

# 貴金属比サンプリングを用いた 疑似乱数発生アルゴリズム

大田 龍弥      桑名 杏奈

片山 翔吾      小林 春夫

群馬大学 理工学府 電子情報部門

# 目次

- はじめに
- 従来の乱数発生法
- 貴金属比サンプリングを用いた  
疑似乱数発生アルゴリズムの提案
- 研究内容
  - 従来法との比較
  - 1方向貴金属法
  - 2方向貴金属法
- まとめと今後の課題

# 目次

- はじめに
- 従来の乱数発生法
- 貴金属比サンプリングを用いた  
疑似乱数発生アルゴリズムの提案
- 研究内容
  - 従来法との比較
  - 1方向貴金属法
  - 2方向貴金属法
- まとめと今後の課題

# 目的

貴金属比を用いて作成した数列を  
モンテカルロシミュレーションの乱数として  
使用できないか、評価を行う  
(暗号化に用いることはできない)

# 乱数とは

- 乱数列

全く無秩序に、しかも出現の確率が同じになるように並べられた数字の列

(デジタル大辞泉「乱数」より引用)

- 乱数

乱数列の各要素

- Ex, サイコロ

「1 4 5 5 6 2 4 1 3...」

乱数

乱数列

# 貴金属比とは

- $1 : \frac{n + \sqrt{n^2 + 4}}{2}$  で表される比率のこと
- $n=1$  の時を黄金比  
(第1貴金属比)
- $n=2$  の時を白銀比  
(第2貴金属比)
- $n=3$  の時を青銅比  
(第3貴金属比)
- $\frac{n + \sqrt{n^2 + 4}}{2}$  を 貴金属数 と呼ぶ

# なぜ貴金属比を用いるのか

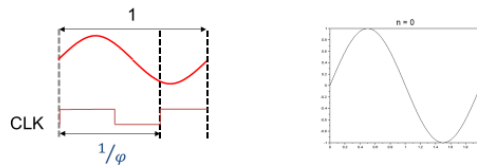
バランスが良い

Our Proposed Optimal Condition

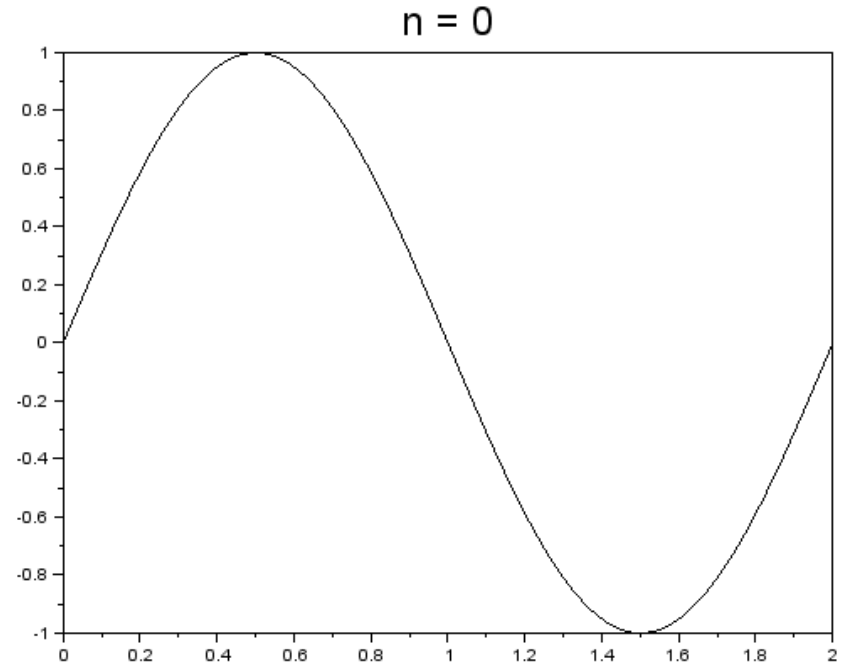
5/77

$$f_{CLK} = \varphi \times f_{sig}$$

$\varphi$  : Golden ratio (= 1.6180339887...)



