12-18-2015

A Critical Analysis of Random Response Techniques

Emanuel Zanzerkia

A Critical Analysis of Random Response Techniques

Emanuel Zanzerkia

Submitted in Partial Completion of the
Requirements for Commonwealth Honors in Mathematics

Bridgewater State University

December 18, 2015

Dr. Kevin Rion, Thesis Director
Dr. Irina Seceleanu, Committee Member
Dr. Mahmoud El Hashash, Committee Member

Critical Analysis of Random Response Techniques

Emanuel Zanzerkia

Contents

Abstract

In order to understand and make informed decision on sensitive topics such as domestic violence and drug use, interviews have been used to collect data. However it is difficult to assess how truthful respondents are since they may not feel at ease revealing the truth to an interviewer. Surveyors of sensitive issues face the problem that respondents may be reluctant to answer truthfully since the respondent may feel pressured socially or may fear the repercussions of their truthful answer. Processes known as random response techniques have been introduced to allow interviewers the ability to extract information they need for a population, while preserving privacy of individual respondents by introducing randomness to the surveying process. The focus of this project was to critically assess the accuracy of two such techniques and the level of privacy protection afforded to the respondent by the techniques. Using the method of moment matching, estimators of the population proportion were created for both techniques. Once the estimators were created, the accuracy of the estimators could be assessed by studying the variance. Finally we measured the level of privacy protection the techniques afforded to respondents by calculating mutual information and entropy.

1 Introduction

Suppose we consider the following scenario. A superintendent of a school district would like to learn how prevalent drug use is among high school students by interviewing a randomly selected sample of the student population. The problem with asking students outright if they use drugs is some students will lie due to a fear of the repercussions from admitting to using drugs. In order to obtain a somewhat accurate estimate for the proportion of students who use drugs, the interviewers need to make them feel at ease with being truthful.

In 1965 S.L Warner developed random response techniques which introduce randomness in the surveying process so no matter which response the respondent provides, there is some ambiguity as to whether the respondent truly has the attribute in question or not. The idea is to scramble the data in such a way that the individual responses cannot be determined but the overall trends can still be determined. The downside of such methods is that some information is lost in the process, and so these techniques are less efficient per sample than non-random (true response) methods.

There are many variants of these techniques, two of which we studied in this research. In both techniques we start with a sample of size n. Each of these n people either has the attribute in question or does not. We denote their true states as $a_1, \ldots, a_n \in \{0, 1\}$ where a person's status is $a_i = 1$ who has the attribute, and is $a_i = 0$ otherwise. These true states are and will remain hidden to the researchers. All the researchers get to see are the respondents answers to the yes/no questions; but due to the random response techniques described below, these responses are random and are only the true status of the respondents an estimable fraction of the time.

To refer to the random responses the researchers can actually see, we let for each $i = 1, \ldots, n$, Y_i be the random response of the i^{th} individual where $Y_i = 1$ when the response is Yes and $Y_i = 0$ when the response is No. Upon interviewing the n people, the observed data set $y_1 \ldots, y_n$ of zeroes and ones is one to which the researchers have full access. From this data set, the researchers can calculate $\bar{y}$, which is the proportion of the sample that responded with Yes.

The researchers are looking to estimate the true population proportion π, but first we focus our attention on estimating the true proportion $\bar{a}$ of the sample that actually has the attribute in question. By using the observable $\bar{y}$ we develop an estimate for $\bar{a}$. This estimate for $\bar{a}$ is then used in turn to estimate the population proportion π.

In critically assessing the non-privacy related performance of the two random response techniques, we not only consider their performance relative to each other, but also to a baseline calculated from direct reporting in which respondents actually report their true states with no concern for privacy preservation.

The analysis of these two techniques begins with developing an estimator for $\bar{a}$. We then measure the accuracy of the estimator by calculating the bias and variance.

Finally we introduce measures for the level of privacy these techniques afford the respondents and apply them to quantify the privacy of the methods.

1.1 One Question Biased Coin Strategy

The first technique is called the One Question Biased Coin Strategy. For this method, we start with a coin that has a Ber(p) distribution, so $\mathbb{P}[C = 1] = p$ and $\mathbb{P}[C = 0] = 1 - p$. Every respondent is told to flip the coin without letting the interviewer see the result. Call this result C_i for $i \in \{1, 2, \ldots, n\}$. If the coin flip resulted in a heads, we have $c_i = 1$ and the respondent tells the truth, meaning $y_i = a_i$. If the coin flip resulted in tails, we have $c_i = 0$ and the respondent lies, meaning $y_i = 1 - a_i$.

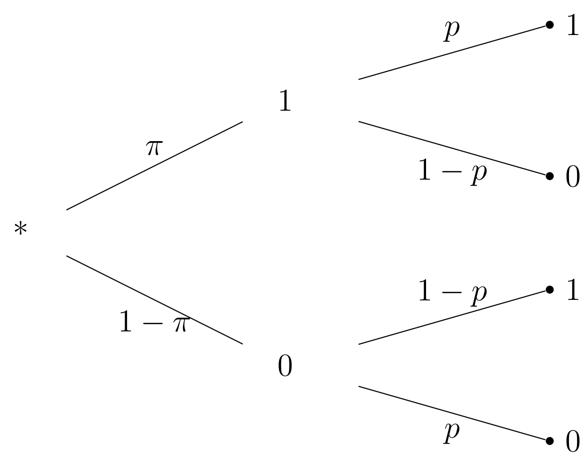


Figure 1: Probability tree diagram for One Question Biased Coin strategy

We will calculate some useful probabilities that will be used in some later calculations. In figure 1, the first nodes show the true values of the respondents, a_i and the second level of nodes shows the respondents observed values, y_i.

From this probability tree we can see the conditional probabilities:

$$\mathbb{P}[y = 1 | a = 1] = p$$
$$\mathbb{P}[y = 1 | a = 0] = 1 - p$$
$$\mathbb{P}[y = 0 | a = 1] = 1 - p$$
$$\mathbb{P}[y = 0 | a = 0] = p$$

To obtain the joint probabilities, we multiply the conditional probability with the corresponding probability that a is 1 or 0. Therefore

$$\begin{aligned}\mathbb{P}[y=1,a=1] &= \pi p\\ \mathbb{P}[y=1,a=0] &= (1-\pi)(1-p)\\ \mathbb{P}[y=0,a=1] &= \pi(1-p)\\ \mathbb{P}[y=0,a=0] &= (1-\pi)p\end{aligned}$$

Applying the law of total probability to these joint probabilities, we have

$$\begin{aligned}\mathbb{P}(y=1) &= \pi p + (1-\pi)(1-p)\\ \mathbb{P}(y=0) &= (1-\pi)p + \pi(1-p)\end{aligned}$$

These two probabilities will be useful in our assessment of privacy protection.

Another way of looking at these probabilities is to consider the technique as a one step Markov process. We have true states A_i that get transitioned into observed states Y_i. The transition matrix for this process is

$$\begin{bmatrix} p & 1-p \\ 1-p & p \end{bmatrix}$$

where the ij^{th} entry is the probability that a person with true state i has observed state j. Multiplying this transition matrix with the vector $(1-\pi,\pi)$, where $1-\pi$ is the probability that the individual as true state $a_i = 0$ and π is the probability that the true state $a - i = 1$, gives us

$$(1-\pi,\pi)\begin{bmatrix} p & 1-p \\ 1-p & p \end{bmatrix} = ((1-\pi)p + \pi(1-p), (1-\pi)(1-p) + \pi p)$$

We see that the two entries in the vector are the probabilities we calculated for $y = 0$ and $y = 1$.

1.2 Two Question Bernoulli(p) Strategy

The second technique is called the *Two Question Bernoulli(p) Strategy.* For this method we start with two questions and a coin that has a Ber(p) distribution. The first question asks about the attribute of interest, while the second is about the flip of the coin. An example is given in figure 2.

Question 1: Do you use recreational drugs?	YES	NO
Question 2: Is the second flip of your fair coin a head?	YES	NO

Figure 2: Sample survey questions in the *Two Question Ber(p)* method.

The respondent is asked to flip the coin twice without letting the interviewer know the results of the coin tosses. Let C_i be the result of the first coin toss of the i^{th} individual, and let D_i be the result of the second coin toss. If $c_i = 1$ meaning the first flip of the coin resulted in heads, the respondent answers the first question truthfully. Therefore $y_i = a_i$. If $c_i = 0$ meaning the first flip of the coin resulted in tails, the respondent answers the second question. Therefore $y_i = d_i$.

We now calculate the same probabilities that were calculated for the One Question Biased Coin strategy. Calculating the conditional probabilities, we first consider an individual with true state $a = 1$. For this individual to have an observed state $y = 1$, he either needs to flip heads on the first coin flip, $c = 1$, or flip tails on the first coin flip, $c = 0$, then heads on the second coin flip, $d = 1$. This gives the probability

$$\begin{aligned}\mathbb{P}[y = 1|a = 1] &= p + (1-p)p \\ &= p(2-p)\end{aligned}$$

For the same individual to have an observed state $y = 0$, he must have both the first and second coin flips be tails, $c = 0$ and $d = 0$. This gives the probability

$$\mathbb{P}[y = 0|a = 1] = (1-p)^2$$

We now consider an individual with true state $a = 0$. For this individual to have observed state $y = 1$, he must have the first coin flip land tails, $c = 0$, and then the second coin flip land heads, $d = 0$. Thus the probability of this happening is

$$\mathbb{P}[y = 1|a = 0] = p(1-p)$$

Finally, for this individual with true state $a = 0$ to have observed value $y = 0$, he either needs the first coin flip to land heads, $c = 1$, or he needs both the first and second coin flips to land tails, $c = 0$ and $d = 0$. Thus the probability is

$$\mathbb{P}[y = 0|a = 0] = p + (1-p)^2$$

To obtain the joint probabilities, we multiply the conditional probability with the corresponding probability that a is 1 or 0. Therefore

$$\begin{aligned}\mathbb{P}[y = 1, a = 1] &= \pi p(2-p) \\ \mathbb{P}[y = 1, a = 0] &= p(1-p)(1-\pi) \\ \mathbb{P}[y = 0, a = 1] &= \pi(1-p)^2 \\ \mathbb{P}[y = 0, a = 0] &= (1-\pi)p + (1-\pi)(1-p)^2\end{aligned}$$

Applying the law of total probability to these joint probabilities we have

$$\begin{aligned}\mathbb{P}(y = 1) &= \pi p(2-p) + (1-\pi)(1-p)p = \pi p + p - p^2 \\ \mathbb{P}(y = 0) &= \pi(1-p)^2 + (1-\pi)p + (1-\pi)(1-p)^2 = 1 - \pi p - p + p^2\end{aligned}$$

Just like the *One Question Biased Coin* technique, we can express the *Two Question Bernoulli(p)* technique as a one step Markov process with transition matrix

$$\begin{bmatrix} p + (1-p)^2 & p(1-p) \\ (1-p)^2 & p(2-p) \end{bmatrix}$$

where the ij^{th} entry is the probability that a person with true state i has observed state j. As before, we multiply this transition matrix with the vector $(1-\pi, \pi)$, to get

$$(1-\pi, \pi)\begin{bmatrix} p + (1-p)^2 & p(1-p) \\ (1-p)^2 & p(2-p) \end{bmatrix} = (1 - \pi p - p + p^2, \pi p + p - p^2)$$

Again we see that the two entries in the vector are the probabilities we calculated for $y = 0$ and $y = 1$.

