A degree theorem and decision methods for algebras of affine forms

by H. van Maaren*

Department of Applied Mathematics, Twente University of Technology, P.O. Box 217, 7500 AE Enschede, the Netherlands

Communicated by Prof. T.A. Springer at the meeting of September 27, 1980

1. INTRODUCTION

This paper continues investigations started in [2] where we were concerned with three major problems in the study of algebras of linear forms:

(A) Which algebras of R-linear forms are finitely generated?
(B) Which algebras are generated by forms with a restricted number of variables?
(C) Can one provide a decision method for the algebra generated by a given set of R-linear forms?

In the above, it is understood that R is a commutative ring with 1. An *R-linear form* is an expression $\sum_{i=0}^{n} \lambda_i x_i$, where $n \geq 0$, $\lambda_i \in R$. An *algebra* $\mathscr{A}$ of R-linear forms is a set of such forms closed under substitutions: if $f(x_0, \ldots, x_k) = \sum_i \mu_i x_i$ and $g_i(x_0, \ldots, x_n) = \sum_j \lambda_j^i x_j$ are forms in $\mathscr{A}$ then $h(x_0, \ldots, x_n) = f(g_0(x_0, \ldots, x_n), \ldots, g_k(x_0, \ldots, x_n)) = \sum_j (\sum_i u_i \lambda_j^i) x_j$ is a form in $\mathscr{A}$. A form $\sum \lambda_i x_i$ is *affine* whenever $\sum \lambda_i = 1$.

1.1. In [2] we discussed the relationships between algebras of linear forms and algebras of affine forms. In [3] we were concerned with applications of the results in [2] with respect to the various theories of (general) *convexity*.

* This paper contains the results of the investigations of the author during his stay at the Mathematics Dept. of the University of Utrecht, the Netherlands.

The first goal of this paper is to solve the problems A^*, B^* and C^* for a certain class of rings, denoted by $\mathscr{K}$. (Here, problems A^*, B^* and C^* are just the problems A, B and C with *"linear"* replaced by *"affine"*.)

1.2. Class $\mathscr{K}$ includes (see 2.2)

(a) *all rings of finite characteristic*

(b) *the ring of integers*

Also problems A^*, B^* and C^* are solved if

(c) *R has characteristic 0 and the algebra contains a form $\sum \lambda_i x_i$ where some λ_i is a negative rational number*

The solution consists of a detailed description of the algebras involved and uses two ideals which can be associated to the algebra (see 2.8).

A remarkable consequence of the results is that, for class $\mathscr{K}$, all algebras are generated by their forms of *three* variables $\lambda_1 x_1 + \lambda_2 x_2 + \lambda_3 x_3$ ($\sum \lambda_i = 1$).

In case $R = \mathbb{Z}$ it can even be shown that any algebra of affine forms is generated by *one* form.

The results can be found in section 2. This section also includes a representation theorem for algebras of R-affine forms ($R \in \mathscr{K}$), due to *A. Szendrei*. This theorem, together with the results previously mentioned provides completely satisfactory answers to questions A^*, B^* and C^*, restricted to class $\mathscr{K}$.

1.3. The second goal of the underlying paper is to give a decision method for algebras of affine forms in cases where the above solutions do not apply.

In section 3 we present a decision procedure for the algebra $\mathscr{A}(X)$ generated by the *convex weight function* $Xx_0 + (1-X)x_1$. Since any algebra $\mathscr{A}$ containing a form $\lambda x_0 + (1-\lambda)x_1$ includes the algebra $\mathscr{A}(\lambda)$ (a homomorphic copy of $\mathscr{A}(X)$) such a procedure is quite welcome. Although the procedure is algebraically of nature (it consists of an investigation of the roots of the coefficients $p_i(X) \in \mathbb{Z}[X]$ of the form $p_0(X)x_0 + \ldots + p_n(X)x_n$, using *Sturm's* theorem) it could only be shown sofar using *analytic* methods.

