曲豆豆的数学垃圾堆

(不成体系的杂笔) 1.01 版

曲豆豆 整理

2024 年 6 月 5 日

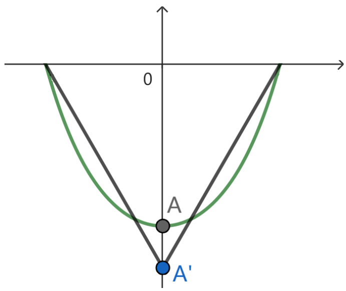
图: 曲豆豆穿上博士服, 就好像真的是博士一样.

目录

1. 微积分、微分方程与数学模型

1.1 悬链线的重心

如下图, 将一条质量分布均匀、可任意弯曲、不可伸缩的理想细绳的两端固定在天花板上, 该细绳在重力作用下自然下垂. 在细绳所在竖直平面上适当建立坐标系 xOy, 使得重力沿 y 轴负方向, 并且细绳两端点的坐标为 $(\pm R, 0)$, 细绳最低点为 A.



杨昊同学提出如下问题: 将细绳最低点 A 竖直向下拖动, 直到细绳被拉直为图中黑色折线, 从物理角度, 细绳在重力作用下自然下垂时处于稳定状态, 重心最低; 而被外力 "拉直" 之后, 重心显然会升高; 能否通过定量计算来验证此结论? 为此, 我们需要分别计算细绳在自然下垂时与被 "拉直" 时重心的位置.

众所周知, 细绳在自然下垂时的形状是**悬链线**, 其方程形如

$$y = \frac{1}{\omega}\left(\cosh \omega x - \cosh \omega R\right), \tag{1.1}$$

其中 $\omega, R > 0$ 为常数. 记该细绳的长度为 $2L$, 则

$$L := \int_0^R \sqrt{1 + (y')^2}\mathrm{d}x = \int_0^R \cosh \omega x \mathrm{d}x = \frac{1}{\omega}\sinh \omega R.$$

注意细绳关于 y 轴对称, 直接计算该细绳重心的纵坐标 y_0 如下:

$$\begin{aligned}
y_0 &= \frac{1}{L}\int_0^R y\sqrt{1+(y')^2}\mathrm{d}x \\
&= \frac{1}{\omega L}\int_0^R (\cosh\omega x-\cosh\omega R)\cosh\omega x\mathrm{d}x \\
&= \frac{1}{\sinh\omega R}\left(\int_0^R \cosh^2\omega x\mathrm{d}x-\cosh\omega R\int_0^R \cosh\omega x\mathrm{d}x\right) \\
&= \frac{1}{\sinh\omega R}\left(\int_0^R \frac{\cosh 2\omega x+1}{2}\mathrm{d}x-\frac{1}{\omega}\cosh\omega R\sinh\omega R\right) \\
&= \frac{1}{\sinh\omega R}\left(\frac{R}{2}-\frac{\sinh\omega R\cosh\omega R}{2\omega}\right) \\
&= \frac{R}{2\sinh\omega R}-\frac{\cosh\omega R}{2\omega}.
\end{aligned}$$

而细绳被 "拉直" 之后, 重心的纵坐标 $\tilde{y}_0$ 为

$$\tilde{y}_0=-\frac{1}{2}\sqrt{L^2-R^2}=-\frac{1}{2\omega}\sqrt{\sinh^2\omega R-\omega^2R^2}.$$

于是只需验证不等式 $\tilde{y}_0>y_0$ 即可, 具体步骤如下:

$$\begin{aligned}
\tilde{y}_0>y_0 &\Leftrightarrow \sinh\omega R\sqrt{\sinh^2\omega R-\omega^2R^2}<\sinh\omega R\cosh\omega R-\omega R \\
&\Leftrightarrow \sinh^2\omega R\left(\sinh^2\omega R-\omega^2R^2\right)<(\sinh\omega R\cosh\omega R-\omega R)^2 \\
&\Leftrightarrow \sinh^2\omega R-2\omega R\sinh\omega R\cosh\omega R+\omega^2R^2\cosh^2\omega R>0 \\
&\Leftrightarrow (\sinh\omega R-\omega R\cosh\omega R)^2>0,
\end{aligned}$$

而由 $\omega R>0$ 易知 $\sinh\omega R-\omega R\cosh\omega R\neq 0$, 从而得证.

1.2 挖穿地球的最速降线

最速降线问题众所周知, 现在我们考虑它的一个变种:

习题 1.1. 将地球视为半径为 R, 密度为 ρ 的均匀球体, 给定地球表面上的两点 A, B, 我们希望挖一条从 A 到 B 的地下隧道, 使得初速度为 0 的质点 m 从 A 出发在地球引力作用下 (不计一切摩擦) 沿隧道滑行至 B 所用时间最短. 不考虑地球自转的影响, 试求满足此要求的隧道的形状.

为研究此问题, 我们先做一些准备工作. 记 r 为质点到球心的距离 $(r \le R)$, 则众所周知, 质点 m 所受引力大小只与 r 有关, 且其值为

$$F(r) = \frac{Gm}{r^2} \cdot \frac{4}{3}\pi r^3 \rho = \frac{4\pi G\rho}{3} mr =: kmr,$$

这里 $k := \frac{4\pi G\rho}{3}$ 为常数, 其中 G 为万有引力常量. 从而质点的引力势能

$$V(r) = \frac{1}{2}kmr^2, \quad (r \le R). \tag{1.2}$$

由于不计一切摩擦, 质点的机械能守恒, 因此当质点距离地心 r 时, 质点的速度大小 v 满足 $\frac{1}{2}mv^2 = V(R) - V(r)$, 整理得

$$v(r) = \sqrt{k(R^2 - r^2)}. \tag{1.3}$$

1.2.1 初步尝试: 直线隧道的情形

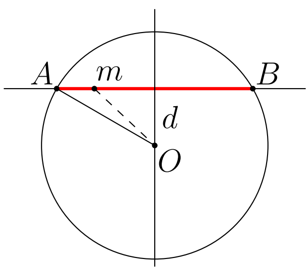


图: 直线隧道的情形

一种天真的想法是, 既然 “两点之间线段最短”, 那就把隧道挖成连接 A, B 两点的线段. 这样的隧道长度最短, 但是否一定意味着沿隧道滑行所用时间最短呢? 我们不妨先考虑这种天真想法.

如上图, 设地心为 O, 在平面 ABO 建立以 O 为原点的直角坐标系使得隧道 (线段 AB) 平行于 x 轴, 记质点 m 的横坐标为 x, 点 O 到线段 AB 的距离为 d. 则由(1.3)式可知

$$\frac{\mathrm{d}x}{\mathrm{d}t} = \sqrt{k(R^2 - (x^2 + d^2))} = \sqrt{k(L^2 - x^2)},$$

其中 $L := \sqrt{R^2 - d^2}$ 为隧道长度的一半, 于是立刻求得质点从 A 到 B 的总滑行时间

$$\begin{aligned} T &= \int_{-L}^{L} \frac{\mathrm{d}t}{\mathrm{d}x}\mathrm{d}x = \frac{2}{\sqrt{k}} \int_0^L \frac{1}{\sqrt{L^2 - x^2}}\mathrm{d}x \\ &= \frac{2}{\sqrt{k}} \int_0^{\frac{\pi}{2}} \frac{1}{L\cos\alpha} \cdot L\cos\alpha \, \mathrm{d}\alpha = \frac{\pi}{\sqrt{k}}. \end{aligned} \tag{1.4}$$

因此, 无论 A, B 两点距离如何, 质点沿线段隧道滑行的总时间始终为 $\frac{\pi}{\sqrt{k}}$. 特别地, 即使当 A, B 两点很接近, 沿线段隧道从 A 滑行到 B 的用时也还是 $\frac{\pi}{\sqrt{k}}$, 这就有些奇怪. 或许沿着笔直隧道滑行有些吃亏, 还应该有用时更短的路线.

1.2.2 模型建立: 变分法, 欧拉-拉格朗日方程, 守恒量

到底应该把隧道修成什么形状呢? 我们如下考虑:

1. 符合要求的隧道一定位于 OAB 平面内, 其中 O 为地心. 否则, 考虑该隧道在 OAB 平面的投影, 容易验证质点在该投影上的滑行时间比原来更短.

2. 于是, 在 OAB 平面上建立以 O 为原点的**极坐标系** (r,θ), 记 A,B 两点的**角位置**分别为 θ_0 与 $\theta_1 := \theta_0+\Delta\theta$, 这里 $\Delta\theta$ 为 A,B 两点的**角距离**, 不妨 $0<\Delta\theta\leq\pi$.

3. 在沿符合要求的隧道滑行时, 质点的角位置 $\theta(t)$ 关于时间 t 单调不减, 否则也可以适当修改隧道的形状使得滑行时间更短. 因此不妨先假设 $\theta(t)$ 关于 t 严格单调递增, 于是隧道的形状可用极坐标方程
$$r=r(\theta) \tag{1.5}$$
来描述. 这里的函数 $r(\theta)$ 满足边值条件
$$r(\theta_0)=r(\theta_1)=R, \tag{1.6}$$
我们需要求出函数 $r(\theta)$ 的解析式.

4. 对于沿符合要求的隧道 $r=r(\theta)$ 滑行的质点, 当质点角位置为 θ 时, 质点的速度大小 v 满足
$$v^2=\dot{r}^2+r^2\dot{\theta}^2=(r_\theta^2+r^2)\dot{\theta}^2,$$
其中 $\dot{r}=\frac{\mathrm{d}r}{\mathrm{d}t}, \dot{\theta}=\frac{\mathrm{d}\theta}{\mathrm{d}t}, r_\theta=\frac{\mathrm{d}r}{\mathrm{d}\theta}$. 又由(1.3)式可知 $v^2=k(R^2-r^2)$, 从而 $\frac{\mathrm{d}\theta}{\mathrm{d}t}=\sqrt{k\frac{R^2-r^2}{r_\theta^2+r^2}}$, 因此质点从 A 滑行到 B 所用时间为
$$\begin{aligned} T[r] = &\int_{\theta_0}^{\theta_1}\frac{\mathrm{d}t}{\mathrm{d}\theta}\mathrm{d}\theta=\frac{1}{\sqrt{k}}\int_{\theta_0}^{\theta_1}\sqrt{\frac{r_\theta^2+r^2}{R^2-r^2}}\mathrm{d}\theta \\ =: &\int_{\theta_0}^{\theta_1}L(r,r_\theta)\mathrm{d}\theta, \end{aligned} \tag{1.7}$$
其中函数
$$L(r,r_\theta):=\sqrt{\frac{r_\theta^2+r^2}{k(R^2-r^2)}} \tag{1.8}$$

是此系统的**拉格朗日量**. 注意总时间 $T[r]$ 与隧道的形状, 即函数 $r(\theta)$ 有关, 它是 "函数 $r(\theta)$ 的函数", 即所谓的**泛函**.

5. 于是问题转化为: 求定义在 $[\theta_0, \theta_1]$ 且满足边值条件(1.5)的函数 $r(\theta)$, 使得总时间 $T[r]$(1.7)取到最小值. 这是典型的泛函极值问题, 我们需要用**变分法**.

   这里不妨再次回顾变分法的基本思想: 假设隧道 $r = r(\theta)$ 使得总时间 $T[r]$ 最短, 那么把这条隧道的形状稍微改变一点点, 那么质点沿改变后的隧道滑行的总时间将不比原来短; 特别注意, 在改变隧道形状过程中隧道两端点的位置始终不变.

6. 设 $r = r(\theta)$ 是符合要求的隧道. 任取函数 $a\colon [\theta_0, \theta_1] \to \mathbb{R}$ 使得

$$a(\theta_0) = a(\theta_1) = 0,$$

   并任取足够接近 0 的参数 ε, 则沿曲线 $\theta \mapsto r(\theta) + \varepsilon a(\theta)$ 的滑行时间不少于沿 $r(\theta)$ 的滑行时间, 即 $T[r + \varepsilon a] \geq T[r]$, 从而

$$\left.\frac{\mathrm{d}}{\mathrm{d}\varepsilon}\right|_{\varepsilon=0} T[r + \varepsilon a] = 0$$

   对任何满足 $a(\theta_0) = a(\theta_1) = 0$ 的函数 $a(\theta)$ 都成立. 而

$$\begin{aligned} 0 = \left.\frac{\mathrm{d}}{\mathrm{d}\varepsilon}\right|_{\varepsilon=0} T[r + \varepsilon a] &= \left.\frac{\mathrm{d}}{\mathrm{d}\varepsilon}\right|_{\varepsilon=0} \int_{\theta_0}^{\theta_1} L(r + \varepsilon a, r_\theta + \varepsilon a_\theta)\mathrm{d}\theta \\ &= \int_{\theta_0}^{\theta_1} \left(\frac{\partial L}{\partial r} \cdot a + \frac{\partial L}{\partial r_\theta} \cdot a_\theta\right) \mathrm{d}\theta = \int_{\theta_0}^{\theta_1} a \frac{\partial L}{\partial r} \mathrm{d}\theta + \int_{\theta_0}^{\theta_1} \frac{\partial L}{\partial r_\theta} \mathrm{d}a \\ &= \int_{\theta_0}^{\theta_1} a \left(\frac{\partial L}{\partial r} - \frac{\mathrm{d}}{\mathrm{d}\theta} \frac{\partial L}{\partial r_\theta}\right) \mathrm{d}\theta, \end{aligned}$$

   这里 $L := L(r, r_\theta)$. 再由函数 $a(\theta)$ 的任意性, 立即得到

$$\frac{\partial L}{\partial r} - \frac{\mathrm{d}}{\mathrm{d}\theta} \frac{\partial L}{\partial r_\theta} = 0, \tag{1.9}$$

这正是著名的**欧拉-拉格朗日方程**. 将 L 的表达式(1.8)代入上述方程, 经过一番暴力的求导计算 (建议用计算机完成) 整理得

$$r(R^2-r^2)r_{\theta\theta}=(2R^2-r^2)r_\theta^2+R^2r^2, \tag{1.10}$$

这是关于 $r(\theta)$ 的二阶常微分方程, 其形式复杂, 难以直接求解.

7. 不过我们可以通过寻找**守恒量**来简化计算. 由(1.9)可得

$$\frac{\mathrm{d}L}{\mathrm{d}\theta}=\frac{\partial L}{\partial r}r_\theta+\frac{\partial L}{\partial r_\theta}r_{\theta\theta}=\left(\frac{\mathrm{d}}{\mathrm{d}t}\frac{\partial L}{\partial r_\theta}\right)r_\theta+\frac{\partial L}{\partial r_\theta}r_{\theta\theta}=\frac{\mathrm{d}}{\mathrm{d}\theta}\left(r_\theta\frac{\partial L}{\partial r_\theta}\right),$$

因此

$$H:=L-r_\theta\frac{\partial L}{\partial r_\theta} \tag{1.11}$$

是守恒量 (常数), 称为此系统的**哈密顿量**; 而从 L 得到 H 的上述操作常被称为**勒让德变换**.

8. 将拉格朗日量 L 的表达式(1.8)代入方程(1.11), 得

$$H=\frac{r^2}{\sqrt{k(R^2-r^2)(r^2+r_\theta^2)}}\geq 0,$$

变形整理得

$$r_\theta^2=r^2\left(\frac{1}{kH^2}\frac{r^2}{R^2-r^2}-1\right), \tag{1.12}$$

这是关于函数 $r(\theta)$ 的一阶常微分方程.

综上所述, 符合要求的隧道 $r=r(\theta)$ 应满足方程(1.10), 从而满足方程(1.12). 注意这里面的 k, H 都为常数, 并且 $k=\frac{4\pi G\rho}{3}>0$, $H\geq 0$. 接下来只需要研究此方程.

1.2.3 模型求解: 定性分析与定量计算

在定量求解方程(1.12)之前, 我们先对它作一些定性分析.

1. 注意方程(1.12)左边恒非负, 于是

$$r^2\left(\frac{1}{kH^2}\frac{r^2}{R^2-r^2}-1\right)\geq 0,$$

这当且仅当

$$r\geq\sqrt{\frac{kH^2}{1+kH^2}}R. \tag{1.13}$$

这表明隧道上的点到地心的距离 r 不小于 $\sqrt{\frac{kH^2}{1+kH^2}}R$. 此外注意(1.13)的等号成立当且仅当 $r_\theta=0$.

由于 $r(\theta_0)=r(\theta_1)=R$, 从而由一元微积分中的罗尔定理可知存在某个角位置 $\xi\in(\theta_0,\theta_1)$ 使得 $r_\theta(\xi)=0$. 此时(1.13)取到等号, 因此隧道最低点到地心的距离

$$d=\sqrt{\frac{kH^2}{1+kH^2}}R. \tag{1.14}$$

可见, 隧道最低点到地心的距离 d 与参数 H 有关, H 越大则 d 越接近 R, 从而隧道越 "浅"; 而当 $H=0$ 时 $d=0$, 隧道经过地心.

2. 关于函数 $r(\theta)$ 的单调性. 将(1.12)两边开方得

$$r_\theta=\pm r\sqrt{\frac{1}{kH^2}\frac{r^2}{R^2-r^2}-1}, \tag{1.15}$$

我们应妥善处理上式右边的正负号. 由方程(1.10)可知

$$r_{\theta\theta}=\frac{(2R^2-r^2)r_\theta^2+R^2r^2}{r(R^2-r^2)}>0,$$

从而导函数 r_θ 在区间 (θ_1,θ_2) 严格递增. 又因为在 $\theta=\xi$ 处有 $r_\theta(\xi)=0$, 从而函数 $r(\theta)$ 的单调性总结如下:

θ	(θ_1,ξ)	ξ	(ξ,θ_2)
$\frac{\mathrm{d}r}{\mathrm{d}\theta}$	$-$	0	$+$
r	$\searrow$	最小值	$\nearrow$

特别地, $r(\theta)$ 满足微分方程

$$r_\theta=\begin{cases}-r\sqrt{\frac{1}{kH^2}\frac{r^2}{R^2-r^2}-1}, & \theta\in(\theta_1,\xi)\\ r\sqrt{\frac{1}{kH^2}\frac{r^2}{R^2-r^2}-1}, & \theta\in(\xi,\theta_2)\end{cases}. \tag{1.16}$$

3. 注意 $r(\theta)$ 满足边值条件(1.5), 从而当 $\theta\to\theta_1$ 或者 $\theta\to\theta_2$ 时, $r\to R$; 此时由(1.16)可知 $r_\theta\to\infty$. 这说明曲线 $r=r(\theta)$ 在两端点 A,B 处的切线经过地心.

4. 我们可以把隧道最低点的角位置 ξ 定量计算出来. 只需注意

$$\begin{aligned}\xi-\theta_1&=\int_{\theta_1}^{\xi}\mathrm{d}\theta=\int_R^d\frac{\mathrm{d}\theta}{\mathrm{d}r}\,\mathrm{d}r\\&=\int_d^R\frac{1}{r}\left(\frac{1}{kH^2}\frac{r^2}{R^2-r^2}-1\right)^{-\frac{1}{2}}\mathrm{d}r,\end{aligned}$$

为计算上述定积分, 我们考虑换元 $r\leftrightarrow\varphi$ 如下:

$$\coth^2\varphi=\frac{1}{kH^2}\frac{r^2}{R^2-r^2}\quad\Leftrightarrow\quad r^2=R^2\frac{kH^2\coth^2\varphi}{1+kH^2\coth^2\varphi}, \tag{1.17}$$

则容易验证

$$\frac{\mathrm{d}r}{r}=-\frac{1}{(1+kH^2\coth^2\varphi)\sinh\varphi\cosh\varphi},$$

$$\left(\frac{1}{kH^2}\frac{r^2}{R^2-r^2}-1\right)^{-\frac{1}{2}}=\sinh\varphi.$$

此外, 当 $r\to R$ 时, $\coth^2\varphi\to+\infty$, 从而 $\varphi\to 0$; 当 $r\to d=\sqrt{\frac{kH^2}{1+kH^2}}R$ 时, $\coth^2\varphi\to 1$, 从而 $\varphi\to+\infty$. 于是原积分化为

$$\begin{aligned}
\xi-\theta_1 &= \int_d^R\frac{1}{r}\left(\frac{1}{kH^2}\frac{r^2}{R^2-r^2}-1\right)^{-\frac{1}{2}}\mathrm{d}r\\
&=\int_0^{+\infty}\frac{1}{1+kH^2\coth^2\varphi}\frac{1}{\cosh\varphi}\mathrm{d}\varphi\\
&=\int_0^{+\infty}\frac{1}{1+kH^2\coth^2\varphi}\frac{1}{\cosh^2\varphi}\mathrm{d}\sinh\varphi\\
&=\frac{1}{1+kH^2}\int_0^{+\infty}\frac{t^2}{(t^2+1)\left(t^2+\frac{kH^2}{1+kH^2}\right)}\mathrm{d}t\\
&=\frac{\pi}{2}\left(1-\sqrt{\frac{kH^2}{1+kH^2}}\right).
\end{aligned}$$

在区间 (ξ,θ_2) 中执行完全类似的操作, 也能得到

$$\theta_2-\xi=\frac{\pi}{2}\left(1-\sqrt{\frac{kH^2}{1+kH^2}}\right),$$

于是 $\xi-\theta_1=\theta_2-\xi$, 所以 ξ 恰为区间 (θ_1,θ_2) 的中点, 即

$$\xi=\frac{\theta_1+\theta_2}{2}. \tag{1.18}$$

此外, 隧道两端点 A,B 的角距离 $\Delta\theta$ 满足

$$\begin{aligned}
\Delta\theta=\theta_2-\theta_1 &= (\theta_2-\xi)+(\xi-\theta_1)\\
&=\pi\left(1-\sqrt{\frac{kH^2}{1+kH^2}}\right),
\end{aligned}\tag{1.19}$$

由此解得

$$H=\frac{1}{\sqrt{k}}\frac{1-\frac{\Delta\theta}{\pi}}{\sqrt{1-\left(1-\frac{\Delta\theta}{\pi}\right)^2}},\tag{1.20}$$

可见参数 H 与隧道两端的角距离有关, 随角距离 $\Delta\theta$ 的增大而减小; 这也是参数 H 的几何意义.

5. 我们甚至还可以把在轨滑行的总时间算出来, 并将其与 “天真的” 线段轨道情形(1.4)做作比较. 我们先算出质点从起点 $\theta=\theta_1$ 滑到最低点 $\theta=\xi$ 所用的时间 T_1. 由(1.7)(1.8)以及(1.16)可得

$$\begin{aligned}
T_1&=\frac{1}{\sqrt{k}}\int_{\theta_1}^{\xi}\sqrt{\frac{r_\theta^2+r^2}{R^2-r^2}}\mathrm{d}\theta=\frac{1}{kH}\int_{\theta_1}^{\xi}\frac{r^2}{R^2-r^2}\mathrm{d}\theta\\
&=\frac{1}{kH}\int_R^d\frac{r^2}{R^2-r^2}\frac{\mathrm{d}\theta}{\mathrm{d}r}\,\mathrm{d}r\\
&=\frac{1}{kH}\int_R^d\frac{r^2}{R^2-r^2}\frac{1}{r}\left(\frac{1}{kH^2}\frac{r^2}{R^2-r^2}-1\right)^{-\frac{1}{2}}\mathrm{d}r\\
&=H\int_0^{+\infty}\frac{\cosh\varphi}{\sinh^2\varphi(1+kH^2\coth^2\varphi)}\mathrm{d}\varphi\quad(\text{换元(1.17)})\\
&=\frac{H}{1+kH^2}\int_0^{+\infty}\frac{\mathrm{d}t}{t^2+\frac{kH^2}{1+kH^2}}\quad(\text{换元 } t=\sinh\varphi)\\
&=\frac{\pi}{2\sqrt{k}}\frac{1}{\sqrt{1+kH^2}}.
\end{aligned}$$

同理, 质点从最低点 $\theta=\xi$ 滑行到终点 $\theta=\theta_2$ 所用的时间 T_2 也为 $\frac{\pi}{2\sqrt{k}}\frac{1}{\sqrt{1+kH^2}}$, 因此质点在此隧道滑行的总时长

$$T=\frac{\pi}{\sqrt{k}}\frac{1}{\sqrt{1+kH^2}}\leq\frac{\pi}{\sqrt{k}}.\tag{1.21}$$

可见沿此隧道滑行用时确实比之前沿线段轨道滑行更省时间, 且 H 的值越大, 效果越明显.

1.2.4 球内最速降线的参数方程

我们暂时停下前进的脚步, 总结已有的结果. 记地心为 O, 给定地球表面 A, B 两点, 我们有以下输入数据:

- R, ρ: 分别为地球的半径与密度; G: 万有引力常数;
- $k := \frac{4\pi G\rho}{3}$ 是常数, 由地球本身所决定;
- $\Delta\theta$: 隧道起点与终点的角距离, 即 $\angle AOB$ 的大小, 取值于 $(0, \pi]$.

