Private Information Retrieval from Heterogeneous Uncoded Caching Databases

Karim Banawan Batuhan Arasli Yi-Peng Wei Sennur Ulukus
Department of Electrical and Computer Engineering
University of Maryland, College Park, MD 20742
kbanawan@umd.edu barasli@umd.edu ypwei@umd.edu ulukus@umd.edu

***Abstract*—We consider private information retrieval (PIR) of a single file out of K files from N non-colluding databases with *heterogeneous storage constraints* $\boldsymbol{m} = (m_1, \cdots, m_N)$. The aim of this work is to jointly design the content placement phase and the retrieval phase in order to minimize the download cost in the PIR phase. We characterize the optimal PIR download cost as a linear program. By analyzing the structure of the optimal solution of this linear program, we show that, surprisingly, the optimal download cost in our heterogeneous case matches its homogeneous counterpart where all databases have the same average storage constraint $\mu = \frac{1}{N}\sum_{n=1}^{N} m_n$. We show the optimum content placement explicitly for $N = 3$.**

I. Introduction

The problem of private information retrieval (PIR), introduced in [1], has attracted much interest in the information theory community with leading efforts [2]–[6]. In the classical setting of PIR, a user wants to retrieve a file out of K files from N databases, each storing the same content of entire K files, such that no individual database can identify the identity of the desired file. Sun and Jafar [7] characterized the optimal normalized download cost of the classical setting to be $D^* = 1 + \frac{1}{N} + \cdots + \frac{1}{N^{K-1}}$. Fundamental limits of many variants of the problem have been investigated in [8]–[35].

A common assumption in most of these works is that the databases have sufficiently large storage space that can accommodate all K files in a replicated manner. This may not be the case for peer-to-peer (P2P) and device-to-device (D2D) networks, where information retrieval takes place directly between the users. Here, user devices (databases) will have *limited* and *heterogeneous* sizes. This motivates the investigation of PIR from databases with *heterogeneous storage constraints*. We aim to jointly design the storage mechanism (content assignment) and the retrieval scheme such that the normalized PIR download cost is minimized.

Reference [24] studies PIR from *homogeneous storage-limited* databases. In [24], each database has the *same* limited storage space of μKL bits, where $0 \leq \mu \leq 1$. The goal is to find the optimal centralized uncoded caching scheme (content assignment) that minimizes the PIR download cost. [24] shows that symmetric batch caching scheme in [36] for placement along with Sun-Jafar scheme in [7] for retrieval result in the lowest normalized download cost. The optimal storage-download cost tradeoff is characterized by the lower convex hull of the N pairs $(\frac{t}{N}, 1 + \frac{1}{t} + \cdots + \frac{1}{t^{K-1}})$, $t = 1, 2, \cdots, N$.

This work was supported by NSF Grants CNS 15-26608, CCF 17-13977 and ECCS 18-07348.

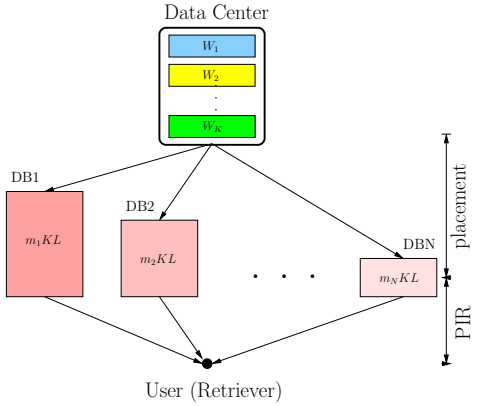

Fig. 1. PIR from databases with heterogeneous storage sizes.

Meanwhile, the content assignment problem for *heterogeneous* databases (caches) is investigated in the context of coded caching in [37]. In the coded caching problem [36], the aim is to jointly design the placement and delivery phases in order to minimize the traffic load during peak hours. Reference [37] proposes an optimization framework where placement and delivery schemes are optimized by solving a linear program. Using this optimization framework, [37] investigates the effects of heterogeneity in cache sizes on the delivery load memory tradeoff with uncoded placement.

In this paper, we investigate PIR from databases with heterogeneous storage sizes (see Fig. 1). The nth database can accommodate $m_n KL$ bits, where L is the file size, i.e., the storage system is constrained by the storage size vector $\boldsymbol{m} = (m_1, \cdots, m_N)$. We aim to characterize the optimal normalized PIR download cost of this problem, and the corresponding optimal placement and optimal retrieval schemes. We focus on uncoded placement as in [24] and [37].

