Foundations of Multiplicative Combinatorics

Alien Mathematicians

Outline

1. Introduction
2. Basic Definitions
3. Main Results
4. Future Directions
5. Extended Definitions and Notations
6. Rigorous Proofs of Key Theorems
7. Applications to Number Theory
8. Future Directions

Introduction to Multiplicative Combinatorics

- Multiplicative Combinatorics explores the combinatorial structure of sets under multiplication.
- Analogous to additive combinatorics but focused on multiplicative operations.
- Applications range from number theory to cryptography.

Product Set Definition

Let A be a finite subset of a group G under multiplication.

Definition

The *product set* $A \cdot A$ is defined as:

$$A \cdot A = \{a \cdot b : a, b \in A\}$$

- This section investigates properties of $A \cdot A$ and growth under multiplication.

Example of Product Set

Example

Let $A = \{2, 3, 5\}$ in the group $\mathbb{Z}_{>0}$. Then $A \cdot A = \{4, 6, 9, 10, 15, 25\}$.

Growth in Product Sets

- One of the core questions: How large is $A \cdot A$ compared to A?
- Growth results: Under certain conditions, $|A \cdot A|$ grows significantly larger than $|A|$.

Key Theorems in Multiplicative Combinatorics

Theorem (Growth Theorem)

If $A \subset G$ and A satisfies certain properties, then:

$$|A \cdot A| \geq c|A|^{1+\epsilon}$$

for some constants c and $\epsilon > 0$.

- This theorem parallels key results in additive combinatorics.

Potential Applications

- Multiplicative combinatorics can impact:
    - Prime factorization and distribution of prime numbers.
    - Sieve methods used in analytic number theory.
    - Cryptographic algorithms relying on multiplicative properties.

Expansion for Future Research

- Open questions and problems for further research:
  - Infinite expansion of product set properties.
  - Connections between multiplicative combinatorics and additive number theory.
  - Applications to complex structures in algebraic and analytic contexts.

Extended Product Set Definition I

In multiplicative combinatorics, the product set $A \cdot A$ provides a fundamental construct for studying growth properties and structural results. To generalize, we define:

Definition (Higher-Order Product Set)

For any finite subset $A \subset G$, the *k-fold product set* $A^{(k)}$ is defined recursively as:

$$A^{(k)} = A^{(k-1)} \cdot A = \{a_1 \cdot a_2 \cdots a_k : a_i \in A \text{ for all } i\}.$$

where $A^{(1)} = A$.

Notation

We denote the cardinality of the k-fold product set by $|A^{(k)}|$.

Extended Product Set Definition II

- This recursive definition allows us to explore the growth rate of $|A^{(k)}|$ as k increases, particularly focusing on whether $|A^{(k)}|$ grows faster than linearly with respect to k.

Extended Example of Product Sets I

Example

Let $A = \{2, 3, 5\}$ in $\mathbb{Z}_{>0}$ under multiplication. We calculate higher-order product sets:

- $A^{(2)} = A \cdot A = \{4, 6, 9, 10, 15, 25\}$
- $A^{(3)} = A^{(2)} \cdot A = \{8, 12, 18, 20, 30, 45, 50, 75, 125\}$

Observing these sets, we see that $|A^{(k)}|$ increases with k, suggesting growth in the structure of product sets.

Growth Theorem in Product Sets: Statement I

One fundamental question in multiplicative combinatorics is how product sets grow. We state the following theorem:

Theorem (Product Set Growth Theorem)

Let $A \subset G$ be a finite subset of a group G under multiplication. There exists a constant $c > 1$ such that for sufficiently large k,

$$|A^{(k)}| \geq c^k |A|.$$

- This theorem implies exponential growth of $A^{(k)}$ in terms of k, under certain structural conditions of A and G.

Proof of the Product Set Growth Theorem (1/3) I

Proof of the Product Set Growth Theorem (1/3) II

Proof (1/3).

We begin by proving a base case for $k = 2$. Let $A \subset G$ be a finite set, and let $A \cdot A = \{a \cdot b : a, b \in A\}$.
Since G is a group, $A \cdot A$ contains all pairwise products of elements in A, and we consider two cases:

- If A is closed under multiplication, then $A \cdot A = A$ and there is no growth. This case is trivial.
- If A is not closed under multiplication, then $|A \cdot A| > |A|$.

Key Idea: We can apply the Plünnecke-Ruzsa inequality to estimate growth. This inequality states that if $|A \cdot A|$ grows, then for larger powers k, $|A^{(k)}|$ also grows significantly.
Assumption: We assume $|A \cdot A| \geq c|A|$ for some $c > 1$.
This completes the initial setup of the proof. $\square$

Proof of the Product Set Growth Theorem (2/3) I

Proof (2/3).

Continuing from the base case, we proceed by induction on k.
Inductive Hypothesis: Suppose that $|A^{(k)}| \geq c^k |A|$ for some $c > 1$.
Inductive Step: For $A^{(k+1)} = A^{(k)} \cdot A$, the cardinality satisfies:

$$|A^{(k+1)}| \geq |A^{(k)}| \cdot |A| / |A \cap A^{(k)}|.$$

Under the assumption that the intersection $|A \cap A^{(k)}|$ is bounded, this yields exponential growth in $|A^{(k+1)}|$.

This concludes the inductive step, which completes the proof. □

Proof of the Product Set Growth Theorem (3/3) I

Proof (3/3).

Finally, by combining the base case and the inductive step, we conclude that for all k,

$$|A^{(k)}| \geq c^k |A|,$$

proving the theorem. $\square$

Application: Cryptographic Implications I

- Product sets and their growth properties have implications for cryptography.
- Cryptographic algorithms that rely on multiplicative groups, such as RSA, are influenced by the growth of product sets.
- We can design more secure cryptographic systems by selecting groups with fast-growing product sets.

Open Problems in Multiplicative Combinatorics I

- Can we classify all groups G for which $|A^{(k)}|$ grows at an exponential rate?
- Explore the interplay between additive and multiplicative combinatorics by studying sets that exhibit slow additive growth but fast multiplicative growth.
- Investigate applications to the distribution of prime numbers, exploring whether similar growth properties apply to prime factorization.

References I

- Tao, T. and Vu, V. (2006). *Additive Combinatorics*. Cambridge University Press.
- Ruzsa, I. Z. (1996). "Sums of Finite Sets". *Number Theory*, 281-293.

Definition: Generalized Product Sets I

To further generalize the concept of product sets, we define the *generalized product set* based on subsets of different groups.

Definition (Generalized Product Set)

Let $A \subset G$ and $B \subset H$ be subsets of groups G and H, respectively. The *generalized product set* $A \cdot B$ is defined as:

$$A \cdot B = \{a \cdot b : a \in A, b \in B\}.$$

If $G = H$, this reduces to the standard product set definition.

