[1]

Intertwining operators for $L^2(E)$

Jorge Soto Andrade and Jorge Vargas
Universidad de Chile Casilla 653,
Santiago de Chile, Chile
and FAMAF Universidad Nacional de Córdoba
5000 Córdoba, Argentine

October 30, 2007

Abstract

Let (E, q) be a finite dimensional quadratic vector space over a finite field. For the usual representation of the isometry group of (E, q) in the space of complex valued functions on E, we analyze when the polynomial algebra spanned by one mean average operator is the whole algebra of intertwining operators.

Let F be a finite field with $q = p^n$ elements. (From now on, p is an odd prime number) We fix a $m-$dimensional vector space E over F. We also fix $b : E \times E \to F$ a nondegenerate bilinear symmetric form. We define $Q(x) = b(x, x)$ and $d(x, y) = b(x - y, x - y)$. The sphere of center x and radius r will be denoted by $S_m(x, r)$. We usually will drop the subindex m. As usullay $M_r : L^2(E) \to L^2(E)$ is the mean average operator defined by

$$(M_r f)(x) = \sum_{v \in S(x,r)} f(v) \tag{1}$$

*Supported by CONICYT, Fund. Andes, French Cooperation Office (Chile) and CONICET, CONICOR, SECYTUNC (Argentine)

The purposse of this note is to analyze, for a fix r, whether or not the polynomials in M_r span the algebra of intertwining operators for the left regular representation of the isometry group of b in $L^2(E)$. We recall that the theorem of the intertwining number says the algebra of intertwining operators is linearly spanned by all the M_r. (cf. [M], [Wa])

More precisely:

Theorem 1. a) If $[F : Z_p] > 1$ or $F = Z_p$ and E is odd dimensional then the algebra spanned by a M_r ($r \in F^*$ fixed) is a proper subalgebra of the whole algebra of intertwining operators. This also holds if $p = 3$.
b) If $F = Z_p, p > 3$ and E is even dimensional then the algebra spanned by a M_r is the whole algebra of intertwining operators.

Note: In [Sta] D. Stanton proves that one mean average operator generates the whole intertwining algebra, but his metric is real valued instead of being $F-$valued.

We begin collecting the ingredients necessary for the proof.

We denote by $\Psi : F \to C^*$ the composition of the trace from F to the prime field followed by a generator of the dual group to the additive group of the prime field.

The eigenfunctions of the operator M_r are the functions

$$\varphi_r(y) = \sum_{v \in S(\vec{0}, r)} \Psi(b(v, y)) \tag{2}$$

Actually, φ_r only depends on $s = d(y, \vec{0})$ and not on y itself. From now on, we will write $\varphi_r(s)(s \in F)$ instead of $\varphi_r(y)$.
Let A be a $2-$dimensional asociative algebra over F. Then A is either isomorphic to $F \times F$ or to K the second degree extension of F. In $F \times F$ we consider the hyperbolic form $h = \frac{1}{2}(x_1 y_2 + x_2 y_1)$. Let N denote the associated quadratic form to h. Thus $N(x_1, x_2) = x_1 x_2$. We recall that $Tr : A \to F$ is $Tr(x_1, x_2) = x_1 + x_2$. We will denote by Tr, N the trace and the norm of the field extension K/F. Since the degree of K over F is two, N is the quadratic form of a symmetric bilinear form over F on K. We will denote this symmetric form by N. We recall that the Bessel function attached to the data (A, Tr, N, Ψ) is

$$J_0^A(a) = \sum_{w \in A,\, N(w) = a} \Psi(Tr(w)) \quad (a \in F)$$

Thus, for $A = F \times F$

$$J_0^A(a) = \sum_{x_1 x_2 = a} \Psi(x_1 + x_2) = \sum_{t \in F^*} \Psi(t + \frac{a}{t})$$

