Diameters of Homogeneous Spaces

Michael H. Freedman[1] , Alexei Kitaev[2] and Jacob Lurie[3]

11-04-2002

Technical Report
MSR-TR-2002-119

Let G be a compact connected Lie group with trivial center. Using the action of G on its Lie algebra, we define an operator norm $|\ |_G$ which induces a bi-invariant metric $d_G(x, y) = |Ad(yx^{-1})|_G$ on G. We prove the existence of a constant $\beta \approx .12$ (independent of G) such that for any closed subgroup $H \subsetneq G$, the diameter of the quotient G/H (in the induced metric) is $\geq \beta$.

Microsoft Research
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
http://www.research.microsoft.com

1 Introduction

Finding a lower bound to the (operator norm) diameter of homogeneous spaces G/H, G compact is a natural geometric problem. It can also be motivated by considering quantum computation. In standard models [NC] the state space of a (theoretical) quantum computer is a Hilbert space with a tensor decomposition, $(\mathbb{C}^2)^{\otimes n}$. A "gate" is a local unitary operation acting on a small number, perhaps two, tensor factors (and as the identity on the remaining factors). One often wonders if a certain set of local gates is "universal" meaning that the closed subgroup H they generate satisfies $U(1)H = U(2^n)$. We produce a constant $\beta \approx .12$ so that diam $U(2^n)/U(1)H < \beta$ implies universality, where diameter is to be computed in the operator norm. This norm is well-suited here because it is stable under $\otimes_{\mathrm{id}}$.

Because the operator norm is bi-invariant it suffices to check that every element b in the ball of radius 2β about the identity of $SU(2^n)$ has $\mathrm{Ball}_\beta(b) \cap H \neq \emptyset$. In principle this leads to an algorithm to test if a gate set is universal. Such an algorithm will be exponentially slow in n. But often it is assumed that identical gates can be applied on any pair of $\mathbb{C}^2$ factors; in this case universality for $n = 2$ is sufficient to imply universality for all n.

Let G be a compact Lie group with trivial center. The semisimplicity of G implies that the (negative of the) Killing form is a natural positive-definite, bi-invariant inner product on the Lie algebra $\mathfrak{g}$ of G. We let $||x||_{\mathfrak{g}}$ denote the induced (Euclidean) norm on $\mathfrak{g}$. We use this to define the *operator norm* on G as follows:

$$|g|_G = \sup_{||y||_{\mathfrak{g}}=1} |\angle(y, \mathrm{Ad}_g\, y)|$$

where $\angle(y, \mathrm{Ad}_g\, y)$ denotes the usual Euclidean angle between the vectors y and $\mathrm{Ad}_g\, y$, normalized so that it lies in the interval $[-\pi, \pi]$. Since angles between vectors in a Euclidean space obey a triangle inequality, we deduce the inequality $|gh|_G \leq |g|_G + |h|_G$. It is also clear that $|g|_G = 0$ if and only if Ad_g is the identity, which implies that g is the identity since the adjoint action of G is faithful up to the center of G, and we have assumed that the center of G is trivial.

We define a distance on G by the formula $d_G(g, g') = |g^{-1}g'|_G$. It is easy to check that this defines a bi-invariant metric on G, where all distances are bounded above by π. Note that d_G is continuous on G, hence there is a continuous bijection from G with its usual topology to G with the topology induced by d_G. Since the source is compact and the target Hausdorff (this fails if G has nontrivial center, since the operator norm of a central element is equal to zero), we deduce that the metric d_G determines the usual topology on G.

For any closed subgroup H of G, the homogeneous space G/H inherits a quotient metric given by the formula

$$d_{G/H}(p,q) = \inf d_G(\widetilde{p}, \widetilde{q}) = \inf_{gp=q} |g|_G$$

where the first infimum is taken over all pairs $\widetilde{p}, \widetilde{q} \in G$ lifting the pair $p, q \in G/H$. Note that if H is contained in H', then the diameter of G/H is at least as large as that of G/H'.

