中国科学: 数学 2023 年 第 53 卷 第 2 期: 151 ∼ 186
SCIENTIA SINICA Mathematica
《中国科学》杂志社
SCIENCE CHINA PRESS
综 述

源于分布式网络的离散模型与组合学方法

献给朱烈教授 80 华诞

韩雪姣[1], 张一炜[2,3], 殷剑兴[4], 吴佃华[5*]

1. 首都师范大学数学科学学院, 北京 100048;
2. 山东大学教育部密码技术与信息安全重点实验室, 青岛 266237;
3. 山东大学网络空间安全学院, 青岛 266237;
4. 苏州大学数学科学学院, 苏州 215006;
5. 广西师范大学数学与统计学院, 桂林 541006
E-mail: xjhan@cnu.edu.cn, ywzhang@sdu.edu.cn, jxyin@suda.edu.cn, dhwu@gxnu.edu.cn

收稿日期: 2022-04-28; 接受日期: 2022-06-21; 网络出版日期: 2022-09-28; * 通信作者
国家重点研发计划 (批准号: 2021YFA1001000)、国家自然科学基金 (批准号: 12001323 和 12161010) 和山东省自然科学基金 (批准号: ZR2021YQ46) 资助项目

摘要 近年来, 分布式网络环境架构下的诸多新型信息科学问题为经典信息论和编码理论带来了新的挑战. 这些问题的研究涉及多种离散模型, 组合设计、图论、组合编码和极值组合学等组合学方法在其中发挥了至关重要的作用. 本文选取网络编码、索引编码、编码缓存、分布式计算和隐私保护信息检索这 5 个源于分布式网络环境的信息科学前沿热点问题, 简要介绍各问题研究进展, 并着重介绍其中涉及的离散模型与组合学思想方法. 同时, 本文针对上述多个专题分别给出一些新结果.

关键词 分布式网络 网络编码 索引编码 编码缓存 分布式计算 隐私保护信息检索

MSC (2020) 主题分类 05B99, 68P30, 68R05

1 背景简介

数字化、网络化和智能化是新一轮科技革命的突出特征, 也是新一代信息技术的聚焦点, 产业升级换代为这些特征赋予新的内涵. 数字化从计算机化向数据化发展, 后者的核心是对信息技术革命与经济社会活动交融生成的大数据的深刻认识与深层利用. 网络化已从互联网延拓到以工业互联网、车联网、智能家居为代表的物联网, 实现人、物、服务之间交叉互联. 智能化是信息技术发展的永恒追求, 引领人工智能技术一代代发展.

新一代信息技术的发展, 必然会产生诸多新型信息科学问题, 为经典信息论和编码理论带来新挑战. 特别地, 在当前大数据时代背景下, 分布式网络环境架构引领了近 20 年来的信息科学多个前沿热点方向. 本文围绕分布式网络环境架构下的下述 5 个信息问题展开讨论.

英文引用格式: Han X J, Zhang Y W, Yin J X, et al. Discrete configurations and combinatorial methods originated from distributed network (in Chinese). Sci Sin Math, 2023, 53: 151–186, doi: 10.1360/SSM-2022-0074

网络编码: 网络通信最基本的目的是将信息从信源节点无差错地传输至信宿节点. 在传统路由网络中, 中间节点只有接力传输的作用. 网络编码通过赋予网络节点一定的计算能力, 有效提升了网络吞吐量. 网络编码思想对信息论、编码理论、密码学和计算机科学等相关领域产生了深远影响.

索引编码: 在一个多用户广播网络中, 信源通过广播形式将信息发送给用户, 以期每个用户得到自己所需信息. 若信源知晓每个用户提前掌握的边信息, 则可通过编码对其广播内容进行压缩, 以减少所需广播数据量. 这个问题被称为索引编码, 其很多理念与技术源于网络编码思想, 旨在提高无线网络的吞吐量、时延和可靠性等性能.

无线网络编码缓存: 网络环境的普及使大众生活对网络的依赖越来越强. 随着移动视频点播等技术的发展, 移动通信业务量爆炸增长. 无线网络缓存方案旨在利用数据传输低峰期的空闲网络带宽, 按一定策略预先将数据分发至网络用户端的缓存之中, 以缓解数据传输高峰期的网络堵塞.

分布式计算: 随着数据量增长和人工智能深入发展, 数据处理的规模和复杂度与日俱增, 同时人们对数据处理的时间要求更为严苛. 许多大型计算任务无法在单个数据处理终端完成, 必须利用分布式计算思想, 将大型计算任务分拆为多个小型子任务并分发至多个数据处理终端. 分布式计算方案的设计需综合考虑来自掉队者、数据安全和算力浪费等多方面的挑战.

隐私保护信息检索: 分布式网络环境为信息安全领域带来新的挑战与机遇. 隐私保护信息检索是信息安全领域经典问题之一, 其目的是使用户在检索信息的同时保护其个人行为隐私. 这个问题在集中式存储环境中已有一定系统性的研究, 主要依赖于密码学思想方法. 而在引入到分布式网络环境后, 产生了一系列新型信息安全问题.

上述问题在某种层面上也展示了 “通信” 与 “计算” 这两个信息处理的基本环节之间的交融. 网络编码思想及其衍生问题, 以一定的计算负荷换取通信效率, 而分布式计算则是以一定的通信负荷简化数据计算任务. 通信与计算的结合是当前信息科学问题总体趋势, 也符合未来 “通算一体化网络” 新型信息论研究的发展需求.

远至经典信息论中图的香农容量, 近至分布式存储编码中再生码的割集界, 离散模型和组合学方法与信息科学的发展一直密不可分, 尤其在近年来分布式网络环境架构下的新型信息科学问题研究中, 诸多离散模型层出不穷, 组合编码、组合设计、图论和极值组合等组合学领域思想方法扮演着越来越重要的角色. 在这些数学工具为信息科学提供理论支撑的同时, 信息科学也为离散模型和组合学方法的研究带来新的动力, 一定程度上反哺于数学理论发展.

基于以上背景, 本文围绕上述源于分布式网络环境的信息科学问题展开综述, 着重介绍其中涉及的离散模型和组合学方法, 期望能吸引组合界同仁关注这一交叉研究方向. 第 2 节阐述网络编码理论的发展及其与子空间设计的关联. 第 3 节介绍索引编码问题及其中基于图论的研究方法. 第 4 和 5 节的主题分别是无线网络缓存方案和分布式计算, 它们都可以用某种与极值图论或组合设计密切相关的组合阵列刻画. 第 6 节讨论隐私保护信息检索方案及其中的组合思想. 在其中部分章节, 本文利用相关组合方法给出一些新的结果. 最后, 第 7 节总结全文, 并简要讨论一些以上主题中涉及组合学思想方法的未来研究方向.

2 网络编码

2.1 研究现状

定义 2.1 (网络) 一个通信网络可以表示为一个有向无圈多重图 $\mathcal{D} = (\mathcal{V}, \mathcal{E})$, 其中, 顶点集 $\mathcal{V}$

$=\mathcal{S}\cup\mathcal{R}\cup\mathcal{M}$, $\mathcal{S}$ 为若干信源节点, $\mathcal{R}$ 为若干信宿节点, $\mathcal{M}$ 为若干中间节点. 每条有向边代表从其起点向其终点传输信息的信道, 每个信道可传输一个单位大小的信息. 对于任意节点 $P\in\mathcal{V}$, 记其输入边集和输出边集分别为 $\mathrm{In}(P)$ 和 $\mathrm{Out}(P)$. 一般假设信源节点无输入边, 信宿节点无输出边.

网络中每个信源节点拥有若干单位大小的独立信息, 信源节点将信息组织成数据包, 经由通信网络中的信道发送出去. 每个中间节点对其接收到的数据包进行必要的复制存储后再按某种规则发送. 最终目的是使各信宿节点可通过其收到的所有数据包得到所有信源发送的信息.

在传统路由网络中, 中间节点 $P\in\mathcal{M}$ 只有接力传输的作用, 即 $\mathrm{Out}(P)$ 中每条边传输的数据只能是来自 $\mathrm{In}(P)$ 中某条边上数据的复制, 这严重限制了网络传输性能. 2000 年, Ahlswede 等 [2] 在其开创性论文中提出网络编码思想, 突破性地赋予中间节点处理数据的功能, 并证明利用编码方法可使网络传输容量达到基于最大流最小割定理的理论上限 [45, 48], 有效提升了网络吞吐量. 网络编码思想对信息论、编码理论、密码学和计算机科学等相关领域产生的深远影响, 可参见文献 [13, 40, 87] 及其中的参考文献.

定义 2.2 (网络编码) 对于一个给定的网络 $\mathcal{D}=(\mathcal{V},\mathcal{E})$, $\mathcal{D}$ 上的网络编码指的是其所有边上的一簇编码函数. 对于每个信源节点 $S\in\mathcal{S}$, $\mathrm{Out}(S)$ 中每条边上的数据包即为 S 所产生的单位信息. 对于中间节点 $P\in\mathcal{M}$, $\mathrm{Out}(P)$ 中每条边上的数据包为 $\mathrm{In}(P)$ 所有边上的数据包的函数. 若上述所有函数均为线性函数, 则此编码方案称为线性网络编码. 若每个信宿节点 $R\in\mathcal{R}$ 可通过其收到的所有数据包解码得到所有信源发送的信息, 则称此网络编码是网络 $\mathcal{D}$ 的一个解, 也称网络 $\mathcal{D}$ 可解.

显然, 一个网络可解的必要条件是每个信宿节点与所有信源节点之间的最小割大于等于全部信源节点产生的单位信息个数. 网络编码思想奠基性的贡献是证明上述必要条件同时也是充分条件. Li 等 [77] 证明在上述条件下, 利用有限域上的线性编码即可找到网络的解. Koetter 和 Médard [67] 给出线性网络编码的局部和全局代数表示, 清晰刻画了线性网络编码问题. Jaggi 等 [58] 给出构造线性网络编码的多项式时间算法, 但此算法需预知网络的具体拓扑结构. 然而, 很多实际应用中并不能预先知晓网络拓扑结构, 为此 Ho 等 [55] 进一步提出随机线性网络编码, 这一思想使线性网络编码有了真正走向实际应用的可能. 在网络编码方案设计中, 基域大小会影响各节点运算复杂度, 因此人们希望在尽可能小的域上寻找网络的解. Ebrahimi 和 Fragouli [42] 将早期的标量网络编码推广至矢量网络编码, 即将每条边上的数据包从标量 (有限域上的一个符号) 推广至矢量 (有限域上的一个向量), 而中间节点的数据处理方式也从对若干标量的线性组合推广至对若干向量的矩阵运算. Etzion 和 Wachter-Zeh [46] 将秩度量码和子空间码应用到矢量网络编码构造中, 显著降低了基域大小.

例 2.1 蝴蝶网络如图 1 所示, 该网络具有一个信源节点 S、两个信宿节点 R_1 和 R_2 及四个中间节点 M_1、M_2、M_3 和 M_4. 其中信源节点拥有两个单位大小的信息 x 和 y, 每条有向边表示一条信道, 可传输一个单位大小的信息. 该网络下每个信宿节点与信源节点之间最小割为 2, 即理论上信宿节点最多能接收到两个单位大小的信源信息. 在传统路由网络中, 中间节点仅能存储与转发消息, 因此 M_3 指向 M_4 的信道上只能在 x 或 y 之中选择一个进行传输, 进而两个信宿节点会有其中之一无法得到所有信源信息. 网络编码思想赋予中间节点处理数据的能力, 节点 M_3 接收到 x 和 y 并将 $x+y$ 传输给 M_4, 从而使得两个信宿节点均可获得所有信源信息.

实际网络通信中, 信道噪声、链路故障和恶意攻击等因素会给数据带来替换错误或擦除错误, 且通信网络中的错误会随着网络传播而逐步积累, 比点对点通信中的错误更难分析处理. 因此, 研究带有纠错性能的网络编码是必要的. Cai 和 Yeung [22] 于 2002 年首次提出网络纠错码的概念, 作为传统代数纠错码在网络编码理论中的推广. 文献 [23, 24] 将源自点对点网络的代数编码方法推广至网络纠错码中. 刻画传统纠错码性能的一些界也被推广至网络纠错码中 [131], 包括球填充界 (Hamming 界)、

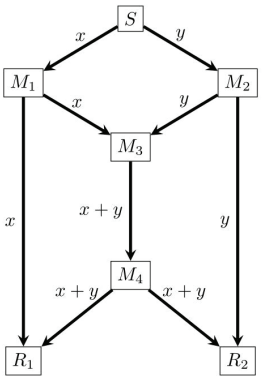

图 1　蝴蝶网络

球覆盖界 (Gilbert-Varshamov 界) 和 Singleton 型界. Zhang[143,144] 提出网络纠错码极小距离的定义, 并进一步独立提出改进的 Singleton 型界. 类似传统代数编码, 达到改进 Singleton 型界的网络纠错码被称为线性网络纠错极大距离可分码, 简称为网络 MDS (maximum distance separable) 码. 网络 MDS 码的存在性已被证明, 文献 [51,88,131] 给出了具体构造方法.

以上网络纠错码的研究, 都需要已知网络拓扑结构. 当网络拓扑结构未知时, 随机网络编码模型中也可以设计性能良好的纠错码. 文献 [66,103] 开启这一研究方向, 定义了子空间上的距离和子空间码, 由此给出随机线性网络纠错码, 并给出这类码的球填充界与球覆盖界等理论分析. 接下来第 2.2 小节将重点介绍子空间码及其与组合设计理论中的子空间设计的关联.

2.2　子空间码和子空间设计

Koetter 和 Kschischang[66] 首先定义了子空间码并将其运用在随机线性网络编码的纠错中. 下面首先引入随机线性网络编码模型, 然后介绍子空间码如何在其中进行纠错.

定义 2.3 (随机线性网络编码)　考虑具有单个信源单个信宿的网络, 信源拥有 M 个单位大小的信息, 信宿与信源之间的最小割大于等于 M, 网络有 T 条边但拓扑结构未知. 每条边传输的数据视为 $\mathbb{F}_q^n$ 上的矢量 (用行向量表示). 信源将 M 个信息 $X_1, X_2, \ldots, X_M$ 输入网络, 其中 $X_i \in \mathbb{F}_q^{1\times n}$ $(i = 1, 2, \ldots, M)$. 对于任意中间节点 $P \in \mathcal{M}$, $\mathrm{Out}(P)$ 中每条边上的数据包是 $\mathrm{In}(P)$ 中所有边上的数据包的随机线性组合. 最终信宿节点通过其接收到的数据包, 以一定概率得到全部 M 个原始信息.

在无噪声情形下, 假设信宿节点接收到 N 个数据包 $Y_1, Y_2, \ldots, Y_N$ $(1 \leqslant j \leqslant N)$. 数据包 $Y_j \in \mathbb{F}_q^{1\times n}$ 可表示为 $Y_j = \sum_{i=1}^{M} a_{j,i}X_i$, 其中系数 $a_{j,i} \in \mathbb{F}_q$ 是未知且随机的. 在有噪声情形下, 记 $E_t \in \mathbb{F}_q^{1\times n}$ 为第 t $(1 \leqslant t \leqslant T)$ 条边上出现的错误, 此时信宿节点接收到的数据包可表示为 $Y_j = \sum_{i=1}^{M} a_{j,i}X_i + \sum_{t=1}^{T} b_{j,t}E_t$, 其中 $b_{j,t} \in \mathbb{F}_q$ 也是未知且随机的. 该模型用矩阵形式可表示为

$$Y = AX + BE,$$

其中, $Y_{N\times n}$ 的第 j 行为 Y_j $(j = 1, 2, \ldots, N)$, $X_{M\times n}$ 的第 i 行为 X_i $(i = 1, 2, \ldots, M)$, $E_{T\times n}$ 的第 t 行为 E_t $(t = 1, 2, \ldots, T)$, $A = [a_{j,i}]_{N\times M}$ 与 $B = [b_{j,t}]_{N\times T}$ 是对应的随机矩阵.

首先观察无噪声时的模型 $Y = AX$. 由于 A 是完全随机的, 那么信源发送的 X 与信宿收到的 Y 之间最大的相通之处是什么? 答案是由两者的行向量各自张成的子空间. 这两个子空间以极大的概率保持一致. 受此启发, 在随机线性网络编码模型中, Koetter 和 Kschischang[66] 提出了子空间码, 其核心思想是用子空间来代表所传输的信息. 令 $\mathcal{P}(\mathbb{F}_q^n)$ 代表 $\mathbb{F}_q^n$ 上的所有子空间, 信源节点发送的信息是

$\mathcal{P}(\mathbb{F}_q^n)$ 中的某个空间 V, 发送方法即选取矩阵 $X \in \mathbb{F}_q^{M\times n}$ 使得 $V = \langle X\rangle$, 即 V 是由 X 的行向量生成的空间. 信宿节点收到矩阵 $Y \in \mathbb{F}_q^{N\times n}$, 通过分析子空间 $U = \langle Y\rangle$ 推断原始信息对应的子空间 V.

在此设定下, 回顾一些涉及子空间的常用符号. 对两个子空间 U 和 V, $U + V = \{u + v : u \in U, v \in V\}$ 是同时包含 U 和 V 的最小子空间. 如果 $U \cap V = \{0\}$, 则 $U + V$ 为两个空间的直和, 记为 $U \oplus V$.

定义 2.4 (擦除算子) 对于任意正整数 $k \geqslant 0$, 定义作用在 $\mathcal{P}(\mathbb{F}_q^n)$ 上的算子 $\mathcal{H}_k$: 如果 $\dim(V) > k$, 则 $\mathcal{H}_k(V)$ 为 V 上随机选取的 k 维子空间, 否则 $\mathcal{H}_k(V) = V$. $\mathcal{H}_k$ 称为 $\mathcal{P}(\mathbb{F}_q^n)$ 上的擦除算子.

定义 2.5 (算子信道) 定义 $C : \mathcal{P}(\mathbb{F}_q^n) \to \mathcal{P}(\mathbb{F}_q^n)$ 为算子信道, 信道的输入 V 和输出 U 满足

$$U = \mathcal{H}_k(V) \oplus E,$$

其中, $k = \dim(U \cap V)$, E 代表错误空间. 在输入 V 输出 U 的过程中, 称该算子信道发生了 $\rho = \dim(V) - k$ 个维度擦除与 $t = \dim(E)$ 个维度错误.

接下来定义两个子空间的距离.

定义 2.6 (子空间距离) 设 V 和 V' 是 $\mathcal{P}(\mathbb{F}_q^n)$ 中的两个子空间, 其距离定义为

$$d_S(V, V') = \dim(V + V') - \dim(V \cap V') = \dim(V) + \dim(V') - 2\dim(V \cap V').$$

文献 [66] 验证了上述距离是 $\mathcal{P}(\mathbb{F}_q^n)$ 上的度量. 基于子空间距离, 可定义如下子空间码.

定义 2.7 (子空间码) 非空集合 $\mathcal{C} \subseteq \mathcal{P}(\mathbb{F}_q^n)$ 为一个子空间码, $\mathcal{C}$ 中每个子空间称为一个码字, 码的极小距离定义为

$$d_S(\mathcal{C}) = \min_{V,V'\in\mathcal{C},V\neq V'} d_S(V, V').$$

特别地, 若码 $\mathcal{C}$ 各码字维数相同, 则称其为常维码 (constant dimension code), 也称 Grassmannian 码.

上述子空间码的定义可以视为经典 Hamming 距离下的码在向量空间上的推广. 类似地, 常维码也是经典常重码在向量空间上的推广. 相较于一般的子空间码, 常维码更容易刻画与构造, 即便如此, 构造码率大的常维码仍不是一件容易的事情.

若随机线性网络编码的算子信道的输入 V 取自某个子空间码 $\mathcal{C}$, 信宿在接收到输出 U 时, 可以寻找 $\mathcal{C}$ 中与 U 距离最近的子空间 $\hat{V}$, 即 $\hat{V} = \arg\min_{V\in\mathcal{C}} d_S(V, U)$. 这种最小距离解码方法类似于经典 Hamming 距离下的码的极大似然译码算法. 文献 [66] 中的下述定理揭示了子空间码在随机线性网络编码的算子信道下的性能.

定理 2.1 [66] 设子空间码 $\mathcal{C} \subseteq \mathcal{P}(\mathbb{F}_q^n)$ 为算子信道的输入集, 输入信息 $V \in \mathcal{C}$ 经过信道转化为输出 $U = \mathcal{H}_k(V) \oplus E$, 其中 $\dim(E) = t$. 称信道发生的最大擦除维数为 $\rho = \max\{0, \max_{V\in\mathcal{C}} \dim(V) - k\}$. 如果 $2(t + \rho) < d_S(\mathcal{C})$, 则最小距离解码方法可以利用 U 成功解出 V.

类似经典组合设计和常重码的天然联系, 子空间设计是获得常维子空间码的重要组合工具.

定义 2.8 (子空间设计) 给定有限域 $\mathbb{F}_q$、正整数 $0 \leqslant t \leqslant k \leqslant v$ 和正整数 λ. 令 $X = \mathbb{F}_q^v$, $\mathcal{A}$ 是 X 的若干 k 维子空间 (称为区组) 组成的多重集. 若 X 的每个 t 维子空间恰好包含于 $\mathcal{A}$ 的 λ 个区组中, 则称 $(X, \mathcal{A})$ 为 t-$(v, k, \lambda)_q$ 子空间设计.

子空间设计, 作为经典组合设计的 q- 模拟, 在文献 [15, 25] 中被提出. Delsarte [39] 以更一般的视角描述了子空间设计问题. 一个平凡的子空间设计可以取 $\mathcal{A}$ 为 X 的全部 k 维子空间, 共计 $\begin{bmatrix} v \\ k \end{bmatrix}_q = \prod_{i=0}^{k-1} \frac{q^v - q^i}{q^k - q^i} = \prod_{i=0}^{k-1} \frac{q^{v-i} - 1}{q^{k-i} - 1}$ 个, 任意 t 维子空间恰好包含于 $\lambda = \begin{bmatrix} v-t \\ k-t \end{bmatrix}_q$ 个 k 维子空间中. 而非

平凡子空间设计的存在性问题在长达 20 年的时间里悬而未决, 直到文献 [118] 成功构造了参数为 2-$(v,3,7)_2$, $v\equiv 1,5\ (\mathrm{mod}\ 6)$, $v\geqslant 7$ 的子空间设计. 该构造被文献 [108,109] 推广至任意有限域 $\mathbb{F}_q$ 上的 2-$(v,3,q^2+q+1)_q$. 文献 [21] 给出了参数为 3-$(8,4,11)_2$ 的子空间设计, 这也是第一个 $t=3$ 的非平凡子空间设计. 迄今为止, 还没有发现 $t\geqslant 4$ 的非平凡子空间设计.

特别地, 当 $\lambda=1$ 时, t-$(v,k,1)_q$ 子空间设计也称 q-Steiner 系 (q-Steiner system), 记作 $\mathbb{S}_q(t,k,v)$. 利用 q-Steiner 系可以直接构造如下常维码.

