第 20 卷 第 6 期
1998 年 11 月

电 子 科 学 学 刊
JOURNAL OF ELECTRONICS

Vol.20 No.6
Nov. 1998

一种可用于非线性码译码神经网络模型研究 [1]

马晓敏　　杨义先　　章照止 *

(北京邮电大学信息工程系 126 信箱　北京　100088)
*(中国科学院系统科学研究所　北京　100080)

摘　要　本文提出一种非线性码神经网络译码方案，在纠错能力范围内对满足码距特性的一般非线性码以零错误概率进行纠错译码，并在检错能力范围内检错。文中具体描述了神经网络模型构造、学习算法及其理论依据。最后通过非线性等重码的译码实例表明此方案的有效性及理论和应用价值。

关键词　非线性码，译码，神经网络
中图号　TN918, TN-052

1　引　言

与线性分组码相比较，非线性码码字个数多、编码效率高、保密性强，在现代通信中正得到越来越多的使用。到目前为止，已有一些研究非线性码特性及探索的成果出现 [1−3]。但是非线性码仍缺乏完善的理论基础，因此非线性码译码也尚无成熟的理论指导和有效的一般方法。由于神经网络具有并行、记忆联想、可学习及非线性逼近等特点，用于译码可改善信道译码的速度和性能。近年来，出现了利用神经网络进行非线性码译码方案 [4−6]，但是由于所采用的 Hopfield 、前向多层网等神经网络模型固有的局部极小、容量小、泛化能力弱等缺点，导致这些译码方案在规模和可靠性上都受到限制，并且纠错能力弱 (只能纠 1 个错)，很难实用化。

本文对文献 [7, 8] 线性分组码译码方案的神经网络结构和学习算法的局限性作进一步研究，提出一种新的可适于满足距离特性的一般非线性码的神经网络译码方案。下面首先给出非线性码的定义和表示，并讨论其特性。然后，对非线性码神经网络译码模型、学习算法、纠错译码过程作系统的描述和分析。最后给出非线性码的译码实例。

2　非线性码神经网络译码模型

2.1　非线性码描述

定义　二进 $(n, M, d_{\min})$ 码 C 是 M 个 n 位二元向量的集合，在这个集合里，任意两个码字间的汉明距离大于或等于 $d_{\min}$，即 $d_{\min}$ 为码 C 的最短距离。

注意　非线性码的描述形式与线性分组码稍有不同，线性分组码的 $(n, k, d_{\min})$ 相当于上述定义的 $(n, 2^k, d_{\min})$。另外，对于线性分组码，码字间的最小距离等于码字的最小汉明重量，即

$$W_{\min}(C) = d_{\min}. \tag{1}$$

而对于非线性码，码间距离与码字最小汉明重量一般不相等，当 $\mathbf{0} = \{0, 0, \cdots, 0\}$ 作为非线性码 C 的码字，则有

$$W_{\min}(C) \geq d_{\min}. \tag{2}$$

[1] 1997-08-01 收到，1998-04-10 定稿
国家自然科学基金资助项目 (批准号 69772035, 69896240)

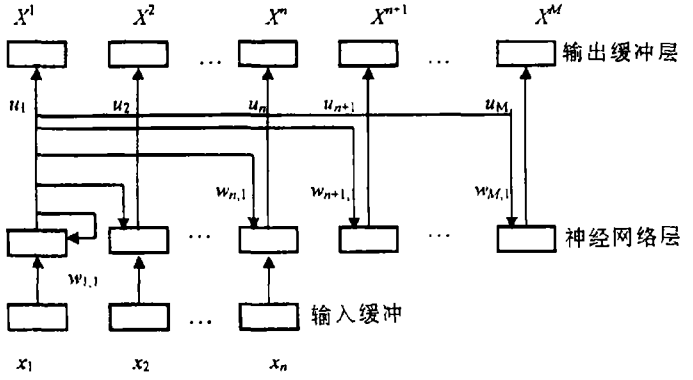

图 1 神经网络译码结构框图

2.2 用于译码的神经网络模型 对于码 $C(n,M,d_{\min})$，它有 M 个码字 $X_1,X_2,\cdots,X_M$，每个码字有 n 个二进位 $X^h=(x_1^h,x_2^h,\cdots,x_n^h)$, $x_i^h\in\{0,1\}$, 其相应的神经网络译码模型结构如图 1 所示：它有 M 个神经元，输入为 n 个码元，每个输出代表一个译码码矢，一般 $M>n$，每个神经元 i 满足如下关系：

$$u_i(t+\tau)=l\left[\sum_{j=1}^{n}a_{ij}u_j(t)-\theta_i\right],\quad i=1,\cdots,M. \tag{3}$$

