编码引论 第二次Project 个人报告

小组成员：马泽余 陈森睿 秦达飞

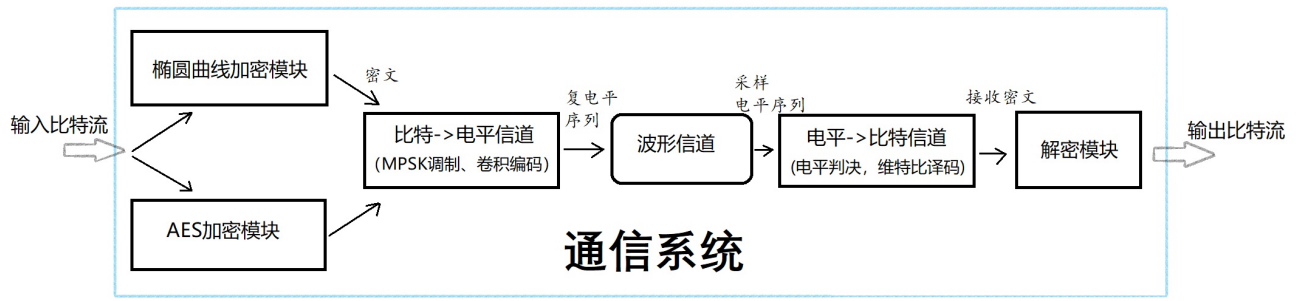
本部分撰写人：陈森睿

主要内容：信道编码参数设计、波形信道设计与仿真分析（含误码率曲线等）

整体概括

本次实验中，我们完成了一个带通AGWN信道中的完整通信系统，支持安全编码和各种参数的卷积编码。我们对此通信系统做了完善的理论与仿真分析。

系统框图如下：



我们的主要工作包括以下内容：

工作	说明	负责人
椭圆曲线非对称加密	参照secp256k1的标准，实现了256bit质数的高精度运算椭圆曲线加密，将信息映射到椭圆曲线的点上进行加密，可随机生成小于基点阶数的足够多秘钥。	马泽余
AES对称加密	基于AES标准实现了AES-128、AES-192、AES-256对称加密，并结合已有C代码进行了加速。	秦达飞
电平信道设计	基于第一次作业的电平信道进行修改，设计适合于波形信道的接口，负责完成电平调制解调、卷积码编译码等。	秦达飞
波形信道设计与仿真	设计AWGN波形信道，包括计算编码参数、编写信道函数、仿真获得信号波形、功率谱等。	陈森睿
系统联调	在无加密的情况下找到了最好的信道调制方式；给出了整体系统设计，完成了安全传输任务。	全员参与

本报告汇报我的工作，主要包括：信道编码参数设计、波形信道设计、无加密时的联调仿真等。

编码参数设计

任务

- $300 \sim 3400Hz$带通信道，AGWN噪声
- 线性传输，收发端采用滚降系数$\alpha = 0.5$根号升余弦滤波
- 待传数据大小1kB，要求5秒内完成传输
- 要求：设计编码参数（进制数、符号率、卷积码效率等）

分析

设定符号率R_s，调制比特数M。传输速率$R_b = MR_s$应满足

$$R_b = MR_s \geq 1600 \text{ bits/sec} \tag{1.1}$$

可利用的带宽$B = 3100Hz$，因此复基带成型滤波器对应的单边带宽应满足$B_s \leq 1550Hz$。而成型滤波器为根号升余弦，带宽$B_s = \frac{1+\alpha}{2}R_s$，因此

$$\frac{1+\alpha}{2}R_s \leq \frac{1}{2}B \tag{1.2}$$

得出$Rs \leq 2066Hz$，据此可以设计(M, R_s)如下。我们的设计思路是：尽可能用尽5秒，以换取频带资源的节省。增大M可减小带宽占用，但可能增大误码率。

