非线性网络编码实例研究*)

李令雄　龙冬阳

（中山大学计算机系　广州 510275）（广东省信息安全重点实验室　广州 510275）

摘　要　在网络编码研究中，线性编码技术已趋于成熟，但它有着需要大字符表且不适用于非多播网络的弱点，这推动了对非线性编码的研究。本文给出编码函数的新描述，在此基础上将非线性编码分成两类：证明了前者与线性编码等价，能从线性编码中构造出，且具有相同的编码能力；证明了后者的存在性。

关键词　多播，网络编码，线性编码，非线性编码

Nonlinear Network Coding: A Case Study

LI Ling-xiong　LONG Dong-yang

(Dept. of Computer Science, Sun Yat-sen University, Guangzhou 510275, China)

(Guangdong Key Laboratory of Information Security Technology, Guangzhou 510275, China)

Abstract　In the area of network coding, linear code can achieve the maximum capacity of multicast networks by large alphabets. However, it is insufficient for non-multicast networks. Meanwhile nonlinear code is of interest for its possibility to achieve the network coding capacity by small alphabet, or its possibility to deal with other networks. There is no schema of nonlinear code in our literature. In this paper, a novel characterization of nonlinear code is proposed. We reveal that a kind of nonlinear code can be induced from linear code, and it has the same coding ability as linear code. We also show the existence of another kind of polynomial code.

Keywords　Multicast, Network coding, Linear code, Nonlinear code

1　引言

传统网络中，节点只有路由转发功能，而在网络编码的模型中，节点允许对接收到的信息进行编码和转发。图 1 为该模型的示意图，其中 x 和 y 为二元域上的符号，节点 3 执行编码操作(模 2 加法)并转发，每个终端节点能从所接收到的信息中解码出所需信息(x 和 y)。

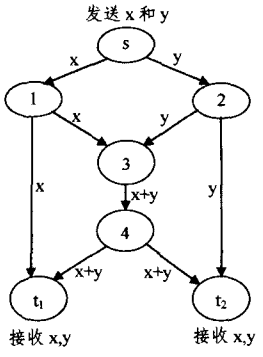

图 1　网络编码模型

网络编码技术首先由 Ahlswede[1] 等人引入。它证明了：若源节点与每个终端节点间的最小割都是 k，则使用网络编码技术能一次性从源节点传输 k 个消息到每个终端节点。Li[2] 等人证明在字符表足够大的条件下，采用线性网络编码方法总能达到多播网络的最大容量。文献[2-6]研究了线性编码的构造算法。由于大字符表会导致传输的延迟和更多的带宽消耗，而小字符表更便于传输，因此字符表问题引起广泛关注。对一些特殊拓扑的网络，Feder 等[7] 和 Rasala 等[8] 给出字符表大小的下界：它的规模等于终端节点数的平方根。文献[8]还指出：对一般网络求可行字符表的最小值是个 NP-难问题。另一方面，Dougherty 等[9] 证明：在给定字符表的情况下，线性编码不足以处理所有多播网络。而对非多播网络，文献[10]和[8]指出：即使在字符表足够大的情况下，线性编码也不足以处理所有网络。非线性编码能否避免线性编码的这些弱点，这是个未知问题。非线性编码被认为是个有意义的新方向[8]。

目前对非线性编码的研究还处于起步阶段。本文首先提出非线性编码的多项式描述，称为多项式码。然后与线性码进行比较。在一般的情况下，多项式码至少具有与线性码相当的编码能力。我们演示了从线性编码构造多项式编码的方法。最后，我们证明了更复杂的多项式编码也存在，证明过程利用了编码函数和拉丁矩阵之间的有趣联系。

2　模型

多播问题可用五元组 (G, s, D, C, M) 描述：有向无圈图 $G:=(V,E)$；源节点 $s\in V$；终端节点集合 $D\subset V$；各边的容量集合 $C:=\{c(e)\mid e\in E, c(e)\in Z\}$；$n$ 维消息 $M=(m_1,\cdots,m_n)$，$m_i\in\Sigma$。图 G 描述通讯网络，其中 V 为节点集合，表示路由或计算机；$E=V\times V$ 为边集合，表示通信信道。源节点 s 产生消息 M，需要传输到每个终端节点 $v\in D$。消息 M 是个 n 维符号向量，其中每个符号 m_i 都取自同一字符表 Σ。字符表大小(记为 q)通常约定为某个素数的幂，从而在字符表上可定义有限域结构[9]。下文中讨论编码操作时，我们直接把字

