Minimum guesswork discrimination between quantum states

Weien Chen,[1,2,3,*] Yongzhi Cao,[1,2] Hanpin Wang,[1,2] and Yuan Feng[3,†]

[1] *Institute of Software, School of Electronics Engineering and Computer Science, Peking University, China*
[2] *Key Laboratory of High Confidence Software Technologies, Ministry of Education, China*
[3] *Centre for Quantum Computation and Intelligent Systems, University of Technology, Sydney, Australia*

(Dated: October 21, 2014)

Error probability is a popular and well-studied optimization criterion in discriminating non-orthogonal quantum states. It captures the threat from an adversary who can only query the actual state once. However, when the adversary is able to use a brute-force strategy to query the state, discrimination measurement with minimum error probability does not necessarily minimize the number of queries to get the actual state. In light of this, we take Massey's guesswork as the underlying optimization criterion and study the problem of minimum guesswork discrimination.

Quantitative information flow (QIF) analysis has been an active topic in security community during the last decades [1–10]. The aim of QIF analysis is to quantify the amount of sensitive information leaked by a (classical) *covert channel* [1] from a high-level entity Alice, whose secret information (e.g., a password) is mathematically described as a random variable X taking value from $\{x_i : 1 \leq i \leq n\}$ with probability distribution $\{p(x_i)\}$, to a low-level entity Bob, whose partial information about X is described as another random variable Y with alphabet $\{y_j : 1 \leq j \leq m\}$. The correlation between X and Y is determined by the channel matrix $\{p(y_j|x_i)\}$ of the covert channel. We observe that quantum state discrimination [11–27], which is a fundamental problem in quantum information theory, can be seen as a special case of QIF analysis. In the setting of quantum state discrimination, Alice first encodes her secret messages $\{x_i\}$ into quantum states $\{\rho_{x_i}\}$ giving rise to an ensemble of quantum states $\mathcal{E} = \{p(x_i), \rho_{x_i}\}$. We call this $\mathcal{E}$ a *quantum encoding* of X. Alice then prepares a secret message x_i with probability $p(x_i)$ and gives ρ_{x_i} to Bob, who has full knowledge about the ensemble $\mathcal{E}$ and aims to identify the actual value x_i of X realized by Alice. In order to get information about X, Bob performs a *positive operator-valued measure* (POVM) $\Pi = \{\pi_{y_j} : 1 \leq j \leq m\}$ on the quantum state ρ_{x_i} received and stores the measurement outcome in Y. The channel matrix is then given by the Born rule [28], $p(y_j|x_i) = \mathrm{Tr}(\rho_{x_i}\pi_{y_j})$.

In the literature of QIF analysis, researchers have proposed different figures of merit to quantify how successfully Bob can identify the secret value of X given knowledge about Y, according to different adversarial strategies which Bob may adopt. In particular, it is well-known that error probability, guesswork, and the Shannon entropy deal with one-shot strategy, brute-force strategy, and subset membership strategy, respectively, and thus play important and complementary roles in QIF analysis [29–31]. In the quantum setting, it is clear that one-shot strategy and subset membership strategy have been considered. Error probability and the Shannon entropy have been widely studied in quantum information theory, and led a large amount of research on *minimum error discrimination* (MED) [22–26, 32], accessible information [15–17, 33, 34], quantum source coding [13, 35], quantum channel capacity [36–38], etc. However, to the best of our knowledge, no work has addressed brute-force strategy in the context of quantum state discrimination.

The above observation motivates us to consider Massey's guesswork [39, 40] as the optimization criterion in quantum state discrimination. We name the new problem *minimum guesswork discrimination* (MGD). In contrast to the MED scenario where Bob has only one chance to ask Alice "is $X = x$?" for some x chosen based on his measurement outcome, in the MGD scenario

