网络纠错基础理论研究

（申请清华大学工学博士学位论文）

培 养 单 位： 电子工程系

学　　科： 信息与通信工程

研　究　生： 肖 智 清

指 导 教 师： 王　　京　教　授

二〇一六年五月

Fundamental Limits of Network Error Correction

Dissertation Submitted to

Tsinghua University

in partial fulfillment of the requirement

for the degree of

Doctor of Philosophy

in

Information and Communication Engineering

by

Xiao Zhiqing

Dissertation Supervisor: Professor Wang Jing

May, 2016

关于学位论文使用授权的说明

本人完全了解清华大学有关保留、使用学位论文的规定，即：

清华大学拥有在著作权法规定范围内学位论文的使用权，其中包括：（1）已获学位的研究生必须按学校规定提交学位论文，学校可以采用影印、缩印或其他复制手段保存研究生上交的学位论文；（2）为教学和科研目的，学校可以将公开的学位论文作为资料在图书馆、资料室等场所供校内师生阅读，或在校园网上供校内师生浏览部分内容；（3）根据《中华人民共和国学位条例暂行实施办法》，向国家图书馆报送可以公开的学位论文。

本人保证遵守上述规定。

（保密的论文在解密后遵守此规定）

作者签名：_____ 导师签名：_____

日　　期：_____ 日　　期：_____

摘 要

本文研究通信网络中恶意攻击引入的篡改等错误对通信系统的影响，分析网络纠错的极限性能。本研究关注在有向图上的无噪通信，求解在任意给定有向图上的以下两个指标：

(1) 信道容量域。给定图上各链路的速率和纠错能力，求解网络纠错码可能达到的消息速率集合的闭包（即信道容量域）。对于信道容量域内部的消息速率，需构造相应的信道编码来实现这个速率的可靠传输；如果有一个码的消息速率在信道容量域外，需构造攻击方案使得传输不能正确进行。

(2) 容许速率域。给定图上需要可靠传输的消息速率和纠错能力，求解可以实现可靠通信的网络纠错码的链路速率的集合的闭包（即容许速率域）。对于容许速率域内部的链路速率，需构造相应的信源编码来实现可靠传输；如果有一个码的链路速率在容许速率之外，需构造攻击方案使得传输不能正确进行。

本文考虑的场景和主要结果如下：

(1) 一般有向网络中有且只有一个单播链路的场景。在这个场景下，只有一个源节点、一个目的节点。敌对方可以对链路上的信号进行篡改。主要的结果包括：给出了一般有向网络新的信道容量上界的求法，分析了有向网络的容许速率域并得到了外界，求得了两点网络对抗给定数目链路差错的容许速率域，分析了三点网络对抗给定数目链路差错的信道容量。

(2) 多址接入网络中有多个源节点、一个目的节点的场景。在这个场景中，多个源节点的信源可以是相关的，源节点和目的节点直接相连。敌对方可以干扰源节点和目的节点之间的传输。主要的结果包括：求得了多址接入网络分布式分层分集的容许速率域。

(3) 一般有向网络中有多个业务的场景。在这个场景下可能有多个单播或组播业务。主要的结果包括：证明了敌对方在前面提到的篡改攻击的基础上，再在网络中任意部分引入有限延时，也不会改变信道容量域和容许速率域。

关键词：网络纠错；组合信道；信道容量域；容许速率域

Abstract

This dissertation considers adversarial errors in communication networks, and analyzes the fundamental limitations of network error correction. This paper focuses on noiseless communications in directed graphs, and tries to solve the following two information-theoretical indices for arbitrary directed graphs:

(1) Capacity region. Fixing link rates and error-combating capability, the capacity region is defined as the closure of the set of message rates of network error correction codes. For any message rate inside the capacity region, a channel code needs to be constructed to transmit the message at that rate correctly; for any code whose message rate resides outside the capacity region, an attack strategy needs to be constructed to impede communications.

(2) Admissible region. Fixing the message rates and error-combating capability, the admissible region is defined as the closure of the set of link rates of network error correction codes. For any link rates inside the admissible region, a source code needs to be constructed to transmit the message correctly; for any code whose link rates reside outside the admissible region, an attack strategy needs to be constructed to impede communications.

Specifically, three scenarios are investigated:

(1) One unicast scenario. In this scenario, there are only one source node and only one destination node, and the adversary can temple with the signals on the links. Results include: A novel approach to derive the upper bound on the capacity in general directed networks; analysis of admissible region of general directed networks and an upper bound; solution of the admissible region in two-node networks; and analysis of the capacity in three-node networks.

(2) Multiple-access scenario. The primary result is to find the admissible region of distributed multi-level diversity model in the multiple-access network, where sources may be correlated.

(3) Multiple unicast/multicast scenario. The primary result is to prove that bounded delay in the combinatorial channel does not degrade the capacity region and the admissible region.

Key words: network error correction; adversarial error; channel capacity region; admissible region.

目 录

主要符号对照表

$\mathcal{A}$	敌对方可能控制的资源组合集
$A_{s^n \circ q^n}^{(z,z)}$	交互模型 $s^n \circ q^n$ 中纠正任意 z 个错的网络纠错码的最大消息集大小
$A_{s^n \circ q^n}^{(z,0)}$	交互模型 $s^n \circ q^n$ 中检出任意 z 个错的网络纠错码的最大消息集大小
$\mathcal{B}_{R,\mathcal{A}}$	有向图中消息速率为 R 、对抗错误 $\mathcal{A}$ 的容许速率域割集外界
$\mathsf{C},\mathsf{C}',\mathsf{C}'',\mathsf{C}'''$	网络纠错码
$\mathrm{CW}^n(m)$	某网络纠错码在消息为 m 时的码字
$\mathcal{C},\mathcal{C}(\mathbf{d}_{\mathcal{E}})$	信道容量域
C	信道容量
$C_{UB,s}$	三节点网络中由割 $\mathcal{E}_c(\{v_s\})$ 导出的信道容量上界
$C_{UB,t}$	三节点网络中由割 $\mathcal{E}_c(\{v_s,v_r\})$ 导出的信道容量上界
$\mathbf{d}_{\mathcal{E}}$	延时参数 $\mathbf{d}_{\mathcal{E}} \triangleq (d_e : e \in \mathcal{E})$，其中 d_e 是链路 $e \in \mathcal{E}$ 上的延时
Dec	译码器
$d_H(X_I,Y_I)$	Hamming 距离 $d_H(X_I,Y_I) \triangleq \left\lvert\{i \in I : X_i \neq Y_i\}\right\rvert$
$\mathcal{E}$	有向图中的链路集合
$\mathcal{E}_+,\mathcal{E}_+(\mathcal{V}_s)$	[由节点集 $\mathcal{V}_s$ 导出的] 前向链路集 $\{e \in \mathcal{E} : \mathrm{Tail}(e) \in \mathcal{V}_s, \mathrm{Head}(e) \notin \mathcal{V}_s\}$
$\mathcal{E}_-,\mathcal{E}_-(\mathcal{V}_s)$	[由节点集 $\mathcal{V}_s$ 导出的] 反向链路集 $\{e \in \mathcal{E} : \mathrm{Tail}(e) \notin \mathcal{V}_s, \mathrm{Head}(e) \in \mathcal{V}_s\}$
$\mathcal{E}_c,\mathcal{E}_c(\mathcal{V}_s)$	[由节点集 $\mathcal{V}_s$ 导出的] 割 $\mathcal{E}_c(\mathcal{V}_s) \triangleq \mathcal{E}_+(\mathcal{V}_s) \cup \mathcal{E}_-(\mathcal{V}_s)$
$\mathcal{E}_p$	路径 $p \in \mathcal{P}$ 经过的链路的集合
$\mathcal{E}_{st},\mathcal{E}_{ts},\mathcal{E}_{sr},\mathcal{E}_{rs},\mathcal{E}_{rt},\mathcal{E}_{tr}$	三节点网络中的链路集合，如 $\mathcal{E}_{st} \triangleq \{e \in \mathcal{E} : \mathrm{Tail}(e) = v_s \text{且} \mathrm{Head}(e) = v_t\}$
ε	交互模型中表示检测到错误的消息，其他情况表示小的正实数
Enc	编码器
$f_\alpha^{\mathbf{w}}$	线性规划 $\mathsf{LP}_{K,\alpha}^{\mathbf{w}}$ 的最优值
$\mathbf{f}_{\mathcal{E}} \triangleq (f_e : e \in \mathcal{E})$	链路速率
$\mathcal{G}$	有向图
$H(X)$	随机变量 X 的熵，或信号 X 的 Hartlay 信息（$H(X) \triangleq \log\lvert\mathcal{X}\rvert$）
$\mathrm{Head}(e)$	有向边 $e \in \mathcal{E}$ 的终点
$[i_1 : i_2]$	整数区间 $\{i \in \mathbb{Z} : i_1 \leq i \leq i_2\}$

$(i_1:i_2]$	整数区间$\{i\in\mathbb{Z}:i_1<i\le i_2\}$
$[i_1:i_2)$	整数区间$\{i\in\mathbb{Z}:i_1\le i<i_2\}$
$[i_1,i_2]$	实数区间$\{i\in\mathbb{R}:i_1\le i\le i_2\}$
$(i_1,i_2]$	实数区间$\{i\in\mathbb{R}:i_1<i\le i_2\}$
$[i_1,i_2)$	实数区间$\{i\in\mathbb{R}:i_1\le i<i_2\}$
I	区间
$\mathcal{I}(\text{事件})$	示性函数，其中事件真时为 1，假时为 0
$\mathrm{In}(v)$	以节点$v\in\mathcal{V}$结束的所有有向边的集合
$\mathcal{K}$	[单播/组播] 业务的集合
K	[单播/组播] 业务的个数
$\mathsf{LP}^{\mathbf{w}}_{K,\alpha}$，$\overline{\mathsf{LP}}^{\mathbf{w}}_{K,\alpha}$	以$\mathbf{w}\triangleq(w_1,w_2,\cdots,w_K)$为参数有$K$个自变量的线性规划问题
$\mathcal{M}$	消息集
M	发送的消息
$\hat{M}$	恢复的消息
$\mathbb{N}$	自然数集合
n	交互系统中的传输次数，有向图中网络纠错码的码长
$\mathrm{Out}(v)$	以节点$v\in\mathcal{V}$起始的所有有向边的集合
$\mathcal{P}$	路径集合
$\mathcal{P}(\mathcal{X})$	集合$\mathcal{X}$的幂集$\mathcal{P}(\mathcal{X})\triangleq\{X:X\subseteq\mathcal{X}\}$
$\mathcal{P}(\mathcal{X},i)$	集合$\mathcal{X}$的所有元素个数$\le i$的子集的集合
	$\mathcal{P}(\mathcal{X},i)\triangleq\{X\subseteq\mathcal{X}:\lvert X\rvert\le i\}$
$\mathcal{Q}$	[链路或传输的] 信号集
$\mathbb{R}$	实数集合
$\mathbb{R}_+$	非负实数集合
R	网络纠错码的消息速率
$\mathcal{R}$，$\mathcal{R}(\mathbf{d}_{\mathcal{E}})$	容许速率域
$\mathcal{R}^*_K$	多址接入直连网络实现分布式多层分集的容许速率域
$s^n\circ q^n$	交互模型，其中$s^n\triangleq(s_i:i\in[1:n])$表示传输方向，$q^n\triangleq(q_i:i\in[1:n])$
	表示各次传输的信号集大小
$\Sigma_z^{(d)}(\mathbf{f}^{(1)},\mathbf{f}^{(2)},\ldots,\mathbf{f}^{(d)})$	
	向量组$\mathbf{f}^{(1)},\mathbf{f}^{(2)},\ldots,\mathbf{f}^{(d)}$的删 z 和
$\mathcal{T}$	[由有向图生成的] 树
$\mathrm{Tail}(e)$	有向边$e\in\mathcal{E}$的起点

U^n	[多次重复的] 随机信源
$\hat{U}^n$	恢复出的 [多次重复的] 随机信源
$\mathcal{U}^n$	[多次重复的] 随机信源集合
$\mathcal{V}$	有向图中的节点集合
V	集合$[1:K]$的子集
v_s	源节点
v_t	目的节点
v_r	[三节点网络中的] 中继节点
$\mathbb{V}_{K,\alpha}$	集合$\{V \subseteq [1:K]:1 \le \lvert V \rvert \le \alpha\}$
$\mathbb{V}'_{K,\alpha}[V]$	集合$\{V' \subseteq [1:K] \backslash V : \lvert V' \rvert + \lvert V \rvert = \alpha\}$（其中$V \in \mathbb{V}_{K,\alpha}$）
$\mathbb{W}_K$	集合$\{(w_1, w_2, \cdots, w_K) \in \mathbb{R}_+^K : w_1 \ge w_2 \ge \cdots \ge w_K \ge 0\}$
X，X_i，X_e	[传输/链路的] 输入信号
$\lceil \mathbf{x} \rceil$	向量$\mathbf{x}$各元素上取整得到的新向量
$\lVert \mathbf{x} \rVert, \lVert \mathbf{A} \rVert$	向量和矩阵的元素 1 范数（各元素绝对值的和）
$\mathbf{x} \ge \mathbf{y}$，$\mathbf{A} \ge \mathbf{B}$	向量或矩阵间的大小关系（逐元素满足不等式关系）
$\lvert \mathcal{X} \rvert$	集合$\mathcal{X}$中元素的个数
Y，Y_i，Y_e	[传输/链路的] 输出信号
$\mathbb{Z}$	整数集合
z	错误的链路个数（一个自然数）
$\mathbf{0}$	各元素均为 0 的向量
$\mathbf{1}$	各元素均为 1 的向量

主要概念与定义索引

第 1 章　绪论

内容提要

本章介绍了研究背景，并对全文内容进行了介绍，描述了本文将要研究的各个子问题。对全文工作和创新点进行了总结，对遗留问题进行了介绍。

● 1.1 节介绍研究背景。通信网络中，恶意节点和链路会引入错误，带来重大影响。基于点对点的纠错方法和基于加密的安全协议不能处理此类错误（1.1.1 节）。这样的错误与传统物理层通信中遇到的错误的最大区别在于，本文中错误不是随机产生的，它是由当前网络拓扑、通信方案和被攻击者控制的资源组合唯一确定的（1.1.2 节）。错误可能是节点引入的，也可能是由链路引入的。在分析时，节点引入的错误和链路引入的错误可以相互转化。错误的具体形式有篡改、延时、删除等方法，其中篡改是最恶劣且最一般的攻击形式（1.1.3 节）。

● 1.2 节介绍研究目标与核心问题。本研究的目标是从理论上分析通信系统中的攻击错误会对系统的性能带来什么样的影响。1.2.1 节通过例子说明了攻击可能会造成通信容量降低，或是占用资源增加；1.2.2 节介绍了定量研究影响的核心问题：信道容量域问题与容许速率域问题。

● 1.3 节介绍其他研究人员的研究成果，包括分层分集码、网络纠错码等相关论文。

● 1.4 节介绍本文的研究方法：为了求得信道容量域与容许速率域，一方面要构造攻击方案得到它们的外界，另外一方面要构造网络纠错码得到它们的内界（1.4.1 节）；攻击方案构造的思想有：抽屉原理、信息支配、熵不等式等（1.4.2 节），网络纠错码的构造方法有基于码本的构造、组合知识传递、链路速率均一化等（1.4.3 节）。接着，从单次信道使用到多次信道使用的角度出发，考虑了单次交互模型，并介绍了关于该模型研究的主要结论和创新点（1.4.4 节）。

● 1.5 节介绍本文研究的三个场景：单发单收场景（1.5.1 节）、多发单收场景（1.5.2 节）、多发多收场景（1.5.3 节），介绍了各场景的模型、主要结论、创新点。1.5.4 节对创新点进行凝练和梳理。

● 1.6 节对全文的结构进行梳理。

1.1 研究背景

1.1.1 通信网络中的攻击错误会带来影响

在互联网时代，分布式应用已经融入了人们的日常生活。利用 P2P 技术的 uTorrent①、迅雷②、RaySource③等数据分享应用大大加速了数据的流动，基于 BOINC 框架④的 Climateprediction⑤、Quake-Catcher⑥、World Community Grid⑦等众筹计算应用获得了一个又一个鼓舞人心的成果，基于协同验证的 bitcoin⑧、Monero⑨、Litecoin⑩等无中心财富系统一次又一次牵动资本市场的神经，基于 git 的版本管理系统(11)和其衍生工具(12)成为知识流动的新载体。大量普通互联网用户的自发参与使得系统算力大大增加。

但是将不可靠的节点或链路资源引入系统的通信环节，可能会引来错误（特别是那些不能被通信底层识别的错误），最终导致传输的消息受污染，产生巨大后果。

案例 1：Kazaa 的噩梦 [1]

Kazaa 是 Sharman Networks[2] 于 2001 年推出的 [2]、基于自有 P2P 通信协议 FastTrack 的 [2] 文件分享应用 [2]。FastTrack 网络活跃用户曾高达 300 万人[1]，含有内容 5PB[1]，是当时最大的文件分享网络之一[1]。后来在 Kazza 系统中发现恶意节点，使得传输的数据块含有计算机病毒。在 2006 年 02 月时已有超过 22% 的数据块含有病毒[2]。Kazaa 于 2012 年 08 月停止运营 [2]。

1. 本案例改编自 https://en.wikipedia.org/wiki/Kazaa 和参考文献[1,2]。
2. 数据来源：https://en.wikipedia.org/wiki/Kazaa。

① 参见 http://www.utorrent.com/。
② 参见 http://www.xunlei.com/。
③ 参见 http://www.rayfile.com/。
④ 参见 http://boinc.berkeley.edu/。
⑤ 参见 http://www.climateprediction.net/。
⑥ 参见 http://qcn.stanford.edu/。
⑦ 参见 https://www.worldcommunitygrid.org/。
⑧ 参见 https://bitcoin.org/。
⑨ 参见 https://getmonero.org/。
⑩ 参见 https://litecoin.org/。
11 参见 https://git-scm.com/。
12 参见 https://github.com/、https://www.gitbook.com/。

案例 2：Apple 安全神话的破灭[1]

2015 年 9 月，微信、高德地图、滴滴打车、网易云音乐的 iOS 版[2]感染了称为“XCodeGhost”恶意代码，受影响的用户数超过 1 亿[3]。事件原因是不少开发者并没有直接从 Apple 的数据源上下载开发工具 XCode[4]，而是通过 P2P 下载等其他下载渠道，下载到了植入病毒的开发工具[4]。这种接力式下载造成了恶意程序的大范围传播。

1. 本案例改编自 https://en.wikipedia.org/wiki/XcodeGhost 和 http://baike.baidu.com/item/XcodeGhost。
2. 数据来源：http://tele.ofweek.com/2015-09/ART-8320506-8420-29006213.html。
3. 数据来源：腾讯安全应急响应中心，https://security.tencent.com/index.php/blog/msg/96。
4. 数据来源：http://baike.baidu.com/item/XcodeGhost。

案例 3：Tor 网络的“蜜罐”危机[1]

Tor 是一种匿名通信网络[2]。志愿者免费贡献节点和带宽搭建所谓的“洋葱路由”[2]，为其他用户免费提供虚拟通道，让其他用户免受流量过滤或嗅探分析[2]，保持其佚名性[2]。后有传言 NSA、FBI 等机构自主部署代理节点，伪装成志愿者，修改经过管道的数据，最终往佚名用户浏览器上植入嗅探代码以了解佚名用户的真实身份。这样的节点被业内人士称为“蜜罐节点”。2013 年 10 月，在“蜜罐节点”的帮助下，FBI 定位并逮捕了黑市交易网站 Silk Road 的负责人[3]。随后 Tor 网络发起为 Tor 网络捐款的号召，以用自有资金搭建可信节点，以遏制不断增加的恶意节点对佚名性带来的威胁[4]。

1. 本案例改编自 https://en.wikipedia.org/wiki/Tor_(anonymity_network) 和 http://www.deepwebs.org/2015/08/tor.html。
2. 信息来源：https://en.wikipedia.org/wiki/Tor_(anonymity_network)。
3. 信息来源：https://en.wikipedia.org/wiki/Silk_Road_(marketplace) 和 http://reason.com/blog/2016/03/02/fbi-beat-tor-anonymity-via-academic-rese。
4. 信息来源：https://www.torproject.org/donate/donate.html.en。

在以上的案例中，通信网络混入了不可靠的节点，通过篡改数据等方式，使得通信终端得到的消息并不是正确的消息。这样的错误无法被通信底层识别，也不能通过基于加密的安全算法识别，其原因如下：

(1) 错误往往经过了精心设计，所以其无法被低层通信协议识别。某个节点（或链路）在承担通信任务时，我们可以认为它具有发送（或承载）多种信号的能力（如果它不能发送任何信号或是只能发送一种信号，则它的行为是确定的，不具有通信能力）。假设在合法情况下，该节点可能发送的信号包括 x 和 $\bar{x}$。现在考虑这样的错误：当该节点应该发送 x 时，它却发送 $\bar{x}$。对于该信号的接收者

而言，由于 x 和 $\bar{x}$ 都是可能的发送选项，所以接收者不可能存在某种方案，识别出信号已被修改。

(2) 基于密钥的安全技术无法从根本上对抗这样的错误。一方面，引入错误的节点很可能有异常强大的计算能力或是充裕的计算时间（正如之前的三个案例中介绍的那样，为了篡改某数据块可以长达数月的线下计算，中间节点还可能是由 NSA、FBI 这样的机构部署的），计算出私钥是完全可能的。另一方面，当前加密算法的安全性往往基于未经证明的数学难题（比如大数分解），不排除现在或将来有方法能够轻易地解决它们（比如使用量子 Shor 算法进行大数分解[3,4]）。例如在 2013 年有报道发现，NSA 研究了在几个小时内破解 DHC 1024 密钥的方法，并应用在 Tor 网络的解密中[①]（随后 Tor 网络将加密算法升级到 ECDHE[②]）。目前确实存在着一些用加密方法辅助保证安全的文献，但是这样的方案中加密只是增加了攻击的计算复杂度，而并不能在根本上解决问题。值得一提的是，如果为了使用加密算法而使用另外的安全信道来传输连续的密钥流，那么就在事实上已经使用了分布式的网络校验与纠错方案（后称网络纠错码），而这样的方案中的安全性本质上是由安全信道保证，而不是由加密方案保证。

下面通过一个例子来描述通信网络中的攻击错误和网络纠错码。

例 1.1：考虑某单播业务，源节点 v_s 要向目标节点 v_t 发送消息。如图 1.1，节点 v_s 和 v_t 只能通过中继节点 v_r 连接。如果敌对方控制了中继节点 v_r，并且敌对方会尽其所能使得 v_t 收到错误的消息，那么由于 v_s 发送的所有信号都会被 v_r 篡改，v_s 不可能向 v_t 发送任何有价值的信息。

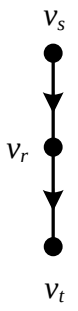


图 1.1　源节点 v_s 和目的节点 v_t 通过中继节点 v_r 连接

① 信息来源：http://blog.erratasec.com/2013/09/tor-is-still-dhe-1024-nsa-crackable.html
② 信息来源：http://tor-commits.torproject.narkive.com/gLyXyY24/tor-maint-0-2-4-switch-ecdhe-group-default-logic-for-bridge-relay-tls。

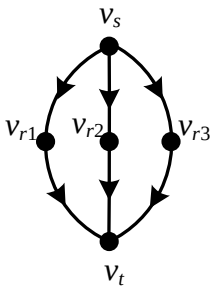


图 1.2　源节点v_s和目的节点v_t通过三个中继节点v_{r1}、v_{r2}和v_{r3}连接

为了保证从源节点v_s到目的节点v_t的可靠通信，可以使用多路由的方案。在图 1.2 中，源节点v_s和目的节点v_t间通过三个中继节点v_{r1}、v_{r2}和v_{r3}传输。假设这三个中继节点中至多有一个节点被敌对方控制。现在源节点v_s在发送消息时，让这三个中继节点同时传输消息给目的节点v_t。在这种情况下，即使敌对方控制了某个中继节点（记为v_{ri}，i是 1,2,3 中的某个数），它也不能篡改信号。这是因为，如果v_{ri}篡改了信号，目的节点v_t收到的三份数据就会不一样。通过比对这三份数据，v_t就会发现哪个中继节点篡改了信号。然后，v_t可以通过没有被篡改的两份数据正确恢复出消息。另外会产生的副产物是，v_t就会意识到某个v_{ri}已经被敌对方控制，将在以后都不再采纳v_{ri}传来的信号。

值得一提的是，如果敌对方控制了两个或是更多的中继节点，那么该网络纠错码不能保证可靠通信。　□

在上述的例子中，图 1.2 所示使用三个中继节点传输消息的就是一种网络纠错码。这种纠错码解决了“网络中敌对方可以控制任意一个中继节点”这样的网络攻击。实际上，网络的拓扑、业务、攻击形式远比这复杂的多，本文将从信息论的角度，对通信系统中的错误及其纠正进行理论研究。

1.1.2 不能用概率模型刻画攻击错误

从上节中的例子可以看出，我们要研究的信道中的错误，并不是以概率形式出现，而是由组合形式出现。

自 C.E. Shannon 创立信息论[5,6]以来，大部分的研究都是将通信信道建模为概率信道，即用转移概率来刻画信道。例如，点对点无记忆信道常用转移概率$p(y|x)$来表征，点对点双向无记忆通信信道常用$p(y_1,y_2|x_1,x_2)$来表征，无记忆中继信道常用$p(y_2,y_3|x_1,x_2)$来表征，多节点无记忆网络信道常用$p(y_1,y_2,\cdots,y_M|x_1,x_2,\cdots,x_M)$表征[7]。概率信道在本质上认为，信道的拓扑是不变

的，信号的传递以概率形式演变。这样的模型特别适合于物理层所面对的通信媒质，例如无线通信物理层需要面对的电磁波信道、光纤通信所要面对的光路。但是，这样的概率模型并不适用于本文需要解决的攻击错误。对于通信系统中的敌对方在理性的情况下，它不会以某种概率发动攻击，而是会以一种最佳的方案进行攻击：如果当前网络纠错码能被攻破而且不会被发现，则敌对方完全可以进行攻击；如果当前系统能够发现所有产生的攻击并将攻击者绳之以法（例如剔除出网络），甚至还能够保证通信的正确性，那么敌对方定然会保存实力，使其掌握的节点和链路像正常的节点和链路一样，不发动攻击[8,9]。从这个意义上看，攻击的发生并不服从概率分布，而是由系统配置和当前状态唯一确定。

这样的组合特性最主要体现在错误资源的组合性。例 1.1 中图 1.2 采用的网络纠错码可以纠正的错误为任意一个中间节点进行的恶意篡改。当敌方最多控制一个中继节点时，敌方掌握的资源组合可能有以下几种：(1) 敌方掌握且仅掌握节点 v_{r1}，这时敌方掌握的资源组合记为 $\{v_{r1}\}$；(2) 敌方掌握且仅掌握节点 v_{r2}，这时敌方掌握的资源组合记为 $\{v_{r2}\}$；(3) 敌方掌握且仅掌握节点 v_{r3}，这时敌方掌握的资源组合记为 $\{v_{r3}\}$；(4) 敌方不掌握任何中继节点，这时敌方掌握的资源组合记为 $\varnothing$。也就是说，在敌方掌握资源的能力限制在至多一个中继节点的情况下，敌方掌握的资源组合必然是集合 $\{\varnothing,\{v_{r1}\},\{v_{r2}\},\{v_{r3}\}\}$ 中的一个元素。这就是信道的组合特性的最主要的表现：敌方掌握的资源的组合，是一个给定的组合集中的某个元素，这个元素代表着网络中资源的组合。在这个资源组合上发送或传递的信号有可能出错，其他信号不会被敌对资源破坏。

这样的组合特性来源于对敌方掌握资源的限制，而这样的限制常常出现在网络安全领域。比如我们对敌方拥有的节点数量有一定的上限估计，或是只希望系统对抗某种强度的敌对势力，或者网络资源只有在允许在敌对势力有某种限制的情况下才能有效使用。例如在例 1.1 的图 1.2 采用的网络纠错码假设敌方最多只能掌握 1 个中继节点。如果敌对势力没有只能掌握 1 个中继节点的限制，而是能够掌握任意两个中继节点，可以证明，这样的网络中不存在网络纠错码可以完成任意数据的通信。

事实上，组合特性是在生活中广泛出现的特性，我们的日常认知中也大量设计纠错能力有限的机制来在有限的代价下对抗可能出现的意外情况。例如：(1) 在专业跳水比赛的分数统计环节往往会去掉一个最高分并去掉一个最低分①，这样的机制可以在有一个裁判偏袒导致分数畸高或有一个裁判偏袒导致分数畸低的情况

① 参见 http://diving.about.com/od/meetscompetitions/a/judgingBasics.htm。

下保证公平，但是不能在所有裁判都同时偏袒导致分数畸高的情况下还得到公平的分数；(2) 为了容错我们常常将数据备份得到两份完全相同的数据[①]，这样的备份方案可以在某一份数据由于硬盘失效或其他原因不能读出的情况下仍然不丢失数据，但是不能解决两个数据备份同时失效的情况；(3) 美国部署的反导弹系统[②]可以同时截拦一定数目的导弹（比如 5 个），但是在同时有数万枚导弹同时对美国本土发动攻击时就无法同时截拦。与这些生活中的例子类似，通过在通信系统中的网络纠错码也往往对假想敌控制的资源有限制性假设，超过此限制性假设的敌对资源引发的错误可能是不能应对的。在最特殊的情况下，如果攻击者控制了所有的链路和中间节点，那么攻击者总可以将一个消息的信号篡改为其他消息的许用码字，即在网络中不可能设计出有任何纠错能力或检错能力的网络纠错码。

另外，由于我们主要研究信道的组合特性，所以我们可以假设每个点对点链路的传输都是无错的。即可以认为底层的通信协议已经保证了网络中各链路通信的可靠性。

由于本研究中的信道是组合信道，所以在本研究中涉及的概念，如信道编码、信源编码、信道容量域、容许速率域都和在概率信道中的相应概念有不同，是组合信道中的对应版本。

关于本研究中组合信道模型及假设的严格数学描述，参见第 3 章。

1.1.3 错误的具体形式

从错误的直接来源分，错误可以分为节点错误和链路错误。从错误的表现形式分，错误可以分为篡改、延时、和删除。

节点错误：当敌对方控制了某个节点的时候，可以控制该节点的所有输出，引发节点错误。值得一提的是，对某个业务而言，如果敌对方控制了源节点或是目的节点中的任何一个，则这个通信业务都不可能正常运行。所以一般在考虑节点错误时，只考虑其中继节点错误，不考虑源节点或是目的节点的错误。

链路错误：当敌对方控制了某个链路时，可以控制该链路的输出，引发链路错误。

① 参见 https://en.wikipedia.org/wiki/Standard_RAID_levels。
② 参见 https://en.wikipedia.org/wiki/United_States_national_missile_defense 和 https://en.wikipedia.org/wiki/Ground-Based_Midcourse_Defense。

节点错误和链路错误之间可以相互转换。敌对方控制了某个节点，就相当于控制了该节点的所有输出链路。当敌对方控制了某条链路时，相当于在该链路上增加了一个被敌对方控制的节点。

当敌对方控制控制了某个节点和链路的输出时，可以维持原有的信号不变，或将原有信号修改为其他另外的信号，或是以某种形式增加信号传输的延时，或使得信号消失形成信号中断的表象。在某个特定的通信系统中敌对方允许的行为和底层通信与协议设计均有关。比如某协议可以要求当传输时延大于某个值时接收端按照信号中断来进行处理，也可以底层保证协议信号不能中断。另外，延时可以与篡改组合使用。

事实上，延时和中断也算是篡改的具体形式：拖延信号的行为也可以看作将原信号在某时刻的值修改为某过去时间的信号的值；中断信号的行为也可看作将原信号篡改为没有信号（例如电平值一直为零）。从这个意义上看，篡改可以包括所有的攻击行为。

1.2 研究目标

在前面的分析中，我们探讨了在通信网络中攻击方引入的错误。本文的目标，就是去分析在通信网络中攻击方的存在可能会造成什么影响。

1.2.1 直观理解攻击对通信网络系统的影响

从直观上看，在通信网络中存在攻击方，可能会造成可靠通信速率降低，占用的网络资源变多。

例 1.2[①]：如图 1.3，网络$\mathcal{G}_3$中有一个单播业务，从源节点v_s到目的节点v_t间有三条容量为 1bit/s 的链路。在网络中不存在错误的情况下，用最大流最小割可以计算该网络容量为 3bit/s。现在如果攻击方可以控制其中任意一条链路，发生恶意篡改错误，则可以证明，从v_s到v_t可靠传输的容量下降为 1bit/s。　□

① 本案例改编自文献[10]。

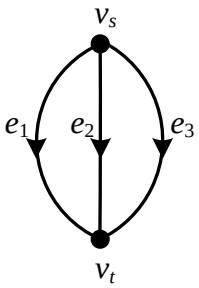


图 1.3　有向图$\mathcal{G}_3$：源节点v_s和目的节点v_t通过三个链路连接（该图改编自文献[10]）

在例 1.2 中，网络中存在错误和不存在错误的情况下，网络的拓扑和各链路速率是相同的。这两种情况的区别就是是否存在错误。存在错误的容量 1bit/s 比不存在错误的容量 3bit/s 小。所以，我们可以直观看出攻击方的存在可能带来的一个影响是：在网络拓扑和链路速率不变的情况下，攻击方的存在会降低可靠通信的速率。

例 1.3：如图 1.3，网络$\mathcal{G}_3$中有一个单播业务，从源节点v_s到目的节点v_t间有需要支持 1bit/s 的消息速率。在网络中不存在错误的情况下，用最大流最小割可以计算得到，当三条链路速率$\left(f_{e_1}, f_{e_2}, f_{e_3}\right)$满足$f_{e_1}+f_{e_2}+f_{e_3}\geq 1\text{bit/s}$时，就可以实现可靠传输。现在如果攻击方可以控制其中任意一条链路，发生恶意篡改错误，则可以证明，三条链路速率$\left(f_{e_1}, f_{e_2}, f_{e_3}\right)$需要同时满足$f_{e_1}\geq 1\text{bit/s}$，$f_{e_2}\geq 1\text{bit/s}$和$f_{e_3}\geq 1\text{bit/s}$，才能保证以 1bit/s 可靠传输消息。 □

在例 1.3 中，在不存在错误和存在错误的情况下，需要可靠支持的消息传输速率是相同的，网络拓扑也是相同的。这两种情况的区别就是是否存在错误。不存在错误的时候链路速率的可取值范围大于存在错误情况下链路速率的可取值范围。所以，从此可以直观看出，攻击错误带来的另一个影响是，在网络拓扑和消息速率不变的情况下，攻击的存在要求可靠通信占用更多的链路资源。

1.2.2 定量分析攻击的影响：信道容量域问题和容许速率域问题

在概率信道的研究中，信道编码设计与其对应的信道容量域的求解和信源编码设计及其对应的容许速率域求解是信息论最核心的两大问题。网络纠错的研究也是如此。

信道容量域是表征一个消息可靠传输快慢指标。当信道容量域范围越大[①]的时候，就表示消息可以可靠传输的速度快，在单位时间能内传更多的消息；信道容

① 严格的说，这里的“大”并不是恰当的数学描述。这里只是直观地表示其包含的空间多、空间的体积大。

量域范围越小的时候，就表示消息可以可靠传输的速度慢。关于信道容量域严格的数学定义，可参见 3.3 节定义 3.1。

网络纠错信道编码与信道容量域问题是：给定网络拓扑和纠错能力，限定网络中的各链路容量，求得该网络可靠通信的容量域及实现容量的信道编码方案。

例 1.4[①]：如图 1.3，网络$\mathcal{G}_3$中有一个单播业务，从源节点v_s到目的节点v_t中有三条容量为 1bit/s 的链路。这三条链路中最多有一条链路会被敌方控制，发生恶意篡改错误。可以证明，从源节点v_s到目的节点v_t可靠传输的容量为$C=1\text{bit/s}$，实现容量的信道编码方案为将消息均在三条链路上原样发送，目的节点用大数判决恢复出消息。这意味着，如果从源节点v_s到目的节点v_t要传递小于 1bit/s 的消息，肯定存在一种信道编码方式能够保证可靠传输；如果从源节点v_s到目的节点v_t要传递大于 1bit/s 的消息，必然不存在一种信道编码方式能够保证可靠传输。 □

容许速率是链路速率的集合，容许速率域是表征耗费网络资源的指标。当容许速率域小[②]的时候，占用的资源少；当容许速率域大的时候，占用的资源多。关于容许速率域严格的数学定义，可参见 3.3 节定义 3.2。

网络纠错信源编码与容许域问题是：在给定网络拓扑和纠错能力，给定需要传输的信源，求得容许速率域及其实现信源无失真通信的信源编码方案。

例 1.5：如图 1.3，网络$\mathcal{G}_3$中有一个单播业务，从源节点v_s到目的节点v_t有三条链路e_1、e_2和e_3，这三条链路中最多有一条会被敌方控制，发生恶意篡改错误。现有$H(U)=1\text{bit/s}$的信源需要从v_s传到v_t。可以证明，在链路e_1、e_2和e_3上容许速率域为

$$\mathcal{R}=\left\{\left(R_{e_1},R_{e_2},R_{e_3}\right):R_{e_1},R_{e_2},R_{e_3}\geq 1\text{ bit/s}\right\}.$$

达到容许域极点$(1,1,1)\text{bit/s}$的信源编码方案是将信源在三条链路上原样发送。这个结论用通俗的话说就是：如果三条链路上允许的速率都大于 1bit/s，则肯定存在一种信源编码方式能够保证可靠传输；如果有任意一条的速率小于 1bit/s，则必然不存在信源编码方式能够保证可靠传输。 □

① 本案例改编自文献[10]。

② 严格的说，这里的“小”并不是恰当的数学描述。这里只是直观地表示其包含的空间少、空间的体积小。

1.3 文献综述

对网络纠错与组合信道的研究包括针对删除的网络分集、针对篡改错误的网络纠错码和探寻组合信道本质的熵空间与熵不等式的研究。本文对其他学者的相关工作进行介绍。本部分涉及的话题与综述与教程文献[11]涉及的话题有重合。

1.3.1 网络分集相关文献：分集码和分层分集码

利用网络中的链路冗余和节点冗余进行差错控制，最早可以追溯到网络生存性问题。在上个世纪，已经有许多研究人员研究了如何利用多条独立的路径，使用分集码[12]来进行网络分集[13]。对分集码的研究可以进一步追溯到对最大距离可分码（又称 MDS 码，Maximum Distance Separable 码）的研究[14]。文献[15]全面介绍了如何利用多路径分集提高网络生存性。

随后，文献[16]和[17]提出了分层分集码的概念。其中，文献[18–20]彻底解决了对称多层分集码的问题。更多关于分层分集码的研究可以参见文献[21–26]。

针对更复杂的网络拓扑，文献[27]首次研究了在网络编码系统中链路失效的问题。更多针对网络编码中链路失效的研究还包括文献[28,29]。

另外，还有采用子空间作为传输对象来进行网络分集。这样的设计成为子空间码。子空间码将每个信源符号映射为一个子空间，而在网络中传输子空间中的基，接收端通过恢复出子空间来恢复出信源符号。子空间码中的随机构造版本由 Koetter 和 Kschischang 提出[30–34]。文献[35]给出了类似于喷泉码的无率码的子空间码构造方法。特别值得一提的是，子空间码不但可以用来分集，还能用来纠正网络中的错误，也属于下一节要介绍的网络纠错码。

1.3.2 网络纠错码相关文献

2002 年，蔡宁和杨伟豪指出可以利用网络编码纠正网络中错误[36]，开启了有关网络纠错的研究。网络纠错码的早期研究主要包括对网络纠错码的差错控制性能和码字界的研究。

网络纠错码的差错控制性能

网络差错控制与传统差错控制最大区别在于差错形式不同。文献[37,10]对重量和距离这两个概念进行了严格的定义和区分。并得到了在线性网络编码下重量和距离的多种性质。文献[10]针对多种度量，给出了两种最小重量译码器，并分析了这两种译码器之间的关系。同时，他分析了非线性网络纠错码的纠错特性与

检错特性。并举例说明了在非线性网络编码中用于纠错时可纠错误数可以超过用于检错时可检错误数的一半。

网络纠错码字界

文献[38]和[39]首次给出了类似于经典纠错码的网络纠错码的 Singleton 限、Hamming 限和 Gilbert-Varshamov 限，它们只能用在各链路速率相等的有向无环图中。

线性网络纠错码

在网络纠错码最初的文献[38,39]中，就已经说明了如何在各链路速率相同的有向无环图中实现线性网络纠错码，并达到容量。张箴等在文献[40–42]中系统分析了线性网络纠错码。该文考虑了单个单播业务或组播业务，扩展了线性网络编码中全局核向量的概念并由此引申出线性网络纠错码的译码方程，该文还定义了线性网络纠错码的最小秩，并指出该最小秩具有经典纠错码纠错数特征。并给出了一种最小秩的译码算法。利用该极小秩得到的改进的 Singleton 界是可以达到的[43–45]。这一结论在事实上给出了在单源单宿各链路速率相等的有向无环图中达到纠正任意 z 条链路错误（z 是一个正整数）的纠错容量的网络纠错方案。

Ho 等在文献[46]中分析了随机网络编码和随机网络纠错码，并给出译码失败的概率限。随机网络纠错码能够更好地适应网络拓扑的变化。随后，Balli 等对其进行了更细致的分析，针对不同的纠检性能对概率界做了推广[47,48]。光炫等人结合对最大距离可分码的扩张域大小进行研究，给出了在文中随机构造算法情况下译码失败概率界[45,49]。

对网络纠错码的构造尝试还包括前文提到的子空间码[30–34]，另外还有基于拟阵的网络纠错码[50]和利用广播变换限制差错传播的编码[54]。

达到容量的网络纠错码：单个源节点的情形

前面提到，采用特殊设计的线性网络编码可以在各链路速率相等的有向无环图中达到 Singleton 界，这意味着它可以在这情况下达到纠正任意 z 条链路错的纠错容量[39–45]。但是，对于一般的可能有环的或是各链路速率不等的网络，线性编码不一定能达到容量[8,55,56]。在单源单宿的有向图中，达到纠错容量的网络纠错方案主要有猜测转发（Guess and Forward）[8,51]和多面体码（Prototype Code）[9,52]。各种方案的总结见表 1.1。

表 1.1　达到网络纠错容量的网络纠错码及其适用范围

实现方案	差错控制形式	网络拓扑
线性网络纠错码[39–45]	纠正 任意 z 条链路错	有向无环图，各链路速率相等
猜测转发 （两节点网络）[8,51]	纠正 任意 z 条链路错	只有两个节点的有向图
猜测转发 （锯齿网络）[8,51]	纠正 任意 z 条链路错	有向无环图，各边速率 满足某些关系的非交叠锯齿网络
某种非线性 网络纠错码[8,51]	纠正 任意 1 条链路错	蟑螂网络，给定某种链路速率
多面体码[9,52]	纠正任意 1 个 中间节点错	有向无环平面图，各边速率相等 每个中间节点的出边数≤min{入边数, 2}

猜测转发[8,51]：这是一种在某些有向图中达到对抗任意 z 条链路错的纠错容量的网络纠错方案。它适合以下两种有向图：(1) 两节点网络，这是一种有环网络，这个网络中除了源节点和宿节点外没有其他节点；(2) 满足某些条件的非交叠锯齿网络（Non-overlapping ZigZag network），这是一种有向无环网络，它包括四点无环网络（Four-node acyclic network），只有在各链路速率满足某些条件的情况下才可以达到容量。

多面体码[9,52]：这是一种能够达到纠正任意一个中间节点错误的纠错容量的网络纠错方案。它能够适用的有向网络需同时满足：(1) 是无环平面图；(2) 各边速率相等；(3) 每个中间节点的入边数大等于出边数，并且每个中间节点的出边数不超过 2。多面体码采用类型论的方法设计。

达到容量的网络纠错码：多址接入的情形

关于多个源节点、一个目的节点的有向网络中的网络纠错信道容量的研究首现于文献[57]。文献[57]讨论各链路速率相同的有向无环网络，考虑在有固定数目的链路错误的情况，构造线性网络纠错码，求得了信道容量域。

文献[58]考虑了网络纠错信源编码问题，其主要是从方法上考虑，其研究模型具有随机性，和本文的模型有区别。

综述与教程

与网络纠错相关的综述和教程文章除了前文提到的文献[11]外，还有文献[60]和[61]。

1.3.3 熵不等式与熵空间相关文献

C.E. Shannon 在创立信息论时就发现了熵不等式的存在性[5]。文献[62]发现的大量的熵不等式均等价于不等式 $I(X_1;X_2\mid X_3)\geq 0$，可以将它们归为一类。文献[63]把这一类的不等式称为 Shannon 类型不等式，并证明了除了 Shannon 不等式外，还存在其他熵不等式，并把其他熵不等式称为非 Shannon 类型不等式。文献[64]首次给出了一个显式的非 Shannon 类型不等式。后来越来越多的非 Shannon 类型不等式被找到[65–70]。文献[70]证明了无穷多个非 Shannon 类型不等式。文献[71]证明了即使是 4 个变量的非 Shannon 不等式就有无穷多个。

熵空间是由熵不等式刻画的空间[63]。文献[72]证明了熵空间与网络信息论中信道容量域问题的等价性。自此学术界意识到网络信息论的核心难点在于熵空间刻画的困难性。在本文中（特别是第 5 章）将大量使用熵不等式的相关结果，包括 Han 不等式[73]。

1.4 研究方法与研究思想

本节先介绍求解信道容量域和容许速率域的一般方法，最后介绍一些攻击方案的构造思想和网络纠错码的构造思想，最后介绍从单次到多次的求解策略和交互信道模型。

1.4.1 求解信道容量域和容许速率域的一般方法

对于某单播业务（一个源节点、一个目的节点的业务）而言，其求解信道容量的基本方法如下：

(1) 下界求取：构造码长为给定正整数 n、消息集合大小为 M_n 的信道编码 C_n，证明其可以正确传递消息，这样可以得到容量的下界 $\sup_{\mathsf{C}_n}\frac{1}{n}\log M_n$。

(2) 上界求取：给定速率 R，对于任意的正整数 n，任意码长为 n、消息集大小大于 2^{nR} 的码，找到一种错误图样（攻击方式），使得消息不能正确传送。

当求得的上界和求得的下界相同时，求得的界就是信道容量，在求取下界时构造的码就是达到容量的信道编码。 □

对于多个业务的可达速率域，也有类似于上述下界求取方法的内界求取方法和类似于上述上界求取方法的外界求取方法。

对于某业务需求的某条链路而言，求解容许速率域的基本方法如下：

(1) 内界求取：构造码长为给定正整数 n、码字集大小为 M_n 的信源编码 C_n，证明其可以正确传递消息，这样得到容许速率内界 $\inf \frac{1}{n}\log M_n$。

(2) 外界求取：给定速率 R，对任意码长为 n、码字集大小小于 2^{nR} 的码，都找到一种攻击方式，使得消息不能正确传送。

当内界和外界相同时，求得的界就刻画了可达速率的上确界，在求取内界时构造的码就是达到容许速率域边缘的信源编码。 □

对于有多条链路的可达速率域，也有类似的内界和外界求取方法。

通过对比信道容量域和容许速率域的求解方法，我们发现，这两个问题的求解有着相同的研究思路。一方面，要构造网络纠错码求得内界；另一方面，要构造攻击方案求得外界。

1.4.2 外界求解与攻击方案构造：抽屉原理、信息支配和熵不等式等

本节介绍外界求解的相关思路。

前文已经提到，一般而言，为了证明一个外界，需要考虑任意一个消息速率或链路速率在外界之外的网络纠错码，证明存在一种攻击方案可以使得这个码不能正确消息。那么，如何找到这个攻击方案呢？

一种最简单、最幼稚的想法，就是将这个网络上所有的码都列举出来，然后一一构造攻击方案使得恢复出的消息不等于原消息。但是由于码的数目是无穷多的（事实上码长 n 就有无穷多的取值），所以将码一一列举是不可能的。所以，更为实际的做法是，将所有的码分为一类或多类，证明每类的码具有某些性质，然后根据这些性质为每一类码设计攻击方案，使得其不能正确传输。

上述过程的核心，就是要发现码具有的性质。下面介绍如何发现这样的性质。

抽屉原理

抽屉原理是人类在组合数学方面发现的最古老的命题之一[①]。它的内容如下（选入本文时有改动）：

原理 1.1（第一抽屉原理，又称 Dirichlet 抽屉原理）： m, n 是两个正整数。信号 $X \triangleq (X_1, X_2)$ 由 X_1 和 X_2 由两部分组成。若信号 X 有 $> mn$ 种可能的取值，且信号 X_1 可能的取值数 $\le n$。则信号 X 必然有两种不同的取值 $x^{(1)} \triangleq \left(x_1^{(1)}, x_2^{(1)}\right)$ 和 $x^{(2)} \triangleq \left(x_1^{(2)}, x_2^{(2)}\right)$，使得 $x_1^{(1)} = x_1^{(2)}$。 □

① 目前主流数学界认为该原理归功于 Dirichlet，1834。

可以利用抽屉原理设计攻击方案。下面通过一个例子简单的说明其可能性。考虑有向图$\mathcal{G}=(\mathcal{V},\mathcal{E})$上的某个网络纠错码$\mathsf{C}$，其码长为$n$，消息速率为$R$，各链路速率为$\mathbf{f}_{\mathcal{E}}\triangleq(f_e:e\in\mathcal{E})$，纠错能力$\mathcal{A}=\{\mathcal{E}\setminus\mathcal{E}_1,\varnothing\}$，其中$\mathcal{E}_1\subseteq\mathcal{E}$是一个链路子集，且满足$\sum_{e\in\mathcal{E}_1}f_e<R$。这个网络纠错码的消息集大小为$2^{nR}$，在这个链路集合$\mathcal{E}_1$上可能的信号数为$2^{n\sum_{e\in\mathcal{E}_1}f_e}$。注意到$2^{n\sum_{e\in\mathcal{E}_1}f_e}<2^{nR}$，根据抽屉原理，我们就发现了码$\mathsf{C}$的一个限制：在消息集上会存在两个不同的消息，会使得在链路集合$\mathcal{E}_1$上传输的信号相同。这样，这个链路集合$\mathcal{E}_1$上传输的信号就不具有分辨两个消息的能力。这样，就发现了一种攻击方案：就是令传输这两个消息时在$\mathcal{E}\setminus\mathcal{E}_1$上传的信号都一样。这样在发送这两个消息时，整个网络上传输的信号都相同。这样目的节点就不可能在这种攻击方案下正确分辨出这两个消息。

信息支配

信息支配是信息处理定理在网络中的一种表现[①]。利用信息支配，可以进一步的发现网络纠错码的限制。

信息处理定理的大意如下：如果变量Y是由变量X经过确定性运算得到的，那么变量Y的取值可能数不大于变量X的取值可能数。定义变量X（或Y）取值的可能数的对数为变量X（或Y）的 Hartley 信息量$H(X)$（或$H(Y)$）[②]，则有$H(Y)\le H(X)$。

在没有错误的网络编码问题中，文献[74]首次提出了“信息支配”这一概念。在有向图$\mathcal{G}=(\mathcal{V},\mathcal{E})$上，对于某个节点集$\mathcal{V}_1\subseteq\mathcal{V}$，它的输出信号（即链路$\mathrm{Out}(\mathcal{V}_1)\triangleq\{e\in\mathcal{E}:\mathrm{Tail}(e)\in\mathcal{V}_1\}$上的信号）是由其输入信号（即链路$\mathrm{In}(\mathcal{V}_1)\triangleq\{e\in\mathcal{E}:\mathrm{Head}(e)\in\mathcal{V}_1\}$上的信号）计算得到。这时，文献[74]称节点集$\mathcal{V}_1$的输入链路$\mathrm{In}(\mathcal{V}_1)$信息支配了输出链路$\mathrm{Out}(\mathcal{V}_1)$。

上述信息支配的概念可以推广到可能有攻击错误的网络。与不存在攻击错误的网络编码模型相比，节点和链路可能被攻击方控制，进而导致输出链路（如前文中的$\mathrm{Out}(\mathcal{V}_1)$）上的信号不仅由输入链路（如前文中的$\mathrm{In}(\mathcal{V}_1)$）确定，还可能由攻击来确定。

特别的，对于某个不可能被攻击方控制的节点集$\mathcal{V}_1\subseteq\mathcal{V}$，在没有攻击的情况下，它的输出信号$X_{\mathrm{Out}(\mathcal{V}_1)}$确实是由它的输入信号$Y_{\mathrm{In}(\mathcal{V}_1)}$完全确定，即$H\left(X_{\mathrm{Out}(\mathcal{V}_1)}\right)\le H\left(Y_{\mathrm{In}(\mathcal{V}_1)}\right)$。利用这个限制可以进一步减小$X_{\mathrm{Out}(\mathcal{V}_1)}$取值的可能数。

① 在无噪网络编码的研究中存在类似的观点。详见后文。

② 在本文中，若变量 X 不是随机变量，则 $H(X)$ 表示 Hartley 信息量。

熵不等式

前面提到了可以利用信息支配得到两个信号集合承载信息的关系。而利用熵不等式，有机会进一步获得多个信号集合承载信息的关系。

考虑图$\mathcal{G}=(\mathcal{V},\mathcal{E})$上的两个链路子集$\mathcal{E}_1,\mathcal{E}_2\subseteq\mathcal{E}$。在没有错误的情况下，其上承载的信号$X_{\mathcal{E}_1}$和$X_{\mathcal{E}_2}$满足不等式[①]

$$H\left(X_{\mathcal{E}_1}\right)+H\left(X_{\mathcal{E}_2}\right)\geq H\left(X_{\mathcal{E}_1\cup\mathcal{E}_2}\right)+H\left(X_{\mathcal{E}_1\cap\mathcal{E}_2}\right).$$

这个不等式刻画了 4 个链路集合$\mathcal{E}_1$、$\mathcal{E}_2$、$\mathcal{E}_1\cup\mathcal{E}_2$、$\mathcal{E}_1\cap\mathcal{E}_2$上承载信号的关系。除了这种次模（submodular）类型的不等式外，还有许多的熵不等式[②]。利用这一不等式，可以进一步刻画多个链路集合上承载信号之间的关系，得到更多的限制以设计攻击方案。

1.4.3 内界求解与网络纠错码构造：组合知识传递、链路速率分割等

本节简要介绍网络纠错码的构造思路。

虽然网络纠错码的码长可以任意长，但是任意一个网络纠错码的码长都是有限的。在构造网络纠错码或攻击方案的时候，往往将码长作为参数进行分析。例如，在构造网络纠错码求解信道容量下界的时候，可以先构造以码长n为参数的码，然后计算它在码长为n的情况下的消息速率为R_n，最后对所有可行的n取速率的上确界得到信道容量的一个下界。所以，对给定码长n的网络纠错码进行分析是整个网络纠错码分析的基础。

组合知识及其传递

组合知识的定义：将一个节点意识到的所有可能的组合视作该节点得到的组合知识。如果某个节点认为攻击方可能掌握的组合和网络纠错码设计之初针对的组合相同，那么这个节点就没有获得任何组合知识，处于无知识状态。如果某个节点能够完全确定攻击方控制了那个组合，那么这个节点就获得了有关攻击方的全部组合知识，处于完全知识状态。

组合知识传递的原理：在传输过程中，在每个节点的知识范围内，可能的错误组合不断减少。这就相当于节点逐渐获得了组合知识。具体而言，当一个节点往另一个节点传输信号时，这个传输既有可能发生错误，也有可能没有错误。如果这个传输没有发生错误，则这个信号承载的知识就会全部传递给下游节点；如

① 这一不等式是熵的次模特性的直接应用。熵的次模特性是熵的定义的自然延伸，一般将其归功于 C.E. Shannon 的成果。

② 除了次模类型的不等式外还有其他不等式这一结果可认为归功于文献[63]中非 Shannon 类型不等式的发现，具体参见 1.3.3 节。

果这个传输发生了错误，则目的节点就知道错误组合包括这次传输。由于有些组合不包括在这两种情形的任意一种情形，所以目的节点有可能据此获得组合信道状态知识。当目的节点了解到足够的组合信道状态知识时，就有可能正确恢复出消息。可以利用这一原理构造网络纠错码。

值得一提的是，对于宿节点而言，它即使最终没能获得全部的组合知识，也可能能正确恢复出消息。

直观理解组合知识传递原理

下面通过一个虚构的故事，来直观了解什么是组合知识，组合知识是如何传递的。

某秘密帮派的老大有甲、乙、丙、丁 4 个小弟。据可靠线报，这 4 个小弟中有且只有两个人是卧底，它常常干扰行动的进行。这时候，对这个老大而言，可能的恶意组合有 {甲, 乙}、{甲, 丙}、{甲, 丁}、{乙, 丙}、{乙, 丁}、{丙, 丁} 六种。这六个组合构成的集合就是初始的组合知识。

一开始老大处于无知识状态。老大在日常的工作中，会去想一些办法了解到底谁是可能的卧底，并尽量保证日常活动的正常开展。

经过一段时间后，老大没得到任何新信息。{甲, 乙}、{甲, 丙}、{甲, 丁}、{乙, 丙}、{乙, 丁}、{丙, 丁} 都是可能的卧底组合，这时老大就处于无知识状态。

再经过一段时间，老大知道了甲一定是卧底，那么可能的卧底组合就变成 {甲, 乙}、{甲, 丙}、{甲, 丁} 三种。这样的老大处于部分知识状态。

另一种可能性是，老大知道了甲一定不是卧底，那么可能的卧底组合就变成 {乙, 丙}、{乙, 丁}、{丙, 丁} 三种。这样的老大也处于部分知识状态。

最后，老大完全确定了丙和丁是卧底，这样的卧底组合就只有 {丙, 丁} 一种，这样的老大就处于完全知识状态。

知识传递：假设在某天，老大已经确定了甲是卧底，另外还知道乙、丙、丁中有且只有一个人是卧底。现在老大与乙、丙、丁三个人一一谈话，试图获得更多的知识。在谈话中，乙告诉老板丙是卧底。那么这时候会有两种情况：

(情况 1) 乙不是卧底。这时候由于乙说丙是卧底，而乙、丙、丁三人中最多有一个是卧底，所以丁不是卧底；

(情况 2) 乙是卧底。由于乙、丙、丁三人中最多有一个是卧底，所以丁不是卧底。

在以上的两种情况中，无论乙是不是卧底，都可以判断出丁不是卧底。这样，卧底的组合就由 {甲, 乙}、{甲, 丙}、{甲, 丁} 三种可能的组合缩小为 {甲, 乙}、{甲, 丙} 两种可能的组合，老大通过与乙的谈话获得了知识。

假设在某时候，老大已经知道了甲不是卧底，可能的组合为 {乙, 丙}、{乙, 丁}、{丙, 丁}。现在某个任务，需要一个人做，而且只有在那个人不是卧底的情况下才能做成。这时老大派甲去做。这样在没有完全知识的情况下也把事情办成了。

链路速率分割

链路速率分割可以将多个速率不同的链路转化为多个相同的子流，便于设计具有特殊结构的编码方案。

考虑下面的情形：在有向图$\mathcal{G}=(\mathcal{V},\mathcal{E})$上的链路速率为$\mathbf{f}_{\mathcal{E}}\triangleq(f_e:e\in\mathcal{E})$。子集$\mathcal{E}_1\subseteq\mathcal{E}$满足其上各链路速率之比为有理数。现试图将$\mathcal{E}_1$上各链路速率分割为诸多一致的子流。分割的方法是这样的：选取一个非常小的正数δ，使得$(f_e/\delta:e\in\mathcal{E}_1)$均为整数。这样，就可以将链路$e\in\mathcal{E}_1$上的速率$f_e$分为$f_e/\delta$个速率为$\delta$的子流，而这些子流都是同质的。得到同质的子流后，就可以有其他各种构造手段，例如设计有代数结构的编码等。当$\mathcal{E}_1$上各链路速率之比含有无理数时，需要先从比为有理数的情形出发，然后对各种有理数的情形取极限得到无理数比。

对于经过链路速率分割后得到的一致的子流，常常在其上部署最大距离可分码。在传统分组码的研究中，(n,k) 最大距离可分码是码长为n的分组码，其任意k个元素都能恢复出消息。只要对分组码中每个码元的进制数q不做限制，对任意的n,k，(n,k) 最大距离可分码总存在[14]。将这个结论应用到前面提到的速率分割后的n个子流中，就可以在获得任意k个子流的情况下得到消息。

小正速率链路

在图中的某些链路上，可以分配一个很小的正的链路速率，这个链路速率可以无限接近 0，但是不等于 0。在这个小正速率链路上可以传输那些仅在检出错误的情况下发送的交互信息，进而达到在没有该链路时达不到的效果。

具体而言，一个网络纠错码在平时正常通信的时候可以不需使用那条很小的正速率链路。但是这条很小的正速率链路的存在具有这样的一种功能：若攻击方胆敢引入攻击，网络纠错码的校验环节就会检测到错误的存在。接着，利用这条很小的正速率链路，可以在各节点间发送交互信息（比如花很长的时间将收到的所有信号都传输一遍），进而发现产生错误的节点或链路。值得注意的是，虽然

交互信息可能很大，需要使用的信道次数很多，但是由于信道使用的次数总是有限的，相比与可以无限使用的信道和源源不断的信源，这样的交互占用的信道次数可以忽略不计。所以，这样的小正速率链路可以有效地完成错误的纠正。另外，由于攻击方也注意到了这一点，所以它往往不会发动攻击。所以在正常情况下这样的小正速率链路上并没有传输任何有价值的信息。

1.4.4 单次交互模型及其码字界

为了分析在给定码长情况下网络纠错码的纠错行为，在讨论本文的核心模型前，本文先研究了一个信道单次使用的交互信道模型，展示后续网络纠错码与攻击的设计思想。

如图 1.4，在单次交互模型中，有一个源节点和一个目的节点。这两个节点间可以交互通信共n次（n是正整数），其中第i次通信（$1\le i\le n$）可以传输信息量为c_i（单位：bit）的信号。假设敌对方至多控制其中的z次通信（z是正整数）。在保证能够检出错误或是纠正错误的情况下，本文研究源节点可以给目的节点发送多少信息（单位：bit）。

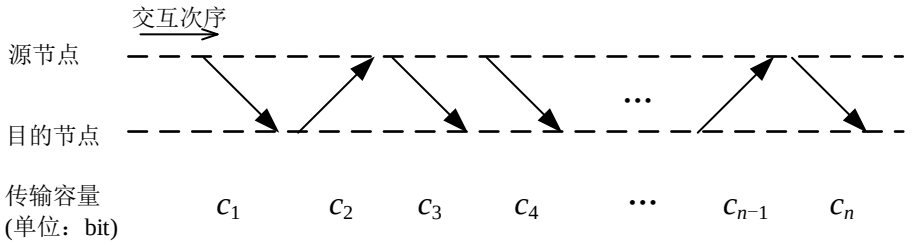


图 1.4　交互信道单次使用模型

<u>对该模型的研究得到的主要结果</u>

(1) 在单次交互模型中，针对要纠正任意z个链路错误的情况，得到了传输信息大小的上界和下界，并讨论了上界和下界的紧性；

(2) 在单次交互模型中，针对要检测任意z个链路错误的情况，得到了传输信息大小的上界和下界，并讨论了上界和下界的紧性。特别的，对于$n=3$的情况网络检错码和网络纠错码的最大码字数的精确表达式，对于$n=4$的网络纠错码也进行了讨论。 □

对这个模型的研究的意义在于，通过研究信道单次使用的情况，为码长为其他正整数（即码长为n）的情况提供思路。具体而言主要包括以下两点：

本部分创新点

(1) 首次从信息论角度（而不是通信复杂度角度）研究了交互式通信的码字界问题，并获得了相关结论；

(2) 讨论了错误发现和错误纠正的关系。不仅研究了需要纠错的码的，还研究了需要发现错误的码。通过分别研究这两种码，更好的了解了错误的发现与纠正过程，为后续纠错容量求解提供理论积累。

(3) 展示了交互式攻击等攻击构造方式和组合知识传递原理等网络纠错码构造方法等思路，验证了这些策略的可行性。

具体内容详见本文第 2 章。本部分相关结果发表在了会议 IEEE Information Theory Workshop① 和会议 IEEE Vehicular Technology Conference② 上。

1.5 研究的具体问题、结论和创新点

本论文的第 3~6 章将具体考虑通信网络。在这些章节中，通信网络将建模成无噪的有向图，求得在给定纠错性能情况下的网络纠错的信道容量域或容许速率域。

本研究将通信网络建模为有向图，并考虑没有噪声、拓扑固定不变的情形。详细的数学模型在第 3 章定义。

1.5.1 单个单播业务的有向网络

本部分考虑在有且只有一个源节点和一个目的节点的情况下敌对方引入的篡改错误。在研究一般的有向图时，本文还特别考虑了两个简单的情形：

(1) 两节点网络：如图 1.5，网络中有且只有一个单播业务，有且只有两个节点，其中一个是源节点v_s，另一个是目的节点v_t。从源节点v_s到目的节点v_t和目的节点v_t到源节点v_s都可能有多条有向链路（也可能没有链路或是只有一条链路）；

① 见在学期间发表的学术论文[1]。
② 见在学期间发表的学术论文[2]。

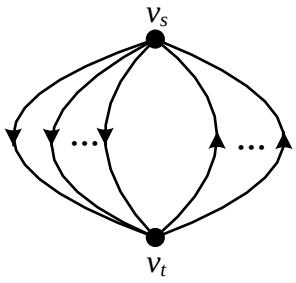


图 1.5　两节点网络：整个网络中只有源节点和目的节点（该图改编自文献[8,55]）

(2) 三节点网络：如图 1.6，网络中有且只有一个单播业务，中有且只有三个节点，分别是源节点v_s、目的节点v_t和中继节点v_r。任意两个节点间都可能有多条有向链路（也可能没有链路或是只有一条链路）。

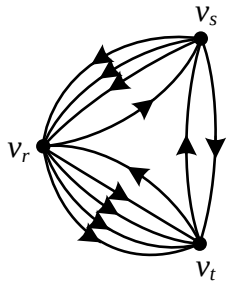


图 1.6　三节点网络：网络中有源节点、目的节点和一个中继节点

一般网络则是可能有很多节点的情况，任意两个节点间都可能有多条链路。

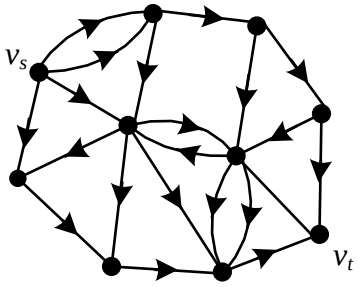


图 1.7　一般网络：网络中有很多节点

本部分主要结果

(1) 两节点网络点对点通信的容许速率域求解：针对在两节点网络，对任意的攻击错误求得了容许速率域，并给出了达到容许速率域内部的链路速率的信源编码方案。

(2) 三节点网络点对点网络纠错容量求解：针对在三节点网络，在至多有 z 条链路错误的限制下，得到了信道容量的上界和下界，给出了实现下界的信道编码方案，并说明在大多数情况下上界等于下界。

(3) 蟑螂网络容许速率域求解：针对蟑螂网络，求出了在任一链路错误情况下的容许速率域。

(4) 一般网络容许速率域求解：针对在一般有向网络中有且只有一个单播业务的情况，得到了容许速率域的外界，并给出该外界在某种结构下紧的证明。

本部分创新点

(1) 首次提出了网络纠错信源编码的概念，并对其容许速率域进行了研究；

(2) 通过研究三节点网络的网络纠错码，探究了中继节点在网络纠错中的作用；

(3) 将新的攻击方案构造方案和新的网络纠错方案应用到信道容量域和容许速率域的求解中，验证了思路的可行性，获得了新结果。

具体内容详见本文第 4 章。本部分相关结果发表在期刊 IEEE Transactions on Communications[①] 和期刊 Tsinghua Science and Technology[②] 上。

1.5.2 多址接入网络

本部分考虑多址接入直连网络上的分布式分层分集。如图 1.8，有 K 个单播业务，每个业务都有自己的源节点 v_{sk}（$1 \le k \le K$），它们都有共同的目的节点。这样的多个单播业务是单个单播业务的一种推广。

