置信传播译码算法的性能测度

贺玉成[1],杨 莉[1],王新梅[1],福田明[2]
(1. 西安电子科技大学综合业务网国家重点实验室,陕西西安 710071;2. 日本静冈大学福田通信工学研究室,日本浜松 432-8561)

摘 要: 本文基于树和有限状态机系统地推导了低密度校验码(LDPC)置信传播译码算法中的消息修正公式,引入了连续消息空间的概率测度,推导了常见二元对称信道输出分布和迭代过程中消息密度进化的计算公式,讨论了算法性能的参数化估计.这种计算分析工具可以用于独立于信道的算法收敛性分析,有助于设计 LDPC 码,有助于分析 LDPC 码译码器的量化效应并实现快速译码方案,使其获得在实时通信系统中的应用.

关键词: 测度; 置信传播算法; 迭代译码; LDPC 码; Turbo 码
中图分类号: TN911.22 **文献标识码**: A **文章编号**: 0372-2112 (2002) 04-0577-04

Measure on the Performance of Belief Propagation Decoding Algorithm

HE Yu-cheng[1], YANG Li[1], WANG Xin-mei[1], FUKUDA Akira[2]
(1. *National Key Lab of Integrated Service Networks, Xidian University, Xi'an, Shaanxi* 710071, *China*;
2. *Fukuda Communications Engineering Lab, Shizuoka University, Hamamatsu* 432-8561, *Japan*)

Abstract: Formulas for updated rules of the belief propagation algorithm applied to low density parity check (LDPC) codes are systematically derived based on the tree and the finite state machine (FSM). The probability measure on the continuous message space is introduced to evaluate the evolution of message densities within iterative decoding rounds, and derivations of the output distributions of common binary symmetric channels and the message density evolution are given in detail. The parameterized estimation of the performance of the algorithm is also discussed. The analytic and calculable means can be used to make systematical analysis for the convergence of BP algorithms independent of channels, and can be of help in designing LDPC codes and analyzing quantization effects for the fast decoding on the purpose of practical applications of LDPC codes to real-time communication systems.

Key words: measurement; belief propagation algorithm; iterative decoding; LDPC codes; Turbo codes

1 引言

和积算法是基于因子图为专家系统开发的一种概率推理算法[1].因子图中,函数节点对每一个相邻变量节点由其他相邻变量节点求和计算边界消息并传递至该变量节点,变量节点对每一个相邻函数节点将其他相邻函数节点传递的边界消息求积后传递至该函数节点,从而调整函数节点的边界计算.消息空间及"和"、"积"运算构成一个半环.引入不同的半环,和积算法可以演化为多种常见算法,包括贝叶斯(Bayesian)网络的 Pearl 置信传播算法、快速傅立叶变换算法、前向/后向算法、Turbo 迭代译码算法[2]、维特比算法以及低密度校验码(LDPC)的大数判决译码算法.纠错码译码中的消息空间总是基于概率测度而定义的,这时,和积算法也称为置信传播(BP)算法.

本文以最大似然测度(measure)引入对数量度(metric)的连续消息空间,系统地分析了低密度校验码置信传播译码算法中的消息传递方式及修正公式,推导了迭代过程中消息密度的进化.关于离散消息的讨论参见文献[3,4].

2 消息传递与计算

设二元码元符号$\{0,1\}$映射为双极信道符号$\{+1,-1\}$后由二元输入信道传输,信道输入集和信道输出集分别由 X 和 Y 表示.设随机变量 $x\in X$ 和 $y\in Y$,软判决译码器基于 y 以最大似然测度 $\mu_{ML}(x)\equiv p(y|x)$ 计算对数似然比量度 $\log(p_{+1}/p_{-1})$,其值域由 A 表示.其中,(p_{+1},p_{-1}) 是节点比特值$\{+1,-1\}$的概率密度[2].在不致混淆的情况下,同构空间$\{0,1\}$和$\{+1,1\}$及其概率密度(p_0,p_1)和(p_{+1},p_{-1})在文中将等价应用.

正则二元 LDPC 码(n,d_v,d_c)的码长为 n,设计码率为 $R\equiv 1-d_v/d_c$.因子图表示中,每个变量节点具有 d_v 条入射边,每个校验节点具有 d_c 条入射边.离散无记忆对称信道模型下,当译码与传输码字无关时,译码错误独立于传输的码字.本文不失一般性地假设编码器输出为全零码字,即信道传输全 1 码字.

