几种 LDPC 码的最小汉明距离的计算

林灯生,李少谦
(电子科技大学通信抗干扰技术国防重点实验室,四川成都 610054)

摘 要: 本文提出一种计算 LDPC 码的真实最小汉明距离的方法.该方法能够用来计算多种 LDPC 码方案的真实最小汉明距离,比如准循环 LDPC 码、pi-旋转 LDPC 码等.该方法是通过计算码的环长间接地找到 LDPC 码最小距离,由于计算环长的计算量要远比直接计算最小汉明距离来得低,因而该算法能够在有限时间内找到 LDPC 码的真实最小距离.通过仿真表明,用目前主流的个人计算机利用该方法找出一个有最小距离 24 的码率为 1/4 的准循环 LDPC 码最小距离大概需要花 77 分钟.

关键词: 低密度奇偶校验 (LDPC) 码; 环长; 最小汉明距离
中图分类号: TN911.22 **文献标识码:** A **文章编号:** 0372-2112 (2007) 6A-069-05

Computing the Minimum Distance of Several Kinds of LDPC Codes

LIN Deng-sheng, LI Shao-qian
(*National key Lab of Communication, University of Electronic Science and Technology of China, Chengdu, Sichuan* 610054, *China*)

Abstract: In this paper, we present a measurement method of the real minimum Hamming distance of several kinds of LDPC codes, including quasi-cyclic LDPC codes, pi-rotation LDPC codes, etc. The minimum distance is indirectly obtained by computing the cycles of the LDPC code. Since the complexity of computing the cycles is much lower than that of direct computing the minimum distance, the method is efficient to compute the minimum distance of the LDPC code. From one of simulation results, it shows that it takes about 77 minutes to compute a minimum distance of 24 for a rate 1/4 quasi-cyclic LDPC code using a common personal computer.

Key words: Low-density parity-check(LDPC)codes; cycle; minimum distance

1 引言

LDPC 码被重发现[1]至今,已有十年左右时间了,而研究其码的性能则引起越来越多的研究者的关注,目前许多研究者也开始对中短码的性能研究产生兴趣[2,3].本文研究的重点是计算中短码的最小汉明距离.然而分析真实的最小汉明距离是非常困难的.文献[3]给出了些短的 LDPC 码最小汉明距离特性.错误脉冲法[4]最早由 C.Berrou 提出,用来计算 turbo 码的自由距离,文献[5]对它做了些改进以适合于 LDPC 码场合.错误脉冲法是一种简单且有效的计算最小汉明距离的方法,但它有一个最大的缺点是不能保证找到的最小距离一定是真实的最小距离.文献[6]给出一种非常好的能够找出 turbo 码真实自由距离的方法.

本文提出一种寻找某些 LDPC 码的真实最小距离的方法.该方法要求这些 LDPC 码校验矩阵能够按行分成两个子矩阵,且其中有一个子矩阵的列重固定为 2,然后先通过计算列重为 2 的子矩阵的环长来找出所有重量小于或等于该码的最小距离上限的码字,再验证该码字是否也是该 LDPC 码的一个全局码字,直到找到所有最小重量的码字.

2 环长和序列重量关系

对于奇偶校验矩阵的列重只有 2 的 LDPC 码,环长和汉明距离之间有如下关系:

定理 1 c 是一个校验矩阵列重为 2 的 LDPC 码的一个码字的充要条件是在该码的校验矩阵中,以 c 中所有的"1"为变量节点一定能组成一个或多个环.这里,多环是指校验矩阵中存在多个互相不相连的单环.这里互相不相连是指每一个变量节点或校验节点最多处在一个单环内.

证明 见附录.

由定理 1,可以导出如下推论:

推论 1 如果一个校验矩阵 $\boldsymbol{H}$ 中仅有一个列列重

收稿日期:2006-06-11;修回日期:2007-10-16
基金项目:国家自然科学基金(No.60496313);企业项目:Intel Research Project on the Key Techniques for TDD MIMO OFDM Systems

为 1,其他所有列列重都为 2,那么该 LDPC 码的所有码字中,列重为 1 的列对应的比特一定为 0.

