The 11th Workshop on Finite Field Theory
and its Application for Pseudo-Random
Sequences (FFTPRS2025)
Hita (Hybrid), September 16-17, 2025

# 迷路法の削岩可能面積と迷路の種類数の関係に関する一考察

# A Study of Relations between Diggable Areas and a Number of Maze Types for Maze Methods

宮崎 武 * 荒木 俊輔 † 上原 聡 ‡
Takeru Miyazaki Shunsuke Araki Satoshi Uehara

**Abstract**— In this paper, we present the results of an investigation into the relation between the number of small-sized maze types and the diggable areas of the maze in the Maze Methods, and provide an estimate of the number of maze types for large-sized mazes that are actually used.

**Keywords**— Deterministic Maze Method, Pseudorandom Number Generator, Maze Types Estimation

## 1 はじめに

乱数は，予測できない値の羅列である．これは公開されない限り生成した本人でしか知りえない情報であり，また一部が公開された後であってもその後にどのような乱数が生成されるのかを予測するのが困難なものである．このような性質があることから，乱数はしばしば情報セキュリティ技術を支える基盤技術の 1 つとして利用されている．物理的な装置やノイズの観測などによって乱数を生成することも可能だが，このような物理乱数は偏りも大きく専用の装置が必要となる．そこで，計算機によって効率的に，かつ，低コストで乱数を生成するため擬似乱数生成器が使用される．擬似乱数は，確定的な計算によって得られる，「乱数と似た性質を持つ系列」である．一般的に，理想的な乱数が持つ性質に似た性質を持つように設計されている．このような理想的な乱数が持つ性質を乱数性といい，擬似乱数がこの乱数性をどれぐらい保持しているのかを様々な方法で調査する．特に統計的な複数の乱数性検定をまとめて行う NIST 検定 [2] などが擬似乱数性の乱数性評価方法として用いられる．

擬似乱数生成器に用いる系列の生成方法としては，様々な提案がなされている．例えば，Shift 演算や XOR 演算といった高速に実行できる演算を組み合わせた XOR Shift [3] や，線形合同法 [4]，二次合同法 [5] など剰余算を用いたもの，カオス系列を計算機上で演算する方式 [6–9] などが挙げられる．我々は，これまでとは異なる新たな擬似乱数生成方式として，「迷路法」を提案した [10, 11]．これは，穴掘り法という迷路作成アルゴリズム [1] を用いた擬似乱数ビット系列の生成法をである．これは作成した迷路によって得られた壁と通路をそれぞれ ‘1’ と ‘0’ のビットに見立てて，擬似乱数ビット列を抽出するものである．また，ごく小さな迷路サイズからでも多数の擬似乱数系列が生成できることについて，理論的な解析も行った [12]．さらに，これを確定的な迷路構成方法とする方式の提案 [13] や，より小さなサイズで同等以上の種類数が構成できるような新しい迷路生成法である外壁のない（連結された）迷路を使用する方式の提案 [14, 15] を行った．

本稿では，ICC-TW2025 のポスターセッション [15] にて発表した内容に基づき，[13] および [14] で提案した方式について，小さなサイズの迷路における全探索により生成可能な迷路の種類数を調査する．また，それぞれの迷路生成方式について，削岩可能面積と迷路種類数のビット数表現の間に直線近似が可能であることを発見した．この近似が正しいとすれば，実際に擬似乱数生成器で使用するような巨大な迷路における迷路種類数の推定値がどの程度になるのかを求めた．

## 2 連結された（外壁のない）迷路法

### 2.1 既存方式

我々は，これまで迷路法と呼んでいる擬似乱数生成器 [11], や確定的な迷路構成方法 [13], を提案してきた．しかしながら，これらの提案方式では，迷路の外壁と呼んでいる迷路の端にある部分は常に壁であり擬似乱数生成には何も反映されない．我々は，この利用されていない部分に着目した．新しい提案方式では，迷路サイズを奇数 × 奇数から偶数 × 偶数に変更し，また迷路の上下端および左右端を接続する．これにより，より小さな迷路サイズで多くの種類の迷路を生成することができる．迷路法において，迷路の形状と生成できる擬似乱数系列は一対一の対応関係がある．よって，迷路の種類数と生

* 〒 818-0117 福岡県太宰府市宰府 6 丁目 3-1 九州情報大学経営情報学部, Faculty of Management and Information Sciences, Kyushu Institute of Information Sciences, 6-3-1 Saifu, Dazaifu, Fukuoka 818-0117, Japan. Email : t-miyazaki@kiis.ac.jp
† 〒 820-8502 福岡県飯塚市川津 680-4 九州工業大学大学院情報工学府, Graduate School of Computer Science and Systems Engineering, Kyushu Institute of Technology, 680-4 Kawazu, Iizuka, Fukuoka 820-8502, Japan.
‡ 〒 808-0135 福岡県北九州市若松区ひびきの 1-1 北九州市立大学国際環境工学部, Faculty of Environmental Engineering, The University of Kitakyushu, 1-1 Hibikino, Wakamatsu, Kitakyushu, Fukuoka 808-0135, Japan.