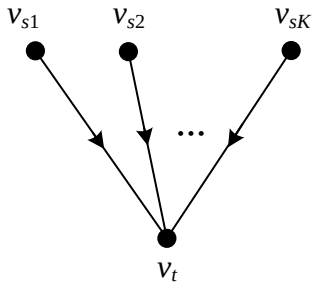


图 1.8　多址接入直连网络

① 见在学期间发表的学术论文[3]。
② 见在学期间发表的学术论文[4]。

本部分主要结果

考虑在多址接入网络中，接入链路可能被敌方攻击的情况下，尽可能多的支持信源传输的情形。具体而言，针对分布式分层分集模型，求得了容许速率域，并设计了相应的信源编码。

本部分创新点

(1) 考虑了在多址接入直连网络中分布式分层分集模型，完全求解了该模型的容许容量域，给出了达到容许速率域的编码。

(2) 将信息支配和熵不等式技术结合，更好的了解了熵不等式之间的关系。

具体内容详见本文第 5 章。本部分相关结果发表在期刊 IEEE Transactions on Information Theory[①] 上。

1.5.3 一般的多业务有向网络

本部分考虑一般的多业务网络，其中的业务可能是单播业务，也可能是组播业务。在这种情况下，假设敌方可以同时引入延时和篡改，考察敌方控制的网络资源对信号进行延时的情况。

本部分主要结果

(1) 信道容量域：证明了对于一般的有向网络，在已有篡改等错误的基础上，再引入有界的延时不会改变信道容量域的大小。并给出了相应的网络纠错码构造方案；

(2) 容许速率域：证明了对于一般的有向网络，在已有篡改等错误的基础上，再引入有界的延时不会改变容许速率域的大小。并给出了相应的网络纠错码构造方案。

其中，有限延时指的是延时的长度有上界。例如，敌方将某信号进行的延时都不超过时间长度T，则该延时是有限延时。再例如，敌方将时刻t的信号$X(t)$（$0\le t<+\infty$）延时t，变成信号$X(t/2)$，则该延时是无限延时（因为延时t可以无限大）。

本部分的创新点

证明了有限延时对网络纠错系统信道容量域和容许速率域没有影响。

① 见在学期间发表的学术论文[5]。

具体内容详见本文第 6 章。本部分相关结果发表在期刊 IEEE Communications Letters[①] 上。

1.5.4 主要结果与创新点小结

前面几个小节提到的主要结果和创新点可以归纳整理如下。

本研究的结论

本研究更精确地刻画了网络纠错信道容量域和容许速率域的更精确刻画，更好地分析了通信系统中攻击方的存在会给系统带来什么样的影响，了解了网络纠错的极限性能。

本研究的创新点（按类型分类）

(1) 问题创新。本论文研究了网络纠错码的容许速率域问题，还考虑了延时带来的影响。这些问题是其他研究都没有涉及的问题；

(2) 求解思路创新。在外界求取的过程中，采用了新的攻击构造策略，比如基于信息支配的构造、熵不等式的运用等。在内界求取的过程中，采用了新的网络纠错码构造方法，例如基于组合知识传递的策略、因果化处理等。其构造策略与之前的研究有根本不同。

(3) 结果创新。在信道容量域和容许速率域方面，得到了新的内界和外界。求解出了新的网络的信道容量域和容许速率域。使人们对攻击错误对系统性能的影响有了更好的了解。

1.6 本文组织结构

第 1 章对研究背景和全文内容进行了全面的介绍，涵盖了本论文研究的各场景、模型、结论和创新点。

第 2 章针对该研究的基本思路，在一个比较简单的模型：单次交互模型上兑现该思路，说明如何利用该思路构造攻击方案和网络纠错方案。

第 3 章对本文考虑的有向图上的网络纠错模型进行严格的数学定义。这章只介绍模型，而没有求解。模型的求解在第 4 章、第 5 章和第 6 章。

第 4 章使用第 3 章描述的模型，求解单发单收情形下的信道容量域和容许速率域；

第 5 章使用第 3 章描述的模型，求解多发单收情形下的容许速率域；

① 见在学期间发表的学术论文[6]。

第 6 章使用第 3 章描述的模型，考虑多发多收情形下延时对信道容量域和容许速率域的影响；

第 7 章简要回顾了全文内容，并介绍了可能的遗留问题。

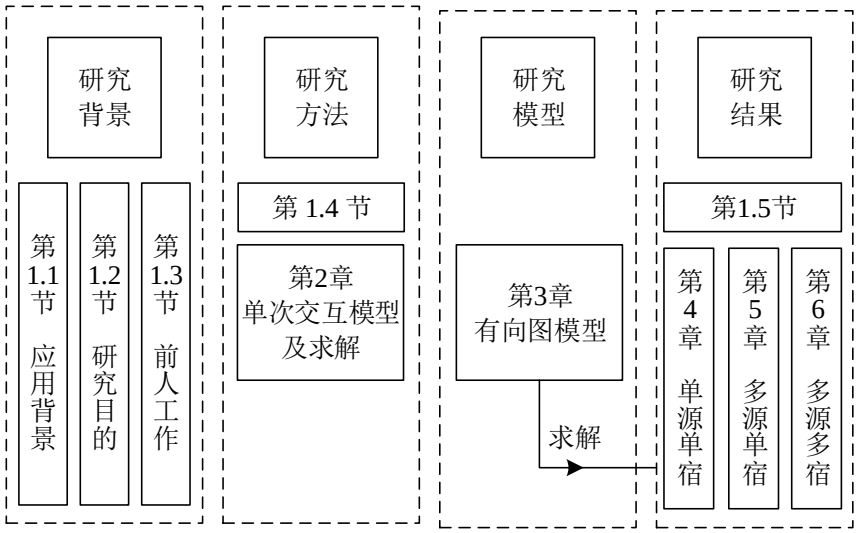


图 1.9　论文结构框图

第 2 章　单次交互模型及其求解

内容提要

本章将讨论两个节点间传输，且信道单次使用的情况。通过对该模型的研究，我们将更好地了解网络纠错码的构造与攻击构造的基本方法和基本思路，为后续的研究奠定基础。

● 2.1 节介绍前人有关两节点间交互式通信的工作。

● 2.2 节介绍单次交互模型，定义单次交互模型上的检错码和纠错码，定义最大码字数问题。

● 2.3 节讨论单次交互模型及其上码的性质，这些性质在 2.4 节、2.5 节和 2.6 节的推导过程会用到。

● 2.4 节讨论传输个数 $n=3$ 的情况，求得了这时检错码和纠错码的最大码字数。

● 2.5 节讨论传输个数 $n=4$ 的情况。

● 2.6 节讨论传输个数 n 为一般正整数的情况。

本章部分内容改编自在学期间发表的学术论文[1,2]。文章的共同作者参与了相关的讨论和研究。

2.1 本章引言

交互是网络纠错的最本质手段之一。只有通过节点间的交互，才能利用链路上承载的知识发现和纠正错误。

对交互极限性能的研究可以追溯到两个节点间通信复杂度和树码的研究，包括无噪声的情况[75]、统计噪声的情况[76]和恶意错误的情况[77]。文献[76,77]首次考虑了纠错的交互式编码。这类文献中主要考虑设计能把没有纠错能力的交互式编码转化为有纠错能力的交互式编码的模拟器。这些工作证明，当每次传输的方向是可以设计时，为了对抗恒定比例的错误，对于通信复杂度的开销是恒定的。除了文献[76,77]以外，后续工作还包括高效地树码构造[78,79]、提升能抵抗的错误率[80–82]等。这些工作都假设在同质的双向传输中，有一小部分恒定比例的双向传输会发生错误，然后构造最少传输次数（即通信复杂度）的交互式编码。

与前文的着力点不同，本章将从码字界的角度来分析交互纠错的极限性能。

码字界问题最初是计算在分组码中满足距离关系的码本的最大大小。对于码长为n，任意两个码字距离$\geq d$，每个码元进制为q的情形，码本的最大大小可记为$A_q(n,d)$。尽管在某些参数下有一些闭式解（如$A_q(n,n)=q$和$A_q(n,1)=q^n$），但是对于任意的n，d，q并没有一般的显示表达式（而且这事实上是一个困难问题）。目前只得到了一些上界和下界。其中上界包括：

(1) 显式表达式界。如 Hamming 界[83]、Singleton 界[12]、Elias-Bassalygo 界[84]等；

(2) 递归界。如 Johnson 界[85,86]、Zinoview-Litsyn-Laihonen 界[87]等；

(3) 优化界。如线性规划界[88]、Schirijver 半定规划界[89–91]等。

另外，在参数有其他限制的条件下还有其他结果，如在$d/n>1-1/q$时适用的 Plotkin 界[92]。Brouwer 表[93]对在$q=2,3,4,5$的情况进行了总结。

在这种普通码字界的基础上，后来有发展出了混合码码字界。混合码是各码元进制数允许不同的码。关于混合码字界的文献包括：

(1) 完备混合码。除了覆盖半径为 0 和n的平凡混合码外，文献[94–96]还构造了其他完备混合码；

(2) 二三进制混合码。文献[97–99]考虑了码元是二进制或三进制的混合码。

本章讨论的交互式纠错码与前述码字界问题有着明显的区别。之前的普通码字界研究和混合码字界研究是在没有交互的情况下完成的。没有交互时，码本就完全表征了码的性能。在引入交互后，码本不足以完全表示码的情况。其根本原因在于，码本只说明在正确传输时编码器的行为，而没有规定在错误传输时码的行为。如果编码器在收到异常输入后能做出明智的反映，有机会得到更大的错误对抗能力。

本章的研究结果主要针对单次交互模型上检错码和纠错码的最大码字数进行刻画。本章将从最简单的三次传输交互模型入手，然后研究四次传输交互模型，最后研究一般的有限次传输交互模型，求得检错码和纠错码的最大码字数的上界和下界，通过刻画最大码字数以研究错误对单次交互模型上检错码和纠错码的极限性能。

2.2 单次交互模型

符号定义

$\mathbb{N}$是自然数集合，$\mathbb{Z}$是整数集合，$\mathbb{R}$是实数集合。对于两个数$i_1,i_2\in\mathbb{R}$，定义整数区间$[i_1:i_2]\triangleq\{i\in\mathbb{Z}:i_1\leq i\leq i_2\}$，$(i_1:i_2]\triangleq\{i\in\mathbb{Z}:i_1<i\leq i_2\}$，$[i_1:i_2)\triangleq\{i\in\mathbb{Z}:i_1\leq i<i_2\}$（以上区间均只含有整数；当$i_1>i_2$时区间均为空）。

单次交互模型

单次交互模型如图 2.1：源节点要通过 n 次消息传输，向目的节点发送消息。在这 n 次传输中，有些传输是从源节点到目的节点的，有些传输是从目的节点到源节点的。对于任意的 $i\in[1:n]$，第 i 次传输（$i\in[1:n]$）的传输方向为

$$s_i \triangleq \begin{cases} +1, & \text{传输从源节点到目的节点} \\ -1, & \text{传输从目的节点到源节点,} \end{cases} \tag{2–1}$$

并且可以传输给定集合 $\mathcal{Q}_i \triangleq [0:q_i)$ 中的一个信号，其中 $q_i=|\mathcal{Q}_i|$ 是第 i 次传输信号集的大小。传输次数 n、各次传输的方向 $s^n \triangleq (s_i:i\in[1:n])$ 和信号集大小 $q^n \triangleq (q_i:i\in[1:n])$ 都是事先确定的。

值得一提的是，q_i 完全表示了每次传输可以传递信息量。即，第 i 次传输可传递信息 $\log q_i$ bit。

这样的一个交互模型记为 $s^n\circ q^n$。

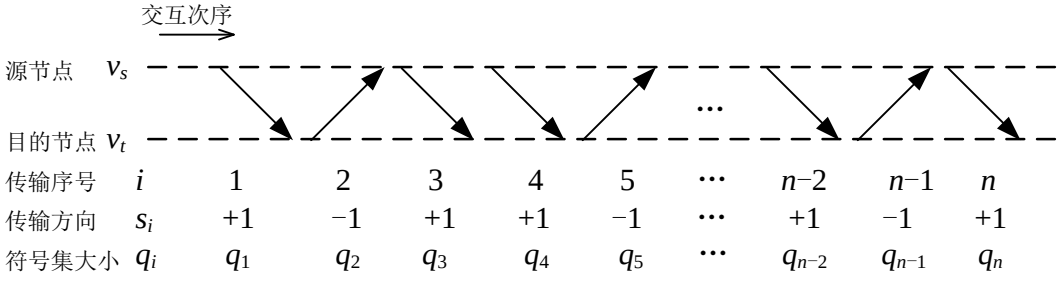


图 2.1　单次交互模型示意

记源节点想要发送的消息为 M。记第 i 次传输时源节点发送的信号为 X_i，目的节点接收的信号为 Y_i。

对于区间 $I\subseteq[1:n]$、信号序列 $\{X_i:i\in[1:n]\}$ 和整数 $i_1,i_2\in[1:n]$，记 $I_+\triangleq\{i\in I:s_i=+1\}$，$I_-\triangleq\{i\in I:s_i=-1\}$，$X_I\triangleq\{X_i:i\in I\}$，$X^{i_1}\triangleq X_{[1:i_1]}$，$X_+^{i_1}\triangleq\{X_i:i\in[1:i_1],s_i=+1\}$，$X_-^{i_1}\triangleq\{X_i:i\in[1:i_1],s_i=-1\}$。

对于区间 I 上的两个序列 X_I 和 Y_I，定义其 Hamming 距离为

$$d_H(X_I,Y_I)\triangleq\big|\{i\in I:X_i\neq Y_i\}\big|. \tag{2–2}$$

当敌对方能够控制任意 z 次（$z\in\mathbb{N}$）传输时，有

$$d_H(X^n,Y^n)\le z. \tag{2–3}$$

网络纠错码

一个在 $s^n \circ q^n$ 上的交互式网络纠错码 $\mathsf{C} \triangleq \left(\mathcal{M}, \mathrm{Enc}^n, \mathrm{Dec}\right)$（见图 2.2，本章以后简称码）由以下三部分定义：

(1) 消息集为 $\mathcal{M}$；

(2) n 个编码器 $\mathrm{Enc}^n \triangleq \left(\mathrm{Enc}_i : i \in [1:n]\right)$；

(3) 1 个译码器 Dec。

这里的编码器和译码器都是确定性的（即输出由输入唯一确定）。

源节点知道消息 $M \in \mathcal{M}$，包括编码器 Enc_+^n，其中

$$\begin{aligned} \mathrm{Enc}_i : \mathcal{M} \times \prod_{j \in [1:i]_-} \mathcal{Q}_j &\to \mathcal{Q}_i \\ M \times \quad Y_-^i \quad &\mapsto X_i. \end{aligned}$$

目的节点包括编码器 Enc_-^n 和译码器 Dec，其中

$$\begin{aligned} \mathrm{Enc}_i : \prod_{j \in [1:i]_+} \mathcal{Q}_j &\to \quad \mathcal{Q}_i \\ Y_+^i \quad &\mapsto \quad X_i \\ \mathrm{Dec} : \prod_{j \in [1:n]_+} \mathcal{Q}_j &\to \mathcal{M} \cup \{\varepsilon\} \\ Y_+^n \quad &\mapsto \quad \hat{M}. \end{aligned}$$

在本章中，$\varepsilon \notin \mathcal{M}$ 表示错误指示符号，当译码结果为 ε 时表示发现了错误。

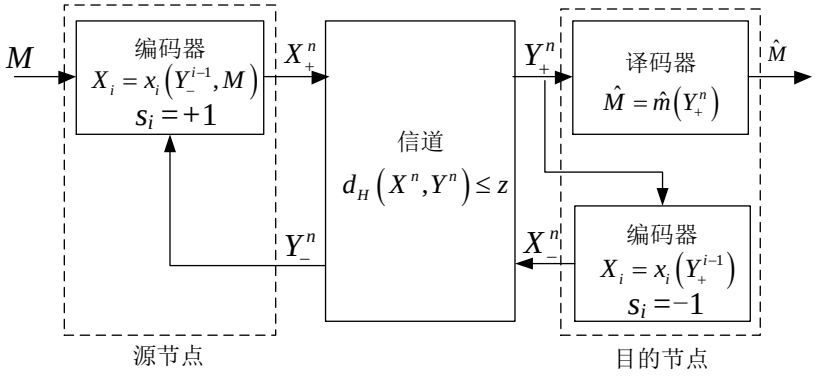


图 2.2　交互式网络纠错码示意图

网络纠错码的检错纠错能力

定义 2.1（纠 z 个错）：C 是 $s^n \circ q^n$ 上的码。如果当 $d_H\left(X^n, Y^n\right) \le z$ 时有 $\hat{M} = M$，则称码 C 能纠 z 个错。 □

定义 2.2（检 z 个错）：C 是 $s^n \circ q^n$ 上的码。如果

(1) 当 $d_H\left(X^n,Y^n\right)\le z$ 时有 $\hat{M}=M$ 或 $\hat{M}=\varepsilon$，且

(2) 当 $X^n=Y^n$ 时有 $\hat{M}=M$，

则称码C能检 z 个错。 □

假设敌对方能够知道消息 M，也能知道网络纠错码。这样的敌对方事实上知道系统中的全部信息。这样的假设保证了通信方不能通过隐藏信息来获得安全，也是一种对通信方比较保守的估计，同时也是对敌对方能力的一种简单假设。

记基于这 n 次传输的所有能够纠 z 个错的网络纠错码的消息集大小的最大值为 $A^{(z,z)}_{s^n\circ q^n}$；记基于这 n 次传输的所有能够检 z 个错的网络纠错码的消息集大小的最大值为 $A^{(z,0)}_{s^n\circ q^n}$。

对该模型研究主要集中在对码字界的研究，即在所有能纠 z 个错或是能检 z 个错的情况下，消息集大小的最大值（即 $A^{(z,z)}_{s^n\circ q^n}$ 和 $A^{(z,0)}_{s^n\circ q^n}$）是多少。在解决这个问题的过程中同时会得到以下问题的解答：

(1) 对于消息集大小小等于最大值时，通信方如何构造网络纠错码对抗错误；

(2) 对于消息集大小大于最大值的网络纠错码，敌对方如何进行攻击使得通信不能可靠进行。

2.3 准备工作

本节介绍在后续小节的推导过程中需要用到的一些概念和结论。

性质 2.1（平凡的情形）：(1) $1\le A^{(z,z)}_{s^n\circ q^n}\le A^{(z,0)}_{s^n\circ q^n}\le \prod_{i\in[1:n]_+} q_i$，　（2–4）

(2) $$A^{(0,0)}_{s^n\circ q^n}=\prod_{i\in[1:n]_+} q_i,\qquad (2\text{–}5)$$

(3) 对于任意 $q'\ge+2$，有

$$A^{(z,0)}_{s^n\circ q^n}=A^{(z,0)}_{\left(-q',s^n\circ q^n\right)}=A^{(z,0)}_{\left(s^n\circ q^n,-q'\right)}$$

$$A^{(z,z)}_{s^n\circ q^n}=A^{(z,z)}_{\left(-q',s^n\circ q^n\right)}=A^{(z,z)}_{\left(s^n\circ q^n,-q'\right)}.$$ □

证明：由于结论比较明显，这里仅提供证明大意。

(1) 由于在$[1:n]_+$上信号的取值一共只有$\prod_{i\in[1:n]_+} q_i$种，所以$A^{(z,z)}_{s^n\circ q^n}$和$A^{(z,0)}_{s^n\circ q^n}$均$\le \prod_{i\in[1:n]_+} q_i$。另外消息集大小为 1 时总能使$\hat{M}=M$，所以$A^{(z,z)}_{s^n\circ q^n}$和$A^{(z,0)}_{s^n\circ q^n}$均$\ge 1$。另外，由于能纠$z$错码都是检$z$错码，所以$A^{(z,z)}_{s^n\circ q^n}\le A^{(z,0)}_{s^n\circ q^n}$。

(2) 由于 (1) 有$A^{(0,0)}_{s^n\circ q^n}\le \prod_{i\in[1:n]_+} q_i$。而将消息直接编码可以构造出消息集大小为$\prod_{i\in[1:n]_+} q_i$的码。所以得证。

(3) 在首次从源节点到目的节点的传输之前的传输，目的节点不持有任何有效信息，所以那些传输不会起到实质作用。对于最后一次从源节点到目的节点的传输之后的传输，不参与译码过程，也没有实质作用。 □

2.3.1 与上界证明有关的性质

首先来定义码字。一个码的码字就是在没有错误的情况下传输的信号。对于给定的码，每个消息对应一个码字。

定义 2.3（码字）：C 是$s^n\circ q^n$上的码。$m\in\mathcal{M}$，$c^n\in\prod_{i=1}^{n}\mathcal{Q}_i$。若当$M=m$且$X^n=Y^n$时有$X^n=c^n$，则称$c^n$为消息$m$的码字。记$\mathrm{CW}_i(m)\triangleq c_i$（$i\in[1:n]$）。 □

根据码字的定义，码字有以下性质：

性质 2.2（码字的性质）：C 是$s^n\circ q^n$上的码。$m\in\mathcal{M}$。则

$$\begin{aligned}\mathrm{Enc}_i\left(m,\mathrm{CW}_-^i(m)\right)&=\mathrm{CW}_i(m),\quad i\in[1:n]_+\\ \mathrm{Enc}_i\left(\mathrm{CW}_+^i(m)\right)&=\mathrm{CW}_i(m),\quad i\in[1:n]_-\\ \mathrm{Dec}\left(\mathrm{CW}_+^n(m)\right)&=m.\end{aligned}$$

□

性质 2.2 通过对码字这一概念，对编码器和译码器的行为进行了约束。

接下来我们来考虑和译码器有关的一些引理。

引理 2.1（检z错码译码器输入不同）：C 是$s^n\circ q^n$上能检z个错的码。$m,\bar{m}\in\mathcal{M}$（$m\ne\bar{m}$）是两个不同的消息。$y^n\in\prod_{i=1}^{n}\mathcal{Q}_i$是在传输消息$M=m$时$Y^n$的

取值，且满足 $d_H\left(X^n,Y^n\right)\le z$；$\bar{y}^n\in\prod_{i=1}^{n}\mathcal{Q}_i$ 是在传输消息 $M=\bar{m}$ 时 Y^n 的取值，且满足 $\bar{y}^n=\bar{x}^n$。则 $y_+^n\neq\bar{y}_+^n$。 □

证明：用反证法。反设存在两个不同的消息 $m,\bar{m}\in\mathcal{M}$，存在 $y^n,\bar{y}^n\in\prod_{i=1}^{n}\mathcal{Q}_i$ 使得 $d_H\left(x^n,y^n\right)\le z$ 且 $\bar{y}^n=\bar{x}^n$，并且有 $y_+^n=\bar{y}_+^n$。考虑以下两种情况：

(情况 1) $M=m$，$X^n=x^n$，$Y^n=y^n$。这时有 $d_H\left(X^n,Y^n\right)\le z$。因为码 C 能检 z 个错，由检错码的定义（定义 2.2(1)）有 $\hat{M}=m$ 或 $\hat{M}=\varepsilon$。因为 $\bar{m}\in\mathcal{M}$，$\varepsilon\notin\mathcal{M}$ 且 $m\neq\bar{m}$，所以 $\mathrm{Dec}\left(y_+^n\right)\neq\bar{m}$。

(情况 2) $M=\bar{m}$，$X^n=\bar{x}^n$，$Y^n=\bar{y}^n$。这时有 $Y^n=X^n$。因为码 C 能检 z 个错，由检错码的定义（定义 2.2(2)）有 $\hat{M}=\bar{m}$。所以 $\mathrm{Dec}\left(y_+^n\right)=\bar{m}$。

这两种情况，一种要求译码器满足 $\mathrm{Dec}\left(y_+^n\right)\neq\bar{m}$，另一种要求译码器满足 $\mathrm{Dec}\left(y_+^n\right)=\bar{m}$。译码器不可能同时满足这两个要求，矛盾。所以命题得证。 □

引理 2.2（纠 z 错码译码器输入不同）：C 是 $s^n\circ q^n$ 上能纠 z 个错的码。

$m,\bar{m}\in\mathcal{M}$（$m\neq\bar{m}$）是两个不同的消息。$y^n\in\prod_{i=1}^{n}\mathcal{Q}_i$ 是在传输消息 $M=m$ 时 Y^n 的取值，且满足 $d_H\left(X^n,Y^n\right)\le z$；$\bar{y}^n\in\prod_{i=1}^{n}\mathcal{Q}_i$ 是在传输消息 $M=\bar{m}$ 时 Y^n 的取值，且满足 $d_H\left(\bar{x}^n,\bar{y}^n\right)\le z$。则 $y_+^n\neq\bar{y}_+^n$。 □

证明：用反证法。反设存在两个不同的消息 $m,\bar{m}\in\mathcal{M}$，存在 $y^n,\bar{y}^n\in\prod_{i=1}^{n}\mathcal{Q}_i$ 使得 $d_H\left(x^n,y^n\right)\le z$ 且 $d_H\left(\bar{x}^n,\bar{y}^n\right)\le z$，并且有 $y_+^n=\bar{y}_+^n$。考虑以下两种情况：

(情况 1) $M=m$，$X^n=x^n$，$Y^n=y^n$。这时有 $d_H\left(X^n,Y^n\right)\le z$。因为码 C 能纠 z 个错，由纠错码的定义有 $\hat{M}=m$。因为 $m\neq\bar{m}$，所以 $\mathrm{Dec}\left(y_+^n\right)\neq\bar{m}$。

(情况 2) $M=\bar{m}$，$X^n=\bar{x}^n$，$Y^n=\bar{y}^n$。这时有 $d_H\left(X^n,Y^n\right)\le z$。因为码 C 能纠 z 个错，由纠错码的定义有 $\hat{M}=\bar{m}$。所以 $\mathrm{Dec}\left(y_+^n\right)=\bar{m}$。

这两种情况，一种要求译码器满足 $\mathrm{Dec}\left(y_+^n\right)\neq\bar{m}$，另一种要求译码器满足 $\mathrm{Dec}\left(y_+^n\right)=\bar{m}$。译码器不可能同时满足这两个要求，矛盾。所以命题得证。 □

接下来利用与证明引理 2.1 和引理 2.2 类似的思路，得到检错码和纠错码的码字需要满足的一些条件。

引理 2.3（检 z 错）：C 是 $s^n \circ q^n$ 上能检 z 个错的码。$m,\bar{m} \in \mathcal{M}$ 是两个不同的消息。$c^n \triangleq \mathrm{CW}^n(m)$，$\bar{c}^n \triangleq \mathrm{CW}^n(\bar{m})$。则不存在整数 $n' \in [0:n]$ 使得

$$d_H\left(c^{n'}, \bar{c}^{n'}\right) + \left|(n':n]_+\right| \le z . \qquad \square$$

证明：用反证法。假设存在 $n' \in [0:n]$ 满足条件。

定义 $I_{a+} \triangleq \left\{i \in [1:n']_+ : c_i \ne \bar{c}_i\right\}$，$I_{a-} \triangleq \left\{i \in [1:n']_- : c_i \ne \bar{c}_i\right\}$。由于 $d_H\left(c^{n'}, \bar{c}^{n'}\right) = \left|I_{a+}\right| + \left|I_{a-}\right|$，所以

$$\left|I_{a+}\right| + \left|I_{a-}\right| + \left|(n':n]_+\right| \le z . \qquad (2\text{–}6)$$

考虑以下两种情况：

(情况 1) $M = m$，且 $Y_{I_{a+}} = \bar{c}_{I_{a+}}$，$Y_{I_{a-}} = c_{I_{a-}}$，$Y_{(n',n]_+} = \bar{c}_{(n',n]_+}$，$Y_{[1:n']\setminus(I_{a+}\cup I_{a-})} = X_{[1:n']\setminus(I_{a+}\cup I_{a-})}$。这时显然有 $d_H\left(X^n, Y^n\right) \le z$。利用性质 2.2 可以得到译码器的输入为 $\bar{c}_-^n$。由于码 C 能检 z 个错，所以 $\mathrm{Dec}\left(\bar{c}_+^n\right) = m$ 或 $\mathrm{Dec}\left(\bar{c}_+^n\right) = \varepsilon$。因为 $\bar{m} \in \mathcal{M}$，$\varepsilon \notin \mathcal{M}$ 且 $m \ne \bar{m}$，所以 $\mathrm{Dec}\left(\bar{c}_+^n\right) \ne \bar{m}$。

(情况 2) $M = \bar{m}$，且 $Y^n = X^n$。因为 $\bar{c}^n = \mathrm{CW}^n(\bar{m})$，所以译码器的输入为 $\bar{c}_+^n$。由于码 C 能检 z 个错，所以 $\mathrm{Dec}\left(\bar{c}_-^n\right) = \bar{m}$。

以上两种情况，一种要求译码器满足 $\mathrm{Dec}\left(\bar{c}_+^n\right) \ne \bar{m}$，另一种要求译码器满足 $\mathrm{Dec}\left(\bar{c}_-^n\right) = \bar{m}$。译码器不可能同时满足这两个要求，矛盾。命题得证。 $\square$

引理 2.4（纠 z 错）：C 是 $s^n \circ q^n$ 上能纠 z 个错的码。$m,\bar{m} \in \mathcal{M}$ 是两个不同的消息。$c^n \triangleq \mathrm{CW}^n(m)$，$\bar{c}^n \triangleq \mathrm{CW}^n(\bar{m})$。则不存在整数 $n' \in [0:n]$ 和 $n'' \in [0:n']$ 使得

$$\left|I_a\right| \le z \qquad (2\text{–}7)$$

$$\left|\bar{I}_a\right| \le z \qquad (2\text{–}8)$$

$$\left|I_a\right| + \left|\bar{I}_a\right| + \left|(n':n]_+\right| \le 2z , \qquad (2\text{–}9)$$

其中

$$I_a \triangleq \left\{i \in [1:n''] : c_i \ne \bar{c}_i\right\} \cup (n'':n']_-$$

$$\bar{I}_a \triangleq \left\{i \in (n'':n'] : c_i \ne \bar{c}_i\right\} \cup (n'':n']_- . \qquad \square$$

证明：用反证法。反设存在整数 $n' \in [0:n]$ 和 $n'' \in [0:n']$ 满足条件。

定义 $I_{a+} \triangleq \left\{i \in [1:n'']_+ : c_i \ne \bar{c}_i\right\}$，$I_{a-} \triangleq \left\{i \in [1:n'']_- : c_i \ne \bar{c}_i\right\} \cup (n'':n]_-$，$\bar{I}_{a+} \triangleq \left\{i \in (n'':n]_+ : c_i \ne \bar{c}_i\right\}$，$\bar{I}_{a-} \triangleq (n'':n]_-$。显然有

$$\left|I_a\right| = \left|I_{a+}\right| + \left|I_{a-}\right|$$

$$\left|\bar{I}_a\right| = \left|\bar{I}_{a+}\right| + \left|\bar{I}_{a-}\right| .$$

易知存在 $n_p \in (n':n]$ 使得

$$|I_{a+}|+|I_{a-}|+\left|(n':n_p]_+\right| \le z$$
$$|\bar{I}_{a+}|+|\bar{I}_{a-}|+\left|(n_p:n]_+\right| \le z.$$

考虑以下两种情况：

(情况 1) $M=m$，$Y_{I_{a+}}=\bar{c}_{I_{a+}}$，$Y_{I_{a-}}=c_{I_{a-}}$，$Y_{(n':n_p]_+}=\bar{y}_{(n':n_p]_+}$（$\bar{y}_{(n':n_p]_+}$ 的值由下文定义），对于其他 i 有 $Y_i=X_i$。显然这时 $d\left(X^n,Y^n\right)\le z$。

记目的节点在 $(n_p:n]_+$ 收到的符号为 $y_{(n_p:n]_+}$。这时，考虑到 I_{a+} 和 $\bar{I}_{a+}$ 的定义，可以知道译码器在 $[1:n'']_+$、$(n'':n']_+$、$(n':n_p]_+$ 和 $(n_p:n]_+$ 的输入分别为 $\bar{c}_+^{n''}$，$c_{(n'':n']_+}$，$\bar{y}_{(n':n_p]_+}$ 和 $y_{(n_p:n]_+}$。由于码 C 能纠 z 个错，所以 $\mathrm{Dec}\left(\bar{c}_+^{n''},c_{(n'':n']_+},\bar{y}_{(n':n_p]_+},y_{(n_p:n]_+}\right)=m$。

(情况 2) $M=\bar{m}$，$Y_{\bar{I}_{a+}}=c_{\bar{I}_{a+}}$，$Y_{\bar{I}_{a-}}=\bar{c}_{\bar{I}_{a-}}$，$Y_{(n_p:n]_+}=y_{(n_p:n]_+}$，对于其他的 i 有 $Y_i=X_i$。显然这时 $d\left(X^n,Y^n\right)\le z$。

记目的节点在 $(n_p:n]_+$ 收到的符号为 $\bar{y}_{(n_p:n]_+}$。这时，考虑到 I_{a+} 和 $\bar{I}_{a+}$ 的定义，可以知道译码器在 $[1:n'']_+$、$(n'':n']_+$、$(n':n_p]_+$ 和 $(n_p:n]_+$ 的输入分别为 $\bar{c}_+^{n''}$，$c_{(n'':n']_+}$，$\bar{y}_{(n':n_p]_+}$ 和 $y_{(n_p:n]_+}$。由于码 C 能纠 z 个错，所以 $\mathrm{Dec}\left(\bar{c}_+^{n''},c_{(n'':n']_+},\bar{y}_{(n':n_p]_+},y_{(n_p:n]_+}\right)=\bar{m}$。

这两种情况一种要求 $\mathrm{Dec}\left(\bar{c}_+^{n''},c_{(n'':n']_+},\bar{y}_{(n':n_p]_+},y_{(n_p:n]_+}\right)=m$，另一种要求 $\mathrm{Dec}\left(\bar{c}_+^{n''},c_{(n'':n']_+},\bar{y}_{(n':n_p]_+},y_{(n_p:n]_+}\right)=\bar{m}$。由于 $m\ne\bar{m}$，矛盾。命题得证。 □

引理 2.5（纠 z 错）：C 是 $s^n\circ q^n$ 上能纠 z 个错的码。$m,\bar{m}\in\mathcal{M}$ 是两个不同的消息。$c^n\triangleq\mathrm{CW}^n(m)$，$\bar{c}^n\triangleq\mathrm{CW}^n(\bar{m})$。则不存在整数 $n'\in[0:n]$ 使得

$$d_H\left(c^{n'},\bar{c}^{n'}\right)\le z$$

$$d_H\left(c^{n'},\bar{c}^{n'}\right)+\left|(n':n]_+\right|\le 2z\,.$$ □

证明： 在引理 2.4 中取 $n''=n'$（此时有 $I_a=[1:n']$ 和 $\bar{I}_a=\varnothing$）即可得证。 □

引理 2.6（检错上界）：考虑 $s^n \circ q^n$ 和 $z \in \mathbb{N}$。令

$$n'_{\min} \triangleq \min\left\{n' \in [0:n] : \left|(n':n]_+\right| \le z\right\}. \tag{2–10}$$

则

$$A^{(z,0)}_{s^n \circ q^n} \le \prod_{i \in [1:n'_{\min}]_+} q_i . \qquad \square$$

证明：用反证法。假设在 $s^n \circ q^n$ 上存在检 z 错的码 C，其消息集大小大于 $\prod_{i \in [1:n'_{\min}]_+} q_i$。根据抽屉原理，$\exists m, \bar{m} \in \mathcal{M}$（$m \ne \bar{m}$）使得 $\mathrm{CW}^{n'_{\min}}_+(m) = \mathrm{CW}^{n'_{\min}}_+(\bar{m})$。令 $c^n \triangleq \mathrm{CW}^n(m)$，$\bar{c}^n \triangleq \mathrm{CW}^n(\bar{m})$。因为 $c^{n'_{\min}}_+ = \bar{c}^{n'_{\min}}_+$，所以 $\mathrm{Enc}^{n'_{\min}}_-$ 的输入都是一样的，所以进而有 $c^{n'_{\min}} = \bar{c}^{n'_{\min}}$。这样存在整数 $n' = n'_{\min}$ 使得

$$d_H\left(c^{n'}, \bar{c}^{n'}\right) + \left|(n':n]_+\right| \le z .$$

与引理 2.3 矛盾。这样我们就证明了所有的检 z 个错的码的大小都 $\le \prod_{i \in [1:n'_{\min}]_+} q_i$。 $\square$

引理 2.7（检错不能）：考虑 $s^n \circ q^n$ 和 $z \in \mathbb{N}$。若 $\left|[1:n]_+\right| \le z$，则 $A^{(z,0)}_{s^n \circ q^n} = 1$。 $\square$

证明：$\left|[1:n]_+\right| \le z$，所以引理 2.6 中 $n'_{\min} = 0$。所以 $[1:n'_{\min}]_+ = \varnothing$，$A^{(z,0)}_{s^n \circ q^n} \le 1$。 $\square$

引理 2.8（纠错上界）：考虑 $s^n \circ q^n$ 和 $z \in \mathbb{N}$。令

$$n'_{\min} \triangleq \min\left\{n' \in [0:n] : \left|(n':n]_+\right| \le 2z\right\}. \tag{2–11}$$

则

$$A^{(z,z)}_{s^n \circ q^n} \le \prod_{i \in [1:n'_{\min}]_+} q_i . \qquad \square$$

证明：用反证法。假设在 $s^n \circ q^n$ 上存在检 z 错的码 C，其消息集大小大于 $\prod_{i \in [1:n'_{\min}]_+} q_i$。根据抽屉原理，$\exists m, \bar{m} \in \mathcal{M}$（$m \ne \bar{m}$）使得 $\mathrm{CW}^{n'_{\min}}_+(m) = \mathrm{CW}^{n'_{\min}}_+(\bar{m})$。令 $c^n \triangleq \mathrm{CW}^n(m)$，$\bar{c}^n \triangleq \mathrm{CW}^n(\bar{m})$。因为 $c^{n'_{\min}}_+ = \bar{c}^{n'_{\min}}_+$，所以 $\mathrm{Enc}^{n'_{\min}}_-$ 的输入都是一样的，所以进而有 $c^{n'_{\min}} = \bar{c}^{n'_{\min}}$。这样就存在整数 $n' = n'' = n'_{\min}$ 和区间 $I_a = \bar{I}_a = \varnothing$，使得

$$\left|I_a\right| \le z \tag{2–12}$$

$$\left|\overline{I}_a\right| \le z \tag{2–13}$$

$$\left|I_a\right| + \left|\overline{I}_a\right| + \left|\left(n' : n\right]_+\right| \le 2z \tag{2–14}$$

$$I_a = \left\{i \in \left[1 : n''\right] : c_i \ne \overline{c}_i\right\} \bigcup \left(n'' : n'\right]_- \tag{2–15}$$

$$\overline{I}_a = \left\{i \in \left(n'' : n'\right] : c_i \ne \overline{c}_i\right\} \bigcup \left(n'' : n'\right]_- . \tag{2–16}$$

这与引理 2.4 矛盾。这样我们就证明了所有的检 z 个错的码的大小都 $\le \prod_{i \in [1:n'_{\min}]_+} q_i$。 □

引理 2.9（纠错不能）：考虑 $s^n \circ q^n$ 和 $z \in \mathbb{N}$。若 $\left|\left[1:n\right]_+\right| \le 2z$，则 $A^{(z,z)}_{s^n \circ q^n} = 1$。□

证明：因为 $\left|\left[1:n\right]_+\right| \le 2z$，所以引理 2.8 中 $n'_{\min} = 0$。所以 $\left[1:n'_{\min}\right]_+ = \varnothing$，$A^{(z,z)}_{s^n \circ q^n} \le 1$。得证。 □

2.3.2 与下界证明有关的性质

引理 2.10（构造纠 z 错码）：考虑 $s^n \circ q^n$。$A, A' \in \mathbb{N}$ 满足 $1 \le A' \le A$。若存在 $n' \in \left[1:n\right]$，$n'' \in \left[n' : n\right]$ 使得

(1) 在 $s^{n'} \circ q^{n'}$ 存在检 z 错码 C'，其大小为 A，并且当 $\left[1:n'\right]$ 中的错误数 $\le z$ 时只会剩下 A' 种可能的消息；

(2) $A^{(z-1,z-1)}_{-s_{(n':n'']} \circ q_{(n':n'']}} \ge \binom{A}{A'}$；

(3) $A^{(z-1,z-1)}_{s_{(n'':n]} \circ q_{(n'':n]}} \ge A'$。

则存在消息集大小为 A 的检 z 错码。 □

对于这种存在性命题，先构造码（不妨记为码 C），然后证明码 C 有给定的纠错能力。

构造码 C：（编码器）(1) 在 $s^{n'} \circ q^{n'}$ 使用了条件 (1) 中的码 C' 来传输；(2) 因为 $A^{(z-1,z-1)}_{-s_{(n':n'']} \circ q_{(n':n'']}} \ge \binom{A}{A'}$，所以在 $-s_{(n':n'']} \circ q_{(n':n'']}$ 上存在一个消息集为 $\left[0:A\right)$ 的可以纠 $\left(z-1\right)$ 个错的码。目的节点对码 C' 进行译码，如果译码结果 $\hat{M}' \ne \varepsilon$ 则后续编码器任意发送符号；如果 $\hat{M}' = \varepsilon$，则用列表编码进行译码，可以确定出一个大小不大于 A' 的消息集合，使得所有可能的消息都在这个消息集合内。进一步，采用某种规则可以选取一个大小等于 A' 的消息集合（比如规则可以是选择所有可能的集合

中字典序最大的集合，记选得的集合为 $\mathcal{M}' \triangleq \{m'_0, m'_1, \cdots, m'_{A'-1}\}$），使得所有可能的消息都在这个集合内。编码器 $\mathrm{Enc}_{(n':n'']}$：因为 $\mathcal{M}$ 的大小为 A' 的子集一共有 $\binom{A}{A'}$ 个，所以可以将 $\mathcal{M}'$ 编为 $\left[0:\binom{A}{A'}\right)$ 中的一个符号并发送。这个码记为 C''；(3) 若 $\hat{M}' \neq \varepsilon$ 源节点译出码 C'' 的结果 $\hat{M}''$，这个结果对应于消息集中的 A' 个消息（不妨设这 A' 个消息为 $m_i, 0 \le i \le A'-1$）。因为 $A^{(z-1,z-1)}_{s_{(n'':n]} \circ q_{(n'':n]}} \ge A'$，在 $s_{(n'':n]} \circ q_{(n'':n]}$ 上存在消息集大小为 A' 的纠 $(z-1)$ 错的码 C'''。如果 $\exists i \in [0:A')$ 使得 $M = m'_i$，则用码 C''' 发送 i，否则发送任意符号。

（译码器）若 $\hat{M}' \neq \varepsilon$，则 $\hat{M} = \hat{M}'$；否则确定出集合 $\mathcal{M}'$ 并对码 C''' 进行译码得到 $\hat{M}'''$，则 $\hat{M} = m'_{\hat{M}'''}$。

证明码 C 能纠 z 错： 限定 $d_H(X^n, Y^n) \le z$。考虑以下两种情况：

(情况 1) $\hat{M}' \neq \varepsilon$。由于 C' 可以检 z 个错，所以 $\hat{M}' = M$。又因为 $\hat{M} = \hat{M}'$，所以 $\hat{M} = M$。

(情况 2) $\hat{M}' = \varepsilon$。由于 C' 可以检 z 个错，所以 $d_H(X^{n'}, Y^{n'}) > 0$。所以 $d_H(X_{(n':n'']}, Y_{(n':n'']}) \le z-1$ 或 $d_H(X_{(n'':n]}, Y_{(n'':n]}) \le z-1$。所以纠 $(z-1)$ 错的 C'' 和 C''' 都能正确传输。其中，码 C'' 让源节点知道目的节点可能存在哪 A' 个可能的译码结果，码 C''' 告诉目的节点应译为 A' 个可能结果中的哪个结果。最终 $\hat{M} = M$。

综上，$\hat{M} = M$。所以码 C 能纠 z 错。 □

以上就是所有的准备工作。

2.4 三个传输交互模型及其求解

2.4.1 模型与结果

本节考虑三个传输交互模型。三个传输交互模型是一种特殊的交互模型，其中源节点与目的节点间有三个传输，其传输方向分别为：$s_1 = +1$，$s_2 = -1$，$s_3 = +1$（如图 2.3）。显然，如果去除其中任意的一个传输，都不能形成交互。所以三个传输交互模型是最简单的一种交互模型。

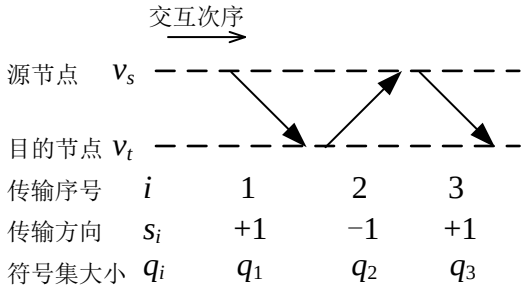


图 2.3　三个传输交互模型

该模型的结论见下面的定理 2.1。该定理完全刻画了三个传输模型的检错能力和纠错能力。

定理 2.1（三个传输）：$A^{(z,z)}_{+q_1,-q_2,+q_3}=\begin{cases} q_1q_3, & z=0 \\ 1, & z>0, \end{cases}$

$$A^{(z,0)}_{+q_1,-q_2,+q_3}=\begin{cases} q_1q_3, & z=0 \\ \min\{q_1,q_2(q_3-1)\}, & z=1 \\ 1, & z\geq 2. \end{cases}$$ □

前文已经提到，纠 z 错的最大消息集大小 $A^{(z,z)}_{+q_1,-q_2,+q_3}$ 和检 z 错的最大消息集大小 $A^{(z,0)}_{+q_1,-q_2,+q_3}$ 完全表征了三个传输交互模型的检错、纠错性能极限。定理 2.1 给出了 $A^{(z,z)}_{+q_1,-q_2,+q_3}$ 和 $A^{(z,0)}_{+q_1,-q_2,+q_3}$ 的闭式解，就彻底完成了三个传输交互模型的检错、纠错性能极限的全部刻画。

2.4.2 定理证明

从结果上看，三个传输模型既是最简单的交互模型模型，又是在检错的情况下得到非平凡结果的最小模型。定理 2.1 的唯一的不平凡结果，就是确定了 $A^{(1,0)}_{+q_1,-q_2,+q_3}$ 的取值。

本节证明定理 2.1。首先来考虑其中检 1 错的情况。

对于任意的码，定义 $\mathcal{M}_i(c_i)\triangleq\{m\in\mathcal{M}:\mathrm{CW}_i(m)=c_i\}$，$\mu_i(c_i)\triangleq|\mathcal{M}_i(c_i)|$（$c_i\in\mathcal{Q}_i$）。

引理 2.11：C 是 $+q_1,-q_2,+q_3$ 上检 1 错的码，则其消息集大小 $\leq q_2(q_3-1)$。 □

证明：用反证法。反设其上的码 C 的消息集大小 $>q_2(q_3-1)$。根据抽屉原理，存在 $\theta\in\mathcal{Q}_2$ 使得 $|\mathcal{M}_2(\theta)|>q_3-1$。考虑以下情况：

(情况 1) 存在两个不同的消息 $\bar{m},\tilde{m}\in\mathcal{M}_2(\theta)$（$\bar{m}\neq\tilde{m}$）使得 $\mathrm{CW}_3(\bar{m})=\mathrm{CW}_3(\tilde{m})$。进一步考虑以下两种子情况：

(情况 1.1) 译码器满足 $\mathrm{Dec}\left(\mathrm{CW}_1(\bar{m}),\mathrm{CW}_3(\bar{m})\right)\neq\bar{m}$。这时，当 $M=\bar{m}$，$X^3=Y^3$ 时，译码器输入为 $\mathrm{CW}_1(\bar{m}),\mathrm{CW}_3(\bar{m})$，输出 $\hat{M}\neq\bar{m}$。所以 $\hat{M}\neq M$。根据检错码的定义，码 C 不能检 1 错。

(情况 1.2) 译码器满足 $\mathrm{Dec}\left(\mathrm{CW}_1(\bar{m}),\mathrm{CW}_3(\bar{m})\right)=\bar{m}$。这时，当 $M=\tilde{m}$，$Y_1=\mathrm{CW}_1(\bar{m})$，$X_2X_3=Y_2Y_3$ 时，有 $d_H\left(X^3,Y^3\right)\leq 1$ 并且 $Y_2=X_2=\mathrm{Enc}_2\left(\mathrm{CW}_1(\bar{m})\right)=\mathrm{CW}_2(\bar{m})$，$Y_3=X_3=\mathrm{Enc}_3\left(\tilde{m},\mathrm{CW}_2(\bar{m})\right)=\mathrm{CW}_3(\bar{m})$。所以译码器输入为 $\mathrm{CW}_1(\bar{m}),\mathrm{CW}_3(\bar{m})$，输出 $\hat{M}=\bar{m}$。所以 $\hat{M}\neq M$ 且 $\hat{M}\neq\varepsilon$。根据检错码的定义，码 C 不能检 1 错。

(情况 2) 不存在两个不同的消息 $\bar{m},\tilde{m}\in\mathcal{M}_2(\theta)$（$\bar{m}\neq\tilde{m}$）使得 $\mathrm{CW}_3(\bar{m})=\mathrm{CW}_3(\tilde{m})$。因为 $\left|\mathcal{M}_2(\theta)\right|>q_3-1$，所以

$$\left\{\mathrm{CW}_3(m):m\in\mathcal{M}_2(\theta)\right\}=\{0,1,\cdots,q_3-1\}. \tag{2–17}$$

固定某个 $m\in\mathcal{M}\setminus\mathcal{M}_2(\theta)$。令 $\hat{c}_3=\mathrm{Enc}_3(m,\theta)$。由于式（2–17），$\exists\hat{m}\in\mathcal{M}_2(\theta)$ 使得 $\hat{c}_3=\mathrm{CW}_3(\hat{m})$。因为 $m\in\mathcal{M}_2(\theta)$ 且 $\hat{m}\in\mathcal{M}_2(\theta)$，所以 $m\neq\hat{m}$。显然，$\mathrm{CW}^3(\hat{m})=\left\{\mathrm{CW}_1(\hat{m}),\theta,\hat{c}_3\right\}$。考虑以下两种子情况：

(情况 2.1) 译码器满足 $\hat{m}=\mathrm{Dec}\left(\mathrm{CW}_1(\hat{m}),\hat{c}_3\right)$。这时，当 $M=m$，$Y_1=\mathrm{CW}_1(\hat{m})$，$X_2X_3=Y_2Y_3$ 时，有 $d_H\left(X^3,Y^3\right)\leq 1$ 并且 $Y_2=X_2=\mathrm{Enc}_2\left(\mathrm{CW}_1(\hat{m})\right)=\theta$，$Y_3=X_3=\mathrm{Enc}_3(m,\theta)=\hat{c}_3$，$\hat{M}=\mathrm{Dec}\left(\mathrm{CW}_1(\hat{m}),\hat{c}_3\right)=\hat{m}$。所以 $\hat{M}\neq M$ 且 $\hat{M}\neq\varepsilon$。根据检错码的定义，码 C 不能检 1 错。

(情况 2.2) 译码器满足 $\hat{m}\neq\mathrm{Dec}\left(\mathrm{CW}_1(\hat{m}),\hat{c}_3\right)$。这时，当 $M=\hat{m}$，$X^3=Y^3$ 时，译码器输入为 $\mathrm{CW}_1(\hat{m}),\hat{c}_3$，输出 $\hat{M}\neq\hat{m}$。根据检错码的定义，码 C 不能检 1 错。

综上，码 C 不能检 1 错。矛盾。所以引理得证。　□

引理 2.12：在 $+q_1,-q_2,+q_3$ 上，存在消息集大小为 $\min\left\{q_1,q_2(q_3-1)\right\}$ 的检 1 错码。　□

构造码 C：令 $A\triangleq\min\left\{q_1,q_2(q_3-1)\right\}$，$A'\triangleq q_3-1$。显然有 $\dfrac{A}{A'}\leq q_2$。定义下面的码

（编码器）　$$\mathrm{Enc}_1(M)\triangleq M \tag{2–18}$$

$$\mathrm{Enc}_2(Y_1)\triangleq\left\lfloor\frac{Y_1}{A'}\right\rfloor \tag{2–19}$$

$$\mathrm{Enc}_3\left(M,Y_2\right)\triangleq\begin{cases}M \bmod A', & Y_2=\lfloor M/A'\rfloor\\ A', & Y_2\neq\lfloor M/A'\rfloor\end{cases} \tag{2–20}$$

（译码器）
$$\mathrm{Dec}\left(Y_1,Y_3\right)\triangleq\begin{cases}Y_1, & Y_1 \bmod A'=Y_3\\ \varepsilon, & Y_1 \bmod A'\neq Y_3.\end{cases} \tag{2–21}$$

证明码C能检 1 错：(1) 当$d_H\left(X^3,Y^3\right)\leq 1$时，考虑以下两种情况：

(情况 1) $Y_1=X_1$。这时，因为$\mathrm{Dec}\left(Y_1,Y_3\right)=Y_1$或$\mathrm{Dec}\left(Y_1,Y_3\right)=\varepsilon$，所以$\hat{M}=M$或$\hat{M}=\varepsilon$。

(情况 2) $Y_1\neq X_1$。这时，$\lfloor Y_1/A'\rfloor\neq\lfloor X_1/A'\rfloor$或$Y_1 \bmod A'\neq X_1 \bmod A'$。另外由于$d_H\left(X^3,Y^3\right)\leq 1$，所以$Y_2=X_2$，$Y_3=X_3$。

(情况 2.1) $\lfloor Y_1/A'\rfloor\neq\lfloor X_1/A'\rfloor$。由于$Y_2=X_2=\lfloor Y_1/A'\rfloor$且$\lfloor M/A'\rfloor=\lfloor X_1/A'\rfloor$，$Y_2\neq\lfloor M/A'\rfloor$。于是$Y_3=X_3=A'\neq Y_1 \bmod A'$。于是$\hat{M}=\varepsilon$。

(情况 2.2) $\lfloor Y_1/A'\rfloor=\lfloor X_1/A'\rfloor$。这时有$Y_1 \bmod A'\neq X_1 \bmod A'$。由于$Y_3=X_3=M \bmod A'=X \bmod A'$或$Y_3=X_3=A'$，所以$Y_1 \bmod A'\neq Y_3$。进而$\hat{M}=\varepsilon$。

同时考虑情况 1 和情况 2，在$d_H\left(X^3,Y^3\right)\leq 1$时$\hat{M}=M$或$\hat{M}=\varepsilon$。

(2) 当$X^3=Y^3$时，易知$Y_1=X_1=M$，$Y_2=X_2=\left\lfloor\dfrac{M}{A'}\right\rfloor$，$Y_3=X_3=M \bmod A'$，所以$\hat{M}=Y_1=M$。

综上，根据定义，码C能检 1 个错。　□

定理 2.1 的证明：由性质 2.1(2) 知$A^{(0,0)}_{+q_1,-q_2,+q_3}=q_1q_3$。由引理 2.7 知$z\geq 2$时$A^{(2,0)}_{+q_1,-q_2,+q_3}=1$。由引理 2.9 知$z\geq 1$时$A^{(1,1)}_{+q_1,-q_2,+q_3}=1$。

在引理 2.6 中$z=1$时$n'_{\min}=1$，所以$A^{(1,0)}_{+q_1,-q_2,+q_3}\leq q_1$。又由引理 2.11 知$A^{(1,0)}_{+q_1,-q_2,+q_3}\leq q_2\left(q_3-1\right)$，所以$A^{(1,0)}_{+q_1,-q_2,+q_3}\leq\min\left\{q_1,q_2\left(q_3-1\right)\right\}$。再由引理 2.12 知$A^{(1,0)}_{+q_1,-q_2,+q_3}\geq\min\left\{q_1,q_2\left(q_3-1\right)\right\}$，所以$A^{(1,0)}_{+q_1,-q_2,+q_3}=\min\left\{q_1,q_2\left(q_3-1\right)\right\}$。这样定理 2.1 得证。　□

2.5 四个传输交互模型及其求解

2.5.1 模型与结果

本节考虑四个传输交互模型。上节提到，三个传输交互模型可以分析检错的最简单非平凡情况，而对于纠错只有平凡情况。要讨论纠错的非平凡情况，最少需要四个传输。

四个传输交互模型中源节点与目的节点间有四个传输。四个传输模型有两种具体的形式，下称模型甲和模型乙。模型甲的四个传输的方向分别为：$s_1=+1$，$s_2=+1$，$s_3=-1$，$s_4=+1$（如图 2.4）。模型乙的四个传输的方向分别为：$s_1=+1$，$s_2=-1$，$s_3=+1$，$s_4=+1$（如图 2.5）。

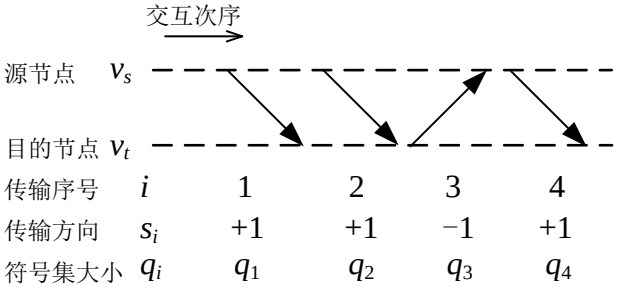


图 2.4　四个传输模型甲

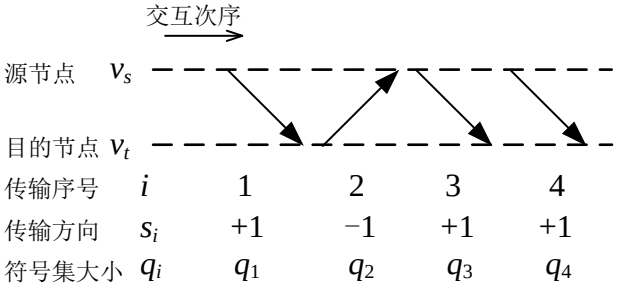


图 2.5　四个传输模型乙

与三个传输模型类似，由性质 2.1(2) 可知，$A^{(0,0)}_{+q_1,+q_2,-q_3,+q_4}=q_1q_2q_4$，$A^{(0,0)}_{+q_1,-q_2,+q_3,+q_4}=q_1q_3q_4$；由引理 2.9 可知 $A^{(z,z)}_{+q_1,+q_2,-q_3,+q_4}=1$（$z>1$），$A^{(z,z)}_{+q_1,-q_2,+q_3,+q_4}=1$（$z>1$）。所以我们将重点考虑 $z=1$ 的情况。

当 $q_1=q_2=q_3=q_4$ 时，消息集大小就是 q_1。

命题 2.1：$A^{(1,1)}_{+q,+q,-q,+q}=q$，$A^{(1,1)}_{+q,-q,+q,+q}=q$。　□

证明：在模型甲和模型乙中，都有三条从源节点到目的节点的传输，在这三次传输上重复编码发送消息，可以纠正 1 个错。所以 $A^{(1,1)}_{+q,+q,-q,+q}\ge q$，$A^{(1,1)}_{+q,-q,+q,+q}\ge q$。另外考虑引理 2.8，当 $z=1$ 时 $n'_{\min}=1$。所以 $A^{(1,1)}_{+q,+q,-q,+q}\le q$，$A^{(1,1)}_{+q,-q,+q,+q}\le q$。命题得证。 □

命题 4.1 给出了 $A^{(1,1)}_{+q,+q,-q,+q}$ 和 $A^{(1,1)}_{+q,-q,+q,+q}$ 的闭式解，完全刻画了在四个传输交互模型的各传输信号集大小相同情况下的纠 1 错码的极限性能。值得一提的是，$A^{(1,1)}_{+q,+q,-q,+q}$ 和 $A^{(1,1)}_{+q,-q,+q,+q}$ 都等于 $A^{(1,1)}_{+q,+q,+q}=q$，即它们的最大消息集大小都等于在没有反馈传输情况下的消息集大小。所以，这时反馈传输事实上没有帮助。也就是说，在交互式传输模型中，反馈传输不一定会有实质性的帮助。

当 q_1,q_2,q_3,q_4 不全相等时，情况复杂的多。

定理 2.2（四个传输）：(1) （模型甲）

$$\min\left\{q_1,q_2,\max\left\{q_3\left(q_4-1\right),2q_4\right\}\right\}\le A^{(1,1)}_{+q_1,+q_2,-q_3,+q_4}\le\min\left\{q_1,q_2,q_3^{q_4}\right\};$$

(2) （模型乙）$\max\left\{\min\left\{q_1,q_2\left(q_3-1\right),q_4\right\},\min\left\{q_1,q_3,q_2\left(q_4-1\right)\right\},\right.$

$$\left.\min\left\{q_1,q_2,\left(q_3-1\right)\left(q_4-1\right)+1\right\}\right\}\le A^{(1,1)}_{+q_1,-q_2,+q_3,+q_4}$$

$$\le\min\left\{q_1,q_2\left(q_3-1\right),q_2\left(q_4-1\right),\min_{k=1,2,\cdots}\left\{\max\left\{\left(k-1\right)q_2,\left(q_3-k\right)\left(q_4-k\right)+k\right\}\right\}\right\}.$$ □

定理 2.2 对四个传输交互模型的纠 1 码的最大消息集大小 $A^{(1,1)}_{+q_1,+q_2,-q_3,+q_4}$ 和 $A^{(1,1)}_{+q_1,-q_2,+q_3,+q_4}$ 进行了刻画。具体而言，为这两个值都提供了上界和下界。这些上界和下界帮助了解四个传输交互模型的纠 1 码的极限性能。

对于模型甲，当 $q_2,q_3,q_4\ge q_1$ 或 $q_3=q_4=2$ 时，上界和下界相等。证明之后还会给出一个上下界不等的例子（$+5,+5,-3,+2$，其在定理 2.2 中的上界为 5，下界为 4），并证明了 $A^{(1,1)}_{+5,+5,-3,+2}=4$。

对于模型乙当 $q_2,q_3,q_4\ge q_1$ 或 $q_3=2$ 或 $q_4=2$ 时，上界和下界相等。证明之后还会给出一个上下界不等的例子（$+6,-2,+5,+5$，其在定理 2.2 中的上界为 6，下界为 5），并证明了 $A^{(1,1)}_{+6,-2,+5,+5}=5$。

2.5.2 定理证明

引理 2.13：考虑 $s^n\circ q^n$，$I\subseteq[1:n]$，则

$$A^{(1,1)}_{s^n\circ q^n}\ge\min\left\{A^{(1,0)}_{s_I\circ q_I},\prod_{i\in[1:n]_+\setminus I}q_i\right\}.$$ □

证明：设 $A=\min\left\{A^{(1,0)}_{s_I\circ q_I},\prod_{i\in[1:n]_+\setminus I}q_i\right\}$，显然有 $A^{(1,0)}_{s_I\circ q_I}\geq A$ 且 $\prod_{i\in[1:n]_+\setminus I}q_i\geq A$。所以，在 $s_I\circ q_I$ 上可以构造消息集大小为 A 的检 1 错的码 C'，在 $[1:n]_+\setminus I$ 可以将消息集大小为 A 的消息再原样发送一次（记为 C''）。用码 C' 和码 C'' 构造消息集大小为 A 的码 C。译码器：当 C' 的译码结果 $\hat{M}'\neq\varepsilon$ 时，$\hat{M}=\hat{M}'$；否则 $\hat{M}=\hat{M}''$。

下证码 C 可以纠 1 错。限定 $d_H\left(X^4,Y^4\right)\leq 1$。考虑以下两种情况：

(情况 1) $\hat{M}'\neq\varepsilon$。因为码 C' 能检 1 错，所以 $\hat{M}'=M$，进而 $\hat{M}=M$；

(情况 2) $\hat{M}'=\varepsilon$。因为码 C' 能检 1 错，所以 $d_H\left(X_I,Y_I\right)>0$。进而 $X_{[1:n]_+\setminus I}=Y_{[1:n]_+\setminus I}$，所以 $\hat{M}=\hat{M}''=M$。

综上，$\hat{M}=M$。所以码 C 能检 1 错。由于码 C 的消息集大小为 A，所以 $A^{(1,1)}_{s^n\circ q^n}\geq A$，得证。 □

引理 2.14（模型甲下界）：$A^{(1,1)}_{+q_1,+q_2,-q_3,+q_4}\geq\min\left\{q_1,q_2,q_3\left(q_4-1\right)\right\}$. □

证明：在引理 2.13 中，取 $I=[2:4]$。由定理 2.1 知 $A^{(1,0)}_{+q_2,-q_3,+q_4}\geq\min\left\{q_2,q_3\left(q_4-1\right)\right\}$，所以 $A^{(1,1)}_{+q_1,+q_2,-q_3,+q_4}\geq\min\left\{q_1,\min\left\{q_2,q_3\left(q_4-1\right)\right\}\right\}$
$=\min\left\{q_1,q_2,q_3\left(q_4-1\right)\right\}$。 □

引理 2.15（模型甲下界）：$A^{(1,1)}_{+q_1,+q_2,-q_3,+q_4}\geq\min\left\{q_1,q_2,2q_4\right\}$. □

证明：设 $A\triangleq\min\left\{q_1,q_2,2q_4\right\}$。不妨假设 $q_4<A$（否则用重复编码即可）。显然有 $q_1\geq A$，$q_2\geq A$，$2q_4\geq A$。构造消息集大小为 A 的码 C：

（编码器）　$\mathrm{Enc}_1\left(M\right)\triangleq M$

$$\mathrm{Enc}_2\left(M\right)\triangleq M$$

$$\mathrm{Enc}_3\left(Y_1,Y_2\right)\triangleq\begin{cases}1, & \left|Y_1-Y_2\right|=q_4\\ 0, & \text{其他}\end{cases}$$

$$\mathrm{Enc}_4\left(Y_3,M\right)\triangleq\begin{cases}M, & M\in[0:q_4)\\ M-q_4, & M\in[q_4:A)\text{且}Y_3=0\\ 1, & M=q_4\text{且}Y_3\neq 0\\ 0, & M=(q_4:A)\text{且}Y_3\neq 0.\end{cases}$$

（译码器） $\mathrm{Dec}(Y_1,Y_2,Y_4)\triangleq$

$$\begin{cases} Y_1, & Y_1=Y_2 \\ Y_4, & Y_1\neq Y_2 \text{且}(Y_1=Y_4 \text{或} Y_2=Y_4) \\ Y_4+q_4, & \wp \text{且}(Y_1=Y_4+q_4 \text{或} Y_2=Y_4+q_4) \\ Y_1, & \wp \text{且} Y_1\neq Y_4+q_4 \text{且} Y_2\neq Y_4+q_4 \text{且} |Y_1-Y_2|=q_4 \text{且} Y_1\in[q_4:A) \text{且} \mathrm{Enc}_4(1,Y_1)=Y_4 \\ Y_2, & \wp \text{且} Y_1\neq Y_4+q_4 \text{且} Y_2\neq Y_4+q_4 \text{且} |Y_1-Y_2|=q_4 \text{且} Y_2\in[q_4:A) \text{且} \mathrm{Enc}_4(1,Y_2)=Y_4 \\ \text{不关心}, & \text{其他}, \end{cases}$$

其中 $\wp$ 表示 Y_1、Y_2、Y_4 两两不等。

译码器的构造利用了以下性质：当 $|Y_1-Y_2|=q_4$ 时，由于 $2q_4\geq A$ 且 $1\leq q_4<A$，所以 $Y_1\in[q_4:A)$ 和 $Y_2\in[q_4:A)$ 不会同时成立。

下面证明码 C 能够检 1 错。限定 $d_H\left(X^4,Y^4\right)\leq 1$。考虑以下情况：

(情况 1) $M\in[0:q_4)$。这种情况下，$X_1=X_2=X_4=M$。又因为 $d_H\left(X^4,Y^4\right)\leq 1$，所以 Y_1、Y_2、Y_4 中至多有一个不是 M。根据译码规则前两条（即当 $Y_1=Y_2$ 时 $\hat{M}=Y_1$，当 $Y_1\neq Y_2$ 且 $(Y_1=Y_4$ 或 $Y_2=Y_4)$ 时 $\hat{M}=Y_4$，所以 $\hat{M}=M$。

(情况 2) $M\in[q_4:A)$。考虑以下子情况：

(情况 2.1) $X_3=0$。这种情况下，进一步分为以下情况：

(情况 2.1.1) 若 $X_1X_2=Y_1Y_2$，则 $Y_1=Y_2=M$，利用译码规则第 1 条（当 $Y_1=Y_2$ 时 $\hat{M}=Y_1$），有 $\hat{M}=M$。