我们将符合题设的连接 A, B 两点的地下隧道称为**球内最速降线**, 即在连接 A, B 的所有地下隧道中, 质点从 A 静止出发沿此隧道滑行至 B 的用时最短. 我们已有球内最速降线的如下参数:

- d: 球内最速降线上的点到地心的最近距离;
- H: 质点在沿球内最速降线滑行过程中的某守恒量;
- T: 质点沿球内最速降线从 A 静止出发滑行至 B 的用时.

d, H, T 自然视为 $\Delta\theta$ 的函数, 其具体表达式如下 (留做习题):

$$d = \left(1 - \frac{\Delta\theta}{\pi}\right) R, \tag{1.22}$$

$$H = \frac{1}{\sqrt{k}} \frac{1 - \frac{\Delta\theta}{\pi}}{\sqrt{1 - \left(1 - \frac{\Delta\theta}{\pi}\right)^2}}, \tag{1.23}$$

$$T = \frac{\pi}{\sqrt{k}} \sqrt{1 - \left(1 - \frac{\Delta\theta}{\pi}\right)^2}. \tag{1.24}$$

也容易看出, 给定 $d, H, T, \Delta\theta$ 这四个参数之中的任何一个, 其余三个将被唯一确定.

下面我们来写出球内最速降线的具体表达式. 我们已有球内最速降线的微分方程(1.16), 这是最简单的常微分方程, 按道理说两边直接积分暴力计算就能解出来, 但我们还是想把方程的解写得漂亮一些. 用(1.14)将微分方程(1.16)中的常数 H 用 d 来表示, 有

$$\frac{\mathrm{d}r}{\mathrm{d}\theta}=\begin{cases}-\frac{rR}{d}\sqrt{\frac{r^2-d^2}{R^2-r^2}} & \theta\in(\theta_1,\xi),\\ \frac{rR}{d}\sqrt{\frac{r^2-d^2}{R^2-r^2}} & \theta\in(\xi,\theta_2),\end{cases}\tag{1.25}$$

其中 ξ 为轨道离地心最近处的角位置, 在前文已经得到 $\xi=\frac{\theta_1+\theta_2}{2}$. 我们想绕开避免对上述方程右端正负号的分段讨论, 于是先如下观察: 当 θ 从 θ_1 变化到 ξ 时, r 从 R 单调减少至 d, 从而 $\sqrt{\frac{r^2-d^2}{R^2-r^2}}$ 从 $+\infty$ 单调减少至 0; 同理也可分析当 θ 从 ξ 变化到 θ_2 时 $\sqrt{\frac{r^2-d^2}{R^2-r^2}}$ 的变化情况. 于是注意到, $\pm\sqrt{\frac{r^2-d^2}{R^2-r^2}}$ 在区间 (θ_1,θ_2) 的变化趋势非常像 $\phi\mapsto\cot\frac{\phi}{2}$ 在 $\phi\in(0,2\pi)$ 中的样子. 从而考虑引入中间变量 ϕ 如下

$$\cot\frac{\phi}{2}:=\begin{cases}\sqrt{\frac{r^2-d^2}{R^2-r^2}} & \phi\in(0,\pi];\\ -\sqrt{\frac{r^2-d^2}{R^2-r^2}} & \phi\in(\pi,2\pi),\end{cases}\tag{1.26}$$

将 ϕ 视为新的自变量, 并将 r,θ 都视为关于 ϕ 的函数. 则由上式可知 r 与 ϕ 满足如下关系 (留给读者练习):

$$r^2=\frac{R^2+d^2}{2}+\frac{R^2-d^2}{2}\cos\phi,\qquad \phi\in(0,2\pi),\tag{1.27}$$

后文将说明此式的初等几何含义. 而由微分方程(1.25)可得 θ 与 ϕ 满足如下关系:

$$\begin{aligned}\frac{\mathrm{d}\theta}{\mathrm{d}\phi}&=\frac{\mathrm{d}\theta}{\mathrm{d}r}\cdot\frac{\mathrm{d}r}{\mathrm{d}\phi}=-\frac{d}{Rr}\tan\frac{\phi}{2}\cdot\frac{-(R^2-d^2)}{4r}\sin\phi\\&=\frac{d(R^2-d^2)}{2R}\cdot\frac{1-\cos\phi}{(R^2+d^2)+(R^2-d^2)\cos\phi},\end{aligned}$$

从而有

$$
\begin{aligned}
\theta &= \frac{d(R^2-d^2)}{2R}\int\frac{1-\cos\phi}{(R^2+d^2)+(R^2-d^2)\cos\phi}\mathrm{d}\phi\\
&= \frac{d(R^2-d^2)}{2R}\int\frac{1-\frac{t^2-1}{t^2+1}}{(R^2+d^2)+(R^2-d^2)\frac{t^2-1}{t^2+1}}\cdot\frac{-2}{t^2+1}\mathrm{d}t\\
&\qquad\text{(万能代换 } t=\cot\frac{\phi}{2}\text{)}\\
&= -\frac{d(R^2-d^2)}{R^3}\int\frac{1}{(t^2+1)\left(t^2+\frac{d^2}{R^2}\right)}\mathrm{d}t\\
&= \frac{d}{R}\int\left(\frac{1}{t^2+1}-\frac{1}{t^2+\frac{d^2}{R^2}}\right)\mathrm{d}t\\
&= \frac{d}{R}\cdot\frac{\pi-\phi}{2}-\arctan\left(\frac{R}{d}\cot\frac{\phi}{2}\right)+C,
\end{aligned}
$$

注意初值条件: 当 $\phi\to 0$ 时 $\theta\to\theta_1$, 由此可确定积分常数

$$
C=\theta_1+\left(1-\frac{d}{R}\right)\frac{\pi}{2}.
$$

综上所述, 我们有:

性质 1.2. *记号承上, 则球内最速降线在极坐标下的参数方程为:*

$$
\begin{cases}
r=\left(\dfrac{R^2+d^2}{2}+\dfrac{R^2-d^2}{2}\cos\phi\right)^{\frac{1}{2}},\\
\theta=\theta_1-\dfrac{d}{2R}\phi+\dfrac{\pi}{2}-\arctan\left(\dfrac{R}{d}\cot\dfrac{\phi}{2}\right),
\end{cases}
\tag{1.28}
$$

其中参数 $\phi\in(0,2\pi)$.

我们对此参数方程稍作讨论. 在前文(1.22)我们已有 $\Delta\theta=\pi\left(1-\frac{d}{R}\right)$; 于是当参数 ϕ 分别趋于 $0, 2\pi$ 时, θ 分别趋于 θ_1 以及 $\theta_1+\pi\left(1-\frac{d}{R}\right)=$

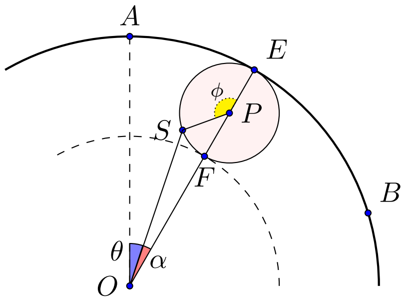
$\theta_1 + \Delta\theta = \theta_2$, 这与前文结果吻合. 此外, 当参数 $\phi = \pi$ 时, $\theta = \theta_1 + \frac{\pi}{2}\left(1 - \frac{d}{R}\right) = \theta_1 + \xi$, 其中 ξ 见前文(1.18)式, 是球内最速降线距地心最近点的角位置; 而此时 $r = \left(\frac{R^2+d^2}{2} - \frac{R^2-d^2}{2}\right)^{\frac{1}{2}} = d$ 也就应该是离地心的最近距离.

1.2.5 初等几何解释, 圆内摆线

球内最速降线的参数方程(1.28)中的参数 $\phi \in (0, 2\pi)$ 有明显的初等几何含义. 只需将 $r = r(\phi)$ 的解析式改写为

$$r^2 = \left(\frac{R+d}{2}\right)^2 + \left(\frac{R-d}{2}\right)^2 + 2 \cdot \frac{R+d}{2} \cdot \frac{R-d}{2} \cos\phi, \tag{1.29}$$

就不难发现这很像初等几何学中的**余弦定理**表达式, 只不过这里的 ϕ 代表某个三角形的外角而不是内角. 另一个观察是, 隧道起点与终点的球面距离 (大圆弧长) 为 $R\Delta\theta = \pi(R-d)$, 这恰为半径为 $\frac{R-d}{2}$ 的圆的周长.



(1.30)

事实上, 想象一个半径为 $\frac{R-d}{2}$ 的圆, 记作 $\odot P$, 此圆与地球 (记作 $\odot O$) 内切于点 A, $\odot P$ 上的一个定点 S 与 A 重合 (上图未画出); 令 $\odot P$ 沿 $\odot O$ 内壁无打滑地向 B 点滚动, 滚动过程中两圆始终内切, 切点记作 E. 当滚动角度 ϕ 时, 点 S 的位置如上图所示. 由前文可知, 当 $\odot P$ 滚动一周

后, 两圆恰好内切于点 B. 我们断言: 在此滚动过程中, 点 S 的轨迹即为球内最速降线; 反之, 球内最速降线都形如此.

在上图中, $|PS| = \frac{R-d}{2}$ 为 $\odot P$ 的半径, $|OP| = \frac{R+d}{2}$, $|OF| = d$, $\phi := \angle EOS$ 为 $\odot P$ 的旋转角, $\theta := \angle AOS$ 表示点 S 的角位置 (这里不妨 $\theta_1 = 0$, 并且临时约定 θ 沿顺时针方向为正; 此外, 图中所画为滚动角度 ϕ 很小的情形), 再记 $\alpha := \angle SOP$, 以及 $r := |OS|$ 为 S 到地心的距离. 于是在 $\triangle OSP$ 中使用余弦定理, 立即得知 r 与 ϕ 所满足的关系恰为(1.29).

$\odot P$ 不打滑地滚动表明圆弧 ES 与 EA 的弧长相等, 从而

$$\theta - \theta_1 = \frac{R-d}{2R}\phi - \alpha \tag{1.31}$$

(图中所标注的 θ 实际应该是 $\theta - \theta_1$). 接下来只需用 ϕ 来表示 α. 在 $\triangle OSP$ 中分别使用正弦定理与余弦定理可得

$$\sin\alpha = \frac{R-d}{2r}\sin\phi, \qquad \cos\alpha = \frac{r^2 + Rd}{r(R+d)},$$

两式相除并再次使用(1.29)式, 整理得

$$\tan\alpha = \frac{(R-d)\sin\phi}{(R+d)+(R-d)\cos\phi} = \frac{(R-d)\cot\frac{\phi}{2}}{R\cot^2\frac{\phi}{2} + d},$$

并注意 $|\alpha| < \frac{\pi}{2}$, 因此

$$\alpha = \arctan\frac{(R-d)\cot\frac{\phi}{2}}{R\cot^2\frac{\phi}{2} + d}.$$

将此代入(1.31)可得 $\theta = \theta(\phi)$ 的表达式如下:

$$\theta = \theta_1 + \frac{R-d}{2R}\phi - \arctan\frac{(R-d)\cot\frac{\phi}{2}}{R\cot^2\frac{\phi}{2} + d}, \tag{1.32}$$

这看起来似乎与参数方程(1.28)第二式不太一样? 但其实是一样的, 我们只需继续整理下去:

$$
\begin{aligned}
\text{(1.32)右边} &= \theta_1 - \frac{d}{2R}\phi + \frac{\pi}{2} - \frac{\pi-\phi}{2} - \arctan\frac{(R-d)\cot\frac{\phi}{2}}{R\cot^2\frac{\phi}{2}+d} \\
&= \theta_1 - \frac{d}{2R}\phi + \frac{\pi}{2} - \left(\arctan\cot\frac{\phi}{2} + \arctan\frac{(R-d)\cot\frac{\phi}{2}}{R\cot^2\frac{\phi}{2}+d}\right) \\
&= \theta_1 - \frac{d}{2R}\phi + \frac{\pi}{2} - \arctan\frac{\cot\frac{\phi}{2} + \frac{(R-d)\cot\frac{\phi}{2}}{R\cot^2\frac{\phi}{2}+d}}{1-\frac{(R-d)\cot^2\frac{\phi}{2}}{R\cot^2\frac{\phi}{2}+d}} \\
&= \theta_1 - \frac{d}{2R}\phi + \frac{\pi}{2} - \arctan\left(\frac{R}{d}\cot\frac{\phi}{2}\right),
\end{aligned}
$$

刚好是参数方程(1.28)的第二式. 从而断言得证.

这也给参数方程(1.28)中的参数 ϕ 以几何解释: 小圆沿大圆内壁滚动的角度. 由此初等几何解释, 球内最速降线也被称为**圆内摆线**.

1.3 诺特定理: 对称性与守恒律

笔者从小就被洗脑 “空间平移不变 $\Leftrightarrow$ 动量守恒”, “时间平移不变 $\Leftrightarrow$ 能量守恒”, 以及更一般的 “**对称性等价于守恒律**”, 但笔者小时候只把这当成一句哲学理念, 而未深究其数学表述. 而如今, 我们稍微花一点点精力来思考一下对称性与守恒律的关系, 尤其是: *时间平移不变怎么就能量守恒了?*

设某个物理系统的拉格朗日量为

$$L = L(\boldsymbol{q}, \dot{\boldsymbol{q}}, t), \tag{1.33}$$

其中 $\boldsymbol{q} = (q^1, q^2, ..., q^n)$ 为广义坐标. 众所周知, 该系统随时间的演化

$t \mapsto \boldsymbol{q}(t)$ 满足**欧拉-拉格朗日方程**

$$\frac{\mathrm{d}}{\mathrm{d}t}\frac{\partial L}{\partial \dot{q}^i} = \frac{\partial L}{\partial q^i}, \quad 1 \le i \le n. \tag{1.34}$$

演化路径 $t \mapsto \boldsymbol{q}(t)$ 的**无穷小变换**是指形如

$$\begin{aligned} \boldsymbol{q}(t) \mapsto\ & \tilde{\boldsymbol{q}}(t) := \boldsymbol{q}(t) + \varepsilon \cdot \delta\boldsymbol{q}(t), \\ t \mapsto\ & \tilde{t} := t + \varepsilon \cdot \delta t, \end{aligned} \tag{1.35}$$

的变量替换, 其中 $t \mapsto \delta\boldsymbol{q}(t)$ 是给定的函数, δt 是给定的常数, 而 ε 为无穷小量. 熟练的读者可以像物理学家一样把 ε 略去不写, 而直接把 $\delta\boldsymbol{q}, \delta t$ 视为无穷小量.

如果无穷小变换(1.35)使得

$$\delta L := \left.\frac{\mathrm{d}}{\mathrm{d}\varepsilon}\right|_{\varepsilon=0} L(\tilde{\boldsymbol{q}}(\tilde{t}), \dot{\tilde{\boldsymbol{q}}}(\tilde{t}), \tilde{t}) = 0, \tag{1.36}$$

称为该无穷小变换为**无穷小对称**. 这正是所谓 “对称性”.

下面看如何从对称性导出 “守恒律”. 设 $t \mapsto \boldsymbol{q}(t)$ 为系统随时间的演化, 它满足欧拉-拉格朗日方程(1.34); 对任意无穷小变换(1.35), 对无穷小量 ε 泰勒展开直接计算得

$$\begin{aligned} L(\tilde{\boldsymbol{q}}(\tilde{t}), \dot{\tilde{\boldsymbol{q}}}(\tilde{t}), \tilde{t}) =\ & L(\boldsymbol{q}, \dot{\boldsymbol{q}}, t) + \varepsilon \left(\frac{\partial L}{\partial q^i}\dot{q}^i + \frac{\partial L}{\partial \dot{q}^i}\ddot{q}^i + \frac{\partial L}{\partial t} \right)\delta t \\ & + \varepsilon \left(\frac{\partial L}{\partial q^i}\delta q^i + \frac{\partial L}{\partial \dot{q}^i}\delta \dot{q}^i \right) + O(\varepsilon^2), \end{aligned}$$

从而立刻得到

$$\begin{aligned} \delta L &= \left(\frac{\partial L}{\partial q^i}\dot{q}^i + \frac{\partial L}{\partial \dot{q}^i}\ddot{q}^i + \frac{\partial L}{\partial t} \right)\delta t + \left(\frac{\partial L}{\partial q^i}\delta q^i + \frac{\partial L}{\partial \dot{q}^i}\delta \dot{q}^i \right) \\ &= \frac{\mathrm{d}L}{\mathrm{d}t}\delta t + \left[\frac{\mathrm{d}}{\mathrm{d}t}\left(\frac{\partial L}{\partial \dot{q}^i} \right)\delta q^i + \frac{\partial L}{\partial \dot{q}^i}\delta \dot{q}^i \right] \end{aligned}$$

$$= \frac{\mathrm{d}}{\mathrm{d}t}\left(\frac{\partial L}{\partial \dot{q}^i}\delta q^i + L\delta t\right) = \frac{\mathrm{d}}{\mathrm{d}t}\left(p_i\delta q^i + L\delta t\right),$$

其中 $p_i := \frac{\partial L}{\partial \dot{q}^i}$ 是**广义动量**. 这表明, (1.35)是无穷小对称, 当且仅当

$$p_i\delta q^i + L\delta t \tag{1.37}$$

是守恒量. 此乃著名的**诺特定理** (的拉格朗日力学版本).

下面考察一些例子.

例题 **1.3.**(空间平移不变 $\Leftrightarrow$ 动量守恒). 给定向量 $\boldsymbol{q}_0 = (q_0^1, ..., q_0^n) \in \mathbb{R}^n$, 考虑沿 $\boldsymbol{q}_0$ 方向的空间平移变换

$$\boldsymbol{q}(t) \mapsto \boldsymbol{q}(t) + \varepsilon\boldsymbol{q}_0,$$

相应的无穷小变换(1.35)满足

$$\delta t = 0, \qquad \delta q^i = q_0^i, \quad (1 \le i \le n).$$

若它是无穷小对称, 则相应的守恒量(1.37)为 $p_i q_0^i$, 这恰为广义动量 $\boldsymbol{p}$ 在 $\boldsymbol{q}_0$ 方向的分量 (的常数倍).

例题 **1.4.**(时间平移不变 $\Leftrightarrow$ 能量守恒). 考虑时间平移变换

$$\begin{aligned} \boldsymbol{q}(t) &\mapsto \boldsymbol{q}(t-\varepsilon) = \boldsymbol{q}(t) - \varepsilon\dot{\boldsymbol{q}}(t) + O(\varepsilon^2), \\ t &\mapsto t + \varepsilon, \end{aligned}$$

相应的无穷小变换(1.35)满足

$$\delta t = 1, \qquad \delta q^i = -\dot{q}^i, \quad (1 \le i \le n).$$

若它是无穷小对称, 则相应的守恒量(1.37)为 $-p_i\dot{q}^i + L$, 这恰为该系统的哈密顿量 $H = p_i\dot{q}^i - L$ 的常数倍.

例题 **1.5.**(空间旋转不变 $\Leftrightarrow$ 角动量守恒). 考虑 $\mathbb{R}^3$ 中的单粒子系统

$$L=\frac{1}{2}m|\dot{\boldsymbol{r}}|^2-V(\boldsymbol{r}),$$

其中 $\boldsymbol{r}=(x,y,z)$ 为粒子的位置. 给定 $\boldsymbol{\omega}\in\mathbb{R}^3$, 考虑位置矢量 $\boldsymbol{r}$ 绕原点以角速度 $\boldsymbol{\omega}$ 的旋转变换, 其无穷小变换满足

$$\delta\boldsymbol{r}=\boldsymbol{\omega}\times\boldsymbol{r},\qquad \delta t=0.$$

若它是无穷小对称, 则相应的守恒量(1.37)为

$$\boldsymbol{p}\cdot\delta\boldsymbol{r}=\boldsymbol{p}\cdot(\boldsymbol{\omega}\times\boldsymbol{r})=\boldsymbol{\omega}\cdot(\boldsymbol{r}\times\boldsymbol{p})=\boldsymbol{\omega}\cdot\boldsymbol{J},$$

这恰为粒子角动量 $\boldsymbol{J}$ 在角速度 $\boldsymbol{\omega}$ 方向上的分量 (的常数倍).

1.4 一个简单的正交矩阵积分计算题

2024 年 6 月 4 日上午, 北京某高校. 不懂分析 的LSQ 老师听说笔者最近在学习矩阵积分, 便决定出题考一考笔者. 题目是这样的:

习题 **1.6.** 考虑正交群 $\mathrm{O}(n)$ 上使得其体积为 1 的 Harr 测度 $\mathrm{d}X$. 在此意义下, 等式

$$\int_{\mathrm{O}(n)}\mathrm{tr}X\,\mathrm{d}X=0,\tag{1.38}$$

$$\int_{\mathrm{O}(n)}(\mathrm{tr}X)^2\mathrm{d}X=1\tag{1.39}$$

为什么成立呢?

LSQ 进一步解释道: 这里的正交群 $\mathrm{O}(n)$ 显然被视为概率空间, Harr 测度 $\mathrm{d}X$ 是相应的概率测度, 而正交矩阵的迹 $\mathrm{tr}X$ 被视为随机变量. 在

此意义下, 等式(1.38)(1.39)相当于说, 随机变量 $\mathrm{tr}X$ 的均值与方差分别为 $0, 1$.

据 LSQ 说, 这题是某人问他的. 提问者以为此题很难, 需要用高等工具, 比如李群理论中的 Weyl 积分公式之类的. 但实际上, 这题很初等. 笔者读完题目后就立刻注意到, 考虑换元积分

$$X \mapsto -X,$$

则 $\int_{\mathrm{O}(n)} \mathrm{tr}X\,\mathrm{d}X = -\int_{\mathrm{O}(n)} \mathrm{tr}X\,\mathrm{d}X$, 因此(1.38)成立. 这个做法利用了积分区域 $\mathrm{O}(n)$ 的对称性, 本质上与奇函数在对称区间上的积分为零没什么区别. LSQ 对此表示满意, 随后吐槽道: 毕竟 $\mathrm{O}(n)$ 有两个连通分支, 如果把积分区域换成连通分支 $\mathrm{SO}(n)$, 或许就非常困难了.

这个困难的问题暂且不提, 我们来看(1.39)为什么成立. 笔者当时站在黑板前, 对着此式发呆数分钟也毫无想法, 毕竟式中的平方项使得对称换元 $X \mapsto -X$ 技巧无效.

LSQ 见笔者毫无想法, 忍不住公布了答案, 他给的解法既暴力又优雅——暴力之处在于强行展开矩阵元, 逐个矩阵元考虑; 优雅之处在于充分利用积分区域 $\mathrm{O}(n)$ 的对称性. 具体如下:

(1.39)式的证明. 首先直接展开得

$$\begin{aligned}\int_{\mathrm{O}(n)} (\mathrm{tr}X)^2 \mathrm{d}X &= \sum_{i,j=1}^{n} \int_{\mathrm{O}(n)} X_{ii}X_{jj}\mathrm{d}X \\ &= \sum_{i=1}^{n} \int_{\mathrm{O}(n)} X_{ii}^2 \mathrm{d}x + \sum_{i\neq j} \int_{\mathrm{O}(n)} X_{ii}X_{jj}\mathrm{d}X.\end{aligned}$$

若 $i \neq j$, 考虑将矩阵 X 的第 j 列乘以 (-1) 而其余各列保持不变的变换, 显然 $\mathrm{O}(n)$ 在该变换下保持不变, 由此易知 $\int_{\mathrm{O}(n)} X_{ii}X_{jj}\mathrm{d}X = 0$. 之后考虑对 X 作行置换, 列置换, 显然这种操作也保持 $\mathrm{O}(n)$ 不变, 由此可

知对任意 $i,j,k,\ell\in\{1,2,...,n\}$ 都有

$$\int_{\mathrm{O}(n)} X_{ij}^2\mathrm{d}X=\int_{\mathrm{O}(n)} X_{k\ell}^2\mathrm{d}X,$$

从而

$$\int_{\mathrm{O}(n)}(\mathrm{tr}X)^2\mathrm{d}X=\sum_{i=1}^{n}\int_{\mathrm{O}(n)} X_{ii}^2\mathrm{d}x=n\int_{\mathrm{O}(n)} X_{11}^2\mathrm{d}X.$$

于是我们只需要计算 X 的某个矩阵元平方的期望. 而这是容易的: 注意 X 为正交矩阵, $X^{\mathrm{T}}X=I$, 于是

$$n=\int_{\mathrm{O}(n)}\mathrm{tr}(X^{\mathrm{T}}X)\mathrm{d}X=\sum_{i,j=1}^{n}\int_{\mathrm{O}(n)} X_{ij}^2\mathrm{d}X=n^2\int_{\mathrm{O}(n)} X_{11}^2\mathrm{d}X,$$

从而 $\int_{\mathrm{O}(n)} X_{11}^2\mathrm{d}X=\frac{1}{n}$. 因此 $\int_{\mathrm{O}(n)}(\mathrm{tr}X)^2\mathrm{d}X=n\int_{\mathrm{O}(n)} X_{11}^2\mathrm{d}X=1$. □

之后笔者便与 LSQ 闲扯了几句, 闲扯之中偶然提到, 如果把(1.39)左边稍微改一下, 把 trace 的平方改成平方的 trace, 那是否也能计算? 即能否计算出

$$\int_{\mathrm{O}(n)}\mathrm{tr}(X^2)\mathrm{d}X$$

的值. 简单讨论后我们发现, 这个变式也很容易, 用完全相同的处理技巧即可: 首先直接展开

$$\int_{\mathrm{O}(n)}\mathrm{tr}(X^2)\mathrm{d}X=\sum_{i=1}^{n}\int_{\mathrm{O}(n)} X_{ii}^2\mathrm{d}X+\sum_{i\neq j}\int_{\mathrm{O}(n)} X_{ij}X_{ji}\mathrm{d}X.$$

右边第一项已经做过; 而当 $i\neq j$ 时, 依然考虑将 X 的第 j 列乘以 (-1) 而其余列保持不变的变换, 由此易知 $\int_{\mathrm{O}(n)} X_{ij}X_{ji}\mathrm{d}X=0$. 综上, 我们有

$$\int_{\mathrm{O}(n)}\mathrm{tr}(X^2)\mathrm{d}X=1.$$

2. 代数、数论与密码学

2.1 多项式的结式及其应用

数论、代数、代数几何等领域常出现与多项式有关的具体计算. 处理这些计算问题的工具有很多, **结式** (resultant) 是其中之一. 结式是发展于 19 世纪的古老工具, 最初被用于求解多元多项式方程组; 虽说如今似乎有些过时, 被更现代的工具所替代 (例如 **Gröbner 基**), 但结式在理论推导与具体计算上仍有值得借鉴之处. 本节介绍结式的概念与性质, 及其在代数学领域中的若干应用.

