数论在近似分析中的应用

1981年颁发的国家自然科学一等奖。除此而外，王元在区间中殆素数分布、最小原根估计及哥德巴赫数的研究也有一定的影响。

从1959年开始，华罗庚与王元研究了在近似分析中，如何用基于数论思想的可计算与决定性方法来尽可能取代统计实验的蒙特卡罗方法的问题。他们建议的方法基于代数数论与丢番图逼近论。这一方法用于重积分近似计算很有效。国外称为“华-王方法”。获陈嘉庚物质科学奖。

1980年以后，他从事于代数解析数论的研究。将有理数域上的关于丢番图方程与不等式的结果，推广至代数数域上去，得到同等精密的结果。他关于这方面的系统研究，已总结成专著《代数数域上的丢番图方程与不等式》，已在德国施普林格出版社出版。

他花了很多心血培养中国的年轻数论学家。冯克勤、裴定一、陆洪文、谢盛刚、陆鸣皋、於坤瑞、徐广善、王连祥、朱尧辰与张荣肖等教授都曾在他直接领导下工作过。他的研究工作也对其他一些数学家产生过影响。

王元也注意数学普及工作，曾协助华罗庚从事中学生数学竞赛活动，也曾去中国工业部门普及数学方法。还为中学生与工程技术人员撰写过数学普及书。

一、导　引

蒙特卡罗方法的要旨为将一个分析问题变为一个答案相同的概率问题，然后用统计模拟来研究后面这个问题。因此对于一些很难用经典计算方法求解的问题就有可能用蒙特卡罗方法得到满意的结果。但蒙特卡罗方法的计算误差仍嫌太大。近似分析中的数论方法是近30年来兴起与发展的。这一方法的要旨是用一个$\mathbb{R}^s$中区域D上的一个决定性的与可计算的点集P来代替蒙特卡罗方法中的随机数列。P要求在某种意义下在D上一致分布。通常称P为伪随机贯，而数论方法又称为伪蒙特卡罗方法。在已知的情况下，由数论方法得到的结果都比蒙特卡罗方法得到的结果更精密，无论从理论的角度来说还是从应用的角度说皆然。

卡罗波夫（1957，1959），拉夫卡（1961），哈尔顿（1960），华罗庚与王元（1960，1964）首先建议了单位立方体上的伪随机贯。他们的方法及其应用均详细地述于华罗庚与王元的书《数论在近似分析的应用》[1981，施普林格出版社与科学出版社]中。

华罗庚与王元的方法基于经典代数数论与丢番图逼近论的应用。本文的目的在于给他们的方法与其应用一个通俗阐述。有兴趣了解细节的读者可以参阅上述华罗庚与王元的书。我们还向读者介绍王元与方开泰最近发表的关于数论方法在应用统计中的应用的文章，见《数学年刊》(中国)，11B，51－65，384－394。

二、一致分布

我们将在本节给出$\mathbb{R}^s$一个区域D的一个点集贯一致分布的定义及一个集合的偏差的定义。为简单计，我们仅考虑$D=[0,1]^s=G_s$为s一维单位立方体的情况。我们用$\mathbf{r}=(r_1,\cdots,r_s)$表示一个实矢量及$|\mathbf{r}|=r_1\cdots r_s$。命$n_1<n_2<\cdots$为一个自然数列及

$$P_{n_l}(k)=\left(x_1^{(n_l)}(k),\cdots,x_s^{(n_l)}(k)\right),\quad 1\leqslant k\leqslant n_l$$

为一个 G_s 中的点集，再命 $N(n_l,\mathbf{r})$ 表示集合 $P_{n_l}(k)$ $(1\leqslant k\leqslant n_l)$ 中满足

$$0\leqslant x_i^{(n_l)}(k)\leqslant r_i,\qquad 1\leqslant i\leqslant s$$

的点数及

$$\sup_{\mathbf{r}\in G_s}\left|\frac{N(n_l,\mathbf{r})}{n_l}-|\mathbf{r}|\right|=D(n_l)。$$