Sampling points disperse uniformly through measurement



(出典: H Kobayashi,

“Time Domain Signal Processing Techniques and Their Applications”,  
ICMEMIS2019, Dec 2019 )

# 目次

- はじめに
- 従来の乱数発生法
- 貴金属比サンプリングを用いた  
疑似乱数発生アルゴリズムの提案
- 研究内容
  - 従来法との比較
  - 1方向貴金属法
  - 2方向貴金属法
- まとめと今後の課題



# 線形合同法

$$x_{n+1} = (ax_n + b) \bmod m \quad (m > a, b \quad a > 0 \quad b \geq 0)$$

によって、発生される乱数列。

- 実用的なアルゴリズムではメモリが最小
- ExcelやC言語のrand関数に用いられる
- 多次元では規則的に分布されるので暗号化には使用できない

# メルセンヌ・ツイスタ(MT)法

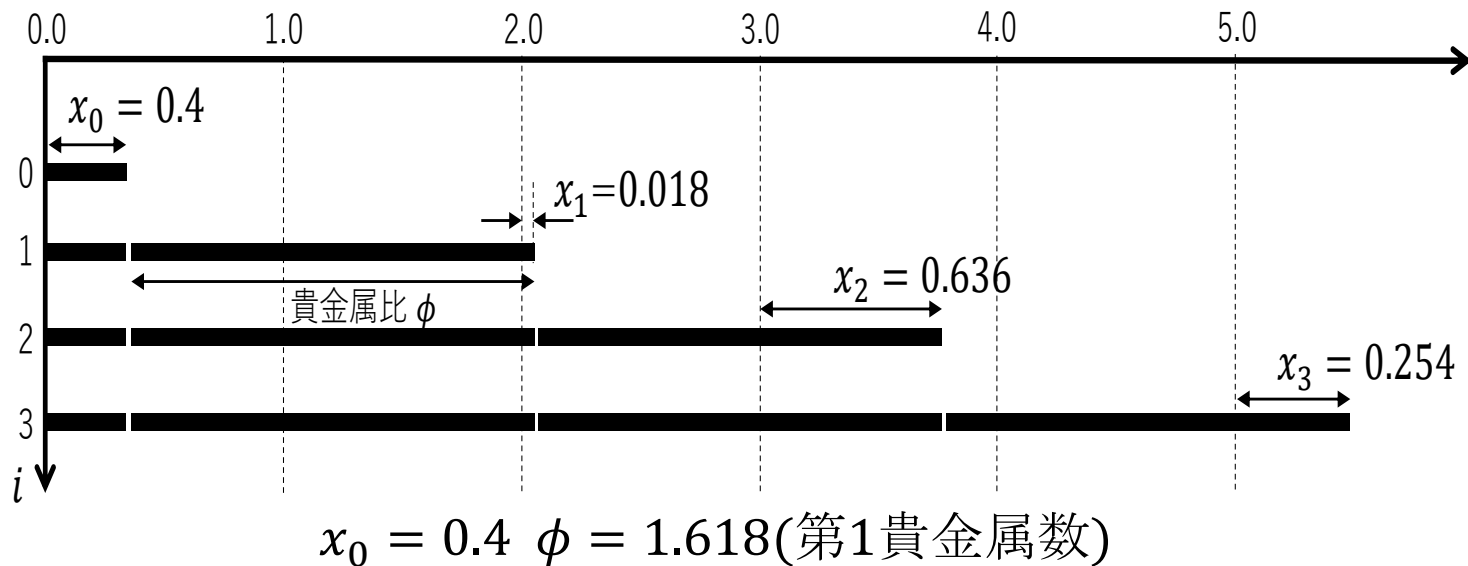
- 1996年に国際会議で発表された方法
- 擬似乱数の生成速度が速い
- 周期が $2^{19937} - 1$

# 目次

- はじめに
- 従来の乱数発生法
- 貴金属比サンプリングを用いた  
疑似乱数発生アルゴリズムの提案
- 研究内容
  - 従来法との比較
  - 1方向貴金属法
  - 2方向貴金属法
- まとめと今後の課題

# 命名「貴金属法」

- 任意の貴金属数を $\phi$ 、 $x_0$ を0.0~1.0
- $x_{i+1} = (\phi + x_i) - [\phi + x_i]$   
によって乱数列を生成する
- この方法を貴金属法と呼ぶ