We are now in a position to state the main result:

Theorem 1. *Let G be a compact connected Lie group with trivial center and $H \subsetneq G$ a proper compact subgroup of G. Then the diameter of G/H with respect to the metric $d_{G/H}$ is no smaller than β, where β is the smallest real solution to the transcendental equation* $\cos^2(\alpha-\beta) + \sin^2(\alpha-\beta)\sin(\beta) = \cos(4\beta)$ *and* $\cos(\alpha) = \frac{7}{8}$.

One can estimate that the constant β is approximately .124332.

Example 2. Consider the case where $G = H \times H$ is a product, and H is embedded diagonally. Choose an element $h \in H$ with $|h|_H = \pi$ (such an element exists in any nontrivial one parameter subgroup). Then in $H \times H$, the distance $d_{H\times H}(h \times 0, h' \times h')$ is equal to the larger of $d_H(h, h')$ and $d_H(h', e)$. By the triangle inequality, this distance is at least $\frac{\pi}{2}$. It follows that the diameter of G/H is at least $\frac{\pi}{2}$.

Remarks:

(1) For any orthogonal representation $\tau : G \to O(V)$ of a group G, we can define an operator norm on G with respect to V:

$$|g|_{G,\tau} = \sup_{||v||=1} |\angle(v, gv)|$$

This construction has the following properties:

- If V is the complex plane $\mathbb{C}$, and $g \in G$ acts by multiplication by $e^{i\alpha}$ where $-\pi \leq \alpha \leq \pi$, then $|g|_{G,\tau} = |\alpha|$.
- Given any subgroup $H \subseteq G$, the restriction of $|\,|_{G,\tau}$ to H is equal to $|\,|_{H,\tau|H}$.
- The operator norm associated to a direct sum of representations τ_i of G is the supremum of the operator norms associated to the representations τ_i.
- In particular, the operator norm on G associated to a representation V is identical with the operator norm on G associated to the complexification $V \otimes_{\mathbb{R}} \mathbb{C}$ (with its induced Hermitian structure).
- To evaluate $|g|_{G,\tau}$, we can replace G by the subgroup generated by g and V by its complexification, which decomposes into one-dimensional complex eigenspaces under the action of g. We deduce that $|g|_{G,\tau}$ is the supremum of $|\log \lambda_j|$, where $\{\lambda_j\}$ is the set of eigenvalues for the action of g on V (and the logarithms are chosen to be of absolute value $\leq \pi$).

(2) The reader may be curious about the diameter of G/H relative to the Riemannian quotient of the Killing metric d_K. If we let N denote the dimension of $\mathfrak{g}$, then we have

$$d \leq d_K \leq \frac{3N^{\frac{1}{2}}d}{2}$$

(3) We ask if the quotient $SO(3)/I$ is the homogenous space of smallest diameter, where $I \simeq A_5$ denotes the symmetry group of the icosahedron.

(4) We wonder if there is a similar universal lower bound to the diameter of double coset spaces $K \diagdown G \diagup H$, G as above, K, $H \subset G$ closed subgroups. Our method does not apply directly.

(5) Although suggested by a modern subject the theorem could easily have been proved a hundred years ago and in fact may have been (or may be) known.

2 Small Subgroups

Throughout this section, G shall denote a compact, connected Lie group with trivial center. We give a quantitative version of the principle that discrete subgroups of G generated by "sufficiently small" elements are automatically abelian. We will use this in the proof of Theorem 1 in the case where H is discrete.

We will need to understand the operator norm on G a bit better. To this end, we introduce the *operator norm*

$$|x|_{\mathfrak{g}} = \sup_{||y||_{\mathfrak{g}}=1} ||[x,y]||_{\mathfrak{g}}$$

on the Lie algebra $\mathfrak{g}$ of G. This is a G-invariant function on $\mathfrak{g}$, so we can unambiguously define the operator norm of any tangent vector to the manifold G by transporting that tangent vector to the origin (via left or right translation) and then applying $x \mapsto |x|_{\mathfrak{g}}$.

