中国科学: 数学 2023 年 第 53 卷 第 2 期: 187～216
SCIENTIA SINICA Mathematica
综 述

稀疏超图: 从理论到应用

献给朱烈教授 80 华诞

上官冲[1*], 葛根年[2]

1. 山东大学数学与交叉科学研究中心, 青岛 266237;
2. 首都师范大学数学科学学院, 北京 100048
E-mail: theoreming@163.com, gnge@zju.edu.cn

收稿日期: 2022-01-14; 接受日期: 2022-03-18; 网络出版日期: 2022-07-28; * 通信作者
国家重点研发计划 (批准号: 2020YFA0712100 和 2018YFA0704703)、国家自然科学基金 (批准号: 12101364 和 11971325)、山东省自然科学基金 (批准号: ZR2021QA005) 和北京学者计划资助项目

摘要 给定正整数 r、e 和 v, 如果某个 r- 一致超图的任意 e 条不同边的并都包含至少 $v+1$ 个顶点, 则称其是 (v,e)- 自由 (free) 或者 (v,e)- 稀疏的. 稀疏超图的概念由 Brown、Erdős 和 Sós 在 20 世纪 70 年代提出. 目前, 研究给定顶点数的稀疏超图所能包含最大边数的上下界已成为极值组合学研究领域内的核心问题之一. 该问题的研究方法丰富多变, 涉及组合、概率、代数和数论等多个领域. 本文介绍 Brown、Erdős 和 Sós 关于稀疏超图的两个重要猜想的最新研究进展以及稀疏超图在极值组合与信息科学中的若干应用, 包括朱烈曾作出突出贡献的完美哈希 (Hash) 矩阵、可分哈希矩阵等几类信息安全中的研究问题. 此外, 本文在某些参数下给出完美哈希矩阵与求并 - 自由 (union-free) 超图的新构造. 本文的构造改进了相应问题的已知最优下界.

关键词 稀疏超图 Brown-Erdős-Sós 猜想 完美哈希矩阵 可消去 (cancellative) 超图 求并 - 自由超图 集中式编码缓存 组合列表译码 局部可修复码

MSC (2020) 主题分类 05B20, 05B40, 05C65, 05D05, 05D40, 11B30, 60A86, 68P30, 94B25

1 稀疏超图的起源、历史与发展

1.1 简介

稀疏超图 (sparse hypergraphs) 问题是 Brown 等 [12] 和 Sós 等 [71] 在 20 世纪 70 年代提出的一类经典的 Turán 型问题 (Turán-type problem). 该问题受到了多位著名领袖组合学家的重视, 目前已成为极值组合学研究领域内的核心问题之一. 与之相关的研究方法丰富多变, 涉及组合、概率、代数和数论等多个领域. 特别地, 人们对稀疏超图的研究极大地推动了正则性方法 (regularity method) 的发

英文引用格式: Shangguan C, Ge G N. Sparse hypergraphs: From theory to applications (in Chinese). Sci Sin Math, 2023, 53: 187–216, doi: 10.1360/SSM-2022-0008

展. 这一强有力的方法已成为离散数学的重要研究工具, 其创始人 Szemerédi 也获得了 2012 年的 Abel 奖 (Abel prize). 除此之外, 作为一种拥有优美性质的组合构型, 稀疏超图有着众多令人意想不到的应用. 多种不同参数的稀疏超图被广泛应用于极值组合、编码理论、信息安全与理论计算机科学等诸多领域, 为相关研究带来了新的思想和工具. 本文回顾稀疏超图研究的理论成果以及丰富应用, 着重介绍其主要研究方法. 在该领域内依然有众多困难的未解之谜, 吸引着人们不断尝试.

1.2 Turán 型问题

超图 (hypergraph) $\mathcal{H}=(V(\mathcal{H}),E(\mathcal{H}))$ 由点集 $V(\mathcal{H})$ 和边集 $E(\mathcal{H})$ 所构成, 其中, $V(\mathcal{H})$ 是一个给定的有限集, $E(\mathcal{H})$ 是 $V(\mathcal{H})$ 的幂集的一个子集. 为了叙述方便, 通常认为 $\mathcal{H}=E(\mathcal{H})$. 如果存在正整数 r, 使得对于任意 $A\in\mathcal{H}$ 都有 $|A|=r$, 则称超图 $\mathcal{H}$ 为 r- 一致的 (r-uniform). 也简称 r- 一致超图为 r- 超图.

设 $\mathcal{F}$ 和 $\mathcal{H}$ 均为 r- 超图, 如果 $\mathcal{H}$ 的任何子超图 (subhypergraph) 都不同构于 $\mathcal{F}$, 则称 $\mathcal{H}$ 为 $\mathcal{F}$- 自由的; 反之, $\mathcal{H}$ 总是包含 $\mathcal{F}$ 的至少一个拷贝 (copy). 设 $\mathscr{F}$ 为一族 r- 超图构成的非空有限集合, 如果对于任意 $\mathcal{F}\in\mathscr{F}$, $\mathcal{H}$ 都是 $\mathcal{F}$- 自由的, 则称 $\mathcal{H}$ 是 $\mathscr{F}$- 自由的. $\mathscr{F}$ 的 Turán 数 $\mathrm{ex}_r(n,\mathscr{F})$ 被定义为具有 n 个顶点的 $\mathscr{F}$- 自由 r- 超图所能含有的最大边数. 当 $|\mathscr{F}|=1$ 即 $\mathscr{F}=\{F\}$ 时, 简记 $\mathrm{ex}_r(n,\{F\})=\mathrm{ex}_r(n,F)$. 人们将研究函数 $\mathrm{ex}_r(n,\mathscr{F})$ 上下界的问题称为 Turán 型问题 (Turán-type problems), 这是因为这类问题源于匈牙利数学家 Turán[81] 在 20 世纪 40 年代的开创性工作. 本文所涉及的超图都是 r- 超图, 且有如下约定: (1) r 总是给定的正整数, 而 n 可以趋于无穷大; (2) 在本文研究的 $\mathscr{F}$- 自由 Turán 型问题中, $\mathscr{F}$ 总是给定的, 其定义不依赖于 n.

显然, 对于任意 $\mathscr{F}$ 都有 $0\leqslant\mathrm{ex}_r(n,\mathscr{F})\leqslant\binom{n}{r}$. Katona 等[43] 证明了, 对于任意给定的 $\mathscr{F}$, 极限

$$\lim_{n\to\infty}\frac{\mathrm{ex}_r(n,\mathscr{F})}{\binom{n}{r}}$$

总是存在的. 称该极限为 $\mathscr{F}$ 的 Turán 密度 (Turán density). 如果存在实数 $0\leqslant\alpha\leqslant r$, 使得当 n 趋于无穷大时有 $\mathrm{ex}_r(n,\mathscr{F})=\Theta(n^\alpha)$, 则称 α 为 $\mathscr{F}$ 的 Turán 指数 (Turán exponent). 如果 $\mathscr{F}$ 的 Turán 指数小于 r (即其 Turán 密度为 0), 则称对应的 Turán 型问题是退化的 (degenerate). 对于退化型 Turán 问题, 如果极限 $\lim_{n\to\infty}\frac{\mathrm{ex}_r(n,\mathscr{F})}{n^\alpha}$ 存在, 则称该极限为 $\mathscr{F}$ 的退化型 Turán 密度 (degenerate Turán density). Katona 等[43] 实际上证明了任意给定的 $\mathscr{F}$ 都存在 Turán 密度, 那么, 任意给定的 $\mathscr{F}$ 是否都存在 Turán 指数? 实际上, 稀疏超图与该问题密切相关.

当 $r=2$ 时, 人们通常称 2- 超图也为图 (graph). 对于图的 Turán 数, 人们已有丰富的研究成果. 1907 年, Mantel[49] 证明了对有 3 个顶点的完全图 (complete graph) K_3 有 $\mathrm{ex}_2(n,K_3)=\lfloor\frac{n^2}{4}\rfloor$. 1941 年, Turán[81] 将 Mantel 的结果推广到一般的完全图 K_t ($t\geqslant 3$), 并对于任意正整数 n 都确定了 $\mathrm{ex}_2(n,K_t)$ 的精确值. 我们一般认为 Turán 的这篇文献开创了极值图论这个研究领域. 随后, Erdős 和 Stone[25] 及 Erdős 和 Simonovits[24] 证明了极值图论的奠基性定理, 即 Erdős-Stone-Simonovits 定理:

定理 1.1[24,25] 设 $\mathscr{F}$ 为一族图构成的有限集, 则当 n 充分大时,

$$\mathrm{ex}_2(n,\mathscr{F})=\frac{\chi(\mathscr{F})-2}{\chi(\mathscr{F})-1}\cdot\frac{n^2}{2}+o(n^2),$$

其中, $\chi(\mathscr{F})=\min\{\chi(F):F\in\mathscr{F}\}$, 这里 $\chi(F)$ 为图 F 的染色数 (chromatic number), 即所需最少的颜色数, 使得 F 存在任意相邻顶点都不同色的点染色.

当 $r=2$ 时, 定理 1.1 给出了所有有限集 $\mathscr{F}$ 的 Turán 密度. 如果 $\chi(\mathscr{F})\geqslant 3$, 则定理 1.1 还给出了 $\mathrm{ex}_2(n,\mathscr{F})$ 的近似值. 例如, $\mathrm{ex}_2(n,K_t)=\frac{t-2}{t-1}\frac{n^2}{2}+o(n^2)$. 然而, 如果 $\chi(\mathscr{F})=2$, 则由定理 1.1 仅可知 $\mathrm{ex}_2(n,\mathscr{F})=o(n^2)$—人们并不能得出 $\mathscr{F}$ 确切的 Turán 指数. 对此情形, Erdős[19] 有如下著名的有理指数存在性猜想 (rational exponents conjecture):

猜想 1.1 (参见文献 [19, 公式 (1)]) 设 $\mathscr{F}$ 为一族图构成的有限集, 若 $\chi(\mathscr{F})=2$, 则存在有理数 $\alpha\in[0,1)$ 和实数 $c>0$, 使得

$$\lim_{n\to\infty}\frac{\mathrm{ex}_2(n,\mathscr{F})}{n^{1+\alpha}}=c.$$

要对所有的 $\chi(\mathscr{F})=2$ 完全解决上述猜想是一个非常困难的问题, 感兴趣的读者可参见文献 [31] 的综述. 接下来, 会看到人们对稀疏超图的研究说明猜想 1.1 对超图来说 ($r\geqslant 3$) 是不成立的.

1.3 稀疏超图的 Turán 型问题

给定正整数 r、e 和 v, 称 r- 超图 $\mathcal{H}$ 是 (v,e)- 自由的, 如果它的任意 e 条不同边的并都包含至少 $v+1$ 个顶点, 即对于任意 $A_1,\dots,A_e\in\mathcal{H}$, 都有

$$\left|\bigcup_{i=1}^{e}A_i\right|\geqslant v+1.$$

用函数 $f_r(n,v,e)$ 表示 n 个顶点的 (v,e)- 自由 r- 超图所能包含的最大边数. 记

$$\mathcal{G}_r(v,e)=\left\{\mathcal{F}\subseteq\binom{[v]}{r}:|\mathcal{F}|=e,|V(\mathcal{F})|\leqslant v\right\},$$

则根据定义有 $f_r(n,v,e)=\mathrm{ex}_r(n,\mathcal{G}_r(v,e))$. 因此关于 $f_r(n,v,e)$ 的研究是典型的超图 Turán 型问题. 由于其所含边数的稀疏性, 人们也称 (v,e)- 自由的 r- 超图为稀疏超图[30].

不难看出, 当 $v\leqslant r$ 时, $f_r(n,v,e)=\binom{n}{r}$; 当 $v\geqslant er$ 时, $f_r(n,v,e)=0$; 当 $v=er-1$ 时, $f_r(n,v,e)=\lfloor\frac{n}{r}\rfloor$. 此外, 当 $e=2$ 时, r- 超图 $\mathcal{H}$ 是 $(v,2)$- 自由的当且仅当对于任意不同的 $A,B\in\mathcal{H}$ 都有 $|A\cap B|\leqslant 2r-v-1$. 此时 Rödl[56] 利用巧妙的 "Rödl 针法" 证明了

$$\lim_{n\to\infty}f_r(n,v,2)\cdot\left(\binom{n}{2r-v}\Big/\binom{r}{2r-v}\right)^{-1}=1.$$

事实上, $f_r(n,v,2)$ 的研究也是组合设计的重要课题 (参见文献 [13]). 近期, Keevash[45] 在相关问题的研究中取得了重大突破, 他证明了对于任意满足某些必要整除性条件的参数都有

$$f_r(n,v,2)=\binom{n}{2r-v}\Big/\binom{r}{2r-v}.$$

由于上述结果, 在下面的讨论中总是假设 $r\geqslant 2$, $e\geqslant 3$, $r+1\leqslant v\leqslant er-2$. 在这个参数范围内, Brown 等[12] 得到了 $f_r(n,v,e)$ 的一般上下界:

$$C_1n^{\frac{er-v}{e-1}}\leqslant f_r(n,v,e)\leqslant C_2n^{\lceil\frac{er-v}{e-1}\rceil},\tag{1.1}$$

其中 C_1 和 C_2 是与 n 无关且仅依赖于 r、e 和 v 的两个常数. 由 (1.1) 不难看出, 当 $\frac{er-v}{e-1}$ 为正整数时, $f_r(n,v,e)=\Theta(n^{\frac{er-v}{e-1}})$. 人们由此知道了函数 $f_r(n,v,e)$ 的渐近阶, 并称 $\frac{er-v}{e-1}$ 为 $f_r(n,v,e)$ 的 Turán 指数; 而当 $e-1\nmid er-v$ 时, (1.1) 并不能给出函数 $f_r(n,v,e)$ 的渐近阶. 上述两种情形导致人们作出如下两个猜想.

猜想 1.2 (Brown-Erdős-Sós 第一猜想)　对于任意给定的正整数 $r > k \geqslant 2$ 和 $e \geqslant 3$, 都有

$$n^{k-o(1)} < f_r(n, er-(e-1)k+1, e) = o(n^k),$$

即对于任意给定的 $\epsilon > 0$, 都有

$$\lim_{n\to\infty} \frac{f_r(n, er-(e-1)k+1, e)}{\epsilon n^k} = 0, \quad \lim_{n\to\infty} \frac{f_r(n, er-(e-1)k+1, e)}{n^{k-\epsilon}} = \infty.$$

猜想 1.3 (Brown-Erdős-Sós 第二猜想)　对于任意给定的正整数 $r > k \geqslant 2$ 和 $e \geqslant 3$, 极限

$$\lim_{n\to\infty} \frac{f_r(n, er-(e-1)k, e)}{n^k}$$

总是存在.

上述两个猜想是稀疏超图研究中的两个核心问题. 事实上, 在 Brown 等最初的文献 [12] 中, 他们仅提到了猜想 1.2 和 1.3 的部分情形: 他们认为, 猜想 1.2 对 $r = 3$、$k = 2$ 和 $e = 3$ 成立, 猜想 1.3 对 $r = 3$、$k = 2$ 和 $e \geqslant 3$ 成立. 经过后来研究者的不断补充与发展 (如文献 [4,22,32,63] 等), 这两个猜想才有了如今的形式. 为了叙述方便, 又由于 Brown 等是这类问题的最早研究者, 本文还是称这两个猜想为 "Brown-Erdős-Sós 第一猜想" 和 "Brown-Erdős-Sós 第二猜想". 下面分别介绍猜想 1.2 和 1.3 的研究进展.

1.3.1 Brown-Erdős-Sós 第一猜想

首先, 根据 (1.1) 有

$$\Omega(n^{k-\frac{1}{e-1}}) = f_r(n, er-(e-1)k+1, e) = O(n^k). \tag{1.2}$$

显然, (1.2) 未能解决猜想 1.2 的任何一种情形. 实际上, 猜想 1.2 的第一种情形 (即 $r = 3, k = 2, e = 3$) 由 Ruzsa 和 Szemerédi [59] 在 1976 年解决, 他们证明了著名的 $(6, 3)$- 定理:

$$n^{2-o(1)} < f_3(n, 6, 3) = o(n^2). \tag{1.3}$$

Ruzsa 和 Szemerédi 的上述结果是极值图论发展历史中的一个里程碑, (1.3) 上界的证明利用了 Szemerédi [78] 的图正则性引理 (graph regularity lemma), 这也是正则引理的最早几个应用之一, 充分显示了其强大的威力; (1.3) 下界的证明利用了 Behrend [6] 构造的不含 3- 长等差数列的正整数集, 并搭建了连接极值图论与加法数论这两个领域的桥梁. Ruzsa 和 Szemerédi 的结果同时也说明了猜想 1.1 对超图来说 ($r \geqslant 3$) 是不正确的, 因为 $f_3(n, 6, 3)$ 显然没有 Turán 指数. 1986 年, Erdős 等 [22] 将 (1.3) 的上下界推广到一般的 $r \geqslant 3$, 他们证明了

$$n^{2-o(1)} < f_r(n, 3r-3, 3) = o(n^2). \tag{1.4}$$

2006 年, Alon 和 Shapira [4] 进一步证明了猜想 1.2 对所有的 $e = 3$ 都成立, 他们得到对于任意给定的正整数 $r > k \geqslant 2$ 都有

$$n^{k-o(1)} < f_r(n, 3r-2k+1, 3) = o(n^k). \tag{1.5}$$

令人遗憾的是, 到目前为止, 对于任意 $e \geqslant 4$, 人们都不能同时证明猜想 1.2 的上下界. 2005 年, Sárközy 和 Selkow [61] 对于 $k \geqslant 3$ 证明了

$$f_r(n, 4r-3k+1, 4) = o(n^k). \tag{1.6}$$

Nagle 等 [51] 对于所有 $r \geqslant k+1 = e$ 证明了

$$f_r(n, (k+1)r-k^2+1, k+1) = o(n^k). \tag{1.7}$$

2021 年, Ge 和 Shangguan [32] 证明了猜想 1.2 的上界对于所有 $r \geqslant k+1 \geqslant e$ 都成立, 下界对于所有 $r \geqslant 3$、$k = 2$ 和 $e \in \{4, 5, 7, 8\}$ 都成立.

