C.R. Math. Rep. Acad. Sci. Canada - Vol. V, No. 1, February 1983 Février

---

C.R. Math. Rep. Acad. Sci. Canada - Vol. V, No. 1, February 1983 Février

ON THE WIGNER QUASI-PROBABILITY DISTRIBUTION FUNCTION II

Walter Schempp

Presented by P.C. Greiner, F.R.S.C.

As is well known, to fully understand any mathematical system we must understand the transformations of the system and especially those transformations of the given system that leave some particular aspects of the system invariant. In the preceding papers [2],[3],[4],[5] we have been concerned with the transformation behaviour of the radar autoambiguity function $H(f;.,.)$ with respect to the complex envelope $f \in \mathscr{S}(R^n)$ of L^2-norm $\|f\| = 1$. Moreover, the first part [6] of this series of papers has been concerned with the transformation behaviour of the Wigner quasi-probability distribution function $P(f;.,.)$ with respect to the state f of a non-relativistic quantum mechanical system of n degrees of freedom. In particular, if $\sigma \rightsquigarrow T_\sigma$ denotes the (projective) oscillator representation of the real symplectic group $Sp(n,R)$, we pointed out that the identity

$$H(f;x,y) = H(f';x',y')$$

holds for a function $f' \in \mathscr{S}(R^n)$ of L^2-norm $\|f'\| = 1$ and for all pairs $(x,y) \in R^n \oplus R^n$ and suitable pairs $(x',y') \in R^n \oplus R^n$ if and only if there exists a unique symplectic automorphism $\sigma \in Sp(n,R)$ of the time-frequency space $R^n \oplus R^n$ and a number ζ of the unit circle $U = U(1,C)$ such that

$$\sigma(x',y') = (x,y), \quad \zeta T_\sigma(f) = f'$$

holds. Similarly, we have

$$P(f;x,y) = P(f';x',y')$$

for all $(x,y) \in \mathbf{R}^n \oplus \mathbf{R}^n$ and suitable pairs $(x',y') \in \mathbf{R}^n \oplus \mathbf{R}^n$ if and only if there exists a unique symplectic automorphism $\sigma \in \mathbf{Sp}(n,\mathbf{R})$ of the phase space $\mathbf{R}^n \oplus \mathbf{R}^n$ such that the identities

$$\sigma(x',y') = (x,y), \; \zeta T_{\check{\sigma}}(f) = f'$$

hold where $\check{\sigma} \in \mathbf{Sp}(n,\mathbf{R})$ denotes the contragredient automorphism of σ and $\zeta \in \mathbf{U}$.

It is the purpose of the present paper to deal with the case where both functions $H(f;.,.)$ and $P(f;.,.)$ admit the same transformation behaviour. Thus we are concerned with the condition

$$\sigma = \check{\sigma} ,$$

i.e., with the case that σ belongs to the group

$$\mathbf{SO}(2n,\mathbf{R}) \cap \mathbf{Sp}(n,\mathbf{R}).$$

It should be observed that this group forms a maximal compact subgroup of $\mathbf{Sp}(n,\mathbf{R}) \subset \mathbf{SL}(2n,\mathbf{R})$ that is Lie isomorphic with the unitary group $\mathbf{U}(n,\mathbf{C})$.

Let K denote the maximal torus in $\mathbf{SO}(2n,\mathbf{R}) \cap \mathbf{Sp}(n,\mathbf{R})$ formed by the elements

$$\left[\begin{array}{ccc|ccc}
\cos\theta_1 & & 0 & \sin\theta_1 & & 0 \\
 & \ddots & & & \ddots & \\
0 & & \cos\theta_n & 0 & & \sin\theta_n \\
\hline
-\sin\theta_1 & & 0 & \cos\theta_1 & & 0 \\
 & \ddots & & & \ddots & \\
0 & & -\sin\theta_n & 0 & & \cos\theta_n
\end{array}\right]$$

where $(\theta_1,\ldots,\theta_n) \in \mathbf{R}^n$. In the case $n = 1$ we have $\mathbf{Sp}(1,\mathbf{R}) = \mathbf{SL}(2,\mathbf{R})$ and, of course, $K = \mathbf{SO}(2,\mathbf{R})$.

1. K-Invariant Wigner Quasi-Probability Distribution Functions

Keeping to the notations above, our first result reads as follows:

Theorem 1. *Let* $f \in \mathcal{S}(\mathbf{R}^n)$ *have standardized* L^2*-norm* $\|f\| = 1$ *and let the associated Wigner quasi-probability distribution function satisfy*

$$P(f;x,y) = P(f;-y,x)$$

for all pairs $(x,y) \in \mathbf{R}^n \oplus \mathbf{R}^n$. *Then the identities*

$$P(f;x,y) = P(f;\sigma(x,y))$$

and

$$H(f;x,y) = H(f;\sigma(x,y))$$

hold for all $\sigma \in K$ *and all* $(x,y) \in \mathbf{R}^n \oplus \mathbf{R}^n$. *Moreover, there exists a multi-index* $m = (m_1,\ldots,m_n) \in \mathbf{N}^n$ *and a number* $\zeta \in \mathbf{U}$ *such that*

$$f = \zeta W_m$$

holds where

$$W_m = W_{m_1} \otimes \ldots \otimes W_{m_n}$$

denotes the Hermite-Weber function of degree m *on* $\mathbf{R}^n$.

The proof depends upon the structural properties of $Sp(n,\mathbf{R})$. Obviously it will be enough to consider the case $n = 1$. For the radar autoambiguity function $H(f;.,.)$ in this case, also see Wilcox [8] and the paper [1].

2. The First Step

Let $\Theta \in \mathbf{R}$ be such that $\cos \Theta = 0$ i.e., we consider the element

$$\tau = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

of K. Let $\mathfrak{n}$ denote the three-dimensional real Heisenberg Lie algebra with one-dimensional center $\mathfrak{z}$ and fix a canonical symplectic basis $\{X,Y\}$ of $\mathfrak{n}/\mathfrak{z}$. Choose as the reference polarization

$$\mathfrak{l} = X.\mathbf{R} \oplus \mathfrak{z}$$

in $\mathfrak{n}$. Then we obtain by the formula

$$T_\sigma = \overline{\mathcal{F}}_{\mathfrak{l},\sigma(\mathfrak{l})} \circ \gamma(\sigma)$$

displayed in [4] and [6] for the transformation T_σ associated with σ under the oscillator representation of $Sp(n,\mathbf{R})$:

$$T_\tau = \overline{\mathcal{F}}_{\mathbf{R}}$$

on $\mathcal{S}(\mathbf{R})$. Since the Fourier cotransform $\overline{\mathcal{F}}_{\mathbf{R}}$ admits the Hermite-Weber functions $(W_m)_{m \geq 0}$ as its eigenfunctions with eigenvalues $(i)^m$, the condition $f = \zeta\, W_m$ for certain degrees $m \in \mathbf{N}$ becomes obvious.

3. The Second Step

Suppose that $\cos\theta \neq 0$. Then the elements

$$\sigma = \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix}$$

of K admit the factorization

$$\begin{bmatrix} 1 & 0 \\ -\tan\theta & 1 \end{bmatrix} \begin{bmatrix} \cos\theta & 0 \\ 0 & \cos^{-1}\theta \end{bmatrix} \begin{bmatrix} 1 & \tan\theta \\ 0 & 1 \end{bmatrix}$$

within the group $Sp(1,\mathbf{R}) = SL(2,\mathbf{R})$. In the case

$$\sigma'_\theta = \begin{bmatrix} 1 & \tan\theta \\ 0 & 1 \end{bmatrix}$$

we obtain by the same formula as used in Section 2

$$T_{\sigma'_\theta} F : t \rightsquigarrow e^{\pi i (\tan\theta) t^2} F(t)$$

for any function $F \in \mathcal{S}(\mathbf{R})$. Similarly, in case of the transformation

$$\sigma_\theta = \begin{bmatrix} \cos\theta & 0 \\ 0 & \cos^{-1}\theta \end{bmatrix}$$

a short computation shows

$$T_{\sigma_\Theta}F: t \rightsquigarrow (\sqrt{|\cos\Theta|})^{-1} F((\cos\Theta)^{-1}t).$$

Finally, in the case

$$\sigma''_\Theta = \begin{bmatrix} 1 & 0 \\ -\tan\Theta & 1 \end{bmatrix}$$

we obtain analogously

$$\bar{\mathscr{F}}_R(T_{\sigma''_\Theta}F): t \rightsquigarrow \zeta_\Theta\, e^{\pi i(\tan\Theta)t^2}\, \bar{\mathscr{F}}_R F(t)$$

where the number $\zeta_\Theta \in U$ can be expressed explicitly in terms of the Maslov index. From this formula, the transformation $T_{\sigma''_\Theta}$ can easily be recovered.

In view of these facts and the well-known transformation rules of the Hermite-Weber functions the following result can be established. It completes the proof of Theorem 1 supra.

Theorem 2. *There exists for all $\Theta \in \mathbf{R}$ and all $m \in \mathbf{N}$ a number $\zeta_{\Theta,m} \in U$ such that the identity*

$$T_{\sigma''_\Theta} \circ T_{\sigma_\Theta} \circ T_{\sigma'_\Theta}(W_m) = \zeta_{\Theta,m} W_m$$

holds.

The number $\zeta_{\Theta,m}$ can be computed explicitly. Theorem 2 generalizes a result of Wallach [7].

4. Positivity of P(f;.,.)

Theorem 1 supra implies immediately (cf. |6|)

Theorem 3. *Suppose $f \in \mathscr{S}(\mathbf{R}^n)$ with $\|f\| = 1$ and*

$$P(f;x,y) = P(f;-y,x) \geq 0$$

for all $(x,y) \in \mathbf{R}^n \oplus \mathbf{R}^n$. Then we have

$$f = \zeta W_{(0,\ldots,0)},$$

i.e., *the function f is up to a factor* $\zeta \in U$ *the n-variate Gaussian density*.

References

1. Hebsaker, H.M., Schempp, W.: Radar detection, quantum mechanics, and nilpotent harmonic analysis. Meth. Verf. der math. Physik (to appear)
2. Schempp, W.: Radar reception and nilpotent harmonic analysis I. C.R. Math. Rep. Acad. Sci. Canada **4**, 43-48 (1982)
3. Schempp, W.: Radar reception and nilpotent harmonic analysis II. C.R. Math. Rep. Acad. Sci. Canada **4**, 139-144 (1982)
4. Schempp, W.: Radar reception and nilpotent harmonic analysis III. C.R. Math. Rep. Acad. Sci. Canada **4**, 219-224 (1982)
5. Schempp, W.: Radar reception and nilpotent harmonic analysis IV. C.R. Math. Rep. Acad. Sci. Canada **4** (1982)
6. Schempp, W.: On the Wigner quasi-probability distribution function I. C.R. Math. Rep. Acad. Sci. Canada **4** (1982)
7. Wallach, N.: Symplectic geometry and Fourier analysis. Brookline, MA: Math Sci Press 1977
8. Wilcox, C.H.: The synthesis problem for radar ambiguity functions. The University of Wisconsin, Mathematics Research Center. Madison, WI. Tech. Summary Report **157** (1960)

Lehrstuhl fuer Mathematik I
Universitaet Siegen
Hoelderlinstrasse 3
D-5900 Siegen, W. Germany

Received September 20, 1982

C.R. Math. Rep. Acad. Sci. Canada - Vol. V, No.1, February 1983 Février

A NOTE ON EFFICIENT GENERATION OF IDEALS

Budh S. Nashier

Presented by P. Ribemboim, F.R.S.C.

We are dealing with rings which are commutative Noetherian with identity. We also assume that the rings under consideration have finite Krull dimension. If M is a finitely generated module over a ring R, we let $\mu(M)$ denote the least number of elements in M that can generate M as an R-module. For an ideal I in a ring R, it is a well-known fact that $\mu(I/I^2) \leq \mu(I) \leq \mu(I/I^2)+1$. In [4] we studied a few classes of regular polynomial rings in which for certain ideals the lower bound in the above inequality is attained. One of the theorems we had proved therein says the following:

THEOREM 1. ([4], Theorem 2.9). Let A be a d-dimensional regular local algebra with a separating ground field. Assume that the residue field of A is infinite. Let $R = A[T_1,\dots,T_n]$ be a polynomial ring. Then

(1) If I is an ideal in R such that $\mathrm{ht}(I) > \min\{d,n+2\}$ and $\mu(I/I^2) \geq \dim(I)+2$, then $\mu(I) = \mu(I/I^2)$.

(2) If I is a prime ideal in R such that $\mathrm{ht}(I) > \min\{d,n+1\}$ and $\mu(I/I^2) \geq \dim(I)+2$, then $\mu(I) = \mu(I/I^2)$.

We recall that if A is a local ring then we say that A is a local algebra with a ground field if A is a localization of an affine k-algebra for some field k. In this context k will be called a ground field for A. A local algebra with a ground field may possess several ground fields. If A is a local algebra with a ground field K such that the residue field of A is a finite separable extension of K, then we say that A is a local algebra with a separating ground field K.

