model-for-epsilon

August 31, 2022

0.1 Model For Choosing ϵ

0.1.1 Introduction

This notebook tries to implement the model presented in (1) for setting the ϵ and other crucial parameters for a differentially-private study.

It first tries to replicate the results mentioned in the various cost scenarios in Section 5.2 to ensure that we have implemented the model correctly.

Then, it applies the model to the specific use-case under consideration in the report.

The purpose of this is to utilize their model to gain some research insight into the kind of parameter values that might apply in a DP protocol for a mood app.

Derivation of the various key equations can be found in the paper; this notebook will simply identify and highlight the equations that are relevant for determining what values key parameters must take in a given study.

A **few results** from this analysis: (a) a lower bound on N (i.e., how 'large' a dataset must be) for a DP analysis on our use case; (b) a significantly large budget could be required for a mood app that wanted to allow for multiple DP queries; (c) in the case where there is just a single query being made, a DP version of the mood app is cheaper than a non-private version **with some caveats** bearing what is said in the assumptions section and the end.

0.1.2 Summary of Model

Modelling Actual Complexities The model that (1) propose 'provides a principled way to choose reasonable values for and based on parameters with more immediate connections to the real world.' (1, p2). These parameters include the accuracy constraint of a study, the budget analysts have for incentivizing participation, the number of participants that would be required to satisfy a given privacy guarantee…and so on.

Though this model is more complex than the standard one where the sole parameter is ε (and δ in some cases), the authors argue that this complexity (from the greater number of parameters) "is present in the real world". (1, p23) Analysts really do have a budget; individuals really do need to be compensated;… etc. Rather than, rolling up various and distinct considerations into a single parameter ε, this model enables one to more clearly recognize them and consider how they bear on one another. As they put it, their model "forces the user to think quantitatively about how a private study would affect real events" (1, p23)

Description The model considers the imapact of ε and δ on two principal actors in a differentially-private study: the analyst and prospective participants. It can be used to determine the range of acceptable values for both parameters. (1, p2) In this notebook we consider just ε DP and so will not consider the parameter δ.

The differentially-private **study** that a given individual is considering particpation in will be carried out regardless of whether they opt to participate or not. (1, p8). So, what the individuals end up weighing is whether they are sufficiently compensated for the increase in expected cost for participating. (1, p)

Relation To Use Case In our case, we are not considering whether or not individuals will participate in some study or not, but rather whether or not they will choose to use the mood app. I comment on how to make these two situations (study vs. app) analogical in the section on the cost scenario in the use case.

Assumptions The authors acknowledge that their model makes some simplifying assumptions, namely (1, p2): "that participants fear some specific bad events when particpating in the study" and "that they can estimate the expected cost from these events even when they do not participate…".

The latter assumption is suspsectfor reasons the authors themselves indicate: psychological research suggests that humans can be biased in reasoning about uncertain events (1, p23). The former assumption is not as suspect at least in our use case– it's not hard to imagine that users will fear specific events (i.e., leakage of their personal input data) from using the app.

Anyhow, we will allow for these assumptions for our exploratory analysis.

0.1.3 Defining Model Parameters - Simple Single Query Case

First, we will define the model parameters for a simple analysis case where we, as analysts, want to estimate the population mean μ i.e., the proportion of some population that has some property P.

We want to conduct the study for this estimate in a differentially-private way, aiming to satisfy the following equation with the mechanism M that we use:

$$\Pr[M(D) \in S] \leq e^{\varepsilon} \cdot \Pr\left[M\left(D'\right) \in S\right]$$

Where D and D' are adjacent datasets (in their definition, datasets of the same size but which differ in terms of the contents of one of their records), and S being a possible output of the mechanism M. This equation is to be satisfied for all possible S and pairs D & D'.