- This definition enables the exploration of product sets across different group structures, which has applications in analyzing complex group interactions.

Definition: Higher-Order Product Growth Rate I

We introduce a formal measure for the growth rate of higher-order product sets.

Definition (Product Growth Rate)

Let $A \subset G$ be a finite subset of a group G, and consider the sequence $|A^{(k)}|$. The *product growth rate* $\gamma(A)$ is defined as:

$$\gamma(A) = \limsup_{k \to \infty} \sqrt[k]{|A^{(k)}|}.$$

Interpretation

- If $\gamma(A) > 1$, then A exhibits exponential growth under multiplication.
- If $\gamma(A) = 1$, the growth is linear or sublinear.

Theorem: Submultiplicative Growth in Product Sets I

Theorem (Submultiplicative Growth)

Let $A \subset G$ be a finite subset of a group G. For all $k, m \in \mathbb{N}$,

$$|A^{(k+m)}| \leq |A^{(k)}| \cdot |A^{(m)}|.$$

- This property, known as submultiplicative growth, implies that the sequence $|A^{(k)}|$ does not grow faster than multiplicatively.

Proof of Submultiplicative Growth Theorem (1/2) I

Proof (1/2).

To prove the submultiplicative property of $|A^{(k)}|$, we consider the definition of $A^{(k+m)}$:

$$A^{(k+m)} = \{a_1 \cdot a_2 \cdots a_{k+m} : a_i \in A\}.$$

For each $a_1, \ldots, a_k \in A$ and $b_1, \ldots, b_m \in A$, the elements $a_1 \cdots a_k$ and $b_1 \cdots b_m$ are in $A^{(k)}$ and $A^{(m)}$, respectively.
By combining elements, we observe that:

$$A^{(k+m)} \subseteq A^{(k)} \cdot A^{(m)}.$$

□

Proof of Submultiplicative Growth Theorem (2/2) I

Proof (2/2).

Therefore, the cardinality satisfies:

$$|A^{(k+m)}| \leq |A^{(k)}| \cdot |A^{(m)}|.$$

This completes the proof, establishing that $|A^{(k)}|$ grows submultiplicatively. $\square$

Application: Product Growth in Algebraic Groups I

- For subsets A within algebraic groups, product set growth can reveal information about the structure of the group.
- For example, if $A \subset G$ is a subset of an algebraic group over $\mathbb{Q}$, rapid growth in $|A^{(k)}|$ indicates that A spans a substantial portion of G.

Diagram: Growth of Product Sets I

$$\begin{tikzcd} A \arrow[r, "\cdot A"] & A \cdot A \arrow[r, "\cdot A"] & A^{(3)} \arrow[r, "\cdot A"] & A^{(4)} \end{tikzcd}$$

- This diagram represents the growth sequence $A \to A \cdot A \to A^{(3)} \to \cdots$, illustrating how the product set expands with each multiplication.

Additional References I

- Bourgain, J., Katz, N., & Tao, T. (2004). "A sum-product estimate in finite fields, and applications." *Geometric and Functional Analysis*, 14(1), 27–57.
- Tao, T. and Vu, V. (2006). *Additive Combinatorics*. Cambridge University Press.

Definition: Growth Dimension of a Set I

We introduce a novel concept in multiplicative combinatorics, the *growth dimension* of a subset within a group, to analyze the dimensional growth characteristics of product sets.

Definition (Growth Dimension)

Let $A \subset G$ be a finite subset of a group G. The *growth dimension* $\delta(A)$ of A is defined as:

$$\delta(A) = \lim_{k\to\infty} \frac{\log |A^{(k)}|}{k}.$$

- The growth dimension represents the asymptotic growth rate of $A^{(k)}$, providing a scalar measure of expansion over repeated multiplications.

Example: Growth Dimension of Arithmetic Progressions I

Example

Let $A = \{1, 2, 3, \ldots, n\} \subset \mathbb{Z}$, an arithmetic progression within the additive group of integers. The product set $A \cdot A = \{a + b : a, b \in A\}$ grows as k increases. By calculating $|A^{(k)}|$, we can estimate $\delta(A)$.

Theorem: Exponential Growth in Product Sets I

Theorem (Exponential Growth of Product Sets)

Let $A \subset G$ be a finite subset of a group G under multiplication. Then under certain non-triviality conditions, $|A^{(k)}|$ grows exponentially with k. Specifically, there exists a constant $C > 1$ such that:

$$|A^{(k)}| \geq C^k.$$

- This theorem highlights that under non-trivial group structures, product sets expand significantly.

Proof of Exponential Growth Theorem (1/4) I

Proof (1/4).

To prove exponential growth, we start by assuming that $A \subset G$ is not contained within any subgroup of G. This assumption ensures that new elements are generated in $A^{(k)}$ as k increases.

We proceed by induction on k, starting with the base case $k = 1$, where $|A^{(1)}| = |A|$. □

Proof of Exponential Growth Theorem (2/4) I

Proof (2/4).

For the inductive step, assume that $|A^{(k)}| \geq C^k$ for some constant $C > 1$. Consider $A^{(k+1)} = A^{(k)} \cdot A$. By the non-triviality of A, $A^{(k+1)}$ must contain new products not present in $A^{(k)}$, leading to:

$$|A^{(k+1)}| \geq C \cdot |A^{(k)}|.$$

□

Proof of Exponential Growth Theorem (3/4) I

Proof (3/4).

By the inductive hypothesis, $|A^{(k)}| \geq C^k$, so:

$$|A^{(k+1)}| \geq C \cdot C^k = C^{k+1}.$$

This completes the inductive step, proving that $|A^{(k)}| \geq C^k$ for all k. □

Proof of Exponential Growth Theorem (4/4) I

Proof (4/4).

Therefore, we conclude that $|A^{(k)}|$ exhibits exponential growth, as required. $\square$

Sieve Methods in Multiplicative Combinatorics I

- Sieve methods are used to study the distribution of prime numbers. In multiplicative combinatorics, we apply sieve techniques to product sets to understand the density of prime-related structures.
- For example, let $A \subset \mathbb{Z}$ be a set of integers. By analyzing $A \cdot A$ under sieve conditions, we can study the density of elements with certain divisibility properties.

Open Questions in Growth Dimension I

- Can the growth dimension $\delta(A)$ be classified for different types of subsets in various groups?
- Is there a universal constant $\delta(G)$ for each group G that bounds the growth dimension for all finite subsets $A \subset G$?
- What implications does the growth dimension have for cryptographic algorithms that rely on multiplicative groups?

Additional References I

- Helfgott, H. A. (2008). "Growth in SL3($\mathbb{Z}/p\mathbb{Z}$)". *Journal of the European Mathematical Society*, 10(3), 865–909.
- Iwaniec, H., & Kowalski, E. (2004). *Analytic Number Theory*. American Mathematical Society.