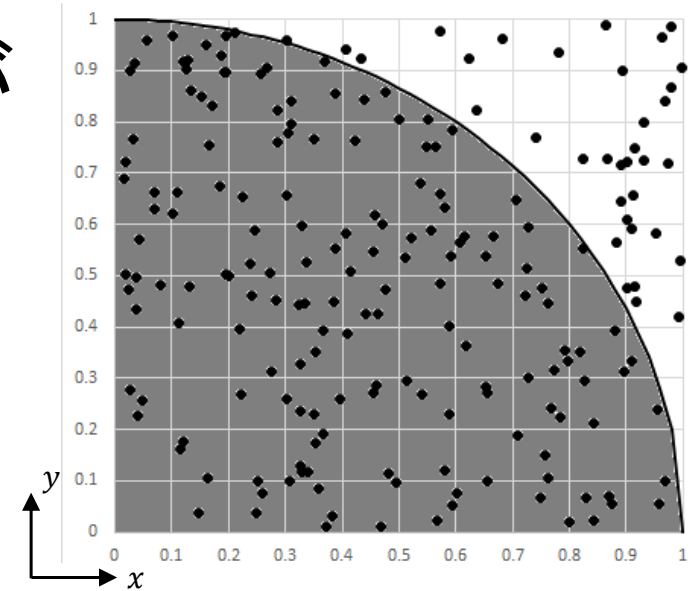
# 目次

- はじめに
- 従来の乱数発生法
- 貴金属比サンプリングを用いた  
疑似乱数発生アルゴリズムの提案
- **研究内容**
  - 従来法との比較
  - 1方向貴金属法
  - 2方向貴金属法
- まとめと今後の課題

# モンテカルロ・シミュレーション

- 0.0~1.0内に発生される点が円内にある確率は面積比に近似できる

$$\frac{\text{円内の点数}}{\text{発生点数}} = \text{面積比}$$



- 今回、測定結果を4倍にすることで近似される値は $\pi$ になる

# 従来法との比較

- 比較対象

rand関数 MT法 規則的に並べたもの

1方向貴金属法 2方向貴金属法

- rand関数、MT法のシード値を**10**に固定

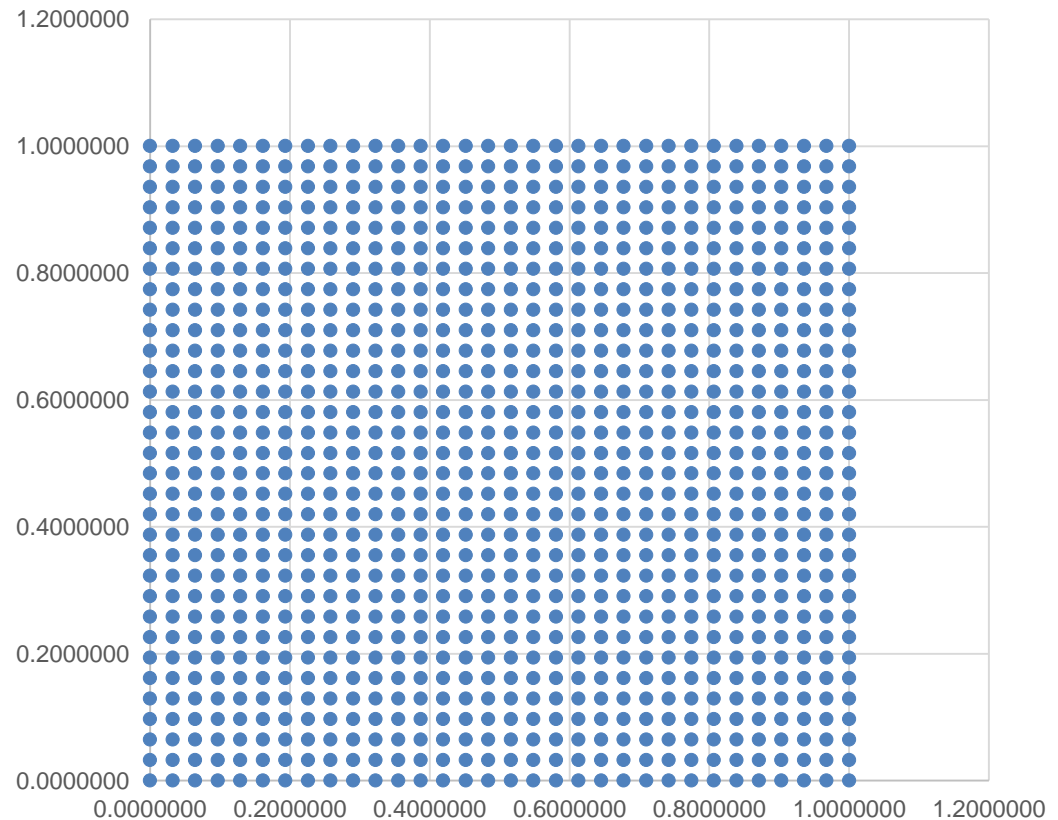
1方向貴金属法→第1貴金属数(黄金比)

2方向貴金属法→第1貴金属数(黄金比)

と第2貴金属数(白銀比)

