UNIVERSITY OF CALIFORNIA
RIVERSIDE

On The Asymptotics Of Some Low-Delay Transmission Scenarios

A Dissertation submitted in partial satisfaction
of the requirements for the degree of

Doctor of Philosophy

in

Electrical Engineering

by

Ceren Sevinç

March 2022

Dissertation Committee:

Professor Ertem Tuncel, Chairperson
Professor Ilya Dumer
Professor Başak Güler

The Dissertation of Ceren Sevinç is approved:

Committee Chairperson

University of California, Riverside

Acknowledgments

First and foremost, I would like to thank my advisor Prof. Ertem Tuncel wholeheartedly for his generous guidance and continuous support throughout this journey. Prof. Tuncel was a role model not only in his academic excellence, but also in his professionalism and above all his generosity and kindness. There are no words to express how fortunate I have felt to have a supportive advisor like him. I hope to carry his legacy with me as I go through the next chapter in life. I am also grateful for all the opportunities he provided me, from the chance to attend several conferences to funding me throughout my Ph.D. I had the honor of becoming well acquainted with Prof. Tuncel and his family, an acquaintance that I will cherish for a very long time.

I would like to express my sincere gratitude to my Ph.D. committee members Prof. Ilya Dumer and Prof. Başak Güler for taking time to serve in the committee. I also thank Prof. Yingbo Hua, Prof. Samet Oymak and Prof. Jiasi Chen for serving on my Qualifying exam committee and for their helpful feedback.

I would like to acknowledge Prof. Deniz Gündüz and my colleagues from my internship at the Information Processing lab at the Imperial College in London. I enjoyed working with the group and learned a lot from them.

My deepest gratitude goes to my parents for their love and support every step of the way. Although they are thousands of miles away, I feel their love and support every day. Finally, I would like to thank UC Riverside not only for the academic journey, but also for introducing me to my partner in life, Joe.

The content of this dissertation is a reprint of the materials in the following publications:

1. **C. Sevinç** and E. Tuncel. (2018). On asymptotic analysis of energy-distortion tradeoff for low-delay transmission over Gaussian channels. *IEEE International Symposium on Information Theory (ISIT)*, June 2018, pp 2599–2603.

2. **C. Sevinç** and E. Tuncel. (2018). On energy-distortion exponents for low-delay Gaussian broadcasting. *IEEE International Symposium on Information Theory (ISIT)*, June 2018, pp 2604–2608.

3. **C. Sevinç** and E. Tuncel. (2019). On the analysis of energy-distortion tradeoff for zero-delay transmission over Gaussian broadcast channels. *IEEE International Symposium on Information Theory (ISIT)*, July 2019, pp 2758–2762.

4. **C. Sevinç** and E. Tuncel. (2021). On asymptotic analysis of energy-distortion tradeoff for low-delay transmission over Gaussian broadcast channels. *IEEE Transactions on Communications*, vol. 69, no. 7, July 2021, pp 4448–4460.

5. **C. Sevinç** and E. Tuncel. (2021). Information theoretic approach on randomized response models in surveys. *IEEE International Symposium on Information Theory (ISIT)*, 2021, pp. 3338-3342.

6. **C. Sevinç** and E. Tuncel. (2022). A privacy-preserving voting and survey scheme by using information theoretic approach *IEEE International Symposium on Information Theory (ISIT)*, *submitted.*

7. **C. Sevinç** and E. Tuncel. (2022). A privacy-preserving voting and survey scheme by using information theoretic approach *IEEE Transactions on Information Theory, to be submitted.*

To my beloved parents, Joe, and Boğaziçi University family who is standing for academic freedom.

ABSTRACT OF THE DISSERTATION

On The Asymptotics Of Some Low-Delay Transmission Scenarios

by

Ceren Sevinç

Doctor of Philosophy, Graduate Program in Electrical Engineering
University of California, Riverside, March 2022
Professor Ertem Tuncel, Chairperson

The first part of the thesis focuses on asymptotic energy-distortion performance of zero- and low-delay transmission of Gaussian sources over energy-limited Gaussian channels. A lower bound for the leading term in the negative logarithm of the distortion, termed the *energy-distortion exponent*, is derived through an achievable scheme based on high-resolution quantization coupled with orthogonal signaling. The higher-order term in the negative logarithm of the distortion, termed the *energy-distortion dispersion*, is optimized while keeping the leading term, the energy-distortion exponent, at its optimal (respectively, the best known) value for the zero-delay (respectively, low-delay) regime. In contrast with the decaying dispersion previously reported in the literature, the proposed coding scheme achieves a constant dispersion. When the scheme is optimized, this constant can be improved with respect to its naïve value, i.e., that achieved by optimizing purely the source coding performance instead of the end-to-end distortion. Lastly, a tradeoff of achievable energy-distortion exponents is derived for broadcast scenarios by extending the point-to-point scheme to include a successive refinement source coder coupled with two rounds of orthogonal signaling.

The second part examines the idea of randomized response together with the method of types and large deviations techniques to analyze the accuracy of potential electronic privacy-preserving voting and survey schemes. Previous work by Tuncel [1] proposed a voting scheme in which votes are randomly changed by the system before being transmitted with a chosen flipping probability to preserve the privacy of the voters. The vulnerable interval in [1], where the voting results are very close to 50%–50%, is tackled by introducing a third possible outcome referred to as "too close to call". This third outcome is used as a feedback to adjust the flipping probability so that small upper bounds on the probability of wrongly calling the election could be given. A natural tradeoff arises between the probability of wrongly calling the election and the probability of a too-close-to-call outcome.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Classical information theoretic approaches for source and channel coding depend on mapping large blocks of source samples to large blocks of channel symbols under average power and bandwidth constraints. Such approaches may become irrelevant in some cases, particularly in emerging internet of things (IoT) technologies where (i) the measured phenomenon is almost always very slowly varying, thus inducing an extremely low sampling rate and a very delay-intolerant regime, (ii) there is ample time to communicate the measurement, thereby resulting in a very high *relative* channel bandwidth, and (iii) a small average power consumption per channel symbol translates into huge energy consumption per source sample due to the high relative bandwidth. Subsequently, new communication limits must be explored for the case where *very few source samples* M (as few as $M = 1$) are mapped to *very large blocks of channel symbols* N under energy constraints, instead of power constraints. This would constitute a zero-delay and low-delay framework in the sense of source delay, i.e., transmission without waiting for new source samples to occur, or transmission after combining only a few source samples, respectively.

Energy-distortion tradeoff was introduced in [3] in order to characterize the minimum average reconstruction distortion that can be achieved under a total energy constraint (per source sample) without any restriction on the channel bandwidth. Authors in [4] proposed the concept of energy-distortion exponent as a prominent performance metric defined as

$$\Theta = \lim_{\gamma \to \infty} -\frac{1}{\gamma} \ln D(\gamma)\,,$$

where γ denotes the signal energy-to-noise ratio (ENR), and $D(\gamma)$ is the minimum mean square-error (MSE). They then showed that for Gaussian sources and channels, the exponential energy-distortion behavior of Shannon-theoretic M-to-N mappings (where both M and N are allowed to be arbitrarily large) can be replicated in the 1-to-infinity mapping regime so long as catastrophic *outage* events are allowed with vanishingly small probability, and the MSE distortion is measured conditioned on non-outage. In [5], the same scenario was undertaken with respect to the *overall* distortion for any M-to-infinity regime. It was shown that achievable exponents coincide with those in the Shannon-theoretic setting when $M \to \infty$, making the proposed scheme exponent-optimal asymptotically in M.

In [6], an achievable tradeoff of exponents for the overall distortion was derived for broadcast channels for any M. The energy-distortion problem for Gaussian broadcasting was later studied in [7], [8] under the constraint of a private message sent to the better receiver with a given rate. Energy-distortion tradeoff for the transmission of a pair of correlated Gaussian sources over a two-user Gaussian broadcast channel with noiseless and causal channel output feedback was explored in [9].

Later, we investigate the more detailed characterization of broadcast channels for zero-delay scenario as in the point-to-point case in [5], which takes the higher order term *energy-distortion dispersion*, i.e. $\Upsilon_1(\gamma)$, into consideration in the analysis of the energy-distortion tradeoff with 1-to-infinity source-channel mapping, $D_1(\gamma)$, in the form of

$$-\ln D_1(\gamma) = \Theta_1 \cdot \gamma + \Upsilon_1(\gamma) + o(1)\,, \tag{1.1}$$

for large γ, where $\Upsilon_1(\gamma)$ is sub-linear in γ, i.e., $\lim_{\gamma\to\infty} \Upsilon_1(\gamma)/\gamma = 0$. We also suggest a convenient approach by optimizing the variance of the Gaussian point-density function to be able to extend the energy-distortion dispersion analysis to Gaussian broadcast channels.

The second part of the dissertation explores a different application of a low-delay communication in which we analyze an electronic privacy-preserving voting and survey schemes by using a locally differential private mechanism of randomized response and assess the performance bounds by utilizing the method of types and large deviation techniques.

In the age of internet and big data, the need for data privacy is becoming increasingly recognized. There is growing interest in the question: How do we protect the privacy of a user while we perform an informative analysis on a dataset using statistics and/or machine learning? In this regard, differential privacy [10] has gained popular attention in the past decade, and is often regarded as the gold standard for data privacy of users in data analysis. The further mathematical discussion of the differential privacy is provided in [11]. The main idea behind differential privacy is to inject some random noise to a user input to give the user plausible deniability. This is typically done in one of two ways: in a (i) centralized or (ii) local framework, which are shown in Figure 1.1.

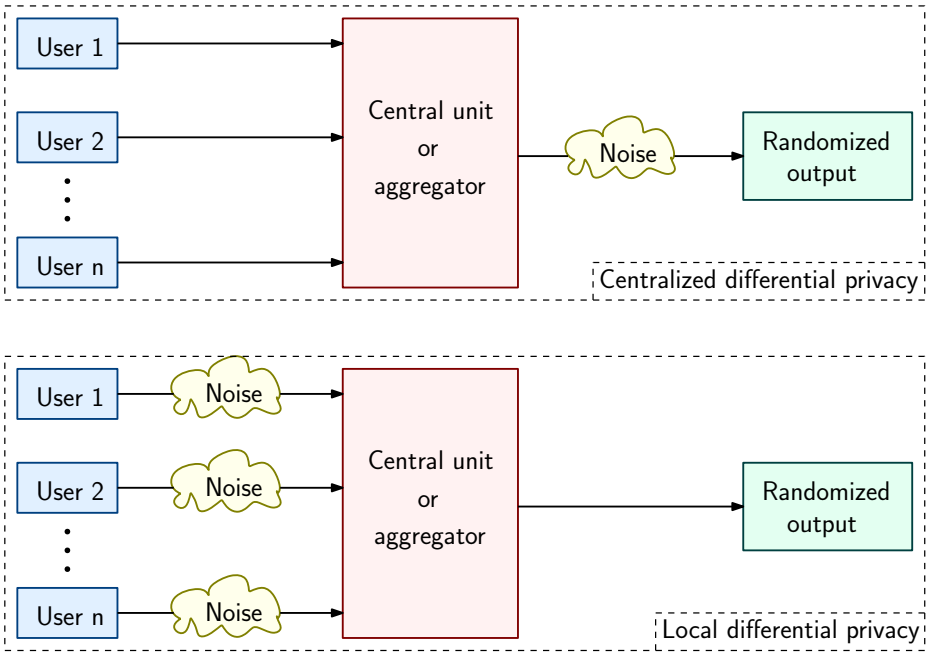

Figure 1.1: Two approaches of differential privacy: (a) centralized (b) local.

In the case of centralized differential privacy, the real data is sent to a central unit, known as the aggregator. The aggregator transforms the data with a differentially private mechanism to produce anonymized output. This approach has been also applied on data mining [12], deep learning [13]. Recently, The U.S. Census Bureau has also started research on differential privacy as part of modernization of disclosure avoidance, and another prominent work can be found in [14]. In this model, users must trust the aggregator for keeping protection of their sensitive data. However, the central unit is often prone to adversarial attacks which compromise user privacy. Similarly, the central unit might not be trusted in certain cases, such as untrustworthy operators or authoritarian governments. Moreover, the requirement of processing the whole data and adding noise to the dataset at once to increase accuracy induces system delay.

An alternative to central differential privacy is local differential privacy (LDP), in which noise is locally added on each data before being transmitted to the central unit. Although this approach has recently gained attraction in the technology industry, i.e., RAPPOR from Google [15], Apple iOS [16], Microsoft [17], its origins can be traced back to 1965, in which Warner introduced the randomized response model in [18] to protect the privacy of respondents in a survey. When respondents are asked questions on sensitive topics, they may refuse to answer or may give an untruthful response as a result of concerns over their privacy, thereby biasing the survey. To eliminate this bias, Warner suggests that respondents are asked to react to either one of the mirrored sentences, i.e., "I belong to attribute A" and " I do not belong to A" with a YES or NO, depending on the outcome of a randomization device, such as an unfair coin toss or a spinner without revealing their pick to the interviewer. Later, this approach was extended to multiple sensitive attributes in [19], [20]. For more applications of LDP, we refer the reader to [21–25], and the references therein.

1.1 Outline

Chapter 2 is dedicated to preliminaries and notation for point-to-point transmission over additive white Gaussian noise (AWGN) channel and Gaussian broadcast channel. Moreover, tools of high resolution quantization are introduced.

Chapter 3 provides the derivation of achievable energy-distortion exponents for general M and the details of an achievable energy-distortion dispersion analysis for $M = 1$ and $M = 2$ in point-to-point AWGN channels. Furthermore, we utilize Monte Carlo simulations to validate the high resolution distortion assumptions.

In Chapter 4, an achievable tradeoff of energy-distortion exponents for broadcast channels are derived, for which a simple parametric computation algorithm is also discussed.

In Chapter 5, we move on to a different application, i.e., privacy-preserving voting mechanism, which was introduced in [1]. We present preliminaries, problem definition, and the relationship between number of voters, the allowed probability of incorrectly calling the election, and the level of privacy (i.e., amount of randomization). a case study of The 2020 US Presidential Election for the given voting mechanism.

Chapter 6 focuses on resolving the drawback of mechanism in [1], which has a vulnerable interval when the voting results are very close to 50%–50%, by introducing a third possible outcome referred to as "too close to call". The tradeoff between the probability of wrongly calling the election and the probability of a too-close-to-call outcome is investigated.

In Chapter 7, we extend privacy-preserving voting mechanism to surveys, which require YES/NO responses to increase cooperation and privacy that can help reduce bias by taking an information theoretic approach on the randomized response models.

Some of the proofs are deferred to Appendix A.

Part I

On Asymptotic Analysis of Energy-Distortion Tradeoff for Low-Delay Transmission over Gaussian Channels

Chapter 2

Preliminaries

2.1 Introduction

A voluminous amount of data (several exabytes) is generated each day, and waiting to be processed by big data algorithms. Along with smart phones, one of the highest contributors to the explosion of the volume of data is the Internet of Things (IoT), which refers to a network of everyday objects such as wearables, appliances (e.g., smart refrigerators, thermostats, doorbells), and many others, that can take measurements through the use of embedded sensors and actuators, and can transmit the information collected about the objects (or people) to nearby devices, such as phones, tablets, laptops, etc.

Especially prevalent in the IoT framework are the communication scenarios where the data sampling rate is very small due to the slowly varying nature of the measured phenomenon. For example, for a diabetes patient monitoring their glucose level, it suffices to take a reading once every 5 minutes. Similarly, an Apple Watch measures the resting heart rate every 5 minutes, although during workouts it may go up to once every few seconds.

Another example is temperature control through a smart thermostat, whereby the room temperature is measured once every minute. Finally, smart meters take measurements every 15 minutes, although it is conceivable that they will eventually be capable of transmitting readings every minute.

Classical information theoretic approaches for source-channel coding rely on mapping large blocks of source samples to large blocks of channel symbols while satisfying average power and bandwidth constraints. Such approaches are inapplicable in the aforementioned scenarios, as the extremely low sampling rate imposes large communication delays if block coding is used. But at the same time, the low sampling rate creates ample time between samples to communicate the measurements, thereby resulting in a very high *relative* channel bandwidth. That, in turn, implies that it is the total energy consumption per source symbol that should be constrained, as opposed to the power consumption per channel symbol, as even small quantities of the latter translates into a huge quantities of the former in this setting. To sum up, new communication limits must be explored for the case where *very few source samples* M (as few as $M = 1$) are mapped to *very large blocks of channel symbols* N (idealized as $N \to \infty$) under energy and distortion constraints.

This would constitute a "low-delay" framework in two senses. First, for low values of M (respectively $M = 1$), there will be low (respectively zero) *source* delay, i.e., the encoding/decoding process will not have to wait for more than M source samples to occur. But more importantly, if the channel bandwidth is high enough, $M = 1$ also corresponds to actual low communication delay, because large amounts of channel symbols can be transmitted in a very short period of time after the source sample occurs. For example,

Bluetooth communication channels have 1MHz of bandwidth, which would ideally allow for as many as $N = 500,000$ channel symbols to be sent in one second. Contrasting with minutes between source samples, the communication delay will therefore be in the order of seconds (or fractions thereof) in practice.

A Shannon-theoretic analysis of the energy-distortion tradeoff for Gaussian sources and channels was provided in [3], where M and N were both allowed to increase without bound. It was shown that

$$D = e^{-\gamma} \tag{2.1}$$

where γ denotes the signal energy-to-noise ratio (ENR) per source symbol. In [4], it was shown that the same exponential energy-distortion behavior as in (2.1) can actually be obtained in a 1-to-N mapping regime in which *outage* events (i.e., catastrophic reconstruction) are allowed with vanishingly small probability, and the MSE distortion is measured conditioned on non-outage.

In this work, instead of conditioning on the occasional outage event only, we analyze the *end-to-end* MSE achieved by mapping M source samples to infinitely-long channel words. Defining $D_M(\gamma)$ as the energy-distortion tradeoff, i.e., the minimum MSE achievable under the ENR γ using an M-to-infinity source-channel mapping, we analyze

$$-\ln D_M(\gamma) = \Theta_M \, \gamma + \Upsilon_M(\gamma) + o(1)\,, \tag{2.2}$$

for large γ, where $\Upsilon_M(\gamma)$ is sub-linear in γ, i.e.,

$$\lim_{\gamma\to\infty} \frac{\Upsilon_M(\gamma)}{\gamma} = 0 \,.$$

Here, Θ_M is the coefficient of the dominant term, termed the *energy-distortion exponent*. Seeing a parallel between (2.2) and recent results in finite blocklength source and channel coding, whereby higher-order terms of the coding rate as a function of the blocklength is investigated [26, 27], we define the higher order term $\Upsilon_M(\gamma)$ as the *energy-distortion dispersion*.

We do not limit our attention to only $M = 1$, because for the cases where some delay is tolerable, a few source samples can be combined and coded at once to utilize the advantage of vector coding. For instance, a heart rate data that is collected every 5 seconds during a workout session can recorded by a smart phone with as much as 15 seconds of delay, so a smart watch can combine up to three readings before transmitting them.

For $M = 1$, Burnashev [28] arrived at the conclusion that

$$-\ln D_1(\gamma) \leq \frac{1}{6}\gamma + C\ln(1+\gamma) - \ln C \,,$$

for some constant C and large enough γ.[1] This implies $\Theta_1 \leq \frac{1}{6}$ as an upper bound to the maximum energy-distortion exponent. In fact, Θ_1 is exactly equal to $\frac{1}{6}$ as implied in [2,30,31], and [29, Chapter 8], which showed $\Theta_1 \geq \frac{1}{6}$ through achievable schemes. Therefore,

[1] While Burnashev's result was for uniform sources, it was noted in the same work [28] that the result can be extended to any well-behaving source.

Burnashev's result also implies

$$\Upsilon_1(\gamma) \leq C \ln(1+\gamma) - \ln C \ .$$

To the best of our knowledge, the only known achievable energy-distortion dispersion was implicitly provided in [2] and can be shown after some algebra that

$$\Upsilon_1(\gamma) \geq -\ln \frac{5\gamma}{3} \ . \tag{2.3}$$

In this work, we show through an achievable scheme that the energy-distortion exponent for any $M > 1$ can be lower bounded as

$$\Theta_M \geq \frac{M}{(\sqrt{M}+\sqrt{2})^2} \ . \tag{2.4}$$

As can be seen, the right hand side of (2.4) is a monotonically increasing sequence converging to 1, so this achievable scheme is optimal when $M \to \infty$, as a higher exponent cannot be achieved due to (2.1). Analyzing the dispersion achieved by the proposed scheme, we also obtain

$$\Upsilon_1(\gamma) \geq -1.7006 \ ,$$

which is an improvement compared to (2.3), as the latter becomes a trivial lower bound when $\gamma \to \infty$.

We then turn to the Gaussian broadcast scenario, where the same device is transmitting its readings to multiple control units in a degraded fashion. As usual, different

receivers might represent either separate physical IoT devices, or the same device suffering from different possible levels of communication noise. Energy-distortion exponents in the broadcast setting was first discussed in [4], where the asymptotic ($M \to \infty$) exponent tradeoff at the two receivers was derived using the achievability and converse results of [32]. It was then shown that if vanishingly unlikely outage events are allowed, the same exponents in [4] can be achieved using 1-to-N coding schemes, thereby generalizing the results for point-to-point coding in the same work. As in the same spirit in point-to-point coding, we explore the *end-to-end* MSE achieved by mapping M source samples to infinitely-long channel words. Specifically, we derive an achievable energy-distortion exponent tradeoff for arbitrary M and show that the tradeoff region expands as M increases and eventually converges to the tradeoff in [4] as $M \to \infty$. Our results for the point-to-point and broadcast scenarios have appeared in a preliminary form in [5] and [6], [33], respectively. The extended studies are presented with supporting proofs in a coherent flow, and validity of the high resolution distortion formulas are tested and justified via Monte Carlo simulations in [34].

2.2 Preliminaries

2.2.1 Point-to-point Transmission

Let $\mathbf{X}$ be a real-valued M-dimensional source to be transmitted over the AWGN channel $\mathbf{V} = \mathbf{U} + \mathbf{W}$, where $\mathbf{U}$ and $\mathbf{V}$ are N-dimensional channel input and output vectors, respectively. The channel noise $\mathbf{W}$ is independent of $\mathbf{U}$, and $\mathbf{W} \sim \mathcal{N}(\mathbf{0}, \sigma_W^2 \mathbf{I})$, where σ_W^2 is the noise variance. The encoder $\phi_{M,N} : \mathbb{R}^M \to \mathbb{R}^N$ maps $\mathbf{X}$ into $\mathbf{U}$, and the decoder $\psi_{M,N} : \mathbb{R}^N \to \mathbb{R}^M$ estimates $\mathbf{X}$ from $\mathbf{V}$ as $\hat{\mathbf{X}}$.

Definition 1 *An energy-distortion pair* (D, E) *is achievable if for any* $\epsilon > 0$*, there exist large enough* M, N *and* $(\phi_{M,N}, \psi_{M,N})$ *such that*

$$\frac{1}{M}\mathbb{E}\left[||\mathbf{U}||^2\right] \leq E + \epsilon$$
$$\frac{1}{M}\mathbb{E}\left[||\mathbf{X} - \hat{\mathbf{X}}||^2\right] \leq D(1+\epsilon)\ .$$

We also fix M as a finite number and let only N grow without bound, and accordingly make the following M-achievability definition.

Definition 2 *An energy-distortion pair* (D, E) *is* M*-achievable if for any* $\epsilon > 0$*, there exist large enough* N *and* $(\phi_{M,N}, \psi_{M,N})$ *such that*

$$\frac{1}{M}\mathbb{E}\left[||\mathbf{U}||^2\right] \leq E + \epsilon$$
$$\frac{1}{M}\mathbb{E}\left[||\mathbf{X} - \hat{\mathbf{X}}||^2\right] \leq D(1+\epsilon)\ .$$

We refer to $\gamma = \frac{E}{\sigma_W^2}$ as the *energy-to-noise ratio* (ENR) per source symbol, and define achievability and M-achievability of a pair (D, γ) similarly. We also define $D(\gamma)$ (respectively $D_M(\gamma)$) as the minimum achievable (respectively M-achievable) D for a given γ. Note that $D(\gamma) = D_\infty(\gamma) \stackrel{\Delta}{=} \lim_{M\to\infty} D_M(\gamma)$.

As was mentioned in the introduction, characterization of $D(\gamma)$ is a solved problem, because it was shown in [3] that

$$D(\gamma) = e^{-\gamma} \tag{2.5}$$

On the other hand, much less is known about $D_M(\gamma)$.

In our pursuit of characterizing M-achievable (D, γ) pairs, we utilize a scheme whereby $\mathbf{X}$ is quantized using a vector quantization with $N \gg 1$ regions, and use orthogonal signaling to transmit the quantization index in N channel uses. That is, the quantized indices are mapped into orthogonal channel input vectors such that

$$\mathbf{U} = \sqrt{ME}\, \mathbf{e}_{k(\mathbf{X})}$$

where $1 \leq k(\mathbf{X}) \leq N$ is the vector quantization index, and $\mathbf{e}_k$ is the kth unit vector in $\mathbb{R}^N$. Note that the energy expended per source symbol is always equal to E.

