k 冗余多播网络中网络编码算法设计与分析

王 静[①②] 刘向阳[③] 王新梅[①]
[①](西安电子科技大学综合业务网国家重点实验室 西安 710071)
[②](长安大学信息工程学院 西安 710064)
[③](西安通信学院军事综合信息网教研室 西安 710106)

摘 要：k 冗余多播网络采用网络编码可实现最大多播速率 k 的信息传输。该文利用最大距离可分码已有成果，给出 k 冗余多播网络在不同发送速率下所需的最小有限域，构造最大距离可分码 $[n,k]$ 生成矩阵，将其列向量作为信源输出链路的全局编码向量，设计网络码字，实现网络编码。应用实例表明该网络编码方法相对现有的通用网络编码算法而言，具有更低的计算复杂度。

关键词：网络编码；k 冗余多播网络；最大距离可分码；有限域
中图分类号：TN911.22 **文献标识码**：A **文章编号**：1009-5896(2009)10-2411-05

Design and Analysis of Network Coding Algorithm in k-Redundant Multicast Network

Wang Jing[①②] Liu Xiang-yang[③] Wang Xin-mei[①]
[①](*State Key Lab of Integrated Service Networks*, *Xidian University.*, *Xi'an* 710071, *China*)
[②](*School of Information Engineering*, *Chang'an University*, *Xi'an* 710064, *China*)
[③](*Military Comprehensive Information Network Teaching Office*, *Xi'an Communication College*, *Xi'an* 710106, *China*)

Abstract: For k -redundant multicast network, the maximum multicast rate can be achieved with network coding. The minimal finite field which is enough to implement network coding for different multicast rate in k -redundant multicast network is obtained, by using some results of MDS codes available. To design codes of multicast network and implement network coding, a generator matrix of a $[n,k]$ MDS code is constructed based on the obtained minimal finite field, and its column vectors are allocated to output links of the source as their global coding vectors. An application instance shows that, compared with present universal approaches of network coding, this approach has lower computation complexity.

Key words: Network coding; k -redundant multicast network; Maximum Distance Separable (MDS) codes; Finite field

1 引言

近年来，多播传输变得越来越重要，已经成为现代通信中一个重要的组成部分。如果仅仅使用目前的多播传输技术，很多网络实际传输速率并不能达到网络本身所能提供的速率上限，即目前的技术还没有充分利用网络资源。

传统的网络节点只是将收到的数据路由、转发，并不进行数据的数学运算。Ahlswede等在2000年首次提出了网络编码理论[1]，其核心思想是网络中的节点可采用不加冗余的编码，以充分利用已有网络资源进行更加有效的数据传输。此思想突破了一直以来数据传输的固定模式，从而为进一步提高目前的网络传输速率奠定了基础。基于网络编码的多播传输，其传输速率可以达到最大流，即网络流量的理论上限值。Li等人[2]随后表明采用线性网络编码在有限大的域中多播传输速率能够达到速率上限 C 。Koetter等人[3]给出了网络编码的一种代数算法，此算法是指数时间算法，具有较大的计算复杂度。Sanders等人[4]提出了一种多项式时间算法，Lun等人[5]从线性规划角度研究多播网络的网络编码，Fragouli等人[6,7]将网络编码问题作为网络信息流分解问题来研究，给出了相应最小子树图的求解算法。这几种算法适用于所有的单源多播网络。但是针对某些具有一定特点的多播网络，有可能没必要使用上述方法，而使用更简单的方法。

Zhu 等人[8]提出了 k 冗余多播网络的概念，指出

2008-05-20 收到，2008-12-22 改回
国家 863 计划项目 (2007AA01Z215)，国家自然科学基金(60502046，60573034)和国家青年科学基金(60503010)资助课题

