1) let $t \in \{-1,0,1\}^n$ be a vector with at least m non-zero entries and let $u \in \{0,1\}^n$ be a uniformly random vector.
We want to show that:

$$\Pr(|u \cdot t| \le \sqrt{m}/4) \le c \quad , \quad c<1$$

because u is uniformly random, and m entries of t are non zero, $|u \cdot t|$ would be the sum of approximately $m/2$ independent variables with value $\{-1,1\}$, essentially a random walk. And by the CLT, with n and m sufficiently large, $|u \cdot t|$ is approximately gaussian.
We can thus use a normal approximation for the simple random walk

$\hookrightarrow \mathrm{Var}(|u \cdot t|) = m/2$

thus, the standard deviation of $|u \cdot t|$ is approximately $\sqrt{m/2}$.
thus, the probability of it falling between $[-\sqrt{m}/4, \sqrt{m}/4]$ (z-score $= \frac{1}{\sqrt{2}}$) is approximately 0.52, which is a constant less than 1.

another explaination is that the

the r.v. $|u \cdot t|$ behave like a $N(0, m/2)$,

and the STD is $\sqrt{m/2}$, we can say the STD is

at least $\sqrt{m}/2$ with high probability. This would

also make $Pr(|u \cdot t| \leq \sqrt{m}/4) \leq \frac{7}{10}$. In other words, it

is bounded away from 1, with a constant strictly

less than 1.

However, we do have error, since this problem is discrete

and we also cannot grarentee exactly $m/2$, but due to

large n, m, and CLT, we can be pretty condident it

is close, so it is a grassian as well. So the error of

$c =$ 0.9, when we had stricter constants like 0.52 and 0.7,

comes from the fact that the variance can change based

on the # of "random walks" we take, but is still at

least $\sqrt{m}/2$ with high probability (larger bound for error)

Thus, we can still say that $Pr(|u \cdot t| \leq \sqrt{m}/4) < c$, $c < 1$

and in this case we set c to be the generous term $9/10$

Back to the problem, if $D_0 \in B$, it differs from D by at least $256\alpha^2 n^2$ indicies, if $t = D_0 - D$, $t \in \{-1, 0, 1\}^n$ and t has at least $256\alpha^2 n^2$ non zero entries. And since queries are chosen at random, s_j is chosen at random uniformly $s_j \in \{0,1\}^n$, $s_j = F_j$

Then, $Pr(|F_j \cdot (D - D_0)| \leq \frac{\sqrt{256\alpha^2 n^2}}{4}) \leq 9/10$

from the previous part, which simplifies to

$Pr(|q_{s_j}(D_0) - q_{s_j}(D)| \leq 4\alpha n) \leq \frac{9}{10}$

2) let $y = \{M(s(X;I)) \quad \}$

we can use.

$$Pr(B|A) = \frac{P(A,B)}{P(A)}$$

then, $$Pr(y \in T \mid 1 \in I) = \frac{Pr(y \in T \cap 1 \in I)}{Pr(1 \in I)}$$

$$= \frac{\sum_{1 \in I} Pr(y \in T \in I)}{m/n}$$

Similarly, $$Pr(y \mid 1 \notin I) = \frac{Pr(y \in T \cap 1 \notin I)}{Pr(1 \notin I)} = \frac{\sum_{1 \notin I} Pr(y \in T \notin I)}{\frac{n-m}{n}}$$

Then, we have

$$(n-m) \sum_{1 \in I} Pr(y \in T, I) \leq e^{\varepsilon} m \sum_{1 \notin I} Pr(y \in T, I)$$

$= (n-m)(m/n) \leq (m)\left(\frac{n-m}{n}\right) e^{\varepsilon}$, since $1 \in I$ is mapped m times and $1 \notin I$ is mapped $\frac{n-m}{n}$ times

$= 1 \leq e^{\varepsilon}$, which is always true.

3) if we don't know anything about the size of the sets G_i, the sensitivity is trivially 2. This is because if we have a 2 clusters, $n=1$, and G_1 contains $\|X_i\|_1 = 1$, then if we change it so that $\|X_i\| = 1$ but now belongs to G_2, we have a change of 1 in both C_1' and C_2', with the ℓ_1-sensitivity then being 2.

