2021年6月3日
電気電子情報工学実験II (b)
実践的・競技プログラミング（2021年度）（3）

ダブリング（繰り返し二乗法）

廣田悠輔 *)
*) y-hirota@u-fukui.ac.jp

はじめに

- 競技プログラミングで頻出のテクニックであるダブリングについて解説する.
  - ダブリングは繰り返し二乗法とも呼ばれる.
  - 競技プログラミング以外でもよく用いられる.

- 簡潔に言えば, 「n ステップ後の状態を $\log n$ ステップの計算で求めるテクニック」がダブリングである.

問題例（線形合同法により生成される疑似乱数列の予測）

問題文

線形合同法では，初期値（シード）r_0，正整数 p，q が与えられるとき，以下の式により疑似乱数列 $r_1, r_2, \ldots$ を生成する．

$$r_{i+1} = (r_i \times p + 1) \bmod q$$

ただし，$a \bmod b$ は a を b で割った余りである．疑似乱数列の n 番目の値 r_n を出力するプログラムを作成せよ．

制約

- $1 \leq n \leq 10^{16}$
- $1 \leq r_0 \leq 10^5$
- $2 \leq p \leq 10^5$
- $2 \leq q \leq 10^5$

出力

疑似乱数列 n 番目の値 r_n を出力せよ．

愚直な方法

- $r_1, r_2, \ldots, r_n$ を式の通りの方法で順番に計算する.

✓ 計算量の概算
- 全体の計算量： $O(n)$
  - 乱数あたりの生成に必要な計算量： $O(1)$
  - 生成すべき乱数の数： n

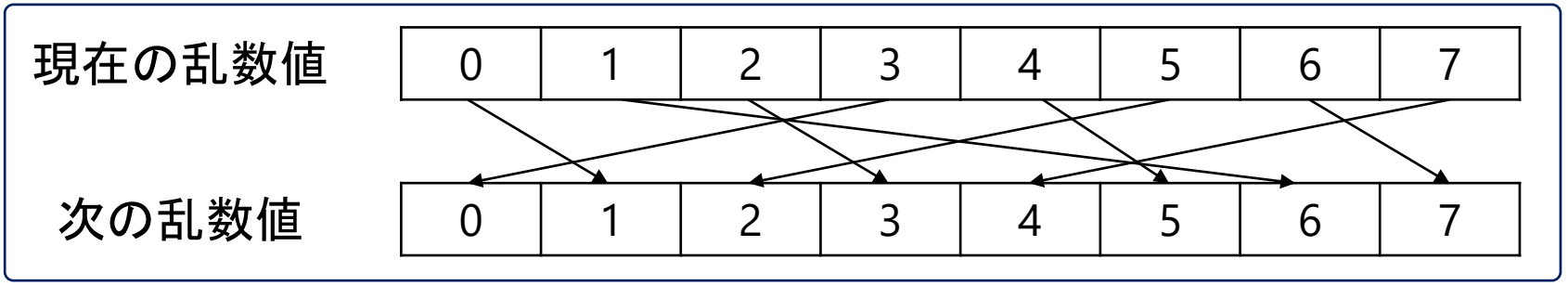
✓ 最大で $n = 10^{16}$ なので，時間がかかりすぎる.

ダブリングによる高速な方法 [1/8]

洞察 [1]

- 現在の乱数値 r_i と定数 p, q が分かっていれば，次の乱数値 r_{i+1} は一意に定まる．
- 現在の乱数値が $0, 1, \ldots, q-1$ である場合それぞれについて，次の乱数値を求めておいてその対応付けを記録しておく．そうすれば，以後は，乗算や剰余計算をせずに次の乱数値を調べることができる．

