A Mixture Binary RRT Model With A Unified Measure Of Privacy And Efficiency

Maxwell Lovig - UL Lafayette

Sumaita Rahman- UNC Greensboro

Mentor: Dr. Sat Gupta

Co-Mentors: Dr. Sadia Khalil, Pujita Sapra

Acknowledgements

The University of North Carolina at Greensboro, for providing us the opportunity to conduct undergraduate research.

NSF for funding us with **NSF grant DMS-1950549**

Outline

- Initial RRT Models
- Proposed Binary Mixture RRT Model
- Privacy Loss and Primary Protection
- Unified Measure of Privacy and Efficiency
- Simulations
- Major Takeways
- Future Work
- References

The Innate Responsibility for Survey Making and Taking

When creating a survey there is a subtle sense of cooperation between two parties: the survey maker and the survey taker. The former makes the rules and the latter decides when to follow them.

The survey maker wants information of its demographic

The survey taker wants their information to be private and secure

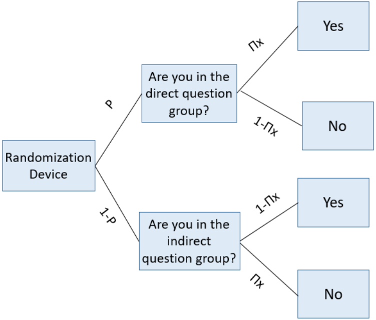
How does RRT accomplish this

Binary RRT (Randomized Response Techniques) effectively randomly changes the yes/no response from a survey taker unbeknownst to the survey maker. This is usually accomplished through a secondary question which occurs at a random rate of 1-p. With the sensitive question (with a true population occurrence at π_x) at probability p.

Sensitive Question:
"Have you purposefully neglected care of your parents?"

Alternate Questions:
"Have you never purposefully neglected care of your parents?"
(Warner's Model)
-OR-
"Is your favorite color blue?
(Greenberg's Model)

Indirect Question Model [Warner, 1965]

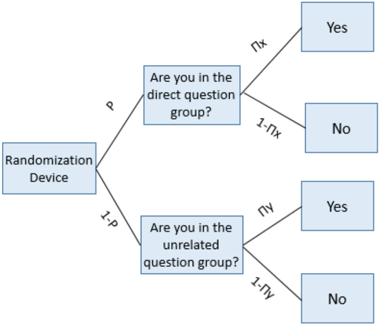


$$P_y = p\pi_x + (1-p)(1-\pi_x)$$

$$\widehat{\pi_x} = \frac{\widehat{P_y} - (1-p)}{2p-1}; p \neq \frac{1}{2}$$

$$Var(\widehat{\pi_x}) = \frac{P_y(1-P_y)}{(n-1)(2p-1)^2}; p \neq \frac{1}{2}$$

Unrelated Question Model [Greenberg et al., 1969]



$$P_y = p\pi_x + (1-p)\pi_y$$

$$\widehat{\pi_x} = \frac{\widehat{P_y} - (1-p)\pi_y}{p}$$

$$Var(\widehat{\pi_x}) = \frac{P_y(1-P_y)}{(n-1)p^2}$$

Untruthfulness even under RRT

Now imagine yourself as a participant of a survey. Of course there is some level of privacy in which you would answer truthfully for. If the survey maker does not provide this level of privacy (i.e. a value of p which is too high) you may still find lying is a viable option and as such RRT will usually never have 100% compliance to instructions.

For example given the following with Greenberg's Model parameters:

n = 500, $\pi_x = .3$, $\pi_y = .1$

p	1-p	A	$\hat{\pi}$	$\widehat{MSE}$	MSE
.5	.5	1	.29984	.00128	.00128
.5	.5	.9	.27023	.00209	.00218
.5	.5	.8	.23967	.00478	.00488
.7	.3	1	.30023	.00076	.00075
.7	.3	.9	.27006	.00160	.00165
.7	.3	.8	.24035	.00424	.00435

Solution to remaining untruthfulness

Proposed by [Young et al., 2019] a primer question was proposed to ask the participant "Do you trust this model" (i.e. would you respond truthfully). As this information itself is sensitive it must also be placed in a RRT survey format.

This extra information gives us a value of A. The proportion of participants who respond truthfully to the instructions of RRT and would not lie with the current parameters in RRT.

The conundrum

Efficiency: The ability for the researcher to get close to the true proportion of π_x, measured by MSE

Privacy: The sense of security in the participant of the survey. This have many diverse measures.

Overall, Greenberg's model tends to have better efficiency measures while Warner's model tends to have better privacy.

So it seems that a "mixture" of the two models would be able to strike a balance in these two categories.

