群论在概率中的应用

Group Theory in probability

数学科学学院 概率统计系

张泽宇 PB12001071

刘党政 副教授

二〇一六年五月

中国科学技术大学

University of Science and Technology of China

本科毕业论文

A Dissertation for the Bachelor's Degree

群论在概率中的应用

Group Theory in probability

姓　　名	张泽宇
B.S. Candidate	Zeyu Zhang
导　　师	刘党政 副教授
Supervisor	A/Prof.Dangzheng Liu

二〇一六年五月

May 2016

中国科学技术大学

学士学位论文

题	目	群论在概率中的应用
院	系	数学科学学院 概率统计系
姓	名	张泽宇
学	号	PB12001071
导	师	刘党政 副教授

二〇一六年五月

University of Science and Technology of China

A Dissertation for the Bachelor's Degree

Group Theory in probability

B.S. Candidate Zeyu Zhang

Supervisor A/Prof.Dangzheng Liu

Hefei, Anhui 230026, China

May 2016

致　　谢

在本科的最后阶段，我选择了概率统计作为研究方向，而确实在概率中有很多吸引人的问题及结论，我十分希望能够与大家分享一些相关内容，这也是本文撰写的目的之一，诚然，本文的完成离不开各位老师的指导和同学们之间的帮助。

首先我想感谢导师刘党政副教授对我研究方向的指导。刘老师是带领我走近概率论的领路人，也正是概率论中各种广泛的应用和奇妙的结论让我选择了概率论作为研究方向。在学习过程中刘老师多次给出了指导和帮助，在与刘老师的电邮交流中，我也明确了相关学习的进程和步骤。

然后我想感谢班主任夏晶老师和张永兵副教授对我的关怀和教导。夏晶老师在本科四年生活中给予了我很多生活和学业上的帮助，让我度过了一段美好而轻松的大学生活，而张永兵老师对我学科知识的教育以及平日里学习数学的方法的交流给了我继续进行科学研究的动力。我能有幸获得这段科研经历很大程度上是因为他们对我的帮助。

感谢陈卿教授，李皓昭副教授以及赵立丰副教授，他们在我之后出国深造上给了不少建议及帮助。

最后，感谢父母以及其余家人对我的理解与支持。

张泽宇

2016 年 5 月 26 日

目　录

摘　要

在现代概率统计中，代数中的群表示论具有十分重要的作用。在很多实际问题中，这些问题都会具有一些群论的背景。本文主要目的是利用一些群表示论的结果去研究一些与群相关的概率问题，尤其是群上的随机游走。我们首先会在第一章中介绍一些群表示论的相关概念的基本定义及结论，进而在第二章定义群上概率测度直接的距离，再给出“close to random”的概念，最后利用群表示论的知识给出群上随机游走的相关结论。

关键字:　群表示论 概率论 随机游走 概率测度

Abstract

In the modern probability theory and statistics, algebra and group representation theory play a very important role. In many practical problems, those problems have some relative background with group theory.
This thesis is aimed to solve some problem in probability, especially the random walk in group. The first chapter will introduce some relative concept and conclusion about group theory. In the second chapter, we will give a measure of variables and what is "close to random". Further more, some examples and conclusion about random walk in group will be given.

Keywords: group representation theory, probability theory, random walk, probability measure

第一章　前言

在实际生活中，很多问题的结构其实都与群论有关，举个例子 [1]，考虑一份人数为 500 人份的关于他们心中 5 个不同的巧克力品牌的排名的问卷调查。这个排名可以看做是作用在 5 个物体上的置换群 S_5, 自然的，对于这类问题，人们便可以利用群论的知识做出各种不同的分析。除了这些问题外，群上的概率的卷积形式提示我们，对于 n 步概率我们可以利用 n 次卷积来研究，同时我们又注意到在群表示论中，群上的函数都可由其上的所有不可约表示所张成，同时我们注意到，很多概率问题都具有群的结构，比如对于圆环上的随机游走，我们可以看做是 s_p 上的 n 步概率。本文主要对 Persi Diaconis 的 Group Representation Theory in Probability and Statistics[2] 中关于群表示论在随机游走中的应用进行了归纳总结，在本文第一章中，我们将介绍群表示论的相关定义及一些重要定理，以便为后文做好铺垫。在第二章中，我们开始介绍如何利用群表示论的相关知识对随机变量距离进行估计，这样我们便能得知什么时候一个 n 步概率会接近均匀分布 [3]。

第二章　群表示论及特征

一、　定义及例子

定义 2.0.1. 设 G 是一个乘法群，运算规则为 $S*T \to ST$，单位元记为 id，逆元记为 s^{-1}。我们称 ρ 为群 G 上的一个表示，当 ρ 把 G 中的每个元素都映为一个可逆矩阵，且满足 $\rho(st) = \rho(s)\rho(t)$。这样，我们可以把 ρ 看做是一个 G 到 $GL(V)$ 的一个同态，其中 $GL(V)$ 是向量空间 V 上的所有可逆线性变换组成的乘法群。向量空间 V 的维数 d_ρ 称为表示 ρ 的维数。

定义 2.0.2. 如果 W 是向量空间 V 在 G 下的**不变子空间**（$i.e$，$\rho(s)W \subset W$ 对所有 $s \in G$ 成立），则限制在 W 上的表示 ρ 给出了一个子表示。显然，零空间和全空间是 ρ 在 V 上的两个平凡的子表示。如果 ρ 没有非平凡的子表示，则称 ρ 是不可约的。