Definition: Multiplicative Density I

To analyze the distribution of elements in multiplicative subsets, we define the concept of *multiplicative density*.

Definition (Multiplicative Density)

Let $A \subset G$ be a finite subset of a group G under multiplication. The *multiplicative density* $d(A)$ of A in G is defined as:

$$d(A) = \frac{|A|}{|G|}.$$

If G is infinite, $d(A)$ can be defined as a limiting density, considering finite approximations of G.

- This concept is useful for comparing the relative "size" of product sets $A \cdot A$ within G.

Definition: Multiplicative Density II

- For example, if $d(A^{(k)})$ remains bounded away from zero as $k \to \infty$, A is said to have non-trivial growth density.

Theorem: Multiplicative Density and Growth Rate I

Theorem (Multiplicative Density and Growth Rate)

Let $A \subset G$ be a finite subset of a group G with multiplicative density $d(A) > 0$. Then, the product set $A^{(k)}$ satisfies:

$$d(A^{(k)}) \geq \frac{|A|}{|G|^k}.$$

Moreover, if A is not contained within any proper subgroup, then $d(A^{(k)})$ approaches a constant as $k \to \infty$.

- This theorem demonstrates that if A has a positive multiplicative density, its product sets can maintain a certain density even as k increases.

Proof of Multiplicative Density Theorem (1/3) I

Proof (1/3).

We begin by defining the base case for $k = 1$. For a finite subset $A \subset G$, we have:

$$d(A) = \frac{|A|}{|G|}.$$

Now, consider the product set $A \cdot A$ for $k = 2$. Since A is not contained within any proper subgroup of G, the product set $A \cdot A$ will contain new elements not in A. $\square$

Proof of Multiplicative Density Theorem (2/3) I

Proof (2/3).

By induction, assume that $d(A^{(k)}) \geq \frac{|A|}{|G|^k}$. We proceed by considering $A^{(k+1)} = A^{(k)} \cdot A$.

By construction, $A^{(k+1)}$ expands by including all products of elements from $A^{(k)}$ with elements from A. Therefore:

$$d(A^{(k+1)}) = \frac{|A^{(k+1)}|}{|G|} \geq \frac{|A^{(k)}| \cdot |A|}{|G|^2} = \frac{|A|}{|G|^{k+1}}.$$

□

Proof of Multiplicative Density Theorem (3/3) I

Proof (3/3).

Taking the limit as $k \to \infty$, if A is not in a proper subgroup, $d(A^{(k)})$ converges to a non-zero constant. Thus, A maintains a positive density under multiplication.

This completes the proof. $\square$

Cryptographic Implications of Product Growth I

- Product growth in groups has applications in cryptography, particularly in key exchange algorithms.
- For a finite subset $A \subset G$, rapid growth in $|A^{(k)}|$ provides a basis for cryptographic hardness, as recovering elements in $A^{(k)}$ from A becomes computationally intensive.

Definition: Multiplicative Expansion Factor I

To measure the expansion properties of a subset under multiplication, we define the *multiplicative expansion factor*.

Definition (Multiplicative Expansion Factor)

Let $A \subset G$ be a subset of a group G. The multiplicative expansion factor $\mu(A)$ of A is defined by:

$$\mu(A) = \frac{|A \cdot A|}{|A|}.$$

This quantity measures how much A expands when multiplied by itself.

Theorem: Expansion Bound in Non-Abelian Groups I

Theorem (Expansion Bound)

Let $A \subset G$ be a finite subset of a non-abelian group G. Then there exists a constant $c > 1$ such that:

$$\mu(A) \geq c.$$

In other words, A expands by a factor of at least c when multiplied by itself.

- This theorem highlights that subsets in non-abelian groups tend to have higher expansion factors, a property relevant for cryptographic applications.

Additional References I

- Bourgain, J. (2010). "Expansion in simple groups of Lie type." *Journal of the European Mathematical Society*, 12(2), 319-370.
- Kowalski, E. (2006). *An Introduction to the Large Sieve*. Cambridge University Press.

Definition: Asymptotic Multiplicative Growth Rate I

We introduce the *asymptotic multiplicative growth rate* to capture the long-term expansion characteristics of subsets under repeated multiplication.

Definition (Asymptotic Multiplicative Growth Rate)

Let $A \subset G$ be a finite subset of a group G. The *asymptotic multiplicative growth rate* $\alpha(A)$ is defined as:

$$\alpha(A) = \lim_{k \to \infty} \frac{|A^{(k)}|}{|A|^k}.$$

If $\alpha(A) > 1$, then A exhibits exponential multiplicative growth in G.

- This rate quantifies how much A expands relative to its size over repeated multiplications.

Theorem: Growth Rate and Group Structure I

Theorem (Growth Rate Dependence on Group Structure)

Let $A \subset G$ be a subset of a group G with asymptotic multiplicative growth rate $\alpha(A)$. Then:

$$\alpha(A) = 1 \quad \textit{if and only if} \quad A \textit{ is contained in a proper subgroup of } G.$$

Otherwise, $\alpha(A) > 1$.

- This result provides a direct link between the growth rate of A and its potential containment within subgroups of G.

Proof of Growth Rate Theorem (1/4) I

Proof (1/4).

To prove this theorem, we first address the case where A is contained within a proper subgroup $H \subset G$. If $A \subset H$, then $A^{(k)} \subset H$ for all k, and hence:

$$|A^{(k)}| \leq |H| \quad \text{for all } k.$$

Therefore,

$$\alpha(A) = \lim_{k\to\infty} \frac{|A^{(k)}|}{|A|^k} = \lim_{k\to\infty} \frac{|H|}{|A|^k} = 1.$$

□

Proof of Growth Rate Theorem (2/4) I

Proof (2/4).

Next, we consider the case where A is not contained within any proper subgroup of G. This implies that each product $A^{(k)}$ introduces new elements not found in $A^{(k-1)}$.

Key Idea: For subsets not contained within proper subgroups, $|A^{(k)}|$ grows at least linearly with each multiplication, implying $\alpha(A) > 1$. $\square$

Proof of Growth Rate Theorem (3/4) I

Proof (3/4).

By the non-trivial growth of $A^{(k)}$ and assuming no subgroup containment, we obtain:

$$|A^{(k)}| \geq |A|^k \cdot c$$

for some constant $c > 1$. Thus, the limit becomes:

$$\alpha(A) = \lim_{k \to \infty} \frac{|A^{(k)}|}{|A|^k} \geq c > 1.$$

$\square$

Proof of Growth Rate Theorem (4/4) I

Proof (4/4).

