Gallagher遍历定理的形式化

Oliver Nash ！ 英国理工学院，伦敦，英国

摘要

Gallagher遍历定理是度量数论中的一项结果。它指出，用有理数逼近实数时，会呈现一种引人注目的“全有或全无”特性。我们讨论了在 Lean定理证明器中对这一结果的形式化。该结果本身就颇具意义，同时也是 Koukoulopoulos 和 Maynard 最近证明 Duffin-Schaeffer猜想所必需的一项关键预备结果。

2012年 ACM 学科分类 计算数学 → 概率与统计

关键词与短语 Lean证明助手、测度论、度量数论、遍历性、Gallagher定理、Duffin-Schaeffer猜想

补充材料该形式化内容可在 Lean 数学库的主分支中找到， `mathlib`。

软件（源代码）： `https://github.com/leanprover-community/mathlib`

致谢我很高兴感谢 Andrew Pollington，他在 2022年于布朗大学（ICERM）举行的「好奇数学家的 Lean」会议上提出了这个项目。我还要感谢 Anatole Dedecker、Heather Macbeth、Patrick Massot 和 Junyan Xu，他们都给予了直接帮助。最后，我尤其要感谢 Sébastien Gouëzel 提出了许多有益的建议，也感谢 Kevin Buzzard 与我进行了许多有用的交流。

arXiv:2302.00448v1 [cs.LO] 1 Feb 2023

1 引言

菲尔兹奖除了表彰年轻数学家的杰出成就外，还为更广泛的数学界提供了一项宝贵服务：让人们关注近期的重要成果。近年来，这种关注对形式化社区产生了显著的积极影响。Buzzard、Commelin 和 Massot 对完美空间定义的形式化 [3]，以及 Commelin、Topaz 等人在液体张量实验 [5] 中取得的卓越成果，都是对 2018年菲尔兹奖得主 Peter Scholze 的研究进行形式化的项目成果。除此之外，这些项目还表明，如今的证明助手能够处理当代数学中复杂的构造。

2022年，James Maynard 获得了菲尔兹奖，颁奖词特别提到了他在素数结构以及丢番图逼近方面的工作。我们在颁奖词的完整版本中读到：

> Maynard 还在丢番图逼近领域取得了基础性成果，他与Koukoulopoulos共同解决了Duffin-Schaeffer猜想。

Maynard 获奖消息公布后不久，Andrew Pollington 向作者建议，将 Koukoulopoulos 和 Maynard 对 Duffin-Schaeffer猜想的证明形式化，是一个值得追求的目标。考虑到这将是一项艰巨的工作，他建议先专注于若干必要的预备工作。其中或许最重要的是 Gallagher遍历定理 [7]（另见 [11] 引理 5.1）。定理陈述如下：

▶ **定理 1** (Gallagher 定理)。 设 $\delta_1, \delta_2, \ldots$ 是一个实数序列，并设：

$$W = \{x \in \mathbb{R} \mid \exists\, q \in \mathbb{Q}, |x - q| < \delta_{\mathrm{denom}(q)}\ i.o.\}.$$

2 Gallagher遍历定理的形式化

那么 W 几乎相等于 $\emptyset$ 或 $\mathbb{R}$。

这里值得作几点说明：

- 记号 denom(q) 表示 q （既约形式下）的分母。它是一个严格为正的自然数。定义W中出现的字母“i.o.”需要特别注意：它们是“无穷多次”的缩写。该记号表示， $x \in W$ 当且
- 仅当存在一个由有理数组成的无限序列 q_0， q_1，.....（它可能依赖于 x），满足 denom(q_0) $<$ denom(q_1) $< \cdots$，并且对所有 i 都有 $|x - q_i| < \delta_{\mathrm{denom}(q_i)}$ 。“几乎相等”这一说法表明这是一个度量数论定理：它的意思是，这些集合除去一个勒贝格测度为零的集合后相等。令人惊讶且完全不显然的是， W 竟会呈现出这种二分行为。

本文旨在讨论作者对 Gallagher 定理的形式化。这项工作使用 Lean证明助手及其 `mathlib` 库 [12]完成。更确切地说，我们形式化了以下内容：

列表 1 Gallagher 定理

```
theorem add_well_approximable_ae_empty_or_univ(δ : ℕ → ℝ) (hδ : tendsto δ at_top (N
```

相关符号将在后文说明。经过进一步研究，可以去掉假设 $h\delta$，即 $\delta_n \to 0$ as $n \to \infty$。事实上，这凸显了证明中一个有趣的特点：证明采用了两种完全独立的论证，一种是测度论论证，假设 $h\delta$ ；另一种是数论论证，假设其否定。随后，我们运用排中律，无条件地推出结论。假设 $h\delta$ 的测度论论证要困难得多，也是我们已将其形式化的部分。

本文面向非专业读者，结构安排如下。第 2 节概述相关的基本概念，以便将 Gallagher 定理重新诠释为关于圆上有限阶点的加厚集之上极限的结果。我们还对度量数论作一些一般性讨论。第 3 节介绍所需的最重要基础结果。勒贝格密度定理是 Gallagher 证明中的主力工具。第 4 节讨论 Cassels 提出的一条关键测度论引理，该引理本身也颇具独立价值。第 5 节讨论我们所需的关于遍历映射的结果，着重强调圆上一些映射的遍历性。第 6 节引入近似有限阶点，并以此为工具证明 Gallagher 定理。最后，在第 7 节中，我们还将讨论这项工作可以进一步拓展的方向等内容。大部分情况下，我们不会深入讨论证明细节。主要的例外是 Gallagher 定理本身的证明，因为我们希望，对 Gallagher 思路的阐述能比其他面向专家的论述（例如 [7] 定理 1 或 [10]定理 2.7(B)）更易于理解。