(情况 2.1.2) 若 $X_1\neq Y_1$，则 $Y_2=X_2=M$ 且 $Y_4+q_4=X_4+q_4=M$。利用译码规则第 3 条（当 $Y_1\neq Y_2$ 且 $Y_1\neq Y_4$ 且 $Y_2\neq Y_4$ 且 $(Y_1=Y_4+q_4$ 或 $Y_2=Y_4+q_4)$ 时 $\hat{M}=Y_4+q_4$），有 $\hat{M}=M$。

(情况 2.1.3) 若 $X_2\neq Y_2$，则 $Y_1=X_1=M$ 且 $Y_4+q_4=X_4+q_4=M$。利用译码规则第 3 条，有 $\hat{M}=M$。

(情况 2.2) $X_3=1$。这时有 $|Y_1-Y_2|=q_4$，进而 $Y_1\neq Y_2$，所以 $d_H\left(X^2,Y^2\right)>0$，进而 $Y_3=X_3=1$，$Y_4=X_4$。通过对 M 进行分类讨论可以知道（当 $M=q_4$ 时 $Y_4=1$，当 $M\in(q_4:A)$ 时 $Y_4=0$），可以知道 $Y_1\neq Y_4+q_4$ 且 $Y_2\neq Y_4+q_4$。另外，由于 $X_1=M$，$X_2=M$，故 Y_1 和 Y_2 必有一个为 M。之前证明过 $Y_1\in[q_4:A)$ 和 $Y_2\in[q_4:A)$ 不会同时成立，所以 Y_1 和 Y_2 中属于 $[q_4:A)$ 的必然等于 M。所以 $\hat{M}=M$。

综上，$\hat{M}=M$。所以码 C 能纠 1 个错。 □

我们来看模型甲的上界。

引理 2.16（模型甲上界）：(1) $A^{(1,1)}_{+q_1,+q_2,-q_3,+q_4}\leq q_1$；

(2) $A^{(1,1)}_{+q_1,+q_2,-q_3,+q_4} \le q_2$. □

证明：(1) 在引理 2.8 中，$z=1$时 $n'_{\min}=1$，所以 $A^{(1,1)}_{+q_1,+q_2,-q_3,+q_4} \le q_1$。

(2) 证明方法与引理 2.8 中的方法类似。用反证法。假设存在纠 1 错码C，其消息集大小$>q_2$。则存在两个不同的消息$m,\bar{m}$使得$\mathrm{CW}_2(m)=\mathrm{CW}_2(\bar{m})$。定义 $\hat{y}_4 \triangleq \mathrm{Enc}_4\left(m,\mathrm{CW}_3(\bar{m})\right)$。考虑以下两种情况：

(情况 1) 译码器满足$\mathrm{Dec}\left(\mathrm{CW}_1(\bar{m}),\mathrm{CW}_2(\bar{m}),\hat{y}_4\right)\neq m$。考虑$M=m$，$Y_1=\mathrm{CW}_1(\bar{m})$，$Y_{[2:4]}=X_{[2:4]}$。这时$Y_2=X_2=\mathrm{CW}_2(m)=\mathrm{CW}_2(\bar{m})$，$Y_3=X_3=\mathrm{Enc}_3\left(\mathrm{CW}_1(\bar{m}),\mathrm{CW}_2(\bar{m})\right)=\mathrm{CW}_3(\bar{m})$，$\hat{M}=\left(\mathrm{CW}_1(\bar{m}),\mathrm{CW}_2(m),\hat{y}_4\right)\neq m$。所以$\hat{M}\neq M$。根据检错码的定义，码$\mathsf{C}$不能检 1 错。

(情况 2) 译码器满足$\mathrm{Dec}\left(\mathrm{CW}_1(\bar{m}),\mathrm{CW}_2(\bar{m}),\hat{y}_4\right)=m$。考虑$M=\bar{m}$，$Y^3=X^3$，$Y_4=\hat{y}_4$。这时$\hat{M}=\left(\mathrm{CW}_1(\bar{m}),\mathrm{CW}_2(\bar{m}),\hat{y}_4\right)=m$。所以$\hat{M}\neq M$。根据检错码的定义，码$\mathsf{C}$不能检 1 错。

综上，码C不能检 1 错，得到矛盾。得证。 □

引理 2.17（模型甲上界）：$A^{(1,1)}_{+q_1,+q_2,-q_3,+q_4} \le q_3^{q_4}$. □

证明：用反证法。反设存在纠 1 错的码C，使得消息集大小$>q_3^{q_4}$。根据抽屉原理，存在两个不同的消息$m,\bar{m}$，使得$\forall y_3\in\mathcal{Q}_3$，有$\mathrm{Enc}_4(m,y_3)=\mathrm{Enc}_4(\bar{m},y_3)$。令$\hat{y}_3=\mathrm{Enc}_3\left(\mathrm{CW}_1(\bar{m}),\mathrm{CW}_2(m)\right)$，$\hat{y}_4=\mathrm{Enc}_4(m,\hat{y}_3)$，则有$\hat{y}_4=\mathrm{Enc}_4(\bar{m},\hat{y}_3)$。考虑以下两种情况：

(情况 1) 译码器满足$\mathrm{Dec}\left(\mathrm{CW}_1(\bar{m}),\mathrm{CW}_2(m),\hat{y}_4\right)\neq m$。这时考虑$M=m$，$Y_1=\mathrm{CW}_1(\bar{m})$，$Y_{[2:4]}=X_{[2:4]}$。这时，$Y_2=X_2=\mathrm{CW}_2(m)$，$Y_3=X_3=\mathrm{Enc}_3\left(\mathrm{CW}_1(\bar{m}),\mathrm{CW}_2(m)\right)=\hat{y}_3$，$Y_4=X_4=\mathrm{Enc}_4(m,\hat{y}_3)=\hat{y}_4$，$\hat{M}=\mathrm{Dec}\left(\mathrm{CW}_1(\bar{m}),\mathrm{CW}_2(m),\hat{y}_4\right)\neq m$，有$\hat{M}\neq M$。这说明码$\mathsf{C}$不能纠 1 错。

(情况 2) 译码器满足$\mathrm{Dec}\left(\mathrm{CW}_1(\bar{m}),\mathrm{CW}_2(m),\hat{y}_4\right)=m$。这时考虑$M=\bar{m}$，$Y_1=X_1$，$Y_2=\mathrm{CW}_2(m)$，$Y_{[3:4]}=X_{[3:4]}$。这时，$Y_1=X_1=\mathrm{CW}_1(\bar{m})$，$Y_3=X_3=\mathrm{Enc}_3\left(\mathrm{CW}_1(\bar{m}),\mathrm{CW}_2(m)\right)=\hat{y}_3$，$Y_4=X_4=\mathrm{Enc}_4(m,\hat{y}_3)=\hat{y}_4$，$\hat{M}=\mathrm{Dec}\left(\mathrm{CW}_1(\bar{m}),\mathrm{CW}_2(m),\hat{y}_4\right)=m$，有$\hat{M}\neq M$。这说明码$\mathsf{C}$不能纠 1 错。

综上，码C不能纠 1 错，得到矛盾。得证。 □

证明（定理 2.2 模型甲部分）：由引理 2.14 和引理 2.15 知 $A^{(1,1)}_{+q_1,+q_2,-q_3,+q_4}\geq\min\{q_1,q_2,q_3(q_4-1)\}$ 且 $A^{(1,1)}_{+q_1,+q_2,-q_3,+q_4}\geq\min\{q_1,q_2,2q_4\}$，所以 $A^{(1,1)}_{+q_1,+q_2,-q_3,+q_4}\geq\min\{q_1,q_2,\max\{q_3(q_4-1),2q_4\}\}$。

由引理 2.16 知 $A^{(1,1)}_{+q_1,+q_2,-q_3,+q_4}\leq q_1$ 和 $A^{(1,1)}_{+q_1,+q_2,-q_3,+q_4}\leq q_2$，再由引理 2.17 知 $A^{(1,1)}_{+q_1,+q_2,-q_3,+q_4}\leq q_3^{q_4}$，所以 $A^{(1,1)}_{+q_1,+q_2,-q_3,+q_4}\leq\min\{q_1,q_2,q_3^{q_4}\}$。 □

这样就证明了定理 2.2 中的模型甲的部分。

接着考虑模型乙。先考虑其下界。

引理 2.18（模型乙下界）：(1) $A^{(1,1)}_{+q_1,-q_2,+q_3,+q_4}\geq\min\{q_1,q_2(q_3-1),q_4\}$；

(2) $A^{(1,1)}_{+q_1,-q_2,+q_3,+q_4}\geq\min\{q_1,q_3,q_2(q_4-1)\}$. □

证明：(1) 在引理 2.13 中取 $I\triangleq[1:3]$，有 $A^{(1,0)}_{s^3\circ q^3}=\min\{q_1,q_2(q_3-1)\}$。所以 $A^{(1,1)}_{+q_1,-q_2,+q_3,+q_4}\geq\min\{q_1,q_2(q_3-1),q_4\}$。

(2) 在引理 2.13 中取 $I\triangleq\{1,2,4\}$，有 $A^{(1,0)}_{s_{\{1,2,4\}}\circ q_{\{1,2,4\}}}=\min\{q_1,q_2(q_4-1)\}$。所以 $A^{(1,1)}_{+q_1,-q_2,+q_3,+q_4}\geq\min\{q_1,q_2(q_3-1),q_3\}$。 □

引理 2.19（模型乙下界）：$A^{(1,1)}_{+q_1,-q_2,+q_3,+q_4}\geq\min\{q_1,q_2,(q_3-1)(q_4-1)+1\}$. □

证明：设 $A\triangleq\min\{q_1,q_2,(q_3-1)(q_4-1)+1\}$。显然 $q_1\geq A$，$q_2\geq A$，$(q_3-1)(q_4-1)+1\geq A$。对于 $x\in\mathbb{N}$，定义

$$\langle x\rangle_3\triangleq\left\lceil\frac{x}{q_4-1}\right\rceil \tag{2–22}$$

$$\langle x\rangle_4\triangleq\begin{cases}x\bmod(q_4-1), & x\bmod(q_4-1)\neq 0\\ q_4-1, & x\bmod(q_4-1)=0\end{cases} \tag{2–23}$$

$$\langle x\,|\,y\rangle_3\triangleq\begin{cases}\langle x\rangle_3, & x=y\text{或}\langle x\rangle_3\neq\langle y\rangle_3\\ 0, & x\neq y\text{且}\langle x\rangle_3=\langle y\rangle_3\end{cases} \tag{2–24}$$

$$\langle x\,|\,y\rangle_4\triangleq\begin{cases}\langle x\rangle_4, & x=y\text{或}\langle x\rangle_4\neq\langle y\rangle_4\\ 0, & x\neq y\text{且}\langle x\rangle_4=\langle y\rangle_4.\end{cases} \tag{2–25}$$

可以证明，对于 $x,y\in\mathbb{N}$，若 $\langle x\,|\,y\rangle_3=\langle y\rangle_3\neq 0$，则 $x=y$。（用反证法证明：反设 $x\neq y$。考虑以下两种情况：(情况 1) $\langle x\rangle_3=\langle y\rangle_3$。这时候有 $\langle x\,|\,y\rangle_3=0$ 与

$\langle x|y\rangle_3 \neq 0$矛盾;(情况 2) $\langle x\rangle_3 \neq \langle y\rangle_3$。这时候有$\langle x|y\rangle_3 = \langle x\rangle_3 \neq \langle y\rangle_3$与$\langle x|y\rangle_3 = \langle y\rangle_3$矛盾。）类似的，若$\langle x|y\rangle_4 = \langle y\rangle_4 \neq 0$，则$x = y$。

构造码C：（编码器）

$$\mathrm{Enc}_1(M) \triangleq M \tag{2–26}$$

$$\mathrm{Enc}_2(Y_1) \triangleq Y_1 \tag{2–27}$$

$$\mathrm{Enc}_3(M, Y_2) \triangleq \begin{cases} 0, & M = 0 \\ \langle M\rangle_3, & M \neq 0 \text{且} Y_2 = 0 \\ \langle M|Y_2\rangle_3, & M \neq 0 \text{且} Y_2 \neq 0 \end{cases} \tag{2–28}$$

$$\mathrm{Enc}_4(M, Y_2) \triangleq \begin{cases} 0, & M = 0 \\ \langle M\rangle_4, & M \neq 0 \text{且} Y_2 = 0 \\ \langle M|Y_2\rangle_4, & M \neq 0 \text{且} Y_2 \neq 0. \end{cases} \tag{2–29}$$

（译码器）　$\mathrm{Dec}(Y_1, Y_3, Y_4) \triangleq$

$$\begin{cases} 0, & Y_1 = 0 \text{且}(Y_3 = 0 \text{或} Y_4 = 0) \\ \hat{m} \text{使得} \langle \hat{m}\rangle_3 = Y_3 \text{且} \langle \hat{m}\rangle_4 = Y_4, & Y_1 = 0 \text{且} Y_3 \neq 0 \text{且} Y_4 \neq 0 \\ 0, & Y_1 \neq 0 \text{且} Y_3 = Y_4 = 0 \\ \hat{m} \text{使得} \langle \hat{m}|Y_1\rangle_3 = Y_3 \text{且} \langle \hat{m}|Y_1\rangle_4 = Y_4, & Y_1 \neq 0 \text{且} (Y_3 \neq 0 \text{或} Y_4 \neq 0). \end{cases} \tag{2–30}$$

下面证明，码C能纠 1 个错。按照Enc_3、Enc_4的编码规则分类：

(情况 1) 若$M = 0$，则$X_1 = X_3 = X_4 = 0$，这时有$Y_3 = Y_4 = 0$或$Y_1 = Y_3 = 0$或$Y_1 = Y_4 = 0$，所以$\hat{M} = 0$

(情况 2) 若$M \neq 0$，$Y_2 = 0$，则$Y_3 = \langle M\rangle_3 \neq 0$，$Y_4 = \langle M\rangle_4 \neq 0$。

(情况 2.1) 若$Y_1 = 0$，则按照译码规则 2 译得$\hat{M} = M$。

(情况 2.2) 若$Y_1 \neq 0$，则$Y_1 = M$。注意到$\langle M|M\rangle_3 = \langle M\rangle_3$和$\langle M|M\rangle_4 = \langle M\rangle_4$，按照译码规则 4 译得$\hat{M} = M$。

(情况 3) 若$M \neq 0$，$Y_2 \neq 0$。令$Y_2 = \bar{m}$（$\bar{m}$可以等于M），因为$Y_2 = \bar{m}$，所以$Y_1 = \bar{m}$或$Y_1 = M$。均有$Y_1 \neq 0$。$Y_3 = \langle M|\bar{m}\rangle_3$，$Y_4 = \langle M|\bar{m}\rangle_4$。无论$M$和$\bar{m}$是否相等，$Y_3$、$Y_4$至少有一个不为 0。

(情况 3.1) 若$M = \bar{m}$，则$X_1 = Y_1$且$X_2 = Y_2$。$X_3 = \langle M\rangle_3$，$X_4 = \langle M\rangle_4$。则有$Y_3 = \langle M\rangle_3$或$Y_4 = \langle M\rangle_4$。

(情况 3.2) 若$M \neq \bar{m}$，则

(情况 3.2.1) 若$\langle M\rangle_3=\langle\bar{m}\rangle_3$且$\langle M\rangle_4\neq\langle\bar{m}\rangle_4$，则$Y_3=0$，$Y_4=\langle M\rangle_4$；

(情况 3.2.2) 若$\langle M\rangle_3\neq\langle\bar{m}\rangle_3$且$\langle M\rangle_4=\langle\bar{m}\rangle_4$，则$Y_3=\langle M\rangle_3$，$Y_4=0$；

(情况 3.3.3) 若$\langle M\rangle_3\neq\langle\bar{m}\rangle_3$且$\langle M\rangle_4\neq\langle\bar{m}\rangle_4$，则$Y_3=\langle M\rangle_3$，$Y_4=\langle M\rangle_4$。

综合考虑 (情况 3.1) 和 (情况 3.2)，有$Y_3=\langle M\rangle_3$或$Y_4=\langle M\rangle_4$。之前已经知道，对于$x,y\in\mathbb{N}$，若$\langle x\mid y\rangle_3=\langle y\rangle_3\neq 0$则有$x=y$。由译码规则 4 知，对于$\forall m\in\mathcal{M}$，$\forall y_4\in\mathcal{Q}_4$，均有$\mathrm{Dec}\left(m,\langle m\rangle_3,y_4\right)=m$。用类似的方法，可以证明对于$\forall m\in\mathcal{M}$，$\forall y_3\in\mathcal{Q}_3$，均有$\mathrm{Dec}\left(m,y_3,\langle m\rangle_4\right)=m$。所以$\hat{M}=M$。

综上，$\hat{M}=M$。码C能纠 1 个错。得证。 □

引理 2.20（模型乙码字的限制）：C是$+q_1,-q_2,+q_3,+q_4$上的纠 1 错码。$m,\bar{m}\in\mathcal{M}$（$m\neq\bar{m}$）是两个不同的消息。若$\mathrm{CW}_2(m)=\mathrm{CW}_2(\bar{m})$，则有$\mathrm{CW}_3(m)\neq\mathrm{CW}_3(\bar{m})$且$\mathrm{CW}_4(m)\neq\mathrm{CW}_4(\bar{m})$。 □

证明：用反证法。下面仅证明当$\mathrm{CW}_2(m)=\mathrm{CW}_2(\bar{m})$时有$\mathrm{CW}_3(m)\neq\mathrm{CW}_3(\bar{m})$。$\mathrm{CW}_4(m)\neq\mathrm{CW}_4(\bar{m})$的证明方法相同，从略。

反设消息m和$\bar{m}$使得$\mathrm{CW}_2(m)=\mathrm{CW}_2(\bar{m})$和$\mathrm{CW}_3(m)=\mathrm{CW}_3(\bar{m})$同时成立。考虑以下两种情况：

(情况 1) 译码器满足$\mathrm{Dec}\left(\mathrm{CW}_1(\bar{m}),\mathrm{CW}_3(m),\mathrm{CW}_4(m)\right)\neq m$。这时考虑$M=m$，$Y_1=\mathrm{CW}_1(\bar{m})$，$Y_{[2:4]}=X_{[2:4]}$，则有$Y_2=X_2=\mathrm{CW}_2(m)$，$Y_3=X_3=\mathrm{CW}_3(m)$，$Y_4=X_4=\mathrm{CW}_4(m)$，$\hat{M}=\mathrm{Dec}\left(\mathrm{CW}_1(\bar{m}),\mathrm{CW}_3(m),\mathrm{CW}_4(m)\right)\neq m$，所以有$d_H\left(Y^4,X^4\right)\leq 1$且$\hat{M}\neq M$，码$\mathsf{C}$不能纠 1 错。

(情况 2) 译码器满足$\mathrm{Dec}\left(\mathrm{CW}_1(\bar{m}),\mathrm{CW}_3(m),\mathrm{CW}_4(m)\right)=m$。这时考虑$M=\bar{m}$，$Y^3=X^3$，$Y_4=\mathrm{CW}_4(m)$，则有$Y_1=X_1=\mathrm{CW}_1(\bar{m})$，$Y_2=X_2=\mathrm{CW}_2(\bar{m})=\mathrm{CW}_2(m)$，$Y_3=X_3=\mathrm{CW}_3(\bar{m})=\mathrm{CW}_3(m)$，$\hat{M}=\mathrm{Dec}\left(\mathrm{CW}_1(\bar{m}),\mathrm{CW}_3(m),\mathrm{CW}_4(m)\right)\neq m$，所以有$d_H\left(Y^4,X^4\right)\leq 1$且$\hat{M}\neq M$，码$\mathsf{C}$不能纠 1 错。

以上两种情况，码C都不能纠 1 错。得到矛盾。得证。 □

引理 2.21（模型乙的限制）：C是$+q_1,-q_2,+q_3,+q_4$上的纠 1 错码。$m,\bar{m}\in\mathcal{M}_2$（$m\neq\bar{m}$）是两个不同的消息。则有$\mathrm{Enc}_3\left(\bar{m},\mathrm{CW}_2(m)\right)\neq\mathrm{CW}_3(m)$且$\mathrm{Enc}_4\left(\bar{m},\mathrm{CW}_2(m)\right)\neq\mathrm{CW}_4(m)$。 □

证明：用反证法。下面仅证明$\mathrm{Enc}_3\left(\bar{m},\mathrm{CW}_2(m)\right)\neq\mathrm{CW}_3(m)$。$\mathrm{Enc}_4\left(\bar{m},\mathrm{CW}_2(m)\right)\neq\mathrm{CW}_4(m)$的证明方法相同，从略。

反设消息m和$\bar{m}$使得$\mathrm{Enc}_3\left(\bar{m},\mathrm{CW}_2(m)\right)=\mathrm{CW}_3(m)$。记$c_4^{\times}\triangleq\mathrm{Enc}_4\left(\bar{m},\mathrm{CW}_2(m)\right)$。考虑以下两种情况：

(情况 1) 译码器满足 $\mathrm{Dec}\left(\mathrm{CW}_1(m),\mathrm{CW}_3(m),c_4^{\times}\right)\neq m$。这时考虑 $M=m$，$Y^3=X^3$，$Y_4=c_4^{\times}$。则有 $\hat{M}=\mathrm{Dec}\left(\mathrm{CW}_1(m),\mathrm{CW}_2(m),c_4^{\times}\right)\neq m$。所以 $d_H\left(X^4,Y^4\right)\leq 1$ 且 $\hat{M}\neq M$。码 C 不能纠 1 错；

(情况 2) 译码器满足 $\mathrm{Dec}\left(\mathrm{CW}_1(m),\mathrm{CW}_3(m),c_4^{\times}\right)=m$。这时考虑 $M=\bar{m}$，$Y_1=\mathrm{CW}_1(m)$，$Y_{[2:4]}=X_{[2:4]}$。则有 $Y_2=X_2=\mathrm{CW}_2(m)$，$Y_3=X_3=\mathrm{Enc}_3\left(\bar{m},\mathrm{CW}_2(m)\right)=\mathrm{CW}_3(m)$，$Y_4=X_4=\mathrm{Enc}_4\left(\bar{m},\mathrm{CW}_2(m)\right)=c_4^{\times}$。$\hat{M}=\mathrm{Dec}\left(\mathrm{CW}_1(m),\mathrm{CW}_3(m),c_4^{\times}\right)=m$。所以 $d_H\left(X^4,Y^4\right)\leq 1$ 且 $\hat{M}\neq M$。码 C 不能纠 1 错。

以上两种情况，码 C 都不能纠 1 错。得到矛盾。这样就证明了 $\mathrm{Enc}_3\left(\bar{m},\mathrm{CW}_2(m)\right)\neq\mathrm{CW}_3(m)$。 □

引理 2.22（模型乙上界）：$A^{(1,1)}_{+q_1,-q_2,+q_3,+q_4}\leq q_2(q_3-1)$ 且 $A^{(1,1)}_{+q_1,-q_2,+q_3,+q_4}\leq q_2(q_4-1)$。

□

证明：用反证法。下面仅证明 $A^{(1,1)}_{+q_1,-q_2,+q_3,+q_4}\leq q_2(q_3-1)$。$A^{(1,1)}_{+q_1,-q_2,+q_3,+q_4}\leq q_2(q_4-1)$ 的证法类似，从略。

反设存在纠 1 错的码 C，其消息集大小 $>q_2(q_3-1)$。根据抽屉原理，$\exists\theta\in\mathcal{Q}_2$ 使得 $\left|\mathcal{M}_2(\theta)\right|=q_3$。再考虑到引理 2.20，有

$$\left\{\mathrm{CW}_3(m):m\in\mathcal{M}_2(\theta)\right\}=[0:q_3). \tag{2–31}$$

固定 $\bar{m}\in\mathcal{M}\setminus\mathcal{M}_2(\theta)$，记 $c_3=\mathrm{Enc}_3(\bar{m},\theta)$。由于式（2–31），所以 $\exists m\in\mathcal{M}_2(\theta)$ 使得 $\mathrm{CW}_3(m)=c_3$，进而 $\mathrm{Enc}_3(\bar{m},\theta)=\mathrm{CW}_3(m)$。这与引理 2.21 矛盾。命题得证。

□

引理 2.23（模型乙）：C 是 $+q_1,-q_2,+q_3,+q_4$ 上的纠 1 错码。$m,\bar{m}\in\mathcal{M}_2$（$m\neq\bar{m}$）是两个不同的消息。$\forall y_1\in\mathcal{Q}_1$，有 $\mathrm{Enc}_3\left(m,\mathrm{Enc}_1(y_1)\right)\neq\mathrm{Enc}_3\left(\bar{m},\mathrm{Enc}_1(y_1)\right)$ 或 $\mathrm{Enc}_3\left(m,\mathrm{Enc}_1(y_1)\right)\neq\mathrm{Enc}_3\left(\bar{m},\mathrm{Enc}_1(y_1)\right)$。 □

证明：用反证法。反设 $\exists y_1\in\mathcal{Q}_1$，$y_2=\mathrm{Enc}_2(y_1)$，使得 $\mathrm{Enc}_3(m,y_2)=\mathrm{Enc}_3(\bar{m},y_2)$ 且 $\mathrm{Enc}_4(m,y_2)=\mathrm{Enc}_4(\bar{m},y_2)$。考虑以下两种情况：

(1) 译码器满足 $\mathrm{Dec}\left(y_1,\mathrm{Enc}_3(m,y_2),\mathrm{Enc}_4(m,y_2)\right)\neq m$。这时考虑 $M=m$，$Y_1=y_1$，$Y_{[2:4]}=X_{[2:4]}$，则有 $\hat{M}=\mathrm{Dec}\left(y_1,\mathrm{Enc}_3(m,y_2),\mathrm{Enc}_4(m,y_2)\right)\neq m$。由于 $d_H\left(X^4,Y^4\right)\leq 1$ 且 $\hat{M}\neq M$，所以码 C 不能纠 1 错。

(情况 2) 译码器满足 $\mathrm{Dec}\left(y_1,\mathrm{Enc}_3(m,y_2),\mathrm{Enc}_4(m,y_2)\right)=m$。这时考虑 $M=\bar{m}$，$Y_1=y_1$，$Y_{[2:4]}=X_{[2:4]}$，则有 $Y_3=X_3=\mathrm{Enc}_3(\bar{m},y_2)=\mathrm{Enc}_3(m,y_2)$，

$Y_4 = X_4 = \mathrm{Enc}_4(\bar{m}, y_2) = \mathrm{Enc}_4(m, y_2)$，$\hat{M} = \mathrm{Dec}(y_1, \mathrm{Enc}_3(m, y_2), \mathrm{Enc}_4(m, y_2)) = m$。由于 $d_H(X^4, Y^4) \le 1$ 且 $\hat{M} \ne M$，所以码 C 不能纠 1 错。

以上两种情况码 C 均不能纠 1 错。矛盾。命题得证。 □

引理 2.24（模型乙上界）：

$$A^{(1,1)}_{+q_1,-q_2,+q_3,+q_4} \le \min_{k=1,2,\cdots} \left\{ \max\left\{ (k-1)q_2, (q_3-k)(q_4-k)+k \right\} \right\}.$$ □

证明：固定 $k \in [1:+\infty)$。

(情况 1) $k < \max\limits_{y_2 \in \mathcal{Q}_2} |\mathcal{M}_2(y_2)|$。这时

$$|\mathcal{M}| \le \sum_{y_2 \in \mathcal{Q}_2} |\mathcal{M}_2(y_2)| = \max_{y_2 \in \mathcal{Q}_2} |\mathcal{M}_2(y_2)| \cdot q_2 = (k-1)q_2.$$

(情况 2) $k \ge \max\limits_{y_2 \in \mathcal{Q}_2} |\mathcal{M}_2(y_2)|$。这时 $\exists c_2 \in \mathcal{Q}_2$ 使得 $|\mathcal{M}_2(c_2)| \ge k$。考虑 $\mathcal{M}_2(c_2)$ 的某个大小为 k 的子集 $\mathcal{M}'$。由引理 2.20 可知 $\left|\left\{\mathrm{CW}_3(m') : m' \in \mathcal{M}'\right\}\right| = k$，$\left|\left\{\mathrm{CW}_4(m') : m' \in \mathcal{M}'\right\}\right| = k$。由引理 2.21 可知 $\left|\mathrm{CW}_3(m) : m \in \mathcal{M} \setminus \mathcal{M}'\right| \le q_3 - k$，$\left|\mathrm{CW}_4(m) : m \in \mathcal{M} \setminus \mathcal{M}'\right| \le q_4 - k$。由引理 2.23 可知 $|\mathcal{M} \setminus \mathcal{M}'| \le (q_3-k)(q_4-k)$。所以 $|\mathcal{M}| \le (q_3-k)(q_4-k)+k$。

同时考虑以上两种情况，有 $|\mathcal{M}| \le \max\left\{(k-1)q_2, (q_3-k)(q_4-k)+k\right\}$。得证。

□

证明（定理 2.2 模型乙部分）：由引理 2.18 和引理 2.19 可得下界。由引理 2.22 和引理 2.24 可得上界。 □

这样就完成了定理 2.2 模型乙部分的证明。至此，定理 2.2 证毕。

2.5.3 两个数值例子

如前所述，我们将要给出两个上下界不紧的例子：$A^{(1,1)}_{+5,+5,-3,+2}$ 和 $A^{(1,1)}_{+6,-2,+5,+5}$。如前所述，定理 2.2 并不能完全确定出这两个值。但是我们还是有其他的手段来求得这两个值。

首先我们来证明 $A^{(1,1)}_{+5,+5,-3,+2} = 4$。

引理 2.25（模型甲中 $q_3 = 3$，$q_4 = 2$）：$A^{(1,1)}_{+q_1,+q_2,-3,+2} \le 4$. □

证明：用反证法。存在纠 1 错的码 C，其消息集大小 A 满足 $A > 4$。

不妨设 $\mathrm{Enc}_1(M) \triangleq M$，$\mathrm{Enc}_2(M) \triangleq M$。

考虑 $y_1, y_2 \in \mathcal{M}$。当 $y_1 \neq y_2$ 时，考虑 $\mathrm{Dec}(y_1, y_2, y_4)$（$y_4 \in \{0,1\}$），它对于不同的 y_4，有的时候要输出 y_1，有的时候要输出 y_2。由于 y_4 只能在 $\{0,1\}$ 中选，只有两种可能，所以不妨设 $\mathrm{Dec}(y_1, y_2, 0) = y_1$，$\mathrm{Dec}(y_1, y_2, 1) = y_2$。

$\forall m \in \mathcal{M}$，定义

$$\Theta_1(m) \triangleq \{\mathrm{Enc}_3(m, y_2) : y_2 \in \mathcal{M} \setminus \{m\}\}, \tag{2–32}$$

$$\Theta_2(m) \triangleq \{\mathrm{Enc}_3(m, y_2) : y_2 \in \mathcal{M} \setminus \{m\}\}. \tag{2–33}$$

可以证明，$\Theta_1(m) \bigcap \Theta_2(m) = \varnothing$。（证法如下：用反证法，反设 $\exists y_1, y_2 \in \mathcal{M} \setminus \{m\}$，$y_3 \in \mathcal{Q}_3$ 使得 $\mathrm{Enc}_3(y_1, m) = \mathrm{Enc}_3(m, y_2) = y_3$。考虑两种情况：(情况 1) $\mathrm{Enc}_4(m, y_3) = 0$。这时当 $M = m$，$Y_1 = X_1$，$Y_2 = y_2$，$Y_{[3:4]} = X_{[3:4]}$ 时 $\hat{M} = y_2$；(情况 2) $\mathrm{Enc}_4(m, y_3) = 1$。这时当 $M = m$，$Y_1 = y_1$，$Y_{[2:4]} = X_{[2:4]}$ 时 $\hat{M} = y_1$。得到矛盾。）另外注意到 $|\Theta_1(m)| + |\Theta_2(m)| \leq q_3 = 3$，由抽屉原理可知 $|\Theta_1(m)| = 1$ 或 $|\Theta_2(m)| = 1$。

记 $\Sigma_1 \triangleq \{m \in [0:A) : |\Theta_1(m)| = 1\}$，$\Sigma_2 \triangleq \{m \in [0:A) : |\Theta_2(m)| = 1\}$。则有 $|\Sigma_1| + |\Sigma_2| = A$。因为假设 $A > 4$，由抽屉原理知必有 $|\Sigma_1| > 2$ 或 $|\Sigma_2| > 2$。不妨设 $\Sigma_1 \triangleq \{0,1,2\}$。

对任意 $m \in \Sigma_1$，定义 $\theta_1(m) \in \mathcal{Q}_3$ 使得 $\Theta_1(m) = \{\theta_1(m)\}$。

则有 $\mathrm{Enc}_4(m, \theta_1(m)) = 1$ 且 $\forall \bar{m} \neq m$，$\mathrm{Enc}_4(\bar{m}, \theta_1(m)) = 0$。所以，$(\theta_1(m) : m \in \Sigma_1)$ 两两不等。

在之前 $\Sigma_1 = \{0,1,2\}$ 的基础上，不妨再设 $\theta_1(m) = m$（$m \in \Sigma_1$）。所以，对于 $\tilde{m} \notin \mathcal{M} \setminus \Sigma_1$，有 $\forall y_2 \in \mathcal{Q}_2$，都会导致 $X_4 \equiv 0$。所以当 $Y_2 = \tilde{m}$ 时不能译出 $\tilde{m}$，译码错误。

这样我们就证明了码 C 不能纠 1 错，得到矛盾。得证。 □

命题 2.2：$A^{(1,1)}_{+5,+5,-3,+2} = 4$. □

证明：由定理 2.2 可得 $4 \leq A^{(1,1)}_{+5,+5,-3,+2} \leq 5$。引理 2.25 说明 $A^{(1,1)}_{+5,+5,-3,+2} \leq 4$。所以 $A^{(1,1)}_{+5,+5,-3,+2} = 4$。 □

下面来证明 $A^{(1,1)}_{+6,-2,+5,+5} = 5$。

引理 2.26（模型乙 $q_2 = 2$）：$A^{(1,1)}_{+q_1,-2,+q_3,+q_4}$ 小于下列优化问题的最优值：

$$
\begin{array}{ll}
\text{maximize} & \mu_2(0)+\mu_2(1) \\
\text{over} & \mu_2(0),\mu_2(1),\lambda_3,\lambda_4,\lambda_{34} \\
\text{s.t.} & \lambda_{34}=\big(q_3-\mu_2(0)\big)\big(q_4-\mu_2(0)\big)-\mu_2(1) \\
 & \lambda_3\lambda_4\geq\lambda_{34}\geq 0 \\
 & A-\lambda_{34}\leq q_3-\lambda_3 \\
 & A-\lambda_{34}\leq q_4-\lambda_4.
\end{array}
$$

□

证明：考虑某纠 1 错的码 C。设其消息集大小为 A。显然有 $A\leq q_1$。

不妨设 $\mathrm{Enc}_1(M)\triangleq M$。$\forall y_2\in\{0,1\}$ 定义 $\mu_2(y_2)\triangleq\big|\mathcal{M}_2(y_2)\big|$。显然有 $A=\mu_2(0)+\mu_2(1)$。

由于 $\mathcal{Q}_2=\{0,1\}$，所以可以不妨假设

$$
\mathrm{Enc}_2(Y_1)\triangleq\begin{cases}0, & Y_1\in\big[0:\mu_2(0)\big)\\ 1, & Y_1\in\big[\mu_2(0):\mu_2(0)+A\big)\\ \text{不关心}, & \text{其他}.\end{cases}
\tag{2–34}
$$

引理 2.20 证明了，任给两个不同的消息 $m,\bar{m}\in\mathcal{M}_2(0)$，有 $\mathrm{Enc}_3(m,0)\neq\mathrm{Enc}_3(\bar{m},0)$。所以，不妨假设 $\forall m\in\mathcal{M}_2(0)$ 有 $\mathrm{Enc}_3(m,0)=m$。同理，可假设 $\forall m\in\mathcal{M}_2(0)$ 有 $\mathrm{Enc}_4(m,0)=m$。

由于引理 2.21，$\forall\bar{m}\in\mathcal{M}_2(1)$，有 $\mathrm{Enc}_3(\bar{m},0)\notin\big[0:\mu_2(0)\big)$ 且 $\mathrm{Enc}_4(0,\bar{m})\notin\big[0:\mu_2(0)\big)$。所以

$$
\Big\{\mathrm{Enc}_{[3:4]}(m,0):m\in\mathcal{M}_2(1)\Big\}\subseteq\big[\mu_2(0):q_3\big)\times\big[\mu_2(0):q_4\big).
$$

另外，引理 2.23 证明了对于 $\forall\bar{m},\tilde{m}\in\mathcal{M}_2(1)$，$\mathrm{Enc}_3(\bar{m},0)\neq\mathrm{Enc}_3(\tilde{m},0)$ 或 $\mathrm{Enc}_4(\bar{m},0)\neq\mathrm{Enc}_4(\tilde{m},0)$。所以

$$
\mu_2(1)=\Big|\Big\{\mathrm{Enc}_{[3:4]}(m,0):m\in\mathcal{M}_2(1)\Big\}\Big|,
\tag{2–35}
$$

进而

$$
\mu_2(1)\leq\big(q_3-\mu_2(0)\big)\big(q_4-\mu_2(0)\big).
\tag{2–36}
$$

定义 $\lambda_{34}\triangleq\big(q_3-\mu_2(0)\big)\big(q_4-\mu_2(0)\big)-\mu_2(1)$。显然有 $\lambda_{34}\geq 0$。

定义

$$
\begin{aligned}
\Lambda_{34}&\triangleq\big[\mu_2(0):q_3\big)\times\big[\mu_2(0):q_4\big)\setminus\Big\{\mathrm{Enc}_{[3:4]}(m,0):m\in\mathcal{M}_2(1)\Big\}\\
\lambda_3&\triangleq\Big|\Big\{y_3\in\big[\mu_2(0):q_3\big):\exists(y_3,y_4)\in\Lambda_{34}\Big\}\Big|\\
\lambda_4&\triangleq\Big|\Big\{y_4\in\big[\mu_2(0):q_4\big):\exists(y_3,y_4)\in\Lambda_{34}\Big\}\Big|,
\end{aligned}
$$

显然有 $\lambda_3\lambda_4 \geq |\Lambda_{34}| = \lambda_{34}$。

可以证明，$\forall m \in \mathcal{M}_2(0)$，$\mathrm{Enc}_{[3:4]}(m,1) = (m,m)$ 或 $\mathrm{Enc}_{[3:4]}(m,1) \in \Lambda_{34}$。所以，

$$\begin{aligned}
&\left|\left\{\mathrm{Enc}_3(m,1): m \in \mathcal{M}_2(0)\right\}\right| \\
&= \left|\left\{\mathrm{Enc}_3(m,1): m \in \mathcal{M}_2(0)\right\} \setminus \Lambda_{34}\right| + \left|\left\{\mathrm{Enc}_3(m,1): m \in \mathcal{M}_2(0)\right\} \cap \Lambda_{34}\right| \\
&= \left(\mu_2(0) - \lambda_{34}\right) + \lambda_3.
\end{aligned}$$

另外根据定义有

$$\mu_2(1) = \left|\mathcal{M}_2(1)\right| = \left|\left\{\mathrm{Enc}_3(m',1): m' \in \mathcal{M}_2(y_2')\right\}\right|, \tag{2–37}$$

所以

$$\begin{aligned}
&A - \lambda_{34} + \lambda_3 \\
&= \left(\mu_2(0) - \lambda_{34} + \lambda_3\right) + \mu_2(1) \\
&= \left|\left\{\mathrm{Enc}_3(m,1): m \in \mathcal{M}_2(0)\right\}\right| + \left|\left\{\mathrm{Enc}_3(m',1): m' \in \mathcal{M}_2(1)\right\}\right|.
\end{aligned} \tag{2–38}$$

考虑到引理 2.21 说

$$\left\{\mathrm{Enc}_3(m,1): m \in \mathcal{M}_2(0)\right\} \cap \left\{\mathrm{Enc}_3(m',1): m' \in \mathcal{M}_2(1)\right\} = \varnothing, \tag{2–39}$$

所以

$$\begin{aligned}
&\left|\left\{\mathrm{Enc}_3(m,1): m \in \mathcal{M}_2(0)\right\}\right| + \left|\left\{\mathrm{Enc}_3(m',1): m' \in \mathcal{M}_2(1)\right\}\right| \\
&= \left|\left\{\mathrm{Enc}_3(m,1): m \in \mathcal{M}_2(0)\right\} \cup \left\{\mathrm{Enc}_3(m',1): m' \in \mathcal{M}_2(1)\right\}\right| \\
&\leq \left|\left\{\mathrm{Enc}_3(m,1): m \in \mathcal{M}\right\}\right| \\
&\leq q_3.
\end{aligned} \tag{2–40}$$

由（2–38）式和（2–40）式可以推得

$$A - \lambda_{34} \leq q_3 - \lambda_3. \tag{2–41}$$

同理，$A - \lambda_{34} \leq q_4 - \lambda_4$。

这样就完成了命题的证明。 □

命题 2.3： $A^{(1,1)}_{+6,-2,+5,+5} = 5$。 □

证明： 由定理 2.2 知 $5 \leq A^{(1,1)}_{+6,-2,+5,+5} \leq 6$。再考虑引理 2.26，对数值进行穷举，可以发现 6 不可达。所以 $A^{(1,1)}_{+6,-2,+5,+5} = 5$。 □

2.6 有限个传输交互模型的求解

2.6.1 结果

在三个交互模型和四个交互模型中的思想可以直接推广到更多个交互的情况。不幸的是，推广后的形式不是特别的简洁。

定理 2.3（检错码和纠错码）(1)

$$A_{s^n\circ q^n}^{(z,0)} \le \min_{n'\in[0:n]:\left|(n':n]_+\right|\le z} Q_{s^{n'}\circ q^{n'}}^{\left(z-\left|(n':n]_+\right|\right)} \tag{2–42}$$

$$A_{s^n\circ q^n}^{(z,z)} \le \min_{\substack{n'\in[0:n],n''\in[0:n']:2\left|(n'':n']_-\right|+\left|(n':n]_+\right|\le 2z \\ z',z''\in\left[0:z-\left|(n'':n']_-\right|\right]:z'+z''\le 2z-2\left|(n'':n']_-\right|-\left|(n':n]_+\right|}} Q_{s^{n''}\circ q^{n''}}^{(z'')} P_{s_{(n'':n']}\circ q_{(n'':n']}}^{(z')}, \tag{2–43}$$

其中

$$Q_{s_{[i_1:i_2]}\circ q_{[i_1:i_2]}}^{(z)} \triangleq \begin{cases} \prod_{i\in[i_1:i_2]_+} q_i, & z=0 \\ \min_{i_a\in[i_1:i_2]_+} \prod_{i\in[i_1:i_a)_+} q_i \cdot \min_{I^*\subseteq(i_a:i_2]:\left|I^*\right|<z} \prod_{i\in(i_a:i_2]\setminus I^*} q_i, & z>0 \end{cases}$$

$$P_{s_{[i_1:i_2]}\circ q_{[i_1:i_2]}}^{(z)} \triangleq \min_{I^*\subseteq(i_a:i_2]_+:\left|I^*\right|<z} \prod_{i\in(i_a:i_2]\setminus I^*} q_i.$$

(2) 当 $s_n q_n \ge +2$ 时，

$$A_{s^n\circ q^n}^{(z,0)} \ge \max_{n'\in[1:n]} \min\left\{ A_{s^{n'}\circ q^{n'}}^{(z-1,0)}, \max\left\{ \prod_{i\in(n':n]_+} q_i, \prod_{i\in(n':n)_-} q_i \right\} \right\};$$

(3)
$$A_{s^n\circ q^n}^{(z,z)} \ge \max_{0=n_0<n_1<n_2<\cdots<n_z<n_{z+1}=n} \min_{0\le i\le z} A_{s_{(n_i:n_{i+1}]}\circ q_{(n_i:n_{i+1}]}}^{(z-i,0)}. \qquad \square$$

定理 2.3 对一般的有限个交互模型下检 z 错码的最大消息集大小 $A_{s^n\circ q^n}^{(z,0)}$ 和纠 z 错码的最大消息集大小 $A_{s^n\circ q^n}^{(z,z)}$ 进行了刻画，得到了它们的上界和下界。虽然上界和下界并不总是相等，即定理 2.3 并没有在一般的情况下完全确定出 $A_{s^n\circ q^n}^{(z,z)}$ 和 $A_{s^n\circ q^n}^{(z,0)}$ 的值，但是还是能够求得很多情况下 $A_{s^n\circ q^n}^{(z,z)}$ 和 $A_{s^n\circ q^n}^{(z,0)}$ 的值。

例 2.1：使用定理 2.3 可立即得到 $A_{+2,+3,-6,+2}^{(1,0)}=6$，$A_{+2,+2,-4,+2,-4,+3}^{(1,1)}=4$。 $\square$

在例 2.1 中，通过直接使用定理 2.3，就得到了 $A_{+2,+3,-6,+2}^{(1,0)}$ 和 $A_{+2,+2,-4,+2,-4,+3}^{(1,1)}$ 的值，体现了定理 2.3 的刻画能力。

2.6.2 定理证明

本节证明定理 2.3。先考虑定理 2.3 中第 (1) 部分，即上界的证明。

引理 2.27（检错上界）：考虑 $s^n\circ q^n$。$n'\in[0:n]$ 和 $\varnothing\ne I_a\subseteq[1:n']$ 满足

(1) $\left|I_a\right|+\left|\left(n':n\right]_+\right|\le z$，

(2) $s_{i_a}=+1$，其中 $i_a\triangleq\min_{i\in I_a} i$。则 $s^n\circ q^n$ 上检 z 个错的码最大消息集大小

$$A^{(z,0)}_{s^n\circ q^n}\le\prod_{i\in I_{\mathrm{EQ}}} q_i\,, \tag{2–44}$$

其中 $I_{\mathrm{EQ}}\triangleq\left[1:i_a\right)_+\cup\left(\left[i_a:n'\right]\setminus I_a\right)$。 □

证明：用反证法。假设在 $s^n\circ q^n$ 上存在码 C，其消息集大小大于 $\prod_{i\in I_{\mathrm{EQ}}} q_i$。根据抽屉原理，$\exists m,\bar m\in\mathcal{M}$（$m\ne\bar m$）使得 $\mathrm{CW}_{I_{\mathrm{EQ}}}\left(m\right)=\mathrm{CW}_{I_{\mathrm{EQ}}}\left(\bar m\right)$。令 $c^n=\mathrm{CW}^n\left(m\right)$，$\bar c^n=\mathrm{CW}^n\left(\bar m\right)$。因为 $c_+^{i_a-1}=\bar c_+^{i_a-1}$，所以 $\mathrm{Enc}_-^{i_a-1}$ 的输入都是一样的，所以进而有 $c^{i_a-1}=\bar c^{i_a-1}$。所以 $\forall i\notin I_a\cup\left(n':n\right]_+$，均有 $c_i=\bar c_i$。所以

$$d_H\left(c^{n'},\bar c^{n'}\right)+\left|\left(n':n\right]_+\right|\le\left|I_a\right|+\left|\left(n':n\right]_+\right|\le z\,.$$

根据引理 2.3，这个码不能检 z 个错，得出矛盾。这样我们就证明了所有的检 z 个错的码的大小都 $\le\prod_{i\in I_{\mathrm{EQ}}} q_i$。 □

引理 2.28（纠错上界）：考虑 $s^n\circ q^n$。$n'\in\left[0:n\right]$，$n''\in\left[0:n'\right]$，$\varnothing\ne I_a\subseteq\left[1:n'\right]$ 和 $\bar I_a\subseteq\left[n'':n'\right]$满足

(1) $\left|I_a\right|\le z$，$\left|\bar I_a\right|\le z$，且 $\left|I_a\right|+\left|\bar I_a\right|+\left|\left(n':n\right]_+\right|\le 2z$；

(2) $I_a\bigcap\left(n'':n'\right]=\left(n'':n'\right]_-$ 且 $\left(n'':n'\right]_-\subseteq\bar I_a$；

(3) $i_a\le n''$ 且 $s_{i_a}=+1$，其中 $i_a\triangleq\min_{i\in I_a} i$。

则 $s^n\circ q^n$ 上纠 z 个错的码最大消息集大小

$$A^{(z,0)}_{s^n\circ q^n}\le\prod_{i\in I_{\mathrm{EQ}}} q_i\,, \tag{2–45}$$

其中 $I_{\mathrm{EQ}}\triangleq\left[1:i_a\right)_+\cup\left(\left[i_a:n'\right]\setminus I_a\setminus\bar I_a\right)$。 □

证明：用反证法。假设在 $s^n\circ q^n$ 上存在码 C，其消息集大小大于 $\prod_{i\in I_{\mathrm{EQ}}} q_i$。根据抽屉原理，$\exists m,\bar m\in\mathcal{M}$（$m\ne\bar m$）使得 $\mathrm{CW}_{I_{\mathrm{EQ}}}\left(m\right)=\mathrm{CW}_{I_{\mathrm{EQ}}}\left(\bar m\right)$。令 $c^n=\mathrm{CW}^n\left(m\right)$，$\bar c^n=\mathrm{CW}^n\left(\bar m\right)$。因为 $c_+^{i_a-1}=\bar c_+^{i_a-1}$，所以 $\mathrm{Enc}_-^{i_a-1}$ 的输入都是一样的，所以进而有 $c^{i_a-1}=\bar c^{i_a-1}$。所以 $\forall i\notin I_a\cup\bar I_a\cup\left(n':n\right]_+$，均有 $c_i=\bar c_i$。所以

$$d_H\left(c^{n'},\bar c^{n'}\right)+\left|\left(n':n\right]_+\right|\le\left|I_a\right|+\left|\bar I_a\right|+\left|\left(n':n\right]_+\right|\le 2z\,. \tag{2–46}$$

根据引理 2.5，这个码不能纠 z 个错，得出矛盾。这样，我们就证明了所有的纠 z 个错的码的大小都 $\le \prod_{i\in I_{\mathrm{EQ}}} q_i$ 。 □

接着考虑下界的证明。

引理 2.29（构造检 z 错码）：考虑 $s^n \circ q^n$ 。A 是一个正整数。若存在 $n' \in [1:n]$ 使得 $A^{(z-1,0)}_{s^{n'}\circ q^{n'}} \ge A$，$\prod_{i\in(n':n]_+} q_i \ge A$，则在 $s^n \circ q^n$ 上存在消息集大小为 A 的检 z 错码。 □

构造码 C：（编码器）(1) 在 $s^{n'} \circ q^{n'}$ 处使用消息集大小为 A 的检 $(z-1)$ 错的码 C'；(2) 在 $q_{(n':n]_+}$ 处将消息再发一遍，记为码 C''。

（译码器）先查看码 C' 收到的部分是否检测到错误。如果检测到错误，那么译码器输出 ε；如果没有检测到错误，则译码器比较 C' 和 C'' 的译码结果（分别记为 $\hat{M}'$ 和 $\hat{M}''$）。如果 $\hat{M}' = \hat{M}''$，则译码器输出 $\hat{M}'$；否则译码器输出 ε。

证明码 C 可检 z 错：(1) 当 $d_H\left(X^n, Y^n\right) \le z$ 时，考虑以下情况。

(情况 1) $\hat{M}' = M$。由于 $\hat{M} = \hat{M}'$ 或 $\hat{M} = \varepsilon$，故 $\hat{M} = M$ 或 $\hat{M} = \varepsilon$；

(情况 2) $\hat{M}' = \varepsilon$。这时 $\hat{M} = \varepsilon$。

(情况 3) $\hat{M}' \ne M$ 且 $\hat{M}' \ne \varepsilon$。这时，这时 $d_H\left(X^{n'}, Y^{n'}\right) > z-1$，所以 $X_{(n':n]} = Y_{(n':n]}$，进而 $\hat{M}'' = M$。进一步的，$\hat{M}' \ne \hat{M}''$。所以 $\hat{M} = \varepsilon$。

以上三种情况均有 $\hat{M} = M$ 或 $\hat{M} = \varepsilon$。

(2) 当 $X^n = Y^n$ 时，因为码 C' 能检 $(z-1)$ 错，所以 $\hat{M}' = M$。另外 $\hat{M}'' = M$，所以 $\hat{M} = M$。

综上两点，根据检 z 错码的定义，C 可以检 z 个错。 □

引理 2.30（构造检 z 错码）：考虑 $s^n \circ q^n$ 。$A, A' \in \mathbb{N}$ 满足 $1 \le A' \le A$。若存在 $n' \in [1:n]$，$n'' \in [n':n]$ 使得 $A^{(z-1,0)}_{s^{n'}\circ q^{n'}} \ge A$，$\prod_{i\in(n':n'']_-} q_i \ge \frac{A}{A'}$，$\prod_{i\in(n'':n]_+} q_i \ge A'+1$，则在 $s^n \circ q^n$ 上存在消息集大小为 A 的检 z 错码。 □

构造码 C：（编码器）(1) 因为 $A^{(z-1,0)}_{s^{n'}\circ q^{n'}} \ge A$，所以在 $s^{n'} \circ q^{n'}$ 上采用消息集大小为 A 的检 $(z-1)$ 错的码 C'。在 $s^{n'} \circ q^{n'}$ 上的编码器使用码 C' 的编码器。(2) 在 $q_{(n':n'']_-}$ 上，目的节点可以得到 C' 的译码结果 $\hat{M}'$。如果 $\hat{M}' \ne \varepsilon$，编码器 $\mathrm{Enc}_{(n':n'']_-}$ 直接将 $\left\lfloor \frac{\hat{M}'}{A'} \right\rfloor$ 发回给源节点。这部分记为 C''。(3) 在 $q_{(n'':n]_+}$ 上，$\prod_{i\in(n'':n]_+} q_i \ge A'+1$，所以源

节点可以传输$[0:A')\cup\{\varepsilon\}$中的一个符号。源节点首先判断C″是否正确传输了组号。如果正确传输，源节点再发送$M \bmod A'$；否则发送ε。这部分记为C‴。

（译码器）若$\hat{M}'=\varepsilon$或$\hat{M}'''=\varepsilon$或$\hat{M}' \bmod A' \neq \hat{M}'''$，则$\hat{M}=\varepsilon$。否则$\hat{M}=\hat{M}'$。

证明码C可检z错：(1) 当$d_H\left(X^n,Y^n\right)\leq z$时，考虑以下情况。

(情况 1) $\hat{M}'=M$。由于$\hat{M}=\hat{M}'$或$\hat{M}=\varepsilon$，故$\hat{M}=M$或$\hat{M}=\varepsilon$；

(情况 2) $\hat{M}'=\varepsilon$。这时$\hat{M}=\varepsilon$。

(情况 3) $\hat{M}'\neq M$且$\hat{M}'\neq\varepsilon$。这时$d_H\left(X^{n'},Y^{n'}\right)>z-1$，所以$X_{(n':n]}=Y_{(n':n]}$。由于$\hat{M}'\neq M$且$\hat{M}'\neq\varepsilon$，必有$\hat{M}''\neq\left\lfloor\frac{M}{A'}\right\rfloor$或$\hat{M}'''\neq M \bmod A'$。进一步，有$\hat{M}=\varepsilon$。

以上三种情况均有$\hat{M}=M$或$\hat{M}=\varepsilon$。

(2) 当$X^n=Y^n$时，因为码C′能检$(z-1)$错，所以$\hat{M}'=M$。另外$\hat{M}''=\left\lfloor\frac{M}{A'}\right\rfloor$和$\hat{M}'''=M \bmod A'$，所以$\hat{M}=M$。

综上两点，根据检z错码的定义，C可以检z个错。 □

引理 2.31（构造检z错码）：考虑$s^n\circ q^n$满足$s_n q_n\geq+2$。$A\in\mathbb{N}$。若存在$n'\in[1:n]$使得$A^{(z-1,0)}_{s^{n'}\circ q^{n'}}\geq A$且$\prod_{i\in(n':n)_-}q_i\geq A$，则在$s^n\circ q^n$上存在消息集大小为$A$的检$z$错码。

证明：令$A'=1$，$n''=n-1$。现在验证引理 2.30 的条件。由于$\prod_{i\in(n':n)_-}q_i\geq A$且$(n':n)=(n':n'']$，所以$\prod_{i\in(n':n'']_-}q_i\geq\frac{A}{A'}$。由于$s_n q_n\geq+2$，所以$\prod_{i\in(n':n]_+}q_i\geq 2$。于是引理 2.30 的条件均满足，命题成立。 □

引理 2.32（构造纠z错码）：考虑$s^n\circ q^n$。$A\in\mathbb{N}$。若存在$n'\in[1:n]$使得$A^{(z-1,0)}_{s^{n'}\circ q^{n'}}\geq A$且$A^{(z-1,z-1)}_{s_{(n':n]}\circ q_{(n':n]}}\geq A$，则存在消息集大小为$M$的检$z$错码。 □

证明：在引理 2.10 中，取$A'=A$，$n'=n''$即得。 □

引理 2.33（纠z错下界）考虑$s^n\circ q^n$上的一个分划$0=n_0<n_1<n_2<\cdots<n_z<n_{z+1}=n$。$A$是一个正整数，且满足对$i\in[0:z]$均有$A^{(z-i,0)}_{s_{(n_i:n_{i+1}]}\circ q_{(n_i:n_{i+1}]}}\geq A$。则$A^{(z,z)}_{s^n\circ q^n}\geq A$。 □

证明：下面用数学归纳法证明对 $j\in[0:z]$，有 $A^{(j,j)}_{s_{(n_{z-j}:n]}\circ q_{(n_{z-j}:n]}}\geq A$。

(初始条件) 对于 $j=0$，

$$A^{(j,j)}_{s_{(n_{z-j}:n]}\circ q_{(n_{z-j}:n]}}\Big|_{j=0}=A^{(z-i,0)}_{s_{(n_i:n_{i+1}]}\circ q_{(n_i:n_{i+1}]}}\Big|_{i=z}\geq A. \tag{2–47}$$

所以，在 $(n_z:n]$ 上存在码 C_0。

(递推关系) 设已经对某个 $j\in[0:z)$ 证明了 $A^{(j,j)}_{s_{(n_{z-j}:n]}\circ q_{(n_{z-j}:n]}}\geq A$，即在 $s_{(n_{z-j}:n]}\circ q_{(n_{z-j}:n]}$ 上存在消息集大小为 A 的纠 j 错的码 C_j。

下面要证 $A^{(j+1,j+1)}_{s_{(n_{z-j-1}:n]}\circ q_{(n_{z-j-1}:n]}}\geq A$，即在 $s_{(n_{z-j-1}:n]}\circ q_{(n_{z-j-1}:n]}$ 在存在消息集大小为 A 的纠 $j+1$ 错的码 C_{j+1}。

在 $s_{(n_{z-j}:n]}\circ q_{(n_{z-j}:n]}$ 上使用码 C_j。在 $s_{(n_{z-j-1}:n_{z-j}]}\circ q_{(n_{z-j-1}:n_{z-j}]}$ 上我们知道

$$A^{(j,0)}_{s_{(n_{z-j-1}:n_{z-j}]}\circ q_{(n_{z-j-1}:n_{z-j}]}}=A^{(z-i,0)}_{s_{(n_i:n_{i+1}]}\circ q_{(n_i:n_{i+1}]}}\Big|_{i=n-z}\geq A, \tag{2–48}$$

所以存在检 j 错的码 C'_j。根据引理 2.32，存在纠 $(j+1)$ 错的码 C_{j+1}。递推关系得证。

在递推关系中取 $j=z$ 可完成证明。 □

定理 2.3 的证明：(1) 由引理 2.27 和引理 2.28 可得。

(2) 任取 $n'\in[1:n]$，定义

$$A_{n'}\triangleq\min\left\{A^{(z-1,0)}_{s^{n'}\circ q^{n'}},\max\left\{\prod_{i\in(n':n]_+}q_i,\prod_{i\in(n':n)_-}q_i\right\}\right\}.$$

显然，有 $A^{(z-1,0)}_{s^{n'}\circ q^{n'}}\geq A_{n'}$，并且 $\prod_{i\in(n':n]_+}q_i\geq A_{n'}$ 或 $\prod_{i\in(n':n)_-}q_i\geq A_{n'}$。分类讨论：

(情况 1) $\prod_{i\in(n':n]_+}q_i\geq A_{n'}$。这时满足了引理 2.29 的条件，存在消息集大小为 $A_{n'}$ 的检 z 错码；

(情况 2) $\prod_{i\in(n':n)_-}q_i\geq A_{n'}$。这时满足了引理 2.31 的条件，存在消息集大小为 $A_{n'}$ 的检 z 错码。

综合考虑以上两种情况，均存在消息集大小为 $A_{n'}$ 的检 z 错码。所以 $A^{(z,0)}_{s^n\circ q^n}\geq A_{n'}$。得证。

(3) 由引理 2.33 可得。 □

这样就完成了定理 2.3 的证明。

第 3 章　有向网络和网络纠错模型

内容提要

本章再正式重新介绍有向网络的基本概念和字母定义。这些定义将在第 4 章、第 5 章、和第 6 章用到。

● 3.1 节描述有向网络模型；

● 3.2 节介绍在有向图上网络纠错码的定义，以及网络纠错码的三大性能指标：消息速率、链路速率和纠错能力；

● 3.3 节定义有向图上的信道容量域问题和容许速率域问题。

一些符号定义

任给集合 $\mathcal{X}$ 和自然数 i，定义 $|\mathcal{X}|$ 为 $\mathcal{X}$ 中元素的个数，$\mathcal{P}(\mathcal{X}) \triangleq \{X : X \subseteq \mathcal{X}\}$，$\mathcal{P}(\mathcal{X}, i) \triangleq \{X \subseteq \mathcal{X} : |X| \le i\}$。（注：字母 $\mathcal{P}$ 不用作一元操作符或是二元操作符时可以有其他含义，比如单独使用字母 $\mathcal{P}$ 可表示有向图上路径的集合。）

对于某个序列 $\{S_x : x \in \mathcal{X}\}$，记 $S_{\mathcal{X}} \triangleq (S_x : x \in \mathcal{X})$。另外，记 $\mathbf{0}_{\mathcal{X}} \triangleq (0 : x \in \mathcal{X})$ 为有 $|\mathcal{X}|$ 个元素的全 0 列表（或向量、矩阵），$\mathbf{1}_{\mathcal{X}} \triangleq (1 : x \in \mathcal{X})$ 为有 $|\mathcal{X}|$ 个元素的全 1 列表（或向量、矩阵），$\mathbf{2}_{\mathcal{X}} \triangleq (2 : x \in \mathcal{X})$ 为有 $|\mathcal{X}|$ 个元素的全 2 列表（或向量、矩阵）。

对于向量 $\mathbf{a}_{\mathcal{X}}$，$\mathbf{a}_{\mathcal{X}} \ge \mathbf{0}_{\mathcal{X}}$ 表示对任意的 $x \in \mathcal{X}$ 均有 $a_x \ge 0$。若向量 $\mathbf{a}_{\mathcal{X}}$ 满足 $\mathbf{a}_{\mathcal{X}} \ge \mathbf{0}_{\mathcal{X}}$，则其元素 1 范数[①] $\|\mathbf{a}_{\mathcal{X}}\| \triangleq \sum_{x \in \mathcal{X}} a_x$。类似的，对于矩阵 $\mathbf{A}$，$\mathbf{A} \ge \mathbf{O}$ 表示其所有元素都非负，其中 $\mathbf{O}$ 表示全 0 矩阵。若 $\mathbf{A} \ge \mathbf{O}$，则元素 1 范数 $\|\mathbf{A}\|$ 是矩阵 $\mathbf{A}$ 各元素之和。

3.1 有向网络模型

网络用有向图 $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ 定义。其中，$\mathcal{V}$ 是节点集，$\mathcal{E}$ 是边集。节点和边统称资源。边都是有向边。图 $\mathcal{G}$ 可能有环也可能没环。两个节点间可能有重边也可能没有重边。对于某个节点 $v \in \mathcal{V}$，$\mathrm{Out}(v)$ 表示从节点 v 出发的所有有向边的集合，$\mathrm{In}(v)$ 表示以节点 v 结束的所有有向边的集合。对于某个有向边 e，$\mathrm{Tail}(e)$ 表示边 e 出发的那个节点，$\mathrm{Head}(e)$ 表示边 e 终止的那个节点。

① 在没有特别说明的情况下，本文中向量、矩阵、高阶张量的范数都是元素 1 范数。

敌对方可能控制一些资源（边或节点）。每种可能控制的节点和边称为一种组合。例如对某种组合 A，满足 $A\subseteq\mathcal{V}\cup\mathcal{E}$。在敌对方可能控制的资源受限的假定下，所有可能的组合记为 $\mathcal{A}$。

通信方可以在这个网络上有许多业务（比如单播业务、多播业务、广播业务）。通信方业务的集合记为 $\mathcal{K}$。对于某个业务 $k\in\mathcal{K}$，它会有一个源节点 $v_s^{(k)}$ 和若干个目的节点（目的节点集合记为 $\mathcal{V}_t^{(k)}$）。每个业务需要将消息从源节点传到各目的节点。一种最简单的情况是网络中只有一个单播业务，这时这个唯一的业务的源节点记为 v_s，这个唯一的业务的唯一目的节点记为 v_t。

3.2 网络纠错码的定义和性能指标

在某个网络中，可以设计许多不同的网络纠错码。但是最终在系统中只能选择一种网络纠错码来使用。值得一提的是，即使网络中有多个业务时，也只有一个码。也就是说，业务间是可以编码的。

一个网络纠错码 C 可以由信道使用次数 n（又称码长）、消息集 $\left\{\mathcal{M}^{(k)}:k\in\mathcal{K}\right\}$、编码器 $\left\{\mathrm{Enc}_e:e\in\mathcal{E}\right\}$ 和译码器 $\left\{\mathrm{Dec}_v^{(k)}:v\in\mathcal{V}_t^{(k)},k\in\mathcal{K}\right\}$ 定义。在这 n 次信道使用中，链路输入为 $X_e^n\triangleq\left(X_{e,i}:i\in[1:n]\right)$，输出为 $Y_e^n\triangleq\left(Y_{e,i}:i\in[1:n]\right)$。编码器和译码器如下：

（编码器）　$$\mathrm{Enc}_{e,i}:M^{\left(\{k\in\mathcal{K}:\mathrm{Tail}(e)=k\}\right)},Y_{\mathrm{In}(\mathrm{Tail}(e))}^{i-1}\mapsto X_{e,i},\quad e\in\mathcal{E},i\in[1:n]$$

（译码器）　$$\mathrm{Dec}_v^{(k)}:Y_{\mathrm{In}(v)}^n\mapsto\hat{M}_v^{(k)}\quad k\in\mathcal{K},v\in\mathcal{V}_t^{(k)}.$$

网络纠错码 C 有三个性能指标：

(1) 消息速率。消息速率 $R^{(k)}$ 定义为

$$R^{(k)}\triangleq\frac{1}{n}\log_2\left|\mathcal{M}^{(k)}\right|. \tag{3–1}$$

(2) 链路速率。对于某个链路 e，其链路速率为 f_e 定义为 $f_e\triangleq\log_2 q_e$，$\mathcal{Q}_e\triangleq[0:q_e)$ 是链路上的每次信道使用时符号可能取值的集合。

(3) 纠错能力。对于某个节点和链路组合 $A\subseteq\mathcal{V}\cup\mathcal{E}$，如果无论 A 的输出有怎样的错误，无论要传输的消息是消息集中的哪个消息，总使得对所有的 $k\in\mathcal{K}$ 和 $v\in\mathcal{V}_t^{(k)}$ 有 $\hat{M}_v^{(k)}=M^{(k)}$，则称码 C 可以对抗组合 A。码 C 可以对抗的所有组合成为其纠错能力，记为 $\mathcal{A}$。

例 3.1：在图 1.3 所示的网络 $\mathcal{G}_3$ 中，源节点和目的节点通过三条链路相连。现在此网络中有一个称为“重复编码+大数判决”的网络纠错码 C_n，它的消息集

$\mathcal{M} \triangleq \{0,1\}$，码长为$n$，每次信道使用的时候源节点都将消息在各链路上发送一次，即

$$\mathrm{Enc}_{e,i}(M) \triangleq M, \quad e \in \mathcal{E}. \tag{3–2}$$

发送结束后目的节点进行大数判决决定恢复出的消息。

对于这个网络纠错码C_n，它的消息速率为：

$$\begin{aligned} R &= \frac{1}{n}\log_2 2 \\ &= \frac{1}{n}. \end{aligned}$$

链路速率为

$$\begin{aligned} \mathbf{f}_{\mathcal{E}} &= (\log_2 2 : e \in \mathcal{E}) \\ &= \mathbf{1}_{\mathcal{E}}. \end{aligned}$$

