**, Article 1869. <https://doi.org/10.3390/sym14091869>

-
- [11] Jaleel, H.A., Kaarthik, S., Sathish, S. and Bhattacharjee, K. (2023) Multiple-Stream Parallel Pseudo-Random Number Generation with Cellular Automata. In: Manzoni, L., Mariot, L. and Roy Chowdhury, D., Eds., *Lecture Notes in Computer Science*, Springer Nature Switzerland, 90-104. https://doi.org/10.1007/978-3-031-42250-8_7
- [12] Poornima, I.G.A., Yogaraja, C.A., Venkatesh, R., Sudha, M.S. and Vijayalakshmi, B. (2024) Pseudo Random Number Generator Based on Cellular Automata with Self Organized Criticality. *SN Computer Science*, **5**, Article No. 454. <https://doi.org/10.1007/s42979-024-02750-3>
- [13] Bardell, P.H., McAnney, W.H. and Savir, J. (1987) Built-In Test for VLSI: Pseudorandom Techniques. Wiley.
- [14] Dhingra, S. (2005) Comparison of LFSR and CA for BIST. Term Paper, Auburn University.
- [15] Rukhin, A., *et al.* (2010) A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. NIST Special Publication 800-22 rev.1a.
- [16] Rajski, J., Tyszer, J., Kassab, M., Mukherjee, N., Thompson, R., *et al.* (2002) Embedded Deterministic Test for Low Cost Manufacturing Test. *Proceedings of the International Test Conference*, Baltimore, 10 October 2002, 301-310. <https://doi.org/10.1109/test.2002.1041773>
- [17] L'Ecuyer, P. and Simard, R. (2007) TestU01: A C Library for Empirical Testing of Random Number Generators. *ACM Transactions on Mathematical Software*, **33**, 1-40. <https://doi.org/10.1145/1268776.1268777>