The operator norm on $\mathfrak{g}$ is related to the operator norm on G by the following:

Lemma 3. *The exponential map $x \mapsto \exp(x)$ induces a bijection between $\mathfrak{g}_0 = \{x \in \mathfrak{g} : |x|_{\mathfrak{g}} < \frac{2\pi}{3}\}$ and $G_0 = \{g \in G : |g|_G < \frac{2\pi}{3}\}$. This bijection preserves the operator norms.*

Proof. First, we claim that the map $x \mapsto \exp(x)$ does not increase the operator norm. This follows from the fact that the eigenvalues of $\exp(x)$ have the form $\exp(\kappa)$, where κ is an eigenvalue of x. It follows that the exponential map sends $\mathfrak{g}_0$ into G_0.

Choose $g \in G_0$, and fix a maximal torus T containing g. Let $\mathfrak{t}$ be the Lie algebra of T. Decompose $\mathfrak{g} \otimes_{\mathbb{R}} \mathbb{C}$ into eigenspaces for the action of T: $\mathfrak{g} \otimes_{\mathbb{R}} \mathbb{C} = \mathfrak{t} \otimes_{\mathbb{R}} \mathbb{C} \oplus \bigoplus_{\alpha} \mathfrak{g}_{\alpha}$. The element g acts by an eigenvalue $\Lambda(\alpha)$ on each nonzero eigenspace $\mathfrak{g}_{\alpha}$. Since g is an orthogonal transformation, we may write $\Lambda(\alpha) = e^{i\lambda(\alpha)}$. Since $g \in G_0$, it is possible to choose the function λ so that $-\frac{2\pi}{3} < \lambda(\alpha) < \frac{2\pi}{3}$ for each root α. This determines the function λ uniquely.

Choose a system Δ of simple roots, and let x be the unique element of $\mathfrak{t}$ such that $\alpha(x) = \lambda(\alpha)$ for each $\alpha \in \Delta$. It follows immediately that $\exp(x) = g$ (since G has trivial center). To show that $x \in \mathfrak{g}_0$, we need to show that $|\alpha(x)| < \frac{2\pi}{3}$ for all roots α. For this, it will suffice to prove that $\alpha(x) = \lambda(\alpha)$ for all roots α.

The uniqueness of λ implies immediately that $\lambda(-\alpha) = -\lambda(\alpha)$. Thus, it will suffice to prove that the equation $\alpha(x) = \lambda(\alpha)$ holds when α is positive (with respect to the root basis Δ). Since the equation is known to hold whenever $\alpha \in \Delta$, it will suffice to prove that $\alpha(x) = \lambda(\alpha)$, $\beta(x) = \lambda(\beta)$ implies

$$(\alpha + \beta)(x) = \lambda(\alpha + \beta).$$

In other words, we need to show that the quantity

$$\epsilon = \lambda(\alpha + \beta) - \lambda(\alpha) - \lambda(\beta)$$

is equal to zero. By construction, $|\epsilon| < 2\pi$. On the other hand, since $\Lambda(\alpha)\Lambda(\beta) = \Lambda(\alpha + \beta)$, we deduce that $e^{i\epsilon} = 1$, so that ϵ is an integral multiple of 2π. It follows that $\epsilon = 0$, as desired.

It is clear from the construction that $|x|_{\mathfrak{g}} = |g|_G$. To complete the proof, we need to show that g has no other logarithms lying in $\mathfrak{g}_0$. This follows from the fact that any unitary transformation (in particular, the adjoint action of g on $\mathfrak{g}$) which does not have -1 as an eigenvalue has a unique logarithm whose eigenvalues are of absolute value $< \pi$. $\square$

Lemma 4. *Let $p : [0,1] \to G$ be a smooth function with $p(0)$ equal to the identity of G. Then $|p(1)|_G \leq \int_0^1 |p'(t)|_{\mathfrak{g}} dt$.*

