arXiv:2603.19656v1 [cs.CR] 20 Mar 2026

基于元胞自动机的资源高效的最大等分布伪随机数生成器

Bhuvaneswari A

蒂鲁吉拉伯利国家理工学院计算机科学与工程系，*620015*，泰米尔纳德邦，印度

Kamalika Bhattacharjee*

印度工程科学与技术学院（希布布尔）信息技术系，豪拉，*711103*，西孟加拉邦，印度

摘要

等分布是一项用于衡量线性伪随机数生成器（PRNG）均匀性的理论质量标准。在本文中，我们首先证明，现有的所有基于线性元胞自动机（CA）的伪随机数生成器（PRNG）在等分布特性方面都较为薄弱。随后，我们提出了一系列采用度为 $31 \leq k \leq 128$ （接近计算机字长）的线性最大长度元胞自动机、具有时间间隔（$2 \leq s \leq 10$）的轻量级组合型基于元胞自动机的伪随机数生成器。我们证明，这些伪随机数生成器不仅能够实现最大周期，还满足最大等分布性质。最后，我们证明，这些组合最大长度元胞自动机伪随机数生成器几乎通过了所有经验测试套件，其速度和性能均可与梅森旋转算法相媲美。

关键词：最大长度元胞自动机、轻量级组合型伪随机数生成器、周期、等分布、时间间隔、统计检验

*通讯作者电子邮箱：abhuvanesh15@gmail.com（Bhuvaneswari A），kamalika.it@gmail.com（Kamalika Bhattacharjee）

1. 引言

伪随机数生成器（PRNG）旨在生成周期长度长、效率高且理论质量良好的随机数序列。凭借这些特性，它们被广泛应用于仿真、密码学和赌博等各种领域。伪随机数生成器是一种确定性算法，它以一个随机种子值为起点，生成一串称为伪随机数的数值。伪随机数生成器的主要特性包括周期长、可复现性、均匀性和效率。除了这些特性之外，还需满足某些理论质量要求，例如等分布，它用于衡量每个可能维度上的均匀性 [6]。伪随机数生成器还应通过所有或大多数用于确定随机性质量的基准经验测试平台。

当今大多数伪随机数生成器都基于线性反馈移位寄存器（LFSR），其底层存在负责实现较长周期和按比特运算的本原多项式（模2）。目前存在许多基于LFSR的伪随机数生成器，例如Tausworthe、 [8], 梅森旋转算法、 [12],GFSR、扭曲广义反馈移位寄存器 [13], 、WELL [11], 以及Xorshift生成器 [19],等，它们基于模2线性递推关系生成伪随机数序列。这些生成器被称为线性伪随机数生成器。这类伪随机数生成器易于实现，可以用矩阵代数进行刻画，其均匀性也可以通过等分布来衡量。经典的基于LFSR的伪随机数生成器称为Tausworthe生成器。当多项式包含较少数量的非零系数（N_1）时，它能够高效地生成随机数（下文中，“随机”一词仅表示“伪随机”）。然而，它无法满足等分布性质以及许多基本统计检验。此外，由于多项式包含较少的 N_1，每一步仅有少量比特发生变化，其余比特在多个周期内始终主要保持为零。在密码学中，这被称为低扩散能力问题 [6], ，不利于随机性。之所以采用此类多项式，是因为缺乏既具有较高扩散性质、又具备较大度数的本原多项式。

为了解决这些局限，文献中采用了两种方法。第一种是使用组合生成器 [2]，通过异或（XOR）运算，将多个由度相对较小的本原多项式生成的伪随机序列组合起来。这类组合伪随机数生成器若经过精心选择参数，不仅能够达到良好的理论性能指标

，还能产生适合随机性应用的长周期。另一种方法是使用调温——一种输出变换函数——来处理由高阶线性递推生成的比特，从而提高等分布性 [9]。然而，这两种方法只有在线性递推的组成部分具有足够大的阶时才效果良好。与此同时，许多现代应用需要轻量级伪随机数生成器，既适合在现场可编程门阵列平台上以硬件方式实现，又能高效运行并适配多核 CPU 或图形处理器的字长。这些轻量级伪随机数生成器受到资源利用率限制，因此容易受到安全缺陷的影响 [22]，而这些缺陷源于随机性质量不佳。最新的轻量级伪随机数生成器旨在利用逻辑斯蒂映射等的混沌特性。[23, 24]，但这使得它们无法通过理论性能指标进行测试。

在此背景下，元胞自动机（CA）作为一种自然的计算模型，长期以来一直被誉为物理系统中随机性的来源 [14]，因而成为一种极佳的替代方案。元胞自动机使用简单的局部规则并行更新每个元胞的状态，由此产生全局动态行为。由于具有局部性、固有并行性和简洁性，元胞自动机（CA）一直广泛应用于硬件实现 [15]。这些优点促使研究人员将元胞自动机用作伪随机数生成器 [1]。为此，人们主要使用混沌的最大长度元胞自动机；它们是最简单形式的元胞自动机——初等元胞自动机（ECA）的一种变体 [15, 17, 10]。与线性反馈移位寄存器类似，最大长度元胞自动机也存在相应的模 2 本原多项式，可产生长度为 2^k-1 的周期，其中 k 为元胞自动机的规模。这些元胞自动机也被用于设计轻量级的多流伪随机数生成器 [17, 18]。然而，尽管这些伪随机数生成器的资源效率很高，其随机性质量仍未达到基准统计检验所衡量的水平 [17]。此外，这些基于元胞自动机的伪随机数生成器的理论品质指标也尚不明确。

因此，在这项工作中，我们的目标是利用最大长度元胞自动机设计资源高效的伪随机数生成器。参考文献 [4] 和 [7] 提供了获取最大长度元胞自动机的良好资源，本工作将利用这些资源。为了获得更长的周期和最大等分布，我们将在伪随机数生成器中组合多个最大长度元胞自动机。为使其轻量化，每个元胞自动机组件均限制为不超过 128 比特，组件数量限制为两个。这些最大长度元胞自动机均具有混沌特性，在硬件和内存需求方面都很高效。不过，由于具有混沌特性，这些元胞自动机组件会呈现自相似模式。为了打破这些模式

并系统地提高随机性质量，我们采用时间间隔技术。我们展示了利用这些元胞自动机可以构建资源高效、速度快、周期长，同时具有最大等分布特性的伪随机数生成器，并且能够通过所有基准测试平台中的大多数测试。

2. 伪随机数生成器及质量标准

伪随机数生成器（PRNG）可用数学方式定义如下 [6]:

定义 1. *PRNG* G 是一种由(S, μ, f, U, g) 构成的结构：其中S 是有限状态集，μ是起始状态 S 上的概率分布，该起始状态称为种子； $f : S \to S$ 是用于更新状态的转移函数， U 是输出空间， $g : S \to U$ 是输出函数。

根据 μ，选择一个初始状态 $s_0 \in S$ 作为种子。初始时，输出为 $u_0 = g(s_0)$。每一步 $i \geq 1$都按 $s_i = f(s_{i-1})$计算新状态，并产生相应的输出 $u_i = g(s_i)$。序列（u_i）$_{i\geq 0}$ 称为由 G生成的伪随机序列。

2.1. 线性伪随机数生成器的一般框架

基于 $\mathbb{F}_2$ 上的矩阵线性递推的线性伪随机数生成器的一般框架由以下方程 [6]表示。

$$x_n = Ax_{n-1} \tag{1}$$

$$y_n = Bx_n \tag{2}$$

$$u_n = \sum_{l=1}^{w} y_{n,l-1} 2^{-l} = .\, y_{n,0} y_{n,1} y_{n,2} \cdots \tag{3}$$

在这些方程中， x_n 是步骤 n 处的 k 比特状态向量， y_n 是步骤 n处的 w 比特输出向量。 k 和 w 均为正整数。 A 是转移矩阵或特征矩阵， B 是输出变换矩阵或调温矩阵。在步骤 n，得到的输出随机数是实数 $u_n \in [0, 1)$。通过选择合适的矩阵 A 和 B，任何线性伪随机数生成器都可以纳入这一框架。

该序列的另一种表示形式见参考文献 [5]。这里，伪随机序列 $u_i \in [0, 1)$ $i = 1, 2, \cdots$定义如下：

$$u_i = \sigma(f_i(x)/M(x)) \text{ where } f_i(x) = (g(x) f_{i-1}(x) + h(x)) \pmod{M(x)} \tag{4}$$

这里， $g(x)$ $h(x)$ $M(x)$ 和 $f_i(x)$ 是 GF{2, x} 中的多项式，而 σ 是从 GF{2, x} 到实数域的映射。对于 Tausworthe 生成器，$M(x)$ 是度为 k 、模 2 意义下不可约的特征多项式， $h(x) = 0$， $g(x) =$(x^s(模 $M(x)$))，其中 $0 < s < 2^k - 1$，且 gcd(s， 2^k –1) $= 1$。这种多项式表示形式通常有助于从理论上分析伪随机数生成器的特性。

2.2. 组合伪随机数生成器

组合伪随机数生成器将多个不同的、形式如公式 1 所示的递推关系（组成部分）组合起来，具体如下。假设我们有 j 个分量$j = 1$， 2、.....、J。对于生成器 j，设 A_j为 $k_j \times k_j$转移矩阵， B_j 为 $w \times k_j$ 输出变换矩阵。在步骤 n时， k_j 比特状态向量为 $x_{j,\ n}$。该组合生成器在步骤 n的输出由以下公式 [9]定义：

$$y_n = B_1 x_{1,n} \oplus B_2 x_{2,n} \oplus \cdots \oplus B_j x_{j,n} \tag{5}$$

$$u_n = \sum_{\ell=1}^{w} y_{n,\ell}\, 2^{-\ell} \tag{6}$$

这里， $\oplus$ 表示按位异或运算。该组合生成器与公式 1 给出的生成器类似，其 $k = k_1 + \cdots + k_j$参数为 $A =$diag(A_1、.....、 A_J)，以及 $B =$ (B_1、.....、 B_J)。令 P_j(z)表示每个组成部分 A_j 的特征多项式j。因此，A的特征多项式为 P(z) $= P_1$(z) $\cdots P_J$(z)。由于该多项式是可约的，组合伪随机数生成器无法达到 $2^k - 1$ 的最大周期。选择要组合的组成部分至关重要，因为根据组成部分的选择不同，所得生成器可能具有较长的周期和更优的理论性质。假设我们选择参数，使得每个组成部分 i 的度为 k_i，具有最大周期 $2^{k_i} - 1$，并且所选组成部分的周期长度互素。那么，该组合伪随机数生成器的周期就是各个组成部分周期的最小公倍数（LCM），如命题 1 [5]所述。

命题1 ([5])**.** 由 $U_n =$$u_n^{(1)}$异或 $\cdots$异或 $u_n^{(J)}$， $n = 1, 2, \ldots$ 定义的组合伪随机序列，周期为 $\prod_{j=1}^{J} \left(2^{\deg(M^{(j)})} - 1\right)$，当且仅当对于每个具有特征多项式 $M^{(j)}$ 的序列 $u_n^{(j)}$，序列 $2^{\deg(M^{(j)})} - 1$， $j = 1, \ldots, J$ 的周期两两互素。

2.3. 理论品质指标

伪随机数生成器最重要的理论性质是，其生成的数在任意维度上均匀分布。输出值的这种均匀性可以通过一种称为等分布性的过程来评估。将生成器的输出值视为 $\Psi_t = \{(u_0, \ldots, u_{t-1}) : x_0 \in \mathbb{F}_2\}$。$\mathbb{F}_2$-线性生成器的均匀性通过使用 $\Psi_I = \{(u_{i_1}, \ldots, u_{i_t}) : x_0 \in \mathbb{F}_2\}$ 来评估，其中 $I = \{i_1, \ldots, i_t\}$ 是一组固定的非负整数有序组，且 $0 \leq i_1 < \mathbb{F}_2$ [6]。对于 $I = \{0, \ldots, t-1\}$，返回初始集合 $\Psi_t = \Psi_I$。

设$\mathbf{q} = (q_1、\ldots\ldots、q_t)$为任意非负整数向量。沿各个轴 $j = 1、\ldots\ldots、t$ 将单位超立方体 $[0,1)^t$ 划分为 2^{q_j} 个等长区间。这样便将 $[0,1)^t$ 划分为 $2^{q_1+\cdots+q_t}$ 个大小和形状相同的长方体。若集合 Ψ_I 在每个长方体中恰好包含 2^q 个点，其中 q满足 $k - q = q_1 + \cdots + q_t$，则称 Ψ_I 为$\mathbf{q}$-等分布。只有当 $q_1 + \cdots + q_t \leq k$ 时，这才是可能的。这种$\mathbf{q}$-等分布可用于衡量线性伪随机数生成器的均匀性。通过构造相应的二进制矩阵并检查其秩来进行验证。使用以下步骤生成二进制矩阵 $(\mathcal{B})$ [6]。

- 令 $j = 1, 2, \ldots k$
- 启动生成器，令 $j = 1, 2, \ldots k$，假设 $x_0 = e_j$为初始状态，且 e_j 为单位向量，其在位置 j处为 1，其余位置为 0
- 对每个 j 值，将生成器运行 t 个时间步
- 获取每一步的输出 u_n
- 提取第 1 步输出的 q_1 个最高有效位， q_2 第 2 步的，以及第 t 步的 q_t
- 这些提取出的比特构成二进制矩阵的 j^{th}列。对每一列重复此操作 j

2.3.1. (t, ℓ)-等分布

对于$\mathbf{q}$-等分布，当 k 的值很大时，计算非常困难。在这种情况下，只考虑较小一类向量$\mathbf{q}$：其中所有坐标 q_j 都等于某个常数 $l \geq 1$。也就是说，只考虑每个坐标的 l 个最高有效位，这会将单位超立方体 $[0,1)^t$ 划分为 2^{tl} 个立方体。如果 Ψ_I 对于$\mathbf{q} = (l, \ldots, l)$是$\mathbf{q}$-等分布的，那么称 Ψ_I具有 l比特精度的 t-分布。可以使用以下命题 2 验证各个生成器 [3]的这种(t, l)-等分布。

命题 2 ([3])。 当且仅当矩阵$\mathcal{B}_{t,\ell,s}$ 的秩为（满）秩 $t\ell$时，该序列是(t,ℓ)-等分布的。若 $\ell_t = \lfloor k/t \rfloor < k/t \leq L$，则当且仅当矩阵$\mathcal{B}_{t,\ell_t+1,s}$ 的秩为 k时，该序列也不会发生碰撞 $CF(t)$。

满足此特性的 l 的最大值称为 Ψ_I 的分辨率，记为 l_I。它不能超过 l_t^* =min(L, $\lfloor k/t \rfloor$)。 Ψ_I 的分辨率差距定义为 $\Lambda_I = l_t^* - l_I$。维度 t 下的分辨率差距定义为 $\Lambda_t = \ell_t^* - \ell_t$，分辨率 ℓ 下的维度差距定义为 $\Delta_\ell = t_\ell^* - t_\ell$。

这些概念不仅适用于不可约多项式，也适用于可约多项式（组合生成器） [3]。对于组合生成器，先计算每个分量对应的二进制矩阵。然后将这些矩阵纵向拼接，得到一个等分布 $\widetilde{\quad}$ $\widetilde{\quad}$ 矩阵（$\mathcal{B}_{t,\ l,\ s}$）。对于 j 个分量，$\mathcal{B}_{t,\ l,\ s}$ 是 $\mathcal{B}_1$，$\mathcal{B}_2$，.....，$\mathcal{B}_J$ 的纵向拼接，其中 $\mathcal{B}_1$ 提供前 k_1 列， $\mathcal{B}_2$ 提供接下来的 k_2 列，以此类推， $\mathcal{B}_J$ 提供最后的 k_J 列。该组合生成器的（t， l）等分布见命题 3 [3]。