# 規則的

- 比較対象として用いる
- 点同士の距離が等間隔



$N = 1024$



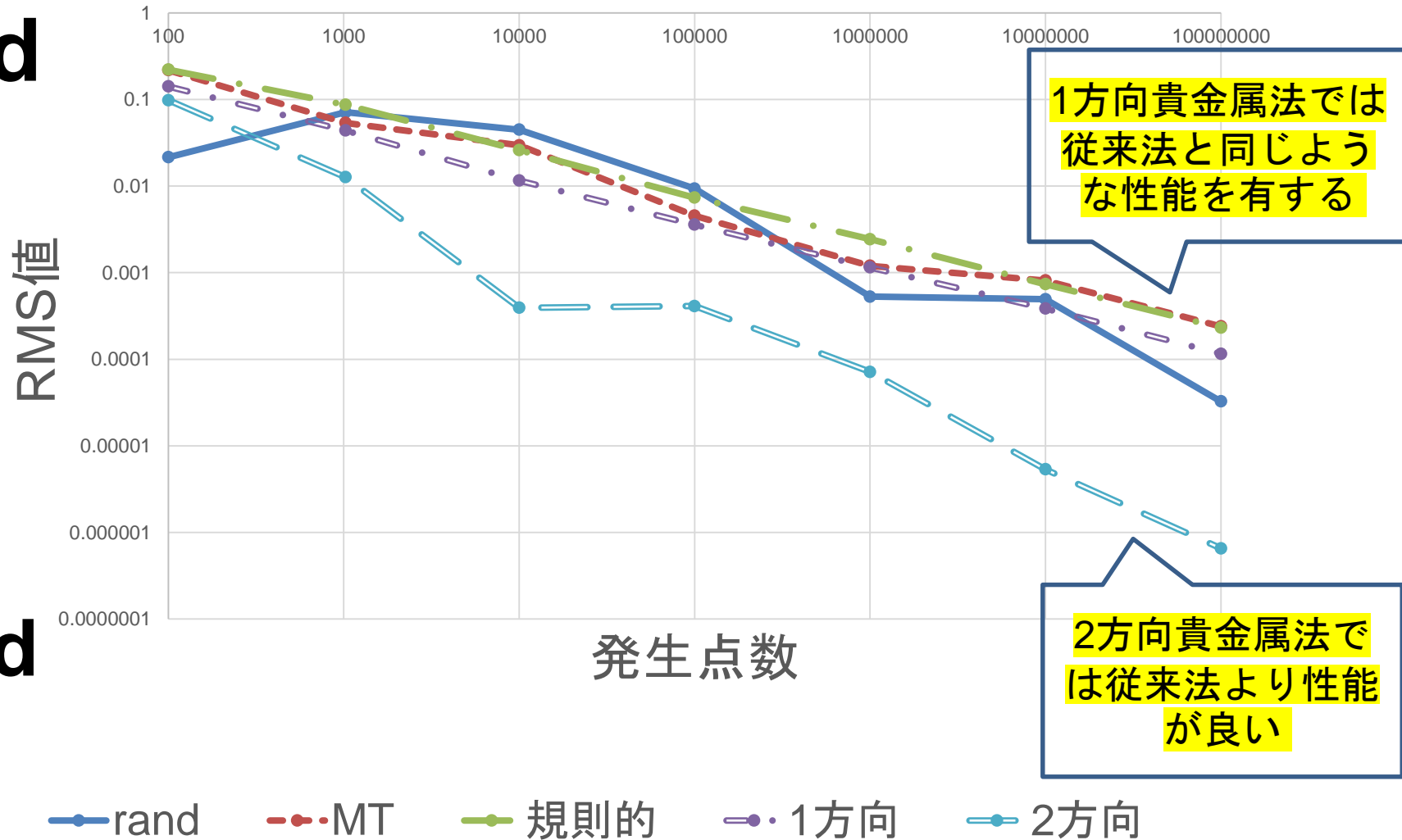
# 従来法との比較(計算結果)

**Bad**

↑

↓

**Good**



# 目次

- はじめに
- 従来の乱数発生法
- 貴金属比サンプリングを用いた  
疑似乱数発生アルゴリズムの提案
- **研究内容**
  - 従来法との比較
  - **1方向貴金属法**
  - 2方向貴金属法
- まとめと今後の課題