For $A = K$

$$J_0^A(a) = \sum_{w \in E,\, N(w) = a} \Psi(w + \bar{w})$$

Here, bar denotes the nontrivial element of the Galois extension K/F.
Up to isomorphism every nondegenerate, even dimensional, quadratic spaces over F is isomorphic to

$$(F^{2(n-1)} \quad \oplus A, \;\; h \oplus \cdots \oplus h \oplus N)$$

For a proof (c.f. [Se]). A lengthly calculation shows that:
Theorem 2.

$$\text{For}\, s \in F^* \quad \varphi_r(s) = \; q^{n-1}\, J_0^A(rs)$$

For a proof (cf [MMST])
Next, we spell out the two cases. $A = F \times F$, hence the quadratic space is

$$(F^{2n}, \;\; h \oplus \cdots \oplus h) \;(n\, \text{times})$$

and

$$\varphi_r(s) = q^{n-1} \sum_{t \in F^*} \Psi(t + \frac{rs}{t}) \tag{He}$$

$A = K$, hence the quadratic space is

$$(F^{2(n-1)} \oplus K, \quad h \oplus \cdots \oplus h \oplus N)$$

and

$$\varphi_r(s) = q^{n-1} \sum_{y \in E,\, y\bar{y} = rs} \Psi(y + \bar{y}) \tag{Ne}$$

We now consider the odd dimensional case. Then (E, q) is equivalent to

$$(F^{2n} \oplus F, \quad h \oplus \cdots \oplus h \oplus a x_0^2\,)$$

Here $a = 1$ or $a \in F^*$ is a nonsquare. For a proof (c.f. [Se].)
Let $\epsilon : F \to C^*$ defined by $\epsilon(0) = 0, \epsilon(F^{*^2}) = 1, \epsilon(x) = -1 \text{for}\, x \notin F^{*^2}$.
A lengthly calculation shows:

Theorem 3.
$$\varphi_r(s) = q^{n-1} G_F \sum_{t\in F^*} \epsilon(\frac{t}{a})\Psi(t + \frac{sr}{t})$$
Here, G_F stands for a Gauss sum associated to F.
For a proof (cf [MMST])
We now begin to study whenever the algebra spanned by a M_r agrees with the whole algebra of intertwining operators for $L^2(E)$. Let $Iso(E)$ be the group of isometries of E with respect to the nondegenerate quadratic form Q. Thus, $Iso(E)$ is the semidirect product of $O(Q, E)$ and E. For a proof consult [Ar]. Let π be the natural representation of $Iso(E)$ in $L^2(E)$. It is clear that M_r belongs to the algebra of intertwining operators for π. Let $\varphi_r(s)$ be the $s-$eigenvalue for M_r $(s \in F)$. (cf. (2))

Lemma 4. The subalgebra spanned by a M_r $(r \neq 0)$ is equal to the algebra of intertwining operators if and only if the function $s \to \varphi_r(s)$ is one to one.

Proof: Since $(Iso(E), O(q, E))$ is a Gelfand pair, $L^2(E)$ decomposes with multiplicity free as $Iso(E)-$module. Also, the structure of the unitary dual to $Iso(E)$ implies that we may write $L^2(E) = \oplus_s V_s$ with V_s an $Iso(E)-$irreducible representation on V_s. Hence, V_s is not equivalent to V_t for $t \neq s$. On V_s, M_r acts by $\varphi_r(s)$. Therefore, the algebra of intertwining operators has dimension q. The algebra of intertwining operators has a basis $e_s = (\delta_{st} id_{V_s})_{t\in F}$, $(s \in F)$. The change of basis matrix to the powers of M_r is the Vandermonde matrix associated to $(\varphi_r(s))_{(s\in F)}$. Hence, the lemma follows.

