20131910023-金洋

IT-EX09-HAMMING-CRC  
1.Hamming 码如何纠正一位错误?

答：利用矩阵H的结构译码。矩阵H称作奇偶校验矩阵并具有如下性质:对任意码字c均有Hc=0。设是第i个位置为1其余位置为0的向量。如果码字的第i个位置损坏，则接收到的向量为。如果将矩阵H与这个接收到的向量相乘，则得到这正好是H的第i列向量。因此，通过计算就可以发现接收向量的哪一个位置损坏了。

2.讨论 CRC 码的检错能力.

答：CRC即循环冗余校验码（Cyclic Redundancy Check）：是数据通信领域中最常用的一种差错校验码，其特征是信息字段和校验字段的长度可以任意选定。

CRC的原理：若设码字长度为N，信息字段为K位，校验字段为R位(N=K+R)，则对于CRC码集中的任一码字，存在且仅存在一个R次多项式g(x)，使得：其中:m(x)为K次信息多项式， r(x)为R-1次校验多项式，g(x)称为生成多项式：

发送方通过指定的g(x)产生CRC码字，接收方则通过该g(x)来验证收到的CRC码字。

生成多项式：16位的CRC码产生的规则是先将要发送的二进制序列数左移16位后,再除以一个多项式,最后所得到的余数既是CRC码。任意一个由二进制位串组成的代码都可以和一个系数仅为‘0’和‘1’取值的多项式一一对应。

首先可确定的是，CRC码是一种检错纠错能力很强的校验码。

当接收方检测到CRC码字出错，要求重发，即可能实现纠错。

检错：CRC码被G(x)整除，所得的余数与出错位之间有唯一的对应关系。根据这一关系便可立即确定出错位的位置。

注：若某位出错，则余数不为0.对此余数补零后继续作模2除法，又得到一个不为0的余数。

3.如何在基础有限域的基础上通过不可约多项式进行域的扩张?

答：设L是一个域。如果K是L的一个[子集](http://baike.so.com/doc/5587470-5800065.html" \t "http://baike.so.com/doc/_blank)在域L中的加法与乘法运算封闭且K中每个元素的加法与乘法逆仍在K中，则我们说K是L的一个子域，L看作K上的扩域，叫做K上的域扩张，记作L/K。

L的包含K的任一子域叫做域扩张L/K的一个中间域(或中间扩张或子扩张)。

给定一个域扩张L/K以及L的一个子集S，我们记K(S)为L包含K与S的最小子域。我们说K(S)由将S中元素添加到K中生成。如果S只包含一个元素s，我们通常将K({s})记成K(s)。这样形式的域扩张L=K(s)称为单扩张，而s称为这个扩张的本原元。

给定一个域扩张L/K，则L也可视为K上一个矢量空间。L中的元素是矢量而K中的元素是数量。矢量加法就是L中加法，数量乘法是用K中的元素乘以L中的元素。这个矢量空间的维数称为扩张的度数，记作[L:K]。

度数1的扩张(即L等于K)称为平凡扩张。度数为2和3的扩张分别称为二次扩张与三次扩张。由度数是有限或无限决定一个扩张称为有限扩张或无限扩张。

在F的扩域E中取子集S，F中添加S后生成的扩域记作F(S)F(S)，要注意这个定义总是以扩域E的存在为前提的。考察F(S1)(S2)，由定义知它是包含F,S1,S2F,S1,S2的域，而(S1∪S2)是包含F,S1∪S2的最小域，故有F(S1∪S2)⊆F(S1)(S2)F。同样也可以推到F(S1)(S2)⊆F(S1∪S2)，这样就得到了公式（1）。

F(S1)(S2)=F(S2)(S1)==F(S1∪S2)