

双单播网络编码的构造方法

蒲保兴, 莫智懿

(梧州学院大数据与软件工程学院, 广西 梧州 543002)

摘要: 为在双单播网络中运用网络编码技术进行数据传输, 提出了一种双单播网络编码的构造方法。所提方法在源点实施预编码策略, 采用随机线性网络编码方法并结合多目标优化进化算法来设计各信道的局部编码向量; 在宿点运用矩阵零空间的基向量来消除部分信息干扰, 再运用二级预编码策略来控制源点的发送速率, 从而能够解码。所提方法不仅能确定双单播网络编码的近似可达信息率区域, 还能为可达信息率区域中的每一向量构造可行的传输方案。理论推导与仿真计算表明了所提方法的有效性。

关键词: 双单播网络编码; 随机线性网络编码; 可达信息率区域; 源点预编码策略; 矩阵的零空间

中图分类号: TP911

文献标识码: A

doi: 10.11959/j.issn.1000-436x.2020139

Construction method of double unicast network coding

PU Baoxing, MO Zhiyi

School of Data Science and Software Engineering, Wuzhou University, Wuzhou 543002, China

Abstract: In order to use network coding technology for data transmission in double unicast network, a construction method of double unicast network coding was proposed. The pre-coding strategy was implemented at each source node, the random linear network coding combined to the multi-objective optimization evolutionary algorithm was adopted to design the local coding vector of each channel. At the each sink node, the base vector of zero space of matrix was used to eliminate some information interference, and then the two-level pre-coding strategy was used to control the transmission rate at source. Thus, each sink node could be decoded successfully. With the proposed method, the approximate reachable information rate region of double unicast network coding could be determined and the transmission scheme for each vector in the reachable information rate region could be designed. Theoretical derivation and simulation calculation show the effectiveness of the proposed method.

Key words: double unicast network coding, random linear network coding, reachable information rate region, pre-coding strategy of source node, zero space of matrix

1 引言

单源网络编码^[1-3]已经得到了深入广泛的研究, 并获得了较好的研究成果。对于多源网络编码^[4]而言, 尽管其已被学术界长期关注并被持续地研究, 但仍没有获得突破性的进展。虽然多源网络编码是一个相当困难的问题, 但多单播网络编码^[5]是多源网络编码中一种比较容易的情形。文献[6]的研究表

明, 任意一个多源有向无环网络必定存在一个相应的多单播网络, 两者具有等价的网络编码可解性。即如果在其中一个网络上存在可行的线性网络编码传输方案, 则在另一个网络上必定存在相应的可行线性的网络编码传输方案。因此, 研究多单播网络编码不仅是网络编码技术应用于多单播网络的需要, 也是解决一般多源网络编码问题的有效途径。据此, 学术界的研究重点已转移到了多单播网

收稿日期: 2020-02-21; 修回日期: 2020-06-05

通信作者: 莫智懿, mofly_0214@126.com

基金项目: 广西创新驱动发展专项基金资助项目 (No.AA18118036)

Foundation Item: Guangxi Innovation-Driven Development Special Fund Project (No.AA18118036)

络编码的层面上。在多单播网络编码中，最简单的情形是双单播网络编码^[7-9]。在已有的研究中，许多学者试图运用信息论技术及图论的工具来探索双单播网络编码的可达信息率区域。文献[10]的研究表明，2个嵌套信息的容量区域是可以描述的，这2个信息中一个被称为公有消息，另一个被称为私有消息，其中，公有消息可拥有3个接收者，私有消息可拥有无数个接收者。文献[11]的研究表明，关于信息的描述，线性网络编码对多源网络是不充分的。文献[12]推导了双单播网络在实现发送速率向量(1,1)的充要条件。文献[13]提出了双单播网络的广义网络共享界(generalized network sharing outer bound)。文献[14]分析了广义的网络共享界在某些特殊的双单播网络中的紧致性。文献[15]和文献[16]针对双单播网络编码的广义网络共享界分别给出了代数解析和网络级联解析。但文献[7]已经证明，求解多单播网络编码的可达信息率区域是一个NPC问题(non-deterministic polynomial complete problem)，即使求解最简单的双单播网络编码，也是NPC问题。该文还表明，双单播网络编码并不比 k ($k>2$, k 是网络中存在的源-宿对的数目)单播网络编码来得容易，即双单播网络编码完全体现了多单播网络编码的困难度。在实际应用中，一方面，需要对双单播网络编码进行求解，另一方面，求出其精确解又是一个NPC问题，从而探索出近似的、较优的可行解技术是解决这一问题的有效途径。

已有的研究尽管关注双单播网络编码的可达信息率区域的计算，但忽略了网络编码的构造。由于多源问题的困难性，即使运用信息论或图论的相关技术能求出近似的可达信息率区域，但针对可达信息率区域中的某一个点(即选定一个特定可行的源点数据发送速率向量)，构造相应的可行的网络编码数据传输方案仍然相当困难。换句话说，若仅估算出了可达信息率区域，针对该区域中的二维向量仍然难以构造相应的网络编码数据传输方案。这与单源网络编码完全不同，对于单源网络编码而言，只要源点的数据发送速率不超过最大流-最小割界，则存在有效的算法来构造可行的网络编码数据传输方案。其主要原因是单源网络编码只有一个源点，不存在消息干扰；但对于具有多个源点的网络而言，宿点接收到的信息是各源点消息的线性组合，即存在消息干扰。若只求出了近似的可达信息率区域，而没有给出构造传输方案的方法，则该方

法仅有理论价值，没有实际应用的价值。因此，从实际应用的角度出发，应该把这2个问题给合起来进行研究，不仅要给出近似的可达信息率区域，还要给出可达信息率区域中各发送速率向量对应的网络编码数据传输方案。

解决双单播网络编码问题的关键是让宿点消除干扰，文献[9]运用源点预编码策略作用于双单播网络的信息不等式提出了求解双单播网络编码近似可达信息率区域的方法，但该方法仅对文献[17]提出的双单播网络的可达信息率区域所满足的信息不等式实现了可计算化，未涉及网络编码的构造。

本文的贡献如下。基于文献[9]的思想，即在源点进行预编码，使宿点接收到的全局编码矩阵的某些列强迫为零列，把文献[18]提出的线性网络编码的导出技术由单源情形扩展到了双单播网络情形，并从源点预编码和信息熵的角度严格证明了导出技术的正确性。在此基础上，本文采用多目标优化进化算法并结合随机线性网络编码技术来形成传输方案，提出了选择预编码矩阵的策略：用宿点的信息转换矩阵的零向量空间的基向量和行向量空间的基向量共同来确定预编码矩阵的列向量，从而使宿点的全局编码矩阵的某些列变为全零列，在宿点消除了部分信息干扰。根据双单播情形下的网络编码的导出技术，运用二级预编码策略来控制源点的发送速率。结合以上策略，本文提出了双单播网络编码的构造方法。所提方法不仅能求出双单播网络编码的近似可达的信息率区域，同时针对求出的可达信息率区域中的任何一个整数坐标点，还提供了构造可行的网络编码数据传输方案的具体方法。

2 预备知识

双单播网络编码^[8]。在一个有向无环网络 $G=(V,E)$ 中， V 为节点集， E 为有向边集。假设网络中有向边的容量为整数，单位容量的有向边称为信道，若有向边的容量大于1，则被看作多条单位容量的信道。网络中有2个源点 $\{s_1, s_2\} \subset V$ ，2个宿点 $\{t_1, t_2\} \subset V$ ，宿点 t_i ($i=1,2$)只需要接收来自源点 s_i 的信息，在数据传输过程中共享网络的传输资源，网络的中间节点运用网络编码技术来转发数据。双单播网络编码如图1所示，其中， \mathbf{X}_i ($i=1,2$)表示源点 s_i 发送的字符向量， $\mathbf{Y}_i = \mathbf{M}_1 \mathbf{X}_1 + \mathbf{M}_2 \mathbf{X}_2$ 表示宿点 t_i 接收到的字符向量，其具体的含义见后续的说明。

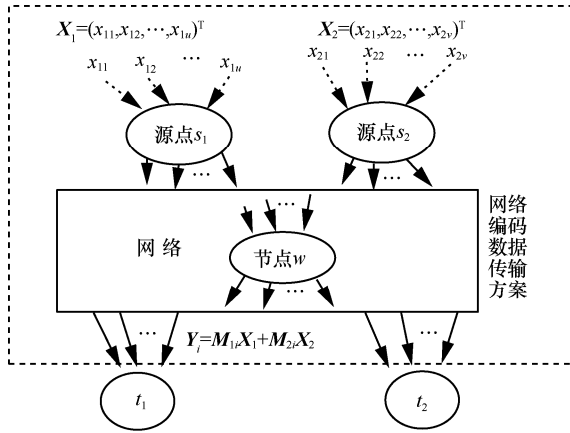


图 1 双单播网络编码

网络编码的工作机理^[1]如下。选定有限域 $GF(q)$ (其中 q 为 2 的幂), 在一次数据传输过程中, 源点 s_1 发送了有限域 $GF(q)$ 中的 u 个字符至网络, 这 u 个字符形成一个字符向量, 记为 \mathbf{X}_1 , 如式(1)所示。

$$\mathbf{X}_1 = (x_{11}, x_{12}, \dots, x_{1u})^T \quad (1)$$

源点 s_2 发送有限域 $GF(q)$ 中的 v 个的字符至网络, 这 v 个字符形成一个字符向量, 记为 \mathbf{X}_2 , 如式(2)所示。

$$\mathbf{X}_2 = (x_{21}, x_{22}, \dots, x_{2v})^T \quad (2)$$

把 2 个源点发送的字符看作一个 $u+v$ 维的列向量, 如式(3)所示。

$$\mathbf{X} = \begin{pmatrix} \mathbf{X}_1 \\ \mathbf{X}_2 \end{pmatrix} \quad (3)$$

