

시작하기 전에

통용되는 한국어 단어가 있는 수학 용어는 별도의 설명 없이 한국어로 썼고, 그렇지 않은 경우에는 처음 쓸 때 영어 용어를 병기했습니다.

한국어	영어
최소 작용	minimal action
무작위 행보	random walk
등거리사상	isometry
한정된	bounded
받침	support
한계	bound
상한/하한	upper/lower bound
최소 상한	supremum
매물	embedding
궤도	orbit
준군	semigroup
군, 환, 체 맞춤 사상	homomorphism

원의 위상동형사상 군에서 자유 부분군과 TITS 대안

최인혁

ABSTRACT. 본 논문에서는 위상적인 원 S^1 의 자기위상동형사상 군 $\text{Homeo}(S^1)$ 안에서의 자유 부분군의 존재성 및 확률적인 일반성(genericity)을 살펴본다. 1부에서는 Étienne Ghys가 묻고 Gregory Margulis가 증명한 원의 위상동형사상 군에 대한 약한 위상적인 Tits 대안(Tits alternative)을 소개한다. 그말인즉 원의 위상동형사상으로 이루어진 임의의 군 G 는 다음 중 정확히 하나를 만족한다는 것인데, (i) G 의 모든 원소가 동시에 보존하는 원 위의 확률 측도가 존재하거나 혹은 (ii) G 의 원소 두 개 f, g 및 서로 겹치지 않는 원의 열린 부분집합 U_1, U_2, V_1, V_2 가 존재하여,

$$f(S^1 \setminus U_1) \subseteq U_2, f(S^1 \setminus U_2) \subseteq U_1, g(S^1 \setminus V_1) \subseteq V_2, g(S^1 \setminus V_2) \subseteq V_1$$

가 성립한다는 것이다. 이때 f, g 의 순서쌍 (f, g) 를 Schottky 순서쌍이라 부른다. 만약 G 의 모든 원소가 동시에 고정하는 점이 존재하지 않고 G 의 작용이 강하게 팽창적(strongly expansive)이라면 반드시 (ii)의 경우에 해당하며, 이때 상기한 열린 집합들 U_i, V_i 는 모두 열린 구간(interval)으로 잡을 수 있다.

2부에서는 약한 위상적인 Tits 대안의 결과물로서 얻은 Schottky 순서쌍을 무작위 행보(random walk)에 활용하는 법을 다룬다. 이를 통해 다음 두 정리에 대한 새로운 증명을 제시한다:

- (1) 자유 부분군의 일반성 (Martín Gilabert Vio): $\text{Homeo}(S^1)$ 위의 서로 독립인 두 무작위 행보 $(Z_n)_{n>0}, (Z'_n)_{n>0}$ 가 $\text{Homeo}(S^1)$ 의 어떤 부분군 G 의 모든 원소를 빠짐없이 지나고, G 의 모든 원소가 동시에 보존하는 원 위의 확률 측도가 없다고 가정하자. 그러면 0과 1 사이에 있는 상수 q 가 존재하여, 충분히 큰 모든 n 에 대해

$$\mathbb{P}(\text{두 위상동형사상 } Z_n \text{과 } Z'_n \text{은 차수 2인 } \text{Homeo}(S^1) \text{의 자유 부분군을 생성해 냄}) \geq 1 - q^n$$

이 성립한다.

- (2) 무작위 행보의 지수함수적인 축약성 (Dominique Malicet): $\text{Homeo}(S^1)$ 위의 무작위 행보 $(Z_n)_{n>0}$ 가 $\text{Homeo}(S^1)$ 의 어떤 부분군 G 의 모든 원소를 빠짐없이 지나고, G 의 모든 원소가 동시에 보존하는 원 위의 확률 측도가 없다고 가정하자. 그러면 0과 1 사이에 있는 상수 q 가 존재하여 다음이 성립한다. 원 위의 임의의 점 $x \in S^1$ 마다 그를 포함하는 열린 구간 $I_x \subseteq S^1$ 가 존재하여, 각 자연수 $n \in \mathbb{Z}_{>0}$ 마다

$$\mathbb{P}(n \text{보다 큰 각각의 } k \text{에 대해 } \text{diam}(I_x) \leq q^k \text{임}) \geq 1 - q^n$$

이 성립한다. 더 나아가, 원 위의 임의의 점 $x \in S^1$ 와 임의의 자연수 $n \in \mathbb{Z}_{>0}$ 이 주어졌을 때,

$$\mathbb{P}\left(\begin{array}{l} \text{Lebesgue 측도가 } 1 - q^n \text{ 이상이면서 } x \text{를 포함하는 열린 집합 } E(x) \subseteq S^1 \text{가 존재하여} \\ n \text{보다 큰 각각의 } k \text{에 대해 } Z_k \cdot E(x) \text{의 Lebesgue 측도가 } q^k \text{ 이하임} \end{array}\right) \geq 1 - q^n$$

이 성립한다.

위 명제는 Gilabert Vio 및 Malicet이 증명한 버전을 조금 더 강화한 것인데, 기존에는 주어진 사건의 확률이 n 이 커짐에 따라 1로 수렴함을 증명한 한편, 여기서는 그 확률이 1에 수렴하는 속도가 지수함수적임을 논한다.

사건 나열의 확률이 0 혹은 1로 수렴함을 보이는 데 흔히 에르고딕 이론(ergodic theory)을 활용하는데, Gilabert Vio 및 Malicet 또한 그러한 접근을 택하고 있다. 다만, 에르고딕 이론적인 논법으로는 사건의 확률의 지수함수적인 감소를 곧바로 관찰하기 쉽지 않다. 본 논문에서는 최근 등거리사상 군 위의 무작위 행보 이론에서 큰 진전을 이끌어낸 Sébastien Gouëzel의 방향 전환 기법(pivoting technique)을 이용해 위 명제를 조합적으로 증명한다.

이를 위해 3부에서는 먼저 거리공간의 등거리사상 군에 대한 Gouëzel의 방향 전환 기법을 개괄한다. 그후, 등거리사상 군이 아닌 (어쩌면 그 대적점에 있다고 할 수 있는) 원의 위상동형사상 군에 방향 전환 기법을 어떻게 적용할지 고찰한다.

핵심 단어. 무작위 행보, 원의 위상동형사상 군, 동기화(synchronization), Tits 대안, Schottky 순서쌍
MSC classes: 20F67, 30F60, 57M60, 60G50

1. 원의 위상동형사상 군 및 MARGULIS의 약한 TITS 대안

{sec:homeoS1}

이 절에서는 Margulis가 증명하고 Ghys가 별도로 설명한 Homeo(S^1) 위에서의 약한 Tits 대안(weak Tits alternative)를 살펴 본다. 이 절의 내용에는 새로운 것은 없으나, Margulis 및 Ghys가 택한 방법을 약간 틀어 설명하려고 한다. 이는 즉, 컴팩트한 Lie 군의 Haar 측도 혹은 원의 위상동형사상의 회전수(rotation number)을 사용하지 않은 채, 아래 정리에서 얘기하는 π 및 c 를 직접 빚겠다는 뜻이다. 이 절의 내용의 원전은 [Mar00] 및 [Ghy01]이다.

이 절의 목표는 다음 정리를 증명하는 것이다.

정리 1.1. Homeo(S^1)의 임의의 부분군 G 에 대해, 다음 중 정확히 한 가지가 성립한다.

- (1) G 의 모든 원소가 동시에 보존하는 원 위의 확률 측도가 존재한다.
- (2) 준결레바꾸기(semiconjugation) 및 유한 차수 덮음(finite-degree covering)을 통해 원래 G 의 작용에 잘 들어맞는 또다른 G 의 작용을 건설할 수 있는데, 이 새로운 작용에 대하여, 서로 겹치지 않는 원의 열린 구간에 결부된 Schottky 순서쌍이 G 안에 존재한다. 자세히 말하자면,
 - 단조증가성이고(monotone) 차수가 1인 원의 연속사상 $c : S^1 \rightarrow S^1$,
 - 원의 자가 덮음 사상 $\pi : S^1 \rightarrow S^1$

이 존재하고, 또 군 맞춤 사상 $\rho : G \rightarrow \rho(G) \leq \text{Homeo}(S^1)$ 이 존재하여, 각 $g \in G$ 마다

$$\pi \circ c \circ g = \rho(g) \circ \pi \circ c$$

가 성립하는 한편, $\rho(G)$ 의 원소 두 개 f, g 및 서로 겹치지 않는 원의 열린 구간 I_1, I_2, J_1, J_2 가 존재하여,

$$f(S^1 \setminus I_1) \subseteq I_2, f^{-1}(S^1 \setminus I_2) \subseteq I_1, g(S^1 \setminus J_1) \subseteq J_2, g^{-1}(S^1 \setminus J_2) \subseteq J_1,$$

가 성립한다.

정리 1.2. Homeo(S^1)의 어떤 부분군 G 가 원 위에서 근접적인(proximal) 작용을 가지면서 군 원소 전체가 동시에 보존하는 고정점을 가지지 않는다. 그러면 G 의 원소 f, g 및 서로 겹치지 않는 원의 열린 구간 I_1, I_2, J_1, J_2 가 존재하여,

$$f(S^1 \setminus I_1) \subseteq I_2, f^{-1}(S^1 \setminus I_2) \subseteq I_1, g(S^1 \setminus J_1) \subseteq J_2, g^{-1}(S^1 \setminus J_2) \subseteq J_1,$$

가 성립한다.

이는 특히 G' 가 차수 2인 자유 부분군을 가짐을 의미한다 (Margulis).

1.1. 원의 위상동형사상 위상공간 및 측도공간으로서, 원 S^1 는 실수 집합 \mathbb{R} 을 $\mathbb{Z} \simeq \langle z \mapsto z + 1 \rangle$ 의 작용으로 자른 것이다. 이를 기록하는 사영(projection) $\Pi : \mathbb{R} \rightarrow S^1$ 을 기억하도록 하자.

원 S^1 의 자기위상동형사상(self-homeomorphism)들은 자기들끼리 군을 이룬다. 이 군을 Homeo(S^1)로 표기한다. Homeo(S^1)은 매우 많은 부분군을 품고 있기에 어떤 군들이 Homeo(S^1)의 부분군으로 나타날 수 있는지 물어볼 수 있다. 이를 위해 다음 개념을 정의하자. 어떤 군 G 로부터 Homeo(S^1)로 향하는 군 맞춤 사상(group homomorphism) $\varphi : G \rightarrow \text{Homeo}(S^1)$ 를 다른 말로 S^1 상의 작용(action)이라고 부른다. 다시 말해, 어떤 군 G 가 원 S^1 에 작용한다는 것은, 군 맞춤 사상 $\varphi : G \rightarrow \text{Homeo}(S^1)$ 를 하나 정한다는 것이다.

연속함수 $f : S^1 \rightarrow S^1$ 를 생각하자. 이때, $\Pi \circ \tilde{f} = f \circ \Pi$ 가 성립하게끔 하는 연속함수 $\tilde{f} : \mathbb{R} \rightarrow \mathbb{R}$ 가 존재한다. 이때 \tilde{f} 를 f 의 \mathbb{R} 로의 끌어올림(lift)이라고 부른다. f 의 끌어올림 \tilde{f} 는 유일하지는 않지만

$z \mapsto z + 1$ 의 작용을 통해 모든 선택지 사이를 오갈 수 있다. 더욱이, $\tilde{f}(x+1) - \tilde{f}(x)$ 는 정수 값을 가지며, 그 값은 \tilde{f} 의 선택지 혹은 $x \in \mathbb{R}$ 의 선택지에 의존하지 않는다. 이 정수 값을 f 의 차수(degree)라고 부른다. 합성함수의 차수는 두 성분 함수의 차수의 곱이고, 이로써 원의 위상동형사상의 차수는 반드시 1 혹은 -1 이어야 함을 알 수 있다. 또한, 차수가 1인 위상동형사상들의 집합은 $\text{Homeo}(S^1)$ 의 지수 2짜리 부분군을 이루고, 이를 $\text{Homeo}_+(S^1)$ 로 표기한다. 차수가 1인 위상동형사상을 다른 말로 **방향 보존 위상동형사상**이라고 부르기도 한다.

한편, 주어진 연속함수 $f : S^1 \rightarrow S^1$ 에 대해, 그 끌어올림 \tilde{f} 는 유일하지 않지만 끌어올림의 단조증가성, 단조감소성 및 단조성은 잘 정의된다. 이를 바탕으로 f 의 단조증가/감소성 및 단조성을 정의한다.

1.2. 켈레바꾸기 및 준켈레바꾸기(conjugation and semiconjugation). S^1 을 위상공간으로 보면 S^1 의 위상동형사상 f 의 위상적 동역학을 분석할 때, 이를테면 $f(x)$ 가 x 보다 $1/3$ 바퀴 앞서 있는지를 묻는 것은 그다지 의미 있는 질문이 아니다. S^1 의 각 점에 매겨진 좌표, 즉 거리 구조를 신경 쓰지 않기 때문이다. 다시 말해, f 의 위상적 동역학을 공부하고 싶다면 S^1 의 위상 구조를 보존하는 좌표 변환에 의해 좌우되지 않는 성질 혹은 불변량을 알아야 한다. 이에 다음 개념이 필요해진다.

정의 1.3. 두 위상동형사상 $f, g \in \text{Homeo}(S^1)$ 가 서로의 위상적 좌표변형(topological conjugate)이라는 것은 어떤 위상동형사상 $h \in \text{Homeo}(S^1)$ 가 존재하여 $h \circ f = g \circ h$ 가 성립한다는 것이다. 이때, $g = hfh^{-1}$ 을 f 의 h 에 의한 위상적 좌표변형이라고 한다. 다른 관점에서 보면, 위상동형사상 $h \in \text{Homeo}(S^1)$ 가 주어질 때마다 $f \mapsto hfh^{-1}$ 라는 $\text{Homeo}(S^1)$ 안의 자기사상이 정의되는데, 이 자기사상을 h 에 의한 켈레바꾸기(conjugation by h)라고 부른다.

마찬가지로, 어떤 군 Γ 의 원에 대한 두 작용 $\Phi_1, \Phi_2 : \Gamma \rightarrow \text{Homeo}(S^1)$ 가 서로의 위상적 좌표변형이라는 것은, 어떤 위상동형사상 $h \in \text{Homeo}(S^1)$ 가 존재하여 각 $g \in \Gamma$ 마다 $h \circ \Phi_1(g) = \Phi_2(g) \circ h$ 가 성립한다는 것이다.

어떤 위상동형사상을 위상적으로 켈레바꾸더라도 (위상적) 동역학적인 성질은 하나도 잃지 않는다. 한편, 어떤 위상동형사상들은 원의 특정 부분에서는 복잡한 동역학을 보이고, 다른 부분에서는 재미없는 동역학을 보인다. 이때, 전자 영역을 그대로 남겨 복잡한 동역학적 정보는 살리면서 후자 영역은 각 연결성분을 한 점으로 압축해 자명한 정보는 무시하면 편리하다. 이러한 정보의 축약은 (위상동형사상 대신) 단조적이고 차수가 1인 연속사상이 담당하기에 다음 개념이 필요해진다.

정의 1.4. 두 위상동형사상 $f, g \in \text{Homeo}(S^1)$ 에 대해, g 가 f 의 준좌표변형(semiconjugate)이라는 것은 단조적인 차수 1짜리 연속사상 $h : S^1 \rightarrow S^1$ 가 존재하여 $h \circ f = g \circ h$ 가 성립한다는 것이다.

마찬가지로, 어떤 군 Γ 의 원에 대한 두 작용 $\Phi_1, \Phi_2 : \Gamma \rightarrow \text{Homeo}(S^1)$ 가 준좌표변형이라는 것은, 단조적인 차수 1짜리 원의 연속사상 h 가 존재하여 각 $g \in \Gamma$ 마다 $h \circ \Phi_1(g) = \Phi_2(g) \circ h$ 가 성립한다는 것이다.

명제 1.5. $\text{Homeo}(S^1)$ 의 임의의 부분군 G 에 대해 다음 셋 중 정확히 하나가 성립한다.

- (1) 유한한 G -궤도가 존재한다. 즉, $\#\{gx : g \in G\} < +\infty$ 인 점 x 을 원에서 잡을 수 있다.
- (2) 모든 G -궤도가 원 안에서 조밀하다. 다시 말해, 그 어느 $x \in S^1$ 에 대해서도 $G \cdot x \subseteq S^1$ 의 닫음(closure)이 원 전체다.
- (3) G 에 불변하는 (공집합이 아닌) 닫힌 부분집합 중 최소한이고, 무한집합이면서 원 전체가 아닌 $K \subsetneq S^1$ 이 존재한다.

(3)의 경우에는 G 에 불변하는 (공집합이 아닌) 닫힌 부분집합 중 최소한인 K 는 유일하고, Cantor 집합과 위상동형이며, 그 어느 G -궤도의 집적점 집합에도 포함된다. (*)

{dfn:semicon

{prop:tricho

Proof. S^1 의 부분집합에 대한 다음 성질을 먼저 정의하자. 먼저

$$\mathcal{S} := \{A \subseteq S^1 : A \text{는 공집합이 아닌 컴팩트 집합이면서 } G \text{에 불변함}\}$$

를 정의하자. 그러면 \mathcal{S} 의 원소 간에는 집합 포함관계라는 부분순서(partial order)가 정의되어 있다. 이제, 어떤 $A \in \mathcal{S}$ 가 \mathcal{S} 안에서 최소한(minimal)일 때, A 가 G -최소한이라고 하겠다. 이제 $x \in A$ 를 임의로 하나 뽑은 뒤, x 의 G -궤도 $G \cdot x$ 를 생각하자. A 가 G -불변이기에 $G \cdot x$ 는 A 에 포함된다. 그러면 $G \cdot x$ 의 닫음 $\overline{G \cdot x}$ 역시 A 의 부분집합이면서 G -불변이고, 닫혀 있기까지 하다. 이에 A 의 최소성으로부터 $A = \overline{G \cdot x}$ 임이 따라나온다. 이 관찰을 요약하면 다음과 같다.

주장 1.6. S^1 의 부분집합 A 가 G -최소한이라고 하자. 그러면 그 어느 $x \in A$ 에 대해서도, x 의 G -궤도 $G \cdot x$ 의 닫음 $\overline{G \cdot x}$ 는 A 와 일치한다.

이제 원래 명제로 돌아가자. Zorn의 보조정리에 의해, G -최소한인 부분집합은 적어도 하나는 존재한다. 그중 하나를 K 라고 이름붙이자. K 의 집적점 집합

$$K' := \{x \in S^1 : \text{서로 다른 } k_1, k_2, \dots \text{가 있어 } \lim_i k_i = x \text{가 성립함}\}$$

과 K 의 경계 $\partial K := K \setminus \text{int } K$ 는 각각 G -불변인 K 의 닫힌 부분집합이 된다. 이때 다음 중 하나가 성립한다.

- (a) $K' = \emptyset$: 이는 K 가 유한집합이라는 뜻이다. 주장 1.6에 의해, 그 어느 $x \in K$ 에 대해서도 K 는 x 의 G -궤도 $G \cdot x$ 와 일치한다. 즉 (1)이 성립한다.
- (b) $\partial K = \emptyset$: 이는 $K = S^1$ 을 의미하며, 주장 1.6에 의해, 그 어느 $x \in K = S^1$ 에 대해서도 K 는 $G \cdot x$ 의 닫음 $\overline{G \cdot x}$ 와 일치한다. 즉 (2)가 성립한다.
- (c) K' 도 ∂K 도 공집합이 아님: 이 경우 K 는 무한집합이고 원 전체는 아니다. 즉 (3)이 성립한다.

한편 결론부의 (1)과 (2)가 양립할 수 없음은 분명하다. 따라서 [(a) \Rightarrow (1) \Rightarrow (a) 혹은 (c)] 및 [(b) \Rightarrow (2) \Rightarrow (b) 혹은 (c)]가 성립한다. 여기에 더해 [(3) \Rightarrow (*)]를 증명하기만 하면,

$$[(c) \Rightarrow (3) \Rightarrow (*) \Rightarrow \text{임의의 } G\text{-최소한인 집합은 Cantor 집합} \Rightarrow (a) \text{도 } (b) \text{도 아님}]$$

임을 알 수 있어, [(a) \Leftrightarrow (1)], [(b) \Leftrightarrow (2)], [(c) \Leftrightarrow (3)]을 완성하게 된다.

이제 [(3) \Rightarrow (*)]을 완성하기 위해서는 다음을 관찰하면 된다.

주장 1.7. S^1 의 부분집합 A 가 G -최소한이면서 무한집합이고 원 전체는 아니라고 하자. 그러면 A 는 Cantor 집합과 위상동형이다. 그러면 임의의 $x \in S^1$ 에 대해, $G \cdot x$ 의 집적점 집합은 A 를 포함한다.

실제로, 주장 1.6 및 주장 1.7를 상정하고, K 및 K_1 가 G -최소한임과 동시에 K 가 조건 (c)를 만족한다고 가정하자. 그러면 (공집합이 아님을 이용해) K_1 의 임의의 원소 x 를 뽑으면 $G \cdot x$ 의 극점 집합은 K 를 포함하는데, 이 극점 집합은 주장 1.6에 의해 K_1 에 포함된다. 따라서 $K \subseteq K_1$ 이고, K_1 의 최소성으로부터 $K = K_1$ 임을 이끌어낼 수 있다.

이제 주장 1.7를 증명하는 일만 남았다. 먼저, A 가 무한집합이라는 것은 A' 가 공집합이 아니라는 것이고, A 가 원 전체가 아니라는 것은 ∂A 가 공집합이 아니라는 것이다. A 가 G -불변인 닫힌 집합이기에 이 두 집합 A' 및 ∂A 는 A 에 포함된 G -불변인 닫힌 집합이다. 그러면 A 의 최소성으로부터 $A' = \partial A = A$ 임을 알 수 있다. 이는 곧 A 가 Cantor 집합과 위상동형이라는 뜻이다.

이제 원 위의 임의의 점 x 를 잡고 그 궤도 $G \cdot x$ 를 생각하자. 만약 $x \in A$ 라면 $\overline{G \cdot x}$ 는 A 에 포함된 (공집합이 아닌) G -불변인 닫힌 집합이기에, A 의 최소성으로부터 $\overline{G \cdot x} = A$ 임을 알 수 있다. 다음으로

x 가 A 밖에 있다고 가정하자. 그러면 x 는 $S^1 \setminus A$ 의 어떤 연결성분 $(a, b) \subseteq S^1$ 에 포함되어 있다. 이제 임의의 $y \in A$ 가 $G \cdot x$ 의 극점임을 결론짓기 위해서는, y 의 임의의 근방 N 에 대해 $N \cap (G \cdot x)$ 의 크기가 무한하다는 것만 보이면 된다.

여기서 A 가 완벽집합(perfect set)이기 때문에 N 은 무한히 많은 A 의 원소를 가지고 있다. 임의의 자연수 k 를 정하고, $A \cap N$ 의 원소 $2k + 1$ 개를 뽑은 뒤 (근방 N 안에서 정의된 방향에 따라) 왼쪽부터 순서대로 a_0, a_1, \dots, a_{2k} 이라고 이름붙이자. 이제 각 $i = 1, \dots, k$ 마다 주장 1.6에 의해 a_{2i-1} 은 $G \cdot a$ 의 극점이고, 따라서 $g_i a \in (a_{2i-2}, a_{2i})$ 이게끔 하는 $g_i \in G$ 가 존재한다. 이때 $g_i(a, b)$ 는 한쪽 끝점이 $[a_{2i-2}, a_{2i}]$ 안에 위치하는 $S^1 \setminus A$ 의 연결성분이고, a_{2i-2} 및 a_{2i} 는 $S^1 \setminus A$ 바깥에 있음을 주목하라. 이는 $g_i x \in (g_i a, g_i b) \subseteq (a_{2i-2}, a_{2i}) \subseteq N$ 을 의미한다. $(a_0, a_2), (a_2, a_4), \dots, (a_{2k-2}, a_{2k})$ 는 서로 겹치지 않는 구간들이기에, $g_1 x, \dots, g_k x$ 는 모두 서로 다른 x 의 G -궤도 점들이다. 요약하자면, 임의의 자연수 k 에 대해 $N \cap (G \cdot x)$ 의 크기는 k 이상이다. 다시 말해, $N \cap (G \cdot x)$ 의 크기는 무한하다. \square

위 명제에서의 (2)의 경우에, 즉 G -궤도가 원 안에서 조밀할 때 G 의 작용이 *최소한이다*(minimal)라고 한다. 최소한이 아닌 작용의 경우 G -궤도가 신경쓰는 영역, 즉 $\overline{G \cdot x}$ 만을 남기고 나머지를 정의역에서 삭제함으로써 최소한인 작용으로 환원할 수 있다는 점에서 이 용어의 의미가 드러난다. 다만, 이 과정은 $\overline{G \cdot x}$ 가 충분히 커서 여전히 원을 이룰 수 있을 때만 유용하다. 위 명제 속 (1)에서의 유한한 G -궤도는 원을 이루기에 너무 작지만, (3)에서의 Cantor set은 S^1 로의 전사함수를 가지기에 상기한 전략을 적용할 수 있다. 위 명제에서의 (3)의 경우, G 가 예외적인 최소 집합 K 를 가진다고 말하기도 한다.

명제 1.8. 만약 $\text{Homeo}_+(S^1)$ 의 한 부분군 G 가 예외적인 최소 집합을 가질 경우, 준켈레바꾸기를 통해 최소한인 작용으로 바꿀 수 있다. 다시 말해, G 로부터 $\text{Homeo}_+(S^1)$ 의 다른 부분군 G' 로 향하는 군 맞춤 사상 $\rho: G \rightarrow G'$ 및 단조적인 차수 1짜리 연속사상 $h: S^1 \rightarrow S^1$ 가 존재하여 $h \circ g = \rho(g) \circ h$ 가 성립한다.