At the receiver, we use maximum likelihood (ML) decoding given as

$$\hat{K} = \underset{1 \leq k \leq N}{\arg\max}\ \Pr[\mathbf{V} | k(\mathbf{X}) = k] \ .$$

Because the noise $\mathbf{W}$ is i.i.d. Gaussian, this boils down to a nearest-neighbor decoder, i.e.,

$$\hat{K} = \underset{1 \leq k \leq N}{\arg\min}\ ||\mathbf{V} - \sqrt{ME}\mathbf{e}_k||^2 \ ,$$

which, in turn, is the same as

$$\hat{K} = \underset{1 \leq k \leq N}{\arg\max}\ \mathbf{V}^T \mathbf{e}_k = \underset{1 \leq t \leq N}{\arg\max}\ V_t \ .$$

The receiver then outputs

$$\hat{\mathbf{X}} = \mathbf{r}_{\hat{K}}$$

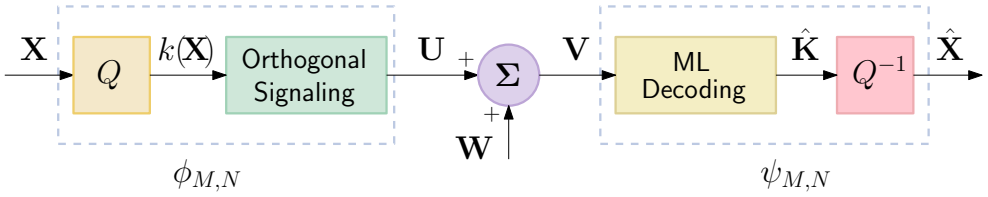

Figure 2.1: Block diagram of the proposed coding scheme for an M-dimensional source. Q and Q^{-1} refer to quantization and reconstruction of the source, respectively.

where $\mathbf{r}_k$ is the kth reconstruction level of the M-dimensional quantizer. This proposed coding scheme is illustrated as a block diagram in Figure 2.1.

We denote by $\mathcal{O}$ the outage event, i.e., occasional decoding errors:

$$\mathcal{O} = \left\{ k(\mathbf{X}) \neq \hat{K} \right\}. \tag{2.6}$$

While ML decoding is not optimal, it simplifies the analysis and makes it tractable. More specifically, i) the outage event $\mathcal{O}$ becomes independent of $\mathbf{X}$, which will be convenient in the sequel, and ii) incorrect decoding induces a uniform distribution over each of the $N-1$ incorrect quantization regions in $\mathbb{R}^M$. To see the latter, observe that

$$\underset{1\leq t\leq N,\, t\neq k(\mathbf{X})}{\arg\max} \; V_t = \underset{1\leq t\leq N,\, t\neq k(\mathbf{X})}{\arg\max} \; W_t$$

and that W_t is an i.i.d. sequence.

Before we close this section, it is worth mentioning that other approaches in the literature, most notably the work by Zeger and Manzella [35] which was developed for communication over binary symmetric channels and later adapted to Gaussian channels by Hochwald in [36], may be utilized in the current scenario, after adjusting for energy instead

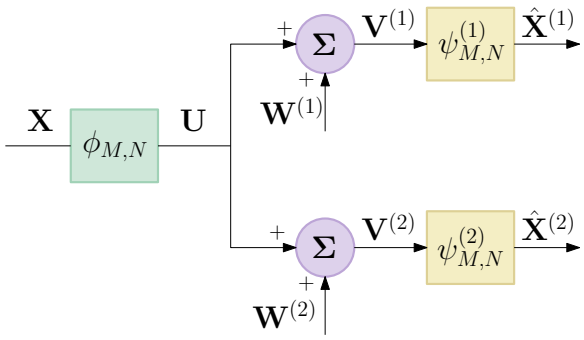

Figure 2.2: The block diagram for transmission of a Gaussian source sequence $\mathbf{X}$ over the Gaussian broadcast channel $\mathbf{V}^{(i)} = \mathbf{U} + \mathbf{W}^{(i)}$, $i = 1, 2$. Each receiver estimates its version $\hat{\mathbf{X}}^{(i)}$ of the source.

of channel input power. One advantage our approach has is that it produces a constructive scheme which is very easy to implement in practice. Another is that it easily generalizes to broadcast channels, as we discuss next.

2.2.2 Broadcast Channels

Let $\mathbf{X}$ be a real-valued M-dimensional source to be transmitted over the broadcast channel $\mathbf{V}^{(i)} = \mathbf{U} + \mathbf{W}^{(i)}$, $i = 1, 2$, where $\mathbf{U}$ is the N-dimensional channel input as in the point-to-point case, and $\mathbf{V}^{(i)}$ are the output vectors at the two receivers. The channel noise $\mathbf{W}^{(i)}$ are independent of $\mathbf{U}$, and $\mathbf{W}^{(i)} \sim \mathcal{N}(\mathbf{0}, \sigma^2_{W_i}\mathbf{I})$. We also define

$$\rho = \frac{\sigma^2_{W_1}}{\sigma^2_{W_2}}.$$

and without loss of generality, assume that $\rho > 1$, i.e., the second receiver is "better."

The encoder $\phi_{M,N} : \mathbb{R}^M \to \mathbb{R}^N$ maps $\mathbf{X}$ into $\mathbf{U}$, and the decoder at the ith receiver $\psi^{(i)}_{M,N} : \mathbb{R}^N \to \mathbb{R}^M$ estimates $\mathbf{X}$ from $\mathbf{V}^{(i)}$ as $\hat{\mathbf{X}}^{(i)}$ for $i = 1, 2$. Figure 2.2 depicts the scenario. We refer to $\gamma_i = \frac{E}{\sigma^2_{W_i}}$ as the ENR per source symbol observed at each receiver $i = 1, 2$.

Clearly,

$$\gamma_2 = \rho\gamma_1 \ .$$

Definition 3 *An energy-distortion triplet* $\left(D^{(1)}, D^{(2)}, E\right)$ *is achievable if for any* $\epsilon > 0$*, there exist large enough* M, N *and* $(\phi_{M,N}, \psi^{(1)}_{M,N}, \psi^{(2)}_{M,N})$ *such that*

$$\frac{1}{M}\mathbb{E}\left[||\mathbf{U}||^2\right] \leq E + \epsilon$$
$$\frac{1}{M}\mathbb{E}\left[||\mathbf{X} - \hat{\mathbf{X}}^{(i)}||^2\right] \leq D^{(i)}(1+\epsilon)$$

for $i = 1, 2$*.*

In [37], the region of achievable $(D^{(1)}, D^{(2)}, E)$ was analyzed and inner and outer bounds were provided. We focus instead on the tradeoff with finite M as defined next.

Definition 4 *An energy-distortion triplet* $\left(D^{(1)}, D^{(2)}, E\right)$ *is* M*-achievable if for any* $\epsilon > 0$*, there exist large enough* N *and* $(\phi_{M,N}, \psi^{(1)}_{M,N}, \psi^{(2)}_{M,N})$ *such that*

$$\frac{1}{M}\mathbb{E}\left[||\mathbf{U}||^2\right] \leq E + \epsilon$$
$$\frac{1}{M}\mathbb{E}\left[||\mathbf{X} - \hat{\mathbf{X}}^{(i)}||^2\right] \leq D^{(i)}(1+\epsilon)$$

for $i = 1, 2$*.*

We modify the scheme described in the point-to-point case as follows. Let $N = N_1 + N_2$ with $N_1 \gg 1$ and $N_2 \gg 1$. We quantize $\mathbf{X}$ with successive refinement with N_1 levels in the base layer and N_2 levels in the refinement layer. We then use orthogonal signaling and maximum likelihood decoding as in point-to-point transmission, with the modification

that the transmission is done in two rounds: In the jth round, $j = 1, 2$, the channel is used N_j times to transmit the jth layer quantization index, i.e., $\mathbf{U} = [\mathbf{U}_1\ \mathbf{U}_2]$ such that

$$\mathbf{U}_1 = \sqrt{\tau ME}\ \mathbf{e}_{k_1(\mathbf{X})}$$

$$\mathbf{U}_2 = \sqrt{\bar{\tau} ME}\ \mathbf{e}_{k_2(\mathbf{X})}\ ,$$

where $1 \leq k_j(\mathbf{X}) \leq N_j$ is the jth layer vector quantization index, $0 \leq \tau \leq 1$ and $\bar{\tau} = 1 - \tau$.

Although both receivers have access to both rounds, i.e., $\mathbf{V}^{(i)} = [\mathbf{V}_1^{(i)}\ \mathbf{V}_2^{(i)}]$, $i = 1, 2$, only the second receiver attempts to decode the refinement layer, thereby discarding $\mathbf{V}_2^{(1)}$. The first receiver performs maximum likelihood decoding as in the point-to-point case, i.e.,

$$\hat{K}_1^{(1)} = \underset{1 \leq t \leq N_1}{\arg\max}\ V_{1,t}^{(1)}$$

and then outputs $\hat{\mathbf{X}}^{(1)} = \mathbf{r}_{\hat{K}_1^{(1)}}$. The second receiver also performs maximum likelihood decoding as

$$\hat{K}_j^{(2)} = \underset{1 \leq t \leq N_j}{\arg\max}\ V_{j,t}^{(2)}$$

for round $j = 1, 2$, and outputs $\hat{\mathbf{X}}^{(2)} = \mathbf{r}_{\hat{K}_2^{(2)}|\hat{K}_1^{(2)}}$. Here $\mathbf{r}_{k_1}$ is the k_1th reconstruction level of the base layer quantizer, and $\mathbf{r}_{k_2|k_1}$ is the conditional k_2th reconstruction level at the refinement layer given the k_1th reconstruction level of the base layer.

Occasional decoding errors of quantization index $k_j(\mathbf{X})$ at receiver i will be denoted by the outage event

$$\mathcal{O}_j^{(i)} = \left\{ k_j(\mathbf{X}) \neq \hat{K}_j^{(i)} \right\}\ , \tag{2.7}$$

where the event $\mathcal{O}_2^{(1)}$ is moot, as mentioned above.

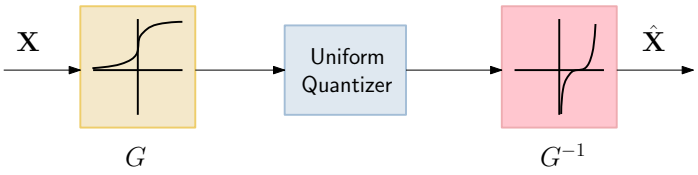

Figure 2.3: Compander model, where G is a nonlinear compressor and G^{-1} is a nonlinear expander.

2.2.3 High Resolution Quantization

Our proposed scheme is formulated by exploiting high-resolution quantization theory, which can be justified by the fact that the number of quantization levels N must increase exponentially with γ to guarantee an exponentially decaying distortion, as will be apparent in the sequel. Distortion in the high-resolution regime is best understood with the help of companders [38] as shown in Figure 2.3. First, a nonlinear compressor G reduces the spread of large amplitudes and maps the source sample to $[0, 1]$. Then, the source is uniformly quantized in the compressed domain with N levels. Finally, a nonlinear expander G^{-1} reverses this process by expanding the small amplitudes of uniformly quantized output. As a result, the overall impact of compander turns into a non-uniform quantizer.

As explained in [38], when N is large, an equivalent framework for non-uniform quantization is provided by the point density function, $\lambda(x) = \frac{dG}{dx}$, which approximately indicates the fraction of quantization points per unit width centered at x. It also has the convenient property that $\lambda(x) \geq 0$ and

$$\int_{-\infty}^{\infty} \lambda(x)dx = 1 \ .$$

That is, its behavior is the same as that of a probability density function (pdf).

It is well-known (cf. [38–40]) that the MSE distortion incurred by an N-level scalar quantizer employing $\lambda(\cdot)$ as the point density function satisfies

$$\lim_{N\to\infty} N^2\mathbb{E}\big[(X - r_{k(X)})^2\big] = d(\lambda(\cdot)) \triangleq \frac{1}{12}\int_{-\infty}^{\infty} \frac{f(x)}{\lambda^2(x)}dx \tag{2.8}$$

whenever the integral converges, where $r_{k(X)}$ is the output of the quantizer as mentioned before, and $f(x)$ is the source pdf. The integral above is known as the Bennett integral.

The Bennett integral and interpretation of point density function $\lambda(\mathbf{x})$ need to be revisited for the case where $M > 1$. In [41], it was proven that

$$\begin{aligned}\lim_{N\to\infty} N^{2/M}\frac{1}{M}\mathbb{E}\big[\,\|\mathbf{X}-\mathbf{r}_{k(\mathbf{X})}\|^2\,\big] &= d_M(m(\cdot),\lambda(\cdot)) \\ &\triangleq \int \frac{m(\mathbf{x})f(\mathbf{x})}{\lambda^{2/M}(\mathbf{x})}d\mathbf{x}\end{aligned} \tag{2.9}$$

whenever the integral converges. Here, $\lambda(\mathbf{x})$ indicates the fraction of codevectors per unit volume and $m(\cdot)$ is the inertial profile that designates the normalized moment of inertia of quantization cells as a function of location, surmising that cells have a certain lattice tessellation and neighboring cells exhibit a similar normalized moment of inertia. According to Gersho's conjecture [40], $m(\mathbf{x}) = C(M)$ is the optimal choice, [2] where

$$C(M) = \frac{1}{M}\inf_{H\in H_M} I(H)\,,$$

with $I(H)$ being the normalized inertia of a convex polytope H and H_M being the class of admissible polytopes in $\mathbb{R}^M$.

[2] As we seek an *upper bound* to the distortion, we will just set $m(\mathbf{x}) = C(M)$ and will not need this conjecture to be true in the sequel.

When we set $m(\mathbf{x}) = C(M)$, optimal point density function for the purpose of minimizing the MSE distortion becomes

$$\lambda_M^*(\mathbf{x}) = \frac{f^{M/(M+2)}(\mathbf{x})}{\int f^{M/(M+2)}(\mathbf{x}')d\mathbf{x}'} \, . \tag{2.10}$$

as shown in [41].

In this work, we consider zero-delay or low-delay scenarios to determine dispersion, where $M = 1$ or $M = 2$ respectively. For these two cases, optimal polytopes, hence the exact values of $C(M)$, are known. It is clear that $C(1) = \frac{1}{12}$. Fejes-Tóth [42] and Newman [43] showed that the optimal polytope for $M = 2$ is the regular hexagon, yielding

$$C(2) = \frac{5\sqrt{3}}{108} \approx 0.0802 \, .$$

For the cases where $M > 2$, one of the two well-known upper bounds on $C(M)$ can be used. Those are the simple cube upper bound [40]

$$C(M) \leq \frac{1}{12} \approx 0.0833 \, ,$$

and the Zador upper bound [39]

$$C(M) \leq \frac{1}{M}\Gamma\left(1 + \frac{2}{M}\right) V_M^{-2/M} \, ,$$

where $\Gamma(\cdot)$ is the gamma function, and V_M is the volume of the unit sphere in M dimensions. For similar discussions on vector quantization, the reader can refer to [44–47] and the references therein.

From (2.9), it can be easily observed that distortion due to the quantization decreases like $N^{-2/M}$ with an accompanied constant that depends on the source pdf, point density, and inertial profile. We also assume that the source pdf, the compressor/expander functions are sufficiently *smooth* and well-behaved throughout the work so that (2.9) holds.

Chapter 3

Achievable Energy-Distortion Exponent and Dispersion Analysis for Point-to-Point Channel

3.1 Achievable Energy-Distortion Exponents

The energy-distortion exponent is a useful performance metric, particularly in the absence of a fully characterized $D_M(\gamma)$. We derive a lower bound on energy-distortion exponent and dispersion by using the achievable scheme that we discussed in the previous section. The theorem that we will be presenting reveals that our coding scheme is exponent-optimal for $M = 1$ and for $M \to \infty$, i.e., it achieves the exponent $\Theta_1 = \frac{1}{6}$ and $\Theta_\infty = 1$. To the best of our knowledge, this paper is the first to study the energy-distortion exponent for $1 < M < \infty$.

Theorem 1 (Point-to-point energy-distortion exponents): *The scheme proposed in Section 2.2.1 can achieve an exponent given by*

$$\lim_{\gamma\to\infty} -\frac{1}{\gamma}\ln D_M(\gamma) \geq \theta_M \triangleq \begin{cases} 1/6 & M=1 \\ \frac{M}{(\sqrt{M}+\sqrt{2})^2} & M>1 \end{cases}, \tag{3.1}$$

with the choice

$$N = ce^{\alpha\gamma}\,, \tag{3.2}$$

where α is properly picked and c is a constant.

Proof. Let $\mathbb{D}_M(\gamma)$ denote the MSE distortion achieved by the proposed scheme. It can be bounded using the outage notation as

$$\begin{aligned} D_M(\gamma) &\leq \mathbb{D}_M(\gamma) \\ &\leq \frac{1}{M}\Big[\Pr[\mathcal{O}]\cdot\mathbb{E}\big[\parallel \mathbf{X}-\hat{\mathbf{X}}\parallel^2 \big|\mathcal{O}\big] + \mathbb{E}\big[\parallel \mathbf{X}-\hat{\mathbf{X}}\parallel^2 \big|\mathcal{O}^c\big]\Big]. \end{aligned} \tag{3.3}$$

We proceed by bounding each of the terms in (3.3).

Distortion outside the outage region for the optimal high resolution quantizer can be upper bounded by setting $m(\mathbf{x}) = C(M)$ in the M-dimensional Bennett integral given in (2.9), i.e.,

$$\frac{1}{M}\mathbb{E}[\parallel \mathbf{X}-\hat{\mathbf{X}}\parallel^2 |\mathcal{O}^c] \leq N^{-\frac{2}{M}}\Big[\epsilon + d_M(C(M),\lambda(\cdot))\Big] \tag{3.4}$$

for any $\epsilon > 0$ and large enough N. Defining

$$P_e(N|\Gamma) = \begin{cases} \delta e^{\left(\ln N - \frac{\Gamma}{4}\right)} & \ln N \leq \frac{\Gamma}{8} \\ \delta e^{-\frac{1}{2}\left(\sqrt{\Gamma} - \sqrt{2\ln N}\right)^2} & \frac{\Gamma}{8} \leq \ln N \leq \frac{\Gamma}{2} \end{cases},$$

where $\delta = \frac{1}{2} + \frac{1}{2\sqrt{2}} \approx 0.8536$, we state the following lemma:

Lemma 1 $\Pr[\mathcal{O}]$ *can be upper bounded as*

$$\Pr[\mathcal{O}] \leq P_e(N|M\gamma) \tag{3.5}$$

Proof. We defer the proof to Appendix A.2. ■

Finally, the last term in (3.3) representing the MSE conditioned on outage can be bounded as in the next lemma.

Lemma 2 *For any $\epsilon > 0$, the proposed scheme satisfies*

$$\mathbb{E}\left[\parallel \mathbf{X} - \hat{\mathbf{X}} \parallel^2 \left| \mathcal{O} \right.\right] \leq \epsilon + \mathbb{E}\left[\parallel \mathbf{X} \parallel^2 \right] + \int ||\tilde{\mathbf{x}}||^2 \lambda(\tilde{\mathbf{x}}) d\tilde{\mathbf{x}} \tag{3.6}$$

for large enough N.

Proof. We refer reader to Appendix A.3 for the proof. ■

Now, from (3.3)-(3.6) and (3.2), it follows that

$$\lim_{\gamma \to \infty} -\frac{1}{\gamma} \ln D_M(\gamma) \geq \min\left\{ \frac{2\alpha}{M}, g(\alpha|M) \right\}, \tag{3.7}$$

with

$$g(\alpha|s) \stackrel{\Delta}{=} \begin{cases} \frac{s}{4} - \alpha & \alpha \leq \frac{s}{8} \\ \frac{1}{2}\left(\sqrt{s} - \sqrt{2\alpha}\right)^2 & \frac{s}{8} \leq \alpha \leq \frac{s}{2} \end{cases},$$

for any $s \geq 0$ and $0 < \alpha \leq \frac{s}{2}$. Thus, the problem becomes a max min problem and the maximum exponent is evidently achieved when

$$g(\alpha|M) = \frac{2\alpha}{M}, \tag{3.8}$$

yielding the lower bound on the achieved exponent given in (3.1). ■

Remark 1 *The lower bound in (3.1) is increasing in M, and matches the best possible exponent, i.e., $\frac{1}{6}$ for $M = 1$, and 1 as $M \to \infty$. Thus, we can conclude that for these two cases, this simple scheme is exponent-optimal. Unfortunately, the converse in [28] is hard to generalize for higher dimensions $M > 1$, and it remains as an open problem.*

Remark 2 *With the choice of $N = ce^{\alpha\gamma}$, even mediocre values of γ will quickly drive N to a very large number, thus making the high-resolution assumption also practical. This is further discussed and demonstrated in Section 3.2.4.*

3.2 Achievable Energy-Distortion Dispersion for $M = 1$

To the best of our knowledge, the only work in the literature addressing the dispersion (albeit indirectly) is [2], where an analytical upper bound for the distortion was

derived using a uniform quantizer and maximum a posteriori (MAP) receiver:

$$D_1(\gamma) < e^{-\gamma/6}\left(\frac{\sqrt{6}}{\sqrt{\pi\gamma}}\left(1+e^{-\gamma/6}\left(\frac{4\gamma}{3}+1\right)\right)+\frac{5\gamma}{3}\right). \tag{3.9}$$

For large γ, this can be re-written as

$$-\ln D_1(\gamma) \geq \frac{1}{6}\gamma - \ln\frac{5\gamma}{3} + o(1)\ . \tag{3.10}$$

In comparison, with the choice of N as in (3.2) and α as in (3.8), our scheme achieves

$$-\ln D_1(\gamma) \geq \frac{1}{6}\gamma + \upsilon(c,\lambda) + o(1) \tag{3.11}$$

for large γ, where $\upsilon(c,\lambda)$ is a function of the chosen c and the point-density function $\lambda(\mathbf{x})$, but does not depend on γ, i.e.,

$$\upsilon(c,\lambda) = -\ln\left[\delta c\left(1+\int_{-\infty}^{\infty}x^2\lambda(x)dx\right)+\frac{1}{12c^2}\int_{-\infty}^{\infty}\frac{f(x)}{\lambda(x)^2}dx\right]. \tag{3.12}$$

Comparing (3.11) to (3.10) therefore reveals that while both schemes achieve the same exponent, the dispersion achieved by the scheme in [2] results in a dispersion diverging to $-\infty$ as $\gamma \to \infty$. In contrast, our scheme achieves a constant dispersion $\upsilon(c,\lambda)$. In the rest of this section, we compare different approaches that can be taken for the design of the point density function $\lambda(\mathbf{x})$, along with an optimized c, and analyze and compare the dispersion achieved by each approach.

3.2.1 The Naïve approach

If we disregard the end-to-end distortion and optimize $\lambda(x)$ only to minimize the high-resolution quantization error, i.e., the second term in (3.12) (as would be done in source coding), then it follows from (2.10) that $\lambda(\mathbf{x})$ is the normalized cubic root of the source pdf when $M = 1$. For unit-variance Gaussian sources, that translates to $\lambda(x) \sim \mathcal{N}(0, 3)$. Substituting $\lambda(x)$ in (3.12) yields after some algebra

$$\upsilon(c, \lambda) = \upsilon(c) \stackrel{\Delta}{=} -\ln\left[4\delta c + \frac{\sqrt{3}\pi}{2c^2}\right] ,$$

optimizing which, with respect to c, then yields

$$c = \left(\frac{\sqrt{3}\pi}{4\delta}\right)^{\frac{1}{3}} \approx 1.1681$$

and as a result,

$$\upsilon(c, \lambda) \approx -1.7888 . \tag{3.13}$$

3.2.2 σ-optimal Gaussian pdf approach

If $\lambda(x)$ is kept as a zero-mean Gaussian with a general variance $\sigma^2 > 2$, (3.12) becomes

$$\upsilon(c, \lambda) = \upsilon(c, \sigma^2) \stackrel{\Delta}{=} -\ln\left[\delta c\left(1 + \sigma^2\right) + \frac{\pi\sigma^3}{6c^2\sqrt{\sigma^2 - 2}}\right] .$$

Solving for optimal σ^2 and c via $\frac{\partial \upsilon}{\partial c} = \frac{\partial \upsilon}{\partial \sigma^2} = 0$ yields

$$\sigma^2 = 1 + \sqrt{2} \approx 2.4142 \tag{3.14}$$

$$c = \sqrt[3]{\frac{\pi\sigma^3}{3\delta(1+\sigma^2)\sqrt{\sigma^2-2}}} \approx 1.2794\,. \tag{3.15}$$

The corresponding maximum value of the dispersion than becomes

$$\upsilon(c,\lambda) \approx -1.7215\,, \tag{3.16}$$

i.e., slightly larger than achieved by the naïve approach.

3.2.3 λ-optimal approach

In this approach, we aim to find the optimal point density function $\lambda(x)$ defined as the solution to

$$\begin{aligned} \underset{c,\lambda(x)}{\text{maximize}} \quad & \upsilon(c,\lambda) \\ \text{subject to} \quad & -\lambda(x) \leq 0 \\ & \int_{-\infty}^{\infty} \lambda(x)dx = 1\,. \end{aligned}$$

The result of this optimization was found numerically as

$$\upsilon(c,\lambda) \approx -1.7006\,. \tag{3.17}$$

We refer the reader to Appendix A.1 for the details of this result. Comparing with (3.13), this dispersion translates into ≈ 0.38dB improvement in distortion.