概率密度(p_0,p_1)可以等价表示为变换度量 $\Delta p=p_0-p_1$ 和 $m=\log(p_0/p_1)$,且

收稿日期:2000-11-13;修回日期:2001-04-15
基金项目:国家自然科学基金(No.69972035)

$$m = \log \frac{1 + \Delta p}{1 - \Delta p} \tag{1}$$

$$\Delta p = \frac{e^m - 1}{e^m + 1} = \tanh \frac{m}{2} \tag{2}$$

设 M 表示置信传播迭代译码过程中进化的对数似然比消息空间. 显然,初始消息空间 $A \subseteq M$.

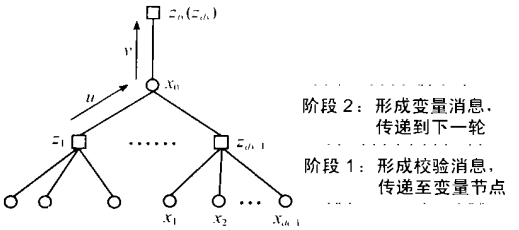

图 1 消息传递的局部子树

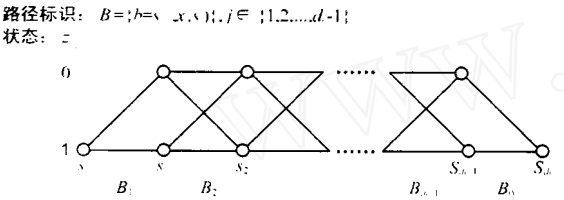

图 2 校验关系的 FSM 表示

迭代初始化主要由信道接收值按映射 $\phi^{(0)}: R \to A$ 计算初始消息 u_0,并传递给变量节点. 每轮迭代包括校验消息传递和变量消息传递两个阶段. 在第 l 轮迭代中,校验消息由映射函数 $\phi_c^{(l)}: M^{(d_c - 1)} \to M$ 形成,传递给变量节点;变量消息由映射函数 $\phi_v^{(l)}: A \times M^{(d_v - 1)} \to M$ 形成,传递给校验节点,用于下一轮校验消息计算. 完成预定次数的迭代后,算法终止于变量消息传递. 图 1 的理想局部树图描述了消息的计算和传递过程,这里没有考虑并行边和短循环路径.

给定序偶 (x_0, z_0),每一个校验节点 $z \in \{z_1, \cdots, z_{d_v - 1}\}$ 要传递给 x_0 的消息 u,由各自的孩子变量节点在上次迭代中传递来的消息进行计算. z 与其相邻变量节点的约束关系可用图 2 所示的有限状态机描述[2]. 这是一个一阶马尔可夫源,状态空间为 $GF(2)$,初始状态为零状态,部分校验和为转移状态,转移分支标识 $b_j \in B_j$ 为 3 重 (s_{j-1}, x_j, s_j),且 $|B_j| = 4$. 对 b_j 引入半环 $(R_+, +, \cdot)$ 作概率测度,"+"和"·"分别表示非负实数环 R_+ 上的实数加法和乘法运算. 不同时刻 $k < l$ 的一对状态 s_k 和 s_l 之间,每条路径的路径值为其级连分支测度值的乘积,所有路径值之和称为该状态对的流值 (flow). 每个二元变量 x_j 表示相应变量节点对应的码元比特,且 $s_j = s_{j-1} + x_j = \sum_{k=1}^{j} x_k$. 设当前校验节点 $z = s_{d_c}$,消息 u 为

$$u = \log \frac{P(s_{d_c} = 0 \mid x_0 = 0)}{P(s_{d_c} = 0 \mid x_0 = 1)} = \log \frac{P(s_{d_c - 1} = 0)}{P(s_{d_c - 1} = 1)}$$

$$= \log \frac{P\left(\sum_{j=1}^{d_c - 1} x_j = 0\right)}{P\left(\sum_{j=1}^{d_c - 1} x_j = 1\right)} \tag{3}$$