为了描述方便, 本文认为源点 s_1 发送的 u 个字符由源点 s_1 的 u 条虚拟输入信道分别输入; 源点 s_2 发送的 v 个字符由源点 s_2 的 v 条虚拟输入信道分别输入。由此可知每一个节点 (包括源点) 均具有输入信道, 如图 1 所示。在数据传输过程中, 各中间节点 (不包括宿点) 把从其输入信道接收到的字符经线性组合后再转发至该节点的输出信道。对于每一条信道 $e_i \in E$ (记信道的尾节点 $\text{tail}(e_i)=k$, 信道的头节点 $\text{head}(e_i)=l$, 其中, $k, l \in V$), 该信道上传输的字符记为 y_{e_i} , 则根据文献[1], 通过式(4)计算 y_{e_i} , 称 $\{f_{j,i}, e_j | \text{head}(e_j)=k\}$ 为信道 e_i 的局部编码向量。

$$y_{e_i} = \sum_{\{e_j | \text{head}(e_j)=k\}} f_{j,i} y_{e_j} \quad (4)$$

定义 1 对于双单播网络编码, 所有节点的输出信道的局部编码向量组成一个集合, 称为网络编码数据传输方案。

在本文中, 网络编码数据传输方案用符号 θ 表示, 为了叙述简洁, 简称为“传输方案 θ ”。

由于有向无环图的拓扑特征, 按照网络节点的拓扑顺序, 节点输出信道传输的字符按式(4)进行递归与迭代运算, 则每一信道所传输的字符必定能表示成源点所发送的信息字符的线性组合, 如式(5)所示。

$$y_{e_i} = \sum_{j=1}^u \alpha_{e_i,j} x_{1j} + \sum_{j=1}^v \beta_{e_i,j} x_{2j} \quad (5)$$

其向量形式如式(6)所示。

$$y_{e_i} = (\alpha_{e_i,1}, \alpha_{e_i,2}, \dots, \alpha_{e_i,u}, \beta_{e_i,1}, \beta_{e_i,2}, \dots, \beta_{e_i,v}) \mathbf{X} \quad (6)$$

其中, \mathbf{X} 是源点发送的字符向量, 如式(3)所示。称 $\mathbf{Y}_{e_i} = (\alpha_{e_i,1}, \alpha_{e_i,2}, \dots, \alpha_{e_i,u}, \beta_{e_i,1}, \beta_{e_i,2}, \dots, \beta_{e_i,v})$ 为信道 e_i 的全局编码向量。对于网络中的任意一个节点, 把其每一条输入信道的全局编码向量作为矩阵的一行, 形成一个矩阵, 则这个矩阵为该节点的全局编码矩阵。

由前文可知, 式(5)或式(6)描述了信道 e_i 传输的字符、信道的全局编码向量 \mathbf{Y}_{e_i} 和源点发送的字符向量 \mathbf{X} 三者之间的数学关系。类似于计算信道传输的字符, 信道的全局编码向量可以按式(7)进行计算。

$$\mathbf{Y}_{e_i} = \sum_{\{e_j | \text{head}(e_j)=k\}} f_{j,i} \mathbf{Y}_{e_j} \quad (7)$$

如果采用随机线性网络编码方法传输数据, 则信道 e_i 传输的信息包括两方面的内容: 信道传输的字符和信道的全局编码向量, 它们分别通过式(4)和式(7)进行计算。

在按式(4)和式(7)所示的递归与迭代计算过程中, 根据网络的拓扑顺序, 首先需要计算源点输出信道的全局编码向量和传输的字符, 源点 s_1 的 u 条虚拟输入信道携带的字符分别为 $x_{11}, x_{12}, \dots, x_{1u}$, 则它们的全局编码向量分别为 $u+v$ 维的单位向量, 其中第 i ($i=1, 2, \dots, u$) 条虚拟输入信道的全局编码向量的第 i 个分量为 1, 其余分量为 0。则源点 s_1 的全局编码矩阵为 $(\mathbf{I}_{u \times u} \mathbf{0}_{u \times v})$, 其中, $\mathbf{I}_{u \times u}$ 是 u 阶的单位矩阵, $\mathbf{0}_{u \times v}$ 是 u 行 v 列的零矩阵。

同理, 源点 s_2 的全局编码矩阵为 $(\mathbf{0}_{v \times u} \mathbf{I}_{v \times v})$ 。

对于某一个宿点 t_i , 选定 δ_i 条输入信道, 根据式(6)的对应关系, 把输入信道的全局编码向量、信道传输的字符、源点发送的字符进行关联, 将形成一个线性方程组。宿点 t_i 的 δ_i 条输入信道的全局编码矩阵的分块矩阵形式为 $(\mathbf{M}_{i1} \mathbf{M}_{i2})$, 宿点 t_i 的 δ_i 条

输入信道所传输的字符形成的向量为 Y_i , 则 Y_i 可以通过式(8)进行计算。

$$Y_i = (M_{1i} \ M_{2i})X \quad (8)$$

其中, Y_i 是一个 δ_i 维的列向量; $(M_{1i} \ M_{2i})$ 是一个 δ_i 行 $u+v$ 列的矩阵, M_{1i} 是源点 s_1 的虚拟输入信道至宿点 t_i 的消息转换矩阵, M_{2i} 是源点 s_2 的虚拟输入信道至宿点 t_i 的消息转换矩阵。 Y_i 、 M_{1i} 和 M_{2i} 中的元素均为有限域 $GF(q)$ 中的字符。

如前所述, 由于源点 s_1 的全局编码矩阵为 $(I_{u \times u} \ \mathbf{0}_{u \times v})$, 源点 s_2 的虚拟输入信道的全局编码矩阵为 $(\mathbf{0}_{v \times u} \ I_{v \times v})$, 在传输方案 θ 指引下, 各信道的全局编码向量按式(7)进行计算。注意到, 式(7)与式(4)的形式相同, 式(7)是在式(4)的基础上把信道上传输的字符 y_{e_j} 换成信道的全局编码向量 Y_{e_j} , 从而宿点 t_i 的全局编码矩阵的计算为

$$H_i = M_{1i}(I_{u \times u} \ \mathbf{0}_{u \times v}) + M_{2i}(\mathbf{0}_{v \times u} \ I_{v \times v}) = (M_{1i} \ M_{2i})$$

这就表明, 分别按式(4)和式(7)计算信道携带的字符和全局编码向量能够满足式(5)的对应关系, 因此可得式(8)即为宿点 t_i 所析出的线性方程组。

性质 1 选择双单播网络的传输方案 θ , 则宿点 $t_i (i=1,2)$ 的全局编码矩阵 $(M_{1i} \ M_{2i})$ 由传输方案 θ 唯一确定。

采用网络编码技术传输数据必须要构造网络编码数据传输方案 θ , 即确定各信道的局部编码向量, 也称为网络编码构造。构造传输方案包括 2 个任务: 首先要确定源点的数据发送速率, 然后针对选定的源点数据发送速率来确定各信道的局部编码向量。对于双单播网络, 因有 2 个源点, 2 个源点的数据发送速率形成了一个二维向量, 称之为源点数据发送速率向量。选定了源点数据发送速率向量后, 接下来的任务是如何确定传输方案 θ , 按照传输方案 θ 中指定的局部编码向量进行数据传输后, 使宿点能够通过求解线性方程组来恢复源点发送的消息。

定义 2 针对双单播网络, 对于给定的源点数据发送速率向量 (u,v) , 若存在相应的传输方案, 使宿点通过解码能获得所需的消息, 则称 (u,v) 是可达的, 该传输方案是可行的, 所有可达的源点数据发送速率向量组成的集合称为可达信息率区域^[4]。

解决双单播网络编码的构造问题首先需要确定可达信息率区域, 然后针对可达信息率区域中的每一点, 再构造相应的可行的传输方案。因为存在

s_1-t_1 和 s_2-t_2 这 2 个会话, 它们共享网络资源, 形成了一种竞争的态势, 从而求解双单播网络编码的可达信息率区域的问题是一个双目标优化问题, 可达信息率区域是双目标优化问题的 Pareto 集。