The **Key Parameters And Variables**: ϵ - the *privacy budget* of our study ; B - the budget the analyst has for compensating participants ; N - number of participants in study ; E - a participant's expected 'base cost'– the cost that they would incur from the study's output given they don't participate (see previous section) ; D_N - *sample*– private database formed by contributions of N participants ; $g(D_N)$ - *calculated sample mean*– proportion of particpants with property P ; T - *desired error* for our study ; $A(\epsilon, N)$ - *failure probability*– probability that the mechanism we use exceeds T ; α - *target accuracy*– the desired accuracy level for our mechanism

Budget Constraint Participants need to be compensated in order to incentivise them to participate in studies. Each individual needs to be paid $(e^\epsilon - 1)E$ (the worst-case increase in their expected cost from participating in the study), so the analysts budget has the following constraint:

$$(e^\epsilon - 1)E \leq B$$

Below, we implement this in Python code:

[ ]:
```
from math import exp

def within_budget(epsilon: float, expected_cost: float, budget: float) -> bool:
    return ((exp(epsilon) - 1) * expected_cost) <= budget
```

Accuracy Constraint At the same time, analysts have to ensure that their study affords them a sufficiently accurate estimate of their target metric (in this case, the population mean). That is represented by:

$$A(\varepsilon, N) := 2\exp\left(-\frac{NT^2}{12}\right) + \exp\left(-\frac{TN\varepsilon}{2}\right) \leq \alpha$$

Below is the implemtation in Python code:

[ ]:
```
def within_accuracy_constraint(epsilon: float, N: int, desired_error: float,␣
 ↪accuracy_constraint: float) -> bool:
    first_term = 2 * exp(-1 * (N * ((desired_error**2)) / 12))
    second_term = exp(-1 * ((desired_error * N * epsilon) / 2))
    return (first_term + second_term) <= accuracy_constraint
```

The goal is to find ϵ and N values that satisfy these two constraints.

Sufficient Conditions For Feasible N and ϵ Values The authors introduce a sufficient condition for feasible ϵ and N values

$$3\exp\left(\frac{-NT^2}{12}\right) \leq \alpha$$
$$\left(e^\varepsilon - 1\right)EN \leq B$$

i.e., ϵ and N values that satisfy these equations are feasible values for a study to go ahead within the aforementioned accuracy and budget constraints. However, if ϵ and N values cannot be found to satisfy these equations, that does not mean that there aren't any feasible ϵ and N values for the study. To prove that, one would need to check the accuracy and budget constraints.

These can be solved for bounds on N and ϵ

$$N \geq \frac{12}{T^2}\ln\frac{3}{\alpha}$$

and

$$\frac{T}{6} \leq \varepsilon \leq \ln\left(1 + \frac{BT^2}{12E\ln\frac{3}{\alpha}}\right)$$

Below is the implementation in Python code:

[ ]:

```
from math import log # natural log by default

def parameters_feasible_for_accuracy(N: int, desired_error: float,␣
 ↪accuracy_constraint: float) -> bool:
    return (3 * exp(-1 * (N * (desired_error**2)) / 12)) <= accuracy_constraint

def parameters_feasible_for_budget(N: int, expected_cost: float, epsilon:␣
 ↪float, budget: float) -> bool:
    return (((exp(epsilon) - 1) * expected_cost) * N) <= budget

def lower_bound_for_N(desired_error: float, accuracy_constraint: float) ->␣
 ↪float:
    return (12 / (desired_error**2)) * log(3 / accuracy_constraint)

def lower_bound_for_epsilon(desired_error: float) -> float:
    return desired_error / 6

def max_value_for_epsilon(budget: float, desired_error: float, expected_cost:␣
 ↪float, accuracy_constraint: float) -> float:
    return log(1 + (budget * (desired_error**2)) / (12 * expected_cost * log(3 /
 ↪ accuracy_constraint)))
```

Bound On Base Cost E From the equation:

$$\varepsilon \leq \ln\left(1 + \frac{BT^2}{12E\ln\frac{3}{\alpha}}\right)$$

If we consider max value for ε, then if we solve for E, we have:

$$E = \frac{BT^2}{12\ln\frac{3}{\alpha}(e^{\varepsilon} - 1)}$$

Where, this gives us a max value for a feasible base expected cost value i.e., if participants have a base expected cost E that exceeds this value, then the study is not feasible.

