网络编码研究基础

蒲保兴　秦波莲◎著

NETWORK CODING

中国工信出版集团
人民邮电出版社
POSTS & TELECOM PRESS

网络编码研究基础

蒲保兴　秦波莲◎著

人民邮电出版社
北京

图书在版编目（CIP）数据

网络编码研究基础 / 蒲保兴，秦波莲著. -- 北京 : 人民邮电出版社，2016.12
ISBN 978-7-115-43562-0

Ⅰ. ①网… Ⅱ. ①蒲… ②秦… Ⅲ. ①计算机网络－编码程序－程序设计 Ⅳ. ①TP393

中国版本图书馆CIP数据核字(2016)第223044号

内 容 提 要

网络编码是一种新型的数据传输技术，现已成为网络信息论的一个重要的研究方向，对网络技术的发展具有深远的意义。

本书系统地阐述了网络编码的基本原理，在介绍有限域算术运算方法的基础上，详细地介绍了确定性网络编码构造方法和随机网络编码构造方法，并详细地描述了仿真实现过程。此外，本书还介绍了作者多年来对网络编码的研究成果。

本书可作为信息类专业研究生的参考书，也可作为从事网络编码研究的入门教材。

◆ 著　　蒲保兴　秦波莲
责任编辑　邢建春
执行编辑　吴彤云
责任印制　彭志环

◆ 人民邮电出版社出版发行　　北京市丰台区成寿寺路 11 号
邮编　100164　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
固安县铭成印刷有限公司印刷

◆ 开本：700×1000　1/16
印张：15.5　　2016 年 12 月第 1 版
字数：303 千字　　2016 年 12 月河北第 1 次印刷

定价：88.00 元

读者服务热线：(010)81055488　印装质量热线：(010)81055316
反盗版热线：(010)81055315

前　言

网络编码是一种新型的数据传输技术，与传统的路由传输技术相比，中间节点不仅具有存储和转发数据的功能，还可以对接收到的信息进行编码后再进行传输。网络编码能提高网络的传输性能，在提升网络的吞吐率、实现网络的负载均衡、增加网络的顽健性与安全性等方面具有优势，但因节点需要编码或解码，数据传输过程中也增加了编码运算代价。

采用网络编码技术实现数据传输的关键是构造网络编码方案，编码方案不仅决定了宿点能否解码，还决定了网络的吞吐率和编码运算代价。显然，提高网络的吞吐率、降低编码运算代价对网络编码的实际应用具有重要的意义，是网络编码方案优化构造的两个重要目标。

笔者围绕这两个目标，对网络编码进行了潜心的研究，在多年研究的基础上撰写了本书。本书主要包括了以下几个方面的内容：（1）网络编码的基本原理；（2）在介绍了有限域算术运算方法的基础上，阐述了确定性网络编码和随机网络编码构造方法，并给出了仿真实验平台；（3）提出了网络编码导出与扩展技术；（4）讨论了未知网络拓扑环境下网络编码优化构造方法；（5）讨论了网络编码运算代价与环境参数（伽罗华域、多播率和数据块长）之间的关系；（6）对多源网络编码的优化构造进行了研究。

本书共分为10章，第1章为绪论，介绍了网络编码的基本概念、起源和发展；第2章阐述了阅读本书所需要的相关理论和技术，主要包括网络最大流的概念和算法、有限域的算术运算方法等；第3章阐述了线性网络编码的基本原理和技术，重点介绍了确定性网络编码和随机网络编码构造方法，并给出仿真实验平台；第4章运用了代数知识提出了线性网络编码的导出与扩展技术，它是第5章和第6章的基础；第5章给出了未知网络拓扑环境下确定性网络编码构造算法；第6章给出了网络编码优化构造方法，并给出了网络拓扑动态变化环境下的编码策略；第7章对网络编码的运算代价进行了估算与分析；第8章给出了一种分级网络编码构造方

