New sample - Urgent!

Nguyen Thi Thu Quyen

July 18, 2022

Abstract

This is a review on the estimation of the security parameter α by sampling coefficients of Fourier representation instead of usual representation.

1 Revisit on Gaussian sampling

1.1 Object interested

$$\alpha^2 q = ||\tilde{B}_{f,g}||_{\mathcal{K}} = \max(||\varphi(ff^* + gg^*)||_\infty, ||\frac{q^2}{\varphi(ff^* + gg*)}||_\infty)$$

Goal: Minimizing α.

1.2 Sampling Fourier coefficients

- FFT

  $$\varphi : Z[X]/(\phi) \longrightarrow C^n$$
  $$(f_0, \cdots, f_{n-1}) \longmapsto (f(\omega_0), \cdots, f(\omega_{n-1}))$$

  Then $||\varphi(ff^* + gg^*)||_\infty = \max_i(|f(\omega_i)|^2 + |g(\omega_i)|^2)$.

- Mitaka's design: Sampling f_i from a discrete gaussian $D_{Z,0,\sigma_0}$ then $\varphi(f)$ behaves like normal vector of standard deviation $\sigma_0\sqrt{n}$.

- This sample: Sampling $f(\omega_i)$ as a normal vector ($\rightarrow$ center and σ is to be verified) then reconstruct f (by integral rounding/approximating $\rightarrow$ to be verified). Since $f(\omega_i), g(\omega_i) \in C$:

  $$f(\omega_i) = a_i + ib_i \quad f(\omega_i) = c_i + id_i$$

  Then

  $$\alpha^2 q = \max_i(a_i^2 + b_i^2 + c_i^2 + d_i^2, \frac{q^2}{a_i^2 + b_i^2 + c_i^2 + d_i^2})$$

  .

2 Experiments of This sample

2.1 Description of experiment

- **Input:** $a_i, b_i, c_i, d_i \hookleftarrow \mathcal{N}(0, \sigma)$.
- **Output:** ? Distribution of $\alpha(q, \sigma, \mathrm{dim})$.

2.2 Premier results

- 05/07: Not so good: $\alpha > 2.78$ → recheck code
- 06/07: Median $\alpha = 1.78$, $\min \alpha = 1.04$ with $\mathrm{dim} = 5, q = 17497, \sigma \approx 73$. Observations:
  - Bigger dim, bigger α (intuitionally understandable): $\mathrm{dim} > 100$, $\alpha > 2$
  - Bigger q, bigger σ (intuitionally understandable): $q \approx 10^5$, $\sigma \approx 70$.

2.3 Improving/Testing direction

2.3.1 Use $\mathcal{N}(c = \tilde{q}, \sigma)$

2.3.2 Reconsider distribution (not gaussian anymore)

2.4 Works to do

- Recheck code
- Test directions
- Heuristic analyse for Observations

3 Sampling uniformly in annulus

As seen above, gaussian as distribution of Fourier coefficients makes it hard to obtain $\alpha \approx 1.15$. In this section we attack the problem with another approach: Fix α (small) at the beginning then make sure (high probability) that we can find the pair of Fourier coefficients corresponding.

3.1 Object interested

$$\alpha^2 q = ||\tilde{B}_{f,g}||_{\mathcal{K}} = \max(||\varphi(ff^* + gg^*)||_\infty, ||\frac{q^2}{\varphi(ff^* + gg*)}||_\infty)$$

With fixed α we have

$$\max_i(|f(\omega_i)|^2 + |g(\omega_i)|^2) \leq \alpha^2 q$$
$$\max_i(\frac{q^2}{|f(\omega_i)|^2 + |g(\omega_i)|^2}) \leq \alpha^2 q$$

So for $\forall i$:

$$\frac{q}{\alpha^2} \leq |f(\omega_i)|^2 + |g(\omega_i)|^2 \leq \alpha^2 q$$

Goal: Find $f(\omega_i), g(\omega_i)$ with $(i = 0, \cdots, n-1)$.