秉承 `mathlib` 对数学统一性的强调，所有工作都通过一系列 27 个拉取请求直接添加到 `mathlib` 的主分支中，合计新增代码净行数略高于 3,500 行。因此，今后的所有 `mathlib` 用户都能自动使用这些内容。本文还提供了指向 `mathlib` 中相关位置的永久链接，每个链接都以符号 标示。此外，我们还精心挑选了一些代码清单（例如上文的清单 1），其中包含 Lean 代码。我们通常希望借此帮助读者将关键的非形式化表述与其形式化对应版本进行比较。

2 基本概念

我们概述一些基本概念，以统一记号并帮助非专家读者。

2.1 几乎相等的集合

给定一个带有测度 μ 的可测空间，当测度不会引起歧义时，我们采用以下记号：

$$s =_{a.e.} t, \tag{1}$$

表示两个子集 s、t 关于 μ 几乎相等。我们回顾一下，这等价于以下两个零测度条件：

$$\mu(s \setminus t) = 0 \quad \text{and} \quad \mu(t \setminus s) = 0. \tag{2}$$

2.2 无限多次满足条件

Gallagher 定理讨论的是满足某个条件“无穷多次”的点集。一般来说，给定某个背景类型 X 的子集序列 s_0，s_1，$\ldots$，记号 $\exists \cdots\ i.o.$ 定义为[1]：

$$\{x : X \mid \exists\ n \in \mathbb{N}, x \in s_n\ i.o.\} = \{x : X \mid \text{the set } \{n \in \mathbb{N} \mid x \in s_n\} \text{ is infinite}\}. \tag{3}$$

事实上，这个集合还有另一种表示；不难看出：

$$\{x : X \mid \exists\ n \in \mathbb{N}, x \in s_n\ i.o.\} = \limsup s, \tag{4}$$

其中：

$$\limsup s = \bigcap_{n \geq 0} \bigcup_{i \geq n} s_i.$$

在形式化关于无穷多次属于某个子集族的点集的结果时，因此可以使用（3）的语言，或者使用上极限的语言来表述。我们选择了后者。这样更合适，因为上极限对任意完备格都有意义，而（3）则仅适用于某个类型的子集格。因此，所开发的所有 API 都有更广泛的适用性。

在证明过程中，使用由谓词 $p\colon\ \mathbb{N} \to \mathsf{Prop}$ 所界定的上极限很有帮助。这可以定义为：

$$\limsup_{p} s = \bigcap_{n \geq 0} \bigcup_{p(i), i \geq n} s_i. \tag{5}$$

我们添加的实际定义 `filter.blimsup` 略有不同，因此也适用于条件完备格（例如 $\mathbb{R}$）；不过，我们提供了一个引理，证明它在完备格（例如 `set` $\mathbb{R}$）中等价于（5）。利用 `blimsup`，我们可以处理由谓词 p 定义的子族的上极限，而无需将索引类型转换为子类型。例如，给定两个谓词 p、q，我们可以表达以下有用的恒等式：

$$\underset{p \vee q}{\text{上极限}}\ s = \underset{p}{\text{上极限}}\ s \cup \underset{q}{\text{上极限}}\ s, \tag{6}$$

形式化表示为：

[1] 这是非正式文献中通篇使用的标准记号。

列表 2 由两个谓词的逻辑或限定的上极限

```
@[simp] lemma blimsup_or_eq_sup :

```

无需涉及任何子类型。这是全文采用的一种标准设计模式 `mathlib` .

2.3 加厚集

使用上文引入的语言，定理 1 陈述中出现的集合 W 可以定义为:

$$W = \limsup_{n>0} s,$$

其中:

$$s_n = \{x \in \mathbb{R} \mid \exists\, q \in \mathbb{Q}, \mathrm{denom}(q) = n, |x - q| < \delta_n\}.$$

这些子集 s_n 具有一种特殊形式：它们是加厚集。一般而言，给定一个度量空间X，如果 $s \subseteq X$ 和 $\delta \in \mathbb{R}$，则 s 的（开） δ-加厚集为:

$$\mathrm{Th}(\delta, s) = \{x \in X \mid \exists\, y \in s, d(x, y) < \delta\}.$$

这推广了开球的概念。幸运的是，Gouezel 关于 Gromov-Hausdorff度量的研究 [8]已在 `mathlib` 中引入了加厚集 。因此，我们可以将 W 表示为:

$$W = \limsup_{n>0} \mathrm{Th}(\delta_n, \{q \in \mathbb{Q} \mid \mathrm{denom}(q) = n\}).$$

事实证明，使用加厚集这一术语在形式上非常方便，不仅适用于 Gallagher 定理，也适用于例如引理 5（下文将讨论）。

2.4 圆作为赋范群

定理 1 中出现的子集 W 显然满足周期性条件[2]:

$$1 + W = W,$$

因此它下降为圆 $\mathbb{S} = \mathbb{R}/\mathbb{Z}$的一个子集。这个商实际上是一个赋范群；给定一个 $x \in \mathbb{R}$，它代表陪集 $\hat{x} \in \mathbb{S}$，其范数满足:

$$\|\hat{x}\| = |x - \mathrm{round}(x)| \tag{7}$$

其中 round(x) 是最接近 x 的整数。由于范数赋予我们一个度量，我们可以谈论 $\mathbb{S}$ 的子集的加厚集。

此外， $\mathbb{Q}/\mathbb{Z} \subseteq \mathbb{S}$ 恰好是 $\mathbb{S}$ 中有限阶点的集合。因此，Gallagher 定理可被视为确立了圆 $\mathbb{S}$ 在赋范群范畴中具有的一种特殊性质。正如我们将看到的，这种观点很有用，因为 Gallagher 定理的证明依赖于这样一个事实：某些变换在视为映射 $\mathbb{S} \to \mathbb{S}$ 时是遍历的。