方案编号	M (bits/symbol)	R_s (Hz)	传输速率R_b(bit/sec)	占用频段 (Hz)
(1)	1	1665.0	1665	[1017.5, 2682.5]
(2)	2	832.5	1665	[1433.8, 2266.3]
(3)	3	555.0	1665	[1572.5, 2127.5]

有卷积编码的情况： 卷积编码可以降低通信过程的误码率。设卷积编码效率为R_c，则(1.1)改为

$$R_b = R_c R_s M \geq 1600 \text{ bits} \tag{1.1}$$

其他要求不变。设计如下：

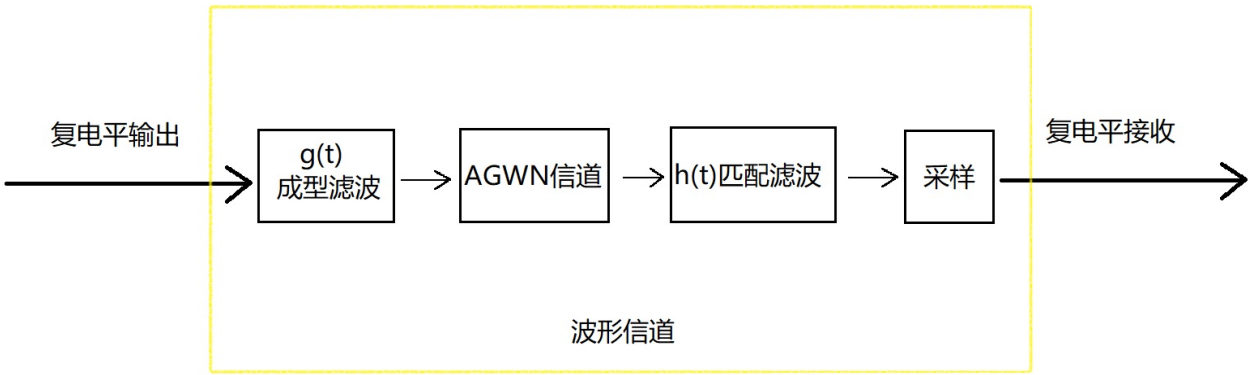
方案编号	M (bits/symbol)	R_s (Hz)	R_c	传输速率(bit/sec)	占用频段 (Hz)
(4)	2	1665.0	1/2	1665	[1433.8, 2266.3]
(5)	3	1665.0	1/3	1665	[1572.5, 2127.5]

波形信道

本部分讨论波形信道部份的设计、并仿真给出信号波形、功率谱、误码性能等

架构

波形信道的整体架构如下图



单独划分出波形信道，使得系统更加模块化，带来若干好处：一方面，上一次作业完成的电平信道可以很容易地与之联接（只需调整好输出电平大小）；另一方面，卷积码、安全编码模块与信道解耦，便于独立设计。

实现

0.全局参数

我选取采样率$f_{real} = 33300Hz$来刻画波形。程序中，方便起见，将采样率归一化。

以 [$M = 1$，$R_s = 1665Hz$，无卷积] 的参数为例：程序中`Rs=1/20`，载波中心频率`fc=1/18`。

电平信道提供模值为1的复电平符号序列，并负责解调、译码采样得到的复电平序列。因此这两步不在此处讨论。

注：仿真中绝大多数操作在等效复基带进行。

1.成型滤波

为获得根号升余弦滤波器，先根据R_s得到根升的频谱，再用傅里叶逆变换回到时域。

```
Gc = 1.*(abs(f)<=Rs/4) + 0.5*(1+sin(2*pi/Rs*abs(f))).*(abs(f)>Rs/4 & abs(f)<=3*Rs/4); %升余弦频谱
Gs = sqrt(Gc);%根升
g = (IFT*Gs)';%逆变换到时域
```

