ROBERT BROOKS

On the angles between certain arithmetically defined subspaces of $C^n$


<http://www.numdam.org/item?id=AIF_1987__37_1_175_0>
ON THE ANGLES BETWEEN CERTAIN ARITHMETICALLY DEFINED SUBSPACES OF 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 \( \mathbb{C}^n \). 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 \( \theta \) some fixed number, for instance \( \frac{1}{5} \), we consider linear spaces \( V^\theta \) (resp. \( W^\theta \)) 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 \( V^\theta \) and \( W^\theta \), 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 \( \mathbb{C}^n \), and let \( \{w_j\} \) be the "Fourier transform" of this basis

\[
w_j = \frac{1}{\sqrt{n}} (\xi^j, \xi^{2j}, \ldots, \xi^{nj})
\]

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

Key-words: Angles — \( \lambda_1 \) — Eigenvalues — Kloosterman sum.
where \( \zeta = e^{2\pi i/n} \) is a primitive \( n\)-th root of 1. Then clearly
\[
|\langle v_i, w_j \rangle| = \frac{1}{\sqrt{n}} \quad \text{for all } i,j.
\]

For a number \( \alpha \), let us denote by \( \lfloor \alpha \rfloor \) the distance from \( \alpha \) to the nearest integer
\[
\lfloor \alpha \rfloor = \inf_{n \in \mathbb{Z}} |\alpha - n|.
\]

Let \( V^\theta \) and \( W^\theta \) denote the spaces spanned by
\[
\left\{ v_i: \left[ \frac{i}{n} \right] < \theta \right\} \quad \text{and} \quad \left\{ w_j: \left[ \frac{j}{n} \right] < \theta \right\}
\]
respectively. For \( \sigma_n \), a permutation of the integers \((\text{mod } n)\), let
\( W^\theta_{\sigma_n} \) be the space spanned by
\[
\left\{ w_j: \left[ \frac{\sigma_n(j)}{n} \right] < \theta \right\}.
\]
Then we will show :

**Theorem 1.** (a) For any \( \theta \), the angle between \( V^\theta \) and \( W^\theta \)
tends to 0 as \( n \) tends to \( \infty \).

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

By "sufficiently mixing", we mean that, for all \( i \), we do not
have both \( \left[ \frac{\sigma_n(i)}{n} \right] < \theta \) and \( \left[ \frac{\sigma_n(i+1)}{n} \right] < \theta \). Clearly,
weaker hypotheses on the \( \sigma_n \) 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 \( \chi \) denote an even multiplicative character \((\text{mod } p)\). Then
set \( \{ v_i \}, \{ w_j \} \) to be the following bases for \( \mathbb{C}^{p+1} \):

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

\[
v_p = (0, \ldots, 0, 1)
\]

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

\[ k = 0, \ldots, p-1 \]
where \( \bar{m} \) denotes the reciprocal of \( m \) (mod \( p \)). Note that

\[
\langle v_j, w_k \rangle = \frac{1}{p} \sum_{x=1}^{p-1} \chi(k) \xi^{jx+kx} = \frac{1}{p} S_\chi(j, k, p)
\]

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 \( V_\theta \) and \( W_\theta \) the vectors spanned by

\( \{v_j: \lceil i/p \rceil < \theta\} \) and \( \{w_j: \lfloor j/p \rfloor < \theta\} \)

respectively, our second result is:

**Theorem 2.** For \( \theta \) sufficiently small, the angle between \( V_\chi \) and \( W_\chi \) stays bounded away from 0 as \( p \) tends to \( \infty \), uniformly with respect to \( \chi \).

Our proof of Theorem 2 relies on the deep theorem of Selberg \([6]\) that, when \( \Gamma_n \) is a congruence subgroup of \( \text{PSL}(2, \mathbb{Z}) \), then the first eigenvalue \( \lambda_1(H^2/\Gamma_n) \) of the spectrum of the Laplacian satisfies

\[
\lambda_1(H^2/\Gamma_n) \geq \frac{3}{16}.
\]