Lemma 5. For $\sigma \in Gal(F/Z_p)$, $a \in F$ then
$$J_0^{F\times F}(\sigma(a)) = J_0^{F\times F}(a)$$
$$J_0^{K}(\sigma(a)) = J_0^{K}(a)$$
$$\sum_{t\in F^*} \epsilon(\frac{t}{b})\Psi(t + \frac{\sigma(a)}{t}) = \sum_{t\in F^*} \epsilon(\frac{t}{b})\Psi(t + \frac{a}{t})$$
Proof: First of all $\Psi(z) = \Psi_0(Tr(z))$, where Tr is the trace of the field extension F/Z_p and Ψ_0 is a generator for the dual to the additive group of Z_p. Hence, $J_0^{F\times F}(\sigma(a)) = \sum_{t\in F^*} \Psi_0(Tr(t + \frac{\sigma(a)}{t}))$. Now, $\sigma F^* = F^*$, $Tr(\sigma(u)) = Tr(u)$ $u \in F$. Thus, we can make $t = \sigma(s)$, and the first equality follows. The proof of the second equality follows from $N(\sigma(u)) = N(u)$. The third equality follows after we recall that $Gal(F/Z_p)$ is an abelian group.

Next, we prove the first assertion in a) in theorem 1. Since $[F : Z_p] > 1$, the Galois group of F over Z_p is nontrivial. Hence, lemma 5 says that the functions $J_0^{F\times F}$, J_0^K are not one to one. On the other hand multiplication by a nonzero scalar r is a bijection. Thus, theorem 2 says that φ_r is not injective, by lemma 4 we have proved the first statement in part a) of theorem 1. The second statement follows from:

Lemma 6. Let $f(s) = \sum_{v\in Z_p^*} \Psi(v + \frac{s}{v})\epsilon(v)$, then f is not injective.

Proof: For $p = 3$, $f(1) = f(2)$ follows by a direct calculation. For $p > 3$ we prove that $f(a) = f(b)$ for any pair a, b not squares in Z_p.
Indeed, $\Psi(x) = \xi^x$ for a fixed $p-$root of the unity ξ. Let N, S denote the set of nonsquares (squares) in Z_p. Thus $f(s) = \sum_{v\in S} \Psi(v+\frac{s}{v})-\sum_{v\in N} \Psi(v+\frac{s}{v}) = \sum_{k=0}^{p-1} c_k(s)\xi^k - \sum_{k=0}^{p-1} d_k(s)\xi^k = \sum_{k=0}^{p-1}(c_k(s) - d_k(s))\xi^k$. Here,

$$c_k(s) = |\{v \in S : v + \frac{s}{v} = k\}|,\ d_k(s) = |\{v \in N : v + \frac{s}{v} = k\}|$$

Now since a, b are non squares we have that $c_0(a) = c_0(b), \text{and} d_0(a) = d_0(b)$. Next, if v is a solution to $v + \frac{a}{v} = k$ the other solution is $\frac{a}{v}$, hence for a nonsquare a we have that $c_k(a) \in \{0, 1\}$. Besides,

$$\begin{array}{lcl} c_k(a) = 0 & \Longleftrightarrow & d_k(a) = 0 \\ c_k(a) = 1 & \Longleftrightarrow & d_k(a) = 1 \end{array}$$

Hence, for a nonsquare in Z_p we have that $c_k(a) = d_k(a)$ for every $k \in Z_p$. Thus, we have proved lemma 6.
Therefore, theorem 3 says that the second statement en a) of theorem 1 follows.
In order to show part b) of theorem 1 we need some lemmas.
Recall that $K := F[\sqrt{\delta}]$ with $\delta \in F$ a nonsquare. For this case $Tr : K \to Z_p$ is $Tr(x + \sqrt{\delta}y) = 2x$, $N(x + \sqrt{\delta}y) = x^2 - \delta y^2$. $\Psi_0 : Z_p \to C^*$ is a generator of the dual group to Z_p. $\Psi : F \to C^*$ is the character $\Psi = \Psi_0 \circ Tr$

Lemma 7.

$$\text{For any } a \in F,\ J_0^{F\times F}(a) = -J_0^K(a)$$

Proof: We claim that that if a is not a square in F, then

$$\{\frac{a}{t} + t : t \in F^*\} \cap \{2x = Tr(w) : w \in K,\ Nw = a\} = \emptyset \qquad (4)$$

$$\{\frac{a}{t} + t : t \in F^*\} \cup \{2x = Tr(w) : w \in K,\ Nw = a\} = F \qquad (4)$$