设源点 s_i 至宿点 t_i 的最大流为 $\min\text{-cut}(s_i, t_i)$ ($i=1,2$), 记 $k_{1-1}=\min\text{-cut}(s_1, t_1)$, $k_{2-2}=\min\text{-cut}(s_2, t_2)$ 。记 $\{s_1, s_2\}$ 至 t_1 的最大流为 k_{12-1} , $\{s_1, s_2\}$ 至 t_2 的最大流为 k_{12-2} 。由最大流最小割定理, 可限制源点 s_1 的数据发送速率的取值范围为 $[0, k_{1-1}]$ 。同理, 可限制源点 s_2 的数据发送速率的取值范围为 $[0, k_{2-2}]$ 。本文只考虑源点发送速率为整数的情况。

本文采用以下策略来寻求可达信息率区域: 选定 $(u,v) \in ([0, k_{1-1}] \times [0, k_{2-2}])$, 其中, u 和 v 均为整数。针对源点数据发送率向量 (u,v) 寻找可行的数据传输方案, 如能找到, 则 (u,v) 是可达的, 记下相应的网络编码数据传输方案。对所有 $(u,v) \in ([0, k_{1-1}] \times [0, k_{2-2}])$ 进行判断, 则可以获得可达信息率区域。

宿点需要通过解码获得源点发送的消息, 则必须求解式(8)所示的线性方程组。将式(8)表示为 $AX=B$ 的形式, 其中系数矩阵 $A=(M_{1i} \ M_{2i})$ 为 m 行 n 列矩阵, $n=u+v$ 。

若系数矩阵 A 中某一列的元素全为零, 则称之为全零列, 表明该列对应的未知量不存在, 其含义为该列所对应的由源点发送的字符没有传输至宿点, 只有系数矩阵的非全零列才对应一个未知量。关于线性方程组求解, 文献[20]给出了如下定理。

定理 1 记 $\text{rank}(A)$ 为矩阵 A 的秩, 对于线性方程组 $AX=B$, 若系数矩阵不存在全零列, 则线性方程组有解的充要条件为 $\text{rank}(A)$ 等于系数矩阵的列数。

针对系数矩阵存在全零列的情况, 有如下推论。

推论 1 对于线性方程组 $AX=B$, 记 $\pi(A)$ 为矩阵 A 中非全零列的列数, 则线性方程组有解的充要条件为 $\text{rank}(A)=\pi(A)$ 。

推论 1 的成立是明显的, 因为只要去掉系数矩阵的全零列, 同时去掉全零列所对应的未知量, 则可以满足定理 1 的条件。

下面, 叙述矩阵的行空间与零空间的概念^[20]。矩阵 A 的列空间就是由矩阵 A 的列向量所张成的 m 维向量空间的一个线性子空间, 记为 $R(A)$; 矩阵 A 的行空间就是由矩阵 A 的所有行向量所张成的 n 维向量空间的一个线性子空间, 记为 $R(A^T)$ 。

矩阵 A 的零空间是由齐次线性方程组 $AX=0$ 的所有解张成的 n 维向量空间的一个线性子空间, 记

为 $N(\mathbf{A})$ 。由零空间的定义可得,对于任意的 $\mathbf{y} \in N(\mathbf{A})$, 满足 $\mathbf{A}\mathbf{y}=\mathbf{0}$ 。

根据线性代数的理论可知,矩阵 \mathbf{A} 的行空间与零空间互为正交补,矩阵 \mathbf{A} 的行空间与零空间的和构成了 n 维的向量空间。

3 源点预编码技术及网络编码的导出

3.1 源点的预编码

如图 1 所示,选择传输方案 θ , 宿点 t_1 选定其 k_{12-1} 条输入信道,宿点 t_2 选定其 k_{12-2} 条输入信道(即 $\delta_1 = k_{12-1}, \delta_2 = k_{12-2}$)。根据式(8)可知,宿点 t_1 和 t_2 对应的线性方程组分别为

$$\mathbf{Y}_1 = \mathbf{M}_{11}\mathbf{X}_1 + \mathbf{M}_{21}\mathbf{X}_2 = (\mathbf{M}_{11} \ \mathbf{M}_{21}) \begin{pmatrix} \mathbf{X}_1 \\ \mathbf{X}_2 \end{pmatrix} \quad (9)$$

$$\mathbf{Y}_2 = \mathbf{M}_{12}\mathbf{X}_1 + \mathbf{M}_{22}\mathbf{X}_2 = (\mathbf{M}_{12} \ \mathbf{M}_{22}) \begin{pmatrix} \mathbf{X}_1 \\ \mathbf{X}_2 \end{pmatrix} \quad (10)$$

如前所述, $\mathbf{M}_{ij}(i,j=1,2)$ 是源点 i 至宿点 j 的信息转换矩阵。其中, \mathbf{M}_{11} 是 k_{12-1} 行 u 列矩阵, \mathbf{M}_{21} 是 k_{12-1} 行 v 列矩阵。 \mathbf{M}_{12} 是 k_{12-2} 行 u 列矩阵, \mathbf{M}_{22} 是 k_{12-2} 行 v 列矩阵, \mathbf{Y}_1 和 \mathbf{Y}_2 分别是 k_{12-1} 维和 k_{12-2} 维的列向量。由性质 1, $\mathbf{M}_{ij}(i,j=1,2)$ 由传输方案 θ 唯一确定。

传输方案 θ 中是在源点实施预编码。源点的预编码不是直接把消息字符分别注入源点的虚拟输入信道,而是把消息字符经过线性组合后再分别注入源点的虚拟输入信道,如图 2 所示。

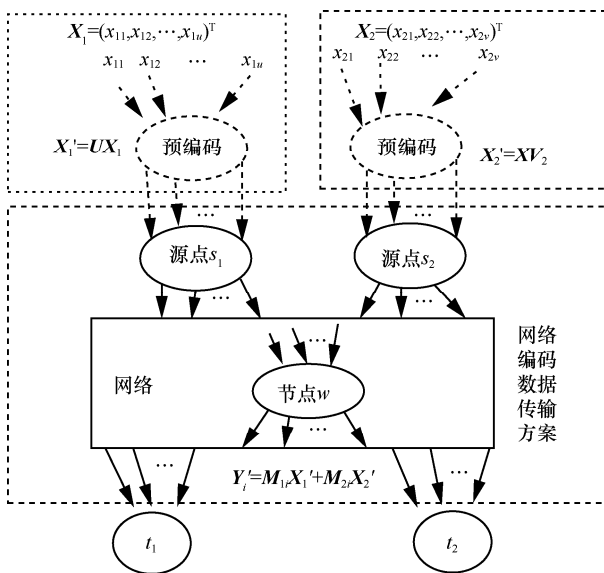


图 2 双单播网络编码的源点预编码

对于源点 s_1 , 假设要传输的消息字符向量如式(1)所示,先对这 u 个字符进行预编码,其编码方式如下。

$$\begin{aligned} x_{11}' &= \rho_{11}x_{11} + \rho_{12}x_{12} + \dots + \rho_{1u}x_{1u} \\ x_{12}' &= \rho_{21}x_{11} + \rho_{22}x_{12} + \dots + \rho_{2u}x_{1u} \\ &\vdots \\ x_{1u}' &= \rho_{u1}x_{11} + \rho_{u2}x_{12} + \dots + \rho_{uu}x_{1u} \end{aligned}$$

记 $\mathbf{X}'_1 = (x'_{11}, x'_{12}, \dots, x'_{1u})^T$, 则编码方式简记为

$$\mathbf{X}'_1 = \mathbf{U}\mathbf{X}_1 \quad (11)$$

其中, \mathbf{U} 表示一个 u 阶方阵, 每一个系数均为有限域 $\text{GF}(q)$ 的元素, 也称为预编码矩阵。

同理, 可以在源点 s_2 实施预编码, 设预编码矩阵为 v 阶方阵 \mathbf{V} , 经预编码后形成的字符向量如式(12)所示。

$$\mathbf{X}'_2 = \mathbf{V}\mathbf{X}_2 \quad (12)$$

现在把向量 \mathbf{X}'_1 中的分量分别注入源点 s_1 的虚拟输入信道, 其全局编码矩阵为 $(\mathbf{U} \ \mathbf{0}_{u \times v})$; 把向量 \mathbf{X}'_2 中的分量分别注入源点 s_2 虚拟输入信道, 其全局编码矩阵为 $(\mathbf{0}_{v \times u} \ \mathbf{V})$ 。再按传输方案 θ 进行数据传输, 则宿点 t_1 和 t_2 接收的信息字符向量分别按式(13)和式(14)计算。

$$\mathbf{Y}'_1 = \mathbf{M}_{11}\mathbf{X}'_1 + \mathbf{M}_{21}\mathbf{X}'_2 \quad (13)$$

$$\mathbf{Y}'_2 = \mathbf{M}_{12}\mathbf{X}'_1 + \mathbf{M}_{22}\mathbf{X}'_2 \quad (14)$$

在实施预编码的前提下, 若再次对 \mathbf{X}'_1 和 \mathbf{X}'_2 实施预编码, 则称为二级预编码。

3.2 网络编码的导出

文献[18]提出了单源多播网络的线性网络编码的导出与扩展技术, 本文利用源点的预编码技术提出双单播网络的线性网络编码的导出技术。

定义 3 若 u, v, u_1, v_1 均为整数, 且满足 $u_1 \leq u, v_1 \leq v$, 则称 (u_1, v_1) 受控于 (u, v) , 也称 (u, v) 控制 (u_1, v_1) , 记为 $(u_1, v_1) \prec (u, v)$ 。

