

Operating Characteristics for Classical and Quantum Binary Hypothesis Testing

Other titles in Foundations and Trends® in Signal Processing

Foundations of User-Centric Cell-Free Massive MIMO

Özlem Tugfe Demir, Emil Björnson and Luca Sanguinetti

ISBN: 978-1-68083-790-2

Data-Driven Multi-Microphone Speaker Localization on Manifolds

Bracha Laufer-Goldshtein, Ronen Talmon and Sharon Gannot

ISBN: 978-1-68083-736-0

Recent Advances in Clock Synchronization for Packet-Switched Networks

Anantha K. Karthik and Rick S. Blum

ISBN: 978-1-68083-726-1

Biomedical Image Reconstruction: From the Foundations to Deep Neural Networks

Michael T. McCann and Michael Unser

ISBN: 978-1-68083-650-9

Compressed Sensing with Applications in Wireless Networks

Markus Leinonen, Marian Codreanu and Georgios B. Giannakis

ISBN: 978-1-68083-646-2

Operating Characteristics for Classical and Quantum Binary Hypothesis Testing

Catherine A. Medlock

Massachusetts Institute of Technology
USA
cmedlock@mit.edu

Alan V. Oppenheim

Massachusetts Institute of Technology
USA
avo@mit.edu

now

the essence of knowledge

Boston — Delft

Foundations and Trends[®] in Signal Processing

Published, sold and distributed by:

now Publishers Inc.
PO Box 1024
Hanover, MA 02339
United States
Tel. +1-781-985-4510
www.nowpublishers.com
sales@nowpublishers.com

Outside North America:

now Publishers Inc.
PO Box 179
2600 AD Delft
The Netherlands
Tel. +31-6-51115274

The preferred citation for this publication is

C.A. Medlock and A.V. Oppenheim. *Operating Characteristics for Classical and Quantum Binary Hypothesis Testing*. Foundations and Trends[®] in Signal Processing, vol. 15, no. 1, pp. 1–120, 2021.

ISBN: 978-1-68083-883-1

© 2021 C.A. Medlock and A.V. Oppenheim

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, mechanical, photocopying, recording or otherwise, without prior written permission of the publishers.

Photocopying. In the USA: This journal is registered at the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923. Authorization to photocopy items for internal or personal use, or the internal or personal use of specific clients, is granted by now Publishers Inc for users registered with the Copyright Clearance Center (CCC). The 'services' for users can be found on the internet at: www.copyright.com

For those organizations that have been granted a photocopy license, a separate system of payment has been arranged. Authorization does not extend to other kinds of copying, such as that for general distribution, for advertising or promotional purposes, for creating new collective works, or for resale. In the rest of the world: Permission to photocopy must be obtained from the copyright owner. Please apply to now Publishers Inc., PO Box 1024, Hanover, MA 02339, USA; Tel. +1 781 871 0245; www.nowpublishers.com; sales@nowpublishers.com

now Publishers Inc. has an exclusive license to publish this material worldwide. Permission to use this content must be obtained from the copyright license holder. Please apply to now Publishers, PO Box 179, 2600 AD Delft, The Netherlands, www.nowpublishers.com; e-mail: sales@nowpublishers.com

Foundations and Trends[®] in Signal Processing

Volume 15, Issue 1, 2021

Editorial Board

Editor-in-Chief

Yonina Eldar
Weizmann Institute
Israel

Editors

Pao-Chi Chang
*National Central
University*

Pamela Cosman
*University of California,
San Diego*

Michelle Effros
*California Institute of
Technology*

Yariv Ephraim
George Mason University

Alfonso Farina
Selex ES

Sadaoki Furui
*Tokyo Institute of
Technology*

Georgios Giannakis
University of Minnesota

Vivek Goyal
Boston University

Sinan Gunturk
Courant Institute

Christine Guillemot
INRIA

Robert W. Heath, Jr.
*The University of Texas at
Austin*

Sheila Hemami
Northeastern University

Lina Karam
Arizona State University

Nick Kingsbury
University of Cambridge

Alex Kot
*Nanyang Technical
University*

Jelena Kovacevic
New York University

Geert Leus
TU Delft

Jia Li
*Pennsylvania State
University*

Henrique Malvar
Microsoft Research

B.S. Manjunath
*University of California,
Santa Barbara*

Urbashi Mitra
*University of Southern
California*

Björn Ottersten
KTH Stockholm

Vincent Poor
Princeton University

Anna Scaglione
*University of California,
Davis*

Mihaela van der Shaar
*University of California,
Los Angeles*

Nicholas D. Sidiropoulos
*Technical University of
Crete*

Michael Unser
EPFL

P.P. Vaidyanathan
*California Institute of
Technology*

Ami Wiesel
*The Hebrew University of
Jerusalem*

Min Wu
University of Maryland

Josiane Zerubia
INRIA

Editorial Scope

Topics

Foundations and Trends® in Signal Processing publishes survey and tutorial articles in the following topics:

- Adaptive signal processing
- Audio signal processing
- Biological and biomedical signal processing
- Complexity in signal processing
- Digital signal processing
- Distributed and network signal processing
- Image and video processing
- Linear and nonlinear filtering
- Multidimensional signal processing
- Multimodal signal processing
- Multirate signal processing
- Multiresolution signal processing
- Nonlinear signal processing
- Randomized algorithms in signal processing
- Sensor and multiple source signal processing, source separation
- Signal decompositions, subband and transform methods, sparse representations
- Signal processing for communications
- Signal processing for security and forensic analysis, biometric signal processing
- Signal quantization, sampling, analog-to-digital conversion, coding and compression
- Signal reconstruction, digital-to-analog conversion, enhancement, decoding and inverse problems
- Speech/audio/image/video compression
- Speech and spoken language processing
- Statistical/machine learning
- Statistical signal processing
 - Classification and detection
 - Estimation and regression
 - Tree-structured methods

Information for Librarians

Foundations and Trends® in Signal Processing, 2021, Volume 15, 4 issues. ISSN paper version 1932-8346. ISSN online version 1932-8354. Also available as a combined paper and online subscription.

Contents

1	Introduction	1
2	Operating Characteristics for Classical Binary Hypothesis Testing	7
2.1	Framework for Binary Hypothesis Testing	8
2.2	Minimum Probability of Error Decision Rules	11
2.3	Minimum Risk Decision Rules	12
2.4	Neyman-Pearson Optimal Decision Rules	13
2.5	Receiver Operating Characteristics	15
2.6	Classical Measurement Operating Characteristics	27
3	Operating Characteristics for Quantum Binary State Discrimination	28
3.1	Preliminaries	29
3.2	The Postulates of Quantum Mechanics	31
3.3	Quantum Binary State Discrimination	35
3.4	Minimum Probability of Error Decision Rules	37
3.5	Decision Operating Characteristics for Quantum Systems .	38
3.6	Measurement Operating Characteristics for Quantum Systems	39

4	A Perspective on Frame Representations	45
4.1	Preliminaries	46
4.2	Analysis and Synthesis Operators and Maps	48
4.3	Dual Frames	50
4.4	Parseval Frames and Naimark's Theorem	52
4.5	Frame Representations of Operator Spaces	56
4.6	Robustness of Frame Representations	60
5	An Operator Frame View of Quantum Measurement	65
5.1	Operator Spaces in Quantum Mechanics	66
5.2	Qubit State Discrimination using Platonic Solids	72
5.3	Robustness of IOC POVMs for Quantum State Estimation	73
6	Qubit State Discrimination on the Eto Spheres	78
6.1	Optimal Distributions of M Points on a Sphere	79
6.2	Results and Simulations	81
7	Summary, Reflections, and Further Thoughts	82
	Acknowledgements	89
	Appendices	90
A	Optional Appendices	91
A.1	Optimal Neyman-Pearson Decision Regions	91
A.2	Orthonormality of the $\{ w_k\rangle\}$ (Section 4.1)	92
A.3	Expressions for a Synthesis Map (Section 4.2)	95
A.4	The Adjoint of a Linear Transformation (Sections 4.2 and 4.3)	95
A.5	The Canonical Dual Frame (Sections 4.3 and 4.6)	98
A.6	Naimark's Theorem (Section 4.4.2)	100
A.7	An Oversampling Frame in Classical Signal Processing (Section 4.6.2)	101
A.8	Change of Basis in \mathcal{W} (Section 4.6.2)	104
A.9	Generalized Operator Frames (Section 4.5.2)	106
A.10	Distribution of Relative Frequencies (Section 5.3)	107

B Traditional Appendices	109
B.1 Generation of P_f - P_d Projection of LRT ROC from Suboptimal SVT ROC	109
B.2 QMOCs Generated using Standard Measurements are Ellipses	110
References	115

Operating Characteristics for Classical and Quantum Binary Hypothesis Testing

Catherine A. Medlock¹ and Alan V. Oppenheim²

¹*Massachusetts Institute of Technology; cmedlock@mit.edu*

²*Massachusetts Institute of Technology; avo@mit.edu*

ABSTRACT

This monograph addresses operating characteristics for binary hypothesis testing in both classical and quantum settings and overcomplete quantum measurements for quantum binary state discrimination. We specifically explore decision and measurement operating characteristics defined as the tradeoff between probability of detection and probability of false alarm as parameters of the pre-decision operator and the binary decision rule are varied. In the classical case we consider in detail the Neyman-Pearson optimality of the operating characteristics when they are generated using threshold tests on a scalar score variable rather than threshold tests on the likelihood ratio. In the quantum setting, informationally overcomplete POVMs are explored to provide robust quantum binary state discrimination. We focus on equal trace rank one POVMs which can be specified by arrangements of points on a sphere that we refer to as an Etro sphere.

Nomenclature

ROC	Receiver operating characteristic	3
POVM	Positive operator-valued measure	4
IC	Informationally complete	5
IOC	Informationally overcomplete	5
Etro	Equal trace rank one	5
LRT	Likelihood ratio test	7
SVT	Score variable threshold test	7
CDOC	Classical decision operating characteristic	7
CMOC	Classical measurement operating characteristic	7
MPE	Minimum probability of error	11
MAP	Maximum a posteriori	11
AUC	Area under an ROC	16
CDF	Cumulative distribution function	18

Nomenclature

iii

QMS	Quantum mechanical system	28
QDOC	Quantum decision operating characteristic	29
QMOC	Quantum measurement operating characteristic	29
ENTF	Equal norm tight frame	63
Etro	Equal trace rank one	65

Preamble

Our intention while preparing this monograph has been for it to be readable and interesting to an audience with a wide range of backgrounds. It is written to have a strong tutorial review flavor with some perspectives that hopefully many readers will find to be interesting and somewhat novel. We anticipate that many parts of the monograph will be familiar to readers with a strong background in classical signal processing and other parts to readers with a strong background in quantum mechanics. And it is our hope that both audiences will find the perspectives on the shared issues and overlap between the two fields to be interesting. Some readers may find it helpful in acquiring a broad sense of the scope of the monograph to start by reading the summary remarks and further thoughts given in Section 7. It should be noted however, that the discussion there uses terminology and notation introduced in earlier sections. In writing a monograph intended for an audience with diverse backgrounds part of the challenge is that there are many results referred to in the presentation that will be well-known to readers with backgrounds in one of the disciplines but less so in the other. And with some of these results, we anticipate that some of the readers will want to see or be reminded of a somewhat detailed explanation while others will be very familiar with it. To accommodate these differences we identify these as exercises for the reader to be worked out or not as they choose. The details for verifying those results are contained in the appendix

denoted as Appendix A. A second appendix denoted as Appendix B contains the details of a variety of possibly less familiar results that would be included in a traditional appendix mainly for the purpose of not interrupting the flow of the main body.