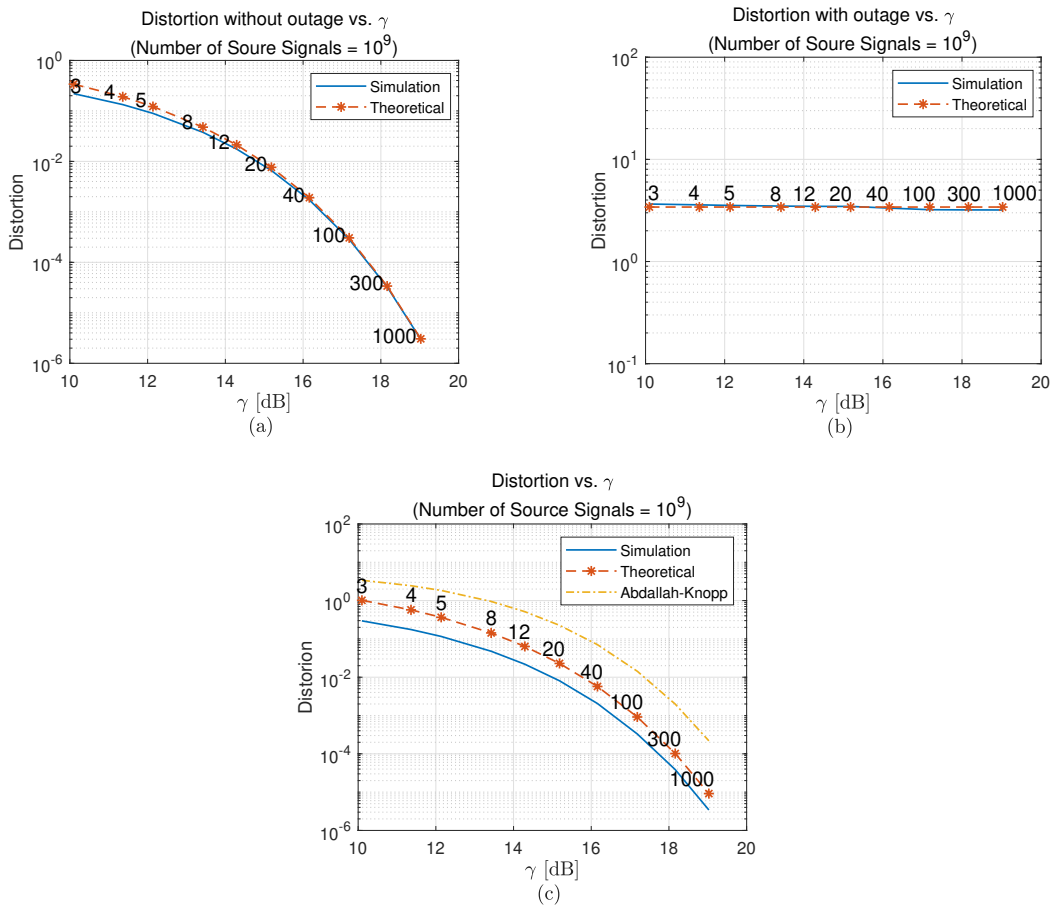

Figure 3.1: The accuracy of the high resolution assumption for the MSE distortion conditioned on no outage and outage are depicted in (a) and (b), respectively. In (c), performance of the scheme in [2] given in (3.9) is compared to both the theoretical upper bound and the simulated result for our σ-optimal approach. Numbers around markers represent $N = ce^{\alpha\gamma}$ values.

3.2.4 Practical Energy-Distortion Tradeoff

In this section, we simulate the proposed end-to-end communication system and test the validity of the high resolution approximation for low to moderate values of γ. For brevity, we only test Gaussian point density function $\lambda(x) = \mathcal{N}(0, \sigma^2)$, where σ^2 is as in (3.14) as discussed above.

We generate Gaussian source samples $X_t \sim \mathcal{N}(0,1)$ for $1 \leq t \leq 10^9$. These samples are each passed through a nonlinear compressor function $G(x) = \int_{-\infty}^{x} \lambda(y)dy$ and then uniformly quantized with $N = ce^{\alpha\gamma}$ levels in the interval $(0,1)$, where $\alpha = \frac{1}{12}$ is the solution of (3.8) for $M = 1$, and c is as in (3.15). Quantized indices $k(X_t)$ are then coded with orthogonal signaling and transmitted through AWGN channel $V_t = U_t + W_t$, where $W_t \sim \mathcal{N}(0,1)$. At the receiver end, maximum likelihood detection is applied, the decoded $\hat{K}_t$ is mapped to $(0,1)$ and passed through the expander function G^{-1}, and the resultant $\hat{X}_t$ is output. The event $\mathcal{O}_t = \{k(X_t) \neq \hat{K}_t\}$ is also detected whenever it occurs.

In Figure 3.1(a) and (b), we compare the high resolution approximations of $\mathbb{E}\big[(X - \hat{X})^2 \big| \mathcal{O}^c\big]$ and $\mathbb{E}\big[(X - \hat{X})^2 \big| \mathcal{O}\big]$ provided in (3.4) and (3.6), respectively, to their simulated counterparts. As can be seen, with this choice of $\lambda(x)$, when γ is around 17dB (i.e., $N \approx 100$), the high resolution approximations become very accurate. In Figure 3.1(c), we compare the performance of the scheme in [2] with that of our σ-optimal approach. We observe that (i) there is a wide gap between the simulated distortion and the theoretical upper bound to it provided in (3.11), stemming from the looseness of the bound on probability of decoding error $\Pr[\mathcal{O}]$ in Lemma 1, and (ii) the gap between our approach and the scheme in [2] increases with growing γ, as one would predict by comparing (3.10) and (3.11).

3.3 Achievable Energy-Distortion Dispersion for $M = 2$

As was explained in the Introduction, it is sometimes feasible to introduce a small amount of source delay. Here, we analyze the case $M = 2$, where the source $\mathbf{X}$ is bivariate

Gaussian with zero mean and covariance matrix $\mathbf{C_X} = \mathbf{I}$. We note that although the exponent achieved by the proposed algorithm is not provably optimal, it is worth analyzing and optimizing the achieved dispersion to obtain a full picture as to how distortion behaves for large γ.

For $M = 2$, the solution to (3.8) is achieved by $\alpha = \frac{1}{4}$, and we will therefore use $N = ce^{\frac{\gamma}{4}}$ quantization levels. In parallel to (3.11) and (3.12), for large N, the bound becomes

$$-\ln D_2(\gamma) \geq \frac{1}{4}\gamma + \upsilon(c,\lambda) + o(1) \tag{3.18}$$

for large γ, where $\upsilon(c,\lambda)$ is

$$\upsilon(c,\lambda) = -\ln\left[\frac{1}{2}\delta c\left(2 + \int \parallel \boldsymbol{x} \parallel^2 \lambda(\boldsymbol{x})d\boldsymbol{x}\right) + \frac{5\sqrt{3}}{108c}\int \frac{f(\boldsymbol{x})}{\lambda(\boldsymbol{x})}d\boldsymbol{x}\right]. \tag{3.19}$$

3.3.1 The Naïve approach

As a result of naïvely done quantization in (2.10), $\lambda(\mathbf{x})$ reduces to $\lambda(\mathbf{x}) \sim \mathcal{N}(\mathbf{0}, 2\mathbf{I})$, which, after substituting into (3.19), yields

$$\upsilon(c) = -\ln\left[3\delta c + \frac{10\sqrt{3}\pi}{27c}\right],$$

It can then be readily shown that this induces $c \approx 0.7870$ as the optimal choice with the corresponding dispersion $\upsilon(c,\lambda) \approx -1.5137$.

3.3.2 σ-optimal Gaussian pdf approach

For simplicity, we set $\lambda(\mathbf{x}) = \mathcal{N}(\mathbf{0}, \sigma^2\mathbf{I})$, and optimize over σ^2 as well as c. In this case, (3.19) becomes

$$\upsilon(c, \sigma^2) = \delta c \left(1 + \sigma^2\right) + \frac{5\sqrt{3}\pi}{54c} \frac{\sigma^4}{\sigma^2 - 1} \, .$$

Solving $\frac{\partial \upsilon}{\partial c} = \frac{\partial \upsilon}{\partial \sigma^2} = 0$ results in

$$\begin{aligned} \sigma^2 &= \frac{1 + \sqrt{5}}{2} \approx 1.6180 \\ c &= \sqrt{\frac{5\sqrt{3}\pi}{54\delta} \frac{\sigma^4}{(\sigma^4 - 1)}} \approx 0.9773 \, , \end{aligned}$$

leading to

$$\upsilon(c, \sigma^2) = -1.4742 \, .$$

3.3.3 λ-optimal approach

The result of this optimization was found numerically as

$$\upsilon(c, \lambda) \approx -1.4686 \, , \tag{3.20}$$

yielding an about 0.20dB improvement over the naive approach. We refer the reader to Appendix A.1 for the details of this result.

Chapter 4

Achievable Energy-Distortion Exponent and Dispersion Analysis for Broadcast Channels

4.1 Achievable Energy-Distortion Exponents

Let $\mathbb{D}_M^{(i)}(\gamma_i) = \mathbb{E}[\| \mathbf{X} - \hat{\mathbf{X}}_i \|^2]$ denote the end-to-end the expected distortion achieved by the scheme proposed in Section 2.2.2 at receiver i. As in point-to-point communication, we let N_1 and N_2 grow exponentially fast with γ_1 and γ_2, respectively, i.e.,

$$N_1 = c_1 e^{\alpha_1 \gamma_1} \tag{4.1}$$

$$N_2 = c_2 e^{\alpha_2 \gamma_2} \ . \tag{4.2}$$

$$\mathbb{D}_M^{(1)}(\gamma_1) \le \frac{1}{M}\Bigg[\Pr[\mathcal{O}_1^{(1)}] \cdot \mathbb{E}\Big[\| \mathbf{X} - \hat{\mathbf{X}}_1 \|^2 \, \Big| \mathcal{O}_1^{(1)} \Big] + \mathbb{E}\Big[\| \mathbf{X} - \hat{\mathbf{X}}_1 \|^2 \, \Big| \mathcal{O}_1^{(1),c} \Big] \Bigg]$$
$$\le \frac{1}{M} P_e(N_1, \tau M \gamma_1) \left[\epsilon + \mathbb{E}\big[\| \mathbf{X} \|^2 \big] + \int ||\tilde{\mathbf{x}}||^2 \lambda(\tilde{\mathbf{x}}) d\tilde{\mathbf{x}} \right]$$
$$+ N_1^{-2/M} [\epsilon + d_M(C(M), \lambda(\cdot))] \tag{4.3}$$
$$\mathbb{D}_M^{(2)}(\gamma_2) = \frac{1}{M}\Bigg[\Pr[\mathcal{O}_1^{(2),c}] \Pr[\mathcal{O}_2^{(2),c}] \cdot \mathbb{E}\Big[\| \mathbf{X} - \hat{\mathbf{X}}_2 \|^2 \, \Big| \mathcal{O}_1^{(2),c}, \mathcal{O}_2^{(2),c} \Big]$$
$$+ \Pr[\mathcal{O}_1^{(2),c}] \Pr[\mathcal{O}_2^{(2)}] \cdot \mathbb{E}\Big[\| \mathbf{X} - \hat{\mathbf{X}}_2 \|^2 \, \Big| \, \mathcal{O}_1^{(2),c}, \mathcal{O}_2^{(2)} \Big]$$
$$+ \Pr[\mathcal{O}_1^{(2)}] \Pr[\mathcal{O}_2^{(2),c}] \cdot \mathbb{E}\Big[\| \mathbf{X} - \hat{\mathbf{X}}_2 \|^2 \, \Big| \, \mathcal{O}_1^{(2)}, \mathcal{O}_2^{(2),c} \Big]$$
$$+ \Pr[\mathcal{O}_1^{(2)}] \Pr[\mathcal{O}_2^{(2)}] \cdot \mathbb{E}\Big[\| \mathbf{X} - \hat{\mathbf{X}}_2 \|^2 \, \Big| \, \mathcal{O}_1^{(2)}, \mathcal{O}_2^{(2)} \Big] \Bigg]$$
$$\le \frac{1}{M}\Bigg[\mathbb{E}\Big[\| \mathbf{X} - \hat{\mathbf{X}}_2 \|^2 \, \Big| \, \mathcal{O}_1^{(2),c}, \mathcal{O}_2^{(2),c} \Big] + P_e(N_2, \bar{\tau} M \gamma_2) \, \mathbb{E}\Big[\| \mathbf{X} - \hat{\mathbf{X}}_2 \|^2 \, \Big| \, \mathcal{O}_1^{(2),c}, \mathcal{O}_2^{(2)} \Big]$$
$$+ P_e(N_1, \tau M \gamma_2) \, \mathbb{E}\Big[\| \mathbf{X} - \hat{\mathbf{X}}_2 \|^2 \, \Big| \, \mathcal{O}_1^{(2)}, \mathcal{O}_2^{(2),c} \Big]$$
$$+ P_e(N_1, \tau M \gamma_2) P_e(N_2, \bar{\tau} M \gamma_2) \cdot \mathbb{E}\Big[\| \mathbf{X} - \hat{\mathbf{X}}_2 \|^2 \, \Big| \mathcal{O}_1^{(2)}, \mathcal{O}_2^{(2)} \Big] \Bigg]. \tag{4.4}$$

We also let $0 \le \tau \le 1$ determine what fraction of available energy is allocated to the first layer description. Clearly, the distortion at receiver 1 mimics the point-to-point distortion analyzed in Section 3, resulting in (4.3) for any $\epsilon > 0$ and large enough N_1, where Lemmas 1 and 2 are employed as before. On the other hand, the distortion at receiver 2 has a more complicated given in (4.4). We proceed by analyzing each expectation in (4.4):

• $\mathbb{E}\Big[\| \mathbf{X} - \hat{\mathbf{X}}_2 \|^2 \, \Big| \, \mathcal{O}_1^{(2),c}, \mathcal{O}_2^{(2),c} \Big]$: This distortion is the same as in (3.4), except there are $N_1 N_2$ quantization levels. That is,

$$\frac{1}{M}\mathbb{E}\Big[\| \mathbf{X} - \hat{\mathbf{X}}_2 \|^2 \, \Big| \mathcal{O}_1^{(2),c}, \mathcal{O}_2^{(2),c} \Big] \le (N_1 N_2)^{-2/M} [\epsilon + d_M(C(M), \lambda(\cdot))] \tag{4.5}$$

for any $\epsilon > 0$ and large enough N_1, N_2.[1]

[1] While the well-known notion of successive refinability is about finite rates but infinite blocklengths, we

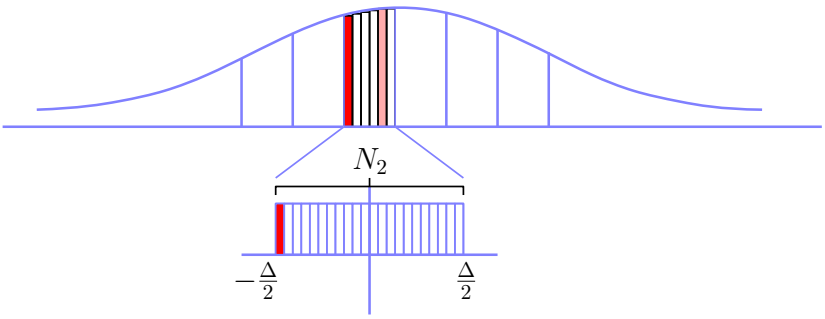

Figure 4.1: Description of the case where there is no outage in the first layer, while there is an outage in the second layer.

• $\mathbb{E}\Big[\parallel \mathbf{X} - \hat{\mathbf{X}}_2 \parallel^2 \Big| \mathcal{O}_1^{(2),c}, \mathcal{O}_2^{(2)} \Big]$: This case is illustrated in Figure 4.1 for $M = 1$. As $N_1 \to \infty$, the input pdf is nearly constant over the first layer quantization region $\mathcal{R}_i$, i.e., $f(\mathbf{x}) \approx f_i$ for $\mathbf{x} \in \mathcal{R}_i$. The following lemma bounds this distortion for large N_1, N_2.

Lemma 3 *For any $\epsilon > 0$ and large enough N_1, N_2,*

$$\frac{1}{M}\mathbb{E}\Big[\| \mathbf{X} - \hat{\mathbf{X}}_2 \|^2 \Big| \mathcal{O}_1^{(2),c}, \mathcal{O}_2^{(2)} \Big] \leq N_1^{-2/M} \big[\epsilon + 2 d_M(C(M), \lambda(\cdot)) \big]. \tag{4.6}$$

Proof. Using similar steps as in the proof of Lemma 2, one can show that for each $1 \leq i \leq N_1$,

$$\mathbb{E}\Big[\| \mathbf{X} - \hat{\mathbf{X}}_2 \|^2 \Big| \mathcal{O}_1^{(2),c}, \mathcal{O}_2^{(2)}, \mathbf{X} \in \mathcal{R}_i \Big] \leq \frac{N_2}{N_2 - 1} \Big(\mathbb{E}\big[\| \mathbf{X} - \mathbf{r}_i \|^2 \,\big|\, \mathbf{X} \in \mathcal{R}_i \big] + \mathbb{E}\big[\| \tilde{\mathbf{X}} - \mathbf{r}_i \|^2 \big] \Big)$$

where it is assumed that each $\mathbf{r}_i$ is chosen as the centroid of the cell $\mathcal{R}_i$ (which is the optimal choice to minimize MSE), and $\tilde{\mathbf{X}}$ is a fictitious random vector distributed uniformly over the second layer reconstruction points $\mathbf{r}_{j|i}$. But since $f(\mathbf{x}) \approx f_i$ for $\mathbf{x} \in \mathcal{R}_i$, the distribution

are in the regime of finite blocklengths and very large quantization rates. Because the optimal quantizer at the first and second stages use the same point-density function, successive refinability is readily granted.

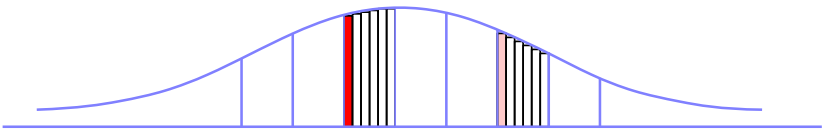

Figure 4.2: An example of the case where there is an outage in the first layer, but the second layer is decoded correctly when $M = 1$.

of $\mathbf{X}$ conditioned on $\mathbf{X} \in \mathcal{R}_i$ is also almost uniform in $\mathcal{R}_i$. That implies for large enough N_2 that

$$\mathbb{E}\Big[\| \mathbf{X} - \hat{\mathbf{X}}_2 \|^2 \, \big| \mathcal{O}_1^{(2),c}, \mathcal{O}_2^{(2)}, \mathbf{X} \in \mathcal{R}_i \Big] \leq \epsilon + 2\, \mathbb{E}\big[\| \mathbf{X} - \mathbf{r}_i \|^2 \, \big| \mathbf{X} \in \mathcal{R}_i \big]$$

which yields (4.6) after averaging over the first layer index i. ■

• $\mathbb{E}\Big[\| \mathbf{X} - \hat{\mathbf{X}}_2 \|^2 \, \big| \mathcal{O}_1^{(2)}, \mathcal{O}_2^{(2),c} \Big]$: This case is illustrated in Figure 4.2 for $M = 1$. Once there is an outage in the first layer, causing catastrophic distortion as shown in Lemma 2, whether there is outage in the second layer or not does not change the distortion much. That is because in the regime of large N_1, the first layer quantization cells are already small, and where exactly the second layer reconstruction falls inside the incorrect first layer quantization cell adds at most ϵ to the distortion.

Using Lemma 2, we can therefore write

$$\mathbb{E}\Big[\| \mathbf{X} - \hat{\mathbf{X}}_2 \|^2 \, \big| \mathcal{O}_1^{(2)}, \mathcal{O}_2^{(2),c} \Big] \leq \epsilon + \mathbb{E}\big[\| \mathbf{X} \|^2 \big] + \int ||\tilde{\mathbf{x}}||^2 \lambda(\tilde{\mathbf{x}}) d\tilde{\mathbf{x}} \tag{4.7}$$

as $N_1, N_2 \to \infty$.

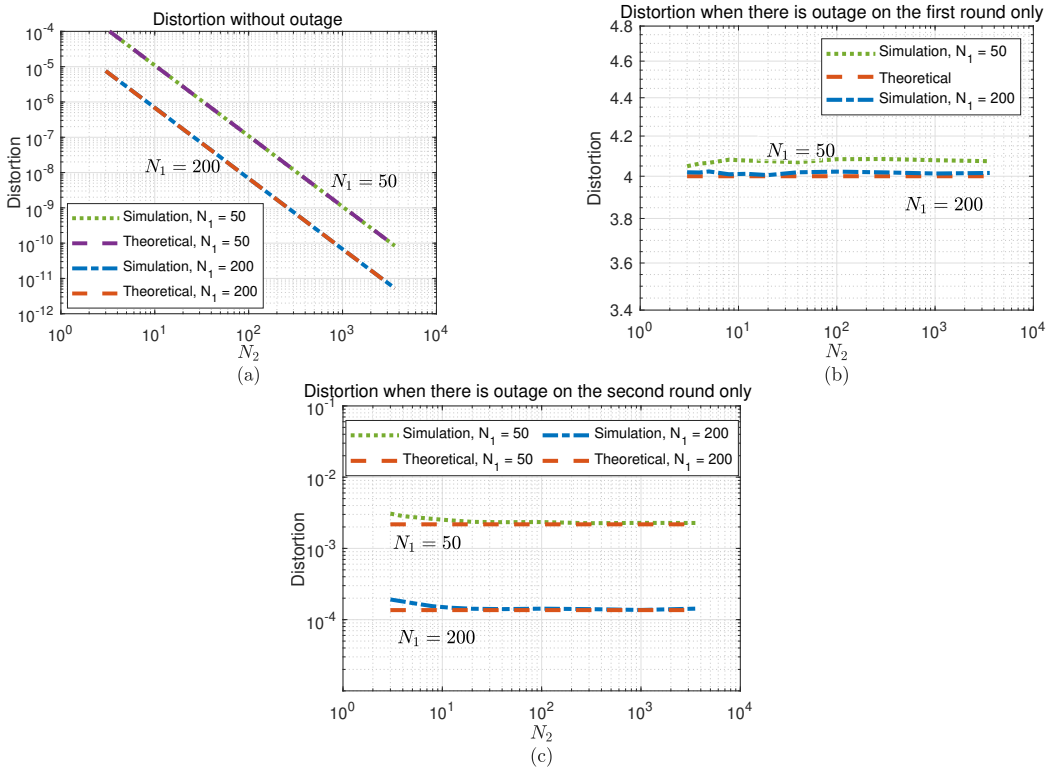

Figure 4.3: The accuracy of the high resolution assumption for the MSE distortion at the second receiver conditioned on (a) no outage at either layer, (b) outage at the first round of transmission only, and (c) outage at the second round of transmission only. Numbers around markers represent $N_2 = c_2 e^{\alpha_2 \gamma_2}$.

• $\mathbb{E}\Big[\| \mathbf{X} - \hat{\mathbf{X}}_2 \|^2 \Big| \mathcal{O}_1^{(2)}, \mathcal{O}_2^{(2)} \Big]$: Using the same reasoning we put forth for the previous expectation, the upper bound (4.7) also applies to this expectation. On the other hand, this expectation is multiplied by $P_e(N_1, \tau M \gamma_2) P_e(N_2, \bar{\tau} M \gamma_2)$, which decays much faster than the second and the third term for large γ_2, and therefore the contribution of this term to the distortion is only $o(1)$, and it can be ignored.

In Figure 4.3, we demonstrate the accuracy of the high-resolution approximations introduced in (4.5)-(4.7) when N_1 is fixed, and N_2 is varied. As can be seen, all three approximations are accurate when both N_1 and N_2 are high enough. We are now ready to analyze the behavior of (4.3) and (4.4) for large γ_1 and γ_2, respectively.

Theorem 2 *For any* $0 \leq \tau \leq 1$ *and* $0 < \alpha_1 \leq \frac{M\tau}{2}$, *let*

$$\beta_{1,M}(\alpha_1, \tau) \stackrel{\Delta}{=} \min\left\{\frac{2\alpha_1}{M}, g(\alpha_1|M\tau)\right\} \tag{4.8}$$

and

$$\beta_{2,M}(\alpha_1, \tau) \stackrel{\Delta}{=} \min\left\{\frac{2\alpha_1}{M\rho} + \bar{\tau}\theta_M, g\left(\frac{\alpha_1}{\rho}\Big|M\tau\right)\right\} \tag{4.9}$$

with $\bar{\tau} = 1 - \tau$.

Then the exponent pair $\left\{\beta_{1,M}(\alpha_1, \tau), \beta_{2,M}(\alpha_1, \tau)\right\}$ *is* M*-achievable, i.e.,*

$$\lim_{\gamma_1 \to \infty} -\frac{1}{\gamma_1} \ln \mathbb{D}_M^{(1)}(\gamma_1) \geq \beta_{1,M}(\alpha_1, \tau) \tag{4.10}$$

$$\lim_{\gamma_2 \to \infty} -\frac{1}{\gamma_2} \ln \mathbb{D}_M^{(2)}(\gamma_2) \geq \beta_{2,M}(\alpha_1, \tau)\ . \tag{4.11}$$

Proof. We set N_1 and N_2 as in (4.1) and (4.2), respectively, for some α_2 to be determined. Proof of (4.10) follows from (4.3) exactly the same way (3.7) follows from (3.2)-(3.6) with α_1 and γ_1 replacing α and γ, respectively.

