A NOTE ON FINDING A RATIONAL SYMMETRIC MATRIX FOR A GIVEN SEPARABLE POLYNOMIAL

MICHAEL SOLTYS*

Abstract. Given a separable polynomial $p(x) \in \mathbb{Q}[x]$, which splits in $\mathbb{R}[x]$, is it possible to find a symmetric matrix over $\mathbb{Q}$ whose eigenvalues are precisely the roots of $p(x)$? This note investigates this questions, and provides a condition on $p(x)$ under which it is always possible to find such a matrix—the question whether such a matrix can be found unconditionally is left open. The condition we give is that the Vandermonde matrix of the roots of $p(x)$ be (quasi) orthogonal.

1. Introduction. In this note we are concerned with the following question: given a polynomial $p(x)$ of degree n over $\mathbb{Q}$, i.e., p has rational coefficients, such that p splits in $\mathbb{R}[x]$, i.e., $p(x) = (x-\lambda_1)(x-\lambda_2)\cdots(x-\lambda_n)$, where the λ_i's are all distinct real numbers, is it possible to find a symmetric matrix A_p over $\mathbb{Q}$ such that the eigenvalues of A_p are precisely the roots of $p(x)$, i.e.,

$$A_p \sim D = \mathrm{Diag}(\lambda_1, \lambda_2, \ldots, \lambda_n)? \tag{1.1}$$

("$\sim$" denotes similarity of matrices, and "$\mathrm{Diag}(\lambda_1, \lambda_2, \ldots, \lambda_n)$" denotes a diagonal matrix, with $\lambda_1, \lambda_2, \ldots, \lambda_n$ on the main diagonal.)

The tacit assumption in (1.1) is that A_p is an $n \times n$ matrix, i.e., $A_p \in \mathbb{Q}_{n\times n}$. If this is required, then in general it is not true that such an A_p can be found, as the following example[1] illustrates: there is no rational symmetric 2×2 matrix M with characteristic polynomial $x^2 - 3 = (x+\sqrt{3})(x-\sqrt{3})$.

Suppose by way of contradiction that there is such a rational symmetric 2×2 matrix M, and let

$$M = \begin{bmatrix} a & b \\ b & c \end{bmatrix},$$

so the characteristic polynomial of M, p_M, is given by

$$p_M(x) = x^2 + (-a-c)x + (ac - b^2).$$

Since $-a - c = 0$, it follows that $-a^2 - b^2 = -3$, so $a^2 + b^2 = 3$, which is not possible if a, b are rational numbers. To see this, just clear the denominators, and consider arithmetic modulo 3. We get that for some integers x, y (not both zero), we have $x^2 + y^2 \equiv 0 \pmod 3$; this is not possible.

Of course, our example leaves open the question whether there exists a rational symmetric matrix of dimension greater than 2 which has $\pm\sqrt{3}$ as eigenvectors.

Given a polynomial $p(x) \in \mathbb{Q}[x]$ of degree n, such that $p(x)$ splits over $\mathbb{R}$, i.e., $p(x) = (x-\lambda_1)(x-\lambda_2)\cdots(x-\lambda_n)$, define a *Vandermonde matrix of its roots* to be

*SOLTYS@MCMASTER.CA

[1] This example is due to Stephen Cook; private communication to the author.

the following matrix:

$$V_p = \begin{bmatrix} 1 & \lambda_1 & \lambda_1^2 & \dots & \lambda_1^{n-1} \\ 1 & \lambda_2 & \lambda_2^2 & \dots & \lambda_2^{n-1} \\ & & & \vdots & \\ 1 & \lambda_n & \lambda_n^2 & \dots & \lambda_n^{n-1} \end{bmatrix}. \tag{1.2}$$

We say that V_p is *quasi-orthogonal* if

$$V_p^t V_p = rI \quad \text{where } r \in \mathbb{Q}. \tag{1.3}$$

In this note we show that if $p(x) \in \mathbb{Q}[x]$ of degree n, which splits over $\mathbb{R}$, and its matrix V_p is quasi-orthogonal, then there exists a $2n \times 2n$ symmetric rational matrix whose eigenvalues are precisely $\lambda_1, \lambda_2, \dots, \lambda_n$.

