软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2011,22(3):558−571 [doi: 10.3724/SP.J.1001.2011.03737]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

线性网络编码的导出与扩展*

蒲保兴[1,2+], 杨路明[2], 王伟平[2]

[1](邵阳学院 信息工程系,湖南 邵阳 422001)

[2](中南大学 信息科学与工程学院,湖南 长沙 410083)

Generation and Extension of Linear Network Coding

PU Bao-Xing[1,2+], YANG Lu-Ming[2], WANG Wei-Ping[2]

[1](Department of Information Engineering, Shaoyang College, Shaoyang 422001, China)

[2](School of Information Science and Engineering, Central South University, Changsha 410083, China)

+ Corresponding author: E-mail: pubook@yahoo.com.cn

Pu BX, Yang LM, Wang WP. Generation and extension of linear network coding. *Journal of Software*, 2011, 22(3):558−571. http://www.jos.org.cn/1000-9825/3737.htm

Abstract: Aiming at a single-source multicast network, this paper studies the intrinsic mechanism of linear network coding and proposes a technique of generation and extension between two coding schemes at different multicast rates. The coding scheme is a generation of some coding schemes at higher multicast rate, and it is also an extension of some coding schemes at lower multicast rates. Furthermore, the determinate relationship among channels' global encoding vectors under two generation-extension coding schemes is discovered. By adopting random network coding, several important properties are derived, which are some of the application values and are helpful in implementing a single-source multicast connection with linear network coding. Several related applications are listed. In particular, this paper highlight a way to improve the throughput of single-source multicast network in dynamic environment and presents a random network coding approach based on retransmission and variable multicast rate, under the condition that each sink node has a feedback path to the source node. Compared with random network coding, this approach is a better way of improving the throughput of network. Simulation experiments of the listed applications have been done, and the results validate the conclusions derived from theoretical analyses.

Key words: single-source multicast network; random network coding; generation and extension of coding scheme; variable multicast rate; retransmission

摘 要: 针对单源组播网络,通过对线性网络编码的内在机理进行分析,提出了不同组播率下编码方案之间的导出与扩展技术:任意一个编码方案可以由某些较高组播率下的编码方案导出,同时可以由某些较低组播率下的编码方案扩展而成.研究了具有导出与扩展关系的两个编码方案下全局编码向量间的相互联系,结合随机网络编码方法,导出了几个重要的性质.这些性质有助于有效地运用线性网络编码技术实现单源组播连接,具有一定的应用价值.列出了几个方面的应用,着重讨论了在动态环境下如何提高单源组播连接的吞吐率问题,在宿点具有至源点反馈路径

* 基金项目: 国家自然科学基金(60673164, 60873265); 湖南省教育厅科研项目(06A065)
收稿时间: 2008-10-31; 修改时间: 2009-03-30; 定稿时间: 2009-08-31

的前提下,提出了一种基于重传与变组播率的随机网络编码方法.与随机网络编码方法相比,该方法能够提高网络的吞吐率.对列出的应用进行了仿真实验,结果验证了理论分析的结论.

关键词: 单源组播;随机网络编码;编码方案的导出与扩展;变组播率;重传

中图法分类号: TP393 **文献标识码**: A

网络编码[1−4]是一种新型的数据传输技术,与传统的路由技术相比,能提高网络的吞吐率、鲁棒性和安全性.Ahlswede 等人[1]首次提出了网络编码的概念,并指出:通过网络中间节点的编码可以实现单源组播网络的最大流界,而传统的路由技术在一般情况下不能达到这个极限.李硕彦等人[2]提出了线性网络编码技术,并证明了线性网络编码技术可以充分实现这一功能.Koetter 等人[3]给出了线性网络编码的代数框架.因线性网络编码具有简单的特点,从而得到了深入广泛地研究[4−8].

运用线性网络编码进行数据传输必须构造编码方案:确定源点的数据传输速率(组播率)和各信道的编码系数.已有文献主要针对同一组播率下的编码方案进行研究,而对不同组播率下编码方案之间的关系研究较少.针对网络拓扑已知的环境,文献[6]提出了确定性网络编码方法,运用网络的全局拓扑知识采用集中式的方法首先求出组播容量,再确定每一信道的编码系数,然后采用确定性网络编码传输方法传输数据,这是一种理想的数据传输方案.针对拓扑未知的环境,文献[8]提出了随机网络编码方法(random network coding,简称 RNC).

在实际应用中,运用线性网络编码技术会面临以下问题:1) 有时需要以不同的组播率进行数据传输,若采用已有的方法,则针对不同的组播率需要设计不同的编码方案,不仅增加了计算量,因编码节点需保存不同组播率下的编码系数,还占用了大量的存储空间;2) 尽管有文献[9,10]基于网络编码提出了分布式计算最小编码信道数的方法,在假定信道能反向传输数据的前提下,针对某一指定的可行组播率(不超过组播容量),采用启发式方法与 RNC 相结合的策略,给出了计算满足指定组播率条件下网络所需的最小编码信道数的方法,但必须事先给定一个可行的组播率,且只能求出最小编码信道数而不能构造相应的编码方案;3) 文献[11]研究了网络编码的最小花费问题,在一定的假设条件下给出了一个分布式求解方法,但需同样假定组播容量是已知的;4) 文献[12,13]研究了动态网络拓扑环境下的线性网络编码问题,均假定组播容量是已知且不变的.而在实际应用中,若源点缺乏全局网络拓扑知识,获知网络的组播容量是一件困难的事情,从而选定一个可行的组播率也是困难的;此外,在数据传输过程中,因接收点的随机加入或离开,节点或链路的失效会造成网络拓扑随时间动态变化,从而导致了组播容量的变化.为使网络吞吐率尽可能地大,组播率应与组播容量相等.因此,在数据传输过程中需要动态地测试组播容量,以便动态地更改组播率.

针对单源组播网络,通过对线性网络编码的内在机理进行分析,提出了不同组播率下编码方案的导出与扩展技术:一个组播率为 h 的编码方案能够导出一个组播率为 $k(2\leqslant k\leqslant h)$ 的编码方案,而后者仅在源点输出信道的编码系数略有不同;而一个组播率为 k 的编码方案通过扩展源点输出信道的编码系数,便可以得到一个组播率为 h 的编码方案.运用线性代数的相关理论对互为导出与扩展的两个编码方案进行研究,我们发现,信道的全局编码向量具有确定的关系.运用这一关系,结合 RNC,推导出了几个重要的性质.这些性质对于运用线性网络编码技术具有一定的实用价值,能够有效地解决以下问题:不同组播率下的编码方案可共享编码系数,而不需重新构造编码方案;可以在线测试组播容量,且能把测试组播容量嵌入到数据传输过程中,而不会中断数据传输;能在线构造确定的编码方案.本文列出了几个方面的应用,特别针对网络拓扑动态变化的单源组播网络进行了重点研究,在假定宿点能反馈信息至源点的条件下,提出了基于重传与变组播率的随机网络编码方法(random network coding based on retransmission and variable multicast rate,简称 RNC-RVMR).在数据传输过程中动态测试组播容量并调整组播率,以适应网络拓扑的变化.该方法与 RNC 相比可以提高网络的吞吐率.我们对列出的应用进行了仿真实验,结果验证了理论分析的结论.

1 相关知识

以下根据文献[5]来叙述线性网络编码的相关定义.一个单源组播网络用有向无环多重图 $G=(V,E)$ 表示,其

中,V 为节点集,E 为有向边集,$T\subset V$ 代表宿点集,$s\in V$ 是源点.为讨论方便,限定链路的容量为整数.若网络节点之间存在容量大于 1 的有向链路,把它分成多条有向边.有向边 $e=(u,v)\in E$ 代表节点 u 至节点 v 的单位容量的有向信道,其中:u 称为 e 的始点,记为 $u=tail(e)$;v 称为 e 的终点,记为 $v=head(e)$.记 $In(v)=\{d\in E:head(d)=v\}$为 v 的输入信道集合,记 $Out(u)=\{e\in E:tail(e)=u\}$为 u 的输出信道集合.

定义 1(组播率和组播容量). 单源组播网络的组播率是指源点的数据传输速率,记为 h;组播容量记为 C,等于源点与所有宿点之间的最小割值[1].