法；第9章给出基于随机网络编码的差错控制方法；第10章对多源网络编码进行了研究。附录给出了网络编码仿真实验平台的程序和使用说明。

本书得到了湖南省教育厅重点科研项目（11A111，12A068）的资助。由于水平有限，书中难免存在缺点和疏漏之处，敬请广大读者批评指正。

蒲保兴

2016年4月

目　录

第1章 绪 论

网络传输和处理能力的大幅提高使基于网络的应用越来越多，特别是音频和视频技术的发展和成熟，使网络音频、视频应用成为最重要的应用之一，诸如视频点播、视频会议、远程学习、计算机协同操作等多媒体应用也随之出现。这些多媒体应用和一般的网络应用相比，有数据量大、时延要求高、持续时间长等特点。要解决这些具有传输带宽大、实时性强、有多点接收等特征的问题，需要采用不同于单播与广播机制的转发技术。多播是一种点到多点（或多点到多点）的通信方式[1]，由源点发送数据到多个宿点，且源点只需发送同一报文。多播通信方式能够有效地利用网络的带宽，提高了网络资源的利用率。作为一种新型的网络通信方式，多播通信方式具有广阔的应用前景，典型地可应用在视频点播、网络会议、远程教育、网络电话、交互游戏、分布式多媒体数据库等大量新型的多媒体通信应用领域。为实现这一新型的通信方式，需要对多播通信的理论与应用进行深入广泛的研究。自从20世纪90年代以来，基于路由技术的多播通信研究已经得到了蓬勃的发展，研究人员提出了多个多播路由算法[2,3]。21世纪初提出的网络编码技术[4~6]为网络理论与应用拓展了一个新的方向，相应地为多播通信方式提供了一个新的平台，面向多播通信的网络编码技术研究成为一个令人关注的热点，并得到了飞速地发展[7,8]。

网络编码是一种新型的数据传输技术，它与传统的路由技术相比，最大不同之处在于：在数据传输过程中，中间节点不仅能对接收到的消息直接转发，还可以把接收到的消息进行运算后再转发。

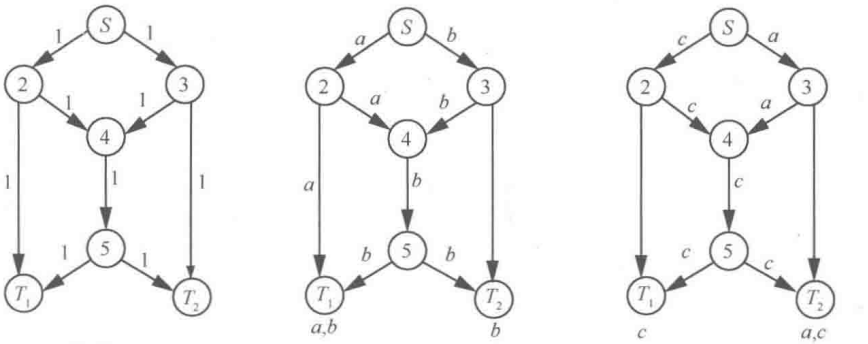
网络编码技术是通信网络中信息处理和传输理论研究上的重大突破[9]，它推广了传统的路由技术，其核心思想是既允许网络中间节点对传输的信息进行转发和复制，又可以进行信息编码，而路由本身则被认为是一种特殊的网络编码。与传统的路由技术相比，网络编码在提升网络的吞吐量、节省网络带宽的资源消耗、

均衡网络负载、增加网络的顽健性和安全性等方面具有优势[9~12]。经过几年的发展，网络编码的理论研究已取得了可喜的进展，在应用基础和工程实践方面的研究已全方位地展开，网络编码已成为一项融合信息论、代数学、图论、网络流理论和优化理论等多门学科的交叉技术，且日益引起更多研究者的热切关注，为现有的网络体系结构、协议设计方法、信息交换方式和网络管理模式带来了革命性的变化[7,9]，国外多所著名大学和许多知名的 IT 研究机构都在积极开展网络编码的理论和应用研究[14~16]。

