Single-Server Private Information Retrieval With Side Information Under Arbitrary Popularity Profiles

Alejandro Gomez-Leos and Anoosheh Heidarzadeh

Abstract—This paper introduces a generalization of the Private Information Retrieval with Side Information (PIR-SI) problem called Popularity-Aware PIR-SI (PA-PIR-SI). The PA-PIR-SI problem includes one or more remote servers storing copies of a dataset of $K$ messages, and a user who knows $M$ out of $K$ messages—the identities of which are unknown to the server—as a prior side information, and wishes to retrieve one of the remaining $K-M$ messages. The goal of the user is to minimize the amount of information they must download from the server while revealing no information about the identity of the desired message. In contrast to PIR-SI, in PA-PIR-SI, the dataset messages are not assumed to be equally popular. That is, given the $M$ side information messages, each of the remaining $K-M$ messages is not necessarily equally likely to be the message desired by the user. In this work, we focus on the single-server setting of PA-PIR-SI, and establish lower and upper bounds on the capacity of this setting—defined as the maximum possible achievable download rate. Our upper bound holds for any message popularity profile, and is the same as the capacity of single-server PIR-SI. We prove the lower bound by presenting a PA-PIR-SI scheme which takes a novel probabilistic approach—carefully designed based on the popularity profile—to integrate two existing PIR-SI schemes. The rate of our scheme is strictly higher than that of the only existing PIR-SI scheme applicable to the PA-PIR-SI setting.

I. INTRODUCTION

In the Private Information Retrieval (PIR) problem, a user wants to obtain one message belonging to a dataset of $K$ messages with copies stored on a single (or multiple) remote server(s), while revealing no information about the identity of the desired message to the server(s). The goal of the user is to privately retrieve their desired message while downloading the minimum possible amount of information from the server(s). It was shown in [1] that in the single-server setting, the user must download the entire dataset in order to achieve the privacy requirement, whereas in the multi-server setting, the user can achieve a much higher download rate. While the maximum achievable download rate—referred to as capacity—of single-server PIR was characterized very early on, the capacity of multi-server PIR was left open until the seminal work by Sun and Jafar [2].

In recent years, several variations of PIR have been studied by the coding and information theory community. This includes multi-server PIR [3]–[13], single-server PIR with side information [14]–[23], multi-server PIR with side information [15], [24]–[31], multi-message PIR (MPIR) [32], [33], and MPIR with side information [34]–[39].

In this work, we revisit the problem of single-server PIR with side information (PIR-SI) [15]. In PIR-SI, the user knows $M$ out of $K$ dataset messages—the identities of which are unknown to the server—as a prior side information, and wants to retrieve one other message without revealing the identity of the desired message to the server. As was shown in [15], the capacity of single-server PIR-SI is given by $[K/(M+1)]^{-1}$. This result hinges on the assumptions that (i) the $M$ side information messages are chosen uniformly at random, and (ii) given these $M$ messages, each of the remaining $K-M$ messages is equally likely to be the message required by the user. While the assumption (i) can be readily justified from the server's perspective, the assumption (ii) may not always be feasible in practice. This is because in many real-world scenarios, not all dataset messages are equally popular. In particular, recent studies show that the Zipf, Gamma, or Weibull distributions are more appropriate statistical models for online data access patterns as compared to the uniform distribution [40]–[42]. This implies the need for new PIR models which take into account the popularity of the dataset messages.

In [43], the authors characterize the capacity of PIR under any arbitrary popularity profile. To the best of our knowledge, there is, however, no prior result on the capacity of PIR-SI under any non-uniform popularity profile. Motivated by this, in this work, we introduce a generalization of the PIR-SI problem, referred to as Popularity-Aware PIR-SI (PA-PIR-SI), which takes into account the popularity of the messages. In particular, the PA-PIR-SI problem reduces to the PIR-SI problem when all the messages are equally popular.