这项工作开始时， `mathlib` 已经包含了一个将圆表示为单位模复数的模型，称为 `circle` 。尽管该模型与$\mathbb{R}/\mathbb{Z}$在自然意义下等价，但这种等价性使用了与我们的工作无关的指数映射和对数映射。因此，我们引入了第二个模型，称为 `add_circle` ，其定义为 $\mathbb{R}/\mathbb{Z}$:

[2] 如果 q 逼近 x，那么 $1 + q$ 以相同的误差逼近 $1 + x$，且 denom$(1 + q)$ = denom(q)。

列表 3 加法圆

```
def add_circle {𝕂 : Type*} [linear_ordered_add_comm_group 𝕂]
  [topological_space 𝕂] [order_topology 𝕂] (p : 𝕂) :=
𝕂 / zmultiples p
```

其中，$p = 1$ 这恰好是 $\mathbb{R}/\mathbb{Z}$，但我们允许 p 取一般值，以支持其他应用[3]。

顾名思义，`circle` 承载了 `mathlib` 的一个 `group` 类实例，而 `add_circle`承载了 `add_group` 的一个实例。有趣的是，`mathlib`的加法-乘法设计模式如此便利地允许这两种模型共存。

随后为 `add_circle` 开发了大量 API，尤其是该类`normed_add_comm_group` 的一个实例，它满足恒等式 (7)，并且利用有理数刻画有限阶点：

$$\{y \in \mathbb{S} \mid o(y) = n\} = \{[q] \in \mathbb{S} \mid q \in \mathbb{Q}, \operatorname{denom}(q) = n\}, \tag{8}$$

其中，记号 $o(y) = n$ 表示 y 的阶为 n。

使用我们所有的新术语，Gallagher 定理的表述如下：

▶ **定理 2** (Gallagher 定理). 设 $\delta_1, \delta_2, \ldots$ 为一个实数序列，并设：

$$W = \limsup_{n>0} \operatorname{Th}(\delta_n, \{y \in \mathbb{S} \mid o(y) = n\}).$$

那么 $W =_{a.e.} \emptyset$ 或 $W =_{a.e.} \mathbb{S}$。

利用 (7) 以及 (8)，定理 2 显然等价于定理 1。

2.5 度量数论

度量数论研究实数（及相关空间）的算术性质，这些性质相对于勒贝格测度而言在“几乎处处”成立。Gallagher 定理中的算术性质是有理数逼近。

举例来说，考虑由 $\mathbb{I}$ 所有具有无穷多个二次近似有理逼近的实数组成的集合：

$$\begin{aligned}\mathbb{I} &= \{x \in \mathbb{R} \mid \exists\, q \in \mathbb{Q}, |x - q| < 1/\operatorname{denom}(q)^2 \ i.o.\} \\ &= \limsup_{n>0} \operatorname{Th}(1/n^2, \{q \in \mathbb{Q} \mid \operatorname{denom}(q) = n\}).\end{aligned}$$

至少从 19th 世纪初以来，人们就已知道，$\mathbb{I}$ 恰好是无理数的集合[4]：

$$\mathbb{I} = \mathbb{R} \setminus \mathbb{Q}. \tag{9}$$

从度量数论的角度看这一结果，我们注意到，由于 $\mathbb{Q}$ 的勒贝格测度为零，$\mathbb{I}$ 几乎相等于 $\mathbb{R}$。因此，度量数论学者会满足于将（9）概括为：

$$\mathbb{I} =_{a.e.} \mathbb{R},$$

而不必担心 $\mathbb{I}$ 具体包含哪些数。

从度量数论学家的视角来看，其优势在于，许多问题都能以这种形式得到解答。Gallagher 定理就是这一现象中格外优美的一个例子。

[3] 例如，`mathlib` 使用 $p = 2\pi$ 来定义角度。[4] 感谢 Michael Geißer 和 Michael Stoll，`mathlib` 知道这个事实。

3 倍增测度与勒贝格密度定理

勒贝格密度定理是测度论中的一项基础性结果，也是证明 Gallagher 定理所必需的。尽管我们只需将它应用于圆，但密度定理普遍成立，因此我们费了一番功夫，在相当弱的假设下将其形式化[5]。

3.1 倍增测度

密度定理成立的一类方便使用的测度是倍增测度。

▶**定义 3**。设 X 是一个带有测度 μ的可测度量空间。若存在 $C \geq 0$ 和 $\delta > 0$，使得对所有 $0 < \epsilon \leq \delta$ 和 $x \in X$均有：我们称 μ 为倍增测度。

$$\mu(B(x, 2\epsilon)) \leq C\mu(B(x, \epsilon)).$$

其中 $B(x, r)$ 表示以 x为中心、半径为 r 的闭球。

作者为形式化密度定理之目的，将相应的形式定义添加到了 `mathlib` 中：

代码清单 4 倍增测度的定义

```
class is_doubling_measure
```

上面的代码没有明确提及参数 δ，因为我们使用 `mathlib`关于谓词沿滤子最终成立这一概念的标准记号。

在我们的应用中，需要将密度定理应用于圆上的 Haar测度 [13]。当然，这实际上就是熟悉的弧长测度，因此半径为 ϵ 的闭球的体积由给出：

$$\mu(B(x, \epsilon)) = \min(1, 2\epsilon).$$

取 $C = 2$，由此可知圆上的 Haar测度是倍增的。我们将这一事实登记 d 为一个类型类实例，如下所示：

代码清单 5 圆周的倍增测度

```
instance : is_doubling_measure (volume : measure (add_circle T)) :=
```

