Problem 4, TFJM

Equipe d'Orsay

April 9, 2012

0.1 Preliminaries on roots of unity

We will denote by ζ_n the complex number $e^{\frac{2i\pi}{n}}$. Let Φ_n be the nth cyclotomic polynomial, i.e. the monic polynomial whose roots are the primitive nth roots of unity. For instance, if p is a prime, then

$$\Phi_p = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + ... + X + 1,$$

since all nontrivial pth roots of unity are primitive. We will need the following classical, but difficult result:

Theorem 0.1. *The polynomial Φ_n has integer coefficients and is irreducible in $\mathbf{Q}[X]$.*

The fact that Φ_n has integer coefficients follows by induction from the identity

$$\prod_{d|n} \Phi_d = X^n - 1,$$

which is a consequence of the fact that any nth root of unity is a primitive root of order d for a unique $d|n$. The irreducibility assertion is much harder and we will admit it. When n is a prime, the proof is easier, since we can apply directly Eisenstein's irreducibility criterion to $\Phi_p(X + 1)$.

Corollary 0.2. *If $f \in \mathbf{Q}[X]$ is a polynomial such that $f(\zeta_n) = 0$, then Φ_n divides f.*

Proof. Since Φ_n is irreducible in $\mathbf{Q}[X]$, we have $\gcd(f, \Phi_n) \in \{1, \Phi_n\}$. We cannot have $\gcd(f, \Phi_n) = 1$, as otherwise there would be $A, B \in \mathbf{Q}[X]$ such that $Af + B\Phi_n = 1$ and evaluating at ζ_n would yield $0 = 1$. Hence $\gcd(f, \Phi_n) = \Phi_n$ and Φ_n divides f. □

We will frequently use the following result, which is just a translation of the previous corollary:

Lemma 0.3. *Let p be a prime and let $a_0, a_1, ..., a_{p-1} \in \mathbf{Q}$. Then $a_0 + a_1\zeta_p + ... + a_{p-1}\zeta_p^{p-1} = 0$ if and only if $a_0 = a_1 = ... = a_{p-1}$.*

Proof. One implication is immediate, since

$$1 + \zeta_p + ... + \zeta_p^{p-1} = \frac{\zeta_p^p - 1}{\zeta_p - 1} = 0.$$

For the other implication, the corollary shows that $a_0 + a_1 X + ... + a_{p-1} X^{p-1}$ is a multiple of $\Phi_p = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + ... + X + 1$. Since it has degree at most $p-1$, there must exist a constant c such that $a_0 + a_1 X + ... + a_{p-1} X^{p-1} = c\Phi_p$, and the result follows. □

The previous lemma has a stronger form, which we will take for granted, since it requires more input from abstract algebra. Before giving the statement, let us introduce the useful notation

$$\mathbf{Q}(\zeta_n) = \{f(\zeta_n) | \quad f \in \mathbf{Q}[X]\}.$$

Lemma 0.4. *Let p_1, p_2 be distinct prime numbers, ζ a root of Φ_{p_1} and $x_0, ..., x_{p_1 - 1} \in \mathbf{Q}(\zeta_{p_2})$. Then $\sum_{j=0}^{p_1 - 1} x_j \zeta^j = 0$ if and only if $x_0 = x_1 = ... = x_{p_1 - 1}$.*

Proof. One implication is clear, so assume that $\sum_{j=0}^{p_1 - 1} x_j \zeta^j = 0$. Then $\sum_{j=0}^{p_1 - 2} y_j \zeta^j = 0$, where $y_j = x_j - x_{p_1 - 1}$. We can write $y_j = \sum_{k=0}^{p_2 - 2} a_{kj} \zeta_{p_2}^k$ for some rational numbers a_{kj}. Then

$$\sum_{k=0}^{p_2 - 2} \sum_{j=0}^{p_1 - 2} a_{kj} \zeta^j \zeta_{p_2}^k = 0.$$

However, using theorem 0.1 and abstract algebra, one can prove that the numbers $(\zeta^j \zeta_{p_2}^k$ are linearly independent over $\mathbf{Q}$, so the previous relation yields $a_{kj} = 0$ for all k, j and so $y_j = 0$ for all j. This proves the lemma. □

Without loss of generality, we will assume in the following that the affixes of the regular n-gon are ζ_n^k, with $0 \leq k < n$. Then the centroid of the polygon is the origin of the plane. Hence, giving a stable subset of vertices of the polygon is the same as giving an n-tuple of integers $(a_0, ..., a_{n-1})$, where each a_i equals 0 or 1 and where $a_0 + a_1 \zeta_n + ... + a_{n-1} \zeta_n^{n-1} = 0$ (we consider the empty set as stable, corresponding to the sequence $(0, 0, ..., 0)$).