在本节我们约定:

1. A 是唯一分解整环 (UFD), 例如 $\mathbb{Z}$, $\mathbb{Z}[x_1, x_2, ..., x_n]$ 等.
2. $A[x]$ 是环 A 上的多项式环. 则由代数学中众所周知的结果, $A[x]$ 也是 UFD. 对于正整数 n, 记

   $$A^{(n)}[x] := \{f \in A[x] \mid \deg f < n\},$$

   注意 $A^{(n)}[x]$ 是秩为 n 的自由 A-模.
3. 记 $\mathbb{F} := \mathrm{Frac}(A)$ 是整环 A 的分式域, $\overline{\mathbb{F}}$ 是 $\mathbb{F}$ 的代数闭包.

2.1.1 结式的概念与基本性质

我们想研究如下问题: 对于多项式 $f, g \in A[x]$, 如何判断 f, g 的最大公因式的次数是否大于 1? [其实想问: 如何判断 f 与 g 在 $\overline{\mathbb{F}}$ 的代数

闭包上是否有公共零点?] 若 R 是域, 则可以用欧几里得辗转相除法. 而对于一般情况, 注意到:

引理 2.1. 设多项式 $f,g\in A[x]$ 的次数分别为 m,n, 记 $d:=\gcd(f,g)$ 为 f 与 g 的最大公因式, 则

$$\deg d\geq 1 \quad\Longleftrightarrow\quad \exists\,(u,v)\in A^{(n)}[x]\times A^{(m)}[x],\quad uf+vg=0.$$

证明. 如果 f,g 不互素, 则 $\deg d\geq 1$, 此时取 $u:=\frac{g}{d}$, $v:=-\frac{f}{d}$ 即可. 另一方面, 如果存在符合题设的 u,v, 则由 $uf+vg=0$ 可知 $f|vg$, 从而 $\frac{f}{d}|v\cdot\frac{g}{d}$. 而 $\frac{f}{d}$ 与 $\frac{g}{d}$ 互素, 因此 $\frac{f}{d}|v$. 于是 $m>\deg v\geq\deg\frac{f}{d}=m-\deg d$, 所以 $\deg d\geq 1$. 引理得证. □

引入自由 A-模同态 $R_{f,g}\colon A^{(n)}[x]\times A^{(m)}[x]\to A^{(n+m)}[x]$ 如下:

$$R_{f,g}(u,v):=uf+vg. \tag{2.40}$$

则引理2.1可改写为: $\deg d\geq 1$ 当且仅当 $R_{f,g}$ 不是单同态. 注意 $A^{(n)}[x]$ 是自由 A-模, 具有标准基 $\{1,x,x^2,\ldots,x^{n-1}\}$; 并且 $R_{f,g}$ 可用标准基下的矩阵来表示. 若记

$$\begin{aligned} f&=f_0+f_1x+f_2x^2+\cdots+f_mx^m,\\ g&=g_0+g_1x+g_2x^2+\cdots+g_nx^n, \end{aligned} \tag{2.41}$$

其中 $f_i,g_i\in A$, 且 $f_m,g_n\neq 0$, 则自由 A-模同态 $R_{f,g}$ 在标准基下的矩阵

为

$$\mathrm{Syl}_x(f,g) := \begin{pmatrix} f_0 & & & & g_0 & & \\ f_1 & f_0 & & & g_1 & \ddots & \\ \vdots & f_1 & \ddots & & g_2 & \ddots & g_0 \\ f_m & \vdots & \ddots & f_0 & \vdots & \ddots & g_1 \\ & f_m & & f_1 & g_n & & g_2 \\ & & \ddots & \vdots & & \ddots & \vdots \\ & & & f_m & & & g_n \end{pmatrix}, \tag{2.42}$$

该矩阵称为多项式 f 与 g 的 **Sylvester 矩阵**. 注意 $\mathrm{Syl}(f,g)$ 是环 A 上的 $(n+m)$ 阶方阵, 其主对角线由 n 个 f_0 与 m 个 g_n 组成.

定义 2.2. 对于多项式 $f,g\in A[x]$, 记

$$\mathrm{Res}_x(f,g) := \det \mathrm{Syl}_x(f,g), \tag{2.43}$$

称为多项式 f 与 g 的**结式**(resultant).

考虑 Sylvester 矩阵 $\mathrm{Syl}_x(f,g)$ 的伴随矩阵 $\mathrm{Syl}_x^*(f,g)$, 即

$$\mathrm{Syl}_x(f,g)\,\mathrm{Syl}_x^*(f,g) = \det \mathrm{Syl}_x(f,g)\cdot I_{n+m} = \mathrm{Res}_x(f,g)\cdot I_{n+m},$$

其中 I_{n+m} 是环 A 上的 $(n+m)$ 阶单位矩阵. 由此容易证明:

习题 2.3. 设 $f,g\in A[x]$ 的次数分别为 m,n, 记 $d:=\gcd(f,g)$, 则

1. $\deg d > 1$ 当且仅当 $\mathrm{Res}_x(f,g)=0$.

2. 存在 $(u,v)\in A^{(n)}[x]\times A^{(m)}[x]$ 使得 $\mathrm{Res}_x(f,g)=uf+vg$.

上述习题的 (2) 表明, $\mathrm{Res}_x(f,g)$ 属于环 $A[x]$ 的由 f,g 所生成的理想.

考虑环 A 的分式域 $\mathbb{F} := \operatorname{Frac} A$, 并记 $\overline{\mathbb{F}}$ 为 $\mathbb{F}$ 的代数闭包 (或足够大的扩域), 则(2.41)式在 $\overline{\mathbb{F}}$ 中可分解为

$$\begin{aligned} f &= f_m(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_m), \\ g &= g_n(x-\beta_1)(x-\beta_2)\cdots(x-\beta_n), \end{aligned} \tag{2.44}$$

其中 $\alpha_1,...,\alpha_m$ 与 $\beta_1,...,\beta_n$ 都是 $\overline{\mathbb{F}}$ 中的元素, 它们分别为多项式 f 与 g 的根.

定理 2.4. 记号承上, 则有

$$\operatorname{Res}_x(f,g) = f_m^n g_n^m \prod_{\substack{1\le i\le m \\ 1\le j\le n}} (\beta_j - \alpha_i). \tag{2.45}$$

特别地, $\operatorname{Res}_x(f,g)=0$ 当且仅当 f,g 在 $\overline{\mathbb{F}}$ 上有公共根.

证明. 引入 A 上的 $(m+n+2)$ 元多项式环

$$\hat{A} := A[\hat{f}_m, \hat{g}_n; \hat{\alpha}_1,...,\hat{\alpha}_m; \hat{\beta}_1,...,\hat{\beta}_n],$$

其中 $\hat{f}_m, \hat{g}_n; \hat{\alpha}_1,...,\hat{\alpha}_m; \hat{\beta}_1,...,\hat{\beta}_n$ 是独立的形式变元. 再引入多项式 $\hat{f}, \hat{g} \in \hat{A}[x]$ 如下:

$$\begin{aligned} \hat{f} &:= \hat{f}_m(x-\hat{\alpha}_1)(x-\hat{\alpha}_2)\cdots(x-\hat{\alpha}_m), \\ \hat{g} &:= \hat{g}_n(x-\hat{\beta}_1)(x-\hat{\beta}_2)\cdots(x-\hat{\beta}_n). \end{aligned}$$

注意如下 A-模同态 $\mathrm{ev}\colon \hat{A} \to \overline{\mathbb{F}}$

$$\hat{f}_m \mapsto f_m, \quad \hat{g}_n \mapsto g_n, \quad \hat{\alpha}_i \mapsto \alpha_i, \quad \hat{\beta}_j \mapsto \beta_j.$$

如果证明了 $\hat{A}$ 上的等式

$$\operatorname{Res}_x(\hat{f},\hat{g}) = \hat{f}_m^n \hat{g}_n^m \prod_{\substack{1\le i\le m \\ 1\le j\le n}} (\hat{\beta}_j - \hat{\alpha}_i), \tag{2.46}$$

则将此式两边作用 ev 即得证. 下证(2.46)式.

直接考察 $\hat{f}$ 与 $\hat{g}$ 的 Sylvester 矩阵, 由行列式的基本性质易知

$$\mathrm{Res}_x(\hat{f},\hat{g}) = \hat{f}_m^n \hat{g}_n^m \hat{H},$$

其中 $\quad \hat{H} := \mathrm{Res}_x\left(\prod_{i=1}^{m}(x-\hat{\alpha}_i)\,,\,\prod_{j=1}^{n}(x-\hat{\beta}_j)\right) \in A[\hat{\alpha}_1,...,\hat{\alpha}_m;\hat{\beta}_1,...,\hat{\beta}_n].$

将 $\hat{H}$ 视为环 $A[\hat{\alpha}_1,...,\hat{\alpha}_m]$ 上的关于变元 $\hat{\beta}_1,...,\hat{\beta}_n$ 的多项式. 对于每个 $1 \le j \le n$ 以及 $1 \le i \le m$, 注意当 $\hat{\beta}_j = \hat{\alpha}_i$ 时, $\prod_{i=1}^{m}(x-\hat{\alpha}_i)$ 与 $\prod_{j=1}^{n}(x-\hat{\beta}_j)$ 具有次数 ≥ 1 的公因式, 从而由习题2.3可知 $\hat{H}|_{\hat{\beta}_j=\hat{\alpha}_i} = 0$. 这表明 $\hat{H}$ 能被 $(\hat{\beta}_j-\hat{\alpha}_i)$ 整除. 从而 $\hat{H}$ 形如

$$\hat{H} = \hat{C}\prod_{\substack{1\le i\le m\\1\le j\le n}}(\hat{\beta}_j-\hat{\alpha}_i), \tag{2.47}$$

其中 $\hat{C} \in A[\hat{\alpha}_1,...,\hat{\alpha}_m;\hat{\beta}_1,...,\hat{\beta}_n]$. 下面只需证明 $\hat{C}=1$.

对每个 $1\le j\le n$, 将 $\hat{H}$ 与 $\hat{C}$ 视为关于 $\hat{\beta}_j$ 的多项式, 则由(2.47),

$$\deg_{\hat{\beta}_j}\hat{H} = \deg_{\hat{\beta}_j}\hat{C} + m.$$

另一方面, 直接写出 Sylvester 矩阵 $\mathrm{Syl}_x(\hat{f},\hat{g})$ 并观察其行列式, 易知 $\deg_{\hat{\beta}_j}\hat{H} \le m$. 从而 $\deg_{\hat{\beta}_j}\hat{C}=0$. 同理 $\deg_{\hat{\alpha}_i}\hat{C}=0$. 因此 $\hat{C}\in A$.

在(2.47)式中, 令 $\hat{\beta}_1=\hat{\beta}_2=\cdots=\hat{\beta}_n=0$, 则该式右边等于 $\hat{C}(-1)^{mn}(\hat{\alpha}_1\hat{\alpha}_2\cdots\hat{\alpha}_m)^n$. 另一方面, 注意此时 Sylvester 矩阵

$$\mathrm{Syl}_x\left(\prod_{i=1}^{m}(x-\hat{\alpha}_i)\,,\,x^n\right)$$

是上三角阵, 直接计算其行列式可知 $\hat{H}=(-1)^{mn}(\hat{\alpha}_1\hat{\alpha}_2\cdots\hat{\alpha}_m)^n$. 因此 $\hat{C}=1$, 定理得证. $\square$

由此定理, 立刻得到结式的诸多运算性质, 见下述习题.

习题 2.5. 若 $f, g, h \in A[x]$, $\varepsilon \in A$, 记 $m := \deg f$, $n := \deg g$, 则有

1. $\operatorname{Res}_x(g, f) = (-1)^{mn} \operatorname{Res}_x(f, g)$.
2. $\operatorname{Res}_x(\varepsilon f, g) = \varepsilon^n \operatorname{Res}_x(f, g)$.
3. $\operatorname{Res}_x(f, x-\varepsilon) = f(\varepsilon)$.
4. $\operatorname{Res}_x(fg, h) = \operatorname{Res}_x(f, h) \operatorname{Res}_x(g, h)$.

习题 2.6. 记号同上题, 则还有如下性质:

1. $\operatorname{Res}_x(f(x+\varepsilon), g(x+\varepsilon)) = \operatorname{Res}_x(f(x), g(x))$.
2. $\operatorname{Res}_x(f(\varepsilon x), g(\varepsilon x)) = \varepsilon^{mn} \operatorname{Res}_x(f(x), g(x))$.

我们还有如下重要性质:

性质 2.7. 设 $f, g \in A[x]$ 的次数分别为 m, n, 若存在 $q, r \in A[x]$ 使得

$$f = qg + r,$$

且 $k := \deg r < \deg g$, 则

$$\operatorname{Res}_x(f, g) = (-1)^{nk} g_n^{m-k} \operatorname{Res}_x(g, r),$$

其中 g_n 为 g 的最高次项 x^n 的系数.

证明. 在 $\mathbb{F} := \operatorname{Frac} A$ 的足够大的扩域中, 记 $g(x) = g_n(x-\beta_1)\cdots(x-\beta_n)$, 则

$$\operatorname{Res}_x(f, g) = g_n^m \operatorname{Res}_x\left(f\,,\prod_{j=1}^{n}(x-\beta_j)\right)$$

$$
\begin{aligned}
&= g_n^m \prod_{j=1}^{n} f(\beta_j) = g_n^m \prod_{j=1}^{n} r(\beta_j) \\
&= g_n^{m-k} \operatorname{Res}_x(r, g) = (-1)^{nk} g_n^{m-k} \operatorname{Res}_x(g, r),
\end{aligned}
$$

得证. □

注记 2.8. 上述性质给出了计算结式的高效算法.

2.1.2 用结式解多项式方程组

历史上, 结式最初被用于求解多项式方程组. 对于二元多项式 $f, g \in \mathbb{C}[x, y]$, 我们希望在 $\mathbb{C}$(或其他代数闭域) 中解关于 x, y 的方程组

$$
\begin{cases}
f(x, y) = 0, \\
g(x, y) = 0.
\end{cases} \tag{2.48}
$$

注意到, 如果 $(x_0, y_0) \in \mathbb{C}^2$ 是方程组(2.48) 的一个解, 则 y_0 是多项式 $f, g \in \mathbb{C}[x, y] \cong (\mathbb{C}[x])[y]$ 的公共根; 特别地, f 与 g 作为环 $\mathbb{C}[x]$ 上的关于 y 的多项式, 有公共根, 所以 $\operatorname{Res}_y(f, g) = 0$. 这其实是消元法, 将 y 消掉.

上述 "消元法" 容易推广到更多元的多项式上. 例如我们随手编一道题:

习题 2.9. 在 $\mathbb{C}$ 上解关于 x, y, z 的方程组

$$
\begin{cases}
xz + y^2 + z^2 = 8, \\
4xy + 5yz^3 = 9, \\
x^2 + 3y^2 z + 23 = 0.
\end{cases} \tag{2.49}
$$

[$(x, y, z) = (2, 3, -1)$ 是该方程组的一个解. 除此之外还有别的解吗?]

解. 将方程组中的 3 个方程都视为环 $\mathbb{C}[x,y]$ 上的关于变元 z 的多项式. 类似原因, 应该有 $\begin{cases} \mathrm{Res}_z(y^2-8+xz+z^2, 4xy-9+5yz^3)=0 \\ \mathrm{Res}_z(y^2-8+xz+z^2, x^2+23+3y^2z)=0 \end{cases}$, 经计算可得

$$\begin{cases} 20x^4y^2-45x^3y-60x^2y^4+464x^2y^2+135xy^3+1008xy \\ \qquad -25y^8+600y^6-4800y^4+12800y^2-81=0 \\ x^4-3x^3y^2+46x^2-69xy^2+9y^6-72y^4+529=0 \end{cases},$$

从而将 z 消去, 只需求解上述关于 x,y 的方程组. 再用结式消去 y, 经过暴力计算可得关于 x 的多项式方程

$$(x-2)^2F(x)G(x)=0, \tag{2.50}$$

其中 $F,G\in\mathbb{C}[x]$ 的次数分别是 15, 17, 具体表达式分别是

$$\begin{aligned} F(x)=\ & 15625x^{15}-283750x^{14}-964900x^{13}+8656000x^{12}+50966940x^{11} \\ & +1644957015x^{10}+14207783014x^9+86652061193x^8 \\ & +616119120680x^7+2814555246283x^6+11437322767827x^5 \\ & +48009988716483x^4+114975459599056x^3 \\ & +286286988616187x^2+638569073069411x \\ & -476809020260513, \\ G(x)=\ & 7290000x^{17}-15255000x^{16}+715407625x^{15}-2725329625x^{14} \\ & +38123578475x^{13}-172670600675x^{12}+1346691556605x^{11} \\ & -5925967748625x^{10}+31792829112199x^9-123786880325107x^8 \\ & +478133593383110x^7-1480393966386167x^6 \\ & +3818405557147272x^5-7920782241197577x^4 \end{aligned}$$

$$+ 9272495275430911x^3 - 6717415381685293x^2$$
$$+ 2902982359159976x - 476809020260513.$$

从而由(2.50)解得 $x = 2$, 或者 x 是多项式 F 或 G 的根. 对于上述每个 x, 再去求解 y, z 即可. 计算过程过于暴力, 从略. 但至少能看出, 原方程组除了 $(x, y, z) = (2, 3, -1)$ 这组解之外, 肯定还有别的解. $\square$

注记 **2.10.** 结式的计算可由计算机完成, 例如用符号计算软件 Mathematica.

```
In[14]:= A = Resultant[x z + y^2 + z^2 - 8, 4 x y + 5 y z^3 - 9, z]
              结式
         B = Resultant[x z + y^2 + z^2 - 8, x^2 + 3 y^2 z + 23, z]
              结式
Out[14]= 81 + 1008 x y + 45 x^3 y - 12800 y^2 - 464 x^2 y^2 -
          20 x^4 y^2 - 135 x y^3 + 4800 y^4 + 60 x^2 y^4 - 600 y^6 + 25 y^8

Out[15]= 529 + 46 x^2 + x^4 - 69 x y^2 - 3 x^3 y^2 - 72 y^4 + 9 y^6

In[17]:= Resultant[A, B, y] // Factor
         结式                  因式分解
```

2.1.3 判别式与结式

对于多项式 $f \in A[x]$, 我们关心 f 是否有重根. 如果 $\alpha \in \overline{\mathbb{F}}$ 是 f 的重根, 则 f 能被 $(x-\alpha)^2$ 整除, 记 $f = (x-\alpha)^2 g$, 其中 $g \in \overline{\mathbb{F}}[x]$, 则

$$f' := \frac{\mathrm{d}f}{\mathrm{d}x} = (x-\alpha)(2g + (x-\alpha)g'),$$

从而 f 与 f' 有公因式 $(x-\alpha)$, 因此 $\mathrm{Res}_x(f, f') = 0$.

性质 2.11. 设 $f = f_0 + f_1x + \cdots + f_mx^m \in A[x]$, 其中 $f_m \neq 0$, 则

$$\operatorname{Res}_x(f, f') = (-1)^{\frac{m(m-1)}{2}} f_m^{2m-1} \prod_{i<j} (\alpha_i - \alpha_j)^2, \tag{2.51}$$

其中 $\alpha_1, ..., \alpha_m \in \overline{\mathbb{F}}$ 使得 $f = f_m \prod_{i=1}^m (x - \alpha_i)$.

证明. 从而由结式的运算性质 (见习题2.5) 并注意

$$f' = \sum_{i=1}^{m} \prod_{j \neq i} (x - \alpha_j),$$

直接计算如下:

$$\begin{aligned}
\operatorname{Res}_x(f, f') &= f_m^{2m-1} \operatorname{Res}_x\left(\prod_{i=1}^{m} (x - \alpha_i), f'\right) \\
&= (-1)^{m(m-1)} f_m^{2m-1} \prod_{i=1}^{m} \operatorname{Res}_x(f', x - \alpha_i) \\
&= (-1)^{m(m-1)} f_m^{2m-1} \prod_{k=1}^{m} f'(\alpha_k) \\
&= (-1)^{\frac{m(m-1)}{2}} f_m^{2m-1} \prod_{1 \leq i < j \leq m} (\alpha_i - \alpha_j)^2,
\end{aligned}$$

从而得证. □

定义 2.12. 设 $f = f_0 + f_1 x + \cdots + f_m x^m \in A[x]$, 其中 $f_m \neq 0$, 定义

$$\operatorname{Disc}_x(f) := f_m^{2m-2} \prod_{1\le i<j\le m} (\alpha_i - \alpha_j)^2, \tag{2.52}$$

其中 $\alpha_1, ..., \alpha_m \in \overline{\mathbb{F}}$ 使得 $f = f_m \prod_{i=1}^m (x - \alpha_i)$. 上述 $\operatorname{Disc}_x(f)$ 称为多项式 f 的**判别式** *(discriminant)*.

由定义可知, f 有重根当且仅当判别式 $\operatorname{Disc}_x(f) = 0$; 而性质2.11表明判别式与结式满足关系

$$f_m \operatorname{Disc}_x(f) = (-1)^{\frac{m(m-1)}{2}} \operatorname{Res}_x(f, f'). \tag{2.53}$$

此外, 通过简单计算也容易验证, 对任意 $f, g \in A[x]$ 都有

$$\operatorname{Disc}_x(fg) = \operatorname{Disc}_x(f) \operatorname{Disc}_x(g) \left[\operatorname{Res}_x(f, g)\right]^2. \tag{2.54}$$

[提示: 利用(2.45)(2.53)式直接验证之.]

例题 **2.13.** 若 $f = ax^2 + bx + c \in A[x]$ 是 2 次多项式, 则 $f' = 2ax + b$, 从而

$$\operatorname{Disc}_x(f) = -\frac{1}{a} \operatorname{Res}_x(ax^2 + bx + c, 2ax + b) = b^2 - 4ac,$$

与初中数学所谓 $\Delta = b^2 - 4ac$ 相符合.

例题 **2.14.** 若 $f = x^3 + ax + b \in A[x]$, 验证: $\operatorname{Disc}_x(x) = -4a^3 - 27b^2$.

例题 **2.15.** 设 p 为奇素数, 验证: 分圆多项式 (cyclotomic polynomial)

$$\Phi_p(x) := \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1 \in \mathbb{Z}[x] \tag{2.55}$$

的判别式 $\operatorname{Disc}_x(\Phi_p) = (-1)^{\frac{p-1}{2}} p^{p-2}$.

证明. 注意 $(x-1)\Phi_p = x^p - 1$, 利用(2.54)式直接计算即可, 留给读者. $\square$

2.1.4 代数数的零化多项式

我们知道, 对于实数 $\alpha \in \mathbb{C}$, 如果存在整系数多项式 $f \in \mathbb{Z}[x]$ 使得 $f(\alpha) = 0$, 则称 α 为**代数数**, f 是 α 的一个**零化多项式**. 记

$$\mathbb{A} := \left\{\alpha \in \mathbb{C} \,\middle|\, \alpha \text{ 是代数数}\right\} \tag{2.56}$$

为全体代数数构成的集合.

例题 **2.16.** 设 $\alpha, \beta \in \mathbb{C}$ 分别满足方程 $\alpha^3 - \alpha + 3 = 0$ 与 $\beta^4 - 3\beta + 1 = 0$. 试寻找多项式 $f \in \mathbb{Z}[x]$ 使得 $f(\alpha + \beta) = 0$, 从而 $\alpha + \beta$ 也是代数数.