根据香农理论，在单源多播网络中，源点的最大传输速率是分离源点与所有宿点间的最小割值（最大流界）[17,18]。基于路由技术的多播连接是通过构造多播树实现的，传统的多播树如最小费用多播树，其构造过程一般是 NP 难问题[19]，并对于一般的网络拓扑难以达到其最大流界。这主要是因为人们普遍认为在传统的路由机制中，网络中传输的信息是不能叠加的，因此中间节点只需进行信息的转发或复制。2000 年，Ahlswede 等[4]首次提出了网络编码的思想：在网络信息传输过程中，允许中间节点转发的信息是其输入信息在有限域上的编码组合。该文并且证明：采用网络编码技术可以实现单源多播网络的“最大流界”，并举例说明了传统的路由技术在一般情况下难以达到这个极限，从而采用网络编码传输技术可以提升单源多播网络的吞吐量。2003 年，李硕彦等[5]提出了线性网络编码技术，并证明了采用线性网络编码技术完全可以实现单源多播网络的最大流界，该文获得了“2005 年美国电机与电子工程师学会（IEEE）信息论文学会论文奖”，该项奖是 30 多年来首次由亚洲研究人员所获。线性网络编码的核心思想是：网络节点输出信道传输的信息是该节点所接收信息的线性组合。因线性网络编码具有操作简单的特点，并可运用向量代数的理论来进行相应的证明[20]，从而其理论与应用得到了深入广泛地研究，如无特别说明，本书所述的网络编码均指线性网络编码。

1.1 蝴蝶网络

图 1-1（a）是典型的蝴蝶网络，在不少文献中用于描述网络编码的原理，它是一个有向无环单源多播网络，其中节点 S 是源点，T_1 和 T_2 是宿点，节点 2、3、4、5 为中间节点。设每条链路的信道容量均为 1，即每条链路在单位时间内最多只能传输一个字符，而源点 S 欲通过网络多播信息至两个宿点 T_1、T_2。若采用路由传输技术，因为节点 4 至节点 5 的信道是数据传输的瓶颈，在一个时间单元内，源点最多只能多播一个 1.5 个字符至两个宿点，若采用网络编码技术，则可以多播 2 个字符。



(a) 蝴蝶网络　(b) 第1个时间单元的数据传输　(c) 第2个时间单元的数据传输

图 1-1　蝴蝶网络及路由传输方式

采用路由传输方式，则数据传输方式如图 1-1（b）和图 1-1（c）所示。在第 1 个时间单元内，数据传输方式如下。

（1）S 把字符 a 传输至输出信道<S,2>，把字符 b 传输至输出信道<S,3>。

（2）节点 2 从信道<S,2>上接收到字符 a 后，把它分别转发至输出信道<2,T_1>和<2,4>；节点 3 从信道<S,3>上接收到字符 b 后，把它转发至输出信道<3,4>和<3,T_2>。

（3）节点 4 尽管收到了两个字符，它们分别来自于信道<2,4>和<3,4>，由于信道<4,5>是数据传输的瓶颈，它在一个时间单元内只能传输一个字符。不妨令节点 4 转发的字符为 b，由节点 5 接收，节点 5 把接收到的字符从其输出信道分别转发出去，从而 T_1 收到了字符 a 和 b，而 T_2 只收到字符 b。因此，以一个时间单元为传输周期，则源点只能成功地多播 1 个字符至每一个宿点，如图 1-1（b）所示。

若以两个时间单元为一个传输周期，第 1 个时间单元的传输情况如图 1-1（b）所示，而第 2 个时间单位的传输情况如图 1-1（c）所示，从而在 2 个时间单元内，源点成功地多播了 3 个字符（a,b,c）至每一个宿点，则平均每个时间单元实现了多播 1.5 个字符。

若采用网络编码，即中间节点允许把接收到的信息进行编码后再转发，则能在每个时间单元内实现多播 2 个字符。在一个时间单元内各信道的传输情况如图 1-2 所示，传输方式如下。

（1）S 把字符 a 传输至输出信道<S,2>，把字符 b 传输至输出信道<S,3>。

（2）节点 2 从信道<S,2>上接收到字符 a 后，把它分别转发至输出信道<2,T_1>和<2,4>；节点 3 从信道<S,3>上接收到字符 b 后，把它转发至输出信道<3,4>和<3,T_2>。

（3）节点 4 分别从信道<2,4>和<3,4>上接收字符 a 和字符 b 后，对接收到的信息进行编码，即做异或运算：$c = a \oplus b$，然后把编码运算的结果 c 传输至输出

信道<4,5>。

（4）节点 5 从信道<4,5>收到信息 c 后，把它分别传输至信道<5,T_1>和<5,T_2>。

（5）宿点 T_1 分别从信道<2,T_1>和<5,T_1>上收到信息 a 和 c 后，做异或运算 $a \oplus c$，得到 b，从而宿点 T_1 接收到了源点播出的信息 a 和 b；同理，宿点 T_2 分别从信道<3,T_2>和<5,T_2>上收到信息 b 和 c 后，做异或运算 $b \oplus c$，得到 a，从而宿点 T_2 也接收到了源点播出的信息 a 和 b。