We focus on the single-server setting of the PA-PIR-SI problem, and for the ease of exposition, we assume that $K$ and $M$ are such that $M+1$ divides $K$. We establish lower and upper bounds on the capacity of PA-PIR-SI in the single-server setting. In particular, we show that the capacity is upper bounded by $(M+1)/K$. Note that this upper bound does not depend on the popularity profile, and is indeed the same as the capacity of PIR-SI under the uniform popularity profile when $M+1$ divides $K$. To prove the upper bound, we rely on a mix of combinatorial and information-theoretic arguments. To derive a lower bound on the capacity, we propose a PA-PIR-SI scheme, referred to as Randomized Code Selection (RCS), which takes into account the message popularity profile. The RCS scheme takes a novel probabilistic approach—carefully designed based on the popularity of the messages—for selecting between two existing PIR-SI schemes which were proposed in [15].
A motivating example—not presented here due to space constraints—can be found in the long version of this work, [44]. This example highlights the limitations of the existing PIR-SI schemes under a non-uniform popularity profile, and demonstrates how the RCS scheme can overcome these limitations. The RCS scheme is applicable for any arbitrary popularity profile, and achieves a rate strictly higher than $1/(K-M)$—which is the rate of the only existing PIR-SI scheme applicable for non-uniform popularity profiles, i.e., the MDS Code scheme of [15]. In addition, our simulations for several commonly-used popularity profiles show that the random variables $X_{i}$ are independent and the PMF of $W$ is given by

$$p_{w,s}(W^{*}|S^{*}) = \begin{cases} \frac{\lambda_{W^{*}}}{\lambda_{S^{*}}} & \forall W^{*} \in \mathcal{K}, \forall S^{*} \in [\mathcal{K}\backslash W^{*}]^{M}, \\ 0 & \text{otherwise}, \end{cases}$$

Note that for fixed $S^{*}$, $W$ can realize any index $W^{*}$ in $\mathcal{K}\backslash S^{*}$, and the greater is the popularity $\lambda_{W^{*}}$, the higher is the probability of $W = W^{*}$.

Given that the joint PMF of $W$ and $S$ is given by

$$p_{w,s}(W^{*}, S^{*}) = \begin{cases} \frac{1}{K} \frac{\lambda_{W^{*}}}{\lambda_{S^{*}}} & \forall W^{*} \in \mathcal{K}, \forall S^{*} \in [\mathcal{K}\backslash W^{*}]^{M}, \\ 0 & \text{otherwise}, \end{cases}$$

and the PMF of $W$ is given by

$$p_{w}(W^{*}) = \frac{1}{K} \sum_{S^{*} \in [\mathcal{K}\backslash W^{*}]^{M}} \frac{\lambda_{W^{*}}}{\lambda_{S^{*}}} \forall W^{*} \in \mathcal{K}. \quad (2)$$

We assume that the joint distribution of $W$ and $S$ is known to both the user and the server, whereas the realizations $W$ and $S$ are known only by the user and not the server.

Given the demand index $W$ and the side information index set $S$, the user sends a query $Q^{W,S}$ which is a (potentially stochastic) function of $W$ and $S$. The server responds with an answer $A^{W,S}$ which is a deterministic function of the user’s query $Q^{W,S}$ and the messages $X_{1}, \ldots, X_{K}$. Thus, $H(A^{W,S}|Q^{W,S}, X_{K}) = 0$. Note that the randomness in $Q^{W,S}$ is due to the randomness in the query construction, and the randomness in $A^{W,S}$ is due to the randomness in $Q^{W,S}$ and $X_{K}$. For the ease of notation, we denote $Q^{W,S}$, $A^{W,S}$, $Q^{W,S}_{T}$, and $A^{W,S}_{T}$ by $Q$, $A$, $Q$, and $A$, respectively.

We require that the query $Q$ and the answer $A$ satisfy the following two conditions:

1) **Decodability:** Given $Q$ and $X_{S}$, the user must be able to decode the demand message $X_{W}$ from $A$, i.e.,

$$H(X_{W}|A, Q, X_{S}) = 0. \quad \text{2) **Privacy:** The server must not gain any information about the demand index $W$ from the query $Q$, i.e.,}$$

$$P(W = W^{*}|Q = Q) = P(W = W^{*}) \quad \forall W^{*} \in \mathcal{K}.$$
III. MAIN RESULTS

In this section, we summarize our main results on the capacity of PA-PIR-SI.