解. 记 $x := \alpha + \beta$, 则 α, β, x 满足多项式方程组

$$\begin{cases} \alpha^3 - \alpha + 3 = 0 \\ \beta^4 - 3\beta + 1 = 0 \\ x - \alpha - \beta = 0, \end{cases}$$

之后用2.1.2小节的消元法将 α, β 消去, 即可得 x 满足的多项式方程. 易知 $\alpha + \beta$ 的零化多项式 $f(x)$ 可以取为

$$\begin{aligned} f(x) = &\ \mathrm{Res}_\beta\left(\mathrm{Res}_\alpha(\alpha^3 - 3\alpha + 3, x - \alpha - \beta), \beta^4 - 3\beta + 1\right) \\ = &\ -x^{12} + 4x^{10} - 3x^9 - 9x^8 + 36x^7 - 247x^6 \\ &\quad + 126x^5 + 312x^4 - 693x^3 - 251x^2 - 24x - 13. \end{aligned}$$

$\square$

例题 2.17. $\alpha, \beta \in \mathbb{C}$ 同上题, 试寻找多项式 $g \in \mathbb{Z}[x]$ 使得 $g(\alpha\beta) = 0$, 从而 $\alpha\beta$ 也是代数数.

解. 记 $x := \alpha\beta$, 则 α, β, x 满足多项式方程组

$$\begin{cases} \alpha^3 - \alpha + 3 = 0 \\ \beta^4 - 3\beta + 1 = 0 \\ x - \alpha\beta = 0, \end{cases}$$

用结式消去 α, β 即可得到 x 满足的多项式方程. 易知 $x = \alpha\beta$ 的零化多项式 $g(x)$ 可以取为

$$\begin{aligned} g(x) = & \operatorname{Res}_\beta\left(\operatorname{Res}_\alpha(\alpha^3 - 3\alpha + 3, x - \alpha\beta), \beta^4 - 3\beta + 1\right) \\ = & -x^{12} - 27x^9 - 2x^8 - 234x^6 + 9x^5 \\ & + 35x^4 - 729x^3 + 81x - 81. \end{aligned}$$

□

将上述方法推广到一般, 容易证明:

定理 2.18. 设 $\alpha, \beta \in \mathbb{A}$, 则 $\alpha \pm \beta \in \mathbb{A}$, $\alpha\beta \in \mathbb{A}$, 并且当 $\beta \neq 0$ 时还有 $\frac{\alpha}{\beta} \in \mathbb{A}$.

[从而 $\mathbb{A}$ 关于通常的加法与乘法运算构成域, 称为代数数域.]

证明. 用结式消元方法可以直接得到 $\alpha \pm \beta$, $\alpha\beta$, $\frac{\alpha}{\beta}$ 的零化多项式, 请读者自行总结相应的算法. □

2.2 Paillier 加密算法

Paillier 加密算法是一个支持加法同态的公钥密码系统, 由 Paillier 在 1999 年的欧密会 (EUROCRYPT) 上首次提出. 该算法效率较高, 安全性证明完备, 从而具有广泛的实际应用. 本节介绍该算法及其数学原理.

对于正整数 n, 记 $\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$, 则 $\mathbb{Z}_n$ 在通常的加法与乘法运算下构成交换环. $\mathbb{Z}_n^*$ 为 $\mathbb{Z}_n$ 的乘法单位群. 众所周知, 群 $\mathbb{Z}_n^*$ 的阶为 $\phi(n)$, 其中 ϕ 为欧拉 ϕ-函数. 为了更清晰地表述 Paillier 加密算法, 我们需要下列引理作为铺垫:

引理 2.19. 对于正整数 $n \geq 2$, 记

$$\mathcal{S}_n := \left\{ nk+1 \mod n^2 \,\middle|\, k \in \mathbb{Z} \right\} \subseteq \mathbb{Z}_{n^2}^*, \tag{2.57}$$

则 $\mathcal{S}_n$ 是乘法群 $\mathbb{Z}_{n^2}^*$ 的子群, 并且映射

$$L\colon \mathcal{S}_n \to \mathbb{Z}_n, \qquad x \mapsto \frac{x-1}{n} \tag{2.58}$$

是乘法群 $\mathcal{S}_n$ 与加法群 $\mathbb{Z}_n$ 的同构.

引理 2.20. 对于正整数 $n \geq 2$, 则映射

$$\begin{aligned} \mathbb{Z}_n^* &\to \mathbb{Z}_{n^2}^* \\ r &\mapsto r^n \end{aligned} \tag{2.59}$$

良定, 且为乘法群 $\mathbb{Z}_n^*$ 与 $\mathbb{Z}_{n^2}^*$ 的同态.

证明. 都容易验证, 留给读者练习. □

现在开始介绍 Paillier 加密算法. 取定两个不同的素数 p, q, 记

$$n := pq, \tag{2.60}$$

$$\lambda := \text{l.c.m.}(p-1, q-1), \tag{2.61}$$

即 λ 是 $p-1$ 与 $q-1$ 的最小公倍数. 易知 λ 是乘法群 $\mathbb{Z}_n^* \cong \mathbb{Z}_p^* \times \mathbb{Z}_q^*$ 中元素的最大阶数, 从而对任意 $r \in \mathbb{Z}_n^*$, 都有 $r^\lambda \equiv 1 \mod n$. 进而容易验证

$$\forall\, c \in \mathbb{Z}_{n^2}^*, \quad c^\lambda \in \mathcal{S}_n, \tag{2.62}$$

其中乘法群 $\mathcal{S}_n$ 的定义见(2.57).

定义 2.21. 沿用上文记号, 对于 $g \in \mathbb{Z}_{n^2}^*$, 如果 $L(g^\lambda) \in \mathbb{Z}_n^*$, 其中群同构 L 的定义见(2.58)式, 则称 g 为 n 的一个 ***Paillier* 生成元**, 此时记 $L(g^\lambda)$ 的乘法逆元

$$\mu := L(g^\lambda)^{-1} \in \mathbb{Z}_n^*. \tag{2.63}$$

实际应用中, Paillier 生成元可以按下述方式选取:

例题 **2.22.**(快速密钥). 记号承上, 如果 n 与 $\phi(n) = (p-1)(q-1)$ 互素, 则 $g := n+1$ 是 n 的一个 Paillier 生成元.

证明. 这是因为, 若 $g \equiv n+1 \mod n^2$, 则二项式定理展开易得

$$g^\lambda \equiv (n+1)^\lambda \equiv 1 + n\lambda \mod n^2,$$

从而 $L(g^\lambda) \equiv \lambda \mod n$. 由初等数论易验证在题设条件下 λ 与 n 互素, 故 $L(g^\lambda) \in \mathbb{Z}_n^*$, 从而 g 为 n 的一个 Paillier 生成元. □

Paillier 加密算法的基本资料如下:

给定 $n = pq$, 取定 Paillier 生成元 $g \in \mathbb{Z}_{n^2}^*$, 记

- **明文空间**: $\{0, 1, 2, ..., n-1\} \subseteq \mathbb{Z}$.
- **密文空间**: $\mathbb{Z}_{n^2}^*$.
- **公钥**: (n, g).
- **私钥**: (λ, μ).

其中 λ, μ 的定义见(2.61),(2.63)式.

定义**加密映射** $\mathscr{E}$ 与**解密映射** $\mathscr{D}$ 如下:

$$\begin{aligned} \mathscr{E}\colon \mathbb{Z} \times \mathbb{Z}_n^* &\to \mathbb{Z}_{n^2}^* \\ (m, r) &\mapsto g^m \cdot r^n, \end{aligned} \tag{2.64}$$

$$\begin{aligned} \mathscr{D}\colon \mathbb{Z}_{n^2}^* &\to \mathbb{Z}_n \\ c &\mapsto \mu \cdot L(c^\lambda). \end{aligned} \tag{2.65}$$

映射 $\mathscr{E}$ 与 $\mathscr{D}$ 的良定性分别由引理2.20与(2.62)式所保证. 显然 $\mathscr{E}$ 与 $\mathscr{D}$ 都是群同态.

Paillier 算法加密, 解密的原理如下:

性质 2.23. *记号同上, 则有如下群同态交换图:*

$$\begin{tikzcd} \mathbb{Z} \times \mathbb{Z}_n^* \arrow[r, "\mathscr{E}"] \arrow[dr, "\pi"'] & \mathbb{Z}_{n^2}^* \arrow[d, "\mathscr{D}"] \\ & \mathbb{Z}_n \end{tikzcd} , \tag{2.66}$$

其中投影映射 $\pi\colon (m, r) \mapsto m \mod n$.

证明. 对任意 $m \in \mathbb{Z}$ 以及 $r \in \mathbb{Z}_n^*$, 我们有

$$\begin{aligned}
\mathscr{D}(\mathscr{E}(m,r)) &= \mathscr{D}\left(g^m \cdot r^n\right) = \mu \cdot L\left((g^m \cdot r^n)^\lambda\right) \\
&= \mu \cdot L\left((g^\lambda)^m \cdot (r^\lambda)^n\right) \\
&= \mu \cdot L\left((g^\lambda)^m\right) && (\text{注意 } r^\lambda \equiv 1 \mod n) \\
&= \mu \cdot mL(g^\lambda) && (\text{注意 } L \text{ 是群同态}) \\
&= m \mod n, && (\text{由 } \mu \text{ 的定义})
\end{aligned}$$

从而得证. □

综上所述, 我们将 Paillier 加密算法总结如下:

算法 2.24. *(Paillier 加密算法) 给定公钥 (n, g) 与私钥 (λ, μ).*

- **加密:** *对于明文 $m \in \{0, 1, 2, ..., n-1\} \subseteq \mathbb{Z}$, 随机选取 $r \in \mathbb{Z}_n^*$, 得到密文 $c = \mathscr{E}(m, r)$.*
- **解密:** *对于密文 $c \in \mathbb{Z}_{n^2}^*$, 则 $\mathscr{D}(c)$ 为明文所在的模 n 剩余类.*

注记 **2.25.** Paillier 加密算法的安全性:

1. 私钥 (λ, μ) 的私密性依赖于大素因数分解的困难性.
2. 关于暴力破解: 若密文 c 所对应的明文为 m, 则 $cg^{-m} \in \mathbb{Z}_{n^2}^*$ 是 n 次剩余 (即为 $\mathbb{Z}_{n^2}^*$ 中的某个元素的 n 次幂); 而对于合数 n, 判断 $\mathbb{Z}_{n^2}^*$ 中的元素是否为 n 次剩余是非常困难的, 目前为止没有多项式时间的算法可以攻破.

3. 初等概率论

3.1 重积分与几何概型

3.1.1 线段长度的期望

考虑如下问题:

习题 **3.1.** 在边长为 1 的正方形内独立、随机取两个点 A, B, 求线段 AB 长度的期望.

不妨该正方形区域为 $[0,1]^2 = \{(x,y) \mid x, y \in [0,1]\}$, 记点 A, B 的坐标分别是 $(x_1, y_1), (x_2, y_2)$, 则 x_1, x_2, y_1, y_2 是相互独立的随机变量, 且都服从 $[0,1]$ 上的均匀分布. 注意线段 AB 的长度 L 满足

$$L = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2},$$

从而直接计算得

$$\begin{aligned}
\mathbb{E}[L] &= \int_{[0,1]^4} \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}\, \mathrm{d}x_1 \mathrm{d}x_2 \mathrm{d}y_1 \mathrm{d}y_2 \\
&= 4 \int_{[0,1]^2} \sqrt{u^2 + v^2}\, \mathrm{d}u \mathrm{d}v \int_0^{1-u} \mathrm{d}x_1 \int_0^{1-v} \mathrm{d}y_1 \\
&\qquad (\text{换元 } u := x_2 - x_1, v := y_2 - y_1, \text{并用对称性、调整积分次序}) \\
&= 4 \int_0^1 (1-u)\, \mathrm{d}u \int_0^1 (1-v) \sqrt{u^2 + v^2}\, \mathrm{d}v \\
&= 4 \int_0^1 (1-u) \left(\frac{\sqrt{1+u^2}}{6} - \frac{u^2\sqrt{1+u^2}}{3} + \frac{u^3}{3} + \frac{u^2}{2} \ln \frac{1+\sqrt{1+u^2}}{u} \right) \mathrm{d}u \\
&= \frac{2+\sqrt{2}}{15} + \frac{\ln(1+\sqrt{2})}{3} \approx 0.521045.
\end{aligned}$$

上述计算的中间过程较复杂, 留给读者练习.

3.1.2 高维球的体积

杨昊同学提供了一道好玩的题目:

习题 **3.2.** 曲豆豆扔飞镖. 假设曲豆豆扔出的飞镖总是落在平面上某个边长为 2 的正方形区域 $S=[-1,1]^2$ 中, 飞镖落点在 S 中均匀分布, 且各次扔飞镖的落点相互独立. 考虑如下游戏: 首先记 C_1 为以正方形区域 S 的中心 O 为圆心, 半径为 1 的圆.

- 曲豆豆第 1 次扔飞镖, 记飞镖落点为 P_1.
- 如果 P_1 在圆 C_1 外部, 则游戏结束; 否则过点 P_1 作线段 OP_1 的垂线 ℓ_1, 并以 O 为圆心, 以直线 ℓ_1 截圆 C_1 的弦长的一半为半径作圆, 该圆记作 C_2, 然后游戏继续, 曲豆豆准备第 2 次扔飞镖.
- 一般地, 当曲豆豆第 n 次扔飞镖时, 记飞镖落点为 P_n.
- 如果 P_n 在圆 C_n 外部, 则游戏结束; 否则过点 P_n 作线段 OP_n 的垂线 ℓ_n, 并以 O 为圆心, 以直线 ℓ_n 截圆 C_n 的弦长的一半为半径作圆, 该圆记作 C_{n+1}, 然后游戏继续, 曲豆豆准备第 $(n+1)$ 次扔飞镖.

当游戏结束时, 记 N 为曲豆豆扔飞镖的总次数, 求 N 的分布列与期望.

在正式计算求解之前, 先交代更多的记号. 记圆 C_n 的半径为 R_n, 落点 P_n 的坐标为 (x_n,y_n), 其中 x_n,y_n 视为随机变量, 它们相互独立且服从 $[-1,1]$ 上的均匀分布. 容易验证 $\{R_n\}$ 满足如下递推关系:

$$R_1=1,\qquad R_{n+1}=\sqrt{R_n^2-x_n^2-y_n^2}\quad(n\geq 1). \tag{3.1}$$

这个 R_n 可以称为“容许半径”: 只有当第 n 个飞镖落在半径 R_n 范围内时, 游戏才能继续. 注意随着投掷次数 n 的增大, R_n 在不断地变小, 从

而游戏越来越难以继续; 如果飞镖落点离中心点 O 越近, 则 $\{R_n\}$ 减小得越慢; 曲豆豆为了能多玩几局这种飞镖, 应当每次都尽可能让飞镖落点接近中心点 O.

解. 记号承上, 对于每个正整数 n, 先计算 $\mathbb{P}(N \geq n)$, 即曲豆豆至少扔了 n 次飞镖的概率. 注意曲豆豆一开始总是会扔 1 次, 从而 $\mathbb{P}(N \geq 1) = 1$. 而当 $n \geq 2$ 时, 由递推关系(3.1)易知, $N \geq n$ 当且仅当

$$x_1^2 + y_1^2 + x_2^2 + y_2^2 + \cdots + x_{n-1}^2 + y_{n-1}^2 < 1.$$

(即, 只有当前 $(n-1)$ 次表现 "都挺好" 时, 曲豆豆才能有机会扔第 n 次). 于是

$$\begin{aligned}
\mathbb{P}(N \geq n) &= \frac{\int_{x_1^2+y_1^2+\cdots+x_{n-1}^2+y_{n-1}^2<1} \mathrm{d}x_1 \mathrm{d}y_1 \cdots \mathrm{d}x_{n-1} \mathrm{d}y_{n-1}}{\int_{[-1,1]^{n-1}} \mathrm{d}x_1 \mathrm{d}y_1 \cdots \mathrm{d}x_{n-1} \mathrm{d}y_{n-1}} \\
&= \frac{1}{4^{n-1}} \int_{x_1^2+y_1^2+\cdots+x_{n-1}^2+y_{n-1}^2<1} \mathrm{d}x_1 \mathrm{d}y_1 \cdots \mathrm{d}x_{n-1} \mathrm{d}y_{n-1}.
\end{aligned}$$

从而对于 $n \geq 1$,

$$\mathbb{P}(N \geq n+1) = \frac{1}{4^n} \int_{x_1^2+y_1^2+\cdots+x_n^2+y_n^2<1} \mathrm{d}x_1 \mathrm{d}y_1 \cdots \mathrm{d}x_n \mathrm{d}y_n = \frac{1}{4^n} \mathrm{Vol}(\mathbb{B}^{2n}),$$

其中 $\mathbb{B}^{2n}$ 是 $2n$ 维欧氏空间 $\mathbb{R}^{2n}$ 中的单位球, $\mathrm{Vol}(\mathbb{B}^{2n})$ 为该球的体积. 虽然高维球体体积公式众所周知, 但高中生一般来说可能没有听说过. 不如在此重新推导一遍, 这里只需要考虑偶数维球体的情形.

$$\begin{aligned}
\mathrm{Vol}(\mathbb{B}^{2n}) &= \int_{x_1^2+y_1^2+\cdots+x_n^2+y_n^2<1} \mathrm{d}x_1 \mathrm{d}y_1 \cdots \mathrm{d}x_n \mathrm{d}y_n \\
&= \int_{x_n^2+y_n^2<1} \mathrm{d}x_n \mathrm{d}y_n \\
&\quad \times \int_{x_1^2+y_1^2+\cdots+x_{n-1}^2+y_{n-1}^2<1-x_n^2-y_n^2} \mathrm{d}x_1 \mathrm{d}y_1 \cdots \mathrm{d}x_{n-1} \mathrm{d}y_{n-1}
\end{aligned}$$

$$
\begin{aligned}
&= \int_{x_n^2+y_n^2<1} (1-x_n^2-y_n^2)^{n-1}\mathrm{Vol}(\mathbb{B}^{2n-2})\mathrm{d}x_n\mathrm{d}y_n \\
&= \mathrm{Vol}(\mathbb{B}^{2n-2}) \cdot \int_0^{2\pi} \mathrm{d}\theta \int_0^1 r(1-r^2)^{n-1}\mathrm{d}r \\
&= \frac{\pi}{n}\mathrm{Vol}(\mathbb{B}^{2n-2}).
\end{aligned}
$$

再注意首项 $\mathrm{Vol}(\mathbb{B}^2) = \pi$, 从而易知

$$
\mathrm{Vol}(\mathbb{B}^{2n}) = \frac{\pi^n}{n!},
$$

此乃 $2n$ 维单位球体的体积公式. 因此曲豆豆至少扔 $n+1$ 次飞镖的概率 $\mathbb{P}(N \geq n+1) = \frac{(\pi/4)^n}{n!}$, 进而随机变量 N 的分布列如下: 对于 $n \geq 1$,

$$
\mathbb{P}(N=n) = \mathbb{P}(N \geq n) - \mathbb{P}(N \geq n+1) = \frac{(\pi/4)^{n-1}}{(n-1)!} - \frac{(\pi/4)^n}{n!}.
$$

通过上述分布列直接计算可知, N 的期望

$$
\begin{aligned}
\mathbb{E}[N] = \sum_{n=1}^{\infty} n\mathbb{P}(N=n) &= \sum_{n=1}^{\infty} \left(\frac{nx^{n-1}}{(n-1)!} - \frac{nx^n}{n!}\right)\Bigg|_{x=\frac{\pi}{4}} \\
&= \left(\frac{\mathrm{d}}{\mathrm{d}x}(x\mathrm{e}^x) - x\mathrm{e}^x\right)\Bigg|_{x=\frac{\pi}{4}} = \mathrm{e}^{\frac{\pi}{4}}.
\end{aligned}
$$

□

注记 3.3. 注意上题中的概率 $\mathbb{P}(N \geq n+1) = \frac{1}{4^n}\mathrm{Vol}(\mathbb{B}^{2n})$ 其实是 $2n$ 维单位球的体积与该球的 “外切立方体” 的体积之比. 该比值为 $\frac{(\pi/4)^n}{n!}$, 随 n 的增大而迅速趋于零.

接下来考虑此题的一个变种.

变式 3.4. 游戏规则与例题3.2完全相同, 但是曲豆豆经过一段时间练习, 镖法更精准, 飞镖的落点不再是在正方形区域 $S = [-1,1]^2$ 均匀分布了,

而是在正方形 S 的内切圆 C_1 内均匀分布. 记 N 为曲豆豆扔飞镖的总次数, 求 N 的分布列与期望.

注意此时的曲豆豆第一次扔飞镖时一定把飞镖扔进圆 C_1 内, 从而游戏一定会继续, $\mathbb{P}(N \geq 2) = 1$. 此外曲豆豆的飞镖落点比之前更倾向于接近圆心, 从而游戏持续轮数应该会比之前更多.

解. 记号与方法类似, 易知对任意 $n \geq 1$,

$$\mathbb{P}(N \geq n+1) = \frac{\mathrm{Vol}(\mathbb{B}^{2n})}{\mathrm{Vol}(\mathbb{B}^2)^n} = \frac{\pi^n/n!}{\pi^n} = \frac{1}{n!},$$

从而 $\mathbb{P}(N = n) = \frac{1}{(n-1)!} - \frac{1}{n!}\,(n \geq 1)$, 且

$$\begin{aligned}\mathbb{E}[N] &= \sum_{n=1}^{\infty} n\mathbb{P}(N=n) = \sum_{n=1}^{\infty} n\left(\frac{1}{(n-1)!} - \frac{1}{n!}\right) \\ &= \sum_{n=0}^{\infty}\frac{n+1}{n!} - \sum_{n=1}^{\infty}\frac{n}{n!} = \sum_{n=0}^{\infty}\frac{1}{n!} = \mathrm{e}.\end{aligned}$$

□

3.2 De Moivre-Laplace 定理与正态分布

将二项分布取某种极限可得到所谓**正态分布**, 这是一个十分重要的概率分布, 这里介绍其推导过程. 记 $X_1, X_2, X_3, \ldots$ 是一列独立同分布的随机变量, 且服从参数为 p 的两点分布: $\mathbb{P}(X_k = 1) = p$, $\mathbb{P}(X_k = 0) = q$, 其中 $p \in (0,1)$, $q = 1-p$. 则众所周知, 对每个正整数 n, 随机变量

$$S_n := X_1 + X_2 + \cdots + X_n$$

服从参数为 n, p 的二项分布, 即 $\mathbb{P}(S_n = k) = \binom{n}{k}p^k q^{n-k}$. 而二项分布的期望与方差为

$$\mathbb{E}[S_n] = np, \qquad \mathrm{Var}(S_n) = npq.$$

适当将 S_n 作伸缩、平移变换, 引入随机变量

$$Z_n := \frac{S_n - np}{\sqrt{npq}}, \tag{3.2}$$

则 Z_n 的期望与方差分别为 $0, 1$. 事实上, 当 $n \to +\infty$ 时, 上述随机变量 Z_n 将趋近于标准正态分布, 见如下定理:

定理 3.5. (De Moivre-Laplace). 记号承上, 则对任意实数 $\alpha < \beta$ 都成立

$$\lim_{n\to\infty} \mathbb{P}(\alpha < Z_n \leq \beta) = \frac{1}{\sqrt{2\pi}} \int_\alpha^\beta \mathrm{e}^{-\frac{x^2}{2}} \mathrm{d}x, \tag{3.3}$$

从而随机变量 $\{Z_n\}$ 依分布收敛于标准正态分布 $\Phi(x) = \frac{1}{\sqrt{2\pi}}\mathrm{e}^{-\frac{x^2}{2}}$.