* e-mail:cwe@pku.edu.cn
† e-mail:Yuan.Feng@uts.edu.au

Bob carries out multiple such queries until hitting Alice's prepared message. Guesswork, the new criterion, quantifies the expected number of queries that Bob needs to make. Formally, for two random variables X and Y, the *guesswork* of X given Y is defined by

$$\mathrm{G}(X|Y) \triangleq \sum_{j=1}^{m} p(y_j) \sum_{i=1}^{n} \sigma_j(i) p(x_i|y_j),$$

where each σ_j is a permutation on $\{1, \cdots, n\}$ such that $p(x_i|y_j) \geq p(x_{i'}|y_j)$ implies $\sigma_j(i) \leq \sigma_j(i')$. The guesswork $\mathrm{G}(X|Y)$ quantifies the expected number of queries ("is $X = x$?") that Bob needs to guess the actual value of X after he observes the value of Y. Now we define the optimization goal in MGD. Given $\mathcal{E}$ being a quantum encoding of X, the *minimum guesswork* of $\mathcal{E}$ is given by

$$\mathrm{G}^{opt}(\mathcal{E}) \triangleq \min_{\Pi \in \mathcal{M}} \mathrm{G}(X|Y), \tag{1}$$

where $\mathcal{M}$ is the set of all POVMs. Note that in this definition, Y is completely determined by $\mathcal{E}$ and Π as described in the first paragraph. In the following, we give several alternative characterizations of $\mathrm{G}^{opt}(\mathcal{E})$. The first one states that the optimal POVM achieving $\mathrm{G}^{opt}(\mathcal{E})$ can always be taken as a complete measurement.

Proposition 1. *Let $\mathcal{E}$ be a quantum encoding of a random variable X, and $\mathrm{G}^{opt}(\mathcal{E})$ be defined in Eq.(1). It holds that $\mathrm{G}^{opt}(\mathcal{E}) = \min_{\Pi \in \mathcal{M}_c} \mathrm{G}(X|Y)$, where $\mathcal{M}_c$ is the set of all POVMs consisting of only rank-one measurement operators.*

The second characterization shows that a POVM consisting of $n!$ measurement operators suffices to achieve minimum guesswork when $\mathcal{E}$ comprises n quantum states.

Proposition 2. *Let $\mathcal{E}$ be a quantum encoding of a random variable X, and $\mathrm{G}^{opt}(\mathcal{E})$ be defined in Eq.(1). It holds that $\mathrm{G}^{opt}(\mathcal{E}) = \min_{\Pi \in \mathcal{M}_{n!}} \mathrm{G}(X|Y)$, where $\mathcal{M}_{n!}$ is the set of all POVMs consisting of exactly $n!$ measurement operators.*

Based on Eldar et al.'s analogous results in MED [41], we reduce MGD to a semidefinite programming problem, which has numerical solutions within any desired accuracy in mathematics, and derive necessary and sufficient conditions satisfied by the optimal POVM to achieve minimum guesswork.

Proposition 3. *Let $\mathcal{E}$ be a quantum encoding of a random variable X, and $\mathrm{G}^{opt}(\mathcal{E})$ be defined in Eq.(1). It holds that $\mathrm{G}^{opt}(\mathcal{E}) = \max_A \mathrm{Tr}(A)$, where A ranges over all Hermitian operators satisfying $A \leq \sum_{i=1}^{n} \sigma(i) p(x_i) \rho_{x_i}$ for any permutation σ on $\{1, \cdots, n\}$.*

Proposition 4. *Let $\mathcal{E}$ be a quantum encoding of a random variable X, and $\mathrm{G}^{opt}(\mathcal{E})$ be defined in Eq.(1). A POVM $\{\pi_{y_1}, \pi_{y_2}, \cdots, \pi_{y_{n!}}\}$ achieves $\mathrm{G}^{opt}(\mathcal{E})$ if and only if for any permutation σ on $\{1, \cdots, n\}$ it holds that*

$$\sum_{i=1}^{n} \sum_{j=1}^{n!} \sigma_j(i) p(x_i) \rho_{x_i} \pi_{y_j} \leq \sum_{i=1}^{n} \sigma(i) p(x_i) \rho_{x_i}.$$

It is worth noting that Proposition 4 can also be proved directly using the technique introduced in [42].

To discuss the relationship between MGD and MED, we need to introduce some notations. Given two random variables X and Y, the *error probability* of guessing X given Y is defined by

$$\mathrm{P}_{err}(X|Y) \triangleq 1 - \sum_{j=1}^{m} p(y_j) \max_{1 \leq i \leq n} p(x_i|y_j).$$

The *minimum error probability* of $\mathcal{E}$ used in MED is then given by

$$\mathrm{P}_{err}^{opt}(\mathcal{E}) \triangleq \min_{\Pi \in \mathcal{M}} \mathrm{P}_{err}(X|Y). \tag{2}$$

By the following theorem, we show that minimum guesswork can be bounded from both directions in terms of minimum error probability. Moreover, when discriminating two quantum states, the two criteria coincide.