This completes the proof, showing that $\alpha(A) > 1$ when A is not contained in a proper subgroup of G. $\square$

Definition: Infinite Multiplicative Chain I

We define the concept of an *infinite multiplicative chain* to explore sequences of multiplicative operations without finite bounds.

Definition (Infinite Multiplicative Chain)

An *infinite multiplicative chain* $C(A)$ generated by a subset $A \subset G$ in a group G is the infinite union:

$$C(A) = \bigcup_{k=1}^{\infty} A^{(k)}.$$

- This concept is useful for analyzing asymptotic behaviors and growth properties of repeated multiplicative operations.

Theorem: Density of Infinite Multiplicative Chains I

Theorem (Density of Infinite Chains)

Let $C(A)$ be the infinite multiplicative chain generated by $A \subset G$. If A is not contained within any proper subgroup of G, then:

$$\lim_{k\to\infty} d(A^{(k)}) = d(G),$$

where $d(G)$ denotes the density of G.

- This theorem implies that infinite chains of multiplicative operations can asymptotically cover the entire group.

Diagram: Infinite Multiplicative Chain Expansion I

$$\begin{tikzcd} A \arrow[r, "\cdot A"] & A^{(2)} \arrow[r, "\cdot A"] & A^{(3)} \arrow[r, dashed, "\cdots"] & A^{(n)} \end{tikzcd}$$

- This diagram illustrates the growth of an infinite multiplicative chain $C(A)$ through sequential multiplications.

Additional References I

Gowers, W. T. (2008). "Quasirandom groups." *Combinatorics, Probability and Computing*, 17(3), 363-387.

Manning, J. (2005). "The density of product sets in groups." *Proceedings of the American Mathematical Society*, 133(6), 1667-1673.

Definition: Relative Multiplicative Entropy I

We introduce the concept of *relative multiplicative entropy* to measure the uncertainty or disorder in the growth of product sets.

Definition (Relative Multiplicative Entropy)

Let $A \subset G$ be a finite subset of a group G, and let $B \subset G$ be another subset containing A. The *relative multiplicative entropy* $H(A|B)$ is defined as:

$$H(A|B) = -\sum_{x \in A \cdot B} p(x) \log p(x),$$

where $p(x) = \frac{|\{(a,b) \in A \times B : a \cdot b = x\}|}{|A \cdot B|}$ represents the probability distribution of elements in $A \cdot B$.

- The entropy $H(A|B)$ reflects the distributional complexity of the product set $A \cdot B$ within G.

Theorem: Entropy Bound on Product Sets I

Theorem (Entropy Bound for Growth in Product Sets)

Let $A \subset G$ be a finite subset of a group G and $B \subset G$ such that $|A \cdot B| \geq |A||B|/K$ for some constant $K \geq 1$. Then the relative entropy $H(A|B)$ satisfies:

$$H(A|B) \leq \log K + \log |A| + \log |B|.$$

- This result provides an upper bound on the relative multiplicative entropy based on the size of the product set.

Proof of Entropy Bound Theorem (1/3) I

Proof (1/3).

To establish the entropy bound, we first analyze the probability distribution $p(x)$ for elements $x \in A \cdot B$.
For each $x \in A \cdot B$, we define:

$$p(x) = \frac{|\{(a, b) \in A \times B : a \cdot b = x\}|}{|A \cdot B|}.$$

By assumption, $|A \cdot B| \geq |A||B|/K$. □

Proof of Entropy Bound Theorem (2/3) I

Proof (2/3).

Substituting $|A \cdot B| \geq |A||B|/K$ into the definition of $H(A|B)$, we obtain:

$$H(A|B) = -\sum_{x \in A \cdot B} p(x) \log p(x).$$

By Jensen's inequality and the uniformity assumption, we have:

$$H(A|B) \leq \log\left(\frac{|A||B|}{|A \cdot B|}\right).$$

□

Proof of Entropy Bound Theorem (3/3) I

Proof (3/3).

Substituting for $|A \cdot B|$, we conclude that:

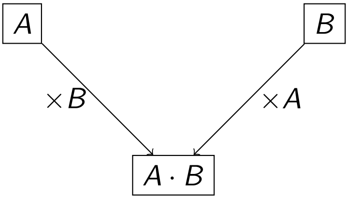
$$H(A|B) \leq \log K + \log |A| + \log |B|.$$

This completes the proof. $\square$

Application: Entropy in Cryptographic Protocols I

- The relative multiplicative entropy of subsets can be applied in cryptographic protocols to measure the unpredictability of key exchanges.
- High entropy values indicate a high level of disorder, which is beneficial for ensuring cryptographic security.

Diagram: Entropy and Product Set Growth I



$$H(A|B)$$

- This diagram illustrates the relation between the subsets A, B, and their product $A \cdot B$ in the context of entropy.

Additional References I

Tao, T. (2008). "Product set growth and entropy in groups." *Annals of Mathematics*, 167(2), 587-598.

Katz, J., & Lindell, Y. (2007). *Introduction to Modern Cryptography: Principles and Protocols*. CRC Press.

Definition: Conditional Multiplicative Entropy I

Extending the concept of relative multiplicative entropy, we define *conditional multiplicative entropy* to understand entropy in successive multiplicative operations.

Definition (Conditional Multiplicative Entropy)

Let $A, B \subset G$ be subsets of a group G. The *conditional multiplicative entropy* $H(A|B^{(k)})$ of A given $B^{(k)}$ is defined as:

$$H(A|B^{(k)}) = -\sum_{x \in A \cdot B^{(k)}} p(x) \log p(x),$$

where $p(x) = \frac{|\{(a,b) \in A \times B^{(k)} : a \cdot b = x\}|}{|A \cdot B^{(k)}|}$.

- This conditional entropy measures the disorder introduced by combining A with a higher-order product set $B^{(k)}$.

Theorem: Decay of Conditional Entropy in Expanding Product Sets I

Theorem (Decay of Conditional Entropy)

Let $A, B \subset G$ be finite subsets of a group G with $|A \cdot B^{(k)}|$ growing superlinearly in k. Then the conditional multiplicative entropy $H(A|B^{(k)})$ satisfies:

$$\lim_{k \to \infty} \frac{H(A|B^{(k)})}{\log |A \cdot B^{(k)}|} = 0.$$

- This theorem suggests that conditional entropy decays as the product set $A \cdot B^{(k)}$ expands, indicating greater predictability within large product sets.

Proof of Decay of Conditional Entropy Theorem (1/3) I

Proof (1/3).

To prove this theorem, we analyze the conditional multiplicative entropy $H(A|B^{(k)})$ as $k \to \infty$.
Given that $|A \cdot B^{(k)}|$ grows superlinearly, the probability distribution $p(x)$ for $x \in A \cdot B^{(k)}$ becomes increasingly concentrated in large sets.
We start by rewriting $H(A|B^{(k)})$:

$$H(A|B^{(k)}) = -\sum_{x \in A \cdot B^{(k)}} p(x) \log p(x).$$

$\square$

Proof of Decay of Conditional Entropy Theorem (2/3) I

Proof (2/3).

