ANNALES DE L'INSTITUT FOURIER

ROBERT BROOKS

On the angles between certain arithmetically defined subspaces of $\mathbf{C}^n$

Annales de l'institut Fourier, tome 37, nº 1 (1987), p. 175-185

<http://www.numdam.org/item?id=AIF_1987__37_1_175_0>

Ann. Inst. Fourier, Grenoble
37, 1 (1987), 175-185

ON THE ANGLES BETWEEN CERTAIN ARITHMETICALLY DEFINED SUBSPACES OF $\mathbf{C}^n$

by Robert BROOKS(*)

In this note, we consider the following problem: Let $\{v_i\}$ and $\{w_j\}$ be two sets of unitary bases for $\mathbf{C}^n$. The bases $\{v_i\}$ and $\{w_j\}$ are about as "independent as possible" if, for all i and j, $|\langle v_i, w_j\rangle|$ is on the order of $\frac{1}{\sqrt{n}}$. For θ some fixed number, for instance $\frac{1}{5}$, we consider linear spaces V^θ (resp. W^θ) spanned by $[\theta \cdot n]$ of the vectors in the set $\{v_i\}$ (resp. $\{w_j\}$, where [ ] denotes the greatest integer function. What can one say about the angle between V^θ and W^θ, as n tends to infinity ?

In view of the paper [5], we may view such a question as relating to the prediction theory of such subspaces, although we do not see a direct connection between the methods of [5] and the present paper.

Let us consider the following special cases: In the first case, let $\{v_i\}$ be the standard basis for $\mathbf{C}^n$, and let $\{w_j\}$ be the "Fourier transform" of this basis

$$w_j = \frac{1}{\sqrt{n}}(\zeta^j, \zeta^{2j}, , , \ldots, \zeta^{nj})$$

(*) Partially supported by NSF grant DMS-83-15522 ; Alfred P. Sloan fellow.

Key-words : Angles – λ_1 – Eigenvalues – Kloosterman sum.

where $\zeta = e^{2\pi i/n}$ is a primitive *n-th* root of 1. Then clearly $|\langle v_i, w_j\rangle| = \frac{1}{\sqrt{n}}$ for all i, j.

For a number α, let us denote by $[[\alpha]]$ the distance from α to the nearest integer

$$[[\alpha]] = \inf_{n \in \mathbf{Z}} |\alpha - n|.$$

Let V^θ and W^θ denote the spaces spanned by

$$\left\{ v_i : \left[\left[\frac{i}{n}\right]\right] < \theta \right\} \quad \text{and} \quad \left\{ w_j : \left[\left[\frac{i}{n}\right]\right] < \theta \right\}$$

respectively. For σ_n a permutation of the integers $(\mathrm{mod}\ n)$, let $\mathrm{W}^\theta_{\sigma_n}$ be the space spanned by $\left\{ w_j : \left[\left[\frac{\sigma_n(j)}{n}\right]\right] < \theta \right\}$. Then we will show :

THEOREM 1. – (a) *For any* θ, *the angle between* V^θ *and* W^θ *tends to* 0 *as* n *tends to* ∞.

(b) *If the permutations* σ_n *are "sufficiently mixing", then the angle between* V^θ *and* $\mathrm{W}^\theta_{\sigma_n}$ *stays bounded away from* 0 *as* n *tends to* ∞.

By "sufficiently mixing", we mean that, for all i, we do not have both $\left[\left[\frac{\sigma_n(i)}{n}\right]\right] < \theta$ and $\left[\left[\frac{\sigma_n(i+1)}{n}\right]\right] < \theta$. Clearly, weaker hypotheses on the σ_n would also allow us to conclude (b), but we will not explore this question here.

Now let us consider the following different example: for a prime p, let χ denote an even multiplicative character $(\mathrm{mod}\, p)$. Then set $\{v_i\}$, $\{w_j\}$ to be the following bases for $\mathbf{C}^{p+1}$:

$$v_j - \frac{1}{\sqrt{p}}(1, \zeta^j, \ldots, \zeta^{(n-1)j}, 0)\, j = 0, \ldots, p-1$$

$$v_p = (0, \ldots, 0, 1)$$

$$w_k = \frac{1}{\sqrt{p}}(0, \chi(1)\,\zeta^{-k}, \chi(2)\,\zeta^{-\overline{2k}}, \ldots, \chi(n-1)\,\zeta^{-(\overline{n-1})k}, 1)$$

$$k = 0, \ldots, p-1$$

$w_p = (1, 0, \ldots, 0)$

where $\bar{m}$ denotes the reciprocal of $m \pmod p$. Note that

$$\langle v_j, w_k \rangle = \frac{1}{p} \sum_{x=1}^{p-1} \overline{\chi(k)}\ \zeta^{(jx + k\bar{x})} = \frac{1}{p} S_\chi(j, k, p)$$

where $S_\chi(j, k, p)$ is a Kloosterman sum. The fact that the bases $\{v_k\}$, $\{w_k\}$ are about as "independent as possible" is a deep result of A. Weil [7] that $|S_\chi(j, k, p)| < 2\sqrt{p}$.