在所有其他参数下, 猜想 1.2 的上界和下界都未能被证明, 人们只知道一些弱化的结果. 例如, 对于上界, Sárközy 和 Selkow [60] 利用图正则引理证明了, 对于所有给定的 $r > k \geqslant 2$ 和 $e \geqslant 3$ 都有

$$f_r(n, er-(e-1)k+\lfloor \log e \rfloor, e) = o(n^k). \tag{1.8}$$

Conlon 等 [15] 利用超图正则引理 (hypergraph regularity lemma) 将上述结果改进为

$$f_r\left(n, er-(e-1)k+O\left(\frac{\log e}{\log\log e}\right), e\right) = o(n^k). \tag{1.9}$$

对于下界, Shangguan 和 Tamo [64] 利用概率方法将 (1.2) 中的结果改进为

$$f_r(n, er-(e-1)k+1, e) = \Omega(n^{k-\frac{1}{e-1}}(\log n)^{\frac{1}{e-1}}). \tag{1.10}$$

上述 $f_r(n, er-(e-1)k+1, e)$ 的新下界与猜想值仍然有很大距离, 尤其是人们不知道是否存在一个常数 $\epsilon > 0$, 使得对所有 $r > k \geqslant 2$ 和 $e \geqslant 3$ 都有

$$f_r(n, er-(e-1)k+1, e) = \Omega(n^{k-\frac{1}{e-1}+\epsilon}).$$

综上所述, 目前已知猜想 1.2 的上界对于所有 $r \geqslant k+1 \geqslant e$ 都成立, 下界对于所有 $r > k \geqslant 2$、$e = 3$ 与 $r > k = 2$、$e \in \{4, 5, 7, 8\}$ 都成立. 猜想 1.2 上界的第一个未解决情形是研究是否有

$$f_3(n, 7, 4) = o(n^2),$$

即所谓的 $(7, 4)$ 问题. 目前, 对于猜想 1.2 上界的研究, 人们多采用正则性方法; 对于猜想 1.2 下界的研究, 人们多采用加法数论与概率方法. 第 3 节将举例说明人们是如何利用这些方法来解决 Brown-Erdős-Sós 第一猜想的若干子情形. 表 1 总结了 Brown-Erdős-Sós 第一猜想的研究情况.

表 1 Brown-Erdős-Sós 第一猜想的研究情况

	已解决情形	部分进展
上界	$r \geqslant k+1 \geqslant e \geqslant 3$ [4, 22, 32, 51, 59, 61]	(1.1) [12]、(1.8) [60]、(1.9) [15]
下界	$r \geqslant k+1 \geqslant 3$, $e = 3$ [4, 22, 59]; $r \geqslant 3$, $k = 2$, $e \in \{4, 5, 7, 8\}$ [32]	(1.10) [64]

1.3.2 Brown-Erdős-Sós 第二猜想

与猜想 1.2 不同, 直到 2019 年才由 Glock [34] 证明了猜想 1.3 的第一种情形 (即 $r=3$, $k=2$, $e=3$):

$$\lim_{n\to\infty}\frac{f_3(n,5,3)}{n^2}=\frac{1}{5}. \tag{1.11}$$

Glock 的证明利用了某个特殊图的图填充 (graph packing) [53]. Shangguan 和 Tamo [63] 利用诱导图填充 (induced graph packing) [28] 和递归构造 (recursive construction) 将 Glock 的结果从 $r=3$ 推广到一般的 $r\geqslant 4$, 得到了

$$\lim_{n\to\infty}\frac{f_r(n,3r-4,3)}{n^2}=\frac{1}{r^2-r-1}. \tag{1.12}$$

对于所有其他情形, 猜想 1.3 都是完全公开的. 目前, 人们只知道函数 $f_r(n,er-(e-1)k,e)$ 的一些上下界. 例如, Shangguan 和 Tamo [63] 利用多项式方法证明了

$$\frac{1}{r^k-r}\leqslant\liminf_{n\to\infty}\frac{f_r(n,3r-2k,3)}{n^k}\leqslant\limsup_{n\to\infty}\frac{f_r(n,3r-2k,3)}{n^k}\leqslant\frac{1}{k!\binom{r}{k}-\frac{k!}{2}}. \tag{1.13}$$

最近, Sidorenko [69] 证明了

$$f_r(n,r+2,3)\geqslant\left(\frac{1}{r}-o(1)\right)\binom{n}{r-1}, \tag{1.14}$$

这改进了 (1.13) 在 $k=r-1$ 时下界的结果. 此外, Bohman 和 Warnke [10] 以及 Glock 等 [35] 分别独立地证明了, 对于任意给定的 $e\geqslant 4$ 都有

$$f_3(n,e+2,e)\geqslant\left(\frac{1}{6}-o(1)\right)n^2. \tag{1.15}$$

注意到猜想 1.3 只要求证明极限 $\lim_{n\to\infty}\frac{f_r(n,er-(e-1)k,e)}{n^k}$ 的存在性, 并不要求计算出其精确值. 表 2 总结了 Brown-Erdős-Sós 第二猜想的研究情况.

1.4 稀疏超图的应用

作为组合数学的重要研究对象之一, 稀疏超图被广泛应用于极值组合、编码理论、信息安全与理论计算机科学等诸多领域. 人们将相关领域的问题转化为某类稀疏超图的存在与构造问题, 再对其加以研究. 这些转化往往都不是直截了当的, 而是具有相当的技巧性. 对于这些应用, 本文选取 “完美与可分哈希矩阵” “可消去与求并 - 自由超图” “集中式编码缓存” “组合列表译码” “局部可修复码” 等课题展开较为详细的阐述. 我们也在前两个课题的研究中取得了一些新进展, 详细内容见定理 5.4 和 5.6. 表 3 总结了不同参数下稀疏超图的应用情况.

表 2 Brown-Erdős-Sós 第二猜想的研究情况

已解决情形	部分进展
$r\geqslant 3$, $k=2$, $e=3$ [34,63]	(1.13) [63]、(1.14) [69]、(1.15) [10,35]

表 3 不同参数下稀疏超图的应用情况

应用名称	对应稀疏超图参数	参考文献
完美哈希矩阵	$(er-r,e)$- 自由 r- 超图	[62, 定理 7.1]
t- 可消去超图	$(tr+\lceil\frac{2r-t-1}{t+2}\rceil,t+2)$- 自由 $+$ $(2r-\lceil\frac{2r-t-1}{t+2}\rceil-1,2)$- 自由 r- 超图	[65, 引理 2.3]
2- 可消去超图	$(2r,3)$- 自由 r- 超图, $2\nmid r$	[65, 引理 2.4]
t- 求并 - 自由超图	$(tr-r,t)$- 自由 $+$ $(tr,2t)$- 自由 r- 部 r- 超图	[65, 引理 2.5]
集中式编码缓存	$(6,3)$- 自由 3- 部 3- 超图	[67, 定理 10]
具有 (ρ,L)- 列表译码性质的 r 长 q 元纠错码	$(r+(L+1)\rho r,L+1)$- 自由 r- 部 r- 超图 每部都含 q 个顶点	[36, 引理 4.5]
局部可修复码	$(ir-i,i)$- 自由 r- 超图, 对于所有 $1\leqslant i\leqslant e$	[84, 定理 3.1] [46, 定理 V.8 和 V.9]

1.5 一些记号

对于正整数 n, 记 $[n]:=\{1,\dots,n\}$. 若超图 $\mathcal{H}$ 的顶点集大小为 n, 则不失一般性记 $V(\mathcal{H})=[n]$. 如果没有特别指出, 我们一般认为 n 趋于无穷大. 对于有限集 X, 用 $\binom{X}{r}:=\{A\subseteq X:|A|=r\}$ 表示由 X 的所有 r- 元子集所构成的集合. 对于正整数 $1\leqslant k\leqslant r$, 用 K_r^k 表示具有 r 个顶点的完全 k- 超图, 即

$$E(K_r^k)=\binom{[r]}{k}.$$

如果集合 A 满足 $|A|=r$, 则用 $K_r^k(A)$ 表示顶点集为 A 的完全 k- 超图.

设 $f:=f(n)$ 和 $g:=g(n)$ 为依赖于 n 的函数, 如果 $\lim_{n\to\infty}\frac{f}{g}=0$, 则记 $f=o(g)$; 如果存在某个不依赖于 n 的常数 C 使得 $f\leqslant Cg$, 则记 $f=O(g)$; 如果存在 C 使得 $f\geqslant Cg$, 则记 $f=\Omega(g)$; 如果 $f=O(g)$ 和 $f=\Omega(g)$ 同时成立, 则记 $f=\Theta(g)$.

将多次用到多部超图与矩阵的等价关系. 称一个 r- 超图 $\mathcal{H}$ 是 r- 部的 (r-partite), 如果 $V(\mathcal{H})$ 可以被划分为 r 个两两互不相交的子集, $V(\mathcal{H})=\bigcup_{i=1}^r V_i$, 使得对于任意 $A\in\mathcal{H}$ 和 $1\leqslant i\leqslant r$ 都有 $|A\cap V_i|=1$. 如果对于任意 $1\leqslant i\leqslant r$ 都有 $|V_i|=q$, 则不失一般性, 假设 $V_i=\{(i,a):1\leqslant a\leqslant q\}$. 此时, 对于每一条边 $A=\{(i,x_i):1\leqslant i\leqslant r,1\leqslant x_i\leqslant q\}\in\mathcal{H}$, 定义映射

$$\begin{aligned}&\psi:\mathcal{H}\to[q]^r,\\&\quad A\mapsto\psi(A)=(x_1,\dots,x_r).\end{aligned}$$

以下观察是显然的.

声明 1.1 依据映射 ψ, 以 $\{V_i:1\leqslant i\leqslant r\}$ 为顶点集划分的 r- 部 r- 超图 $\mathcal{H}=\{A_1,\dots,A_m\}$ 可以被等价地表示为一个 $r\times m$ 的 q 元矩阵 $M_{\mathcal{H}}=(\psi(A_1)^{\mathrm{T}},\dots,\psi(A_m)^{\mathrm{T}})$, 使得对于 $1\leqslant i\leqslant m$, 该矩阵的第 i 列为 $\psi(A_i)^{\mathrm{T}}$.

1.6 文章结构

第 2 节介绍一般参数下稀疏超图的理论界. 第 2.1 小节介绍 Brown-Erdős-Sós 的经典上下界 (参见定理 2.1) 及其证明, 第 2.2 小节叙述 Shangguan-Tamo 的改进型下界 (参见定理 2.2) 及其证明概要.

第 3 节介绍猜想 1.2 的研究进展. 第 3.1 小节讨论猜想 1.2 的上界与超图移除引理的关系, 并给出猜想上界对于所有 $r\geqslant k+1\geqslant e$ 都成立的证明 (参见定理 3.1); 第 3.2 小节讨论猜想 1.2 的下界与加法数论的关系, 并给出 (1.3) 的下界的证明 (参见定理 3.2).

第 4 节介绍猜想 1.3 的研究进展. 第 4.1 小节讨论猜想 1.3 的上界, 并给出 (1.13) 的上界的证明 (参见定理 4.1); 第 4.2 小节讨论猜想 1.2 的下界与近似最优图填充的关系, 并给出 (1.11) 的证明 (参见定理 4.2).

第 5 节介绍稀疏超图在极值组合中的两个应用. 第 5.1 小节介绍如何利用稀疏超图来构造可分与完美哈希矩阵, 第 5.2 小节介绍如何利用稀疏超图来构造可消去超图和求并 - 自由超图. 本文也在与这两小节相关的课题上取得了一些新进展, 参见定理 5.4 和 5.6.

第 6 介绍稀疏超图在信息科学中的 3 个应用. 第 6.1 小节讨论 $(6,3)$- 自由 3- 超图与集中式编码缓存方案的关系, 第 6.2 小节讨论如何利用稀疏超图来构造具有优异组合列表译码性质的纠错码, 第 6.3 小节介绍如何利用稀疏超图构造在存储编码领域发挥着重要作用的局部可修复码.

第 7 节总结全文, 并给出一些值得研究的公开问题.

2 一般参数下稀疏超图的理论界

本节主要讨论一般参数下函数 $f_r(n,v,e)$ 的上下界. 第 2.1 小节给出 (1.1) 的具体证明, 第 2.2 小节叙述 (1.10) 的证明思路. 本节的主要目的是说明 $f_r(n,v,e)$ 的值实际上等于某个超图的最大独立集大小, 因而在研究中可以利用图论与概率方法的相关知识.

2.1 Brown-Erdős-Sós 的经典上下界

我们将利用 “算两次” (double counting) 这一组合技巧来证明 (1.1) 的上界, 并利用超图独立集的一个简单下界来证明 (1.1) 的下界. 给定 r- 超图 $\mathcal{H}$, 若点集 $S\subseteq V(\mathcal{H})$ 中不包含 $\mathcal{H}$ 的任意一条边, 即 $\binom{S}{r}\cap\mathcal{H}=\emptyset$, 则称 S 为 $\mathcal{H}$ 的独立集 (independent set). 称 $\mathcal{H}$ 的独立数 (independence number) $\alpha(\mathcal{H})$ 为 $V(\mathcal{H})$ 所包含的最大独立集的大小, 即

$$\alpha(\mathcal{H}):=\max\{|S|:\ S\subseteq\ V(\mathcal{H})\ \text{是}\ \mathcal{H}\ \text{的一个独立集}\}.$$

对于每个顶点 $v\in V(\mathcal{H})$, 定义 v 在 $\mathcal{H}$ 中的度数 (degree) $\mathrm{d}_{\mathcal{H}}(v)$ 为 $\mathcal{H}$ 中包含 v 的边的数目, 即 $\mathrm{d}_{\mathcal{H}}(v):=|\{v\in A:A\in\mathcal{H}\}|$. 当不会引起混淆时, 我们将省略下标 $\mathcal{H}$. 定义 $\mathcal{H}$ 的最大度 (maximum degree) 和平均度 (average degree) 分别为

$$\Delta(\mathcal{H}):=\max\{\mathrm{d}(v):v\in V(\mathcal{H})\}\quad\text{和}\quad\mathrm{d}(\mathcal{H}):=\frac{\sum_{v\in V(\mathcal{H})}\mathrm{d}(v)}{|V(\mathcal{H})|}.$$

显然, $\Delta(\mathcal{H})\geqslant\mathrm{d}(\mathcal{H})$. 下面的引理给出了 r- 超图最大独立数的一个简单下界.

引理 2.1 [72] 给定正整数 $r\geqslant 2$, 则存在一个仅依赖于 r 的常数 $C:=C(r)$, 使得对于任意 r- 超图 $\mathcal{H}$ 都有

$$\alpha(\mathcal{H})\geqslant C\frac{|V(\mathcal{H})|}{\mathrm{d}(\mathcal{H})^{\frac{1}{r-1}}}.$$

本小节的目标是证明如下定理 (即 (1.1)).

定理 2.1 (参见文献 [12, 第 4 节]) 对于任意给定的正整数 $r\geqslant 2$, $e\geqslant 2$, $r+1\leqslant v\leqslant er-2$, 都有

$$C_1n^{\frac{er-v}{e-1}}\leqslant f_r(n,v,e)\leqslant C_2n^{\lceil\frac{er-v}{e-1}\rceil},$$

其中, C_1 和 C_2 是与 n 无关且仅依赖于 r、e 和 v 的数.