1

Introduction

Binary decisions guide our everyday lives in situations both critical and trivial. The choices made by politicians and physicians may have consequential implications on a global or individual scale. Perhaps less consequential is whether or not we choose to carry an umbrella on a cloudy day. Any choice made inherently involves a conscious, subconscious, or formal tradeoff between benefits and detriments. The defense of a country, the prolongation of life, the ability to keep dry in a downpour, may come at the cost of soldiers' lives, the quality of life of an individual patient, or the wasted effort of toting an umbrella on a rain-free day. In some cases our analysis of the compounding factors may be informal and the worst case outcome fairly inconsequential. But when the worst case outcome could have severe consequences as, for example, in a clinical setting or when deciding whether or not to fire a missile, it is much more desirable to have a structured analysis and process for arriving at a final decision. This may be a complicated task for many reasons, including the fact that the assignment of relative costs to the outcomes of the two possible decisions is often a judgement call itself. We may also lack a historical dataset that is large enough to allow for accurate estimation of important quantities such as the a priori probabilities, discussed further in Section 2.

In this monograph we focus on a particular set of well-studied metrics for framing the problem of binary hypothesis testing, keeping in mind that there are many alternatives, generalizations, and extensions of the viewpoints and results expressed here. We specifically consider the scenario in which one of two possible hypotheses, denoted as H_0 or H_1 , is true. The objective is to make a decision as to which is true using a sample value of a random variable often referred to as the score variable, which is comprised of one or more numerical values associated with the outcome of some measurement or observation. The score variable may be a scalar or a vector and may have been constructed as a composition of multiple measurements and observations. Traditionally H_0 is referred to as the null hypothesis and H_1 as the positive hypothesis, implying that H_1 is the hypothesis of significance (the target is present, the patient has the disease, etc.). In this monograph we use that convention. For convenience we refer to the entire system used to distinguish between the null and positive hypotheses as the discrimination system. The components of the discrimination system are defined in Section 2. Historically a quantity considered to be of significance in binary hypothesis testing is the probability of error, denoted as P_e and defined as the probability of identifying H_0 to be true given that H_1 is in fact true or vice versa. Other probabilities that may be of interest are (i) the probability of detection, denoted by P_d and defined as the probability of deciding that H_1 is true given that it is indeed true, (ii) the probability of a miss, denoted by P_m and defined as the probability of deciding that H_0 is true given that in fact H_1 is true, and (iii) the probability of false alarm, denoted by P_f and defined as the probability of deciding that H_1 is true given that H_0 is in fact true. Also of importance are the a priori probabilities associated with whether H_0 or H_1 is true apart from any measurement or decision. Various of these probabilities are connected mathematically through the rules of probability. For example, the probability of error can be expressed as a combination of the probability of detection, the probability of false alarm, and the underlying a priori probabilities.

Since in many scenarios the a priori probabilities are difficult or impossible to assess, it has become common in many contexts to formulate the decision making process without explicitly requiring knowledge

of these probabilities. One approach that has become widespread for accomplishing this is to focus on the tradeoff between P_f and P_d , often displayed using what is commonly referred to as a receiver operating characteristic (ROC). ROCs originated in the radar signal detection community, where they were used to characterize systems that detected the presence or absence of military targets during World War II [1]. The use of ROCs has become increasingly prevalent in a very broad set of application areas including biostatistics and machine learning [2]–[8]. In contrast to the problem of radar signal detection for which there are often good mathematical models for the signals and disturbances, in other contexts the score variable is typically a finely-tuned combination of many measurements and is therefore often less amenable to mathematical analysis and modeling.

More generally, the term operating characteristic is used in this monograph to refer to any characterization, such as a curve, table, or graph, of the tradeoff between P_f and P_d as one or more parameters of the discrimination system is varied. When displaying operating characteristics we will choose to utilize a two-dimensional graph of P_f versus P_d . Consequently the parameter or parameters being varied are not immediately visible or explicit. This is especially important in Sections 2.5.4 and 2.5.5 when we consider multiple operating characteristics that were generated using variations of distinct parameters but have identical graphs of P_f versus P_d . We take the viewpoint that an operating characteristic itself is essentially a trajectory in a higher-dimensional space with coordinates corresponding to all of the parameters being varied in addition to P_f and P_d . A graph of P_f versus P_d is the projection of this trajectory onto the P_f - P_d plane. Distinct trajectories including those with different numbers of variable parameters may correspond to the same P_f - P_d projection. For the majority of our discussion we will be concerned only with the characteristics of the P_f - P_d projection of a given operating characteristic. Thus, for the sake brevity we will only explicitly distinguish between an operating characteristic and its P_f - P_d projection when absolutely necessary, as in Sections 2.5.4 and 2.5.5.

Sections 2 and 3 of this monograph address operating characteristics associated with binary hypothesis testing in the classical setting and the setting of quantum mechanics, respectively. By “classical” we mean in

particular that the measurement or observation processes that lead to a realized value of the score variable are not constrained by the postulates of quantum mechanics. The principles of classical binary hypothesis testing are very well-understood and as outlined above, ROCs are widely used in many classical settings. The principles of quantum binary state discrimination are also well-formulated. As we discuss in Section 3, a typical formulation of the quantum binary state discrimination problem consists of a quantum mechanical system that has been prepared in one of two quantum states by two distinct laboratory procedures or physical environments, each corresponding to one of the two hypotheses H_0 or H_1 . The objective is to decide which procedure was used based on the outcome of a measurement on the system. An elegant solution to the problem of determining the measurement strategy that achieves minimum probability of error was derived by Helstrom [9].

Just as in the classical setting, the above formulation of the quantum binary hypothesis testing problem naturally involves a tradeoff between P_f and P_d and therefore it also involves the notion of an operating characteristic. But operating characteristics of any kind are significantly less prevalent in the quantum binary hypothesis testing literature. Perhaps one of the principal reasons for this is that although there are many similarities between the classical and quantum scenarios, there are also some fundamental differences that stem from the underlying differences between the postulates of classical versus quantum physics. Of particular importance and as described in Section 3 are the stipulations made by the postulates of quantum mechanics about the state of a quantum system and about the concept of quantum measurement. Of particular importance is the relationship between a specific quantum measurement and a set of Hermitian operators that form a positive operator-valued measure (POVM).

The theme of Sections 4 through 6 is how quantum measurements that employ redundant, or overcomplete, representations of the state of the system being measured can be used, at least in some cases, to increase the robustness of binary discrimination strategies. We start in Section 4 by describing our viewpoint on some of the basic concepts of frame theory, with the main objective of introducing the mathematical machinery and notation necessary to apply the concepts to quantum

measurement. We then describe how these concepts can be applied to an operator space consisting of all Hermitian operators on another Hilbert space. The relevant operator space \mathcal{V} in quantum mechanics contains all density operators and POVM elements. This leads to a discussion in Section 5 regarding informationally complete (IC) quantum measurements, which are measurements that map every quantum state to a unique probability distribution over the possible measurement outcomes [10]–[22]. IC quantum measurements that are strictly overcomplete are sometimes referred to as informationally overcomplete (IOC) quantum measurements [19]. While the benefits of using IOC measurements have been investigated in the context of quantum state estimation [19], [20], less attention has been given to their utility in quantum binary state discrimination. We review a fundamental result stating that every IC or IOC POVM is a frame for \mathcal{V} . IOC POVMs with a larger number M of elements correspond to frame representations of \mathcal{V} that are more overcomplete.

A crucial concept in our discussion of the operator space \mathcal{V} is a specific direct-sum decomposition of \mathcal{V} into two orthogonal subspaces \mathcal{U} and \mathcal{U}^\perp . All density operators have a constant component in \mathcal{U}^\perp and can be distinguished from each other by their components in \mathcal{U} . For the density operator of a qubit the component in \mathcal{U} corresponds to its Bloch vector. We define a counterpart to the Bloch ball and corresponding Bloch sphere in relation to the class of POVMs that we refer to as equal trace rank one (Etro) POVMs. An Etro POVM corresponding to a qubit measurement can be fully specified by M points on what we refer to as an Etro sphere of radius $\sqrt{2}/M$. This is exactly analogous to how a pure state qubit density operator can be specified by a single point on the Bloch sphere. POVMs constructed using Platonic solids are Etro POVMs in our terminology and are used often in the literature. We provide evidence through simulation that when POVMs constructed from Platonic solids are used for qubit binary state discrimination, there is a tradeoff in probability of error between the number L of identically-prepared quantum mechanical systems and the number M of POVM elements. POVMs constructed from Platonic solids have been of particular interest in the quantum state estimation community because they are all either IC or IOC, and because they

all provide straightforward state reconstruction formulas. Since we are interested in state discrimination rather than estimation, we do not require the state to be reconstructed. Consequently in Section 6 we also performed an exploratory investigation into IC and IOC POVMs constructed using other arrangements of points on an Etró sphere. In particular the problem we consider is that of distinguishing between two pure state qubit density operators. It is assumed that the angle between their Bloch vectors is known but that the overall alignment of the Bloch vectors relative to the Bloch sphere is not. Equivalently, it is assumed that the two Bloch vectors are known and the relative rotational orientation of the Bloch and Etró spheres is unknown. We compare the performance of a variety of POVMs using their minimum and maximum probabilities of error over all possible orientations, as well as the difference between the two. Intuitively it is expected that higher values of M and distributions of points on an Etró sphere that are maximally spread in some sense would lead to POVMs that are less sensitive to changes in the relative orientation of the Bloch and Etró spheres. Indeed, this is what we observed for values of M between 4 and 12 and for distributions of points that were maximally spread with respect to numerous established criteria.

Acknowledgements

The preparation of this manuscript began several years ago and evolved in ways that we didn't imagine at the beginning. Throughout this evolution we had the good fortune of having rich discussions with a number of colleagues. We are particularly eager to thank Isaac Chuang and Qi Ding for their collaborative efforts on various aspects of the work and James Ward for his insightful comments and detailed suggestions for improvement. We also had very helpful and in depth technical discussions with Petros Boufounos. We received valuable technical perspective from George Verghese, Yonina Eldar, and Meir Feder. Finally, we would like to thank Yonina Eldar for inviting us write this monograph and Mike Casey for patiently encouraging us and accepting moving deadlines as we continued to develop the content.

Appendices

A

Optional Appendices

Since this monograph was intended for an audience with a diverse set of backgrounds, the purpose of the derivations contained in the following Appendices A.1 to A.10 is to provide some level of detail surrounding concepts and results that are likely familiar to some readers but perhaps not to others. Many of the derivations can also be found in some form in many classical signal processing, linear algebra, or quantum mechanics textbooks and review monographs. The title of each section contains a reference to the section in the main body of the monograph where the concept was first mentioned.

A.1 Optimal Neyman-Pearson Decision Regions

The following reasoning was adapted from [25]. Assume that the decision region \mathcal{D} has been chosen to be Neyman-Pearson optimal. Then by definition it is impossible to modify it in such a way that P_d is increased while P_f stays the same. Mathematically we can think of modification of the decision region as taking two small portions of the real axis, one that lies in \mathcal{D} and is denoted as the interval $[s, s + ds]$ and one that lies outside of \mathcal{D} and is denoted as the interval $[s', s' + ds']$, and interchanging their decision region assignments. In other words, we

remove the interval $[s, s + ds]$ from \mathcal{D} and add the interval $[s', s' + ds']$. The resulting changes in P_f and P_d are

$$\Delta P_f = f_0(s') ds' - f_0(s) ds \quad (\text{A.1a})$$

$$\Delta P_d = f_1(s') ds' - f_1(s) ds. \quad (\text{A.1b})$$

If we assume that the value of P_f stays the same ($\Delta P_f = 0$), then since the original decision region was Neyman-Pearson optimal we know by definition that the value of P_d must have stayed the same or decreased ($\Delta P_d \leq 0$). Applying these conditions to Equations (A.1) and combining them together leads to the requirement that

$$\frac{f_1(s') ds'}{f_0(s') ds'} \geq \frac{f_1(s) ds}{f_0(s) ds}. \quad (\text{A.2})$$

After cancelling the factors of ds and ds' , the right-hand side of the inequality is equal to the likelihood ratio at the point $S = s$, which lay in the original, Neyman-Pearson optimal decision region \mathcal{D} . Similarly, the left-hand side is the likelihood ratio as the point $S = s'$, which lay outside of this region. Since the intervals $[s, s + ds]$ and $[s', s' + ds']$ were arbitrary so long as they lay inside or outside of \mathcal{D} , respectively, Equation (A.2) says that for the Neyman-Pearson optimal decision region \mathcal{D} , the likelihood ratio for values of the score variable lying inside \mathcal{D} is always greater than or equal to the likelihood ratio for values lying outside \mathcal{D} . In other words, the Neyman-Pearson optimal decision regions represent a threshold test on the likelihood ratio.