Thanks is due to *prof. dr. J.J. Duistermaat* who suggested me simplifications of earlier versions of lemma 3.7 and theorem 3.12.

2. SIMPLICES SERIES ON IDEMPOTENT INTERVALS

2.1. The study of algebras of affine forms is concerned with the coefficients λ_i of the form $\sum \lambda_i x_i$ rather than with the form itself. For an algebra $\mathscr{A}$ the *associated simplices series* $\Delta^0, \Delta^1, \Delta^2, \ldots$ is defined by:

$$(\lambda_0, \ldots, \lambda_n) \in \Delta^n \text{ iff } \lambda_0 x_0 + \ldots + \lambda_n x_n \in \mathscr{A}.$$

In section 2 of [2] we started investigations on simplices series. The *1-simplex* Δ^1 of a simplices series consists of tuples $(\lambda, 1-\lambda)$, where $\lambda \in \omega_\Delta \subset R$. The set ω_Δ is called the *associated interval* of $\Delta^0, \Delta^1, \Delta^2, \ldots$. As is shown in [2], the set $I(\omega_\Delta) = \omega_\Delta \cap -\omega_\Delta$ is an ideal of $\mathbb{Z}(\omega_\Delta)$, the subring of R generated by ω_Δ.

Now, the main theorem on intervals, the proof of which can be found in 4.6 of [2] states that

2.2. *for any interval ω in any ring R we have*

$$\lambda(1-\lambda)(\sum\omega\cap-\sum\omega)\subset I(\omega), \text{ for any } \lambda\in\omega.$$

Here, $\sum\omega=\{\lambda_0+\ldots+\lambda_n \mid n\geq 0,\ \lambda_i\in\omega\}$.

As one notices, if $1\in\sum\omega\cap-\sum\omega$, the interval involved consists of *idempotents* modulo the corresponding ideal. Intervals satisfying

$$\lambda\in\omega\rightarrow\lambda^2\equiv\lambda \bmod I(\omega)$$

shall be called *idempotent intervals.*

Now class $\mathscr{K}$ (see 1.2) consists of those rings in which any interval is an idempotent interval. *A. Szendrei* has shown in [5] that $\mathscr{K}$ is *not* an *elementary class*, but a so called *local variety*.

Using 2.2 it is easily verified that $\mathscr{K}$ includes $\mathbb{Z}$ and the rings of finite characteristic (since $1\in\omega$, for any interval ω, and $\lambda\in\omega\rightarrow 1-\lambda\in\omega$ for any $\lambda\in\omega$).

It turns out that simplices series with idempotent associated interval are satisfactory describable, as will be shown in the next theorem. In the sequal, we frequently use techniques developed in [2].

2.3. For an (affine) simplices series $\Delta^0,\Delta^1,\Delta^2,\ldots$ the set

$$I_\Delta=\{\mu\in R \mid (1,\mu,-\mu)\in\Delta^2\}$$

is easily shown to constitute an ideal of $\mathbb{Z}(\omega_\Delta)$. It will be called the *associated ideal.*

2.4. LEMMA: Let $\Delta^0,\Delta^1,\Delta^2,\ldots$ be an (affine) simplices series, ω_Δ the associated interval and $I(\omega_\Delta)$ the corresponding ideal. Then

$$2I(\omega_\Delta)\subset I_\Delta\subset I(\omega_\Delta).$$

Moreover

$$\lambda\in I(\omega_\Delta)\cap 2\mathbb{Z}(\omega_\Delta) \text{ implies } \lambda\in I_\Delta.$$

PROOF: Let $\lambda\in I(\omega_\Delta)$. It follows that

$$\lambda(\lambda,1-\lambda,0,0)+(1-\lambda)(0,0,-\lambda,1+\lambda)\in\Delta^3.$$

Thus

$$(\lambda^2,\lambda-\lambda^2,-\lambda+\lambda^2,1-\lambda^2)\in\Delta^3,$$

yielding

$$(\lambda^2+1-\lambda^2,\lambda-\lambda^2,-\lambda+\lambda^2)\in\Delta^2,$$

so $\lambda-\lambda^2\in I_\Delta$.