定义 4 对于双单播网络的一个源点发送率向量为 (u, v) 的传输方案, 在源点 s_1 和 s_2 分别实施式(11)和式(12)所示的预编码, 则从传输方案 θ 中导出了一个新的传输方案, 本文称前者为原始方案, 后者为导出方案。

定理 2 线性网络编码的导出。若一个双单播网络编码的源点发送率向量 (u, v) 是可达的, 则对于任意 (u_1, v_1) , 且 $(u_1, v_1) \prec (u, v)$, (u_1, v_1) 也是可达的,

且从源点可达的发送速率向量 (u,v) 的任何一个可行的网络编码数据传输方案可以导出 (u_1,v_1) 的一个可行的网络编码数据传输方案。

证明 由于 (u,v) 是可达的,必存在一个可行的传输方案 θ 。在其指引下,宿点 t_1 和 t_2 对应的线性方程组分别如式(9)和式(10)所示。在此基础上,分别对源点 s_1 和 s_2 实施如式(11)和式(12)所示的预编码,预编码矩阵 U 和 V 表示如下。

$$U = \begin{pmatrix} I_{u_1 \times u_1} & \mathbf{0}_{u_1 \times (u-u_1)} \\ \mathbf{0}_{(u-u_1) \times u_1} & \mathbf{0}_{(u-u_1) \times (u-u_1)} \end{pmatrix}, V = \begin{pmatrix} I_{v_1 \times v_1} & \mathbf{0}_{v_1 \times (v-v_1)} \\ \mathbf{0}_{(v-v_1) \times v_1} & \mathbf{0}_{(v-v_1) \times (v-v_1)} \end{pmatrix}$$

则宿点 t_1 和 t_2 分别得到如式(13)与式(14)所示的线性方程组。由于 θ 是关于 (u,v) 的一个可行传输方案,则式(9)和式(10)能解出 X_1 和 X_2 。

比较式(9)和式(13)所代表的线性方程组,两者具有相同的系数矩阵,只是未知量与常数项不同,由推论1,则式(9)和式(13)代表的线性方程组具有相同的可解性,同理,式(10)与式(14)表示的线性方程组也具有相同的可解性。因此,式(13)和式(14)能解出 X'_1 和 X'_2 ,其中, $X'_1 = UX_1 = (x_{11}, x_{12}, \dots, x_{1u_1}, 0, \dots, 0)^T$, $X'_2 = VX_2 = (x_{21}, x_{22}, \dots, x_{2v_1}, 0, \dots, 0)^T$ 。这说明了源点 s_1 实际上仅向网络传输了字符向量 $(x_{11}, x_{12}, \dots, x_{1u_1})$,且宿点 t_1 能解码出 $(x_{11}, x_{12}, \dots, x_{1u_1})$ 。同理,源点 s_2 实际上仅向网络传输了字符向量 $(x_{21}, x_{22}, \dots, x_{2v_1})$,且宿点 t_2 可以解码出 $(x_{21}, x_{22}, \dots, x_{2v_1})$ 。由此说明,源点发送速率向量 (u_1, v_1) 是可达的,而且通过源点的预编码,可从可达信息率向量 (u,v) 的一个可行的传输方案 θ 导出关于 (u_1, v_1) 的一个可行的传输方案,且导出的传输方案仅在源点实施预编码,其余信道的局部编码向量与传输方案 θ 相同。证毕。

假设源点产生的消息字符是随机变量,且相互独立,每个字符均匀地在有限域 $GF(q)$ 上选取,若向量 X_1 的维数为 u 、向量 X_2 的维数为 v ,根据信息论可知, $H(X_1)=uq$, $H(X_2)=vq$ (注: $H(\cdot)$ 表示随机变量的香农信息熵, $I(\cdot; \cdot)$ 表示2个随机变量的互熵)。

定理3 对于一个源点的发送速率向量为 (u,v) 的可行传输方案,可以导出一个源点发送速率向量为 (u_1, v_1) 的可行传输方案,其中 $(u_1, v_1) < (u, v)$ 。导出的传输方案只需在源点实施预编码,其他信道的局部编码向量保持不变,且源点 s_1 的预编码矩阵 U 为 u 阶方阵, U 的后 $u \sim u_1$ 列均为全零列,且满足

$\text{rank}(U_1)=u_1$;由对称性,源点 s_2 的预编码矩阵 V 为 v 阶方阵, V 的后 $v \sim v_1$ 列均为全零列,且满足 $\text{rank}(V)=v_1$ 。

证明 源点经过预编码后,2个源点实际上是分别把 $X'_1 = UX_1$ 和 $X'_2 = VX_2$ 传送到网络中,首先证明经过预编码后源点的实际发送率向量为 (u_1, v_1) 。为证明这一结论,只需计算 X'_1 和 X'_2 的熵。由于 U 的后 $u \sim u_1$ 列为全零列,则

$$X'_1 = UX_1 = \begin{pmatrix} \rho_{11} & \rho_{12} & \dots & \rho_{1u_1} & 0 & \dots & 0 \\ \rho_{21} & \rho_{22} & \dots & \rho_{2u_1} & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \rho_{u_1 1} & \rho_{u_1 2} & \dots & \rho_{u_1 u_1} & 0 & \dots & 0 \end{pmatrix} \begin{pmatrix} x_{11} \\ x_{12} \\ \vdots \\ x_{1u} \end{pmatrix} = \begin{pmatrix} \rho_{11} & \rho_{12} & \dots & \rho_{1u_1} \\ \rho_{21} & \rho_{22} & \dots & \rho_{2u_1} \\ \vdots & \vdots & \ddots & \vdots \\ \rho_{u_1 1} & \rho_{u_1 2} & \dots & \rho_{u_1 u_1} \end{pmatrix} \begin{pmatrix} x_{11} \\ x_{12} \\ \vdots \\ x_{1u_1} \end{pmatrix} \quad (15)$$

记 $Z_1 = (x_{11}, x_{12}, \dots, x_{1u_1})^T$,则有 X'_1 的每一个分量可以用 X 的前 u_1 个分量的线性表示,即每一个分量都是 Z_1 的函数,从而 X'_1 是 Z_1 的函数,根据信息论的理论^[19],有 $H(X'_1|Z_1)=0$,此外, $H(X'_1)=I(X'_1; Z_1)+H(X'_1|Z_1)=I(X'_1; Z_1)=H(Z_1)-H(Z_1|X'_1)$,由熵的非负性,则 $H(Z_1|X'_1) \geq 0$,从而得到

$$H(X'_1)=H(Z_1)-H(Z_1|X'_1) \leq H(Z_1) \quad (16)$$

另一方面,由于 U 的秩为 u_1 ,根据矩阵代数的理论,则可以从 U 中的行向量中找到 u_1 行,成为 U 的行向量的极大无关组,本文记它们的行下标分别为 r_1, r_2, \dots, r_{u_1} ,则这 u_1 行对应于 X'_1 的 u_1 个分量,这 u_1 个分量按式(15)所示的对应关系的矩阵形式为

$$\begin{pmatrix} x'_{1r_1} \\ x'_{1r_2} \\ \vdots \\ x'_{1r_{u_1}} \end{pmatrix} = \begin{pmatrix} \rho_{r_1 1} & \rho_{r_1 2} & \dots & \rho_{r_1 u_1} \\ \rho_{r_2 1} & \rho_{r_2 2} & \dots & \rho_{r_2 u_1} \\ \vdots & \vdots & \ddots & \vdots \\ \rho_{r_{u_1} 1} & \rho_{r_{u_1} 2} & \dots & \rho_{r_{u_1} u_1} \end{pmatrix} \begin{pmatrix} x_{11} \\ x_{12} \\ \vdots \\ x_{1u_1} \end{pmatrix} \quad (17)$$

由于极大无关组对应行向量是线性无关的,式(17)中的 u_1 阶矩阵是可逆的。求解式(17)所示的线性方程组,可得 $Z_1 = (x_{11}, x_{12}, \dots, x_{1u_1})^T$ 的每个分量可以被 $(x'_{1r_1}, x'_{1r_2}, \dots, x'_{1r_{u_1}})$ 线性表示,因此 Z_1 也是 X'_1 的函数,与上述证明类似,可以得到

$$H(Z_1) \leq H(X'_1) \quad (18)$$

结合式(16)和式(18), 可得 $H(\mathbf{Z}_1)=H(\mathbf{X}'_1)$ 成立。此外, 由于 \mathbf{Z}_1 中有 u_1 个独立同分布的 $\text{GF}(q)$ 中的字符, 从而得到 $H(\mathbf{Z}_1)=u_1q$, 也即 $H(\mathbf{X}'_1)=u_1q$ 。

同理可证, $H(\mathbf{X}'_2)=v_1q$, 故经预编码后源点实际发送速率向量为 (u_1, v_1) 。

由于式(9)和式(13)具有相同的可解性, 经源点预编码后, 宿点 t_1 可以求解式(13)所示的线性方程组得到 \mathbf{X}'_1 , 利用式(17), 宿点可以恢复出字符向量 \mathbf{Z}_1 ; 同理, 宿点 t_2 可以恢复出字符向量 $\mathbf{Z}_2 = (x_{21}, x_{22}, \dots, x_{2v})^T$, 从而通过源点的预编码技术导出了一个源点发送率向量为 (u_1, v_1) 的可行的传输方案。证毕。