2 Estimator

An estimator is a function that when evaluated gives estimates for a parameter of interest. To produce an estimator, various methods can be used. Depending on the context of the problem, some may perform better than others. For this analysis we started with the method of moment matching to generate an estimator for the proportion of the sample that have the attribute in question.

2.1 Method of Moments Estimator

Moments are characterizations of a distribution. "For each integer n, the nth *moment of X* (or $F_X(x)$), μ'_n, is

$$\mu'_n = \mathbb{E}[X^n]$$

The nth *central moment of X*, μ_n, is

$$\mu_n = \mathbb{E}(X-\mu)^n$$

where $\mu = \mu'_1 = \mathbb{E}[X]$" (Casella & Berger, 2002). In this work, the two relevant moments are the first moment which is the mean, or expected value of X, and the second central moment which is the variance. These moments are used in describing the distribution of a random variable, and are also used to generate estimators.

The method of moment matching produces a system of equations which equate the sample moments with the theoretical moments. This system of equations is then solved for the theoretical moments producing estimators for the parameters of interest. Our usage of the method of moment matching equates the first moment of the observed values with the first moment of the true values of the individuals. We can then solve the equation for the first moment of the true value of the individuals.

For the direct reporting technique, since each respondent reveals their true state, $y_i = a_i$ and so our estimator becomes

$$g_0(y_1, \ldots, y_n) = \bar{y}. \tag{1}$$

2.1.1 One Question Biased Coin Estimator

For this random response technique, if the respondent flips heads, she reports her true value, and if she flips tails, she lies. Therefore

$$Y_i = \begin{cases} a_i, & C_i = 1 \\ 1 - a_i, & C_i = 0 \end{cases}$$

So $Y_i = 1[C_i = 1]a_i + 1[C_i = 0](1 - a_i)$. We now calculate the expected value of Y_i. Thus

$$\begin{aligned}
\mathbb{E}[Y_i] &= \mathbb{E}[1[C_i = 1]a_i + 1[C_i = 0](1 - a_i)] \\
&= \mathbb{E}[1[C_i = 1]a_i] + \mathbb{E}[1[C_i = 0](1 - a_i)] \\
&= a_i\mathbb{E}[1[C_i = 1]] + (1 - a_i)\mathbb{E}[1[C_i = 0]] \\
&= a_i(p) + (1 - a_i)(1 - p)
\end{aligned}$$

Taking $\mathbb{E}[Y_i] = a_i(p)+(1-a_i)(1-p)$, we can find an expression for $\mathbb{E}[Y_1+Y_2+\cdots+Y_n]$ and ultimately find an expression for $\mathbb{E}[\bar{Y}]$. Since expected value is a linear operation, we have $\mathbb{E}\left[\sum_{i=1}^{n} Y_i\right] =$

$\sum_{i=1}^{n} \mathbb{E}[Y_i]$ which then leads to

$$\begin{aligned}\mathbb{E}[Y_1 + Y_2 + \cdots + Y_n] &= \mathbb{E}[Y_1] + \mathbb{E}[Y_2] + \cdots + \mathbb{E}[Y_n] \\ &= a_1(p) + (1 - a_1)(1 - p) + a_2(p) + (1 - a_2)(1 - p) + \cdots + a_n(p) + (1 - a_n)(1 - p) \\ &= (a_1 + a_2 + \cdots + a_n)p + (n - [a_1 + a_2 + \cdots + a_n])(1 - p)\end{aligned}$$

Since $a_1 + a_2 + \cdots + a_n = n\bar{a}$, we get that $\mathbb{E}[Y_1 + Y_2 + \cdots + Y_n] = n\bar{a}p + n(1-\bar{a})(1-p)$. Furthermore, since expected value is a linear operation, we have $\mathbb{E}[\bar{Y}] = \frac{1}{n}\mathbb{E}\left[\sum_{i=1}^{n} Y_i\right] = \bar{a}p + (1 - \bar{a})(1 - p)$. Replacing $\mathbb{E}[\bar{Y}]$ with $\bar{y}$ and solving for $\bar{a}$ we get $\bar{a} = \frac{\bar{y}-1+p}{2p-1}$ and so our estimator is

$$g_1(y_1, \ldots, y_n) = \frac{\bar{y} - 1 + p}{2p - 1} \tag{2}$$

2.1.2 Properties of the One Question Biased Coin Estimator

We first want to take a look at the range of the estimator as a function of p. Since the values of Y_i are either one or zero, we know that $0 \leq \bar{y} \leq 1$. Furthermore since the estimator is strictly increasing for any value of $p \neq 1/2$, we have

$$\begin{cases} \frac{p}{2p-1} \leq g_1 \leq \frac{p-1}{2p-1}, & p \in [0, 1/2) \\ \frac{p-1}{2p-1} \leq g_1 \leq \frac{p}{2p-1}, & p \in (1/2, 1] \end{cases}$$

This gives us expressions for the upper bound and lower bound of $\bar{a}$ for any given p value.

Figure 3 shows the graph of the upper and lower bounds of $\bar{a}$ vs p. The horizontal line is $\bar{a} = 1$. The upper bound and lower bound always traps the interval $[0, 1]$ for any value of $0 \leq p \leq 1$. What this means is that with our estimator g_1, no matter what value of p is chosen for the coin, we have the potential to calculate $\bar{a}$ within $[0, 1]$. However when $p \neq 0$ and $p \neq 1$, we have the potential to calculate an estimate of $\bar{a} \notin [0, 1]$. As p approaches 0 or 1, the bounded region is only slightly larger than $[0, 1]$, however as p approaches 1/2, the region bounded gets larger and larger. Therefore we need to find what values of $\bar{y}$ give us reasonable values for estimates of $\bar{a}$ given a value of p

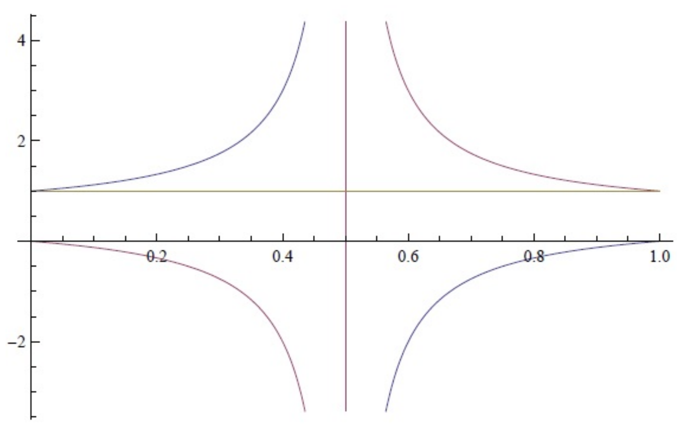


Figure 3: Graph of upper bound and lower bound of g_1 for $\bar{a}$ vs. p.

Since we want the estimate of $\bar{a}$ to be within the interval $[0,1]$, we need to set $0 \leq \frac{\bar{y}-1+p}{2p-1} \leq 1$. Solving for $\bar{y}$ we get

$$\begin{cases} p \leq \bar{y} \leq 1-p, & p \in [0,1/2) \\ 1-p \leq \bar{y} \leq p, & p \in (1/2,1] \end{cases}$$

Looking at figure 4, we see the upper and lower bounds for $\bar{y}$ that will give meaningful values of $\bar{a}$ for a given value of p. So as p approaches $1/2$, the values of $\bar{y}$ are more limited.

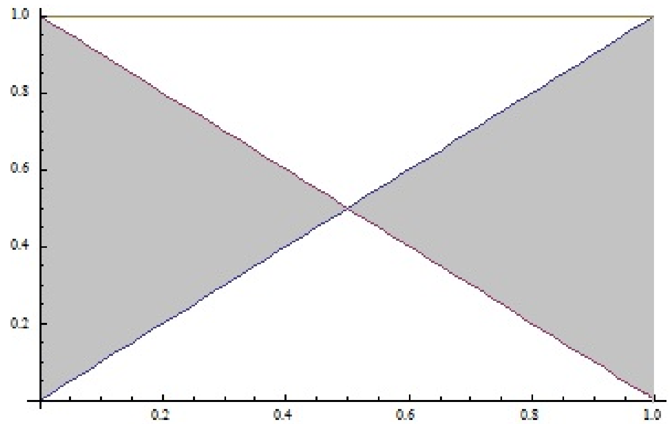


Figure 4: Graph of upper bound and lower bound for $\bar{y}$ vs. p.

2.1.3 Two Question Ber(p) Estimator

For the Two Question Ber(p) technique, if the flip of the first coin lands heads, the respondent truthfully reports their true value. If however the first flip lands tails, the respondent reports the value of the second coin flip. Therefore

$$Y_i = \begin{cases} a_i, & C_i = 1 \\ D_i, & C_i = 0 \end{cases}$$

We can take this piece-wise expression for Y_i and change it in closed form.

$$Y_i = 1[C_i = 1]a_i + 1[C_i = 0]D_i$$

We now find the expected value of Y_i using the fact that $\mathbb{E}[D_i] = p$ since D_i is the result of a coin that has distribution $Ber(p)$.

$$\begin{aligned} \mathbb{E}[Y_i] &= \mathbb{E}[1[C_i = 1]a_i + 1[C_i = 0]D_i] \\ &= a_i(p) + (1-p)\mathbb{E}[D_i] \\ &= a_i(p) + (1-p)p \end{aligned}$$

Using this expression for the value of $\mathbb{E}[Y_i]$, we find $\mathbb{E}[\bar{Y}]$ by first finding $\mathbb{E}[Y_1 + Y_2 + \cdots + Y_n]$.

$$\begin{aligned} \mathbb{E}[Y_1 + Y_2 + \cdots + Y_n] &= a_1 p + (1-p)p + a_2 p + (1-p)p + \cdots + a_n p + (1-p)p \\ &= (a_1 + a_2 + \cdots + a_n)p + n(1-p)p \\ &= n\bar{a}p + n(1-p)p \end{aligned}$$

Dividing through by n, we get $\mathbb{E}[\bar{Y}] = \frac{\mathbb{E}[Y_1+Y_2+\cdots+Y_n]}{n} = \bar{a}p + (1-p)p$. Finally, we replace $\mathbb{E}[\bar{Y}]$ with $\bar{y}$ and solve for $\bar{a}$ to get $\bar{a} = \frac{\bar{y}}{p} - 1 + p$. Therefore our estimator for the Two Question Ber(p) technique is

$$g_2(y_1, \ldots, y_n) = \frac{\bar{y}}{p} - 1 + p \tag{3}$$

Looking at this expression for $\bar{a}$ we see that p cannot equal zero. This makes sense since if $p = 0$ then every respondent flips tails and thus they report D_i and thus we do not get any usable data.