定义 2.0.3. 设 P 和 Q 是有限群 G 上的概率，则 $P(s) \geq 0, \sum_s P(s) = 1$。定义 $\boldsymbol{P}$ **和** $\boldsymbol{Q}$ **的卷积**：$P * Q = \sum_t P(st^{-1})Q(t)$，再定义群 G 上的均匀分布：$U(s) = 1/|G|$，注意到 $U * U = U$，对任意 G 上的概率 P，$U * P = U$。

定义 2.0.4. 令 P 是有限群 G 上的一个概率，则 $\boldsymbol{P}$ **在表示** ρ **下的傅里叶变换**为

$$\hat{p}(\rho) = \sum_s P(s)\rho(s).$$

对于一般的函数 P 我们也类似定义其在 ρ 下的傅里叶变换。

二、　基本理论

定理 2.0.1. 令 $\rho : G \longrightarrow GL(V)$ 是 G 在 V 上的一个线性表示，令 W 是 V 在 G 下的一个不变子空间. 则存在 W 的一个补空间 W^0，且 W^0 在 G 下不变。

证： 令 $<,>_1$ 是 v 中的内积，定义一个新的内积如下 $< u,v >= \sum_s < \rho(s)u, \rho(s)v >_1$. 则 $< u,v >=< \rho(s)u, \rho(s)v >$。W 在 V 中的正交补空间即为 W^0。

注解 2.0.1. 正如上面证明中所讨论的，内积 $<,>$ 具有不变性，这意味着，如果 e_i 是内积 $<,>$ 的一组单位正交基，则 $< \rho(s)e_i, \rho(s)e_j >= \delta_{ij}$，这也意味着 $\rho(s)$ 是单位阵，故我们可以假设我们的表示是单位的。

注解 2.0.2. 对于定理 *1.0.1* 中的不变子空间 W 和 W_0，我们称 V 可以记为 W 和 W_0 的直和，记为 $V = W \oplus W_0$。

定理 2.0.2. 每个表示都可以分为一些不可约表示的直和。

证: 对定理 1 用归纳法即证。

定义 2.0.5. 对于任意一个表示 ρ，我们记 $\chi_\rho(s) = Tr\ \rho(s)$, 我们称 χ_ρ 是**表示 ρ 的特征** ***(Character)****[4]*，由迹的不变性，我们知道 $\chi_\rho(s)$ 与 V 的基的选取无关。故我们有如下关于特征的性质。

命题 2.0.1. 设 χ 是表示 ρ 的特征，且表示 ρ 的维数为 d。则：
(1): $\chi(id) = d$;
(2)$\chi(s^{-1}) = \chi(s)^*$;
(3)$\chi(tst^{-1}) = \chi(s)$.

证：
(1): 由迹的性质知成立。
(2): 因为 G 是有限群，故 $\rho(s^a) = I$ 对某个 a 成立。由此可知 $\rho(s)$ 的特征根 λ_i 是 1 的单位根。则

$$\begin{aligned}\chi(s)^* &= Tr\ \rho(s)^* \\ &= \sum \lambda_i^* = \sum 1/\lambda \\ &= Tr\ \rho(s)^{-1} = Tr\ \rho(s^{-1}) = \chi(s^{-1})\end{aligned}$$

(3): 由 Tr(AB)=Tr(BA) 知成立。

命题 2.0.2. 令 χ_1, χ_2 分别是 $\rho_1 : G \longrightarrow GL(V_1), \rho_2 : G \longrightarrow GL(V_2)$ 的特征，则 $\rho_1 \oplus \rho_2 = \chi_1 + \chi_2$。

下面我们考虑在同一个群上的两个表示，一个是在空间 V 上的表示 ρ，另一个是在空间 W 上的表示 τ。我们称他们是**等价的 (equivalent)**如果存在一个一一的从 V 映到 W 的线性映射 f 满足：$\tau_s \circ f = f \circ \rho_s$。

定理 2.0.3 (Schur 定理). *令 $\rho^1 \longrightarrow GL(V_1), \rho^2 \longrightarrow GL(V_2)$ 是两个 G 上的不可约表示，令 f 是从 V_1 到 V_2 的线性映射且满足*

$$\rho_s^2 \circ f = f \circ \rho_s^1$$

对任意 s 成立，则：
(1): 如果 ρ^1, ρ^2 不等价，则 $f=0$.
(2): 如果 $V_1 = V_2, \rho^1 = \rho^2$, 则 $f = c * id$, 其中 c 是常数.

证： 注意到 f 的像与核都是 G 下的不变子空间，对核，如果 $f(v) = 0$, 则 $f\rho_s^1(v) = \rho_s^2 f(v)$, 故 $\rho_s^1(s)$ 在核里。对于 f 的像 $w = f(v)$,$\rho_s^2(w) = f\rho_s^1(v)$ 在像里，又 ρ_1 不可约，故核空间和像空间要么是零空间要么是全空间。
对 (1) 假设 $f \neq 0$，则 Ker=0, 像空间为全空间，故 f 为双射，这与 ρ_1, ρ_2 不等价矛盾。
对 (2)，$f = 0$ 时结论成立，当 $f \neq 0$ 时，f 有非零特征值 λ，则映射 $f^1 = f - \lambda I$ 满足 $\rho_s^2 f^1 = f^1 \rho_s^1$, 且 f_1 的核是非平凡的，故 $f^1 \equiv 0$。

