概述

10个填空，一个2分。其他全是大题

曾老师负责的前半部分内容，难度远大于刘老师负责的后半部分。

如果你**不做作业**或者说**全是抄的**，我只能说等着挂科，同学，该该，挂挂，嘻嘻、。

而且这一年前半部分没有任何教材、PPT等。破防了。

以作业顺序说一下哪些考了哪些没考

曾老师的内容

LFSR寄存器：1大题，11分（还是10来着，记不得）

题目是4bit的移位寄存器。给了你8个状态流

要求：

1.求出反馈（本原）多项式

2.求出初始状态

作业内容

有难度，但相对于曾老师的其他题已经算是简单了。呜呜呜

svd：1大题，忘了多少分，巨难

并未考用手对矩阵进行svd分解

题干给出原始图像和水印图像的SVD分解方式

两问：

第一问：咋提取？

第二问：有同学（如果让我知道你是谁我得谢谢你）提出两次嵌入，即:将真水印w_true嵌入假水印w_false。再将w_false嵌入原始图形，问你全部嵌入过程

范数、距离相似度

填空题考了一个Levenshtein distance，总共就两分。

这一节课没发作业无从复习

最优化：1大题，10分

二元函数的二阶牛顿法

长得跟这一样，你只要看了就会

例：试用牛顿法求 $\min f(x)=x_1^2+25x_2^2$

解：令 $x^0=(2,2)^T$（初值）

$$\nabla f(x^0)=\begin{pmatrix}\frac{\partial f}{\partial x_1}\\ \frac{\partial f}{\partial x_2}\end{pmatrix}=\begin{pmatrix}2x_1\\ 50x_2\end{pmatrix}=\begin{pmatrix}4\\ 100\end{pmatrix}$$

$$H(x^0)=\nabla^2 f(x^0)=\begin{pmatrix}\frac{\partial^2 f}{\partial x_1^2} & \frac{\partial^2 f}{\partial x_1\partial x_2}\\ \frac{\partial^2 f}{\partial x_2\partial x_1} & \frac{\partial^2 f}{\partial x_2^2}\end{pmatrix}=\begin{pmatrix}2 & 0\\ 0 & 50\end{pmatrix}$$

$$\therefore x^1=x^0-\frac{\nabla f(x^0)}{\nabla^2 f(x^0)}$$

$$=\begin{pmatrix}2\\ 2\end{pmatrix}-\begin{pmatrix}2 & 0\\ 0 & 50\end{pmatrix}^{-1}\begin{pmatrix}4\\ 100\end{pmatrix}$$

$$=\begin{pmatrix}2\\ 2\end{pmatrix}-\frac{1}{100}\begin{pmatrix}50 & 0\\ 0 & 2\end{pmatrix}\begin{pmatrix}4\\ 100\end{pmatrix}$$

$$=\begin{pmatrix}0\\ 0\end{pmatrix}$$

由判决条件（收敛条件）$\|\nabla f(x^1)\|=0$，或 $\|f(x^1)\|=0$

故 $x^1=\begin{pmatrix}0\\ 0\end{pmatrix}$ 为极小点。

马尔科夫

只有一个填空，让判断一个链的周期性、常返性

隐马尔科夫HMM：1大题，忘了多少分，巨难

题目背景就是作业内容，比作业内容还更简单一点，去掉了无密钥的状态

但是，你会作业不代表你会这个。考场上和平时是不一样的

第一问：写出状态转移矩阵，1分

第二问：判断是否存在稳定状态，求出极限状态

第三问：给你一条观测序列，算算最有可能的隐含序列

第四问：这个芯片是不是泄露了信息，如何改进？，1分

第三问占这题一半以上分数，根本没法算。时间也不够

刘老师的内容

Bloom过滤器

只在填空题中涉及了它的m和k的公式

数论

欧拉函数有一个填空

乘法逆元是基本知识

欧拉定理和EEA计算逆元并未考到

代数基础：群元素的阶、生成元、子群 1大题

作业内容。作业会了这个就会

椭圆曲线 ： 1大题

作业内容，比作业多了一个椭圆曲线的阶。作业会了这个就会

概率论部分（自学但是很重要）

最大似然估计：1大题，10分。跟作业内容一模一样。

退一步说，就算你没做作业，这题也不难，吃上学期概率论老本也能做

朴素贝叶斯分类的假设，平滑处理，一个填空

差分隐私的并行合成性质，一个填空

随机几何

二维的 HPPP 节点与其最近邻居的距离分布 ，一个填空，直接让你写概率分布

坎贝尔定理没考。