*)本文受国家自然科学基金项目(60273062, 60573039)及广东省自然科学基金项目(04205407, 5003350)资助。李令雄　博士研究生；龙冬阳　博士，教授，博士生导师。

符表看成域。不失一般性，边容量 $c(e)$ 通常可假设为 1[1]，即每条边一次能传输 Σ 中的一个符号。

在网络编码的模型中，各边都对应着一个编码函数，它决定了当源节点发送 M 时，该边传输的内容。对从 v 到 v' 的有向边 e，编码函数可用如下公式描述：

$$\phi_e:=\begin{cases}\sum^{|M|}\to\sum & \text{if } v=s\\ \sum^{|E_I(v)|}\to\sum & \text{if } v\neq s\end{cases}$$

其中 $E_I(v)$ 是节点 v 的入边集合。

全体边对应的编码函数的集合称为网络的编码，它描述了该网络的传输方案。若全体终端节点都能从所接受到的内容中恢复出 M，则该网络编码称为可行的，否则称为不可行的。若所有编码函数都是线性函数，则网络编码称为线性的，否则称为非线性的。由于线性编码函数较容易实现，大部分研究工作都集中在线性网络编码，对非线性编码函数的研究较少。

本文提出编码函数的更一般的形式。首先引入以下的代数性质[11]：

引理 若 Σ 是大小为 q 的有限域，则函数 $f:\Sigma^k\to\Sigma$ 总可用系数取自 Σ 且在各变元上度均小于 q 的 k 元多项式表示。

例如当 Σ 为二元域，函数 $f:\Sigma^2\to\Sigma$ 共有十六种不同的形式，可用 $\{0,x,y,x+y,xy,x+xy,y+xy,x+y+xy,1,x+1,y+1,x+y+1,xy+1,x+xy+1,y+xy+1,x+y+xy+1\}$ 表示，其中 0 和 1 分别表示零元和幺元。

由于每个非线性编码函数都可以用一个多项式唯一表示，我们称非线性编码为多项式编码。

引入独立和独立集的定义如下：

两个函数 $f,f':\Sigma^2\to\Sigma$ 称为独立的，当且仅当存在函数 $g:\Sigma^2\to\Sigma^2$ 使得对每个 $(\alpha,\beta)\in\Sigma^2$，有 $g(f(\alpha,\beta),f'(\alpha,\beta))=(\alpha,\beta)$；或等价地，对点 $(\alpha,\beta),(\alpha',\beta')\in\Sigma^2$，当且仅当 $(\alpha,\beta)\neq(\alpha',\beta')$，有 $(f(\alpha,\beta),f'(\alpha,\beta))\neq(f(\alpha',\beta'),f'(\alpha',\beta'))$。

独立描述了编码的可恢复性：将源消息 (α,β) 分别作为编码函数 f,f' 的输入，若 f,f' 是独立的，则能从它们的输出中恢复出 (α,β)。

函数集合 $\{f_1,\cdots,f_n\mid f_i:\Sigma^2\to\Sigma\}$ 称为独立集，如果它们两两独立。当 n 的取值为最大，集合称为最大独立集（MIS）。对 MIS，我们有 $n=q+1$（证明略）。下文讨论的函数，如无特别声明，都为 $f:\Sigma^2\to\Sigma$ 的形式。

3 主要结论

本节集中讨论传输二维消息。首先，我们讨论二元字符表，举例证明多项式编码不如线性编码强大，这是由于二元字符表上的非线性函数都不具有可解码的性质。然后，我们讨论多元字符表，证明了从线性编码中可推导出一类多项式编码，它具有相同的编码能力。在这类多项式编码中，仅源节点执行非线性操作。最后，我们证明在多元字符表上一般形式的多项式编码（中间节点执行非线性操作）的存在性。

3.1 二元字符表（$q=2$）

本小节在二元字符表上比较多项式编码和线性编码。首先有以下引理：

引理 1 若函数 $f,f':\Sigma^2\to\Sigma$ 独立，则它们是 q 到 1 的映射。

证明：假设 f 不是 q 到 1 的映射，则它会在超过 q 个点上取相同值（记为 γ）。f' 在这些点上只能取 q 种不同值，由鸽笼原理，这些点中至少有两个点上 f' 的取值相同，将两个点记为 (α,β) 和 (α',β')。因此，我们有 $f(\alpha,\beta)=f(\alpha',\beta')$ 和 $f'(\alpha,\beta)=f'(\alpha',\beta')$，这与 f,f' 独立的性质产生矛盾。