The purpose of this note is to remove the restriction on the ground field in Theorem 1. To be precise we prove

THEOREM 1'. Theorem 1 is true when A is a d-dimensional regular local algebra with any ground field.

We shall reduce the case of an arbitrary ground field to that of a separating ground field. For this we need a few results, some of them are well-know Let us first recall that if (A',m') and (A,m) are local rings, then $A' \subset A$ is called a local extension if $m' \subset m$.

LEMMA 2. Let $A' \subset A$ be a flat local extension. Then if A is regular so is A'.

PROOF. See [3, Theorem 51, page 155].

LEMMA 3. Let $R' \subset R$ be rings such that R' is regular. Suppose that R is faithfully flat over R'. Then for any ideal J in R', $\mathrm{ht}(J) = \mathrm{ht}(JR)$.

PROOF. We may as well assume that J is a prime ideal in R'. Since R' is regular it follows that $\mathrm{ht}(J) = \mathrm{grade}(J)$. Now R is faithfully flat over R' and so we get that $JR \neq R$ and that $\mathrm{grade}(J) \leq \mathrm{grade}(JR)$. Also we know that $\mathrm{grade}(JR) \leq \mathrm{ht}(JR)$. Hence $\mathrm{ht}(J) \leq \mathrm{ht}(JR)$. To prove the reverse inequality, we observe that the "going-down theorem" holds for a flat extension [3, Theorem 4, page 33]. This is equivalent to saying that if p is any minimal prime over JR in R then $p \cap R' = J$. Now we can leave it to the reader to easily conclude that $\mathrm{ht}(J) = \mathrm{ht}(JR)$.

The next couple of facts are concerned with some properties of maximal ideals in polynomial rings.

LEMMA 4. Let $R = A[T]$ be a polynomial ring over a ring A. Let M be a maximal ideal in R. Then $M \cap A$ is a maximal ideal in A if and only if M contains a monic polynomial.

PROOF. Let $M \cap A = p$. Suppose M contains a monic polynomial. Then it follows that $A/p \hookrightarrow R/M$ is an integral extension and hence A/p is a field as R/M is so. Conversely, if p is a maximal ideal then M/pR is a non-zero ideal in the PID $(A/p)[T]$. Now it is obvious that M contains a monic polynomial.

PROPOSITION 5. Let A be a regular local ring of dimension d. Let $R = A[T_1,\dots,T_n]$ be a polynomial ring. Then any maximal ideal in R has height $d+n$ or $d+n-1$.

PROOF. We shall use induction on n. Suppose $n=1$ so that $R = A[T]$. Let M be a maximal ideal in R and let $M \cap A = p$. Then $\bar{M}$ is a maximal ideal in $\bar{A}[T]$, where $\bar{M} = M/pR$ and $\bar{A} = A/p$. As $\bar{M} \cap \bar{A} = (0)$, by a theorem of Artin and Tate [1], $\dim(\bar{A}) \leq 1$. This implies that either p is the maximal ideal of A or p is a prime ideal in A of height $d-1$ ($\dim(\bar{A})+\mathrm{ht}(p) = \dim(A)$ as A is regular local), and accordingly $\mathrm{ht}(M) = d+1$ or d.

Now suppose that $n \geq 2$ and M is a maximal ideal in $R = A[T_1,\dots,T_n]$. By a lemma of Davis and Geramita [2, Lemma 2], we may assume that M contains a polynomial monic in T_n with coefficients in $R_1 = A[T_1,\dots,T_{n-1}]$. Therefore $M \cap R_1$ is a maximal ideal in R_1, by Lemma 4. By induction hypothesis $M \cap R_1$ has height $d+n-1$ or $d+n-2$. Hence M has height $d+n$ or $d+n-1$ as desired.

Q.E.D.

Combining the above results we get

PROPOSITION 6. Let A', A be d-dimensional regular local rings such that $A' \subset A$ is a flat local extension. Let $R' = A'[T_1,\dots,T_n]$ and $R = A[T_1,\dots,T_n]$

be polynomial rings. Then for any ideal J in R', $\mathrm{ht}(J) = \mathrm{ht}(JR)$ and $\dim(J) = \dim(JR)$.

PROOF. The first assertion follows from Lemma 3, as R is faithfully flat over R' (see [3]). If J is contained in a maximal ideal of height $d+n$ in R', then JR would be contained in a maximal ideal of height $d+n$ in R. Since R' and R are catenary rings (even regular) and $\mathrm{ht}(J) = \mathrm{ht}(JR)$, we conclude that $\dim(J) = \dim(JR)$. Suppose J is not contained in any maximal ideal of height $d+n$ in R'. We claim that JR is not contained in any maximal ideal of height $d+n$ in R. Let m' and m denote the maximal ideals of A' and A respectively. Then a maximal ideal in R' (resp. in R) has height $d+n$ if and only if it contains $m'R'$ (resp. mR). From the supposition it then follows that J and $m'R'$ are co-maximal and hence JR and mR co-maximal. Therefore JR is not contained in any maximal ideal of height $d+n$ in R and the claim is proved. We now observe that $\mathrm{ht}(J)+\dim(J) = d+n-1 = \mathrm{ht}(JR)+\dim(JR)$ as the rings are catenary. Hence $\dim(J) = \dim(JR)$. Q.E.D.

We now turn to the proof of Theorem 1'.

PROOF OF THEOREM 1'. Let A be a d-dimensional regular local algebra with a ground field k. We can present A as $A = C_p$, where $C = k[X_1,\dots,X_m]/(f_1,\dots,f_r)$ and p is a regular prime ideal in C. Let I be an ideal in $R = A[T_1,\dots,T_n]$. Suppose that I is generated by $g_1,\dots,g_s$. Let k_o be the prime field of k. Then we can find a finitely generated field extension L (contained in k) of k_o such that L contains all the coefficients of the f_i's and that L contains all the elements of k needed to describe the g_i's. Now define $B = L[X_1,\dots,X_m]/(f_1,\dots,f_r)$, $q = p \cap B$, $A' = B_q$ and $R' = A'[T_1,\dots,T_n]$. We have $B \hookrightarrow B \otimes_L k = C$. We observe that A is a flat extension of C and C is a flat extension of B, therefore A is a flat extension of B. Hence A is a flat extension of A'. Since A' ⊂ A is a local extension, by Lemma 2 A' is a regular. Now, if J is the ideal in R' generated by $g_1,\ldots,g_s$, then JR=I. Further, it is not difficult to see that we can choose the field L so that dim(A') = dim(A) = d. For this, either we take a regular sequence of length d in A and enlarge L (if need be) to describe this sequence in A', or we can enlarge L so that $qC = p$. By a similar reasoning we can also arrange that $\mu(J/J^2) = \mu(I/I^2)$. Obivously $\mu(I) \le \mu(J)$. Therefore $\mu(J) = \mu(J/J^2)$ would give that $\mu(I) = \mu(I/I^2)$. We now complete the proof as follows. By Proposition 6, we get ht(J) = ht(I) and dim(J) = dim(I). Therefore ht(J) > min{d,n+2} or ht(J) > min{d,n+1} as the case would be for ht(I). Moreover, we note that $\mu(I/I^2) \ge \dim(I)+2$ is the same thing as $\mu(J/J^2) \ge \dim(J)+2$. Finally, A' is a regular local algebra with a ground field L and L is a finitely generated field extension of k_o which is perfect; therefore, the proof reduces to the case of Theorem 1 by

LEMMA 7. Let A be a local domain. Suppose that A is a local algebra with a ground field which is a finitely generated field extension of a perfect field. Then A is a local algebra with a separating ground field.

PROOF. See [4, Lemma 2.10].

Sincere thanks are due to Paul Eakin for fruitful discussions.

Current Address:
Budh S. Nashier
Pennsylvania State University
Mont Alto Campus
Mont Alto, PA 17237

REFERENCES

1. E. Artin and J.T. Tate, A note on finite ring extensions, J. Math. Soc. Japan 3 (1951), pp. 74-77.

2. E.D. Davis and A.V. Geramita, Efficient generation of maximal ideals in polynomial rings, Trans. Amer. Math. Soc. 231 (1977), pp. 497-505.

3. H. Matsumura, Commutative Algebra, W.A. Benjamin, Inc., New York, 1970.

4. Budh S. Nashier, Efficient generation of ideals in polynomial rings, to appear.

5. Budh S. Nashier, On the conormal bundle of ideals, to appear.

6. Budh S. Nashier, Projective modules over regular polynomial rings: Quillen-Suslin's conjecture, lecture notes.

Dept. of Mathematics
University of Kentucky
Lexington, KY 40506, U.S.A.

Received October 19, 1982

C.R. Math. Rep. Acad. Sci. Canada - Vol. V, No.1, February 1983 Février

ON CHARACTER RINGS

B.M. Puttaswamaiah

Presented by G. de B. Robinson, F.R.S.C.

Let G be a group of finite order g, F a splitting field for G of characteristic p, and C the complex field. In this paper, by a character, we mean a Brauer character. When $F \subseteq C$, a result of Burnside [1] asserts the existence of a nonlinear irreducible character of G which assumes zero on a conjugate class. If p divides g, this result does not hold in general [2]. This paper determines a necessary and sufficient condition for the existence of such a class, and also describes its dual.

Let FG be the group algebra of G over F, n the number of p-regular conjugate classes and $\mathrm{Irr}(G)$ a full set of irreducible characters of G. The $n \times n$ matrix $A_k = [a_{ij}]$ defined by

$$\varphi^i \varphi^k = \sum_{j=1}^{n} a_{ij} \varphi^j; \quad i = 1,2,\ldots,n,$$

with φ^t in $\mathrm{Irr}(G)$, is the matrix of φ^k, whose eigenvalues $\varphi^k_1, \varphi^k_2, \ldots, \varphi^k_n$ are the values of φ^k [2]. The matrices $A_1, A_2, \ldots, A_n$ generate an algebra of dimension n over the ring of integers, which is studied in [2,3].

Theorem. Let W be an irreducible FG-module with character θ. Then there is a p-regular class on which θ is zero if and only if there exist FG-modules U and V with different characters such that the inner tensor products $U \otimes W$ and $V \otimes W$ afford the same character.

Proof. Let $A = [a_{ij}]$ be the matrix of $\theta = \varphi^k$, and $R_1, R_2, \ldots, R_n$ the rows of A.

Let θ assume zero on a p-regular class. Then $\det(A) = 0$, so the vectors $R_1, R_2, \ldots, R_n$ are linearly dependent over the rational field. Thus there are positive integers a_i and b_j such that

$$\sum_{i=1}^{u} a_i R_i = \sum_{j=1}^{v} b_j R_j \tag{1}$$

where $u + v \leq n$. Let U and V be FG-modules which afford the characters

$$\sum_{i=1}^{u} a_i\varphi^i + \sum_{r=1}^{w} c_r\varphi^r \quad \text{and} \quad \sum_{j=1}^{v} b_j\varphi^j + \sum_{r=1}^{w} c_r\varphi^r; \quad \varphi^t \in \mathrm{Irr}(G),$$

respectively. We shall show that $U\otimes W$ and $V\otimes W$ afford the same character. Indeed, substituting for R_i and R_j in (1), and equating the t-th component, we get

$$\sum_{i=1}^{u} a_i a_{it} = \sum_{j=1}^{v} b_j a_{jt}; \quad t = 1,2,. .,n, \tag{2}$$

so that

$$\sum_{i=1}^{u} a_i \sum_{t=1}^{n} a_{it}\varphi^t + \sum_{r=1}^{w} c_r \sum_{t=1}^{n} a_{rt}\varphi^t = \sum_{j=1}^{v} b_j \sum_{t=1}^{n} a_{jt}\varphi^t + \sum_{r=1}^{w} c_r \sum_{t=1}^{n} a_{rt}\varphi^t, \tag{3}$$

or equivalently

$$\left(\sum_{i=1}^{u} a_i\varphi^i + \sum_{r=1}^{w} c_r\varphi^r \right) \varphi^k = \left(\sum_{j=1}^{v} b_j\varphi^j + \sum_{r=1}^{w} c_r\varphi^r \right) \varphi^k \tag{4}$$

which proves the assertion.

Conversely, let U and V be the FG-modules such that $U\otimes W$ and $V\otimes W$ afford the same character. Let U and V afford the characters $\sum_{i=1}^{u} a_i\varphi^i + \sum_{r=1}^{w} c_r\varphi^r$ and $\sum_{j=1}^{v} b_j\varphi^j + \sum_{r=1}^{w} c_r\varphi^r$ respectively. Then by hypothesis, (4) is satisfied, which in tern implies (3). After cancelling the common part in (3), we use the linear independence of the irreducible characters to obtain (2). These equations imply that $\det(A) = 0$ and so θ assumes zero on a p-conjugate class.

The following result is a dual to the above result.

