曲线插值和译码原理

Darren Glass
Gettysburg 大学数学系
地址：Gettysburg, PA 17325－1486
邮箱：dglass@gettysburg.edu

前言：

我们经常需要在存在干扰信号的情况下传输数据，这些干扰信号可能引起传输错误，比如当我们在网上下载文件、与亲戚朋友打电话、将电脑上的数据发送到打印机的时候。

一个称为编码理论的数学分支正致力于寻找及时发现信息传输过程中的错误并且纠正他们。编码理论的目标是在信息长度变化尽量小的前提下建立尽可能多的冗余。大量的译码理论使用很深奥的数学理论来达到这个目的，但是其中的大量工作却是围绕小学生都知道的

“两点确定一条直线”

的欧几里得几何学展开。准确的说，我们将用更高级的说法来描述这个事实：”

“任意 n 个 x 坐标不同的点确定一个 n-1

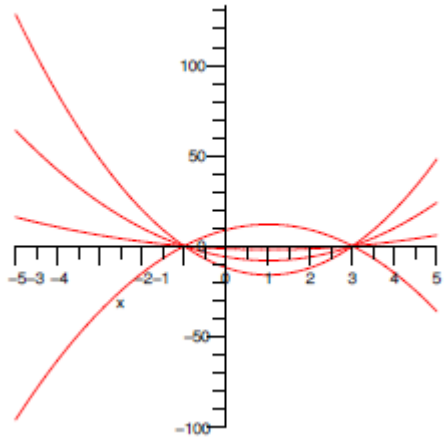
阶多项式 $y = a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$。”

在接下来的部分，我们讨论为什么这个事实是正确的，并介绍几种方法来证明它，紧接着讨论了 Reed 和 Solomon[1960]如何使用它创造了一类纠错码。我们认为，Reed-Solomon 码是一个为受到充分重视的数学应用，但同时它又是一个极其有用而且很容易被任何一个仅上过几周线性代数公开课的学生接受编码。

多项式插值：

通过两点可以作一条直线是欧几里得的假定一；从适用于欧氏几何的解析几何中知道这条线是唯一的。但是为什么三个点决定唯一的一个二次方程？

我们开始给出一个可能的答案：在做抛物线的时候，你可以选择任意两个 x 值作为抛物线的零点。列如：让我们选择两个零点的 x 值：$x_1 = -1, x_2 = 3$。正如你在图一中看到的，许多不同的抛物线均通过这两个零点。事实上，对于任意一个常数 a，曲线 $y = a(x+1)(x-3)$ 通过这两个点（-1,0）和（3,0）



图一

根据在 189 页中引出的事实，我们可以再多选择一个点来确定一个唯一的二次方程。在不选择 x=0 作为任意零点坐标的前提下，我们可以选择 y 轴的截距点作为第三个点。特别的，我们可以指定该曲线过（0,3）点，过这三个点的唯一的多项式是 $y=-x^2+2x+3$（作为一个有趣的侧面，思考如果我们选（0,0）作为 y 轴交点会有什么发生？）

这种基于 x 坐标的通过取点来确定唯一曲线的方法在推广到确定不具有两个零点的或者指定多余三个点（考虑到高阶多项式）的多项式时，用解析几何的方法写下一个详细的证明是很乏味的。

许多学生在线性代数课上见到过一种不同的方法可以来证明这个事实，只要 $x_1,\cdots,x_n$ 不同，下列的范德蒙矩阵就是可逆的。

$$\begin{bmatrix} 1 & x_1 & {x_1}^2 & \cdots & {x_1}^{n-1} \\ 1 & x_2 & {x_2}^2 & \cdots & {x_2}^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_n & {x_n}^2 & \cdots & {x_n}^{n-1} \end{bmatrix}$$

很多线性代数的习题都是证明这个矩阵式可逆的。由于它的可逆性，对于任意的 $y_1,\cdots,y_n$，以下线性系统有唯一解 $a_1,\cdots,a_n$：

$$\begin{bmatrix} 1 & x_1 & {x_1}^2 & \cdots & {x_1}^{n-1} \\ 1 & x_2 & {x_2}^2 & \cdots & {x_2}^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_n & {x_n}^2 & \cdots & {x_n}^{n-1} \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_n \end{bmatrix} = \begin{bmatrix} y_0 \\ y_1 \\ \vdots \\ y_n \end{bmatrix}$$