接下来求它的纠错能力$\mathcal{A}$。我们将对于所有的$\mathcal{E}_a \subseteq \mathcal{E}$依次验证链路集$\mathcal{E}_a$是不是可以对抗的组合，如果是，则$\mathcal{E}_a \in \mathcal{A}$；如果能够找到一种攻击方案使得这个网络纠错方案不能正确译码，则$\mathcal{E}_a \notin \mathcal{A}$。

回顾前文的假设，对于一个组合$\mathcal{E}_a$，若链路$e \in \mathcal{E}_a$，则意味着e的输出可以是由攻击方任意指定的信号序列；若链路$e \notin \mathcal{E}_a$，则意味着e的输出就是输入，在本例子中就是不断输出消息。

首先来看平凡的集合$\varnothing$。这表示网络中没有任何错误。显然这时候能正确译码。所以$\varnothing$是可以对抗的错误。

接着来看单元素集合$\{e\}$，其中$e \in \mathcal{E}$。这时候攻击方有2^{2n+1}种攻击方式，分别是：

(攻击方式 1)　当消息$M=0$时令$Y_e^n = 000....00$；

(攻击方式 2)　当消息$M=0$时令$Y_e^n = 000....01$；

(攻击方式 3)　当消息$M=0$时令$Y_e^n = 000....10$；

…

(攻击方式2^{2n})　当消息$M=0$时令$Y_e^n = 111....11$；

(攻击方式$2^{2n}+1$)　当消息$M=1$时令$Y_e^n = 000....00$；

(攻击方式$2^{2n}+2$)　当消息$M=1$时令$Y_e^n = 000....01$；

…

(攻击方式2^{2n+1})　当消息$M=1$时令$Y_e^n = 111....11$。

可以验证，攻击方使用了哪一种攻击，目的节点恢复出的消息都是正确的消息，所以$\{e\}$（$e\in\mathcal{E}$）也是可以对抗的错误。

接着来看双元素集合$\{e_1,e_2\}$。这时候攻击方采用下面的攻击方式：

(攻击方式) 当消息$M=0$令$Y_{e_1}^n=Y_{e_2}^n=111....11$。

这时，在消息为 0 的时候，目的节点恢复出的消息为 1，所以攻击成功。该网络纠错码不能对抗组合$\{e_1,e_2\}$。

类似的还可以验证，该网络纠错方案不能对抗$\{e_1,e_3\},\{e_2,e_3\},\{e_1,e_2,e_3\}$。

综上，我们求得了该网络纠错码的纠错能力为

$$\mathcal{A}=\mathcal{P}(\mathcal{E},1). \tag{3–3}$$

即该码可以纠正任一链路错。 □

显然，在同一个网络上可能有很多很多不同的网络纠错码。例如，在图 1.2 中消息集大小为M 且码长为n 且链路速率为$\mathbf{1}_{\mathcal{E}}\triangleq(1,1,1)$的网络纠错方案就有$\left(2^{3n}\right)^M\times\left[\prod_{i=1}^{n}2^{(2^i)}\right]^3\times M^{(2^{3n})}$种。

3.3 信道容量域和容许速率域的定义

本节定义有向网络的信道容量域和容许序列域，并给出它们之间的对偶关系。

定义 3.1（有向网络网络纠错信道容量域）：给定的网络$\mathcal{G}$、连接集$\mathcal{K}$、攻击组合$\mathcal{A}$、各链路速率$\mathbf{f}_{\mathcal{E}}=(f_e:e\in\mathcal{E})$。对于某个速率$\mathbf{R}^{(\mathcal{K})}=\left(R^{(k)}:k\in\mathcal{K}\right)$，若存在网络纠错信道码达到速率$\mathbf{R}^{(\mathcal{K})}$，则称速率$\mathbf{R}^{(\mathcal{K})}$是可达速率。所有可达速率的集合的闭包记为信道容量域$\mathcal{C}$。 □

在只有一个业务时，信道容量域$\mathcal{C}$ 是一个闭区间，其最大值又称为信道容量，记为C。

定义 3.2（有向网络网络纠错容许速率域）：给定的网络$\mathcal{G}$、连接集$\mathcal{K}$、攻击组合$\mathcal{A}$、信源参数。对于某个各链路速率$\mathbf{f}_{\mathcal{E}}$，若存在网络纠错信源码各链路速率为$\mathbf{f}_{\mathcal{E}}$，则称速率$\mathbf{f}_{\mathcal{E}}$是容许速率。所有容许速率的集合的闭包记为容许速率域$\mathcal{R}$。 □

例 3.2：如图 1.3，在网络$\mathcal{G}_3$中有一个单播业务，从源节点v_s到目的节点v_t有三条链路相连。

(1) 给定链路速率为$\mathbf{f}_{\mathcal{E}}=(f_e:e\in\mathcal{E})$，纠错能力$\mathcal{A}=\mathcal{P}(\mathcal{E},1)$，则这时的信道容量为$\min_{e\in\mathcal{E}}f_e$。

(2) 在有向图$\mathcal{G}_3$中，给定消息速率为R，链路速率为$\mathbf{f}_{\mathcal{E}}=\left(f_e:e\in\mathcal{E}\right)$，纠错能力$\mathcal{A}=\mathcal{P}\left(\mathcal{E},1\right)$，则这时的容许速率域为

$$\mathcal{R}_{R,\mathcal{P}(\mathcal{E},1)}=\left\{\left(f_1,f_2,f_3\right):f_1\geq R,f_2\geq R,f_3\geq R\right\}.$$ □

和传统概率信息论中的情形一样，信道容量域和容许速率域都是凸集，且信道容量域和容许速率域具有对偶性。

性质 3.1（信道容量域和容许速率域的对偶性）：给定的网络$\mathcal{G}$、连接集$\mathcal{K}$、攻击组合$\mathcal{A}$。各连接信源独立。$\mathbf{f}_{\mathcal{E}}$是一个可能的链路速率，$\mathbf{R}^{(\mathcal{K})}$是一个可能的消息速率。则下面两个命题等价：

(1) 在该网络上进行信道编码，若各链路速率为$\mathbf{f}_{\mathcal{E}}$，则$\mathbf{R}^{(\mathcal{K})}\in\mathcal{C}$，其中$\mathcal{C}$是信道容量域；

(2) 在该网络上进行信源编码，若消息速率为$\mathbf{R}^{(\mathcal{K})}$，则$\mathbf{f}_{\mathcal{E}}\in\mathcal{R}$，其中$\mathcal{R}$是容许速率域。 □

第 4 章　有向网络中的点对点通信

内容提要

本章将考虑第 3 章中介绍的有向网络模型中点对点通信的情形。

● 4.1 节考虑有向网络中点对点通信的信道容量。4.1.1 节定义了一个新的数学运算，以简化后续的表示；4.1.2 节重新考虑了文献[8]中给出的两节点网络信道容量和一般有向网络信道容量的割集上界；4.1.3 节证明了一般有向网络信道容量非零与信道容量割集上界非零的等价关系；4.1.4 节给出了一个信道容量割集上界不紧的例子，并介绍了如何利用信息支配求得那个网络的信道容量。

● 4.2 节考虑有向网络中点对点通信的容许速率域。4.2.1 节推导了容许速率域的割集外界；4.2.2 节推导了两节点网络的容许速率域；4.2.3 节求了一种特殊的网络（蟑螂网络）的容许速率域；4.2.4 节讨论了容许速率域割集外界的紧性，并介绍如何使用信息支配得到更紧的容许速率域外界。

● 4.3 节考虑一种特殊的有向网络（三节点网络）中点对点通信的信道容量。4.3.1 节~4.3.5 节讨论这些网络的内界；4.3.6 列举出一些数值例子。

本章部分内容改编自在学期间发表的学术论文[3,4]。文章的共同作者参与了相关的讨论和研究。

4.1 有向网络点对点信道容量上界

本节的研究结果将针对单发单收的有向网络的信道容量。具体而言，本节先引入一个新的数学运算“删 z 和”，然后用这个数学运算来表示文献[8]中的前人工作“割集上界”（该割集上界非本研究中新取得的成果）。接着给出割集上界的非零性与速率的非零性等价定理。最后给出利用“信息支配”的思想改进上界的方法。

4.1.1 删 z 和

为了后文方便，这里引入一个数学运算。

定义 4.1（删 z 和）：$\mathbf{f}^{(1)},\mathbf{f}^{(2)},\ldots,\mathbf{f}^{(d)}$ 是 d 个向量，其中 $\mathbf{f}^{(i)}$（$1\le i\le d$）的长度是 $n^{(i)}$。定义定义以下优化问题的解为 $\mathbf{f}^{(1)},\mathbf{f}^{(2)},\ldots,\mathbf{f}^{(d)}$ 的删 z 和（记为 $\Sigma_z^{(d)}\left(\mathbf{f}^{(1)},\mathbf{f}^{(2)},\ldots,\mathbf{f}^{(d)}\right)$）：

maximize　$\min\left\|\mathbf{X}'\right\|$，其中最小是针对所有从张量 $\mathbf{X}$ 中

的任意一个或多个维度去掉 z 个平面得到的新张量 $\mathbf{X}'$

over　$\mathbf{X} \triangleq \left(x_{i_1,i_2,\ldots,i_d}\right)_{1\le i_1\le n_1,1\le i_2\le n_2,\ldots,1\le i_d\le n_d}$

s.t.　$\sum_{i_1=1}^{n_1}\sum_{i_2=1}^{n_2}\cdots\sum_{i_{k-1}=1}^{n_{k-1}}\sum_{i_{k+1}=1}^{n_{k+1}}\cdots\sum_{i_d=1}^{n_d} x_{i_1,i_2,\ldots,i_{k-1},i_k,i_{k+1},\ldots,i_d} \le f_{i_k}^{(k)},\quad k\in[1:d], i_k\in[1:n_k]$

$$x_{i_1,i_2,\ldots,i_d}\ge 0,\quad i_1\in[1:n_1], i_2\in[1:n_2],\cdots,i_d\in[1:n_d]. \qquad \square$$

这个优化问题可以转化为一个有 $\Theta\left(\prod_{k=1}^{d} n_k\right)$ 个变量和 $O\left(\begin{pmatrix}\sum_{k=1}^{d} n_k\\ z\end{pmatrix}\right)$ 个非平凡约束的线性规划问题。

为了直观了解这个定义，下面看两个例子：

例 4.1（$d=1$ 时的删 z 和）：向量 $\mathbf{f}^{(1)}$ 的删 z 和可以通过以下方式计算：先将向量 $\mathbf{f}^{(1)}$ 从小到大排序为 $\mathbf{f}' \triangleq \left(f_1', f_2', \ldots, f_{n_1}'\right)^T$，则

$$\Sigma_z^{(d)}\left(\mathbf{f}^{(1)}\right) = \sum_{i=1}^{n_1-z} f_i'. \qquad \square$$

例 4.2（$d=2$ 时的删 z 和）：向量 $\mathbf{f}^{(1)}$ 和 $\mathbf{f}^{(2)}$ 的删 z 和通过以下线性规划计算：

maximize　σ

over　$\mathbf{X} \triangleq \left(x_{i,j}\right)_{1\le i\le n^{(1)},1\le j\le n^{(2)}}, \sigma$

s.t.　$\mathbf{X}\mathbf{1} \le \mathbf{f}^{(1)}$

$\mathbf{X}^T\mathbf{1} \le \mathbf{f}^{(2)}$

$\mathbf{1}_p^T\mathbf{X}\mathbf{1}_q \ge \sigma$，　其中 $\mathbf{1}_p$ 和 $\mathbf{1}_q$ 是元素非0即1的向量，

且满足 $\|\mathbf{1}_p\| + \|\mathbf{1}_p\| \ge n_1 + n_2 - z$

$x_{i,j}\ge 0,\quad 1\le i\le n_1, 1\le j\le n_2.$ $\square$

4.1.2 割集上界

利用割做上界是最直观也最简单的方法。在单源单宿情形下，对某个节点子集 $\mathcal{V}_s\subseteq\mathcal{V}$，若其满足 $v_s\in\mathcal{V}_s$ 和 $v_t\notin\mathcal{V}_s$，就可以导出一个割。具体方法是，定义其中前向链路集 $\mathcal{E}_+(\mathcal{V}_s) \triangleq \left\{e\in\mathcal{E}: \mathrm{Tail}(e)\in\mathcal{V}_s, \mathrm{Head}(e)\notin\mathcal{V}_s\right\}$ 和反向链路集 $\mathcal{E}_-(\mathcal{V}_s) \triangleq \left\{e\in\mathcal{E}: \mathrm{Tail}(e)\notin\mathcal{V}_s, \mathrm{Head}(e)\in\mathcal{V}_s\right\}$，割 $\mathcal{E}_c(\mathcal{V}_s) \triangleq \mathcal{E}_+(\mathcal{V}_s)\cup\mathcal{E}_-(\mathcal{V}_s)$。在不致混淆的情况下，$\mathcal{E}_+(\mathcal{V}_s), \mathcal{E}_-(\mathcal{V}_s), \mathcal{E}_c(\mathcal{V}_s)$ 也可记为 $\mathcal{E}_+, \mathcal{E}_-, \mathcal{E}_c$。

文献[8]中得到了两节点网络对抗任意 z 条链路错误的信道容量，事实上求得了所有可能的基于割的上界中最紧的上界。

下面介绍什么是两节点网络①。两节点网络是有且只有两个节点的网络，网络上只有一个单播业务。从源节点 v_s 到目的节点 v_t 可能没有链路，也可能有一条或多条链路。类似的，从目的节点 v_t 到源节点 v_s 可能没有链路，也可能有一条或多条链路。在这个网络中只能有一种割，即 $\mathcal{E}_+ = \{e \in \mathcal{E} : \mathrm{Tail}(e) = v_s\}$，$\mathcal{E}_- = \{e \in \mathcal{E} : \mathrm{Tail}(e) = v_t\}$。针对两节点网络，文献[8]求得了 $\mathcal{A} = \mathcal{P}(\mathcal{E}, z)$（$z$ 是自然数）时两节点网络的信道容量。

定理 4.1（两节点网络的信道容量，[8]）：z 是一个自然数。对于两节点网络，若 $\mathcal{A} = \mathcal{P}(\mathcal{E}, z)$，则其纠错容量为

$$C = \begin{cases} 0, & |\mathcal{E}_+| \le 2z \\ \Sigma_{n_z}^{(1)}\left(\mathbf{f}_{\mathcal{E}_+}\right), & |\mathcal{E}_+| > 2z, \end{cases} \tag{4–1}$$

其中 $n_z \triangleq \max\left\{z, 2\left(z - |\mathcal{E}_-|\right)\right\}$。 □

上述定理事实上给出了基于割的最紧的上界。考虑一般的网络 $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ 和其上的一个割 $\mathcal{E}_c = \mathcal{E}_+ \cup \mathcal{E}_-$，

$$C_{UB}\left(\mathbf{f}_{\mathcal{E}_c}\right) \triangleq \begin{cases} 0, & |\mathcal{E}_+| \le 2z \\ \Sigma_{n_z}^{(1)}\left(\mathbf{f}_{\mathcal{E}_+}\right), & |\mathcal{E}_+| > 2z \end{cases}$$

就给出了一个信道容量的上界[8]。试想，如果可能得到比 $C_{UB}\left(\mathbf{f}_{\mathcal{E}_c}\right)$ 更紧的界，那么将那个界运用到两节点网络中就会产生矛盾[8]。所以 $C_{UB}\left(\mathbf{f}_{\mathcal{E}_c}\right)$ 是基于割的所有上界中最紧的上界[8]。

4.1.3 割集上界非零和容量非零的关系

本文发现，割集上界不仅是一个数值，它还指示该网络中是否有可能进行可靠通信。

定理 4.2：给定的网络 $\mathcal{G}$、攻击组合 $\mathcal{A}$ 和各链路速率 $\mathbf{f}_{\mathcal{E}}$。信道容量 $C > 0$ 当前仅当其所有割的最小割集上界 > 0；信道容量 $C = 0$ 当前仅当其所有割的最小割集上界 $= 0$。 □

该定理针对割集上界是否为 0 与信道容量是否为 0 之间的关系进行了研究，说明了割集上界为 0 时，信道容量就为 0；割集上界不为 0 时，信道容量就不为 0。

① 两节点网络的描述改编自文献[8]。

为了证明这个定理，先给出几个引理。

引理 4.1：给定网络$\mathcal{G}$和$\mathcal{A}$。若存在$\mathcal{E}_a^{(1)},\mathcal{E}_a^{(2)}\in\mathcal{A}$和割$\mathcal{E}_+\bigcup\mathcal{E}_-$使得$\mathcal{E}_+\subseteq\mathcal{E}_a^{(1)}\bigcup\mathcal{E}_a^{(2)}$，则$C=0$。 □

这个引理的证明是割集上界证明的简单重复。

引理 4.1 的证明：用反证法。反设存在码长为n的网络纠错码，其速率$R>0$。这个码的消息集大小$2^{nR}\geq 2$。令$m^{(1)}$和$m^{(2)}$表示两个不同的消息，令$\mathbf{x}_{\mathcal{E}_+}^{(1)}$表示消息为$m^{(1)}$时在$\mathcal{E}_+$上传输的信号；令$\mathbf{x}_{\mathcal{E}_+}^{(2)}$表示消息为$m^{(2)}$时在$\mathcal{E}_+$上传输的信号。考虑以下两种情况：

(情况 1) 当$\mathcal{E}_+$的输出为$\left(\mathbf{x}_{\mathcal{E}_+\setminus\mathcal{E}_a^{(1)}}^{(1)},\mathbf{x}_{\mathcal{E}_a^{(1)}\cup\mathcal{E}_+}^{(2)}\right)$时译码结果为$\hat{M}=m^{(2)}$。发送消息$M=m^{(1)}$并且敌对方控制$\mathcal{E}_a^{(1)}$，则敌对方就会将$\mathcal{E}_a^{(1)}\bigcup\mathcal{E}_+$上的信号从$\mathbf{x}_{\mathcal{E}_a^{(1)}\cup\mathcal{E}_+}^{(1)}$改为$\mathbf{x}_{\mathcal{E}_a^{(1)}\cup\mathcal{E}_+}^{(2)}$，这样$\mathcal{E}_+$的输出就变为$\left(\mathbf{x}_{\mathcal{E}_+\setminus\mathcal{E}_a^{(1)}}^{(1)},\mathbf{x}_{\mathcal{E}_a^{(1)}\cup\mathcal{E}_+}^{(2)}\right)$。这样$\hat{M}=m^{(2)}$，得到$\hat{M}\neq M$。

(情况 2) 当$\mathcal{E}_+$的输出为$\left(\mathbf{x}_{\mathcal{E}_+\setminus\mathcal{E}_a^{(1)}}^{(1)},\mathbf{x}_{\mathcal{E}_a^{(1)}\cup\mathcal{E}_+}^{(2)}\right)$时译码结果为$\hat{M}\neq m^{(2)}$。发送消息$M=m^{(2)}$并且敌对方控制$\mathcal{E}_a^{(2)}$。由于$\mathcal{E}_+\subseteq\mathcal{E}_a^{(1)}\bigcup\mathcal{E}_a^{(2)}$，所以$\mathcal{E}_+\setminus\mathcal{E}_a^{(1)}\subseteq\mathcal{E}_a^{(2)}$。则敌对方会将$\mathcal{E}_+\setminus\mathcal{E}_a^{(1)}$上的信号从$\mathbf{x}_{\mathcal{E}_+\setminus\mathcal{E}_a^{(1)}}^{(2)}$改为$\mathbf{x}_{\mathcal{E}_+\setminus\mathcal{E}_a^{(1)}}^{(1)}$。这样$\mathcal{E}_+$的输出就变为$\left(\mathbf{x}_{\mathcal{E}_+\setminus\mathcal{E}_a^{(1)}}^{(1)},\mathbf{x}_{\mathcal{E}_a^{(1)}\cup\mathcal{E}_+}^{(2)}\right)$。这样$\hat{M}\neq m^{(2)}$，得到$\hat{M}\neq M$。

在以上两种情况均有$\hat{M}\neq M$，所以该码不能纠正相应的错误。得证。 □

令$\mathcal{P}$表示从源节点v_s到目的节点v_t的所有无环路径（注意这里的$\mathcal{P}$没有自变量，不是一元算子或是二元算子。本文中没有自变量的$\mathcal{P}$都代表路径集合。）对于路径$p\in\mathcal{P}$，令$\mathcal{E}_p$表示路径p经过的链路的集合。对于一个边集$\mathcal{E}_a\in\mathcal{A}$，定义

$$\mathcal{P}_{\mathcal{E}_a}\triangleq\left\{p\in\mathcal{P}:\mathcal{E}_p\bigcap\mathcal{E}_a\neq\varnothing\right\}. \tag{4–2}$$

引理 4.2：给定网络$\mathcal{G}$和两个边集$\mathcal{E}_a^{(1)},\mathcal{E}_a^{(2)}\subseteq\mathcal{E}$，有

$$\mathcal{P}_{\mathcal{E}_a^{(1)}\cup\mathcal{E}_a^{(2)}}=\mathcal{P}_{\mathcal{E}_a^{(1)}}\bigcup\mathcal{P}_{\mathcal{E}_a^{(2)}}. \qquad \square$$

证明：由于式（4–2），有

$$\begin{aligned}\mathcal{P}_{\mathcal{E}_a^{(1)}\cup\mathcal{E}_a^{(2)}} &= \left\{p\in\mathcal{P}:\mathcal{E}_p\bigcap\left(\mathcal{E}_a^{(1)}\bigcup\mathcal{E}_a^{(2)}\right)\neq\varnothing\right\}\\ &= \left\{p\in\mathcal{P}:\left(\mathcal{E}_p\bigcap\mathcal{E}_a^{(1)}\right)\bigcup\left(\mathcal{E}_p\bigcap\mathcal{E}_a^{(2)}\right)\neq\varnothing\right\}\\ &= \left\{p\in\mathcal{P}:\mathcal{E}_p\bigcap\mathcal{E}_a^{(1)}\neq\varnothing\text{或}\mathcal{E}_p\bigcap\mathcal{E}_a^{(2)}\neq\varnothing\right\}\\ &= \left\{p\in\mathcal{P}:\mathcal{E}_p\bigcap\mathcal{E}_a^{(1)}\neq\varnothing\right\}\bigcup\left\{p\in\mathcal{P}:\mathcal{E}_p\bigcap\mathcal{E}_a^{(2)}\neq\varnothing\right\}\\ &= \mathcal{P}_{\mathcal{E}_a^{(1)}}\bigcup\mathcal{P}_{\mathcal{E}_a^{(2)}}.\end{aligned}$$ □

引理 4.3：给定网络$\mathcal{G}$和边集$\mathcal{E}_a\subseteq\mathcal{E}$。若对于所有的割$\mathcal{E}_c=\mathcal{E}_+\bigcup\mathcal{E}_-$均有$\mathcal{E}_+\not\subseteq\mathcal{E}_a$，则存在路径$p\in\mathcal{P}$使得$p\notin\mathcal{P}_{\mathcal{E}_a}$。 □

证明：为了证明这个引理，我们构造一个图$\mathcal{G}$的生成树，使其满足以下两个条件：

(条件 1) 树的根是v_s；

(条件 2) 树的各链路都不属于$\mathcal{E}_a$。

构造这样的树的方法如下：

(第 1 步) 一方面，令$\mathcal{V}_s^{(1)}\triangleq\{v_s\}$，显然有$\left|\mathcal{V}_s^{(1)}\right|=1$。另一方面，由于$\mathcal{E}_+\left(\mathcal{V}_s^{(1)}\right)\not\subseteq\mathcal{E}_a$，所以存在一条链路$e^{(1)}\in\mathcal{E}_+\left(\mathcal{V}_s^{(1)}\right)$使得$e^{(1)}\notin\mathcal{E}_a$。令$\mathcal{E}^{(1)}\triangleq\left\{e^{(1)}\right\}$。显然有$\mathcal{E}^{(1)}\bigcap\mathcal{E}_a=\varnothing$。

(第 2 步) 一方面，令$\mathcal{V}_s^{(2)}\triangleq\mathcal{V}_s^{(1)}\bigcup\left\{\text{Head}\left(e^{(1)}\right)\right\}$。因为$e^{(1)}\in\mathcal{E}_+\left(\mathcal{V}_s^{(1)}\right)$，所以$\text{Head}\left(e^{(1)}\right)\notin\mathcal{V}_s^{(1)}$，进而$\left|\mathcal{V}_s^{(2)}\right|=2$。另一方面，由于$\mathcal{E}_+\left(\mathcal{V}_s^{(2)}\right)\not\subseteq\mathcal{E}_a$，所以存在一条链路$e^{(2)}\in\mathcal{E}_+\left(\mathcal{V}_s^{(2)}\right)$使得$e^{(2)}\notin\mathcal{E}_a$。令$\mathcal{E}^{(2)}\triangleq\mathcal{E}^{(1)}\bigcup\left\{e^{(2)}\right\}$。因为$\mathcal{E}^{(1)}\bigcap\mathcal{E}_a=\varnothing$且$e^{(2)}\notin\mathcal{E}_a$，所以$\mathcal{E}^{(2)}\bigcap\mathcal{E}_a=\varnothing$。

……

(第i步，$i\in(1:|\mathcal{V}|)$) 一方面，令$\mathcal{V}_s^{(i)}\triangleq\mathcal{V}_s^{(i-1)}\bigcup\left\{\text{Head}\left(e^{(i-1)}\right)\right\}$。因为$e^{(i-1)}\in\mathcal{E}_+\left(\mathcal{V}_s^{(i-1)}\right)$，所以$\text{Head}\left(e^{(i-1)}\right)\notin\mathcal{V}_s^{(i-1)}$，进而$\left|\mathcal{V}_s^{(i)}\right|=i$。另一方面，由于$\mathcal{E}_+\left(\mathcal{V}_s^{(i)}\right)\not\subseteq\mathcal{E}_a$，所以存在一条链路$e^{(i)}\in\mathcal{E}_+\left(\mathcal{V}_s^{(i)}\right)$使得$e^{(i)}\notin\mathcal{E}_a$。令$\mathcal{E}^{(i)}\triangleq\mathcal{E}^{(i-1)}\bigcup\left\{e^{(i)}\right\}$。因为$\mathcal{E}^{(i-1)}\bigcap\mathcal{E}_a=\varnothing$且$e^{(i)}\notin\mathcal{E}_a$，所以$\mathcal{E}^{(i)}\bigcap\mathcal{E}_a=\varnothing$。

……

(第$|\mathcal{V}|$步) 令$\mathcal{V}_s^{(|\mathcal{V}|)} \triangleq \mathcal{V}_s^{(|\mathcal{V}|-1)} \cup \left\{\text{Head}\left(e^{(|\mathcal{V}|-1)}\right)\right\}$。由于$e^{(|\mathcal{V}|-1)} \in \mathcal{E}_+\left(\mathcal{V}_s^{(|\mathcal{V}|-1)}\right)$，所以$\text{Head}\left(e^{(|\mathcal{V}|-1)}\right) \notin \mathcal{V}_s^{(|\mathcal{V}|-1)}$，进而$\left|\mathcal{V}_s^{(|\mathcal{V}|)}\right| = |\mathcal{V}|$。所以$\mathcal{V}_s^{(|\mathcal{V}|)} = \mathcal{V}$。

用这$|\mathcal{V}|$步，我们得到了$\mathcal{G}$的一个生成树$\mathcal{T} \triangleq \left(\mathcal{V}, \mathcal{E}^{(|\mathcal{V}|-1)}\right)$，使得$\mathcal{E}^{(|\mathcal{V}|-1)} \cap \mathcal{E}_a = \varnothing$。由于在树内的任意两点间有一个无环的路径，所以从$v_s$到$v_t$有一条路径$p$。又考虑到$\mathcal{E}^{(|\mathcal{V}|-1)} \cap \mathcal{E}_a = \varnothing$且$\mathcal{E}_p \subseteq \mathcal{E}^{(|\mathcal{V}|-1)}$，所以有$\mathcal{E}_p \cap \mathcal{E}_a = \varnothing$。于是$p \notin \mathcal{P}_{\mathcal{E}_a}$。 □

下面证明定理 4.2。

定理 4.2 的证明：由于C不大于割集上界，所以割集上界$=0$时$C=0$。下面只需证明当割集上界>0时$C>0$。

由于割集上界>0，根据引理 4.1，对任意的$\mathcal{E}_a^{(1)}, \mathcal{E}_a^{(2)} \in \mathcal{A}$和割$\mathcal{E}_+ \cup \mathcal{E}_-$，都有$\mathcal{E}_+ \not\subseteq \mathcal{E}_a^{(1)} \bigcup \mathcal{E}_a^{(2)}$。进一步的，存在边$e$使得$e \in \mathcal{E}_+$且$e \notin \mathcal{E}_a^{(1)} \cup \mathcal{E}_a^{(2)}$。根据引理 4.2 和引理 4.3，存在路径$p \notin \mathcal{P}_{\mathcal{E}_a^{(1)} \cup \mathcal{E}_a^{(2)}} = \mathcal{P}_{\mathcal{E}_a^{(1)}} \cup \mathcal{P}_{\mathcal{E}_a^{(2)}}$，即$p \notin \mathcal{P}_{\mathcal{E}_a^{(1)}}$且$p \notin \mathcal{P}_{\mathcal{E}_a^{(2)}}$。将这个路径记为$\bar{p}_{\mathcal{E}_a^{(1)}, \mathcal{E}_a^{(2)}}$。

给定$\mathcal{E}_a \in \mathcal{A}$，令$\bar{\mathcal{P}}_{\mathcal{E}_a} \triangleq \left\{\bar{p}_{\mathcal{E}_a, \mathcal{E}_a^{(2)}} : \mathcal{E}_a^{(2)} \in \mathcal{A}\right\}$。对任意的某个$\mathcal{E}_a^{(2)} \in \mathcal{A}$，由于$\bar{p}_{\mathcal{E}_a, \mathcal{E}_a^{(2)}} \in \bar{\mathcal{P}}_{\mathcal{E}_a}$且$\bar{p}_{\mathcal{E}_a, \mathcal{E}_a^{(2)}} \notin \mathcal{P}_{\mathcal{E}_a^{(2)}}$，所以$\bar{\mathcal{P}}_{\mathcal{E}_a} \not\subseteq \mathcal{P}_{\mathcal{E}_a^{(2)}}$。

考虑下面的网络纠错码：将消息重复编码$|\mathcal{P}|$次，在所有路径上都直接发送。根据前面的分析，一方面，由于$\mathcal{A}$中最多有一个集合被恶意方控制，所以存在一系列路径$\bar{\mathcal{P}}_{\mathcal{E}_a}$并没有被恶意方控制，上面的信号都是正确的；另一方面，不存在一个$\bar{\mathcal{P}}_{\mathcal{E}_a}$能被恶意方完全控制。这样，目的节点$v_t$必然能找到一个$\bar{\mathcal{P}}_{\mathcal{E}_a}$，其上的信号都完全相同，并且一定是正确的。这样我们就构造了一个可以可靠传输消息的网络纠错码，证明了$C>0$。 □

4.1.4 比割集上界更紧的上界

利用信息支配原理，可以得到比割集上界更紧的上界。下面来看一个三节点网络的例子，来看看信息支配原理是如何得到比割集上界更紧的上界的。

下面介绍什么是三节点网络。三节点网络是有且只有三个节点的网络，网络上只有一个单播业务。三个节点分别是源节点v_s、目的节点v_t和中继节点v_r。记任意两个节点之间可能没有链路，也可能有一条或多条链路。定义$\mathcal{E}_{st} \triangleq \{e \in \mathcal{E}: \text{Tail}(e) = v_s \text{且} \text{Head}(e) = v_t\}$；类似的可以定义$\mathcal{E}_{ts}, \mathcal{E}_{sr}, \mathcal{E}_{rs}, \mathcal{E}_{rt}, \mathcal{E}_{tr}$。

直接将割集上界代入三节点网络中，可以得到割集上界。

命题 4.1（三节点网络的割集上界）：三节点网络中，$\mathcal{A} = \mathcal{P}(\mathcal{E}, z)$。则容量有以下上界：当$|\mathcal{E}_{st}| + \min\{|\mathcal{E}_{sr}|, |\mathcal{E}_{rt}|\} \le 2z$时，$C=0$；否则

$$C \le \min\left\{\Sigma^{(1)}_{n_{z,s}}\left(\begin{bmatrix}\mathbf{f}_{\mathcal{E}_{st}}\\ \mathbf{f}_{\mathcal{E}_{sr}}\end{bmatrix}\right), \Sigma^{(1)}_{n_{z,t}}\left(\begin{bmatrix}\mathbf{f}_{\mathcal{E}_{st}}\\ \mathbf{f}_{\mathcal{E}_{rt}}\end{bmatrix}\right)\right\} \tag{4–3}$$

其中

$$n_{z,s} \triangleq \max\left\{z, 2\left(z-|\mathcal{E}_{rs}|-|\mathcal{E}_{ts}|\right)\right\}$$
$$n_{z,t} \triangleq \max\left\{z, 2\left(z-|\mathcal{E}_{tr}|-|\mathcal{E}_{ts}|\right)\right\}. \qquad \square$$

证明：考虑割$\mathcal{E}_c\left(\{v_s\}\right)$，有上界

$$C_{UB,s} \triangleq \Sigma^{(1)}_{n_{z,s}}\left(\begin{bmatrix}\mathbf{f}_{\mathcal{E}_{st}}\\ \mathbf{f}_{\mathcal{E}_{sr}}\end{bmatrix}\right); \tag{4–4}$$

考虑割$\mathcal{E}_c\left(\{v_s, v_r\}\right)$，有上界

$$C_{UB,t} \triangleq \Sigma^{(1)}_{n_{z,t}}\left(\begin{bmatrix}\mathbf{f}_{\mathcal{E}_{st}}\\ \mathbf{f}_{\mathcal{E}_{rt}}\end{bmatrix}\right). \tag{4–5}$$

综上有上界$\min\left\{C_{UB,s}, C_{UB,t}\right\}$。 $\square$

下面来看一个例子，在这个例子中，割集上界并不紧。

例 4.3：考虑图 4.1 中的三节点网络，利用命题 4.1 可以计算得到$C_{UB,s} = C_{UB,t} = 2$。但是可以证明，这个网络的容量$C = 1$。证明如下：

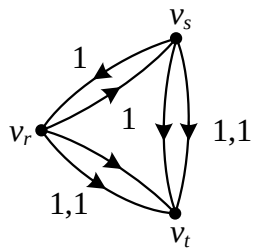


图 4.1　一个容量割集外界不紧的例子

记$\mathrm{CW}_e^n\left(m\right)$为消息$M = m$且网络中没有差错的情况下链路$e \in \mathcal{E}$上的信号。

上界证明$C \le 1$：用反证法。假设存在码长为n的网络纠错码C，其消息速率>1，进而消息集大小$A > 2^n$。记e_{sr}为从v_s到v_t的链路。由于码C的消息集大小$A > 2^n$，由抽屉原理可以知道存在两个不同的消息$m, \bar{m} \in \mathcal{M}$，使得其正常发送时在$e_{sr}$上传输的信号，即$\mathrm{CW}^n_{e_{sr}}\left(m\right) = \mathrm{CW}^n_{e_{sr}}\left(\bar{m}\right)$。

考虑中继节点v_r，其只有一个输入链路e_{sr}，容量为 1；另外它有两个输出链路（记为e_{rt1}和e_{rt2}），容量均为 1。显然链路e_{rt1}和e_{rt2}上的信号所承载的信息都来自于链路e_{sr}上承载的信号。（也就是说，链路e_{sr}支配了链路e_{rt1}和e_{rt2}。）从这个角度看，不妨让链路e_{rt1}和e_{rt2}都传输和链路e_{sr}相同的信号，也就是令$X_{e_{rt1}}^n = X_{e_{rt2}}^n = Y_{e_{sr}}^n$。

(情况 1) $M = m$且$Y_{e_{st2}}^n = \mathrm{CW}_{e_{st2}}^n\left(\bar{m}\right) \neq X_{e_{st2}}^n$。这时候有

$$\begin{aligned} Y_{e_{rt1}}^n = X_{e_{rt1}}^n = Y_{e_{sr}}^n = X_{e_{sr}}^n = \mathrm{CW}_{e_{sr}}^n\left(m\right) \\ Y_{e_{rt2}}^n = X_{e_{rt2}}^n = Y_{e_{sr}}^n = X_{e_{sr}}^n = \mathrm{CW}_{e_{sr}}^n\left(m\right) \\ Y_{e_{st1}}^n = X_{e_{st1}}^n = \mathrm{CW}_{e_{st1}}^n\left(m\right). \end{aligned}$$

所以译码器

$$\mathrm{Dec}: \mathcal{Q}_{e_{rt1}}^n \times \mathcal{Q}_{e_{rt2}}^n \times \mathcal{Q}_{e_{st1}}^n \times \mathcal{Q}_{e_{st2}}^n \to \mathcal{M} \tag{4–6}$$

满足$\mathrm{Dec}\left(\mathrm{CW}_{e_{sr}}^n\left(m\right), \mathrm{CW}_{e_{sr}}^n\left(m\right), \mathrm{CW}_{e_{st1}}^n\left(m\right), \mathrm{CW}_{e_{st2}}^n\left(\bar{m}\right)\right) = m$。

(情况 2) $M = \bar{m}$且$Y_{e_{st1}}^n = \mathrm{CW}_{e_{st1}}^n\left(m\right) \neq X_{e_{st1}}^n$。这时有

$$\begin{aligned} Y_{e_{rt1}}^n = X_{e_{rt1}}^n = Y_{e_{sr}}^n = X_{e_{sr}}^n = \mathrm{CW}_{e_{sr}}^n\left(\bar{m}\right) = \mathrm{CW}_{e_{sr}}^n\left(m\right) \\ Y_{e_{rt2}}^n = X_{e_{rt2}}^n = Y_{e_{sr}}^n = X_{e_{sr}}^n = \mathrm{CW}_{e_{sr}}^n\left(\bar{m}\right) = \mathrm{CW}_{e_{sr}}^n\left(m\right) \\ Y_{e_{st2}}^n = X_{e_{st2}}^n = \mathrm{CW}_{e_{st2}}^n\left(\bar{m}\right). \end{aligned}$$

所以译码器满足$\mathrm{Dec}\left(\mathrm{CW}_{e_{sr}}^n\left(m\right), \mathrm{CW}_{e_{sr}}^n\left(m\right), \mathrm{CW}_{e_{st1}}^n\left(m\right), \mathrm{CW}_{e_{st2}}^n\left(\bar{m}\right)\right) = \bar{m}$。

以上两种情况对译码器提出了不同的要求。考虑到$m \neq \bar{m}$，所以得到矛盾。这样就证明了$C \leq 1$。

下界证明（$C \geq 1$）：考虑以下三个从源节点v_s到目的节点v_t的独立通道：$p_1 \triangleq \{e_{st1}\}$，$p_2 \triangleq \{e_{st2}\}$，$p_3 \triangleq \{e_{sr}, e_{rt1}\}$。对消息进行重复编码，在这三个通道同时发送消息。可以证明，这个码可以达到速率 1。

这样就证明了$C = 1$。　□

在这个例子中，先使用了割集上界得到了上界 2。然后再利用信息支配的思想，得到了另一个上界 1。这说明了割集上界不紧。采用信息支配后得到的上界 1 才是这个网络的真正容量。

4.2 有向网络点对点容许速率域与两节点网络的容许速率域

本节的研究结果将针对单发单收有向网络的容许速率域。具体而言，本节首先讨论一般有向网络的割集外界；然后证明在两节点网络中这个割集外界就是容许速率域；最后采用信息支配给出更紧的界。

4.2.1 容许速率域的割集外界

本节的结论是：采用割的方法，可以得到有向网络容许速率域的割集外界如下：

定理 4.3（有向网络容许速率域割集外界）：给定网络$\mathcal{G}=(\mathcal{V},\mathcal{E})$，$\mathcal{A}\subseteq\mathcal{P}(\mathcal{E})$和单播速率$R>0$。$\mathcal{E}_c=\mathcal{E}_+\bigcup\mathcal{E}_-$是一个割。定义

$$\mathcal{B}_{R,\mathcal{A}}^{(1)}(\mathcal{E}_+)\triangleq\bigcap_{\mathcal{E}_a\in\mathcal{A}}\left\{\mathbf{f}_{\mathcal{E}}\geq\mathbf{0}_{\mathcal{E}}:\left\|\mathbf{f}_{\mathcal{E}_+\setminus\mathcal{E}_a}\right\|\geq R\right\},$$

$$\mathcal{B}_{R,\mathcal{A}}^{(2)}(\mathcal{E}_+,\mathcal{E}_-)\triangleq\bigcap_{\substack{\mathcal{E}_a^{(1)}\in\mathcal{A}:\mathcal{E}_-\subseteq\mathcal{E}_a^{(1)}\\ \mathcal{E}_a^{(2)}\in\mathcal{A}:\mathcal{E}_-\subseteq\mathcal{E}_a^{(2)}}}\left\{\mathbf{f}_{\mathcal{E}}\geq\mathbf{0}_{\mathcal{E}}:\left\|\mathbf{f}_{\mathcal{E}_+\setminus\left(\mathcal{E}_a^{(1)}\bigcup\mathcal{E}_a^{(2)}\right)}\right\|\geq R\right\},$$

$$\mathcal{B}_{R,\mathcal{A}}(\mathcal{E}_+,\mathcal{E}_-)\triangleq\begin{cases}\varnothing, & \exists\mathcal{E}_a^{(1)},\mathcal{E}_a^{(2)}\in\mathcal{A}\text{使得}\mathcal{E}_+\subseteq\mathcal{E}_a^{(1)}\bigcup\mathcal{E}_a^{(2)}\\ \mathcal{B}_{R,\mathcal{A}}^{(1)}(\mathcal{E}_+)\bigcap\mathcal{B}_{R,\mathcal{A}}^{(2)}(\mathcal{E}_+,\mathcal{E}_-), & \text{其他.}\end{cases}$$

则容许速率域

$$\mathcal{R}\subseteq\mathcal{B}_{R,\mathcal{A}}(\mathcal{E}_+,\mathcal{E}_-).$$ □

记割集外界

$$\mathcal{B}_{R,\mathcal{A}}=\bigcap\mathcal{B}_{R,\mathcal{A}}(\mathcal{E}_+,\mathcal{E}_-),\tag{4–7}$$

其中集合交是针对所有的割。

定理 4.3 使用割集的方法，给出了一般网络的容许速率域的外界。这一外界刻画了一般网络的容许速率域。该刻画的有效性将在 4.2.2 节和 4.2.3 节讨论。

引理 4.4：给定网络$\mathcal{G}=(\mathcal{V},\mathcal{E})$、$\mathcal{A}\subseteq\mathcal{P}(\mathcal{E})$，单播速率$R>0$。$\mathcal{E}_c=\mathcal{E}_+\bigcup\mathcal{E}_-$是一个割。对任意容许速率$\mathbf{f}_{\mathcal{E}}\in\mathcal{R}$，需满足对任意$\mathcal{E}_a\in\mathcal{A}$，有

$$\left\|\mathbf{f}_{\mathcal{E}_+\setminus\mathcal{E}_a}\right\|\geq R.$$ □

证明：任取$\mathcal{E}_a\subseteq\mathcal{A}$，考虑敌对方控制资源$\mathcal{E}_a$的情况。这时，即使发送节点和接收节点都通过某种方式知道了这一情况，对于任何流$\mathbf{f}_{\mathcal{E}}\geq\mathbf{0}_{\mathcal{E}}$，也仅有$\left\|\mathbf{f}_{\mathcal{E}_+\setminus\mathcal{E}_a}\right\|$这么多的速率可以在$\mathcal{E}_+$上正常传输。所以任意要支持速率$R$的流$\mathbf{f}_{\mathcal{E}}$都需要满足$\left\|\mathbf{f}_{\mathcal{E}_+\setminus\mathcal{E}_a}\right\|\geq R$。 □

引理 4.5：给定网络$\mathcal{G}=(\mathcal{V},\mathcal{E})$、$\mathcal{A}\subseteq\mathcal{P}(\mathcal{E})$，单播速率$R>0$。$\mathcal{E}_c=\mathcal{E}_+\bigcup\mathcal{E}_-$是一个割。对任意容许速率$\mathbf{f}_{\mathcal{E}}\in\mathcal{R}$，需满足对任意$\mathcal{E}_a^{(1)},\mathcal{E}_a^{(2)}\in\mathcal{A}$，若其满足$\mathcal{E}_-\subseteq\mathcal{E}_a^{(1)}$和$\mathcal{E}_-\subseteq\mathcal{E}_a^{(2)}$，则有

$$\left\|\mathbf{f}_{\mathcal{E}_+\setminus\left(\mathcal{E}_a^{(1)}\cup\mathcal{E}_a^{(2)}\right)}\right\|\geq R.$$ □

证明：用反证法证明。反设存在$\mathbf{f}_{\mathcal{E}}\in\mathcal{R}$和$\mathcal{E}_a^{(1)},\mathcal{E}_a^{(2)}\in\mathcal{A}$，满足$\mathcal{E}_-\subseteq\mathcal{E}_a^{(1)}$、$\mathcal{E}_-\subseteq\mathcal{E}_a^{(1)}$且$\left\|\mathbf{f}_{\mathcal{E}_+\setminus\left(\mathcal{E}_a^{(1)}\cup\mathcal{E}_a^{(2)}\right)}\right\|<R$。

考虑任一链路速率为$\mathbf{f}_{\mathcal{E}}$的网络纠错信源编码C，记信道使用次数为n，则其消息集大小为2^{nR}。令$m^{(1)}$和$m^{(2)}$表示两个不同的消息，令$\mathbf{x}_{\mathcal{E}_+}^{(1)}$表示消息为$m^{(1)}$时在$\mathcal{E}_+$上传输的信号；令$\mathbf{x}_{\mathcal{E}_+}^{(2)}$表示消息为$m^{(2)}$时在$\mathcal{E}_+$上传输的信号。考虑以下两种情况：

(情况 1) 当$\mathcal{E}_+$的输出为$\left(\mathbf{x}_{\mathcal{E}_+\setminus\mathcal{E}_a^{(1)}}^{(1)},\mathbf{x}_{\mathcal{E}_a^{(1)}\cup\mathcal{E}_+}^{(2)}\right)$时译码结果为$M=m^{(2)}$。发送消息$M=m^{(1)}$并且敌对方控制$\mathcal{E}_a^{(1)}$，则敌对方就会将$\mathcal{E}_a^{(1)}\bigcup\mathcal{E}_+$上的信号从$\mathbf{x}_{\mathcal{E}_a^{(1)}\cup\mathcal{E}_+}^{(1)}$改为$\mathbf{x}_{\mathcal{E}_a^{(1)}\cup\mathcal{E}_+}^{(2)}$，这样$\mathcal{E}_+$的输出就变为$\left(\mathbf{x}_{\mathcal{E}_+\setminus\mathcal{E}_a^{(1)}}^{(1)},\mathbf{x}_{\mathcal{E}_a^{(1)}\cup\mathcal{E}_+}^{(2)}\right)$。这样$\hat{M}=m^{(2)}$，得到$\hat{M}\neq M$。

(情况 2) 当$\mathcal{E}_+$的输出为$\left(\mathbf{x}_{\mathcal{E}_+\setminus\mathcal{E}_a^{(1)}}^{(1)},\mathbf{x}_{\mathcal{E}_a^{(1)}\cup\mathcal{E}_+}^{(2)}\right)$时译码结果为$M\neq m^{(2)}$。发送消息$M=m^{(2)}$并且敌对方控制$\mathcal{E}_a^{(2)}$。由于$\mathcal{E}_+\subseteq\mathcal{E}_a^{(1)}\bigcup\mathcal{E}_a^{(2)}$，所以$\mathcal{E}_+\setminus\mathcal{E}_a^{(1)}\subseteq\mathcal{E}_a^{(2)}$。则敌对方会将$\mathcal{E}_+\setminus\mathcal{E}_a^{(1)}$上的信号从$\mathbf{x}_{\mathcal{E}_+\setminus\mathcal{E}_a^{(1)}}^{(2)}$改为$\mathbf{x}_{\mathcal{E}_+\setminus\mathcal{E}_a^{(1)}}^{(1)}$。这样$\mathcal{E}_+$的输出就变为$\left(\mathbf{x}_{\mathcal{E}_+\setminus\mathcal{E}_a^{(1)}}^{(1)},\mathbf{x}_{\mathcal{E}_a^{(1)}\cup\mathcal{E}_+}^{(2)}\right)$。这样$\hat{M}\neq m^{(2)}$，得到$\hat{M}\neq M$。

在以上两种情况均有$\hat{M}\neq M$，所以该码不能纠正相应的错误。得证。 □

定理 4.3 **证明：**由引理 4.3 可知$\mathcal{R}\subseteq\mathcal{B}_{R,\mathcal{A}}^{(1)}(\mathcal{E}_+)$，有引理 5.3 可知$\mathcal{R}\subseteq\mathcal{B}_{R,\mathcal{A}}^{(2)}(\mathcal{E}_+,\mathcal{E}_-)$，所以定理得证。 □

当$\mathcal{A}=\mathcal{P}(\mathcal{E},z)$时，定理 4.3 可简化为以下推论：

推论 4.1：给定网络$\mathcal{G}=(\mathcal{V},\mathcal{E})$、$\mathcal{A}=\mathcal{P}(\mathcal{E},z)$，单播速率$R>0$。则容许速率域有外界

$$\mathcal{B}_{R,\mathcal{P}(\mathcal{E},z)}(\mathcal{E}_+,\mathcal{E}_-)=\begin{cases}\varnothing, & |\mathcal{E}_+|\leq 2z\\ \left\{\mathbf{f}_{\mathcal{E}}\geq\mathbf{0}_{\mathcal{E}}:\Sigma_{n_z}^{(1)}\left(\mathbf{f}_{\mathcal{E}_+}\right)\geq R\right\}, & \text{其他,}\end{cases}\tag{4–8}$$

其中

$$n_z\triangleq\max\left\{z,2\left(z-|\mathcal{E}_-|\right)\right\}.$$ □

这个割集外界是所有可能的割集外界中最紧的割集外界。这可以通过下节两节点网络的容许速率域来论证。

4.2.2 两节点网络的容许速率域

定理 4.4（两节点网络的容许速率域）：考虑两节点网络$\mathcal{G}=(\mathcal{V},\mathcal{E})$，给定$R$和$\mathcal{A}$。割$\mathcal{E}_+\bigcup\mathcal{E}_-$的定义如第 4.1.2 节，$\mathcal{B}_{R,\mathcal{A}}$的定义如式（4–7）。则其容许速率域

$$\mathcal{R}=\mathcal{B}_{R,\mathcal{A}}.$$ □

定理 4.4 完全刻画了两节点网络的容许速率域$\mathcal{R}$，证明了$\mathcal{R}$就等于割集外界$\mathcal{B}_{R,\mathcal{A}}$。这一结论彻底解决了两节点网络的网络纠错信源编码和容许速率域问题。更重要的意义在于，由于两节点网络是一般网络的割的自然抽象，定理 4.4 在事实上已经证明了式（4–7）给出的割集外界是所有可能的割集外界中最紧的外界。

下面考虑定理 4.4 的证明。两节点网络容许速率域可以用文献[8]中的思路，构造猜测转发码来达到。

引理 4.6（两节点网络上的猜测转发）：考虑两节点网络$\mathcal{G}=(\mathcal{V},\mathcal{E})$，给定$R$和$\mathcal{A}$。$\mathcal{B}_{R,\mathcal{A}}$的定义如式（4–7）。则对任意的链路速率$\mathbf{f}_{\mathcal{E}}\in\mathcal{B}_{R,\mathcal{A}}$，任意的$0<\varepsilon<R$，存在链路速率为$\mathbf{f}_{\mathcal{E}}$、消息速率为$R-\varepsilon$、能够对抗错误$\mathcal{A}$的网络纠错码$\mathsf{C}$。 □

下面用一种新的方法来构造猜测转发码，进而证明这个定理。这个新的方法与[8]文中的方法相比，本质上是相同的。但是新的方法使用了不同的构造框架，使得这样的构造可以进一步扩展到更加复杂的网络的码构造中。

这种方法的基本思路是，先进行联络速率分割，针对链路速率$\mathbf{f}_{\mathcal{E}}$，考虑多个链路速率（如$\mathbf{f}_{\mathcal{E}}^{(i)},i\in I$，其中$I=\left[1:\left|I\right|\right]$是指标集，指标集内容视具体情况而定），使得

$$\mathbf{f}_{\mathcal{E}}^{(i)}\geq\mathbf{0}_{\mathcal{E}},\quad i\in I$$
$$\sum_{i\in I}\mathbf{f}_{\mathcal{E}}^{(i)}\leq\mathbf{f}_{\mathcal{E}}.$$

这样就把原来的链路速率$\mathbf{f}_{\mathcal{E}}$分割为多个链路速率$\mathbf{f}_{\mathcal{E}}^{(i)},i\in I$。然后，再对每一个$i=1,2,\ldots,\left|I\right|$依次分配码。对于两个不同的$i_1,i_2\in I$（不妨设$i_1<i_2$），$\mathbf{f}_{\mathcal{E}}^{(i_2)}$上传输的信号可以依赖于$\mathbf{f}_{\mathcal{E}}^{(i_1)}$，即认为$\mathbf{f}_{\mathcal{E}}^{(i_1)}$是先于$\mathbf{f}_{\mathcal{E}}^{(i_2)}$传输的，而不是同时传输的。利用这种先后传输的码达到速率。 □

下面来看两节点网络中的猜测转发码是怎么做的。仅考虑$\left|\mathcal{E}_+\right|>2z$的情况。

引理 4.6 的证明： 链路速率分割：将$\mathcal{E}=\mathcal{E}_+\bigcup\mathcal{E}_-$上的流量$\mathbf{f}_{\mathcal{E}}=\begin{pmatrix}\mathbf{f}_{\mathcal{E}_+}\\ \mathbf{f}_{\mathcal{E}_-}\end{pmatrix}$取出三个子流：$\begin{pmatrix}\mathbf{f}_{\mathcal{E}_+}-\delta_+\mathbf{1}_{\mathcal{E}_+}\\ \mathbf{0}_{\mathcal{E}_-}\end{pmatrix}$、$\begin{pmatrix}\mathbf{0}_{\mathcal{E}_+}\\ \delta_-\mathbf{1}_{\mathcal{E}_-}\end{pmatrix}$和$\begin{pmatrix}\delta_+\mathbf{1}_{\mathcal{E}_+}\\ \mathbf{0}_{\mathcal{E}_-}\end{pmatrix}$，其中$\delta_+,\delta_-$满足

$$0<\delta_+<\min_{e\in\mathcal{E}_+}f_e \tag{4–9}$$

$$0<\delta_{-}<\min_{e\in\mathcal{E}_{-}} f_e \tag{4–10}$$

$$\Sigma_{\mathcal{A}}^{(1)}\left(\mathbf{f}_{\mathcal{E}_{+}}-\delta_{+}\mathbf{1}_{\mathcal{E}_{+}}\right)>R-\varepsilon, \tag{4–11}$$

其中

$$\Sigma_{\mathcal{A}}^{(1)}\left(\mathbf{f}_{\mathcal{E}_{+}}\right)=\min\left\{\min_{\substack{\mathcal{E}_a^{(1)}\in\mathcal{A}:\mathcal{E}_{-}\subseteq\mathcal{E}_a^{(1)}\\ \mathcal{E}_a^{(2)}\in\mathcal{A}:\mathcal{E}_{-}\subseteq\mathcal{E}_a^{(2)}}}\left\|\mathbf{f}_{\mathcal{E}_{+}\setminus\left(\mathcal{E}_a^{(1)}\bigcup\mathcal{E}_a^{(2)}\right)}\right\|,\min_{\mathcal{E}_a\in\mathcal{A}}\left\|\mathbf{f}_{\mathcal{E}_{+}\setminus\mathcal{E}_a}\right\|\right\}. \tag{4–12}$$

而式（4–11）是由 $\mathcal{B}_{R,\mathcal{A}}$ 的定义得到。

显然有

$$\begin{pmatrix}\mathbf{f}_{\mathcal{E}_{+}}-\delta_{+}\mathbf{1}_{\mathcal{E}_{+}}\\ \mathbf{0}_{\mathcal{E}_{-}}\end{pmatrix}+\begin{pmatrix}\mathbf{0}_{\mathcal{E}_{+}}\\ \delta_{-}\mathbf{1}_{\mathcal{E}_{-}}\end{pmatrix}+\begin{pmatrix}\delta_{+}\mathbf{1}_{\mathcal{E}_{+}}\\ \mathbf{0}_{\mathcal{E}_{-}}\end{pmatrix}\le\begin{pmatrix}\mathbf{f}_{\mathcal{E}_{+}}\\ \mathbf{f}_{\mathcal{E}_{-}}\end{pmatrix}. \tag{4–13}$$

接下来分三步依次对三个子流进行编码。

(步骤 1) 在第 1 个子流上，使用码率为 $\dfrac{\Sigma_{\mathcal{A}}^{(1)}\left(\mathbf{f}_{\mathcal{E}_{+}}-\delta_{+}\mathbf{1}_{\mathcal{E}_{+}}\right)}{\left\|\mathbf{f}_{\mathcal{E}_{+}}-\delta_{+}\mathbf{1}_{\mathcal{E}_{+}}\right\|}$ 的最大距离可分码对消息编码，将编码后的结果在流 $\mathbf{f}_{\mathcal{E}_{+}}-\delta_{+}\mathbf{1}_{\mathcal{E}_{+}}$ 上传输（使用这样的最大距离可分码后，可以检测任意的 $\mathcal{E}_a\in\mathcal{A}$ 错误，并且如果限定错误在 $\{\mathcal{E}_a\in\mathcal{A}:\mathcal{E}_{-}\subseteq\mathcal{E}_a\}$ 则还可以纠错）；

(步骤 2) 在第 2 个子流上，目的节点 v_t 进行译码。如果没有检测到错误，则正确译码。否则，将所有收到的数据进行 $\left|\mathcal{E}_{-}\right|$ 次重复编码，通过流 $\delta_{-}\mathbf{1}_{\mathcal{E}_{-}}$ 回传给节点 v_s；

(步骤 3) 在第 3 个子流上，节点 v_s 收到在第 2 个子流上信号。源节点 v_s 将每一个 δ 流的数据和第 1 个子流上的数据比较，以试图猜测第 1 个子流中有哪些链路是错误的。接着，源节点 v_s 再将其在第 2 个子流上所有数据和猜测的结果进行 $\left|\mathcal{E}_{+}\right|$ 次重复编码，通过流 $\delta_{+}\mathbf{1}_{\mathcal{E}_{+}}$ 传给 v_t。

由于不存在 $\mathcal{E}_a^{(1)},\mathcal{E}_a^{(2)}\in\mathcal{A}$ 使得 $\mathcal{E}_{+}\subseteq\mathcal{E}_a^{(1)}\bigcup\mathcal{E}_a^{(2)}$，所以在第 3 个子流上的重复编码总能对抗 $\mathcal{A}$ 中链路错误，进而 v_t 总能正确恢复第 3 个子流的信号。接着，v_t 将其中的信号和第 2 个子流发出的信号相比较，就能知道在第 2 步中的所有错误边。进一步的，在第 2 个子流中非错误边的猜测都是可靠的。这样，如果在第 2 个子流中有非错误的边，则第 1 个子流中的错误边就被定位了；如果在第 2 个子流中所有链路都有错，则敌对组合必在 $\{\mathcal{E}_a\in\mathcal{A}:\mathcal{E}_{-}\subseteq\mathcal{E}_a\}$ 中，第 1 个子流的译码也可以将错误纠正。

通过这样的方案，只要发生一次错误，至少能定为出一条错误链路。而错误的链路个数是有限的，所以第 2 个子流和第 3 个子流的使用次数也是有限的。从长期看，消息速率取决于第 1 个子流，即消息速率为$\Sigma_{\mathcal{A}}^{(1)}\left(\mathbf{f}_{\mathcal{E}_+}-\delta_+\mathbf{1}_{\mathcal{E}_+}\right)$。而$\Sigma_{\mathcal{A}}^{(1)}\left(\mathbf{f}_{\mathcal{E}_+}-\delta_+\mathbf{1}_{\mathcal{E}_+}\right)>R-\varepsilon$，所以得证。 □

定理 4.4 证明：定理 4.3 已经证明$\mathcal{R}\subseteq\mathcal{B}_{R,\mathcal{A}}$。下证$\mathcal{B}_{R,\mathcal{A}}\subseteq\mathcal{R}$。任取$\mathbf{f}_{\mathcal{E}}\in\mathcal{B}_{R,\mathcal{A}}$。由于引理 5.6，对于任意的$0<\varepsilon<R$，在链路速率$\mathbf{f}_{\mathcal{E}}+\varepsilon\mathbf{1}_{\mathcal{E}}$上存在网络纠错码$\mathsf{C}$，其消息速率为$R$并且能对抗错误$\mathcal{A}$。所以$\mathbf{f}_{\mathcal{E}}+\varepsilon\mathbf{1}_{\mathcal{E}}\in\mathcal{R}$。令$\varepsilon\to0$，所以$\mathbf{f}_{\mathcal{E}}$在$\mathcal{R}$的闭包内。又由于$\mathcal{R}$是闭集，所以$\mathbf{f}_{\mathcal{E}}\in\mathcal{R}$。 □

4.2.3 蟑螂网络的容许速率域

本节将考虑著名的蟑螂网络，证明其容许速率域就是割集外界。从这个例子中可以看出割集外界的有效性。

蟑螂网络是如图 4.2 所示的网络，它是网络纠错理论研究常常分析的对象。在蟑螂网络中，有三个节点$\mathcal{V}_u=\{v_{u1},v_{u2},v_{u3}\}$与源节点$v_s$通过链路$\mathcal{E}_u=\{e_{u1},e_{u2},e_{u3}\}$直接相连，有四个节点$\mathcal{V}_d=\{v_{d1},v_{d2},v_{d3},v_{d4}\}$与目的节点$v_t$通过链路$\mathcal{E}_d=\{e_{d1},e_{d2},e_{d3},e_{d4}\}$直接相连，节点集$\mathcal{V}_u$还和节点集$\mathcal{V}_d$通过 6 条链路$\mathcal{E}_m=\{e_{m1},e_{m2},e_{m3},e_{m4},e_{m5},e_{m6}\}$以某种特定的方式相连。其中任意一条链路都可能被敌对方控制，即$\mathcal{A}=\mathcal{P}(\mathcal{E},1)$。

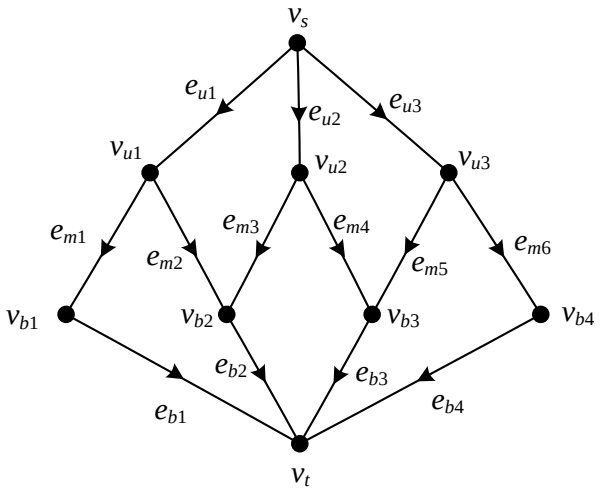


图 4.2　蟑螂网络（本图改编自文献[8,55,56]）

关于蟑螂网络的研究历史：文献[8,55,56]证明在链路速率为$\left(\mathbf{f}_{\mathcal{E}_u},\mathbf{f}_{\mathcal{E}_m},\mathbf{f}_{\mathcal{E}_b}\right)=\left(\mathbf{2}_{\mathcal{E}_u},\mathbf{1}_{\mathcal{E}_m},\mathbf{1}_{\mathcal{E}_b}\right)$的蟑螂网络中，线性网络纠错码不能达到纠错容量。这使得该网络成

为首个不能用线性方式达到容量的网络设置。文献[8,55,56]还构造了一种非线性的网络纠错码，它在中间节点v_{b2}和v_{b3}处进行的额外的校验，最终达到了网络纠错容量。文献[9]首次将该网络命名为蟑螂网络（rockroach network）。

本节的主要结论如下。

命题 4.2（蟑螂网络的容许速率域）：蟑螂网络在$\mathcal{A}=\mathcal{P}(\mathcal{E},1)$时的容许速率域为

$$\mathcal{R}=\mathcal{B}_{R,\mathcal{P}(\mathcal{E},1)}. \qquad \square$$

命题 4.2 完全刻画了蟑螂网络的容许速率域。值得一提的是，在外界刻画的过程中仅使用了割集外界，体现了割集外界对复杂网络刻画的有效性。

接下来考虑该命题 4.2 的证明。不失一般性，不妨仅考虑$R=1$的情况。证明将通过以下三各步骤完成：

(第 1 步) 利用割集外界的性质，确定$\mathcal{B}_{1,\mathcal{P}(\mathcal{E},1)}$中的链路速率需要满足的约束。具体而言，就是列举出$\mathcal{B}_{1,\mathcal{P}(\mathcal{E},1)}$的所有半平面；

(第 2 步) 得到$\mathcal{B}_{1,\mathcal{P}(\mathcal{E},1)}$的所有极点；

(第 3 步) 证明$\mathcal{B}_{1,\mathcal{P}(\mathcal{E},1)}$的所有极点都可以渐进达到，即证明所有的极点都在容许速率域$\mathcal{R}$内。这样就证明了整个$\mathcal{B}_{1,\mathcal{P}(\mathcal{E},1)}$都在容许速率域内，进而$\mathcal{R}=\mathcal{B}_{R,\mathcal{P}(\mathcal{E},1)}$。

$\square$

命题 4.2 证明的第 1 步（列举$\mathcal{B}_{1,\mathcal{P}(\mathcal{E},1)}$的所有半平面）：根据割集外界的结果，对于任意一个容许速率$\mathbf{f}_{\mathcal{E}}\triangleq\left(f_e:e\in\mathcal{E}\right)$均需满足以下不等式：

$$\begin{aligned}
f_{e_{u1}}&\geq 1 \text{ 由于割}\{e_{u1},e_{u2},e_{u3}\}\\
f_{e_{u2}}&\geq 1 \text{ 由于割}\{e_{u1},e_{u2},e_{u3}\}\\
f_{e_{u3}}&\geq 1 \text{ 由于割}\{e_{u1},e_{u2},e_{u3}\}\\
f_{e_{m1}}+f_{e_{m2}}&\geq 1 \text{ 由于割}\{e_{m1},e_{m2},e_{u2},e_{u3}\}\\
f_{e_{m3}}+f_{e_{m4}}&\geq 1 \text{ 由于割}\{e_{u1},e_{m3},e_{m4},e_{u3}\}\\
f_{e_{m5}}+f_{e_{m6}}&\geq 1 \text{ 由于割}\{e_{u1},e_{u2},e_{m5},e_{m6}\}\\
f_{e_{m1}}+f_{e_{m6}}&\geq 1 \text{ 由于割}\{e_{m1},e_{b2},e_{b3},e_{m6}\}\\
f_{e_{m1}}+f_{e_{m4}}&\geq 1 \text{ 由于割}\{e_{m1},e_{b2},e_{m4},e_{u3}\}\\
f_{e_{m3}}+f_{e_{m6}}&\geq 1 \text{ 由于割}\{e_{u1},e_{m3},e_{b3},e_{m6}\}\\
f_{e_{b1}}+f_{e_{b2}}&\geq 1 \text{ 由于割}\{e_{b1},e_{b2},e_{b3},e_{b4}\}\\
f_{e_{b1}}+f_{e_{b3}}&\geq 1 \text{ 由于割}\{e_{b1},e_{b2},e_{b3},e_{b4}\}\\
f_{e_{b1}}+f_{e_{b4}}&\geq 1 \text{ 由于割}\{e_{b1},e_{b2},e_{b3},e_{b4}\}\\
f_{e_{b2}}+f_{e_{b3}}&\geq 1 \text{ 由于割}\{e_{b1},e_{b2},e_{b3},e_{b4}\}
\end{aligned}$$

$$
\begin{aligned}
&f_{e_{b2}} + f_{e_{b4}} \ge 1 \text{ 由于割} \{e_{b1}, e_{b2}, e_{b3}, e_{b4}\} \\
&f_{e_{b3}} + f_{e_{b4}} \ge 1 \text{ 由于割} \{e_{b1}, e_{b2}, e_{b3}, e_{b4}\} \\
&f_{e_{b1}} + f_{e_{m2}} \ge 1 \text{ 由于割} \{e_{b1}, e_{m2}, e_{u2}, e_{u3}\} \\
&f_{e_{b1}} + f_{e_{m4}} \ge 1 \text{ 由于割} \{e_{b1}, e_{b2}, e_{m4}, e_{u3}\} \\
&f_{e_{b1}} + f_{e_{m6}} \ge 1 \text{ 由于割} \{e_{b1}, e_{b2}, e_{b3}, e_{m6}\} \\
&f_{e_{b2}} + f_{e_{m1}} \ge 1 \text{ 由于割} \{e_{m1}, e_{b2}, e_{b3}, e_{b4}\} \\
&f_{e_{b2}} + f_{e_{m4}} \ge 1 \text{ 由于割} \{e_{m1}, e_{b2}, e_{m4}, e_{u3}\} \\
&f_{e_{b2}} + f_{e_{m6}} \ge 1 \text{ 由于割} \{e_{m1}, e_{b2}, e_{b3}, e_{m6}\} \\
&f_{e_{b3}} + f_{e_{m1}} \ge 1 \text{ 由于割} \{e_{m1}, e_{b2}, e_{b3}, e_{b4}\} \\
&f_{e_{b3}} + f_{e_{m3}} \ge 1 \text{ 由于割} \{e_{u1}, e_{m3}, e_{b3}, e_{b4}\} \\
&f_{e_{b3}} + f_{e_{m6}} \ge 1 \text{ 由于割} \{e_{b1}, e_{b2}, e_{b3}, e_{m6}\} \\
&f_{e_{b4}} + f_{e_{m1}} \ge 1 \text{ 由于割} \{e_{m1}, e_{b2}, e_{b3}, e_{b4}\} \\
&f_{e_{b4}} + f_{e_{m3}} \ge 1 \text{ 由于割} \{e_{u1}, e_{m3}, e_{b3}, e_{b4}\} \\
&f_{e_{b4}} + f_{e_{m5}} \ge 1 \text{ 由于割} \{e_{u1}, e_{u2}, e_{m5}, e_{b4}\}
\end{aligned}
$$