这里 $l[x]=\begin{cases}1, & \text{当}x>0,\\ 0, & \text{当}x\le 0,\end{cases}$ $u_i(t)$ 是神经元在时刻 t 的状态，θ_i 是神经元 i 的阈值，τ 为传输延迟，a_{ij} 表示神经元 j 到神经元 i 的连接权系数。上述表达式用矢量表示为

$$\boldsymbol{U}(t+\tau)=l[\boldsymbol{A}\boldsymbol{U}(t)-\boldsymbol{\theta}]. \tag{4}$$

这种神经网络与 Hopfield 模型相似，神经元之间高度互连，并行运算。但它们之间的本质区别在于，此模型的输入输出个数不相等，且神经元之间的联接是非对称的。

与文献 [7, 8] 神经网络模型不同的是，这里的神经元代表了码 C 中的所有码字，没有把 $\mathbf{0}=\{0,0,\cdots,0\}$ 码字作为缺省输出，因为非线性码不一定有 $\mathbf{0}$ 码字，如果 $\mathbf{0}\in C$，则有一个神经元输出代表此码字。在下面我们将会看到，这种结构上的变化，为非线性码译码提供了必要的环境，也给线性码译码过程增加了检错能力，提高了译码可靠性。

3 神经网络译码训练

设码 $C=\{X^1,X^2,\cdots,X^M\}$ 可纠正 e 个错误，即码间最短距离 $d_{\min}\ge 2e+1$。训练神经网络对码 C 进行译码可分为权系数和阈值确定两步进行。

第一步 确定权系数。利用 $X^1,X^2,\cdots,X^M$ 作为训练样本，权系数由如下式确定：设定初始值 $a_{pk}=0$，对于码字样本 X^h：

$$a'_{pk}=\begin{cases}1/[W_H(X^h)], & \text{当}X^h\ne\{0\}\quad p=h\quad \text{且}X_k^h=1;\\ -1/[W_H(X^h)], & \text{当}X^h\ne\{0\}\quad p=h\quad \text{且}X_k^h=0;\\ -\beta, & \text{当}X^h=\{0\}\quad p=h;\\ a_{pk}, & \text{当}p\ne h.\end{cases} \tag{5}$$

上式中 $W_H(X^h)$ 为码字 X^h 的汉明重量，β 为一个常数，$\beta \geq 1/[W_{\max}(C)]$, $W_{\max}(C) = \max_h\{W_H(X^h)\}$

第二步 确定阈值. 对于码 C，神经网络的阈值确定如下：

$$\theta_h = \begin{cases} -\varepsilon - e\Delta_h, & \text{当} X^h = \{0\}; \\ 1 - \varepsilon - e\Delta_h, & \text{当} X^h \neq \{0\}; \end{cases} \tag{6}$$

这里

$$\Delta_h = \begin{cases} 1/[W_H(X^h)], & \text{当} X^h \neq \{0\}; \\ \beta, & \text{当} X^h = \{0\}; \end{cases}$$

上式中，ε 理论上为无穷小，具体实现时限制为：$0 < \varepsilon < 1/[W_{\max}(C)]$.

定理 对任意输入 $\forall X^h \in C$，设 X^h 和 y 分别为传输和接收码矢，且有 $d_H(X^h, y) \leq e$，如果阈值减小 $e\Delta h$，即当依照 (5), (6) 式确定权系数矩阵及阈值，必有且只有第 h 个神经元被激活，即

$$u_h = 1, \quad u_r = 0(\forall r \neq h).$$

证明 (1) 当 C 不包括 **0** 码字时

(a) 对于满足 $d_H(X^h, y) \leq e$ 的 y，有

$$A_h y - \theta_h = 1 - \frac{d_H(X^h, y)}{W_H(X^h)} - (1 - \varepsilon - e\Delta_h) \geq 1 - \frac{e}{W_H(X^h)} - 1 + \varepsilon + \frac{e}{W_H(X^h)} = \varepsilon > 0, \quad \text{故} \quad u_h = 1.$$