At the second receiver, from (4.4)-(4.7) we have

$$\begin{aligned}\mathbb{D}_M^{(2)}(\gamma_2) \leq & (N_1 N_2)^{-2/M}[\epsilon + d_M(C(M), \lambda(\cdot)) \\ & + P_e(N_2, \bar{\tau} M \gamma_2) N_1^{-2/M}\left[\epsilon + 2d_M(C(M), \lambda(\cdot))\right] \\ & + P_e(N_1, \tau M \gamma_2)\left[\epsilon + \mathbb{E}\left[\ \|\mathbf{X}\|^2\ \right] + \int \|\tilde{\mathbf{x}}\|^2\ \lambda(\tilde{\mathbf{x}}) d\tilde{\mathbf{x}}\right]\end{aligned} \tag{4.12}$$

and thus

$$\lim_{\gamma_2\to\infty} -\frac{1}{\gamma_2}\ln \mathbb{D}_M^{(2)}(\gamma_2) \geq \min\left\{\frac{2}{M}\left(\frac{\alpha_1}{\rho}+\alpha_2\right), \frac{2\alpha_1}{M\rho}+g(\alpha_2|M\bar{\tau}), g\left(\frac{\alpha_1}{\rho}\Big|M\tau\right)\right\}. \quad (4.13)$$

Note that for any fixed α_1 and τ, one can choose the best α_2 to maximize the minimum in (4.13) as

$$\alpha_2^*(M,\tau) = \frac{M\bar{\tau}}{2}\theta_M \quad (4.14)$$

with θ_M defined as in (3.1), thereby simplifying (4.13) to

$$\begin{aligned}\lim_{\gamma_2\to\infty} -\frac{1}{\gamma_2}\ln \mathbb{D}_M^{(2)}(\gamma_2) &\geq \min\left\{\frac{2\alpha_1}{M\rho}+\bar{\tau}\theta_M, g\left(\frac{\alpha_1}{\rho}\Big|M\tau\right)\right\}\\ &= \beta_{2,M}(\alpha_1,\tau) \quad (4.15)\end{aligned}$$

finishing the proof. ■

We next analyze the tradeoff between $\beta_{1,M}(\alpha_1,\tau)$ and $\beta_{2,M}(\alpha_1,\tau)$. From (4.8) and (4.9), it is clear that to understand the tradeoff, we need to keep track of the conditions for which $\frac{2\alpha_1}{M} \lessgtr g(\alpha_1|M\tau)$ and $\frac{2\alpha_1}{M\rho}+\bar{\tau}\theta_M \lessgtr g\left(\frac{\alpha_1}{\rho}|M\tau\right)$.

It is not hard to show that $\frac{2\alpha_1}{M} \lessgtr g(\alpha_1|M\tau)$ implies

$$\alpha_1 \lessgtr \frac{M\theta_M}{2}\tau \quad (4.16)$$

for $0 \leq \tau \leq 1$.

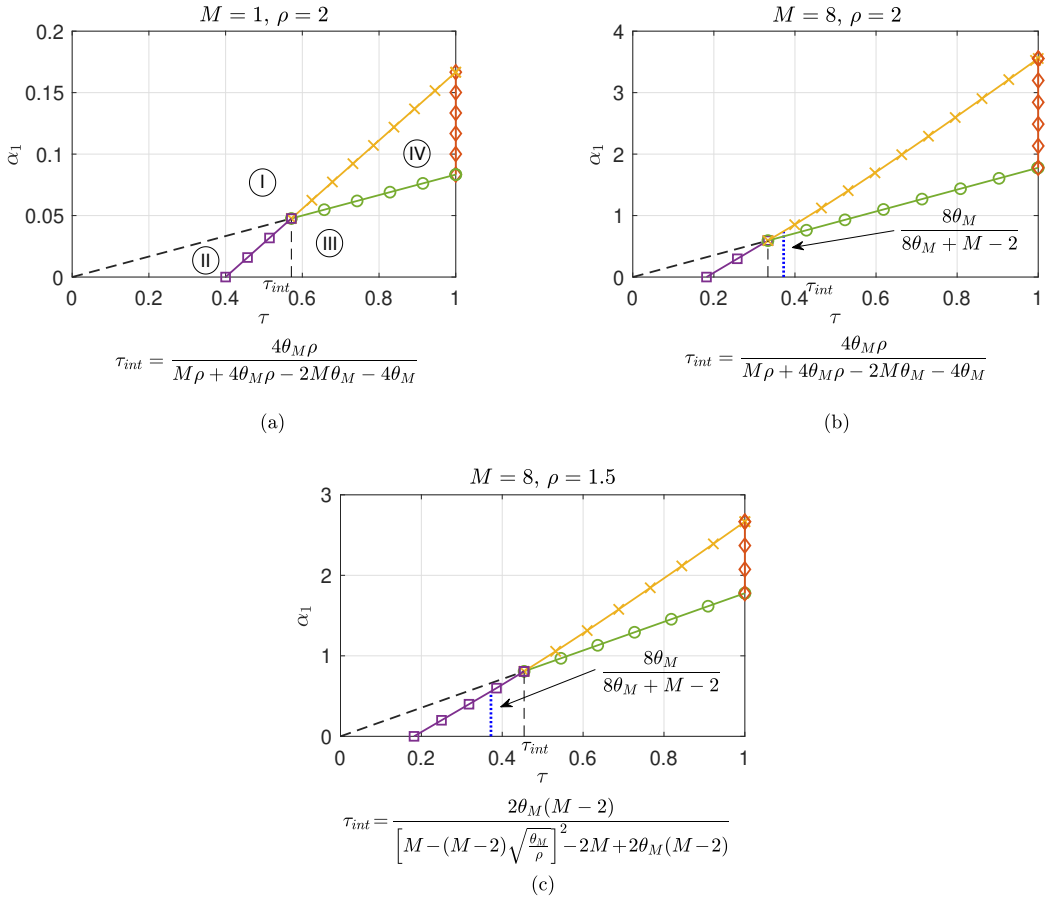

Figure 4.4: All the relevant subregions of (α_1, τ) pairs for the optimal tradeoff of $\left(\beta_{1,M}, \beta_{2,M}\right)$ are shown for the cases (a) $M = 1, \rho = 2$, (b) $M = 8, \rho = 2$, and (c) $M = 8, \rho = 1.5$.

On the other hand, $\frac{2\alpha_1}{M\rho} + \bar{\tau}\theta_M \lessgtr g\left(\frac{\alpha_1}{\rho}|M\tau\right)$ has two possible outcomes. For $M > 2$, it translates after some algebra to

$$\alpha_1 \lessgtr \frac{M\rho}{4(M+2)}\left[(4\theta_M + M)\tau - 4\theta_M\right] \tag{4.17}$$

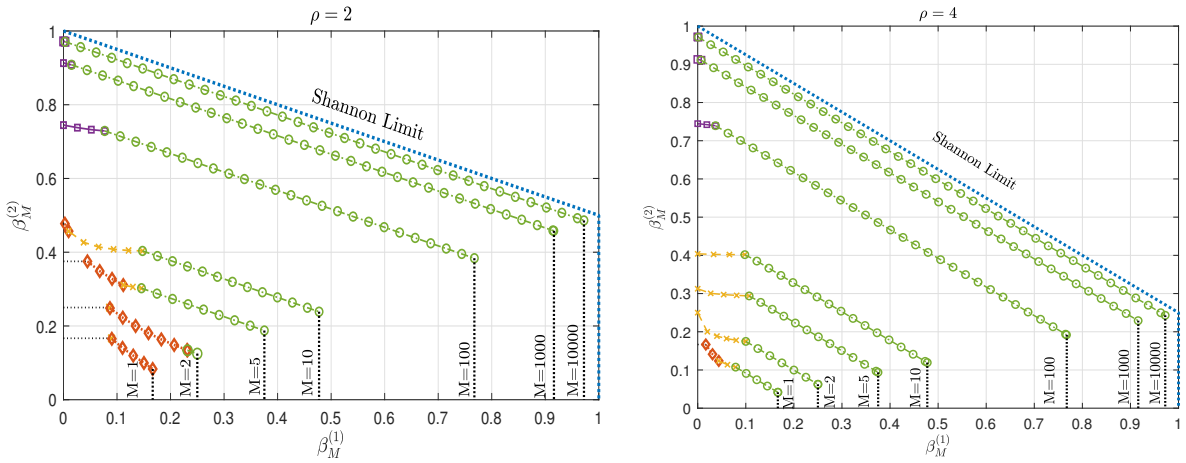

Figure 4.5: How $(\beta_{1,M}, \beta_{2,M})$ tradeoff evolves as M increases. The markers match with those in Figure 4.4 for the optimal (τ, α_1).

for $\frac{4\theta_M}{4\theta_M+M} \leq \tau \leq \frac{8\theta_M}{8\theta_M+M-2}$ and

$$\alpha_1 \leqslant \frac{\rho}{2}\left(\frac{\sqrt{M\tau} - \sqrt{2\tau + 2\theta_M\bar{\tau}\left(1-\frac{2}{M}\right)}}{1-\frac{2}{M}}\right)^2 \tag{4.18}$$

for $\frac{8\theta_M}{8\theta_M+M-2} \leq \tau \leq 1$. But for $M \leq 2$, it translates to (4.17) for the entire interval $\frac{4\theta_M}{4\theta_M+M} \leq \tau \leq 1$.

Now, it can be shown that the conditions (4.16)-(4.18) divides the (α_1, τ)-plane into four regions, as depicted in Figure 4.4a, where the green (circle marker) and purple-yellow (square-cross markers) curves correspond to $\frac{2\alpha_1}{M} = g(\alpha_1|M\tau)$ and $\frac{2\alpha_1}{M\rho} + \bar{\tau}\theta_M = g\left(\frac{\alpha_1}{\rho}|M\tau\right)$, respectively. Furthermore, after some algebra, the intersection of the two curves can be found at $\tau = \tau_{int}$, where

$$\tau_{int} = \frac{4\theta_M\rho}{4\rho\theta_M + M\rho - 2M\theta_M - 4\theta_M}, \tag{4.19}$$

for either $M \leq 2$ and all $\rho > 1$ or $M > 2$ and $\rho \geq 4\theta_M$, and

$$\tau_{int} = \frac{2\theta_M(M-2)}{\left(M-(M-2)\sqrt{\frac{\theta_M}{\rho}}\right)^2 - 2M + 2\theta_M(M-2)}\,, \tag{4.20}$$

for $M > 2$ and $\rho < 4\theta_M$. Note that (4.19) corresponds to the case where the intersection occurs at the linear part of $\frac{2\alpha_1}{M\rho} + \bar{\tau}\theta_M = g\left(\frac{\alpha_1}{\rho}|M\tau\right)$ as governed by (4.17) with equality. This case is exemplified by Figure 4.4(a) and 4.4(b). Similarly, (4.20) corresponds to the case where the intersection occurs in the quadratic part governed by (4.18) with equality, an example of which is shown in Figure 4.4(c).

In light of this division of the (α_1, τ)-plane, we show in the next lemma that the tradeoff of best possible energy-distortion exponents can be computed by focusing on only a limited set of (α_1, τ) pairs.

Lemma 4 *The optimal tradeoff between $\beta_{1,M}(\alpha_1, \tau)$ and $\beta_{2,M}(\alpha_1, \tau)$ is achieved by the collection of (α_1, τ) satisfying one of the following:*

1. $\frac{2\alpha_1}{M} = g(\alpha_1|M\tau)$ *and* $\tau \geq \tau_{int}$
2. $\frac{2\alpha_1}{M\rho} + \bar{\tau}\theta_M = g\left(\frac{\alpha_1}{\rho}|M\tau\right)$
3. $\frac{2\alpha_1}{M} > g(\alpha_1|M\tau), g\left(\frac{\alpha_1}{\rho}|M\tau\right) > \frac{2\alpha_1}{M\rho} + \bar{\tau}\theta_M$, *and* $\tau = 1$.

Proof. We analyze the behavior of $(\beta_{1,M}, \beta_{2,M})$ in each region in Figure 4.4(a) separately:

- Region I: In this region, $\beta_{1,M} = g(\alpha_1|M\tau)$ and $\beta_{2,M} = g\left(\frac{\alpha_1}{\rho}|M\tau\right)$. Since both are increasing in τ, we can improve both $\beta_{1,M}$ and $\beta_{2,M}$ simultaneously by increasing τ, until either $\frac{2\alpha_1}{M} = g(\alpha_1|M\tau)$ or $\frac{2\alpha_1}{M\rho} + \bar{\tau}\theta_M = g\left(\frac{\alpha_1}{\rho}|M\tau\right)$.

- Region II: As one increases τ keeping α_1 constant, $\beta_{1,M} = \frac{2\alpha_1}{M}$ stays the same and $\beta_{2,M} = g\left(\frac{\alpha_1}{\rho}|M\tau\right)$ increases, until $\frac{2\alpha_1}{M\rho} + \bar{\tau}\theta_M = g\left(\frac{\alpha_1}{\rho}|M\tau\right)$.

- Region III: Since $\beta_{1,M} = \frac{2\alpha_1}{M}$ and $\beta_{2,M} = \frac{2\alpha_1}{M\rho} + \bar{\tau}\theta_M$ and both are increasing in α_1, one can improve both $\beta_{1,M}$ and $\beta_{2,M}$ simultaneously by increasing α_1, until either $\frac{2\alpha_1}{M} = g(\alpha_1|M\tau)$ or $\frac{2\alpha_1}{M\rho} + \bar{\tau}\theta_M = g\left(\frac{\alpha_1}{\rho}|M\tau\right)$.

- Region IV: In this region, since $\beta_{1,M} = g(\alpha_1|M\tau)$ is convex in (α_1, τ), its maximum over the line $\beta_{2,M} = \frac{2\alpha_1}{M\rho} - \theta_M\tau = c$ for arbitrary c must be achieved on the boundary of the region, that is, when either $\frac{2\alpha_1}{M} = g(\alpha_1|M\tau)$, or $\frac{2\alpha_1}{M\rho} + \bar{\tau}\theta_M = g\left(\frac{\alpha_1}{\rho}|M\tau\right)$, or $\frac{2\alpha_1}{M} > g(\alpha_1|M\tau), g\left(\frac{\alpha_1}{\rho}|M\tau\right) > \frac{2\alpha_1}{M\rho} + \bar{\tau}\theta_M$, and $\tau = 1$.

■

Remark 3 *The first and the second conditions in Lemma 4 are satisfied when* (4.16) *and* (4.17)-(4.18) *are satisfied with equality, respectively. The third condition translates to*

$$\frac{M\theta_M}{2} < \alpha_1 < \frac{M\theta_M\rho}{2} \tag{4.21}$$

together with $\tau = 1$.

Figure 4.5 shows the resultant $\left(\beta_{1,M}, \beta_{2,M}\right)$ tradeoff computed using Lemma 4 for two sample cases of ρ values as a function of M. Clearly, as $M \to \infty$, the entire region

of Shannon-theoretic exponents derived in [4] is exhausted. The next lemma shows this analytically.

Lemma 5 *As $M \to \infty$, any (β_1, β_2) with $0 \leq \beta_1 \leq 1$ and*

$$\beta_2 = 1 - \beta_1 \left(1 - \frac{1}{\rho}\right) \tag{4.22}$$

can be achieved by the scheme described above.

Proof. Take all (α_1, τ) pairs on the curve $\frac{2\alpha_1}{M} = g(\alpha_1 | M\tau)$, i.e., those satisfying (4.16) with equality. As $M \to \infty$, we have

$$\begin{aligned} \frac{2\alpha_1}{M} = g(\alpha_1|M\tau) &\to \tau \\ \frac{2\alpha_1}{M\rho} + \bar{\tau}\theta_M &\to 1 - \tau\left(1 - \frac{1}{\rho}\right) \\ g\left(\frac{\alpha_1}{\rho}|M\tau\right) &\to \infty \end{aligned}$$

resulting in

$$\begin{aligned} \beta_{1,M} &\to \tau \\ \beta_{2,M} &\to 1 - \tau\left(1 - \frac{1}{\rho}\right) . \end{aligned}$$

for all $0 \leq \tau \leq 1$. ■

4.2 Achievable Dispersion Analysis in Broadcast Channels

In this section, we investigate the more detailed characterization of broadcast channels for zero-delay scenario as in the point-to-point case, which takes the higher order term *energy-distortion dispersion*, i.e. $\nu(\gamma)$, into consideration in the analysis of the energy-distortion tradeoff with 1-to-infinity source-channel mapping, $D_1(\gamma)$, in the form of (3.10), for large γ, where $\Upsilon_1(\gamma)$ is sub-linear in γ, i.e., $\lim_{\gamma\to\infty} \Upsilon_1(\gamma)/\gamma = 0$. It is important to note that analyzing the higher order term in point-to-point case for $M = 1$ has more significance as the optimal exponent is known. However, we provide a way to extend the energy-distortion dispersion analysis to Gaussian broadcast channels, by optimizing the variance of the Gaussian point-density function as in Section 3.2.2.

Distortion expression in (3.14) can be updated for the base layer as follows.

$$\mathbb{D}_1^{(1)}(\gamma_1) \leq e^{-\tau\gamma_1/6}\left[\left(1+\sigma^2\right)\delta c_1 + \frac{\pi\sigma^3}{6c_1^2\sqrt{\sigma^2-2}}\right]$$

which induces the energy-distortion dispersion given by

$$\nu^{(1)}(c,\sigma^2) \geq -\ln\left(\left(1+\sigma^2\right)\delta c_1 + \frac{\pi\sigma^3}{6c_1^2\sqrt{\sigma^2-2}}\right). \tag{4.23}$$

By proceeding with (6.3) for the refinement layer and using σ-optimal approach in Section 3.2.2 amd the results of (3.5),(4.1), (4.2), (2.8), we get

$$\mathbb{D}_1^{(2)}(\gamma_2) \leq \frac{1}{N_1^2N_2^2}d\left(\lambda(x)\right) + \frac{2}{N_1^2}d\left(\lambda(x)\right)P_e\left(N_2,\bar{\tau}\gamma_2\right) + \left(1+\int x^2\lambda(x)dx\right)P_e\left(N_1,\tau\gamma_2\right)$$

$$
\begin{aligned}
&\leq \frac{\exp(-2\alpha_1\gamma_1)\exp(-2\alpha_2\gamma_2)}{c_1^2c_2^2}\cdot\frac{\pi\sigma^3}{6\sqrt{\sigma^2-2}} \\
&\quad+\frac{2\exp(-2\alpha_1\gamma_1)}{c_1^2}\cdot\frac{\pi\sigma^3}{6\sqrt{\sigma^2-2}}\ \delta c_2\exp(\alpha_2\gamma_2)\exp(-\frac{1}{4}\bar{\lambda}\gamma_2) \\
&\quad+\left(1+\sigma^2\right)\delta c_1\exp(\alpha_1\gamma_1)\ exp(-\frac{1}{4}\lambda\gamma_2) \\
&=\exp(-\frac{2}{\rho}\alpha_1\gamma_2)\cdot\frac{\pi\sigma^3}{c_1^26\sqrt{\sigma^2-2}}\left[\frac{\exp(-\frac{1}{6}\bar{\lambda}\gamma_2)}{c_2^2}+2\delta c_2\exp(-\frac{1}{6}\bar{\lambda}\gamma_2)\right] \\
&\quad+\left(1+\sigma^2\right)\delta c_1\exp(\frac{1}{\rho}\alpha_1\gamma_2)\exp(-\frac{1}{4}\lambda\gamma_2) \\
&\leq e^{-\left(\frac{1}{6}\bar{\tau}+\frac{2}{\rho}\alpha_1\right)\gamma_2}\frac{\pi\sigma^3}{6c_1^2\sqrt{\sigma^2-2}}\left[\frac{1}{c_2^2}+2\delta c_2\right]+e^{-\left(\frac{1}{4}\tau-\frac{1}{\rho}\alpha_1\right)\gamma_2}\left(1+\sigma^2\right)\delta c_1\ . \qquad (4.24)
\end{aligned}
$$

For the choice of τ where the energy-distortion exponent tradeoff remains in the *non-degenerate* region, i.e., when $\tau \geq \frac{2\rho}{5\rho-3}$, the first exponent in (4.24) will dominate the expression, thereby setting its coefficient as the dispersion term such that

$$
\nu^{(2)} \geq -\ln\left(\frac{\pi\sigma^3}{6c_1^2\sqrt{\sigma^2-2}}\left[\frac{1}{c_2^2}+2\delta c_2\right]\right)\ , \qquad (4.25)
$$

Clearly, optimization of c_2 yields $c_2=\frac{1}{\sqrt[3]{\delta}}$, and thus

$$
\nu^{(2)}(c,\sigma^2) \geq -\ln\left(\frac{\pi\sigma^3\delta^{2/3}}{2c_1^2\sqrt{\sigma^2-2}}\right)\ . \qquad (4.26)
$$

Figure 4.6 shows the tradeoff between optimal $(\nu_1^{(1)},\nu_1^{(2)})$ pair for Gaussian sources in zero-delay Gaussian broadcast channels. where parameters c_1 and σ^2 are exhaustively searched and found to be $c_1=1.2$ and $\sigma^2=2.41$, respectively.

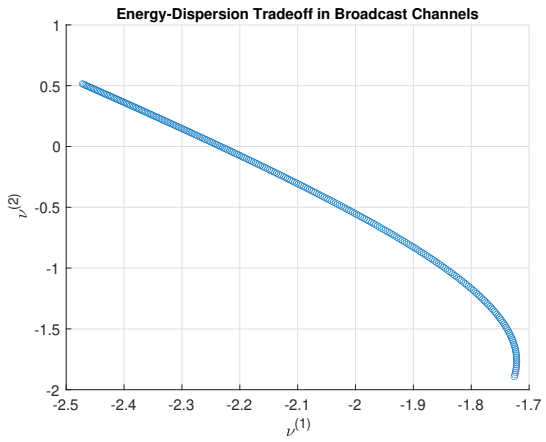

Figure 4.6: Dispersion tradeoff in broadcast channels.

4.3 Conclusion

Motivated by the IoT applications where the source is very slowly varying and therefore sampled very infrequently, we analyzed the exponential decaying speed of the distortion as a function of energy for transmission of M-dimensional i.i.d. Gaussian sources over N-dimensional Gaussian broadcast channels. N is allowed to increase without bound with increasing energy, while M is fixed. The growing of N is necessary for our analysis as we rely on high-resolution quantization theory. But it is also justified by the IoT applications since one would have ample time (and hence bandwidth) to communicate the measurement(s) to the control unit.

While we showed that the resultant achievable exponent region grows with increasing M and converges to the Shannon-theoretic limit at infinite M, it is not clear if there is matching "converse" result for the more interesting case of small M.

Part II

A Privacy-Preserving Voting and Survey Scheme by Using Information Theoretic Approach

Chapter 5

A Privacy-Preserving Voting Scheme

5.1 Introduction

Everyone has right to fair and free elections to determine the elected representatives legitimately in a democratic country. However, the low voter turnout might undermine the true choice of the citizens. In the UK, the voter turnout at the European Union (EU) referendum that resulted in a 51.9% vote for "Brexit" was only 72%. Although this was a record turnout for a UK-wide referendum, this corresponds to approximately 38% of the entire population wanting to leave the EU. Later reports showed that one of the deciding factors in the outcome of the Brexit referendum was a low voter turnout among the young population (18 to 24 year-olds). While there are conflicting reports on the exact turnout

among the young population (38% [1] vs 64% [2]), it is unanimously accepted that the choice of remaining in the EU is high among the young population, with the estimates ranging between $70\% - 75\%$. Coupled with the fact that there is a negative correlation between turnout and average age, the Brexit referendum could have gone much differently with a higher turnout. As another example, in the 2018 midterm US elections, only half of the population eligible to vote actually ended up voting. In the 2020 Presidential Elections, voter turnout was recorded as 66.2% [3]. Similar to the case in the UK, voter turnout among young Americans (18 to 29 year-olds) recorded as 45%, and 53% in 2016 and 2020 presidential elections, respectively[4].

One of the main reasons for the low turnout is often associated with the political apathy among young people. Another prominent reason in the US is that voting is not made easy for everyone, e.g., the election day is not a holiday. Besides, voter suppression on especially minorities and low-income families brings about lower turnout. Moreover, COVID-19 times have brought some other challenges such as following different deadlines for mail-in ballots, keeping safety and social distancing measures in case of long lines, or shortages in poll workers, to name a few. To combat all these challenges, a viable alternative to increase voter participation might be electronic voting, whereby voters can either use their smartphones or their computers at home, or go to public places with computers having access to the Internet (such as schools, libraries, etc.). About 90% of adults in the US had access to the Internet and 81% owned smartphones in 2019, while these numbers increase

[1] `https://www.arcgis.com/apps/Cascade/index.html?appid=b59e96164e6d44578accc378b9574d6f`

[2] https://www.theguardian.com/politics/2016/jul/09/young-people-referendum-turnout-brexit-twice-as-high

[3] `https://en.wikipedia.org/wiki/Voter_turnout_in_United_States_presidential_elections`

[4] https://circle.tufts.edu/latest-research/election-week-2020

to 100% and 96% among the young population, respectively [5] [6]. These increasing statistics in the last decade are making electronic voting a more favorable method. This may also result in increase in young voter turnout, thereby helping their voices to be better heard on issues that matter to them the most, such as student debt, access to healthcare, and the increasing youth unemployment rates.

While an electronic voting system may simplify the whole voting process, the central or governmental unit may be able to track IP addresses of the voters and/or the voter ID. Hence, protecting the privacy of the voters appears as one of the major issues to be resolved. One simple solution can be the randomized response (RR) method that has been suggested in the pioneering work [18] to eliminate self-censorship or bias in responses of a poll by increasing cooperation and trust between interviewees and interviewers. Warner employs an unbiased maximum likelihood estimator and analyzes its variance (i.e., mean square error) as a quality metric. They also compare this mean square error with that of conventional estimates that suffer from response/non-response bias. Further studies that are based on statistics can be also found in [48], [49], and [50].