证明 对于上界, 设 $\mathcal{H}$ 为 (v,e)- 自由的 r- 超图, $V(\mathcal{H})=[n]$, 并记 $\lceil\frac{er-v}{e-1}\rceil=t$. 不难看出, $[n]$ 的任何一个 t- 元子集最多被 $\mathcal{H}$ 的 $e-1$ 条边所包含. 这是因为, 如果存在 $T\in\binom{[n]}{t}$ 和两两不同的 $A_1,\ldots,A_e\in\mathcal{H}$, 使得 $T\subseteq\bigcap_{i=1}^{e}A_i$, 则

$$\left|\bigcup_{i=1}^{e}A_i\right|\leqslant|T|+\sum_{i=1}^{e}|A_i\setminus T|=t+e(r-t)=er-(e-1)\left\lceil\frac{er-v}{e-1}\right\rceil\leqslant v,$$

与 $\mathcal{H}$ 的 (v,e)- 自由性质相矛盾. 通过用两种方法计算 $|\{(T,A):T\in\binom{[n]}{t},A\in\mathcal{H},T\subseteq A\}|$ 可以得到下面的不等式:

$$|\mathcal{H}|\cdot\binom{r}{t}\leqslant\binom{n}{t}\cdot(e-1).$$

为了证明下界, 我们构造如下的辅助 e- 超图 $\mathcal{F}$, 其中, $V(\mathcal{F})=\binom{[n]}{r}$, e 个不同的点 $A_1,\ldots,A_e\in\binom{[n]}{r}$ 构成 $\mathcal{F}$ 的一条边当且仅当 $|\bigcup_{i=1}^{e}A_i|\leqslant v$. 根据定义不难看出

$$\alpha(\mathcal{F})=f_r(n,v,e)\quad\text{和}\quad\mathrm{d}(\mathcal{F})\leqslant\Delta(\mathcal{F})\leqslant\binom{n-r}{v-r}\binom{v}{r}^{e-1}.$$

因此, 由引理 2.1 可知

$$f_r(n,v,e)=\alpha(\mathcal{H})\geqslant C\binom{n}{r}\cdot\binom{n-r}{v-r}^{-\frac{1}{e-1}}\cdot\binom{v}{r}^{-1}=\Omega(n^{\frac{er-v}{e-1}}).$$

证毕. □

2.2 Shangguan-Tamo 的改进型下界

由定理 2.1 下界的证明可知, 计算 $f_r(n,v,e)$ 的值等价于计算 e- 超图 $\mathcal{F}$ 的独立数. 引理 2.1 给出了任意一致超图独立数的下界, 那么对这个特殊的超图 $\mathcal{F}$ 而言, 其独立数是否存在一个更好的下界? 这个问题的答案是肯定的. 称一个超图为线性的 (linear), 如果其任意两条不同边最多包含一个公共顶点. 在 Ajtai 等 [1] 的工作基础上, Duke 等 [16] 证明了如下结论:

引理 2.2 (参见文献 [16, 定理 2]) 给定正整数 $r\geqslant3$, 则存在一个仅依赖于 r 的常数 $C:=C(r)$, 使得对于任意线性 r- 超图 $\mathcal{H}$ 都有

$$\alpha(\mathcal{H})\geqslant C|V(\mathcal{H})|\cdot\left(\frac{\log\mathrm{d}(\mathcal{H})}{\mathrm{d}(\mathcal{H})}\right)^{\frac{1}{r-1}}.$$

利用引理 2.2, Shangguan 和 Tamo [64] 证明了如下结论:

定理 2.2 (参见文献 [64, 定理 3]) 对于任意给定的正整数 $r\geqslant2$, $e\geqslant2$, $r+1\leqslant v\leqslant er-2$, 若 $\gcd(e-1,er-v)=1$, 则存在一个具有

$$\Omega(n^{\frac{er-v}{e-1}}(\log n)^{\frac{1}{e-1}})$$

条边的 r- 超图, 使得其对于所有 $2\leqslant i\leqslant e$ 都是 $(ir-\lceil\frac{(i-1)(er-v)}{e-1}\rceil,i)$- 自由的. 特别地, 令 $i=e$, 则

$$f_r(n,v,e)=\Omega(n^{\frac{er-v}{e-1}}(\log n)^{\frac{1}{e-1}}).$$

定理 2.2 有如下的推论:

命题 2.1 (参见文献 [65, 引理 2.1]) 给定正整数 $s \geqslant 1$、$r \geqslant 3$ 和 (v_i, e_i) $(1 \leqslant i \leqslant s)$, 使得 $v_i \geqslant r+1$, $e_i \geqslant 2$.

(a) 令 $h := \min\{\frac{e_i r - v_i}{e_i - 1} : 1 \leqslant i \leqslant s\}$, 则存在 r- 超图, 其具有 $\Omega(n^h)$ 条边, 且对于任意 $1 \leqslant i \leqslant s$ 都是 (v_i, e_i)- 自由的.

(b) 进一步地, 如果有 $e_1 \geqslant 3$、$\gcd(e_1 - 1, e_1 r - v_1) = 1$ 以及对于任意 $2 \leqslant i \leqslant s$ 都有

$$\frac{e_1 r - v_1}{e_1 - 1} < \frac{e_i r - v_i}{e_i - 1},$$

则存在 r- 超图, 使得其具有 $\Omega(n^{\frac{e_1 r - v_1}{e_1 - 1}} (\log n)^{\frac{1}{e_1 - 1}})$ 条边, 且对于任意 $1 \leqslant i \leqslant s$ 都是 (v_i, e_i)- 自由的.

文献 [64] 并不是直接对 e- 超图 $\mathcal{F}$ 利用引理 2.2, 而是先用概率方法挑选出 $\mathcal{F}$ 的某个具有较好性质的诱导子超图 (诱导子超图的独立集一定也是原超图的独立集), 再对该诱导子超图利用引理 2.2. 此外, 将 $v = er - (e-1)k + 1$ 代入定理 2.2 中可得 (1.10).

3 Brown-Erdős-Sós 第一猜想

本节主要介绍猜想 1.2 的研究进展. 第 3.1 小节讨论猜想 1.2 的上界, 第 3.2 小节讨论猜想 1.2 的下界. 上述两个小节分别阐述超图移除引理和加法数论是如何在猜想 1.2 的上下界的研究中发挥重要作用的.

3.1 猜想 1.2 的上界与超图移除引理

本小节的主要任务是证明猜想 1.2 的上界对所有给定的正整数 $r \geqslant k+1 \geqslant e \geqslant 3$ 都成立. 注意到 (1.3)–(1.7) 中的上界都是上述结论的特殊情形. 事实上, 这有其必然原因: 这些上界的证明分别利用了三角形移除引理 (triangle removal lemma)、图移除引理 (graph removal lemma) 以及某个特殊超图的移除引理, 而本节介绍的证明利用了最近才被证明的、完全版本的超图移除引理 (hypergraph removal lemma). 图移除引理与超图移除引理分别是图正则引理 (graph regularity lemma) 与超图正则引理 (hypergraph regularity lemma) 的推论, 相关内容是组合数学与图论的核心研究领域之一, 感兴趣的读者可参见文献 [14].

引理 3.1 (超图移除引理, 参见文献[14, 定理 1.2]) 给定正整数 $r \geqslant 2$ 与 r- 超图 $\mathcal{F}$, 对于任意 $\epsilon > 0$, 都存在 $\delta := \delta(\epsilon) > 0$, 使得对于任意 r- 超图 $\mathcal{H}$, 如果其仅包含不超过 $\delta |V(\mathcal{H})|^{|V(\mathcal{F})|}$ 个 $\mathcal{F}$ 的拷贝, 则可以从 $\mathcal{H}$ 中删去最多 $\epsilon |V(\mathcal{H})|^r$ 条边, 得到 $\mathcal{H}$ 的一个 $\mathcal{F}$- 自由的子超图.

通过超图移除引理, 容易推导出如下结论:

引理 3.2 给定正整数 $r \geqslant 2$ 与 r- 超图 $\mathcal{F}$, 对于任意 $\epsilon > 0$, 都存在 $\delta := \delta(\epsilon) > 0$ 使得如下结论成立: 如果需要删去至少 $\epsilon |V(\mathcal{H})|^r$ 条边才能使某个 r- 超图 $\mathcal{H}$ 成为 $\mathcal{F}$- 自由的, 则 $\mathcal{H}$ 一定至少包含 $\delta |V(\mathcal{H})|^{|V(\mathcal{F})|}$ 个 $\mathcal{F}$ 的拷贝.

下面将利用引理 3.2 证明猜想 1.2 的上界对于所有给定的正整数 $r \geqslant k+1 \geqslant e \geqslant 3$ 都成立.

定理 3.1 (参见文献 [32, 定理 1.3]) 对于所有给定正整数 $r \geqslant k+1 \geqslant e \geqslant 3$ 都有

$$f_r(n, er - (e-1)k + 1, e) = o(n^k).$$

证明 设 r、k 和 e 满足定理条件, $\mathcal{H}$ 是具有 n 个顶点的 $(er - (e-1)k + 1, e)$- 自由 r- 超图. 若存在某个常数 $\epsilon > 0$ 使得 $|\mathcal{H}| \geqslant \epsilon n^k$, 以下将利用引理 3.2 推导出矛盾.

首先, 不难看出, 对于任意 $A\in\mathcal{H}$, 仅存在 $\mathcal{H}\setminus\{A\}$ 的最多 $e-2$ 条边, 使得它们分别与 A 有至少 k 个交点. 否则, 存在 $e-1$ 条不同边 $A_1,\dots,A_{e-1}$ 使得对于任意 $1\leqslant i\leqslant e-1$ 都有 $|A\cap A_i|\geqslant k$, 则有

$$\left|\bigcup_{i=1}^{e-1}A_i\cup A\right|\leqslant er-(e-1)k,$$

与假设矛盾. 因此, 存在 $\mathcal{H}$ 的子超图 $\mathcal{H}'$ 满足 $|\mathcal{H}'|\geqslant\frac{\epsilon}{e-1}n^k$ 以及对于任意不同的 $A,B\in\mathcal{H}'$ 都有 $|A\cap B|\leqslant k-1$.

接下来, 通过 $\mathcal{H}'$ 构造如下的 k- 超图 $\mathcal{H}^*$ 来辅助定理的证明: 顶点集 $V(\mathcal{H}^*)$ 满足

$$V(\mathcal{H}^*)\subseteq V(\mathcal{H}')\subseteq V(\mathcal{H});$$

边集 $E(\mathcal{H}^*)$ 定义如下: 对于每条边 $A\in\mathcal{H}'$, 都构造一个 k- 超图 $K_r^k(A):=\binom{A}{k}$, 并令

$$\mathcal{H}^*=\bigcup_{A\in\mathcal{H}'}K_r^k(A).$$

容易看出, $A\in\mathcal{H}'$ 与 $K_r^k(A)\subseteq\mathcal{H}^*$ 之间是一一对应的, 而 $\mathcal{H}^*$ 由所有 $K_r^k(A)$ 的边的并形成. 此外, 对任意不同的 $A,B\in\mathcal{H}'$, k- 超图 $K_r^k(A)$ 与 $K_r^k(B)$ 是边不交的, 这是因为对于不同的 $A,B\in\mathcal{H}'$ 有 $|A\cap B|\leqslant k-1$.

我们构造了一个 k- 超图 $\mathcal{H}^*$, 它包含 K_r^k 的至少 $|\mathcal{H}'|\geqslant\frac{\epsilon}{e-1}n^k$ 个边不交的拷贝. 因此, 需要删去至少 $\frac{\epsilon}{e-1}n^k$ 条边才能使 $\mathcal{H}^*$ 变为 K_r^k- 自由的. 由引理 3.2 可知, $\mathcal{H}^*$ 包含至少 δn^r 个与 K_r^k 同构的子超图. 接下来, 估计 $\mathcal{H}^*$ 中如下 K_r^k 拷贝的数量: 它至少有两条边是同一个 $A\in\mathcal{H}'$ 的 k- 子集. 注意到以下观察:

- $A\in\mathcal{H}'$ 有至多 $O(n^k)$ 种选择;
- K_r^k 的两条边决定了其至少 $k+1$ 个顶点;
- 选定上面的 $k+1$ 个顶点之后, 其余的 $r-k-1$ 个顶点有最多 n^{r-k-1} 种选择.

因此, 上述 K_r^k 拷贝的数量至多为

$$|\mathcal{H}'|\cdot\binom{\binom{r}{k}}{2}\cdot n^{r-k-1}=O(n^{r-1}),$$

在 n 充分大时远小于 δn^r.

综上所述, 一定存在一个 $K_r^k\subseteq\mathcal{H}^*$, 它的 $\binom{r}{k}$ 条 k- 边来自于 $\mathcal{H}'$ 的 $\binom{r}{k}$ 条不同的 r- 边. 特别地, 对于 $r\geqslant k+1\geqslant e$, 总是存在 $K_{k+1}^k\subseteq K_r^k$. 取任意这样一个 K_{k+1}^k 的 e 条不同边, 记作 $B_1,\dots,B_e$. 设 $A_1,\dots,A_e$ 为 $\mathcal{H}'$ 中与它们对应的 e 条边, 满足 $B_i\subseteq A_i$ $(1\leqslant i\leqslant e)$. 则由 $|\bigcup_{i=1}^e B_i|\leqslant k+1$ 可知,

$$\left|\bigcup_{i=1}^{e}A_i\right|\leqslant re-(ek-(k+1))=e(r-k)+k+1,$$

这与 $\mathcal{H}'$ 的 $(er-(e-1)k+1,e)$- 自由性质矛盾. 证毕. □

3.2 猜想 1.2 的下界与加法数论

本小节首先介绍加法数论中重要的 sum-free (求和 - 自由) 集; 再介绍利用求和 - 自由集构造稀疏超图的一般思想 (实际上, 利用该方法求和 - 自由集也可以被用来构造不含其他禁止构型的超图); 最后以 Ruzsa 和 Szemerédi [59] 的经典构造为例, 具体给出 (1.3) 下界的证明.

设 s 为正整数, 考虑线性方程 $\sum_{i=1}^{s} a_i x_i = 0$, 其中系数 $a_1, \ldots, a_s$ 与未知数 $x_1, \ldots, x_s$ 均为整数. 如果 $\sum_{i=1}^{s} a_i = 0$, 则称该方程为齐次线性方程. 此时, 不难看出 $x_1 = \cdots = x_s$ 为方程的一组解, 称这组解为平凡解. 对于集合 $M \subseteq [n]$, 如果对于任意满足 $\sum_{i=1}^{s} a_i m_i = 0$ 的 $m_1, \ldots, m_s \in M$ 都有 $m_1 = \cdots = m_s$, 则称 M 不含上述方程的非平凡解. 关于非平凡解的定义实际上是 Ruzsa[58] 原始定义的一个简化版本.

1947 年, Behrend[6] 考虑了不含方程 $x_1 + x_2 = 2x_3$ 非平凡解的集合, 这类集合也被称为是不含 3 长等差数列的集合 (3-term-arithmetic-progression-free), 这是由于上述方程的非平凡解实际上构成 3 长等差数列 x_1、x_3 和 x_2. 记 $r_k(n)$ 为 $[n]$ 的不含 k 长等差数列的最大子集的大小. Behrend[6] 证明了

$$r_3(n) > \frac{n}{2^{O(\sqrt{\log n})}} = n^{1-o(1)}. \tag{3.1}$$

目前, $r_k(n)$ 上下界的估计是加法数论的核心问题, 相关研究利用了多种数学工具.

如何利用求和 - 自由集来构造稀疏超图? 给定正整数 $r \geqslant 3$ 和求和 - 自由集合 $M \subseteq [n]$, 可以按如下方式构造一个 r- 部 r- 超图 $\mathcal{H}$, 它的顶点集为 $V(\mathcal{H}) = \bigcup_{i=1}^{r} V_i$, 每个 V_i 都是正整数集, 边集为

$$\mathcal{H} = \{A(y,m) : A(y,m) = (y + b_1 m, \ldots, y + b_r m), y \in [n], m \in M\},$$

其中, $A(y,m)$ 是一个有序的 r- 元组, 使得对于每个 $1 \leqslant i \leqslant r$ 都有 $y + b_i m \in V_i$, $\mathcal{B} := \{b_1, \ldots, b_r\} \subseteq [n]$ 是一个 r- 元整数集合, 它是依据集合 $M \subseteq [n]$ 的求和 - 自由性质来设计的. 容易验证如下结论:

引理 3.3 如果对于任意 $i \neq j$ 都有 $b_i \neq b_j$, 则按照上面的方式构造的超图 $\mathcal{H}$ 是一个有 $n|M|$ 条边的线性超图.

证明 不难看出 $|\mathcal{H}| = n|M|$, 只需证明其任意两条不同边最多有一个公共点. 如若不然, 假设对 $(y,m) \neq (y',m')$ 有 $|A(y,m) \cap A(y',m')| \geqslant 2$, 则存在 $1 \leqslant i, j \leqslant r$ $(i \neq j)$ 使得

$$\begin{cases} y + b_i m = y' + b_i m', \\ y + b_j m = y' + b_j m'. \end{cases}$$

则 $y - y' = b_i(m' - m) = b_j(m' - m)$, 这意味着 $(y,m) = (y',m')$, 与假设矛盾. □

下面给出 Ruzsa 和 Szemerédi[59] 利用不含 3 长等差数列的正整数集合来构造 $(6,3)$- 自由 3- 超图的经典证明.

定理 3.2[59] $f_3(n,6,3) = \Omega(n \cdot r_3(n)) > n^{2-o(1)}$.