注解 2.0.3. *群 G 上的一致分布定义为 $U(s) = 1/|G|$, 对于平凡表示 ρ，$\hat{U}(\rho) = 1$, 对于其他非平凡不可约表示 $\hat{U}(\rho) = 0$.*

推论 2.0.1. *令 h 是任意从 h_1 到 h_2 的线性映射。令*

$$h^0 = \frac{1}{|G|} \sum (\rho_t^2)^{-1} h \rho_t^1$$

则
(1): 如果 ρ^1, ρ^2 不等价，则 $h^0 = 0$。
(2): 如果 $V_1 = V_2$,$\rho^1 = \rho^2$，则 $h^0 = c * id, c = Tr\ h/d_\rho$。

证： 容易验证 h_0 满足 Schur 定理中 f 的条件，故由 Schur 定理 [5] 知成立，对 h_0 表达式的两端取 Tr，算得 $c = Tr\ h/d_\rho$。

假设推论 1 中的 ρ_1, ρ_2 矩阵形式为

$$\rho_t^1 = (r_{i_1j_1}(t)), \rho_t^2 = (r_{i_2j_2}(t))$$

线性映射 h^0, h 由 $x_{i_2i_1}, x^0_{i_2i_1}$ 确定。则

$$x^0_{i_2i_1} = \frac{1}{|G|}\sum_{tj_1j_2} r_{i_2j_2}(t^{-1})x_{j_2j_1}r_{j_1i_1}(t)$$

在推论 1 中的情形 (1) 下，$h^0 \equiv 0$ 对所有 h 成立当且仅当 $x_{j_2j_1}$ 的系数全为 0，故我们有如下推论：

推论 2.0.2. *在情形 (1) 下*

$$\frac{1}{|G|}\sum_{t\in G} r_{i_2j_2}(t^{-1})r_{j_1i_1}(t) = 0$$

对所有 i_1, i_2, j_1, j_2 成立。

推论 2.0.3. *在情形 (2) 下*

$$\frac{1}{|G|}\sum_{t\in G} r_{i_2j_2}(t^{-1})r_{j_1i_1}(t) = \begin{cases} \frac{1}{d_\rho} & i_1 = i_2, j_1 = j_2 \\ 0 & \text{其他情况} \end{cases}$$

证：在 (2) 下，$h^0 = \lambda I, x^0_{i_2i_1} = \lambda\delta_{i_2i_1}, \lambda = \frac{1}{d_\rho}\sum \delta j_2j_1x_{j_2j_1}$，即

$$\frac{1}{|G|}\sum_{tj_1j_2} r_{i_2j_2}(t^{-1})x_{j_2j_1}r_{j_2i_1}(t) = \frac{\delta_{i_1i_2}}{d_\rho}\sum_{j_1j_2}\delta_{j_1j_2}x_{j_1j_2}$$

由 h 的任意性，上式两端 $x_{j_2j_1}$ 系数相同。由此即得结论。

三、 特征的正交性

我们引入函数之间的内积 $(\phi|\psi) = \frac{1}{|G|}\sum \phi(t)\psi(t)^*$, 其中 $\phi(t)^*$ 表示复共轭，又由 Remark1.0.1 知，所有表示都可以假设是单位的，故 $r(s)^* = r(s)^{-1}$ 其中 r 为任意群 G 上的一个表示。我们由如下定理：

定理 2.0.4. 不可约表示的特征构成一组标准正交基。

证： 令 ρ 是不可约表示，χ 是其特征，且其矩阵形式为 $\rho_t = r_{ij}(t)$. 故 $\chi(t) = \sum r_{ii}(t), (\chi|\chi) = \sum_{i,j}(r_{ii}|r_{jj})$. 由推论三知 $(r_{ii}|r_{jj}) = \frac{1}{d_\rho}\delta_{ij}$. 如果 χ, χ' 是两个不等价表示的特征，则 $(\chi|\chi') = \sum_{ij}(r_{ii}|r'_{jj})$ 由推论二知 $(r_{ii}|r'_{jj}) = 0$.

定理 2.0.5. 令 ρ 是群 G 的一个表示，其特征为 ϕ,V 为其表示空间，设 V 可直和分解为以下不可约表示：

$$V = W_1 \oplus \cdots \oplus W_k,$$

则如果 W 是一个不可约表示且特征为 χ，则所有 W_i 中等同于 W 的表示的个数为 $(\phi|\chi)$.

证： 令 W_i 的特征为 χ_i, 则由性质二 $\phi = \chi_1 + \cdots + \chi_k$, 又由定理三知，$(\chi_i|\chi) = 1$ 当且仅当 $\chi_i = \chi$。

注解 2.0.4. 由以上推导我们可以看出，表示可以由其特征唯一确定（在同态意义下）。

定理 2.0.6. 设 ϕ 是某个表示的特征，则 $(\phi|\phi) = 1$ 当且仅当该表示是不可约的。

证： 注意到 $V = m_1W_1 \oplus \cdots \oplus m_nW_n$ 这里 m_i 表示 V 的直和分解中包含 m_i 个 W_i（在同态意义下），则 $(\phi|\phi) = \sum m_i^2$，由此知定理成立。

四、 正则表示的分解和 Fourier 逆变换

定义 2.0.6. 令 e_s 构成向量空间的一组基，$s \in G$，定义 $\rho_s(e_t) = e_{st}$, 我们称这样的表示为**正则表示**。