Motivated by [37], we first show that the optimal normalized download cost is characterized by a linear program. For the achievability, each message is partitioned into $2^N - 1$ partitions (the size of the power set). For every partition, we apply the Sun-Jafar scheme [7]. The linear program is a consequence of optimizing the achievable download cost with respect to the partition sizes subject to the storage constraints. For the converse, we slightly modify the converse in [24] to be valid

for the heterogeneous case. These achievability and converse proofs result in exactly the same linear program, yielding the exact capacity for this PIR problem for all K, N, $\boldsymbol{m}$. This is unlike the caching problem in [37], where the linear program is only an achievability, and is the exact capacity only in special cases. By studying the properties of the solution of the linear program, we show that, surprisingly, the optimal normalized download cost for the heterogeneous case is identical to its homogeneous counterpart where the homogeneous storage constraint is $\mu = \frac{1}{N}\sum_{n=1}^{N} m_n$. For $N = 3$, we give the explicit (parametric in $\boldsymbol{m}$) optimal content assignment.

II. System Model

We consider a system with K i.i.d. L-length messages,

$$H(W_1, \cdots, W_K) = KL, \quad H(W_k) = L,\ k \in [K] \tag{1}$$

The system consists of N databases. The storage size of the nth database is $m_n KL$ bits for some $0 \le m_n \le 1$. We denote the contents of the nth database by Z_n, such that,

$$H(Z_n) \le m_n KL, \quad n \in [N] \tag{2}$$

The system operates in two phases: In the placement phase, the data center stores the message set in the N databases. The placement is done in a *centralized* fashion [36]. We focus on uncoded placement as in [24], i.e., file W_k is partitioned as,

$$W_k = \bigcup_{\mathcal{S}\subseteq[N]} W_{k,\mathcal{S}} \tag{3}$$

where $W_{k,\mathcal{S}}$ is the set of W_k bits that appear in the database set $\mathcal{S} \subseteq \mathcal{P}([N])$, where $\mathcal{P}(\cdot)$ is the power set. $H(W_{k,\mathcal{S}}) = |W_{k,\mathcal{S}}|L$, where $0 \le |W_{k,\mathcal{S}}| \le 1$. Under an uncoded placement, we have the following message size constraint,

$$1 = \frac{1}{KL}\sum_{k=1}^{K} H(W_k) = \frac{1}{KL}\sum_{k=1}^{K}\sum_{\mathcal{S}\subseteq[N]} H(W_{k,\mathcal{S}}) = \sum_{\mathcal{S}\subseteq[N]} \alpha_{\mathcal{S}} \tag{4}$$

where $\alpha_{\mathcal{S}} = \frac{1}{K}\sum_{k=1}^{K} |W_{k,\mathcal{S}}|$. In addition, we have the individual database storage constraints,

$$m_n \ge \frac{1}{KL} H(Z_n) = \sum_{\mathcal{S}\subseteq[N], n\in\mathcal{S}} \alpha_{\mathcal{S}}, \quad n \in [N] \tag{5}$$

In the retrieval phase, the user is interested in retrieving W_θ, $\theta \in [K]$ privately. The user submits a query $Q_n^{[\theta]}$ to the nth database. Since the user has no information about the files, the messages and queries are statistically independent, i.e.,

$$I(W_{1:K}; Q_{1:N}^{[\theta]}) = 0 \tag{6}$$

The nth database responds with an answer string, which is a function of the received query and the stored content, i.e.,

$$H(A_n^{[\theta]} | Q_n^{[\theta]}, Z_n) = 0, \quad n \in [N] \tag{7}$$

To ensure privacy, the query submitted to the nth database when intended to retrieve W_θ should be statistically indistinguishable from the one when intended to retrieve $W_{\theta'}$, i.e.,

$$(Q_n^{[\theta]}, A_n^{[\theta]}, W_{1:K}) \sim (Q_n^{[\theta']}, A_n^{[\theta']}, W_{1:K}),\ \theta, \theta' \in [K] \tag{8}$$

The user needs to decode the desired message W_θ reliably from the received answer strings, consequently,

$$H(W_\theta | Q_{1:N}^{[\theta]}, A_{1:N}^{[\theta]}) = o(L) \tag{9}$$

where $\frac{o(L)}{L} \to 0$ as $L \to \infty$.

An achievable PIR scheme satisfies constraints (8) and (9) for some file size L. The download cost D is the size of the total downloaded bits from all databases,

$$D = \sum_{n=1}^{N} H(A_n^{[\theta]}) \tag{10}$$

For a given storage constraint vector $\boldsymbol{m}$, we aim to jointly design the placement phase (i.e., Z_n, $n \in [N]$) and the retrieval scheme to minimize the normalized download cost $D^* = \frac{D}{L}$.