Indeed, $\frac{a}{t}+t=2x$ implies that $(\frac{1}{2}(\frac{a}{t}+t))^2-\delta y^2=a$ for some $y\in F$. This yields that $\frac{1}{4}(\frac{-a}{t}+t)^2=\delta y^2$. Since a,δ are not squares in F, and $y\neq 0$ we have a contradiction. Thus, the intersection is empty. On the other hand, the fact that a is not a square implies that the function $t\to\frac{a}{t}+t$ is two to one. Thus, the cardinal of the first set is $\frac{q-1}{2}$. Moreover, the fact that the prime field is not of order two, implies that the function $w\to Tr(w)$ from $Nw=a$ is two to one. Thus, the number of elements of the second set is $\frac{q+1}{2}$ and we obtain the second equality in (4).
The same computation shows that if $a=t_0^2,\ t_0\in F$, then

$$\{\frac{a}{t}+t:t\in F^*\}\cap\{2x=Tr(w):w\in K,\ Nw=a\}=\{\pm 2t_0\}\qquad(5)$$

$$\{\frac{a}{t}+t:t\in F^*\}\cup\{2x=Tr(w):w\in K,\ Nw=a\}=F\qquad(5)$$

Indeed, since $a=t_0^2$ the function $t\to\frac{a}{t}+t$ is two to one in $F^*-\{\pm t_0\}$. Thus, the cardinal of the first set is $\frac{q-1-2}{2}+2=\frac{q+1}{2}$. The cardinal of the second set is $\frac{q+1-2}{2}+2=\frac{q+3}{2}$. Hence, the union is F.
We now are ready to finish the proof of lemma 7.

$$J_0^{F\times F}(a)+J_0^K(a)=\sum_{t\in F^*}\Psi_0(\frac{a}{t}+t)+\sum_{w\in K,x^2-\delta y^2=a}\Psi_0(2x)$$

If a is not a square in F, according to (4) in the above sum we are considering each element of F twice. Thus, the Schur orthogonality relations applied to Ψ_0 yield,

$$J_0^{F\times F}(a)+J_0^K(a)=2\sum_{u\in F}\Psi_0(u)=0.$$

According to (5) if $a\neq 0$ is a square in F, in the sum we are considering each element of F twice, except for $\pm t_0$. Hence,

$$J_0^{F\times F}(a)+J_0^K(a)=2(\sum_{u\in F,u\neq\pm t_0}\Psi_0(u))+\Psi_0(t_0)+\Psi_0(-t_0)=$$
$$2\sum_{u\in F}\Psi_0(u)+3(\Psi_0(t_0)+\Psi_0(-t_0))=0$$

$$J_0^{F\times F}(0)+J_0^K(0)=\sum_{u\in F^*}\Psi_0(u)+$$

$$+\sum_{x^2-\delta y^2=0}\Psi_0(2x)=\sum_{u\in F^*}\Psi_0(u)+\Psi_0(0)=$$
$$\sum_{t\in F}\Psi_0(t)=0.$$

And we have conclude the proof of lemma 7.

Lemma 8. For $F=Z_p,\ p>3\ J_0^K$ is an injective function.

Proof: Recall that $[K:Z_p]=2$ and that $K=Z_p[\sqrt{\delta}]$ with δ a nonsquare in Z_p. Let ξ be the $p-$root of one that determines Ψ_0. Thus, $\Psi_0(k)=\xi^k$.

$$J(a):=J_0^K(a)=\sum_{x^2-\delta y^2=a;\,x,y\in Z_p}\Psi_0(2x)$$

Hence,

$$J(a)=\sum_{x^2-\delta y^2=a;\,x,y\in Z_p}\xi^{2x}=\sum_{k=0}^{k=p-1}c_k(a)\xi^k.$$