more formally, since changing one value x can shift one data point from one to another changing the $|G_i|$ both by a maximum of 1 and C_i by $\frac{1}{|G_i|}$

$$\max(f) \left(0 + \frac{1}{|G_i|_{min}} \right) + \left(0 + \frac{1}{|G_j|_{min}^{2nd}} \right), \; i \neq j$$

$$\leq \frac{2}{\min_i |G_i|}$$

4) a) define $A = M(D) \in S$

$B = M(D') \in S$

we can break this problem down for all subsets S

1) if S is empty or doesn't contain D, D', or $\perp$

$|Pr(A) - Pr(B)| = |0-0| \leq \delta$

2) if S contains $D, D', \perp$

$|Pr(A) - Pr(B)| = |1-1| = 0 \leq \delta$

3) S contains D, D' but not $\perp$

$|Pr(A) - Pr(B)| = |\delta - \delta| = 0 \leq \delta$

4) S contains D and not $D', \perp$

$|Pr(A) - Pr(B)| = |\delta - 0| = \delta \leq \delta$

5) $D' \in S$, $D, \perp \notin S$

$|Pr(A) - Pr(B)| = |0-\delta| = \delta \leq \delta$

6) $\perp \in S$, $D, D' \notin S$

$|Pr(A) - Pr(B)| = |1-\delta-(1-\delta)| = 0 \leq \delta$

7) $\perp, D \in S$, $D' \notin S$ and $\perp, D' \in S$, $D \notin S$

$|Pr(A) - Pr(B)| = |1-(1-\delta)| = \delta = \delta \leq \delta$

Since $|Pr(A) - Pr(B)| \leq \delta$, M is δ-DP

4) b) without loss of generality, let $x \sim x'$ differ at x_1, with $x[0] = x'$

for $S = \{S_1, \dots, S_n\}$

Then, $\Pr(M(x) = S) = \Pr(Y_1 = S_1) \prod_{j=2}^{n} \Pr(Y_j = S_j)$

$\Pr(M(x') = S) = \Pr(Y_1' = S_1) \prod_{j=2}^{n} \Pr(Y_j' = S_j)$

since $Y_j = S_j$ for $2 \le j \le n$

$\prod_{j=2}^{n} \Pr(Y_j = S_j) = \prod_{j=2}^{n} \Pr(Y_j' = S_j) \le 1$

subtracting

$\underbrace{\Pr(M(x) = S) - \Pr(M(x') = S)}$ $= \left(\prod_{j=2}^{n} \Pr(Y_j = S_j)\right) \to \le 1$

$\cdot \left(\Pr(Y_1 = S_1) - \Pr(Y_1' = S_1)\right)$

$\le \Pr(Y_1 = S_1) - \Pr(Y_1' = S_1)$

if $S_1 = x_1$, then

$\Pr(Y_1 = S_1) - \Pr(Y_1' = S_1) = \delta - 0 = \delta$

if $S_1 = x_1'$, then $\Pr(Y = S_1) - \Pr(Y_1' = S_1) = 0 - \delta = -\delta$

if $S_1 \ne x_1, x_1'$, then $\Pr(Y_1 = S_1) - \Pr(Y_1' = S_1) = 0 - 0 = 0$

if $S_1 = \perp$, then $\Pr(Y_1 = S_1) - \Pr(Y_1' = S_1) = 1-\delta - (1-\delta) = 0$

then $|\Pr(M(x) = S) - \Pr(M(x') = S)| \le \delta$,

which is δ-DP

5) Take $n=1$, and $X = \{1\}$. Then, $X' = \{0\}$

then, for all ε, there exist an interval S where

$Pr(\tilde{f}(X') \in S) = 0$, and $Pr(\tilde{f}(X) \in S) > 0$,

where

$$Pr(\hat{f}(X) \in S) \leq e^{\varepsilon} Pr(\tilde{f}(X') \in S)$$

$$= c \leq e^{\varepsilon}(0) \quad , \text{ where } c > 0$$

which fails the definition of ε-DP

for all $\varepsilon \in \mathbb{R}$, the interval $[-3/\varepsilon, 3/\varepsilon]$, where the last interval $[3/\varepsilon - 1, 3/\varepsilon]$ that $\tilde{f}(X')$ applies has probability 0, since $0 + 3/\varepsilon$ (highest that $\tilde{f}(X')$ can produce is always $\leq 1 + 3/\varepsilon$ which is what $\tilde{f}(X)$ can produce. Thus, $Pr(\tilde{f}(X) \in [3/\varepsilon - 1, 3/\varepsilon]) = \frac{\varepsilon}{6}$, but $Pr(\tilde{f}(X') \in [3/\varepsilon - 1, 3/\varepsilon]) = 0$, if $\varepsilon > 6$ the intervals don't overlap, also not ε-DP

so $\frac{\varepsilon}{6} \leq e^{\varepsilon}(0)$ doesn't satisfy the definition of ε-DP

if $\varepsilon > 6$, then the intervals are completely disjoint, giving zero privacy.