（例）$p = 5, q = 8$ の場合



- ✓ $r_0 = 3$ ならば $r_1 = 0$，$r_5 = 6$ ならば $r_6 = 7$ といった具合に，乗算・剰余計算せずとも次の乱数が分かる．

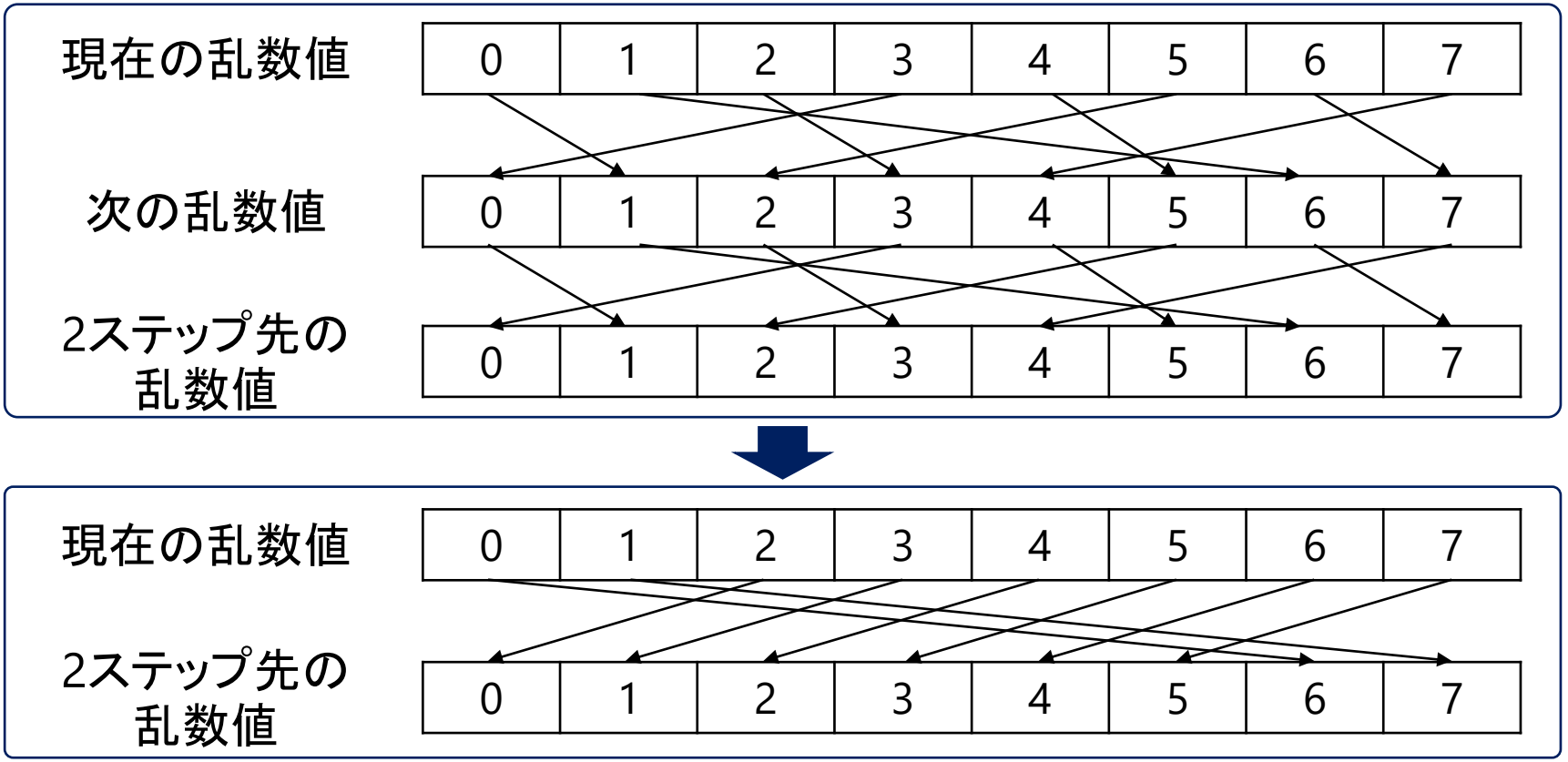
ダブリングによる高速な方法 [2/8]

洞察 [2]

- 現在の乱数値から次の乱数値への対応付けが分かっていれば，さらにその次の乱数値への対応も分かる.
- すなわち，現在の乱数値から，2ステップ先の乱数値の対応付けを調べるられる.

ダブリングによる高速な方法 [3/8]

（例）$p = 5, q = 8$ の場合



- ✓ $r_0 = 3$ ならば $r_2 = 1$，$r_5 = 6$ ならば $r_7 = 4$ といった具合に，
  乗算・剰余計算せずとも2ステップ先の乱数が分かる．