Where,

$$c_k(a)=\sharp\{w=x+\sqrt{\delta}y:2x\ \equiv kmod(p),x^2-\delta y^2=a\}.$$

Thus, $c_k(a)=\sharp\{y\in Z_p:(\frac{k}{2})^2-\delta y^2=a\}=\sharp\{y\in Z_p:\frac{k^2-4a}{4\delta}=y^2\}$. Hence, $c_k(a)\leq 2$. Actually, since $p>2$ we have:

If a is a square in Z_p, then $c_{\pm 2\sqrt{a}}(a)=1$ (6)

For any a in Z_p and for $k\neq\pm 2\sqrt{a}$, $c_k(a)\in\{0,2\}$. $c_0(a)=\sharp\{y:\frac{-4a}{4\delta}=y^2\}$. Thus, c_0 is constant on the set of squares in Z_p and on the set of nonsquares in Z_p. (7)

For $a\neq 0$, $c_0(a)\in\{0,2\}$, $c_0(0)=1, c_k(0)=0\,\text{for}\,k\neq 0$. (8)

The first two affirmations are obvious. The third one follows from the fact that δ is not a square in Z_p.

$J(a)=J(b)$ implies $c_k(a)-c_0(a)=c_k(b)-c_0(b),\text{for}\,k=1,\ldots,p-1,$ (9)

Indeed, since $1+\xi+\cdots+\xi^{p-1}=\xi^p-1=0$, we obtain $J(a)=\sum_k c_k(a)\xi^k=\sum_{k=1}^{k=p-1}(c_k(a)-c_0(a))\xi^k$. Now Galois Theory (c.f. [L],) says that $\xi,\ldots,\xi^{p-1}$ are linearly independent over rational numbers Q. Therefore, (9) follows.

$J(a)=J(0)$ implies $a=0$. (10)

We assume $a\neq 0$. Since $J(a)=J(0)$, (9) implies that $c_k(0)-c_0(0)=c_k(a)-c_0(a)$. Next (8) says that $c_k(a)-c_0(a)=0-1=-1\,\text{if}\,k>0$. Thus, $c_k(a)=-1-0=-1\,\text{or}\,c_k(a)=-1+2=1$. If we had $c_k(a)=1\,\text{for every}\,1\leq$

$k \leq p-1$ the hypothesis $p > 3$ forces that there exist $k \leq p-1$ so that $k \neq \pm 2\sqrt{a}$. Hence, we have contradicted (6). Thus, $a = 0$.
Next, we prove that for a, b squares $J(a) = J(b)$ implies $a = b$.
Since a, b are squares (7) yields $c_0(a) = c_0(b)$. Thus, $c_k(a) = c_k(b)$ for every k. The last equality and (6) imply $1 = c_{2\sqrt{a}}(a) = c_{2\sqrt{a}}(b) = c_{2\sqrt{b}}(b)$. Thus, $2\sqrt{a} = \pm 2\sqrt{b}$. Hence, $a = b$.
For a a square and b a nonsquare, $J(a) = J(b)$ yields, as before, $1 = c_{2\sqrt{a}}(a) = c_{2\sqrt{a}}(b)$. But, b is a nonsquare, hence $c_k(b) \in \{0, 2\}$. A contradiction.
Finally, we prove if a, b are nonsquares, $J(a) = J(b)$ yields $a = b$.
The hypothesis on a, b together with (7) gives $c_0(a) = c_0(b)$. Thus, the hypothesis on J implies $c_k(a) = c_k(b)$ for every k.
Let $S_i(a) = \{k : c_k(a) = i\}$. The hypothesis on a, b yield $S_i(a) = S_i(b)$ for every i, and $S_1(a) = S_1(b) = \emptyset$. Recall that K is a second degree extension of Z_p. Tr, N denote the norm and the trace of K over Z_p.

