J. Chosun Natural Sci.
Vol. 13, No. 1 (2020) pp. 8 – 12
https://doi.org/10.13160/ricns.2020.13.1.8

A Minimum Error Discrimination problem for Linearly independent Pure States Related Quantum Safe Cryptography

Tae Ryong Park†

Abstract

In this paper we study the Minimum Error Discrimination problem (MED) for ensembles of linearly independent (LI) pure states. By constructing a map from the set on those ensembles we show that the Pretty Good Measurement (PGM) and the optimal measurement for the MED are related by the map.

Keywords: Pretty Good Measurement, Optimal Measurement, Quantum Safe Cryptography

1. Introduction

Quantum state discrimination underlies various applications in quantum information processing tasks. It essentially describes the distinctivity of quantum systems in different states, and the general process of extracting classical information from quantum systems. It is also useful in quantum information applications, such as characterization of mutual information in cryptographic protocols, or as a technique to derive fundamental theorems in quantum foundations. It has deep connections to physical principles such as relativistic causality. Quantum state discrimination traces a long history of several decades, starting with early attempts to formalize information processing of physical systems such as optical communication with photons. Nevertheless, in most cases, optimal strategies of quantum state discrimination remain unsolved, and related applications are only valid in some limited cases. Quantum algorithm has been discovered, especially for some issues related to number theory and topology using quantum computing, which can lead to tremendous speed improvements. These speed improvements can not invalidate existing encryption techniques, but in the case of symmetric keys, the length of the key must be taken much larger to make the encryption technique valid. Quantum-resistant cryptographic algorithms are used in the same meaning as quantum safety codes. More over, Quantum-resistant cryptographic algorithms are cryptographic systems that operates on existing computers resists to quantum attacks. The following Table 1 shows the existing crypto-algorithms affected by stability. Candidates for quantum-resistant algorithms largely include grid-based algorithms, polynomial-based algorithms, hash-based signature algorithms.

To develop this quantum tolerance algorithm, it is a quantum identification that must be preceded numerically and physically, and this discussion has long been going on. In this paper, we propose a method to solve the problem of having a minimum error under certain conditions in a mathematical way.

Table 1. Cryptographic algorithm

Cryptographic algorithm	Type	Goal	Influence of quantum computers
AES	Symmetric key	Encryption and decryption	Big size key
SHA-2, SHA-3	Hash	Hashing	Big size hashed value(output)
RSA	Public key	Digital signature and key setting	Not safe
ECDSA, ECDH	Public key	Digital signature and key exchange	Not safe
DSA	Public key	Digital signature	Not safe

Dept. of Computer Engineering, Seokyeong University 124 Seogyeong-ro, Seongbuk-gu, Seoul, 02173, Korea

†Corresponding author : trpark@skuniv.ac.kr
(Received : March 5, 2020, Revised : March 9, 2020, Accepted : March 14, 2020)

Suppose two people - Alice and Bob - are communicating. In quantum state discrimination, Alice provides a collection of states and transform the classical information to Bob using a quantum mechanical channel. Bob detects the information by using an appropriate measurement. A key assumption in this scenario is that both parties make a prior arrangement concerning the ensemble of quantum states. We may formulate the discrimination problem in the following way. Formally, we may formulate the optimization problem in the following way. Let $\mathcal{H}$ be a d-dimensional Hilbert space. In preparation, we have an ensemble $P=\{p_i,|\psi_i\rangle\langle\psi_i|\}_{i=1}^{d}$, where $|\psi_1\rangle,|\psi_2\rangle,\ldots,|\psi_d\rangle$ is linearly independent pure states in $\mathcal{H}$ and $span\{|\psi_1\rangle,\langle\psi_2|,\ldots,|\psi_d\rangle\}=\mathcal{H}$. The probabilities $p_1, \ldots, p_d$ is referred as a priori probability, $p_i>0$ and $\Sigma_{i=1}^{d}\ p_i=1$. Alice choose a quantum state using the probability distribution $\{p_i\}$ and sends it to Bob and then Bob must figure out the state using an appropriate measurement, which minimizes the probability of a detection error. More explicitly, we seek the positive operator valued measurement (POVM) with elements $\{E_1, ..., E_d\}$ that maximizes the probability of success $p_s=\Sigma_{i=1}^{n}p_i\langle\psi_i|E_i|\psi_i\rangle$ subject to $E_i\geq 0$ for all i and $\Sigma_{i=1}^{d}\ E_i=Id$. Equivalently, we seek the matrix Z that minimizes Tr Z subject to $Z\geq p_i|\psi_i\rangle\langle\psi_i|$ for all i. The duality problem can be summarized as follows:

