软件学报 ISSN 1000-9825, CODEN RUXUEW E-mail: jos@iscas.ac.cn
Journal of Software,2012,23(3):688−699 [doi: 10.3724/SP.J.1001.2012.03963] http://www.jos.org.cn

Tel/Fax: +86-10-62562563

严格线性散播网络编码*

司菁菁[1,3+], 庄伯金[2], 蔡安妮[2]

[1](燕山大学 信息工程学院,河北 秦皇岛 066004)

[2](北京邮电大学 信息与通信工程学院,北京 100876)

[3](计算机软件新技术国家重点实验室(南京大学),江苏 南京 210093)

Strict Linear Dispersion Network Code

SI Jing-Jing[1,3+], ZHUANG Bo-Jin[2], CAI An-Ni[2]

[1](School of Information Engineering, Yanshan University, Qinhuangdao 066004, China)

[2](School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China)

[3](State Key Laboratory for Novel Software Technology at Nanjing University, Nanjing 210093, China)

+ Corresponding author: E-mail: sjj@ysu.edu.cn

Si JJ, Zhuang BJ, Cai AN. Strict linear dispersion network code. *Journal of Software*, 2012,23(3):688−699. http://www.jos.org.cn/1000-9825/3963.htm

Abstract: To solve problem that cannot be coded, which is inherent in the linear broadcast and linear dispersion, this paper proposes a new type of linear network code—the strict linear dispersion. A construction algorithm is proposed and it proves that the demanded finite field size is not higher than that of linear dispersion. Moreover, some special transition matrices are defined and the transition feasibility from linear dispersion to strict linear dispersion is proved. If combined with a special packetization strategy, the strict linear dispersion can present advantages over linear dispersion when applied in heterogeneous networks. It can also realize multi-rate transmission with a single network code session and provide convenience to the construction of network code on the extended network.

Key words: network coding; linear dispersion; strict linear dispersion; transition matrix; multi-rate

摘 要: 针对线性广播和线性散播网络编码在保证节点或节点集解码空间维数方面的不足,提出了一类新的线性网络编码——严格线性散播网络编码.给出了严格线性散播的定义,并设计了相应的构造算法.此种网络编码增强了对网络中任意非源节点集的输入链路上的全局编码核的限制,但其构造所需的有限域的阶并不大于普通的线性散播.此外,还提出了多种转换矩阵的概念,并证明了普通线性散播到严格线性散播的转换矩阵的存在性.结合特殊的数据打包策略,论证了严格线性散播在异构网络中的应用优势:一方面,它能够利用单一网络编码会话实现异构网络中的多速率信息传输;另一方面,它能够为异构网络拓扑结构的扩展提供便利.

关键词: 网络编码;线性散播;严格线性散播;转换矩阵;多速率

中图法分类号: TP393 **文献标识码**: A

* 基金项目: 国家自然科学基金(60832001,61071200); 河北省自然科学基金(F2010001294); 秦皇岛市科学技术研究与发展计划(201001A052)

收稿时间: 2009-11-17; 定稿时间: 2010-10-26

2000年,Ahlswede等人[1]首次提出了网络编码的概念.其核心思想是:网络中任意中间节点的操作不再仅限于存储转发,而是能够对接收到的数据进行函数运算,从而充分利用带宽资源进行更有效的数据传输.单源无环网络上的线性网络编码按照对全局编码核线性无关性的要求,按照由低到高的顺序可以分成 4 类[2]:线性组播(linear multicast)、线性广播(linear broadcast)、线性散播(linear dispersion)和一般线性网络编码(generic linear network code).网络编码理论的早期研究工作[3−6]主要集中于线性组播——信源为所有信宿发送相同的数据.然而,异构性是网络的固有特性,资源分配的不均匀以及端系统处理能力的差异是其存在的根源.在这一前提下,若按照组播传统意义上的单速率机制,则发送速率由接收带宽最低的信宿决定.这会使得网络中的所有信宿无论接收能力如何都要受到瓶颈信宿速率的影响,显然带来了接收者之间的严重的不公平性问题.

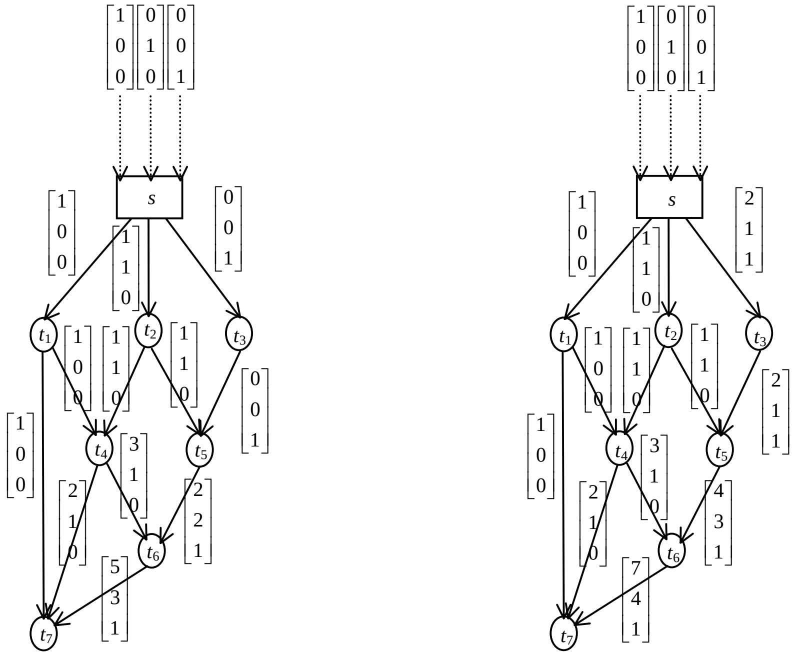
为了适应网络的异构性,近年来,学者们基于信源分层编码提出了一类分层组播网络编码方案(layered multicast)[7−10].这些方案将信源数据编码成具有不同重要性的多个编码层;每个编码层利用独立的线性组播进行传输;具有不同接收能力的信宿通过参加不同数量的组播,最大化其吞吐量.然而,这类方案是基于叠加编码(superposition coding)的思想进行组播内(intra-session)网络编码的,网络必须能够为每个组播划分出带宽满足要求的独立的编码子图.因此,此类方案对于一般的异构网络来说未必是最优的.为了进一步提高异构网络中的资源利用率,学者们还提出了一类基于组播间(inter-session)网络编码的多速率信息传输方案[11−13].虽然组播间线性网络编码拓展了编码对象的选择范围,但是却为信宿端解码带来了困难:网络中,某信宿接收到的网络编码数据可能是由其希望接收的组播对象与其不希望接收的组播对象进行线性组合构成的,因此,信宿需要接收到较多的编码数据才能解码出其所需的组播对象.此外,从本质上讲,以上两类方案都是利用多组播会话(multiple multicast sessions)实现异构网络中的多速率信息传输的.它们都需要在多个组播会话间进行网络资源的优化分配,因此需要设计并求解复杂的优化问题,而这些优化问题常常是有 NP 难度的[14].近几年,学者们还提出了一类结合利用数据非均衡保护和随机线性网络编码的数据传输方案[15−18].这类方案根据网络状态事先对信源数据进行非均衡保护,即加入一定数量的冗余信息,从而使得网络中的异构信宿能够根据其接收到的网络编码数据解码出一定数量的信源数据.然而,这类传输方案是基于随机网络编码的,即网络中的各个信宿是以一定的成功概率[18]解码出部分信源数据的.若需要明确保证网络中各信宿的接收解码能力,则需要对信源编码、非均衡保护策略和网络编码设计进行联合优化.

为了避免复杂的资源优化问题,本文研究如何利用单一确定性线性网络编码会话实现异构网络中的多速率信息传输.根据线性广播和线性散播的定义,它们能够为网络中具有不同接收能力的节点传输不同数量的线性无关网络编码数据,因此具有应用于异构网络的潜力.然而,线性广播和线性散播仅能保证节点或节点集的接收空间的维数,却不能保证其解码空间的维数[19],即线性广播和线性散播无法保证网络节点接收到的网络编码数据能够部分解码.对于某些节点或节点集,其接收到的网络编码数据甚至是完全不可解的.

以如图 1(a)所示的一个 3 维线性散播为例.假设信源 s 发送的数据包为 $\boldsymbol{x}_1\boldsymbol{x}_2\boldsymbol{x}_3$.节点集$\{t_3,t_5\}$由其输入链路 st_3 和 t_2t_5 接收到 2 个网络编码数据包 $\boldsymbol{y}_{st_3}=[\boldsymbol{x}_1,\boldsymbol{x}_2,\boldsymbol{x}_3][0,0,1]^T=\boldsymbol{x}_3$ 和 $\boldsymbol{y}_{t_2t_5}=[\boldsymbol{x}_1,\boldsymbol{x}_2,\boldsymbol{x}_3][1,1,0]^T=\boldsymbol{x}_1+\boldsymbol{x}_2$,但其仅能解码出 1 个信源数据包 $\boldsymbol{x}_3$.节点 t_2 由其输入链路 st_2 接收到网络编码数据包 $\boldsymbol{y}_{st_2}=[\boldsymbol{x}_1,\boldsymbol{x}_2,\boldsymbol{x}_3][1,1,0]^T=\boldsymbol{x}_1+\boldsymbol{x}_2$,却解码不出任何信源数据包.