4 基于源点预编码的宿点干扰消除

在源点实施预编码后, 宿点 t_1 和 t_2 分别得到式(13)和式(14)所示的线性方程组。把式(11)和式(12)分别代入式(13)和式(14), 则得到

$$\mathbf{Y}'_1 = \mathbf{M}_{11}\mathbf{U}\mathbf{X}_1 + \mathbf{M}_{21}\mathbf{V}\mathbf{X}_2 \quad (19)$$

$$\mathbf{Y}'_2 = \mathbf{M}_{12}\mathbf{U}\mathbf{X}_1 + \mathbf{M}_{22}\mathbf{V}\mathbf{X}_2 \quad (20)$$

要使式(19)和式(20)能求解, 则需要满足推论 1, 必须让系数矩阵的非全零列的数目 $\pi(\mathbf{A})$ 与矩阵的秩相等。根据秩的性质, 有 $\text{rank}(\mathbf{A}) \leq \pi(\mathbf{A})$; 当 $\text{rank}(\mathbf{A}) < \pi(\mathbf{A})$ 时, 因矩阵的秩不会增加, 则应减小 $\pi(\mathbf{A})$ 的值。如果适当地选取预编码矩阵的元素, 使式(19)和式(20)的系数矩阵出现全零列, 从而达到了减小 $\pi(\mathbf{A})$ 的目标。

宿点 t_1 对应的系数矩阵为 $\mathbf{A} = (\mathbf{M}_{11}\mathbf{U} \ \mathbf{M}_{21}\mathbf{V})$, 其中, $\mathbf{M}_{11}\mathbf{U}$ 和向量 \mathbf{X}_1 对应, 而 \mathbf{X}_1 中的分量是宿点 t_1 所需要的消息; $\mathbf{M}_{21}\mathbf{V}$ 和向量 \mathbf{X}_2 对应, \mathbf{X}_2 是宿点 t_1 不需要的, 可以看作信息干扰。因此, 要使矩阵 \mathbf{A} 出现全零列, 应在 $\mathbf{M}_{21}\mathbf{V}$ 中出现, 且 \mathbf{U} 应为满秩矩阵; 同理, 对于宿点 t_2 , 应让 $\mathbf{M}_{12}\mathbf{U}$ 出现全零列, 且 \mathbf{V} 应为满秩矩阵。

基于以上分析, 预编码矩阵 \mathbf{U} 的选取方法如下。首先求 \mathbf{M}_{21} 的行空间 $R(\mathbf{M}_{21}^T)$, 再求矩阵 \mathbf{M}_{21} 的零空间 $\mathbf{N}(\mathbf{M}_{21})$ 。记 $\tau = \text{rank}(\mathbf{N}(\mathbf{M}_{21}))$, 注意这 2 个子空间互为正交补, 因 \mathbf{M}_{21} 的列数为 v , 从而 $\text{rank}(R(\mathbf{M}_{21}^T)) = v - \tau$ 。记 $\{a_1, a_2, \dots, a_\tau\}$ 为 $\mathbf{N}(\mathbf{M}_{21})$ 的一组基向量, $\{a_{\tau+1}, \dots, a_v\}$ 为 $R(\mathbf{M}_{21}^T)$ 的一组基向量, 则 $\{a_1, a_2, \dots, a_\tau, a_{\tau+1}, \dots, a_v\}$ 构成了 $\text{GF}(q)$ 域上 v 维线性空间的一组基向量, 令预编码矩阵 \mathbf{V} 的列向量分别

取上述的基向量, 如式(21)所示。

$$\mathbf{V} = (a_1 \ a_2 \ \dots \ a_\tau \ a_{\tau+1} \ \dots \ a_v) \quad (21)$$

同理, 求出 u 维向量空间的子空间 $\mathbf{N}(\mathbf{M}_{12})$ 的一组基向量 $\{\beta_1, \beta_2, \dots, \beta_\lambda\}$, 记 $\lambda = \text{rank}(\mathbf{N}(\mathbf{M}_{12}))$, 再求出 $R(\mathbf{M}_{12}^T)$ 的一组基向量 $\{\beta_{\lambda+1}, \beta_{\lambda+2}, \dots, \beta_u\}$, 则预编码矩阵 \mathbf{U} 的列向量如式(22)所示。

$$\mathbf{U} = (\beta_1 \ \beta_2 \ \dots \ \beta_\lambda \ \beta_{\lambda+1} \ \dots \ \beta_u) \quad (22)$$

由于 \mathbf{U} 和 \mathbf{V} 的列向量分别由 u 维向量空间和 v 维向量空间的基向量构成, 从而 \mathbf{U} 和 \mathbf{V} 均为满秩矩阵。

把 \mathbf{U} 和 \mathbf{V} 分别代入式(19)和式(20), 则式(19)中的分块矩阵 $\mathbf{M}_{21}\mathbf{V}$ 至少有前 τ 列为全零列, 式(20)中的分块矩阵 $\mathbf{M}_{12}\mathbf{U}$ 至少有 λ 列为全零列。

5 基于干扰消除的网络编码优化构造

5.1 二级预编码策略

本文采用二级预编码策略, 具体如图 3 所示, 其中, 预编码 1 用于控制源点的实际发送速率, 预编码 2 用于消除宿点的干扰。

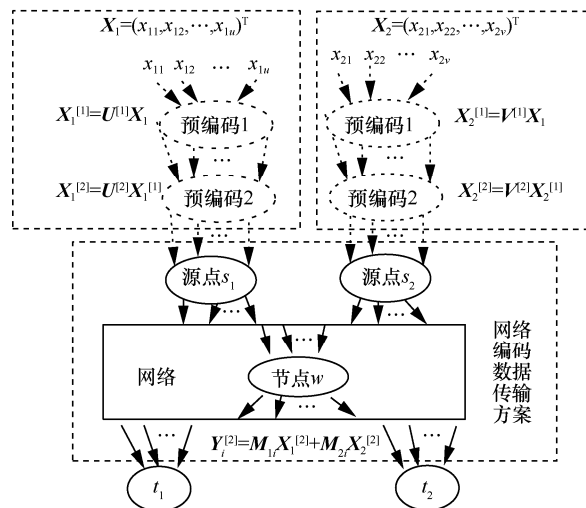


图 3 二级编码策略示意

源点的数据发送速率假设为 (u, v) , 选取传输方案 θ , 在此基础上, 在源点实施如式(23)所示的预编码 1。

$$\mathbf{X}_1^{[1]} = \mathbf{U}^{[1]}\mathbf{X}_1, \mathbf{X}_2^{[1]} = \mathbf{V}^{[1]}\mathbf{X}_2 \quad (23)$$

$\mathbf{U}^{[1]}$ 为 u 阶方阵, 如式(24)所示。

$$\mathbf{U}^{[1]} = \begin{pmatrix} w_1 & 0 & 0 & \dots & 0 \\ 0 & w_2 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & w_u \end{pmatrix} \quad (24)$$

$V^{[1]}$ 为 v 阶方阵，如式(25)所示。

$$V^{[1]} = \begin{pmatrix} z_1 & 0 & 0 & \cdots & 0 \\ 0 & z_2 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & z_v \end{pmatrix} \quad (25)$$

其中， $w_i(i=1,2,\dots,u)$ 和 $z_j(j=1,2,\dots,v)$ 均为 $GF(q)$ 中的元素，其值为 1 或 0。

在实施了预编码 1 的基础上，再在源点实施如式(26)所示的预编码 2。

$$X_1^{[2]} = U^{[2]} X_1^{[1]}, X_2^{[2]} = V^{[2]} X_2^{[1]} \quad (26)$$

把 $X_1^{[2]}$ 的各分量分别注入源点 s_1 的虚拟输入信道，把 $X_2^{[2]}$ 的各分量分别注入源点 s_2 的虚拟输入信道，并按传输方案 θ 的规定实施数据传输，那么宿点 t_i 得到的线性方程组为

$$Y_i^{[2]} = M_{1i} X_1^{[2]} + M_{2i} X_2^{[2]} \quad (27)$$

把式(23)和式(26)代入式(27)，则宿点 t_1 和 t_2 得到的线性方程组分别如式(28)和式(29)所示。

$$Y_1^{[2]} = M_{11} U^{[2]} U^{[1]} X_1 + M_{21} V^{[2]} V^{[1]} X_2 \quad (28)$$

$$Y_2^{[2]} = M_{12} U^{[2]} U^{[1]} X_1 + M_{22} V^{[2]} V^{[1]} X_2 \quad (29)$$

把式(28)写成如式(30)所示形式。

$$Y_1^{[2]} = \begin{pmatrix} M_{11} U^{[2]} & M_{21} V^{[2]} \end{pmatrix} \begin{pmatrix} U^{[1]} & \mathbf{0}_{u \times v} \\ \mathbf{0}_{v \times u} & V^{[1]} \end{pmatrix} \begin{pmatrix} X_1 \\ X_2 \end{pmatrix} \quad (30)$$