单位圆对应于取 $T = 1$，但代码允许任意 $T > 0$。借助这个实例，Lean 知道，对于倍增测度证明的任何结果都自动适用于圆上的 Haar测度。

[5] 我们很幸运，Sébastien Gouëzel 最近添加了一套极为通用的 Vitali族理论，使这一切成为可能。

3.2 密度定理

我们形式化的密度定理版本如下：

▶**定理 4.** 设 X 是一个带有测度 μ的可测度量空间。假设X 具有第二可数拓扑，且 μ 是倍增且局部有限的。设 $S \subseteq X$ 和$K \in \mathbb{R}$，那么对于几乎所有 $x \in S$，给定任意点序列 w_0，$w_1, \ldots$ 以及距离$\delta_0, \delta_1, \ldots$，若：

- $\delta_j \to 0$ 当 $j \to \infty$ 且，$x \in B(w_j$，
- $K\delta_j)$ 对于足够大的 j，

则：

$$\frac{\mu(S \cap B(w_j, \delta_j))}{\mu(B(w_j, \delta_j))} \to 1,$$

当 $j \to \infty$。

即使在特殊情形 $K = 1$和 $w_0 = w_1 = \cdots = x$中，这个结果也相当有力[6]。x 满足定理陈述中所述性质的点称为密度 1 的点。用这种说法，勒贝格密度定理断言，一个集合中几乎所有的点都具有密度 1。特别地，如果 $\mu(S) > 0$，那么必定存在一个密度为 1 的点。例如，如果 $X = \mathbb{R}$ 且 S 是闭区间 $[0, 1]$,，那么密度为 1 的点集就是开区间 (0，1)。

事实上，我们添加到 `mathlib` 中的形式化版本稍微一般一些，因为它允许 w 和 δ 是从任意带有滤子的空间映射而来的映射。在给出一个预备性的 `variables`陈述之后：

代码清单 6 密度定理的变量

```
variables {α : Type*} [metric_space α] [measurable_space α] (μ : measure α)
  [is_doubling_measure μ] [second_countable_topology α] [borel_space α]
  [is_locally_finite_measure μ]
```

它看起来是这样的：

代码清单 7 关于倍增测度的勒贝格密度定理

```
lemma is_doubling_measure.ae_tendsto_measure_inter_div (S : set α) (K : ℝ) :
```

证明方法的核心是为 `is_doubling_measure` 构建足够的 API，以证明这类测度空间具有某些自然的子集族，称为 Vitali族，然后调用 Gouëzel 在独立项目 [9] 中加入的引理 `vitali_family.ae_tendsto_measure_inter_div` 。

4 卡塞尔引理

Gallagher 定理证明中的一个关键要素是 Cassels 提出的以下结果。

[6] 事实上，这可能是文献中最常见的版本。

▶**引理 5.** 设 X 是一个带有测度 μ的可测度量空间。假设 X具有第二可数拓扑，且 μ 是倍增且局部有限的。设 $s_0, s_1, \ldots$ 是 X 的一个子集序列， $r_0, r_1, \ldots$ 是一个实数序列，并且 $r_n \to 0$ 当 $n \to \infty$ 时。对任意 $M > 0$ ，令:

$$W_M = \text{Th}(Mr_n, s_n) \text{ 的上极限,}$$

那么:

$$W_M =_{a.e.} W_1,$$

也就是说，除去零测集， W_M 不依赖于 M。

这基本上就是 [4] 中的引理 9，只是在以下特殊情况下:
(a) X 是开区间(0,1)，**(b)** μ 是勒贝格测度，**(c)** s_n 是点序列，而非子集序列。

复用列表 6 中的 `variables` 后，我们添加到`mathlib` 中的引理 5 的形式化版本如下:

列表 8 卡塞尔引理

```
theorem blimsup_thickening_mul_ae_eq
```

这里有几点需要说明:

- 语法 `s =ᵐ[μ] t` 是 `mathlib` 对集合（或函数）的记法 s，表示它们相对于测度 μ t 几乎相等。这是常见非正式记法 (1) 的形式化等价表示。

- 这些类型标注 `:` `set` α 的出现，是因为`mathlib`的格论库中存在一个尚未解决的 类型类菱形 。问题在于，类型 `set` α 在定义上等于 $\alpha \to$Prop。由于 Prop 是一个完备布尔代数，因此 $\alpha \to$Prop 是一个完备布尔代数。不幸的是，虽然 `set` α上的完备布尔代数结构在数学上等于 $\alpha \to$Prop 上的结构，但二者在定义上并不相等。严格来说，由于 `set` α 是一个类型同义词，这个菱形是允许存在的，但解决它仍然会很有用。[7]

- 列表 8 以 `blimsup`的形式表述，即由谓词 p所界定的上极限。正如第（2.2）节所述，这使我们无需处理子类型。我们将看到，在 Gallagher 定理的证明中应用这一引理时，这样做十分方便。

- 卡塞尔引理的证明中，关键在于勒贝格密度定理 4。根据 (2)，卡塞尔引理要求我们证明两个零测度条件。视 $M < 1$ or $M > 1$ 而定，对于卡塞尔引理 5 陈述中出现的两个集合，这两个条件中恰有一个是显然成立的。要证明那个非平凡的零测度条件，可以用反证法：假设该测度严格为正，应用密度定理得到一个密度为 1 的点，再证明这对于倍增测度是不可能的。唯一非平凡的依赖是勒贝格密度定理。

