MATHEMATICS

A DETERMINANT RELATED TO THE JACOBI SYMBOL

BY

J. H. VAN LINT

(Communicated at the meeting of January 27, 1973)

The determinant treated in this note came up in a recent investigation of computer-blurred pictures by D. SLEPIAN [1]. The problem was to determine when the original picture can be uniquely reconstructed from the blurred picture. In the mathematical model the picture is a $n \times m$ matrix of nonnegative integers. The blurring is a replacement of each entry by a weighted average of the elements in some specified neighborhood of that entry. One of the most simple (but fundamental) cases led to the following determinant.

Definition: $F(n, a)$ is the determinant of the n by n matrix F with entries f_{ij} $(i=1, \ldots, n; j=1, \ldots, n)$ defined as follows:

$$f_{ij}:=\begin{cases} 2 \text{ if } i+j \leqslant a+1 \text{ or } i+j \geqslant 2n-a+1, \\ 0 \text{ if } |j-i| \geqslant a+1, \\ 1 \text{ otherwise.} \end{cases}$$

We make the restriction $a<n$.

To our great surprise this relatively harmless looking determinant turned out to be connected with the Jacobi symbol.

In fact we shall prove

Theorem:

$$F(n, a)=(2a+1)(-1)^{a(n-1)}\left(\frac{n}{2a+1}\right).$$

For a definition of the Jacobi symbol (h/k) we refer to textbooks on elementary number theory, e.g. [2], Chapter 11. Here we make the additional convention

$$\left(\frac{h}{k}\right):=0 \text{ if } (h, k)>1.$$

Proof of Theorem: We define the n vectors $\underline{x}^{(k)}$ $(k=0, 1, \ldots, n-1)$ by

$$\underline{x}^{(k)}:=\left(\cos\frac{\pi k}{2n}, \cos\frac{3\pi k}{2n}, \ldots, \cos\frac{(2n-1)\pi k}{2n}\right).$$

Using the standard elementary trigonometric identities one immediately sees that the $\underline{x}^{(k)}$ are a set of n orthogonal vectors. We claim that the $\underline{x}^{(k)}$ are eigenvectors of the matrix F. For $k=0$ this is obvious since all rowsums of F are $2a+1$. We see that $2a+1$ is an eigenvalue of F. For $k=1, \ldots, n-1$ we use the fact that the cosine is an even function. From this it follows that the inner product of row l of F and the vector $\underline{x}^{(k)}$ is

$$\sum_{j=-a}^{a} \cos \frac{\pi k(2l-1-2j)}{2n} = \frac{\sin \dfrac{\pi k(2a+1)}{2n}}{\sin \dfrac{\pi k}{2n}} \cos \frac{\pi k(2l-1)}{2n}.$$

Therefore

$$\underline{x}^{(k)} F^T = \frac{\sin \dfrac{\pi k(2a+1)}{2n}}{\sin \dfrac{\pi k}{2n}} \underline{x}^{(k)}.$$

and we have thus proved that

$$F(n, a) = (2a+1) \prod_{k=1}^{n-1} \frac{\sin \dfrac{\pi k(2a+1)}{2n}}{\sin \dfrac{\pi k}{2n}}. \tag{1}$$

We divide the integers mod $4n$ which are not divisible by n into the $n-1$ disjoint subsets $C_k := \{k, 2n-k, 2n+k, 4n-k\}$. Notice that for every k and for every $j \in C_k$ the value of $|\sin \pi j/2n|$ depends only on k. If we multiply the integers mod $4n$ by $2a+1$ and if $(2a+1, n)=1$ then this mapping induces a permutation of the sets C_k $(k=1, \ldots, n-1)$. From these two statements it follows that the product on the right hand side of (1) has absolute value 1 if $(2a+1, n)=1$. If $(2a+1, n)>1$ then the product contains a factor equal to 0 in the numerator and $F(n, a)=0$. It remains to determine the sign of the product in the case $(2a+1, n)=1$. To do this we must count the number of integers $k \in [1, n-1]$ for which $(2a+1)k(\text{mod } 4n)$ is in the interval $(2n, 4n)$. Now the number of integers $k \in [1, n-1]$ for which $(2a+1)k$ is in the interval $((2\varrho-1)2n, (2\varrho)2n)$ is

$$\min\left(n-1, \left[2\varrho \frac{2n}{2a+1}\right]\right) - \left[(2\varrho-1)\frac{2n}{2a+1}\right]$$

for $2\varrho-1 \leqslant a$.

Therefore the number of integers we are counting is

$$\sum_{i=1}^{a} (-1)^i \left[i \frac{2n}{2a+1}\right] + m(a),$$

where $m(a)=0$ if a is even and $m(a)=n-1$ if a is odd. Hence the product on the right hand side of (1) is equal to

$$(-1)^{a(n-1)+\sum_{i=1}^{a}\left[i\frac{2n}{2a+1}\right]}.$$

The theorem now follows from the well known identity

$$\left(\frac{2n}{2a+1}\right)=(-1)^{\sum_{i=1}^{a}\left[i\frac{2n}{2a+1}\right]},$$

(cf. [2], p. 90 Theorem 37).

Remark: The reader may be interested in finding a more elementary proof of this theorem. Let

$$G(n,a):=\frac{(-1)^{a(n-1)}F(n,a)}{(2a+1)}.$$

By elementary row and column operations it is possible to show that $G(n, a)$ is periodic in n with period $2a+1$. Then, for a suitable subset of values of n, elementary row and column operations, if suitably chosen, lead to the relation

$$G(n,a)=G(n-2a-1,\ -\tfrac{1}{2}+|2n-5a-2\tfrac{1}{2}|).$$

Using the quadratic reciprocity law (cf. [2], Chapter 10) one can show that the Jacobi symbol satisfies the same relation and then the result easily follows. Although this is the approach one is most likely to take at first (and in fact this is how we arrived at the theorem), the details are tedious and the proof is less elegant than the one presented here.

Remark: Work on this problem was done when the author was a visiting research worker at Bell Laboratories, Murray Hill, N.J. Although the theorem of this note is not significant in any way, it is interesting that such amusing mathematical problems came up in the study of blurring pictures and the retrieval of information.

Technological University
Dept. of Mathematics
Eindhoven, The Netherlands

REFERENCES

1. Slepian, D., On Computer-Blurred Pictures, Bell Laboratories memorandum (unpublished).
2. Rademacher, H., Lectures on Elementary Number Theory, Blaisdell Publishing Company, New York (1964).