BFV Homomorphic Encryption Part 2 - Rounding Polynomials

Notes by Linus Tang.

These notes have not been thoroughly reviewed. Any errors below are my own responsibility.

Sources:
- The original scheme by (Zvika Brakerski), Junfeng Fan, Frederik Vercauteren:
  - https://eprint.iacr.org/2012/144.pdf
- An improvement by Hao Chen and Kyoohyung Han:
  - https://eprint.iacr.org/2018/067.pdf

These notes are almost entirely based on the paper by Chen and Han. In section 2, we generalize some of the propositions from Chen and Han, and present substantially different proofs.

Assumed background knowledge:
- Comfortability with modular arithmetic and polynomials in one variable
  - If you're just here for the math, that's all you need; go ahead and read section 2, and perhaps try to prove the propositions yourself before reading the solutions.
  - If you want the cryptographic context, read Part 1 first!
    - https://www.mit.edu/~linust/files/BFV_Homomorphic_Encryption_Part_1.pdf

Contents

1. Recap on BFV Bootstrapping

Bootstrapping is the most expensive operation in any FHE scheme. In 2012, Junfeng Fan and Frederik Vercauteren showed how to bootstrap a ciphertext to lower noise by computing the decryption function

$$(\mathsf{C}_1, \mathsf{C}_2, \mathsf{SK}) \mapsto \left[\left\lfloor \frac{\mathsf{C}_1 + \mathsf{C}_2 \cdot \mathsf{SK}}{\Delta} \right\rceil\right]_t$$

homomorphically, in a circuit with multiplicative depth $O(\log t + \log N)$. The difficulty of writing this circuit came from the division and rounding. They prepared for this step by performing the addition in binary with a ciphertext for each binary digit. Then dividing and rounding became a simple matter of truncating some binary digits.

In 2018, Hao Chen and Kyoohyung Han found an alternate method of handling the rounding operation homomorphically. Their solution allows t and q to be powers of any prime p and involves finding a low-degree polynomial that removes the last base-p digit from a number.

2. Digit Removal Polynomials

In this section we present the relevant mathematical tools in a mostly self-contained manner.

Let p be a prime and Z_p be a set of representatives of $\mathbb{Z}/p\mathbb{Z}$, that is, a set of p integers that leave distinct remainders upon division by p.

For an integer x, let $[x]_p$ denote the element of Z_p that is congruent to x mod p.

More generally, for a positive integer v, let $[x]_{p^v}$ be the unique integer $x_0 + px_1 + \cdots + p^{v-1}x_{v-1}$ that is congruent to x mod p, where $x_0, \ldots, x_{v-1} \in Z_p$.

Proposition 0.1: There exists a degree-p polynomial F with the following property: For all positive integers k and all $z_0 \in Z_p$, and all integers z,

$$z \equiv z_0 \pmod{p^k} \Rightarrow F_e(z) \equiv z_0 \pmod{p^{k+1}}.$$

For example, if $p = 2$ and $Z_p = \{0, 1\}$, then $F_e(x) = x^2$ works for all e.

We present two proofs below.

Proof 1. Use Lagrange interpolation to find a polynomial f of degree at most $p - 1$ such that

$$f(z_0) = \frac{z_0^p - z_0}{p}$$

for all $z_0 \in Z_p$. This is possible because the elements of Z_p are distinct mod p.

We show that $F(z) = z^p - pf(z)$ works.

Indeed, for $z_0 \in Z_p$ and $z = z_0 + p^k z_1$, we have

$$\begin{aligned} F(z) &= \left(z_0 + p^k\right)^p - pf\left(z_0 + p^k z_1\right) \\ &\equiv \left(z_0^p + p \cdot z_0^{p-1} p^k + \cdots\right) - pf(z_0) \\ &\equiv z_0^p - p\left(\frac{z_0^p - z_0}{p}\right) \\ &= z_0, \end{aligned}$$

as desired.

Proof 2. The polynoial $F(z) = z + \prod_{j \in Z_p} (z - j)$ works.

Indeed, for $z_0 \in Z_p$ and $z = z_0 + p^k z_1$, we have

$$\prod_{\substack{j \in Z_p, \\ j \neq z_0}} (z - j) \equiv -1 \pmod{p}$$

by Wilson's Theorem, so

$$\begin{aligned} F(z) &= \left(z_0 + p^k z_1\right) + \prod_{j \in Z_p} (z - j) \\ &= \left(z_0 + p^k z_1\right) + p^k z_1 \prod_{\substack{j \in Z_p, \\ j \neq z_0}} (z - j) \\ &= z_0 + p^k z_1 \left(1 + \prod_{\substack{j \in Z_p, \\ j \neq z_0}} (z - j)\right) \\ &\equiv z_0 \pmod{p^{e+1}}. \end{aligned}$$

We are also interested in constructing a family of low-degree polynomials G_e which computes a specific function mod p^e.

We first present a simple proof that a degree $\leq ep - 1$ is achievable, then a more involved proof that achieves degree $\leq (e-1)(p-1) + 1$.

