Notes

Maxim Zhilyaev

May 4, 2020

1 Abstract

We study a variety of the shuffling protocols for reporting one-hot vectors from multiple users with respect to privacy, sensitivity and practicality. From a practical standpoint, the cost of shuffling is not zero. Too many shuffled records may render a particular protocol impractical, even though its other metrics show good performance. We specifically consider protocols that minimize the number (but not necessarily the size) messages between a user device and the shuffler.

Assuming that the data comes from a universe $\mathcal{X} = [d]$ of d elements. Each individual $i \in [n]$ of n users has a data element $x_i \in \mathcal{X}$. We will write a data entry in bold $\boldsymbol{x}_i \in \{0,1\}^d$ to be the one-hot vector where x_i is zero in every position except position $\boldsymbol{x}_i \in \mathcal{X}$, where it is one. Furthermore, we will denote a dataset $\boldsymbol{x} = \{x_1, \ldots, x_n\}$ to be a collection of all users' one-hot vectors. We consider multiple mix-net protocols for reporting 1-hot vectors. A simple one would require each user to donate his data $\boldsymbol{x}_i$ in clear, but, in addition, inject some fake reports $z_j \in \mathcal{X}$ for $j \in [m]$, and corresponding one-hot vector notation $\boldsymbol{z}_j$, where each data entry is chosen uniformly at random from $\mathcal{X}$. We then pass $\{\boldsymbol{x}_i : i \in [n]\}$ and $\{\boldsymbol{z}_j : j \in [m]\}$ to an anonymizer that shuffles the data and makes it impossible to determine whether a data record is real or fake. We call it the "clear-fake records" protocol and show that it provides adequate protection with the cost proportional to $[d]$. Hence if dimensions are not large then the "clear-fake records" protocol is preferred for its simplicity.

When $[d]$ is significant, the cost of sending and shuffling many fake records becomes prohibitive. Another protocol is developed, which parameters are independent of $[d]$. It's called a "fake and flip" protocol, whereby a user still generates true and fake one-hot report vectors that are both randomized by bit flipping before being sent to the shuffler. This enables adequate protection at reasonable cost. Depending on the data collection setting, various flavors of the "fake and flip" protocol are discussed.

In discussing mathematical properties of the protocols involving randomization we will rely upon results received for a single dimension bit reporting. Which results we provide in the first sections, along with some theoretical result claiming that if a randomization algorithm $\mathcal{R}$ is (ϵ, δ)-private on a dataset of n elements, it's also (ϵ, δ)-private on a dataset of $n + 1$ elements, that is adding more elements to the shuffled set does not reduce privacy. These results are, then, used to develop

bounds for each protocol.

2 Differential Privacy Setup

A record is an element of some space $\mathcal{D}$, and a database $\mathbf{x}$ is a vector of n records: $\mathbf{x} = (x_1, \ldots, x_n) \in \mathcal{D}^n$. A randomized algorithm $\mathcal{R}$ maps the database into another space: $\mathcal{R} : \mathcal{D}^n \to \mathcal{S}$. The result of applying an algorithm to a database is termed an **transcript**. The notion of differential privacy for an algorithm $\mathcal{R}$ is that the resulting transcripts does not change substantially when a record in the database is modified, i.e., transcripts are not sensitive to particular individual records in the database. Hence, releasing transcript of $\mathcal{R}$ publicly will not jeopardize privacy, since information regarding individual records cannot be gained by analyzing the outcome of $\mathcal{R}(\mathbf{x})$.

Differential privacy for a randomized algorithm $\mathcal{R}$ is formulated by comparing the transcripts generated by applying $\mathcal{R}$ to two very similar databases $\mathbf{x}, \mathbf{x}' \in \mathcal{D}^n$. We say the databases **differ in one row** if $\sum_{i=1}^{n} I(x_i \neq x_i') = 1$. Such datasets are commonly called **neighboring** database or **neighbors**.

Definition. A randomized algorithm $\mathcal{R}$ is (ϵ, δ)-**differentially private** if, for any two databases $\mathbf{x}, \mathbf{x}' \in \mathcal{D}^n$ differing in one row,

$$\mathsf{P}[\mathcal{R}(\mathbf{x}) \in S] \leq \exp(\epsilon) \cdot \mathsf{P}[\mathcal{R}(\mathbf{x}') \in S] + \delta \tag{2.1}$$

for all $S \subset \mathcal{S}$ (measurable).

In other words, the outcomes from the two databases databases differing in one row are close in distribution, may be with the exception of very unlikely outcomes whose probability is less than δ

Definition. A randomized algorithm $\mathcal{R}$ generates point-wise (ϵ, δ)-**indistinguishable** outcomes for two databases $\mathbf{x}, \mathbf{x}' \in \mathcal{D}^n$ when

$$\mathsf{P}\left(\exp(-\epsilon) \leq \frac{\mathsf{P}[\mathcal{R}(\mathbf{x}) = s]}{\mathsf{P}[\mathcal{R}(\mathbf{x}') = s]} \leq \exp(\epsilon)\right) \geq 1 - \delta \tag{2.2}$$

Proposition 2.1. *A randomized algorithm $\mathcal{R}$ is (ϵ, δ)-**differentially private** if for every pair of neighboring databases $\mathbf{x}, \mathbf{x}' \in \mathcal{D}^n$, $\mathcal{R}$ generates point-wise (ϵ, δ)-**indistinguishable** outcomes. Per reference [2]*

To restate.

$$\mathsf{P}\left(\frac{\mathsf{P}[\mathcal{R}(\mathbf{x}) = s]}{\mathsf{P}[\mathcal{R}(\mathbf{x}') = s]} \leq \exp(\epsilon)\right) \geq 1 - \delta, \textit{ for any two neighbors } \mathbf{x}, \mathbf{x}' \tag{2.3}$$

$$\implies \mathcal{R} \textit{ is } (\epsilon, \delta) - \textit{\textbf{differentially private}} \tag{2.4}$$

2.1 Single record shuffling protocol

There are n users, each holding a user value $x_i \in \mathcal{X}$. User values form a database of user records a dataset $\boldsymbol{x} = \{x_1, \ldots, x_n\}$. Each user applies a randomization procedure $\mathcal{R}(x) : \mathcal{R} : \mathcal{X} \to \mathcal{S}$, then submits $\mathcal{R}(x_i)$ to an anonymizer that shuffles the data and makes it impossible to determine whether a data record is real or fake. We call this algorithm

$$M(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n) = \pi(\mathcal{R}(x_1), \ldots, \mathcal{R}(x_n)) \text{ where } \pi \text{ permutes its elements.}$$

If $\mathcal{S}$ finite, then we can write the output of M as a histogram over the entire database, as in $M(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n) = \sum_{i=1}^{n} \boldsymbol{x}_i + \sum_{j=1}^{m} \boldsymbol{z}_j$. Note that rather than inject random noise to these counts, as in central differential privacy, we want to consider *anonymized differential privacy*, where data records are transmitted through a mix net to break any identifiers with each data entry and the server sees the aggregated records in some random order. In this model, there is no trusted server that injects noise to ensure DP. Rather, the user needs to only trust the anonymizer to shuffle real and fake records.

We then consider the privacy loss for a general mechanism M. Consider an outcome $h \in \mathbb{N}^d$, which is a histogram over the full dataset domain and neighboring datasets $\boldsymbol{x}$ and $\boldsymbol{x}'$.

Suppose $\mathcal{S}$ is finite. If which is common in cases where the transcript involves integer counts, then the distribution of the transcript $A(\mathbf{x})$ can be represented using its pmf $\mathsf{P}[A(\mathbf{x}) = s]$ for $s \in \mathcal{S}$

3 Reporting randomized bits in the mix-net model

It is instructive to first consider the case where each record in the collection consists of a single bit, as the expressions simplify considerably.

When $L = 1$, each original and synthetic record is either 1 or 0, and the transformation R flips each record with probability q. Partition the collection space $\mathcal{D}^n$ according to the number of records that are 1:

$$\mathcal{D}^n = \bigcup_{m=0}^{n} \mathcal{D}^n_m \qquad \text{where} \qquad \mathcal{D}^n_m := \left\{ \mathbf{x} \in \mathcal{D}^n \, : \, \sum_{i=1}^{n} I(x_i = 1) = m \right\}.$$

For $\mathbf{x} \in \mathcal{D}^n_m$, we have

$$A(\mathbf{x}) = \Phi \circ R(\mathbf{x}) = \big(A_n(m), n - A_n(m)\big),$$

where

$$\begin{aligned} A_n(m) &:= \sum_{i=1}^{n} I(R(x_i) = 1) = \sum_{i:\, x_i = 1} I(R(1) = 1) + \sum_{i:\, x_i = 0} I(R(0) = 1) \\ &\sim Bin(m, p) + Bin(n - m, q), \end{aligned}$$

a sum of two independent Binomial random variables with support $\{0, \ldots, n\}$. Furthermore, if $\mathbf{x} \in \mathcal{D}^n_m$ and $\mathbf{x}, \mathbf{x}'$ differ in one row, then $\mathbf{x}' \in \mathcal{D}^n_{m-1} \cup \mathcal{D}^n_{m+1}$. Defining

$$\pi_n(s; m) := \frac{\mathsf{P}[A_n(m) = s]}{\mathsf{P}[A_n(m+1) = s]} \qquad \text{for} \;\; s \in \{0, \ldots, n\} \text{ and } m \in \{0, \ldots, n-1\},$$

the privacy ratio becomes

$$\pi\big((s, n-s);\, \mathbf{x}, \mathbf{x}'\big) = \begin{cases} \pi_n(s; m-1) & x_1 = 1 \\ \pi_n(s; m)^{-1} & x_1 = 0 \end{cases}.$$

Hence, in the $L = 1$ case, it suffices to study the behaviour of $\pi_n(s; m)$.