针对上述问题,本文提出了一类新的线性网络编码——严格线性广播和严格线性散播,此类网络编码通过对全局编码核进行更严格的限制来换取非源节点或非源节点集接收数据的部分解码能力.本文提出了严格线性散播的构造算法,并证明了构造严格线性散播所需的有限域的阶及复杂度均不高于普通线性散播.此外,本文还提出了一系列转换矩阵的概念,并推导出了线性散播与严格线性散播之间的转换关系.结合一种特殊的信源数据打包策略,本文论证了严格线性散播在异构网络中的应用优势:一方面,严格线性散播使得网络中具有不同接收带宽的信宿均能够接收并解码出一定数量的信源编码层,克服了线性广播和线性散播在保证接收数据部分解码能力方面的不足,利用单一网络编码会话实现了异构网络中的多速率信息传输;另一方面,严格线性散播还能为异构网络拓扑结构的扩展提供便利.若有新的子网络希望接入,则只需根据子网络的位置及其中信宿的接收需求,将其与原网络中具有相应接收能力的节点集相连.之后,只需独立地设计子网络上的网络编码,而无

需改变原网络中应用的网络编码,更不需要在扩展后的整个网络上重新设计网络编码.



(a) 有限域$\mathbb{F}_8$上的一个 3 维线性散播　　(b) 有限域$\mathbb{F}_8$上的一个 3 维严格线性散播

Fig.1　Examples for linear dispersion and strict linear dispersion respectively

图 1　线性散播和严格线性散播的举例

1　网络模型及线性网络编码的基本概念

本文讨论单源有向无环网络 $G=(V,E,s)$,其中,V 为节点集,E 为链路集,s 为源节点.假设网络中每条链路均为单位容量,某节点 t 的输入链路集合和输出链路集合分别用 $In(t)$和 $Out(t)$表示.令 $In(s)$表示源节点 s 的虚拟输入链路(imaginary link)集,用以模拟信源数据的生成.若存在节点 $t\in V$ 使得链路 $d\in In(t),e\in Out(t)$,则将链路对(d,e)称作一个邻接对.网络 G 中非源节点的个数用整数 n 表示.

令$\mathbb{F}_q$表示阶为 q 的有限域.网络 G 的一个$\mathbb{F}_q$域ω维线性网络编码为每个邻接对(d,e)赋予一个标量 $k_{d,e}\in\mathbb{F}_q$,并为每条链路 $e\in E$ 赋予一个ω维列向量 $\boldsymbol{f}_e\in\mathbb{F}_q^{\omega}$,使得:

a) 对于任意节点 $t\in V$ 的任意输出链路 $e\in Out(t)$, $\boldsymbol{f}_e=\sum_{d\in In(t)}k_{d,e}\boldsymbol{f}_d$;

b) 源节点 s 的ω条虚拟输入链路对应的列向量$\{\boldsymbol{f}_e:e\in In(s)\}$构成向量空间 $\mathbb{F}_q^{\omega}$ 的自然基(natural basis).

向量$\boldsymbol{f}_e$称作链路 e 的全局编码核(global encoding kernel),$|In(t)|\times|Out(t)|$维矩阵 $\boldsymbol{K}_t=[k_{d,e}]_{d\in In(t),e\in Out(t)}$称作节点 t 的局部编码核(local encoding kernel).本文用$(\{\boldsymbol{f}_e:e\in E\},\{\boldsymbol{K}_t:t\in V\})$描述网络 G 的一个$\mathbb{F}_q$域ω维线性网络编码.

若用 $\boldsymbol{F}_{\xi}=[\boldsymbol{f}_e]_{e\in\xi}$表示以链路集合$\xi$中所有链路的全局编码核为列而形成的$\omega\times|\xi|$维矩阵,则任意节点 t 的局部编码核与其输入、输出链路的全局编码核间的关系可以表示为矩阵形式:

$$\boldsymbol{F}_{Out(t)}=\boldsymbol{F}_{In(t)}\boldsymbol{K}_t \tag{1}$$

网络 G 中,源节点 s 到某非源节点 t 的最大流用 max$flow(t)$表示,s 到某非源节点集 T 的最大流用 max$flow(T)$表示.记向量空间 $\boldsymbol{V}_t=span(\{\boldsymbol{f}_d:d\in In(t)\})$,$\boldsymbol{V}_T=span(\{\boldsymbol{f}_d:d\in\cup_{t\in T}In(t)\})$.

定义 1(**线性广播和线性散播**)[2]. 网络 G 的一个$\mathbb{F}_q$域ω维线性网络编码:

a) 若对于任意的非源节点 $t\in V$ 均有 $\dim(V_t)=\min\{\omega,\max flow(t)\}$,则称其为网络 G 的一个 $\mathbb{F}_q$ 域 ω 维线性广播;

b) 若对于任意的非源节点集 $T\subset V$ 均有 $\dim(V_T)=\min\{\omega,\max flow(T)\}$,则称其为网络 G 的一个 $\mathbb{F}_q$ 域 ω 维线性散播.

性质 1[2]. 若网络 G 的一个 $\mathbb{F}_q$ 域 ω 维线性网络编码是线性散播,则它也是线性广播.

定理 1(线性散播的存在性定理). 给定有限域 $\mathbb{F}_q$ 和具有 n 个非源节点的单源有向无环网络 G.若 $q>2^n-1$,则网络 G 的 $\mathbb{F}_q$ 域 ω 维线性散播必存在.

证明:由于网络 G 中有 n 个非源节点,因此其中非空的非源节点集的个数为 2^n-1.由文献[20]中的定理 1 可知,当 $q>2^n-1$ 时,一定能够为网络 G 构建一个 $\mathbb{F}_q$ 域 ω 维线性散播. □

若采用 $\mathbb{F}_q$ 域 ω 维线性网络编码 $(\{\boldsymbol{f}_e:e\in E\},\{\boldsymbol{K}_t:t\in V\})$ 在网络 G 中传输信源数据包 $\boldsymbol{x}_1,\boldsymbol{x}_2,\ldots,\boldsymbol{x}_\omega$,则任意链路 e 上传输的网络编码数据包为 $[\boldsymbol{x}_1,\boldsymbol{x}_2,\ldots,\boldsymbol{x}_\omega]\cdot\boldsymbol{f}_e$,任意非源节点 t 由其输入链路集 $In(t)$ 接收到的网络编码数据包为 $\{[\boldsymbol{x}_1,\boldsymbol{x}_2,\ldots,\boldsymbol{x}_\omega]\cdot\boldsymbol{f}_d:d\in In(t)\}$.若 $(\{\boldsymbol{f}_e:e\in E\},\{\boldsymbol{K}_t:t\in V\})$ 是线性广播,则根据定义 1,网络中任意满足 $\max flow(t)\geqslant\omega$ 的非源节点 t 的接收空间维数 $\dim(V_t)=\omega$,因此 t 能够根据 $\{[\boldsymbol{x}_1,\boldsymbol{x}_2,\ldots,\boldsymbol{x}_\omega]\cdot\boldsymbol{f}_d:d\in In(t)\}$ 解码出 $\boldsymbol{x}_1,\boldsymbol{x}_2,\ldots,\boldsymbol{x}_\omega$.然而,对于任何 $\max flow(t)<\omega$ 的非源节点 t,其接收空间维数 $\dim(V_t)=\max flow(t)<\omega$,因此不能由 $\{[\boldsymbol{x}_1,\boldsymbol{x}_2,\ldots,\boldsymbol{x}_\omega]\cdot\boldsymbol{f}_d:d\in In(t)\}$ 完全解码出 $\boldsymbol{x}_1,\boldsymbol{x}_2,\ldots,\boldsymbol{x}_\omega$.此时,是否能够由 $\{[\boldsymbol{x}_1,\boldsymbol{x}_2,\ldots,\boldsymbol{x}_\omega]\cdot\boldsymbol{f}_d:d\in In(t)\}$ 解码出部分信源数据包取决于 $\{\boldsymbol{f}_d:d\in In(t)\}$ 的具体情况,而线性广播本身对此未作出要求.以上分析说明,线性广播仅保证了网络中任意非源节点 t 的接收空间的维数等于 $\min\{\omega,\max flow(t)\}$,而不能保证其解码空间的维数.同样,线性散播仅能够保证网络中任意非源节点集 T 的接收空间的维数,而不能保证其解码空间的维数.

记 $\boldsymbol{f}_e^k=[\boldsymbol{I}_k\ \ \boldsymbol{0}_{k\times(\omega-k)}]\boldsymbol{f}_e$,即取 $\boldsymbol{f}_e$ 的前 k 个元素形成的 k 维列向量,其中,$k<\omega$,$\boldsymbol{I}_k$ 表示 k 阶单位矩阵,$\boldsymbol{0}_{k\times(\omega-k)}$ 表示 $k\times(\omega-k)$ 维零矩阵.记矩阵 $\boldsymbol{A}_{\omega\times h}^k=[\boldsymbol{I}_k\ \ \boldsymbol{0}_{k\times(\omega-k)}]\boldsymbol{A}_{\omega\times h}$,即由 $\omega\times h$ 维矩阵 $\boldsymbol{A}_{\omega\times h}$ 的前 k 行形成的 $k\times h$ 维子阵,其中,$k<\omega$.记向量空间 $\boldsymbol{V}_t^k=span(\{\boldsymbol{f}_d^k:d\in In(t)\})$,$\boldsymbol{V}_T^k=span(\{\boldsymbol{f}_d^k:d\in\cup_{t\in T}In(t)\})$.

2 严格线性网络编码

2.1 严格线性广播和严格线性散播的定义

定义 2(严格线性广播和严格线性散播). 网络 G 的一个 $\mathbb{F}_q$ 域 ω 维线性网络编码:

a) 若对于任意非源节点 $t\in V$ 均有 $\dim(\boldsymbol{V}_t^{m_t})=m_t$,则称其为网络 G 的一个 $\mathbb{F}_q$ 域 ω 维严格线性广播,其中,

$$m_t=\min\{\omega,\max flow(t)\};$$

b) 若对于任意非源节点集 $T\subset V$ 均有 $\dim(\boldsymbol{V}_T^{m_T})=m_T$,则称其为网络 G 的一个 $\mathbb{F}_q$ 域 ω 维严格线性散播,其中,

$$m_T=\min\{\omega,\max flow(T)\}.$$

本文提出的严格线性散播(严格线性广播)要求任何矩阵 $\boldsymbol{F}_{\cup_{t\in T}In(t)}$ $(\boldsymbol{F}_{In(t)})$ 中的前 $m_T(m_t)$ 个行向量线性无关.对比定义 1,线性散播(线性广播)只要求矩阵 $\boldsymbol{F}_{\cup_{t\in T}In(t)}$ $(\boldsymbol{F}_{In(t)})$ 中存在 $m_T(m_t)$ 个线性无关的行向量.因此,与线性散播(线性广播)相比,严格线性散播(严格线性广播)对全局编码核提出了更高的要求,且具有以下性质:

性质 2. 若网络 G 的一个 $\mathbb{F}_q$ 域 ω 维线性网络编码是严格线性广播,则它也是线性广播.