Proof. G 의 예외적인 최소 집합을 K 라고 하자. 그러면 $S^1 \setminus K$ 는 가산 개의 서로 겹치지 않는 열린 구간으로 이루어져 있는데, 각각의 열린 구간의 단음을 한 점으로 묶어 내면 그 몫공간(quotient space)은 여전히 위상적인 원이 된다. 다시 말해, $S^1 \setminus K$ 의 각 연결 성분 및 그 양 끝점을 한 점으로 축약시키는 단조적인 연속 함수 $h: S^1 \rightarrow S^1$ 가 존재한다는 것이다. (K 가 이를테면 표준적인 Cantor 집합이라면 h 는 Cantor 3진 함수로 구현할 수 있다.) 이때 임의의 $y \in S^1$ 에 대해 $h^{-1}(y)$ 는 $S^1 \setminus K$ 의 한 연결 성분의 단음이거나 혹은 한 점이다. 즉 $h^{-1}(y)$ 는 어떠한 경우에도 연결된 부분집합이고, h 의 차수는 ± 1 임을 알 수 있다. 여기서 치역인 원에 적절한 방향을 줌으로써 h 의 차수가 1이게 할 수 있다.

이제 각 $g \in G$ 에 대해 $\rho(g)$ 를 구성해 보자. 임의의 점 $y \in S^1$ 에 대해, $h^{-1}(y)$ 는 $S^1 \setminus K$ 의 한 연결성분의 단음이거나 혹은 한 점이다. g 는 최소 집합인 K 를 보존하기에, $S^1 \setminus K$ 의 연결성분을 연결성분으로 보낸다. 따라서, $g(h^{-1}(y))$ 는 여전히 $S^1 \setminus K$ 의 한 연결성분의 단음이거나 혹은 한 점이고, 따라서 h 를 취하면 한 점으로 묶여 나온다. 이 덕분에, y 의 $\rho(g)$ 에 의한 함숫값을 $(\rho(g))(y) := (h \circ g)(h^{-1}(y))$ 로 잘 정의할 수 있다. 주어진 g 에 대해, $f \circ h = h \circ g$ 를 만족하는 함수 $f: S^1 \rightarrow S^1$ 는 상술한 $\rho(g)$ 밖에 없다 (\dagger).

이렇게 정의한 $\rho(g)$ 가 연속일 충분조건은 임의의 열린 구간 U 의 역상 $V := (\rho(g))^{-1}(U)$ 가 열린 구간이라는 것이다. 여기서 $h \circ g$ 가 단조적인 연속함수이기에 $h^{-1}(V) = (h \circ g)^{-1}(U)$ 는 열린 구간인데, 그 끝점들은 $\overline{S^1 \setminus K}$ 안에 위치할 수는 없다 (*). 실제로, 만약 예를 들어 $h^{-1}(V)$ 가 $S^1 \setminus K$ 의 어떤 연결성분 I 와 조금이라도 겹친다면, 모든 $x \in \bar{I}$ 에 대해 $h(x)$ 는 동일하고 이 값이 V 에 들어간다.

따라서 $h^{-1}(V)$ 는 \bar{I} 전체를 포함하고, $h^{-1}(V)$ 의 왼쪽 끝점도 오른쪽 끝점도 \bar{I} 바깥에 형성된다. (*)를 만족하는 열린 구간의 h -이미지는 마찬가지로 열린 구간이기에 증명이 끝난다.

마지막으로, ρ 가 G 의 연산과 잘 어울리는지를 확인하자. 정의로부터

$$h \circ g_1 \circ g_2 = \rho(g_1) \circ h \circ \rho(g_2) = \rho(g_1) \circ \rho(g_2) \circ h$$

임을 관찰할 수 있고, 성질 (†)로부터 $\rho(g_1)\rho(g_2) = \rho(g_1g_2)$ 을 이끌어낼 수 있다. 특히, $\rho(id) = id$ 임을 알기에 각 $g \in G$ 마다 $\rho(g)\rho(g^{-1}) = \rho(g^{-1})\rho(g) = id$ 가 성립한다. 연속인 역함수를 가지는 연속함수인 $\rho(g)$ 는 S^1 의 자기위상동형사상이어야만 한다. 이로써 증명이 끝난다. \square

1.3. 팽창성(Expansivity) 혹은 근접성(Proximality). 이 절에서는 $\text{Homeo}(S^1)$ 의 부분군에 대한 동역학적인 특성을 하나 정의하고, $\text{Homeo}(S^1)$ 의 부분군이 만족할 수 있는 이분법적인 상황을 기술할 것이다. 이는 정리 1.2을 위한 예비적인 단계로 볼 수 있다.

정의에 앞서 $\text{Homeo}(S^1)$ 안에 있는 부분군 두 개를 살펴보겠다. 이 논의에서 원 S^1 을 복소평면 \mathbb{C} 안의 단위원 $\{z : |z| = 1\}$ 과 동일시하겠다. 이 원은 Poincaré 계량이 없어진 원판 $\mathbb{D} := \{z : |z| < 1\}$ 의 가장자리로 볼 수 있으며, \mathbf{D} 의 등거리사상 군

$$\text{PSU}(1, 1) := \left\{ \begin{pmatrix} \alpha & \beta \\ \beta^* & \alpha^* \end{pmatrix} : \alpha, \beta \in \mathbb{C}, |\alpha|^2 - |\beta|^2 = 1 \right\}$$

은 자연히 S^1 에 작용한다. 즉 $\text{PSL}(1, 1)$ 을 $\text{Homeo}(S^1)$ 의 부분군으로 간주할 수 있다.

$\text{PSU}(1, 1)$ 안에는 원점 기준 회전 $\begin{pmatrix} e^{i\theta/2} & 0 \\ 0 & e^{-i\theta/2} \end{pmatrix}$ 들이 살고 있다. 이 회전들의 집합 \mathcal{R} 은 더 작은 부분군을 이루며, S^1 위의 호 길이를 보존한다. 즉 원점 기준 각도를 이용해 S^1 위에 거리 구조 d 혹은 길이 측도 μ 를 구성하면, \mathcal{R} 은 (S^1, d) 의 등거리사상 군이 되고 또 (S^1, μ) 라는 확률 공간의 측도 보존사상 군이 된다. 이렇게 S^1 상의 어떤 확률 측도 혹은 거리 구조를 보존하는 부분군이 \mathcal{R} 만 있는 것은 아니다. 예를 들면, 원점 $\mathbf{0}$ 을 다른 점 $p \in \mathbf{D}$ 로 옮기는 행렬 $M_p \in \text{PSU}(1, 1)$ 을 생각하면, M_p 에 의한 \mathcal{R} 의 켈레바꿈(conjugate) $\mathcal{R}_p := M_p \mathcal{R} M_p^{-1}$ 은 이제 $M_p^* d$ 및 $M_p^* \mu$ 라는 새로운 거리 구조 및 확률 측도를 보존하는 군이 된다. 비록 $M_p^* d$ 와 d 가 다른 거리 구조이기는 하지만 상수배 동치 관계에 있다. 즉 $C^{-1}d \leq M_p^* d \leq Cd$ 이 성립하게끔 하는 양수 C 가 존재한다. 따라서 \mathcal{R}_p 는 비록 d 를 보존하지는 않으나 심각하게 뒤를 수는 없다. 다시 말하자면, \mathcal{R}_p 의 원소들은 (S^1, d) 위에서 *균일연속하다* (equicontinuous).

한편, \mathbb{D} 는 곡률이 -4인 쌍곡 곡면들의 보편적 덮개 공간(universal covering space)이기도 하다. 따라서 $\text{PSU}(1, 1)$ 안의 이산 군(discrete group)들 \mathbb{D} 에 어떻게 작용하는지를 보는 것이 중요한데, 이러한 군들을 *Fuchsian* 군이라고 부른다. 이제 유한한 넓이를 가지는 쌍곡 곡면을 하나 생각하자. 이 곡면은 \mathbb{D} 를 어떤 Fuchsian 군 $G \leq \text{PSU}(1, 1)$ 로 잘라낸 것인데, 이 G 에는 반드시 균일연속성을 해치는 원소가 존재한다. 구체적으로, G 의 원소인 행렬 $f \in G$ 및 S^1 위의 서로 다른 점 x 및 y 가 존재하여, $S^1 \setminus y$ 안의 임의의 콤팩트 집합 K 에 대해 $\lim_{i \rightarrow +\infty} \text{diam}(y \cup f^i K) = 0$ 이 성립하고, $S^1 \setminus x$ 안의 임의의 콤팩트 집합 K 에 대해 $\lim_{i \rightarrow +\infty} \text{diam}(x \cup f^{-i} K) = 0$ 이 성립한다. 이러한 G 의 원소를 쌍곡행렬(hyperbolic matrix) 혹은 쌍곡적인 원소(hyperbolic element)라고 부른다. 또, x 를 f 의 작용에 대한 밀개(repeller), y 를 끌개(attractor)라고 부른다. 이 두 점은 정확히 f 의 작용에 대한 S^1 상의 고정점(fixed point theorem)이다.

실은, G 에는 본질적으로 다른 쌍곡적인 원소가 수없이 많이 존재한다. 구체적으로, f 의 작용에 대한 밀개 x 및 끌개 y , 그리고 g 의 작용에 대한 밀개 x' 및 끌개 y' 네 점이 모두 서로 다르게끔 G 의 원소 두

개 $f, g \in G$ 를 찾을 수 있다. 이 경우, x, y, x', y' 를 각각 포함하는 충분히 작은 열린 구간들 I_1, I_2, J_1, J_2 를 잡으면 이들 열린 구간들 또한 서로 겹치지 않는다. 또한 f 및 g 의 동역학이 쌍곡적이기에 충분히 큰 N 에 대해

$$f^N(S^1 \setminus I_1) \subseteq I_2, f^{-N}(S^1 \setminus I_2) \subseteq I_1, \\ g^N(S^1 \setminus J_1) \subseteq J_2, g^{-N}(S^1 \setminus J_2) \subseteq J_1$$

가 성립한다. 이는 곧 정리 1.2에서 얻고자 했던 결론 중 한 경우인데, 우리 논증에서 중요한 역할을 하는 상황이기 때문에 이름을 따로 붙이겠다.

정의 1.9. 원의 자기위상동형사상 f 와 g 를 생각하자. 만약

$$f(S^1 \setminus U_1) \subseteq U_2, f(S^1 \setminus U_2) \subseteq U_1, g(S^1 \setminus V_1) \subseteq V_2, g(S^1 \setminus V_2) \subseteq V_1$$

를 만족하는 서로 겹치지 않는 원의 열린 부분집합 U_1, U_2, V_1, V_2 가 존재한다면, f 와 g 의 순서쌍 (f, g) 를 $(U_1, U_2, V_1, V_2$ 에 결부된) Schottky 순서쌍이라고 부른다.

위 두 예시에서 대조되는 동역학은 일반적인 $\text{Homeo}(S^1)$ 의 부분군에서도 관찰된다는 것이 바로 정리 1.2의 주제다. 이제 정리 1.2을 몇 단계에 걸쳐 증명하겠다. 먼저 정리 1.2의 두 결론이 양립할 수 없음을 관찰하자.

보조정리 1.10. $\text{Homeo}(S^1)$ 의 부분군 G 가 원 위의 어떤 확률 측도를 보존한다고 하자. 그러면 G 안에는 Schottky 순서쌍이 존재할 수 없다. 특히, G 는 정리 1.2의 (2)의 경우에 해당할 수 없다.

Proof. G 가 $\text{Homeo}(S^1)$ 의 부분군이라고 하자. 만약 G 가 정리 1.2의 (2)의 경우에 해당한다면 G 는 Schottky 순서쌍을 가진다는 것을 보이자. 이를 위해 어떤 덮음 사상 c , 준결레바꾸기 π , 군 맞춤 사상 ρ 및 열린 구간 I_i, J_i 에 결부된 $\rho(G)$ 안의 Schottky 순서쌍 (f, g) 을 통해 G 가 정리 1.2의 (2)의 결론을 만족한다고 가정하고, $\rho(f) = f, \rho(g) = g$ 인 두 원소 $f, g \in G$ 를 잡자. 그러면

$$f(S^1 \setminus (\pi \circ c)^{-1}(I_1)) = (\pi \circ c)^{-1}(f(S^1 \setminus I_1)) \subseteq (\pi \circ c)^{-1}(I_2)$$

가 성립한다. 비슷한 이유로

$$f(S^1 \setminus (\pi \circ c)^{-1}(I_2)) \subseteq (\pi \circ c)^{-1}(I_1), g(S^1 \setminus (\pi \circ c)^{-1}(I_1)) \subseteq (\pi \circ c)^{-1}(I_2), g(S^1 \setminus (\pi \circ c)^{-1}(I_2)) \subseteq (\pi \circ c)^{-1}(I_1)$$

를 관찰할 수 있다. 또 I_1, I_2, J_1, J_2 가 서로 겹치지 않는 열린 구간이니 (연속사상인) $\pi \circ c$ 로 이들의 역상을 취하면 서로 겹치지 않는 열린 집합이 된다. 이로써 (f, g) 가 G 안의 Schottky 순서쌍임을 알 수 있다.

이제, 서로 겹치지 않는 열린 집합 U_1, U_2, V_1, V_2 에 결부된 Schottky 순서쌍 (f, g) 가 주어졌을 때, f 와 g 가 동시에 보존하는 확률 측도가 없다는 것만 보이면 된다. 이를 위해, f 및 g 가 어떤 유한 측도 μ 를 동시에 보존한다고 가정하자. 이때, $\{f^i(S^1 \setminus (U_1 \cup U_2)) : i \in \mathbb{Z}\}$ 는 서로 겹치지 않는 집합들의 모임임을 관찰할 수 있다. 이는

$$U_2 \supseteq f(S^1 \setminus U_1) \supseteq f(U_2) \supseteq f^2(S^1 \setminus U_1) \supseteq \dots f^i(U_2) \supseteq f^{i+1}(S^1 \setminus U_1) \supseteq f^{i+1}(U_2) \supseteq \dots$$

라는 포함관계로부터 따라나온다. f 가 μ 를 보존하므로 $f^i(S^1 \setminus (U_1 \cup U_2))$ 에 모두 같은 μ 값을 부여하는데, 이 집합들이 서로 겹치지 않으므로

$$\mu\left(\bigcup_{i \in \mathbb{Z}} f^i(S^1 \setminus (U_1 \cup U_2))\right) = \sum_{i \in \mathbb{Z}} \mu\left(f^i(S^1 \setminus (U_1 \cup U_2))\right) = \infty \cdot \mu(S^1 \setminus (U_1 \cup U_2))$$

가 성립한다. μ 가 유한 측도이므로, $S^1 \setminus (U_1 \cup U_2)$ 의 μ 값이 0일 수밖에 없다.

마찬가지 이유로, g 와 집합 $S^1 \setminus (V_1 \cup V_2)$ 사이 관계를 생각하면 $\mu(S^1 \setminus (V_1 \cup V_2)) = 0$ 을 관찰할 수 있다. 이제 $S^1 = (S^1 \setminus (U_1 \cup U_2)) \cup (S^1 \setminus (V_1 \cup V_2))$ 임을 이용하면 $\mu(S^1)$ 또한 0임을 알 수 있다. 즉, f 와 g 둘 다에 의해 보존되는 유한 측도는 영측도밖에 없고, 확률 측도는 보존될 수 없다. 이로써 증명이 끝난다. \square

이제 정리 1.2의 이분법적인 상황을 기술하기 위한 개념을 하나 정의하겠다.

정의 1.11. Homeo(S^1)의 부분군 G 가 주어졌을 때, 만약 원의 각 점 $x \in S^1$ 마다 그를 포함하는 열린 구간 $I_x \subsetneq S^1$ 이 존재해 $\{\text{diam}(gI_x) : g \in G\}$ 의 최대 하한이 0이 된다면, G 의 작용이 팽창적(expansive)이라고 부른다. 만약 임의의 닫힌 구간 $I \subsetneq S^1$ 에 대해 $\inf_{g \in G} \text{diam}(gI) = 0$ 가 성립한다면, G 의 작용이 강하게 팽창적(strongly expansive)이라고 부른다.

이것과 연관된 개념으로 근접성(proximality)가 있다. Homeo(S^1)의 어떤 부분군 G 의 작용이 근접적(proximal)이라는 것은, 임의의 $x, y \in S^1$ 에 대해 $\inf_{g \in G} d(gx, gy) = 0$ 이라는 뜻이다. G 의 작용이 강하게 팽창적이라면 반드시 근접적이어야 함은 쉽게 관찰할 수 있다. G 의 작용이 최소한이라는 가정 하에, 그 역 또한 성립함을 곧 관찰할 것이다.

보조정리 1.12. 원 위의 최소한인 작용은 팽창적이거나 혹은 균일연속하다.

Proof. Homeo(S^1)의 부분군 G 를 하나 생각하고, G 의 작용이 최소한이지만 균일연속하지 않다고 가정하자. 두번째 조건은 다시말해 어떤 $\epsilon > 0$ 및 $x_n, y_n \in S^1, g_n \in G$ 가 존재해 $\lim_{n \rightarrow \infty} d(x_n, y_n) = 0$ 및 $d(g_n x_n, g_n y_n) > \epsilon$ 이 성립한다는 뜻이다. 여기서 x_n 과 y_n 을 양 끝점으로 가지는 원 위의 구간은 두 개가 있는데, 그중 크기가 더 작은 것을 I_n 이라고 부르자. 이는 $\lim_{n \rightarrow \infty} \text{diam}(I_n) = 0$ 임을 보장한다. $g_n I_n$ 의 중점을 c_n 이라고 부르겠다.

원은 콤팩트하므로, $(x_n)_{n>0}, (y_n)_{n>0}$ 및 $(g_n)_{n>0}$ 을 어떤 부분나열로 대신함으로써 $(g_n x_n)_{n>0}, (g_n y_n)_{n>0}$ 및 $(g_n c_n)_{n>0}$ 가 각각 원 위의 어떤 점 a, b 및 c 로 수렴한다는 것을 보장할 수 있다. 이때 $d(a, b) = \lim_n d(g_n x_n, g_n y_n) > \epsilon$ 임을 관찰할 수 있다.

이제 c 를 중점으로 하는 길이 $\frac{1}{10}d(a, b)$ 짜리 구간 I 를 생각하자. 그러면 충분히 큰 n 에 대해 다음이 성립한다.

$$(1) \quad d(c, g_n c_n) < \frac{1}{100}d(a, b) \leq \text{diam}(I)/2 \text{이므로 } g_n c_n \text{은 } I \text{에 포함된다.}$$

$$(2) \quad d(g_n x_n, c) > d(a, c) - d(a, g_n x_n) > 0.4d(a, b) \text{이므로 } g_n x_n \text{은 } I \text{ 바깥에 있다. 마찬가지로, } g_n y_n \text{은 } I \text{ 바깥에 있다.}$$

즉, I 는 $S^1 \setminus \{g_n x_n, g_n y_n\}$ 를 이루는 두 열린 구간 중 $g_n c_n$ 을 포함하는 구간인 $g_n I_n$ 에 포함되어 있다. 이는 곧

$$g_n^{-1}I \subseteq g_n^{-1}(g_n I_n) = I_n, \quad \lim_{n \rightarrow \infty} \text{diam}(g_n^{-1}I) = 0$$

이라는 사실로 이어진다.

이제 임의의 점 $x \in S^1$ 을 생각하자. G 의 작용이 최소한이라고 가정했으므로 $d(gx, c) < \frac{1}{10}d(a, b)$, 즉 $gx \in I$ 이게끔 하는 $g \in G$ 가 존재한다. 이 경우 $g^{-1}I$ 는 x 의 근방인 열린 구간이면서 $\lim_{n \rightarrow \infty} \text{diam}(g_n^{-1}g \cdot (g^{-1}I)) = 0$ 을 만족한다. 각각의 $x \in S^1$ 에 대해 이러한 열린 구간을 잡아줄 수 있으므로, G 의 작용은 팽창적이라고 할 수 있다. \square

이제 S^1 안의 구간을 생각할 때 방향이 중요해지므로 다음을 상기하도록 하자. 먼저, 사영 $\Pi : \mathbb{R} \rightarrow S^1$ 을 고정했다는 사실을 기억하자. S^1 위의 구간이란 원 전체가 아닌 연결된 부분집합을 뜻한다. 원

위의 닫힌 구간을 만들기 위해서는, 차이가 1보다 작은 두 실수 $a < b$ 를 고정한 뒤, (a, b) 를 사영하면 된다. 이때, $\Pi(a)$ 를 $\Pi([a, b])$ 의 왼쪽 끝점, $\Pi(b)$ 를 $\Pi([a, b])$ 의 오른쪽 끝점이라고 부른다. 그리고 $\Pi([a, b])$ 를 편의상 $[\Pi(a), \Pi(b)]$ 로 나타내겠다. 물론 원 위의 특정 닫힌 구간 I 를 사영으로 가지는 \mathbb{R} 위의 닫힌 구간 $[a, b]$ 는 수없이 많지만, 그 $[a, b]$ 의 선택지와 무관하게 I 의 왼쪽 끝점 및 오른쪽 끝점은 일관성 있게 정의된다. 마찬가지로 열린 구간 및 반열림 구간의 왼쪽/오른쪽 끝점들을 정의한다. 그러면 다음을 관찰할 수 있다:

{fact:oriPre

사실 1.13. $\text{Homeo}(S^1)$ 의 원소 g 에 대해 다음 조건들은 동치이다:

- (1) g 는 방향 보존 위상동형사상이다.
- (2) 원 위의 임의의 구간 I 에 대해 gI 의 왼쪽 끝점은 $g \cdot (I$ 의 왼쪽 끝점)이다.
- (3) 원 위에 (점이 아닌) 어떤 구간 I 가 존재해, gI 의 왼쪽 끝점은 $g \cdot (I$ 의 왼쪽 끝점)이다.

$\text{Homeo}(S^1)$ 의 임의의 부분군 G 를 다룰 때 방향 보존 위상동형사상들로 이루어진 그 부분군 $G \cap \text{Homeo}(S^1)$ 에 먼저 집중하면 편할 때가 있다. 이 과정에서 동역학적인 특성을 그다지 잃지 않는다는 것을 다음 보조정리를 통해 알 수 있다.

{lem:passing

보조정리 1.14. $\text{Homeo}(S^1)$ 의 한 부분군 G 이 주어졌을 때, G 가 명제 1.5의 특정 결론에 해당할 필요충분조건은 $G \cap \text{Homeo}(S^1)$ 가 그 결론에 해당하는 것이다. 다시 말해, 유한한 G -궤도가 존재할 필요충분조건은 유한한 $G \cap \text{Homeo}(S^1)$ -궤도가 존재한다는 것이고, 모든 G -궤도가 원 안에서 조밀할 필요충분조건은 모든 $G \cap \text{Homeo}(S^1)$ -궤도가 원 안에서 조밀하다는 것이며, G -불변인 공집합이 아닌 닫힌 부분집합 중 최소한인 Cantor 집합이 존재할 필요충분조건은 $G \cap \text{Homeo}(S^1)$ -불변인 공집합이 아닌 닫힌 부분집합 중 최소한인 Cantor 집합이 존재한다는 것이다.

Proof. 편의상 $G_+ := G \cap \text{Homeo}(S^1)$ 로 표기하겠다. 또 편의상, 비어 있지 않은 G -불변인 닫힌 집합 중 포함 관계상 최소한인 집합을 G -최소한이라고 부르겠다.

$G = G_+$ 인 경우에는 명제가 당연하므로 $G \setminus \text{Homeo}(S^1)$ 가 어떤 원소 r 을 가지고 있을 때만 다루면 된다. 이때 G_+ 는 G 의 지수 2짜리 정규 부분군이 되며, G 는 $G_+ \cup rG_+ = G_+ \cup G_+r$ 의 형태가 된다.

먼저 유한한 G_+ -궤도가 존재한다고 가정해 보자. 다시 말해, $G_+ \cdot y$ 가 유한집합이 되게끔 하는 $y \in S^1$ 이 존재한다는 뜻이다. 이 경우, $G \cdot y = G_+y \cup rG_+y$ 또한 유한집합이 되어, G 또한 명제 1.5의 결론 (1)을 만족한다. 역으로, 어떤 점의 G -궤도가 유한하면 G_+ -궤도는 그것보다 클 수 없으니 역시 유한하다.

이제 G_+ -최소한인 Cantor 집합 K 가 존재한다고 하자. 명제 1.5에 의하면 G_+ 는 결론 (1)에 해당할 수 없으므로, 그 어느 유한 집합도 보존할 수 없다. 그러니 G 또한 그 어느 유한집합도 보존할 수 없다.

(*) 한편, K 및 rK 는 내부(interior)가 공집합인 Cantor 집합들이므로 그 합집합 또한 내부가 비어 있다. 다시 말해, $K \cup rK$ 는 원 전체가 아닌 콤팩트 집합이다. 또 G_+ 의 각 원소는 K 는 물론, rK 또한 보존한다. 이는 임의의 $g \in G_+$ 에 대해 $r^{-1}gr$ 또한 G_+ 의 원소이므로

$$g(rK) = r \cdot (r^{-1}gr) \cdot K = rK$$

이기 때문이다. 한편, r 은 K 를 rK 로 보내고 rK 를 $r^2K = K$ 로 보내기에, $K \cup rK$ 를 보존한다. 이를 고려했을 때, G -최소한인 부분집합 K' 를 하나 잡으면 K' 는 결코 원 전체일 수 없고, (*) 때문에 유한집합일 수도 없다. 따라서 K' 는 무한집합이면서 원 전체가 아닌 집합이다. 즉, G 는 명제 1.5의 결론 (3)을 만족한다.