Proof. For N sufficiently large, we can write $p(\frac{i+1}{N}) = p(\frac{i}{N})\exp(\frac{x_i}{N})$, where x_i is approximately equal to the derivative of p at $\frac{i}{N}$. Thus, as N goes to ∞, the average $\frac{|x_0|_{\mathfrak{g}} + \ldots + |x_{N-1}|_{\mathfrak{g}}}{N}$ converges to the integral on the right hand side of the desired inequality. By the triangle inequality, it will suffice to prove that $|p(\frac{i}{N})^{-1}p(\frac{i+1}{N})|_G \leq |\frac{|x_i|_{\mathfrak{g}}}{N}|_{\mathfrak{g}}$. If N is sufficiently large, then this follows immediately from Lemma 3. $\square$

Remark 5. The metric d_G on G is not necessarily a path metric: given $g, h \in G$, there does not necessarily exist a path in G having length equal to $d_G(g,h)$. However, it follows from Lemma 3 that d_G is a path metric *locally on G*. The length of a (smooth) path can be obtained by integrating the operator norm of the derivative of a path. Replacing d_G by the associated path metric only increases distances, so that Theorem 1 remains valid for the path metric associated to d_G. This modified version of Theorem 1 makes sense (and remains true) for compact Lie groups G with finite center.

We can now proceed to the main result of this section. Let α denote the smallest positive real number satisfying $\cos(\alpha) = \frac{7}{8}$.

Theorem 6. *Let $H \subset G$ be a discrete subgroup. Let $h, k \in H$ and suppose $|h|_G < \frac{\pi}{2}$, $|k|_G < \alpha$. Then $[h, k] = 1$.*

Proof. We define a sequence of elements of G by recursion as follows: $h_0 = h$, $h_{n+1} = [h_n, k]$. Let C satisfy the equation $\frac{C^2}{4} = 2 - 2\cos|k|_G$. Then the assumption on k ensures that $C < 1$. Our first goal is to prove that the operator norm of the sequence $\{h_n\}$ obeys the estimate $|h_n|_G < C^n \frac{\pi}{2}$. For $n = 0$, this is part of our hypothesis. Assuming that the estimate $|h_n|_G < C^n \frac{\pi}{2}$ is valid, we can use Lemma 3 to write $h_n = \exp(x)$, $|x|_{\mathfrak{g}} < C^n \frac{\pi}{2}$. Now define $p(t) = [\exp(tx), k]$, so that $p(0) = 1$ and $p(t) = h_{n+1}$.

Using Lemma 4, we deduce that $|h_{n+1}|_G \leq \int_0^1 |p'(t)|_{\mathfrak{g}} \leq \sup_t |p'(t)|_{\mathfrak{g}}$. On the other hand, the vector $p'(t)$ can be written as a difference

$$R_{p(t)}x - L_{\exp(tx)k\exp(-tx)}R_{k^{-1}}x$$

where R_g and L_g denote left and right translation by g. We obtain

$$\begin{aligned}
|p'(t)|_{\mathfrak{g}} &= |x - \operatorname{Ad}_{\exp(tx)k\exp(-tx)} x|_{\mathfrak{g}} \\
&= |\operatorname{Ad}_{\exp(-tx)} x - \operatorname{Ad}_{k\exp(-tx)} x|_{\mathfrak{g}} \\
&= |x - \operatorname{Ad}_k x|_{\mathfrak{g}} \\
&= \sup_{||y||_{\mathfrak{g}}=1} ||[x - \operatorname{Ad}_k x, y]||_{\mathfrak{g}} \\
&\leq \sup_{||y||_{\mathfrak{g}}=1}(||[x,y] - Ad_k[x,y]||_{\mathfrak{g}} + ||Ad_k[x,y] - [Ad_k x, y]||_{\mathfrak{g}}) \\
&\leq \sup_{||y||_{\mathfrak{g}}=1} ||[x,y] - Ad_k[x,y]||_{\mathfrak{g}} + \sup_{||y||_{\mathfrak{g}}=1} ||[x, y - Ad_k^{-1}y]||_{\mathfrak{g}} \\
&\leq \sqrt{2 - 2\cos|k|_G}\sup_{||y||_{\mathfrak{g}}=1} ||[x,y]||_{\mathfrak{g}} + |x|_{\mathfrak{g}} \sup_{||y||_{\mathfrak{g}}=1} ||y - Ad_k^{-1}y]||_{\mathfrak{g}} \\
&\leq 2\sqrt{2 - \cos|k|_G}|x|_{\mathfrak{g}} \\
&= C|x|_{\mathfrak{g}} \\
&< C^{n+1}\frac{\pi}{2},
\end{aligned}$$

as desired.

