

On Golden Gates and Discrepancy

Examining the Efficiency of Universal Gate Sets

Brent Mode

University of Louisville

August 9, 2017

Advisor: Dr. Steven Damelin



Quantum Computation v. Classical Computation

Classical Computation

- Classical computers, or just computers, rely on Boolean logic gates to execute programs.

Quantum Computation v. Classical Computation

Classical Computation

- Classical computers, or just computers, rely on Boolean logic gates to execute programs.
- All classical programs are formed from a combination of AND, OR, and NOT gates.

Quantum Computation v. Classical Computation

Classical Computation

- Classical computers, or just computers, rely on Boolean logic gates to execute programs.
- All classical programs are formed from a combination of AND, OR, and NOT gates.
- These programs are synthesized exactly, since the spectrum of possible programs is discrete.

Quantum Computation v. Classical Computation

Classical Computation

- Classical computers, or just computers, rely on Boolean logic gates to execute programs.
- All classical programs are formed from a combination of AND, OR, and NOT gates.
- These programs are synthesized exactly, since the spectrum of possible programs is discrete.
- In other words, if you can dream it, it can be done exactly.

Quantum Computation v. Classical Computation

Quantum Computation

- Quantum computing utilizes a quantum system consisting of two discrete states, $|0\rangle$ and $|1\rangle$.

Quantum Computation v. Classical Computation

Quantum Computation

- Quantum computing utilizes a quantum system consisting of two discrete states, $|0\rangle$ and $|1\rangle$.
- Thus, a single qubit is in the state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$.

Quantum Computation v. Classical Computation

Quantum Computation

- Quantum computing utilizes a quantum system consisting of two discrete states, $|0\rangle$ and $|1\rangle$.
- Thus, a single qubit is in the state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$.
- While a classical logic gate takes one or two inputs and returns a single output, a quantum logic gate acts as a linear map on $|\psi\rangle$.

Quantum Computation v. Classical Computation

Quantum Computation

- Quantum computing utilizes a quantum system consisting of two discrete states, $|0\rangle$ and $|1\rangle$.
- Thus, a single qubit is in the state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$.
- While a classical logic gate takes one or two inputs and returns a single output, a quantum logic gate acts as a linear map on $|\psi\rangle$.
- A 1-qubit quantum gate X acts on $|\psi\rangle$ to produce $|\psi'\rangle$.

Quantum Computation v. Classical Computation

Quantum Computation

- Quantum computing utilizes a quantum system consisting of two discrete states, $|0\rangle$ and $|1\rangle$.
- Thus, a single qubit is in the state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$.
- While a classical logic gate takes one or two inputs and returns a single output, a quantum logic gate acts as a linear map on $|\psi\rangle$.
- A 1-qubit quantum gate X acts on $|\psi\rangle$ to produce $|\psi'\rangle$.
- While classical logic gates are discrete, X can be any 2×2 matrix such that, since $|\psi|^2 = 1$, then $|\psi'|^2 = 1$.

An Unfortunate Number of Definitions

- *Unitary Group* - The group of all 1-qubit quantum gates is defined as:
$$U(2) = \{X \in GL_2(\mathbb{C}) \mid X^\dagger X = I\}.$$

An Unfortunate Number of Definitions

- *Unitary Group* - The group of all 1-qubit quantum gates is defined as:
 $U(2) = \{X \in GL_2(\mathbb{C}) \mid X^\dagger X = I\}.$

- *Special Unitary Group* - This can be simplified by the mapping $\frac{X}{\sqrt{|X|}}$
to be: $SU(2) = \{X \in U(2) \mid \det X = 1\}.$

An Unfortunate Number of Definitions

- *Unitary Group* - The group of all 1-qubit quantum gates is defined as:
 $U(2) = \{X \in GL_2(\mathbb{C}) \mid X^\dagger X = I\}$.
- *Special Unitary Group* - This can be simplified by the mapping $\frac{X}{\sqrt{|X|}}$ to be: $SU(2) = \{X \in U(2) \mid \det X = 1\}$.
- *Projective Special Unitary Group* - Further, for quantum gates it is also valid to view the gates X and $-X$ as the same, which leads us to:
 $PSU(2) = SU(2)/Z(SU(2))$.