For the same reasons $(-\lambda)-(-\lambda)^2 \in I_\Delta$, thus $\lambda-\lambda^2-(-\lambda-(-\lambda)^2)=2\lambda \in I_\Delta$.

Moreover, $\lambda \in I_\Delta$ yields $\lambda, -\lambda \in \omega_\Delta$, hence $\lambda \in I(\omega_\Delta)$. Now, if $\lambda \in I(\omega_\Delta)$ and $\lambda = 2r$, for $r \in \mathbb{Z}(\omega_\Delta)$, it follows that $2\lambda r \in I_\Delta$, hence $\lambda^2 \in I_\Delta$, and thus $\lambda = \lambda^2 + +\lambda - \lambda^2 \in I_\Delta$.

2.5. LEMMA: Let $\Delta^0, \Delta^1, \Delta^2, \ldots$ be an (affine) simplices series with idempotent associated interval ω_Δ. Then

(i) $\lambda \in \omega_\Delta$ implies $\lambda(1-\lambda) \in I_\Delta$,

(ii) $(\lambda_0, \ldots, \lambda_n) \in \Delta^n$ implies $\lambda_i \lambda_j \in I_\Delta$ for all $i \neq j$.

PROOF: (i) If $\lambda \in \omega_\Delta$, both $(0, -\lambda(1-\lambda), 1+\lambda(1-\lambda))$ and $(\lambda^2, 0, 1-\lambda^2)$ are elements of Δ^2. Hence $\lambda(0, -\lambda(1-\lambda), 1+\lambda(1-\lambda)) + (1-\lambda)(\lambda^2, 0, 1-\lambda^2) \in \Delta^2$. Thus $\lambda^2(1-\lambda) \in I_\Delta$ and for the same reasons $\lambda(1-\lambda)^2 \in I_\Delta$. We obtain $\lambda - \lambda^2 = = \lambda^2(1-\lambda) + \lambda(1-\lambda)^2 \in I_\Delta$.

(ii) Suppose $(\lambda_0, \ldots, \lambda_n) \in \Delta^n$. Then $(\lambda_i, \lambda_j, 1-(\lambda_i+\lambda_j)) \in \Delta^2$ for all $i \neq j$, and consequently

$$\lambda_i(\lambda_i, \lambda_j, 1-(\lambda_i+\lambda_j)) + (1-\lambda_i)(1,0,0) \in \Delta^2.$$

Thus $(1+\lambda_i^2-\lambda_i, \lambda_i\lambda_j, -\lambda_i\lambda_j-(\lambda_i^2-\lambda_i)) \in \Delta^2$ and since $\lambda_i^2 - \lambda_i \in I_\Delta$ it follows that $(1, \lambda_i\lambda_j, -\lambda_i\lambda_j) \in \Delta^2$.

2.6. Using the above lemma we see that Δ^n consists of vectors, the coordinates of which form a system of *orthogonal idempotents* modulo the ideal I_Δ.

In the following lemma we show that any such system forms a tuple belonging to the series involved.

2.7. LEMMA: If $\Delta^0, \Delta^1, \Delta^2, \ldots$ is an (affine) simplices series and ω_Δ is idempotent, the following statements hold:

(i) If $\lambda_0, \ldots, \lambda_n \in \omega_\Delta$ and $\lambda_i\lambda_j \in I(\omega_\Delta)$, for $i \neq j$, then $\sum \lambda_i \in \omega_\Delta$.

(ii) If $\lambda_0, \ldots, \lambda_n \in \omega_\Delta$ and $\sum \lambda_i = 1$, $\lambda_i\lambda_j \in I_\Delta$, for $i \neq j$, then $(\lambda_0, \ldots, \lambda_n) \in \Delta^n$.