3.1 Recursive relationship over n and m

The conditioning argument (**??**) yields a recursive relationship that lets us express the distribution of A_n in terms of that of A_{n-1}.

Recall that $A_n(m)$ is the outcome of applying the bit transformation R to n original bits, m of which are 1 and $n - m$ are 0. For $m \geq 1$, we can condition on the outcome of one of the original 1s:

$$A_n(m) \sim Ber(p) + Bin(m-1, p) + Bin(n-m, q) \sim Ber(p) + A_{n-1}(m-1),$$

and so

$$\mathsf{P}[A_n(m) = s] = p\,\mathsf{P}[A_{n-1}(m-1) = s-1] + q\,\mathsf{P}[A_{n-1}(m-1) = s]. \tag{3.1}$$

If $s = 0$, the first term on the RHS is interpreted as 0, and if $s = n$, the last term is. Similarly, for $m \leq n-1$, conditioning on an original 0,

$$A_n(m) \sim Ber(q) + Bin(m, p) + Bin(n-m-1, q) \sim Ber(q) + A_{n-1}(m),$$

from which

$$\mathsf{P}[A_n(m) = s] = q\,\mathsf{P}[A_{n-1}(m) = s-1] + p\,\mathsf{P}[A_{n-1}(m) = s]. \tag{3.2}$$

The recursive formulas (3.1) and (3.2) give some insight into how the distribution of $A_n(m)$ changes as n and m vary:

- as n increases by 1, the probabilities shift slightly, with $\mathsf{P}[A_n(m) = 0] \leq \mathsf{P}[A_{n-1}(m) = 0]$ and $\mathsf{P}[A_n(m) = s]$ falling between $\mathsf{P}[A_{n-1}(m) = s-1]$ and $\mathsf{P}[A_{n-1}(m) = s]$ for each $s \geq 1$ (i.e., the hump of the pmf shifts to the right);
- the distribution of $A_n(m+1)$ is not so different to that of $A_n(m)$, since $\mathsf{P}[A_n(m) = s]$ and $\mathsf{P}[A_n(m+1) = s]$ both lie between consecutive pmf values of $A_{n-1}(m)$. In particular, this allows us to express the privacy ratio $\pi(s; m)$ in terms of $A_{n-1}(m)$.

Writing $P_{n,m}(s) := \mathsf{P}[A_n(m) = s]$, the formulas (3.1) and (3.2) can be expressed as

$$P_{n,m}(s) = pP_{n-1,m-1}(s-1) + qP_{n-1,m-1}(s) \quad \text{for } \ 0 \leq s \leq n, \ \ 1 \leq m \leq n$$

and

$$P_{n,m}(s) = qP_{n-1,m}(s-1) + pP_{n-1,m}(s) \quad \text{for } \ 0 \leq s \leq n, \ \ 0 \leq m \leq n-1.$$

3.2 The probability ratio

The probabilities in the privacy ratio represent the likelihood of observing the same synthetic collection outcome given two different original collections. In the expression $\pi_n(s;m) = P_{n,m}(s)/P_{n,m+1}(s)$, the probabilities correspond to the distributions of $A_n(m)$ and $A_n(m+1)$, respectively. However, using the decomposition (3.1) and (3.2), we can rewrite π_n in terms of probabilites from the same distribution, which is more convenient to work with.

Applying (3.2) to the numerator and (3.1) to the denominator, we obtain

$$\pi_n(s;m) = \frac{qP_{n-1,m}(s-1) + pP_{n-1,m}(s)}{pP_{n-1,m}(s-1) + qP_{n-1,m}(s)} = \frac{q + p\frac{P_{n-1,m}(s)}{P_{n-1,m}(s-1)}}{p + q\frac{P_{n-1,m}(s)}{P_{n-1,m}(s-1)}}$$

for $s \geq 1$, and $\pi_n(0;m) \equiv p/q$. Define the **probability ratio**

$$\rho_n(s;m) := \frac{P_{n,m}(s)}{P_{n,m}(s-1)} \qquad \text{for} \quad 1 \leq s \leq n$$

a ratio of consecutive probabilities from the distribution of $A_n(m)$, and let $g(x) = \frac{q+px}{p+qx}$, so that $\pi_n = g \circ \rho_{n-1}$. The function g is increasing over $x > 0$, since

$$g'(x) = \frac{p-q}{(p+qx)^2} > 0.$$

Therefore, properties of monotonicity and extrema established for ρ_n (for all n) carry over to π_n as well.

The probability ratio can be expressed in a concise way using the following recursive property of the distribution of $A_n(m)$.

Lemma 3.1. *For $n \geq 1$,*

$$(s+1)P_{n,m}(s+1) = \left\{(m-s)\frac{p}{q} + (n-m-s)\frac{q}{p}\right\}P_{n,m}(s) + (n-s+1)P_{n,m}(s-1) \tag{3.3}$$

for $0 \leq m \leq n$ and $0 \leq s \leq n-1$ (with $P_{n,m}(-1) := 0$).

Proof. We proceed by induction on n. Suppose first $n = 1$, $s = 0$. If $m = 1$, then $A_1(1) \sim Ber(p)$, and (3.3) holds since $(mp/q + (1-m)q/p) \cdot P_{1,1}(0) = p = P_{1,1}(1)$. The argument is similar when $m = 0$. Next assume (3.3) holds for $A_{n-1}(m)$, and suppose $m \leq n-1$ and $1 \leq s \leq n-2$. Observe that

$$
\begin{aligned}
&\left\{(m-s)\frac{p}{q} + (n-m-s)\frac{q}{p}\right\}P_{n,m}(s) + (n-s+1)P_{n,m}(s-1) \\
&\quad = \left\{(m-s)\frac{p}{q} + (n-1-m-s)\frac{q}{p}\right\}\bigl[qP_{n-1,m}(s-1) + pP_{n-1,m}(s)\bigr] \\
&\qquad\qquad + (n-1-s+1)\bigl[qP_{n-1,m}(s-2) + pP_{n-1,m}(s-1)\bigr] + \frac{q}{p}P_{n,m}(s) + P_{n,m}(s-1) \\
&\quad = p\Biggl[\left\{(m-s)\frac{p}{q} + (n-1-m-s)\frac{q}{p}\right\}P_{n-1,m}(s) + (n-1-s+1)P_{n-1,m}(s-1)\Biggr] \\
&\qquad + q\Biggl[\left\{(m-(s-1))\frac{p}{q} + (n-1-m-(s-1))\frac{q}{p}\right\}P_{n-1,m}(s-1) \\
&\qquad\qquad\qquad\qquad\qquad\qquad + (n-1-(s-1)+1)P_{n-1,m}(s-2)\Biggr] \\
&\qquad - \left(p + \frac{q^2}{p}\right)P_{n-1,m}(s-1) - qP_{n-1,m}(s-2) + \frac{q^2}{p}P_{n-1,m}(s-1) + qP_{n-1,m}(s) \\
&\qquad + qP_{n-1,m}(s-2) + pP_{n-1,m}(s-1) \\
&\quad = p(s+1)P_{n-1,m}(s+1) + qsP_{n-1,m}(s) + qP_{n-1,m}(s) \\
&\quad = (s+1)\bigl[qP_{n-1,m}(s) + pP_{n-1,m}(s+1)\bigr] = (s+1)P_{n,m}(s+1),
\end{aligned}
$$

applying the induction hypothesis for s and for $s-1$ together with (3.2). If $s = 0$, the argument is similar:

$$
\begin{aligned}
\left\{m\frac{p}{q} + (n-m)\frac{q}{p}\right\}P_{n,m}(0) &= p\left\{m\frac{p}{q} + (n-1-m)\frac{q}{p}\right\}P_{n-1,m}(0) + qP_{n-1,m}(0) \\
&= pP_{n-1,m}(1) + qP_{n-1,m}(0) = P_{n,m}(1).
\end{aligned}
$$

□

Given m, the probability ratio can be expressed using (3.3):

$$
\begin{aligned}
\rho(s+1;m) &= \frac{m-s}{s+1}\frac{p}{q} + \frac{n-m-s}{s+1}\frac{q}{p} + \frac{n-s+1}{s+1}\frac{1}{\rho(s;m)} \\
\rho(1;m) &= m\frac{p}{q} + (n-m)\frac{q}{p}
\end{aligned}
$$

Write

$$
\eta(s) := \frac{n-s+1}{s+1} \qquad \text{and} \qquad \gamma_m(s) := \frac{1}{s+1}\left[(m-s)\frac{p}{q} + (n-m-s)\frac{q}{p}\right],
$$

to get

$$
\rho(s+1;m) = \eta(s)\rho(s;m)^{-1} + \gamma_m(s)\,; \quad \rho(1;m) = \gamma_m(0). \tag{3.4}
$$

Note also that $\gamma_m(s)$ can be expressed in terms of $\mathsf{E}\,A_n(m) = \mu_m = nq + m(p-q)$:

$$
(s+1)\gamma_m(s) = \frac{\mu_m - s}{pq} - n + 2s.
$$

The probability ratio has the following properties (TODO):

- decreasing in s for fixed m
- increasing in m for fixed s.

3.3 Bounding the probability ratio

For A to satisfy local differential privacy, the privacy ratio $\pi_n(s;m)$ must be bounded for all s except for a set of small probability with respect to the distribution $\mathsf{P}[A_n(m) = \cdot]$. Furthermore, this bound must hold regardless of the original collection described through m.