若 $D(n)=o(1)$，即 $\lim\limits_{n\to\infty}D(n)=0$，则称集合贯 $(P_{n_l}(k))$ $(n_1<n_2<\cdots)$ 在外尔(1916)意义之下一致分布并有偏差 $D(n)$ 或简称集合 $P_n(k)$ $(1\leqslant k\leqslant n)$ 有偏差 $D(n)$。

$D(n)$ 表示一个点集贯或一个点集的均匀度的测度。我们需要找出偏差小的贯，而这个贯可以用作伪随机贯。由近似分析的角度，我们还要求 $P_n(k)$ 的表达式简单些。

三、分圆域与丢番图逼近

我们用 $\mathbb{Q}$ 表示有理数域。假定 α 是一个代数数；即 α 是一个整系数的既约方程 $f(x)=0$ 的根，则 $\mathbb{Q}(\alpha)=\{\beta=\beta(\alpha)\mid\beta=r_0+r_1\alpha+\cdots+r_{s-1}\alpha^{s-1},\ r_i\in\mathbb{Q}\}$ 也是一个域，此处 s 表示 $f(x)$ 的次数。假定 $\alpha^{(1)}(=\alpha),\alpha^{(2)},\cdots,\alpha^{(s)}$ 为 $f(x)=0$ 的所有根。我们称 $\beta^{(i)}=\beta(\alpha^{(i)})$ $(2\leqslant i\leqslant s)$ 为 β 的共轭。如果 $\prod\limits_{i=1}^{s}\beta^{(i)}=\pm1$，则我们称 β 是一个单位。

命 p 为一个素数 $\geqslant5$ 及 $s=\frac{p-1}{2}$，则 $\mathscr{R}_s=\mathbb{Q}(\cos\frac{2\pi}{p})$ 是一个 s 次域。我们称它为分圆域。命 g 为 $\bmod p$ 的一个原根，即当 $1\leqslant l<p-1$ 时，$g^l\not\equiv1\pmod p$，则熟知

$$\varepsilon_j=\frac{\sin\frac{\pi}{p}g^{j+1}}{\sin\frac{\pi}{p}g^j},\qquad 1\leqslant j\leqslant s-1$$

为 $\mathscr{R}_s$ 的一组独立单位，即矩阵 $(\varepsilon_j^{(i)})$ $(2\leqslant i\leqslant s,\ 1\leqslant j\leqslant s-1)$ 的行列式非零。所以方程组

$$\begin{aligned}&\left|\varepsilon_1^{x_1}\cdots\varepsilon_{s-1}^{x_{s-1}}\right|=N,\\&\left|\varepsilon_1^{(i)x_1}\cdots\varepsilon_{s-1}^{(i)x_{s-1}}\right|=N^{-\frac{1}{s-1}},\quad 2\leqslant i\leqslant s\end{aligned}$$

有唯一的解 $(x_1,\cdots,x_{s-1})$。命 $a_i=[x_i]$，$1\leqslant i\leqslant s-1$，此处 $[x]$ 表示 x 的整数部分，则得一个单位

$$\eta=\pm\varepsilon_1^{a_1}\cdots\varepsilon_{s-1}^{a_{s-1}}$$

满足

$$\eta>N,\ \eta^{(i)}\ll N^{-\frac{1}{s-1}},\qquad 2\leqslant i\leqslant s,$$

从而我们得到一组单位 $(\eta_l)(l=1,2,\cdots)$ 满足

$$\eta_l > l, \quad \eta_l^{(i)} \ll \eta^{-\frac{1}{s-1}}, \ i = 2,\cdots,s, \ l = 1,2,\cdots. \tag{1}$$

命

$$n_l = \sum_{i=1}^{s}\eta_l^{(i)}, \ \omega_j = 2\cos\frac{2\pi j}{p}, \text{及 } h_j = \sum_{i=1}^{s}\omega_j^{(i)}\eta_l^{(i)}, 1 \leqslant j \leqslant s-1,$$

则熟知 n_l 与 $h_j(1 \leqslant j \leqslant s-1)$ 都是普通整数。由 (1) 可知

$$n_l = \eta_l + O(n_l^{-\frac{1}{s-1}}) = \eta_l(1 + O(n_l^{-1-\frac{1}{s-1}})),$$
$$h_j = \omega_j\eta_l + O(n_l^{-\frac{1}{s-1}}) = \omega_j\eta_l(1 + O(n_l^{-1-\frac{1}{s-1}})).$$