a_{is} 的唯一性也意味着最高 n-1 阶且过指定点的多项式的唯一。

$$P(x)=a_{n-1}x^{n-1}+\cdots+a_1x+a_0$$

除了有用的曲线插值，范德蒙矩阵也应用在离散傅立叶变换，表象理论、对称群，以及数学的其他许多方面。

通过拉格朗日插值可以很快找到a_{is}，拉格朗日插值通过以下形式定义多项式。

$$p(x)=\sum_{j=1}^{n} y_i \prod_{i\neq j} \frac{x-x_i}{x_j-x_i}$$

编码理论：

编码理论的目标是为了纠正错误而在信息中加入尽可能多的冗余同时保持消息的合理长度。

比如，你想传输 8675309，但是你担心线路噪声过大从而导致错误。一种简单的做法是传输信息两次，如果收到的信息是 8679300 和 8695329，那么很容易确定错误发生了，因为两次的传输结果不一致。可以确定两次传输结果的第三位至少有一个是错误的。不幸的是，我们无法确定那个信息的第三位是正确的。

稍微复杂一些的方法就是传输这个信息三次，这样接受者或许可以纠正错误。假设收到的信息是 8679300/8695329/8775309。解码的大致规则：如果两个以上的传输结果同一位相同，就认为它是正确的，因为同一位置的信息出现相同的错误的可能性是很小的。

你有可能猜到了：如果想要更准确的传输信息，就多重复几次。这确实有效，但是随着传输长度的增加，会占用更多的带宽（或者通话时间）。

然而，还有许多其他的纠错方法，许多人以复杂的方式运用尖端的的数学。有兴趣的初学者可以开始了解盖伦[1993]或罗马[1997]。

Reed-Solomon 码

Reed-Solomon 码只需要简单的多项式插值来纠正错误，比以上简单的方法更加高效。

例子。假定我们要传输信息（1，-2，-1）。首先把这些信息作为多项式系数进行编码：$f(x)=x^2-2x-1$。然后，计算在规定的点的值并传输这些值。例如，假定这些预先选择点是 0,1,2,3,4；所以我们计算 f(0) =-1，f(2)=-2,f(2)=-1,f(3)=2,f(4)=7.传输信息（-1，-2，-1,2,7）。

如果没有错误，接收到的信息可以利用拉格朗日插值或者其他的方法求出唯一的通过点（0，-1），（1，-2），（2，-1），（3,2），（4,7）的二次函数，二次函数的系数就是预期信息。

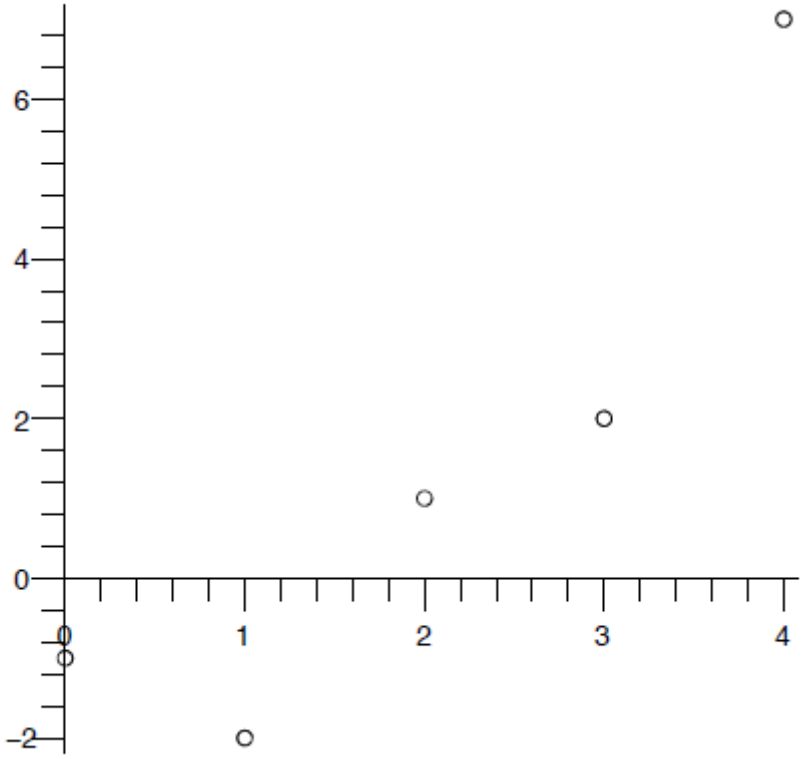
我们来看一下这种方法的优点，注意在收到的信息中有一个是错误的将会发生什么。例如：收到的信息是 C=（-1，-2,1,2,7）。