成できる擬似乱数系列の生成数は同一であり，より小さな迷路サイズから多くの擬似乱数系列を生成することが可能となる．

### 2.2　提案する擬似乱数生成器

本稿で提案する擬似乱数生成器のアルゴリズムを以下に示す。

1. 幅を $2w$,，高さ $2h$ と定数 $R$ をする．
2. $2w \times 2h$ サイズの長方形型の壁を配列 $A[2w, 2h]$ として準備する．
3. $A[1, 1]$ を通路に変える．
4. (奇数，奇数) 地点が通路である地点から上下左右に 2 連続で壁が連結している (ただし，上下と左右の端は連結しているものとする) 箇所を全て探し，その座標を候補配列 $C$ に入れる．
5. $C$ に一つも候補が無くなったらステップ 7. に進み，それ以外は次のステップに進む．
6. $C[R \bmod t]$ に格納されている 2 連続の壁 $A[x, y]$ を通路に変える．ただし，$t$ は $C$ に格納された候補数である．その後で，$C[i]$ から先程通路に変えた $A[x, y]$ を含む候補を全て取り除き，$C$ の順番を詰めて整理し，ステップ 4. に戻る．
7. 全ての (奇数, 偶数) および (偶数，奇数) 座標から，壁を ‘1’ として，通路を ‘0’ としてビット抽出する．

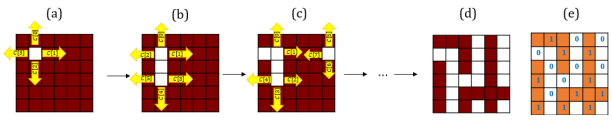


図 1: 小さな $6 \times 6$ サイズでの擬似乱数ビット列生成例

図 1 は縦，横がどちらも 6 で $R = 2$ とした場合の提案方式の小さな例を示したものである．

$6 \times 6$ の正方形型配列を全て壁にしておく．最初に，$A[1, 1]$ を通路にする．次に，(奇数，奇数) 地点が通路である地点から削岩できる候補を探す．この例では，上から時計回りの順番で方向を考える．最初は，候補を考える地点は $(1, 1)$ からしか存在しない．このとき，この地点からそれぞれ 4 方向に 2 連続で壁を掘ることができるから，図 1-(a) で示したような 4 つの候補が得られる．つまり，$C[0]$ は上下端が連結していることを考えれば，$(1, 1)$ から上方向は $(1, 0)$ と $(1, 5)$ である．また，$C[1]$ は $(1, 1)$ から右方向に $(2, 1)$ と $(3, 1)$ で，$C[2]$ は $(1, 1)$ から下方向に $(1, 2)$ と $(1, 3)$ である．そして，$C[3]$ は，左右端が連結していることを考えれば $(1, 1)$ から左方向に $(0, 1)$ と $(5, 1)$ である．4 つの候補があるので，$t = 4$ であり，これから $R \bmod t = 2$ であるから，ステップ 6. においてこれら 4 つの候補の中から $C[2]$ が選択される．

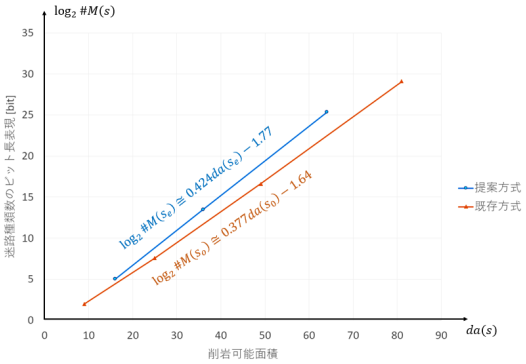


図 2: 削岩可能面積と迷路の種類数の関係

よって，$C[2]$ の 2 つの壁，言い換えれば $A[1, 2]$ と $A[1, 3]$ の 2 か所の壁を通路に変える．そして，$C[2]$ は候補から削除され，$t = 3$ となり，また $C[2] \leftarrow C[3]$ のように整理する．