Theorem. Let $F \subseteq C$. *Given a conjugate class* K, *there is an irreducible FG-module with character* θ, *which is zero on* K, *if and only if there exist different nonempty normal subsets M and N, and non-negative integers* $a_1, a_2, \ldots, a_n, b_1, b_2, \ldots b_n$ *such that* $(\sum_{i=1}^{n} a_i c_i)k = (\sum_{j=1}^{n} b_j c_j)k$ *and* $MK = NK$ *where* $\mathrm{supp}(\sum_{i=1}^{n} a_i c_i) = M$, $\mathrm{supp}(\sum_{i=1}^{n} b_j c_j) = N$ *and* $\mathrm{supp}(k) = K$.

Proof. The class sums $C_1, C_2, \ldots, C_n$ form a basis of the centre Z of FG. The matrix $B_k = [b_{ij}]$ of K is given by .

$$C_i C_k = \sum_{j=1}^{n} b_{ij} C_j ; \quad i = 1,2,\ldots,n \tag{4}$$

where C_k is the class sum of K. Let $\{T^1, T^2, \ldots, T^n\}$ be a full set of irreducible representations of G, and let the FG-module V_i afford T^i, and the character φ^i. As $T^t(C_i)$ lies in the centre of the image of T^t, it follows by Schur's Lemma that $T^t(C_i) = \omega_i^t I$, with ω_i^t in F. Taking trace on both sides, we get $z_t \omega_i^t = h_i \varphi_i^t$ where h_i is the number of elements in the i-th class, and $z_t = \varphi^t(1)$. The equations (4) yield

$$\omega_i^t \omega_k^t = \sum_{j=1}^{n} b_{ij} \omega_j^t ; \quad i = 1,2,\ldots,n$$

from which it follows that $\omega_k^1, \omega_k^2, \ldots, \omega_k^n$ are the eigenvalues of B_k and $\det(B_k) = \omega_k^1 \omega_k^2 \cdots \omega_k^n$.

Suppose that V_r affords φ^r, and φ^r assumes zero on K. Then $z_r \omega_k^r = h_k \varphi_k^r = 0$. Thus $\det(B_k) = 0$ and the rows of B_k are linearly dependent. There exist positive integers a_i and b_j such that

$$\sum_{i=1}^{u} a_i b_{it} = \sum_{j=1}^{v} b_j b_{jt} ; \quad t = 1,2,\ldots,n . \tag{5}$$

Let M and N be the supports of the elements

$$\sum_{i=1}^{u} a_i C_i + \sum_{k=1}^{w} c_k C_k \quad \text{and} \quad \sum_{j=1}^{v} b_j C_j + \sum_{k=1}^{w} c_k C_k \tag{6}$$

respectively, where c_k may be zero. Then (5) and (6) imply

$$\sum_{i=1}^{u} a_i \sum_{t=1}^{n} b_{it} C_t + \sum_{r=1}^{w} c_r \sum_{t=1}^{n} b_{rt} C_t = \sum_{j=1}^{v} b_j \sum_{t=1}^{n} b_{jt} C_t + \sum_{r=1}^{w} c_r \sum_{t=1}^{n} b_{rt} C_t , \tag{7}$$

which is equivalent to the assertion

$$\left(\sum_{i=1}^{u} a_i C_i + \sum_{r=1}^{w} c_r C_r \right) C_k = \left(\sum_{j=1}^{v} b_j C_j + \sum_{r=1}^{w} c_r C_r \right) C_k . \tag{8}$$

This proves the result in one direction.

Conversely, let M and N be non-empty normal subsets and $a_1, a_2, \ldots, a_n$, $b_1, \ldots, b_n$ be integers satisfying the hypothesis. Write $\sum_{i=1}^{n} a_i C_i$ and $\sum_{j=1}^{n} b_j C_j$ in the form

$$\sum_{i=1}^{u} a_i C_i + \sum_{r=1}^{w} c_r C_r \quad \text{and} \quad \sum_{j=1}^{v} b_j C_j + \sum_{r=1}^{w} c_r C_r ,$$

respectively. By hypothesis, (8) is satisfied, which in turn implies (7). After cancelling the common part, we use linear independence of the class sums to obtain (5), which is equivalent to the assertion that $\det(B_k) = 0$. Hence there is an irreducible character, which assumes 0 on K.

Lemma. For any n integers $a_1, a_2, \ldots, a_n$,

$$\prod_{x \in G} \left(\sum_{i=1}^{n} a_i \varphi^i(x) \right)$$

is a rational integer.

Proof. The algebra generated by $A_1, A_2, \ldots, A_n$ over C is a semisimple commutative algebra [2]. The eigenvalues of $\sum_{i=1}^{n} a_i A_i$ are

$$\omega_j = \sum_{i=1}^{n} a_i \varphi_j^i \; ; \quad j = 1, 2, \ldots, n$$

whose product is an integer. The minimum polynomial of ω_j over the rational field, is a factor of the characteristic polynomial f of $\sum_{i=1}^{n} a_i A_i$, so that every algebraic conjugate of ω_j is also a root of f. The product of the roots of the minimum polynomial of the algebraic integer ω_j is a rational integer. Taking repetitions into account, we can write

$$\{ \sum_{i=1}^{n} a_i \varphi^i(x) \mid x \in G \} = S_1 \cup S_2 \cup \cdots \cup S_t$$

where $S_i \cap S_j = \varphi$ for $i \neq j$ and the members of each S_i are algebraic conjugates. The result now follows.

Corollary. For any φ^i, $\prod_{x \in G} \varphi^i(x) / \varphi(1)$ is a rational integer.

Theorem. Let $F \subseteq C$. For any irreducible FG-module W of dimension > 1, there exist nonisomorphic FG-modules U and V such that $U \otimes W$ and $V \otimes W$ are isomorphic.

Proof. See [2].

A weak version of a dual to the above result is the following variation of a result of Burnside [1]. Let $F \subseteq C$ and G be simple. Let K be a nontrivial class of G such that $(|K|, \varphi(1)) = 1$ for some φ in $\mathrm{Irr}(G)$. Then φ assumes zero on K.

REFERENCES

1. Feit, W. Character of Finite Groups, Benjamin (1967).
2. Puttaswamaiah, B.M. Determination of Brauer Characters, CJM 26 (1974).
3. Robinson, G. deB. Tensor Product Representations, J. of Algebra 20(1972).

Dept. of Mathematics
Carleton University
Ottawa, Ontario
Canada K1S 5B6

Received October 23, 1982

C.R. Math. Rep. Acad. Sci. Canada - Vol. V, No.1, February 1983 Février

NONEXPANSIVE MAPPINGS ON BANACH LATTICES

Jonathan Borwein and Brailey Sims
Presented by P.A. Fillmore, F.R.S.C.

1. Introduction.

A mapping T defined on a weakly compact convex subset C of a Banach space X is said to be nonexpansive if $||T(x)-T(y)|| \leq ||x-y||$ for all x and y in C; and X is said to have the (weak) fixed point property (FPP) if every such mapping has a fixed point. Classical results ([4],[7]) show that every uniformly convex Banach space and those with normal structure have the fixed point property. Until recently other positive results remained fragmentary. Moreover, it was only in 1981 that Alspach [1] showed that $L_1[0,1]$ does not have the FPP (see also [11],[12]).

Also, Maurey [10] showed, using ultrapower techniques, that $c_0(\mathbb{N})$ and reflexive subspaces of $L_1[0,1]$ have the FPP. In this paper we refine Maurey's ideas on c_0 and remove the dependence on ultrapowers. We are then able to show that many Banach spaces satisfy simple and verifiable lattice-theoretic criteria and so have the FPP. In particular we: (1) characterize order-complete M spaces with the FPP; (2) show that $c_0(S)$, $c(S)$, and Day's norm on $c_0(S)$ have the FPP; (3) recover-much strengthened-examples due to Karlovitz [6] and others; (4) exhibit spaces without asymptotic normal structure which have the FPP.

Full details of these and other results are forthcoming in [3].

2. Basic results.

A sequence (x_n) in C is approximately fixed for T if $||x_n-T(x_n)||$ tends to 0 . It is a simple consequence of the Contraction Principle that such sequences exist. The following basic construction allows us to replace approximate fixed points by fixed points of a related mapping. Let $l_\infty(X)$ and $c_0(X)$ denote the substitution spaces of X into $l_\infty(\mathbb{N})$ and

$c_0(\mathbb{N})$, with elements $[x]:=(x_n)$. Define $[X]$ to be the quotient $l_\infty(X)/c_0(X)$ with $\|[x]\|:=\limsup_{n\to\infty}\|x_n\|$, and define $[C]:=(\prod_{n=1}^{\infty} C)/c_0(X)$. Then $[C]$ is closed bounded and convex and $[T]([x]):=[T(x_n)]$ defines a nonexpansive mapping on $[C]$. It is clear that $[x]$ is fixed for $[T]$ exactly when (x_n) is approximately fixed for T .

In any Banach space, the <u>quasi-midpoint set</u> $Q(y,z):=\{w\in C:\|y-w\|=\|z-w\|=(1/2)\|y-z\|\}$ is a nonempty closed convex subset of C . If T is nonexpansive and C is closed convex and T-invariant then $Q(y,z)$ is also T-invariant whenever y and z are fixed. The first result follows from the Contraction Principle and a diagonal arguement applied to $[T]$ on $Q([x],[y])$. Maurey gives a similar (slightly weaker) result using ultrapowers.

<u>Proposition 1</u>. ([3]) <u>Suppose that C is a minimal T-invariant weakly compact convex subset of X containing 0. Suppose also that (x_n) and (y_n) are approximately fixed for T in C and that $\lim_{n\to\infty}\|x_n-y_n\| = \operatorname{diam}(C)$. Then there exists a sequence (z_n) of approximately fixed points in C with</u>

$$(1) \qquad \lim_{n\to\infty}\|x_n-z_n\| = \lim_{n\to\infty}\|y_n-z_n\| = (1/2)\lim_{n\to\infty}\|z_n\| = (1/2)\operatorname{diam}(C) .$$

The existence of diametral approximately fixed points can always be guaranteed ([3],[6],[10]). We also need two lattice-theoretic concepts. A subset C of a Banach lattice will be called <u>weakly orthogonal</u> if

$$(2) \qquad \liminf_{n\to\infty}\liminf_{m\to\infty}\| \, |x_n-\bar{x}|\wedge|x_m-\bar{x}| \, \|= 0$$

whenever (x_n) converges weakly to $\bar{x}$ in C. A lattice Y is said to be <u>weakly orthogonal</u> whenever all its weakly compact subsets are. It is relatively easy to show that $c(S)$, $c_0(S)$, $l_p(S)$ $(1\le p<\infty)$ are weakly orthogonal while $l_\infty(\mathbb{N})$ and non-atomic L_p spaces are not. Obviously, any norm-compact set is weakly orthogonal. It is also easy to see that every Orlicz sequence space with the "delta-two" condition [9] is weakly orthogonal. Finally, we define the Riesz angle of a Banach lattice by

(3) $$a(X) := \sup\{\||x|\vee|y|\| : \|x\| \le 1, \|y\| \le 1\}.$$

Proposition 2. ([3]) (a) For any Banach lattice X, $1 \le a(X) \le 2$ with $a(X)=1$ if and only if X is an M space. (b) If X is an abstract L_p space ($1 \le p \le \infty$) then $a(X) = 2^{1/p}$. (c) Let X be a full substitution space on an index set I and $(X_i : i \in I)$ is a family of Banach lattices. Then for the substitution space $P := P(X_i, X)$

(4) $$a(P) \le a(X) \sup_{i \in I} a(X_i) \quad .$$

The fundamental inequality involving the Riesz angle is:

(5) $$\|z\| \le a(X)(\|x-z\|\vee\|x-y\|) + \||x|\wedge|y|\|.$$

and is easily established.

3. Fixed point theorems.

Recall that the Mazur distance between two Banach spaces X and Y is given by $d(X,Y) := \inf\{\|U\|\|U^{-1}\| : U$ is an isomorphism of X onto $Y\}$.

Theorem 1. ([3]) A Banach space X has the FPP if there exists a weakly orthogonal Banach lattice Y such that

(6) $$d(X,Y)\, a(Y) < 2 \quad .$$

Proof. We suppose that T is nonexpansive on a minimal invariant weakly compact subset C. Select an approximately fixed sequence (a_n). On extracting a subsequence and translating we may assume that (a_n) is weakly null and that 0 lies in C. Now use (6) to pick an isomorphism U of X onto Y with (7) $\|U\|\,\|U^{-1}\|a(Y) < 2$. Since Y is weakly orthogonal, we can find subsequences (x_n) and (y_n) of (a_n) with (8) $\| |Ux_n| \wedge |Uy_n| \|$ tending to zero in norm. Since any approximately fixed sequence is diametrizing [6] we can also assume that (9) $\|x_n - y_n\|$ tends to diam(C). Proposition 1 produces a third approximately fixed sequence (z_n) satisfying (1). Now (5) shows that

$$(10)\quad \limsup_{n\to\infty} \|Uz_n\| \leq a(Y) \limsup_{n\to\infty} (\|Ux_n - Uz_n\|) \vee (\|Uy_n - Uz_n\|) + \limsup_{n\to\infty} \| |Ux_n| \wedge |Uy_n| \|$$

Now (1), (8) and (10) combine to show that $2\,\mathrm{diam}(C) \leq \|U\|\,\|U^{-1}\| a(Y) \mathrm{diam}(C)$. Since (7) holds C must be singleton.