2.1.4 Properties of the Two Question Ber(p) Estimator

Similar to section 1.2, we want to first look at the range of the estimator. We have that $0 \leq \bar{y} \leq 1$ and the estimator for $\bar{a}$ is strictly increasing for all values of p. Therefore we have

$$p - 1 \leq \; g_2 \leq \frac{1}{p} - 1 + p$$

This gives the upper and lower bounds for $\bar{a}$ given any value of p. Figure 5 shows the upper and

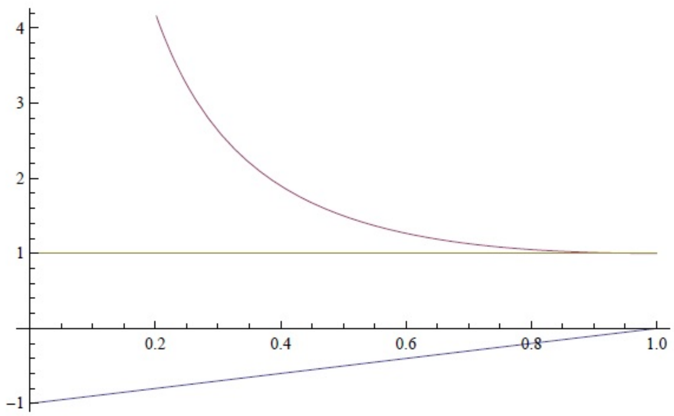


Figure 5: Graph of upper bound and lower bound for $\bar{a}$ vs. p.

lower bounds for g_2 given any value $p \in [0, 1]$. Similar to the One-Question estimator, the upper and lower bound traps the interval $[0, 1]$ and therefore no matter what value of p is chosen, we can calculate an estimate of $\bar{a}$ within $[0, 1]$. However, just like the One-Question estimator, we have the potential to calculate estimates of of $\bar{a}$ that are not in $[0, 1]$. As p approaches 1, the region bounded approaches $[0, 1]$, but as p approaches 0, the region gets much larger. We now have to find what values of $\bar{y}$ give us reasonable estimates for $\bar{a}$ given p.

Since $0 \leq \bar{a} \leq 1$, we set $0 \leq \bar{y}/p - 1 + p \leq 1$ to find the upper and lower bound of $\bar{y}$. Solving for $\bar{y}$ we get

$$p - p^2 \leq \bar{y} \leq 2p - p^2$$

From figure 6, we can see that as p approaches 1, the interval of $\bar{y}$ values that give estimates of $\bar{a}$ that lie within $[0, 1]$ gets bigger. This makes sense since as p approaches 1, more of the sample is reporting their actual value thus making $\bar{y}$ closer to $\bar{a}$.

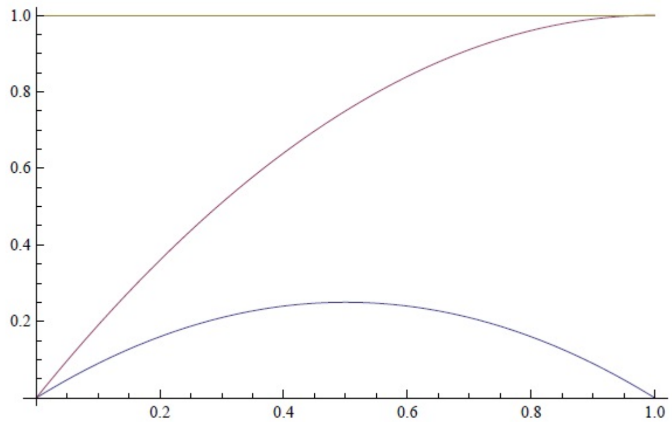


Figure 6: Graph of upper bound and lower bound for $\bar{y}$ vs. p

2.2 Admissibility of an Estimator

As mentioned earlier, there are many methods to develop estimators. This means that for each of the two techniques being studied, there is a set of estimators for the parameter we are looking for. To narrow down this set of estimators, we look at the admissibility of each estimator. An estimator is admissible if there does not exist another estimator that outperforms the estimator at any point. Therefore, an estimator is not admissible if there exists an estimator that is as good as the estimator at all points, and better at some points. Furthermore, if an estimator generates values that are outside the permissible range, it cannot be admissible.

Both estimators derived using the method of moments generate values of the parameter that are outside the permissible range of $0 \leq \bar{a} \leq 1$, and therefore they are not admissible. We move onto developing Bayesian estimators for the two random response techniques.

2.3 Bayesian Estimator

The fundamental idea behind Bayesian estimation is that we start with a prior assumption about the distribution of the parameter in question and then as we gather data we adjust the distribution creating a posterior distribution. When we take the expected value of this posterior distribution, we get an estimator for the parameter.

The adjustment of the prior distribution to the posterior distribution relies on Bayes' theorem:

$$f_{\Pi|Y}(\pi|y) = \frac{f_{Y|\Pi}(y|\pi)f_{\Pi}(\pi)}{f_Y(y)}$$

Assuming a beta prior distribution, where $\alpha : \beta$ is the odds ratio, we have $f_{\Pi}(\pi) \sim$Beta(α, β) and therefore $f_{\Pi}(\pi) = \frac{\pi^{\alpha-1}(1-\pi)^{\beta}-1}{\text{Beta}(\alpha,\beta)}$. Once we develop expressions for $f_{Y|\Pi}(y|\pi)$ and $f_Y(y)$ we can apply Bayes' theorem to get the expression for $f_{\Pi|Y}(\pi|y)$. This will give us the posterior distribution which we will take the expected value of to obtain the Bayesian estimator.

2.3.1 One Question Biased Coin Estimator

In section 1.1, we developed the following probabilities

$$\mathbb{P}(Y = 1) = \pi p + (1 - \pi)(1 - p)$$
$$\mathbb{P}(Y = 0) = (1 - \pi)p + \pi(1 - p)$$

From these probabilities, we obtain the expression $f_{Y|\Pi}(y|\pi) = p^y(1-p)^{1-y}\pi + p^{1-y}(1-p)^y(1-\pi)$.

Applying the law of total probability in the continuous case to $f_{Y,\Pi}(y,\pi)$, we obtain an expression for $f_Y(y)$. We integrate $f_{Y|\Pi}(y|\pi)f_\Pi(\pi)$ with respect to π from 0 to 1 to get

$$\begin{aligned}
f_Y(y) &= \int_0^1 f_{Y|\Pi}(y|\pi)f_\Pi(\pi)\mathrm{d}\pi \\
&= p^y(1-p)^{1-y}\int_0^1 \pi f_\Pi(\pi)\mathrm{d}\pi + p^{1-y}(1-p)^y\int_0^1 (1-\pi)f_\Pi(\pi)\mathrm{d}\pi \\
&= p^y(1-p)^{1-y}\mathbb{E}[\Pi] + p^{1-y}(1-p)^y\mathbb{E}[1-\Pi]
\end{aligned}$$

Since the prior distribution of Π was assumed to be a Beta distribution, we have $\mathbb{E}[\Pi] = \frac{\alpha}{\alpha+\beta}$. This then gives us $f_Y(y) = p^y(1-p)^{1-y}\left(\frac{\alpha}{\alpha+\beta}\right) + p^{1-y}(1-p)^y\left(1-\frac{\alpha}{\alpha+\beta}\right)$.

Now that we have the expressions for $f_\Pi(\pi)$, $f_{Y|\Pi}(y|\pi)$, and $f_Y(y)$ we can apply Bayes' theorem to get

$$\begin{aligned}
f_{\Pi|Y}(\pi|y) &= \frac{[p^y(1-p)^{1-y}\pi + p^{1-y}(1-p)^y(1-\pi)][\pi^{\alpha-1}(1-\pi)^{\beta-1}]}{f_Y(y)\mathrm{Beta}(\alpha,\beta)} \\
&= \frac{p^y(1-p)^{1-y}\pi^\alpha(1-\pi)^{\beta-1} + p^{1-y}(1-p)^y\pi^{\alpha-1}(1-\pi)^\beta}{f_Y(y)\mathrm{Beta}(\alpha,\beta)} \\
&= \frac{\mathrm{Beta}(\alpha+1,\beta)p^y(1-p)^{1-y}\pi^\alpha(1-\pi)^{\beta-1}}{f_Y(y)\mathrm{Beta}(\alpha,\beta)\mathrm{Beta}(\alpha+1,\beta)} + \frac{\mathrm{Beta}(\alpha,\beta+1)p^{1-y}(1-p)^y\pi^{\alpha-1}(1-\pi)^\beta}{f_Y(y)\mathrm{Beta}(\alpha,\beta)\mathrm{Beta}(\alpha,\beta+1)}
\end{aligned}$$

We can rewrite the fractions to see the posterior as a mixture of two Beta distributions.

$$\left(\frac{\mathrm{Beta}(\alpha+1,\beta)p^y(1-p)^{1-y}}{f_Y(y)\mathrm{Beta}(\alpha,\beta)}\right)\left(\frac{\pi^\alpha(1-\pi)^{\beta-1}}{\mathrm{Beta}(\alpha+1,\beta)}\right) + \left(\frac{\mathrm{Beta}(\alpha,\beta+1)p^{1-y}(1-p)^y}{f_Y(y)\mathrm{Beta}(\alpha,\beta)}\right)\left(\frac{\pi^{\alpha-1}(1-\pi)^\beta}{\mathrm{Beta}(\alpha,\beta+1)}\right)$$

If we let $A_1(y,p) = \frac{\mathrm{Beta}(\alpha+1,\beta)p^y(1-p)^{1-y}}{f_Y(y)\mathrm{Beta}(\alpha,\beta)}$ and $B_1(y,p) = \frac{\mathrm{Beta}(\alpha,\beta+1)p^{1-y}(1-p)^y}{f_Y(y)\mathrm{Beta}(\alpha,\beta)}$, we get our final result for our posterior distribution

$$f_{\Pi|Y}(\pi|y) = A_1(y,p)f_\Pi(\pi|\alpha+1,\beta) + B_1(y,p)f_\Pi(\pi|\alpha,\beta+1)$$

where

$$\begin{aligned}
A_1(y,p) &= \frac{\mathrm{Beta}(\alpha+1,\beta)p^y(1-p)^{1-y}}{f_Y(y)\mathrm{Beta}(\alpha,\beta)} = \frac{p^y(1-p)^{1-y}\alpha\Gamma(\alpha\beta)}{f_Y(y)\Gamma((\alpha+1)\beta)} \\
B_1(y,p) &= \frac{\mathrm{Beta}(\alpha,\beta+1)p^{1-y}(1-p)^y}{f_Y(y)\mathrm{Beta}(\alpha,\beta)} = \frac{p^{1-y}(1-p)^y\beta\Gamma(\alpha\beta)}{f_Y(y)\Gamma((\alpha+1)\beta)}
\end{aligned}$$

and

$$f_Y(y) = p^y(1-p)^{1-y}\left(\frac{\alpha}{\alpha+\beta}\right) + p^{1-y}(1-p)^y\left(1-\frac{\alpha}{\alpha+\beta}\right).$$