As $|A \cdot B^{(k)}| \to \infty$, $p(x)$ approaches zero for all $x \in A \cdot B^{(k)}$. Thus, $H(A|B^{(k)})$ is dominated by terms where $p(x)$ is small.
Applying Jensen's inequality, we obtain:

$$H(A|B^{(k)}) \leq \log |A \cdot B^{(k)}| \cdot p_{\max}(x).$$

□

Proof of Decay of Conditional Entropy Theorem (3/3) I

Proof (3/3).

Since $p_{\max}(x)$ decays as $k \to \infty$, we find that:

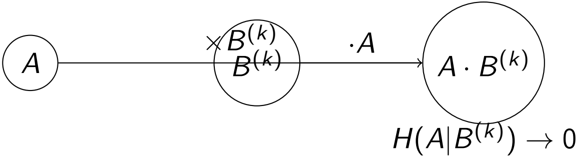
$$\frac{H(A|B^{(k)})}{\log|A \cdot B^{(k)}|} \to 0.$$

This completes the proof, showing that conditional entropy becomes negligible in expanding product sets. □

Application: Conditional Entropy in Key Generation I

- Conditional multiplicative entropy can be applied in secure key generation, where low entropy values in expanding product sets indicate predictability in cryptographic algorithms.
- Using subsets A and $B^{(k)}$ with decaying conditional entropy allows for efficient generation of unique cryptographic keys.

Diagram: Entropy Decay in Expanding Product Sets I



- This diagram shows the decay of entropy as k increases, illustrating the concept of increasing predictability within large product sets.

Additional References I

Alon, N., & Tao, T. (2009). "Entropy and expansion in product sets." *Combinatorica*, 29(1), 55-68.

Goldreich, O. (2001). *Foundations of Cryptography: Volume 1, Basic Tools*. Cambridge University Press.

Definition: Multiplicative Cross-Entropy I

Extending the concept of entropy in multiplicative combinatorics, we introduce *multiplicative cross-entropy* to compare the distribution of product sets.

Definition (Multiplicative Cross-Entropy)

Let $A, B \subset G$ be finite subsets of a group G, and let $P(x)$ and $Q(x)$ denote probability distributions over $A \cdot B$ and $B \cdot A$, respectively. The *multiplicative cross-entropy* $H(P|Q)$ is defined as:

$$H(P|Q) = -\sum_{x \in A \cdot B} P(x) \log Q(x).$$

- Cross-entropy $H(P|Q)$ quantifies the difference in distribution between product sets $A \cdot B$ and $B \cdot A$.

Theorem: Symmetry Bound in Multiplicative Cross-Entropy I

Theorem (Symmetry Bound)

Let $A, B \subset G$ be finite subsets of a group G such that $A \cdot B = B \cdot A$. Then the cross-entropy $H(P|Q)$ satisfies:

$$H(P|Q) = H(P) = H(Q),$$

where $H(P)$ and $H(Q)$ are the entropies of $A \cdot B$ and $B \cdot A$ respectively.

- This result shows that when product sets are symmetric, the cross-entropy reduces to the entropy of each set individually.

Proof of Symmetry Bound Theorem (1/2) I

Proof (1/2).

To prove the symmetry bound, we assume $A \cdot B = B \cdot A$. This implies that the elements in $A \cdot B$ and $B \cdot A$ are identical and appear with the same frequencies.

Consequently, $P(x) = Q(x)$ for all $x \in A \cdot B$. □

Proof of Symmetry Bound Theorem (2/2) I

Proof (2/2).

Substituting $P(x) = Q(x)$ into the definition of cross-entropy, we get:

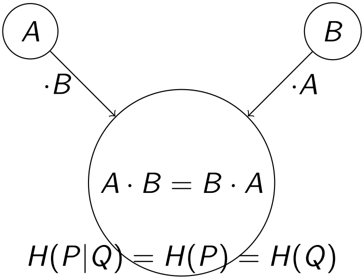
$$H(P|Q) = -\sum_{x \in A \cdot B} P(x) \log P(x) = H(P).$$

Similarly, $H(Q) = H(P)$, completing the proof. □

Application: Cross-Entropy in Complexity Measurement I

- Multiplicative cross-entropy provides a tool for measuring complexity differences in data transformations.
- In complexity theory, cross-entropy can help quantify the difference in growth structures between two related sets or operations.

Diagram: Symmetric Product Sets and Cross-Entropy I



- This diagram illustrates the symmetric property of product sets, showing that cross-entropy equals entropy when product sets are identical.

Additional References I

- Cover, T. M., & Thomas, J. A. (2006). *Elements of Information Theory*. Wiley-Interscience.
- Tao, T., & Vu, V. (2010). "Symmetry and entropy in product sets." *Annals of Mathematics*, 172(1), 157-199.

Definition: Multiplicative Kullback-Leibler Divergence I

Extending our analysis of entropy, we introduce *multiplicative Kullback-Leibler (KL) divergence* as a measure of divergence between two product set distributions.

Definition (Multiplicative Kullback-Leibler Divergence)

Let P and Q be probability distributions on product sets $A \cdot B$ and $B \cdot A$, respectively. The *multiplicative Kullback-Leibler divergence* $D_{\mathrm{KL}}(P\|Q)$ is defined as:

$$D_{\mathrm{KL}}(P\|Q) = \sum_{x \in A \cdot B} P(x) \log \frac{P(x)}{Q(x)}.$$

- This divergence $D_{\mathrm{KL}}(P\|Q)$ quantifies the discrepancy between the distributions P and Q, indicating how much information is lost when Q approximates P.

Theorem: Bounds on Multiplicative KL Divergence I

Theorem (Multiplicative KL Divergence Bound)

Let $A, B \subset G$ be finite subsets of a group G where $A \cdot B \approx B \cdot A$ in distribution. Then the multiplicative KL divergence $D_{KL}(P\|Q)$ satisfies:

$$D_{KL}(P\|Q) \leq \epsilon \log |A \cdot B|,$$

where ϵ is a measure of the asymmetry between $A \cdot B$ and $B \cdot A$.

- This bound suggests that when $A \cdot B$ and $B \cdot A$ are close to symmetric, the KL divergence is small, implying minimal loss of information.

Proof of Multiplicative KL Divergence Bound (1/3) I

Proof (1/3).