线性网络编码操作在有限域(也称为伽罗华域)上,本文采用伽罗华域 $GF(2^m)$[14],信息的编码操作对应于伽罗华域上的字符运算.在单位时间内,假设源点播出的信息字符为 $x_1,x_2,\ldots,x_h$,每一字符均为 m 比特,属于 $GF(2^m)$上的字符.信道 $e\in E$ 传输的信息记为 $y(e)$,也属于 $GF(2^m)$上的字符.

定义 2(局部编码向量). 采用线性网络编码,每一节点的输出信道 e 传输的信息是该节点所有输入信道传输信息的线性组合.这个线性组合的系数构成该信道的局部编码向量,记为 $\boldsymbol{m}(e)$.则有:

$$\boldsymbol{m}(e)=\{m_{d,e}\in GF(2^m):d\in In(tail(e))\} \tag{1}$$

$$y(e)=\sum_{d\in In(tail(e))} m_{d,e}y(d) \tag{2}$$

定义 3(全局编码向量和全局编码矩阵). 若采用线性网络编码以组播率 h 传输数据,每一信道 e 传输的信息均可以表示为源点播出信息 $x_1,x_2,\ldots,x_h$ 的线性组合,这个线性组合的系数构成一个向量,记为 $\boldsymbol{g}(e)=(g_{e,1},g_{e,2},\ldots,g_{e,h})$,则

$$y(e)=\sum_{i=1}^{h} g_{e,i}x_i \tag{3}$$

$$\boldsymbol{g}(e)=\sum_{d\in In(tail(e))} m_{d,e}\boldsymbol{g}(d) \tag{4}$$

对于任意节点 $v\in V$,该节点所有输入信道的全局编码向量构成了一个$|In(v)|$行、h 列的矩阵,称为该节点的全局编码矩阵,记为 $\boldsymbol{M}_v$,每一信道的全局编码向量构成矩阵的一个行向量(注:$|\cdot|$为集合的元素个数或向量的分量个数,以下同).由公式(3),宿点可以通过其全局编码矩阵和接收到的信息字符形成一个线性方程组,只有当该线性方程组的系数矩阵的秩等于组播率 h,宿点才能恢复出源点的信息.

由公式(4),不难得出 $\boldsymbol{g}(e)=\boldsymbol{m}(e)\boldsymbol{M}_v$(这里是一个 1 行、$|In(v)|$列的矩阵和一个$|In(v)|$行、$h$ 列矩阵的乘积).

定义 4(编码方案). 单源组播网络以组播率 h 采用线性网络编码进行数据传输,各信道的局部编码向量的集合称为一个组播率为 h 的编码方案.在该编码方案下,若所有宿点的全局编码矩阵的秩均为 h,则称为一个可行编码方案.

一个编码方案不一定是可行的,其最大组播率为 $H=|Out(s)|$;若是可行的,其组播率不能超过组播容量[2].

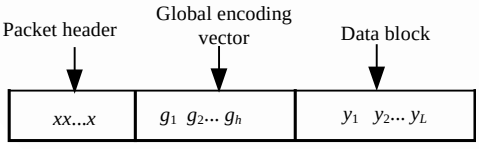

Fig.1 Structure of a data packet with RNC

图 1 随机线性网络编码的数据包格式

文献[8]提出了 RNC,与确定性网络编码方法[6]相比,该方法不需要获知全局网络拓扑知识.它在数据传输过程中随机地产生编码系数,即所有编码节点为其输出信道随机生成局部编码向量,为使宿点实现解码.每一编码节点不仅需要进行信息编码运算,同时还需要计算输出信道的全局编码向量,且把全局编码向量与传输的信息以数据包形式沿输出信道传输至下游节点.根据文献[5],若组播率为 h,则信道上传输的数据包的格式如图 1 所示.

L 称为数据块的长度,在一批数据传输叶,源点播出了 hL 个字符.一般来说,源点需播出的信息量远远超过这个数,因而需要进行若干批数据传输才能完成整个数据传输任务.

2 线性网络编码方案的导出与扩展

以下提出了不同组播率下线性网络编码的导出与扩展技术.对于一个单源组播网络 G,在选定了伽罗华域

$GF(2^m)$的前提下,构造一个单源组播网络的编码方案需要确定组播率 h 和各信道的局部编码向量.由定义 4,一个单源组播网络的网络编码方案是所有信道的局部编码向量的集合,在本文中,用ξ,ψ,ζ等符号表示编码方案(编码方案是各信道的局部编码向量的集合,则这里的ξ,ψ,ζ表示集合变量).因每一编码方案必须对应于一个确定的组播率,则需要研究不同组播率下的编码方案之间的关系.

定义 5. 一个编码方案ξ对应的组播率记为$\delta(\xi)$;在编码方案ξ下,对于信道 $e\in E$,其局部编码向量记为 $\boldsymbol{m}(e,\xi)$,全局编码向量记为 $\boldsymbol{g}(e,\xi)$;节点 v 的全局编码矩阵记为 $\boldsymbol{M}(v,\xi)$.

由定义 2 和定义 3,在编码方案ξ下,信道 e 的局部编码向量的维数为$|In(tail(e))|$,全局编码向量的维数为$\delta(\xi)$.

对于编码方案ξ,不妨记其组播率为 $h(h=\delta(\xi))$,源点相当于具有 h 条虚拟输入信道,它们把要传输的 h 个字符以及 h 维向量空间上的 h 个单位向量分别注入至源点,则对于源点的输出信道,其局部编码向量的维数也是 h,且全局编码向量与局部编码向量相等.而其余信道的局部编码向量的维数与组播率 h 无关,即

$$|\boldsymbol{m}(e,\xi)|=\begin{cases}|In(tail(e))|, & 若e\notin Out(s)\\ h, & 若e\in Out(s)\end{cases} \tag{5}$$

由公式(5),组播率为 h 的编码方案ξ包含了组播率为 $k(2\leqslant k\leqslant h)$的编码方案(指在同一伽罗华域下,下同).

定义 6(线性网络编码方案的导出与扩展). 对于一个编码方案ξ,其组播率$\delta(\xi)$记为 h,则称由公式(6)确定的一个编码方案ζ(其组播率$\delta(\zeta)$记 $k(2\leqslant k\leqslant h)$)是由$\xi$导出的,称$\xi$是由$\zeta$扩展而成,并称$\xi$和$\zeta$具有导出与扩展关系.

$$\zeta=\{\boldsymbol{m}(e,\zeta):e\in E\ 且\ \boldsymbol{m}(e,\zeta)满足公式(7)\} \tag{6}$$

$$\boldsymbol{m}(e,\zeta)=\begin{cases}由\ \boldsymbol{m}(e,\xi)的前k个分量构成, & e\in Out(s)\\ \boldsymbol{m}(e,\xi), & e\notin Out(s)\end{cases} \tag{7}$$

公式(7)的含义为:当 e 为源点 s 的输出信道时,则信道 e 在编码方案ζ下的局部编码向量由在编码方案ξ下的局部编码向量的前 k 个分量构成;对于其他信道,在ζ下的局部编码向量与ξ下的局部编码向量相同.例如,图 2 中的ζ是由ξ导出的.

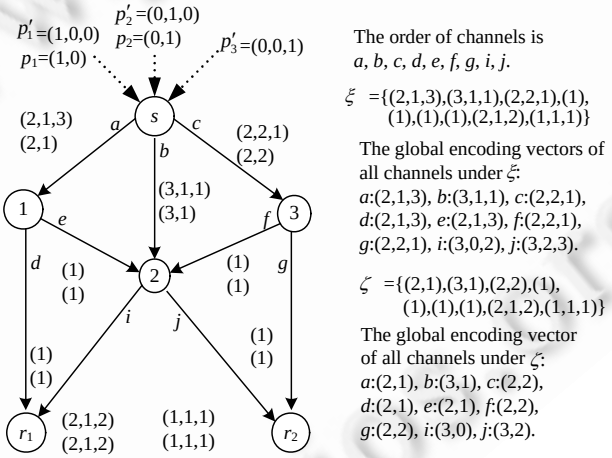

Fig.2 An illustration for generation and extension of coding schemes

图 2 编码方案的导出与扩展示意图

从定义 6 可知,对于一个组播率为 k 的编码方案,只要对源点输出信道的局部编码向量进行扩展,在每一个局部编码向量尾部添加 $h-k$ 个分量,构成维数为 h 的向量,而对于其他信道保持其局部编码向量不变,则形成了一个组播率为 h 的编码方案.

