Theory and remarks about Lab 3

January 10, 2016

Finding ω and the prime to use

For computing the NTT of a vector with length N, where N is a power of 2 for Fast NTT, the following is required for p:

$$p = k \cdot N + 1 \tag{1}$$

And thus:

$$k = (p - 1)/N \tag{2}$$

For a vector with length 16 k could be 1 such that $1 \cdot 16 + 1 = p = 17$. The function `rootsofunity(N)` finds the next prime number greater than `N`. We can use this to iteratively search for the right k.

Suppose we call the function for $k = 1$:

```
[root prime] = rootsofunity(N)
```

With our root g and prime p we can determine k (see equation 2). Given k we choose $\omega = g^k$. This choice is valid since: $\omega^N \equiv 1(mod\ p)$:

$$\omega^N \equiv (g^k)^N \equiv (g^{(p-1)/N})^N \equiv g^{p-1} \equiv 1(mod\ p) \tag{3}$$

The last step $g^{p-1} = 1$ follows from Femat's little theorem. Apart from this, the NTT is completely analogous to the FFT, except that the result will be in modulus p. Therefore, you will have to apply a modulus operation every time you compute a multiplication or division.

Moreover, for computing the Inverse NTT you will have to read:

$$x[k] = \frac{1}{N} \sum_{n=0}^{N-1} X[n]\omega^{-nk} \tag{4}$$

Note that k is now used as the index of the output signal $x[k]$ (it is not k from equation 2). As:

$$x[k] = N^{-1} \sum_{n=0}^{N-1} X[n]\omega^{-nk} \tag{5}$$

In modular arithmetic, you cannot simply apply division as you would normally do, since you are only working with integers in modulus p. You will have to multiply with the inverse of N, which can be computed with `modinverse(n, p)`.

Conventions in Matlab

To avoid floating-point errors, use `rem(x,p)` instead of `mod(x,p)`.

There are different versions of the FFT based on the root as discussed during the lectures. The FFT in Matlab chooses $\omega = e^{-j2\pi/N}$. If you want to ensure that the results of your own FFT agree with those of Matlab you will have to use $\omega = e^{-j2\pi/N}$. For the inverse transformation you will have to use $\omega = e^{j2\pi/N}$.