在 k 冗余多播网络中采用网络编码，网络的多播传输速率可以提高将近一倍。Zhu 等人给出了构造 k 冗余多播网络的分布式算法，但没有给出有效的网络编码方法。本文针对 k 冗余多播网络，利用最大距离可分码目前已有成果，得出信源不同发送速率下网络编码所需有限域大小的最小值。根据最大距离可分码 $[n,k]$ 生成矩阵的任意 k 个列向量线性无关，将其列向量作为信源输出链路的全局编码向量，实现了 k 冗余多播网络的网络编码，达到了该类网络所允许的最大传输速率。

2 k 冗余多播网络

对于无环多播网络 $G=(V,E)$，V 是节点集，E 是链路集，链路具有单位带宽。采用文献[8]中的算法可以得到网络 G 对应的 k 冗余多播网络。下面介绍 k 冗余多播网络的概念：

定义 1(k 冗余多播网络)[8] 一个单源多播的 k 冗余多播网络是一个有向非循环图(DAG)，具有下面两个特性：

(1)节点集 V 由 3 个离散子集 $\{s\}\cup V_I\cup V_T$ 构成：$\{s\}$ 为源节点，其入度 $\text{indegree}(s)=0$ 且出度 $\text{outdegree}(s)>0$；V_I 为中间节点，用 $u_i\,(1\le i\le|V_I|)$ 来标记，其入度 $1\le\text{indegree}(u_i)\le k$ 且出度 $\text{outdegree}(u_i)>0$；V_T 为接收节点，用 $t_i\,(1\le i\le|V_T|)$ 标记，其入度 $\text{indegree}(t_i)=k$ 且出度 $\text{outdegree}(t_i)\ge 0$；

(2)如果网络中链路具有单位带宽，对于入度为 k 的节点其最大流为 k。

图 1 给出了一个 2 冗余多播网络。s 是源节点，其入度为 0，出度为 3；u_1,u_2,u_3 是中间节点，其入度为 1，出度为 2；t_1,t_2,t_3 表示接收节点，其入度为 2，出度为 0。假定图 1 中链路具有单位带宽，每个接收节点的入度为 2，它们的最大流也为 2，$F_{\text{multicast}}=2$。

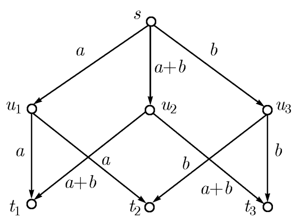

图 1 一个 2 冗余多播网络

采用图 1 中的编码方式进行多播传输时达到了速率 $F_{\text{multicast}}$，其中信息 a 和 b 在源路由器上被编码成 $a+b$ 后发送到中间节点 u_2。接收节点 t_1 可以通过 a 和 $a+b$ 得到 b，同理接收节点 t_3 也可以得到 a 和 b。如果不采用网络编码，无法实现速率为 2 的多播传输。

3 k 冗余多播网络的网络编码

k 冗余多播网络中信源 s 以单位时间速率 k 产生信息向量 $\boldsymbol{X}=[x_1\ x_2\ \cdots\ x_k]\in F_q^k$，并发送给接收节点 $t_1,t_2,\cdots,t_{|V_T|}$。对于任意链路 e，存在全局编码向量 $\boldsymbol{c}(e)=[\alpha_1(e)\ \alpha_2(e)\cdots\ \alpha_k(e)]^{\mathrm{T}}(\alpha_i(e)\in F_q)$，使得 e 上传输的符号 $y(e)$ 满足

$$y(e)=\alpha_1(e)x_1+\alpha_2(e)x_2+\cdots+\alpha_k(e)x_k$$
$$=[x_1\ x_2\ \cdots\ x_k]\underbrace{\begin{bmatrix}\alpha_1(e)\\\alpha_2(e)\\\vdots\\\alpha_k(e)\end{bmatrix}}_{\boldsymbol{c}(e)}\tag{1}$$