如果我们把这五个点画出来，很容易检测传输过程中发生了一个错误，因为这些点不在位于一条抛物线上（图二）。此外，我们可以找一条通过尽可能多的点的多项式来纠正这个错误。

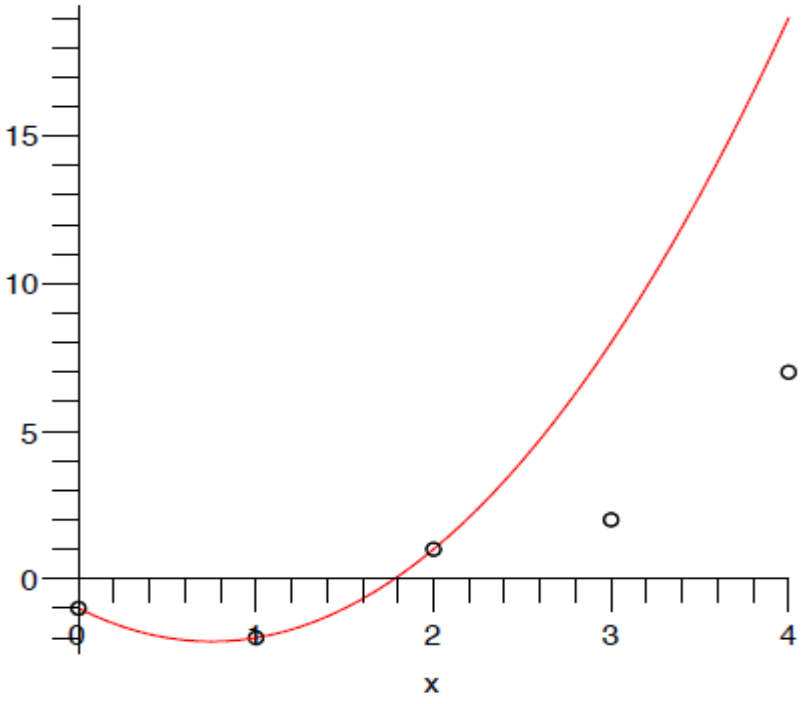
如果对前三个点做插值（例如用拉格朗日插值），得到$f_1(x)=2x^2-3x-1$，但是有两个点不符合。

相似的，如果选中间三个点去确定二次多项式，得到$f_2(x)=-x^2+6x-7$，这又有另外另个点不符合。但是，如果我们选第一个，第二个，第四个点去确定二次多项式，就得到

$f(x)=x^2-2x-1$，它同时通过了第五个点！这就是在五个点不在同一条抛物线上时我们能得到的最好的结果。



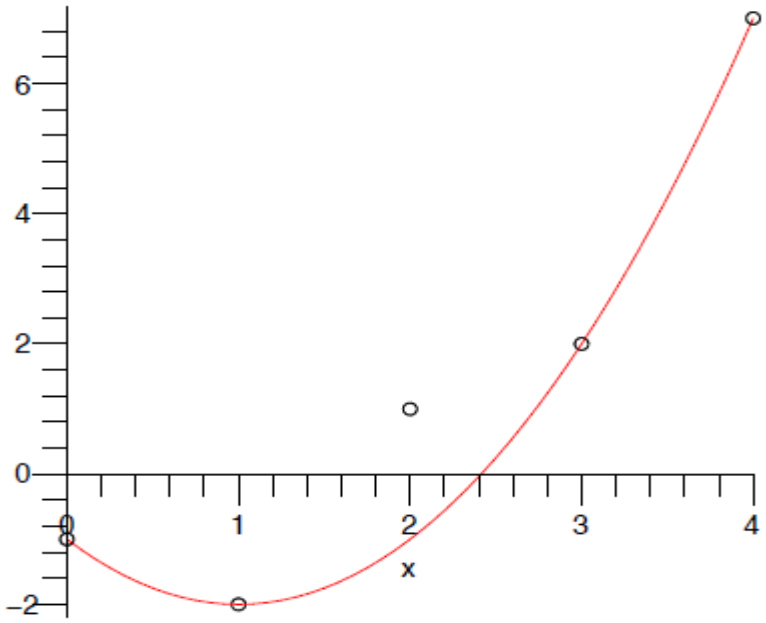
图二：传输错误导致点不在同一条抛物线上



图三：抛物线过前三个点但是不过后两个点

此外，由于任意三个点确定一条抛物线，没有通过任何其他四个点的多项式。因此，这

个过程就恢复了原始的信息。将这个例子和最初幼稚的发送两次的方法作比较，我们发送了较短的信息（五个字符而不是六个）并且纠正了错误，而不是去识别结果。这是 Reed-Solomon 码优势的表现。