Taking the expected value of this posterior distribution to generate the Bayesian estimator, we get

$$\begin{aligned}
\mathbb{E}[\Pi|Y=y] &= \int_0^1 \pi f_{\Pi|Y}(\pi|y)\mathrm{d}\pi \\
&= A_1(y,p)\mathbb{E}[\mathrm{Beta}(\alpha+1,\beta)] + B_1(y,p)\mathbb{E}[\mathrm{Beta}(\alpha,\beta+1)] \\
&= A_1(y,p)\left(\frac{\alpha+1}{\alpha+\beta+1}\right) + B_1(y,p)\left(\frac{\alpha}{\alpha+\beta+1}\right)
\end{aligned}$$

2.3.2 Two Question Ber(p) Estimator

From section 1.2, we obtain the following probabilities for the Two Question Ber(p) technique

$$\begin{aligned}\mathbb{P}(Y=1) &= \pi p(2-p) + (1-\pi)(1-p)p \\ \mathbb{P}(Y=0) &= \pi(1-p)^2 + (1-\pi)p + (1-\pi)(1-p)^2\end{aligned}$$

Using these probabilities, we get $f_{Y|\Pi}(y|\pi) = (2p-p^2)^y(1-p)^{2(1-y)}\pi + (p-p^2)^y(1-p+p^2)^{1-y}(1-\pi)$. We can now use this to find the expression for $f_Y(y)$. Integrating $f_{Y|\pi}(y|\pi)f_\Pi(\pi)$ with respect to π from 0 to 1, we get

$$\begin{aligned}f_Y(y) &= \int_0^1 f_{Y|\Pi}(y|\pi)f_\Pi(\pi)\mathrm{d}\pi \\ &= (2p-p^2)^y(1-p)^{2(1-y)}\int_0^1 \pi f_\Pi(\pi)\mathrm{d}\pi + (p-p^2)^y(1-p+p^2)^{1-y}\int_0^1(1-\pi)f_\Pi(\pi)\mathrm{d}\pi \\ &= (2p-p^2)^y(1-p)^{2(1-y)}\mathbb{E}[\Pi] + (p-p^2)^y(1-p+p^2)^{1-y}\mathbb{E}[1-\Pi]\end{aligned}$$

Since the prior distribution of Π was assumed to be a Beta distribution, we have $\mathbb{E}[\pi] = \frac{\alpha}{\alpha+\beta}$. This then gives us $f_Y(y) = (2p-p^2)^y(1-p)^{2(1-y)}\left(\frac{\alpha}{\alpha+\beta}\right) + (p-p^2)^y(1-p+p^2)^{1-y}\left(1-\frac{\alpha}{\alpha+\beta}\right)$.

Now that we have the expressions for $f_\Pi(\pi)$, $f_{Y|\Pi}(y|\pi)$, and $f_Y(y)$ we can apply Bayes' theorem to get

$$\begin{aligned}f_{\Pi|Y}(\pi|y) &= \frac{[(2p-p^2)^y(1-p)^{2(1-y)}\pi + (p-p^2)^y(1-p+p^2)^{1-y}(1-\pi)][\pi^{\alpha-1}(1-\pi)^{\beta-1}]}{f_Y(y)\mathrm{Beta}(\alpha,\beta)} \\ &= \frac{(2p-p^2)^y(1-p)^{2(1-y)}\pi^\alpha(1-\pi)^{\beta-1} + (p-p^2)^y(1-p+p^2)^{1-y}\pi^{\alpha-1}(1-\pi)^\beta}{f_Y(y)\mathrm{Beta}(\alpha,\beta)} \\ &= \frac{\mathrm{Beta}(\alpha+1,\beta)(2p-p^2)^y(1-p)^{2(1-y)}\pi^\alpha(1-\pi)^{\beta-1}}{f_Y(y)\mathrm{Beta}(\alpha,\beta)\mathrm{Beta}(\alpha+1,\beta)} \\ &\qquad + \frac{\mathrm{Beta}(\alpha,\beta+1)(p-p^2)^y(1-p+p^2)^{1-y}\pi^{\alpha-1}(1-\pi)^\beta}{f_Y(y)\mathrm{Beta}(\alpha,\beta)\mathrm{Beta}(\alpha,\beta+1)}\end{aligned}$$

We can rewrite the fractions to see the posterior as a mixture of two Beta distributions.

$$\left(\frac{\mathrm{Beta}(\alpha+1,\beta)(2p-p^2)^y(1-p)^{2(1-y)}}{f_Y(y)\mathrm{Beta}(\alpha,\beta)}\right)\left(\frac{\pi^\alpha(1-\pi)^{\beta-1}}{\mathrm{Beta}(\alpha+1,\beta)}\right) + \left(\frac{\mathrm{Beta}(\alpha,\beta+1)(p-p^2)^y(1-p+p^2)^{1-y}}{f_Y(y)\mathrm{Beta}(\alpha,\beta)}\right)\left(\frac{\pi^{\alpha-1}(1-\pi)^\beta}{\mathrm{Beta}(\alpha,\beta+1)}\right)$$

If we let $A_2(y,p) = \frac{\mathrm{Beta}(\alpha+1,\beta)(2p-p^2)^y(1-p)^{2(1-y)}}{f_Y(y)\mathrm{Beta}(\alpha,\beta)}$ and $B_2(y,p) = \frac{\mathrm{Beta}(\alpha,\beta+1)(p-p^2)^y(1-p+p^2)^{1-y}}{f_Y(y)\mathrm{Beta}(\alpha,\beta)}$, we get our final result for our posterior distribution

$$f_{\Pi|Y}(\pi|y) = A_2(y,p)f_\Pi(\pi|\alpha+1,\beta) + B_2(y,p)f_\Pi(\pi|\alpha,\beta+1)$$

where $$A_2(y,p) = \frac{\mathrm{Beta}(\alpha+1,\beta)(2p-p^2)^y(1-p)^{2(1-y)}}{f_Y(y)\mathrm{Beta}(\alpha,\beta)} = \frac{(2p-p^2)^y(1-p)^{2(1-y)}\alpha\Gamma(\alpha\beta)}{f_Y(y)\Gamma((\alpha+1)\beta)}$$

$$B_2(y,p) = \frac{\mathrm{Beta}(\alpha,\beta+1)(p-p^2)^y(1-p+p^2)^{1-y}}{f_Y(y)\mathrm{Beta}(\alpha,\beta)} = \frac{(p-p^2)^y(1-p+p^2)^{1-y}\beta\Gamma(\alpha\beta)}{f_Y(y)\Gamma((\alpha+1)\beta)}$$

and $$f_Y(y) = (2p-p^2)^y(1-p)^{2(1-y)}\left(\frac{\alpha}{\alpha+\beta}\right) + (p-p^2)^y(1-p+p^2)^{1-y}\left(1-\frac{\alpha}{\alpha+\beta}\right).$$

Taking the expected value of this posterior distribution to generate the Bayesian estimator, we get

$$\begin{aligned}
\mathbb{E}[\Pi|Y=y] &= \int_0^1 \pi f_{\Pi|Y}(\pi|y)\mathrm{d}\pi \\
&= A_2(y,p)\mathbb{E}[\text{Beta}(\alpha+1,\beta)] + B_2(y,p)\mathbb{E}[\text{Beta}(\alpha,\beta+1)] \\
&= A_2(y,p)\left(\frac{\alpha+1}{\alpha+\beta+1}\right) + B_2(y,p)\left(\frac{\alpha}{\alpha+\beta+1}\right)
\end{aligned}$$

3 Accuracy of the Estimators

Now that we have derived estimators for our random response techniques, we need to see how accurate they are. We first start with proving that the estimators are unbiased by showing the difference between the expected value of the estimator and $\bar{a}$ is zero.

Starting with the estimator for the One Question Biased Coin technique, we have

$$\begin{aligned}
\mathbb{E}[g_1] - \bar{a} &= \mathbb{E}\left[\frac{\bar{Y}-1+p}{2p-1}\right] - \frac{\bar{y}-1+p}{2p-1} \\
&= \frac{\bar{y}-1+p}{2p-1} - \frac{\bar{y}-1+p}{2p-1} \\
&= 0
\end{aligned}$$

Therefore the estimator for the One Question Biased Coin technique is unbiased. We next look at the estimator for the Two Question Ber(p) technique.

$$\begin{aligned}
\mathbb{E}[g_2] - \bar{a} &= \mathbb{E}\left[\frac{\bar{Y}}{p} - 1 + p\right] - \frac{\bar{y}}{p} - 1 + p \\
&= \left(\frac{\bar{y}}{p} - 1 + p\right) - \left(\frac{\bar{y}}{p} - 1 + p\right) \\
&= 0
\end{aligned}$$

Since both estimators are unbiased, we can measure accuracy by measuring the variance of the estimators.

Variance is a measure of how spread out the observed values of a random variable are. If the variance is low, then the distribution of the random variable is less spread out while a high variance means the data is more spread out. For accuracy, we want the distribution of the values to have little spread and also be close to the actual value. Since the estimators we are using are unbiased, the values will be close to the actual value and so we only need to concern ourselves with the variance.

With any sampling process, there will be some variance that naturally occurs in the process. This is seen with the variance from the direct reporting technique. Recall from equation 1 that

$g_0 = \bar{y}$. Therefore:

$$\mathrm{Var}(\bar{\mathrm{Y}}) = \mathrm{Var}\left(\frac{\sum\limits_{\mathrm{i}=1}^{\mathrm{n}} \mathrm{Y_i}}{\mathrm{n}}\right) = \frac{\mathrm{Var}\left(\sum\limits_{\mathrm{i}=1}^{\mathrm{n}} \mathrm{Y_i}\right)}{n^2}$$

$$\begin{aligned} &= \frac{\sum\limits_{i=1}^{n} \mathrm{Var}(\mathrm{Y_i})}{n^2} \\ &= \frac{n\mathrm{Var}(\mathrm{Y_i})}{n^2} \\ &= \frac{\mathrm{Var}(\mathrm{Y_i})}{n} \end{aligned} \tag{4}$$

Since the Y_i's are Ber(π) distributed, we have $\mathrm{Var}(\mathrm{Y_i}) = \pi(1-\pi)$. Therefore

$$\mathrm{Var}(\mathrm{g_0}) = \frac{\pi(1-\pi)}{\mathrm{n}} \tag{5}$$

We can consider the fact that the distribution of the respondents reported values depends on the distribution of their true values. Therefore we can look at the situation as a hierarchical model which allows us to use the conditional variance identity to resolve the variance of each estimator. "For any two random variables X and Y,

$$\mathrm{Var}(\mathrm{X}) = \mathbb{E}(\mathrm{Var}(\mathrm{X}|\mathrm{Y})) + \mathrm{Var}(\mathbb{E}(\mathrm{X}|\mathrm{Y}))$$

provided that the expectations exist"(Casella & Berger, 2002). This allows us to see the breakdown of the variance of our estimators.

3.1 Variance of the Method of Moment Estimators

Since the method of moment estimators have closed forms, it is easier to introduce the concepts of variance with these estimators.