因此得联立有理逼近

$$\frac{h_j}{n_l} = \omega_j + O(n_l^{-1-\frac{1}{s-1}}), \ 1 \leqslant j \leqslant s-1. \tag{2}$$

集合贯

$$P_{n_l}(k) = \left(\frac{k}{n_l}, \left\{\frac{h_1 k}{n_l}\right\}, \cdots, \left\{\frac{h_{s-1}k}{n_l}\right\}\right), 1 \leqslant k \leqslant n_l, \ l = 1,2,\cdots \tag{3}$$

即被看作伪随机贯，此处 $\{x\}$ 表示 x 的分数部分。我们可以证明 $(P_{n_l}(k))$ 的偏差为

$$D(n_l) = O(n_l^{-\frac{1}{2}-\frac{1}{2(G-1)}+\varepsilon}), \tag{4}$$

此处 ε 为任意正数。

对于其他一些与 G_s 不同的区域上的伪随机贯亦可以得到。

四、应　　用

1. 数值积分

考虑定积分

$$I(f) = \int_{G_s} f(\underset{=}{x})d\underset{=}{x} = \int_0^1\cdots\int_0^1 f(x_1,\cdots,x_s)dx_1\cdots dx_s,$$

我们有求积公式

$$I(f) \cong \frac{1}{n_l}\sum_{k=1}^{n_l} f(P_{n_l}(k)). \tag{5}$$

特别当 $s=2$ 时有 $n_l=F_{l+2}$ 及 $h_1=F_{l+1}$，此处 (F_l) 是斐波那契贯，即 (F_l) 由 $F_0=0$，$F_1=1$，$F_{l+1}=F_l+F_{l-1}$ $(l\geqslant 1)$ 定义，我们有

$$\int_0^1\int_0^1 f(x_1,x_2)dx_1dx_2 \cong \frac{1}{F_{l+2}}\sum_{k=1}^{F_{l+2}} f\left(\frac{k}{F_{l+2}}, \left\{\frac{F_{l+1}k}{F_{l+2}}\right\}\right). \tag{6}$$

假定

$$\frac{\partial^{2m} f}{\partial x_1^m \partial x_2^m}, \quad m \geqslant 1$$

及其低次导数连续且囿于 C 时，我们可以证明公式(6)的误差项为 $O\ (CF_{l+2}^{-m}\log F_{l+2})$。

2. 插值法

我们要求寻找一个低次的三角多项式去逼近一个周期函数 $f\ (\underline{x})$。我们将 $f\ (\underline{x})$ 展开成傅里叶级数

$$f(\underline{x}) \sim \sum_{\underline{m}} C(\underline{m}) e^{2\pi i(\underline{m}, \underline{x})}。$$

由于

$$C(\underline{m}) = \int_{G_s} f(\underline{x}) e^{-2\pi i(\underline{m}, \underline{x})} d\,\underline{x},$$

当 $|\underline{m}| = \overline{m}_1 \cdots \overline{m}_s \leqslant N$ 时，我们可以用数值积分法来处理 $C\ (\underline{m})$，此处 $\overline{n} = \max\ (1, |n|)$。$\sum\limits_{|\underline{m}|>N} |C\ (\underline{m})|$ 则可归入误差项。

3. 最优化

假定 $f\ (\underline{x})$ 为 D 上的一个连续函数。我们要求它的整体极大值 M 及一个极大点 $\underline{x}^*$，即满足 $f\ (\underline{x})^* = M$ 的一个点。有很多梯度法可以求解这类极值问题。可惜只有少数情况下才能得到整体极大。若 $f\ (\underline{x})$ 不是单峰函数，及 D 的维数较大，例如 D 的维数$\geqslant 5$，因为在迭代过程中，解答非常依赖于初始点的选取，所以往往只能得到 $f\ (\underline{x})$ 的一个局部极大。因此我们用下面的程序来寻求 M 与 $\underline{x}^*$ 的近似值：

$$m_1 = f(\underline{x}_1),$$

$$m_{k+1} = \begin{cases} m_k, & \text{当 } f(\underline{x}_{k+1}) \leqslant m_k, \\ f(\underline{x}_{k+1}), & \text{当 } f(\underline{x}_{k+1}) \geqslant m_k, \end{cases}$$