PROOF: (i) For $n=1$, notice that $\lambda_0+\lambda_1 = \lambda_0 \cdot 1 + (1-\lambda_0)\lambda_1 + \lambda_0\lambda_1$. Thus $\lambda_0+\lambda_1 \in \omega_\Delta + I(\omega_\Delta) \subset \omega_\Delta$.

Now assume $\lambda_0, \ldots, \lambda_n$ are as in the premise of (i). Then $\lambda_0, \ldots, \lambda_{n-1}$ are such, as are $(\lambda_0 + \ldots + \lambda_{n-1}), \lambda_n$. Now apply case $n=1$.

(ii) Again, we proceed by induction.

For $n=1$, it is evidently true.

Suppose $\lambda_0, \ldots, \lambda_{n+1}$ are as in the premisse of (ii). Then $\lambda_0, \ldots, \lambda_{n-1}$ are orthogonal modulo I_Δ and thus also orthogonal modulo $I(\omega_\Delta)$.

According to (i) $\sum_{i=0}^{n-1} \lambda_i \in \omega_\Delta$. Hence $\{\lambda_0, \ldots, \lambda_{n-1}, 1 - \sum_{i=0}^{n-1} \lambda_i\}$ is a system of orthogonal (modulo I_Δ) elements in ω_Δ summing up to 1.

By induction hypothesis it follows that

$$(\lambda_0, \ldots, \lambda_{n-1}, 1 - \textstyle\sum_{i=0}^{n-1} \lambda_i) \in \Delta^n.$$

To finish the proof, note that

$$\lambda_n(\lambda_0, \ldots, \lambda_{n-1}, 1 - \sum_{i=0}^{n-1} \lambda_i, 0) + (1 - \lambda_n)(\lambda_0, \ldots, \lambda_{n-1}, 0, 1 - \sum_{i=0}^{n-1} \lambda_i) =$$

$$= (\lambda_0, \ldots, \lambda_{n-1}, \lambda_n - \sum_{i=1}^{n-1} \lambda_i\lambda_n, 1 - \sum_{i=0}^{n-1} \lambda_i - \lambda_n + \sum_{i=0}^{n-1} \lambda_i\lambda_n) \in \Delta^{n+1}$$

and that

$$\sum_{i=0}^{n-1} \lambda_i\lambda_n \in I_\Delta.$$

2.8. THEOREM: Let $\Delta^0, \Delta^1, \Delta^2, \ldots$ be an (affine) simplices series with idempotent associated interval. Then we have

$$\Delta^n = \{\lambda \in R^{n+1} \mid \sum \lambda_i = 1,\ \lambda_i \in \omega_\Delta,\ \lambda_i\lambda_j \in I_\Delta\ (i \neq j)\}.$$

The proof consists of the combination of the preceding lemmas.

2.9. REMARK: Notice that for an interval $\omega \subset R$ and an ideal I satisfying $2I(\omega) \subset I \subset I(\omega)$ the sequence $\Delta^0, \Delta^1, \Delta^2, \ldots$ defined by

$$\Delta^n = \{\lambda \in \mathbb{Z}(\omega)^{n+1} \mid \sum \lambda_i = 1,\ \lambda_i \in \omega,\ \lambda_i\lambda_j \in I\}$$

constitutes a simplices series. However, it need *not* be a series with associated interval ω: the condition

$$\lambda \in \omega \to \lambda(1 - \lambda) \in 2I(\omega)$$

is not always satisfied.

Therefore, in general, a $1-1$ *correspondence* between ideals I with $2I(\omega) \subset I \subset I(\omega)$ and simplices series with associated interval ω is *not* available.

We close this section with mentioning a very useful representation theorem for affine simplices series over rings in $\mathscr{K}$.

2.10. THEOREM: (*A. Szendrei*): If $\Delta^0, \Delta^1, \Delta^2, \ldots$ is an (affine) simplices series over a ring $R \in \mathscr{K}$ there exists a class $\mathscr{I}$ of mutually prime ideals in the ring $\mathbb{Z}(\omega_\Delta)$ such that

$$\Delta^n = \bigcap_{I \in \mathscr{I}} \Delta_I^n, \text{ for each } n \geq 0,$$

where Δ_I^n is the n-simplex $\{\lambda \in \mathbb{Z}(\omega_\Delta) \mid \sum \lambda_i = 1, \text{ all but one } \lambda_i \in I\}$.