证明 (反证法).假设 H 中列重为 1 的列对应的比特为"1"时是该码的一个码字 c,则与该变量节点处在同一个奇偶校验行的其他的 c 中"1"比特对应的变量节点必然有奇数个,这样在除去列重为 1 列之后剩余的奇偶校验矩阵中一定不能形成环能够包含这所有节点(奇数个节点),根据定理 1,因此在这剩余的奇偶校验矩阵中不能存在任何码字,包括全零码字,所以列重为 1 的比特只能为"0".

利用定理 1,我们很容易通过找出奇偶校验矩阵列重为 2 的 *LDPC* 码最小环长来确定最小汉明距.而对于一般列重大于 2 的 *LDPC* 码则没有该性质,可是对于某些 *LDPC* 码,我们可以将这些码的校验矩阵按行分成两个子矩阵,其中一个是列重为 2 的子矩阵 H_1,另一个是剩下的子矩阵 H_2.这样通过计算 H_1 矩阵环,就可以确定 H_1 中的码字,如果它同时也是 H_2 的码字,则该码字就是全局的码字,即 H 的码字.这样只要找到同时是 H_1 和 H_2 的码字中最小重量的码字,那么就找到该码的最小重量.为了方便下面的讨论,我们把 H_1 称为基本矩阵,H_2 称为辅助矩阵.

3 环长的测量及优化

下面介绍一种简单的判断环的方法.该方法可以用图 1 来描述:

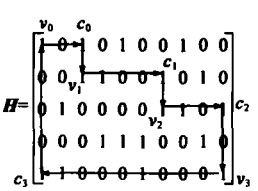


图 1 环的形成

假设我们要寻找有变量节点 v_0 参与的环.与 v_0 相连的校验节点有 $\rho-1$ 种可能,这里 ρ 为行重量,我们选择其中一个校验节点 c_0,由于列重只有 2,那么与 c_0 相连的变量节点只有一个,用 v_1 表示,那么与 v_1 相连的校验节点又有 $\rho-1$ 种可能性,假设我们选择的是 c_1,与 c_1 相连的唯一的变量节点为 v_2,依此类推.最后要使得这些节点形成环,则最后一个校验节点 c_j 一定要与第一变量节点 v_0 相连.使用该方法搜索出所有的环长为 g 的环的搜索空间为

$$2n(\rho-1)^{g/2} \tag{1}$$

这里 n 为码长,由于上述方法搜索过程中每一个环都被重复地搜索了 g 遍,如果去掉这种重复搜索,则搜索空间就下降到 $2n(\rho-1)^{g/2}/g$.

该算法计算量与半环长成指数增长.因而当 ρ 比较大时,所需的搜索空间比较大.下面介绍一种方法能够有效地降低计算环长的计算量.这种方法只要计算一半的环长,然后将两个半环组成一个环.比如,如图 1 所示,我们先找 v_0 点到 v_2 点的一条路径 $v_0\rightarrow c_0\rightarrow v_1\rightarrow c_1\rightarrow v_2$,然后再找一条从 v_0 点到 v_2 点的路径 $v_0\rightarrow c_3\rightarrow v_3\rightarrow c_2\rightarrow v_2$,如果这两条路径不重合,那么它们一定能形成一个环.计算任意两个节点之间半环长为 $g/2$ 的半环的搜索空间为

$$4n^2(\rho-1)^{g/4} \tag{2}$$

同样,找一个长为 l 的半环,也可以将两个长为 $l/2$ 的半环通过首尾相连而成.这样,我们可以通过递归的方法,由短的半环递归地寻找长的半环,最后再找出所有整环.

另外,对于某些特殊的 H 矩阵的环还具有如下一个性质:

定理 2 对于具有列重为 2 的校验矩阵的 LDPC 码,如果可以将这个校验矩阵按行分成两个列重都为 1 的子矩阵,则原来校验矩阵 H 的环长一定能被 4 整除,也就是说,该码一定没有奇重量的码字.

证明 由于只有两层,所以校验节点到变量节点只能从第一层到第二层或第二层到第一层.如果用校验节点 -> 变量节点 -> 校验节点 -> 变量节点,那么节点所在层可这样表示(假设从第一层开始):1 -> 1 -> 2 -> 2 -> 1 -> 1 -> … -> 2 -> 2,最后一个节点一定跟第一个节点处在不同的层.而为了满足这个要求,环长必需是 4 的整数倍.