역으로, 만약 G -최소한인 Cantor 집합 K 가 존재하면, G_+ 또한 이를 보존하기에 G_+ 는 명제 1.5의 결론 (2)를 만족할 수 없다. 다시 말해, G_+ 는 유한한 궤도를 가지거나 혹은 명제 1.5의 결론 (3)을

만족해야 한다. 하지만 G_+ 가 유한한 궤도를 가지면 G 또한 그러하다는 것을 관찰했으니, G 가 명제 1.5의 결론 (3)을 만족한다는 가정에 모순이다. 따라서 G_+ 는 명제 1.5의 결론 (3)을 만족해야 한다. 이로써 $[(G_+$ 가 명제 1.5의 결론 (3)을 만족) \Leftrightarrow (G 가 명제 1.5의 결론 (3)을 만족)]이 증명되었다. \square

다음으로, 균일연속한 작용에 대해 다음 사실이 성립한다.

보조정리 1.15. $\text{Homeo}(S^1)$ 의 어떤 부분군 G 의 작용이 최소한이면서 균일연속하다고 하자. 그러면 G 는 켈레바꾸기를 통해 원 위의 Lebesgue 측도를 보존하는 군으로 나타낼 수 있다. 즉, 켈레바꾸기를 통해, G 를 원의 회전(rotation) 및 지름에 대한 반전들(reflection)로 이루어진 군으로 변환할 수 있다.

Proof. 증명을 위해, 최소한이고 균일연속한 작용을 보이는 원의 자기위상동형사상 군 G 를 고정하겠다. 편의상 $G \cap \text{Homeo}_+(S^1)$ 를 G_+ 로 나타내겠다. 그러면 당연히 G_+ 의 작용도 균일연속하다. 또한 보조정리 1.14에 의해 G_+ 의 작용은 최소한이기도 하다. 다시 말해,

(1.1) 임의의 $x, y \in S^1$ 에 대해, $\lim_{n \rightarrow \infty} g_n x = y$ 이게끔 하는 G_+ 의 원소 나열 $(g_n)_{n>0}$ 이 존재한다.

G 의 작용이 균일연속이므로, 각 $\epsilon > 0$ 마다 $0 < \delta = \delta(\epsilon) < \epsilon$ 이 존재하여, 임의의 $g \in G$ 및 $\text{diam}(I) < \delta$ 인 임의의 구간 I 에 대해 $\text{diam}(gI) < \epsilon$ 이 성립한다. 이제 다음을 살펴보자.

주장 1.16. 원 위의 임의의 두 점 $x, y \in S^1$, 임의의 양수 $\epsilon > 0$ 및 임의의 방향 보존 위상동형사상 $g \in G_+$ 에 대해,

$$d(x, gx) < \delta(\epsilon) \Rightarrow d(y, gy) < 2\epsilon,$$

이 성립한다.

주장 1.16의 증명 x 와 gx 를 두 끝점으로 가지는 닫힌 구간 중 크기가 δ 이하인 것을 I 라고 하자. 이때 $I = [x, gx]$, 즉 x 가 I 의 왼쪽 끝점인 경우만 다루면 충분하다. 그렇지 않은 경우 $I' = [gx, gy]$ 및 $g^{-1} \in G \cap \text{Homeo}_+(S^1)$ 에 대해 살펴보면 되기 때문이다.

이제 다음을 관찰하자.

- (1) 각 $i \geq 0$ 에 대해, $\text{diam}(I) < \delta$ 이고 $g^i \in G_+$ 이므로 $\text{diam}(g^i I) < \epsilon$ 이다.
- (2) 각 $i > 0$ 에 대해 $g^{i-1} I$ 의 오른쪽 끝점과 $g^i I$ 의 왼쪽 끝점은 $g^i x$ 로 동일하다.

이제 $\mathcal{A} := \{i \geq 0 : g^i I \subseteq [x, y]\}$ 로 두면 다음 두 가능성이 생긴다.

- (1) $\mathcal{A} = \mathbb{Z}_{\geq 0}$: 이 경우, $x, g^1 x, g^2 x, \dots$ 는 $[x, y]$ 위에 순서대로 왼쪽에서 오른쪽으로 놓여 있다. 이들의 극한점 c 를 잡으면 $x, gx, g^2 x, \dots$ 는 왼쪽으로부터 c 로 점점 다가오며, $d(g^i x, c) \searrow 0$ 가 성립한다. 따라서 $d(g^i x, g^{i+1} x)$ 의 극한도 0이다. 이 말은 곧, 제아무리 작은 $\eta > 0$ 에 대해서도 $d(g^i x, g^{i+1} x) < \eta$, $d(g^{-i} \cdot g^i x, g^{-i} \cdot g^{i+1} x) = d(x, gx)$ 를 만족하는 i 가 존재한다는 뜻인데, 이는 $\{g^j : j \in \mathbb{Z}\} \subseteq G$ 의 균일연속성에 위배된다.
- (2) \mathcal{A} 에 속하지 않는 양의 정수가 존재하는 경우: 그러한 양의 정수 중 가장 작은 것을 N 이라고 두면, y 는 $[g^N x, g^{N+1} x]$ 에 속하게 된다. 이는 곧 $gy \in [g^{N+1} x, g^{N+2} x]$ 를 의미하기도 한다. 이 두 구간은 $g^{N+1} x$ 라는 공통점을 가지는 한편 둘 다 ϵ 보다 크기가 작으므로,

$$d(y, gy) < \text{diam}([g^N x, g^{N+1} x]) + \text{diam}([g^{N+1} x, g^{N+2} x]) < 2\epsilon$$

라는 결론을 얻는다. \square

거의 같은 증명을 통해 다음 결과도 관찰할 수 있다.

주장 1.17. 원 위의 임의의 구간 $J \subseteq S^1$ 및 G 의 임의의 원소 $g \in G$ 에 대해,

$$gJ \subseteq J \Rightarrow gJ = J$$

가 성립한다.

주장 1.17의 증명.. 먼저, g 가 방향 보존성일 때만 증명하면 된다는 것을 관찰하자. 실제로, 일반적인 $g \in G$ 에 대해 $gJ \subseteq J$ 가 성립하면 $g^2J \subseteq gJ \subseteq J$ 또한 성립한다. 이제 방향 보존성인 g^2 에 대해 명제를 적용하면 $g^2J = J$ 를 이끌어낼 수 있고, 이는 곧 $g^2J = gJ = J$ 임을 의미한다. 또, J 가 닫힌 구간일때만 증명해도 충분하다.

이제 증명을 위해 g 가 방향 보존성이면서 $gJ \subseteq J$ 임을 가정하자. 이로부터 gJ 와 J 의 왼쪽 끝점 및 오른쪽 끝점이 쌍마다 일치한다는 것을 보이기만 하면 된다. 귀류법을 적용하기 위해, gJ 의 왼쪽 끝점이 J 의 왼쪽 끝점과 일치하지 않는다고 가정해 보자. $J = [x, y]$ 로 표기하면, 이는 $d(x, gx) > 0$ 임을 의미한다. 또한 $I := [x, gx]$ 는 J 에 포함되어 있다. 이제, 각 $i > 0$ 에 대해 $g^iI \subseteq g^iJ \subseteq g^{i-1}J \subseteq \dots \subseteq J$ 가 성립하고, $g^{i-1}I$ 의 오른쪽 끝점과 g^iI 의 왼쪽 끝점은 g^ix 로 동일하다. 그말인즉, x, gx, g^2x, \dots 는 J 위에 순서대로 왼쪽에서 오른쪽으로 놓여 있다. 이들의 극한점 c 를 잡으면 x, gx, g^2x, \dots 는 왼쪽으로부터 c 로 점점 다가오며, $d(g^ix, c) \searrow 0$ 가 성립한다. 따라서 $d(g^ix, g^{i+1}x)$ 의 극한도 0이다. 이 말은 곧, 제아무리 작은 $\eta > 0$ 에 대해서도 $d(g^ix, g^{i+1}x) < \eta$, $d(g^{-i} \cdot g^ix, g^{-i} \cdot g^{i+1}x) = d(x, gx)$ 를 만족하는 i 가 존재한다는 뜻인데, 이는 $\{g^j : j \in \mathbb{Z}\} \subseteq G$ 의 균일연속성에 위배된다. 따라서 gJ 의 왼쪽 끝점과 J 의 오른쪽 끝점은 일치해야 한다.

이제 gJ 의 오른쪽 끝점이 J 의 오른쪽 끝점과 일치하지 않는다고 가정해 보자. 그말은 $J' := S^1 \setminus (g \text{ int } J)$ 라는 구간의 왼쪽 끝점과 $g^{-1}J' = S^1 \setminus \text{int } J$ 의 왼쪽 끝점이 일치하지 않는다는 말이다. 더하여 $g^{-1}J' \subseteq J'$ 가 성립한다. 상술한 논증을 적용하면 마찬가지로 모순을 얻는다. 이로써 증명이 끝난다. \square

주장 1.16는 다음과 같은 결과를 낳는다.

주장 1.18. 임의의 두 점 $x, y \in S^1$ 및 G_+ 안의 임의의 원소 나열 $(g_n)_{n>0}$ 에 대해

$$(g_n x)_{n>0} \text{가 수렴함} \Leftrightarrow (g_n y)_{n>0} \text{가 수렴함}$$

이 성립한다.

또한, G 가 균일연속하므로, 어떤 점 $x \in S^1$ 으로 수렴하는 점의 나열 $x_1, x_2, \dots \in S^1$ 및 G 안의 임의의 원소 나열 $(g_n)_{n<0}$ 에 대해

$$(g_n x)_{n>0} \text{가 수렴함} \Leftrightarrow (g_n x_n)_{n>0} \text{가 수렴함}$$

이 성립한다. 또 두 나열이 수렴할 경우 그 수렴값 또한 일치한다. 이를 종합하면 다음과 같다.

주장 1.19. 원 안에서 수렴하는 임의의 점의 나열 $(x_n)_{n>0}$, 임의의 점 $y \in S^1$ 및 G_+ 안의 임의의 원소 나열 $(g_n)_{n>0}$ 에 대해

$$(g_n x_n)_{n>0} \text{가 수렴함} \Leftrightarrow (g_n y)_{n>0} \text{가 수렴함}$$

이 성립한다.

이제 본격적으로 G_+ 가 보존하는 측도를 건설하겠다. 이를 위해 $x_0 \in S^1$ 을 고정하자.

주장 1.20. 각 $N \in \mathbb{Z}_{>1}$ 마다, 다음을 만족하는 점 $x_{1;N}, x_{2;N}, \dots, x_{N-1;N} \subseteq S^1$ 이 각각 유일하게 존재한다. 편의상

$$x_{kN+l;N} := x_{l;N}, \quad x_{kN;N} := x_0 \quad (k \in \mathbb{Z}, l \in \{1, \dots, N-1\})$$

로 표기하겠다.

- (1) 구간 $(x_0 := x_{0;N}, x_{1;N}), (x_{1;N}, x_{2;N}), \dots, (x_{N-1;N}, x_{N;N} := x_0)$ 들은 서로 겹치지 않는다.
- (2) $\lim_n g_n x_0 = x_{1;N}$ 이게끔 하는 임의의 G_+ 의 원소 나열 $(g_n)_{n>0}$ 에 대해 (참고: 문장 1.1), $\lim_n g_n^k x_{i;N} = x_{i+k;N}$ 가 각 $i, k \in \mathbb{Z}$ 마다 성립한다.

주장 1.20의 증명.. 문장 1.1에 의해, 임의의 $y \in S^1$ 가 주어졌을 때 $\lim_n g_n x_0 = y$ 이게끔 하는 G_+ 의 원소 나열 $(g_n)_{n>0}$ 이 존재한다. 이때 각 $k > 0$ 에 대하여 $x_k(y) := \lim_n g_n^k x_0$ 로 정의하면, 주장 1.19 덕분에 $x_k(y)$ 의 정의에서 나타나는 극한은 잘 정의되며, 그 값은 원소 나열 $(g_n)_{n>0}$ 의 선택지에 의존하지 않는다. 또 주장 1.19 덕분에 $x_1(y), x_2(y), \dots$ 각각은 y 에 대해 연속이다. 이제,

$$\begin{aligned} \mathcal{A} &:= \{y \in S^1 \setminus \{x_0\} : (x_0 := x_0(y), y := x_1(y)), (x_1(y), x_2(y)), \dots, (x_{N-1}(y), x_N(y)) \text{이 서로 겹치지 않음}\} \\ &= \left\{ y \in S^1 \setminus \{x_0\} : \sum_{k=1}^N ((x_{k-1}(y), x_k(y)) \text{의 길이}) \leq 1 \right\} \end{aligned}$$

라는 집합을 정의하겠다. (여기서 $x_k(y)$ 들이 잘 정의된다는 것은 주장 1.19이 보장한다.) 먼저 \mathcal{A} 의 영역이 어느 정도 제한되어 있다는 점을 관찰하겠다. 이를 위해, $\delta = \delta(1/10)$ 를 잡은 뒤, $[x_0, y]$ 의 길이가 $1 - 0.5\delta$ 를 넘도록 하는 $y \in S^1$ 을 생각해보자. 그런 y 에 대해 $g_n x_0 \rightarrow y$ 인 원소 나열 $(g_n)_{n>0}$ 을 가져오면 충분히 큰 n 에 대해 $d(x_0, g_n x_0) > 2 \cdot \epsilon$ 가 성립하고, 주장 1.16에 의해 $d(g_n x_0, g_n^2 x_0)$ 는 δ 보다 커진다. 이에 따라 (x_0, x_1) 및 (x_1, x_2) 의 길이 합은 1보다 크고 두 구간은 겹칠 수밖에 없다. 따라서 이러한 y 는 \mathcal{A} 에 속할 수 없다. 다시 말해, \mathcal{A} 가 길이 $1 - 0.5\delta$ 이하인 구간에 포함되어 있다.

이제 \mathcal{A} 의 최소 상한을 생각하자. 더 엄밀하게는,

$$I := \bigcap_{y \in \mathcal{A}} [x_0, y] \subseteq S^1$$

는 원 위의 구간이기에 어떤 $s \in S^1$ 에 대하여 $[x_0, s]$ 또는 $[x_0, s)$ 의 형태인데, 이 s 를 \mathcal{A} 의 상한이라고 부르겠다. 그러면 함수 $x_1(y), x_2(y), \dots$ 의 연속성에 의해, $\sum_{k=1}^N ((x_{k-1}(s), x_k(s)) \text{의 길이}) = 1$ 임을 알 수 있다. 이는 곧 $x_N(y) = x_0$ 임을 의미하고, 이로부터 귀납적으로 $x_{kN+l} = x_l$ 임이 따라나온다. 더하여, 주장 1.19을 다시 한번 적용하면 $\lim_n g_n^k x_i = x_{i+k}$ 를 관찰할 수 있다.

이제 남은 것은 점 $x_{1;N}, x_{2;N}, \dots, x_{N-1;N}$ 의 유일성이다. 참고로, 명제의 조건으로부터 $x_{1;N}$ 의 유일성만 증명해 내면, (2)의 조건 $\lim_n g_n^k x_{1;N} = x_{1+k;N}$ 로부터 나머지 점들의 유일성은 따라나온다. (이는 또다시 주장 1.19 덕분이다) 따라서,

$$(1.2) \quad \sum_{k=1}^N ((x_{k-1}(y), x_k(y)) \text{의 길이}) = 1$$

이게끔 하는 y 의 유일성만 보이면 된다.

이를 귀류법으로 보이기 위해, 등식 1.2가 성립하게끔 하는 서로 다른 두 입력값 $y_1, y_2 \in S^1 \setminus x_0$ 가 있다고 가정하자. 일반성을 잃지 않고 y_1 이 y_2 보다 더 왼쪽에 있다고 가정하자. 즉, $\epsilon_1 := ([x_0, y_2]$ 의 길이) -

$([x_0, y_1]$ 의 길이) > 0 이라고 가정하는 것이다. 귀납적으로,

$$\epsilon_{i+1} := \delta(\epsilon_i/4)$$

를 정의하자. 이로부터 $x_N(y_2)$ 가 $x_N(y_1)$ 보다 ϵ_N 이상 오른쪽에 있다는 것을 보여, $x_N(y_2) = x_N(y_1)$ 에 모순임을 이끌어내는 것이 우리의 목표다.

이를 위해, 귀납적으로 $x_k(y_2)$ 가 $x_k(y_1)$ 보다 ϵ_k 이상 오른쪽에 있다고 해보자. 이와 함께 $\lim_n g_n x_0 = y_1, \lim_n h_n x_0 = y_2$ 인 원소 나열 $(g_n)_{n>0}, (h_n)_{n>0}$ 을 준비하자. 그러면 충분히 큰 n 에 대해, $h_n^k g_n^{-k} \cdot g_n^k x_0 = h_n^k x_0$ 는 $g_n^k x_0$ 보다 $\epsilon_k/2$ 이상 오른쪽에 있다. 그러면 주장 1.16에 의해 $h_n^k g_n^{-k} \cdot g_n^{k+1} x_0$ 는 $g_n^{k+1} x_0$ 로부터 최소 $\delta(\epsilon_k/2)$ 이상 떨어져 있어야 한다. 또, 만약 $h_n^k g_n^{-k} \cdot g_n^{k+1} x_0$ 가 $g_n^{k+1} x_0$ 보다 오른쪽에 있지 않다면,

$$h_n g_n^{-k} \cdot [g_n^k x_0, g_n^{k+1} x_0] \subsetneq [g_n^k x_0, g_n^{k+1} x_0]$$

가 성립해 주장 1.17에 모순이다. 이를 종합하면, $h_n^k g_n x_0$ 는 $g_n^{k+1} x_0$ 보다 최소 ϵ_{k+1} 이상 오른쪽에 있음을 알 수 있다. 또, (충분히 큰 n 에 대해) $x_0, h_n x_0, (h_n x_0, h_n^2 x_0), \dots, (h_n^k x_0, h_n^{k+1} x_0)$ 은 순서대로 왼쪽부터 오른쪽으로 줄지어 놓인 구간들이고 $g_n x_0$ 이 $(x_0, h_n x_0)$ 사이에 있으므로, $h_n^{k+1} x_0$ 은 $h_n^k g_n x_0$ 보다도 더욱 오른쪽에 있다. 즉 충분히 큰 n 에 대해 항상 $h_n^{k+1} x_0$ 은 $g_n^{k+1} x_0$ 보다 ϵ_{k+1} 이상 오른쪽에 있으므로, $x_{k+1}(y_1)$ 및 $x_{k+1}(y_2)$ 의 위치 관계에 대한 주장이 따라나온다. 이로써 증명이 끝난다. \square

이제, 각각의 $N \in \{2^k : k \in \mathbb{Z}_{>1}\}$ 마다, $x_{k;N}$ 을 $x_{k/N}$ 이라고 표기하겠다. 이 표기가 일관성 있기 위해서는 $x_{k;N} = x_{2k;2N}$ 라는 등식이 항상 성립해야 하는데, 이는 주장 1.20의 결론의 조건 (2) 및 $x_{i;j}$ 들의 유일성으로부터 따라나온다.

이로부터 유한 2진 소수들 $\mathcal{S} := \{\Pi(i/2^k) : k > 0, i = 1, \dots, 2^k\} \subseteq S^1$ 로부터 S^1 로의 사상 $\rho : a \mapsto x_a$ 가 잘 정의된다. 주장 1.20의 결론의 조건 (1)로부터 이 사상이 단조적임을 알 수 있다. 또 이 사상은 $\mathcal{S} \subseteq S^1$ 에 제한해서 보았을 때도 균일연속하다. 실제로, 임의의 $\epsilon > 0$ 이 주어졌을 때 $\delta = \delta(\epsilon)$ 을 잡을 수 있다. 이때 만약 어떤 $k > 0$ 및 $i \in \{1, \dots, 2^k\}$ 에 대해 $d(x_{(i-1)/2^k}, x_{i/2^k}) > 2\epsilon$ 이 성립한다면, 주장 1.16에 의해 다른 모든 $j \in \{1, \dots, 2^k\}$ 에 대해서도 $d(x_{(j-1)/2^k}, x_{j/2^k}) > \delta$ 임을 알 수 있다. 이는 곧

$$2^k \cdot \delta < \sum_{j=1}^{2^k} ((x_{(j-1)/2^k}, x_{j/2^k}) \text{의 길이}) \leq 1$$

라는 결론으로 이어져, k 의 상한을 하나 제시한다. 다시 말해, 이 상한보다 더 큰 k 에 대해서는 각 i 에 대해 $[x_{(i-1)/2^k}, x_{i/2^k}]$ 의 길이가 ϵ 이하이다.

이처럼 ρ 가 원 위에서 조밀한 집합인 \mathcal{S} 로부터 S^1 로 향하는 단조적인 균일연속 사상이기에, ρ 는 S^1 에서 S^1 로 향하는 단조적인 연속사상으로 확장된다. 또한, ρ 의 차수를 계산하는 한 방법으로 $[0, 1]$ 을 따라 $\Pi^{-1} \circ \rho \circ \Pi$ 의 변화량을 적분하는 것이 있는데, \mathcal{S} 안의 점점 조밀해지는 샘플 입력값들을 이용해 계산했을 때 항상 그 값이 1이도록 정의했기에 (이는 주장 1.20의 결론 (1), 즉 등식 1.2에 다름 아니다) ρ 의 차수 또한 1이다. 즉, ρ 는 S^1 위의 위상동형사상이다.

이제 S^1 상의 Lebesgue 측도 μ 의 당겨옴(pullback) $\rho^* \mu$ 를 정의할 수 있다. 즉, Borel 집합 $A \subseteq S^1$ 에 대해 $(\rho^* \mu)(A) := \mu(\rho^{-1}(A))$ 로 정의하는 것이다. 이 측도가 G_+ 의 작용에 불변한다는 것을 증명하기 위해서는 각각의 $s \in [0, 1]$ 에 대해 $I = [x_0, x_s]$ 의 측도가 G_+ 의 작용에 의해 변하지 않음을 관찰하기만 하면 된다. 이를 위해 $g \in G_+$ 을 하나 생각하자. 그러면 각 $k > 0$ 마다

$$g x_0 \in [x_{(i(k)-1)/2^k}, x_{i(k)/2^k}], \quad g x_s \in [x_{(j(k)-1)/2^k}, x_{j(k)/2^k}]$$

를 만족하는 $i(k), j(k)$ 가 있다. 이때 $(\rho^* \mu)(A) = \lim_k 2^{-k} [j(k) - i(k)] = s$ 로 정의된다.

이제, 주장 1.20에 의해 다음을 보장할 수 있다. 어떤 G 의 원소 h_k 가 $d(hx_0, x_{1/2^k})$ 를 충분히 작게 한다면, $h_k^{-i(k)}x_0$ 는 $x_{(i(k)-1)/2^k}$ 를 $x_{(2^k-1)/2^k}$ 근처로, $x_{i(k)/2^k}$ 를 x_0 근처로 보낸다. 이는 특히

$$h_k^{-i(k)}gx_0 \in h_k^{-i(k)}[x_{(i(k)-1)/2^k}, x_{i(k)/2^k}] \subseteq [x_{(2^k-2)/2^k}, x_{1/2^k}]$$

가 성립함을 의미한다. 마찬가지로, $d(hx_0, x_{1/2^k})$ 가 충분히 작기만 하다면,

$$h_k^{-i(k)}gx_s \in h_k^{-i(k)}[x_{(j(k)-1)/2^k}, x_{j(k)/2^k}] \subseteq [x_{(j(k)-i(k)-2)/2^k}, x_{(j(k)-i(k)+1)/2^k}]$$

가 성립한다. 이제 k 를 무한대로 보낼 때, $h_k^{-i(k)}g$ 는 x_0 를 점점 x_0 가까이 보낸다. 그러면 주장 1.18에 의해 $h_k^{-i(k)}gx_s$ 또한 x_s 에 가까워진다. 따라서 $2^{-k}(j(k) - i(k))$ 가 s 로 수렴하고, $[x_0, x_s]$ 의 $g[x_0, x_s]$ 의 $\rho^*\mu$ 값은 s 로 일치하게 된다. 즉 임의의 $g \in G_+$ 가 x_0 를 왼쪽 끝점으로 가지는 임의의 구간의 $\rho^*\mu$ 값을 보존하고, 이는 G_+ 가 $\rho^*\mu$ 값을 보존함을 의미한다.

만약 $G_+ = G$ 라면 이대로 증명이 끝난다. 그렇지 않은 경우, 각각의 $r \in G \setminus G_+$ 가 측도 $\rho^*\mu$ 를 보존함을 증명해야 한다. 즉, 임의의 닫힌 구간 I 에 대해 $r\rho^{-1}(I)$ 와 $\rho^{-1}(I)$ 의 길이가 같음을 확인해야 한다. 귀류법을 적용하기 위해 어떤 $r \in G \setminus G_+$, 어떤 $0 < \epsilon < 0.1$ 및 어떤 닫힌 구간 I 에 대해, $r\rho^{-1}(I)$ 가 $\rho^{-1}(I)$ 보다 ϵ 이상 길다고 가정해 보자. 그러면 $\rho^{-1}(I)$ 의 왼쪽 끝점을 $r\rho^{-1}(I)$ 의 왼쪽 끝점으로부터 오른쪽으로 $\epsilon/4$ 이상 $\epsilon/2$ 이하 떨어져 있도록 보내는 $g \in G_+$ 가 존재한다. 이는 G_+ 의 작용이 최소한 이기 때문이다. 이때 $g\rho^{-1}(I)$ 의 길이는 $\rho^{-1}(I)$ 와 같으므로, $g\rho^{-1}(I)$ 는 $r\rho^{-1}(I)$ 에 포함되면서 그 왼쪽 끝점이 차이나게 된다. 다시 말해, $gI \subseteq rI$ 이다. 이는 $rg^{-1} \in G$ 라는 사실 및 주장 1.17에 모순이다. 따라서 이러한 일은 생길 수 없고, 각 $r \in G \setminus G_+$ 역시 측도 $\rho^*\mu$ 를 보존한다. \square

이제 원 위에서 최소한이지만 균일연속하지 않은 작용들, 즉 팽창적인 작용들을 살펴보겠다.