其中`IFT`矩阵由`prefourier`函数获得。注意`prefourier`中的时域采样率必须为1（即`g`对应采样率为1）。

注：时频变换最好用`fft`，可以避免采样率的麻烦，效率也更高。

利用`g`进行成型滤波。设电平信道给出复电平序列`a`，则成型滤波后的复基带信号为

$$S_B(t)=\sum_n a_n g(t-nT_s)$$

其中$T_s=\dfrac{1}{R_s}$，代码如下

```
s_num = length(a);
wlen = (s_num-1)*Ts*fs+len;%Sb数组长度
for k = 1:s_num
    Sb = Sb + [zeros(1,(k-1)*Ts),a(k)*g,zeros(1,wlen-(k-1)*Ts-len)]; %逐符号成型滤波
end
t = [1:wlen]; %对应时间
```

2.AGWN信道

AGWN信道部份的关键在于正确表达E_b/n_0。以下讨论假设E_b，n_0已分别给定。

对于有卷积码的情况，设卷积编码效率 R_c，记编码比特能量$E_{b,c}$，则

$$\frac{E_{b,c}}{n_0}=\frac{1}{R_c}\frac{E_b}{n_0}$$

因此，在波形信道部份，只需将给定的E_b/n_0换算成$E_{b,c}/n_0$，就可等效为无信道编码的情况。接下来只讨论无卷积码的情况。

信号能量部分：

成型滤波后E_{b_0}的表达式如下

$$E_{b_0}=\frac{1}{M}\mathbb{E}\left(|a_n|^2\right)\int|g(t)|^2dt$$

电平映射均采用MPSK且幅度设置为1，理论计算给出$\int|g(t)|^2dt=R_s$，因此$E_{b_0}=\dfrac{R_s}{M}$。现在需要将其提升到给定的E_b值，只需对`sb`乘一个系数$\sqrt{2ME_b/R_s}$，如下

```
Sb = sqrt(M*2*Eb/Rs)*Sb; %修正后的Eb/n0是我们需要的值
```

注意：由于在复基带，比特能量是$2E_b$

噪声功率部分：

噪声功率无穷大，但在以采样率f_s仿真时，相当于提前做了一个$\frac{fs}{2}$低通滤波，最终加在采样点上的噪声功率为$\frac{n_0 f_s}{2}$。复基带上则是实、虚部各加功率为$n_0 f_s$的噪声。

```
I = real(Sb);
Q = imag(Sb);
S = I.*cos(2*pi*fc*t)-Q.*sin(2*pi*fc*t);%上变频，发送信号实带通波形
Qn = Q + randn(1,length(t))*n1;
In = I + randn(1,length(t))*n1;
Sn = In.*cos(2*pi*fc*t)-Qn.*sin(2*pi*fc*t);%加噪信号实带通波形
Sbn = In + j*Qn; %加噪信号复基带波形
```

3.匹配滤波与采样

```
normFactor = 1/sqrt(M*2*Eb*Ecur); %电平信道匹配因子
h = normFactor * g; %匹配滤波器
R = conv(Sbn,h,'same'); %滤波
sampTime = ([0:s_num-1]*Ts) + 10*Ts + 1;
a_re = R(sampTime); %采样
```

这里着重讨论`normFactor`：这个因子的作用是，确保最终得到的电平模值期望为1，以便后续的电平信道正常完成译码。计算方式如下：无`normFactor`时，采样值的模值期望为

$$\begin{aligned} E_a =& A_0 (g*h)(t)_{|t=0} \\ =& A_0 (g*g)(t)_{|t=0} \\ =& A_0 \int (g(t))^2 dt \\ =& A_0 R_s \end{aligned}$$