III. Main Results

Theorem 1 characterizes the optimal download cost under heterogeneous storage constraints in terms of a linear program. A sketch of the proof of Theorem 1 is given in Section IV.

Theorem 1 *For PIR from databases with heterogeneous storage constraints $\boldsymbol{m} = (m_1, \cdots, m_N)$, the optimal normalized download cost is the solution of the following linear program,*

$$\begin{aligned} \min_{\alpha_{\mathcal{S}} \ge 0} \quad & \sum_{\ell=1}^{N} \sum_{\mathcal{S}:|\mathcal{S}|=\ell} \alpha_{\mathcal{S}} \left(1 + \frac{1}{\ell} + \cdots + \frac{1}{\ell^{K-1}}\right) \\ \text{s.t.} \quad & \sum_{\mathcal{S}:|\mathcal{S}|\ge 1} \alpha_{\mathcal{S}} = 1, \quad \sum_{\mathcal{S}:n\in\mathcal{S}} \alpha_{\mathcal{S}} \le m_n, \quad n \in [N] \end{aligned} \tag{11}$$

where $\mathcal{S} \in \mathcal{P}([N])$.

Theorem 2 shows the equivalence between the download cost of the heterogeneous and homogeneous cases.

Theorem 2 *The normalized download cost of the PIR problem with heterogeneous storage constraints $\boldsymbol{m} = (m_1, \cdots, m_N)$ is equal to the normalized download cost of the PIR problem with homogeneous storage constraints $\mu = \frac{1}{N}\sum_{n=1}^{N} m_n$ for all databases, i.e., $D^*(\boldsymbol{m})$ is given by the lower convex hull of the following pairs for $t = 1, \cdots, N$,*

$$\left(t = \sum_{n=1}^{N} m_n, \tilde{D}_t = 1 + \frac{1}{t} + \cdots + \frac{1}{t^{K-1}}\right) \tag{12}$$

This implies that the storage asymmetry does not hurt the PIR capacity. The proof of Theorem 2 is given in Section V.

IV. Representative Example: $K = 3$ and $N = 3$

We introduce the main ingredients of the achievability and converse proofs using the example of $K = 3$ and $N = 3$.

A. Converse Proof

We note that [24, Theorem 1] can be applied to any storage constrained PIR problem with arbitrary storage $Z_{1:N}$.

Hence, specializing to the case of $K = 3$ and $N = 3$ with i.i.d. messages and uncoded content leads to [24, eqn. (39)],

$$D \geq L + \frac{4}{27}\sum_{k=1}^{3} H(W_k) + \frac{11}{108}\sum_{i=1}^{3}\sum_{k=1}^{3} H(W_k|Z_i) + \frac{17}{54}\sum_{i=1}^{3}\sum_{k=1}^{3} H(W_k|\mathbf{Z}_{[3]\setminus i}) + o(L) \quad (13)$$

Using the uncoded storage assumption in (3), we can further write the lower bound in (13) as,

$$D \geq L + \frac{2}{3}\sum_{\substack{\mathcal{S}\subseteq[3]\\|\mathcal{S}|=1}}\sum_{k=1}^{3} |W_{k,\mathcal{S}}|L + \frac{1}{4}\sum_{\substack{\mathcal{S}\subseteq[3]\\|\mathcal{S}|=2}}\sum_{k=1}^{3} |W_{k,\mathcal{S}}|L + \frac{4}{27}\sum_{\substack{\mathcal{S}\subseteq[3]\\|\mathcal{S}|=3}}\sum_{k=1}^{3} |W_{k,\mathcal{S}}|L + o(L) \quad (14)$$

Normalizing with L, taking the limit $L \to \infty$, and using the definition $\alpha_{\mathcal{S}} = \frac{1}{K}\sum_{k=1}^{K} |W_{k,\mathcal{S}}|$ leads to the following lower bound on the normalized download cost D^*,

$$D^* \geq 1 + 2\sum_{\substack{\mathcal{S}\subseteq[3]\\|\mathcal{S}|=1}} \alpha_{\mathcal{S}} + \frac{3}{4}\sum_{\substack{\mathcal{S}\subseteq[3]\\|\mathcal{S}|=2}} \alpha_{\mathcal{S}} + \frac{4}{9}\sum_{\substack{\mathcal{S}\subseteq[3]\\|\mathcal{S}|=3}} \alpha_{\mathcal{S}} \quad (15)$$

$$= 3\sum_{\substack{\mathcal{S}\subseteq[3]\\|\mathcal{S}|=1}} \alpha_{\mathcal{S}} + \frac{7}{4}\sum_{\substack{\mathcal{S}\subseteq[3]\\|\mathcal{S}|=2}} \alpha_{\mathcal{S}} + \frac{13}{9}\sum_{\substack{\mathcal{S}\subseteq[3]\\|\mathcal{S}|=3}} \alpha_{\mathcal{S}} \quad (16)$$

where (16) follows from the message size constraint (4).