Denoting by V^θ and W^θ_χ the vectors spanned by

$$\{v_i : [[i/p]] < \theta\} \quad \text{and} \quad \{w_j : [[j/p]] < \theta\}$$

respectively, our second result is:

THEOREM 2. – *For θ sufficiently small, the angle between V^θ_χ and W^θ_χ stays bounded away from 0 as p tends to ∞, uniformly with respect to χ.*

Our proof of Theorem 2 relies on the deep theorem of Selberg [6] that, when Γ_n is a congruence subsgroup of PSL $(2, \mathbf{Z})$, then the first eigenvalue $\lambda_1(\mathbf{H}^2/\Gamma_n)$ of the spectrum of the Laplacian satisfies $\lambda_1(\mathbf{H}^2/\Gamma_n) \geqslant \frac{3}{16}$.

Another important ingredient in Theorem 2 is our recent work [3] on the behavior of λ_1 in a tower of coverings. Indeed it is not difficult to find an extension of Theorem 2 which is actually equivalent, given [3], to Selberg's theorem, at least after replacing "$\frac{3}{16}$" by "some positive constant".

The main number-theoretic input into Selberg's theorem is the Weil estimate. Theorem 1 shows that, by contrast, the conclusion of Theorem 2 cannot be achieved directly by appealing to the Weil estimate, and suggests an interpretation of Selberg's theorem in terms of the random distribution of Kloosterman sums.

The proof of Theorem 1 is completely elementary.

We would like to thank Peter Sarnak for useful discussions, and Alice Chang for showing us the paper [5] and for her suggestions.

1. A Lemma.

In this section, we give a simple lemma in linear algebra which is the key to proving Theorems 1 and 2.

Suppose U and T are unitary matrices acting on $\mathbf{C}^n$. For a given value δ, let U^δ (resp. T^δ) be the subspace spanned by the eigenvectors of U (resp. T) whose eigenvalues λ satisfy $|\lambda - 1| < \delta$. Let $U_\perp^\delta$ and $V_\perp^\delta$ denote the perpendicular subspaces.

Denote by $k(U,T)$ the expression

$$k(U,T) = \inf_{\|X\|=1} \max(\|U(X) - X\|, \|T(X) - X\|).$$

Let $\alpha(\delta)$ denote the cosine of the angle between U^δ and T^δ:

$$\alpha(\delta) = \sup_{X \in U^\delta, Y \in V^\delta} \frac{|\langle X, Y\rangle|}{\|X\|\,\|Y\|}.$$

The main result of this section is:

LEMMA. — $\delta\sqrt{\dfrac{1-\alpha^2}{2}} \leqslant k(U,T) \leqslant \sqrt{\delta^2\alpha^2 + 4(1-\alpha^2)}$.

Proof. — To show the right-hand inequality, let X be a unit-length vector in U^δ such that its orthogonal projection Y onto T^δ is of maximum length $\alpha(\delta)$.

Since $X \in U^\delta$, we have $\|U(X) - X\| \leqslant \delta$. Writing

$$X = Y + Y^\perp, \; Y^\perp \in T_\perp^\delta,$$

we see that

$$\|T(X) - X\|^2 = \|T(Y) - Y\|^2 + \|T(Y^\perp) - Y^\perp\|^2 \leqslant \delta^2 \cdot \alpha^2 + 4(1-\alpha^2).$$

So $k(U,T) \leqslant \max(\delta, \sqrt{\delta^2\alpha^2 + 4(1-\alpha^2)})$. When $\delta < 2$, the second term on the right is $\geqslant \delta$. When $\delta \geqslant 2$, then $\alpha = 1$ and again the second term is $\geqslant \delta$.