证明 设 $M \subseteq [n]$ 不含 3 长的等差数列. 按照如下方式构造一个 3- 部 3- 超图 $\mathcal{H}$, 它的顶点集为 $V(\mathcal{H}) = \bigcup_{i=1}^{3} V_i$, 其中对于每个 $V_i = [i \cdot n]$ $(1 \leqslant i \leqslant 3)$, 它的边集为

$$\mathcal{H} = \{A(y,m) : A(y,m) = (y, y + m, y + 2m), y \in [n], m \in M\},$$

并且满足对于 $1 \leqslant i \leqslant 3$ 有 $y + (i-1)m \in V_i$. 由 (3.1) 可知, 要证明上述命题, 只需证明 $\mathcal{H}$ 是 $(6,3)$- 自由的. 如若不然, 则存在 3 条不同边 $A_1 = A(y_1, m_1)$, $A_2 = A(y_2, m_2)$, $A_3 = A(y_3, m_3) \in \mathcal{H}$ 使得

$$\left| \bigcup_{i=1}^{3} A_i \right| \leqslant 6. \tag{3.2}$$

由引理 3.3 可知, 对于任意 $i \neq j$ 有 $|A_i \cap A_j| \leqslant 1$. 因此 (3.2) 成立当且仅当对于任意 $i \neq j$ 有 $|A_i \cap A_j| = 1$. 由于 $\mathcal{H}$ 是 3- 部超图, 不失一般性, 假设

$$A_1 \cap A_2 \in V_1, \quad A_2 \cap A_3 \in V_2, \quad A_1 \cap A_3 \in V_3,$$

则有

$$\begin{cases} y_1 = y_2, \\ y_2 + m_2 = y_3 + m_3, \\ y_3 + 2m_3 = y_1 + 2m_1, \end{cases}$$

将 3 个等式左右两边分别相加再消去 y_1、y_2 和 y_3, 可得 $m_2 + m_3 = 2m_1$. 根据假设可知, M 不含 3 长等差数列, 因而有 $m_1 = m_2 = m_3$, 代入上述方程组可得 $(y_1, m_1) = (y_2, m_2) = (y_3, m_3)$, 与假设矛盾. 综上所述, $\mathcal{H}$ 确实是 $(6,3)$- 自由的. 证毕. □

为了利用求和 - 自由集构造不含其他禁止构型的组合结构, 人们从多个角度对 Behrend[6] 的构造进行了推广. 例如, 利用 Behrend 的构造方法, 容易证明如下更为一般的结果:

引理 3.4 (参见文献 [32, 引理 3.4]) 设 $s \geqslant 2, a_1, \ldots, a_s, n$ 全为正整数, 其中 s 是固定的, 而 $a_1, \ldots, a_s$ 可以随 n 变动, 则存在一个集合 $M \subseteq [n]$ 满足 $|M| \geqslant \frac{n}{2^{O(\sqrt{\log n \log \sum_{i=1}^{l} a_l})}}$, 且不含下述方程的非平凡解:

$$\sum_{i=1}^{s} a_i x_i = \left(\sum_{i=1}^{s} a_i\right) x_{s+1}.$$

我们还可以证明, 存在一个充分大的集合 $M \subseteq [n]$, 使得其不含多个方程的非平凡解.

引理 3.5 (参见文献 [32, 引理 3.7]) 令 $0 < a < 1$ 为一个给定的常数, t 为一个给定的正整数. 令

$$\sum_{i=1}^{s} a_{ij} x_i = 0, \quad 1 \leqslant j \leqslant t$$

为 t 个齐次线性方程. 如果对于 $j = 1, \ldots, t$, 都存在集合 $M_j \subseteq [n]$, 使得 $|M_j| \geqslant \frac{n}{2^{O(\log^a n)}}$ 且其不含第 j 个方程的非平凡解, 则存在一个集合 $M \subseteq [n]$, 使得 $|M| \geqslant \frac{n}{2^{O(\log^a n)}}$ 且其不含上述任意一个方程的非平凡解.

更多的相关推广可参见文献 [2,4,30,32,58,62]. 正是利用各种不同的求和 - 自由集及其构造, Alon 和 Shapira[4] 证明了对于所有 $r > k \geqslant 2$ 和 $e = 3$ 都有

$$f_r(n, 3r - 2k + 1, 3) > n^{k - o(1)}.$$

Ge 和 Shangguan[32] 证明了对于所有 $r > k = 2$ 和 $e \in \{4, 5, 7, 8\}$ 都有

$$f_r(n, r - 2e + 3, e) > n^{2 - o(1)}.$$

文献 [32] 实际上证明了如下更强的结论:

定理 3.3 (参见文献 [32, 定理 1.6, 1.7]) 对于任意给定正整数 $r \geqslant 3$ 和 $n \to \infty$, 存在一个线性的 r- 部 r- 超图 $\mathcal{H}$, 使得 $|\mathcal{H}| > n^{2 - o(1)}$, 并且对于所有 $e \in \{3, 4, 5, 7, 8\}$, $\mathcal{H}$ 都是 $(er - 2e + 3, e)$- 自由的.

4 Brown-Erdős-Sós 第二猜想

本节主要介绍猜想 1.3 的研究进展. 第 4.1 小节给出 (1.13) 上界的证明, 注意到, 该上界蕴含了 (1.11) 和 (1.12) 的上界; 第 4.2 小节给出 (1.11) 下界的证明, 并讨论证明 (1.12) 下界的一些主要想法.

4.1 猜想 1.3 的上界

本小节证明 (1.13) 的上界部分, 注意到, (1.11) 和 (1.12) 的上界部分都是其简单的推论.

定理 4.1 (参见文献 [63, 定理 6]) 对于给定的正整数 $r > k \geqslant 2$, 有

$$\limsup_{n\to\infty} \frac{f_r(n, 3r-2k, 3)}{n^k} \leqslant \frac{1}{k!\binom{r}{k} - \frac{k!}{2}}.$$

我们需要如下引理. 令 $\mathcal{H} \subseteq \binom{[n]}{r}$ 为一个 r- 超图, $T \subseteq [n]$ 是一个子集, T 在 $\mathcal{H}$ 中的度数 $\mathrm{d}_{\mathcal{H}}(T)$ 为 $\mathcal{H}$ 中包含 T 的边数, 即 $\mathrm{d}_{\mathcal{H}}(T) = |\{A \in \mathcal{H} : T \subseteq A\}|$.

引理 4.1 (参见文献 [63, 引理 12]) 任给一个 r- 超图 $\mathcal{H}$, 我们都可以删去它的最多 $\binom{n}{k-1}$ 条边, 得到一个子超图 $\mathcal{F} \subseteq \mathcal{H}$, 使得 $\mathcal{F}$ 不含度数为 1 的 $(k-1)$- 子集.

定理 4.1 的证明 令 $\mathcal{H}$ 为任意 $(3r-2k, 3)$- 自由的 r- 超图, $\mathcal{F}$ 为 $\mathcal{H}$ 的子超图, 并满足引理 4.1 的结论. 因此, $|\mathcal{H}| \leqslant |\mathcal{F}| + \binom{n}{k-1}$. 要证明定理 4.1, 只需要证明

$$|\mathcal{F}| \leqslant \frac{2\binom{r}{k}}{2\binom{r}{k}-1}\frac{\binom{n}{k}}{\binom{r}{k}}.$$

由于 $\mathcal{F}$ 是 $(3r-2k, 3)$- 自由的, 所以 $[n]$ 的任意 k- 子集在 $\mathcal{F}$ 中的度数最多为 2. 对于 $i \in \{1, 2\}$, 令 $\mathcal{K}_i \subseteq \binom{[n]}{k}$ 为 $[n]$ 中度数为 i 的 k- 子集构成的集合, 即

$$\mathcal{K}_i = \left\{K \in \binom{[n]}{k} : \mathrm{d}_{\mathcal{F}}(K) = i\right\}.$$

因此, 对于任意 $A \in \mathcal{F}$ 和 $K \in \binom{A}{k}$, 都有 $K \in \mathcal{K}_1$ 或者 $K \in \mathcal{K}_2$. 由上面的讨论不难证明

$$\binom{r}{k}|\mathcal{F}| = |\mathcal{K}_1| + 2|\mathcal{K}_2|. \tag{4.1}$$

对于 $K = \{x_1, \ldots, x_k\} \in \mathcal{K}_2$, 设 A 和 B 为 $\mathcal{F}$ 中包含 K 的两条边, 因此 $|A \cap B| \geqslant k$. 我们声明, 实际上有 $|A \cap B| = k$. 取 $a \in A \setminus B$, 考虑 $(k-1)$- 子集 $\{x_1, \ldots, x_{k-2}, a\} \subseteq A$. 由于 $\mathcal{F}$ 不含度数为 1 的 $(k-1)$- 子集, $\mathrm{d}_{\mathcal{F}}(\{x_1, \ldots, x_{k-2}, a\}) \geqslant 2$, 所以存在一条边 $C \in \mathcal{F} \setminus \{A, B\}$ 使得 $\{x_1, \ldots, x_{k-2}, a\} \subseteq C$. 若 $|A \cap B| \geqslant k+1$, 则有

$$|A \cup B \cup C| \leqslant 3r - |A \cap B| - |A \cap C| \leqslant 3r - (k+1) - (k-1) = 3r - 2k, \tag{4.2}$$

与假设矛盾.

对于 k- 子集 $K \in \mathcal{K}_2$ 以及包含它的两条边 $A, B \in \mathcal{F}$, 定义集合 $\Phi_K := (\binom{A}{k} \cup \binom{B}{k}) \setminus \{K\}$. 由于 $|A \cap B| = k$, 所以有

$$|\Phi_K| = 2\binom{r}{k} - 2. \tag{4.3}$$

类似 (4.2), 可以证明

$$\Phi_K \subseteq \mathcal{K}_1. \tag{4.4}$$

我们声明如下结论成立.

声明 4.1 对于任意不同的 $K, K' \in \mathcal{K}_2$, 都有 $\Phi_K \cap \Phi_{K'} = \emptyset$.

假设上述结论是正确的, 由 (4.3) 和 (4.4) 可知

$$|\mathcal{K}_2| \left(2\binom{r}{k} - 2\right) \leqslant |\mathcal{K}_1|. \tag{4.5}$$

此外, 容易看出

$$|\mathcal{K}_1| + |\mathcal{K}_2| \leqslant \binom{n}{k}. \tag{4.6}$$

结合 (4.1)、(4.5) 和 (4.6) 可知

$$\begin{aligned}
\binom{r}{k}|\mathcal{F}| &= |\mathcal{K}_1| + 2|\mathcal{K}_2| \\
&= \frac{2\binom{r}{k}}{2\binom{r}{k}-1}(|\mathcal{K}_2| + |\mathcal{K}_1|) + \frac{1}{2\binom{r}{k}-1}\left(\left(2\binom{r}{k} - 2\right)|\mathcal{K}_2| - |\mathcal{K}_1|\right) \\
&\leqslant \frac{2\binom{r}{k}}{2\binom{r}{k}-1}(|\mathcal{K}_2| + |\mathcal{K}_1|) \\
&\leqslant \frac{2\binom{r}{k}}{2\binom{r}{k}-1}\binom{n}{k}.
\end{aligned}$$

证毕.

接下来, 用反证法证明声明 4.1. 如果存在两个不同的 k- 子集 $K, K' \in \mathcal{K}_2$ 使得 $\Phi_K \cap \Phi_{K'} \neq \emptyset$, 则存在 $A' \in \mathcal{F}$ 使得 $K, K' \subseteq A'$ (否则, 与 (4.4) 矛盾). 假设 $B', C' \in \mathcal{F}$ 为满足 $A' \cap B' = K$ 和 $A' \cap C' = K'$ 的两条边, 则有

$$|A' \cup B' \cup C'| \leqslant 3r - |A' \cap B'| - |A' \cap C'| = 3r - 2k,$$

与假设矛盾. □

4.2 猜想 1.3 的下界与图填充

本小节的目标是证明如下结论:

定理 4.2 (参见文献 [34, 定理 2]) $\lim_{n\to\infty} \frac{f_3(n,5,3)}{n^2} = \frac{1}{5}$.

定理 4.2 的上界是定理 4.1 在 $r = 3$ 且 $k = 2$ 时的推论, 下面证明其下界. 该证明是由 Glock [34] 给出的, 他巧妙地利用了图填充研究领域中的一个著名结果. 考虑两个图 H 和 G, G 的一个 H- 填充 (H-packing) 是指 G 的一族两两边不交 (edge-disjoint) 的子图 $H_1, H_2, \ldots$, 其中每个 H_i 都是 H 的拷贝. 显然, G 的任意 H- 填充最多能包含 $\frac{|G|}{|H|}$ 个两两边不交的 H 的拷贝. 下面的结论说明, 该上界对于 $G = K_n$ 是渐近最优的.

引理 4.2 (参见文献 [53, 定理 1.1]) 任给图 H 以及常数 $\epsilon > 0$, 存在一个常数 $n_0 = n_0(H, \epsilon)$, 使得对于任意 $n > n_0$, K_n 都有一个大小至少为 $(1-\epsilon)\frac{n^2}{2|H|}$ 的 H- 填充.

为了利用引理 4.2 来证明定理 4.2, Glock [34] 定义了一个特殊的图 H_t. 对于 $t \in \mathbb{Z}^+$, 定义 $H_t = (V(H_t), E(H_t))$ 的顶点集为 $V(H_t) = \{a, b, x_1, \ldots, x_t, y_1, \ldots, y_t\}$, 边集为

$$H_t = \{ab\} \cup \{ax_i, ay_i, bx_i, by_i, x_iy_i : 1 \leqslant i \leqslant t\}.$$

不难看出, $|H_t| = 5t+1$. 为了利用 K_n 的 H_t- 填充来构造达到定理 4.2 下界的 $(5,3)$- 自由 3- 超图, Glock 在顶点集 $V(H_t)$ 上定义了如下的 3- 超图:

$$\hat{H}_t = \{ax_iy_i, bx_iy_i : 1 \leqslant i \leqslant t\}.$$

显然, $|\hat{H}_t| = 2t$. 不难验证如下结论:

引理 4.3 $\hat{H}_t$ 是 $(5,3)$- 自由的.

记 $H_t^{(1)}, \ldots, H_t^{(m)}$ 为满足引理 4.2 的一个 H_t- 填充, 则 $m \geqslant (1-\epsilon)\frac{n^2}{10t+2}$. 相应地, 可以构造 3- 超图 $\hat{H}_t^{(1)}, \ldots, \hat{H}_t^{(m)}$. 考虑这 m 个 3- 超图的并

$$\mathscr{H}_t := \bigcup_{i=1}^{m} \hat{H}_t^{(i)}.$$

引理 4.4 $\mathscr{H}_t$ 是 $(5,3)$- 自由的 3- 超图, 且 $|\mathscr{H}_t| = 2tm$.

证明 首先证明 $|\mathscr{H}_t| = 2tm$. 根据定义可知, 对于任意 $1 \leqslant i < j \leqslant m$, $H_t^{(i)}$ 与 $H_t^{(j)}$ 都是边不交的. 由此不难看出, $\hat{H}_t^{(i)}$ 与 $\hat{H}_t^{(j)}$ 也是边不交的. 由于对于任意 $1 \leqslant i \leqslant m$ 都有 $|\hat{H}_t^{(i)}| = 2t$, 因此有

$$|\mathscr{H}_t| = \sum_{i=1}^{m} |\hat{H}_t^{(i)}| = 2mt.$$

下面证明 $\mathscr{H}_t$ 是 $(5,3)$- 自由的. 如若不然, 假设存在 3 条不同边 $A_1, A_2, A_3 \in \mathscr{H}_t$, 使得 $|\bigcup_{j=1}^{3} A_j| \leqslant 5$ 以及对于 $1 \leqslant j \leqslant 3$ 有 $A_j \in \hat{H}_t^{(i_j)}$, 其中 $1 \leqslant i_1, i_2, i_3 \leqslant m$. 由 $|\bigcup_{j=1}^{3} A_j| \leqslant 5$ 不难看出, A_1、A_2 和 A_3 中一定有两条边恰好包含两个交点, 不妨假设 $|A_1 \cap A_2| = 2$. 因此, $H_t^{(i_1)}$ 与 $H_t^{(i_2)}$ 至少有一条公共边. 当 $i_1 \neq i_2$ 时, $H_t^{(i_1)}$ 与 $H_t^{(i_2)}$ 是边不交的 H_t 拷贝, 所以只能有 $i_1 = i_2$.

由于 $|A_1 \cup A_2| = 4$ 且 $|\bigcup_{j=1}^{3} A_j| \leqslant 5$, 不难看出 $|A_3 \cap (A_1 \cup A_2)| \geqslant 2$, 由此可以推导得到 $H_t^{(i_3)}$ 与 $H_t^{(i_1)}$ 至少有一条公共边, 因此有 $i_3 = i_1$.