It follows that the operator norms of the sequence $\{h_n\}$ converge to zero. Therefore the sequence $\{h_n\}$ converges to the identity of G. Since H is a discrete subgroup, it follows that h_n is equal to the identity if n is sufficiently large. We will next show that $h_n = 1$ for all $n > 0$, using an argument of Frobenius which proceeds by a descending induction on n. Once we know that $h_1 = 1$, the proof will be complete.

Assume that $h_{n+1} = 1$. Then k commutes with h_n, and therefore also with $h_n k = h_{n-1} k h_{n-1}^{-1}$. It follows that $\mathfrak{g} \otimes_{\mathbb{R}} \mathbb{C}$ admits a basis whose elements are eigenvectors for both k and $h_{n-1} k h_{n-1}^{-1}$. If the eigenvalues are the same in both cases, then we deduce that $k = h_{n-1} k h_{n-1}^{-1}$, so that h_n is the identity and we are done. Otherwise, there exists $v \in \mathfrak{g} \otimes_{\mathbb{R}} \mathbb{C}$ which is an eigenvector for both k and $h_{n-1} k h_{n-1}^{-1}$, with different eigenvalues. Equivalently, both v and $h_{n-1} v$ are eigenvectors for k, with different eigenvalues. Thus v and $h_{n-1} v$ are orthogonal, which implies $|h_{n-1}|_G \geq \frac{\pi}{2}$, a contradiction. $\square$

3 The Proof when H is Discrete

In this section, we will give the proof of Theorem 1 in the case where H is a discrete subgroup. The idea is to show that if G/H is too small, then H contains noncommuting elements which are close to the identity, contradicting Theorem 6.

In the statements that follow, we let α denote the smallest positive real solution to $\cos(\alpha) = \frac{7}{8}$ and β the smallest positive real solution to the transcendental equation $\cos^2(\alpha - \beta) + \sin^2(\alpha - \beta) \cos(\frac{\pi}{2} - \beta) = \cos(4\beta)$.

Lemma 7. *Let G be a compact, connected Lie group with trivial center. Then there exist elements $h, k \in G$ having the property that for any $h', k' \in G$ with $d_G(h, h'), d_G(k, k') < \beta$, we have $|h'|_G < \frac{\pi}{2}$, $|k'|_G < \alpha$, and $[h', k'] \neq 1$.*

Proof. Choose a (local) embedding $p : SU(2) \to G$ corresponding to a root of some simple component of G. We will assume that if the relevant component has roots of two different lengths, then the embedding p corresponds to a long root. This ensures that the weights of $SU(2)$ acting on $\mathfrak{g}$ are no larger than the weights of the adjoint representation.

In the Lie algebra $\mathfrak{so}(3)$ of $SU(2)$, we let x and y denote infinitesimal rotations of angles $\frac{\pi}{2} - \beta$ and $\alpha - \beta$ about orthogonal axes. Then, by the above condition on weights, we deduce that $h = p(\exp(x))$ and $k = p(\exp(y))$ satisfy the conditions $|h|_G = \frac{\pi}{2} - \beta$, $|k|_G = \alpha - \beta$.