보조정리 1.21. Homeo(S^1)의 어느 부분군 G 의 작용이 최소한이면서 팽창적이라고 하자. 그러면 강하게 팽창적인 작용을 가지는 부분군 $\rho(G) \leq \text{Homeo}(S^1)$ 로 향하는 군 맞춤 사상 $\rho : G \rightarrow \rho(G) \leq \text{Homeo}(S^1)$ 및 원의 자가 덮음 사상 $\pi : S^1 \rightarrow S^1$ 이 존재하여 각 $g \in G$ 마다

$$\pi \circ g = \rho(g) \circ \pi$$

가 성립한다.

Proof. 이번에도 $G_+ := G \cap \text{Homeo}(S^1)$ 로 두면, $G = G_+$ 이거나 혹은 G_+ 가 G 의 지수 2짜리 정규 부분군이다. 그 어느 경우이든, G 의 작용이 최소한이므로 G_+ 의 작용 또한 최소한임을 기억하자. G 가 이미 강하게 팽창적인 경우 π 및 ρ 를 항등사상들로 두는 것으로 증명이 끝난다. 이제 G 가 팽창적이되 강하게 팽창적이지는 않다고 가정해 보자. 그렇다면 G_+ 또한 팽창적이되 강하게 팽창적이지는 않다. 편의상, 어떤 구간 $I \subseteq S^1$ 가 $\inf_{g \in G_+} \text{diam}(gI) = 0$ 을 만족할 때 I 가 축약 가능하다(contractible)고 부르겠다. 그러면 다음을 쉽게 관찰할 수 있다.

사실 1.22. 임의의 구간 $I, J \subseteq S^1$ 및 $g \in G_+$ 에 대해,

$$I \text{가 축약 가능하고 } gJ \subseteq I \text{임} \Rightarrow J \text{가 축약 가능함}$$

이 성립한다.

G_+ 에 대한 가정으로부터, 축약 가능한 열린 구간 I 및 축약 불가능한 원 전체가 아닌 열린 구간 J 가 적어도 하나씩 존재함을 알 수 있다. G_+ 의 작용이 최소한이므로, $\{g^{-1}I : g_+ \in G\}$ 및 $\{g^{-1}(S^1 \setminus J) :$

$g_+ \in G$ 는 각각 S^1 의 열린 집합 덮개가 된다. Lebesgue 덮음 보조정리에 의해 적당한 $\epsilon_G > 0$ 에 대해 다음이 보장된다: 임의의 구간 $A \subseteq S^1$ 에 대해

$$(1.3) \quad \begin{aligned} \text{diam}(A) < \epsilon_G &\Rightarrow A \subseteq g^{-1}I \text{를 만족하는 } g_+ \in G \text{가 존재함} \Rightarrow A \text{는 축약 가능,} \\ \text{diam}(A) > 1 - \epsilon_G &\Rightarrow A \supseteq g^{-1}J \text{를 만족하는 } g_+ \in G \text{가 존재함} \Rightarrow A \text{는 축약할 수 없음} \end{aligned}$$

가 성립한다.

특히,

$$\mathcal{A}_x := \{y \in S^1 \setminus \{x\} : [x, y] \text{가 축약 가능함}\}$$

은 길이 ϵ_G 짜리 구간을 포함하면서 길이 $1 - \epsilon_G$ 짜리 구간에 포함된다. 또한, 사실 1.22로부터 다음을 알 수 있는데, 만약 $y \in \mathcal{A}_x$ 이고 $z \in [x, y]$ 라면 $z \in \mathcal{A}_x$ 라는 점이다. 이를 종합하면, \mathcal{A}_x 라는 집합은 어떤 $y \neq x$ 에 대해 (x, y) 혹은 $(x, y]$ 라는 형태를 가진다. 이때 이 점 y 를 $\phi(x)$ 라고 정의하겠다.

{claim:contr

주장 1.23. 사상 $\phi : S^1 \rightarrow S^1$ 와 G_+ 의 원 위의 작용은 호환 가능하다. 그말인즉, 임의의 $x \in S^1$ 및 임의의 $g \in G_+$ 에 대해 $\phi(gx) = g\phi(x)$ 가 성립한다.

Proof. $x \in S^1$ 및 $g \in G_+$ 를 임의로 생각했을 때, 각각의 $y \in \mathcal{A}_x$ 마다 $[x, y]$ 는 축약 가능하고, 따라서 사실 1.22에 의해 $[gx, gy] = g[x, y]$ 또한 축약 가능하다. 이로부터 $\mathcal{A}_{gx} \subseteq g\mathcal{A}_x$ 임이 따라나온다. 마찬가지로 이유로 $\mathcal{A}_x \subseteq g^{-1}\mathcal{A}_{gx}$ 가 성립하고, g 가 일대일대응이므로 $g\mathcal{A}_x \subseteq \mathcal{A}_{gx}$ 또한 성립한다. 즉 $\mathcal{A}_{gx} = g\mathcal{A}_x$ 이므로 증명이 끝난다. \square

이제 다음과 같은 ϕ 의 ‘단조성’을 쉽게 관찰할 수 있다. 사실 원에서 자기 자신으로 가는 사상의 단조성을 얘기하기 위해서는 실수 집합으로 끌어올려야 하기에, 그 사상의 연속성을 논하는 것이 먼저여야 한다. 하지만 우리 증명에서는 ‘단조성’이 연속성보다 먼저 필요하다.

{claim:contr

주장 1.24. 그 어떤 $x, y \in S^1$ 에 대해서도, $[y, \phi(y)]$ 가 $[x, \phi(x)]$ 에 포함되는 일은 일어나지 않는다.

Proof. 귀류법을 적용하기 위해, $[y, \phi(y)] \subseteq [x, \phi(x)]$ 를 가정해 보자. 이는 $\phi(x) \notin [y, \phi(y)]$ 를 의미한다. 한편, $(x, \phi(x))$ 에 포함되어 있는 $(y, \phi(x))$ 의 각 점 z 에 대해 $[y, z] \subseteq [x, z]$ 는 축약 가능하다. 그렇다면 $\phi(y)$ 의 정의상 $[y, \phi(x)]$ 는 $[y, \phi(y)]$ 에 포함되어야 한다. 이는 $\phi(x)$ 가 $[y, \phi(y)]$ 바깥에 있다는 관찰과 모순이기에 증명이 끝난다. \square

이제 ϕ 의 연속성을 보이겠다. 귀류법을 적용하기 위해,

$$\lim_n x_n = a = \lim_n y_n, \quad \lim_n \phi(x_n) = b \neq c = \lim_n \phi(y_n)$$

을 만족하는 세 점 $a, b, c \in S^1$ 및 원 위의 점의 나열 $(x_n)_{n>0}, (y_n)_{n>0}$ 을 생각하자. 일반성을 잃지 않고, $c \in (a, b)$ 라고 가정하자.

G_+ 의 작용이 최소한이기에 b 를 (c, b) 안으로 보내는 $g \in G_+$ 가 존재한다. 이때 만약 ga 가 $[a, gb]$ 안에 있으면 $[ga, gb]$ 는 (a, b) 에 포함되고, 충분히 큰 n 및 그보다 더욱 충분히 큰 m 에 대해 $[gy_m, g\phi(y_m)]$ 가 $[y_n, \phi(y_n)]$ 에 포함된다. 이는 주장 1.24에 모순이다. 다음으로, 만약 $ga \in (gb, a)$ 라면 (ga, gb) 는 $[a, c]$ 를 포함하고, 충분히 큰 n 에 대해 $[gy_n, g\phi(y_n)]$ 가 $[x_n, \phi(x_n)]$ 을 포함한다. 이는 마찬가지로 모순이다. 마지막으로, g 는 일대일대응이기에 $ga \neq gb$ 이다. 따라서 가정한 상황은 생길 수 없고, ϕ 는 연속하다.

이제 점 $x_0 := \Pi(0) \in S^1$ 를 고정하고, $\tilde{\phi}(0) = ([x_0, \phi(x_0)])$ 의 길이를 만족하는 ϕ 의 \mathbb{R} 로의 끌어올림 $\tilde{\phi}$ 를 생각하면, $\tilde{\phi}(t) := [t + \epsilon_G, t + 1 - \epsilon_G]$ 가 항상 성립한다. 이는 곧 ϕ 의 차수가 1임을 의미한다.

다음으로 ϕ 가 일대일 사상임을 보이겠다. 귀류법을 적용하기 위해, 어떤 $a \in S^1$ 에 대해 $\phi^{-1}(a)$ 가 한 개 이상의 점을 가지고 있다고 가정하자. $x \in \phi^{-1}(a)$ 에 대한 $[x, a]$ 의 길이의 최대 하한을 m , 최소 상한을

M 이라고 하면 $\epsilon_G \leq m < M \leq 1 - \epsilon_G$ 이 성립한다. $[b, a]$ 의 길이가 M , $[c, a]$ 의 길이가 m 이게끔 하는 두 점 $b, c \in S^1$ 을 잡으면, b 와 c 는 $\phi^{-1}(a)$ 의 집적점이기에 ϕ 의 연속성에 의해 둘 다 $\phi^{-1}(a)$ 에 속한다.

이제 c 를 (b, c) 안으로 보내는 어떤 $g \in G_+$ 를 생각하자. 이때 만약 $ga \in (a, gc)$ 라면 $[c, \phi(c)] = [c, a] \subseteq [gc, ga] = [gc, \phi(gc)]$ 가 성립해 주장 1.24에 모순이다. 만약 $ga \in (gc, a)$ 라면 $[gc, ga] = [gc, \phi(gc)]$ 가 $[b, a] = [b, \phi(b)]$ 에 포함되어 역시 주장 1.24에 모순이다. 마지막으로, g 는 일대일대응이기에 $ga \neq gc$ 이다. 이를 종합하면, c 를 (b, c) 안으로 보내는 $g \in G_+$ 는 반드시 a 를 고정해야 한다는 것이다. 여기서 (gc, a) 안에 c 가 포함되어 있음을 유념하자. 이는 곧 $g^{-1}c \in g^{-1}(gc, a) = (c, g^{-1}a) = (c, a)$ 임을 의미한다. 다시 말해, $[g^{-1}c, a]$ 는 $[c, a]$ 보다 짧은 구간이면서, $\phi(g^{-1}c) = g^{-1}\phi(c) = g^{-1}a = a$ 가 성립한다. 이는 $x \in \phi^{-1}a$ 에 대한 $[x, a]$ 의 길이의 최솟값이 c 에서 구현된다는 사실에 모순이다.

위 모순에 의해, ϕ 가 일대일 사상이라는 것이 따라나온다. 그러면 $\phi : S^1 \rightarrow S^1$ 는 연속이고 일대일 사상이면서 차수가 1이다. 이는 곧 ϕ 가 방향 보존 위상동형사상임을 의미한다.

이제 $x \in S^1$ 을 임의로 하나 고정한 뒤, $S_k(x) := \sum_{i=1}^k ([\phi^{i-1}x, \phi^i(x)])$ 의 길이가 1 이하이도록 하는 양의 정수 k 중 최댓값을 N 이라고 적자. (N 은 반드시 유한하고, 특히 반드시 $1/\epsilon_G$ 이하이다.) 만약 $\phi^N x = x$ 라면 $S_N(x) = 1$ 이 성립하고, 이 경우 $y = x$ 로 둔다. 만약 그렇지 않다면, $S_N(x) < 1$, $S_{N+1}(x) > 1$ 이 성립한다. 그러면 $[\phi^{N-1}x, x]$ 는 $[\phi^{N-1}x, \phi^N x]$ 보다 짧은 부분구간이므로 축약가능하고, 따라서 G_+ 의 원소 나열 $(g_n)_{n>0}$ 이 존재해 $d(g_n \phi^N x, g_n x) = d(\phi^N g_n x, g_n x) \rightarrow 0$ 이 성립한다. 필요하다면 $(g_n)_{n>0}$ 을 적당한 부분나열로 대체함으로써 나열 $(g_n x)_{n>0}$ 이 어떤 점 $y \in S^1$ 로 수렴한다는 것을 보장할 수 있다. 한편, $S_N(x) < 1$ 로부터 $(x, \phi x), \dots, (\phi^{N-1}x, \phi^N x)$ 가 모두 서로 겹치지 않음을 알 수 있는데, 각각의 g_n 은 위상동형사상이므로 구간들의 겹침 여부를 보존한다. 즉, $(g_n x, g_n \phi x = \phi g_n x), \dots, (\phi^{N-1} g_n x, \phi^N g_n x)$ 는 모두 겹치지 않으므로, $S_N(g_n x) \leq 1$ 이 각 n 마다 성립한다. 이제 ϕ 의 연속성을 이용하면 $S_N(y) \leq 1$ 임을 알 수 있다. 한편, $g_n x \rightarrow y$ 이고 $d(\phi^N g_n x, g_n x) \rightarrow 0$ 이므로, ϕ 의 연속성에 의해 $\phi^N y = y$ 이다. 이 사실과 $\epsilon_G N \leq S_N(y) \leq 1$ 를 결합하면 $S_N(y) = 1$ 임을 알 수 있다. 즉,

$$[y, \phi y], [\phi y, \phi^2 y], \dots, [\phi^{N-1} y, \phi^N y = y]$$

는 그 내부끼리는 서로 겹치지 않으면서 원 전체를 덮는다.

이제 y 를 임의의 $g \in G_+$ 로 움직여 보자. 그러면

$$[gy, \phi gy], \dots, [\phi^{N-1} gy, \phi^N gy = g \phi^N y = gy]$$

의 내부끼리 겹치지 않는다는 사실이 유지되기에, $S_N(gy) = 1$ 가 성립한다. 이제 임의의 점 $z \in S^1$ 이 주어졌을 때 $g_n y \rightarrow z$ 이게끔 하는 G_+ 의 원소 나열 $(g_n)_{n>0}$ 을 잡으면, 모든 $S_N(g_n y) = 1$ 이 성립하고 (ϕ 의 연속성의 결과인) $S_N(\cdot)$ 의 연속성으로부터 $S_N(z) = 1$ 임을 알 수 있다. 즉, $S_N(\cdot)$ 는 원 위에서 항상 1이라는 상수값을 가진다. 다시 말해, 임의의 점의 ϕ -궤도는 점 N 개짜리 집합이고, S^1 의 각 ϕ -궤도를 한 점씩으로 묶어 내면 차수 N 짜리 덮음 사상 $\pi : S^1 \rightarrow S^1$ 가 만들어진다. ϕ 와 G_+ 의 작용이 호환 가능하기에, G_+ 는 몫공간인 S^1 에도 자연스럽게 작용한다.

이제 G 전체가 몫공간인 S^1 에 자연스럽게 작용하기 위해서는 $G \setminus G_+$ 의 각 원소의 작용이 덮음 사상 π 와 호환 가능해야 한다. 이에 다음을 관찰하자.

주장 1.25. 임의의 $x \in S^1$ 및 임의의 $r \in G \setminus G_+$ 에 대해, $r\phi(x) = \phi^{-1}(rx)$ 가 성립한다.

주장 1.25의 증명 $I = [x, \phi(x)]$ 라고 두고, $rI = [r\phi(x), rx]$ 는 다음 세 가지 중 하나를 만족한다.

- (1) $rI \subsetneq [r\phi(x), \phi r\phi(x)]$: 이 경우, ϕ 의 연속성을 이용하면 $rI \subseteq (c, \phi(c))$ 인 점 $c \in S^1$ 를 잡아줄 수 있다. 이제 G_+ 의 작용이 최소한이라는 점과 ϕ 의 연속성을 이용하면 $rI \subseteq (gx, \phi gx) =$

$(gx, g\phi x)$ 이게끔 하는 $g \in G_+$ 를 찾을 수 있다. 이는 곧 $rI \subsetneq gI$ 및 $I \subsetneq r^{-1}gI \subsetneq r^{-1}gr^{-1}gI$ 를 의미한다. 여기서 $h := r^{-1}gr^{-1}g$ 는 G_+ 의 원소이므로, 주장 1.23에 의해 $[x, \phi(x)] \subsetneq hI = [hx, h\phi(x)] = [hx, \phi(hx)]$ 임을 얻는다. 이는 ϕ 가 순증가한다는 사실에 모순이다.

(2) $rI \supsetneq [r\phi(x), \phi r\phi(x)]$: 이 경우, $r' := r^{-1}$, $y := r\phi(x)$, $J := [y, \phi y]$ 에 대해 생각해 보면 $r'J \subsetneq r'rI = [\phi^{-1}(r'r\phi(x)), r'r\phi(x)]$ 가 성립한다. 그러면 위와 비슷한 이유로 $r'J \subsetneq gJ = g[y, \phi(y)]$ 이도록 하는 $g \in G_+$ 를 찾을 수 있다. 그러면 $r'^{-1}gr'^{-1}g$ 는 G_+ 의 원소이면서 J 를 그보다 더 큰 구간으로 보내는데, 이는 ϕ 가 순증가한다는 사실에 모순이다.

(3) $rx = \phi r\phi r(x)$ 가 성립한다.

이중 세번째 경우만이 가능하므로 증명이 끝난다. \square

즉 $G \setminus G_+$ 의 임의의 원소 r 은 임의의 $x \in S^1$ 가 주어졌을 때 그 ϕ -궤도 $\{x, \phi x, \dots, \phi^{N-1}x\}$ 를 다른 ϕ -궤도 $\{rx, \phi^{-1}(rx), \phi^{-2}(rx), \dots, \phi^{-(N-1)}rx\} = \{rx, \phi(rx), \dots, \phi^{N-1}(rx)\}$ 로 보낸다는 것을 알 수 있고, 따라서 G 전체가 몫공간인 S^1 에도 자연스럽게 작용한다. 즉, π 와 호환되는 군 맞춤 사상 $\rho: G \rightarrow \rho(G)$ 가 존재한다.

이제 몫공간 S^1 에서 임의의 닫힌 구간 I 가 주어졌을 때, $S^1 \setminus I$ 안의 점 c 를 하나 잡으면 $\pi^{-1}(I)$ 는 N 개의 연결 성분으로 이루어져 있으며 각각은 $[c, \phi(c)), [\phi(c), \phi^2(c)), \dots, [\phi^{N-1}(c), \phi^N(c) = c)$ 안에 포함되어 있다. 예를 들어 $[c, \phi(c))$ 안에 있는 연결성분 \tilde{I} 를 택하면, \tilde{I} 는 축약 가능하고 $\inf_{g \in G} \text{diam}(g\tilde{I}) = 0$ 이 성립한다. 이 사실은 덮음 사상 π 를 통해서도 전달되므로 $\inf_{g \in G} \text{diam}(\rho(g)I) = 0$ 또한 성립한다. 따라서 $\rho(G)$ 의 작용은 강하게 팽창적이다. \square

여기서 근접성에 관한 논의를 잠깐 마무리짓겠다. 만약 $\text{Homeo}(S^1)$ 의 어떤 부분군 G 의 작용이 최소한이라면, G 의 작용은 균일연속하거나, 팽창적이되 강하게 팽창적이지는 않거나, 혹은 강하게 팽창적이다. G 의 작용이 균일연속한 경우, 켈레바꾸기를 통해 S^1 의 등거리사상 군으로 나타낼 수 있다. 이 경우 임의의 두 점 $x, y \in S^1$ 사이 거리는 G 의 작용에 의해 보존되므로, 이 작용은 근접적일 수 없다. 만약 G 의 작용이 팽창적이되 강하게 팽창적이지는 않다면, 보조정리 1.21에서 기술하는 원의 자가 덮음 사상 $\pi: S^1 \rightarrow S^1$ 이 존재해 G 의 작용과 π 는 호환 가능하고, 몫공간 S^1 에서의 G 의 작용은 강하게 팽창적이다. 이 경우 π 는 차수가 1보다 큰 덮음 사상이어야 한다. 이제 어떤 점 $y \in S^1$ 을 잡은 뒤 $\pi^{-1}(y)$ 안의 서로 다른 두 점 $a, b \in \pi^{-1}(y)$ 을 고르면, 그 어느 $g \in G$ 를 가져와도 ga 및 gb 는 같은 π -값을 가지는 다른 점들이다. 이러한 점들 사이 거리는 0에 한없이 가까울 수 없기에 (보조정리 1.21의 증명에서 $d(x, \theta(x)) > \epsilon_G$ 가 항상 성립했음을 기억하라), $\inf_{g \in G} d(ga, gb) > 0$ 이다. 따라서 이 경우에도 G 의 작용은 근접적일 수 없다. 요약하자면, $\text{Homeo}(S^1)$ 의 어떤 부분군 G 의 작용이 최소한이라는 가정 하에, G 의 작용이 만약 근접적이라면 반드시 강하게 팽창적이어야 한다.

이제 어떤 $G \leq \text{Homeo}(S^1)$ 의 작용이 최소한이고 강하게 팽창적이라면 G 안에는 서로 겹치지 않는 열린 구간 네 개에 결부된 Schottky 순서쌍이 존재함을 관찰하자. 이를 위해 임의의 (원 전체가 아닌) 열린 구간 I 을 생각하자. 그러면 I 도 $J := (\int I_1)^c$ 도 축약가능한 구간이므로 $\lim_n \text{diam}(g_n I) = \lim_n \text{diam}(h_n J) = 0$ 이게끔 하는 G 의 원소 나열 $(g_n)_{n>0}$ 및 $(h_n)_{n>0}$ 이 존재한다. 이때, $\{g_n I : n > 0\}$ 의 집적점 x 및 $\{h_n J : n > 0\}$ 의 집적점 y 를 서로 다른 것으로 잡을 수 있는지 살펴보자. 이것이 불가능한 유일한 경우는 $(g_n I)_{n>0}$ 및 $(h_n J)_{n>0}$ 가 모두 같은 점 $x \in S^1$ 로 수렴할 때뿐인데, 이 경우에는 x 를 $S^1 \setminus \{x\}$ 안으로 보내는 어떤 $g' \in G$ 를 잡으면 $(g_n I)_{n>0}$ 의 집적점인 x 와 $(g'h_n J)_{n>0}$ 의 집적점인 $g'x$ 는 서로 다른 점이 된다. 물론 $g'h_n J$ 의 크기 또한 0으로 수렴하므로, $(h_n)_{n>0}$ 대신 $(g'h_n)_{n>0}$ 을 사용함으로써 앞의 질문에 대답할 수 있다. 즉, G 안의 적당한 원소 나열 $(g_n)_{n>0}$ 및 $(h_n)_{n>0}$ 및 원

위의 서로 다른 점 $x, y \in S^1$ 가 존재하여

$$\text{diam}(g_n I \cup x) \rightarrow 0, \quad \text{diam}(h_n J \cup x) \rightarrow 0$$

이게끔 할 수 있다.

이제 $\{x, y\}$ 와 $\{fx, fy\}$ 가 원소를 공유하지 않게끔 하는 $f \in G$ 를 찾고자 한다. 먼저, G 의 작용이 최소한이기에 $f_1(x), \dots, f_6(x)$ 가 (x, y) 안의 서로 다른 여섯 개의 점이 되도록 하는 G 의 원소 f_1, \dots, f_6 를 찾을 수 있다. 여기서 f_i 들 중 어느 하나라도 y 를 $\{x, y\}$ 밖의 점으로 보내면 그 원소를 f 로 쓰면 된다. 그렇지 않고 예를 들어 f_1y, f_2y 및 f_3y 가 $\{x, y\}$ 안의 어떤 한 점 p 로 일치한다고 해보자. 그러면 p 를 (x, y) 안으로 보내는 어떤 원소 $f' \in G$ 가 존재할 텐데, 이때 $f'f_1y, f'f_2y$ 및 $f'f_3y$ 는 서로 다른 세 점이기에, 이들 중 적어도 하나는 x 도 y 도 아니다. 따라서 $f'f_iy \notin \{x, y\}$ 인 $i \in \{1, 2, 3\}$ 을 잡을 수 있고, 이때 $f'f_ix = f'p$ 또한 $\{x, y\}$ 바깥에 있어 $f'f_i$ 를 f 로 쓸 수 있다.

이제, 충분히 큰 n 에 대해, $g_n I, h_n J, f g_n I, f h_n J$ 는 서로 다른 네 점에 충분히 가까운 구간들이므로 서로 겹치지 않는다. 이제 $F = h_n g_n^{-1}$ 및 $G = f h_n g_n^{-1} f$ 를 생각하면 F 는 $g_n I^c$ 를 $h_n \bar{J}$ 로 보내고, F^{-1} 는 $h_n J^c$ 를 $g_n \bar{I}$ 로 보내며, G 는 $f g_n I^c$ 를 $f h_n \bar{J}$ 로, G^{-1} 는 $f h_n J^c$ 를 $f g_n \bar{I}$ 로 보낸다. 이제 $g_n I, h_n J, f g_n I, f h_n J$ 를 모두 살짝씩 키워 열린 구간으로 만들되 여전히 서로 겹치지 않게끔 할 수 있고, (F, G) 는 이 구간들에 결부된 Schottky 순서쌍이 된다.

2. 응용: 무작위 행보의 지수함수적 축약성 및 확률론적인 Tits 대안

이 절에서는 기존에 알려진 결과를 약간 더 확장한 버전을 논하기에, 설명문을 영어로 달아 둔다. (이하 영문)

We study two consequences of the weak Tits alternative of Margulis' and Ghys' weak Tits alternative on $\text{Homeo}(S^1)$. These consequences are concerned with random walks on $\text{Homeo}(S^1)$, and were proven earlier by Martín Gilabert Vio and Dominique Malicet, respectively. Our purpose is to give a different approach that gives an additional quantitative bound. This quantitative bound is stable under perturbation of the underlying measure for the random walk.