综上所述, $A_1, A_2, A_3 \in \hat{H}_t^{(i_1)}$ 且 $|\bigcup_{j=1}^{3} A_j| \leqslant 5$, 与引理 4.3 矛盾. 证毕. □

定理 4.2 下界的证明 对于任意常数 $\epsilon > 0$, 对 H_t 应用引理 4.2, 得到对于充分大的 n, 存在大小至少为 $(1-\epsilon)\frac{n^2}{10t+2}$ 的 H_t- 填充. 由引理 4.4 可知, 应用该 H_t- 填充可以构造出边数至少为 $(1-\epsilon)\frac{n^2}{10t+2}\cdot 2t$ 的 $(5,3)$- 自由 3- 超图. 当 t 充分大时, 该超图边数趋近于 $(1-o(1))\frac{n^2}{5}$. 证毕. □

Shangguan 和 Tamo [63] 将定理 4.2 的结果从 $r=3$, $e=3$, $k=2$ 推广到更一般的 $r \geqslant 3$, $e=3$, $k=2$. 对于任意 $\epsilon > 0$, 他们都构造了边数为 $(1-\epsilon)\frac{n^2}{r^2-r-1}$ 的 $(3r-4,3)$- 自由 r- 超图. 文献 [63] 的构造实际上是一个关于 r 的递归构造, 其初始情形是 Glock 在 $r=3$ 时的构造. 文献 [63] 利用了如下比引理 4.2 更强的结论:

引理 4.5 (参见文献 [28, 定理 2.2] 和 [5, 定理 3.2]) 任给图 H 以及常数 $\epsilon > 0$, 存在一个常数 $n_0 = n_0(H, \epsilon)$, 使得对于任意 $n > n_0$, K_n 都有一个 H- 填充 $H^{(1)}, \ldots, H^{(m)}$, 使得 $m \geqslant (1-\epsilon)\frac{n^2}{2|H|}$, 并同时具有如下两个性质:

(i) 对于任意 $1 \leqslant i \neq j \leqslant m$, $H^{(i)}$ 与 $H^{(j)}$ 至多有两个公共顶点;

(ii) 如果对于某对 $1 \leqslant i \neq j \leqslant m$, $H^{(i)}$ 与 $H^{(j)}$ 恰好有两个公共顶点 $\{a,b\}$, 则 $\{a,b\}$ 既不是 $H^{(i)}$ 的边, 也不是 $H^{(j)}$ 的边.

人们也称满足上述两个性质的 H- 填充为 H 的诱导图填充. 显然, 引理 4.5 是引理 4.2 的加强版本, 能否进一步发掘引理 4.5 以构造其他参数的稀疏超图, 是一个非常值得研究的问题.

5 稀疏超图与极值组合

本节介绍稀疏超图在极值组合中的两个应用. 第 5.1 小节介绍如何利用稀疏超图来构造可分与完美哈希矩阵, 第 5.2 小节介绍如何利用稀疏超图来构造可消去超图与求并 - 自由超图.

5.1 可分与完美哈希矩阵

设 Q 为 q- 元有限集, M 为定义在 Q 上的 $r\times m$ q- 元矩阵. 对于 M 的任意行 f 与任意列子集 C, 用 $f(C)\subseteq Q$ 表示 C 中的每一列在行 f 上的取值所构成的集合. 给定 t 个正整数 $w_1,\dots,w_t$, 称矩阵 M 为 $\{w_1,\dots,w_t\}$- 可分 (separating) 的, 如果对于任意 t 个两两不交的、满足 $|C_i|=w_i$ $(1\leqslant i\leqslant t)$ 的列子集 $C_1,\dots,C_t$, 都存在 M 的某一行 g 使得 $g(C_1),\dots,g(C_t)$ 也是两两不交的 (作为 Q 的子集). 注意到, 这里 $\{w_1,\dots,w_t\}$ 可以为一个多重集. 为了叙述方便, 称上述矩阵为 $(r,m,q,\{w_1,\dots,w_t\})$- 可分哈希矩阵 (separating Hash matrix). 在文献中, 可分哈希矩阵与所谓的可分哈希族 (separating Hash family) [74] 是等价的, 它看作是可分哈希族的矩阵表示.

可分哈希矩阵是一种基本的组合构型, 不同参数的可分哈希矩阵蕴涵了丰富的组合结构. 下面是部分例子.

• 当 $w_1=\cdots=w_t=1$ 时, $(r,m,q,\{1,\dots,1\})$- 可分哈希矩阵也被称为 t- 完美哈希族 (perfect Hash family) 或者 t- 完美哈希矩阵 (perfect Hash matrix). 完美哈希族由 Mehlhorn [50] 在 1984 年定义, 它在密码学 [75,82]、数据库管理 [50]、环路设计 [52] 和算法设计 [3] 中都有重要应用.

• Elias [18] 考虑了满足 $t=q,w_1=\cdots=w_q=1$ 时的完美哈希矩阵, 它可以被应用于一种零错误列表译码信道 (即所谓的 $q/(q-1)$ 信道).

• 当 $t=2$, $w_1=1$, $w_2=w\geqslant 2$ 时, $(r,m,q,\{1,w\})$- 可分哈希矩阵等价于 w- 防诬陷码 (frameproof code); 当 $t=2$, $w_1=w_2=w\geqslant 2$ 时, $(r,m,q,\{w,w\})$- 可分哈希矩阵等价于 w- 安全防诬陷码 (secure frameproof code). 防诬陷码与安全防诬陷码分别由 Boneh 和 Shaw [11] 以及 Stinson 等 [73] 定义, 这两种码都是所谓的指纹码 (fingerprinting codes), 可以用来保护正版信息.

• 同时满足 $\{1,1,1\}$ 与 $\{2,2\}$ 两种可分性质的可分哈希矩阵被称为父代识别码 (parent-identifying codes), 该码也属于指纹码, 可以被用来追踪盗版者 (参见文献 [40]).

值得一提的是, 朱烈在相关问题的研究中取得了出色的成果. Stinson 等 [75] 利用正交表 (orthogonal array) 与递归构造给出了几类完美哈希矩阵的确定性构造; 利用类似的方法, 他们还构造出几类新的可分哈希矩阵, 并将其应用于可分系统 (separating systems)、密钥分发模式 (key distribution patterns)、组合群试算法 (group testing algorithms)、覆盖 - 自由 (cover-free) 集族和安全防诬陷码等组合对象的构造. 此外, Stinson 等 [76] 给出了 (w,r)- 覆盖 - 自由集族大小的两个新上界, (w,r)- 覆盖 - 自由集族与完美哈希矩阵等组合结构联系紧密, 在组合群试和追踪方案中都有重要应用.

对于正整数 $r,q,w_1,\dots,w_t$, 用 $C(r,q,\{w_1,\dots,w_t\})$ 表示最大的 m, 使得存在 $(r,m,q,\{w_1,\dots,w_t\})$- 可分哈希矩阵. 人们对 $C(r,q,\{w_1,\dots,w_t\})$ 上下界的研究主要有以下两个方向: (1) 给定 $q,t,w_1,\dots,w_t$, 令 r 趋于无穷大; (2) 给定 $r,t,w_1,\dots,w_t$, 令 q 趋于无穷大. 本文主要关心第二种情形, 此时, 人们发现可分哈希矩阵 (尤其是完美哈希矩阵) 与稀疏超图具有紧密联系. 因此研究 $f_r(n,v,e)$ 上下界的重要方法都可以被用来研究 $C(r,q,\{w_1,\dots,w_t\})$ 的上下界. 下面简述相关研究成果.

为了方便, 本节总是记 $u=\sum_{i=1}^t w_i$, Shangguan 和 Ge [62] 证明了 $C(r,q,\{w_1,\dots,w_t\})$ 满足如下的迭代不等式:

引理 5.1 (参见文献 [62, 引理 3.1]) 对于任意正整数 $1 \leqslant \ell \leqslant r$ 和 $1 \leqslant i \leqslant t$, 有

$$C(r,q,\{w_1,\ldots,w_t\}) \leqslant q^{\ell} + \max\{u-1, C(r-\ell,q,\{w_1,\ldots,w_i-1,\ldots,w_t\})\}.$$

利用引理 5.1 可以得出 $C(r,q,\{w_1,\ldots,w_t\})$ 的上界:

定理 5.1 (参见文献 [62, 定理 1.5]) 设 $1 \leqslant c \leqslant u-1$ 为满足 $r \equiv c \pmod{u-1}$ 的唯一正整数, 则有

$$C(r,q,\{w_1,\ldots,w_t\}) \leqslant \max\{u, cq^{\lceil r/(u-1)\rceil} + (u-1-c)q^{\lfloor r/(u-1)\rfloor}\}.$$

对于下界, 当 $w_1 = \cdots = w_t = 1$ 时, 简记 $C(r,q,\{1,\ldots,1\}) := p_t(r,q)$. 根据定义不难看出, $C(r,q,\{w_1,\ldots,w_t\}) \geqslant p_u(r,q)$. Blackburn[7] 利用 Lovász 局部引理证明了存在一个仅依赖于 t 和 r 的数 $c_{t,r}$, 使得 $p_t(r,q) \geqslant c_{t,r}q^{\frac{r}{t-1}}$. 结合以上讨论可知, 给定 $r,t,w_1,\ldots,w_t$, 当 q 充分大时有

$$\Omega(q^{\frac{r}{u-1}}) = C(r,q,\{w_1,\ldots,w_t\}) = O(q^{\lceil\frac{r}{u-1}\rceil}). \tag{5.1}$$

由 (1.1) 与 (5.1) 不难看出, $C(r,q,\{w_1,\ldots,w_t\})$ 的上下界与 $f_r(n,v,e)$ 的上下界具有相似的特性, 即能否利用初等方法得到渐近阶当且仅当相关参数是否满足某种整除性条件 (实际上, 这种现象会在本文中多次出现).

利用声明 1.1 所提到的矩阵与多部超图的等价关系, Shangguan 和 Ge[62] 证明了下述结论:

定理 5.2 (参见文献 [62, 定理 5.4、6.5、7.1 和推论 7.2]) (i) $p_3(3,q) = f_3(3q,6,3) + O(q)$, 因而对于充分大的 q 有 $q^{2-o(1)} < p_3(3,q) = o(q^2)$;

(ii) 对于充分大的 q 有 $q^{2-o(1)} < p_4(4,q) = o(q^2)$;

(iii) 记 $u = \sum_{i=1}^{t} w_i$, 则有 $\Omega(f_r(rq, ur-r, u)) = p_u(r,q) \leqslant C(r,q,\{w_1,\ldots,w_t\})$;

(iv) 当 $2 \nmid r$ 且 $r \geqslant 3$ 时有 $p_3(r,q) > q^{\lceil\frac{r}{2}\rceil - o(1)}$ (利用 (iii) 和 (1.5)).

结合引理 5.1 和定理 5.2(i) 和 5.2(ii), Ge 等[33] 证明了下述结论:

定理 5.3 (参见文献 [33, 定理 4.1]) 给定正整数 $t \geqslant 3, w_1,\ldots,w_t \geqslant 2$, 当 $t \geqslant 3$ 或者 $t = 2$ 且 $\min\{w_1,w_2\} \geqslant 2$ 时, 对于充分大的 q 有 $C(\sum_{i=1}^{t} w_i, q, \{w_1,\ldots,w_t\}) = o(q^2)$.

注意到定理 5.3 对于 $t = 2$ 以及 $\{w_1,w_2\} = \{1,w\}$ 不成立. 实际上, 当 q 为素数幂且 $q \geqslant r$ 时, 利用 Reed-Solomon 码容易构造出 $(r, q^{\lceil\frac{r}{w}\rceil}, q, \{1,w\})$- 可分哈希矩阵 (即 w- 防诬陷码)[8], 因此可知对于充分大的 q 有 $C(r,q,\{1,w\}) = \Omega(q^{\lceil\frac{r}{w}\rceil})$.

利用定理 5.2(iii), 可以得出关于可分哈希矩阵以及完美哈希矩阵最大列数的新下界:

定理 5.4 (i) 当 $\gcd(r,u-1) = 1$ 时有 $C(r,q,\{w_1,\ldots,w_t\}) \geqslant p_u(r,q) = \Omega(q^{\frac{r}{u-1}}(\log q)^{\frac{1}{u-1}})$;

(ii) 当 $u \in \{3,4,5,7,8\}$ 时有 $p_u(2u-3,q) > q^{2-o(1)}$.

证明 定理 5.4 中的两个结论分别是定理 2.2 与 3.3 的两个推论. □

不难看出定理 5.4 在某些参数下改进了 (5.1) 的下界.

5.2 可消去与求并 - 自由超图

设 t 为正整数, $\mathcal{H}$ 为 r- 超图, 如果对于任意 $t+2$ 条不同边 $A_1,\ldots,A_t,B,C \in \mathcal{H}$, 都有

$$\left(\bigcup_{i=1}^{t} A_i\right) \cup B \neq \left(\bigcup_{i=1}^{t} A_i\right) \cup C,$$

则称 $\mathcal{H}$ 为 t- 可消去的. 如果对于任意两个满足 $1\leqslant|\mathcal{A}|,|\mathcal{B}|\leqslant t$ 的集合 $\mathcal{A},\mathcal{B}\subseteq\mathcal{H}$, 都有

$$\bigcup_{A\in\mathcal{A}}A\neq\bigcup_{B\in\mathcal{B}}B,$$

则称 $\mathcal{H}$ 为 t- 求并 - 自由的. t- 可消去与 t- 求并 - 自由的 r- 超图都是极值组合与极值集合论的经典研究对象. 本小节将介绍如何利用稀疏超图构造满足上述性质的 r- 超图.

1- 可消去与 2- 求并 - 自由超图的研究分别始于 Katona[42] 以及 Erdős 和 Moser[23] 的工作, 而一般参数下 t- 可消去与 t- 求并 - 自由超图的研究则分别始于 Füredi[29] (关于 2- 可消去超图, 也可参见文献 [47]) 以及 Kautz 和 Singleton[44] 的工作.

当 $t\geqslant3$ 时, 人们关于 t- 可消去与 t- 求并 - 自由超图的知识大多源自另一种组合结构, 即覆盖 - 自由超图. 称 r- 超图 $\mathcal{H}$ 是 t- 覆盖 - 自由的, 如果对于任意 $t+1$ 条不同边 $A_1,\dots,A_t,B\in\mathcal{H}$, 都有

$$B\nsubseteq\bigcup_{i=1}^{t}A_i.$$

t- 覆盖 - 自由超图由 Erdős 等[20,21] 引入 (关于其另一种定义, 参见文献 [44]). 不难得到覆盖 - 自由超图与可消去超图以及求并 - 自由超图的如下关系 (以下 (a) 的证明可参见文献 [29, 定理 3.2]; (b) 可以直接由定义推导出来):

(a) 如果超图 $\mathcal{H}$ 是 $(t+1)$- 覆盖 - 自由的, 则它也是 t- 可消去的; 如果 $\mathcal{H}$ 是 t- 可消去的, 则存在一个 $\mathcal{H}$ 的子超图, 使得它有至少 $|\mathcal{H}|-(1+\lfloor\frac{t}{2}\rfloor)$ 条边, 并且是 $\lfloor\frac{t}{2}\rfloor$- 覆盖 - 自由的.

(b) 如果 $\mathcal{H}$ 是 t- 覆盖 - 自由的, 则它也是 t- 求并 - 自由的; 如果 $\mathcal{H}$ 是 t- 求并 - 自由的, 则它也是 $(t-1)$- 覆盖 - 自由的.

以下总是假设 r 和 t 是给定的正整数, n 趋于无穷大. 分别用 $F_t(n,r)$、$C_t(n,r)$ 和 $U_t(n,r)$ 表示定义在 n 个顶点上的 t- 覆盖 - 自由、t- 可消去以及 t- 求并 - 自由的 r- 超图能够包含的最大边数. Frankl 和 Füredi[28] 证明了, 对于所有 r 和 t 有

$$F_t(n,r)=(\gamma(r,t)+o(1))n^{\lceil\frac{r}{t}\rceil},\tag{5.2}$$

其中 $\gamma(r,t)$ 是仅依赖于 r 和 t 的常数. 由上面的观察 (a)、(b) 以及 (5.2) 可知 (参见文献 [30, (10)] 和 [29, (4.2)])

$$\Omega(n^{\lceil\frac{r}{t+1}\rceil})=C_t(n,r)=O(n^{\lceil\frac{r}{\lfloor t/2\rfloor}\rceil})\quad\text{以及}\quad\Omega(n^{\lceil\frac{r}{t}\rceil})=U_t(n,r)=O(n^{\lceil\frac{r}{t-1}\rceil}).\tag{5.3}$$

在 (5.3) 中, 关于 $C_t(n,r)$ 和 $U_t(n,r)$ 的 Turán 指数的上下界相去甚远. 尽管如此, 却鲜有文献能够改进 (5.3) 中的上下界. 以下列举仅有的几个结果.

对于可消去超图, 人们已知 $\frac{0.28}{2^r}\binom{n}{r}<C_1(n,r)\leqslant\frac{2^r}{\binom{2r}{r}}\binom{n}{r}$ (上下界分别参见文献 [26, 80]) 以及 $\Omega(n^{\lfloor\frac{r}{2}\rfloor})=C_2(n,r)=O(n^{\lceil\frac{r}{2}\rceil})$[29]、$n^{2-o(1)}<C_2(n,3)=O(n^2)$[29]. 对于求并 - 自由超图, 人们已知 $U_2(n,r)=\Theta(n^{\lceil4r/3\rceil/2})$[27] 以及 $n^{2-o(1)}<U_r(n,r)=O(n^2)$[30].