An Unfortunate Number of Definitions

- *Unitary Group* - The group of all 1-qubit quantum gates is defined as:
 $U(2) = \{X \in GL_2(\mathbb{C}) \mid X^\dagger X = I\}$.
- *Special Unitary Group* - This can be simplified by the mapping $\frac{X}{\sqrt{|X|}}$ to be: $SU(2) = \{X \in U(2) \mid \det X = 1\}$.
- *Projective Special Unitary Group* - Further, for quantum gates it is also valid to view the gates X and $-X$ as the same, which leads us to: $PSU(2) = SU(2)/Z(SU(2))$.
- *Metric on $SU(2)$* - We need to define a notion of distance on $SU(2)$, so we use the invariant metric,
$$d_{SU(2)}^2(X, Y) = 1 - \frac{|Tr(X^\dagger Y)|}{2}, \text{ where } d : SU(2) \rightarrow \mathbb{R}_{\geq 0}.$$

The Problem at Hand

- The difficulty in quantum computing is the overwhelming number of possible programs available to us as quantum logic gate circuits.

The Problem at Hand

- The difficulty in quantum computing is the overwhelming number of possible programs available to us as quantum logic gate circuits.
- Unlike in classical computing, it is impossible to exactly synthesize every possible program using a handful of gates.

The Problem at Hand

- The difficulty in quantum computing is the overwhelming number of possible programs available to us as quantum logic gate circuits.
- Unlike in classical computing, it is impossible to exactly synthesize every possible program using a handful of gates.
- This is the same problem that occurs when comparing the rational numbers to the real numbers.

The Problem at Hand

- The difficulty in quantum computing is the overwhelming number of possible programs available to us as quantum logic gate circuits.
- Unlike in classical computing, it is impossible to exactly synthesize every possible program using a handful of gates.
- This is the same problem that occurs when comparing the rational numbers to the real numbers.
- What is needed is a way to approximate every element of $SU(2)$ using a circuit built from a small set of specially chosen quantum gates.

The Problem at Hand

- The difficulty in quantum computing is the overwhelming number of possible programs available to us as quantum logic gate circuits.
- Unlike in classical computing, it is impossible to exactly synthesize every possible program using a handful of gates.
- This is the same problem that occurs when comparing the rational numbers to the real numbers.
- What is needed is a way to approximate every element of $SU(2)$ using a circuit built from a small set of specially chosen quantum gates.
- The problem is then two-fold: Find a good gate set and come up with an approximation algorithm.

An Example Universal Gate Set

- A universal gate set is a 'good' gate set: The group generated by the elements in the set is dense in $SU(2)$.

An Example Universal Gate Set

- A universal gate set is a 'good' gate set: The group generated by the elements in the set is dense in $SU(2)$.

- My work has focused on the set T that is defined below:

$$T = \{s_1, s_2, s_3, s_1^{-1}, s_2^{-1}, s_3^{-1}, I, iX, iY, iZ\}, \text{ where}$$
$$s_1 = \frac{1}{\sqrt{5}}(I + 2iX), s_2 = \frac{1}{\sqrt{5}}(I + 2iY), s_3 = \frac{1}{\sqrt{5}}(I + 2iZ), \text{ and } X, Y, \text{ and } Z \text{ are the Pauli matrices.}$$

An Example Universal Gate Set

- A universal gate set is a 'good' gate set: The group generated by the elements in the set is dense in $SU(2)$.
- My work has focused on the set T that is defined below:
$$T = \{s_1, s_2, s_3, s_1^{-1}, s_2^{-1}, s_3^{-1}, I, iX, iY, iZ\},$$
 where
$$s_1 = \frac{1}{\sqrt{5}}(I + 2iX), s_2 = \frac{1}{\sqrt{5}}(I + 2iY), s_3 = \frac{1}{\sqrt{5}}(I + 2iZ),$$
 and X , Y , and Z are the Pauli matrices.
- These elements are combined to form reduced words of increasing length, with iX , iY , and iZ then inserted at the front to quadruple the number of elements of a certain length.