4 几种 LDPC 码的最小距离测量

根据第二章的论述,为了能够使用上述方法,要求 LDPC 码的校验阵必须是能够按行分成两个子矩阵,并且其中有个子矩阵的列重为 2.而某些实用的 LDPC 码往往带有这种性质,比如某些准循环 LDPC 码,π-旋转 LDPC 码等,它们的校验矩阵都可以分解成我们需要的形式,而且这些码都属于易编码的 LDPC 码,因此研究它们的最小距离具有很强的应用价值.下面就介绍用上述方法计算最小汉明距离的具体过程.

第一步,将该码的校验矩阵上下分成两个子矩阵,其中一个矩阵 H_1 列重为 2,作为基本矩阵,另外一个作为辅助矩阵 H_2;

第二步,采用前述半环的方法找出任意两节点长度为 $g/2$ 的半环并存储所有的半环.g 的初始值取 H_1 最小环长;

第三步,检验单环情况.将 $g/2$ 长的半环拼成整环并存储,并检验该环对应的码字是否也是 H_2 的一个码字,如果是,则最小汉明重量就是当前环长的一半,即 $g/2$,记录下最小码字的个数;

第四步,检验多环情况.找出所有能使总环长为 g 的多环,并检验多环对应的码字是否也是 H_2 的一个码字,如果是,也记下最小码字数;

第五步，如果找到了最小码字，则停止，否则将环长从 g 增加到 $g+2$，回到第二步.

环的数目是跟环长成指数增大的，因而当环长很长时，存储这些环需要大量的存储空间，为了节省存储空间，根据我们的经验，如果要计算的码最小汉明是 d_m，那么只要存储环长小于 d_m 的环和半环长小于 $d_m/2$ 的半环就可以了.这是因为：当计算环长大于 d_m 并小于 $2d_m$ 的单环的时候，可以用前面已经存储的半环作为四分之一环来组成半环，进而再组成整环，那么前面存储的最长的半环为 $d_m/2$，就可以组成最长为 d_m 的半环，和 $2d_m$ 的整环.而检验多环情况时候，要组成最长总长为 $2d_m$ 的多环，则如果其中一个环长大于 d_m，则其他环的总环长就一定小于 d_m，这个大于 d_m 的单环可以由半环实时地计算得到，而小于 d_m 的环可以直接到存储区中取得，因而没必要存储长度大于 d_m 的环.

下面就具体介绍我们的方法分别在准循环 LDPC 码和 π-旋转 LDPC 码中的应用.

4.1 准循环 LDPC 码

准循环 LDPC 码最早由 Y.Kou 等提出[7].这类码的基本的特点是它们的奇偶校验阵由许多循环子矩阵构成的，因而具有准循环的特性，我们可以利用这个特点进一步地将计算最小距离的复杂度降低到原来的 ρ/n.另外，由于准循环 LDPC 码能够找到定理 2 需要的 $\boldsymbol{H}_1$，因而还可以利用定理 2 来进一步降低计算量.

作为例子，我们采用文献[8]中介绍的第一类构造法，选用参数如下：$t=9$，$m=109$，这样可构造出奇偶校验矩阵为 $109\times(9\times109)$ 的准循环 LDPC 码，选取其中的 4 个循环矩阵，再利用行列分解方法进行列分解[7]，分解后使每个循环子矩阵都是循环置换矩阵，然后再选取其中的三层置换阵，这样就得到了一个列重为 3，行重为 4，码长为 436 和码率约为 1/4 的准循环 LDPC 码，它们的奇偶校验矩阵如下：

$$\boldsymbol{H}=\begin{bmatrix} \boldsymbol{I}(0) & \boldsymbol{I}(0) & \boldsymbol{I}(0) & \boldsymbol{I}(0) \\ \boldsymbol{I}(1) & \boldsymbol{I}(12) & \boldsymbol{I}(35) & \boldsymbol{I}(93) \\ \boldsymbol{I}(45) & \boldsymbol{I}(104) & \boldsymbol{I}(49) & \boldsymbol{I}(43) \end{bmatrix} \tag{3}$$