If $\{E_i\}_{i=1}^{d}$ is an element of the optimal POVM, then for some Hermitian matrix Z, $\Sigma_{i=1}^{d}p_i\langle\psi_i|E_i|\psi_i\rangle=\mathrm{Tr}Z$ and hence $(Z-p_i|\psi_i\rangle\langle\psi_i|)E_i=E_i(Z-p_i|\psi_i\rangle\langle\psi_i|)=0$.

Summing over i and using the relation $\Sigma_{i=1}^{d}\ E_i=Id$, we have

$$Z=\sum_{i=1}^{d}p_iE_i\,|\psi_i\rangle\langle\psi_i| = \sum_{i=1}^{d}p_i|\psi_i\rangle\langle\psi_i|E_i$$

Thus we get the following relations

$$E_j(p_j|\psi_j\rangle\langle\psi_j|-p_i|\psi_i\rangle\langle\psi_i|)\,E_i=0$$

and $\sum_{i=1}^{d}p_i\,|\psi_i\rangle\langle\psi_i|E_i\geq p_j\,|\psi_j\rangle\langle\psi_j|$.

From this and[1] and[2] one may prove the following: An optimal d-POVM $\{E_i\}_{i=1}^{d}$ satisfy the relations

(1) $E_j(p_j|\psi_j\rangle\langle\psi_j|-p_i\,|\psi_i\rangle\langle\psi_i|)\ E_i=0$

(2) $\sum_{i=1}^{d}p_i\,|\psi_i\rangle\langle\psi_i|E_i\geq p_j|\psi_j\rangle\langle\psi_j|$

2. An Ensemble of Linearly Independent Pure States

In this section, we follow the computation of[7], see also[8], adapted to the case of linealy independent pure states. Let us fix a linearly independent states $\{|\psi_i\rangle\}_{i=1}^{n}$ and let $\mathcal{E}(\psi)=\{P=\{p_i,|\psi_i\rangle\langle\psi_i|\}_{i=1}^{n}\,|\,\sum_{i=1}^{n}p_i=1,p_i>0\}$ be the set of ensembles of linearly independent pure states. Let $E=\{E_i\}_{i=1}^{n}$ be an optimal POVM for $P=\{p_i,|\psi_i\rangle\langle\psi_i|\}_{i=1}^{n}$. Since the states $\{|\psi_i\rangle\}_{i=1}^{n}$ are linearly independent, there is dual vectors $\{|\phi_i\rangle\}_{i=1}^{n}$ such that $\langle\phi_i|\psi_j\rangle=\delta_{ij}$. Suppose that $\langle\psi_k|E_k|\psi_k\rangle=0$ for some k. Define $E'=P_kE_iP_k+\frac{1}{\langle\phi_k|\phi_k\rangle}|\phi_k\rangle\langle\phi_k|$

where P_k is the projection onto the space spanned by the n-1 vectors $\{|\psi_i\rangle\}_{i=1}^{n}$ excluding $|\psi_k\rangle$. Then we have

$$\begin{aligned}\langle\psi_i|E_i'|\psi_i\rangle &= \langle\psi_i|P_kE_iP_k|\psi_i\rangle \\ &\quad+\frac{1}{\langle\phi_k|\phi_k\rangle}\langle\psi_i|\phi_k\rangle\langle\phi_k|\psi_i\rangle \\ &= \langle\psi_i|P_kE_iP_k|\psi_i\rangle+\delta_{ik}\delta_{ki}\end{aligned}$$

Thus

$$\langle\psi_i|E_i'|\psi_i\rangle=\begin{cases}\langle\psi_i|E_i|\psi_i\rangle & for\ i\neq k\\ \dfrac{1}{\langle\phi_k|\phi_k\rangle} & for\ i=k\end{cases}$$

and

$$\sum_{i=1}^{n}p_i\,\langle\psi_i|E_i|\psi_i\rangle\leq\sum_{i=1}^{n}p_i\,\langle\psi_i|E_i'|\psi_i\rangle.$$

Then $E=\{E_i\}_{i=1}^{n}$ is not optimal one and hence it satisfies $\langle\psi_i|E_i|\psi_i\rangle\neq 0$ for all i.