命题 3 ([3])。 当且仅当矩阵$\widetilde{\mathcal{B}}_{t,l,s}$ 的秩为满秩 tl时，该序列是(t,l)等分布的。若 $lt = \lfloor k/t \rfloor < k/t \leq L$，则当且仅当矩阵$\mathcal{B}_{t,lt+1,s}$ 的秩为 k时，该序列也满足 $\widetilde{CF}(t)$ 。

2.3.2. 最大等分布

假设一个具有 t 维度的单位超立方体被划分为 $2^{t\ell}$ 个大小相等的立方单元。生成器生成一系列 t维点或向量，并根据各自的值将其放入相应的单元中。参数 ℓ_t 表示维度 t上的分辨率，其定义为每个单元包含相同数量点时ℓ所能达到的最大值。当生成器在所有维度 [3]上达到 ℓ_t 的最大值时，称其为最大等分布（ME）生成器。

要判断该序列是否为最大等分布，无需计算 l_t 在 t = 1、2、.....、 k 时的值。以下命题 4 指出，当且仅当对所有 $t \in \Phi_1 \cup \Phi_2$ [3]均满足 $\Lambda_t = 0$ 时，最大周期序列才是最大等分布。

命题 4 ([3]). 当且仅当对所有 $t \in \Phi_1 \cup \Phi_2$， $\Lambda_t = 0$时，最大周期序列是最大等分布的。当且仅当对所有 $l \in \Psi_1 \cup \Psi_2$， $\Delta_l = 0$ 时，它也具有最大等分布性。

这里， L 是计算机的字长，

$$\Phi_1 = \left\{ \max\left(2, \left\lfloor \frac{k}{L} \right\rfloor\right), \ldots, \left\lfloor \sqrt{k} \right\rfloor \right\} \tag{7}$$

$$\Phi_2 = \left\{ t = \left\lfloor \frac{k}{\ell} \right\rfloor \,\middle|\, \ell = 1, \ldots, \left\lfloor \sqrt{k} \right\rfloor \right\} \tag{8}$$

$$\Psi_1 = \{1, \ldots, \lfloor \sqrt{k} \rfloor\} \tag{9}$$

$$\Psi_2 = \{\ell = \lfloor k/t \rfloor \mid t = \max(2, \lfloor k/L \rfloor), \ldots, \lfloor \sqrt{k-1} \rfloor\} \tag{10}$$

这里，维度 t (l_t) 的分辨率表示序列保持（t, l）-等分布时 $l \leq L$ 的最大值，其中 $l_t \leq l_t^*$ 和 l_t^*= 为 $\min(L, \lfloor k/t \rfloor)$。

3. 最大周期元胞自动机与基于线性元胞自动机的伪随机数生成器

元胞自动机（CA）是一种数学模型，包含一个由元胞构成的网格，其中每个元胞可取有限状态集 $\mathcal{S}$ 中的任意状态。每个元胞根据当前元胞的状态及其邻居的状态，使用局部规则（R）更新自身状态。这些邻域组合称为规则最小项（RMT）。每个时间步 t 的状态集合称为一个构型。所有元胞均由局部规则并行更新，因此元胞自动机从一个构型演化到下一个构型。

本文研究有限初等元胞自动机（ECA）。它是一种一维、二状态、三邻域的元胞自动机——每个元胞根据其左邻居、自身和右邻居的状态来更新状态。零边界条件下，元胞自动机包含 n 个元胞；也就是说，元胞编号从 0 到 $n-1$，末端元胞的邻居设为零（0）。因此，邻域组合从 000 到 111，共有 $2^3 = 8$ 个可能的规则最小项。初等元胞自动机规则总计有 $2^{2^3} = 256$ 条，编号从 0 到 255。例如，初等元胞自动机规则 90 和 150 定义如下:

$$\text{Rule 90:} \quad S_i^{t+1} = S_{i-1}^t \oplus S_{i+1}^t,$$

$$\text{Rule 150:} \quad S_i^{t+1} = S_{i-1}^t \oplus S_i^t \oplus S_{i+1}^t.$$

其中， S_i^t 是元胞 i 在第 t^{th} 个时间步的状态。

在元胞自动机中，如果每个元胞都使用相同的规则 R 更新状态，则称其为均匀元胞自动机。否则，称其为非均匀元胞自动机。在一个含 n个元胞的非均匀元胞自动机中，使用规则向量 $\mathcal{R} = \langle R_0, R_1, \ldots\ldots, R_{n-1} \rangle$，而不是单一规则 R

其中， i^{th} 使用规则 R_i 更新其状态。在元胞自动机中，如果转移函数（局部规则）是线性映射，则称该元胞自动机为线性元胞自动机。此处，构型空间可视为向量空间。例如，初等元胞自动机规则 90 和 150 是线性元胞自动机。线性非均匀元胞自动机中一种值得关注的类型称为最大长度元胞自动机。这类元胞自动机的一个重要特征是能够提供$2^n - 1$的最大周期长度。研究表明，当且仅当规则向量仅包含规则 90 和 150，且特征多项式在二元伽罗瓦域 GF(2) 上为本原多项式时，线性元胞自动机才是最大长度元胞自动机 [7]。此外，在零边界条件下，只有规则 90 和 150 的某种特定组合才能产生最大长度元胞自动机。线性最大长度元胞自动机也可以用线性代数来刻画。任何线性最大长度元胞自动机都可表示为 $n \times n$ 特征矩阵。

定义 2。 特征矩阵 T 是一个阶数为 $n \times n$的矩阵，定义如下：

$$T[i,j] = \begin{cases} 1, & if\ cell\ i\ depends\ on\ cell\ j \\ 0, & otherwise \end{cases}$$

例如，一个 $\mathcal{R}=\langle 150,\ 90,\ 90,\ 90,\ 90\rangle$ 的 5 单元最大周期元胞自动机的特征矩阵如下所示。该矩阵的特征多项式是本原多项式——该元胞自动机的周期长度为 $2^5-1=31$。

$$T = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

文献 [4], 中展示了若干规模为 $n = 1$ 至 500 的一维线性最大周期元胞自动机：最多 2 个元胞位置采用规则150，其余所有位置均采用相同的规则90。文献 [7] 介绍了两个不同规模的近似均匀最大周期元胞自动机，分别命名为 CA（$90'$）和 CA（$150'$）；当规模 n 是索菲·热尔曼素数 [7]时，它们的周期长度也达到最大值 2^n-1。CA（$90'$）表示所有元胞均采用规则90，唯有第一个元胞采用规则150。同理，CA（$150'$）表示所有元胞均采用规则150，唯有第一个元胞采用规则90。因此，除第一个元胞外，其余所有位置均采用相同的规则。

3.1. 基于线性元胞自动机的伪随机数生成器

由于线性元胞自动机可以通过线性代数运算高效实现，而且线性最大周期元胞自动机具有与线性反馈移位寄存器相似的特性，因此它们被用于伪随机数生成器的设计 [15, 17]。基于线性最大周期元胞自动机的伪随机数生成器被提出作为一种适用于硬件实现的高效模型 [15]。本文采用32位最大周期元胞自动机 $\mathcal{R}_1 = \langle 90,$ 150, 90, 90, 90, 150, 150, 90, 90, 90, 90, 90, 150, 90, 90, 150, 150, 90, 150, 150, 150, 90, 150, 150, 150, 150, 90, 150, 90, 150, 90, $150\rangle$ 生成用于内建自测试（BIST）的伪随机数。在 [10], 中，采用规模为 n=1409 的线性 CA（150′）（本文将其命名为 $\mathcal{R}_2$）设计了一种伪随机数生成器，其速度和随机性测试结果可与梅森旋转算法相媲美。在[17], 中，利用35位 CA（150′）（本文将其命名为 $\mathcal{R}_3$）设计了一种多流并行伪随机数生成器；它只浪费3位即可生成32位随机数，但未能通过大多数统计测试平台。随后，考虑到当前的计算机字长，开发了一种64位多流并行伪随机数生成器，它采用64位最大周期元胞自动机，在 3^{rd} 和 5^{th} 个元胞处使用规则150，在其他元胞处使用规则90（本文将其命名为 $\mathcal{R}_4$） [18]；经过调温后，它也通过了测试平台中的几乎所有测试。然而，尽管基于线性元胞自动机的伪随机数生成器具有较长的周期和较快的速度，但此前从未考察过这些生成器的理论品质指标（等分布性）。因此，我们将在下一节对它们进行测试。

3.2. 现有基于线性元胞自动机的伪随机数生成器的均匀分布

这里，我们首先选取大小分别为 32（$\mathcal{R}_1$）、35（$\mathcal{R}_3$）、64（$\mathcal{R}_4$）和 1409（$\mathcal{R}_2$）的线性最大长度元胞自动机，并按照第2.3节中讨论的步骤分析其理论性质（等分布）。为分析此类伪随机数生成器的等分布性质，我们首先将基于元胞自动机的伪随机数生成器纳入第2.1节所述的框架中。假设规则向量的大小为 k。那么，矩阵 A 是根据定义 2 得到的、针对该规则向量的大小为 $k \times k$ 的转移矩阵 T，矩阵 B 则是 $k \times k$ 单位矩阵的 w 行。

例如，对于一个大小为 32 的规则向量 $\mathcal{R}_1$，我们根据命题 3 检验其最大等分布性。根据该命题，只有当所有t值（t, l）都满足等分布时，才能称其为最大等分布。这里 $t \in \{2, 3, 4, 5, 6, 8, 10, 16, 32\}$。在这些 t值中，只有 $t = 32$ 达到了（t, l）等分布。因此，这个大小为 32 的基于线性元胞自动机的伪随机数生成器并非最大等分布。表1给出了规则向量 $\mathcal{R}1$对应的等分布结果。

同样，其余元胞自动机 $\mathcal{R}_2$，$\mathcal{R}_3$ 和 $\mathcal{R}_4$ 也未能满足最大等分布性。

表1：规则向量 $\mathcal{R}1$ 的基于线性元胞自动机的伪随机数生成器均匀分布测试

t	$l_t^* = \min(L, \lfloor k/t \rfloor)$	l_t ($l_t \leq l_t^*$)	**Rank**	**等分布**
2	16	16	18	非 (t, l)-均匀分布
3	10	10	13	非 (t, l)-均匀分布
4	8	8	12	非 (t, l)-均匀分布
5	6	6	11	非 (t, l)-均匀分布
6	5	5	11	非 (t, l)-均匀分布
8	4	4	12	非 (t, l)-均匀分布
10	3	3	13	非 (t, l)-均匀分布
16	2	2	17	非 (t, l)-均匀分布
32	1	1	32	(t, l)-均匀分布

因此，现有的这些基于线性元胞自动机的伪随机数生成器都无法实现最大等分布。为了解决这一问题，在接下来的章节中，我们的目标是设计轻量级的基于元胞自动机的伪随机数生成器，同时满足优质伪随机数生成器所必需的理论质量标准。

4. 基于元胞自动机的组合伪随机数生成器中的元胞自动机组件来源

我们的主要目标是开发能够实现较长周期和最大等分布的基于元胞自动机的伪随机数生成器。如第 1 节所述，线性反馈移位寄存器生成器有两种成熟的方法可实现这一要求——（1）使用适当的输出变换函数或调温，或（2）设计一个参数适当的组合生成器。调温是一种外部函数，需要额外的计算单元（硬件）。此外，如元胞自动机的情况 $\mathcal{R}_2$ 或 $\mathcal{R}_4$所示，如果底层本原多项式的度不够大，调温也可能无法实现等分布。

由于我们希望设计兼具硬件效率和轻量化，并完全基于元胞自动机的特性，因此倾向于不使用任何输出变换或调温。因此，我们选择设计能够实现最大等分布的线性最大周期元胞自动机组合生成器。为确保伪随机数生成器轻量且资源高效，我们将元胞自动机组件的元胞数量限制为最多 n 128 个，因此只需 128 比特即可。为获得较长的周期，我们选择组成基于元胞自动机的组合伪随机数生成器的组件，使其最大周期为 $(2^n - 1)$，且各周期两两互素。

如前所述，元胞自动机很容易在硬件上实现。一个元胞可以用一个存储比特或触发器（FF）表示，并配以实现更新其状态规则的组合电路。例如，最大长度元胞自动机 $\mathcal{R}=\langle 150,\ 90,\ 90,\ 90,\ 90\rangle$ 的硬件实现如图1所示。这里可以看到，规则90只需要一个双输入异或

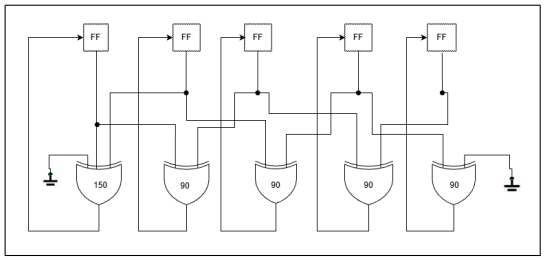


图1：最大长度元胞自动机的硬件实现 $\langle 150,\ 90,\ 90,\ 90,\ 90\rangle$门，而规则150需要一个三输入异或门。因此，在所选元胞自动机中，如果几乎所有元胞都采用相同规则，就可以复制用于单个元胞的相同硬件模块，从而使设计更具成本效益。

现在，为了使我们的生成器具备资源效率，我们要寻找这类最大周期元胞自动机，其中大多数元胞采用相同的规则。文献中有两项资源提供了此类最大周期元胞自动机的列表，分别见参考文献 [4]和参考文献 [7]。参考文献 [4]列出了度数最高达500的线性最大周期元胞自动机，其中只有两个元胞采用规则150，其余元胞均采用相同的规则90。而参考文献 [7] 则给出了两种不完善策略，用元胞自动机（90’）和元胞自动机（150’）生成度为 n的本原多项式。据称，当 n 是索菲·热尔曼素数时，这类元胞自动机能够生成周期为 2^n-1 的序列；其中只有第一个元胞采用规则150（或规则90），其余元胞均采用规则90（或规则150）。这类最大长度元胞自动机非常适合硬件实现，因为大多数元胞遵循相同规则，只有位于特定位置的一两个元胞例外。

然而，最重要的问题是，这些元胞自动机是否有潜力成为设计优质伪随机数生成器的良好随机性来源。研究表明，元胞自动机只有在混沌的（定义在无限格点上）并满足一些理想特性时，才能成为良好的随机性来源，例如不偏向任何特定状态、两个方向上都存在信息流，且周期非常长 [25]。由于我们采用的是最大周期元胞自动机，它们自然满足周期较长这一条件。此外，规则 90 和 150 是平衡规则，因为更新函数并非双向.....