We further lower bound (16) by minimizing the right hand side with respect to $\{\alpha_{\mathcal{S}}\}_{\mathcal{S}\subseteq[3]}$ under storage constraints. Thus, the solution of the following linear program serves as a lower bound (converse) for the normalized download cost,

$$\begin{aligned} \min_{\alpha_{\mathcal{S}}\geq 0} \quad & 3(\alpha_1+\alpha_2+\alpha_3)+\frac{7}{4}(\alpha_{12}+\alpha_{13}+\alpha_{23})+\frac{13}{9}\alpha_{123} \\ \text{s.t.} \quad & \alpha_1+\alpha_2+\alpha_3+\alpha_{12}+\alpha_{13}+\alpha_{23}+\alpha_{123} = 1 \\ & \alpha_1+\alpha_{12}+\alpha_{13}+\alpha_{123} \leq m_1 \\ & \alpha_2+\alpha_{12}+\alpha_{23}+\alpha_{123} \leq m_2 \\ & \alpha_3+\alpha_{13}+\alpha_{23}+\alpha_{123} \leq m_3 \end{aligned} \quad (17)$$

B. Achievability Proof

In the placement phase, let $|W_{k,\mathcal{S}}| = \alpha_{\mathcal{S}}$ for all $k \in [K]$. Assign the partition $W_{k,\mathcal{S}}$ to the set $\mathcal{S}$ of the databases for all $k \in [K]$. To retrieve W_θ privately, $\theta \in [K]$, the user applies the Sun-Jafar scheme [7] over the partitions of the files.

The partitions $W_{k,1}$, $W_{k,2}$, $W_{k,3}$ are placed in a single database. Thus, we apply [7] with $N = 1$, and download

$$K(|W_{k,1}| + |W_{k,2}| + |W_{k,3}|)L = 3(\alpha_1 + \alpha_2 + \alpha_3)L \quad (18)$$

The partitions $W_{k,12}$, $W_{k,13}$, $W_{k,23}$ are placed in two databases. Thus, we apply [7] with $N = 2$, and download

$$\left(1 + \frac{1}{2} + \frac{1}{2^2}\right)(\alpha_{12} + \alpha_{13} + \alpha_{23})L \quad (19)$$

Finally, the partition $W_{k,123}$ is placed in all three databases. Thus, we apply [7] with $N = 3$, and download

$$\left(1 + \frac{1}{3} + \frac{1}{3^2}\right)|W_{k,123}|L = \frac{13}{9}\alpha_{123}L \quad (20)$$

Concatenating the downloads, the file W_θ is reliably decodable. Hence, we have the following download cost,

$$\bar{D} = 3(\alpha_1+\alpha_2+\alpha_3)+\frac{7}{4}(\alpha_{12}+\alpha_{13}+\alpha_{23})+\frac{13}{9}\alpha_{123} \quad (21)$$

which matches the lower bound in (17) and is subject to the same constraints. Hence, the solution to the linear program in (17) gives the *exact PIR capacity* of our problem.

V. Equivalence to the Homogeneous Problem

We prove Theorem 2, which implies an equivalence between the solution of (11) with heterogeneous storage constraints $\boldsymbol{m}$ and the solution of (11) with homogeneous storage constraint $\mu = \frac{1}{N}\sum_{n=1}^{N} m_n$. To that end, let $\beta_n = \sum_{\mathcal{S}:|\mathcal{S}|=n} \alpha_{\mathcal{S}}$. By adding the individual storage size constraints in (11), we write the following relaxed problem,

$$\begin{aligned} \min_{\beta_n\geq 0} \quad & \sum_{n=1}^{N} \beta_n \tilde{D}_n \\ \text{s.t.} \quad & \sum_{n=1}^{N} \beta_n = 1, \quad \sum_{n=1}^{N} n\beta_n \leq m_s \end{aligned} \quad (22)$$

where $m_s = \sum_{n=1}^{N} m_n$ and $\tilde{D}_n$ is defined in (12). The solution of the relaxed problem is potentially lower than (11), since the optimal solution of (11) is feasible in (22). Note that the relaxed problem (22) is exactly the linear program constructed for the homogeneous problem with storage constraint of $\mu = \frac{1}{N}\sum_{n=1}^{N} m_n$. Thus, it suffices to prove that the optimal solution of (22) can be mapped back to a feasible solution of (11) to settle the equivalence between the two solutions.