向量 $\boldsymbol{c}(e)=[\alpha_1(e)\ \alpha_2(e)\ \cdots\ \alpha_k(e)]^{\mathrm{T}}$ 是有限域 F_q 中的一个 k 维向量。

k 冗余多播网络中存在源节点到各接收节点的路径族，每一路径族包含 k 条离散路径。假定信源具有 n 条输出链路，根据 Max-flow Min-cut 定理[1]可以得到 $n\ge k$。若信源 n 条输出链路中任意 k 条链路的全局编码向量线性无关，则接收节点 k 条输入链路上的全局编码向量线性无关，接收节点收到 k 个正确符号，从而正确译出信源信息。

定理 1 k 冗余多播网络如果要以信息速率 k 传输信息，则信源 n 条输出链路中任意 k 条链路上的全局编码向量必须线性无关，确保接收节点 k 条输入链路对应的全局编码向量线性无关。

证明 对于接收节点 $t_j\ (1\le j\le|V_T|)$，在 k 冗余多播网络中存在 k 条离散路径，得到信源对应的 k 条输出链路和接收节点 t_j 的 k 条输入链路。设这 k 条输入链路的全局编码向量分别为 $[\alpha_{11}\ \alpha_{12}\cdots\ \alpha_{1k}]^{\mathrm{T}}$，$[\alpha_{21}\ \alpha_{22}\ \cdots\ \alpha_{2k}]^{\mathrm{T}}$，$\cdots$，$[\alpha_{k1}\ \alpha_{k2}\ \cdots\ \alpha_{kk}]^{\mathrm{T}}$。则接收节点 t_j 从 k 条输入链路上收到的 k 个比特 $y_1^j,y_2^j,\cdots,y_k^j$ 可以表示如下：

$$[y_1^j\ y_2^j\ \cdots\ y_k^j]=[x_1\ x_2\ \cdots\ x_k]\begin{bmatrix}\alpha_{11}&\alpha_{21}&\cdots&\alpha_{k1}\\\alpha_{12}&\alpha_{22}&\cdots&\alpha_{k2}\\\vdots&\vdots&\ddots&\vdots\\\alpha_{1k}&\alpha_{2k}&\cdots&\alpha_{kk}\end{bmatrix}\tag{2}$$

如果要从这 k 个比特 $y_1^j,y_2^j,\cdots,y_k^j$ 中解出 $[x_1\ x_2\ \cdots\ x_k]$，则 $\begin{bmatrix}\alpha_{11}&\alpha_{21}&\cdots&\alpha_{k1}\\\alpha_{12}&\alpha_{22}&\cdots&\alpha_{k2}\\\vdots&\vdots&\ddots&\vdots\\\alpha_{1k}&\alpha_{2k}&\cdots&\alpha_{kk}\end{bmatrix}$ 必须可逆，即 $[\alpha_{11}\ \alpha_{12}\ \cdots\ \alpha_{1k}]^{\mathrm{T}}$，$[\alpha_{21}\ \alpha_{22}\ \cdots\ \alpha_{2k}]^{\mathrm{T}}$，$\cdots$，$[\alpha_{k1}\ \alpha_{k2}\cdots\ \alpha_{kk}]^{\mathrm{T}}$ 必须线性无关，从而得到

$$[y_1^j\ y_2^j\ \cdots\ y_k^j]\begin{bmatrix}\alpha_{11} & \alpha_{21} & \cdots & \alpha_{k1}\\ \alpha_{12} & \alpha_{22} & \cdots & \alpha_{k2}\\ \vdots & \vdots & \ddots & \vdots\\ \alpha_{1k} & \alpha_{2k} & \cdots & \alpha_{kk}\end{bmatrix}^{-1}=[x_1\ x_2\ \cdots\ x_k]\quad(3)$$