To get the left-hand inequality, let X be a vector of length 1 minimizing $\sup(\|U(X) - X\|, \|T(X) - X\|)$. Write

$$X = X_U + X_T + X_\perp$$

where $X_U \in U^\delta$, $X_T \in T^\delta$, and $X_\perp \in U_\perp^\delta \cap T_\perp^\delta$. Then

$$\|U(X) - X\|^2 \geqslant \delta^2 [(1 - \alpha^2) \|X_T\|^2 + \|X_\perp\|^2]$$

$$\|T(X) - X\|^2 \geqslant \delta^2 [(1 - \alpha^2) \|X_U\|^2 + \|X_\perp\|^2]$$

and so

$$\delta^2 (1 - \alpha^2) \|X\|^2 \leqslant \|U(X) - X\|^2 + \|T(X) - X\|^2 \leqslant 2 k^2 (U, T)$$

and so $k(U, T) \geqslant \delta \sqrt{\dfrac{1 - \alpha^2}{2}}$.

From the left-hand estimate, we see that for δ fixed, and hence for δ arbitrarily small, a lower bound for $1 - \alpha^2$ gives a lower bound for $k(U, T)$. From the right-hand side, we see that a lower bound for $k(U, T)$ gives, for $\delta \ll k(U, T)$, a lower bound for $1 - \alpha^2$.

2. Proof of Theorem 1.

Let $v_i = (0, 0, \ldots, 1, 0, \ldots, 0)$ be the standard basis for $\mathbf{C}^n$ and let

$$w_j = \frac{1}{\sqrt{n}} (\zeta^j, \zeta^{2j}, \ldots, \zeta^{nj}).$$

Let V be the unitary transformation whose eigenvectors are the v_i's, with $V(v_i) = \zeta^i v_i$. Of course, the matrix for V is simply the diagonal matrix

$$V = \begin{pmatrix} \zeta^1 & & 0 \\ & \zeta^2 & \\ 0 & & \zeta^n \end{pmatrix}.$$

Similarly, let W be the unitary transformation whose eigenvectors are the $w_j's$, with $W(w_j) = \zeta^j \cdot w_j$. We compute:

LEMMA. —

$$\mathrm{W} = \begin{pmatrix} 0 & 1 & 0 & . & . & . & 0 \\ 0 & 0 & 1 & & 0 & . & 0 \\ 1 & 0 & 0 & . & . & . & 0 \end{pmatrix}.$$

Proof. — $\mathrm{W} = \mathrm{EVE}^{-1}$, where $\mathrm{E} = (e_{ij})$ is given by

$$e_{ij} = \frac{1}{\sqrt{n}} \zeta^{ij}.$$

The lemma now follows by routine calculation.

To prove Theorem 1 (a) it suffices, from the lemma of § 1, to show that $k(\mathrm{V}, \mathrm{W})$ tends to 0 as n tends to infinity.

But $\mathrm{V} - \mathrm{I}$ has the matrix expression

$$\begin{pmatrix} \zeta - 1 & & 0 \\ & \zeta^2 - 1 . & \\ 0 & & \cdot \zeta^n - 1 \end{pmatrix}$$

so that any element in V^θ satisfies

$$\| (\mathrm{V} - \mathrm{I})(v) \| \leqslant 2 \left| \sin \left(\frac{\theta}{2} \right) \right| \| v \|. \tag{*}$$

Now consider the vector v_n whose jth coordinate is 1 for $[[j/n]] < \theta$, and is 0 otherwise. Then we have that $v_n \in \mathrm{V}^\theta$, so that, by (*) we have

$$\| (\mathrm{V} - \mathrm{I})(v_n) \| \leqslant 2 \left| \sin \left(\frac{\theta}{2} \right) \right| \| v_n \|.$$

On the other hand, from the lemma, we compute easily that

$$\| (\mathrm{W} - \mathrm{I})(v_n) \| = \sqrt{2}.$$

Since $\| v_n \| = \sqrt{2 [n \cdot \theta] + 1}$, where [ ] denotes the greatest integer function, we have that

$$k(\mathrm{V}, \mathrm{W}) \leqslant \sup \left(2 \left| \sin \left(\frac{\theta}{2} \right) \right|, \frac{1}{\sqrt{[n \cdot \theta] + \frac{1}{2}}} \right).$$

It is then evident that as $n \longrightarrow \infty$, we may choose $\theta \longrightarrow 0$ such that the right-hand side $\longrightarrow 0$, establishing Theorem 1 (a).