证明. 直接计算得

$$\begin{aligned} \mathbb{P}(\alpha < Z_n \leq \beta) &= \mathbb{P}\left(\alpha\sqrt{npq} + np < S_n \leq \beta\sqrt{npq} + np\right) \\ &= \sum_{k \in I_{n;\alpha,\beta}} \mathbb{P}(S_n = k), \end{aligned} \tag{3.4}$$

其中

$$I_{n;\alpha,\beta} := (\alpha\sqrt{npq} + np, \beta\sqrt{npq} + np] \cap \mathbb{Z}.$$

对于每个 $k \in I_{n;\alpha,\beta}$, 记 $x := \frac{k-np}{\sqrt{npq}}$, 则 $x \in (\alpha, \beta]$. 注意 x 不仅与 k 有关, 而且与 n 有关. 易知

$$\begin{aligned} k &= np + x\sqrt{npq}, \\ n - k &= nq - x\sqrt{npq}, \end{aligned} \tag{3.5}$$

从而当 $n \to +\infty$ 时, k 与 $(n-k)$ 也趋于无穷 (关于 $x \in (\alpha, \beta]$ 一致). 从而对 $n, k, (n-k)$ 使用 **Stirling 公式**

$$n! = \sqrt{2\pi n}\left(\frac{n}{\mathrm{e}}\right)^n (1 + o(1)), \quad n \to \infty$$

可知当 $n \to \infty$ 时

$$\begin{aligned}\mathbb{P}(S_n = k) &= \frac{n!}{k!(n-k)!} p^k q^{n-k} \\ &= \left(\frac{n}{2\pi k(n-k)}\right)^{\frac{1}{2}} \left(\frac{np}{k}\right)^k \left(\frac{nq}{n-k}\right)^{n-k} (1+o(1)).\end{aligned} \tag{3.6}$$

而由(3.5)式, 可知当 $n \to \infty$ 时

$$\begin{aligned}\frac{n}{2\pi k(n-k)} &= \frac{n}{2\pi \left(np + x\sqrt{npq}\right)\left(nq - x\sqrt{npq}\right)} \\ &= \frac{1}{2\pi npq}(1+o(1)).\end{aligned} \tag{3.7}$$

然后再注意到

$$\begin{aligned}&\ln\left[\left(\frac{np}{k}\right)^k \left(\frac{nq}{n-k}\right)^{n-k}\right] \\ &= -\left(np + x\sqrt{pq}\cdot n^{\frac{1}{2}}\right) \ln\left(1 + x\sqrt{\frac{q}{p}}\cdot n^{-\frac{1}{2}}\right) \\ &\qquad - \left(nq - x\sqrt{pq}\cdot n^{\frac{1}{2}}\right) \ln\left(1 - x\sqrt{\frac{p}{q}}\cdot n^{-\frac{1}{2}}\right) \\ &= -\left(np + x\sqrt{pq}\cdot n^{\frac{1}{2}}\right)\left(x\sqrt{\frac{q}{p}}\cdot n^{-\frac{1}{2}} - \frac{qx^2}{2p}\cdot\frac{1}{n} + o(\frac{1}{n})\right) \\ &\qquad - \left(nq - x\sqrt{pq}\cdot n^{\frac{1}{2}}\right)\left(-x\sqrt{\frac{p}{q}}\cdot n^{-\frac{1}{2}} - \frac{px^2}{2q}\cdot\frac{1}{n} + o(\frac{1}{n})\right) \\ &= \left(-x\sqrt{pq}\cdot n^{\frac{1}{2}} - \frac{1}{2}qx^2 + o(1)\right) + \left(x\sqrt{pq}\cdot n^{\frac{1}{2}} - \frac{1}{2}px^2 + o(1)\right) \\ &= -\frac{1}{2}x^2 + o(1),\end{aligned}$$

从而当 $n \to \infty$ 时,

$$\left(\frac{np}{k}\right)^k \left(\frac{nq}{n-k}\right)^{n-k} = \mathrm{e}^{-\frac{1}{2}x^2}(1+o(1)). \tag{3.8}$$

将(3.7)(3.8)式代入(3.6)可知当 $n \to \infty$ 时

$$\mathbb{P}(S_n = k) = \frac{1}{\sqrt{2\pi npq}} \mathrm{e}^{-\frac{1}{2}x^2}(1 + o(1))$$

关于 $x \in (\alpha, \beta]$ 一致. 因此

$$\begin{aligned}
&\lim_{n\to\infty} \mathbb{P}(\alpha < Z_n \le \beta) = \lim_{n\to\infty} \sum_{k \in I_{n;\alpha,\beta}} \mathbb{P}(S_n = k) \\
= &\lim_{n\to\infty} \sum_{x \in (\alpha,\beta] \cap \frac{1}{\sqrt{npq}}\mathbb{Z}} \frac{1}{\sqrt{2\pi npq}} \mathrm{e}^{-\frac{x^2}{2}}(1 + o(1)) = \frac{1}{\sqrt{2\pi}} \int_\alpha^\beta \mathrm{e}^{-\frac{x^2}{2}} \mathrm{d}x.
\end{aligned}$$

□

3.3 两正整数互素的概率

考虑如下“问题”:

独立地随机取两个正整数, 取到的两个数互素的概率是多少?

然而, “随机取正整数”的操作在概率论中不可能实现. 这是因为, 如果每个正整数 k 都能取到, 并且被取到的概率都相等, 都为 $r > 0$, 则概率的可数可加性导致

$$1 = \sum_{k=1}^{\infty} \mathbb{P}(\text{取到 } k) = \sum_{k=1}^{\infty} r = +\infty,$$

矛盾. 不过, 此“问题”的下述“伪解”具有启发性:

伪解. 设所有素数从小到大依次是

$$p_1 < p_2 < p_3 < \cdots. \tag{3.9}$$

现在设 a,b 是随机选取的正整数. 如果 a,b 互素, 那么对任意 k, p_k 不是 a,b 的公因数. 由于 a 随机选取, 所以 a 模 p_k 的余数服从 $\{0,1,2,...,p_k-1\}$ 上的均匀分布, 特别地, a 能被 p_k 整除的概率为 $\frac{1}{p_k}$. 同样, b 能被 p_k 整除的概率也是 $\frac{1}{p_k}$. 再注意 a,b 相互独立, 因此

$$\mathbb{P}(p_k\text{ 不是 }a,b\text{ 的公因数}) = 1-\frac{1}{p_k^2},$$

于是

$$\mathbb{P}(a,b\text{互素}) = \prod_{k=1}^{\infty}\left(1-\frac{1}{p_k^2}\right).$$

最后, 再由众所周知的恒等式

$$\begin{aligned}\prod_{k=1}^{\infty}\left(1-\frac{1}{p_k^2}\right) &= \left(\prod_{k=1}^{\infty}(1+\frac{1}{p_k^2}+\frac{1}{p_k^4}+\cdots)\right)^{-1} \\ &= \left(\sum_{n=1}^{\infty}\frac{1}{n^2}\right)^{-1} = \frac{6}{\pi^2}\end{aligned} \tag{3.10}$$

可知 a,b 互素的概率是 $\frac{6}{\pi^2}$. □

当然不会仅仅到此为止. 我们希望将此问题的表述以及解答过程严格化, 使之成为真正的数学. 关键在于修改 "随机取正整数" 的说法. 为此, 我们退而求其次, 先固定一个正整数 n, 在集合

$$[n] := \{1,2,3,...,n\} \tag{3.11}$$

中随机取元素, 使得取到每个元素的概率都是 $\frac{1}{n}$; 则

$$\mathbb{P}_n := \frac{\#\{(a,b)\in[n]^2 \mid \mathrm{gcd}(a,b)=1\}}{n^2}$$

是事件 "在 $[n]$ 中有放回地依次抽取两个数 a,b, 使得 a,b 互素" 的概率. 这里的 $\#X$ 是指有限集合 X 的元素个数. 然后考虑 $\mathbb{P}_n$ 在 $n\to+\infty$ 时的极限, 将 "随机取两正整数, 取到的两个数互素" 的概率解释为 $\lim\limits_{n\to+\infty}\mathbb{P}_n$.

定理 3.6. 以下等式成立:

$$\lim_{n\to+\infty}\frac{\#\{(a,b)\in[n]^2\,|\,\mathrm{gcd}(a,b)=1\}}{n^2}=\frac{6}{\pi^2}. \tag{3.12}$$

证明. 沿用(3.9)式的记号. 对每个正整数 k, 中国剩余定理

$$\mathbb{Z}/(p_1p_2\cdots p_k\mathbb{Z})\cong(\mathbb{Z}/p_1\mathbb{Z})\times(\mathbb{Z}/p_2\mathbb{Z})\times\cdots\times(\mathbb{Z}/p_k\mathbb{Z})$$

表明, 从 $[p_1p_2\cdots p_k]$ 中任取正整数 a, 将 a 模 p_i,p_j $(i\neq j)$ 的余数分别视为两个随机变量, 则这两个随机变量独立.

一方面, 任意取定正整数 $k, M_0\in\mathbb{N}^*$, 记 $n_k:=p_1p_2\cdots p_k$. 对任意 $n>M_0n_k$, 考虑带余除法

$$n=Mn_k+r_k, \tag{3.13}$$

其中正整数 $M\geq M_0$, 余数 $0<r_k<n_k$, 则

$$\begin{aligned}
&\#\left\{(a,b)\in[n]^2\,\middle|\,\mathrm{gcd}(a,b)=1\right\}\\
\geq&\#\left\{(a,b)\in[Mn_k]^2\,\middle|\,\mathrm{gcd}(a,b)=1\right\}\\
\geq&\#\left\{(a,b)\in[Mn_k]^2\,\middle|\,\forall i=1,...,k,\ p_i\nmid\mathrm{gcd}(a,b)\right\}\\
&\quad-\sum_{m\geq k+1}\#\left\{(a,b)\in[Mn_k]^2\,\middle|\,p_m|a\text{ 且 }p_m|b\right\}\\
=&(Mn_k)^2\prod_{i=1}^{k}\left(1-\frac{1}{p_i^2}\right)-\sum_{m\geq k+1}\lfloor\frac{Mn_k}{p_m}\rfloor^2
\end{aligned}$$

$$\geq (Mn_k)^2 \left(\prod_{i=1}^{k} \left(1 - \frac{1}{p_i^2}\right) - \sum_{m \geq k+1} \frac{1}{p_m^2} \right).$$

所以

$$\begin{aligned}
\mathbb{P}_n &= \frac{\#\{(a,b) \in [n]^2 \mid \mathrm{gcd}(a,b) = 1\}}{n^2} \\
&\geq \left(\prod_{i=1}^{k} \left(1 - \frac{1}{p_i^2}\right) - \sum_{m \geq k+1} \frac{1}{p_m^2} \right) \left(\frac{Mn_k}{n}\right)^2 \\
&\geq \left(\prod_{i=1}^{k} \left(1 - \frac{1}{p_i^2}\right) - \sum_{m \geq k+1} \frac{1}{p_m^2} \right) \left(1 - \frac{1}{M_0 + 1}\right)^2.
\end{aligned}$$

令 $n \to +\infty$, 可知对任意正整数 k, M_0 都成立

$$\liminf_{n \to +\infty} \mathbb{P}_n \geq \left(\prod_{i=1}^{k} \left(1 - \frac{1}{p_i^2}\right) - \sum_{m \geq k+1} \frac{1}{p_m^2} \right) \left(1 - \frac{1}{M_0 + 1}\right)^2,$$

再依次令 $M_0 \to +\infty, k \to +\infty$, 可得

$$\liminf_{n \to +\infty} \mathbb{P}_n \geq \prod_{i=1}^{\infty} \left(1 - \frac{1}{p_i^2}\right) = \frac{6}{\pi^2}.$$

另一方面, 当 $n > M_0 n_k$ 时, 沿用(3.13)式, 有

$$\begin{aligned}
&\# \left\{(a,b) \in [n]^2 \,\middle|\, \mathrm{gcd}(a,b) = 1\right\} \\
\leq &\# \left\{(a,b) \in [n]^2 \,\middle|\, \forall i = 1, ..., k,\ p_i \nmid \mathrm{gcd}(a,b)\right\} \\
\leq &\# \left\{(a,b) \in [Mn_k]^2 \,\middle|\, \forall i = 1, ..., k,\ p_i \nmid \mathrm{gcd}(a,b)\right\} + \left(n^2 - (Mn_k)^2\right) \\
\leq & n^2 \prod_{i=1}^{k} \left(1 - \frac{1}{p_i^2}\right) + \frac{2n^2}{M_0},
\end{aligned}$$

令 $n \to +\infty$, 可知对任意正整数 k, M_0 都有

$$\limsup_{n\to+\infty} \mathbb{P}_n \leq \prod_{i=1}^{k}\left(1-\frac{1}{p_i^2}\right)+\frac{2}{M_0},$$

再依次令 $M_0 \to +\infty, k \to +\infty$, 可得

$$\limsup_{n\to+\infty} \mathbb{P}_n \leq \prod_{i=1}^{\infty}\left(1-\frac{1}{p_i^2}\right)=\frac{6}{\pi^2}.$$

综上可得 $\lim\limits_{n\to+\infty} \mathbb{P}_n = \frac{6}{\pi^2}$, 得证. □

3.4 财务管理: Miller-Orr 模型

3.4.1 引言

笔者的一个女性朋友最近在备考注册会计师 CPA, 她在学习的过程中遇到了一个看上去很复杂的所谓 "**现金返回线公式**", 这个公式在国内的会计应试辅导书里通常长这个妖冶邪异的样子:

$$R = \sqrt[3]{\frac{3b\delta^2}{4i}} + L. \tag{3.14}$$

按道理说, 财务会计那些东西也就是加减乘除, 但这公式里居然出现三次根号 $\sqrt[3]{\ }$, 这确实有些诡异, 其中必有魔法. 那位女性朋友被这个三次根号 $\sqrt[3]{\ }$ 吓到之后就找到笔者, 想听听笔者的见解.

笔者虽然是数学专业, 但额外技能点全都加到了**物理** (以及**卖萌**) 上, 对财务、会计、金融那些东西一窍不通, 更是听不懂她满嘴的财务术语. 可是笔者对公式中的三次根号 $\sqrt[3]{\ }$ 突然产生了强烈的好奇, 并认为这或许是破除笔者对财务会计类专业 "也就会加减乘除" 的偏见的绝佳机会, 于是笔者决定查阅相关资料, 企图搞清楚这个公式.

首先, 百度查不出任何有营养的信息; 而通过查阅知乎, 笔者得知这是财务管理的 "**Miller-Orr 模型**". 但关于 Miller-Orr 模型的详细推导, 尤其是为什么会出现三次根号 $\sqrt[3]{\ }$, 笔者在中文互联网上查不到任何有价值的免费公开资料 (或许是因为笔者的中文资料查阅能力、中文阅读理解能力有限). 于是笔者只好去墙外某著名学术平台反复查阅, 直到找到原始文献

> Miller M H, Orr D. *A model of the demand for money by firms* [J]. The Quarterly journal of economics, 1966, 80(3): 413-435.

果然, 那妖冶邪异的公式还真就是从这文章里冒出来的.

以下是笔者在阅读原始文献的基础上对这个所谓 "Miller-Orr 模型" 所产生的一些个人理解 (在数学细节处理方面与原文略有出入). 但由于笔者完全不熟悉财务会计专业知识, 在有关专业术语的表达方面可能会显得十分幼稚且业余, 甚至会不小心夹杂粗鄙之语.

3.4.2 故事背景

公式并不是从天而降的, 它一定有故事背景. 事实上, 故事可以是这样的: 有一个 "油泰" 商人曲豆豆, 他开了一家投机倒把的金融公司. 这家油泰公司大概是这样运作的:

1. 公司的资产分为两部分: **证券**与**现金**. 前者可以粗俗地认为是银行存款或者别的什么投资, 可以 "钱生钱、利滚利"; 而后者就是手里的现金.

2. 证券与现金这两类资产可以相互转换. 可以在任意时刻将任意数量的证券卖出换成现金, 或者在任意时刻用任意数量的现金来买证券; 无论是用现金买证券还是卖证券得现金, 每一次**交易**都是瞬间完成.

3. 证券类资产收益稳定, 单位时间的利率 (例如, 日利率) 始终为 ν.

4. 投机倒把的油泰商人曲豆豆当然更喜欢证券资产, 毕竟有利息可以赚. 逐利的曲豆豆认为吃利息是理所当然的, 而没有吃到利息就是亏了; 故持有现金越多, 曲豆豆感觉亏得就越多——这就是所谓**机会成本**. 假设公司有现金资产 W, 如果这些现金都换成证券, 那单位时间就能收获 νW 的利息; 而曲豆豆实际上并没有吃到这想象中 νW 的利息. 换言之, 单位时间的机会成本为 νW.

5. 证券与现金的转换过程中会产生**交易成本**: 每一次交易 (无论是买证券还是卖证券) 都要花费 γ 元的手续费. 注意这里的 γ 是常数, 与每次交易的数额无关.

6. 由于频繁投机倒把, 公司的现金总量 $W(t)$ 每时每刻都随时间 t 变化: 若 t 时刻的现金数量为 $W(t)$, 则经过一段微小的时间 Δt 之后, 现金数量有 $\frac{1}{2}$ 的概率增加 ΔW, 有 $\frac{1}{2}$ 的概率减少 ΔW, 其中 ΔW 是与 Δt 有关的常数. 可见, $t+\Delta t$ 时刻的现金数量是服从两点分布的随机变量. 再假设该随机变量的**方差**与 Δt 成正比, 即

$$\mathrm{Var}(W(t+\Delta t)) = \sigma^2 \Delta t,$$

其中 $\sigma > 0$ 为常数, 表示现金单位时间变化的**标准差**. 容易验证上式等价于

$$\Delta W = \sqrt{\sigma^2 \Delta t}. \tag{3.15}$$

也就是说, 现金数量 $W(t)$ 可以先近似为离散时间 Δt 的对称随机游走. 众所周知, 这个随机过程在 $\Delta t \to 0$ 时会趋于**布朗运动** (也叫 **Wiener 过程**): 若 $t=0$ 时刻的现金数量为 x, 则 t 时刻现金数量 $W(t)$ 的概率密度函数为

$$f_{W(t)}(y) = \frac{1}{\sqrt{2\pi\sigma^2 t}} \mathrm{e}^{-\frac{(y-x)^2}{2\sigma^2 t}}.$$

事实上, 布朗运动才是描述现金数量随机变化的真正数学模型; 而我们在接下来的数学处理中, 采取离散时间对称随机游走来逼近布朗运动.

作为这家油泰公司的高层, 曲豆豆需要管理公司的现金资产:

- 现金资产不能太多, 否则会增加**机会成本**.
- 现金资产绝对不能低于某个下限, 否则公司有倒闭的危险. 这里不妨假定**现金资产的下限**为 0, 换言之, 曲豆豆必须保证现金资产始终大于 0.
- 所以, 一个朴素的想法是, 当现金资产很多的时候, 曲豆豆就应该用适量的现金来购买证券; 而当现金资产为 0 时, 曲豆豆就要立刻卖掉一些证券.
- 但是买卖证券也不能太过频繁, 否则会增加**交易成本**.
- 总之, 曲豆豆需要综合考虑机会成本与交易成本, 设计一个最优的现金资产管理方案, 使单位时间内的现金管理总成本最小化.

3.4.3 数学模型建立

按某些商业习俗, 这家油泰公司采用如下的现金资产管理方案:

1. 取定实数
$$0 < r < h, \tag{3.16}$$
其中 h 被称为**现金资产的上限**, 而 r 被称为**现金返回线**.

2. 记该公司在 t 时刻的现金资产为 $W(t)$,

(a) 如果 $0 < W(t) < h$, 则曲豆豆不做任何买卖证券操作, 任由 $W(t)$ 随机变化;

(b) 如果 $W(t) \geq h$, 则曲豆豆立刻买入证券, 使得买入证券后的现金资产为 r;

(c) 如果 $W(t) \leq 0$, 则曲豆豆立刻卖出证券, 使得卖出证券后的现金资产为 r.

3. 在曲豆豆的上述买卖证券操作的干预下, t 时刻的现金资产 $W(t)$ 是随机变量, 其取值范围始终被限制在 $[0, h]$. 随机变量族 $\{W(t)\}_{t\geq 0}$ 构成一个随机过程, 它是布朗运动的某个变种.

我们考察在上述管理策略下的单位时间内的现金管理总成本.

定义 3.7. 对于上文中的随机过程 $W(t)$, 引入如下:

1. 对于 $t>0$, 记随机变量 $N(t)$ 为时间段 $[0,t]$ 内的证券买卖总次数, 再记
$$\overline{N} := \lim_{t\to\infty} \frac{\mathbb{E}[N(t)]}{t} \tag{3.17}$$
为单位时间内证券交易的平均次数.

2. 记 $\overline{W}$ 为现金资产的平均值, 即
$$\overline{W} := \lim_{t\to\infty} \mathbb{E}[W(t)]. \tag{3.18}$$

3. 于是, 单位时间内的现金管理总成本 c 为
$$c := \nu\overline{W} + \gamma\overline{N}, \tag{3.19}$$
其中 $\nu\overline{W}$ 与 $\gamma\overline{N}$ 分别是单位时间内的机会成本与交易成本; $\nu,\gamma>0$ 为常数, 其含义见上一小节.

特别注意, 随机过程 $W(t)$ 与 r,h 的选取有关, 进而单位时间内的现金管理总成本 $c=c(r,h)$ 也是关于 r,h 的函数. 于是, 这家油泰公司高层面临的问题是:

习题 **3.8.** 适当选取现金资产的上限 h 以及现金返回线 r, 使得单位时间内的现金管理总成本(3.19)最小.

至此, 我们已经完全把这个资产管理问题转化为数学问题. 接下来就该用数学方法来解决此问题了.

3.4.4 机会成本的计算

我们首先来给出机会成本 $\nu\overline{W}$ 的具体表达式, 这就需要我们用 h, r 来表示 $\overline{W}$. 数学上可以证明, 随着时间 $t\to\infty$, 随机变量 $W(t)$ 的概率密度函数 $f_{W(t)}(x)$ 会收敛于某个固定的函数 $f_\infty(x)$, 并且 f_∞ 初值 $W(0)$ 无关. 该分布在随机过程中被称为**极限分布**. 此时, 有

$$\overline{W}=\int_0^h xf_\infty(x)\mathrm{d}x. \tag{3.20}$$

下面我们来求 $f_\infty(x)$. 按前文所说, 我们用足够小时间间隔的对称随机游走来逼近布朗运动. 取定足够大的正整数 n, 将现金资产的范围区间 $[0,h]$ 等分为 n 份:

$$0<\frac{h}{n}<\frac{2h}{n}<\cdots<\frac{(n-1)h}{n}<h, \tag{3.21}$$

并假设现金资产的数量 $W(t)$ 的取值范围是 $\left\{\frac{kh}{n}\,\middle|\,0\le k\le n,\ k\in\mathbb{Z}\right\}$, 并且存在某个整数 $k_0\in\{1,2,...,n-1\}$, 使得现金返回线 r 满足

$$r=\frac{k_0h}{n}. \tag{3.22}$$

由前文(3.15), 我们设每经过一个单位时间

$$\Delta t=\frac{h^2}{n^2\sigma^2}, \tag{3.23}$$

总资产 $W(t)$ 增加或减少 $\Delta W=\frac{h}{n}$. 对于正整数 s, 设从 $t=0$ 时起经过 s 个单位时间 $s\Delta t$ 后的现金资产数量为 $W_n(s)$, 则有离散时间随机过程 $\{W_n(s)\}_{s=0}^\infty$, 注意它这是**有限状态 Markov 链**. 我们只需先对每个固定的 n 计算出 $\{W_n(s)\}$ 在 $s\to\infty$ 时的极限分布, 然后再令 $n\to\infty$ 即可得到 $f_\infty(x)$. 对于整数 $k\in\{0,1,2,...,n\}$, 记

$$p_{nk}:=\lim_{s\to\infty}\mathbb{P}\left(W_n(s)=\frac{kh}{n}\right), \tag{3.24}$$

则易知数列 $\{p_{nk}\}_{k=0}^{n}$ 满足如下递推关系:

$$\begin{aligned} p_{nk} &= \frac{1}{2}\left(p_{n,k-1}+p_{n,k+1}\right), \qquad k\notin\{0,k_0,n\}, &(3.25)\\ p_{n0} &= p_{nn}=0, &(3.26)\\ p_{nk_0} &= \frac{1}{2}\left(p_{n,k_0-1}+p_{n,k_0+1}+p_{n1}+p_{n,n-1}\right), &(3.27)\end{aligned}$$

以及归一化条件

$$\sum_{k=0}^{n} p_{nk}=1. \tag{3.28}$$

上述这些条件足以将数列 $\{p_{nk}\}_{k=0}^{n}$ 的通项公式强行求出来, 但这里其实没有这个必要.

观察(3.25), 不难发现 $\{p_{n0},p_{n1},\dots,p_{nk_0}\}$ 与 $\{p_{nk_0},p_{n,k_0+1},\dots,p_{nn}\}$ 都是等差数列. 于是我们**相信** (也不难给出严格证明, 但这从略), 当 $n\to\infty$ 时, 极限分布的概率密度函数 $f_\infty(x)$ 在区间 $(0,r)$ 与 (r,h) 上的限制都是一次函数; 再结合(3.26)(3.27), 我们也相信 $f_\infty(0)=f_\infty(h)=0$, 并且 $f_\infty(x)$ 在 $x=r$ 处连续. 再注意归一化条件

$$\int_0^h f_\infty(x)\mathrm{d}x=1,$$

不难得到

$$f_\infty(x)=\begin{cases}\frac{2}{hr}x, & x\in[0,r],\\ -\frac{2}{h(h-r)}(x-h), & x\in[r,h].\end{cases} \tag{3.29}$$

于是由(3.20), 公司现金资产的平均值 $\overline{W}$ 为

$$\begin{aligned}\overline{W} &= \int_0^h x f_\infty(x)\mathrm{d}x\\ &= \int_0^r \frac{2}{hr}x^2\mathrm{d}x+\int_r^h -\frac{2}{h(h-r)}x(x-h)\mathrm{d}x\end{aligned}$$

$$
\begin{aligned}
&= \frac{2}{3hr}r^3 - \frac{2}{h(h-r)}\left(\frac{1}{3}(h^3-r^3) - \frac{h}{2}(h^2-r^2)\right) \\
&= \frac{h+r}{3},
\end{aligned}
$$

因此单位时间内的**机会成本**

$$
\nu\overline{W} = \frac{\nu}{3}(h+r). \tag{3.30}
$$

3.4.5 交易成本的计算

下面我们来考察交易成本, 为此需要计算单位时间内证券交易的平均次数 $\overline{N}$. 若记

$$
\overline{T} := \text{相邻两次证券交易的平均时间间隔},
$$

则我们容易相信, $\overline{N}$ 与 $\overline{T}$ 满足关系

$$
\overline{N} = (\overline{T})^{-1}. \tag{3.31}
$$

上式可以用随机过程的有关理论严格证明, 这里就从略了.