定理 2.2 一个 q-Steiner 系 $\mathbb{S}_q(t,k,v)$ 可视为 $\mathcal{P}(\mathbb{F}_q^v)$ 中的常维码, 极小距离为 $d=2k-2t+2$.

于是, 构造常维码的一种方法即是寻找对应的 q-Steiner 系. 易知, 若 $\mathbb{S}_q(t,k,v)$ 存在, 则对于任意 i $(1\leqslant i\leqslant t-1)$, $\mathbb{S}_q(t-i,k-i,v-i)$ 也存在. 于是 $\mathbb{S}_q(t,k,v)$ 的存在需要整除性必要条件: 对于任意 $0\leqslant i\leqslant t-1$, $\begin{bmatrix}v-i\\t-i\end{bmatrix}_q/\begin{bmatrix}k-i\\t-i\end{bmatrix}_q$ 需为整数.

记 $A_q(v,d;k)$ 为 $\mathbb{F}_q^v$ 上极小距离为 d、码字维数为 k 的常维码的码字个数最大值. 维数 k 决定了极小距离至多为 $d=2k$, 此时对应的常维码中任意两个 k 维子空间 U 和 V 只有平凡交集 $U\cap V=\{0\}$. 这种码类也称为 k- 部分展形 (partial k-spread). 易得 $A_q(v,2k;k)\leqslant\frac{q^v-1}{q^k-1}$, 且该上界在 $k\mid v$ 时是可达的, 取等号时对应的码也称为 k- 展形 (k-spread), 本质上即为 q-Steiner 系 $\mathbb{S}_q(1,k,v)$. 当 $k\nmid v$ 时, 记 $v=tk+r$, $1\leqslant r\leqslant k-1$, 则 $A_q(v,2k;k)\leqslant\lfloor\frac{q^v-1}{q^k-1}\rfloor=\sum_{s=0}^{t-1}q^{sk+r}$. 构造达到此上界的 k- 部分展形是一个困难的问题. 文献 [16] 给出下述结果.

定理 2.3 设 v 和 k 为正整数, $v=tk+r$, $t\geqslant 2$, $1\leqslant r\leqslant k-1$. 则存在 $\mathbb{F}_q^v$ 上的 k- 部分展形 $\mathcal{S}$, 且 $|\mathcal{S}|=1+\sum_{s=1}^{t-1}q^{sk+r}$. 由此可得 $A_q(v,2k;k)\geqslant 1+\sum_{s=1}^{t-1}q^{sk+r}$.

此下界与理论上界仅相差 q^r-1. 曾有学者猜测这个差距在任何参数下都不会再缩小, 但文献 [44] 给出了 $\mathbb{F}_2^8$ 上包含 34 个子空间的 3- 部分展形, 这也是迄今为止唯一能突破 q^r-1 这个差距的例子. 此外, 目前常维码的已知结果包括 $m\geqslant 2$ 和 $q=2$ 时 $A_2(3m+1,6;3)$、$A_2(3m+2,6;3)$、$A_2(4m+1,8;4)$、$A_2(4m+2,8;4)$ 的值, 目前未确定的最小参数是 $129\leqslant A_2(11,8;4)\leqslant 132$.

已知的非平凡 q-Steiner 系除了上述展形结构之外仅有 $\mathbb{S}_2(2,3,13)$. 在其他参数下寻找 q-Steiner 系或证明其不存在性是子空间设计中极为重要也极为困难的问题. 特别地, $\mathbb{S}_2(2,3,7)$ (即 Fano 平面的 q- 模拟) 的存在性仍是一个公开问题. 除子空间设计外, 通过构造秩度量码和轨迹码等代数编码方法也可以获得子空间码. 子空间码的更多内容可参见文献 [50].

3 索引编码

3.1 研究现状

索引编码 (index coding) 由 Birk 和 Kol[17] 提出, 本质上是一类信源编码问题, 与网络编码思想密切相关. 索引编码问题的数学模型如下. 单个信源与 K 个用户之间通过一条无噪广播信道相连. 信源拥有 N 个相互独立的长度为 B 的文件 $\mathcal{W}=\{W_1,W_2,\ldots,W_N\}$, $W_i\in\mathbb{F}_q^B$ $(i\in[N]\triangleq\{1,2,\ldots,N\})$. 对于第 k 个用户, $k\in[K]$, 记 $U_k=(\mathcal{K}_k,\mathcal{W}_k)$, 其中 $\mathcal{K}_k\subseteq\mathcal{W}$ 代表用户 k 已知的文件集 (也称为该用户的边信息集), $\mathcal{W}_k\subseteq(\mathcal{W}\setminus\mathcal{K}_k)$ 代表用户 k 需求的文件集, 而余下的 $\mathcal{W}\setminus(\mathcal{K}_k\cup\mathcal{W}_k)$ 称为用户 k 的干扰集. 索引编码问题研究在已知 $\{U_k:k\in[K]\}$ 的情形下, 信源应如何通过编码方式设计广播内容, 使所有用户可由广播内容和自身的边信息集译码得到所需文件.

若对于任意两个不同用户 k_1 和 k_2 有 $\mathcal{W}_{k_1}\cap\mathcal{W}_{k_2}=\emptyset$, 则称该索引编码问题是单播的, 否则称其为组播的. 更进一步地, 若每个用户只需求单个文件且各用户需求不同, 则称其为单一单播索引编码

问题. 对于一般单播索引编码问题, 可将单个用户 k 视作 $|\mathcal{W}_k|$ 个拥有同样边信息集但需求信息互不相同的子用户, 于是所有单播索引编码问题皆可视作单一单播索引编码问题. 本节剩余部分仅讨论单一单播索引编码问题, 并不失一般性假设 $N=K$.

一个索引码由一个编码函数和 N 个解码函数组成. 编码函数为 $E:\mathbb{F}_q^{NB}\to\mathbb{F}_q^{RB}$, 该编码函数将文件 $W_1,W_2,\ldots,W_N$ 压缩为信源广播内容 $X=E(W_1,W_2,\ldots,W_N)$.

用户 k 的解码函数为 $D_k:\mathbb{F}_q^{RB}\times\mathbb{F}_q^{|\mathcal{K}_k|B}\to\mathbb{F}_q^{B}$, 用户 k 利用接收到的信源广播内容和自身边信息集译码得到所需文件, 即 $D_k(X,W_{\mathcal{K}_k})=W_k$.

参数 R 称为索引码的码长. 索引编码最基本的问题是在已知 $\{U_k:k\in[K]\}$ 的情形下寻找码长最小的索引码, 达到码长最小值的索引码即称为最优的. 若编码函数 E 是线性的, 则称该索引码为线性索引码. 进一步地, 如果线性编码函数 E 只涉及若干完整文件的线性组合, 则称其为线性标量索引码; 如果编码函数 E 是以文件的每个符号为单位进行运算, 则称其为线性矢量索引码.

索引编码问题可由其边信息图刻画. 单播问题的边信息图一般由简单有向图表示, 基于对此图的分析, 文献 [12] 给出了索引码的奠基性结果, 证明了线性最优标量索引码的码长等于边信息图的最小秩 (minrank), 并提出了基于边信息图的最大无圈诱导子图点数的 (非线性) 索引码码长下界. 当信息图为有向无圈图、完美图等图类时, 上述方法能完整解决索引编码问题, 但对一般的边信息图计算最小秩被证明为 NP (non-deterministic polynomial) 困难. 最小秩方法同样适用于组播索引编码问题. 文献 [3,89,101,115,121] 研究了组播索引编码问题, 该问题的边信息图一般由有向二部图或有向超图表示, 文献 [101,115] 分别借助有向二部图的边信息图提出了文件分区多播和用户分区多播的方法.

单播索引编码的设计与图染色之间也密切关联. 一方面, 索引编码码长上界可由边信息图的团覆盖数控制, 在边信息图可转化为无向图时这一数值又等于其补图的染色数. 另一方面, 由边信息图导出的混淆图, 其染色数直接决定了索引码码长的理论极限. 因此, 图染色的相关结论与方法被自然地引入到索引编码研究中. 特别地, 基于图染色的方法, 文献 [3,81] 给出了非线性索引码能够突破线性索引码最小秩码长限制的例子.

基于分布式网络背景, 假设原始信息分布式存储于多个信源, 文献 [90] 提出多信源索引编码问题, 这是索引编码问题研究的重要分支. 虽然多信源模型比单信源复杂, 但单信源的某些研究方法可以推广至多信源的情形. 例如, 文献 [116] 将单信源模型的环覆盖界、完全图覆盖界和局部染色界推广到两个信源的单一单播索引编码的研究中, 文献 [117] 将基于混淆图染色的索引码的构造方法引入到特定信息图下的双信源索引码的设计中, 文献 [75] 将单信源模型下的最小秩方法推广到多信源情形.

索引编码的研究还有许多变种. 文献 [36] 提出安全索引编码问题, 利用随机线性索引码达到一定抵抗窃听的能力. 文献 [63] 提出索引编码中的隐私保护问题, 以防止网络中各用户的边信息集或需求集的泄露. 柔性索引编码模型不再预设用户具体需求, 只需给每个用户传递一个不在其边信息集中的新文件, 这个领域的工作包括 NP 困难的最优线性码的构造 [20]、多项式时间算法下的次优索引码的构造 [104] 和基于图染色手段的最优码长分析 [69,78–80] 等.

3.2 索引编码中的图论方法

设信源拥有 $\mathcal{W}=\{W_1,W_2,\ldots,W_N\}$, 为方便讨论, 只考虑 $W_i\in\mathbb{F}_2$. $W_i\in\mathbb{F}_q^B$ 的情形也可自然推广. 用户 k 拥有边信息集 $\mathcal{K}_k\subseteq\mathcal{W}$ 且需求 W_k $(1\leqslant k\leqslant N)$.

定义 3.1 (边信息图) 一个单一单播索引编码问题的边信息图 $D=(V,E)$ 是简单有向图, 其中 $V=\{1,2,\ldots,N\}$, 顶点 k 代表需求 W_k 的用户 k. 有向边 $(i,j)\in E$ 当且仅当 $W_j\in\mathcal{K}_i$, 即

W_j 落在用户 i 的边信息集中. $\mathrm{Out}(i)=\{j\in V:(i,j)\in E\}$ 即为用户 i 的边信息集 $\mathcal{K}_i$ 的指标集, $\mathrm{In}(i)=\{j\in V:(j,i)\in E\}$ 即为边信息集中包含 W_i 的用户的指标集.

文献 [12] 定义了边信息图的最小秩, 并证明了最小秩的值即为线性最优标量索引码的码长.

定义 3.2 (最小秩)　对给定的边信息图 $D=(V,E)$, 如果矩阵 $A=(a_{ij})_{N\times N}$ 满足 (1) $a_{ii}=1$; (2) 若 $(i,j)\notin E$, 则 $a_{ij}=0$, 则称这样的矩阵 A 适配于图 D. D 的最小秩定义为

$$\mathrm{minrk}_2(D):=\min\{\mathrm{rk}_2(A):A\text{ 适配于 }D\},$$

其中 $\mathrm{rk}_2(A)$ 代表矩阵 A 在 $\mathbb{F}_2$ 上的秩.

定理 3.1　对给定的边信息图 D, 线性最优标量索引码的码长即为 $\mathrm{minrk}_2(D)$.

最优线性索引码的构造如下. 设矩阵 A 适配于图 D 且 $\mathrm{rk}_2(A)=\mathrm{minrk}_2(D)$. 对 A 做行变换, 使得前 $\mathrm{minrk}_2(D)$ 行线性无关, 记为 A', 而后 $N-\mathrm{minrk}_2(D)$ 行全为 0. 令索引码的编码函数为

$$X=A'(W_1,W_2,\ldots,W_N)^{\mathrm{T}}.$$

于是码长即为 $\mathrm{minrk}_2(D)$. 每个用户收到 X 即等价于收到 $Y=A(W_1,W_2,\ldots,W_N)^{\mathrm{T}}$. 用户 k 的解码只需使用 $A_k\cdot(W_1,W_2,\ldots,W_N)^{\mathrm{T}}$, 其中 A_k 代表矩阵 A 的第 k 行. 在这个线性组合中, W_k 的系数非零, 而用户 k 干扰集中文件的系数皆为 0, 于是用户 k 可以利用其部分边信息求解出所需求的 W_k.

利用上述方法可以确定 n 个点的有向圈对应的索引编码问题的线性最优码长为 $n-1$, 文献 [12] 同时指出, 如果边信息图中不存在圈, 则最优码长为该图的点数, 即只能依次发送每个文件才能满足全部用户的需求. 因此最优码长的下界可由边信息图点数最大的无圈诱导子图给出. 该下界虽然是从线性编码角度得出的, 但同样适用于非线性索引码.

定理 3.2　记 $\mathrm{MAIS}(D)$ 为简单有向图 D 的最大无圈诱导子图 (maximal acyclic induced subgraph, MAIS) 的点数, 则以 D 为边信息图的索引码的码长至少为 $\mathrm{MAIS}(D)$.

例 3.1　单个信源与 4 个用户之间通过一条无噪广播信道相连. 信源拥有 4 个相互独立的文件 $\mathcal{W}=\{W_1,W_2,W_3,W_4\}$. 4 个用户分别为 $U_1=(\{W_2,W_4\},\{W_1\})$, $U_2=(\{W_1\},\{W_2\})$, $U_3=(\{W_2\},\{W_3\})$, $U_4=(\{W_3\},\{W_4\})$. 则该问题的边信息图 D 如图 2 所示. 注意到 D 是包含有向圈的, 但由顶点 2、3 和 4 诱导的子图是无圈的, 因此该问题的 MAIS 下界为 3. 达到最优码长的方案可以是依次广播 W_1+W_2、W_3 和 W_4.

事实上, 最优非线性索引码的码长可由下述混淆图的染色数决定, 混淆图的定义如下.

定义 3.3 (混淆图)　设有向图 D 是某索引编码问题的边信息图, 构造无向图 $C(D)$ 如下. 点集 $V=\mathbb{F}_2^N$, 两个顶点 $\boldsymbol{u}=(u_1,\ldots,u_N)$ 与 $\boldsymbol{v}=(v_1,\ldots,v_N)$ 之间连边当且仅当存在 $i\in[N]$, 满足 $u_i\neq v_i$ 且对于任意 $(i,j)\in D$ 有 $u_j=v_j$. 称无向图 $C(D)$ 为 D 的混淆图.

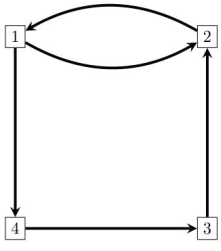

图 2　索引编码边信息图示例

混淆图中的每个顶点实则对应于 $\{W_1, W_2, \ldots, W_N\}$ 一组可能的取值. 若 $\boldsymbol{u}$ 和 $\boldsymbol{v}$ 在混淆图中连边, 则用户 i 所拥有的边信息完全一致, 而自身需要译码得到的 W_i 不同, 于是索引码的必要条件是一定要将 $\boldsymbol{u}$ 和 $\boldsymbol{v}$ 编码为不同的码字, 否则将导致用户 i 的解码失败. 因此, 编码函数 $E: \mathbb{F}_2^N \longrightarrow \mathbb{F}_2^R$ 的值域大小至少需为混淆图染色数 $\chi(C(D))$, 从而码长有下界 $\log_2 \chi(C(D))$. 达到此界的非线性索引码的构造可基于混淆图 $C(D)$ 的任意一个使用 $\chi(C(D))$ 种颜色的染色, 编码函数将信息映射为其对应顶点的颜色标号的二进制表示, 用户在知晓此染色信息后, 从图中所有染此色的点中寻找到唯一的与自身边信息吻合的点, 进而通过此点译码得到所需信息.

结合上述码长上下界的基本结果可知, 若对于信息图 G 有 $\mathrm{minrk}_2(D) = \mathrm{MAIS}(D)$ 或 $\mathrm{minrk}_2(D) = \log_2 \chi(C(D))$, 则最优码长可确定且线性编码方式即能达到最优. 例如, 完美图、奇洞及其补图对应的最优索引码长都达到 $\mathrm{minrk}_2(D)$. 但在一般情形下, 无论求解最小秩或求解混淆图的染色数都是 NP 困难的, 更多做法是利用已知最优码长的特殊图类覆盖边信息图.

当确定部分特殊图类对应的最优码长后, 对于一般的信息图 D, 可以考虑用已解决的图类对 D 做顶点覆盖, 即将顶点集划分为 $V_1, V_2, \ldots, V_t$, 再将每个 V_i 诱导的子图看作一个子问题分别解决. 例如, 由最小秩方法知 n 个点完全图对应的线性最优码长为 1, 编码函数为将这 n 个点对应的文件进行异或运算. 将 D 的顶点集拆分为若干完全子图 (即做 D 的团覆盖) 即可得到最优码长的上界, 当 D 是无向图 (即有向边是成对出现的) 时, D 的补图 $\overline{D}$ 的染色数即为 D 的团覆盖数. 更进一步地, 对 $\overline{D}$ 运用分数染色方法, 可以获得更小的上界: 对 $\overline{D}$ 的每个顶点染 b 个颜色使相邻的两个顶点无相同颜色, 则 $\frac{\chi_f(\overline{D})}{b}$ 是最优码长上界, 其中 $\chi_f(\overline{D})$ 为 $\overline{D}$ 的分数染色数. 对应的编码策略为, 将每个顶点对应的文件均匀地分为 b 份并随机分配给子文件一个该点的颜色, 且每个文件的子文件分配的颜色各不相同, 编码函数即为将每个颜色下的子文件进行异或运算. 分数染色方法是一种矢量线性编码策略, 线性编码策略可以视为其特殊情形, 因此 $\frac{\chi_f(\overline{D})}{b} \leqslant \chi(\overline{D})$.

3.3 新的结果

基于分布式网络背景, 文献 [90] 提出了多信源索引编码问题. 许多单信源模型下的方法可以推广至多信源模型的研究之中. 本小节以双信源为例, 将单信源模型中的 MAIS 下界思想加以推广.

考虑两个信源、N 个用户的无噪单一单播索引编码问题. 假设该索引编码系统中具有 N 个相互独立的文件 $\mathcal{W} = \{W_1, W_2, \ldots, W_N\}$, 这些文件分布式地存放于两个信源中, 两个信源拥有的信息分别记为 S_1 和 S_2, $S_1 \cup S_2 = \mathcal{W}$. 该索引编码问题的边信息图 D 与单信源模型下的定义相同.

仿照单信源模型的 MAIS 下界, 可以证明, 对于满足下列性质的边信息图, 最优索引编码的码长必须为 N, 也即不存在比逐个广播所有文件更好的方法.

定理 3.3 在双信源无噪单一单播索引编码问题中, 如果边信息图 D 中不包含以下结构:

(A) 顶点全部在 S_1 或 S_2 的指标集中的有向圈;

(B) $S_1 \cap S_2 \neq \emptyset$ 的指标集中的某个顶点位于 D 的某个有向圈中;

(C) $S_1 \cap S_2 \neq \emptyset$ 的指标集中的某个顶点通过一条有向路径指向某个有向圈中的顶点,

则该索引编码问题的最优码长为 N.

证明 回顾有向图中强连通的定义. 一个有向简单图的两个顶点 u 与 v 之间, 若既存在从 u 到 v 的有向路径, 又存在从 v 到 u 的有向路径, 则称两个点之间强连通. 强连通是顶点集上的等价关系, 对应的每个等价类称为一个强连通分支.

考虑一个不包含定理所述结构的信息图 D, 设 D 共有 s 个强连通分支, $1 \leqslant s \leqslant N$. 将这 s 个强连通分支编号为 $D_1, D_2, \ldots, D_s$, 使得该标号下对于任意 $1 \leqslant i < j \leqslant s$ 都不存在由 D_j 中的点指向 D_i 中的点的有向边. 同时各强连通分支还有如下性质.

(1) 顶点个数大于 1 的强连通分支必然同时包含 U_1 和 U_2 两个指标集中的点, 其中 $U_1 = S_1 \setminus S_2$ 和 $U_2 = S_2 \setminus S_1$ 分别为两个信源独有的文件. 这一性质由 D 不包含结构 (A) 和 (B) 决定.

(2) 若 $S_1 \cap S_2 \neq \emptyset$, 则此指标集中的每一个顶点都是单独的强连通分支, 该性质由 D 不包含结构 (B) 决定.

(3) 若 $S_1 \cap S_2 \neq \emptyset$, 则此指标集中每一个顶点所在的强连通分支编号均大于所有点数大于 2 的强连通分支标号, 该性质由 D 不包含结构 (C) 决定.

对于任意 $A \subseteq \mathcal{W}$, 令 $D|_A$ 为 D 由 A 的指标集诱导的子图. 当 $k = 1$, 即 D 为强连通时, 由上述性质可知 $S_1 \cap S_2 = \emptyset$, $\mathcal{W}$ 是 S_1 和 S_2 的不交并. 因此每个文件的发送只能来自唯一信源. 因此 $R(D) = R(D|_{U_1}) + R(D|_{U_2})$. $R(D|_{U_1})$ 和 $R(D|_{U_2})$ 各自可视为单信源索引编码问题且各自的信息图无有向圈, 则由 MAIS 下界可知 $R(D) = |U_1| + |U_2| = N$.

设 $s \geqslant 2$, $|V(D_s)| \geqslant 2$, 注意到 D 的顶点数有限, 且没有任何从 D_s 出发指向其他强连通分支的顶点, 即 D_s 中顶点对应用户的边信息只在 D_s 中. 由上述分析知 $R(D_s) = R(D_s|_{U_1}) + R(D_s|_{U_2}) = |V(D_s)|$, 即每个 D_s 中顶点代表的信息都只能通过该信源系统发送信息本身来满足用户的需求, 且发送完毕后可以在 D 中直接删掉对应的顶点和与之相连的有向边. 设删后的图为 D', 则 D' 中没有任何从 D_{s-1} 出发指向其他强连通分支的顶点, 按上述分析依次类推得 $R(D) = N$. □

由此, 当边信息图中包含一个无以上三种结构的诱导子图时, 对应的最优索引码码长的下界即为该诱导子图的顶点数. 这样的子图也可以通过删除边信息图的顶点及其邻边, 直到边信息图中不再包含以上三种结构的方式得到.

注 3.1 在定理 3.3 提到的三种结构均可能在双信源情形下使信源广播量减 1, (A) 结构可视为单信源情形, 自然有向圈结构可带来广播量减 1; 设 (B) 和 (C) 结构中出现的一个 $S_1 \cap S_2$ 中文件为 W_t, 则对应的编码策略为分别将结构中除 W_t 的点与 W_t 进行异或运算并由信源 S_1 广播包含 U_1 中文件的内容, 信源 S_2 广播其他内容, 此时的广播量比结构中的点数少 1.