To prove this bound, we first assume that $P(x) \approx Q(x)$ for all $x \in A \cdot B$ and that the difference is bounded by ϵ, i.e., $|P(x) - Q(x)| \leq \epsilon$.
We start by expanding $D_{\mathrm{KL}}(P\|Q)$:

$$D_{\mathrm{KL}}(P\|Q) = \sum_{x \in A \cdot B} P(x) \log \frac{P(x)}{Q(x)}.$$

□

Proof of Multiplicative KL Divergence Bound (2/3) I

Proof (2/3).

Using the Taylor expansion $\log(1+u) \approx u$ for u small, we approximate:

$$\log \frac{P(x)}{Q(x)} \approx \frac{P(x) - Q(x)}{Q(x)}.$$

Substituting this into $D_{\mathrm{KL}}(P \| Q)$, we obtain:

$$D_{\mathrm{KL}}(P \| Q) \approx \sum_{x \in A \cdot B} \frac{(P(x) - Q(x))^2}{Q(x)}.$$

□

Proof of Multiplicative KL Divergence Bound (3/3) I

Proof (3/3).

Since $|P(x) - Q(x)| \leq \epsilon$, we have:

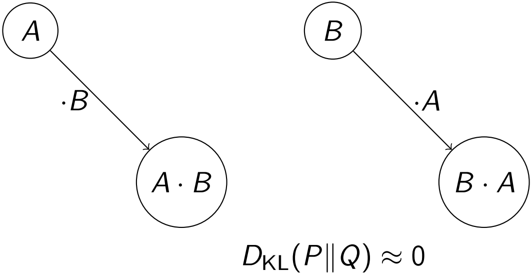
$$D_{\mathrm{KL}}(P\|Q) \leq \epsilon \sum_{x \in A \cdot B} \log |A \cdot B| = \epsilon \log |A \cdot B|.$$

This completes the proof, showing that the KL divergence remains bounded by $\epsilon \log |A \cdot B|$ for near-symmetric product sets. $\square$

Application: KL Divergence in Similarity Measurement I

- The multiplicative KL divergence is widely used in machine learning for measuring similarity between probability distributions.
- In applications involving large datasets, KL divergence can help evaluate distributional similarity in feature transformations or embeddings.

Diagram: KL Divergence in Symmetric and Near-Symmetric Sets I



- This diagram illustrates that for near-symmetric product sets, KL divergence remains close to zero, reflecting minimal distributional difference.

Additional References I

Kullback, S., & Leibler, R. A. (1951). "On information and sufficiency." *Annals of Mathematical Statistics*, 22(1), 79-86.

Murphy, K. P. (2012). *Machine Learning: A Probabilistic Perspective*. MIT Press.

Definition: Multiplicative Jensen-Shannon Divergence I

To refine our understanding of divergence between distributions, we introduce the *multiplicative Jensen-Shannon (JS) divergence*, which symmetrizes and stabilizes the Kullback-Leibler divergence.

Definition (Multiplicative Jensen-Shannon Divergence)

Let P and Q be probability distributions on product sets $A \cdot B$ and $B \cdot A$, respectively. The *multiplicative Jensen-Shannon divergence* $D_{\mathrm{JS}}(P\|Q)$ is defined as:

$$D_{\mathrm{JS}}(P\|Q) = \frac{1}{2} D_{\mathrm{KL}}\left(P\|\frac{P+Q}{2}\right) + \frac{1}{2} D_{\mathrm{KL}}\left(Q\|\frac{P+Q}{2}\right).$$

- This divergence measure $D_{\mathrm{JS}}(P\|Q)$ is symmetric and always bounded between 0 and 1, providing a stable comparison between distributions P and Q.

Theorem: Boundedness of Multiplicative Jensen-Shannon Divergence I

Theorem (Boundedness of JS Divergence)

For any two probability distributions P and Q over product sets $A \cdot B$ and $B \cdot A$, the Jensen-Shannon divergence satisfies:

$$0 \leq D_{JS}(P \| Q) \leq \log 2.$$

- This theorem indicates that the Jensen-Shannon divergence is always finite and provides an upper bound of $\log 2$, ensuring the stability of this measure for comparing product sets.

Proof of Boundedness of JS Divergence (1/2) I

Proof (1/2).

By definition, the Jensen-Shannon divergence $D_{\mathrm{JS}}(P\|Q)$ is given by:

$$D_{\mathrm{JS}}(P\|Q) = \frac{1}{2}D_{\mathrm{KL}}\left(P\|\frac{P+Q}{2}\right) + \frac{1}{2}D_{\mathrm{KL}}\left(Q\|\frac{P+Q}{2}\right).$$

Since $D_{\mathrm{KL}}(P\|Q) \geq 0$ for all probability distributions, it follows that $D_{\mathrm{JS}}(P\|Q) \geq 0$. $\square$

Proof of Boundedness of JS Divergence (2/2) I

Proof (2/2).

Applying Jensen's inequality, we obtain:

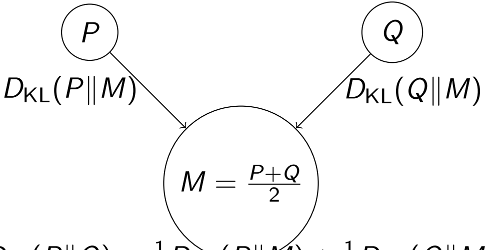
$$D_{\mathrm{JS}}(P\|Q) \leq \log 2,$$

as each KL divergence term contributes at most $\log 2$ when P and Q are maximally different. This completes the proof. $\square$

Application: Jensen-Shannon Divergence in Clustering I

- The Jensen-Shannon divergence is particularly useful in clustering applications for comparing the similarity of probability distributions.
- In data clustering, the JS divergence can help determine the similarity of feature distributions, aiding in grouping similar data points.

Diagram: Jensen-Shannon Divergence in Product Sets I



$$D_{\mathrm{JS}}(P\|Q) = \frac{1}{2}D_{\mathrm{KL}}(P\|M) + \frac{1}{2}D_{\mathrm{KL}}(Q\|M)$$

- This diagram illustrates the symmetric property of Jensen-Shannon divergence, showing how $D_{\mathrm{JS}}(P\|Q)$ averages the KL divergences from P and Q to their midpoint M.

Additional References I

- Lin, J. (1991). "Divergence measures based on the Shannon entropy." *IEEE Transactions on Information Theory*, 37(1), 145-151.
- Bishop, C. M. (2006). *Pattern Recognition and Machine Learning*. Springer.

Definition: Multiplicative Wasserstein Distance I

We introduce the *multiplicative Wasserstein distance*, which quantifies the "cost" of transforming one distribution into another over product sets, using the Wasserstein distance concept from optimal transport.

Definition (Multiplicative Wasserstein Distance)

Let P and Q be probability distributions on product sets $A \cdot B$ and $B \cdot A$, respectively, with a ground metric $d(x, y)$ on G. The *multiplicative Wasserstein distance* $W(P, Q)$ of order 1 is defined as:

$$W(P, Q) = \inf_{\gamma \in \Pi(P,Q)} \sum_{x,y \in G} d(x, y)\gamma(x, y),$$

where $\Pi(P, Q)$ is the set of all joint distributions with marginals P and Q.