PROOF: See [4].

2.11. Let us emphasize again that theorems 2.8 and 2.10 provide the answers to questions A^*, B^* and C^* of the introduction. Especially in cases where R is a principal ring and the number of idempotents mod $I(\omega_\Delta)$, as well as the number of ideals I satisfying $2I(\omega_\Delta) \subset I \subset I(\omega_\Delta)$, is finite, the description of the series involved (and hence of the algebras) is quite elegant (see also [1]).

Another feature concerning affine simplices series is useful also: *any finitely generated series is single-generated.*

This can be seen using the fact that the series generated by $(\lambda_0, \ldots, \lambda_n)$ and $(\mu_0, \ldots, \mu_m)$ coincides with the series generated by

$$(\mu_0\lambda_0, \ldots, \mu_0\lambda_n, \mu_1\lambda_0, \ldots, \mu_1\lambda_n, \ldots, \mu_m\lambda_0, \ldots, \mu_m\lambda_n)$$

(by *compression*, see 2.2 of [2]).

3. A DECISION METHOD FOR $\mathscr{A}(X)$

3.1. *The algebra* $\mathscr{A}(X)$ generated by the convex weight function $Xx_0 + (1-X)x_1$ consists of forms

$$p_0(X)x_0 + \ldots + p_n(X)x_n;\ p_i(X) \in \mathbb{Z}[X];\ \textstyle\sum_{i=0}^{n} p_i(X) = 1(X).$$

To provide a decision method for $\mathscr{A}(X)$ means (in terms of simplices series) to be able to decide whether a given $n+1$-tuple $(p_0(X), \ldots, p_n(X))$ is an element of the n-simplex of the series generated by $(X, 1-X)$.

First we investigate case $n=1$. A tuple $(p(X), 1-p(X))$ is an element of the 1-simplex of the series generated by $(X, 1-X)$ if $p(X)$ is an element of the interval generated by X in $\mathbb{Z}[X]$. This interval will be denoted by $\omega(X)$.

3.2. In section 4 of [2] it is shown that $\omega(X)$ consists of the polynomials

$$\textstyle\sum_{j=0}^{N} A_j X^{N-j}(1-X)^j,\ A_j \in \mathbb{Z},\ 0 \le A_j \le \binom{N}{j},\ N \ge 0.$$

3.3. However, expressions as 3.2 may yield polynomials of degree *less* than N. Hence, although being a *combinatorial description* of $\omega(X)$, 3.2 does not provide a *decision procedure*. We shall eliminate this problem, using analytic properties of the ring of polynomials with real coefficients.

3.4. LEMMA: Let $p(X) = \sum_{i=0}^{m} a_i X^i;\ a_i \in \mathbb{Z}$. Then $p(X) \in \omega(X)$ iff there exists a natural number N such that for any j $(0 \le j \le N)$:

$$0 \le \textstyle\sum_{i=0}^{m} a_i \binom{N-i}{j} \Big/ \binom{N}{j} \le 1.$$

PROOF: For fixed $N \ge m$, a polynomial $p(X) = \sum_{i=0}^{m} a_i X^i$ can be written (uniquely) as $\sum_{j=0}^{N} A_j^{(p)} X^{N-j}(1-X)^j$.

It is left to the reader to verify that in this case

$$(\star) \qquad A_j^{(p)} = \textstyle\sum_{i=0}^{m} a_i \binom{N-i}{j}.$$

Now, the proof of the lemma follows by applying 3.2.