We claim that the pair $h, k \in G$ satisfies the conclusion of the lemma. To see this, choose any pair $h', k' \in G$ with $d(h, h'), d(k, k') < \beta$. Then we deduce $|h'|_G < \frac{\pi}{2}$, $|k'|_G < \alpha$ from the triangle inequality. To complete the proof, we must show that h' and k' do not commute. To see this, we let v denote the image in $\mathfrak{g}$ of a vector in $\mathfrak{so}(3)$ about which x is an infinitesimal rotation. Then $hv = v$, while $\angle(v, kv) = \alpha - \beta$. Elementary trigonometry now yields

$$\begin{aligned}\angle(hkv, khv) &= \angle(hkv, kv) \\ &= \cos^{-1}(\cos^2(\alpha-\beta) + \sin^2(\alpha-\beta)\cos(\tfrac{\pi}{2}-\beta)) \\ &= \cos^{-1}(\cos(4\beta)) = 4\beta.\end{aligned}$$

By the triangle inequality, we get

$$\begin{aligned}4\beta &= \angle(hkv, khv) \\ &\leq \angle(hkv, h'kv) + \angle(h'kv, h'k'v) + \angle(h'k'v, k'h'v) \\ &\quad +\angle(k'h'v, k'hv) + \angle(k'hv, khv) \\ &< 4\beta + \angle(h'k'v, k'h'v),\end{aligned}$$

which implies $\angle(h'k'v, k'h'v) > 0$ so that $[h', k'] \neq 1$. $\square$

We can now complete the proof of Theorem 1 in the case where H is discrete:

Proof. Choose $h, k \in G$ satisfying the conclusion of Lemma 7. Since G/H has diameter less than β, the cosets hH and kH are within β of the identity coset in G/H, which implies that there exist $h', k' \in H$ with $d(h, h'), d(k, k') < \beta$. Lemma 7 ensures that h' and k' do not commute, which contradicts Theorem 6. $\square$

4 The Proof when G is Simple

In this section, we give the proof of the main theorem in the case where H is nondiscrete and G is simple. The idea in this case is to show that because the Lie algebra $\mathfrak{h}$ of H cannot be a G-invariant subspace of $\mathfrak{g}$, the action of G automatically moves it quite a bit: this is made precise by Theorem 10. Since $\mathfrak{h}$ is invariant under the action of H, this will force G/H to have large diameter in the operator norm.

We begin with some general remarks about angles between subspaces of a Hilbert space. Let V be a real Hilbert space, and let $U, W \subseteq V$ be linear subspaces. The angle $\angle(U, W)$ between U and W is defined to be

$$\max\Big(\sup_{u\in U-\{0\}} \inf_{w\in W-\{0\}} |\angle(u, w)|, \sup_{w\in W-\{0\}} \inf_{u\in U-\{0\}} |\angle(u, w))|\Big).$$

Note that for a fixed unit vector $u \in U$, the cosine of the minimal angle $\angle(u, w)$ with $w \in W$ is equal to the length of the orthogonal projection of u onto $W^\perp$. Thus, the sine of the minimal (positive) angle is equal to the length of the orthogonal projection of u onto $W^\perp$. Consequently we have

$$\sin(\sup_{u \in U - \{0\}} \inf_{w \in W - \{0\}} |\angle(u, w)|) = \sup_{||u||=1, ||w^\perp||=1} \langle u, w^\perp \rangle$$

which is symmetric in U and $W^\perp$. From this symmetry we can deduce:

Lemma 8. *For any pair of subspaces $U, W \subseteq V$, the angle $\angle(U, W)$ is equal to the angle $\angle(U^\perp, W^\perp)$.*

We will also need the following elementary fact:

Lemma 9. *Let V be a finite-dimensional Hilbert space, and let A be an endomorphism of V having rank k. Then $|\operatorname{Tr}(A)| \leq k|A|$.*

Proof. Choose an orthonormal basis $\{v_i\}_{1 \leq i \leq n}$ for V having the property that $Av_i = 0$ for $i > k$. Then

$$|\operatorname{Tr}(A)| = |\sum_i \langle v_i, Av_i \rangle| \leq \sum_{1 \leq i \leq k} |\langle v_i, Av_i \rangle| \leq \sum_{1 \leq i \leq k} |A| = k|A|$$

□

We now proceed to the main point.