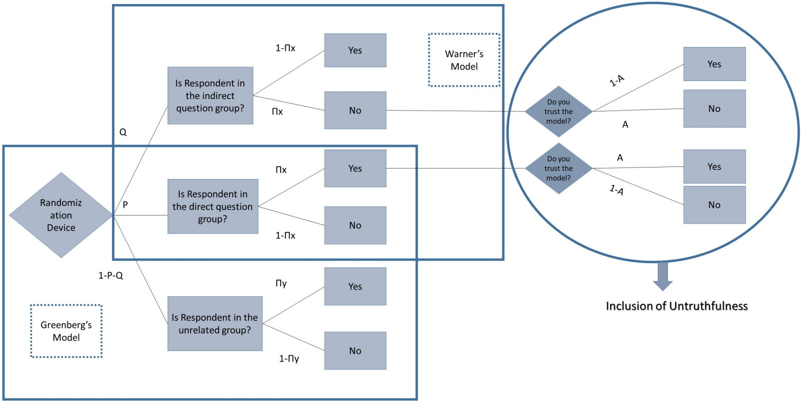


Figure: The Proposed Mixture Model Under Untruthfulness

Derivation of MSE When Estimating for A and π_x

$p_0 =$ The proportion of the direct question used in a Greenberg model to estimate truthfulness.
$\pi_{y0} =$ The proportion of people who would answer yes to the unrelated question in the Greenberg model to estimate A
p, q, π_x, π_y, A are all the same from the introduction of the mixture model

Question 1: (With Greenberg) Do you trust the model?

$$P_{y0} = P_0(Yes) = p_0 A + (1 - p_0)\pi_{y0}$$

$$\hat{A} = \frac{\hat{P}_{y0} - (1 - p_0)\pi_{y0}}{p_0} \tag{1}$$

$$E(\hat{A}) = A,\ Var(\hat{A}) = \frac{P_{y0}(1 - P_{y0})}{(n-1)p_0^2} \tag{2}$$

Question 2: (With Mixture Model) Do you have sensitive trait?

$$P_y = P(Yes) = \pi_x A(p-q) + q + (1-p-q)\pi_y$$

$$\hat{\pi}_x = \frac{\hat{P}_y - q - (1-p-q)\pi_y}{\hat{A}(p-q)};\ p \neq q \tag{3}$$

$$E(\hat{P}_y) = P_y = \pi_x A(p-q) + q + (1-p-q)\pi_y,\ Var(\hat{P}_y) = \frac{P_y(1-P_y)}{(n-1)(p-q)^2};\ p \neq q \tag{4}$$

Then using first order Taylor's approximation, $\hat{\pi_x}$ can be approximated by:

$$\hat{\pi}_x \approx \frac{P_y - q - (1-p-q)\pi_y}{A(p-q)} - (\hat{A}-A)\left[\frac{P_y - q - (1-p-q)\pi_y}{A^2(p-q)}\right] + (\hat{P}_y - P_y)\left[\frac{1}{A(p-q)}\right]] \tag{5}$$

$[where\ p \neq q]$

It is easy to see from (5) that,

$$E(\hat{\pi}_x) = \pi_x$$

$$Var(\hat{\pi}_x) = \left[\frac{P_y - q - (1-p-q)\pi_y}{A^2(p-q)}\right]^2 Var(\hat{A}) + \left[\frac{1}{A(p-q)}\right]^2 Var(\hat{P}_y)$$

$Var(\hat{A})$ is given in (2) and $Var(\hat{P}_y)$ is given in (4)

[Lanke, 1976], in previous work, described privacy loss as,

$$\delta = \mathrm{Max}(\eta_1, \eta_2)$$

$$\eta_1 = Pr(S|Y) = \frac{pA\pi_x + (1-p-q)\pi_x\pi_y + q\pi_x(1-A)}{\pi_x A(p-q) + q + (1-p-q)\pi_y}$$

$$\eta_2 = Pr(S|N) = \frac{qA\pi_x + (1-p-q)(1-\pi_y)\pi_x + p\pi_x(1-A)}{1-[\pi_x A(p-q) + q + (1-p-q)\pi_y]}$$

Result: δ is at its minimum if p = q, min(δ) = π_x

Proof:

$\implies$ Let $p = q$, then

$$P(S|Y) = \frac{\pi_x[pA+(1-p-q)\pi_y+q(1-A)]}{\pi_x A(p-q)+q+(1-p-q)\pi_x} = \pi_x$$

$$P(S|N) = \frac{\pi_x[qA+(1-p-q)(1-\pi_y)+p(1-A)]}{\pi_x A(q-p)+p+(1-p-q)(1-\pi_y)} = \pi_x$$

$$\text{Hence } \delta = \pi_x, \ \textit{when } p = q$$

Now Assume,

$\exists p$ and $\exists q$ st. $P(S|Y) < \pi_x$ and $P(S|N) < \pi_x$

$$\implies \frac{P(S \cap Y)}{P(Y)} < \pi_x \text{ and } \frac{P(S \cap N)}{P(N)} < \pi_x$$

$$\implies P(S \cap Y) < \pi_x P(Y) \text{ and } P(S \cap N) < \pi_x P(N)$$

$$\implies P(S \cap Y) + P(S \cap N) < \pi_x P(Y) + \pi_x P(N)$$

$$\implies P(S) < \pi_x$$

This creates a contradiction proving that $Min\ \delta = \pi_x$ and it is attained at $p = q$

Primary Protection

If one wants to transform privacy loss into Primary Protection then the following formula can be applied. This measure was introduced by [Fligner et al., 1977]

$$PP = \frac{1-\delta}{1-\pi_x};$$

$$\delta \in [\pi_x, 1] \textit{ and } \pi_x \in [0, 1]$$

Researchers have to deal with two factors for a RRT model. One factor is the efficiency of the model and another is the Privacy.[Gupta et al., 2018]came up with following Unified Measure of Privacy and Efficiency for RRT model.

$$M = \frac{Var(\hat{\mu_x})}{PL};\ PL = E(Z - Y)^2$$

Proposed Unified Measure

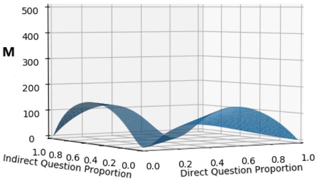
From the concepts of [Lanke, 1976] loss to privacy, [Fligner et al., 1977] Primary Protection and [Gupta et al., 2018] Unified Measure of Privacy and Efficiency, we propose the following Unified Measure,

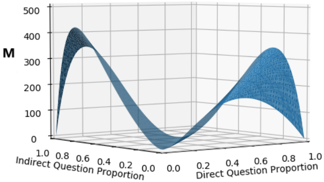
$$\mathbb{M} = \frac{PP}{MSE}$$

Simulations: $\pi_x = .4,\ \pi_y = .1,\ p_0 = .7,\ \pi_{y0} = .1.$

Subscript Meanings:
S - simulated values, T - theoretical values
1 - Accounting A, 2 - Not Accounting A
Rose is Warner's. Blue is Greenberg's, No color is Mixture
Bolded Values are theoretical, non-bolded are empirical

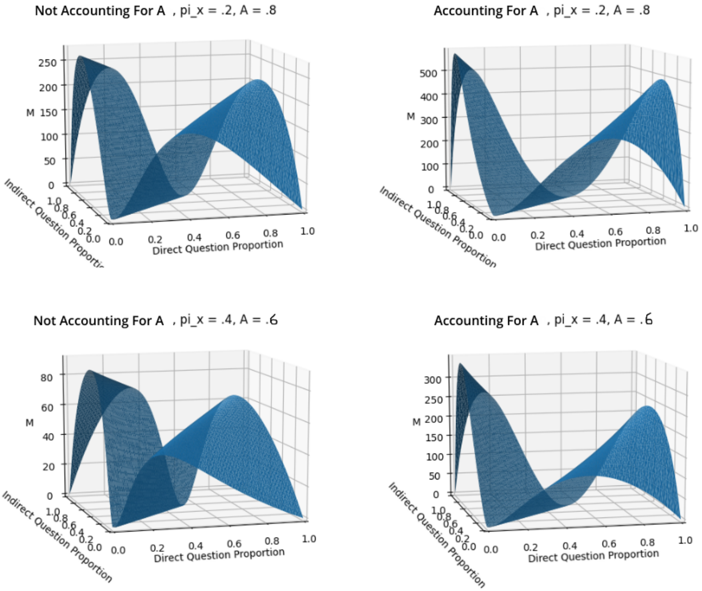
p	q	1-p-q	A	$\hat{\pi}_1$	MSE_1	$\hat{\pi}_2$	MSE_2	PP	M_1	M_2
.4	0	.6	1	.3998	.0023	.3994	.0021	.2726	120.2388	128.1228
					.0023		**.0022**	**.2727**	**119.7078**	**126.8913**
.4	0	.6	.8	.4006	.0031	.3103	.0083	.3190	102.6930	38.6041
					.0032		**.0085**	**.3191**	**98.6590**	**37.3304**
.4	.1	.5	1	.4007	.0044	.4003	.0043	.5556	125.1477	129.8006
					.0045		**.0044**	**.5555**	**122.9716**	**126.5855**
.4	.1	.5	.8	.3997	.0066	.3190	.0107	.6101	92.3568	56.8758
					.0067		**.0108**	**.6097**	**90.9995**	**56.5176**
.4	.6	0	1	.4012	.01275	.4006	.0126	.8331	65.3209	66.3605
					.0126		**.0125**	**.8333**	**65.9596**	**66.6400**
.4	.6	0	.8	.3997	.0193	.3193	.0187	.8617	44.6630	46.0447
					.0197		**.0189**	**.8621**	**43.7237**	**45.6000**
.7	0	.3	1	.3998	.0010	.3997	.0009	.0969	97.0556	110.8450
					.0010		**.0009**	**.0968**	**96.4091**	**110.6230**
.7	0	.3	.8	.4012	.0013	.3206	.0071	.1177	89.9563	16.6216
					.0015		**.0073**	**.1181**	**80.9974**	**16.2355**
.7	.1	.2	1	.4002	.0014	.3999	.0013	.3333	236.6728	258.1805
					.0014		**.0013**	**.3333**	**236.1485**	**259.8958**
.7	.1	.2	.8	.4003	.0020	.3201	.0076	.3850	195.2027	50.6466
					.0021		**.0077**	**.3855**	**181.9029**	**50.0634**
.7	.3	0	1	.4003	.0032	.3999	.0031	.6523	203.5105	211.5794
					.0032		**.0031**	**.6522**	**201.2790**	**209.6190**
.7	.3	0	.8	.3997	.0049	.3194	.0096	.7013	143.3820	73.2478
					.0050		**.0095**	**.7009**	**139.1116**	**73.6955**