定理 1. 对于一个组播率为 $k(2\leqslant k)$的编码方案,可以由某一个组播率为 $h(k\leqslant h)$的编码方案导出;反之,一个组播率为 h 的编码方案可以由某一个组播率为 k 的编码方案扩展而成.

定理 1 可以根据定义 6 推出,显然成立.

3 几个重要性质

对于具有导出与扩展关系的两个编码方案,分别记为ξ和ζ,其组播率分别为 h 和 k.在这两个编码方案下,每一信道的全局编码向量可以唯一确定.对于同一信道,它们在这两个编码方案下的全局编码向量分别为 $\boldsymbol{g}(e,\xi)$ 和 $\boldsymbol{g}(e,\zeta)$.那么这两个向量具有什么关系?以下讨论这个问题.

定理 2. 设有两个整数 k 和 h,且满足 $2\leqslant k\leqslant h$.ξ是某一个编码方案,且$\delta(\xi)=h$;ζ是由ξ导出的编码方案,且$\delta(\zeta)=k$.则在两个编码方案下,对于任意信道 $e\in E$,它的全局编码向量具有以下关系:$\boldsymbol{g}(e,\zeta)$的 k 个分量与 $\boldsymbol{g}(e,\xi)$的前 k 个分量对应相同.即,若 $\boldsymbol{g}(e,\xi)=(g_1,g_2,\ldots,g_k,g_{k+1},\ldots,g_h)$,则 $\boldsymbol{g}(e,\zeta)=(g_1,g_2,\ldots,g_k)$.

证明:采用归纳法.

1) 当 $e\in Out(s)$时,由上所述,源点输出信道的局部编码向量与全局编码向量相等,则有 $\boldsymbol{g}(e,\zeta)=\boldsymbol{m}(e,\zeta)$,$\boldsymbol{g}(e,\xi)=\boldsymbol{m}(e,\xi)$成立.根据定义 6,结论成立.

2) 假设对于编码节点 $v(v\neq s)$,若 $d\in In(v)$时结论成立,即 $\boldsymbol{g}(d,\xi)=(\boldsymbol{g}(d,\zeta)\boldsymbol{g}')$.其中,$\boldsymbol{g}'$是一个含有 $h-k$ 个分量的向量**.不妨记节点 v 的输入信道分别为 $d_1,d_2,\ldots,d_{|In(v)|}$,并注意到定义 3,节点的全局编码矩阵是由其输入信道的全局编码向量组成,则

$$\boldsymbol{M}(v,\zeta)=\begin{pmatrix}\boldsymbol{g}(d_1,\zeta)\\ \boldsymbol{g}(d_2,\zeta)\\ \vdots\\ \boldsymbol{g}(d_{|In(v)|},\zeta)\end{pmatrix} \tag{8}$$

$$\boldsymbol{M}(v,\xi)=\begin{pmatrix}\boldsymbol{g}(d_1,\xi)\\ \boldsymbol{g}(d_2,\xi)\\ \vdots\\ \boldsymbol{g}(d_{|In(v)|},\xi)\end{pmatrix}=(\boldsymbol{M}(v,\zeta)\boldsymbol{M}') \tag{9}$$

其中,$\boldsymbol{M}'$是一个$|In(v)|$行、$h-k$ 列的矩阵.

因ζ是由ξ导出的,对于 $e\in Out(v)$,由定义 6 有 $\boldsymbol{m}(e,\zeta)=\boldsymbol{m}(e,\xi)$.

假定 $\boldsymbol{m}(e,\zeta)=(m_1,m_2,\ldots,m_{|In(v)|})$,再根据公式(4),则

$$\boldsymbol{g}(e,\zeta)=\boldsymbol{m}(e,\zeta)\boldsymbol{M}(v,\zeta)=(m_1\ldots m_{|In(v)|})\begin{pmatrix}\boldsymbol{g}(d_1,\zeta)\\ \boldsymbol{g}(d_2,\zeta)\\ \vdots\\ \boldsymbol{g}(d_{|In(v)|},\zeta)\end{pmatrix} \tag{10}$$

$$\boldsymbol{g}(e,\xi)=\boldsymbol{m}(e,\xi)\boldsymbol{M}(v,\xi)=(m_1\ldots m_{|In(v)|})\begin{pmatrix}\boldsymbol{g}(d_1,\xi)\\ \boldsymbol{g}(d_2,\xi)\\ \vdots\\ \boldsymbol{g}(d_{|In(v)|},\xi)\end{pmatrix} \tag{11}$$

结合公式(8)~公式(11),并根据分块矩阵相乘的性质,得出

$$\boldsymbol{g}(e,\xi)=\boldsymbol{m}(e,\xi)\boldsymbol{M}(v,\xi)=\boldsymbol{m}(e,\zeta)(\boldsymbol{M}(v,\zeta)\boldsymbol{M}')=(\boldsymbol{g}(e,\zeta)\boldsymbol{m}(e,\zeta)\boldsymbol{M}').$$

因此,$\boldsymbol{g}(e,\xi)$写成了两部分:前一部分就是 $\boldsymbol{g}(e,\zeta)$,共有 k 个分量;后一部分由 $\boldsymbol{m}(e,\zeta)\boldsymbol{M}'$求出,共有 $h-k$ 个分量.从而说明了对于节点 v 的输出信道,结论也成立.

上面说明了这样一个事实:定理的结论对于源点输出信道的全局编码向量是成立的.而对于非源点的节点,只要定理的结论对于输入信道的全局编码向量是成立的,则定理的结论对其输出信道的全局编码向量必定是

** 这里把向量写成了矩阵形式,并利用了矩阵分块的概念:把一个 h 维的向量看成是一个 1 行 h 列的矩阵.例如,(1,2,3,4)=(1 2 3 4)=((1 2) (3 4)).

成立的.

因单源组播网络是一个有向无环图,所有的节点存在一个偏序,按照这个偏序反复使用公式(4),则可以把所有信道的全局编码向量求出.由归纳法原理,结论成立.证毕. □

图 2 给出了定理 2 的一个示例.在图 2 中,各链路的容量均为 1,s 为源点,r_1 和 r_2 为宿点.ξ是一个组播率为 3 的编码方案,而ζ是由ξ导出且组播率为 2 的编码方案.采用的伽罗华域为 $GF(2^2)$,其生成多项式为 x^2+x+1.分别在两个编码方案下采用公式(4)计算信道的全局编码向量,所得结果如图 2 所示.为书写方便,各分量写成 4 进制形式,显然满足定理 2 的结论.

节点 v 的全局编码矩阵 $\boldsymbol{M}(v,\xi)$是一个$|In(v)|$行、h 列的矩阵,若选取该矩阵的前 k 列,则可构成一个$|In(v)|$行、k 列的矩阵.

定义 7($\boldsymbol{N}(\boldsymbol{A},k)$). 设 $\boldsymbol{A}$ 是一个矩阵,而 k 是一个不超过矩阵 $\boldsymbol{A}$ 的列数的正整数,记 $\boldsymbol{N}(\boldsymbol{A},k)$是由矩阵 $\boldsymbol{A}$ 的前 k 列构成的矩阵.

$\boldsymbol{N}(\boldsymbol{A},k)$是一个这样的矩阵,其行数与 $\boldsymbol{A}$ 的行数相同,列数为 k.