In this part, we utilize the privacy-preserving voting mechanism that has been proposed in [1]. Unlike the statistical approaches on RR models, this method exploits standard information theoretic tools, such as the method of types and large deviations, in order to analyze the tradeoff between the privacy of the voters and probability that the elections will be accurately called. The voting app on the smartphone or the website randomly flips the votes before transmitting it to the governmental unit. Hence, the actual

[5] https://www.statista.com/statistics/489255/percentage-of-us-smartphone-owners-by-age-group/
[6] https://www.statista.com/statistics/266587/percentage-of-internet-users-by-age-groups-in-the-us/

vote can be treated as an unknown type, and the random alteration of votes can be thought of as a discrete memoryless channel. Each person's vote independently goes through the same random channel, and thus neither an adversarial party nor the government is able to unequivocally resolve what each individual vote was. On the other hand, despite the self-imposed randomness in the system, thanks to the law of large numbers, the election can be more and more accurately called as the number of voters grow. It is also important to note that the system does not generate any delay as the voters (i.e., the source samples) are spread out in space as opposed to time.

We mainly focus on referendums or elections where there are only two options, i.e. YES and NO or Candidate A and B are on the ballot. The votes are passed through a binary symmetric channel and flipping probability of the vote is regarded as the privacy parameter. The 2020 US Presidential Elections are considered as a case study. For simplicity, it will be regarded as an election with only 2 candidates. We analyze the probability of incorrectly calling the result for the US presidential elections, which depends on number of voters and the level of privacy. As the algorithm performs well on the cases where the difference is not close to $50\% - 50\%$, we do not include the analysis of dominantly Red and Blue States, and focus on 9 swing or "close-call" states in which the maximum separation is $47\% - 53\%$, namely: Arizona, Florida, Georgia, Michigan, Nevada, North Carolina, Pennsylvania, Texas, and Wisconsin. Our voting mechanism successfully called the elections for all states with a guaranteed probability of error of 10^{-6} even if the votes are flipped with probability of 30%, except for Arizona, Georgia, and Wisconsin. We can guarantee the same probability of error for only up to 18% flipping ratio for the case of Wisconsin, while the allowable

flipping ratio can only be up to 6% for the case of Arizona and Georgia. Unsurprisingly, the votes had to be re-counted in both states.

5.2 Preliminaries

We will rely heavily on types and their properties. For a detailed discussion on types and their properties, we refer the reader to [51]. We only cover the properties which will prove most useful in the sequel.

For finite alphabets $\mathcal{X}$ and $\mathcal{Y}$, and vectors $\mathbf{x} \in \mathcal{X}^n$ and $\mathbf{y} \in \mathcal{Y}^n$, the *type* of $\mathbf{x}$, denoted $P_{\mathbf{x}}$, and the *conditional type* of $\mathbf{y}$ given $\mathbf{x}$, denoted $V_{\mathbf{y}|\mathbf{x}}$, are defined as probability mass functions satisfying

$$P_{\mathbf{x}}(a) = \frac{1}{n} N(a|\mathbf{x}) \ , \ a \in \mathcal{X}$$

and

$$P_{\mathbf{x}}(a) V_{\mathbf{y}|\mathbf{x}}(b|a) = \frac{1}{n} N(a, b|\mathbf{x}, \mathbf{y}) \ , \ a \in \mathcal{X} \ , \ b \in \mathcal{Y}$$

where $N(a|\mathbf{x})$ is the number of occurrences of the letter $a \in \mathcal{X}$ in $\mathbf{x}$, and similarly $N(a, b|\mathbf{x}, \mathbf{y})$ is the number of occurrences of the pair $(a, b) \in \mathcal{X} \times \mathcal{Y}$ in $(\mathbf{x}, \mathbf{y})$.

The type class P, denoted T_P^n, is defined as

$$T_P^n = \{\mathbf{x} \in \mathcal{X}^n : P_{\mathbf{x}} = P\} \ .$$

For each $\mathbf{x} \in \mathcal{X}^n$, the set of vectors $\mathbf{y}$ having conditional type $V_{\mathbf{y}|\mathbf{x}} = V$ is denoted by $T_V^n(\mathbf{x})$, and is called the *V-shell* of $\mathbf{x}$.

We also denote by $\mathcal{M}(\mathcal{X})$ and $\mathcal{C}(\mathcal{Y}|\mathcal{X})$ the set of all *marginal* probability distributions on $\mathcal{X}$ and the set of all *conditional* distributions from $\mathcal{X}$ to $\mathcal{Y}$, respectively. Finally, we denote by $\mathcal{M}^n(\mathcal{X})$ the set of all valid types (i.e., non-empty type classes) of length-n sequences over $\mathcal{X}$, and by $\mathcal{C}_P^n(\mathcal{Y}|\mathcal{X})$ the set of all valid conditional types (i.e., non-empty V-shells) of length-n sequences over $\mathcal{Y}^n$ given any $\mathbf{x} \in T_P^n$.

Information measures such as entropy, conditional entropy, divergence, and conditional divergence are all defined in the standard way. However, we follow the notation of [51] to emphasize their dependencies on probability mass functions, i.e.,

$$H(P) = -\sum_{a\in\mathcal{X}} P(a)\log P(a) \tag{5.1}$$

$$H(V|P) = -\sum_{a\in\mathcal{X}} P(a)\sum_{b\in\mathcal{Y}} V(b|a)\log V(b|a) \tag{5.2}$$

$$D(P||Q) = \sum_{a\in\mathcal{X}} P(a)\log\frac{P(a)}{Q(a)} \tag{5.3}$$

$$D(V||W|P) = \sum_{a\in\mathcal{X}} P(a)\sum_{b\in\mathcal{Y}} V(b|a)\log\frac{V(b|a)}{W(b|a)} \tag{5.4}$$

where here and in the sequel, we use natural logarithms.

Let $[PV]$ indicate the marginal distribution on $\mathcal{Y}$ given by

$$\sum_{a\in\mathcal{X}} P(a)V(b|a)\ .$$

Observe that if $\mathbf{x} \in T_P^n$ and $\mathbf{y} \in T_V^n(\mathbf{x})$, then $\mathbf{y} \in T_{[PV]}^n$ also.

Property 1 *For any $n \geq 1$, the number of distinct types in $\mathcal{M}^n(\mathcal{X})$ is polynomial in n. More specifically,*

$$|\mathcal{M}^n(\mathcal{X})| \leq (n+1)^{|\mathcal{X}|} . \tag{5.5}$$

Similarly, for any $P \in \mathcal{M}^n(\mathcal{X})$,

$$|\mathcal{C}_P^n(\mathcal{Y}|\mathcal{X})| \leq (n+1)^{|\mathcal{X}|\cdot|\mathcal{Y}|} \tag{5.6}$$

These bounds can be tightened significantly when $|\mathcal{X}| = |\mathcal{Y}| = 2$:

$$|\mathcal{M}^n(\mathcal{X})| = n+1 \tag{5.7}$$

and

$$|\mathcal{C}_P^n(\mathcal{Y}|\mathcal{X})| \leq (\tfrac{n}{2}+1)^2 . \tag{5.8}$$

Property 2 *For any $P \in \mathcal{M}^n(\mathcal{X})$, the size of T_P^n can be bounded as*

$$|T_P^n| \leq e^{nH(P)} . \tag{5.9}$$

Similarly, for any $\mathbf{x} \in T_P^n$, we have

$$|T_V^n(\mathbf{x})| \leq e^{nH(V|P)} . \tag{5.10}$$

Property 3 *If* $\mathbf{X}$ *is generated i.i.d.*$\sim Q \in \mathcal{M}(\mathcal{X})$*, then*

$$\Pr[\mathbf{X} = \mathbf{x}] = e^{-n[H(P_{\mathbf{x}}) + D(P_{\mathbf{x}}||Q)]} \ . \tag{5.11}$$

Similarly, for a given $\mathbf{x} \in \mathcal{X}^n$*, if* $\mathbf{Y}$ *is generated conditionally i.i.d.* $\sim W \in \mathcal{C}(\mathcal{Y}|\mathcal{X})$*, then*

$$\Pr[\mathbf{Y} = \mathbf{y}|\mathbf{X} = \mathbf{x}] = e^{-n\left[H(V_{\mathbf{y}|\mathbf{x}}|P_{\mathbf{x}}) + D(V_{\mathbf{y}|\mathbf{x}}||W|P_{\mathbf{x}})\right]} \ . \tag{5.12}$$

Finally, using the last two properties, we obtain the following.

Property 4 *If* $\mathbf{X}$ *is generated i.i.d.*$\sim Q \in \mathcal{M}(\mathcal{X})$*, then for any* $P \in \mathcal{M}^n(\mathcal{X})$

$$\Pr[\mathbf{X} \in T_P^n] \leq e^{-nD(P||Q)} \ . \tag{5.13}$$

Similarly, for a given $\mathbf{x} \in T_P^n$*, if* $\mathbf{Y}$ *is generated conditionally i.i.d.*$\sim W \in \mathcal{C}(\mathcal{Y}|\mathcal{X})$*, then for any* $V \in \mathcal{C}_P^n(\mathcal{Y}|\mathcal{X})$*,*

$$\Pr[\mathbf{Y} \in T_V^n(\mathbf{x})] \leq e^{-nD(V||W|P)} \ . \tag{5.14}$$

5.3 Privacy-Preserving Voting Mechanism

Let $\mathcal{X}$ be the list of options on a ballot in an election with n voters. For example, $\mathcal{X} = \{\text{Blue Candidate}, \text{Red Candidate}\}$ in the US presidential elections. We define $\mathbf{x} \in \mathcal{X}^n$ as the *vote vector* and $\mathcal{O}_k$, $k = 1, 2$ as the possible *election outcomes*, which partition the space of all possible vote vectors $\mathcal{X}^n$ in a non-overlapping manner.

It is clear that in a fair election (one person one vote), the election outcome should depend on the vote vector $\mathbf{x}$ only through its type. That is, each $\mathcal{O}_k$ must be a union of certain type classes. For example, in the presidential elections, letting $\mathcal{O}_1$ and $\mathcal{O}_2$ represent a vote for Joe Biden (BLUE) and Donald Trump (RED), respectively[7],

$$\mathcal{O}_1 = \bigcup_{P\in\mathcal{M}^n(\mathcal{X}):\, P(\text{BLUE})>P(\text{RED})} T_P^n \tag{5.15}$$

$$\mathcal{O}_2 = \bigcup_{P\in\mathcal{M}^n(\mathcal{X}):\, P(\text{RED})\geq P(\text{BLUE})} T_P^n\,. \tag{5.16}$$

We define $\mathcal{O}(\mathbf{x})$ as the index of the election outcome corresponding to $\mathbf{x}$. That is, $\mathcal{O}(\mathbf{x}) = k$ if and only if $\mathbf{x} \in \mathcal{O}_k$. We also abuse the notation and use $\mathcal{O}(P)$ for the outcome corresponding to the type class T_P^n.

In this paper, we propose a voting mechanism whereby voters indicate their choices on the ballot through some electronic medium, such as a website, or an app on their smartphones. For each voter $1 \leq i \leq n$, the website or app passes their vote $x_i \in \mathcal{X}$ through a binary symmetric channel $W = \text{BSC}(\alpha)$ where some $\alpha < \frac{1}{2}$, with an output alphabet $\mathcal{Y}$ before sending it to the central governmental unit where votes will be counted, i.e., $\mathcal{X} = \mathcal{Y} = \{\text{BLUE}, \text{RED}\}$. Advantages of choosing of a symmetric channel can be listed as follows. Firstly, it allows us to treat BLUE and RED votes equally, thereby controlling privacy with only one parameter, α. Secondly, it induces a tractable error exponent for the further analysis.

Then, the output space $\mathcal{Y}^n$ is also partitioned into decision regions $\mathcal{D}_k$, $k = 1, 2$, and outcome k will be declared if $\mathbf{y} \in \mathcal{D}_k$. To maintain the fairness of the system, the

[7]When there are even number of voters, ties are assumed to be broken in favor of Red Candidate.

decision regions should also be unions of type classes in $\mathcal{M}^n(\mathcal{Y})$. We define $\mathcal{D}(\mathbf{y})$ and $\mathcal{D}(Q)$ for $\mathbf{y} \in \mathcal{Y}^n$ and $Q \in \mathcal{M}^n(\mathcal{Y})$ similarly to $\mathcal{O}(\mathbf{x})$ and $\mathcal{O}(P)$ above. As a result of the symmetry, the decision regions should be in line with the outcome regions given by (5.15) and (5.16), i.e.,

$$\mathcal{D}_1 = \bigcup_{Q \in \mathcal{M}^n(\mathcal{Y}):\, Q(\text{BLUE}) > Q(\text{RED})} T_Q^n \tag{5.17}$$

$$\mathcal{D}_2 = \bigcup_{Q \in \mathcal{M}^n(\mathcal{Y}):\, Q(\text{RED}) \geq Q(\text{BLUE})} T_Q^n \,. \tag{5.18}$$

As was mentioned in the Introduction, this random alteration of the votes will protect the privacy of the voters, as either the government or an adversarial party tapping into the communication will not be able to resolve any individual voter's choice unequivocally (the noisier the channel, the more the uncertainty). At the same time, as we will discuss, the collective election outcome can be more and more accurately estimated by the governmental unit as n increases.

The probability of the occurrence of an erroneous election result is given by

$$P_e(\mathbf{x}) \stackrel{\Delta}{=} \Pr[\mathcal{D}(\mathbf{Y}) \neq \mathcal{O}(\mathbf{x}) | \mathbf{x}] \,.$$

Observe that because both the election outcomes $\mathcal{O}_k$ and decision regions $\mathcal{D}_j$ are unions of type classes, $P_e(\mathbf{x})$ depends on $\mathbf{x}$ only through its type $P_{\mathbf{x}}$. Upper bound on $P_e(\mathbf{x})$ is given by (we refer reader to [1, eq. (13)] for the proof)

$$P_e(\mathbf{x}) \leq e^{-n\left[D(V_n^*(P)||W|P) - \frac{2\log(\frac{n}{2}+1)}{n}\right]} \tag{5.19}$$

where $V_n^*(P)$ is defined as

$$V_n^*(P) = \arg \min_{V \in \mathcal{C}_P^n(\mathcal{Y}|\mathcal{X}):\ \mathcal{D}([PV]) \neq \mathcal{O}(P)} D(V||W|P) \ . \tag{5.20}$$

As can be seen from (5.19), the probability of incorrectly calling the election result vanishes exponentially so long as $D(V_n^*(P)||W|P)$ is bounded away from 0 as $n \to \infty$. The rest of the paper is devoted to evaluating this exponent for the simple referendum elections.

Assume that voters desire that (i) the probability of an erroneous election outcome is upper bounded by δ whenever $p < \frac{1}{2} - \xi$ or $p > \frac{1}{2} + \xi$ for some (ξ, δ) pair, and (ii) their privacy is protected by a BSC with parameter α. In this case, we get [1, eq. (22)]

$$\begin{aligned} D(V_n^*(P)||W|P) &\geq D(V^*(P)||W|P) \\ &= \frac{(1-2\alpha)^2}{2\alpha(1-\alpha)}\xi^2 + \mathcal{O}(\xi^3) \end{aligned} \tag{5.21}$$

for $p = \frac{1}{2} + \xi$.

5.4 A Case Study: US Presidential Elections

This paper focuses on the 2020 US Presidential Elections as a case study for the proposed voting scheme. While several candidates across multiple parties run for elections, as in most democratic systems, the US Presidential Elections typically boil down to a race between two candidates: (i) the strongest candidate of the Republican Party (Red

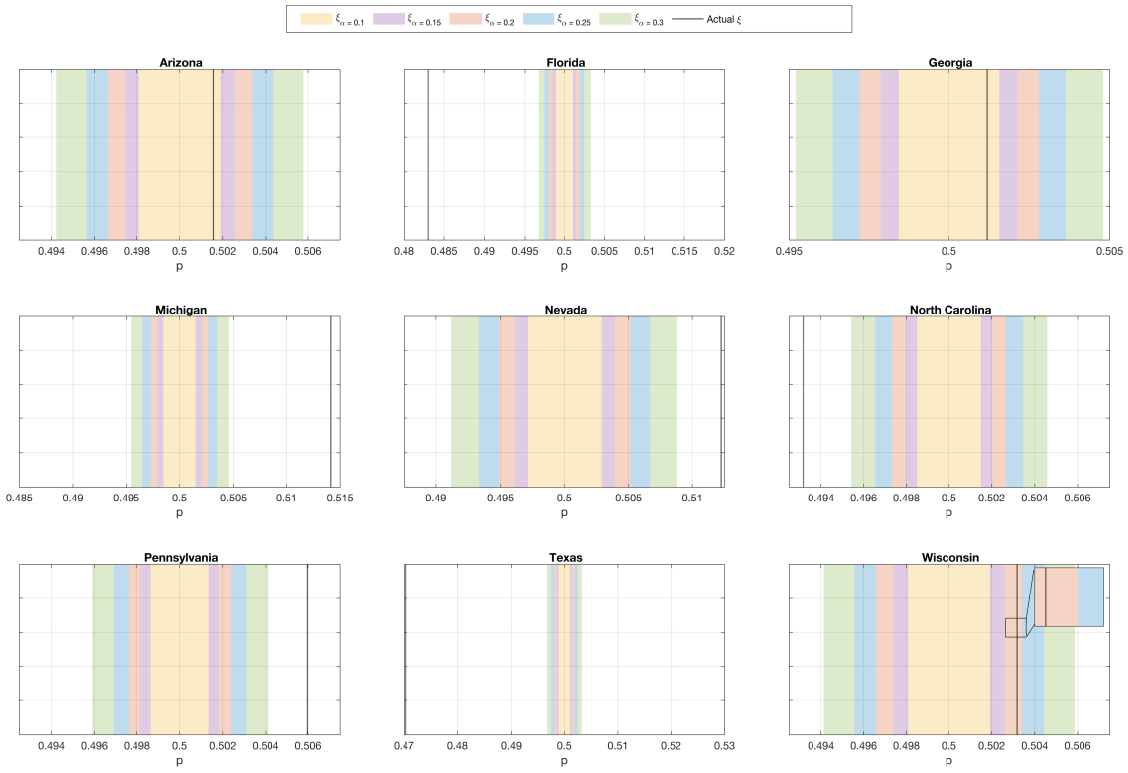

Figure 5.1: The actual ξ of the 2020 US Presidential Elections for each of the 9 swing states and ξ_α, the minimum deviation from the $50\% - 50\%$ threshold above which the δ-bound holds for the proposed voting mechanism. The yellow, purple, orange, blue, and green shaded areas represent the regions of ξ values that correspond to $\alpha = 0.1, \alpha = 0.15, \alpha = 0.2, \alpha = 0.25$, and $\alpha = 0.3$, respectively. Note that each colored region encompasses the colored regions within it. The actual ξ values are shown in black, solid lines.

candidate) and (ii) the strongest candidate of the Democratic Party (Blue candidate). This "tradition" can be traced back to the 1876 US Presidential Elections. However, the number of votes going to the other candidates is non-zero. As such, the percentage of votes for the two main candidates are normalized to sum up to 100%. Moreover, the states that are predominantly Red or Blue are excluded from the analysis, as the algorithm performs well when the margin between the percentage of votes is much larger than $50\% - 50\%$. We pay particular attention to the 9 close-call or "swing" states, namely: Arizona, Florida, Georgia, Michigan, Nevada, North Carolina, Pennsylvania, Texas, and Wisconsin.

The total number of votes for the two main candidates in a state determines the value of n for that particular state. We set a δ-bound on the probability of error, i.e., we upper bound the right-hand side of (5.19) to guarantee that the probability of flipping the final election result is less than a predetermined value δ, which was chosen to be $\delta = 10^{-6}$ for all the states. Next, we calculate ξ_α, the minimum deviation from the $50\% - 50\%$ threshold above which the δ-bound holds, for different flipping probabilities, i.e., $\alpha = 0.1, \alpha = 0.15, \alpha = 0.2, \alpha = 0.25$, and $\alpha = 0.3$. These values of ξ_α are compared to the actual margin of votes from the 2020 US Presidential Elections for the 9 swing states and are shown in Figure 5.1.

The results in Figure 5.1 can be categorized into three. The first category is where the actual ξ is outside all of the ξ_α regions, such as in Florida, Michigan, Nevada, North Carolina, Pennsylvania, and Texas. This indicates that the specified δ-bound will be satisfied for all the specified values of α. The second category is where the actual ξ is inside all of the ξ_α regions, such as in Arizona and Georgia. In such cases, the δ-bound cannot be guaranteed for any of the specified α. The third category is where the ξ is outside some of the ξ_α regions and inside the others, such as in Wisconsin. In this particular case, the δ-bound is satisfied for $\alpha = 0.1$, $\alpha = 0.15$, and $\alpha = 0.2$, but not for $\alpha = 0.25$ or $\alpha = 0.3$. This analysis could also be conducted on past data to predict ξ before an election and select the flipping probability α accordingly. For example, assuming the next election cycle will produce similar ξ values as the 2020 elections, an α of 0.15 (or less) should be used in Wisconsin, whereas an α of 0.3 (or more) could be used in Texas.

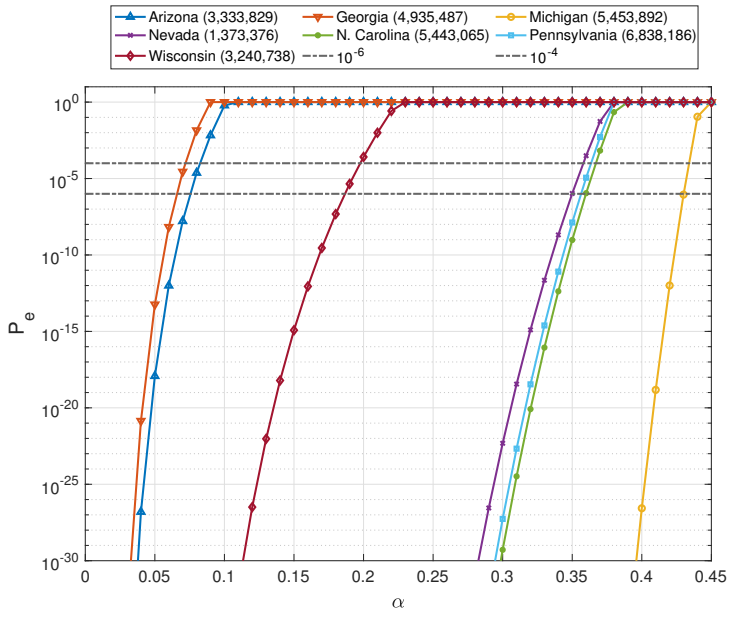

Figure 5.2: Calculated probability of error for different states (n), α values for the corresponding ξ values.

The next natural question that arises is: What is the value of α below which the δ-bound is always guaranteed? To answer this question, the probability of error is calculated using the actual ξ for varying values of α. Figure 5.2 depicts the probability of error for the aforementioned states as a function of α. The 10^{-6} and 10^{-4} δ-bounds are shown for comparison. Note that Texas and Florida were omitted from Figure 5.2 as their error probabilities are too small compared to the rest. The value of α below which the δ-bound is always guaranteed, denoted $\alpha^\star$, can be readily obtained from the intersection of the probability of error curve with the δ-bound. The values of n, actual ξ, and $\alpha^\star$ for the swing states (excluding Texas and Nevada) are summarized in Table 5.1.

Remark 4 *The effect of the total number of votes n can be observed by focusing on Michigan and Nevada. Although the actual ξ are close, i.e.* 1.41356%, 1.22312%, *respectively;*

State	n	Actual ξ	$\alpha^\star$
Arizona	3,333,829	0.0015683	0.0753194
Georgia	4,935,487	0.0011933	0.0656223
Michigan	5,453,892	0.0141356	0.4300946
Nevada	1,373,376	0.0122312	0.3499085
North Carolina	5,443,065	-0.0068418	0.3598532
Pennsylvania	6,838,186	0.0059709	0.3562917
Wisconsin	3,240,738	0.0031795	0.1865765

Table 5.1: The values of n, actual ξ, and $\alpha^\star$ for the swing states (excluding Texas and Nevada).

Michigan ($n = 5,453,892$) achieves a lower probability of error compared to Nevada ($n = 1,373,376$) for the same α (see Figure 5.2. Alternatively, fixing the probability of error yields a significantly larger $\alpha^\star$ for Michigan compared to Nevada (see Table 5.1).

Chapter 6

Modified Privacy-Preserving Voting Scheme

6.1 Introduction

In this section, we utilize a modified version of the privacy-preserving voting mechanism proposed in [1]. Unlike the statistical approaches on RR models, this method exploits information theoretic tools, such as the method of types and large deviations, in order to analyze the tradeoff between the privacy of the voters and the probability that the elections will be correctly called. The voting app on the smartphone or the website randomly flips the votes before transmitting it to the central unit. Hence, the actual vote can be treated as an unknown type, and the random alteration of votes can be thought of as a discrete memoryless channel. Each person's vote independently goes through the same random channel, and thus neither an adversarial party nor the government is able to unequivocally resolve

what each individual vote was. Despite the self-imposed randomness in the system, the election can be more and more accurately called as the number of voters grows thanks to the law of large numbers. It is also important to note that the system does not generate any delay as the voters (i.e., the source samples) are spread out in space as opposed to time. The detection or composite hypothesis testing problem in elections is further extended to the estimation problems in polls or surveys in [52], where a worst-case analysis of the effect of randomization on estimation performance over each possible percentage of YES answers is carried out.