Let $Z=\sum_{i=1}^{n}p_i\,E_i|\psi_i\rangle\langle|\psi_i|$. Then

$$\begin{aligned}&E_j(Z-p_j|\psi_j\rangle\langle\psi_j|\\ &\quad=E_j\left(\sum_{i=1}^{n}p_i\,|\psi_i\rangle\langle\psi_i|-p_j|\psi_j\rangle\langle\psi_j|\right)\\ &\quad=0\end{aligned}$$

For each k,

$$E_j\left(\sum_{i=1}^{n}p_iE_i\,|\psi_i\rangle\langle\psi_i|-p_j|\psi_j\rangle\langle\psi_j|\right)|\phi_k\rangle=0$$

This implies that $E_j(p_kE_k|\psi_k\rangle)=\delta_{jk}p_jE_j|\psi_j\rangle$ and $E_jE_k|\psi_k\rangle=\delta_{jk}E_k|\psi_k\rangle$

Thus for each k, $E_k|\psi_k\rangle$ is an eigenvector for E_j whose eigenvalues are 0 or 1. There is only one 1 eigenvalue. Thus $\mathrm{Tr}E_i=1$ for all i and $E_iE_j=\delta_{ij}E_i$.

For a given ensemble $P=\{p_i,|\psi_i\rangle\langle\psi_i|\}_{i=1}^{n}$, optimal POVM for P is unique. In fact if $\{E_i\}_{i=1}^{n}$ and $\{E'_i\}_{i=1}^{n}$ are two optimal POVM for P. Then the convex combination $II=\{tE_i+(1-t)E'_i\}_{i=1}^{n}$ is also an optimal POVM for P. Then by the above calculation, $II_iII_j=\delta ijII_i \Leftrightarrow E_i=E'_i$.

Summarizing one can construct the following map $OP:\mathcal{E}(\psi)\rightarrow\wp(E)$ where $\wp(E)$ is the set of all POVM

$E=\{E_i\}_{i=1}^n$ satisfying the following conditions:

1. $E_i \geq 0$ for all i
2. $\Sigma_i E_i = Id$
3. $E_i E_j = \delta_{ij} E_i$

and $OP(P)$ = the optimal POVM for P.

In the below, the inverse map of the map $\mathrm{OP}:\varepsilon(\psi)\to\wp(E)$ will be constructed and this construction provides a good criterion for optimal POVM. For any element $P=\{p_i|\psi_i\rangle\langle\psi_i|\}_{i=1}^n \in \varepsilon(\psi)$, let OP(P) $=\{II_i\}_{i=1}^n \in \wp(E)$ and let $Z=\Sigma_{i=1}^n p_i|\psi_i\rangle\langle\psi_i|II_i$. Then $(\{II_i\}_{i=1}^n, Z)$ is the optimal dual pair for the minimum error discrimination for P. Define a relation $R:\varepsilon(\psi)\to\varepsilon(\psi)$ by $\mathcal{R}(\mathrm{P})=\mathrm{Q}:=\{q_i,\sigma_i\}_{i=1}^n$, where $q_i=\frac{\mathrm{Tr}(Z^2 II_i)}{\mathrm{Tr}(Z^2)}$ and $\sigma_i := \frac{ZII_iZ}{\mathrm{Tr}(Z^2 II_i)}$ such that $\sigma_i \geq 0$, $\mathrm{Tr}(\sigma_i)=1$ and $\sigma_i=|\psi_i\rangle\langle\psi_i|$ for all i. Given any $P\in\varepsilon(\psi)$, the optimal dual pair $(\{II_i\}_{i=1}^n, Z)$ is uniquely determined and thus $R(P)=Q$ is uniquely determined. Hence the map $R:\varepsilon(\psi)\to\varepsilon(\psi)$ is well-defined.