Theorem 1. *Let $\mathcal{E}$ be a quantum encoding of a random variable X, and $\mathrm{G}^{opt}(\mathcal{E})$ and $\mathrm{P}_{err}^{opt}(\mathcal{E})$ be defined in Eq.(1) and Eq.(2), respectively. It holds that*

$$\frac{1}{2(1-\mathrm{P}_{err}^{opt}(\mathcal{E}))} + \frac{1}{2} \leq \mathrm{G}^{opt}(\mathcal{E}) \leq \frac{n}{2}\mathrm{P}_{err}^{opt}(\mathcal{E}) + 1$$

and if $n = 2$, $\mathrm{G}^{opt}(\mathcal{E}) = \mathrm{P}_{err}^{opt}(\mathcal{E}) + 1$.

We also study the relationship between minimum guesswork and accessible information of a quantum ensemble $\mathcal{E}$. In particular, we derive upper and lower information-theoretic bounds on minimum guesswork. These two bounds are both tight in that they can be achieved by some $\mathcal{E}$.

Theorem 2. *Let $\mathcal{E}$ be a quantum encoding of a random variable X and $\mathrm{G}^{opt}(\mathcal{E})$ be defined in Eq.(1). Provided $\mathrm{H}(X_\pi) \geq 2$ for any measurement operator π, it holds that*

$$\mathrm{G}^{opt}(\mathcal{E}) \geq \frac{1}{4} \cdot 2^{\mathrm{H}(X)-\chi(\mathcal{E})} + 1.$$

In Theorem 2, $\mathrm{H}(X) \triangleq -\sum_{i=1}^{n} p(x_i)\log p(x_i)$ is the Shannon entropy; $\chi(\mathcal{E}) \triangleq \mathrm{S}(\sum_{i=1}^{n} p(x_i)\rho_{x_i}) - \sum_{i=1}^{n} p(x_i)\mathrm{S}(\rho_{x_i})$ is the well-known Holevo bound on accessible information of $\mathcal{E}$ [33], where $\mathrm{S}(\rho) \triangleq -\mathrm{Tr}(\rho\log\rho)$ is the von Neumann entropy of ρ; the random variable X_π is defined by $\Pr(X_\pi = x_i) \triangleq p(x_i)\mathrm{Tr}(\rho_{x_i}\pi)/\mathrm{Tr}(\rho\pi)$ with $\rho = \sum_{i=1}^{n} p(x_i)\rho_{x_i}$.

Theorem 3. *Let $\mathcal{E}$ be a quantum encoding of a random variable X and $\mathrm{G}^{opt}(\mathcal{E})$ be defined in Eq.(1). It holds that*

$$\mathrm{G}^{opt}(\mathcal{E}) \leq \frac{n-1}{2\log n}(\mathrm{H}(X) - \Lambda(\mathcal{E})) + 1.$$

In Theorem 3, $\Lambda(\mathcal{E}) \triangleq \mathrm{Q}(\sum_{i=1}^{n} p(x_i)\rho_{x_i}) - \sum_{i=1}^{n} p(x_i)\mathrm{Q}(\rho_{x_i})$ is a lower bound on accessible information of $\mathcal{E}$ [34], where $\mathrm{Q}(\rho) \triangleq -\sum_k \prod_{l\neq k} \frac{\lambda_k}{\lambda_k - \lambda_l}\lambda_k \log\lambda_k$ and λ_k's are eigenvalues of ρ. In [34], $\mathrm{Q}(\rho)$ is called the subentropy of ρ .

Furthermore, we investigate the max-min problem $\max_{\mathcal{E}} \mathrm{G}^{opt}(\mathcal{E})$ and provide sufficient and necessary conditions on the quantum encoding $\mathcal{E}$ when making no measurement at all would be the optimal strategy for Bob.