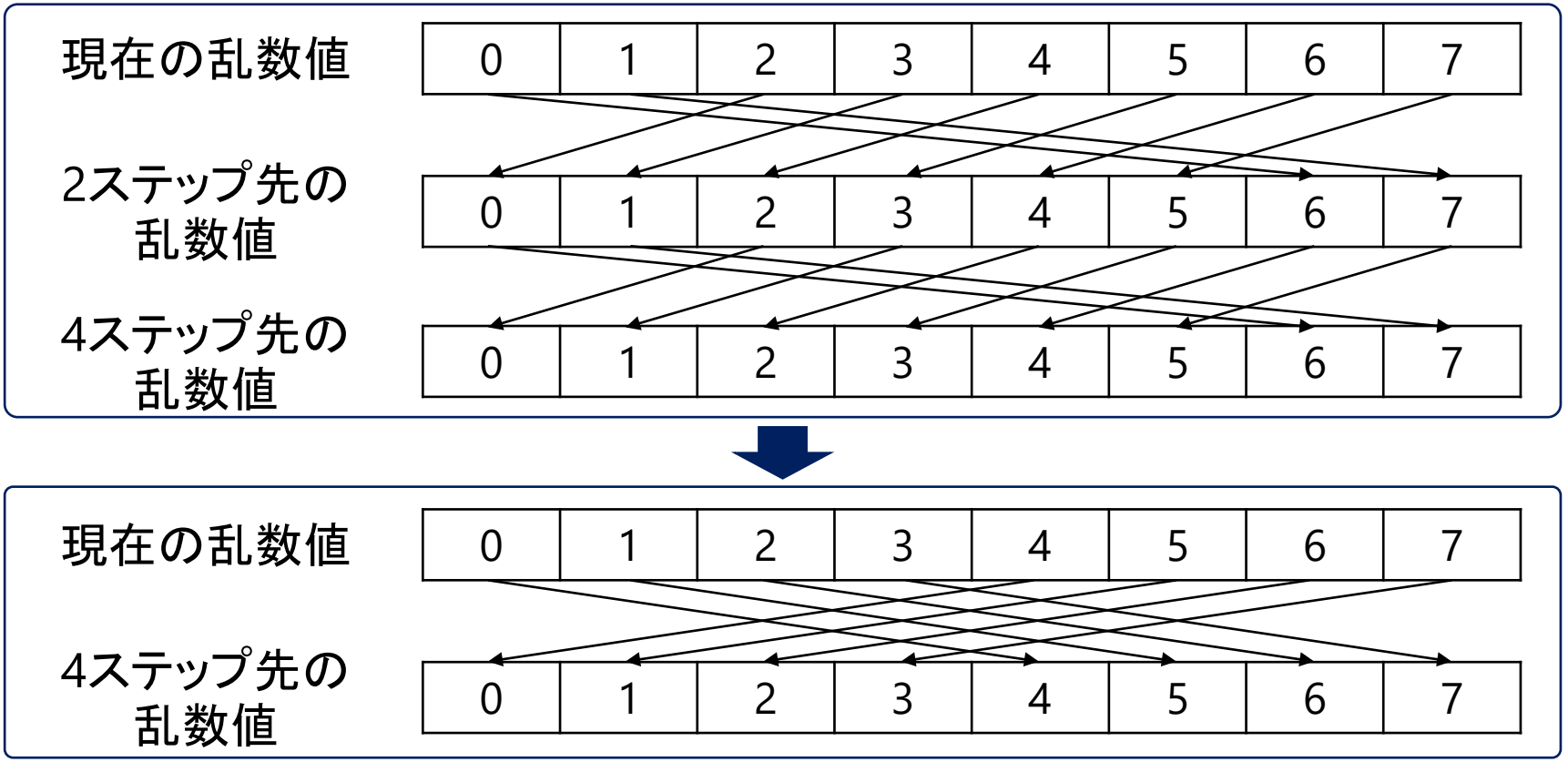
ダブリングによる高速な方法 [4/8]

洞察 [3]

- 同じことを繰り返せば，4ステップ先，8ステップ先，...と2のべき乗回先の乱数値の対応付けを調べることができる.

ダブリングによる高速な方法 [5/8]

（例）$p = 5, q = 8$ の場合



ダブリングによる高速な方法 [6/8]

洞察 [4]

- 任意の正整数 n は2のべき乗（$1, 2, 4, 8, \ldots$）の和として表現できる.
- したがって，n ステップ後の乱数値は，べき乗ステップ後の対応付けの組み合わせによって効率的に求められる.

（例）$n = 333$ の場合

- $n = 333 = 256 + 64 + 8 + 4 + 1$ である.
- したがって，1, 2, 4, 8, ..., 256 ステップ先までの対応付けを調べて，以下の順で乱数を調べれば良い.

ダブリングによる高速な方法 [7/8]

- ✓ 計算量の概算
  - すべての対応付けを調べる計算量： $O(q \log n)$
    - 1回の対応付けを調べる計算量： $O(q)$
    - 調べるべき対応付けの数： $O(\log n)$
  - 対応付けを適用した n ステップ先の乱数生成： $O(\log n)$

- ✓ 愚直な方法と比べて極めて計算量が少ない.

ダブリングによる高速な方法 [8/8]

- 以上のように，1ステップ後の対応付けをもとに，2ステップ後，4ステップ後，8ステップ後，... と次々と対応付けを求めて，その結果を元に具体的な値について n ステップ後の状態を求めるテクニックをダブリングという.

補足

- 線形合同法の値予測は，ダブリング以外の方法でも行うことができる．最も簡単な方法は疑似乱数列の周期性を使う方法である．
- 線形合同法による疑似乱数は，現在の乱数値から次の乱数値が定まる．このため，この乱数列には周期性があり，その周期の長さは最大でも q と短い．
- 周期性を利用すれば，n 番目の値を少ない計算量で予測できる．
  - $r_0, r_1, \ldots, r_q$ の疑似乱数を生成すれば，少なくとも1回は重複する値が出現するので，そこから求める．
  - n を周期で割って余り s を求める．
  - $r_n = r_s$ であるので，$r_0, r_1, \ldots, r_s$ を順に計算する（$s < q$ に注意）．