推论 1. 若ξ是组播率为 h 的一个编码方案,而ζ是由ξ导出且组播率为 k 的编码方案,则对于任一节点 $v\in T$,在编码方案ζ下的全局编码矩阵是由在编码方案ξ下的全局编码矩阵的前 k 列组成,即

$$\boldsymbol{M}(v,\zeta)=\boldsymbol{N}(\boldsymbol{M}(v,\xi),k) \tag{12}$$

证明:由定理 2,并根据定义 3,节点的全局编码矩阵由其输入信道的全局编码向量组成,每一个向量组成了矩阵的一行,显然结论成立.证毕. □

推论 2. 若ξ是组播率为 h 的一个编码方案,而ζ是由ξ导出且组播率为 k 的编码方案,则ζ是可行编码方案的充分必要条件是,对于每一个宿点 $r\in T$,有 $rank(\boldsymbol{N}(\boldsymbol{M}(r,\xi),k))=k$.其中,$rank(\cdot)$表示矩阵的秩.

证明:根据推论 1,对于每一宿点 $r\in T$,它在编码方案ζ下的全局编码矩阵为 $\boldsymbol{N}(\boldsymbol{M}(v,\xi),k)$,即 $\boldsymbol{M}(r,\zeta)=\boldsymbol{N}(\boldsymbol{M}(r,\xi),k)$,再根据定义 4,结论成立.证毕. □

性质 1. 若ξ是一个组播率为 h 的可行编码方案,且 $2\leqslant k\leqslant h$,则由ξ导出且组播率为 k 的编码方案ζ必定是可行的.

证明:因ξ是可行的,从而任一宿点 $r\in T$ 在ξ下的全局编码矩阵的秩为 h,即 $rank(\boldsymbol{M}(r,\xi))=h$ 成立.注意到这个矩阵只有 h 列,且矩阵的行数不小于 h,从而这个矩阵的 h 个列向量必定线性无关.那么,该矩阵的前 k 个列向量必定线性无关,由这个矩阵的前 k 列构成的矩阵其秩必为 k,即 $rank(\boldsymbol{N}(\boldsymbol{M}(v,\xi),k))=k$ 成立.再由推论 1,则任一宿点在编码方案ζ下的全局编码矩阵的秩必为 k,由推论 2,结论成立.证毕. □

源点 s 能获知其输出信道数 $H=|Out(s)|$,记 $Vs=\{s\}$,则 $\langle Vs,\overline{Vs}\rangle$ 是分离源点 s 与所有宿点的一个割集,其割值为 H,记 C 为组播容量.由定义 1,则有 $C\leqslant H$.从而,H 为源点选定组播率提供了一个上界.

在单组播网络中,让 $\max flow(s,r)$为分离源点 s 与宿点 r 的最小割值.在单源组播网络中,若以组播率 H 采用随机网络编码方法组播数据至所有宿点,相当于随机构造了一个组播率为 H 的编码方案.不妨记其编码方案为 ψ,且满足$\delta(\psi)=H$.

引理 1. 设ψ是一个组播率为 H 的编码方案,则在编码方案ψ下,每一宿点 $r\in T$ 的全局编码矩阵的秩不会超过 $\max flow(s,r)$,即

$$rank(\boldsymbol{M}(r,\psi))\leqslant \max flow(s,r), r\in T \tag{13}$$

证明:由最大流-最小割定理,对于宿点 $r\in T$,必存在一个分离源点 s 与宿点 r 的最小割,该割中有且只有 $\max flow(s,r)$条信道,这 $\max flow(s,r)$条信道携带的全局编码向量张成了 H 维向量空间的一个子空间,该子空间的秩不超过 $\max flow(s,r)$.由线性网络编码的特点[2],宿点 r 的每一输入信道的全局编码向量一定可以表示成这个最小割中的信道所携带的全局编码向量的线性组合.由线性代数知识,宿点 r 的全局编码矩阵的秩不能超过 $\max flow(s,r)$,不等式(13)成立.证毕. □

在不等式(13)两边取最小值,再由定义 1,则下式成立:

$$\min_{r\in T}\{rank(\boldsymbol{M}(r,\psi)\}\leqslant \min_{r\in T}\{\max flow(s,r)\}=C \tag{14}$$

文献[8]指出:在单源组播网络中以组播率 C 采用 RNC 组播数据,且采用的伽罗华域的阶为 $q(q>|T|,|T|$为宿点个数),则所有宿点全局编码矩阵的秩均为 C 的概率大于 0.当伽罗华域的阶足够大时,这个概率接近于 1,不妨记这个概率为 P_q.注意到当所有宿点的全局编码矩阵的秩为 C 时,则对应一个组播率为 C 的可行编码方案.由于RNC产生的编码系数在伽罗华域上是均匀和随机的,从而以组播率为 C 采用RNC进行数据传输,相当从组播率为 C 的所有编码方案中随机地选择了一个编码方案,该编码方案是可行的概率为 P_q.

定理 3. 在单源组播网络中以组播率 H 采用 RNC 组播数据,且采用的伽罗华域的阶为 $q(q>|T|)$.记相应的编码方案为 ψ,宿点 $r\in T$ 的全局编码矩阵的前 C 列构成的矩阵记为 $\boldsymbol{N}(\boldsymbol{M}(r,\psi),C)$,则对于所有宿点 r,矩阵 $\boldsymbol{N}(\boldsymbol{M}(r,\psi),C)$的秩等于 C 的概率为 P_q,即

$$P_r\left\{\psi:\underset{r\in T}{\wedge}(rank(N(M(r,\psi),C))=C)\right\}=P_q \tag{15}$$

其中,$P_r(\cdot)$表示概率,$\wedge$表示逻辑与.

证明:在其阶为 q 的伽罗华域下,不妨假设有 α 个组播率为 C 的编码方案,其中有 β 个是可行的.注意到随机产生一个组播率为 C 的编码方案,相当于在 α 个组播率为 C 的编码方案中均匀随机地选择一个,那么其选中的编码方案为可行的概率为 β/α.如上所述,采用 RNC 组播数据至网络,相当于随机生成了一个编码方案,则 $P_q=\beta/\alpha$.再注意到 $C\leqslant H$,并由定理 1:每一个组播率为 C 的编码方案均可以由某一个组播率为 H 的编码方案导出,每一个组播率为 H 的编码方案均可以由某一个组播率为 C 的编码方案扩展而成.则对组播率为 C 的编码方案,只需对源点输出信道的局部编码向量进行扩展,每一向量扩展 $H–C$ 个分量,便构成了组播率为 H 的编码方案.注意到源点有 H 条输出信道,在对组播率为 C 的编码方案扩展至组播率为 H 的编码方案时,源点每一输出信道的局部编码向量扩展了 $H–C$ 个分量,则组播率为 H 的编码方案比组播率为 C 的编码方案多了 $H(H–C)$个分量,由 RNC 在 q 阶伽罗华域上取各分量值的均匀性和随机性,再根据乘法原理,则组播率为 H 的编码方案数为 $\alpha q^{H(H-C)}$,其中有 $\beta q^{H(H-C)}$个编码方案是由组播率为 C 的可行编码方案扩展而成的,因而随机构造一个组播率为 H 的编码方案,它是由组播率为 C 的可行编码方案扩展而成的概率为 P_q.由推论 2,结论成立.证毕. □

性质 2. 对于单源组播网络,以组播率 H 采用 RNC 传输数据,不妨记其编码方案为 ψ,则宿点 $r\in T$ 接收到所有的数据包后,析出全局编码矩阵,并按公式(16)计算 $\chi(r,\psi)$,源点按公式(17)计算 $\sigma(\psi)$,则:

1) $\sigma(\psi)$不超过 C;

2) 当采用的伽罗华域足够大时,$\sigma(\psi)=C$ 的概率接近于 1.

$$\chi(r,\psi)=\max_{1\leqslant h\leqslant H}\{h:rank(\boldsymbol{N}(\boldsymbol{M}(r,\psi),h))=h\} \tag{16}$$

$$\sigma(\psi)=\min_{r\in T}\{\chi(r,\psi)\} \tag{17}$$

证明:根据定义 7,对于任一宿点 $r\in T$,$\boldsymbol{N}(\boldsymbol{M}(r,\psi),h)$是由 $\boldsymbol{M}(r,\psi)$前 h 列构成的矩阵.由矩阵的性质,当 $h\leqslant H$ 时,必有

$$rank(\boldsymbol{N}(\boldsymbol{M}(r,\psi),h))\leqslant rank(\boldsymbol{M}(r,\psi))$$

成立,再根据公式(16),从而有

$$\chi(r,\psi)=\max\{h:rank(\boldsymbol{N}(\boldsymbol{M}(r,\psi),h))=h\}\leqslant rank(\boldsymbol{M}(r,\psi))$$

成立,对上式的两端取最小值,有

$$\min_{r\in T}\{\chi(r,\psi)\}\leqslant\min_{r\in T}\{rank(\boldsymbol{M}(r,\psi))\}$$

成立,再根据公式(14)、公式(17),必定有 $\sigma(\psi)\leqslant C$,从而上面的结论 1)成立.

