

HERMITE'S QUADRATIC FORM

KENNETH R. DRIESSEL

I mainly follow Basu, Pollack and Roy(2003) .

Date: December 11, 2006.

Definition: Let

- $P := X^p + a_{p-1}X^{p-1} + \dots + a_0$ and
- $Q := X^q + b_{q-1}X^{q-1} + \dots + b_0$

be polynomials in $D[X]$ where D is an ordered ring and $q < p$. Let C be an algebraically closed extension of the field of fractions of D . Then **Hermite's quadratic form**, $\text{Herm}(P, Q)$ is defined by

$$\text{Herm}(P, Q) := D^p \rightarrow C :$$

$$(f_1, \dots, f_p) \mapsto \sum \{\mu(x)Q(x)(f_1 + f_2x + \dots + f_px^{p-1})^2 : x \in C \wedge P(x) = 0\}$$

where $\mu(x)$ is the multiplicity of x as a root of P . Note that the (j, k) th entry in the matrix (with respect to the standard basis of D^p) associated with this quadratic form is

$$\sum \{\mu(x)Q(x)x^{j+k-2} : x \in C \wedge P(x) = 0\}$$

since

$$\text{Herm}(P, Q)(f_1, \dots, f_p) = \sum_j^p \sum_k^p \sum \{\mu(x)Q(x)x^{j+k-2} : x \in C \wedge P(x) = 0\}.$$

Definition: Let $H \in D^{n \times n}$ be a square matrix with entries in a ring. Then H is a **Hankel matrix** if it has equal entries on its anti-diagonals – that is, for all i, j, i', j' between 0 and n , $i + j = i' + j' \implies H(i, j) = H(i', j')$. For example, when $n = 4$ a Hankel matrix has the following form:

$$\begin{pmatrix} s_0 & s_1 & s_2 & s_3 \\ s_1 & s_2 & s_3 & s_4 \\ s_2 & s_3 & s_4 & s_5 \\ s_3 & s_4 & s_5 & s_6 \end{pmatrix}.$$

Note that the matrix associated with Hermite's quadratic form is a Hankel matrix.

Definition: Let P and Q be polynomials with coefficients in an ordered ring D . And let R be a real closed extension of the fraction field of D . Then the **Tarski query**, $\text{TaQ}(Q, P)$, is defined by

$$\text{TaQ}(Q, P) := \#\{\text{sign}(Q(x)) : x \in R \wedge P(x) = 0\}$$

where sign is the sign function. (Note that $\text{TaQ}(Q, P)$ is the number of roots of P in R at which Q is positive minus the number of roots of P at which Q is negative.)

We aim to prove the following theorem:

Theorem 1. Hermite's Univariate Root Counting Theorem. *Let D be an ordered ring, let R be a real closed extension of the fraction field of D and let C be an algebraically closed extension of R . Let P and Q be polynomials in $D[X]$ with the degree of Q less than the degree of P . Then*

- $\text{Rank}(\text{Herm}(P, Q)) = \#\{x \in C : P(x) = 0 \wedge Q(x) \neq 0\}$ and

- $\text{Signature}(\text{Herm}(P, Q)) = \text{TaQ}(Q, R)$.

We shall need some preliminary results.

Definition: Let K be a field and let P be a polynomial with degree p with coefficients in K . Let $A := K[X]/(P)$ be the ring of polynomials $K[X]$ modulo P . Note that the map $A \times A \rightarrow A : (f, g) \rightarrow fg$ is a well defined bilinear map on A . For f in A we define the map $L(f)$ by

$$L(f) := A \rightarrow A : g \mapsto fg.$$

Note that $L(f)$ is linear on A . In other words we have a map

$$L : A \rightarrow \text{Lin}(A \rightarrow A) : f \mapsto L(f)$$

where $\text{Lin}(A \rightarrow A)$ is the algebra of linear maps on A .