射的，因此无法生成任意状态。接下来，我们需要考察这些元胞自动机是否具有信息流，以及是否呈现混沌特性。文献 [16]，中设计了一种方法，用于计算左右两个方向的信息流，并利用一个称为P-参数的参数预测非均匀元胞自动机的混沌行为。

为了通过 P-参数预测混沌属性，信息流分两部分计算。首先，计算一个元胞的邻居受到该元胞微小变化影响的概率；这一过程称为信息传播。接下来，评估这种影响对邻居造成的作用，而邻居又可能反过来影响原元胞。这称为信息烹制。 p-参数是一个有序对（p_1， p_2）。从抽象意义上说，如果网格上始终存在信息流，那么， p_1 就是每个元胞两个方向上信息传播最大值中的最小值。类似地，计算 p_2 时，对每个元胞，首先分别找出两个方向上信息传播和信息烹制的最大值，再取其中的较小值。所有元胞的这些值中的最小值就是 p_2。如果 p_1， p_2都很高，则认为该元胞自动机具有混沌性，且将 (0。75，0。5) 视为混沌的阈值。然而，由于我们用于伪随机数生成器的元胞自动机是有限的，因此无法直接应用这一参数。

为了解决这一问题，并了解其在无限格点上定义时的行为，我们考察网格上任意元胞采用规则90或规则150并不断复制时的信息传播和信息烹制，并计算P-参数值。对于规则90，各个方向上始终都会发生信息传播和信息烹制，因此概率为100%。然而，对于规则150，各个方向上始终会发生信息传播，但不会发生信息烹制。因此，只要规则向量同时使用规则90和规则150， P-参数的值就是（p_1， p_2） = （1，1）。例如，考虑具有 $\mathcal{R}=\langle 150, 90, 90, 90, 90\rangle$的5单元线性最大长度元胞自动机。对于此元胞自动机，参数值为（p_1， p_2） = （1，1）；因此，它满足混沌性质。由于我们所有的线性最大长度元胞自动机都使用规则90和规则150，因此它们都满足混沌性质。因此，凭借高效硬件实现和混沌特性，这些最大长度元胞自动机被用于设计轻量级组合型元胞自动机伪随机数生成器，相关内容将在后续章节讨论。

5. 组合最大长度元胞自动机伪随机数生成器：第一阶段

组合伪随机数生成器通常由多个组成部分构成。这里，每个最大长度元胞自动机都视为一个组成部分。首先，选取两个周期互素的最大长度元胞自动机。两个元胞自动机均演化 t个时间步。在每个时间步，通过异或运算（采用左侧或右侧填充）组合两个元胞自动机配置，从而得到一个新的随机序列。该序列称为组合随机数序列。此过程如算法1所示。

算法1 组合双分量最大长度元胞自动机伪随机数生成器

要求： 两个最大长度元胞自动机 CA_1，CA_2 其周期互素
要求： 时间步数 t 以及每个元胞自动机规则向量的大小 k_j
要求： 种子（构型） $S_1^{(0)} \in \{0,1\}^{k_1}$，$S_2^{(0)} \in \{0,1\}^{k_2}$
确保： U {组合随机序列}
1: $U \leftarrow [\,]$
2: 用长度为 k_j 的随机配置（种子）S_j 初始化每个最大长度元胞自动机 CA_j
3: **对于** $n=1$ **到** t，**执行**
4: $u_1^{(n)} \leftarrow$下一状态(CA_1)
5: $u_2^{(n)} \leftarrow$下一状态(CA_2)
6: $u_n \leftarrow u_1^{(n)} \oplus u_2^{(n)}$
7: 将 u_n 追加到 U
8: **结束循环**
9:**返回** U

设 k 为最大长度元胞自动机的大小，其周期为$\rho = 2^k - 1$，并令 u_n^j 表示由 j^{th}最大长度元胞自动机生成的随机序列。组合随机序列表示为：

$$u = u_n^1 \oplus u_n^2 \oplus \cdots \oplus u_n^j$$

在本研究中，我们关注两个分量，即 j=2 和 $u_n = u_n^1 \oplus u_n^2$，其中 u_n^1 是由第一个元胞自动机生成的序列，u_n^2 是由第二个元胞自动机生成的序列。此外，基于元胞自动机的组合伪随机数生成器中的每个分量的周期为 $\rho_j = 2^{k_j} - 1$，且两个分量的周期长度互素，因此这个双分量基于元胞自动机的组合伪随机数生成器的周期等于 LCM($2^{k_1}-1$, $2^{k_2}-1$) =($2^{k_1}-1$)($2^{k_2}-1$)。随后，我们测试这些组合伪随机数生成器的等分布性。

表2：组成部分最大长度元胞自动机的特征

k	**最大长度元胞自动机**	**k/2**	**N_1**	**N_1/k**	**k**	**最大长度元胞自动机**	**k/2**	**N_1**	**N_1/k**
29	1	14	11	0.38	79	9	39	11	0.14
30	1	15	9	0.30	80	1,71	40	31	0.39

k	最大长度元胞自动机	k/2	N_1	N_1/k	k	最大长度元胞自动机	k/2	N_1	N_1/k
31	11	15	5	0.16	81	1	40	25	0.30
32	1,15	16	11	0.34	82	1,69	41	33	0.40
33	1	16	11	0.33	83	1	41	27	0.32
34	1,19	17	11	0.32	84	36	42	39	0.46
35	1	17	13	0.37	85	1,46	42	27	0.32
36	6	18	16	0.44	86	1	43	31	0.36
37	9	18	17	0.46	87	13	43	15	0.17
38	7	19	13	0.34	88	5	44	41	0.47
39	1	19	13	0.33	89	1	44	29	0.33
40	8	20	17	0.42	90	1	45	31	0.34
41	1	20	17	0.41	91	15	45	19	0.21
42	19	21	23	0.55	92	3,71	46	45	0.49
43	3	21	17	0.39	93	33	46	21	0.22
44	4,26	22	21	0.47	94	42	47	25	0.26
45	9	22	17	0.37	95	1	47	13	0.14
46	2,10	23	19	0.41	96	6	48	35	0.36
47	13	23	9	0.19	97	1,82	48	27	0.28
48	15	24	19	0.40	98	8	49	35	0.36
49	1,10	24	21	0.43	99	13	49	25	0.25
50	11	25	27	0.54	100	1,67	50	27	0.27
51	1	25	17	0.33	101	1,20	50	33	0.32
52	2,29	26	17	0.32	102	33	51	35	0.34
53	1	26	21	0.40	103	15	51	21	0.20
54	9	27	25	0.46	104	2,40	52	27	0.26
55	17	27	11	0.20	105	1	52	31	0.29
56	4,14	28	25	0.45	106	30	53	45	0.42
57	9	28	17	0.29	107	19	53	25	0.23
58	17	29	25	0.43	108	1,35	54	37	0.34
59	4,15	29	17	0.28	109	1,4	54	41	0.38
60	2,38	30	21	0.35	110	13	55	37	0.34
61	1,10	30	27	0.44	111	27	55	13	0.12
62	5	31	19	0.30	112	2,5	56	43	0.38
63	31	31	3	0.04	113	1	56	23	0.20
64	3,5	32	21	0.32	114	22	57	43	0.37
65	1	32	13	0.20	115	41	57	19	0.16
66	1,19	33	21	0.31	116	16	58	37	0.32
67	15	33	17	0.25	117	33	58	27	0.23
68	8	34	23	0.34	118	30	59	37	0.31
69	1	34	23	0.33	119	1	59	19	0.16
70	1,37	35	17	0.24	120	3,73	60	37	0.30
71	17	35	15	0.21	121	45	60	19	0.15
72	6,55	36	29	0.40	122	14	61	35	0.29
73	9	36	25	0.34	123	51	61	15	0.12
74	1	37	29	0.39	124	21	62	33	0.27
75	7	37	19	0.25	125	13	62	19	0.15
76	2,22	38	33	0.43	126	40	63	21	0.16
77	3,44	38	29	0.38	127	15	63	11	0.08
78	1,41	39	19	0.24	128	1,29	64	27	0.21

5.1. 使用规则 *150 [4],* 最多考虑 *2* 个元胞

我们首先选取文献 [4] 中度数介于32和64之间的最大周期元胞自动机，其中最多两个元胞采用规则150，其余元胞均采用规则90。表2列出了这些元胞自动机。这里， k 表示相应线性最大周期元胞自动机的多项式大小或度数。相应的规则向量由采用规则的元胞位置表示

150。例如，大小为32的最大长度元胞自动机包含1和15；这意味着编号为2和15的元胞仅使用规则150，其余元胞使用规则90。通过这种方式，我们首先从该表中选取所有周期长度互素的双分量组合。总共有306种可能的组合。我们发现，尽管每种组合都实现了接近 $2^{k_1+k_2}$的大周期，但没有一种组合达到最大等分布。

由于双分量组合元胞自动机伪随机数生成器均未满足最大等分布特性，我们还将分量数量从两个增加到三个，以观察是否有所改进。我们选取 $32 \leq k_1, k_2, k_3 \leq 64$范围内的3分量组合（$k_1, k_2, k_3$）。共找到1433种两两互素的组合。这些组合的周期长度同样接近 $2^{k_1+k_2+k_3}$，但我们再次观察到其不满足最大等分布。因此，这些双分量和三分量组合型基于元胞自动机的伪随机数生成器均可获得接近 $2^{k_1+k_2+\cdots+k_j}$的大周期，但未能满足作为随机性理论品质指标所必需的最大等分布特性。因此，我们不再进一步增加分量数量。

示例 *1*。考虑两个大小分别为 *31*(k_1) 和 *32*(k_2) 的最大周期元胞自动机；其周期分别为 $\rho_1 = 2^{31} - 1$和 $\rho_2 = 2^{32} - 1$。相应的规则向量为 $\mathcal{R}1=\langle 90$、*90*、*90*、*90*、*90*、*90*、*90*、*90*、*90*、*90*、*90*、*150*、*90*、*90*、*90*、*90*、*90*、*90*、*90*、*90*、*90*、*90*、*90*、*90*、*90*、*90*、*90*、*90*、*90*、*90*、*90*、*90*、*90*、*90*、$90\rangle$ 和 $\mathcal{R}2=\langle 150$、*90*、*90*、*90*、*90*、*90*、*90*、*90*、*90*、*90*、*90*、*90*、*90*、*90*、*90*、*150*、*90*、*90*、*90*、*90*、*90*、*90*、*90*、*90*、*90*、*90*、*90*、*90*、*90*、*90*、*90*、*90*、*90*、*90*、$90\rangle$。这两个元胞自动机的周期互素，因为 *gcd*(2^{31}*–1,* $2^{32} - 1$*)* $= 1$；因此，将两个元胞自动机的构型结合起来，可实现约为 2^{63} 的较大周期。接下来，为了测试等分布，首先使用方程*7*计算 ϕ_1 和 ϕ_2 的值；其中 $\Phi_1 = \{2, 3, 4, 5, 6, 7\}$ 和 $\Phi_2 = \{9, 10, 12, 15, 21, 31, 63\}$。因此， $t = \Phi_1 \cup \Phi_2 = \{2, 3, 4, 5, 6, 7, 9, 10, 12,$*15*、*21*、*31*、$63\}$。然而，在所有 t 个值中，只有两个 t 值满足 *(t, l)*-等分布。因此，该伪随机数生成器未实现最大等分布。这些结果显示在下面的表*3*中。

表3：组合元胞自动机伪随机数生成器（31,32）的等分布

t	$l_t^* =$ 最小值(L, $\lfloor k/t \rfloor$)	l_t ($l_t \leq l_t^*$)	**Rank**	**等分布**
2	31	31	39	非(t, l)均匀分布
3	21	21	33	非(t, l)均匀分布
4	15	15	29	非（t， l）均匀分布
5	12	12	29	非（t， l）均匀分布

表3——接上页

t	$l_t^* = \min(L, \lfloor k/t \rfloor)$	l_t ($l_t \leq l_t^*$)	**Rank**	**等分布**
6	10	10	26	非 (t, l)-均匀分布
7	9	9	27	非 (t, l)-均匀分布
9	7	7	29	非（t, l）均匀分布
10	6	6	29	非（t, l）均匀分布
12	5	5	31	非（t, l）均匀分布
15	4	4	34	非（t, l）均匀分布
21	3	3	45	非（t, l）均匀分布
31	2	2	62	（t, l）均匀分布
63	1	1	63	(t, l)-均匀分布

5.2. 考虑 $CA(90')$ 或 $CA(150')$

接下来，我们将元胞自动机的大小增加到 128，同时从文献 [7]中取 $CA($90′) 和 $CA($150′)。将大小接近 32、64 和 128 的此类元胞自动机组合起来，并针对周期长度和等分布性质进行分析。大小接近 128 的最大长度 $CA($90′) 和 $CA($150′) 的元胞长度分别为 105、113、119；大小接近 64 的元胞长度为 65、69；大小接近 32 的元胞长度为 26、29、35、39。在此，我们以下列三种方式组合这些元胞自动机：(i) $CA($90′) 与 $CA($90′)；(ii). $CA($150′) 与 $CA($150′) (iii)。 $CA($90′) 与 $CA($150′) 以及$CA($150′) 与 $CA($90′)。

表4展示了组合生成器中，元胞自动机规模接近32、64和128时的双分量互素组合。这里我们同样观察到，伪随机数生成器的周期长度接近 $2^{k_1+k_2}$，其中 k_1 是第一个组成部分的规模， k_2 是第二个组成部分的规模。然而，在测试最大等分布性质时，它们同样都未能达到最大等分布。因此，使用 CA（90′）和 CA（150′）的组合伪随机数生成器也能实现接近最大值的周期，但无法实现最大等分布特性。下一节将进一步改进伪随机数生成器，使其达到最大等分布。

表4：使用 $CA($90′) 和 $CA($150′) 的组合伪随机数生成器组合

CA	**具有互素组合的组合伪随机数生成器**		
	$CA(90')$**与** $CA(90')$ (k_1, k_2)**：** (90′, 90′)	CA(150′) **与** CA(150′) (k_1, k_2)**：** (150′, 150′)	CA(90′) **与** CA(150′) (k_1, k_2)**：** (90′, 150′)
接近 32	(26,29), (26,35), (29,35), (29,39), (35,39)	(26,29), (26,35), (29,35), (29,39), (35,39)	(26,29), (29,26), (26,35), (35,26), (29,35), (35,29), (29,39), (39,29), (35,39), (39,35)
接近 64	(65,69)	(65,69)	(65,69), (69,65)

接近 128	(105,113), (113,119)	(105,113), (113,119)	(105,113), (113,105), (113,119), (119,113)

6. 组合最大长度元胞自动机伪随机数生成器：第二阶段

混沌元胞自动机的问题之一是，它们倾向于生成自相似且自组织的图案，例如谢尔宾斯基三角形和等边三角形 [25]。这会使生成器失去随机性。因此，为了打破这些对称图案、提升随机性质量，文献 [15]提出了位点间隔的概念。这意味着不再使用每个时间步的配置，而是跳过若干步。这样可以提升随机数的质量，并实现更好的等分布。

为了开发这样的伪随机数生成器，我们选取两个周期长度互素的最大周期元胞自动机，并运行 t 个时间步。现在，不再组合每个时间步的元胞自动机构型，而是跳过 $s-1$ 步，并在每隔 s^{th} 步时组合构型。例如，如果 $s = 2$，则每隔两步组合一次序列。该过程如算法2所示。

算法2 带时间间隔的双分量最大长度元胞自动机伪随机数生成器

要求： 两个最大周期元胞自动机 CA_1，CA_2，其周期互素 ρ_1，ρ_2
要求： 时间步数 t、步长 s, s 必须满足 gcd(s，$\rho 1\rho_2$) = 1，以及各元胞自动机规则的大小向量 k_1，k_2
要求： 初始配置（种子） $S_1^{(0)} \in \{0,1\}^{k_1}$, $S_2^{(0)} \in \{0,1\}^{k_2}$
确保： U {组合随机序列}
$U \leftarrow [\,]$
使用种子 S_j初始化每个元胞自动机 CA_j
对 $n = 1$ **至** t **执行**
  对 $i = 1$ **至** s **执行**
    $u_1^{(n)} \leftarrow$下一状态(CA_1)
    $u_2^{(n)} \leftarrow$下一状态(CA_2)
  结束循环
  $u_n \leftarrow u_1^{(n)} \oplus u_2^{(n)}$
  将 u_n 追加到 U
结束循环
返回 U

由于每隔 $s-1$ 步就会跳过一些构型，从伪随机数生成器的角度来看，每个组成部分都可以表示为矩阵 $A = (T)^s$，其中 T 是该组成部分的最大长度元胞自动机的特征矩阵。设 ρ_i 和 ρ_j 分别为第一和第二个组成部分的周期长度。那么 ρ 是两个组成部分周期的最小公倍数；也就是说，$\rho = \text{lcm}(\rho_i, \rho_j)$。如果

$\gcd(s,\ \rho) = 1$，则这个具有时间间隔的组合伪随机数生成器可实现接近 $2^{k_1+k_2}$ 的较大周期。否则，周期为 $\rho_{\gcd(s,\ \rho)}$。这些结论可由以下命题推导得出，该命题与命题1类似。

命题5. 设 k_1 和 k_2 是两个本原多项式（模2）的度，其周期分别为 ρ_1 和 ρ_2，满足 $gcd(\rho_1, \rho_2) = 1$，且 $s > 1$ 是时间间隔大小。如果 $gcd(s, \rho) = 1$，那么时间间隔为 s 的组合生成器的周期接近最大值，即 $\rho = lcm(\rho_1, \rho_2) \approx 2^{k_1+k_2}$。否则，周期为 $\rho = \frac{\rho}{gcd(s,\rho)}$