Fix $\delta > 0$. Given m, we show that the probability ratio for $s \in [\mu_m - \delta, n]$ is bounded by a value $\rho(s^*; 0)$, where s^* is expressed in terms of $\mu_0 - \delta$. Together with the fact that $P_{n,m}(\mu_m - \delta) \leq P_{n,0}(\mu_0 - \delta)$ (TODO - is this necessary?), this implies that the bound for local differential privacy, required to hold for all m, can be computed in terms of $A_n(0)$ alone. Note that, since ρ is decreasing in s for fixed m, it is sufficient to consider the probability ratio at the smallest integer value belonging to the interval $[\mu_m - \delta, n]$.

TODO: how to handle the left endpoint. What is the min value of δ?

For $\delta > 0$ let $s_m(\delta) := \lceil \mu_m - \delta \rceil \vee 0$, and define $R_m(\delta) := \rho(s_m(\delta); m)$. Note that $R_m(\delta) \leq R_m(\delta')$ for $\delta \leq \delta'$, and $s_m(\delta + 1) = (s_m(\delta) - 1) \vee 0$.

Proposition 3.1.

$$R_m(\delta) \leq R_0(\delta + 2) \qquad \textit{for} \;\; m = 0, \ldots, n$$

provided $\delta > \sigma_0 + 1$, *where* $\sigma_0^2 = \mathsf{Var}\, A_n(0) = npq$.

Proof. Fix $\delta > \sigma_0 + 1$. (TODO) If $s_0(\delta) < 2$

Assume $s_0(\delta) \geq 2$, and suppose $R_m(\delta) > R_0(\delta + 2)$ for some m. Then, we have

$$R_0(\delta) \leq R_0(\delta + 1) \leq R_0(\delta + 2) < R_m(\delta) \leq R_m(\delta + 1),$$

implying that

$$R_0(\delta + 2)^{-1} = \frac{R_0(\delta + 1) - \gamma_0(s_0(\delta + 2))}{\eta(s_0(\delta + 2))} > \frac{R_m(\delta) - \gamma_m(s_m(\delta + 1))}{\eta(s_m(\delta + 1))} = R_m(\delta + 1)^{-1}$$

via (3.4). Write $s_m := s_m(\delta + 1)$, $s_0 := s_0(\delta + 2)$. Since $R_m(\delta) > R_0(\delta + 1)$ by assumption, we obtain:

$$\big\{\eta(s_m) - \eta(s_0)\big\} R_0(\delta + 1) + \big\{\eta(s_0)\gamma_m(s_m) - \eta(s_m)\gamma_0(s_0)\big\} > 0. \tag{3.5}$$

Furthermore,

$$\eta(s_m) - \eta(s_0) = \frac{n - s_m + 1}{s_m + 1} - \frac{n - s_0 + 1}{s_0 + 1} = -\frac{(n + 2)(s_m - s_0)}{(s_0 + 1)(s_m + 1)},$$

and

$$\begin{aligned}&\eta(s_0)\gamma_m(s_m) - \eta(s_m)\gamma_0(s_0)\\ &\quad = \frac{n-s_0+1}{s_0+1}\cdot\frac{(\mu_m - s_m)/pq - n + 2s_m}{s_m+1} - \frac{n-s_m+1}{s_m+1}\cdot\frac{(\mu_0 - s_0)/pq - n + 2s_0}{s_0+1}\\ &\quad = \frac{(n+2)(s_m-s_0) + (\mu_0 s_m - \mu_m s_0)/pq + (n+1)[\mu_m - \mu_0 - (s_m - s_0)]/pq}{(s_0+1)(s_m+1)},\end{aligned}$$

so (3.5) implies

$$\begin{aligned}&-(n+2)(s_m-s_0)(R_0(\delta+1)-1)+\\ &\qquad\qquad \frac{\mu_0(s_m-s_0) - m(p-q)s_0}{pq} + \frac{(n+1)[m(p-q)-(s_m-s_0)]}{pq} > 0. \qquad (3.6)\end{aligned}$$

Now, let $\delta_0 := \delta - \{\lceil \mu_0 - \delta\rceil - (\mu_0 - \delta)\} = \mu_0 - \lceil \mu_0 - \delta \rceil$, i.e., $\delta_0 = \inf\{\lambda : s_0(\lambda) = s_0(\delta)\}$. Then $s_0(\delta) = s_0(\delta_0) = \mu_0 - \delta_0$, an integer, and $s_m(\delta_0) - s_m(\delta) \in \{0,1\}$, since $0 \le \delta - \delta_0 < 1$. Consequently, since

$$s_m(\delta_0) - s_0(\delta_0) = \lceil \mu_0 + m(p-q) - \delta_0\rceil - (\mu_0 - \delta_0) = \lceil m(p-q)\rceil,$$

$$\begin{aligned}s_m - s_0 &= (s_m(\delta)-1) - (s_0(\delta)-2) = s_m(\delta) - s_m(\delta_0) + \lceil m(p-q)\rceil + 1\\ &\in \bigl\{\lceil m(p-q)\rceil, \lceil m(p-q)\rceil + 1\bigr\},\end{aligned}$$

and

$$\begin{aligned}\mu_0(s_m - s_0) - m(p-q)s_0 &= \mu_0(s_m-s_0) - m(p-q)(s_0(\delta_0)-2)\\ &= \mu_0[(s_m-s_0) - m(p-q)] + m(p-q)(\delta_0+2).\end{aligned}$$

Applying these identities in (3.6) gives

$$-(n+2)(s_m-s_0)(R_0(\delta+1)-1) + \frac{m(p-q)(\delta_0+2)}{pq} + \frac{n+1-\mu_0}{pq}\bigl(m(p-q) - (s_m-s_0)\bigr) > 0.$$

Since $s_m - s_0 \ge m(p-q)$,

$$(n+2)(R_0(\delta+1)-1) < \frac{\delta_0+2}{pq}\frac{m(p-q)}{s_m-s_0} < \frac{\delta_0+2}{pq}. \qquad (3.7)$$

Next, recall that $R_0(\delta+1) = P_{n,0}(s_0(\delta+1))/P_{n,0}(s_0(\delta+1)-1)$. Since $P_{n,0}(\cdot) = \mathsf{P}[Bin(n,q) = \cdot]$,

$$R_0(\delta+1) - 1 = \frac{n - s_0(\delta+1)+1}{s_0(\delta+1)}\cdot\frac{q}{p} - 1 = \frac{\mu_0 - (\mu_0 - \delta_0 - 1) + q}{p(\mu_0 - \delta_0 - 1)} = \frac{\delta_0 + q + 1}{p(\mu_0 - \delta_0 - 1)}.$$

Hence, substituting this expression in (3.7) yields

$$\begin{aligned}&(\delta_0+2)(\mu_0 - \delta_0 - 1) > (n+2)q(\delta_0+q+1) > \mu_0(\delta_0+q+1)\\ \iff& -\delta_0^2 - 3\delta_0 + 2\mu_0 - 2 > (1+q)\mu_0\\ \iff& -\delta_0^2 - 3\delta_0 + npq > 0,\end{aligned}$$

which requires that δ_0 lie between the roots of the quadratic equation. In particular,

$$\delta_0 \leq -\frac{3}{2} + \frac{1}{2}\sqrt{9 + 4npq} \leq -\frac{3}{2} + \frac{3}{2} + \sqrt{npq} = \sqrt{npq}.$$

Finally, since $0 \leq \delta - \delta_0 < 1$, we conclude that

$$\delta = \delta_0 + \delta - \delta_0 < \sigma_0 + 1,$$

contradicting our initial choice of δ. □

4 Reporting randomized bits in the mix-net model

There are $n+1$ single bit records being sent through a shuffler. Before sending, each bit is randomized with $\mathcal{R}$ - that is, flipped with probability q and kept unchanged with probability $p = 1 - q$. the outcome S is the sum of randomized bits. Let D be a set of n bits and construct a neighboring pair of datasets by adding to D a set bit and a 0 zero bit. Then the privacy loss ratio at any given value of S is expressed as:

$$R(S|D) = \frac{P(S|D \cup 0)}{P(S|D \cup 1)} \tag{4.1}$$

Each probability allows conditioning on possible values the added bit could generate:

$$P(S|D \cup 0) = p \cdot P(S|D) + q \cdot P(S - 1|D) \tag{4.2}$$

Indeed, if 0 bit is randomized to itself (with probability p), then S must be generated by D alone, while if 0 bit was flipped (with probability q) then D must generate $S - 1$ total bit sum. Similarly

$$P(S|D \cup 1) = p \cdot P(S - 1|D) + q \cdot P(S|D) \tag{4.3}$$

Combining two conditioning expressions into the privacy loss ratio one arrives to:

$$R(S|D) = \frac{p \cdot P(S|D) + q \cdot P(S-1|D)}{p \cdot P(S-1|D) + q \cdot P(S|D)} = \frac{p\frac{P(S|D)}{P(S-1|D)} + q}{p + q\frac{P(S|D)}{P(S-1|D)}} \tag{4.4}$$

Let $\rho(S) = \frac{P(S|D)}{P(S-1|D)}$ be a **probability ratio** between adjacent values of S. It's related to $R(S)$ as in:

$$R(S|D) = \frac{p\frac{P(S|D)}{P(S-1|D)} + q}{p + q\frac{P(S|D)}{P(S-1|D)}} = \frac{q + p\rho(S)}{p + q\rho(S)} \tag{4.5}$$

Let $g(x) = \frac{q+px}{p+qx}$, the function g is increasing over $x > 0$, since

$$g'(x) = \frac{p - q}{(p + qx)^2} > 0.$$

Therefore, properties of monotonicity and extrema established for $\rho(S)$ carry over to $R(S)$ as well.