0.2 Question 1

Let p be a prime number. Recall that we need to find the number of sequences $(a_0, ..., a_{p-1})$, where $a_i \in \{0, 1\}$ and $\sum_{i=0}^{p-1} a_i \zeta_p^i = 0$. By lemma 0.3, this relation is equivalent to $a_0 = a_1 = ... = a_{p-1}$. Recalling that we decided to count the empty set as a stable subset, we deduce that there are 2 stable subsets: the empty set and the set consisting of all vertices of the polygon.

0.3 Question 2

Suppose that p_1, p_2 are different prime numbers and let $n = p_1p_2$. We need to find the number of sequences $(a_k)_{0\leq k<n}$ such that $a_k \in \{0, 1\}$ for all k and

$$\sum_{k=0}^{p_1p_2-1} a_k\zeta_{p_1p_2}^k = 0.$$

Splitting the indices modulo p_1 and noting that $\zeta_{p_1p_2}^{kp_1+j} = \zeta_{p_1p_2}^j\zeta_{p_2}^k$, the previous relation becomes

$$\sum_{k=0}^{p_2-1}\sum_{j=0}^{p_1-1} a_{kp_1+j}\zeta_{p_1p_2}^j\zeta_{p_2}^k = 0,$$

and this is also equivalent to

$$\sum_{j=0}^{p_1-1}(\sum_{k=0}^{p_2-1} a_{kp_1+j}\zeta_{p_2}^k)\zeta_{p_1p_2}^j = 0.$$

If we set $x_j = \sum_{k=0}^{p_2-1} a_{kp_1+j}\zeta_{p_2}^k$, then $x_j \in \mathbf{Q}(\zeta_{p_2})$ and the desired relation becomes

$$\sum_{j=0}^{p_1-1} x_j\zeta_{p_1p_2}^j = 0.$$

Next, choose $u, v \in \mathbf{Z}$ such that $up_2 + vp_1 = 1$ (they exist by Bézout's theorem). Then

$$\zeta_{p_1p_2} = \zeta_{p_1p_2}^{up_2+vp_1} = \zeta_{p_1}^u\zeta_{p_2}^v,$$

so the previous relation becomes

$$\sum_{j=0}^{p_1-1}(x_j\zeta_{p_2}^{vj})(\zeta_{p_1}^u)^j = 0.$$

Note that $\zeta := \zeta_{p_1}^u$ is a primitive root of unity, of order p_1. Lemma 0.4 shows that the previous relation holds if and only if

$$x_0 = x_1\zeta_{p_2}^v = ... = x_{p_1-1}\zeta_{p_2}^{v(p_1-1)}.$$

Since

$$x_0 = \sum_{k=0}^{p_2-1} a_{kp_1}\zeta_{p_2}^k,$$

we obtain the **intermediate conclusion**: a sequence $(a_0, a_1, ..., a_{p_1p_2-1})$ defines a stable set if and only if there exists a sequence $e = (e_0, ..., e_{p_2-1})$ whose terms are 0 or 1 and such that

$$x_j = \left(\sum_{k=0}^{p_2-1} e_k\zeta_{p_2}^k\right)(\zeta_{p_2}^{-v})^j, \quad \forall 0 \leq j \leq p_1 - 1.$$

Lemma 0.5. *Any sequence $e = (e_0, ..., e_{p_2-1}) \in \{0,1\}^{p_1}$ such that $e \neq (0,0,...,0), (1,1,...,1)$, gives rise to a unique stable set, by the recipe described above.*

Proof. It is enough to prove that for all $0 \leq j < p_1$ there exists a unique sequence $(a_{kp_1+j})_{0 \leq k < p_2} \in \{0,1\}^{p_2}$ such that

$$\sum_{k=0}^{p_2-1} a_{kp_1+j}\zeta_{p_2}^k = (\zeta_{p_2}^{-v})^j \cdot \sum_{k=0}^{p_2-1} e_k \zeta_{p_2}^k.$$