We make an important remark. We say that a probability measure μ on $\text{Homeo}(S^1)$ is *nondegenerate* if its support $\langle\langle \text{supp } \mu \rangle\rangle$, the complement of the largest open subset of $\text{Homeo}(S^1)$ that attains zero hitting measure, is a *subgroup* of G . By nature, $\langle\langle \text{supp } \mu \rangle\rangle$ is indeed a subsemigroup, but is not always a subgroup. This requirement is needed to implement Margulis-Ghys weak Tits alternative on $\text{Homeo}(S^1)$.

To begin with, we recall the following theorem recently proven by Martín Gilabert Vio:

정리 2.1 ([GV24, Theorem A]). *Let μ_1, μ_2 be nondegenerate probability measures on $\text{Diff}_+^1(S^1)$ such that the actions of $G_1 = \langle\langle \text{supp } \mu_1 \rangle\rangle$ and of $G_2 = \langle\langle \text{supp } \mu_2 \rangle\rangle$ are proximal, and such that for every $i = 1, 2$, either*

- (1) *the support of μ_i is finite, or*
- (2) *the support of μ_i is included in $\text{Diff}_+^{1+\tau}(S^1)$ for some $\tau \in (0, 1)$ and the integrals*

$$\int_{G_i} \max \{ |g|_{\text{Lip}}, |g^{-1}|_{\text{Lip}} \}^\delta d\mu(g), \int_{G_i} |\log g'|_\tau d\mu(g),$$

are finite for some $\delta > 0$.

Let $(Z_n)_{n>0}$ and $(Z'_n)_{n>0}$ be independent (left) random walks generated by μ_1 and μ_2 , respectively. Then there exists $q \in (0, 1)$ such that

$$\mathbb{P}(Z_n \text{ and } Z'_n \text{ comprise a ping-pong pair}) \geq 1 - q^n$$

for all $n \in \mathbb{Z}_{>0}$.

We have not defined a ping-pong pair, which will come shortly after. For now, it suffices to know that ping-pong pairs in $\text{Homeo}(S^1)$ generates a free subgroup. As a consequence of this exponential bound, Gilabert Vio proved that independent random walks eventually generate free subgroups almost surely.

The above Theorem 2.1 is concerned with random diffeomorphisms in a subgroup with proximal action. A companion result for more general homeomorphisms is as follows.

정리 2.2 ([GV24, Theorem C]). *Let μ_1, μ_2 be nondegenerate probability measures on $\text{Homeo}_+^1(S^1)$ such that the actions of $G_1 = \langle\langle \text{supp } \mu_1 \rangle\rangle$ and of $G_2 = \langle\langle \text{supp } \mu_2 \rangle\rangle$ do not admit invariant probability measure. Let $(Z_n)_{n>0}$ and $(Z'_n)_{n>0}$ be independent (left) random walks generated by μ_1 and μ_2 , respectively. Then the following holds almost surely:*

$$\lim_{N \rightarrow \infty} |\{0 \leq n \leq N \mid Z_n \text{ and } Z'_n \text{ comprise a ping-pong pair}\}| = 1.$$

Our first result is that one can describe exponential genericity of ping-pong pairs for independent random walks on $\text{Homeo}(S^1)$.

Theorem A. *Let μ_1 and μ_2 be nondegenerate probability measures on $\text{Homeo}(S^1)$ such that the actions of $G_1 = \langle\langle \text{supp } \mu_1 \rangle\rangle$ and of $G_2 = \langle\langle \text{supp } \mu_2 \rangle\rangle$ do not admit invariant probability measure. Let $(Z_n)_{n>0}$ and $(Z'_n)_{n>0}$ be independent random walks generated by μ_1 and μ_2 , respectively. Then the following holds almost surely: Then there exists $\kappa > 0$ such that*

$$(2.1) \quad \mathbb{P}(Z_n \text{ and } Z'_n \text{ comprise a ping-pong pair}) \geq 1 - \frac{1}{\kappa} e^{-\kappa n}$$

for all $n \in \mathbb{Z}_{>0}$.

Furthermore, the coefficient κ is stable under perturbation in the following sense: there exist neighborhoods \mathcal{U}_1 of μ_1 and \mathcal{U}_2 of μ_2 in the space of probability measures on $\text{Homeo}(S^1)$ (in the weak-* topology), respectively, so that Inequality 2.1 holds even if $(Z_n)_{n>0}$ is driven by an arbitrary measure in \mathcal{U}_1 and $(Z'_n)_{n>0}$ is driven by an arbitrary measure in \mathcal{U}_2 .

Let us now recall the exponential synchronizing proven by Dominique Malicet.

정리 2.3 ([Mal17, Theorem A]). *Let μ be a probability measure on $\text{Homeo}(S^1)$ such that the action of $G = \langle\langle \text{supp } \mu \rangle\rangle$ does not admit invariant probability measure. Let $(Z_n)_{n>0}$ be independent (left) random walks generated by μ . Then there exists $q \in (0, 1)$ such that for each $x \in S^1$, for almost every random path $(Z_n(\omega))_{n>0}$, there exists a neighborhood $I_{x,\omega}$ of x such that*

$$\text{diam}(Z_n(\omega)(I)) \leq q^n$$

for all $n \in \mathbb{Z}_{>0}$.

Our second result strengthens this result by providing an exponential bound on the error event:

Theorem B. Let μ be a nondegenerate probability measure on $\text{Homeo}(S^1)$ such that the action of $G = \langle\langle \text{supp } \mu \rangle\rangle$ does not admit invariant probability measure. Let $(Z_n)_{n>0}$ be independent (left) random walks generated by μ . Then there exists $\kappa > 0$ such that for each $x \in S^1$,

$$(2.2) \quad \mathbb{P} \left(\omega : \begin{array}{l} \text{there exists a neighborhood } I_{x,\omega} \text{ of } x \text{ such that} \\ \text{diam}(Z_k(\omega)(I_{x,\omega})) \leq q^k \text{ for } k \geq n \end{array} \right) \geq 1 - \frac{1}{\kappa} e^{-\kappa n}$$

for all $n \in \mathbb{Z}_{>0}$.

Furthermore, the coefficient κ is stable under perturbation. That means, there exists a neighborhood \mathcal{U} of μ in the space of probability measures on $\text{Homeo}(S^1)$ (in the weak-* topology) so that Inequality 2.2 holds (for the same uniform $\kappa > 0$) even if $(Z_n)_{n>0}$ is driven by an arbitrary measure in \mathcal{U} .

This theorem follows from the special case where the action of G is proximal. In such a case, one can give more description about $I_{x,\omega}$:

Theorem C. Let μ be a nondegenerate probability measure on $\text{Homeo}(S^1)$ such that the action of $G = \langle\langle \text{supp } \mu \rangle\rangle$ is proximal. Let $(Z_n)_{n>0}$ be the (left) random walk generated by μ . Then there exists $\kappa > 0$ such that for each $x \in S^1$,

$$(2.3) \quad \mathbb{P} \left(\omega : \begin{array}{l} \text{there exists a neighborhood } I_{x,\omega} \text{ of } x \text{ such that} \\ \text{diam}(I_{x,\omega}) \geq 1 - q^n \text{ and } \text{diam}(Z_k(\omega)(I_{x,\omega})) \leq q^k \text{ for } k \geq n \end{array} \right) \geq 1 - \frac{1}{\kappa} e^{-\kappa n}$$

for all $n \in \mathbb{Z}_{>0}$.

Furthermore, the coefficient κ is stable under perturbation. That means, there exists a neighborhood \mathcal{U} of μ in the space of probability measures on $\text{Homeo}(S^1)$ (in the weak-* topology) so that Inequality 2.2 holds (for the same uniform $\kappa > 0$) even if $(Z_n)_{n>0}$ is driven by an arbitrary measure in \mathcal{U} .

Remark 2.4. In Theorem B and C, it is important that the choice of $I_{x,\omega}$ depends on $I_{x,\omega}$. It is easy to construct a random walk (say, a nearest-neighbor random walk on a surface group acting on $S^1 = \partial\mathbb{H}^2$) such that for any nonempty open set O , there exists $\epsilon > 0$ such that

$$\mathbb{P}(\text{diam}(Z_n \cdot O) > 1/2) > \epsilon$$

for each $n \in \mathbb{Z}_{>0}$.

The statements in Theorem A, B, C still hold even if the the step distributions for the random walk are independent but non-identical, as long as they are distributed according to measures chosen from \mathcal{U} or \mathcal{U}_1 and \mathcal{U}_2 , respectively.

We finally observe one another result for proximal actions.

Theorem D. Let μ be a nondegenerate probability measure on $\text{Homeo}(S^1)$ such that the action of $G = \langle\langle \text{supp } \mu \rangle\rangle$ is proximal. Let $(Z_n)_{n>0}$ be the random walk generated by μ . Then there exists $\kappa > 0$ such that for each $x, y \in S^1$,

$$(2.4) \quad \mathbb{P}_{Z_n \sim \mu^{*n}}(d(Z_n x, Z_n y) < e^{-\kappa n}) \geq 1 - \frac{1}{\kappa} e^{-\kappa n}$$

for all $n \in \mathbb{Z}_{>0}$.

Furthermore, the coefficient κ is stable under perturbation. That means, there exists a neighborhood \mathcal{U} of μ in the space of probability measures on $\text{Homeo}(S^1)$ (in the weak-* topology) so that Inequality 2.2 holds (for the same uniform $\kappa > 0$) even if $(Z_n)_{n>0}$ is driven by an arbitrary measure in \mathcal{U} .

In Theorem A or D, it is not important if the random walk is a right random walk or left random walk. Indeed, the estimate is a snapshot at step n . In Antonov's work and Malicet's work [Mal17], the authors mainly discussed exponential synchronization for left random walk.

Our results are purely for homeomorphism groups. The only property of the group element that we use is the following: If I and J are nested intervals of S^1 , their images are also nested.

Our method is based on Gouëzel's pivoting technique, which is first introduced in [Gou22] and led to a remarkable exponential estimate for random walks on Gromov hyperbolic spaces. There has been several attempts to generalize Gouëzel's technique to a broader setting, and this paper is in line with those efforts. We use Schottky dynamics exhibited by Schottky pairs of homeomorphisms to implement Gouëzel's pivoting time construction. It turns out that the 1-dimensionality of the ambient space is somehow crucial, but the more crucial thing is the nesting of the Schottky regions. For instance, the particular choice of Lebesgue measure (when measuring the diameter of intervals) is not important; we have:

정리 2.5. *The statement in Theorem B and C hold even if the diameter $\text{diam}(\cdot)$ is replaced with $\nu(\cdot)$ for an arbitrary probability measure ν on S^1 .*

{thm:main5}

So above, ν need not be absolutely continuous with respect to Leb , but could be e.g., a measure concentrated on a Cantor set or as such.

For brevity, we will only prove Theorem A for proximal actions, and Theorem C and D. The general case follows from Margulis' and Ghys' weak Tits alternative (see Remark 2.8).

2.1. $\text{Homeo}(S^1)$ 위의 확률 측도와 Schottky 집합 $\text{Homeo}(S^1)$ 에는 흔히 (컴팩트-열림 위상과 동일한) C^0 -위상을 주는데, 이 위상 구조에 대해 $\text{Homeo}(S^1)$ 는 폴란드 공간(Polish space) 및 위상군(topological group)이 된다. 그러면 $\text{Homeo}(S^1)$ 위의 확률 측도들의 모임에 약한 위상을 줄 수 있다. 이는 $\text{Homeo}(S^1)$ 위의 유계인 연속 함수 f 및 실수 $a < b$ 에 대해

$$\left\{ \mu : a < \int_{\text{Homeo}(S^1)} f d\mu < b \right\}$$

형태인 측도 집합들을 위상 구조의 기저로 삼겠다는 것이다.

앞으로 논할 $\text{Homeo}(S^1)$ 위의 측도는 모두 (컴팩트-열림 위상 구조에 대한) Borel 측도이다. $\text{Homeo}(S^1)$ 위의 측도 μ 및 ν 가 주어졌을 때 그 합성곱(convolution)을

$$(\mu * \nu)(A) := (\mu \times \nu) \left(\left\{ (g, h) \in (\text{Homeo}(S^1))^2 : gh \in A \right\} \right)$$

과 같이 정의할 수 있다. 또한, μ 의 n 번 자기합성곱 $\mu * \dots * \mu$ 를 μ^{*n} 으로 줄여 쓰겠다. 그리고 $\mu(K) = 1$ 을 만족하는 $\text{Homeo}(S^1)$ 의 닫힌 집합 K 중 가장 작은 것을 μ 의 받침(support)이라고 부르고 $\text{supp } \mu$ 로 표기하겠다. 그러면 $\text{Homeo}(S^1)$ 의 원소 g 에 대해, g 가 $\text{supp } \mu$ 에 포함될 필요충분조건은 g 의 임의의 근방이 항상 0보다 큰 μ -값을 가진다는 것이다.

정의 2.6. 원의 자기위상동형사상 f 및 원 위의 서로 겹치지 않는 부분집합 U_1, U_2 을 생각하자. 만약

$$f(S^1 \setminus U_1) \subseteq U_2, f(S^1 \setminus U_2) \subseteq U_1$$

가 성립하면, f 를 (U_1, U_2) -쌍곡적인 위상동형사상이라고 부른다. 또, (U_1, U_2) -쌍곡적인 위상동형사상의 집합을 $\mathfrak{S}(U_1, U_2)$ 로 표기한다.

만약 U_1 및 U_2 가 열린 집합이라면 $\mathfrak{S}(U_1, U_2)$ 또한 열린 집합이고, 둘이 닫힌 집합이라면 $\mathfrak{S}(U_1, U_2)$ 또한 닫힌 집합임을 관찰할 수 있다.

정의 2.7. 서로 겹치지 않는 원 위의 닫힌 구간 $I_1, \dots, I_N, J_1, \dots, J_N$ 에 대해 $\text{Homeo}(S^1)$ 의 부분집합 $S := \mathfrak{S}(I_1, J_1) \cup \dots \cup \mathfrak{S}(I_N, J_N)$ 를 $(I_1, \dots, I_N, J_1, \dots, J_N)$ 에 결부된 Schottky 집합이라고 부른다. 이때 N 을 S 의 분해능(resolution)이라고 부른다. 각각의 $s \in \mathfrak{S}(I_i, J_i)$ 마다 $s \in \mathfrak{S}(I_i, J_i)$ 이게끔 하는 I_i 및 J_i 가 유일하게 결정되는데, 이들을 각각 $I(s)$ 및 $J(s)$ 라고 적겠다.

만약 어떤 구간 \mathcal{I} 이 존재해 $I_1 \cup \dots \cup I_N \subseteq \text{int}(S^1 \setminus \mathcal{I})$ 및 $J_1 \cup \dots \cup J_N \subseteq \text{int} \mathcal{I}$ 가 성립한다면 \mathcal{I} 를 S 의 중선(median)이라고 부른다.

양수 $\epsilon > 0$ 및 서로 겹치지 않는 닫힌 구간 $I_1, \dots, I_N, J_1, \dots, J_N$ 에 결부된 Schottky 집합 S 를 생각하자. 이때,

$$i = 1, \dots, N \text{마다 } \mu(\mathfrak{S}(I_i, J_i)) > \epsilon/N$$

을 만족하는 $\text{Homeo}(S^1)$ 상의 측도 μ 를 (S, ϵ) -맞춤 측도라고 부르고,

$$i = 1, \dots, N \text{마다 } \mu(\mathfrak{S}(I_i, J_i)) = 1/N$$

을 만족하는 $\text{Homeo}(S^1)$ 상의 측도 μ 는 S 위에서 Schottky-균일하다고 말한다.

n:reduction}

Remark 2.8. 이후에 이어질 내용에서는 무작위 행보가 빠짐없이 지나는 부분군 G 의 작용이 근접적이라는 것을 가정할 것이다. 일반적인 경우에 있어서는, 정리 1.2에서 보장하는 군 맞춤 사상 ρ 를 사용해 $\rho(G)$ 의 S^1 상의 작용에 대해서 공부하기만 하면 충분하다. 왜냐하면 $\rho(G)$ 에는 (구간들에 결부된) Schottky 순서쌍이 존재하기 때문이다. 여기서 $\rho(G)$ 가 작용하는 S^1 에는 S^1 상의 Lebesgue 측도를 $\pi \circ c$ 로 앞으로 밀어낸(pushforward) 측도 $(\pi \circ c)^* \text{Leb}$ 를 부여한다. 이렇게 했을때, 무작위 행보가 아랫층, 즉 $\rho(G)$ 위에서 걸어나간다고 간주했을 때, $(\pi \circ c)^* \text{Leb}$ 측도를 기준으로 지수함수적인 축약성을 보이면, 윗층인 (S^1, Leb) 에서도 국소적인 지수함수적 축약성을 보인다는 것을 관찰하는 것은 어렵지 않다.

보조정리 2.9. $\text{Homeo}(S^1)$ 위의 확률 측도 μ 를 생각하자. 만약 $\text{supp } \mu$ 가 Schottky 순서쌍을 하나 포함하고 있다면, 임의의 양의 정수 N 가 주어질 때마다 $\epsilon > 0$, $m \in \mathbb{Z}_{>0}$ 및 중선 달린 분해능 N 짜리 Schottky 집합 S' 가 존재해 μ^{*m} 이 (S', ϵ') -맞춤 측도가 된다.

Proof. 가정에 의해, $\text{supp } \mu$ 는 Schottky 순서쌍 $\{f_1, f_2\}$ 을 하나 포함한다. 이는 다시 말해, 서로 겹치지 않는 원 위의 닫힌 구간 I_1, I_2, J_1, J_2 이 존재해 $f_i \in \mathfrak{S}(I_i, J_i)$ 가 성립한다는 뜻이다.

여기서 I_i, J_i 의 배치에 따라 경우를 나눌 수 있다. 만약 $I_1 \cup I_2 \subseteq \mathcal{I}$ 및 $J_1 \cup J_2 \subseteq S^1 \setminus \mathcal{I}$ 이게끔 하는 닫힌 구간 \mathcal{I} 가 존재한다면, 이 \mathcal{I} 를 기록해 두겠다. 그렇지 않은 경우, I_1, J_1, I_2, J_2 는 순서대로 시계방향 혹은 반시계방향으로 배치되어 있다. 어느 경우이건, I_1, J_1 및 I_2 를 포함하되 J_2 와는 겹치지

않는 구간을 하나 잡아 \mathcal{I} 로 쓰겠다. 이는 $\{f_1, f_2\}$ 용 중선으로 볼 수는 없지만, $\{f_2^2, f_2f_1\}$ 용 중선으로 볼 수 있다. 실제로

$$f'_1 := f_2f_1, f'_2 := f_2^2, I'_1 := I_1, J'_1 := f_2J_1, I'_2 := I_2, J'_2 := f_2J_2$$

에 대해 $f_i(S^1 \setminus I'_i) \subseteq J'_i, f_i^{-1}(S^1 \setminus J'_i) \subseteq I'_i$ 가 성립함은 물론,

$$J'_1 \cap J'_2 = f_2(J_1 \cap J_2) = \emptyset, (I'_1 \cup I'_2) \cap (J'_1 \cup J'_2) \subseteq (I_1 \cup I_2) \cap f_2(S^1 \setminus I_2) \subseteq (I_1 \cup I_2) \cap J_2 = \emptyset$$

이 성립한다. 또 I_1, I_2 와는 만나지 않되 J_2 를 포함하는 닫힌 구간 \mathcal{I} 는 쉽게 잡을 수 있는데, 이때 $\text{int } \mathcal{I}$ 는 $\text{int } J_2$ 의 부분집합인 J'_1 및 J'_2 도 포함한다. 따라서 이러한 \mathcal{I} 는 $\{f'_1, f'_2\}$ 용 중선으로 볼 수 있다. 여기서 $f'_1, f'_2 \in \text{supp } \mu^{*2}$ 임에 주목하라.

위의 논의를 비추어 보았을 때, 필요하다면 μ^{*2} 로 μ 를 갈음함으로써, 서로 겹치지 않는 닫힌 구간 I_1, I_2, J_1, J_2 에 결부된 Schottky 순서쌍 $\{f_1, f_2\}$ 는 (닫힌) 중선 \mathcal{I} 를 가진다고 가정할 수 있다. 이제 $\{1, 2\}^N$ 의 원소들을 꼬리표 삼아 위상동형사상 2^N 개를 나열하려고 한다. 그말인즉 $\sigma \in \{1, 2\}^N$ 가 주어질 때마다

$$f_\sigma := f_{\sigma(1)}f_{\sigma(2)} \cdots f_{\sigma(N)}, I_\sigma := f_\sigma^{-1}(\overline{S^1 \setminus \mathcal{I}}), J_\sigma := f_\sigma \mathcal{I}$$

를 정의하면, f_σ^2 는 $S^1 \setminus I_\sigma$ 를 J_σ 안으로 보내고 f_σ^{-2} 는 $S^1 \setminus J_\sigma$ 를 I_σ 로 안으로 보낸다. 또한,

$$\begin{aligned} J_\sigma &= f_{\sigma(1)} \cdots f_{\sigma(N)} \mathcal{I} = f_{\sigma(1)} \cdots f_{\sigma(N-1)} J_{\sigma(N)} \\ &\subseteq f_{\sigma(1)} \cdots f_{\sigma(N-1)} \mathcal{I} = f_{\sigma(1)} \cdots f_{\sigma(N-2)} J_{\sigma(N-1)} \\ &\subseteq \cdots \subseteq J_{\sigma(1)} \subseteq \text{int } \mathcal{I} \end{aligned}$$

가 성립한다. 비슷한 이유로 $I_\sigma \subseteq \text{int}(S^1 \setminus \mathcal{I})$ 가 성립한다. 이는 곧 임의의 $\sigma, \sigma' \in \{1, 2\}^N$ 에 대해 I_σ 와 $J_{\sigma'}$ 는 겹치지 않는다는 뜻이기도 하다. 이제 $\{1, 2\}^N$ 의 서로 다른 두 원소 σ 및 σ' 를 생각하자. 그러면 $\sigma(i) \neq \sigma'(i)$ 인 정수 i 가 반드시 존재하며, 그런 정수 중 가장 작은 것을 잡겠다. 그러면

$$J_\sigma \subseteq f_{\sigma(1)} \cdots f_{\sigma(i-1)} J_{\sigma(i)}, J_{\sigma'} \subseteq f_{\sigma'(1)} \cdots f_{\sigma'(i-1)} J_{\sigma'(i)}$$

는 서로 겹치지 않음을 확인할 수 있다. 비슷한 이유로, I_σ 와 $I_{\sigma'}$ 도 겹치지 않는다. 요약하자면, 우리는 서로 겹치지 않는 닫힌 구간 $2 \cdot 2^N$ 개 $\{I_\sigma, J_\sigma : \sigma \in \{1, 2\}^N\}$ 을 설계했는데, $(\text{supp } \mu^{*N})$ 은 각각의 $\mathcal{S}(I_\sigma, J_\sigma)$ 와 겹친다. 또, $\cup_\sigma I_\sigma \subseteq \text{int } \mathcal{I}$ 및 $\cup_\sigma J_\sigma \subseteq \text{int}(S^1 \setminus \mathcal{I})$ 가 성립한다.

이제, I_σ, J_σ 들을 살짝 늘려 여전히 서로 겹치지 않게 할 수 있다. 다시 말해, $I_\sigma \subseteq \text{int } I'_\sigma, J_\sigma \subseteq \text{int } J'_\sigma$ 를 만족하는 서로 겹치지 않는 닫힌 구간 $\{I'_\sigma, J'_\sigma : \sigma \in \{1, 2\}^N\}$ 을 잡을 수 있다. 또, $\cup_\sigma I'_\sigma \subseteq \text{int}(S \setminus \mathcal{I})$ 및 $\cup_\sigma J'_\sigma \subseteq \text{int } \mathcal{I}$ 가 여전히 성립하게끔 하는 것도 어렵지 않다.

그러면 각각의 $\sigma \in \{1, 2\}^N$ 에 대해 $\mathcal{S}(\text{int } I_\sigma, \text{int } J_\sigma)$ 는 $\text{supp } \mu^{*N}$ 과 겹치는 열린 집합이고, 따라서 양수인 μ^{*N} -값을 가진다. 이는 곧 $S = \{\mathcal{S}(I'_\sigma, J'_\sigma) : \sigma \in \{1, 2\}^N\}$ 라는 (\mathcal{I} 를 중선으로 가지는) Schottky 집합 및 적당한 $\epsilon > 0$ 에 대해 μ^{*N} 가 (S, ϵ) -맞춤 측도임을 의미한다. \square

명제 2.10. 임의의 양수 $\epsilon > 0$, 자연수 m 및 100보다 큰 자연수 N 이 주어졌을 때 다음을 만족하는 $\kappa = \kappa(\epsilon, m, N) > 0$ 이 존재한다.

구간 \mathcal{I} 를 중선으로 가지는 분해능 N 짜리 Schottky 집합 S 및 $\text{Homeo}(S^1)$ 위의 확률 측도 μ 에 대해, μ^{*m} 이 (S, ϵ) -맞춤 측도임을 가정하자. 그러면 각 자연수 n 에 대해 어떤 확률 공간 Ω_n , 가측 부분집합 $A_n \subseteq \Omega_n$, A_n 의 가측 분할 $\mathcal{P}_n = \{\mathcal{E}_\alpha\}_\alpha$, 그리고 $\text{Homeo}(S^1)$ 의 원소들을 값으로 가지는 확률변수들 $Z_n, \{w_i\}_{i=0, \dots, [\kappa n]}, \{s_i\}_{i=1, \dots, [\kappa n]}$ 가 존재하여 다음이 성립한다:

$$(1) \mathbb{P}(A_n) \geq 1 - \frac{1}{\kappa} e^{-\kappa n}.$$

- (2) \mathcal{P}_n 을 이루는 각 동치류 $\mathcal{E} \in \mathcal{P}_n$ 에 한정해서 보았을 때, $w_0, \dots, w_{\lfloor \kappa n \rfloor}$ 는 각각 고정된 위상동형 사상들이고, s_i 들은 각각 S 위에서 Schottky 맞춤 균일분포를 가지는 독립인 확률변수들이다.
- (3) A_n 안에서는 $i = 1, \dots, \lfloor \kappa n \rfloor - 1$ 각각에 대해 $w_i \mathcal{I} \subseteq \mathcal{I}$ 이다.
- (4) Z_n 는 μ^{*n} 의 분포를 따르며, A_n 위에서 $Z_n = w_0 s_1 w_1 \cdots s_{\lfloor \kappa n \rfloor} w_{\lfloor \kappa n \rfloor}$ 이다.