在计算 $\overline{T}$ 之前, 我们回忆现金资产数量 $W(t)$ 的变化过程: 不妨 $t=0$ 时刻的现金数量为 r, 而 $W(t)$ 随着时间 t 的流逝而随机地变化, 当 $W(t)$ 的值变化到 0 或 h 时, 曲豆豆立刻通过买卖证券将现金数量重新调整为 r, 然后开启下一个 “交易周期”, 如此周而复始. 每一个这样的 “交易周期” 的平均用时就是 $\overline{T}$.

我们考虑一个更一般的问题: 若初始时刻 $t=0$ 拥有现金资产 x, 其中 $x \in (0,h)$, 则有随机变量

$$
T(x) := \text{现金资产数量到达 0 或者 } h \text{ 所用的时间}. \tag{3.32}
$$

在随机过程理论中, 随机变量 $T(x)$ 是一种**停时** (stopping time). 我们当然不会在这里深究随机过程理论, 毕竟这涉及超出本笔记范围的高等概率论. 不过我们容易看出,

$$\overline{T} = \mathbb{E}[T(r)]. \tag{3.33}$$

为计算 $\overline{T}$, 我们不如直接把函数 $x \mapsto \mathbb{E}[T(x)]$ 的显式表达式给求出来.

为此, 我们还是用离散时间的对称随机游走来逼近. 依然沿用上一小节的设定(3.21)-(3.23). 对每个 $k \in \{0, 1, 2, ..., n\}$, 我们记

$$T_{nk} := \text{现金资产数量从 } \frac{kh}{n} \text{ 到 } 0 \text{ 或者 } h \text{ 所用时间}, \tag{3.34}$$

$$t_{nk} := \mathbb{E}[T_{nk}] \tag{3.35}$$

可见数列 $\{T_{nk}\}_{k=1}^{n}$ 是函数 $T(x)$ 的离散版本.

若初始时刻 $t = 0$ 的现金资产总量为 $\frac{kh}{n}$, 则经过一个单位时间 Δt 之后, 现金资产变为 $\frac{(k-1)h}{n}$ 或者 $\frac{(k+1)h}{n}$; 然后再经过 $t_{n,k-1}$ 或 $t_{n,k+1}$ 的时间, 现金资产变为 0 或 r. 由此我们相信, 数列 $\{t_{nk}\}_{k=0}^{n}$ 满足递推关系

$$t_{nk} = \Delta t + \frac{1}{2}(t_{n,k-1} + t_{n,k+1}), \qquad 1 \le k \le n-1, \tag{3.36}$$

其中单位时间 Δt 满足(3.23). 此外 $\{t_{nk}\}$ 显然还要满足边值条件

$$t_{n0} = t_{nn} = 0. \tag{3.37}$$

由(3.36)(3.37)容易求得数列 $\{t_{nk}\}_{k=0}^{n}$ 的通项

$$t_{nk} = \frac{1}{\sigma^2}\frac{kh}{n}\left(h - \frac{kh}{n}\right), \quad 0 \le k \le n.$$

令 $n \to \infty$, 由上式容易看出

$$\mathbb{E}[T(x)] = \frac{1}{\sigma^2}x(h-x), \tag{3.38}$$

因此交易成本

$$\gamma\overline{N} = \gamma\overline{T}^{-1} = \frac{\gamma}{\mathbb{E}[T(r)]} = \frac{\sigma^2\gamma}{r(h-r)}. \tag{3.39}$$

3.4.6 最优现金返回线公式的推导

综合机会成本(3.30)与交易成本(3.39), 我们得到:

定理 3.9. 给定现金资产的上限 h 与现金返回线 r, 其中 $0 < r < h$, 则单位时间内的现金管理总成本 c, 见(3.19), 满足

$$c = \frac{\nu}{3}(h+r) + \frac{\sigma^2\gamma}{r(h-r)}, \tag{3.40}$$

其中 $\sigma, \gamma, \nu > 0$ 为常数, 它们分别为

$$\begin{aligned} \sigma &:= \text{现金单位时间变化的标准差}, \\ \gamma &:= \text{每次证券交易所产生的交易成本}, \\ \nu &:= \text{证券资产在单位时间的利率}. \end{aligned}$$

至此, 我们终于能把习题3.8翻译为纯数学问题:

习题 **3.10.**(习题3.8的等价表述). 求二元函数

$$c(r,h) = \frac{\nu}{3}(h+r) + \frac{\sigma^2\gamma}{r(h-r)}$$

在 $\{(r,h) \in \mathbb{R}^2 \,|\, 0 < r < h\}$ 上的最小值, 并求出相应的最小值点. 其中 σ, γ, ν 为大于零的常数.

解. 方便起见, 不如引入新的自变量

$$r' := h - r,$$

将总成本 c 视为关于 r, r' 的函数. 在此意义下

$$c = \frac{\nu}{3}(2r + r') + \frac{\sigma^2\gamma}{rr'}, \qquad r, r' > 0. \tag{3.41}$$

若 (r,r') 为函数 c 的最小值点, 则应该有

$$\frac{\partial c}{\partial r} = \frac{2\nu}{3} - \frac{\sigma^2\gamma}{r^2 r'} = 0,$$
$$\frac{\partial c}{\partial r'} = \frac{\nu}{3} - \frac{\partial\sigma^2\gamma}{\partial r(r')^2} = 0,$$

从而解得

$$r = \left(\frac{3\sigma^2\gamma}{4\nu}\right)^{\frac{1}{3}}, \tag{3.42}$$
$$r' = 2r. \tag{3.43}$$

容易验证上述 (r,r') 确实是 c 的最小值点, 并且相应的最小值为

$$c_{\min} = \left(6\nu^2\sigma^2\gamma\right)^{\frac{1}{3}}.$$

□

注记 3.11. (3.42)正是出现在 CPA 应试教材中的那个那个妖冶邪异的公式(3.14). 唯一的区别在于, 我们这里假设现金资产的下限为 0, 而不是某个一般的正实数 L. 如果规定公司的现金资产下限为 L, 完全类似的方法可以得到返回线公式

$$r = \left(\frac{3\sigma^2\gamma}{4\nu}\right)^{\frac{1}{3}} + L,$$

此时(3.43)式的相应版本为

$$h - r = 2(r - L),$$

即

$$h = 3r - 2L, \tag{3.44}$$

这正是 CPA 应试教辅中所谓“现金资产上限与现金资产下限, 现金返回线之间的关系”.

注记 **3.12.** 我们也可以用均值不等式来计算 c 的最小值:

$$
\begin{aligned}
c &= \frac{\nu}{3}(2r+r') + \frac{\sigma^2\gamma}{rr'} \\
&\geq \frac{2\sqrt{2}\nu}{3}\sqrt{rr'} + \frac{\sigma^2\gamma}{rr'} \\
&= \frac{\sqrt{2}\nu}{3}\sqrt{rr'} + \frac{\sqrt{2}\nu}{3}\sqrt{rr'} + \frac{\sigma^2\gamma}{rr'} \\
&\geq 3\sqrt[3]{\left(\frac{\sqrt{2}\nu}{3}\sqrt{rr'}\right)^2 \cdot \frac{\sigma^2\gamma}{rr'}} \\
&= \left(6\nu^2\sigma^2\gamma\right)^{\frac{1}{3}},
\end{aligned}
$$

检查均值不等式的取等条件也可得(3.42)(3.43).

至此, 笔者自以为理解了这个现金资产管理的所谓 Miller-Orr 模型.

4. 非交换代数与几何

本章用于记录笔者学习李群李代数以及非交换代数的心得点滴.

4.1 B-C-H 公式及其应用

设李代数 $\mathfrak{g} = \mathfrak{gl}(n, \mathbb{C})$, 若 $X, Y, Z \in \mathfrak{g}$ 满足 $\mathrm{e}^X\mathrm{e}^Y = \mathrm{e}^Z$, 则有众所周知的 **Baker-Campbell-Hausdorff** 公式:

$$
Z = X + Y + \frac{1}{2}[X,Y] + \frac{1}{12}[X,[X,Y]] - \frac{1}{12}[Y,[X,Y]] + \cdots, \tag{4.1}
$$

其中省略号代表的项的表达式非常复杂, 感兴趣者可查阅 **Dynkin 公式**, 而我们只需知道它形如 X, Y 反复作李括号. 事实上, 下述引理比公式(4.1)更加基本:

引理 4.1. 对于李代数 $\mathfrak{g} = \mathfrak{gl}(n, \mathbb{C})$, 以及 $\mathfrak{g}$ 上的可微曲线 $\gamma\colon (-\delta, \delta) \to \mathfrak{g}$, $t \mapsto \gamma(t)$, 其中 $\delta > 0$, 则有如下求导公式:

$$\frac{\mathrm{d}}{\mathrm{d}t} \mathrm{e}^{\gamma(t)} = \mathrm{e}^{\gamma(t)} \left(\frac{1 - \mathrm{e}^{-\operatorname{ad}_{\gamma(t)}}}{\operatorname{ad}_{\gamma(t)}} \right) (\gamma'(t)) \tag{4.2}$$

$$= \left[\left(\frac{\mathrm{e}^{\operatorname{ad}_{\gamma(t)}} - 1}{\operatorname{ad}_{\gamma(t)}} \right) (\gamma'(t)) \right] \mathrm{e}^{\gamma(t)}, \tag{4.3}$$

其中 $\operatorname{ad}\colon \mathfrak{g} \to \mathfrak{gl}(\mathfrak{g})$, $X \mapsto \operatorname{ad}_X$ 是李代数 $\mathfrak{g}$ 的伴随表示.

此引理的证明详见各种李群李代数教材, 例如 [GTM235], 这里不再重复. 不过我们还是简要回忆一下如何用此引理来推导(4.1)式: 设 $\mathfrak{g}$ 中的曲线 $Z(t)$ 满足

$$\mathrm{e}^{Z(t)} = \mathrm{e}^{tX} \mathrm{e}^{tY}, \qquad t \in [0, 1],$$

则 $Z(0) = 0$, 并且我们只需要计算 $Z(1)$; 为此, 将上式两边对 t 求导, 得到 $Z'(t)$ 的表达式, 最后由 $Z(1) = Z(0) + \int_0^1 Z'(t)\mathrm{d}t$ 经过一番计算即可得到(4.1), 甚至能给出省略号部分的完整表达式.

我们来看引理4.1在可积方程簇理论中的应用. 考虑形式变元 u 的如下微分多项式环

$$\mathcal{A} := C^\infty(u)[u_x, u_{xx}, ..., u^{(k)}, ...],$$

即 $\mathcal{A}$ 中的元素光滑地依赖 u, 且多项式地依赖 jet 变元 $u_x, u_{xx}, ...$. 定义 $\mathcal{A}$ 上的分次 deg 如下: 对任意 $\varphi \in C^\infty(0)$, $\deg \varphi(u) := 0$; 对于 $k \geq 1$, 规定 $\deg u^{(k)} = k$. 则在此分次下, 有**微分分次代数** $(\mathcal{A}, \partial_x)$, 其中微分算子

∂_x 按通常方式自然定义: $\partial_x \varphi(u) = \varphi'(u)u_x, \partial_x u^{(k)} = u^{(k+1)}$. 记 $\mathcal{A}$ 关于分次 deg 的直和分解为

$$\mathcal{A} = \bigoplus_{k=0}^{\infty} \mathcal{A}_k,$$

其中 $\mathcal{A}_k$ 是 $\mathcal{A}$ 中 k 次齐次元之全体, 注意 $\partial_x(\mathcal{A}_k) \subseteq \mathcal{A}_{k+1}$, 换言之微分算子 ∂_x 的次数是 1. 考虑 $\mathcal{A}$ 的完备化

$$\hat{\mathcal{A}} := \varinjlim_{k\to\infty} \left(\bigoplus_{i=1}^{k} \mathcal{A}_i\right) \cong \prod_{k\geq 0} \mathcal{A}_k. \tag{4.4}$$

我们习惯将 $\hat{\mathcal{A}}$ 中的元素 $f = (f_0, f_1, ..., f_k, ...)$ $(f_k \in \mathcal{A}_k)$ 记作

$$f = \sum_{k=0}^{\infty} \varepsilon^k f_k,$$

这里的形式参数 ε 视为无穷小量, 用于标记各项的次数. 在此约定下, 微分算子 ∂_x 被重新记为 $\varepsilon\partial_x$. 另外, $\hat{\mathcal{A}}$ 自然视为 $\mathcal{A}[\![\varepsilon]\!]$ 的子环.

注意 $\hat{\mathcal{A}}$ 中元素通过乘法作用自然视为 $\hat{\mathcal{A}}$ 上的线性算子, 即有

$$\begin{aligned} \hat{\mathcal{A}} &\hookrightarrow \mathfrak{gl}(\hat{\mathcal{A}}) \\ f &\mapsto (g \mapsto fg). \end{aligned}$$

此外, 微分算子 $\varepsilon\partial_x$ 本身就是 $\hat{\mathcal{A}}$ 上的线性算子. 考虑由这两类线性算子 (的线性组合) 构成的李代数

$$\mathfrak{g} := \hat{\mathcal{A}} \oplus \mathbb{C}\varepsilon\partial_x \subseteq \mathfrak{gl}(\hat{\mathcal{A}}), \tag{4.5}$$

这是无穷维李代数.

例题 4.2. 记号承上, 对于 $f, g \in \hat{\mathcal{A}}$, 则在 $\mathfrak{g}$ 中有交换关系

$$[f, g] = 0$$

$$[\varepsilon\partial_x, f] = \varepsilon\partial_x \circ f - f \circ \varepsilon\partial_x = \varepsilon\partial_x(f).$$

从而 $\hat{\mathcal{A}}$ 是 $\mathfrak{g}$ 的阿贝尔子代数, 且是 $\mathfrak{g}$ 的理想.

一般来说, 对于无穷维线性空间上的线性算子 X, 其指数映射 $\exp X$ 未必良定; 但对于(4.5)中的李代数 $\mathfrak{g}$, 指数映射

$$\begin{aligned} \exp\colon \mathfrak{g} &\to \mathrm{GL}(\hat{\mathcal{A}}) \\ X &\mapsto \mathrm{e}^X \end{aligned}$$

是良定的, 容易验证 $\mathrm{e}^X := \sum_{k\geq 0} \frac{X^k}{k!}$ 在 ε-进制拓扑下收敛. 特别地, 对于微分算子 $\varepsilon\partial_x \in \mathfrak{g}$, 记其指数映射

$$\Lambda := \mathrm{e}^{\varepsilon\partial_x}, \tag{4.6}$$

这是离散可积方程簇中常见的**差分算子**.

在学习**分数阶 Volterra 方程簇** (Fractional Volterra Hierarchy, FVH) 时, 笔者遇到了这样的一个等式:

性质 4.3. 记号承上, 则在 $\mathfrak{g}$ 中成立

$$\log\left(\mathrm{e}^u\Lambda\right) = \varepsilon\partial_x + \frac{\varepsilon\partial_x}{\Lambda - 1}(u), \tag{4.7}$$

即 $\exp\left(\varepsilon\partial_x + \frac{\varepsilon\partial_x}{\Lambda-1}(u)\right) = \mathrm{e}^u\Lambda$. 注意这里 $\frac{\varepsilon\partial_x}{\Lambda-1}(u) \in \hat{\mathcal{A}} \subseteq \mathfrak{g}$.

提出此公式的某人说, 这个式子 "容易" 从 B-C-H 公式(4.1)推出来, 但笔者认为没那么简单.

证明. 对于 $t \in [0,1]$, 记 $\mathfrak{g}$ 上的光滑曲线 $Z(t) := \log\left(\mathrm{e}^{tu}\Lambda\right)$, 即

$$\mathrm{e}^{Z(t)} = \mathrm{e}^{tu}\Lambda, \tag{4.8}$$

则首先有 $Z(0)=\log\Lambda:=\varepsilon\partial_x$. 我们只需要计算 $Z(1)$. 利用(4.3)(假装这些公式对合适的无穷维李代数也成立) 对上式两边求导, 有

$$\left[\frac{\mathrm{e}^{\mathrm{ad}_{Z(t)}}-1}{\mathrm{ad}_{Z(t)}}(Z'(t))\right]\mathrm{e}^{Z(t)}=u\mathrm{e}^{tu}\Lambda=u\mathrm{e}^{Z(t)},$$

从而立刻得到

$$Z'(t)=\frac{\mathrm{ad}_{Z(t)}}{\mathrm{e}^{\mathrm{ad}_{Z(t)}}-I}(u). \tag{4.9}$$

另一方面, 注意对任意 $f\in\hat{\mathcal{A}}\subseteq\mathfrak{g}$ 都有

$$\begin{aligned}\mathrm{e}^{\mathrm{ad}_{Z(t)}}(f)=&\ \mathrm{e}^{Z(t)}\circ f\circ\mathrm{e}^{-Z(t)}=\mathrm{e}^{tu}\Lambda\circ f\circ\Lambda^{-1}\mathrm{e}^{-tu}\\ =&\ \Lambda(f):=\mathrm{e}^{\varepsilon\partial_x}(f)\in\hat{\mathcal{A}}\subseteq\mathfrak{g},\end{aligned}$$

从而有

$$\mathrm{ad}_{Z(t)}(f)=\log\left(1+\left(\mathrm{e}^{\mathrm{ad}_{Z(t)}}-1\right)\right)(f)=\sum_{k\geq1}(-1)^{k+1}\frac{\left(\mathrm{e}^{\mathrm{ad}_{Z(t)}}-1\right)^k}{k}(f)$$
$$=\sum_{k\geq1}(-1)^{k+1}\frac{\left(\mathrm{e}^{\varepsilon\partial_x}-1\right)^k}{k}(f)=\varepsilon\partial_x(f).$$

特别地, 在上式中取 $f=u,u_x,...,u^{(k)},...$, 并结合(4.9)式可得

$$\begin{aligned}Z(1)=&\ Z(0)+\int_0^1Z'(t)\mathrm{d}t=\varepsilon\partial_x+\int_0^1\frac{\mathrm{ad}_{Z(t)}}{\mathrm{e}^{\mathrm{ad}_{Z(t)}}-1}(u)\mathrm{d}t\\ =&\ \varepsilon\partial_x+\int_0^1\frac{\varepsilon\partial_x}{\mathrm{e}^{\varepsilon\partial_x}-1}(u)\mathrm{d}t=\varepsilon\partial_x+\frac{\varepsilon\partial_x}{\Lambda-1}(u),\end{aligned}$$

从而得证. □

4.2 Schouten-Nijenhuis 括号与超泊松括号

设 M 为 n 维光滑流形, $\mathrm{PV}^p(M) := \Gamma\left(M, \bigwedge^p TM\right)$ 为 M 上的 p-**向量场**之全体 $(p \geq 0)$, 记

$$\mathrm{PV}^\bullet(M) := \bigoplus_{p \geq 0} \mathrm{PV}^p(M),$$

其中元素统称为 M 上的**多重向量场**. 在局部坐标 $(u^1, u^2, ..., u^n)$ 下, $\mathrm{PV}^p(M)$ 中的元素都形如

$$P = P^{i_1 i_2 \cdots i_p} \frac{\partial}{\partial u^{i_1}} \wedge \frac{\partial}{\partial u^{i_2}} \wedge \cdots \wedge \frac{\partial}{\partial u^{i_p}}. \tag{4.10}$$

在 $\mathrm{PV}^\bullet(M)$ 上有众所周知的 **Schouten-Nijenhuis 括号**

$$[,]\colon\ \mathrm{PV}^\bullet(M) \times \mathrm{PV}^\bullet(M) \to \mathrm{PV}^\bullet(M), \tag{4.11}$$

它是 $\mathbb{R}$-双线性映射, 可如下直接定义: 对任意 $X_1, X_2, ..., X_p$; $Y_1, Y_2, ...,$ $Y_q \in \mathrm{Vect}(M) \cong \mathrm{PV}^1(M)$, 以及 $f, g \in C^\infty(M) \cong \mathrm{PV}^0(M)$,

$$\begin{aligned}
&[X_1 \wedge X_2 \wedge \cdots \wedge X_p\, , Y_1 \wedge Y_2 \wedge \cdots \wedge Y_q] \\
:= &\sum_{i=1}^{p} \sum_{j=1}^{q} (-1)^{i+j} [X_i, Y_j] \wedge \left(X_1 \wedge \cdots \wedge \widehat{X}_i \wedge \cdots \wedge X_p\right) \\
&\qquad \wedge \left(Y_1 \wedge \cdots \wedge \widehat{Y}_j \wedge \cdots \wedge Y_q\right),
\end{aligned} \tag{4.12}$$

$$\begin{aligned}
&[X_1 \wedge X_2 \wedge \cdots \wedge X_p\, , g] \\
:= &\sum_{i=1}^{p} (-1)^{p-i} X_i(g) \left(X_1 \wedge \cdots \wedge \widehat{X}_i \wedge \cdots \wedge X_p\right),
\end{aligned} \tag{4.13}$$

$$\begin{aligned}
&[f\, , Y_1 \wedge Y_2 \wedge \cdots \wedge Y_q] \\
:= &\sum_{j=1}^{q} (-1)^{j} Y_j(f) \left(Y_1 \wedge \cdots \wedge \widehat{Y}_j \wedge \cdots \wedge Y_q\right),
\end{aligned} \tag{4.14}$$

$$[f, g] := 0. \tag{4.15}$$

特别地, 对于通常的切向量场 $X, Y \in \mathrm{Vect}(M) \cong \mathrm{PV}^1(M)$, 它们的 Schouten-Nijenhuis 括号 $[X, Y]$ 恰为通常的李括号.

可以证明由(4.12)-(4.15) 所给出的 $[,]$ 良好定义, 并且满足如下运算律: 对任意 $P \in \mathrm{PV}^p(M), Q \in \mathrm{PV}^q(M), R \in \mathrm{PV}^r(M)$ 都有

1. $[P, Q] \in \mathrm{PV}^{p+q-1}(M)$, 其中特别规定 $\mathrm{PV}^{-1}(M) := \{0\}$;

2. 超反对称性
$$[P, Q] = -(-1)^{(p-1)(q-1)}[Q, P]; \tag{4.16}$$

3. 超 Leibniz 法则
$$[P, Q \wedge R] = [P, Q] \wedge R + (-1)^{(p-1)q} Q \wedge [P, R]; \tag{4.17}$$

4. 超 Jacobi 恒等式
$$[P, [Q, R]] = [[P, Q], R] + (-1)^{(p-1)(q-1)}[Q, [P, R]]. \tag{4.18}$$

注记 **4.4.** 超 Leibniz 法则也可对偶地写成
$$[Q \wedge R, P] = Q \wedge [R, P] + (-1)^{r(p-1)}[[Q, P], R]; \tag{4.19}$$

超 Jacobi 恒等式也可改写为如下轮换对称形式
$$\begin{aligned} 0 = \ & (-1)^{(p-1)(r-1)}[P, [Q, R]] \\ & + (-1)^{(q-1)(p-1)}[Q, [R, P]] \\ & + (-1)^{(r-1)(q-1)}[R, [P, Q]]. \end{aligned}$$

注记 **4.5.** 相比显式表达式(4.12)-(4.15), 我们更关心 Schouten-Nijenhuis 括号的运算律. 事实上, 可以证明 $[,]$ 被初始条件

$$[f,g] := 0, \qquad [X,f] := X(f), \qquad [X,Y] := \mathcal{L}_X Y$$

$(\forall f,g \in C^\infty(M),\ X,Y \in \mathrm{Vect}(M))$ 以及运算律(4.16),(4.17)所唯一确定. 特别注意, 如果超反对称性与超 Leibniz 法则成立, 那么超 Jacobi 恒等式自动成立, 这可通过对 $p+q+r$ 使用数学归纳法来直接验证.

在哈密顿系统的研究中常需要通过具体计算 Schouten-Nijenhuis 括号来验证哈密顿结构; 而显式表达式(4.12)-(4.15)过于繁琐, 尤其在无穷维流形的推广情形之下更难以用于具体计算. 而本节的目的正是寻求 Schouten-Nijenhuis 括号的简便算法.