We write the Lagrangian function corresponding to (22) as,

$$\mathcal{L} = \sum_{n=1}^{N} \beta_n \tilde{D}_n - \gamma\sum_{n=1}^{N} \beta_n + \lambda\sum_{n=1}^{N} n\beta_n - \sum_{n=1}^{N} \mu_n\beta_n \quad (23)$$

The optimality conditions are given by,

$$\tilde{D}_n - \gamma + n\lambda - \mu_n = 0, \quad n \in [N] \quad (24)$$

We have the following structural insights about the relaxed problem. The first insight is that at most two non-zero βs exist.

Lemma 1 *There does not exist a subset $\mathcal{N}$, such that $|\mathcal{N}| \geq 3$ and $\beta_n > 0$ for all $n \in \mathcal{N}$.*

Proof: Assume for sake of contradiction that there exists $\mathcal{N}$ such that $|\mathcal{N}| \geq 3$. Hence, $\mu_n = 0$ for all $n \in \mathcal{N}$. From the optimality conditions in (24), we have,

$$\gamma = \tilde{D}_n + n\lambda, \quad n \in \mathcal{N} \quad (25)$$

This results in $|\mathcal{N}|$ independent equations in 2 unknowns, which is an inconsistent linear system if $|\mathcal{N}| \geq 3$, Therefore, we have a contradiction. ■

The second lemma states that if two βs are positive, then they must be consecutive.

Lemma 2 *If $\beta_{n_1} > 0$, and $\beta_{n_2} > 0$, then $n_2 = n_1 + 1$.*

Proof: Assume for sake of contradiction that $\beta_{n_1} > 0$, $\beta_{n_2} > 0$, such that $n_2 = n_1+2$, and that $\beta_{n_0} = 0$ where $n_0 = n_1+1$. Then, from the optimality conditions, we have,

$$\tilde{D}_{n_1} - \gamma + n_1\lambda = 0 \tag{26}$$

$$\tilde{D}_{n_0} - \gamma + (n_1+1)\lambda - \mu_0 = 0 \tag{27}$$

$$\tilde{D}_{n_2} - \gamma + (n_1+2)\lambda = 0 \tag{28}$$

Solving for μ_0 leads to $\mu_0 = \tilde{D}_{n_0} - \frac{1}{2}(\tilde{D}_{n_1} + \tilde{D}_{n_2})$. Since D_n is convex in n, we have $\tilde{D}_{n_0} \leq \frac{1}{2}(\tilde{D}_{n_1} + \tilde{D}_{n_2})$, which implies $\mu_0 \leq 0$. From Lemma 1, $\mu_0 \neq 0$, therefore $\mu_0 < 0$, which is a contradiction. ■

The third lemma states that having m_s to be an integer leads to activating a single β only.

Lemma 3 *$\beta_j = 1$ and $\beta_n = 0$ for all $n \neq j$ if and only if $m_s = j < N$, where $j \in \mathbb{N}$.*

Proof: From the optimality conditions, we have,

$$\tilde{D}_j - \gamma + j\lambda = 0 \tag{29}$$

$$\tilde{D}_n - \gamma + n\lambda - \mu_n = 0, \quad n \neq j \tag{30}$$

Substituting γ from (29) in (30) leads to,

$$(\tilde{D}_n - \tilde{D}_j) + (n-j)\lambda = \mu_n \geq 0 \tag{31}$$

which further implies that $\lambda \geq \frac{\tilde{D}_j - \tilde{D}_n}{n-j}$. Choose $n > j$. Since $\tilde{D}_n$ is monotonically decreasing in n, $\lambda \geq c > 0$ for some positive constant $c = \frac{\tilde{D}_j - \tilde{D}_n}{n-j}$. Since $\lambda > 0$, the inequality $\sum_{n=1}^{N} n\beta_n \leq m_s$ is met with equality. To have a feasible solution for the two equations $\sum_{n=1}^{N} \beta_n = 1$ and $\sum_{n=1}^{N} n\beta_n = m_s$, we must have $m_s = j$ and $\beta_j = 1$. ■

Now, we show the solution for the relaxed problem for non-integer m_s in the following lemma.