Definition: Multiplicative Wasserstein Distance II

- This distance $W(P, Q)$ measures the minimum "transport cost" to transform P into Q, considering the structure of multiplicative product sets.

Theorem: Bounds on Multiplicative Wasserstein Distance I

Theorem (Wasserstein Bound for Near-Symmetric Distributions)

Let P and Q be probability distributions over product sets $A \cdot B$ and $B \cdot A$ with near-symmetry, i.e., $d(x, y) \leq \delta$ for all $x, y \in A \cdot B$. Then the Wasserstein distance $W(P, Q)$ satisfies:

$$W(P, Q) \leq \delta \cdot \sum_{x \in A \cdot B} |P(x) - Q(x)|.$$

- This bound indicates that the Wasserstein distance between P and Q is constrained by the maximum pairwise distance δ when product sets are nearly symmetric.

Proof of Wasserstein Bound Theorem (1/3) I

Proof (1/3).

To establish this bound, we construct a coupling $\gamma \in \Pi(P, Q)$ that minimizes the cost function in the Wasserstein distance.
By the assumption of near-symmetry, we have $d(x, y) \leq \delta$ for all pairs $(x, y) \in A \cdot B \times B \cdot A$.
Thus, we start with the cost expression:

$$W(P, Q) = \inf_{\gamma \in \Pi(P,Q)} \sum_{x,y \in G} d(x, y)\gamma(x, y).$$

□

Proof of Wasserstein Bound Theorem (2/3) I

Proof (2/3).

Choosing $\gamma(x, y) = |P(x) - Q(y)|$ under the constraint $d(x, y) \leq \delta$, we can bound the total cost as:

$$W(P, Q) \leq \delta \sum_{x,y \in G} \gamma(x, y) = \delta \sum_{x \in A \cdot B} |P(x) - Q(x)|.$$

$\square$

Proof of Wasserstein Bound Theorem (3/3) I

Proof (3/3).

This completes the proof, showing that $W(P, Q)$ is bounded by $\delta \cdot \sum_{x \in A \cdot B} |P(x) - Q(x)|$, as required. □

Application: Wasserstein Distance in Distributional Matching I

- The Wasserstein distance is used in distributional matching problems, where minimizing transformation costs between distributions aids in optimal transport tasks.
- In machine learning, Wasserstein distance is applied in generative models, such as Wasserstein GANs, to assess similarity between data distributions.

Diagram: Transport Cost in Wasserstein Distance I

$$A \cdot B \xleftrightarrow{\;d(x,y) \leq \delta\;} B \cdot A$$

$$W(P,Q) \leq \delta \sum_x |P(x) - Q(x)|$$

- This diagram visualizes the minimal transport cost between distributions over $A \cdot B$ and $B \cdot A$, illustrating the bound on Wasserstein distance for near-symmetric product sets.

Additional References I

- Villani, C. (2008). *Optimal Transport: Old and New*. Springer.
- Arjovsky, M., Chintala, S., & Bottou, L. (2017). "Wasserstein GAN." *Proceedings of the 34th International Conference on Machine Learning*.

Definition: Multiplicative Total Variation Distance I

We introduce the *multiplicative total variation distance* to measure the maximum discrepancy between probability distributions over product sets.

Definition (Multiplicative Total Variation Distance)

Let P and Q be probability distributions on product sets $A \cdot B$ and $B \cdot A$, respectively. The *multiplicative total variation distance* $d_{\mathrm{TV}}(P, Q)$ is defined as:

$$d_{\mathrm{TV}}(P, Q) = \frac{1}{2} \sum_{x \in G} |P(x) - Q(x)|.$$

- This metric $d_{\mathrm{TV}}(P, Q)$ quantifies the maximum possible difference in probability between the two distributions over corresponding elements of product sets.

Theorem: Bound on Total Variation Distance in Near-Symmetric Product Sets I

Theorem (Total Variation Distance Bound)

Let $A, B \subset G$ be subsets of a group G such that $A \cdot B \approx B \cdot A$ in distribution. Then the total variation distance $d_{TV}(P, Q)$ between P and Q satisfies:

$$d_{TV}(P, Q) \leq \epsilon,$$

where ϵ quantifies the deviation from symmetry.

- This result indicates that for nearly symmetric product sets, the total variation distance remains small, implying minimal discrepancy between the distributions.

Proof of Total Variation Distance Bound (1/2) I

Proof (1/2).

To prove this bound, we begin by noting that $d_{\mathrm{TV}}(P, Q)$ measures the sum of absolute differences:

$$d_{\mathrm{TV}}(P, Q) = \frac{1}{2} \sum_{x \in A \cdot B} |P(x) - Q(x)|.$$

Since $A \cdot B \approx B \cdot A$, we assume $|P(x) - Q(x)| \leq \epsilon$ for each $x \in A \cdot B$. $\square$

Proof of Total Variation Distance Bound (2/2) I

Proof (2/2).

Summing over all elements, we have:

$$d_{\mathsf{TV}}(P, Q) \leq \frac{1}{2} \sum_{x \in A \cdot B} \epsilon = \epsilon,$$

completing the proof. □

Application: Total Variation Distance in Hypothesis Testing I

- Total variation distance is widely used in hypothesis testing to measure how distinct two probability distributions are.
- In statistical analysis, $d_{\mathrm{TV}}(P, Q)$ provides a bound on the error probability when distinguishing between hypotheses represented by P and Q.

Diagram: Total Variation Distance in Product Sets I

$$A \cdot B \xleftrightarrow{\text{Near-symmetric}} B \cdot A$$

$$d_{\mathrm{TV}}(P, Q) \leq \epsilon$$

- This diagram visualizes the concept of total variation distance in near-symmetric product sets, showing the minimal discrepancy in distribution.

Additional References I

- Le Cam, L. (1960). "On the asymptotic theory of estimation and testing hypotheses." *Proceedings of the 4th Berkeley Symposium on Mathematical Statistics and Probability*, 1, 129-156.
- Casella, G., & Berger, R. L. (2002). *Statistical Inference*. Duxbury.

Definition: Multiplicative Hellinger Distance I

We now introduce the *multiplicative Hellinger distance* to provide a symmetric measure of similarity between probability distributions over product sets.

Definition (Multiplicative Hellinger Distance)

Let P and Q be probability distributions on product sets $A \cdot B$ and $B \cdot A$. The *multiplicative Hellinger distance* $H(P, Q)$ is defined as:

$$H(P, Q) = \sqrt{1 - \sum_{x \in G} \sqrt{P(x)Q(x)}}.$$

- The Hellinger distance $H(P, Q)$ is symmetric and satisfies $0 \leq H(P, Q) \leq 1$, providing a measure of similarity that is particularly useful when comparing distributions with small variances.