命题 2.0.3. 正则表示的特征 r_G 由下式确定:

$$r_G(1) = |G|$$

$$r_G(s) = 0, s \neq 1$$

。

证： $\rho_1(e_s) = e_s$ 故 $\mathrm{Tr}\rho_1 = |G|$. 当 $s \neq 1$ 时 $\rho_s e_t = e_{st} \neq e_t$ 故 ρ_s 对角元全为 0。

推论 2.0.4. *正则表示的直和分解中不可约表示 W_i 的个数恰好为其维数 d_i。*

证：

$$\begin{aligned}(r_G|\chi_i) &= \frac{1}{|G|}\sum_{s\in G} r_G(s)\chi_i^*(s)\\ &= \chi_i^*(1)\\ &= d_i\end{aligned}$$

推论 2.0.5. .

a): 维数 d_i 满足 $\sum d_i^2 = |G|$

b): 若 $s \in G, s \neq 1$，$\sum d_i\chi_i(s) = 0$

证: 由推论 5 知 $r_G(s) = \sum d_i\chi_i(s)$。令 s=1, 则得 a), 令 s 为 G 中任意非 id 的元素则得 b).

定理 2.0.7. .

a)Fourier 逆变换定理. 令 f 是 G 上的函数，则

$$f(s) = \frac{1}{|G|}\sum d_i\, Tr(\rho_i(s^{-1})\hat{f}(\rho_i))$$

b)Plancherel 法则. 令 f 和 h 是 G 上的函数，则

$$\sum f(s^{-1})h(s) = \frac{1}{|G|}\sum d_i\, Tr(\hat{f}(\rho_i)\hat{h}(\rho_i))$$

证.

a) 注意到，等式左右两端对 f 是线性，故只需验证 $f = \delta_{st}$ 时结论是否成立即可。(因为 $f(s_i) = \sum_{j=1}^{n} f(s_i)\delta_{s_i s_j}$), 则

$$\hat{f}(\rho_i) = \rho_i(t),$$

等式右端为 $\frac{1}{|G|}\sum d_i\chi_i(s^{-1}t)$, 带入验证即得结论。
b) 同样，等式两端对 f 是线性的，故只需对 $f=\delta_{st}$ 时验证结论是否成立即可，即

$$h(t^{-1})=\frac{1}{|G|}\sum d_i\mathrm{Tr}(\rho_i(t)\hat{h}(\rho_i))$$

此即 a) 中结论。

五、 不可约表示的个数

定义 2.0.7. *共轭关系在群上的划分中起到了关键的作用，我们称 s 和 t 是共轭的，当且仅当存在群 G 中的某元素 u 使得 $usu^{-1}=t$ 成立，在这种共轭关系下，我们就可以把群分成不同的共轭等价类。如果函数 f 作用在 G 的每个共轭类下均为常数则我们称 f 为*类函数（***class function***）.

命题 2.0.4. *令 f 是 G 上的一个类函数，令 $\rho:G\to GL(V)$ 是某个 G 上的不可约表示，则 $\hat{f}(\rho)=\lambda I$ 且*

$$\lambda=\frac{1}{d_\rho}\sum f(t)\chi_\rho(t)=\frac{|G|}{d_\rho}(f|\chi_\rho^*)$$

证：

$$\begin{aligned}\rho_s\hat{f}(\rho)\rho_s^{-1}&=\sum f(t)\rho(s)\rho(t)\rho(s^{-1})\\&=\sum f(t)\rho(sts^{-1})\\&=\sum f(sts^{-1})\rho(sts^{-1})\\&=\hat{f}(\rho)\end{aligned}$$

又由 Schur 定理知 $\hat{f}(\rho)=\lambda I$, 再对等式两端取迹即得 λ。

定理 2.0.8. *不可约表示的特征 $\chi_1,\cdots,\chi_h$ 构成了所有类函数的一组标准正交基。*

证: 由表示的特征的性质我们知道，特征是类函数，且由定理 3 知他们是标准正交的，下面只需说明只需这些 $\chi_1, \cdots, \chi_h$ 便足够，否则，存在 χ_{h+1} 使得

$$\begin{aligned}(\chi_i, \chi_{h+1}) &= 0 \\ &= \frac{1}{|G|}\sum \chi_i(t)\chi_{h+1}(t^{-1}) \\ &= \frac{1}{|G|}\sum \chi_i(t)\chi_{h+1}(t^{-1}tt^{-1}) \\ &= (\chi_i, \chi_{h+1}^*)\end{aligned}$$

, 由推论 7 知 $\hat{\chi}_{h+1}(\rho) = 0$, 再由 Fourier 逆变换定理知 $\chi_{h+1} = 0$。

定理 2.0.9. 不可约表示的个数等于共轭等价类的个数。

证：定理 6 说明不可约表示的个数 h 等于所有 g 上的类函数构成的函数空间的维数，同时，对于类函数来说，其在每个共轭类上都有一个确定的值，故类函数空间的维数即共轭类的个数。

定理 2.0.10. 下列性质等价
a)G 是阿贝尔群.
b) 所有 G 的不可约表示的维数为 *1.*

证：由 G 是阿贝尔群知一共有 $|G|$ 个共轭类，同时 $\sum d_\rho^2 = |G|$, 由定理 7 知，不可约表示的个数为 $|G|$，故 $d_\rho = 1$。反过来，若 $d_\rho = 1$, 则由 $|G|$ 个不可约表示，即有 $|G|$ 个共轭类, 故 G 是阿贝尔群。