又根据定理 3,则 $\sigma(\psi)\geqslant C$ 的概率为 P_q,从而当伽罗华域较大时,$\sigma(\psi)=C$ 的概率接近于 1.证毕. □

显然,由公式(17)求出的 $\sigma(\psi)$是一个整数,且对于任一宿点 r,有 $\sigma(\psi)\leqslant\chi(r,\psi)$.而由公式(16),$\boldsymbol{M}(r,\psi)$的前 $\chi(r,\psi)$列构成的矩阵其秩必为 $\chi(r,\psi)$,则 $\boldsymbol{M}(r,\psi)$的前 $\sigma(\psi)$列构成的矩阵其秩必为 $\sigma(\psi)$,从而可从 ψ中导出一个组播率为 $\sigma(\psi)$的可行编码方案.

公式(16)的含义是:对于任一宿点 r,寻找一个最大的 h,且满足全局编码矩阵 $\boldsymbol{M}(r,\psi)$的前 h 列构成的矩阵的秩为 h.可以通过对矩阵 $\boldsymbol{M}(r,\psi)$作行初等变换,把矩阵化为上三角形式来计算公式(16),限于篇幅,不作详细讨论.

若取整数 k,且满足$\sigma(\psi)<k\leqslant H$,由公式(17),则必存在一个宿点 r',有 $k>\chi(r',\psi)$,即 $\boldsymbol{M}(r',\psi)$的前 k 列构成的矩阵其秩小于 k.由推论 2,则由编码方案ψ导出的一个组播率为 k 的编码方案必定是不可行的.因此,$\sigma(\psi)$是所有从ψ中导出的可行编码方案的最大组播率.从而以下定理显然成立.

定理 4. 对于一个组播率为 H 的编码方案ψ,按公式(17)计算$\sigma(\psi)$,则可以从ψ中导出一个组播率为$\sigma(\psi)$的可行编码方案,且$\sigma(\psi)$是所有从ψ中导出的可行编码方案的最大组播率.

4 应 用

以上定理、推论与性质有助于有效地运用线性网络编码技术,具有一定的实用价值,以下列举几个应用.

4.1 不同组播率下编码系数的共享

由性质 1,若单源组播网络具有一个组播率为 h 的可行编码方案,则可以任意选择组播率 $k(2\leqslant k\leqslant h)$进行数据传输,而不用重新构造编码方案.

记原有可行编码方案为ξ,其组播率为$\delta(\xi)=h$,若采用组播率 k 进行数据传输,则可以采用ξ的导出编码方案.由性质 1,ξ的导出编码方案必定是可行的.在组播率为 k 的导出编码方案下,源点输出信道的局部编码向量取其在ξ下的局部编码向量的前 k 个分量,而其余信道的局部编码向量保持不变,从而各节点只要保存组播率为 h 的可行编码方案的编码系数,便可以采用组播率 k 进行数据传输.

4.2 测试组播容量及构造编码方案

性质 2 提供了一个测试组播容量的方法.因源点能够获知其输出信道数 H,则能以组播率 H 采用 RNC 组播实验包至所有宿点,由于仅关心宿点的全局编码矩阵,则数据块可以为空,实验包的格式如图 3 所示.

若以组播率为 H 采用 RNC 组播实验包至网络,相当于随机产生了一个编码方案,不妨记为 ψ(其中,$\delta(\psi)=H$).所有宿点只需按公式(16)计算$\chi(r,\psi)$,源点按公式(17)计算$\sigma(\psi)$,则由定理 3 和性质 2,当伽罗华域较大时,$\sigma(\psi)=C$ 的概率为 P_q 且接近于 1.把一次传输实验包的过程称为一次测试,为确保测试出组播容量,对于网络拓扑不变的环境可以采用蒙托卡罗法进行多次测试.在多次测试中,记录最好的测试结果,因每次测试均为独立随机的实验,相当于进行贝努里实验.若进行 n 次测试,则能测试出组播容量的概率为 $1-(1-P_q)^n$.显然,当采用的伽罗华域较大且测试次数较多时,能测试出组播容量是一个大概率事件.这一策略还可以用于构造编码方案,只需在测试过程中各节点保存$\sigma(\psi)$值最大时对应的编码系数,则在测试出组播容量 C 的同时,可以从中导出组播率为 C 的编码方案,则构造出了组播率为 C 的可行编码方案.与文献[6]提出的确定性网络编码方法相比,该方法具有操作简单的特点.

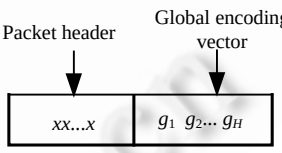

Fig.3 Structure of a trial packet
图 3 实验包的结构

对于静态网络(网络拓扑在完成整个数据传输任务的过程中不会发生变化),若所有宿点能反馈信息至源点,则可以在线测试组播容量并构造出确定的网络编码方案,且各编码系数保存在相应的节点中,从而可以采用确定的网络编码数据传输策略传输数据.

4.3 动态环境下单源组播网络编码数据传输策略

在实际应用中,对单源组播网络来说,一方面源点很难获知全局网络拓扑信息;另一方面,因链路失效,或者因存在多个数据传输任务而相互竞争网络资源,从而实现同一传输任务的网络拓扑是动态变化的.此外,对于某些单源组播传输任务来说,宿点要求完整、正确地接收源点播出的信息.

假设源点不能获知整个网络的全局拓扑知识,每一宿点存在至源点的反馈路径,通过该路径可以反馈信息至源点;每一节点具有足够的存储空间以保存相应的信息,并具有任一阶伽罗华域的计算能力;在整个数据传输过程中,网络拓扑会发生变化;信道是无错的.即,信道要么传输信息正确;要么信道无效,不传输任何信息.我们的目标是,设计一个有效的网络编码数据传输策略,使网络的吞吐率尽可能地大,并使所有宿点能够完整、正确地接收源点播出的信息.

针对这类问题,源点选取合适的组播率进行网络编码数据传输,是提高吞吐率的关键,只有当组播率不超过且接近组播容量时,才能使网络的吞吐率较大.若组播率大于组播容量,必定会有宿点不能恢复出源点的信息;若组播率小于组播容量,则浪费了网络资源.因网络拓扑未知,显然不能采用确定性网络编码传输策略,也不能单纯地采用RNC,因为采用RNC的前提是必须事先确定组播率.我们利用线性网络编码的导出与扩展技术提出了 RNC-RVMR,利用宿点能反馈信息至源点的特性,采用重传和在数据传输过程中测试组播容量相结合的策略,动态地更改组播率并重传宿点不能解码的信息.

RNC-RVMR 的基本思想是:采用 RNC 同时实现两个组播率 H 与 h 的数据传输,以组播率为 H 的编码方案测试组播容量,因测试组播容量仅关心宿点的全局编码矩阵的秩,从而只需传输全局编码向量,不用传输数据;以组播率为 h 的编码方案实现数据传输.因此在一次数据传输过程中,相当于随机产生了两个编码方案 ψ 和 ξ,其中,$\delta(\psi)=H,\delta(\xi)=h$,且 ξ 是由 ψ 导出的编码方案.信道上传输的数据包格式如图 4 所示.

