APPENDIX.A

We present detailed estimates of

$$\sum_{\mathbf{y}\in\Sigma_q^{n-tb}} |D_t^b(\mathbf{y})|^{-1},$$

which were omitted in Section IV, and which complete the proof of the upper bound on $M_q(n,(t,b))$.

Note that

$$\sum_{\mathbf{y}\in\Sigma_q^{n-tb}} |D_t^b(\mathbf{y})|^{-1} = \sum_{r=1}^{n-(t+1)b+1} \sum_{\substack{\mathbf{y}\in\Sigma_q^{n-tb}\\ |U_b(\mathbf{y})|=r}} |D_t^b(\mathbf{y})|^{-1}.$$

Thus, by the lower bound on $|D_t^b(\mathbf{y})|$ in Theorem 2, we have

$$\begin{aligned}
&\sum_{\mathbf{y}\in\Sigma_q^{n-tb}} |D_t^b(\mathbf{y})|^{-1}\\
\le&\sum_{r=r'+1}^{n-(t+1)b+1} \sum_{\substack{\mathbf{y}\in\Sigma_q^{n-tb}\\ |U_b(\mathbf{y})|=r}} \binom{r-(t-1)b}{t}^{-1}\\
&+\sum_{r=1}^{r'} \sum_{\substack{\mathbf{y}\in\Sigma_q^{n-tb}\\ |U_b(\mathbf{y})|=r}} 1\\
=&\sum_{r=r'+1}^{n-(t+1)b+1} \frac{\left|\{\mathbf{y}\in\Sigma_q^{n-tb} : |U_b(\mathbf{y})|=r\}\right|}{\binom{r-(t-1)b}{t}}\\
&+\sum_{r=1}^{r'} \left|\{\mathbf{y}\in\Sigma_q^{n-tb} : |U_b(\mathbf{y})|=r\}\right|\\
=&q^b \sum_{r=r'+1}^{n-(t+1)b+1} (q-1)^{r-1} \frac{\binom{n-tb-b}{r-1}}{\binom{r-(t-1)b}{t}} \qquad (15)\\
&+q^b \sum_{r=1}^{r'} (q-1)^{r-1} \binom{n-tb-b}{r-1}, \qquad (16)
\end{aligned}$$

where $r' \ge (t-1)(b+1)$ is a parameter to be determined later, and the last equality follows from

$$\left|\{\mathbf{y}\in\Sigma_q^{n-tb} : |U_b(\mathbf{y})|=r\}\right| = \binom{n-tb-b}{r-1} q^b (q-1)^{r-1},$$

see Claim 4 in Appendix A of [13] for a detailed proof.

To further estimate (15) and (16), we consider the following binomial random variable $X \sim \text{Binomial}(N,\theta)$ with parameters $N = n-(t+1)b$ and $\theta = \frac{q-1}{q}$. The expectation of X is $\mu \triangleq \mathbb{E}(X) = N\theta$ and the variance is $\text{Var}(X) = N\theta(1-\theta)$. Moreover, by the Chernoff bound, it holds that

$$\Pr(X \ge (1-\epsilon)\mu) \le e^{\left(-\frac{\epsilon^2\mu}{2}\right)}.$$

The term in (16) can be simplified as

$$\begin{aligned}
&q^b \sum_{r=0}^{r'-1} (q-1)^r \binom{N}{r}\\
=&\, q^{N+b} \sum_{r=0}^{r'-1} \binom{N}{r} \left(1-\frac{1}{q}\right)^r \left(\frac{1}{q}\right)^{N-r}\\
=&q^{N+b} \Pr(X < r'). \qquad (17)
\end{aligned}$$

Moreover, since $\binom{r-(t-1)b}{t}$ is monotone increasing in r, thus the term in (15) can be simplified as

$$\begin{aligned}
&q^b \sum_{r=r'+1}^{n-(t+1)b+1} (q-1)^{r-1} \frac{\binom{n-tb-b}{r-1}}{\binom{r-(t-1)b}{t}}\\
\le&\frac{q^b}{\binom{r'+1-(t-1)b}{t}} \sum_{r=r'+1}^{n-(t+1)b+1} (q-1)^{r-1} \binom{n-tb-b}{r-1}\\
=&\frac{q^b}{\binom{r'+1-(t-1)b}{t}} \sum_{r=r'}^{N} (q-1)^r \binom{N}{r}\\
\le&\frac{q^{N+b}}{\binom{r'+1-(t-1)b}{t}}, \qquad (18)
\end{aligned}$$

where the last inequality follows by $\sum_{r=r'}^{N}(q-1)^r\binom{N}{r} \le q^N$.

Setting $r' = \mu - \sqrt{2tN\ln N}$ in (18) and (17), then by the Chernoff bound, the RHS of (17) is at most

$$\begin{aligned}
q^{N+b}\cdot e^{-\frac{tN\ln N}{\mu}} \le& \frac{q^{N+b}}{N^{\frac{tq}{q-1}}}\\
=&o\left(\frac{q^{n-tb}}{(n-(t+1)b)^t}\right),
\end{aligned}$$

as $n\to\infty$. Meanwhile, by

$$\begin{aligned}
&\binom{r'+1-(t-1)b}{t} \ge \frac{(\mu-(t-1)b)^t}{t!}(1-o(1))\\
=&\left(\frac{q-1}{q}\right)^t \left(n-2tb-\frac{(t-1)b}{q}\right)^t \frac{1}{t!}(1-o(1)) \qquad (19)
\end{aligned}$$

as $n\to\infty$, the RHS of (18) is at most

$$\frac{q^{N+b+t}t!}{(q-1)^t\left(n-2tb-\frac{(t-1)b}{q}\right)^t}(1+o(1)).$$

In total, this leads to

$$\begin{aligned}
&\sum_{\mathbf{y}\in\Sigma_q^{n-tb}} |D_t^b(\mathbf{y})|^{-1}\\
\le&\frac{t!q^{n-tb+t}}{(q-1)^t\left(n-2tb-\frac{(t-1)b}{q}\right)^t}(1+o(1))
\end{aligned}$$

and confirms the upper bound in Theorem 1.