Brief Introduction to Number Theoretic Transform

From the Perspective of Ring Theory

Cesare Huang Cheng Wei

Academia Sinica

January 8, 2025

TABLE OF CONTENTS

Motivation and Goals

- **Core Problem**: Fast polynomial multiplication in $\mathbb{Z}_p[x]/(x^n - 1)$, where n is a power of 2.
  The problems we deal with include more general quotient rings, but in this slide, we firstly focus on such simple ring for the purpose of illustration.
- **Background**:
  - In many applications in cryptography, we have to multiply the elements in the ring of the kind $\mathbb{Z}_p[x]/(x^n - 1)$, which is a very time-consuming operation.
  - Suppose we can perform such operation more efficiently, then in the same cost of computational resource (i.e., time), we can perform such multiplication for larger n, and thus improve the security level of the cryptographic scheme.
- **Structure of This Slide**:
  1. Rings and factorization basics
  2. Searching for roots in $\mathbb{Z}_p$
  3. Butterfly Operation (key focus)
  4. Implementation details
  5. Extensions and applications

- We first take a step back to deal with the multiplication in the ring $\mathbb{Z}/n\mathbb{Z}$.
- For example, let's consider the toy example of multiplication in the ring $\mathbb{Z}/105\mathbb{Z}$.
- Note that $105 = 3 \cdot 5 \cdot 7$, and the factors are co-prime (ideals), so we have the following decomposition:

$$\mathbb{Z}/105\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$$

- Suppose we want to perform the multiplication $31 * 27 = 102$ in the ring $\mathbb{Z}/105\mathbb{Z}$
- We first project the operands (31, 27) to the three "coordinate"-rings:

$$31 \mapsto (1, 1, 3) \quad 27 \mapsto (0, 2, 6)$$

- Multiply the corresponding "coordinates" to get

$$(1, 1, 3) \cdot (0, 2, 6) = (0, 2, 4)$$

- Finally, we recombine the result to get the final answer: The process involves the so-called Chinese Remainder Theorem (CRT), that is, to find the solution to the system

$$x \equiv 0 \pmod 3, \quad x \equiv 2 \pmod 5, \quad x \equiv 4 \pmod 7$$

The solution is $x = 102$, which is the answer to the original multiplication.

Remarks on CRT

- Some may argue that the final recombination step is even costly. However, there exists some efficient algorithms to perform the CRT.
- Another advantage of the RNS CRT approach is that, after decomposing the ring into several "coordinate"-rings, we can perform the multiplication in the "coordinate"-rings in parallel.
- If the whole process involves many times of multiplication, we can leave the big integers in the RNS coordinate representations, and after performing all required multiplications, recombine the results via the CRT once.
- Such technique is applicable in real-world, for example, to compute a discrete logarithm in the ring $\mathbb{Z}/n\mathbb{Z}$.
- For more discussion on the RNS, see the paper:

- So far, we have seen many notations like

$$\mathbb{Z}/n\mathbb{Z}, \quad \mathbb{Z}[x]/(x^n-1), \quad \mathbb{Z}_p[x]/(x^n-1)$$

- These are examples of quotient rings.
- The meaning of $\mathbb{Z}/n\mathbb{Z}$ is familiar to us, it means that all operations are performed modulo n.
- We can extend the idea to polynomial operations:
  - the set $\mathbb{Z}[x]$ is the set of all polynomials with integer coefficients. Operations are performed as usual.
  - the set $\mathbb{Z}[x]/(x^n-1)$ thus meanes that all operations are performed modulo x^n-1.
  - For example, in the ring $\mathbb{Z}[x]/(x^2-1)$,

$$(x+1)\cdot(x+2) = x^2+3x+2 \equiv 3x+4 \pmod{x^2-1}$$

- Generally, $\mathbb{Z}[x]/(f(x))$: Polynomial congruences where $f(x) \equiv 0$.
- We also write the quotient integer rings $\mathbb{Z}/n\mathbb{Z}$ as $\mathbb{Z}_n$
- Hence, the meaning of $\mathbb{Z}_p[x]/(x^n-1)$ is that the coefficients are reduced modulo p, and the polynomial is reduced modulo x^n-1.

Residual Number System and Theory of Quotient Rings

Decomposition of $\mathbb{Z}[x]/(x^2-1)$

- From the experience of the RNS, we now try the same trick on the problem of multiplication in the ring $\mathbb{Z}[x]/(x^2-1)$.
- Easy to see that $x^2-1=(x-1)(x+1)$, and the factors are co-prime (ideals), so we have the following decomposition:

$$\mathbb{Z}[x]/(x^2-1) \cong \mathbb{Z}[x]/(x-1) \times \mathbb{Z}[x]/(x+1)$$

- Suppose we want to multiply $(3+1x)\cdot(2+7x)=13+23x$ in the ring $\mathbb{Z}[x]/(x^2-1)$.
- We first project the operands to the two "coordinate"-rings:

$$3+1x \mapsto (4,2), \quad 2+7x \mapsto (9,-5)$$

- Multiply the corresponding "coordinates" to get

$$(4,2)\cdot(9,-5)=(36,-10)$$

- Finally, we recombine the result to get the final answer: that is, to find the solution to the system

$$f(x) \equiv 36 \pmod{x-1}, \quad f(x) \equiv -10 \pmod{x+1}$$

  The solution is $f(x)=13+23x$,
- It seems that the recombination is very hard to solve. But, no, see the next slide.

- A saying goes that "How to go forward then how to go back" (Cesare Huang, 2024).
- Let $a+bx$ be in the ring $\mathbb{Z}[x]/(x^2-1)$, then we have the following projection:

$$\begin{aligned} \mathbb{Z}[x]/(x^2-1) &\cong \mathbb{Z}[x]/(x-1) \times \mathbb{Z}[x]/(x+1) \\ a+bx &\mapsto (a+b, a-b) \\ \frac{A+B}{2} + \frac{A-B}{2}x &\mapsto (A, B) \end{aligned}$$

- Hence, the recombination is easy, once receive the (A, B) from the component-wise multiplication, the solution in $\mathbb{Z}[x]/(x^2-1)$ is simply

$$\frac{A+B}{2} + \frac{A-B}{2}x$$

- Check:

$$f(x) \equiv 36 \pmod{x-1}, \quad f(x) \equiv -10 \pmod{x+1}$$

The solution is $f(x) = 13 + 23x$,

- Let's now give a full analysis on the fast multiplication in the ring $\mathbb{Z}[x]/(x^2-1)$ just invented.
- The steps:
  1. Project the ring elements into two "coordinate"-rings.
  2. Perform the multiplication in the "coordinate"-rings.
  3. Recombine the results.
- Let $a+bx$ and $c+dx$ be the two operands,
- The operations used are:
  1. 4 integer add/sub.
  $$a+bx \mapsto (a+b, a-b), \quad c+dx \mapsto (c+d, c-d)$$
  2. 2 integer multiplications
  $$(a+b, a-b)\cdot(c+d, c-d) = ((a+b)(c+d), (a-b)(c-d)) := (A, B)$$
  3. 2 integer add/sub and division by 2.
  $$(A, B) \mapsto \frac{A+B}{2} + \frac{A-B}{2}x$$
  The division by 2 can be done by bit shifting, which is very fast in computer arithmetic.

  Total: 2 integer multiplications, 6 integer add/sub, 2 division by 2.
- The usual multiplication in the ring $\mathbb{Z}[x]/(x^2-1)$ involves 4 integer multiplications, 2 integer add/sub.

REFERENCES I