ISS-P-067

Shor のアルゴリズムにおける周期検出についての研究

小野　凜成†　西野　洋介†
†　都立多摩科学技術高等学校

1. はじめに

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．

2. 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の１つ. 手順は以下の通り.

1. 合成数 N，任意の自然数 a（0＜a＜N）を用意.
2. $a^1,a^2,a^3\cdots$ 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. $a^{T/2}$ ± 1 と N の最大公約数を計算.
5. 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.

3. 方針

Shor のアルゴリズムの中で最も計算量の大きい周期検出の過程を，ノイマン型コンピュータを用いてより少ない時間で算出することにより巨大な素因数分解，すなわち RSA 暗号を解読する.

4. 研究仮説

配列 r が循環するため, 最初の数 r_0 は一定の間隔 M で出現する．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 とみなすことができる.

4.1 仮説１

a を固定して，一定の範囲の値をとる N の周期を全て算出するのに要した計算時間 t を出すことにより，広範囲の N に対しての平均計算時間が小さい a，及び平均計算時間の小さい a の規則性を発見できると仮設.

4.2 仮説２

配列 R を縦軸=要素, 横軸=N にした折れ線グラフをスペクトル分析することにより, 周期の要素を得られると仮説.

4.3 仮説３

縦軸=N の周期平均算出時間，横軸=N としたグラフから規則性を読み取り，より大きな N の平均算出時間を予測することで周期検出の処理回数を減少させられると仮説.

4.4 仮説４

実験中に a の値に関わらず周期 T が一定の N があった.

このことから, 一定の範囲の値をとる a で N の周期 T を算出し，その周期 T の散らばり度合いを標準偏差で算出したとき，a の値に左右されにくい N が出現すると仮説.

5. 検証結果・考察

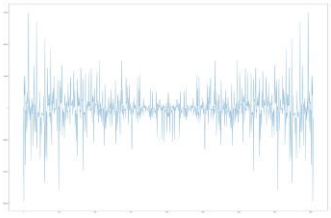

図１

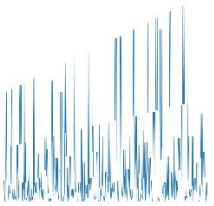

図２

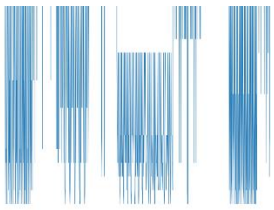

図３ 図２の左下の拡大図

5.1 仮説１，３の検証結果１，３

2≦a≦9999，10000≦N≦1000000 で 3 週間計算し続けたが, 計算量が大きすぎて約 1/1000 しか終了していなかったため, 算出できなかった.

5.2 仮説２の検証結果２

実験に用いたすべての(N,a)において，左右対称のグラフ（例：図１）が出力され, 仮説とは異なる結果が得られた.

5.3 仮説４の検証結果４

棒グラフのようなグラフ（図２）が出力された．これは折れ線グラフが同じ高さで上下を繰り返している（図３）ため棒状に見えるが，折れ線グラフである．これらから標準偏差 0 の N は頻繁に出現するという結果が得られた.

6. 今後の方針

- 仮説１，３を検証したプログラムを高速化する.
- 検証結果４を仮説１，３の検証に応用する.
- 検証結果４の標準偏差の大小の規則性を発見する.

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

Copyright © 2022 IEICE