(b) 对于 $d_H(X^h, y') \geq e + 1$ 的 y' 有

$$A_h y' - \theta_h = 1 - \frac{d_H(X^h, y')}{W_H(X^h)} - (1 - \varepsilon - e\Delta_h) \leq 1 - \frac{e+1}{W_H(X^h)} - 1 + \varepsilon + \frac{e}{W_H(X^h)} = -\frac{1}{W_H(X^h)} + \varepsilon,$$

因 $\varepsilon < \frac{1}{W_{\max}(C)}$, 故 $A_h y' - \theta_h < 0 \Rightarrow u_h = 0$.

(c) 对于 $\forall r \neq h$，由 $d_H(X^h, y) \leq e \Rightarrow d_H(X^r, y) \geq e + 1$，故当输入为 y 时，

$$A_r y - \theta_r = 1 - \frac{d_H(X^r, y)}{W_H(X^r)} - (1 - \varepsilon - e\Delta_r) < 0, \quad \text{故} u_r = 0.$$

(2) 当 C 包含码字 $X^h = \mathbf{0}$，其余非零码字间结论证明同 (1)．对于 $X^h = \mathbf{0}$，有

(a) 当 $d_H(X^h, y) \leq e$，有：$A_h y - \theta_h \geq -e\beta + \varepsilon + e\Delta_h = \varepsilon > 0 \Rightarrow u_h = 1$.

(b) 当 $d_H(X^h, y') \geq e + 1$，有 $A_h y' - \theta_h \leq -(e+1)\beta + \varepsilon + e\Delta_h = -\beta + \varepsilon$．因 $\beta \geq 1/[W_{\max}(C)]$, $\varepsilon < 1/[W_{\max}(C)]$, 故 $A_h y' - \theta_h < 0 \Rightarrow u'_h = 0$.

(c) 当 $\forall r \neq h$, $d_H(X^h, y) \leq e \Rightarrow d_H(X^r, y) \geq e + 1$, 必有 $A_r y - \theta_r < 0 \Rightarrow u_r = 0$． 证毕

上述定理表明：当码字间最小距离 $d_{\min} \geq 2e + 1$，按 (5), (6) 式调整阈值，神经网络输出与码输入 C 中的各个码字是一一对应的，神经网络可纠 e 个错误，而对于大于 e 个错误的接收码字，神经网络所有神经元的输出端为 **0**．由定理的证明过程可知，神经网络译码器适应于码间距离满足一定特性的所有线性码或非线性码，对码距与重量间的关系和全 **0** 码字的出现没有要求．从而拓展了文献 [7, 8] 方案只适于线性分组码译码的局限性．

4 译码实现及举例

神经网络译码器针对码 C 进行训练后，就可以作为译码器对来自二进对称信道 (BSC) 的码字进行译码。译码器既可以软件实现也可以集成为一个可编程的硬件芯片。其学习和译码过程如下：

(1) 设置初始连接权系数 $a_{ij}=0$ 。

(2) 把码 C 中的码字作为样本，按 (5),(6) 式确定神经网络的权系数、阈值。

(3) 输入接收样本 y 至神经网络输入端。

(4) 如果有一个 h 神经元激活，即 $u_h=1, u_r=0(\forall r\neq h)$ ，则译码成功，输出第 h 端对应码 C 中的码字。如果 $u_r=0(\forall r)$ ，则 y 有多于 e 个错误出现，可请求重发。

(5) 转至 (3) 接收新码字，直至结束。

注：文献 [7] 中神经网络对码字 $y=\{\mathbf{0}\}+e'(e'\leq e)$ 及 $y': d(y',c)\geq e+1$ 的输出均为 $u=0$，这样在实际译码过程中易将错误个数大于 e 个的码字错译成码字 $\mathbf{0}$ 。而本译码方案避免了这种情形，增加了译码的可靠性，还可以在检错能力范围内检出错误。

通过软件仿真实现前述译码方案，并对若干非线性码进行纠错译码，表明此方案对于非线性码的各种错误模式均可正确译码或检错。从而证明了其对非线性码译码的有效性。下面举一例加以说明：