An Example Universal Gate Set

- A universal gate set is a 'good' gate set: The group generated by the elements in the set is dense in $SU(2)$.
- My work has focused on the set T that is defined below:
$$T = \{s_1, s_2, s_3, s_1^{-1}, s_2^{-1}, s_3^{-1}, I, iX, iY, iZ\}$$
, where
$$s_1 = \frac{1}{\sqrt{5}}(I + 2iX), s_2 = \frac{1}{\sqrt{5}}(I + 2iY), s_3 = \frac{1}{\sqrt{5}}(I + 2iZ)$$
, and X , Y , and Z are the Pauli matrices.
- These elements are combined to form reduced words of increasing length, with iX , iY , and iZ then inserted at the front to quadruple the number of elements of a certain length.
- We say that $\Omega = \langle T \rangle$ is the group generated by T .

An Example Universal Gate Set

- A universal gate set is a 'good' gate set: The group generated by the elements in the set is dense in $SU(2)$.
- My work has focused on the set T that is defined below:
$$T = \{s_1, s_2, s_3, s_1^{-1}, s_2^{-1}, s_3^{-1}, I, iX, iY, iZ\}$$
, where
$$s_1 = \frac{1}{\sqrt{5}}(I + 2iX), s_2 = \frac{1}{\sqrt{5}}(I + 2iY), s_3 = \frac{1}{\sqrt{5}}(I + 2iZ)$$
, and $X, Y,$
and Z are the Pauli matrices.
- These elements are combined to form reduced words of increasing length, with $iX, iY,$ and iZ then inserted at the front to quadruple the number of elements of a certain length.
- We say that $\Omega = \langle T \rangle$ is the group generated by T .
- Then $V(t)$ is defined as the set of elements in Ω of length at most t .

Connection to Discrepancy

A Different Way to Approach the Problem

- Recall that $PSU(2)$ is just as valid a group for representing gates as $SU(2)$.

Connection to Discrepancy

A Different Way to Approach the Problem

- Recall that $PSU(2)$ is just as valid a group for representing gates as $SU(2)$.
- It is interestingly the case that $PSU(2) \approx SO(3)$ and that $SU(2) \approx S^3$, where the $SO(3)$ is the rotation group of the sphere S^2 , the first relation is by isomorphism, and the second relation is by diffeomorphism.

Connection to Discrepancy

A Different Way to Approach the Problem

- Recall that $PSU(2)$ is just as valid a group for representing gates as $SU(2)$.
- It is interestingly the case that $PSU(2) \approx SO(3)$ and that $SU(2) \approx S^3$, where the $SO(3)$ is the rotation group of the sphere S^2 , the first relation is by isomorphism, and the second relation is by diffeomorphism.
- Thus, it follows that elements of Ω correspond to solutions to: $x_1^2 + x_2^2 + x_3^2 + x_4^2 = 5^t$, and can be projected onto the sphere.