Theorem 1. For PA-PIR-SI with K messages and M side information messages such that \( M + 1 \) is a divisor of \( K \) and strictly less than \( \sqrt{K} \), under any popularity profile \( \Lambda \), the capacity is upper bounded by \( R_{\text{UB}} \) defined as

\[
R_{\text{UB}} = \frac{M + 1}{K},
\]

and is lower bounded by \( R_{\text{LB}} \) defined as

\[
\left( K - M - \left( K - M - \frac{K}{M + 1} \right) \right) \times \Gamma_{[1,2:M+1]} \frac{p_{W,S}(\{1\}, \{2 : M + 1\})}{p_{W}(\{1\})} \left( \frac{K - 1}{M} \right)^{-1},
\]

where \( \Gamma_{[1,2:M+1]} \) is given by

\[
\min_{i \in [K-M]:K} \left\{ 1, \frac{p_{W,S}(\{i\}, [K - M : K] \setminus \{i\})}{p_{W,S}(\{1\}, [2 : M + 1])} \right\}.
\]

Remark 1. Note that the lower bound \( R_{\text{LB}} \)—which is the rate achieved by our scheme—is valid only for \( K \) and \( M \) such that \( (M + 1) / K \) and \( M + 1 < \sqrt{K} \) whereas the upper bound \( R_{\text{UB}} \) holds for all \( K \) and \( M \). While our scheme can be modified so that it is applicable for any \( K \) and \( M \), the modified scheme’s description is lengthy and notation-heavy, and its analysis is tedious and involved. To avoid confusing the reader with technical details, in this work we present the simplest form of our scheme (i.e., for \( K \) and \( M \) satisfying the above conditions), and demonstrate its superiority over the MDS Code scheme of [15]—which is the only existing PIR-SI scheme applicable for arbitrary popularity profiles.

Remark 2. By the result of [43, Theorem 1] on the capacity of semantic PIR, the capacity of single-server PIR (without side information) under any arbitrary (uniform or non-uniform) popularity profile is \( 1/K \). That is, the privacy can be achieved only by downloading the entire dataset. While the capacity of single-server PA-PIR-SI remains open in general, the result of Theorem 1 shows that for any popularity profile, the capacity lies between \( 1/(K - M) \) and \( (M + 1)/K \), and hence, greater than \( 1/K \). This result extends our prior understanding of the role of side information in single-server PIR-SI under the uniform popularity profile, to arbitrary popularity profiles.

IV. ACHIEVABILITY SCHEME

In this section, we propose a PA-PIR-SI scheme for arbitrary popularity profiles. The proposed scheme, which we refer to as the Randomized Code Selection (RCS) scheme, is applicable for any parameters \( K \) and \( M \) such that \( M + 1 \) is a divisor of \( K \) and strictly less than \( \sqrt{K} \) and any field size \( q \geq K \). An illustrative example of the RCS scheme can be found in the long version of this work, [44].

Randomized Code Selection (RCS) Scheme: For any \( W^* \in K \) and \( S^* \in [K \setminus W]^M \), we define

\[
\Gamma_{W,S^*} = \Gamma_{[1,2:M+1]} \frac{p_{W,S}(\{1\}, [2 : M + 1]) p_{W}(W^*)}{p_{W,S}(W^*, S^*) p_{W}(\{1\})},
\]

where \( \Gamma_{[1,2:M+1]} \) is given by (5). Given the demand index \( W \) and the side information index set \( S \), the user randomly selects the Partition-and-Code scheme of [15] with probability \( \Gamma_{W,S} \), or the MDS Code scheme of [15] with probability \( 1 - \Gamma_{W,S} \), and follows the selected scheme as described below. In the following, we refer to the Partition-and-Code scheme and the MDS Code scheme as Scheme I and Scheme II, respectively.