$$Tr\{z = x + \sqrt{\delta}y \in K : x^2 - \delta y^2 = a\} = S_2(a). \tag{11}$$

In fact, $Tr(z) = 2x$ and $\frac{(2x)^2 - 4a}{4\delta} = \frac{x^2 - a}{\delta} = \frac{\delta y^2}{\delta} = y^2$. Note that y is nonzero because a is a nonsquare. Hence, $2x \in S_2(a)$. On the other hand, let $u \in S_2(a)$. Thus, $\frac{u^2 - 4a}{4\delta} = y^2$ has two solutions $y_\pm$. Obviously, $\frac{u}{2} + \sqrt{\delta}y_\pm$ is in $\{z \in K : x^2 - \delta y^2 = a\}$ and we have proved the other inclusion. Also, since $y \neq 0$ we obtain that the map $Tr : \{z = x + \sqrt{\delta}y \in K : x^2 - \delta y^2 = a\} \to S_2(a)$ is two to one. Since $\sharp\{z = x + \sqrt{\delta}y \in K : x^2 - \delta y^2 = a\} = p + 1$ for $a \neq 0$. We obtain,

$$\text{For } a \text{ a nonsquare in } Z_p \text{ we have } \sharp S_2(a) = \frac{p+1}{2}. \tag{12}$$

The fact that a, b are nonsquare together with (11) and $J(a) = J(b)$ imply that $S_2(a) = \{2x : x^2 - \delta s_x^2 = a, \text{for some } s_x\} = \{2x : x^2 - \delta y_x^2 = b, \text{for some } y_x\} = S_2(b)$. Next, we assume $a \neq b$. Then $x^2 - \delta s_x^2 = a, x^2 - \delta y_x^2 = b$ yield $y_x^2 - s_x^2 = \frac{b-a}{\delta}$. Set $A_x = (\pm s_x, \pm y_x)$. A_x has four elements, otherwise $\pm s_x = \pm y_x$ for some combination of $\pm$. Thus, $a = x^2 - \delta s_x^2 = x^2 - \delta y_x^2 = b$, a contradiction. Also, s_x, y_x are nonzero because a, b are not a square in Z_p. The fact that $y_x^2 - s_x^2 = \frac{b-a}{\delta}$ implies that $A_x \subset H_{\frac{b-a}{\delta}} := \{(s, t) \in Z_p \times Z_p : s^2 - t^2 = \frac{b-a}{\delta}\}$.
Note that $A_{-x} = A_x$. Moreover, $A_x \cap A_z \neq \emptyset$ implies $z = \pm x$. In fact, $(\pm s_x, \pm y_x) \in A_x \cap A_z$ yields $x^2 - \delta s_x^2 = a, z^2 - \delta s_x^2 = a$, thus, $z^2 = x^2$. Let R be a set of representatives for the equivalence relation $x \sim -x$ in $S_2(a)$. The above consideration has as a consequence that $H_{\frac{b-a}{\delta}} \supseteq \cup_{x \in R} A_x$, a disjoint union. Now, if -1 is not a square in Z_p, then (12) implies that $\sharp R = \frac{p+1}{4}$.

Finally, we recall that $\sharp H_{\frac{b-a}{\delta}} = p - 1$. Hence, we obtain $p - 1 \geq 4\frac{p+1}{4}$, a contradiction. For the case -1 is a square in Z_p we have that $p - 1 \geq 4[(\frac{p+1}{2} - 1)\frac{1}{2} + 1] = p + 3$, another contradiction. Therefore $a = b$ and we have proved lemma 8. Now theorem 1 b) follows.

Bibliography

[Ar] Artin, E., Geometric Algebra, Interscience, 1962.

[L] Lang, S., Algebra, Addison Wesley, 1965.

[M] Mackey, G., The theory of unitary group representations. The University of Chicago Univ. Press, 1976

[MMST] Medrano A., Myers P., Stark H., Terras A., Finite analogues of euclidean space, Journal of Computation and Applied Mathematics 68 (1996) 221-238

[Se] Serre J.P., A course in arithmetic, Springer Verlag, 1978.

[St] Stanton D., Orthogonal Polynomials and Chevalley Groups, Special functions: group theoretical aspects and applications, Ed. Askey and Korwinder, Reidel 1984.

[Wa] Warner, Garth, Harmonic Analysis on semisimple Lie Groups, Springer Verlag, 1972.