Another important ingredient in Theorem 2 is our recent work \([3]\) on the behavior of \( \lambda_1 \) 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 $\mathbb{C}^n$. For a given value $\delta$, let $U^\delta$ (resp. $T^\delta$) be the subspace spanned by the eigenvectors of $U$ (resp. $T$) whose eigenvalues $\lambda$ satisfy $|\lambda - 1| < \delta$. Let $U^\perp_1$ and $V^\perp_1$ 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 $U^\delta$ and $T^\delta$:

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

The main result of this section is:

**Lemma.** $-\delta \sqrt{\frac{1 - \alpha^2}{2}} \leq k(U, T) \leq \delta \alpha^2 + 4(1 - \alpha^2)$.

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

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

$$X = Y + Y^\perp, Y^\perp \in T^\perp_1,$$

we see that

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

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

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

$$X = X_U + X_T + X_L$$

where $X_U \in U^\delta$, $X_T \in T^\delta$, and $X_L \in U_1^\delta \cap T_1^\delta$. Then

$$\|U(X) - X\|^2 \geq \delta^2 \left[(1 - \alpha^2) \|X_T\|^2 + \|X_L\|^2\right]$$

$$\|T(X) - X\|^2 \geq \delta^2 \left[(1 - \alpha^2) \|X_U\|^2 + \|X_L\|^2\right]$$

and so

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

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

From the left-hand estimate, we see that for $\delta$ fixed, and hence for $\delta$ 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 $C^n$ and let

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

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

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

Similarly, let $W$ be the unitary transformation whose eigenvectors are the $w_i$'s, with $W(w_i) = \xi^i \cdot w_i$. We compute:
**Lemma.** \( W = \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & 0 & \ldots & 0 \\ 1 & 0 & 0 & \ldots & 0 \end{pmatrix} \)

**Proof.** \( W = E V E^{-1} \), where \( E = (e_{ij}) \) is given by
\[
e_{ij} = \frac{1}{\sqrt{n}} i^j.
\]
The lemma now follows by routine calculation.

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

But \( V - I \) has the matrix expression
\[
\begin{pmatrix}
\xi - 1 & 0 \\
0 & \xi^2 - 1 \\
0 & \ldots & \xi^n - 1
\end{pmatrix}
\]
so that any element in \( V^\theta \) satisfies
\[
\| (V - I) (\nu) \| \leq 2 \sin \left( \frac{\theta}{2} \right) \| \nu \|.
\]

Now consider the vector \( \nu_n \) whose \( j \)th coordinate is 1 for \( \lfloor j/n \rfloor \leq \theta \), and is 0 otherwise. Then we have that \( \nu_n \in V^\theta \), so that, by (*) we have
\[
\| (V - I) (\nu_n) \| \leq 2 \sin \left( \frac{\theta}{2} \right) \| \nu_n \|.
\]

On the other hand, from the lemma, we compute easily that
\[
\| (W - I) (\nu_n) \| = \sqrt{2}. 
\]
Since \( \| \nu_n \| = \sqrt{2 \lfloor n \cdot \theta \rfloor + 1} \), where \( \lfloor \cdot \rfloor \) denotes the greatest integer function, we have that
\[
k(V, W) \leq \sup \left( 2 \sin \left( \frac{\theta}{2} \right), \frac{1}{\sqrt{n \cdot \theta + 1}} \right).
\]

It is then evident that as \( n \to \infty \), we may choose \( \theta \to 0 \) such that the right-hand side \( \to 0 \), establishing Theorem 1\((a)\).
To establish 1 (b), we first notice from the computation of the lemma that whenever $\sigma_n$ is sufficiently mixing,
\[ \| (W \sigma_n - I) v \| = (\sqrt{2}) \| v \| \]
for $v \in V^\theta$. Fixing $\theta$, for $v \in V^\theta$, let us write
\[ v = w + w^1, w \in W^\theta_{\sigma_n}, w^1 \in (W^\theta_{\sigma_n})^1. \]

\[ 2 \| v \|^2 = \| W_{\sigma_n} (v) - v \|^2 = \| W_{\sigma_n} (w) - w \|^2 + \| W_{\sigma_n} (w^1) - w^1 \|^2 \]
\[ \leq 4 \sin^2 (\pi \theta) \cdot \| w \|^2 + 4 \| w^1 \|^2 = 4 \sin^2 (\pi \theta) \cdot \| w \|^2 \]
\[ + 4 (\| v \|^2 - \| w \|^2) \]
from which we see that
\[ 4 (1 - \sin^2 (\pi \theta)) \| w \|^2 \leq 2 \| v \|^2 \]
so that \[ \frac{\| w \|}{\| v \|} \leq \frac{1}{(\sqrt{2})} \cos (\pi \theta), \]
\[ \alpha \leq \left( \frac{1}{\sqrt{2}} \right) \cos (\pi \theta). \]
Choosing $\theta$ 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 $\pi^i (M)$ 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 $\pi^i$'s.