A.2 Orthonormality of the $\{|w_k\rangle\}$ (Section 4.1)

We wish to show that no generality is lost by assuming that the basis vectors $\{|w_k\rangle, 1 \leq k \leq M\}$ for \mathcal{W} are orthonormal with respect to the $\langle \cdot | \cdot \rangle$ inner product. Assume that they are not and let $\{|e_k\rangle\}$ be a basis for \mathcal{W} that is orthonormal with respect to the $\langle \cdot | \cdot \rangle$ inner product. Thus

$$\langle e_j | e_k \rangle = \delta_{jk}, \quad 1 \leq j, k \leq M, \quad (\text{A.3})$$

where δ_{jk} takes the value 1 if $j = k$ and 0 otherwise. Now we define a function $f(\cdot, \cdot)$ that takes two vectors in \mathcal{W} as input and outputs a

complex number. It is defined to satisfy the following properties,

$$f(a u_j + b u_k, u_\ell) = a^* f(u_j, u_\ell) + b^* f(u_k, u_\ell) \quad (\text{A.4a})$$

$$f(u_j, a u_k + b u_\ell) = a f(u_j, u_k) + b f(u_j, u_\ell) \quad (\text{A.4b})$$

$$f(u_j, u_k) = f(u_k, u_j)^* \quad (\text{A.4c})$$

$$f(w_j, w_k) = \delta_{jk}, \quad 1 \leq j, k \leq M. \quad (\text{A.4d})$$

In Equations (A.4), $|u_j\rangle$, $|u_k\rangle$, and $|u_\ell\rangle$ are arbitrary vectors in \mathcal{W} , a and b are arbitrary complex numbers, and the superscript $*$ indicates complex conjugation. Equations (A.4) imply that the function $f(\cdot, \cdot)$ is also positive definite. That is, if $|u\rangle = \sum_k c_k |w_k\rangle$ is an arbitrary nonzero vector in \mathcal{W} , then $f(u, u) > 0$ since

$$|u\rangle = \sum_{k=1}^M c_k |w_k\rangle \neq 0 \in \mathcal{W} \text{ (arbitrary nonzero vector in } \mathcal{W}) \quad (\text{A.5a})$$

$$f(u, u) = \left(\sum_{j=1}^M c_j |w_j\rangle, \sum_{k=1}^M c_k |w_k\rangle \right) \quad (\text{A.5b})$$

$$= \sum_{j,k=1}^M c_j^* c_k f(w_j, w_k) \text{ by conjugate bilinearity} \quad (\text{A.5c})$$

$$= \sum_{j=1}^M |c_j|^2 \text{ since } f(w_j, w_k) = \delta_{jk} \quad (\text{A.5d})$$

$$> 0 \text{ since } |u\rangle \neq 0. \quad (\text{A.5e})$$

Thus $f(\cdot, \cdot)$ is a valid inner product function on \mathcal{W} and $\{|w_k\rangle\}$ is orthonormal with respect to this inner product. We will now show that there is an invertible linear operator L on \mathcal{W} such that

$$f(L|u_1\rangle, L|u_2\rangle) = \langle u_1 | u_2 \rangle \quad (\text{A.6})$$

for all $|u_1\rangle, |u_2\rangle \in \mathcal{W}$. This implies that all calculations can be made with the $f(\cdot, \cdot)$ inner product, and then the inverse of L can be used to “translate” the answers back to the $\langle \cdot | \cdot \rangle$ inner product. Note that

because the $\{|w_k\rangle\}$ form a basis for \mathcal{W} , to satisfy Equation (A.6) it is sufficient to have a linear operator L such that

$$f(L|w_j\rangle, L|w_\ell\rangle) = \langle w_j|w_\ell\rangle, \quad 1 \leq j, \ell \leq M. \quad (\text{A.7})$$

Equation (A.6) follows from Equation (A.7) by the properties of the inner product functions $f(\cdot, \cdot)$ and $\langle \cdot | \cdot \rangle$. To find an appropriate linear operator L , let $|w_j\rangle$ and $|w_\ell\rangle$ be any two of the $\{|w_k\rangle\}$ (possibly with $j = \ell$) and write them in terms of the $\{|e_k\rangle\}$,

$$|w_j\rangle = \sum_{k=1}^M a_k |e_k\rangle, \quad |w_\ell\rangle = \sum_{k=1}^M c_k |e_k\rangle. \quad (\text{A.8})$$

Substituting into the left- and right-hand sides of Equation (A.6) and simplifying, we find

$$\begin{aligned} f(L|w_j\rangle, L|w_\ell\rangle) &= f\left(\sum_{k=1}^M a_k L|e_k\rangle, \sum_{m=1}^M d_m L|e_m\rangle\right) \\ &= \sum_{k,m=1}^M a_k^* d_m f(L|e_k\rangle, L|e_m\rangle) \end{aligned} \quad (\text{A.9a})$$

$$\langle w_j|w_\ell\rangle = \left\langle \sum_{k=1}^M a_k |e_k\rangle \left| \sum_{m=1}^M d_m |e_m\rangle \right. \right\rangle = \sum_{k=1}^M a_k^* d_k \quad (\text{A.9b})$$

For the two to be equal, it is sufficient to have $(L|e_k\rangle, L|e_m\rangle) = \delta_{km}$ for all $1 \leq k, m \leq M$. One operator that satisfies this condition is the linear operator L that is also defined to satisfy

$$L|e_k\rangle = |w_k\rangle, \quad 1 \leq k \leq M. \quad (\text{A.10})$$

This operator is clearly invertible, and using it to further simplify the left-hand side of Equation (A.7) leads to

$$(L|e_k\rangle, L|e_m\rangle) = \sum_{k,m=1}^M a_k^* d_m f(w_k, w_m) = \sum_{k=1}^M a_k^* d_k, \quad (\text{A.11})$$

so Equation (A.7) is satisfied.

A.3 Expressions for a Synthesis Map (Section 4.2)

To see why F_0 can sometimes be written in the form $F_0 = \sum_k |f_k\rangle \langle g_k|$ where the $\{|g_k\rangle\}$ are different from the $\{|w_k\rangle\}$, note that instead of defining F_0 using Equation (4.5) we could equivalently define it according to the relation

$$F|w_k\rangle = |f_k\rangle, \quad 1 \leq k \leq M. \quad (\text{A.12})$$

Equation (4.5) then follows by linearity. For Equation (A.12) to be true the $\{|g_j\rangle\}$ must satisfy the relation

$$\sum_{j=1}^M |f_j\rangle \langle g_j|w_k\rangle = |f_k\rangle, \quad 1 \leq k \leq M. \quad (\text{A.13})$$

We can then expand the $\{|f_j\rangle\}$ and $\{|g_j\rangle\}$ as linear combinations of the $\{|w_j\rangle\}$ to arrive at a system of linear equations in which the unknowns are the basis coefficients of the $\{|g_j\rangle\}$. Depending on the frame, the equations may or may not have multiple solutions.

Another way to look at it is to note that if the $\{|f_k\rangle\}$ are linearly dependent, then there is a linear combination of them that is equal to zero. Let $\{b_k\}$ be a set of coefficients such that

$$\sum_{k=1}^M b_k |f_k\rangle = 0. \quad (\text{A.14})$$

Then to satisfy Equation (A.13) it is sufficient to have

$$\langle g_j|w_k\rangle = \delta_{jk} b_k, \quad 1 \leq j, k \leq M, \quad (\text{A.15})$$

where $\delta_{jk} = 1$ if $j = k$ and 0 otherwise. This is again a system of linear equations that may or may not have more than one solution depending on the frame.

A.4 The Adjoint of a Linear Transformation (Sections 4.2 and 4.3)

Assume that $\{|f_k\rangle\}$ is a given frame for \mathcal{V} and that A_0 and F_0 are its analysis and synthesis maps, respectively. The adjoint of F_0 , denoted by F_0^\dagger , is defined as the linear operator on \mathcal{W} that satisfies

$$\langle u_1|F_0u_2\rangle = \langle F_0^\dagger u_1|u_2\rangle \text{ for all } |u_1\rangle, |u_2\rangle \in \mathcal{W}. \quad (\text{A.16})$$

We wish to show that $F_0^\dagger = A_0$. Substituting Equation (4.6) into the left-hand side of Equation (A.16) and using the linearity of the inner product, we find

$$\langle u_1 | F_0 u_2 \rangle = \sum_{k=1}^M \langle u_1 | f_k \rangle \langle w_k | u_2 \rangle. \quad (\text{A.17})$$

On the other hand, since $\langle x | y \rangle = \langle y | x \rangle^*$ for any two vectors $|x\rangle, |y\rangle \in \mathcal{W}$, we have $\langle F_0^\dagger u_1 | u_2 \rangle = \langle u_2 | F_0^\dagger u_1 \rangle^*$. Substituting back into Equation (A.16) leads to

$$\langle u_2 | F_0^\dagger u_1 \rangle = \left(\sum_{k=1}^M \langle u_1 | f_k \rangle \langle w_k | u_2 \rangle \right)^* \quad (\text{A.18a})$$

$$= \sum_{k=1}^M \langle u_2 | w_k \rangle \langle f_k | u_1 \rangle \quad (\text{A.18b})$$

$$= \langle u_2 | \left(\sum_{k=1}^M |w_k\rangle \langle f_k| \right) | u_1 \rangle, \quad (\text{A.18c})$$

and since this must be true for all $|u_1\rangle, |u_2\rangle \in \mathcal{W}$, we must have

$$F_0^\dagger = \sum_{k=1}^M |w_k\rangle \langle f_k| = A_0. \quad (\text{A.19})$$

Next let \mathcal{R} be an arbitrary subspace of \mathcal{W} and consider the orthogonal projection operator $\mathcal{P}_{\mathcal{R}}$ from \mathcal{W} onto \mathcal{R} . We wish to show that $\mathcal{P}_{\mathcal{R}}^\dagger = \mathcal{P}_{\mathcal{R}}$, i.e.,

$$\langle u_1 | \mathcal{P}_{\mathcal{R}} u_2 \rangle = \langle \mathcal{P}_{\mathcal{R}}^\dagger u_1 | u_2 \rangle \text{ for all } |u_1\rangle, |u_2\rangle \in \mathcal{W}. \quad (\text{A.20})$$

Equation (A.20) follows directly from decomposing $|u_1\rangle$ and $|u_2\rangle$ into their components in \mathcal{R} and \mathcal{R}^\perp .