Furthermore,

$$ZII_iZ = \left(\sum_{i=1}^n p_j|\psi_j\rangle\langle\psi_j|II_j\right) II_i \left(\sum_{k=1}^n p_k II_k|\psi_k\rangle\langle\psi\right)$$
$$= p_i^2|\psi_i\rangle\langle\psi_i|II_i|\psi_i\rangle\langle\psi_i|$$

$$Tr(Z^2 II_i) = \mathrm{Tr}\left(p_i^2|\psi_i\rangle\langle\psi_i|II_i|\psi_i\rangle\langle\psi_i|\right)\mathrm{Tr} = p_i^2\langle\psi_i|II_i|\psi_i\rangle\langle\psi_i|\psi_i\rangle = p_i^2\langle\psi_i|II_i|\psi_i\rangle$$

$$\sigma_i = \frac{ZII_iZ}{Tr(Z^2 II_i)} = \frac{p_i^2|\psi_i\rangle\langle\psi_i|II_i|\psi_i\rangle\langle\psi_i|}{p_i^2\langle\psi_i|II_i|\psi_i\rangle} = |\psi_i\rangle\langle\psi_i|.$$

3. The Pretty Good (PGM)

The Pretty Good Measurement (PGM) can be described as a map from $\varepsilon(\psi)$ to itself. Let $Q=\{q_i|\psi_i\rangle\langle\psi_i|\}_{i=1}^n \in \varepsilon(\psi)$ and let $\rho_q=\Sigma_{i=1}^n q_i|\psi_i\rangle\langle\psi_i|$. Define a map $\mathrm{PGM}:\varepsilon(\psi)\to\wp(\mathrm{E})$ as follows. For $\mathrm{PGM(Q)} := \{E_i^q\}_{i=1}^n$ where

$$E_i^q := \rho_q^{-1/2} q_i|\psi_i\rangle\langle\psi_i|\rho_q^{-1/2}$$

such that

(1) $E_i^q \geq 0$ for all i (2) $\sum_{i=1}^n E_i^q = \mathrm{Id}$
(3) $\mathrm{Rank} E_i^q = 1$ (4) $E_i^q E_j^q = \delta_{ij} E_i^q$.

Note that by (1) and (2) $\{E_i^q\}_{i=1}^n$ is a POVM. To check the condition (2),

$$\sum_{i=1}^n E_i^q = \sum_{i=1}^n \rho_q^{-1/2} q_i|\psi_i\rangle\langle\psi_i|\rho_q^{-1/2} = \rho_q^{-1/2}\rho_q\rho_q^{-1/2} = Id.$$

The condition (4) follows from the following computation:

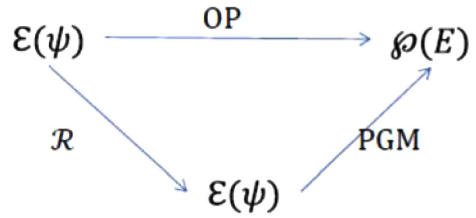
$$E_i^q = \rho_q^{-1/2} q_i|\psi_i\rangle\langle\psi_i|\rho_q^{-1/2}$$
$$= UD^{-1}U^\dagger\sqrt{q_i}|\psi_i\rangle\langle\psi_i|\sqrt{q_i}UD^{-1}U^\dagger$$
$$= UD^{-1}U^\dagger M|i\rangle\langle i|M^\dagger UD^{-1}V^\dagger$$
$$= UD^{-1}U^\dagger UDV^\dagger|i\rangle\langle i|VDU^\dagger UD^{-1}V^\dagger$$
$$= UV^\dagger|i\rangle\langle i|VU^\dagger$$

$$E_i^q E_j^q = UV^\dagger|i\rangle\langle i|VU^\dagger UV^\dagger|j\rangle\langle j|VU^\dagger$$
$$= UV^\dagger|i\rangle\langle i|j\rangle\langle j|VU^\dagger$$
$$= \delta_{ij}UV^\dagger|i\rangle\langle i|VU^\dagger = \delta_{ij}E_i^q$$

In the above computation. For an orthonormal basis $\{|i\rangle\}_{i=1}^n$ for the Hilbert space $\mathcal{H}$ such that $M|i\rangle=\sqrt{q_i}|\psi_i\rangle$. Then

$$\rho_q = \sum_{i=1}^n q_i|\psi_i\rangle\langle\psi_i| = \sum_{i=1}^n M|i\rangle\langle i|M^\dagger = MM^\dagger.$$

Using the Singular value decomposition of $M=UDV^\dagger$, where U, V are Hermitian and $D=diag(d_1,...,d_n)$ and $MV=UD$, $\rho_q^{-1/2}=UD^{-1}U^\dagger$. Summarizing the maps, the following diagram commutes