3.1.1 One Question Biased Coin Variance

We first want to find the variance of the estimator for the One Question Biased Coin method and then resolve it into its parts. Recall from equation 2 that the estimator for this method is $g_1 = \frac{\bar{y}-1+p}{2p-1}$. Therefore

$$\begin{aligned} \mathrm{Var}(\mathrm{g_1}) &= \mathrm{Var}\left(\frac{\bar{\mathrm{Y}}-1+\mathrm{p}}{2\mathrm{p}-1}\right) \\ &= \frac{\mathrm{Var}(\bar{\mathrm{Y}})}{(2p-1)^2} \end{aligned}$$

From equation 4, we now have

$$\mathrm{Var}(\mathrm{g_1}) = \frac{\mathrm{Var}(\mathrm{Y_i})}{\mathrm{n}(2\mathrm{p}-1)^2}$$

Since the Y_i's have distribution $\text{Ber}(\pi p + (1-p)(1-\pi))$, we have

$$\begin{aligned}\text{Var}(\text{g}_1) &= \frac{(\pi p + (1-p)(1-\pi))(1 - \pi p - (1-p)(1-\pi))}{n(2p-1)^2} \\ &= \frac{(\pi p + (1-p)(1-\pi))((1-p)\pi + p(1-\pi))}{n(2p-1)^2}\end{aligned}$$

This gives us an expression for the overall variance for the One Question Biased Coin estimator which is graphed in figure 7. Notice that the variance gets infinitely bigger as p approaches $1/2$. This shows that we cannot get an accurate estimate of $\bar{a}$ if we set p to a value close to $1/2$ which makes sense since if half of the people are not telling the truth, we have scrambled the data so much that we cannot extract the real value. We now want to use the conditional variance identity to break up the expression. We will use $X_1, X_2, \ldots, X_n$ as the true states of the n members of the random sample. For conciseness, let $\tilde{X} = (X_1, X_2, \ldots, X_n)$ and $\tilde{Y} = (Y_1, Y-2, \ldots, Y-n)$. We will first calculate $\text{Var}(\mathbb{E}[\text{g}_1(\tilde{\text{Y}})|\tilde{\text{X}}])$ and then subtract it from the overall variance to obtain $\mathbb{E}[\text{Var}(\text{g}_1(\tilde{\text{Y}})|\tilde{\text{X}}]$.

We start off with finding $\mathbb{E}[g_1(\tilde{Y})|\tilde{X}]$.

$$\begin{aligned}\mathbb{E}\left[\frac{\bar{y} - (1-p)}{2p-1}\middle|\tilde{X}\right] &= \mathbb{E}\left[\frac{\frac{1}{n}\sum y_i - (1-p)}{2p-1}\middle|\tilde{X}\right] \\ &= \frac{\mathbb{E}[\sum Y_i|\tilde{X}]}{n(2p-1)} - \frac{1-p}{2p-1} \\ &= \frac{\sum \mathbb{E}[Y_i|\tilde{X}]}{n(2p-1)} - \frac{1-p}{2p-1}\end{aligned}$$

We now need to find the variance of this expression. The conditional distribution of Y_i depends on what value X_i is taking, and so the conditional distribution for $Y_i|X_i = 1$ is $\text{Ber}(p)$ whereas the conditional distribution for $Y_i|X_i = 0$ is $\text{Ber}(1-p)$. Our sample consists of n_1 $\text{Ber}(p)$ distributed random variables and n_2 $\text{Ber}(1-p)$ distributed random variables where n_1 and n_2 are unknown. However, since the variance of both of these distributions is the same, namely $p(1-p)$, the values

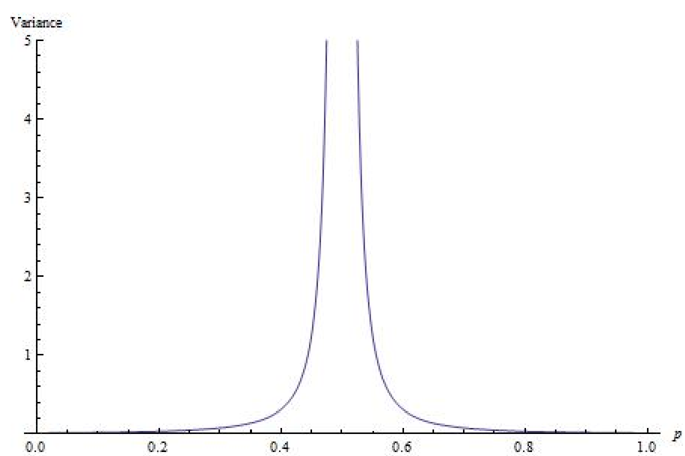


Figure 7: Graph of the variance for the One Question Biased Coin estimator. $n = 20$

of n_1 and n_2 are not necessary in calculating the variance of g_1. Therefore

$$\begin{aligned}
\mathrm{Var}(\mathbb{E}[\mathrm{g_1}(\tilde{\mathrm{Y}})|\tilde{\mathrm{X}}]) &= \mathrm{Var}\left(\frac{\sum \mathbb{E}[\mathrm{Y_i}|\mathrm{X_i} = \mathrm{x_i}]}{\mathrm{n}(2\mathrm{p}-1)} - \frac{1-\mathrm{p}}{2\mathrm{p}-1}\right) \\
&= \frac{1}{n^2(2p-1)^2}\sum_{i-1}^{n} \mathrm{Var}(\mathbb{E}[\mathrm{Y_i}|\mathrm{X_i} = \mathrm{x_i}]) \\
&= \frac{np(1-p)}{n^2(2p-1)^2} \\
&= \frac{p(1-p)}{n(2p-1)^2}
\end{aligned}$$

We now take this expression and subtract it from the total variance to get $\mathbb{E}[\mathrm{Var}(\mathrm{g_1}(\tilde{\mathrm{Y}})|\tilde{\mathrm{X}}]$.

$$\frac{(\pi p + (1-p)(1-\pi))((1-p)\pi + p(1-\pi))}{n(2p-1)^2} - \frac{p(1-p)}{n(2p-1)^2} = \frac{\pi(1-\pi)}{n}$$

We notice that this last expression is equal to the variance of the direct reporting and so it is the variance that occurs from the sampling process. That means the other expression $\frac{p(1-p)}{n(2p-1)^2}$ is the variability due to the randomization process.

3.1.2 Two Question Ber(p) Variance

For the Two Question Ber(p) variance, we will employ the same strategy that was used for the One Question Biased Coin. We first start with finding the overall variance of the estimator, and then use the conditional variance identity to break the expression up.

Recall from equation 3 that the estimator for the Two Question Ber(p) strategy is $g_2 = \frac{\bar{y}}{p} - 1 + p$. Therefore

$$\begin{aligned}
\mathrm{Var}(\mathrm{g_2}) &= \mathrm{Var}\left(\frac{\bar{\mathrm{Y}}}{\mathrm{p}} - 1 + \mathrm{p}\right) \\
&= \frac{\mathrm{Var}(\bar{\mathrm{Y}})}{p^2}
\end{aligned}$$

Using equation 4, we get

$$\mathrm{Var}(\mathrm{g_2}) = \frac{\mathrm{Var}(\mathrm{Y_i})}{\mathrm{np}^2}$$

Since the overall distribution of the Y_i's in this strategy is Ber$(\pi p + p - p^2)$, we get

$$\mathrm{Var}(\mathrm{g_2}) = \frac{(\pi\mathrm{p} + \mathrm{p} - \mathrm{p}^2)(1 - \pi\mathrm{p} - \mathrm{p} + \mathrm{p}^2)}{\mathrm{np}^2}$$

This gives us an expression for the overall variance for the Two Question Ber(p) estimator which is graphed in figure 8. Notice that the variance gets infinitely bigger as p approaches 0. This shows that we cannot get an accurate measure of $\bar{a}$ if we set p to a value close to 0 which makes sense since if p is close to 0, most of the responses given will be noise since they will be answering the second question and not the first. We now want to use the conditional variance identity to break up the expression. We will first calculate $\mathbb{E}[\mathrm{Var}(\mathrm{g_2}(\tilde{\mathrm{Y}})|\tilde{\mathrm{X}}]$ and then subtract it from the overall variance to obtain $\mathrm{Var}(\mathbb{E}[\mathrm{g_2}(\tilde{\mathrm{Y}})|\tilde{\mathrm{X}})$.

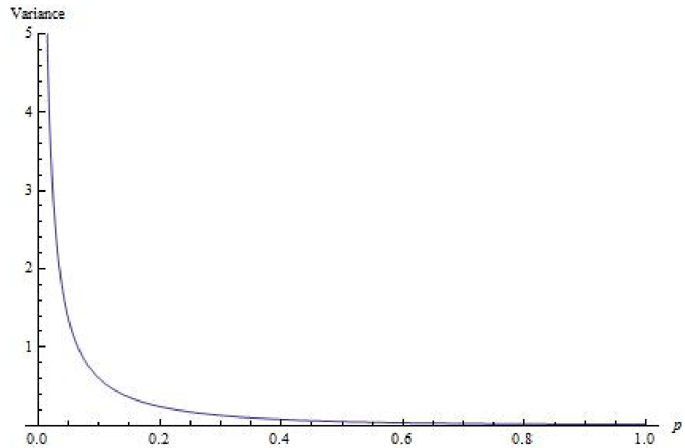


Figure 8: Graph of the variance for the Two Question Ber(p) estimator. $n = 20$

We start with finding $\mathrm{Var}(\mathrm{g_2}(\tilde{\mathrm{Y}})|\tilde{\mathrm{X}})$.

$$\begin{aligned}\mathrm{Var}(\mathrm{g_2}(\tilde{\mathrm{Y}})|\tilde{\mathrm{X}}) &= \mathrm{Var}\left(\frac{\bar{\mathrm{Y}}}{\mathrm{p}} - 1 + \mathrm{p}\middle|\tilde{\mathrm{X}}\right)\\ &= \frac{\mathrm{Var}(\bar{\mathrm{Y}}|\tilde{\mathrm{X}})}{p^2}\\ &= \frac{\mathrm{Var}(\sum \mathrm{Y_i}|\tilde{\mathrm{X}})}{n^2p^2}\\ &= \frac{\sum_{i=1}^{n} \mathrm{Var}(\mathrm{Y_i}|\tilde{\mathrm{X}})}{n^2p^2}\end{aligned}$$

At this stage we can replace $\mathrm{Var}(\mathrm{Y_i}|\tilde{\mathrm{X}})$ with $\mathrm{Var}(\mathrm{Y_i}|\mathrm{X_i})$ since each observed value only is affected by the true state of that individual and no others. Therefore $\mathrm{Var}(\mathrm{g_2}(\tilde{\mathrm{Y}})|\tilde{\mathrm{X}}) = \frac{\sum \mathrm{Var}(\mathrm{Y_i}|\mathrm{X_i})}{\mathrm{n^2p^2}}$.

We now need expressions for the variance of the Y_i's. When $x_i = 0$, the conditional distribution is $\mathrm{Ber}(p(1-p))$ and when $x_i = 1$ the conditional distribution is $\mathrm{Ber}(p(2-p))$. Unlike the One Question Biased Coin strategy, the variance of these two conditional distributions are not equal, so we will have to split the data into two smaller sets, one where $x_i = 1$ and the other where $x_i = 0$. Let n_1 be the number of individuals in the first subset and U_1 be a $\mathrm{Ber}(p(1-p))$ distributed random variable. Similarly, let n_2 be the number of individuals in the second subset and U_2 be a $\mathrm{Ber}(p(2-p))$ distributed random variable.