引理 2 每个线性函数 $f=ax+by+c$ 都是 q 到 1 的映射，其中 $(a,b,c)\in\Sigma^3$，$(a,b)\neq(0,0)$，0 表示域上的零元。

证明：a）若 $b=0$，则 $f=ax+c$。由于域中每个元都有加法逆元，每个非零元都有乘法逆元，我们有：$f(\alpha,\beta)=f(\alpha',\beta')\Leftrightarrow a\alpha+c=a\alpha'+c\Leftrightarrow\alpha=\alpha'$，其中 $(\alpha,\beta),(\alpha',\beta')\in\Sigma^2$。因此，当 x 变化时，f 取不同值，当 x 取值确定时，y 可取 q 种不同值。因此 f 是 q 到 1 的映射。b）当 $a=0$，则 $f=by+c$。证明同上。c）若 $a\neq0,b\neq0$，则 $f=ax+by+c$。对 $\alpha,\gamma\in\Sigma$，有 $f(\alpha,y)=\gamma\Leftrightarrow a\alpha+by+c=\gamma\Leftrightarrow y=b^{-1}(\gamma+(-(a\alpha+c)))$，其中 b^{-1} 为 b 的乘法逆元，$-(a\alpha+c)$ 为 $a\alpha+c$ 的加法逆元。因此，对每个固定值 γ 和任意 $\alpha\in\Sigma$，存在某个确定值 $\beta\in\Sigma$ 使得 $f(\alpha,\beta)=\gamma$。因此 f 是 q 到 1 的映射。

注意到 $f:\Sigma^2\to\Sigma$ 上 q 到 1 映射的函数共有 $\prod_{i=0}^{q^k-1}C_{q^k-iq}^{q}$ 种（排列组合），而线性函数有 $(q^2-1)q$ 个（排列组合），结合引理 1 和引理 2，可得：

推论 3 当 $q=2$，若两函数 f,f' 独立，则它们都是线性函数。

定理 4 存在多播网络，在二元字符表上有可行的线性编码，但无可行的多项式编码。

证明：将图 1 中的多播网络记为 G，它有可行的线性编码。接下来证明：G 上可行编码都是线性的。

可行的编码要求源消息能够从图中任意割上传输的内容中恢复出来，而 G 中的所有割都只有两条边，因此若编码是可行的，则割上对应的函数是独立的。由推论 3 可知，此时所有函数都是线性函数。因此 G 上可行编码总是线性的，得证。

3.2 多元字符表（$q\geqslant3$）

在多元字符表上，非线性编码通常被认为难于构造，但本节定理 9 将证明一类多项式编码能较容易地从线性码中推导出来。我们首先引入两个引理：

引理 5 两个函数 f,f' 是独立的，当且仅当函数 $af+b$，f' 是独立的，其中 $a,b\in\Sigma$，且 $a\neq0$。

证明：令 $g=af+b$。由于 Σ 是个域，对 $(\alpha,\beta),(\alpha',\beta')\in\Sigma^2$，则有 $g(\alpha,\beta)=g(\alpha',\beta')\Leftrightarrow af(\alpha,\beta)+b=af(\alpha',\beta')+b\Leftrightarrow f(\alpha,\beta)=f(\alpha',\beta')$。若 f,f' 独立，则有 $(f(\alpha,\beta),f'(\alpha,\beta))=(f(\alpha',\beta'),f'(\alpha',\beta'))\Leftrightarrow(\alpha,\beta)=(\alpha',\beta')$。因此，我们有 $(g(\alpha,\beta),f'(\alpha,\beta))=(g(\alpha',\beta'),f'(\alpha',\beta'))\Leftrightarrow(\alpha,\beta)=(\alpha',\beta')$。因此，$g$ 和 f' 互相独立。反之同理，得证。

定义 f 的等价集合为

$[f]=\{af+b\mid a,b\in\Sigma,a\neq0\}$。

引理 6 若函数 f,f' 互相独立，则函数 f,g 互相独立，其中 $g=af+bf'+c,a\neq0,b\neq0,(a,b,c)\in\Sigma^3$。