6) (M1) $M1(x) = [\bar{x} + Z]_0^1$, $Z \sim Lap(2/n)$

Clamping $\bar{x}+Z$ is a post processing step, and we proved post processing does not reveal additional information.

more formally, if $g(x) = \bar{x} + Z$, which is ε-DP, then $M_1(x) = [g(x)]_0^1$ is also ε-DP by post processing

Thus, M_1 is still ε-DP

To find the smallest value of ε, we know $Lap(\Delta/\varepsilon)$ is ε-DP so we find Δ.

$\Delta \bar{x} = 1/n$ (we can change one value from 0 to 1)

so $Lap\left(\frac{1/n}{\varepsilon}\right) = Lap(2/n)$

$\rightarrow \varepsilon = 1/2$,

$M_1(x)$ is $1/2$-DP

6) (M2) from the prev part, we have $\Delta = 1/n$

$$\frac{Pr(M2(x)=1)}{Pr(M2(x')=1)} \leq e^{\varepsilon}$$ to satisfy DP.

However if $\bar{x}$ change by $1/n$, the above ratio is

$$\frac{\bar{x}+1/n}{\bar{x}} \leq e^{\varepsilon}.$$ If $\bar{x}=0$ (x' is all zero and x has 1 one), then it is infinite and $\geq e^{\varepsilon}$.

Similarly, $$\frac{Pr(M2(x)=0)}{Pr(M2(x')=0)} \leq e^{\varepsilon}$$

$$= \frac{1-\bar{x}}{1-\bar{x}-\frac{1}{n}} \leq e^{\varepsilon}$$ where if $\bar{x} = 1-1/n$, it goes to infinite again, as there is no bound on n.

Thus, there is no ε where $\frac{Pr(M2(x)=0 \text{ or } 1)}{Pr(M2(x')=0 \text{ or } 1)}$ where e^{ε} is bounded by infinite, so M2 is not ε-DP for any finite ε.

7) a) $X \sim X'$. without loss of generality, let's say they differ at first element, X_1 and X_1'

if $X_1' = X_1 + c$, when $c > 2tn$

$$f(X') = f(X) + c/n = f(X) + 2t$$

$\frac{1}{e}$

for 1-DP, we have

$$Pr(M(X) \in S) \le e \, Pr(M(X') \in S)$$

suppose that $Pr(|M(X) - f(X)| < t) \ge 0.9$ for $t \in \mathbb{R}$, X.

Let $S = [f(X)-t, f(X)+t]$, $T = [f(X')-t, f(X')+t]$

$\rightarrow$ $Pr(M(X) \in S) \ge 0.9$ since S and T disjoint

then, $Pr(M(X') \in S) \le 1 - \underbrace{Pr(|M(X') - f(X')| \le t)}_{\text{if } \ge 0.9}$

$$Pr(M(X') \in S \le 0.1$$

from DP, $0.9 \le Pr(M(X) \in S) \le e \, Pr(M(X') \in S)$.

plugging our numbers in

$0.9 \le e \cdot 0.1$, which is a contradiction. Thus, for any finite $t > 0$, there is no 1-DP algorithm M s.t. $Pr(|M(X) - f(X)| \le t) \ge 0.9$

7) b) here, the max Δ happens if we change one value in X from $-R$ to R or vise versa, resulting in an Δ of $\frac{2R}{n}$.

then, this is just a scaled case of $M(X)$ in the $X \in \{0,1\}^n$ case, where $A_2(X) = f(X) + Lap(2R/\varepsilon n)$, where $2R/n = \Delta$, which we already proved is ε-DP

Then, $Pr(|A_2(X) - f(X)| \leq \frac{CR}{n\varepsilon}) \geq 0.9$ is just

$Pr(|Z| \leq \frac{CR}{n\varepsilon}) \geq 0.9$, where $Z \sim Lap(2R/\varepsilon n)$ is a r.v.

using the cdf for $Lap(b) \rightarrow 1/2 \cdot \exp(-t/b)$. Since we are taking the absolute value, our interval is 2x this, so

$Pr(|Lap(b)| \leq t) = 1 - e^{-t/b}$ $\rightarrow$ CDF of $Lap(b)$ $\frac{1}{2}\exp(\frac{x-\mu}{b})$ $x \leq \mu$

then, $Pr(|Lap(2R/n\varepsilon)| \leq CR/n\varepsilon \geq 0.9$

$1 - e^{-(CR/n\varepsilon)/(2R/n\varepsilon))} =$

$= 1 - e^{-C/2} \geq 0.9. \quad = \quad e^{-C/2} \leq 0.1$

$\underline{C \geq 2\ln(10)}$. This value of C

satisfies $Pr(|A_2(X) - f(X)| \leq \frac{CR}{2\varepsilon}) \geq 0.9$.

