第4回中高生情報学研究コンテスト@情報処理学会2022.3.5

Shorのアルゴリズムにおける周期検出についての研究

東京都立多摩科学技術高等学校
小野　凜成

研究の背景

量子コンピュータ本体を扱う研究は特定の設備を使用できる組織しか行うことができない。よって RSA暗号がいつ危険になるのかを、その組織以外が十分に理解できない可能性がある。
したがって、量子コンピュータがRSA暗号を解読する前にRSA暗号の危険性を証明する必要がある。

研究の目的

ノイマン型コンピュータで”Shorのアルゴリズム”を用いてRSA暗号を解読するために、Shorのアルゴリズムの中で大部分の計算量を占める過程2,3をより少ない時間で通過する。

研究知識

- Shorのアルゴリズム…素因数分解をするアルゴリズム

1. 合成数N、任意の自然数a（$0 < a < N$）を用意
2. $a^1,a^2,a^3 \ldots a^n$ を計算し、それぞれをNで割った余りを求める
3. 2で求めた余りの配列Rの中で循環する配列rの要素数(周期T)を検出
4. $a^{T/2} \pm 1$とNの最大公約数を計算
5. 求まった2つの数が因数
6. 1~5を5の因数が素数になるまで繰り返す→素因数分解完成

・量子コンピュータ
量子の重ね合わせにより、高速計算が可能なコンピュータ。
・ノイマン型コンピュータ
量子コンピュータ以外のコンピュータ。すなわち従来のコンピュータ。
・RSA暗号
２つの巨大な素数P,Qとその合成数Nを用いた暗号形式
P,Qのどちらかが Nから導き出せれば解読できる
合成数NからP,Qを求めるには巨大な素因数分解をする必要があり、古典コンピュータの場合莫大な時間がかかる為、安全とされている。

研究仮説

配列Rの中で循環する配列rがある
⇒配列rの最初の数r_0が一定の間隔Mで出現
間隔M ＝ 周期Tである確率は、合成数Nが大きくなるにつれ余りのパターンが増えるため1に近づく。RSA暗号における合成数Nは膨大な数である為、間隔M ＝ 周期Tである確率が限りなく1に近い。
よって、間隔M ＝ 周期Tとみなす。
例

```
a = 2
N = 1000
[48, 96, 192, 384, 768, 536, 72, 144, 288, 576, 152, 304, 608, 216, 432, 864, 728, 456, 912, 824,
648, 296, 592, 184, 368, 736, 472, 944, 888, 776, 552, 104, 208, 416, 832, 664, 328, 656, 312,
624, 248, 496, 992, 984, 968, 936, 872, 744, 488, 976, 952, 904, 808, 616, 232, 464, 928, 856,
712, 424, 848, 696, 392, 784, 568, 136, 272, 544, 88, 176, 352, 704, 408, 816, 632, 264, 528, 56,
112, 224, 448, 896, 792, 584, 168, 336, 672, 344, 688, 376, 752, 504, 8, 16, 32, 64, 128, 256,
512, 24, 48, 96, 192, 384, 768, 536, 72, 144, 288, 576, 152, 304, 608, 216, 432, 864, 728, 456,
912, 824, 648, 296, 592, 184, 368, 736, 472, 944, 888, 776, 552, 104, 208, 416, 832, 664, 328,
656, 312, 624, 248, 496, 992, 984, 968, 936, 872, 744, 488, 976, 952, 904, 808, 616, 232, 464,
928, 856, 712, 424, 848, 696, 392, 784, 568, 136, 272, 544, 88, 176, 352, 704, 408, 816, 632, 264,
528, 56, 112, 224, 448, 896, 792, 584, 168, 336, 672, 344, 688, 376, 752, 504, 8, 16, 32, 64, 128,
256, 512, 24, 48, 96, 192, 384, 768, 536, 72, 144, 288, 576, 152, 304, 608, 216, 432, 864, 728,
456, 912, 824, 648, 296, 592, 184, 368, 736, 472, 944, 888, 776, 552, 104, 208, 416, 832, 664,
328, 656, 312, 624, 248, 496, 992, 984, 968, 936, 872, 744, 488, 976, 952, 904, 808, 616, 232,
464, 928, 856, 712, 424, 848, 696, 392, 784, 568, 136, 272, 544, 88, 176, 352, 704, 408, 816, 632,
264, 528, 56, 112, 224, 448, 896, 792, 584, 168, 336, 672, 344, 688, 376, 752, 504, 8, 16, 32, 64,
128, 256, 512, 24, 48, 96, 192, 384, 768, 536, 72, 144, 288, 576, 152, 304, 608, 216, 432, 864,
728, 456, 912, 824, 648, 296, 592, 184, 368, 736, 472, 944, 888, 776, 552, 104, 208, 416, 832,
664, 328, 656, 312, 624, 248, 496, 992, 984, 968, 936, 872, 744, 488, 976, 952, 904, 808, 616,
232, 464, 928, 856, 712, 424, 848, 696, 392, 784, 568, 136, 272, 544, 88, 176, 352, 704, 408, 816,
632, 264, 528, 56, 112, 224, 448, 896, 792, 584, 168, 336, 672, 344, 688, 376, 752, 504, 8, 16,
32, 64, 128, 256, 512, 24, 48, 96, 192, 384, 768, 536, 72, 144, 288, 576, 152]
```