Corollary 1. (a) *Every weakly orthogonal lattice with Riesz angle less than two has the FPP.*

(b) *A Banach space X such that* $d(X, l_p) < 2^{1-1/p}$ *has the FPP (for* $1<p<\infty$) .

(c) *A Banach space X such that* $d(X, c(S)) < 2$ *or* $d(X, c_0(S)) < 2$ *has the FPP*.

Corollary 2. *An abstract L_p space* $(1 \leq p \leq \infty)$ *or an abstract order-complete M space has the FPP if and only if it contains no isometric copy of* $L_1[0,1]$.

Proof. For $p>1$, L_p spaces are uniformly convex and the result is trivial. For $p = 1$, it is a consequence of Alspach's example, the fact that atomic L_1 spaces have the FPP, and the fact that a non-atomic L_1 space contains a copy of $L_1[0,1]$. Finally, any order-complete M space which contains no copy of $l_\infty(\mathbb{N})$ is isomorphic and isometric to $c_0(S)$ on some index set S [8].

Example 1. ([6]) (a) Let $1 \leq p \leq r < \infty$ and let $t > 0$. Consider $X := X(p,r,t)$ as $l_p(S)$ renormed by $\|x\| := \|x\|_r \vee (t\|x\|_p)$. For $p = 2$,

$r = \infty$ these norms were studied in [2], [6]. It is immediate that X is weakly orthogonal and Proposition 2 (c) shows that $a(X) \leq 2^{1/p} < 2$. Thus X has the FPP. Baillon and Schönberg [2] showed that $X(2,\infty,t)$ has normal structure only for $t > 1/\sqrt{2}$, and asymptotic normal structure only for $t > 1/2$. Their results, therefore, only apply for $t > 1/2$.

(b) It is almost immediate that Day's norm on $c_0(S)$ [5] has $d(X,c_0(S)) \leq \sqrt{3}/2 < 2$. Corollary 1 (c) shows that Day's norm has the FPP. Note that $d(c(S),c_0(S)) = 3$ and the two parts of Corollary 1(c) are thus distinct. Note also that $c_0(S)$ is locally uniformly convex, but is not uniformly convex in every direction [5].

Remark 1. Our results can be rephrased so that they apply to weakly orthogonal sets in arbitrary lattices. In particular, every weakly orthogonal subset of $l_\infty(S)$ has the FPP. This is interesting because every Banach space is isometric to a subspace of some $l_\infty(S)$. One can therefore show that a class of spaces has the FPP by showing that their isometric images are weakly orthogonal in the l_∞ lattice structure. Conversely, it follows that any isometric image of the $L_1[0,1]$ unit interval must fail to be weakly orthogonal since such sets admit nonexpansive mappings without fixed points [12]. Is it possible to use these ideas to show that (super-) reflexive spaces have the FPP?

5. References.

1. Alspach, D.E., "A fixed point free nonexpansive map", Proc. Amer. Math. Soc., 82(1981), 423-424.

2. Baillon, J.B. and Schönberg, R., "Asymptotic normal structure and fixed points of nonexpansive mappings", Proc. Amer. Math. Soc., 81 (1981), 257-264.

3. Borwein, J.M. and Sims B., "Nonexpansive mappings on Banach lattices and related topics", in preprint.

4. Browder, F.E., "Nonexpansive nonlinear operators in Banach spaces", Proc. Nat. Acad. Sci., U.S.A. 54(1965), 1041-1044.

5. Day M.M., Normed linear spaces, 3rd edition (Springer-Verlag, 1973).

6. Karlovitz, L., "Existence of fixed points of nonexpansive mappings in a space without normal structure", Pacific J. Math., 66(1976), 153-159.

7. Kirk, W.A., "A fixed point theorem for mappings which do not increase distance", The American Math. Monthly, 72(1965), 1004-1006.

8. Lacey, E., The isometric theory of classical Banach spaces (Springer-Verlag, 1974).

9. Lindenstrauss, J. and Tzafriri, L., Classical Banach spaces, I. Sequence spaces (Springer-Verlag, 1977).

10. Maurey B., "Points fixes des contractions de certains faiblement compact de L", preprint.

11. Schechtman, G., "On commuting families of nonexpansive operators", Proc. Amer. Math. Soc., 84(1982), 373-376.

12. Sine, R., "Remarks on the example of Alspach", preprint.

Dalhousie University
Halifax, N.S. B3H 4H8

Received November 2, 1982

C.R. Math. Rep. Acad. Sci. Canada - Vol. V, No.1, February 1983 Février

CARACTERISATION DE LA FONCTION $f(x) = x$ PAR UN SYSTEME DE DEUX EQUATIONS FONCTIONNELLES

Peter Volkmann

Presented by J. Aczél, F.R.S.C.

Résumé. Désignons par R l'ensemble des nombres réels. Le théorème suivant sera démontré.

Théorème. Soit $f:R \longrightarrow R$ une solution des équations fonctionnelles

$$f(x^2) = f(x)^2 \;,\; f(1 + x) = 1 + f(x) \qquad (x \in R).$$

Alors

$$(1) \quad f(x) = x \qquad (x \in R).$$

Démonstration. D'abord il est clair que

$$f(x) \geqslant 0 \qquad (x \geqslant 0),$$

$$(2) \quad f(m + x) = m + f(x) \qquad (m \text{ entier}, x \in R).$$

La formule

$$f(-x) = -f(x) \qquad (x \in R)$$

est une conséquence des relations

$$1 + 2f(-x) + f(x)^2 = 1 + 2f(-x) + f(-x)^2 = (1 + f(-x))^2$$

$$= f(1 - x)^2 = f(-1 + x)^2 = (-1 + f(x))^2 = 1 - 2f(x) + f(x)^2.$$

Soit maintenant

$$m \leqslant x \leqslant n$$

avec m,n entiers. On a

$$x - m \geqslant 0 \;,$$

d'où

$$f(x) - m = f(x - m) \geqslant 0 \;,$$

donc

$$m \leqslant f(x).$$

Puisque $-n \leqslant -x$, on obtient de même

$$-n \leqslant f(-x),$$

d'où

$$f(x) = -f(-x) \leqslant n.$$

En résumant,

$$m \leqslant x \leqslant n \Longrightarrow m \leqslant f(x) \leqslant n \qquad (m,n \text{ entiers}; x \in R).$$

Si l'on fait $m = [x] =$ partie entière de x et $n = [x] + 1$, il résulte aisément

$$|x - f(x)| \leqslant 1 \qquad (x \in R).$$

Si $k = 2^n$ (n entier, $\geqslant 1$), cette inégalité fournit

$$1 \geqslant |x^k - f(x^k)| = |x^k - f(x)^k| =$$

$$= |x - f(x)| \cdot |x^{k-1} + x^{k-2}f(x) + \dots + f(x)^{k-1}|.$$

Si de plus $x > 1$ (donc $f(x) \geqslant 0$), il résulte

$$|x - f(x)| \leqslant 1/x^{2^n-1} \longrightarrow 0 \qquad (n \longrightarrow \infty),$$

donc

$$f(x) = x \qquad (x > 1).$$

En tenant compte de (2), on en déduit (1).

Remarque. Il me faut exprimer ma gratitude à M. le Professeur F.Radó. Une conversation avec lui en 1982 à Oberwolfach a inspiré les considérations ci-dessus.

Ringstr. 6
6729 Neuburg am Rhein
ALLEMAGNE OCCIDENTALE

Received November 15, 1982

C.R. Math. Rep. Acad. Sci. Canada - Vol. V, No.1, February 1983 Février

THE SIGNATURE OF A REAL CLIFFORD ALGEBRA

W. H. Greub

Presented by G.de B. Robinson, F.R.S.C

1. The signature of an associative algebra. Let A be a finite dimensional associative algebra with unit element e and denote left multiplication by $\mu(a)$,

$$\mu(a)b = a\cdot b.$$

The Killing form of A is the bilinear function K_A defined by

(1) $$K_A(a,b) = \frac{1}{\dim A}\operatorname{tr}(\mu(a)\circ\mu(b))$$

or equivalently,

$$K_A(a,b) = \frac{1}{\dim A}\operatorname{tr}\mu(ab).$$

It follows directly from (1) that

(2) $$K_A(a,b) = K_A(b,a)$$

and

$$K_A(e,e) = 1.$$

Moreover, if $\varphi : A \xrightarrow{\cong} A'$ is an isomorphism, then

(3) $$K_A = \varphi^* K_{A'}.$$

In fact,

$$(\varphi^* K_{A'})(a,b) = K_{A'}(\varphi a, \varphi b) = \operatorname{tr}\mu(\varphi(ab)).$$

Since

$$\mu(\varphi a)\circ\varphi = \varphi\circ\mu(a)$$

it follows that

$$(\varphi^* K_{A'})(a,b) = \operatorname{tr}(\varphi\circ\mu(ab)\circ\varphi^{-1}) =$$
$$= \operatorname{tr}\mu(a,b) = K(a,b).$$

Finally, let $\mathcal{B}$ be a second finite dimensional associative algebra and consider the tensor product $A\otimes\mathcal{B}$. Then we have

$$\mu(a\otimes b) = \mu(a)\otimes\mu(b), \quad a\in A,\ b\in\mathcal{B}$$

and thus

$$\operatorname{tr}\mu(a\otimes b)=\operatorname{tr}\mu(a)\cdot\operatorname{tr}\mu(b)$$

This implies that

$$K_{A\otimes B}(a\otimes b,a'\otimes b')=K_A(a,a')\cdot K_B(b,b'). \tag{4}$$

2. The signature of A. The signature of the Killing form K_A will be called the signature of A and will be denoted by σ_A. It follows from (3) that $\sigma_{A'}=\sigma_A$ if A and A' are isomorphic. Formula (4) implies that

$$\sigma_{A\otimes B}=\sigma_A\cdot\sigma_B .$$

Example 1: Let $\mathbb{C}$ be the algebra of complex numbers, considered as a 2-dimensional algebra over $\mathbb{R}$. Then we have

$$K_{\mathbb{C}}(a,b)=\operatorname{Re}(ab),\qquad a,b\in\mathbb{C}.$$

Thus, $K_{\mathbb{C}}(1,1)=1$ and $K_{\mathbb{C}}(i,i)=-1$ and so $\sigma_{\mathbb{C}}=0$.

Example 2: Consider the algebra of quaternions. Its Killing form is given by

$$K_{\mathbb{H}}(a,b)=(a,\bar{b})$$

where $\bar{b}$ denotes the conjugate quaternion. Now choose an orthonormal basis of the form e,e_1,e_2,e_3 where e denotes the unit element. Then we have $K_{\mathbb{H}}(e,e)=1$ and $K_{\mathbb{H}}(e_j,e_j)=-1$, $j=1,2,3$ It follows that $\sigma_{\mathbb{H}}=-2$.

Example 3: Let V be a real n-dimensional vector space and let $L(V)$ be the algebra of linear transformations of V. Since

$$\operatorname{tr}\mu(\alpha)=n\operatorname{tr}\alpha,\qquad \alpha\in L(V),$$

it follows that

$$K(\alpha,\beta)=\frac{1}{n^2}\,n\operatorname{tr}(\alpha\circ\beta)=\frac{1}{n}\operatorname{tr}(\alpha\circ\beta)$$

and thus

$$\sigma_{L(V)}=n.$$

3. The Killing form of a $\mathbb{Z}_2$-graded algebra. Let A be a $\mathbb{Z}_2$-graded algebra and write

$$A=A^0\oplus A^1.$$

Recall that

$$A^0 \cdot A^0 \subset A^0, \quad A^1 \cdot A^1 \subset A^0$$

and

$$A^0 \cdot A^1 \subset A^1, \quad A^1 \cdot A^0 \subset A^1.$$

Thus, if $a_1 \in A_1$, we have $\operatorname{tr} \mu(a_1) = 0$. It follows that

$$K_A(a, b) = K_A(a_0, b_0) + K_A(a_1, b_1),$$

where $a = a_0 + a_1$ and $b = b_0 + b_1$. Hence, setting $K_A^0(a, b) = K_A(a_0, b_0)$ and $K_1(a, b) = K_A(a_1, b_1)$ we have the formula

$$K_A(a, b) = K_A^0(a, b) + K_A^1(a, b), \quad a, b \in A$$

Proposition I: Let A and B be finite dimensional $\mathbb{Z}_2$-graded algebras and consider the skew tensor product $A \hat{\otimes} B$. Then

$$K^0_{A\hat{\otimes}B}(a \otimes b, a' \otimes b') = K_A^0(a, a') K_B^0(b, b') - K_A^1(a, a') K_B^1(b, b')$$

and

$$K^1_{A\hat{\otimes}B}(a \otimes b, a' \otimes b') = K_A^0(a, a') K_B^1(b, b') + K_A^1(a, a') K_B^0(b, b').$$

Proof: This follows directly from the relations

$$(a \otimes b)_0 = a_0 \otimes b_0 + a_1 \otimes b_1 \qquad a \in A, \ b \in B$$

$$(a \otimes b)_1 = a_0 \otimes b_1 + a_1 \otimes b_0,$$

and the definition of the multiplication in $A \hat{\otimes} B$.