Below is the code implementation:

[ ]:

```
def bound_on_base_cost_E(budget: float, desired_error: float,␣
 ↪accuracy_constraint: float, epsilon: float):
    return (budget * (desired_error**2)) / (12 * log(3 / accuracy_constraint) *␣
↪(exp(epsilon) - 1))
```

Let's do a sanity check for our implementations.

The authors offer the following illustration at the end of ibid. Section 5.1. We plug in the values and see if we get the same result

[ ]:

```
T = 0.05
a = 0.05
epsilon = T / 6
B = 3.0 * (10**4)

print(f'Given a desired error of {T}, accuracy_constraint of {a}, and budget of␣
 ↪{B}:\n')
print(f'Lower bound for N: {lower_bound_for_N(T, a)}') # should bound N to be␣
 ↪~20000, as stated on p13
print(f'Max value for Base Cost E: {bound_on_base_cost_E(B, T, a, epsilon)}') #␣
 ↪should bound E to be less than ~182, as stated on p13
print(f'The parameters are feasible for accuracy constraint:␣
 ↪{parameters_feasible_for_accuracy(20_000, T, a)}') # should return True
print(f'The parameters are feasible for budget constraint:␣
 ↪{parameters_feasible_for_budget(20_000, 175, epsilon, B)}') # should return␣
 ↪True
```

```
Given a desired error of 0.05, accuracy_constraint of 0.05, and budget of
30000.0:

Lower bound for N: 19652.85389866608
Max value for Base Cost E: 182.41731464520467
The parameters are feasible for accuracy constraint: True
The parameters are feasible for budget constraint: True
```

Here we see a nice feature of the model can be seen from this: we are given a lower bound for N, which helps us put a quantity to how 'large' a dataset would need to be for a differentially-private application in the use case.

Considering Cost Scenarios Now that we have implementations of the key equations in the paper's model, let us now consider how to evaluate the feasibility of a study in our use-case given a particular cost scenario.

These cost scenarios consider what the model implies for studies that are trying to recruit participants. Participants consider whether or not to participate, however the study is going to go ahead regardless of their decision. They try to weigh the increase in expected cost that would result in participating against the compensation they'd receive for doing so.

In section 5.2, the method for considering each cost scenario is this: given our aforementioned T (desired error), B (budget), α (accuracy_constraint) and base ε values (from here): (i) what is the expected base cost of a prospective participant in the given scenario? ;(ii) does that fit within the bound on E that our model describes? If so, the study is feasible. ;(iii) if not, to determine definitively whether a study is feasible, we plug in the parameter values into the budget and accuracy constraints and check (via a numerical solver) whether there are any possible solutions. If not, then the study is definitely infeasible.

Cost Scenario In The Use-Case One way the model could be applied to the use case is in considering an individual who is deciding whether or not to use the mood app. For our use case, the compensation consists in benefitting from the services the app provides; the budget has already been spent and the app providers are going to run their differentially-private studies on the data of users.

However, this also highlights a difference between the scenarios described in the paper and our use case. In the various cost scenarios, users in a sense already 'bear' the data that could potentially be leaked as a result of participating in a study– for instance, in the smoking data study cost scenario, the prospective participant is a smoker, and so it is possible that the data that *would* be in the dataset if they participated does get leaked to others even if they do not participate (e.g. if someone sees them smoking).

In the case of the mood app however, if users choose not to use the app, then they would not, strictly speaking, 'bear' the data that *would* be in the database if they used it. For instance, if the mood app wants to track what resources they are using, if they do not use the app, then they would not fear the exposure of that data (because they haven't used the app!).

Nonetheless, we can still identify a similar risk they consider in whether to use the app: information about their private mental or emotional state gets leaked. That is what the app interactions approximate, and individuals will want to weigh this risk.

With this technicality out of the way, we can return to considering the cost scenario. The decision is whether or not to participate in their studies/study by using the app yourself.

We follow a similar procedure as in the paper to first consider the cost scenario.

However, the first step brings us to an issue to consider.