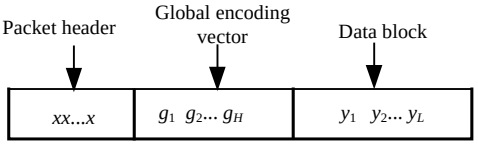

Fig.4 Structure of data packet of RNC-RVMR

图 4 RNC-RVMR 的数据包格式

实施方法如下:源点相当于具有 H 条虚拟输入信道,它们分别注入 H 维向量空间的单位向量至源点 s,记为 $\boldsymbol{p}_1,\boldsymbol{p}_2,\ldots,\boldsymbol{p}_H$,前 h 条虚拟输入信道分别把要发送的字符注入至源点 s,记为 $x_1,x_2,\ldots,x_h$,如图 5 所示.图 5 表示一个动态环境下的单源组播网络在静态时的拓扑结构,其中,s 是源点,r_1~r_5 均为宿点,其余为中间节点,源点需组播数据至所有的宿点.

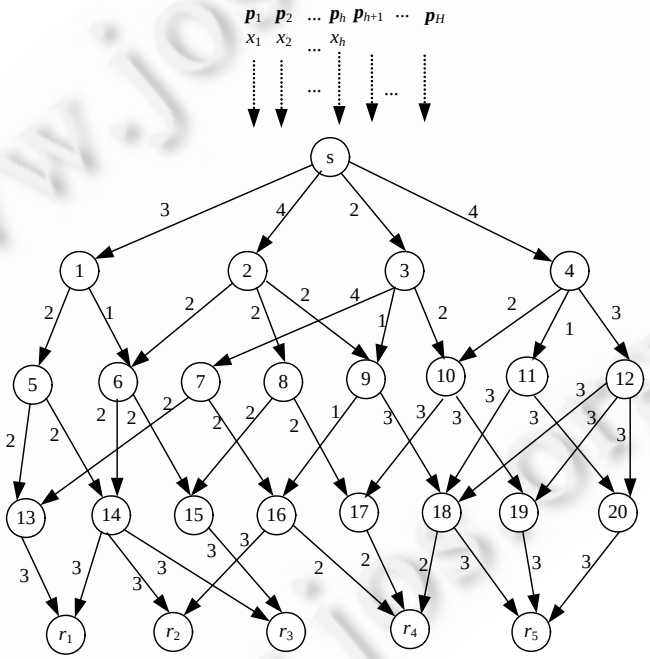

Fig.5 Vectors and characters injected by the imaginary incoming channels of the source node

图 5 源点虚拟输入信道注入的向量与字符

对于源点 s 的输出信道 $e\in Out(s)$,其局部编码向量 $\boldsymbol{m}(e)$ 是一个 H 维的向量,设 $\boldsymbol{m}(e)=(m_{e,1},\ldots,m_{e,H})$,各分量由源点随机产生,则信道 e 传输的全局编码向量与字符分别按公式(18)和公式(19)计算.

$$\boldsymbol{g}(e)=\sum_{i=1}^{H}m_{e,i}\boldsymbol{p}_i=\boldsymbol{m}(e) \tag{18}$$

$$y(e)=\sum_{i=1}^{h}m_{e,i}x_i \tag{19}$$

若 $e\in Out(v)(v\neq s)$,其局部编码向量见公式(1),各分量由节点 v 随机产生,信道 e 传输的全局编码向量和字符分别按公式(4)和公式(2)计算.

宿点接收到所有的数据包后,从中析出全局编码矩阵 $\boldsymbol{M}(r,\psi)$.注意到 $\boldsymbol{M}(r,\psi)$是一个$|In(r)|$行、H 列的矩阵,由推论 1,该矩阵的前 h 列恰好是宿点在编码方案ξ下的全局编码矩阵,记为 $\boldsymbol{M}(r,\xi)$.若 $\boldsymbol{M}(r,\xi)$的秩为 h,则利用$\boldsymbol{M}(r,\xi)$来进行解码,否则不能解码.宿点再按公式(16)计算$\chi(r,\psi)$,然后把是否能解码的信息和$\chi(r,\psi)$的值通过反馈路径发送至源点.

源点在收到了所有宿点的反馈信息后,首先判断是否需要重传,只要存在一个宿点不能解码,则源点以相同的组播率重传该批信息,否则进行下一批数据传输.在进行下一批数据传输前,源点按公式(17)计算$\sigma(\psi)$,并根据$\sigma(\psi)$来调整组播率.有校正和不校正两种方法,采用不校正的方法时,取组播率为$\sigma(\psi)$,即让下一批数据传输的组播率与测试值$\sigma(\psi)$相等;采用校正的方法是让组播率略低于$\sigma(\psi)$,即按公式(20)调整组播率,其中,p 为调整量.

$$h=\begin{cases}\sigma(\psi), & \text{不校正}\\ \sigma(\psi)-p, & \text{校正}\end{cases} \tag{20}$$

设一次数据传输(包括重传)所需的时间为一个时间单位,称为一个时间段,在整个数据传输过程中,用序号 t 来标识各时间段.事实上,$\sigma(\psi)$反映了上一时间段网络的组播容量.当网络的组播容量在相邻两个时间段间的变化不很频繁时,则可以采用不校正的方法.

为使宿点区分是重传还是新传输的信息,数据包的包头应携带传输的批号.当宿点发现数据包中的批号与上一批传输的数据包的批号相同时,则能判断出是重传的数据包.

为使宿点提高重传时解码的概率,每一宿点设置一个缓冲区,用于保存其不能解码的数据包,以便与重传的数据包一同进行解码(注意到公式(3)和图 4,宿点能从接收到的数据包中析出全局编码向量和字符构成方程,多个数据包能形成方程组).以下分析表明,这样能提高重传时信息的解码概率.由线性网络编码的原理,很容易得出如下结论:当源点以相同的组播率采用 RNC 对同一批信息进行两次或多次传输时,宿点可以把两次或多次接收到的方程联立成方程组,以解出源点播出的信息.

由前面所述,对于一次数据传输,宿点 r 只能接收到$|In(r)|$个线性方程.若发生重传时,把原来前一批(或多批)不能解码的方程一同联立,则所得到的方程数增加,那么从较多的方程中找到秩为 h 的极大无关组的概率也相应地增大.例如,设组播率为 10,假设某一宿点第一次收到了 9 个的数据包,而这 9 个数据包构成的线性方程组的秩小于 10,不能解出源点的信息,则要求源点重传.当宿点收到重传的 9 个数据包后,连同原来的数据包将可以构成 18 个线性方程,其中后 9 个方程是重传时接收到的.显然,从这 18 个方程中选择 10 个线性无关的方程比仅从后 9 个方程中选择将具有较大的概率.

尽管采用这种策略测试出的组播容量是上一时间段网络的组播容量,但当组播容量的变化具有一定的平稳性,相邻两个时间段间组播容量的变化不是很频繁,并结合了重传技术,则仍不失为一种较好的策略.它能跟踪网络拓扑的变化,使组播率尽可能地适应组播容量的变化,且把测试组播容量的操作嵌入至数据传输过程中,不会中断网络的数据传输.RNC-RVMR 的有效性取决于以下因素:为使测试出的组播容量反映实际值,必须采用较大阶的伽罗华域;为使传输每一批数据时网络的组播容量与其前一时间段的组播容量接近,要求相邻两个时间段间的网络组播容量变化不频繁.在这种环境下,RNC-RVMR 比 RNC 提高了网络的吞吐率.

与 RNC 相比,RNC-RVMR 传输的全局编码向量要增加 $H–h$ 个分量,且宿点需要对矩阵进行两次计算:第 1 次是计算 $\boldsymbol{M}(r,\xi)$的秩;第 2 次是按公式(16)进行计算.但一般来说,传输的数据块较长,则全局编码向量增加的部分相对较小.另外,网络编码的宗旨是用节点的计算能力提高网络的吞吐率,当宿点计算速度较快时,提出的方法是有效的.

5 仿真测试

尽管上述建立了一套完整的理论,并采用数学方法严格证明了其定理、推论和性质的正确性,为使理论更为可信,需通过仿真测试进一步说明上述定理、推论和性质的正确性和有效性.其仿真过程通过编程在微机上模拟网络编码的数据传输,其运行环境为 Pentium® D CPU 2.80GHZ.

5.1 仿真测试1

测试目标是为了验证性质 1、定理 3、性质 2 的正确性和有效性.

采用 5 个测试用例,每一个测试用例是一个单源组播网络,采用文献[15]的方法随机产生,并进行手工调整(去掉一些孤立点,调整部分链路的容量),采用邻接矩阵来表示各测试用例.各测试用例的参数见表 1.