Corollary: The signatures of $K^0_{A\hat{\otimes}B}$ and $K^1_{A\hat{\otimes}B}$ are given by

$$\sigma^0_{A\hat{\otimes}B} = \sigma_A^0 \cdot \sigma_B^0 - \sigma_A^1 \cdot \sigma_B^1$$

and

$$\sigma^1_{A\hat{\otimes}B} = \sigma_A^0 \cdot \sigma_B^1 - \sigma_A^1 \cdot \sigma_B^0.$$

respectively.

4. The signature of a Clifford algebra. Let E be an n-dimensional vector space with a non-degenerate inner product of type (p, q), $p + q = n$ and let C_E

denote the Clifford algebra over E. Recall that $\dim C_E = 2^n$. The Killing form of C_E will be denoted by K_E. Thus,

$$K_E(a,b) = \frac{1}{2^n} \operatorname{tr} \mu(a \cdot b), \qquad a, b \in C_E$$

We show that for $x \in E$ and $y \in E$

$$(5) \qquad K_E(x,y) = (x,y)_E .$$

In fact, since

$$x^2 = (x,x)_E \cdot e, \qquad x \in E,$$

we have

$$K_E(x,x) = \frac{1}{2^n}(x,x)_E \operatorname{tr} \iota = (x,x)_E$$

and (5) follows.

Next observe that C_E is a $\mathbb{Z}_2$-graded algebra (cf. [1], sec 10.6) and write, as in sec. 3,

$$K_E = K_E^0 + K_E^1 .$$

Theorem I: The signatures of K_E^0 and K_E^1 are given by

$$\sigma_E^0 = 2^{\frac{n}{2}} \cos \frac{s\pi}{4}$$

and

$$\sigma_E^1 = 2^{\frac{n}{2}} \sin \frac{s\pi}{4}$$

where $s = p - q$. Thus the signature of K_E is given by

$$\sigma_E = 2^{\frac{n}{2}} \left(\cos \frac{s\pi}{4} + \sin \frac{s\pi}{4} \right).$$

Proof: If $n = 1$, we have $s = 1$ or $s = -1$. In the first case

$$\sigma_E^0 = 1 = 2^{\frac{1}{2}} \cos \frac{\pi}{4}, \quad \sigma_E^1 = 1 = 2^{\frac{1}{2}} \sin \frac{\pi}{4}$$

whereas in the second case

$$\sigma_E^0 = 1 = 2^{\frac{1}{2}} \cos\left(-\frac{\pi}{4}\right), \quad \sigma_E^1 = -1 = 2^{\frac{1}{2}} \sin\left(-\frac{\pi}{4}\right)$$

Thus the theorem holds for $n = 1$.

Now assume by induction that the theorem is correct for vector spaces of dimension $< n$ and let E be an n-dimensional vector space. Choose an orthogonal decomposition into proper subspaces, $E = E_1 \oplus E_2$. Then C_E is the skew tensor product of the $\mathbb{Z}_2$-graded Clifford algebras C_{E_1} and C_{E_2},

$$C_E \cong C_{E_1} \hat{\otimes} C_{E_2}$$

Let n_1, n_2 (resp. s_1, s_2) denote the dimensions (resp. signatures) of E_1 and E_2. Then we have by induction

$$\sigma_{E_1}^0 = 2^{\frac{n_1}{2}} \cos \frac{s_1\pi}{4}, \quad \sigma_{E_1}^1 = 2^{\frac{n_1}{2}} \sin \frac{s_1\pi}{4}$$

and

$$\sigma_{E_2}^0 = 2^{\frac{n_2}{2}} \cos \frac{s_2\pi}{4}, \quad \sigma_{E_2}^1 = 2^{\frac{n_2}{2}} \sin \frac{s_2\pi}{4}.$$

Now Proposition I implies that

$$\sigma_E^0 = 2^{\frac{n}{2}} \left(\cos \frac{s_1\pi}{4} \cos \frac{s_2\pi}{4} - \sin \frac{s_1\pi}{4} \sin \frac{s_2\pi}{4} \right) = 2^{\frac{n}{2}} \cos \frac{s\pi}{4}$$

$$\sigma_E^1 = 2^{\frac{n}{2}} \left(\sin \frac{s_1\pi}{4} \cos \frac{s_2\pi}{4} + \cos \frac{s_1\pi}{4} \sin \frac{s_2\pi}{4} \right) = 2^{\frac{n}{2}} \sin \frac{s\pi}{4}.$$

Thus the induction is closed and the proof is complete

5. Isomorphism theorems. From now on we shall denote C_E by $C(p,q)$.

Theorem II: The algebra $C(p,q)$ is isomorphic to the algebra of linear transformations of a vector space if and only if

$$s = 8k \quad \text{or} \quad s = 8k + 2, \quad k \in \mathbb{Z}.$$

Proof: Assume that

$$C(p,q) \cong L(V)$$

where V is a vector space. Then

$$2^n = (\dim V)^2$$

and so n must be even, $n = 2m$. Since

$$\sigma_E = 2^m \left(\cos \frac{s\pi}{4} + \sin \frac{s\pi}{4} \right)$$

and

$$\sigma_{L(V)} = 2^m,$$

it follows that

$$\cos \frac{s\pi}{4} + \sin \frac{s\pi}{4} = 1$$

which implies that $s = 8k$ or $s = 8k + 2$, $k \in \mathbb{Z}$.

Conversely, if s is of this form, it follows from the general isomorphism theorems on Clifford algebras (cf. [1] sec. 10.22) that $C(p,q) \cong L(\wedge \mathbb{R}^m)$ where $n = 2m$.

Corollary: $C(n,0) \cong L(V)$ if and only if $n = 8k$ or $n = 8k+2$ and $C(0,n) \cong L(V)$ if and only if $n = 8k$ or $n = 8k+6$. Next consider two algebras $C(p,q)$ and $C(p',q')$ where $p+q = n$ and $p'+q' = n$.

Theorem III: The algebras $C(p,q)$ and $C(p',q')$ are isomorphic if and only if

$$s'-s = 8k \quad \text{or} \quad s'+s = 8k+2, \quad k \in \mathbb{Z}$$

They are isomorphic as $\mathbb{Z}_2$-graded algebras, if and only if $s'-s = 8k$, $k \in \mathbb{Z}$.

Proof: If

$$C(p,q) \cong C(p',q')$$

it follows that

$$\cos\frac{s\pi}{4} + \sin\frac{s\pi}{4} = \cos\frac{s'\pi}{4} + \sin\frac{s'\pi}{4}$$

whence

$$s'-s = 8k \quad \text{or} \quad s'+s = 8k+2, \quad k \in \mathbb{Z}$$

Now assume that $C(p,q)$ and $C(p',q')$ are isomorphic as $\mathbb{Z}_2$-graded algebras. Then we have the relations

$$\cos\frac{s\pi}{4} = \cos\frac{s'\pi}{4}, \quad \sin\frac{s\pi}{4} = \sin\frac{s'\pi}{4},$$

which imply that $s'-s = 8k$, $k \in \mathbb{Z}$.

Conversely, suppose that $s'-s = 8k$ or $s'+s = 8k+2$. Then by the general structure theorems (cf. [1], sec. 10.22) $C(p,q) \cong C(p',q')$. Moreover, if $s'-s = 8k$, then $C(p,q)$ and $C(p',q')$ are isomorphic as $\mathbb{Z}_2$-graded algebras.

Corollary: The algebras $C(p,q)$ and $C(q,p)$ are isomorphic if and only if $s = 4k$, $k \in \mathbb{Z}$. If this condition is satisfied, they are isomorphic as $\mathbb{Z}_2$-graded algebras.

Example: Consider the algebras $C(7,0)$ and $C(5,2)$. Then $s = 7$, $s' = 3$ and so $s'-s = -4$ and $s'+s = 10$. It follows that these algebras are isomorphic but not isomorphic as $\mathbb{Z}_2$-graded algebras.

[1] W. Greub, Multilinear Algebra, second edition, Springer New York, 1978.

[2] I.R. Porteous: Topological Geometry Van Nostrand Reinhold Company, London, 1969.

Dept. of Mathematics
University of Toronto
Toronto, Ontario, Canada M5S 1A1

Received November 22, 1982

C.R. Math. Rep. Acad. Sci. Canada - Vol. V, No.1, February 1983 Février

ON THE WIGNER QUASI-PROBABILITY DISTRIBUTION FUNCTION III

Walter Schempp

Presented by P. Scherk, F.R.S.C.

In the preceding part [9] of this series of papers we have been concerned specifically with radially symmetric, i.e., $SO(2,\mathbf{R})$-invariant Wigner quasi-probability distribution functions $P(f;.,.)$ with respect to states $f \in \mathscr{S}(\mathbf{R})$, $\|f\| = 1$, of a non-relativistic quantum mechanical system of one degree of freedom (cf. [8]). It is the purpose of the present part to continue these investigations in order to establish some more details in this direction by a systematic application of the techniques of nilpotent harmonic analysis. In particular our approach will show that harmonic analysis of the Heisenberg nilpotent group $\tilde{A}(\mathbf{R})$ attached to the field $\mathbf{R}$ provides a framework in which to place the radial case in a extremely smooth manner. The key fact for our procedure is that the symplectic group $\mathbf{Sp}(1,\mathbf{R})$ which forms the automorphism group of $\tilde{A}(\mathbf{R})$ leaving the center Z ($\cong \mathbf{R}$) of $\tilde{A}(\mathbf{R})$ pointwise fixed forms (expressed in the language of electrical engineering) also the group of all energy preserving invariants of the radar ambiguity surface with respect to the signal envelope f (cf. [5],[6],[7]).

Let $\mathbf{Mp}(1,\mathbf{R})$ denote the metaplectic group which forms the unique two-fold covering group of the group $\mathbf{Sp}(1,\mathbf{R}) = \mathbf{SL}(2,\mathbf{R})$, and let $\tilde{\sigma} \longrightarrow \sigma$ denote the projection (or covering) map involved. Moreover, let $\tilde{\sigma} \longrightarrow T_{\tilde{\sigma}}$ denote the oscillator (sometimes Weil-Shale or metaplectic) representation of $\mathbf{Mp}(1,\mathbf{R})$ acting on the complex Hilbert space $L^2(\mathbf{R})$. If the identity

$$P(f;x,y) = P(f';x',y')$$

holds for another quantum mechanical state $f' \in \mathscr{S}(\mathbf{R})$, $\|f'\| = 1$, and all points (x,y), (x',y') of the real phase plane $\mathbf{R}^2$, then we know that there exists a unique linear mapping $\sigma \in SL(2,\mathbf{R})$ such that

$$\sigma(x,y) = (x',y'), \quad T_{\tilde{\sigma}}(f) = \zeta f'$$

holds where $\check{\sigma}$ denotes the contragredient automorphism of σ and $\zeta \in \mathbf{U}$. Consider the rotation $\sigma \in SO(2,\mathbf{R})$ given by the matrix

$$\sigma = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \qquad (\theta \in \mathbf{R}).$$

Then of course $\check{\sigma} = \sigma$. Let $\mathfrak{sl}(2,\mathbf{R})$ denote the Lie algebra of $SL(2,\mathbf{R})$ given by the matrices

$$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \, a+d = 0, \; a,b,c,d \in \mathbf{R} \right\}$$

and identify the Lie algebra of $Mp(1,\mathbf{R})$ with $\mathfrak{sl}(2,\mathbf{R})$. Moreover, let Exp denote the exponential mapping of $\mathfrak{sl}(2,\mathbf{R})$ into $Mp(1,\mathbf{R})$. If we look at the special element

$$J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

of $\mathfrak{sl}(2,\mathbf{R})$ then it is easy to check that

$$\tilde{\sigma} = \operatorname{Exp}(-\theta J)$$

is an appropriate choice. Thus in order to identify the states $f \in \mathscr{S}(\mathbf{R})$ which give rise to radially symmetric Wigner quasi-probability distribution functions $P(f;.,.)$ on the real phase plane $\mathbf{R}^2$ it will be necessary and sufficient to determine a Hilbert basis of $L^2(\mathbf{R})$ the elements of which belong to the space $\mathscr{S}(\mathbf{R})$ and form simultaneously eigenfunctions of the linear operators $T_{\operatorname{Exp}(-\theta J)}$ for all $\theta \in \mathbf{R}$.