이 명제를 가정하면 무작위 행보에 의한 지수함수적으로 가까워짐은 쉽게 증명할 수 있다. 이제부터, S^1 위에 확률 측도 Len 을 하나 고정하겠다. 정리 A, C 및 D를 위해서는 Lebesgue 측도를 이 측도로 삼으면 되고, 정리 B를 위해서는 Remark 2.8과 같이 조치해주면 된다. 정리 2.5를 위해서는 일반적인 측도로 두면 된다.

보조정리 2.11. 원의 위상동형사상 $w \in \text{Homeo}(S^1)$, 구간 \mathcal{I} 를 중선으로 가지는 분해능 N 짜리 Schottky 집합 S 및 S 위의 Schottky-맞춤 균일 분포 μ 를 생각하자. 그러면

$$\mathbb{P}_{s \sim \mu} \left(\text{Len}(ws\mathcal{I}) \leq \frac{1}{\sqrt{N}} \text{Len}(w\mathcal{I}) \right) \geq 1 - \frac{1}{\sqrt{N}}$$

이 성립한다.

Proof. 먼저, 서로 겹치지 않는 닫힌 구간 $I_1, \dots, I_N, J_1, \dots, J_N$ 을 찾아서 $S = \{\mathfrak{S}(I_1, J_1), \dots, \mathfrak{S}(I_N, J_N)\}$ 꼴로 적자. 이때, $\mathfrak{S}(I_i, J_i)$ 의 원소들은 \mathcal{I} 를 J_i 안으로 집어넣는다. (*) 여기서 wJ_1, \dots, wJ_N 들은 $w\mathcal{I}$ 라는 구간에 포함되며 서로 겹치지 않는다. 따라서 이들의 길이의 합은 \mathcal{I} 의 길이보다 작거나 같고

$$\text{Ind} := \left\{ i : \text{Len}(wJ_i) \geq \frac{1}{\sqrt{N}} \text{Len}(w\mathcal{I}) \right\}$$

의 크기가 최대 \sqrt{N} 임을 관찰할 수 있다. 또한 (*)에 따르면, $i \notin \text{Ind}$ 를 고정했을 때 $\mathfrak{S}(I_i, J_i)$ 의 임의의 원소 s 에 대해 $\text{Len}(ws\mathcal{I}) \leq \frac{1}{\sqrt{N}} \text{Len}(w\mathcal{I})$ 가 성립한다. 이를 종합하여

$$\begin{aligned} \mathbb{P}_{s \sim \mu} \left(\text{Len}(ws\mathcal{I}) \leq \frac{1}{\sqrt{N}} \text{Len}(w\mathcal{I}) \right) &\geq \mathbb{P}_{s \sim \mu} (s \in \mathfrak{S}(I_i, J_i) : i \notin \text{Ind}) \\ &\geq \frac{1}{N} (N - \sqrt{N}) = 1 - \frac{1}{\sqrt{N}} \end{aligned}$$

를 관찰할 수 있다. □

보조정리 2.12. 구간 \mathcal{I} 를 중선으로 가지는 분해능 $N \geq 100$ 짜리 Schottky 집합 S 및 위상동형사상 $w_0, \dots, w_n \in \text{Homeo}(S^1)$ 을 고정하되, $i = 1, \dots, n$ 에 대해 $w_i \mathcal{I} \subseteq \mathcal{I}$ 를 가정하자. 그러면 서로 독립이면서 각각 S 위에서 Schottky-맞춤 균일 분포를 가지는 s_1, \dots, s_n 에 대해

$$\mathbb{P} \left(\text{Len}(w_0 s_1 w_1 \cdots s_n w_n \cdot \mathcal{I}) \leq \frac{1}{N^{n/4}} \text{Len}(w_0 \mathcal{I}) \right) \geq 1 - e^{-n/4}$$

이 성립한다.

Proof. 이번에도 $S = \{\mathfrak{S}(I_1, J_1), \dots, \mathfrak{S}(I_N, J_N)\}$ 꼴로 적고 증명을 시작하겠다. 여기서, $\mathfrak{S}(I_i, J_i) \in S$ 의 임의의 원소 s 는 \mathcal{I} 를 J_i 안으로 보내기에, $s\mathcal{I} \subseteq \mathcal{I}$ 가 항상 성립함을 주목하자. 즉,

$$W_0 \mathcal{I} \supseteq W_0 s_1 \mathcal{I} \supseteq W_1 \mathcal{I} \supseteq W_1 s_1 \mathcal{I} \supseteq \dots \supseteq W_n \mathcal{I} \quad (W_k = W_k(s_0, \dots, s_k) := w_0 s_1 w_1 \dots s_k w_k)$$

는 s_i 들의 선택지에 무관하게 항상 성립한다.

이제, $0 \leq k \leq n-1$ 및 $\{s_i : 1 \leq i \leq k\}$ 의 선택지를 하나 고정한 상태에서

$$\mathbb{P}_{s_{k+1} \sim S} \text{ 위의 Schottky-맞춤 균일 분포 } \left(\text{Len}(W_k s_{k+1} \mathcal{I}) \leq \frac{1}{\sqrt{N}} \text{Len}(W_k \mathcal{I}) \right) \geq 1 - \frac{1}{\sqrt{N}}$$

가 성립한다는 것은 보조정리 2.11에서 관찰했다. 다시 말해,

$$E_k := \left\{ (s_1, \dots, s_k) : \text{Len}(W_{k-1} s_k \mathcal{I}) \leq \frac{1}{\sqrt{N}} \text{Len}(W_{k-1} \mathcal{I}) \right\}$$

로 두었을 때 s_1, \dots, s_k 의 선택지에 무관하게 $\mathbb{P}(E_{k+1} | s_1, \dots, s_k) \geq 1 - 1/\sqrt{N}$ 이다. 이로부터

$$(2.5) \quad \{\text{eqn:ekSumEst}\} \quad \mathbb{P} \left(\sum_{k=1}^n 1_{E_k} \geq n/2 \right) \geq \mathbb{P} \left(B(n, 1 - 1/\sqrt{N}) \geq n/2 \right)$$

임을 알 수 있다. 여기서, $B(n, 1 - 1/\sqrt{N})$ 란 평균값이 $1 - 1/\sqrt{N}$ 이고 서로 독립인 Bernoulli 변수 n 개를 합한 이항확률변수를 얘기한다. 이 확률값을 어렵하기 위해 Markov 부등식을 이용하겠다. 즉

$$e^{-n/2} \cdot \mathbb{P} \left(B(n, 1 - 1/\sqrt{N}) \leq n/2 \right) \leq \mathbb{E} \left[e^{-B(n, 1 - 1/\sqrt{N})} \right] \leq \left(\frac{1}{\sqrt{N}} + e^{-1} \right)^n$$

를 관찰하겠다는 것이다. 여기서 $\sqrt{N} \geq 10$ 이라는 가정으로부터 $1/\sqrt{N} + e^{-1} \leq e^{-3/4}$ 를 얻는다. 이는 곧 $\mathbb{P} \left(B(n, 1 - 1/\sqrt{N}) \leq n/2 \right) \leq e^{-n/4}$ 를 의미하며, 부등식 2.5과 결합하면 증명이 끝난다. \square

이제 비슷한 것을 생각하자.

보조정리 2.13. 원 위의 두 점 $x, y \in S^1$, 위상동형사상 $w \in \text{Homeo}(S^1)$, 구간 I 를 중선으로 가지는 분해능 N 짜리 Schottky 집합 S 및 S 위의 Schottky-맞춤 균일 분포 μ 를 생각하자. 그러면

$$\mathbb{P}_{s \sim \mu} (\{x, y\} \cap s\mathcal{I} = \emptyset) \geq 1 - 2/N$$

이 성립한다.

Proof. 이번에도 $S = \{\mathfrak{G}(I_1, J_1), \dots, \mathfrak{G}(I_N, J_N)\}$ 꼴로 두겠다. 그러면 $\mathfrak{G}(I_i, J_i) \in S$ 의 임의의 원소 s 는 $\mathcal{I} \subseteq S^1 \setminus I_i$ 를 J_i 안으로 보낸다. 여기서 J_1, \dots, J_N 은 서로 겹치지 않는 구간들이므로, $\text{Ind} := \{i : \{x, y\} \cap J_i \neq \emptyset\}$ 을 정의하면 Ind 의 크기는 2 이하다. 이에

$$\mathbb{P}_{s \sim \mu} (\{x, y\} \cap I = \emptyset) \geq \mathbb{P}_{s \sim \mu} (s \in \mathfrak{G}(I_i, J_i) : i \notin \text{Ind}) \geq \frac{1}{N}(N - 2)$$

를 얻는다. \square

보조정리 2.14. 원 위의 두 점 $x, y \in S^1$, 구간 \mathcal{I} 를 중선으로 가지는 분해능 $N \geq 6$ 짜리 Schottky 집합 S 및 위상동형사상 $w_0, \dots, w_n \in \text{Homeo}(S^1)$ 을 고정하되, $i = 1, \dots, n$ 에 대해 $w_i \mathcal{I} \subseteq I$ 임을 가정하자. 그러면 서로 독립이면서 각각 S 위에서 Schottky-맞춤 균일 분포를 가지는 s_1, \dots, s_n 에 대해

$$\mathbb{P} (\{x, y\} \cap w_0 s_1 w_1 \cdots s_n w_n \mathcal{I} = \emptyset) \geq 1 - e^{-n}$$

이 성립한다.

Proof. 보조정리 2.12의 증명에서와 같이,

$$W_0 \mathcal{I} \supseteq W_0 s_1 \mathcal{I} \supseteq W_1 \mathcal{I} \supseteq W_1 s_1 \mathcal{I} \supseteq \dots \supseteq W_n \mathcal{I} \quad (W_k = W_k(s_0, \dots, s_k) := w_0 s_1 w_1 \dots s_k w_k)$$

는 s_i 의 선택지에 무관하게 성립한다. 또, $0 \leq k \leq n-1$ 및 $\{s_i : 1 \leq i \leq k\}$ 의 선택지를 고정했을 때

$$\mathbb{P}_{s_{k+1} \sim S} \text{ 위의 Schottky-맞춤 균일분포 } (s_{k+1} \mathcal{I} \cap \{W_k^{-1} x, W_k^{-1} y\} = \emptyset) \geq 1 - 2/N$$

가 성립한다는 것을 보조정리 2.13에서 관찰했다. 다시 말해,

$$E_k := \{(s_1, \dots, s_k) : \{x, y\} \cap W_{k-1}s_k\mathcal{I} = \emptyset\}$$

로 두면 s_1, \dots, s_k 의 선택지에 무관하게 $\mathbb{P}(E_{k+1}|s_1, \dots, s_k) \geq 1 - 2/N$ 이 성립한다. 이로부터

$$\mathbb{P}(\{x, y\} \cap W_n\mathcal{I} = \emptyset) \geq \mathbb{P}(E_1 \cup \dots \cup E_n) \geq 1 - (2/N)^n \geq 1 - e^{-n}$$

임을 알 수 있다. □

위 보조정리의 상황은 다음과 같이 해석할 수도 있다. 구간 \mathcal{I} 를 중선으로 가지는 분해능 $N \geq 6$ 짜리 Schottky 집합 $S = \{\mathfrak{S}(I_i, J_i) : i = 1, \dots, N\}$ 이 주어졌을 때, $\check{S} := \{\mathfrak{S}(J_i, I_i) : i = 1, \dots, N\}$ 는 구간 $S^1 \setminus \mathcal{I}$ 를 중선으로 가지는 Schottky 집합이 된다. 이제 S 위의 Schottky-맞춤 균일 분포 μ 를 생각하면, $\check{\mu}(\cdot) := \mu(\cdot^{-1})$ 로 정의된 확률 분포 $\check{\mu}$ 는 \check{S} 위의 Schottky-맞춤 균일 분포가 된다. 마지막으로, 위상동형사상 w_0, \dots, w_n 을 고정하면, 각 $i = 0, \dots, n-1$ 에 대해 $w_i \subseteq \mathcal{I}$ 임은 곧 $w_i^{-1}(S^1 \setminus \mathcal{I}) \subseteq (S^1 \setminus \mathcal{I})$ 임을 함의한다. 이제 보조정리 2.14를 적용하면 임의의 $x, y \in S^1$ 에 대해

$$\mathbb{P}_{s_i^{-1}} : \text{독립적으로 } \check{S} \text{ 위에 Schottky-맞춤 분포 } (\{x, y\} \cap w_n^{-1}s_n^{-1}w_{n-1}^{-1} \dots s_1^{-1}w_0^{-1}(S^1 \setminus \mathcal{I}) = \emptyset) \geq 1 - e^{-n}$$

가 성립한다. 이를 뒤집어 말하면,

$$\mathbb{P}_{s_i} : \text{독립적으로 } S \text{ 위에 Schottky-맞춤 분포 } (w_0s_1w_1 \dots s_nw_n \cdot \{x, y\} \subseteq \mathcal{I}) \geq 1 - e^{-n}$$

라는 것이다. 이를 따로 기록해 두겠다.

expShrink4.5}

보조정리 2.15. 원 위의 두 점 $x, y \in S^1$, 구간 \mathcal{I} 를 중선으로 가지는 분해능 $N \geq 6$ 짜리 Schottky 집합 S 및 위상동형사상 $w_0, \dots, w_n \in \text{Homeo}(S^1)$ 을 고정하되, 각 $i = 0, \dots, n-1$ 마다 $w_i\mathcal{I} \subseteq \mathcal{I}$ 임을 가정하자. 그러면 서로 독립이면서 각각 S 위에서 Schottky-맞춤 균일 분포를 가지는 s_1, \dots, s_n 에 대해

$$\mathbb{P}(w_0s_1w_1 \dots s_nw_n \cdot \{x, y\} \subseteq \mathcal{I}) \geq 1 - e^{-n}$$

이 성립한다.

이제, 다음을 증명할 수 있다.

n: expShrink}

정리 2.16. 임의의 양수 $\epsilon > 0$, 자연수 m 및 100보다 큰 자연수 N 이 주어졌을 때, 다음을 만족하는 $\kappa_1 = \kappa_1(\epsilon, m, N) > 0$ 이 존재한다. 구간 \mathcal{I} 를 중선으로 가지는 분해능 100짜리 Schottky 집합 S 및 $\text{Homeo}(S^1)$ 위의 확률 측도 μ 에 대해 μ^{*m} 이 (S, ϵ) -맞춤 측도임을 가정하자. 그러면 임의의 $x, y \in S^1$ 및 임의의 자연수 n 에 대해

$$\mathbb{P}_{Z_n \sim \mu^{*n}}(d(Z_nx, Z_ny) \leq e^{-\kappa_1 n}) \geq 1 - \frac{1}{\kappa_1} e^{-\kappa_1 n}$$

이 성립한다.

Proof. 먼저 명제 2.10에서 보장하는 $\kappa = \kappa(\epsilon, m, N)$ 을 기록해 두자. 이어서 자연수 n 을 고정했을 때, 명제 2.10에서 기술하는 대로 확률 공간 Ω_n , 가측 부분집합 A_n , A_n 의 가측 분할 $\mathcal{P}_n = \{\mathcal{E}_\alpha\}_\alpha$, 그리고 확률 변수들 $Z_n, w_0, \dots, w_{\lfloor \kappa n \rfloor}, s_1, \dots, s_{\lfloor \kappa n \rfloor}$ 을 잡을 수 있다.

이제 \mathcal{P}_n 안의 임의의 동치류 $\mathcal{E} \in \mathcal{P}_n$ 을 고정하자. \mathcal{E} 에 한정했을 때, $w_0, \dots, w_{\lfloor \kappa n \rfloor}$ 는 상수인 위상동형사상들이고 $s_1, \dots, s_{\lfloor \kappa n \rfloor}$ 은 S 위에서 Schottky-맞춤 균일분포를 가지는 독립변수들이다. 또한, $w_1, \dots, w_{\lfloor \kappa n \rfloor}$ 각각은 $w_i\mathcal{I} \subseteq \mathcal{I}$ 를 만족한다. 이 덕분에 보조정리 2.12 및 보조정리 2.15를 적용할 수 있다.

먼저 편의상 $w'_0 := w_0 s_1 w_1 \cdots s_{[0.5\kappa n]} w_{[0.5\kappa n]}$ 라는 확률변수를 정의하자. 이 위상동형사상은 $s_1, \dots, s_{[0.5\kappa n]}$ 의 선택지에 의존한다. 보조정리 2.12에 의해,

$$\mathbb{P}\left(\text{Len}(w'_0 \mathcal{I} = w_0 s_1 w_1 \cdots s_{[0.5\kappa n]} w_{[0.5\kappa n]} \cdot \mathcal{I}) \leq \frac{1}{N^{[\kappa n]/8}} \cdot 1 \mid \mathcal{E}\right) \geq 1 - e^{-n/4}$$

가 성립한다. 위에서 기술하는 사건은 $s_{[0.5\kappa n]+1}, \dots, s_{[\kappa n]}$ 를 이용하지 않음에 주목하라. 또한 보조정리 2.15에 의해 w'_0 의 선택지와 무관하게

$$\mathbb{P}\left(w'_0 s_{[0.5\kappa n]+1} w_{[0.5\kappa n]+1} \cdots s_{[\kappa n]} w_{[\kappa n]} \cdot \{x, y\} \subseteq w'_0 \mathcal{I} \mid \mathcal{E}, w'_0\right) \geq 1 - e^{-n}$$

이 성립한다. 이를 결합하면,

$$\mathbb{P}\left(d(Z_n x, Z_n y) \leq \text{Len}(w'_0 \cdot \mathcal{I}) \leq \frac{1}{N^{[\kappa n]/8}} \mid \mathcal{E}\right) \geq (1 - e^{-n/4})(1 - e^{-n}) \geq 1 - 2 \cdot e^{-n/4}$$

을 얻는다. 이 하한을 임의의 $\mathcal{E} \in \mathcal{P}_n$ 위에서 얻을 수 있으므로, 이를 종합하여

$$\begin{aligned} \mathbb{P}\left(d(Z_n x, Z_n y) \leq N^{-[\kappa n]/8}\right) &\geq \sum_{\mathcal{E} \in \mathcal{P}_n} \mathbb{P}(\mathcal{E}) \mathbb{P}\left(d(Z_n x, Z_n y) \leq N^{-[\kappa n]/8} \mid \mathcal{E}\right) \\ &\geq \sum_{\mathcal{E} \in \mathcal{P}_n} \mathbb{P}(\mathcal{E}) \cdot (1 - 2e^{-n/4}) \\ &= (1 - 2e^{-n/4}) \mathbb{P}(A_n) \geq (1 - 2e^{-n/4})(1 - e^{-\kappa n}) \end{aligned}$$

를 얻는다. □

이제 free group 향해.

보조정리 2.17. 4보다 큰 정수 N 을 고정하고 닫힌 구간 $2N$ 개 $I_1, \dots, I_N, J_1, \dots, J_N$ 를 생각하되, I_1, \dots, I_N 들끼리는 서로 겹치지 않으며 J_1, \dots, J_N 들끼리도 서로 겹치지 않는다고 가정하자. 그러면 임의의 위상동형사상 $g \in \text{Homeo}(S^1)$ 에 대해,

$$\#\{(i, j) \in \{1, \dots, N\}^2 : I_i \text{와 } gJ_j \text{가 겹침}\} \leq 3N\sqrt{N}$$

가 성립한다.

Proof. 먼저

$$\mathcal{C} = \mathcal{C}(g) := \{I_i : \#\{j : I_i \cap gJ_j \neq \emptyset\} \geq \sqrt{N}\}$$

을 정의하겠다. 특히, \mathcal{C} 의 각 원소는 $\{gJ_1, \dots, gJ_N\}$ 중 두 개 이상의 구간과 만나며, 특정 J_j 안에 완전히 포함되어 있을 수 없다. 이로부터 각각의 gJ_j 가 겹칠 수 있는 \mathcal{C} 의 원소는 최대 두 개임을 관찰할 수 있다. 즉,

$$\begin{aligned} 2N = 2\#\{gJ_j : j = 1, \dots, N\} &\geq 2\#\{gJ_j : gJ_j \text{가 } \mathcal{C} \text{의 어떤 원소와 겹침}\} \\ &\geq \#\{(I_i, gJ_i) : I_i \cap gJ_i \neq \emptyset, I_i \in \mathcal{C}\} \\ &\geq \#\mathcal{C} \cdot \min_{I_i \in \mathcal{C}} \#\{J_j : I_i \cap gJ_j \neq \emptyset\} \\ &\geq \#\mathcal{C}\sqrt{N} \end{aligned}$$

를 얻으며, \mathcal{C} 의 크기는 $2\sqrt{N}$ 보다 작다.

이제 $I_i \notin C$ 를 고정했을 때, I_i 와 겹치는 gJ_j 의 개수는 \sqrt{N} 이하이다. 이를 모두 종합하면,

$$\begin{aligned} \#\{(i, j) \in \{1, \dots, N\}^2 : I_i \text{와 } gJ_j \text{가 겹침}\} &\leq \#C \cdot N + (N - \#C) \cdot \sqrt{N} \\ &\leq 2N\sqrt{N} + N\sqrt{N} = 3N\sqrt{N} \end{aligned}$$

을 얻기에 증명이 끝난다. \square

보조정리 2.18. 구간 \mathcal{I} 및 \mathcal{I}' 를 각각 중선으로 가지는 분해능 $N \geq 4$ 짜리 Schottky 집합들 S 및 S' 를 생각하자. 또, 서로 독립이면서 각각 S 및 S' 위에서 Schottky-맞춤 균일 분포를 가지는 확률변수 s 및 s' 를 생각하자. 그러면 임의의 위상동형사상 $g \in \text{Homeo}(S^1)$ 에 대해,

$$\mathbb{P}(s'gs\bar{\mathcal{I}} \subseteq \text{int } \mathcal{I}') \geq 1 - 3/\sqrt{N}$$

가 성립한다.

Proof. 여느 때와 같이 $S = \{\mathfrak{G}(I_1, J_1), \dots, \mathfrak{G}(I_N, J_N)\}$ 및 $S' = \{\mathfrak{G}(I'_1, J'_1), \dots, \mathfrak{G}(I'_N, J'_N)\}$ 로 두자. 그러면 $S(I'_i, J'_i) \in S'$ 의 임의의 원소 s' 의 역원 s'^{-1} 는 $S^1 \setminus \mathcal{I}'$ 를 I'_i 안으로 보내고, $S(I_j, J_j) \in S$ 의 임의의 원소 s 는 $\bar{\mathcal{I}}$ 를 J_i 안으로 보낸다. 이제,

$$\text{Ind} := \{(i, j) : I'_i \text{와 } gJ_j \text{가 겹침}\}$$

를 잡으면 그 크기는 $3N\sqrt{N}$ 이하이다. 또한, $(i, j) \notin \text{Ind}$ 인 경우 임의의 $s \in \mathfrak{G}(I_i, J_i)$ 및 $s' \in \mathfrak{G}(I'_j, J'_j)$ 를 잡으면,

$$gs\bar{\mathcal{I}} \subseteq gJ_j \subseteq S^1 \setminus I'_i \subseteq s'^{-1} \text{int } \mathcal{I}'$$

가 성립한다. 이를 종합하면

$$\mathbb{P}(s'gs\bar{\mathcal{I}} \subseteq \text{int } \mathcal{I}') \geq \mathbb{P}(s \in \mathfrak{G}(I_i, J_i), s' \in \mathfrak{G}(I'_j, J'_j) : (i, j) \notin \text{Ind}) \geq 1 - 3/\sqrt{N}$$

를 얻는다. \square

보조정리 2.19. 구간 \mathcal{I} 및 \mathcal{I}' 를 각각 중선으로 가지는 분해능 $N \geq 100$ 짜리 Schottky 집합들 S 및 S' 를 생각하자. 또, $i = 1, \dots, n$ 마다 S 위에서 Schottky-맞춤 균일 분포를 가지는 확률변수 s_i 및 S' 위에서 Schottky-맞춤 균일 분포를 가지는 확률변수 s_{-i} 를 생각하되, $\{s_i : 1 \leq |i| \leq n\}$ 는 모두 독립이라고 가정하자. 더하여 위상동형사상 $\{w_i : -n \leq i \leq n\}$ 을 고정하되, $1 \leq i \leq n$ 일 때 $w_i\mathcal{I} \subseteq \mathcal{I}$ 및 $w_{-i}\mathcal{I}' \subseteq \mathcal{I}'$ 임을 가정하자. 그러면

$$\mathbb{P}(w_{-n}s_{-n} \cdots w_{-1}s_{-1} \cdot w_0 \cdot s_1w_1 \cdots s_nw_n \cdot \bar{\mathcal{I}} \subseteq \text{int } \mathcal{I}') \geq 1 - e^{-n}$$

이 성립한다.