Connection to Discrepancy

A Different Way to Approach the Problem

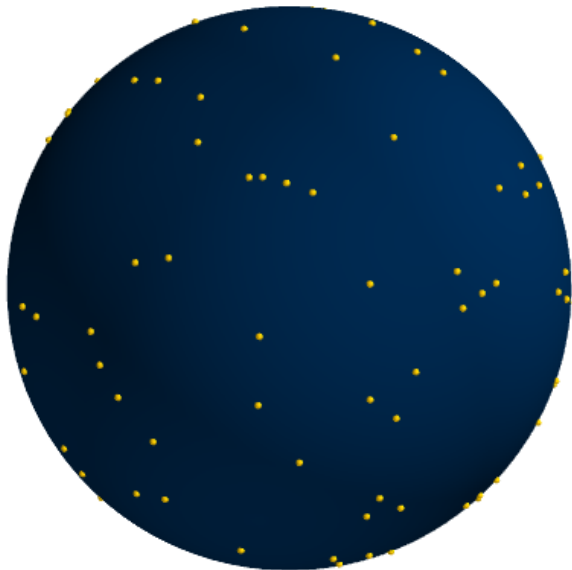
- Recall that $PSU(2)$ is just as valid a group for representing gates as $SU(2)$.
- It is interestingly the case that $PSU(2) \approx SO(3)$ and that $SU(2) \approx S^3$, where the $SO(3)$ is the rotation group of the sphere S^2 , the first relation is by isomorphism, and the second relation is by diffeomorphism.
- Thus, it follows that elements of Ω correspond to solutions to: $x_1^2 + x_2^2 + x_3^2 + x_4^2 = 5^t$, and can be projected onto the sphere.
- This is a well-studied problem in number theory and lends itself to being studied numerically.

Connection to Discrepancy

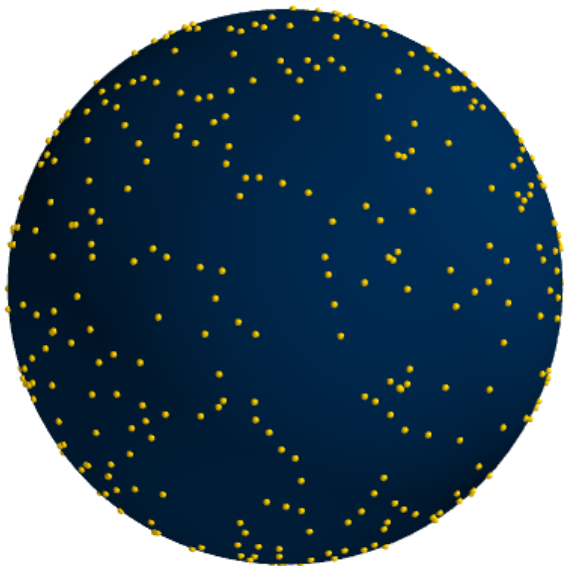
A Different Way to Approach the Problem

- Recall that $PSU(2)$ is just as valid a group for representing gates as $SU(2)$.
- It is interestingly the case that $PSU(2) \approx SO(3)$ and that $SU(2) \approx S^3$, where the $SO(3)$ is the rotation group of the sphere S^2 , the first relation is by isomorphism, and the second relation is by diffeomorphism.
- Thus, it follows that elements of Ω correspond to solutions to: $x_1^2 + x_2^2 + x_3^2 + x_4^2 = 5^t$, and can be projected onto the sphere.
- This is a well-studied problem in number theory and lends itself to being studied numerically.
- In many ways, we can change the quantum problem to a study of how well this point set is distributed on the sphere.