把式(29)写成如式(31)所示形式。

$$Y_2^{[2]} = \begin{pmatrix} M_{12} U^{[2]} & M_{22} V^{[2]} \end{pmatrix} \begin{pmatrix} U^{[1]} & \mathbf{0}_{u \times v} \\ \mathbf{0}_{v \times u} & V^{[1]} \end{pmatrix} \begin{pmatrix} X_1 \\ X_2 \end{pmatrix} \quad (31)$$

记式(30)的系数矩阵为 C ，式(31)的系数矩阵为 B 。

记式(22)所示的列向量为 $U^{[2]}$ ，式(21)所示的列向量为 $V^{[2]}$ ，现在来计算 $(M_{11} U^{[2]} \ M_{21} V^{[2]})$ 和 $(M_{12} U^{[2]} \ M_{22} V^{[2]})$ 。因为 $V^{[2]}$ 的前 τ 列是 $N(M_{21})$ 的基向量，则分块矩阵 $M_{21} V^{[2]}$ 的前 τ 列必为全零列；同理，分块矩阵 $M_{12} U^{[2]}$ 的前 λ 列必定为全零列。注意到，矩阵 C 和 B 均是 2 个矩阵的乘积，在相乘的 2 个矩阵中，后者是对角矩阵，因此，根据对角矩阵相乘的特点，若 $\tau \neq 0$ ，则矩阵 C 的第 $u+1, u+2, \dots, u+\tau$ 列必定为全零列；同理，矩阵 B 的前 λ 列必定为全零列。

尽管系数矩阵 C 和 B 中出现了一些全零列，但

不一定能满足推论 1 的条件，接下来，通过选取合适的 $U^{[1]}$ 和 $V^{[1]}$ 中的对角线元素来增加全零列的数目，使式(30)和式(31)能满足推论 1。

根据矩阵相乘的性质，若 $w_i=0$ ，则矩阵 C 和 B 的第 i 列必定为全零列；若 $z_j=0$ ，则矩阵 C 和 B 的第 $u+j$ 列必定为全零列。

由定理 2 和定理 3 可知， $(\sum_{i=1}^u w_i, \sum_{i=1}^v z_i)$ 是源点实际的数据发送速率向量，从而通过检测 $(\sum_{i=1}^u w_i, \sum_{i=1}^v z_i)$ 的可达性来确定源点的可达信息率区域，对于任意整数对 $(u_1, v_1) \in ([0, k_{1-1}] \times [0, k_{2-2}])$ ，令 $\sum_{i=1}^u w_i = u_1, \sum_{i=1}^v z_i = v_1$ ，按以上置零规则来确定 $w_i(i=1,2,\dots,u)$ ， $z_i(i=1,2,\dots,v)$ 的值，则可以形成 $U^{[1]}$ 和 $V^{[1]}$ ，再代入式(30)和式(31)所示的线性方程组，并根据推论 1 来检测这 2 个线性方程组的可解性，如式(30)和式(31)是可解的，则表明 (u_1, v_1) 是可达的，所有的可达发送率向量 (u_1, v_1) 形成可达信息率区域。

置零规则：在需要置 $w_i (i=1,2,\dots,u)$ ， $z_j (j=1,2,\dots,v)$ 的值为零时，应优先选取下标大者的元素。例如，若需设置 w_i 中的一个元素为 0，则应让下标最大的元素 w_u 为 0，其余元素均为 1；若需设置 w_i 中的 2 个元素为 0，则应让下标最大的 2 个元素 w_u 和 w_{u-1} 为 0，其余元素均为 1。

5.2 可达信息率区域边界点及其相应的传输方案

由定理 2 可知，可达信息率区域内部节点的可行传输方案可以由边界点的可行传输方案导出。为了减少计算量，只需要找出可达信息率区域的边界点，并保存相应的网络编码数据传输方案。

可达信息率区域边界点集合的定义具体如下。

设 P 为可达信息率区域， Q 为可达信息率区域的边界点形成的集合， R 为可达信息率区域内部点形成的集合。 R 的定义如下： $\forall (u_1, v_1) \in R$ ，则 $\exists (u_2, v_2) \in P$ ，有 (u_2, v_2) 控制 (u_1, v_1) ，即 $(u_1, v_1) \prec (u_2, v_2)$ ，且 $(u_1, v_1) \neq (u_2, v_2)$ 。则 $Q = P - R$ 就是边界点形成的集合。

为了保存边界点的传输方案，现定义一个二元组 $\langle (x, y), \theta \rangle$ ，其中第一个元素是边界点的二维坐标，第二个元素是这个边界点所依赖的传输方案。记这些二元组形成的集合为 Q' ，其定义为 $Q' = \{ \langle (x, y), \theta \rangle : (x, y) \in Q \}$ 。求边界点集合 Q' 的递归算法如算法 1 所示。

算法 1 求边界点集合 Q' 的递归算法

```

输入  $\langle (x,y), \theta \rangle, Q'$ 
输出  $Q'$ 
juge(int x,int y)
{
if(x==0||y==0)
    {return//递归结束}
end if
if(  $(x,y)$  是可达的)
{
    if( $\exists \langle (u_1,v_1), \theta \rangle \in Q'$ , 且  $(u_1,v_1) \prec (x,y)$ )
        {  $Q' = Q' - \langle (u_1,v_1), \theta \rangle$  }
    end if
    if( $\exists \langle (u_1,v_1), \theta \rangle \in Q'$  且  $(x,y) \prec (u_1,v_1)$ )
        {do nothing}
    else
        {  $Q' = Q' \cup \langle (x,y), \theta \rangle$  }
        return }
    end if
}
}
else
{
    juge(x-1, y)
    juge(x, y-1)
}
}
end if
}

```

5.3 传输方案的优化

本文采用随机线性网络编码方法得到传输方案 θ , 则能唯一地确定 $(M_{11} \ M_{21})$ 和 $(M_{12} \ M_{22})$, 进而唯一确定 $(M_{11} U^{[2]} \ M_{21} V^{[2]})$ 和 $(M_{12} U^{[2]} \ M_{22} V^{[2]})$, 从而它们的全零列的列数 τ 和 λ 可唯一确定, 因此, τ 和 λ 是 θ 的函数, 分别记为 $\tau(\theta)$ 、 $\lambda(\theta)$ 。当 $\tau(\theta)$ 和 $\lambda(\theta)$ 的值较大时, 则在预编码 1 中只需让 w_i 、 z_i 中较少项置 0, 就能使式(30)和式(31)满足推论 1, 则源点的实际发送速率较大。因此, 需要寻找较优的传输方案 θ , 使 $\tau(\theta)$ 和 $\lambda(\theta)$ 的值尽可能大, 这是一个双目标优化问题。

记 Ω 为所有传输方案的集合, 则该双目标优化问题描述如式(32)所示。

$$\begin{aligned}
 & \max (\tau(\theta), \lambda(\theta)) \\
 & \text{s.t. } \theta \in \Omega
 \end{aligned} \tag{32}$$

式(32)所示的双目标优化问题可以通过多目标进化算法来求解。文献[21-22]运用多目标进化算法求最优的网络传输方案的近似解, 也可以采用蒙特卡罗法来求式(32)的近似最优解。本文采用文献[22]类似的方法, 运用了相同的遗传表示, 只是适应度函数与文献[22]不相同, 求出的最优解是一个 Pareto 边界。

5.4 算法描述

算法 2 双单播网络的构造算法

步骤 1 利用 Ford-Fulkerson 算法^[23], 分别求双单播网络的 k_{1-1} 、 k_{2-2} 、 k_{12-1} 、 k_{12-2} 。令 $u=k_{1-1}$ 、 $v=k_{2-2}$, 针对源点的数据发送速率向量 (u,v) , 运用类似文献[22]的方法求出式(32)的近似最优解, 记为 Γ 。

步骤 2 选定近似最优解中的一个传输方案 $\theta \in \Gamma$, 并置 $\Gamma = \Gamma - \{\theta\}$ 。则由 θ 唯一确定 M_{11} 、 M_{21} 、 M_{12} 、 M_{22} 、 $U^{[2]}$ 、 $V^{[2]}$ 、 $(M_{11} U^{[2]} \ M_{21} V^{[2]})$ 和 $(M_{12} U^{[2]} \ M_{22} V^{[2]})$, 并得出 τ 和 λ 值。

步骤 3 针对 θ , 调用算法 1。

步骤 4 判断 Γ 是否为空集, 若不为空集, 则转到步骤 2, 否则算法结束。

算法结束后, Q' 为可达信息率区域的边界点及其相应的传输方案的二元组形成的集合。下面说明这一事实: 若通过算法 2 求出了 Q' , 则① 通过 Q' 可以获得可达信息率区域 P ; ② 对于 $\forall (x,y) \in P$, 可以找出以 (x,y) 为数据发送速率向量的可行传输方案。