Theorem 10. *Let G be a compact Lie group acting irreducibly on a (necessarily finite dimensional) complex Hilbert space V. Let $W \neq 0, V$ be a nontrivial subspace. Then there exists $g \in G$ such that $\angle(W, gW) \geq \frac{\pi}{4}$.*

Proof. Suppose, to the contrary, that $\angle(W, gW) < \frac{\pi}{4}$ for all $g \in G$. Let V have dimension n. Replacing W by $W^\perp$ if necessary, we may assume that the dimension k of W satisfies $k \leq \frac{n}{2}$.For any subspace $U \subseteq V$, we let Π_U denote the orthogonal projection onto U.

For each $g \in G$, projection from gW onto $W^\perp$ or from $W^\perp$ to gW shrinks lengths by a factor of $\sin \angle(W, gW) \leq \sin \frac{\pi}{4}$ at least. It follows that

$$|\Pi_{W^\perp} \Pi_{gW} \Pi_{W^\perp}| \leq |\Pi_{W^\perp} \Pi_{gW}|\ |\Pi_{gW} \Pi_{W^\perp}| < \frac{1}{2}.$$

Using the identity $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$, we deduce

$$\begin{aligned}\mathrm{Tr}(\Pi_{gW}\Pi_{W^\perp}) &= \mathrm{Tr}(\Pi_{gW}\Pi_{W^\perp}\Pi_{W^\perp}) \\ &= \mathrm{Tr}(\Pi_{W^\perp}\Pi_{gW}\Pi_{W^\perp}) \leq k|\Pi_{W^\perp}\Pi_{gW}\Pi_{W^\perp}| \\ &< \tfrac{k}{2}.\end{aligned}$$

Integrating this result over G (with respect to a Haar measure which is normalized so that $\int_G 1 = 1$), we deduce

$$\mathrm{Tr}((\int_G \Pi_{gW})\Pi_{W^\perp}) = \int_G \mathrm{Tr}(\Pi_{gW}\Pi_{W^\perp}) < \frac{n}{2}.$$

On the other hand, $\int_G \Pi_{gW}$ is a G-invariant element of $\mathrm{End}(V)$. Since V is irreducible, Schur's lemma implies that $\int_G \Pi_{gW} = \lambda 1_V$ for some scalar $\lambda \in \mathbb{C}$. We can compute λ by taking traces:

$$\begin{aligned}n\lambda &= \mathrm{Tr}(\lambda 1_V) \\ &= \mathrm{Tr}(\textstyle\int_G \Pi_{gW}) \\ &= \textstyle\int_G \mathrm{Tr}(\Pi_{gW}) = k,\end{aligned}$$

so that $\lambda = \frac{k}{n}$. Thus $\frac{k(n-k)}{n} = \mathrm{Tr}(\frac{k}{n}\Pi_W^\perp) < \frac{k}{2}$, so that $2(n-k) < n$, a contradiction. □

From Theorem 10, one can easily deduce the analogous result in the case when V is a real Hilbert space, provided that $V \otimes_{\mathbb{R}} \mathbb{C}$ remains an irreducible representation of G. Using this, we can easily complete the proof of Theorem 1 in the case where G is simple and H is nondiscrete (with an even better constant).

Proof. Let $\mathfrak{h}$ denote the Lie algebra of H. Since $H \neq G$ and G is connected, $\mathfrak{h} \subsetneq \mathfrak{g}$. Since H is nondiscrete, $\mathfrak{h} \neq 0$. Since $\mathfrak{g} \otimes_{\mathbb{R}} \mathbb{C}$ is an irreducible representation of G, we deduce that there exists $g \in G$ such that $\angle(g\mathfrak{h}, \mathfrak{h}) \geq \frac{\pi}{4}$. Now one deduces that for any $h \in H$, $gh' \in gH$, the distance

$$d(gh', h) = |gh'h^{-1}|_G \geq \angle(gh'h^{-1}\mathfrak{h}, \mathfrak{h}) = \angle(g\mathfrak{h}, \mathfrak{h}) \geq \frac{\pi}{4}.$$

It follows that the distance between the cosets gH and H in G/H is at least $\frac{\pi}{4}$. □