To establish 1 (b), we first notice from the computation of the lemma that whenever σ_n is sufficiently mixing,

$$\| (W\sigma_n - I)\, v \| = (\sqrt{2})\, \| v \|$$

for $v \in V^\theta$. Fixing θ, for $v \in V^\theta$, let us write

$$v = w + w^\perp ,\, w \in W^\theta_{\sigma_n} ,\, w^\perp \in (W^\theta_{\sigma_n})^\perp .$$

$$2\,\| v \|^2 = \| W_{\sigma_n}(v) - v \|^2 = \| W_{\sigma_n}(w) - w \|^2 + \| W_{\sigma_n}(w^\perp) - w^\perp \|^2$$

$$\leqslant 4 \sin^2(\pi\theta) \cdot \| w \|^2 + 4\, \| w^\perp \|^2 = 4 \sin^2(\pi\theta) \cdot \| w \|^2 + 4\,(\| v \|^2 - \| w \|^2)$$

from which we see that

$$4\,(1 - \sin^2(\pi\theta))\, \| w \|^2 \leqslant 2\, \| v \|^2 \quad \text{so that} \quad \frac{\| w \|}{\| v \|} \leqslant \frac{1}{(\sqrt{2})} \cos(\pi\theta),$$

$$\alpha \leqslant \left(\frac{1}{\sqrt{2}}\right) \cos(\pi\theta).$$

Choosing θ smaller that $\frac{1}{4}$ then establishes Theorem 1 (b).

3. Proof of Theorem 2.

We begin this section with a quick review of the result of [3]. For M a compact manifold, and $M^{(i)}$ a family of finite covering spaces of M, we seek conditions of a combinatorial nature on $\pi_1(M), \pi_1(M^{(i)})$ which govern the asymptotic behavior of $\lambda_1(M^{(i)})$ as i tends to infinity.

To state the main result of [3], let us assume that the $M^{(i)}$'s are normal coverings of M, so that the group $\pi^i = \pi_1(M)/\pi_1(M^{(i)})$ are defined. Let us also fix generators $g_1, \ldots, g_k$ for $\pi(M)$ – note that $g_1, \ldots, g_k$ also generate all the π^i's.

Let H_i denote orthogonal complement to the constant function in $L^2(\pi^i)$, which carries an obvious unitary structure preserved by the action of π^i.

If H is any space on which π acts unitarily, denote by $k(H)$

the "Kazhdan distance" from H to the trivial representation defined by

$$k(\mathrm{H}) = \inf_{\|\mathrm{X}\|=1} \ \sup_{i=1,\ldots,k} \ \|g_i(\mathrm{X}) - \mathrm{X}\|.$$

Then we have :

THEOREM ([3]). – *The following two conditions are equivalent :*

a) *There exists* $c > 0$ *such that* $\lambda_1(\mathrm{M}^{(i)}) > c$ *for all* i

b) *There exists* $k > 0$ *such that* $k(\mathrm{H}_i) > k$ *for all* i.

We may now extend this result in the following way: we observe that each non-trivial representation of π^i occurs as an orthogonal direct summand in H_i, and furthermore that

$$k\left(\bigoplus_{i=1}^{n} \mathrm{H}_i\right) = \inf\ k(\mathrm{H}_i).$$

Hence we may rephrase the Theorem as follows:

COROLLARY. – *The following two conditions are equivalent :*

a) *There exist* $c > 0$ *such that* $\lambda_1(\mathrm{M}^{(i)}) > c$ *for all* i.

b) *There exist* $k > 0$ *such that for all* i *and for every non-trivial irreducible unitary representation* H *of* π^i, $k(\mathrm{H}) > k$.

We now observe that, using the technique of [1] and [2], we may weaken the hypothesis that M be compact. To explain this briefly, let us assume that M has finite volume, and let F be a fundamental domain for M in $\widetilde{\mathrm{M}}$.

Recall from [1] that M satisfies an "isoperimetric condition at infinity" if there is a compact subset K of F such that $h(\mathrm{F} - \mathrm{K}) > 0$ where h denote the Cheeger isoperimetric constant, with Dirichlet conditions on $\partial\mathrm{K}$ and Neumann conditions on $\partial\mathrm{F} - \partial\mathrm{K}$.

When M is a Riemann surface with finite area and a complete metric of constant negative curvature, then it is easily seen that M satisfies an isoperimetric condition at infinity.

The technique of [1] and [2] then applies directly to show how to adapt the arguments of the compact case to the case when M satisfies an isoperimetric condition at infinity.