次に，先程掘った箇所からの新しい候補を探す．新しい (奇数，奇数) 地点である $(3, 1)$ から右，下，左方向に掘ることが可能であるから，これらを順に $C[3], C[4]$ と $C[5]$ として追加する．この時点で，図 1-(b) のようになり，$t = 6$ である．再び，ステップ 6. において $C[2]$ に格納されている候補が選ばれ，$A[0, 1]$ と $A[5, 1]$ が通路となる．そして再度候補の整理と新しい候補を追加したものが図 1-(c) に示したものとなる．この処理を全ての候補が無くなるまで繰り返すと，全ての (奇数，奇数) 地点が通路になる．その結果を図 1-(d) に示す．この後，全ての (奇数, 偶数) および (偶数，奇数) 座標から順番に見て，壁を ‘1’ として，通路を ‘0’ と変換したものを図 1-(e) に示す．これより，‘1000110001010111111’ という 18 ビットの系列をこの迷路から抽出することができた．

### 2.3　構成可能な正方形型迷路種類数の推定

次に，既存方式 [13] と提案方式の正方形型迷路における迷路の種類数推定を行う．ここで，迷路種類数 $\#M(s)$ を，1 辺が $s$ の正方形型迷路における迷路の構成可能な種類総数と定義する．ただし，提案方式の $R$ の設定を変えても生成することが出来ない迷路も含むものとする．これは，将来的に $R$ の選択方法を定数から変化させた場合にも対応するためである．本稿では，この $\#M(s)$ を $s$ を用いた近似式で表現することを目指す．最初に，小さな正方形型迷路の全探索により $\#M(s)$ を調査する．一辺が，$s_o$ (奇数) のものは $s_o \leq 11$ の範囲で調査した．また，$s_e$ (偶数) のものは $s_e \leq 10$ の範囲を調査することを試みたが，しかし $s_e = 10$ の場合に全ての候補数である約 $1.21 \times 10^{14}$ 個を調査することができず，途中までであるが少なくとも $10^{10}$ 個の迷路が存在していることを確認できたに留まっている．

表 1 は，これらの結果をまとめたものである．ここで，削岩可能面積 $da(s)$ は，迷路から削岩することができない外壁部分を取り除いた面積を意味する．よって，既存方式では，$da(s_o)$ では 1 辺が $s_o$ の正方形に対してその外壁部分を除いた $(s_o-2)^2$ と表せられる．また，提案方式では $da(s_o)$ では 1 辺が $s_e$ の正方形に対して外壁部分は無く全て削岩可能だから ${s_e}^2$ となる．

表 1: 小さな正方形迷路での迷路種類数

| 既存方式 [13] | | | 提案方式 | | |
|---|---|---|---|---|---|
| $s_o$ | $da(s_o)$ | $\#M(s_o)$ | $s_e$ | $da(s_e)$ | $\#M(s_e)$ |
| 3 | 1 | 1 | 2 | 4 | 1 |
| 5 | 9 | 2 | 4 | 16 | 6 |
| 7 | 25 | 42 | 6 | 36 | 312 |
| 9 | 49 | 5918 | 8 | 64 | 54276 |
| 11 | 81 | 6499660 | 10 | 100 | $(>10^{10})$ |

この表 1 において，それぞれの行を参照すれば左側の既存方式に対して縦横がそれぞれ 1 つずつ小さな迷路である右側の提案方式は迷路の種類数が同数かより多くなっていることと，その差は迷路サイズが大きくなるに連れて増大していることが確認できる．

この結果から，より大きな迷路における $\#M(s)$ を推定する．我々は．既存方式と提案方式どちらにおいても，迷路種類数のビット数表現，つまり，2 を底とした対数で表現された値が，$da(s)$ と直線近似できることを発見した．図 2 にそれぞれの関係を示す．この図において，水平軸は $da(s)$ の値を意味し，垂直軸は $\#M(s)$ のビット数表現である．

この図より，既存方式の迷路種類数推定値 $\#M(s_o)$ と提案方式の迷路種類数推定値 $\#M(s_e)$ はそれぞれ以下のような式で表現できる．

$$\#M(s_o) \simeq 2^{0.377(s_o-2)^2-1.64} = 0.321 \times 2^{0.377(s_o-2)^2},$$
$$\#M(s_e) \simeq 2^{0.424{s_e}^2-1.77} = 0.294 \times 2^{0.424{s_e}^2}.$$