Estimating Base Cost In Our Use Case As the authors note in the section on making further refinements to their model (1, p23), the model does not describe how to determine the base cost for individuals. Moreover, there does not seem to be a totally rigorous way to do this especially in our use case. How might we quantify a privacy loss that results from using the app? It is hard to definitely say. As the authors note, psychological research also suggests that humans can be biased in reasoning about uncertain events. (1, p23)

Nonetheless, here is one suggestion. A cost scenario the authors consider is one in which individuals are deciding whether or not to participate in a study that involves their movie rating data.

The base cost envisioned in that scenario is the probability that, though they do not participate, a person's movie rating records are nonetheless released multiplied by the punitive damages specified by the Video Protection Act of 1998 (at least $2500).

It seems that individuals would fear disclosure of their inputs in a mood app for similar reasons, but to far greater degrees. So, let us stipulate the individual estimates that it would be 10 times as bad to have their information about their mental or emotional state leaked. This seems possible–

the data revealed by how one has used a mood app is presumably far more personal than however they have rated movies they might have watched.

So, we now need to determine what the probability of this happening if they do not use the app. As with the author's assessment of the movie rating case, disclosure seems to be a 'low probability event' i.e., 0.0001 (p 14).

Above we saw that our study parameters gave us an upper bound on the base cost E as 182.42 (2 dp.). Given the estimated base cost of this scenario $(0.0001 * 25000 = 2.5)$, the study is feasible (provided we have the requisite N).

0.1.4 Adjusting Model Parameters - Multiple Queries

Now, let us consider a case where we don't want to answer just a single query, but multiple queries.

The authors rely on the work of (2), who contributed this algorithm: **Multiplicative Weights Exponential Mechanism** (MWEM). This is a mechanism for answering multiple counting queries i.e., queries of the form "What fraction of the records in the database satisfy property P?" (1, p15)

For instance, say that the space of records in a dataset are bit strings of length d i.e., $X = \{0,1\}^d$. An individual bit could be thought of as a binary value on whether or not a given individual has a certain property P. Then, we can treat queries like "What fraction of subjects are male, smokers and above 50" as counting queries (1, p15)

To use their model with the MWEM, they need to define an accuracy bound, which they do as (1, p15):

$$T = \left(\frac{128 \ln|\mathscr{X}| \ln\left(\frac{32|\mathscr{C}| \ln|\mathscr{X}|}{\beta T^2}\right)}{\varepsilon N} \right)^{1/3}$$

And defining the accuracy function $A(\varepsilon, N)$ to be the probablity β exceeds the target error T on any query (1, p15):

$$A(\varepsilon, N) := \beta = \frac{32|\mathscr{C}| \ln|\mathscr{X}|}{T^2} \exp\left(-\frac{\varepsilon N T^3}{128 \ln|\mathscr{X}|}\right)$$

And, as before, we want to satisfy the accuracy constraint $A(\varepsilon, N) < \alpha$ and the budget constraint $(e^{\epsilon} - 1)EN \leq B$ (1, p15)

Let's try code this up and apply it to our use case. We just need to implement the accuracy bound as it is what is different from the single query setting.

```
[ ]: def accuracy_function_for_MWEM(record_space: int, number_of_queries: int,␣
     ↪desired_error: float, epsilon: float, N: int) -> float:
         return ((32 * number_of_queries * log(record_space) ) / (desired_error **␣
     ↪2)) * (exp(- (epsilon * N * (desired_error ** 3)) / 128 * log(record_space)␣
     ↪))


     # parameters for movie cost scenario
```

```
accuracy_constraint = 0.05
budget = 2 * (10 ** 6)
record_space = 2 ** 8
T = 0.2
queries = 10_000


# within accuracy constraint? Should return yes.
epsilon = 2.3
N = 8.7 * (10 ** 5)
result = accuracy_function_for_MWEM(record_space, queries, T, epsilon, N) <=␣
 ↪accuracy_constraint
print(result)
```

```
True
```

And let's consider whether we would meet our budget constraint in the use case. We plug in our the base expected cost from our previous description of the cost scenario, $E = 2.5$ and these new parameter values (for ε, N, etc.)