其中$A_0 = \sqrt{2ME_b/R_s}$是成型滤波时乘在`g`上的系数，综上有

$$E_a = \sqrt{2ME_bR_s}$$

将`normFactor`取为其倒数，即可把采样模值归一化为1。

仿真

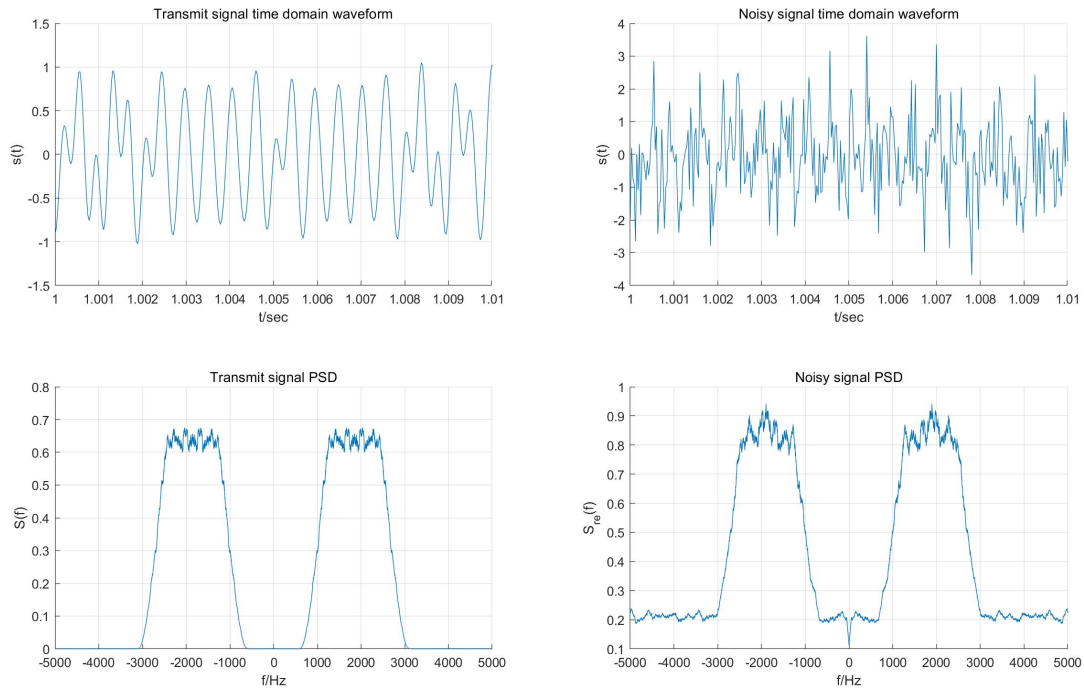
本部分对于前述传输任务，给出波形信道上的仿真结果。为了获得误比特率，仿真过程也用到了电平信道。

1.无卷积 传输过程仿真

待传输信息：8kB随机比特序列

参数选取： $M = 1\ \text{bit/symbol}$，$R_s = 1665Hz$，无卷积编码，$E_b/n_0 = 8dB$，取定$E_b = 1$

发射信号与加噪信号（时域波形与功率谱）：



注：均用真实频率展示。其中时域仅展示10ms的波形，功率谱加了一定长度的矩形滑动窗。

分析

- 从时域看，噪声功率远远大于信号功率，信号似乎完全被淹没；从功率谱看，有效频段内的信号功率明显高于噪声功率，应有办法区分。
- 功率谱大致呈现出升余弦状，与设计相符

关于功率谱取值的进一步讨论：

采用`fft`计算功率谱，代码如下

```
Fs = conv(abs(fft(S)/(length(S))).^2,ones(1,500)/500,'same');
Fs = fftshift(Fs);
ff = ([-length(Fs)/2:length(Fs)/2-1]/length(Fs));
plot(ff*f_real,Fs*f_real); %绘图时，归一化频率转成实际频率
```