证明：对 $(\alpha,\beta),(\alpha',\beta')\in\Sigma^2$，若 $(f(\alpha,\beta),g(\alpha,\beta))=(f(\alpha',\beta'),g(\alpha',\beta'))$，则 $\begin{cases}f(\alpha,\beta)=f(\alpha',\beta')\\ g(\alpha,\beta)=g(\alpha',\beta')\end{cases}\Rightarrow\begin{cases}f(\alpha,\beta)=f(\alpha',\beta')\\ f'(\alpha,\beta)=f'(\alpha',\beta')\end{cases}$。由 f,f' 互相独立，可得 $(\alpha,\beta)=(\alpha',\beta')$。因此，$f,g$ 互相独立。

由引理 5 和引理 6，可得：

推论 7 若函数 f,f' 互相独立，则从每个等价集合 $[f]$，$[f']$，$[f+f']$，$\cdots$，$[f+(q-1)f']$（其中 1 为域中幺元）中各选一个函数将构成最大独立集（MIS）。

定义函数 π_i 为 $\pi_i(x_1,\cdots,x_n)=x_i$，记 $f_x=\pi_1(x,y)$，$f_y=\pi_2(x,y)$。由推论 7，从每个等价集合$[f_x]$，$[f_y]$，$[f_x+f_y]$，…，$[f_x+(q-1)f_y]$中各选一个函数将构成最大独立集(*MIS*)。令 $L=[f_x]\cup[f_y]\cup[f_x+f_y],\cdots,\cup[f_x+(q-1)f_y]$，注意到$|L|=(q+1)q(q-1)$，因此 L 集合包含了所有线性函数。特别地，我们有：

推论 8 如果 f,f'为线性函数，则它们互相独立，或者有 $f'\in[f]$。

于是可得到以下结论：

定理 9 在多元字符表($q\geqslant 3$)上，可行线性编码 C 总存在对应的可行多项式编码 C'。

证明：假设存在独立于 f_x 的多项式函数 f(非线性)，则将 L 中的所有 f_y 函数用 f 代替，可得集合

$$L'=[f_x]\cup[f]\cup[f_x+f],\cdots,\cup[f_x+(q-1)f]$$

同样地，将线性编码 C 中所有 f_y 函数用 f 代替，可以得到多项式编码 C'。由推论 8，C 中任意两函数若互相独立，则它们在 C' 中对应的函数会分属于 L' 中不同的等价集合，因此它们对应的函数在 L' 中也互相独立。即，若 C 为可行编码，则 C'也可行。进一步，$q\geqslant 3$ 时 f 是存在的：计有$(q!)^q$ 个函数与 f_x 互相独立，而仅有 $q^2(q-1)$个线性函数独立于 f_x。当 $q\geqslant 3$，有$(q!)^q>q^2(q-1)$，得证。

举例，图 2 演示了这样的多项式编码(对应于图 1)。

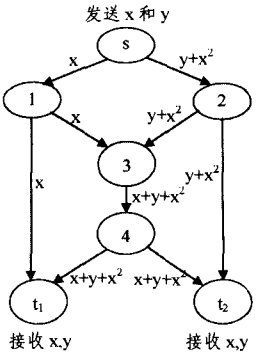

图 2 源节点执行非线性操作的多项式编码

进一步，独立于 f_x 的函数 f 具有以下特征：

定理 10 若函数 f 可写成 $f=yf_1(x)+f_2(x)$的形式，其中 $f_1(x)$，$f_2(x)$为度小于 q 的多项式且对 $\forall x\in\Sigma$有 $f_1(x)\neq 0$，则 f 独立于 f_x。特别地，当 $q=3$ 时，逆命题也成立。

证明：对不同点$(\alpha,\beta),(\alpha',\beta')\in\Sigma^2$，若 $\alpha=\alpha'$，有 $f(\alpha,\beta)=\beta f_1(\alpha)+f_2(\alpha)$和 $f(\alpha,\beta')=\beta' f_1(\alpha)+f_2(\alpha)$。由于 $f_1(\alpha)\neq 0$，有 $f(\alpha,\beta)\neq f(\alpha,\beta')$。若 $\alpha\neq\alpha'$，则有 $f_x(\alpha,\beta)\neq f_x(\alpha',\beta')$。因此，$(f_x(\alpha,\beta),f(\alpha,\beta))\neq(f_x(\alpha',\beta'),f(\alpha',\beta'))$，它们互相独立。反之，符合 f 形式的函数共有$(q-1)^q q^q$ 种，但仅有$(q!)^q$ 种独立于 f_x。当 $q=3$ 时，二者数量相等，因此此时逆命题也成立。