4 编码缓存

4.1 研究现状

网络中数据需求量具有时变性, 数据需求高峰期的网络堵塞影响用户体验, 数据需求低峰期的带宽闲置浪费网络资源. Maddah-Ali 和 Niesen[83] 提出了无线网络缓存方案, 旨在利用低峰期闲暇带宽, 采取一定策略将数据预分发至网络各用户端缓存中, 以减少高峰期通信负荷.

定义 4.1 (编码缓存) 考虑由单个服务器和 K 个用户组成的网络, 服务器与用户间通过一条无噪共享链路相连. 服务器存储 N 个相互独立文件 $W_1, W_2, \ldots, W_N$, $W_i \in \mathbb{F}_2^B$, $i \in [N]$. 用户 $k \in [K]$ 具有独立的缓存, 可用来存储 $Z_k \in \mathbb{F}_2^{MB}$, 其中 M 是给定的实数, $M < N$. 记上述系统为 (K, M, N) 缓存系统.

编码缓存方案分为放置阶段与分发阶段两部分. 在放置阶段, 服务器依照一定策略将数据预存至各用户的缓存中. 在分发阶段, 每个用户向服务器点播一份文件, 服务器以广播形式发送信息, 使得每个用户可由分发阶段的信息和自身缓存得到所点播文件.

定义 4.2 (编码缓存方案) 一个 (K,M,N) 缓存系统中的编码缓存方案由下列函数构成.

• 放置阶段 K 个缓存函数:

$$\phi_k:\mathbb{F}_2^{NB}\longrightarrow\mathbb{F}_2^{MB},\quad k\in[K].$$

每个缓存函数将信息 $W_1,W_2,\ldots,W_N$ 映射为用户 k 的缓存内容 $Z_k:=\phi_k(W_1,W_2,\ldots,W_N)$.

• 分发阶段 N^K 个编码函数:

$$\psi_{(d_1,d_2,\ldots,d_K)}:\mathbb{F}_2^{NB}\longrightarrow\mathbb{F}_2^{RB},$$

其中 $(d_1,d_2,\ldots,d_K)\in[N]^K$ 为各用户在分发阶段所需求的文件指标. 服务器在得知这些指标后将信息 $W_1,W_2,\ldots,W_N$ 映射为所需广播内容 $X_{(d_1,d_2,\ldots,d_K)}:=\psi_{(d_1,d_2,\ldots,d_K)}(W_1,W_2,\ldots,W_N)$.

• 用户端共计 KN^K 个解码函数:

$$\mu_{(d_1,d_2,\ldots,d_K),k}:\mathbb{F}_2^{RB}\times\mathbb{F}_2^{MB}\longrightarrow\mathbb{F}_2^{B},\quad k\in[K].$$

用户 k 利用自身缓存和广播内容解码得到所需求文件 $\mu_{(d_1,d_2,\ldots,d_K),k}(X_{(d_1,d_2,\ldots,d_K)},Z_k)=W_{d_k}$.
其中参数 R 是遍历所有需求 $(d_1,d_2,\ldots,d_K)$ 最坏情况下的传输负载, 称为缓存方案的传输率.

在 (K,M,N) 缓存系统中, 人们希望 R 尽量小, 即数据需求高峰时刻占用网络资源少. 考虑最平凡的非编码方案, 各用户分别缓存每个文件的 $\frac{M}{N}$ 比例的数据, 在数据分发阶段, 服务器可将各用户需求文件中缺失的 $1-\frac{M}{N}$ 部分的数据逐个发放, 在各用户需求相异的最坏情况下有 $R=K(1-\frac{M}{N})$. 贝尔实验室 (Bell Labs) 的 Maddah-Ali 和 Niesen[83] 基于网络编码思想, 创造性提出编码缓存方案. 在放置阶段, 各用户的缓存按一定编码规律存储, 获得局部缓存增益; 在分发阶段, 利用已有缓存信息之间的关系, 设计所需广播内容的特定编码组合, 使得多个用户同时从单次广播中得到所需部分信息, 从而得到全局缓存增益. Maddah-Ali 和 Niesen 的方案传输率为 $R=K(1-\frac{M}{N})\min\{\frac{N}{N+KM},\frac{N}{K}\}$, 这个方案在文献 [138] 中被证明在 $N\geqslant K$ 且非编码放置下 (即放置的缓存仅为各文件独立的数据包, 无编码处理) 达到最优. 然而, R 并非衡量缓存方案优劣的唯一指标, 实现 Maddah-Ali 和 Niesen 的方案需要将每个文件等分为 $F=\binom{K}{KM/N}$ 份 (该数值称为分包数, 影响方案实现的复杂度), 这一数值随 K 呈指数增长, 这是他们方案的一个缺陷. 缓存方案的后续研究中往往给定参数 K 和 $\frac{M}{N}$ (与 K 无关的比例), 研究传输率 R 和分包数 F 作为 K 的函数的表现.

编码缓存方案与组合数学之间的紧密联系, 最初由 Yan 等[127] 通过一类组合阵列刻画, 此阵列称为放置分发阵列 (placement and delivery array, PDA), 描述了放置阶段和分发阶段的具体规则. Yan 等[127] 给出了两类 PDA 的构造, 同 Maddah-Ali 与 Niesen 的方案相比, 在小幅增加传输率 R 的代价下显著降低分包数 F, 但 F 仍随 K 呈指数增长.

Shangguan 等[100] 将 PDA 的构造与极值超图中的 Turán 型问题联系起来, 证明了 PDA 可对应于 3 一致 3 部超图且任意 6 个顶点诱导的子图至多包含 3 条边 (实为极值超图中著名的 $(6,3)$- 问题). 基于此观察, Shangguan 等[100] 给出在传输率 R 保持常数级别时分包数 F 达到 K 的次指数级别的方案, 同时证明 F 不可能达到 K 的线性级别. 沿着类似思路, Shanmugam 等[102] 利用 Ruzsa-Szeméredi 图得到 R 为 K 的多项式级别、F 为 K 的线性级别的缓存方案.

此外, PDA 和对应超图的研究, 与其他多种组合结构之间产生了联系. 基于正交阵列[30]、二部图的强边染色[129] 等方法都被应用于 PDA 的构造中, 基于线性分组码[114]、组合设计[1] 的构造方法虽然没使用 PDA 语言, 但本质上可以转化为 PDA. 文献 [28,122] 讨论了 PDA 的递归构造.

但截至目前, 关于传输率 R 为常数级别而分包数 F 为 K 的多项式级别的缓存方案, 既没有任何构造, 也无法从理论上证明其不存在性.

上述工作针对的是缓存问题提出伊始的模型: 集权式网络 (单个核心服务器统筹规划两个阶段)、非编码放置 (缓存内容为单个文件的部分区块)、离线版本 (数据库无更新). 近年来, 缓存问题模型逐步扩展, 包括但不限于:

• 线性编码放置: 放置阶段的缓存内容可以是文件子数据包的线性组合, 在这种模型下文献 [29] 给出的方案有更小分包数.

• 非集权式编码缓存: 现实中大部分网络并不具备统筹整个编码缓存过程的中央服务器, 文献 [84] 考虑了随机缓存放置时的编码.

• 无线 D2D (device-to-device) 网络下的编码缓存: 该模型下分发阶段由用户完成, 文献 [59] 给出该问题在固定缓存大小时最优传输率的上下界刻画.

• 安全编码缓存模型: 引入安全需求, 防止窃听者通过窃听分发阶段的信息而得到任何原始文件信息, 文献 [98] 给出该问题在固定缓存大小时最优传输率的上下界刻画.

• 多接入网络的编码缓存: 该模型假设网络中有多个缓存单元, 用户可按一定规则从一部分缓存单元中获得信息. 该模型由文献 [52] 提出, 交叉可分解设计 [64]、PDA [97] 和对称索引编码 [95] 等被用来设计该问题的编码缓存方案.

• 在线编码缓存: 服务器中文件动态可变, 进而用户的缓存内容也是动态的, 每轮的分发阶段可以改变其缓存内容. 该模型是文献 [83] 提出的未来研究课题之一, 其目标为在系统长期运行过程中降低数据传输的平均负载. 文献 [91,128] 探讨了此模型下缓存更新的相关算法.

4.2 PDA 及其组合构造

集权式网络、非编码放置、离线版本下的最初编码缓存模型可由 Yan 等 [127] 提出的放置分发阵列 PDA 刻画.

定义 4.3 (放置分发阵列 PDA) 设 K、F、Z 和 S 是正整数, 阵列 $\boldsymbol{P}=[p_{j,k}]_{F\times K}$ 中每个项取自 $[S]=\{1,2,\ldots,S\}$ 或者特殊符号 $*$. 如果 $\boldsymbol{P}$ 满足以下条件:

(1) $*$ 在每列恰好出现 Z 次;

(2) 任意整数 $s\in[S]$ 在每一行、每一列至多出现一次;

(3) 对于任意 $j_1\neq j_2$, $k_1\neq k_2$, 若 $p_{j_1,k_1}=p_{j_2,k_2}=s\in[S]$, 则 $p_{j_1,k_2}=p_{j_2,k_1}=*$,

则称阵列 $\boldsymbol{P}$ 为 (K,F,Z,S)-PDA. 记 g_s 为 $s\in[S]$ 在 PDA 中出现的次数, $(K,F,Z,S)(g_1,g_2,\ldots,g_S)$-PDA 表示 s 恰好出现 g_s 次的 (K,F,Z,S)-PDA. 特别地, 若所有 g_s 都等于 g, 则称 $\boldsymbol{P}$ 为 g- 正则的, 简记为 g-(K,F,Z,S)-PDA 或 g-PDA.

给定一个 (K,F,Z,S)-PDA, 其放置分发阶段及用户解码算法如下.

• 放置阶段: 每个文件等分为 F 个数据包, 即对于任意 $i\in[N]$, 令 $W_i=\{W_{i,j}:j\in[F]\}$. 每个用户 $k\in[K]$ 的缓存为 $Z_k=\{W_{i,j}:p_{j,k}=*,i\in[N]\}$. 易验证每个用户的缓存大小等同于 $\frac{ZN}{F}$ 个文件.

• 分发阶段: 假设各用户需求为 $d=(d_1,d_2,\ldots,d_K)$. 服务器共传输 S 份信息, 其中第 s ($s\in[S]$) 份为下列数据包的异或运算:

$$\bigoplus_{p_{j,k}=s,j\in[F],k\in[K]} W_{d_k,j}.$$

• 用户的解码算法: 用户 $k\in[K]$ 需求文件 W_{d_k}, 且其缓存中已拥有 $\{W_{d_k,j}:p_{j,k}=*\}$, 需要再从广播中获取 $\{W_{d_k,j}:p_{j,k}\in[S]\}$. 设 $\boldsymbol{P}$ 中 $p_{j,k}=s$, 基于 PDA 的第三条性质, 用户 k 已知所有

$\{W_{d_{k'},j}: p_{j,k'}=s, k'\neq k\}$, 于是可从分发阶段的第 s 份信息中译码得到 $W_{d_k,j}$.

综上所述, 当 (K,F,Z,S)-PDA 存在且 $\frac{Z}{F}=\frac{M}{N}$ 时, 该 PDA 可以给出 (K,M,N) 缓存系统中传输率为 $R=\frac{S}{F}$ 的缓存方案. 下面展示 PDA 与超图 [100]、二部图的强边染色 [129] 和 Ruzsa-Szeméredi 图 [102] 等多种组合结构的关联.

例 4.1 考虑一个 $(K=4,M=3,N)$ 缓存系统, 对应下述 $(K=4,F=5,Z=3,S=3)$-PDA:

$$\begin{pmatrix} 1 & * & * & * \\ * & 1 & * & 3 \\ * & * & 1 & 2 \\ 2 & * & 3 & * \\ * & 2 & * & * \end{pmatrix}.$$

每个文件等分为 5 个数据包, 即任意文件 $W_i=\{W_{i,j}: 1\leqslant j\leqslant 5\}$. 以第一个用户为例, 该用户缓存的内容为 $Z_1=\{W_{i,j}: p_{j,1}=*, i\in[N]\}=\{W_{i,2},W_{i,3}W_{i,5}: i\in[N]\}$. 假设各用户的需求为 $d=(1,2,3,4)$, 在分发阶段, 服务器在第 1 个时隙传输为 $W_{1,1}\oplus W_{2,2}\oplus W_{3,3}$, 在第 2 个时隙传输为 $W_{1,4}\oplus W_{2,5}\oplus W_{4,3}$, 在第 3 个时隙传输为 $W_{3,4}\oplus W_{4,2}$.

用户 1 的解码过程如下. 由于缓存中已知 $W_{1,2}$、$W_{1,3}$ 和 $W_{1,5}$, 所以只需求解 $W_{1,1}$ 与 $W_{1,4}$. 注意到第 1 个时隙传输的内容, 用户 1 的缓存中已知 $W_{2,2}$ 与 $W_{3,3}$, 因此可解得 $W_{1,1}$; 在第 2 个时隙传输的内容中, 用户 1 已知 $W_{2,5}$ 与 $W_{4,3}$, 因此可解得 $W_{1,4}$. 其余用户的解码过程与用户 1 类似. 该 PDA 给出的编码缓存方案的传输率为 $\frac{3}{5}$.

4.2.1 利用超图构造 PDA

设 $\mathcal{H}=(V(\mathcal{H}),E(\mathcal{H}))$ 是一个超图, 其中 $V(\mathcal{H})$ 和 $E(\mathcal{H})$ 分别为顶点集和边集, 超图的每条边都是顶点集的一个非空子集. 如果任意两条不同的边 $A,B\in E(\mathcal{H})$ 满足 $|A\cap B|\leqslant 1$, 则称 $\mathcal{H}$ 为线性的. 如果所有边 $A\in E(\mathcal{H})$ 满足 $|A|=r$, 则称 $\mathcal{H}$ 为 r 一致的. 若能用 c 种颜色对 $\mathcal{H}$ 进行顶点染色, 使 $\mathcal{H}$ 的每条边中都没有两个相同颜色的顶点, 则称 $\mathcal{H}$ 是 c 部的. 如果 $\mathcal{H}$ 中任意 e 条边至少包含 $v+1$ 个顶点, 换言之, 任意 v 个顶点诱导的子图边数严格小于 e, 则称 $\mathcal{H}$ 是无 (v,e) 结构的.

Shangguan 等 [100] 发现 (K,F,Z,S)-PDA 可以等价地表示为一个无 $(6,3)$ 结构的线性 3 一致 3 部超图. 超图的三个部分别取为 $\mathcal{F}$、$\mathcal{K}$ 和 $\mathcal{S}$, $|\mathcal{F}|=F$, $|\mathcal{K}|=K$, $|\mathcal{S}|=S$. 当 PDA 中 $p_{j,k}=s$ 时, $\{j,k,s\}\in E(\mathcal{H})$, $j\in\mathcal{F}$, $k\in\mathcal{K}$, $s\in\mathcal{S}$. 按这种方式 PDA 与超图之间一一对应. 从超图的角度, Shangguan 等 [100] 将 PDA 的三条性质重新刻画如下.

定理 4.1 (K,F,Z,S)-PDA 存在当且仅当存在一个无 $(6,3)$ 结构的线性 3 一致 3 部超图, 其中顶点集分为三部 $\mathcal{F}$、$\mathcal{K}$ 和 $\mathcal{S}$, 且 $|\mathcal{F}|=F$, $|\mathcal{K}|=K$, $|\mathcal{S}|=S$, 每个顶点 $k\in\mathcal{K}$ 恰好出现在 $F-Z$ 条边中.

考虑 R 为常数级别的缓存方案, 先前的构造中 F 皆为 K 的指数函数级别, F 的数量级是否可以降低? 若构造 F 为 K 的线性级别, $R=\frac{S}{F}$ 为常数级别的缓存方案, 则对应的超图顶点数目为 $F+K+S=\Theta(K)$ 而边数 $K(F-Z)=\Theta(K^2)$. 然而由极值超图理论中 Ruzsa 和 Szeméredi 著名的 $(6,3)$ 定理 [96] 可知, n 个顶点上无 $(6,3)$ 结构的线性 3 一致 3 超图的边数为 $o(n^2)$. 因此, Shangguan 等 [100] 由超图角度说明 F 不可能是 K 的线性级别, 并进一步给出下述两个构造, 使 F 可取到 K 的次指数级别.

构造 I 设 n、a 和 b 为正整数, 且 $n \geqslant a+b$. 记 $\binom{[n]}{a} = \{A \subseteq [n] : |A| = a\}$ 为 $[n]$ 的所有大小为 a 的子集. 构造 3 一致 3 部超图 $\mathcal{H}_{\mathrm{I}}$ 如下. 顶点集分为 V_1、V_2 和 V_3 三部, 其中, $V_1 = \binom{[n]}{a}$, $V_2 = \binom{[n]}{b}$, $V_3 = \binom{[n]}{a+b}$. $\{A,B,C\} \in E(\mathcal{H}_{\mathrm{I}})$, $A \in V_1$, $B \in V_2$, $C \in V_3$ 当且仅当 $A \cup B = C$. 此构造可推导出一个 $\binom{a+b}{a}$- 正则的 $(\binom{n}{b}, \binom{n}{a}, \binom{n}{a} - \binom{n-b}{a}, \binom{n}{a+b})$-PDA.

构造 II 设 q、m 和 t 为正整数, 且 $q \geqslant 2$, $m \geqslant t$. 记 $\mathbb{Z}_q = \{0,1,\ldots,q-1\}$. 构造 3 一致 3 部超图 $\mathcal{H}_{\mathrm{II}}$ 如下: 顶点集分为 W_1、W_2 和 W_3 三部, 其中, $W_1 = \{(a_1,a_2,\ldots,a_m) : a_i \in \mathbb{Z}_q\}$, $W_2 = \{(\delta_1, \delta_2,\ldots,\delta_t,b_{\delta_1},b_{\delta_2},\ldots,b_{\delta_t}) : 1 \leqslant \delta_1 < \delta_2 < \cdots < \delta_t \leqslant m, b_{\delta_i} \in \mathbb{Z}_q\}$, $W_3 = \{(c_1,c_2,\ldots,c_m,c_{m+1},c_{m+2},\ldots, c_{m+t}) : c_i \in \mathbb{Z}_q, c_{m+j} \in \mathbb{Z}_q \setminus \{q-1\}, 1 \leqslant i \leqslant m, 1 \leqslant j \leqslant t\}$. $\{A,B,C\} \in E(\mathcal{H}_{\mathrm{II}})$, $A \in W_1$, $B \in W_2$, $C \in W_3$ 当且仅当以下条件同时成立 (运算在模 q 的意义下):

- $a_i = c_i$, $i \notin \{\delta_1,\delta_2,\ldots,\delta_t\}$, $1 \leqslant i \leqslant m$;
- $a_{\delta_j} = c_{\delta_j} + c_{m+j} + 1$, $j \in [t]$;
- $b_{\delta_j} = b_{\delta_j}$, $j \in [t]$.

此构造可推导出一个 $\binom{m}{t}$- 正则的 $(\binom{m}{t}q^t, q^m, q^m - q^{m-t}(q-1)^t, q^m(q-1)^t)$-PDA.

4.2.2 利用二部图的强边染色构造 PDA

本小节从二部图强边染色的角度研究 PDA.

定义 4.4 (强边染色) 在图 G 的一个边染色中, 若任意颜色的边所关联的所有顶点诱导的子图中只有这种颜色, 则称此染色为图 G 的一个强边染色. 换言之, 对任意同色的两条边 $\{a,b\}$ 和 $\{c,d\}$, 图中无 $\{a,c\}$、$\{a,d\}$、$\{b,c\}$ 和 $\{b,d\}$ 这些边. 图 G 的强边染色所需的最少颜色数目称为图 G 的强染色数.

设 G 是一个二部图, 顶点分为 X 和 Y 两部, $C = \{c_1,c_2,\ldots,c_t\}$ 是 G 的一个强边染色的颜色集. 可定义 3 一致 3 部超图 $\mathcal{H}$ 如下: 超图的三部顶点分别为 X、Y 和 C, $x \in X$, $y \in Y$, $c \in C$ 之间连边当且仅当图 G 中 $\{x,y\}$ 这条边颜色为 c. 按这种方式, 二部图的强边染色与无 $(6,3)$ 结构的线性 3 一致 3 部超图之间可以自然转化, 进而与 PDA 密切相关. 文献 [100] 从这一角度给出下述定理.

定理 4.2 设 G 是一个二部图, 顶点分为 X 和 Y 两部, C 是其强边染色的颜色集. 则有

- 如果 Y 中的顶点是 d- 正则的, 则 G 的强边染色可诱导出一个 $(|Y|, |X|, |X|-d, |C|)$-PDA.
- 对每个颜色 $c \in C$, 用 r_c 表示 G 中颜色为 c 的边的数目, 记 $r = \min_{c \in C} r_c$, 则 G 的强边染色可诱导出一个 $(|C|, |X|, |X|-r, |Y|)$-PDA.

Yan 等 [129] 通过构造特殊的二部图上的强边染色, 给出了下述 PDA.

构造 III 设 G 是一个二部图, 顶点分为 X 和 Y 两部, C 是其强边染色的颜色集. 令顶点集 $X = \binom{[m]}{a}$, $Y = \binom{[m]}{b}$. $A \in X$ 与 $B \in Y$ 连边当且仅当 $|A \cap B| = \lambda$. 从而 X 中的顶点是 $\binom{a}{\lambda}\binom{m-\lambda}{b-\lambda}$- 正则的. 分别考虑以下两种强边染色方案:

- 对于任意两个不相交的集合 $D, I \subset [m]$, $|D| = a+b-2\lambda$, $|I| = \lambda$, 下述边染相同的颜色:

$$E_{D,I} = \{\{A,B\} \in E(G) : A \setminus B \cup B \setminus A = D, A \cap B = I\},$$

从而 G 的强边染色需要 $\binom{m}{a+b-2\lambda}\binom{m-a-b+2\lambda}{\lambda}$ 种颜色.

- 对于任意两个不相交的集合 $U, V \subset [m]$, 其中 $|U| = a-\lambda$, $|V| = b-\lambda$, 下述边染相同的颜色:

$$E^{U,V} = \{(A,B) \in E(G) : A \setminus B = U, B \setminus A = V\},$$

从而 G 的强边染色需要 $\binom{m}{a+b-2\lambda}\binom{a+b-2\lambda}{a-\lambda}$ 种颜色.

针对不同参数, 选取色数更少的方案, 可得到下述参数的 PDA. 对于任意 $m,a,b,\lambda\in\mathbb{N}^+$, 其中 $0<a,b<m$, $0\leqslant\lambda\leqslant\min\{a,b\}$, 存在 $g-(K,F,Z,S)-$PDA, 其中, $K=\binom{m}{a}$, $F=\binom{m}{b}$, $Z=\binom{m}{b}-\binom{a}{\lambda}\binom{m-a}{b-\lambda}$, $S=\binom{m}{a+b-2\lambda}\cdot\min\{\binom{m-a-b+2\lambda}{\lambda},\binom{a+b-2\lambda}{a-\lambda}\}$, $g=\max\{\binom{a+b-2\lambda}{a-\lambda},\binom{m-a-b+2\lambda}{\lambda}\}$.