[ ]:
```
print(parameters_feasible_for_budget(N, 2.5, epsilon, budget))
```

```
False
```

And this makes sense, because even though the movie ratings study could still go ahead (1, p15), we estimated it's base cost to be ten times lower ($E = 0.25$).

[ ]:
```
# sanity check.
print(parameters_feasible_for_budget(N, 0.25, epsilon, budget))
```

```
True
```

Analysis So for a multi-query use case, it is likely that we will need a much larger budget to compensate for the much larger N value we need to satisfy the accuracy constraint for the number of queries we want to do.

The intuition behind this is that individuals expect to be compensated more in our use case (from using the app) than individuals who are thinking of participating in the movie rating study. Although the parameters here are enough for accuracy, they don't fit within a budget constraint for the mood app. (This is due to the much larger N (~87000) value we're passing in than before (20, 000)). The higher base cost requires a higher budget. (1, p15)

If, for example, we make the budget ten-fold:

[ ]:
```
budget *= 10
```

Then, the parameters described above are feasible for the use case:

[ ]:
```
print(parameters_feasible_for_budget(N, 2.5, epsilon, budget))
```

```
True
```

0.1.5 Private vs. Non-Private Study

An interesting result that their model lets us determine is whether or not a private or non-private version of the app would be cheaper. (1, p15-18)

Intuitively, we would expect a DP study to cost more than its non-private counterpart. A larger sample is required for a DP-study to achieve the same level of accuracy in order to mitigate for the added noise. Thus, assuming that individuals are paid the same amount in both kinds of studies, a DP study would typically be more costly than its non-private counterpart. (1, p16)

However, this is not necessarily the case because unlike DP-studies, their **non-private counterparts cannot bound the harm to individuals** (as DP does through the e^{ε} parameter), as shown e.g. by the successful linkage attacks carried out on anonymized datasets(1, p 16).

In this section, we will follow the authors comparison of the two kinds of studies for a simple single query case of estimating the population mean. (1, p15-18)

Cost In The Non-Private Study (1, p16) We have to define new cost parameters because E as used previously has to do with the expected base cost of a study that is differentially-private.

A non-private counterpart of a DP study releases the raw estimate without adding noise. So, a *possible* worst case scenario for a prospective participant is that their information is completely recovered from the published results.

However, it is unreasonable to require analysts to compensate for the worst case cost W, as in the average case, an attack is likely to only be able to recover a fraction of an individual's information. Denote this fraction ϕ. Then, a non-private study compensates individuals ϕW to incentivize them to participate.

Key Theorems The authors define two theorems to consider for this comparison.

Minimum Number of Participants & Budget Needed For Non-Private Study The minimum number of participants N' needed is:

$$N' \geq \frac{1}{8T^2} \ln \frac{1}{2\alpha}$$

And thus the minimum budget B' for a non-private study is:

$$B' = \phi N' W = \frac{\phi W}{8T^2} \ln \frac{1}{2\alpha}$$

And from this we can derive a

Sufficient Condition For Private Mean Estimation Study To Be Cheaper Than Non-Private Counterpart

$$\frac{T}{6} \leq \ln \left(1 + \frac{\phi W \ln \frac{1}{2\alpha}}{96 E \ln \frac{3}{\alpha}} \right)$$

Proof can be found in (1, p16-17)

[ ]:
```
def private_study_cheaper_than_non_private(lower_bound_for_epsilon: float,␣
 ↪non_private_compensation: float,
                                             accuracy_constraint: float,␣
 ↪expected_base_cost: float) -> bool:
    return lower_bound_for_epsilon <= (log(1 + ((non_private_compensation *␣
 ↪log( 1 / (2 * accuracy_constraint)))
                                                / (96 * expected_base_cost *␣
 ↪log(3 / accuracy_constraint)))))

def minimum_number_of_participants_for_non_private_study(desired_error: float,␣
 ↪accuracy_constraint: float) -> float:
    return (1 / (8 * (desired_error ** 2))) * log(1 / (2 * accuracy_constraint))

def minimum_budget_for_non_private_study(non_private_compensation: float,␣
 ↪desired_error: float, accuracy_constraint: float) -> float:
    return (non_private_compensation / (8 * (desired_error ** 2))) * log(1 / (2␣
 ↪* accuracy_constraint))
```

As a sanity check, let's now replicate the result the authors get for comparisons of the movie ratings study: * The non-private version **requires less participants** ($N' \geq 115$) to achieve the same accuracy as the DP version (which requires $N = 20,000$). * However the total cost is much more.