其中:第二个等式的分子和分母分别为流值 $\rho(s_0, s_{d_c - 1} = 0)$ 和 $\rho(s_0, s_{d_c - 1} = 1)$;第三个等式的分子和分母正好是随机变量 $\{x_j : j = 1, \cdots, d_c - 1\}$ 和为 0、1 的概率分布律 (P_0, P_1),可以由各个随机变量的概率分布律卷积计算. 设 $\Delta P = P_0 - P_1$,Δp_j 为 x_j 概率密度的变换表示,v_j 为 x_j 的发送的消息,结合式 (1) 和 (2),得下列等价的计算式[4,5]:

$$\Delta P = \prod_{j=1}^{d_c - 1} \Delta p_j \tag{4}$$

$$u = \log \frac{1 + \prod_{j=1}^{d_c - 1} \Delta p_j}{1 - \prod_{j=1}^{d_c - 1} \Delta p_j} \tag{5}$$

$$\tanh \frac{u}{2} = \prod_{j=1}^{d_c - 1} \tanh \frac{v_j}{2} \tag{6}$$

变量节点 x_0 向校验节点 z_0 传递的消息 v,由其它 $d_v - 1$ 个校验节点 $\{z_1, \cdots, z_{d_c - 1}\}$,在阶段 1 传递来的消息 $\{u_1, \cdots, u_{d_v - 1}\}$ 及变量节点 x_0 的初始消息 u_0 计算如下:

$$v = \log \frac{P(x_0 = 0 \mid \{z_i = 0\})}{P(x_0 = 1 \mid \{z_i = 0\})} = \log \frac{P(x_0 = 0)\ P(\{z_i = 0\} \mid x_0 = 0)}{P(x_0 = 1)\ P(\{z_i = 0\} \mid x_0 = 1)}$$

$$= \log \frac{P(x_0 = 0) \prod P(z_i = 0 \mid x_0 = 0)}{P(x_0 = 1) \prod P(z_i = 0 \mid x_0 = 1)} = \sum_{i=0}^{d_v - 1} u_i \tag{7}$$

迭代终止后,作如下判决:

$$\hat{x}_j = \operatorname{sign}\left(\sum_{i=0}^{d_v} u_{ji}\right),\ j = 1, 2, \cdots, n \tag{8}$$

其中:$u_{ji}, i = 1, \cdots, d_v$,表示变量 x_j 的所有 d_v 个相邻校验节点传递的消息;u_{j0} 表示变量 x_j 的初始消息.

3 消息空间的测度与密度进化

引入消息空间 A 和 M 的勒贝格 (Lebesgue) 概率测度空间 $\prod_A$ 和 $\prod_M$. 校验消息传递和变量消息传递将导致如下的测度空间进化:

$$\Psi_e^{(l)}: \prod_M^{d_c - 1} \to \prod_M \tag{9a}$$

$$\Psi_v^{(l)}: \prod_A \times \prod_M^{d_v - 1} \to \prod_M \tag{9b}$$

连续消息空间的概率测度用概率密度函数表示,简称密度. 测度空间的进化由密度进化反映. 消息密度的进化直接受到初始消息密度的影响,所以取决于信道模型的初始消息密度也称为先验密度.

图 3 反映了在一轮迭代中消息空间及其测度空间的进化过程. 在第 l 轮迭代中,$P(v)$ 是输入消息密度,它在 $l = 1$ 时表示初始消息密度;$R(u)$ 是校验节点传递的消息密度,是输入消息的函数 $\phi_c^{(l)}$ 的密度;$Q(v)$ 是变量节点传递的消息密度,是校验消息的函数 $\phi_v^{(l)}$ 的密度,也是本次迭代完成的进化密度,它将作为下一轮迭代的输入密度.

定理 1 设随机变量 X 具有密度 $f_X(x)$,$-\infty < x < +\infty$. $Y = g(X)$,函数 $g(x)$ 为严格单调函数,则随机变量 Y 的密度为

$$f_Y(y) = \begin{cases} f_X(h(y)) \mid h'(y) \mid, & \alpha < y < \beta \\ 0, & \text{其它} \end{cases} \tag{10}$$

其中:$\alpha = \min\{g(-\infty), g(+\infty)\}$;$\beta = \max\{g(-\infty), g(+\infty)\}$;$h(y)$ 为 $g(x)$ 的反函数.