性质 3. 若网络 G 的一个 $\mathbb{F}_q$ 域 ω 维线性网络编码是严格线性散播,则它也是线性散播.

性质 4. 若网络 G 的一个 $\mathbb{F}_q$ 域 ω 维线性网络编码是严格线性散播,则它也是严格线性广播.

2.2 严格线性散播的构造

根据性质 4,本文主要研究严格线性散播.下面通过修改 Jaggi-Sanders 线性组播构造算法[5],提出一种严格线性散播的构造算法,从而证明严格线性散播的存在性.

对一个具有 n 个非源节点的单源有向无环网络 G,分别用 $T_1,...,T_{2^n-1}$ 表示其 2^n-1 个非空的非源节点集.对于任意非源节点集 T_u,利用路由分析算法[21]预先确定出 m_u 条从源节点 s 到 T_u 的独立路径 $P_{u,1},...,P_{u,m_u}$,其中,$m_u=\min\{\omega,\max flow(T_u)\},u=1,…,2^n-1$.若某链路 e 在从 s 到 T_u 的路径 $P_{u,i}$ 上,则将$\langle u,i\rangle$称为 e 的一个路径标号对(path-index pair).记 $Idx_e=\{\langle u,i\rangle:e\in P_{u,i}\}$为由链路 e 的所有路径标号对构成的集合.

性质 5. 设 $e\in E$,则$|Idx_e|\leqslant 2^n-1$.

算法 1(**严格线性散播的构造算法**). 为网络 G 构造一个$\mathbb{F}_q$域ω维严格线性散播,其中,$q>2^n-1$.

算法的实现过程如图 2 所示.本算法按照网络中信息流由上游节点到下游节点的顺序为每个节点 t 的每条输出链路 $e\in Out(t)$从向量空间 $\boldsymbol{V}_t=span(\{\boldsymbol{f}_d:d\in In(t)\})$中选择满足严格线性散播定义要求的全局编码核 $\boldsymbol{f}_e$.节点的选择顺序保证了对于任意邻接对(d,e),$\boldsymbol{f}_d$ 的分配总在 $\boldsymbol{f}_e$ 之前.

```
{
 Let F_In(s)=I_ω,            //为 s 的ω条虚拟输入链路赋予的全局编码核构成 F_q^ω 的自然基
 for (every link e in network G)
     f_e=the zero vector;    //初始化 f_e
 for (u=1; u≤2^n−1; u++)
     for (i=1; i≤m_u; i++)
         e_u,i=the imaginary link initiating path P_u,i;    //初始化 e_u,i
 for (every node t, in an upstream-to-downstream order)
     for (every link e∈Out(t))
     {
         Choose a vector f in V_t, such that  f^{m_u} ∉ span({f^{m_u}_{e_u,j} : j=1,...,m_u, j≠i})
             for every path-index pair ⟨u,i⟩∈Idx_e;                                  (*)
       f_e=f;              //确定 f_e.
       for (every path-index pair ⟨u,i⟩∈Idx_e)
           e_u,i=e;        //更新 e_u,i
      }
}
```

Fig.2 Pseudocode for algorithm 1

图 2 算法 1 的伪代码

用 $e_{u,i}$ 表示路径 $P_{u,i}$ 上最新一个分配了全局编码核的链路,称为路径 $P_{u,i}$ 的当前链路.

$e_{u,i}$ 从 s 的某虚拟输入链路开始,按照链路输入输出顺序沿路径 $P_{u,i}$ 进行更新.与 Jaggi-Sanders 算法不同,本算法在整个过程中不但始终保证 s 到每个非源节点集 T_u 的路径$\{P_{u,i}:i=1,…,m_u\}$中当前链路$\{e_{u,i}:i=1,…,m_u\}$上的全局编码核 $\{\boldsymbol{f}_{e_{u,i}}:i=1,...,m_u\}$ 线性无关,更进一步要求 $\{\boldsymbol{f}^{m_u}_{e_{u,i}}:i=1,...,m_u\}$ 线性无关.其中,$u=1,…,2^n-1$.

下面分析算法 1 的可行性.由于图 2 中的第(*)行是算法 1 的核心操作,因此只需要分析空间 $\boldsymbol{V}_t$ 中为链路 $e\in Out(t)$选取的满足算法要求的向量 $\boldsymbol{f}$ 的存在性.

记 $\dim(\boldsymbol{V}_t)=r$, $\dim(\boldsymbol{V}_t^{m_u})=r_{m_u}\leqslant r$.当为链路 $e\in Out(t)$选择全局编码核时,若$\langle u,i\rangle\in Idx_e$,则路径 $P_{u,i}$ 的当前链路 $e_{u,i}\in In(t)$, $\boldsymbol{f}_{e_{u,i}}\in\boldsymbol{V}_t$ 且 $\boldsymbol{f}^{m_u}_{e_{u,i}}\in\boldsymbol{V}_t^{m_u}$. 由于已为 $e_{u,i}$ 选择 $\boldsymbol{f}_{e_{u,i}}$, 使得 $\boldsymbol{f}^{m_u}_{e_{u,i}}\notin span(\{\boldsymbol{f}^{m_u}_{e_{u,j}}:j=1,...,m_u,j\neq i\})$, 因此,

$$\dim(\boldsymbol{V}_t^{m_u}\cap span(\{\boldsymbol{f}^{m_u}_{e_{u,j}}:j=1,...,m_u,j\neq i\}))\leqslant r_{m_u}-1,$$

即向量数 $|\boldsymbol{V}_t^{m_u}\cap span(\{\boldsymbol{f}^{m_u}_{e_{u,j}}:j=1,...,m_u,j\neq i\})|\leqslant q^{r_{m_u}-1}$.

根据线性散播的定义要求,对于任意$\langle u,i\rangle\in Idx_e$,向量空间 $\boldsymbol{V}_t$ 中 $\boldsymbol{f}$ 不能选择的向量个数为

$$|\boldsymbol{V}_t^{m_u}\cap span(\{\boldsymbol{f}^{m_u}_{e_{u,j}}:j=1,...,m_u,j\neq i\})|\cdot q^{r-r_{m_u}}\leqslant q^{r_{m_u}-1}\cdot q^{r-r_{m_u}}=q^{r-1}.$$

当 $q>2^n-1$ 时,

$$\sum_{\langle u,i\rangle\in Idx_e}|\boldsymbol{V}_t^{m_u}\cap span(\{\boldsymbol{f}^{m_u}_{e_{u,j}}:j=1,...,m_u,j\neq i\})|\cdot q^{r-r_{m_u}}\leqslant\sum_{\langle u,i\rangle\in Idx_e}q^{r-1}\leqslant(2^n-1)\cdot q^{r-1}<q^r=|\boldsymbol{V}_t| \quad (2)$$

式(2)表明,当 $q>2^n-1$ 时,空间 $\boldsymbol{V}_t$ 中不能选择的向量个数小于空间中的向量总数.因此,必能从 $\boldsymbol{V}_t$ 中选出向量

$\boldsymbol{f}$,使得对于任意$\langle u,i\rangle\in Idx_e$均满足 $\boldsymbol{f}^{m_u}\notin span(\{\boldsymbol{f}^{m_u}_{e_{u,j}}: j=1,...,m_u, j\neq i\})$,即算法 1 是可行的.

定理 2(严格线性散播的存在性定理). 给定有限域$\mathbb{F}_q$和具有 n 个非源节点的单源有向无环网络 G.若 $q>2^n-1$,则网络 G 的$\mathbb{F}_q$域ω维严格线性散播必存在.

算法 1 给出了定理 2 的构造性证明.由定理 1 和定理 2 可见,构建本文提出的严格线性散播所需的有限域的阶并不大于普通的线性散播.

另一方面,若将图 2 第(*)行中的 $\boldsymbol{f}^{m_u}\notin span(\{\boldsymbol{f}^{m_u}_{e_{u,j}}: j=1,...,m_u, j\neq i\})$ 改为 $\boldsymbol{f}\notin span(\{\boldsymbol{f}_{e_{u,j}}: j=1,...,m_u, j\neq i\})$,则算法2构造出的就是一个$\mathbb{F}_q$域$\omega$维普通线性散播.采用类似于文献[5]中的计算过程可分析,利用算法2构建一个$\mathbb{F}_q$域ω维严格线性散播或普通线性散播的复杂度均为 $O(|E|(2^n-1)\omega^2)$.

3 线性散播到严格线性散播的转换

本节研究线性散播与严格线性散播间的转换关系,从而为严格线性散播的构造提供另一种思路.

引理 1. 设$(\{\boldsymbol{f}_e:e\in E\},\{\boldsymbol{K}_t:t\in V\})$是网络 G 的一个$\mathbb{F}_q$域ω维线性网络编码.对于任意无全零行的矩阵:

$$\boldsymbol{A}_{h\times\omega}\in\mathbb{F}_q^{h\times\omega},h<\omega,$$

$(\{\boldsymbol{A}_{h\times\omega}\boldsymbol{f}_e:e\in E\},\{\boldsymbol{A}_{h\times\omega}\boldsymbol{K}_t:t=s\}\cup\{\boldsymbol{K}_t:t\neq s\})$必为网络 G 的一个$\mathbb{F}_q$域 h 维线性网络编码.