例 2.0.1. 我们下面讨论 Z_n 上的不可约表示，这里 Z_n 表示整数模 n 构成的, 加法群。
注意到 Z_n 是阿贝尔群，故所有不可约表示的维数为 *1*，由同态知 $\rho(k) = \rho(1)^k, \rho(1)^n = 1$，故每个不可约表示 ρ 由其在 id 上的像确定，且 $\rho(1)$ 是 *1* 的 n 次单位根，即 $e^{2\pi ij/n}$, 由其确定的不可约表示为 $\rho_j(k) = e^{2\pi ijk/n}$, 这样我们就找出了所有 Z_n 上的不可约表示。对于 Z_n 上的任意函数 f，$\hat{f}(j) = \sum_k f(k)e^{2\pi ijk/n}$, 由傅里叶逆变换知 $f(k) = \frac{1}{n}\sum_j \hat{f}(j)e^{-2\pi ijk/n}$.

第三章　群上的随机游走

六、　问题的背景及提出

我们把群 Z_p 看做是 p 个点均匀分布在一个圆周上，这上面最简单的随机游走即从某一点开始，每次要么向左或者向右且概率都是二分之一，自然地，我们会关心如下问题：需要多少步使得从某一点开始到达指定位置？需要多少步才能走过圆周上的每个点？多少步之后该点的分布接近均匀分布（即到每个点概率相同）?（主要前两个问题的步数是指期望）下面的讨论会告诉我们这三个问题的答案都是 p^2. 除了这种最简单的随机游走外，我们还可以考虑下面这种随机游走：$X_{k+1} = aX_k + b(mod\ p)$ 这里 P 是一个确定的数，且 $X_0 = 0$，通常人们在生成伪随机序列时会用到这种随机游走，选择合适的 a 和 b 即可使得 $X_0, \cdots, X_n$ 是一列伪随机序列。更一般的，我们可以令 a 和 b 是某些随机变量，我们可以通过研究模 p 的仿射群去研究他们的性质，目前来说，对于 a 是随机变量的情况人们还未找到很好的办法研究序列 X_n 的性质，但是对于确定的 a，若 b 是随机变量则我们可以研究序列 X_n 何时接近均匀分布，后文中会给出这个答案 [6]。

除了研究 Z_p 上的随机游走，我们还关心 d 维立方体上的随机游走（即 d 维随机游走），即群 Z_2^d 上的随机游走。对于起始于 d 维立方体某一点的随机游走，下一步到邻接的 d 个定点和保持不动的概率同为 $\frac{1}{d+1}$, 自然地，我们就会想知道，多少步之后这个点最后所处的位置接近均匀分布？

实际问题中，洗牌中的每一次洗牌也可以看做是作用了一次置换群的某个元素，如果我们定义最终洗牌洗匀等价于最终分布接近均匀分布，那么我们会发现，平时我们的对半洗牌方式（在完美的洗牌模型下，我们假设将牌分为数量相等的两堆，且洗牌时恰好保证 a 堆中的牌下面是 b 堆中的牌）下差不多 7 次洗牌即可把 52 张牌洗匀。

七、 基本定义及定理

我们接下来来定义什么是接近均匀，并引入随机变量间的距离。

定义 3.0.8. 令 G 是有限群，P 和 Q 是 G 上的随机变量，定义如下距离

$$\|P-Q\| = \max_{A\subset G} |P(A)-Q(A)| = \frac{1}{2}\sum_{s} \|P(s)-Q(s)\|$$

注解 3.0.5. 这样的距离可以在任意的可测群上推广，使得 G 变成 $Banach$ 空间。对于 G 是紧的情形下，这个测度是有界连续函数且 $\|\ \|$ 是对偶范数。

注解 3.0.6. 考虑 S_n 上的随机游走。这可以看做是对一副由 n 张牌构成的扑克进行的洗牌（洗牌一次可看做是 S_n 上的一个元素作用在这副牌上），对于已经洗好的一副牌，我们将其全部背面朝上，每次我们翻开一张牌，并猜这张牌是多少，如果这副牌已经被洗匀那么猜对正确牌数的期望是

$$H_n = 1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n}$$

如果没有洗匀，那么这个期望值会增加，这样我们就可以定义什么是接近均匀，即概率距离 $\|P-U\|$ 充分小即可。

注解 3.0.7. 除了上面定义的度量外，我们还有如下两种与其等价的度量：
Hellinger 距离 - $d_H(P,Q) = \sum_s (P(s)^{\frac{1}{2}} - Q(s)^{\frac{1}{2}})^2$
Kullback-Leiber 距离 - $I(P,Q) = \sum_s P(s)\log[P(s)/Q(s)]$
满足

$$\frac{d_H}{2} \leqslant \|\ \| \leqslant \sqrt{d_H(1-d_H/4)} \leqslant \sqrt{d_H}$$

$$\sqrt{2}\|\ \| \leqslant \sqrt{I}$$

回忆之前我们定义的群 G 上两个概率测度 P 和 Q 的卷积 $P*Q(s) = \sum_t P(st^{-1})Q(t)$, 注意到 $st^{-1}*t = s$, 也就是说卷积的概率意义 $P*Q(s)$ 是指从 P 中取出任意元素 a，再独立的从 Q 中取出某个元素 b 使得 $ab = s$ 的概率。由乘法原理，自然地，p^{*n} 表示 n 次操作后的概率分布，又有上文中定义的距离，我们很自然的会关心什么时候有 $\|P^{*n}-U\| < \varepsilon$, 我们不加证明的引入如下定理.