从定理 1 可知，要使 k 冗余多播网络以信息速率 k 传输，则信源 n 条输出链路的全局编码向量中任意 k 个必须线性无关。这个特点刚好和最大距离可分码生成矩阵的列向量特点相同，即 $[n,k]$ 最大距离可分码生成矩阵的任意 k 个列向量线性无关[9]。因此，可将最大距离可分码生成矩阵的 n 个 k 维列向量作为信源 n 条输出链路上的全局编码向量。

定理 2[9]　给定 k 和 q，对于 $\mathrm{GF}(q)$ 上的 $[n,k]$ 最大距离可分码，如果用 $m(k,q)$ 表示 n 的最大值，则

当 $k \ge q$ 时，$m(k,q)=k+1$；当 $k<q$ 时，有

$$m(k,q)=\begin{cases}q+2, & q\text{是偶数且}k=3\text{或者}k=q-1\\ q+1, & \text{其它}\end{cases}$$

根据定理 2，容易得到 k 冗余多播网络在信源不同发送速率 k 下所需的最小有限域，如推论 1 所示。

推论 1　已知信源具有 n 条输出链路，且以 k 符号每单位时间发送信息，k 冗余多播网络要实现速率 k 的多播传输，所需的最小有限域 $\mathrm{GF}(q)$ 满足：

(1)当 $n-k=1$ 时，$q=2$；

(2)当 n 是偶数且 $k=3$ 或者 $k=n-3$ 时，q 为大于等于 $n-2$ 的最小素数或素数的幂次；

(3)其它情况下，q 为大于等于 $n-1$ 的最小素数或素数的幂次。

下面讨论 n，k 取不同值时最大距离可分码的生成矩阵，其列向量对应于信源 n 条输出链路上的全局编码向量。设 $\alpha_1,\alpha_2,\cdots,\alpha_{q-1}$ 为 $\mathrm{GF}(q)$ 中不包含零元素的 $q-1$ 个元素。

定理 3　当 $2\le k<q$ 时，取矩阵

$$\begin{bmatrix}1 & 1 & \cdots & 1 & 1 & 0 & 0\\ \alpha_1 & \alpha_2 & \cdots & \alpha_{q-1} & 0 & 1 & 0\\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_{q-1}^2 & 0 & 0 & 0\\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots\\ \alpha_1^{k-1} & \alpha_2^{k-1} & \cdots & \alpha_{q-1}^{k-1} & 0 & 0 & 1\end{bmatrix}$$

中任意 n 列构成 $k\times n$ 矩阵，此子矩阵中任意 k 列线性无关。

证明见附录。

定理 4　当 $k\ge q$ 时，下面 $k\times n(n=k+1)$ 矩阵

$$\begin{bmatrix}1 & 1 & 0 & \cdots & 0\\ 1 & 0 & 1 & \cdots & 0\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ 1 & 0 & 0 & \cdots & 1\end{bmatrix}$$

的任意 k 列线性无关。

证明简单，此处略。

定理 3 和定理 4 中矩阵的列向量数都以达到了定理 2 中的 $m(k,q)$ 值。对 k 和 n 取不同值的 k 冗余多播网络，可以利用推论 1 确定多播速率为 k 时所需的最小网络编码域。再将定理 3 和定理 4 中相应的矩阵列向量作为全局编码向量分配到信源的 n 条输出链路上，从而得到各接收节点路径族中其它链路上的全局编码向量，完成网络编码。

例 1　图 2 给出了一个 3 冗余多播网络，网络具有 9 个中间节点，每一个接收节点都与 3 个中间节点相连。在此 3 冗余多播网络中进行网络编码以达到多播速率 3 比特/单位时间，其中链路具有单位带宽。