我们可以理论验证功率谱取值的正确性：

$$\int \mathbb{S}(f)df = P = E_s R_s = ME_b R_s$$

此仿真条件下，右式理论值为0.05。实际对功率谱积分（求和）得到几乎完全相同的结果：

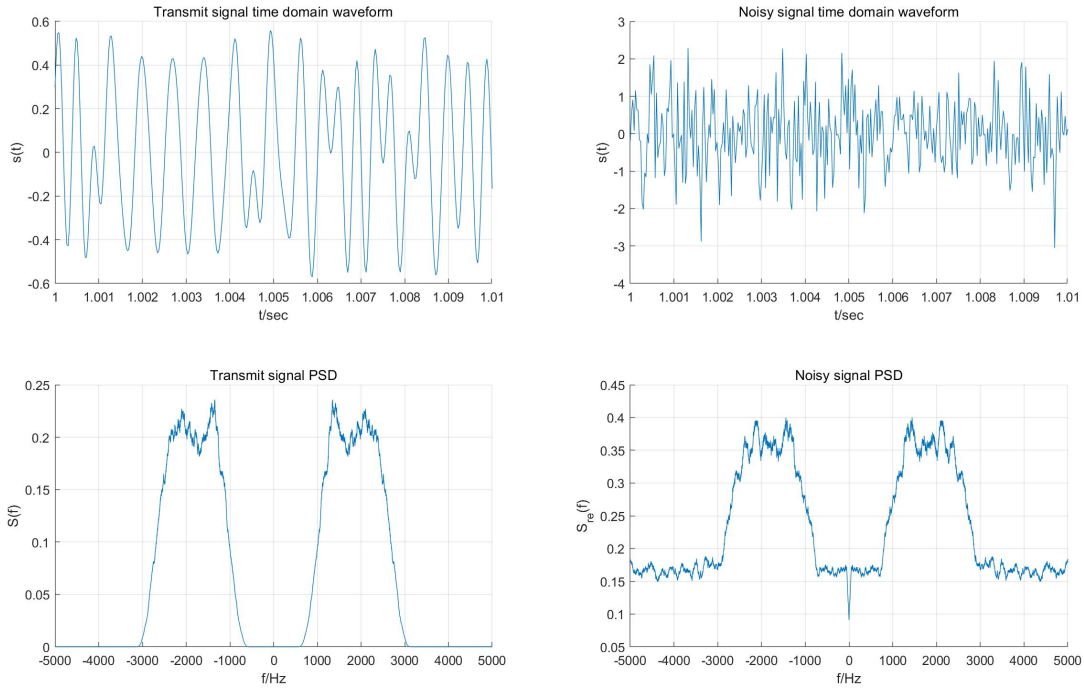
```
>> sum(Fs)
ans =
    0.0499
```

2.有卷积 传输过程仿真

待传输信息：8kB随机比特序列

参数选取： $M=2\ \mathrm{bit/symbol}$，$R_s=1665Hz$，卷积编码效率$R_c=1/2$，硬判决，$E_b/n_0=8dB$，取定$E_b=1$