We can now split the sum of the variances into the two subsets to get

$$\frac{\sum_{i=1}^{n} \mathrm{Var}(\mathrm{Y_i}|\mathrm{X_i})}{n^2p^2} = \frac{n_1\mathrm{Var}\mathrm{U_1}}{n^2p^2} + \frac{n_2\mathrm{Var}(\mathrm{U_2})}{n^2p^2}$$

Since n_1 is the number of individuals who have $x_i = 1$, then n_1/n is the proportion of the sample who have $x_i = 1$ and therefore $n_1/n = \bar{X}$. Furthermore since n_2 is the number of individuals who have $x_i = 0$, then n_2/n is the proportion of the sample who have $x_i = 0$ and therefore $n_2/n = 1-\bar{X}$.

Using this and substituting the variance of the conditional distributions we get

$$\begin{aligned}
\mathrm{Var}(\mathrm{g_2}(\tilde{\mathrm{Y}}|\tilde{\mathrm{X}}) &= \frac{n_1\mathrm{VarU_1}}{n^2p^2} + \frac{n_2\mathrm{Var(U_2)}}{n^2p^2} \\
&= \frac{\bar{X}p(2-p)(1-p(2-p))}{np^2} + \frac{(1-\bar{X}p(1-p)(1-p(1-p))}{np^2} \\
&= \frac{\bar{X}(2-p)(1-p(2-p))}{np} + \frac{(1-\bar{X}(1-p)(1-p(1-p))}{np}
\end{aligned}$$

We now take the expected value of this to get

$$\mathbb{E}[\mathrm{Var}(\mathrm{g_2}(\tilde{\mathrm{Y}})|\tilde{\mathrm{X}}] = \frac{\pi(2-\mathrm{p})(1-\mathrm{p}(2-\mathrm{p}))}{\mathrm{np}} + \frac{(1-\pi(1-\mathrm{p})(1-\mathrm{p}(1-\mathrm{p}))}{\mathrm{np}}$$

Subtracting this from the overall variance gives us

$$\frac{(\pi p + p - p^2)(1-\pi p - p + p^2)}{np^2} - \frac{\pi(2-p)(1-p(2-p))}{np} - \frac{(1-\pi(1-p)(1-p(1-p))}{np} = \frac{\pi(1-\pi)}{n}$$

Just like the One Question Biased Coin strategy, we notice that this last expression is equal to the variance of the direct reporting and so it is the variance that occurs from the sampling process. That means the other expression $\frac{\pi(2-p)(1-p(2-p))}{np} + \frac{(1-\pi(1-p)(1-p(1-p))}{np}$ is the variability due to the randomization process.

3.2 Variance of Bayesian Posterior Distribution

For the variance of the Bayesian posterior distributions, we are looking to calculate $\mathrm{Var}(f_{\Pi|Y}(\pi|y)$. Looking back at the posterior distributions found for the One Question Biased Coin method and the Two Question Ber(p) method we see that both distributions have the same form:

$$A(y,p)f_\Pi(\pi|\alpha+1,\beta) + B(y,p)f_\Pi(\pi|\alpha,\beta+1)$$

We see that this is a weighted sum of two beta distribution, so when we calculate the variance, we will have a weighted sum of the variance of beta distributions. The variance of a beta distribution is $\mathrm{Var}(\mathrm{Beta}(\alpha,\beta)) = \frac{\alpha\beta}{(\alpha+\beta)^2(\alpha+\beta+1)}$. Therefore the variance of the posterior distribution is

$$\begin{aligned}
\mathrm{Var}(f_{\Pi|Y}(\pi|y)) &= \mathrm{Var}(A(y,p)f_\Pi(\pi|\alpha+1,\beta) + B(y,p)f_\Pi(\pi|\alpha,\beta+1)) \\
&= A(y,p)\mathrm{Var}(f_\Pi(\pi|\alpha+1,\beta)) + B(y,p)\mathrm{Var}(f_\Pi(\pi|\alpha,\beta+1)) \\
&= A(y,p)\left(\frac{(\alpha+1)\beta}{(\alpha+\beta+1)^2(\alpha+\beta+2)}\right) + B(y,p)\left(\frac{\alpha(\beta+1)}{(\alpha+\beta+1)^2(\alpha+\beta+2)}\right)
\end{aligned}$$

Hence we have the variance of the Bayesian posterior distribution for the One Question Biased Coin technique is

$$A(y,p)\left(\frac{(\alpha+1)\beta}{(\alpha+\beta+1)^2(\alpha+\beta+2)}\right) + B(y,p)\left(\frac{\alpha(\beta+1)}{(\alpha+\beta+1)^2(\alpha+\beta+2)}\right)$$

where
$$\begin{aligned}
A(y,p) &= \frac{\mathrm{Beta}(\alpha+1,\beta)p^y(1-p)^{1-y}}{f_Y(y)\mathrm{Beta}(\alpha,\beta)} = \frac{p^y(1-p)^{1-y}\alpha\Gamma(\alpha\beta)}{f_Y(y)\Gamma((\alpha+1)\beta)} \\
B(y,p) &= \frac{\mathrm{Beta}(\alpha,\beta+1)p^{1-y}(1-p)^y}{f_Y(y)\mathrm{Beta}(\alpha,\beta)} = \frac{p^{1-y}(1-p)^y\beta\Gamma(\alpha\beta)}{f_Y(y)\Gamma((\alpha+1)\beta)}
\end{aligned}$$

and
$$f_Y(y) = p^y(1-p)^{1-y}\left(\frac{\alpha}{\alpha+\beta}\right) + p^{1-y}(1-p)^y\left(1-\frac{\alpha}{\alpha+\beta}\right).$$

We also have that the variance of the Bayesian posterior distribution for the Two Question Ber(p) technique is

$$A(y,p)\left(\frac{(\alpha+1)\beta}{(\alpha+\beta+1)^2(\alpha+\beta+2)}\right)+B(y,p)\left(\frac{\alpha(\beta+1)}{(\alpha+\beta+1)^2(\alpha+\beta+2)}\right)$$

where $$A(y,p)=\frac{\text{Beta}(\alpha+1,\beta)(2p-p^2)^y(1-p)^{2(1-y)}}{f_Y(y)\text{Beta}(\alpha,\beta)}=\frac{(2p-p^2)^y(1-p)^{2(1-y)}\alpha\Gamma(\alpha\beta)}{f_Y(y)\Gamma((\alpha+1)\beta)}$$

$$B(y,p)=\frac{\text{Beta}(\alpha,\beta+1)(p-p^2)^y(1-p+p^2)^{1-y}}{f_Y(y)\text{Beta}(\alpha,\beta)}=\frac{(p-p^2)^y(1-p+p^2)^{1-y}\beta\Gamma(\alpha\beta)}{f_Y(y)\Gamma((\alpha+1)\beta)}$$

and $$f_Y(y)=(2p-p^2)^y(1-p)^{2(1-y)}\left(\frac{\alpha}{\alpha+\beta}\right)+(p-p^2)^y(1-p+p^2)^{1-y}\left(1-\frac{\alpha}{\alpha+\beta}\right).$$

4 Level of Privacy Protection

The main reason random response techniques were introduced was to make respondents more at ease with being truthful by preserving their privacy. If the interviewer or a third party cannot determine an individuals true state, then that individual will feel more secure and comfortable with the interviewing process. There are many interpretations on what privacy protection is though and so there are many different ways to measure it. For this research, we began measuring the level of privacy protection by using Shannon entropy. From there we moved on to using mutual information and relative entropy. There are still more ways of measuring privacy which will be further explored in the next phase of this research.

4.1 Entropy

Random response techniques preserve the privacy of individual respondents by introducing noise to the data. The initial thought for how to measure privacy protection afforded by these techniques was to measure the uncertainty associated with the observed values, Y_i. Claude Shannon introduced information entropy as a measure of the average uncertainty of a scheme. Shannon entropy is defined as follows.

$$H(X)=\mathbb{E}[-\log_2 \mathrm{X}]=\sum_{\mathrm{x}\in\mathrm{X}}-\mathrm{f(x)}\log_2\mathrm{f(x)}$$

where $f(x)$ is the probability mass function or probability density function (Cover & Thomas, 2006).

For both of our strategies, there are only two values that Y_i can take, namely 0 and 1. Therefore the entropy function will be

$$H(Y)=-\mathbb{P}(Y=0)\log_2\mathbb{P}(\mathrm{Y}=0)-\mathbb{P}(\mathrm{Y}=1)\log_2\mathbb{P}(\mathrm{Y}=1)$$

In sections 1.1 and 1.2, we already calculated $\mathbb{P}(Y=1)$ and $\mathbb{P}(Y=0)$ for both strategies. Using those expressions we get the entropy for the One Question Biased Coin strategy to be

$$H(Y)=-(p\pi+(1-p)(1-\pi))\log_2[\mathrm{p}\pi+(1-\mathrm{p})(1-\pi)]-((1-\mathrm{p})\pi+\mathrm{p}(1-\pi))\log_2[(1-\mathrm{p})\pi+\mathrm{p}(1-\pi)]$$

and the entropy for the Two Question Ber(p) strategy to be

$$H(Y)=-(p\pi+p(1-p))\log_2(\mathrm{p}\pi+\mathrm{p}(1-\mathrm{p}))-(\mathrm{p}(1-\pi)+(1-\mathrm{p})^2)\log_2(\mathrm{p}(1-\pi)+(1-\mathrm{p})^2)$$

In figures 9 and 10, we see the graphs of both entropies. The entropy of the One Question Biased

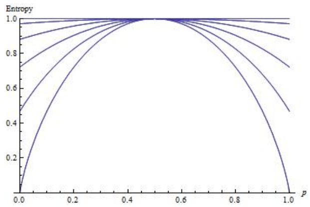


Figure 9: Entropy One Question Biased Coin

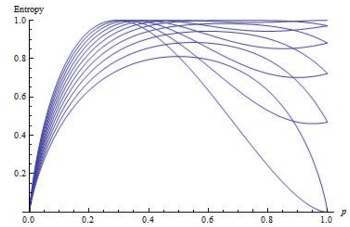


Figure 10: Entropy for Two Question Ber(p).

Coin strategy shows what we expect, that the highest level of entropy occurs when $p = 1/2$ and the lowest level of entropy occurs when $p = 0$ since everyone will be lying and $p = 1$ since everyone will be telling the truth. However the entropy of the Two Question Ber(p) strategy has a feature that doesn't make sense. When $p = 0$ in the Two Question Ber(p) strategy, everyone will be answering the second question, which means the only information we obtain is about the second coin flips. We gain no information about the attribute in question so the privacy level should be at the highest. However, looking at figure 10, we see that the entropy is the lowest at $p = 0$. Since entropy is measuring uncertainty as to which value Y_i will take on, it makes sense that the entropy at $p = 0$ should be low since Y_i will always be 0. We know what value Y_i will always take on so there is no uncertainty. What this means is that Shannon entropy is not measuring what we need to measure.