5 The General Case

We now know that Theorem 1 is valid under the additional assumption that the group G is simple. We will complete the proof by showing how to reduce to this case. The main tool is the following observation:

Proposition 11. *Let $\pi : G \to G'$ be a surjection of compact connected Lie groups with trivial center, let H be a closed subgroup of G and $H' = \pi(H)$ its image in G'. Then $\mathrm{diam}(G'/H') \leq \mathrm{diam}(G/H)$.*

Proof. For any points $x', y' \in G'/H'$, we can lift them to a pair of points $x, y \in G/H$. It will suffice to show $d_{G/H}(x,y) \geq d_{G'/H'}(x',y')$. The left hand side is equal to

$$\inf_{gx=y} |g|_G$$

and the right hand side to

$$\inf_{g'x'=y'} |g'|_{G'}.$$

To complete the proof, it suffices to show that $|g|_G \geq |\pi(g)|_{G'}$. This follows immediately since we may identify the Lie algebra $\mathfrak{g}'$ of G' with a direct summand of $\mathfrak{g}$. $\square$

Now assume that G is a compact, connected Lie group with trivial center. Then it is a product of simple factors $\{G_\alpha\}_{\alpha \in \Lambda}$. Let $\pi_\alpha : G \to G_\alpha$ denote the projection. Let $H \subsetneq G$ be a closed subgroup. If $\pi_\alpha H \neq G_\alpha$ for some $\alpha \in \Lambda$, then $\mathrm{diam}(G/H) \geq \mathrm{diam}(G_\alpha/\pi_\alpha H) \geq \beta$ and we are done. Otherwise, π_α induces a surjection of Lie algebras $\mathfrak{h} \to \mathfrak{g}_\alpha$ for each α. By the structure theory of reductive Lie algebras, we deduce that $\mathfrak{h} = \mathfrak{h}_\alpha \oplus \mathfrak{k}_\alpha$, where π_α is zero on $\mathfrak{k}_\alpha$ and induces an isomorphism $\mathfrak{h}_\alpha \simeq \mathfrak{g}_\alpha$. Since $\mathfrak{h}_\alpha$ is therefore simple, $\mathfrak{k}_\alpha$ may be characterized as the centralizer of $\mathfrak{h}_\alpha$ in $\mathfrak{h}$.

Since $H \neq G$ and G is connected, H must have smaller dimension than G. It follows that the subalgebras $\mathfrak{h}_\alpha \subseteq \mathfrak{h}$ cannot all be distinct. Choose $\alpha, \alpha' \in \Lambda$ with $\mathfrak{h}_\alpha = \mathfrak{h}_{\alpha'}$. The the map $H \to G_\alpha \times G_{\alpha'}$ is not surjective on Lie algebras. Without loss of generality, we may replace G by $G_\alpha \times G_{\alpha'}$ and H by its image in $G_\alpha \times G_{\alpha'}$.

Since the Lie algebra of H now maps isomorphically onto the Lie algebras of the factors G_α and $G_{\alpha'}$, it follows that the connected component H_0 of the identity in H is isomorphic to G_α, which is included diagonally in $G_\alpha \times G_{\alpha'}$. Then $H = H_0(H \cap (G_\alpha \times 1))$. The intersection $K = H \cap (G_\alpha \times 1)$ is normalized by $H_0 = \{(g, g) : g \in G_\alpha\}$, hence it is normalized by $G_\alpha \times \{e\}$. Since $G_{\alpha'}$ is simple, we deduce that $K = \{e\}$. Thus $H = H_0$ is embedded diagonally in $G_\alpha \times G_{\alpha'}$. We have already considered this case in Example 2, where we saw that the diameter of G'/H' is at least $\frac{\pi}{2}$.

Remark 12. If we restrict our attention to the case where H is a *connected* subgroup of G, then our proof gives a better lower bound of $\frac{\pi}{4}$.

References

[NC] Nielsen, M.A., Chuang, I.L., *Quantum computation and quantum information.* Cambridge University Press, Cambridge, 2000. xxvi+676 pp.