The notion of the adjoint of a linear transformation applies much more broadly beyond linear transformations acting on finite-dimensional Hilbert spaces (see, for example, [36]). We consider one extension below to linear transformations whose input and output vector spaces may be different, although we still assume that both spaces are finite-dimensional for simplicity. We will continue to use the superscript \dagger

A.4. *The Adjoint of a Linear Transformation (Sections 4.2 and 4.3)* 97

to denote the adjoint. Consider two finite-dimensional Hilbert spaces $\mathcal{W}_1, \mathcal{W}_2$ and two linear transformations $T : \mathcal{W}_1 \mapsto \mathcal{W}_2, R : \mathcal{W}_2 \mapsto \mathcal{W}_1$ satisfying $R = T^\dagger$. We assume for simplicity that \mathcal{W}_1 and \mathcal{W}_2 have the same inner product denoted by $\langle \cdot | \cdot \rangle$, although this is solely for notational clarity. By definition we have

$$\langle u_2 | Tu_1 \rangle = \langle Ru_2 | u_1 \rangle \text{ for all } |u_1\rangle \in \mathcal{W}_1, |u_2\rangle \in \mathcal{W}_2. \quad (\text{A.21})$$

As stated in Section 4.2, taking the complex conjugate of both sides of Equation (A.21) implies that $T = R^\dagger$. It is well-known that T can always be written as a sum of rank-one operators of the form $|u_2\rangle \langle u_1|$ where $|u_1\rangle \in \mathcal{W}_1$ and $|u_2\rangle \in \mathcal{W}_2$. As an example, one possibility for expressing A in this form would be to use its singular value decomposition. It is straightforward to show using a derivation exactly analogous to the one given above that T^\dagger is the same sum of rank-one operators but with each term of the form $|u_2\rangle \langle u_1|$ replaced by $|u_1\rangle \langle u_2|$.

We will now show that $N(R) = R(T)^\perp$. It will follow by symmetry that $N(T) = R(R)^\perp$. Given an arbitrary vector $|u_2\rangle \in N(R)$, $|u_2\rangle$ must also be an element of $R(T)^\perp$. To see why this is true, let $|y\rangle$ be an arbitrary vector in $R(T)$. By definition there is some $|u_1\rangle \in \mathcal{W}_1$ such that $|y\rangle = T|u_1\rangle$. Then $|u_2\rangle$ is orthogonal to $|y\rangle$,

$$\langle y | u_2 \rangle = \langle Tu_1 | u_2 \rangle = \langle u_1 | Ru_2 \rangle = 0. \quad (\text{A.22})$$

Since $|y\rangle$ was arbitrary, this implies that $N(R)$ is contained in $R(T)^\perp$. On the other hand, let $|u_2\rangle \in \mathcal{W}_2$ be an arbitrary element of $R(T)^\perp$. By definition it must satisfy $\langle y | u_2 \rangle = 0$ for all $|y\rangle \in R(T)$, i.e., $\langle Tu_1 | u_2 \rangle = 0$ for all $|u_1\rangle \in \mathcal{W}_1$. Then $R|u_2\rangle$ must equal 0,

$$\langle Tu_1 | u_2 \rangle = 0 \text{ for all } |u_1\rangle \in \mathcal{W}_1 \quad (\text{A.23a})$$

$$\langle u_1 | Ru_2 \rangle = 0 \text{ for all } |u_1\rangle \in \mathcal{W}_1 \quad (\text{A.23b})$$

$$R|u_2\rangle = 0. \quad (\text{A.23c})$$

This implies that $R(T)^\perp$ is contained in $N(R)$, and because the reverse is also true it must be that the two are identical.

A.5 The Canonical Dual Frame (Sections 4.3 and 4.6)

Let $|v\rangle$ be an arbitrary vector in \mathcal{V} and let $\{|f_k\rangle\}$ be a frame for \mathcal{V} . We wish to find the dual frame $\{|\tilde{f}_k\rangle\}$ of $\{|f_k\rangle\}$ that minimizes the squared norm of the coefficient vector $\tilde{A}_0 |v\rangle = \sum_k \langle \tilde{f}_k | v \rangle |w_k\rangle$. It is sufficient to solve for the analysis map \tilde{A}_0 of the optimal dual frame. Denoting the synthesis map of $\{|f_k\rangle\}$ by F_0 , the problem can be formulated as

$$\underset{\tilde{A}_0 : \mathcal{V} \rightarrow \mathcal{W}}{\text{minimize}} \quad \|\tilde{A}_0 |v\rangle\|^2 \quad (\text{A.24a})$$

$$\text{subject to} \quad F_0 \tilde{A}_0 |v\rangle = |v\rangle \quad (\text{A.24b})$$

The optimal coefficient vector must satisfy $\tilde{A}_0 |v\rangle \in R(A_0)$. To see why this is true, note that $\tilde{A}_0 |v\rangle$ can always be written as the sum of a component in $R(A_0)$ and a component in $R(A_0)^\perp = N(F_0)$,

$$\tilde{A}_0 |v\rangle = |w_1\rangle + |w_2\rangle \quad (\text{A.25})$$

where $|w_1\rangle \in R(A_0)$ and $|w_2\rangle \in N(F_0)$. We have $\|\tilde{A}_0 |v\rangle\|^2 = \|w_1\|^2 + \|w_2\|^2$ and $F_0 \tilde{A}_0 |v\rangle = F_0 |w_1\rangle$. Assume that Equation (A.25) holds for a given dual frame. If $|w_2\rangle$ were nonzero, then we could always find a different dual frame with analysis map \hat{A}_0 satisfying $\hat{A}_0 |v\rangle = |w_1\rangle$. Equation (A.24b) would still be satisfied ($F_0 \hat{A}_0 |v\rangle = F_0 |w_1\rangle = |v\rangle$) and the new coefficient vector would have smaller squared norm ($\|\hat{A}_0 |v\rangle\|^2 \leq \|\tilde{A}_0 |v\rangle\|^2$). Next note that since $|v\rangle$ was assumed to be arbitrary, Equation (A.24b) implies that $\dim R(\tilde{A}_0) \geq N$. Since $\dim R(A_0) = N$ according to Section 4.2, the requirements that $\tilde{A}_0 |v\rangle \in R(A_0)$ for arbitrary $|v\rangle \in \mathcal{V}$ and $\dim R(\tilde{A}_0) \geq N$ together imply that the optimal analysis map satisfies $R(\tilde{A}_0) = R(A_0)$. Therefore, by definition of $R(A_0)$ we must have $\tilde{A}_0 |v\rangle = A_0 |x\rangle$ for some $|x\rangle \in \mathcal{V}$. Substituting into Equation (A.24b), we find that $F_0 \tilde{A}_0 |v\rangle = F_0 A_0 |x\rangle$. It is straightforward to show that the operator $(F_0 A_0)$, often referred to as the frame operator of $\{|f_k\rangle\}$, is always invertible. Thus, $|x\rangle = (F_0 A_0)^{-1} |v\rangle$ and so $\tilde{A}_0 |v\rangle = A_0 |x\rangle = A_0 (F_0 A_0)^{-1} |v\rangle$. Again using the fact that $|v\rangle$ was assumed to be arbitrary, this implies that $\tilde{A}_0 = A_0 (F_0 A_0)^{-1}$, which is exactly equal to the analysis map of the canonical dual frame.

Next we wish to show that of all dual frames, the canonical dual frame minimizes the expected reconstruction error \mathcal{E} as defined in

Equation (4.33). Note that the derivation given below does not assume that the analysis frame is an ENTF. The problem can be formulated as

$$\underset{\tilde{F}_0 : \mathcal{W} \rightarrow \mathcal{V}}{\text{minimize}} \quad \mathbb{E} \left[\|\tilde{F}_0 |w_e\rangle\|^2 \right] \quad (\text{A.26a})$$

$$\text{subject to} \quad \tilde{F}_0 A_0 |v\rangle = |v\rangle \text{ for all } |v\rangle \in \mathcal{V} \quad (\text{A.26b})$$

where the minimization is performed over all linear operators \tilde{F}_0 from \mathcal{W} to \mathcal{V} . Equation (A.26b), which in effect specifies that \tilde{F}_0 must be the synthesis operator of a frame that is dual to the analysis frame, amounts to the requirement that \tilde{F}_0 is a left-inverse of A_0 . A left-inverse is guaranteed to exist because as stated in Section 4.2, A_0 has rank N .

Let \tilde{F}_0 be an arbitrary left-inverse of A_0 and assume that $\{|w_k\rangle, 1 \leq k \leq M\}$ is an orthonormal basis for \mathcal{W} . Further assume that the $\{|w_k\rangle\}$ can be partitioned into an orthonormal $\{|w_k\rangle, 1 \leq k \leq N\}$ for $R(A_0)$ and an orthonormal $\{|w_k\rangle, N+1 \leq k \leq M\}$ for $R(A_0)^\perp$. To fully specify the operator \tilde{F}_0 , it is both necessary and sufficient to specify its action on each of the $\{|w_k\rangle\}$. Its action on $R(A_0)$ must be chosen to satisfy Equation (A.26b) while its action on $R(A_0)^\perp$ can be chosen to minimize $\mathbb{E} \left[\|\tilde{F}_0 |w_e\rangle\|^2 \right]$.

We first consider its action on $R(A_0)$. For each $\{|w_k\rangle, 1 \leq k \leq N\}$, there is a unique vector $|v_k\rangle \in \mathcal{V}$ satisfying $A_0 |v_k\rangle = |w_k\rangle$. Equation (A.26b) implies that $\tilde{F}_0 |w_k\rangle = |v_k\rangle$ for all $1 \leq k \leq N$. The action of \tilde{F}_0 on $R(A_0)^\perp$ can now be chosen to minimize $\|\tilde{F}_0 |w_e\rangle\|^2$. Note that any error vector $|w_e\rangle \in \mathcal{W}$ can be written uniquely as the sum of a component $|w_1\rangle \in R(A_0)$ and a component $|w_2\rangle \in R(A_0)^\perp$,

$$|w_e\rangle = |w_1\rangle + |w_2\rangle = \sum_{k=1}^N c_k |w_k\rangle + \sum_{k=N+1}^M c_k |w_k\rangle, \quad (\text{A.27})$$

where $\{c_k\}$ are the coefficients of $|w_e\rangle$ in the $\{|w_k\rangle\}$ basis. Since the $\{c_k\}$ are related to the $\{e_k\}$ by an orthogonal transformation in \mathcal{W} , they also have zero mean, variance σ^2 , and are pairwise uncorrelated. The expected value of $\|\tilde{F}_0 |w_e\rangle\|^2$ is

$$\mathbb{E} \left[\|\tilde{F}_0 |w_e\rangle\|^2 \right] = \mathbb{E} \left[\|\tilde{F}_0 |w_1\rangle + \tilde{F}_0 |w_2\rangle\|^2 \right]. \quad (\text{A.28a})$$

As we will show below, the expected value is minimized when $\tilde{F}_0 |w_2\rangle$ is set to zero for all possible values of \vec{w}_2 . The vector $\tilde{F}_0 |w_e\rangle$ is equal to

$$\tilde{F}_0 |w_e\rangle = \sum_{k=1}^N c_k \tilde{F}_0 |w_k\rangle + \sum_{k=N+1}^M c_k \tilde{F}_0 |w_k\rangle \quad (\text{A.29a})$$

$$= \sum_{k=1}^N c_k |v_k\rangle + \sum_{k=N+1}^M c_k \tilde{F}_0 |w_k\rangle. \quad (\text{A.29b})$$

Its squared norm is equal to $\langle \tilde{F}_0 |w_e\rangle | \tilde{F}_0 |w_e\rangle \rangle$, and since the $\{c_k\}$ are pairwise uncorrelated all cross terms are equal to zero. Thus,

$$\mathbb{E} \left[\|\tilde{F}_0 |w_e\rangle\|^2 \right] = \mathbb{E} \left[\sum_{k=1}^N c_k^2 \|v_k\|^2 + \sum_{k=N+1}^M c_k^2 \|\tilde{F}_0 |w_k\rangle\|^2 \right] \quad (\text{A.30a})$$

$$= \sum_{k=1}^N \mathbb{E}[c_k^2] \|v_k\|^2 + \sum_{k=N+1}^M \mathbb{E}[c_k^2] \|\tilde{F}_0 |w_k\rangle\|^2 \quad (\text{A.30b})$$

$$= \sigma^2 \sum_{k=1}^N \|v_k\|^2 + \sigma^2 \sum_{k=N+1}^M \|\tilde{F}_0 |w_k\rangle\|^2. \quad (\text{A.30c})$$

Since the value of the first sum is fixed and since all terms in both sums must be non-negative, the minimal value is obtained when the second sum is equal to zero, which happens when $\tilde{F}_0 |w_k\rangle = 0$ for all $N+1 \leq k \leq M$. Thus, the optimal left-inverse \tilde{F}_0 inverts A_0 over its range and acts as the zero operator on $R(A_0)^\perp$. The unique left-inverse with these properties is the Moore-Penrose pseudoinverse of A_0 (see, for example, Section 1 of [39]). Explicitly, the pseudoinverse is equal to

$$A_0^* = (A_0^\dagger A_0)^{-1} A_0^\dagger = (F_0 A_0)^{-1} F_0, \quad (\text{A.31})$$

and this corresponds exactly to the synthesis operator of the canonical dual frame [39].