这里，$\boldsymbol{I}(i)$，当 $i=0$ 时，表示单位矩阵，当 $i\neq0$ 时，表示将单位阵中每一个行向量都向右循环移 i 位后得到的循环置换矩阵.同样方法，我们又得到一个列重为 3，行重为 8，码长为 776 和码率约为 5/8 的准循环 LDPC 码，它们的奇偶校验矩阵如下：

$$\boldsymbol{H}=\begin{bmatrix} \boldsymbol{I}(0) & \boldsymbol{I}(0) & \boldsymbol{I}(0) & \boldsymbol{I}(0) & \boldsymbol{I}(0) & \boldsymbol{I}(0) & \boldsymbol{I}(0) & \boldsymbol{I}(0) \\ \boldsymbol{I}(1) & \boldsymbol{I}(25) & \boldsymbol{I}(43) & \boldsymbol{I}(8) & \boldsymbol{I}(6) & \boldsymbol{I}(53) & \boldsymbol{I}(64) & \boldsymbol{I}(48) \\ \boldsymbol{I}(35) & \boldsymbol{I}(2) & \boldsymbol{I}(50) & \boldsymbol{I}(86) & \boldsymbol{I}(16) & \boldsymbol{I}(12) & \boldsymbol{I}(9) & \boldsymbol{I}(31) \end{bmatrix} \tag{4}$$

下面就应用我们的方法找出这两个码的真实最小距离，具体结果已列在表 1 中.

表 1　两个准循环 *LDPC* 码的最小距离、对应的码字数以及计算时间

码率 R	1/4	5/8
码长 n	436	776
最小距离 dm	24	12
最小码字个数 Am	545	194
计算时间(分钟)*	77	2

* CPU 使用奔腾四处理器，主频为 2GHz

4.2 π-旋转 LDPC 码

π-旋转 LDPC 码[9]是一种简单且易于硬件实现的 LDPC 码，该码的奇偶校验矩阵有一个非常简洁的形式，如下式所示：

$$\boldsymbol{H}=[\boldsymbol{H}^p\,|\,\boldsymbol{H}^d]=\begin{bmatrix} 1 & 0 & 0 & L & 0 & \pi_A & \pi_B & \pi_C & \pi_D \\ 1 & 1 & 0 & L & 0 & \pi_B & \pi_C & \pi_D & \pi_A \\ M & & & & M & \pi_C & \pi_D & \pi_A & \pi_B \\ 0 & 0 & 0 & L & 1 & \pi_D & \pi_A & \pi_B & \pi_C \end{bmatrix}$$

其中 $\boldsymbol{H}^p$ 是一个双对角方阵，$\boldsymbol{H}^d$ 是一个列重和行重都为 4 的稀疏矩阵，其中 π_A 是一个随机生成的 $L\times L$ 的置换矩阵，π_B 是 π_A 方阵旋转 90 度而成的，π_C 是 π_B 沿与前面相同方向旋转 90 度得到的，而 π_D 是 π_C 旋转 90 度得到的.

将 $\boldsymbol{H}$ 按行分成两个等行长的子矩阵，去掉这两个子矩阵中列重为 0 的列，然后将上半矩阵作为基本矩阵 $\boldsymbol{H}_1$，下半矩阵作为辅助矩阵 $\boldsymbol{H}_2$，那么这两个子矩阵的右半矩阵列重都为 2，而 $\boldsymbol{H}_1$ 的左半矩阵除了最后一列的列重为 1 外，其他列列重都是 2.

根据推论 1，$\boldsymbol{H}_1$ 的所有码字中最后一列对应的比特一定都为 0，所以计算环时候，可以忽略掉这个比特.文献[9]对 π-旋转 LDPC 码做了进一步的优化，得到些性能优异的 LDPC 码，下面将应用我们的方法找出该文中几个优化的 π-旋转 LDPC 码的真实最小距离，具体结果见表 2.

表 2　几种码率为 1/2 的 π-旋转 LDPC 码的最小距离、对应的码字数以及计算时间

码长 n	1008	504	248
最小距离 d_m	18	14	12
最小码字个数 A_m	16	16	64
信息位数 w	2	2	2/40,4/24*
计算时间(分钟)	1324	3	1

* x/y 中，x 是最小距离码字中信息位的个数，y 是信息位数为 x 的最小码字个数.