4.2 Mutual Information

Since Shannon entropy does not measure what we need to measure, we need to come up with another measure for privacy protection. One interpretation for privacy protection is that if the interviewer, or some third party knows the observed Y_i value, how much information does that give him about the respondents true value A_i. If it gives very little information then we can say the respondents privacy is preserved while if knowing Y_i gives a lot of information about A_i then privacy is not well preserved. This idea is measured with mutual information.

We first look at the definition of mutual information given by Paul E. Pfeiffer. The mutual information in two events A and B is given by the expression

$$g(A : B) = \log_2 \frac{\mathbb{P}(\mathrm{AB})}{\mathbb{P}(\mathrm{A})\mathbb{P}(\mathrm{B})} \qquad \text{(in bits)}$$

This expression can also be written as

$$g(A : B) = \log_2 \frac{\mathbb{P}(\mathrm{A|B})}{\mathbb{P}(\mathrm{A})} = \log_2 \frac{\mathbb{P}(\mathrm{B|A})}{\mathbb{P}(\mathrm{B})}$$

(Pfeiffer, 1978). Some properties of mutual information appear from these expressions. In the first expression, we can note that mutual information is symmetric, meaning $g(A : B) = g(B : A)$. Secondly, from the two other expressions we can see that mutual information can take on any value both positive and negative depending on whether $\mathbb{P}(A|B) > \mathbb{P}(A)$ or $\mathbb{P}(A|B) < \mathbb{P}(A)$ What this tells us is that if mutual information is positive then knowing event B occurred raises our sense for the likelihood that event A will occur. Furthermore, if mutual information is negative then knowing event B occurred reduces our sense for the likelihood that event A will occur. For both of the random response techniques, we want to calculate $g(A = 1 : Y = 1)$, $g(A = 1 : Y = 0)$, $g(A = 0 : Y = 1)$, and $g(A = 0 : Y = 0)$.

We then look at Thomas Cover and Joy Thomas' definition of mutual information.

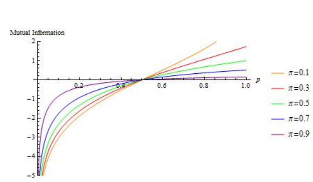
$$I(X;Y) = \sum_{x,y} p(x,y)\log_2 \frac{\mathrm{p(x|y)}}{\mathrm{p(x)}}$$

(Cover & Thomas, 2006). We can see that this definition of mutual information is a weighted average of the individual mutual information's defined by Pfeiffer. We will calculate this as well to see the overall trend in mutual information. While analyzing mutual information, we will not concern ourselves with the sign of the mutual information. Instead, we will only focus on the absolute value. We don't care if knowing Y_i decreases the chance that $A_i = 1$. Instead we care about how strongly it influences our sense that $A_i = 1$

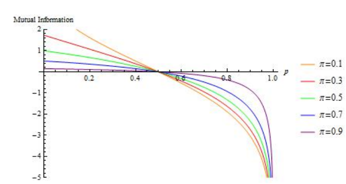
4.2.1 One Question Biased Coin Mutual Information

Calculating the mutual information for the One Question Biased coin technique, we get:

$$g(A=1:Y=1) = \log_2 \frac{\mathrm{p}}{(1-\mathrm{p})(1-\pi)+\mathrm{p}\pi}$$
$$g(A=1:Y=0) = \log_2 \frac{(1-\mathrm{p})}{\mathrm{p}+\pi-2\mathrm{p}\pi}$$
$$g(A=0:Y=1) = \log_2 \frac{1-\mathrm{p}}{(1-\mathrm{p})(1-\pi)+\mathrm{p}\pi}$$
$$g(A=0:Y=0) = \log_2 \frac{(\mathrm{p})}{\mathrm{p}+\pi-2\mathrm{p}\pi}$$
$$\begin{aligned} I(A;Y) = {} & p(1-\pi)\log_2 \frac{\mathrm{p}}{\mathrm{p}+\pi-2\mathrm{p}\pi} + \pi(1-\mathrm{p})\log_2 \frac{1-\mathrm{p}}{\mathrm{p}+\pi-2\mathrm{p}\pi} \\ & + (1-p)(1-\pi)\log_2 \frac{1-\mathrm{p}}{(1-\mathrm{p})(1-\pi)+\mathrm{p}\pi} + \mathrm{p}\pi\log_2 \frac{\mathrm{p}}{(1-\mathrm{p})(1-\pi)+\mathrm{p}\pi} \end{aligned}$$

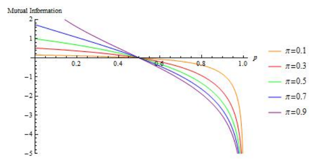


$g(A=1:Y=1) = \log_2 \frac{\mathrm{p}}{(1-\mathrm{p})(1-\pi)+\mathrm{p}\pi}$

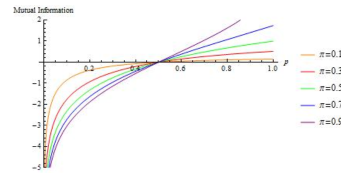


$g(A=1:Y=0) = \log_2 \frac{(1-\mathrm{p})}{\mathrm{p}+\pi-2\mathrm{p}\pi}$

Figure 11, we see the graphs of mutual information. We notice in all the graphs of mutual information that at $p = 1/2$, the mutual information is 0, and when p approaches 0 or 1, the absolute value of mutual information increases. The behavior in the graphs match what we predict from the One Question Biased Coin strategy. When p is set to 1/2, there is no way for us to extract any information about A_i and so knowing Y_i tells us nothing. On the other hand, if p is set to 1, everyone is telling the truth so we gain a lot of information from Y_i and when p is set to 0, everyone is lying so again Y_i gives us a lot of information.



$g(A=0:Y=1)=\log_2\frac{1-\mathrm{p}}{(1-\mathrm{p})(1-\pi)+\mathrm{p}\pi}$



$g(A=0:Y=0)=\log_2\frac{(\mathrm{p})}{\mathrm{p}+\pi-2\mathrm{p}\pi}$

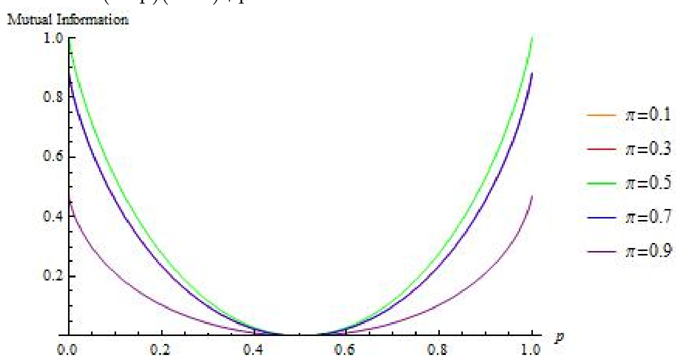


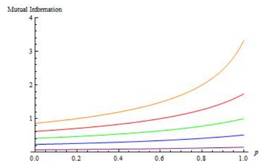
Figure 11: Average mutual information for the One Question Biased Coin strategy

4.2.2 Two Question Ber(p) Mutual Information

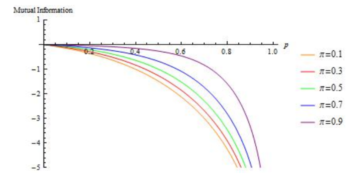
Calculating the mutual information for the Two Question Ber(p) technique, we get:

$$g(A=1:Y=1)=\log_2\frac{\mathrm{p}(2-\mathrm{p})}{\pi\mathrm{p}+\mathrm{p}-\mathrm{p}^2}$$
$$g(A=1:Y=0)=\log_2\frac{(1-\mathrm{p})^2}{1-\mathrm{p}+\mathrm{p}^2\pi\mathrm{p}}$$
$$g(A=0:Y=1)=\log_2\frac{(1-\mathrm{p})\mathrm{p}}{\pi\mathrm{p}+\mathrm{p}-\mathrm{p}^2}$$
$$g(A=0:Y=0)=\log_2\frac{\mathrm{p}+(1-\mathrm{p})^2}{1-\mathrm{p}+\mathrm{p}^2\pi\mathrm{p}}$$
$$\begin{aligned}I(A;Y)=(1-\pi)(1-p+p^2)\log_2\frac{\mathrm{p}+(1-\mathrm{p})^2}{1-\mathrm{p}+\mathrm{p}^2\pi\mathrm{p}}+\pi(1-\mathrm{p})^2\log_2\frac{(1-\mathrm{p})^2}{1-\mathrm{p}+\mathrm{p}^2\pi\mathrm{p}}\\+p(1-p)(1-\pi)\log_2\frac{(1-\mathrm{p})\mathrm{p}}{\pi\mathrm{p}+\mathrm{p}-\mathrm{p}^2}+\mathrm{p}\pi(2-\mathrm{p})\log_2\frac{\mathrm{p}(2-\mathrm{p})}{\pi\mathrm{p}+\mathrm{p}-\mathrm{p}^2}\end{aligned}$$

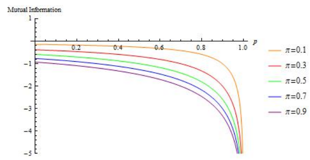
In figure 12, we see the graphs of mutual information. We note that as p approaches 0, the absolute value of the mutual information decreases, and in many instances approaches 0. This matches what our scenario for the Two Question Ber(p) strategy since respondents are answering the second question rather than the first question, so Y_i is giving us no information on the status of A_i. As p increases, more and more respondents are answering question 1 and so the Y_i's are giving us a lot of information about the status of the A_i's.



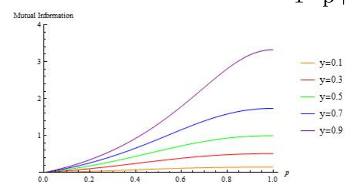
$g(A=1:Y=1)=\log_2\frac{\mathrm{p(2-p)}}{\mathrm{\pi p+p-p^2}}$



$g(A=1:Y=0)=\log_2\frac{\mathrm{(1-p)^2}}{\mathrm{1-p+p^2\pi p}}$



$g(A=0:Y=1)=\log_2\frac{\mathrm{(1-p)p}}{\mathrm{\pi p+p-p^2}}$



$g(A=0:Y=0)=\log_2\frac{\mathrm{p+(1-p)^2}}{\mathrm{1-p+p^2\pi p}}$

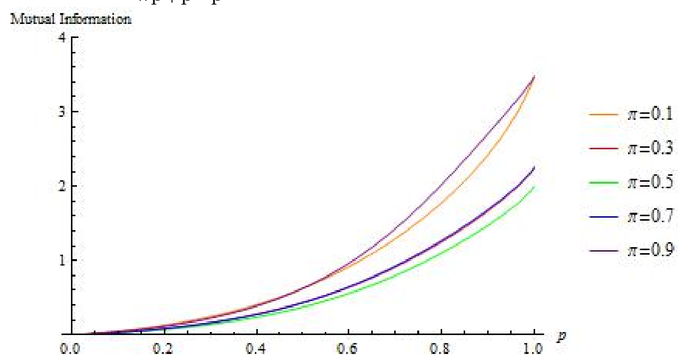


Figure 12: Average mutual information for the Two Question Ber(p) strategy

4.3 Conditional Entropy

Another way of looking at privacy preservation is looking at how much additional information is needed to determine the value of A_i knowing Y_i. In other words, how much uncertainty do we still have of the value of A_i if we know Y_i This is very closely related to the idea brought up for mutual information. In this case, we use conditional entropy to measure the privacy protection. If the conditional entropy is high, there is a lot of uncertainty and therefore a higher level of privacy protection. If the conditional entropy is low, there is less uncertainty and therefore a lower level of privacy protection. Cover and Thomas define conditional entropy as:

$$H(Y|X)=-\mathbb{E}[\log_2\mathbb{P}(\mathrm{Y|X})]=-\sum_{\mathrm{x,y}}\mathrm{p(x,y)\log_2 p(y|x)}$$

(Cover & Thomas, 2006) This expression gives the average conditional entropy. For our two random response techniques, the expression will be

$$H(A|Y)=-\sum_{a,y}p(a,y)\log_2\mathrm{p(a|y)}=-\sum_{\mathrm{a,y}}\mathrm{p(a,y)}\log_2\frac{\mathrm{p(a,y)}}{\mathrm{p(y)}}$$

We need to adjust the expression to the final form since we do not have an expression for $\mathbb{P}(A|Y)$. Like the mutual information, we can also find the individual conditional entropy for the four different scenarios by calculating $-\log_2\frac{\mathrm{p(A=a,Y=y)}}{\mathrm{p(Y=y)}}$.