Let $\{X,Y\}$ be the elements of the Lie algebra $\mathfrak{n}$ of $\tilde{A}(\mathbf{R})$ such that

$$\exp(pX) = (p,0,0), \quad \exp(qY) = (0,q,0)$$

for $p \in \mathbf{R}$, $q \in \mathbf{R}$. Then $X \in \log \mathbf{R}$ and $Y \in \log \mathbf{R}$, and $\{X,Y\}$ forms a basis for $W = \log \mathbf{R} \oplus \log \mathbf{R}$. We will use the coordinates (p,q) relative to this basis to coordinatize the vector subspace W of $\mathfrak{n}$. Notice that $\exp W$ forms the isotropic cross-section to the center Z in the real Heisenberg nilpotent group $\tilde{A}(\mathbf{R})$ (cf. Howe [2]) which lies at the basis of the Bargmann-Fock-Segal model (or complex wave model). If U denotes again the differentiated form of the linear Schrödinger representation U of $\tilde{A}(\mathbf{R})$ acting on $L^2(\mathbf{R})$ then we find that

$$U(X) = -\frac{d}{dx}, \quad U(Y) = 2\pi i x$$

holds. Put

$$Z^- = \frac{1}{2}(X+iY)$$

and

$$Z^+ = \frac{1}{2}(X-iY).$$

Then we get the linear differential operators

$$a^- := U(Z^-) = -{}^1/_2\left(\frac{d}{dx} + 2\pi x\right)$$

and

$$a^+ := U(Z^+) = -{}^1/_2\left(\frac{d}{dx} - 2\pi x\right).$$

as the boson annihilation and creation operators, respectively (cf. Cartier [1]). It is easy to check that the following identities

$$T_{\mathrm{Exp}(\theta J)} a^+ T_{\mathrm{Exp}(-\theta J)} = \zeta_\theta a^+$$

and

$$T_{\mathrm{Exp}(\theta J)} a^- T_{\mathrm{Exp}(-\theta J)} = \bar{\zeta}_\theta a^-$$

hold on the Schwartz-Bruhat space $\mathscr{S}(\mathbf{R})$ of smooth vectors for U where $\theta \in \mathbf{R}$ and $\zeta_\theta \in \mathbf{U}$. If we set

$$W_0 : x \longrightarrow 2^{n/4} e^{-\pi x^2}$$

then the Gaussian $W_0 \in \mathscr{S}(\mathbf{R})$ is a unit vector in the complex Hilbert space $L^2(\mathbf{R})$ and we have

$$T_{\mathrm{Exp}(\theta J)} W_0 = \eta_\theta W_0$$

where $\eta_\theta \in \mathbf{U}$. Obviously

$$a^-(W_0) = 0.$$

The irreducibility of the linear Schrödinger representation U of $\tilde{A}(\mathbf{R})$ implies the well-known fact that the family $(W_m)_{m \geq 0}$ of Hermite-Weber functions (harmonic oscillator wave functions) given by the formulae

$$W_m = \left(\sqrt{\pi^m m!}\right)^{-1} (a^+)^m W_0 \quad (m \in \mathbf{N})$$

forms a Hilbert basis of $L^2(\mathbf{R})$. By inspection of the identities we have derived and in view of the preceding remarks our results are summarized in the following

Theorem 1. Suppose that $f \in \mathscr{S}(\mathbf{R})$, $\|f\| = 1$, and that the identity

$$P(f;x,y) = P(f;-y,x)$$

holds for all pairs $(x,y) \in \mathbf{R}^2$. Then the state f admits the form

$$f = \zeta W_m$$

for certain numbers $m \in \mathbf{N}$ and $\zeta \in \mathbf{U}$, i.e., f is up to a phase factor a harmonic oscillator wave function.

Let us now revert to the radar autoambiguity function

$$H(f;.,.) = \overline{\mathscr{F}}_{\mathbf{R}^2} P(f;.,.),$$

with respect to the signal envelope $f \in \mathscr{S}(\mathbf{R})$, $\|f\|=1$, which is the Fourier cotransform of the Wigner quasi-probability distribution function with respect to the state f. If we denote by $f \otimes \bar{f}$ the dyadic tensor product of f with $\bar{f}$, to wit, the $\mathbf{C}$-linear operator $g \longrightarrow \langle g|f\rangle f$ of trace class in $\mathscr{S}(\mathbf{R})$ with trace given by

$$\mathrm{tr}(f \otimes \bar{f}) = \langle f|f\rangle$$

(cf. Schatten [4]), the notion of U-trace enables us to establish the identity

$$H(f;p,q) = \mathrm{tr}_U(f \otimes \bar{f})\left(\begin{pmatrix} p \\ q \end{pmatrix},0\right)$$

for all pairs $(p,q) \in \mathbf{R}^2$. Thus we obtain

$$\begin{aligned} H(W_m;p,q) &= \langle e^{U(pX+qY)} W_m | W_m \rangle \\ &= (\sqrt{\pi^m m!})^{-1} \langle e^{U(pX+qY)} (a^+)^m W_0 | W_m \rangle \end{aligned}$$

for all $m \in \mathbf{N}$. Let $\tilde{\delta}$ denote the right regular representation of $\tilde{A}(\mathbf{R})$ on $L^2(\tilde{A}(\mathbf{R})/Z)$ transferred to $L^2(W)$ in the natural way by the extension of the isomorphism $\mathscr{S}(\tilde{A}(\mathbf{R})/Z) \rightarrow \mathscr{S}(W)$ associated with the isotropic cross-section to the center Z. Then we obtain for $H(W_m;.,.)$, considered as a function on W, the expression

$$H(W_m;p,q) = (\sqrt{\pi^m m!})^{-1} \tilde{\delta}(Z^+)^m \langle e^{U(pX+qY)} W_0 | W_m \rangle.$$

In view of the identity (cf. Howe [2])

$$\langle e^{U(pX+qY)} W_0 | W_m \rangle = \sqrt{\pi^m/m!}\,(p-iq)^m e^{-(\pi/2)(p^2+q^2)}$$

we obtain

$$H(W_m;p,q) = (1/m!)\tilde{\delta}(Z^+)^m(p-iq)^m e^{-(\pi/2)(p^2+q^2)}.$$

Observe that

$$\tilde{\delta}(X) = \frac{\partial}{\partial p} + \pi iq, \quad \tilde{\delta}(Y) = \frac{\partial}{\partial q} - \pi ip$$

and therefore

$$\begin{aligned}\tilde{\delta}(Z^+) &= (1/2)(\frac{\partial}{\partial p} - i\frac{\partial}{\partial q}) - (\pi/2)(p-iq)\\ &= \frac{1}{2}e^{(\pi/2)(p^2+q^2)}(\frac{\partial}{\partial p} - i\frac{\partial}{\partial q})e^{-(\pi/2)(p^2+q^2)}.\end{aligned}$$

Then we get our final result (cf. Wilcox [10])

$$\begin{aligned}H(W_m;p,q) &= e^{-(\pi/2)(p^2+q^2)}\sum_{0\leq j\leq m}\binom{m}{j}\frac{(-\pi(p^2+q^2))^j}{j!}\\ &= L_m(\pi(p^2+q^2)),\end{aligned} \qquad (m \in \mathbf{N})$$

where L_m denotes the mth Hermite-Laguerre function (= Gaussian× Laguerre polynomial of degree m). Thus we established

Theorem 2. The radar autoambiguity function with respect to the harmonic oscillator wave function W_m as signal envelope admits the form

$$H(W_m;p,q) = L_m(\pi(p^2+q^2)) \qquad (m \in \mathbf{N}).$$

For some related computations see Peetre [3]. This paper however does not indicate any application to the theory of radar detection nor to the Wigner quasi-probability distribution function whereas Wilcox's paper cited above ignores completely the group-theoretical aspects of the radar autoambiguity function.

The same representation-theoretical method which is based on the isotropic cross-section exp W to the center Z in $\tilde{A}(\mathbf{R})$ furnishes for the mixed radar ambiguity function (or radar cross-ambiguity function) with respect to the harmonic oscillator wave functions

$$H(W_m,W_n;p,q) = \mathrm{tr}_U(W_m \otimes \overline{W}_n)(\binom{p}{q},0) \qquad ((m,n) \in \mathbf{N}\times\mathbf{N})$$

the expression

$$H(W_m,W_n;p,q) = \left(\sqrt{\pi^{m+n}/m!n!}\right)e^{-(\pi/2)(p^2+q^2)}(p-iq)^m(-(p+iq))^n \times \sum_{0\leq j\leq \inf(m,n)} \frac{m!}{(m-j)!}\binom{n}{j}(-\pi(p^2+q^2))^{-j}$$

for all pairs $(p,q) \in \mathbf{R}^2$. The fact that the linear Schrödinger representation U of the real Heisenberg group $\tilde{A}(\mathbf{R})$ is square-integrable mod Z implies that the family $(H(W_m,W_n;\cdot,\cdot))_{(m,n)\in \mathbf{N}\times\mathbf{N}}$ forms a Hilbert basis of $L^2(\mathbf{R}^2)$. Therefore we may conclude from this formula again that the functions $(p,q) \longrightarrow H(f;p,q)$ and $(x,y) \longrightarrow P(f;x,y)$ are radially symmetric if and only if $f = \zeta W_m$ for certain numbers $m \in \mathbf{N}$ and $\zeta \in \mathbf{U}$ (cf. [6]).

References

1. Cartier, P.: Quantum mechanical commutation relations and theta functions. In: Algebraic groups and discontinuous subgroups. Proc. Sympos. Pure Math. IX, pp. 361 - 383. Providence, R.I.: Amer. Math. Soc. 1966
2. Howe, R.: Quantum mechanics and partial differential equations. J. Funct. Anal. 38 (1980), 188 - 254
3. Peetre, J.: The Weyl transform and Laguerre polynomials. Matematiche (Catania) 27 (1972), 301 - 323
4. Schatten, R.: Norm ideals of completely continuous operators. Ergebnisse der Mathematik und ihrer Grenzgebiete, Neue Folge, Heft 27. Berlin-Göttingen-Heidelberg: Springer 1960
5. Schempp, W.: Radar reception and nilpotent harmonic analysis I. C.R. Math. Rep. Acad. Sci. Canada 4 (1982), 43 - 48
6. Schempp, W.: Radar reception and nilpotent harmonic analysis II. C.R. Math. Rep. Acad. Sci. Canada 4 (1982), 139 - 144
7. Schempp, W.: Radar reception and nilpotent harmonic analysis III. C.R. Math. Rep. Acad. Sci. Canada 4 (1982), 219 - 224
8. Schempp, W.: On the Wigner quasi-probability distribution function I. C.R. Math. Rep. Acad. Sci. Canada (to appear)
9. Schempp, W.: On the Wigner quasi-probability distribution function II. C.R. Math. Rep. Acad. Sci. Canada (to appear)
10. Wilcox, C.H.: The synthesis problem for radar ambiguity functions. MRC Technical Summary Report, no. 157. Mathematics Research Center, The University of Wisconsin, Madison, Wisconsin 1960

Lehrstuhl für Mathematik I
Universität Siegen
Hölderlinstrasse 3
D-5900 Siegen
Federal Republic of Germany

Received December 1, 1982

C.R. Math. Rep. Acad. Sci. Canada - Vol. V, No.1, February 1983 Février

THE THEORY OF ∀∃ ELEMENTARY CONDITIONS ON RINGS

John Lawrence

Presented by P. Ribenboim, F.R.S.C.

ABSTRACT: In his book [5], L. Rowen mentions that a natural continuation of the work already done on polynomial identities and their generations in ring theory would be a systematic study of ∀∃ elementary conditions on rings. In this paper we announce some results in this direction.

An AEC sentence is one of the form

$$P:\ \forall x_1 \ldots x_m \exists y_1 \ldots y_n [\bigwedge_k E_k(x_1,\ldots,x_m,y_1,\ldots,y_n) = 0],$$

where $E_k(x_1,\ldots,y_n)$ is a polynomial in the language of rings. If R is a ring in which the sentence P holds, for each m-tuple $(a_1,\ldots,a_m)$ of elements of R, choose an n-tuple of elements such that

$$\bigwedge_k E_k(a_1,\ldots,a_m,\psi_1(a_1,\ldots,a_m),\ldots,\psi_n(a_1,\ldots,a_m)) = 0.$$

Now the functions $\psi_i(x_1,\ldots,x_m)$ are m-ary operations which satisfy the identities

$$\bigwedge_k E_k(x_1,\ldots,x_m,\psi_1(x_1,\ldots,x_m),\ldots,\psi_n(x_1,\ldots,x_m)) = 0.$$

These new operations on R are called Skolem operations and the algebra obtained by adjoining these operations to R is denoted by $(R,\vec{\psi})$.

The class of rings defined by AEC sentence is a Skolem class if the class has free rings. Thus, for each set X there is a ring

$\mathbb{F}(X)$ in the class and a set embedding $\phi: X \to \mathbb{F}(X)$ such that given a ring R in the class and a set map $\alpha: X \to R$, there is a unique ring morphism $\beta: \mathbb{F}(X) \to R$ such that $\alpha = \beta \circ \phi$.

Theorem A[2]. For the class C of rings defined by an AEC sentence P, the following are equivalent.

1) C is a Skolem class.
2) For each ring R in C there is a set of Skolem operations $\vec{\psi}_R$ such that each ring morphism $\gamma: R \to T$ is an algebra morphism $\gamma: (R,\vec{\psi}_R) \to (T,\vec{\psi}_T)$. The algebras $\{(R,\vec{\psi}_R)\}$ form a variety.