其他没有列出的约束可以由以上列出的约束推得。以上不等式就刻画了区域 $\mathcal{B}_{1,\mathcal{P}(\mathcal{E},1)}$。 □

命题 4.2 证明的第 2 步（得到 $\mathcal{B}_{1,\mathcal{P}(\mathcal{E},1)}$ 的所有极点）：$\mathcal{B}_{1,\mathcal{P}(\mathcal{E},1)}$ 全部的极点如下（以 $\mathbf{f}_{\mathcal{E}} = \left(\mathbf{f}_{\mathcal{E}_u}, f_{e_{m1}}, \cdots, f_{e_{m6}}, f_{e_{b1}}, \cdots, f_{e_{b4}}\right)$ 的形式）：

$$
\begin{aligned}
\mathbf{f}_{\mathcal{E}}^{(1a)} &= (\mathbf{1}, 1,0,1,0,1,0, && 1,1,1,0) \\
\mathbf{f}_{\mathcal{E}}^{(1b)} &= (\mathbf{1}, 1,0,1,0,0,1, && 1,1,0,1) \\
\mathbf{f}_{\mathcal{E}}^{(1c)} &= (\mathbf{1}, 1,0,0,1,0,1, && 1,0,1,1) \\
\mathbf{f}_{\mathcal{E}}^{(1d)} &= (\mathbf{1}, 0,1,0,1,0,1, && 0,1,1,1) \\
\mathbf{f}_{\mathcal{E}}^{(2a)} &= (\mathbf{1}, 0.5,0.5,0.5,0.5,0,1, && 0.5,0.5,0.5,1) \\
\mathbf{f}_{\mathcal{E}}^{(2b)} &= (\mathbf{1}, 1,0,0.5,0.5,0.5,0.5, && 1,0.5,0.5,0.5) \\
\mathbf{f}_{\mathcal{E}}^{(3)} &= (\mathbf{1}, 0.5,0.5,0.5,0.5,0.5,0.5, && 0.5,0.5,0.5,0.5).
\end{aligned}
$$

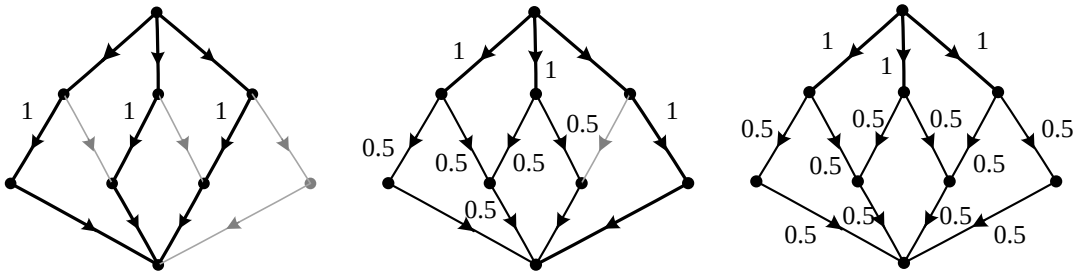
这些极点可以分为 3 类（见图 4.3）：

(第 1 类) 包括极点 $\mathbf{f}_{\mathcal{E}}^{(1a)}, \mathbf{f}_{\mathcal{E}}^{(1b)}, \mathbf{f}_{\mathcal{E}}^{(1c)}, \mathbf{f}_{\mathcal{E}}^{(1d)}$，是三条独立的链路；

(第 2 类) 包括极点 $\mathbf{f}_{\mathcal{E}}^{(2a)}, \mathbf{f}_{\mathcal{E}}^{(2b)}$，是 1 条独立的链路和一个 2-4-3 均匀摆布的链路速率；

(第 3 类) 包括极点 $\mathbf{f}_{\mathcal{E}}^{(3)}$，是 3-6-4 均匀摆布的链路速率。

在同一类中的多个极点是等价的。 □



(类型1)　(类型2)　(类型3)

图 4.3　蟑螂网络容许速率域的三类极点

命题 4.2 证明的第 3 步（证明$\mathcal{B}_{1,\mathcal{P}(\mathcal{E},1)}$的所有极点都可以渐进达到）：接下来逐类证明第 2 步列出的极点都是可以达到的。

(第 1 类) 考虑链路速率$\mathbf{f}_{\mathcal{E}}^{(1a)}$。采用重复编码+大数判决的网络纠错码显然可以达到速率$\mathbf{f}_{\mathcal{E}}^{(1a)}$，证得$\mathbf{f}_{\mathcal{E}}^{(1a)}\in\mathcal{R}$。

(第 2 类) 考虑链路速率$\mathbf{f}_{\mathcal{E}}^{(2a)}$。证明$\mathbf{f}_{\mathcal{E}}^{(2a)}\in\mathcal{R}$的基本思路如下：我们将构造一个码长为$2n$，消息集大小为$2^{2n}$的网络纠错码$\mathsf{C}_{2n}^{(2a)}$，其链路速率为$\mathbf{f}_{\mathcal{E}}^{(2a)}+\Delta\mathbf{f}_{\mathcal{E}}^{(e_{b2},n)}$，其中$\Delta\mathbf{f}_{\mathcal{E}}^{(\{e_{b2}\},n)}\triangleq\left(\Delta f_e^{(\{e_{b2}\},n)}:e\in\mathcal{E}\right)$的定义为

$$\Delta f_e^{(\{e_{b2}\},n)}\triangleq\begin{cases}\dfrac{1}{2n}\left[\log_2\left(2^n+1\right)-1\right], & e=e_{b2}\\ 0, & e\neq e_{b2}.\end{cases}\tag{4–14}$$

然后将证明这个码可以纠正$\mathcal{P}(\mathcal{E},1)$。于是$\mathbf{f}_{\mathcal{E}}^{(2a)}+\Delta\mathbf{f}_{\mathcal{E}}^{(e_{b2},n)}$是容许速率。由于

$$\lim_{n\to+\infty}\left(\mathbf{f}_{\mathcal{E}}^{(2a)}+\Delta\mathbf{f}_{\mathcal{E}}^{(e_{b2},n)}\right)=\mathbf{f}_{\mathcal{E}}^{(2a)},\tag{4–15}$$

所以$\mathbf{f}_{\mathcal{E}}^{(2a)}\in\mathcal{R}$。

码$\mathsf{C}_{2n}^{(2a)}$的构造：令$\mathcal{M}$为消息集，$\mathcal{X}_e$为$2n$次信道使用上链路$e\in\mathcal{E}$的信号集合。不失一般性，令

$$\begin{aligned}\mathcal{M}=\mathcal{X}_{e_{u1}}=\mathcal{X}_{e_{u2}}=\mathcal{X}_{e_{u3}}=\mathcal{X}_{e_{m6}}=\mathcal{X}_{e_{b4}}&=\{0,1\}^n\times\{0,1\}^n\\ \mathcal{X}_{e_{m1}}=\mathcal{X}_{e_{m2}}=\mathcal{X}_{e_{m3}}=\mathcal{X}_{e_{m4}}=\mathcal{X}_{e_{b1}}=\mathcal{X}_{e_{b3}}&=\{0,1\}^n\\ \mathcal{X}_{e_{b2}}&=\{0,1\}^n\bigcup\{\varepsilon\},\end{aligned}$$

其中ε表示指示错误存在的信号。

将消息分为两个部分，即 $M=(M',M'')$，其中 $M',M''\in\{0,1\}^n$ 是两个二进制串。在后续的记号中，X_e 和 Y_e 分别表示在信道 n 次使用范围内链路 $e\in\mathcal{E}$ 的输入和输出。

（编码器）

编码器 e_{u1}，e_{u2}，e_{u3}，e_{m6}，e_{b4}，e_{b1}，e_{b3} 直接转发收到的信号。

编码器 e_{m1} 转发从 e_{u1} 发来的信号的第 1 部分，编码器 e_{m2} 转发从 e_{u1} 发来的信号的第 2 部分，编码器 e_{m3} 转发从 e_{u2} 发来的第 1 部分，编码器 e_{m4} 发送 $Y'_{e_{u2}}\oplus Y''_{e_{u2}}$，即链路 e_{u2} 发来的两个部分信号（分别记为 $Y'_{e_{u2}}$ 和 $Y''_{e_{u2}}$）的按位异或的结果。

编码器 e_{b2} 比较从链路 e_{m2} 发来的信号（记为 $Y_{e_{m2}}$）和从链路 e_{m3} 发来的信号（记为 $Y_{e_{m3}}$）。如果 $Y_{e_{m2}}=Y_{e_{m3}}$，则编码器 e_{b2} 转发从链路 e_{m2} 发来的信号，否则编码器 e_{b2} 输出 ε。

（译码器）

$$\mathrm{Dec}\left(Y_{e_{b1}},Y_{e_{b2}},Y_{e_{b3}},Y_{e_{b4}}\right)\triangleq\begin{cases}\left(Y_{e_{b1}},Y_{e_{b2}}\right), & Y_{e_{b2}}\neq\varepsilon\text{且}Y_{e_{b1}}\oplus Y_{e_{b2}}=Y_{e_{b3}}\\ Y_{e_{b4}}, & Y_{e_{b2}}=\varepsilon\text{或}Y_{e_{b1}}\oplus Y_{e_{b2}}\neq Y_{e_{b3}}.\end{cases}$$

证明码 $\mathsf{C}_{2n}^{(2a)}$ 能纠正 $\mathcal{A}=\mathcal{P}(\mathcal{E},1)$ 错：令 $\overline{\mathcal{E}}\triangleq\{e_{u1},e_{u2},e_{m1},e_{m2},e_{m3},e_{m4},e_{b1},e_{b2},e_{b3}\}$ 且 $\mathcal{E}_p\triangleq\{e_{u3},e_{m6},e_{b4}\}$。

在网络中没有错误的时候，网络中的信号如图 4.4 所示。

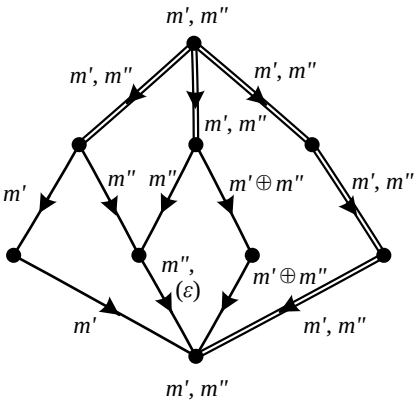


图 4.4　在无错误情况下码 $\mathsf{C}_{2n}^{(2a)}$ 的传输内容示意。其中 $\oplus$ 表示按位异或，符号 (ε) 并不是无错误情况下的传输内容，只是表示其在其他情况下传输 ε 的可能性。

接下来证明，当 $\overline{\mathcal{E}}$ 中有错时，有 $Y_{e_{b2}}=\varepsilon$ 或 $Y_{e_{b1}}\oplus Y_{e_{b2}}\neq Y_{e_{b3}}$。

考虑以下情况：

(情况 1) 在链路$e_{m1},e_{m4},e_{b1},e_{b2},e_{b3}$中的某条链路有错误。在这种情况下，有$Y_{e_{b1}}\oplus Y_{e_{b2}}\neq Y_{e_{b3}}$。

(情况 2) 在链路e_{m2},e_{m3}中的某条链路有错。在这种情况下，编码器e_{b2}会发现不匹配的情况，进而发送信号ε，使得$Y_{e_{b2}}=\varepsilon$。

(情况 3) 在链路e_{u1}上有错。这种情况下，若$Y_{e_{u1}}$的第一部分$Y'_{e_{u1}}$有错，则有$Y_{e_{b1}}\oplus Y_{e_{b2}}\neq Y_{e_{b3}}$；若$Y_{e_{u1}}$的第二部分$Y''_{e_{u1}}$有错，则有$Y_{e_{b2}}=\varepsilon$。

(情况 4) 在链路e_{u2}上有错。这种情况下，若$Y_{e_{u2}}$的第二部分$Y''_{e_{u2}}$有错，则有$Y_{e_{b2}}=\varepsilon$；若在$Y''_{e_{u2}}$正确的情况下$Y_{e_{u2}}$的第一部分有错$Y'_{e_{u2}}$，则有$Y_{e_{b2}}=\varepsilon$。

综合考虑以上情况，当$\overline{\mathcal{E}}$有一条链路出错时，必有$Y_{e_{b2}}=\varepsilon$或$Y_{e_{b1}}\oplus Y_{e_{b2}}\neq Y_{e_{b3}}$。

现在我们考虑译码器的译码结果。

(1) 如果$Y_{e_{b2}}=\varepsilon$或$Y_{e_{b1}}\oplus Y_{e_{b2}}\neq Y_{e_{b3}}$，则在$\overline{\mathcal{E}}$中必有链路错，所以在$\mathcal{E}_p$就没有错。于是可以证明$\hat{M}$是正确的。

(2) 如果$Y_{e_{b2}}\neq\varepsilon$且$Y_{e_{b1}}\oplus Y_{e_{b2}}=Y_{e_{b3}}$，则在$\overline{\mathcal{E}}$中必然无错（这时因为我们刚刚已经证明了当$\overline{\mathcal{E}}$有一条链路出错时，必有$Y_{e_{b2}}=\varepsilon$或$Y_{e_{b1}}\oplus Y_{e_{b2}}\neq Y_{e_{b3}}$），于是可以证明$\hat{M}$是正确的。

综上，我们就证明了码$\mathsf{C}_{2n}^{(2a)}$能纠任意 1 条链路错。

(第 3 类) 考虑链路速率$\mathbf{f}_{\mathcal{E}}^{(3)}$。证明$\mathbf{f}_{\mathcal{E}}^{(3)}\in\mathcal{R}$的基本思路如下：我们将用文献[8]中引理 7 的方法，构造一个码长为$2n$，消息集大小为2^{2n}的网络纠错码$\mathsf{C}_{2n}^{(3)}$，其链路速率为$\mathbf{f}_{\mathcal{E}}^{(3)}+\Delta\mathbf{f}_{\mathcal{E}}^{(\{e_{b2},e_{b3}\},n)}$，其中$\Delta\mathbf{f}_{\mathcal{E}}^{(\{e_{b2},e_{b3}\},n)}\triangleq\left(\Delta f_e^{(\{e_{b2},e_{b3}\},n)}:e\in\mathcal{E}\right)$的定义为

$$\Delta f_e^{(\{e_{b2},e_{b3}\},n)}\triangleq\begin{cases}\dfrac{1}{2n}\left\lfloor\log_2\left(2^n+1\right)-1\right\rfloor, & e\in\{e_{b2},e_{b3}\}\\ 0, & e\notin\{e_{b2},e_{b3}\}.\end{cases}\tag{4–16}$$

然后将证明这个码可以纠正$\mathcal{P}(\mathcal{E},1)$。于是$\mathbf{f}_{\mathcal{E}}^{(3)}+\Delta\mathbf{f}_{\mathcal{E}}^{(\{e_{b2},e_{b3}\},n)}$是容许速率。由于

$$\lim_{n\to+\infty}\left(\mathbf{f}_{\mathcal{E}}^{(3)}+\Delta\mathbf{f}_{\mathcal{E}}^{(\{e_{b2},e_{b3}\},n)}\right)=\mathbf{f}_{\mathcal{E}}^{(3)},\tag{4–17}$$

所以$\mathbf{f}_{\mathcal{E}}^{(3)}\in\mathcal{R}$。

为了证明的完整性，下面还是用文献[8]中引理 7 的相关方法重新构造一遍码（选入本文时有改动）。

码$\mathsf{C}_{2n}^{(3)}$的构造：令$\mathcal{M}$为消息集，$\mathcal{X}_e$为$2n$次信道使用上链路$e\in\mathcal{E}$的信号集合。不失一般性，令

$$\mathcal{M}=\mathcal{X}_{e_{u1}}=\mathcal{X}_{e_{u2}}=\mathcal{X}_{e_{u3}}=\mathbb{F}_4^n\times\mathbb{F}_4^n$$
$$\mathcal{X}_{e_{m1}}=\mathcal{X}_{e_{m2}}=\mathcal{X}_{e_{m3}}=\mathcal{X}_{e_{m4}}=\mathcal{X}_{e_{m5}}=\mathcal{X}_{e_{m6}}=\mathcal{X}_{e_{b1}}=\mathcal{X}_{e_{b4}}=\mathbb{F}_4^n$$
$$\mathcal{X}_{e_{b2}}=\mathcal{X}_{e_{b3}}=\mathbb{F}_4^n\bigcup\{\varepsilon\},$$

其中$\mathbb{F}_4$是大小为 4 的有限域，ε是表示错误存在的信号。

将消息M分为两个部分，即$M=(M',M'')$，其中$M',M''\in\mathbb{F}_4^n$是两个四进制串。

（编码器）

编码器e_{u1}，e_{u2}，e_{u3}，e_{b1}，e_{b4}直接转发收到的信号。

编码器e_{m1}输出$Y'_{e_{u1}}+Y''_{e_{u1}}$；编码器e_{m2}输出$Y'_{e_{u1}}$；编码器e_{m3}输出$Y'_{e_{u2}}$；编码器e_{m4}输出$Y''_{e_{u2}}$；编码器e_{m5}输出$Y''_{e_{u3}}$；编码器e_{m6}输出$Y'_{e_{u3}}+2Y''_{e_{u3}}$。这里的加法和乘法都是在有限域$\mathbb{F}_4$里的运算。

编码器e_{b2}和编码器e_{b3}：

$$\mathrm{Enc}_{e_{b2}}\left(Y_{e_{m2}},Y_{e_{m3}}\right)\triangleq\begin{cases}Y_{e_{m3}}, & Y_{e_{m2}}=Y_{e_{m3}}\\ \varepsilon, & Y_{e_{m2}}\neq Y_{e_{m3}}.\end{cases}$$
$$\mathrm{Enc}_{e_{b3}}\left(Y_{e_{m4}},Y_{e_{m5}}\right)\triangleq\begin{cases}Y_{e_{m4}}, & Y_{e_{m4}}=Y_{e_{m5}}\\ \varepsilon, & Y_{e_{m4}}\neq Y_{e_{m5}}.\end{cases}$$

（译码器）

译码器的行为分为以下四种情况：

(情况 1)　$y_{e_{b2}}=\varepsilon$且$y_{e_{b3}}=\varepsilon$。这时，从$y_{e_{b1}}$和$y_{e_{b4}}$译码得到$\hat{m}$；

(情况 2)　$y_{e_{b2}}=\varepsilon$且$y_{e_{b3}}\neq\varepsilon$。这时，从$y_{e_{b3}}$和$y_{e_{b4}}$译码得到$\hat{m}$；

(情况 3)　$y_{e_{b2}}\neq\varepsilon$且$y_{e_{b3}}=\varepsilon$。这时，从$y_{e_{b1}}$和$y_{e_{b2}}$译码得到$\hat{m}$；

(情况 4)　$y_{e_{b2}}\neq\varepsilon$且$y_{e_{b3}}\neq\varepsilon$。这时，使用$(4,2)$最大距离可分码译码器对$y_{e_{b1}},y_{e_{b2}},y_{e_{b3}}$，$y_{e_{b4}}$进行译码。

证明码$\mathsf{C}_{2n}^{(3)}$能纠正$\mathcal{A}=\mathcal{P}(\mathcal{E},1)$错：当网络中没有错误的时候，各链路上的信号如图 4.5 所示。

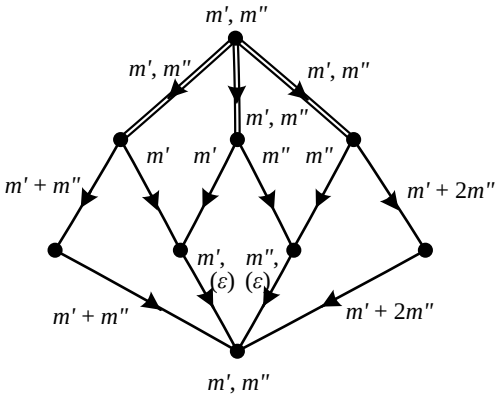
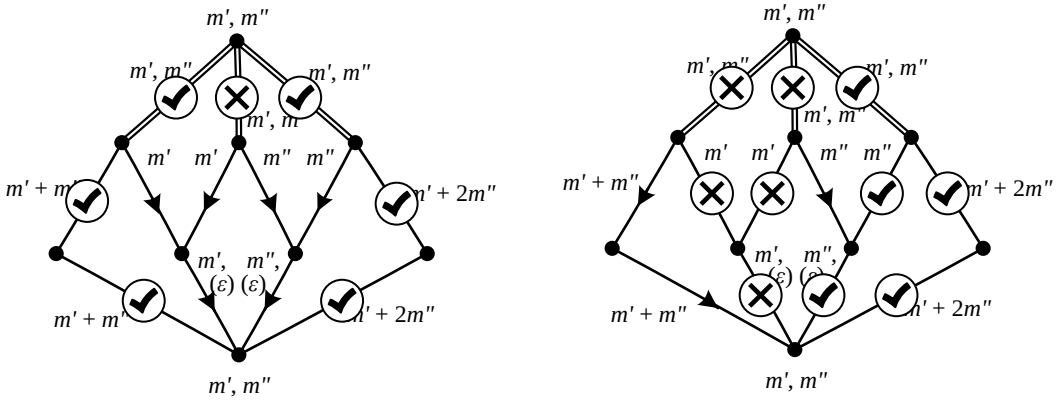


图 4.5　在无错误情况下码 $\mathsf{C}_{2n}^{(3)}$ 的传输内容示意。其中加法和乘法都是 $\mathbb{F}_4$ 上的运算，符号 (ε) 并不是无错误情况下的传输内容，只是表示其在其他情况下传输 ε 的可能性



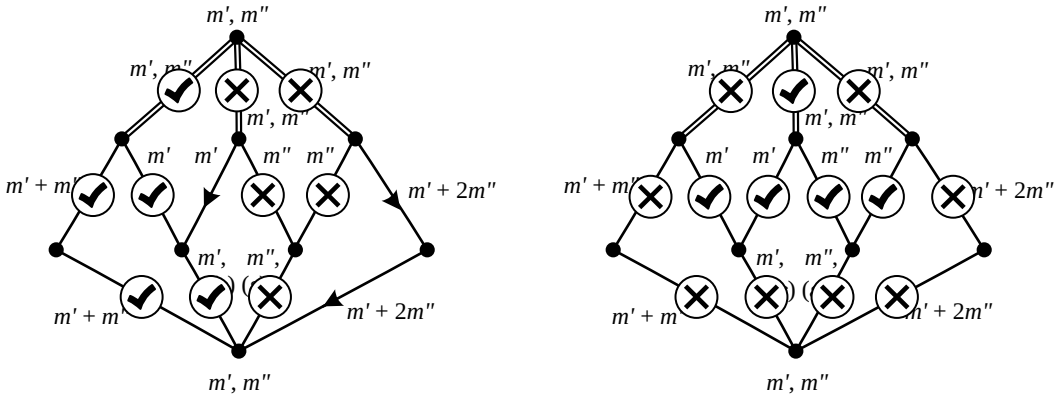


图 4.6　译码器接收的 4 种情况，
其中 √ 表示一定正确传输的链路，× 表示可能错误传输的链路

考虑以下情况（见图 4.6）：

(情况 1) $Y_{e_{b2}}=\varepsilon$ 且 $Y_{e_{b3}}=\varepsilon$。这种情况下，我们可以证明在链路 e_{u2} 上有错误（略）。所以在链路 e_{u1}，e_{u3}，e_{m1}，e_{m6}，e_{b1}，e_{b4} 上传输的信号都是正确的。所以，$Y_{b1}=M'+M''$ 且 $Y_{b4}=M'+2M''$，进而可以正确译出 $\hat{M}$。

(情况 2) $Y_{e_{b2}}=\varepsilon$ 且 $y_{e_{b3}}\neq\varepsilon$。这种情况下，我们可以证明链路 $e_{u1},e_{u2},e_{m2},e_{m3},e_{b2}$ 中的某条链路有错误（略）。进而知道，链路 e_{u3}，e_{m5}，e_{m6}，e_{b3}，e_{b4} 上的信号都是对的。于是，$Y_{b3}=M''$ 且 $Y_{b4}=M'+2M''$，可以正确译出 $\hat{M}$。

(情况 3) $Y_{e_{b2}}\neq\varepsilon$ 且 $Y_{e_{b3}}=\varepsilon$。这种情况下，我们可以证明在链路 $e_{u2},e_{u3},e_{m4},e_{m5},e_{b3}$ 中的某条链路存在错误。进而可以知道，链路 e_{u1}，e_{m1}，e_{m2}，e_{b1}，e_{b2} 上的信号都是正确的。所以 $Y_{b1}=M'+M''$ 且 $Y_{b2}=M'$，于是可以正确译出 $\hat{M}$。

(情况 4) $Y_{e_{b2}}\neq\varepsilon$ 且 $Y_{e_{b3}}\neq\varepsilon$。这种情况下，我们可以证明在链路 $e_{u1},e_{u3},e_{m1},e_{m6},e_{b1},e_{b2},e_{b3},e_{b4}$ 中的某条链路存在错误。进而可以知道，$\left(y_e,e\in\mathcal{E}_b\right)$ 这 4 条链路上最多有一条链路的信号和无错误时的信号不一样。由于信号 $\left(Y_e,e\in\mathcal{E}_b\right)$ 组成了 $(4,2)$ 最大距离可分码，所以我们可以使用最大距离可分码译码器来无误恢复 $\hat{M}$。

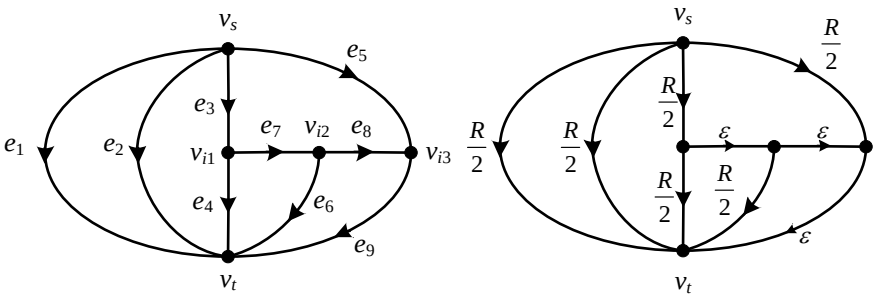
这样我们就证明了码 $\mathsf{C}_{2n}^{(3)}$ 能够对抗任意一条链路错误。　□

4.2.4 容许速率域割集外界的紧性和信息支配外界

前面我们证明了定理 4.3 提供的割集外界是所有基于割的外界中最紧的界。本节将进一步讨论这个界的紧性。

例 4.4：如图 4.7 (a) 的网络中，$\mathcal{A}=\mathcal{P}\left(\mathcal{E},1\right)$，消息速率 $R>0$。考虑图 4.7 (b) 中的流 $\mathbf{f}_{\mathcal{E}}\triangleq\left(f_e:e\in\mathcal{E}\right)$：

$$f_e\triangleq\begin{cases}\dfrac{1}{2}R, & e\in\{e_1,e_2,\cdots,e_6\}\\ \varepsilon, & e\in\{e_7,e_8,e_9\},\end{cases}\qquad(4\text{–}18)$$



(a) 示例网络　　(b) 一个非容许速率

图 4.7　一个容许速率域割集外界不紧的例子

其中 ε 是非常小的正实数，满足 $\varepsilon \ll \frac{1}{4}R$。可以验证 $\mathbf{f}_{\mathcal{E}} \in \mathcal{B}_{R,\mathcal{A}}$。

对于中间节点 v_{i2}，其唯一的输入信号流是链路 e_7 上的 ε 流，链路 e_7 上的信号完全决定了链路 e_6 上的信号。所以链路 e_6 上至多承载含有 ε 信息的信号。再考虑割 $\{e_1, e_2, e_4, e_6, e_9\}$，这时支持的消息速率就不会超过 $\frac{1}{2}R + 2\varepsilon$。考虑到 $\varepsilon \ll \frac{1}{4}R$，在这个链路速率上不可能达到速率 R，即

$$\mathbf{f}_{\mathcal{E}} \notin \mathcal{R}. \tag{4–19}$$

所以在这个例子中割集外界不紧。 □

在这个例子中仍然使用了第 4.1.4 节提到的信息支配原理。从容许速率域的角度看，信息支配原理刻画了容许速率域的边界。

定理 4.5（容许速率域的信息支配）：给定 $\mathcal{G}$、$\mathcal{A}$ 和消息速率 R。容许速率域的边界为 $\partial\mathcal{R}$。对任意的链路速率 $\mathbf{f}_{\mathcal{E}} \in \partial\mathcal{R}$ 和 $e \in \mathcal{E} \setminus \mathrm{Out}(v_s)$，有

$$f_e \le \left\| \mathbf{f}_{\mathrm{In}(\mathrm{Tail}(e))} \right\|. \qquad \square$$

证明：用反证法。假设存在 $\mathbf{f}_{\mathcal{E}} \in \partial\mathcal{R}$ 和 $\bar{e} \in \mathcal{E} \setminus \mathrm{Out}(v_s)$ 满足 $f_{\bar{e}} > \left\| \mathbf{f}_{\mathrm{In}(\mathrm{Tail}(\bar{e}))} \right\|$。记 $\bar{v} \triangleq \mathrm{Tail}(\bar{e})$，$\tilde{v} \triangleq \mathrm{Head}(\bar{e})$。定义新流 $\mathbf{f}'_{\mathcal{E}} \triangleq (f'_e : e \in \mathcal{E})$

$$f'_e \triangleq \begin{cases} f_e, & e \ne \bar{e} \\ \left\| \mathbf{f}_{\mathrm{In}(\bar{v})} \right\|, & e = \bar{e}. \end{cases} \tag{4–20}$$

在新流 $\mathbf{f}'_{\mathcal{E}}$ 上的网络纠错码总是将节点 $\bar{v}$ 收到的所有信号全部在链路 $\bar{e}$ 上转发。这样，如果链路 e 不被控制，则 $\tilde{v}$ 可以收到 $\mathbf{f}_{\mathrm{In}(\bar{v})}$ 上的所有信号。可以证明（从略），$\mathbf{f}'_{\mathcal{E}} \in \mathcal{R}$。所以 $\mathbf{f}_{\mathcal{E}} \notin \partial\mathcal{R}$，得到矛盾。 □

4.3 三节点网络的信道容量

本节的研究结果将针对单发单收的三节点网络的信道容量。具体而言，本节首先介绍什么是三节点网络，然后推导得到三节点网络的一些信道容量下界，包括：包装猜测转发下界、路由猜测转发下界、译码猜测转发下界、路由猜测转发-译码猜测转发第 1 下界、路由猜测转发-译码猜测转发第 2 下界。最后给出一些三节点网络的数值例子。在这些例子中，有些例子的信道容量已经完全求出，有些例子的信道容量并没有完全求出。

下面介绍什么是三节点网络。三节点网络是有且只有三个节点的网络，网络上只有一个单播业务。三个节点分别是源节点 v_s、目的节点 v_t 和中继节点 v_r。任意两个节点之间可能没有链路，也可能有一条或多条链路。

为了分析简单，仅考虑 $\mathcal{A}=\mathcal{P}(\mathcal{E},z)$。

4.3.1 包装猜测转发下界

定理 4.6（包装猜测转发下界）：三节点网络中，$\mathcal{A}=\mathcal{P}(\mathcal{E},z)$。则纠错容量有以下下界：若 $|\mathcal{E}_{sr}|+|\mathcal{E}_{st}|\le 2z$ 或 $n_{rt}\le 2z$，则 $C\ge 0$；否则

$$C\ge \max_{\lambda\ge 0:\Sigma_0^{(1)}\left(\min\left\{\mathbf{f}_{\mathcal{E}_{sr}},\lambda\mathbf{1}_{\mathcal{E}_{sr}}\right\}\right)\le\Sigma_{n_{z,rt}}^{(1)}\left(\mathbf{f}_{\mathcal{E}_{rt}}\right)}\Sigma_{n_{z,st}}^{(1)}\left(\begin{bmatrix}\mathbf{f}_{\mathcal{E}_{st}}\\ \min\left\{\mathbf{f}_{\mathcal{E}_{sr}},\lambda\mathbf{1}_{\mathcal{E}_{sr}}\right\}\end{bmatrix}\right) \tag{4–21}$$

其中 $n_{z,st}\triangleq\max\left\{z,2\left(z-|\mathcal{E}_{ts}|\right)\right\}$ 且 $n_{z,rt}\triangleq\max\left\{z,2\left(z-|\mathcal{E}_{tr}|\right)\right\}$。 □

证明：下面给出在下界不为 0 时下界的达到方法。

链路速率分割：首先计算参数 λ。$\lambda\ge 0$ 是一个注水参数，它在链路 $\mathcal{E}_{sr}$ 上进行注水，注水的总和是 v_r 到 v_t 的纠错容量 $\Sigma_{n_{z,rt}}^{(1)}\left(\mathbf{f}_{\mathcal{E}_{rt}}\right)$。注水后 $\mathcal{E}_{sr}$ 上的速率为 $\min\left\{\mathbf{f}_{\mathcal{E}_{sr}},\lambda\mathbf{1}_{\mathcal{E}_{sr}}\right\}$。考虑子流 $\begin{bmatrix}\mathbf{f}_{\mathcal{E}_{st}\cup\mathcal{E}_{ts}}\\ \min\left\{\mathbf{f}_{\mathcal{E}_{sr}},\lambda\mathbf{1}_{\mathcal{E}_{sr}}\right\}\\ \mathbf{0}_{\mathcal{E}_{rs}}\\ \mathbf{0}_{\mathcal{E}_{rt}\cup\mathcal{E}_{tr}}\end{bmatrix}$ 和 $\begin{bmatrix}\mathbf{0}_{\mathcal{E}_{st}\cup\mathcal{E}_{ts}}\\ \mathbf{0}_{\mathcal{E}_{sr}}\\ \mathbf{0}_{\mathcal{E}_{rs}}\\ \mathbf{f}_{\mathcal{E}_{rt}\cup\mathcal{E}_{tr}}\end{bmatrix}$，显然有

$$\begin{bmatrix}\mathbf{f}_{\mathcal{E}_{st}\cup\mathcal{E}_{ts}}\\ \min\left\{\mathbf{f}_{\mathcal{E}_{sr}},\lambda\mathbf{1}_{\mathcal{E}_{sr}}\right\}\\ \mathbf{0}_{\mathcal{E}_{rs}}\\ \mathbf{0}_{\mathcal{E}_{rt}\cup\mathcal{E}_{tr}}\end{bmatrix}+\begin{bmatrix}\mathbf{0}_{\mathcal{E}_{st}\cup\mathcal{E}_{ts}}\\ \mathbf{0}_{\mathcal{E}_{sr}}\\ \mathbf{0}_{\mathcal{E}_{rs}}\\ \mathbf{f}_{\mathcal{E}_{rt}\cup\mathcal{E}_{tr}}\end{bmatrix}\le\begin{bmatrix}\mathbf{f}_{\mathcal{E}_{st}\cup\mathcal{E}_{ts}}\\ \mathbf{f}_{\mathcal{E}_{sr}}\\ \mathbf{f}_{\mathcal{E}_{rs}}\\ \mathbf{f}_{\mathcal{E}_{rt}\cup\mathcal{E}_{tr}}\end{bmatrix}. \tag{4–22}$$

码分配：(步骤 1) 源节点 v_s 将中继节点 v_r 和目的节点 v_t 视为一体，向 $\{v_r,v_t\}$ 发送最大距离可分码。前向流为 $\begin{bmatrix}\mathbf{f}_{\mathcal{E}_{st}}\\ \min\left\{\mathbf{f}_{\mathcal{E}_{sr}},\lambda\mathbf{1}_{\mathcal{E}_{sr}}\right\}\end{bmatrix}$，反向流为 $\mathbf{f}_{\mathcal{E}_{ts}}$。

(步骤 2) 使用流 $\mathbf{f}_{\mathcal{E}_{rt}\cup\mathcal{E}_{tr}}$，构造消息速率为 $\Sigma_{n_{z,rt}}^{(1)}\left(\mathbf{f}_{\mathcal{E}_{rt}}\right)$ 的猜想转发码。中继节点 v_r 将收到的所有信号重新编码（这可以视为一种“包装”过程），再用猜测转发码发给目的节点 v_t。 □

下面给出定理 4.6 中下界紧的充分条件。

命题 4.3：在定理 4.6 中，当 $\Sigma_0^{(1)}\left(\mathbf{f}_{\mathcal{E}_{sr}}\right)\le\Sigma_{n_{z,rt}}^{(1)}\left(\mathbf{f}_{\mathcal{E}_{rt}}\right)$ 且 $\mathcal{E}_{rs}=\varnothing$ 时，定理 4.6 给出的下界紧。 □

证明：当$\Sigma_0^{(1)}\left(\mathbf{f}_{\mathcal{E}_{sr}}\right)\le\Sigma_{n_{z,rt}}^{(1)}\left(\mathbf{f}_{\mathcal{E}_{rt}}\right)$时，对任意的正实数$\lambda>0$，均有

$$\Sigma_0^{(1)}\left(\min\left\{\mathbf{f}_{\mathcal{E}_{sr}},\lambda\mathbf{1}_{\mathcal{E}_{sr}}\right\}\right)\le\Sigma_{n_{z,rt}}^{(1)}\left(\mathbf{f}_{\mathcal{E}_{rt}}\right). \tag{4–23}$$

于是包装猜测转发下界为$\Sigma_{n_{z,st}}^{(1)}\left(\begin{bmatrix}\mathbf{f}_{\mathcal{E}_{st}}\\ \mathbf{f}_{\mathcal{E}_{sr}}\end{bmatrix}\right)$。

在割$\mathcal{E}_c\left(\{v_s\}\right)$上使用割集上界，得到纠错容量上界也为$\Sigma_{n_{z,st}}^{(1)}\left(\begin{bmatrix}\mathbf{f}_{\mathcal{E}_{st}}\\ \mathbf{f}_{\mathcal{E}_{sr}}\end{bmatrix}\right)$。这说明了包装猜测转发下界就是纠错容量。 □

4.3.2 路由猜测转发下界

定理 4.7（路由猜测转发下界）：三节点网络中，$\mathcal{A}=\mathcal{P}(\mathcal{E},z)$。则纠错容量有以下下界：若$|\mathcal{E}_{st}|+\min\left\{|\mathcal{E}_{sr}|,|\mathcal{E}_{rt}|\right\}\le 2z$，则$C=0$；否则

$$C\ge\min_{n_{zt}+n_{zr}\le n_z'}\left(\Sigma_{n_{zt}}^{(1)}\left(\mathbf{f}_{\mathcal{E}_{st}}\right)+\Sigma_{n_{zr}}^{(2)}\left(\mathbf{f}_{\mathcal{E}_{sr}},\mathbf{f}_{\mathcal{E}_{rt}}\right)\right), \tag{4–24}$$

其中$n_z'\triangleq\max\left\{z,2\left(z-|\mathcal{E}_{ts}|-\min\left\{|\mathcal{E}_{tr}|,|\mathcal{E}_{rs}|\right\}\right)\right\}$。 □

证明：下面给出在下界不为 0 时下界的达到方法。达到的基本思路是，中继节点v_r将接收到的信号转发给目的节点v_t，这样从v_s经v_r到v_t可能有$|\mathcal{E}_{sr}|\times|\mathcal{E}_{rt}|$个子流。让矩阵$\mathbf{X}_{\mathcal{E}_{sr},\mathcal{E}_{rt}}\triangleq\left(x_{e_{sr},e_{rt}}:e_{sr}\in\mathcal{E}_{sr},e_{rt}\in\mathcal{E}_{rt}\right)$表示这些子流，其中$x_{e_{sr},e_{rt}}$表示从链路$e_{sr}\in\mathcal{E}_{sr}$转发到链路$e_{rt}\in\mathcal{E}_{rt}$的流量。这$|\mathcal{E}_{sr}|\times|\mathcal{E}_{rt}|$个子流和从$v_s$不经过$v_r$直接到$v_t$的流$\mathbf{f}_{\mathcal{E}_{st}}$一起，来支持猜测转发码。

接下来推导对于特定的$\mathbf{X}_{\mathcal{E}_{sr},\mathcal{E}_{rt}}$和$\mathbf{f}_{\mathcal{E}_{st}}$，猜测转发码的消息速率。在$\mathbf{X}_{\mathcal{E}_{sr},\mathcal{E}_{rt}}$和$\mathbf{f}_{\mathcal{E}_{st}}$上使用猜测转发与在两节点网络上使用猜测转发（详见引理 4.6 的证明）相比，在第一个子流（引理 4.6 的证明中的$\begin{pmatrix}\mathbf{f}_{\mathcal{E}_+}-\delta_+\mathbf{1}_{\mathcal{E}_+}\\ \mathbf{0}_{\mathcal{E}_-}\end{pmatrix}$）不再是互相独立。为了让猜测转发码依然有效，仍需要在第 1 个子流处检出任意z个错误，并纠正$\max\left\{z-|\mathcal{E}_{ts}|-\min\left\{|\mathcal{E}_{tr}|,|\mathcal{E}_{rs}|\right\},0\right\}$个错误。这里$|\mathcal{E}_{ts}|+\min\left\{|\mathcal{E}_{tr}|,|\mathcal{E}_{rs}|\right\}$是从目的节点$v_t$到源节点$v_s$可以找到的独立路径数，正是猜想转发码第 2 个子流的路径数。为了在第 1 个子流达到上述功能，需要$\mathbf{X}_{\mathcal{E}_{sr}\times\mathcal{E}_{rt}}$和$\mathbf{f}_{\mathcal{E}_{st}}$需要满足以下条件：在$\mathbf{f}_{\mathcal{E}_{st}}$中删去若干流（记删去的流数为$n_{zt}$），再在$\mathbf{X}_{\mathcal{E}_{sr}\times\mathcal{E}_{rt}}$中删去若干行、若干列（记删去的行数和列数之和为$n_{zr}$）。若$n_{zt}+n_{zr}\le n_z'$，则剩下的部分的和均要大于消息速率。用这个条件，可以从一个矩阵$\mathbf{X}_{\mathcal{E}_{sr}\times\mathcal{E}_{rt}}$的取值得到一个消息速率，为

$$\min_{n_{zt}+n_{zr}\le n_z'}\left(\Sigma_{n_{zt}}^{(1)}\left(\mathbf{f}_{\mathcal{E}_{st}}\right)+\Sigma_{n_{zr}}^{(2)}\left(\mathbf{X}_{\mathcal{E}_{sr}\times\mathcal{E}_{rt}}\mathbf{1}_{\mathcal{E}_{rt}},\mathbf{X}_{\mathcal{E}_{sr}\times\mathcal{E}_{rt}}^T\mathbf{1}_{\mathcal{E}_{sr}}\right)\right). \tag{4–25}$$

接着，可以通过优化矩阵 $\mathbf{X}_{\mathcal{E}_{sr}\times\mathcal{E}_{rt}}$ 来使达到的消息速率尽量大。注意到矩阵 $\mathbf{X}_{\mathcal{E}_{sr}\times\mathcal{E}_{rt}}$ 应当满足 $\mathbf{X}_{\mathcal{E}_{sr},\mathcal{E}_{rt}}\mathbf{1}_{\mathcal{E}_{rt}}\le\mathbf{f}_{\mathcal{E}_{sr}}$ 和 $\mathbf{X}^{T}_{\mathcal{E}_{sr},\mathcal{E}_{rt}}\mathbf{1}_{\mathcal{E}_{sr}}\le\mathbf{f}_{\mathcal{E}_{rt}}$。所以经过优化后得到的消息速率为

$$\min_{n_{zt}+n_{zr}\le n'_z}\left(\Sigma^{(1)}_{n_{zt}}\left(\mathbf{f}_{\mathcal{E}_{st}}\right)+\Sigma^{(2)}_{n_{zr}}\left(\mathbf{f}_{\mathcal{E}_{sr}},\mathbf{f}_{\mathcal{E}_{rt}}\right)\right). \tag{4–26}$$

下界得证。 □

下面考虑定理 4.7 给出的下界紧的一些充分条件。不失一般性，仅考虑下界不为 0 的情况。这时有 $|\mathcal{E}_{st}|+|\mathcal{E}_{sr}|>2z$ 且 $|\mathcal{E}_{st}|+|\mathcal{E}_{rt}|>2z$。

命题 4.4：在定理 4.7 中，当 $|\mathcal{E}_{sr}|=|\mathcal{E}_{rt}|=1$ 且 $|\mathcal{E}_{rs}|=|\mathcal{E}_{tr}|$ 时，定理 4.7 给出的下界紧。 □

证明：在这种情况下，记 e_{sr} 为 $\mathcal{E}_{st}$ 的唯一元素，记 e_{rt} 为 $\mathcal{E}_{rt}$ 的唯一元素。仅需考虑 n_{zr} 取值为 0 或 1 的情况。

当 $n_{zr}=0$ 时，$n_{rt}=n'_z$。考虑到 $\Sigma^{(2)}_0\left(\mathbf{f}_{\mathcal{E}_{sr}},\mathbf{f}_{\mathcal{E}_{rt}}\right)=\min\left\{f_{e_{sr}},f_{e_{rt}}\right\}$，下界为

$$\min\left\{f_{e_{sr}},f_{e_{rt}}\right\}+\Sigma^{(1)}_{n'_z}\left(\mathbf{f}_{\mathcal{E}_{st}}\right).$$

当 $n_{zr}=1$ 时，$n_{rt}=n'_z-1$。考虑到 $\Sigma^{(2)}_1\left(\mathbf{f}_{\mathcal{E}_{sr}},\mathbf{f}_{\mathcal{E}_{rt}}\right)=0$，下界为 $\Sigma^{(1)}_{n'_z-1}\left(\mathbf{f}_{\mathcal{E}_{st}}\right)$。综合以上两种情况，得到路由猜测转发下界为

$$\min\left\{\min\left\{f_{e_{sr}},f_{e_{rt}}\right\}+\Sigma^{(1)}_{n'_z}\left(\mathbf{f}_{\mathcal{E}_{st}}\right),\Sigma^{(1)}_{n'_z-1}\left(\mathbf{f}_{\mathcal{E}_{st}}\right)\right\}. \tag{4–27}$$

另外，注意到命题 4.1，考虑割集 $\mathcal{E}_c\left(\{v_s\}\right)$ 可以得到割集上界

$$\Sigma^{(1)}_{n_{z,s}}\left(\begin{bmatrix}\mathbf{f}_{\mathcal{E}_{st}}\\ f_{e_{sr}}\end{bmatrix}\right)=\min\left\{f_{e_{sr}}+\Sigma^{(1)}_{n'_z}\left(\mathbf{f}_{\mathcal{E}_{st}}\right),\Sigma^{(1)}_{n'_z-1}\left(\mathbf{f}_{\mathcal{E}_{st}}\right)\right\}, \tag{4–28}$$

考虑割集 $\mathcal{E}_c\left(\{v_s,v_r\}\right)$ 可以得到割集上界

$$\Sigma^{(1)}_{n_{z,t}}\left(\begin{bmatrix}\mathbf{f}_{\mathcal{E}_{st}}\\ f_{e_{rt}}\end{bmatrix}\right)=\min\left\{f_{e_{st}}+\Sigma^{(1)}_{n'_z}\left(\mathbf{f}_{\mathcal{E}_{st}}\right),\Sigma^{(1)}_{n'_z-1}\left(\mathbf{f}_{\mathcal{E}_{st}}\right)\right\}. \tag{4–29}$$

综合考虑以上两个上界，可以得到上界为

$$\min\left\{\min\left\{f_{e_{sr}},f_{e_{rt}}\right\}+\Sigma^{(1)}_{n'_z}\left(\mathbf{f}_{\mathcal{E}_{st}}\right),\Sigma^{(1)}_{n'_z-1}\left(\mathbf{f}_{\mathcal{E}_{st}}\right)\right\}. \tag{4–30}$$

所以路由猜测转发下界和割集上界相等。 □

命题 4.5：在定理 4.7 中，当 $|\mathcal{E}_{sr}|,|\mathcal{E}_{rt}|,|\mathcal{E}_{st}|\le 2$ 且 $\mathcal{E}_{rs}=\mathcal{E}_{tr}=\mathcal{E}_{ts}=\varnothing$ 时，定理 4.7 给出的下界紧。 □

证明：由于 $\min\left\{|\mathcal{E}_{sr}|,|\mathcal{E}_{rt}|\right\}+|\mathcal{E}_{st}|\le 4$，可以验证，当 $z\ge 2$ 时容量为 0。另外，$z=0$ 是平凡的情形。所以下面只考虑 $z=1$。这时需要 $|\mathcal{E}_{sr}|=|\mathcal{E}_{rt}|=|\mathcal{E}_{st}|=2$ 考虑以下两种情况：

考虑到割集上界（命题 4.1），仅在$\min\{|\mathcal{E}_{sr}|,|\mathcal{E}_{rt}|\}+|\mathcal{E}_{st}|\geq 2z+1$时割集上界才不为 0。不失一般性，仅考虑割集上界不为 0 的情况，这时有$z\leq 1$。另外，$z=0$是平凡的情形。所以下面只考虑$z=1$。这时还要求$\min\{|\mathcal{E}_{sr}|,|\mathcal{E}_{rt}|\}+|\mathcal{E}_{st}|\geq 3$。

(情况 1) $|\mathcal{E}_{sr}|=|\mathcal{E}_{rt}|=|\mathcal{E}_{st}|=2$。这时，记$\mathcal{E}_{sr}=\{e_{sr1},e_{sr2}\}$，$\mathcal{E}_{rt}=\{e_{rt1},e_{rt2}\}$，$\mathcal{E}_{st}=\{e_{st1},e_{st2}\}$。由于$|\mathcal{E}_{st}|=2$，仅需考虑$n_{zt}=0,1,2$的情况。

下面证明$\Sigma_0^{(2)}\left(\mathbf{f}_{\mathcal{E}_{sr}},\mathbf{f}_{\mathcal{E}_{rt}}\right)=\min\left\{\left\|\mathbf{f}_{\mathcal{E}_{sr}}\right\|,\left\|\mathbf{f}_{\mathcal{E}_{rt}}\right\|\right\}$。分$\left\|\mathbf{f}_{\mathcal{E}_{sr}}\right\|\leq\left\|\mathbf{f}_{\mathcal{E}_{rt}}\right\|$和$\left\|\mathbf{f}_{\mathcal{E}_{sr}}\right\|>\left\|\mathbf{f}_{\mathcal{E}_{rt}}\right\|$两种情况考虑。当$\left\|\mathbf{f}_{\mathcal{E}_{sr}}\right\|\leq\left\|\mathbf{f}_{\mathcal{E}_{rt}}\right\|$时，$f_{e_{sr1}}+f_{e_{sr2}}\leq f_{e_{rt1}}+f_{e_{rt2}}$，所以

$$f_{e_{sr1}}-f_{e_{rt1}}\leq f_{e_{rt2}}-f_{e_{sr2}}$$
$$f_{e_{sr2}}-f_{e_{rt2}}\leq f_{e_{rt1}}-f_{e_{sr1}},$$

进而

$$\max\left\{f_{e_{sr1}}-f_{e_{rt1}},0\right\}\leq\max\left\{f_{e_{rt2}}-f_{e_{sr2}},0\right\}$$
$$\max\left\{f_{e_{sr2}}-f_{e_{rt2}},0\right\}\leq\max\left\{f_{e_{rt1}}-f_{e_{sr1}},0\right\}.$$

考虑到对任意的两个实数χ_1,χ_2有$\min(\chi_1,\chi_2)+\max\{\chi_1-\chi_2,0\}=\chi_1$[①]，所以

$$\min\left\{f_{e_{sr1}},f_{e_{rt1}}\right\}+\max\left\{f_{e_{sr1}}-f_{e_{rt1}},0\right\}=f_{e_{sr1}}$$
$$\max\left\{f_{e_{sr2}}-f_{e_{rt2}},0\right\}+\min\left\{f_{e_{sr2}},f_{e_{rt2}}\right\}=f_{e_{sr2}}$$
$$\min\left\{f_{e_{sr1}},f_{e_{rt1}}\right\}+\max\left\{f_{e_{sr2}}-f_{e_{rt2}},0\right\}\leq\min\left\{f_{e_{sr1}},f_{e_{rt1}}\right\}+\max\left\{f_{e_{rt1}}-f_{e_{sr1}},0\right\}=f_{e_{rt1}}$$
$$\max\left\{f_{e_{sr1}}-f_{e_{rt1}},0\right\}+\min\left\{f_{e_{sr2}},f_{e_{rt2}}\right\}\leq\max\left\{f_{e_{rt2}}-f_{e_{sr2}},0\right\}+\min\left\{f_{e_{sr2}},f_{e_{rt2}}\right\}=f_{e_{rt2}}$$

故矩阵

$$\mathbf{X}\triangleq\begin{pmatrix}\min\left\{f_{e_{sr1}},f_{e_{rt1}}\right\} & \max\left\{f_{sr1}-f_{rt1},0\right\}\\ \max\left\{f_{e_{sr2}}-f_{e_{rt2}},0\right\} & \min\left\{f_{e_{sr2}},f_{e_{rt2}}\right\}\end{pmatrix}\tag{4–31}$$

满足$\mathbf{X}\mathbf{1}_{\mathcal{E}_{rt}}\leq\mathbf{f}_{\mathcal{E}_{sr}}$和$\mathbf{X}^T\mathbf{1}_{\mathcal{E}_{sr}}\leq\mathbf{f}_{\mathcal{E}_{rt}}$，且$\|\mathbf{X}\|=\left\|\mathbf{f}_{\mathcal{E}_{rt}}\right\|$。类似的，当$\left\|\mathbf{f}_{\mathcal{E}_{sr}}\right\|>\left\|\mathbf{f}_{\mathcal{E}_{rt}}\right\|$时，矩阵$\mathbf{X}$也满足$\mathbf{X}\mathbf{1}_{\mathcal{E}_{rt}}\leq\mathbf{f}_{\mathcal{E}_{sr}}$和$\mathbf{X}^T\mathbf{1}_{\mathcal{E}_{sr}}\leq\mathbf{f}_{\mathcal{E}_{rt}}$，且$\|\mathbf{X}\|=\left\|\mathbf{f}_{\mathcal{E}_{sr}}\right\|$。易知

$$\Sigma_0^{(2)}\left(\mathbf{f}_{\mathcal{E}_{sr}},\mathbf{f}_{\mathcal{E}_{rt}}\right)=\min\left\{\left\|\mathbf{f}_{\mathcal{E}_{sr}}\right\|,\left\|\mathbf{f}_{\mathcal{E}_{rt}}\right\|\right\}.\tag{4–32}$$

另外，还可以知道

① 该恒等式很可能已经被之前的学者发现了。但是由于其非常简单，所以难以追溯其文献来源。

$$\Sigma_0^{(1)}\left(\mathbf{f}_{\mathcal{E}_{st}}\right)=\left\|\mathbf{f}_{\mathcal{E}_{st}}\right\|$$
$$\Sigma_1^{(1)}\left(\mathbf{f}_{\mathcal{E}_{st}}\right)=\min\left\{f_{e_{st1}},f_{e_{st2}}\right\}$$
$$\Sigma_2^{(1)}\left(\mathbf{f}_{\mathcal{E}_{st}}\right)=0$$
$$\Sigma_1^{(2)}\left(\mathbf{f}_{\mathcal{E}_{sr}},\mathbf{f}_{\mathcal{E}_{rt}}\right)=\min\left\{f_{e_{sr1}},f_{e_{sr2}},f_{e_{rt1}},f_{e_{rt2}}\right\}$$
$$\Sigma_2^{(2)}\left(\mathbf{f}_{\mathcal{E}_{sr}},\mathbf{f}_{\mathcal{E}_{rt}}\right)=0.$$

所以路由猜测转发下界为

$$\min\left\{\Sigma_2^{(2)}\left(\mathbf{f}_{\mathcal{E}_{sr}},\mathbf{f}_{\mathcal{E}_{rt}}\right)+\Sigma_0^{(1)}\left(\mathbf{f}_{\mathcal{E}_{st}}\right),\Sigma_1^{(2)}\left(\mathbf{f}_{\mathcal{E}_{sr}},\mathbf{f}_{\mathcal{E}_{rt}}\right)+\Sigma_1^{(1)}\left(\mathbf{f}_{\mathcal{E}_{st}}\right),\Sigma_0^{(2)}\left(\mathbf{f}_{\mathcal{E}_{sr}},\mathbf{f}_{\mathcal{E}_{rt}}\right)+\Sigma_2^{(1)}\left(\mathbf{f}_{\mathcal{E}_{st}}\right)\right\}$$
$$=\min\left\{\left\|\mathbf{f}_{\mathcal{E}_{st}}\right\|,\min\left\{f_{e_{st1}},f_{e_{st2}}\right\}+\min\left\{f_{e_{sr1}},f_{e_{sr2}},f_{e_{rt1}},f_{e_{rt2}}\right\},\min\left\{\left\|\mathbf{f}_{\mathcal{E}_{sr}}\right\|,\left\|\mathbf{f}_{\mathcal{E}_{rt}}\right\|\right\}\right\}.$$

考虑割集上界（命题 4.1），有 $n_{z,s}=n_{z,t}=2$，且

$$\Sigma_{n_{z,s}}^{(1)}\left(\begin{bmatrix}\mathbf{f}_{\mathcal{E}_{st}}\\ \mathbf{f}_{\mathcal{E}_{sr}}\end{bmatrix}\right)=\min\left\{\left\|\mathbf{f}_{\mathcal{E}_{st}}\right\|,\min\left\{f_{e_{st1}},f_{e_{st2}}\right\}+\min\left\{f_{e_{sr1}},f_{e_{sr2}}\right\},\left\|\mathbf{f}_{\mathcal{E}_{sr}}\right\|\right\}\qquad(4\text{–}33)$$

$$\Sigma_{n_{z,t}}^{(1)}\left(\begin{bmatrix}\mathbf{f}_{\mathcal{E}_{st}}\\ \mathbf{f}_{\mathcal{E}_{rt}}\end{bmatrix}\right)=\min\left\{\left\|\mathbf{f}_{\mathcal{E}_{st}}\right\|,\min\left\{f_{e_{st1}},f_{e_{st2}}\right\}+\min\left\{f_{e_{rt1}},f_{e_{rt2}}\right\},\left\|\mathbf{f}_{\mathcal{E}_{rt}}\right\|\right\},\qquad(4\text{–}34)$$

所以割集上界为

$$\min\left\{\Sigma_{n_{z,s}}^{(1)}\left(\begin{bmatrix}\mathbf{f}_{\mathcal{E}_{st}}\\ \mathbf{f}_{\mathcal{E}_{sr}}\end{bmatrix}\right),\Sigma_{n_{z,t}}^{(1)}\left(\begin{bmatrix}\mathbf{f}_{\mathcal{E}_{st}}\\ \mathbf{f}_{\mathcal{E}_{rt}}\end{bmatrix}\right)\right\}$$
$$=\min\left\{\left\|\mathbf{f}_{\mathcal{E}_{st}}\right\|,\min\left\{f_{e_{st1}},f_{e_{st2}}\right\}+\min\left\{f_{e_{sr1}},f_{e_{sr2}},f_{e_{rt1}},f_{e_{rt2}}\right\},\min\left\{\left\|\mathbf{f}_{\mathcal{E}_{sr}}\right\|,\left\|\mathbf{f}_{\mathcal{E}_{rt}}\right\|\right\}\right\}.$$

路由猜测转发上界与割集上界相同。所以路由猜测转发下界就是纠错容量。

(情况 2) $|\mathcal{E}_{sr}|=|\mathcal{E}_{rt}|=2$ 且 $|\mathcal{E}_{st}|=1$。令 $\mathcal{E}_{st}=\{e_{st}\}$。用类似的方法可以验证路由猜测转发下界和割集上界均为

$$\min\left\{\Sigma_2^{(2)}\left(\mathbf{f}_{\mathcal{E}_{sr}},\mathbf{f}_{\mathcal{E}_{rt}}\right)+\Sigma_0^{(1)}\left(\mathbf{f}_{\mathcal{E}_{st}}\right),\Sigma_1^{(2)}\left(\mathbf{f}_{\mathcal{E}_{sr}},\mathbf{f}_{\mathcal{E}_{rt}}\right)+\Sigma_1^{(1)}\left(\mathbf{f}_{\mathcal{E}_{st}}\right)\right\}$$
$$=\min\left\{f_{e_{st}},f_{e_{sr1}},f_{e_{sr2}},f_{e_{rt1}},f_{e_{rt2}}\right\}.$$

(情况 3) $|\mathcal{E}_{sr}|=|\mathcal{E}_{st}|=2$ 且 $|\mathcal{E}_{rt}|=1$，或是 $|\mathcal{E}_{rt}|=|\mathcal{E}_{st}|=2$ 且 $|\mathcal{E}_{sr}|=1$。也可以验证路由猜测转发下界和割集上界相同，路由猜测转发下界就是容量。 □

4.3.3 译码猜测转发下界

定理 4.8（译码猜测转发下界）：三节点网络中，$\mathcal{A}=\mathcal{P}(\mathcal{E},z)$。则纠错容量有以下下界：如果 $|\mathcal{E}_{sr}|\le 2z$ 且 $|\mathcal{E}_{st}|+|\mathcal{E}_{rt}|\le 2z$，则 $C\ge 0$；否则

$$C \geq \min\left\{\Sigma^{(1)}_{n_{z,sr}}\left(\mathbf{f}_{\mathcal{E}_{sr}}\right), \Sigma^{(1)}_{n_{z,st}}\left(\begin{bmatrix}\mathbf{f}_{\mathcal{E}_{st}}\\ \mathbf{f}_{\mathcal{E}_{rt}}\end{bmatrix}\right)\right\}, \tag{4–35}$$

其中 $n_{z,sr} \triangleq \max\left\{z, 2\left(\left|\mathcal{E}_{rs}\right| - z\right)\right\}$ 且 $n_{z,st} \triangleq \max\left\{z, 2\left(\left|\mathcal{E}_{ts}\right| - z\right)\right\}$。

证明：下面给出在下界不为 0 时下界的达到方法。

链路速率分割：考虑子流 $\begin{bmatrix}\mathbf{0}_{\mathcal{E}_{st}\cup\mathcal{E}_{ts}}\\ \mathbf{f}_{\mathcal{E}_{sr}} - \delta\mathbf{1}_{\mathcal{E}_{sr}}\\ \mathbf{f}_{\mathcal{E}_{rs}}\\ \mathbf{0}_{\mathcal{E}_{rt}}\\ \mathbf{0}_{\mathcal{E}_{tr}}\end{bmatrix}$ 和 $\begin{bmatrix}\mathbf{f}_{\mathcal{E}_{st}\cup\mathcal{E}_{ts}}\\ \delta\mathbf{1}_{\mathcal{E}_{sr}}\\ \mathbf{0}_{\mathcal{E}_{rs}}\\ \mathbf{f}_{\mathcal{E}_{rt}}\\ \mathbf{0}_{\mathcal{E}_{tr}}\end{bmatrix}$，其中 δ 满足 $0 < \delta < \min\limits_{e\in\mathcal{E}_{sr}} f_e$。

显然有

$$\begin{bmatrix}\mathbf{0}_{\mathcal{E}_{st}\cup\mathcal{E}_{ts}}\\ \mathbf{f}_{\mathcal{E}_{sr}} - \delta\mathbf{1}_{\mathcal{E}_{sr}}\\ \mathbf{f}_{\mathcal{E}_{rs}}\\ \mathbf{0}_{\mathcal{E}_{rt}}\\ \mathbf{0}_{\mathcal{E}_{tr}}\end{bmatrix} + \begin{bmatrix}\mathbf{f}_{\mathcal{E}_{st}\cup\mathcal{E}_{ts}}\\ \delta\mathbf{1}_{\mathcal{E}_{sr}}\\ \mathbf{0}_{\mathcal{E}_{rs}}\\ \mathbf{f}_{\mathcal{E}_{rt}}\\ \mathbf{0}_{\mathcal{E}_{tr}}\end{bmatrix} \leq \begin{bmatrix}\mathbf{f}_{\mathcal{E}_{st}\cup\mathcal{E}_{ts}}\\ \mathbf{f}_{\mathcal{E}_{sr}}\\ \mathbf{f}_{\mathcal{E}_{rs}}\\ \mathbf{f}_{\mathcal{E}_{rt}}\\ \mathbf{f}_{\mathcal{E}_{tr}}\end{bmatrix}. \tag{4–36}$$

码分配：(步骤 1) 在第 1 个子流上，源节点 v_s 使用 $\mathbf{f}_{\mathcal{E}_{sr}} - \delta\mathbf{1}_{\mathcal{E}_{sr}}$ 和 $\mathbf{f}_{\mathcal{E}_{rs}}$，构造猜测转发将消息发送给中继节点 v_r；

(步骤 2) 在第 2 个子流，源节点 v_s 和中继节点 v_r 合作，使用猜测转发向目的节点发送 v_t 消息。在猜测转发的过程中，目的节点 v_t 只通过流 $\mathbf{f}_{\mathcal{E}_{ts}}$ 向源节点 v_s 直接提供反馈，而源节点 v_s 将使用 $\delta\mathbf{1}_{\mathcal{E}_{sr}}$ 将这些反馈转发给中继节点 v_r。

采用这样的办法，可以达到速率

$$\min\left\{\Sigma^{(1)}_{n_{z,sr}}\left(\mathbf{f}_{\mathcal{E}_{sr}} - \delta\mathbf{1}_{\mathcal{E}_{sr}}\right), \Sigma^{(1)}_{n_{z,st}}\left(\begin{bmatrix}\mathbf{f}_{\mathcal{E}_{st}}\\ \mathbf{f}_{\mathcal{E}_{rt}}\end{bmatrix}\right)\right\}. \tag{4–37}$$

令 $\delta \to 0$ 得证。 □

下面给出定理 4.8 中下界紧的充分条件。

命题 4.6：在定理 4.8 中，当 $\mathcal{E}_{tr} = \varnothing$ 且 $\left|\mathcal{E}_{sr}\right| > 2z$ 且 $\Sigma^{(1)}_{n_{z,sr}}\left(\mathbf{f}_{\mathcal{E}_{sr}}\right) \geq \Sigma^{(1)}_{n_{z,st}}\left(\begin{bmatrix}\mathbf{f}_{\mathcal{E}_{st}}\\ \mathbf{f}_{\mathcal{E}_{rt}}\end{bmatrix}\right)$ 时，定理 4.8 给出的下界紧。 □