Lemma 4 *For the relaxed problem* (22)*, if $j-1 < m_s < j$, then $\beta^*_{j-1} = j - m_s$ and $\beta^*_j = m_s - (j-1)$.*

Proof: From Lemma 1, at most two βs should be positive. From Lemma 3, exactly two βs are positive. From Lemma 2, they should be consecutive and because of continuity, we must have $\beta_{j-1} > 0$ and $\beta_j > 0$. Thus, on the boundary, we have,

$$\beta_{j-1} + \beta_j = 1 \tag{32}$$

$$(j-1)\beta_{j-1} + j\beta_j = m_s \tag{33}$$

Solving both equations simultaneously results in $\beta^*_{j-1} = j - m_s$ and $\beta^*_j = m_s - (j-1)$. ■

Finally, to show the equivalence between the original linear program in (11) and the relaxed problem in (22), we need to show the existence of a feasible (non-negative) solution of (11) for every optimal solution of (22).

Lemma 5 *There exists a feasible (non-negative) solution, i.e., a feasible content assignment, of* (11) *corresponding to the optimal solution of the relaxed problem of* (22)*.*

Proof: We carry out the existence proof using Farkas' lemma. We illustrate the general idea using the following example with $N = 4$ for the case $1 < m_s < 2$. A more general proof that uses the theory of positive linear dependence can be found in the longer version [38]. Using Lemma 4, we have $\beta^*_1 = 2 - m_s$ and $\beta^*_2 = m_s - 1$. We want to show the existence of $\alpha_i \geq 0$ and $\alpha_{ij} \geq 0$ for all i, j such that,

$$\alpha_1 + \alpha_{12} + \alpha_{13} + \alpha_{14} = m_1 \tag{34}$$

$$\alpha_2 + \alpha_{12} + \alpha_{23} + \alpha_{24} = m_2 \tag{35}$$

$$\alpha_3 + \alpha_{13} + \alpha_{23} + \alpha_{34} = m_3 \tag{36}$$

$$\alpha_4 + \alpha_{14} + \alpha_{24} + \alpha_{34} = m_4 \tag{37}$$

$$\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 2 - m_s \tag{38}$$

$$\alpha_{12} + \alpha_{13} + \alpha_{14} + \alpha_{23} + \alpha_{24} + \alpha_{34} = m_s - 1 \tag{39}$$

This is a linear system with 10 unknowns and 6 equations in the form of $\boldsymbol{A}\boldsymbol{\alpha} = \boldsymbol{b}$, where $\boldsymbol{A}$ is the coefficients matrix. To show the existence of a non-negative solution, we use Farkas' lemma, which states that there exists a non-negative solution $\boldsymbol{\alpha} \geq \mathbf{0}$ that satisfies $\boldsymbol{A}\boldsymbol{\alpha} = \boldsymbol{b}$ if and only if for all $\boldsymbol{y}$ for which $\boldsymbol{A}^T\boldsymbol{y} \geq \mathbf{0}$, we have $\boldsymbol{b}^T\boldsymbol{y} \geq 0$. We transform the system of equations into the reduced-echelon form with:

$$\boldsymbol{A} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & -1 & -1 \\ 0 & 1 & 0 & 0 & 0 & -1 & -1 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 & -1 & 0 & -1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & -1 & -1 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \tag{40}$$

$$\boldsymbol{b} = [1-m_s+m_1 \;\; 1-m_s+m_2 \;\; 1-m_s+m_3 \;\; 1-m_s+m_4 \;\; m_s-1]^T \tag{41}$$

Hence, for any $\boldsymbol{y}$ for which $\boldsymbol{A}^T\boldsymbol{y} \geq \mathbf{0}$ implies that:

$$y_n \geq 0, \quad n \in [4] \tag{42}$$

$$y_5 \geq y_i + y_j, \quad i, j \in [4] \tag{43}$$

Now, we want to show $\boldsymbol{b}^T\boldsymbol{y} \geq 0$. To that end, we have the following implications assuming $\boldsymbol{b} \leq \mathbf{0}$ (the worst case):

$$\begin{aligned} \boldsymbol{b}^T\boldsymbol{y} =& (1-m_s+m_1)y_1 + (1-m_s+m_2)y_2 + (1-m_s+m_3)y_3 \\ &+ (1-m_s+m_4)y_4 + (m_s-1)y_5 \end{aligned} \tag{44}$$

$$\begin{aligned} \geq& m_1y_2 + m_2y_2 + (1-m_s+m_3)y_2 \\ &+ (1-m_s+m_4)y_2 = (2-m_s)y_2 \geq 0 \end{aligned} \tag{45}$$

where (45) follows from (42) and (43) taking into consideration that $1-m_s+m_3 \leq 0$, $1-m_s+m_4 \leq 0$. This concludes the existence proof of a feasible solution that solves the relaxed problem for $N = 4$ and $1 < m_s < 2$. ■

Finally, we give an explicit (parametric in $\boldsymbol{m}$) solution for $N = 3$ in Table I. This assignment solves both the relaxed

TABLE I
EXPLICIT CONTENT ASSIGNMENT FOR $N = 3$, $K = 3$, AND $m_1 \geq m_2 \geq m_3$ (WITHOUT LOSS OF GENERALITY).