发射信号与加噪信号（时域波形与功率谱）：

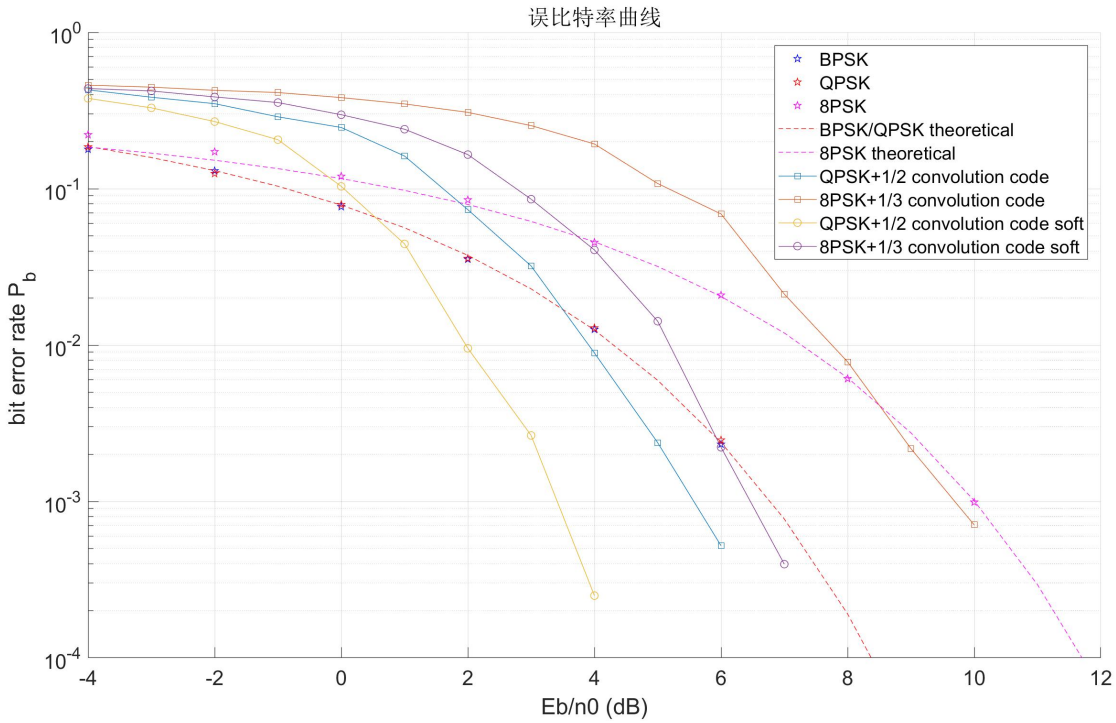


可见与无卷积码的情况没有什么不同。

3.误比特率曲线仿真

五种方案误比特率：

五角星代表的是无卷积码的方案(1)(2)(3)，调制效率M=1,2,3分别对应BPSK, QPSK和8PSK；正方形代表的是有卷积码的两种方案(4)(5)；圆形代表卷积码采用软判决。



注：BPSK/QPSK误比特率理论值为$Q\left(\sqrt{\frac{2E_b}{n_0}}\right)$*；8PSK误比特率理论值为*$\frac{2}{3}Q\left(\sqrt{\frac{E_b}{n_0}}3\left(1-\frac{\sqrt{2}}{2}\right)\right)$*，均为高信噪比近似。*

分析：

- 首先注意到：MPSK的仿真值与理论值吻合度较高，这验证了传输系统的正确性。
- 无卷积码时，BPSK和QPSK误码性能一致（因为BPSK只用了一路信号，浪费了另一路的功率），8PSK则造成更高的误码率；
- 加上卷积编码后，低E_b/n_0时误比特率反而更高（越纠越错），高信噪比时误码率快速下降。$E_b/n_0 \geq 0.5dB$后，QPSK+1/2效率卷积已经是最优方案。
    - 和其他信道编码类似，卷积码带来了一定的编码增益。尽管这个值不容易理论计算。
- 卷积编码软判决的性能明显优于硬判决，方案(4)中软判决比硬判决节省2dB功率，方案(5)中节省约3dB功率。

