密码学与信息安全第二次作业

郭嘉　17345019　数学与应用数学

2020 年 4 月 18 日

1.（第二章第 1 题）

要纠正两位错误，我们只需要这八个码的最短距离至少为 5

下面的八个码字最短距离为 6 显然符合这个要求。

(111000000000000000000000)

(000111000000000000000000)

(000000111000000000000000)

(000000000111000000000000)

(000000000000111000000000)

(000000000000000111000000)

(000000000000000000111000)

(000000000000000000000111)

2.（第二章第 4 题）

不妨设距离为 3 的两个码字为

a=00000 和 b=11100

只需要证明在同构意义下存在唯一的两个码字 c，d 使得 a,b,c,d 组成二元 [5,4,3] 码

首先分析 c 的末两位: 由抽屉原理，存在 a,b 中的一个，使得他们的前三位有两位与 c 相同，这就说明了 c 的末两位必须为 11，否则最短距离小于 3。

对 d 也同理，它得末两位也是 11

再考虑 c,d 的前三位，由于还需要至少 1 位与 a,b 不同，所以它们的前三位不能全是 1 或全是 0，故有两个 0 或两个 1。

然而注意 c，d 间的距离也得是 3，所以他们前三位之和肯定是 111，比如说 100+011 010+101 001+110

但是这三种方案在同构意义下是一样的，所以我们就得到了唯一性。

并给出了这四个码字

00000 11100 10011 01111

得证

3.（第二章第 5 题）

如果存在二元 [n,K,d] 码，我们找到距离为 d 的两个码字，比如说他们的第 i 位不等，那我们把所有码字的第 i 位去掉，那么就得到了一个二元 [n-1,K,d-1] 码

如果存在二元 [n-1,K,d-1] 码，我们找到距离为 d-1 的两个码字, 这两个码字末位后再加 1 位，分别加 0，1。对于其它码字，我们在他们末位也加一位，但是随便加就行。那么我们就得到了一个二元 [n,K,d] 码

得证

4.（第二章第 7 题）

(1) 前面两个参数分别是 2n 和 K_1K_2 是显然的，我们只需要说明最小距离是 min（ d_1, d_2 ）

对于两个不同的码字（ c_1, c_2 ）和（ c_1', c_2' ）

如果 $c_1 = c_1'$ $c_2 \neq c_2'$ 则两者距离最小值为 d_2

如果 $c_1 \neq c_1'$ $c_2 = c_2'$ 则两者距离最小值为 d_1

如果 $c_1 \neq c_1'$ $c_2 \neq c_2'$ 则两者距离最小值为 $d_1 + d_2$

综上所述，最小距离是 min（ d_1, d_2 ）

(2) 前面两个参数分别是 2n 和 K_1K_2 是显然的，我们只需要说明最小距离是 min（ $2d_1, d_2$ ）

如果 $c_1 = c_1'$ $c_2 \neq c_2'$ 则两者距离最小值为 $2d_1$

如果 $c_1 \neq c_1'$ $c_2 = c_2'$ 则两者距离最小值为 d_2

如果 $c_1 \neq c_1'$ $c_2 \neq c_2'$ 首先考察前 n 位的最小距离显然为 d_1

然后考察后 n 位，即 $\mathrm{d}(c_1 + c_2, c_1' + c_2')$

由三角不等式

$\mathrm{d}(c_1 + c_2, c_1' + c_2')+\mathrm{d}(c_1' + c_2', c_1 + c_2') \geq \mathrm{d}(c_1 + c_2, c_1 + c_2')$

即 $\mathrm{d}(c_1 + c_2, c_1' + c_2')\geq d_2 - d_1$

故该种情况距离至少是 $d_1 + d_2 - d_1 = d_2$

综上所述最小距离是 min（ $2d_1, d_2$ ）

得证