4.2.3 利用 Ruzsa-Szeméredi 图构造 PDA

定义 4.5 (Ruzsa-Szeméredi 图) 设 G 是一个二部图. 如果 G 的边集可以表示为 t 个不相交的诱导匹配 $M_1,M_2,\ldots,M_t$ 的并, 且 $\sum_{i=i}^{t}|M_i|=tr$, 则称 G 是一个 (r,t)-Ruzsa-Szeméredi 图.

注意到对 Ruzsa-Szeméredi 图的不相交的诱导匹配的划分自然地定义其一种强边染色. 文献 [100] 给出下述观察.

定理 4.3 设 X 和 Y 是 (r,t)-Ruzsa-Szeméredi 图 G 的两部, $|M_1|=|M_2|=\cdots=|M_t|=r$, 则可诱导出一个 $(t,|X|,|X|-r,|Y|)$-PDA.

在文献 [100] 之前, 文献 [102] 利用最小度至少为 $(1-\frac{M}{N})K$ 的 (r,t)-Ruzsa-Szeméredi 图给出了如下 (K,M,N) 编码缓存方案, 且传输率为 $R=\frac{t}{K}$.

(1) 放置阶段: 将所有文件平均分为 $F=K$ 份, 对不在 G 中的边 $(i,j)\notin E(G)$, 将所有文件的第 i 份放置到第 j 个用户的缓存中, 同时也将所有文件的第 j 份放置到第 i 个用户的缓存中.

(2) 分发阶段: 记 $r_i=|M_i|$, 设 M_i 由以下 r_i 条边组成: $(i_1,i_2),(i_3,i_4),\ldots,(i_{2r_i-1},i_{2r_i})$. 记用户 i 请求的文件为 W_{d_i}, 则中心服务器将发送如下内容给所有的用户:

$$\bigoplus_{k=1}^{r_i}W_{d_{i_{2k}},i_{2k-1}}\oplus W_{d_{i_{2k-1}},i_{2k}},\quad 1\leqslant i\leqslant t.$$

与之前类似, 每个 $i_1,i_2,\ldots,i_{2k}$ 中的用户在上式中仅不知道其需求文件的一个子包, 由此通过将自己缓存的其他相关子包与上述传输内容进行 XOR (exclusive or) 运算后即可得需求文件的子包.

文献 [102] 借助 Alon 等 [4] 构造的如下稠密 Ruzsa-Szeméredi 图, 给出了分包数为 K 线性级别而传输率为 K 多项式级别的编码缓存方案.

定义 4.6 设 C 是正整数, n 是偶数且 $n\geqslant 2C$. 定义图 $G(V,E)$ 如下: $V=[C]^n$, $|V|=K=C^n$. 设 x 和 y 均匀采样于 V, 令 $\mu=\mathbb{E}_{x,y}[\|x-y\|_2^2]$. 对 V 中两点 u 和 v, $(u,v)\in E$ 当且仅当 $|\|u-v\|_2^2-\mu|<n$.

文献 [4] 证明了上述定义的图 G 是 (r,t)-Ruzsa-Szeméredi 图, 其中顶点个数为 $K=C^n$, 边集可以划分为 $t=K^{1+2\frac{\ln 10.5}{\ln C}+o(1)}$ 个不相交的诱导匹配, 且相较于完全图最多缺失 $K^{2-\frac{1}{2C^4\ln C}+o(1)}$ 条边. 文献 [102] 进一步证明了该图每个点度数至少为 $K-2K^{1-\frac{1}{2C^4\ln C}}$. 由此得到 $R=K^{2\frac{\ln 10.5}{\ln C}+o(1)}$, $F=K$ 的 (K,M,N) 编码缓存方案, 其中, $\frac{M}{N}\geqslant 2K^{-\frac{1}{2C^4\ln C}}$, $K=C^n$, $n\geqslant 2C$ 为偶数. 虽然该传输量不是常数, 但当 C 足够大时, $2\frac{\ln 10.5}{\ln C}$ 将落入 $(0,1)$ 之中, 即该缓存方案的分包数是 K 的线性级别, 传输量是指数接近 0 的 K 的多项式级别.

4.3 利用组合设计构造 PDA

文献 [1] 提出了一类 PDA 的构造方法, 从二元矩阵出发, 寻找其最小的单位子矩阵覆盖.

定义 4.7 (二元矩阵的单位子矩阵覆盖) 设矩阵 C 是 $F\times K$ 的二元矩阵, 且矩阵每列中 1 的数目为 Z, 其中行标对应于各文件的分包, 列标对应于每个用户. 令 $\mathcal{C}=\{C_1,C_2,\ldots,C_S\}$ 为 C 的一簇子矩阵, 其中每个 C_i 可通过行列的置换转化为单位矩阵. 若 C 的每一个取值为 1 的项至少出现在一个 C_i 中, 则称 $\mathcal{C}$ 是 C 的单位子矩阵覆盖.

当存在单位子矩阵覆盖 $\mathcal{C}$ 时, 通过将二元矩阵 C 中的 0 替换为 $*$, 将二元矩阵 C 中的每个 1 替换为任意的覆盖此项的子矩阵指标 i, 即可将 C 转化为 (K, F, Z, S)-PDA.

一个设计的关联矩阵中, 行标对应顶点, 列标对应区组. 特定组合设计的关联矩阵每行 1 的数目相等, 该矩阵的转置自然可用于上述思路, 由于覆盖该二元矩阵的单位子矩阵是方阵且可变换为单位阵, 因此直接考虑对该关联矩阵进行覆盖即可. 寻找满足上述条件的特定组合设计并寻找其使参数 S 最小化的单位子矩阵覆盖, 即可得到一系列新的 PDA. 文献 [1] 利用这一思路, 从 $(v, k, 1)$-BIBD (balanced incomplete block design)、对称 $(v, k, 2)$-BIBD、t-$(v, k, 1)$ 设计以及 $\lambda = 1$ 的横截设计 $TD(k, n)$ 等结构出发构造了一系列 PDA 和编码缓存方案. 限于篇幅, 仅以 $(v, k, 1)$-BIBD 为例介绍其单位子矩阵覆盖方法.

设 $(X, \mathcal{A})$ 为 $(v, k, 1)$-BIBD, 对于任意 $x \in X$, 记 $\mathcal{B}_x = \{A_{x_1}, A_{x_2}, \ldots, A_{x_r}\}$, 即所有 $r = \frac{v-1}{k-1}$ 个包含 x 的区组. 对于每个 A_{x_i}, 将其内部元素按整数大小排序, 若 x 为区组 A_{x_i} 中第 j_i 小的元素, 则记为 $A_{x_i}(j_i) = x$.

定理 4.4 在 $(X, \mathcal{A})$ 的关联矩阵 C 中, 对每个 $x \in X$ 定义如下子矩阵 C_x. C_x 的列标对应于 $\mathcal{B}_x$, C_x 的行标对应于 $\{A_{x_i}(j_i + 1 \pmod k)\}$. 则 C_x 是 $r \times r$ 置换矩阵. $\{C_x : x \in X\}$ 构成 C 的一个单位子矩阵覆盖.

利用 $(v, k, 1)$-BIBD 的上述单位子矩阵覆盖可得到用户数目为 v、传输率为 $\frac{k(k-1)}{v-1}$、分包数为 $\frac{v(v-1)}{k(k-1)}$ 的缓存方案. 更多组合设计结构的单位子矩阵覆盖参见文献 [1]. 要说明的是, 当设计的参数 λ 较小时, 导出的方案需要的缓存较大. 沿这一思路, 更值得考虑的是 λ 较大的设计中的单位子矩阵覆盖问题. 此外, 组合设计与 PDA 和缓存之间还有许多其他联系. 例如, 文献 [114] 利用由带特定性质的线性码推导出的可分解设计构造编码缓存方案.

4.4 新的结果

本小节首先给出 PDA 的一种新的递归构造, 借助超图乘法利用两个已知 PDA 构造新的 PDA.

定理 4.5 如果 (K_1, F_1, Z_1, S_1)-PDA 和 (K_2, F_2, Z_2, S_2)-PDA 存在, 则可以得到 $(K_1K_2, F_1F_2, F_1F_2 - (F_1 - Z_1)(F_2 - Z_2), S_1S_2)$-PDA.

证明 记 (K_1, F_1, Z_1, S_1)-PDA 为阵列 $\boldsymbol{P}^{(1)}$, (K_2, F_2, Z_2, S_2)-PDA 为阵列 $\boldsymbol{P}^{(2)}$, 两个阵列分别用线性 3 一致 3 部超图 $\mathcal{H}_1$ 和 $\mathcal{H}_2$ 表示, 其中 $\mathcal{H}_t$ 的顶点集分为 $\mathcal{F}_t$、$\mathcal{K}_t$ 和 $\mathcal{S}_t$ 三部, $\{i_t, j_t, s_t\}$ $(i_t \in \mathcal{F}_t)$, $j_t \in \mathcal{K}_t$ $(s_t \in \mathcal{S}_t)$ 形成一条边当且仅当 $\boldsymbol{P}^{(t)}_{i_t, j_t} = s_t$ $(t \in \{1, 2\})$.

定义超图的乘积 $\mathcal{H} = \mathcal{H}_1 \times \mathcal{H}_2$, $\mathcal{H}$ 的顶点集定义分为 $\mathcal{F}$、$\mathcal{K}$ 和 $\mathcal{S}$ 三部, 其中 $\mathcal{F}$ 为 $\mathcal{F}_1$ 与 $\mathcal{F}_2$ 的 Cartesian 积, $\mathcal{K}$ 和 $\mathcal{S}$ 的定义同理. $\mathcal{H}$ 的边集为 $E(\mathcal{H}) = \{\{(i_1, i_2), (j_1, j_2), (s_1, s_2)\} : \{i_t, j_t, s_t\} \in E(\mathcal{H}_t), t = 1, 2\}$. 记 $\mathcal{H}$ 对应的阵列为 $\boldsymbol{P}$, 由构造知 $\boldsymbol{P}$ 有 F_1F_2 行和 K_1K_2 列. 下面说明 $\boldsymbol{P}$ 为 $(K_1K_2, F_1F_2, F_1F_2 - (F_1 - Z_1)(F_2 - Z_2), S_1S_2)$-PDA, 依次验证 PDA 定义中的 3 个性质.

• 要证每列 $*$ 出现次数一样, 只需证每列非 $*$ 的形如 (s_1, s_2) 的数对出现次数一样. 考虑列标为 (j_1, j_2) 的列, 在 (i_1, i_2) 行的项非 $*$ 当且仅当 $\mathcal{H}_t$ 的第 i_t 行第 j_t 列的项非 $*$, $t = 1, 2$. 符合要求的 i_t 的数目为 $F_t - Z_t$. 因此每列非 $*$ 的项共有 $(F_1 - Z_1)(F_2 - Z_2)$ 个, 而余下的 $F_1F_2 - (F_1 - Z_1)(F_2 - Z_2)$ 项即为 $*$.

• 若点对 (s_1, s_2) 在 $\boldsymbol{P}$ 某列出现两次, 即 $\mathcal{H}$ 中有 $\{(i_1, i_2), (j_1, j_2), (s_1, s_2)\}$ 和 $\{(i'_1, i'_2), (j_1, j_2), (s_1, s_2)\}$ 两条超边, 则导致 $\mathcal{H}_1$ 中存在超边 $\{i_1, j_1, s_1\}$ 和 $\{i'_1, j_1, s_1\}$, 这与 $\boldsymbol{P}^{(1)}$ 的 PDA 性质矛盾. 于是任意一个数对在 $\boldsymbol{P}$ 的任意一列至多出现一次. 对于行同理可证.

• 最后需验证当 $\boldsymbol{P}_{(i_1,i_2),(j_1,j_2)}=\boldsymbol{P}_{(i_1',i_2'),(j_1',j_2')}=(s_1,s_2)$ 时, $\boldsymbol{P}_{(i_1',i_2'),(j_1,j_2)}=\boldsymbol{P}_{(i_1,i_2),(j_1',j_2')}=*$. 因 $\mathcal{H}_1$ 中存在超边 $\{i_1,j_1,s_1\}$ 和 $\{i_1',j_1',s_1\}$, 所以 $\boldsymbol{P}^{(1)}_{i_1,j_1'}=\boldsymbol{P}^{(1)}_{i_1',j_1}=*$, 于是 $\boldsymbol{P}_{(i_1',i_2'),(j_1,j_2)}$ 和 $\boldsymbol{P}_{(i_1,i_2),(j_1',j_2')}$ 两个项无法定义为任何数对, 即这两项为 $*$.

综上可知, $\boldsymbol{P}$ 是 $(K_1K_2,F_1F_2,F_1F_2-(F_1-Z_1)(F_2-Z_2),S_1S_2)$-PDA. □

当前大多已知的 PDA 中 F 随 K 呈指数型增长, 上述构造的 PDA 的优点是可使分包数 F 的增长相对变缓, 由小型 PDA 递归构造得到的新 PDA 有时能构造出具有更小分包数的方案. 在寻找较小分包数的 PDA 方面, 由正交拉丁方的奇异间接积 (singular indirect product) 方法启发得到的构造也具有较好的表现.

定理 4.6 如果 (K_1,F_1,Z_1,S_1)-PDA 和 (K_2,F_2,Z_2,S_2)-PDA 存在, 且 (K_1,F_1,Z_1,S_1)-PDA 阵列的部分行可以构成参数为 (K_1,F_1',Z_1',S_1') 的 PDA, 则存在 $(K_1K_2,F_1'F_2+F_1-F_1',F_1'Z_2+(F_2-Z_2)Z_1'+Z_1-Z_1',S_1\cdot\max\{S_2,K_2\})$-PDA.

证明 设 s 是正整数或 $*$, $A=(a_{i,j})$ 是 $m\times n$ 的矩阵, 定义符号 $(s,A)=((s,a_{i,j}))_{m\times n}$, 其中 $(s,a_{i,j})=*$, 如果 s 与 $a_{i,j}$ 中至少有一个为 $*$.

设 (K_1,F_1,Z_1,S_1)-PDA 对应阵列为 $\boldsymbol{P}^{(1)}$, (K_2,F_2,Z_2,S_2)-PDA 对应阵列为 $\boldsymbol{P}^{(2)}=(p^{(2)}_{i,j})_{K_2\times F_2}$. $\boldsymbol{P}^{(1)}$ 可记作 $\boldsymbol{P}^{(1)}=\binom{\boldsymbol{P}^{(1')}}{\boldsymbol{P}^{(1'')}}$, 上下两部分皆为 PDA 且 $\boldsymbol{P}^{(1')}$ 对应参数为 (K_1,F_1',Z_1',S_1').

记 $\boldsymbol{P}'=(\boldsymbol{P}'_{i,j})_{F_2\times K_2}$, 其中 $\boldsymbol{P}'_{i,j}=(p^{(2)}_{i,j},\boldsymbol{P}^{(1')})$. 记 $\boldsymbol{P}''=((1,\boldsymbol{P}^{(1'')}),(2,\boldsymbol{P}^{(1'')}),\dots,(K_2,\boldsymbol{P}^{(1'')}))$. 定义 $\boldsymbol{P}=\binom{\boldsymbol{P}'}{\boldsymbol{P}''}=(p_{(i_1,i_2),(j_1,j_2)})$, 当 $i_1\leqslant K_2$ 时, 记号 $p_{(i_1,i_2),(j_1,j_2)}$ 表示 $\boldsymbol{P}'_{i_1,j_1}$ 的第 i_2 行第 j_2 列的元素, 当 $i_1=K_2+1$ 时, 该记号表示 $\boldsymbol{P}''$ 中 $(j_1,\boldsymbol{P}^{(1'')})$ 的第 i_2 行第 j_2 列的元素. 由构造知 $\boldsymbol{P}$ 有 $F_1'F_2+(F_1-F_1')$ 行和 K_1K_2 列, 且元素取自 $\mathcal{S}=\{(s_1,s_2):s_1\in[\max\{S_2,K_2\}],s_2\in[S_1]\}$. 下面证明 $\boldsymbol{P}$ 也是 PDA, 且参数为 $(K_1K_2,F_1'F_2+(F_1-F_1'),F_1'Z_2+(F_2-Z_2)Z_1'+Z_1-Z_1',S_1\max\{S_2,K_2\})$.

假设 A 是一个 PDA, 由定义知, 当 s 是正整数时, (s,A) 是 PDA, 且 $*$ 的坐标与 A 保持一致; 当 s 是 $*$ 时, (s,A) 是全 $*$ 矩阵, 也是 PDA. 由此可知, 对于任意正整数 s, $(s,\boldsymbol{P}^{(1)})$ 与 $\boldsymbol{P}''$ 是 PDA, $\boldsymbol{P}'$ 的每个子块也是 PDA.

• 因为 $\boldsymbol{P}^{(2)}$ 是 PDA, 其每列 $*$ 的个数相同, 将 $\boldsymbol{P}'$ 视为 $F_2\times K_2$ 的分块矩阵时, 每个子列全 $*$ 子块个数相同, 为 Z_2 个, 相应的非全 $*$ 的 PDA 子块个数也相同, 为 F_2-Z_2 个. 从而, $\boldsymbol{P}'$ 视为 $F_1'F_2\times K_1K_2$ 的矩阵时, 其每列 $*$ 的个数相同, 为 $F_1'Z_2+(F_2-Z_2)Z_1'$. 已证得 $\boldsymbol{P}''$ 是 PDA, 其每列 $*$ 的个数相同, 为 Z_1-Z_1'. 综上可知, $\boldsymbol{P}$ 每列 $*$ 的个数相同且为 $F_1'Z_2+(F_2-Z_2)Z_1'+Z_1-Z_1'$.

• 将 $\boldsymbol{P}'$ 视为 $F_2\times K_2$ 的分块矩阵时, 每个子块是 PDA, 又因为 $\boldsymbol{P}^{(2)}$ 是 PDA, 则每个子列任意两个子块的非 $*$ 元素对相交为空, 从而 $\boldsymbol{P}'$ 每列中非 $*$ 元素对至多出现一次. 同理对每行也成立, 即 $\boldsymbol{P}$ 的元素对在每行至多出现一次. 考察 $\boldsymbol{P}$ 的第 j 个子列, 该子列前 F_2 个子块来自 $\boldsymbol{P}'$ 的第 j 子列, 最后一个子块为 $(j,\boldsymbol{P}^{(1'')})$. 如果 $j\neq P^{(2)}_{i,j}$, $i\in[F_2]$, 则该子列任意两个子块的非 $*$ 元素相交为空, 否则前 F_2 个子块中包含子块 $(j,\boldsymbol{P}^{(1')})$, 已证得 $(j,\boldsymbol{P}^{(1)})$ 是 PDA, 其每列非 $*$ 元素对无重复, 从而 $\boldsymbol{P}$ 的元素对在每列也至多出现一次.

• 考虑某固定的元素对 (s_1,s_2) 在 $\boldsymbol{P}$ 的出现情形. 如果在某个子块 $(s_1,\boldsymbol{P}^{(1)'})$ 或 $(s_1,\boldsymbol{P}^{(1)''})$ 中出现至少两次, 由这两个子块是 PDA 知该元素对的交叉项位置均为 $*$. 如果该元素对分别出现在两个不同的子块中, 将有两种情形出现: 这两个子块均来自 $\boldsymbol{P}'$ 或一个来自 $\boldsymbol{P}'$ 另一个来自 $\boldsymbol{P}''$. 因为 $\boldsymbol{P}''$ 中任意两个子块的元素不相交, 故不会出现两个子块均来自 $\boldsymbol{P}''$ 的情形. 考虑第一种情形, 注意到这两个子块的第一个元素为 s_1, 则均可用 $(s_1,\boldsymbol{P}^{(1)'})$ 表示, 由于 $\boldsymbol{P}^{(2)}$ 是 PDA, 因此这两个子块交叉位置的子块为全 $*$ 子块, 即元素对 (s_1,s_2) 出现位置的交叉位置元素为 $*$. 考虑第二种情形, 如果这两个

子块来自 $\boldsymbol{P}$ 的第 s_1 个子列, 那么其可以构成阵列 $(s_1, \boldsymbol{P}^{(1)})$, 由于该阵列是 PDA, 则两个 (s_1, s_2) 的交叉位置为 $*$; 如果这两个子块来自不同子列, 不妨设 $p_{(i_1,i_2),(j_1,j_2)} = p_{(K_2+1,i_2'),(s_1,j_2')} = (s_1, s_2)$, 需证 $p_{(K_2+1,i_2'),(j_1,j_2)} = p_{(i_1,i_2),(s_1,j_2')} = *$. 考虑 $p_{(K_2+1,i_2'),(j_1,j_2)}$, 由定义可知 $p_{(K_2+1,i_2'),(j_1,j_2')}$ 的第二个元素与 $p_{(K_2+1,i_2'),(s_1,j_2')}$ 的一致, 均为 s_2. 同时 p_{i_1,j_1} 与 p_{K_2+1,j_1} 构成的阵列中 $*$ 位置与 $\boldsymbol{P}^{(1)}$ 保持一致. 因此 $p_{(K_2+1,i_2'),(j_1,j_2)} = *$. 同理可得 $p_{(i_1,i_2),(s_1,j_2')} = *$.

综上可知, $\boldsymbol{P}$ 是 $(K_1K_2, F_1'F_2 + (F_1 - F_1'), F_1'Z_2 + (F_2 - Z_2)Z_1' + Z_1 - Z_1', S_1 \max\{S_2, K_2\})$-PDA. □

5 分布式计算

5.1 研究现状

分布式计算 (distributed computing) 将大规模数据计算任务拆分成多个小任务, 并分发给多个数据处理终端进行运算, 通过回收各终端返回的运算结果再统一整合得到原任务的计算结果. 分布式计算面临着数据传输量大、算力浪费、掉队者、数据安全等各方面的挑战, 编码技术在其中可起到一定作用.

MapReduce 模型是分布式框架中的经典编程范式, 由谷歌公司于 2004 年提出, 可应用于大规模数据集并行运算 [38]. 下面介绍 MapReduce 的数学模型并结合例子说明其含义.

考虑一个计算任务, 涉及 K 个分布式计算节点, N 个输入数据 $W_1, W_2, \ldots, W_N$ 和 Q 个输出函数 $\{\phi_q : 1 \leqslant q \leqslant Q\}$, 其中每个输出函数 ϕ_q 将输入数据映射为 $u_q = \phi_q(W_1, W_2, \ldots, W_N)$. 假设每个 ϕ_q 都可以被分解成如下形式:

$$\phi_q(W_1, W_2, \ldots, W_N) = h_q(g_{q,1}(W_1), g_{q,2}(W_2), \ldots, g_{q,N}(W_N)),$$

其中函数 $g_{q,n}$ 称为映射函数, 它将数据 W_n 转换为中间值 $v_{q,n} := g_{q,n}(W_n)$; 函数 h_q 称为归约函数, 它将中间值 $\{v_{q,n}\}_{n\in[N]}$ 映射为输出值 $u_q = h_q(v_{q,1}, v_{q,2}, \ldots, v_{q,N})$. 例如, 假设每个 W_i 是非常庞大的文本文件, 每个 ϕ_q 要统计所有文件中某特定的第 q 个关键词的出现次数. ϕ_q 的计算过程可分解为先统计第 n 个文件中第 q 个关键词的出现次数 $g_{q,n}$, 再利用 h_q 函数将 $\{g_{q,n}(W_n) : 1 \leqslant n \leqslant N\}$ 累加.