More explicitly, for $\mathrm{P}=\{p_i|\psi_i\rangle\langle\psi_i|\}_{i=1}^n$, let $(\{II_i\}_{i=1}^n, Z)$ be the optimal dual pair. Then OP(P) $=\{II_i\}_{i=1}^n$ and $\mathcal{R}(\mathrm{P})=\mathrm{Q}:=\{q_i,|\psi_i\rangle\langle\psi_i|\}_{i=1}^n$ and $Z=\sum_{i=1}^n p_i|\psi_i\rangle\langle\psi_i|II_i$, where

$$q_i = \frac{\mathrm{Tr}(Z^2 II_i)}{\mathrm{Tr}(Z^2)} \text{ and } |\psi_i\rangle\langle\psi_i| = \frac{ZII_iZ}{\mathrm{Tr}(Z^2 II_i)}.$$

Thus

$$\rho_q = \sum_{i=1}^n q_i|\psi_i\rangle\langle\psi_i| = \sum_{i=1}^n \frac{\mathrm{Tr}(Z^2 II_i)}{\mathrm{Tr}(Z^2)}\cdot\frac{ZII_iZ}{\mathrm{Tr}(Z^2 II_i)} = \frac{Z^2}{\mathrm{Tr}(Z^2)}$$

And

$$\sqrt{\rho_q} = \frac{Z}{\sqrt{\mathrm{Tr}(Z^2)}}.$$

Let $\mathrm{PGM(Q)}=\{E_i^q\}_{i=1}^n$. Then

$$E_i^q = \rho_q^{-1/2} q_i|\psi_i\rangle\langle\psi_i|\rho_q^{-1/2} = \sqrt{\mathrm{Tr}(Z^2)}\cdot Z^{-1}\cdot\frac{ZII_iZ}{\mathrm{Tr}(Z^2)}\cdot Z^{-1}\cdot\sqrt{\mathrm{Tr}(Z^2)} = II_i$$

When the map $R:\varepsilon(\psi)\rightarrow\varepsilon(\psi)$ is bijective, one has a nice criterion for PGM. For this, one can construct the inverse of the map. Let $\mathrm{Q} \coloneqq \{q_i, |\psi_i\rangle\langle\psi_i|\}_{i=1}^{n} \in \varepsilon(\psi)$ and let $\rho_q = \Sigma_{i=1}^{n} q_i|\psi_i\rangle\langle\psi_i| = UD^2U^\dagger$. Then PGM(Q) = $\{E_i^q\}_{i=1}^{n}$ where

$$E_i^q = \rho_q^{-1/2} q_i|\psi_i\rangle\langle\psi_i|\rho_q^{-1/2} = UV^\dagger|i\rangle\langle i|VU^\dagger$$

And

$$\rho_q = UDU^\dagger, \qquad \rho_q^{-1/2} = UD^{-1}U^\dagger$$

Let $D = D_1 + D_2 + \cdots + D_n, D_i = diag(d_i\delta_{ij})$

Define

$$p_i \coloneqq \frac{d_i}{\sum_{i=1}^{n} d_i} = \frac{\sqrt{q_i}}{\sum_{i=1}^{n}\sqrt{q_i}}$$

Now $P = \{p_i|\psi_i\rangle\langle\psi_i|\}_{i=1}^{n} \in \varepsilon(\psi)$ and define $Z = \frac{\sqrt{q_i}}{\sum_{i=1}^{n}\sqrt{q_i}}$. Then,

$$\begin{aligned} Z - p_i|\psi_i\rangle\langle\psi_i| &= \frac{\sqrt{\rho_q}}{\sum_{j=1}^{n}\sqrt{q_j}} - \frac{\sqrt{q_i}}{\sum_{j=1}^{n}\sqrt{q_j}}|\psi_i\rangle\langle\psi_i| \\ &= \frac{1}{\sum_{j=1}^{n}\sqrt{q_j}}\left(\sqrt{\rho_q} - \sqrt{q_i}|\psi_i\rangle\langle\psi_i|\right) \\ &= \frac{1}{\sum_{j=1}^{n}\sqrt{q_j}}\left(UDU^\dagger - UD_iU^\dagger\right). \end{aligned}$$