A.6 Naimark's Theorem (Section 4.4.2)

Let $\{|f_k\rangle\}$ be an arbitrary frame for \mathcal{V} and assume that there exists an orthonormal basis $\{|w_k\rangle\}$ for \mathcal{W} that satisfies $\mathcal{P}_{\mathcal{V}} |w_k\rangle = |f_k\rangle$ for

$1 \leq k \leq M$. As explained in Section 4.4.3, an arbitrary vector $|v\rangle \in \mathcal{V}$ can always be written as

$$|v\rangle = \sum_{k=1}^M \langle w_k | v \rangle |w_k\rangle = \sum_{k=1}^M b_k |w_k\rangle, \quad (\text{A.32})$$

where we have defined $b_k = \langle w_k | v \rangle$. Since the $\{|w_k\rangle\}$ are an orthonormal basis for \mathcal{W} , the squared norm of $|v\rangle$ is equal to the sum of the squared magnitudes of the $\{b_k\}$, $\|v\|^2 = \sum_k |b_k|^2$. On the other hand and as also explained in Section 4.4.3, since the $\{|w_k\rangle\}$ satisfy the property $\mathcal{P}_{\mathcal{V}} |w_k\rangle = |f_k\rangle$ for $1 \leq k \leq M$, we also have

$$b_k = \langle w_k | v \rangle = \langle f_k | v \rangle, \quad 1 \leq k \leq M. \quad (\text{A.33})$$

Thus,

$$\sum_{k=1}^M |\langle f_k | v \rangle|^2 = \sum_{k=1}^M |b_k|^2 = \|v\|^2 \text{ for all } |v\rangle \in \mathcal{V}, \quad (\text{A.34})$$

which means by definition that $\{|f_k\rangle\}$ is a Parseval frame.

A.7 An Oversampling Frame in Classical Signal Processing (Section 4.6.2)

It is common in many classical signal processing scenarios to sample a bandlimited continuous-time (CT) signal at an integer multiple of its Nyquist rate. This tactic is sometimes referred to as oversampling [25]. In Appendix A.7 we verify explicitly that a particular set of shifted sinc functions forms an ENTFF for a space of bandlimited CT signals. Assume that \mathcal{V} is the set of all finite-energy CT signals bandlimited to $(-\Omega_N, \Omega_N)$ and let $T = \pi/(r\Omega_N)$ for an arbitrary positive integer r . We wish to show that $\{f_k(t)\}$, where

$$f_k(t) = \frac{\sin(\Omega_N(t - kT))}{\pi(t - kT)}, \quad k \text{ an integer}, \quad (\text{A.35})$$

is an ENTF for \mathcal{V} with frame bound $C = 1/T$ and $\|f_k\| = (rT)^{-1/2}$. By definition, this means that

$$\sum_{k=-\infty}^{\infty} |\langle f_k(t), v(t) \rangle|^2 = \frac{\|v(t)\|^2}{T} \quad \text{for all } v(t) \in \mathcal{V} \quad (\text{A.36a})$$

$$\|f_k(t)\| = \frac{1}{\sqrt{rT}} \quad \text{for all } k. \quad (\text{A.36b})$$

Note that we are assuming the following standard inner product on \mathcal{V} ,

$$\langle v_1(t), v_2(t) \rangle = \int_{-\infty}^{\infty} dt v_1(t) v_2(t) \quad \text{for all } v_1(t), v_2(t) \in \mathcal{V}. \quad (\text{A.37})$$

To verify that $\{f_k(t)\}$ satisfies Equation (A.36a), consider $f_k(t)$ for a specific value of k and an arbitrary element $v(t) \in \mathcal{V}$ with CT Fourier transform (CTFT) $V(j\Omega)$. Since $v(t)$ is an element of \mathcal{V} , $V(j\Omega)$ is only nonzero for $|\Omega| \leq \Omega_N$. We will first show that the inner product of $f_k(t)$ with $v(t)$ is equal to $v(t)$ sampled at time $t = kT$, i.e., $\langle f_k(t), v(t) \rangle = v(kT)$. Then we will use Parseval's theorem to show that

$$\sum_{k=-\infty}^{\infty} |\langle f_k(t), v(t) \rangle|^2 = \sum_{k=-\infty}^{\infty} |v(kT)|^2 = \frac{\|v(t)\|^2}{T}. \quad (\text{A.38})$$

Let $y(t)$ be the convolution of $f_k(t)$ with $v(t)$,

$$y(t) = \int_{-\infty}^{\infty} d\tau v(\tau) f_k(t - \tau). \quad (\text{A.39})$$

It is well-known that the CTFT of $y(t)$ is $Y(j\Omega) = F_k(j\Omega) V(j\Omega)$ where $F_k(j\Omega)$ is the CTFT of $f_k(t)$, defined by

$$F_k(j\Omega) = \begin{cases} e^{-j\Omega kT} & \text{if } |\Omega| \leq \Omega_N, \\ 0 & \text{else.} \end{cases} \quad (\text{A.40})$$

Since $f_k(t) = f_k(-t)$, the inner product of $f_k(t)$ with $v(t)$ is equal to $y(t)$ evaluated at $t = 0$,

$$\langle f_k(t), v(t) \rangle = \int_{-\infty}^{\infty} dt f_k(t) v(t) = \int_{-\infty}^{\infty} dt f_k(-t) v(t) = y(0). \quad (\text{A.41})$$

Using the definition of the inverse CTFT, we may express $y(0)$ as

$$y(0) = \left[\frac{1}{2\pi} \int_{-\infty}^{\infty} d\Omega Y(j\Omega) e^{j\Omega t} \right]_{t=0} = \frac{1}{2\pi} \int_{-\infty}^{\infty} d\Omega Y(j\Omega) \quad (\text{A.42a})$$

$$= \frac{1}{2\pi} \int_{-\infty}^{\infty} d\Omega F_k(j\Omega) V(j\Omega). \quad (\text{A.42b})$$

And now substituting Equation (A.40) into Equation (A.42) yields

$$\langle f_k(t), v(t) \rangle = \frac{1}{2\pi} \int_{-\infty}^{\infty} d\Omega V(j\Omega) e^{-j\Omega kT} = v(kT), \quad (\text{A.43})$$

where we have again used the definition of the inverse CTFT. Next we use Parseval's theorem to show that $\sum_k |v(kT)|^2 = \|v(t)\|^2/T$. The discrete time Fourier transform of the sequence $\{v(kT)\}$, denoted by $\hat{V}(e^{j\omega})$, is 2π -periodic and is related to $V(j\Omega)$ via

$$\hat{V}(e^{j\omega}) = \frac{1}{T} V\left(j\frac{\omega}{T}\right), \quad -\pi < \omega \leq \pi. \quad (\text{A.44})$$

Parseval's theorem for discrete time sequences states that

$$\sum_{k=-\infty}^{\infty} |v(kT)|^2 = \frac{1}{2\pi} \int_{-\pi}^{\pi} d\omega \left| \hat{V}(e^{j\omega}) \right|^2. \quad (\text{A.45})$$

Substituting Equation (A.44) into Equation (A.45) and changing the variable of integration to $\Omega = \omega/T$, we find

$$\sum_{k=-\infty}^{\infty} |v(kT)|^2 = \frac{1}{2\pi} \int_{-\pi}^{\pi} d\omega \frac{1}{T^2} \left| V\left(j\frac{\omega}{T}\right) \right|^2 = \frac{1}{2\pi} \int_{-\pi/T}^{\pi/T} d\Omega \frac{1}{T} |V(j\Omega)|^2 \quad (\text{A.46a})$$

$$= \frac{1}{2\pi T} \int_{-\infty}^{\infty} d\Omega |V(j\Omega)|^2 \quad (\text{A.46b})$$

Note that in going from Equation (A.46a) to (A.46b), we have used the fact that $\pi/T = r\Omega_N$ and the fact that by assumption, $V(j\Omega)$ is only nonzero for $|\Omega| \leq \Omega_N$. Finally, Parseval's theorem for CT signals states that

$$\frac{1}{2\pi} \int_{-\infty}^{\infty} d\Omega |V(j\Omega)|^2 = \int_{-\infty}^{\infty} dt |v(t)|^2 = \|v(t)\|^2 \text{ for all } v(t) \in \mathcal{V}. \quad (\text{A.47})$$

In summary, we have

$$\sum_{k=-\infty}^{\infty} |\langle f_k(t), v(t) \rangle|^2 = \sum_{k=-\infty}^{\infty} |v(kT)|^2 = \frac{\|v(t)\|^2}{T}. \quad (\text{A.48})$$

Since Equation (A.48) is true for any $v(t) \in \mathcal{V}$, $\{f_k(t)\}$ is a tight frame for \mathcal{V} with frame bound $C = 1/T$.

To verify Equation (A.36b), we use Parseval's theorem for CT signals to show that $\|f_k(t)\|^2$ is identical for all values of k ,

$$\|f_k(t)\|^2 = \int_{-\infty}^{\infty} dt |f_k(t)|^2 = \frac{1}{2\pi} \int_{-\infty}^{\infty} d\Omega |F_k(j\Omega)|^2 \quad (\text{A.49a})$$

$$= \frac{1}{2\pi} \int_{-\Omega_N}^{\Omega_N} d\Omega |e^{-j\Omega kT}|^2 = \frac{\Omega_N}{\pi}. \quad (\text{A.49b})$$

Since $\Omega_N = \pi/(rT)$, we have

$$\|f_k(t)\| = \frac{1}{\sqrt{rT}} \text{ for all } k. \quad (\text{A.50})$$

A.8 Change of Basis in \mathcal{W} (Section 4.6.2)

Consider $|e\rangle = \sum_k \Delta_k |w_k\rangle$ where the $\{\Delta_k\}$ each have zero mean and variance σ^2 and are pairwise uncorrelated, as specified in Equation (4.31). Let $\{|u_k\rangle\}$ be any orthonormal basis of \mathcal{W} . We wish to show that the components of $|e\rangle$ with respect to $\{|u_k\rangle\}$, which we denote by $\{\Delta'_k\}$, have these same properties. We start by expanding each of the $\{|w_k\rangle\}$ as a linear combination of the $\{|u_k\rangle\}$,

$$|w_k\rangle = \sum_{\ell=1}^M c_{k\ell} |u_\ell\rangle, \quad 1 \leq k \leq M. \quad (\text{A.51})$$

Since the $\{|w_k\rangle\}$ are orthonormal, the $\{c_{k\ell}\}$ satisfy

$$\sum_{\ell=1}^M c_{j\ell} c_{k\ell} = \delta_{jk}, \quad 1 \leq j, k \leq M, \quad (\text{A.52})$$

where δ_{jk} takes the value 1 if $j = k$ and 0 otherwise. Equation (A.52) implies that the $\{c_{k\ell}\}$ also satisfy

$$\sum_{k=1}^M c_{k\ell} c_{km} = \delta_{\ell m}, \quad 1 \leq \ell, m \leq M. \quad (\text{A.53})$$

To see why this is true, consider the $M \times M$ matrix D whose k th row and ℓ th column contains the element $c_{k\ell}$ for $1 \leq k, \ell \leq M$. Equation (A.52) states that the columns of D are orthonormal with respect to the standard inner product (often referred to as the dot product) on \mathbb{C}^M , the canonical M -dimensional complex coordinate space. A square matrix whose columns are orthonormal also has the property that its rows are orthonormal, which is exactly the meaning of Equation (A.53).