3.2 Sampling uniformly in annulus $A(r_1, r_2) = B(0, r_2) \backslash \overline{B(0, r_1)} \subset R^2$

3.2.1 Description/Analyse

Let $t \in A(r_1, r_2)$, then t admits the unique polar representation

$$t = re^{i\theta} = (r\cos\theta, r\sin\theta)$$

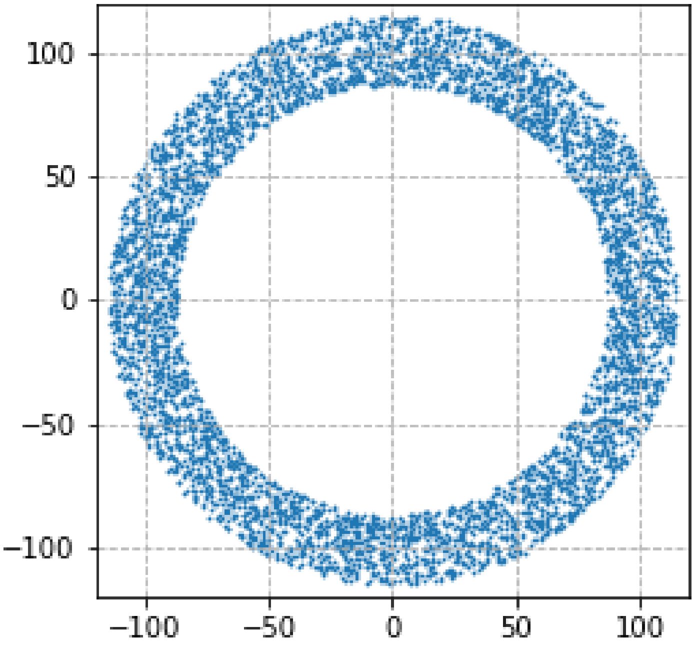
where

$$r \in (r_1, r_2)$$
$$\theta \in [0, 2\pi)$$

We have then $A(r_1, r_2) \cong (r_1, r_2) \times [0, 2\pi)$. Let $r \hookleftarrow U((r_1, r_2))$ and $\theta \hookleftarrow U([0, 2\pi))$ (r and θ are independent). Thus, (r, θ) is uniform in $(r_1, r_2) \times [0, 2\pi)$, consequently, t is uniform in $A(r_1, r_2)$.

3.2.2 Pseudocode

```
Algorithm 1: Sampling uniformly in annulus
    Input  : $r_1, r_2 \in R$
    Output: $t \hookleftarrow U(A(r_1, r_2))$
    $r \hookleftarrow U((r_1, r_2))$
    $\theta \hookleftarrow U([0, 2\pi])$
    return $t = (r\cos\theta, r\sin\theta)$
```



3.3 Back to **Goal**

Let $t = (|f(\omega)|, |g(\omega)|) \in R^2$, so $t \in A(\frac{\sqrt{q}}{\alpha}, \alpha\sqrt{q})$. Applying **Algorithm 1** we find $t = (t_x, t_y) \hookleftarrow U(A(\frac{\sqrt{q}}{\alpha}, \alpha\sqrt{q}))$.

Let

$$f(\omega) = |t_x| e^{i\mu_1}$$
$$g(\omega) = |t_y| e^{i\mu_2}$$

where $\mu \in [0, 2\pi)$, we obtain solutions for **Goal**.

On the other hand, we observe that t_x is uniform on $(\frac{\sqrt{q}}{\alpha}, \alpha\sqrt{q})$ since $\cos\theta$ is uniform on $[0, 1]$. Thus, $f(\omega)$ is uniform on $(\frac{\sqrt{q}}{\alpha}, \alpha\sqrt{q}) \times [0, 2\pi)$.

```
Algorithm 2: Sampling Fourier coefficients
    Input  : $\alpha, q$
    Output: $a, b \in C$ such that $(\frac{\sqrt{q}}{\alpha} \le |a|^2 + |b^2| \le \alpha\sqrt{q})$
    $t \hookleftarrow U(A(\frac{\sqrt{q}}{\alpha}, \alpha\sqrt{q}))$
    $\mu_1, \mu_2 \hookleftarrow U([0, 2\pi])$
    $(a, b) := (|t_x| e^{i\mu_1}, |t_y| e^{i\mu_2})$
    return $a, b$
```

3.4 Works to do

We are now have $\varphi(f) = (f(\omega_i))_n$ and $\varphi(g) = (g(\omega_i))_n$. The next problem is to choose among them the Fourier representations such that their inverses are integral.

3.4.1 Ideas

We have quite a flexibility in choosing μ, this might be the way to approach an integral Fourier inverse. ... to be continued.

4 Integral Fourier inverse

4.1 Object interested

We have

$$\begin{bmatrix} f(\omega_0) \\ f(\omega_1) \\ \vdots \\ f(\omega_{n-1}) \end{bmatrix} = \begin{bmatrix} 1 & \omega_0 & \omega_0^2 & \cdots & \omega_0^{n-1} \\ 1 & \omega_1 & \omega_0^2 & \cdots & \omega_1^{n-1} \\ \vdots & & & & \\ 1 & \omega_{n-1} & \omega_0^2 & \cdots & \omega_{n-1}^{n-1} \end{bmatrix} \begin{bmatrix} f_0 \\ f_1 \\ \vdots \\ f_{n-1} \end{bmatrix}$$

Goal: Choose $(f(\omega_i))_n$ such that $(f_i)_n$ are integers.