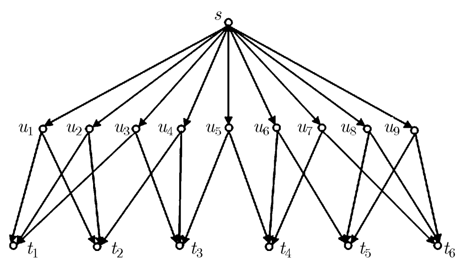

图 2　一个 3 冗余多播网络

此图中 $n=9$，$k=3$。根据推论 1，q 为大于等于 $n-1$ 的最小素数或素数的幂次，得到 $q=2^3$。设 $\alpha_1,\alpha_2,\cdots,\alpha_7$ 为 $\mathrm{GF}(2^3)$ 中不包含零元素的 7 个元素。信源 9 条输出链路上的全局编码向量可由定理 3 中的矩阵列向量来提供。即从矩阵

$$\begin{bmatrix}1 & 1 & \cdots & 1 & 1 & 0 & 0\\ \alpha_1 & \alpha_2 & \cdots & \alpha_7 & 0 & 1 & 0\\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_7^2 & 0 & 0 & 1\end{bmatrix}$$

的 10 个列向量中任选 9 列构成 $k\times n$ 矩阵，其列向量作为信源 9 条输出链路的全局编码向量，于是任一接收节点 3 条输入链路上的全局编码向量线性无关，接收节点正确译出信源信息，实现速率为 3 的多播传输。

4　结束语

k 冗余多播网络采用网络编码可实现最大速率 k 的多播传输，本文利用最大距离可分码已有的成果，给出 k 冗余多播网络在多播速率为 k 时网络编码所需的最小有限域。构造最大距离可分码的生成矩阵，根据最大距离可分码 $[n,k]$ 生成矩阵中任意 k

个列向量线性无关，将其列向量作为信源 n 条输出链路上的全局编码向量，设计网络码字，实现 k 冗余多播网络的网络编码。

附录　定理3证明　首先证明当 $2\le k<q$ 时，上述 $k\times(q+2)$ 矩阵的列向量数大于等于 n 。具有如下情况：

(1)当 $k=3$ 或 $k=q-1\ge 2$ 且 q 为偶数时，$n=q+2$；

(2)其它情况下，$n=q+1<q+2$。

要证 $k\times n$ 子矩阵中任意 k 列线性无关，只需证上述 $k\times(q+2)$ 矩阵中任意 k 列线性无关，为此要证明任意 k 列向量构成的方阵行列式值不为零即可。前 $q-1$ 列中的任意 k 列构成范德蒙方阵，其行列式值显然不为为零。下面证明含最后 3 列中的 $m(0<m\le 3)$ 列的情况。具有一般性，选择 $k\times(q+2)$ 矩阵前 $q-1$ 列中任意 $k-m$ 列，记作 $c_1,c_2,\cdots,c_{k-m}$，其中 $c_i\in\{1,2,\cdots,q-1\}$，且 $c_i\ne c_j(i\ne j;i,j=1,2,\cdots,k-m)$。

(1) $m=1$ 时

(a)如果选择最后3列中的第1列，对应的行列式如下：

$$\begin{vmatrix} 1 & 1 & \cdots & 1 & 1\\ \alpha_{c_1} & \alpha_{c_2} & \cdots & \alpha_{c_{k-1}} & 0\\ \alpha_{c_1}^2 & \alpha_{c_2}^2 & \cdots & \alpha_{c_{k-1}}^2 & 0\\ \vdots & \vdots & \ddots & \vdots & \vdots\\ \alpha_{c_1}^{k-1} & \alpha_{c_2}^{k-1} & \cdots & \alpha_{c_{k-1}}^{k-1} & 0 \end{vmatrix}$$

$$=(-1)^{k+1}\alpha_{c_1}\alpha_{c_2}\cdots\alpha_{c_{k-1}}\begin{vmatrix} 1 & 1 & \cdots & 1\\ \alpha_{c_1} & \alpha_{c_2} & \cdots & \alpha_{c_{k-1}}\\ \vdots & \vdots & \ddots & \vdots\\ \alpha_{c_1}^{k-2} & \alpha_{c_2}^{k-2} & \cdots & \alpha_{c_{k-1}}^{k-2} \end{vmatrix}\ne 0$$