[7] 该菱形已记录在 `mathlib` issue 16932 中。事实上，完备布尔代数结构中只有 `Inf` 和 `Sup` 字段在定义上存在差异，因此应该相当容易解决。

- 尽管将这个引理从其在 [4] 中的原始形式推广所需的修改很直接，但从点推广到子集（等价地，从球推广到加厚集）的推广 (c) 在形式化方面极为有用。在 Gallagher 定理所需的这个引理的应用中，s_n 是圆上阶为 n 的点集。在非正式文献中，可以应用适用于点序列的引理 5 版本，因为圆上每个有限阶都只有有限多个点，因此可以将所有有限阶点枚举成一个点序列。不过，这样在形式化方面会很繁琐。

5 遍历理论

遍历理论研究保测映射。给定测度空间 $(X,\ \mu_X)$ 和 $(Y,\ \mu_Y)$，可测映射 $f\colon X \to Y$ 是保测的，当且仅当：

$$\mu_X(f^{-1}(s)) = \mu_Y(s),$$

对于任意可测集 $s \subseteq Y$。例如，给定任意 $c \in \mathbb{R}$，在定义域和值域上均取勒贝格测度，平移 $x \mapsto c + x$ 总是保测的，而伸缩 $x \mapsto cx$ 只有在 $c = \pm 1$ 时才是保测的。幸运的是，`mathlib` 已经包含了关于保测映射的优秀理论。

5.1 遍历映射，一般理论

在遍历理论中，人们特别关注遍历映射。

▶ **定义 6**。设 (X, μ) 是一个测度空间，且 $f\colon X \to X$ 是保测的。若对任意可测集 $s \subseteq X$：我们称 f 是遍历的，

$$f^{-1}(s) = s \implies s \text{ is almost equal to } \emptyset \text{ or } X.$$

遍历性是 Gallagher 定理证明中的关键概念，因此我们在 `mathlib`中加入了以下定义：

列表 9 预遍历映射 和遍历映射的定义：

```
```

引入中间定义 `pre_ergodic` 是为了支持拟遍历映射的定义；我们也定义了拟遍历映射，但这里不涉及它们。

随后我们为遍历映射建立了一些基础 API，其中包括以下关键结果：

▶ **引理 7.** 设 X 是一个可测空间，配备测度 μ，满足 $\mu(X) < \infty$。假设 $f\colon X \to X$ 是遍历的，$s \subseteq X$ 可测，且像 $f(s)$ 几乎包含于s中，那么 s 与 $\emptyset$ 或 X几乎相等。

这个结果虽然初等，但并非完全显然，其正式表述如下：

列表 10 在遍历映射 下几乎不变的集合：

```
lemma ae_empty_or_univ_of_image_ae_le [is_finite_measure μ]
  (hf : ergodic f μ) (hs : measurable_set s) (hs' : f '' s ≤ᵐ[μ] s) :
  s =ᵐ[μ] (∅ : set X) ∨ s =ᵐ[μ] univ :=
```



图 1 映射 $f\colon y \mapsto 2y$ 是保测的。

这并不是首次在定理证明器中对遍历映射进行形式化，因此我们对上述内容的介绍非常简短。事实上，Isabelle/HOL 的形式化证明档案收录了 Sébastien Gouëzel 在遍历理论方面的大量出色成果，其中也有 Manuel Eberl 的贡献，可在“遍历理论”条目中查阅。该条目包含许多一般遍历理论方面的结果，这些结果尚未添加到 `mathlib` 中。另一方面，我们需要知道圆上的某些特定映射是遍历的，而我们对这些结果的形式化似乎确实是同类工作中的首例。接下来我们将对此展开讨论。

5.2 圆上的遍历映射

为了证明 Gallagher 定理，我们需要以下结果：

▶ **定理 8**。 给定 $n \in \mathbb{N}$，映射：

$$\mathbb{S} \to \mathbb{S}$$
$$y \mapsto ny$$

当 $n \geq 1$ 时是保测的，当 $n \geq 2$时是遍历的。

$y \mapsto ny$ 是保测的这一事实源于 Haar测度的一般唯一性结果。事实上，对于任意紧的、阿贝尔的、可除的拓扑群，该结果都成立。得益于 `mathlib`关于 Haar测度的丰富理论，[13], 很容易为这一结果添加证明。对于初次接触这一事实的读者，我们建议考察图 1，并理解为什么该结果对 $\mathbb{S}$ 成立，尽管对 $\mathbb{R}$却不成立。

证明 $y \mapsto ny$ 是遍历的则更加困难。我们将其证明为以下引理的推论。我们概述证明，以便读者了解其中涉及的内容；读者无需掌握细节：关键在于我们需要使用勒贝格密度定理。

▶ **引理 9**。 设 $s \subseteq \mathbb{S}$ 可测，并且 u_0、u_1..... 是$\mathbb{S}$中的有限阶点序列，满足：$u_i + s$ 与 s 对所有 i，其阶 $o(u_i) \to \infty$ 当 $i \to \infty$时几乎相等。那么 s 与 $\emptyset$ 或 X几乎相等。

证明。 这一结果相当直观： s 几乎相等于 $u_i + s$ 当且仅当它由一组 $o(u_i)$ 分支组成，这些分支均匀分布在整个圆上，除了一个零测度集之外。由于这对所有 i 和 $o(u_i) \to \infty$都成立，因此除去一个零测度集之外，这些分支要么填满整个圆，要么完全不存在。