4.2 Analyse

Lemma 4.1 *Let $f \in C[X]/(\phi)$ and ω be an arbitrary root of ϕ. Then $f(\overline{\omega}) = \overline{f(\omega)}$ if only if $f \in R[X]/(\phi)$.*

Proof: Let $f(x) = (a_{n-1} + ib_{n-1})x^{n-1} + \cdots + (a_0 + ib_0)$. So $f(\overline{\omega}) = \overline{f(\omega)}$ implies that for all roots ω of ϕ

$$h(\omega) = b_{n-1}\omega^{n-1} + b_{n-2}\omega^{n-2} + \cdots + b_1\omega + b_0 = 0$$

We observe that $\deg h = n - 1$ while $\#\{\omega\} = n$, thus, $h \equiv 0$, consequently, $f \in R[X]/(\phi)$.

So by choosing the $f(\omega)$ as

$$\begin{bmatrix} f(\omega_0) \\ \vdots \\ f(\omega_{\frac{n}{2}}) \\ \overline{f(\omega_{\frac{n}{2}})} \\ \vdots \\ \overline{f(\omega_0)} \end{bmatrix}_{n\times 1}$$

we are sure to obtain f_i real. Let round f_i to its closest integer $[f_i]$, we have

$$|f(\omega) - [f](\omega)| = |\sum_{i=0}^{n-1}(f_i - [f_i])\omega^i| \leq \sum_{i=0}^{n-1}|f_i - [f_i]||\omega^i| \leq \frac{n}{2}$$

In practice, the difference is not that big (theoretically we can choose μ_1 (previous section) to reduce this distance (??)). So by choosing $[f]$ integrally close to f, we still can have a Fourier representation of $[f]$ included in the same annulus as f. The algo of this scheme might involve aborts if is not the case (For my experiments for small dimension, I have not encountered aborts, which means the success rate is quite high).

4.3 Pseudocode

Algorithm 3: Integral Fourier inverse

```
Input  : $\alpha, q$
Output: $f_i, g_i$ integers such that $\frac{q}{\alpha^2} \leq |f(\omega_i)|^2 + |g(\omega_i)|^2 \leq \alpha^2 q$.
for $0 \leq i < n$.for $i$=1, $\cdots, \frac{n}{2}$ do
    $f(\omega_i), g(\omega_i) :=$ SampleFourier$(\alpha, q)$
    $f(\omega_{n-i}) := \overline{f(\omega_i)}$
    $g(\omega_{n-i}) := \overline{g(\omega_i)}$
end for
$[f] := Round(FFT^{-1} f(\omega))$
$[g] := Round(FFT^{-1} g(\omega))$
if $([f](\omega), [g](\omega)) \notin A(\frac{\sqrt{q}}{\alpha}, \alpha\sqrt{q})$ then
    Repeat all
end if
return $[f], [g]$
```

4.3.1 Works to do

Experiments for high dimension! If it is not favorable, adjust it to minimize the number of aborts. ...to be continued.

5 Analyse of error of rounding

5.1 Analyse of $\epsilon = f(\omega) - [f](\omega)$

Let $a_j = f_j - [f_j]$, we have

$$f(\omega) - [f](\omega) = \sum_{j=0}^{n-1} a_j \omega^j$$

For fixed ω^j, $a_j \omega^j = a_j \cos(j\theta) + i a_j \sin(j\theta)$.

Assume that a_j follows uniform law over $[-\frac{1}{2}, \frac{1}{2}]$.

Let $X_j = a_j \cos(j\theta)$ we then have X_j uniform over $[-\frac{1}{2}\cos(j\theta), \frac{1}{2}\cos(j\theta)]$. So $X_0, X_1, \cdots, X_{n-1}$ are n independent variables with $E[X_j] = 0$, $E[X_j^2] = \frac{1}{12}\cos(j\theta)^2 = \sigma_j^2 > 0$ and $E[|X_j|^3] = \frac{\cos(j\theta)^3}{32} = \rho_j < \infty$. Also, let

$$S_n = \frac{X_0 + X_1 + \cdots + X_{n-1}}{\sqrt{\sigma_0^2 + \sigma_1^2 + \cdots + \sigma_{n-1}^2}}$$