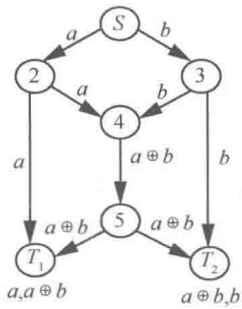


图 1-2　蝴蝶网络中采用网络编码数据传输方式

1.2　网络编码的优点

作为一种新型的数据传输技术，与传统的路由传输技术相比，网络编码具有下述优点：提升了网络的吞吐率；均衡了网络的流量负载；增加了网络的顽健性。

（1）提升网络的吞吐率

图 1-1 和图 1-2 的例子能够说明：在多播方式下，蝴蝶网络在路由传输方式下平均每个时间单元最多只能实现多播 1.5 个字符，而采用网络编码方式可达到 2 个字符。

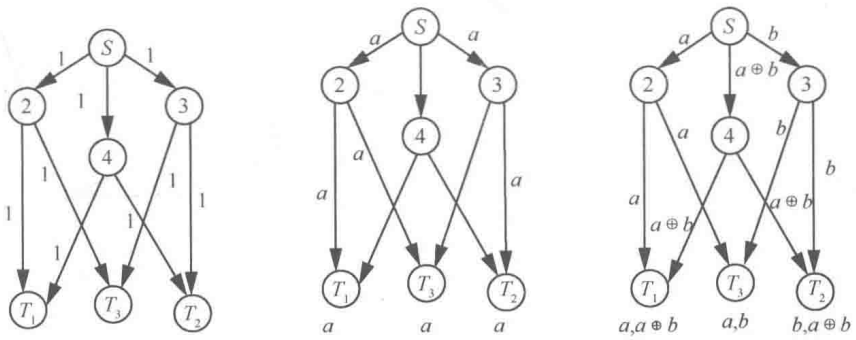
（2）均衡网络的流量负载

图 1-3 描述了这一情形。图 1-3（a）表示网络拓扑，其中每条边的链路容量均为 1。如采用路由传输方式，如图 1-3（b）所示，单位时间内源点 S 只能多播一个字符至宿点 T_1 和 T_2，且网络的负载极不均匀，只有<S,2>和<S,3>等相应的链路传输了信息，而<S,4>等链路没有传输信息。若采用网络编码，如图 1-3（c）所示，则单位时间内源点能播出 2 个字符，且每条链路均传输了消息。

（3）增加网络的顽健性

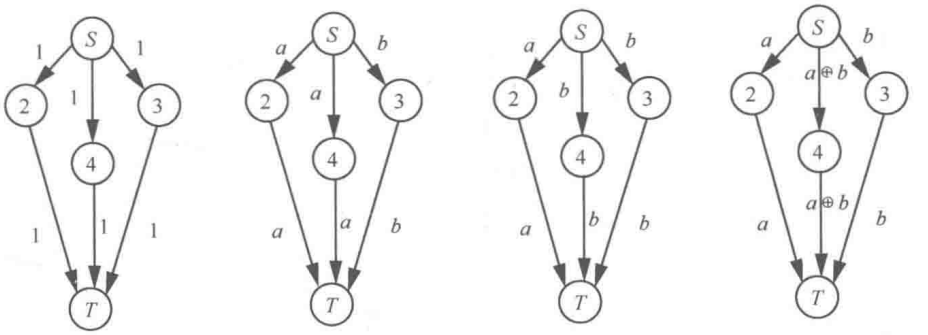
如图 1-4 所示，图 1-4（a）给出了网络拓扑，图 1-4（b）和图 1-4（c）分别给出了路由传输方式，两者均利用于冗余信道。使用冗余信道的目的是当某些信道出现故障时宿点仍能正确地接收源点传送的信息。图 1-4（b）对字符 a 传输 2