3) a) for each X_i, $Y_i = X_i$ w.p. $\frac{e^\varepsilon}{e^\varepsilon + k - 1}$. This is porportional to e^ε

for $s \in \{1, \dots, k\} \setminus \{X_i\}$, $Y_i = s$ w.p. $\frac{1}{e^\varepsilon + k - 1}$.

Then, for all $s \in \{1, \dots, k\}$, $Pr(X_i \in S) = \frac{e^\varepsilon}{e^\varepsilon + k - 1} + \frac{k-1}{e^\varepsilon + k - 1} = 1$

$X \sim X'$. Formally, $Pr(Y_i = y \mid X_i = x_i) = \begin{cases} e^\varepsilon / e^\varepsilon + k - 1 & y_i = x_i \\ 1 / e^\varepsilon + k - 1 & y_i \neq x_i \end{cases}$

without loss of generality, say $X \sim X'$ differs at X_1.

then, $$\frac{Pr(Y = y \mid X)}{Pr(Y = y \mid X')} = \frac{Pr(Y_1 = y_1 \mid X_1)}{Pr(Y_1 = y_1 \mid X_1')} \underbrace{\prod_{j=2}^{n} \frac{Pr(Y_j = y_j \mid X_j)}{Pr(Y_j = y_j \mid X_j')}}_{=1,\ \text{since } X_j = X_j' \text{ for } 2 \le j \le n}$$

$$= \frac{Pr(Y_1 = y_1 \mid X_1 = a)}{Pr(Y_1 = y_1 \mid X_1' = b)} \quad \text{if } \begin{matrix} X_1 = a \\ X_1' = b \end{matrix}$$

Then if $Y_1 = a$

$$= \frac{Pr(Y_1 = a \mid X_1 = a)}{Pr(Y_1 = a \mid X_1' = b)} = \frac{e^\varepsilon / e^\varepsilon + k - 1}{1 / e^\varepsilon + k - 1} = e^\varepsilon$$

cont

if $Y_1 = b$

$$\frac{Pr(Y_1 = b \mid X_1 = a)}{Pr(Y_1 = b \mid X_1' = b)} = \frac{1/e^{\varepsilon}+|k|-1}{e^{\varepsilon}/e^{\varepsilon}+|k|-1} = e^{-\varepsilon}$$

if $Y_1 = c$

$$\frac{Pr(Y_1 = c \mid X_1 = a)}{Pr(Y_1 = c \mid X_1' = b)} = \frac{1/e^{\varepsilon}+|k|-1}{1/e^{\varepsilon}+|k|-1} = 1$$

Thus, the probability is bounded by e^{ε}, proving ε-DP

8) b) convert X_i to a one-hot vector $v_i \in \{0,1\}^k$

$$v_{ij} = \begin{cases} 1 & \text{if } j = X_i \\ 0 & \text{if } j \neq X_i \end{cases}$$

for all v_i, if $v_{ij} = 1$. Let $\varepsilon' = \varepsilon/2$.

$$Y_{ij} = \begin{cases} v_{ij} & \text{w.p. } e^{\varepsilon'}/e^{\varepsilon'}+1 \\ 1-v_{ij} & \text{w.p. } 1/e^{\varepsilon'}+1 \end{cases}$$

similar to the last part, suppose differ at $v_{1,a} = 1$, $v_{1,b} = 0$

$v'_{1,a} = 0$, $v'_{1,b} = 1$

$$\frac{Pr(Y=y \mid X)}{Pr(Y=y \mid X')} = \frac{Pr(Y_1 = y \mid V_1)}{Pr(Y_1 = y \mid V_1')} \cdot \prod_{j=2}^{n} \frac{Pr(Y_j = y \mid V_j)}{Pr(Y_j = y \mid V_j')} \quad =1$$