由以上讨论可知, 人们已在 $t=1$ 与 $t=2$ 且 $2\mid r$ 时决定了 $C_t(n,r)$ 的 Turán 指数, 仅在 $t=2$ 时决定了 $U_t(n,r)$ 的 Turán 指数. Shangguan 和 Tamo[65] 指出了稀疏超图与可消去超图以及求并 - 自由超图的紧密关系, 并缩小了 (5.3) 中上下界的差距. 特别地, 他们证明了如下结论:

引理 5.2 (参见文献 [65, 引理 2.3–2.5]) (i) 如果某个 r- 超图既是 $(tr+\lceil\frac{2r-t-1}{t+2}\rceil,t+2)$- 自由的, 又是 $(2r-\lceil\frac{2r-t-1}{t+2}\rceil-1,2)$- 自由的, 则它也是 t- 可消去的;

(ii) 如果某个 $(2k+1)$- 超图是 $(4k+2,3)$- 自由的, 则它也是 2- 可消去的;

(iii) 如果某个 r- 部 r- 超图既是 $(tr-r,t)$- 自由的, 又是 $(tr,2t)$- 自由的, 则它也是 t- 求并 - 自由的.

根据引理 5.2 可得如下结论:

定理 5.5 (参见文献 [65, 定理 1.1–1.3]) (i) 对于给定正整数 $r\geqslant 3$、$t\geqslant 3$ 和 $n\to\infty$, 有

$$\Omega(n^{\lfloor\frac{2r}{t+2}\rfloor+\frac{2r \pmod{t+2}}{t+1}})=C_t(n,r)=O(n^{\lceil\frac{r}{\lfloor t/2\rfloor+1}\rceil}). \tag{5.4}$$

此外, 如果 $\gcd(2r-\lceil\frac{2r-t-1}{t+2}\rceil,t+1)=1$, 则有 $C_t(n,r)=\Omega(n^{\lfloor\frac{2r}{t+2}\rfloor+\frac{2r \pmod{t+2}}{t+1}}(\log n)^{\frac{1}{t+1}})$.

(ii) 对于任意给定的 $k\geqslant 1$ 和 $n\to\infty$, 有 $C_2(n,2k+1)>n^{k+1-o(1)}$.

(iii) 对于任意给定的 $r\geqslant 3$、$t\geqslant 3$ 和 $n\to\infty$, 有

$$\Omega(n^{\frac{r}{t-1}})=U_t(n,r)=O(n^{\lceil\frac{r}{t-1}\rceil}). \tag{5.5}$$

此外, 如果 $\gcd(r,t-1)=1$, 则有

$$U_t(n,r)=\Omega(n^{\frac{r}{t-1}}(\log n)^{\frac{1}{t-1}}).$$

证明 不难看出 (i) 和 (iii) 的下界可由引理 5.2 与命题 2.1 推导出来, (ii) 的下界可由引理 5.2 与 (1.5) 推导出来. 对于定理的上界部分, 可参见文献 [65]. □

注意到, 对于 $2\mid t$ 以及 $(\frac{t}{2}+1)\mid r$, (5.4) 决定了 $C_t(n,r)$ 的 Turán 指数. Shangguan 和 Tamo[65] 认为, 当 $t,r\geqslant 3$ 时, (5.4) 中的上界可以被进一步改进为 $C_t(n,r)=O(n^{\lceil\frac{2r}{t+2}\rceil})$. 特别地, 决定是否有 $C_3(n,5)=O(n^2)$ 是一个非常有趣的问题. 如果这个猜测是正确的, 则结合 (5.4) 的下界, 我们可以对所有满足 $(t+2)\mid 2r$ 的 r 和 t 给出 $C_t(n,r)$ 的 Turán 指数.

然而, 当 $(t+2)\nmid 2r$ 时, 决定 $C_t(n,r)$ 的渐近阶是一个困难的问题. 例如, Füredi[29] 猜测对于所有给定的 $k\geqslant 1$ 都有 (参见文献 [29, 猜想 12.1])

$$n^{k+1-o(1)}<C_2(n,2k+1)=o(n^{k+1}). \tag{5.6}$$

实际上, 他已经证明, 当 $k=1$ 时, $C_2(n,3)=\Theta(f_3(n,7,4))$ (参见文献 [29, 定理 4.1]).

Blackburn 对定理 5.5(iii) 的下界 $U_t(n,r)=\Omega(n^{\frac{r}{t-1}})$ 有另一个证明 (参见文献 [9, 定理 5]). 显然, 当 $(t-1)\mid r$ 时, (5.5) 给出了 $U_t(n,r)$ 的 Turán 指数. 然而, 当 $(t-1)\nmid r$ 时, 决定 $U_t(n,r)$ 的渐近阶也是不容易的. 实际上, Füredi 和 Ruszinkó[30] 猜测, 对于所有给定的 $r\geqslant 3$ 有

$$U_r(n,r)=o(n^2).$$

他们证明了 $U_r(n,r)=O(f_r(n,r^2-r+1,r+1))$. 通过以上讨论, 可以进一步看出可消去超图、求并 - 自由超图与稀疏超图的相似性, 即当参数不满足某种整除性条件时, 问题变得十分困难.

下面给出求并 - 自由超图的一类新下界:

定理 5.6 当 $n\to\infty$ 时, 有

$$U_5(n,7)>n^{2-o(1)}.$$

证明 由定理 3.3 可知, 当 $r=7$ 时, 存在 7- 部的线性 7- 超图 $\mathcal{H}$, 使得 $|\mathcal{H}|>n^{2-o(1)}$, 并且 $\mathcal{H}$ 同时是 $(28,5)$- 自由与 $(43,8)$- 自由的, 则 $\mathcal{H}$ 显然也是 $(35,10)$- 自由的. 此时, 由引理 5.2(iii) 可知, $\mathcal{H}$ 也是 5- 求并 - 自由的 7- 超图. 证毕. □

6 稀疏超图与信息科学

本节介绍稀疏超图在信息科学中的 3 个应用. 第 6.1 小节讨论 $(6,3)$- 自由 3- 超图与集中式编码缓存方案的关系, 第 6.2 小节讨论如何利用稀疏超图来构造具有优异组合列表译码性质的纠错码, 第 6.3 小节介绍如何利用稀疏超图构造在存储编码领域发挥着重要作用的局部可修复码.

6.1 集中式编码缓存

不断增长的视频传播需求带来了网络的拥堵. 假设一个拥有海量数据的服务器与一组用户相连, 每个用户都希望从服务器中下载所需要的文件, 同一时间的大量需求常常会令网络发生堵塞, 导致系统的延时和超载. 对于该问题, Bell 实验室的两位工程师 Maddah-Ali 和 Niesen [48] 的解决方案是利用靠近末端用户的网络存储空间预先进行数据缓存: 在空闲时段 (网络负载低), 系统将文件的某些片段分发到每个用户的缓存中; 在繁忙时段 (网络负载高), 用户的不同需求可以从这些缓存中获益. 利用该方法, 人们可以减轻网络负载并舒缓其拥塞.

Maddah-Ali 和 Niesen 提出的缓存方案被称为集中式缓存方案 (centralized coded caching scheme, 简记 CCC 方案), "集中式" 意为网络中有一个中心服务器负责调配. CCC 方案有两个阶段: 文件放置阶段 (placement phase), 系统将每个文件中的部分数据按照预先设定好的方案存入用户的缓存; 文件发送阶段 (delivery phase), 系统依据每个用户的需求, 将相关数据包的异或和 (exclusive OR multiplexing) 用共享的链接广播出去. 近期编码缓存已成为信息科学领域的一个热门研究课题.

CCC 方案的核心想法是, 统筹设计文件放置阶段与文件发送阶段, 使得每个用户都可以利用系统广播与自身缓存来解码所需文件. 假设有 K 个用户和 N 个文件, 每个用户有大小为 M 的缓存空间. 不失一般性, 假设每个文件都具有单位大小, 此时整个数据库的大小也是 N. 在文件发送阶段, 系统广播的数据总量被称为这个方案的耗费, 记为 R. 在编码缓存中, 每个单位文件都被划分成 F 个数据包. 一般而言, 给定 K、M 和 N, R 和 F 这两个参数是衡量一个缓存方案优劣的主要指标. 通常假设 $\frac{M}{N}$ 是固定的常数, 将 R 和 F 看作是关于 K 的函数, 以考察它们的表现. CCC 方案的结构如图 1 所示.

对于一个未经编码的缓存方案而言, 每个用户在其缓存里存储了每个文件的 $\frac{M}{N}$ 部分. 根据用户

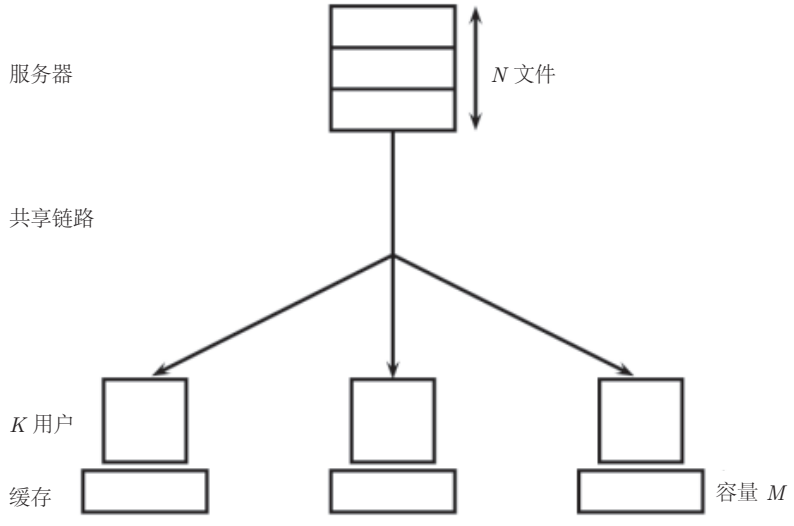

图 1 (K,M,N)-CCC 缓存方案

的需求, 系统将其所需文件剩下的 $1-\frac{M}{N}$ 部分以广播的形式分发出去. 未经编码的缓存方案的耗费是 $R_U = K\cdot(1-\frac{M}{N})$. 容易看出, R_U 是随着 K 线性增长的. 为了实现这个方案, 只需将每个文件分割成 $F_U = N$ 个数据包, F_U 是与 K 无关的一个数.

Maddah-Ali-Niesen 方案可以将耗费显著地降低为 $R_{AN} = K\cdot(1-\frac{M}{N})\cdot\frac{1}{1+KM/N}$. 当 K 充分大时, R_{AN} 的极限是 $\frac{N-M}{M}$, 这是一个与 K 无关的数.

然而, 为了实行 Maddah-Ali-Niesen 方案, 每个文件必须被分割成 $F_{AN} = \binom{K}{KM/N}$ 个数据包, 其中 F_{AN} 是随着 K 指数增长的. 当 K 很大时, 这并不适用于实际情形.

为了减小 F_{AN}, Yan 等 [85] 提出了放置发送阵列 (placement delivery array, PDA) 的概念, 并用其来构造 CCC 方案. PDA 利用一个矩阵, 清楚地表明了在放置阶段每个用户需要缓存什么以及在发送阶段服务器应该广播什么.

设 K、F、Z 和 S 都为正整数, (K,F,Z,S)-PDA 实际上是规模为 $F\times K$ 的阵列 $\mathcal{P} = [p_{j,k}]_{F\times K}$, 其中, $\frac{FM}{N}$ 是整数, $\mathcal{P}$ 中的元素取自集合 $\{*\}\cup\mathcal{S}$, $*$ 是一个特殊符号, $\mathcal{S} = \{1,2,\ldots,S\}$. 不失一般性, 假设每个 $s\in\mathcal{S}$ 在 $\mathcal{P}$ 中都至少出现了一次, 并记 $\mathcal{F} = \{1,\ldots,F\}$, $\mathcal{N} = \{1,\ldots,N\}$. (K,F,Z,S)-PDA 需要满足如下约束条件:

(C1) 符号 $*$ 在每列中都恰好出现了 $Z = \frac{FM}{N}$ 次, 因此每列都含有 $F-Z$ 个整数元素;

(C2) 每行或者每列都不含有相同的整数;

(C3) 对于任意两个不同的位置, 若有 $p_{j_1,k_1} = p_{j_2,k_2} = s\in\mathcal{S}$, $j_1\neq j_2$, $k_1\neq k_2$, 则一定有 $p_{j_1,k_2} = p_{j_2,k_1} = *$.

利用 PDA, Yan 等 [85] 提出了两类缓存方案, 其数据包数 F_{PDA} 显著地小于 F_{AN}, 其耗费 R_{PDA} 仅略微大于 R_{AN}, 但是 F_{PDA} 仍是随 K 呈指数增长的.

至此, 一个有趣且重要的问题是, 研究在 $\frac{M}{N}$ 与 R 都是与 K 无关的常数时, $F := F(K)$ 应该如何取值, 使得存在 (K,M,N)-CCC 缓存方案 (为了叙述方便, 称其为常耗费缓存方案). Maddah-Ali 和 Niesen [48] 及 Yan 等 [85] 的结论说明 $F = \exp(O(K))$ 是可行的, 那么, 更小的 F 是否可行? 特别地, $F = \mathrm{poly}(K)$ 是否可行?

Shangguan 等 [67] 发现了 PDA 与稀疏超图的紧密联系. 根据 (K,F,Z,S)-PDA 的定义, Shangguan 等 [67] 考虑了一个 3- 部 3- 超图 $\mathcal{H}$, 其顶点集分为 3 个部分 $\mathcal{F}$、$\mathcal{K}$ 和 $\mathcal{S}$, 并满足 $|\mathcal{F}| = F$、$|\mathcal{K}| = K$ 和 $|\mathcal{S}| = S$. 3 个顶点 $j\in\mathcal{F}$、$k\in\mathcal{K}$ 和 $s\in\mathcal{S}$ 构成一条边 $\{j,k,s\}\in\mathcal{H}$ 当且仅当阵列 $\mathcal{P}$ 的第 j 行第 k 列的元素恰好是 $s\in\mathcal{S}$, 即 $p_{jk} = s$. 此时, 称 $\mathcal{H}$ 为由 $\mathcal{P}$ 所定义的超图. 容易验证, $\mathcal{H}$ 的边数恰好等于 $\mathcal{P}$ 中整数的个数, 因此有 $|\mathcal{H}| = K(F-Z) = KF(1-\frac{M}{N})$. 下面的定理建立了 PDA 与 $(6,3)$- 自由超图的对应关系:

定理 6.1 (参见文献 [67, 定理 10]) 满足条件 (C1)–(C3) 的 (K,F,Z,S)-PDA 存在当且仅当由它定义的超图 $\mathcal{H}$ 是一个线性的 $(6,3)$- 自由 3- 部 3- 超图, 使得每个顶点 $k\in\mathcal{K}$ 恰好与 $F-Z$ 条边相关联.

由此出发, 文献 [67] 证明了如下结论:

命题 6.1 (参见文献 [67, 定理 12, 构造 I 和 II]) • 不存在 $F = O(K)$, 即分包数随用户数线性增长的常耗费编码缓存方案;

• 存在 $F = \exp(O(\sqrt{K}))$, 即分包数随用户数呈次指数增长的常耗费编码缓存方案.

实际上, 上述第一个结论的证明利用了 $f_3(n,6,3) = o(n^2)$, 第二个结论的证明利用了某些特殊参数下的 $(6,3)$- 自由 3- 超图. 除了与 $(6,3)$- 自由 3- 超图的关系之外, 文献 [67] 还讨论了 PDA 与其他组合结构的关系, 如二部图的强边着色 (strong edge coloring) 和 Ruzsa-Szemerédi 图, 关于相关内容的

进一步的讨论可以分别参见文献 [68, 86].

6.2 组合列表译码

设 q 和 n 均为正整数, Q 为 q 元集合, 对于两个 q 元 n 长向量 $x=(x_1,\dots,x_n)$ 和 $y=(y_1,\dots,y_n)\in Q^n$, 定义 x 与 y 的 Hamming 距离 $\mathrm{d}(x,y)$ 为它们互不相等的分量的个数, 即

$$\mathrm{d}(x,y)=|\{1\leqslant i\leqslant n: x_i\neq y_i\}|.$$

对于任意 $y\in Q^n$ 与 $1\leqslant t\leqslant n$, 将所有与 y 的 Hamming 距离不超过 t 的向量的集合称为以 y 为球心、t 为半径的 Hamming 球, 记为 $\mathrm{B}_t(y):=\{x\in Q^n:\mathrm{d}(x,y)\leqslant t\}$. 称 q 元 n 长向量的集合 $C\subseteq Q^n$ 为一个码 (code). 码 C 的码率 (code rate) 为 $\mathrm{R}(C):=\frac{\log_q|C|}{n}$, 码 C 的最小距离 (minimum distance) 为 $\mathrm{d}(C):=\min\{\mathrm{d}(x,y):x,y\in C,x\neq y\}$.