Proof. 먼저 W_0 는 항등사상으로 둔 뒤, $W_k := s_1w_1 \cdots s_kw_k$ 및 $W_{-k} := w_{-k}s_{-k} \cdots w_{-1}s_{-1}$ 를 정의하겠다. 그러면

$$\begin{aligned} W_0\mathcal{I} &\supseteq W_0s_1\mathcal{I} \supseteq W_1\mathcal{I} \supseteq W_1s_2\mathcal{I} \supseteq \dots \supseteq W_n\mathcal{I}, \\ W_0^{-1}\mathcal{I}' &\subseteq (s_{-1}^{-1}W_0)^{-1}\mathcal{I}' \subseteq W_{-1}^{-1}\mathcal{I}' \subseteq (s_{-2}^{-1}W_{-1})^{-1}\mathcal{I}' \subseteq W_{-2}^{-1}\mathcal{I}' \subseteq \dots \subseteq W_{-n}^{-1}\mathcal{I}' \end{aligned}$$

는 s_i 의 선택지에 무관하게 성립한다. 또,

$$E_k := \{(s_{-k}, \dots, s_{-1}, s_1, \dots, s_k) : (s_{-k}W_{-(k-1)})^{-1} \text{int } \mathcal{I}' \supseteq W_{k-1}s_k\bar{\mathcal{I}}\}$$

를 정의하면, 보조정리 2.18에 의해 s_{-k}, \dots, s_k 의 선택지에 무관하게

$$\mathbb{P}(E_{k+1} \mid s_{-k}, \dots, s_k) \geq 1 - 3/\sqrt{N} \geq 1 - 1/e$$

가 성립한다. 그러면

$$\mathbb{P}(W_n \bar{I} \subseteq W_{-n}^{-1} \text{int } \mathcal{I}') \geq \mathbb{P}(E_1 \cup \dots \cup E_n) \geq 1 - (1/e)^n \geq 1 - e^{-n}$$

임을 알 수 있다. □

정리 2.20. 구간 \mathcal{I} 및 \mathcal{I}' 를 각각 중선으로 가지는 분해능 $N \geq 100$ 짜리 Schottky 집합들 S 및 S' 를 생각하자. 또, $i = 1, \dots, 2n - 1$ 에 대해 $w_i \mathcal{I} \subseteq \mathcal{I}$ 및 $v_i \mathcal{I}' \subseteq \mathcal{I}'$ 가 성립하게끔 위상동형사상 $w_0, v_0, w_1, v_1, \dots, w_{2n}, v_{2n} \in \text{Homeo}(S^1)$ 을 고정하자. 이제 S 위에서 Schottky-맞춤 균일 분포를 가지는 확률변수 s_1, \dots, s_{4n} 및 S' 위에서 Schottky-맞춤 균일 분포를 가지는 확률변수 t_1, \dots, t_{4n} 를 모두 독립적으로 잡자. 그러면

$$\mathbb{P} \left(\begin{array}{c} w_0 s_1 w_1 \cdots s_{2n} w_{2n} \text{과 } v_0 t_1 v_1 \cdots t_{4n} v_{4n} \text{는} \\ \text{Schottky 순서쌍을 이루며 자유 부분군을 생성함} \end{array} \right) \geq 1 - 6e^{-n/10}$$

이 성립한다.

Proof. 다음 사건들을 정의하자.

$$\begin{aligned} E_1 &:= \{s_{n+1} w_{n+1} \cdots s_{2n} w_{2n} \cdot w_0 s_1 w_1 \cdots s_n w_n \bar{\mathcal{I}} \subseteq \text{int } \mathcal{I}\}, \\ E_2 &:= \{t_{n+1} v_{n+1} \cdots t_{2n} v_{2n} \cdot v_0 t_1 v_1 \cdots t_n v_n \bar{\mathcal{I}}' \subseteq \text{int } \mathcal{I}'\}, \\ E_3 &:= \{s_{n+1} w_{n+1} \cdots s_{2n} w_{2n} \cdot v_0 t_1 v_1 \cdots t_n v_n \bar{\mathcal{I}}' \subseteq \text{int } \mathcal{I}\}, \\ E_4 &:= \{t_{n+1} v_{n+1} \cdots t_{2n} v_{2n} \cdot w_0 s_1 w_1 \cdots s_n w_n \bar{\mathcal{I}} \subseteq \text{int } \mathcal{I}'\}, \\ E_5 &:= \{s_{n+1} w_{n+1} \cdots s_{2n} w_{2n} \cdot v_{2n}^{-1} t_{2n}^{-1} \cdots v_{n+1}^{-1} t_{n+1}^{-1} \cdot \overline{S^1 \setminus \mathcal{I}'} \subseteq \text{int } \mathcal{I}\}, \\ E_6 &:= \{v_n^{-1} t_n^{-1} \cdots v_1^{-1} t_1^{-1} v_0^{-1} \cdot w_0 s_1 w_1 \cdots s_n w_n \cdot \bar{\mathcal{I}} \subseteq \text{int}(S^1 \setminus \mathcal{I}')\}. \end{aligned}$$

첫번째 사건을 먼저 들여다보겠다. 이 경우 s_i 들은 모두 S 위에서 Schottky-맞춤 균일 분포를 가지는 독립 확률변수들이고, S 는 \mathcal{I} 를 중선으로 가지며 $i \neq 0, 2n$ 에 대해 $w_i \mathcal{I} \subseteq \mathcal{I}$ 가 성립함을 관찰할 수 있다. (여기서 $w_{2n} \cdot w_0$ 는 \mathcal{I} 를 중첩시키는 역할을 하지 않음에 주의하라.) 그러면 보조정리 2.19에 의해 $\mathbb{P}(E_1) \geq 1 - e^{-n}$ 이 성립한다. 비슷한 이유로, E_2, E_3 및 E_4 의 확률 또한 각각 $1 - e^{-n}$ 이상이다.

다섯 번째 사건을 들여다보기 전에, $S' := \mathfrak{S}(I'_1, J'_1) \cup \dots \cup \mathfrak{S}(I'_N, J'_N)$ 를 거꾸로 뒤집은 Schottky 집합 $\check{S} := \mathfrak{S}(J'_1, I'_1) \cup \dots \cup \mathfrak{S}(J'_N, I'_N)$ 을 기록해 두겠다. 그러면 s_i 들은 모두 S 위에서 Schottky-맞춤 균일 분포를 가지는 독립 확률변수들이고, t_i^{-1} 들은 \check{S}' 위에서 Schottky-맞춤 균일 분포를 가지는 독립 확률변수들이다. 또한 S 는 \mathcal{I} 를 중선으로 가지며 각 i 마다 $w_i \mathcal{I} \subseteq \mathcal{I}$ 가 성립하는 반면, \check{S}' 는 $S^1 \setminus \mathcal{I}'$ 를 중선으로 가지며 각 i 마다 $v_i^{-1}(S^1 \setminus \mathcal{I}') \subseteq (S^1 \setminus \mathcal{I}')$ 가 성립한다. 이제 보조정리 2.19을 적용하면 $\mathbb{P}(E_5) \geq 1 - e^{-n}$ 가 성립한다. 비슷한 이유로 E_6 의 확률 또한 $1 - e^{-n}$ 이상이다.

이제 사건 $E_1 \cup E_2 \cup E_3 \cup E_4 \cup E_5 \cup E_6$ 위에서 구간들

$$\begin{aligned} I^{(1)} &:= (s_{n+1} w_{n+1} \cdots s_{2n} w_{2n})^{-1} (S^1 \setminus \text{int } \mathcal{I}), \\ I^{(2)} &:= (t_{n+1} v_{n+1} \cdots t_{2n} v_{2n})^{-1} \cdot (S^1 \setminus \text{int } \mathcal{I}'), \\ J^{(1)} &:= w_0 s_1 w_1 \cdots s_n w_n \bar{\mathcal{I}}, \\ J^{(2)} &:= v_0 t_1 v_1 \cdots t_n v_n \bar{\mathcal{I}}' \end{aligned}$$

의 위치 관계를 파악하겠다. 먼저 사건 E_1 의 정의에 따라 $I^{(1)}$ 과 $J^{(1)}$ 은 서로 겹치지 않는다. 또 사건 E_2 의 정의에 따라 $I^{(2)}$ 과 $J^{(2)}$ 은 서로 겹치지 않는다. 한편 E_3 의 정의에 따라 $I^{(1)}$ 과 $J^{(2)}$ 도 겹치지 않고, E_4 의 정의에 따라 $I^{(2)}$ 와 $J^{(1)}$ 도 겹치지 않는다. 이제 E_5 의 정의를 들여다보면 $I^{(1)}$ 과 $I^{(2)}$ 가 겹치지 않음을 알 수 있고, E_6 의 정의에 따라 $J^{(1)}$ 과 $J^{(2)}$ 도 겹치지 않는다. 즉 사건 $\cup_{k=1}^6 E_k$ 안에서 위 네 구간은 겹치지 않는다. 또 $w_0 s_1 w_1 \cdots s_{2n} w_{2n}$ 은 $S^1 \setminus I^{(1)}$ 을 정확히 $\text{int } J^{(1)}$ 로 보내고, $v_0 t_1 v_1 \cdots t_{2n} v_{2n}$ 은 $S^1 \setminus I^{(2)}$ 을 정확히 $\text{int } J^{(2)}$ 로 보낸다.

이들 모두 종합하면, 사건 $\cup_{k=1}^6 E_k$ 안에서 $w_0 s_1 w_1 \cdots s_{2n} w_{2n}$ 과 $v_0 t_1 v_1 \cdots t_{2n} v_{2n}$ 는 $I^{(1)}, I^{(2)}, J^{(1)}, J^{(2)}$ 에 결부된 Schottky 순서쌍을 이루며 따라서 $\text{Homeo}(S^1)$ 의 (차수 2짜리) 자유 부분군을 생성한다. 각 k 에 대해 $\mathbb{P}(E_k^c) \leq e^{-n}$ 이므로, $\cup_{k=1}^6 E_k$ 의 확률은 최소 $1 - 6e^{-n}$ 이다. 이로써 증명이 끝난다. \square

이제 정리 2.16의 증명에서와 같이, 명제 2.10에서 보장하는 확률 공간 및 가측 분할을 이용하면 정리 2.20로부터 다음을 이끌어낼 수 있다.

정리 2.21. 임의의 양수 $\epsilon > 0$, 자연수 m 및 100보다 큰 자연수 N 이 주어졌을 때, 다음을 만족하는 $\kappa_2 = \kappa_2(\epsilon, m, N) > 0$ 이 존재한다.

중선 달린 분해능 N 짜리 Schottky 집합 S 및 S' 를 생각한 뒤, $\text{Homeo}(S^1)$ 위의 확률 측도 μ 및 μ' 에 대해, μ^{*m} 이 (S, ϵ) -맞춤 측도이고 μ'^{*m} 이 (S', ϵ') -맞춤 측도임을 가정하자. 그러면 임의의 자연수 n 에 대해

$$\mathbb{P}_{(Z_n, Z'_n) \sim \mu^{*n} \times \mu'^{*n}} (Z_n, Z'_n \text{는 Schottky 순서쌍을 이루며 자유 부분군을 생성함}) \geq 1 - \frac{1}{\kappa_2} e^{-\kappa_2 n}$$

이 성립한다.

2.2. 국소적인 축약 정리 A 및 정리 D는 특정 시점에서의 무작위 행보의 순간적인 배치를 기록한 것이다. 그에 반해, 정리 C는 $x \in S^1$ 및 확률공간의 샘플 ω 라는 입력값을 바탕으로, 모든 시점에 잘 작동하는 $I_{x, \omega}$ 가 존재하는지를 묻고 있다. 이를 구현하기 위해서는 각 n 마다 n -단계 위치 변수 Z_n 가 μ^{*n} 로 분포되어 있다는 사실만으로는 충분하지 않고, $(Z_n)_{n>0}$ 전체의 공동 분포가 어떻게 생겼는지가 필요하다. 실제로, 정리 C의 결과는 원 무작위 행보에 대해서만 성립하고 오른 무작위 행보에 대해서는 성립하지 않는다.

정리 C의 증명 증명을 시작하기에 앞서, 입력값 ϵ, m 및 N 에 대해 명제 2.10가 보장하는 상수 κ 를 잡자. 표기상의 편의를 위해 $1/\kappa \in \mathbb{Z}_{>0}$ 임을 가정하겠다. 그러면 n 이 $100/\kappa$ 의 배수일 때만 증명해도 충분하기에, 앞으로는 $100/\kappa | n$ 를 가정하겠다.

이제 독립적으로 μ -분포를 따르는 스텝 확률변수 g_i 들을 갖춘 확률공간

$$\Omega := (G^{\mathbb{Z}_{>0}}, \mu^{\mathbb{Z}_{>0}})$$

을 고정하겠다. 이 증명에서는 원 무작위 행보를 생각한다. 즉, $Z_i := g_i \cdots g_1$ 와 같이 정의된다.

이제 Ω 를 다음과 같은 곱 형태로 나타낼 수 있다:

$$\cdots \times \Omega_3 \times \Omega_2 \times \Omega_1 =: \Omega.$$

여기서 각 $k > 0$ 에 대해, Ω_k 는 좌표 $(g_{n(2^k-1)}, g_{n(2^k-1)-1}, \dots, g_{n(2^{k-1}-1)+1})$ 들을 표현하는 공간이다. 이때

$$g_{n(2^k-1)} \cdots g_{n(2^{k-1}-1)+l} = Z_{n(2^k-1)} \cdot Z_{n(2^{k-1}-1)+l}^{-1} \quad (l = 0, \dots, n2^{k-1} - 1).$$

라는 관계식이 성립함을 유의하라.

이제 명제 2.10를 각각의 Ω_k 에 적용하겠다. 그러면 Ω_k 는 가측 부분집합 $A^{(k)}$, $A^{(k)}$ 위의 가측 분할 $\mathcal{P}^{(k)} = \{\mathcal{E}_\alpha^{(k)}\}_\alpha$, 그리고 확률 변수

$$\{w_i^{(k)}\}_{i=0, \dots, \kappa n 2^{k-1}}, \{s_i^{(k)}\}_{i=1, \dots, \kappa n 2^{k-1}}$$

를 갖추게 되는데, 이들은 다음을 만족한다:

- (1) $\mathbb{P}(A^{(k)}) \geq 1 - \frac{1}{\kappa} e^{-\kappa \cdot 2^{k-1}}$.
- (2) 각각의 동치류 $\mathcal{E} \in \mathcal{P}_k$ 에 제한해서 생각했을 때, $w_0^{(k)}, \dots, w_{\kappa 2^{k-1}}^{(k)}$ 는 상수인 위상동형사상들이고 $s_i^{(k)}$ 들은 독립적으로 S 위에 Schottky-맞춤 균일하게 분포되어 있다.
- (3) $A^{(k)}$ 위에서, 각 $i = 1, \dots, \kappa 2^{k-1} - 1$ 마다 $w_i^{(k)} \mathcal{I} \subseteq \mathcal{I}$ 가 성립한다;
- (4) 각 $\omega \in A^{(k)}$ 마다

$$(2.6) \quad \begin{aligned} \{ \text{eqn:gnProd} \} \quad w_0^{(k)}(\omega) s_1^{(k)}(\omega) \cdots s_{\kappa 2^{k-1}}^{(k)}(\omega) w_{\kappa 2^{k-1}}^{(k)}(\omega) &= g_{n(2^k-1)}(\omega) g_{n(2^k-1)-1}(\omega) \cdots g_{n(2^{k-1}-1)+1}(\omega) \\ &= Z_{n(2^k-1)}(\omega) \cdot Z_{n(2^{k-1}-1)}^{-1}(\omega) \end{aligned}$$

가 성립한다.

여기서 서로 다른 k 에 대해 그에 딸린 분할들 $\mathcal{P}^{(k)}$ 은 서로 독립적이다.

이제 사건

$$F_k := \left\{ \omega : s_{0.9\kappa n 2^{k+1}}^{(k+1)} w_{0.9\kappa n 2^{k+1}}^{(k+1)} \cdots s_{\kappa n 2^k}^{(k+1)} w_{\kappa n 2^k}^{(k+1)} \cdot w_0^{(k)} s_1^{(k)} w_1^{(k)} \cdots s_{0.1\kappa n 2^{k-1}}^{(k)} w_{0.1\kappa n 2^{k-1}}^{(k)} \mathcal{I} \subseteq \mathcal{I} \right\}$$

를 정의하겠다. 각각의 $\mathcal{E}' \in \mathcal{P}^{(k+1)}$ 및 $\mathcal{E} \in \mathcal{P}^{(k)}$ 마다, $\mathcal{E}' \times \mathcal{E}$ 위에서 F_k 의 조건부 확률은 최소 $1 - e^{-0.1\kappa 2^{k-1}}$ 라는 것을 보조정리 2.19에서 확인했다. 또, 전체공간 안에서 $A^{(k+1)} \times A^{(k)}$ 의 확률은 $1 - \frac{2}{\kappa} e^{-\kappa 2^{k-1}}$ 이상이다. 이제 각 동치류 순서쌍 위에서의 조건부 확률을 모두 더하면

$$\mathbb{P}(F_k) \geq 1 - (2/\kappa + 1)e^{-0.1\kappa n 2^{k-1}} \quad (k = 1, 2, \dots)$$

임을 얻는다.

다음으로, 각 $k \geq 1$ 및 $n(2^k - 1) < t \leq n(2^{k+1} - 1)$ 에 대해

$$End_t := \left\{ \text{Len} \left(Z_t Z_{n(2^k-1)}^{-1} \cdot w_0^{(k)} s_1^{(k)} w_1^{(k)} \cdots s_{0.5\kappa n 2^{k-1}}^{(k)} w_{0.5\kappa n 2^{k-1}}^{(k)} \cdot \mathcal{I} \right) \leq \frac{1}{e^{0.01\kappa t}} \right\}$$

를 정의하겠다. 그러면 $(g_{n(2^{k+1}-1)}, \dots, g_{n(2^k-1)+1}) \in \Omega_{k+1}$ 및 $\mathcal{E} \in \mathcal{P}^{(k)}$ 의 선택지가 주어질 때마다, $Z_t Z_{n(2^k-1)}^{-1}$ 및 $w_0^{(k)}, w_1^{(k)}, \dots$ 는 상수로 고정되는 반면 $s_1^{(k)}, s_2^{(k)}, \dots$ 는 독립적으로 S 위에 Schottky-맞춤 균일하게 분포된다. 이제 보조정리 2.12에 따르면 $\mathbb{P}(End_t | g_{n(2^{k+1}-1)}, \dots, g_{n(2^k-1)+1}, \mathcal{E}) \geq 1 - e^{-0.01\kappa t}$ 가 성립한다. 이제 확률 $1 - \frac{1}{\kappa} e^{-\kappa 2^{k-1}}$ 이상인 $\Omega_{k+1} \times A^{(k)}$ 안에서 다양한 동치류 상의 조건부 확률을 합하면,

$$\mathbb{P}(End_t) \geq 1 - (1/\kappa + 1)e^{-0.01\kappa t} \quad (t = n, n+1, n+2, \dots)$$

를 얻는다.

이제 다음을 주장하겠다:

주장 2.22. $(\cup_{k=1}^\infty F_k) \cap (\cup_{t=n}^\infty End_t)$ 안의 샘플 ω 를 하나 고정하자. 그러면 각각의 $t \geq n$ 및

$$I \subseteq (s_{0.5\kappa n+1}^{(1)} w_{0.5\kappa n+1}^{(1)} \cdots s_{\kappa n}^{(1)} w_{\kappa n}^{(1)})^{-1} \cdot \mathcal{I}$$

를 만족하는 임의의 구간 I 에 대해, $\text{Len}(Z_t I) \leq e^{-0.01\kappa t}$ 가 성립한다.

이를 증명하기 위해 $t \geq n$ 를 하나 정한 뒤, $n(2^k - 1) \leq t \leq n(2^{k+1} - 1)$ 이게끔 하는 $k \geq 1$ 를 생각하자. 만약 $k = 1$ 라면, 정의상

$$Z_{n(2^k-1)}^{-1} \cdot w_0^{(k)} s_1^{(k)} w_1^{(k)} \cdots s_{0.5\kappa n 2^{k-1}}^{(k)} w_{0.5\kappa n 2^{k-1}}^{(k)} = (s_{0.5\kappa+1}^{(1)} w_{0.5\kappa n+1}^{(1)} \cdots s_{\kappa n}^{(1)} w_{\kappa n}^{(1)})^{-1}$$

라는 사실과 $\omega \in \text{End}_t$ 라는 사실로부터 주장을 바로 얻는다. 만약 k 가 1보다 크다면,

$$\begin{aligned} & Z_t Z_{n(2^k-1)}^{-1} \cdot w_0^{(k)} s_1^{(k)} w_1^{(k)} \cdots s_{0.5\kappa n 2^{k-1}}^{(k)} w_{0.5\kappa n 2^{k-1}}^{(k)} \cdot \mathcal{I} \\ & \supseteq Z_t Z_{n(2^k-1)}^{-1} \cdot w_0^{(k)} s_1^{(k)} w_1^{(k)} \cdots s_{0.9\kappa n 2^{k-1}-1}^{(k)} w_{0.9\kappa n 2^{k-1}-1}^{(k)} \cdot \mathcal{I} \\ & \supseteq Z_t Z_{n(2^k-1)}^{-1} \cdot w_0^{(k)} s_1^{(k)} w_1^{(k)} \cdots s_{0.9\kappa n 2^{k-1}-1}^{(k)} w_{0.9\kappa n 2^{k-1}-1}^{(k)} \cdot \\ & \quad s_{0.9\kappa n 2^{k-1}}^{(k)} w_{0.9\kappa n 2^{k-1}}^{(k)} \cdots s_{\kappa n 2^{k-1}}^{(k)} w_{\kappa n 2^{k-1}}^{(k)} \cdot w_0^{(k-1)} s_1^{(k-1)} w_1^{(k-1)} \cdots s_{0.1\kappa n 2^{k-2}}^{(k-1)} w_{0.1\kappa n 2^{k-2}}^{(k-1)} \mathcal{I} \\ & = Z_t \cdot Z_{n(2^{k-1}-1)}^{-1} \cdot w_0^{(k-1)} s_1^{(k-1)} w_1^{(k-1)} \cdots s_{0.1\kappa n 2^{k-2}}^{(k-1)} w_{0.1\kappa n 2^{k-2}}^{(k-1)} \mathcal{I}. \end{aligned}$$

임에 주목하겠다. 여기서 첫 포함관계는 임의의 $s \in S$ 및 $w_i^{(j)}$ 에 대해 $s\mathcal{I} \subseteq \mathcal{I}$ 및 $w_i^{(k)}\mathcal{I} \subseteq \mathcal{I}$ 가 성립하기 때문이다. 두번째 포함관계는 $\omega \in F_{k-1}$ 에 의거하며, 세번째 등호는 등식 2.6 때문이다.

이러한 방식으로 계속 포함 관계를 읽어 나가면, $0.1\kappa n$ 과 $\kappa n - 1$ 사이의 임의의 l 에 대해

$$Z_t \cdot Z_0^{-1} \cdot w_0^{(1)} s_1^{(1)} w_1^{(1)} \cdots s_l^{(1)} w_l^{(2)}$$

가 성립함을 알 수 있다. 여기서도 $s\mathcal{I} \subseteq \mathcal{I}$ 및 $w_i^{(1)}\mathcal{I} \subseteq \mathcal{I}$ 라는 포함관계가 사용된다. 위 등식을 $l = 0.5\kappa n$ 에서 관찰하면 주장을 얻는다.

마지막으로, 다음 집합의 확률을 계산해 보자:

$$Dec := \left\{ \begin{array}{l} \text{Len} \left((s_{0.5\kappa n+1}^{(1)} w_{0.5\kappa n+1}^{(1)} \cdots s_{\kappa n}^{(1)} w_{\kappa n}^{(1)})^{-1} \cdot \mathcal{I} \right) \\ = 1 - \text{Len} \left((w_{\kappa n}^{(1)})^{-1} (s_{\kappa n}^{(1)})^{-1} \cdots (w_{0.5\kappa n+1}^{(1)})^{-1} (s_{0.5\kappa n+1}^{(1)})^{-1} \cdot (S^1 \setminus \mathcal{I}) \right) \\ \geq 1 - 0.01^{n/4} \end{array} \right\}.$$

여기서, S 를 뒤집은 버전인 \check{S} 위에 각 $(s_i^{(1)})^{-1}$ 들이 독립적으로 Schottky-맞춤 균일하게 분포되어 있으며, $S^1 \setminus \mathcal{I}$ 이 \check{S} 의 중선 역할을 함을 상기하라. 또한, 각 $i \neq 0, \kappa n$ 에 대해 $(w_i^{(1)})^{-1}(S^1 \setminus \mathcal{I})$ 가 성립한다. 따라서 보조정리 2.12를 적용할 수 있고 $\mathbb{P}(Dec) \geq 1 - e^{-n/4}$ 임이 따라 나온다.

요약하자면, 우리는 $(\cup_{k=1}^{\infty} F_k) \cap (\cup_{t=n}^{\infty} \text{End}_t) \cap Dec$ 라는 집합을 건설했다. 이 집합의 여집합은 n 에 대해 지수함수적으로 감소하는 확률값을 가진다. 또, 집합 안에서 샘플 ω 가 주어졌을 때, n 이후 단계에서는 지수함수적으로 축약되면서 길이는 최소 $1 - 0.01^{n/4}$ 인 구간을 반드시 잡을 수 있다. 이로써 정리 C의 증명이 끝난다. \square

3. 증추 전환 기법(PIVOTING TECHNIQUE)

먼저 다음을 관찰하자.

보조정리 3.1. 임의의 양수 $\epsilon > 0$ 및 자연수 m 이 주어졌을 때 다음을 만족하는 $\kappa = \kappa(\epsilon, m, N)$ 이 존재한다.