One of the main shortcomings of the approach in [1] was the lack of a feedback system for the cases where the result were very close to $50\% - 50\%$ as the probability of wrongly calling the election was not guaranteed for this vulnerable interval. Introducing a region called "too close to call" allows us to come up with such a feedback system thereby introducing a tradeoff between the probability of wrongly calling the election result and the probability of the too-close-to-call outcome. For the analysis, we mainly focus on referendums or elections where there are only two options, i.e. YES or NO, Candidate A or B, and more specifically the 2020 US Presidential Elections. For simplicity, it will be regarded as an election with only 2 candidates. The votes are passed through a binary symmetric channel and flipping probability of the vote is regarded as the privacy parameter. We analyze the probability of incorrectly calling the result for the 2020 US Presidential Elections, which depends on the number of voters and the flipping probability. Historical data on each state can be utilized to determine the initial flipping probability and the too close to call interval. In a case of too close to call, the election can be repeated with a

lower flipping probability. The probability of correctly calling the elections increases as the election results moves away from the $50\% - 50\%$ interval. For most states, a probability of error as low as 10^{-6} can be guaranteed, even if the votes are flipped with a probability of 0.35 or more. As such, we mainly focus on the more interesting 3 "swing" states in which the maximum separation is $49.4\% - 50.6\%$, namely: Georgia, Arizona, and Pennsylvania. We can guarantee a 10^{-6} probability of error for only up to 0.09, 0.1, and 0.38 flipping probabilities for Georgia, Arizona, and Pennsylvania, respectively. Unsurprisingly, these findings align with the fact that the votes had to be recounted in Georgia and Arizona.

6.2 Proposed Voting Mechanism

Let $\mathcal{X}$ be the list of options on a ballot in an election with n voters. For example, $\mathcal{X} = \{\text{Blue Candidate}, \text{Red Candidate}\}$ in the US presidential elections. We define $\mathbf{x} \in \mathcal{X}^n$ as the *vote vector* and $\mathcal{O}_k$, $k = 1, 2$ as the possible *election outcomes*, which partition the space of all possible vote vectors $\mathcal{X}^n$ in a non-overlapping manner, as in (5.15) and (5.16).

Again, for each voter $1 \leq i \leq n$, the website or app passes their vote $x_i \in \mathcal{X}$ through a binary symmetric channel $W = \text{BSC}(\alpha)$ with some $\alpha < \frac{1}{2}$ and an output alphabet $\mathcal{Y} = \mathcal{X}$, before sending it to the central governmental unit where votes will be counted.

In the new proposed method, the output space $\mathcal{Y}^n$ is partitioned into 3 decision regions $\mathcal{D}_l$, $l = 0, 1, 2$, and outcome l will be declared if $\mathbf{y} \in \mathcal{D}_l$. Here the additional decision region $\mathcal{D}_0$ represents the too-close-to-call outcome, which provides a feedback to the central unit. To maintain the fairness of the system, the decision regions should also be unions of type classes in $\mathcal{M}^n(\mathcal{Y})$. We define $\mathcal{D}(\mathbf{y})$ and $\mathcal{D}(Q)$ for $\mathbf{y} \in \mathcal{Y}^n$ and $Q \in \mathcal{M}^n(\mathcal{Y})$ similarly to

$\mathcal{O}(\mathbf{x})$ and $\mathcal{O}(P)$ above. As a result of the symmetry, the decision regions should be in line with the outcome regions given by (5.15) and (5.16), i.e.,

$$\mathcal{D}_0 = \bigcup_{Q\in\mathcal{M}^n(\mathcal{Y}):\ \frac{1}{2}-\epsilon\le Q(\text{BLUE })\le\frac{1}{2}+\epsilon} T_Q^n \tag{6.1}$$

$$\mathcal{D}_1 = \bigcup_{Q\in\mathcal{M}^n(\mathcal{Y}):\ Q(\text{BLUE})>\frac{1}{2}+\epsilon} T_Q^n \tag{6.2}$$

$$\mathcal{D}_2 = \bigcup_{Q\in\mathcal{M}^n(\mathcal{Y}):\ Q(\text{BLUE })<\frac{1}{2}-\epsilon} T_Q^n \tag{6.3}$$

With the addition of the decision $\mathcal{D}_0$, a new tradeoff is introduced between the probability of declaring an erroneous election result and the probability of the result declared to be too close to call. The probability of the occurrence of an erroneous election result is given by

$$P_e(\mathbf{x}) \stackrel{\Delta}{=} \begin{cases} \Pr[\mathbf{Y}\in\mathcal{D}_2|\mathbf{x}]\ , & \mathbf{x}\in\mathcal{O}_1(\mathbf{x}) \\ \Pr[\mathbf{Y}\in\mathcal{D}_1|\mathbf{x}]\ , & \mathbf{x}\in\mathcal{O}_2(\mathbf{x}) \end{cases}, \tag{6.4}$$

and the probability of calling too close to call is defined by

$$P_t(\mathbf{x}) \stackrel{\Delta}{=} \Pr[(\mathbf{Y})\in\mathcal{D}_0|\mathbf{x}]\ . \tag{6.5}$$

Observe that because both the election outcomes $\mathcal{O}_k$ and decision regions $\mathcal{D}_j$ are unions of type classes, $P_e(\mathbf{x})$ depends on $\mathbf{x}$ only through its type $P_{\mathbf{x}}$. The upper bound on $P_e(\mathbf{x})$ (we refer reader to [1, eq. (13)] for the proof) can be rewritten for the new case as

$$P_e(\mathbf{x}) \le e^{-n\left[D(V_n^*(P)||W|P)-\frac{2\log(\frac{n}{2}+1)}{n}\right]} \tag{6.6}$$

where $V_n^*(P)$ is defined as

$$V_n^*(P) = \arg \min_{V \in \mathcal{C}_P^n(\mathcal{Y}|\mathcal{X}):\ \mathcal{D}([PV])=2} D(V||W|P) \ , \tag{6.7}$$

when $\mathcal{O}(P) = 1$, and

$$V_n^*(P) = \arg \min_{V \in \mathcal{C}_P^n(\mathcal{Y}|\mathcal{X}):\ \mathcal{D}([PV])=1} D(V||W|P) \ , \tag{6.8}$$

when $\mathcal{O}(P) = 2$. Similarly,

$$P_t(\mathbf{x}) \leq e^{-n\left[D(V_{n,0}^*(P)||W|P) - \frac{2\log(\frac{n}{2}+1)}{n}\right]} \tag{6.9}$$

where

$$V_{n,0}^*(P) = \arg \min_{V \in \mathcal{C}_P^n(\mathcal{Y}|\mathcal{X}):\ \mathcal{D}([PV])=0} D(V||W|P) \ . \tag{6.10}$$

As can be seen from (6.6) and (6.9), the probability of incorrectly calling the election result vanishes exponentially so long as $D(V_n^*(P)||W|P)$ and $D(V_{n,0}^*(P)||W|P)$ is bounded away from 0 as $n \to \infty$. By applying the result of [1, eq. (22)], we get

$$\begin{aligned} D(V_n^*(P)||W|P) &\geq D(V^*(P)||W|P) \\ &= \min_{\substack{V \in \mathcal{C}(\mathcal{Y}|\mathcal{X}): \\ V:[PV](\text{BLUE}) \geq \frac{1}{2}+\epsilon}} D_e(V||W|P) \\ &= \min_{\substack{(\beta_1,\beta_2): \\ \beta_1\bar{p}+\bar{\beta}_2 p \geq \frac{1}{2}+\epsilon}} p\left[\beta_2 \log\frac{\beta_2}{\alpha} + \bar{\beta}_2 \log\frac{\bar{\beta}_2}{\bar{\alpha}}\right] \\ &\qquad + \bar{p}\left[\beta_1 \log\frac{\beta_1}{\alpha} + \bar{\beta}_1 \log\frac{\bar{\beta}_1}{\bar{\alpha}}\right] \ , \end{aligned} \tag{6.11}$$

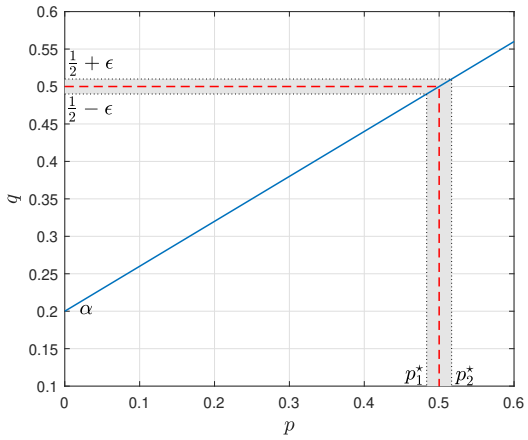

Figure 6.1: Mapping of too close to call interval onto election results.

for $p \leq \frac{1}{2}$. Then [1, Lemma 1] can be adapted to find the minimizing (β_1, β_2) pair (i.e., the V-shell) in (6.11) to satisfy

$$\beta_1 \bar{p} + \bar{\beta}_2 p = \frac{1}{2} + \epsilon \tag{6.12}$$

$$\beta_1 \beta_2 \bar{\alpha}^2 = \bar{\beta}_1 \bar{\beta}_2 \alpha^2 \,. \tag{6.13}$$

Similarly, to find $D(V_n^*(P)||W|P)$ for $p > \frac{1}{2}$, it suffices to replace (6.12) with

$$\beta_1 \bar{p} + \bar{\beta}_2 p = \frac{1}{2} - \epsilon \,. \tag{6.14}$$

For the exponent of the too-close-to-call event $\mathcal{D}_0$, we need to solve the same minimization problem (6.11) defined over the region

$$\frac{1}{2} - \epsilon \leq \beta_1 \bar{p} + \bar{\beta}_2 p \leq \frac{1}{2} + \epsilon \,. \tag{6.15}$$

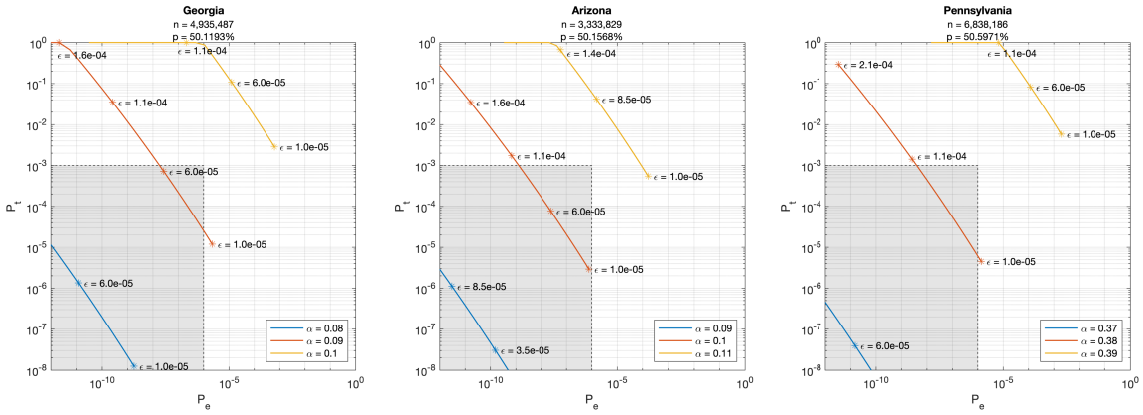

Figure 6.2: P_e - P_t tradeoff of close-call states, namely Georgia, Arizona, Pennsylvania for chosen α flipping probabilities and varying ϵ. Shaded region shows α and ϵ values for the given state that satisfy (δ_e, δ_t) bound on the probability of error and the probability of close-call.

It is not hard to show that in this case, defining

$$p_1^* = \frac{\frac{1}{2} - \epsilon - \alpha}{1 - 2\alpha} \tag{6.16}$$

$$p_2^* = \frac{\frac{1}{2} + \epsilon - \alpha}{1 - 2\alpha}\,, \tag{6.17}$$

the solution is given by $\beta_1 = \beta_2 = \alpha$ whenever

$$p_1^* \leq p \leq p_2^*$$

thereby yielding $D(V_0^*(P)||W|P) = 0$. On the other hand, if $p > p_2^*$, the optimal (β_1, β_2) will be given by (6.12) and (6.13), and similarly if $p < p_1^*$, the optimum pair will be provided by (6.13) and (6.14). For example, for $\epsilon = 0.01$, $\alpha = 0.2$, we get $p_1^* = 0.4833$ and $p_2^* = 0.5167$, as shown in Figure 6.1.

6.3 A Case Study: US Presidential Elections

While several candidates across multiple parties run for elections, as in most democratic systems, the US Presidential Elections typically boil down to a race between two candidates: (i) the strongest candidate of the Republican Party (Red candidate) and (ii) the strongest candidate of the Democratic Party (Blue candidate). This "tradition" can be traced back to the 1876 US Presidential Elections. However, the number of votes going to the other candidates is non-zero. As such, the percentage of votes for the two main candidates are normalized to sum up to 100%. Moreover, the states that are predominantly Red or Blue are excluded from the analysis, as the scheme performs well when the margin between the percentage of votes is much larger than $50\% - 50\%$. We pay particular attention to the 3 close-call or "swing" states, namely: Georgia, Arizona, and Pennsylvania.

6.3.1 Analytical Results

The total number of votes for the two main candidates in a state determines the value of n for that particular state. We set a (δ_e, δ_t) bound on the probability of error and the probability of close-call, i.e., we upper bound the right-hand side of (6.6) and (6.9), respectively, to guarantee that the probability of flipping the final election result is less than a predetermined value (δ_e, δ_t), which were chosen to be $\delta_e = 10^{-6}$ and $\delta_t = 10^{-3}$ for all the states. It is important to note that this value of the (δ_e, δ_t) pair was chosen only for illustrative purposes. The selection of (δ_e, δ_t) remains a topic to be treated in future work. Once the (δ_e, δ_t) pair is set, a natural question arises: What are the (α, ϵ) pairs that guarantee the (δ_e, δ_t)-bounds? To answer this question, the probability of wrongly

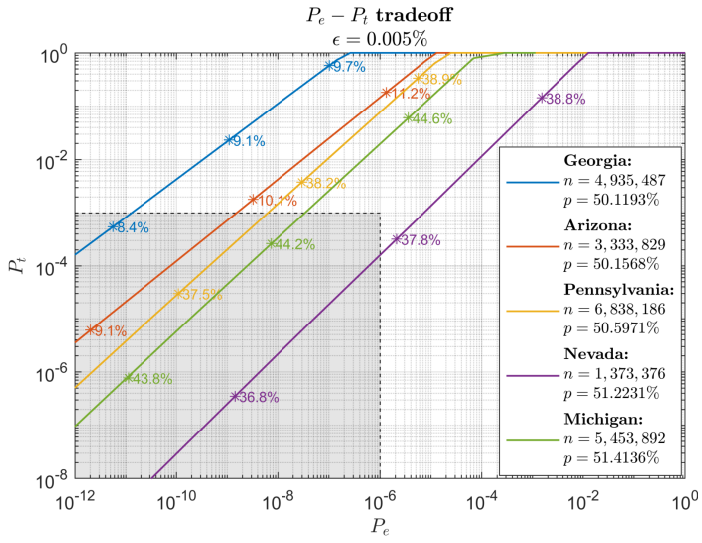

Figure 6.3: P_e - P_t tradeoff for Georgia, Arizona, Pennsylvania, Nevada, and Michigan for $\epsilon = 0.005\%$ and varying α flipping probabilities. Shaded region shows α and ϵ values for the given state that satisfy (δ_e, δ_t) bound on the probability of error and the probability of close-call.

calling the election and the too close to call probability are computed by sweeping over ϵ for different values of α, as shown in Figure 6.2. The region satisfying (δ_e, δ_t)-bound is shaded in gray. It is important to note that decreasing ϵ decreases the probability of a too close to call but increases the error probability. The figure also shows that the α boundary is between 9% and 10% for Georgia, 10% and 11% for Arizona, and 38% and 39% for Pennsylvania.

Another way of visualizing the tradeoff is by sweeping over values of α, as shown in Figure 6.3. In contrast to Figure 6.2, Figure 6.3 shows that decreasing α decreases both the too close to call and error probabilities. As such, one can always select a small enough α that guarantees the (δ_e, δ_t) bounds. This cannot be said about ϵ. Consequently, in the case of a too close event, a good strategy would be to repeat the election with a smaller α.

Remark 5 *The effect of the total number of votes n can be observed by focusing on Michigan and Nevada. Although the actual p are close, i.e.* 51.41356%, 51.22312%, *respectively; Michigan ($n = 5,453,892$) achieves a lower probability of error compared to Nevada ($n = 1,373,376$) for the same α (see Figure 6.3) since Michigan has almost 4 times as many voters as Nevada. Another example showing the effect of n is the fact that Pennsylvania can tolerate a slightly higher privacy parameter than Nevada even though its p is much closer to 50%.*

6.3.2 Monte Carlo Simulations

Another way to validate the voting scheme is through Monte Carlo simulations. One way to simulate a BSC in the voting context is using the binomial distribution. Given the number of total numbers of YES and NO votes, denoted by n_{Y} and n_{N}, respectively, the number of flipped YES and NO answers can be modeled as a binomial random variables. Let $n_{\mathrm{Y}\to\mathrm{N}}$ and $n_{\mathrm{N}\to\mathrm{Y}}$ denote the number of flipped YES and NO answers, respectively. Then, $n_{\mathrm{Y}\to\mathrm{N}}$ will be a binomial random variable with parameters n_{Y} and α, and $n_{\mathrm{N}\to\mathrm{Y}}$ will be a binomial random variable with parameters n_{N} and α. To evaluate error probabilities of 10^{-6}, at least 10^8 realizations must be simulated. It is found impractical to simulate 10^8 or more binomial realizations. As an example, it takes about one hour to generate 10^8 realizations with parameters $n = 250$ and $\alpha = 0.1$. Recall that the voting populations in the U.S. Presidential Elections average to millions of voters in each state. As such, going from $n = 250$ to $n = 2,000,000$ would require days. Since this number cannot be computed precisely, the runtime to generate 5000 binomial realizations with parameters n and $\alpha = 0.1$ is shown as a function of n in Figure 6.4. Note that the hyper-linear growth

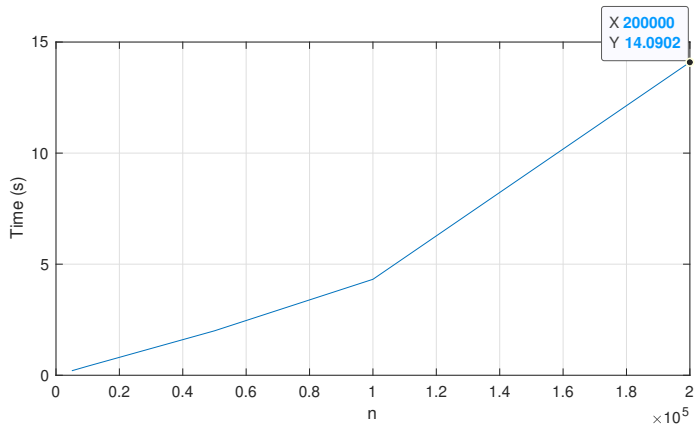

Figure 6.4: Runtime to generate 5000 binomial realizations with parameters n and $\alpha = 0.1$ is shown as a function of n.

of the runtime as a function of n is attributed to the combinatorial nature of generating a binomial random variable. From Figure 6.4, it is predicted that generating 10^8 realizations of binomial random variables with parameters $n = 2,500,000$ and $\alpha = 0.1$ would take about 41 days (the probability α does not affect runtime). That is, each point in Figure 6.3 would require $41 \times 2 = 82$ days to reproduce using Monte Carlo simulations, which in turns means that the plots in Figure 6.3 would require a little less than 17 years to simulate. Instead, the Gaussian approximation of the binomial distribution with a large n is used.

More formally, let $n_{\mathrm{Y}\to\mathrm{N}}$ denote the number of YES votes that flipped to NO votes and $n_{\mathrm{N}\to\mathrm{Y}}$ the number of NO votes that flipped to YES votes. The variable $n_{\mathrm{Y}\to\mathrm{N}}$ can be modeled as a binomial random variable with sample size n_{Y} (commonly known as number of trials) and a flipping probability of α (the complement of the commonly known success probability). For large values of n, we can utilize the central limit theorem to represent the sampling distribution of the sample as a Gaussian distribution. Generally speaking, a binomial random variable X with number of trials n and success probability p can be

approximated as a Gaussian random variable with mean μ and variance σ^2 given by

$$\mu(\mathrm{Y}) = np$$

$$\sigma(\mathrm{Y}) = \sqrt{np\bar{p}}\,.$$

where $\bar{p} = 1 - p$. Using this approximation, $n_{\mathrm{Y}\to\mathrm{N}}$ and $n_{\mathrm{N}\to\mathrm{Y}}$ will be distributed according to

$$n_{\mathrm{Y}\to\mathrm{N}} \sim \mathcal{N}\left(\alpha n_{\mathrm{Y}}, \alpha(1-\alpha)n_{\mathrm{Y}}\right),$$

$$n_{\mathrm{N}\to\mathrm{Y}} \sim \mathcal{N}\left(\alpha n_{\mathrm{N}}, \alpha(1-\alpha)n_{\mathrm{N}}\right).$$

Consequently, the Monte Carlo simulations are realized by drawing from Gaussian distributions with the aforementioned parameters. After flipping, the total number of YES votes will be

$$\bar{n}_{\mathrm{Y}} = (n_{\mathrm{Y}} - n_{\mathrm{Y}\to\mathrm{N}}) + n_{\mathrm{N}\to\mathrm{Y}},$$

and the total number NO votes will be

$$\bar{n}_{\mathrm{N}} = (n_{\mathrm{N}} - n_{\mathrm{N}\to\mathrm{Y}}) + n_{\mathrm{Y}\to\mathrm{N}}.$$

The measured fraction of YES votes is given by

$$q \triangleq \frac{\bar{n}_{\mathrm{Y}}}{n}.$$

In each realization, if $|q - \frac{1}{2}| < \epsilon$, then the number of too close to call events is incremented by one. Otherwise, if $q > \frac{1}{2} + \epsilon$, successful detection is declared. If $q < \frac{1}{2} - \epsilon$, then a missed detection is declared. The probability P_t is calculated by normalizing the number of too to close events by the total number of realizations, and the probability P_e is calculated by the normalizing the number of missed detections by the number of non too close to call events.

Two sets of simulations were conducted to study the P_e - P_t tradeoff: (i) a set where ϵ was swept in the range 0.0001% to 0.04% for varying values of α and (ii) a set where ϵ was fixed to 0.005% and α was swept between 0.125 and 0.475. The number of realizations in the first set of simulations varied from 2×10^9 to 10^{10}. The results for the first set of simulations are shown in Figure 6.5. A total of 10^9 Monte Carlo realizations were conducted for the second simulation set. The results for the second set of simulations are shown in Figure 6.6.

The following can be concluded from Figure 6.5. First, similar to the previous analytical results, it is important to note that decreasing ϵ decreases the probability of a too close to call but increases the error probability. Second, the figure also shows that the α boundary is between 18% and 21% for Georgia, 19% and 22% for Arizona, 43% and 44% for Pennsylvania, and 43% and 44% for Nevada as well. Note that the boundaries for Georgia and Arizona are almost double the ones obtained theoretically in Section 6.3.1. That is because as p gets closer to 50%, the bound becomes more conservative. The bound yields a more conservative boundary for Pennsylvania as well.

The main takeaways from Figure 6.6 are as follow. First, similar to the first set of simulations, the Monte Carlo results show much smaller P_t and P_e probabilities due to the

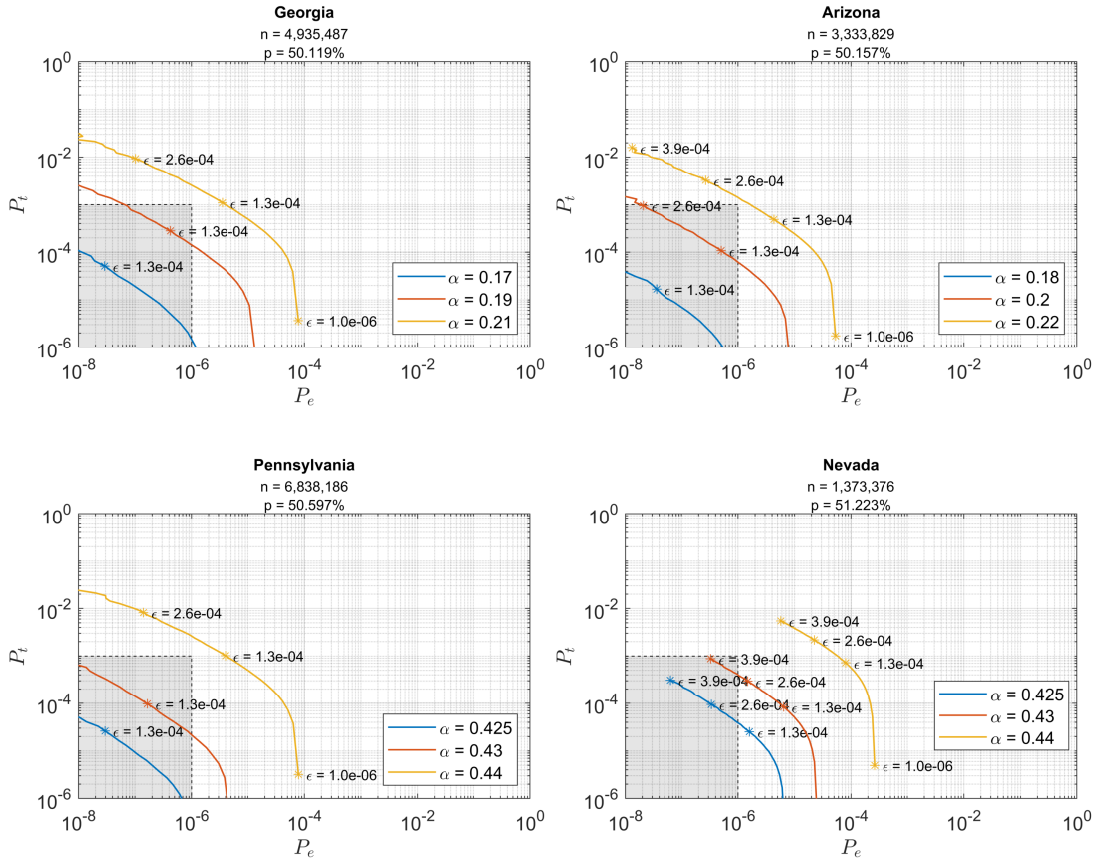

Figure 6.5: Monte Carlo results for the first set of simulations, showing P_e - P_t tradeoff for Georgia, Arizona, Pennsylvania, and Nevada for ϵ sweeping the range 0.0001% to 0.04% and varying values of α. Similar to the plots above, the shaded region shows α and ϵ values for the given state that satisfy (δ_e, δ_t) bound on the probability of error and the probability of close-call. The number of realizations varied from 2×10^9 to 10^{10}.

conservative bounds. Second, the order of the P_e-P_t curves are mostly preserved except for Pennsylvania. This is because the range of α has changed from Figure 6.3. However, the P_e-P_t curve for Pennsylvania remains below that of Georgia and Arizona for all α values. To better see that, P_e and P_t are plotted separately as functions of α in Figure 6.7, which validates that the P_e-P_t curve for Pennsylvania remain below that of Georgia and Arizona, as expected.