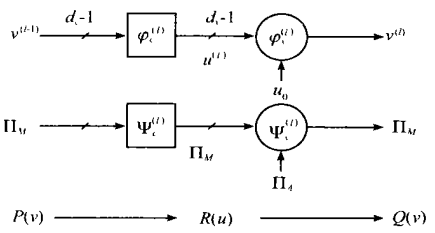

图 3　第 l 轮迭代的密度进化过程

设信道输入为 +1.转移概率为 δ 的 BSC 信道下,正确初始消息等于 $\log[P(+1|+1)/P(+1|-1)]=\log[(1-\delta)/\delta]$,其概率为 $1-\delta$;错误初始消息等于 $\log[P(-1|+1)/P(-1|-1)]=\log[\delta/(1-\delta)]$,其概率为 δ,所以先验密度函数为

$$P_{BSC}^{(0)}(v)=(1-\delta)\Delta\left(v-\log\frac{1-\delta}{\delta}\right)+\delta\Delta\left(v+\log\frac{1-\delta}{\delta}\right) \tag{11}$$

其中 $\Delta(x)$ 为单位冲激函数.

对于均值为 0 和方差为 σ^2 的 AWGN 信道,信道输出 x 的密度为 $P(x)=\exp\{-(x-1)^2/2\sigma^2\}/\sqrt{2\pi}\sigma$,应用定理 1,求得初始消息 $u_0=(2/\sigma^2)x$ 的密度函数为

$$P_{AWGN}^{(0)}(v)=\frac{\sigma}{2\sqrt{2\pi}}\exp\left\{-\frac{(v\sigma^2/2-1)^2}{2\sigma^2}\right\} \tag{12}$$

为便于计算,消息空间再次变换.$\Delta p\in(-1,+1)$ 分解为符号与绝对值两个部分[3],表示为序偶 $(\mathrm{lgsgn}\,\Delta p,-\log|\Delta p|)\in GF(2)\times R_+$,其中 $\mathrm{lgsgn}\,\Delta p=(1-\mathrm{sgn}(\Delta p))/2$.$\Delta p=0$ 时应予以单独考虑.式(4)变换后,并将式(2)代入得[3,4]:

$$\left(\mathrm{lgsgn}\left(\tanh\frac{u}{2}\right),-\log\left|\tanh\frac{u}{2}\right|\right)=\left(\sum_{j=1}^{d_c-1}\mathrm{lgsgn}\left(\tanh\frac{v_j}{2}\right),-\sum_{j=1}^{d_c-1}\log\left|\tanh\frac{v_j}{2}\right|\right) \tag{13}$$

其中,第一个分量的加法基于 $GF(2)$,第二个分量的加法基于实数域.消息空间的变换导致其测度密度的相应变换.

消息变换函数 $y=-\log|\tanh(v/2)|\in R_+$,在 $v>0$ 和 $v<0$ 两个区间内分别严格单调,变换与反变换具有对称的函数形式.对数似然比 $v>0$ 时,变换对为 $y=-\log[\tanh(v/2)]$ 和 $v=-\log[\tanh(y/2)]$;当 $v<0$ 时,变换对为 $y=-\log[\tanh(-v/2)]$ 和 $-v=-\log[\tanh(y/2)]$.设变换空间 $GF(2)\times R_+$ 的密度为 $P_Y=(P_Y^0(y),P_Y^1(y))$,其中 $P_Y^0(y)=P_Y(0,y)$ 和 $P_Y^1(y)=P_Y(1,y)$ 分别对应 $v>0$ 和 $v<0$ 两种情况.已知对数似然比消息密度 $P_M(v)$,应用定理 1,变换消息 $y>0$ 的密度 P_Y 为[4]

$$P_Y^0(y)=\frac{1}{\sinh y}P_M\left[-\log\left(\tanh\frac{y}{2}\right)\right] \tag{14a}$$

$$P_Y^1(y)=\frac{1}{\sinh y}P_M\left[\log\left(\tanh\frac{y}{2}\right)\right] \tag{14b}$$

若已知变换消息密度 P_Y,则对数似然比消息的密度为

$$P_M(v)=\begin{cases}\dfrac{1}{\sinh v}P_Y^0\left[-\log\left(\tanh\dfrac{v}{2}\right)\right], & v>0\\ \dfrac{1}{\sinh(-v)}P_Y^1\left[-\log\left(\tanh\dfrac{-v}{2}\right)\right], & v<0\end{cases} \tag{15}$$

其中,$\sinh x=(e^{2x}-1)/2e^x$.