↑N = 1000, a = 2の場合、100間隔で48(r_0)が５つ出現
48から要素数100個の配列xが循環している為、周期T ＝ 100

＜仮説１＞
配列Rを縦軸=a^n/Nの余り、横軸=nにした折れ線グラフをスペクトル分析すれば、グラフからより簡単に周期を算出できると仮説。

＜仮説２＞
周期が2の時の(N,a)の規則性を見つければ周期検出の過程を省略することが可能になり、さらに$a^{T/2} \pm 1$の値も最小になるため因数分解の計算時間も小さくなると仮説。

＜仮説３＞
一定の範囲のaについてのNの周期Tをグラフに表し、規則性を見出すことで、(N,a)の周期をその規則性から算出できるようになり、処理時間が短くなると仮説。

実験

- ＜仮説１＞についての＜実験１＞

Shorのアルゴリズムの配列Rをスペクトル分析してグラフ化する。

- ＜仮説２＞についての＜実験２＞

縦軸=a、横軸=Nとし、周期が2のときの(N,a)値をとり、 Na座標平面上に点を打った離散図を作成し、そこから規則性を見出す。
また、グラフの形状を知るために一部a <Nを満たしていない範囲がある。100≦N≦600, 2≦a≦250の範囲で行った。

- ＜仮説３＞についての＜実験３＞

$(N,a)=(N_1,a_1),(N_1,a_2),(N_1,a_3),\cdots,(N_1,a_n),(N_2,a_1),\cdots,(N_m,a_n)$についての周期を順番に配列Tに入れて、縦軸= T(j)横軸=jとした折れ線グラフを作成し、そのグラフから規則性を見出す。
100≦N≦2000, 2≦a≦100の範囲で行った。

結果

- ＜実験１＞の＜結果１＞

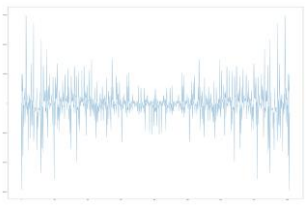
検証した全ての(N,a)について左右対称なグラフ(例１)になった。

- ＜実験２＞の＜結果２＞

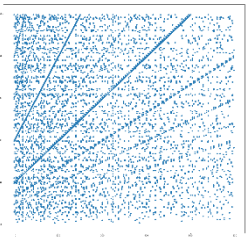
一部規則性のある直線(図１)が現れた。

- ＜実験３＞の＜結果３＞

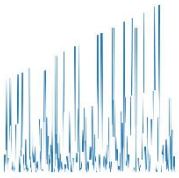
一定の範囲ごとに棒状の形状を示し、棒グラフのような折れ線グラフ(図２)を生成した。



↑例１



↑図１



←図２

考察

＜結果１＞より、
- 配列Rはスペクトル分析をした時に常に左右対称であるということを示唆。

＜結果２＞より、
- 放射状にいくつかの直線が現れているということを示唆。
- この直線は連続的であるため、この直線を数式a= $f(x)$で表すことが出来れば周期検出の処理時間が一気に短縮されると推察。

＜結果３＞より、
- 棒の幅は等間隔である為、棒の幅はNが同一の範囲と推察。
- グラフの形状から、周期が高頻度で激しく振動している、またNを定数とした時、aの値が異なっても同じ周期が頻繁に出ることを示唆。
- 棒の長さの変化から、Nにおける最大の周期には規則性があると推察。

今後の課題

・スペクトル分析した結果がなぜ左右対称になるのか原因を探す。
・図１、図2の規則性を具体的な数式に表す。

参考文献

[1]https://algorithm.joho.info/programming/python/numpy-fast-fourier-transform/#toc1
[2]https://qiita.com/SamN/items/649a49e91a2a400542d3
[3]https://qiita.com/SamN/items/ed23f6f86f1781fac2c6
[4]https://qiita.com/QUANON/items/e7b181dd08f2f0b4fdbe
[5]https://qiita.com/renesisu727/items/24fc4cd8fa2635b00a0d