We now apply these considerations to the manifolds

$$M^{(n)} = \mathbf{H}^2/\Gamma_n, \quad \text{where} \quad \Gamma_n \subset \mathrm{PSL}(2, \mathbf{Z})$$

is the congruence subgroup

$$\Gamma_n = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} (\mathrm{mod}\ n) \right\}.$$

According to the theorem of Selberg [6] mentioned above,

$$\lambda_1(\mathbf{H}^2/\Gamma_n) > \frac{3}{16}.$$

Let us fix generators

$$V = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \qquad W = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$$

for $\mathrm{PSL}(2, \mathbf{Z})$, and observe that $\mathbf{H}^2/\Gamma_n$ is a finite area Riemann surface covering $\mathrm{H}^2/\mathrm{PSL}(2, \mathbf{Z})$, with covering group

$$\pi^n = \mathrm{PSL}(2, \mathbf{Z}/n).$$

It follows from the corollary that there is a constant $k > 0$ such that, for H any non-trivial irreducible representation of $\mathrm{PSL}(2, \mathbf{Z}/n)$, we have $k(\mathrm{H}) > k$.

We now let n be a prime p, and fix a Dirichlet character χ (mod p). We will assume that $\chi(-1) = 1$. We now consider the following representation H_χ, which is the representation associated to χ in the continuous series of representations of $\mathrm{PSL}(2, \mathbf{Z}/n)$: The representation of H_χ is the set of all functions f on

$$\mathbf{Z}/p \times \mathbf{Z}/p - \{0\}$$

which transform according to the rule

$$f(tx, ty) = \chi(t) f(x, y), \quad t \in (\mathbf{Z}/p)^* \tag{*}$$

and where $\mathrm{PSL}(2, \mathbf{Z}/p)$ acts on f by the rule

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} f(x, y) = f(ax + cy, bx + dy).$$

We may take as a basis for H_χ the functions

$$f_a(x, 1) = 1 \quad \text{if} \quad x = a$$
$$= 0 \ \text{otherwise}$$
$$f_a(1, 0) = 0$$

for $a = 0, \ldots, p-1$ and

$$f_\infty(x, 1) = 0 \quad \text{for} \quad x = 0, \ldots, p-1$$
$$f_\infty(1, 0) = 1$$

using (*) to extend the f_a's to all values of x, y.

Then an orthonormal basis of eigenvectors of V is given by

$$v_b = \frac{1}{\sqrt{p}}\left(\sum_{x=0}^{p-1} \zeta^{bx} \cdot f_x\right) \qquad V(v^b) = \zeta^b v_b$$

$$v_\infty = f_0 \qquad V(v_\infty) = v_\infty,$$

and an orthonormal basis of eigenvectors of W is given by

$$w_b = \frac{1}{\sqrt{p}}\left(\sum_{x=0}^{p-1} \zeta^{-bx} \chi(x) f_{\bar{x}}\right) \qquad W(w_b) = \zeta^b w_b$$

$$w_\infty = f_0 \qquad W(w_\infty) = w_\infty$$

where $\bar{x}$ is the multiplicative inverse of x (mod p), and $\bar{0} = \infty$.

When χ is the trivial character, the vector

$$\sqrt{\frac{p}{p+1}}\, v_0 + \frac{1}{\sqrt{p+1}}\, v_\infty = \sqrt{\frac{p}{p+1}}\, w_0 + \frac{1}{\sqrt{p+1}}\, w_\infty$$

splits off as a trivial representation, but for all other characters χ, H_χ is irreducible [4].

Theorem 2 is now an immediate consequence of the corollary above, the lemma of § 1, and Selberg's theorem.

BIBLIOGRAPHIE

[1] R. BROOKS, The Bottom of the Spectrum of a Riemannian Covering, *Crelles J.*, 357 (1985), 101-114.

[2] R. BROOKS, The Spectral Geometry of the Apollonian Packing, *Comm. P. Appl. Math.*, XXXVIII (1985), 357-366.

[3] R. BROOKS, The Spectral Geometry of a Tower of Coverings, *J. Diff. Geom.*, 23 (1986), 97-107.

[4] GELFAND, GRAEV, and PYATETSKII-SHAPIRO, *Representation Theory and Automorphic Functions*, W.B. Saunders Co. ,1969.

[5] H. HELSON and D. SARASON, Past and Future, *Math. Scand.*, 21 (1967), 5-16.

[6] A. SELBERG, On the Estimation of Fourier Coefficients of Modular Forms, *Proc. Symp. Pure Math*, VIII (1965), 1-15.

[7] A. WEIL, On Some Exponential Sums, *Proc. Nat. Acad. Sci. USA*, 34 (1948), 204-207.

Manuscrit reçu le 9 juillet 1985
révisé le 14 mai 1986.

Robert BROOKS,
Dept. of Mathematics
University of Southern California
Los Angeles, CA 90089-1113 (USA).