Existence is clear, since $(\zeta_{p_2}^{k-vj})_{0 \leq k < p_2}$ is just a permutation of $(\zeta_{p_2}^k)_{0 \leq k < p_2}$. For uniqueness, assume that a'_{kp_1+j} is another such sequence. Then $\sum_{k=0}^{p_2-1}(a_{kp_1+j} - a'_{kp_1+j})\zeta_{p_2}^k = 0$ and lemma 0.3 yields

$$a_{kp_1+j} - a'_{kp_1+j} = a_j - a'_j$$

for all $0 \leq k < p_2$. If $a_j \neq a'_j$, then since all $a_r \in \{0,1\}$, we must have either $a_{kp_1+j} = 0$ for all k or $a_{kp_1+j} = 1$ for all k. But then $\sum_{k=0}^{p_2-1} a_{kp_1+j}\zeta_{p_2}^k = 0$, so $\sum_{k=0}^{p_2-1} e_k \zeta_{p_2}^k = 0$. Lemma 0.3 shows that e_k are all equal, a contradiction. This finishes the proof of the lemma.

□

It remains to deal with the sequences $e = (0, ..., 0)$ and $e = (1, 1, ..., 1)$. In both cases, the system of equations $x_j = \left(\sum_{k=0}^{p_2-1} e_k \zeta_{p_2}^k\right)(\zeta_{p_2}^{-v})^j$ for all $0 \leq j \leq p_1 - 1$ is equivalent to

$$\sum_{k=0}^{p_2-1} a_{kp_1+j}\zeta_{p_2}^k = 0.$$

This means that for all j we have $a_j = a_{j+p_1} = ... = a_{j+(p_2-1)p_1}$ (by lemma 0.3 again). For each j this yields two possibilities for the sequence $(a_{kp_1+j})_k$ and so the sequences $e = (0, ..., 0)$ and $e = (1, 1, ..., 1)$ yield 2^{p_1} stable sets, described as above.

Finally, we obtain $(2^{p_2} - 2) + 2^{p_1} = 2^{p_1} + 2^{p_2} - 2$ stable sets.

0.4 Question 3

Consider the problem of describing the stable sets for a regular p^n-gon, where p is a prime and $n \geq 2$. This is the same as describing the sequences $(a_0, ..., a_{p^n-1}) \in \{0,1\}^{p^n}$ for which

$$\sum_{i=0}^{p^n-1} a_i \zeta_{p^n}^i = 0.$$

By corollary 0.2, this is equivalent to $\Phi_{p^n} | \sum_{i=0}^{p^n-1} a_i X^i$. Next, the primitive p^nth roots of unity are all p^nth roots of unity except the p^{n-1}th roots of unity, hence

$$\Phi_{p^n} = \frac{X^{p^n} - 1}{X^{p^{n-1}} - 1} = \sum_{j=0}^{p-1} X^{jp^{n-1}}.$$

Hence, if $\Phi_{p^n} | \sum_{i=0}^{p^n-1} a_i X^i$, then we can find rational numbers $b_0, b_1, ..., b_{p^{n-1}-1}$ such that

$$\sum_{i=0}^{p^n-1} a_i X^i = \left(\sum_{j=0}^{p-1} X^{jp^{n-1}} \right) \left(\sum_{k=0}^{p^{n-1}-1} b_k X^k \right)$$

$$= b_0(1 + X^{p^{n-1}} + X^{2p^{n-1}} + ...) + b_1(X + X^{p^{n-1}+1} + ...) + ...$$

Identifying coefficients, we obtain

$$a_j = a_{j+p^{n-1}} = ... = a_{j+(p-1)p^{n-1}}$$

for $0 \leq j < p^{n-1}$. Conversely, if the previous relations are satisfied for $0 \leq j < p^{n-1}$, then an immediate computation yields

$$\sum_{i=0}^{p^n-1} a_i X^i = \Phi_{p^n} \cdot \left(\sum_{j=0}^{p^{n-1}-1} a_j X^j \right).$$

So the stable sets are described by sequences $(a_j)_j$ such that

$$a_j = a_{j+p^{n-1}} = ... = a_{j+(p-1)p^{n-1}}$$

for $0 \leq j < p^{n-1}$. Clearly, there are $2^{p^{n-1}}$ such sets.