式(13)表示在变换空间 $GF(2)\times R_+$ 上,校验消息是函数 $\phi_c^{(l)}$ 的 d_c-1 个独立同分布的输入消息之和,所以其密度 $R_Y=(R_Y^0(y),R_Y^1(y))$ 是 d_c-1 个相同输入变换密度 P_Y 的卷积,即 $R_Y=\otimes^{d_c-1}P_Y$,其中 $\otimes$ 为卷积运算符,P_Y 由对数似然比输入消息的密度 $P(v)$ 按式(14a)和(14b)变换得到.卷积运算在进行傅立叶变换后转换为乘积运算.空间 $GF(2)\times R_+$ 上的函数 P_Y 的傅立叶变换 $F(R_Y)$ 为:

$$F_P[s,0]=L_P^0(s)+L_P^1(s) \tag{16a}$$

$$F_P[s,1]=L_P^0(s)-L_P^1(s) \tag{16b}$$

其中 $L_P^0(s)=L[P_Y^0(y)]$ 和 $L_P^1(s)=L[P_Y^1(y)]$ 是拉普拉斯变换,即傅立叶变换域为实数域.设第 $l-1$ 轮迭代结束后变量节点传递的对数似然比消息密度为 $P^{(l-1)}$,空间 $GF(2)\times R_+$ 上消息密度相应为 $P_Y^{(l-1)}$,则第 l 轮迭代中在 $GF(2)\times R_+$ 空间上校验消息的密度 $R_Y^{(l)}$ 的傅立叶变换 $F(R_Y^{(l)})$ 的计算式为

$$F_R^{(l)}[s,0]=[L_P^{(l-1),0}(s)+L_P^{(l-1),1}(s)]^{d_c-1} \tag{17a}$$

$$F_R^{(l)}[s,1]=[L_P^{(l-1),0}(s)-L_P^{(l-1),1}(s)]^{d_c-1} \tag{17b}$$

该式计算结果经傅立叶逆变换得 $R_Y^{(l)}$,再由式(15)计算出对数似然比消息空间上校验消息的密度 $R^{(l)}(u)$.

如式(7)所示,变量节点传递的消息 v 是该节点的初始消息 u_0 与函数 $\phi_v^{(l)}$ 的其它 d_v-1 个独立同分布输入消息 $\{u_i\}$ 之和,所以其密度 $Q(v)$ 是先验密度 $P^{(0)}(u)$ 和 d_v-1 个相同密度 $R(u)$ 的卷积,即 $Q=P^{(0)}*(\otimes^{d_v-1}R)$.第 l 轮的密度 $Q(v)$ 就是该轮迭代结束后所有变量节点传递的 nd_v 个同分布消息的密度 $P^{(l)}$.应用傅立叶变换对,求得第 l 轮迭代结束后的消息密度为[4]

$$P^{(l)}=F^{-1}[F(P^{(0)})F(R^{(l)})^{d_v-1}] \tag{18}$$

4　密度估计的参数化

置信传播算法的收敛性反映于消息空间分布密度向正确消息集中.随着迭代次数的增加,每轮迭代后因子图中传播的不正确变量节点消息的比例应该逐渐趋于 0,使译码器高概率正确译码.许多信道模型可以用一个特征参数来描述,如 BSC 信道的错误转移概率 δ 和零均值 AWGN 信道的均方差 σ.先验密度是信道特征参数的函数,先验密度直接影响着密度进化.

给定一个 (n,d_v,d_c) 码,密度函数是信道特征参数的单调增函数[4],存在一个极值 α^*,当信道特征参数 $\alpha\le\alpha^*$ 时,算法高概率收敛.极值 α^* 就定义为置信传播算法的容量.

给定信道特征参数 α,译码器容量也是编码参数的函数.文[3]给出了几种正则 LDPC 码在 BSC 信道下消息空间为 $GF(2)$ 时的译码器容量.

上述消息密度的分析基于无循环路径的树图,但是当码长足够大时,译码器统计平均性能一致收敛于译码器容量.一方面,若信道参数 $\alpha\le\alpha^*$,给定足够大的码长,当迭代次数趋于无穷次时,任意 (n,d_v,d_c) 码均可以实现信息的可靠传输.另一方面,设定预期译码错误概率,经过相应的迭代次数后,

当码长 n 较大时,任意 (n, d_v, d_c) 码的性能按码长 n 指数地依概率 1 界定在该译码错误概率内[4,6].

