18.310 Homework 11 Solutions

Due Tuesday November 26th at 6PM

---

1. Determine the Discrete Fourier transform (over the complex numbers) for the sequence y_0, y_1, y_2, y_3 where $y_0 = 0$, $y_1 = 1$, $y_2 = 2$ and $y_3 = 3$.

   Solution: We have $n = 4$ points. So using the definition of discrete fourier transform:

$$c_k = \sum_{j=0}^{n-1} y_j e^{-2\pi ijk/n},$$

   we get

$$c_0 = 1 + 2 + 3 = 6,$$
$$c_1 = e^{-\pi/2i} + 2e^{-\pi i} + 3e^{-3\pi/2i} = -i - 2 + 3i = 2i - 2,$$
$$c_2 = e^{-\pi i} + 2e^{-2\pi i} + 3e^{-3\pi} = -1 + 2 - 3 = -2,$$

   and

$$c_3 = e^{-3\pi/2i} + 2e^{-3\pi i} + 3e^{-9\pi/2i} = i - 2 - 3i = -2i - 2.$$

   Now take the inverse Fourier transform for the sequence of complex numbers c_0, c_1, c_2, c_3 you just obtained. Show your calculations.

   If we take the inverse given by

$$y_j = \frac{1}{n} \sum_{k=0}^{n-1} c_k e^{2\pi ijk/n}$$

   we get

$$y_0 = \frac{1}{4}(6 + 2i - 2 - 2 - 2i - 2) = 0,$$
$$y_1 = \frac{1}{4}(6 + (2i - 2)e^{\pi/2i} - 2e^{\pi i} - (2i + 2)e^{3\pi/2i}) = \frac{1}{4}(6 + (-2 - 2i) + 2 - (2 - 2i)) = 1,$$
$$y_2 = \frac{1}{4}(6 + (2i - 2)e^{\pi i} - 2e^{2\pi i} - (2i + 2)e^{3\pi i}) = \frac{1}{4}(6 + (-2i + 2) - 2 + (2i + 2)) = 2,$$
$$y_3 = \frac{1}{4}(6 + (2i - 2)e^{3\pi/2i} - 2e^{3\pi i} - (2i + 2)e^{9\pi/2i}) = \frac{1}{4}(6 + (2 + 2i) + 2 - (-2 + 2i)) = 3$$

   justifying its name.

2. Suppose we want to multiply two binary numbers u and v using Discrete Fourier Transforms performed over $\mathbb{Z}_p$ for an appropriate prime p. For simplicity, let's assume that u and v have only 4 bits (for just 4 bits, it will be much more cumbersome than doing the usual long multiplication, but you probably don't want to have a homework problem in which you need to multiply two 10^6-bit integers....). It will be easier for you if you use excel for the various

calculations in this exercise. We will need to compute the Discrete Fourier Transforms of u and v, multiply the corresponding coefficients, and take the inverse Fourier transform, and then perform the carryover to get the product of u and v in binary. Since the product of u and v can have 8 bits, we will be performing Fourier transforms on sequences of $n = 8$ numbers. (Thus, if we are multiplying $u = 1010$ (ten in binary) by $v = 0111$ (seven in binary), we would see these numbers as 00001010 and 00000111, and hope to get seventy in binary as the product.)

(a) Explain why we can use $p = 17$ in this specific case of multiplying two 4-bit numbers. Can we use any smaller p (remember p has to be a prime)? Explain. What would be the smallest prime p you would use if we were multiplying two 8-bit numbers?

Solution: There are two conditions that p need to satisfy. The first one is that it needs to be large enough so that we can recover the coefficients of the convolution from their values modulo p. The coefficients of the convolution will be between 0 and $4 \cdot 1^2 = 4$ and so for this purpose we need to take $p \geq 5$. (The 2^{2b} bound in the lecture notes is an upper bound to the real bound which is $(2^b - 1)^2$, the largest product possible with b bits. In our case $b = 1$ so the real bound is $4(2-1)^2 = 4$.) The second condition is that our prime p needs to have an n-th root of unity (here $n = 8$); for this, we need that p satisfies the equation $p = mn + 1$ with m integer. The first one to satisfy it is $p = 17$, and that's why we use it.

In the case of multiplying two 8 bit integers, we get that the maximum coefficient of the convolution is 8, so using $p > 8$ are candidates. Since we are looking at products of size at most 16 bits, we need to find a prime with a 16th root of unity, i.e. $p = 16m + 1$. So 17 also works in this case.