Note that our example polynomial $x^2-3 = (x+\sqrt{3})(x-\sqrt{3})$ does not satisfy (1.3), while the polynomial $x^2 - 1 = (x-1)(x+1)$ does.

We leave open the question whether the condition given by (1.3) is necessary. It is plausible that in general we can unconditionally find a rational symmetric matrix as required, albeit of size greater than the degree of the polynomial. This seems to be an interesting open question.

2. Main Result. We now prove the main result of this note. We start with lemma 2.1, and then we state and prove our result as theorem 2.3.

LEMMA 2.1. *Suppose that $p(x) = x^n + p_{n-1}x^{n-1} + \cdots + p_0 \in \mathbb{Q}[x]$ is a separable polynomial of degree n that splits in $\mathbb{C}[x]$, that is, $p(x) = (x-\lambda_1)(x-\lambda_2)\cdots(x-\lambda_n)$, where the $\lambda_i \in \mathbb{C}$ are all distinct. Then, if V_p is quasi-orthogonal, there exists a* symmetric *matrix $A_p \in \mathbb{Q}_{n\times n}$ (i.e., an $n \times n$ matrix over $\mathbb{Q}$) such that:*

$$A_p \sim D := Diag(\lambda_1^2, \lambda_2^2, \dots, \lambda_n^2),$$

that is, A_p is similar to a diagonal matrix whose eigenvalues are the λ_i^2.

Proof. First of all, since all the λ_i's are distinct, it follows that:

$$C_p = \begin{bmatrix} 0 & 0 & \dots & -p_0 \\ 1 & 0 & \dots & -p_1 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 1 & -p_{n-1} \end{bmatrix} \sim D$$

where C_p is the companion matrix of $p(x)$.

Note that from general considerations about bases of eigenvectors (for distinct eigenvalues) we know that V_p is invertible. However, we can also check it directly, since V_p is the Vandermonde matrix, and therefore its determinant is $\Pi_{i<j}(\lambda_i - \lambda_j)$. Since all the λ_i's are distinct, it follows that $\det(V_p) \neq 0$, and hence V_p is invertible.

CLAIM 2.2. $V_p C_p V_p^{-1} = D$.

Proof. (of claim 2.2)

$$\begin{aligned} V_p C_p V_p^{-1} = D &\iff V_p C_p = D V_p \\ &\iff C_p^t V_p^t = V_p^t D, \end{aligned}$$

and the last statement holds iff $\forall i$, the i-th column of V_p^t is the eigenvector of C_p^t corresponding to λ_i. This in turn is true iff $(\lambda_i I - C_p^t)(V_p^t)_i = 0$, where $(V_p^t)_i$ denotes the i-th column of the matrix V_p^t.

The last statement in the above paragraph holds since

$$(\lambda_i I - C_p^t)(V_p^t)_i = \begin{bmatrix} \lambda_i & -1 & 0 & \dots & 0 \\ 0 & \lambda_i & -1 & \dots & 0 \\ & & & \vdots & -1 \\ p_0 & p_1 & p_2 & \dots & \lambda_i + p_{n-1} \end{bmatrix} \begin{bmatrix} 1 \\ \lambda_i \\ \lambda_i^2 \\ \vdots \\ \lambda_i^{n-1} \end{bmatrix},$$

and the product of the two right-hand side matrices is clearly the zero column-vector. (End of proof of claim 2.2.) □

Now,

$$D^2 = D \cdot D = [(V_p^t)^{-1} C_p^t (V_p^t)][V_p C_p V_p^{-1}] = (V_p^{-1})^t \underbrace{[C_p^t (V_p^t) V_p C_p]}_{(*)} V_p^{-1},$$

and the matrix in the middle, namely $(*)$, is symmetric, and furthermore, it is rational. This is going to be our matrix[2], i.e., our A_p. □