The above theorem enables us to prove several results about Skolem classes: a Skolem class is closed under direct and inverse limit, intersection, and equalizers of pairs of maps. If a ring R is in a Skolem class, e is an idempotent in R and $2a = 0$ implies $a = 0$ in R, then the ring eRe is in the Skolem class. A rather weak structure theorem for primitive rings in non-trivial Skolem classes is also proved. This, of course, is motivated by Kaplansky's theorem on primitive rings in non-trivial varieties of rings.

An example of a Skolem class is the class C of strongly regular rings, defined by $\forall x \exists y [x^2 y = x]$. Let R be a strongly regular ring and let $V_C(R)$ stand for the class of rings which are homomorphic images of strongly regular subrings of direct products of copies of R. This is a subvariety of the variety of strongly regular rings. In particular, if D and D' are division rings, then $V_C(D') \subset V_C(D)$ if and only if D' satisfies all strongly regular identities satisfied by D. This happens if and only if D' is a subring of an ultrapower of D. The rational identities studied by S. Amitsur and G. Bergman can be considered (in a natural way) as a subset of the strongly regular identities.

Not all classes of rings defined by AEC sentences are Skolem classes; indeed R. Raphael proved that the class of von Neumann regular rings, defined by $\forall x \exists y[xyx = x]$, is not a Skolem class.

Let P be an AEC sentence and let S be a set of rings in which the sentence P holds. Denote by $V(S,P)$ the variety of algebras generated by $\{(R,\vec{\psi})\}$, where R goes over all rings in S and $\vec{\psi}$ goes over all possible Skolem operations. If R is a ring and $V(\{R\},P) \subset V(S,P)$, we say that the ring R is in the variety $V(S,P)$.

Theorem B [3]. 1. *If* $T \in V(S,P)$ *and* R *is a subring of* T *in which* P *holds, then* $R \in V(S,P)$.

2. *If the direct product of rings* $R \times T \in V(S,P)$, *then* $R \in V(S,P)$.

3. *If* $\prod_{i \in I} R_i$ *is a direct product of rings indexed by* I *and for every finite subset* $U \subset I$ *we have* $\prod_{i \in U} R_i \in V(S,P)$, *then* $\prod_{i \in I} R_i \in V(S,P)$.

Let F be a field and let $M_n(F)$ be the $n \times n$ matrix ring over F. If P is an AEC sentence, define

$$S(P) = \{M_n(F): P \text{ holds in } M_n(F)\}.$$

In [4], we do some work in characterizing the set $S(P)$ when F is field of rational numbers.

Theorem C [4]. *If $S(P)$ is infinite, then every subring of a direct product of copies of rings in $S(P)$ in which P holds, is in* $V(S(P),P)$.

If X is a set, then $\mathbb{F}(S,P,X)$ stands for the free algebra in $V(S,P)$ generated by the set X.

Theorem D [4]. *If $S(P)$ is infinite and X is an infinite set, then* $\mathbb{F}(S(P),P,X)$ *is prime* (as a ring).

Theorem E [4]. *Suppose that P is an AEC sentence such that* $S(P)$ *is infinite, Q is a positive sentence and there is a subring of a direct product of copies of rings in $S(P)$ in which $P \wedge \sim Q$ holds. Then there is a prime ring which is a subdirect product of rings in $S(P)$ in which* $P \wedge \sim Q$ *holds.*

K. Goodearl has asked whether a regular subdirect product of simple Artinian rings is unit regular [1]. Let us look at this problem in the special case where the simple Artinian rings are matrix rings over a fixed field F. The sentence P is now the defining sentence for von Neumann regularity. Goodearl's question has an affirmative answer if and only if the ring $\mathbb{F}(S(P),P,\{x\})$ is unit regular. If this ring is unit regular, then the element x has a unit quasi-inverse which is a polynomial $p(x)$ in one variable x and the regular ring operations. Recently G. Sinnamon discovered a polynomial $p_2(x)$ which defines a unit quasi-inverse for 2×2 matrices.

References

[1] K. Goodearl, Von Neumann Regular Rings, Pitman (1979).

[2] J. Lawrence, Skolem categories of rings.

[3] __________, Generic rings defined by first order sentences.

[4] __________, Universal-existential setences and matrix rings.

[5] L. Rowen, Polynomial Identities in Ring Theory, Academic Press (1980).

Department of Pure Mathematics
University of Waterloo
Waterloo, Ontario
Canada, N2L 3G1

Received December 11, 1982

C.R. Math. Rep. Acad. Sci. Canada - Vol. V, No.1, February 1983 Février

GENERALIZED BÄCKSTRÖM-ORDERS OF FINITE TYPE

K.W. Roggenkamp

Presented by P. Ribenboim, F.R.S.C.

Let R be a complete Dedekind domain with field of fractions K and A a finite dimensional separable K-algebra. An R-order Λ in A is said to be a generalized Bäckström-order provided there exists a hereditary R-order Γ with $\operatorname{rad}\Gamma \subset \Lambda \subset \Gamma$, and if P is an indecomposable projective Λ-lattice, then $\operatorname{rad}_\Lambda P = Q \oplus X$, where Q is a projective Λ-lattice and X is a Γ-lattice.

It is clear that this generalizes Bäckström-orders [RR1], in fact whereas Bäckström-orders are the integral analogue of radical-square-zero algebras, generalized Bäckström-orders correspond to hereditary algebras [R]. We next associate a valued graph γ to (Λ, Γ). Let $\{P_i\}_{1\leq i\leq n}$ be the non-isomorphic indecomposable projective Λ-lattices and $\{X_j\}_{1\leq j\leq m}$ the non-isomorphic indecomposable Γ-lattices. The vertices γ_0 of γ are labelled $\{p_i, x_j, 1\leq i\leq n, 1\leq j\leq m\}$. We draw an arrow $p_i \to p_i'$ provided P_i is not a Γ-lattice and P_i is a direct summand of $\operatorname{rad}_\Lambda P_i'$ with multiplicity n_i. For an indecomposable Λ-lattice Y we write $\mathfrak{f}(Y) = \operatorname{End}_\Lambda(Y)/\operatorname{rad}\operatorname{End}_\Lambda(Y)$. The valuation on the edge $p_i \to p_i'$ $(d_{i,i'}, d'_{i,i'})$ is given by

$$d'_{i,i'} = n_i$$

$$d_{i,i'} = \dim_{\mathfrak{f}(P_i')}(\mathfrak{f}(P_i)^{n_i}) .$$

We draw an edge $x_j \to p_i$ provided X_j is a direct summand of $\operatorname{rad}_\Lambda P_i$. The valuation is defined as above.

We say that γ is <u>contractible</u>, if the dual valued oriented graph is reducible in the sense of [RR2].

Theorem I: Let Λ be generalized Bäckström-order with hereditary order Γ, and associated valued oriented graph γ. Λ has a finite number of non-isomorphic indecomposable lattices if and only if γ can be contracted to a disjoint union of Dynkin graphs.

The number of indecomposable Λ-lattices - in case this number is finite - can be computed as follows. For the sake of simplicity we assume the valuation to be (1,1) on each edge (the general case is treated in [R]) for each source j_o in γ_o we define the function

$$f_{j_o}: \gamma_o \to \mathbb{N}$$

by $f(i) = 1$ if there is an oriented path from j_o to i and $f(i) = 0$ otherwise. Let now

$$f_o = \sum_{j_o \text{ source}} f_{j_o} .$$

We then form the Riedtmann quiver $\mathbb{Z}_\gamma$ [Ri] and extend f_o to a function

$$f : \mathbb{Z}_\gamma \to \mathbb{N}$$

as follows. We define it inductively as additive extension of f_o [HPR] except that we place zero's on (i,n) for $n \geq n_o$ provided $f(i,n_o-1) > 0$ but $f(i,n_o) < 0$.

Theorem II: If Λ is a generalized Bäckström-order, then f has finite support, and the non-isomorphic indecomposable Λ-lattices M are in bijection with the points $(i,n) \in \mathbb{Z}_\gamma$ such that $f(i,n) > 0$ except for the points (i,o), where i is a source in γ. In that case $f(i,n)$ determines the number of indecomposable Γ-lattices into which ΓM decomposes.

Remark: If Λ is a generalized Bäckström-order of finite lattice type, then the Auslander-Reiten quiver of Λ [R1] can be computed inductively by starting with the lattices $\{X_j, P_i,\ 1\le j\le m,\ 1\le i\le n\}$ If $\mathfrak{k}$ is the residue field of R and $\mathfrak{A}$ is the $\mathfrak{k}$-tensor algebra of γ, let S be the category of $\mathfrak{A}$-modules which have a projective socle. Then the Auslander-Reiten quiver $\mathfrak{A}_S$ of S is simply connected. There exists a covering

$$\rho:\ \mathfrak{A}_S \to \mathfrak{A}_\Lambda$$

where $\mathfrak{A}_\Lambda$ is the Auslander-Reiten quiver of Λ. In such a way that $|\rho^{-1}(M)| = 1$ if M is not a Γ-lattice and $|\rho^{-1}(X_j)| = 2$. $1\le j\le m$.

References:

[HPR] Happel,D. - U.Preiser - C.M.Ringel: "Vinberg's characterization of Dynkin diagrams using subadditive functions". Representation Theory II, Springer LN 832 (1980),280-294.

[Ri] Riedtmann,C.: "Algebren, Darstellungsköcher, Überlagerungen und zurück". Com.Helv. 55 (1980), 199-224.

[RR1] Ringel,C.M. - K.W.Roggenkamp: "Diagrammatic methods in the representation theory of orders". J.of Algebra, Vol.60, Nr.1 (1979), 11-42.

[RR2] Ringel,C.M. - K.W.Roggenkamp: "Socle determined categories of representations of artinian hereditary tensor algebras". J.of Algebra, Vol.64, Nr.1 (1980), 249-269.

[R1] Roggenkamp,K.W.: "Generalized Bäckström-orders of finite type and their Auslander-Reiten species". Preprint I,II,III.

Pfaffenwaldring 57
D-7000 Stuttgart
W. Germany

Received December 15, 1982

C.R. Math. Rep. Acad. Sci. Canada - Vol. V, No.1, February 1983 Février

AUSLANDER-REITEN QUIVERS FOR SOME TORSION THEORIES OF HEREDITARY ALGEBRAS

K.W. Roggenkamp

Presented by P. Ribenboim, F.R.S.C.

Let $\mathfrak{k}$ be a field and A a connected finite dimensional hereditary $\mathfrak{k}$-algebra. By S we denote the full subcategory of A-mod having as objects modules with a projective socle. Let Γ be the valued oriented graph of A [DRS]. Γ is said to be contractible, if the dual graph is reducible in the sense of [RR], where it was shown that S is of finite module type if and only if Γ is contractible to a valued Dynkin graph. The aim of this note is to describe the Auslander-Reiten quiver $\mathfrak{A}(S)$ of S in case S is of finite type. We assume from now on that Γ is a valued oriented tree. Let P be the direct sum of the non-isomorphic maximal projective A-modules. We define the function - Γ_o are the vertices -

$$f_o : \Gamma_o \to \mathbb{N}$$

$$i \mapsto n_i \quad \text{if } S_i, \text{ the simple}$$

A-module corresponding to i, occurs n_i times as composition factor in P. Let $\mathbb{Z}\Gamma$ be the valued Riedtmann quiver constructed from Γ [HPR]. We then define the disturbed additive function

$$f : \mathbb{Z}\Gamma_o \to \mathbb{N}$$

as follows. It is inductively defined as additive extension of f_o on $\Gamma_o = \{(i,o)\}$ except we place zero's on (i,n) for $n \geq n_o$ provided $f(i,n_o-1) > 0$ but $f(i,n_o) \leq 0$. It follows from [AS] that S has left and right Auslander-Reiten sequences.

Theorem: (i) S is of finite type iff f has finite support, iff Γ can be contracted to a Dynkin diagram.

(ii) If $\mathcal{S}$ is of finite type, then $\mathfrak{A}(\mathcal{S})$ is simply connected, and all modules are in the Auslander-Reiten orbits in $\mathcal{S}$ of the projective modules in modA.

(iii) There is a bijection between the indecomposable modules in $\mathcal{S}$ and the vertices (i,n) with $f(i,n) \neq 0$. If M corresponds to (i,n) then $f(i,n)$ is the number of simple summands in the socle of M.

(iv) Under the identification in (ii) the Auslander-Reiten quiver of $\mathcal{S}$ is the full subquiver of $\mathbb{Z}\Gamma$ consisting of the points (i,n) with $f(i,n) > 0$.

Proposition: *If A is arbitrary then Brauer-Thrall I holds for* $\mathcal{S}$.

The proofs will appear in [R]; they use a detailed study of Auslander-Reiten sequences in $\mathcal{S}$.

Remarks: 1.) Let A be artinian and $(\mathfrak{T},\mathfrak{F})$ a torsion theory in A-mod then both for $\mathfrak{T}$ and for $\mathfrak{F}$ Brauer Thrall I holds in a suitable formulation.