定理 3.0.11 (Koss). 令 G 是一个紧群，设 P 是 G 上的一个概率测度且满足存在 $n_0, c, 0 < c < 1$, 对于所有 $n > n_0$ 有：

$$P^{*n}(A) > cU(A)对所有开集\ A$$

则对所有的 k

$$\|P^{*k} - U\| \leqslant (1-c)^{[k/n_0]}$$

定理 3.0.12 (上界引理). 令 Q 是有限群 G 上的概率测度则

$$\|Q - U\|^2 \leqslant \frac{1}{4}\sum d_\rho Tr(\hat{Q}(\rho)\hat{Q}(\rho)^*)$$

这里求和是对所有非平凡不可约表示求和。

证：

$$\begin{aligned} 4\|Q-U\|^2 &= \{\sum_s |Q(s)-U(s)|\}^2 \\ &\leqslant |G|\sum |Q(s)-U(s)|^2 \\ &= \sum d_\rho \mathrm{Tr}(\hat{Q}(\rho)\hat{Q}(\rho)^*) \end{aligned}$$

其中，第一个不等号是 Cauchy 不等式，第二个等号是在 Plancherel 法则中令 $f \equiv 1$,$h = (Q-U)(Q-U)^*$, 且 $\hat{Q}(\rho) = 1, \rho = id, \hat{U}(\rho) = 0, \rho \neq id.$

八、 圆上的随机游走

考虑 Z_p, 模 p 的加法群, 定义 $P(1) = P(-1) = \frac{1}{2}, P(j) = 0$其他情况.

定理 3.0.13. 对 $n \geqslant p^2, p$ 为奇数且大于 7 有

$$\|P^{*n} - U\| \leqslant e^{-an/p^2}, a = \pi^2/2$$

证：在第一章最后的例子中，我们讨论了 Z_p 的所以不可约表示，为 $\rho_j(k) = e^{2\pi ijk/p}$，故

$$\begin{aligned} \hat{P}(\rho_j) &= \sum_k (P(k)\rho(k)) \\ &= \frac{1}{2}(e^{\frac{2\pi ij}{p}} + e^{\frac{-2\pi ij}{p}}) \\ &= \cos(2\pi j/p) \end{aligned}$$

下面先引入一个引理：

引理 3.0.1. *令 ρ 是任意表示,P,Q 是群 G 上的两个概率测度则:*

$$P \hat{*} Q(\rho) = \hat{P}(\rho)\hat{Q}(\rho)$$

证：

$$\begin{aligned}
P \hat{*} Q(\rho) &= \sum_s P * Q(s)\rho(s) \\
&= \sum_s \sum_t P(st^{-1})Q(t)\rho(s) \\
&= \sum_s \sum_t P(st^{-1})Q(t)\rho(st^{-1})\rho(t) \\
&= \sum_t \sum_s P(st^{-1})\rho(st^{-1})Q(t)\rho(t) \\
&= \sum_t \sum_v P(v)\rho(v)Q(t)\rho(t) \\
&= \hat{P}(\rho)\hat{Q}(\rho)
\end{aligned}$$

回到原命题证明。由上界引理知：

$$\begin{aligned}
\|P^{*n} - U\|^2 &\leqslant \frac{1}{4}\sum Tr(\hat{P^{*n}}(\rho)\hat{P^{*n}}(\rho)^*) \\
&= \frac{1}{4}\sum \{\hat{P}(\rho)\}^{2n} \quad \text{由引理知} \\
&= \frac{1}{4}\sum_{j=1}^{p-1} \cos(2\pi j/p)^{2n} \\
&= \frac{1}{2}\sum_{j=1}^{(p-1)/2} \cos(2\pi j/p)^{2n}
\end{aligned}$$

下面我们只需要对上面这个 cos 求和估计其上界即可，令 $h(x) = \log(e^{x^2/2\cos x}, h'(x) = x - \tan x \leqslant 0; h(x) \leqslant h(0) = 0$ 故我们有：

$$\cos x \leqslant e^{-x^2/2} \quad x \in [0, \pi/2]$$

利用上式我们有：

$$\begin{aligned}\|P^{*n}-U\|^2 &\leqslant \frac{1}{2}\sum_{j=1}^{(p-1)/2} e^{-\pi^2 j^2 n/p} \leqslant \frac{1}{2}e^{-\pi^2 n/p^2}\sum_{j=1}^{\infty} e^{-\pi^2(j^2-1)n/p^2} \\ &\leqslant \frac{1}{2}e^{-\pi^2 n/p}\sum_{j=0}^{\infty} e^{-3\pi^2 jn/p^2} \\ &= \frac{1}{2}\frac{e^{-\pi^2 n/p^2}}{1-e^{-3\pi^2 n/p^2}}\end{aligned}$$

又对任意 n 和奇数 p，若 $n \geqslant p^2$ 则 $[2(1-e^{-3\pi^2}]^{-1} < 1$ 这样我们就证明了结论。

九、 Z_2^d 上的随机游走

我们先来定义群 Z_2^d，Z_2^d 可以看做是 n 维立方体的 2^d 个定点，故我们可以用二进制去表示所有顶点，记这些顶点为

$$\underbrace{(0,0,\cdots,0)}_{\text{d 个}},\cdots,\underbrace{(1,1,\cdots,1)}_{\text{d 个}}$$