Scheme I: The user partitions the message indices \( 1,...,K \) into \( N \triangleq K/(M + 1) \) parts \( Q_1,\ldots,Q_N \), each of size \( M + 1 \), as outlined below. First, the user chooses an index \( j^* \in [N] \) uniformly at random, and assigns the indices in \( W \cup S \) to the part \( Q_{j^*} \). The user then takes the remaining \( K - (M + 1) \) message indices \( K \setminus (W \cup S) \), and randomly partitions them into the remaining \( N - 1 \) parts \( Q_j \)’s for \( j \in [N] \setminus \{j^*\} \). Then, the user constructs the query \( Q_{W,S} = \{Q_1,\ldots,Q_N\} \), and sends it to the server.

Given \( Q_{W,S} \), the server computes \( A_j = \sum_{i \in Q_j} X_i \) for each \( j \in [N] \). Then, the server constructs the answer \( A_{W,S} = \{A_1,\ldots,A_N\} \), and sends it back to the user.

Given \( A_{W,S} \), the user recovers their demand message \( X_W \) by subtracting off the contribution of the side information messages \( X_S \) from \( A_j \), i.e., \( X_W = A_j - \sum_{i \in S} X_i \).

Scheme II: First, the user chooses \( K \) arbitrary (but distinct) elements \( \omega_1,\ldots,\omega_K \) from \( \mathbb{F}_q^* \), and constructs \( K - M \) vectors \( Q_1,\ldots,Q_{K-M} \), where \( Q_j = [\omega_1^{-1},\ldots,\omega_K^{-1}] \) for each \( j \in [K - M] \). Then, the user constructs the query \( Q_{W,S} = \{Q_1,\ldots,Q_{K-M}\} \), and sends it to the server.

Given \( Q_{W,S} \), the server computes \( A_j = \sum_{i=1}^{K} \omega_i^{-j-1} X_i \) for each \( j \in [K - M] \). The server then constructs the answer \( A_{W,S} = \{A_1,\ldots,A_{K-M}\} \), and sends it back to the user.

Given \( A_{W,S} \), the user recovers their demand message \( X_W \) along with all \( K - (M + 1) \) messages \( X_{K\setminus(W\cup S)} \) by subtracting off the contribution of the side information messages \( X_S \) from \( A_1,\ldots,A_{K-M} \), and solving the resulting system of \( K - M \) equations with \( K - M \) unknowns \( X_{K\setminus S} \).
A. Proof of Decodability and Privacy

Since both Schemes I and II satisfy the decodability condition, it should be obvious that the RCS scheme also satisfies this requirement. It thus remains to show that the RCS scheme also satisfies the privacy condition.

Consider a query constructed by the RCS scheme. When the query is formed by Scheme II, it should be obvious that the privacy condition is satisfied because Scheme II constructs the query independently of the realization \((W, S)\). In the following, we show that the privacy condition is also satisfied when the query is formed by Scheme I.

Recall that any query formed by Scheme I is a partition of \(K\) with \(N = K/(M + 1)\) parts, each of size \(M + 1\). We denote by \(Q\) the set of all such partitions. For each \(Q \in Q\), let \(Q_1, \ldots, Q_N\) denote the \(N\) parts forming the partition \(Q\).

**Lemma 1.** For any query (partition) \(Q \in Q\), the privacy condition is satisfied if for any \(i, j \in [N]\) and for any \(W_i \in Q_i, W_j \in Q_j\), it holds that

\[
\Gamma_{W_i S_i} = \Gamma_{W_j S_j} \frac{p_{W,S}(W_i, S_i)p_{W}(W_j)}{p_{W,S}(W_j, S_j)p_{W}(W_i)},
\]

where \(S_i = Q_i \setminus W_i\) and \(S_j = Q_j \setminus W_j\).

**Proof.** The proof can be found in [44].

By Lemma 1, the privacy requirement entails that the condition in (7) must hold for any two parts \(Q_i\) and \(Q_j\) in any partition \(Q\). For the proof of privacy, it thus suffices to show that our choice of \(\Gamma_{W^*, S^*}\) in (6) satisfies (7).

Fix arbitrary \(W^* \in K\) and \(S^* \in [K \setminus W^*]^M\) such that \(W^* \cup S^*\) is one of the parts in the partition \(Q\). We consider the following cases separately: (i) \(Q_i = [M + 1]\) for some \(i \in [N]\), and (ii) \(Q_i \neq [M + 1]\) for any \(i \in [N]\).