证明：不失一般性，仅考虑$|\mathcal{E}_{st}|+|\mathcal{E}_{rt}|>2z$的情况。当$\Sigma^{(1)}_{n_{z,sr}}\left(\mathbf{f}_{\mathcal{E}_{sr}}\right)\geq\Sigma^{(1)}_{n_{z,st}}\left(\begin{bmatrix}\mathbf{f}_{\mathcal{E}_{st}}\\ \mathbf{f}_{\mathcal{E}_{rt}}\end{bmatrix}\right)$时，译码猜测转发下界为$\Sigma^{(1)}_{n_{z,st}}\left(\begin{bmatrix}\mathbf{f}_{\mathcal{E}_{st}}\\ \mathbf{f}_{\mathcal{E}_{rt}}\end{bmatrix}\right)$。注意到割$\mathcal{E}_c\left(\{v_s,v_r\}\right)$导出的割集上界$\Sigma^{(1)}_{n_{z,st}}\left(\begin{bmatrix}\mathbf{f}_{\mathcal{E}_{st}}\\ \mathbf{f}_{\mathcal{E}_{rt}}\end{bmatrix}\right)$等于译码猜测转发上界，所以译码猜测转发下界即是纠错容量。　□

4.3.4 路由猜测转发-译码猜测转发-第1下界

定理 4.9（路由猜测转发-译码猜测转发-第 1 下界）：三节点网络中，$\mathcal{A}=\mathcal{P}(\mathcal{E},z)$。则纠错容量有以下下界：若$n_{sr}+n_{st}\leq 2z$或$n_{sr}+n_{tr}\leq 2z$或$n_{rt}\leq 2z$，则$C\geq 0$；否则

$$C\geq\min\left\{\min_{n_{zt}+n_{zr}\leq n'_z}\left(\Sigma^{(1)}_{n_{zr}}\left(\mathbf{f}_{\mathcal{E}_{sr}}\right)+\Sigma^{(2)}_{n_{zt}}\left(\mathbf{f}_{\mathcal{E}_{st}},\mathbf{f}_{\mathcal{E}_{tr}}\right)\right),\Sigma^{(1)}_{n_{z,rt}}\left(\mathbf{f}_{\mathcal{E}_{rt}}\right)\right\}\tag{4–38}$$

其中$n'_z\triangleq\max\left\{z,2\left(z-|\mathcal{E}_{rs}|-\min\left\{|\mathcal{E}_{rt}|,|\mathcal{E}_{ts}|\right\}\right)\right\}$和$n_{z,rt}\triangleq\max\left\{z,2\left(z-|\mathcal{E}_{tr}|\right)\right\}$。　□

证明：下面给出在下界不为 0 时下界的达到方法。

链路速率分割：考虑两个子流$\begin{bmatrix}\mathbf{f}_{\mathcal{E}_{st}\cup\mathcal{E}_{ts}\cup\mathcal{E}_{sr}\cup\mathcal{E}_{rs}}\\ \delta_{rt}\mathbf{1}_{\mathcal{E}_{rt}}\\ \mathbf{f}_{\mathcal{E}_{tr}}-\delta_{tr}\mathbf{1}_{\mathcal{E}_{tr}}\end{bmatrix}$和$\begin{bmatrix}\mathbf{0}_{\mathcal{E}_{st}\cup\mathcal{E}_{ts}\cup\mathcal{E}_{sr}\cup\mathcal{E}_{rs}}\\ \mathbf{f}_{\mathcal{E}_{rt}}-\delta_{rt}\mathbf{1}_{\mathcal{E}_{rt}}\\ \delta_{tr}\mathbf{1}_{\mathcal{E}_{tr}}\end{bmatrix}$，其中$\delta_{rt},\delta_{tr}$满足$0<\delta_{rt}<\min\limits_{e\in\mathcal{E}_{rt}}f_e$和$0<\delta_{tr}<\min\limits_{e\in\mathcal{E}_{tr}}f_e$。显然有

$$\begin{bmatrix}\mathbf{f}_{\mathcal{E}_{st}\cup\mathcal{E}_{ts}\cup\mathcal{E}_{sr}\cup\mathcal{E}_{rs}}\\ \delta_{rt}\mathbf{1}_{\mathcal{E}_{rt}}\\ \mathbf{f}_{\mathcal{E}_{tr}}-\delta_{tr}\mathbf{1}_{\mathcal{E}_{tr}}\end{bmatrix}+\begin{bmatrix}\mathbf{0}_{\mathcal{E}_{st}\cup\mathcal{E}_{ts}\cup\mathcal{E}_{sr}\cup\mathcal{E}_{rs}}\\ \mathbf{f}_{\mathcal{E}_{rt}}-\delta_{rt}\mathbf{1}_{\mathcal{E}_{rt}}\\ \delta_{tr}\mathbf{1}_{\mathcal{E}_{tr}}\end{bmatrix}\leq\begin{bmatrix}\mathbf{f}_{\mathcal{E}_{st}\cup\mathcal{E}_{ts}\cup\mathcal{E}_{sr}\cup\mathcal{E}_{rs}}\\ \mathbf{f}_{\mathcal{E}_{rt}}\\ \mathbf{f}_{\mathcal{E}_{tr}}\end{bmatrix}.\tag{4–39}$$

码分配：(步骤 1) 在第 1 个子流上，源节点v_s在目的节点v_t的帮助下，使用路由猜想转发将消息发送给中继节点v_r。中继节点v_r译出消息。根据定理 4.7，该码可以支持可靠速率

$$\min_{n_{zt}+n_{zr}\leq n'_z}\left(\Sigma^{(1)}_{n_{zr}}\left(\mathbf{f}_{\mathcal{E}_{sr}}\right)+\Sigma^{(2)}_{n_{zt}}\left(\mathbf{f}_{\mathcal{E}_{st}},\mathbf{f}_{\mathcal{E}_{tr}}-\delta_{tr}\mathbf{1}_{\mathcal{E}_{tr}}\right)\right).\tag{4–40}$$

(步骤 2) 中继节点v_r使用猜想转发将消息发送给目的节点v_t。该部分可支持可靠速率$\Sigma^{(1)}_{n_{z,rt}}\left(\mathbf{f}_{\mathcal{E}_{rt}}-\delta_{rt}\mathbf{1}_{\mathcal{E}_{rt}}\right)$。

综合以上两步，构造出的码可支持速率

$$\min\left\{\min_{n_{zt}+n_{zr}\leq n'_z}\left(\Sigma^{(1)}_{n_{zr}}\left(\mathbf{f}_{\mathcal{E}_{sr}}\right)+\Sigma^{(2)}_{n_{zt}}\left(\mathbf{f}_{\mathcal{E}_{st}},\mathbf{f}_{\mathcal{E}_{tr}}-\delta_{tr}\mathbf{1}_{\mathcal{E}_{tr}}\right)\right),\Sigma^{(1)}_{n_{z,rt}}\left(\mathbf{f}_{\mathcal{E}_{rt}}-\delta_{rt}\mathbf{1}_{\mathcal{E}_{rt}}\right)\right\}.\tag{4–41}$$

令 $\delta_{rt}\to 0$、$\delta_{tr}\to 0$ 得证。 □

下面给出定理 4.9 中下界紧的充分条件。

命题 4.7：在定理 4.9 中，当 $|\mathcal{E}_{rt}|\geq|\mathcal{E}_{ts}|$ 且 $|\mathcal{E}_{rt}|>2z$ 且 $|\mathcal{E}_{st}|=|\mathcal{E}_{tr}|$ 且 $\mathbf{f}_{\mathcal{E}_{st}}\leq\mathbf{f}_{\mathcal{E}_{tr}}$ 且 $\Sigma^{(1)}_{n_{z,rt}}\left(\mathbf{f}_{\mathcal{E}_{rt}}\right)\geq\Sigma^{(1)}_{n_{z,s}}\left(\begin{bmatrix}\mathbf{f}_{\mathcal{E}_{sr}}\\ \mathbf{f}_{\mathcal{E}_{st}}\end{bmatrix}\right)$ 时（其中 $n_{z,rt}\triangleq\max\left\{z,2\left(z-|\mathcal{E}_{tr}|\right)\right\}$，$n_{z,s}\triangleq\max\left\{z,2\left(z-|\mathcal{E}_{rs}|-|\mathcal{E}_{ts}|\right)\right\}$），定理 4.9 给出的下界紧。 □

证明：不妨假设 $|\mathcal{E}_{sr}|+|\mathcal{E}_{st}|>2z$。

由于 $|\mathcal{E}_{rt}|\geq|\mathcal{E}_{ts}|$，所以在第 1 个子流中猜测转发码从中继节点 v_r 到源节点 v_s 的独立反馈路径数为 $|\mathcal{E}_{rs}|+|\mathcal{E}_{ts}|$，并且有 $n'_z=n_{z,s}$。

由于 $|\mathcal{E}_{st}|=|\mathcal{E}_{tr}|$ 且 $\mathbf{f}_{\mathcal{E}_{st}}\leq\mathbf{f}_{\mathcal{E}_{tr}}$，可以证明（从略），

$$\Sigma^{(1)}_{n_{z,s}}\left(\begin{bmatrix}\mathbf{f}_{\mathcal{E}_{sr}}\\ \mathbf{f}_{\mathcal{E}_{st}}\end{bmatrix}\right)=\min_{n_{zt}+n_{zr}\leq n'_z}\left(\Sigma^{(1)}_{n_{zr}}\left(\mathbf{f}_{\mathcal{E}_{sr}}\right)+\Sigma^{(2)}_{n_{zt}}\left(\mathbf{f}_{\mathcal{E}_{st}},\mathbf{f}_{\mathcal{E}_{tr}}\right)\right).\qquad(4\text{–}42)$$

注意到 $\Sigma^{(1)}_{n_{z,rt}}\left(\mathbf{f}_{\mathcal{E}_{rt}}\right)\geq\Sigma^{(1)}_{n_{z,s}}\left(\begin{bmatrix}\mathbf{f}_{\mathcal{E}_{sr}}\\ \mathbf{f}_{\mathcal{E}_{st}}\end{bmatrix}\right)$，所以路由猜测转发-译码猜测转发第 1 下界为 $\Sigma^{(1)}_{n_{z,s}}\left(\begin{bmatrix}\mathbf{f}_{\mathcal{E}_{sr}}\\ \mathbf{f}_{\mathcal{E}_{st}}\end{bmatrix}\right)$。

注意到这个界和割 $\mathcal{E}_c\left(\{v_s\}\right)$ 导出的割集上界 $C_{UB,s}\triangleq\Sigma^{(1)}_{n_{z,s}}\left(\begin{bmatrix}\mathbf{f}_{\mathcal{E}_{sr}}\\ \mathbf{f}_{\mathcal{E}_{st}}\end{bmatrix}\right)$ 相同，所以该下界紧。 □

4.3.5 路由猜测转发-译码猜测转发-第2下界

定理 4.10（路由猜测转发-译码猜测转发-第 2 下界）：三节点网络中，$\mathcal{A}=\mathcal{P}(\mathcal{E},z)$。则纠错容量有以下下界：若 $|\mathcal{E}_{sr}|+|\mathcal{E}_{st}|\leq 2z$ 或 $|\mathcal{E}_{sr}|+|\mathcal{E}_{tr}|\leq 2z$ 或 $|\mathcal{E}_{rt}|+|\mathcal{E}_{st}|\leq 2z$，则 $C\geq 0$；否则

$$C\geq\max_{\mathbf{f}^{(1)}_{st},\mathbf{f}^{(2)}_{st}>\mathbf{0}:\mathbf{f}^{(1)}_{st}+\mathbf{f}^{(2)}_{st}=\mathbf{f}_{st}}\left\{\min_{n_{zt}+n_{zr}\leq n'_z}\left(\Sigma^{(1)}_{n_{zr}}\left(\mathbf{f}_{\mathcal{E}_{sr}}\right)+\Sigma^{(2)}_{n_{zt}}\left(\mathbf{f}^{(1)}_{\mathcal{E}_{st}},\mathbf{f}_{\mathcal{E}_{tr}}\right)\right),\Sigma^{(1)}_{n_{z,st}}\left(\begin{bmatrix}\mathbf{f}_{\mathcal{E}_{rt}}\\ \mathbf{f}^{(2)}_{\mathcal{E}_{st}}\end{bmatrix}\right)\right\},\qquad(4\text{–}43)$$

其中 $n'_z\triangleq\max\left\{z,2\left(z-|\mathcal{E}_{rs}|-\min\left\{|\mathcal{E}_{rt}|,|\mathcal{E}_{ts}|\right\}\right)\right\}$ 或 $n_{z,st}\triangleq\max\left\{z,2\left(z-|\mathcal{E}_{ts}|\right)\right\}$。 □

证明：下面给出在下界不为 0 时下界的达到方法。这时有 $|\mathcal{E}_{sr}|+|\mathcal{E}_{st}|>2z$，$|\mathcal{E}_{sr}|+|\mathcal{E}_{tr}|>2z$ 和 $|\mathcal{E}_{rt}|+|\mathcal{E}_{st}|>2z$。

链路速率分割：在链路速率 $\begin{bmatrix}\mathbf{f}_{\mathcal{E}_{st}}\\ \mathbf{f}_{\mathcal{E}_{ts}}\\ \mathbf{f}_{\mathcal{E}_{sr}}\\ \mathbf{f}_{\mathcal{E}_{rs}}\\ \mathbf{f}_{\mathcal{E}_{rt}}\\ \mathbf{f}_{\mathcal{E}_{tr}}\end{bmatrix}$ 中取出 $\begin{bmatrix}\mathbf{f}^{(1)}_{\mathcal{E}_{st}}\\ \frac{1}{2}\delta_{ts}\mathbf{1}_{\mathcal{E}_{ts}}\\ \mathbf{f}_{\mathcal{E}_{sr}}-\delta_{sr}\mathbf{1}_{\mathcal{E}_{sr}}\\ \delta_{rs}\mathbf{1}_{\mathcal{E}_{rs}}\\ \delta_{rt}\mathbf{1}_{\mathcal{E}_{rt}}\\ \mathbf{f}_{\mathcal{E}_{tr}}-\delta_{tr}\mathbf{1}_{\mathcal{E}_{tr}}\end{bmatrix}$ 和 $\begin{bmatrix}\mathbf{f}^{(2)}_{\mathcal{E}_{st}}+\delta_{tr}\mathbf{1}_{\mathcal{E}_{st}}\\ \frac{1}{2}\delta_{ts}\mathbf{1}_{\mathcal{E}_{ts}}\\ \delta_{sr}\mathbf{1}_{\mathcal{E}_{sr}}\\ \mathbf{0}_{\mathcal{E}_{rs}}\\ \mathbf{f}_{\mathcal{E}_{rt}}-\delta_{rt}\mathbf{1}_{\mathcal{E}_{rt}}\\ \delta_{tr}\mathbf{1}_{\mathcal{E}_{tr}}\end{bmatrix}$ 两个子流，其中 $\delta_{ts},\delta_{sr},\delta_{rs},\delta_{rt},\delta_{tr}$ 满足

$$\begin{aligned}0<\delta_{ts}&<\min_{e\in\mathcal{E}_{ts}} f_e\\ 0<\delta_{sr}&<\min_{e\in\mathcal{E}_{sr}} f_e\\ 0<\delta_{rs}&<\min_{e\in\mathcal{E}_{rs}} f_e\\ 0<\delta_{rt}&<\min_{e\in\mathcal{E}_{rt}} f_e\\ 0<\delta_{tr}&<\min_{e\in\mathcal{E}_{rt}\cup\mathcal{E}_{st}} f_e,\end{aligned}$$

$\mathbf{f}^{(1)}_{\mathcal{E}_{st}},\mathbf{f}^{(2)}_{\mathcal{E}_{st}}>\mathbf{0}_{\mathcal{E}_{st}}$ 满足 $\mathbf{f}^{(1)}_{\mathcal{E}_{st}}+\mathbf{f}^{(2)}_{\mathcal{E}_{st}}+\delta_{tr}\mathbf{1}_{\mathcal{E}_{st}}=\mathbf{f}_{\mathcal{E}_{st}}$。可以验证，

$$\begin{bmatrix}\mathbf{f}^{(1)}_{\mathcal{E}_{st}}\\ \frac{1}{2}\delta_{ts}\mathbf{1}_{\mathcal{E}_{ts}}\\ \mathbf{f}_{\mathcal{E}_{sr}}-\delta_{sr}\mathbf{1}_{\mathcal{E}_{sr}}\\ \delta_{rs}\mathbf{1}_{\mathcal{E}_{rs}}\\ \delta_{rt}\mathbf{1}_{\mathcal{E}_{rt}}\\ \mathbf{f}_{\mathcal{E}_{tr}}-\delta_{tr}\mathbf{1}_{\mathcal{E}_{tr}}\end{bmatrix}+\begin{bmatrix}\mathbf{f}^{(2)}_{\mathcal{E}_{st}}+\delta_{tr}\mathbf{1}_{\mathcal{E}_{st}}\\ \frac{1}{2}\delta_{ts}\mathbf{1}_{\mathcal{E}_{ts}}\\ \delta_{sr}\mathbf{1}_{\mathcal{E}_{sr}}\\ \mathbf{0}_{\mathcal{E}_{rs}}\\ \mathbf{f}_{\mathcal{E}_{rt}}-\delta_{rt}\mathbf{1}_{\mathcal{E}_{rt}}\\ \delta_{tr}\mathbf{1}_{\mathcal{E}_{tr}}\end{bmatrix}\le\begin{bmatrix}\mathbf{f}_{\mathcal{E}_{st}}\\ \mathbf{f}_{\mathcal{E}_{ts}}\\ \mathbf{f}_{\mathcal{E}_{sr}}\\ \mathbf{f}_{\mathcal{E}_{rs}}\\ \mathbf{f}_{\mathcal{E}_{rt}}\\ \mathbf{f}_{\mathcal{E}_{tr}}\end{bmatrix}. \tag{4–44}$$

码分配：(步骤 1) 在第 1 个子流上，源节点 v_s 在目的节点 v_t 的帮助下，使用路由猜测转发码向中继节点 v_r 发送消息。中继节点 v_r 译出消息。此步可支持可靠速率

$$\min_{n_{zt}+n_{zr}\le n'_z}\left(\Sigma^{(1)}_{n_{zr}}\left(\mathbf{f}_{\mathcal{E}_{sr}}-\delta_{sr}\mathbf{1}_{\mathcal{E}_{sr}}\right)+\Sigma^{(2)}_{n_{zt}}\left(\mathbf{f}^{(1)}_{\mathcal{E}_{st}},\mathbf{f}_{\mathcal{E}_{tr}}-\delta_{tr}\mathbf{1}_{\mathcal{E}_{tr}}\right)\right), \tag{4–45}$$

其中 $n'_z\triangleq\max\left\{z,2\left(z-|\mathcal{E}_{rs}|-\min\left\{|\mathcal{E}_{rt}|,|\mathcal{E}_{ts}|\right\}\right)\right\}$。

(步骤 2) 在第 2 个子流上，中继节点 v_r 和源节点 v_s 一起协作，使用猜测转发码，向目的节点 v_t 发送消息。其中目的节点 v_t 的反馈先都发给源节点 v_s，然后源节点 v_s 再通过路径 $v_s\to v_r$ 和 $v_s\to v_t\to v_r$ 将反馈信息告诉 v_r。这步可以达到速率

$\Sigma_{n_{z,rt}}^{(1)}\left(\begin{bmatrix}\mathbf{f}_{\mathcal{E}_{st}}^{(2)}+\delta_{tr}\mathbf{1}_{\mathcal{E}_{st}}\\ \mathbf{f}_{\mathcal{E}_{rt}}-\delta_{rt}\mathbf{1}_{\mathcal{E}_{rt}}\end{bmatrix}\right)$。

综合以上两步，则有速率

$$\min\left\{\min_{n_{zt}+n_{zr}\le n'_z}\left(\Sigma_{n_{zr}}^{(1)}\left(\mathbf{f}_{\mathcal{E}_{sr}}-\delta_{sr}\mathbf{1}_{\mathcal{E}_{sr}}\right)+\Sigma_{n_{zt}}^{(2)}\left(\mathbf{f}_{\mathcal{E}_{st}}^{(1)},\mathbf{f}_{\mathcal{E}_{tr}}-\delta_{tr}\mathbf{1}_{\mathcal{E}_{tr}}\right)\right),\Sigma_{n_{z,rt}}^{(1)}\left(\begin{bmatrix}\mathbf{f}_{\mathcal{E}_{st}}^{(2)}+\delta_{tr}\mathbf{1}_{\mathcal{E}_{st}}\\ \mathbf{f}_{\mathcal{E}_{rt}}-\delta_{rt}\mathbf{1}_{\mathcal{E}_{rt}}\end{bmatrix}\right)\right\}.$$

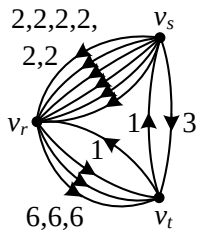
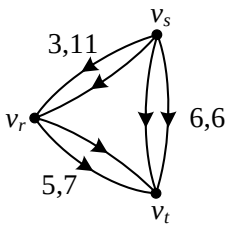
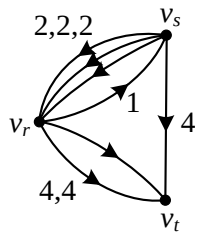
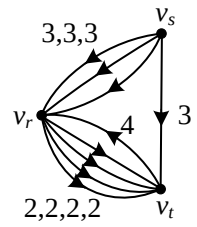
对$\mathbf{f}_{\mathcal{E}_{st}}^{(1)}$和$\mathbf{f}_{\mathcal{E}_{st}}^{(2)}$的值进行优化，再令$\delta_{sr}\to 0$、$\delta_{tr}\to 0$和$\delta_{rt}\to 0$则可得证。　□

事实上，译码转发可以视作路由猜测转发-译码猜测转发第 2 下界的一个特例。在路由猜测转发-译码猜测转发中，若其第 1 步骤不利用目的节点v_t，而直接在源节点v_s和中继节点v_r之间通信，那就退化为译码转发了。从此可知，当译码转发能达到容量的时候，猜测转发-译码猜测转发第 2 下界都能达到容量。在后文中还会给出译码猜测转发下界不能达到容量，但是猜测转发-译码猜测转发第 2 下界达到容量的例子。

4.3.6 一些数值例子

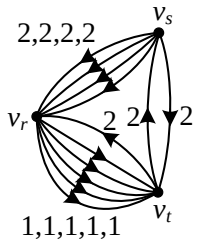
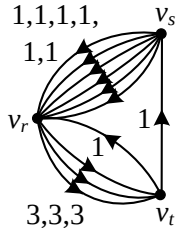
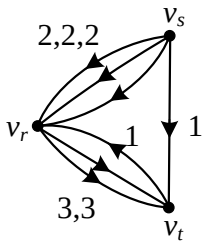
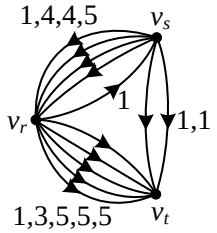
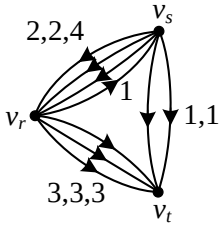
前文我们已经给出了三节点网络中的许多下界。遗憾的是，没有一个下界是紧的。但是，将这些下界综合起来考虑，就能够达到绝大多数三节点网络的容量。表 4.1 给出了一些三节点网络的例子，以期在数值上有直观的理解。

表 4.1　一些三节点网络信道容量的数值例子

三节点网络	割集上界	包装猜测转发下界	路由猜测转发下界	译码猜测转发下界	路由猜测转发-译码猜测转发第 1 下界	路由猜测转发-译码猜测转发第 2 下界
	12 （紧）	12 （紧）	11	8	9	11
	9 （紧）	0	9 （紧）	0	0	0
	4 （紧）	0	3	4 （紧）	0	4 （紧）
	6 （紧）	4	$5\frac{1}{3}$	3	6 （紧）	5

（未完）

续表 4.1　一些三节点网络信道容量的数值例子

	5 （紧）	4	5 （紧）	4	4	5 （紧）
	5 （紧）	5 （紧）	4	4	4	5 （紧）
	3 （紧）	0	1	1	0	3 （紧）
	11	$5\frac{2}{3}$	7	9	9	9
	6	4	4	4	4	4

第 5 章　多址接入模型的求解

内容提要

本章考虑有多个源节点、一个目的节点的有向网络中的容许速率域问题，求得了分布式分层分集的容许速率域。多个源节点处的信源不一定是独立的。

● 5.1 节给出本章研究的模型及其结论。

● 5.2 节给出 5.1 节中定理的证明。

本章内容改编自在学期间发表的学术论文[5]。文章的共同作者参与了相关的讨论和研究。

5.1 模型与结果

本章考虑图 5.1 中的多址接入模型。在网络中有 $K+1$ 个节点，其中 K 个节点是源节点，1 个节点是目的节点。对于任意一个源节点 $v_{s,k}$（$k \in [1:K]$），它和目的节点 v_t 间都通过链路 e_k 直接相连。每条链路都有可能被敌对方控制（或等价的，相应的源节点会被敌对方控制）。当恶意方控制了某些链路时，它会切断链路的链接。假设每个源节点都有 K 个信源要发送给目的节点。我们需要设计网络纠错码，使得当攻击方切断任意若干个中间链路时都能恢复出足够多的信息。更具体的说，令节点 v_{sk} 要发送的信源为 $U_{k,[1:K]} \triangleq \left(U_{k,\alpha} : \alpha \in [1:K]\right)$（当信道多次使用时，信源会产生多个独立同分布的实现），我们希望对任意的 $V \subseteq [1:K]$，当链路集 $\{e_k : k \in V\}$ 能正确传输时，目的节点都能恢复出 $U_{V,[1:|V|]} \triangleq \left(U_{k,\alpha} : k \in V, \alpha \in [1:\lfloor |V| \rfloor]\right)$。这样的码又称为分布式分层分集码。

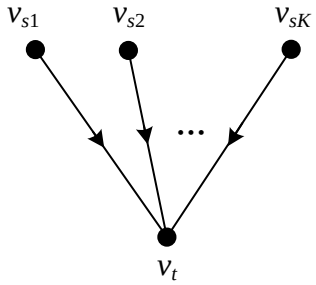


图 5.1　多址接入网络

码的定义

严格的说，本章要研究的信源编码定义如下：

定义 5.1（分布式分层分集码）：一个$\left(n,\left(q_k:k\in[1:K]\right)\right)$的码包括以下部分：

(1) K 个编码器：其中 Enc_k（$k\in[1:K]$）将信源序列$U_{k,[1:K]}^n$映射到$[0:q_k)$的一个符号S_k上，即

$$\begin{aligned}\mathrm{Enc}_k:\prod_{\alpha=1}^{K}\mathcal{U}_{k,\alpha}^n &\to [0:q_k)\\ U_{k,[1:K]}^n &\mapsto \quad S_k\end{aligned}$$

(2) 2^K-1个译码器：其中译码器Dec_V（$\varnothing\subsetneqq V\subseteq[1:K]$）能试图根据$S_V$来恢复$U_{V,[1:|V|]}^n$的一个版本（记为$\hat{U}_{V,[1:|V|]}^n$），即

$$\begin{aligned}\mathrm{Dec}_V:\prod_{k\in V}[0:q_k) &\to \prod_{k\in V}\prod_{\alpha=1}^{|V|}\mathcal{U}_{k,\alpha}^n\\ S_V \quad &\mapsto \quad \hat{U}_{V,[1:|V|]}^n.\end{aligned}$$ □

容许速率域

定义 5.2（多址接入网络容许速率域）：一个速率对$\left(R_k:k\in[1:K]\right)$称为容许的，当且仅当对任意的正数$\varepsilon>0$，存在一个$\left(n,\left(q_k:k\in[1:K]\right)\right)$码，使得

(1)（速率约束）

$$\frac{1}{n}\log q_k\le R_k+\varepsilon,\quad k\in[1:K];\tag{5–1}$$

(2)（重建约束）

$$\Pr\left\{U_{V,[1:|V|]}^n\ne\hat{U}_{V,[1:|V|]}^n\right\}\le\varepsilon,\quad \varnothing\subsetneqq V\subseteq[1:K].\tag{5–2}$$

容许速率域$\mathcal{R}_K^*$定义为所有容许速率对的集合。 □

5.1.1 多层Slepian-Wolf码

这里构造一种特殊的码，我们姑且称其为多层 Slepian-Wolf 码。我们后面会证明它可以达到全部的容许速率域，是最优码。

该码的编码包括两个部分：层内编码和层间编码。

(1) 层内编码：对于某个$\alpha\in[1:K]$，用常规的 Slepian-Wolf 编码[101]将$U_{[1:K],\alpha}^n\triangleq\left(U_{k,\alpha}^n:k\in[1:K]\right)$编为速率$r_{[1:K],\alpha}\triangleq\left(r_{k,\alpha}:k\in[1:K]\right)$。定义

$$\mathcal{R}_{K,\alpha} \triangleq \left\{ \left(r_{k,\alpha} : k \in [1:K] \right) : \sum_{k \in V} r_{k,\alpha} \geq H\left(U_{V,\alpha} \,|\, U_{V',\alpha} \right), V \in \mathbb{V}_{K,\alpha}, V' \in \mathbb{V}'_{K,\alpha}[V] \right\},$$

其中

$$\mathbb{V}_{K,\alpha} \triangleq \left\{ V \subseteq [1:K] : 1 \leq |V| \leq \alpha \right\}$$

$$\mathbb{V}'_{K,\alpha}[V] \triangleq \left\{ V' \subseteq [1:K] \backslash V : |V'| + |V| = \alpha \right\}, \quad V \in \mathbb{V}_{K,\alpha}.$$

值得一提的是，根据 Slepian-Wolf 编码的研究结果[102]，若 $r_{[1K]\alpha} \in \mathcal{R}_{K,\alpha}$，则对所有满足 $|V| = \alpha$ 的集合 $V \subseteq [1:K]$，可以以接近于 1 的概率恢复出 $U^n_{[1:K],\alpha}$。

(2) 层间编码：对于 $k \in [1:K]$，编码器 Enc_k 将上步的 K 个输出通过叠加编码得到最终输出符号。这样得到的链路速率域为：

$$\begin{aligned} \mathcal{R}_K &\triangleq \sum_{\alpha=1}^{K} \mathcal{R}_{K,\alpha} \\ &= \left\{ \sum_{\alpha=1}^{K} \left(r_{k,\alpha} : k \in [1:K] \right) : \left(r_{k,\alpha} : k \in [1:K] \right) \in \mathcal{R}_{K,\alpha}, \alpha \in [1:K] \right\}. \end{aligned}$$

显然这个速率域是容许速率域的一个内界，即

$$\mathcal{R}_K \subseteq \mathcal{R}_K^*. \tag{5–3}$$

□

5.1.2 主要结果

本章的主要结果针对分布式分层分集模型的容许速率域，证明了多层 Slepian-Wolf 码可以达到全部的容许速率域，是最优码。

定理 5.1（多址接入网络）：当 $K \leq 3$ 时，$\mathcal{R}_K = \mathcal{R}_K^*$。 □

定义 5.3（对称信源）：考虑信源 $U_{[1:K],[1:K]}$。如果对于 $\forall \alpha \in [1:K]$ 和满足 $|V| = |V'|$ 的两个集合 $V, V' \subseteq [1:K]$ 均有 $H\left(U_{V,\alpha}\right) = H\left(U_{V',\alpha}\right)$，则称信源 $U_{[1:K],[1:K]}$ 是对称的。□

定理 5.2（对称信源容许速率域）：如果信源 $U_{[1:K],[1:K]}$ 是对称的，那么 $\mathcal{R}_K = \mathcal{R}_K^*$。

□

定理 5.1 和定理 5.2 证明了 $\mathcal{R}_K = \mathcal{R}_K^*$，即待求的容许速率域 $\mathcal{R}_K$ 和多层 Slepian-Wolf 码可以达到的链路速率域 $\mathcal{R}_K^*$ 完全相同。它的意义包括：(1) 这一结果给出了分布式分层分集模型的容许速率域 $\mathcal{R}_K$ 的表示，即说明了 $\mathcal{R}_K$ 就是 $\mathcal{R}_K^*$。这一论断完全刻画了分布式分层分集模型的的极限性能；(2) 通过证明多层 Slepian-Wolf 码的可达链路速率域 $\mathcal{R}_K^*$ 就是分布式分层分集模型的容许速率域 $\mathcal{R}_K$，说明了多层 Slepian-Wolf 码可以达到容许速率域 $\mathcal{R}_K$ 中的所有容许速率，论证了 Slepian-Wolf 是分布式分层分集模型的最优码。

文献[16,17]中研究的分层分集模型的结果是定理 5.1 和定理 5.2 的特殊情况，即定理 5.1 证明了文献[16]中的结论，定理 5.2 证明了文献[17]中的结论。具体而言，让所有的$\forall \alpha \in [1:K]$有$U_{1,\alpha}=U_{2,\alpha}=\cdots=U_{K,\alpha}$就可以得到相应分层分集的结果。

定理 5.1 和定理 5.2 的证明见下一节。

5.2 定理证明

本节证明定理 5.1 和定理 5.2。证明的过程包括三个步骤：

(1) 分析$\mathcal{R}_K$的支撑超平面。具体而言，首先我们将逐个分析$\mathcal{R}_{K,\alpha}$（$\alpha \in [1:K]$）的支撑超平面，将寻找超平面的过程转化为分析含参线性规划问题，分析线性规划问题的 Lagrange 乘子[①]；

(2) 基于上一步找到的 Lagrange 乘子，构造一系列的熵不等式；

(3) 使用上一步构造的熵不等式，得到$\mathcal{R}_K$的一个外界，这个外界刚好和$\mathcal{R}_K^*$吻合。在证得$\mathcal{R}_K^* \subseteq \mathcal{R}_K$后，由于$\mathcal{R}_K \subseteq \mathcal{R}_K^*$，所以$\mathcal{R}_K^*=\mathcal{R}_K$。 □

在后续的几个小节中，我们将分别讨论这个三个环节。

5.2.1 含参线性规划的超平面分析

每个$\mathcal{R}_{K,\alpha}$的支持超平面由以$\mathbf{w} \triangleq (w_1, w_2, \cdots, w_K) \in \mathbb{R}_+^K$为参数的线性规划刻画：

$$\begin{aligned} \mathsf{LP}_{K,\alpha}^{\mathbf{w}}: \ \text{minimize} \quad & \sum_{k=1}^{K} w_k r_{k,\alpha} \\ \text{over} \quad & r_{k,\alpha}, \quad k \in [1:K] \\ \text{s.t.} \quad & \sum_{k \in V} r_{k,\alpha} \geq H\left(U_{V,\alpha} | U_{V',\alpha}\right), \quad V \in \mathbb{V}_{K,\alpha}, V' \in \mathbb{V}'_{K,\alpha}[V]. \end{aligned}$$

不失一般性，我们接下来将只分析w_k（$k \in [1:K]$）非负且有序的情况，即

$$\mathbb{W}_K \triangleq \{\mathbf{w}: w_1 \geq w_2 \geq \cdots \geq w_K \geq w_{K+1} \triangleq 0\}.$$

为了后续分析的方便，对于每个$\alpha \in [1:K]$，将$\mathbb{W}_K$划分为α个部分，即：

① 线性规划、线性规划的 Lagrange 乘子等概念及其相关性质是公知内容。更多信息可参见 https://en.wikipedia.org/wiki/Linear_programming 和 http://mathworld.wolfram.com/LagrangeMultiplier.html。

$$\mathbb{W}_{K,\alpha}^{(0)} \triangleq \left\{ \mathbf{w} \in \mathbb{W}_K : w_1 \le \frac{1}{\alpha - 1} \sum_{k=2}^{K} w_k \right\},$$

$$\mathbb{W}_{K,\alpha}^{(l)} \triangleq \left\{ \mathbf{w} \in \mathbb{W}_K : w_l > \frac{1}{\alpha - l} \sum_{k=l+1}^{K} w_k \text{ and } w_{l+1} \le \frac{1}{\alpha - (l+1)} \sum_{k=l+2}^{K} w_k \right\}, \quad l \in [1 : \alpha - 2],$$

$$\mathbb{W}_{K,\alpha}^{(\alpha-1)} \triangleq \left\{ \mathbf{w} \in \mathbb{W}_K : w_{\alpha-1} > \sum_{k=\alpha}^{K} w_k \right\}.$$

由于对于任意 $\mathbf{w} \in \mathbb{W}_K$，我们有

$$w_l > \frac{1}{\alpha - l} \sum_{k=l+1}^{K} w_k \quad \Rightarrow \quad w_{l'} > \frac{1}{\alpha - l'} \sum_{k=l'+1}^{K} w_k, \quad l' \in [1 : l]$$

$$w_l \le \frac{1}{\alpha - l} \sum_{k=l+1}^{K} w_k \quad \Rightarrow \quad w_{l'} \le \frac{1}{\alpha - l'} \sum_{k=l'+1}^{K} w_k, \quad l' \in [l : \alpha).$$

所以 $\mathbb{W}_{K,\alpha}^{(0)}, \cdots, \mathbb{W}_{K,\alpha}^{(\alpha-1)}$ 确实是 $\mathbb{W}_K$ 的一个分划。

对于 $\alpha = 0$，设定 $\mathbb{W}_{K,1}^{(0)} \triangleq \mathbb{W}_K$。

利用当今学术界主流的 Lagrange 乘子的定义，可以得到 $\mathsf{LP}_{K,\alpha}^{\mathbf{w}}$ 的 Lagrange 乘子的定义。

定义 5.4（Lagrange 乘子）：设 $f_\alpha^{\mathbf{w}}$ 为 $\mathsf{LP}_{K,\alpha}^{\mathbf{w}}$ 的最优值。若 $\left(c_{V|V',\alpha} : V \in \mathbb{V}_{K,\alpha}, V' \in \mathbb{V}'_{K,\alpha}[V]\right)$ 满足：

$$\sum_{V \in \mathbb{V}_{K,\alpha}} \sum_{V' \in \mathbb{V}'_{K,\alpha}[V]} c_{V|V',\alpha} H\left(U_{V,\alpha} \,|\, U_{V',\alpha}\right) = f_\alpha^{\mathbf{w}}, \tag{5–4}$$

$$\sum_{V \in \mathbb{V}_{K,\alpha} : k \in V} \sum_{V' \in \mathbb{V}'_{K,\alpha}[V]} c_{V|V',\alpha} = w_k, \quad k \in [1 : K], \tag{5–5}$$

$$c_{V|V',\alpha} \ge 0, \quad V \in \mathbb{V}_{K,\alpha}, V' \in \mathbb{V}'_{K,\alpha}[V],$$

则称 $\left(c_{V|V',\alpha} : V \in \mathbb{V}_{K,\alpha}, V' \in \mathbb{V}'_{K,\alpha}[V]\right)$ 是 $\mathsf{LP}_{K,\alpha}^{\mathbf{w}}$ 的 Lagrange 乘子。 □

对于 $\alpha = 1$ 和 $\alpha = K$ 的情况，我们很容易就能得到 $\mathsf{LP}_{K,\alpha}^{\mathbf{w}}$ 的 Lagrange 乘子。

引理 5.1（$\alpha = 1$）：对于以 $\mathbf{w} \in \mathbb{R}_+^K$ 为参数的线性规划，其最优解 $\left(r_{k,1}^{\text{opt}} : k \in [1 : K]\right)$ 为

$$r_{k,1}^{\text{opt}} \triangleq H\left(U_{k,1}\right), \quad k \in [1 : K].$$

Lagrange 乘子 $\left(c_{V|\varnothing,1} : V \in \mathbb{V}_{K,1}\right)$ 为

$$c_{\{k\}|\varnothing,1} \triangleq w_k, \quad k \in [1 : K].$$ □

引理 5.2（$\alpha = K$）：对于以 $\mathbf{w} \in \mathbb{W}_K$ 为参数的线性规划 $\mathsf{LP}_{K,K}^{\mathbf{w}}$，最优解为

$$r_{k,K}^{\mathrm{opt}} \triangleq H\left(U_{k,K} \,|\, U_{[k+1:K],K}\right), \quad k \in [1:K],$$

Lagrange 乘子为：

$$\begin{aligned} c_{[1:k][k+1:K],K} &\triangleq w_k - w_{k+1}, \quad k \in [1:K], \\ c_{V[1:K]\setminus V,K} &\triangleq 0, \qquad\qquad \text{其他.} \end{aligned}$$

□

但是对于一般的 $\alpha \in (1:K)$，得到 Lagrange 乘子并不容易。接下来，我们试图对 $K=3$，$\alpha = 2$ 这种情形进行分析。由此可以看出其形式还是很复杂的。

接下来我们先来分析 $\mathsf{LP}_{3,2}^{\mathbf{w}}$。为了求得 $\mathsf{LP}_{3,2}^{\mathbf{w}}$，我们将进行以下三个步骤：

(1) 构造一个新的优化问题 $\widetilde{\mathsf{LP}}_{3,2}^{\mathbf{w}}$，求得其 Lagrange 乘子；

(2) 证明 $\widetilde{\mathsf{LP}}_{3,2}^{\mathbf{w}}$ 和 $\mathsf{LP}_{3,2}^{\mathbf{w}}$ 的可行域相等；

(3) 利用 $\widetilde{\mathsf{LP}}_{3,2}^{\mathbf{w}}$ 的 Lagrange 乘子求得 $\mathsf{LP}_{3,2}^{\mathbf{w}}$ 的 Lagrange 乘子。 □

首先来看第一步。考虑一个新的线性规划问题：

$$\begin{aligned} \widetilde{\mathsf{LP}}_{3,2}^{\mathbf{w}}: \ \text{maximize} \quad & \sum_{k=1}^{3} w_k r_{k,2} \\ \text{over} \quad & r_{k,2}, \quad k \in [1:3] \\ \text{s.t.} \quad & r_{k,2} \ge \psi_{\{k\}}, \quad k \in [1:3] \\ & r_{i,2} + r_{j,2} \ge \psi_{\{i\}} + \psi_{\{i,j\}} + \psi_{\{j\}}, \quad i,j \in [1:3], i \ne j, \end{aligned}$$

其中 ψ_V，$V \in \mathbb{V}_{3,2}$ 是非负实数。

类似的 $\widetilde{\mathsf{LP}}_{3,2}^{\mathbf{w}}$ 也有相应的 Lagrange 乘子。令 $\tilde{f}_{\boldsymbol{\psi}}^{\mathbf{w}}$ 是 $\widetilde{\mathsf{LP}}_{3,2}^{\mathbf{w}}$ 的最优值。若 $\left(\tilde{c}_{V,2} : V \in \mathbb{V}_{3,2}\right)$ 满足

$$\begin{aligned} \sum_{k=1}^{3} \tilde{c}_{\{k\},2} \psi_{\{k\}} + \sum_{i,j \in [1:3], i<j} \tilde{c}_{\{i,j\},2} \left(\psi_{\{i\}} + \psi_{\{i,j\}} + \psi_{\{j\}}\right) &= \tilde{f}_{\boldsymbol{\psi}}^{\mathbf{w}}, \\ \sum_{V \in \mathbb{V}_{3,2}: k \in V} \tilde{c}_{V,2} &= w_k, \qquad k \in [1:3], \\ \tilde{c}_{V,2} &\ge 0, \qquad V \in \mathbb{V}_{3,2}, \end{aligned}$$

则 $\left(\tilde{c}_{V,2} : V \in \mathbb{V}_{3,2}\right)$ 是 $\widetilde{\mathsf{LP}}_{3,2}^{\mathbf{w}}$ 的 Lagrange 乘子。

为了求解这个 Lagrange 乘子，我们可以考虑以下五种情况，见表 5.1。

现在，在 $\widetilde{\mathsf{LP}}_{3,2}^{\mathbf{w}}$ 中取

表 5.1　$\widetilde{\mathsf{LP}}_{3,2}^{\mathbf{w}}$ 的最优解和 Lagrange 乘子

情况	条件	最优解	Lagrange 乘子
1	$\mathbf{w}\in\mathbb{W}_{3,2}^{(0)}$ $\psi_{\{1,2\}}\le\psi_{\{1,3\}}+\psi_{\{2,3\}}$ $\psi_{\{1,3\}}\le\psi_{\{1,2\}}+\psi_{\{2,3\}}$ $\psi_{\{2,3\}}\le\psi_{\{1,2\}}+\psi_{\{1,3\}}$	$\tilde{r}_{1,2}^{\mathrm{opt}}\triangleq\psi_{\{1\}}+\frac{1}{2}\left(\psi_{\{1,2\}}+\psi_{\{1,3\}}-\psi_{\{2,3\}}\right)$ $\tilde{r}_{2,2}^{\mathrm{opt}}\triangleq\psi_{\{2\}}+\frac{1}{2}\left(\psi_{\{1,2\}}-\psi_{\{1,3\}}+\psi_{\{2,3\}}\right)$ $\tilde{r}_{3,2}^{\mathrm{opt}}\triangleq\psi_{\{3\}}+\frac{1}{2}\left(-\psi_{\{1,2\}}+\psi_{\{1,3\}}+\psi_{\{2,3\}}\right)$	$\tilde{c}_{\{1,2\},2}\triangleq\frac{1}{2}\left(w_1+w_2-w_3\right)$ $\tilde{c}_{\{1,3\},2}\triangleq\frac{1}{2}\left(w_1-w_2+w_3\right)$ $\tilde{c}_{\{2,3\},2}\triangleq\frac{1}{2}\left(-w_1+w_2+w_3\right)$ $\tilde{c}_{V,2}\triangleq 0,\quad$ 其他
2	$\mathbf{w}\in\mathbb{W}_{3,2}^{(0)}$ $\psi_{\{1,2\}}>\psi_{\{1,3\}}+\psi_{\{2,3\}}$	$\tilde{r}_{1,2}^{\mathrm{opt}}\triangleq\psi_{\{1\}}+\psi_{\{1,3\}}$ $\tilde{r}_{2,2}^{\mathrm{opt}}\triangleq\psi_{\{2\}}+\psi_{\{1,2\}}-\psi_{\{1,3\}}$ $\tilde{r}_{3,2}^{\mathrm{opt}}\triangleq\psi_{\{3\}}$	$\tilde{c}_{\{3\},2}\triangleq -w_1+w_2+w_3$ $\tilde{c}_{\{1,2\},2}\triangleq w_2$ $\tilde{c}_{\{1,3\},2}\triangleq w_1-w_2$ $\tilde{c}_{V,2}\triangleq 0,\quad$ 其他
3	$\mathbf{w}\in\mathbb{W}_{3,2}^{(0)}$ $\psi_{\{1,3\}}>\psi_{\{1,2\}}+\psi_{\{2,3\}}$	$\tilde{r}_{1,2}^{\mathrm{opt}}\triangleq\psi_{\{1\}}+\psi_{\{1,2\}}$ $\tilde{r}_{2,2}^{\mathrm{opt}}\triangleq\psi_{\{2\}}$ $\tilde{r}_{3,2}^{\mathrm{opt}}\triangleq\psi_{\{3\}}+\psi_{\{1,3\}}-\psi_{\{1,2\}}$	$\tilde{c}_{\{2\},2}\triangleq -w_1+w_2+w_3$ $\tilde{c}_{\{1,2\},2}\triangleq w_1-w_3$ $\tilde{c}_{\{1,3\},2}\triangleq w_3$ $\tilde{c}_{V,2}\triangleq 0,\quad$ 其他
4	$\mathbf{w}\in\mathbb{W}_{3}$ $\psi_{\{2,3\}}>\psi_{\{1,2\}}+\psi_{\{1,3\}}$	$\tilde{r}_{1,2}^{\mathrm{opt}}\triangleq\psi_{\{1\}}$ $\tilde{r}_{2,2}^{\mathrm{opt}}\triangleq\psi_{\{2\}}+\psi_{\{1,2\}}$ $\tilde{r}_{3,2}^{\mathrm{opt}}\triangleq\psi_{\{3\}}+\psi_{\{2,3\}}-\psi_{\{1,2\}}$	$\tilde{c}_{\{1\},2}\triangleq w_1-w_2+w_3$ $\tilde{c}_{\{1,2\},2}\triangleq w_1-w_3$ $\tilde{c}_{\{2,3\},2}\triangleq w_3$ $\tilde{c}_{V,2}\triangleq 0,\quad$ 其他
5	$\mathbf{w}\in\mathbb{W}_{3,2}^{(1)}$ $\psi_{\{2,3\}}\le\psi_{\{1,2\}}+\psi_{\{1,3\}}$	$\tilde{r}_{1,2}^{\mathrm{opt}}\triangleq\psi_{\{1\}}$ $\tilde{r}_{2,2}^{\mathrm{opt}}\triangleq\psi_{\{2\}}+\psi_{\{1,2\}}$ $\tilde{r}_{3,2}^{\mathrm{opt}}\triangleq\psi_{\{3\}}+\psi_{\{1,3\}}$	$\tilde{c}_{\{1\},2}\triangleq w_1-w_2-w_3$ $\tilde{c}_{\{1,2\},2}\triangleq w_2$ $\tilde{c}_{\{1,3\},2}\triangleq w_3$ $\tilde{c}_{V,2}\triangleq 0,\quad$ 其他

$$\psi_{\{k\}} \triangleq H\left(U_{k,2} \mid U_{\nu_k,2}\right), \quad k \in [1:3],$$
$$\psi_{\{i,j\}} \triangleq \max\left\{H\left(U_{i,2},U_{j,2}\right)-\psi_i-\psi_j,0\right\}, \quad i,j \in [1:3], i \neq j,$$

其中 $\nu_k \triangleq \arg\max_{\nu \in [1:3]\setminus\{k\}} H\left(U_{k,2} \mid U_{\nu,2}\right)$。另外，定义

$$\widetilde{\mathcal{R}}_{3,2} \triangleq \Big\{\left(r_{k,2}:k \in [1:3]\right): r_{k,2} \geq \psi_{\{k\}}, k \in [1:3],$$
$$r_{i,2}+r_{j,2} \geq \psi_{\{i\}}+\psi_{\{i,j\}}+\psi_{\{j\}}, i,j \in [1:3], i \neq j\Big\}.$$

可以证明，$\widetilde{\mathcal{R}}_{3,2} = \mathcal{R}_{3,2}$。

引理 5.3：$\widetilde{\mathcal{R}}_{3,2} = \mathcal{R}_{3,2}$。 □

证明：见图 5.2，这个图即是 $\widetilde{\mathcal{R}}_{3,2}$ 的图，又是 $\mathcal{R}_{3,2}$ 的图。所以 $\widetilde{\mathcal{R}}_{3,2} = \mathcal{R}_{3,2}$。 □

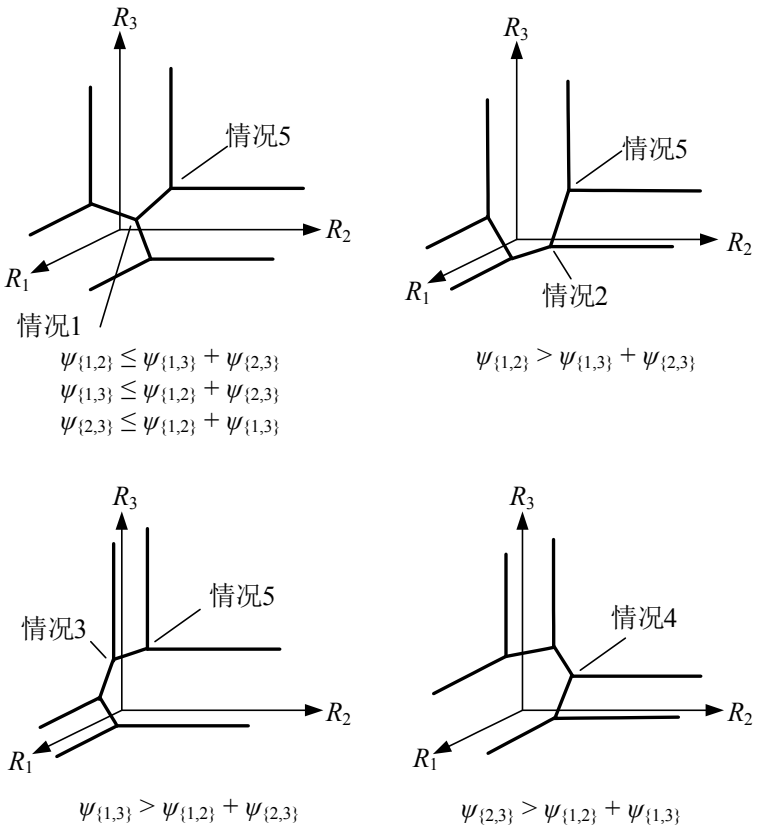


图 5.2　可行域 $\mathcal{R}_{3,2}$ 示意图

引理 5.4：设 i,j,k 是 $[1:3]$ 中三个互不相等的整数。则：

(1)

$$\psi_{\{i\}}+\psi_{\{i,j\}}+\psi_{\{j\}} = \begin{cases} H\left(U_{i,2},U_{j,2}\right), & H\left(U_{i,2},U_{j,2}\right) \geq \psi_{\{i\}}+\psi_{\{j\}}, \\ H\left(U_{i,2} \mid U_{k,2}\right)+H\left(U_{j,2} \mid U_{k,2}\right), & H\left(U_{i,2},U_{j,2}\right) < \psi_{\{i\}}+\psi_{\{j\}}. \end{cases}$$

(2) 如果$\psi_{\{i,j\}}>\psi_{\{i,k\}}+\psi_{\{j,k\}}$，则$\psi_{\{i\}}+\psi_{\{i,j\}}+\psi_{\{j\}}=H\left(U_{i,2},U_{j,2}\right)$；

(3) 如果$\psi_{\{i\}}+\psi_{\{i,j\}}+\psi_{\{j\}}=H\left(U_{i,2}\,|\,U_{k,2}\right)+H\left(U_{j,2}\,|\,U_{k,2}\right)$，则

$$\begin{aligned}\psi_{\{i\}}+\psi_{\{i,k\}}+\psi_{\{k\}}&=H\left(U_{i,2},U_{k,2}\right),\\ \psi_{\{j\}}+\psi_{\{j,k\}}+\psi_{\{k\}}&=H\left(U_{j,2},U_{k,2}\right).\end{aligned}$$

□

证明：(1) 根据$\psi_{\{i,j\}}$的定义，当$H\left(U_{i,2},U_{j,2}\right)\geq\psi_{\{i\}}+\psi_{\{j\}}$时，有$\psi_{\{i\}}+\psi_{\{i,j\}}+\psi_{\{j\}}=H\left(U_{i,2},U_{j,2}\right)$；当$H\left(U_{i,2},U_{j,2}\right)<\psi_{\{i\}}+\psi_{\{j\}}$时，我们有

$$\begin{aligned}\psi_{\{i\}}&=H\left(U_{i,2}\,|\,U_{k,2}\right),\\ \psi_{\{j\}}&=H\left(U_{j,2}\,|\,U_{k,2}\right),\\ \psi_{\{i,j\}}&=0,\end{aligned}$$

所以

$$\psi_{\{i\}}+\psi_{\{i,j\}}+\psi_{\{j\}}=H\left(U_{i,2}\,|\,U_{k,2}\right)+H\left(U_{j,2}\,|\,U_{k,2}\right).$$

得证。

(2) 注意到$\psi_{\{i,j\}}>\psi_{\{i,k\}}+\psi_{\{j,k\}}$时$\psi_{\{i,j\}}>0$，所以根据$\psi_{\{i,j\}}$的定义有

$$\psi_{\{i\}}+\psi_{\{i,j\}}+\psi_{\{j\}}=H\left(U_{i,2},U_{j,2}\right).$$

(3) 考虑到$\psi_{\{i\}}\geq H\left(U_{i,2}\,|\,U_{k,2}\right)$，$\psi_{\{j\}}\geq H\left(U_{j,2}\,|\,U_{k,2}\right)$且$\psi_{\{i,j\}}\geq 0$，有

$$\begin{aligned}\psi_{\{i\}}&=H\left(U_{i,2}\,|\,U_{k,2}\right),\\ \psi_{\{j\}}&=H\left(U_{j,2}\,|\,U_{k,2}\right),\\ \psi_{\{i,j\}}&=0.\end{aligned}\tag{5–6}$$

则$\psi_{\{i\}}+\psi_{\{i,j\}}+\psi_{\{j\}}=H\left(U_{i,2}\,|\,U_{k,2}\right)+H\left(U_{j,2}\,|\,U_{k,2}\right)$。

注意到

$$\begin{aligned}&H\left(U_{i,2},U_{k,2}\right)\\&=H\left(U_{i,2}\,|\,U_{k,2}\right)+H\left(U_{k,2}\right)\\&=\psi_{\{i\}}+H\left(U_{k,2}\right)\\&\geq\psi_{\{i\}}+\psi_{\{k\}},\end{aligned}\tag{5–7}$$

其中式（5–7）是由于式（5–6）。由于对称性，所以$H\left(U_{j,2},U_{k,2}\right)\geq\psi_{\{j\}}+\psi_{\{k\}}$。再考虑到$\psi_{\{i,k\}}$和$\psi_{\{j,k\}}$的定义，就可得证。 □

根据上述引理，$\psi_{\{i\}}+\psi_{\{i,j\}}+\psi_{\{j\}}$（$i,j\in[1:3],i\neq j$）的取值可能有以下 4 种情况：

(情况 A)

$$\begin{aligned}
&\psi_{\{1\}}+\psi_{\{1,2\}}+\psi_{\{2\}}=H\left(U_{1,2},U_{2,2}\right),\\
&\psi_{\{1\}}+\psi_{\{1,3\}}+\psi_{\{3\}}=H\left(U_{1,2},U_{3,2}\right),\\
&\psi_{\{2\}}+\psi_{\{2,3\}}+\psi_{\{3\}}=H\left(U_{2,2},U_{3,2}\right);
\end{aligned}$$

(情况 B)

$$\begin{aligned}
&\psi_{\{1\}}+\psi_{\{1,2\}}+\psi_{\{2\}}=H\left(U_{1,2},U_{2,2}\right),\\
&\psi_{\{1\}}+\psi_{\{1,3\}}+\psi_{\{3\}}=H\left(U_{1,2},U_{3,2}\right),\\
&\psi_{\{2\}}+\psi_{\{2,3\}}+\psi_{\{3\}}=H\left(U_{2,2}\,|\,U_{1,2}\right)+H\left(U_{3,2}\,|\,U_{1,2}\right);
\end{aligned}$$

(情况 C)

$$\begin{aligned}
&\psi_{\{1\}}+\psi_{\{1,2\}}+\psi_{\{2\}}=H\left(U_{1,2},U_{2,2}\right),\\
&\psi_{\{1\}}+\psi_{\{1,3\}}+\psi_{\{3\}}=H\left(U_{1,2}\,|\,U_{2,2}\right)+H\left(U_{3,2}\,|\,U_{2,2}\right),\\
&\psi_{\{2\}}+\psi_{\{2,3\}}+\psi_{\{3\}}=H\left(U_{2,2},U_{3,2}\right);
\end{aligned}$$

(情况 D)

$$\begin{aligned}
&\psi_{\{1\}}+\psi_{\{1,2\}}+\psi_{\{2\}}=H\left(U_{1,2}\,|\,U_{3,2}\right)+H\left(U_{2,2}\,|\,U_{3,2}\right),\\
&\psi_{\{1\}}+\psi_{\{1,3\}}+\psi_{\{3\}}=H\left(U_{1,2},U_{3,2}\right),\\
&\psi_{\{2\}}+\psi_{\{2,3\}}+\psi_{\{3\}}=H\left(U_{2,2},U_{3,2}\right);
\end{aligned}$$

现在，我们可以通过考虑$\widetilde{\mathsf{LP}}^{\mathbf{w}}_{3,2}$中所有的 Lagrange 乘子（见表 5.1，情况 1 到情况 5）和前述的四种情形（即情况 A 到情况 D）结合起来，得到$\mathsf{LP}^{\mathbf{w}}_{3,2}$的 Lagrange 乘子。例如，考虑情况 2 和情况 C 同时满足的情形（下成为情况 2C），可以验证

$$\begin{aligned}
\psi_{\{1\}}&=H\left(U_{1,2}\,|\,U_{2,2}\right),\\
\psi_{\{3\}}&=H\left(U_{3,2}\,|\,U_{2,2}\right),\\
\psi_{\{1,3\}}&=0,\\
\psi_{\{1\}}+\psi_{\{1,2\}}+\psi_{\{2\}}&=H\left(U_{1,2},U_{2,2}\right).
\end{aligned}$$

再考虑表 5.1 中给出的最优解$\left(\tilde{r}^{\mathrm{opt}}_{k,2}:k\in[1:3]\right)$，有

$$\begin{aligned}
&\tilde{r}^{\mathrm{opt}}_{1,2}=\psi_{\{1\}}+\psi_{\{1,3\}}=H\left(U_{1,2}\,|\,U_{2,2}\right),\\
&\tilde{r}^{\mathrm{opt}}_{2,2}=\psi_{\{2\}}+\psi_{\{1,2\}}-\psi_{\{1,3\}}=\left(\psi_{\{1\}}+\psi_{\{1,2\}}+\psi_{\{2\}}\right)-\left(\psi_{\{1\}}+\psi_{\{1,3\}}\right)=H\left(U_{2,2}\right),\\
&\tilde{r}^{\mathrm{opt}}_{3,2}=\psi_{\{3\}}=H\left(U_{3,2}\,|\,U_{2,2}\right).
\end{aligned}$$

由于引理 5.3 说$\widetilde{\mathcal{R}}_{3,2}=\mathcal{R}_{3,2}$，所以$\mathsf{LP}^{\mathbf{w}}_{3,2}$的最优解$r^{\mathrm{opt}}_{k,2}=\tilde{r}^{\mathrm{opt}}_{k,2}$（$k\in[1:K]$）。于是，$\mathsf{LP}^{\mathbf{w}}_{3,2}$的最优值为

$$f^{\mathbf{w}}_{2}=w_1H\left(U_{1,2}\,|\,U_{2,2}\right)+w_2H\left(U_{2,2}\right)+w_3H\left(U_{3,2}\,|\,U_{2,2}\right).$$

表 5.2　$\mathrm{LP}_{3,2}^{\mathrm{w}}$ 的 Lagrange 乘子

情况	$c_{\{1\}\|\{\nu_1\},2}$	$c_{\{2\}\|\{\nu_1\},2}$	$c_{\{3\}\|\{\nu_1\},2}$	$c_{\{1,2\}\|\varnothing,2}$	$c_{\{1,3\}\|\varnothing,2}$	$c_{\{2,3\}\|\varnothing,2}$
1A	0	0	0	$\frac{w_1+w_2-w_3}{2}$	$\frac{w_1-w_2+w_3}{2}$	$\frac{-w_1+w_2+w_3}{2}$
1B	0	$\frac{-w_1+w_2+w_3}{2}$	$\frac{-w_1+w_2+w_3}{2}$	$\frac{w_1+w_2-w_3}{2}$	$\frac{w_1-w_2+w_3}{2}$	0
1C	$\frac{w_1-w_2+w_3}{2}$	0	$\frac{w_1-w_2+w_3}{2}$	$\frac{w_1+w_2-w_3}{2}$	0	$\frac{-w_1+w_2+w_3}{2}$
1D	$\frac{w_1+w_2-w_3}{2}$	$\frac{w_1+w_2-w_3}{2}$	0	0	$\frac{w_1-w_2+w_3}{2}$	$\frac{-w_1+w_2+w_3}{2}$
2A	0	0	$-w_1+w_2+w_3$	w_2	w_1-w_2	0
2B	0	0	$-w_1+w_2+w_3$	w_2	w_1-w_2	0
2C	w_1-w_2	0	w_3	w_2	0	0
3A	0	$-w_1+w_2+w_3$	0	w_1-w_3	w_3	0
3B	0	$-w_1+w_2+w_3$	0	w_1-w_3	w_3	0
3D	w_1-w_3	w_2	0	0	w_3	0
4A	$w_1-w_2+w_3$	0	0	w_2-w_3	0	w_3
4C	$w_1-w_2+w_3$	0	0	w_2-w_3	0	w_3
4D	w_1	w_2-w_3	0	0	0	w_3
5A	$w_1-w_2-w_3$	0	0	w_2	w_3	0
5B	w_1-w_2	0	w_3	w_2	0	0
5C	$w_1-w_2-w_3$	0	0	w_2	w_3	0
5D	w_1-w_3	w_2	0	0	w_3	0

a. 对于 $k'\neq\nu_k$，取 $c_{\{k\}\|\{k'\},2}\triangleq 0$。

并且如下定义的$\left(c_{V|V',2}:V\in\mathbb{V}_{3,2},V'\in\mathbb{V}'_{3,2}[V]\right)$：

$$\begin{aligned}c_{\{1\}|\{2\},2}&\triangleq w_1-w_2,\\ c_{\{3\}|\{2\},2}&\triangleq w_3,\\ c_{\{1,2\}|\varnothing,2}&\triangleq w_2,\\ c_{V|V',2}&\triangleq 0,\quad \text{其他}\end{aligned}$$

是$\mathsf{LP}^{\mathbf{w}}_{3,2}$的 Lagrange 乘子。

用类似的方法可以得到其他情况下的 Lagrange 乘子（见后文引理 5.5）。值得一提的是，并不是所有的组合都是有意义的。具体而言，情况 2D、情况 3C 和情况 4B 违反了引理 5.4 (2)，所以这三种组合并不存在。

引理 5.5：对于以$\mathbf{w}\in\mathbb{W}_3$为参数的线性规划$\mathsf{LP}^{\mathbf{w}}_{3,2}$，表 5.2 中的$\left(c_{V|V',2}:V\in\mathbb{V}_{3,2},\ V'\in\mathbb{V}'_{3,2}[V]\right)$是其 Lagrange 乘子。对于更一般的以$\mathbf{w}\in\mathbb{R}^3_+$为参数的线性规划$\mathsf{LP}^{\mathbf{w}}_{3,2}$的 Lagrange 乘子可以通过交换$w_1$、$w_2$和$w_3$的次序得到。 □

至此，我们就得到了$\mathsf{LP}^{\mathbf{w}}_{3,2}$的 Lagrange 乘子。

对于一般的K，我们将只考虑对称信源的情况。当信源$U_{[1:K],[1:K]}$对称时，$V\in\mathbb{V}_{K,\alpha}$和$V'\in\mathbb{V}'_{K,\alpha}[V]$只通过$|V|$的值来影响$H\left(U_{V,\alpha}|U_{V',\alpha}\right)$的值。所以，原线性规划$\mathsf{LP}^{\mathbf{w}}_{K,\alpha}$可以改写成以下更简单的线性规划问题：

$$\begin{aligned}\overline{\mathsf{LP}}^{\mathbf{w}}_{K,\alpha}:\ \text{minimize}\quad & \sum_{k=1}^{K}w_k r_{k,\alpha}\\ \text{over}\quad & r_{k,\alpha},\quad k\in[1:K],\\ \text{s.t.}\quad & \sum_{k\in V}r_{k,\alpha}\geq H_{|V|,\alpha},\quad V\in\mathbb{V}_{K,\alpha}.\end{aligned}$$

显然线性规划$\overline{\mathsf{LP}}^{\mathbf{w}}_{K,\alpha}$也有自己的 Lagrange 乘子。

定义 5.5（Lagrange 乘子）：设$\overline{f}^{\mathbf{w}}_{\alpha}$是$\overline{\mathsf{LP}}^{\mathbf{w}}_{K,\alpha}$的最优值，若$\left(c_{V,\alpha}:V\in\mathbb{V}_{K,\alpha}\right)$满足：

$$\sum_{V\in\mathbb{V}_{K,\alpha}}c_{V,\alpha}H_{|V|,\alpha}=\overline{f}^{\mathbf{w}}_{\alpha},\tag{5–8}$$

$$\sum_{V\in\mathbb{V}_{K,\alpha}:k\in V}c_{V,\alpha}=w_k,\quad k\in[1:K],\tag{5–9}$$

$$c_{V,\alpha}\geq 0,\quad V\in\mathbb{V}_{K,\alpha},\tag{5–10}$$

则称$\left(c_{V,\alpha}:V\in\mathbb{V}_{K,\alpha}\right)$是$\overline{\mathsf{LP}}^{\mathbf{w}}_{K,\alpha}$的 Lagrange 乘子。 □

对于$l\in[0:\alpha)$，定义

$$r_{k,\alpha}^{(l)}\triangleq\begin{cases}H_{k,\alpha}-H_{k-1,\alpha}, & k\in[1:l],\\ \dfrac{H_{\alpha,\alpha}-H_{l,\alpha}}{\alpha-l}, & k\in[l+1:K],\end{cases}$$