3.3 多元字符表上更一般的编码

能否允许中间节点执行非线性操作，从而构造更一般的多项式编码？本节给出肯定的回答。首先引入一些定义：

一个 q 阶拉丁矩阵是个 $q\times q$ 方阵，它的行及列都是 q 个符号的一种排列[12]。二元函数 $f:\Sigma^2\to\Sigma$能被写成矩阵$\{a_{xy}\}$的形式，其中 x 行 y 列的元素 a_{xy}取值满足 $a_{xy}=f(x,y)$。同样地，f_x,f_y 可分别写成矩阵 $a_{xy}=x$ 和 $a_{xy}=y$。由拉丁矩阵定义可知：一个拉丁矩阵唯一表示了一个独立于 f_x 且独立于 f_y 的函数 f。我们把 q 阶拉丁矩阵的总个数记为 $LS(q)$，它的值满足以下公式[12]：

$$LS(q)\geqslant\frac{(q!)^{2q}}{q^{q^2}}$$

而从排列组合上可知，同时独立于 f_x 和 f_y 的线性函数共有 $q(q-1)^2$ 个。不难证明以下不等式(证明略)：

$$\frac{(q!)^{2q}}{q^{q^2}}\geqslant q(q-1)^2$$

由此可知存在多项式函数同时独立于 f_x 和 f_y。例如当 $q=5$ 时，x^3+y^3是这样的函数。我们可构造多项式编码如图 3 示。

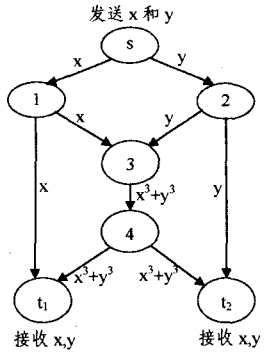

图 3 中间结点执行非线性编码的多项式编码

结束语 本文提出非线性编码的新描述。基于该描述，证明了一类非线性编码有着线性码相同的结构，并能从线性码中构造出来；证明了另一个类非线性编码的存在性。

参 考 文 献

[1] Ahlswede R, Cai N, Li S Y R, et al. Network information flow. IEEE Transactions on Information Theory, 2000, 46(4): 1204-1216

[2] Li S Y R, Cai N. Linear network coding. IEEE Transactions on Information Theory, 2003, 49(2): 371-381

[3] Ho T, Koetter R, Medard M, et al. The benefits of coding over routing in a randomized setting // IEEE International Symposium on Information Theory (ISIT). 2003

[4] Chou P, Wu Y, Jain K. Practical network coding // Allerton Conference on Communication, Control, and Computing. 2003

[5] Jaggi S, Sanders P, Chou P, et al. Polynomial time algorithms for multicast network code construction. IEEE Transactions on Information Theory, 2005, 51(6): 1973-1982

[6] Koetter R, Medard M. An algebraic approach to network coding. IEEE/ACM Transactions on Networking (TON), 2003, 11(5): 782-795

[7] Feder M, Ron D, Tavory A. Bounds on linear codes for network multicast // Electronic Colloquium on Computational Complexity (ECCC). 2003, 10(033)

[8] Lehman A, Lehman E. Complexity classification of network information flow problems // Proceedings of the Fifteenth Annual ACM-SIAM Symposium on Discrete Algorithms. 2004: 142-150

[9] Dougherty R, Freiling C, Zeger K. Linearity and solvability in multicast networks. IEEE Transactions on Information Theory, 2004, 50(10): 2243-2256

[10] Dougherty R, Freiling C, Zeger K. Insufficiency of linear coding in network information flow. IEEE Transactions on Information Theory, 2005, 51(8): 2745-2759

[11] Greuel G, Greuel G, Pfister G. A Singular Introduction to Communicative Algebra. Berlin: Springer, 2002

[12] Van Lint J, Wilson R. A Course in Combinatorics. 2ed. Cambridge: Cambridge University Press, 2001