If D contains m set bits, then the distribution of S is a sum of two binomial distributions (a Poisson Binomial distribution):

$$S \sim Bin(m, p) + Bin(n - m, q)$$

Lemma 4.1. *When 0-bit is replaced with a set bit, the resulting privacy loss ratio $R(S)$ decreases monotonically as S grows, reaching its maximum in $S = 0$ and minimum in $S = N$.*

Proof. As show by Wang, Y. H. (1993). "On the number of successes in independent trials", for any Poisson Binomial distribution, the probability of consecutive values are related as follows

$$\begin{aligned} & P(S)^2 > P(S-1) \cdot P(S+1) \\ \implies & \rho(S-1) > \rho(S) \\ \implies & R(S-1) > R(S) \end{aligned}$$

□

Lemma 4.2. *When 0-bit is replaced with a set bit, the resulting privacy loss ratio $R(S)$ decreases monotonically as S grows, reaching its maximum in $S = 0$ and minimum in $S = N$.*

Proof. As show by Wang, Y. H. (1993). "On the number of successes in independent trials", for any Poisson Binomial distribution, the probability of consecutive values are related as follows

$$\begin{aligned} & P(S)^2 > P(S-1) \cdot P(S+1) \\ \implies & \rho(S-1) > \rho(S) \\ \implies & R(S-1) > R(S) \end{aligned}$$

□

Lemma 4.3. *Denote a collections of n bits containing r set bits and $n-r$ zero bits as D_r. Further denote the corresponding quantities:*

- *privacy loss ratio at a particular value S as $R(S|D_r) = \frac{P(S|D_r)}{P(SD'_r)}z$*
- *probability ratio at a particular value S as $\rho(S|D_r) = \frac{P(S|D_r)}{P(S-1|D_r)}$*
- *expected value of S as $\mu_r = p \cdot r + q \cdot (n - r)$*

Choose a distance l such that $l \geq npq$, then

$$\rho[\mu_r - l|D_r] \leq \rho[\mu_0 - (l+2)|D_0]$$

That is, the probability ratio for any collection is bound by the probability ratio of the zero collection.

Proof. PROOF IS INVOLVED AND WILL BE GIVEN LATER IN APPENDIX. Max needs to fix Dave's notations, skipping for now. □

From lemma (4.3) immediately follow corollaries below

Corollary 4.1. *For left deviations $l \geq npq$ from the mean the privacy loss ratio for the collection of n bits is bounded by the privacy loss ratio for the collection of n zero bits*

$$R[\mu_r - l|D_r] \leq R[\mu_0 - (l+2)|D_0]$$

Proof. From (4.5)

$$R(S|D_r) = \frac{q + p\rho_r(S)}{p + q\rho_r(S)}$$

Given that $\rho_r(S) \leq \rho_0(S)$, we have

$$\begin{aligned} R(S|D_r) = \frac{q + p\rho_r(S)}{p + q\rho_r(S)} \leq R(S|D_0) &= \frac{q + p\rho_0(S)}{p + q\rho_0(S)} \\ qp + q^2\rho_0(S) + p^2\rho_r(S) + pq \cdot \rho_0(S) \cdot \rho_r(S) \leq qp + p^2\rho_0(S) + q^2\rho_r(S) &+ pq \cdot \rho_0(S) \cdot \rho_r(S) \\ \rho_r(S)(p^2 - q^2) \leq \rho_0(S)&(p^2 - q^2) \\ \rho_r(S) \leq &\rho_0(S) \end{aligned}$$

□

The next corollary bounds the right tail of distribution

Corollary 4.2. *For right deviations $l \geq npq$ from the mean, the privacy loss ratio for the collection of n bits is bounded by the privacy loss ratio for the collection of n set bits*

$$R[\mu_r + l|D_r] \leq R[\mu_n + l + 2|D_n]$$

Proof. TODO - proving by symmetry between D_0 and D_n distributions. □

Using the bound (4.42) and the fact that all-zero and all-set bit collections provide identical bounds to the privacy loss ratio for the left and the right side of distribution, we finally arrive to an important theorem.

Proposition 4.1. *randomization procedure $\mathcal{R}$ is (ϵ, δ)-private on a collection n bits, when the flipping frequency q obeys the bound below*

$$q \geq \frac{3 \cdot ln\frac{2}{\delta}}{n\left[1 - e^{-\epsilon} - 2\frac{p-q}{npq}\right]^2} \tag{4.6}$$

Note that the term $2\frac{p-q}{npq}$ appeared due to $l+2$ correction of both corollaries above. For sufficiently large n, this term diminishes to zero, which simplifies the bound to the form of lemma (4.5)

Lemma 4.4. *If randomization procedure $\mathcal{R}$ is (ϵ, δ)-private on a collection n bits, it's also (ϵ, δ)-private on a collection of $n+1$ bits. In other words, if n bit are protected with flipping frequency q, then all collections of greater size are also protected with same q.*

Proof. Let D_n be a collection of n bits and derive a neighboring collection D'_n by replacing a single bit. Since $\mathcal{R}$ is (ϵ, δ)-private for n bits, then for any set of outcomes W

$$P(\mathcal{R}(D'_n) \in W) \leq \exp(\epsilon) P(\mathcal{R}(D_n) \in W) + \delta \tag{4.7}$$

$$\Longrightarrow \qquad P(\mathcal{R}(D'_n) \in W) - \exp(\epsilon) P(\mathcal{R}(D_n) \in W) \leq \delta \tag{4.8}$$

Now add a 0 bit to both D_n and D'_n. The probability of the extended collections D_{n+1} and D'_{n+1} generating a particular outcome S is given by (4.2)

$$P(\mathcal{R}(D_{n+1}) = S) = P(\mathcal{R}(D_n) = S) \cdot p + P(\mathcal{R}(D_n) = S - 1) \cdot q \tag{4.9}$$

Assume that $\mathcal{R}(D_{n+1})$ is not (ϵ, δ)-private, then there must exists a set W' such that

$$P(\mathcal{R}(D'_{n+1}) \in W') > \exp(\epsilon) P(\mathcal{R}(D_{n+1}) \in W') + \delta \tag{4.10}$$

Suppose W' contains r distinct outcomes $W' = \{S_1, S_2, \cdots, S_r\}$, then

$$P(\mathcal{R}(D_{n+1}) \in W') = \sum_i^r P(\mathcal{R}(D_{n+1}) = S_i) \tag{4.11}$$

$$= \sum_i^r \left[P(\mathcal{R}(D_n) = S_i) + P(\mathcal{R}(D_n) = S_i - 1) \cdot q\right] \text{ by (4.9)} \tag{4.12}$$

$$= p \sum_i^r P(\mathcal{R}(D_n) = S_i) + q \sum_i^r P(\mathcal{R}(D_n) = S_i - 1) \tag{4.13}$$

Define a set $W'' = \{S_1 - 1, S_2 - 1, \cdots, S_r - 1\}$, then (4.2) can be rewritten in the form membership probabilities.

$$P(\mathcal{R}(D_{n+1}) \in W') = p \sum_i^r P(\mathcal{R}(D_n) = S_i) + q \sum_i^r P(\mathcal{R}(D_n) = S_i - 1) \tag{4.14}$$

$$= p \cdot P(\mathcal{R}(D_n) \in W') + q \cdot P(\mathcal{R}(D_n) \in W'') \tag{4.15}$$

In the same fashion we arrive to the expression of $P(\mathcal{R}(D'_{n+1}) \in W')$

$$P(\mathcal{R}(D'_{n+1}) \in W') = p \cdot P(\mathcal{R}(D'_n) \in W') + q \cdot P(\mathcal{R}(D'_n) \in W'') \tag{4.16}$$

Plugging the above probabilities into (4.13), we arrive to an inequality that must hold if $\mathcal{R}(D_{n+1})$ is not (ϵ, δ)-private.

$$P(\mathcal{R}(D'_{n+1}) \in W') > \exp(\epsilon) P(\mathcal{R}(D_{n+1}) \in W') + \delta \tag{4.17}$$

$$P(\mathcal{R}(D'_{n+1}) \in W') - \exp(\epsilon) P(\mathcal{R}(D_{n+1}) \in W') > \delta \tag{4.18}$$

$$p \cdot P(\mathcal{R}(D'_n) \in W') + q \cdot P(\mathcal{R}(D'_n) \in W'') - p \cdot P(\mathcal{R}(D_n) \in W') - q \cdot P(\mathcal{R}(D_n) \in W'') > \delta \tag{4.19}$$

$$p \left[P(\mathcal{R}(D'_n) \in W') - P(\mathcal{R}(D_n) \in W')\right] + q \left[P(\mathcal{R}(D'_n) \in W'') - P(\mathcal{R}(D_n) \in W'')\right] > \delta \tag{4.20}$$

However (4.7) implies that

$$\begin{aligned}
& && \left[P(\mathcal{R}(D'_n) \in W') - P(\mathcal{R}(D_n) \in W')\right] \leq \delta \\
&\text{and} && \left[P(\mathcal{R}(D'_n) \in W'') - P(\mathcal{R}(D_n) \in W'')\right] \leq \delta \\
&\implies && p\left[P(\mathcal{R}(D'_n) \in W') - P(\mathcal{R}(D_n) \in W')\right] + q\left[P(\mathcal{R}(D'_n) \in W'') - P(\mathcal{R}(D_n) \in W'')\right] \leq p\delta + q\delta \\
&\implies && p\left[P(\mathcal{R}(D'_n) \in W') - P(\mathcal{R}(D_n) \in W')\right] + q\left[P(\mathcal{R}(D'_n) \in W'') - P(\mathcal{R}(D_n) \in W'')\right] \leq \delta(p+q) \\
&\implies && p\left[P(\mathcal{R}(D'_n) \in W') - P(\mathcal{R}(D_n) \in W')\right] + q\left[P(\mathcal{R}(D'_n) \in W'') - P(\mathcal{R}(D_n) \in W'')\right] \leq \delta
\end{aligned}$$