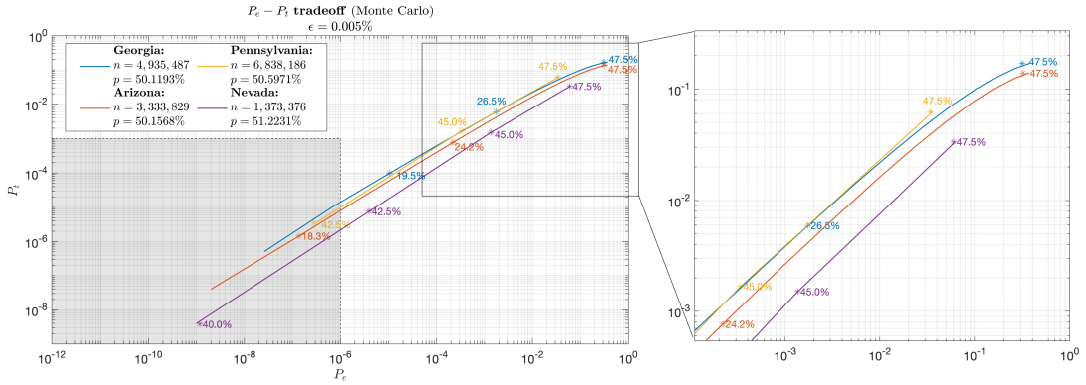

Figure 6.6: Monte Carlo results for the second set of simulations, showing P_e - P_t tradeoff for Georgia, Arizona, Pennsylvania, and Nevada for $\epsilon = 0.005\%$ and α sweeping the range 0.125 and 0.475. Similar to the plots above, the shaded region shows α and ϵ values for the given state that satisfy (δ_e, δ_t) bound on the probability of error and the probability of close-call. A total of 10^9 Monte Carlo realizations were conducted.

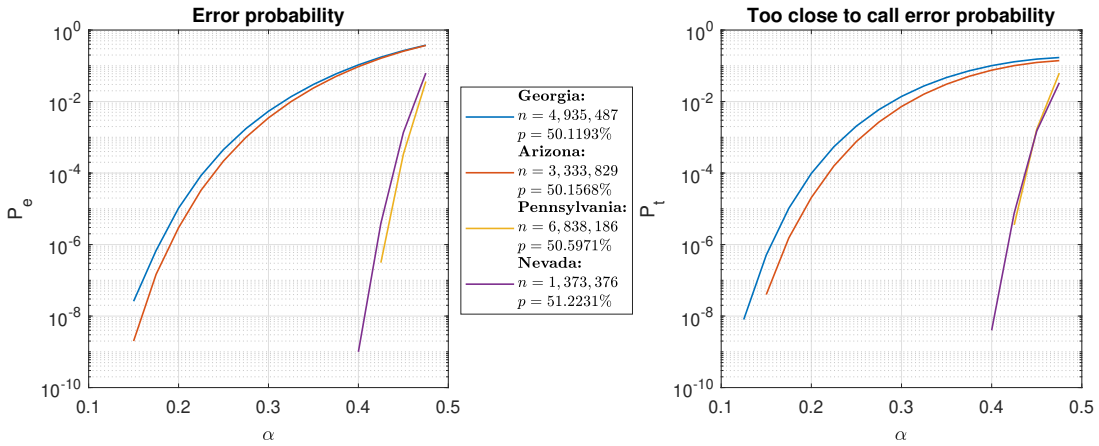

Figure 6.7: Monte Carlo results for the second set of simulations, showing P_e as a function of α, P_t as a function α for Georgia, Arizona, Pennsylvania, and Nevada for $\epsilon = 0.005\%$. A total of 10^9 Monte Carlo realizations were conducted.

6.4 Conclusion

Electronic voting will become prevalent with the widespread use of personal devices. To protect the privacy of voters, a voting mechanism was put forth by [1] that

randomly flips the vote of users to preserve their privacy. This paper extends the voting scheme in [1] by adding a third outcome referred to as "too close to call" for the cases were the election result is very close to $50\% - 50\%$. This outcome guarantees that the desired probability of calling the wrong election result is satisfied . The too close to call outcome is used as feedback system to change the privacy parameter to guarantee a certain probability of wrongly calling the election. This new outcome naturally introduces a tradeoff between the probability of wrongly calling the election result and the probability of falling into the too close to call region. This paper analyzed the aforementioned tradeoff using the 2020 US Presidential Elections as a case study.

Chapter 7

Information Theoretic Approach on Randomized Response Models in Surveys

7.1 Introduction

Survey biases can appear in different forms such as sampling bias, non-response bias, response bias, and question order bias. Non-response or response bias especially may occur when interviewees are asked questions on sensitive topics to which interviewees may self-censor their response or hesitate to answer altogether to avoid social undesirability and feeling of self-embarrassment, or simply to preserve their privacy. The research in [53] exhibited that misreporting is widespread when the survey includes sensitive topics. In [54], similar findings were observed in more autocratic countries when interviewees were asked questions regarding the citizen-state relationship with the fear of the government.

Two very prominent examples of this phenomenon are possibly the US presidential elections in 2016 and 2020. It is widely hypothesized that "shy" Trump voters swayed the polls, which respectively showed Clinton and Biden ahead by a large margin of points in many swing states, whereas the results were either in Trump's favor or the margin was much smaller. Surveys around the COVID-19 pandemic are also very likely to suffer from this bias. For example, if participants are asked about whether they think vaccines are safe, or whether they will take the vaccine, they might shy away from telling the truth.

The randomized response (RR) method has been suggested to eliminate the bias in responses in the pioneering work [18] by increasing cooperation and trust between interviewees and interviewers. The author in [18] utilizes an unbiased maximum likelihood estimator and analyzes its variance (i.e., mean square error) as a quality metric. They also compare this mean square error with that of conventional estimates that suffer from response/non-response bias. Further studies that are based on statistics can be also found in [48], [49], [50].

In this paper, we take an information theoretic approach on the RR model for surveys which require YES/NO responses to increase cooperation and privacy that can help reduce bias. Our work differs from the aforementioned literature in that instead of the mean square error of the randomized estimate, we target the probability of deviation of the estimate of percentage of YES answers from its true value by more than a small, acceptable margin.

In a related previous work [1], a referendum scenario in which the votes are randomized by passing them through a binary symmetric channel (BSC) was studied. It was

shown that the exponent of the probability of incorrectly calling the election can be well-approximated to be proportional to the square of how far the true vote is from $50\% - 50\%$. This result was then leveraged to understand the interplay between number of voters, the allowed probability of incorrectly calling the election, and the level of privacy (i.e., amount of randomization). As was noted in [1], the randomized response setup creates a unique opportunity to utilize standard information theoretic tools, such as the method of types and large deviations, to estimate relevant probabilities. The actual collective survey response can be treated as an unknown *type*, and the randomization of responses can be thought of as a *discrete memoryless channel*. Moreover, in contrast with a typical communication scenario, since the participants of the survey are distributed in space as opposed to time, and since there is no "channel coding", the system incurs neither delay nor complexity, thereby making the analysis applicable in a real-world scenario.

Two important differences between our work and [1] are i) the problem addressed here is that of estimation and not detection, and ii) we leave no "vulnerable" interval in the true percentage of YES answers where no guarantees can be made. Indeed, the problem in [1] was that of composite hypothesis testing (Were YES votes more than NO votes?) and the probability of misdetection was not guaranteed to be small enough when the true results are very close to $50\% - 50\%$. In contrast, we conduct a worst-case analysis of the effect of randomization on estimation performance over each possible percentage of YES answers.

Our analysis shows that with as little as $100,000$ participants, the probability of the estimate of the percentage of YES answers deviating from its true value by more than

$\pm 1\%$ is *at worst* about 2×10^{-6} when the answers are passed through a BSC with a flip probability of 0.1. If the flip probability is increased to about 0.3, the same performance can be achieved with $1,000,000$ participants. While in the old days enrolling a million participants into a survey would be practically impossible, with the advent of smart phones and with the guarantee of this much privacy, the scenario becomes much less far-fetched.

7.2 Proposed Survey Mechanism and Analysis of Error Exponents

Let $\mathcal{X}$ be the list of options on a question in a poll or survey with n participants. We define $\mathbf{x} \in \mathcal{X}^n$ as the *response vector*. It is clear that in a fair questionnaire (one person one response), the poll outcome should depend on the response vector $\mathbf{x}$ only through its type $P_{\mathbf{x}}$.

In this paper, we propose a survey mechanism whereby participants indicate their responses through some electronic medium, such as a website, or an app on their smartphones. For each participant $1 \leq i \leq n$, the website or app passes their choice $x_i \in \mathcal{X}$ through a discrete random channel W with an output alphabet $\mathcal{Y}$ before sending it to the central unit (or a survey master) where survey results will be processed. As was mentioned in the Introduction, this randomization will protect the privacy of the voters, as either the surveying agency or any adversarial party tapping into the communication will not be able to resolve any individual participant's choice unequivocally (the noisier the channel, the more the uncertainty).

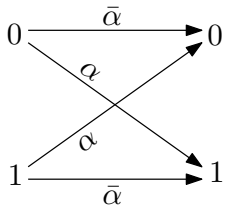

Figure 7.1: Channel $W(y|x)$ randomizing the response.

We will be focusing on simple polls with $\mathcal{X} = \{\text{YES}, \text{NO}\}$ and binary symmetric channels with flip probability $\alpha < \frac{1}{2}$ for randomization, as shown in Figure 7.1 (where we use the notation $\bar{s} = 1 - s$ for any $0 \leq s \leq 1$). As Warner [18] originally proposed, this randomization can alternatively be achieved by tossing an (unfair) coin for each participant and asking them the opposite question whenever the outcome is heads (i.e., with probability α). At the receiving end, the survey master would be oblivious to whether the original or the opposite question is asked for any given user. (They will only know whether they received a YES or a NO answer.)

Upon receiving the randomized response vector $\mathbf{y} \in \mathcal{Y}^n$, the survey master is to estimate $P_{\mathbf{x}}$. Equivalently, given that $\mathcal{X} = \{\text{YES}, \text{NO}\}$, we can denote

$$p = P_{\mathbf{x}}(\text{YES})$$

and reduce the problem to estimation of p. To maintain the fairness of the system, the estimate $\hat{p}$ should depend on $\mathbf{y}$ only through its type $P_{\mathbf{y}}$. Therefore, we will interchangeably use $\hat{p}$, $\hat{p}(\mathbf{y})$, $\hat{p}(P_{\mathbf{y}})$, or even $\hat{p}(P_{\mathbf{y}}(\text{YES}))$ depending on the context.

Note that this is a non-Bayesian estimation problem, in that by the nature of surveying the public for an unknown opinion or a trait, one cannot incorporate any information about the *prior* distribution of p. In non-Bayesian estimation, traditionally one would seek

unbiased estimators with minimum variance (or mean-square error), as Warner [18] did. That is, ensure

$$\mathbb{E}[\hat{p}] = p$$

and minimize

$$\mathbb{E}[(\hat{p} - p)^2]$$

simultaneously for all $0 \leq p \leq 1$ if possible. The reader is referred to [55] for a comprehensive treatment of non-Bayesian estimation.

Here, we take a different, large-deviations approach and strive to minimize

$$P_e \stackrel{\Delta}{=} \max_{0 \leq p \leq 1} \Pr[|\hat{p} - p| > \epsilon] \,, \tag{7.1}$$

i.e, the worst-case probability that the estimate $\hat{p}$ deviates from the true value p by more than $\epsilon > 0$. To analyze this probability, for any $\mathbf{x}$ with $p = P_{\mathbf{x}}(\text{YES})$, we write

$$\begin{aligned}
P_e(\mathbf{x}) &= \sum_{\mathbf{y}: |\hat{p}(\mathbf{y}) - p| > \epsilon} \Pr[\mathbf{Y} = \mathbf{y} | \mathbf{x}] \\
&= \sum_{V \in \mathcal{C}_P^n(\mathcal{Y}|\mathcal{X}):\ |\hat{p}([PV]) - p| > \epsilon} \Pr[\mathbf{Y} \in T_V^n(\mathbf{x}) | \mathbf{x}] \\
&\stackrel{(a)}{\leq} \sum_{V \in \mathcal{C}_P^n(\mathcal{Y}|\mathcal{X}):\ |\hat{p}([PV]) - p| > \epsilon} e^{-nD(V||W|P)} \\
&\stackrel{(b)}{\leq} |\mathcal{C}_P^n(\mathcal{Y}|\mathcal{X})| e^{-nD(V_n^*(P)||W|P)} \\
&\stackrel{(c)}{\leq} \left(\frac{n}{2} + 1\right)^2 e^{-nD(V_n^*(P)||W|P)}
\end{aligned} \tag{7.2}$$

where in (a), we used Property 4, in (b) the fact that there are only polynomially many

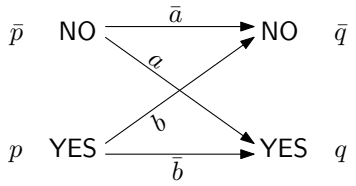

Figure 7.2: V-shell as a binary channel

conditional types, and in (c) Equation (5.8). Here, $V_n^*(P)$ is defined as

$$V_n^*(P) = \arg \min_{\substack{V \in \mathcal{C}_P^n(\mathcal{Y}|\mathcal{X}) : \\ |\hat{p}([PV]) - p| > \epsilon}} D(V||W|P) \; . \tag{7.3}$$

We next tackle the minimization in (7.3). One can treat a V-shell as a fictitious (and generally asymmetric) binary channel as shown in Figure 7.2, where

$$q = [PV](\text{YES}) \; .$$

Now,

$$\begin{aligned} \min_{\substack{V \in \mathcal{C}_P^n(\mathcal{Y}|\mathcal{X}) : \\ |\hat{p}([PV]) - p| > \epsilon}} D(V||W|P) &= \min_{\substack{Q \in \mathcal{M}^n(\mathcal{X}) : \\ |\hat{p}(Q) - p| > \epsilon}} \; \min_{\substack{V \in \mathcal{C}_P^n(\mathcal{Y}|\mathcal{X}) : \\ Q = [PV]}} D(V||W|P) \\ &\geq \min_{\substack{0 \leq q \leq 1 : \\ |\hat{p}(q) - p| \geq \epsilon}} \; \min_{\substack{0 \leq a, b \leq 1 : \\ q = \bar{p}a + p\bar{b}}} pD(b||\alpha) + \bar{p}D(a||\alpha) \end{aligned} \tag{7.4}$$

with the abuse of notation

$$D(s||t) = s \log \frac{s}{t} + \bar{s} \log \frac{\bar{s}}{\bar{t}}$$

for any $0 \leq s, t \leq 1$. Here, we take the standard approach of setting $0 \log 0 = 0$.

Bringing together (7.1)-(7.4), we can write for each estimator $\hat{p}(q)$

$$P_e \leq \left(\frac{n}{2}+1\right)^2 e^{-nD^*(\hat{p})} \tag{7.5}$$

with

$$D^*(\hat{p}) \stackrel{\Delta}{=} \min_{0\leq p\leq 1} \min_{\substack{0\leq q\leq 1: \\ |\hat{p}(q)-p|\geq\epsilon}} \min_{\substack{0\leq a,b\leq 1: \\ q=\bar{p}a+p\bar{b}}} pD(b||\alpha)+\bar{p}D(a||\alpha)\ . \tag{7.6}$$

7.3 Maximum Likelihood Estimator and Its Performance

Stemming from (7.5), it is desirable to find the estimator $\hat{p}(q)$ that would maximize $D^*(\hat{p})$ over all possible estimators for fixed α and ϵ. While it is not easy to solve this maximization problem, here we analyze $D^*(\hat{p})$ for the maximum likelihood estimator

$$\hat{p}(q) = \begin{cases} \frac{q-\alpha}{1-2\alpha} & \alpha \leq q \leq 1-\alpha \\ 0 & q<\alpha \\ 1 & q>1-\alpha \end{cases} \tag{7.7}$$

which is shown in Figure 7.3.[1]

The following lemma proves that for this $\hat{p}(q)$, the solution of the inner two minimizations in (7.6) reduces to solving a quadratic equation.

[1] This is the estimator analyzed in Warner [18] as well, and indeed maximizes the likelihood of observing type Q given that the true response has type P.

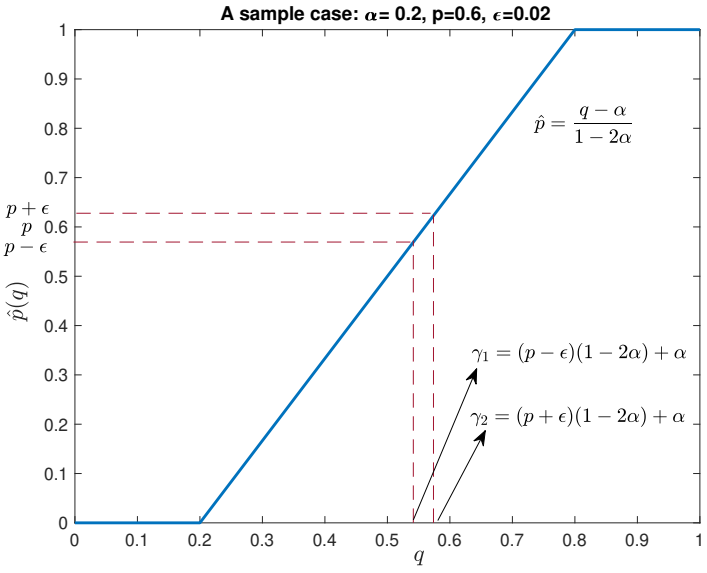

Figure 7.3: The estimator $\hat{p}(q)$ and the behavior of $|\hat{p}(q) - p| > \epsilon$

Lemma 6 *Define*

$$\gamma_1 = (p-\epsilon)(1-2\alpha)+\alpha$$

$$\gamma_2 = (p+\epsilon)(1-2\alpha)+\alpha\ .$$

Then for the estimator $\hat{p}(q)$ *in* (7.7)*, the solution to*

$$D^*(\hat{p}|p) \stackrel{\Delta}{=} \min_{\substack{0\le q\le 1:\\ |\hat{p}(q)-p|\ge\epsilon}} \ \min_{\substack{0\le a,b\le 1:\\ q=\bar{p}a+p\bar{b}}} pD(b||\alpha)+\bar{p}D(a||\alpha)$$

is given by the pair $0 \le a, b \le 1$ *satisfying*

$$ab\bar{\alpha}^2 = \bar{a}\bar{b}\alpha^2 \tag{7.9}$$

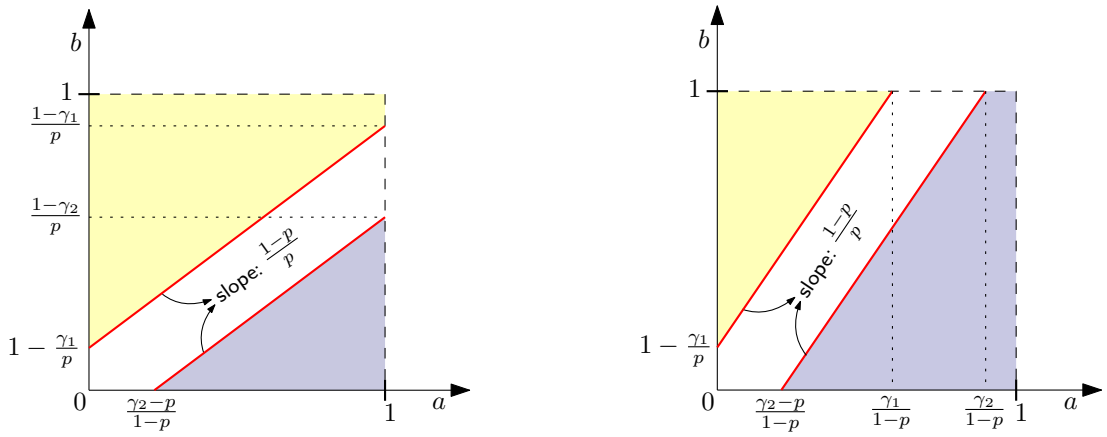

Figure 7.4: Admissible (a, b) pairs, depending on whether $\frac{\bar{p}}{p}$ is less than or greater than 1.

and

$$b = \frac{\bar{p}}{p}a + 1 - \frac{\gamma_i}{p} \tag{7.10}$$

simultaneously, for either $i = 1$ or $i = 2$, whichever yields a lower divergence.

Proof. First observe that the objective function is convex in (a, b). The gradient vector of the objective function for a fixed (p, q) yields

$$\nabla\Big[pD(b||\alpha) + \bar{p}D(a||\alpha)\Big] = \begin{bmatrix} \bar{p}\log\frac{a\bar{\alpha}}{\bar{a}\alpha} \\ \\ p\log\frac{b\bar{\alpha}}{\bar{b}\alpha} \end{bmatrix} \tag{7.11}$$

As demonstrated in Figure 7.3, $q < \gamma_1$ and $q > \gamma_2$ represent admissible values for the outer minimization. Translating this, together with $q = \bar{p}a + p\bar{b}$, into admissible (a, b) pairs, we obtain

$$b \geq \frac{\bar{p}}{p}a + 1 - \frac{\gamma_1}{p}\ , \tag{7.12}$$

and

$$b \leq \frac{\bar{p}}{p}a + 1 - \frac{\gamma_2}{p} \ . \tag{7.13}$$

This results in two possible scenarios in the a-b plane depending on the value of slope $\frac{\bar{p}}{p}$, which are illustrated in Figure 7.4. The optimum (a, b) must lie on one of the following:

(i) Boundaries defined by $a = 0$, $b = 0$, $a = 1$, $b = 1$.

(ii) Lines that are defined by (7.12) and (7.13) .

(iii) Interior (shaded) regions that remain between the boundaries (i) and lines (ii).

Case (i) can never provide a solution as can be seen from the behavior of (7.11), i.e., the gradient has infinite magnitude and points outward for any of $a = 0$, $b = 0$, $a = 1$, $b = 1$. As for case (iii), it requires the gradient in (7.11) to be zero, i.e., $a = b = \alpha$. That, in turn, implies $q = \bar{p}\alpha + p\bar{\alpha}$, and therefore $\hat{p}(q) = p$, which is inadmissible. It then follows that the solution must lie on either of the lines of (7.12) or (7.13), whichever yields a lower objective function.

The proof is then complete by observing that the gradient vector should be normal to the lines, translating into

$$\begin{bmatrix} \bar{p} \log \frac{a\bar{\alpha}}{\bar{a}\alpha} \\ \\ -p \log \frac{\bar{b}\alpha}{b\bar{\alpha}} \end{bmatrix} = \lambda \begin{bmatrix} \bar{p} \\ \\ -p \end{bmatrix}$$

for some λ, which, in turn, gives (7.9). ■

α	ϵ	n	P_e
0.1	0.02	22,500	$6.5312\ 10^{-6}$
0.2	0.02	75,000	$5.0537\ 10^{-6}$
0.25	0.02	130,000	$2.3150\ 10^{-6}$
0.1	0.01	100,000	$2.0334\ 10^{-6}$
0.2	0.01	320,000	$7.7452\ 10^{-6}$
0.1	0.005	420,000	$4.1604\ 10^{-6}$

Table 7.1: Several numerical results on the upper bound on P_e for different values of α, ϵ, n.

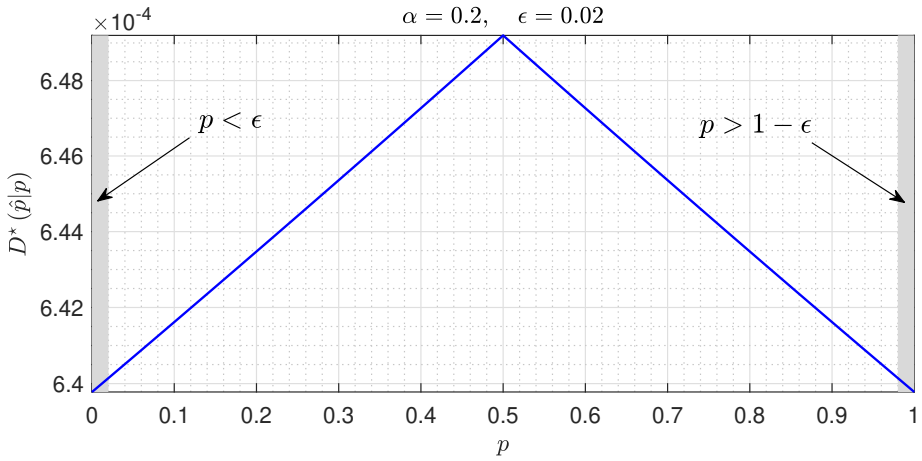

Figure 7.5: The exponent $D^*(\hat{p}|p)$ as a function of p for $\epsilon = 0.02$, $\alpha = 0.2$, i.e., when responses are flipped with 20% probability and survey results are allowed to deviate from the true percentage by at most 2%.