首先, 由 Q' 的定义, 可以从集合 Q' 中得到 Q , 进而获得 R , 从而得到 $P=R \cup Q$ 。

对于 $\forall (u_1,v_1) \in Q$, 必存在 $\langle (u_1,v_1), \theta_1 \rangle \in Q'$, 其中 θ_1 表示发送速率向量 (u_1,v_1) 所依赖的传输方案。从算法 1 的求解过程可知, 由传输方案 θ_1 可以唯一确定 M_{11} 、 M_{21} 、 M_{12} 、 M_{22} , 进而唯一确定 $U^{[2]}$ 和 $V^{[2]}$, 由 (u_1,v_1) 可以得出在 $U^{[1]}$ 和 $V^{[1]}$ 需要置零的项数, 再按照置零规则, 则矩阵 $U^{[1]}$ 和 $V^{[1]}$ 唯一确定, 因此, 由传输方案 θ_1 导出的传输方案唯一确定。

对于 $\forall (u_2,v_2) \in R$, 由 R 的定义, 必定存在 $(u_1,v_1) \in Q$, 满足 $(u_2,v_2) \prec (u_1,v_1)$, 由此可知, (u_1,v_1) 导出传输方案唯一确定, 再根据定理 2, 则能够以 (u_1,v_1) 的导出传输方案为基础, 在源点再次进行预编码, 导出关于 (u_2,v_2) 的可行传输方案。由于 $P=R \cup Q$, 则上述结论成立。

综上, 算法 2 特别适用于实际应用场景。从算法的结果 Q' 中不仅能得出可达信息率区域, 且对于区域中的每一点, 能容易地得到相应的可行传输方案。

值得说明的是，由于本文只能求出式(32)的近似最优解，故求出的可达信息率区域也是近似最优的。

6 算例

图4表示一个双单播网络，容易求出 $k_{1-1}=k_{1-2}=k_{12-1}=k_{12-2}=3$ 。选择伽罗华域 $GF(2^3)$ ，其不可约多项式为 x^3+x+1 ，写成二进制形式为(1011)₂。选定源点数据发送率向量为 $(u,v)=(3,3)$ ，现运用随机线性网络编码方法并结合多目标优化的进化策略来确定较优的传输方案，本例只求出了一个传输方案，在该传输方案下，宿点 t_1 和宿点 t_2 的全局编码向量形成的矩阵分别如式(33)和式(34)所示。

$$(M_{11} \ M_{21}) = \begin{pmatrix} 011 & 011 & 100 & \vdots & 000 & 010 & 110 \\ 010 & 111 & 000 & \vdots & 010 & 111 & 111 \\ 001 & 001 & 011 & \vdots & 001 & 111 & 101 \end{pmatrix} \quad (33)$$

$$(M_{12} \ M_{22}) = \begin{pmatrix} 000 & 110 & 100 & \vdots & 000 & 011 & 100 \\ 010 & 100 & 010 & \vdots & 000 & 111 & 010 \\ 011 & 100 & 110 & \vdots & 011 & 011 & 111 \end{pmatrix} \quad (34)$$

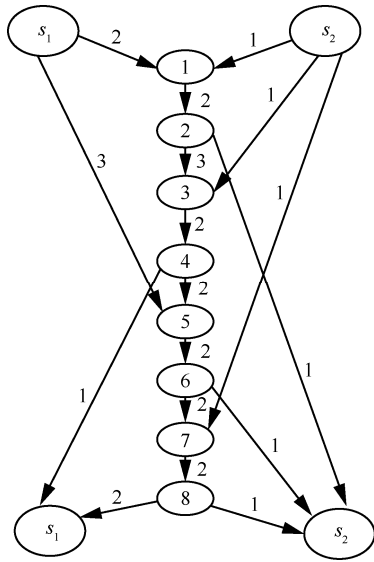


图4 一个双单播网络实例

求出预编码2的预编码矩阵，如式(35)所示。

$$U^{[2]} = \begin{pmatrix} 100 & 000 & 010 \\ 111 & 110 & 100 \\ 001 & 100 & 010 \end{pmatrix}, V^{[2]} = \begin{pmatrix} 111 & 000 & 010 \\ 011 & 010 & 111 \\ 001 & 110 & 111 \end{pmatrix} \quad (35)$$

从而可得

$$(H_{11}U^{[2]} \ H_{21}V^{[2]}) = \begin{pmatrix} 001 & 111 & 010 & 000 & 110 & 001 \\ 000 & 100 & 101 & 000 & 001 & 100 \\ 000 & 001 & 000 & 000 & 110 & 111 \end{pmatrix}$$

$$(H_{12}U^{[2]} \ H_{22}V^{[2]}) = \begin{pmatrix} 000 & 100 & 110 & 001 & 011 & 011 \\ 000 & 110 & 110 & 000 & 010 & 110 \\ 000 & 000 & 111 & 000 & 010 & 111 \end{pmatrix} \quad (36)$$

可以看出，无论是宿点 t_1 还是宿点 t_2 ，均不能求解线性方程组，因为这2个系数矩阵的非全零列数均为4，而矩阵的秩均为3，所以必须在源点利用预编码1来控制源点的实际发送速率。

源点实施二级预编码后，宿点 t_1 得到的线性方程组的系数矩阵为

$$(H_{11}U^{[2]}U^{[1]} \ H_{21}V^{[2]}V^{[1]}) = \begin{pmatrix} 001w_1 & 111w_2 & 010w_3 & 000z_1 & 110z_2 & 001z_3 \\ 000w_1 & 100w_2 & 101w_3 & 000z_1 & 001z_2 & 100z_3 \\ 000w_1 & 001w_2 & 000w_3 & 000z_1 & 110z_2 & 111z_3 \end{pmatrix} \quad (37)$$

宿点 t_2 得到的线性方程组的系数矩阵为

$$(H_{12}U^{[2]}U^{[1]} \ H_{22}V^{[2]}V^{[1]}) = \begin{pmatrix} 000w_1 & 100w_2 & 110w_3 & 001z_1 & 011z_2 & 011z_3 \\ 000w_1 & 110w_2 & 110w_3 & 000z_1 & 010z_2 & 110z_3 \\ 000w_1 & 000w_2 & 111w_3 & 000z_1 & 010z_2 & 111z_3 \end{pmatrix} \quad (38)$$

在式(37)和式(38)中，系数矩阵均为3行6列的矩阵，每个矩阵均有1个全零列，要使系数矩阵满足推论1的条件，至少还要让每个矩阵的另外2列为全零列，则必须让 w_i 和 z_i ($i=1,2,3$) 中的其中2项置零，根据置零规则，有以下3种置零方式，具体如下。

- 1) $w_1=1, w_2=w_3=0, z_i=1 (i=1,2,3)$ 。
- 2) $z_1=1, z_2=z_3=0, w_i=1 (i=1,2,3)$ 。
- 3) $w_1=w_2=1, w_3=0, z_1=z_2=1, z_3=0$ 。

从而得到预编码1的3组矩阵，如式(39)所示。

$$\begin{pmatrix} 100 \\ 000 \\ 000 \end{pmatrix} \begin{pmatrix} 100 \\ 010 \\ 001 \end{pmatrix}, \begin{pmatrix} 100 \\ 010 \\ 001 \end{pmatrix} \begin{pmatrix} 100 \\ 000 \\ 000 \end{pmatrix}, \begin{pmatrix} 100 \\ 010 \\ 000 \end{pmatrix} \begin{pmatrix} 100 \\ 010 \\ 000 \end{pmatrix} \begin{pmatrix} 100 \\ 010 \\ 000 \end{pmatrix} \quad (39)$$

它们对应的实际发送速率向量分别为(1,3)、(3,1)、(2,2)。

现分析第3种情况，其余2种情况类似。因实际的发送速率向量为(2,2)，在一次数据传输中，假设源点 s_1 传输的字符向量为 $X_1=(111,110,?)^*$ ，源点

* 为了所提的方法具有统一性，尽管实际上只发送2个字符，但采用发送3个字符的格式，最后一个字符没有传输至网络，因此，该字符的选取随意，本文用“?”表示。

s_2 传输的字符向量为 $\mathbf{X}_2=(100,010,?)$, 则源点 s_1 的预编码矩阵为

$$\mathbf{U}^{[2]}\mathbf{U}^{[1]} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \end{pmatrix} \quad (40)$$

经预编码后得到的字符向量为

$$\mathbf{U}^{[2]}\mathbf{U}^{[1]}\mathbf{X}_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 111 \\ 110 \\ ? \end{pmatrix} = \begin{pmatrix} 001 \\ 001 \\ 010 \end{pmatrix} \quad (41)$$

源点 s_2 的预编码矩阵为

$$\mathbf{V}^{[1]}\mathbf{V}^{[2]} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \end{pmatrix} \quad (42)$$

$$\mathbf{V}^{[1]}\mathbf{V}^{[2]}\mathbf{X}_2 = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 100 \\ 010 \\ ? \end{pmatrix} = \begin{pmatrix} 001 \\ 011 \\ 011 \end{pmatrix} \quad (43)$$

源点经预编码后, 分别把预编码矩阵对应的全局编码向量和预编码后的字符采用已定的网络编码数据传输方案进行传输。则宿点 t_1 把得到的全局编码矩阵和接收到的字符进行联立形成线性方程组, 如式(44)所示。

$$\begin{pmatrix} 001 & 111 & 000 & 000 & 110 & 000 \\ 000 & 100 & 000 & 000 & 001 & 000 \\ 000 & 001 & 000 & 000 & 110 & 000 \end{pmatrix} \begin{pmatrix} x_{11} \\ x_{12} \\ x_{13} \\ x_{21} \\ x_{22} \\ x_{23} \end{pmatrix} = \begin{pmatrix} 100 \\ 111 \\ 001 \end{pmatrix} \quad (44)$$