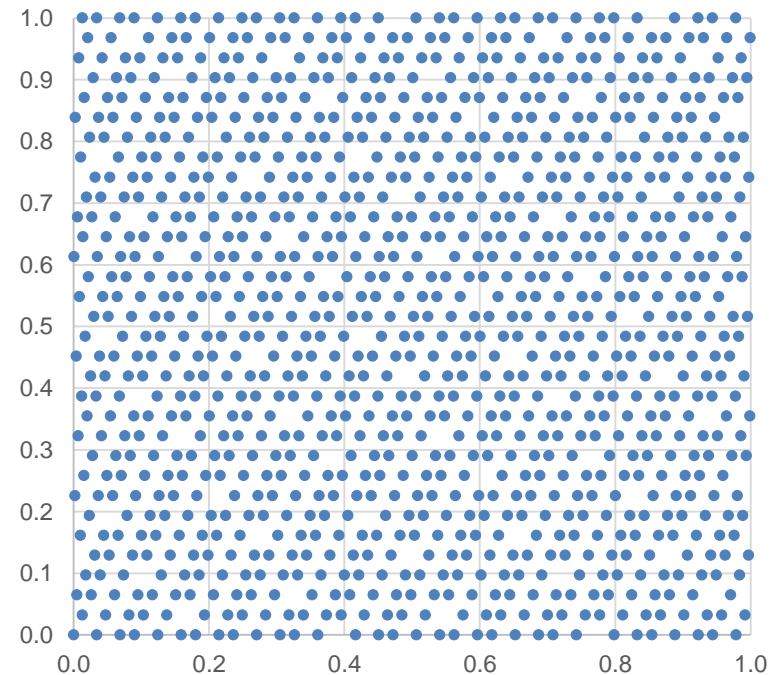
# 1方向貴金属法

- X方向→貴金属法
- Y方向→規則的
- 計算結果でRMS値を算出
- 使用する貴金属数

第1貴金属数(1.6180...)

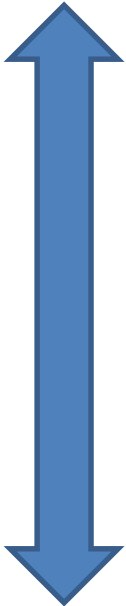
第2貴金属数(2.4121...)

第3貴金属数(3.3028...)