其中$H_{0,\alpha}\triangleq 0$。

在后面，我们将要证明$\left(r_{k,\alpha}^{(l)}:k\in[1:K]\right)\in\mathcal{R}_{K,\alpha}$。为了证明$\left(r_{k,\alpha}^{(l)}:k\in[1:K]\right)\in\mathcal{R}_{K,\alpha}$，我们先来证明一个引理：

引理 5.6：考虑K个随机变量$X_{[1:K]}$，对于所有满足$|V|=|V'|$的两个集合$V,V'\subseteq[1:K]$，均有$H(X_V)=H(X_{V'})$。则对任意满足$i_1\le i_2\le j$的$i_1,i_2,j\in[1:K]$，均有

$$\frac{H\left(X_{[1:i_1]}\mid X_{[i_1+1:j]}\right)}{i_1}\le\frac{H\left(X_{[1:i_2]}\mid X_{[i_2+1:j]}\right)}{i_2}.$$ □

证明：当$i_1=i_2$时不等式两边相等，不等式显然成立。下面只考虑$i_1<i_2$的情况。

$$\begin{aligned}&i_2H\left(X_{[1:i_2]}\mid X_{[i_2+1:j]}\right)\\&=\sum_{k=1}^{i_2}H\left(X_{[1:i_2]}\mid X_{[i_2+1:j]}\right)\\&=\sum_{k=1}^{i_2}H\left(X_k\mid X_{[i_2+1:j]}\right)+\sum_{k=1}^{i_2}H\left(X_{[1:i_2]\setminus\{k\}}\mid X_{\{k\}\bigcup[i_2+1:j]}\right)\\&\ge H\left(X_{[1:i_2]}\mid X_{[i_2+1:j]}\right)+i_2H\left(X_{[1:i_2-1]}\mid X_{[i_2:j]}\right).\end{aligned}$$

于是，

$$\frac{H\left(X_{[1:i_2-1]}\mid X_{[i_2:j]}\right)}{i_2-1}\le\frac{H\left(X_{[1:i_2]}\mid X_{[i_2+1:j]}\right)}{i_2}.$$

这样我们就可以用数学归纳法证得结论。 □

引理 5.7：对于$l\in[0:\alpha)$，

$$\left(r_{k,\alpha}^{(l)}:k\in[1:K]\right)\in\mathcal{R}_{K,\alpha}.$$ □

证明：任意固定某个$V\in\mathbb{V}_{K,\alpha}$。令$V_1\triangleq V\bigcap[1:l]$，$V_2\triangleq V\setminus V_1$。接下来，我们要证明

$$\sum_{k\in V_1} H\left(U_{k,\alpha}\,|\,U_{[k+1:\alpha],\alpha}\right)+|V_2|\frac{H\left(U_{[l+1:\alpha],\alpha}\right)}{\alpha-l}\geq H\left(U_{[1:|V|],\alpha}\,|\,U_{[|V|+1:\alpha],\alpha}\right). \tag{5–11}$$

一方面，当$V_1\neq\varnothing$且$V_2\neq\varnothing$时有

$$\begin{aligned}&\sum_{k\in V_1} H\left(U_{k,\alpha}\,|\,U_{[k+1:\alpha],\alpha}\right)\\&=\sum_{\tau=1}^{|V_1|} H\left(U_{\langle V_1\rangle_\tau,\alpha}\,|\,U_{[\langle V_1\rangle_\tau+1:\alpha],\alpha}\right)\\&\geq\sum_{\tau=1}^{|V_1|} H\left(U_{\tau,\alpha}\,|\,U_{[\tau+1:\alpha],\alpha}\right) &\text{（5–12）}\\&=H\left(U_{[1:|V_1|],\alpha}\,|\,U_{[|V_1|+1:\alpha],\alpha}\right), &\text{（5–13）}\end{aligned}$$

其中式（5–12）是由于对$\tau\in[1:|V_1|]$均有$\langle V_1\rangle_\tau\geq\tau$，并且信源是对称的。

另一方面，

$$\begin{aligned}&|V_2|\frac{H\left(U_{[l+1:\alpha],\alpha}\right)}{\alpha-l}\\&\geq|V_2|\frac{H\left(U_{[1:\alpha-l],\alpha}\,|\,U_{[\alpha-l+1:\alpha-|V_1|],\alpha}\right)}{\alpha-l}\\&\geq H\left(U_{[1:|V_2|],\alpha}\,|\,U_{[|V_2|+1:\alpha-|V_1|],\alpha}\right) &\text{（5–14）}\\&=H\left(U_{[|V_1|+1:|V|],\alpha}\,|\,U_{[|V|+1:\alpha],\alpha}\right), &\text{（5–15）}\end{aligned}$$

其中（5–14）是因为引理 5.6 并且$\alpha-l\geq|V_2|$。将式（5–13）和式（5–15）结合，则可以证得当$V_1\neq\varnothing$且$V_2\neq\varnothing$时式（5–11）成立。

另外，当$V_1=\varnothing$时由式（5–15）可得式（5–11）成立，当$V_2=\varnothing$时由式（5–13）可得式（5–11）成立。这样就完成了引理的证明。　□

对任意的$\alpha\in[1:K]$和$l\in[0:\alpha)$，定义

$$\Omega_{K,\alpha}^{(l)}\triangleq\left\{V\subseteq[1:K]:|V|=\alpha,[1:l]\subseteq V\right\}.$$

前文提到，$\mathbb{W}_{K,\alpha}^{(0)},\cdots,\mathbb{W}_{K,\alpha}^{(\alpha-1)}$是$\mathbb{W}_K$的一个分划。对于$\mathbf{w}\in\mathbb{W}_K$和$\alpha\in[1:K]$，令$l_\alpha^{\mathbf{w}}$表示在$[0:\alpha)$使得$\mathbf{w}\in\mathbb{W}_{K,\alpha}^{(l_\alpha^{\mathbf{w}})}$。可以验证，

$$0=l_1^{\mathbf{w}}\leq l_2^{\mathbf{w}}\leq\cdots\leq l_{K-1}^{\mathbf{w}}\leq l_K^{\mathbf{w}}.$$

进一步的，对于$\mathbf{w}\in\mathbb{W}_K$和$\alpha\in[1:K]$，可以定义

$$\lambda_{\alpha}^{\mathbf{w}} \triangleq \frac{1}{\alpha - l_{\alpha}^{\mathbf{w}}} \sum_{k=l_{\alpha}^{\mathbf{w}}+1}^{K} w_k$$

$$\begin{aligned}
\mathbb{C}_{K,\alpha}^{\mathbf{w}} \triangleq \Big\{ \Big(c_{V,\alpha} : V \in \mathbb{V}_{K,\alpha} \Big) : & \\
c_{[1:k],\alpha} = w_k - w_{k+1}, \quad & k \in \big[1 : l_{\alpha}^{\mathbf{w}}\big), && \text{(5–16)} \\
c_{\left[1:l_{\alpha}^{\mathbf{w}}\right],\alpha} = w_{l_{\alpha}^{\mathbf{w}}} - \lambda_{\alpha}^{\mathbf{w}}, & && \text{(5–17)} \\
c_{V,\alpha} \geq 0, \quad & V \in \Omega_{K,\alpha}^{\left(l_{\alpha}^{\mathbf{w}}\right)}, && \text{(5–18)} \\
c_{V,\alpha} = 0, \quad & \text{其他}, && \text{(5–19)} \\
\sum_{V \in \Omega_{K,\alpha}^{\left(l_{\alpha}^{\mathbf{w}}\right)} : k \in V} c_{V,\alpha} = w_k, \quad & k \in \Big(l_{\alpha}^{\mathbf{w}} : K \Big] \Big\}. && \text{(5–20)}
\end{aligned}$$

注意当$l_{\alpha}^{\mathbf{w}} = 0$时，（5–16）和（5–17）是不存在的。另外，可以通过坐标变换，将$\mathbb{C}_{K,\alpha}^{\mathbf{w}}$的定义扩展到$\mathbf{w} \in \mathbb{R}_{+}^{K}$上。

引理 5.8：对任意的$\mathbf{w} \in \mathbb{W}_K$，给定$\left(c_{V,\alpha-1} : V \in \mathbb{V}_{K,\alpha-1} \right) \in \mathbb{C}_{K,\alpha-1}^{\mathbf{w}}$和$\left(c_{V,\alpha} : V \in \mathbb{V}_{K,\alpha} \right) \in \mathbb{C}_{K,\alpha}^{\mathbf{w}}$，有

$$\begin{aligned}
\sum_{V \in \Omega_{K,\alpha}^{\left(l_{\alpha}^{\mathbf{w}}\right)}} c_{V,\alpha} = \lambda_{\alpha}^{\mathbf{w}}, & && \text{(5–21)} \\
\sum_{V \in \mathbb{V}_{K,\alpha} : k \in V} c_{V,\alpha} = w_k, \quad & k \in \big[1 : K\big], && \text{(5–22)} \\
c_{V,\alpha} \geq 0, \quad & V \in \mathbb{V}_{K,\alpha}, && \text{(5–23)} \\
c_{\left[1:l_{\alpha-1}^{\mathbf{w}}\right],\alpha} - c_{\left[1:l_{\alpha-1}^{\mathbf{w}}\right],\alpha-1} = \theta_{\alpha}^{\mathbf{w}} \geq 0, & && \text{(5–24)} \\
\sum_{V \in \mathbb{V}_{K,\alpha}} c_{V,\alpha} = \begin{cases} \dfrac{1}{\alpha} \displaystyle\sum_{k=1}^{K} w_k, & l_{\alpha}^{\mathbf{w}} = 0, \\ w_1, & l_{\alpha}^{\mathbf{w}} > 0, \end{cases} & && \text{(5–25)}
\end{aligned}$$

其中

$$\theta_{\alpha}^{\mathbf{w}} \triangleq \left(\lambda_{\alpha}^{\mathbf{w}} - \sum_{k=l_{\alpha-1}^{\mathbf{w}}+1}^{l_{\alpha}^{\mathbf{w}}} (\alpha - 1 - k) c_{[1:k],\alpha} \right) \frac{1}{\alpha - 1 - l_{\alpha-1}^{\mathbf{w}}}. \qquad \text{(5–26)}$$

□

证明：我们来逐一验证式（5–21）到式（5–25）。

(1) 式（5–21）可由下式验证：

$$\begin{aligned}\sum_{k=l_\alpha^{\mathbf{w}}+1}^{K} w_k &= \sum_{k=l_\alpha^{\mathbf{w}}+1}^{K} \sum_{V\in\Omega_{K,\alpha}^{(l_\alpha^{\mathbf{w}})}:k\in V} c_{V,\alpha} \\ &= \sum_{V\in\Omega_{K,\alpha}^{(l_\alpha^{\mathbf{w}})}} c_{V,\alpha} \sum\nolimits_{k\in V\setminus\left[1:l_\alpha^{\mathbf{w}}\right]} 1 \\ &= \left(\alpha - l_\alpha^{\mathbf{w}}\right) \sum_{V\in\Omega_{K,\alpha}^{(l_\alpha^{\mathbf{w}})}} c_{V,\alpha}.\end{aligned}$$

(2) 式（5–22）的验证需要考虑以下两种情况：

(情况 1) $k\in\left[1:l_\alpha^{\mathbf{w}}\right]$。这种情况下，

$$\begin{aligned}\sum_{V\in\mathbb{V}_{K,\alpha}:k\in V} c_{V,\alpha} &= \sum_{i=k}^{l_\alpha^{\mathbf{w}}} c_{[1:i],\alpha} + \sum_{V\in\Omega_{K,\alpha}^{(l_\alpha^{\mathbf{w}})}} c_{V,\alpha} \\ &= w_k - \lambda_\alpha^{\mathbf{w}} + \sum_{V\in\Omega_{K,\alpha}^{(l_\alpha^{\mathbf{w}})}} c_{V,\alpha} \\ &= w_k, \qquad (5\text{–}27)\end{aligned}$$

其中（5–27）是由于式（5–21）。

(情况 2) $k\in\left(l_\alpha^{\mathbf{w}}:K\right]$。这种情况下，

$$\sum_{V\in\mathbb{V}_{K,\alpha}:k\in V} c_{V,\alpha} = \sum_{V\in\Omega_{K,\alpha}^{(l_\alpha^{\mathbf{w}})}:k\in V} c_{V,\alpha} = w_k.$$

于是得证。

(3) 式（5–23）的验证：由于 $\mathbf{w}\in\mathbb{W}_{K,\alpha}^{(l_\alpha^{\mathbf{w}})}$，所以当 $l_\alpha^{\mathbf{w}}\geq 1$ 时 $w_{l_\alpha^{\mathbf{w}}} - \lambda_\alpha^{\mathbf{w}} \geq 0$。进而得证。

(4) 式（5–24）的验证：考虑以下三种情况：

(情况 1) $l_{\alpha-1}^{\mathbf{w}} \leq l_\alpha^{\mathbf{w}} - 2$。这时有

$$\sum_{k=l_{\alpha-1}^{\mathbf{w}}+1}^{l_\alpha^{\mathbf{w}}} (\alpha - 1 - k) c_{[1:k],\alpha} = \left(\alpha - 1 - l_{\alpha-1}^{\mathbf{w}}\right) w_{l_{\alpha-1}^{\mathbf{w}}+1} - \sum_{k=l_{\alpha-1}^{\mathbf{w}}+1}^{l_\alpha^{\mathbf{w}}} w_k - \left(\alpha - 1 - l_\alpha^{\mathbf{w}}\right)\lambda_\alpha^{\mathbf{w}} \qquad (5\text{–}28)$$

且

$$\begin{aligned}\left(\alpha - l_\alpha^{\mathbf{w}}\right)\lambda_\alpha^{\mathbf{w}} + \sum_{k=l_{\alpha-1}^{\mathbf{w}}+1}^{l_\alpha^{\mathbf{w}}} w_k &= \sum_{k=l_\alpha^{\mathbf{w}}+1}^{K} w_k + \sum_{k=l_{\alpha-1}^{\mathbf{w}}+1}^{l_\alpha^{\mathbf{w}}} w_k \\ &= \sum_{k=l_{\alpha-1}^{\mathbf{w}}+1}^{K} w_k \\ &= \left(\alpha - 1 - l_{\alpha-1}^{\mathbf{w}}\right)\lambda_{\alpha-1}^{\mathbf{w}}. \qquad (5\text{–}29)\end{aligned}$$

所以

$$\begin{aligned}\theta_{\alpha}^{\mathbf{w}} &= \left(\lambda_{\alpha}^{\mathbf{w}} - \sum_{k=l_{\alpha-1}^{\mathbf{w}}+1}^{l_{\alpha}^{\mathbf{w}}} (\alpha-1-k)c_{[1:k],\alpha}\right)\frac{1}{\alpha-1-l_{\alpha-1}^{\mathbf{w}}} \\ &= \left(\lambda_{\alpha}^{\mathbf{w}} - \left(\alpha-1-l_{\alpha-1}^{\mathbf{w}}\right)w_{l_{\alpha-1}^{\mathbf{w}}+1} + \sum_{k=l_{\alpha-1}^{\mathbf{w}}+1}^{l_{\alpha}^{\mathbf{w}}} w_k + \left(\alpha-1-l_{\alpha}^{\mathbf{w}}\right)\lambda_{\alpha}^{\mathbf{w}}\right)\frac{1}{\alpha-1-l_{\alpha-1}^{\mathbf{w}}} \quad (5\text{–}30) \\ &= \left(\left(\alpha-l_{\alpha}^{\mathbf{w}}\right)\lambda_{\alpha}^{\mathbf{w}} + \sum_{k=l_{\alpha-1}^{\mathbf{w}}+1}^{l_{\alpha}^{\mathbf{w}}} w_k - \left(\alpha-1-l_{\alpha-1}^{\mathbf{w}}\right)w_{l_{\alpha-1}^{\mathbf{w}}+1}\right)\frac{1}{\alpha-1-l_{\alpha-1}^{\mathbf{w}}} \\ &= \left(\left(\alpha-1-l_{\alpha-1}^{\mathbf{w}}\right)\lambda_{\alpha-1}^{\mathbf{w}} - \left(\alpha-1-l_{\alpha-1}^{\mathbf{w}}\right)w_{l_{\alpha-1}^{\mathbf{w}}+1}\right)\frac{1}{\alpha-1-l_{\alpha-1}^{\mathbf{w}}} \quad (5\text{–}31) \\ &= \lambda_{\alpha-1}^{\mathbf{w}} - w_{l_{\alpha-1}^{\mathbf{w}}+1} \quad (5\text{–}32) \\ &= c_{\left[1:l_{\alpha-1}^{\mathbf{w}}\right],\alpha} - c_{\left[1:l_{\alpha-1}^{\mathbf{w}}\right],\alpha-1},\end{aligned}$$

其中（5–30）是由于（5–28），（5–31）是由于（5–29）。可以验证：

$$\begin{aligned}\left(\alpha-1-l_{\alpha-1}^{\mathbf{w}}\right)\lambda_{\alpha-1}^{\mathbf{w}} &= \sum_{k=l_{\alpha-1}^{\mathbf{w}}+1}^{K} w_k \\ &= \sum_{k=l_{\alpha-1}^{\mathbf{w}}+2}^{K} w_k + w_{l_{\alpha-1}^{\mathbf{w}}+1} \\ &\geq \left(\alpha-2-l_{\alpha-1}^{\mathbf{w}}\right)w_{l_{\alpha-1}^{\mathbf{w}}+1} + w_{l_{\alpha-1}^{\mathbf{w}}+1} \quad (5\text{–}33) \\ &= \left(\alpha-1-l_{\alpha-1}^{\mathbf{w}}\right)w_{l_{\alpha-1}^{\mathbf{w}}+1}, \quad (5\text{–}34)\end{aligned}$$

其中式（5–33）是由于$\mathbf{w}\in\mathbb{W}_{K,\alpha-1}^{\left(l_{\alpha-1}^{\mathbf{w}}\right)}$。将（5–32）和（5–34）结合可得$\theta_{\alpha}^{\mathbf{w}}\geq 0$。

(情况 2) $l_{\alpha-1}^{\mathbf{w}} = l_{\alpha}^{\mathbf{w}} - 1$。注意到

$$\begin{aligned}\left(\alpha-l_{\alpha}^{\mathbf{w}}\right)\lambda_{\alpha}^{\mathbf{w}} &= \sum_{k=l_{\alpha}^{\mathbf{w}}+1}^{K} w_k \\ &= \left(\alpha-1-l_{\alpha-1}^{\mathbf{w}}\right)\lambda_{\alpha-1}^{\mathbf{w}} - w_{l_{\alpha}^{\mathbf{w}}} \\ &= \left(\alpha-l_{\alpha}^{\mathbf{w}}\right)\lambda_{\alpha-1}^{\mathbf{w}} - w_{l_{\alpha}^{\mathbf{w}}}. \quad (5\text{–}35)\end{aligned}$$

进而有

$$\begin{aligned}\theta_{\alpha}^{\mathbf{w}} &= \left(\lambda_{\alpha}^{\mathbf{w}} - \left(\alpha-1-l_{\alpha}^{\mathbf{w}}\right)c_{\left[1:l_{\alpha}^{\mathbf{w}}\right],\alpha}\right)\frac{1}{\alpha-1-l_{\alpha-1}^{\mathbf{w}}} \\ &= \left(\lambda_{\alpha}^{\mathbf{w}} - \left(\alpha-1-l_{\alpha}^{\mathbf{w}}\right)\left(w_{l_{\alpha}^{\mathbf{w}}} - \lambda_{\alpha}^{\mathbf{w}}\right)\right)\frac{1}{\alpha-l_{\alpha}^{\mathbf{w}}} \\ &= \lambda_{\alpha-1}^{\mathbf{w}} - w_{l_{\alpha}^{\mathbf{w}}} \quad (5\text{–}36) \\ &= c_{\left[1:l_{\alpha-1}^{\mathbf{w}}\right],\alpha} - c_{\left[1:l_{\alpha-1}^{\mathbf{w}}\right],\alpha-1},\end{aligned}$$

其中（5–36）是由于（5–35）。由式（5–34）和式（5–36）可得$\theta_\alpha^{\mathbf{w}} \geq 0$。

(情况 3) $l_{\alpha-1}^{\mathbf{w}} = l_\alpha^{\mathbf{w}}$。这时

$$\theta_\alpha^{\mathbf{w}} = \frac{1}{\alpha - 1 - l_{\alpha-1}^{\mathbf{w}}} \lambda_\alpha^{\mathbf{w}} \geq 0.$$

另外，

$$\begin{aligned}
\frac{1}{\alpha - 1 - l_{\alpha-1}^{\mathbf{w}}} \lambda_\alpha^{\mathbf{w}} &= \frac{1}{\left(\alpha - 1 - l_\alpha^{\mathbf{w}}\right)\left(\alpha - l_\alpha^{\mathbf{w}}\right)} \sum_{k=l_\alpha^{\mathbf{w}}+1}^{K} w_k \\
&= \left(\frac{1}{\alpha - 1 - l_\alpha^{\mathbf{w}}} - \frac{1}{\alpha - l_\alpha^{\mathbf{w}}} \right) \sum_{k=l_\alpha^{\mathbf{w}}+1}^{K} w_k \\
&= \lambda_{\alpha-1}^{\mathbf{w}} - \lambda_\alpha^{\mathbf{w}} \\
&= c_{\left[1:l_{\alpha-1}^{\mathbf{w}}\right],\alpha} - c_{\left[1:l_{\alpha-1}^{\mathbf{w}}\right],\alpha-1}.
\end{aligned}$$

综合以上三种情况，式（5–24）得证。

(4) 式（5–25）的验证：考虑以下两种情况：

(情况 1) $l_\alpha^{\mathbf{w}} = 0$。这时

$$\begin{aligned}
\sum_{V \in \mathbb{V}_{K,\alpha}} c_{V,\alpha} &= \sum_{V \in \Omega_{K,\alpha}^{(0)}} c_{V,\alpha} \\
&= \frac{1}{\alpha} \sum_{k=1}^{K} w_k, \qquad \text{（5–37）}
\end{aligned}$$

其中式（5–37）是因为式（5–21）。

(情况 2) $l_\alpha^{\mathbf{w}} > 0$。这时

$$\begin{aligned}
\sum_{V \in \mathbb{V}_{K,\alpha}} c_{V,\alpha} &= \sum_{k=1}^{l_\alpha^{\mathbf{w}}-1} c_{[1:k],\alpha} + c_{\left[1:l_\alpha^{\mathbf{w}}\right],\alpha} + \sum_{V \in \Omega_{K,\alpha}^{\left(l_\alpha^{\mathbf{w}}\right)}} c_{V,\alpha} \\
&= \sum_{k=1}^{l_\alpha^{\mathbf{w}}-1} \left(w_k - w_{k+1}\right) + \left(w_{l_\alpha^{\mathbf{w}}} - \lambda_\alpha^{\mathbf{w}}\right) + \sum_{V \in \Omega_{K,\alpha}^{\left(l_\alpha^{\mathbf{w}}\right)}} c_{V,\alpha} \\
&= \sum_{k=1}^{l_\alpha^{\mathbf{w}}-1} \left(w_k - w_{k+1}\right) + \left(w_{l_\alpha^{\mathbf{w}}} - \lambda_\alpha^{\mathbf{w}}\right) + \lambda_\alpha^{\mathbf{w}} \qquad \text{（5–38）} \\
&= w_1,
\end{aligned}$$

其中式（5–38）是因为式（5–21）。

综合以上两种情况，（5–25）得证。 □

利用以上几个引理，我们可以证明$\mathbb{C}_{K,\alpha}^{\mathbf{w}}$中的每个元素都是$\overline{\mathsf{LP}}_{K,\alpha}^{\mathbf{w}}$的 Lagrange 乘子。

引理 5.9：给定以$\mathbf{w}\in\mathbb{W}_K$为参数的线性规划$\overline{\mathsf{LP}}_{K,\alpha}^{\mathbf{w}}$，则$\left(r_{k,\alpha}^{\left(l_\alpha^{\mathbf{w}}\right)}:k\in[1:K]\right)$是线性规划的最优解，$\left(c_{V,\alpha}:V\in\mathbb{V}_{K,\alpha}\right)\in\mathbb{C}_{K,\alpha}^{\mathbf{w}}$是 Lagrange 乘子。 □

证明：引理 5.7 告诉我们$\left(r_{k,\alpha}^{\left(l_\alpha^{\mathbf{w}}\right)}:k\in[1:K]\right)\in\mathcal{R}_{K,\alpha}$。考虑任一$\left(c_{V,\alpha}:V\in\mathbb{V}_{K,\alpha}\right)\in\mathbb{C}_{K,\alpha}^{\mathbf{w}}$，由引理 5.14 可知$\left(c_{V,\alpha}:V\in\mathbb{V}_{K,\alpha}\right)$满足式（5–9）和式（5–10）。注意到

$$\begin{aligned}\sum_{k=1}^{K}w_k r_{k,\alpha}^{\left(l_\alpha^{\mathbf{w}}\right)}&=\sum_{k=1}^{l_\alpha^{\mathbf{w}}}w_k\left(H_{k,\alpha}-H_{k-1,\alpha}\right)+\sum_{k=l_\alpha^{\mathbf{w}}+1}^{K}w_k\frac{H_{\alpha,\alpha}-H_{l_\alpha^{\mathbf{w}},\alpha}}{\alpha-l_\alpha^{\mathbf{w}}}\\&=\sum_{k=1}^{l_\alpha^{\mathbf{w}}-1}\left(w_k-w_{k+1}\right)H_{k,\alpha}+\left(w_{l_\alpha^{\mathbf{w}}}-\lambda_\alpha^{\mathbf{w}}\right)H_{l_\alpha^{\mathbf{w}},\alpha}+\lambda_\alpha^{\mathbf{w}}H_{\alpha,\alpha}\\&=\sum_{k=1}^{l_\alpha^{\mathbf{w}}-1}c_{[1:k],\alpha}H_{k,\alpha}+c_{\left[1:l_\alpha^{\mathbf{w}}\right],\alpha}H_{l_\alpha^{\mathbf{w}},\alpha}+\sum_{V\in\Omega_{K,\alpha}^{\left(l_\alpha^{\mathbf{w}}\right)}}c_{V,\alpha}H_{\alpha,\alpha}\qquad(5\text{–}39)\\&=\sum_{V\in\mathbb{V}_{K,\alpha}}c_{V,\alpha}H_{|V|,\alpha},\end{aligned}$$

其中式（5–39）是因为（5–21）。另一方面，对任意的$\left(r_{k,\alpha}:k\in[1:K]\right)\in\mathcal{R}_{K,\alpha}$，

$$\begin{aligned}\sum_{k=1}^{K}w_k r_{k,\alpha}&=\sum_{k=1}^{K}\sum_{V\in\mathbb{V}_{K,\alpha}:k\in V}c_{V,\alpha}r_{k,\alpha}\\&=\sum_{V\in\mathbb{V}_{K,\alpha}}c_{V,\alpha}\sum_{k\in V}r_{k,\alpha}\\&\geq\sum_{V\in\mathbb{V}_{K,\alpha}}c_{V,\alpha}H_{|V|,\alpha}.\end{aligned}$$

于是$\left(r_{k,\alpha}^{\left(l_\alpha^{\mathbf{w}}\right)}:k\in[1:K]\right)$是最优解，$\left(c_{V,\alpha}:V\in\mathbb{V}_{K,\alpha}\right)$满足（5–8），是 Lagrange 乘子。 □

5.2.2 以Lagrange乘子为系数的熵不等式

前面已经得到了优化问题$\mathsf{LP}_{K,\alpha}^{\mathbf{w}}$的 Lagrange 乘子。在这一步，我们将证明，对于固定的$\mathbf{w}\in\mathbb{R}_+^K$，优化问题列$\left(\mathsf{LP}_{K,\alpha}^{\mathbf{w}}:\alpha\in[1:K]\right)$存在一套 Lagrange 乘子$\left(c_{V|V',\alpha}:V\in\mathbb{V}_{K,\alpha},V'\in\mathbb{V}'_{K,\alpha}[V]\right)$（$\alpha\in[1:K]$），使得对任意的$K$个随机变量$X_{[1:K]}$，和$\alpha\geq\alpha'$，均满足

$$\sum_{V\in\mathbb{V}_{K,\alpha'}}\sum_{V'\in\mathbb{V}'_{K,\alpha'}[V]}c_{V|V',\alpha'}H\left(X_V\mid X_{V'}\right)\geq\sum_{V\in\mathbb{V}_{K,\alpha}}\sum_{V'\in\mathbb{V}'_{K,\alpha}[V]}c_{V|V',\alpha}H\left(X_V\mid X_{V'}\right).\qquad(5\text{–}40)$$

值得一提的是，这里的K个随机变量$X_{[1:K]}$是任意的、与系统无关的K个随机变量（而不是某链路的输入）。这个不等式中，对这K个随机变量的分布没有任何假设。这样的不等式称为熵不等式。

下面来验证式（5–40）。

当$K=1$时，式（5–40）无须验证。

当$K=2$时，式（5–40）的正确性可以由下列引理证明：

引理 5.10：$\left(c_{V|\varnothing,1}:V\in\mathbb{V}_{K,1}\right)$是$\mathsf{LP}_{K,1}^{\mathrm{w}}$的 Lagrange 乘子，$\left(c_{V|V',\alpha}:V\in\mathbb{V}_{K,\alpha},\right.$ $\left.V'\in\mathbb{V}'_{K,\alpha}[V]\right)$是$\mathsf{LP}_{K,\alpha}^{\mathrm{w}}$的 Lagrange 乘子。则对于任意$K$个随机变量$X_{[1:K]}$，有

$$\sum_{V\in\mathbb{V}_{K,1}} c_{V|\varnothing,1}H\left(X_V\right)\geq \sum_{V\in\mathbb{V}_{K,\alpha}}\sum_{V'\in\mathbb{V}'_{K,\alpha}[V]} c_{V|V',\alpha}H\left(X_V\mid X_{V'}\right). \qquad \square$$

证明：根据引理 5.1 和式（5–5），有

$$c_{\{k\}|\varnothing,1}=w_k=\sum_{V\in\mathbb{V}_{K,\alpha}:k\in V}\sum_{V'\in\mathbb{V}'_{K,\alpha}[V]} c_{V|V',\alpha},\quad k\in[1:K]. \tag{5–41}$$

可以验证，

$$\begin{aligned}
&\sum_{V\in\mathbb{V}_{K,1}} c_{V|\varnothing,1}H\left(X_V\right)\\
&=\sum_{k=1}^{K} c_{\{k\}|\varnothing,1}H\left(X_k\right)\\
&=\sum_{k=1}^{K}\sum_{V\in\mathbb{V}_{K,\alpha}:k\in V}\sum_{V'\in\mathbb{V}'_{K,\alpha}[V]} c_{V|V',\alpha}H\left(X_k\right) \qquad (5–42)\\
&=\sum_{V\in\mathbb{V}_{K,\alpha}}\sum_{V'\in\mathbb{V}'_{K,\alpha}[V]} c_{V|V',\alpha}\sum_{k\in V}H\left(X_k\right)\\
&\geq\sum_{V\in\mathbb{V}_{K,\alpha}}\sum_{V'\in\mathbb{V}'_{K,\alpha}[V]} c_{V|V',\alpha}H(X_V)\\
&\geq\sum_{V\in\mathbb{V}_{K,\alpha}}\sum_{V'\in\mathbb{V}'_{K,\alpha}[V]} c_{V|V',\alpha}H(X_V\mid X_{V'}),
\end{aligned}$$

其中式（5–42）是由于（5–41）。这样就完成了引理的证明。 $\square$

当$K=3$时，引理 5.10 可以验证$\alpha'=1$且$\alpha=2$时的情况。要完全验证不等式（5–40），还需要验证$\alpha'=2$且$\alpha=3$这种情况。也就是说，我们要证明如下引理：

引理 5.11：$\left(c_{V|V',2}:V\in\mathbb{V}_{3,2},V'\in\mathbb{V}'_{3,2}[V]\right)$是引理 5.5 中的 Lagrange 乘子，$\left(c_{V,3}:V\in\mathbb{V}_{3,3}\right)$是引理 5.2 中的 Lagrange 乘子，则对任意的三个随机变量$X_{[1:3]}$，有

$$\sum_{V\in\mathbb{V}_{3,2}}\sum_{V'\in\mathbb{V}'_{3,2}[V]} c_{V|V',2}H\left(X_V\mid X_{V'}\right)\geq\sum_{V\in\mathbb{V}_{3,3}} c_{V,3}H\left(X_V\mid X_{[1:3]\setminus V}\right). \qquad \square$$

证明：为了证明上述不等式，需要将$\left(c_{V|V',2}:V\in\mathbb{V}_{3,2},V'\in\mathbb{V}'_{3,2}[V]\right)$的表达式代入验证。如前所述，我们只考虑$\mathbf{w}\in\mathbb{W}_3$的诸情况（见表 5.2），验证如下：

(情况 1A) 这时有$\mathbf{w}\in\mathbb{W}_{3,2}^{(0)}$，

$$\begin{aligned}
&\frac{1}{2}(w_1+w_2-w_3)H(X_1,X_2)+\frac{1}{2}(w_1-w_2+w_3)H(X_1,X_3)\\
&\quad+\frac{1}{2}(-w_1+w_2+w_3)H(X_2,X_3)\\
&=(w_1-w_2)\big(H(X_1,X_2)+H(X_1,X_3)-H(X_1,X_2,X_3)\big)\\
&\quad+(w_2-w_3)H(X_1,X_2)\\
&\quad+\frac{1}{2}(-w_1+w_2+w_3)\big(H(X_1,X_2)+H(X_1,X_3)+H(X_2,X_3)\big)\\
&\quad+(w_1-w_2)H(X_1,X_2,X_3)\\
&\geq(w_1-w_2)H(X_1)+(w_2-w_3)H(X_1,X_2)\\
&\quad+\frac{1}{2}(-w_1+w_2+w_3)\big(H(X_1,X_2)+H(X_1,X_3)+H(X_2,X_3)\big)\\
&\quad+(w_1-w_2)H(X_1,X_2,X_3)\\
&\geq(w_1-w_2)H(X_1)+(w_2-w_3)H(X_1,X_2)+w_3H(X_1,X_2,X_3) \qquad (5\text{–}43)\\
&\geq(w_1-w_2)H(X_1|X_2,X_3)+(w_2-w_3)H(X_1,X_2|X_3)\\
&\quad+w_3H(X_1,X_2,X_3),
\end{aligned}$$

其中式（5–43）是因为 Han 不等式[73]。

(情况 1B) 这时有$\mathbf{w}\in\mathbb{W}_{3,2}^{(0)}$且$\nu_2=\nu_3=1$，

$$\begin{aligned}
&\frac{1}{2}\left(-w_1+w_2+w_3\right)\left(H\left(X_2\mid X_1\right)+H\left(X_3\mid X_1\right)\right)+\frac{1}{2}\left(w_1+w_2-w_3\right)H\left(X_1,X_2\right)\\
&\quad+\frac{1}{2}\left(w_1-w_2+w_3\right)H\left(X_1,X_3\right)\\
&\geq\frac{1}{2}\left(-w_1+w_2+w_3\right)\left(H\left(X_2\mid X_1,X_3\right)+H\left(X_3\mid X_1,X_2\right)\right)\\
&\quad+\frac{1}{2}\left(w_1+w_2-w_3\right)H\left(X_1,X_2\right)+\frac{1}{2}\left(w_1-w_2+w_3\right)H\left(X_1,X_3\right)\\
&=\left(w_1-w_2\right)\left(H\left(X_1,X_2\right)+H\left(X_1,X_3\right)-H\left(X_1,X_2,X_3\right)\right)+\left(w_2-w_3\right)H\left(X_1,X_2\right)\\
&\quad+\frac{1}{2}\left(-w_1+w_2+w_3\right)\left(H\left(X_3\mid X_1,X_2\right)+H\left(X_1,X_2\right)\right)\\
&\quad+\frac{1}{2}\left(-w_1+w_2+w_3\right)\left(H\left(X_2\mid X_1,X_3\right)+H\left(X_1,X_3\right)\right)+\left(w_1-w_2\right)H\left(X_1,X_2,X_3\right)\\
&\geq\left(w_1-w_2\right)H\left(X_1\right)+\left(w_2-w_3\right)H\left(X_1,X_2\right)+w_3H\left(X_1,X_2,X_3\right)\\
&\geq\left(w_1-w_2\right)H\left(X_1\mid X_2,X_3\right)+\left(w_2-w_3\right)H\left(X_1,X_2\mid X_3\right)+w_3H\left(X_1,X_2,X_3\right).
\end{aligned}$$

(情况 1C) 这时有 $\nu_1=\nu_3=2$，

$$\begin{aligned}
&\frac{1}{2}\left(w_1-w_2+w_3\right)\left(H\left(X_1\mid X_2\right)+H\left(X_3\mid X_2\right)\right)\\
&\quad+\frac{1}{2}\left(w_1+w_2-w_3\right)H\left(X_1,X_2\right)+\frac{1}{2}\left(-w_1+w_2+w_3\right)H\left(X_2,X_3\right)\\
&\geq\frac{1}{2}\left(w_1-w_2+w_3\right)\left(H\left(X_1\mid X_2,X_3\right)+H\left(X_3\mid X_1,X_2\right)\right)\\
&\quad+\frac{1}{2}\left(w_1+w_2-w_3\right)H\left(X_1,X_2\right)+\frac{1}{2}\left(-w_1+w_2+w_3\right)H\left(X_2,X_3\right)\\
&=\left(w_1-w_2\right)H\left(X_1\mid X_2,X_3\right)+\left(w_2-w_3\right)H\left(X_1,X_2\right)\\
&\quad+\frac{1}{2}\left(-w_1+w_2+w_3\right)\left(H\left(X_1\mid X_2,X_3\right)+H\left(X_2,X_3\right)\right)\\
&\quad+\frac{1}{2}\left(w_1-w_2+w_3\right)\left(H\left(X_3\mid X_1,X_2\right)+H\left(X_1,X_2\right)\right)\\
&=\left(w_1-w_2\right)H\left(X_1\mid X_2,X_3\right)+\left(w_2-w_3\right)H\left(X_1,X_2\right)+w_3H\left(X_1,X_2,X_3\right)\\
&\geq\left(w_1-w_2\right)H\left(X_1\mid X_2,X_3\right)+\left(w_2-w_3\right)H\left(X_1,X_2\mid X_3\right)+w_3H\left(X_1,X_2,X_3\right).
\end{aligned}$$

(情况 1D) 这时有 $\nu_1=\nu_2=3$，

$$\begin{aligned}
&\frac{1}{2}\left(w_1+w_2-w_3\right)\left(H\left(X_1\mid X_3\right)+H\left(X_2\mid X_3\right)\right)\\
&\quad+\frac{1}{2}\left(w_1-w_2+w_3\right)H\left(X_1,X_3\right)+\frac{1}{2}\left(-w_1+w_2+w_3\right)H\left(X_2,X_3\right)\\
&\geq\frac{1}{2}\left(w_1+w_2-w_3\right)\left(H\left(X_1\mid X_2,X_3\right)+H\left(X_2\mid X_3\right)\right)\\
&\quad+\frac{1}{2}\left(w_1-w_2+w_3\right)H\left(X_1,X_3\right)+\frac{1}{2}\left(-w_1+w_2+w_3\right)H\left(X_2,X_3\right)\\
&\geq\left(w_1-w_2\right)H\left(X_1\mid X_2,X_3\right)+\left(w_2-w_3\right)H\left(X_1,X_2\mid X_3\right)\\
&\quad+\frac{1}{2}\left(-w_1+w_2+w_3\right)\left(H\left(X_1\mid X_2,X_3\right)+H\left(X_2,X_3\right)\right)\\
&\quad+\frac{1}{2}\left(w_1-w_2+w_3\right)\left(H\left(X_2\mid X_1,X_3\right)+H\left(X_1,X_3\right)\right)\\
&=\left(w_1-w_2\right)H\left(X_1\mid X_2,X_3\right)+\left(w_2-w_3\right)H\left(X_1,X_2\mid X_3\right)+w_3H\left(X_1,X_2,X_3\right).
\end{aligned}$$

(情况 2A) 和 (情况 2B) 这时有 $\mathbf{w}\in\mathbb{W}_{3,2}^{(0)}$，

$$\begin{aligned}
&\left(-w_1+w_2+w_3\right)H\left(X_3\mid X_{\nu_3}\right)+w_2H\left(X_1,X_2\right)+\left(w_1-w_2\right)H\left(X_1,X_3\right)\\
&\geq\left(-w_1+w_2+w_3\right)H\left(X_3\mid X_1,X_2\right)+w_2H\left(X_1,X_2\right)+\left(w_1-w_2\right)H\left(X_1,X_3\right)\\
&=\left(w_1-w_2\right)\left(H\left(X_1,X_2\right)+H\left(X_1,X_3\right)-H\left(X_1,X_2,X_3\right)\right)+\left(w_2-w_3\right)H\left(X_1,X_2\right)\\
&\quad+\left(-w_1+w_2+w_3\right)\left(H\left(X_3\mid X_1,X_2\right)+H\left(X_1,X_2\right)\right)+\left(w_1-w_2\right)H\left(X_1,X_2,X_3\right)\\
&\geq\left(w_1-w_2\right)H\left(X_1\right)+\left(w_2-w_3\right)H\left(X_1,X_2\right)+w_3H\left(X_1,X_2,X_3\right)\\
&\geq\left(w_1-w_2\right)H\left(X_1\mid X_2,X_3\right)+\left(w_2-w_3\right)H\left(X_1,X_2\mid X_3\right)+w_3H\left(X_1,X_2,X_3\right).
\end{aligned}$$

(情况 2C) 和 (情况 5B)

$$\begin{aligned}
&\left(w_1-w_2\right)H\left(X_1\mid X_{\nu_1}\right)+w_3H\left(X_3\mid X_{\nu_3}\right)+w_2H\left(X_1,X_2\right)\\
&\geq\left(w_1-w_2\right)H\left(X_1\mid X_2,X_3\right)+w_3H\left(X_3\mid X_1,X_2\right)+w_2H\left(X_1,X_2\right)\\
&=\left(w_1-w_2\right)H\left(X_1\mid X_2,X_3\right)+\left(w_2-w_3\right)H\left(X_1,X_2\right)+w_3H\left(X_1,X_2,X_3\right)\\
&\geq\left(w_1-w_2\right)H\left(X_1\mid X_2,X_3\right)+\left(w_2-w_3\right)H\left(X_1,X_2\mid X_3\right)+w_3H\left(X_1,X_2,X_3\right).
\end{aligned}$$

(情况 3A) 和 (情况 3B) 这时有 $\mathbf{w}\in\mathbb{W}_{3,2}^{(0)}$，

$$\begin{aligned}
&\left(-w_1+w_2+w_3\right)H\left(X_2\mid X_{\nu_2}\right)+\left(w_1-w_3\right)H\left(X_1,X_2\right)+w_3H\left(X_1,X_3\right)\\
&\geq\left(-w_1+w_2+w_3\right)H\left(X_2\mid X_1,X_3\right)+\left(w_1-w_3\right)H\left(X_1,X_2\right)+w_3H\left(X_1,X_3\right)\\
&=\left(w_1-w_2\right)\left(H\left(X_1,X_2\right)+H\left(X_1,X_3\right)-H\left(X_1,X_2,X_3\right)\right)+\left(w_2-w_3\right)H\left(X_1,X_2\right)\\
&\quad+\left(w_1-w_2\right)H\left(X_1,X_2,X_3\right)+\left(-w_1+w_2+w_3\right)\left(H\left(X_2\mid X_1,X_3\right)+H\left(X_1,X_3\right)\right)\\
&\geq\left(w_1-w_2\right)H\left(X_1\right)+\left(w_2-w_3\right)H\left(X_1,X_2\right)+w_3H\left(X_1,X_2,X_3\right)\\
&\geq\left(w_1-w_2\right)H\left(X_1\mid X_2,X_3\right)+\left(w_2-w_3\right)H\left(X_1,X_2\mid X_3\right)+w_3H\left(X_1,X_2,X_3\right).
\end{aligned}$$

(情况 3D) 和 (情况 5D) 这时有$\nu_1=\nu_2=3$，

$$\begin{aligned}
&(w_1-w_3)H(X_1\mid X_3)+w_2H(X_2\mid X_3)+w_3H(X_1,X_3)\\
&\geq(w_1-w_3)H(X_1\mid X_3)+w_2H(X_2\mid X_1,X_3)+w_3H(X_1,X_3)\\
&=(w_1-w_2)H(X_1\mid X_3)+(w_2-w_3)H(X_1,X_2\mid X_3)+w_3H(X_1,X_2,X_3)\\
&\geq(w_1-w_2)H(X_1\mid X_2,X_3)+(w_2-w_3)H(X_1,X_2\mid X_3)+w_3H(X_1,X_2,X_3).
\end{aligned}$$

(情况 4A) 和 (情况 4C)

$$\begin{aligned}
&(w_1-w_2+w_3)H(X_1\mid X_{\nu_1})+(w_2-w_3)H(X_1,X_2)+w_3H(X_2,X_3)\\
&\geq(w_1-w_2+w_3)H(X_1\mid X_2,X_3)+(w_2-w_3)H(X_1,X_2)+w_3H(X_2,X_3)\\
&=(w_1-w_2)H(X_1\mid X_2,X_3)+(w_2-w_3)H(X_1,X_2)+w_3H(X_1,X_2,X_3)\\
&\geq(w_1-w_2)H(X_1\mid X_2,X_3)+(w_2-w_3)H(X_1,X_2\mid X_3)+w_3H(X_1,X_2,X_3).
\end{aligned}$$

(情况 4D) 这时有$\nu_1=\nu_2=3$，

$$\begin{aligned}
&w_1H(X_1\mid X_3)+(w_2-w_3)H(X_2\mid X_3)+w_3H(X_2,X_3)\\
&\geq(w_1-w_2+w_3)H(X_1\mid X_2,X_3)\\
&+(w_2-w_3)\big(H(X_1\mid X_3)+H(X_2\mid X_3)\big)+w_3H(X_2,X_3)\\
&=(w_1-w_2)H(X_1\mid X_2,X_3)\\
&+(w_2-w_3)\big(H(X_1\mid X_3)+H(X_2\mid X_3)\big)+w_3H(X_1,X_2,X_3)\\
&\geq(w_1-w_2)H(X_1\mid X_2,X_3)+(w_2-w_3)H(X_1,X_2\mid X_3)+w_3H(X_1,X_2,X_3).
\end{aligned}$$

(情况 5A) 和 (情况 5C)

$$\begin{aligned}
&(w_1-w_2-w_3)H(X_1\mid X_{\nu_1})+w_2H(X_1,X_2)+w_3H(X_1,X_3)\\
&\geq(w_1-w_2)H(X_1\mid X_2,X_3)+(w_2-w_3)H(X_1,X_2)\\
&+w_3\big(H(X_1,X_2)+H(X_1,X_3)-H(X_1)\big)\\
&\geq(w_1-w_2)H(X_1\mid X_2,X_3)+(w_2-w_3)H(X_1,X_2)+w_3H(X_1,X_2,X_3)\\
&\geq(w_1-w_2)H(X_1\mid X_2,X_3)+(w_2-w_3)H(X_1,X_2\mid X_3)+w_3H(X_1,X_2,X_3).
\end{aligned}$$

这样就完成了引理的验证。 □

对于一般的K，我们考虑信源对称的情况。

定义示性函数

$$\mathcal{I}(\text{事件})\triangleq\begin{cases}1, & \text{事件为真}\\ 0, & \text{事件为假.}\end{cases}$$

首先来证明几个引理：

引理 5.12：对于满足 $\lambda_\alpha^{\mathbf{w}}>0$ 的 $\mathbf{w}\in\mathbb{W}_K$，和 $\left(c_{V,\alpha}:V\in\mathbb{V}_{K,\alpha}\right)\in\mathbb{C}_{K,\alpha}^{\mathbf{w}}$，定义 $\left(c_{V',\alpha-1}:V'\in\mathbb{V}_{K,\alpha-1}\right)$ 如下：

$$
\begin{aligned}
c_{[1:k],\alpha-1} &\triangleq w_k-w_{k+1},\quad k\in\left[1:l_{\alpha-1}^{\mathbf{w}}\right),\\
c_{\left[1:l_{\alpha-1}^{\mathbf{w}}\right],\alpha-1} &\triangleq w_{l_{\alpha-1}^{\mathbf{w}}}-\lambda_{\alpha-1}^{\mathbf{w}},\\
c_{V',\alpha-1} &\triangleq \frac{\theta_\alpha^{\mathbf{w}}}{\lambda_\alpha^{\mathbf{w}}}\sum_{V\in\Omega_{K,\alpha}^{\left(l_\alpha^{\mathbf{w}}\right)}:V'\subseteq V} c_{V,\alpha}\\
&\qquad+\frac{1}{\lambda_\alpha^{\mathbf{w}}}\sum_{V\in\Omega_{K,\alpha}^{\left(l_\alpha^{\mathbf{w}}\right)}} c_{V,\alpha}\sum_{k=l_{\alpha-1}^{\mathbf{w}}+1}^{l_\alpha^{\mathbf{w}}} c_{[1:k],\alpha}\sum_{\tau=k+1}^{\alpha}\mathcal{I}\left\{V'=\langle V\rangle_{[1:\alpha]\setminus\{\tau\}}\right\},\quad V'\in\Omega_{K,\alpha-1}^{\left(l_{\alpha-1}^{\mathbf{w}}\right)},\\
c_{V',\alpha-1} &\triangleq 0,\quad \text{其他},
\end{aligned}
$$

其中 $\theta_\alpha^{\mathbf{w}}$ 由式（5–26）给出。则以下命题为真：

(1) $\left(c_{V',\alpha-1}:V'\in\mathbb{V}_{K,\alpha-1}\right)\in\mathbb{C}_{K,\alpha-1}^{\mathbf{w}}$.

(2) 对于任意 K 个随机变量 $X_{[1:K]}$，有

$$
\sum_{V'\in\mathbb{V}_{K,\alpha-1}} c_{V',\alpha-1}H\left(X_{V'}\right)\geq\sum_{V\in\mathbb{V}_{K,\alpha}} c_{V,\alpha}H\left(X_V\right).
$$

□

证明：(1) 显然式（5–16）、式（5–17）和式（5–19）成立。另外，式（5–24）说明式（5–18）成立。接下来验证式（5–20）。

考虑某个整数 $k\in\left(l_{\alpha-1}^{\mathbf{w}}:K\right]$。我们有

$$
\begin{aligned}
&\sum_{V'\in\Omega_{K,\alpha-1}^{\left(l_{\alpha-1}^{\mathbf{w}}\right)}:k\in V'}\ \sum_{V\in\Omega_{K,\alpha}^{\left(l_\alpha^{\mathbf{w}}\right)}:V'\subseteq V}\frac{c_{V,\alpha}}{\alpha-1-l_{\alpha-1}^{\mathbf{w}}}\\
&\quad=\sum_{V\in\Omega_{K,\alpha}^{\left(l_\alpha^{\mathbf{w}}\right)}:k\in V}\frac{\left|\left\{V'\in\Omega_{K,\alpha-1}^{\left(l_{\alpha-1}^{\mathbf{w}}\right)}:k\in V'\subseteq V\right\}\right|}{\alpha-1-l_{\alpha-1}^{\mathbf{w}}}c_{V,\alpha}\\
&\quad=\sum_{V\in\Omega_{K,\alpha}^{\left(l_\alpha^{\mathbf{w}}\right)}:k\in V} c_{V,\alpha}.
\end{aligned}
\tag{5–44}
$$

注意到

$$
\begin{aligned}
&\sum_{V'\in\Omega_{K,\alpha-1}^{\left(l_{\alpha-1}^{\mathbf{w}}\right)}:k\in V'}\frac{1}{\lambda_\alpha^{\mathbf{w}}}\sum_{V\in\Omega_{K,\alpha}^{\left(l_\alpha^{\mathbf{w}}\right)}} c_{V,\alpha}\sum_{i=l_{\alpha-1}^{\mathbf{w}}+1}^{l_\alpha^{\mathbf{w}}} c_{[1:i],\alpha}\sum_{\tau=i+1}^{\alpha}\mathcal{I}\left\{V'=\langle V\rangle_{[1:\alpha]\setminus\{\tau\}}\right\}\\
&\quad=\frac{1}{\lambda_\alpha^{\mathbf{w}}}\sum_{V\in\Omega_{K,\alpha}^{\left(l_\alpha^{\mathbf{w}}\right)}} c_{V,\alpha}\sum_{i=l_{\alpha-1}^{\mathbf{w}}+1}^{l_\alpha^{\mathbf{w}}} c_{[1:i],\alpha}\sum_{\tau=i+1}^{\alpha}\ \sum_{V'\in\Omega_{K,\alpha-1}^{\left(l_{\alpha-1}^{\mathbf{w}}\right)}:k\in V'}\mathcal{I}\left\{V'=\langle V\rangle_{[1:\alpha]\setminus\{\tau\}}\right\}.
\end{aligned}
\tag{5–45}
$$

另外，

$$\sum_{\tau=i+1}^{\alpha}\sum_{V'\in\Omega_{K,\alpha-1}^{\left(l_{\alpha-1}^{\mathbf{w}}\right)}:k\in V'}\mathcal{I}\left\{V'=\langle V\rangle_{[1:\alpha]\setminus\{\tau\}}\right\}$$

$$=\sum_{\tau=i+1}^{\alpha}\mathcal{I}\left\{k\in\langle V\rangle_{[1:\alpha]\setminus\{\tau\}}\right\}$$

$$=(\alpha-1-i)\mathcal{I}\{k\in V\}+\mathcal{I}\left\{k\in\langle V\rangle_{[1:i]}\right\},\quad V\in\Omega_{K,\alpha}^{\left(l_{\alpha}^{\mathbf{w}}\right)},i\in\left(l_{\alpha-1}^{\mathbf{w}}:l_{\alpha}^{\mathbf{w}}\right].\qquad(5\text{–}46)$$

于是，

$$\sum_{V'\in\Omega_{K,\alpha-1}^{\left(l_{\alpha-1}^{\mathbf{w}}\right)}:k\in V'}\frac{1}{\lambda_{\alpha}^{\mathbf{w}}}\sum_{V\in\Omega_{K,\alpha}^{\left(l_{\alpha}^{\mathbf{w}}\right)}}c_{V,\alpha}\sum_{i=l_{\alpha-1}^{\mathbf{w}}+1}^{l_{\alpha}^{\mathbf{w}}}c_{[1:i],\alpha}\sum_{\tau=i+1}^{\alpha}\mathcal{I}\left\{V'=\langle V\rangle_{[1:\alpha]\setminus\{\tau\}}\right\}$$

$$=\frac{1}{\lambda_{\alpha}^{\mathbf{w}}}\sum_{V\in\Omega_{K,\alpha}^{\left(l_{\alpha}^{\mathbf{w}}\right)}}c_{V,\alpha}\sum_{i=l_{\alpha-1}^{\mathbf{w}}+1}^{l_{\alpha}^{\mathbf{w}}}c_{[1:i],\alpha}\left((\alpha-1-i)\mathcal{I}\{k\in V\}+\mathcal{I}\left\{k\in\langle V\rangle_{[1:i]}\right\}\right)\qquad(5\text{–}47)$$

$$=\frac{1}{\lambda_{\alpha}^{\mathbf{w}}}\sum_{i=l_{\alpha-1}^{\mathbf{w}}+1}^{l_{\alpha}^{\mathbf{w}}}(\alpha-1-i)c_{[1:i],\alpha}\sum_{V\in\Omega_{K,\alpha}^{\left(l_{\alpha}^{\mathbf{w}}\right)}:k\in V}c_{V,\alpha}$$

$$+\frac{1}{\lambda_{\alpha}^{\mathbf{w}}}\sum_{V\in\Omega_{K,\alpha}^{\left(l_{\alpha}^{\mathbf{w}}\right)}:k\in V}c_{V,\alpha}\sum_{i=l_{\alpha-1}^{\mathbf{w}}+1}^{l_{\alpha}^{\mathbf{w}}}c_{[1:i],\alpha}\mathcal{I}\left\{k\in\langle V\rangle_{[1:i]}\right\},\qquad(5\text{–}48)$$

其中（5–47）是通过将式（5–46）代入式（5–45）中得到的。

将式（5–44）和式（5–48）结合，有

$$\sum_{V'\in\Omega_{K,\alpha-1}^{\left(l_{\alpha-1}^{\mathbf{w}}\right)}:k\in V'}c_{V',\alpha-1}$$

$$=\sum_{V\in\Omega_{K,\alpha}^{\left(l_{\alpha}^{\mathbf{w}}\right)}:k\in V}c_{V,\alpha}+\frac{1}{\lambda_{\alpha}^{\mathbf{w}}}\sum_{V\in\Omega_{K,\alpha}^{\left(l_{\alpha}^{\mathbf{w}}\right)}:k\in V}c_{V,\alpha}\sum_{i=l_{\alpha-1}^{\mathbf{w}}+1}^{l_{\alpha}^{\mathbf{w}}}c_{[1:i],\alpha}\mathcal{I}\left\{k\in\langle V\rangle_{[1:i]}\right\}.\qquad(5\text{–}49)$$

考虑以下两种情况：

(情况 1) $k\in\left(l_{\alpha-1}^{\mathbf{w}}:l_{\alpha}^{\mathbf{w}}\right]$。这时，

$$\sum_{V\in\Omega_{K,\alpha}^{\left(l_{\alpha}^{\mathbf{w}}\right)}:k\in V}c_{V,\alpha}=\sum_{V\in\Omega_{K,\alpha}^{\left(l_{\alpha}^{\mathbf{w}}\right)}}c_{V,\alpha}$$

$$=\lambda_{\alpha}^{\mathbf{w}},\qquad(5\text{–}50)$$

$$\mathcal{I}\left\{k\in\langle V\rangle_{[1:i]}\right\}=\mathcal{I}\left\{k\in[1:i]\right\},\quad V\in\Omega_{K,\alpha}^{\left(l_{\alpha}^{\mathbf{w}}\right)},i\in\left(l_{\alpha-1}^{\mathbf{w}}:l_{\alpha}^{\mathbf{w}}\right],\qquad(5\text{–}51)$$

其中式（5–50）是因为式（5–21）。所以，从式（5–49）可以进一步推得

$$
\begin{aligned}
&\sum_{V'\in\Omega_{K,\alpha-1}^{\left(l_{\alpha-1}^{\mathbf{w}}\right)}:k\in V'} c_{V',\alpha-1} \\
&= \sum_{V\in\Omega_{K,\alpha}^{\left(l_{\alpha}^{\mathbf{w}}\right)}:k\in V} c_{V,\alpha} + \frac{1}{\lambda_\alpha^{\mathbf{w}}} \sum_{V\in\Omega_{K,\alpha}^{\left(l_{\alpha}^{\mathbf{w}}\right)}:k\in V} c_{V,\alpha} \sum_{i=l_{\alpha-1}^{\mathbf{w}}+1}^{l_\alpha^{\mathbf{w}}} c_{[1:i],\alpha} \mathcal{I}\left\{k\in[1:i]\right\} \\
&= \sum_{V\in\Omega_{K,\alpha}^{\left(l_{\alpha}^{\mathbf{w}}\right)}:k\in V} c_{V,\alpha} + \frac{1}{\lambda_\alpha^{\mathbf{w}}} \sum_{i=k}^{l_\alpha^{\mathbf{w}}} c_{[1:i],\alpha} \sum_{V\in\Omega_{K,\alpha}^{\left(l_{\alpha}^{\mathbf{w}}\right)}:k\in V} c_{V,\alpha} \qquad (5\text{–}52) \\
&= \lambda_\alpha^{\mathbf{w}} + \sum_{i=k}^{l_\alpha^{\mathbf{w}}} c_{[1:i],\alpha} \qquad (5\text{–}53) \\
&= w_k,
\end{aligned}
$$

其中式（5–52）是因为式（5–51），式（5–53）是因为式（5–50）。

(情况 2) $k\in\left(l_\alpha^{\mathbf{w}}:K\right]$。这时，

$$
\begin{aligned}
\sum_{V'\in\Omega_{K,\alpha-1}^{\left(l_{\alpha-1}^{\mathbf{w}}\right)}:k\in V'} c_{V',\alpha-1} &= \sum_{V\in\Omega_{K,\alpha}^{\left(l_{\alpha}^{\mathbf{w}}\right)}:k\in V} c_{V,\alpha} \qquad (5\text{–}54) \\
&= w_k,
\end{aligned}
$$

其中式（5–54）是因为式（5–49）和

$$
\mathcal{I}\left\{k\in\langle V\rangle_{[1:i]}\right\}=0,\quad V\in\Omega_{K,\alpha}^{\left(l_\alpha^{\mathbf{w}}\right)}, i\in\left(l_{\alpha-1}^{\mathbf{w}}:l_\alpha^{\mathbf{w}}\right].
$$

这样就验证了式（5–20）。

(2) 注意到

$$
\begin{aligned}
&\sum_{\tau=i+1}^{|V|} H\left(X_{\langle V\rangle_{[1:|V|]\setminus\{\tau\}}}\right) \\
&= \sum_{\tau=i+1}^{|V|} H\left(X_{\langle V\rangle_{[1:|V|]\setminus\{\tau\}}} \mid X_{\langle V\rangle_{[1:i]}}\right) + \sum_{\tau=i+1}^{|V|} H\left(X_{\langle V\rangle_{[1:i]}}\right) \\
&= \sum_{\tau=i+1}^{|V|} H\left(X_{\langle V\rangle_{[1:|V|]\setminus\{\tau\}}} \mid X_{\langle V\rangle_{[1:i]}}\right) + \left(|V|-i\right) H\left(X_{\langle V\rangle_{[1:i]}}\right) \\
&\geq \left(|V|-1-i\right) H\left(X_V \mid X_{\langle V\rangle_{[1:i]}}\right) + \left(|V|-i\right) H\left(X_{\langle V\rangle_{[1:i]}}\right) \qquad (5\text{–}55) \\
&= \left(|V|-1-i\right) H\left(X_V\right) + H\left(X_{\langle V\rangle_{[1:i]}}\right),\quad i\in\left[0:|V|\right), \qquad (5\text{–}56)
\end{aligned}
$$

其中式（5–55）是因为 Han 不等式[73]。所以我们有

$$\begin{aligned}
&\sum_{V'\in\Omega_{K,\alpha-1}^{\left(l_{\alpha-1}^{\mathbf{w}}\right)}}\frac{\theta_\alpha^{\mathbf{w}}}{\lambda_\alpha^{\mathbf{w}}}\sum_{V\in\Omega_{K,\alpha}^{\left(l_\alpha^{\mathbf{w}}\right)}:V'\subseteq V}c_{V,\alpha}H\left(X_{V'}\right)\\
&=\frac{\theta_\alpha^{\mathbf{w}}}{\lambda_\alpha^{\mathbf{w}}}\sum_{V\in\Omega_{K,\alpha}^{\left(l_\alpha^{\mathbf{w}}\right)}}c_{V,\alpha}\sum_{V'\in\Omega_{K,\alpha-1}^{\left(l_{\alpha-1}^{\mathbf{w}}\right)}:V'\subseteq V}H\left(X_{V'}\right)\\
&=\frac{\theta_\alpha^{\mathbf{w}}}{\lambda_\alpha^{\mathbf{w}}}\sum_{V\in\Omega_{K,\alpha}^{\left(l_\alpha^{\mathbf{w}}\right)}}c_{V,\alpha}\sum_{\tau=l_{\alpha-1}^{\mathbf{w}}+1}^{\alpha}H\left(X_{\langle V\rangle_{[1:\alpha]\setminus\{\tau\}}}\right)\\
&\geq\frac{\theta_\alpha^{\mathbf{w}}}{\lambda_\alpha^{\mathbf{w}}}\sum_{V\in\Omega_{K,\alpha}^{\left(l_\alpha^{\mathbf{w}}\right)}}c_{V,\alpha}\left(\left(\alpha-1-l_{\alpha-1}^{\mathbf{w}}\right)H\left(X_V\right)+H\left(X_{\left[1:l_{\alpha-1}^{\mathbf{w}}\right]}\right)\right) \qquad (5\text{–}57)\\
&=\sum_{V\in\Omega_{K,\alpha}^{\left(l_\alpha^{\mathbf{w}}\right)}}c_{V,\alpha}H\left(X_V\right)-\frac{1}{\lambda_\alpha^{\mathbf{w}}}\sum_{i=l_{\alpha-1}^{\mathbf{w}}+1}^{l_\alpha^{\mathbf{w}}}\left(\alpha-i-1\right)c_{[1:i],\alpha}\sum_{V\in\Omega_{K,\alpha}^{\left(l_\alpha^{\mathbf{w}}\right)}}c_{V,\alpha}H\left(X_V\right)\\
&\quad+\left(c_{\left[1:l_{\alpha-1}^{\mathbf{w}}\right],\alpha}-c_{\left[1:l_{\alpha-1}^{\mathbf{w}}\right],\alpha-1}\right)H\left(X_{\left[1:l_{\alpha-1}^{\mathbf{w}}\right]}\right), \qquad (5\text{–}58)
\end{aligned}$$

其中式（5–57）是因为式（5–56），式（5–58）是因为式（5–21）和式（5–24）。进一步的，

$$\begin{aligned}
&\sum_{V'\in\Omega_{K,\alpha-1}^{\left(l_{\alpha-1}^{\mathbf{w}}\right)}}\frac{1}{\lambda_\alpha^{\mathbf{w}}}\sum_{V\in\Omega_{K,\alpha}^{\left(l_\alpha^{\mathbf{w}}\right)}}c_{V,\alpha}\sum_{i=l_{\alpha-1}^{\mathbf{w}}+1}^{l_\alpha^{\mathbf{w}}}c_{[1:i],\alpha}\sum_{\tau=i+1}^{\alpha}\mathcal{I}\left\{V'=\langle V\rangle_{[1:\alpha]\setminus\{\tau\}}\right\}H\left(X_{V'}\right)\\
&=\frac{1}{\lambda_\alpha^{\mathbf{w}}}\sum_{V\in\Omega_{K,\alpha}^{\left(l_\alpha^{\mathbf{w}}\right)}}c_{V,\alpha}\sum_{i=l_{\alpha-1}^{\mathbf{w}}+1}^{l_\alpha^{\mathbf{w}}}c_{[1:i],\alpha}\sum_{\tau=i+1}^{\alpha}H\left(X_{\langle V\rangle_{[1:\alpha]\setminus\{\tau\}}}\right)\\
&\geq\frac{1}{\lambda_\alpha^{\mathbf{w}}}\sum_{V\in\Omega_{K,\alpha}^{\left(l_\alpha^{\mathbf{w}}\right)}}c_{V,\alpha}\sum_{i=l_{\alpha-1}^{\mathbf{w}}+1}^{l_\alpha^{\mathbf{w}}}c_{[1:i],\alpha}\left(\left(\alpha-1-i\right)H\left(X_V\right)+H\left(X_{[1:i]}\right)\right) \qquad (5\text{–}59)\\
&=\frac{1}{\lambda_\alpha^{\mathbf{w}}}\sum_{i=l_{\alpha-1}^{\mathbf{w}}+1}^{l_\alpha^{\mathbf{w}}}\left(\alpha-1-i\right)c_{[1:i],\alpha}\sum_{V\in\Omega_{K,\alpha}^{\left(l_\alpha^{\mathbf{w}}\right)}}c_{V,\alpha}H\left(X_V\right)+\frac{1}{\lambda_\alpha^{\mathbf{w}}}\sum_{i=l_{\alpha-1}^{\mathbf{w}}+1}^{l_\alpha^{\mathbf{w}}}c_{[1:i],\alpha}H\left(X_{[1:i]}\right)\sum_{V\in\Omega_{K,\alpha}^{\left(l_\alpha^{\mathbf{w}}\right)}}c_{V,\alpha}\\
&=\frac{1}{\lambda_\alpha^{\mathbf{w}}}\sum_{i=l_{\alpha-1}^{\mathbf{w}}+1}^{l_\alpha^{\mathbf{w}}}\left(\alpha-1-i\right)c_{[1:i],\alpha}\sum_{V\in\Omega_{K,\alpha}^{\left(l_\alpha^{\mathbf{w}}\right)}}c_{V,\alpha}H\left(X_V\right)+\sum_{i=l_{\alpha-1}^{\mathbf{w}}+1}^{l_\alpha^{\mathbf{w}}}c_{[1:i],\alpha}H\left(X_{[1:i]}\right), \qquad (5\text{–}60)
\end{aligned}$$