, 他们之间的运算为位运算, 即对应位置的数相加再模 2，这样便构成了一个加法群，每个元素的补是其位运算的补，单位元为 $(0,0,\cdots,0)$ 显然，这是一个阿贝尔群，故其所有不可约表示都是 1 维的，且有 2^d 个。

我们可以构造如下 d^2 个不可约表示：对任意 Z_2^d 的元素 y，设 $\rho_y(x) = (-1)^{y\cdot x}$, 这里 $(-1)^{x\cdot y}$ 定义如下：设 y 的 $y_1,\cdots,y_s$ 位全为 1，其余位为 0，$(-1)^{x\cdot y} = \sum_{j=1}^{s}(-1)^{x_{y_j}}$，这里 x_{y_j} 表示 x 的第 y_j 位，下面说明这是一个不可约表示，对 x_1, x_2 有

$$\begin{aligned}\rho_{x_1+x_2}(y) &= (-1)^{(x_1+x_2)y} \\ &= (-1)^{x_1 y}(-1)^{x_2 y} \\ &= \rho_{x_1}(y)\rho_{x_2}(y)\end{aligned}$$

上面第一个等号后面的加号是位运算，第二个等号是因为 x_1, x_2 中的 0 不对 -1 的幂的结果有影响，即位运算中 0+1,1+0,0+0 均可拆开，对于位运算中的 1+1，两个 -1 相乘为 1，而 1+1 位运算结果是 0，$(-1)^0 = 1$, 故 1+1 也可拆开。故这是一个 Z_2^d 上的表示，又因为该表示是一维的，故为不可约表示。

我们再来介绍 Z_2^d 上的随机游走。定义

$$P(0) = P(0\cdots01) = P(0\cdots10) = \cdots = P(10\cdots0) = \frac{1}{1+d}$$

即从原点出发的随机游走有 $\frac{1}{d+1}$ 的概率在下一步走到 d 个邻接顶点或者不动。则我们有如下定理：

定理 3.0.14. *设 P 是如上定义在 Z_2^d 上的随机游走，令 $k = \frac{1}{4}(d+1)[\log d + c]$，则*

$$\|P^{*n} - U\|^2 \leqslant \frac{1}{2}(e^{e^{-c}} - 1)$$

证：

$$\begin{aligned}
\hat{P}(x) &= \sum_y (-1)^{x\cdot y} P(y) \\
&= \frac{1}{d+1}\{(-1)^{x\cdot(0,\cdots,0)} + \cdots + (-1)^{x\cdot(1,\cdots,0)}\} \\
&= \frac{1}{d+1}\{1 + \sum_{i=1}^{d}(-1)^{x_i}\} \\
&= 1 - \frac{2\omega(x)}{d+1} \text{ 这里 } \omega(x) \text{ 是 x 中的 1 的个数}
\end{aligned}$$

由上界引理有：

$$\begin{aligned}
\|P^{*k} - U\|^2 &\leqslant \frac{1}{4}\sum_{x\neq 0}(\hat{P}(x))^{2k} \\
&= \frac{1}{4}\sum_{j=1}^{d}\binom{d}{j}(1 - \frac{2j}{d+1})^{2k} \\
&\leqslant \frac{2}{4}\sum_{j=1}^{d/2}\frac{d^j}{j!}e^{-j\log d - jc} \\
&= \frac{1}{2}\sum_{j=1}^{d/2}\frac{e^{-jc}}{j!} \leqslant \frac{1}{2}(e^{e^{-c}} - 1)
\end{aligned}$$

这样我们就完成了证明。

十、 带有随机乘子的随机游走

下面我们来讨论具有随机乘子的随机游走，这类随机游走通常在计算机领域和密码学中用来生成伪随机序列。设 P 是某个奇数，令 $X_0 = 0, X_n = 2X_{n-1} + \varepsilon_n \ (mod\ p)$ 这里 ε_i 是独立同的离散均匀分布，等概率取值为 $0, \pm 1$，我们令 P_n 是 X_n 的分布, 自然地我们会关心什么时候 P_n 的分布接近均匀分布。

定理 3.0.15. 设 P_n 定义如上文，若

$$n \geqslant \log_2 p[\frac{\log\log_2 p}{\log 9} + s]$$

则

$$\|P_n - U\|^2 \leqslant \frac{1}{2}(e^{9^{-s}} - 1)$$

证：$X_0 = 0, X_1 = \varepsilon_1, X_2 = 2\varepsilon_1 + \varepsilon_2, \cdots, X_n = 2^{n-1}\varepsilon_1 + \cdots + \varepsilon_n \ (mod\ p)$. 又有第一章我们讨论的 Z_p 上的所有不可约表示为 $\rho_j(k) = e^{2\pi ijk/p}$, 再由之前讨论的随机变量卷积的概率意义我们知 P_n 的傅里叶变换为：

$$\prod_{\alpha=0}^{n-1}(\frac{1}{3} + \frac{2}{3}\cos\frac{2\pi 2^\alpha j}{p})$$

又由余弦函数的性质，不难得到：

$$(\frac{1}{3} + \frac{2}{3}\cos(2\pi x))^2 \leqslant h(x) = \begin{cases} \frac{1}{9} & x \in [\frac{1}{4}, \frac{3}{4}) \\ 1 & \text{其他情况} \end{cases}$$