Substituting Equation (A.51) into the expression for $|e\rangle$ and rearranging, we find

$$|e\rangle = \sum_{k=1}^M \Delta_k \left(\sum_{\ell=1}^M c_{k\ell} |u_k\rangle \right) = \sum_{\ell=1}^M \left(\sum_{k=1}^M \Delta_k c_{k\ell} \right) |u_k\rangle. \quad (\text{A.54})$$

The components $\{\Delta'_k\}$ can thus be expressed as $\Delta'_k = \sum_{\ell} \Delta_k c_{k\ell}$ for $1 \leq k \leq M$. We may now derive the desired result using the linearity of expectation and the properties of the $\{\Delta_k\}$,

$$\mathbb{E}[\Delta'_k] = \sum_{k=1}^M \mathbb{E}[\Delta_k] c_{k\ell} = 0 \quad (\text{A.55a})$$

$$\mathbb{E}[\Delta'_j \Delta'_k] = \sum_{j,k=1}^M \mathbb{E}[\Delta_j \Delta_k] c_{j\ell} c_{k\ell} \quad (\text{A.55b})$$

$$= \begin{cases} \sigma^2 \sum_{k=1}^M c_{k\ell}^2 & \text{if } j = k \\ 0 & \text{if } j \neq k \end{cases} \quad (\text{A.55c})$$

$$= \begin{cases} \sigma^2 & \text{if } j = k \\ 0 & \text{if } j \neq k \end{cases} \quad \dots \quad (\text{A.55d})$$

Note that in Equation (A.55d) we have used Equation (A.53). Thus, we have shown that the $\{\Delta'_k\}$ have zero mean and variance σ^2 and are pairwise uncorrelated.

The fact that the $\{\Delta'_k\}$ are uncorrelated can also be interpreted in terms of the matrix D . This viewpoint is the one most commonly used when considering a general decorrelation transformation of a vector-valued random variable. Consider the vector-valued random variable $\vec{\Delta}$ whose k th component is the random variable Δ_k for $1 \leq k \leq M$.

Similarly, let $\vec{\Delta}'$ be the vector-valued random variable with components $\{\Delta'_k\}$. Since $\Delta'_k = \sum_{\ell} \Delta_k c_{k\ell}$ for $1 \leq k \leq M$, we have $\vec{\Delta}' = D \vec{\Delta}$. Since the components of $\vec{\Delta}'$ clearly have zero mean, the covariance matrix of $\vec{\Delta}'$ can be expressed as

$$\mathbb{E}[\vec{\Delta}'(\vec{\Delta}')^T] = D \mathbb{E}[\vec{\Delta} \vec{\Delta}^T] D^T. \quad (\text{A.56})$$

The $\{\Delta_k\}$ satisfy $\mathbb{E}[\Delta_j \Delta_k] = \sigma^2 \delta_{jk}$ by assumption, implying that $\mathbb{E}[\vec{\Delta} \vec{\Delta}^T] = \sigma^2 I_M$ where I_M is the $M \times M$ identity matrix. Thus, Equation (A.56) can be simplified to

$$\mathbb{E}[\vec{\Delta}'(\vec{\Delta}')^T] = \sigma^2 D I_M D^T = \sigma^2 D D^T = \sigma^2 I_M, \quad (\text{A.57})$$

where in the last line we have used that fact that $D D^T = I_M$ because the rows of D are orthonormal. The component in the j th row and k th column of the matrix $\mathbb{E}[\vec{\Delta}'(\vec{\Delta}')^T]$ is $\mathbb{E}[\Delta'_j \Delta'_k]$, and Equation (A.56) states that it is equal to σ^2 if $j = k$ and 0 otherwise, as expected.

A.9 Generalized Operator Frames (Section 4.5.2)

The definition of a special class of IC POVMs referred to as tight IC POVMs relies on the notion of a generalized operator frame with respect to (w.r.t.) a given measure, as introduced in [11]. Given a measure $\alpha(\cdot)$ that maps each $1 \leq k \leq M$ to a non-negative number $\alpha(k) \geq 0$, a set of operators $\{|F_k\rangle\rangle\}$ in \mathcal{V} is a generalized operator frame for \mathcal{V} w.r.t. $\alpha(\cdot)$ if

$$C \|V\|^2 \leq \sum_{k=1}^M \alpha(k) |\langle\langle F_k|V\rangle\rangle|^2 \leq D \|V\|^2 \text{ for all } |V\rangle\rangle \in \mathcal{V}, \quad (\text{A.58})$$

for some $0 < C \leq D < \infty$.

Example A.1. Equation (4.26) is a special case of Equation (A.58) in which $\alpha(\cdot)$ is the counting measure, defined by

$$\alpha(k) = 1, \quad 1 \leq k \leq M. \quad (\text{A.59})$$

Thus, a set of operators satisfying Equation (4.26) is a frame for \mathcal{V} w.r.t. the counting measure.

Example A.2. The trace measure [11] is defined by

$$\alpha(k) = \text{Tr}(F_k), \quad 1 \leq k \leq M. \quad (\text{A.60})$$

Note that Equation (A.60) only represents a valid measure when $\text{Tr}(F_k) \geq 0$ for all values of k . One instance in which this is true is when the $\{|F_k\rangle\rangle\}$ are the elements of a POVM. Substituting Equation (A.60) into Equation (A.58) leads to

$$C \|V\|^2 \leq \sum_{k=1}^M \text{Tr}(F_k) |\langle\langle F_k|V\rangle\rangle|^2 \leq D \|V\|^2 \text{ for all } |V\rangle\rangle \in \mathcal{V} \quad (\text{A.61})$$

for some $0 < C \leq D < \infty$. A set of operators $\{|F_k\rangle\rangle\}$ in \mathcal{V} satisfying Equation (A.61) is a frame for \mathcal{V} w.r.t. the trace measure. A tight frame for \mathcal{V} w.r.t. the trace measure is one for which the upper and lower bounds in Equation (A.61) can both be set to the same value. Note that in finite dimensions, if $\{|F_k\rangle\rangle\}$ is a frame for \mathcal{V} w.r.t. the trace measure, then $\{\sqrt{|\text{Tr}(F_k)|} |F_k\rangle\rangle\}$ is a frame for \mathcal{V} w.r.t. the counting measure.

A.10 Distribution of Relative Frequencies (Section 5.3)

While the following derivation is motivated by the quantum state estimation problem considered in Section 5.3, the concepts and conclusions rely only on the laws of probability and not on the postulates of quantum mechanics. Therefore we state the results without any reference to density operators or quantum measurement. Let X be a discrete random variable that takes values in the set $\{1, \dots, M\}$ with probability mass function (PMF) $\{p(1), \dots, p(M)\}$, i.e.,

$$X = k \text{ with probability } p(k), \quad 1 \leq k \leq M. \quad (\text{A.62})$$

Assume that $\{x_i, 1 \leq i \leq L\}$ is a set of L independent realizations of X and consider the set of relative frequencies $\{\hat{p}(k) = \ell_k/L\}$, where ℓ_k is the number of realizations $\{x_i\}$ that are equal to k . Defining $d_k = \hat{p}(k) - p(k)$ for $1 \leq k \leq M$, the goal is to evaluate the expected values $\mathbb{E}[d_k]$ and $\mathbb{E}[d_j d_k]$ for all $1 \leq j, k \leq M$.

We first address the case where $j = k$. Let k be a fixed integer between 1 and M . To compute $\mathbb{E}[d_k]$, note that the value of ℓ_k is

binomially distributed with parameters $p(k)$ and L [ref]. Its expected value is $\mathbb{E}[\ell_k] = L p(k)$ and its variance is $\text{var}(\ell_k) = L p(k) (1 - p(k))$. Using linearity of expectation we find that, unsurprisingly, the expected value of d_k is equal to zero,

$$\mathbb{E}[d_k] = \mathbb{E} \left[p(k) - \frac{\ell_k}{L} \right] = p(k) - \frac{L p(k)}{L} = 0. \quad (\text{A.63})$$

The variance of d_k is

$$\text{var}(d_k) = \text{var} \left(p(k) - \frac{\ell_k}{L} \right) = \frac{\text{var}(\ell_k)}{L^2} = \frac{p(k) (1 - p(k))}{L}. \quad (\text{A.64})$$

Furthermore, since $\mathbb{E}[d_k] = 0$ we have $\mathbb{E}[d_k^2] = \text{var}(d_k)$.

Now let j and k be fixed integers between 1 and M with $j \neq k$. To compute $\mathbb{E}[d_j d_k]$, note that the joint distribution of $\{\ell_1, \dots, \ell_M\}$ is given by a multinomial distribution with parameters L and $\{p_1, \dots, p_M\}$ [ref]. It can be shown using the properties of the multinomial distribution that

$$\mathbb{E}[\ell_j \ell_k] = L p(j) p(k) (L - 1). \quad (\text{A.65})$$

Using linearity of expectation and the fact that $\mathbb{E}[\ell_j] = L p(j)$ and $\mathbb{E}[\ell_k] = L p(k)$, we find that the value of $\mathbb{E}[d_j d_k]$ is

$$\mathbb{E}[d_j d_k] = \mathbb{E} \left[\left(\frac{\ell_j}{L} - p(j) \right) \left(\frac{\ell_k}{L} - p(k) \right) \right] \quad (\text{A.66a})$$

$$= \frac{\mathbb{E}[\ell_j \ell_k]}{L^2} - p(j) p(k) = -\frac{p(j) p(k)}{L}. \quad (\text{A.66b})$$

B

Traditional Appendices

B.1 Generation of P_f - P_d Projection of LRT ROC from Suboptimal SVT ROC

An explanation of the procedure is shown in Figure B.1. The graphs in Figure B.1a show P_f^{SVT} , P_d^{SVT} , and the derivative $dP_d^{\text{SVT}}/dP_f^{\text{SVT}}$ as functions of the score variable. According to Equation (2.31) the derivative is equal to the likelihood ratio function. Note that these graphs are caricatures used only for visualization, since the procedure does not require explicit knowledge of any of the aforementioned quantities as functions of the score variable. A fixed LRT threshold value $\eta_0 \geq 0$ identifies multiple disjoint regions of s for which $f_1(s)/f_0(s) \geq \eta_0$, highlighted in green for $\eta_0 = 1$ in the figure. Together these regions comprise $\mathcal{D}_{\text{LRT}}(\eta_0)$. Each individual region j covers an interval $[a_j, b_j]$ with $a_j < b_j$ and corresponds to the segment in the P_f - P_d projection of the SVT ROC with endpoints $(h_f(b_j), h_d(b_j))$ and $(h_f(a_j), h_d(a_j))$. The integrals of $f_0(\cdot)$ and $f_1(\cdot)$ over the region, shown in Figure B.1b,

can be expressed as

$$\int_{a_j}^{b_j} ds f_0(s) = (1 - F_0(a_j)) - (1 - F_0(b_j)) = h_f(a_j) - h_f(b_j) \quad (\text{B.1a})$$

$$\int_{a_j}^{b_j} ds f_1(s) = (1 - F_1(a_j)) - (1 - F_1(b_j)) = h_d(a_j) - h_d(b_j) \quad (\text{B.1b})$$

which are simply the changes in P_f^{SVT} and P_d^{SVT} between the endpoints of the segment. Summing these changes over all regions corresponds to summing the integrals of $f_0(\cdot)$ and $f_1(\cdot)$ over each disjoint portion of $\mathcal{D}_{\text{LRT}}(\eta)$. The resulting P_f - P_d projection of the LRT ROC made by varying η_0 over its entire range is illustrated in Figure B.1c.