2.) If $\mathfrak{T}$ $(\mathfrak{F})$ have Auslander-Reiten sequences then for sections in the stable Auslander-Reiten quiver, the question whether they can be contracted to Dynkin graphs plays a similar rôle for finitenessquestions as do the Dynkin diagrams for A-mod (à la Riedtmann). The subadditive functions must be replaced by disturbed subadditive functions.

References

[AS] Auslander, M. - S.O.Smalø: Almost split sequences in subcategories.
J.of Algebra, to appear.

[DRS] Dowbor, P. - C.M.Ringel - D.Simson: Hereditary artinian rings of finite representation type.
Representation Theory II, Springer Lecture Notes 832 (1980), 232-241.

[HPR] Happel, D. - U.Preiser - C.M.Ringel: Vinberg's characterization of Dynkin diagrams using subadditive functions.
Representation Theory II, Springer Lecture Notes 832 (1980), 280-294.

[Ri] Riedtmann, C.: Algebren, Darstellungsköcher, Überlagerungen und zurück.
Com.Helvet. 55 (1980), 199-224.

[RR] Ringel, C.M. - K.W.Roggenkamp: Socle-determined categories of representations of artinian hereditary tensor algebras.
J.of Algebra 64 (1980), 249-269.

[R] Roggenkamp, K.W.: Generalized Bäckström orders of finite type and their Auslander-Reiten quivers I,II,III.
Preprint (1982).

Pfaffenwaldring 57
D-7000 Stuttgart
W. Germany

Received December 15, 1982

C.R. Math. Rep. Acad. Sci. Canada - Vol. V, No.1, February 1983 Février

INCOMPLETE RESIDUE SYSTEMS TO A COMPOSITE MODULUS

J.H.H. Chalk, F.R.S.C.

1. Let $k \geq 2$ denote the modulus and write $k = \ell k_*$, where k_* is the square-free part of k. Define

(1) $$C = C_k = \{\underline{x} = (x_1, x_2, \ldots, x_N) \in \mathbb{Z}^N : 0 \leq x_i < k \quad (1 \leq i \leq N)\}$$

and let $\phi : \mathbb{Z}^N \longrightarrow C$ be a mapping of the standard lattice $\mathbb{Z}^N$ into the complex field $\mathbb{C}$. Let

(2) $$F(\underline{z}) = \sum_{\underline{x} \in C} \phi(\underline{x}) e(\underline{z}.\underline{x}), \qquad (\underline{z} \in \mathbb{Z}^N)$$

where $e(t) = e_k(t) = \exp(2\pi it/k)$ and $\underline{z}.\underline{x}$ denotes the usual Euclidean inner product. Since

(3) $$\sum_{\underline{x} \in C} e(\underline{x}.\underline{y}) = \begin{cases} k^N, & \text{if } \underline{y} \equiv \underline{0} \pmod{k} \\ 0, & \text{otherwise} \end{cases}$$

we have, in particular,

$$\phi(\underline{x}) = k^{-N} \sum_{\underline{z} \in C} F(\underline{z}) e(-\underline{y}.\underline{z})$$

and so $F(\underline{z})$ may be viewed as a Fourier coefficient for $\phi(\underline{x})$, relative to the modulus k. We also define

(5) $$\Phi(C) = \max_{\underline{0} \neq \underline{z} \in C} |F(\underline{z})|,$$

and for convenience of notation, appropriate the modulus sign $|.|$ for another purpose, denoting

$$|S| = \mathrm{card}(S \cap \mathbb{Z}^N)$$

for any bounded subset S of $\mathbb{R}^N$. If S is a subset of $\mathbb{Z}^N$, a general question on incomplete residue systems mod k is that of estimating the difference between a given sum of the form

$$\sum_{\underline{x}\in S} \phi(\underline{x}) \tag{7}$$

and the proportion

$$|S|\,|C|^{-1} \sum_{\underline{x}\in C} \phi(\underline{x}) \tag{8}$$

of the complete sum mod k, which may be 'expected' to approximate it if the values of ϕ are sufficiently well distributed throughout C. Note that it is not necessary to restrict S to be a subset of C and indeed this is useful if certain residue classes in the sum (7) are to be counted with multiplicity. The inequalities of Vinogradov and of Mordell, which are closely related (see [1] for references and a brief survey of their work), provide a bound for

$$L_1(S,\phi) = \sum_{\underline{x}\in S} \phi(\underline{x}) - |S|\,|C|^{-1} \sum_{\underline{x}\in C} \phi(\underline{x}) \tag{9}$$

in the shape*

$$L_1(S,\phi) << \Phi(C)E_1(S)|C|^{-1}, \tag{10}$$

where

$$E_1(S) = \sum_{\underline{0}\neq\underline{z}\in C} \left|\sum_{\underline{y}\in S} e(\underline{z},\underline{y})\right| \tag{11}$$

---

* Here, as elsewhere, the implied constant in the Vinogradov symbol "<<" is absolute.

is a special type of exponential sum $\bmod k$, independent of the choice of ϕ. It is easy to estimate $E_1(S)$ with precision in the special case when $S = B$ is a "box" of the type

(12) $B = \{\underline{x} : a_i \le x_i \le a_i + h_i, \ (h_i > 0, \ 1 \le i \le N)\}$

but not, to my knowledge, in any other essentially different case. In fact (cf. [2], §3),

$$E_1(B) << |C| \log^N |C| . \tag{13}$$

On comparing the terms in (9) and (10) and using (13), we see that, if $\Phi(C)$ is of lower order of magnitude than the complete sum $\sum_{\underline{x} \in C} \phi(\underline{x})$ as $k \to \infty$, then the main term (8) in the asymptotic formula (10) dominates the error term (on the right of (10)). In applications, $\phi(\underline{x})$ is usually a counting function for solutions of a given polynomial congruence

$$f(\underline{x}) \equiv 0 \pmod{k}, \tag{14}$$

where $f \in Z[\underline{x}]$, e.g.

$$\phi(\underline{x}) = k^{-1} \sum_{t=1}^{k} e\big(tf(\underline{x})\big) = \begin{cases} 1, & \text{if } f(\underline{x}) \equiv 0 \pmod{k}, \\ 0, & \text{otherwise,} \end{cases} \tag{15}$$

and, indeed, for k prime and for a wide class C of polynomials f our knowledge of exponential sums to a prime modulus k have produced such estimates for $\Phi(C)$, (cf. [1] for references). Thus, for $S = B$, $f \in C$ and k a sufficiently large prime we know that the solutions $\underline{x} \bmod k$ of (14) are in a certain sense distributed uniformly throughout C.

At this stage it is appropriate to mention the work of Tietäväinen [5], who circumvented the difficulties of estimating $E_1(S)$ when S is not of the type in (12) by introducing a *weighted* counting function. Thus he considered

$$L_2(S,\phi) = |S|^{-1} \sum_{\underline{x}\in S, \underline{y}\in S} \phi(\underline{x}+\underline{y}) - |S||C|^{-1} \sum_{\underline{x}\in C} \phi(\underline{x}) \tag{16}$$

in place of $L_1(S,\phi)$ and obtained a bound of the form

$$L_2(S,\phi) << \Phi(C)E_2(S)|C|^{-1}|S|^{-1} , \tag{17}$$

where

$$E_2(S) = \sum_{\underline{0}\neq\underline{z}\in C} \left| \sum_{\underline{y}\in S} e(\underline{z}.\underline{y}) \right|^2 . \tag{18}$$

Now, the exact value of $E_2(S)$ is easy to compute in the case $S \subset C$; in fact

$$E_2(S) = |C||S| - |S|^2 \quad (S \subset C) \tag{19}$$

and the estimate

$$E_2(S) << |S|(|S+C| - |S|) \quad (S \not\subset C) \tag{20}$$

for the remaining case is straightforward (cf. [1], §4).

In an article (to be published in the Indagationes), I have provided explicit estimates valid for arbitrary modulus k (sufficiently large) and for polynomial congruences (14) where f is restricted to satisfy mild conditions of non-degeneracy, viz.,

(A) $f(\underline{x})$ has no singular zeros in the finite field $\mathbb{F}_p$, for each $p \mid k$.

(B) $f(\underline{x})$ has no linear factors in $\mathbb{F}_p[\underline{x}]$, for each $p \mid k$.

The main results are contained in the following theorem, the proof of which incorporates a refinement of Tietäväinen's argument:

<u>THEOREM</u>. (k <u>odd</u>). <u>Suppose</u> $f \in \mathbb{Z}[\underline{x}]$ <u>satisfies</u> (A) <u>and</u> (B). <u>Then</u>

(i) $L_2(S,\phi) \ll k^{-1} k_*^{2N-5/2}$, $(S \subset C_{k^*})$,

(ii) $L_2(S,\phi) \ll k^{-1} k_*^{N-5/2} \left(|S + C_{k_*}| - |S|\right)$, $(S \not\subset C_{k_*})$.

As an application, we consider an example with $N = 2$, where the modulus k is arbitrary and S is not restricted to be a subset of C: let

$$f(\underline{x}) = x_1^2 + x_2^2 - a, \quad (a,k) = 1, \tag{21}$$

$$S = \{\underline{x} \in \mathbb{Z}^2 : x_1^2 + x_2^2 \le X, \quad x_1 > 0, \quad x_2 > 0\}. \tag{22}$$

This is the 'circle problem in arithmetic progression', for

$$L_1(S,\phi) = \frac{1}{4} \sum_{\substack{n \le X \\ n \equiv a \pmod{k}}} r(n) - \frac{\pi}{4} H_k(a) \frac{X}{k}, \tag{23}$$

where $r(n)$ denotes the number of representations of n as a sum of two squares, $\phi(\underline{x})$ is as defined in (15) and

$$\sum_{\underline{x} \in C} \phi(\underline{x}) = k\, H_k(a) = k \prod_{p \mid k} \left(1 - \chi(p) p^{-1}\right), \tag{24}$$

$\chi(n)$ being the non-principal character mod 4. By a different method based upon analytic techniques, R.A. Smith [3] has proved that, for this example,

$$(25) \qquad L_1(S,\phi) \ll X^{(2/3)+\beta}\, k^{-1/2(1+3\beta)}\, (a,k)^{1/2} d(k) ,$$

for any β with $0 < \beta < 1/3$, provided that

$$X \gg k^{3/2} .$$

This may be compared with the estimate

$$(26) \qquad L_2(S,\phi) \ll \begin{cases} k^{-1}k_*^{3/2} , & \text{if } X \le k_*^2 \\ X^{1/2}k^{-1}k_*^{1/2} , & \text{if } X > k_*^2 \end{cases}$$

given by the theorem. Thus, for k odd and square-free, for example, it is clear that the error terms (on the right of (26)) are sharper for the weighted sums in $L_2(S,\phi)$. However, neither of the estimates (25), (26) has significance when $X \ll k^{3/2}$ and it would be of considerable interest to reduce this handicap. Recently Iwaniec has informed me that one can expect to obtain $x \ll k^{4/3+\varepsilon}$, assuming the validity of Hooley's hypothesis ([3],p.44).

References

1. J.H.H. Chalk, "The Vinogradov-Mordell-Tietäväinen Inequalities", Proc. Kon. Ned. Akad. v. Wet., A, 83 (4), (1980), 367-374.

2. ________, "The Number of Solutions of Congruences in Incomplete Residue Systems", Canad. J. of Math., 15 (1963), 291-296.

3. C. Hooley, "Greatest Prime Factor of a Cubic Polynomial", J. reine Agnew. Math., 303-4 (1978), 21-50.

4. R.A. Smith, "The Circle Problem in Arithmetic Progressions", Canad. Math. Bull., 11, No. 2, (1968), 175-184.

5. A. Tietäväinen, "On the Solvability of Equations in Incomplete Finite Fields", Ann. Univ. Turkuensio, A, 102 (1967), 3-12.

Received January 10, 1983

Department of Mathematics
University of Toronto
Toronto, Ontario, Canada
M5S 1A1

MAILING ADDRESSES

1. J. Borwein
Dept. of Mathematics
Dalhousie University
Halifax, Nova Scotia, Canada B3H 4H8

2. J.H.H. Chalk
Dept. of Mathematics
University of Toronto
Toronto, Ontario, Canada M5S 1A1

3. W.H. Greub
Dept. of Mathematics
University of Toronto
Toronto, Ontario, Canada M5S 1A1

4. J. Lawrence
Dept. of Pure Mathematics
University of Waterloo
Waterloo, Ontario, Canada N2L 3G1

5. B.S. Nashier
Dept. of Mathematics
University of Kentucky
Lexington, KY 40506, U.S.A.

6. B.M. Puttaswamaiah
Dept. of Mathematics
Carleton University
Ottawa, Ontario, Canada K1S 5B6

7. K.W. Roggenkamp
Pfaffenwaldring 57
D-7000 Stuttgart
West Germany

8. W. Schempp
Lehrstuhl für Mathematik I
Universität Siegen
Holderlinstrasse 3
D-5700 Siegen
West Germany

9. B. Sims
Dept. of Mathematics
Dalhousie University
Halifax, Nova Scotia, Canada B3H 4H8

10. P. Volkmann
Ringstr. 6
6729 Neuburg am Rhein
West Germany