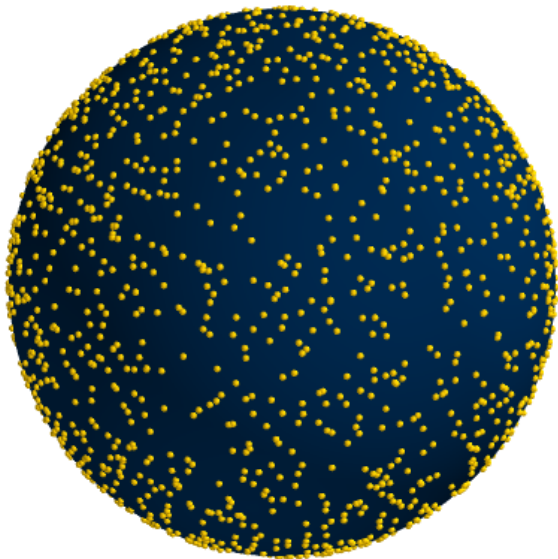
The Points of $V(2)$



The Points of $V(3)$



The Points of $V(4)$



Efficiency and Discrepancy

Solovay-Kitaev and Efficiency

- The Solovay-Kitaev Theorem states that for $X \in SU(2)$ and a symmetric universal set of quantum gates, for a given $\varepsilon > 0$, there exists some $\omega \in \Omega$ of length $O(\log^c(\frac{1}{\varepsilon}))$ approximating X within distance ε .

Efficiency and Discrepancy

Solovay-Kitaev and Efficiency

- The Solovay-Kitaev Theorem states that for $X \in SU(2)$ and a symmetric universal set of quantum gates, for a given $\varepsilon > 0$, there exists some $\omega \in \Omega$ of length $O(\log^c(\frac{1}{\varepsilon}))$ approximating X within distance ε .
- This guarantees that an approximation exists, but does not robustly address the relative efficiency of different choices of gate set.

Efficiency and Discrepancy

Solovay-Kitaev and Efficiency

- The Solovay-Kitaev Theorem states that for $X \in SU(2)$ and a symmetric universal set of quantum gates, for a given $\varepsilon > 0$, there exists some $\omega \in \Omega$ of length $O(\log^c(\frac{1}{\varepsilon}))$ approximating X within distance ε .
- This guarantees that an approximation exists, but does not robustly address the relative efficiency of different choices of gate set.
- To that end, Sarnak introduces the covering exponent, defined below, to serve this purpose:

$$K(T) \equiv \limsup_{\varepsilon \rightarrow 0} \frac{\log |V(t_\varepsilon)|}{\log\left(\frac{1}{\mu(B(\varepsilon))}\right)},$$

where t_ε is the smallest t such that for the given ε , $V(t_\varepsilon)$ approximates all of $SU(2)$ within a distance ε , $B(\varepsilon)$ is an arbitrary ball of radius ε in $SU(2)$ and μ is a Haar measure on $SU(2)$.

Efficiency and Discrepancy

Bounds on K

- From the definition, it follows that if T approximates all of $SU(2)$ with optimal efficiency, then $K(T) = 1$.

Bounds on K

- From the definition, it follows that if T approximates all of $SU(2)$ with optimal efficiency, then $K(T) = 1$.
- This is not the case: Sarnak has proven that $\frac{4}{3} \leq K(T) \leq 2$.

Efficiency and Discrepancy

Bounds on K

- From the definition, it follows that if T approximates all of $SU(2)$ with optimal efficiency, then $K(T) = 1$.
- This is not the case: Sarnak has proven that $\frac{4}{3} \leq K(T) \leq 2$.
- However, T is optimally efficient *almost everywhere*.

Bounds on K

- From the definition, it follows that if T approximates all of $SU(2)$ with optimal efficiency, then $K(T) = 1$.
- This is not the case: Sarnak has proven that $\frac{4}{3} \leq K(T) \leq 2$.
- However, T is optimally efficient *almost everywhere*.
- It is suspected that $K(T) = \frac{4}{3}$; what remains is for this to be proven or refuted.

Efficiency and Discrepancy

Conjecture on K

- We conjecture $\varepsilon \leq f(t_\varepsilon)5^{-t_\varepsilon/4}$ for a function $f : (0, \infty) \rightarrow (1, \infty)$ satisfying:

$$\lim_{t_\varepsilon \rightarrow \infty} \log(f(t_\varepsilon))/t_\varepsilon$$

exists with value 0.

Efficiency and Discrepancy

Conjecture on K

- We conjecture $\varepsilon \leq f(t_\varepsilon)5^{-t_\varepsilon/4}$ for a function $f : (0, \infty) \rightarrow (1, \infty)$ satisfying:

$$\lim_{t_\varepsilon \rightarrow \infty} \log(f(t_\varepsilon))/t_\varepsilon$$

exists with value 0.