Not Accounting for A and Accounting for A Respectively

$$\pi_x = 0.3, \pi_y = 0.1, n = 500, A = 0.80$$


Not Accounting For A , pi_x = .2, A = .8
Accounting For A , pi_x = .2, A = .8
Not Accounting For A , pi_x = .4, A = .6
Accounting For A , pi_x = .4, A = .6
M
Direct Question Proportion
Indirect Question Proportion

$$n = 500,\ \pi_y = .1$$

Given a choice of p there is a corresponding q such that our unified measure is maximized. Meaning we have a good mix of privacy and efficiency. the choice of p is still vital as it is now the main factor for how one avoids large amounts of untruthfulness in models.

Once we choose a p one can begin to find the most optimal mixture of (1-p) between q and 1-p-q for a model with respect to $\mathbb{M}$ with a prior guess of what π_x would be.

Major Takeaways

Of course there are fluctuations where each model is optimized due to π_x, π_y, and if one accounts for A or not, but in General:

- for most values, $\mathbb{M}$ is significantly higher if one accounts for A
- if $p \in [0, .15] \bigcup [.4, .85]$, then the mixture model has a higher $\mathbb{M}$, making it the best choice of a model for a significant portion of p.
- the p $=$ 0 branch results in the highest $\mathbb{M}$ overall, indicating that using only indirect question and unrelated question might be the new standard for RRT
- Of course these results vary with the parameters of the models but the mixed model does have its place as it balances out efficiency and privacy well

Future Work

- Untruthfulness in the unrelated question part of Greenberg Model [Edgell et al., 1982], which can be alleviated by the mixture model
- Mixture Model with Optionality [Gupta et al., 2002]
- Estimating the function of parameters p and q versus levels of untruthfulness to optimize parameters.

Edgell, S. E., Himmelfarb, S., and Duchan, K. L. (1982).
Validity of forced responses in a randomized response model.
Sociological Methods Research, 11(1):89–100.

Fligner, M. A., Policello, G. E., and Singh, J. (1977).
A comparison of two randomized response survey methods with consideration for the level of respondent protection.
Communications in Statistics - Theory and Methods, 6(15):1511–1524.

Greenberg, B. G., Abul-Ela, A.-L. A., Simmons, W. R., and Horwitz, D. G. (1969).
The unrelated question randomized response model: Theoretical framework.
Journal of the American Statistical Association, 64(326):520–539.

Gupta, S., Gupta, B., and Singh, S. (2002).
Estimation of the sensitivity level of personal interview survey questions.
Journal of Statistical Planning and Inference, 100(2):239–247.

Gupta, S., Mehta, S., Shabbir, J., and Khalil, S. (2018).
A unified measure of respondent privacy and model efficiency in quantitative rrt models.
Journal of Statistical Theory and Practice, 12(3):506–511.

Lanke, J. (1976).
On the degree of protection in randomized interviews.
International Statistical Review / Revue Internationale de Statistique, 44(2):197–203.

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

Young, A., Gupta, S., and Parks, R. (2019).
A binary unrelated-question rrt model accounting for untruthful responding.
Involve, 12(7):1163–1173.