证明。考虑由以下定义的两个伪随机序列

$$f_i(x) = a(x)^s\, f_{i-s}(x) \pmod{m_1(x)},$$
$$g_i(x) = b(x)^s\, g_{i-s}(x) \pmod{m_2(x)},$$

其中，$m_1(x)$ 和 $m_2(x)$ 是两个模2本原多项式，输出每隔 s^{th} 步提取一次。然后，根据公式4，组合序列由 $V_i(x) = \overline{f_i(x)\, m_1(x) + g_i(x)\, m_2(x)}$（模1）得出。

考虑多项式 $Z_i(x) = m_2(x)f_i(x)+m_1(x)g_i(x)$（mod $m_1(x)m_2(x)$）。那么，$V_i(x) = \overline{Z_i(x)}\ \overline{m_1(x)m_2(x)}$。现在，令 $A(x) = n_1(x)m_2(x)(a(x)^s)+n_2(x)m_1(x)(b(x)^s)$，其中 $n_1(x)m_2(x) \equiv 1 \pmod{m_1(x)}$ 且 $n_2(x)m_1(x) \equiv 1 \pmod{m_2(x)}$。那么，

$$\begin{aligned}
A(x)Z_i(x) &= (n_1(x)m_2(x)(a(x)^s) + n_2(x)m_1(x)(b(x)^s))(m_2(x)f_i(x) + m_1(x)g_i(x)) \\
&= n_1(x)m_2^2(x)(a(x)^{2s})f_{i-s}(x) + n_2(x)m_1^2(x)(b(x)^{2s})g_{i-s}(x) \pmod{m_1(x)m_2(x)} \\
&= m_2(x)(a(x)^s)f_i(x) + m_1(x)(b(x)^s)g_i(x) \pmod{m_1(x)m_2(x)} \\
&= m_2(x)f_{i+s}(x) + m_1(x)g_{i+s}(x) \pmod{m_1(x)m_2(x)} \\
&= Z_{i+s}(x) \pmod{m_1(x)m_2(x)}
\end{aligned}$$

这符合公式4的形式。因此，如果 s 与 $m_1(x)m_2(x)$ 互素，组合生成器将实现接近最大周期的周期。也就是说，当 $\gcd(s,\ \rho) = 1$ 时，$\rho = \mathrm{lcm}(\rho_1, \rho_2) \approx 2^{k_1+k_2}$；否则，它会缩短为 $\rho_{\gcd(s,\ \rho)}$。因此，证明如下。 □

因此，如果我们的最大长度元胞自动机的大小互素，且时间间隔大小与每个元胞自动机周期的乘积互素，那么通过时间间隔进行组合，就能使组合序列达到接近最大周期的周期。但是，增大 s 的值意味着需要进行更多计算才能生成序列中的下一个数，这显然会增加

生成器的时间复杂度。因此，为了使生成器更加轻量，本研究将 s 设为 $2 \leq s \leq 10$。

此外，这次我们还考虑了度为 k 的特征多项式中非零系数的数量（N_1）。由于非零系数所占比例N_1/k 接近50%，可将其作为伪随机数生成器 [6]的次级优值指标。我们还将元胞自动机的最大规模增至128，即将每个组成部分的规模设为 $32 \leq k_i \leq 128$。然后，我们测试这种组合型基于元胞自动机的伪随机数生成器在时间间隔下的等分布性。下面将讨论满足特定 s 值的最大等分布条件的这类组合型基于元胞自动机的伪随机数生成器。

6.1. 考虑最多包含*2*个元胞且采用规则*150*的情况

表2列出了参考文献 [4]中度为32至128的所有可能元胞自动机组件的特性。在此表中， N_1 表示非零系数的数量，同时也列出了范围s $32 \leq k_i \leq 128$ s内哪些最大周期元胞自动机满足次级优值指标的结果。现在，我们将两种情况的元胞自动机组合起来： N_1 值接近度的一半，以及 N_1 不接近度的一半。

6.1.1. 将最大长度元胞自动机与接近度的一半的 N_1 结合：

查阅表2可知，只有五个最大周期元胞自动机（元胞自动机规模分别为 37、42、44、50 和 92）的 N_1 值接近其度的一半。从这 5 个最大周期元胞自动机中，可以构成以下双分量互素组合：$(k_1,\ k_2) = (37,\ 42)$，$(37,\ 44)$，$(37,\ 50)$，以及 $(37,\ 92)$。对于与各分量周期长度乘积互素的范围 $2 \leq s \leq 10$ 内的 s 值，所有这些组合都能实现较大的周期。但只有 3 种组合达到最大等分布（ME）。下表5描述了这些组合的等分布结果。这里， s 周期 表示在哪些 s 值下可达到接近最大周期的周期， $s\ ME$ 表示生成器在哪些 s 值下达到 ME。列 $\rho\ ME$ 指出生成器在哪些 s 值下既达到 ME，又实现接近最大周期。例如，对于组合伪随机数生成器 $(k_1,\ k_2)$，当 $k_1 = 37$ 和 $k_2 = 42$ 时， $s = 2,\ 4,\ 5,\ 8,\ 10$ 时，其周期等于最小公倍数 LCM $(2^{37} - 1,\ 2^{42} - 1) \approx 2^{79}$，并且在 $s = 8,\ 10$ 时满足最大等分布。

6.1.2. 将最大长度元胞自动机与 N_1 不接近度数一半的元胞自动机结合：

除了上文提到的五个最大长度元胞自动机外，表2中的所有其他最大长度元胞自动机，其 N_1 值都不接近该度的一半。

表5：组合伪随机数生成器的等分布

$\mathbf{k_1}$	$\mathbf{k_2}$	s**周期** (ρ)	s **ME**	ρ **ME**
37	42	2, 4, 5, 8, 10	8, 10	8, 10
37	44	2, 4, 7, 8	7, 8	7,8
37	50	2, 4, 5, 7, 8, 10	10	10
37	92	2, 4, 7, 8	-	-

接下来，我们从这些元胞自动机中找出所有周期互素的双分量组合；总共得到2725种组合。如上文所述，对于与 ρ互素的 s 值，所有组合都能产生较长的周期。随后我们测试其等分布性：在这2725种可能的组合中，有368种组合达到最大等分布。这些结果汇总于下表6。这里， s 周期、 s 最大等分布 和 ρ 最大等分布 的含义与之前相同。在这368种最大等分布组合中，一些组合伪随机数生成器既实现最大等分布，周期也接近 $2^{k_1+k_2}$ ；另一些则实现了最大等分布，但周期并不接近最大值；在这种情况下，伪随机数生成器的周期为$^{\rho}$ $_{\gcd(s,\rho)}$。

表6：具有时间间隔的组合型基于元胞自动机的伪随机数生成器的等分布

k_1	k_2	s**周期** (ρ)	s **ME**	ρ **ME**	k_1	k_2	s **周期** (ρ)	s **ME**	ρ **ME**
31	32	2,4,7,8	5,6,7,8,9,10	7,8	34	47	2,4,5,7,8,10	7,8,9,10	8,10
31	33	2,3,4,5,6,8,9,10	8,9,10	8,9,10	34	49	2,4,5,7,8,10	7,8,9,10	8,10
31	34	2,4,5,7,8,10	5,6,7,8,9,10	5,7,8,10	34	53	2,4,5,7,8,10	9,10	10
31	35	2,3,4,5,6,7,8,9,10	8,9,10	8,9,10	34	55	2,4,5,7,8,10	8,9,10	8,10
31	36	2,4,87,8,9,10	7,8,9,10	8	34	57	2,4,5,8,10	9,10	10
31	38	2,4,5,7,8,10	7,8,9,10	8,10	34	59	2,4,5,7,8,10	10	10
31	39	2,3,4,5,6,8,9,10	8,9,10	8,9,10	34	61	2,4,5,7,8,10	10	10
31	40	2,4,7,8	8,9,10	8	34	63	2,4,5,8,10	10	10
31	41	2,3,4,5,6,7,8,9,10	8,9,10	8,9,10	34	65	2,4,5,7,8,10	10	10
31	43	2,3,4,5,6,7,8,9,10	7,9,10	7,9,10	35	36	2,4,8	9,10	-
31	45	2,3,4,5,6,8,9,10	8,9,10	8,9,10	35	38	2,4,5,7,8,10	9,10	10
31	46	2,4,5,7,8,10	7,8,9,10	7,10	35	43	2,3,4,5,6,7,8,9,10	9,10	9,10
31	47	2,3,4,5,6,7,8,9,10	8,9,10	8,9,10	35	46	2,4,5,7,8,10	9,10	10
31	48	2,4,8	8,9,10	8	35	47	2,3,4,5,6,7,8,9,10	8,9,10	8,9,10
31	49	2,3,4,5,6,7,8,9,10	8,9,10	8,9,10	35	48	2,4,8	7,8,9,10	8
31	50	2,4,5,7,8,10	10	8,10	35	52	2,4,7,8	9,10	-
31	51	2,3,4,5,6,8,9,10	8,9,10	8,9,10	35	54	2,4,5,8,10	9,10	10
31	52	2,4,7,8	8,9,10	8	35	57	2,3,4,5,6,8,9,10	9,10	9,10
31	53	2,3,4,5,6,7,8,9,10	9,10	9,10	35	58	2,4,5,7,8,10	9,10	10
31	54	2,4,5,8,10	9,10	10	35	59	2,3,4,5,6,7,8,9,10	9,10	9,10
31	55	2,3,4,5,6,7,8,9,10	9,10	9,10	35	61	2,3,4,5,6,7,8,9,10	10	10
31	57	2,3,4,5,6,8,9,10	9,10	9,10	35	62	2,4,5,7,8,10	10	10
31	58	2,4,5,7,8,10	9,10	10	35	64	2,4,7,8	10	-
31	59	2,3,4,5,6,7,8,9,10	10	10	35	66	2,4,5,8,10	10	10
31	60	2,4,8	10	-	35	67	2,3,4,5,6,7,8,9,10	10	10
31	61	2,3,4,5,6,7,8,9,10	10	10	35	68	2,4,7,8	10	-
32	33	2,4,8	9,10	-	36	47	2,4,8	7,8,9,10	8
32	43	2,4,7,8	6,7,8,9,10	7,8	36	41	2,4,8	9,10	-
32	45	2,4,8	7,8,9,10	8	36	43	2,4,8	9,10	-
32	47	2,4,7,8	7,8,9,10	7,8	36	49	2,4,8	9,10	-

k_1	k_2	s周期 (ρ)	s ME	ρ ME	k_1	k_2	s 周期 (ρ)	s ME	ρ ME
32	49	2,4,7,8	8,9,10	8	36	53	2,4,8	9,10	-
32	51	2,4,8	9,10	-	36	55	2,4,8	8,9,10	8
32	53	2,4,7,8	9,10	-	36	59	2,4,8	9,10	-
32	55	2,4,7,8	9,10	-	36	61	2,4,8	10	-
32	57	2,4,8	9,10	-	36	65	2,4,8	10	-
32	59	2,4,7,8	10	-	36	67	2,4,8	10	-
32	61	2,4,7,8	10	-	37	50	2,4,8	9,10	-
32	63	2,4,8	10	-	37	92	2,4,8	9,10	-
33	34	2,4,5,8,10	9,10	10	38	39	2,4,5,8,10	10	10
33	38	2,4,5,8,10	9,10	10	38	41	2,4,5,7,8,10	9,10	10
33	40	2,4,8	9,10	-	38	43	2,4,5,7,8,10	9,10	10
33	43	2,3,4,5,6,8,9,10	9,10	9,10	38	45	2,4,5,8,10	8,9,10	10
33	46	2,4,5,8,10	8,9,10	8,10	38	47	2,4,5,7,8,10	9,10	10
33	47	2,3,4,5,6,8,9,10	8,9,10	8,9,10	38	49	2,4,5,7,8,10	9,10	10
33	49	2,3,4,5,6,8,9,10	8,9,10	8,9,10	38	51	2,4,5,8,10	9,10	10
33	50	2,4,5,8,10	8,9,10	8,10	38	53	2,4,5,7,8,10	9,10	10
33	52	2,4,8	10	-	38	55	2,4,5,7,8,10	8,9,10	8,10
33	56	2,4,8	10	-	38	59	2,4,5,7,8,10	9,10	10
33	58	2,4,5,8,10	9,10	10	38	61	2,4,5,7,8,10	9,10	10
33	59	2,3,4,5,6,8,9,10	9,10	9,10	38	63	2,4,5,8,10	10	10
33	61	2,3,4,5,6,8,9,10	10	10	38	65	2,4,5,7,8,10	10	10
33	62	2,4,5,8,10	10	10	38	67	2,4,5,7,8,10	10	10
34	35	2,4,5,7,8,10	9,10	10	38	69	2,4,5,8,10	10	10
34	39	2,4,5,8,10	9,10	10	39	40	2,4,8	9,10	-
34	41	2,4,5,7,8,10	9,10	10	39	43	2,3,4,5,6,8,9,10	9,10	9,10
34	43	2,4,5,7,8,10	8,9,10	8,10	39	46	2,4,5,8,10	9,10	10
34	45	2,4,5,8,10	7,8,9,10	8,10	39	47	2,3,4,5,6,8,9,10	9,10	9,10
39	49	2,3,4,5,6,8,9,10	9,10	9,10	45	47	2,3,4,5,6,8,9,10	8,9,10	8,9,10
39	50	2,4,5,8,10	9,10	10	45	49	2,3,4,5,6,8,9,10	9,10	9,10
39	55	2,3,4,5,6,8,9,10	9,10	9,10	45	52	2,4,8	9,10	-
39	56	2,4,8	9,10	-	45	53	2,3,4,5,6,8,9,10	10	10
39	58	2,4,5,8,10	9,10	10	45	56	2,4,8	9,10	-
39	59	2,3,4,5,6,8,9,10	9,10	9,10	45	58	2,4,5,8,10	8,9,10	8,10
39	61	2,3,4,5,6,8,9,10	9,10	9,10	45	59	2,3,4,5,6,8,9,10	9,10	9,10
39	62	2,4,5,8,10	10	10	45	61	2,3,4,5,6,8,9,10	9,10	9,10
39	67	2,3,4,5,6,8,9,10	10	10	45	62	2,4,5,8,10	9,10	10
39	68	2,4,8	10	-	45	64	2,4,8	9,10	-
40	41	2,4,7,8	9,10	-	45	67	2,3,4,5,6,8,9,10	10	10
40	43	2,4,7,8	8,9,10	8	46	47	2,4,5,7,8,10	9,10	10
40	47	2,4,7,8	9,10	-	46	49	2,4,5,7,8,10	10	10
40	49	2,4,7,8	9,10	-	46	51	2,4,5,8,10	9,10	10
40	51	2,4,8	9,10	-	46	53	2,4,5,7,8,10	10	10
40	57	2,4,8	10	-	46	55	2,4,5,7,8,10	10	10
40	59	2,4,7,8	9,10	-	46	57	2,4,5,8,10	10	10
40	61	2,4,7,8	9,10	-	46	59	2,4,5,7,8,10	9,10	10
40	63	2,4,8	10	-	46	63	2,4,5,8,10	9,10	10
40	67	2,4,7,8	10	-	46	65	2,4,5,7,8,10	9,10	10
41	43	2,3,4,5,6,7,8,9,10	9,10	9,10	46	67	2,4,5,7,8,10	10	10
41	45	2,3,4,5,6,8,9,10	9,10	9,10	47	48	2,4,8	9,10	-
41	46	2,4,5,7,8,10	9,10	10	47	49	2,3,4,5,6,7,8,9,10	9,10	9,10
41	47	2,3,4,5,6,7,8,9,10	8,9,10	8,9,10	47	50	2,4,5,7,8,10	9,10	10
41	48	2,4,8	8,10	8	47	51	2,3,4,5,6,8,9,10	9,10	9,10
41	49	2,3,4,5,6,7,8,9,10	9,10	9,10	47	52	2,4,7,8	8,10	8
41	50	2,4,5,7,8,10	9,10	10	47	53	2,3,4,5,6,7,8,9,10	9,10	9,10
41	54	2,4,5,8,10	9,10	10	47	54	2,4,5,8,10	9,10	10
41	55	2,3,4,5,6,7,8,9,10	9,10	9,10	47	55	2,3,4,5,6,7,8,9,10	9,10	9,10
41	57	2,3,4,5,6,8,9,10	9,10	10	47	56	2,4,7,8	8,9,10	8
41	58	2,4,5,7,8,10	9,10	10	47	60	2,4,8	9,10	-
41	59	2,3,4,5,6,7,8,9,10	9,10	10	47	64	2,4,7,8	9,10	-