(b)如果选择最后3列中的第2列，对应的行列式如下：

$$\begin{vmatrix} 1 & 1 & \cdots & 1 & 0\\ \alpha_{c_1} & \alpha_{c_2} & \cdots & \alpha_{c_{k-1}} & 1\\ \alpha_{c_1}^2 & \alpha_{c_2}^2 & \cdots & \alpha_{c_{k-1}}^2 & 0\\ \vdots & \vdots & \ddots & \vdots & \vdots\\ \alpha_{c_1}^{k-1} & \alpha_{c_2}^{k-1} & \cdots & \alpha_{c_{k-1}}^{k-1} & 0 \end{vmatrix}$$

$$=(-1)^{k+2}\begin{vmatrix} 1 & 1 & \cdots & 1\\ \alpha_{c_1}^2 & \alpha_{c_2}^2 & \cdots & \alpha_{c_{k-1}}^2\\ \vdots & \vdots & \ddots & \vdots\\ \alpha_{c_1}^{k-1} & \alpha_{c_2}^{k-1} & \cdots & \alpha_{c_{k-1}}^{k-1} \end{vmatrix}$$

根据广义范德蒙行列式的性质[10]，上述行列式可表述为

$$(-1)^{k+2}\left(\sum_{i=1}^{k-1}\alpha_{c_1}\alpha_{c_2}\cdots\alpha_{c_{i-1}}\alpha_{c_{i+1}}\cdots\alpha_{c_{k-1}}\right)\cdot\begin{vmatrix} 1 & 1 & \cdots & 1\\ \alpha_{c_1} & \alpha_{c_2} & \cdots & \alpha_{c_{k-1}}\\ \vdots & \vdots & \ddots & \vdots\\ \alpha_{c_1}^{k-2} & \alpha_{c_2}^{k-2} & \cdots & \alpha_{c_{k-1}}^{k-2} \end{vmatrix}\ne 0$$

(c)如果选择最后3列中的第3列，对应的行列式如下：

$$\begin{vmatrix} 1 & 1 & \cdots & 1 & 0\\ \alpha_{c_1} & \alpha_{c_2} & \cdots & \alpha_{c_{k-1}} & 0\\ \alpha_{c_1}^2 & \alpha_{c_2}^2 & \cdots & \alpha_{c_{k-1}}^2 & 0\\ \vdots & \vdots & \ddots & \vdots & \vdots\\ \alpha_{c_1}^{k-1} & \alpha_{c_2}^{k-1} & \cdots & \alpha_{c_{k-1}}^{k-1} & 1 \end{vmatrix}=\begin{vmatrix} 1 & 1 & \cdots & 1\\ \alpha_{c_1} & \alpha_{c_2} & \cdots & \alpha_{c_{k-1}}\\ \vdots & \vdots & \ddots & \vdots\\ \alpha_{c_1}^{k-2} & \alpha_{c_2}^{k-2} & \cdots & \alpha_{c_{k-1}}^{k-2} \end{vmatrix}\ne 0$$

(2) $m=2$ 时

(a)如果选择最后3列中的第1列和第3列，对应的行列式如下：

$$\begin{vmatrix} 1 & 1 & \cdots & 1 & 1 & 0\\ \alpha_{c_1} & \alpha_{c_2} & \cdots & \alpha_{c_{k-2}} & 0 & 0\\ \alpha_{c_1}^2 & \alpha_{c_2}^2 & \cdots & \alpha_{c_{k-2}}^2 & 0 & 0\\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots\\ \alpha_{c_1}^{k-1} & \alpha_{c_2}^{k-1} & \cdots & \alpha_{c_{k-2}}^{k-1} & 0 & 1 \end{vmatrix}$$