be the normalized n^{th} partial sum. Denote F_n the cdf of S_n, and Φ the cdf of the $\mathcal{N}(0,1)$. From Berry-Esseen inequality, il exists for all n an absolute constant C_0 such that

$$\sup_{x \in R} |F_n(x) - \Phi(x)| \leq C_0 \psi_0$$

where $\psi_0 = (\sum_{j=0}^{n-1} \sigma_j^2)^{-3/2} \sum_{k=0}^{n-1} \rho_j$ and $0.5600 > C_0 > 0.4097$. On the other hand we have

$$\sum_{j=0}^{n-1} \sigma_j^2 = \frac{1}{48}(\frac{\sin(2n\theta - \theta)}{\sin\theta} + 2n + 1)$$

Then $C_0\psi_0 \sim O(n)^{-3/2} O(n) = O(\frac{1}{\sqrt{n}})$. So the distribution of S_n and that of a standard Gaussian are different by en error of order $n^{-1/2}$. Thus, asymptotically we have

$$\sum_{j=0}^{n-1} X_j = X \sim \mathcal{N}(0, d_X)$$

where

$$d_X = \sqrt{\frac{1}{48}(\frac{\sin(2n\theta - \theta)}{\sin\theta} + 2n + 1)} = O(\sqrt{n})$$

We repeat this analyse for the imaginary part. Let $Y_j = a_j \sin(j\theta)$ then Y_j is uniform over $[-\frac{1}{2}\sin(j\theta), \frac{1}{2}\sin(j\theta)]$, thus, $Y_0, \cdots, Y_{n-1}$ are n independent random variables with $E[Y_j] = 0$, $E[Y_j^2] = \frac{1}{12}\sin(j\theta)^2 = \delta_j^2 > 0$ and $E[|Y_j|^3] = \frac{\sin(j\theta)^3}{32} = \gamma_j < \infty$. We have

$$\sum_{j=0}^{n-1} \delta_j^2 = \frac{1}{48}(-\frac{\sin(2n\theta - \theta)}{\sin\theta} + 2n + 1)$$

So, asymptotically

$$\sum_{j=0}^{n-1} Y_j = Y \sim \mathcal{N}(0, d_Y)$$

where

$$d_Y = \sqrt{\frac{1}{48}(-\frac{\sin(2n\theta - \theta)}{\sin\theta} + 2n + 1)} = O(\sqrt{n})$$

. Finally we have $\epsilon = X + iY$ where $X \sim \mathcal{N}(0, d_X)$ and $Y \sim \mathcal{N}(0, d_Y)$

5.2 Analyse of $E = |f(\omega)|^2 - |[f](\omega)|^2$

We have $f(\omega) = [f](\omega) - \epsilon$, so

$$\begin{aligned}
|[f](\omega)|^2 &= (f(\omega) + \epsilon)(\overline{f(\omega)} + \overline{\epsilon}) \\
&= |f(\omega)|^2 + f(\omega)\overline{\epsilon} + \overline{f(\omega)}\epsilon + |\epsilon|^2 \\
&= |f(\omega)|^2 + 2\mathbf{Re}(f(\omega)\overline{\epsilon}) + |\epsilon|^2 \\
&= |f(\omega)|^2 + 2\mathbf{Re}(f(\omega))X + 2\mathbf{Im}(f(\omega))Y + X^2 + Y^2
\end{aligned}$$

Similarly we have

$$|[g](\omega)|^2 = |g(\omega)|^2 + 2\mathbf{Re}(g(\omega))X' + 2\mathbf{Im}(g(\omega))Y' + X'^2 + Y'^2$$

where $X, X' \sim \mathcal{N}(0, d_X), Y, Y' \sim \mathcal{N}(0, d_Y)$. So

$$\begin{aligned}
X^2 + X'^2 &\sim \Gamma(1, \frac{1}{2d_X}) \\
Y^2 + Y'^2 &\sim \Gamma(1, \frac{1}{2d_Y})
\end{aligned}$$