[ ]:
```
non_private_average_compensation = 0.002 * 2500
# 2500 is the worst case cost; 0.002 encodes the likelihood of a real␣
 ↪successful deanonimyzation attack, which is hard to estimate. So the authors␣
 ↪use a conservative amount

desired_error = 0.05
accuracy_constraint = 0.05

print(private_study_cheaper_than_non_private(desired_error / 6,␣
 ↪non_private_average_compensation, accuracy_constraint, expected_base_cost=0.
 ↪25)) # should be true
```

```
True
```

Great! Let's now see if, given the same constraints, a private version of our mood app would be cheaper than a non-private version, all else besides E being equal

[ ]:
```
non_private_average_compensation_use_case = 0.002 * 2500 # let's assume␣
 ↪compensation is still the same
print(private_study_cheaper_than_non_private(desired_error / 6,␣
 ↪non_private_average_compensation_use_case, accuracy_constraint,␣
 ↪expected_base_cost=2.5)) # should be true
```

```
True
```

It is! And perhaps this is not so surprising: presumably, it would cost less to incentivize users to use a mood app that attempts to provide strong privacy guarantees than one which does not rely on differentially privacy.

Caveat: Of course, we are just considering a simple query case that is in likelihood too basic to represent all the kinds of queries analaysts might want to do on a mood app user base.

Final Comparison : Size and Cost Running a non-private study on the app would have these budget and participant requirements

```
[ ]: print(f"Min Participants:␣
      ↪{minimum_number_of_participants_for_non_private_study(desired_error,␣
      ↪accuracy_constraint)}")
     print(f"Min Budget:␣
      ↪{minimum_budget_for_non_private_study(non_private_average_compensation_use_case,␣
      ↪desired_error, accuracy_constraint)}")
```

```
Min Participants: 115.12925464970228
Min Budget: 575.6462732485113
```

Whereas the cost of the equivalent private study on the app would cost:

```
[ ]: expected_base_cost = 2.5
     epsilon = 0.0083
     N = 20_000

     print(((exp(epsilon) - 1) * expected_base_cost * N ))
```

```
416.72702479524924
```

Which is must less.

Thus, as with the author's observation for the movie rating study, given the same budget, a non-private study/app could buy more participants/users to further improve its accuracy. So, **some DP studies/apps are more accurate and cheaper than their non-private counterparts** (1, 18)

0.1.6 Concluding Evaluation

We've gleaned the following: a lower bound on N (i.e., how 'large' a dataset must be) for a DP analysis on our use case; a significantly large budget could be required for a mood app that wanted to allow for multiple DP queries ; in the case where there is just a single query being made, a DP version of the mood app is cheaper than a non-private version.

The utility of the various results we've gathered will depend on the extent that my construal of the cost scenario for the use case is tenable. It does not seem like a very large stretch– the authors themselves consider a cost scenario involving an individual who decides whether or not to be part of some online social network (1, p14). So, it seems like their model affords us insights about using differential privacy in a use case like ours.

Further work could be done to explore whether or not a private mood app would indeed be less costly than a non-private mood app. In particular, we'd want to see if this held for the multiple-query case too, given that the budget required for a multi-query DP setting is significantly large (given the relatively high base cost).

---

1 Bibliography

(1) Hsu J, Gaboardi M, Haeberlen A, Khanna S, Narayan A, Pierce BC, et al. Differential Privacy: An Economic Method for Choosing Epsilon. 2014 IEEE 27th Computer Security Foundations Symposium Ithaca: IEEE; Jul 2014. pp. 398-410. 10.1109/CSF.2014.35

(2) Hardt M, Rothblum GN, Servedio RA. Private Data Release via Learning Thresholds. Society for Industrial and Applied Mathematics; 2022.