证明:任何$\mathbb{F}_q$域 h 维线性网络编码为源节点 s 的 h 条虚拟输入链路赋予的全局编码核满足 $\boldsymbol{F}'_{In(s)}=\boldsymbol{I}_h$.任取无全零行的矩阵 $\boldsymbol{A}_{h\times\omega}\in\mathbb{F}_q^{h\times\omega}$,$h<\omega$.对于任意非虚拟链路集$\xi$,记 $\boldsymbol{F}'_\xi=[\boldsymbol{A}_{h\times\omega}\boldsymbol{f}_e]_{e\in\xi}=\boldsymbol{A}_{h\times\omega}\boldsymbol{F}_\xi$.对于源节点 s,在公式(1)的两边同时左乘矩阵 $\boldsymbol{A}_{h\times\omega}$,有 $\boldsymbol{A}_{h\times\omega}\boldsymbol{F}_{Out(s)}=\boldsymbol{A}_{h\times\omega}\boldsymbol{F}_{In(s)}\boldsymbol{K}_s=\boldsymbol{A}_{h\times\omega}\boldsymbol{I}_\omega\boldsymbol{K}_s=\boldsymbol{I}_h\boldsymbol{A}_{h\times\omega}\boldsymbol{K}_s$,即

$$\boldsymbol{F}'_{Out(s)}=\boldsymbol{F}'_{In(s)}(\boldsymbol{A}_{h\times\omega}\boldsymbol{K}_s),\boldsymbol{K}'_s=\boldsymbol{A}_{h\times\omega}\boldsymbol{K}_s.$$

对于任意非源节点 t,在公式(1)两边同时左乘矩阵 $\boldsymbol{A}_{h\times\omega}$,则有 $\boldsymbol{A}_{h\times\omega}\boldsymbol{F}_{Out(t)}=\boldsymbol{A}_{h\times\omega}\boldsymbol{F}_{In(t)}\boldsymbol{K}_t$,即

$$\boldsymbol{F}'_{Out(t)}=\boldsymbol{F}'_{In(t)}\boldsymbol{K}_t,\boldsymbol{K}'_t=\boldsymbol{K}_t.$$

因此,$\{\boldsymbol{A}_{h\times\omega}\boldsymbol{K}_t:t=s\}\cup\{\boldsymbol{K}_t:t\neq s\}$是与全局编码核$\{\boldsymbol{A}_{h\times\omega}\boldsymbol{f}_e:e\in E\}$对应的局部编码核. □

引理 1 证明了任意一个无全零行的矩阵 $\boldsymbol{A}_{h\times\omega}\in\mathbb{F}_q^{h\times\omega}$ 均能将网络 G 的一个$\mathbb{F}_q$域ω维线性网络编码转换成一个$\mathbb{F}_q$域 h 维线性网络编码,$h<\omega$,且得到的 h 维线性网络编码在网络中的所有非源节点上均具有与原ω维线性网络编码相同的局部编码核.然而,转换前后的网络编码的类型未必相同.下面定义一系列转换矩阵的概念,并证明其存在性,从而逐步推导出将线性散播转换成严格线性散播的可行性.

定义 3(线性散播转换矩阵). 设$(\{\boldsymbol{f}_e:e\in E\},\{\boldsymbol{K}_t:t\in V\})$是网络 G 的一个$\mathbb{F}_q$域ω维线性散播,其中,$\omega\geqslant 2$.若矩阵 $\boldsymbol{A}_{h\times\omega}\in\mathbb{F}_q^{h\times\omega}$ 能使$(\{\boldsymbol{A}_{h\times\omega}\boldsymbol{f}_e:e\in E\},\{\boldsymbol{A}_{h\times\omega}\boldsymbol{K}_t:t=s\}\cup\{\boldsymbol{K}_t:t\neq s\})$成为网络 G 的一个$\mathbb{F}_q$域 h 维线性散播,则将矩阵 $\boldsymbol{A}_{h\times\omega}$称为$(\{\boldsymbol{f}_e:e\in E\},\{\boldsymbol{K}_t:t\in V\})$的一个$\omega\to h$ 维线性散播转换矩阵,其中,$h<\omega$.

引理 2[22]. 给定有限域$\mathbb{F}_q$、正整数$\omega\geqslant 2$、$l\leqslant\omega-1$.设 $\boldsymbol{c}_1,\boldsymbol{c}_2,\ldots,\boldsymbol{c}_l\in\mathbb{F}_q^\omega$ 是 l 个ω维线性无关列向量.令$\omega-1$ 维列向量 $\boldsymbol{d}_i=[\boldsymbol{I}_{\omega-1}\ \boldsymbol{b}]\boldsymbol{c}_i,i=1,2,\ldots,l$,其中,$\boldsymbol{b}=[b_1\ b_2\ \ldots\ b_{\omega-1}]^T,b_1,b_2,\ldots,b_{\omega-1}$为$\mathbb{F}_q$域上的变量.存在非零多项式 $p(b_1,b_2,\ldots,b_{\omega-1})=u_0+u_1b_1+u_2b_2+\ldots+u_{\omega-1}b_{\omega-1}$,使得当 $p(b_1,b_2,\ldots,b_{\omega-1})\neq 0$ 时,列向量 $\boldsymbol{d}_1,\boldsymbol{d}_2,\ldots,\boldsymbol{d}_l$ 线性无关.

本文称满足引理 2 的非零多项式 $p(b_1,b_2,\ldots,b_{\omega-1})$为列向量 $\boldsymbol{d}_1,\boldsymbol{d}_2,\ldots,\boldsymbol{d}_l$ 的示性多项式.

引理 3[2]. 令 $P(x_1,x_2,\ldots,x_h)$是有限域$\mathbb{F}_q$上的非零多项式.若有限域的阶 q 大于多项式 P 中任意变量 x_i 的次数,则存在 $v_1,v_2,\ldots,v_h\in\mathbb{F}_q$,使得 $P(v_1,v_2,\ldots,v_h)\neq 0$.

定理 3(线性散播转换矩阵的存在性定理). 若$(\{\boldsymbol{f}_e:e\in E\},\{\boldsymbol{K}_t:t\in V\})$是网络 G 的一个$\mathbb{F}_q$域ω维线性散播,其中,$q>2^n-1,\omega\geqslant 2$.则对于任意正整数 $h<\omega$,必存在一个 $\omega\to h$ 维线性散播转换矩阵 $\boldsymbol{A}_{h\times\omega}\in\mathbb{F}_q^{h\times\omega}$,使得$(\{\boldsymbol{A}_{h\times\omega}\boldsymbol{f}_e:e\in E\},\{\boldsymbol{A}_{h\times\omega}\boldsymbol{K}_t:t=s\}\cup\{\boldsymbol{K}_t:t\neq s\})$成为网络 G 的一个$\mathbb{F}_q$域 h 维线性散播.

证明:构造性证明.设($\{\boldsymbol{f}_e:e\in E\},\{\boldsymbol{K}_t:t\in V\}$)是网络 G 的一个$\mathbb{F}_q$ 域ω维线性散播,$q>2^n-1,\omega\geqslant 2$.对于任意非源节点集 T,其输入链路集$\cup_{t\in T}In(t)$中必存在 m'_T 条链路 $e_1,\dots,e_{m'_T}$,它们对应的ω维全局编码核 $\boldsymbol{f}_{e_1},\dots,\boldsymbol{f}_{e_{m'_T}}$ 线性无关,其中, $m'_T=\min\{\omega-1,\max flow(T)\}\leqslant\min\{\omega,\max flow(T)\}$.取$\omega-1$ 维列向量 $\boldsymbol{b}_{\omega-1}=[b_1\ b_2\ \dots\ b_{\omega-1}]^T$,其中,$b_1,b_2,\dots,b_{\omega-1}$为$\mathbb{F}_q$域上的变量.对于任意 $i=1,2,\dots,m'_T$,令$\omega-1$维列向量 $\boldsymbol{f}'_{e_i}=[\boldsymbol{I}_{\omega-1}\ \boldsymbol{b}_{\omega-1}]\boldsymbol{f}_{e_i}$.由引理 2 可知,存在列向量 $\boldsymbol{f}'_{e_1},\dots,\boldsymbol{f}'_{e_{m'_T}}$ 的示性多项式,记为 $p_T(b_1,b_2,\dots,b_{\omega-1})$.由于网络 G 中至多有 2^n-1 个不同的非空非源节点集,因此这些非源节点集对应的示性多项式的乘积可表示为$\mathbb{F}_q$ 域上的非零多项式 $P(b_1,b_2,\dots,b_{\omega-1})=\prod_T p_T(b_1,b_2,\dots,b_{\omega-1})$, 且 P 中任何变量 b_i 的次数均不超过 2^n-1.由于 $q>2^n-1$,因此由引理 3 可知,存在列向量 $\boldsymbol{v}_{\omega-1}=[v_1\ v_2\ \dots\ v_{\omega-1}]^T$ 使得