$$=(-1)^{3k}\begin{vmatrix} \alpha_{c_1} & \alpha_{c_2} & \cdots & \alpha_{c_{k-2}}\\ \alpha_{c_1}^2 & \alpha_{c_2}^2 & \cdots & \alpha_{c_{k-2}}^2\\ \vdots & \vdots & \ddots & \vdots\\ \alpha_{c_1}^{k-2} & \alpha_{c_2}^{k-2} & \cdots & \alpha_{c_{k-2}}^{k-2} \end{vmatrix}$$

$$=(-1)^{3k}\alpha_{c_1}\alpha_{c_2}\cdots\alpha_{c_{k-2}}\begin{vmatrix} 1 & 1 & \cdots & 1\\ \alpha_{c_1} & \alpha_{c_2} & \cdots & \alpha_{c_{k-2}}\\ \vdots & \vdots & \ddots & \vdots\\ \alpha_{c_1}^{k-3} & \alpha_{c_2}^{k-3} & \cdots & \alpha_{c_{k-2}}^{k-3} \end{vmatrix}\ne 0$$

(b)如果选择最后3列中的第1列和第2列，对应的行列式如下：

$$\begin{vmatrix} 1 & 1 & \cdots & 1 & 1 & 0\\ \alpha_{c_1} & \alpha_{c_2} & \cdots & \alpha_{c_{k-2}} & 0 & 1\\ \alpha_{c_1}^2 & \alpha_{c_2}^2 & \cdots & \alpha_{c_{k-2}}^2 & 0 & 0\\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots\\ \alpha_{c_1}^{k-1} & \alpha_{c_2}^{k-1} & \cdots & \alpha_{c_{k-2}}^{k-1} & 0 & 0 \end{vmatrix}$$

$$=(-1)^{2k+2}\begin{vmatrix} \alpha_{c_1}^2 & \alpha_{c_2}^2 & \cdots & \alpha_{c_{k-2}}^2 \\ \alpha_{c_1}^3 & \alpha_{c_2}^3 & \cdots & \alpha_{c_{k-2}}^3 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{c_1}^{k-1} & \alpha_{c_2}^{k-1} & \cdots & \alpha_{c_{k-2}}^{k-1} \end{vmatrix}$$

$$=\alpha_{c_1}^2\alpha_{c_2}^2\cdots\alpha_{c_{k-2}}^2\begin{vmatrix} 1 & 1 & \cdots & 1 \\ \alpha_{c_1} & \alpha_{c_2} & \cdots & \alpha_{c_{k-2}} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{c_1}^{k-3} & \alpha_{c_2}^{k-3} & \cdots & \alpha_{c_{k-2}}^{k-3} \end{vmatrix}\neq 0$$

(c)如果选择最后 3 列中的第 2 列和第 3 列，对应的行列式如下：

$$\begin{vmatrix} 1 & 1 & \cdots & 1 & 0 & 0 \\ \alpha_{c_1} & \alpha_{c_2} & \cdots & \alpha_{c_{k-2}} & 1 & 0 \\ \alpha_{c_1}^2 & \alpha_{c_2}^2 & \cdots & \alpha_{c_{k-2}}^2 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ \alpha_{c_1}^{k-1} & \alpha_{c_2}^{k-1} & \cdots & \alpha_{c_{k-2}}^{k-1} & 0 & 1 \end{vmatrix}$$

$$=\begin{vmatrix} 1 & 1 & \cdots & 1 & 0 \\ \alpha_{c_1} & \alpha_{c_2} & \cdots & \alpha_{c_{k-2}} & 1 \\ \alpha_{c_1}^2 & \alpha_{c_2}^2 & \cdots & \alpha_{c_{k-2}}^2 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \alpha_{c_1}^{k-2} & \alpha_{c_2}^{k-2} & \cdots & \alpha_{c_{k-2}}^{k-2} & 0 \end{vmatrix}$$