将上述直观论证转化为严格证明的方法，是使用勒贝格密度定理 4。我们必须证明，如果 s 并非几乎为空，那么 $\mu(s) = 1$。勒贝格告诉我们，如果 s 并非几乎为空，那么它必然包含某个点 d，其密度为 1。利用 d，我们构造出以 d 为中心的一列闭球 B_i，使得 $\mu(B_i) = o(u_i)$。由于$u_i + s$ 几乎是 s,

$$\mu(s \cap B_i) = o(u_i)\mu(s) = \mu(B_i)\mu(s).$$

然而，由于 d 具有密度 1，我们知道：

$$\mu(s \cap B_i)/\mu(B_i) \to 1.$$

这两个结果迫使我们得出结论： $\mu(s) = 1$。 ◀

形式化版本略微更具一般性，并在 `mathlib` 中如下所示：

列表 11 引理 9 的形式化表述

```
lemma add_circle.ae_empty_or_univ_of_forall_vadd_ae_eq_self
```

定理 8 由引理 9 推出，因为任何满足 $f^{-1}(s) = s$ 对 $f : y \mapsto ny$的集合 s 都满足 $u_i + s = s$ 对于该序列：

$$u_i = [1/n^i] \in \mathbb{S}.$$

注意，为了使 $o(u_i) = n^i \to \infty$，我们需要 $n \geq 2$。正式表述如下所示，见 `mathlib`：

列表 12 定理 8 的正式表述

```
lemma ergodic_nsmul {n : ℕ} (hn : 1 < n) :
```

事实上，我们需要对定理 8 作如下温和的推广：

▶ **定理 10**。 给定 $n \in \mathbb{N}$ 和 $x \in \mathbb{S}$，映射：

$$\mathbb{S} \to \mathbb{S}$$
$$y \mapsto ny + x$$

若 $n \geq 1$，则为保测；若 $n \geq 2$，则为遍历的。

由定理 8 可轻易得出，因为若我们定义保测等价：

$$e : \mathbb{S} \to \mathbb{S}$$
$$y \mapsto \frac{x}{n-1} + y$$

那么简单计算可得：

$$e \circ g \circ e^{-1} = f,$$

其中 f： $y \mapsto ny$，且 g： $y \mapsto ny + x$。因此，定理 10 可由定理 8 通过以下方式得出：

列表 13 定理 10 化归为定理 8

```
lemma ergodic_conjugate_iff {e : α ≃ᵐ β} (h : measure_preserving e μ μ') :
```

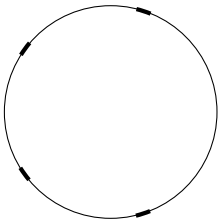

图 2 $\mathbb{S}$ 中近似阶为 5 的点集，距离不超过 $\delta \approx 0.01$。

6 Gallagher 定理

6.1 近似阶点

回顾一下定理 2 的表述中出现的集合 $W \subseteq \mathbb{S}$ 的定义：

$$W = \limsup_{n>0} \mathrm{Th}(\delta_n, \{y \in \mathbb{S} \mid o(y) = n\}).$$

定理 2 的证明关键在于集合 $\mathrm{Th}(\delta_n, \{y \in \mathbb{S} \mid o(y) = n\})$ 与 $\mathbb{S}$ 的群结构之间的相互作用。因此，我们作如下定义：

▶ **定义 11.** 设 A 为半赋范群，$n \in \mathbb{N}$（非零），且 $\delta \in \mathbb{R}$。我们采用以下记号：

$$\mathbb{AO}(A, n, \delta) = \mathrm{Th}(\delta, \{y \in A \mid o(y) = n\}),$$

对于近似阶为 n、距离不超过 δ 的点集。

例如，如图 2 所示，$\mathbb{AO}(\mathbb{S}, n, \delta)$ 是由 $\varphi(n)$ 条直径为 2δ 的弧组成的并集，这些弧以满足 $0 \le m < n$ 且 m 与 n 互素的点 $[m/n]$ 为中心（其中 φ 是欧拉函数）。

定义 11 的形式化对应表述如下：

清单 14 赋范群中的近似阶点

```
@[to_additive] def approx_order_of
  (A : Type*) [seminormed_group A] (n : ℕ) (δ : ℝ) : set A :=
thickening δ {y | order_of y = n}
```

用这种语言来说，我们所需的 $\mathbb{AO}(A, n, \delta)$ 的唯一性质如下：

▶ **引理 12。** 设 A 是一个半赋范交换群，$\delta \in \mathbb{R}$、$a \in A$ 和 m、$n \in \mathbb{N}$（均非零）。则[8]：

(i) $m \cdot \mathbb{AO}(A, n, \delta) \subseteq \mathbb{AO}(A, n, m\delta)$，如果 m, n 互素 *W*；*(ii)* $m \cdot \mathbb{AO}(A, nm, \delta) \subseteq \mathbb{AO}(A, n, m\delta)$ *W*；*(iii)* $a + \mathbb{AO}(A, n, \delta) \subseteq \mathbb{AO}(A, o(a)n, \delta)$，如果 $o(a)$ 与 n 互素 *W*；*(iv)* $a + \mathbb{AO}(A, n, \delta) = \mathbb{AO}(A, n, \delta)$，如果 $o(a)^2$ 整除 n *W*。