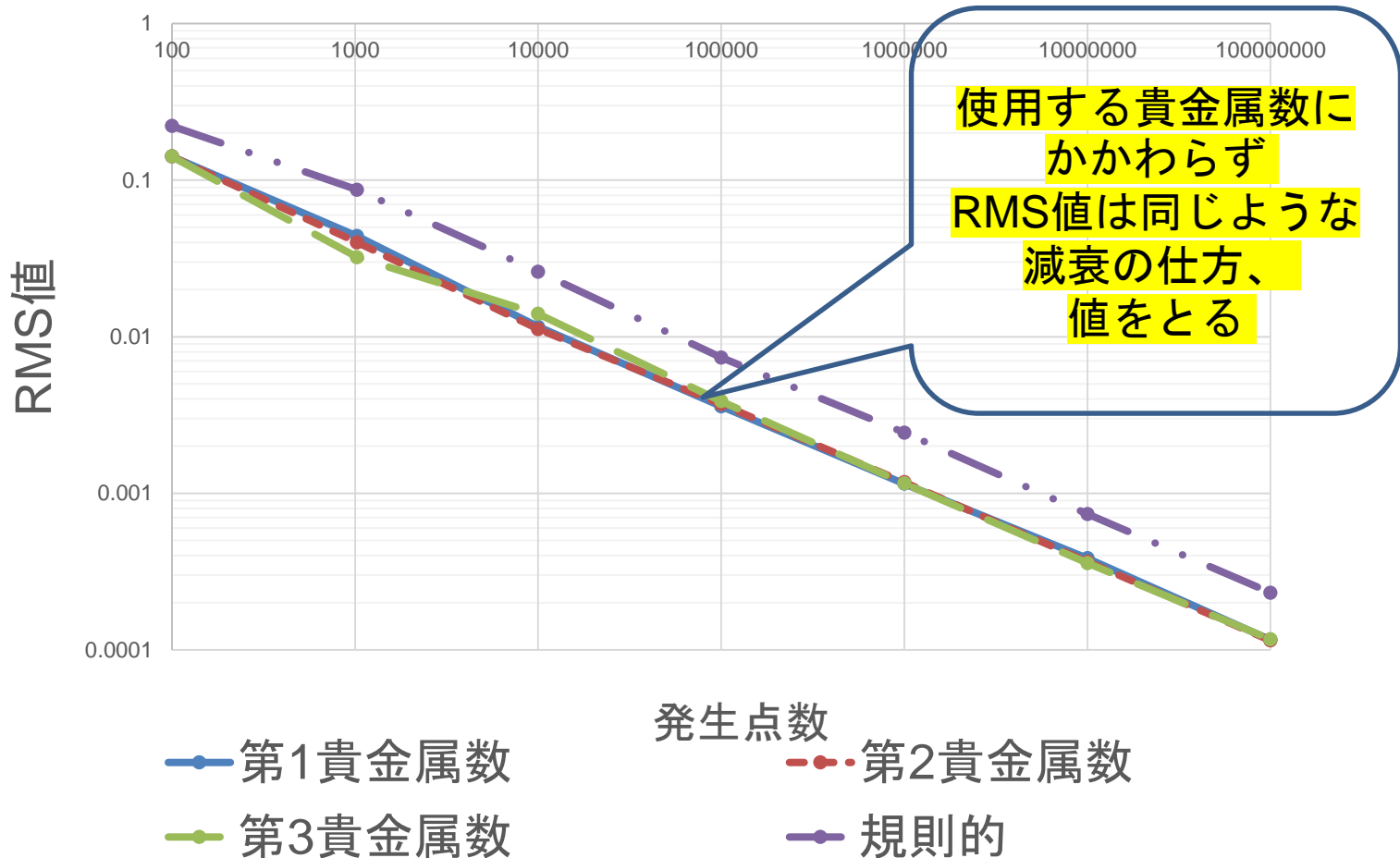


# 1方向貴金属法(計算結果)

**Bad**



**Good**



# 目次

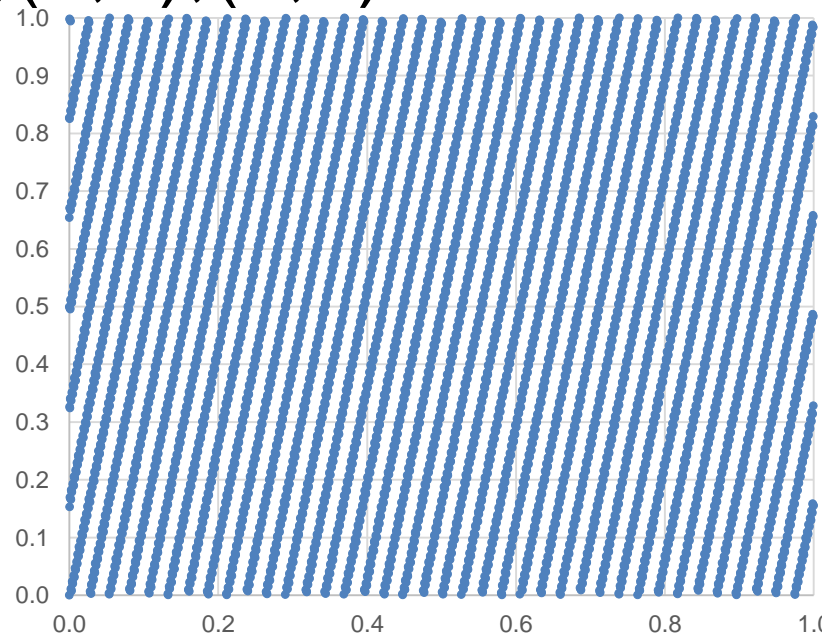
- はじめに
- 従来の乱数発生法
- 貴金属比サンプリングを用いた  
疑似乱数発生アルゴリズムの提案
- **研究内容**
  - 従来法との比較
  - 1方向貴金属法
  - **2方向貴金属法**
- まとめと今後の課題