$$P(v_1,v_2,\dots,v_{\omega-1})=\prod_T p_T(v_1,v_2,\dots,v_{\omega-1})\neq 0.$$

对于任意非源节点集 T, $\{[\boldsymbol{I}_{\omega-1}\ \boldsymbol{v}_{\omega-1}]\boldsymbol{f}_{e_i}:i=1,2,\dots,m'_T\}$ 的示性多项式 $p_T(v_1,v_2,\dots,v_{\omega-1})\neq 0$.进而由引理 2 可知,列向量 $\{[\boldsymbol{I}_{\omega-1}\ \boldsymbol{v}_{\omega-1}]\boldsymbol{f}_{e_i}:i=1,2,\dots,m'_T\}$ 线性无关.因此,矩阵$[\boldsymbol{I}_{\omega-1}\ \ \boldsymbol{v}_{\omega-1}]$是($\{\boldsymbol{f}_e:e\in E\},\{\boldsymbol{K}_t:t\in V\}$)的一个$\omega\to(\omega-1)$维线性散播转换矩阵.若在$\omega-1$ 维线性散播($\{[\boldsymbol{I}_{\omega-1}\ \boldsymbol{v}_{\omega-1}]\boldsymbol{f}_e:e\in E\},\{[\boldsymbol{I}_{\omega-1}\ \boldsymbol{v}_{\omega-1}]\boldsymbol{K}_t:t=s\}\cup\{\boldsymbol{K}_t:t\neq s\}$)的基础上重复上述过程,则可以构造出一个$(\omega-1)\to(\omega-2)$维线性散播转换矩阵$[\boldsymbol{I}_{\omega-2}\ \ \boldsymbol{v}_{\omega-2}]$,其中, $\boldsymbol{v}_{\omega-2}\in\mathbb{F}_q^{\omega-2}$. 因此,$[\boldsymbol{I}_{\omega-2}\ \ \boldsymbol{v}_{\omega-2}]\cdot[\boldsymbol{I}_{\omega-1}\ \ \boldsymbol{v}_{\omega-1}]$是($\{\boldsymbol{f}_e:e\in E\},\{\boldsymbol{K}_t:t\in V\}$)的一个$\omega\to(\omega-2)$维线性散播转换矩阵.反复重复上述过程,对于任意正整数 $h<\omega$,均能构造出($\{\boldsymbol{f}_e:e\in E\},\{\boldsymbol{K}_t:t\in V\}$)的一个$\omega\to h$ 维线性散播转换矩阵$[\boldsymbol{I}_h\ \ \boldsymbol{v}_h]\cdot\ldots\cdot[\boldsymbol{I}_{\omega-2}\ \ \boldsymbol{v}_{\omega-2}][\boldsymbol{I}_{\omega-1}\ \ \boldsymbol{v}_{\omega-1}]$,其中,对于任意 $i=1,2,\dots,\omega-h$, $\boldsymbol{v}_{\omega-i}\in\mathbb{F}_q^{\omega-i}$. □

定理 4. 任给网络 G 的一个$\mathbb{F}_q$ 域ω维线性散播($\{\boldsymbol{f}_e:e\in E\},\{\boldsymbol{K}_t:t\in V\}$),其中,$q>2^n-1,\omega\geqslant 2$.对于任意正整数 $h<\omega$,若矩阵 $\boldsymbol{A}_{h\times\omega}\in\mathbb{F}_q^{h\times\omega}$ 是($\{\boldsymbol{f}_e:e\in E\},\{\boldsymbol{K}_t:t\in V\}$)的一个$\omega\to h$ 维线性散播转换矩阵,则存在一个ω维行向量 $\boldsymbol{a}\in\mathbb{F}_q^{\omega}$,使得矩阵 $\boldsymbol{B}_{(h+1)\times\omega}=\begin{bmatrix}\boldsymbol{A}_{h\times\omega}\\ \boldsymbol{a}\end{bmatrix}\in\mathbb{F}_q^{(h+1)\times\omega}$ 成为($\{\boldsymbol{f}_e:e\in E\},\{\boldsymbol{K}_t:t\in V\}$)的一个$\omega\to(h+1)$维线性散播转换矩阵.

证明:设($\{\boldsymbol{f}_e:e\in E\},\{\boldsymbol{K}_t:t\in V\}$)是网络 G 的一个$\mathbb{F}_q$ 域ω维线性散播,$q>2^n-1,\omega\geqslant 2$.任取正整数 $h<\omega$,设矩阵 $\boldsymbol{A}_{h\times\omega}\in\mathbb{F}_q^{h\times\omega}$ 是($\{\boldsymbol{f}_e:e\in E\},\{\boldsymbol{K}_t:t\in V\}$)的一个$\omega\to h$ 维线性散播转换矩阵.对于任意非源节点集 $T\subset V$,输入链路集合$\cup_{t\in T}In(t)$中必存在 $\bar{m}_T=\min\{h,\max flow(T)\}$ 条链路 $e_1,e_2,\dots,e_{\bar{m}_T}$,它们对应的ω维全局编码核 $\boldsymbol{f}_{e_1},\boldsymbol{f}_{e_2},\dots,\boldsymbol{f}_{e_{\bar{m}_T}}$ 线性无关,且矩阵 $\boldsymbol{A}_{h\times\omega}$能将它们转换成为线性无关的 h 维全局编码核 $\boldsymbol{A}_{h\times\omega}\boldsymbol{f}_{e_1},\boldsymbol{A}_{h\times\omega}\boldsymbol{f}_{e_2},\dots,\boldsymbol{A}_{h\times\omega}\boldsymbol{f}_{e_{\bar{m}_T}}$.

令 $m'_T=\min\{h+1,\max flow(T)\}$,$m_T=\min\{\omega,\max flow(T)\}$.因为 $\dim(\boldsymbol{V}_T)=m_T$,且 $\bar{m}_T\leqslant m'_T\leqslant m_T$,所以$\cup_{t\in T}In(t)$中必存在 $m'_T-\bar{m}_T$ 条链路 $e_{\bar{m}_T+1},\dots,e_{m'_T}$,使得 $\boldsymbol{f}_{e_1},\boldsymbol{f}_{e_2},\dots,\boldsymbol{f}_{e_{\bar{m}_T}},\boldsymbol{f}_{e_{\bar{m}_T+1}},\dots,\boldsymbol{f}_{e_{m'_T}}$ 线性无关.取ω维行向量 $\boldsymbol{a}=[a_1\ a_2\ \dots\ a_\omega]$,其中,$a_1,a_2,\dots,a_\omega$为$\mathbb{F}_q$ 域上的变量.取矩阵 $\boldsymbol{B}_{(h+1)\times\omega}=\begin{bmatrix}\boldsymbol{A}_{h\times\omega}\\ \boldsymbol{a}\end{bmatrix}$,则

$$\boldsymbol{D}_T=[\boldsymbol{f}'_{e_1}\ \boldsymbol{f}'_{e_2}\ \dots\boldsymbol{f}'_{e_{\bar{m}_T}}\dots\boldsymbol{f}'_{e_{m'_T}}]=\boldsymbol{B}_{(h+1)\times\omega}\cdot[\boldsymbol{f}_{e_1}\ \boldsymbol{f}_{e_2}\ \dots\boldsymbol{f}_{e_{\bar{m}_T}}\dots\boldsymbol{f}_{e_{m'_T}}]=\begin{bmatrix}\boldsymbol{A}_{h\times\omega}\boldsymbol{f}_{e_1} & \boldsymbol{A}_{h\times\omega}\boldsymbol{f}_{e_2} & \dots & \boldsymbol{A}_{h\times\omega}\boldsymbol{f}_{e_{\bar{m}_T}} & \dots & \boldsymbol{A}_{h\times\omega}\boldsymbol{f}_{e_{m'_T}}\\ \boldsymbol{a}\boldsymbol{f}_{e_1} & \boldsymbol{a}\boldsymbol{f}_{e_2} & \dots & \boldsymbol{a}\boldsymbol{f}_{e_{\bar{m}_T}} & \dots & \boldsymbol{a}\boldsymbol{f}_{e_{m'_T}}\end{bmatrix}\quad(3)$$

1) 若 $\max flow(T)\leqslant h<h+1$,则 $m'_T-\bar{m}_T$.由于 h 维全局编码核 $\boldsymbol{A}_{h\times\omega}\boldsymbol{f}_{e_1},\boldsymbol{A}_{h\times\omega}\boldsymbol{f}_{e_2},\dots,\boldsymbol{A}_{h\times\omega}\boldsymbol{f}_{e_{\bar{m}_T}}$ 线性无关,因此任取 $\boldsymbol{a}\in\mathbb{F}_q^{\omega}$,$h+1$ 维全局编码核 $\boldsymbol{f}'_{e_1}\ \boldsymbol{f}'_{e_2}\ \dots\boldsymbol{f}'_{e_{\bar{m}_T}}$ 均线性无关;

2) 若 $\max flow(T)\geqslant h+1>h$,则 $m'_T=h+1,\bar{m}_T=h$.$\boldsymbol{D}_T$ 为 $h+1$ 阶方阵.当且仅当 $\det(\boldsymbol{D}_T)\neq 0$ 时, $\boldsymbol{f}'_{e_1}\ \boldsymbol{f}'_{e_2}\ \dots\boldsymbol{f}'_{e_{m'_T}}$ 线性无关.

由公式(3)可知,$\det(\boldsymbol{D}_T)$为 $\boldsymbol{a}$ 的一阶多项式,记 $p_T(a_1,a_2,\dots,a_\omega)=\det(\boldsymbol{D}_T)=u_1a_1+u_2a_2+\dots+u_\omega a_\omega$.我们将满足条件 2)的所有非源节点集 T 对应的行列式 $\det(\boldsymbol{D}_T)$相乘,得到关于 $\boldsymbol{a}$ 的非零多项式:

$$P(a_1,a_2,\dots,a_\omega)=\prod_T\det(\boldsymbol{D}_T)=\prod_T p_T(a_1,a_2,\dots,a_\omega),$$

其中,任意变量 a_i 的次数均不大于 2^n-1.因为 $q>2^n-1$,所以由引理 3 可知,存在 $\boldsymbol{a}\in\mathbb{F}_q^{\omega}$ 使得 $P(a_1,a_2,\dots,a_\omega)\neq 0$,即对

于任意满足条件 2)的非源节点集 T,$\det(\boldsymbol{D}_T)\neq 0$,$h$+1 维全局编码核 $\boldsymbol{f}'_{e_1}\boldsymbol{f}'_{e_2}\ldots\boldsymbol{f}'_{e_{m_T}}$ 线性无关.由条件 1)、条件 2)可知,存在行向量 $\boldsymbol{a}\in\mathbb{F}_q^{\omega}$ 使得矩阵 $\boldsymbol{B}_{(h+1)\times\omega}$满足$\omega\to(h+1)$维线性散播转换矩阵的定义. □

推论 1. 设($\{\boldsymbol{f}_e:e\in E\},\{\boldsymbol{K}_t:t\in V\}$)是网络 G 的一个$\mathbb{F}_q$ 域ω维线性散播,其中,$q>2^n-1$,则存在矩阵 $\boldsymbol{B}_{\omega\times\omega}\in\mathbb{F}_q^{\omega\times\omega}$,使得($\{\boldsymbol{B}_{\omega\times\omega}\boldsymbol{f}_e:e\in E\},\{\boldsymbol{B}_{\omega\times\omega}\boldsymbol{K}_t:t=s\}\cup\{\boldsymbol{K}_t:t\neq s\}$)仍是 G 的一个$\mathbb{F}_q$ 域ω维线性散播.

