A3Q5

October 30, 2023 9:34 PM

(a). For $g(x) = 3ab + 5ac + 7bc$.

Let $F_\omega : F^n \to F^n$ be the Fourier transform.

$$F_\omega(g) = F_\omega(3ab + 5ac + 7bc)$$
$$= F_\omega(3ab) + F_\omega(5ac) + F_\omega(7bc)$$
$$= 3F_\omega(ab) + 5F_\omega(ac) + 7F_\omega(bc)$$
$$= 3(F_\omega(a) \cdot F_\omega(b)) + 5(F_\omega(a) \cdot F_\omega(c)) + 7(F_\omega(b) \cdot F_\omega(c)).$$

F_ω is a Linear Transformation.

pointwise products

Hence $g = F_\omega^{-1}(F_\omega(g))$.

There are 4 distinct FFTs needed instead of 9.

(b). Let $c = ab = x^{2d} + \Delta(x)$ where $\deg \Delta(x) < 2d$.

Let F_ω be the Fourier transform of size $n = 2d$. Then

$$F_\omega(x^{2d} + \Delta(x)) = F_\omega(x^n) + F_\omega(\Delta(x)).$$
$$F_\omega(x^n) = [(\omega^i)^n : 0 \le i < n] = [(\underset{1}{\underset{\shortparallel}{\omega^n}})^i : 0 \le i \le n] = [1, 1, \ldots, 1].$$

So to recover $\Delta(x)$ from $F_\omega(ab) = F_\omega(a) \cdot F_\omega(b)$ we need to compute

$$F_\omega^{-1}(F_\omega(a \cdot b) - F_\omega(x^{2d}))$$
$$= F_\omega^{-1}(F_\omega(a) \cdot F_\omega(b) - [1, 1, \ldots, 1]^T).$$
$$= F_\omega^{-1}(F_\omega(\Delta(x)))$$
$$= \Delta(x).$$

This requires 3 FFTs of size $n = 2d$.