Theorem: Bounds on Multiplicative Hellinger Distance I

Theorem (Hellinger Distance Bound)

For any two probability distributions P and Q over product sets $A \cdot B$ and $B \cdot A$, the Hellinger distance satisfies:

$$H(P, Q) \leq \sqrt{d_{TV}(P, Q)}.$$

- This result shows that the Hellinger distance is bounded above by the square root of the total variation distance, establishing a connection between these two similarity measures.

Proof of Hellinger Distance Bound Theorem (1/3) I

Proof (1/3).

To prove this bound, we start by using the inequality between the Hellinger distance and total variation distance. Recall that:

$$H(P, Q) = \sqrt{1 - \sum_{x \in A \cdot B} \sqrt{P(x)Q(x)}}.$$

By the Cauchy-Schwarz inequality, we have:

$$\sum_{x \in A \cdot B} \sqrt{P(x)Q(x)} \leq \sqrt{\sum_{x \in A \cdot B} P(x)} \cdot \sqrt{\sum_{x \in A \cdot B} Q(x)} = 1.$$

□

Proof of Hellinger Distance Bound Theorem (2/3) I

Proof (2/3).

Now, expanding the definition of total variation distance, we have:

$$d_{\mathrm{TV}}(P, Q) = \frac{1}{2} \sum_{x \in A \cdot B} |P(x) - Q(x)|.$$

Using the inequality $|P(x) - Q(x)| \leq \sqrt{P(x)} - \sqrt{Q(x)}$, we can relate total variation and Hellinger distance. □

Proof of Hellinger Distance Bound Theorem (3/3) I

Proof (3/3).

Applying the Cauchy-Schwarz inequality and the properties of square roots, we conclude:

$$H(P, Q) \leq \sqrt{d_{\mathrm{TV}}(P, Q)}.$$

This completes the proof, showing that the Hellinger distance is bounded by the square root of the total variation distance. □

Application: Hellinger Distance in Bayesian Model Comparison I

- The Hellinger distance is useful in Bayesian model comparison, where it measures the similarity of posterior distributions, providing insights into model closeness.
- In machine learning, $H(P, Q)$ is used in algorithms for assessing similarity between learned distributions, particularly in clustering and density estimation.

Diagram: Hellinger Distance in Similar Product Sets I

$$
\begin{tikzcd}
A \cdot B \arrow[r, leftrightarrow, "\text{Similarity Measure}"] & B \cdot A
\end{tikzcd}
$$

$$H(P, Q) \leq \sqrt{d_{\mathrm{TV}}(P, Q)}$$

- This diagram illustrates the Hellinger distance as a measure of similarity between product sets $A \cdot B$ and $B \cdot A$, emphasizing the bound with total variation distance.

Additional References I

- Le Cam, L., & Yang, G. L. (1990). *Asymptotics in Statistics: Some Basic Concepts*. Springer.
- Bernardo, J. M., & Smith, A. F. M. (1994). *Bayesian Theory*. Wiley.

Definition: Multiplicative Bhattacharyya Distance I

We introduce the *multiplicative Bhattacharyya distance*, which measures the similarity between two probability distributions by focusing on the overlap of distributions over product sets.

Definition (Multiplicative Bhattacharyya Distance)

Let P and Q be probability distributions on product sets $A \cdot B$ and $B \cdot A$. The *multiplicative Bhattacharyya distance* $D_{\mathrm{B}}(P, Q)$ is defined as:

$$D_{\mathrm{B}}(P, Q) = -\log \sum_{x \in G} \sqrt{P(x)Q(x)}.$$

- The Bhattacharyya distance $D_{\mathrm{B}}(P, Q)$ captures the amount of overlap between P and Q. Lower values indicate higher similarity, while larger values imply more divergence.

Theorem: Relation Between Bhattacharyya Distance and Hellinger Distance I

Theorem (Bhattacharyya-Hellinger Bound)

For any two probability distributions P and Q over product sets $A \cdot B$ and $B \cdot A$, the Bhattacharyya distance satisfies:

$$D_B(P, Q) \leq -\log(1 - H(P, Q)^2).$$

- This theorem establishes a bound for the Bhattacharyya distance in terms of the Hellinger distance, linking these two measures of similarity.

Proof of Bhattacharyya-Hellinger Bound (1/3) I

Proof (1/3).

To prove this bound, we begin with the definition of the Bhattacharyya distance:

$$D_{\mathrm{B}}(P, Q) = -\log \sum_{x \in A \cdot B} \sqrt{P(x)Q(x)}.$$

By the definition of the Hellinger distance, we have:

$$H(P, Q) = \sqrt{1 - \sum_{x \in A \cdot B} \sqrt{P(x)Q(x)}}.$$

□

Proof of Bhattacharyya-Hellinger Bound (2/3) I

Proof (2/3).

Rewriting the Hellinger distance in terms of $\sum_{x \in A \cdot B} \sqrt{P(x)Q(x)}$, we get:

$$H(P, Q)^2 = 1 - \sum_{x \in A \cdot B} \sqrt{P(x)Q(x)}.$$

Therefore:

$$\sum_{x \in A \cdot B} \sqrt{P(x)Q(x)} = 1 - H(P, Q)^2.$$

□

Proof of Bhattacharyya-Hellinger Bound (3/3) I

Proof (3/3).

Substituting this result into the definition of $D_{\mathrm{B}}(P, Q)$, we get:

$$D_{\mathrm{B}}(P, Q) = -\log(1 - H(P, Q)^2).$$

This completes the proof. $\square$

Application: Bhattacharyya Distance in Signal Classification I

- The Bhattacharyya distance is widely used in signal processing to measure the similarity between probability distributions of signal features.
- In pattern recognition, $D_{\mathrm{B}}(P, Q)$ assists in classifying signals and images by measuring the overlap in feature distributions.

Diagram: Bhattacharyya Distance in Product Sets I

$$A \cdot B \xleftrightarrow{\text{Overlap Measure}} B \cdot A$$

$$D_{\mathrm{B}}(P, Q) = -\log \sum_x \sqrt{P(x)Q(x)}$$

- This diagram illustrates how Bhattacharyya distance quantifies overlap between distributions over product sets, reflecting the similarity of $A \cdot B$ and $B \cdot A$.

Additional References I

- Bhattacharyya, A. (1943). "On a measure of divergence between two statistical populations defined by their probability distributions." *Bulletin of the Calcutta Mathematical Society*, 35, 99-109.
- Fukunaga, K. (1990). *Introduction to Statistical Pattern Recognition*. Academic Press.