BLACKBOARD PROOFS

CSE202 – WEEK 3

1. Properties of primitive roots of unity

1. If ω is a primitive nth root of unity, then so is ω^{-1}.

Proof. First ω is invertible, since $\omega^n = 1 = \omega\omega^{n-1}$ shows that ω^{n-1} is the inverse of ω. Next, multiplying both sides of $\omega^n = 1$ by ω^{-n} gives $1 = \omega^{-n} = (\omega^{-1})^n$, which shows that ω^{-1} is a nth root of 1. It is primitive since if $\omega^{-t} = 1$, then multiplying both sides by ω^t implies $1 = \omega^t$, which cannot happen for $t \in \{1, \ldots, n-1\}$ since ω is primitive. □

2. If $n = pq$ then ω^p is a primitive qth root of unity.

Proof. It is a qth root of 1 since $(\omega^p)^q = \omega^{pq} = \omega^n = 1$. It is primitive, since $(\omega^p)^t = \omega^{pt}$ and $t \in \{1, \ldots, q-1\}$ implies $pt \in \{1, \ldots, n-p\}$ and $(\omega^p)^t \neq 1$ for those values. □

3. For $\ell \in \{1, \ldots, n-1\}$, $\displaystyle\sum_{j=0}^{n-1} \omega^{\ell j} = 0$.

Proof.

$$\underbrace{(1-\omega^\ell)}_{\neq 0}(1 + \omega^\ell + \cdots + \omega^{(n-1)\ell}) = 1 - \omega^{n\ell} = 0$$

shows that the second factor in the left-hand side is 0. □

2. The DFT of a linear combination of cosines

By linearity it is sufficient to consider the DFT of

$$c\cos(kx+\ell) = c\frac{e^{i\ell}e^{ikx} + e^{-i\ell}e^{-ikx}}{2},$$

given by its evaluations at $(0, 2\pi/n, \ldots, 2(n-1)\pi/n)$. Again by linearity, this DFT decomposes as

$$\frac{ce^{i\ell}}{2}\operatorname{DFT}_\omega(1, e^{2ik\pi/n}, \ldots, e^{2ik(n-1)\pi/n}) + \frac{ce^{-i\ell}}{2}\operatorname{DFT}_\omega(1, e^{-2ik\pi/n}, \ldots, e^{-2ik(n-1)\pi/n}).$$

Since in this computation $\omega = e^{-2i\pi/n}$, this rewrites

$$\frac{ce^{i\ell}}{2}\operatorname{DFT}_\omega(1, \omega^{-k}, \ldots, \omega^{-k(n-1)}) + \frac{ce^{-i\ell}}{2}\operatorname{DFT}_\omega(1, \omega^{k}, \ldots, \omega^{k(n-1)}).$$

The first $\operatorname{DFT}_\omega$ in this sum is the evaluation of

$$1 + \omega^{-k}X + \cdots + \omega^{-k(n-1)}X^{n-1}$$

at the powers of ω. Clearly, at $X = \omega^k$, all summands are equal to 1 and the sum is n. At $X = \omega^j$ with $j \neq k$, the polynomial evaluates to the sum of the first n $\omega^{j-k} = \omega^{n-k+j}$. By the 3rd part of the properties of Section 1, that sum is 0.

Thus we obtain that the first DFT_ω is 0 everywhere except at index k, where it is n. Similarly, the second one is everywhere 0, except at index $n-k$, where it is n. The final formula is obtained by linear combination.

3. Lemma for Divide-and-Conquer

Since $n = 2k$ and $\omega^n = 1$, it follows that

$$0 = \omega^n - 1 = (\omega^k - 1)(\omega^k + 1).$$

Now, since ω is a *primitive* root of 1, $\omega^k \neq 1$ and therefore the last term of the product is 0, ie, $\omega^k = -1$.

Alternatively, this is a special case of part 2 of the properties of primitive roots of unity, with $q = k$ and $p = 2$, as -1 is the only primitive root of unity of order 2.

4. Proof of correctness of the FFT algorithm

For $n = 1$, the algorithm must return $A(1)$, which is a_0 in that case.

Otherwise, since n is a power of 2, k is well-defined and strictly smaller than n, which gives termination of the algorithm.

By Slide 15, the polynomials R_e and R_o are the remainders of the Euclidean division of A by $X^k - 1$ and $X^k + 1$. Then by Slide 14, for all m, R_e and S_o are such that $R_e(\omega^{2m}) = A(\omega^{2m})$ while $S_o(\omega^{2m}) = R_o(\omega^{2m+1}) = A(\omega^{2m+1})$, which concludes the proof.