k_1	k_2	s**周期** (ρ)	s **ME**	ρ **ME**	k_1	k_2	s **周期** (ρ)	s **ME**	ρ **ME**
41	61	2,3,4,5,6,7,8,9,10	9,10	9,10	47	68	2,4,7,8	10	
41	62	2,4,5,7,8,10	10	10	47	72	2,4,8	10	-
41	63	2,3,4,5,6,8,9,10	10	10	47	73	2,3,4,5,7,8,9,10	10	-
41	64	2,4,7,8	10	-	47	57	2,3,4,5,6,8,9,10	9,10	9,10
41	66	2,4,5,8,10	10	10	47	58	2,4,5,7,8,10	9,10	10
41	67	2,3,4,5,6,7,8,9,10	10	10	47	59	2,3,4,5,6,7,8,9,10	9,10	9,10
41	68	2,4,7,8	10	-	47	61	2,3,4,5,6,7,8,9,10	9,10	9,10
43	45	2,3,4,5,6,8,9,10	9,10	9,10	47	62	2,4,5,7,8,10	9,10	10
43	46	2,4,5,7,8,10	9,10	10	47	63	2,3,4,5,6,8,9,10	10	10
43	47	2,3,4,5,6,7,8,9,10	9,10	9,10	47	65	2,3,4,5,6,7,8,9,10	10	10
43	48	2,4,8	8,9,10	8	47	66	2,4,5,8,10	10	10
43	49	2,3,4,5,6,7,8,9,10	9,10	9,10	47	67	2,3,4,5,6,7,8,9,10	10	10
43	50	2,4,5,7,8,10	9,10	10	47	69	2,3,4,5,6,8,9,10	10	10
43	52	2,4,7,8	7,9,10	7	47	70	2,4,5,7,8,10	10	10
43	55	2,3,4,5,6,7,8,9,10	9,10	9,10	47	71	2,3,4,5,6,7,8,9,10	10	10
43	56	2,4,7,8	10	-	48	49	2,4,8	9,10	-
43	57	2,3,4,5,6,8,9,10	9,10	9,10	48	53	2,4,8	9,10	-
43	58	2,4,5,7,8,10	8,10	8,10	48	55	2,4,8	9,10	-
43	59	2,3,4,5,6,7,8,9,10	9,10	9,10	48	59	2,4,8	10	-
43	60	2,4,8	10	-	48	61	2,4,8	9,10	-
43	61	2,3,4,5,6,7,8,9,10	9,10	9,10	48	65	2,4,8	9,10	-
43	62	2,4,5,7,8,10	10	10	48	71	2,4,8	10	-
43	63	2,3,4,5,6,8,9,10	9,10	9,10	48	73	2,4,8	10	-
43	66	2,4,5,8,10	10	10	48	77	2,4,8	10	-
43	67	2,3,4,5,6,7,8,9,10	10	10	49	50	2,4,5,7,8,10	9,10	10
43	68	2,4,7,8	10	-	49	51	2,3,4,5,6,8,9,10	10	10
49	52	2,4,7,8	9,10	-	55	56	2,4,7,8	9,10	-
49	60	2,4,8	9,10	-	55	57	2,3,4,5,6,8,9,10	9,10	9,10
49	68	2,4,7,8	10	-	55	59	2,3,4,5,6,7,8,9,10	10	10
49	53	2,3,4,5,6,7,8,9,10	10	10	55	61	2,3,4,5,6,7,8,9,10	10	10
49	54	2,4,5,8,10	10	10	55	62	2,4,5,7,8,10	10	10
49	55	2,3,4,5,6,7,8,9,10	9,10	9,10	55	63	2,3,4,5,6,8,9,10	9,10	9,10
49	57	2,3,4,5,6,8,9,10	10	10	55	64	2,4,7,8	9,10	-
49	58	2,4,5,7,8,10	8,9,10	8,10	55	68	2,4,7,8	10	-
49	59	2,3,4,5,6,7,8,9,10	9,10	9,10	55	69	2,3,4,5,6,8,9,10	10	10
49	62	2,4,5,7,8,10	10	10	56	57	2,4,8	10	-
49	65	2,3,4,5,6,7,8,9,10	10	10	56	59	2,4,7,8	10	-
49	66	2,4,5,8,10	9,10	10	56	61	2,4,7,8	10	-
49	67	2,3,4,5,6,7,8,9,10	10	10	56	67	2,4,7,8	10	-
49	69	2,3,4,5,6,8,9,10	10	10	56	71	2,4,7,8	10	-
50	51	2,4,5,8,10	9,10	10	57	58	2,4,5,8,10	9,10	10
50	53	2,4,5,7,8,10	9,10	10	57	59	2,3,4,5,6,8,9,10	10	10
50	57	2,4,5,8,10	9,10	10	57	61	2,3,4,5,6,8,9,10	10	10
50	59	2,4,5,7,8,10	9,10	10	57	62	2,4,5,8,10	10	10
50	61	2,4,5,7,8,10	9,10	10	57	70	2,4,5,8,10	10	10
50	63	2,4,5,8,10	10	10	57	77	2,3,4,5,6,8,9,10	10	10
50	67	2,4,5,7,8,10	10	10	58	59	2,4,5,7,8,10	10	10
50	69	2,4,5,8,10	10	10	58	61	2,4,5,7,8,10	9,10	10
50	71	2,4,5,7,8,10	10	10	58	63	2,4,5,8,10	10	10
50	73	2,4,5,7,8,10	10	10	58	65	2,4,5,7,8,10	10	10
51	55	2,3,4,5,6,8,9,10	9,10	9,10	58	69	2,4,5,8,10	10	10
51	56	2,4,8	9,10	-	58	75	2,4,5,8,10	10	10
51	58	2,4,5,8,10	9,10	10	58	77	2,4,5,7,8,10	10	10
51	59	2,3,4,5,6,8,9,10	9,10	9,10	58	81	2,4,5,8,10	10	10
51	67	2,3,4,5,6,8,9,10	9,10	9,10	59	61	2,3,4,5,6,7,8,9,10	10	10
51	71	2,3,4,5,6,8,9,10	10	10	59	60	2,4,8	9,10	-
52	53	2,4,7,8	9,10	8	59	62	2,4,5,7,8,10	10	10
52	55	2,4,7,8	8,9,10	-	59	63	2,3,4,5,6,8,9,10	9,10	9,10
52	57	2,4,8	9,10	-	59	64	2,4,7,8	10	10

k_1	k_2	s周期 (ρ)	s ME	ρ ME	k_1	k_2	s 周期 (ρ)	s ME	ρ ME
52	59	2,4,7,8	9,10	-	59	65	2,3,4,5,6,7,8,9,10	10	10
52	61	2,4,7,8	9,10	-	59	66	2,4,5,8,10	10	10
52	63	2,4,8	10	-	59	70	2,4,5,7,8,10	10	10
52	67	2,4,7,8	10	-	59	72	2,4,8	10	10
52	69	2,4,8	10	-	59	76	2,4,7,8	10	10
52	71	2,4,7,8	10	-	59	77	2,3,4,5,6,7,8,9,10	10	10
53	54	2,4,5,8,10	10	10	59	78	2,4,5,8,10	10	10
53	55	2,3,4,5,6,7,8,9,10v	910	9,10	60	61	2,4,8	9,10	-
53	56	2,4,7,8	9,10	-	60	67	2,4,8	10	-
53	57	2,3,4,5,6,8,9,10	10	10	60	71	2,4,8	10	-
53	58	2,4,5,7,8,10	9,10	10	60	73	2,4,8	10	-
53	59	2,3,4,5,6,7,8,9,10	9,10	9,10	61	63	2,3,4,5,6,8,9,10	10	10
53	60	2,4,8	9,10	-	61	66	2,4,5,8,10	10	10
53	61	2,3,4,5,6,7,8,9,10	10	10	61	77	2,3,4,5,6,7,8,9,10	10	10
53	62	2,4,5,7,8,10	10	10	61	78	2,4,5,8,10	10	10
53	63	2,3,4,5,6,8,9,10	10	10	62	63	2,4,5,8,10	10	10
53	66	2,4,5,8,10	9,10	10	62	77	2,4,5,7,8,10	10	10
53	67	2,3,4,5,6,7,8,9,10	10	10	63	65	2,3,4,5,6,8,9,10	10	10
53	71	2,3,4,5,6,7,8,9,10	10	10	63	67	2,3,4,5,6,8,9,10	10	10
54	55	2,4,5,8,10	9,10	10	63	71	2,3,4,5,6,8,9,10	10	10
54	59	2,4,5,8,10	9,10	10	63	73	2,3,4,5,6,8,9,10	10	10
54	61	2,4,5,8,10	10	10	63	74	2,4,5,8,10	10	10
54	67	2,4,5,8,10	10	10	63	79	2,3,4,5,6,8,9,10	10	10
54	71	2,4,5,8,10	10	10	63	80	2,4,8	10	-
64	71	2,4,7,8	10	-	67	72	2,4,8	10	10
64	77	2,4,7,8	10	-	67	77	2,3,4,5,6,7,8,9,10	10	10
65	66	2,4,5,8,10	10	10	69	71	2,3,4,5,6,8,9,10	10	10
65	71	2,3,4,5,6,7,8,9,10	10	10	70	71	2,4,5,7,8,10	10	10
65	76	2,4,7,8	10	-	70	73	2,4,5,7,8,10	10	10
65	77	2,3,4,5,6,7,8,9,10	10	10	70	79	2,4,5,7,8,10	10	10
66	73	2,4,5,8,10	10	10	71	74	2,4,5,7,8,10	10	10
66	79	2,4,5,8,10	10	10	71	72	2,4,8	10	-
66	83	2,4,5,8,10	10	10	71	75	2,3,4,5,6,8,9,10	10	10
67	68	2,4,7,8	10	-	71	77	2,3,4,5,6,7,8,9,10	10	10
67	69	2,3,4,5,6,8,9,10	10	-	71	78	2,4,5,8,10	10	10
67	70	2,4,5,7,8,10	10	10					

示例 2. 取与示例 *1* 中相同的组合伪随机数生成器。这里，为了改善等分布，我们根据 s 值组合元胞自动机配置。这个由 k_1=*31* 和 k_2=*32*组成部分构成的组合伪随机数生成器，在 s=*{2, 4, 7, 8}* 时达到最大周期。然而，在最大等分布测试中，表 *7* 至表 *10* 显示，在 *4* s个值中，它仅在 s=*7*和 *8* 时实现最大等分布。因此，这个组合伪随机数生成器 *(31,32)* 在s=*7* 和 *8* 时实现接近 2^{63} 的周期和最大等分布。

表 7：基于元胞自动机的伪随机数生成器 (31,32) 在 s=2 时的等分布

t	l_t^* = 最小值(L, $\lfloor k/t \rfloor$)	l_t ($l_t \leq l_t^*$)	***Rank***	等分布
2	*31*	*31*	*47*	非（t, l）-均匀分布
3	*21*	*21*	*46*	非（t, l）-均匀分布
4	*15*	*15*	*41*	非（t, l）-均匀分布
5	*12*	*12*	*38*	非（t, l）-均匀分布

t	l_t^* = 最小值(L, $\lfloor k/t \rfloor$)	l_t ($l_t \le l_t^*$)	$Rank$	等分布
6	10	10	36	非(t,l)-均匀分布
7	9	9	37	非(t,l)-均匀分布
9	7	7	43	非(t,l)-均匀分布
10	6	6	46	非(t,l)均匀分布
12	5	5	53	非(t,l)均匀分布
15	4	4	60	(t,l)均匀分布
21	3	3	63	(t,l)均匀分布
31	2	2	62	(t,l)均匀分布
63	1	1	63	(t,l)均匀分布

表 8： s=4 的基于元胞自动机的组合伪随机数生成器 (31,32) 的等分布

t	l_t^* = 最小值(L, $\lfloor k/t \rfloor$)	l_t ($l_t \le l_t^*$)	$Rank$	等分布
2	31	31	60	非（t, l）-均匀分布
3	21	21	59	非（t, l）-均匀分布
4	15	15	57	非(t,l)均匀分布
5	12	12	54	非(t,l)均匀分布
6	10	10	58	非(t,l)均匀分布
7	9	9	62	非(t,l)均匀分布
9	7	7	63	(t,l)均匀分布
10	6	6	60	(t,l)均匀分布
12	5	5	60	(t,l)-均匀分布
15	4	4	60	(t,l)-均匀分布
21	3	3	63	(t,l)-均匀分布
31	2	2	62	(t,l)-均匀分布
63	1	1	63	(t,l)-均匀分布

表 9： s=7 的基于元胞自动机的组合伪随机数生成器 (31,32) 的等分布

t	l_t^* = 最小值(L, $\lfloor k/t \rfloor$)	l_t ($l_t \le l_t^*$)	$Rank$	等分布
2	31	31	62	(t,l)-均匀分布
3	21	21	63	(t,l)-均匀分布
4	15	15	60	(t,l)-均匀分布
5	12	12	60	(t,l)-均匀分布
6	10	10	60	(t,l)-均匀分布
7	9	9	63	(t,l)-均匀分布
9	7	7	63	(t,l)-均匀分布
10	6	6	60	(t,l)-均匀分布
12	5	5	60	(t,l)-均匀分布
15	4	4	60	(t,l)-均匀分布
21	3	3	63	(t,l)-均匀分布
31	2	2	62	(t,l)-均匀分布
63	1	1	63	(t,l)-均匀分布

表 10： s=8 的基于元胞自动机的组合伪随机数生成器 (31,32) 的等分布

t	l_t^* = 最小值(L, $\lfloor k/t \rfloor$)	l_t ($l_t \le l_t^*$)	$Rank$	等分布
2	31	31	62	(t,l)-均匀分布

表 10 –

t	$l_t^* =$ 最小值$(L,\ \lfloor k/t \rfloor)$	$l_t\ (l_t \le l_t^*)$	**Rank**	等分布
3	21	21	63	(t,l)-均匀分布
4	15	15	60	(t,l)-均匀分布
5	12	12	60	(t,l)-均匀分布
6	10	10	60	(t,l)-均匀分布
7	9	9	63	(t,l)-均匀分布
9	7	7	63	(t,l)-均匀分布
10	6	6	60	(t,l)-均匀分布
12	5	5	60	(t,l)-均匀分布
15	4	4	60	(t,l)-均匀分布
21	3	3	63	(t,l)-均匀分布
31	2	2	62	(t,l)-均匀分布
63	1	1	63	(t,l)-均匀分布

考虑另一个组合伪随机数生成器（k_1，k_2）=（59，64）；它对于 s 值 2、4、8 实现了接近最大周期，并且对于 s=10实现了最大等分布。因此，这个组合伪随机数生成器（59,64）与 s=10 具有最大等分布，但其周期为

$$\frac{\rho}{10\,\rho} \approx 2^{121} \qquad \rho\ 10\ \neq \gcd(,\ )$$

1 1399

（并不接近最大值），因为 gcd(，)。此外，我们还发现了一些组合，它们不仅具有近最大均匀分布，而且周期也接近 $2^{k_1+k_2}$。我们仅对从 2 到 10 的 s 值进行了实验；如果增加 s的值，计算时间会增加，但可能会得到更多最大等分布组合生成器。