为此先引入如下偷懒记号: 将 p-向量场(4.10)简记为

$$P \mapsto \widehat{P} := P^{i_1 i_2 \cdots i_p}\theta_{i_1}\theta_{i_2}\cdots\theta_{i_p}, \tag{4.20}$$

换言之, 我们按照以下规则来改写: 用符号 θ_i 来代替 $\frac{\partial}{\partial u^i}$, 然后将 “$\wedge$” 省略. 这样的 θ_i 被物理学家们称为 **Grassmann 变量**或者**超变量**, 它们之间的乘法是反交换的:

$$\theta_i\theta_j = -\theta_j\theta_i, \tag{4.21}$$

如此便自然进入了**超流形**的世界:

定义 4.6. 对于 n 维光滑流形, 记余切丛 T^*M 的**超化**

$$\widehat{M} := \Pi(T^*M). \tag{4.22}$$

具体地, M 的局部坐标卡 U 诱导 $\widehat{M}$ 的局部坐标卡

$$\widehat{U} \cong U \times \mathbb{R}^{0|n};$$

M 的局部坐标 $(u^1, u^2, ..., u^n)$ 自然给出 $\widehat{M}$ 的局部坐标 $(u^i; \theta_i)$, 这里的超变量 θ_i 表示 $\mathrm{d}u^i$ 的分量.

容易验证, 在另一组局部坐标 $\{\tilde{u}^i\}$ 下, 相应的超变量 $\tilde{\theta}_i$ 与旧坐标 θ_i 之间的转换关系为

$$\tilde{\theta}_i = \frac{\partial u^j}{\partial \tilde{u}^i}\theta_j, \tag{4.23}$$

这恰与切向量场 $\frac{\partial}{\partial u^i}$ 的转换关系相同.

定义 4.7. 对于 n 维光滑流形 M, 定义非交换环 $C^\infty(\widehat{M})$ 如下: 在 M 的局部平凡坐标卡 U 下,

$$C^\infty(\widehat{M})|_U := C^\infty(U)[\theta_1, \theta_2, ..., \theta_n], \tag{4.24}$$

即关于超变量 θ_i 的 $C^\infty(U)$-多项式环, 其中超变量 θ_i 满足(4.21).

我们更习惯把 $C^\infty(\widehat{M})$ 重新记为 $\widehat{\mathcal{A}}^\bullet(M)$, 即

$$\widehat{\mathcal{A}}^\bullet(M) := C^\infty(\widehat{M}). \tag{4.25}$$

注意 $\widehat{\mathcal{A}}^\bullet(M)$ 中的元素按所含超变量的次数有自然的分次

$$\widehat{\mathcal{A}}^\bullet(M) = \bigoplus_{p\geq 0} \widehat{\mathcal{A}}^p(M),$$

俗称**超分次**. “偷懒写法”(4.20)其实给出了**分次代数** ($\mathrm{PV}^\bullet(M), \wedge$) 与 ($\widehat{\mathcal{A}}^\bullet(M), \cdot$) 之间的同构

$$\begin{aligned} \iota\colon\ \mathrm{PV}^\bullet(M) &\to \widehat{\mathcal{A}}^\bullet(M) \\ P &\mapsto \widehat{P}. \end{aligned} \tag{4.26}$$

众所周知, 余切丛 T^*M 有典范的辛结构, 从而 $C^\infty(T^*M)$ 上有典范的泊松括号; 类似地, 余切丛的超化 $\widehat{M} := \Pi(T^*M)$ 有典范的 “**超辛结构**”, 从而 $\widehat{\mathcal{A}}^\bullet(M) := C^\infty(\widehat{M})$ 上有相应的**超泊松括号**, 其定义如下:

定义 4.8. 对于 n 维光滑流形 M 以及 $\widehat{P}, \widehat{Q} \in \widehat{\mathcal{A}}^\bullet(M)$, 定义

$$[\widehat{P}, \widehat{Q}] := \widehat{P}\left(\frac{\overleftarrow{\partial}}{\partial u^i}\frac{\overrightarrow{\partial}}{\partial \theta_i} - \frac{\overleftarrow{\partial}}{\partial \theta_i}\frac{\overrightarrow{\partial}}{\partial u^i}\right)\widehat{Q}. \tag{4.27}$$

如此运算 $[,]\colon \widehat{\mathcal{A}}^\bullet(M) \times \widehat{\mathcal{A}}^\bullet(M) \to \widehat{\mathcal{A}}^\bullet(M)$ 称为**超泊松括号**.

特别注意这里的 $\frac{\overleftarrow{\partial}}{\partial \theta_i}$ 是右微分算子, 它从右边作用于 $\widehat{\mathcal{A}}^\bullet(M)$ 中的元素; 而通常的左微分算子 $\overrightarrow{\partial}$ 常简记为 ∂. 此外还要注意沿超变量的偏导 $\frac{\partial}{\partial \theta_i} := \frac{\overrightarrow{\partial}}{\partial \theta_i}$ 满足如下**超 Leibniz 法则**:

$$\frac{\partial}{\partial \theta_i}(\widehat{P}\widehat{Q}) = \frac{\partial \widehat{P}}{\partial \theta_i}\widehat{Q} + (-1)^p \widehat{P}\frac{\partial \widehat{Q}}{\partial \theta_i} \tag{4.28}$$

对任意 $\widehat{P} \in \widehat{\mathcal{A}}^p(M), \widehat{Q} \in \widehat{\mathcal{A}}^q(M)$ 都成立. 而右微分算子 $\frac{\overleftarrow{\partial}}{\partial \theta_i}$ 满足右作用的超 Leibniz 法则

$$(\widehat{P}\widehat{Q})\frac{\overleftarrow{\partial}}{\partial \theta_i} = \widehat{P}\left(\widehat{Q}\frac{\overleftarrow{\partial}}{\partial \theta_i}\right) + (-1)^q\left(\widehat{P}\frac{\overleftarrow{\partial}}{\partial \theta_i}\right)\widehat{Q}. \tag{4.29}$$

由此容易验证

$$\widehat{P}\frac{\overleftarrow{\partial}}{\partial \theta_i} = (-1)^{p-1}\frac{\partial \widehat{P}}{\partial \theta_i}, \qquad \forall\, \widehat{P} \in \widehat{\mathcal{A}}^p(M). \tag{4.30}$$

由上式可以给出超泊松括号的如下等价定义:

性质 4.9. 设 M 为 n 维光滑流形, 则对任意 $\widehat{P} \in \widehat{\mathcal{A}}^p(M)$, $\widehat{Q} \in \widehat{\mathcal{A}}^q(M)$ 都成立

$$[\widehat{P}, \widehat{Q}] = \frac{\partial \widehat{P}}{\partial u^i} \frac{\partial \widehat{Q}}{\partial \theta_i} + (-1)^p \frac{\partial \widehat{P}}{\partial \theta_i} \frac{\partial \widehat{Q}}{\partial u^i}. \tag{4.31}$$

由此可以直接验证超泊松括号满足与 Schouten-Nijenhuis 括号相同的运算律: 对任意 $\widehat{P} \in \widehat{\mathcal{A}}^p(M)$, $\widehat{Q} \in \widehat{\mathcal{A}}^q(M)$, $\widehat{R} \in \widehat{\mathcal{A}}^r(M)$ 都有

1. $[\widehat{P}, \widehat{Q}] \in \widehat{\mathcal{A}}^{p+q-1}(M)$, 其中特别规定 $\widehat{\mathcal{A}}^{-1}(M) := \{0\}$;

2. 超反对称性
$$[\widehat{P}, \widehat{Q}] = -(-1)^{(p-1)(q-1)}[\widehat{Q}, \widehat{P}]; \tag{4.32}$$

3. 超 Leibniz 法则
$$[\widehat{P}, \widehat{Q}\widehat{R}] = [\widehat{P}, \widehat{Q}]\widehat{R} + (-1)^{(p-1)q}\widehat{Q}[\widehat{P}, \widehat{R}]; \tag{4.33}$$

4. 超 Jacobi 恒等式
$$[\widehat{P}, [\widehat{Q}, \widehat{R}]] = [[\widehat{P}, \widehat{Q}], \widehat{R}] + (-1)^{(p-1)(q-1)}[\widehat{Q}, [\widehat{P}, \widehat{R}]]. \tag{4.34}$$

与注记4.5完全类似, 只需验证超反对称性与超 Leibniz 法则即可, 这两条成立则超 Jacobi 恒等式自动成立. 因此我们立刻得到本小节主要结论:

定理 4.10. 设 M 为 n 维光滑流形, 则对任意 $P, Q \in \mathrm{PV}^\bullet(M)$ 都成立

$$\iota[P, Q] = -[\iota(P), \iota(Q)], \tag{4.35}$$

其中同构映射 ι 的定义见(4.26), 并且上式左右两边的括号分别为 *Schouten-Nijenhuis* 括号与超泊松括号.

证明. 只需考虑 P, Q 为齐次元的情形, 即不妨 $P \in \mathrm{PV}^p(M), Q \in \mathrm{PV}^q(M)$. 注意 Schouten-Nijenhuis 括号与超泊松括号满足相同的运算律 (超反对称性与超 Leibniz 法则), 从而由注记4.5可知只需验证 $(p, q) = (0, 0), (0, 1), (1,$ 的情形即可. 从而定理得证. □

此定理将多重向量场的 Schouten-Nijenhuis 括号运算转化为超变量的运算, 实践表明后者的计算更简便, 尤其是在无穷维流形的推广情形下更能大大简化计算.

4.3 什么是经典 R-矩阵?

本节是本人笔记《辛几何初步》第 3.2.4 节的番外篇, 内容选自 M. A. Semenov-Tyan-Shanskii. *What is a classical R-matrix?*

4.3.1 经典 R-矩阵与双李代数

定义 4.11. 对于 *(有限维 $\mathbb{R}$-)* 李代数 $\mathfrak{g}$ 以及线性算子 $R \in \mathrm{End}(\mathfrak{g})$, 如果二元运算

$$\begin{aligned} [,]_R \colon \mathfrak{g} \times \mathfrak{g} &\to \mathfrak{g} \\ (X, Y) &\mapsto [RX, Y] + [X, RY] \end{aligned} \tag{4.36}$$

是李括号, 则称 R 是**经典 R-矩阵** *(classical R-matrix)*, 并且称 $(\mathfrak{g}, R)$ 为**双李代数** *(double Lie algebra)*.

注意 $[,]_R$ 总是自动满足双线性与反对称性, 从而 R 是经典 R-矩阵当且仅当 $[,]_R$ 满足 Jacobi 恒等式. 对于双李代数 $(\mathfrak{g}, R)$, 我们也将关于括号 $[,]_R$ 的李代数 $(\mathfrak{g}, [,]_R)$ 简记为 $\mathfrak{g}_R$.

众所周知, 李代数 $\mathfrak{g}$ 的对偶空间 $\mathfrak{g}^*$ 上有典范的泊松结构, 即**李-泊松结构**. 而对于双李代数 $(\mathfrak{g}, R)$, 分别记 $\mathfrak{g}^*$ 上的由通常李括号 $[,]$ 与 R-李括号 $[,]_R$ 所诱导的李-泊松括号为 $\{,\}$ 与 $\{,\}_R$. 换言之, 对任意 $f, g \in C^\infty(\mathfrak{g}^*)$ 以及点 $\xi \in \mathfrak{g}^*$, 成立

$$
\begin{aligned}
\{f, g\}(\xi) &= \langle \xi, [\mathrm{d}_\xi f, \mathrm{d}_\xi g] \rangle\,, \\
\{f, g\}_R(\xi) &= \langle \xi, [\mathrm{d}_\xi f, \mathrm{d}_\xi g]_R \rangle\,,
\end{aligned}
\tag{4.37}
$$

这里的 $\mathrm{d}_\xi \colon C^\infty(\mathfrak{g}^*) \to \mathfrak{g}$ 是以下若干映射的复合:

$$
C^\infty(\mathfrak{g}^*) \xrightarrow{\mathrm{d}} \Omega^1(\mathfrak{g}^*) \xrightarrow{\mathrm{ev}_\xi} T^*_\xi \mathfrak{g}^* \cong (\mathfrak{g}^*)^* \cong \mathfrak{g},
$$

且 $\langle , \rangle$ 为 $\mathfrak{g}^*$ 与 $\mathfrak{g}$ 的配对.

李代数 $\mathfrak{g}$ 与 $\mathfrak{g}_R$ 的**余伴随表示**分别记作 ad^* 与 ad^*_R, 即

$$
\mathrm{ad}^*, \mathrm{ad}^*_R \colon \mathfrak{g} \to \mathrm{End}(\mathfrak{g}^*),
$$

使得对任意 $X, Y \in \mathfrak{g}$ 以及 $\xi \in \mathfrak{g}^*$ 都成立

$$
\begin{aligned}
\langle \mathrm{ad}^* X \cdot \xi,\, Y \rangle &= -\langle \xi,\, [X, Y] \rangle, \\
\langle \mathrm{ad}^*_R X \cdot \xi,\, Y \rangle &= -\langle \xi,\, [X, Y]_R \rangle.
\end{aligned}
\tag{4.38}
$$

引理 4.12. 对于双李代数 $(\mathfrak{g}, R)$, 成立

$$
\mathrm{ad}^*_R = \mathrm{ad}^* \circ R + R^* \circ \mathrm{ad}^*,
\tag{4.39}
$$

其中 $R^* \colon \mathfrak{g}^* \to \mathfrak{g}^*$ 是 R 的对偶算子.

证明. 对任意 $X, Y \in \mathfrak{g}$ 以及 $\xi \in \mathfrak{g}^*$, 由相关定义直接验证如下:

$$
\langle \mathrm{ad}^*_R X \cdot \xi, Y \rangle = -\langle \xi, [X, Y]_R \rangle = -\langle \xi, [RX, Y] + [X, RY] \rangle
$$

$$
\begin{aligned}
&= \langle \operatorname{ad}^* RX\cdot\xi, Y\rangle + \langle \operatorname{ad}^* X\cdot\xi, RY\rangle \\
&= \langle (\operatorname{ad}^*\circ R + R^*\circ\operatorname{ad}^*)X\cdot\xi, Y\rangle,
\end{aligned}
$$

从而得证. □

对于 $f\in C^\infty(\mathfrak{g}^*)$, 则 $\operatorname{ad}^*(\mathrm{d}_\xi f)=0$ 对 $\xi\in\mathfrak{g}^*$ 恒成立, 当且仅当对任意 $g\in C^\infty(\mathfrak{g}^*)$ 都有

$$
\{f,g\}(\xi)=\langle\xi,[\mathrm{d}_\xi f,\mathrm{d}_\xi g]\rangle=-\left\langle \operatorname{ad}^*_{\mathrm{d}_\xi f}\cdot\xi,\mathrm{d}_\xi g\right\rangle=0,
$$

即 f 是泊松括号 $\{,\}$ 的 **Casimir 函数**. 因此 $f\in C^\infty(\mathfrak{g}^*)$ 是李-泊松括号 $\{,\}$ 的 Casimir 函数, 当且仅当 $\operatorname{ad}^*(\mathrm{d}_\xi f)=0$ 对 $\xi\in\mathfrak{g}^*$ 恒成立.

引理 4.13. *对于双李代数 $(\mathfrak{g},R)$, 若 $f,g\in C^\infty(\mathfrak{g}^*)$ 是 $\{,\}$ 的 Casimir 函数, 则*

$$
\{f,g\}_R=0.
$$

证明. 由于 f,g 是李-泊松括号 $\{,\}$ 的 Casimir 函数, 从而对任意 $\xi\in\mathfrak{g}^*$ 都有 $\operatorname{ad}^*\mathrm{d}_\xi f=\operatorname{ad}^*\mathrm{d}_\xi g=0$, 因此

$$
\begin{aligned}
\{f,g\}_R(\xi) &= \langle\xi,[\mathrm{d}_\xi f,\mathrm{d}_\xi g]_R\rangle \\
&= \langle\xi,[R(\mathrm{d}_\xi f),\mathrm{d}_\xi g]+[\mathrm{d}_\xi f,R(\mathrm{d}_\xi g)]\rangle \\
&= \langle\operatorname{ad}^*\mathrm{d}_\xi g\cdot\xi,R(\mathrm{d}_\xi f)\rangle-\langle\operatorname{ad}^*\mathrm{d}_\xi f\cdot\xi,R(\mathrm{d}_\xi g)\rangle \\
&= 0,
\end{aligned}
$$

从而得证. □

引理 4.14. 对于双李代数 $(\mathfrak{g}, R)$, 若哈密顿量 $H \in C^\infty(\mathfrak{g}^*)$ 是关于 $\{,\}$ 的 *Casimir* 函数, 则 H 关于李-泊松括号 $\{,\}_R$ 的哈密顿演化方程为

$$\frac{\mathrm{d}\xi}{\mathrm{d}t} = \mathrm{ad}^* R(\mathrm{d}_\xi H) \cdot \xi, \tag{4.40}$$

这里 $t \mapsto \xi := \xi(t)$ 为 $\mathfrak{g}^*$ 中的曲线.

证明. 该哈密顿演化方程众所周知的表达式应该是

$$\frac{\mathrm{d}\xi}{\mathrm{d}t} = \mathrm{ad}_R^* \mathrm{d}_\xi H \cdot \xi,$$

然后利用(4.39)并注意 $\mathrm{ad}^* \mathrm{d}_\xi H = 0$ 即可. □

5. 可积系统理论

本章用于收集笔者在可积系统理论的学习, 教学与科研中的各种随笔, 主要涉及 Dubrovin-Frobenius 流形理论以及双哈密顿结构的形变.

5.1 Frobenius 流形的 Legendre 变换

Frobenius 流形是二维拓扑场论 (2D TFT) 的 primary free energy 所满足的 Witten-Dijkgraaf-Verlinde-Verlinde 结合性方程 (简称 **WDVV 方程**) 的几何模型, 由 Dubrovin 在 20 世纪 90 年代引入. Frobenius 流形的数学定义有若干不同的版本, 而本小节临时采用如下约定:

定义 5.1. *所谓* ***Frobenius* 流形**, *是指四元组* $(M, \eta, \cdot, e)$, *其中:*

- M *是* n *维复流形,* η *是* M *上的全纯 (伪) 黎曼度量;*
- $\cdot$ *是* M *上的* $(1, 2)$*-型张量,* e *为* M *上的切向量场,*

使得满足以下条件:

1. *度量* η *是平坦的;*
2. *任意* $p \in M$, *切空间* T_pM *具有* ***Frobenius* 代数***结构* $(T_pM, \eta, \cdot)$, *使得* $\eta, \cdot$ *分别为该 Frobenius 代数的内积与乘法, 并且* e *处处是该 Frobenius 乘法的单位元;*
3. *若引入* $(0, 3)$*-型张量* c: $(X, Y, Z) \mapsto \eta(X \cdot Y, Z)$, *并记* ∇ *为度量* η *的 Levi-Civita 联络, 则* $(0, 4)$*-型张量* ∇c *是 4-对称的.*

由于度量 η 是平坦的, 我们不妨取 Frobenius 流形的一组平坦坐标 $\{v^\alpha\}$. 在此坐标下, 度量 η 形如

$$\eta = \eta_{\alpha\beta}\, \mathrm{d}v^\alpha \otimes \mathrm{d}v^\beta, \tag{5.1}$$

其中 $(\eta_{\alpha\beta})$ 是常系数可逆方阵. 此外, 张量 c 在该坐标下形如

$$c = c_{\alpha\beta\gamma}\, \mathrm{d}v^\alpha \otimes \mathrm{d}v^\beta \otimes \mathrm{d}v^\gamma.$$

由张量 ∇c 的 4-对称性可知, (局部) 存在函数 $F = F(v^1, ..., v^n)$ 使得

$$c_{\alpha\beta\gamma} = \frac{\partial^3 F}{\partial v^\alpha \partial v^\beta \partial v^\gamma}, \tag{5.2}$$

如此 F 称为 Frobenius 流形的**势函数**. 在此语境下, Frobenius 代数乘法的结合性等价于如下方程:

$$\frac{\partial^3 F}{\partial v^\alpha \partial v^\beta \partial v^\lambda} \eta^{\lambda\mu} \frac{\partial^3 F}{\partial v^\mu \partial v^\gamma \partial v^\delta} = \frac{\partial^3 F}{\partial v^\delta \partial v^\beta \partial v^\lambda} \eta^{\lambda\mu} \frac{\partial^3 F}{\partial v^\mu \partial v^\gamma \partial v^\alpha}, \tag{5.3}$$

这正是著名的 WDVV 方程, 其中 $(\eta^{\alpha\beta}) := (\eta_{\alpha\beta})^{-1}$.

注记 **5.2.** 在别的版本的定义中, 单位向量场 e 需要满足 $\nabla e = 0$, 即要求单位向量场的平坦性. 而本小节中的 Frobenius 流形并不被要求具有此性质 (这种单位向量场未必平坦的情形在某些别的场合被笔者称为 "广义 Frobenius 流形"). 此外, Dubrovin 关于 Frobenius 流形的原始定义中还要求其具有某种 "拟齐次性", 需要具有所谓 "欧拉向量场", 而本小节对此也无要求.

对于给定的 Frobenius 流形 $(M, \eta, \cdot, e)$, 我们可以通过某种方式引入一个新的度量 $\hat{\eta}$, 使得 M 在新度量 η 与原来的乘法 $\cdot$ 意义下成为另一个 Frobenius 流形 $(M, \hat{\eta}, \cdot, e)$, 这样的变换被称为 Frobenius 流形的 **Legendre 变换**, 它最初也是由 Dubrovin 所提出. 本小节的目的是将 Legendre 变换适当推广.

定义 5.3. *Frobeinus 流形 $(M, \eta, \cdot, e)$ 上的切向量场 $b \in \mathrm{Vect}(M)$ 称为* ***Legendre* 向量场***, 如果 b 同时满足以下两条:*

1. *b 关于 Frobenius 乘法处处可逆;*
2. *令 M 上的 $(1,1)$-型张量场 $B\colon X \mapsto b \cdot X$, 则 ∇B 是 2-对称的, 其中 ∇ 是关于度量 η 的 Levi-Civita 联络.*

取关于度量 η 的平坦坐标 $\{v^\alpha\}$, 在此坐标下记

$$b = b^\alpha \frac{\partial}{\partial v^\alpha},$$

则张量 B 在该坐标下的系数矩阵 (B^β_α) 为

$$B^\beta_\alpha = b^\lambda c^\beta_{\lambda\alpha}.$$

于是, b 为 Frobenius 乘法的可逆元当且仅当矩阵 (B^β_α) 处处可逆; 而 ∇B

是 2-对称性等价于

$$\partial_\gamma B_\alpha^\beta = \partial_\alpha B_\gamma^\beta. \tag{5.4}$$

常见的例子是, 如果 b 在平坦坐标下的各分量系数 b^α 都是常数, 则 ∇B 的 2-对称性, 也就是上式, 自动成立.

接下来给出本小节主要结果:

定理 5.4. 设 b 为 *Frobenius* 流形 $(M, \eta, \cdot, e)$ 的 *Legendre* 向量场, 引入 M 上的 $(0,2)$-型张量 $\hat{\eta}$ 如下:

$$\hat{\eta}(X, Y) := \eta(b \cdot X, b \cdot Y), \tag{5.5}$$

则 $(M, \hat{\eta}, \cdot, e)$ 也是 *Frobenius* 流形.

对任意 $p \in M$, $(T_pM, \hat{\eta}, \cdot)$ 显然也构成 Frobenius 代数; 于是只需再验证以下两点:

- $\hat{\eta}$ 是平坦度量;
- $\hat{\nabla}\hat{c}$ 是 4-对称的, 其中 $\hat{c}$: $(X, Y, Z) \mapsto \hat{\eta}(X \cdot Y, Z)$, 并且 $\hat{\nabla}$ 是关于度量 $\hat{\eta}$ 的 Levi-Civita 联络.

用整体定义的张量语言来验证它们, 是十分枯燥复杂的; 我们最好还是充分利用一些特殊技巧: 为证明 $\hat{\eta}$ 的平坦性, 我们不要去直接验算黎曼曲率张量, 而是去构造相应的平坦坐标 $\hat{v}^\alpha$; 为证明 $\hat{\nabla}\hat{c}$ 的 4-对称性, 我们不要直接求张量的协变导数, 而是去构造相应的势函数 $\hat{F}$.

定理5.4的证明. 取定关于度量 η 的一组平坦坐标 v^α, 使得 η 形如(5.1). 再记 F 为(5.2)中的势函数.

1. 断言: 存在局部坐标 $\{\hat{v}^\alpha\}$, 使得

$$\hat{\eta} = \eta_{\alpha\beta} \mathrm{d}\hat{v}^\alpha \otimes \mathrm{d}\hat{v}^\beta, \tag{5.6}$$

从而 $\hat{\eta}$ 在坐标 $\hat{v}^\alpha$ 下是常系数的, 从而 $\hat{\eta}$ 平坦. 注意到, 如果(5.6)成立, 则应该有

$$\eta_{\alpha\beta} = \hat{\eta}\left(\frac{\partial}{\partial \hat{v}^\alpha}, \frac{\partial}{\partial \hat{v}^\beta}\right) = \eta\left(b \cdot \frac{\partial}{\partial \hat{v}^\alpha}, b \cdot \frac{\partial}{\partial \hat{v}^\beta}\right),$$

由此可见, 如果能够找到局部坐标 $\{\hat{v}^\alpha\}$ 使得

$$\frac{\partial}{\partial v^\alpha} = b \cdot \frac{\partial}{\partial \hat{v}^\alpha}, \tag{5.7}$$

那么如此 $\{\hat{v}^\alpha\}$ 即为所求; 而容易验证(5.7)等价于

$$\frac{\partial \hat{v}^\alpha}{\partial v^\beta} = B^\alpha_\beta := b^\lambda c^\alpha_{\lambda\beta}. \tag{5.8}$$

上述方程的解 $\hat{v}^\alpha$ 的存在性的相容性条件恰为(5.4). 断言得证.