Which contradicts (4.20) and proves the lemma. □

4.1 properties of zero valued collection

A homogenous collection of n zero bits is an important spacial case, hence we present findings for it below. Let D consists of n zero bits, then the neighbor D' is achieved by replacing a zero bit with set bit. The outcome of applying procedure c is a sum of randomized bits S. The following relationships hold.

$$\mu = E(S) = q \cdot n \tag{4.21}$$

$$P(S = i|D) = \binom{n}{i} q^i p^{n-i} \tag{4.22}$$

$$P(S = i|D') = \binom{n-1}{i} q^{i+1} p^{n-1-i} + \binom{n-1}{i-1} q^{i-1} p^{n-i+1} \tag{4.23}$$

$$R(i) = \frac{P(s = i|D')}{P(s = i|D)} = \frac{\binom{n}{i} q^i p^{n-i}}{\binom{n-1}{i} q^{i+1} p^{n-1-i} + \binom{n-1}{i-1} q^{i-1} p^{n-i+1}} \tag{4.24}$$

$$\frac{1}{R(i)} = \frac{n-i}{n}\frac{q}{p} + \frac{i}{n}\frac{p}{q} \tag{4.25}$$

By applying Chernoff bound to the distribution of s, we receive

$$P(|S - \mu| > t\mu) \leq 2e^{-\frac{t^2\mu}{3}} \tag{4.26}$$

Setting $t = \sqrt{\frac{3}{\mu} ln\frac{2}{\delta}}$ one arrives to

$$P\left(|S - \mu| > \sqrt{3nq \cdot ln\frac{2}{\delta}}\right) \leq \delta \tag{4.27}$$

Setting $l = \sqrt{3nq \cdot ln\frac{2}{\delta}}$, one is ensured that values of $P(S \in [\mu - l, \mu + l]) \geq 1 - \delta$. Conditioned on

$S \in [\mu - l, \mu + l]$ we bound the privacy loss ratio $R(i)$ in this interval in the following way:

$$e^{\epsilon} \geq R(i) \geq e^{-\epsilon} \tag{4.28}$$

$$\implies \qquad e^{-\epsilon} \leq \frac{1}{R(i)} \leq e^{\epsilon} \tag{4.29}$$

$$\implies \qquad e^{-\epsilon} \leq \frac{n-i}{n}\frac{q}{p} + \frac{i}{n}\frac{p}{q} \leq e^{\epsilon} \tag{4.30}$$

We first bound the left side of the inequality, setting $i = \mu - l$

$$\frac{n-i}{n}\frac{q}{p} + \frac{i}{n}\frac{p}{q} \geq e^{-\epsilon} \tag{4.31}$$

$$\frac{n-(\mu-l)}{n}\frac{q}{p} + \frac{\mu-l}{n}\frac{p}{q} \geq e^{-\epsilon} \tag{4.32}$$

$$\frac{n-(nq-l)}{n}\frac{q}{p} + \frac{nq-l}{n}\frac{p}{q} \geq e^{-\epsilon} \tag{4.33}$$

$$\frac{np+l}{n}\frac{q}{p} + \frac{nq-l}{n}\frac{p}{q} \geq e^{-\epsilon} \tag{4.34}$$

$$q + \frac{l}{n}\frac{q}{p} + p - \frac{l}{n}\frac{p}{q} \geq e^{-\epsilon} \tag{4.35}$$

$$1 - \frac{l}{n}\frac{p-q}{pq} \geq e^{-\epsilon}. \tag{4.36}$$

$$l \leq \left[1 - e^{-\epsilon}\right]\frac{npq}{p-q} \tag{4.37}$$

Plugging expression for l one arrives to the bound of q

$$\sqrt{3nq \cdot ln\frac{2}{\delta}} \leq \left[1 - e^{-\epsilon}\right]\frac{npq}{p-q} \tag{4.38}$$

$$\frac{(p-q)^2}{q \cdot p^2} \leq \frac{n\left[1 - e^{-\epsilon}\right]^2}{3ln\frac{2}{\delta}} \tag{4.39}$$

$$\text{since } \frac{(p-q)^2}{p^2} \leq 1 \text{ , then} \tag{4.40}$$

$$\frac{(p-q)^2}{q \cdot p^2} \leq \frac{1}{q} \leq \frac{n\left[1 - e^{-\epsilon}\right]^2}{3ln\frac{2}{\delta}} \tag{4.41}$$

$$q \geq \frac{3ln\frac{2}{\delta}}{n\left[1 - e^{-\epsilon}\right]^2} \tag{4.42}$$

In a similar fashion, one arrives to the right side bound

$$i = \mu + l \tag{4.43}$$

$$\frac{l}{n}\frac{p-q}{pq} \leq e^{\epsilon} - 1 \tag{4.44}$$

$$\sqrt{3nq \cdot ln\frac{2}{\delta}} \leq \left[e^{\epsilon} - 1\right]\frac{npq}{p-q} \tag{4.45}$$

$$q \geq \frac{3ln\frac{2}{\delta}}{n\left[e^{\epsilon}-1\right]^2} \tag{4.46}$$

Note that since $x + 1/x \geq 2$, then

$$e^{\epsilon} - 1 \geq 1 - e^{-\epsilon}$$

Which implies that if q bound (4.42) is met, then (4.46) is also met, which leads to the following lemma

Lemma 4.5. *Bit flipping randomization procedure $\mathcal{R}$ applied to a collection of n zero bits is* (ϵ, δ)*-private if the bit flipping frequency q satisfies* (4.42)

$$q \geq \frac{3 \cdot ln\frac{2}{\delta}}{n\left[1 - e^{-\epsilon}\right]^2}$$

By using the symmetry property of all-zero and all-set bits distributions, one arrives at the the identical statement for all-set bits collection

Lemma 4.6. *Bit flipping randomization procedure $\mathcal{R}$ applied to a collection of n set bits is* (ϵ, δ)*-private if the bit flipping frequency q satisfies* (4.42)

$$q \geq \frac{3 \cdot ln\frac{2}{\delta}}{n\left[1 - e^{-\epsilon}\right]^2}$$

5 Clear Reports

Assume that the data comes from a universe $\mathcal{X} = [d]$ of d elements. Each individual $i \in [n]$ of n users has a data element $x_i \in \mathcal{X}$. We will write a data entry in bold $\boldsymbol{x}_i \in \{0,1\}^d$ to be the one-hot vector where x_i is zero in every position except position $\boldsymbol{x}_i \in \mathcal{X}$, where it is one. Furthermore, we will denote a dataset $\boldsymbol{x} = \{x_1, \ldots, x_n\}$ to be a collection of all users' one-hot vectors. We will have each user donate his data $\boldsymbol{x}_i$. Further, we will inject some fake reports $z_j \in \mathcal{X}$ for $j \in [m]$, and corresponding one-hot vector notation $\boldsymbol{z}_j$, where each data entry is chosen uniformly at random from $\mathcal{X}$. We then pass $\{\boldsymbol{x}_i : i \in [n]\}$ and $\{\boldsymbol{z}_j : j \in [m]\}$ to an anonymizer that shuffles the data and makes it impossible to determine whether a data record is real or fake. We call this algorithm

$$M(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n) = \pi(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n, \boldsymbol{z}_1, \ldots, \boldsymbol{z}_m) \text{ where } \pi \text{ permutes its elements.}$$

We then compute the privacy loss of such an algorithm M. Equivalently, we could write the output as a histogram over the entire database, as in $M(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n) = \sum_{i=1}^{n} \boldsymbol{x}_i + \sum_{j=1}^{m} \boldsymbol{z}_j$. Note that rather than inject random noise to these counts, as in central differential privacy, we want to consider *anonymized differential privacy*, where data records are transmitted through a mix net to break any identifiers with each data entry and the server sees the aggregated records in some random order. In this model, there is no trusted server that injects noise to ensure DP. Rather, the user needs to only trust the anonymizer to shuffle real and fake records.

We then consider the privacy loss for a general mechanism M. Consider an outcome $h \in \mathbb{N}^d$, which is a histogram over the full dataset domain and neighboring datasets $\boldsymbol{x}$ and $\boldsymbol{x'}$.

$$L(h) = \log \left(\frac{\Pr[M(\boldsymbol{x}) = h]}{\Pr[M(\boldsymbol{x'}) = h]} \right) \tag{5.1}$$

If we can bound $L(h)$ by ϵ for any outcome h then we say that M is ϵ-DP. If we can bound $L(h)$ by ϵ with probability at least $1 - \delta$ where the randomness is over $h \sim M(\boldsymbol{x})$, then we say that M is (ϵ, δ)-DP.