事实上，性质（iv）在较弱假设下也成立：$r(o(a))o(a)$ 整除 n，其中 $r(l)$ 表示自然数 l 的根基；不过，我们只需要引理中陈述的版本。

为支持定理 2，我们最后给出一个定义：

[8] 如果 $s \subseteq A$ 记号 $m \cdot s$ 表示 $\{my \mid y \in s\}$。

▶ **定义 13.** 设 A 为一个半赋范群，$\delta_1, \delta_2, \ldots$ 为一个实数序列。我们采用以下记号：

$$\mathbb{WA}(A,\ \delta) = \text{上极限 } \mathbb{AO}(A,\ n,\ \delta_n),\ n>0$$

相对于 δ，对于由 A 中可由有限阶点良好逼近的元素组成的集合。

注意，$W = \mathbb{WA}(\mathbb{S},\ \delta)$，其中 W 是定理 2陈述中出现的集合。定义 13 的形式对应为：

列表 15 赋范群中的可良好逼近元素集合

```
@[to_additive] def well_approximable
  (A : Type*) [seminormed_group A] (δ : ℕ → ℝ) : set A :=
blimsup (λ n, approx_order_of A n (δ n)) at_top (λ n, 0 < n)
```

该定义的加法版本为 `add_well_approximable`。

6.2 主定理

我们终于可以将所有内容整合起来，并给出主要结果的证明。为方便读者，我们在此重述上文列表 1 中的形式化陈述：

列表 16 Gallagher 定理

```
theorem add_well_approximable_ae_empty_or_univ(δ : ℕ → ℝ) (hδ : tendsto δ at_top (N
```

记号 $\forall^m x, \cdots$ 应读作“对几乎所有 $x \cdots$”，这是标准的 `mathlib` 记法。利用引理 `filter.eventually_eq_empty` 和 `filter.eventually_eq_univ`，列表 16 中的陈述等价于：

▶ **定理 14** (Gallagher 定理（含 $\delta \to 0$)。设 $\delta_1, \delta_2, \ldots$ 是一个实数序列，满足 $\delta_n \to 0$ 当 $n \to \infty$时。则 $\mathbb{WA}(\mathbb{S}, \delta)$ 几乎相等于 $\emptyset$ 或 $\mathbb{S}$。

证明。对于每个素数 $p \in \mathbb{N}$ 我们定义三个集合[9]：

$$A_p = \text{上极限 } \mathbb{AO}(\mathbb{S},\ n,\ \delta_n),\ n>0,\ p \nmid n \quad B_p = \text{上极限 } \mathbb{AO}(\mathbb{S},\ n,\ \delta_n),\ n>0,\ p \| n$$
$$C_p = \text{上极限 } \mathbb{AO}(\mathbb{S},\ n,\ \delta_n)。\ n>0,\ p^2 | n$$

令 $W = \mathbb{WA}(\mathbb{S},\ \delta)$；考虑到 (6)，显然对于任意 p：

$$W = A_p \cup B_p \cup C_p. \tag{10}$$

我们声称这些集合具有以下性质：
(a) A_p 在遍历映射作用下几乎不变：$y \mapsto py$，**(b)** B_p 在遍历映射作用下几乎不变：$y \mapsto py + [1/p]$,

[9] 记号 $p \| n$ 表示 p 恰好整除 n 一次。

(c) C_p 在映射 $y \mapsto y + [1/p]$ 下不变。

要了解 (a) 为何成立，请考虑：

$$\begin{aligned} p \cdot A_p &= p \cdot \limsup_{n>0, p\nmid n} \mathbb{AO}(\mathbb{S}, n, \delta_n) \\ &\subseteq \limsup_{n>0, p\nmid n} p \cdot \mathbb{AO}(\mathbb{S}, n, \delta_n) \\ &\subseteq \limsup_{n>0, p\nmid n} \mathbb{AO}(\mathbb{S}, n, p\delta_n) && \text{根据引理 12 的第 (i) 部分} \\ &=_{a.e.} A_p && \text{根据引理 5。} \end{aligned}$$

通过非常相似的论证可以说明 (b) 为何成立，只需使用引理 12 的第 (ii)、(iii) 部分，而非第 (i) 部分。

命题 (c) 实际上最为直接，可由引理 12 的第 (iv) 部分直接得出。

现在，如果对于任意素数 p， A_p 都不是几乎空的，那么由于它在一个遍历映射下几乎不变，引理 7 告诉我们，它必定与 $\mathbb{S}$几乎相等。既然 $A_p \subseteq W$、 W 也必定与 $\mathbb{S}$ 几乎相等，那么我们就没有什么需要证明的了。

因此，我们可以假设对于所有素数 p， A_p 都是几乎空的。通过完全相同的论证，我们也可以假设对于所有素数 p， B_p 都是几乎空的。由 (10) 可知，这意味着：

$$W =_{a.e.} C_p \quad \text{for all } p.$$

因此，根据 (c)，对于所有素数 p， W 在映射 $y \mapsto y + [1/p]$ 下几乎不变。应用引理 9 即可得到结论。◀

省略代码注释后，这段 `mathlib`中的非正式证明虽然只有 ~ 30 行，其形式化版本却需要 101 行。

7 最后的话

7.1 去除 $\delta_n \to 0$ 假设

如引言中所述，定理 14 中关于 $\delta_n \to 0$ 的假设可以去掉。一个不错的后续项目是补上这种情况下的证明。将 δ_n 替换为 max(δ_n，0) 后，我们可以假设对所有 n， $0 \le \delta_n$。据此，若 $\delta_n \not\to 0$, 则事实上：

$$\mathbb{WA}(\mathbb{S}, \delta) = \mathbb{S}.$$

注意，这是集合的真正相等关系；它并非测度论结果。主要工作是建立关于约数计数函数和欧拉函数增长的一些经典界。

事实上，Bloom 和 Mehta 已经在他们令人印象深刻的单位分数项目中，将所需的一些界形式化了 形式化 Bloom 的突破 [1, 2]。相关结果迁移到 `mathlib` 后，去掉 $\delta_n \to 0$ 假设就会更加容易。