2. 记号承上, 断言: (局部) 存在函数 $\hat{F}$, 使得成立

$$\frac{\partial^2 \hat{F}}{\partial \hat{v}^\alpha \partial \hat{v}^\beta} = \frac{\partial^2 F}{\partial v^\alpha \partial v^\beta}. \tag{5.9}$$

为证此断言, 只需验证如下相容性条件:

$$\frac{\partial}{\partial \hat{v}^\gamma}\left(\frac{\partial^2 F}{\partial v^\alpha \partial v^\beta}\right) = \frac{\partial}{\partial \hat{v}^\alpha}\left(\frac{\partial^2 F}{\partial v^\gamma \partial v^\beta}\right).$$

注意(5.7), 从而

$$\frac{\partial}{\partial \hat{v}^\gamma}\left(\frac{\partial^2 F}{\partial v^\alpha \partial v^\beta}\right) = (B^{-1})^\lambda_\gamma c_{\lambda\alpha\beta} = \eta\left(b^{-1} \cdot \frac{\partial}{\partial v^\gamma} \cdot \frac{\partial}{\partial v^\alpha}, \frac{\partial}{\partial v^\beta}\right),$$

其中 b^{-1} 是向量场 b 关于 Frobenius 乘法的逆. 由乘法 $\cdot$ 的结合性可知上述相容性条件满足, 断言得证.

3. 最后, 由 $\hat{\eta}$ 的定义以及(5.7)(5.9), 容易验证 $\hat{F}$ 满足如下等式:

$$\hat{c}_{\hat{\alpha}\hat{\beta}\hat{\gamma}} := \hat{\eta}\left(\frac{\partial}{\partial\hat{v}^{\alpha}}\cdot\frac{\partial}{\partial\hat{v}^{\beta}},\frac{\partial}{\partial\hat{v}^{\gamma}}\right) = \frac{\partial^3\hat{F}}{\partial\hat{v}^{\alpha}\partial\hat{v}^{\beta}\partial\hat{v}^{\gamma}}, \tag{5.10}$$

从而立刻得到 $\hat{\nabla}\hat{c}$ 是 4-对称的.

综上, 定理得证. □

注记 5.5. 沿用前文记号. 我们回忆, 在平坦坐标 $\{v^{\alpha}\}$ 下, 分别记 Legendre 向量场 b 与单位向量场 e 为

$$b = b^{\alpha}\frac{\partial}{\partial v^{\alpha}}, \quad e = e^{\alpha}\frac{\partial}{\partial v^{\alpha}},$$

则单位向量场在新坐标 $\hat{v}^{\alpha}$ 下的系数恰为 Legendre 向量场在旧坐标 v^{α} 下的系数, 即

$$e = b^{\alpha}\frac{\partial}{\partial\hat{v}^{\alpha}}. \tag{5.11}$$

下面我们来看一些例子.

例题 5.6. 考虑 2 维 Frobenius 流形

$$F_{\mathrm{Toda}} = \frac{1}{2}v^2u + \mathrm{e}^u, \tag{5.12}$$

其中平坦坐标 $(v,u) := (v^1, v^2)$, 并且在此坐标下, 度量 $\eta = \begin{pmatrix} & 1 \\ 1 & \end{pmatrix}$. 若取 Legendre 向量场 $b = \frac{\partial}{\partial u}$, 则相应的新坐标为

$$\hat{v} = v, \quad \hat{u} = \mathrm{e}^u,$$

新的势函数为

$$F_{\mathrm{NLS}} = \frac{1}{2}\hat{v}^2\hat{u} + \frac{\hat{u}^2}{2}\left(\log\hat{u} - \frac{3}{2}\right).$$

这是 Toda 流形与非线性薛定谔 (NLS) 流形之间的变换关系.

例题 5.7. 考虑 2 维 Frobenius 流形

$$F_{\mathrm{Toda}} = \frac{1}{2}v^2 u + \mathrm{e}^u, \tag{5.13}$$

其中平坦坐标 $(v, u) := (v^1, v^2)$, 并且在此坐标下, 度量 $\eta = \begin{pmatrix} & 1 \\ 1 & \end{pmatrix}$. 若取 Legendre 向量场 $b = \frac{\partial}{\partial u}$, 则相应的新坐标为

$$\hat{v} = v, \quad \hat{u} = \mathrm{e}^u,$$

新的势函数为

$$F_{\mathrm{NLS}} = \frac{1}{2}\hat{v}^2\hat{u} + \frac{\hat{u}^2}{2}\left(\log\hat{u} - \frac{3}{2}\right).$$

这是 Toda 流形与非线性薛定谔 (NLS) 流形之间的变换关系.

反过来, 也可以通过适当的 Legendre 向量将 Toda 流形变为 Ablowitz-Ladik 流形. 事实上, Toda, NLS 以及 AL 这三者可以通过 Legendre 变换互相得到.

例题 5.8. 考虑 2 维 Frobenius 流形

$$F_{\mathrm{DA}_2} = -\frac{1}{48}v^3 + \frac{3}{32}v^2u^2 - \frac{3}{64}vu^4 + \frac{9}{640}u^6, \tag{5.14}$$

其中平坦坐标 $(v, u) := (v^1, v^2)$, 并且在此坐标下, 度量 $\eta = \begin{pmatrix} & 1 \\ 1 & \end{pmatrix}$. 若取 Legendre 向量场 $b = \frac{\partial}{\partial v}$, 则相应的新坐标 $(\hat{v}, \hat{u})$ 与旧坐标 (v, u) 满足

$$\begin{cases} \hat{v} = \frac{3}{8}vu - \frac{3}{16}u^3, \\ \hat{u} = -\frac{1}{8}v + \frac{3}{16}u^2, \end{cases}$$

记 $\hat{F}=\hat{F}(\hat{v},\hat{u})$ 为新的势函数, 则由(5.9)可知

$$\left(\frac{\partial^2\hat{F}}{\partial\hat{v}^\alpha\partial\hat{v}^\beta}\right)=\left(\frac{\partial^2 F_{\mathrm{DA}_2}}{\partial v^\alpha\partial v^\beta}\right)=\begin{pmatrix}\hat{u} & \hat{v}\\ \hat{v} & 12\hat{u}^2\end{pmatrix},$$

因此 $\hat{F}$ 可以取为

$$\hat{F}=\frac{1}{2}\hat{v}^2\hat{u}+\hat{u}^4,$$

这刚好是 A_2-流形的势函数 F_{A_2}.

事实上, 笔者强烈怀疑(5.14)这个 (广义)Frobenius 流形与 A_2-型奇点有密切联系.

5.2 中心不变量的简便计算

设 $(\mathcal{P}_1,\mathcal{P}_2)$ 是半单的流体力学型双哈密顿结构, 其在局部坐标 v^α 下有表达式

$$\mathcal{P}_a^{\alpha\beta}=g_a^{\alpha\beta}\partial_x+\Gamma^{\alpha\beta}_{\gamma;a}v^\gamma_x\quad(a=1,2).$$

众所周知, $g_a:=(g_a^{\alpha\beta})$ 是平坦的 (伪) 黎曼 (反变) 度量, $\{\Gamma^{\alpha\beta}_{\gamma;a}\}$ 是度量 g_a 的 Levi-Civita 联络的 (反变) Christoeffel 系数 $(a=1,2)$. 关于参数 λ 的方程 $\det(g_2-\lambda g_1)=0$ 的 n 个不同的根 $u^1,...,u^n$ 构成底流形上的一组局部坐标, 称为**正则坐标** (canonical coordinate). 反变度量 $g_a\,(a=1,2)$ 在正则坐标 u^i 下形如下述对角型

$$g_1^{ij}=\delta^{ij}f^i,\quad g_2^{ij}=\delta^{ij}u^if^i,\tag{5.15}$$

其中 $f^1,...,f^n$ 是底流形上的光滑函数.

我们一直习惯用拉丁字母 $i,j,k...$ 表示张量在正则坐标 u^i 下的系数分量, 而用希腊字母 $\alpha,\beta,\gamma...$ 表示张量在一般坐标 v^α 下的系数分量. 此外, 对于 (模长足够大的) 参数 $\lambda\in\mathbb{C}$, 我们记

$$g_\lambda:=g_2-\lambda g_1,\qquad \mathcal{P}_\lambda:=\mathcal{P}_2-\lambda\mathcal{P}_1.\tag{5.16}$$

设 $(\tilde{\mathcal{P}}_1, \tilde{\mathcal{P}}_2)$ 是上述双哈密顿结构 $(\mathcal{P}_1, \mathcal{P}_2)$ 的一个形变, 其形如

$$\begin{aligned}\tilde{\mathcal{P}}_a^{\alpha\beta} =& \ \mathcal{P}_a^{\alpha\beta} + \sum_{s\geq 1} \varepsilon^s \left(\sum_{t=0}^{s+1} P_{s,t;a}^{\alpha\beta} \partial_x^t \right) \\ =& \ g_a^{\alpha\beta}\partial_x + \Gamma_{\gamma;a}^{\alpha\beta} v_x^\gamma \\ & + \varepsilon \left(H_a^{\alpha\beta}\partial_x^2 + \cdots \right) + \varepsilon^2 \left(K_a^{\alpha\beta}\partial_x^3 + \cdots \right) + O(\varepsilon^3),\end{aligned} \tag{5.17}$$

这里的 ε 为无穷小形变参数, $P_{s,t;a}^{\alpha\beta}$ 是底流形的 jet 空间上的齐次微分多项式, 其微分分次为 $s+1-t$. 我们特别关心一阶与二阶形变项的领头项 $H_a = (H_a^{\alpha\beta})$, $K_a = (K_a^{\alpha\beta})$, 并注意到

$$H_a^{\alpha\beta} = -H_a^{\beta\alpha}, \quad K_a^{\alpha\beta} = K_a^{\beta\alpha}.$$

类似地, 对于参数 λ, 我们也记

$$H_\lambda := H_2 - \lambda H_1, \quad K_\lambda := K_2 - \lambda K_1. \tag{5.18}$$

一个重要的结果是, 半单双哈密顿结构 $(\mathcal{P}_1, \mathcal{P}_2)$ 的形变的 Miura 变换等价类能够被一族单变量光滑函数 $c_i = c_i(u)$, $i = 1, 2, ..., n$ 所完全刻画, 这 n 个函数 c_i 称为该形变的**中心不变量**. 换言之, $(\mathcal{P}_1, \mathcal{P}_2)$ 的两个形变是 Miura 变换等价的, 当且仅当它们有相同的中心不变量. 在正则坐标 u^i 下, 中心不变量 c_i 的定义为

$$c_i = \frac{1}{3(f^i)^2} \left(K_2^{ii} - u^i K_1^{ii} + \sum_{k\neq i} \frac{(H_2^{ki} - u^i H_1^{ki})^2}{f^k(u^k - u^i)} \right). \tag{5.19}$$

按道理说, 上式右边应该是底流形上的光滑函数; 然而可以证明 c_i 只与第 i 个正则坐标分量 u^i 有关, 即 $c_i = c_i(u^i)$ 自然被视为单变量函数. 此外, 从上式可见中心不变量只与低阶形变项的领头项 H_a, K_a 有关.

我们在研究半单双哈密顿结构的形变的具体例子时, 往往要具体计算相应的中心不变量. 直接用定义式(5.19)来计算并不是好主意, 其计算量往往巨大而恐怖. 我们迫切需要简洁高效的算法.

感谢 Falqui, Lorenzoni 提供如下方法:

定理 5.9. 记号承上, 引入张量

$$A_\lambda := K_\lambda + \frac{1}{2} H_\lambda^{\mathrm{T}} g_\lambda^{-1} H_\lambda, \tag{5.20}$$

则中心不变量 $c_i = c_i(u^i)$ 满足

$$c_i = -\frac{1}{3f^i} \operatorname{Res}_{\lambda=u^i} \operatorname{tr}\left(g_\lambda^{-1} A_\lambda\right). \tag{5.21}$$

注意 g_λ 与 A_λ 都是 $(2,0)$-型张量, 从而 $g_\lambda^{-1}A_\lambda$ 是 $(1,1)$-型张量, 于是函数 $\operatorname{tr}\left(g_\lambda^{-1}A_\lambda\right)$ 在底流形上整体定义, 不依赖局部坐标选取.

证明. 注意在正则坐标 u^i 下有 $(g_\lambda^{-1})_{ij} = -\frac{\delta_{ij}}{f^i}\frac{1}{\lambda-u^i}$, 从而

$$\begin{aligned}
\operatorname{tr}\left(g_\lambda^{-1}A_\lambda\right) &= \sum_{k=1}^{n} (g_\lambda^{-1})_{kk} A_\lambda^{kk} \\
&= -\sum_{k=1}^{n} \frac{1}{f^k(\lambda-u^k)} \left(K_\lambda^{kk} + \frac{1}{2}\sum_{\ell\neq k} \frac{(H_\lambda^{\ell k})^2}{f^\ell(u^\ell-\lambda)} \right) \\
&= -\sum_{k=1}^{n} \frac{K_\lambda^{kk}}{f^k(\lambda-u^k)} + \frac{1}{2}\sum_{\substack{k,\ell=1\\ k\neq\ell}}^{n} \frac{(H_\lambda^{k\ell})^2}{f^k f^\ell(\lambda-u^k)(\lambda-u^\ell)} \\
&= -\sum_{k=1}^{n} \frac{K_\lambda^{kk}}{f^k(\lambda-u^k)} + \sum_{k=1}^{n}\sum_{\ell\neq k} \frac{(H_\lambda^{k\ell})^2}{f^k f^\ell(u^k-u^\ell)} \frac{1}{\lambda-u^k},
\end{aligned}$$

于是立刻得到

$$\operatorname{Res}_{\lambda=u^i} \operatorname{tr}\left(g_\lambda^{-1}A_\lambda\right)$$

$$= -\frac{1}{f^i}\left(K_2^{ii} - u^i K_1^{ii} + \sum_{k\neq i}\frac{(H_2^{ki} - u^i H_1^{ki})^2}{f^k(u^k - u^i)}\right) = -3f^i c_i,$$

定理得证. □

我们通过具体例子来看如何用公式(5.21)来计算中心不变量.

例题 5.10. 考虑 Boussinesq 方程的双哈密顿结构

$$\tilde{\mathcal{P}}_1 = \begin{pmatrix} & \partial_x \\ \partial_x & \end{pmatrix},$$

$$\tilde{\mathcal{P}}_2 = \begin{pmatrix} 2V\partial_x + V_x + \varepsilon^2\partial_x^3 & 3U\partial_x + 2U_x \\ 3U\partial_x + U_x & \mathcal{Q} \end{pmatrix},$$

其中坐标函数 $V := v^1, U := v^2$, 并且

$$\mathcal{Q} := \frac{16}{3}V\partial_x V + \varepsilon^2\left(\frac{5}{3}V\partial_x^3 + \frac{5}{3}\partial_x^3 V - V_{xx}\partial_x - \partial_x V_{xx}\right) + \frac{\varepsilon^4}{3}\partial_x^5.$$

试计算 $(\tilde{\mathcal{P}}_1, \tilde{\mathcal{P}}_2)$ 的中心不变量.

解. 直接计算可知张量 $g_a, H_a, K_a\,(a = 1, 2)$ 在 $(P, Q) = (v^1, v^2)$ 坐标下的系数矩阵分别为

$$g_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad g_2 = \begin{pmatrix} 2V & 3U \\ 3U & \frac{16}{3}V^2 \end{pmatrix},$$

$$H_1 = H_2 = K_1 = 0, \qquad K_2 = \begin{pmatrix} 1 & 0 \\ 0 & \frac{10}{3}V \end{pmatrix}.$$

于是在 (V, U) 坐标下直接计算可得

$$\operatorname{tr}\left(g_\lambda^{-1}A_\lambda\right) = -\frac{12V^2}{\lambda^2 - 6U\lambda + \left(9U^2 - \frac{32}{3}V^3\right)}.$$

接下来求解关于 λ 的方程 $\det(g_\lambda)=0$ 得正则坐标

$$
\begin{aligned}
u^1 &= 3U - \frac{4\sqrt{6}}{3}V^{\frac{3}{2}},\\
u^2 &= 3U + \frac{4\sqrt{6}}{3}V^{\frac{3}{2}},
\end{aligned}
$$

之后通过坐标变换可得 g_1 在 (u^1,u^2) 坐标下的系数矩阵的对角元

$$
f^1=-12\sqrt{6V},\qquad f^2=12\sqrt{6V}.
$$

最后将相关数据代入公式(5.21), 直接计算得中心不变量

$$
c_1=c_2=\frac{1}{48}.
$$

至少是常中心不变量, 也还行. □

例题 5.11. 考虑 2 分量 Camassa-Holm 方程的双哈密顿结构

$$
\begin{aligned}
\tilde{\mathcal{P}}_1 &= \begin{pmatrix} & \partial_x-\varepsilon\partial_x^2\\ \partial_x+\varepsilon\partial_x^2 & \end{pmatrix},\\
\tilde{\mathcal{P}}_2 &= \begin{pmatrix} 2V\partial_x+V_x & U\partial_x\\ \partial_x U & -2\partial_x \end{pmatrix},
\end{aligned}
$$

其中坐标函数 $V:=v^1, U:=v^2$. 试计算 $(\tilde{\mathcal{P}}_1,\tilde{\mathcal{P}}_2)$ 的中心不变量.

解. 直接计算可知张量 $g_a, H_a, K_a\,(a=1,2)$ 在 $(P,Q)=(v^1,v^2)$ 坐标下的系数矩阵分别为

$$
g_1=\begin{pmatrix}0&1\\1&0\end{pmatrix},\qquad g_2=\begin{pmatrix}2V&U\\U&-2\end{pmatrix},
$$

$$H_1 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad H_2 = K_1 = K_2 = 0,$$

于是在 (V, U) 坐标下直接计算可得

$$\operatorname{tr}\left(g_\lambda^{-1} A_\lambda\right) = -\frac{\lambda^2}{\lambda^2 - 2U\lambda + (4V + U^2)}$$

接下来求解关于 λ 的方程 $\det(g_\lambda) = 0$ 得正则坐标

$$\begin{aligned} u^1 &= U - 2\mathrm{i}V^{\frac{1}{2}}, \\ u^2 &= U + 2\mathrm{i}V^{\frac{1}{2}}, \end{aligned}$$

之后通过坐标变换可得 g_1 在 (u^1, u^2) 坐标下的系数矩阵的对角元

$$f^1 = -2\mathrm{i}V^{-\frac{1}{2}}, \qquad f^2 = 2\mathrm{i}V^{-\frac{1}{2}}.$$

最后将相关数据代入公式(5.21), 直接计算得中心不变量

$$\begin{aligned} c_1 &= -\frac{1}{24}(u^1)^2, \\ c_2 &= -\frac{1}{24}(u^2)^2. \end{aligned}$$

□

例题 5.12. 考虑 Toda 方程簇的双哈密顿结构

$$\begin{aligned} \tilde{\mathcal{P}}_1 &= \begin{pmatrix} 0 & \Lambda - 1 \\ 1 - \Lambda^{-1} & 0 \end{pmatrix}, \\ \tilde{\mathcal{P}}_2 &= \begin{pmatrix} \Lambda \mathrm{e}^u - \mathrm{e}^u \Lambda^{-1} & v(\Lambda - 1) \\ (1 - \Lambda^{-1})v & (\Lambda - \Lambda^{-1}) \end{pmatrix}, \end{aligned}$$

其中坐标函数 $v := v^1, u := v^2$, 而 $\Lambda := \mathrm{e}^{\varepsilon \partial_x}$ 为平移算子. 试计算 $(\tilde{\mathcal{P}}_1, \tilde{\mathcal{P}}_2)$ 的中心不变量.

解. 直接计算可知张量 $g_a, H_a, K_a\,(a=1,2)$ 在 $(v,u)=(v^1,v^2)$ 坐标下的系数矩阵分别为

$$g_1=\begin{pmatrix}0&1\\1&0\end{pmatrix},\qquad g_2=\begin{pmatrix}2\mathrm{e}^u&v\\v&2\end{pmatrix},$$

$$H_1=\begin{pmatrix}0&\frac{1}{2}\\-\frac{1}{2}&0\end{pmatrix},\qquad H_2=\begin{pmatrix}0&\frac{1}{2}v\\-\frac{1}{2}v&0\end{pmatrix},$$

$$K_1=\begin{pmatrix}0&\frac{1}{6}\\\frac{1}{6}&0\end{pmatrix},\qquad K_2=\begin{pmatrix}\frac{1}{3}\mathrm{e}^u&\frac{1}{6}v\\\frac{1}{6}v&\frac{1}{3}\end{pmatrix},$$

于是在 (v,u) 坐标下直接计算可得

$$\mathrm{tr}\left(g_\lambda^{-1}A_\lambda\right)=\frac{1}{3}-\frac{(\lambda-v)^2}{4\left(\lambda^2-2v\lambda+(v^2-4\mathrm{e}^u)\right)}$$

接下来求解关于 λ 的方程 $\det(g_\lambda)=0$ 得正则坐标

$$\begin{aligned}u^1&=v-2\mathrm{e}^{\frac{u}{2}},\\u^2&=v+2\mathrm{e}^{\frac{u}{2}},\end{aligned}$$

之后通过坐标变换可得 g_1 在 (u^1,u^2) 坐标下的系数矩阵的对角元

$$f^1=-2\mathrm{e}^{\frac{u}{2}},\qquad f^2=2\mathrm{e}^{\frac{u}{2}}.$$

将相关数据代入公式(5.21)可得中心不变量

$$c_1=c_2=\frac{1}{24}.$$

果然是 $\frac{1}{24}$, 如此甚好. □

例题 5.13. 考虑 Ablowitz-Ladik 方程簇的双哈密顿结构

$$\tilde{\mathcal{P}}_1 = \begin{pmatrix} Q\Lambda^{-1} - \Lambda Q & (1-\Lambda)Q \\ Q(\Lambda^{-1}-1) & 0 \end{pmatrix},$$

$$\tilde{\mathcal{P}}_2 = \begin{pmatrix} 0 & P(\Lambda-1)Q \\ Q(1-\Lambda^{-1})P & Q(\Lambda-\Lambda^{-1})P \end{pmatrix},$$

其中坐标函数 $P := v^1$, $Q := v^2$, 而 $\Lambda := \mathrm{e}^{\varepsilon\partial_x}$ 为平移算子. 试计算 $(\tilde{\mathcal{P}}_1, \tilde{\mathcal{P}}_2)$ 的中心不变量.

解. 直接计算可知张量 $g_a, H_a, K_a\,(a=1,2)$ 在 $(P,Q)=(v^1,v^2)$ 坐标下的系数矩阵分别为

$$g_1 = \begin{pmatrix} -2Q & -Q \\ -Q & 0 \end{pmatrix}, \qquad g_2 = \begin{pmatrix} 0 & PQ \\ PQ & 2Q^2 \end{pmatrix},$$

$$H_1 = \begin{pmatrix} 0 & -\frac{1}{2}Q \\ \frac{1}{2}Q & 0 \end{pmatrix}, \qquad H_2 = \begin{pmatrix} 0 & \frac{1}{2}PQ \\ -\frac{1}{2}PQ & 0 \end{pmatrix},$$

$$K_1 = \begin{pmatrix} -\frac{1}{3}Q & -\frac{1}{6}Q \\ -\frac{1}{6}Q & 0 \end{pmatrix}, \qquad K_2 = \begin{pmatrix} 0 & \frac{1}{6}PQ \\ \frac{1}{6}PQ & \frac{1}{3}Q^2 \end{pmatrix},$$

于是在 (P,Q) 坐标下直接计算可得

$$\mathrm{tr}\left(g_\lambda^{-1}A_\lambda\right) = \frac{1}{12} - \frac{Q\lambda}{\lambda^2 + (2P-4Q)\lambda + P^2}.$$

接下来求解关于 λ 的方程 $\det(g_\lambda)=0$ 得正则坐标

$$u^1 = -P + 2Q - 2\sqrt{Q^2 - PQ},$$
$$u^2 = -P + 2Q + 2\sqrt{Q^2 - PQ},$$

之后通过坐标变换可求得度量 g_1 在 (u^1, u^2) 坐标下的系数矩阵的对角元 f^1, f^2, 其表达式复杂, 这里从略. 最后将相关数据代入公式(5.21)并交给计算机暴力计算, 求得中心不变量

$$c_1 = c_2 = \frac{1}{24}.$$

果然是 $\frac{1}{24}$, 如此甚好. $\square$