宿点 t_2 把得到的全局编码矩阵和接收到的字符进行联立形成线性方程组, 如式(45)所示。

$$\begin{pmatrix} 000 & 100 & 000 & 001 & 011 & 000 \\ 000 & 110 & 000 & 000 & 010 & 000 \\ 000 & 000 & 000 & 000 & 010 & 000 \end{pmatrix} \begin{pmatrix} x_{11} \\ x_{12} \\ x_{13} \\ x_{21} \\ x_{22} \\ x_{23} \end{pmatrix} = \begin{pmatrix} 111 \\ 110 \\ 100 \end{pmatrix} \quad (45)$$

式(44)和式(45)显然满足推论 1 的条件, 从而可以求解。式(44)可以解出 x_{11} 、 x_{12} 、 x_{22} , 其结果为 $(x_{11}, x_{12}, x_{22}) = (111, 110, 010)$; 式(45)可以解出 x_{12} 、 x_{21} 、 x_{22} , 其结果为 $(x_{12}, x_{21}, x_{22}) = (110, 100, 010)$ 。

综上, 宿点 t_1 能解码出源点 s_1 的 2 个字符, 宿点 t_2 能解码出源点 s_2 的 2 个字符, 即源点的发送率向量为(2,2)。

其他 2 种情况可以类似地进行讨论。

综合这 3 种情况, 可以得到源点的可达信息率区域, 如图 5 所示, 其中, 横坐标的单位是字符/单位时间。

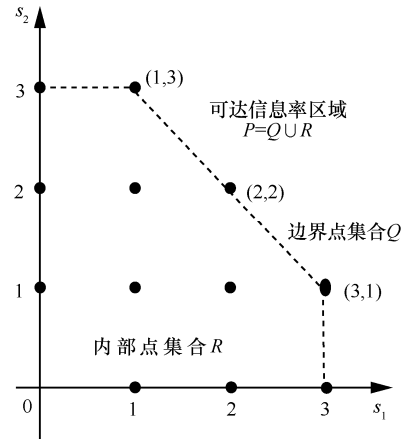


图 5 双单播网络的可达信息率区域

以上给出了可达信息率区域边界点的网络编码数据传输方案, 对于可达信息率区域的坐标为整数的内部点, 由定理 2 可知, 可以从边界点的网络编码数据传输方案中导出。例如, 对于坐标为(2,1)的点, 可以从边界点(2,2)或(3,1)的网络编码数据传输方案中导出。

7 结束语

本文提出了一种双单播网络编码的构造方法, 采用源点预编码技术, 中间节点采用随机线性网络编码技术, 并结合多目标优化进化策略来确定传输方案, 利用源点至宿点的信息转换矩阵的零向量空间的基向量和行向量空间的基向量共同来确定源点的预编码矩阵的列向量, 实现了在宿点消除信息干扰的目标。由双单播情形下的网络编码导出技术, 提出了二级预编码策略来控制源点的发送速率, 从而能够得到可行的网络传输方案。由多目标进化策略, 可以求出双单播网络编码的近似的可达信息率区域的边界点及相应的可行传输方案。本文还论证了如下结论: 只需要求出可达信息率区域边界点的可行传输方案, 内部点的传输方案可以从相应边界点的传输方案中导出。因此, 所提方法不仅可以求出双单播网络编

码的近似可达信息率区域, 还为求出的可达信息率区域的每一个整数坐标点提供了构造可行传输方案的方法, 适合于网络编码技术的实际应用。

多单播网络是一个比较困难的问题, 能否把这一方法推广到三单播网络乃至源点数更多的多单播网络, 将是下一步需要进行的研究工作。

参考文献:

- [1] KOETTER R, MEDARD M. An algebraic approach to network coding[J]. IEEE/ACM Transactions on Networking, 2003, 11(5): 782-795.
- [2] JAGGI S, SANDERS P, CHOU P A, et al. Polynomial time algorithms for multicast network code construction[J]. IEEE Transactions on Information Theory, 2005, 51(6): 1973-1982.
- [3] HO T, MEDARD M, KOETTER R, et al. A random linear network coding approach to multicasts[J]. IEEE Transactions on Information Theory, 2006, 52(10): 4413-4430.
- [4] YEUNG R W, LI S Y R, CAI N, et al. Network coding theory part II: multiple source[J]. Communications & Information Theory, 2005, 2(5):330-381.
- [5] 金振坤, 黄佳庆, 程文青. 多单播模型下的网络编码研究[J]. 小型微型计算机系统, 2012, 33(5):1023-1028.
JIN Z K, HUANG J Q, CHENG W Q. Survey of network coding for multiple unicast model[J]. Journal of Chinese Computer Systems, 2012, 33(5):1023-1028.
- [6] DOUGHERTY R, ZEGER K. Nonreversibility and equivalent constructions of multiple-unicast networks[J]. IEEE Transactions on Information Theory, 2006, 52(11):5067-5077.
- [7] KAMATH S, ANANTHARAM V, TSC D, et al. The two-unicast problem[J]. IEEE Transactions on Information Theory, 2018, 64(5):3865-3882.
- [8] HUANG S, RAMAMOORTHY A. An achievable region for the double unicast problem based on a minimum cut analysis[J]. Transactions on Communications, 2013, 61(7):2890-2899.
- [9] XU X, LI Z Y, LIANG G Y, TRACEY H. An achievable region for double-unicast networks with linear network coding[J]. IEEE Transactions on Communications, 2014, 62(10): 3621-3630.
- [10] BIDOKHTI S S, PRABHAKARAN V M, DIGGAVI S N. On multicasting nested message sets over combination networks[C]// Information Theory Workshop. Piscataway: IEEE Press, 2012: 2741-2749.
- [11] DOUGHERTY R, FREILING C, ZEGER K. Insufficiency of linear coding in network information flow[J]. IEEE Transactions on Information Theory, 2005, 51(8): 2745-2759.
- [12] WANG C C, SHROFF N B. Pairwise intersession network coding on directed networks[J]. IEEE Transactions on Information Theory, 2012, 56(8): 3879-3900.
- [13] KAMATH S U, TSE D N C, ANANTHARAM V. Generalized network sharing outer bound and the two-unicast problem[C]// International Symposium on Network Coding. Piscataway: IEEE Press, 2011: 285-291.
- [14] ZENG W, CADAMBE V, MEDARD M. On the tightness of the generalized network sharing bound for the two-unicast-Z network[C]// IEEE International Symposium on Information Theory. Piscataway: IEEE Press, 2013: 365-369.
- [15] SHOMORONY I, AVESTIMEHR A S. A generalized cut-set bound for deterministic multi-flow networks and its applications[C]// 2014 IEEE International Symposium on Information Theory. Piscataway: IEEE Press, 2014: 271-275.
- [16] ZENG W, CADAMBE V R, MEDARD M. An edge reduction lemma for linear network coding and an application to two-unicast networks[C]//2012 50th Annual Allerton Conference on Communication, Control, and Computing. Piscataway: IEEE Press, 2012: 509-516.
- [17] GANAL A E, COSTA M H M. The capacity region of a class of deterministic interference channels[J]. IEEE Transactions on Information Theory, 1982, 28(5): 343-346.
- [18] 蒲保兴, 杨路明, 王伟平. 线性网络编码的导出与扩展[J]. 软件学报, 2011, 22(3): 558-571.
PU B X, YANG L M, WANG W P. Generation and extension of linear network coding[J]. Journal of Software, 2011, 22(3):558-571.
- [19] YEUNG R W. Information theory and network Coding[M]. New York: Springer, 2008:56-68.
- [20] BERNSTEIN D S. Matrix mathematics: theory, facts and formulas[M]. New Jersey: Princeton University Press, 2009.
- [21] KIM M, MURIEL M, TRASLOV D. An evolutionary approach to inter-session network coding[C]//IEEE INFOCOM 2009 - The 28th Conference on Computer Communication. Piscataway: IEEE Press, 2009: 450-458.
- [22] 蒲保兴, 杨路明, 王伟平. 最优线性网络编码的分布式构造方法[J]. 系统工程与电子技术, 2009, 31(11): 2761-2766.
PU B X, YANG L M, WANG W P. Distributed construction of optimal linear network coding[J]. Systems Engineering and Electronics, 2009, 31(11): 2761-2766.
- [23] 谢金星, 邢文训, 王振波. 网络优化[M]. 北京: 清华大学出版社, 2009: 79-82.
XIE J X, XING W X, WANG Z B. Network optimization[M]. Beijing: Tsinghua University Press, 2009: 79-82.

[作者简介]



蒲保兴(1965—), 男, 湖南邵阳人, 博士, 梧州学院教授, 主要研究方向为网络编码、智能计算。



莫智懿(1984—), 男, 湖南益阳人, 梧州学院高级工程师, 主要研究方向为网络编码。