Notes on Holevo’s Theorem

Aliefya Mahalva Ayn • 10 May 2025

1. Introduction

Communication stands as a cornerstone of human civilization and scientific endeavor. From the drum beat to the complex signals transmitted through optical fibers, the goal remains: to reliably convey information from one point to another. With the advent of quantum mechanics, a new paradigm for information processing and communication emerged- quantum information theory. This field explores how the properties of quantum systems, such as superposition and entanglement, can be harnessed or how they fundamentally limit our ability to process information. At its core lies Holevo’s theorem, a fundamental result established by Alexander Holevo in 1973 that imposes an essential limit on the amount of classical information that can be extracted from quantum systems.

Holevo’s Theorem addresses a critical question: how much classical information can be reliably transmitted using quantum states? If a sender (Alice) encodes a classical message by preparing one of several possible quantum states and sends it to a receiver (Bob), how much information about the original message can Bob ultimately obtain through measurement? In the classical world, if a bit is encoded as either voltage level A or voltage level B, and these levels are sufficiently distinct, Bob can, in principle, determine the original bit perfectly. However, in the quantum world, the situation is more subtle.