Theorem 4. *Let X be a random variable and $\mathcal{E} = \{p(x_i), \rho_{x_i} : 1 \leq i \leq n\}$ a quantum encoding of X. Let $\mathrm{G}^{opt}(\mathcal{E})$ be defined in Eq.(1), and $\mathrm{G}(X) \triangleq \sum_{i=1}^{n} \sigma(i)p(x_i)$ such that $p(x_i) \geq p(x_j)$ implies $\sigma(i) \leq \sigma(j)$. Then $\mathrm{G}^{opt}(\mathcal{E}) = \mathrm{G}(X)$ holds if and only if for any $1 \leq i, j \leq n$ the following condition holds:*

$$p(x_i) \geq p(x_j) \Rightarrow p(x_i)\rho_{x_i} \geq p(x_j)\rho_{x_j}.$$

Consequently, it holds that $\max_{\mathcal{E}} \mathrm{G}^{opt}(\mathcal{E}) = \mathrm{G}(X)$ for any random variable X.

A direct corollary of Theorem 4 is that, for a uniformly distributed variable X, a quantum encoding $\mathcal{E}$ achieving $\mathrm{G}^{opt}(\mathcal{E}) = \mathrm{G}(X)$ must be formed by identical states.

The full version of this work is available online: arXiv:1410.5180.

---

[1] Jonathan K Millen. Covert channel capacity. In *Proceedings of the IEEE Symposium on Security and Privacy*, pages 60–60. IEEE Computer Society, 1987.

[2] John McLean. Security models and information flow. In *Proceedings of the IEEE Symposium on Security and Privacy*, pages 180–187. IEEE Computer Society, 1990.

[3] James W Gray III. Toward a mathematical foundation for information flow security. *Journal of Computer Security*, 1(3):255–294, 1992.

[4] Gavin Lowe. Quantifying information flow. In *Proceedings of the IEEE Computer Security Foundations Workshop*, pages 18–18. IEEE Computer Society, 2002.

[5] Boris Köpf and David Basin. An information-theoretic model for adaptive side-channel attacks. In *Proceedings of the 14th ACM conference on Computer and communications security*, pages 286–296. ACM, 2007.

[6] Konstantinos Chatzikokolakis, Catuscia Palamidessi, and Prakash Panangaden. On the bayes risk in information-hiding protocols. *Journal of Computer Security*, 16(5):531–571, 2008.

[7] Geoffrey Smith. On the foundations of quantitative information flow. In *Foundations of Software Science and Computational Structures*, pages 288–302. Springer, 2009.

[8] Geoffrey Smith. Quantifying information flow using min-entropy. In *Eighth International Conference on Quantitative Evaluation of Systems (QEST)*, pages 159–167. IEEE, 2011.

[9] Mário S Alvim, Konstantinos Chatzikokolakis, Catuscia Palamidessi, and Geoffrey Smith. Measuring information leakage using generalized gain functions. In *IEEE Computer Security Foundations Symposium (CSF)*, pages 265–279. IEEE, 2012.

[10] Mário S Alvim, Konstantinos Chatzikokolakis, Annabelle McIver, Carroll Morgan, Catuscia Palamidessi, Geoffrey Smith, et al. Additive and multiplicative notions of leakage, and their capacities. In *IEEE Computer Security Foundations Symposium (CSF)*, 2014.

[11] Carl Wilhelm Helstrom. *Quantum detection and estimation theory*. Academic press, 1976.

[12] Edward Davies. Information and quantum measurement. *IEEE Trans. Inf. Theory*, 24(5):596–599, 1978.

[13] Benjamin Schumacher. Quantum coding. *Phys. Rev. A*, 51(4):2738, 1995.

[14] Christopher A Fuchs and Asher Peres. Quantum-state disturbance versus information gain: Uncertainty relations for quantum information. *Phys. Rev. A*, 53(4):2038, 1996.

[15] Masashi Ban, Kouichi Yamazaki, and Osamu Hirota. Accessible information in combined and sequential quantum measurements on a binary-state signal. *Phys. Rev. A*, 55:22–26, Jan 1997.

[16] Masao Osaki, Osamu Hirota, and Masashi Ban. The maximum mutual information without coding for binary quantum-state signals. *J. Mod. Opt.*, 45(2):269–282, 1998.

[17] Masahide Sasaki, Stephen M Barnett, Richard Jozsa, Masao Osaki, and Osamu Hirota. Accessible information and optimal strategies for real symmetrical quantum sources. *Phys. Rev. A*, 59(5):3325, 1999.