The following proposition says that the map L is a representation of A . One of the standard guidelines in the study of associative algebras is: “Look at the representations”.

Proposition 1. *Let K, P and L be as in the last definition. Then the map L is a homomorphism from the algebra A into the algebra $\text{Lin}(A \rightarrow A)$.*

Proof. It is easy to see that L is a linear map. We also have $L(f_1 f_2) = L(f_1) \circ L(f_2)$ since $L(f_1 f_2)(g) = f_1 f_2 g = (L(f_1) \circ L(f_2))(g)$. \square

Proposition 2. *For every f in A ,*

$$\text{Trace}(L(f)) = \sum \{\mu(x)f(x) : x \in C \wedge P(x) = 0\}.$$

Proof. The proof is by induction on the number of roots of P in C .

Case: The polynomial P has only one root.

Then $P = (X - x)^p$ where p is the degree of P and x is the root.

Claim: In the algebra A , $(f - f(x))^p = 0$.

Note that x is root of $f(X) - f(x)$. Hence there is a polynomial g such that $f(X) - f(x) = (X - x)g(X)$. Then $(f(X) - f(x))^p = (X - x)^p(g(X))^p$.

Claim: We have $\text{Trace}(L(f)) = pf(x)$.

Since L is an algebra homomorphism we have $L((f - f(x))^p) = 0$; in other words, $L(f - f(x))$ is nilpotent. Hence $\text{Trace}(L(f - f(x))) = 0$. We then have $\text{Trace}(L(f)) = \text{Trace}(f(x)I) = pf(x)$.

This completes the proof of the proposition in this case.

Case: The polynomial P has more than one root.

In this case, there exist polynomials P_1 and P_2 such that $P = P_1 P_2$ and P_1 and P_2 are relatively prime. Since the greatest common divisor of P_1 and P_2 is 1, there exist polynomials U_1 and U_2 such that $P_1 U_1 + P_2 U_2 = 1$. Let $e_1 := U_2 P_2$ and $e_2 := U_1 P_1$.

Claim: In the algebra A we have $e_1 + e_2 = 1$, $e_1 e_2 = 0$, $e_1^2 = e_1$ and $e_2^2 = e_2$. In other words, these two elements are “orthogonal” idempotents in the algebra A . (One of the standard guidelines in the study of associative algebras is: “Look to the idempotents.”)

The first property follows immediately from the definitions of e_1 and e_2 . We also have $e_1e_2 = U_1U_2P = 0$. Hence $e_1^2 = e_1(1 - e_2) = e_1 - e_1e_2 = e_1$. Similarly, e_2 is an idempotent.

Claim: Let $A_1 := K[X]/(P_1)$ and $A_2 := K[X]/(P_2)$. The map

$$A_1 \times A_2 \rightarrow A : (Q_1, Q_2) \mapsto Q_1e_1 + Q_2e_2$$

is an vector space isomorphism.

The map is clearly linear. It is surjective since $Q = (e_1 + e_2)Q = e_1Q + e_2Q$. It is injective since the dimensions of the domain and co-domain are the same; in particular, $\dim A_1 + \dim A_2 = \deg P_1 + \deg P_2 = \deg P = \dim A$.

Claim: The algebras A_1 and A_2 are invariant subspaces for $L(f)$. (Here we are using the last claim to identify each A_i with its image in A .) In particular, if $f_1 := f \bmod P_1$ and $f_2 := f \bmod P_2$ then $L(f_1)$ is the restriction of $L(f)$ to A_1 and $L(f_2)$ is the restriction of $L(f)$ to A_2 . Hence $\text{Trace}(L(f)) = \text{Trace}(L(f_1)) + \text{Trace}(L(f_2))$.

To finish the proof in this case we simply note that the number of distinct roots of P_1 is less than the number of distinct roots of P and the number of distinct roots of P_2 is also less than the number of distinct roots of P . Hence the induction hypothesis applies. □