Lecture 8: Multiples of a Polynomial with Small Norm

Example: Let $A(x) = \sum_{j=0}^{d} a_j x^j = a_d \prod_{j=1}^{d} (x - \alpha_j) \in \mathbb{Z}[x]$ be divisible by $\Phi_m(x)$, and consider $w(x) \in \mathbb{Z}[x]$ such that $w(x)\Phi_m(x) = x^m - 1$. Then the Euclidean norm of $A(x)w(x)(x^{km} + x^{(k-1)m} + \cdots + x^m + 1)$ for any positive integer k is bounded above by a quantity that is independent of k. For some N, there is $Q(x) \in \mathbb{Z}[x]$ with arbitrarily large Euclidean norm such that $\|AQ\| \leq N$.

Theorem (F. & Solan): Let $A(x) \in \mathbb{Z}[x]$ be a polynomial having no cyclotomic factors. Let $N \geq 1$. If $Q(x) \in \mathbb{Z}[x]$ and $\|A(x)Q(x)\| \leq N$, then $\|Q\|$ is bounded by a function depending only on $A(x)$ and N.

Reduction to Irreducibles: Suppose the theorem is true for irreducible $A(x)$. Then consider $A_0(x) = \prod_{j=1}^{m} f_j(x)$ where the $f_j(x)$ are irreducible non-cylotomic polynomials in $\mathbb{Z}[x]$ and where repeated factors may occur. Apply the theorem with $A(x) = f_k(x)$ where k ranges from 1 to $m-1$.

Reduction to Bounds on Gaps in Exponents of Terms with Non-zero Coefficients: The proof given here for the theorem will be based on considering two cases, one dealing with irreducibles $A(x)$ that contain at least one root inside the unit disk and the other dealing with the case that all the roots of $A(x)$ are on the unit disk. In both cases, we consider $P(x) = A(x)Q(x) = \sum_{j=1}^{n} c_j x^{d_j}$ where $0 = d_1 < d_2 < \cdots < d_n = \deg P(x)$ and each c_j non-zero. Define $P_J(x) = \sum_{j=1}^{J} c_j x^{d_j}$ (and $P_0(x) = 0$). We will show that if $A(x) \nmid P_J(x)$, then $d_{J+1} \leq C(d_J + D)$ where $C \geq 1$ and $D \geq 1$ depend only on $A(x)$ and N. We explain here why this is sufficient.

Consider three cases: (i) $A(x) \nmid P_J(x)$ for all $J \in \{1, 2, \dots, n-1\}$, (ii) $A(x)|P_J(x)$ for some J and $d_{J+1} - d_J \leq N^2 C^{N^2} D$ for all $J \leq n-1$, and (iii) for some $J \leq n-1$, $d_{J+1} - d_J > N^2 C^{N^2} D$. For (i), $d_{J+1} \leq C(d_J + D)$ implies $d_J \leq JC^J D$ for each J so that $\deg P = d_n \leq nC^n D$. Note that $n \leq \|P\|^2 \leq N^2$ so that $\deg P \leq N^2 C^{N^2} D$. Since Q is a factor of a polynomial with degree and norm bounded by functions of $A(x)$ and N, so is the norm of Q. For (ii), sum the inequality $d_{J+1} - d_J \leq N^2 C^{N^2} D$ over J to deduce $\deg P \leq nN^2 C^{N^2} D \leq N^4 C^{N^2} D$, and the bound on the norm of Q follows.

For (iii), let $S = \{J_1, J_2, \dots, J_r\}$ and $S' = S \cup \{0\}$ be such that $1 \leq J_1 < J_2 < \cdots < J_r \leq n-1$ and $J \in S$ if and only if $d_{J+1} - d_J > N^2 C^{N^2} D$. We show $A(x)|P_J(x)$ for each $J \in S$. Assume otherwise, and let $i \in \{1, 2, \dots, r\}$ be minimal such that $A(x) \nmid P_{J_i}(x)$. Let $J' \in \{1, 2, \dots, J_i - 1\}$ be maximal such that $A(x)|P_{J'}(x)$. Consider $(P(x) - P_{J'}(x))/x^{d_{J'+1}}$, a multiple of $A(x)$ with norm $\leq \|P\| \leq N$. Hence, $d_{J+1} - d_{J'+1} \leq C(d_J - d_{J'+1} + D)$ for $J' < J \leq J_i$. Using the argument of (i), $d_{J_i+1} - d_{J'+1} \leq N^2 C^{N^2} D$, contradicting $d_{J_i+1} - d_{J'+1} \geq d_{J_i+1} - d_{J_i} > 2dN^2 C^{N^2}$. Thus, $A(x)|P_J(x)$ for each $J \in S$. Write $P(x) = \sum_{J \in S'} h_J(x) x^{d_{J+1}}$ in the obvious way so that $A(x)|h_J(x)$ for each $J \in S'$. Setting $w_J(x) = h_J(x)/A(x)$, $Q(x) = \sum_{J \in S'} w_J(x) x^{d_{J+1}}$. Either (i) or (ii) applies with with $P(x)$ replaced by $h_J(x)$ so that the norm of each $w_J(x)$ is bounded by a function of $A(x)$ and N. Since $r + 1 \leq n \leq N^2$, the same is true of the norm of Q.