We now focus on M being the mechanism described above, which injects m fake reports. We can then write the privacy loss in the following way where we assume, without loss of generality, that $\boldsymbol{x}$ and $\boldsymbol{x}'$ only differ in the first record, i.e. $\boldsymbol{x}_i = \boldsymbol{x}'_i$ for all $i \neq 1$.

$$\begin{aligned} L(h) &= \log \left(\frac{\Pr[x_1 + \sum_{i=2}^n \boldsymbol{x}_i + \sum_{j=1}^m \boldsymbol{z}_j = h]}{\Pr[x'_1 + \sum_{i=2}^n \boldsymbol{x}_i + \sum_{j=1}^m \boldsymbol{z}_j = h]} \right) \\ &= \log \left(\frac{\Pr[\sum_{j=1}^m \boldsymbol{z}_j = h - \boldsymbol{x}_1 - \sum_{i=2}^n \boldsymbol{x}_i]}{\Pr[\sum_{j=1}^m \boldsymbol{z}_j = h - \boldsymbol{x}'_1 - \sum_{i=2}^n x_i]} \right) \\ &= \log \left(\frac{\Pr[\sum_{j=1}^m \boldsymbol{z}_j = h - \sum_{i=1}^n \boldsymbol{x}_i]}{\Pr[\sum_{j=1}^m \boldsymbol{z}_j = h - \sum_{i=1}^n \boldsymbol{x}_i - (\boldsymbol{x}'_1 - \boldsymbol{x}_1)]} \right) \end{aligned}$$

We denote $\hat{h}$ to be the histogram of the fake records only $\hat{h} = h - \sum_{i=1}^n \boldsymbol{x}_i$, with respective counts in each histogram bin $\hat{h} = \{\hat{h}_1, \hat{h}_2, \dots, \hat{h}_d\}$. Then the privacy loss ratio can be written as:

$$L(h) = \log \left(\frac{\Pr[\sum_{j=1}^m \boldsymbol{z}_j = \hat{h}]}{\Pr[\sum_{j=1}^m \boldsymbol{z}_j = \hat{h} + \boldsymbol{x}_1 - \boldsymbol{x}'_1)]} \right)$$

The one-hot vectors $\boldsymbol{x}_1$ and $\boldsymbol{x}'_1$ may only differ in two positions, let these positions be ℓ and ℓ'. $\boldsymbol{x}_1$ and $\boldsymbol{x}'_1$ must have opposite bit-values in positions i and i' (otherwise these vectors are identical). Without loss of generality assume $x_{1,\ell} = 1, x_{1,\ell'} = 0$ and $x'_{1,\ell} = 0, x'_{1,\ell'} = 1$. Adding $\boldsymbol{x}_1$ adds 1 to h_i, while subtracting $\boldsymbol{x}'_1$ removes 1 from h'_ℓ. Hence, if $\hat{h} = \{\hat{h}_1, \hat{h}_2, \dots, \hat{h}_\ell, \dots, \hat{h}_{\ell'}, \dots, \hat{h}_d\}$, then $\hat{h} + \boldsymbol{x}_1 - \boldsymbol{x}'_1 = \{\hat{h}_1, \hat{h}_2, \dots, \hat{h}_\ell + 1, \dots, \hat{h}_{\ell'} - 1, \dots, \hat{h}_d\}$.

Further, note that the count the fake bits $\hat{h}_\ell = \sum_{j=1}^m \boldsymbol{z}_{j,\ell}$ is a binomial distribution $h_\ell \sim \mathrm{Bin}(m, 1/d)$, and the distribution of the fake bit counts across the bins takes the multinomial form $\hat{h} \sim \mathrm{Multinomial}(m, (1/d, \cdots, 1/d))$. We then aim to bound the following quantity.

$$\begin{aligned} L(h) &= \log\left(\frac{\Pr[\sum_{j=1}^m \boldsymbol{z}_j = \hat{h}]}{\Pr[\sum_{j=1}^m \boldsymbol{z}_j = \hat{h} + \boldsymbol{x}_1 - \boldsymbol{x}'_1]}\right) \\ &= \log\left(\frac{\binom{m}{\hat{h}_1, \hat{h}_2, \ldots, \hat{h}_\ell, \ldots, \hat{h}_{\ell'}, \ldots, \hat{h}_d}}{\binom{m}{hath_1, \hat{h}_2, \ldots, \hat{h}_\ell + 1, \ldots, \hat{h}_{\ell'} - 1, \ldots, \hat{h}_d}}\right) \\ &= \log\left(\frac{\hat{h}_\ell + 1}{\hat{h}_{\ell'}}\right) \end{aligned}$$

It must be stressed that for a given pair of $(\boldsymbol{x}_1, \boldsymbol{x}'_1)$, the corresponding position pair (ℓ, ℓ') where their bits are different is fixed, and the privacy loss only surfaces while observing the counts in the corresponding histogram bins $(h_\ell, h_{\ell'})$. It's entirely possible to see high ratio between counts in some other histogram bins, but it wouldn't contribute to the privacy loss for a concrete pair $(\boldsymbol{x}_1, \boldsymbol{x}'_1)$. This observation allows us to focus only on a single pair of the histogram bins, ignoring the rest of the histogram as immaterial.

By applying a Chernoff bound, we have a bound (symmetric for the upper and lower tail) for the sum of the fake bits in any bin $\hat{h}_k = \sum_{j=1}^m z_{j,k}, k \in [d]$

$$\Pr\left[\left|\hat{h}_k - \frac{m}{d}\right| > t\frac{m}{d}\right] \leq 2e^{-\frac{m}{d}\frac{t^2}{3}}, \qquad \text{for } 0 < t < 1.$$

Choose t to fit the expression below, hence $t = \sqrt{\frac{3d}{m}\log\frac{4}{\delta}}$. Using this expression for t turns our Chernoff bound into the following,

$$Pr\left[\left|\bar{h}_k - \frac{m}{d}\right| > \sqrt{\frac{3m}{d}\log\frac{4}{\delta}}\right] \leq \frac{\delta}{2} \tag{5.2}$$

Given any pair of the histogram bins at positions (ℓ, ℓ'), the probability of observing large deviation from the mean in at least one bin obeys the unions bound.

$$\Pr\left[\max_{k \in (\ell, \ell')}\left|\hat{h}_k - \frac{m}{d}\right| > \sqrt{\frac{3m}{d}\log\frac{4}{\delta}}\right] \leq \delta$$

We then condition on the event that both counts $\hat{h}_l$ or $\hat{h}_{l'}$ fall in the interval $m/d \pm \sqrt{\frac{3m}{d}\log\frac{4}{\delta}}$, which event occurs with probability at least $1 - \delta$. Conditioned on there being the given number of fake records, we can upper bound the privacy ratio $L(h)$

$$L(h) = \log\left(\frac{\hat{h}_\ell + 1}{\hat{h}_{\ell'}}\right) \leq \log\left(\frac{m/d + \sqrt{\frac{3m}{d}\log\frac{4}{\delta}} + 1}{m/d - \sqrt{\frac{3m}{d}\log\frac{4}{\delta}}}\right) \leq \epsilon \tag{5.3}$$

From the above, we then get a condition on the number of fake records, m, to ensure DP.

$$\begin{aligned}
&\frac{m/d + \sqrt{\frac{3m}{d}\log\frac{4}{\delta}} + 1}{m/d - \sqrt{\frac{3m}{d}\log\frac{4}{\delta}}} \leq e^\epsilon \\
\implies &\frac{m}{d}(e^\epsilon - 1) - \sqrt{\frac{3m}{d}\log\frac{4}{\delta}}(e^\epsilon + 1) - 1 \geq 0 \\
\implies &\frac{m}{d}(e^\epsilon - 1) - \sqrt{\frac{3m}{d}\log\frac{4}{\delta}}(e^\epsilon + 1) \geq 0 \\
\implies &\sqrt{\frac{m}{d}}\left(\sqrt{\frac{m}{d}}(e^\epsilon - 1) - \sqrt{3\log\frac{4}{\delta}}(e^\epsilon + 1)\right) \geq 0 \\
\implies &\sqrt{\frac{m}{d}}(e^\epsilon - 1) - \sqrt{3\log\frac{4}{\delta}}(e^\epsilon + 1) \geq 0 \\
\implies &\sqrt{\frac{m}{d}} \geq \frac{\sqrt{3\log\frac{4}{\delta}}(e^\epsilon + 1)}{e^\epsilon - 1} \\
\implies &\frac{m}{d} \geq 3\log\frac{4}{\delta}\left(\frac{e^\epsilon + 1}{e^\epsilon - 1}\right)^2
\end{aligned}$$

As for the lower bound of $L(h)$, it's met if the upper bound is met.

$$\begin{aligned}
&L(h) = \log\left(\frac{\hat{h}_\ell + 1}{\hat{h}_{\ell'}}\right) \geq \log\left(\frac{m/d - \sqrt{\frac{3m}{d}\log\frac{4}{\delta}} + 1}{m/d + \sqrt{\frac{3m}{d}\log\frac{4}{\delta}}}\right) \geq -\epsilon \\
\implies &\frac{m/d - \sqrt{\frac{3m}{d}\log\frac{4}{\delta}} + 1}{m/d + \sqrt{\frac{3m}{d}\log\frac{4}{\delta}}} \geq e^{-\epsilon} \\
\implies &\frac{m/d + \sqrt{\frac{3m}{d}\log\frac{4}{\delta}}}{m/d - \sqrt{\frac{3m}{d}\log\frac{4}{\delta}} + 1} \leq e^{\epsilon} \\
\implies &\frac{m/d + \sqrt{\frac{3m}{d}\log\frac{4}{\delta}}}{m/d - \sqrt{\frac{3m}{d}\log\frac{4}{\delta}} + 1} < \frac{m/d + \sqrt{\frac{3m}{d}\log\frac{4}{\delta}} + 1}{m/d - \sqrt{\frac{3m}{d}\log\frac{4}{\delta}}} \leq e^{\epsilon}
\end{aligned}$$

6 Fake records and bit flipping

We now apply the exact same protocol, whereby users produce n real and m fake reports, but require each 1-hot vector to bit bit-flipped with frequency q. A randomization procedure $\mathcal{R}(y)$ flips each bit of an arbitrary 1-hot-vector y with probability q and keeps it the same with probability $p = 1 - q$. The resulting mechanism M_r becomes a permutation of randomized true and fake records:

$$M_r(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n) = \pi(\mathcal{R}(\boldsymbol{x}_1), \ldots, \mathcal{R}(\boldsymbol{x}_n), \mathcal{R}(\boldsymbol{z}_1), \ldots, \mathcal{R}(\boldsymbol{z}_m)) \text{ where } \pi \text{ permutes its elements.}$$