3.5. Let $R(X)$ be the set of polynomials $p(X)$ satisfying

$$(\star) \qquad \begin{cases} p(X) \in \mathbb{Z}[X];\ \{p(0), p(1)\} \subset \{0,1\}, \textit{ and for all} \\ r \in \mathbb{R}\colon\ 0 < r < 1 \textit{ implies } 0 < p(r) < 1. \end{cases}$$

It is easily checked that $R(X) \cup \{0(X), 1(X)\}$ is an interval in $\mathbb{Z}[X]$ which includes X, and hence includes $\omega(X)$. It is our aim to show equality.

3.6. First, we observe that for large N

$$(\star) \qquad \binom{N-j}{j} \Big/ \binom{N}{j} = \left(\frac{N-j}{N}\right) \frac{\left(\frac{N-j}{N} - \frac{1}{N}\right) \cdots \left(\frac{N-j}{N} - \frac{i-1}{N}\right)}{\left(1 - \frac{1}{N}\right) \cdots \left(1 - \frac{i-1}{N}\right)}$$

"behaves" like $(N-j/N)^i$, and hence the conditions

$$0 \leq \sum_{i=0}^{m} a_i \binom{N-i}{j} \Big/ \binom{N}{j} \leq 1$$

from lemma 3.4 may be read as $0 \leq p(1-(j/N)) \leq 1$, which is a strong indication towards our claim $\omega(X) = R(X)$, since N may be chosen arbitrarily large.

To eliminate difficulties appearing at the boundary points 0 and 1 we need to go into detail.

3.7. LEMMA: Let $p(X) = \sum_{i=0}^{m} a_i X^i$;

$$p_N(X) = \sum_{i=0}^{m} a_i \frac{X\left(X - \frac{1}{N}\right) \cdots \left(X - \frac{i-1}{N}\right)}{\left(1 - \frac{1}{N}\right) \cdots \left(1 - \frac{i-1}{N}\right)}.$$

If $p^{(1)}(0) = p^{(2)}(0) = \ldots = p^{(s)}(0)$ and $p^{(1)}(1) = \ldots = p^{(r)}(1) = 0$ we have

$$p_N\left(\frac{1}{N}\right) = \ldots = p_N\left(\frac{s}{N}\right) = p_N(0)$$

and

$$p_N\left(1 - \frac{1}{N}\right) = \ldots = p_N\left(1 - \frac{r}{N}\right) = p_N(1).$$

(Here, $p^{(k)}(a) = ((d^k/dX^k)\, p(X))_{X=a}$).

PROOF: If $p^{(i)}(0) = i! a_i = 0$ for $i = 1, \ldots, s$ it follows that

$$p_N(X) = a_0 + \sum_{i=s+1}^{N} a_i \frac{X\left(X - \frac{1}{N}\right) \cdots \left(X - \frac{i-1}{N}\right)}{\left(1 - \frac{1}{N}\right) \cdots \left(1 - \frac{i-1}{N}\right)}.$$

Hence

$$X\left(X - \frac{1}{N}\right) \cdots \left(X - \frac{s}{N}\right)$$

is a factor of $p_N(X)-a_0$, thus

$$p_N\left(\frac{1}{N}\right)=\ldots=p_N\left(\frac{s}{N}\right)=p_N(0)=a_0.$$

Now, the mapping I_N: $p\to p_N$ assigns to p the unique polynomial p_N of degree $\leq m$ with the property

$$(1)\qquad p_N\left(\frac{j}{N}\right)=A_{N-j}^{(p)}/\binom{N}{j}\qquad (j=0,\ldots,N)$$

(see 3.4 (★) and 3.6 (★)).

For a polynomial $p(X)$, let $\tilde{p}(X)=p(1-X)$. Using (1), we see that I_N and $\sim$ commute (because $A_j^{(\tilde{p})}=A_{N-j}^{p}$).