6.2. 考虑 $CA(90')$ 或 $CA(150')$

接下来，我们将接近 32、64 和 128 且时间间隔为 $CA(90')$ 和 $CA(150')$ 的元胞自动机组合起来。这里，只有一个元胞自动机的 N_1 接近其度的一半，其余元胞自动机的度都不接近一半。因此，我们组合表4中给出的所有接近 32、64 和 128 的双分量互素组合。

同样，所有组合伪随机数生成器组合（接近 32、64 和 128）对于那些 s 值，当 gcd(s，ρ) = 1 时，都能达到最大周期。然而，在进行等分布测试时，形式为 $CA(90')$ 与 $CA(90')$ 以及 $CA(150')$ 与 $CA(150')$ 的组合型基于元胞自动机的伪随机数生成器，对于接近 64 和 128 的元胞自动机不满足最大均匀分布性质，但对于接近 32 的元胞自动机则具有近最大均匀分布和最大周期。不过，将 $CA(90')$ 与 $CA(150')$ 组合的生成器，对于接近 32 和 64 的元胞自动机满足最大等分布和最大周期；对于接近 128 的元胞自动机，则具有近最大等分布性质，同时也达到最大周期。这些结果总结于下表11中。

表11：使用 $CA(90')$ 和 $CA(150')$ 的组合伪随机数生成器的等分布

CA	具有最大周期和最大等分布（或接近最大等分布）的组合伪随机数生成器		
	(k_1, k_2, s)：$(90', 90', s)$	(k_1, k_2, s)：$(150', 150', s)$	(k_1, k_2, s)：$(90', 150', s)$
接近 32	几乎达到最大等分布：(26,29,10), (26,35,10), (29,35,10)	几乎达到最大等分布：(26,29,10), (26,35,10), (29,35,10)	最大等分布：(26,29,{5,7,8,10}), (29,26,{5,7,8,10}), (26,35,{5,7,8,10}), (35,26,{5,7,8,10}), (29,39,{6,8,9,10}), (39,29,{6,8,9,10}), (35,39,{6,8,9,10}), (39,35,{6,8,9,10}), (29,35,{5,6,7,8,9,10}), (35, 29, {5, 6, 7, 8, 9, 10})
接近 64	非最大等分布	非最大等分布	最大等分布：(65,69,10), (69,65,10)
接近 128	非最大等分布	非最大等分布	几乎达到最大等分布：(105,113,{9,10}), (113,105,{9,10}), (113,119,10), (119,113,10)

下一节将使用统计测试平台对这些（几乎或）最大等分布组合生成器进行测试。

7. 实验结果与分析

本节介绍所提出的组合型基于元胞自动机的伪随机数生成器的实验结果。分析重点包括以下几个方面：经验测试结果、通过时空图进行验证，以及性能（速度）。

7.1. 经验测试

经验测试用于评估伪随机数生成器的随机性质量。现有多种可用于测试伪随机数生成器的经验测试，包括 $Dieharder$ [20], $SmallCrush$ 和 $BigCrush$ [21] 测试。在本研究中，我们首先对采用时间间隔、具有最大等分布特性的组合最大长度元胞自动机伪随机数生成器进行测试。因此，我们的实验首先在 Dieharder 中测试这些伪随机数生成器：针对表5和表6中提到的所有组合及相应的 s值生成伪随机数，并生成一个大小为 1.5 GB 的二进制文件。

我们观察到，N_1 接近度的一半的组合最大长度元胞自动机伪随机数生成器（表5）未能通过 Dieharder 中的大多数测试。因此，我们不再对其进行 SmallCrush 和 BigCrush 测试。由此可见，这类组合型基于元胞自动机的伪随机数生成器可能实现最大周期和最大等分布，但无法通过统计测试平台。

我们还测试了组合伪随机数生成器，它们在 Dieharder 上几乎达到最大等分布。共有 1399 种组合实现了近乎最大等分布。我们从中选取跳跃步长最小的组合伪随机数生成器；

它们是 (31，33，5)，(31，35，5)，(31，38，5)，(31，39，5)，(31，41，5)，(31，43，5)，(31，46，5)，(31，49，5)，(31，51，5)，(33，43，5)，以及 (33，47，5)。但这些伪随机数生成器在 Dieharder 的大多数测试中均未通过，因此不再进一步测试。

随后，我们使用 CA（90′）和 CA（150′）测试组合型基于元胞自动机的伪随机数生成器，它们如表11所述，满足最大等分布或近最大等分布。我们发现，尽管采用时间间隔、使用 CA（90′）和 CA（150′）的组合型基于元胞自动机的伪随机数生成器能够提供接近最大周期的周期，并满足最大等分布（或近最大等分布），但使用 Dieharder 进行测试时，这些伪随机数生成器并未取得更好的统计测试结果。

表12：线性伪随机数生成器的周期长度、等分布和统计测试结果 s

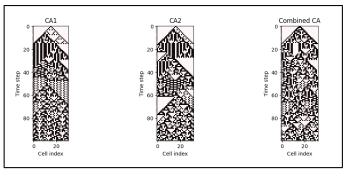
PRNG	周期（$\approx \rho$）	等分布	Dieharder	SmallCrush	BigCrush	
组合式元胞自动机伪随机数生成器（k_1，k_2，s）（ρ 接近最大值）						
(31，32，7)	2^{63}	ME	1	1	11	
(31，32，8)	2^{63}	ME	1	1	7	
(31，40，8)	2^{71}	ME	7	3	16	
(35，48，8)	2^{83}	ME	8	4	19	
(41, 48, 8)	2^{89}	ME	9	2	13	
(43, 48, 8)	2^{91}	ME	5	2	11	
(47，56，8)	2^{103}	ME	4	2	13	
组合元胞自动机伪随机数生成器(k_1, k_2, s)（ρ 不接近最大值）						
(31，32，5)	2^{61}	ME	3	3	20	
(31、32、6)	2^{62}	ME	2	1	15	
(31，32，9)	2^{62}	ME	全部通过	1	6	
(31, 32, 10)	2^{61}	ME	全部通过	2	6	
(31, 40, 9)	2^{70}	ME	全部通过	2	16	
(31，40，10)	2^{69}	ME	全部通过	2	13	
(33, 40, 9)	2^{72}	ME	全部通过	1	15	
(33，40，10)	2^{71}	ME	全部通过	1	14	
(33, 56, 10)	2^{87}	ME	1	3	12	
(35，48，7)	2^{81}	ME	10	5	20	
(35, 48, 9)	2^{80}	ME	1	2	13	
(35, 48, 10)	2^{81}	ME	1	1	13	
(35，64，10)	2^{97}	ME	1	3	11	
(39，40，9)	2^{78}	ME	1	1	13	
(39、40、10)	2^{77}	ME	1	1	11	
(39, 56, 9)	2^{94}	ME	1	2	11	
(39, 56, 10)	2^{93}	ME	1	1	10	
(41, 48, 10)	2^{87}	ME	全部通过	1	13	
(41，64，10)	2^{103}	ME	1	3	12	
(43, 48, 9)	2^{88}	ME	1	1	12	
(43，48，10)	2^{89}	ME	全部通过	1	10	
(43，56，10)	2^{97}	ME	1	1	10	
(45，56，9)	2^{100}	ME	全部通过	1	11	
(45, 56, 10)	2^{99}	ME	全部通过	1	10	
(45，64，9)	2^{108}	ME	2	3	13	
(45, 64, 10)	2^{107}	ME	2	2	10	
(47，56，9)	2^{102}	ME	全部通过	1	11	
(47，56，10)	2^{101}	ME	全部通过	1	11	
(47，64，9)	2^{110}	ME	1	2	12	
(47, 64, 10)	2^{109}	ME	1	2	10	
(47, 72, 10)	2^{117}	ME	1	2	10	
(51, 56, 9)	2^{106}	ME	全部通过	1	12	

伪随机数生成器	周期（$\approx \rho$）	等分布	Dieharder	SmallCrush	BigCrush	
(51, 56, 10)	2^{105}	ME	全部通过	1	10	
（53，56，9）	2^{108}	ME	全部通过	1	11	
(53，56，10)	2^{107}	ME	全部通过	1	11	
(55, 56, 9)	2^{110}	ME	全部通过	1	7	
(55, 56, 10)	2^{109}	ME	全部通过	1	7	
(59, 64, 10)	2^{121}	ME	全部通过	1	11	
(63, 64, 10)	2^{125}	ME	1	1	13	
(63，80，10)	2^{141}	ME	全部通过	3	11	
(67，72，10)	2^{137}	ME	全部通过	全部通过	7	
(71，72，10)	2^{141}	ME	全部通过	2	9	
现有线性伪随机数生成器						
Tausworthe（组合式）	2^{88}	ME	全部通过	全部通过	7	
梅森旋转算法	$2^{19937}-1$	非最大等分布	全部通过	全部通过	3	
WELL512a	2^{512}	ME	全部通过	全部通过	6	
WELL1024a	2^{1024}	ME	全部通过	全部通过	7	

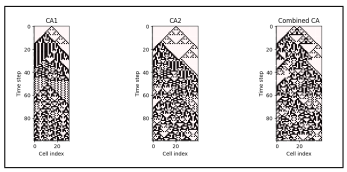
最后，我们使用 Dieharder 测试表6中的组合最大长度元胞自动机伪随机数生成器，其中 N_1 不接近度的一半。共有368种组合达到最大等分布。在这些组合中，以下组合伪随机数生成器通过了 Dieharder 中的大多数测试（超过100项）：$(k_1, k_2, s) =$ (31, 32, $\{5,6,7,8,9,10\}$), (31, 40,$\{8,9,10\}$), (33, 40, $\{9,10\}$), (33, 56, $\{10\}$), (35, 48, $\{7,8,9,10\}$), (35, 64, $\{10\}$), (39, 40, $\{9,10\}$), (39, 56, $\{9,10\}$), (41, 48, $\{8,10\}$), (41, 64, $\{10\}$), (43, 48, $\{8,9,10\}$), (43, 56, $\{9,10\}$), (45, 56, $\{9,10\}$), (45, 64, $\{9,10\}$), (47, 56, $\{8,9,10\}$), (47, 64, $\{9,10\}$), (47, 72, $\{10\}$), (51, 56, $\{9,10\}$), (53, 56, $\{9,10\}$), (55, 56, $\{9,10\}$), (59, 64, $\{10\}$), (63, 64, $\{10\}$), (63, 80, $\{10\}$), (67, 72, $\{10\}$), (71, 72, $\{10\}$)。其中一些组合伪随机数生成器达到最大等分布，且周期接近 $2^{k_1+k_2}$的最大周期；另一些则达到最大等分布，周期为 $\rho/\gcd(s,\rho)$。因此，我们使用 SmallCrush 和 BigCrush 测试这些组合伪随机数生成器。结果如表12所示。随后，我们将这些结果与广为人知的线性伪随机数生成器进行比较，包括 Tausworthe（组合型）、梅森旋转算法、WELL512a 和 WELL1024a。从表12可以看出，我们提出的许多生成器表现与这些标准生成器不相上下，证明了它们作为伪随机数生成器的有效性。

7.2. 使用时空图进行验证

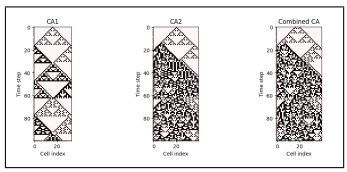
现在，我们使用时空图来探究组合生成器表现良好的原因。时空图以图形方式表示元胞自动机在每个时间步的演化过程。在该时空图中，x 轴表示元胞自动机配置（或伪随机数生成器的状态），y 轴表示时间步。这里，黑色元胞表示状态 1，白色元胞表示状态 0。因此，利用这些时空图，



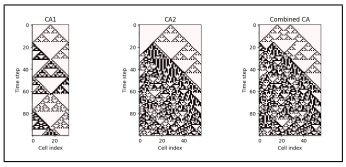
(a) $(k_1,\ k_2)$： (31，32)



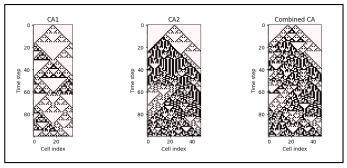
(b) (k_1, k_2) : (31,40)



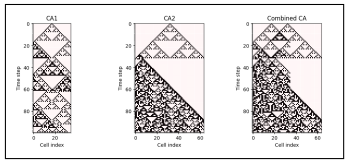
(c) $(k_1,\ k_2)$: (33，40)



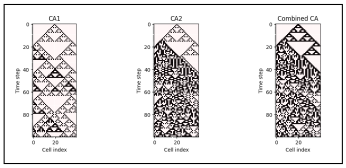
(d) $(k_1,\ k_2)$: （33，56)



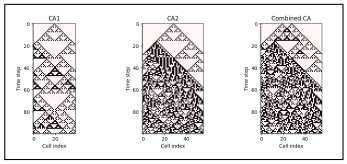
(e) (k_1, k_2) : (35,48)



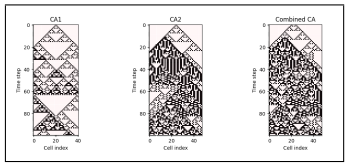
(f) $(k_1,\ k_2)$: （35，64)



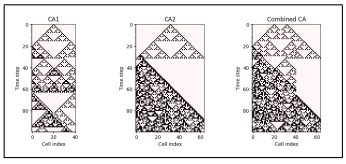
(g) (k_1, k_2): （39,40)



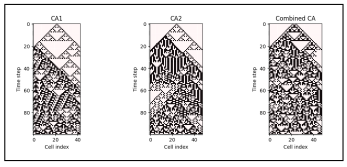
(h) (k_1, k_2) : (39,56)



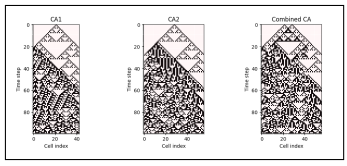
(i) $(k_1,\ k_2)$: （41，48)



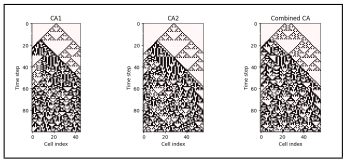
(j) (k_1, k_2): （41,64)



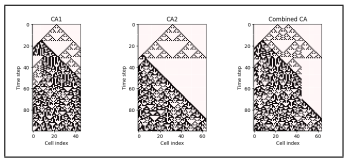
(k) (k_1, k_2): （43,48)



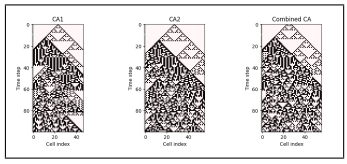
(l)（k_1, k_2）：（43,56）



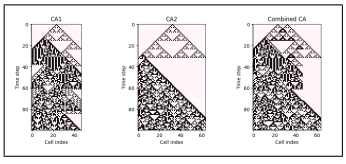
(m) (k_1, k_2) : (45,56)



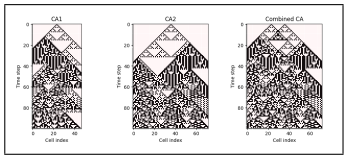
(n) (k_1, k_2) : (45,64)



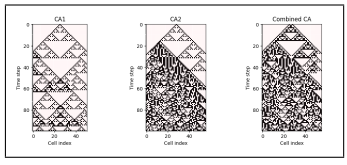
(o) (k_1, k_2) : (47,56)



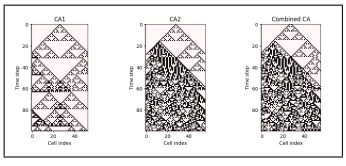
(p) $(k_1,\ k_2)$: （47，64)



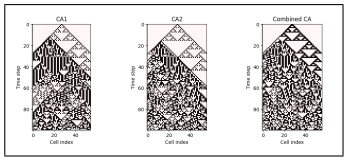
(q) $(k_1,\ k_2)$: (47，72)