Figure 7.5 shows how $D^*(\hat{p}|p)$ varies as a function of p when $\alpha = 0.2$ and $\epsilon = 0.02$. As can be seen from the figure, $p = 0$ or $p = 1$ achieves $D^*(\hat{p})$ in this case. As a matter of fact, we observed that this is always true for any (α, ϵ), although an analytical proof is absent at the moment.

Using Lemma 1 and this observation, we also evaluated (7.5) for various α, ϵ, and n values such that the upper bound on P_e is in the order of 10^{-6}. Some of the evaluated values are provided in Table I.

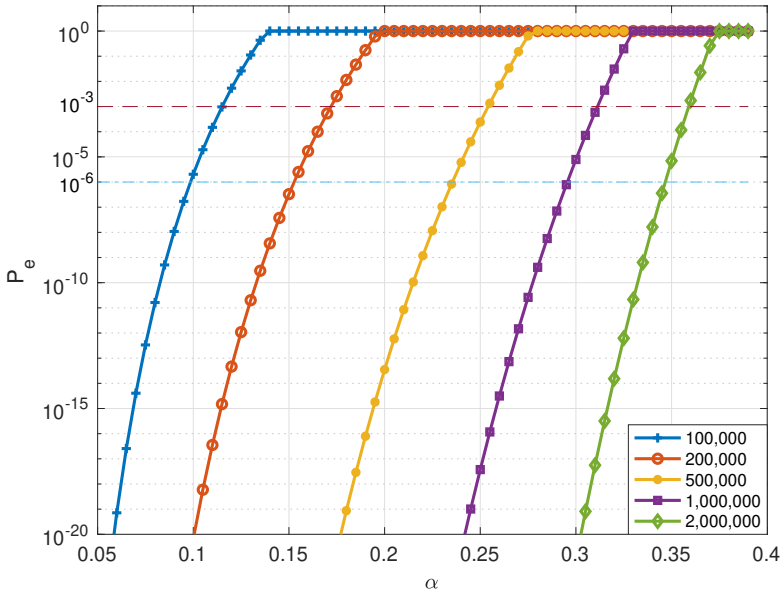

Figure 7.6: Upper bound on the probability of error P_e is evaluated for varying α values for different number of participants, n, when $\epsilon = 0.01$.

Finally, Figure 7.6 depicts the relationship between the probability of error and α for varying number of participants for a fixed $\epsilon = 0.01$. Threshold probabilities of 10^{-3}, 10^{-6} are also plotted as reference points with horizontal dashed and dotted-dashed lines, respectively. As expected, the more participants n the survey has, the more reliable the estimation is at the same randomization level α. To be more specific, with $100,000$ participants, we can only flip the survey responses with 10% probability to be able to ensure that the probability that the estimated survey result does not stay within 1% of its true value is in the order of 10^{-6}. In contrast, when we have $2,000,000$ participants, the same accuracy can be achieved even when the survey responses are flipped with 35% probability.

Appendix A

Proofs

A.1 λ optimization

A.1.1 1-dimensional Gaussian Sources

It is easy to check that the argument of the natural logarithm in (3.12) is convex in $\lambda(x)$. Therefore, by using the Euler-Lagrange theorem of variational calculus, the optimal point density function (for a fixed c) is found to be

$$\lambda_c(x) = \frac{1}{6^{1/3}c^{2/3}} \frac{f(x)^{1/3}}{(\delta c x^2 + \beta)^{1/3}}, \tag{A.1}$$

with the Lagrange multiplier $\beta \geq 0$. It remains to pick β such that $\lambda_c(x)$ integrates to 1. Since (A.1) is decreasing in β, we can always find such a β provided that $\int \lambda_c(x)dx \geq 1$ for $\beta = 0$. Following this logic and substituting $\beta = 0$ in (A.1), we observe that c has to satisfy

$$c \leq c_0 \triangleq \left(\frac{1}{108\delta^2\pi}\right)^{1/6} \Gamma\left(\frac{1}{6}\right) \approx 2.2219\,. \tag{A.2}$$

For each $c \leq c_0$, denote by β_c the value of β satisfying $\int \lambda_c(x)dx = 1$. After some algebra, (3.12) then reduces to

$$\upsilon(c, \lambda_c) = -\ln\left[\delta c\left(1 + \frac{3}{2}\int_{-\infty}^{\infty} x^2\lambda_c(x)dx\right) + \frac{\beta_c}{2}\right]$$

The optimal values of c, β_c, and $\upsilon(c, \lambda_c)$ are numerically found to be $c^* \approx 1.3719$, $\beta_{c^*} \approx 1.1764$, and $\upsilon(c^*, \lambda_{c^*}) \approx -1.7006$, respectively.

A.1.2 2-dimensional Gaussian Sources

Proceeding as in the 1-dimensional case, and noting that the argument of the natural logarithm in (3.19) is convex in $\lambda(\mathbf{x})$, we obtain

$$\lambda_c(\mathbf{x}) = \sqrt{\frac{5\sqrt{3}}{108\pi}} \cdot \frac{e^{-\|\mathbf{x}\|^2/4}}{(\delta c^2 \parallel \mathbf{x} \parallel^2 + 2c\beta_c)^{1/2}}\,, \tag{A.3}$$

where for each c, β_c is to be picked to integrate $\lambda_c(\mathbf{x})$ to 1. Substituting this into (3.19) and numerically solving for the optimal values of c and β_c, we obtain $c^* \approx 1.0017$, $\beta_{c^*} \approx 0.8741$, and the corresponding dispersion becomes $\upsilon(c^*, \beta_{c^*}) \approx -1.4686$.

A.1.3 2-dimensional Gaussian Sources

Proceeding as in the 1-dimensional case, and noting that the argument of the natural logarithm in (3.19) is convex in $\lambda(\mathbf{x})$, we obtain

$$\lambda_c(\mathbf{x}) = \sqrt{\frac{5\sqrt{3}}{108\pi}} \cdot \frac{e^{-\|\mathbf{x}\|^2/4}}{(\delta c^2 \parallel \mathbf{x} \parallel^2 + 2c\beta_c)^{1/2}}\,, \tag{A.4}$$

where for each c, β_c is to be picked to integrate $\lambda_c(\mathbf{x})$ to 1. Substituting this into (3.19) and numerically solving for the optimal values of c and β_c, we obtain $c^* \approx 1.0017$, $\beta_{c^*} \approx 0.8741$, and the corresponding dispersion becomes $v(c^*, \beta_{c^*}) \approx -1.4686$.

A.2 Probability of Decoding Error

The proof follows steps similar to [4]. For notational simplicity, we take $M = 1$. The result for general M can be obtained by replacing E with ME (or γ with $M\gamma$). Unlike the proof in [4], we use a tighter version of the Chernoff bound, i.e.,

$$Q(x) \stackrel{\Delta}{=} \frac{1}{\sqrt{2\pi}} \int_x^\infty e^{-\frac{s^2}{2}} ds \leq \frac{1}{2} e^{-\frac{x^2}{2}} \tag{A.5}$$

for all $x \geq 0$, to obtain a tighter result.

We have

$$\begin{aligned}
\Pr[\mathcal{O}] &= 1 - \int_{-\infty}^{\infty} f_W(w_1) \Pr\left[\max_{2 \leq i \leq N} \{W_i\} < \sqrt{E} + w_1\right] dw_1 \\
&= 1 - \int_{-\infty}^{\infty} f_W(w_1) \prod_{i=2}^{N} \Pr\left[W_i < \sqrt{E} + w_1\right] dw_1 \\
&= \int_{-\infty}^{\infty} f_Z(z) \left\{1 - (1 - Q(\sqrt{\gamma} + z))^{N-1}\right\} dz.
\end{aligned}$$

where $f_Z(z) = \frac{1}{\sqrt{2\pi}} e^{-\frac{z^2}{2}}$.

For any $\gamma \geq 2 \ln N$, we set $\mu = \sqrt{2 \ln N} - \sqrt{\gamma}$, and write

$$\Pr[\mathcal{O}] = P_{\mathcal{O},1} + P_{\mathcal{O},2} \ ,$$

where

$$P_{\mathcal{O},1} = \int_{-\infty}^{\mu} f_Z(z) \left\{1 - (1 - Q(\sqrt{\gamma} + z))^{N-1}\right\} dz$$
$$P_{\mathcal{O},2} = \int_{\mu}^{\infty} f_Z(z) \left\{1 - (1 - Q(\sqrt{\gamma} + z))^{N-1}\right\} dz \,.$$

By following similar steps as in [4], we obtain

$$P_{\mathcal{O},1} \leq \int_{-\infty}^{\mu} f_Z(z)\, dz = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\mu} e^{-\frac{z^2}{2}} dz = Q(-\mu) \leq \frac{1}{2} e^{-\frac{\mu^2}{2}}, \tag{A.6}$$

where in the last step, we used $\mu \leq 0$.

To bound $P_{\mathcal{O},2}$, we observe that

$$\begin{aligned} 1 - (1 - Q(\sqrt{\gamma} + z))^{N-1} &\leq (N-1)\, Q(\sqrt{\gamma} + z) \\ &\leq \frac{N}{2} e^{-\frac{(\sqrt{\gamma}+z)^2}{2}} \end{aligned}$$

for all $z \geq -\sqrt{\gamma}$. Since $\mu > -\sqrt{\gamma}$, it follows that

$$\begin{aligned} P_{\mathcal{O},2} &\leq \frac{N}{2} \int_{\mu}^{\infty} f_Z(z)\, e^{-\frac{(\sqrt{\gamma}+z)^2}{2}} dz \\ &= \frac{N}{2\sqrt{2\pi}} e^{-\frac{\gamma}{4}} \int_{\mu+\sqrt{\frac{\gamma}{4}}}^{\infty} e^{-s^2} ds \\ &= \frac{N}{2\sqrt{2}} e^{-\frac{\gamma}{4}} Q\left(\sqrt{2}\left(\mu + \sqrt{\frac{\gamma}{4}}\right)\right) \\ &\leq \begin{cases} \frac{N}{2\sqrt{2}} e^{-\frac{\gamma}{4} - \left(\mu + \sqrt{\frac{\gamma}{4}}\right)^2} & \mu \geq -\sqrt{\frac{\gamma}{4}}\,, \\ \frac{N}{2\sqrt{2}} e^{-\frac{\gamma}{4}} & \mu < -\sqrt{\frac{\gamma}{4}}\,. \end{cases} \end{aligned} \tag{A.7}$$

Finally, it can be shown after some algebra that

$$Ne^{-\frac{\gamma}{4}-(\mu+\sqrt{\frac{\gamma}{4}})^2} = e^{-\frac{\mu^2}{2}} . \tag{A.8}$$

By combining (A.6), (A.7), and (A.8), we obtain

$$\begin{aligned}\Pr[\mathcal{O}] &\leq \left(\frac{1}{2}+\frac{1}{2\sqrt{2}}\right) e^{-\frac{\mu^2}{2}} \\ &= \delta e^{-\frac{1}{2}\left[\sqrt{\gamma}-\sqrt{2\ln N}\right]^2}\end{aligned}$$

for all $e^{\frac{\gamma}{8}} \leq N \leq e^{\frac{\gamma}{2}}$, with $\delta = \frac{1}{2}+\frac{1}{2\sqrt{2}}$. Similarly for all $N \leq e^{\frac{\gamma}{8}}$,

$$\begin{aligned}\Pr[\mathcal{O}] &\leq Ne^{-\frac{\gamma}{4}}\left(\frac{1}{2\sqrt{2}}+\frac{1}{2}e^{-\left(\sqrt{2\ln N}-\sqrt{\frac{\gamma}{4}}\right)^2}\right) \\ &= \delta e^{\ln N-\frac{\gamma}{4}} .\end{aligned}$$

A.3 MSE Conditioned on Outage

Let $\mathcal{R}_i$ and $\hat{\mathbf{x}}_i$ denote the ith quantization region and the corresponding quantized value, respectively. We then estimate the resultant distortion by

$$\begin{aligned}\mathbb{E}\left[\parallel \mathbf{X}-\hat{\mathbf{X}} \parallel^2 \left|\mathcal{O}\right.\right] &\overset{(a)}{=} \sum_{i=1}^{N} \mathbb{E}\left[\parallel \mathbf{X}-\hat{\mathbf{X}} \parallel^2 \left|\mathcal{O}, \mathbf{X}\in\mathcal{R}_i\right.\right] \Pr\left[\mathbf{X}\in\mathcal{R}_i\right] \\ &\overset{(b)}{=} \frac{1}{N-1}\sum_{i=1}^{N}\sum_{\substack{j=1\\ j\neq i}}^{N} \mathbb{E}\left[\parallel \mathbf{X}-\mathbf{r}_j \parallel^2 \left|\mathcal{O}, \mathbf{X}\in\mathcal{R}_i\right.\right] \Pr[\mathbf{X}\in\mathcal{R}_i] \\ &\overset{(c)}{=} \frac{1}{N-1}\sum_{i=1}^{N}\sum_{\substack{j=1\\ j\neq i}}^{N} \mathbb{E}\left[\parallel \mathbf{X}-\mathbf{r}_j \parallel^2 \left|\mathbf{X}\in\mathcal{R}_i\right.\right] \Pr[\mathbf{X}\in\mathcal{R}_i]\end{aligned}$$

$$
\begin{aligned}
&\leq \frac{N}{N-1}\sum_{i=1}^{N}\Pr[\mathbf{X}\in\mathcal{R}_i]\sum_{j=1}^{N}\frac{1}{N}\mathbb{E}\left[\parallel \mathbf{X}-\mathbf{r}_j \parallel^2 \,\middle|\, \mathbf{X}\in\mathcal{R}_i\right] \\
&\overset{(d)}{=} \frac{N}{N-1}\mathbb{E}[\parallel \mathbf{X}-\tilde{\mathbf{X}} \parallel^2] \\
&= \frac{N}{N-1}\left(\mathbb{E}[\parallel \mathbf{X} \parallel^2]+\mathbb{E}[\parallel \tilde{\mathbf{X}} \parallel^2]\right) \qquad \text{(A.9)}
\end{aligned}
$$

where (a) follows from the independence of the outage event $\mathcal{O}$ and $\mathbf{X}$, (b) from the fact that when outage happens, $\hat{\mathbf{X}}$ is distributed uniformly on the *incorrect* quantized values $\mathbf{r}_j$, $j \neq i$, (c) from the independence of $\mathbf{X}$ from $\mathcal{O}$ even when $\mathbf{X} \in \mathcal{R}_i$ is given, and finally (d) by defining a fictitious variable $\tilde{\mathbf{X}}$ independent of $\mathbf{X}$ and distributed uniformly over all quantization levels $\mathbf{r}_j$. Clearly, it follows from (A.9) that as $N \to \infty$, (3.6) is satisfied for any $\epsilon > 0$.

Bibliography

[1] E. Tuncel. On error exponents under a privacy-preserving voting regime. In *2019 IEEE International Symposium on Information Theory (ISIT)*, pages 797–801, 2019.

[2] F. A. Abdallah and R. Knopp. Source-channel coding for very-low bandwidth sources. In *2008 IEEE Information Theory Workshop*, pages 184–188, May 2008.

[3] A. Jain, D. Gunduz, S. R. Kulkarni, H. V. Poor, and S. Verdu. Energy-distortion tradeoffs in Gaussian joint source-channel coding problems. *IEEE Transactions on Information Theory*, 58(5):3153–3168, May 2012.

[4] E. Koken, D. Gunduz, and E. Tuncel. Energy-distortion exponents in lossy transmission of Gaussian sources over Gaussian channels. *IEEE Transactions on Information Theory*, 63(2):1227–1236, Feb. 2017.

[5] C. Sevinç and E. Tuncel. On asymptotic analysis of energy-distortion tradeoff for low-delay transmission over Gaussian channels. In *2018 IEEE International Symposium on Information Theory (ISIT)*, pages 2599–2603, June 2018.

[6] C. Sevinç and E. Tuncel. On energy-distortion exponents for low-delay Gaussian broadcasting. In *2018 IEEE International Symposium on Information Theory (ISIT)*, pages 2604–2608, June 2018.

[7] S. I. Bross and H. Zalach. Distortion bounds for source broadcasting and asymmetric data transmission with bandwidth expansion. In *2017 IEEE International Symposium on Information Theory (ISIT)*, pages 101–105, June 2017.

[8] Shraga I. Bross and Hagai Zalach. Source broadcasting and asymmetric data transmission with bandwidth expansion. *IEEE Transactions on Communications*, 67(10):6698–6710, 2019.

[9] Y. Murin, Y. Kaspi, R. Dabora, and D. Gündüz. Energy-distortion tradeoff for the Gaussian broadcast channel with feedback. In *2016 IEEE International Symposium on Information Theory (ISIT)*, pages 1829–1833, July 2016.

[10] Cynthia Dwork. Differential privacy. In Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener, editors, *Automata, Languages and Programming*, pages 1–12, Berlin, Heidelberg, 2006. Springer Berlin Heidelberg.

[11] Cynthia Dwork and Aaron Roth. The algorithmic foundations of differential privacy. *Foundations and Trends® in Theoretical Computer Science*, 9(3–4):211–407, 2014.

[12] Arik Friedman and Assaf Schuster. Data mining with differential privacy. In *Proceedings of the 16th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, KDD '10, page 493–502, New York, NY, USA, 2010. Association for Computing Machinery.

[13] Martin Abadi, Andy Chu, Ian Goodfellow, H. Brendan McMahan, Ilya Mironov, Kunal Talwar, and Li Zhang. Deep learning with differential privacy. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, CCS '16, page 308–318, New York, NY, USA, 2016. Association for Computing Machinery.

[14] Christopher T. Kenny, Shiro Kuriwaki, Cory McCartan, Evan T. R. Rosenman, Tyler Simko, and Kosuke Imai. The use of differential privacy for census data and its impact on redistricting: The case of the 2020 u.s. census. *Science Advances*, 7(41):eabk3283, 2021.

[15] Úlfar Erlingsson, Vasyl Pihur, and Aleksandra Korolova. Rappor: Randomized aggregatable privacy-preserving ordinal response. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, CCS '14, page 1054–1067, New York, NY, USA, 2014. Association for Computing Machinery.

[16] Differential Privacy Team. Learning with privacy at scale. [Online]. `https://machinelearning.apple.com/research/learning-with-privacy-at-scale`, December 2017.

[17] Bolin Ding, Janardhan Kulkarni, and Sergey Yekhanin. Collecting telemetry data privately. In *Advances in Neural Information Processing Systems 30: Annual Conference on Neural Information Processing Systems 2017, December 4-9, 2017, Long Beach, CA, USA*, pages 3571–3580, 2017.

[18] Stanley L. Warner. Randomized response: A survey technique for eliminating evasive answer bias. *Journal of the American Statistical Association*, 60(309):63–69, 1965.

[19] Ajit C. Tamhane. Randomized response techniques for multiple sensitive attributes. *Journal of the American Statistical Association*, 76(376):916–923, 1981.

[20] Gábor Szűcs. Random response forest for privacy-preserving classification. *Journal of Computational Engineering*, 2013:1–6, 01 2013.

[21] Teng Wang, Xuefeng Zhang, Jingyu Feng, and Xinyu Yang. A comprehensive survey on local differential privacy toward data statistics and analysis. *Sensors*, 20(24):7030, Dec 2020.

[22] Graham Cormode, Somesh Jha, Tejas Kulkarni, Ninghui Li, Divesh Srivastava, and Tianhao Wang. Privacy at scale: Local differential privacy in practice. In *Proceedings of the 2018 International Conference on Management of Data*, SIGMOD '18, page 1655–1658, New York, NY, USA, 2018. Association for Computing Machinery.

[23] Tianhao Wang, Jeremiah Blocki, Ninghui Li, and Somesh Jha. Locally differentially private protocols for frequency estimation. In *26th USENIX Security Symposium (USENIX Security 17)*, pages 729–745, Vancouver, BC, August 2017. USENIX Association.

[24] Angel M. Del Rey, Xingxing Xiong, Shubo Liu, Dan Li, Zhaohui Cai, and Xiaoguang Niu. A comprehensive survey on local differential privacy. *Security and Communication Networks*, 2020:8829523, 2020.

[25] Björn Bebensee. Local differential privacy: a tutorial, 2019.

[26] V. Kostina and S. Verdu. Fixed-length lossy compression in the finite blocklength regime. *IEEE Transactions on Information Theory*, 58(6):3309–3338, June 2012.

[27] Y. Polyanskiy, H. V. Poor, and S. Verdu. Channel coding rate in the finite blocklength regime. *IEEE Transactions on Information Theory*, 56(5):2307–2359, May 2010.

[28] M.V. Burnashev. On minimum attainable mean-square error in transmission of a parameter over a channel with white Gaussian noise. *Problems Inform. Transmission*, 21(4):247–257, 1985.

[29] J.M. Wozencraft and I.M. Jacobs. *Principles of communication engineering.* Wiley, 1965.

[30] N. Merhav. On optimum parameter modulation-estimation from a large deviations perspective. *IEEE Transactions on Information Theory*, 58(12):7215–7225, Dec. 2012.

[31] Omri Lev and Anatoly Khina. Energy-limited joint source–channel coding via analog pulse position modulation. In *2021 IEEE Information Theory Workshop (ITW)*, pages 1–6, 2021.

[32] Z. Reznic, M. Feder, and R. Zamir. Distortion bounds for broadcasting with bandwidth expansion. *IEEE Transactions on Information Theory*, 52(8):3778–3788, Aug. 2006.

[33] C. Sevinç and E. Tuncel. On the analysis of energy-distortion tradeoff for zero-delay transmission over Gaussian broadcast channels. In *2019 IEEE International Symposium on Information Theory (ISIT)*, pages 2758–2762, 2019.

[34] Ceren Sevinç and Ertem Tuncel. On asymptotic analysis of energy-distortion tradeoff for low-delay transmission over gaussian channels. *IEEE Transactions on Communications*, 69(7):4448–4460, 2021.

[35] K. Zeger and V. Manzella. Asymptotic bounds on optimal noisy channel quantization via random coding. *IEEE Transactions on Information Theory*, 40(6):1926–1938, 1994.

[36] B. Hochwald. Tradeoff between source and channel coding on a Gaussian channel. *IEEE Transactions on Information Theory*, 44(7):3044–3055, 1998.

[37] E. Koken and E. Tuncel. On the energy-distortion tradeoff for the Gaussian broadcast problem. In *2016 IEEE International Symposium on Information Theory (ISIT)*, pages 1839–1843, July 2016.

[38] Allen Gersho and Robert M. Gray. *Vector Quantization and Signal Compression*. Kluwer Academic Publishers, Norwell, MA, USA, 1991.

[39] P.L. Zador. *Development and Evaluation of Procedures for Quantizing Multivariate Distributions*. PhD thesis, Stanford University, 1963.

[40] A. Gersho. Asymptotically optimal block quantization. *IEEE Transactions on Information Theory*, 25(4):373–380, July 1979.

[41] S. Na and D. L. Neuhoff. Bennett's integral for vector quantizers. *IEEE Transactions on Information Theory*, 41(4):886–900, Jul 1995.

[42] L. Fejes-Tóth. Sur la representation d'une population infinie par un nombre fini d'elements. *Acta Math. Acad. Sci. Hungar.*, 10:76–81, 1959.

[43] D. J. Newman. The hexagon theorem. *Bell Lab. Tech. Memo.*, 1964. published in the special issue on quantization of the IEEE Trans. Inform. Theory, vol. IT-28, pp. 137–139, Mar. 1982.

[44] E. Agrell and T. Eriksson. Optimization of lattices for quantization. *IEEE Transactions on Information Theory*, 44(5):1814–1828, Sep. 1998.

[45] J. Samuelsson. Multidimensional companding quantization of the Gaussian source. *IEEE Transactions on Information Theory*, 49(5):1343–1351, May 2003.

[46] R. Zamir and M. Feder. On lattice quantization noise. *IEEE Transactions on Information Theory*, 42(4):1152–1159, Jul 1996.

[47] E. S. Barnes and N. J. A. Sloane. The optimal lattice quantizer in three dimensions. *SIAM J. Alg. Discr. Methods*, 4:30–41, Mar. 1983.

[48] D. G. Horvitz, B. G. Greenberg, and J. R. Abernathy. Randomized response: A data-gathering device for sensitive questions. *International Statistical Review / Revue Internationale de Statistique*, 44(2):181–196, 1976.

[49] Shaul K. Bar-Lev, Elizabeta Bobovitch, and Benzion Boukai. A note on randomized response models for quantitative data. *Metrika: International Journal for Theoretical and Applied Statistics*, 60(3):255–260, November 2004.

[50] Giancarlo Diana, Marco Giordan, and Pier Francesco Perri. Randomized response surveys: A note on some privacy protection measures. *Model Assisted Statistics and Applications*, 8:19–28, 02 2013.

[51] Imre Csiszár and János Körner. *Information Theory: Coding Theorems for Discrete Memoryless Systems*. Cambridge University Press, 2 edition, 2011.

[52] Ceren Sevinc and Ertem Tuncel. Information theoretic approach on randomized response models in surveys. In *2021 IEEE International Symposium on Information Theory (ISIT)*, pages 3338–3342, 2021.

[53] Roger Tourangeau and Ting Yan. Sensitive questions in surveys. *Psychological Bulletin*, 133(5):859–883, 2007.

[54] Marcus Tannenberg. The autocratic trust bias: Politically sensitive survey items and self-censorship. *Social Science Research Network*, 2017.

[55] Steven M. Kay. *Fundamentals of Statistical Signal Processing: Estimation Theory*. Prentice-Hall, Inc., USA, 1993.