Proposition 0.2: For all positive integers e, there exists a degree $\leq ep - 1$ polynomial G_e such that for all integers z,

$$G_e(z) \equiv [z]_p \pmod{p^e}.$$

Proof. Note that $F^{e-1}(z)$ (meaning F composed with itself $e-1$ times) is a high-degree polynomial which satisfies

$$F^{e-1}(z) \equiv [z]_p \pmod{p^e}$$

for all z.

By polynomial long division, we can write $F^{e-1}(z) = z(z-1)...(z-ep+1)Q(z) + G_e(z)$ for some polynomial G_e of degree at most $ep - 1$. Furthermore, we have

$$G_e(z) \equiv F^{e-1}(z) \equiv [z]_p \pmod{p^e}$$

because $z(z-1)\cdots(z-ep+1) \equiv 0 \pmod{p^e}$ for all integers z.

Proposition 0.3: For all positive integers e, there exists a degree $\leq (e-1)(p-1) + 1$ polynomial G_e such that for all integers z,

$$G_e(z) \equiv [z]_p \pmod{p^e}.$$

Proof. Let Δ^k denote the kth finite difference operator. [TODO: Spell out definition]

The main claim is as follows:

Suppose function $h : \mathbb{Z} \to \mathbb{Z}$ and integers $k \geq 0$ and $e \geq 1$ satisfy both of the following:
- There exists an integer polynomial g_1 such that $g_1(z) \equiv h(z) \pmod{p^e}$ for all z.
- $\Delta^d h$ vanishes mod p^e (i.e. $\left(\Delta^d h\right)(z) \equiv 0 \pmod{p^e}$ for all z).

Then there exists an integer polynomial g_2 with degree at most $d-1$ such that $g_2(z) \equiv h(z) \pmod{p^e}$ for all z.

In other words, given an integer function h, if h agrees with some integer polynomial and vanishes under a low-order finite difference, then h agrees with some low-degree integer polynomial.

Proof. [TODO: Prove]

Now we can apply the claim to our target function $h(z) = [z]_p$, by supplying the high-degree polynomial representation $g_1 = F^{e-1}$.

It suffices now to show that $\Delta^{(e-1)(p-1)+2} h$ vanishes mod p^e.

We induct on e. The base case $e = 1$ holds because $\Delta^1 h$ is congruent to 1 mod p everywhere, implying that $\Delta^2 h$ vanishes mod p.

We now assume that

$$h_k = \Delta^{(k-1)(p-1)+2} h$$

vanishes mod p^k and prove that

$$h_{k+1} = \Delta^{k(p-1)+2} h = \Delta^{p-1} h_k$$

vanishes mod p^{k+1}.

Indeed, since h_k vanishes mod p^k and satisfies $h_k(z) = h_k(z+p)$ for all z, we have that

$$\begin{aligned}
(\Delta^p h_k)(z) &= \sum_{i=0}^{p} (-1)^i \binom{p}{i} h_k(z+p-i) \\
&\equiv \sum_{i \in \{0,p\}} (-1)^i \binom{p}{i} h_k(z+p-i) \\
&= h_k(z+p) + (-1)^p h_k(z) \\
&= (1 + (-1)^p) h_k(z) \\
&\equiv 0 \ \left(\mathrm{mod}\, p^{k+1}\right),
\end{aligned}$$

as desired.

This completes the induction. The hypothesis of the claim is satisfied with $d = (p-1)(e-1)+2$, which proves the proposition.

Remark. Propositions 0.1 and 0.3 correspond to Lemmas 2 and 3 in [CH'18]. But I thought their proofs were unnecessarily convoluted so I found more natural proofs.

3. Bootstrapping and Analysis

Recall that the multiplicative depth of a circuit is the maximum number of multiplication gates in any path through the circuit.

In order to bootstrap to low noise, we want to design a circuit $\mathcal{C}$ consisting of additions and multiplications over $(\mathbb{Z}/t\mathbb{Z})[x]/(x^N+1)$, which inputs $\mathsf{Proc}(\mathsf{C}_1, \mathsf{C}_2, \mathsf{SK})$ and outputs $\left[\left\lfloor \frac{\mathsf{C}_1 + \mathsf{C}_2 \cdot \mathsf{SK}}{\Delta} \right\rceil\right]_t$, where $\mathsf{Proc}(\mathsf{C}_1, \mathsf{C}_2, \mathsf{SK})$ is a "preprocessing" function of $\mathsf{C}_1, \mathsf{C}_2, \mathsf{SK}$ of our choice that outputs a tuple of elements of $\mathbb{Z}[x]/(x^N+1)$.

For example, in the original BFV scheme, the processing of $(\mathsf{C}_1, \mathsf{C}_2, \mathsf{SK})$ results in the binary coefficients of SK and some binary digits of the coefficients of C_1 and C_2, which are then fed into the circuit $\mathcal{C}$ whose main component is a binary addition.

[TODO: Finish describing CH bootstrapping]