当前对 MapReduce 框架的分析一般分映射、数据洗牌和归约三个阶段, 每个阶段详情如下.

映射阶段 (map phase): 中央控制节点进行数据分发, 每个计算节点得到数据 $\mathcal{W}_k \subseteq \{W_1, W_2, \ldots, W_N\}$. 中央控制节点也将归约函数分发至各计算节点, 即事先将最终的 "汇总" 任务进行分发. 同时, 中央控制节点还将映射函数分发给各计算节点, 每个计算节点 k 需要首先完成各映射函数及其对应数据的计算, 得到部分中间值 $\mathcal{C}_k \subseteq \{v_{q,n} : q \in [Q], W_n \in \mathcal{W}_k\}$.

数据洗牌阶段 (data shuffling): 被分配了归约函数计算任务的计算节点往往需要来自其他计算节点的中间值的辅助, 因此各计算节点之间需要一定的数据交互. 每个节点 k 将其得到的中间值 $\mathcal{C}_k$ 进行编码处理, 生成一个长度等同于 ℓ_k 个中间值大小的信息 $X_k = \varphi_k(\mathcal{C}_k)$, 以广播形式传达至其他计算节点.

归约阶段 (reduce phase): 每个被分配了归约函数计算任务的节点 $k \in [K]$, 通过对部分广播信息进行解码, 得到自身所需的中间值, 再结合自己在映射阶段已计算得到的部分中间值, 完成归约函数的计算, 并将最终结果反馈给中央控制节点.

继续以文本关键词统计为例解释上述三个阶段. 假设有 $K = 3$ 个计算节点和 $N = 3$ 个庞大的文本文件 W_1、W_2 和 W_3, 需统计三个关键词的数目 $\phi_p(W_1, W_2, W_3)$、$\phi_q(W_1, W_2, W_3)$ 和 $\phi_r(W_1, W_2, W_3)$. 中

央控制节点按下述规则分配文件给每个计算节点: $\mathcal{W}_1=\{W_1,W_2\}$, $\mathcal{W}_2=\{W_2,W_3\}$, $\mathcal{W}_3=\{W_1,W_3\}$, 同时也将三个归约任务 h_p、h_q 和 h_r 依次分配给三个计算节点. 在映射阶段, 每个计算节点计算的中间值[1)] 依次为 $\mathcal{C}_1=\{v_{p,1},v_{p,2},v_{q,1},v_{r,2}\}$, $\mathcal{C}_2=\{v_{p,3},v_{q,2},v_{q,3},v_{r,2}\}$, $\mathcal{C}_3=\{v_{p,3},v_{q,1},v_{r,1},v_{r,3}\}$. 在数据洗牌阶段, 每个中间值转化为二元序列并分拆为两部分, $v_{x,n}=(v_{x,n}^{(1)},v_{x,n}^{(2)})$, $x\in\{p,q,r\}$, $n\in\{1,2,3\}$. 第 1 个计算节点广播 $v_{q,1}^{(1)}+v_{r,2}^{(1)}$, 第 2 个计算节点广播 $v_{p,3}^{(1)}+v_{r,2}^{(2)}$, 第 3 个计算节点广播 $v_{p,3}^{(2)}+v_{q,1}^{(2)}$. 在归约阶段, 第 1 个计算节点自身已知 $v_{p,1}$ 和 $v_{p,2}$, 从广播内容中可译码得到 $v_{p,3}^{(1)}$ 和 $v_{p,3}^{(2)}$ 进而合并为 $v_{p,3}$, 则可完成归约函数 $h_p(v_{p,1},v_{p,2},v_{p,3})$ 的计算. 另两个计算节点同理.

衡量 MapReduce 模型表现主要参数有两个. 其一是计算负载 $r=\frac{\sum_{k=1}^{K}\mathcal{W}_k}{N}$, 它意味着平均每个输入数据被分配给 r 个计算节点. 记 K 个计算节点、N 个输入数据、Q 个输出函数且计算负载为 r 的 MapReduce 方案为 (K,Q,r,N)-MapReduce 方案. 其二是传输负载 $L=\frac{\sum_{k=1}^{K}\ell_k}{NQ}$, 它表示数据洗牌过程中传输数据总量与全部中间值的数据量的比值.

计算负载和传输负载两个参数之间有着天然的制约关系. 若计算负载为 r, 则意味着每个计算节点平均持有 $\frac{Nr}{K}$ 个数据, 欲完成单个归约函数的计算时缺失了 $N-\frac{Nr}{K}$ 个中间值. 按最平凡的数据洗牌思路, 将每个计算节点缺失的中间值依次广播, 传输负载将达到 $L=\frac{Q(N-\frac{Nr}{K})}{QN}=1-\frac{r}{K}$. 这样的数据洗牌方式在 MapReduce 的具体实现中限制了整体效率. Chowdhury 等 [33] 观察到在 Facebook 的 Hadoop 集群中数据洗牌阶段平均占整体运行时间的 33%. Li 等 [76] 论证了数据洗牌阶段可通过编码方式压缩广播内容, 给出了计算负载和传输负载间的权衡, 当计算负载为 r 时, 理论最优传输负载为 $\frac{1}{r}(1-\frac{r}{K})$, 是非编码时的 $\frac{1}{r}$. 例如, 在前文中的例子中, 编码方法将传输负载由平凡的 $\frac{1}{3}$ 降低为 $\frac{1}{6}$.

迄今为止, 达到理论传输负载最优值的方案仅在 $\binom{K}{r}\mid N$ 时得以实现. 当整除性无法满足时, 组合方法在分布式计算方案的探索中发挥了重要作用. 基于组合设计 [68,124] 和 PDA 方法 [61,93,130] 等可得到多种参数下的 MapReduce 模型, 相较于非编码方案具有更小的传输负载.

分布式计算除优化 MapReduce 模型数据洗牌过程外, 仍有很多值得研究的课题, 部分课题及其参考文献如下:

• 对抗掉队者的研究: 当一个大型计算任务拆分为多个子任务并分发给多个计算节点时, 计算速度慢或失联的计算节点是阻碍整体计算任务更快完成的主要原因 [37], 这类节点称为掉队者. 对抗掉队者的研究通常取决于具体计算内容, 如大型矩阵乘法和梯度下降算法等. 编码方法的引入通过增加计算冗余尽可能地降低掉队者对整体计算任务的影响. 特别地, 在大型矩阵乘法中运用的多项式编码思想也可以推广用于保护原始矩阵的数据安全. 对抗掉队者问题的核心是寻找计算量和数据传输量尽可能小且编码与解码复杂度低的编码分布式计算方法. 针对大型矩阵乘法的研究可参见文献 [47,54,92,136,137,139], 针对梯度下降算法的研究可参见文献 [26,53,94,113,133].

• 编码的弹性计算: 其产生背景是云服务提供商推出了一种用少于原始费用的价格使用未充分利用的虚拟计算机业务 [7,8]. 该业务的缺陷在于, 当低优先级的计算任务由这类虚拟计算机承担时, 一旦出现高优先级的作业, 机器可能被抢占, 导致低优先级的任务失败, 但相应地, 新的机器也可随时加入计算. 由于虚拟机频繁离开与加入的不可预估性 [86], 传统的立即停止全局任务直到所有机器恢复正常与采取对抗掉队者的策略均失效. 因此需要构建一个弹性运行框架 [34,132], 使离开机器的任务可以无缝地分配给现有机器及新加入机器. 更多内容参见文献 [35,65,125,126].

• 移动边缘计算: 移动边缘计算核心思想, 即通过汇集网络边缘的可用资源, 将计算提供方从云处

1) 每个节点的计算内容由其归约任务及后续数据洗牌阶段决定, 且根据其被分配的文件均可计算出相应的中间值. 注意到一个简单的方案可直接令节点 k 计算 $\mathcal{C}_k=\{v_{p,n},v_{q,n},v_{r,n}:W_n\in\mathcal{W}_k\}$, 即分别统计自身持有的两个文件中三个关键词的数目, 然而这样会造成各计算节点的资源浪费.

理中心转移到更接近数据生成的地方 [57, 82], 回避了远程数据中心在核心网络和回程网络中存在长时间传播延迟和拥塞的缺点 [82]. 在移动边缘计算框架下, 用户将计算任务转移到位于网络边缘的服务器中, 由服务器处理数据并返回结果. 由于边缘计算能支持低延迟和高带宽的计算任务, 其已成为 5G 移动网络的支柱 [57]. 移动边缘计算系统的功能与分布式计算系统类似, 由此两者实践中容易出现的问题也有共通之处, 如掉队者、数据传输时导致的延迟, 用户私密数据的保护及系统鲁棒性的维持等. 更多内容参见文献 [18, 70, 73, 74, 140].

5.2 PDA 在 MapReduce 模型下的应用

文献 [93] 指出, 在第 4 节缓存方案的构造中扮演了重要角色的放置分发阵列 PDA, 也可以用来构建 MapReduce 方案.

定理 5.1 假设存在一个 $(K, N, r, S)(g_1, g_2, \ldots, g_S)$-PDA, 则可以构造出一个参数为 $(K, Q = K, r, N)$ 的编码 MapReduce 方案, 且该方案的数据传输负载为 $L = \frac{1}{NK}\sum_{i=1}^{S}\frac{g_i}{g_i-1}$. 特别地, 如果 $g_i = g$ 对任意 $i \in [S]$ 成立, 则 $L = \frac{1}{g-1}(1-\frac{r}{K})$.

令 $\boldsymbol{P} = (p_{n,k})$ 为 $(K, N, r, S)(g_1, g_2, \ldots, g_S)$-PDA, 阵列的行对应于各输入数据, 列对应于各计算节点. 如果 $p_{n,k} = *$, 则表示数据 W_n 被分配给计算节点 k; 如果 $p_{n,k} = s \in [S]$, 则表示数据 W_n 未被分配给计算节点 k. 设输出函数个数 $Q = K$ (也可推广至 $K \mid Q$, 此时发送方案分成 $\frac{Q}{K}$ 次进行, 每一次完成 $Q = K$ 个函数结果的输出, 过程与下述一致), 每个计算节点 k 可计算其持有数据对应的各中间值 $\{v_{q,n} : q \in [Q], p_{n,k} = *\}$. 设计算节点 k 被分配的归约任务为 h_k, 为使该节点完成归约函数的计算, 尚缺少的中间值为 $\{v_{k,n} : p_{n,k} \neq *\}$.

数据洗牌过程需要完成各节点缺失的中间值的交互, 这个过程可依赖于 PDA 如下构造. 对 PDA 中的任意一项 $s \in [S]$, 记 $K_s = \{k \in [K] : \exists\, n, p_{n,k} = s\}$ 为参加第 s 次数据洗牌过程的节点, 节点数目共 g_s 个. 第 s 次数据洗牌涉及的中间值为 $\{v_{k,n} : k \in K_s, p_{n,k} = s\}$. 每个中间值被均匀分为 $g_s - 1$ 份, 标号方式为 $v_{k,n} = (v_{k,n}^t)_{t \in K_s \setminus \{k\}}$. 第 s 次数据洗牌过程中每个节点 $k \in K_s$ 发送 $\bigoplus_{p_{n,k'}=s, k' \in K_s \setminus \{k\}} v_{k',n}^k$.

首先要说明这个发送是可行的, 这是因为基于 PDA 的第三条性质, 节点 k 拥有所有的中间值 $\{v_{k',n} : p_{n,k'} = s, k' \in K_s \setminus \{k\}\}$. 再说明这个交互过程是有效的, 对于任意 $p_{n,k} = s$, 在节点 k 所缺失的中间值 $v_{k,n} = (v_{k,n}^t)_{t \in K_s \setminus \{k\}}$ 中, 每一部分 $v_{k,n}^t$ 可由计算节点 t 在第 s 次数据洗牌过程发送的 $\bigoplus_{p_{n,k}=s, k \in K_s \setminus \{t\}} v_{k,n}^t$ 中译得. 最后, 不难计算第 s 次数据洗牌过程的数据传输总量等同于 $\frac{g_s}{g_s-1}$ 份大小的中间值. 于是整个方案的传输负载为 $L = \frac{1}{NK}\sum_{i=1}^{S}\frac{g_i}{g_i-1}$.

例 5.1 沿用例 4.1 的 $(K = 4, N = 5, r = 3, S = 3)(g_1 = 3, g_2 = 3, g_3 = 2)$-PDA, 分析其对应的 MapReduce 方案:

$$\begin{pmatrix} 1 & * & * & * \\ * & 1 & * & 3 \\ * & * & 1 & 2 \\ 2 & * & 3 & * \\ * & 2 & * & * \end{pmatrix}.$$

此 PDA 对应的方案中涉及 4 个计算节点和 5 个数据. 以节点 1 为例, 数据 W_2、W_3 和 W_5 被分配给节点 1. 节点 1 所缺失的中间值为 $v_{1,1}$ 和 $v_{1,4}$. 前三个节点共同参与了第一次数据洗牌过程, 他们将中间值 $v_{i,i}$ ($i \in [3]$) 均匀分为两份并标号: $v_{1,1} = (v_{1,1}^2, v_{1,1}^3)$, $v_{2,2} = (v_{2,2}^1, v_{2,2}^3)$, $v_{3,3} = (v_{3,3}^1, v_{3,3}^2)$. 其

中节点 1 发送数据 $v^1_{2,2}+v^1_{3,3}$ 并收到了来自节点 2 的数据 $v^2_{1,1}+v^2_{3,3}$ 和来自节点 3 的数据 $v^3_{1,1}+v^3_{2,2}$. 由于节点 1 已知数据 W_2 和 W_3, 则可译码得到 $v^2_{1,1}$ 和 $v^3_{1,1}$ 的值从而得到整个中间值 $v_{1,1}$. 类似地, 在由节点 1、2 和 4 共同参与的第二次数据洗牌过程中, 节点 1 得到中间值 $v_{1,4}$.

先前的部分 MapReduce 构造 [68, 76] 本质上可视作上述基于 PDA 的构造的特殊情形. 基于 PDA 构造 MapReduce 方案切实可行, 但参数还不够灵活, 尤其需考虑可以达到文献 [76] 给出的计算负载和传输负载最优权衡的参数. 另外, 与基于 PDA 的构造类似, 在编码缓存的构造中利用的完全图覆盖设计的思想也可迁移到 MapReduce 的构造中, 文献 [68] 基于可分解设计的方案便是如此.

5.3 新的结果

在缓存方案的研究中, PDA 阵列中每列的 $*$ 数目一般为定值, 这保证由其推导出的缓存方案中每个缓存空间的大小相同. 而在分布式计算 MapReduce 模型中, 每列的 $*$ 为定值这一限定并不是必要的. 从 PDA 出发, 对行和列的删减, 使余下的阵列仍然保持了 PDA 的第二和三条性质, 依然可推导出对应的 MapReduce 方案. 本小节将证明, 这种操作可推导出达到计算负载和传输负载最优权衡的方案.

定理 5.2 假设存在 $(K,N,r,S)(g_1,g_2,\dots,g_S)$-PDA. 设阵列的某行包含数字 $s_{i_1},s_{i_2},\dots,s_{i_t}$, 则通过删除此行后的阵列, 可以推导出参数为 $(K,Q=K,\frac{rN-K+t}{N-1},N-1)$ 的编码 MapReduce 方案, 且该方案的数据传输负载为

$$L=\frac{t+\sum_{i\in[S]\setminus\{i_1,\dots,i_t\}}\frac{g_i}{g_i-1}}{(N-1)K}.$$

证明 考虑删除一行后的 PDA 所推导出的 MapReduce 方案与原 PDA 所推导出的方案的区别. 若所删除的第 n 行中有某个数字 $p_{n,k}=s$, 则原第 s 次数据洗牌过程中的传输总量等同于 $\frac{g_s}{g_s-1}$ 份大小的中间值. 现将第 s 次数据洗牌过程改为只由计算节点 k 进行广播, 广播内容为 $\bigoplus_{p_{n,k'}=s,k'\in K_s\setminus\{k\}}v_{k',n}$, 即可使得其他 K_s 中的计算节点得到其缺失的中间值, 此时第 s 次数据洗牌过程中的传输总量等同于单位 1 份的中间值, 相较于之前减少了 $\frac{1}{g_s-1}$.

当删除的行包含数字 $s_{i_1},s_{i_2},\dots,s_{i_t}$ 时, 对应的 t 次数据洗牌过程均节省了一定的传输量, 方案的总传输负载即为

$$L=\frac{t+\sum_{i\in[S],i\neq i_1,\dots,i_s}\frac{g_i}{g_i-1}}{(N-1)K}.$$

同时, 方案的计算负载也变为 $\frac{rN-K+t}{N-1}$. 最终得到 $(K,Q=K,r,N-1)$ 的编码 MapReduce 方案. □

文献 [76] 证明了传输负载与计算负载和用户数目之间的权衡, 即固定 r 和 K 时, 最小的传输负载为 $L=\frac{1}{r}(1-\frac{r}{K})$, 但给出的达到该权衡的方案需要满足 $N\mid\binom{K}{r}$ 这一整除性条件.

考虑下述 PDA: 行数为 $N=\binom{K}{r}$, 每行的行标及 $*$ 的取法对应于 $[K]$ 的所有 r 元子集. 对于任意 $[K]$ 的 $r+1$ 元集 A 和任意 $k\in A$, 令 $p_{A\setminus\{k\},k}=s_A$. 这本质上为 Maddah-Ali 和 Niesen [83] 最初的缓存方案所对应的 PDA. 该 PDA 中任意非 $*$ 的元出现 $r+1$ 次, 可推导出参数为 $(K,Q=K,r,N=\binom{K}{r})$ 的编码 MapReduce 方案, 传输负载为 $L=\frac{1}{r}(1-\frac{r}{K})$ 达到最优. 从这个 PDA 出发做定理 5.2 中的操作, 则可在保持计算负载 r 不变的情形下, 减少输入数据 N 的数目, 而仍达到最优传输负载. 事实上, 可以对此 PDA 删减多行, 只要每行的非 $*$ 指标互不相同, 推导出的方案都仍具有最优传输负载. 于是这种方法给出了在不满足整除性条件 $N\mid\binom{K}{r}$ 下的一类达到最优权衡的方案.

6 隐私保护信息检索

在网络生活中, 用户时常需要在某个数据库中检索特定数据. 基于用户检索请求, 检索服务商们可以搜集信息并分析用户个人偏好. 虽然这在某种层面上给用户带来一定便利性, 但暴露了用户的个人隐私. 在检索某些敏感数据时, 用户的隐私迫切需要得到保护.

隐私保护信息检索 (private information retrieval, PIR) 最早由 Chor 等[31,32] 提出, 使得用户可以在保证自己行为隐私的前提下检索特定数据. 最初的 PIR 模型考虑如何在 n 个比特位中检索一个特定比特位的值, 且使服务器无法得知所检索比特位指标的任何信息. 文献 [31,32] 已证明, 若仅有一个服务器且服务器能得知用户所有的查询请求, 则唯一的 (信息论安全意义下的) 解决方案是迫不得已地下载整个数据库. 然而, 在有多个服务器时, 用户的检索需求可以被分拆为若干子需求发送至各个服务器, 其中每个子需求并不会暴露用户行为的隐私, 而用户再综合各服务器的反馈进行解码计算完成检索. 例如, 若有两个服务器同时存储数据库 $\boldsymbol{x}=(x_1,x_2,\ldots,x_n)\in\mathbb{F}_2^n$, 用户可随机选取 $\boldsymbol{a}\in\mathbb{F}_2^n$ 并分别发送问询 $\boldsymbol{a}$ 和 $\boldsymbol{a}+\boldsymbol{e}_i$ 给两个服务器, 其中 $\boldsymbol{e}_i$ 为仅在第 i 位取 1 而其余位取 0 的单位向量. 两个服务器分别反馈 $\boldsymbol{a}\cdot\boldsymbol{x}^{\mathrm{T}}$ 和 $(\boldsymbol{a}+\boldsymbol{e}_i)\cdot\boldsymbol{x}^{\mathrm{T}}$ 这两个比特. 用户将这两个反馈相加得到 x_i 这一比特的值. 由于 $\boldsymbol{a}$ 的随机性, 每个服务器独自无法得知用户所检索文件指标的任何信息.

在 PIR 这一话题从密码学领域提出伊始, 衡量 PIR 方案优劣的主要指标是整个检索过程中涉及的数据传输量, 这既包括用户向服务器传送的检索请求 (上传量), 也包括服务器向用户反馈的数据 (下载量). 上述简单例子并不理想, 因为整个过程涉及的数据传输量为 $2n+2$ (包括了 2 比特的下载和 $2n$ 比特的上传). 之后, 一系列 PIR 方案将数据传输量逐步减小, 当前两个服务器上的 PIR 数据传输量最优值为 Dvir 和 Gopi[41] 给出的 $O(n^{\sqrt{\log\log n/\log n}})$. 在这个研究过程中, PIR 方案与局部可解码 (locally decodable codes) 和密码学中的不经意传输 (oblivious transfer) 等领域密切相关. 有关密码学领域的 PIR 研究的历史与最新进展, 可参见文献 [14,41,43,134,135] 及其中的参考文献.

随着大数据时代的到来, 以纠删码、再生码和局部可修复码为代表的分布式存储系统的研究逐渐兴起, 多个服务器以一定编码形式存储数据. 在这一背景下, 分布式存储系统中的 PIR 方案成为一个新的课题[6,19,27,99]. 分布式存储系统中的 PIR 问题与密码学领域 PIR 问题的研究主要有以下两点区别. 第一, 新模型下考虑如何从 n 个文件中检索一个特定的文件, 文件的大小可以充分大. 在这一设定下, 文献 [27] 指出, 分布式存储系统中 PIR 方案的上传量一般是不依赖于文件大小的常数值, 而下载量则与文件大小成正比, 于是优化目标仅考虑占主导部分的下载量而忽视上传量. 第二, 先前经典的 PIR 问题一般都假设每个服务器存储了完整的信息 (即基于复制存储), 而在分布式存储系统中, 每个服务器可以只存储编码之后的一小部分信息, 于是需要考虑新型的 PIR 方案.

基于以上动机, 分布式存储系统中的 PIR 问题的基本模型如下. 考虑一个由 N 个服务器组成的分布式存储系统, 系统中存储了由 M 个文件组成的数据库, 其中每个文件经由同一个 (N,K)-MDS 码 (极大距离可分码) 存储于各服务器. 用户需要检索其中任意一个文件, 且使得所检索文件的指标信息不会暴露给任意 T 个可合谋的服务器. 这样的 PIR 方案记为一个 $(N,K,T;M)$-PIR 方案. 一个方案的 PIR 码率 R 定义为所检索文件的大小与整个过程中的数据下载量的比值. 在所有可行的 PIR 方案中, PIR 码率的最大值称为 PIR 容量, 记为 $C=C(N,K,T;M)$.