例 C 为 $n=8$ 的非线性等重码 [5]:

$$C_1=\{11110000\}^T,\ C_2=\{00001111\}^T,\ C_3=\{11001100\}^T,\ C_4=\{00110011\}^T,$$
$$C_5=\{11000011\}^T,\ C_6=\{00111100\}^T,\ C_7=\{10101010\}^T,\ C_8=\{01010101\}^T.$$

可以看出上述码的码参数为 (8, 8, 4) ，此码可纠正 $e=1$ 个错误，检两个错误。其神经网络译码器有 8 个神经元，由 (5) 式可得其权系数矩阵，阈值初始化为 $1-\varepsilon(\varepsilon<0.25)$, $\Delta=\Delta_h=1/[W_h(X^h)]=1/4$, $e\Delta=1/4$, $\theta_1=\theta_2=\cdots=\theta_8=3/4-\varepsilon$ 。神经网络训练完毕后，当接收码字： $y=\{01110000\}^T$ 。经过一次迭代可得： $A_1y-\theta_1=3/4-(1-e\Delta-\varepsilon)=3/4-1+1/4+\varepsilon=\varepsilon>0\Rightarrow u_1=1$ ，第一个神经元激活。又经计算机编程验证，对于 $\forall r\neq 1$, $A_ry-\theta_r<0$,译码唯一,这样可得译码码字为 $C_1=\{11110000\}^T$ 。当接收码字 $y=\{00110000\}$, 有： $A_1y-=\theta_1=2/4-1+1/4+\varepsilon=-1/4+\varepsilon=-1/4+\varepsilon<0(\varepsilon<1/4)\Rightarrow u_1=0$ 。同样对于 $\forall r\neq 1$, $A_ry-\theta_r<0\Rightarrow u_r=0$ ，没有神经元激活意味着接收码字存在 2 位以上的错误，申请重发。

致谢 感谢北京邮电大学信息安全中心全体老师与同学的热情协助！

参 考 文 献

[1] Macwilliams F J, *et al.* The Theory of Error-correcting Codes. New York: North-Holland, 1977.

[2] Bruck J, *et al.* Neural networks error correcting codes and polynomials over the binary n cube. IEEE Trans. on Inform. Theory, 1989, IT-35(4): 976–987.

[3] 杨义先，林须端. 编码密码学. 北京：人民邮电出版社， 1992, 304–456.

[4] 杨义先. 人工神经网络能量函数与纠错码译码算法. 模式识别与人工智能， 1991, 4(3): 22–27.

[5] Jin Fan, *et al.* A new class of nonlinear error control codes based on neural networks. JSJO, 1995, 3(2): 109–116.

[6] 许成谦，等. 神经网络与非线性码最小加权距离译码算法. 北京邮电大学学报， 1994, 17(2): 23–26.

[7] Espositom A, *et al.* A neural network for error correcting decoding of binary linear codes. Neural Networks, 1994, 7(1): 195–202.

[8] Lifang Li, *et al.* A modified learning rule of the neural network for error correcting decoding. Proc. of ICONIP'95, Beijing: 1995: 562–565.

A NEURAL NETWORK FOR DECODING OF NONLINEAR CODES

Ma Xiaomin Yang Yixian Zhang Zhaozhi*

(*Dept. of Infm. Eng., Beijing University of Posts and Telecommunications, Beijing*100088)

*(*Institute of System Science, Academia Sinica, Beijing* 100080)

Abstract A decoding strategy for nonlinear codes using a neural network is presented. Within the capacity of error correction, it can correct and detect errors of general nonlinear codes which have some specific code distance with zero error probability. This paper describes structure of the neural network, learning algorithm and theory analysis. Finally, one decoding example: nonlinear constant weight code is demonstrated to prove the availability and values of theory and application.

Key words Nonlinear codes, Decoding, Neural networks

马晓敏： 男， 1964 年出生，副教授，博士生，研究领域为智能信息处理，编码密码，软件无线电等.

杨义先： 男， 1961 年出生，教授，博士生导师，研究领域为密码，编码，网络信息安全，信号与信息处理等.

章照止： 男， 1934 年出生，研究员，研究领域为密码，编码，神经网络等.