这样我们便可以用

$$\prod_{\alpha=0}^{n-1} h(\{\frac{2^\alpha j}{p}\})$$

作为上界，其中 { } 是小数部分。设 x 的二进制表示为 $x = .\alpha_1\alpha_2\alpha_3\cdots$ 则

$$h(x) = \begin{cases} \frac{1}{9} & \alpha_1 \neq \alpha_2 \\ 1 & \alpha_1 = \alpha_2 \end{cases}$$

令 A(x.n) 表示 x 的二进制表示的前 n 个字符中改变的数目，即：$A(x, n) = |\{1 \leqslant i < n : \alpha_i \neq \alpha_{i+1}\}|$. 注意到，乘上 2^α 相当于把 x 的二进制表示的小数点后移了 α 位。故我们有：

$$\prod_{\alpha=0}^{n-1} h(\{\frac{2^\alpha j}{p}\}) \leqslant 9^{-A(j/p),n}$$

我们先对 $p=2^t-1$ 的情况讨论，此时 j/p 为：

$$\begin{aligned}
1/p &= \overbrace{00\cdots01}^{t}\ \overbrace{00\cdots01}^{t}\cdots \\
2/p &= 00\cdots10\ 00\cdots10\cdots \\
3/p &= 00\cdots11\ 00\cdots11\cdots \\
p-1/p &= 11\cdots10\ 11\cdots10\cdots
\end{aligned}$$

因为我们只需找到充分大的 n 即可，故我们可设 n=rt，那么 j/p 的前 n 个位置改变了至少 r 次（每 t 个元素中至少改变一次）故：

$$\begin{aligned}
\sum_{j=1}^{p-1}\prod_{\alpha=0}^{n-1} h\{\frac{2^\alpha j}{p}\} &\leqslant \sum_{j=1}^{p-1} 9^{-rA(j/p,t)} \\
&\leqslant 2\sum_{k=1}^{t}\binom{t}{k}9^{-kr} \\
&= 2[(1+9^{-r})^t-1] \\
&\leqslant 2[e^{t9^{-r}}-1]
\end{aligned}$$

上式中第一个不等式利用了 j/p 前 n 个位置至少改变 r 次即 $A(j/p,n)\geqslant rA(j/p,t)$, 第二个不等号是因为注意到

$$|j:A(\frac{j}{p},t)=k|\leqslant 2\binom{t}{k}$$

这个结论是因为二进制表示中 1 带来的相邻数位的不同至多 2 个，故有 k 个不同相对于从 t 位中选出 k 个 1。再成对 $k=A(\frac{j}{k},t)$ 求和即得。这样再在最终式中令 $r=\frac{\log t}{\log 9}+s$ 即得结论：

$$\|P_n-U\|^2\leqslant[e^{9^{-s}}-1]$$

下面再对一般的奇数 P 讨论，设 t 满足 $2^{t-1}<p<2^t$，令 $r=\frac{\log t}{\log 9}+s$,n=rt, 我们将 j/p 的二进制展开的前 n 位分成 r 块，每块长为 t，记它们为 B(i,j)：

$$j/p=\overbrace{\alpha_1\cdots\alpha_t}^{B(1,j)}\overbrace{\alpha_{t+1}\cdots\alpha_{2t}}^{B(2,j)}\cdots\overbrace{\alpha_{(r-1)t+1}\cdots\alpha_{rt}}^{B(r,j)}$$

则

$$\sum_{j=1}^{p-1}\prod_{\alpha=0}^{n-1} h(\{\frac{2^\alpha j}{p}\})\leqslant\sum_{j=1}^{p-1}9^{-A(B(1,j))-\cdots-A(B(r,j))} \tag{3-1}$$

又由 $2^{t-1} < p < 2^p$ 故所有在第一列的块 $B(1,j)$ 均不同，且至少有一个相邻数位改变。此外，注意到 $(2,p) = 1$，第 i 列上的块均不取决于 i（因为在二进制下 $(2,p) = 1$ 则 1/p 为无限循环小数)。我们引入如下引理：

引理 3.0.2. *若* $0 < \alpha < 1, a \leqslant a', b \leqslant b'$ *则*

$$\alpha^{a+b'} + \alpha^{a'+b} \leqslant \alpha^{a+b} + \alpha^{a'+b'}$$

证：将 $(\alpha^a - \alpha^{a'})(\alpha^b - \alpha^{b'}) \geqslant 0$ 展开即得。由引理，我们便能把相同的块合并且使上界不减，这样式 (2-1) 中的上界就可放大为

$$\sum_{j=1}^{p-1} 9^{-rA(j/2^t-1,t)}$$

这样就回到了 $p = 2^t - 1$ 的情况。综上命题得证。

参考文献

[1] P.Diaconis. Patterns in eigenvalues. *Bulletion of the American Mathematical Society*, 40(2):155–178, 2003.

[2] P. Diaconis and P.J. Forrester. A. hurwitz and the origins of random matrix theory in mathematics. *Mathematical Physics,arXiv:1512.09229*, 7(3):1–4, 2015.

[3] Persi Diaconis. *Group Representations in Probability and Statistics*. Institute of Mathematical Statistics,Hayward,California, 1988.

[4] 丘维声. *群表示论*. 高等教育出版社, 2005.

[5] David S. Dummit. *Abstract Algebra*. Wiley, 2003.

[6] David R.Stirzaker Geoffery R.Grimmett. *Probability and random processes*. Mathematical Institute,University of Oxford, 2001.