在本方向的奠基性工作中, Sun 和 Jafar[105] 解决了 $K=T=1$ 的情形 (基于复制存储的系统, 服务器之间无合谋), 得到了 $C(N,K=1,T=1;M)=(1+\frac{1}{N}+\cdots+\frac{1}{N^{M-1}})^{-1}$. 进而, 文献 [107] 解决了 $K=1$ 而 $2\leqslant T\leqslant N-1$ 的情形 (T- 合谋 PIR), 文献 [9] 解决了 $T=1$ 而 $2\leqslant K\leqslant N-1$ 的情形 (MDS 编码下的 PIR). 而针对 $K\geqslant 2$ 而 $T\geqslant 2$ 的非退化情形, 文献 [49,106,110,142] 给出了若干可行

方案, 但此时的最优 PIR 容量 (尤其是非线性方案下的) 尚未完整解决. 在最近的文献 [56] 中, 线性方案的最优 PIR 容量已基本解决.

近几年, PIR 这一热点问题有了更多变种. 限于篇幅, 这里只简要介绍其中几类.

• 多文件 PIR: 用户需同时检索 $P \geqslant 2$ 个文件. Banawan 和 Ulukus 最早在文献 [10] 中说明, 存在比直接执行 P 次单文件 PIR 方案更好的解决方法. 他们给出了 $K = T = 1$ 时检索 $P \geqslant \frac{M}{2}$ 个文件的最优方案. 当 $P < \frac{M}{2}$ 时, 他们得到的方案与下界之间也仅有一个很小的差距.

• 带纠删纠错性质的 PIR: 这个问题假设某些服务器无法响应或者反馈中带有错误, 而用户在检索之前并不知晓哪些服务器有故障. 于是, PIR 方案中需设计更多冗余以完成纠删和纠错 (参见文献 [11,111,141]).

• 带有缓存/边际信息的 PIR: 这个方向假设用户提前拥有一定的边际信息, 从而在 PIR 方案的设计中可以利用这些边际信息提高 PIR 码率. 此方向的研究又按照边际信息的形式、是否允许服务器在检索后得知用户的边际信息等附加设定继续细分 (参见文献 [62,112]).

• 非 MDS 编码下的分布式存储系统中的 PIR: 考虑在非 MDS 编码下如何达到与 MDS 编码下相同的 PIR 容量 (参见文献 [71]), 考虑分布式存储研究中常用的再生码 (尤其是基于矩阵乘积的再生码) 或者局部可修复码下的 PIR 方案 (参见文献 [72]).

• 带有其他额外安全要求的 PIR: 考虑额外的安全约束, 如对称安全, 即用户不可以得知除了检索文件之外的其他任何文件的任何信息; 再如通过添加一定的随机干扰以使若干服务器也无法得知原始数据 (参见文献 [60,123]).

• PIR 文件的最优分包数目: 文献 [105] 及其后续的一些方案虽能达到各模型下的最优, 但方案的实现往往需要将文件切分为庞大数目的分包 (分包数通常为文件数目 M 的指数函数级别). 在考虑最坏情况下载量的意义下, 文献 [145] 率先讨论达到 PIR 容量时的分包数下界. 之后, 在考虑下载量期望值的意义下, 最优分包数目显著下降 (参见文献 [119]).

关于 PIR 的其他发展以及与隐私保护意义下的分布式计算相关的各种问题, 也可参见近期的文献 [120]. 本节剩余部分将介绍 $K \geqslant 2$ 而 $T \geqslant 2$ 下的多文件 PIR 问题, 并展示研究此问题的组合学思想方法.

6.1 问题模型

下面介绍 PIR 模型的具体数学模型.

考虑一个由 N 个服务器组成的分布式存储系统, 以一定的编码方式存储了由 M 个文件组成的数据库, 文件记为 $W^{[1]}, W^{[2]}, \ldots, W^{[M]} \in \mathbb{F}_q^{L\times K}$, 其中每个文件长度为 LK 且以一个 $L \times K$ 的矩阵的形式来表示. 不同的文件之间相互独立, 用信息论的语言来说, 每个文件的信息量为 $H(W^{[i]}) = LK$, 所有文件的总信息量为 $H(W^{[1]}, W^{[2]}, \ldots, W^{[M]}) = MLK$.

每个文件经由同一个 (N, K)-MDS 码独立存储于分布式系统之中, 这一存储码的生成矩阵记为

$$\boldsymbol{G} = [\boldsymbol{g}_1\boldsymbol{g}_2\cdots\boldsymbol{g}_N]_{K\times N}. \tag{6.1}$$

由 MDS 码 (即极大距离可分码) 的性质可知, 上述矩阵中的任何 K 个列向量线性无关. 文件的具体存储方式如下: 考虑文件 $W^{[i]}$ 的矩阵表示中的第 j $(1 \leqslant j \leqslant L)$ 行, 记为 $\boldsymbol{w}_j^{[i]} \in \mathbb{F}_q^K$. 将 K 长向量 $\boldsymbol{w}_j^{[i]}$ 编码成 n 长向量 $\boldsymbol{w}_j^{[i]}\boldsymbol{G}$, 第 n 个服务器存储的是 $\boldsymbol{w}_j^{[i]}\boldsymbol{g}_n$, 进而遍历所有文件的矩阵表示的所有行之后,

第 n 个服务器上存储的整个内容 $\boldsymbol{y}_n \in \mathbb{F}_q^{ML}$ 为所有行向量在 $\boldsymbol{g}_n$ 上的投影, 即

$$\boldsymbol{y}_n = \begin{pmatrix} W^{[1]} \\ \vdots \\ W^{[M]} \end{pmatrix} \boldsymbol{g}_n = [\boldsymbol{w}_1^{[1]}\boldsymbol{g}_n \cdots \boldsymbol{w}_L^{[1]}\boldsymbol{g}_n \boldsymbol{w}_1^{[2]}\boldsymbol{g}_n \cdots \boldsymbol{w}_L^{[2]}\boldsymbol{g}_n \cdots \boldsymbol{w}_1^{[M]}\boldsymbol{g}_n \cdots \boldsymbol{w}_L^{[M]}\boldsymbol{g}_n]^{\mathrm{T}}. \tag{6.2}$$

当用户需要检索文件 $W^{[i]}$ 时, 检索过程包含了问询的上传和反馈的下载两个部分. 问询的上传需要依赖于某些不为服务器所知的随机策略, 这个随机策略影响了问询的具体形式进而有助于隐私的保护. 经由这种随机因素的影响, 用户对第 n 个服务器上传一簇问询, 记为 $Q_n^{[i]}$ $(1 \leqslant n \leqslant N)$. 这些问询也要与具体的文件内容完全无关, 即问询与文件之间的互信息为 0:

$$I(Q_1^{[i]}, Q_2^{[i]}, \ldots, Q_N^{[i]}; W^{[1]}, W^{[2]}, \ldots, W^{[M]}) = 0. \tag{6.3}$$

第 n 个服务器收到问询之后, 做出的反馈记为 $A_n^{[i]}$, 它由收到的问询 $Q_n^{[i]}$ 和服务器存储内容 $\boldsymbol{y}_n$ 唯一确定:

$$H(A_n^{[i]}|Q_n^{[i]}, \boldsymbol{y}_n) = H(A_n^{[i]}|Q_n^{[i]}, W^{[1]}, W^{[2]}, \ldots, W^{[M]}) = 0. \tag{6.4}$$

当用户从所有服务器得到反馈之后, 通过一定译码过程得到所需要检索的文件 $W^{[i]}$. PIR 方案需要保证译码的正确性:

$$H(W^{[i]}|Q_1^{[i]}, Q_2^{[i]}, \ldots, Q_N^{[i]}, A_1^{[i]}, A_2^{[i]}, \ldots, A_N^{[i]}) = 0. \tag{6.5}$$

在整个检索过程中, 假设任意 T 个服务器之间可合谋分析用户的检索行为, 这些服务器所能分析的即为用户向它们发送的问询, 或者等价地说, 它们向用户发送的反馈. PIR 模型需要保证任意 T 个合谋的服务器无法得到关于文件指标 i 的任何信息:

$$I(i; Q_{\mathcal{T}}^{[i]}) = I(i; A_{\mathcal{T}}^{[i]}) = 0, \quad \forall \mathcal{T} \subseteq \{1, 2, \ldots, N\}, \quad |\mathcal{T}| = T. \tag{6.6}$$

满足以上要求的 PIR 方案可能多种多样, 其评价指标为 PIR 码率, 即检索文件的大小与整个下载量的比值 $\frac{H(W^{[i]})}{\sum_{n=1}^{N} H(A_n^{[i]})}$. PIR 容量 C 指所有可行的 PIR 方案中的最大 PIR 码率.

以上是经典的 PIR 模型的数学描述. 针对多文件检索, 需做如下微调.

用户需要同时检索 $2 \leqslant P \leqslant M$ 个文件, 记这些文件的指标为 $\mathcal{P} = \{i_1, i_2, \ldots, i_P\} \subset \{1, 2, \ldots, M\}$, 记 $W^{[\mathcal{P}]} = \{W^{[i]}, i \in \mathcal{P}\}$. 检索这些文件的过程中所涉及的问询和反馈也对应地记为 $Q_n^{[\mathcal{P}]}$ 和 $A_n^{[\mathcal{P}]}$. 上述的相关约束替换如下:

$$\text{(多文件检索的问询)} \quad I(Q_1^{[\mathcal{P}]}, Q_2^{[\mathcal{P}]}, \ldots, Q_N^{[\mathcal{P}]}; W^{[1]}, W^{[2]}, \ldots, W^{[M]}) = 0, \tag{6.7}$$

$$\text{(多文件检索的反馈)} \quad H(A_n^{[\mathcal{P}]}|Q_n^{[\mathcal{P}]}, \mathcal{G}, \boldsymbol{y}_n) = H(A_n^{[\mathcal{P}]}|Q_n^{[\mathcal{P}]}, \mathcal{G}, W^{[1]}, W^{[2]}, \ldots, W^{[M]}) = 0, \tag{6.8}$$

$$\text{(检索的准确性)} \quad H(W^{[\mathcal{P}]}|Q_1^{[\mathcal{P}]}, Q_2^{[\mathcal{P}]}, \ldots, Q_N^{[\mathcal{P}]}, A_1^{[\mathcal{P}]}, A_2^{[\mathcal{P}]}, \ldots, A_N^{[\mathcal{P}]}, \mathcal{F}, \mathcal{G}) = 0, \tag{6.9}$$

$$\text{(检索的隐私性)} \quad I(\mathcal{P}; Q_{\mathcal{T}}^{[\mathcal{P}]}) = I(\mathcal{P}; A_{\mathcal{T}}^{[\mathcal{P}]}) = 0, \quad \forall \mathcal{T} \subseteq \{1, 2, \ldots, N\}, \quad |\mathcal{T}| = T. \tag{6.10}$$

同样, 多文件检索方案的 PIR 码率定义为

$$\frac{\sum_{i \in \mathcal{P}} H(W^{[i]})}{\sum_{n=1}^{N} H(A_n^{[\mathcal{P}]})}, \tag{6.11}$$

而所有可行方案中最大的码率为此时的 PIR 容量, 记为 C^P.

6.2 多文件检索 PIR 方案

多文件检索的一个简单的方式是连续执行 P 次单文件检索版本的 PIR 方案. 然而, 在检索单个文件的同时也可能得到其他文件的部分额外信息, 这额外的收益说明检索多文件的 PIR 码率一定会比单文件检索的码率更好. 而事实上, 由 Banawan 和 Ulukus[10] 设计的多文件检索方案, 其 PIR 码率甚至还要优于追加考虑了额外收益的单文件检索方案对应的值.

多文件检索方案的构造比较复杂, 即便是对于 $K = T = 1$ 的退化情形, 文献 [10] 中的方案在 $P \geqslant \frac{M}{2}$ 和 $P < \frac{M}{2}$ 时的构造也有差异. 本文只考虑 $P \geqslant \frac{M}{2}$ 的情形. $P < \frac{M}{2}$ 时的思路类似但表述复杂, 在此省略. 本小节余下部分将分三个子小节: 第一小节利用信息论不等式给出多文件检索 PIR 方案在退化情形下的码率上限, 第二小节讨论 $P \geqslant \frac{M}{2}$ 时的具体方案, 第三小节对方案进行分析讨论.

6.2.1 退化情形下的多文件检索 PIR 方案码率上限

本小节用信息论工具分析多文件检索 PIR 方案码率上限. $K = T = 1$ 的情形已在文献 [10] 中刻画. 下面将考虑其他退化情形, 即 $K = 1$ 或 $T = 1$ (注: 对于非退化情形, 即 $K \geqslant 2$ 且 $T \geqslant 2$, 即便是单文件检索模型的刻画也是很困难的, 尚无很好的结果).

给定参数 P、N、K 和 T 之后, 最小下载量是文件总数 M 的函数, 记为 Ω_M. 类似于文献 [10], 需要下述符号:

$$\mathcal{Q} \triangleq \{Q_n^{[\mathcal{P}]} : \mathcal{P} \subset \{1, 2, \ldots, M\}, |\mathcal{P}| = P, n \in \{1, 2, \ldots, N\}\}, \tag{6.12}$$

$$A_{n_1:n_2}^{[\mathcal{P}]} \triangleq \{A_{n_1}^{[\mathcal{P}]}, A_{n_1+1}^{[\mathcal{P}]}, \ldots, A_{n_2}^{[\mathcal{P}]}\}, \quad n_1 \leqslant n_2, \quad n_1, n_2 \in \{1, 2, \ldots, M\}. \tag{6.13}$$

不失一般性, 可以假设方案具有高度对称性 (既在文件层面又在服务器层面), 因为可以对任意非对称方案通过遍历文件之间的置换和服务器之间的置换使之转化为一个对称方案. 于是可以假定, 对于任意两组检索指标集 $\mathcal{P}_1$ 和 $\mathcal{P}_2$ 及任意两个服务器, 如第 m 和 n 个, 总有下式成立:

$$H(A_n^{[\mathcal{P}_1]} \mid \mathcal{Q}) = H(A_m^{[\mathcal{P}_2]} \mid \mathcal{Q}). \tag{6.14}$$

与上述等式类似, 考虑已知部分文件时的条件熵, 也有下式成立:

$$H(A_n^{[\mathcal{P}_1]} \mid W^{[\mathcal{S}]}, \mathcal{Q}) = H(A_m^{[\mathcal{P}_2]} \mid W^{[\mathcal{S}]}, \mathcal{Q}), \quad \forall \mathcal{S} \subset \{1, 2, \ldots, M\}. \tag{6.15}$$

多文件检索 PIR 方案码率的分析中的关键点为下述递推关系:

$$\begin{aligned} PL &= H(W^{[\mathcal{P}]}) \\ &= H(W^{[\mathcal{P}]}|\mathcal{Q}) \\ &= I(W^{[\mathcal{P}]}; A_{1:N}^{[\mathcal{P}]}|\mathcal{Q}) + H(W^{[\mathcal{P}]}|A_{1:N}^{[\mathcal{P}]}, \mathcal{Q}) \\ &= I(W^{[\mathcal{P}]}; A_{1:N}^{[\mathcal{P}]}|\mathcal{Q}) \\ &= H(A_{1:N}^{[\mathcal{P}]}|\mathcal{Q}) - H(A_{1:N}^{[\mathcal{P}]}|W^{[\mathcal{P}]}, \mathcal{Q}) \\ &\leqslant \sum_{1 \leqslant n \leqslant N} H(A_n^{[\mathcal{P}]}|\mathcal{Q}) - H(A_{1:N}^{[\mathcal{P}]}|W^{[\mathcal{P}]}, \mathcal{Q}). \end{aligned} \tag{6.16}$$

注意其中的 $\sum_{1 \leqslant n \leqslant N} H(A_n^{[\mathcal{P}]} \mid \mathcal{Q})$ 是总共的下载量. 于是此递推关系也可表述为

$$\Omega_M \geqslant PL + H(A_{1:N}^{[\mathcal{P}]} \mid W^{[\mathcal{P}]}, \mathcal{Q}). \tag{6.17}$$

余下的技巧是如何对上述不等式的后半部分做估计. 对 $T=1$ 或 $K=1$ 这两种情形分别讨论.

• 情形一: $T=1$.

基于由 MDS 码带来的 "任意 K 个服务器拥有全部信息" 性质和方案的对称性, 有

$$H(A_{1:N}^{[\mathcal{P}]} \mid W^{[\mathcal{P}]}, \mathcal{Q}) \geqslant KH(A_1^{[\mathcal{P}]} \mid W^{[\mathcal{P}]}, \mathcal{Q}). \tag{6.18}$$

服务器分析检索指标集 $\mathcal{P}$ 的一种方法是, 分析它收到的问询 (或者等价地说, 它做出的反馈) 基于任何文件子集的条件熵. 于是方案的隐私性必须使得下述约束成立:

$$H(A_1^{[\mathcal{P}]} \mid W^{[\mathcal{P}]}, \mathcal{Q}) = H(A_1^{[\mathcal{P}]} | W^{[\mathcal{P}']}, \mathcal{Q}), \quad \forall \mathcal{P}' \subset \{1, 2, \ldots, M\}, \quad |\mathcal{P}'| = P. \tag{6.19}$$

当 $M \geqslant 2P$ 时, 可以选择检索指标集 $\mathcal{P}'$ 使之与 $\mathcal{P}$ 交集为空集. 于是, $H(A_1^{[\mathcal{P}]} \mid W^{[\mathcal{P}']}, \mathcal{Q})$ 刻画了拥有同样参数 P、N、K 和 T 但是总文件个数为 $M-P$ 时的 PIR 方案在一个服务器上的下载量. 则有下述递推式:

$$\Omega_M \geqslant PL + \frac{K}{N}\Omega_{M-P}, \quad M \geqslant 2P. \tag{6.20}$$

此外, 当 $M < 2P$ 时, 文献 [10] 证明了 $H(A_1^{[\mathcal{P}]} \mid W^{[\mathcal{P}]}, \mathcal{Q})$ 大于等于 $\frac{(M-P)L}{N}$, 于是有 $\Omega_M \geqslant PL + \frac{K}{N}(M-P)L$, $M < 2P$. 递归地使用递推式 (6.20) 可得到

$$\Omega_M \geqslant PL\left(1 + \frac{K}{N} + \left(\frac{K}{N}\right)^2 + \cdots + \left(\frac{K}{N}\right)^{\lfloor \frac{M}{P} \rfloor - 1}\right) + \left(\frac{K}{N}\right)^{\lfloor \frac{M}{P} \rfloor}\left(M - P\left\lfloor \frac{M}{P} \right\rfloor\right)L. \tag{6.21}$$

于是得到多文件检索 PIR 容量的一个上界

$$C^P = \frac{PL}{\Omega_M} \leqslant \left(\frac{1 - (\frac{K}{N})^{\lfloor \frac{M}{P} \rfloor}}{1 - \frac{K}{N}} + \left(\frac{M}{P} - \left\lfloor \frac{M}{P} \right\rfloor\right)\frac{K^{\lfloor \frac{M}{P} \rfloor}}{N^{\lfloor \frac{M}{P} \rfloor}}\right)^{-1}. \tag{6.22}$$

特别地, 当 $M \leqslant 2P$ 时,

$$C^P \leqslant \left(1 + \frac{K(M-P)}{PN}\right)^{-1}. \tag{6.23}$$

注意到当 $K=1$ 时, 上述结论与文献 [10] 中相符.

• 情形二: $K=1$.

与 (6.18) 类似, 下述断言成立:

$$H(A_{1:N}^{[\mathcal{P}]} \mid W^{[\mathcal{P}]}, \mathcal{Q}) \geqslant TH(A_1^{[\mathcal{P}]} \mid W^{[\mathcal{P}]}, \mathcal{Q}). \tag{6.24}$$

无论如何设计一个 PIR 方案, 都可以将具体的问询分为两类. 一类是与检索文件相关的问询, 一类是与检索文件无关的问询 (即其他文件的部分数据的线性组合, 在方案中充当了边际信息的角色). 每个第一类问询将对最后的检索数据提供一单位量的信息. 在最优方案中, 每个第一类问询所提供的一单位量的信息一定是相互独立的, 否则方案会有进一步提升的空间. 在任意 T 个合谋服务器的视野中, 由于它们不能获取检索文件指标集的任何信息, 因此在这些服务器内部的第二类问询所提供的信息也必须是相互独立的. 这就是上述断言所蕴含的思想.

基于上文对 $H(A_1^{[\mathcal{P}]} \mid W^{[\mathcal{P}]}, \mathcal{Q})$ 的分析, 可得到下述递推关系:

$$\Omega_M \geqslant PL + \frac{T}{N}\Omega_{M-P}, \quad M \geqslant 2P. \tag{6.25}$$

此外, 当 $M<2P$ 时, 文献 [10] 证明了 $H(A_1^{[\mathcal{P}]}\mid W^{[\mathcal{P}]},\mathcal{Q})$ 大于等于 $\frac{(M-P)L}{N}$. 于是有 $\Omega_M\geqslant PL+\frac{T}{N}(M-P)L$, $M<2P$. 递归地使用递推式 (6.25) 可得到

$$\Omega_M\geqslant PL\left(1+\frac{T}{N}+\left(\frac{T}{N}\right)^2+\cdots+\left(\frac{T}{N}\right)^{\lfloor\frac{M}{P}\rfloor-1}\right)+\left(\frac{T}{N}\right)^{\lfloor\frac{M}{P}\rfloor}\left(M-P\left\lfloor\frac{M}{P}\right\rfloor\right)L. \tag{6.26}$$

于是得到多文件检索 PIR 容量的一个上界

$$C^P=\frac{PL}{\Omega_M}\leqslant\left(\frac{1-(\frac{T}{N})^{\lfloor\frac{M}{P}\rfloor}}{1-\frac{T}{N}}+\left(\frac{M}{P}-\left\lfloor\frac{M}{P}\right\rfloor\right)\frac{T^{\lfloor\frac{M}{P}\rfloor}}{N^{\lfloor\frac{M}{P}\rfloor}}\right)^{-1}. \tag{6.27}$$

特别地, 当 $M\leqslant 2P$ 时,

$$C^P\leqslant\left(1+\frac{T(M-P)}{PN}\right)^{-1}. \tag{6.28}$$

注意到当 $T=1$ 时, 上述结论与文献 [10] 中相符.

6.2.2 $P\geqslant\frac{M}{2}$ 时的多文件检索 PIR 方案

本小节系统介绍方案的构造, 具体分如下几个步骤.