此处 $(\underline{x}_1, \underline{x}_2, \cdots)$ 是一个 D 上的一致分布贯，即 $P_n = (\underline{x}_1, \underline{x}_2, \cdots, \underline{x}_n)$ 是一个一致分布点集。经过一个大次数 n 的迭代后，如果 $f\ (\underline{x})$ 适合某些正则条件，则可以希望 m_n 很接近 M。为了提高这个方法的有效性，我们取一个在 D 上一致分布的具有 n_1 个点的集合 P_1，并找出 $f\ (\underline{x})$ 在 P_1 上的极大点 $\underline{x}_1^*$。然后把 D 缩小成一个较小的区域 D_1，它包含 $\underline{x}_1^*$，在 D_1 上作同样的极值问题。如此等等，直到得到一个满意解为止。这个过程称为最优化问题的数论方法的序贯程序，并记之为 SNTO。

4. 试验设计

假定我们需要安排一系列试验以求出在某种意义之下的最佳生产工艺过程。如果需考虑 m ($\geqslant 2$) 个独立因素，而每个因素有 k 个水平，则所有可能试验的总数为 k^m。因为

k^m 这个数太大，所以不可能安排所有的试验。因此我们应该选出具有下述性质的一部分试验，即通过这些试验，我们可以得到一个相当好的生产工艺过程。基于正交拉丁方理论与群论上设计的正交设计具有下述性质：这些试验中每个因素的每个水平及任何两个因素的任何水平组合都相等。这就是正交设计合理的原因，它使试验数目降低至 $O(k^2)$。然而当 k 较大时，试验总数仍嫌太多。现在将因素个数看成空间之维数。我们给每一个试验一个数量表示 l/k $(0\leqslant l<k)$。则我们共得到 G_m 中的 k^m 个点，每个点对应一个试验，而且是一一对应。我们可以用数论方法在这 k^m 个点中找出一个低偏差的含有 k 个点的集合 P 并且按照 P 的点来安排试验。这种方法称为均匀设计。均匀设计合理的理由为 P 在 G_m 上一致分布（王元与方开泰，《科学通报》，1981，485—489）。

假定因素是不独立的。我们将这 m 个因素记为 X_1，…，X_m。假定它们满足 $X_1+\cdots+X_m=1$，$X_i\geqslant 0$ $(1\leqslant i\leqslant m)$，则上述关系式定义了一个单纯形 T。我们可以按照一个在 T 上一致分布的点集来安排试验。

5. 模拟

我们用“情况研究”来说明数论方法在几何概率与模拟问题上的应用。给一个以原点为中心的单位圆 K 及分别以 P_1，…，P_m 为中心与 R_1，…，R_m 为半径的 m 个随机圆 O_1，…，O_m，命 $v(S)$ 表示

$$S=K\cap(O,\cup\cdots\cup O_m)$$

的面积。假定

$$P_i\sim N_2(0,\sigma_i I_2),$$

此处 $\sigma_i>0$ 及 I_2 表示 2×2 恒等方阵。我们需要求出 $v(S)$ 的分布。因两个圆相重叠部分的面积可以由这两个圆的圆心之间的距离来表示，所以当 $m=1$ 时，我们易求出 $v(S)$ 的分布。当 $m>1$ 时，难于求出 $v(S)$ 的解析表达式，故很自然的方法就是用模拟方法 。假定集合 P 含有 N 个点，它在 K 上一致分布。我们用计算机产生 m 个随机圆，其圆心为 $P_i\sim N_2(0,\sigma_i,I_2)$，其半径为 R_i $(1\leqslant i\leqslant m)$。假定 P 的 N 个点中有 M 个被这 m 个随机圆所覆盖，则我们得到关于 $v(S)$ 的一个观察值 $\pi M/N$。我们再产生 m 个随机圆，于是得到另一个观察值，继续这个步骤即可得到 $v(S)$ 的经验分布。因为两个圆的交的面积是已知的，我们可以取 $m=1$ 来比较各种方法的优劣，比较的结果说明数论方法优于古典方法与蒙特卡罗方法。