Table 1 Parameters of test cases

表 1 各测试用例的参数

Test case order	$\|V\|$	$\|E\|$	$\|T\|$	H	C
1	24	136	10	13	7
2	36	175	10	11	10
3	41	202	10	12	9
4	47	237	10	13	12
5	52	261	10	14	11

每一个测试用例的宿点个数$|T|$均为 10.表中$|V|$为总的节点个数,$|E|$为总的信道数,H 为源点的输出信道数,C 为组播容量值.

测试方法:对每一测试用例,在选定的伽罗华域 $GF(2^m)$下,以组播率 H 采用 RNC 组播数据至网络,称为一次试播.如上所述,一次试播相当于随机产生了一个组播率为 H 的编码方案,不妨记为ψ.每一测试用例在不同的伽罗华域下分别试播 500 次,统计出所有宿点全局编码矩阵的前 $k(k=k_1,C$,其中,k_1 为不超过组播容量 C 的整数)列构成的矩阵 $\boldsymbol{N}(\boldsymbol{M}(r,\psi),k)$ 的秩为 k 的概率.即分别统计 $P_r\left\{\psi:\underset{r\in T}{\wedge}(rank(\boldsymbol{N}(\boldsymbol{M}(r,\psi),k_1))=k_1)\right\}$ 和 $P_r\left\{\psi:\underset{r\in T}{\wedge}(rank(\boldsymbol{N}(\boldsymbol{M}(r,\psi),C))=C)\right\}$,所得结果见表 2.

Table 2 Simulation results

表 2 仿真结果

m	Test case No.1		Test case No.2		Test No.3		Test case No.4		Test case No.5	
	k=6	k=7	k=9	k=10	k=8	k=9	k=10	k=12	k=10	k=11
4	0.926	0.352	0.878	0.288	0.972	0.702	0.996	0.340	0.992	0.926
5	0.986	0.654	0.972	0.590	0.992	0.836	0.998	0.664	1.000	0.954
6	0.996	0.776	0.994	0.790	0.998	0.946	1.000	0.804	1.000	0.984
7	1.000	0.896	0.996	0.910	0.998	0.962	1.000	0.908	1.000	0.992
8	1.000	0.956	1.000	0.956	1.000	0.974	1.000	0.946	1.000	0.996
9	1.000	0.976	1.000	0.976	1.000	0.992	1.000	0.984	1.000	1.000
10	1.000	0.990	1.000	0.990	1.000	0.998	1.000	0.986	1.000	1.000
11	1.000	0.998	1.000	0.994	1.000	0.998	1.000	0.994	1.000	1.000
12	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000

根据前面的阐述,事实上,每次试播时,随机产生了 3 个编码方案,其组播率分别为 k_1,C,H.当 $H>C$ 时,第 3 个编码方案必定是不可行的,前两个编码方案均是第 3 个编码方案的导出编码方案,第 1 个编码方案也是第 2 个编码方案的导出编码方案.对每一次试播,我们还验证当第 2 个编码方案可行时,第 1 个编码方案的可行性.

例如:对于测试用例 2,选定一个伽罗华域 $GF(2^4)$,以组播率 11 从源点采用 RNC 组播数据至网络 500 次,每一次数据传输相当于随机产生了一个编码方案,不妨记为ψ,每一宿点 r 对应的全局编码矩阵为 $\boldsymbol{M}(r,\psi)$.然后分别计算 $\boldsymbol{N}(\boldsymbol{M}(r,\psi),9)$和 $\boldsymbol{N}(\boldsymbol{M}(r,\psi),10)$的秩(这里取 $k_1=9,C=10$).对于所有的宿点 $r\in T$,若 $\boldsymbol{N}(\boldsymbol{M}(r,\psi),9)$的秩均为 9,称之为命中一次,表 2 中的 0.878 就是 500 次试播中所有宿点的全局编码矩阵的前 9 列构成的矩阵其秩为 9 的概率.同理,0.288 是 500 次测试中每一宿点的全局编码矩阵的前 10 列构成的矩阵的秩为 10 的概率.

对测试用例 1 的仿真结果进行分析:注意到整数 10 为测试用例 1 的组播容量,从而说明了对于测试用例 1,若采用伽罗华域为 $GF(2^4)$,公式(15)的概率仅为 0.288;若采用的伽罗华域为 $GF(2^{11})$,则公式(15)的概率达到了 0.994.若采用性质 2 的方法计算$\sigma(\psi)$,则$\sigma(\psi)$=10 的概率为 0.994,从而说明了若采用性质 2 的方法测试组播容量,则在 500 次试播中有 497 次能够测试出组播容量.从而当伽罗华域较大时,公式(15)的概率较大,采用性质 2 的方法能够测试出组播容量也是一个大概率事件.

对于其他的测试用例,结合表 1 中的组播容量值对表 2 的仿真结果进行观察,得到了相似的结论,从而验证了定理 3、性质 2 的正确性.

实验结果还表明,每当第 2 个编码方案是可行的,第 1 个编码方案也是可行的,从而验证了性质 1 的正确性.

从表 2 可以看出,所采用的伽罗华域只需 m>8.对于每一个测试用例,无论公式(15)的概率还是性质 2 中$\sigma(\psi)$=C 的概率均接近于 1.即对于所选的测试用例来说,并不需要很大的伽罗华域.

注意以下事实:采用公式(17)求$\sigma(\psi)$,则$\sigma(\psi))\geqslant k(k\leqslant C)$的充要条件是对于所有的 $r\in T$,有 $rank(N(\boldsymbol{M}(r,\psi),k))=k$ 成立.从表 2 中可以看出,当 m 较大时,对于单次试播,尽管公式(17)中的$\sigma(\psi)$可能达不到 C,但与 C 很接近.例如,对于测试用例 1,5,当 m>6 时,每一次试播均使$\sigma(\psi)$的值不低于 C–1.

5.2 仿真测试2

验证采用线性网络编码的导出与扩展技术测试组播容量的可行性和有效性.测试方法是:设置一个变量 w,初始时置 0,源点以组播率 H 采用 RNC 组播实验包至网络,宿点按公式(16)计算$\chi(r,\psi)$,源点按公式(17)计算$\sigma(\psi)$,并采用蒙托卡罗算法进行多次试播,记录最好的试播结果.即每次试播结束把 w 值与$\sigma(\psi)$值进行比较,若 w 值较小,则把$\sigma(\psi)$值替换 w 值.停止试播的条件为:当连续 3 次 w 值不被更改时停止试播.在不同的伽罗华域下分别针对以上提出的测试用例进行仿真测试,每一种情况测试 100 次,统计出平均试播次数,仿真结果见表 3.

Table 3 Average number of trials for testing multicast capacity

表 3 测试组播容量所需的平均试播次数

m	4	5	6	7	8	9	10	11	12
Test case No.1	6.14	4.53	4.27	4.18	4.03	4.02	4.00	4.00	4.00
Test case No.2	7.26	4.85	4.30	4.09	4.09	4.02	4.02	4.01	4.00
Test case No.3	4.55	4.15	4.06	4.05	4.02	4.00	4.00	4.00	4.00
Test case No.4	5.64	4.58	4.27	4.12	4.03	4.03	4.03	4.00	4.00
Test case No.5	4.07	4.04	4.03	4.00	4.00	4.00	4.00	4.00	4.00

仿真结果表明,采用这种方法均能测试出组播容量,且随着所采用的伽罗华域的阶增大,所需的平均试播次数明显减少,说明了方法的可行性和有效性.

5.3 仿真测试3

以测试用例 5 为基础(假设以上产生的测试用例 5 为网络静态时的拓扑结构)来构造一个动态变化的网络拓扑:在 t=1,11,21,31 时让网络拓扑发生突变,而在接下来的时间段内网络拓扑不发生变化.而突变是在静态网络的基础上让每一信道的失效率为$(t-15)^2/800$,通过计算机模拟记录每一批数据传输时网络拓扑的变化,以邻接矩阵的形式记录下来,并求出各时间段的组播容量,见表 4.