# 2方向貴金属法

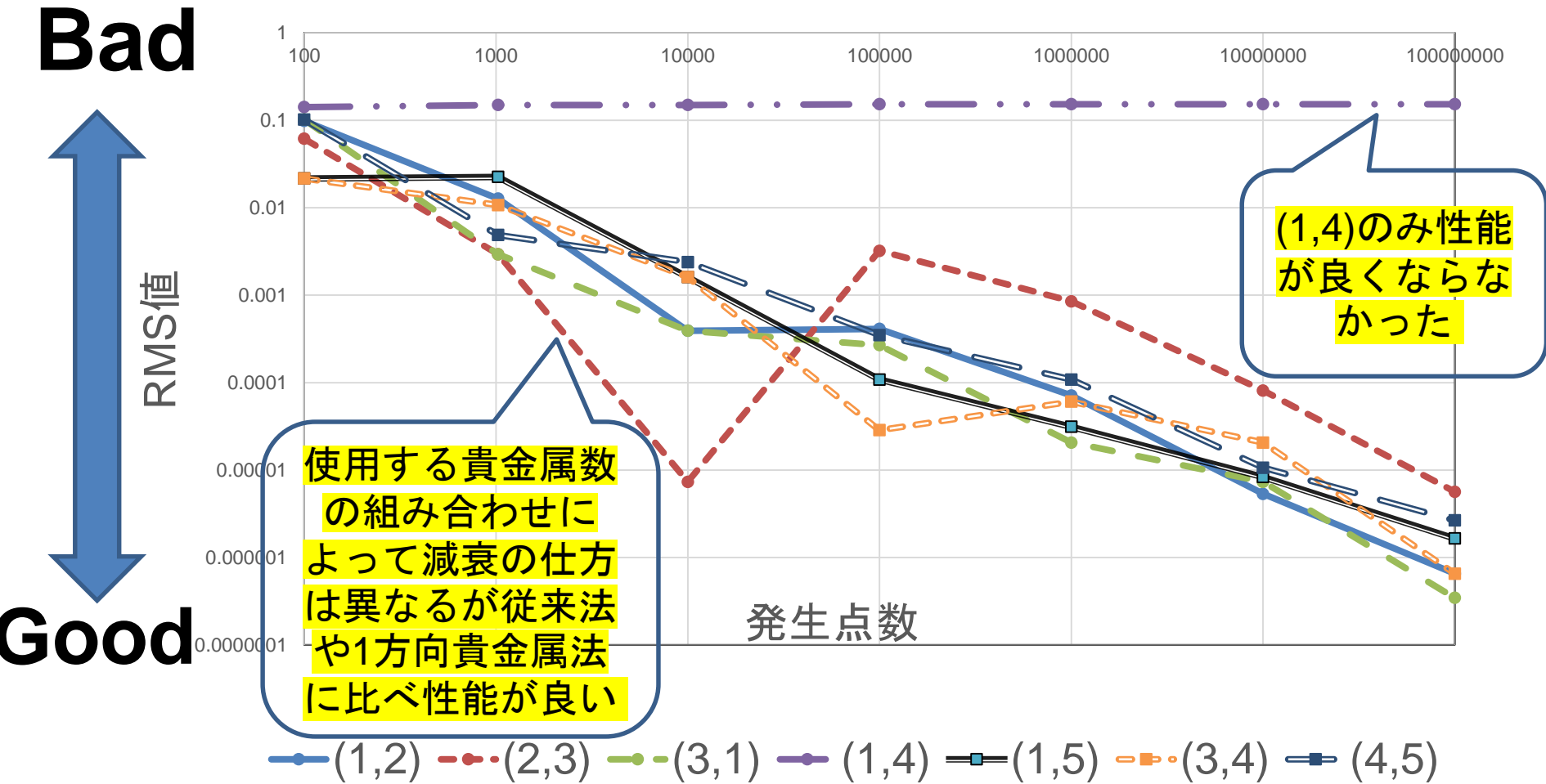
- X方向、Y方向→貴金属法
- 計算結果からRMS値を算出
- 貴金属数の組み合わせは以下の通り  
(1,2),(2,3),(3,1),(1,4),(1,5),(3,4),(4,5)

第4貴金属数(4.2361...)

第5貴金属数(5.1953...)



# 2方向貴金属法(計算結果)



# 避けるべき組み合わせ

- X方向、Y方向→貴金属法
- 測定結果からRMS値を算出
- 貴金属数の組み合わせは以下の通り

(1,2),(1,4),(2,14)

第1貴金属数(1.6180...)

第4貴金属数(4.2361...)

第2貴金属数(2.414213...)

第14貴金属数(21.14213...)