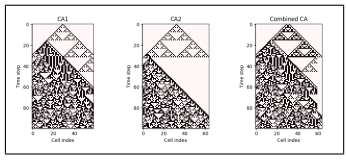
(r) $(k_1,\ k_2)$: （51，56)



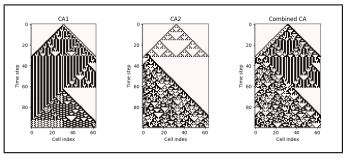
(s) (k_1, k_2) : (53,56)



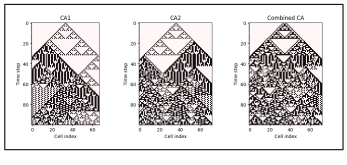
(t) $(k_1,\ k_2)$: （55，56)



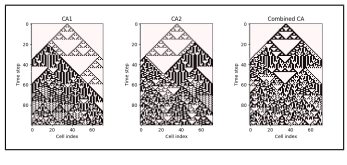
(u) (k_1, k_2): (59,64)



(v) (k_1, k_2) : (63,64)

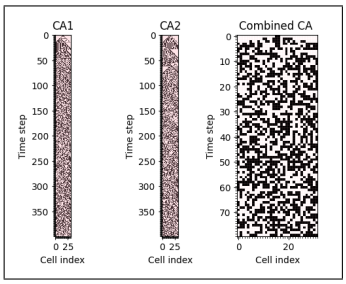


(w) $(k_1,\ k_2)$: （67，72)

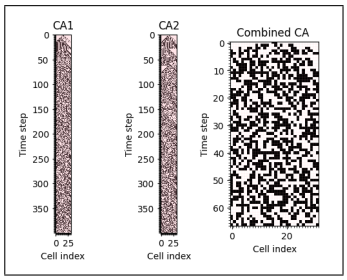


(x) $(k_1,\ k_2)$: （71，72)

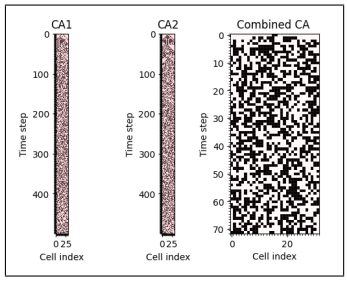
图2：由 $s = 1$ 表12中的30个组成部分构成的组合型基于元胞自动机的伪随机数生成器



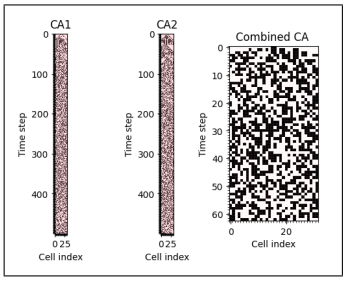
(a) $(k_1,\ k_2,\ s)$: (31，32，5)



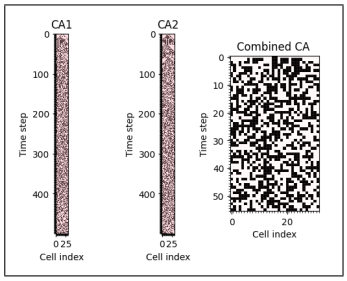
(b) (k_1, k_2, s) : $(31, 32, 6)$



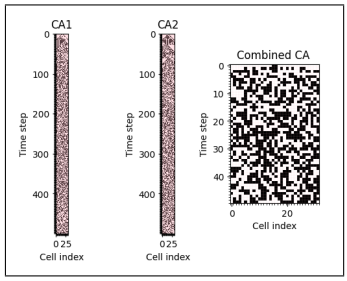
(c) $(k_1,\ k_2,\ s)$: (31，32，7)



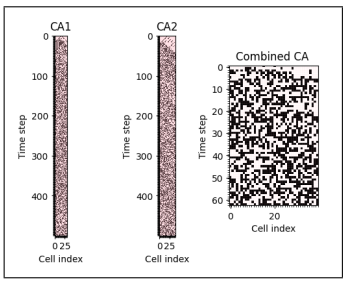
(d) (k_1, k_2, s): （31，32，8)



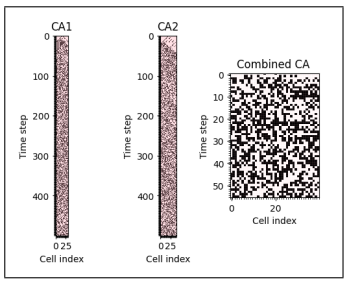
(e) $(k_1,\ k_2,\ s)$: (31，32，9)



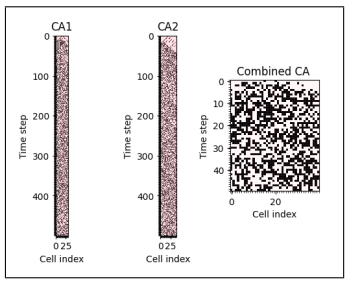
(f) $(k_1,\ k_2,\ s)$: (31，32，10)



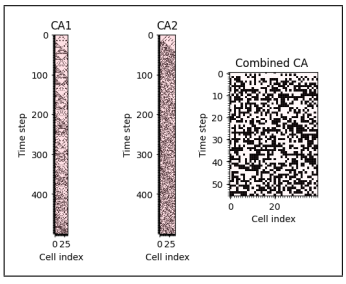
(g) $(k_1,\ k_2,\ s)$: (31，40，8)



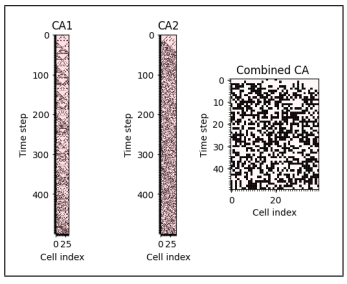
(h) (k_1, k_2, s) : $(31, 40, 9)$



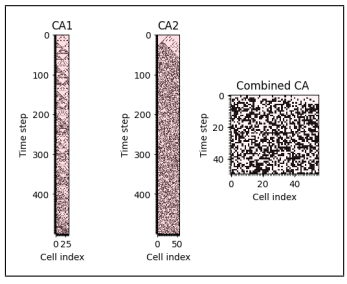
(i) $(k_1,\ k_2,\ s)$: (31，40，10)



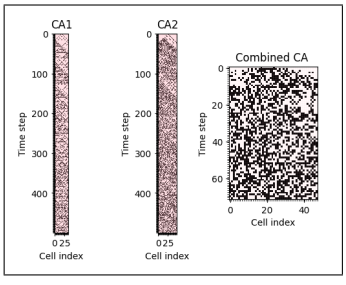
(j) (k_1, k_2, s) : $(33, 40, 9)$



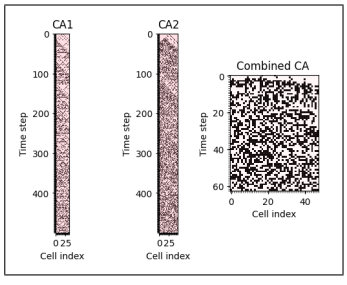
(k) $(k_1,\ k_2,\ s)$: (33，40，10)



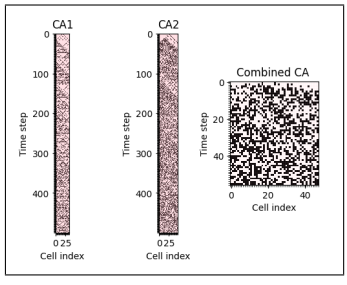
(l) $(k_1,\ k_2,\ s)$: (33，56，10)



(m) (k_1, k_2, s) : $(35, 48, 7)$

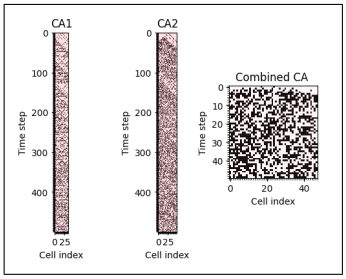


(n) $(k_1,\ k_2,\ s)$: （35，48，8)

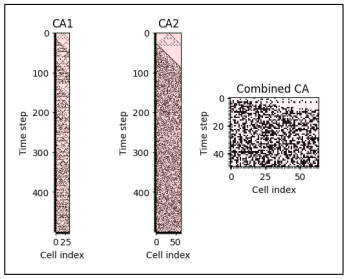


(o) (k_1, k_2, s) : $(35, 48, 9)$

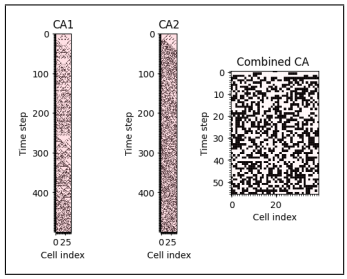
图3：具有时间间隔的组合型基于元胞自动机的伪随机数生成器的时空图



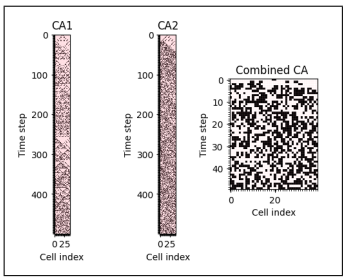
(a) $(k_1,\ k_2,\ s)$: (35，48，10)



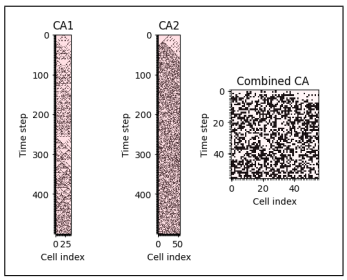
(b) (k_1, k_2, s) : (35, 64, 10)



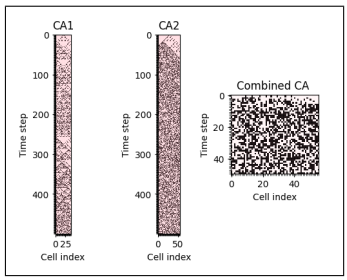
(c) $(k_1,\ k_2,\ s)$: (39，40，9)



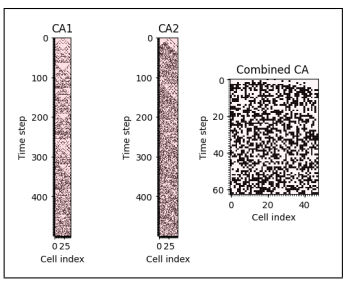
（d）(k_1, k_2, s): （39, 40, 10)



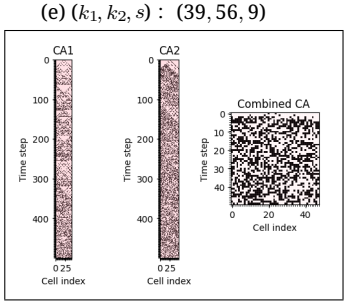
(e) (k_1, k_2, s) : (39, 56, 9)



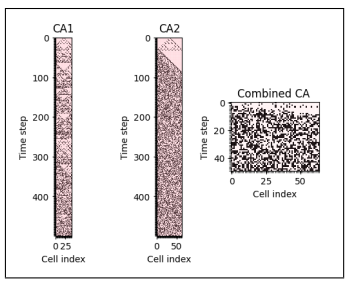
(f) $(k_1,\ k_2,\ s)$: (39，56，10)



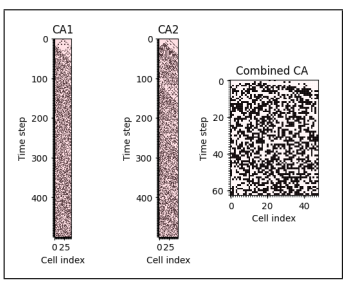
(g) $(k_1,\ k_2,\ s)$: (41，48，8)



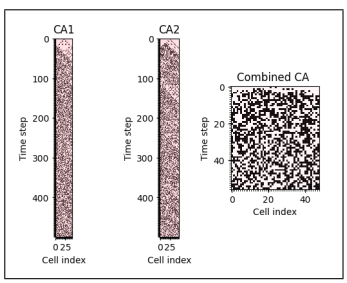
(h) $(k_1,\ k_2,\ s)$: (41，48，10)



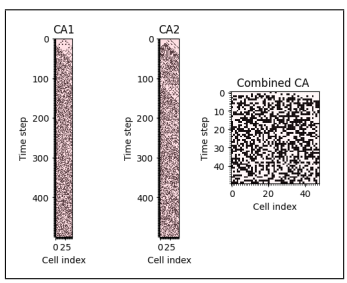
(i) $(k_1,\ k_2,\ s)$: (41，64，10)



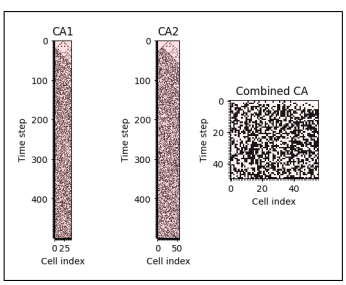
(j) $(k_1,\ k_2,\ s)$: (43，48，8)



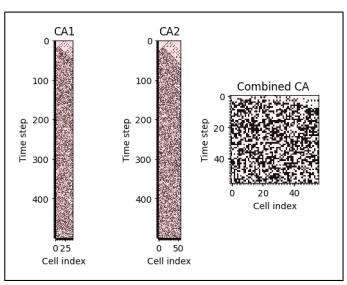
(k) $(k_1,\ k_2,\ s)$: (43，48，9)



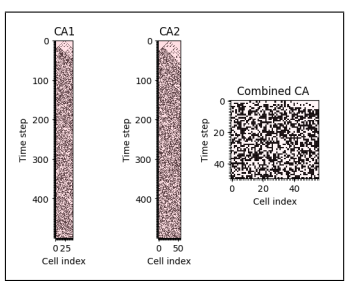
(l) $(k_1,\ k_2,\ s)$: (43，48，10)



(m) $(k_1,\ k_2,\ s)$: (43，56，10)



(n) $(k_1,\ k_2,\ s)$: (45，56，9)



(o) $(k_1,\ k_2,\ s)$: (45，56，10)

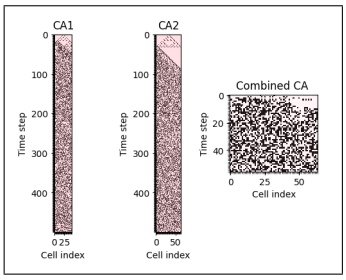
图4：时间间隔下组合型基于元胞自动机的伪随机数生成器的时空图

我们可以根据这些时空图生成的模式，轻松分析元胞自动机的行为 [1]。

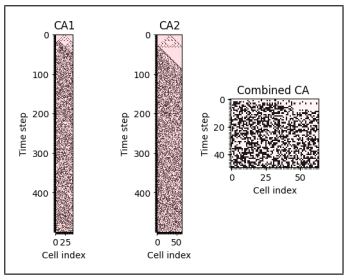
我们检查表12中所有采用时间间隔的组合最大长度元胞自动机伪随机数生成器的时空图，其中将初始配置（种子）设为一种标准的非随机模式：中间比特设为1，其余比特均设为0。首先，我们分别为各个组成部分以及不采用任何时间间隔的组合生成器绘制时空图，如图2所示。可以看到，不使用时间间隔时，元胞自动机组件的自相似模式在组合元胞自动机中也清晰可见。此外，由于采用异或进行组合，组成元胞自动机固有的混沌特性并未在组合元胞自动机中消失。随后，我们为表12中的所有组合伪随机数生成器绘制采用时间间隔的时空图，并比较各个组成部分与组合元胞自动机的行为。在每幅图中，元胞自动机组件均演化500个时间步，并根据 s 的值，在组合元胞自动机中打印出不同随机数的数量。结果如图3至图6所示。从这些图中可以看出，对于所有在统计检验中表现良好的组合，组合生成器时空图中的模式都完全消失，数值呈现出色彩噪声般的效果；这证明了它们具备成为优质随机性来源的能力。