First, consider the case (i). Taking \(W_i = \{1\}\) and \(S_i = [2 : M + 1]\), the condition in (7) reduces to

\[
\Gamma_{W^*, S^*} = \Gamma_{W^*, S^*} \frac{p_{W,S}(\{1\}, [2 : M + 1])p_{W}(W^*)}{p_{W,S}(W^*, S^*)p_{W}(\{1\})},
\]

which is consistent with our choice of \(\Gamma_{W^*, S^*}\) (cf. (6)).

Next, consider the case (ii). Recall that by assumption, \(M + 1 < \sqrt{K}\), i.e., \(N = K/(M + 1) > (M + 1)^2\), or equivalently, \(N > M + 1\). Since the partition \(Q\) consists of \(N > M + 1\) parts, by the pigeonhole principle, there exists some \(k \in [N]\) such that \(Q_k\) and \([M + 1]\) are disjoint. Let \(Q^* \in Q\) be an arbitrary partition such that both parts \(Q_k\) and \([M + 1]\) belong to the partition \(Q^*\). Recall that the privacy condition requires that for any given partition, the condition in (7) must hold for any two parts of that partition. Note also that \(Q_k\) and \([M + 1]\) are two parts of the same partition \(Q^*\). Let \(W_k\) be an arbitrary index in the part \(Q_k\), and let \(S_k = Q_k \setminus W_k\). Then, by (7), it is required that

\[
\Gamma_{W_k S_k} = \Gamma_{W_k S_k} \frac{p_{W,S}(\{1\}, [2 : M + 1])p_{W}(W_k)}{p_{W,S}(W_k, S_k)p_{W}(\{1\})},
\]

Note also that \(W^* \cup S^*\) and \(W_k \cup S_k\) are two parts of the partition \(Q\). Thus, by (7), we require that

\[
\Gamma_{W^*, S^*} = \Gamma_{W_k S_k} \frac{p_{W,S}(W_k, S_k)p_{W}(W^*)}{p_{W,S}(W^*, S^*)p_{W}(W_k)}.\]

Combining (8) and (9), it follows that we must have

\[
\Gamma_{W^*, S^*} = \Gamma_{1\{1\}, [2 : M + 1]} \frac{p_{W,S}(\{1\}, [2 : M + 1])p_{W}(W^*)}{p_{W,S}(W^*, S^*)p_{W}(\{1\})},
\]

which coincides with our choice of \(\Gamma_{W^*, S^*}\) (cf. (6)). This completes the proof of privacy.

B. Proof of Achievable Rate

By construction, the server’s answer to the user’s query consists of \(K/(M + 1)\) (or \(K - M\)) linearly independent combinations of the messages \(X_1, \ldots, X_K\) for Scheme I (or Scheme II). Since \(X_1, \ldots, X_K\) are independent and uniformly distributed over \(\mathbb{F}_q^M\), then \(A_1, \ldots, A_K/(M + 1)\) (or \(A_1, \ldots, A_{K-M}\)) are independent and uniformly distributed over \(\mathbb{F}_q^M\). Thus, \(H(A^{[W^*]}_i)\) is equal to \(H(A_1, \ldots, A_K/(M + 1)B\) or \(H(A_1, \ldots, A_{K-M})\) for Scheme I or Scheme II, respectively. Using the joint PMF of \(W\) and \(S\), the rate of the RCS scheme is given by

\[
\left(\sum_{W^* \in K, S^* \in [K \setminus W^*]^M} \frac{p_{W,S}(W^*, S^*)}{\Gamma_{W^*, S^*} \left(\frac{K}{M + 1} + (1 - \Gamma_{W^*, S^*})(K - M)\right)}\right)^{-1}.
\]

Substituting for \(\Gamma_{W^*, S^*}\) using (6), we can rewrite (10) as

\[
\left(\frac{K}{M - \frac{K}{M + 1}}\right) \times \frac{\Gamma_{W^*, S^*} \left(\frac{K}{M + 1} + (1 - \Gamma_{W^*, S^*})(K - M)\right)}{\Gamma_{1\{1\}, [2 : M + 1]} \Gamma_{W^*, S^*} \left(\frac{K}{M + 1} + (1 - \Gamma_{W^*, S^*})(K - M)\right)}^{-1},
\]

which is the expression for \(R_{LB}\) in Theorem 1 (cf. (4)).