定义 4(线性散播全维转换矩阵). 给定网络 G 的一个$\mathbb{F}_q$ 域ω维线性散播($\{\boldsymbol{f}_e:e\in E\},\{\boldsymbol{K}_t:t\in V\}$),$\omega\geqslant 2$.若矩阵 $\boldsymbol{C}_{\omega\times\omega}\in\mathbb{F}_q^{\omega\times\omega}$ 满足对于任意正整数 $h\leqslant\omega$, $\boldsymbol{C}_{\omega\times\omega}^{h}\in\mathbb{F}_q^{h\times\omega}$ 均是($\{\boldsymbol{f}_e:e\in E\},\{\boldsymbol{K}_t:t\in V\}$)的一个 $\omega\to h$ 维线性散播转换矩阵,其中, $\boldsymbol{C}_{\omega\times\omega}^{h}=[\boldsymbol{I}_h\ \ \boldsymbol{0}_{h\times(\omega-h)}]\boldsymbol{C}_{\omega\times\omega}$, 则将矩阵 $\boldsymbol{C}_{\omega\times\omega}$称为($\{\boldsymbol{f}_e:e\in E\},\{\boldsymbol{K}_t:t\in V\}$)的一个$\omega$维线性散播全维转换矩阵.

定理 5(线性散播全维转换矩阵的存在性定理). 任给网络 G 的一个$\mathbb{F}_q$ 域ω维线性散播,其中,$q>2^n-1$,$\omega\geqslant 2$,它的ω维线性散播全维转换矩阵必存在.

证明:设($\{\boldsymbol{f}_e:e\in E\},\{\boldsymbol{K}_t:t\in V\}$)是网络 G 的一个$\mathbb{F}_q$ 域ω维线性散播,其中 $q>2^n-1$,$\omega\geqslant 2$.由定理 3 可知,其存在一个$\omega\to 1$ 维线性散播转换矩阵 $\boldsymbol{C}_{1\times\omega}\in\mathbb{F}_q^{1\times\omega}$.再由定理 4 可知,存在行向量 $\boldsymbol{a}_1\in\mathbb{F}_q^{\omega}$,使得矩阵 $\boldsymbol{C}_{2\times\omega}=\begin{bmatrix}\boldsymbol{C}_{1\times\omega}\\ \boldsymbol{a}_1\end{bmatrix}\in\mathbb{F}_q^{2\times\omega}$ 成为($\{\boldsymbol{f}_e:e\in E\},\{\boldsymbol{K}_t:t\in V\}$)的一个 $\omega\to 2$ 维线性散播转换矩阵.依此类推,存在行向量 $\boldsymbol{a}_i\in\mathbb{F}_q^{\omega}$,$i$=2,…,$\omega$–1,使得矩阵 $\boldsymbol{C}_{(i+1)\times\omega}=\begin{bmatrix}\boldsymbol{C}_{i\times\omega}\\ \boldsymbol{a}_i\end{bmatrix}\in\mathbb{F}_q^{(i+1)\times\omega}$ 成为一个$\omega\to(i+1)$维线性散播转换矩阵.

当 $i=\omega-1$ 时,矩阵 $\boldsymbol{C}_{\omega\times\omega}\in\mathbb{F}_q^{\omega\times\omega}$ 满足($\{\boldsymbol{f}_e:e\in E\},\{\boldsymbol{K}_t:t\in V\}$)的$\omega$维线性散播全维转换矩阵的定义. □

定义 5(ω维线性散播→ω维严格线性散播转换矩阵). 设($\{\boldsymbol{f}_e:e\in E\},\{\boldsymbol{K}_t:t\in V\}$)是网络 G 的一个$\mathbb{F}_q$ 域ω维线性散播,$\omega\geqslant 2$.若矩阵 $\boldsymbol{A}_{\omega\times\omega}\in\mathbb{F}_q^{\omega\times\omega}$ 能使($\{\boldsymbol{A}_{\omega\times\omega}\boldsymbol{f}_e:e\in E\},\{\boldsymbol{A}_{\omega\times\omega}\boldsymbol{K}_t:t=s\}\cup\{\boldsymbol{K}_t:t\neq s\}$)成为网络 G 的一个$\mathbb{F}_q$ 域ω维严格线性散播,则称矩阵 $\boldsymbol{A}_{\omega\times\omega}$为($\{\boldsymbol{f}_e:e\in E\},\{\boldsymbol{K}_t:t\in V\}$)的一个$\omega$维线性散播→$\omega$维严格线性散播转换矩阵.

以如图 1(a)所示的$\mathbb{F}_8$域 3 维线性散播为例,矩阵 $\boldsymbol{A}_{3\times 3}=\begin{bmatrix}1&0&2\\0&1&1\\0&0&1\end{bmatrix}$ 可以将其转换为如图 1(b)所示的$\mathbb{F}_8$域 3 维严格线性散播.

定理 6(ω维线性散播→ω维严格线性散播转换矩阵的存在性定理). 任给网络 G 的一个$\mathbb{F}_q$ 域ω维线性散播,其中,$q>2^n-1$,$\omega\geqslant 2$,它的ω维线性散播→ω维严格线性散播转换矩阵必存在.

证明:设($\{\boldsymbol{f}_e:e\in E\},\{\boldsymbol{K}_t:t\in V\}$)是网络 G 的一个$\mathbb{F}_q$ 域ω维线性散播,其中,$q>2^n-1$,$\omega\geqslant 2$.由定理 5 可知,存在它的ω维线性散播全维转换矩阵 $\boldsymbol{A}_{\omega\times\omega}$.取 G 中的任意非源节点集 T,在其输入链路集$\cup_{t\in T}In(t)$中必存在 $m_T=\min\{\omega,\max flow(T)\}$条链路 $e_1,\ldots,e_{m_T}$,它们对应的ω维全局编码核 $\boldsymbol{f}_{e_1},\ldots,\boldsymbol{f}_{e_{m_T}}$ 线性无关,且 $\boldsymbol{A}_{\omega\times\omega}^{m_T}$ 能将其转换成线性无关的 m_T 维全局编码核$\{\boldsymbol{A}_{\omega\times\omega}^{m_T}\boldsymbol{f}_{e_i}:i=1,2,\ldots,m_T\}$,即$\{\boldsymbol{f}'^{m_T}_{e_i}=[\boldsymbol{I}_{m_T}\ \ \boldsymbol{0}_{m_T\times(\omega-m_T)}]\boldsymbol{A}_{\omega\times\omega}\boldsymbol{f}_{e_i}:i=1,2,\ldots,m_T\}$ 是线性无关的.

因此,($\{\boldsymbol{A}_{\omega\times\omega}\boldsymbol{f}_e:e\in E\},\{\boldsymbol{A}_{\omega\times\omega}\boldsymbol{K}_t:t=s\}\cup\{\boldsymbol{K}_t:t\neq s\}$)是网络 G 的一个$\mathbb{F}_q$ 域ω维严格线性散播.

即,$\boldsymbol{A}_{\omega\times\omega}$满足($\{\boldsymbol{f}_e:e\in E\},\{\boldsymbol{K}_t:t\in V\}$)的$\omega$维线性散播→$\omega$维严格线性散播转换矩阵的定义. □

由定理 6 可知,当 $q>2^n-1$ 时,任何一个给定的$\mathbb{F}_q$域ω维线性散播均能转换成一个$\mathbb{F}_q$域ω维严格线性散播.此定理从另一个角度证明了严格线性散播的存在性,并为严格线性散播的构造提供了另一种思路.

4 严格线性散播在异构网络中的应用优势

文献[18]设计了一种特殊的信源数据打包方案.此方案首先利用分层编码将信源数据编码成重要性逐层递减的 L 层;然后采用如图 3 所示的方法将信源数据打包成ω个数据包 $\boldsymbol{x}_1,\boldsymbol{x}_2,\ldots,\boldsymbol{x}_\omega$,使得第 k 层的所有数据块{$\boldsymbol{B}_{k,i}$:

i=1,…,D_k}仅包含在前 N_k 个数据包 $\boldsymbol{x}_1,...,\boldsymbol{x}_{N_k}$ 内,而在后ω–N_k 个数据包 $\boldsymbol{x}_{N_k+1},\boldsymbol{x}_{N_k+2},...,\boldsymbol{x}_\omega$ 中的对应元素均为 0,其中,k=1,…,L,N_1≤N_2≤…≤N_L=ω.假设($\{\boldsymbol{f}_e:e\in E\},\{\boldsymbol{K}_t:t\in V\}$)是采用算法 1 为异构网络 G 构造的一个$\mathbb{F}_q$域ω维严格线性散播,下面讨论利用($\{\boldsymbol{f}_e:e\in E\},\{\boldsymbol{K}_t:t\in V\}$)在 G 上传输 $\boldsymbol{x}_1,\boldsymbol{x}_2,…,\boldsymbol{x}_\omega$的优势.