B.2 QMOCs Generated using Standard Measurements are Ellipses

We show that any QMOC generated according to the method described in Example 3.3 of Section 3.6, in which two-outcome quantum measurements with associated standard POVMs are used to distinguish between arbitrary qubit density matrices ρ_0 and ρ_1 with $d = 2$, is an ellipse. More specifically, it is a rotated ellipse in the P_f - P_d plane centered at the point $(1/2, 1/2)$. The derivation also applies to the case where ρ_0 and ρ_1 represent two pure states with $d > 2$, as long as the standard POVMs used to generate the QMOC have the following properties: The first two elements of the POVM, E_1 and E_2 , should be analogous to those defined by Equation (3.19), but with the additional requirement that $|v_1\rangle$ and $|v_2\rangle$ should lie in the plane defined by the two pure states. The other measurement elements must therefore project onto subspaces of the orthogonal complement of that plane. Again the final decision is H_1 if the measurement outcome associated with E_2 occurs and H_0 if the measurement outcome associated with E_1 occurs. The other possible outcomes have zero probability of occurring and can be associated with either final decision. Essentially, this reduces the problem to that of distinguishing between two pure states with $d = 2$.

B.2. QMOCs Generated using Standard Measurements are Ellipses 111

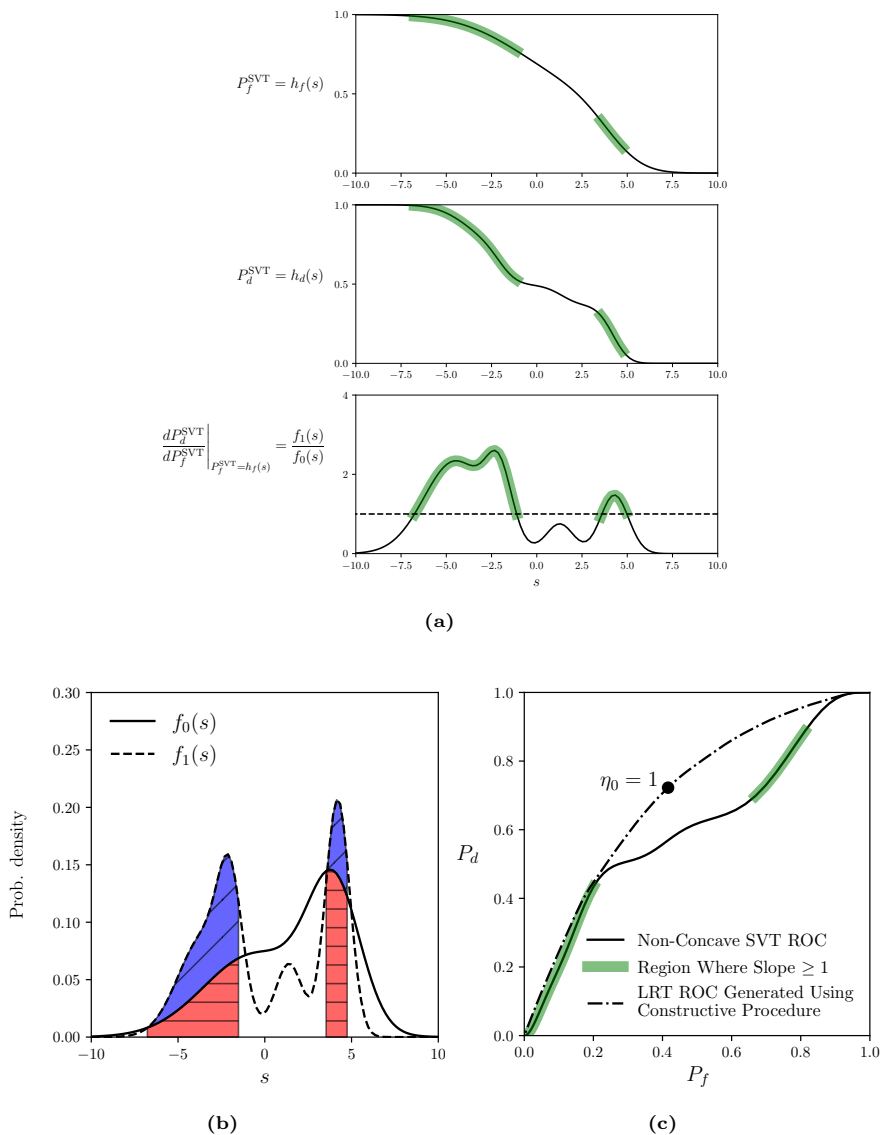


Figure B.1: (a) Probability of false alarm, probability of detection, and derivative of SVT ROC as functions of the score variable. The highlighted regions represent regions where the derivative of the curve is greater than or equal to $\eta_0 = 1$. (b) Integrals of the conditional PDFs over the LRT decision region $\mathcal{D}_{\text{LRT}}(\eta_0)$ for $\eta_0 = 1$. (c) P_f - P_d projections of non-concave SVT ROC and LRT ROC generated using the procedure given in the text.

The coordinates of the QMOC in terms of the angle θ are

$$P_f = \text{Tr}(E_1 \rho_0) = a_0 \cos^2 \left(\frac{\theta}{2} \right) + a_1 \sin^2 \left(\frac{\theta}{2} \right) \quad (\text{B.2a})$$

$$P_d = \text{Tr}(E_1 \rho_1) = b_0 \cos^2 \left(\frac{\theta - \alpha}{2} \right) + b_1 \sin^2 \left(\frac{\theta - \alpha}{2} \right). \quad (\text{B.2b})$$

Assuming for the moment that this is the parametric equation of a rotated ellipse centered at $(1/2, 1/2)$, we can center the ellipse at the origin and use trigonometric identities to derive equations for the centered coordinates,

$$P_f - \frac{1}{2} = \frac{a_0 - a_1}{2} \cos \theta \quad (\text{B.3a})$$

$$P_f - \frac{1}{2} = \frac{b_0 - b_1}{2} \cos(\theta - \alpha). \quad (\text{B.3b})$$

For ease of notation we now make the substitutions

$$x = P_f - \frac{1}{2}, \quad y = P_d - \frac{1}{2}, \quad a = \frac{a_0 - a_1}{2}, \quad b = \frac{b_0 - b_1}{2}, \quad (\text{B.4})$$

and introduce the functions $f_x(\cdot)$ and $f_y(\cdot)$, so that the centered coordinates become

$$x = f_x(\theta) = a \cos \theta \quad (\text{B.5a})$$

$$y = f_y(\theta) = b \cos(\theta - \alpha). \quad (\text{B.5b})$$

(Note that the x and y above should not be confused with the $\{|x_i\}$ and $\{|y_i\}$ in Equations (3.11).) The objective now is to show that $x = f_x(\theta)$ and $y = f_y(\theta)$ represent a rotated ellipse centered at the origin. That is, the objective is to show that they can be written in the form

$$x = g_x(t) = q \cos \beta \cos t - r \sin \beta \sin t \quad (\text{B.6a})$$

$$y = g_y(t) = q \sin \beta \cos t + r \cos \beta \sin t \quad (\text{B.6b})$$

for some angle of rotation β from the horizontal, semi-major axis q , semi-minor axis r , and parameter t (which will prove inconsequential for our purposes). The functions $g_x(\cdot)$ and $g_y(\cdot)$ have been introduced for convenience. We can solve for the parameters q , r , β in terms of the

B.2. QMOCs Generated using Standard Measurements are Ellipses 113

known values of a , b , α by using Equations (B.5) and (B.6) to find the points on each ellipse with maximum x - and y -values and then setting their coordinates equal to one another. Taking the derivative of $f_x(\theta)$ and setting it to zero, we find that the point with maximum x -value occurs at $\theta_x = 0$ and has coordinates $(f_x(0), f_y(0)) = (a, b)$. The point with maximum y -value occurs at $\theta_y = \alpha$ and has coordinates $(f_x(\alpha), f_y(\alpha)) = (a \cos \alpha, b)$. Similarly, the point on the ellipse described by Equations (B.6) with maximum x -value occurs at $t_x = \tan^{-1}(-(r/q) \tan \beta)$ and has coordinates

$$g_x(t_x) = \sqrt{q^2 \cos^2 \beta + r^2 \sin^2 \beta} \quad (\text{B.7a})$$

$$g_y(t_x) = \frac{q^2 - r^2}{\sqrt{q^2 / \sin^2 \beta + r^2 / \cos^2 \beta}}. \quad (\text{B.7b})$$

The point with maximum y -value occurs at $t_y = \tan^{-1}(r/(q \tan \beta))$ and has coordinates

$$g_x(t_y) = \frac{q^2 - r^2}{\sqrt{q^2 / \cos^2 \beta + r^2 / \sin^2 \beta}} \quad (\text{B.8a})$$

$$g_y(t_y) = \sqrt{q^2 \sin^2 \beta + r^2 \cos^2 \beta}. \quad (\text{B.8b})$$

Setting $f_x(0) = g_x(t_x)$, $f_y(0) = g_y(t_x)$, $f_x(\alpha) = g_x(t_y)$, and $f_y(\alpha) = g_y(t_y)$ and solving for q , r , and β in terms of a , b , and α yields

$$\beta = \frac{1}{2} \tan^{-1} \left(\frac{2ab \cos \alpha}{a^2 - b^2} \right) \quad (\text{B.9a})$$

$$q = \left[\frac{1}{2} \left(a^2 + b^2 + \frac{a^2 - b^2}{\cos(2\beta)} \right) \right]^{1/2} \quad (\text{B.9b})$$

$$r = \left[\frac{1}{2} \left(a^2 + b^2 - \frac{a^2 - b^2}{\cos(2\beta)} \right) \right]^{1/2}. \quad (\text{B.9c})$$

It can be verified through straightforward algebra that when β , q , and r are given by Equations (B.9), the coordinates $x = f_x(\theta)$, $y = f_y(\theta)$ in Equation (B.5) satisfy the equation that defines an ellipse:

$Ax^2 + Bxy + Cy^2 + D = 0$ with $B^2 - 4AC < 0$, where

$$A = q^2 \sin^2 \beta + r^2 \cos^2 \beta \quad (\text{B.10a})$$

$$B = 2(q^2 - r^2) \sin \beta \cos \beta \quad (\text{B.10b})$$

$$C = q^2 \cos^2 \beta + r^2 \sin^2 \beta \quad (\text{B.10c})$$

$$D = -q^2 r^2. \quad (\text{B.10d})$$

This verifies our initial assumption that $x = f_x(\theta)$ and $y = f_y(\theta)$ are the coordinates of an ellipse that is centered at the origin, rotated by an angle β from the horizontal, and has semi-major axis q and semi-minor axis r . The original QMOC is the same ellipse centered at the point $(1/2, 1/2)$.