(小数部が) $\times 2$

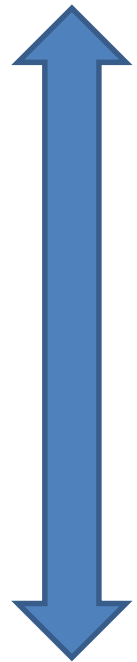


(小数部が) $\times 10$

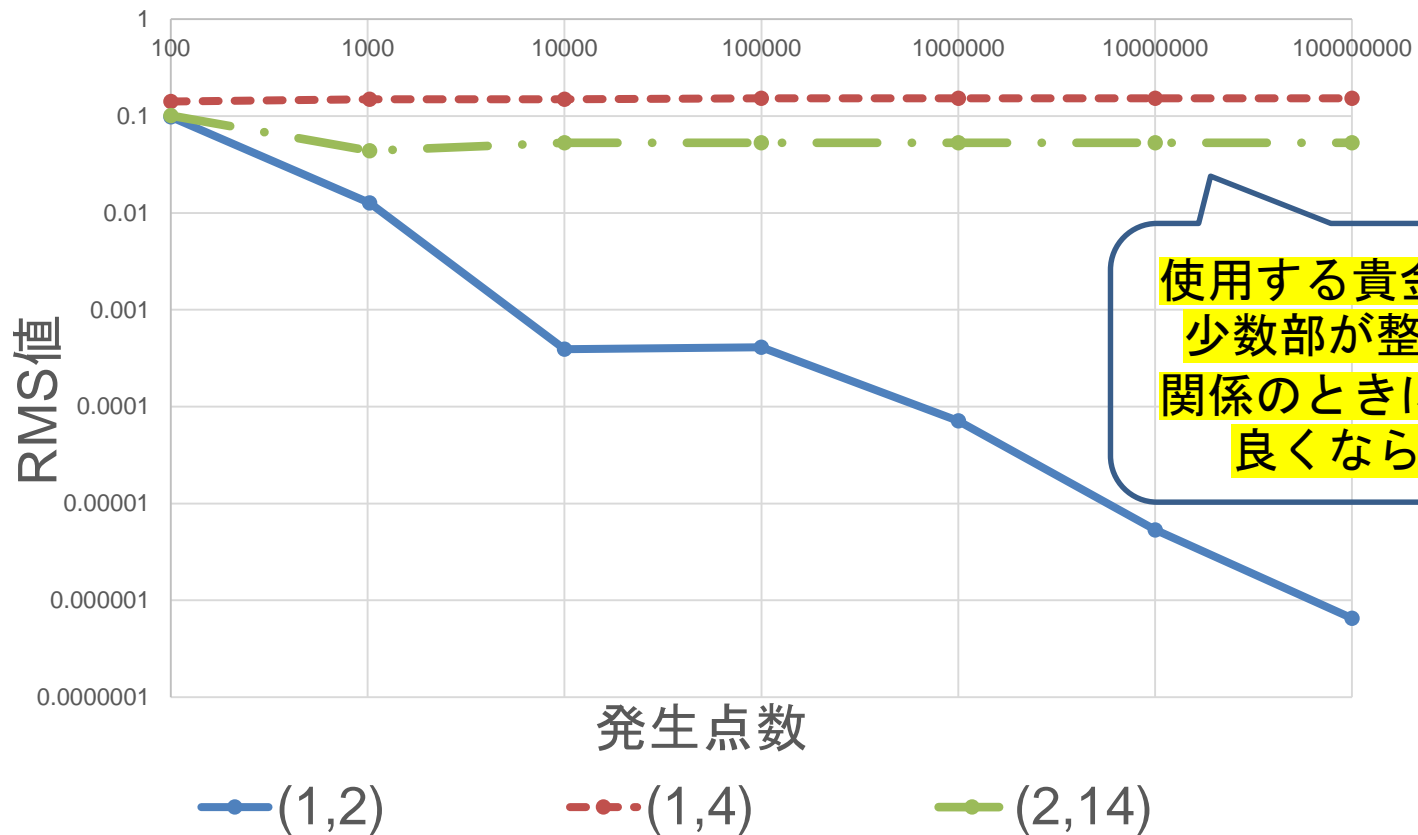


# 避けるべき組み合わせ(計算結果)

Bad



Good



# 目次

- はじめに
- 従来の乱数発生法
- 貴金属比サンプリングを用いた  
疑似乱数発生アルゴリズムの提案
- 研究内容
  - 従来法との比較
  - 1方向貴金属法
  - 2方向貴金属法
- **まとめと今後の課題**

# まとめ

- 1方向貴金属法  
貴金属数によらず同等の値をとる  
従来法と同等の性能を有する
- 2方向貴金属法  
1方向貴金属法や従来法よりも  
性能は良くなる  
2方向の貴金属比のそれぞれの  
小数部が整数倍の関係を満たしたとき  
性能の改善は見られない

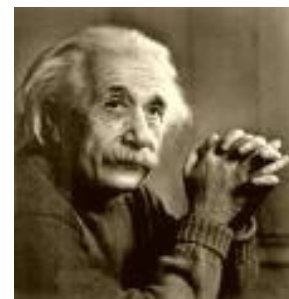
# 今後の展望

- モンテカルロシミュレーション以外での  
測定方法で評価
- モンテカルロシミュレーションにおいて  
平面内に設定する図形の変更

# 最後に：モンテカルロ法 = サイコロ遊び

「神は サイコロ遊びなどされない」

Albert Einstein 量子力学を批判



「アインシュタインよ、神が何をなさるかなど  
注文をつけるべきではない」

Niels Henrik David Bohr

量子力学の育ての親



我々は神ではないので

サイコロ遊び(モンテカルロ法)のための  
疑似乱数発生アルゴリズムを研究

# 謝辞

---

本研究はJSPS科研費 21K04190  
の助成を受けたものです。

ご清聴  
ありがとうございました

# 質疑応答

Q. 貴金属比を使用する理由

A. ページ7のように以前から黄金比にかかわる研究を本研究室で行い、よい結果がでると予想していた。また、フィボナッチ数列から近似できる特徴から他の無理数より他分野においても応用ができると考えている。



# 質疑応答

Q.(ページ19について) 貴金属法を使用するとある法則に基づいているように見られるが(斜めに分布しているように)どう考えているか

A.今回は、モンテカルロシミュレーションの評価が良くなるという点に重点を置いて考えているので、重要視はしていないが、今後考える点の1つとして考えている。