Since the probability \(\Gamma_{W^*, S^*}\) takes a value in the interval \([0, 1]\), it readily follows that \(\Gamma_{1\{1\}, [2 : M + 1]}\) is lower bounded by 0, and upper bounded by

\[
\min_{W^*, S^*} \left\{p_{W,S}(W^*, S^*)p_{W}(\{1\}) / p_{W,S}(\{1\}, [2 : M + 1])p_{W}(W^*)\right\},
\]

where the minimization is over all \(W^* \in K\) and all \(S^* \in [K \setminus W^*]^M\). According to (11), for fixed \(K\) and \(M\), the rate of the RCS scheme is an increasing function of \(\Gamma_{1\{1\}, [2 : M + 1]}\), and hence, the rate is maximized when \(\Gamma_{1\{1\}, [2 : M + 1]}\) is equal to (12). It remains to show that (12) and our choice of \(\Gamma_{1\{1\}, [2 : M + 1]}\) in (5) are equal.

Instead of working directly with (12), it is more convenient to analyze the following minimization problem:

\[
\min_{W^*, S^*} \left\{p_{W,S}(\{1\}, [2 : M + 1]) / p_{W,S}(W^*, S^*) / p_{W}(W^*)\right\}.
\]
where the minimization is over all \( W^* \in \mathcal{K} \) and all \( S^* \in [\mathcal{K} \setminus W^*]^M \). Note that (12) is equal to (13) times the constant term \( p_{W}(\{1\})/p_{W,S}(\{1\}, [2 : M + 1]) \). By (1) and (2), we have

\[
p_{W,S}(W^*, S^*) = \frac{1}{\lambda_{S^*}} \left( \sum_{T \in [\mathcal{K} \setminus W^*]^M} \frac{1}{\lambda_T} \right)^{-1}.
\]

For any given \( W^* \in \mathcal{K} \), it is easy to see that (14) is minimized for \( S^* \in [\mathcal{K} \setminus W^*]^M \) such that \( \lambda_{S^*} \) is maximum, or equivalently, \( \lambda_{S^*} = \sum_{i \in S^*} \lambda_i \) is minimum. For any given \( W^* \), we can determine \( S^* \) that minimizes \( \lambda_{S^*} \), as follows. Recall that \( \lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_K \) by assumption. We consider the following two cases separately: (i) \( W^* \in [1 : K - M] \), and (ii) \( W^* \in [K - M + 1 : K] \). In the case (i), \( \lambda_{S^*} \) is minimized for \( S^* = [K - M + 1 : K] \). This is because the sum of the last \( M \) \( \lambda_i \)'s yields the minimum sum over all \( M \)-subsets of \( \{\lambda_i : i \in \mathcal{K}\} \). In the case (ii), \( \lambda_{S^*} \) is minimized for \( S^* = [K - M : K] \setminus W^* \). This is because \( W^* \) is one of the last \( M + 1 \) indices in \( \mathcal{K} \), and the \( M \)-subset \( S^* \) cannot contain \( W^* \). Hence, we can rewrite (13) as

\[
\min_{i \in [1 : K - M]} \frac{p_{W,S}(\{1\}, [2 : M + 1])}{p_{W}(\{1\})},
\]

\[
\min_{i \in [K - M + 1 : K]} \frac{p_{W,S}(\{1\}, [K - M + 1 : K])}{p_{W}(\{1\})},
\]

\[
\min_{i \in [K - M : K]} \frac{p_{W,S}(\{1\}, [K - M : K] \setminus \{i\})}{p_{W}(\{i\})}.
\]

Lemma 2. For any popularity profile \((\lambda_1, \ldots, \lambda_K)\) such that \( \lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_K > 0 \), it holds that

\[
\min_{i \in [1 : K - M]} \frac{p_{W,S}(\{i\}, [K - M + 1 : K])}{p_{W}(\{i\})} = \frac{p_{W,S}(\{K - M + 1 : K\})}{p_{W}(\{K - M + 1 : K\})},
\]

Proof. The proof can be found in [44].

