NTRU FOR GROUP ALGEBRAS

JACKSON WALTERS

1. NTRU Over Finite Group Algebras

Classical NTRU is usually formulated in the quotient ring

$$R = \mathbb{Z}[x]/(x^N - 1).$$

This ring has a natural interpretation as a group algebra. If C_N is the cyclic group of order N, with generator r, then

$$\mathbb{Z}[C_N] \cong \mathbb{Z}[x]/(x^N - 1), \qquad r^i \leftrightarrow x^i.$$

Thus classical NTRU can be viewed as an encryption scheme over the group algebra of a cyclic group. The package `ntru-group-algebra` generalizes this idea by replacing C_N with a more general finite group G, such as a dihedral group or a symmetric group.

1.1. **The Group Algebra Setting.** Let G be a finite group. The integral group algebra $\mathbb{Z}[G]$ consists of formal sums

$$a = \sum_{g \in G} a_g g, \qquad a_g \in \mathbb{Z}.$$

Addition is coefficientwise, and multiplication is induced by the group law:

$$\left(\sum_{g \in G} a_g g\right)\left(\sum_{h \in G} b_h h\right) = \sum_{g,h \in G} a_g b_h (gh).$$

When $G = C_N$, this is exactly cyclic convolution modulo $x^N - 1$. For a nonabelian group, such as a dihedral or symmetric group, the multiplication is generally noncommutative, so the order of factors matters.

For moduli p and q, we work in

$$(\mathbb{Z}/p\mathbb{Z})[G] \qquad \text{and} \qquad (\mathbb{Z}/q\mathbb{Z})[G].$$

1.2. **Basic NTRU-Style Construction.** Choose a small private element

$$f \in \mathbb{Z}[G]$$

which is invertible modulo both p and q. Write its inverses as

$$F_p \equiv f^{-1} \pmod{p}, \qquad F_q \equiv f^{-1} \pmod{q}.$$

Choose another small element $g \in \mathbb{Z}[G]$. The public key is

$$h \equiv F_q g \pmod{q}.$$

To encrypt a plaintext m, whose coefficients are centered modulo p, choose a small random blinding element r, and compute

$$e \equiv phr + m \pmod{q}.$$

To decrypt, multiply on the left by f:

$$fe \equiv f(phr + m) \equiv pfhr + fm \pmod{q}.$$

Since $h \equiv F_q g \pmod{q}$, we have

$$fhr \equiv fF_q gr \equiv gr \pmod{q}.$$

Therefore

$$fe \equiv pgr + fm \pmod{q}.$$

If the coefficients of $pgr + fm$ are small enough that reduction modulo q does not wrap them around, center-lifting recovers the integer element

$$pgr + fm.$$

Reducing modulo p kills the first term:

$$pgr + fm \equiv fm \pmod{p}.$$

Finally, multiplying by F_p recovers the message:

$$F_p(fm) \equiv m \pmod{p}.$$

Thus the scheme follows the same structure as classical NTRU, but with polynomial multiplication replaced by multiplication in $\mathbb{Z}[G]$.

1.3. **Why This Generalizes Classical NTRU.** Classical NTRU is recovered by taking

$$G = C_N.$$

In that case, each group algebra element

$$\sum_{i=0}^{N-1} a_i r^i$$

corresponds to a polynomial

$$\sum_{i=0}^{N-1} a_i x^i$$

modulo $x^N - 1$. The group law $r^i r^j = r^{i+j}$ becomes cyclic polynomial multiplication. Therefore

$$\mathbb{Z}[C_N] \cong \mathbb{Z}[x]/(x^N - 1),$$

and the group-algebra construction is literally classical NTRU in the cyclic case.

Replacing C_N by another finite group G gives an NTRU-style system over a different algebraic platform. When G is nonabelian, the algebra becomes noncommutative, so one must fix a consistent convention. In this package, we use the left-sided convention

$$h = F_q g, \qquad e = phr + m, \qquad \text{decrypt by computing } fe.$$

1.4. **Fast Multiplication Using Fourier Transforms.** Naive multiplication in $\mathbb{Z}[G]$ costs roughly

$$O(|G|^2)$$

coefficient operations, because every pair of group elements can contribute to the product.

For suitable finite fields, we can accelerate multiplication using the finite group Fourier transform. Over a semisimple group algebra, the Fourier transform decomposes an element into matrix blocks indexed by irreducible representations:

$$a \longmapsto \{\widehat{a}(\rho)\}_{\rho \in \widehat{G}}.$$

Under this transform, group-algebra multiplication becomes blockwise matrix multiplication:

$$\widehat{ab}(\rho) = \widehat{a}(\rho)\widehat{b}(\rho),$$

up to the normalization convention used by the transform.

The package uses the auxiliary packages

`fft-dihedral` and `fft-symmetric`

to accelerate multiplication for dihedral and symmetric group algebras. The dihedral case uses the representation theory of D_{2n}, while the symmetric case uses Young's seminormal representations for S_n. In compatible prime fields, this gives a fast transform-based multiplication routine instead of dense convolution over all pairs of group elements.

1.5. **Research Status.** This construction should be viewed as research software, not production cryptography. It demonstrates that classical NTRU naturally extends from the cyclic group algebra $\mathbb{Z}[C_N]$ to more general group algebras $\mathbb{Z}[G]$. The main computational challenge is efficient arithmetic in these group algebras, especially multiplication and inversion. Fourier transforms provide one route to fast arithmetic when the underlying field and group representation theory are compatible.