Lemma 1. Suppose $A(x)$ is irreducible and has a root with absolute value < 1. Let N be such that $\|P\| \leq N$, and let $J \in \{1, 2, \dots, n-1\}$. If $A(x)|P(x)$ and $A(x) \nmid P_J(x)$, then $d_{J+1} \leq C(d_J + 2d)$ where $C = \log N / \log(M(A)/|a_0|)$.

Lemma 2. Suppose the roots of $A(x)$ are distinct and have absolute value ≥ 1. Suppose further that no root of $A(x)$ is a root of unity. Let N be such that $\|P\| \leq N$, and let $J \in \{1, 2, \ldots, n-1\}$. If $A(x)|P(x)$ and $A(x) \nmid P_J(x)$, then $d_{J+1} - d_J \leq 2^d d^{d^2+d} N^{2d} \|A\|^{2d^2-2d}$.

Proof of Lemma 1:

- Let R_J denote the resultant of $A(x)$ and $P_J(x)$, and let λ denote the number of roots of $A(x)$ having absolute value < 1.
- By properties of resultants,

$$1 \leq |R_J| = |a_d|^{d_J} \prod_{j=1}^{d} |P_J(\alpha_j)| = |a_d|^{d_J} \prod_{|\alpha_j|<1} |P(\alpha_j) - P_J(\alpha_j)| \prod_{|\alpha_k|\geq 1} |P_J(\alpha_k)|$$

$$\leq |a_d|^{d_J} \prod_{|\alpha_j|<1} \left(|\alpha_j|^{d_{J+1}} \sum_{h=J+1}^{n} |c_h| \right) \prod_{|\alpha_k|\geq 1} \left(|\alpha_k|^{d_J} \sum_{i=1}^{J} |c_i| \right) \leq \left(\frac{|a_0|}{M(A)} \right)^{d_{J+1}} M(A)^{d_J} N^{2d}.$$

- Taking logarithms produces the bound in the lemma.

Proof of Lemma 2:

- Write $Q(x) = \sum_{j=0}^{m} q_j x^j$ where $q_0 q_m \neq 0$, and define $q_j = 0$ for $j \notin [0, m]$.
- The linear recurrence $0 = a_0 q_k + a_1 q_{k-1} + \cdots + a_d q_{k-d}$ of order d holds for $d_J < k < d_{J+1}$.
- Observe that

$$Q(x) = P(x) \sum_{j=1}^{d} \left(\frac{-1}{\alpha_j A'(\alpha_j)} \right) \frac{1}{1 - x/\alpha_j} = P(x) \sum_{h=0}^{\infty} x^h \sum_{j=1}^{d} \frac{-\alpha_j^{-h}}{\alpha_j A'(\alpha_j)}$$

$$= \sum_{k=0}^{\infty} x^k \sum_{\substack{i \\ d_i \leq k}} c_i \sum_{j=1}^{d} \frac{-\alpha_j^{-(k-d_i)}}{\alpha_j A'(\alpha_j)} = \sum_{k=0}^{\infty} x^k \sum_{j=1}^{d} \frac{-\alpha_j^{-k}}{\alpha_j A'(\alpha_j)} \sum_{\substack{i \\ d_i \leq k}} c_i \alpha_j^{d_i}$$

- Deduce $q_k = \sum_{j=1}^{d} \frac{-P_J(\alpha_j)}{\alpha_j A'(\alpha_j)} \alpha_j^{-k}$ for $1 \leq J \leq n-1$ and $d_J \leq k < d_{J+1}$; since $|\alpha_j| \geq 1$ for each j, we deduce that $|q_k| \leq B_J = \sum_{i=1}^{J} |c_i| \sum_{j=1}^{d} 1/|A'(\alpha_j)|$ for all $k < d_{J+1}$.
- We claim that $d_{J+1} - d_J \leq (2B_J + 1)^d$. Assume otherwise. Then there exists k_1 and k_2 with $d_J \leq k_1 < k_2 < d_{J+1}$ such that $\langle q_{k_1-d+1}, \ldots, q_{k_1} \rangle = \langle q_{k_2-d+1}, \ldots, q_{k_2} \rangle$. Then $\{q_j\}_{k_1-d<j<d_{J+1}}$ is cyclic with cycle length $\omega \leq k_2 - k_1$. Define

$$Q_t(x) = \sum_{j=0}^{d_{J+1}-\omega-1} q_j x^j + \left(\sum_{j=d_{J+1}-\omega}^{d_{J+1}-1} q_j x^j \right) (1 + x^\omega + \cdots + x^{\omega t}) + x^{\omega t} \sum_{j=d_{J+1}}^{m} q_j x^j.$$

  Then $\|Q_t A\| = \|QA\| \leq N$ and $(Q_t(x) - Q(x))A(x) = (x^{\omega t} - 1) \sum_{j=J+1}^{n} c_j x^{d_j}$. From $A(x)|P(x)$, we deduce $A(x)|P_J(x)$, a contradiction.

- The estimate $d_{J+1} - d_J \leq (2B_J + 1)^d$ leads to a bound of the type sought.