第 1 步: 令 α 和 β 为满足下式的最小的正整数:

$$\alpha\binom{N}{K}=(\alpha+\beta)\left(\binom{N}{K}-\binom{N-T}{K}\right). \tag{6.29}$$

假设在充分大的域上有 $((\alpha+\beta)\binom{N}{K},\alpha\binom{N}{K})$-MDS 码, 其生成矩阵的转置记为 $\mathrm{MDS}_{(\alpha+\beta)\binom{N}{K}\times\alpha\binom{N}{K}}$.

第 2 步: 令 $L=(\alpha+\beta)\binom{N}{K}$. 从 $\mathbb{F}_q$ 上的所有 $L\times L$ 满秩矩阵中, 独立并均匀地选取 M 个随机矩阵 $S_1,\ldots,S_M$.

第 3 步: 构造一个辅助矩阵, 大小为 $\binom{N-1}{K-1}\times N$, 其中包含了 $\binom{N}{K}$ 个符号, 每个符号各出现 K 次, 每 K 列共享一个相同的符号.

第 4 步 (构建问询结构中的基本模块): 问询结构中包含 $M\alpha+P\beta$ 个模块.

前 $M\alpha$ 个模块记为 $\Lambda_\lambda^{[m]}$ $(1\leqslant\lambda\leqslant\alpha,\ 1\leqslant m\leqslant M)$. 在这类模块中, 每个问询只针对一个文件 $W^{[m]}$. 记出现在模块 $\Lambda_\lambda^{[m]}$ $(1\leqslant\lambda\leqslant\alpha)$ 中的针对文件 $W^{[m]}$ 的问询为 $a^{[m]}_{[(\beta+\lambda-1)\binom{N}{K}+1:(\beta+\lambda)\binom{N}{K}]}$. 模块设定为与辅助矩阵同构的形态, 即任意 K 个服务器上有一个相同的问询.

取一个随机的 MDS 码生成矩阵 $\boldsymbol{H}\in\mathbb{F}_q^{P\times M}$. 例如, 这个矩阵可以是某个 Reed-Solomon 码的生成矩阵辅以列向量的随机置换:

$$\boldsymbol{H}=\begin{pmatrix}\boldsymbol{h}_1\\ \boldsymbol{h}_2\\ \vdots\\ \boldsymbol{h}_P\end{pmatrix}=\begin{pmatrix}h_{11}&h_{12}&\cdots&h_{1M}\\ h_{21}&h_{22}&\cdots&h_{2M}\\ \vdots&\vdots&\ddots&\vdots\\ h_{P1}&h_{P2}&\cdots&h_{PM}\end{pmatrix}. \tag{6.30}$$

后 $P\beta$ 个模块记为 $\Lambda_{\lambda,p}^{\Sigma}$ $(1\leqslant p\leqslant P,\ 1\leqslant\lambda\leqslant\beta)$. 在这类模块中, 每个问询都涉及 M 个文件. 同样每个模块设定为与辅助矩阵同构的形态, 即任意 K 个服务器上有一个相同的问询. 当辅助矩阵的某

一个位置为 $x \in \{1,2,\ldots,\binom{N}{K}\}$ 时, 模块 $\Lambda_{\lambda,p}^{\Sigma}$ 中对应的问询设定为下面的形式和:

$$\boldsymbol{h}_p \cdot (a^{[1]}_{(\lambda-1)\binom{N}{K}+x}, a^{[2]}_{(\lambda-1)\binom{N}{K}+x}, \ldots, a^{[M]}_{(\lambda-1)\binom{N}{K}+x}) = \sum_{m=1}^{M} h_{pm} a^{[m]}_{(\lambda-1)\binom{N}{K}+x}. \tag{6.31}$$

第 5 步 (对检索文件的问询设定): 对于所检索的每个文件 $W^{[m]}$ $(1 \leqslant m \leqslant P)$, 与之相关的检索符号设置为 $a^{[m]}_{[1:L]} = S_m W^{[m]}$.

第 6 步 (对非检索文件的问询设定): 对于每一个非检索文件 $W^{[m]}$, 与之相关的检索符号如下设置. 选取矩阵 S_m 的前 $\alpha\binom{N}{K}$ 行, 记作 $S_m[(1:\alpha\binom{N}{K}),:]$. 检索符号 $a^{[m]}_{[1:L]}$ 设置为

$$a^{[m]}_{[1:L]} = \mathrm{MDS}_{(\alpha+\beta)\binom{N}{K}\times\alpha\binom{N}{K}} S_m \left[\left(1:\alpha\binom{N}{K}\right),:\right] W^{[m]}. \tag{6.32}$$

针对 $P \geqslant \frac{M}{2}$ 的多文件检索 PIR 方案叙述完毕. 下面举一个具体的例子: $N=4$, $K=2$, $T=2$, $M=3$, $P=2$.

三个文件分别记为 $W^{[1]}$、$W^{[2]}$ 和 $W^{[3]}$. 方案中所涉及的参数计算如下: $\alpha=5$, $\beta=1$, $L=36$. 假设每个文件长度为 72, 表示为一个大小为 36×2 的矩阵, 即

$$W^{[1]} = \begin{pmatrix} \boldsymbol{w}_1^{[1]} \\ \vdots \\ \boldsymbol{w}_{36}^{[1]} \end{pmatrix}, \quad W^{[2]} = \begin{pmatrix} \boldsymbol{w}_1^{[2]} \\ \vdots \\ \boldsymbol{w}_{36}^{[2]} \end{pmatrix}, \quad W^{[3]} = \begin{pmatrix} \boldsymbol{w}_1^{[3]} \\ \vdots \\ \boldsymbol{w}_{36}^{[3]} \end{pmatrix}, \tag{6.33}$$

其中 $\boldsymbol{w}_i^{[1]}, \boldsymbol{w}_i^{[2]}, \boldsymbol{w}_i^{[3]} \in \mathbb{F}_q^2$, $1 \leqslant i \leqslant 36$, 这里 $\mathbb{F}_q$ 是一个充分大的有限域. 假设文件 $W^{[1]}$ 和 $W^{[2]}$ 是用户所需检索的文件.

从 $\mathbb{F}_q$ 上所有 36×36 的满秩矩阵中, 独立并均匀地选取三个随机矩阵 $S_1, S_2, S_3 \in \mathbb{F}_q^{36\times 36}$. 假设存在一个 $(36,30)$-MDS 码, 其生成矩阵的转置记为 $\mathrm{MDS}_{36\times 30}$. 选取矩阵 S_3 的前 30 行记为 $S_3[(1:30),:]$. 构造针对三个文件的检索符号如下:

$$a^{[1]}_{[1:36]} = S_1 W^{[1]}, \quad a^{[2]}_{[1:36]} = S_2 W^{[2]}, \quad a^{[3]}_{[1:36]} = \mathrm{MDS}_{36\times 30} S_3[(1:30),:] W^{[3]}.$$

以上三组检索符号将组合成整个方案中的所有问询. 所有问询被划分到 17 个模块之中. 在前 15 个模块中, 每个问询仅是针对某文件的单个检索符号, 而在后两个模块中, 每个问询是三个检索符号的组合. 整个结构如下所示.

前 15 个模块, $\lambda \in \{1,2,3,4,5\}$, $x \in \{1,2,3\}$:

$$\Lambda_{\lambda}^{[x]}: \left\{ \begin{array}{cccc} \text{Server I} & \text{Server II} & \text{Server III} & \text{Server IV} \\ \hline a^{[x]}_{6\lambda+1} & a^{[x]}_{6\lambda+1} & a^{[x]}_{6\lambda+2} & a^{[x]}_{6\lambda+2} \\ a^{[x]}_{6\lambda+3} & a^{[x]}_{6\lambda+4} & a^{[x]}_{6\lambda+3} & a^{[x]}_{6\lambda+4} \\ a^{[x]}_{6\lambda+5} & a^{[x]}_{6\lambda+6} & a^{[x]}_{6\lambda+6} & a^{[x]}_{6\lambda+5} \end{array} \right\}.$$

后两个模块:

$$\Lambda_{1}^{\Sigma}: \left\{ \begin{array}{cccc} \text{Server I} & \text{Server II} & \text{Server III} & \text{Server IV} \\ \hline a_1^{[1]}+a_1^{[2]}+a_1^{[3]} & a_1^{[1]}+a_1^{[2]}+a_1^{[3]} & a_2^{[1]}+a_2^{[2]}+a_2^{[3]} & a_2^{[1]}+a_2^{[2]}+a_2^{[3]} \\ a_3^{[1]}+a_3^{[2]}+a_3^{[3]} & a_4^{[1]}+a_4^{[2]}+a_4^{[3]} & a_3^{[1]}+a_3^{[2]}+a_3^{[3]} & a_4^{[1]}+a_4^{[2]}+a_4^{[3]} \\ a_5^{[1]}+a_5^{[2]}+a_5^{[3]} & a_6^{[1]}+a_6^{[2]}+a_6^{[3]} & a_6^{[1]}+a_6^{[2]}+a_6^{[3]} & a_5^{[1]}+a_5^{[2]}+a_5^{[3]} \end{array} \right\}.$$

$$\Lambda_2^{\Sigma}:\left\{\begin{array}{cccc}\text{Server I} & \text{Server II} & \text{Server III} & \text{Server IV}\\ \hline z_1a_1^{[1]}+z_2a_1^{[2]}+z_3a_1^{[3]} & z_1a_1^{[1]}+z_2a_1^{[2]}+z_3a_1^{[3]} & z_1a_2^{[1]}+z_2a_2^{[2]}+z_3a_2^{[3]} & z_1a_2^{[1]}+z_2a_2^{[2]}+z_3a_2^{[3]}\\ z_1a_3^{[1]}+z_2a_3^{[2]}+z_3a_3^{[3]} & z_1a_4^{[1]}+z_2a_4^{[2]}+z_3a_4^{[3]} & z_1a_3^{[1]}+z_2a_3^{[2]}+z_3a_3^{[3]} & z_1a_4^{[1]}+z_2a_4^{[2]}+z_3a_4^{[3]}\\ z_1a_5^{[1]}+z_2a_5^{[2]}+z_3a_5^{[3]} & z_1a_6^{[1]}+z_2a_6^{[2]}+z_3a_6^{[3]} & z_1a_6^{[1]}+z_2a_6^{[2]}+z_3a_6^{[3]} & z_1a_5^{[1]}+z_2a_5^{[2]}+z_3a_5^{[3]}\end{array}\right\},$$

其中 z_1、z_2 和 z_3 是 $\mathbb{F}_q$ 中随机取的三个不同元素.

检索文件 $W^{[1]}$ 和 $W^{[2]}$ 等价于检索所有 $a_{[1:36]}^{[1]}$ 和 $a_{[1:36]}^{[2]}$, 这是因为 S_1 和 S_2 均为满秩矩阵, 其中, $a_{[7:36]}^{[1]}$、$a_{[7:36]}^{[2]}$ 和 $a_{[7:36]}^{[3]}$ 可被直接检索. 进而 $a_{[1:6]}^{[3]}$ 依据 $\mathrm{MDS}_{36\times30}$ 的 MDS 性质可由 $a_{[7:36]}^{[3]}$ 解出. 于是, 模块 Λ_1^{Σ} 和 Λ_2^{Σ} 中的所有来自文件 3 的干扰项均可被化简. 于是余下的形如 $a_i^{[1]}+a_i^{[2]}$ 和 $z_1a_i^{[1]}+z_2a_i^{[2]}$ $(1\leqslant i\leqslant 6)$ 的问询即可解出. 通过求解 6 组方程组得到 $a_{[1:6]}^{[1]}$ 和 $a_{[1:6]}^{[2]}$.

本方案对于任意两个合谋的服务器有完全的隐私性. 在任何两个服务器的视野中, 它们一共收到了涉及每个文件的 30 个问询符号. 这些问询符号每一个都对应于 $\mathbb{F}_q^{36}$ 中的一个向量. 回顾 S_1、S_2、S_3 和 $(36,30)$-MDS 码的选取, 可知每个文件涉及的 30 个问询符号所对应的向量都是线性无关的. 再加上整个问询结构在文件方面的对称性, 任意两个服务器无法判定检索指标集的任何信息, 从而用户隐私得以保证.

上述方案的码率达到了 $\frac{36\times2\times2}{12\times5\times3+12+12}=\frac{12}{17}$. 作为比较, 如果简单使用两次单文件检索 PIR 方案的话, 则码率仅为 $\frac{61}{91}<\frac{12}{17}$.

6.2.3 方案分析

每个问询符号出现在 K 个不同的服务器上, 故而它对应的信息可被正确译码. 于是对于每个文件 $W^{[m]}$ 都可得到所有的检索符号 $a_{[\beta\binom{N}{K}+1:L]}^{[m]}$. 进而由 $\mathrm{MDS}_{(\alpha+\beta)\binom{N}{K}\times\alpha\binom{N}{K}}$ 的 MDS 性质, 对于每个非检索文件, 可利用 $a_{[\beta\binom{N}{K}+1:L]}^{[m]}$ 解得 $a_{[1:\beta\binom{N}{K}]}^{[m]}$. 将这些干扰项从 $P\beta$ 个模块 $\Lambda_{\lambda,p}^{\Sigma}$ 中去除, 余下的是一组由 β 个方程构成的方程组. 每个方程组的系数来自矩阵 $\boldsymbol{H}$ 中的某 P 列, 故系数矩阵为一个 $P\times P$ 可逆矩阵. 通过求解此方程组, 对每个检索文件可译码得到 $a_{[1:\beta\binom{N}{K}]}^{[m]}$, 于是每个检索文件的所有 L 个检索符号都被获取, 这等价于检索得到了每个检索文件 (因为 S_m 是满秩矩阵).

此方案在任意 T 个服务器合谋的情形下仍保持隐私性. 从任意 T 个服务器的角度看, 整体的问询结构对于所有文件都是对称的. 这 T 个服务器上总共涉及的每个文件的检索符号数目均为 $(\alpha+\beta)(\binom{N}{K}-\binom{N-T}{K})$. 提取每个检索符号的系数形成一个 $\mathbb{F}_q^L$ 中的向量. 由检索符号的构造方法及 $((\alpha+\beta)\binom{N}{K},\alpha\binom{N}{K})$-MDS 码的性质可知, 每个文件对应的检索符号均为 $\mathbb{F}_q^L$ 中一个随机的 $\alpha\binom{N}{K}$ 维空间. 于是这些合谋的服务器无法从检索需求中判断出文件之间的任何差异, 检索文件的指标信息得以成功隐藏.

方案的 PIR 码率计算如下:

$$\frac{PLK}{(M\alpha+P\beta)K\binom{N}{K}}=\frac{P\alpha+P\beta}{M\alpha+P\beta}=\frac{\binom{N}{K}}{\frac{M}{P}(\binom{N}{K}-\binom{N-T}{K})+\binom{N-T}{K}}.\tag{6.34}$$

再次注意目前针对的是 $P\geqslant\frac{M}{2}$ 的情形. 当 $T=1$ 时, 上述码率为 $(1+\frac{K(M-P)}{PN})^{-1}$, 与 (6.23) 中推导的容量相符. 当 $K=1$ 时, 上述码率为 $(1+\frac{T(M-P)}{PN})^{-1}$, 与 (6.28) 中推导的容量相符. 对于 $P\geqslant\frac{M}{2}$, 上述方案在退化的参数情形下达到最优. 上述分析总结如下.

定理 6.1 当 $T+K\leqslant N$ 且 $P\geqslant \frac{M}{2}$ 时, 存在 $(N,K,T;M)$ P 文件 PIR 方案, 且 PIR 码率达到 $\frac{\binom{N}{K}}{\frac{M}{P}(\binom{N}{K}-\binom{N-T}{K})+\binom{N-T}{K}}$. 此方案在 $K=1$ 或 $T=1$ 的参数退化情形时达到最优.

最后简要讨论连续执行 P 次单文件 PIR 方案这一平凡方法. 利用本文最初的单文件版本方案, 连续执行 P 次的 PIR 码率仅为

$$(1+R^{M-1}P-R^{M-1})(1+R+R^2+\cdots+R^{M-1})^{-1}, \tag{6.35}$$

其中 $R=1-\frac{\binom{N-T}{K}}{\binom{N}{K}}$. 需要注意的是这里的计算已经将每次方案能略微获取其他 $P-1$ 个文件的部分信息这一事实考虑在内. 作为对比, 本文多文件方案码率要优于这种平凡方法, 这只需要证明

$$1+R+\cdots+R^{M-1}>\left(\frac{M}{P}R+1-R\right)(1+R^{M-1}P-R^{M-1}). \tag{6.36}$$

不等号右边或者是在 $P=M$ 时达到最大值 $1+(M-1)R^{M-1}$), 或者是在 $P=\frac{M}{2}$ 时达到最大值 $(1+R)(1+(\frac{M}{2}-1)R^{M-1})$). 无论如何, 这两个值都严格小于不等号左边. 这证明了本文多文件 PIR 方案确实优于连续执行 P 次单文件 PIR 方案这种平凡方法, 故而是有意义的.

7 结论

本文选取了 5 个源于分布式网络的信息科学问题, 探讨其中涉及的离散模型与组合学方法. 事实上, 组合数学与信息科学的交织关联远不止这些. 在当今大数据时代与网络安全的背景下, 越来越多的信息科学问题为组合数学带来新的机遇与挑战, 这需要工程背景与数学背景的研究人员更多地交流与合作. 特别地, 针对本文中的具体课题, 下述与组合学相关的研究方向值得进一步的探索.

• 组合设计中的 q-Steiner 结构可推导出最优常维码, 但目前已知存在的非平凡结构除展形之外仅有 $\mathbb{S}_2(2,3,13)$. 另外, 由部分展形推导出的最优常维码的结果也很有限. 该方向值得考虑的公开问题包括新参数下的 q-Steiner 结构的存在性尤其 q-Fano 平面的存在性问题和由部分展形能推导出的更多的最优常维码问题.

• 针对一般索引编码问题码长估计, 图染色方法起到了至关重要的作用, 混淆图的染色数给出了码长下界. 下一步需要考虑如何利用以格理论为代表的代数方法和以干扰对齐方法为代表的编码手段构造接近最优的码类以及如何将各种组合方法推广至多信源索引编码问题中.

• 编码缓存方案的变种五花八门, 但其原始模型中分包数与传输率的制约关系仍未完全解决. 目前, 在传输率为用户数目的线性级别时, 只存在分包数为用户数目次指数级别的方案. 能否将分包数降为用户数目多项式级别是编码缓存方案中最根本的问题之一. 为此, 需研究对应的 PDA 或超图的构造方法或给出不存在性的严格证明.

• 针对分布式计算中 MapReduce 模型的构建, 绝大多数达到计算负载与传输负载最优权衡的方案需要满足一定的整除性条件, 下一步的研究问题是如何在非整除条件下构造达到或接近最优权衡的一系列方案, 并进一步寻找参数更为灵活的构造方法.

• 隐私保护信息检索一般模型下的 PIR 容量仍未完全解决, 尤其在文件数目仅有两个的特殊情形下, 已有一些超过线性方案 PIR 容量的例子. 下一步值得探讨的问题是如何得到文件数目较少时超过线性方案 PIR 容量的系统构造, 并由此探究固定文件数目下的最优 PIR 容量.

除以上这些与组合学密切相关的问题之外, 本文所涉及主题的其他进一步研究问题, 读者可以参看以下各主题的综述文献中的相关内容: 网络编码 [13]、索引编码 [5]、编码缓存 [85]、分布式计算 [76] 和隐私保护信息检索 [120].

致谢 感谢审稿人的有益建议.

参考文献

1 Agrawal S, Sree K V S, Krishnan P. Coded caching based on combinatorial designs. In: Proceedings of the 2019 IEEE International Symposium on Information Theory (ISIT). Paris: IEEE, 2019, 1227–1231
2 Ahlswede R, Cai N, Li S Y R, et al. Network information flow. IEEE Trans Inform Theory, 2000, 46: 1204–1216
3 Alon N, Lubetzky E, Stav U, et al. Broadcasting with side information. In: Proceedings of the 2008 IEEE Symposium on Foundations of Computer Science. Philadelphia: IEEE, 2008, 823–832
4 Alon N, Moitra A, Sudakov B. Nearly complete graphs decomposable into large induced matchings and their applications. In: Proceedings of the 2012 ACM Symposium on Theory of Computing. New York: ACM, 2012, 1079–1090
5 Arbabjolfaei F, Kim Y H. Fundamentals of index coding. FNT Commun Inf Theor, 2018, 14: 163–346
6 Augot D, Levy-dit-Vehel F, Shikfa A. A storage-efficient and robust private information retrieval Scheme allowing few servers. In: Cryptology and Network Security. CANS 2014. Lecture Notes in Computer Science, vol. 8813. Cham: Springer, 2014, 222–239
7 Azure Batch. https://azure.microsoft.com/en-us/pricing/details/batch/, 2018
8 Azure Batch. https://docs.microsoft.com/en-us/azure/batch/batch-low-pri-vms, 2018
9 Banawan K, Ulukus S. The capacity of private information retrieval from coded databases. IEEE Trans Inform Theory, 2018, 64: 1945–1956
10 Banawan K, Ulukus S. Multi-message private information retrieval: Capacity results and near-optimal schemes. IEEE Trans Inform Theory, 2018, 64: 6842–6862
11 Banawan K, Ulukus S. The capacity of private information retrieval from Byzantine and colluding databases. IEEE Trans Inform Theory, 2019, 65: 1206–1219
12 Bar-Yossef Z, Birk Z, Jayram T S, et al. Index coding with side information. In: Proceedings of the 2006 IEEE Symposium on Foundations of Computer Science. Berkeley: IEEE, 2006, 197–206
13 Bassoli R, Marques H, Rodriguez J, et al. Network coding theory: A survey. IEEE Commun Surv Tutorials, 2013, 15: 1950–1978
14 Beimel A, Ishai Y, Kushilevitz E, et al. Breaking the $O(n^{1/(2k-1)})$ barrier for information-theoretic private information retrieval. In: Proceedings of the 43rd Annual IEEE Symposium on Foundations of Computer Science. Vancouver: IEEE, 2002, 261–270
15 Berge C, Ray-Chaudhuri D. Unsolved problems. In: 1972 Hypergraph Seminar: Ohio State University. Lecture Notes in Mathematics. Berlin: Springer, 1974, 278–287
16 Beutelspacher A. Partial spreads in finite projective spaces and partial designs. Math Z, 1975, 145: 211–229
17 Birk Y, Kol T. Informed-source coding-on-demand (ISCOD) over broadcast channels. In: Proceedings of IEEE INFOCOM'98. San Francisco: IEEE, 1998, 1257–1264
18 Bitar R, Xing Y, Keshtkarjahromi Y, et al. Private and rateless adaptive coded matrix-vector multiplication. J Wireless Com Network, 2021, 2021: 15
19 Blackburn S R, Etzion T, Paterson M B. PIR schemes with small download complexity and low storage requirements. IEEE Trans Inform Theory, 2020, 66: 557–571
20 Brahma S, Fragouli C. Pliable index coding. IEEE Trans Inform Theory, 2015, 61: 6192–6203
21 Braun M, Kerber A, Laue R. Systematic construction of q-analogs of t-(v,k,λ)-designs. Des Codes Cryptogr, 2005, 34: 55–70
22 Cai N, Yeung R W. Network coding and error correction. In: Proceedings of the 2002 IEEE Information Theory Workshop. Bangalore: IEEE, 2002, 119–122
23 Cai N, Yeung R W. Network error correction, I: Basic concepts and upper bounds. Commun Inf Syst, 2006, 6: 19–35
24 Cai N, Yeung R W. Network error correction, II: Lower bounds. Commun Inf Syst, 2006, 6: 37–54
25 Cameron P J. Generalisation of Fisher's inequality to fields with more than one element. In: McDonough T P, Mavron V C, eds. Combinatorics. London Mathematical Society Lecture Note Series. Cambridge: Cambridge University Press, 1974, 9–13
26 Cao H, Yan Q, Tang X, et al. Adaptive gradient coding. IEEE/ACM Trans Networking, 2022, 30: 717–734
27 Chan T, Ho S, Yamamoto H. Private information retrieval for coded storage. In: Proceedings of the 2015 IEEE International Symposium on Information Theory (ISIT). Hong Kong: IEEE, 2015, 2842–2846
28 Cheng M, Jiang J, Yan Q, et al. Constructions of coded caching schemes with flexible memory size. IEEE Trans Commun, 2019, 67: 4166–4176
29 Cheng M, Li J, Tang X, et al. Linear coded caching scheme for centralized networks. IEEE Trans Inform Theory,