[18] Igor D Ivanovic. How to differentiate between non-orthogonal states. *Phys. Lett. A*, 123(6):257–259, 1987.

[19] Dennis Dieks. Overlap and distinguishability of quantum states. *Phys. Lett. A*, 126(5):303–306, 1988.

[20] Asher Peres. How to differentiate between non-orthogonal states. *Phys. Lett. A*, 128(1):19, 1988.

[21] Yonina C Eldar and G David Forney Jr. On quantum detection and the square-root measurement. *IEEE Trans. Inf. Theory*, 47(3):858–872, 2001.

[22] Alexander S Holevo. Statistical decision theory for quantum systems. *J. Multivariate Anal.*, 3(4):337–394, 1973.

[23] Horace P Yuen, Robert S Kennedy, and Melvin Lax. Optimum testing of multiple hypotheses in quantum detection theory. *IEEE Trans. Inf. Theory*, 21(2):125–134, 1975.

[24] Masashi Ban, Keiko Kurokawa, Rei Momose, and Osamu Hirota. Optimum measurements for discrimination among symmetric quantum states and parameter estimation. *Int. J. Theor. Phys.*, 36(6):1269–1288, 1997.

[25] Stephen M Barnett. Minimum-error discrimination between multiply symmetric states. *Phys. Rev. A*, 64(3):030303, 2001.

[26] Yonina C Eldar, Alexandre Megretski, and George C Verghese. Optimal detection of symmetric mixed quantum states. *IEEE Trans. Inf. Theory*, 50(6):1198–1207, 2004.

[27] Sarah Croke, Erika Andersson, Stephen M Barnett, Claire R Gilson, and John Jeffers. Maximum confidence quantum measurements. *Phys. Rev. Lett.*, 96(7):070401, 2006.

[28] Andrew M Gleason. Measures on the closed subspaces of a hilbert space. *Journal of mathematics and mechanics*, 6(6):885–893, 1957.

[29] Christian Cachin. *Entropy measures and unconditional security in cryptography.* PhD thesis, Swiss Federal Institute of Technology Zurich, 1997.

[30] Thomas M Cover and Joy A Thomas. *Elements of information theory 2nd edition.* Wiley-interscience, 2006.

[31] Mário S Alvim, Miguel E Andrés, Catuscia Palamidessi, et al. Probabilistic information flow. In *Proceedings of the IEEE Symposium on Logic in Computer Science*, pages 314–321, 2010.

[32] Joonwoo Bae and Won-Young Hwang. Minimum-error discrimination of qubit states: Methods, solutions, and properties. *Phys. Rev. A*, 87(1):012334, 2013.

[33] Alexander S Holevo. Statistical problems in quantum physics. In *Proceedings of the Second Japan-USSR Symposium on Probability Theory*, pages 104–119. Springer, 1973.

[34] Richard Jozsa, Daniel Robb, and William K Wootters. Lower bound for accessible information in quantum mechanics. *Phys. Rev. A*, 49(2):668, 1994.

[35] Richard Jozsa and Benjamin Schumacher. A new proof of the quantum noiseless coding theorem. *J. Mod. Opt.*, 41(12):2343–2349, 1994.

[36] Paul Hausladen, Richard Jozsa, Benjamin Schumacher, Michael Westmoreland, and William K Wootters. Classical information capacity of a quantum channel. *Phys. Rev. A*, 54(3):1869, 1996.

[37] AS Holevo. The capacity of the quantum channel with general signal states. *IEEE Trans. Inf. Theory*, 44(1):269–273, 1998.

[38] Benjamin Schumacher and Michael D Westmoreland. Sending classical information via noisy quantum channels. *Phys. Rev. A*, 56(1):131, 1997.

[39] James L Massey. Guessing and entropy. In *Proceedings of the IEEE International Symposium on Information Theory*, page 204, 1994.

[40] E. Arikan. An inequality on guessing and its application to sequential decoding. *IEEE Trans. Inf. Theory*, 42(1):99–105, Jan 1996.

[41] Yonina C Eldar, Alexandre Megretski, and George C Verghese. Designing optimal quantum detectors via semidefinite programming. *IEEE Trans. Inf. Theory*, 49(4):1007–1012, 2003.

[42] SM Barnett and S Croke. On the conditions for discrimination between quantum states with minimum error. *J. Phys. A*, 42(6):1–4, 2009.