(b) What are all the *primitive* 8th-root of unity over $\mathbb{Z}_{17}$ (read the lecture notes or use excel...)?

Solution: From the lecture notes: The 8th roots of unity are 2, 8, 9 ad 15. For example $2^8 = 256 = 17 \times 15 + 1$.

(c) Suppose we use $z = 2$ as a primitive 8th-root of unity. What is $z^{-1} \pmod{17}$?

Solution: Since 2 is an 8th root of unity $2^{-1} = 2^7 = 128 = 9 \pmod{17}$.

(d) Using $\mathbb{Z}_{17}$ and $z = 2$ as primitive 8th-root of unity, what is the Discrete Fourier transform for $u = 00001010$ (i.e., for the sequence with $u_i = 1$ for $i \in 1, 3$ and 0 for $i \in \{0, 2, 4, 5, 6, 7\}$)? Call it a. And what is b, the DFT for $v = 00000111$? Remember that, here, the DFT of $(y_0, y_1, \cdots, y_{n-1})$ is given by

$$c_k \equiv \sum_{j=0}^{n-1} y_j \left(z^{-1}\right)^{jk} \pmod{17},$$

for $k = 0, \cdots, n-1$.

Solution: I will drop the symbol $\pmod{17}$ in the next calculations, to make it easier to read. First it will be useful to list the powers of $2^{-1} = 9$. They are

$$9^0 = 0, 9^1 = 9, 9^2 = 13, 9^3 = 15, 9^4 = 16, 9^5 = 8, 9^6 = 4, 9^7 = 2.$$

Using the formula we get that

$$a_0 = 1 + 1 = 2,$$

$$a_1 = 9 + 9^3 = 7,$$
$$a_2 = 9^2 + 9^6 = 0,$$
$$a_3 = 9^3 + 9 = 7,$$
$$a_4 = 9^4 + 9^4 = 15,$$
$$a_5 = 9^5 + 9^7 = 10,$$
$$a_6 = 9^6 + 9^2 = 0,$$
$$a_7 = 9^7 + 9^5 = 10.$$

So $a = (2, 7, 0, 7, 15, 10, 0, 10)$. In a very similar fashion we obtain

$$b = (3, 6, 13, 3, 1, 5, 4, 7).$$

(e) Multiply the corresponding coefficients (over $\mathbb{Z}_{17}$) and compute the inverse DFT (remember that in the DFT you will be using $z = 2$ rather than z^{-1}, and that there will be an additional factor n^{-1} (mod 17). Is this what you expected? How much is uv in binary?

Solution: Since we are regarding the numbers as polynomials, multiplying this polynomials corresponds to a convolution of their coefficients, which in transform domain corresponds to usual multiplication, so the transform of the coefficients of the multiplied polynomial corresponds to

$$ab = (6, 8, 0, 4, 15, 16, 0, 2).$$

First notice that $8^{-1} = 2^{-3} = 2^5 = 32 = 15$, and the powers of 2 are of course the inverse table to the powers of 9:

$$2^0 = 1, 2^1 = 2, 2^2 = 4, 2^3 = 8, 2^4 = 16, 2^5 = 15, 2^6 = 13, 2^7 = 9.$$

Call the coefficients of the multiplied polynomials d_k for $k = 0, \ldots, 7$, then we may calculate them from ab using the inverse transform:

$$d_0 = 15(6 + 8 + 4 + 15 + 16 + 2) = 0,$$

$$d_1 = 15(6, 8, 0, 4, 15, 16, 0, 2) \cdot (1, 2, 4, 8, 16, 15, 13, 9) = 15(6+16+32+240+240+18) = 1,$$
$$d_2 = 15(6, 8, 0, 4, 15, 16, 0, 2) \cdot (1, 4, 16, 13, 1, 4, 16, 13) = 1,$$

and similarly
$$d_3 = 2, d_4 = 1, d_5 = 1, d_6 = 0, d_7 = 0.$$

So $d = (0, 1, 1, 2, 1, 1, 0, 0)$. If we remember we are looking at coefficients of a polynomial, we get that the product is then $2 + 4 + 16 + 16 + 32 = 70$, which is correct since our initial numbers were 10 and 7. The product in binary can be seen by carrying over the elements in d, so we get 01000110(remember elements in d are in inverse order per our definition of u and v.

18.310 Principles of Discrete Applied Mathematics
Fall 2013