Without los of generality assume $\boldsymbol{x}_1$ is replaced with $\boldsymbol{x}'_1$ to receive a neighboring data set $\boldsymbol{x}'$. The outcome is a histogram $g \in \mathbb{N}^d$ containing sums of randomized bits in each dimension, and the privacy loss:

$$L(g) = \log\left(\frac{\Pr[M_r(\boldsymbol{x}) = g]}{\Pr[M_r(\boldsymbol{x}') = g]}\right) \tag{6.1}$$

The combined set $\boldsymbol{x} + \boldsymbol{z}$ gives raise to a histogram $h \in \mathbb{N}^d$ received by applying the before discussed mechanism M (clear true records plus fake records). Hence, the $Pr[M_r(x) = g]$ can be written as a sum of probabilities over the domain of h:

$$\begin{aligned} Pr[M_r(x) = g] &= \sum_{h \in \mathbb{N}^d} Pr\left[M(\boldsymbol{x}) = h\right] \cdot Pr[g|h] \\ \implies L(g) &= \log\left(\frac{\sum_{h \in \mathbb{N}^d} Pr\left[M(\boldsymbol{x}) = h\right] \cdot Pr[g|h]}{\sum_{h' \in \mathbb{N}^d} Pr\left[M(\boldsymbol{x}') = h'\right] \cdot Pr[g|h']}\right) \end{aligned}$$

Noting that

$$Pr\left[M(\boldsymbol{x}) = h\right] = Pr\left[M(\boldsymbol{x}') = h - \boldsymbol{x}_1 + \boldsymbol{x}'_1\right]$$

And regrouping the privacy loss ratio to have summands with same $Pr\left[M(\boldsymbol{x}) = h\right]$ in identical positions in numerator and denominator, and applying (8.2) we have:

$$\begin{aligned} \log\left(\max_{h \in \mathbb{N}^d}\left(\frac{Pr\left[M(\boldsymbol{x}) = h\right] \cdot Pr[g|h]}{Pr\left[M(\boldsymbol{x}') = h - \boldsymbol{x}_1 + \boldsymbol{x}'_1\right] \cdot Pr[g|h - \boldsymbol{x}_1 + \boldsymbol{x}'_1]}\right)\right) &\geq L(g) \text{ , and} \\ L(g) \geq log\left(\min_{h \in \mathbb{N}^d}\left(\frac{Pr\left[M(\boldsymbol{x}) = h\right] \cdot Pr[g|h]}{Pr\left[M(\boldsymbol{x}') = h - \boldsymbol{x}_1 + \boldsymbol{x}'_1\right] \cdot Pr[g|h - \boldsymbol{x}_1 + \boldsymbol{x}'_1]}\right)\right) \end{aligned}$$

Probabilities $Pr\left[M(\boldsymbol{x}) = h\right]$ and $Pr\left[M(\boldsymbol{x}') = h - \boldsymbol{x}_1 + \boldsymbol{x}'_1\right]$ cancel each other out in each ratio, hence giving us the bounds of the privacy loss over domain of h .

$$\log\left(\max_{h\in\mathbb{N}^d}\left(\frac{Pr[g|h]}{Pr[g|h-\boldsymbol{x}_1+\boldsymbol{x}'_1]}\right)\right)\geq L(g)\geq log\left(\min_{h\in\mathbb{N}^d}\left(\frac{Pr[g|h]}{Pr[g|h-\boldsymbol{x}_1+\boldsymbol{x}'_1]}\right)\right)$$

Since bits are flipped independently, the probability of finding certain number of bits in a particular histogram bin g_l depends only on how many not-yet-randomized set bits there are in the dimension l, that is the value of h_l. Such independence allows to re-write $Pr[g|h]$ as a product of probabilities for each dimension.

$$Pr[M_r(x)=g]=Pr[\{g_1,g_2,,\ldots,g_d\}|\{h_1,h_2,,\ldots,h_d\}]=\prod_{i=1}^{d}Pr[g_i|h_i]$$

Without loss of generality assume that $\boldsymbol{x}_1$ and $\boldsymbol{x}'_1$ differ in the first and second positions, that is $\boldsymbol{x}_{1,1}=1,\boldsymbol{x}_{1,2}=0$ and $\boldsymbol{x}'_{1,1}=0,\boldsymbol{x}'_{1,2}=1$, then

$$\begin{aligned}
&h-\boldsymbol{x}_1+\boldsymbol{x}'_1=\{h_1-1,h_2+1,,\ldots,h_d\}\\
\Longrightarrow\ &\frac{Pr[g|h]}{Pr[g|h-\boldsymbol{x}_1+\boldsymbol{x}'_1]}=\frac{Pr[\{g_1,g_2,,\ldots,g_d\}|\{h_1,h_2,,\ldots,h_d\}]}{Pr[\{g_1,g_2,,\ldots,g_d\}|\{h_1-1,h_2+1,,\ldots,h_d\}]}\\
\Longrightarrow\ &\frac{Pr[g|h]}{Pr[g|h-\boldsymbol{x}_1+\boldsymbol{x}'_1]}=\frac{Pr[g_1|h_1]Pr[g_2|h_2]\prod_{i=3}^{d}Pr[g_i|h_i]}{Pr[g_1|h_1-1]Pr[g_2|h_2+1]\prod_{i=3}^{d}Pr[g_i|h_i]}\\
\Longrightarrow\ &\frac{Pr[g|h]}{Pr[g|h-\boldsymbol{x}_1+\boldsymbol{x}'_1]}=\frac{Pr[g_1|h_1]}{Pr[g_1|h_1-1]}\cdot\frac{Pr[g_2|h_2]}{Pr[g_2|h_2+1]}
\end{aligned}$$

Plugging the above formula into (6.1), the privacy loss bounds become:

$$\begin{aligned}
&\max_{h\in\mathbb{N}^d}\left(\log\left(\frac{Pr[g_1|h_1]}{Pr[g_1|h_1-1]}\cdot\frac{Pr[g_2|h_2]}{Pr[g_2|h_2+1]}\right)\right)\geq L(g)\geq\min_{h\in\mathbb{N}^d}\left(\log\left(\frac{Pr[g_1|h_1]}{Pr[g_1|h_1-1]}\cdot\frac{Pr[g_2|h_2]}{Pr[g_2|h_2+1]}\right)\right)\\
\Longrightarrow\ &\max_{h\in\mathbb{N}^d}\left(\log\left(\frac{Pr[g_1|h_1]}{Pr[g_1|h_1-1]}\right)\right)+\max_{h\in\mathbb{N}^d}\left(\log\left(\frac{Pr[g_2|h_2]}{Pr[g_2|h_2+1]}\right)\right)\geq L(g)\text{ , and}\\
&L(g)\geq\min_{h\in\mathbb{N}^d}\left(\log\left(\frac{Pr[g_1|h_1]}{Pr[g_1|h_1-1]}\right)\right)+\min_{h\in\mathbb{N}^d}\left(\log\left(\frac{Pr[g_2|h_2]}{Pr[g_2|h_2+1]}\right)\right)
\end{aligned}$$

Basically, the privacy loss is bound by the sum of privacy losses in each of the affected dimensions. Which enables relatively simple path to the bound. We employ the results of lemma (4.4), which says that if $\mathcal{R}$ is (ϵ,δ)-private on a collection r bits, it's also (ϵ,δ)-private on collection of $r+1$ bits. Therefore, a privacy loss could be bounded for the m fake records only, and that will provide sufficient noise for the extra n real records.

Suppose that r fake records (out of m) happened to have zero bits in the affected dimensions (1 and 2). We will show later that $r\to m$, for large d. Then we are bounding the product of privacy loss ratios in the affected dimensions to stay between $e^{-\epsilon}$ and e^{ϵ} with probability $1-\delta$.

$$P\left(e^{\epsilon}\geq\frac{Pr[g_1|h_1]}{Pr[g_1|h_1-1]}\cdot\frac{Pr[g_2|h_2]}{Pr[g_2|h_2+1]}\geq\frac{1}{e^{\epsilon}}\right)\leq 1-\delta \tag{6.2}$$

We achieve condition of (6.2) by bounding the ratio in each dimension separately. Suppose that the following holds

$$P\left(e^{\frac{\epsilon}{2}} \geq \frac{Pr[g_1|h_1]}{Pr[g_1|h_1-1]} \geq \frac{1}{e^{\frac{\epsilon}{2}}}\right) \leq 1-\delta/2$$

and

$$P\left(e^{\frac{\epsilon}{2}} \geq \frac{Pr[g_2|h_2]}{Pr[g_2|h_2+1]} \geq \frac{1}{e^{\frac{\epsilon}{2}}}\right) \leq 1-\delta/2$$

Then, by the union bound, the combined probability of either ratio falling outside its bound is δ, and with probability $1-\delta$, both ratios stay between $e^{-\frac{\epsilon}{2}}$ and $e^{\frac{\epsilon}{2}}$, hence the product of the ratios is bounded in $[e^{-\epsilon}, e^{\epsilon}]$.

Proposition 6.1.

7 Appendix: Ratios of sums: properties

Here we establish some results around bounding and comparing ratios of sums, which will be useful in working with the privacy ratio.