Now, if $p^{(1)}(1)=\ldots=p^{(r)}(1)=0$ it follows that $\tilde{p}^{(1)}(0)=\ldots=\tilde{p}^{(r)}(0)=0$ and hence, by the first part of the proof

$$I_N(\tilde{p})\left(\frac{1}{N}\right)=\ldots=I_N(\tilde{p})\left(\frac{r}{N}\right)=\tilde{p}_N(0).$$

Since I_N and $\sim$ commute we obtain finally

$$p_N\left(1-\frac{1}{N}\right)=\ldots=p_N\left(1-\frac{r}{N}\right)=p_N(1).$$

3.8. LEMMA: If $p(X)=\sum a_iX^i\in R(X)$ then there exists N such that $p_N(X)$ (as defined in 3.7) satisfies:

$$0\leq p_N\left(\frac{k}{N}\right)\leq 1 \text{ for all } 0\leq k\leq N.$$

PROOF: Suppose $p(X)\in R(X)$ and assume that $p^{(1)}(X)$ has an s-fold zero in 0 and an r-fold zero in 1 (r and s may happen to be 0). Let $\varepsilon>0$ be such that it *separates* the distinct zeros of $p^{(1)}(X)$ and 0 and 1 (i.e. if $\alpha_1,\ldots,\alpha_k$ are all distinct (complex) zeros $\neq 0,1$ of $p^{(1)}(X)$ then $\{z\mid |z-\alpha_i|<\varepsilon\}$, $\{z\mid |z|<\varepsilon\}$ and $\{z\mid |z-1|<\varepsilon\}$ are disjoint sets). Since $p_N(X)$ converges to $p(X)$, $p_N^{(1)}(X)$ converges to $p^{(1)}(X)$ and zeros of $p_N^{(1)}(X)$ converge to zeros of $p^{(1)}(X)$.

Hence an N_1 may be chosen such that for all $N\geq N_1$ there are *at most* s zeros of $p_N^{(1)}(X)$ in $[-\varepsilon,\varepsilon]$ and *at most* r of them in $[1-\varepsilon,1+\varepsilon]$.

Moreover, N_1 can be taken such that $s/N_1<\varepsilon$ and $r/N_1<\varepsilon$. Again, since $p_N(X)$ converges to $p(X)$, and since $0<p(\alpha)<1$ for $\alpha\in[\varepsilon,1-\varepsilon]$, there exists N_2 such that, for $N\geq N_2$ and all $\alpha\in[\varepsilon,1-\varepsilon]$: $0<p_N(\alpha)<1$.

Now, let $N\geq N_1$ and $N\geq N_2$. Lemma 3.7 shows that

$$p_N\left(\frac{1}{N}\right)=\ldots=p_N\left(\frac{s}{N}\right)=p_N(0)$$

and

$$p_N\left(1-\frac{1}{N}\right)=\ldots=p_N\left(1-\frac{r}{N}\right)=p_N(1)$$

and hence $p_N^{(1)}(X)$ has s zeros in $[0,s/N]$ and r zeros in $[1-(r/N),1]$.

Since at most s zeros appear in $[-\varepsilon, \varepsilon]$ it follows that $p_N^{(1)}(X)$ has no zeros in $[s/N, \varepsilon]$. By similar reasoning, no zeros of $p_N^{(1)}(X)$ appear in $(1-\varepsilon, 1-(r/N))$. We conclude that $p_N(X)$ is *monotonic* on $[s/N, \varepsilon]$ and on $[1-\varepsilon, 1-(r/N)]$. Consequently, since

$$p_N\left(\frac{s}{N}\right) = p(0) \in \{0, 1\}$$

and

$$p_N\left(1 - \frac{r}{N}\right) = p(1) \in \{0, 1\}$$

it shows that $0 \leq p_N(\alpha) \leq 1$ for all $s/N \leq \alpha \leq 1-(r/N)$. Moreover,

$$p_N(0) = p_N\left(\frac{1}{N}\right) = \ldots = p_N\left(\frac{s}{N}\right)$$

and

$$p_N(1) = p_N\left(1 - \frac{1}{N}\right) = \ldots = p_N\left(1 - \frac{r}{N}\right)$$

and the statement of the lemma follows.