方案对比：

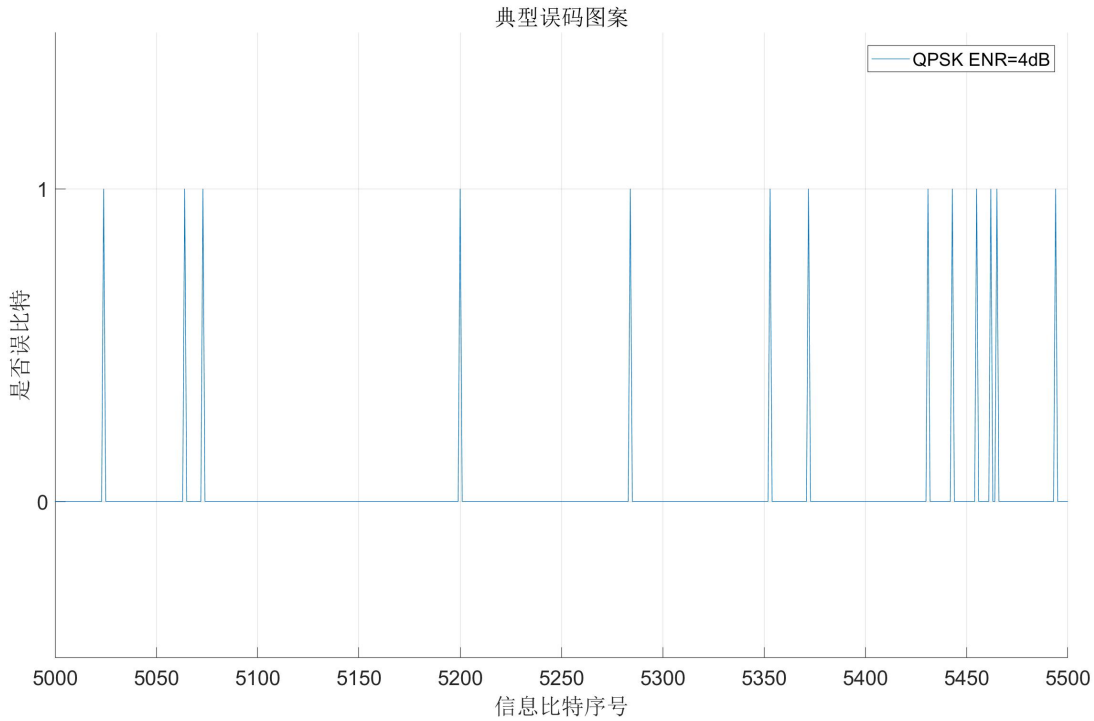
从误码率的角度看，$E_b/n_0 > 0.5dB$ 时最好使用方案(4)[QPSK+1/2卷积]，$E_b/n_0 < 4dB$时采用方案(2)[QPSK]；

若想节约带宽，可以选择方案(3)，或[8PSK+1/2卷积]（相应的符号率可以更小）之类的方案。

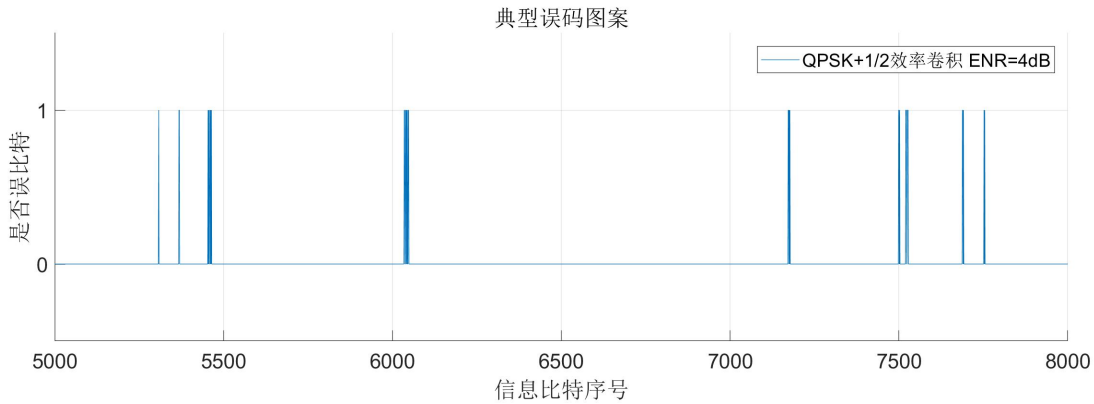
如果不在意解码复杂度，卷积码最好一律采用软判决。

4.典型误码图案

方案(2) QPSK 无卷积 $E_b/n_0 = 4dB$:



方案(4) QPSK+1/2效率卷积 $E_b/n_0 = 4dB$:



分析：采用卷积码时，信道误码明显呈现突发性；不采用卷积码时，信道误码基本呈现随机性。（理论上QP）

接口定义

本节给出波形信道接口定义，完整实现见附件

```
function [out] = WaveChannel(sstream,M,m,ENR)
    %%%%%%%%%%%%%%%%%%
    %parameter
    %sstream: input complex symbol stream
    %M : modeling bits per symbol (1=BPSK,2=4QAM,3=8PSK)
    %m : inversed coding rate of convolution code (m=1,2,3 => Rc=1,1/2,1/3)
    %ENR: Eb/n0(dB form). For noise-free case, omit this parameter or set as inf
    %output
    %out: received sampled complex symbol stream
    %%%%%%%%%%%%%%%%%%
    %must use row vector
    %%%%%%%%%%%%%%%%%%
```