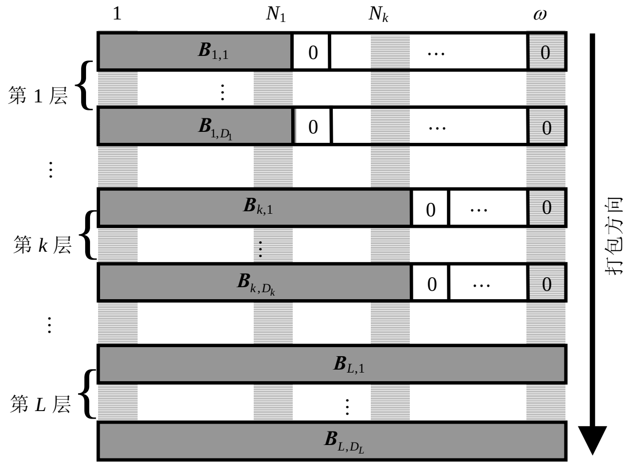


Fig.3 A source-data packetization strategy applicable with strict linear dispersion

图 3 一种适用于严格线性散播的信源数据打包方案

4.1 网络中任意非源节点集/非源节点的部分解码能力

在网络 G 中,任意非源节点集 $T\subset V$ 由其输入链路集$\cup_{t\in T}In(t)$接收到的网络编码数据包为$\{[\boldsymbol{x}_1,\boldsymbol{x}_2,…,\boldsymbol{x}_\omega]\cdot\boldsymbol{f}_d: d\in\cup_{t\in T}In(t)\}$,其中,对应于第 k 信源编码层数据块 $\boldsymbol{B}_{k,i}$ 的元素为$\{\boldsymbol{B}_{k,i}\cdot\boldsymbol{f}_d^{N_k}:d\in\cup_{t\in T}In(t)\}$.

当且仅当 $\dim(\boldsymbol{V}_T^{N_k})=N_k$ 时,根据非源节点集 T 接收到的网络编码数据包可以解码出第 k 信源编码层的所有数据块$\{\boldsymbol{B}_{k,i}:i=1,…,D_k\}$,进而重建出第 k 层对应的原始信源数据.由于($\{\boldsymbol{f}_e:e\in E\},\{\boldsymbol{K}_t:t\in V\}$)是网络 G 的一个$\mathbb{F}_q$域ω维严格线性散播,因此对于任意非源节点集 T,都有 $\dim(\boldsymbol{V}_T^{m_T})=m_T$,其中,$m_T$=min{$\omega$,max$flow(T)$}.此外,对于任意整数 1≤$r$≤$m_T$,都有 $\dim(\boldsymbol{V}_T^r)=r$.因此,对于网络中的任意非源节点集 T,只要 m_T≥N_l,则根据其接收到的网络编码数据包$\{[\boldsymbol{x}_1,\boldsymbol{x}_2,…,\boldsymbol{x}_\omega]\cdot\boldsymbol{f}_d:d\in\cup_{t\in T}In(t)\}$必能解码出前 l 个信源编码层的所有数据块$\{\boldsymbol{B}_{k,i}:i=1,…,D_k,k=1,…,l\}$,进而重建出前 l 个编码层对应的原始信源数据.

特别地,对于网络中的任意非源节点 $t\in V$,只要 m_t≥N_l,则根据其接收到的网络编码数据包$\{[\boldsymbol{x}_1,\boldsymbol{x}_2,…,\boldsymbol{x}_\omega]\cdot\boldsymbol{f}_d: d\in In(t)\}$必能解码出前 l 个信源编码层的所有数据块$\{\boldsymbol{B}_{k,i}:i=1,…,D_k,k=1,…,l\}$,进而重建出前 l 个编码层对应的原始信源数据.因此,本文提出的严格线性散播能够为网络中的任意非源节点提供与其接收能力相匹配的部分解码能力.此结论对于严格线性广播也同样成立.

例 1:假设在如图 1 所示的网络中信源数据编码成 3 层,第 1 层~第 3 层数据分别为$[a_1,a_2]$,$[b_1,b_2]$和$[c_1,c_2,c_3]$.利用如图 3 所示的打包方案将信源数据打包成 3 个数据包 $\boldsymbol{x}_1=[a_1,b_1,c_1]^T$,$\boldsymbol{x}_2=[a_2,b_2,c_2]^T$ 和 $\boldsymbol{x}_3=[0,0,c_3]^T$.下面以节点 t_5 的接收及解码情况为例,比较线性散播和严格线性散播为网络节点提供的部分解码能力.若利用如图 1(a)所示的 3 维线性散播在网络中传输信源数据包 $\boldsymbol{x}_1\boldsymbol{x}_2\boldsymbol{x}_3$,则节点 t_5 由输入链路 t_2t_5 和 t_3t_5 接收到的网络编码数据包分别为 $\boldsymbol{y}_{t_2t_5}=[\boldsymbol{x}_1,\boldsymbol{x}_2,\boldsymbol{x}_3]\boldsymbol{f}_{t_2t_5}=[a_1+a_2,b_1+b_2,c_1+c_2]^T$ 和 $\boldsymbol{y}_{t_3t_5}=[\boldsymbol{x}_1,\boldsymbol{x}_2,\boldsymbol{x}_3]\boldsymbol{f}_{t_3t_5}=[0,0,c_3]^T$.此时,节点 t_5 不能完整地解码出任何信源编码层,因此不能重建出任何信源数据.若利用如图 1(b)所示的 3 维严格线性散播在网络中传输信源数据包 $\boldsymbol{x}_1\boldsymbol{x}_2\boldsymbol{x}_3$,则节点 t_5 由输入链路 t_2t_5 和 t_3t_5 接收到的网络编码数据包分别为 $\boldsymbol{y}'_{t_2t_5}=[\boldsymbol{x}_1,\boldsymbol{x}_2,\boldsymbol{x}_3]\boldsymbol{f}'_{t_2t_5}=[a_1+a_2,b_1+b_2,c_1+c_2]^T$ 和 $\boldsymbol{y}'_{t_3t_5}=[\boldsymbol{x}_1,\boldsymbol{x}_2,\boldsymbol{x}_3]\boldsymbol{f}'_{t_3t_5}=[2a_1+a_2,2b_1+b_2,2c_1+c_2+c_3]^T$.此时,节点 t_5 能解码出第 1 信源编码

层$[a_1,a_2]$和第 2 信源编码层$[b_1,b_2]$,因此能够以一定质量重建出原始信源数据.

此例表明,即使采用如图 3 所示的信源数据打包方案,普通线性散播也无法保证异构网络中任意非源节点接收到的网络编码数据具有部分解码能力.然而,结合此信源数据打包方案,本文提出的严格线性散播(严格线性广播)却能够保证网络中的任意非源节点均能获得与其接收能力相匹配的部分解码能力.

4.2 简化网络拓扑结构扩展后的网络编码设计

假设在网络 G 附近存在一个子网络 $G_1=(V_1,E_1,s_1)$,且 G_1 中信宿希望接收到网络 G 中源节点 s 生成的部分信源编码层.为了满足子网络 G_1 中接收节点的需要,一种最直接的网络编码设计方案,是在扩展后的整个网络 $G'=G+G_1$ 上重新设计网络编码.然而,如果在原网络 G 中采用了如图 3 所示的打包方案,将 s 生成的 L 层信源编码数据构造成ω个数据包 $\boldsymbol{x}_1,\boldsymbol{x}_2,\dots,\boldsymbol{x}_\omega$,且利用一个$\mathbb{F}_q$域$\omega$维严格线性散播($\{\boldsymbol{f}_e:e\in E\},\{\boldsymbol{K}_t:t\in V\}$)进行传输,则能够简化网络拓扑结构扩展后的网络编码设计.此时,网络编码设计的主要步骤为:

1) 根据 G_1 中源节点 s_1 的位置以及 G_1 中信宿需要接收到的信源 s 数据的最大编码层数,将 s_1 与网络 G 中具有相应接收能力的节点集 T 相连.原网络 G 上应用的严格线性散播保证了节点集 T 的解码空间的维数,进而保证了 s_1 能从节点集 T 获得子网络 G_1 中信宿需要的信源 s 的数据;

2) 在子网络 G_1 上独立设计满足传输需求的网络编码.由于 s_1 已从接入节点集 T 获得了子网络 G_1 中所有信宿需求的 s 信源数据,因此,为了实现子网络 G_1 中的信息传输,只需要在 G_1 中独立地设计网络编码,而无需更改原网络 G 上各链路的全局编码核,更不需要在扩展后的整个网络 $G'=G+G_1$ 上重新设计网络编码.

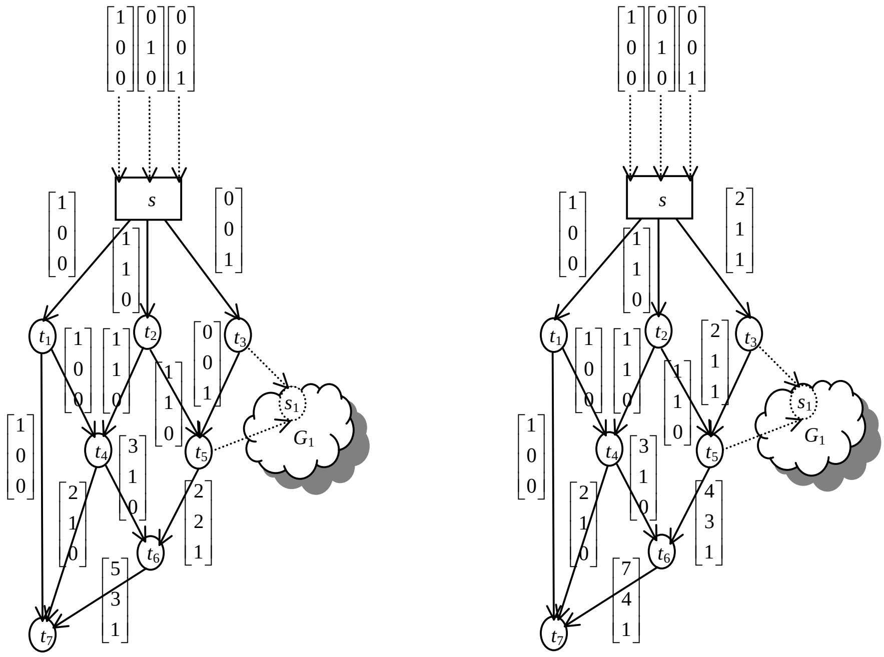
以在 G_1 上实现严格线性散播为例,由定理 2 可知,独立设计 G_1 上的严格线性散播所需的有限域的阶为 $2^{n_1}-1$, 其中,n_1 为子网络 G_1 中非源节点的个数;而在扩展后的整个网络 G' 上重新设计严格线性散播所需的有限域的阶为 $2^{n+n_1}-1$. 因此,原网络 G 上应用的基于严格线性散播的信息传输方案为在接入网络上设计满足传输需求的网络编码提供了便利.相反,若在原网络 G 上应用的是普通线性散播,则其不能保证 G 中各非源节点集的解码空间维数,即无法保证 s_1 能够从原网络中具有相应接收能力的接入节点集获取子网络 G_1 所需的信源 s 的生成数据.因此,子网络 G_1 上的网络编码设计无法独立于原网络 G 进行.