给定设计码率 R_C,使信道容量 $C = R_C$ 的信道特征参数上限 α_C 就是该码率下的 Shannon 限. 译码器容量 α^* 与信道特征参数具有同样的量纲,它与上限 α_C 之间的差异能够表征设计的码性能与 Shannon 限之间的距离.

设 $N_0 = 2\sigma_C^2$ 为零均值 AWGN 信道的单边噪声功率谱密度,调制幅度为 $x_0 = \pm 1$,则比特信噪比的 Shannon 限为 $E_b/N_0 = x_0^2/2R_C\sigma_C^2$. 译码器容量 σ^* 与极限参数 σ_C 之间的距离定义为 $\Delta_S \equiv 20\log_{10}(\sigma_C/\sigma^*)$ dB. 表 1 给出了几种正则 LDPC 码的置信传播译码器容量及其与 Shannon 限的距离[3,4].

上述密度进化分析基于绝对连续条件. 实施计算时,需要对消息及其密度同时进行量化处理,并应用 FFT 技术. 表 1 的结果是基于均匀量化得到的,性能不是最佳. 若对消息空间采用基于消息密度的合理非均匀量化方案,能够改进译码性能,使译码器容量进一步接近 Shannon 限.

表 1 AWGN 信道下译码器容量及其与 Shannon 限的距离

d_v	d_c	R_C	σ^*	σ_C	E_b/N_0(dB)	Δ_S(dB)
3	6	0.5	0.88	0.979	0.184	0.926
4	8	0.5	0.83	0.979	0.184	1.434
5	10	0.5	0.79	0.979	0.184	1.863
3	5	0.4	1.00	1.148	-0.230	1.199
4	6	0.333	1.01	1.295	-0.484	2.159
3	4	0.25	1.26	1.549	-0.790	1.794

5 结论

本文在对数似然比消息空间上,基于树和有限状态机对低密度校验码置信传播译码过程进行了系统的分析,推导了迭代译码中的消息密度进化,讨论了置信传播算法性能的参数化估计. 应用这种方法可对译码算法收敛性作出独立于信道的系统分析,使码性能的估计不只局限于计算机仿真. 对于设计和评价 LDPC 码及其量化译码方案,使 LDPC 码在保证较高编码增益时可以实现快速译码,获得在实时通信系统中的应用,这是一个非常有用的理论和实用工具. 它可以直接用于非正则 LDPC 的分析[6],还可以推广至 Turbo 迭代译码算法的分析. 目前,密度进化理论及其高斯逼近已经成功地应用于容量逼近的低密度编码设计以及 Turbo 码分析中. 但是,如何将密度进化分析应用于非均匀量化译码方案设计以及衰落信道等多特征参数信道下的算法性能分析,还有待于进一步研究.

参考文献:

[1] Kschischang F R, Frey B J, Loeliger H A. Factor graphs and the sum-product algorithm [J]. IEEE Trans IT, 2001, 47(2): 498 - 519.

[2] Heerard C, Wicker S B. Turbo Coding [M]. Now York: L Kluwer Academic Publishers, 1999.

[3] Gallager R G. Low density parity check codes [J]. IRE Trans IT, 1962, 8(1): 21 - 28.

[4] Richardson T, Urbanke R. The capacity of low-density parity check codes under message-passing decoding [J]. IEEE Tyan IT, 2001, 47(2): 599 - 618.

[5] Mackay D. Good error-correcting codes based on very sparse matrices [J]. IEEE Trans IT, 1999, 45(2): 399 - 431.

[6] Luby M G, Mitzenmacher M, Shokrollahi M A, Spielman D A. Improved low-density parity-check codes using irregular graphs and belief propagation [A]. ISIT'98 [C]. Cambridge: MA, 1998.

作者简介:

贺玉成 男,1964 年 12 月出生于山西太原,1989 年毕业于西安电子科技大学,获通信与电子系统工学硕士学位,现为该校博士研究生,曾经从事跳频移动通信、保密语音通信、差错控制编码以及格码的研究,从事计算机网络工程及系统软件的开发研制工作,曾获得部级科技进步奖,1999～2000 年在日本静冈大学进行学习和研究,目前的研究方向是 LDPC 码、Turbo 码及编码调制技术.

杨 莉 分别于 1988 年和 1991 年在西安电子科技大学获工学学士和工学硕士学位,留校任教至今,曾经从事研究密码学,目前主要研究计算机接口技术、Turbo 码及编码调制技术.