总结

本次实验，我主要负责了波形信道部份的设计与仿真。这一部分内容主要涉及通信与网络课程知识，难点在于用离散样点刻画连续波形时，对符号能量、比特能量、噪声功率谱密度的表达。

我首先根据信道带宽和传输速率要求，设计了不同(R_s,R_m,R_c)的编码方案。之后完成了信道函数编写，并对通信系统展开联调，获得了不同方案的误比特率曲线，不同时刻的信号波形、功率谱，以及典型误码图案等。其中仿真值与理论推导结果成功对应。

本次实验，我有以下收获：

1.深入理解了如何用离散采样系统表述连续波形。其中重点包括用`fft`计算频谱、功率谱，相关代码如下：

```
Fsn = abs(fft(Sn)/(length(Sn))).^2; %功率谱psd
Fsn = fftshift(Fsn);
ff = ([-length(Fs)/2:length(Fs)/2-1]/length(Fs));
```

这样做的前提是采样率`fs`归一化。`fs`归一化还有其他好处，例如离散的`sum`，`conv`直接对应积分、卷积的结果，不需要调整系数。

上面的例子中，还要注意功率谱的定义。我们在相关课程里讨论的主要是随机过程的功率谱，需对自相关函数做傅里叶变换。事实上，对确定信号的功率谱还有更直接的定义，就是其频谱的模平方。

2.理解了E_b/n_0的物理意义和仿真表达。E_b/n_0描述通信系统克服单位强度的噪声所付出的能量，是一个客观的指标，任何编码方式都可以用此指标对比纠错性能。仿真中，根据E_b和(R_m,R_c)计算出符号能量E_s，将每个符号成型滤波后波形能量的期望值调整到E_s，而n_0的表达，首先默认存在一个低通采样，之后直接按定义乘出噪声功率即可（细节前面已经讨论）。另外注意，等效复基带上的$E_{b,B}$，$n_{0,B}$与实际值是有一定换算关系的，前面已经讨论。

3.对编码增益的理解：观察误比特率曲线，高信噪比时，卷积编码达到同样的误码率所需E_b/n_0优于无编码情况，这个优势就是编码增益的体现。采用简单的重复码是无法获得这种编码增益的。

4.进一步加强了采用Matlab仿真通信系统的能力。

由于本次实验中我着力解决信道相关问题，对安全编码部份参与较少。实际的密码实现是由马泽余（非对称椭圆曲线加密）与秦达飞（对称AES加密）完成的。本报告中设计的结果都不涉及加密、解密过程。我也参与了信道、安全编码联调，发现加上密码后误码率的性质有了变化。简单而言，由于加了密码，传输过程一旦出现很小的错误，接收端解出的明文可能有巨大差别，甚至可能解不出明文。因此，想要利用安全编码，信道质量必须足够好，或者需要用足够强的信道编码来保护密文。这部分仿真主要由秦达飞进行。

附 文件清单

我负责的主要文件：

`WaveChannel.m`：波形信道的完整代码，其中包括波形、功率谱的计算与绘制。

`Simulation.m`：仿真误比特率的代码，同时是完整通信系统的示例代码。

`第二次Project_整体报告.pdf`：列出小组所有工作的整体架构，阐明分工。

`第二次Project_陈森睿.pdf`：我的个人报告，即此文件。

其他重要文件：

`genKey.m`：椭圆曲线加密算法，由马泽余实现。

`bits2syms.m`，`syms2bits.m`：电平信道，前者实现比特到复电平的调制，后者将接收到的复电平判决为比特。由秦达飞基于第一次作业实现。

`aesxxx.m`等文件：AES加密算法，秦达飞实现。

其他文件大多来自第一次project。