码的极小距离决定了其在唯一译码 (unique decoding) 模型下所能纠正的错误数目. 注意到, Hamming 距离满足三角形不等式, 因此任意半径不超过 $\lfloor\frac{\mathrm{d}(C)-1}{2}\rfloor$ 的 Hamming 球最多只能包含一个码字, 即对于任意 $y\in Q^n$, $t\leqslant\lfloor\frac{\mathrm{d}(C)-1}{2}\rfloor$ 都有

$$|\mathrm{B}_t(y)\cap C|\leqslant 1. \tag{6.1}$$

在 Hamming 模型或者对抗噪声模型下 (adversarial noise model), 假设传输方发送的是码字 $x\in C$, 接收方收到的是向量 $y\in Q^n$, 如果传输中发生的替换错误数量 (即使得 $x_i\neq y_i$ 的 i 的数量) 不超过 $\lfloor\frac{\mathrm{d}(C)-1}{2}\rfloor$, 则依据 (6.1), 接收方可以利用 y 唯一译码出 x.

人们希望码的码率与极小距离越大越好. 然而, 在码长 n 与字母集大小 q 给定时, 码率越大, 则极小距离越小; 极小距离越大, 则码率越小. 研究码率与极小距离之间的权衡, 是组合编码领域的根本性问题. 由于篇幅所限, 本文对此仅介绍经典的 Singleton 界 [70], 对于其他相关内容, 感兴趣的读者可参见文献 [38].

定理 6.2 (Singleton 界, 参见文献 [38, 定理 4.3.1]) 对于任意码 $C\subseteq Q^n$, $|Q|=q$, 都有

$$|C|\leqslant q^{n-\mathrm{d}(C)+1}.$$

由定理 6.2 可知, 唯一译码的纠错数目上限不能超过 $\lfloor\frac{\mathrm{d}(C)-1}{2}\rfloor$. 为了突破这个限制, Elias [17] 和 Wozencraft [83] 分别于 1957 和 1958 年独立提出了列表译码 (list decoding, LD) 的概念. 给定实数 $\rho\in[0,1]$ 与正整数 $L\in\mathbb{Z}^+$, 称码 $C\subseteq Q^n$ 是 (ρ,L)- 列表译码的, 如果对于任意 $y\in Q^n$, 都有

$$|\mathrm{B}_{\rho n}(y)\cap C|\leqslant L.$$

称 ρ 为列表译码半径 (list decoding radius), L 为列表大小 (list size). 不难看出, 当 $L=1$ 时, 我们得到了 (6.1), 即码 C 是 $(\rho,1)$-LD 的当且仅当 $\rho n\leqslant\lfloor\frac{\mathrm{d}(C)-1}{2}\rfloor$.

在列表译码模型下, 如果 y 为输入, 则译码器的输出不是唯一的, 而是 $\mathrm{B}_{\rho n}(y)\cap C$ 中不超过 L 个的码字. 作为唯一译码模型的补充与延拓, 列表译码以牺牲译码精度为代价, 获得了比唯一译码更强的纠错能力. 在极限情形下, 列表译码可以纠正的错误数量可以近似达到 $\mathrm{d}(C)$, 即唯一译码的两倍 (参见文献 [38, 定理 7.4.2]).

给定码长 n 与字母集大小 q, 组合列表译码主要关心码的 3 个参数: 码率 R、列表译码半径 ρ 和列表大小 L. 人们希望码率与列表译码半径越大越好, 列表大小越小越好, 然而这 3 者之间也需要满足一定的权衡.

为了方便起见, 以下总是假设 ρn 为正整数. 用 $A(n,q,\rho,L)$ 表示 n 长 q 元 (ρ,L)- 列表译码的码最多能含有的码字个数. Shangguan 和 Tamo[66] 证明了如下推广的 Singleton 界:

定理 6.3 (参见文献 [66, 定理 1.2]) 设 n、q 和 L 为正整数, $\rho\in(0,\frac{L}{L+1}]$ 为实数, 则

$$A(n,q,\rho,L)\leqslant Lq^{n-\lfloor\frac{L+1}{L}\rho n\rfloor}.$$

在 $A(n,q,\rho,L)$ 的下界方面, Goldberg 等[36] 证明了, 当 n 和 L 给定且 q 充分大时, 稀疏超图能够被用来构造具有 (ρ,L)- 列表译码性质的纠错码. 声明 1.1 叙述了一类超图与矩阵之间的等价关系. 不难看出, 声明 1.1 中提到的超图 $\mathcal{H}$ 也可以被等价地看作 r 长 q 元、大小为 m 的纠错码: 我们只需将纠错码中的码字看作矩阵 $M_{\mathcal{H}}$ 的列. 利用这个观察, 文献 [36] 证明了如下结论:

引理 6.1 (参见文献 [36, 引理 4.5]) 设 $\mathcal{H}$ 为一个 r- 部 r- 超图, 且每部的大小都为 q. 如果 $\mathcal{H}$ 是 $(r+(L+1)\rho r,L+1)$- 自由的, 则码 $C_{\mathcal{H}}=\{\psi(A):A\in\mathcal{H}\}\subseteq[q]^r$ 是 (ρ,L)- 列表译码的.

根据引理 6.1 以及稀疏超图的已知构造, 不难得出以下结论:

命题 6.2 (参见文献 [36, 命题 4.6]) 对于给定正整数 n 和 L, 以及满足 ρn 为正整数的实数 $\rho\in(0,\frac{L}{L+1}]$, 当 $q\to\infty$ 时,

(i) $A(n,q,\rho,L)=\Omega(q^{n-\frac{\rho(L+1)}{L}})$;

(ii) 如果 $\gcd(L,rn)=1$, 则有 $A(n,q,\rho,L)=\Omega(q^{n-\frac{\rho n(L+1)}{L}}\cdot\log^{\frac{1}{L}}q)$;

(iii) $A(n,q,\rho,2)>q^{n-\frac{3\rho n-1}{2}-o(1)}$.

证明 不难看出 (注意到, 在利用引理 6.1 时, 我们用 n 代替了 r), (i) 是引理 6.1 与定理 2.1 的推论, (ii) 是引理 6.1 与定理 2.2 的推论, (iii) 是引理 6.1 与 (1.5) 的推论. □

若 q 是一个素数幂, $Q=\mathbb{F}_q$ 是包含 q 个元素的有限域, 如果码 $C\subseteq\mathbb{F}_q^n$ 恰好为向量空间 $\mathbb{F}_q^n$ 的 k 维子空间, 则称其为 $[n,k]_q$- 线性码 (linear code, LC). 文献 [36] 证明了如下比定理 6.3 稍好的结果:

命题 6.3 (参见文献 [36, 命题 3.6]) 对于给定正整数 L 以及满足 ρn 为正整数的实数 $\rho\in(0,\frac{L}{L+1}]$, 存在一个整数 $n(\rho,L)$, 使得对于所有 $n\geqslant n(\rho,L)$ 有

$$A^{\mathrm{LC}}(n,q,\rho,L)\leqslant q^{n-\lceil\frac{L+1}{L}\rho n\rceil},$$

其中 $A^{\mathrm{LC}}(n,q,\rho,L)$ 表示 n 长 q 元具有 (ρ,L)- 列表译码性质的线性码最多能含有的码字个数.

结合命题 6.2 和 6.3, 人们可以得到如下的有趣结果: 当 n 和 L 给定、$q\to\infty$ 以及 $L\nmid\rho n$ 时, $A^{\mathrm{LC}}(n,q,\rho,L)\ll A(n,q,\rho,L)$, 即在某些参数条件下, 具有相同列表译码能力的线性码的最大码字个数远小于非线性码的最大码字个数.

最后, 再介绍稀疏超图与一类经典纠错码—Reed-Solomon 码 (简称为 RS 码) 的组合列表译码能力的关系. RS 码由 Reed 和 Solomon[55] 在 1960 年代引入, 它在理论与实践中都非常重要, 因而也被人们称为是 "the greatest code of them all" (参见文献 [38, 第 5 节] 标题). 设 $q\geqslant n$ 且 q 为一个素数幂, $\alpha_1,\ldots,\alpha_n$ 为 $\mathbb{F}_q$ 中的 n 个不同元素, 由 $\alpha_1,\ldots,\alpha_n$ 所定义的 RS 码为

$$C_{\mathrm{RS}[n,k]}:=\{(f(\alpha_1),\ldots,f(\alpha_n)):f\in\mathbb{F}_q[x],\deg(f)<k\},\tag{6.2}$$

这里用 $\mathbb{F}_q[x]$ 表示由系数取自有限域 $\mathbb{F}_q$ 的多项式所构成的集合. 由于 $\mathbb{F}_q[x]$ 中次数小于 k 次的多项式恰好有 q^k 个, 因此 $|C_{\mathrm{RS}[n,k]}|=q^k$. 此外不难验证 (6.2) 所定义的码是一个 $[n,k]$- 线性码.

列表译码研究领域中著名的 Johnson 界说明, 当 n 充分大时, 任意一个具有码率 $R=\frac{k}{n}$ 的 $[n,k]$-RS 码都是 $(1-\sqrt{R},qn^2)$- 列表译码的 (参见文献 [41] 或者 [38, 定理 7.3.3]). 人们称 $1-\sqrt{R}$ 为 RS 码

的 Johnson 半径. 近半个世纪以来, 是否存在列表译码半径能够超越 Johnson 半径的 RS 码, 一直是编码理论与理论计算机科学中的难题之一, 并受到众多学者的关注 (如文献 [39, 77] 等).

直到 2014 年, 才由 Rudra 和 Wootters [57] 证明确实存在列表译码半径能够超越 Johnson 半径的 RS 码, 然而他们得到的 RS 码的码率、列表译码半径与列表大小之间的权衡关系与命题 6.3 中的界相去甚远. 2020 年, Shangguan 和 Tamo [66] 证明了, 当 $L=2$ 时, 只要 q 充分大, 对于任意 $2 \mid \rho n$ 都存在达到命题 6.3 上界的 RS 码, 即存在具有 $(\frac{2}{3}(1-R),2)$- 列表译码性质的 RS 码. 文献 [66] 中的关于这一结论的证明较为复杂, 但是如果从稀疏超图的观点来看, 将 $r=n$、$L=2$ 和 $\rho=\frac{2}{3}(1-R)$ 代入引理 6.1 可知, 只要 n- 部 n- 超图是 $(3n-2k,3)$- 自由的, 则对应的码是 $(\frac{2}{3}(1-R),2)$- 列表译码的. 实际上, 通过仔细研究文献 [63] 中关于 $(3n-2k,3)$- 自由超图的构造不难看出, 文献 [66] 中的上述结论可以看作引理 6.1 与 (1.13) 的下界的推论.

6.3 局部可修复码

为确保数据存储的可靠性, 传统方法将同一文件的多个副本存储在不同的存储单元上. 在现代数据中心以 EB 计数 (1 EB $=10^9$ GB) 的庞大数据量面前, 就存储开销而言, 这种复制策略显然是极其低效的. 为了减少存储开销, 满足不同条件的存储码被引入到数据存储的编码方案中.

称一个 $[n,k]_q$- 线性码 C 为 r- 局部可修复码 (locally recoverable code, LRC), 如果对于任意 $1\leqslant i\leqslant n$ 都存在 r 个不包含 i 的坐标 $\{i_1,\dots,i_r\}\subseteq\{1,\dots,n\}$, 使得对于任意码字 $x=(x_1,\dots,x_n)\in C$, 都可以通过 $x_{i_1},\dots,x_{i_r}$ 恢复出 x_i. 我们将满足上述条件的码记为 (n,k,r)-LRC, $\{i_1,\dots,i_r\}$ 也被称为 i 的修复集. Gopalan 等 [37] 证明了 (n,k,r)-LRC 的最小距离 d 满足如下的 Singleton- 型上界:

$$d\leqslant n-k-\left\lceil\frac{k}{r}\right\rceil+2.$$

码字数量达到该上界的局部可修复码也被称为是最优的. 关于最优 LRC 的进一步讨论, 感兴趣的读者可参见文献 [79].

在实际应用中, 人们总是希望在给定大小的有限域上构造尽可能长的最优局部可修复码. Xing 和 Yuan [84] 发现了这一问题与稀疏超图的联系, 提出了如下的构造方案. 一个 $[n,k]_q$- 线性码 C 的校验矩阵 (parity check matrix) 是指, 一个 $(n-k)\times n$ 的矩阵 H, 满足 $x\in C$ 当且仅当 $Hx^{\mathrm{T}}=0$. 为了方便起见, 不妨假设 $r+1\mid n$. 令 $m:=\frac{n}{r+1}$, 并令 I_m 为 m 阶的恒等矩阵, $\boldsymbol{j}$ 为 $r+1$ 长的全 1 向量. 不难验证, 一个具有如下形式校验矩阵的线性码为 r- 局部可修复码:

$$H=\begin{pmatrix} I_m\otimes\boldsymbol{j}\\ A\end{pmatrix},$$

其中, $\otimes$ 代表 Kronecker 乘积, A 可以是任意一个 $(n-k-m)\times n$ 的矩阵. 实际上, 若 $Hx^{\mathrm{T}}=0$, 则 x 的任意一个分量 x_i 都满足一个恰好有 $r+1$ 个变量的线性方程.

通过挑选具有某些特殊性质的矩阵 A, Xing 和 Yuan [84] 在 $r\geqslant d-2$ 的情形下构造出了最优局部可修复码. 他们的构造方法如下所述. 对一个集合 $A=\{\alpha_1,\dots,\alpha_{r+1}\}\subseteq\mathbb{F}_q$, 用 $V(A)$ 表示 $(d-2)\times(r+1)$ 的 Vandermonde 矩阵, 该矩阵的第 i 行第 j 列元素为 α_j^i. 文献 [84] 证明了如下结论:

定理 6.4 (参见文献 [84, 定理 3.1]) 设 $d\geqslant 11$, $r\geqslant d-2$, 令 C 为 $[n,k]_q$ 线性码, 且其校验矩

阵为

$$H=\begin{pmatrix} I_m\otimes \boldsymbol{j} \\ V(A_1),\ldots,V(A_m)\end{pmatrix},$$

则 C 是一个最小距离为 d 的最优 (n,k,r)-LRC 当且仅当对于每个 $1\leqslant i\leqslant \lfloor\frac{d-1}{2}\rfloor$,

$$\mathcal{A}:=\{A_1,\ldots,A_m\}\subseteq\binom{\mathbb{F}_q}{r+1}$$

都是 (ir,i)- 自由的 $(r+1)$- 超图.

下面的结果实际上是定理 6.4 与命题 2.1 的推论.

命题 6.4 (参见文献 [84, 定理 1.1]) 如果 $d\geqslant 11$, $r\geqslant d-2$, $(r+1)\mid n$, 则存在最小距离为 d、码长 $n=\Omega(q(q\log q)^{\lceil (d-3)/2\rceil})$ 的最优 (n,k,r)-LRC.

Prakash 等 [54] 引入了 (n,k,r,δ) -LRC 的概念, 将每个修复集只能修复一个错误的定义推广到可以修复 $\delta-1$ 个错误的情形. 在这种定义下, 前文介绍的 (n,k,r)-LRC 实际上是 $\delta=2$ 的特殊情形. 类似地, Prakash 等证明了 (r,δ) -LRC 的 Singleton 型界

$$d\leqslant n-k+1-\left(\left\lceil\frac{k}{r}\right\rceil-1\right)(\delta-1).$$

码字数量达到该上界的局部可修复码也被称为是最优 (n,k,r,δ) -LRC.

通过构造具有分块 Vandermonde 型的校验矩阵, Kong 等 [46] 建立了稀疏超图与最优 (n,k,r,δ)-LRC 的校验矩阵间的关系. 他们证明了如下结论:

定理 6.5 (参见文献 [46, 定理 V.8]) 给定正整数 $\delta\geqslant 2$, $r\geqslant d-\delta$, $d\geqslant 2\delta+1$. 记

$$R=r+\delta-1,\quad \mu=\left\lfloor\frac{d-1}{\delta}\right\rfloor,$$

并设 $\mathcal{H}$ 为以 $V=\mathbb{F}_q$ 为顶点集的 R- 超图, 如果对于所有 $2\leqslant i\leqslant\mu$, $\mathcal{H}$ 均是 $(iR-\lfloor(i-1)\frac{\delta}{2}\rfloor-1,i)$- 自由的, 则可以利用 $\mathcal{H}$ 构造最优 (n,k,r,δ)-LRC, 并且其最小距离为 d, 码长为 $n=R|E|$.

通过一些已有的结果和概率方法, Kong 等 [46] 给出了一系列满足上述稀疏性条件的超图构造, 从而得到了具有超线性长度的最优 (n,k,r,δ)-LRC (详细结果参见文献 [46, 表 1]).

7 结论

本文介绍了 Brown、Erdős 和 Sós 关于稀疏超图的两个重要猜想及其最新进展以及稀疏超图在极值组合与信息科学中的若干有趣应用. 关于稀疏超图的研究方兴未艾, 还有很多公开问题没有得到解决. 下面列举与本文相关的一些重要公开问题, 供读者探讨.

