Moisej Plistiev

June 11, 2024

1 Factor Function

In the past decades, several significant results regarding the complexity of analytic functions have been obtained:

1. An analytic function is computable in polynomial time if and only if its Taylor series is a polynomial-time computable sequence.Müller [1987]
2. The derivative of a polynomial-time computable analytic function is also computable in polynomial time.Ker-I. KO [1982]
3. The integral of a polynomial-time computable analytic function is also computable in polynomial time. Ker-I Ko [1988]

These facts provide a different approach to the problem of integer factorization. Let us introduce the function

$$f(x) := \sin^2(\frac{\pi t}{x}) + \sin^2(\pi x)$$

where t is a natural number. The function has an interesting property:

Theorem 1. *On the interval* $[2, t]$ *the function* $f(x)$ *equals zero if and only if* $x \mid t$

Proof. Proof is based on 3 simple facts:

- The function is non-negative
- $\sin^2(\frac{\pi t}{x}) = 0$ if and only if $\frac{t}{x}$ is a natural number
- $\sin^2(\pi x) = 0$ if and only if x is a natural number

□

The function has essential singularity at 0 and is analytic everywhere else. It has a set of conjugate complex zeros. We could transform $f(x)$ shifting on parameter v:

$$f_{shifted}(x) := \sin^2(\frac{\pi t}{x+v}) + \sin^2(\pi x)$$

and compress on parameter v

$$f_{compressed}(x) := \sin^2(\frac{\pi t}{vx}) + \sin^2(\pi v x)$$

It can be also formulated as maxima version: the function, which has maxima iff x divides t:

$$f(x) := \cos^2(\frac{\pi t}{x}) + \cos^2(\pi x)$$

For a Diophantine equation $= ax^2 + by = c$ there is a following property: The equation has zero if the function

$$f_(x, y) := \sin^2(\pi x) + \sin^2(\pi y) + (ax^2 + by - c)^2$$

equals 0. The function has a lot of maxima and minima, therefore the classical root-finding methods such as Newton-Raphson fail to be reliably fast, since they require a good initial approximation. Since the function is analytic in the region we interested we could use other classical way: complex integration with Newton polynomials or with bisection search based argument on principle, which makes the complexity of the problem similar to the complexity of integration. That's why there would be useful to try other method.

2 Root finding

The theorems of Ker -I. Ko, Friedmann and Müller, stating that the integration of polynomial time computable analytic function is also polynomial time computable allows us to use another approach to the root - finding, using integration. It is based on the modulation of the starting analytic function on the interval with the set of composition with other analytic functions and simple geometric interpretation of the integral. Our goal is to construct a step function and find the points of greatest increase using binary search and linear difference.

2.1 Step 1 - Initial Transformation using the Error Function

- Taking function f(x) analytic on the interval $[a_1, a_2]$. Transform the function $f(x)$ using the error function to obtain $g(x) = 1 - \text{erf}(a \cdot f(x)^2)$. This ensures that $g(x)$ approaches zero for most values of x except near the zeros of $f(x)$, where it will have sharp peaks approaching 1.
- Choose a large value for the parameter a. The choice of a affects the sharpness of the peaks in the transformed function. This problem will be shown later.

We will use our function

$$f(x) := \sin^2(\frac{\pi t}{x}) + \sin^2(\pi x)$$

as example, but it has not to be squared since it is positive. In this particular case we could use as

$$g(x) : (1/2(\cos^2(\frac{\pi t}{x}) + \cos^2(\pi x)))^a$$

instead of

$$g(x) := 1 - \text{erf}(a * (\sin^2(\frac{\pi t}{x}) + \sin^2(\pi x)))$$

Increasing parameter a we get more and more flat graph of the function, where all the values of $f(x)$ except x such that $f(x) = o$ are close to zero, so for x large enough we get a picture, where only values of the function in the small neighborhood of the roots are not close to zero.

2.2 Step 2 - Modulation of the Transformed Function

- Apply the modulation to $g(x)$ using the function $h(x) = -\cos(\pi(g(x) + 1)^b)$, where b has to be an even number. This aims to ensure that the integral of the resulting function forms a "ladder" pattern, with distinct steps corresponding to the zeros of $f(x)$, since the peaks become to thin and the area under it decreases. Modulation makes the area much greater.
- Choose a suitable value for the parameter b for the modulation function. The value of b influences the shape of the modulation.

2.3 Step 3 - Integration and binary search

- Compute the integral of the modulated function, $H(x) = \int h(g(x))\,dx$. The integral is expected to have a step-like pattern.
- Perform a binary search on $H(x)$ within a suitable interval to detect the zeros of $f(x)$. The regions with the maximal linear growth are desired since they are correspond the roots because the are situated on the x which have peaks. We choose to points g_0 and g_1 between which the single (for the simplicity) is situated. Then we take g_2 between (in the middle) of them and compare the differences $H(g_1) - H(g_2)$ and $H(g_1) - H(g_0)$. Than we choose the interval which has the grater linear difference, say $H(g_1) - H(g_2)$ and repeat the procedure: we choose a point g_3 in the middle of $[H(g_1), H(g_2])$ and compare $H(g_1) - H(g_3)$ wit $H(g_3) - H(g_2)-$ and repeat it until we get desired precision.
- Refine the detected zeros using a root-finding algorithm like Newton's method for higher accuracy if needed.

2.4 Problems and limitations

- The complexity of the method could depend on the parameters a and b
- In the case of $f(x) := \sin^2(\frac{\pi t}{x}) + \sin^2(\pi x)$ the problem of "false zeros" could play a role: false zero is a value of the function $f(x)$ close to zero but not equal it is a problem since the modulation cannot distinct true zero and the value close enough what leads to the necessity to choose large a what could make the whole algorithm not polynomial time computable.

If the number of significant digits in the lowest value of the function, distinct from zero, is polynomial with respect to the number of digits of t, and since the value of a depends on it, then the algorithm can be computed in polynomial time. Additionally, there is a second option: if the number of values with a number of digits exceeding a polynomial amount is less than $\log(t)$, check each zero, both false and real, by dividing t by all of them.

References

N. Müller. Taylor series. `https://ub-deposit.fernuni-hagen.de/rsc/viewer/mir_derivate_00001451/Mueller_Taylor_Series_1987.pdf?page=17`, 1987. Accessed: [put the date you accessed the PDF].

Harvey FRIEDMAN Ker-I. KO. Computational complexity of real functions. *Theoretical Computer Science*, 1982. Accessed: 2024-01-18.

Harvey Friedman Ker-I Ko. Computing power series in polynomial time. *ADVANCES IN APPLIED MATHFMATICS 9*, 9(9):40, 1988. doi: 10.1016/0196-8858(88)90006-1. URL `https://www.sciencedirect.com/science/article/pii/0196885888900061`. Accessed: 2024-01-18.