この推定値が正しいとすれば，$\#M(s_e)$ の $s_e = 10$ における推定値は，

$$\#M(10) = 0.294 \times 2^{42.4} > 2^{40} > 10^{12}.$$

となり，全探索を完了させるには困難な値であったことが推測できる．

また，もしこの推定値が迷路サイズが大きくなっても正しいと仮定すれば，迷路 1 辺が $s_e = 1000$ のときその種類数は約 42 万ビットであり，迷路 1 辺が $s_e = 10000$ のときその種類数は約 4200 万ビットだと推測できる．

## 3 まとめ

本稿では，我々は連結した外壁のない迷路を用いた新しい迷路を用いた擬似乱数生成器の提案を行った．そして，我々は提案方式が既存方式よりも小さな迷路サイズからより多くの種類の系列を生成できることを示した．また，小さな迷路において削岩可能面積と迷路種類数のビット数表現に直線近似が出来るという関係を示し，迷路のサイズから迷路種類数の推定値を求めた．これから，より大きな迷路である 1 辺が 1000 や 10000 であるときの迷路種類数について考察した．今後の課題は，提案方式より得られた擬似乱数系列についてより詳細な論理的乱数性検証を行うことである．

## 参考文献


[1] S. Ishida, “迷路自動生成アルゴリズム,” *https://www5d.biglobe.ne.jp/ stssk/maze/make.html,* 最終閲覧日 2025/9/12.

[2] NIST, “A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications,” Special Publication 800-22 Rev.1a, 2008.

[3] G. Marsaglia, “Xorshift RNGs,” Journal of Statistical Software Vol.8, 2003.

[4] 木村, 斎藤, “線形合同法による暗号化用擬似乱数生成法, ” 数理解析研究所講究録, 1504 巻, pp.123-135, 2006.

[5] D. Knuth, “Generating Uniform Random Numbers,” *The Art of Computer Programing,* 3rd edition, Vol. 2, pp.10-40, 1997.

[6] T. Miyazaki, S. Araki, and S. Uehara, “Some Properties of Logistic Maps over Integers,” *Special Section on Signal Design and its Application in Communications,* IEICE Trans. Fundamentals, Vol.E93-A, No.11, pp.2258-2265, 2010.

[7] T. Miyazaki, S. Araki, Y. Nogami, and S. Uehara, “Rounding Logistic Maps over Integers and the Properties of the Generated Sequences,” IEICE Trans. Fundamentals, Vol. E94-A, No.9, pp.1817-1825, 2011.

[8] 宮崎, 荒木, 上原, 野上, “整数上のロジスティック写像による擬似乱数生成器における部分系列カオス尺度を用いた乱数性の改善法,” 日本応用数理学会年会, 応用カオス (1)-4, 2021.

[9] S. Eguchi, T. Miyazaki, S. Uehara, S. Araki, Y. Nogami, “A Study on Relationship Between Period and Number of Divisions in Piecewise Logistic Map over Integer,” IEEE International Con-

ference on Consumer Electronics - Taiwan(ICCE-TW2021), 2021

[10] 宮崎, 荒木, 上原, “穴掘り法による迷路を用いた擬似乱数生成における迷路サイズと種類数に関する一考察,” 2023 年暗号と情報セキュリティシンポジウム (SCIS2023), 2C3-3, 2023.

[11] T. Miyazaki, S. Araki, S. Uehara, “How to Construct Pseudorandom Bit Sequences from Mazes by a Method Digging Out Walls,” IEEE International Conference on Consumer Electronics - Taiwan(ICCE-TW2023), E8-8, 2023

[12] 宮崎, 荒木, 上原, “迷路法によって生成される系列の種類数の理論的解析に関する一考察,” 第 9 回有限体理論とその擬似乱数系列生成への応用ワークショップ (FFTPRS2023), 講演 6 , 2023.

[13] T. Miyazaki, S. Araki, S. Uehara, “A Study on a New Pseudorandom Number Generator with Deterministic Maze Construction,” IEEE International Conference on Consumer Electronics - Taiwan(ICCE-TW2024), E4-3, 2024

[14] 宮崎, 荒木, 上原, “外壁の無い確定的な迷路法による擬似乱数生成法に関する一考察,” 第 10 回有限体理論とその擬似乱数系列生成への応用ワークショップ (FFTPRS2024), 講演 7 , 2024.

[15] T. Miyazaki, S. Araki, S. Uehara, “A Pseudorandom Number Generator by Maze Method without Outer-Walls,” IEEE International Conference on Consumer Electronics - Taiwan(ICCE-TW2025), Poster Session B PB07, 2025