1 Combining MW Update Rule w/ Sparse Vector

The queries to Sparse Vector will be about the error $E_i = |f_i(x) - f_i(x^t)|$. Sparse Vector can only notify if something is above threshold. Since Sparse Vector cannot capture the absolute value, two copies of Sparse Vector must be run to ask about $f_i(x) - f_i(x^t)$ and $f_i(x^t) - f_i(x)$.

\begin{algorithm}
\textbf{Algorithm 1} Private MW($x$, $\{f_i\}$, $\epsilon, \delta, \alpha, \beta, Q$)

\begin{enumerate}
  \item Let $c = \frac{4 \ln|\mathbb{X}|}{\alpha^2}$,
  \item if $\delta = 0$ then
    \begin{enumerate}
      \item Let $T = \frac{18c(\ln(2|Q|) + \ln(\frac{4c}{\beta}))}{\epsilon \|x\|}$
    \end{enumerate}
  \item else
    \begin{enumerate}
      \item Let $T = \frac{(2 + 32\sqrt{2})\sqrt{c\ln(2/\delta)(\ln(k) + \ln(\frac{4c}{\beta}))}}{\epsilon \|x\|}$
    \end{enumerate}
  \end{enumerate}

\textbf{end if}

Initialize Sparse($x$, $\{f_i\}$, $T$, $c$, $\epsilon$, $\delta$), Outputting $\{E_i\}$

Let $t = 0, x^o \in \Delta(\mathbb{X})$ s.t. $x^o_i = \frac{1}{|\mathbb{X}|}$ \forall $i \in |\mathbb{X}|$

\textbf{for all} Queries $f_i$ \textbf{do}

\begin{enumerate}
  \item Let $f_{2i-1}'(x) = f_i - f_i(x^t)$
  \item Let $f_{2i}(x) = f_i(x^t) - f_i(x)$
  \item if $E_{2i-1} = \bot$ and $E_{2i} = \bot$ \textbf{then}
    \begin{enumerate}
      \item Let $a_i = f_i(x^t)$
    \end{enumerate}
  \item else
    \begin{enumerate}
      \item if $E_{2i-1} \in \mathbb{R}$ \textbf{then}
        \begin{enumerate}
          \item Let $a_i = f_i(x^t) + E_{2i-1}$
        \end{enumerate}
      \item else
        \begin{enumerate}
          \item Let $a_i = f_i(x^t) - E_{2i}$
        \end{enumerate}
    \end{enumerate}
  \end{enumerate}

\textbf{end if}

Let $x^{t+1} = MW(x^t, f_i, a_i)$

Let $t = t + 1$

\textbf{end for}
\end{algorithm}
Theorem 1. Private MW is \((\varepsilon, \delta)-\text{DP}\)

Proof. Follows immediately from privacy of Sparse Vector because Private MW only accesses the data through Sparse Vector. Everything else is post-processing.

\(\square\)

Theorem 2. With probability \((1 - \beta)\), \(\forall f_i\), Private MW returns an answer \(a_i\) s.t. \(|f_i(x) - a_i| \leq 3\alpha\) for:

\((\delta = 0)\),

\[\alpha = \left( \frac{36 \ln|X| \left[ \ln|Q| + \ln \left( \frac{32 \ln|X|^{\frac{1}{2}} \|x\|^{\frac{2}{3}}}{\beta} \right) \right]}{\|x\|^2 \varepsilon} \right)^{\frac{1}{2}}\]

\((\delta > 0)\),

\[\alpha = \left( \frac{(2 + 32\sqrt{2}) \sqrt{\ln|X| \ln \frac{2}{\delta} \left( \ln|Q| + \ln \frac{32\|x\|}{\beta} \right)}}{\|x\|^2 \varepsilon} \right)^{\frac{1}{2}}\]

Remark 1. When \(\delta > 0\), accuracy is better in terms of \(\|x\|\) because of the better composition theorems for \((\varepsilon, \delta)\)-DP.

Proof. Use Sparse Vector accuracy theorem to show that w.h.p,

1. MW update rule is only called when \(|f_i(x) - f_i(x^t)|\) is large,

2. and the released noisy approximation to \(f_i(x)\) is accurate.

Recall from Lecture 10, these were the two conditions needed to prove that MW converged quickly. Then use MW convergence theorem to show that after \(c = \frac{4 \ln|X|}{\alpha^2}\) updates, Private MW answers all queries in \(Q\) approximately correctly.

\(\square\)

Sparse Vector gives error that scales like \(O \left( \frac{\ln|X| \left[ \ln|Q| + \ln \frac{\varepsilon}{\beta} \right]}{\varepsilon \|x\| \alpha^2} \right)\) for k-sensitivity \(\frac{1}{\|x\|}\) queries, where at most \(c\) are above threshold. The only "payment" in the privacy budget is for those \(c\) queries, so noise \(O \left( \frac{c}{\varepsilon \|x\|} \right)\) can be added to each query.

In this case where \(k = |Q|\) and \(c = \frac{4 \ln|X|}{\alpha^2}\). These bounds are achieved by plugging this into the Sparse Vector guarantee

\[\alpha = O \left( \frac{\ln|X| \left[ \ln|Q| + \ln \frac{\varepsilon}{\beta} \right]}{\varepsilon \|x\| \alpha^2} \right)\]

and solving.