Then $(X^2 + X'^2) + (Y^2 + Y'^2)$ follows the gamma convolution distribution (GCD):

$$GCD(a, b; \alpha, \beta, x) = \frac{b^a \beta^\alpha}{\Gamma(a + \alpha)} e^{-bx} x^{a+\alpha-1} F(\alpha, a + \alpha, (b - \beta)x) 1_{x>0}$$

with $F(A, B, Z) = \frac{\Gamma(B)}{\Gamma(B-A)\Gamma(A)} \int_0^1 e^{Zu} u^{A-1}(1-u)^{B-A-1} du$. Since $a = \alpha = 1, b = \frac{1}{2d_X}, \beta = \frac{1}{2d_Y}$, then $A = 1, B = 2, Z = (\frac{1}{2d_X} - \frac{1}{2d_Y})x$ we obtain the density function of $T = (X^2 + X'^2) + (Y^2 + Y'^2)$

$$f_T(x) = GCD(1, \frac{1}{2d_X}; 1, \frac{1}{2d_Y}, x) = \frac{1}{2(d_Y - d_X)}(e^{-\frac{x}{2d_y}} - e^{-\frac{x}{2d_X}}) \xrightarrow{x \to +\infty} 0$$

Moreover $E[T] = d_X + d_Y, Var(T) = d_X^2 + d_Y^2$ (there might be a constant). On the other hand, from the construction in the previous section $\mathbf{Re}(f(\omega)), \mathbf{Im}(f(\omega)) \leq \alpha\sqrt{q}$. So we consider the terms $2\mathbf{Re}(f(\omega))X, 2\mathbf{Im}(f(\omega))Y$ as noise of distribution $\mathcal{N}(0, 4\alpha^2 q d_X^2)$. Therefore

$$|f|^2 + |g|^2 - [f]^2 - [g]^2 \sim \mathcal{N}(0, 4\alpha^2 q(d_X^2 + d_Y^2) + \mathcal{D}_T(d_X + d_Y, d_X^2 + d_Y^2) = \mathcal{G}$$

with $E[\mathcal{G}] = d_X + d_Y$ and $Var(\mathcal{G}) = (4\alpha^2 q + 1)(d_X^2 + d_Y^2)$. So if we want $[f]^2 + [g]^2$ to fall in $A(\sqrt{q}/\alpha, \alpha\sqrt{q})$, we need to sample f, g in $A(q/\alpha^2 - E[\mathcal{G}] + \sqrt{Var(\mathcal{G})}, q\alpha^2 - E[\mathcal{G}] - \sqrt{Var(\mathcal{G})})$ where $\sqrt{Var(\mathcal{G})} \sim 2\alpha\sqrt{q}\frac{\sqrt{2}}{24}\sqrt{n} = \frac{\sqrt{2}}{12}\alpha\sqrt{qn}$.

all the computations need reviewing!!!! ...to be continued

6 Integral Fourier inverse (discrete correction)

6.1 Problem encountered

In the algo 3, rounding can push some Fourier coordinates out of the annulus, but resampling naively does not ensure an output. In the next part we suggest a solution for this problem.

6.2 Analyse

Rounding can push points away but not too far, thus we can re-approach the annulus by gradually incrementing or decrementing some coefficients of $[f], [g]$.

Let $f' \in Z[X]$ such that $f' - [f] = (0, \cdot, \pm 1, \cdots, 0)$ ($f', [f]$ are different by ± 1 at i^{th} position). Then $f'(\omega) = [f](\omega) \pm \omega^i$. We have

$$\begin{aligned}|f'(\omega)|^2 &= ([f](\omega) \pm \omega^i)(\overline{[f](\omega)} \pm \overline{\omega^i})\\ &= |[f](\omega)|^2 \pm [f](\omega)\overline{\omega^i} \pm \overline{[f](\omega)}\omega^i + 1\\ &= |[f](\omega)|^2 \pm 2Re([f](\omega)\overline{\omega^i}) + 1\\ &= |[f](\omega)|^2 \pm 2|[f](\omega)|\cos\beta + 1\end{aligned}$$

So

$$||f'(\omega)|^2 - |[f](\omega)|^2| \leq 2|f(\omega)| + 1$$

The idea is that if $f = (f_0, \cdots, f_i, \cdots, f_{n-1})$ is not good then we increment/decrement it to $f' = (f_0, \cdots, f_i \pm 1, \cdots, f_{n-1})$ until f, g are good. This idea needs more analyse on how many time we repeat ... to be continued !!!

6.3 Pseudocode

Algorithm 4: Integral Fourier inverse

```
Input  : $\alpha, q$
Output: $f, g$ integers such that $\frac{q}{\alpha^2} \leq |f(\omega_i)|^2 + |g(\omega_i)|^2 \leq \alpha^2 q$
$ff, gg :=$ IntFourierInv($\alpha, q$) ;                /* ff,gg are integral */
while $(FFT(ff), FFT(g)) \notin A(\frac{\sqrt{q}}{\alpha}, \alpha\sqrt{q})$ do
    $i :=$ PosOfRing($ff, gg$)
    $ff[i] = \pm 1$
end while
return $[f], [g]$
```

References