References

- [1] J. A. Swets, R. M. Dawes, and J. Monahan, "Better decisions through science," *Scientific American*, vol. 283, no. 4, 2000, pp. 82–87.
- [2] T. Fawcett, "An Introduction to ROC Analysis," *Pattern Recognition Letters*, vol. 27, no. 8, 2006, pp. 861–874.
- [3] N. A. Obuchowski, "Receiver Operating Characteristic Curves and Their Use in Radiology," *Radiology*, vol. 229, no. 1, 2003, pp. 3–8.
- [4] M. H. Zweig and G. Campbell, "Receiver-Operating Characteristic (ROC) Plots: A Fundamental Evaluation Tool in Clinical Medicine," *Clinical Chemistry*, vol. 39, no. 4, 1993, pp. 561–577.
- [5] K. A. Spackman, "Signal Detection Theory: Valuable Tools for Evaluating Inductive Learning," in *Proceedings of the Sixth International Workshop on Machine Learning*, Morgan Kaufmann Publishers Inc., pp. 160–163, 1989.
- [6] J. R. Beck and E. K. Shultz, "The Use of Relative Operating Characteristic (ROC) Curves in Test Performance Evaluation," *Archives of Pathology & Laboratory Medicine*, vol. 110, no. 1, 1986, pp. 13–20.

- [7] T. N. Sainath and C. Parada, “Convolutional Neural Networks for Small-Footprint Keyword Spotting,” in *Proceedings of the Sixteenth Annual Conference of the International Speech Communication Association*, 2015.
- [8] R. M. Stein, “The Relationship Between Default Prediction and Lending Profits: Integrating ROC Analysis and Loan Pricing,” *Journal of Banking & Finance*, vol. 29, no. 5, 2005, pp. 1213–1236.
- [9] C. W. Helstrom, “Detection Theory and Quantum Mechanics,” *Information and Control*, vol. 10, no. 3, 1967, pp. 254–291.
- [10] G. M. D’Ariano, P. Perinotti, and M. F. Sacchi, “Informationally Complete Measurements and Group Representation,” *Journal of Optics B: Quantum and Semiclassical Optics*, vol. 6, no. 6, 2004, S487–S491.
- [11] A. J. Scott, “Tight Informationally Complete Quantum Measurements,” *Journal of Physics A: Mathematical and General*, vol. 39, no. 43, 2006, pp. 13 507–13 530.
- [12] J. M. Renes, R. Blume-Kohout, A. J. Scott, and C. M. Caves, “Symmetric Informationally Complete Quantum Measurements,” *Journal of Mathematical Physics*, vol. 45, no. 6, 2004, pp. 2171–2180.
- [13] B. Bodmann and J. Haas, *A Short History of Frames and Quantum Designs*, 2017. arXiv: [1709.01958](https://arxiv.org/abs/1709.01958) [quant-ph].
- [14] M. B. Ruskai, “Some Connections between Frames, Mutually Unbiased Bases, and POVM’s in Quantum Information Theory,” *Acta Applicandae Mathematicae*, vol. 108, no. 3, 2009, pp. 709–719.
- [15] S. T. Flammia, A. Silberfarb, and C. M. Caves, “Minimal Informationally Complete Measurements for Pure States,” *Foundations of Physics*, vol. 35, no. 12, 2005, pp. 1985–2006.
- [16] J. Finkelstein, “Pure-State Informationally Complete and ‘Really’ Complete Measurements,” *Physical Review A*, vol. 70, no. 5, 2004, 052107.
- [17] D. M. Appleby, “Symmetric Informationally Complete Measurements of Arbitrary Rank,” *Optics and Spectroscopy*, vol. 103, no. 3, 2007, pp. 416–428.

- [18] C. A. Fuchs, M. C. Hoang, and B. C. Stacey, “The SIC Question: History and State of Play,” *Axioms*, vol. 6, no. 3, 2017, 21.
- [19] H. Zhu, “Quantum State Estimation and Symmetric Informationally Complete POMs,” Ph.D. dissertation, PhD thesis, National University of Singapore, 2012. 1, 5, 2012.
- [20] H. Zhu, “Quantum State Estimation with Informationally Overcomplete Measurements,” *Physical Review A*, vol. 90, no. 1, 2014, 012115.
- [21] H. Zhu, “Super-Symmetric Informationally Complete Measurements,” *Annals of Physics*, vol. 362, 2015, pp. 311–326.
- [22] G. M. D’Ariano and P. Perinotti, “Optimal Data Processing for Quantum Measurements,” *Physical Review Letters*, vol. 98, no. 2, 2007, 020403.
- [23] C. A. Medlock and A. V. Oppenheim, “Optimal ROC Curves from Score Variable Threshold Tests,” in *ICASSP 2019-2019 IEEE International Conference on Acoustics, Speech and Signal Processing*, IEEE, pp. 5327–5330, 2019.
- [24] C. W. Helstrom, *Elements of Signal Detection and Estimation*. Prentice-Hall, Inc., 1994.
- [25] A. V. Oppenheim and G. C. Verghese, *Signals, Systems and Inference*. Pearson, 2015.
- [26] J. M. Lobo, A. Jiménez-Valverde, and R. Real, “Auc: A misleading measure of the performance of predictive distribution models,” *Global Ecology and Biogeography*, vol. 17, no. 2, 2008, pp. 145–151.
- [27] D. J. Hand, “Measuring Classifier Performance: A Coherent Alternative to the Area Under the ROC Curve,” *Machine Learning*, vol. 77, no. 1, 2009, pp. 103–123.
- [28] M. Rosenblatt, “Remarks on Some Nonparametric Estimates of a Density Function,” *The Annals of Mathematical Statistics*, vol. 27, no. 3, 1956, pp. 832–837.
- [29] E. Parzen, “On Estimation of a Probability Density Function and Mode,” *The Annals of Mathematical Statistics*, vol. 33, no. 3, 1962, pp. 1065–1076.
- [30] E. Torgersen, *Comparison of Statistical Experiments*, vol. 36. Cambridge University Press, 1991.

- [31] H. L. Van Trees, *Detection, Estimation, and Modulation Theory, Part I: Detection, Estimation, and Linear Modulation Theory*. Wiley, New York, 1968.
- [32] Provost, F. J., Fawcett, T., *et al.*, “Analysis and Visualization of Classifier Performance: Comparison under Imprecise Class and Cost Distributions,” in *Proceedings of the Third International Conference on Knowledge Discovery and Data Mining*, vol. 97, pp. 43–48, 1997.
- [33] C. Medlock, A. Oppenheim, I. Chuang, and Q. Ding, “Operating characteristics for binary hypothesis testing in quantum systems,” in *2019 57th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, IEEE, pp. 1136–1145, 2019.
- [34] A. Peres, *Quantum theory: concepts and methods*, vol. 57. Springer Science & Business Media, 2006.
- [35] M. A. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*. Cambridge University Press, 2016.
- [36] S. K. Berberian, *Notes on Spectral Theory*. D. Van Nostrand Company, Inc., 1966.
- [37] A. Bodor and M. Koniorczyk, “Receiver Operation Characteristics of Quantum State Discrimination,” *Journal of Russian Laser Research*, vol. 38, no. 2, 2017, pp. 150–163.
- [38] P. G. Casazza, “The Art of Frame Theory,” *Taiwanese Journal of Mathematics*, vol. 4, no. 2, 2000, pp. 129–201.
- [39] P. G. Casazza and G. Kutyniok, *Finite Frames: Theory and Applications*. Springer, 2012.
- [40] P. G. Casazza, G. Kutyniok, and F. Philipp, “Introduction to finite frame theory,” in *Finite frames*, Springer, 2013, pp. 1–53.
- [41] J. Kovacevic and A. Chebira, “Life Beyond Bases: The Advent of Frames (Part I),” *IEEE Signal Processing Magazine*, vol. 24, no. 4, 2007, pp. 86–104.
- [42] J. Kovacevic and A. Chebira, “Life Beyond Bases: The Advent of Frames (Part II),” *IEEE Signal Processing Magazine*, vol. 24, no. 4, 2007, pp. 86–104.
- [43] S. Banerjee and A. Roy, *Linear Algebra and Matrix Analysis for Statistics*. CRC Press, 2014.

- [44] G. Strang, *Introduction to Linear Algebra*. Wellesley-Cambridge Press, 2016.
- [45] P. G. Casazza, M. Fickus, D. G. Mixon, J. Peterson, and I. Smalyanau, “Every Hilbert Space Frame has a Naimark Complement,” *Journal of Mathematical Analysis and Applications*, vol. 406, no. 1, 2013, pp. 111–119.
- [46] M. G. Paris, “The modern tools of quantum mechanics,” *The European Physical Journal Special Topics*, vol. 203, no. 1, 2012, pp. 61–86.
- [47] A. Peres, “Neumark’s theorem and quantum inseparability,” *Foundations of Physics*, vol. 20, no. 12, 1990, pp. 1441–1453.
- [48] V. K. Goyal, M. Vetterli, and N. T. Thao, “Quantized Overcomplete Expansions in \mathbb{R}^N : Analysis, Synthesis, and Algorithms,” *IEEE Transactions on Information Theory*, vol. 44, no. 1, 1998, pp. 16–31.
- [49] P. G. Casazza and J. Kovačević, “Equal-Norm Tight Frames with Erasures,” *Advances in Computational Mathematics*, vol. 18, no. 2-4, 2003, pp. 387–430.
- [50] C. M. Caves, C. A. Fuchs, and R. Schack, “Unknown Quantum States: The Quantum de Finetti Representation,” *Journal of Mathematical Physics*, vol. 43, no. 9, 2002, pp. 4537–4559.
- [51] J. Řeháček, Y. S. Teo, and Z. Hradil, “Determining Which Quantum Measurement Performs Better for State Estimation,” *Physical Review A*, vol. 92, no. 1, 2015, 012108.
- [52] R. B. A. Adamson and A. M. Steinberg, “Improving Quantum State Estimation with Mutually Unbiased Bases,” *Physical Review Letters*, vol. 105, no. 3, 2010, 030406.
- [53] T. Decker, D. Janzing, and T. Beth, “Quantum Circuits for Single-Qubit Measurements Corresponding to Platonic Solids,” *International Journal of Quantum Information*, vol. 2, no. 03, 2004, pp. 353–377.
- [54] W. Słomczyński and A. Szymusiak, “Highly Symmetric POVMs and Their Informational Power,” *Quantum Information Processing*, vol. 15, no. 1, 2016, pp. 565–606.

- [55] S. Brandsen, M. Dall'Arno, and A. Szymusiak, "Communication capacity of mixed quantum t-designs," *Physical Review A*, vol. 94, no. 2, 2016, pp. 022335-1–022335-8.
- [56] C. Medlock, A. Oppenheim, and P. Boufounos, *Informationally overcomplete povms for quantum state estimation and binary detection*, 2020. arXiv: [2012.05355](https://arxiv.org/abs/2012.05355) [quant-ph].
- [57] Q. Ding, C. A. Medlock, and A. V. Oppenheim, "POVM design for quantum state discrimination," *2021 Asilomar Conference on Signals, Systems, and Computing*, forthcoming.
- [58] D. P. Hardin, T. Michaels, and E. B. Saff, "A Comparison of Popular Point Configurations on S^2 ," *arXiv:1607.04590*, 2016.
- [59] E. B. Saff and A. B. Kuijlaars, "Distributing Many Points on a Sphere," *The mathematical intelligencer*, vol. 19, no. 1, 1997, pp. 5–11.
- [60] P. C. Leopardi, "Distributing Points on the Sphere: Partitions, Separation, Quadrature and Energy," Ph.D. dissertation, University of New South Wales, Sydney, Australia, 2007.
- [61] N. J. A. Sloane, *Spherical Codes: Nice Arrangements of Points on a Sphere in Various Dimensions*. [Online]. Available: <http://neilsloane.com/packings/>.