上述行列式与第(1)种情况中的(b)形式相同，其行列式值不为 0。

(3) $m=3$时，对应的行列式如下：

$$\begin{vmatrix} 1 & 1 & \cdots & 1 & 1 & 0 & 0 \\ \alpha_{c_1} & \alpha_{c_2} & \cdots & \alpha_{c_{k-3}} & 0 & 1 & 0 \\ \alpha_{c_1}^2 & \alpha_{c_2}^2 & \cdots & \alpha_{c_{k-3}}^2 & 0 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ \alpha_{c_1}^{k-1} & \alpha_{c_2}^{k-1} & \cdots & \alpha_{c_{k-3}}^{k-1} & 0 & 0 & 1 \end{vmatrix}$$

$$=(-1)^{4k}\begin{vmatrix} \alpha_{c_1}^2 & \alpha_{c_2}^2 & \cdots & \alpha_{c_{k-3}}^2 \\ \alpha_{c_1}^3 & \alpha_{c_2}^3 & \cdots & \alpha_{c_{k-3}}^3 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{c_1}^{k-2} & \alpha_{c_2}^{k-2} & \cdots & \alpha_{c_{k-3}}^{k-2} \end{vmatrix}$$

$$=\alpha_{c_1}^2\alpha_{c_2}^2\cdots\alpha_{c_{k-3}}^2\begin{vmatrix} 1 & 1 & \cdots & 1 \\ \alpha_{c_1} & \alpha_{c_2} & \cdots & \alpha_{c_{k-3}} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{c_1}^{k-4} & \alpha_{c_2}^{k-4} & \cdots & \alpha_{c_{k-3}}^{k-4} \end{vmatrix}\neq 0$$

参 考 文 献

[1] Ahlswede R, Cai Ning, and Li S Y R, *et al.*. Network information flow [J]. *IEEE Transactons on Inf. Theory*, 2000, 46(4): 1204–1216.

[2] Li S Y R, Yeung R W, and Cai Ning. Linear network coding [J]. *IEEE Transactons on Inf. Theory*, 2003, 49(2): 371–381.

[3] Koetter R and Medard M. An algebraic approach to network coding [J]. *IEEE/ACM Transactons on Networking*, 2003, 11(5): 782–795.

[4] Jaggi S, Sanders P, and Chou P A, *et al.*. Polynomial time algorithms for multicast network code construction [J]. *IEEE Transactons on Inf. Theory*, 2005, 51(6): 1973–1982.

[5] Lun D S, Ratnakar N, and Medard M, *et al.*. Minimum-cost multicast over coded packet networks [J]. *IEEE Trans. on Inf. Theory*, 2006, 52(6): 2608–2623.

[6] Fragouli C and Soljanin E. Information flow decomposition for network coding [J]. *IEEE Transactons on Inf. Theory*, 2006, 52(3): 829–848.

[7] Fragouli C, Soljanin E, and Shokrollahi A. Network coding as a coloring problem [C]. In Proceedings of IEEE Annual Conference on Information Sciences and Systems, Princeton, NJ, USA, March 2004: 1–6.

[8] Zhu Ying, Li Baochun, and Guo Jiang. Multicast with network coding in application-layer overlay networks [J]. *IEEE Journal on Selected Areas in Communications*, 2004, 22(1): 107–120.

[9] MacWilliams F J and Sloane N J A. The Theory of Error-Correcting Codes [M]. Amsterdam: North-Holland Mathematical Library, 1977, Chapter 11.

[10] Ernst T. Generalized vandermonde determinants. http://www. math.uu.se/research/pub/Ernst1.pdf. 2007,7.

王　静：　女，1982年生，博士生，讲师，研究方向为网络编码理论及其路由算法.

刘向阳：　男，1982年生，博士生，助教，研究方向为网络编码理论.

王新梅：　男，1937年生，教授，博士生导师，研究方向为信道编码、信息理论和信息安全等.