THEOREM 2.3. *Suppose that $p(x) = x^n + p_{n-1}x^{n-1} + \cdots + p_0 \in \mathbb{Q}[x]$ is a separable polynomial that splits in $\mathbb{R}$, that is, $p(x) = (x-\lambda_1)(x-\lambda_2)\cdots(x-\lambda_n) \in \mathbb{R}[x]$, and all the λ_i's are distinct. If V_p is quasi-orthogonal, then there exists a symmetric matrix over $\mathbb{Q}_{2n\times 2n}$ whose eigenvalues are the λ_i's.*

Proof. Let $q(x) = p(x^2)$. Then $q(x) \in \mathbb{Q}[x]$ as well, and

$$\begin{aligned} q(x) &= (x^2 - \lambda_1)(x^2 - \lambda_2)\cdots(x^2 - \lambda_n) \\ &= (x - \sqrt{\lambda_1})(x + \sqrt{\lambda_1})(x - \sqrt{\lambda_2})(x + \sqrt{\lambda_2})\cdots(x - \sqrt{\lambda_n})(x + \sqrt{\lambda_n}). \end{aligned}$$

Note that $\sqrt{\lambda_i}$ may be purely real or purely imaginary, as $\lambda_i \in \mathbb{R}$, so $\sqrt{\lambda_i}^2 \in \mathbb{R}$. Also, there are $2n$ roots of $q(x)$, and they are all distinct:

$$\sqrt{\lambda_1}, -\sqrt{\lambda_1}, \sqrt{\lambda_2}, -\sqrt{\lambda_2}, \dots, \sqrt{\lambda_n}, -\sqrt{\lambda_n}.$$

So we can apply lemma 2.1 to $q(x)$.

Note that C_q, the companion matrix of $q(x)$, is a $2n \times 2n$ matrix, and so is the rational symmetric matrix $A_q = C_q^t V_p^t V_p C_q$, and

$$\begin{aligned} A_q &\sim D(\sqrt{\lambda_1}^2, -\sqrt{\lambda_1}^2, \sqrt{\lambda_2}^2, -\sqrt{\lambda_2}^2, \dots, \sqrt{\lambda_n}^2, -\sqrt{\lambda_n}^2) \\ &= D(\lambda_1, -\lambda_1, \lambda_2, -\lambda_2, \dots, \lambda_n, -\lambda_n), \end{aligned}$$

and this finishes the proof. □

[2]Or, rather, a multiple of our matrix; since $(V_p^{-1})^t (V_p^{-1}) = rI$, we let $A_p = r(C_p^t (V_p^t) V_p C_p)$, which is now similar to D^2 via $\frac{1}{\sqrt{r}}(V_p^{-1})$ and its transpose.

Finally, note that we can relax the condition (1.3) a little bit, and only require that $V_p^t V_p = rI$, and not insist explicitly that $r \in \mathbb{Q}$. This is because $r \in \mathbb{Q}$ *a priori* as we show next:

$$V_p^t V_p = \begin{bmatrix} s_0 & s_1 & \dots & s_{n-1} \\ s_1 & s_2 & \dots & s_n \\ & & \vdots & \\ s_{n-1} & s_n & \dots & s_{2n-2} \end{bmatrix}$$

where $s_i = \lambda_1^i + \lambda_2^i + \cdots + \lambda_{n-1}^i = \mathrm{tr}(C_p^i)$, and $\mathrm{tr}(C_p^i) \in \mathbb{Q}$ (i.e., the trace of a power of a rational matrix is a rational number).

3. Conclusion. Do we need the condition that V_p is quasi-orthogonal? We know for sure that in general our rational symmetric matrix will be larger than the degree of the polynomial, but if a condition is required is there one that is weaker than quasi-orthogonality? It was pointed out[3] that there exists a vast literature by Ed Bender on the conditions for the existence of a symmetric matrix over $\mathbb{Q}$; it would be interesting to find out if those results relate directly to the question posed in this note.

REFERENCES

[1] Michael Artin. *Algebra*. Prentice-Hall, 1991.
[2] David S. Dummit and Richard M. Foote. *Abstract Algebra*. Prentice Hall, 1991.
[3] Paul R. Halmos. *Linear Algebra Problem Book*. The Mathematical Association of America, 1995.
[4] W. Keith Nicholson. *Linear algebra with applications*. PWS Publishing Company, 1995.

[3]Robert Guralnick, editor of ELA, private communication.