Maximal Gain Attack (MGA) on kRR, OUE, and OLH

Idea: For each fake user, choose a reported value y that maximizes

$$\sum_{t \in T} \mathbf{1}_{S(y)}(t),$$

where T is the set of target items and $S(y)$ is the support set of y.

Protocol	MGA mechanism for each fake user
kRR	Domain $D = [d]$, support $S(y) = \{y\}$. Maximize $\sum_{t \in T} \mathbf{1}_{S(y)}(t) \leq 1$, so choose any target: fake user *always reports* a target item $y \in T$.
OUE	Domain $D = \{0,1\}^d$, support $S(y) = \{v : y_v = 1\}$. Maximize $\sum_{t \in T} \mathbf{1}_{S(y)}(t) \leq \lvert T \rvert$ by setting $y_t = 1$ for all $t \in T$. To mimic genuine users, also set $l \approx p + (d-1)q - \lvert T \rvert$ *additional non–target bits* to 1, so the total number of 1s matches the expected number for honest users.
OLH	Domain $D = \{(H, a)\}$, support $S(H, a) = \{v : H(v) = a\}$. Maximize $\sum_{t \in T} \mathbf{1}_{S(H,a)}(t) \leq \lvert T \rvert$ by choosing a hash function H and bucket a such that many targets collide: $H(t) =$