Case	Assignment
$1 \leq m_s \leq 2$ $m_1 + m_2 \geq 1$ $m_1 + m_3 \geq 1$ $m_2 + m_3 \geq 1$	$\alpha_1 = 2 - m_s$ $\alpha_2 = \alpha_3 = 0$ $\alpha_{12} = m_1 + m_2 - 1$ $\alpha_{13} = m_1 + m_3 - 1$ $\alpha_{23} = 1 - m_1$
$1 \leq m_s \leq 2$ $m_1 + m_2 \geq 1$ $m_1 + m_3 \geq 1$ $m_2 + m_3 \leq 1$	$\alpha_1 = 2 - m_s$ $\alpha_2 = \alpha_3 = 0$ $\alpha_{12} = m_1 + m_2 - 1$ $\alpha_{13} = m_1 + m_3 - 1$ $\alpha_{23} = 1 - m_1$
$1 \leq m_s \leq 2$ $m_1 + m_2 \geq 1$ $m_1 + m_3 \leq 1$ $m_2 + m_3 \leq 1$	$\alpha_1 = 1 - (m_2 + m_3)$ $\alpha_2 = 1 - (m_1 + m_3)$ $\alpha_3 = m_3$ $\alpha_{12} = m_s - 1$ $\alpha_{13} = \alpha_{23} = 0$
$1 \leq m_s \leq 2$ $m_1 + m_2 \leq 1$ $m_1 + m_3 \leq 1$ $m_2 + m_3 \leq 1$	$\alpha_1 = 1 - (m_2 + m_3)$ $\alpha_2 = 1 - (m_1 + m_3)$ $\alpha_3 = m_3$ $\alpha_{12} = m_s - 1$ $\alpha_{13} = \alpha_{23} = 0$
$2 \leq m_s \leq 3$	$\alpha_{23} = 1 - m_1$ $\alpha_{13} = 1 - m_2$ $\alpha_{12} = 1 - m_3$

problem (22) and the original problem (11), and matches its homogeneous counterpart in [24] where $\mu = \frac{m_1+m_2+m_3}{3}$.

REFERENCES

[1] B. Chor, E. Kushilevitz, O. Goldreich, and M. Sudan. Private information retrieval. *Journal of the ACM*, 45(6):965–981, November 1998.

[2] N. B. Shah, K. V. Rashmi, and K. Ramchandran. One extra bit of download ensures perfectly private information retrieval. In *IEEE ISIT*, June 2014.

[3] T. Chan, S. Ho, and H. Yamamoto. Private information retrieval for coded storage. In *IEEE ISIT*, June 2015.

[4] A. Fazeli, A. Vardy, and E. Yaakobi. Codes for distributed PIR with low storage overhead. In *IEEE ISIT*, June 2015.

[5] R. Tajeddine and S. El Rouayheb. Private information retrieval from MDS coded data in distributed storage systems. In *IEEE ISIT*, July 2016.

[6] H. Sun and S. A. Jafar. Blind interference alignment for private information retrieval. In *IEEE ISIT*, July 2016.

[7] H. Sun and S. A. Jafar. The capacity of private information retrieval. *IEEE Trans. on Info. Theory*, 63(7):4075–4088, July 2017.

[8] H. Sun and S. A. Jafar. The capacity of robust private information retrieval with colluding databases. *IEEE Trans. on Info. Theory*, 64(4):2361–2370, April 2018.

[9] H. Sun and S. A. Jafar. The capacity of symmetric private information retrieval. *IEEE Trans. on Info. Theory*, 65(1):322–329, January 2019.

[10] K. Banawan and S. Ulukus. The capacity of private information retrieval from coded databases. *IEEE Trans. on Info. Theory*, 64(3):1945–1956, March 2018.

[11] Q. Wang and M. Skoglund. Symmetric private information retrieval for MDS coded distributed storage. In *IEEE ICC*, May 2017.

[12] R. Freij-Hollanti, O. Gnilke, C. Hollanti, and D. Karpuk. Private information retrieval from coded databases with colluding servers. *SIAM Journal on Applied Algebra and Geometry*, 1(1):647–664, 2017.

[13] K. Banawan and S. Ulukus. Multi-message private information retrieval: Capacity results and near-optimal schemes. *IEEE Trans. on Info. Theory*, 64(10):6842–6862, October 2018.