5 数字结果

如果知道了一个码的最小距离，那么应用联合界

就能计算出近似的误码率或误帧率的下界.由联合界计算近似误码率和误帧率公式如下[6]:

$$\mathrm{FER}\approx\frac{1}{2}A_m\mathrm{erfc}\left(\sqrt{d_mR\frac{E_b}{N_0}}\right) \tag{6}$$

和

$$\mathrm{BER}\approx\frac{1}{2}\frac{w}{k}A_m\mathrm{erfc}\left(\sqrt{d_mR\frac{E_b}{N_0}}\right) \tag{7}$$

针对上一章中给出的几种码,根据上式,我们计算出了它们的近似误码率或误帧率,根据码的分类分别被列在图 2 和图 3 中,为了与仿真性能比较,相应地在图中也给出了这些码的误码率或误帧率的仿真结果.从结果可以看出,随着信噪比的增加,仿真结果不断地逼近联合界算出的 BER 或 FER.

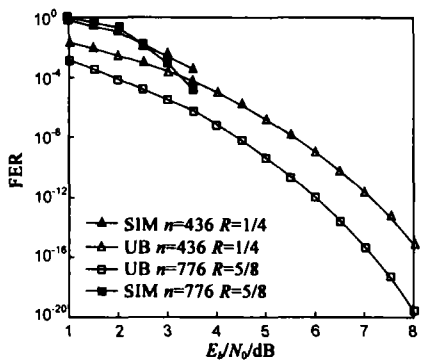


图 2 准循环 LDPC 码的 FER 性能和近似联合界.其中,SIM 代表通过仿真得到的曲线,UB 代表通过近似联合界得到的曲线

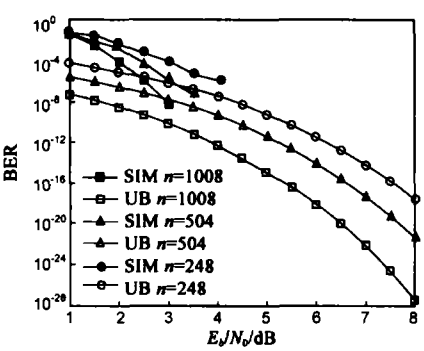


图 3 π-旋转 LDPC 码 BER 性能和近似联合界

6 结论

本文提出一种利用计算环长来找某些 LDPC 码的真实最小距离的方法.该方法要求这些 LDPC 码校验矩阵能够按行分成两层,并且其中有一层的列重固定为 2(少数列重为 1 亦可),而许多实用的 LDPC 码方案都具有该特点,比如某些准循环 LDPC 码,π-旋转 LDPC 码等.该方法通过计算列重为 2 的子矩阵的环长来找出所有重量小于或等于该码的最小距离上限的码字,然后再验证该码字是否也是该 LDPC 码的一个码字.由于计算一个非常稀疏的校验矩阵中的某一环长的环所搜索的空间远比直接计算一个码字所搜索的空间来得小,因而该方法能够在可接受的时间内找到相当大的最小距离来.本文还给出了许多实际的例子,在这些例子中,我们找到的最大的最小距离是 24.最后算出了这些码的近似联合界并给出这些码的误码率和误帧率仿真结果,结果说明联合界能够很好地反映了一个码的错误平层性能.

附录

定理 1 的证明

充分性 要使 $\boldsymbol{c}$ 是一个码字,$\boldsymbol{c}$ 需满足 $\boldsymbol{c}\times\boldsymbol{H}\bmod 2=\boldsymbol{0}$,$\boldsymbol{H}$ 为奇偶校验矩阵.如图 4 所示,由于环中所有参与奇偶校验的变量节点个数都为偶数,说明环中所有的变量节点做奇偶校验结果都为 0.又由于 $\boldsymbol{H}$ 的列重只有 2,而 $\boldsymbol{c}$ 中"1"比特在 $\boldsymbol{H}$ 中对应的每个节点都处在环当中,所以 $\boldsymbol{c}$ 中"1"比特对应所有节点奇偶校验结果都为 0,即 $\boldsymbol{c}\times\boldsymbol{H}\bmod 2=\boldsymbol{0}$,所以 $\boldsymbol{c}$ 一定是一个码字.