By the result of Lemma 2, the minimization problem in (15) can be simplified further as

\[
\min_{i \in [K - M : K]} \left\{ \frac{p_{W,S}(\{1\}, [2 : M + 1])}{p_{W}(\{1\})}, \frac{p_{W,S}(\{1\}, [K - M + 1 : K])}{p_{W}(\{1\})}, \frac{p_{W,S}(\{K - M + 1 : K\})}{p_{W}(\{K - M + 1 : K\})} \right\},
\]

or equivalently,

\[
\min_{i \in [K - M : K]} \left\{ \frac{p_{W,S}(\{1\}, [2 : M + 1])}{p_{W}(\{1\})}, \frac{p_{W,S}(\{1\}, [K - M + 1 : K] \setminus \{i\})}{p_{W}(\{i\})} \right\}.
\]

Since (13), (15), and (16) are equal, and (12) is equal to (13) times \( p_{W}(\{1\})/p_{W,S}(\{1\}, [2 : M + 1]) \), it then follows that (12) and (5) are equal, as was to be shown.

\[
\min_{i \in [K - M : K]} \left\{ \frac{p_{W,S}(\{1\}, [2 : M + 1])}{p_{W}(\{1\})}, \frac{p_{W,S}(\{1\}, [K - M + 1 : K] \setminus \{i\})}{p_{W}(\{i\})} \right\}.
\]

Fig. 1. The ratios \( R_{RCS}/R_{UB} \) and \( R_{MDS}/R_{UB} \) versus \( K \), for \( M = 1 \) and different models for the popularity profile.

Fig. 2. The ratios \( R_{RCS}/R_{UB} \) and \( R_{MDS}/R_{UB} \) versus \( K \), for different \( M \) and the Zipf model for the popularity profile.

V. SIMULATIONS

In this section, we compare the rate of the RCS scheme and that of the MDS Code scheme of [15], with respect to the capacity upper bound \( R_{UB} \) (see (3)). In the following, we denote the rates of the RCS scheme and the MDS Code scheme by \( R_{RCS} \) and \( R_{MDS} \), respectively. Note that \( R_{RCS} = R_{LB} \) (see (4)), and \( R_{MDS} = 1/(K - M) \) (from [15]).

It is generally agreed that the Zipf, Gamma, and Weibull distributions are appropriate models for the popularity profile [40]–[42]. Motivated by this, in our simulations we consider popularity profiles generated according to each of these distributions. In addition, we consider very small values of \( M \) which are of significant practical importance.

Fig. 1 depicts \( R_{RCS}/R_{UB} \) and \( R_{MDS}/R_{UB} \), for \( M = 1 \) and different \( K \), where \( \lambda_1, \ldots, \lambda_K \) are sampled from each of the following distributions: (i) Zipf with parameters \( N = 100 \) and \( s = 1 \), (ii) Gamma with shape and scale parameters 0.62 and 31.22, respectively, and (iii) Weibull with shape and scale parameters 0.79 and 16.80, respectively. (The above parameters were chosen such that all three distributions have the same mean and the same variance.) As can be seen in Fig. 1, for a fixed distribution, as \( K \) increases, \( R_{RCS}/R_{UB} \) approaches 1, whereas \( R_{MDS}/R_{UB} \) approaches 1/2.

Fig. 2 depicts \( R_{RCS}/R_{UB} \) and \( R_{MDS}/R_{UB} \) for \( M \in \{1, 2, 3\} \) and different \( K \), where \( \lambda_1, \ldots, \lambda_K \) are sampled from the Zipf distribution with parameters \( N = 100 \) and \( s = 1 \). In Fig. 2, one can observe that for each \( M \), as \( K \) increases, \( R_{RCS}/R_{UB} \) approaches 1, while \( R_{MDS}/R_{UB} \) approaches 1/(\( M + 1 \)). It can also be seen that for fixed \( K \) (or \( M \)), the advantage of the RCS scheme over the MDS Code scheme is more pronounced as \( M \) (or \( K \)) increases.