2021, 67: 1732–1742
30 Cheng M, Wang J, Zhong X, et al. A framework of constructing placement delivery arrays for centralized coded caching. IEEE Trans Inform Theory, 2021, 67: 7121–7131
31 Chor B, Goldreich O, Kushilevitz E, et al. Private information retrieval. In: Proceedings of the IEEE 36th Annual Foundations of Computer Science. Milwaukee: IEEE, 1995, 41–50
32 Chor B, Kushilevitz E, Goldreich O, et al. Private information retrieval. J ACM, 1998, 45: 965–981
33 Chowdhury M, Zaharia M, Ma J, et al. Managing data transfers in computer clusters with orchestra. SIGCOMM Comput Commun Rev, 2011, 41: 98–109
34 Chun B G, Condie T, Chen Y, et al. Apache REEF: Retainable evaluator execution framework. ACM Trans Comput Syst, 2017, 35: 1–31
35 Dau H, Gabrys R, Huang Y-C, et al. Optimizing the transition waste in coded elastic computing. In: Proceedings of the 2020 IEEE International Symposium on Information Theory (ISIT). Los Angeles: IEEE, 2020, 174–178
36 Dau S H, Skachek V, Chee Y M. On the security of index coding with side information. IEEE Trans Inform Theory, 2012, 58: 3975–3988
37 Dean J, Corrado G, Monga R, et al. Large scale distributed deep networks. In: Proceedings of the 25th International Conference on Neural Information Processing Systems. Red Hook: Curran Associates, 1223–1231
38 Dean J, Ghemawat S. MapReduce: Simplified data processing on large clusters. Commun ACM, 2008, 51: 107–113
39 Delsarte P. Association schemes and t-designs in regular semilattices. J Combin Theory Ser A, 1976, 20: 230–243
40 Dimakis A G, Ramchandran K, Wu Y, et al. A survey on network codes for distributed storage. Proc IEEE, 2011, 99: 476–489
41 Dvir Z, Gopi S. 2-server PIR with subpolynomial communication. J ACM, 2016, 63: 1–15
42 Ebrahimi J B, Fragouli C. Algebraic algorithms for vector network coding. IEEE Trans Inform Theory, 2011, 57: 996–1007
43 Efremenko K. 3-query locally decodable codes of subexponential length. SIAM J Comput, 2012, 41: 1694–1703
44 El-Zanati S, Jordon H, Seelinger G, et al. The maximum size of a partial 3-spread in a finite vector space over $GF(2)$. Des Codes Cryptogr, 2010, 54: 101–107
45 Elias P, Feinstein A, Shannon C E. A note on the maximum flow through a network. IEEE Trans Inform Theory, 1956, 2: 117–119
46 Etzion T, Wachter-Zeh A. Vector network coding based on subspace codes outperforms scalar linear network coding. In: Proceedings of the 2016 IEEE International Symposium on Information Theory (ISIT). Barcelona: IEEE, 2016, 1949–1953
47 Dutta S, Fahim M, Haddadpour F, et al. On the optimal recovery threshold of coded matrix multiplication. IEEE Trans Inform Theory, 2020, 66: 278–301
48 Ford Jr. L R, Fulkerson D R. Maximal flow through a network. Canad J Math, 1956, 8: 399–404
49 Freij-Hollanti R, Gnilke O W, Hollanti C, et al. Private information retrieval from coded databases with colluding servers. SIAM J Appl Algebra Geometry, 2017, 1: 647–664
50 Greferath M, Pavčević M O, Silberstein N, et al. Network Coding and Subspace Designs. Switzerland: Springer, 2018
51 Guang X, Fu F W, Zhang Z. Construction of network error correction codes in packet networks. IEEE Trans Inform Theory, 2013, 59: 1030–1047
52 Hachem J, Karamchandani N, Diggavi S N. Coded caching for multi-level popularity and access. IEEE Trans Inform Theory, 2017, 63: 3108–3141
53 Halbawi W, Azizan-Ruhi N, Salehi F, et al. Improving distributed gradient descent using Reed-Solomon codes. In: Proceedings of the 2018 IEEE International Symposium on Information Theory (ISIT). Vail: IEEE, 2018, 2027–2031
54 Hasircioglu B, Gomez-Vilardebo J, Gunduz D. Speeding up private distributed matrix multiplication via bivariate polynomial codes. In: Proceedings of the 2021 IEEE International Symposium on Information Theory (ISIT). Melbourne: IEEE, 2021, 1853–1858
55 Ho T, Médard M, Koetter R, et al. A random linear network coding approach to multicast. IEEE Trans Inform Theory, 2006, 52: 4413–4430
56 Holzbaur L, Freij-Hollanti R, Li J, et al. Toward the capacity of private information retrieval from coded and colluding servers. IEEE Trans Inform Theory, 2022, 68: 517–537
57 Hu Y C, Patel M, Sabella D, et al. Mobile edge computing—A key technology towards 5G. ETSI White Paper, 2015, 11: 1–16
58 Jaggi S, Sanders P, Chou P A, et al. Polynomial time algorithms for multicast network code construction. IEEE Trans Inform Theory, 2005, 51: 1973–1982

59 Ji M, Caire G, Molisch A F. Fundamental limits of caching in wireless D2D networks. IEEE Trans Inform Theory, 2016, 62: 849–869

60 Jia Z, Jafar S A. On the asymptotic capacity of X-secure T-private information retrieval with graph-based replicated storage. IEEE Trans Inform Theory, 2020, 66: 6280–6296

61 Jiang J, Qu L. Cascaded coded distributed computing schemes based on placement delivery arrays. IEEE Access, 2020, 8: 221385

62 Kadhe S, Garcia B, Heidarzadeh A, et al. Private information retrieval with side information. IEEE Trans Inform Theory, 2020, 66: 2032–2043

63 Karmoose M, Song L, Cardone M, et al. Private broadcasting: An index coding approach. In: Proceedings of the 2017 IEEE International Symposium on Information Theory (ISIT). Aachen: IEEE, 2017, 2543–2547

64 Katyal D, Muralidhar P N, Rajan B S. Multi-access coded caching schemes from cross resolvable designs. IEEE Trans Commun, 2021, 69: 2997–3010

65 Kiani S, Adikari T, Draper S C. Hierarchical coded elastic computing. In: Proceedings of the 2021 IEEE International Conference on Acoustics, Speech and Signal Processing. Toronto: IEEE, 2021, 4045–4049

66 Koetter R, Kschischang F R. Coding for errors and erasures in random network coding. IEEE Trans Inform Theory, 2008, 54: 3579–3591

67 Koetter R, Médard M. An algebraic approach to network coding. IEEE/ACM Trans Networking, 2003, 11: 782–795

68 Konstantinidis K, Ramamoorthy A. Resolvable designs for speeding up distributed computing. IEEE/ACM Trans Networking, 2020, 28: 1657–1670

69 Krishnan P, Mathew R, Kalyanasundaram S. Pliable index coding via conflict-free colorings of hypergraphs. In: Proceedings of the 2021 IEEE International Symposium on Information Theory (ISIT). Melbourne: IEEE, 2021, 214–219

70 Kuikui L, Tao M, Zhang J, et al. Multi-cell mobile edge coded computing: Trading communication and computing for distributed matrix multiplication. In: Proceedings of the 2020 IEEE International Symposium on Information Theory (ISIT). Los Angeles: IEEE, 2020, 215–220

71 Kumar S, Lin H Y, Rosnes E, et al. Achieving maximum distance separable private information retrieval capacity with linear codes. IEEE Trans Inform Theory, 2019, 65: 4243–4273

72 Lavauzelle J, Tajeddine R, Freij-Hollanti R, et al. Private information retrieval schemes with product-matrix MBR codes. IEEE Trans Inform Forensic Secur, 2020, 16: 441–450

73 Li K, Tao M, Chen Z. A computation-communication tradeoff study for mobile edge computing networks. In: Proceedings of the 2019 IEEE International Symposium on Information Theory (ISIT). Paris: IEEE, 2019, 2639–2643

74 Li K, Tao M, Chen Z. Exploiting computation replication for mobile edge computing: A fundamental computation-communication tradeoff study. IEEE Trans Wireless Commun, 2020, 19: 4563–4578

75 Li M, Ong L, Johnson S J. Multi-sender index coding for collaborative broadcasting: A rank-minimization approach. IEEE Trans Commun, 2019, 67: 1452–1466

76 Li S, Maddah-Ali M A, Yu Q, et al. A fundamental tradeoff between computation and communication in distributed computing. IEEE Trans Inform Theory, 2017, 64: 109–128

77 Li S Y R, Yeung R W, Cai N. Linear network coding. IEEE Trans Inform Theory, 2003, 49: 371–381

78 Liu T, Tuninetti D. Decentralized pliable index coding. In: Proceedings of the 2019 IEEE International Symposium on Information Theory (ISIT). Paris: IEEE, 2019, 532–536

79 Liu T, Tuninetti D. Private pliable index coding. In: Proceedings of the 2019 IEEE Information Theory Workshop (ITW). Visby: IEEE, 2019, 1–5

80 Liu T, Tuninetti D. Secure decentralized pliable index coding. In: Proceedings of the 2020 IEEE International Symposium on Information Theory (ISIT). Los Angeles: IEEE, 2020, 1729–1734

81 Lubetzky E, Stav U. Nonlinear index coding outperforming the linear optimum. IEEE Trans Inform Theory, 2009, 55: 3544–3551

82 Mach P, Becvar Z. Mobile edge computing: A survey on architecture and computation offloading. IEEE Commun Surv Tutorials, 2017, 19: 1628–1656

83 Maddah-Ali M A, Niesen U. Fundamental limits of caching. IEEE Trans Inform Theory, 2014, 60: 2856–2867

84 Maddah-Ali M A, Niesen U. Decentralized coded caching attains order-optimal memory-rate tradeoff. IEEE/ACM Trans Networking, 2015, 23: 1029–1040

85 Maddah-Ali M A, Niesen U. Coding for caching: Fundamental limits and practical challenges. IEEE Commun Mag, 2016, 54: 23–29

86 Mahajan K, Chowdhury M, Akella A, et al. Dynamic query re-planning using QOOP. In: Proceedings of the 2018

Symposium on Operating Systems Design and Implementation. Carlsbad: USENIX Association, 2018, 253–267
87 Matsuda T, Noguchi T, Takine T. Survey of network coding and its applications. IEICE Trans Commun, 2011, E94-B: 698–717
88 Matsumoto R. Construction algorithm for network error-correcting codes attaining the singleton bound. IEICE Trans Fundamentals Electron Commun Comput Sci, 2007, E90-A: 1729–1735
89 Neely M J, Tehrani A S, Zhang Z. Dynamic index coding for wireless broadcast networks. IEEE Trans Inform Theory, 2013, 59: 7525–7540
90 Ong L, Ho C K, Lim F. The single-uniprior index-coding problem: The single-sender case and the multi-sender extension. IEEE Trans Inform Theory, 2016, 62: 3165–3182
91 Pedarsani R, Maddah-Ali M A, Niesen U. Online coded caching. IEEE/ACM Trans Networking, 2016, 24: 836–845
92 Ramamoorthy A, Das A B, Tang L. Straggler-resistant distributed matrix computation via coding theory: Removing a bottleneck in large-scale data processing. IEEE Signal Process Mag, 2020, 37: 136–145
93 Ramkumar V, Kumar P V. Coded MapReduce schemes based on placement delivery array. In: Proceedings of the 2019 IEEE International Symposium on Information Theory (ISIT). Paris: IEEE, 2019, 3087–3091
94 Raviv N, Tamo I, Tandon R, et al. Gradient coding from cyclic MDS codes and expander graphs. IEEE Trans Inform Theory, 2020, 66: 7475–7489
95 Reddy K S, Karamchandani N. Structured index coding problem and multi-access coded caching. IEEE J Sel Areas Inf Theory, 2021, 2: 1266–1281
96 Ruzsa I, Szeméredi E. Triple systems with no six points carrying three triangles. In: Combinatorics. Amsterdam-New York: North-Holland, 1978, 939–945
97 Sasi S, Rajan B S. Multi-access coded caching scheme with linear sub-packetization using PDAs. In: Proceedings of the 2021 IEEE International Symposium on Information Theory (ISIT). Melbourne: IEEE, 2021, 861–866
98 Sengupta A, Tandon R, Clancy T C. Fundamental limits of caching with secure delivery. IEEE Trans Inform Forensic Secur, 2015, 10: 355–370
99 Shah N B, Rashmi K V, Ramchandran K. One extra bit of download ensures perfectly private information retrieval. In: Proceedings of the 2014 IEEE International Symposium on Information Theory (ISIT). Honolulu: IEEE, 2014, 856–860
100 Shangguan C, Zhang Y, Ge G. Centralized coded caching schemes: A hypergraph theoretical approach. IEEE Trans Inform Theory, 2018, 64: 5755–5766
101 Shanmugam K, Dimakis A G, Langberg M. Graph theory versus minimum rank for index coding. In: Proceedings of the 2014 IEEE International Symposium on Information Theory (ISIT). Honolulu: IEEE, 2014, 291–295
102 Shanmugam K, Tulino A M, Dimakis A G. Coded caching with linear subpacketization is possible using Ruzsa-Szeméredi graphs. In: Proceedings of the 2017 IEEE International Symposium on Information Theory (ISIT). Aachen: IEEE, 2017, 1237–1241
103 Silva D, Kschischang F R, Koetter R. A rank-metric approach to error control in random network coding. IEEE Trans Inform Theory, 2008, 54: 3951–3967
104 Song L, Fragouli C. A polynomial-time algorithm for pliable index coding. IEEE Trans Inform Theory, 2018, 64: 979–999
105 Sun H, Jafar S A. The capacity of private information retrieval. IEEE Trans Inform Theory, 2017, 63: 4075–4088
106 Sun H, Jafar S A. Private information retrieval from MDS coded data with colluding servers: Settling a conjecture by Freij-Hollanti et al. IEEE Trans Inform Theory, 2018, 64: 1000–1022
107 Sun H, Jafar S A. The capacity of robust private information retrieval with colluding databases. IEEE Trans Inform Theory, 2018, 64: 2361–2370
108 Suzuki H. 2-designs over $GF(2^m)$. Graphs Combin, 1990, 6: 293–296
109 Suzuki H. 2-designs over $GF(q)$. Graphs Combin, 1992, 8: 381–389
110 Tajeddine R, Gnilke O W, El Rouayheb S. Private information retrieval from MDS coded data in distributed storage systems. IEEE Trans Inform Theory, 2018, 64: 7081–7093
111 Tajeddine R, Gnilke O W, Karpuk D, et al. Private information retrieval from coded storage systems with colluding, Byzantine, and unresponsive servers. IEEE Trans Inform Theory, 2019, 65: 3898–3906
112 Tandon R. The capacity of cache aided private information retrieval. In: Proceedings of the 2017 55th Annual Allerton Conference on Communication, Control, and Computing. Monticello: IEEE, 2017, 108–1082
113 Tandon R, Lei Q, Dimakis A G, et al. Gradient coding: Avoiding stragglers in distributed learning. In: Proceedings of the 34th International Conference on Machine Learning. Sydney: PMLR, 2017, 3368–3376
114 Tang L, Ramamoorthy A. Coded caching schemes with reduced subpacketization from linear block codes. IEEE Trans Inform Theory, 2018, 64: 3099–3120

115 Tehrani A S, Dimakis A G, Neely M J. Bipartite index coding. In: Proceedings of the 2012 IEEE International Symposium on Information Theory. Cambridge: IEEE, 2012, 2246–2250

116 Thapa C, Ong L, Johnson S J. Graph-theoretic approaches to two-sender index coding. In: Proceedings of the 2016 IEEE Globecom Workshops. Washington: IEEE, 2016, 1–6

117 Thapa C, Ong L, Johnson S J, et al. Structural characteristics of two-sender index coding. Entropy, 2019, 21: 615

118 Thomas S. Designs over finite fields. Geom Dedicata, 1987, 24: 237–242

119 Tian C, Sun H, Chen J. Capacity-achieving private information retrieval codes with optimal message size and upload cost. IEEE Trans Inform Theory, 2019, 65: 7613–7627

120 Ulukus S, Avestimehr S, Gastpar M, et al. Private retrieval, computing, and learning: Recent progress and future challenges. IEEE J Sel Areas Commun, 2022, 40: 729–748

121 Unal S, Wagner A B. A rate-distortion approach to index coding. IEEE Trans Inform Theory, 2016, 62: 6359–6378

122 Wang J, Cheng M, Wan K, et al. Novel frameworks for coded caching via cartesian product with reduced subpacketization. arXiv:2108.08486, 2021

123 Wang Q, Skoglund M. Symmetric private information retrieval from MDS coded distributed storage with non-colluding and colluding servers. IEEE Trans Inform Theory, 2019, 65: 5160–5175

124 Woolsey N, Chen R-R, Ji M. A new combinatorial design of coded distributed computing. In: Proceedings of the 2018 IEEE International Symposium on Information Theory (ISIT). Vail: IEEE, 2018, 726–730

125 Woolsey N, Chen R-R, Ji M. Heterogeneous computation assignments in coded elastic computing. In: Proceedings of the 2020 IEEE International Symposium on Information Theory (ISIT). Los Angeles: IEEE, 2020, 168–173

126 Woolsey N, Chen R-R, Ji M. Coded elastic computing on machines with heterogeneous storage and computation speed. IEEE Trans Commun, 2021, 69: 2894–2908

127 Yan Q, Cheng M, Tang X, et al. On the placement delivery array design for centralized coded caching scheme. IEEE Trans Inform Theory, 2017, 63: 5821–5833

128 Yan Q, Parampalli U, Tang X, et al. Online coded caching with random access. IEEE Commun Lett, 2017, 21: 552–555

129 Yan Q, Tang X, Chen Q, et al. Placement delivery array design through strong edge coloring of bipartite graphs. IEEE Commun Lett, 2018, 22: 236–239

130 Yan Q, Wigger M, Yang S, et al. A fundamental storage-communication tradeoff for distributed computing with straggling nodes. IEEE Trans Commun, 2020, 68: 7311–7327

131 Yang S, Yeung R W, Ngai C K. Refined coding bounds and code constructions for coherent network error correction. IEEE Trans Inform Theory, 2011, 57: 1409–1424

132 Yang Y, Interlandi M, Grover P, et al. Coded elastic computing. In: Proceedings of the 2019 IEEE International Symposium on Information Theory (ISIT). Paris: IEEE, 2019, 2654–2658

133 Ye M, Abbe E. Communication-computation efficient gradient coding. In: Proceedings of the 35th International Conference on Machine Learning. Stockholm: PMLR, 2018, 5606–5615

134 Yekhanin S. Towards 3-query locally decodable codes of subexponential length. J ACM, 2008, 55: 1–16

135 Yekhanin S. Private information retrieval. Commun ACM, 2010, 53: 68–73

136 Yu Q, Li S, Raviv N, et al. Lagrange coded computing: Optimal design for resiliency, security, and privacy. In: Proceedings of the 2019 International Conference on Artificial Intelligence and Statistics. Naha: PMLR, 2019, 1215–1225

137 Yu Q, Maddah-Ali M A, Avestimehr A S. Polynomial codes: An optimal design for high-dimensional coded matrix multiplication. In: Proceedings of the 31st International Conference on Neural Information Processing Systems. Red Hook: Curran Associates, 2017, 4406–4416

138 Yu Q, Maddah-Ali M A, Avestimehr A S. The exact rate-memory tradeoff for caching with uncoded prefetching. IEEE Trans Inform Theory, 2018, 64: 1281–1296

139 Yu Q, Maddah-Ali M A, Avestimehr A S. Straggler mitigation in distributed matrix multiplication: Fundamental limits and optimal coding. IEEE Trans Inform Theory, 2020, 66: 1920–1933

140 Zhang J, Simeone O. On model coding for distributed inference and transmission in mobile edge computing systems. IEEE Commun Lett, 2019, 23: 1065–1068

141 Zhang Y, Ge G. Private information retrieval from MDS coded databases with colluding servers under several variant models. arXiv:1705.03186, 2017

142 Zhang Y, Ge G. A general private information retrieval scheme for MDS coded databases with colluding servers. Des Codes Cryptogr, 2019, 87: 2611–2623

143 Zhang Z. Network error correction coding in packetized networks. In: Proceedings of the 2006 IEEE Information Theory Workshop. Chengdu: IEEE, 2006, 433–437

144 Zhang Z. Linear network error correction codes in packet networks. IEEE Trans Inform Theory, 2008, 54: 209–218
145 Zhang Z, Xu J. The optimal sub-packetization of linear capacity-achieving PIR schemes with colluding servers. IEEE Trans Inform Theory, 2019, 65: 2723–2735

Discrete configurations and combinatorial methods originated from distributed network

Xuejiao Han, Yiwei Zhang, Jianxing Yin & Dianhua Wu

Abstract In recent years, many new problems of information science originating from distributed networks have brought new challenges to the classical information theory and coding theory. The research of these problems involves many discrete configurations. Combinatorial methods such as combinatorial design theory, graph theory, combinatorial coding theory and extremal combinatorics have been playing an important role in the research of these problems. In this paper, we briefly survey the progress on five hot frontier topics originating from distributed networks, including network coding, index coding, coded caching, distributed computing, and private information retrieval. In particular, we emphasize the discrete configurations and combinatorial methods related to these topics. For some of the topics, we also provide a few new results.

Keywords **distributed network, network coding, index coding, coded caching, distributed computing, private information retrieval**

MSC(2020) **05B99, 68P30, 68R05**

doi: 10.1360/SSM-2022-0074