必要性 很显然,码字 $\boldsymbol{c}$ 中"1"比特在 $\boldsymbol{H}$ 中的所有变量节点参与某一个奇偶校验的变量节点个数一定都是偶数个.如果 $\boldsymbol{c}$ 的重量为 w,由于 $\boldsymbol{H}$ 的列重为 2,所以总共就有 $2w$ 个变量节点参与奇偶校验.将这 $2w$ 个变量节点对每个行按照行顺序分成 w 个段,每一段由 2 个变量节点组成.随机地取其中一个节点作为起始的变量节点,如图 4 中的 a 节点,然后沿行方向选该节点所处的段中另一点作为下一个节点,而该节点在列方向有唯一的一个变量节点与之相连($\boldsymbol{H}$ 的列重为 2),而这个新的变量节点在行方向又有唯一的一个节点与之相连(即与该变量节点处在一个段内的另一个节点),这样经过一些节点最后一个节点一定是起点的变量节点 a 列相连,从而形成一个环.这是因为这样形成的路线显然一定不会重合,而如果不会回到原点的话,这条路线只能到某一节点终止,但这是不可能的,因为对于每一个节点都一定有一个且唯一一个与之相连,因此必然最终要回到原点,形成一个环路.如果这个环没有包括了所有的码字中"1"对应的节点,如图 4(b)所示,则再从这些剩余的节点中任选一个(图中 b 点)当作起始点,与上一个环一样,他们必然会形成另一个环,而且他们不会与前一个环重叠.如此下去则码字 c 中所有"1"比特对应的节点都最终会处在某一个环中.

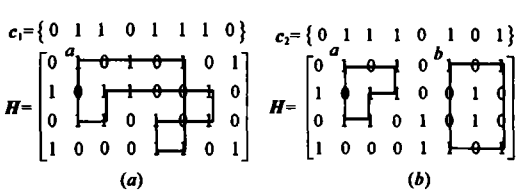


图 4 奇偶校验矩阵列重为 2 的 LDPC 码的环长与码字的关系

参考文献:

[1] D J C MacKay, R M Neal. Near Shannon limit performance of

low density parity check codes[J]. IEE Electron Lett, 1996, 32 (18): 1645 - 1646, .

[2] C Y Di, D Proietti, I E Telatar, T J Richardson, R L Urbanke. Finite-length analysis of low-density parity-check codes on the binary erasure channel[J]. IEEE Trans Inform Theory, June 2002 48(6): 1570 - 1579.

[3] L Wei. Several properties of short LDPC codes[J]. IEEE Trans. Commun, May 2004, 52(5): 721 - 727.

[4] C Berrou, S Vaton, M Jezequel, C Douillard. Computing the minimum distance of linear codes by the error impulse method [A]. Proc IEEE Global Telecommunications Conference[C]. Taipei, Taiwan: IEEE Press. 2002, 2: 1017 - 1020.

[5] X Y Hu, M P C Fossorier, E. Eleftheriou. On the computation of the minimum distance of low-density parity-check codes [A]. Proc 2004 IEEE Int Conf Communications[C]. Paris, France: IEEE Press, 2004, 2: 767 - 771.

[6] R Garello, P Pierleoni, S Benedetto. Computing the free distance of turbo codes and serially concatenated codes with Interleavers: algorithms and applications[J]. IEEE J Select Areas Commun., May 2001, 19(5): 800 - 812.

[7] Y Kou, S Lin, M Fossorier. Low-density parity-check codes based on finite geometries a rediscovery and new results[J]. IEEE Trans Inform. Theory, Nov. 2001, 47(7): 2711 - 2736.

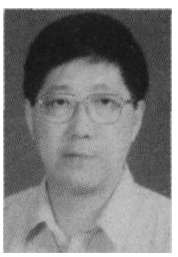
[8] B Ammar, B Honary, Y Kou, J Xu, S Lin. Construction of low-density parity-check codes based on balanced incomplete block designs[J]. IEEE Trans Inform Theory, June 2004, 50(6): 1257 - 1268.

[9] R Echard, S C Chang. Design considera-tions leading to the development of good π-rotation LDPC codes[J]. IEEE Commun Lett, May, 2005, 9(5): 447 - 449.

作者简介：

林灯生　男，1974 年 8 月生于福建省连江县. 1998 年获电子科技大学电子工程专业学士学位. 2004 年获电子科技大学通信与信息系统专业工学硕士学位，目前在电子科技大学通信抗干扰技术国防重点实验室攻读博士学位. 主要研究方向为信道编码.

E-mail: linds@uestc.edu.cn



李少谦　男，四川成都人，教授、博士生导师，电子科技大学通信抗干扰技术国家级重点实验室主任，国家 863 计划通信主题专家组成员，主要研究方向为扩频通信、移动通信等.

E-mail: lsq@uestc.edu.cn