公开问题 7.1 (猜想 1.2 上界的第一种未解决情形) 是否有 $f_3(n,7,4)=o(n^2)$?

公开问题 7.2 (猜想 1.2 下界的弱化版本, 对 (1.1) 与 (1.10) 两式下界的改进) 是否存在一个常数 $\epsilon>0$, 使得对于所有 $r>k\geqslant 2$, $e\geqslant 3$ 都有

$$f_r(n,er-(e-1)k+1,e)=\Omega(n^{k-\frac{1}{e-1}+\epsilon})?$$

公开问题 7.3 (猜想 1.3 在 $e=3$ 时的情形, 对 (1.13) 更细致的刻画) 极限 $\lim_{n\to\infty}\frac{f_r(n,3r-2k,3)}{n^k}$ 是否存在?

公开问题 7.4 (猜想 1.3 在 $e\geqslant 4$ 时的第一种情形) 极限 $\lim_{n\to\infty}\frac{f_3(n,6,4)}{n^2}$ 是否存在?

公开问题 7.5 能否进一步发掘或加强引理 4.5 以构造其他参数的稀疏超图?

公开问题 7.6 (可消去 - 超图的上界的进一步改进) 当 $t,r\geqslant 3$ 时, 是否有

$$C_t(n,r)=O(n^{\lceil\frac{2r}{t+2}\rceil})?$$

特别地, 是否有 $C_3(n,5)=O(n^2)$? (如果这个猜测是正确的, 则结合 (5.4) 的下界, 可以对所有满足 $(t+2)\mid 2r$ 的 r 和 t 给出 $C_t(n,r)$ 的 Turán 指数.)

公开问题 7.7 (线性码的列表译码能力) 是否对于任意给定的正整数 $L,n,\rho n\in\mathbb{Z}$ 且 $L\mid\rho n$, 当 q 充分大时, 都存在达到命题 6.3 中上界 $A^{\mathrm{LC}}(n,q,\rho,L)\leqslant q^{n-\lceil\frac{L+1}{L}\rho n\rceil}$ 的线性码? 特别地, 能否利用稀疏超图来构造这类线性码?

致谢 孔祥梁博士提供了第 6.3 小节的部分内容, 两位审稿人对本文提出了宝贵的修改意见, 作者对他们表示感谢.

参考文献

1 Ajtai M, Komlós J, Pintz J, et al. Extremal uncrowded hypergraphs. J Combin Theory Ser A, 1982, 32: 321–335
2 Alon N, Fischer E, Szegedy M. Parent-identifying codes. J Combin Theory Ser A, 2001, 95: 349–359
3 Alon N, Naor M. Derandomization, witnesses for Boolean matrix multiplication and construction of perfect Hash functions. Algorithmica, 1996, 16: 434–449
4 Alon N, Shapira A. On an extremal hypergraph problem of Brown, Erdős and Sós. Combinatorica, 2006, 26: 627–645
5 Alon N, Yuster R. On a hypergraph matching problem. Graphs Combin, 2005, 21: 377–384
6 Behrend F A. On sets of integers which contain no three terms in arithmetical progression. Proc Natl Acad Sci USA, 1946, 32: 331–332
7 Blackburn S R. Perfect Hash families: Probabilistic methods and explicit constructions. J Combin Theory Ser A, 2000, 92: 54–60
8 Blackburn S R. Frameproof codes. SIAM J Discrete Math, 2003, 16: 499–510
9 Blackburn S R. Probabilistic existence results for separable codes. IEEE Trans Inform Theory, 2015, 61: 5822–5827
10 Bohman T, Warnke L. Large girth approximate Steiner triple systems. J Lond Math Soc (2), 2019, 100: 895–913
11 Boneh D, Shaw J. Collusion-secure fingerprinting for digital data. IEEE Trans Inform Theory, 1998, 44: 1897–1905
12 Brown W G, Erdős P, Sós V T. Some extremal problems on r-graphs. In: New Directions in the Theory of Graphs. (Proceedings Third Ann Arbor Conf, Univ Michigan, Ann Arbor, Mich, 1971.) New York: Academic Press, 1973, 53–63
13 Colbourn C J, Dinitz J H, eds. Discrete Mathematics and its Applications. Handbook of Combinatorial Designs, 2nd ed. Boca Raton: Chapman & Hall/CRC, 2007
14 Conlon D, Fox J. Graph removal lemmas. In: Surveys in Combinatorics 2013. London Mathematical Society Lecture Note Series, vol. 409. Cambridge: Cambridge University Press, 2013, 1–49
15 Conlon D, Gishboliner L, Levanzov Y, et al. A new bound for the Brown-Erdös-Sós problem. J Combin Theory Ser B, 2023, 158: 1–35
16 Duke R A, Lefmann H, Rödl V. On uncrowded hypergraphs. Random Structures Algorithms, 1995, 6: 209–212
17 Elias P. List decoding for noisy channels. Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge, Rep. No. 335, 1957, 12pp
18 Elias P. Zero error capacity under list decoding. IEEE Trans Inform Theory, 1988, 34: 1070–1074
19 Erdős P. On the combinatorial problems which I would most like to see solved. Combinatorica, 1981, 1: 25–42
20 Erdős P, Frankl P, Füredi Z. Families of finite sets in which no set is covered by the union of two others. J Combin Theory Ser A, 1982, 33: 158–166
21 Erdős P, Frankl P, Füredi Z. Families of finite sets in which no set is covered by the union of r others. Israel J Math, 1985, 51: 79–89

22 Erdős P, Frankl P, Rödl V. The asymptotic number of graphs not containing a fixed subgraph and a problem for hypergraphs having no exponent. Graphs Combin, 1986, 2: 113–121
23 Erdős P, Moser L. Problem 35. In: Proceedings Conf Combin Structures and Appl Calgary, 1969. New York: Gordon and Breach, 1970, 506
24 Erdős P, Simonovits M. A limit theorem in graph theory. Studia Sci Math Hungar, 1966, 1: 51–57
25 Erdős P, Stone A H. On the structure of linear graphs. Bull Amer Math Soc (N S), 1946, 52: 1087–1091
26 Frankl P, Föredi Z. Union-free hypergraphs and probability theory. European J Combin, 1984, 5: 127–131
27 Frankl P, Füredi Z. Union-free families of sets and equations over fields. J Number Theory, 1986, 23: 210–218
28 Frankl P, Füredi Z. Colored packing of sets. In: Combinatorial Design Theory. North-Holland Mathematics Studies, vol. 149. Amsterdam: North-Holland, 1987, 165–177
29 Füredi Z. 2-cancellative hypergraphs and codes. Combin Probab Comput, 2012, 21: 159–177
30 Füredi Z, Ruszinkó M. Uniform hypergraphs containing no grids. Adv Math, 2013, 240: 302–324
31 Füredi Z, Simonovits M. The history of degenerate (bipartite) extremal graph problems. In: Erdős Centennial. Bolyai Society Mathematical Studies, vol. 25. Budapest: János Bolyai Math Soc, 2013, 169–264
32 Ge G, Shangguan C. Sparse hypergraphs: New bounds and constructions. J Combin Theory Ser B, 2021, 147: 96–132
33 Ge G, Shangguan C, Wang X. Some intriguing upper bounds for separating Hash families. Sci China Math, 2019, 62: 269–282
34 Glock S. Triple systems with no three triples spanning at most five points. Bull Lond Math Soc, 2019, 51: 230–236
35 Glock S, Kühn D, Lo A, et al. On a conjecture of Erdős on locally sparse Steiner triple systems. Combinatorica, 2020, 40: 363–403
36 Goldberg E, Shangguan C, Tamo I. Singleton-type bounds for list-decoding and list-recovery, and related results. arXiv:2112.05592, 2021
37 Gopalan P, Huang C, Simitci H, et al. On the locality of codeword symbols. IEEE Trans Inform Theory, 2012, 58: 6925–6934
38 Guruswami V, Rudra A, Sudan M. Essential coding theory. Draft available at http://cse.buffalo.edu/faculty/atri/courses/coding-theory/book/, 2019
39 Guruswami V, Sudan M. Improved decoding of Reed-Solomon and algebraic-geometry codes. IEEE Trans Inform Theory, 1999, 45: 1757–1767
40 Hollmann H D L, van Lint J H, Linnartz J P, et al. On codes with the identifiable parent property. J Combin Theory Ser A, 1998, 82: 121–133
41 Johnson S M. A new upper bound for error-correcting codes. IEEE Trans Inform Theory, 1962, 8: 203–207
42 Katona G O H. Extremal problems for hypergraphs. In: Combinatorics, Part 2: Graph Theory. Foundations, Partitions and Combinatorial Geometry. Proceedings of the NATO Advanced Study Institutes Series, vol. 16. Mathematical Centre Tracts, No. 56. Amsterdam: Math Centrum, 1974, 13–42
43 Katona G, Nemetz T, Simonovits M. On a problem of Turán in the theory of graphs. Mat Lapok (N S), 1964, 15: 228–238
44 Kautz W, Singleton R. Nonrandom binary superimposed codes. IEEE Trans Inform Theory, 1964, 10: 363–377
45 Keevash P. The existence of designs. arXiv:1401.3665, 2014
46 Kong X, Wang X, Ge G. New constructions of optimal locally repairable codes with super-linear length. IEEE Trans Inform Theory, 2021, 67: 6491–6506
47 Körner J, Sinaimeri B. On cancellative set families. Combin Probab Comput, 2007, 16: 767–773
48 Maddah-Ali M A, Niesen U. Fundamental limits of caching. IEEE Trans Inform Theory, 2014, 60: 2856–2867
49 Mantel W. Problem 28 (Solution by H. Gouwentak, W. Mantel, J. Teixeira de Mattes, F. Schuh and W. A. Wythoff). Wiskundige Opgaven, 1907, 10: 60–61
50 Mehlhorn K. Data Structures and Algorithms 3. Multidimensional Searching and Computational Geometry. EATCS Monographs on Theoretical Computer Science. Berlin: Springer-Verlag, 1984
51 Nagle B, Rödl V, Schacht M. Extremal hypergraph problems and the regularity method. In: Topics in Discrete Mathematics. Mathematics, Algorithms and Combinatorics, vol. 26. Berlin: Springer, 2006, 247–278
52 Newman I, Wigderson A. Lower bounds on formula size of Boolean functions using hypergraph entropy. SIAM J Discrete Math, 1995, 8: 536–542
53 Pippenger N, Spencer J. Asymptotic behavior of the chromatic index for hypergraphs. J Combin Theory Ser A, 1989, 51: 24–42

54 Prakash N, Kamath G M, Lalitha V, et al. Optimal linear codes with a local-error-correction property. In: IEEE International Symposium on Information Theory Proceedings. Cambridge: IEEE, 2012, 2776–2780

55 Reed I S, Solomon G. Polynomial codes over certain finite fields. J Soc Ind Appl Math, 1960, 8: 300–304

56 Rödl V. On a packing and covering problem. European J Combin, 1985, 6: 69–78

57 Rudra A, Wootters M. Every list-decodable code for high noise has abundant near-optimal rate puncturings. In: Symposium on Theory of Computing (STOC). New York: ACM, 2014, 764–773

58 Ruzsa I Z. Solving a linear equation in a set of integers I. Acta Arith, 1993, 65: 259–282

59 Ruzsa I Z, Szemerédi E. Triple systems with no six points carrying three triangles. In: Combinatorics, vol. II. Colloquia Mathematica Societatis J?anos Bolyai, vol. 18. Proceedings of Fifth Hungarian Colloquia, Keszthely, 1976. Amsterdam-New York: North-Holland, 1978, 939–945

60 Sárközy G N, Selkow S. An extension of the Ruzsa-Szemerédi theorem. Combinatorica, 2004, 25: 77–84

61 Sárközy G N, Selkow S. On a Turán-type hypergraph problem of Brown, Erdős and T. Sós. Discrete Math, 2005, 297: 190–195

62 Shangguan C, Ge G. Separating Hash families: A Johnson-type bound and new constructions. SIAM J Discrete Math, 2016, 30: 2243–2264

63 Shangguan C, Tamo I. Degenerate Turán densities of sparse hypergraphs. J Combin Theory Ser A, 2020, 173: 105228

64 Shangguan C, Tamo I. Sparse hypergraphs with applications to coding theory. SIAM J Discrete Math, 2020, 34: 1493–1504

65 Shangguan C, Tamo I. New Turán exponents for two extremal hypergraph problems. SIAM J Discrete Math, 2020, 34: 2338–2345

66 Shangguan C, Tamo I. Combinatorial list-decoding of Reed-Solomon codes beyond the Johnson radius. In: Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing (STOC). New York: ACM, 2020, 538–551

67 Shangguan C, Zhang Y, Ge G. Centralized coded caching schemes: A hypergraph theoretical approach. IEEE Trans Inform Theory, 2018, 64: 5755–5766

68 Shanmugam K, Tulino A M, Dimakis A G. Coded caching with linear subpacketization is possible using ruzsa-szeméredi graphs. In: IEEE International Symposium on Information Theory Proceedings (ISIT). Aachen: IEEE, 2017, 1237–1241

69 Sidorenko A. Approximate Steiner $(r-1,r,n)$-systems without three blocks on $r+2$ points. J Combin Des, 2020, 28: 144–148

70 Singleton R C. Maximum distance q-nary codes. IEEE Trans Inform Theory, 1964, 10: 116–118

71 Sós V T, Erdős P, Brown W G. On the existence of triangulated spheres in 3-graphs, and related problems. Period Math Hung, 1973, 3: 221–228

72 Spencer J. Turán's theorem for k-graphs. Discrete Math, 1972, 2: 183–186

73 Stinson D R, van Trung T, Wei R. Secure frameproof codes, key distribution patterns, group testing algorithms and related structures. J Statist Plann Inference, 2000, 86: 595–617

74 Stinson D R, Wei R, Chen K. On generalized separating Hash families. J Combin Theory Ser A, 2008, 115: 105–120

75 Stinson D R, Wei R, Zhu L. New constructions for perfect Hash families and related structures using combinatorial designs and codes. J Combin Dess, 2000, 8: 189–200

76 Stinson D R, Wei R, Zhu L. Some new bounds for cover-free families. J Combin Theory Ser A, 2000, 90: 224–234

77 Sudan M. Decoding of Reed Solomon codes beyond the error-correction bound. J Complexity, 1997, 13: 180–193

78 Szemerédi E. Regular partitions of graphs. In: Problèmes Combinatoires et Théorie des Graphes, vol. 260. Colloq Internat CNRS. Paris: CNRS, 1978, 399–401

79 Tamo I, Barg A. A family of optimal locally recoverable codes. IEEE Trans Inform Theory, 2014, 60: 4661–4676

80 Tolhuizen L M. New rate pairs in the zero-error capacity region of the binary multiplying channel without feedback. IEEE Trans Inform Theory, 2000, 46: 1043–1046

81 Turán P. Eine Extremalaufgabe aus der Graphentheorie. Mat Fiz Lapok, 1941, 48: 436–452

82 Walker II R A, Colbourn C J. Perfect Hash families: Constructions and existence. J Math Cryptol, 2007, 1: 125–150

83 Wozencraft J M. List decoding. Quarterly Progress Report. Cambridge: Research Laboratory of Electronics, MIT, 1958, 48: 90–95

84 Xing C, Yuan C. Construction of optimal locally recoverable codes and connection with hypergraph. arXiv:1811.09142, 2018

85 Yan Q F, Cheng M Q, Tang X H, et al. On the placement delivery array design for centralized coded caching scheme. IEEE Trans Inform Theory, 2017, 63: 5821–5833
86 Yan Q F, Tang X H, Chen Q C, et al. Placement delivery array design through strong edge coloring of bipartite graphs. IEEE Commun Lett, 2018, 22: 236–239

Sparse hypergraphs: From theory to applications

Chong Shangguan & Gennian Ge

Abstract For fixed integers r, e and v, an r-uniform hypergraph is said to be (v,e)-free or (v,e)-sparse if the union of any e distinct edges of it contains at least $v+1$ vertices. The notion of sparse hypergraphs was initially introduced by Brown, Erdős and Sós in the 1970s. Since then, determining the upper and lower bounds on the maximum number of edges that can be contained in a sparse hypergraph with a given number of vertices has become one of the central problems in extremal combinatorics. A number of powerful methods from several disciplines, including combinatorics, probability theory, algebra, and number theory, have been applied to the study of sparse hypergraphs. In this paper, we introduce the recent developments on two important conjectures of Brown, Erdős and Sós on sparse hypergraphs, and discuss some of the applications of sparse hypergraphs to extremal combinatorics and information sciences. We also provide new constructions for perfect Hash matrices and union-free hypergraphs under certain parameters. Our constructions improve the previously best-known lower bounds for these problems.

Keywords **sparse hypergraphs, Brown-Erdős-Sós conjectures, perfect Hash matrices, cancellative hypergraphs, union-free hypergraphs, centralized coded caching, combinatorial list decoding, locally repairable codes**

MSC(2020) **05B20, 05B40, 05C65, 05D05, 05D40, 11B30, 60A86, 68P30, 94B25**

doi: 10.1360/SSM-2022-0008