其中式（5–59）是由于式（5–56），式（5–60）是由于式（5–21）。这样，我们就可以将（5–58）和（5–60）合起来，并且考虑到$i\in\left[1:l_{\alpha-1}^{\mathbf{w}}\right)$时有$c_{[1:i],\alpha-1}=c_{[1:i],\alpha}$，就完成了证明。 □

接下来验证熵不等式。

引理 5.13：对任意的$\mathbf{w}\in\mathbb{R}_+^K$，存在$\left(c_{V,\alpha}:V\in\mathbb{V}_{K,\alpha}\right)\in\mathbb{C}_{K,\alpha}^{\mathbf{w}}$（$\alpha\in[1:K]$），使得对于任意的$K$个随机变量和$\alpha\geq\alpha'$，有

$$\sum_{V'\in\mathbb{V}_{K,\alpha'}}c_{V',\alpha'}H\left(X_{V'}\right)\geq\sum_{V\in\mathbb{V}_{K,\alpha}}c_{V,\alpha}H\left(X_V\right)\tag{5–61}$$

□

证明：由于对称性，仅考虑$\mathbf{w}\in\mathbb{W}_K$。

首先考虑$w_K>0$的情况。这时对任意的$\alpha\in[1:K]$有$\lambda_\alpha^{\mathbf{w}}>0$。定义$\left(c_{V,K}:V\in\mathbb{V}_{K,K}\right)$如下：

$$\begin{aligned}c_{[1:k],K}&\triangleq w_k-w_{k+1},\quad k\in[1:K],\\ c_{V,K}&\triangleq 0,\qquad\text{其他.}\end{aligned}$$

容易验证，$\left(c_{V,K}:V\in\mathbb{V}_{K,K}\right)\in\mathbb{C}_{K,K}^{\mathbf{w}}$。通过引理 5.12，可以依次从$\alpha=K-1$到$\alpha=1$构造满足要求的$\left(c_{V,\alpha}:V\in\mathbb{V}_{K,\alpha}\right)$。

现在考虑$w_1\geq\cdots\geq w_{K-1}>w_K=0$的情况。这时我们只要证明，对于$\mathbf{w}'\triangleq\left(w_1,\cdots,w_{K-1}\right)$，存在$\left(c'_{V,\alpha}:V\in\mathbb{V}_{K,\alpha}\right)\in\mathbb{C}_{K-1,\alpha}^{\mathbf{w}'}$（$\alpha\in[1:K)$）使得对任意$K-1$个随机变量$X_{[1:K-1]}$和$\alpha\geq\alpha'$，均有

$$\sum_{V'\in\mathbb{V}_{K-1,\alpha'}}c'_{V',\alpha'}H\left(X_{V'}\right)\geq\sum_{V\in\mathbb{V}_{K-1,\alpha}}c'_{V,\alpha}H\left(X_V\right).$$

定义$\left(c_{V,\alpha}:V\in\mathbb{V}_{K,\alpha}\right)$（$\alpha\in[1:K)$）如下：

$$\begin{aligned}c_{V,\alpha}&\triangleq c'_{V,\alpha},\quad K\notin V,\\ c_{V,\alpha}&\triangleq 0,\qquad\text{其他.}\end{aligned}$$

定义$\left(c_{V,K}:V\in\mathbb{V}_{K,K}\right)$如下：

$$\begin{aligned}c_{V,K}&\triangleq c'_{V,K-1},\quad K\notin V,\\ c_{V,K}&\triangleq 0,\qquad\text{其他.}\end{aligned}$$

可以验证，$\left(c_{V,\alpha}:V\in\mathbb{V}_{K,\alpha}\right)$（$\alpha\in[1:K]$）满足要求。

在一般对于某个$K'\leq K$有$w_1\geq\cdots\geq w_{K'-1}>w_{K'}=\cdots=w_K=0$情况下可以通过数学归纳法证明。当然对于$w_1=w_2=\cdots=w_K$的情况，则对所有的$\alpha\in[1:K]$和$V\in\mathbb{V}_{K,\alpha}$有$c_{V,\alpha}=0$。

这样就完成了引理的证明。□

5.2.3 外界获得

如前所述，证明的最后一步，就是要利用前面得到的熵不等式，证明$\mathcal{R}_K$是$\mathcal{R}_K^*$的外界。

引理 5.14：给定 $\mathbf{w}\in\mathbb{R}_+^K$。若存在一套 Lagrange 乘子 $\left(c_{V|V',\alpha}: V\in\mathbb{V}_{K,\alpha},\ V'\in\mathbb{V}'_{K,\alpha}[V]\right)$（$\alpha\in[1:K]$）使得式（5–40）成立，则

$$\mathcal{R}_K^*\subseteq\mathcal{R}_K. \qquad \square$$

证明：首先我们用数学归纳法证明，对于 $\forall\left(R_k: k\in[1:K]\right)\in\mathcal{R}_K^*$，有

$$\sum_{k=1}^K w_k\left(R_k+\epsilon\right)\geq\sum_{\alpha=1}^{\beta} f_\alpha^{\mathbf{w}} + \frac{1}{n}\sum_{V\in\mathbb{V}_{K,\beta}}\sum_{V'\in\mathbb{V}'_{K,\beta}[V]} c_{V|V',\beta}H\left(S_V\,|\,U^n_{[1:K],[1:\beta]},S_{V'}\right)-\beta\delta_\epsilon\sum_{k=1}^K w_k,\quad \beta\in[1:K], \tag{5–62}$$

其中 δ_ϵ 在 $\epsilon\to 0$ 时趋于 0。

首先验证 $\beta=1$ 时式（5–62）的正确性。可以验证，

$$\begin{aligned}\sum_{k=1}^K w_k\left(R_k+\epsilon\right)&\geq\frac{1}{n}\sum_{k=1}^K w_k\log M_k\\&\geq\frac{1}{n}\sum_{k=1}^K w_k H(S_k)\\&=\frac{1}{n}\sum_{V\in\mathbb{V}_{K,1}} c_{V|\varnothing,1}H\left(S_V\right),\end{aligned} \tag{5–63}$$

其中用到了引理 5.1 中的结果 $c_{\{k\}|\varnothing,1}\triangleq w_k$（$k\in[1:K]$）。注意到

$$\begin{aligned}H\left(S_V\right)&\geq H\left(U^n_{V,1}\right)+H\left(S_V\,|\,U^n_{V,1}\right)-H\left(U^n_{V,1}\,|\,S_V\right)\\&\geq H\left(U^n_{V,1}\right)+H\left(S_V\,|\,U^n_{V,1}\right)-n\delta_\epsilon \qquad (5–64)\\&\geq H\left(U_{V,1}\right)+H\left(S_V\,|\,U^n_{[1:K],1}\right)-n\delta_\epsilon,\quad V\in\mathbb{V}_{K,1}, \qquad (5–65)\end{aligned}$$

其中（5–64）用到了式（5–2）和 Fano 不等式。将（5–65）代入（5–63），并使用（5–4）可以验证在 $\beta=1$ 情况下式（5–62）的正确性。

接下来验证递推关系。现在假设式（5–62）对 $\beta=B-1$ 成立。考虑到（5–40），我们有

$$\begin{aligned}&\sum_{V\in\mathbb{V}_{K,B-1}}\sum_{V'\in\mathbb{V}'_{K,B-1}[V]} c_{V|V',B-1}H\left(S_V\,|\,U^n_{[1:K],[1:B-1]},S_{V'}\right)\\&\qquad\geq\sum_{V\in\mathbb{V}_{K,B}}\sum_{V'\in\mathbb{V}'_{K,B}[V]} c_{V|V',B}H\left(S_V\,|\,U^n_{[1:K],[1:B-1]},S_{V'}\right).\end{aligned} \tag{5–66}$$

可以验证，

$$
\begin{aligned}
&H\left(S_V \mid U^n_{[1:K],[1:B-1]}, S_{V'}\right)\\
&= H\left(U^n_{V,B}, S_V \mid U^n_{[1:K],[1:B-1]}, S_{V'}\right) - H\left(U^n_{V,B} \mid U^n_{[1:K],[1:B-1]}, S_V, S_{V'}\right)\\
&\geq H\left(U^n_{V,B}, S_V \mid U^n_{[1:K],[1:B-1]}, S_{V'}\right) - n\delta_\epsilon, \quad V \in \mathbb{V}_{K,B}, V' \in \mathbb{V}'_{K,B}, \qquad (5\text{–}67)
\end{aligned}
$$

其中（5–67）是由式（5–2）和 Fano 不等式得到。

另外，

$$
\begin{aligned}
&H\left(U^n_{V,B}, S_V \mid U^n_{[1:K],[1:B-1]}, S_{V'}\right)\\
&\geq H\left(U^n_{V,B} \mid U^n_{[1:K],[1:B-1]}, S_{V'}\right) + H\left(S_V \mid U^n_{[1:K],[1:B]}, S_{V'}\right)\\
&\geq H\left(U^n_{V,B} \mid U^n_{V',B}\right) + H\left(S_V \mid U^n_{[1:K],[1:B]}, S_{V'}\right) \qquad (5\text{–}68)\\
&= H\left(U_{V,B} \mid U_{V',B}\right) + H\left(S_V \mid U^n_{[1:K],[1:B]}, S_{V'}\right), \qquad (5\text{–}69)
\end{aligned}
$$

其中（5–68）是因为$U^n_{V,B} \leftrightarrow U^n_{V',B} \leftrightarrow (U^n_{[1:K],[1:B]}, S_{V'})$是一个 Markov 链。从式（5–66）继续推导，有

$$
\begin{aligned}
&\sum_{V\in\mathbb{V}_{K,B-1}} \sum_{V'\in\mathbb{V}'_{K,B-1}[V]} c_{V|V',B-1} H\left(S_V \mid U^n_{[1:K],[1:B-1]}, S_{V'}\right)\\
&\geq n \sum_{V\in\mathbb{V}_{K,B}} \sum_{V'\in\mathbb{V}'_{K,B}[V]} c_{V|V',B} H\left(U_{V,B} \mid U_{V',B}\right)\\
&+ \sum_{V\in\mathbb{V}_{K,B}} \sum_{V'\in\mathbb{V}'_{K,B}[V]} c_{V|V',B} H\left(S_V \mid U^n_{[1:K],[1:B]}, S_{V'}\right) - n\delta_\epsilon \sum_{V\in\mathbb{V}_{K,B}} \sum_{V'\in\mathbb{V}'_{K,B}[V]} c_{V|V',B} \qquad (5\text{–}70)\\
&\geq n \sum_{V\in\mathbb{V}_{K,B}} \sum_{V'\in\mathbb{V}'_{K,B}[V]} c_{V|V',B} H\left(U_{V,B} \mid U_{V',B}\right)\\
&+ \sum_{V\in\mathbb{V}_{K,B}} \sum_{V'\in\mathbb{V}'_{K,B}[V]} c_{V|V',B} H\left(S_V \mid U^n_{[1:K],[1:B]}, S_{V'}\right) - n\delta_\epsilon \sum_{k=1}^{K} \sum_{V\in\mathbb{V}_{K,B}:k\in V} \sum_{V'\in\mathbb{V}'_{K,B}[V]} c_{V|V',B}\\
&= n f_B^{\mathbf{w}} + \sum_{V\in\mathbb{V}_{K,B}} \sum_{V'\in\mathbb{V}'_{K,B}[V]} c_{V|V',B} H\left(S_V \mid U^n_{[1:K],[1:B]}, S_{V'}\right) - n\delta_\epsilon \sum_{k=1}^{K} w_k, \qquad (5\text{–}71)
\end{aligned}
$$

其中式（5–70）是因为（5–67）和（5–69），式（5–71）是因为（5–4）和（5–5）。将（5–71）和归纳假设结合起来，就证明了在$\beta = B$时归纳假设成立。这样，我们就证明了（5–62）式。

在式（5–62）中将$\beta = K$代入，有

$$
\sum_{k=1}^{K} w_k \left(R_k + \varepsilon\right) \geq \sum_{\alpha=1}^{K} f_\alpha^{\mathbf{w}} - K\delta_\epsilon \sum_{k=1}^{K} w_k \,.
$$

这样就证明了$\mathcal{R}^*_K \subseteq \mathcal{R}_K$。 □

对于信源对称的情况，可以考虑以下更弱的表述：

引理 5.15：若对于任意的 $\mathbf{w}\in\mathbb{R}_+^K$ 均存在 $\left(c_{V,\alpha}:V\in\mathbb{V}_{K,\alpha}\right)\in\mathbb{C}_{K,\alpha}^{\mathbf{w}}$（$\alpha\in[1:K]$）使得式（5–61）成立，则当信源 $U_{[1:K],[1:K]}$ 对称时有 $\mathcal{R}_K^*\subseteq\mathcal{R}_K$。

证明：不失一般性，假设 $\mathbf{w}\in\mathbb{W}_K$。任取 $\left(R_k:k\in[1:K]\right)\in\mathcal{R}_K^*$。

下面我们用数学归纳法证明，对于对称信源，有

$$\begin{aligned}&\sum_{k=1}^{K}w_k\left(R_k+\epsilon\right)\\&\quad\geq\sum_{\alpha=1}^{\beta}\overline{f}_{\alpha}^{\mathbf{w}}+\frac{1}{n}\sum_{k=1}^{l_\beta^{\mathbf{w}}}c_{[1:k],\beta}H\left(S_{[1:k]}\,|\,U_{[1:K],[1:\beta]}^n,U_{[k+1:\beta],K}^n\right)\\&\qquad+\frac{1}{n}\sum_{V\in\Omega_{K,\beta}^{\left(l_\beta^{\mathbf{w}}\right)}}c_{V,\beta}H\left(S_V\,|\,U_{[1:K],[1:\beta]}^n\right)-\beta\delta_\epsilon\sum_{k=1}^{K}w_k,\quad\beta\in[1:K],\end{aligned}\tag{5–72}$$

其中 $\epsilon\to0$ 时 $\delta_\epsilon\to0$。

$\beta=1$ 时的证明与式（5–65）的证明相同。现假设不等式（5–72）对于 $\beta=B-1$ 成立。

注意到式（5–61），我们有

$$\begin{aligned}&\sum_{V'\in\Omega_{K,B-1}^{\left(l_{B-1}^{\mathbf{w}}\right)}}c_{V',B-1}H\left(S_{V'}\,|\,U_{[1:K],[1:B-1]}^n\right)\\&\quad\geq\sum_{k=1}^{l_B^{\mathbf{w}}}\left(c_{[1:k],B}-c_{[1:k],B-1}\mathcal{I}\left\{k\leq l_{B-1}^{\mathbf{w}}\right\}\right)H\left(S_{[1:k]}\,|\,U_{[1:K],[1:B-1]}^n\right)\\&\qquad+\sum_{V\in\Omega_{K,B}^{\left(l_B^{\mathbf{w}}\right)}}c_{V,B}H\left(S_V\,|\,U_{[1:K],[1:B-1]}^n\right),\end{aligned}\tag{5–73}$$

其中由于（5–23）和（5–24），有

$$c_{[1:k],B}-c_{[1:k],B-1}\mathcal{I}\left\{k\leq l_{B-1}^{\mathbf{w}}\right\}\geq0,\ \ k\in\left[1:l_B^{\mathbf{w}}\right].$$

并且当 $k\in\left[1:l_{B-1}^{\mathbf{w}}\right)$ 时有 $c_{[1:k],B-1}=c_{[1:k],B}$。

另外，

$$\begin{aligned}
&\sum_{k=1}^{l_B^{\mathbf{w}}}\left(c_{[1:k],B}-c_{[1:k],B-1}\mathcal{I}\left\{k\le l_{B-1}^{\mathbf{w}}\right\}\right)H\left(S_{[1:k]}\,|\,U_{[1:K],[1:B-1]}^{n}\right)\\
&\quad\ge\sum_{k=1}^{l_B^{\mathbf{w}}}\left(c_{[1:k],B}-c_{[1:k],B-1}\mathcal{I}\left\{k\le l_{B-1}^{\mathbf{w}}\right\}\right)H\left(S_{[1:k]}\,|\,U_{[1:K],[1:B-1]}^{n},U_{[k+1:B],[B:K]}^{n}\right)\\
&\quad=\sum_{k=1}^{l_B^{\mathbf{w}}}c_{[1:k],B}H\left(S_{[1:k]}\,|\,U_{[1:K],[1:B-1]}^{n},U_{[k+1:B],[B:K]}^{n}\right)\\
&\qquad-\sum_{k=1}^{l_{B-1}^{\mathbf{w}}}c_{[1:k],B-1}H\left(S_{[1:k]}\,|\,U_{[1:K],[1:B-1]}^{n},U_{[k+1:B],[B:K]}^{n}\right)\\
&\quad\ge\sum_{k=1}^{l_B^{\mathbf{w}}}c_{[1:k],B}H\left(S_{[1:k]}\,|\,U_{[1:K],[1:B-1]}^{n},U_{[k+1:B],[B:K]}^{n}\right)\\
&\qquad-\sum_{k=1}^{l_{B-1}^{\mathbf{w}}}c_{[1:k],B-1}H\left(S_{[1:k]}\,|\,U_{[1:K],[1:B-1]}^{n},U_{[k+1:B-1],[B-1:K]}^{n}\right).
\end{aligned}\tag{5–74}$$

将式（5–73）和式（5–74）结合，则有

$$\begin{aligned}
&\sum_{k=1}^{l_{B-1}^{\mathbf{w}}}c_{[1:k],B-1}H\left(S_{[1:k]}\,|\,U_{[1:K],[1:B-1]}^{n},U_{[k+1:B-1],[B-1:K]}^{n}\right)+\sum_{V'\in\Omega_{K,B-1}^{\left(l_{B-1}^{\mathbf{w}}\right)}}c_{V',B-1}H\left(S_{V'}\,|\,U_{[1:K],[1:B-1]}^{n}\right)\\
&\quad\ge\sum_{k=1}^{l_B^{\mathbf{w}}}c_{[1:k],B}H\left(S_{[1:k]}\,|\,U_{[1:K],[1:B-1]}^{n},U_{[k+1:B],[B:K]}^{n}\right)+\sum_{V\in\Omega_{K,B}^{\left(l_B^{\mathbf{w}}\right)}}c_{V,B}H\left(S_{V}\,|\,U_{[1:K],[1:B-1]}^{n}\right).
\end{aligned}\tag{5–75}$$

注意到

$$
\begin{aligned}
&H\left(S_{[1:k]} \mid U^n_{[1:K],[1:B-1]}, U^n_{[k+1:B],[B:K]}\right) \\
&\quad = H\left(S_{[1:k]} \mid U^n_{[1:K],[1:B-1]}, U^n_{[k+1:B],[B:K]}, S_{[k+1:B]}\right) \\
&\quad = H\left(S_{[1:B]} \mid U^n_{[1:K],[1:B-1]}, U^n_{[k+1:B],[B:K]}, S_{[k+1:B]}\right) \\
&\quad = H\left(U^n_{[1:B],[1:B]}, S_{[1:B]} \mid U^n_{[1:K],[1:B-1]}, U^n_{[k+1:B],[B:K]}, S_{[k+1:B]}\right) \\
&\qquad - H\left(U^n_{[1:B],[1:B]} \mid U^n_{[1:K],[1:B-1]}, U^n_{[k+1:B],[B:K]}, S_{[1:B]}\right) \\
&\quad \geq H\left(U^n_{[1:B],[1:B]}, S_{[1:B]} \mid U^n_{[1:K],[1:B-1]}, U^n_{[k+1:B],[B:K]}, S_{[k+1:B]}\right) - n\delta_\epsilon \qquad (5\text{–}76) \\
&\quad = H\left(U^n_{[1:B],[1:B]} \mid U^n_{[1:K],[1:B-1]}, U^n_{[k+1:B],[B:K]}, S_{[k+1:B]}\right) \\
&\qquad + H\left(S_{[1:B]} \mid U^n_{[1:K],[1:B-1]}, U^n_{[1:B],[1:B]}, U^n_{[k+1:B],[B:K]}, S_{[k+1:B]}\right) - n\delta_\epsilon \\
&\quad = H\left(U^n_{[1:B],[1:B]} \mid U^n_{[1:K],[1:B-1]}, U^n_{[k+1:B],[B:K]}\right) \\
&\qquad + H\left(S_{[1:k]} \mid U^n_{[1:K],[1:B-1]}, U^n_{[1:B],[1:B]}, U^n_{[k+1:B],[B:K]}\right) - n\delta_\epsilon \\
&\quad \geq nH_{k,B} + H\left(S_{[1:k]} \mid U^n_{[1:K],[1:B]}, U^n_{[k+1:B],[B:K]}\right) - n\delta_\epsilon, \quad k \in \left[1 : l_B^{\mathrm{w}}\right], \qquad (5\text{–}77)
\end{aligned}
$$

其中（5–76）是由于（5–2）和 Fano 不等式。

类似的，我们有

$$
\begin{aligned}
&H\left(S_V \mid U^n_{[1:K],[1:B-1]}\right) \\
&\quad = H\left(U^n_{V,[1:B]}, S_V \mid U^n_{[1:K],[1:B-1]}\right) - H\left(U^n_{V,[1:\alpha]} \mid U^n_{[1:K],[1:B-1]}, S_V\right) \\
&\quad \geq H\left(U^n_{V,[1:B]}, S_V \mid U^n_{[1:K],[1:B-1]}\right) - n\delta_\epsilon \\
&\quad = H\left(U^n_{V,[1:B]} \mid U^n_{[1:K],[1:B-1]}\right) + H\left(S_V \mid U^n_{[1:K],[1:B-1]}, U^n_{V,[1:B]}\right) - n\delta_\epsilon \\
&\quad \geq nH_{|V|,B} + H\left(S_V \mid U^n_{[1:K],[1:B]}\right) - n\delta_\epsilon, \quad V \in \Omega^{\left(l_B^{\mathrm{w}}\right)}_{K,B}. \qquad (5\text{–}78)
\end{aligned}
$$

从式（5–75）继续推导，可以得到

$$\begin{aligned}
&\sum_{k=1}^{l_{B-1}^{\mathbf{w}}} c_{[1:k],B-1} H\left(S_{[1:k]} \mid U_{[1:K],[1:B-1]}^{n}, U_{[k+1:B-1],[B-1:K]}^{n}\right) \\
&\quad + \sum_{V' \in \Omega_{K,B-1}^{\left(l_{B-1}^{\mathbf{w}}\right)}} c_{V',B-1} H\left(S_{V'} \mid U_{[1:K],[1:B-1]}^{n}\right) \\
&\geq n \sum_{V \in \mathbb{V}_{K,B}} c_{V,B} H_{|V|,B} + \sum_{k=1}^{l_B^{\mathbf{w}}} c_{[1:k],B} H\left(S_{[1:k]} \mid U_{[1:K],[1:B]}^{n}, U_{[k+1:B],[B:K]}^{n}\right) \\
&\quad + \sum_{V \in \Omega_{K,B}^{\left(l_B^{\mathbf{w}}\right)}} c_{V,B} H\left(S_V \mid U_{[1:K],[1:B]}^{n}\right) - n\delta_{\epsilon} \sum_{V \in \mathbb{V}_{K,B}} c_{V,B} \qquad (5\text{–}79) \\
&\geq n \overline{f}_B^{\mathbf{w}} + \sum_{k=1}^{l_B^{\mathbf{w}}} c_{[1:k],B} H\left(S_{[1:k]} \mid U_{[1:K],[1:B]}^{n}, U_{[k+1:B],[B:K]}^{n}\right) \\
&\quad + \sum_{V \in \Omega_{K,B}^{\left(l_B^{\mathbf{w}}\right)}} c_{V,B} H\left(S_V \mid U_{[1:K],[1:B]}^{n}\right) - n\delta_{\epsilon} \sum_{k=1}^{K} w_k, \qquad (5\text{–}80)
\end{aligned}$$

其中式（5–79）是因为（5–77）和（5–78），式（5–80）是因为式（5–8）、式（5–25）和引理 5.9。将式（5–80）和归纳假设相结合，可以得到在 $\beta = B$ 时式（5–72）成立。

在式（5–72）中，令 $\beta = K$，则有

$$\sum_{k=1}^{K} w_k \left(R_k + \varepsilon\right) \geq \sum_{\alpha=1}^{K} \overline{f}_{\alpha}^{\mathbf{w}} - K\delta_{\epsilon} \sum_{k=1}^{K} w_k \,.$$

这样就证明了 $\left(R_k : k \in [1:K]\right) \in \mathcal{R}_K$。得证。 □

这样就完成了定理 5.2 的证明。

第 6 章　有向网络中多源多宿的延时模型的求解

内容提要

本章研究延时对网络纠错的影响。本章将证明有限延时不改变网络纠错信道容量域和网络纠错容许速率域。

● 6.1 节介绍前人有关工作，并说明本章内容和之前有关延时的研究的不同之处。

● 6.2 节给出本章研究的模型及其结论。

● 6.3 节给出 6.2 节中定理的证明。

本章部分内容改编自在学期间发表的学术论文[6]。文章的共同作者参与了相关的讨论和研究。

6.1 本章引言

本节介绍学术界前人有关延时对网络极限性能研究的成果，以及网络中归约方法的相关文献。

采用归约来讨论延时可以追溯到文献[104–107]。在这些工作讨论了在无记忆概率网络中延时的影响。它们用条件概率分布来表示信道，并使用归约的方法证明了在网络中任意部分引入了有限延时都不改变网络的信道容量域。

文献[108,109]将归约的方法引入网络纠错的研究，在不考虑延时的情况下用网络的子网络的容量来为容量做界。

本章将考虑在敌对方能进行恶意攻击的情况下延时对无噪网络的影响。如第 1.1.2 节所述，网络纠错的信道是组合信道，其不能用概率刻画，更不是无记忆的。所以，文献[104–107]中的结论不能适用于网络纠错的情况。所以，本章将针对敌对方引入组合错误的场景，考虑延时的影响。

本章的主要结果是证明在网络中存在攻击的情况下，攻击方在原有篡改错误的基础上再引入延时错误，也不会改变信道容量域和容许速率域。其证明的思路将采用前面提到的归约的思路：一方面，用有延时时的网络纠错码构造无延时时的网络纠错码，证明无延时的情况下可以达到有延时时相同的消息速率；另一方面，用无延时时的网络纠错码构造有延时的网络纠错码，证明有延时的情况下可以达到无延时时相同的消息速率。

6.2 模型与结果

延时模型

延时可以由节点引入，也可以由边引入。合法节点上的处理（如物理层的信道编码、调制等）会引入延时，恶意节点也会故意增加延迟。如果某个节点有多个输出（即向多个不同的链路输出），这多个输出的延时可能会不同（也有可能相同）。链路上的通信（比如物理信号的传输、链路级协议的重传等）也需要时间，敌对方也可能会故意增加通信时间。我们可以将节点引入的延时折算到链路上，使得只用链路的延时来同时表征节点引入的延时和链路引入的延时。具体的方法是：对于边$e\in\mathcal{E}$，将$\mathrm{Tail}(e)$引入的延时和e引入的延时都算做链路e的延时。在后文中，就只考虑链路的延时。

对于某条链路$e\in\mathcal{E}$上的延时，其可能是有界的，也可能是无界的。若存在一个非负实数$d_e\in[0,+\infty)$，使得e的延时不超过d_e，那么称e上的延时是有界的。在某个网络中，若对所有的$e\in\mathcal{E}$，e上的延时都是有界的，则称这个网络上的延时是有界的。

假设边e上有恒定延时d_e。定义$\mathbf{d}_{\mathcal{E}}\triangleq(d_e:e\in\mathcal{E})$。当$\mathbf{d}_{\mathcal{E}}$的取值为全零$\mathbf{0}_{\mathcal{E}}\triangleq(0:e\in\mathcal{E})$时，认为整个网络中没有延时。（前几章不考虑延时，就相当于令$\mathbf{d}_{\mathcal{E}}=\mathbf{0}_{\mathcal{E}}$。）

主要结果

本章的第一个结论针对有限延时对信道容量域的影响，判定有延时情况下和无延时情况下信道容量域是否相同。结论如下：

定理 6.1：给定的网络$\mathcal{G}$、连接集$\mathcal{K}$、攻击组合$\mathcal{A}$、各链路速率$\mathbf{f}_{\mathcal{E}}$的情况下，记$\mathcal{C}(\mathbf{d}_{\mathcal{E}})$为延时参数为$\mathbf{d}_{\mathcal{E}}$时的信道容量域。对任意的$\mathbf{d}_{\mathcal{E}}\geq\mathbf{0}_{\mathcal{E}}$，有

$$\mathcal{C}(\mathbf{d}_{\mathcal{E}})=\mathcal{C}(\mathbf{0}_{\mathcal{E}}).$$ □

这个定理说明，无论网络的拓扑是什么样子，无论有多少连接，每个连接是单播还是多播，无论链路速率有多大，无论延迟$\mathbf{d}_{\mathcal{E}}$有多大，在延时情况下的信道容量域$\mathcal{C}(\mathbf{d}_{\mathcal{E}})$总是与没有延时情况下的信道容量域$\mathcal{C}(\mathbf{0}_{\mathcal{E}})$相等（即$\mathcal{C}(\mathbf{d}_{\mathcal{E}})=\mathcal{C}(\mathbf{0}_{\mathcal{E}})$，而不是$\mathcal{C}(\mathbf{d}_{\mathcal{E}})\subsetneqq\mathcal{C}(\mathbf{0}_{\mathcal{E}})$）。简而言之，就是有限延迟不改变信道容量域。

本章的第二个结论针对有限延时对容许速率域的影响，判定有延时情况下和无延时情况下容许速率域是否相同。结论如下：

定理 6.2：给定的网络$\mathcal{G}$、连接集$\mathcal{K}$、攻击组合$\mathcal{A}$、信源参数的情况下，记$\mathcal{R}(\mathbf{d}_{\mathcal{E}})$为延时参数为$\mathbf{d}_{\mathcal{E}}$时的容许速率域。对任意的$\mathbf{d}_{\mathcal{E}}\geq\mathbf{0}_{\mathcal{E}}$，有

$$\mathcal{R}(\mathbf{d}_{\mathcal{E}})=\mathcal{R}(\mathbf{0}_{\mathcal{E}}).$$ □

这个定理说明，无论网络的拓扑是什么样子，无论有多少连接，每个连接是单播还是多播，无论信源如何，无论延迟$\mathbf{d}_{\mathcal{E}}$有多大，在有延时情况下的容许速率域$\mathcal{R}(\mathbf{d}_{\mathcal{E}})$总是等于没有延迟情况下的容许速率域$\mathcal{R}(\mathbf{0}_{\mathcal{E}})$（即$\mathcal{R}(\mathbf{d}_{\mathcal{E}})=\mathcal{R}(\mathbf{0}_{\mathcal{E}})$，而不是$\mathcal{R}(\mathbf{d}_{\mathcal{E}})\subsetneqq\mathcal{R}(\mathbf{0}_{\mathcal{E}})$）。简而言之，就是有限延迟不改变容许容量域。

虽然定理 6.1 和定理 6.2 给出的是对于特定的延时的结果，但是显然对任意有界的延时都有效。直观的究其原因，如果延时有界，那么网络纠错码可以通过主动的拖延时间，将延时延长到界的值，使得延迟成为预先确定的值，这样就把延时确定下来。后文将会对此进行形式化分析。

定理 6.1 和定理 6.2 的证明见下节。

6.3 定理证明

6.3.1 单位延时对信道容量域的影响

本小节将考虑信道容量域问题，证明网络中某条边上的恒定单位延时对没有影响。这个引理的证明是定理 6.1 和定理 6.2 的核心。

引理 6.1：给定的网络$\mathcal{G}$、连接集$\mathcal{K}$、攻击组合$\mathcal{A}$、各链路速率$\mathbf{f}_{\mathcal{E}}$的情况下，记$\mathcal{C}(\mathbf{d}_{\mathcal{E}})$为延时参数为$\mathbf{d}_{\mathcal{E}}$时的信道容量域。对于某个链路$e\in\mathcal{E}$，记

$$\mathbf{d}_e \triangleq \left(0,0,\cdots,0,\underset{\uparrow}{1},0,\cdots,0\right)_{e}.$$

则对任意的$\mathbf{d}_{\mathcal{E}}\geq\mathbf{0}_{\mathcal{E}}$，有

$$\mathcal{C}(\mathbf{d}_{\mathcal{E}})\subseteq\mathcal{C}(\mathbf{d}_{\mathcal{E}}+\mathbf{d}_e).$$ □

证明：下面证明，对于某个速率$\mathbf{R}^{(\mathcal{K})}\triangleq\left(R^{(k)}:k\in\mathcal{K}\right)$，如果对于延迟$\mathbf{d}_{\mathcal{E}}$可以达到速率$\mathbf{R}^{(\mathcal{K})}$，那么延迟$\mathbf{d}_{\mathcal{E}}+\mathbf{d}_e$也可以渐进达到速率$\mathbf{R}^{(\mathcal{K})}$。

在延迟为$\mathbf{d}_{\mathcal{E}}$时，假设某个码长为n的网络纠错码C可以达到速率$\mathbf{R}^{(\mathcal{K})}$。回顾之前的符号定义，在第$i\in[1:n]$时刻，边$\mathcal{E}$上的输入信号为$X_{\mathcal{E},i}$，输出信号为$Y_{\mathcal{E},i}$。这些信号标注在表 6.1 中。在没有错误的情况下，在时间 1 时边e的输入$X_{e,1}$只取决于来自节点$\mathrm{Tail}(e)$的消息（如果有的话）；在时间 2 时边e的输入$X_{e,2}$只取决于前述消息和$\mathrm{Tail}(e)$在时间 1 收到的所有信号；在时间 1 时边e的输出$Y_{e,1}$和$X_{e,1}$相同，等等。表 6.1 给出了整个网络中信号的实例。与前几章不同，前几章常常直接讨论编码器和译码器，但是这里给出的是可观察到的信号。之前我们已经假设，$X_{\mathcal{E},i}$的值是依赖于$Y_{\mathcal{E}}^{i-1}$的。在后文的分析需要用到这个假设。

现在考虑敌对方对信号的篡改带来的影响。如前所述，敌对方控制着某个资源组合。如果敌对方控制某个节点（如节点$\mathrm{Tail}(e)$），那么它就能修改表 6.1 中X_e的所有信号；如果敌对方控制某条链路（如链路e），那么它就能修改表 6.1 中Y_e的所有信号。而这样的错误会传播到其他列。例如，由于Y_e的值由X_e的值决定，所以X_e的值会影响Y_e的值；Y_e的值还可能间接的影响$\mathrm{Tail}(e)$的输入，反过来影响X_e的值。

表 6.1　延时$\mathbf{d}_{\mathcal{E}}$时的网络纠错码C

时间	e的输入	$\mathcal{E}\setminus\{e\}$的输入	e的输出	$\mathcal{E}\setminus\{e\}$的输出
1	$X_{e,1}$	$X_{\mathcal{E}\setminus\{e\},1}$	$Y_{e,1}$	$Y_{\mathcal{E}\setminus\{e\},1}$
2	$X_{e,2}$	$X_{\mathcal{E}\setminus\{e\},2}$	$Y_{e,2}$	$Y_{\mathcal{E}\setminus\{e\},2}$
3	$X_{e,3}$	$X_{\mathcal{E}\setminus\{e\},3}$	$Y_{e,3}$	$Y_{\mathcal{E}\setminus\{e\},3}$
…	…	…	…	…
n	$X_{e,n}$	$X_{\mathcal{E}\setminus\{e\},n}$	$Y_{e,n}$	$Y_{\mathcal{E}\setminus\{e\},n}$

对于消息速率为$\mathbf{R}^{(\mathcal{K})}$的网络纠错码$\mathsf{C}$，它能对抗敌对方的攻击（包括其直接篡改的错误和进一步传播引发的错误）。也就是说，所有译码器都能正确恢复消息。

现在我们用码C构造新的网络纠错码，在延迟为$\mathbf{d}_{\mathcal{E}}+\mathbf{d}_e$的情况下渐进达到速率$\mathbf{R}^{(\mathcal{K})}$。

首先我们考虑在网络中直接应用码C。当延迟为$\mathbf{d}_{\mathcal{E}}+\mathbf{d}_e$时，与延迟为$\mathbf{d}_{\mathcal{E}}$的情况相比，链路$e$多延时 1 个单位时间。这样，$X_{e,1}$和$Y_{e,1}$会比其他发送和接收信号晚 1 个单位时间出现。也就是说，$X_{e,1}$和$Y_{e,1}$出现在时间 2。由于编码器的因果性（即$X_{\mathcal{E},i}$只能在$Y_{\mathcal{E},1},\cdots,Y_{\mathcal{E},i-1}$后出现），所以$X_{\mathcal{E}\setminus\{e\},2}$只能在时刻 3 出现。更糟糕的是，由于边$e$有一个延时，$X_{e,2}$只能在时刻 4 出现。继续这样不断演算下去，所有信号的出现时刻见表 6.2。

从表 6.2 中可以看出，我们用$2n$的时间传来原消息。这样的方案的消息速率只有原来的一半。值得注意的是，表 6.2 中有许多格子是空白的，这意味着有很多资源并没有充分使用。在后文中我们将试图充分利用这些空余的资源。

表 6.2　在延时为 $\mathbf{d}_{\mathcal{E}}+\mathbf{d}_e$ 的情况下使用码 C

时间	e 的输入	$\mathcal{E}\setminus\{e\}$ 的输入	e 的输出	$\mathcal{E}\setminus\{e\}$ 的输出
1		$X_{\mathcal{E}\setminus\{e\},1}$		$Y_{\mathcal{E}\setminus\{e\},1}$
2	$X_{e,1}$		$Y_{e,1}$	
3		$X_{\mathcal{E}\setminus\{e\},2}$		$Y_{\mathcal{E}\setminus\{e\},2}$
4	$X_{e,2}$		$Y_{e,2}$	
5		$X_{\mathcal{E}\setminus\{e\},3}$		$Y_{\mathcal{E}\setminus\{e\},3}$
6	$X_{e,3}$		$Y_{e,3}$	
…	…	…	…	…
$2n-1$		$X_{\mathcal{E}\setminus\{e\},n}$		$Y_{\mathcal{E}\setminus\{e\},n}$
$2n$	$X_{e,n}$		$Y_{e,n}$	

在表 6.3 中，我们在延时为 $\mathbf{d}_{\mathcal{E}}+\mathbf{d}_e$ 的情况下两次部署码 C。第一次部署的输入和输出还是记为 $X_{\mathcal{E},i}$ 和 $Y_{\mathcal{E},i}$，和表 6.2 中的部署是一样的。第一次部署的是输入和输出记为 $\tilde{X}_{\mathcal{E},i}$ 和 $\tilde{Y}_{\mathcal{E},i}$，是表 6.2 中延迟 1 个时间单位的结果。通过这种方法，两个码在 $(2n+1)$ 次信道使用传递了两份消息，达到消息速率 $\frac{2n}{2n+1}\mathbf{R}^{(\mathcal{K})}$。通过码级联等方式，可以让码长任意长。注意到 $n\to+\infty$ 时 $\frac{2n}{2n+1}\to 1$，所以可以渐进达到速率 $\mathbf{R}^{(\mathcal{K})}$。

表 6.3　在延时为$\mathbf{d}_{\mathcal{E}}+\mathbf{d}_e$的情况下多次使用码$\mathsf{C}$

时间	e的输入	$\mathcal{E}\setminus\{e\}$的输入	e的输出	$\mathcal{E}\setminus\{e\}$的输出
1		$X_{\mathcal{E}\setminus\{e\},1}$		$Y_{\mathcal{E}\setminus\{e\},1}$
2	$X_{e,1}$	$\tilde{X}_{\mathcal{E}\setminus\{e\},1}$	$Y_{e,1}$	$\tilde{Y}_{\mathcal{E}\setminus\{e\},1}$
3	$\tilde{X}_{e,1}$	$X_{\mathcal{E}\setminus\{e\},2}$	$\tilde{Y}_{e,1}$	$Y_{\mathcal{E}\setminus\{e\},2}$
4	$X_{e,2}$	$\tilde{X}_{\mathcal{E}\setminus\{e\},2}$	$Y_{e,2}$	$\tilde{Y}_{\mathcal{E}\setminus\{e\},2}$
5	$\tilde{X}_{e,2}$	$X_{\mathcal{E}\setminus\{e\},3}$	$\tilde{Y}_{e,2}$	$Y_{\mathcal{E}\setminus\{e\},3}$
6	$X_{e,3}$	$\tilde{X}_{\mathcal{E}\setminus\{e\},3}$	$Y_{e,3}$	$\tilde{Y}_{\mathcal{E}\setminus\{e\},3}$
7	$\tilde{X}_{e,3}$		$\tilde{Y}_{e,3}$	
…	…	…	…	…
$2n-1$		$X_{\mathcal{E}\setminus\{e\},n}$		$Y_{\mathcal{E}\setminus\{e\},n}$
$2n$	$X_{e,n}$	$\tilde{X}_{\mathcal{E}\setminus\{e\},n}$	$Y_{e,n}$	$\tilde{Y}_{\mathcal{E}\setminus\{e\},n}$
$2n+1$	$\tilde{X}_{e,n}$		$\tilde{Y}_{e,n}$	

用这种方式，我们构造了网络纠错码，在延迟为$\mathbf{d}_{\mathcal{E}}+\mathbf{d}_e$的情况下渐进达到速率$\mathbf{R}^{(\mathcal{K})}$。引理得证。　□

6.3.2 剩余部分的证明

首先来证明定理 6.1。

引理 6.1 告诉我们这样的一个事实：延迟$\mathbf{d}_{\mathcal{E}}+\mathbf{d}_e$虽然比$\mathbf{d}_{\mathcal{E}}$延迟大，但是信道容量域却是一样的。利用这个性质就可以证得定理 6.1。

引理 6.2：给定的网络$\mathcal{G}$、连接集$\mathcal{K}$、攻击组合$\mathcal{A}$、各链路速率$\mathbf{f}_{\mathcal{E}}$的情况下，考虑两个延迟$\mathbf{d}'_{\mathcal{E}}$和$\mathbf{d}''_{\mathcal{E}}$。若$\mathbf{d}'_{\mathcal{E}}\geq\mathbf{d}''_{\mathcal{E}}$，则

$$\mathcal{C}(\mathbf{d}'_{\mathcal{E}}) \subseteq \mathcal{C}(\mathbf{d}''_{\mathcal{E}}).$$ □

证明：任取$\mathbf{R}^{(\mathcal{K})} \in \mathcal{C}(\mathbf{d}'_{\mathcal{E}})$。则在延迟$\mathbf{d}'_{\mathcal{E}}$时存在网络纠错码可以渐进达到这个速率。现在考虑延迟$\mathbf{d}''_{\mathcal{E}}$的情况。首先在每个链路$e$的输入处故意延迟$d'_e - d''_e$，使得整个网络的延迟等价于$\mathbf{d}'_{\mathcal{E}}$。然后在使用之前延迟$\mathbf{d}'_{\mathcal{E}}$时的网络纠错码。这样就在延迟为$\mathbf{d}''_{\mathcal{E}}$的网络中得到新的网络纠错码渐进达到速率$\mathbf{R}^{(\mathcal{K})} \in \mathcal{C}(\mathbf{d}'_{\mathcal{E}})$。引理得证。□

定理 6.1 的证明：由引理 6.1 可以知道$\mathcal{C}(\mathbf{d}_{\mathcal{E}}) \subseteq \mathcal{C}(\mathbf{0}_{\mathcal{E}})$。下面证明$\mathcal{C}(\mathbf{0}_{\mathcal{E}}) \subseteq \mathcal{C}(\mathbf{d}_{\mathcal{E}})$。连续$\prod_{e\in\mathcal{E}} \lceil d_e \rceil$次使用引理 6.2，可以得到

$$\mathcal{C}(\mathbf{0}_{\mathcal{E}}) \subseteq \mathcal{C}(\lceil \mathbf{d}_{\mathcal{E}} \rceil),$$

其中$\lceil \mathbf{d}_{\mathcal{E}} \rceil \triangleq (\lceil d_e \rceil : e \in \mathcal{E})$。另外，引理 6.1 还告诉我们$\mathcal{C}(\lceil \mathbf{d}_{\mathcal{E}} \rceil) \subseteq \mathcal{C}(\mathbf{d}_{\mathcal{E}})$。所以$\mathcal{C}(\mathbf{0}_{\mathcal{E}}) \subseteq \mathcal{C}(\mathbf{d}_{\mathcal{E}})$。定理得证。 □

下面考虑定理 6.2。从性质 3.1 可以看出，定理 6.1 和定理 6.2 实际上是互为对偶的，从定理 6.1 可立即得定理 6.2。当然，我们还可以用证明定理 6.1 的方法直接证明定理 6.2：先证明$\forall \mathbf{d}_{\mathcal{E}} \geq \mathbf{0}_{\mathcal{E}}$，$\mathcal{R}(\mathbf{d}_{\mathcal{E}}) \subseteq \mathcal{R}(\mathbf{d}_{\mathcal{E}} + \mathbf{d}_e)$；再证明对于任意的$\mathbf{d}'_{\mathcal{E}} \geq \mathbf{d}''_{\mathcal{E}}$，$\mathcal{R}(\mathbf{d}'_{\mathcal{E}}) \subseteq \mathcal{R}(\mathbf{d}''_{\mathcal{E}})$；就得证了。

第 7 章　结语

内容提要

- 7.1 节简要回顾全文内容，再次介绍本文的主要结论和创新点。
- 7.2 节介绍本研究遗留的理论问题。

7.1 本文内容回顾

本文通过求解在任意给定有向图上的信道容量域和容许速率域，定量分析了通信网络中的攻击错误对通信网络的性能影响，刻画网络纠错的极限性能。

本文的创新点回顾如下：

(1) 问题创新。本文考虑了一些之前研究没有考虑过的问题。例如，本文考虑了网络纠错容许速率域，并获得了相关结果（如一般网络的容许速率域的内界和外界，两节点网络的容许速率域和蟑螂网络的容许速率域等）。本文还考虑了延时对网络纠错极限性能的影响，并得到相关结果（攻击方在篡改等错误的基础上再引入延时不会改变信道容量域和容许速率域。）。

(2) 方法创新。在构造攻击方案刻画外界和构造纠错码刻画内界的过程中，本研究使用了一些全新的思路。在攻击方案构造方面，通过分析链路之间的连接，得到信息支配的关系，再结合熵不等式，设计出了更凌厉的攻击方案，得到了更紧的外界；在网络纠错码的构造方面，注意到码本不能完全表示网络纠错码，进一步使用了组合知识传递原理设计了更为强大的网络纠错码，得到了更紧的内界。

(3) 结果创新。本文为信道容量域和容许速率域求得了更紧的外界和内界，在更多特别的网络中完全求得了结果。例如：求得了众多三点网络的信道容量，求得了两节点网络和蟑螂网络的容许速率域；求得了多址接入直连信道的容许速率域，等等。

7.2 遗留的问题

在前人与本文的基础上，该研究还遗留有以下理论问题。

(1) 完全刻画信道容量域和容许速率域

如前所述，本论文试图求解信道容量域和容许速率域。但是对于一般的网络和一般的纠错目标，信道容量域和容许速率域并没有完全求出。后续研究可以尝试设计新的纠错码和攻击方案，得到更紧的内界和外界，求出更多网络的纠错目标的信道容量域和容许速率域。

(2) 判定信道容量域问题和容许速率域问题的计算复杂度

网络纠错模型的信道容量域问题和容许速率域问题是一个困难问题，求解信道容量域和容许速率域的困难性不亚于无记忆随机网络的信道容量问题（该问题的计算复杂度等价于熵空间问题[72]）。后续研究可以使用理论计算机中的相关概念，判定信道容量域的求解和容许速率域的求解属于哪一个计算复杂度类。

除了直接涉及的理论问题外，还有一些和本问题的求解直接相关的理论问题。包括：

(1) 普通码字界问题、混合码码字界与交互模型码字界

在第 2 章中我们讨论了单次交互模型的码字界问题。这个问题的困难性不亚于普通的码字界问题和混合码的码字界问题。目前虽然对码字界问题的困难性已经有了认识，但是不排除有其他方法能够得到码字界更加精确的界。

(2) 熵不等式与熵空间刻画问题

由于熵不等式可以用于外界的刻画，所以找到更多的熵不等式对网络纠错问题具有明显的帮助。而熵空间的刻画问题作为信息论最基本、最重要的问题之一，目前也是开放性问题。

7.3 应用展望

本文的研究结果定量分析了通信网络中的攻击错误对通信网络的性能影响，刻画网络纠错的极限性能。在实际应用中，可以将这些研究方法和结果根据实际应用场景的特点和限制进行组合和推广，分析在实际应用场景下的极限性能，判定在关注的场景下是否存在满足给定要求的网络纠错码。

但是，如果将网络纠错码应用在实际系统中，需要考虑实际系统中可能涉及到动态拓扑、有限码长等多种限制，对拓扑的依赖和码的决定也可能会产生很大的开销，这些都需要再进行分析。

参考文献

[1] Liang J, Kumar R, Xi Y, Ross K. Pollution in P2P file sharing systems. IEEE INFOCOM, 2005, 1174–1185.

[2] Shin S, Jung J, Balakrishnan H. Malware prevalence in the KaZaA file-sharing network. ACM SIGCOMM on Internet measurement, 2006, 333–338.

[3] Shor P. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing, 1997, 26(5):1484–1509.

[4] Monz T, Nigg D, Martinez E, Brandl M, Schindler P, Rines R, Wang S, Chuang I, Blatt R. Realization of a scalable Shor algorithm. Science, 2016, 351(6277):1068–1070.

[5] Shannon C. A mathematical theory of communication. Bell System Technical Journal, 1948, 27(3):379–423.

[6] Shannon C. A mathematical theory of communication, Bell System Technical Journal. 1948, 27(4):623–656.

[7] Gamal A, Kim Y. Network Information Theory, Jan. 2012, Cambridge University Press.

[8] Kim S, Ho T, Effros M, Avestimehr A. Network error correction with unequal link capacities. IEEE Trans. Inf. Theory, 2011, 57(2):1144–1163.

[9] Kosut O, Tong L, Tse D. Polytope codes against adversaries in networks. IEEE Trans. Inf. Theory, 2014, 60(6):3308–3344.

[10] Yang S. Coherent network error correction. Ph.D. dissertation, The Chinese University of Hong Kong, Hong Kong, 2008.

[11] Bassoli R, Marques H, Rodriguez J, Shum K, Tafazolli R, Network coding theory: A survey. IEEE Comm. Surveys Tutorials, 2013, 15(4):1950–1978.

[12] Singleton R. Maximum distance q-nary codes. IEEE Trans. Inf. Theory, 1964, 10(2):116–118.

[13] Steiglitz K, Weiner P, Kleitman D. The design of minimum-cost survivable networks. IEEE Trans. Circuit Theory, 1969, 16(4):455–460.

[14] Singleton R. Maximum distance q-nary codes. IEEE Trans. Inf. Theory, 1964, 10(2):116–118.

[15] Bhandari R, Survivable networks: Algorithms for diverse routing. Springer, 1999.

[16] Roche J. Distributed information storage. Ph.D. dissertation, Stanford University, USA, 1992.

[17] Yeung R. Multilevel diversity coding with distortion. IEEE Trans. Inf. Theory, 1995, 41(2):412–422.

[18] Roche J, Yeung R, Hau K. Symmetrical multilevel diversity coding. IEEE Trans. Inf. Theory, 1997, 43(3):1059–1064.

[19] Roche J, Yeung R, Hau K. Multilevel diversity coding with symmetrical connectivity. IEEE Int. Symp. Inf. Theory, 1995, 262.

[20] Yeung R, Zhang Z. On symmetrical multilevel diversity coding. IEEE Trans. Inf. Theory, 1999, 45(2):609–621.

[21] Mohajer S, Tian C, Diggavi S. Asymmetric multilevel diversity coding and asymmetric Gaussian multiple descriptions. IEEE Trans. Inf. Theory, 2010, 56(9):4367–4387.

[22] Mohajer S, Tian C, Diggavi S. Asymmetric Gaussian multiple descriptions and asymmetric multilevel diversity coding, IEEE Int. Symp. Inf. Theory, 2008, 1992–1996.

[23] Balasubramanian A, Ly H, Li S, Liu T, Miller S. Secure symmetrical multilevel diversity coding, IEEE Trans. Inf. Theory, 2013, 59(6):3572–3581.

[24] Jiang J, Marukala N, Liu T. Symmetrical multilevel diversity coding and subset entropy inequalities. IEEE Trans. Inf. Theory, 2014, 60(1):84–103.

[25] Tian C, Liu T. Multilevel diversity coding with regeneration. IEEE Int. Symp. Inf. Theory, 2015. 844–848.

[26] Chen J, Berger T. Robust distributed source coding. IEEE Trans. Inf. Theory, 2008, 54(8):3385–3398.

[27] Koetter R, Medard M. An algebraic approach to network coding. IEEE Trans. Inf. Theory, 2003, 11(5):782–795.

[28] Ho T, Medard M, Koetter R. An information-theoretic view of network management, IEEE Trans. Inf. Theory, 2005, 51(4):1295–1312.

[29] Bahramgiri H, Lahouti F. Robust network coding against path failures. IET Communications, 2010, 4(3):272–284.

[30] Koetter R, Kischischang F. Coding for errors and erasures in random network coding, IEEE Int. Symp. Inf. Theory, 2007. 24–29.

[31] Silva D, Kschischang F, Koetter R. A rank-metric approach to error control in random network coding. IEEE Trans. Inf. Theory, 2008, 54(9):3951–3967.

[32] Silva D, Kschischang F, Koetter R, A rank-metric approach to error control in random network coding. IEEE Inf. Theory Workshop on Inf. Theory for Wireless Networks, 2007. 1–5.

[33] Balli H, Yan X, Zhang Z. On randomized linear network codes and their error correction capabilities. IEEE Trans. Inf. Theory, 2009, 55(7):3148–3160.

[34] Silva D, Kschischang F. Universal secure network coding via rank-metric codes. IEEE Trans. Inf. Theory, 2011, 57(2):1124–1135.

[35] Vyetrenko S. Network coding for error correction. Ph.D. dissertation, California Institute of Technology, USA. 2011.

[36] Cai N, Yeung R. Network coding and error correction. IEEE Inf. Theory Workshop, 2002. 20–25.

[37] Yang S, Yeung R. Characterizations of network error correction/detection and erasure correction. Proc. NetCod, 2007.

[38] Yeung R, Cai N. Network error correction, part I: basic concepts and upper bounds, Communications in Information and Systems, 2006, 6(1):19–36.

[39] N. Cai, R. Yeung. Network error correction, part II: lower bounds. Communications in Information and Systems, 2006, 6(1):37–54.

[40] Zhang Z. Linear network error correction codes in packet networks. IEEE Trans. Inf. Theory, 2008, 54(1):209–218.

[41] Zhang Z, Yan X, Balli H. Some key problems in network error correction coding theory, IEEE Inf. Theory Workshop on Inf. Theory for Wireless Networks, 2007. 1–5.

[42] Zhang Z. Some recent progresses in network error correction coding theory. Workshop on Network Coding, Theory and Applications, 2008. 1–5.

[43] Matsumoto R. Construction algorithm for network error-correcting codes attaining the Singleton bound. IEICE Trans. Fundamentals, 2007, E90-A(9):1729–1735.

[44] Yang S, Yeung R, Ngai C. Refined coding bounds and code constructions for coherent network error correction. IEEE Trans. Inf. Theory, 2011, 57(3):1409–1424.

[45] Guang X, Fu F, Zhang Z. Construction of network error correction codes in packet networks, IEEE Trans. Inf. Theory, 2013, 59(2):1030–1047.

[46] Ho T, Leong B, Koetter R, Mdard M, Effros M, Karger D. Byzantine modification detection in multicast networks with random network coding. IEEE Trans. Inf. Theory, 2008, 54(6):2798–2803.

[47] Balli H. On random linear network coding. Ph.D. dissertation, USC, 2008.

[48] Balli H, Yan X, Zhang Z. On randomized linear network codes and their error correction capabilities. IEEE Trans. Inf. Theory, 2009, 55(7):3148–3160.

[49] Guang X. Random network coding and network error correction coding. Ph.D. dissertation, Nankai University, 2012.

[50] Gadouleau M, Goupil A. A matroid framework for noncoherent random network communications. IEEE Trans. Inf. Theory, 2011, 57(2):1031–1045.

[51] Kim S. Network coding for resource optimzation and error correction. Ph.D. dissertation, Caltech, 2010.

[52] Kosut O. Adversaries in networks. Ph.D. dissertation, Cornell University, Aug. 2010.

[53] Kosut O, Tong L, Tse D. Polytope codes against adversaries in networks. IEEE Int. Symp. Inf. Theory, 2010. 2423–2427.

[54] Koetter R, Medard M. An algebraic approach to network coding. IEEE Trans. Inf. Theory, 2003, 11(5):782–795.

[55] Kim S, Ho T, Effros M, Avestimehr S. Network error correction with unequal link capacities. Allerton Conference, 2009. 1387–1394.

[56] Kosut O, Tong L, Tse D. Nonlinear network coding is necessary to combat general Byzantine attacks. Allerton Conference, 2009. 693–699.

[57] Dikaliotis T, Ho T, Jaggi S, Vyetrenko S, Yao H, Kliewer J, Erez E. Multiple-access network information-flow and correction codes. IEEE Trans. Inf. Theory, 2011, 57(2):1067–1079.

[58] Kosut O, Tong L. Distributed source coding in the presence of Byzantine sensors. IEEE Trans. Inf. Theory, 2008, 54(6):2550–2565.

[59] Ahmed E, Wagner A. Lossy source coding with Byzantine adversaries. IEEE Inf. Theory Workshop, 2011. 462–466.

[60] Zhang Z. Theory and applications of network error correction coding. Proceedings of IEEE, 2011, 99(3):406–420.

[61] Sanna M, Izquierdo E. A survey of linear network coding and network error correction code constructions and algorithms. International Journal of Digital Multimedia Broadcasting, 2011, 1–12.

[62] Yeung R. A framework for linear information inequalities, IEEE Trans. Inf. Theory, 1997, 43(6):1924–1934.

[63] Zhang Z, Yeung R. A non-Shannon-type conditional inequality of information quantities. IEEE Trans. Inf. Theory, 1997, 43(6):1982–1986.

[64] Zhang Z, Yeung R. On characterization of entropy function via information inequalities. IEEE Trans. Inf. Theory, 1998, 44(4):1440–1452.

[65] Yeung R, Zhang Z. A class of non-Shannon-type information inequalities and their applications. IEEE Int. Symp. Inf. Theory, 2001. 231.

[66] Yeung R, Zhang Z. A class of non-Shannon-type information inequalities and their applications. Communications in Information and Systems, 2001, 1:87–100.

[67] Makarychev K, Makarychev Y, Romashcheko A, Vereshchagin N. A new class of non-Shannon type information inequalities for entropies. Communications in Information and Systems, 2002, 2(2):147–166.

[68] Zhang Z. On a new non-Shannon-type information inequality. Communications in Information and Systems, 2003, 3(1):47–60.

[69] Dougherty R, Freiling C, Zeger K. Six new non-Shannon information inequalities. IEEE Int. Symp. Inf. Theory, 2006. 233–236.

[70] Xu W, Wang J, Sun J. A projection method for derivation of non-Shannon-type information inequalities. IEEE Int. Symp. Inf. Theory, 2008. 2116–2120.

[71] Matus F. Infinitely many information inequalities. IEE Int. Symp. Inf. Theory, 2007. 41–44.

[72] Yan X, Yeung R, Zhang Z. An implicit characterization of the achievable rate region for acyclic multisource multisink network coding. IEEE Trans. Inf. Theory, 2012, 58(9):5625–5639.

[73] Han T. Nonnegative entropy measures of multivariate symmetric correlations, Inf. Control, 1978, 36(2):133–156.

[74] Harvey N, Kleinberg R, Lehman A. On the capacity of information networks. IEEE Trans. Inf. Theory, 2006, 52(6):2345–2364.

[75] Yao A. Some complexity questions related to distributive computing. ACM Symp. Theory of Computing, 1979. 209–213.

[76] Schulman L. Communication on noisy channels: A coding theorem for computation. IEEE Symp. Foundations Computer Science, 1992. 724–733.

[77] Schulman L. Deterministic coding for interactive communication. ACM Symp. Theory of Computing, 1993. 747–756.

[78] Gelles R, Moitra A, Sahai A. Efficient and explicit coding for interactive communication. IEEE Symp. Foundations Computer Science, 2011. 768–777.

[79] Braverman M. Towards deterministic tree code constructions. Proc. Innovations in Theoretical Computer Science Conf., 2012. 161–167.

[80] Brakerski Z, Kalai Y. Efficient interactive coding against adversarial noise. IEEE Symp. Foundations Computer Science, 2012. 160–166.

[81] Ghaffari M, Haeupler B. Optimal error rates for interactive coding II: Efficiency and list decoding. IEEE Symp. Foundations Computer Science, 2014. 294–403.

[82] Braverman M, Rao A. Towards coding for maximum errors in interactive communication. ACM Symp. Theory Computing, 2011. 159–166.

[83] Hamming R. Error detecting and error correcting codes. Bell System Technical Journal, 1950, 29, 147–160.

[84] Astola J. An Elias-type bound for Lee codes over large alphabets and its application to perfect codes (Corresp.). IEEE Trans. Inf. Theory, 1982, 28(1):111–113.

[85] Johnson S. On upper bounds for unrestricted binary-error-correcting codes. IEEE Trans. Inf. Theory, 1971, 17(4):466–478.

[86] Mounits B, Etzion T, Litsyn S. Improvement on the Johnson upper bound for error-correcting codes. IEEE Int. Symp. Inf. Theory, 2002, 345.

[87] Laihonen T, Litsyn S. On Upper Bounds for Minimum Distance and Covering Radius of Non-binary Codes. Designs, Codes and Cryptography, 1998, 14(1):71–80.

[88] Delsarte P. An algebraic approach to the association schemes of coding theory. Ph.D. dissertation, Universite Catholique de Louvain, 1973.

[89] Schrijver A. New code upper bounds from the Terwilliger algebra and semidefinite programming. IEEE Trans. Inf. Theory, 2005, 51(8):2859–2866.

[90] Gijswijt D, Mittelmann H, Schrijver A. Semidefinite code bounds based on quadruple distances. IEEE Trans. Inf. Theory, 2012, 58(5):2697–2705.

[91] Kim H, Toan P. Improved semidefinite programming bound on sizes of codes. IEEE Trans. Inf. Theory, 2013, 59(11):7337–7345.

[92] Plotkin M. Binary codes with specified minimum distance. IRE Trans. Inf. Theory, 1960, 6(4):445–450.

[93] Brouwer A. [online] http://www.win.tue.nl/~aeb/codes/.

[94] Herzog M, Schonheim J. Linear and nonlinear single-error-correcting perfect mixed codes. Information and Control, 1971, 18(4):364–368.

[95] Heden O. A new construction of group and nongroup perfect codes. Information and Control, 1977, 34(4):314 – 323.

[96] Etzion T, Greenberg G. Constructions for perfect mixed codes and other covering codes. IEEE Trans. Inf. Theory, 1993, 39(1):209–214.

[97] Hamalainen H, Rankinen S. Upper bounds for football pool problems and mixed covering codes. Journal of Combinatorial Theory, Series A, 1991, 56(1):84 – 95.

[98] Brouwer A, Hamalainen H, Ostergard P, Sloane N. Bounds on mixed binary/ternary codes. IEEE Trans. Inf. Theory, 1998, 44(1):140–161.

[99] Perkins S, Sakhnovich A, Smith D. On an upper bound for mixed error-correcting codes. IEEE Trans. Inf. Theory, 2006, 52(2):708–712.

[100] Ostergard P. Constructions of mixed covering codes. Helsinki University of Technology, Digital Systems Laboratory, Series A: Research Reports. 1991.

[101] Slepian D, Wolf J. Noiseless coding of correlated information sources. IEEE Trans. Inf. Theory, 1973, 19(4):471–480.

[102] Cover T. A proof of the data compression theorem of Slepian and Wolf for ergodic sources (Corresp.). IEEE Trans. Inf. Theory, 1975, 21(2):226–228.

[103] Csiszar I. Linear codes for sources and source networks: Error exponents, universal coding. IEEE Trans. Inf. Theory, 1982, 28(4):585–592.

[104] Koetter R, Effros M, Medard M. On a theory of network equivalence. IEEE Information Theory Workshop, 2009. 326–330.

[105] Effros M. On dependence and delay: capacity bounds for wireless networks. IEEE Wireless Communications and Networking Conference, 2012. 550–554.

[106] Koetter R, Effros M, Medard M. A theory of network equivalence – Part I: Point-to-point channels. IEEE Tran. Inf. Theory, 2011, 57(2):972–995.

[107] Koetter R, Effros M, Medard M. A theory of network equivalence – Part II: Multiterminal channels. IEEE Tran. Inf. Theory, 2014, 60(7):3709–3732.

[108] Kosut O, Kliewer J. Equivalence for networks with adversarial state. IEEE Int. Symp. Inf. Theory, 2014. 2401–2405.

[109] Kosut O, Kliewer J. Equivalence for networks with adversarial state. submitted to IEEE Trans. Inf. Theory. [online] http://arxiv.org/abs/1404.6701.

致　谢

首先感谢我的导师王京教授。在我研究生的学习阶段，王老师以其渊博的知识和开阔的视野帮助我克服选题、开题、结题答辩等一个又一个难关。本研究直接触及网络信息论的理论最前沿，既需要非常充裕的资源在一个很高的平台上进行知识积累和学术交流，又需要容忍在短期内可能没有相关的直接收益，还需要有进入未知领域的胆识。他提供的这样优秀的平台和资源和高度的灵活性是在中国内地是屈指可数的。

感谢清华大学信息技术研究院的李云洲老师。李老师从我的本科毕业设计开始一直到我完成研究的这五年多时间里，深入科研和生活等各领域细节，悉心对我进行深入指导，并为该研究提供了大量资金支持，为最终发表高水平论文起到了重要作用。

感谢我在加拿大 McMaster 大学访学期间的指导老师陈隽老师。陈隽老师惊人的智商、情商和在信息论上深厚的积累让人叹为观止。陈老师的热心指导对我发表在 IEEE Transactions on Information Theory 上的文章有非常大的帮助。

感谢实验室内其他帮助过我的老师和同学。另外香港中文大学的杨升浩老师在清华大学任教期间给我科普了大量的网络信息论知识，也一并感谢。

最后感谢我的爸爸和妈妈对我一如既往的支持与理解。

声　明

本人郑重声明：所呈交的学位论文，是本人在导师指导下，独立进行研究工作所取得的成果。尽我所知，除文中已经注明引用的内容外，本学位论文的研究成果不包含任何他人享有著作权的内容。对本论文所涉及的研究工作做出贡献的其他个人和集体，均已在文中以明确方式标明。

签名：　　日期：

个人简历与在学期间发表的学术论文

个人简历

1989 年 09 月 11 日出生于福建省福州市。

2007 年 8 月考入北京邮电大学通信工程专业，2011 年 7 月本科毕业并获得工学学士学位。

2011 年 9 月免试进入清华大学电子工程系攻读信息与通信工程博士至今。

发表的学术论文

[1] Xiao Z, Li Y, Zhao M, Wang J. Interactive codes to correct and detect omniscient Byzantine adversary. IEEE Information Theory Workshop, 2014. 45–49. (EI 收录，检索号 20152100859644)

[2] Xiao Z, Li Y, Xiao L, Wang J. Size of 1-error-correcting codes in three interactive transmissions. IEEE VTC-spring, 2015. 1–4. (EI 收录，检索号 20153501223596)

[3] Xiao Z, Li Y, Zhao M, Xu X, Wang J. Allocation of network error correction flow to combat Byzantine attacks. IEEE Transactions on Communications, 2015, 63(7):2605–2618. (SCI 收录，检索号 CN1WB，影响因子 1.992)

[4] Xiao Z, Li Y, Wang J. Allocation of network error correction flow on disjoint paths. Tsinghua Science and Technology, 2015, 20(2):182–187. (SCI 收录，检索号 CV7XM)

[5] Xiao Z, Chen J, Li Y, Wang J. Distributed multilevel diversity coding. IEEE Transactions on Information Theory, 2015, 61(11):6368–6384. (SCI 收录，检索号 CU1CI，影响因子 2.326)

[6] Xiao Z, Li Y, Su X, Wang J. Processing delays do not degrade network error-correction capacity in directed networks. IEEE Communications Letters, 2015, 19(12):2054–2057. (SCI 收录，检索号 CY7TX，影响因子 1.268)