- Let $\nu(5^{t_\varepsilon})$ denote the set of integer solutions of the quadratic form:
 $x_1^2 + x_2^2 + x_3^2 + x_4^2 = 5^{t_\varepsilon}$.

Efficiency and Discrepancy

Conjecture on K

- We conjecture $\varepsilon \leq f(t_\varepsilon)5^{-t_\varepsilon/4}$ for a function $f : (0, \infty) \rightarrow (1, \infty)$ satisfying:

$$\lim_{t_\varepsilon \rightarrow \infty} \log(f(t_\varepsilon))/t_\varepsilon$$

exists with value 0.

- Let $\nu(5^{t_\varepsilon})$ denote the set of integer solutions of the quadratic form:
 $x_1^2 + x_2^2 + x_3^2 + x_4^2 = 5^{t_\varepsilon}$.
- Let $M \equiv M_{S^3}(\mathcal{N})$ denote the covering radius of the points $\mathcal{N} = \nu(5^{t_\varepsilon}) \cup \nu(5^{t_\varepsilon-1})$ on the sphere S^3 in \mathbb{R}^4 .

Conjecture on K

- We conjecture $\varepsilon \leq f(t_\varepsilon)5^{-t_\varepsilon/4}$ for a function $f : (0, \infty) \rightarrow (1, \infty)$ satisfying:

$$\lim_{t_\varepsilon \rightarrow \infty} \log(f(t_\varepsilon))/t_\varepsilon$$

exists with value 0.

- Let $\nu(5^{t_\varepsilon})$ denote the set of integer solutions of the quadratic form:
 $x_1^2 + x_2^2 + x_3^2 + x_4^2 = 5^{t_\varepsilon}$.
- Let $M \equiv M_{S^3}(\mathcal{N})$ denote the covering radius of the points $\mathcal{N} = \nu(5^{t_\varepsilon}) \cup \nu(5^{t_\varepsilon-1})$ on the sphere S^3 in \mathbb{R}^4 .
- Then $M \sim f(\log N)N^{-1/4}$. Here $N \equiv N(\varepsilon) = 6 \cdot 5^{t_\varepsilon} - 2$.

Efficiency and Discrepancy

Conjecture on K

- We conjecture $\varepsilon \leq f(t_\varepsilon)5^{-t_\varepsilon/4}$ for a function $f : (0, \infty) \rightarrow (1, \infty)$ satisfying:

$$\lim_{t_\varepsilon \rightarrow \infty} \log(f(t_\varepsilon))/t_\varepsilon$$

exists with value 0.

- Let $\nu(5^{t_\varepsilon})$ denote the set of integer solutions of the quadratic form:
 $x_1^2 + x_2^2 + x_3^2 + x_4^2 = 5^{t_\varepsilon}$.
- Let $M \equiv M_{S^3}(\mathcal{N})$ denote the covering radius of the points $\mathcal{N} = \nu(5^{t_\varepsilon}) \cup \nu(5^{t_\varepsilon-1})$ on the sphere S^3 in \mathbb{R}^4 .
- Then $M \sim f(\log N)N^{-1/4}$. Here $N \equiv N(\varepsilon) = 6 \cdot 5^{t_\varepsilon} - 2$.
- Assuming this conjecture implies that $K(T) \leq \frac{4}{3}$ and then also that $K(T) = \frac{4}{3}$.

Efficiency and Discrepancy

An Invalid Example

On the other hand for a function which grows faster, say

$$f(t_\varepsilon) = t_\varepsilon^{t_\varepsilon}$$

we easily have

$$\log(f(t_\varepsilon))/t_\varepsilon \sim (\log(\log N))$$

which diverges for large enough N .