例 2:信源数据采用与例 1 相同的方式打包成 $\boldsymbol{x}_1\boldsymbol{x}_2\boldsymbol{x}_3$.若利用如图 1(b)所示的 3 维严格线性散播进行传输,则节点集$\{t_3,t_5\}$由输入链路 st_3 和 t_2t_5 接收到网络编码数据包分别为 $\boldsymbol{y}'_{st_3}=[\boldsymbol{x}_1,\boldsymbol{x}_2,\boldsymbol{x}_3]\boldsymbol{f}'_{st_3}=[2a_1+a_2,2b_1+b_2,2c_1+c_2+c_3]^T$ 和 $\boldsymbol{y}'_{t_2t_5}=[\boldsymbol{x}_1,\boldsymbol{x}_2,\boldsymbol{x}_3]\boldsymbol{f}'_{t_2t_5}=[a_1+a_2,b_1+b_2,c_1+c_2]^T$. 因此,节点集$\{t_3,t_5\}$能够解码出前 2 个信源编码层$[a_1,a_2]$和$[b_1,b_2]$.若需将图 1(b)所示的网络 G 拓展成为网络 $G'=G+G_1$,子网络 G_1 的位置如图 4 所示,且 G_1 中的信宿需要接收到的最大信源编码层数为 2,则只需将 G_1 中的源节点 s_1 与其附近的节点集$\{t_3,t_5\}$相连(如图 4(b)中虚线所示).此后,只需在子网络 G_1 中独立地设计满足传输需求的网络编码.对比,若利用图 1(a)所示的 3 维线性散播在网络中传输信源数据包 $\boldsymbol{x}_1\boldsymbol{x}_2\boldsymbol{x}_3$,则节点集$\{t_3,t_5\}$由输入链路 st_3 和 t_2t_5 接收到的编码数据包分别为 $\boldsymbol{y}_{st_3}=[\boldsymbol{x}_1,\boldsymbol{x}_2,\boldsymbol{x}_3]\boldsymbol{f}_{st_3}=[0,0,c_3]^T$ 和 $\boldsymbol{y}_{t_2t_5}=[\boldsymbol{x}_1,\boldsymbol{x}_2,\boldsymbol{x}_3]\boldsymbol{f}_{t_2t_5}=[a_1+a_2,b_1+b_2,c_1+c_2]^T$. 此时,节点集$\{t_3,t_5\}$不能解码出任何信源数据编码层.若采用与图 4(b)相同的连接方式将如图 1(a)所示的网络 G 拓展成如图 4(a)所示的网络 $G'=G+G_1$,则 s_1 无法从节点集$\{t_3,t_5\}$获得子网 G_1 所需的信源信息.因此,子网络 G_1 上的网络编码无法独立于原网络 G 而设计.

5 结 论

本文提出了严格线性散播网络编码的概念及其构建算法,并推导出了线性散播与严格线性散播间的转换关系.若在异构网络中利用严格线性散播传输特殊构建的信源数据包,则网络中具有不同接收能力的信宿均能解码出相应数量的信源编码层.此外,严格线性散播的应用还能为异构网络拓扑结构的扩展提供便利.

如何设计严格线性散播的分布式实现方案,以及如何进一步提高基于严格线性散播的多速率信息传输方案的实际传输效率,是我们下一步的研究工作.



(a) 基于$\mathbb{F}_8$域 3 维线性散播的拓扑扩展　　(b) 基于$\mathbb{F}_8$域 3 维严格线性散播的拓扑扩展

Fig.4　Examples for network topology expansion with linear disperesion and strict linear dispersion respectively

图 4　线性散播和严格线性散播在扩展网络拓扑中的应用举例

References:

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

[2] Yeung RW, Li SYR, Cai N, Zhang Z. Network Coding Theory. Now Publishers, 2006. 11−55.

[3] 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]

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

[5] Jaggi S, Sanders P, Chou PA, Effros M, Egner S, Jain K, Tolhuizen 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]

[6] Ho T, Médard 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]

[7] Zhao J, Yang F, Zhang Q, Zhang ZS, Zhang FY. LION: Layered overlay multicast with network coding. IEEE Trans. on Multimedia, 2006,8(5):1021−1032. [doi: 10.1109/TMM.2006.879847]

[8] Sundaram N, Ramanathan P, Banerjee S. Multirate media streaming using network coding. In: Proc. of the 43rd Allerton Conf. on Communication, Control, and Computing. 2005.

[9] Zhang M, Zhang SY, Liu WY. On the optimal multi-rate throughput for multicast. Journal of Electronics and Information Technology, 2008,30(1):16−20 (in Chinese with English abstract).

[10] Si JJ, Zhuang BJ, Cai AN. Optimal layered multicast using network coding. In: Proc. of the 4th Workshop on Network Coding, Theory, and Applications. 2008. 25−30. [doi: 10.1109/NETCOD.2008.4476173]

[11] Yang M, Yang YY. A linear inter-session network coding scheme for multicast. In: Proc. of the 7th IEEE Int'l Symp. on Network Computing and Applications. 2008. 177−184. [doi: 10.1109/NCA.2008.36]

[12] Wu YN. Distributing layered content using network coding. In: Proc. of the 5th IEEE Annual Communications Society Conf. on Sensor, Mesh and Ad Hoc Communications and Networks Workshops. 2008. 1−4. [doi: 10.1109/SAHCNW.2008.28]

[13] Lin YF, Liang B, Li BC. Priority random linear codes in distributed storage systems. IEEE Trans. on Parallel and Distributed Systems, 2009,20(11):1653−1667. [doi: 10.1109/TPDS.2008.251]

[14] Huang Z, Wang X. Research on the optimization problems in network coding. Journal of Software, 2009,20(5):1349−1361 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3505.htm [doi: 10.3724/SP.J.1001.2009.03505]

[15] Wang H, Xiao S, Kuo CCJ. Robust and flexible wireless video multicast with network coding. In: Proc. of the IEEE Global Telecommunications Conf. 2007. 2129−2133. [doi: 10.1109/GLOCOM.2007.407]

[16] Wang H, Kuo CCJ. Robust video multicast with joint network coding and AL-FEC. In: Proc. of the IEEE Int'l Symp. on Circuits and Systems. 2008. 2062−2065. [doi: 10.1109/ISCAS.2008.4541854]

[17] Ramasubramonian AK, Woods JW. Video multicast using network coding. In: Proc. of the Visual Communications and Image Processing. 2009. [doi: 10.1117/12.805588]

[18] Si JJ, Zhuang B, Cai A. Scalable broadcast with network coding in heterogeneous netoworks. The Journal of China Universities of Posts and Teleco Si JJ, Zhuang B, Cai A. mmunications, 2010,17(5):72-79. [doi: 10.1016/S1005-8885(09)60510-0]

[19] Shao MK, Wu XL, Sarshar N. Rainbow networkflow with network coding. In: Proc. of the 4th Workshop on Network Coding, Theory, and Applications. 2008. 115−120. [doi: 10.1109/NETCOD.2008.4476189]

[20] Tan M, Yeung RW, Ho ST. A unified framework for linear network codes. In: Proc. of the 4th Workshop on Network Coding, Theory, and Applications. 2008. 132−136. [doi: 10.1109/NETCOD.2008.4476192]

[21] Wang J, Liu JM, Wang XM. Performance analysis of multicast routing algorithm based on network coding. Journal of Electronics and Information Technology, 2008,30(11):2605−2608 (in Chinese with English abstract).

[22] Fong SL, Yeung RW. Variable-Rate linear network coding. IEEE Trans. on Information Theory, 2010,56(6):2618−2625. [doi: 10.1109/TIT.2010.2046215]

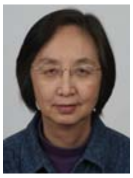
附中文参考文献:

[9] 张牧,张顺颐,刘伟彦.多速率多播最大吞吐量问题研究.电子与信息学报,2008,30(1):16−20.

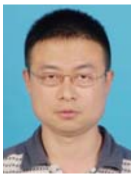
[14] 黄政,王新.网络编码中的优化问题研究.软件学报,2009,20(5):1349−1361. http://www.jos.org.cn/1000-9825/3505.htm [doi: 10.3724/SP.J.1001.2009.03505]

[21] 王静,刘景美,王新梅.基于网络编码的多播路由算法性能分析.电子与信息学报,2008,30(11):2605−2608.

司菁菁(1980－),女,河北秦皇岛人,博士,讲师,主要研究领域为多媒体通信,网络编码.



蔡安妮(1943－),女,博士,教授,博士生导师,主要研究领域为多媒体通信,模式识别.



庄伯金(1976－),男,博士,副教授,主要研究领域为多媒体通信,小波分析,网络编码.