图三：过第一第二第四点的抛物线也通过第五点但是不通过第三点

更一般的，假设我们有一个长度为 k 的消息但是技术能力和时间只能完成长度为 n 的传输。Reed-Solomon 方法以指定 n 个点 $x_1,\cdots,x_n$ 开始。如果这些值能通过一个小于 k 阶的多项式计算生成，那这样 n 个数的数组就可以包含 k 个有效的码值

例子：如果 n=4，$x_1=1,x_2=2,x_3=3,x_4=4$，（-2，-1,0,1）是一个包含两个有效码的编码数组，因为这些点插值形成的多项式 f(x)=x-3 是线性的。但是（0,0,0,1）不是包含二个有效码的编码，因为没有一条一次或者常数曲线通过这四个点。

为了传输信息，构造一个 k-1 阶多项式 g(x),计算多项式在 n 个指定点 $x_1,\cdots,x_n$ 的值并传输他们。由于任何两个含有 k 个有效码的长度为 n 的数组最多只有 k-1 个共同点，如果两个阶数小于 k 的多项式有 k 个共同点，那么他们就是同一个多项式了，所以 n 个点至少有 n-（k-1）个点不同。那么，所以这些 n 维元组必须在预先规定的 n 个点中至少 n-(k-1)个点上不同。所以改变少于 n-k+1 个值在这个 n 元数组中将会导致码文无效，并且我们可以检测到 n-k 个错误。

下面有一个很明显的例子：试着改变任何两个值在这个含有两位有效信息的含有四个元素的数组（-2，-1,0,1）你将看到结果是 4 元组码文失效！更多的，如果你只改变这个含有四个元素的数组其中的一个值，我可以做到纠正它，通过找到这条唯一的通过其它三个点的线。（我甚至在不知道你改变的是哪一个元素的情况下也可以做到纠正它，只要其它三个或四个点是共线的）在下面的情况下：

Reed-Solomon 码可以纠正 $[\frac{n-k}{2}]$ 个错误

海明距离：

一个概念化的情形是将含有 k 个有效码的长度为 n 的编码看做 n 维空间中的一点。但是，我们并不是测量两点间的欧氏距离，我们定义了一种新的以理查德海明命名的海明距离，其值等于坐标不相同的个数。理查德海明被认为是编码理论之父。

在这个概念中，被 194 页的那个多项式包含的两个 k 有效的点必须有 n-k+1 个不同在海明距离中。所以任意的点 x 有至少一个 k 有效点，这个 k 有效点距离最多为$[\frac{n-k}{2}]$，甚至如果有两个 k 有效点 y 和 z，同时他们的距离小于或等于$[\frac{n-k}{2}]$，那么根据三角不等式，y 和 z 的距离最多为 $2[\frac{n-k}{2}]$，也就是严格意义上面的少于 n-k+1。

特别的，如果我们从一个 k 有效点开始，并做一些改变在$[\frac{n-k}{2}]$个位置上，我们原始的点将会是这样一个点：与改变后的点，伴随着一个半径$[\frac{n-k}{2}]$。所以我们可以纠正这些错误通过移动连接 k 有效点并且半径是$[\frac{n-k}{2}]$的点。

总结：

这个方法可以被发展成为像 Goppa 1981 年发展的 AG 码一样高效的码文。这个曲线插值方法有给定阶数的多项式，在 x 轴上每一点都有定义，并且当 x 趋于无穷大时有一个孤立奇点。更进一步，AG 码是在其它有规定零点的曲线或这些使得函数有定义并且按顺序的极点的方面在寻找一些曲线或函数。总体上的思想还是通过计算曲线在 n 个不同点上的值。你就得到一段长度为 n 的码文。或许这里还有许多其它有效的编码译码方法，其主要还是依靠曲线的智慧和灵感和这些规定的使得函数没有定义的零点或极点。依赖于选择曲线和函数，或许能增加效能（或者一个乏缺）在编码和解码中完全明白这个方法需要一些代数与几何和一些相关分析方法，在这些方面 walker[2000]给出了一些非常好的介绍和入门知识。

这里还有一些其它的方法来构造编码。事实上，许多可能会说其实编码译码理论真实的目的也就是定义一些 n 维空间中的一些点集，使得它们能够有效的被包络，同时以一个大距离而拥有最小的总体积。球面包络是一项长期的研究问题，并且也有居多其它的应用，对于这方面可以进一步参考 pfender 和 zieglar 的研究。

参考文献：

Gallian, Joseph. 1993. How computers can read and correct ID numbers.
Math Horizons (Winter 1993): 14–15.