Lemma 7.1. *Suppose $a_1, \dots, a_m, b_1, \dots, b_m \in \mathbb{R}$ with $b_i > 0$ all i. Then*

$$\max\left(\frac{a_1}{b_1}, \dots, \frac{a_m}{b_m}\right) \geq \frac{a_1 + \cdots + a_m}{b_1 + \cdots + b_m} \geq \min\left(\frac{a_1}{b_1}, \dots, \frac{a_m}{b_m}\right).$$

Proof. Write

$$\frac{a_1 + \cdots + a_m}{b_1 + \cdots + b_m} = \frac{a_1}{b_1}\frac{b_1}{b_1 + \cdots + b_m} + \cdots + \frac{a_m}{b_m}\frac{b_m}{b_1 + \cdots + b_m} = \sum_{i=1}^{m} \frac{a_i}{b_i}\lambda_i$$

where $\lambda_1 + \cdots + \lambda_m = 1$. Then

$$\frac{a_1 + \cdots + a_m}{b_1 + \cdots + b_m} = \sum_{i=1}^{m} \frac{a_i}{b_i}\lambda_i \leq \sum_{i=1}^{m} \max\left(\frac{a_i}{b_i}\right)\lambda_i = \max\left(\frac{a_i}{b_i}\right)\sum_{i=1}^{m}\lambda_i = \max\left(\frac{a_i}{b_i}\right)$$

The low bound is derived in a similar fashion. □

References

[1] A Note on Differential Privacy: Defining Resistance to Arbitrary Side Information. Shiva Prasad Kasiviswanathan Adam Smith [2] Privacy Odometers and Filters: Pay-as-you-Go Composition. Ryan Rogers, Aaron Roth, Jonathan Ullman, Salil Vadhan

8 IGNORE BELOW THIS LINE

Suppose a new 1-bit is added to both collections, then $R_{n+1}(S)$ is derived by conditioning

$$R_{n+1}(S) = \frac{P(S|D \cup 1)}{P(S|D' \cup 1)} = \frac{P(S|D)q + P(S-1|D)p}{P(S|D')q + P(S-1|D')p}$$

By lemma (8.2) and lemma (4.2) we have

$$\begin{aligned} \frac{P(S-1|D)}{P(S-1|D'} \geq \frac{P(S|D)q + P(S-1|D)p}{P(S|D')q + P(S-1|D')p} \geq \frac{P(S|D)}{P(SD'} \qquad (8.1)\\ \implies R_n(S-1) \geq R_{n+1}(S) \geq R_n(S) \qquad (8.2)\\ \implies R_n(S) \geq R_{n+1}(S+1) \geq R_n(S+1) \qquad (8.3) \end{aligned}$$

Suppose R_n is (ϵ, δ)-private. Since R_n is monotonically decreasing with S (lemma (4.2)), there exist two values $\alpha + \beta \leq \delta$, such that R_n is upper bounded on the left at a particular limiting value S_α

$$R_n(S_\alpha) \leq e^\epsilon \text{ and } P_n(S \leq S_\alpha) \leq \alpha \qquad (8.4)$$

And it's low bounded on the right at a particular limiting value S_β

$$R_n(S_\beta) \geq \frac{1}{e^\epsilon} \text{ and } P_n(S \geq S_\beta) \leq \beta \qquad (8.5)$$

Consider the left (upper) bound first, and recall that according to (8.3)

$$R_n(S_\alpha) \geq R_{n+1}(S_\alpha + 1) \geq R_n(S_\alpha + 1)$$

$R_{n+1}(S_\alpha + 1)$ is bounded because $R_n(S_\alpha)$ is bounded per (8.4). Hence, R_{n+1} could only be over the bound at S_α, however the cumulative sum of probabilities up to S_α is always less for $n+1$ bits than for n bits.

$$P_{n+1}(S \leq S_\alpha) \leq P_n(S \leq S_\alpha) \qquad (8.6)$$

We shall prove (8.6) in a moment. The important fact is that R_n upper bounds R_{n+1} at the left tail of distribution of S.

Similarly,

As show by Wang, Y. H. (1993). "On the number of successes in independent trials", for any Poisson Binomial distribution, the probability of consecutive values are related as follows

$$\begin{aligned} P(S)^2 > P(S-1) \cdot P(S+1)\\ \implies \rho(S-1) > \rho(S)\\ \implies R(S-1) > R(S) \end{aligned}$$

Lemma 8.1. *The privacy loss reduces as S increases, reaching its maximum in $S = 0$ and minimum in $S = N$.*

the privacy loss reduces as S increases, reaching its maximum in $S = 0$ and minimum in $S = N$.

Note that $\frac{P(S|D)}{P(S-1|D)}$ as a **probability ratio** between adjacent values of S. It's easy to see that privacy loss ratio maximizes when **probability ratio** maximizes.

Recall that $p > q$ and consider two positive values A and B

$$\begin{aligned} \frac{p \cdot A + q}{p + q \cdot A} &\geq \frac{p \cdot B + q}{p + q \cdot B} \\ p^2 A + q^2 B &\geq p^2 B + q^2 A \\ A(p^2 - q^2) &\geq B(p^2 - q^2) \\ A &\geq B \end{aligned}$$

The above confirms that the distributions with largest **probability ratio** also exhibit larger privacy loss ratio. Hence we can focus on studying **probability ratio** instead of privacy loss ratio and choose those D that demonstrate sharpest decrease of probabilities in the left tail.

Consider a collection D of N bits, subjected to randomization procedure $\mathcal{R}$, whereby a bit is flipped with probability q and kept unchanged with probability $p = 1 - q$. The outcome of $\mathcal{R}$ is a a - sum of bits after randomization. The neigboring set D_m is recieved form Assuming that D contains m set bits, we consider a privacy loss ratio R_s computed for the outcome s:

$$R_s = \frac{P(s|D)}{P(s-1|D)}$$

consisting of m ones and $N - m$ zeros. Denote probability of number of successes for that collection as $P(S|D)$. The probability ratio at s is given by:

$$R_s = \frac{P(s|D)}{P(s-1|D)}$$

Denote expectation of s as μ:

$$\mu = mp + (N - m)q$$

For simplicity, denote probabilities at s for D as:

$$P(s|D) = P_s$$

It's known that for all $s < \mu$, the ratio R_s is greater than 1 and increasing:

Property 1.

$$R_{s-1} = \frac{P_{s-1}}{P_{s-2}} > R_s = \frac{P_s}{P_{s-1}} \tag{8.7}$$

$$P_{s-1}^2 > P_s P_{s-2} \tag{8.8}$$

Create two collections by adding to D one 1 and one 0. Call them D_1 and D_0 respectively. The probability of observing s from D_1 the is given by:

$$P(s|D_1) = pP_{s-1} + qP_s$$

Similarly for the second collection (with extra 0):

$$P(s|D_0) = qP_{s-1} + pP_s$$

Now consider the probability ratio for the collections D_1 and D_0 collections at some s:

$$R_s(D_1) = \frac{pP_{s-1} + qP_s}{pP_{s-2} + qP_{s-1}} \tag{8.9}$$

$$R_s(D_0) = \frac{qP_{s-1} + pP_s}{qP_{s-2} + pP_{s-1}} \tag{8.10}$$

N user bits are subjected to

Lemma 8.2. *Suppose $a_1, \ldots, a_m, b_1, \ldots, b_m \in \mathbb{R}$ with $b_i > 0$ all i. Then*

$$\max\left(\frac{a_1}{b_1}, \ldots, \frac{a_m}{b_m}\right) \geq \frac{a_1 + \cdots + a_m}{b_1 + \cdots + b_m} \geq \min\left(\frac{a_1}{b_1}, \ldots, \frac{a_m}{b_m}\right).$$

Proof. Write

$$\frac{a_1 + \cdots + a_m}{b_1 + \cdots + b_m} = \frac{a_1}{b_1}\frac{b_1}{b_1 + \cdots + b_m} + \cdots + \frac{a_m}{b_m}\frac{b_m}{b_1 + \cdots + b_m} = \sum_{i=1}^{m} \frac{a_i}{b_i}\lambda_i$$

where $\lambda_1 + \cdots + \lambda_m = 1$. Then

$$\frac{a_1 + \cdots + a_m}{b_1 + \cdots + b_m} = \sum_{i=1}^{m} \frac{a_i}{b_i}\lambda_i \leq \sum_{i=1}^{m} \max\left(\frac{a_i}{b_i}\right)\lambda_i = \max\left(\frac{a_i}{b_i}\right)\sum_{i=1}^{m}\lambda_i = \max\left(\frac{a_i}{b_i}\right)$$

The low bound is derived in a similar fashion. □

9 JUNK

Given the independence

$$Pr[M_r(x) = g] = \sum_{h \in \mathbb{N}^d} Pr\left[M(\boldsymbol{x}) = h\right] \cdot Pr[g|h] = \sum_{h \in \mathbb{N}^d} \left(Pr\left[M(\boldsymbol{x}) = h\right] \cdot \prod_{i=1}^{d} Pr[g_i|h_i] \right)$$

$$\implies L(g) = \log \left(\frac{\sum_{h \in \mathbb{N}^d} \left(Pr\left[M(\boldsymbol{x}) = h\right] \cdot \prod_{i=1}^{d} Pr[g_i|h_i] \right)}{\sum_{h' \in \mathbb{N}^d} \left(Pr\left[M(\boldsymbol{x}') = h'\right] \cdot \prod_{i=1}^{d} Pr[g_i|h'_i] \right)} \right)$$

More formally, the value of g_l is a sum of binomial distributions Where r is the number of set bits (both clear and fake) in the dimension l. This allows us to

The value of g_l distributed as a sum of two binomial variables.

$$g_l \sim Bin(h_l, p) + Bin(n + m - h_l, q)$$

Applying (8.2) gives bounds of $R(S)$

$$\frac{p \cdot P(S|D) + q \cdot P(S-1|D)}{p \cdot P(S-1|D) + q \cdot P(S|D)} R(S|D) = \frac{p \cdot P(S|D) + q \cdot P(S-1|D)}{p \cdot P(S-1|D) + q \cdot P(S|D)} \tag{9.1}$$