Then, $$\frac{Pr(Y_{1,a} \mid V_{1,a}=1)}{Pr(Y_{1,a} \mid V'_{1,a}=0)} = \begin{cases} \dfrac{e^{\varepsilon'}/(e^{\varepsilon'}+1)}{1/(e^{\varepsilon'}+1)} = e^{\varepsilon/2} & Y_{1,a}=1 \\ \dfrac{1/(e^{\varepsilon'}+1)}{e^{\varepsilon'}/(e^{\varepsilon'}+1)} = e^{-\varepsilon/2} & Y_{1,a}=0 \end{cases}$$

$$\frac{Pr(Y_{1,b} \mid V_{1,b}=0)}{Pr(Y_{1,b} \mid V'_{1,b}=1)} = \begin{cases} \dfrac{1/(e^{\varepsilon'}+1)}{e^{\varepsilon'}/(e^{\varepsilon'}+1)} = e^{-\varepsilon/2} & Y_{1,b}=1 \\ \dfrac{e^{\varepsilon'}/(e^{\varepsilon'}+1)}{1/(e^{\varepsilon'}+1)} = e^{\varepsilon/2} & Y_{1,b}=0 \end{cases}$$

if $c \neq a, b$, then $\dfrac{Pr(Y_{1,c} \mid V_{1,c})}{Pr(Y_{1,c} \mid V'_{1,c})} = 1$

Then for worst case $Y_{1,a} = 1$ and $Y_{1,b} = 0$, we have $\dfrac{Pr(Y_{ij} \mid V_j)}{Pr(Y_{ij} \mid V_j')} = e^{\varepsilon/2} \cdot e^{\varepsilon/2} = e^{\varepsilon}$,

which satisfies ε-DP

9) (M1). Intuitively, we need to find the probability that $z \sim Lap(2/n) > 1$ or < -1, and have δ be that probability, since M_1 is ε-DP within the interval but not outside (similar to HW#5), so we need $\delta = Pr(|Lap(b)| > 1)$

The CDF of $Lap(b)$ is $\frac{1}{2}\exp(\frac{x-\mu}{b})$ for $x \le \mu$.

$Pr(|Lap(b)| \ge 1) = e^{-n/2}$

Then, $\delta = e^{-n/2}$, and $M_1(x)$ is $(\varepsilon, e^{-n/2})$-DP

9) (M2) This is like a continuation of of problem 6.
The issue there was that there exists a case where
in the worst, case, we had

$$\Pr(M_2(x)=1) \le e^{\varepsilon} \cdot \Pr(M_2(x')=1),$$

where worst case x has one 1, and x' is all zeros,
we have $\frac{1}{n} \le e^{\varepsilon} \cdot 0$, so we need to set the
$\delta = 1/n$ so it satisfies (ε, δ)-DP, with

$$\delta = 1/n.$$

Then, $1/n \le e^{\varepsilon} \cdot 0 + 1/n$ works, and is
$(\varepsilon, 1/n)$-DP

10) a) we can show this via an example. In the simple case, let $n=1$, and $X_1 = (b, b)$. Here $\beta(b,b) = \frac{b^2}{b^2} = 1$.

Then, if we choose $X_1 \sim X_1'$ so $X' = (0, 1)$ (or $\lim_{x \to 0} x, b$),

then $B(X') = \frac{b}{\lim_{x \to 0} \infty}$, which is infinite. So Δ is also infinite, and we cannot use regular DP to get a useful estimate

b) $S_{xy} = \sum_i x_i y_i$. Suppose we change (x_i, y_i) to (x_i', y_i')

$$\Delta = \max_{x_i, y_i, x_i', y_i' \in [-b, b]} |x_i y_i - x_i' y_i'|$$. This max is reached

when $x_i y_i = b^2$ and $x_i' y_i' = -b^2$, so Δ is $2b^2$

Thus, $S_{xy} + \text{Lap}(2b^2/\varepsilon)$ is ε-DP for S_{xx}, $\Delta = \max_{x_i, x_i' \in [-b, b]} |x_i^2 - x_i'^2| \leq b^2$, since

x_i^2 and $x_i'^2$ are $\in [0, b^2]$

$S_{xx} + Lap(b^2/\varepsilon)$ is ε-DP

c) we first clip the dataset so for each x_i, y_i,

$$x_i = \begin{cases} b & x_i > b \\ x_i & -b \leq x_i \leq b \\ -b & \text{if } x_i < -b \end{cases} \qquad y_i = \begin{cases} b & y_i > b \\ y_i & -b < y_i < b \\ -b & y_i < -b \end{cases}$$

We can just use simple post processing, with $\varepsilon = \varepsilon/2$ on both

so it is ε overall

$$\tilde{S}_{xy} = S_{xy} + Lap\left(\frac{2b^2}{\frac{\varepsilon}{2}}\right) = S_{xy} + Lap\left(\frac{4b^2}{\varepsilon}\right)$$

$$\tilde{S}_{xy} = S_{xx} + Lap\left(\frac{b^2}{\frac{\varepsilon}{2}}\right) = S_{xx} + Lap\left(\frac{2b^2}{\varepsilon}\right)$$

then, $\tilde{\beta} = \dfrac{\tilde{S}_{xy}}{\tilde{S}_{xx}}$

and β is ε-DP overall