次，而图 1-4（c）对字符 b 传输 2 次。图 1-4（d）采用网络编码传输方式，注意到在网络编码传输方式中，宿点 T 可以任意选取两条输入链路的消息（有可能需要解码）获得源点播出的消息 a 和 b，因此网络中任意一条链路出现故障，宿点仍然能够正确接收源点播出的消息。而对于路由传输方式，则不能满足这个条件，例如，在图 1-4（b）的传输方式中，若链路<S,3>或<3,T>中的某一条出现故障，则宿点必定不能接收到字符 b，同理在图 1-4（c）的传输方式中，若链路<S,2>或<2,T>中某一条出现故障，则宿点必定不能正确地接收字符 a。由此可见采用网络编码提高了网络的顽健性。



(a) 网络拓扑　(b) 路由传输方式　(c) 网络编码传输方式

图 1-3　均衡网络流量负载



(a) 网络拓扑　(b) 路由传输方式1　(c) 路由传输方式2　(d) 网络编码传输方式

图 1-4　增加网络的顽健性

1.3　网络编码的缺点

与路由技术相比，网络编码存在如下不足之处：中间节点必须具有编码功能，宿点必须具有解码功能；中间节点增加了编码的运算代价，宿点增加了解码的运

算代价；中间节点需获知编码的策略，宿点需获知解码的策略。

（1）中间节点必须具有编码功能，宿点必须具有解码的功能

网络编码的实质是中间节点接收到信息后可以对其进行运算（编码），因此，中间节点必须具有能对接收的信息进行编码运算的功能，在传统的路由技术中，路由器等中间节点是不需要具备这些功能的。因此，如要采用网络编码技术，现有的网络体系结构无论从硬件还是软件上均要进行改进。

（2）由于中间节点需要编码、宿点需要解码，导致了中间节点和宿点都增加了运算代价。

（3）中间节点需获知编码策略，宿点需获知解码策略。

中间节点如何进行编码，宿点如何通过接收到的信息进行解码，这就是编码策略和解码策略，这一点非常重要，它有一套具体的规则，只有符合这套规则，才能保证宿点正确地解码恢复出源点的消息，下面章节将讨论这个问题，称之为网络编码的构造方法，就线性网络编码而言，有确定性网络编码构造方法和随机网络编码构造方法。

1.4 网络编码的实质

网络编码的实质是允许中间节点通过对接收到的信息进行运算后再进行转发，从而提高了网络吞吐率，在整体上提高了网络的传输速度，但节点增加了运算开销，从而是通过节点的运算代价来换取网络的吞吐量。

网络编码不同于信源编码，也不同于信道编码，更不同于加密与解密运算。信源编码是为了实现信息的压缩，而信道编码是为了在不可靠信道上实现数据传输，加密与解密是为了在信息的传输过程中把明文转换成密文，从而隐藏信息，防止被人窃听。从参与网络通信的节点类型来看，无论是信源编码、信道编码还是加密与解密运算均只需考虑信源节点和信宿节点，而网络编码涉及网络的中间节点。

1.5 线性网络编码与非线性网络编码

网络编码的实质是中间节点可以把接收到的信息进行运算再进行转发。如果把运算当成一个函数，则中间节点接收到的信息为自变量，运算后的结果为函数值，编码规则为函数运算。在宿点处，再把接收到的信息进行解码后再恢复出源点产生的信息，因此必须保证运算的封闭性，即选定一个集合，对集合中的元素

进行运算，其运算的结果仍然是该集合的元素。

代数中的数域具有运算的封闭性。在线性网络编码中，一般选定一个有限域（即伽罗华域），编码与解码均是对有限域的元素进行操作。无论是源点产生的信息，还是中间节点接收到的信息均看成是有限域中的一个元素。当中间节点对接收到的信息进行运算后，其结果也为该有限域的元素。宿点接收到的信息也是该有限域上的元素，通过解码运算后，得到的结果仍为有限域中的元素。

目前研究的最多的是线性网络编码，线性网络编码具有运算简单、操作方便的特点，但也存在非线性网络编码。

线性网络编码的特点是编码与解码运算均是线性的，中间节点的编码运算结果是该节点接收到的信息的线性组合。

如图 1-5 所示，对于编码节点，它从 3 条输入链路上收到了 3 个消息 y_1、y_2、y_3，这 3 个消息看成同一集合上的 3 个元素，对这 3 个元素进行运算，把运算结果发送至输出链路上。