[14] K. Banawan and S. Ulukus. The capacity of private information retrieval from byzantine and colluding databases. *IEEE Trans. on Info. Theory*, 65(2):1206–1219, February 2019.

[15] Y.-P. Wei, K. Banawan, and S. Ulukus. Fundamental limits of cache-aided private information retrieval with unknown and uncoded prefetching. *IEEE Trans. on Info. Theory*, 65(5):3215–3232, May 2019.

[16] S. Kadhe, B. Garcia, A. Heidarzadeh, S. El Rouayheb, and A. Sprintson. Private information retrieval with side information. Available at arXiv:1709.00112.

[17] Z. Chen, Z. Wang, and S. Jafar. The capacity of private information retrieval with private side information. Available at arXiv:1709.03022.

[18] Y.-P. Wei, K. Banawan, and S. Ulukus. The capacity of private information retrieval with partially known private side information. *IEEE Trans. on Info. Theory*. Submitted November 2017. Also available at arXiv:1710.00809.

[19] Y.-P. Wei, K. Banawan, and S. Ulukus. Cache-aided private information retrieval with partially known uncoded prefetching: Fundamental limits. *IEEE JSAC*, 36(6):1126–1139, June 2018.

[20] Y.-P. Wei and S. Ulukus. The capacity of private information retrieval with private side information under storage constraints. *IEEE Trans. on Info. Theory*. Submitted November 2018. Also available at arXiv:1806.01253.

[21] S. Li and M. Gastpar. Single-server multi-message private information retrieval with side information. Available at arXiv:1808.05797.

[22] M. Mirmohseni and M. A. Maddah-Ali. Private function retrieval. Available at arXiv:1711.04677.

[23] Z. Chen, Z. Wang, and S. Jafar. The asymptotic capacity of private search. In *IEEE ISIT*, June 2018.

[24] M. A. Attia, D. Kumar, and R. Tandon. The capacity of private information retrieval from uncoded storage constrained databases. Available at arXiv:1805.04104v2.

[25] K. Banawan and S. Ulukus. Asymmetry hurts: Private information retrieval under asymmetric-traffic constraints. *IEEE Trans. on Info. Theory*. Submitted January 2018. Also available at arXiv:1801.03079.

[26] K. Banawan and S. Ulukus. Private information retrieval through wiretap channel II: Privacy meets security. *IEEE Trans. on Info. Theory*. Submitted January 2018. Also available at arXiv:1801.06171.

[27] K. Banawan and S. Ulukus. Noisy private information retrieval: Separability of channel coding and information retrieval. *IEEE Trans. on Info. Theory*. Submitted July 2018. Also available at arXiv: 1807.05997.

[28] Z. Jia, H. Sun, and S. Jafar. Cross subspace alignment and the asymptotic capacity of X-secure T-private information retrieval. Available at arXiv:1808.07457.

[29] C. Tian, H. Sun, and J. Chen. Capacity-achieving private information retrieval codes with optimal message size and upload cost. Available at arXiv:1808.07536.

[30] R. Bitar and S. El Rouayheb. Staircase-PIR: Universally robust private information retrieval. Available at arXiv:1806.08825.

[31] S. Kumar, A. G. i Amat, E. Rosnes, and L. Senigagliesi. Private information retrieval from a cellular network with caching at the edge. Available at arXiv:1809.00872.

[32] S. Kumar, H.-Y. Lin, E. Rosnes, and A. G. i Amat. Achieving maximum distance separable private information retrieval capacity with linear codes. Available at arXiv:1712.03898.

[33] Y.-P. Wei, B. Arasli, K. Banawan, and S. Ulukus. The capacity of private information retrieval from decentralized uncoded caching databases. *IEEE Trans. on Info. Theory*. Submitted November 2018. Also available at arXiv:1811.11160.

[34] N. Raviv and I. Tamo. Private information retrieval in graph based replication systems. In *IEEE ISIT*, June 2018.

[35] K. Banawan and S. Ulukus. Private information retrieval from non-replicated databases. Available at arXiv:1901.00004.

[36] M. A. Maddah-Ali and U. Niesen. Fundamental limits of caching. *IEEE Trans. on Info. Theory*, 60(5):2856–2867, May 2014.

[37] A. M. Ibrahim, A. A. Zewail, and A. Yener. Coded caching for heterogeneous systems: An optimization perspective. Available at arXiv:1810.08187.

[38] K. Banawan, B. Arasli, Y.-P. Wei, and S. Ulukus. The capacity of private information retrieval from heterogeneous uncoded caching databases. *IEEE Trans. on Info. Theory*. Submitted February 2019. Also available at arXiv:1902.09512.