Conclusions

- Quantum computing represents a fundamental departure from the classical algorithms of yesteryear.
- Quantum logic gates are represented by arbitrary unitary matrices.
- A major unsolved problem in quantum computing is determining the efficiencies of universal gate sets.
- One can view these gates as points on a sphere and use number theoretic tools like mesh norm and covering exponent.
- We conjecture a condition on mesh norm which allows proof that

$$K(T) = \frac{4}{3}.$$

References

- 1 S.B. Damelin, Q. Liang, B.A.W. Mode, "On Golden Gates and Discrepancy," arxiv:1506.05785 (2017) preprint. Submitted to J. Complex.
- 2 A. Bocharov, Y. Gurevich, and K. Svore. "Efficient decomposition of single-qubit gates into V basis circuits," Phys. Rev. A 88.1 (2013): 012313.
- 3 J. Bourgain, P. Sarnak, and Z. Rudnick, "Local statistics of lattice points on the sphere," arXiv preprint arXiv:1204.0134 (2012).
- 4 C.M. Dawson, M.A. Nielsen, "The Solovay-Kitaev Algorithm," QIC, Vol 6, No 1 (2006), pp 081-095.
- 5 P. Sarnak, "Letter to Scott Aaronson and Andy Pollington on the Solovay-Kitaev Theorem and Golden Gates," <http://publications.ias.edu/sarnak/paper/2637> (2015).
- 6 N. Ross and P. Selinger, "Optimal ancilla-free Clifford+T approximation of z-rotations," QIC. **16**(2016) (11-12), pp 901-953.

Acknowledgments

- Thanks to Dr. Damelin for his collaboration and insights.
- Research for this REU was supported by funding from the National Science Foundation.

Definition of an Invariant Metric

A metric or distance function on a set X is defined as $d : X \times X \rightarrow \mathbb{R}_{\geq 0}$ satisfying $\forall x, y, z \in X$:

- 1 $d(x, y) \geq 0$
- 2 $d(x, y) = 0 \Leftrightarrow x = y$
- 3 $d(x, y) = d(y, x)$
- 4 $d(x, z) \leq d(x, y) + d(y, z)$.

Definition of a Ball A ball in a metric space is defined such that $B(\gamma, \varepsilon) = \{x \in G \mid d(x, \gamma) < \varepsilon\}$.

Definition of a Haar Metric

Let X be a set and $\mathcal{P}(X)$ be the power set of X . Then $\Sigma \subseteq \mathcal{P}(X)$ is called a σ -algebra if it satisfies the following:

- 1 $X \in \Sigma$
- 2 $\forall A \in \Sigma, X - A \in \Sigma$
- 3 $\forall A_1, A_2, \dots \in \Sigma, A_1 \cup A_2 \cup \dots \in \Sigma$

The elements of a σ -algebra are called measurable sets.

Definition of a Haar Metric

In a topological space X , a Borel set is any set that can be formed from open sets using countable unions, countable intersections, and relative complements. The collection of all Borel sets on X forms a σ -algebra called the Borel algebra. Further, the Borel algebra is the smallest algebra containing all open sets.

In a metric space (X, d) , compactness is equivalent to the statement that every infinite subset of X has at least one limit point in X . Similarly, a compact group is a group whose topology is compact.

Definition of a Haar Measure

Let G be a compact group. A normalized Haar measure $\mu : \Sigma \rightarrow \mathbb{R}_{\geq 0}$ on G where Σ is the Borel algebra of G satisfies:

- 1 $\mu(G) = 1$
- 2 $\forall x \in G$ and $S \in \Sigma, \mu(xS) = \mu(S)$

Definition of Mesh Norm The mesh norm or covering radius of a point set with respect to S^d is given as

$$M(\mathcal{N}) \equiv \max_{y \in S^d} \min_{x \in \mathcal{N}} |x - y|$$

where \mathcal{N} is the point set in question. Intuitively, the mesh norm is the radius that is required for balls centered at points of \mathcal{N} to cover all of S^d .