And

$$\left(\frac{1}{\sum_{j=1}^{n}\sqrt{q_j}}\sqrt{\rho_q} - p_i|\psi_i\rangle\langle\psi_i|\right)\cdot E_i^q$$

$$= \frac{1}{\sum_{j=1}^{n}\sqrt{q_j}}\sqrt{\rho_q}\cdot E_i^q - p_i|\psi_i\rangle\langle\psi_i|\cdot E_i^q$$

$$= \frac{1}{\sum_{j=1}^{n}\sqrt{q_j}}\sqrt{\rho_q}\cdot\rho_q^{-\frac{1}{2}} q_i|\psi_i\rangle\langle\psi_i|\rho_q^{-\frac{1}{2}} - p_iq_i|\psi_i\rangle\langle\psi_i| \cdot\rho_q^{-\frac{1}{2}}|\psi_i\rangle\langle\psi_i|\rho_q^{-\frac{1}{2}}$$

$$= \frac{1}{\sum_{j=1}^{n}\sqrt{q_j}}\, q_i|\psi_i\rangle\langle\psi_i|\rho_q^{-\frac{1}{2}} - p_iq_i|\psi_i\rangle\langle\psi_i| \cdot\rho_q^{-\frac{1}{2}}|\psi_i\rangle\langle\psi_i|\rho_q^{-\frac{1}{2}}$$

$$= \left(\frac{1}{\sum_{j=1}^{n}\sqrt{q_j}} - p_i\langle\psi_i|\rho_q^{-\frac{1}{2}}|\psi_i\rangle\right) q_i|\psi_i\rangle\langle\psi_i|\rho_q^{-\frac{1}{2}}$$

$$= 0$$

4. Conclusions

Quantum state discrimination serves as a basic tool for both quantum information theory and the foundation of quantum mechanics. Although general theorems regarding optimal state discrimination remain unsolved, much progress has been gained in recent years on some special cases. The technical difficulty in most general scenario may place strict limitations on the development of some quantum information tasks. Moreover, since the quantum state discrimination is closely related to some existing hard problems, developments in this direction could lead to new perspectives and challenges. The present review has provided a comprehensive introduction to quantum state discrimination and its selected applications.

Following the similar computation given in[3] adapted to the pure states case one may get the inverse map $R^{-1}:\varepsilon(\psi)\rightarrow\varepsilon(\psi)$. The existence of the map assures that the following equations

$$\frac{1}{\sum_{j=1}^{n}\sqrt{q_j}} = p_i\left\langle\psi_i\middle|\rho_q^{-1/2}\middle|\psi_i\right\rangle \quad \text{or} \quad p_i = \frac{\sum_{i=1}^{n}\sqrt{q_j}}{\left\langle\psi_i\middle|\rho_q^{-1/2}\middle|\psi_i\right\rangle}$$

This result is very simple to discriminate linearly independent pure states and this will provide a fruitful data for machine learning for discrimination problem. That will be next task for this paper.

References

[1] V.P. Belavkin, “Optimal multiple quantum statistical hypothesis testing”, Stochastices, vol.1. pp315-345, 1975.

[2] V.P. Belavkin and V. Maslov, “Design of optimal dynamic analyzers: Mathematical aspects of wave pattern recognition”, Mathematical Aspects of Computer Engineering Advances in Science and Technology in USSR Mir Publishers, 1988.

[3] C.W. Helstrom, “Quantum Detection and Estimation Theory”, Academic Press, New York, 1976.

[4] C. Mochon, “Family of generalized pretty good measurements and minimal-error pure-state discrimination problems for which they are opyimal”, Phys. Rev. A 73,032328, 2006.

[5] Y.C. Eldar, A. Magretski and G.C. Verghese, “Designing optimal quantum dectors via semidefinite programming”, IEEE Trans. Inform. Theory 49, pp1007-1012, 2003.

[6] S.M. Barnett and S. Croke, “Quantum state discrimination”, Adv. Opt. Photon. 1, pp 238, 2009.

[7] T. Singal, E. Kim and S. Ghosh, “A structure of minimum error discrimination for linearly independent states”, Phys. Rev. A 99, 052334, 2019.

[8] T. Singal and S. Ghosh, “Minimum error discrimination for an ensemble of linearly independent pure states”, J. Phys. A: Math. Theor. pp 49, 165304, 2016.
[9] P. Hausladen and W.K. Wootters, “A pretty good measurement for distinguishing quantum states”, J. Mod. Opt 41.pp 2385, 1994.
[10] P. Wittek, “Quantum Machine Learning-What quantum computing means to data mining”, Academic Press, 2014.