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

If $H$ is any space on which $\pi$ acts unitarily, denote by $k (H)$
the "Kazhdan distance" from $H$ to the trivial representation defined by
\[ k(H) = \inf \sup \|g_i(X) - X\|. \]
\[ \|X\| = 1 \quad i = 1, \ldots, k \]
Then we have:

**Theorem ([3]).** — The following two conditions are equivalent:

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

b) There exists $k > 0$ such that $k(H_i) > k$ for all $i$.

We may now extend this result in the following way: we observe that each non-trivial representation of $\pi^i$ occurs as an orthogonal direct summand in $H_i$, and furthermore that
\[ k\left( \bigoplus_{i=1}^n H_i \right) = \inf k(H_i). \]
Hence we may rephrase the Theorem as follows:

**Corollary.** — The following two conditions are equivalent:

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

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

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 $\tilde{M}$.

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

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
\[ M^{(n)} = H^2 / \Gamma_n , \text{ where } \Gamma_n \subset PSL(2, \mathbb{Z}) \]
is the congruence subgroup
\[ \Gamma_n = \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{n} \}. \]

According to the theorem of Selberg [6] mentioned above,
\[ \lambda_1 (H^2 / \Gamma_n) > \frac{3}{16}. \]

Let us fix generators
\[ V = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \quad W = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \]
for PSL(2, \mathbb{Z}), and observe that H^2 / \Gamma_n is a finite area Riemann
surface covering H^2 / PSL(2, \mathbb{Z}), with covering group
\[ \pi^n = PSL(2, \mathbb{Z}/n). \]

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

We now let \( n \) be a prime \( p \), and fix a Dirichlet character \( \chi \pmod{p} \). We will assume that \( \chi(-1) = 1 \). We now consider the
following representation \( H_\chi \), which is the representation associated
to \( \chi \) in the continuous series of representations of PSL(2, \mathbb{Z}/n):
The representation of \( H_\chi \) is the set of all functions \( f \) on
\[ \mathbb{Z}/p \times \mathbb{Z}/p - \{0\} \]
which transform according to the rule
\[ f(tx, ty) = \chi(t)f(x, y), \quad t \in (\mathbb{Z}/p)^* \quad (*) \]
and where PSL(2, \mathbb{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 \( H_\chi \) the functions
\[ f_a(x, 1) = 1 \text{ if } x = a \]
\[ = 0 \text{ otherwise} \]
\[ f_a(1, 0) = 0 \]
for \( a = 0, \ldots, p - 1 \) and
\[ f_\infty(x, 1) = 0 \text{ for } x = 0, \ldots, p - 1 \]
\[ f_\infty(1, 0) = 1 \]
using (*) to extend the \( f_a \)'s to all values of \( x, y \).

Then an orthonormal basis of eigenvectors of \( V \) is given by
\[
v_b = \frac{1}{\sqrt{p}} \left( \sum_{x=0}^{p-1} \xi^{bx} \cdot f_x \right)
V(v^b) = \xi^b v_b
\]
\[ v_\infty = f_0 \quad V(v_\infty) = v_\infty. \]
and an orthonormal basis of eigenvectors of \( W \) is given by
\[
w_b = \frac{1}{\sqrt{p}} \left( \sum_{x=0}^{p-1} \xi^{-bx} \chi(x) f_{\bar{x}} \right)
W(w^b) = \xi^b w_b
\]
\[ w_\infty = f_0 \quad W(w_\infty) = w_\infty. \]
where \( \bar{x} \) is the multiplicative inverse of \( x \) (mod \( p \)), and \( \bar{0} = \infty \).

When \( \chi \) 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 \( \chi, H_\chi \) is irreducible [4].

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


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).