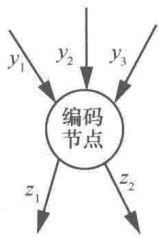


图 1-5　编码节点

$$\begin{cases} z_1 = f_1(y_1, y_2, y_3) \\ z_2 = f_2(y_1, y_2, y_3) \end{cases} \tag{1-1}$$

式（1-1）描述了中间节点的网络编码，节点输出信道上传输的信息是由该节点从输入信道接收到的信息通过运算所得的结果。

若 f_1 和 f_2 均为 y_1、y_2、y_3 的线性组合，则称为线性网络编码，否则称之为非线性网络编码。在式（1-2）中，系数 ξ_{ij}（i=1,2，j=1,2,3）为与信息字符 y_1、y_2、y_3 同属一个集合，属线性网络编码。

$$\begin{cases} z_1 = \xi_{11} y_1 + \xi_{12} y_2 + \xi_{13} y_3 \\ z_2 = \xi_{21} y_1 + \xi_{22} y_2 + \xi_{23} y_3 \end{cases} \tag{1-2}$$

$$\begin{cases} z_1 = y_1^2 + y_1 y_2 + y_2^2 \\ z_2 = y_1 + y_2 + y_1^2 \end{cases} \tag{1-3}$$

若编码如式（1-3）所示，则称为非线性网络编码。

关于非线性网络编码，作者认为可把分组加密算法的 Feistel 结构看成是由非

线网络编码形成的。

文献[21]给出的 Feistel 结构如图 1-6 所示。Feistel 结构采用乘积密码结构，首先把明文（假设为 $2n$ 位二进制数）等分成两部分，左边部分的 n 位记为 L_0，右边 n 位记为 R_0，然后进行 r 轮加密变换，对于第 i 轮加密变换，其变换公式如式（1-4）所示。经过 r 轮变换后，得到 L_r 和 R_r 为密文。

$$\begin{aligned} L_i &= R_{i-1} \\ R_i &= L_{i-1} \oplus F(R_{i-1}, K_i) \end{aligned} \tag{1-4}$$

以上操作可以看成是操作在一个有向无环网络上的从源点到宿点的网络编码运算，假设源点产生 $2n$ 位的信息，把信息划分成两部分，左 n 位和右 n 位，分别传输至后继节点，中间节点接收到信息后，进行编码运算再传输到下一节点，最后宿点接收到的信息就是密文。当 r=4 时，其网络编码的模型如图 1-7 所示。

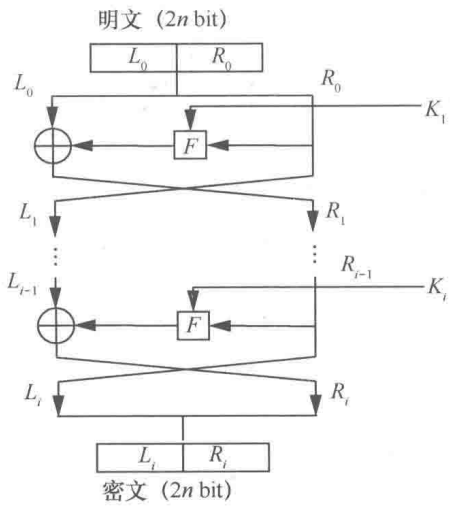


图 1-6　Feistel 结构

图 1-7 中有 10 个节点，其中源点 S 产生明文，宿点 T 得到密文。源点 S 分别通过其输出信道把 L_0 传输至节点 2，把 R_0 传输至节点 1，节点 1 接收到 R_0 后，一方面把 R_0 通过输出信道直接传输至节点 4，另一方面，节点 1 把 R_0 与节点本身产生的子密钥 K_1 进行运算，得到 $F(R_0, K_1)$ 并传输至节点 2；节点 2 从两条输入信道分别接收到信息是 L_0 与 $F(R_0, K_1)$，把两者进行异或运算后，把所得结果传输至节点 3，这样相当于进行了 Feistel 的第一轮加密运算；同理节点 3 和节点 4 把接收到的信息进行编码后再传输，相当于进行了 Feistel 的第二轮加密运算，以此类推，直至宿点 T 收到了 L_4 和 R_4 便形成了密文。假设 T 为宿点，宿点可以通过解码运算恢复出明文，相当于解码得到源点传输的消息。

从以上可以看出，非线性网络编码比线性网络编码更为复杂，其操作也没有