Table 4 Multicast capacity in different time slots

表 4 各时间段的组播容量

t	1	2	…	11	12	…	21	22	…	31	32	…	40
C	5	5	…	7	7	...	6	6	…	3	3	…	3

然后,在变化的网络拓扑环境下组播一个长度为 90Kbyte 的文件至各宿点,分别采用理想方案、RNC-RVMR(组播率不校正)、RNC 进行数据传输,当文件传输完毕,统计信道流过的比特数(如发生数据重传,则信道流过的比特数累加).为了使实验环境相同,RNC 也采用重传技术,参数设置如下:数据包的包头长度为 20 字节,整个数据包的长度为 1 020 字节,每一批数据传输恰在一个时间段内完成.在不同阶的伽罗华域($GF(2^m)$)下进行实验,

每种方法实验 50 次,统计出信道流过的平均比特数,仿真结果如图 6 所示.

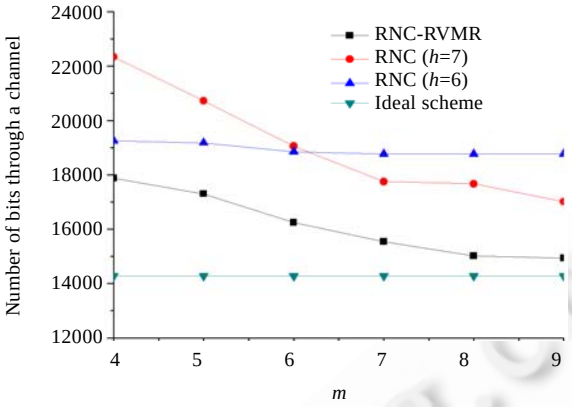

Fig.6 Number of bits through a channel

图 6 信道流过的比特数

采用网络编码技术时,在同一批数据传输过程中,各信道传输的比特数是相等的.因为采用同步机制,则可以用信道流过的比特数来衡量网络的吞吐率.当传输完同一文件后,若信道流过的比特数较小,则说明网络的吞吐率较大.从图 6 可以看出:采用理想方案信道流过的比特数最小,这是因为理想方案不需重传,且每一批数据传输都采用了最大的组播率,其网络的吞吐率达到最大;RNC-RVMR 为其次,劣于理想方案而优于 RNC;而采用 RNC 时,其网络的吞吐率是最低的.这是因为当组播率较大时(h=7),发生重传输的次数较多;当组播率较小时,会有相当一部分批次没有充分利用网络的资源.此外,尽管理想方案是最佳的,但对于本文给定的环境显然是不适合的.

从图 6 可看出,RNC-RVMR 明显优于 RNC,且当采用的伽罗华域的阶增大时,RNC-RVMR 越接近理想方案的性能.其原因为,当伽华域的阶增大时:一方面,每批数据传输时均能测试出组播容量,使网络能以较大的组播率进行数据传输;另一方面,宿点解码成功的概率增大,重传的次数减少.而对于 RNC,因难以选择合适的组播率,要么组播率较大,必定会引起重传;要么组播率较小,没有充分利用网络资源.

6 结束语

针对单源组播网络,通过对线性网络编码的内在机理进行分析,提出了不同组播率下编码方案的导出与扩展的技术.对具有导出与扩展的两个编码方案进行研究,导出了信道全局编码向量之间的确切关系.利用这个关系,结合随机线性网络编码方法,得出了几个重要的性质.这些性质有助于有效地运用线性网络编码技术,具有一定的应用价值.文中列出了 3 个方面的应用:可以实现不同组播率下编码系数的共享;可以分布式地测试组播容量和编码方案;针对网络拓扑动态变化的环境,提出了 RNC-RVMR,该方法在数据传输过程中动态地测试组播容量并更改组播率,并结合了重传策略.RNC-RVMR 除具有简单的特点外,与随机网络编码方法相比,还可以提高网络的吞吐率.对相关的应用进行了仿真测试,仿真结果验证了理论分析的结论.

下一步的工作是在多源组播环境下,如何对这些理论和应用进行推广.

References:

[1] Ahlswede R, Cai N, Li SR, Yeung RW. Network information flow. IEEE Trans. on Information Theory, 2000,46(4):1204−1216. [doi: 10.1109/18.850663]

[2] Li SYR, Yeung RW, Cai N. Linear network coding. IEEE Trans. on Information Theory, 2003,49(2):371−381. [doi: 10.1109/TIT.2002.807285]

[3] Koetter R, Medard M. An algebraoc approach to network coding. IEEE/ACM Trans. on Networking, 2003,11(5):782−795. [doi: 10.1109/TNET.2003.818197]

[4] Yang L, Zheng G, Hu XH. Research on network coding: A survey. Journal of Computer Research and Development, 2008,45(3): 400−407 (in Chinese with English abstract).

[5] Chou PA, Wu YN, Jain K. Practical network coding. In: Willian HS, ed. Proc. of the 41st Annual Allerton Conf. on Communication Control and Computing. Washington: IEEE CPS, 2003. 473−482.

[6] Jaggi S, Sanders P, Chou PA, Effros M, Egner S, Jain K, Tolhuozen LMGM. Polynomial time algorithms for multicast network code construction. IEEE Trans. on Information Theory, 2005,51(6):1973−1982. [doi: 10.1109/TIT.2005.847712]

[7] Fragouli C, Soljanin E. Information flow decomposition for network coding. IEEE Trans. on Information Theory, 2006,51(4): 1295−1312. [doi: 10.1109/TIT.2005.864435]

[8] Ho T, Medard M, Koetter R, Karger DR, Effros M, Shi J, Leong B. A random linear network coding approach to multicast. IEEE Trans. on Information Theory, 2006,52(10):4413−4430. [doi: 10.1109/TIT.2006.881746]

[9] Jabbarihagh M, Lahouti F. A decentralized approach to network coding based on learning. In: Willian R, ed. Proc. of the 2007 IEEE Information Theory Workshop on Information Theory for Wireless Networks. Washington: IEEE ITS, 2007. 1−5. [doi: 10.1109/ITWITWN.2007.4318025]

[10] Kim M, Aggaerwal V, Oreilly UM, Medard M. A doubly distributed genetic algorithm for network coding. In: Thierens D, Beyer HG, eds. Proc. of the 2007 ACM Genetic and Evolutionary Computation Conf. (GECCO 2007). New York: ACM Press, 2007. 1272−1279. [doi: 10.1145/1276958.1277201]

[11] Lun DS, Ratnakar N, Medard M, Koetter R, Karger DR, Ho T, Ahmed E, Zhao F. Minimum-Cost multicast over coded packet networks. IEEE Trans. on Information Theory, 2006,52(6):2608−2623. [doi: 10.1109/TIT.2006.874523]

[12] Ho T, Leong B, Medard M, Koetter R, Chang YH, Effeos M. On the utility of network coding in dynamic environments. In: Agvahml H, Kohno R, eds. Proc. of the Informational Workshop on Wireless Ad-Hoc Networks (IWWAN). Washington: IEEE CPS, 2004. 196−200. [doi: 10.1109/IWWAN.2004.1525570]

[13] Zhao F, Medard M. Online network coding for the dynamic multicast problem. In: Joseph AO, John BA, eds. Proc. of the 2006 IEEE Int'l Symp. on Information Theory. Washington: IEEE CPS, 2006. 1753−1757.

[14] Wang BS. Discrete Mathematics. Changsha: National University of Defence Technology Press, 2004. 263−281 (in Chinese).

[15] Melancon G, Philippe F. Generating connected acyclic digraphs uniformly at random. Information Processing Letters, 2004,90(4): 209−213. [doi: 10.1016/j.ipl.2003.06.002]

附中文参考文献:

[4] 杨林,郑刚,胡晓惠.网络编码研究进展.计算机研究与发展,2008,45(3):400−407.

[14] 王兵山.离散数学.长沙:国防科技大学出版社,2004.263−281.

蒲保兴(1965－),男,湖南邵阳人,博士,副教授,主要研究领域为网络编码,进化计算.

王伟平(1969－),女,博士,教授,主要研究领域为匿名通信,网络编码,信息安全.

杨路明(1947－),男,教授,博士生导师,主要研究领域为数据库信息系统.