7.3. 速度测试

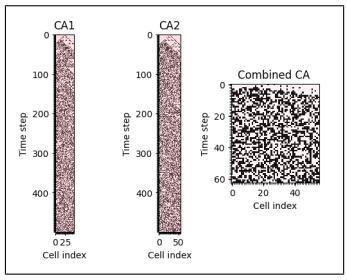
图7展示了我们提出的组合型基于元胞自动机的伪随机数生成器的示例代码。该代码实现了第7.3小节所述的第二种算法。我们在32位和64位计算机上实现并测试了该生成器。性能评估通过测量使用所提出的基于元胞自动机的组合伪随机数生成器生成 10^9 个伪随机数所需的执行时间来进行。正如表12所讨论的，该生成器具有最大周期和最大等分布特性，且统计测试结果良好。随后，我们将这些组合型基于元胞自动机的伪随机数生成器与梅森、GFSR4、WELL 和 Tausworthe 等现有线性生成器的速度进行比较，结果如表13所示。我们发现，我们的伪随机数生成器比梅森旋转算法更快，但比其他不使用任何时间间隔的伪随机数生成器更慢。



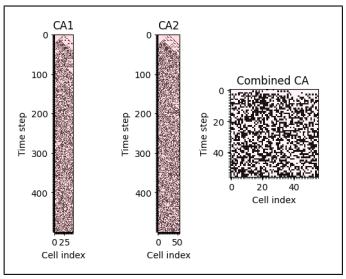
(a) $(k_1,\ k_2,\ s)$: (45, 64, 9)



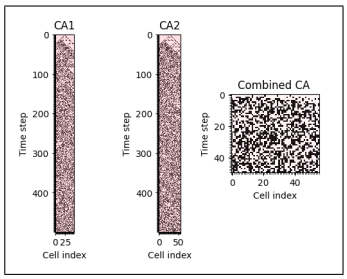
(b) (k_1, k_2, s) : (45, 64, 10)



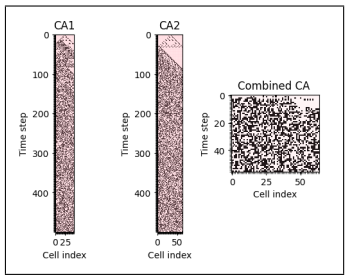
(c) $(k_1,\ k_2,\ s)$: (47, 56, 8)



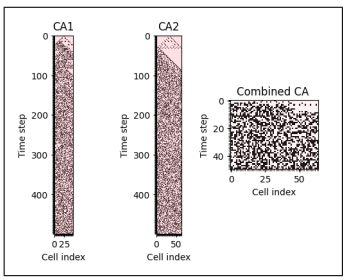
(d) (k_1, k_2, s) : (47, 56, 9)



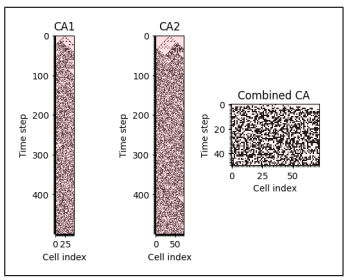
(e) $(k_1,\ k_2,\ s)$: (47, 56, 10)



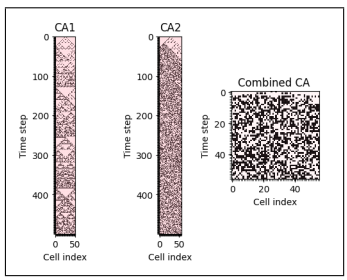
(f) $(k_1,\ k_2,\ s)$: (47, 64, 9)



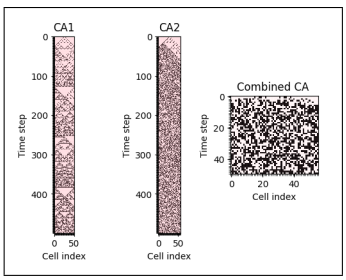
(g) (k_1, k_2, s): (47, 64, 10)



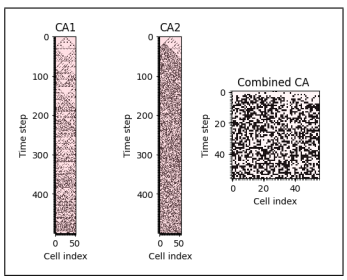
(h) $(k_1,\ k_2,\ s)$: (47, 72, 10)



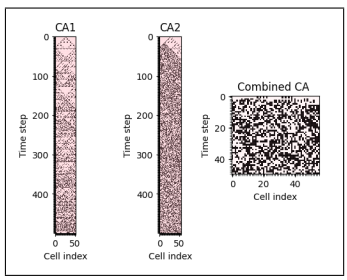
(i) (k_1, k_2, s) : (51, 56, 9)



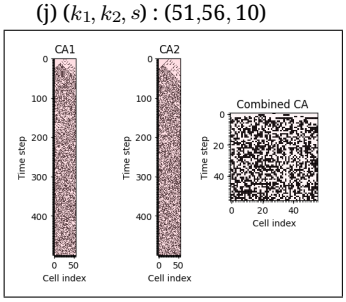
(j) (k_1, k_2, s) : (51,56, 10)



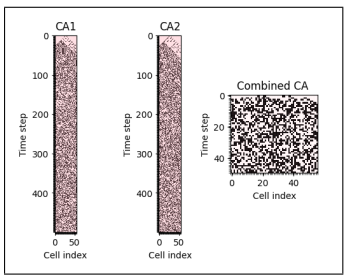
(k) (k_1, k_2, s) : (53, 56, 9)



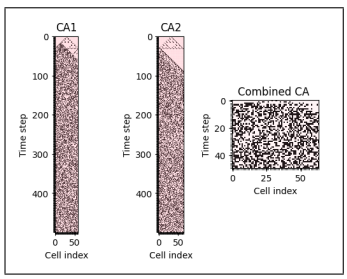
(l) (k_1, k_2, s) : (53, 56, 10)



(m) $(k_1,\ k_2,\ s)$: (55, 56, 9)

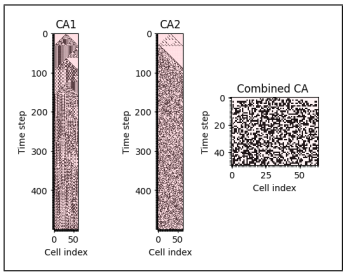


(n) $(k_1,\ k_2,\ s)$: (55, 56, 10)

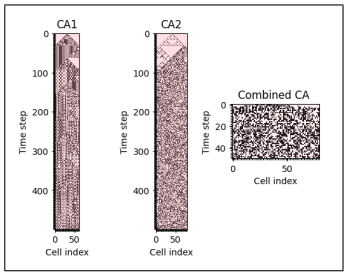


(o) $(k_1,\ k_2,\ s)$: (59, 64, 10)

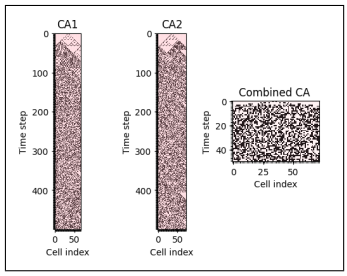
图5：带时间间隔的组合型基于元胞自动机的伪随机数生成器时空图



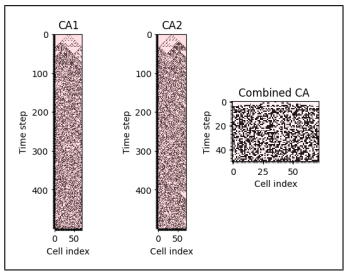
(a) $(k_1,\ k_2,\ s)$：（63，64，10）



(b) $(k_1,\ k_2,\ s)$：（63，80，10）



(c) $(k_1,\ k_2,\ s)$：（67，72，10）



(d) $(k_1,\ k_2,\ s)$：（71，72，10）

图6：具有时间间隔的组合型基于元胞自动机的伪随机数生成器时空图

```
uint64_t pc1, pc2;
int n1, n2, steps, skip, max_len;

uint64_t combined_CA_PRNG()
{
    for (int t = 0; t < steps; t++) {
        if (t % skip == 0)
            x = (pc1 << (max_len - n1)) ^ (pc2 << (max_len - n2));
        pc1 = ((pc1 << 1) & mask1) ^ (pc1 >> 1) ^ (pc1 & rmask1);
        pc2 = ((pc2 << 1) & mask2) ^ (pc2 >> 1) ^ (pc2 & rmask2);
    }
    return x;
}
```

图7：组合式双分量元胞自动机伪随机数生成器

表13：伪随机数生成器的速度比较

PRNG	**周期长度（ρ）**	**CPU 时间（秒）**
元胞自动机伪随机数生成器 (31，32，7)	2^{63}	54
元胞自动机伪随机数生成器 (31，32，8)	2^{63}	60
元胞自动机伪随机数生成器 (31，40，8)	2^{71}	59
元胞自动机伪随机数生成器 (35，48，8)	2^{83}	87
元胞自动机伪随机数生成器 (41，48，8)	2^{89}	83
元胞自动机伪随机数生成器 (43，48，8)	2^{91}	84
元胞自动机伪随机数生成器 (47，56，8)	2^{103}	94
梅森旋转算法	$2^{19937}-1$	116
Tausworthe（组合）	2^{88}	76
GFSR4	–	70

PRNG	周期长度(ρ)	CPU 时间（秒）
WELL512a	$2^{512}-1$	35
WELL1024a	$2^{1024}-1$	42

8. 结论

本文提出了轻量级的组合型基于元胞自动机的伪随机数生成器，它们采用线性最大长度元胞自动机，能够满足最大等分布的理论质量标准。我们从文献 [4, 7] 中选取了两种最大长度元胞自动机，阶数最高可达 128，且其规则向量中使用的不同规则数量最少。不使用时间间隔的基础组合型基于元胞自动机的伪随机数生成器，其周期长度接近最大值，但不具备最大等分布特性。因此，为了改善等分布性，我们在组合型基于元胞自动机的伪随机数生成器中应用时间间隔。为保持其轻量级特性，我们将时间间隔限制在最多 10 步。这些伪随机数生成器不仅周期长度接近最大值，而且实现了最大等分布。随后，我们在 Dieharder 和 TestU01 等基准统计测试平台上开展实验，以评估采用时间间隔的这些组合型基于元胞自动机的伪随机数生成器的统计质量。我们找到了许多组合型基于元胞自动机的伪随机数生成器，它们满足最大等分布要求、周期几乎达到最大值，并且在所有测试平台中通过全部或大部分经验测试。随后，我们表明，这些轻量级组合型线性最大长度元胞自动机伪随机数生成器的性能可与梅森旋转算法及其他若干现有线性生成器相媲美；在等分布性和速度方面，甚至优于梅森旋转算法。不过，由于采用了时间间隔，计算时间有所增加。因此，未来的工作可以致力于设计一种基于元胞自动机的伪随机数生成器，使其周期可与梅森旋转算法或 WELL 相媲美，同时兼具更快的性能和最大等分布特性。

致谢

作者感谢 Sukanta Das 教授以及印度元胞自动机暑期学校 2025 的所有导师一直以来给予的支持、指导和宝贵反馈，这些帮助塑造了本项工作。本研究部分由印度政府通信与信息技术部电子与信息技术部的维斯韦斯瓦拉雅博士生计划资助。

参考文献

[1] Bhattacharjee K, Das S. 寻找优质伪随机数生成器：综述与实证研究。Computer Science Review. 2022 Aug 1;45:100471.[2] Tezuka S. 基于模二多项式算术的随机数生成。报告编号 RT-0017，IBM Research，东京研究实验室。1989 Oct.[3] L'ecuyer P. 最大等分布组合 Tausworthe 生成器。Mathematics of computation. 1996;65(213):203-13.[4] Cattell K, Zhang S. 度数不超过 500 的低成本一维线性混合元胞自动机。Journal of Electronic Testing. 1995 Apr;6(2):255-8.[5] Tezuka S, L'Ecuyer P. 高效且可移植的组合 Tausworthe 随机数生成器。ACM 建模与计算机仿真汇刊（TOMACS）。1991 Apr 1;1(2):99-112.[6] L'Ecuyer P, Panneton F. F2 线性随机数生成器。载于《推进仿真前沿：献给 George Samuel Fishman 的纪念文集》，2009 Jul 17（pp. 169-193）。Boston, MA: Springer US.[7] Adak S, Das S. 在 GF (2) 上生成本原多项式的（不完美）策略。Theoretical Computer Science. 2021 Jun 8;872:79-96.[8] Tausworthe RC. 由模二线性递推关系生成的随机数。Mathematics of Computation. 1965 Apr 1;19(90):201-9.[9]L'Ecuyer P, Panneton F. 基于模 2 线性递推的等分布生成器的构造。载于《Monte Carlo and Quasi-Monte Carlo Methods 2000：2000 年 11 月 27 日至 12 月 1 日在中国香港特别行政区香港浸会大学举行的会议论文集》，2002（pp. 318-330）。柏林，海德堡：Springer Berlin Heidelberg.[10] Bhattacharjee K, More N, Singh SK, Verma N. 基于元胞自动机的梅森旋转算法仿真。Complex Systems. 2023 Apr 1;32(2)。

[11] Panneton F, L’ecuyer P, Matsumoto M. 基于模 2 线性递推的改进型长周期生成器。《ACM 建模与计算机仿真汇刊》。2006年3月1日；32(1):1-6。[12] Matsumoto M, Nishimura T. 梅森旋转算法：一种 623 维等分布均匀伪随机数生成器。《ACM 建模与计算机仿真汇刊》。1998年1月1日；8(1):3-0。[13] Matsumoto M, Kurita Y. 扭曲广义反馈移位寄存器生成器 II。《ACM 建模与计算机仿真汇刊》。1994年7月1日；4(3):254-66。[14] Wolfram S. 物理系统中随机性的起源。《物理评论快报》。1985年7月29日；55(5):449。[15] P. D. Hortensius, R. D. McLeod, W. Pries, D. M. Miller, H. C. Card，基于元胞自动机的内建自测试伪随机数生成器，《IEEE《集成电路与系统计算机辅助设计汇刊》》8 (8) (1989) 842859。[16] Kamilya S, Das S. 非均匀元胞自动机中的混沌研究。《非线性科学与数值模拟通讯》。2019年9月1日；76:116-31。[17] Jaleel HA, Kaarthik S, Sathish S, Bhattacharjee K. 基于元胞自动机的多流并行伪随机数生成。载于：元胞自动机与离散复杂系统国际研讨会，2023年8月24日（第90-104页）。查姆：施普林格·自然瑞士。[18] L’Ecuyer P, Simard R. 用于随机数生成器经验测试的 ANSI C 软件库。技术报告，技术报告，蒙特利尔大学计算机科学与运筹学系；2002年。[19] Marsaglia G. Xorshift 随机数生成器。《统计软件杂志》。2003年7月4日；8:1-6。[20] Brown RG, Eddelbuettel D, Bauer DD. 杜克大学物理系，达勒姆：达勒姆。美国北卡罗来纳州。2018:27708-0305。

[21] L’Ecuyer P, Simard R. 用于随机数生成器经验测试的 ANSI C 软件库。技术报告，技术报告，蒙特利尔大学计算机科学与运筹学系；2002年。[22] Peris-Lopez P, Hernandez-Castro JC, Tapiador JM, Millán ES, van der Lubbe JC. 面向低功耗环境的高效伪随机数生成器中的安全漏洞。载于：新兴无线通信与网络系统安全国际研讨会，2009年9月14日（第25-35页）。柏林，海德堡：Springer Berlin Heidelberg。[23] El Hanouti I, El Fadili H, Souhail W, Masood F. 一种基于鲁棒混沌映射的轻量级伪随机数生成器。载于：2020年第四届数据科学智能计算国际会议（ICDS），2020年10月21日（第1-6页）。IEEE。[24]Shuming Han, Ke Huang, Yuling Luo，一种基于 Logistic 映射的高效轻量级伪随机数生成器，载于 SPIE 13630 论文集，第四届高性能计算与通信工程国际会议（HPCCE 2024），1363006（2025年5月9日）。[25]Bhattacharjee, K.: 元胞自动机：可逆性、半可逆性与随机性。博士论文，IIEST，希布尔（2019），http://arxiv.org/abs/1911.03609