Goppa, V. 1981. Codes on algebraic curves. *Doklady Akademii Nauk SSSR* 259 (6): 1289–1290.

Lay, David. 2003. *Linear Algebra and Its Applications*. 3rd ed. Reading, MA: Addison-Wesley.

Leon S. 1980. *Linear Algebra with Applications*. New York: Macmillan.
Pfender, Florian, and G¨ unter M. Ziegler. 2004. Kissing numbers, sphere packings, and some unexpected proofs. *Notices of the American MathematicalSociety* 51 (8): 873–883.
http://www.ams.org/notices/200408/fea-pfender.pdf .
Reed, I., and G. Solomon. 1960. Polynomial codes over certain finite fields. *SIAM Journal* 8 (2): 300–304.
Roman, S. 1997. *Introduction to Coding and Information Theory*. New York: Springer-Verlag.
Shifrin, T., and M. Adams. 2002. *Linear Algebra: AGeometric Approach*. NewYork: W.H. Freeman.
Walker, J. 2000. *Codes and Curves.* IAS/Park City Mathematical Subseries. Providence, RI: American Mathematical Society, and Princeton, NJ: Institute for Advanced Study.

关于作者:

Darren Glass在Rice大学获得了他的文学学士学位，通过一个双主修数学和数理金融分析。他接着去了Pennsylvania大学，在那里他学习了计算几何并获得了文学硕士和哲学博士学位。几年后，在哥伦比亚大学做一个NSF-VIGE博士后研究，Glass 2005年进入了Gettysburg 大学。主要研究数论和代数几何，着眼于在密码领域和编码理论的应用。在它的空闲时间他喜欢和他的小儿子一起看棒球、烹饪墨西哥食物。

民主党初选的保险和边界

Michael A. Jones
Mathematical Reviews
第四街区 416
Ann Arbor, MI 48103
maj@ams.org
Jennifer M.Wilson
Eugene Lang 大学
The New School for Liberal Arts
纽约, NY 10011
wilsonj@newschool.edu

引言

纽约州参议员希拉里·克林顿和伊利诺伊州联邦参议员巴拉克·奥巴马之间的长期较量使得2008年民主党选举成为近代历史上最激烈的初选之一。全民选举产生的8位候选人里，只有三个人收到了代表权。到了 2008 年二月 5 日的“超级星期二”（这对于 2008 年被冠以“超级骗子星期二”，因为 24 个州举行预选）的时候，除了人气最高的两个候选人之外其他所有的候选人都已经被选出了。是什么使得这个人选急剧缩小？部分答案在于总统选举过程中的指派代表分配。

广为人知的分配就是各个州在美国众议院获得一定数量的名额（参见Eisner [1992]和Malkevitch [2000]）。鲜为人知的是，分摊在民主党总统初选中也起着至关重要的作用。民主代表选拔规则（表一）规定授予代表要依据其在区和州的受欢迎程度的比例（在[Geist, Jones and Wilson 2010]中提到）。然而各州之间的细节有差别，所以竞选是采用了汉密尔顿方法：只有至少得到15%投票的候选人才能获得代表权。

我们在意的是分摊方式和临界值（比如15%）之间的关系。一个较大的临界值能尽快消灭那些支持率不高的候选人。这个特点对于选举初期的格局是有影响的，比如，新罕布尔市州的历史上第一次选举。民主党15%的选择象征着更广泛更具包容性的政治妥协，同时更快更果断的达成了共识，而共和党“赢者垄断”的局面则证明了临界值大可以更快消灭低支持率的候选人。

表一
民主党代表选拔规则
美国民主党2006年，15（D段13部分）

步骤	做法
1	将每一个代表候选人在国会区的得票率换算成三位小数的百分比
2	将第一步得票率低于15%的人除去，重新计算三位小数得票率
3	每个代表候选人的得票百分比乘代表票数
4	按照第三步所得结果取整的数值分配代表票
5	若有剩下的代表票，则奖励给第三步的最高分获得者

我们用切断最少必要支持和足够的候选人接受委托之间关系的方法研究结论。

无论什么分摊方法，一个代表候选人收到的代表票不仅取决于他的民众表决份额，而且取决于其他候选人的票数分配。事实上，下列三种情况可能发生：

1 .候选人不管如何分割民众投票都不足以赢得委任；

2 .以特定的方式分割民众投票可能为代表候选人赢得委任；

3 .候选人无论如何分割民众投票，都足以赢得委任。

这三种情况之间的边界可以被描述为两个优化问题的解决方案