4.3.1 One Question Biased Coin Conditional Entropy

Calculating the conditional entropy for the One Question Biased Coin technique, we get

$$H(A=1|Y=1) = -\log_2 \frac{\mathrm{p}\pi}{1-\mathrm{p}-\pi+2\mathrm{p}\pi}$$

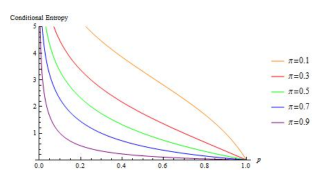
$$H(A=1|Y=0) = -\log_2 \frac{\pi(1-\mathrm{p})}{\mathrm{p}+\pi-2\mathrm{p}\pi}$$

$$H(A=0|Y=1) = -\log_2 \frac{(1-\pi)(1-\mathrm{p})}{1-\mathrm{p}-\pi+2\mathrm{p}\pi}$$

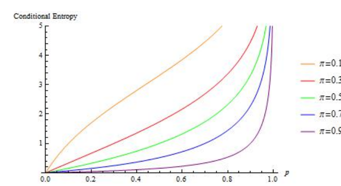
$$H(A=0|Y=0) = -\log_2 \frac{\mathrm{p}(1-\pi)}{\mathrm{p}+\pi-2\mathrm{p}\pi}$$

$$\begin{aligned} H(A|Y) = &-p(1-\pi)\log_2 \frac{\mathrm{p}(1-\pi)}{\mathrm{p}+\pi-2\mathrm{p}\pi} - \pi(1-\mathrm{p})\log_2 \frac{\pi(1-\mathrm{p})}{\mathrm{p}+\pi-2\mathrm{p}\pi} \\ &-(1-p)(1-\pi)\log_2 \frac{(1-\pi)(1-\mathrm{p})}{1-\mathrm{p}-\pi+2\mathrm{p}\pi} - \mathrm{p}\pi\log_2 \frac{\mathrm{p}\pi}{1-\mathrm{p}-\pi+2\mathrm{p}\pi} \end{aligned}$$

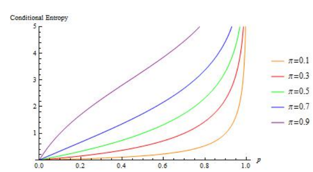
When looking at the individual scenario conditional entropy graphs in figure 13, we notice that



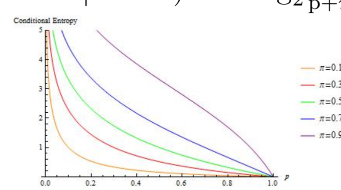
$H(A=1|Y=1) = -\log_2 \frac{\mathrm{p}\pi}{1-\mathrm{p}-\pi+2\mathrm{p}\pi}$



$H(A=1|Y=0) = -\log_2 \frac{\pi(1-\mathrm{p})}{\mathrm{p}+\pi-2\mathrm{p}\pi}$



$H(A=0|Y=1) = -\log_2 \frac{(1-\pi)(1-\mathrm{p})}{1-\mathrm{p}-\pi+2\mathrm{p}\pi}$



$H(A=0|Y=0) = -\log_2 \frac{\mathrm{p}(1-\pi)}{\mathrm{p}+\pi-2\mathrm{p}\pi}$

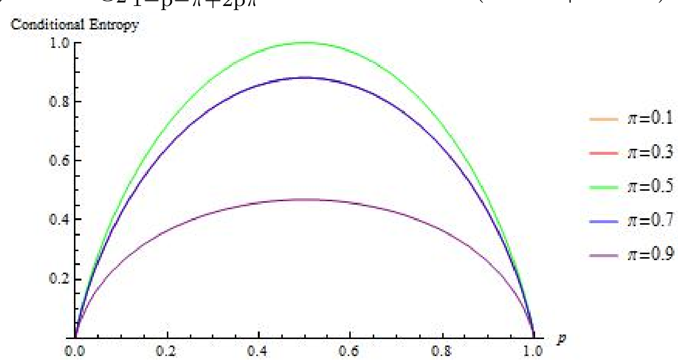


Figure 13: Conditional entropy for the One Question Biased Coin strategy

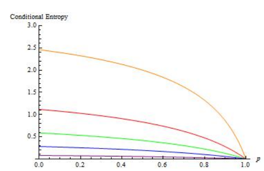
one side of the graph always approaches 0 while the other side increases. It isn't until we average the conditional entropy's where we see the shape that we were looking for. We have the highest entropy when $p = 1/2$ which is what we are looking for, and when $p = 0$ and $p = 1$, the conditional entropy is 0 which also matches our expectations.

4.3.2 Two Question Ber(p) Conditional Entropy

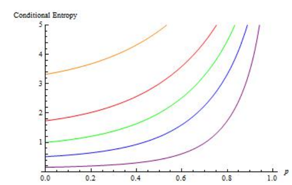
Calculating the conditional entropy for the One Question Biased Coin technique, we get:

$$H(A=1|Y=1) = -\log_2 \frac{\mathrm{p}\pi(2-\mathrm{p})}{1-\mathrm{p}-\pi+2\mathrm{p}\pi}$$
$$H(A=1|Y=0) = -\log_2 \frac{\pi(1-\mathrm{p})^2}{\mathrm{p}-\mathrm{p}^2+\mathrm{p}\pi}$$
$$H(A=0|Y=1) = -\log_2 \frac{(1-\pi)(1-\mathrm{p})\mathrm{p}}{\mathrm{p}-\mathrm{p}^2+\mathrm{p}\pi}$$
$$H(A=0|Y=0) = -\log_2 \frac{(1-\pi)(1-\mathrm{p}+\mathrm{p}^2)}{1-\mathrm{p}+\mathrm{p}^2-\mathrm{p}\pi}$$
$$\begin{aligned} H(A|Y) = &-(1-\pi)(1-p+p^2)\log_2 \frac{(1-\pi)(1-\mathrm{p}+\mathrm{p}^2)}{1-\mathrm{p}+\mathrm{p}^2-\mathrm{p}\pi} - \pi(1-\mathrm{p})^2\log_2 \frac{\pi(1-\mathrm{p})^2}{\mathrm{p}-\mathrm{p}^2+\mathrm{p}\pi} \\ &- (1-\pi)(1-p)p\log_2 \frac{(1-\pi)(1-\mathrm{p})\mathrm{p}}{\mathrm{p}-\mathrm{p}^2+\mathrm{p}\pi} - \mathrm{p}\pi(2-\mathrm{p})\log_2 \frac{\mathrm{p}\pi(2-\mathrm{p})}{1-\mathrm{p}-\pi+2\mathrm{p}\pi} \end{aligned}$$

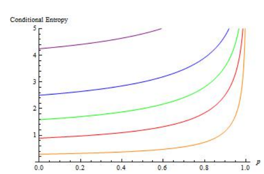
Figure 14 shows the graphs of conditional entropy for the Two Question Ber(p) strategy. The



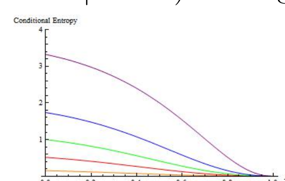
$H(A=1|Y=1) = -\log_2 \frac{\mathrm{p}\pi(2-\mathrm{p})}{1-\mathrm{p}-\pi+2\mathrm{p}\pi}$



$H(A=1|Y=0) = -\log_2 \frac{\pi(1-\mathrm{p})^2}{\mathrm{p}-\mathrm{p}^2+\mathrm{p}\pi}$



$H(A=0|Y=1) = -\log_2 \frac{(1-\pi)(1-\mathrm{p})\mathrm{p}}{\mathrm{p}-\mathrm{p}^2+\mathrm{p}\pi}$



$H(A=0|Y=0) = -\log_2 \frac{(1-\pi)(1-\mathrm{p}+\mathrm{p}^2)}{1-\mathrm{p}+\mathrm{p}^2-\mathrm{p}\pi}$

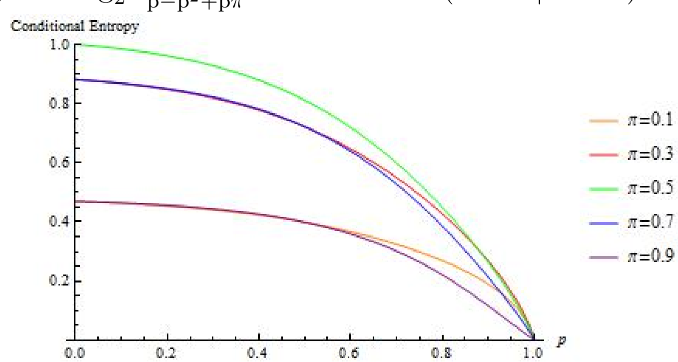


Figure 14: Conditional entropy for the Two Question Ber(p) strategy

highest entropy is obtained when $p = 0$ since none of the respondents are answering the first question, and all observed responses are noise. Also, when $p = 1$ all respondents are answering the first question truthfully and therefore there is no uncertainty as to their true value. These features are seen in the graph of the average conditional entropy. Another aspect of all these measures of privacy which is more apparent in the graphs of figure 14 is the effect that π has on the level of uncertainty. If π is close to 1 or 0, then either almost everyone has the attribute in question or almost no one has the attribute in question, and therefore the amount of uncertainty that we have can't be too high.

References

Casella, G., & Berger, R. L. (2002). *Statistical inference* (2nd Edition ed.). Belmont, CA: Brooks/cole, Cengage Learning.

Cover, T. M., & Thomas, J. A. (2006). *Elements of information theory* (2nd Edition ed.). New Jersey: Wiley.

Pfeiffer, P. E. (1978). *Concepts of probability theory* (2nd Edition ed.). New York, NY: Dover Publications Inc.