7.2 Duffin-Schaeffer 猜想

给定一个实数序列 δ_1， δ_2，……，Gallagher 定理告诉我们， $\mathbb{WA}(\mathbb{S}$， $\delta)$ 几乎相等于 $\emptyset$ 或 $\mathbb{S}$。显而易见的问题是，如何判断这两种情况中

哪一种确实会出现在当前这个序列中。Duffin-Schaeffer猜想如今已成为定理，这要归功于 Koukoulopoulos 和 Maynard；它给出了一个令人满意的答案：

$$\mathbb{WA}(\mathbb{S},\delta) =_{a.e.} \begin{cases} \emptyset & \text{if } \sum \varphi(n)\delta_n < \infty, \\ \\ \mathbb{S} & \text{if } \sum \varphi(n)\delta_n = \infty. \end{cases}$$

其中 φ 是欧拉函数。

证明 $\mathbb{WA}(\mathbb{S},\ \delta) =_{a.e.} \emptyset$ 若 $\sum \varphi(n)\delta_n < \infty$，是非常容易的（这可由 Borel-Cantelli定理的“容易”方向推出）。反过来则极其困难。这个命题最早于 1941 年提出[6]，并且近 80 年来一直是度量数论中最重要的未决问题之一。

考虑到该结果的陈述如此初等，给出反向命题的形式化证明尤其令人满意。在 Gallagher 定理之后，或许下一个最值得攻克的目标是 [11] 中的引理5.2。

7.3 对着 `master` 开发

如果没有 `mathlib` 中涵盖的代数、测度论、拓扑学等方面的庞大理论体系，就不可能完成这里讨论的工作。正如我们所说，我们的所有代码都直接添加到了 `mathlib` 的 `master` 分支中；其中大部分是“库代码”，并非专为 Gallagher 定理编写。

虽然这种方式更难以推进，但我们认为，为了实现当代数学的形式化，这一点至关重要。因此，我们希望以本项目进一步证明这一工作流程能够取得成功，并鼓励更多人效仿。

参考文献

1 Thomas F. Bloom。关于单位分数密度猜想。即将出版，2021年。URL: https://arxiv.org/abs/2112.03726, arXiv:2112.03726. 2 Thomas F. Bloom 和 Bhavik Mehta。单位分数项目。即将出版，2022年。URL: https://b-mehta.github.io/unit-fractions/. 3 Kevin Buzzard、Johan Commelin 和 Patrick Massot。完美空间的形式化。在第9届ACM SIGPLAN认证程序与证明国际会议论文集（CPP 2020），美国路易斯安那州新奥尔良，2020年1月20日至21日，第299–312页，2020年。doi:10.1145/3372885.3373830. 4 J. W. S. Cassels。丢番图逼近中的一些度量定理。I。《剑桥哲学学会会刊》，46:209–218，1950年。 doi:10.1017/s0305004100025676. 5 Johan Commelin、Adam Topaz 等。液体张量实验。即将出版，2022年。另见 https://www.nature.com/articles/d41586-021-01627-2。URL: https://github.com/leanprover-community/lean-liquid. 6 R. J. Duffin 和 A. C. Schaeffer。度量丢番图逼近中的Khintchine问题。《杜克数学杂志》，8:243–255，1941年。URL: http://projecteuclid.org/euclid.dmj/1077492641. 7 Patrick Gallagher。用既约分数逼近。《日本数学会杂志》，13:342–345，1961年。 doi:10.2969/jmsj/01340342. 8 Sébastien Gouëzel。Gromov-Hausdorff空间的形式化。CoRR，abs/2108.13660，2021年。URL: https://arxiv.org/abs/2108.13660, arXiv:2108.13660. 9 Sébastien Gouëzel。mathlib中积分变量替换公式的形式化。在Kevin Buzzard和Temur Kutsia编，智能计算机数学——第15届国际会议（CICM 2022），第比利斯，格鲁吉亚，2022年9月19日至23日，论文集，

第13467卷，出自计算机科学讲义，第3–18页。施普林格，2022年。 doi:10.1007/978-3-031-16681-5_1。10 Glyn Harman。度量数论，第18卷，出自伦敦数学会专著，新系列。克拉伦登出版社、牛津大学出版社，纽约，1998年。11 Dimitris Koukoulopoulos 和 James Maynard。关于Duffin-Schaeffer猜想。《数学年刊》（第*2*辑），192(1):251–307，2020年。 doi:10.4007/annals.2020.192.1.5。12 mathlib社区。Lean数学库。在第*9*届*ACM SIGPLAN*认证程序与证明国际会议论文集，*CPP 2020*，美国路易斯安那州新奥尔良，*2020*年*1*月*20*日至*21*日，第367–381页，2020年。 doi:10.1145/3372885.3373824。13 Floris van Doorn。Haar测度的形式化。在Liron Cohen和Cezary Kaliszyk编，第*12*届交互式定理证明国际会议（*ITP 2021*），第193卷，出自莱布尼茨国际信息学会议论文集（*LIPIcs*），第18:1–18:17页，德国达格施图尔，2021年。达格施图尔城堡——莱布尼茨信息学中心。URL: https://drops.dagstuhl.de/opus/volltexte/2021/13913， doi:10.4230/LIPIcs.ITP.2021.18。