3.9. Now, the combination of the lemmas 3.4, 3.7 and 3.8 shows equality of $\omega(X)$ and $R(X)$, as may easily be verified. The use of analytic methods in the proof of 3.8 might be hard to avoid. To advocate this opinion consider the polynomial $(2X^2-1)^2$.

This polynomial maps the rational inner points of $[0, 1]$ on such points. However, it has a root $\sqrt{\frac{1}{2}}$ and therefore is not a member of $\omega(X)$.

3.10. Note that the equality $\omega(X) = R(X)$ provides a decision method for $\omega(X)$, since by *Sturm's theorem* the number of roots between 0 and 1 of both $p(X)$ and $1-p(X)$ can *effectively* be calculated.

3.11. Finally, we discuss the algebra $\mathscr{A}(X)$ again. So far, we have shown that $p_0(X)x_0 + \ldots + p_n(X)x_n \in \mathscr{A}(X)$ implies $p_i(X) \in \omega(X) = R(X)$ and $\sum p_i(X) = 1(X)$. In the next theorem we show the sufficiency of this condition.

3.12. THEOREM: The algebra $\mathscr{A}(X)$ generated by the convex weight function $Xx_0 + (1-X)x_1$ consists precisely of the forms $p_0(X)x_0 + \ldots + p_n(X)x_n$ satisfying both

(i) $p_i(X) \in \mathbb{Z}[X]$; $\sum p_i(X) = 1(X)$

(ii) $p_i(X) \in \{0(X), 1(X)\}$ or for all $r \in \mathbb{R}$: $0 < r < 1$ implies $0 < p_i(r) < 1$.

PROOF: The one thing left to prove is that for any $n+1$-tuple $(p_0(X), \ldots, p_n(X))$ with $\sum p_i(X) = 1(X)$ and $p_i(X) \in \omega(X)$ the form $p_0(X)x_0 + \ldots + p_n(X)x_n$ is indeed an element of $\mathscr{A}(X)$. According to theorem 3.1 of [2] it

suffices to show that there exist non-negative integers A_l^i and N with

$$(\star) \qquad p_i(X) = \sum_{l=0}^{N} A_l^i X^l (1-X)^{N-l};\ \sum_{i=0}^{n} A_l^i = \binom{N}{l}.$$

Since $p_i(X) \in \omega(X)$ it follows from 3.2 that

$$p_i(X) = \sum_{l=0}^{N_i} A_l^i X^l (1-X)^{N_i - l}$$

for some N_i and A_l^i with

$$0 \leq A_l^i \leq \binom{N_i}{l}.$$

In fact, the N_i's may be assumed to be equal (see 1.6 page 58 of [1]).

Thus $p_i(X) = \sum_{l=0}^{N} A_l^i X^l (1-X)^{N-l}$ whence

$$\sum_{i=0}^{n} p_i(X) = \sum_{l=0}^{N} \sum_{i=0}^{n} A_l^i X^l (1-X)^{N-l}.$$

Since

$$1(X) = \sum_{l=0}^{N} \binom{N}{l} X^l (1-X)^{N-l}$$

and since (for fixed N) the representation of a polynomial $\sum \alpha_i X^i (1-X)^{N-l}$ in this form is unique we obtain

$$\sum_{i=0}^{n} A_l^i = \binom{N}{l}$$

which finishes the proof.

REFERENCES

1. Maaren, H. van – Algebraic Simplices in Modules. Diss., State Univ. of Utrecht (1979).
2. Maaren, H. van and H.J.P. De Smet – Polynomials in Algebras of Linear Forms. Indag. Math. **43**, 195–205 (1981).
3. Maaren, H. van and H.J.P. De Smet – Extremal Points, Separation and Carathéodory-, Helly- and Radon numbers in non real Linear Spaces. Indag. Math. **43**, 207–218 (1981).
4. Szendrei, A. – On the Idempotent Reducts of Modules I. Bolyai Institute, Szeged.
5. Szendrei, A. – On the Idempotent Reducts of Modules II. Bolyai Institute, Szeged.