어떤 Schottky 집합 S 및 $\text{Homeo}(S^1)$ 위의 확률 측도 μ 에 대해, μ^{*m} 이 (S, ϵ) -맞춤 측도임을 가정하자. 그러면 각 자연수 n 에 대해 어떤 확률 공간 Ω_n , 가측 부분집합 $A_n \subseteq \Omega_n$, A_n 의 가측 분할 $\mathcal{P}_n = \{\mathcal{E}_\alpha\}_\alpha$, 그리고 $\text{Homeo}(S^1)$ 의 원소들을 값으로 가지는 확률변수들 $Z_n, \{w_i\}_{i=0, \dots, [\kappa n]}, \{r_i, s_i, t_i\}_{i=1, \dots, [\kappa n]}$ 이 존재하여 다음을 만족한다.

$$(1) \mathbb{P}(A_n) \geq 1 - \frac{1}{\kappa} e^{-\kappa n}.$$

(2) \mathcal{P}_n 을 이루는 각 동치류 $\mathcal{E} \in \mathcal{P}_n$ 에 한정해서 보았을 때, $w_0, \dots, w_{\lfloor \kappa n \rfloor}$ 는 각각 고정된 위상동형 사상들이고, r_i, s_i, t_i 들은 각각 S 위에서 Schottky 맞춤 균일분포를 가지는 독립인 확률변수들이다.

(3) Z_n 는 μ^{*n} 의 분포를 따르며, A_n 위에서 $Z_n = w_0 r_1 s_1 t_1 w_1 \cdots r_{\lfloor \kappa n \rfloor} s_{\lfloor \kappa n \rfloor} t_{\lfloor \kappa n \rfloor} w_{\lfloor \kappa n \rfloor}$ 이다.

Proof. 이 명제를 $3m$ 의 정수 배수인 n 들에 대해서만 증명해도 충분하다. 실제로 $n = 3mk + l$ ($1 \leq l \leq 3m - 1$) 꼴인 정수에 대해서는 다음과 같이 다루면 된다. 먼저 $n = 3mk$ 에 대해 Ω_{3mk} , \mathcal{P}_{3mk} , $(w_i)_i, (r_i, s_i, t_i)_i$ 를 잡은 뒤, $G = \text{Homeo}(S^1)$ 에 대해 (G^l, μ^l) 라는 확률공간을 생각한다. 그러면

$$\Omega_{3mk+l} := \Omega_{3mk} \times G^l,$$

$$\mathcal{P}_{3mk+l} := \mathcal{P}_{3mk} \times G^l = \{\mathcal{E}_\alpha \times (g_1, \dots, g_l) : \mathcal{E}_\alpha \in \mathcal{P}_{3mk}, (g_1, \dots, g_l) \in G^l\}$$

를 정의할 수 있다. 그 후 $(w_i)_i, (r_i, s_i, t_i)_i$ 는 모두 그대로 두되 $w_{\lfloor \kappa n \rfloor}$ 만 $w_{\lfloor \kappa n \rfloor} \cdot g_1 \cdots g_l$ 로 새로 정의하면, 요구하는 성질을 모두 만족할 수 있다.

가정에 의해 μ^{*m} 이 (S, ϵ) -맞춤 측도이므로, S 위에 Schottky-맞춤 균일한 분포를 가지는 적당한 확률 측도 μ_S 및 또다른 $\text{Homeo}(S^1)$ 상의 확률 측도 ν 을 잡아

$$\mu^{*3m} = \epsilon^3 \mu_S^{*3} + (1 - \epsilon^3) \nu$$

꼴로 나타낼 수 있다. 이제 평균 ϵ 짜리 Bernoulli 확률변수 $(\rho_i)_{i=0}^\infty$, μ_S 를 분포로 가지는 확률변수 $(\eta_i^{(1)})_{i=1}^\infty, (\eta_i^{(2)})_{i=1}^\infty$ 및 $(\eta_i^{(3)})_{i=1}^\infty$, ν 를 분포로 가지는 확률변수 $(\nu_i)_{i=1}^\infty$ 를 모두 독립적으로 잡은 뒤

$$\rho_i = 1 \text{ 일 때 } g_i := \eta_i^{(1)} \cdot \eta_i^{(2)} \cdot \eta_i^{(3)}, \quad \rho_i = 0 \text{ 일 때 } g_i = \nu_i$$

라는 규칙으로 g_i 를 정의하면, g_1, g_2, \dots 는 모두 μ^{*3m} 를 분포로 가지는 독립변수가 된다. 이제

$$\{i(1) < i(2) < \dots\} := \{1 \leq i \leq n : \rho_i = 1\}, \quad N := \#\{1 \leq i \leq n : \rho_i = 1\}$$

로 두면 Markov 부등식에 의해

$$e^{-\epsilon n/10m} \cdot \mathbb{P}(N \leq \epsilon n/10m) \leq \mathbb{E} \left[e^{-B(n/3m, \epsilon)} \right] \leq (1 - \epsilon(1 - e^{-1}))^{n/3m} \leq (1 - 0.6\epsilon)^{n/3m} \leq e^{-0.6\epsilon n/3m}$$

가 성립하고, 따라서 N 이 $\epsilon n/10m$ 보다 작을 확률은 $e^{-\epsilon n/10m}$ 이하이다. 이제 $\{N \geq \epsilon n/10m\}$ 위에서

$$w_0 := \prod_{i=1}^{i(1)-1} g_i = \nu_1 \cdots \nu_{i(1)-1},$$

$$w_l := \prod_{i=i(l)+1}^{i(l+1)-1} g_i = \nu_{i(l)+1} \cdots \nu_{i(l+1)-1} \quad (l = 1, \dots, \lfloor \epsilon n/10m \rfloor - 1)$$

$$w_{\lfloor \epsilon n/10m \rfloor} := \prod_{i=i(\lfloor \epsilon n/10m \rfloor)+1}^{n/3m} g_i = \nu_{i(\lfloor \epsilon n/10m \rfloor)+1} \cdots \nu_{n/3m}$$

로 두고 각 $l = 1, \dots, \lfloor \epsilon n/10m \rfloor$ 에 대해 $(r_l, s_l, t_l) := (\eta_{i(l)}^{(1)}, \eta_{i(l)}^{(2)}, \eta_{i(l)}^{(3)})$ 로 두자. 그러면

$$Z_n := g_1 g_2 \cdots g_{n/3} = w_0 r_1 s_1 t_1 w_1 \cdots r_{\lfloor \epsilon n/10m \rfloor} s_{\lfloor \epsilon n/10m \rfloor} t_{\lfloor \epsilon n/10m \rfloor} w_{\lfloor \epsilon n/10m \rfloor}$$

는 μ^{*n} 을 분포로 가진다. 이제 $\{\rho_l, \eta_l : l\}$ 및 $\{\eta_l^{(1)}, \eta_l^{(2)}, \eta_l^{(3)} : l > i(\lfloor \epsilon n/10m \rfloor)\}$ 의 값을 기준으로 동치류를 만들면 주어진 조건을 만족하게 되어 증명이 끝난다. \square

앞에서 본것 다시.

정의 3.2. 자연수 N 을 생각한 뒤 분해능 N 짜리 Schottky 집합 $S = \cup_{i=1}^N \mathfrak{S}(I_i, J_i)$ 을 생각하자. 임의의 위상동형사상 $g \in \text{Homeo}(S^1)$ 에 대해,

$$\mathcal{C}(g; S) := \{I_i : \#\{j : \bar{I}_i \cap g\bar{J}_j \neq \emptyset\} \geq \sqrt{N}\},$$

로 두겠다. 또, 임의의 구간 I 에 대해

$$\mathcal{R}(I; S) := \{J_i : \bar{J}_i \cap \bar{I} \neq \emptyset\}$$

로 두겠다.

보조정리 3.3. 분해능 N 짜리 Schottky 집합 및 임의의 위상동형사상 $g \in \text{Homeo}(S^1)$ 에 대해, $\mathcal{C}(g; S)$ 의 크기는 $2\sqrt{N}$ 보다 작다. 또한, 임의의 $I \in \mathcal{C}(g; S)$ 에 대해 $\mathcal{R}(g^{-1}I; S)$ 의 크기는 $2\sqrt{N}$ 보다 작다.

앞선 정의를 하나 돌이켜 보자. Schottky 집합 $S = \cup_{i=1}^N \mathfrak{S}(I_i, J_i)$ 가 하나 고정되어 있을 때, S 의 각 원소는 어떤 $\mathfrak{S}(I_i, J_i)$ 에 포함되어 있고 이때 I_i 를 $I(s)$ 로, J_i 를 $J(s)$ 로 나타내기로 했음을 기억하라.

정의 3.4. 구간 \mathcal{I} 를 중선으로 가지는 Schottky 집합

$$S := \cup_{i=1}^N \mathfrak{S}(I_i, J_i)$$

을 고정하자. 원의 위상동형사상의 나열 $\mathbf{w} = (w_i)_{i=0}^\infty$ 를 고정한 뒤, S 의 원소의 나열 $\mathbf{r} = (r_i)_{i=1}^\infty, \mathbf{s} = (s_i)_{i=1}^\infty, \mathbf{t} = (t_i)_{i=1}^\infty$ 를 뽑겠다. 편의를 위해 다음과 같은 재귀적인 표기법을 사용하겠다:

$$W_0 := w_0, W_n := W_{n-1} \cdot r_n s_n t_n \cdot w_n \quad (n > 0).$$

음이 아닌 정수 n 에 대해 증추적 구간 (pivotal intervals) $L_n = L_n(\mathbf{r}, \mathbf{s}, \mathbf{t}; \mathbf{w}) \subseteq S^1$ 및 증추 시점 집합 (set of pivotal times) $P_n(\mathbf{r}, \mathbf{s}, \mathbf{t}; \mathbf{w}) \subseteq \{1, \dots, n\}$ 을 다음과 같이 재귀적으로 정의하겠다:

(1) $n = 0$ 일 때는 $L_0 := \mathcal{I}, P_0 := \emptyset$ 으로 둔다.

(2) $n \geq 1$ 일 때는 다음 두 가지 케이스로 나누어 생각한다.

(A) 만약 $J(r_n) \subseteq W_{n-1}^{-1}L_{n-1}$ 및 $I(t_n) \notin \mathcal{C}(w_n; S)$ 가 성립한다면, $L_n := W_{n-1}r_n s_n \mathcal{I}$ 및 $P_n := P_{n-1} \cup \{n\}$ 로 정의한다.

(B) 만약 $J(r_n) \subseteq W_{n-1}^{-1}L_{n-1}$ 또는 $I(t_n) \notin \mathcal{C}(w_n; S)$ 가 성립하지 않으면,

$$\mathcal{Q} := \left\{ i \in P_{n-1} : I(t_i) \notin \mathcal{C}(w_i \cdot W_i^{-1} \cdot W_n; S) \right\}$$

라는 집합을 생각하겠다.

(i) \mathcal{Q} 가 공집합이 아닌 경우 $k := \max \mathcal{Q}$ 에 대해 $L_n := W_{k-1}r_k s_k \mathcal{I}$ 및 $P_n := P_{n-1} \cap \{1, \dots, k\}$ 로 정의한다.

(ii) \mathcal{Q} 가 공집합이라면 $L_n := W_n \mathcal{I}, P_n := \emptyset$ 으로 둔다.

다음 관찰은 정의로부터 곧바로 따라 나온다.

보조정리 3.5. 정의 3.4의 세팅에서, 각각의 음의 아닌 정수 n 에 대해 $P_n(\mathbf{r}, \mathbf{s}, \mathbf{t}; \mathbf{w})$ 및 $L_n(\mathbf{r}, \mathbf{s}, \mathbf{t}; \mathbf{w})$ 는 $(r_i, s_i, t_i)_{i=1}^n, (w_i)_{i=0}^n$ 의 값에만 의존하며, $(r_i, s_i, t_i, w_i)_{i=n+1}^\infty$ 의 값에 의존하지 않는다.

다음으로, 증추 시점에 등장하는 \mathcal{I} 의 복사본들이 중첩되어 있음을 확인하고자 한다. 이는 다음 보조정리로부터 따라 나온다.

보조정리 3.6. 정의 3.4의 세팅에서 음이 아닌 정수 u 를 정한 뒤 연달아 있는 P_u 의 원소들 $l < m$ 을 생각하자. 즉 $l, m \in P_u$ 이고 $l = \max(P_u \cap \{1, \dots, m-1\})$ 임을 가정하는 것이다. 그러면 $W_{l-1}r_l s_l \mathcal{I} \supseteq W_{l-1}r_l s_l t_l (S \setminus I(t_l)) \supseteq W_{m-1}r_m \mathcal{I}$ 가 성립한다.

Proof. 먼저, Schottky 집합 S 및 그 중선 \mathcal{I} 의 성질에 의해, 그 어떤 $t \in S$ 에 대해서도 $S^1 \setminus I(t) \subseteq t^{-1}\mathcal{I}$ 가 성립한다. 이로부터 첫번째 포함관계는 따라 나온다. 따라서 두번째 포함관계만 증명하면 된다. 이를 위해 다음을 관찰하자:

주장 3.7. 숫자 l 은 P_{l-1} 로부터 P_l 이 건설되는 시점에 새로 추가되었어야 한다. 다시 말해, $P_{l-1} = P_l \cup \{l\}$ 이 성립한다.

위를 관찰하기 위해 결론을 부정해 보자. 즉 P_l 는 $P_{l-1} \subseteq \{1, \dots, l-1\}$ 의 부분집합임을 가정하는 것이다. 그러면 P_l 은 물론이고, P_{l+1}, P_{l+2}, \dots 는 모두 l 을 포함할 수 없다. 이후 P_l 로부터 P_{l+1} 이, 또 P_{l+1} 로부터 P_{l+2} 가 건설되는 과정에서는 l 이 추가될 수 없기 때문이다. 하지만 우리는 P_u 이 l 을 포함한다는 것을 알기에 이는 모순이고, 주장이 따라 나온다.

마찬가지 이유로, $P_{m-1} = P_m \cup \{m\}$ 또한 성립한다. 따라서, $n = l$ 단계 및 $n = m$ 단계에서는 정의 3.4에서 기술하는 경우들 중 (2-A)가 성립했다는 것을 알 수 있다.

이제 두번째 주장은 다음과 같다.

주장 3.8. $P_u \cap \{1, \dots, m-1\} = P_{m-1}$ 이 성립한다.

먼저, P_u 이 가지고 있는 $m-1$ 이하인 원소들은 모두 $m-1$ 단계 이전에 얻고 이후 잃어버리지 않았던 숫자들이다. 따라서 이들은 모두 P_{m-1} 에도 속한다. 한편, P_{m-1} 이 가지고 있는 원소는 이후에도 결코 사라지지 않는데, 그 이유는 다음과 같다. 만약 $P_{m-1} \subseteq \{1, \dots, m-1\}$ 의 어떤 원소를 어떤 n 단계 ($n = m, \dots, u$)에서 잃는다면, 그 n 단계에서는 정의 3.4의 (2-B) 시나리오가 벌어지고, 특히 $k = \max Q$ 가 $m-1$ 보다 작아야만 한다. 그렇다면 P_n 은 P_{m-1} 의 원소뿐만 아니라 m 또한 잃게 되는데, P_u 이 m 을 보유하고 있음을 알기에 이는 모순이다. 이로써 주장을 얻는다.

이제 두 가지 경우로 나누어 본 증명을 완료하겠다.

- (1) $l = m-1$: 이 경우, l 단계에서도 (2-A) 시나리오가 벌어졌고 $m = l+1$ 단계에서도 (2-A)가 벌어졌다. 따라서 $J(r_{l+1}) \subseteq W_l^{-1}L_l := (t_l w_l)^{-1}\mathcal{I}$ 가 성립한다. 이는 곧

$$r_{l+1}\mathcal{I} \subseteq J(r_{l+1}) \subseteq (t_l w_l)^{-1}\mathcal{I}, W_l r_{l+1}\mathcal{I} \subseteq W_l (t_l w_l)^{-1}\mathcal{I} = W_{l-1}r_l s_l \mathcal{I}$$

임을 암시하기에 목표한 명제가 성립한다.

- (2) $l < m-1$: 이 경우, $P_{m-1} = P_u \cap \{1, \dots, m-1\} \subseteq \{1, \dots, l\}$ 이 $m-1$ 을 포함하지 않기에, $n = m-1$ 단계에서는 (2-B) 시나리오가 성립했어야 한다. 다만 $P_{m-1} = P_u \cap \{1, \dots, m-1\}$ 이 l 이라는 원소를 포함하기에 (2-B-ii) 시나리오에 해당할 수는 없다. 즉 (2-B-i) 시나리오가 성립했어야 하고, l 은 $(m-1)$ 단계에서의 Q 의 최대 원소이며 $L_{m-1} := W_{l-1}r_l s_l \mathcal{I}$ 가 성립한다. 이제 $n = m$ 단계에서는 (2-A) 시나리오가 벌어졌기에, $J(r_m) \subseteq W_m^{-1}L_{m-1}$ 임을 안다. 다시 말해,

$$W_m r_m \mathcal{I} \subseteq W_m J(r_m) \subseteq L_{m-1} = W_{l-1}r_l s_l \mathcal{I}$$

가 성립해 증명이 끝난다. □

여기서 \mathcal{I} 는 Schottky 집합 S 의 중선이기에 임의의 $s \in S$ 에 대해 $\mathcal{I} \supseteq s\mathcal{I}$ 임을 상기하자. 이와 보조정리 3.6을 조합하면 다음 결과를 얻는다.

따름정리 3.9. 정의 3.4의 세팅에서 음이 아닌 정수 n 을 정한 뒤 $P_n := \{i(1) < i(2) < \dots < i(\#P_n)\}$ 과 같이 순차적으로 나타내면,

$$\begin{aligned} W_{i(1)-1}r_{i(1)}\mathcal{I} \supseteq W_{i(1)-1}r_{i(1)}s_{i(1)}\mathcal{I} \supseteq W_{i(2)-1}r_{i(2)}\mathcal{I} \supseteq W_{i(2)-1}r_{i(2)}s_{i(2)}\mathcal{I} \supseteq \\ \dots \supseteq W_{i(\#P_n)-1}r_{i(\#P_n)}\mathcal{I} \supseteq W_{i(\#P_n)-1}r_{i(\#P_n)}s_{i(\#P_n)}\mathcal{I} \end{aligned}$$

가 성립한다.

다음으로, 분해능이 높은 S 를 가져온 뒤 $\mathbf{r}, \mathbf{s}, \mathbf{t}$ 를 S 위에서 Schottky-균일하게 뽑는다면 정의 3.4에서 시나리오 (2-A)가 성립할 확률이 높다는 것을 관찰하겠다.

보조정리 3.10. 중선 달린 분해능 N 짜리 Schottky 집합 S 및 양의 정수 n 을 고정한 뒤, $\text{Homeo}(S^1)$ 의 원소 나열 $\mathbf{w} = (w_i)_{i=0}^\infty$, S 의 원소 나열 $\mathbf{s} = (s_i)_{i=1}^\infty$ 를 고정하자. 또, S 의 원소 나열 두 개 $\mathbf{r} = (r_i)_{i=1}^\infty$, $\mathbf{t} = (t_i)_{i=1}^\infty$ 를 $i = n$ 번째 항을 제외하고 고정하자. 이때, S 위에 Schottky-균일하게 분포된 임의의 확률 측도 μ 에 대해

$$\mathbb{P}_{r_n, t_n \sim \text{독립적인 } \mu\text{-분포}} (\#P_n(\mathbf{r}, \mathbf{s}, \mathbf{t}; \mathbf{w}) = \#P_{n-1}(\mathbf{r}, \mathbf{s}, \mathbf{t}; \mathbf{w}) + 1) \geq 1 - 4/\sqrt{N}$$

이 성립한다.

Proof. Schottky 집합 S 에 결부된 구간들을 $\{I_i, J_i : i = 1, \dots, N\}$ 로 적겠다. 주어진 고정 입력값으로부터 P_{n-1} 및 L_{n-1} 는 확정된다. 이때 $(n-1)$ 단계에서 세 가지 가능성이 있다:

- (1) 시나리오 (2-A)가 성립했을 경우: 그러면 $I(t_{n-1}) \in \mathcal{C}(w_{n-1}; S)$ 및 $L_{n-1} = W_{n-2}r_{n-1}s_{n-1}\mathcal{I}$ 가 성립한다.
- (2) 시나리오 (2-B-i)가 성립했을 경우: 그러면 $k = \max P_{n-1}$ 에 대해 $I(t_k) \in \mathcal{C}(w_k W_k^{-1} W_{n-1}; S)$ 및 $L_{n-1} := W_{k-1}r_k s_k \mathcal{I}$ 가 성립한다.
- (3) 시나리오 (2-B-ii)가 성립했을 경우: 그러면 $L_{n-1} := W_{n-1}\mathcal{I}$ 는 모든 $W_{n-1}J_i$ 들을 포함한다.

이제, 사건의 필요충분조건은 n 단계에서 (2-A) 시나리오가 성립하는 것이다. 먼저 보조정리 3.3에 따르면

$$\mathbb{P}_{t_n \sim \mu} (I(t_n) \in \mathcal{C}(w_n; S)) \leq \frac{1}{N} \cdot 2\sqrt{N} = \frac{2}{\sqrt{N}}$$

가 성립한다. 이제 위에서 얘기한 세 가능성 각각에 대해 $J(r_n) \subseteq W_{n-1}^{-1}L_{n-1}$ 의 확률을 계산해 보자.

- (1) 시나리오 (2-A)가 성립했을 경우: $I(t_{n-1}) \in \mathcal{C}(w_{n-1}; S)$ 라는 사실에 보조정리 3.3을 적용하면 $\mathcal{R}(w_{n-1}^{-1}I(t_{n-1}); S)$ 의 크기가 $2\sqrt{N}$ 보다 작다는 것을 알 수 있다. 또한 $J(r_n) \notin \mathcal{R}(w_{n-1}^{-1}I(t_{n-1}); S)$ 인 경우,

$$J(r_n) \subseteq S^1 \setminus (\text{int } w_{n-1}^{-1}I(t_{n-1})) \subseteq w_{n-1}^{-1}t_{n-1}^{-1}\mathcal{I} = W_{n-1}^{-1}W_{n-2}r_{n-1}s_{n-1}\mathcal{I} = W_{n-1}^{-1}L_{n-1}$$

가 성립한다. 따라서

$$\mathbb{P}_{r_n \sim \mu} (J(r_n) \subseteq W_{n-1}^{-1}L_{n-1}) \geq \mathbb{P}_{r_n \sim \mu} (J(r_n) \notin \mathcal{R}(w_{n-1}^{-1}I(t_{n-1}); S)) \geq 1 - 2/\sqrt{N}$$

임을 알 수 있다.

(2) 시나리오 (2-B-i)가 성립했을 경우: $I(t_k) \in \mathcal{C}(w_k W_k^{-1} W_{n-1}; S)$ 라는 사실에 보조정리 3.3을 적용하면 $\mathcal{R}(W_{n-1}^{-1} W_k w_k^{-1} I(t_k); S)$ 의 크기가 $2\sqrt{N}$ 보다 작다는 것을 알 수 있다. 또한 $J(r_n) \notin \mathcal{R}(W_{n-1}^{-1} W_k w_k^{-1} I(t_k); S)$ 인 경우,

$$J(r_n) \subseteq S^1 \setminus (\text{int } W_{n-1}^{-1} W_k w_k^{-1} I(t_k)) \subseteq W_{n-1}^{-1} W_k w_k^{-1} t_k^{-1} \mathcal{I} = W_{n-1}^{-1} W_{k-1} r_k s_k \mathcal{I} = W_{n-1}^{-1} L_{n-1}$$

가 성립한다. 이제 (1)에서와 비슷한 계산을 통해 $J(r_n) \subseteq W_{n-1}^{-1} L_{n-1}$ 일 확률이 최소 $1 - 2/\sqrt{N}$ 임을 알 수 있다.

(3) 시나리오 (2-B-ii)가 성립했을 경우: 그러면 $J(r_n)$ 이 J_1, \dots, J_N 중 그 무엇이든 $W_{n-1}^{-1} L_{n-1} = \mathcal{I}$ 에 속하기 때문에, 사건이 일어날 확률은 1이다.

이제 세 가능성에 대해 $I(t_n) \notin \mathcal{C}(w_n; S)$ 및 $J(r_n) \subseteq W_{n-1}^{-1} L_{n-1}$ 일 확률을 종합해 보면 확률이 $1 - 4/\sqrt{N}$ 이상이라고 결론지을 수 있다. \square

이제 중추 회전 기법의 핵심인 보조정리를 하나 증명하겠다. 풀어서 말하자면, $P_n(\mathbf{r}, \mathbf{s}, \mathbf{t})$ 안에 들어 있는 중추 시점에서만 \mathbf{s} 의 선택지를 바꾼다면 중추 시점 집합은 전혀 변하지 않는다는 보조정리이다.

보조정리 3.11. 중선 달린 Schottky 집합 S , 양의 정수 n 및 $\text{Homeo}(S^1)$ 의 원소 나열 $\mathbf{w} = (w_i)_{i=0}^n$ 을 고정한 뒤 S 의 원소 나열 $\mathbf{r} = (r_i)_{i=1}^\infty, \mathbf{s} = (s_i)_{i=1}^\infty, \bar{\mathbf{s}} = (\bar{s}_i)_{i=1}^\infty, \mathbf{t} = (t_i)_{i=1}^\infty$ 를 생각하자. 이때 만약

$$\text{각각의 } i \in \{1, \dots, n\} \setminus P_n(\mathbf{r}, \mathbf{s}, \mathbf{t}; \mathbf{w}) \text{에 대해 } s_i = \bar{s}_i \text{ 임}$$

이 성립한다면, 각각의 $1 \leq l \leq n$ 에 대해 $P_l(\mathbf{r}, \mathbf{s}, \mathbf{t}; \mathbf{w}) = P_l(\mathbf{r}, \bar{\mathbf{s}}, \mathbf{t}; \mathbf{w})$ 또한 성립한다.

Proof. 이 보조정리의 초보적인 경우로서 다음 명제를 생각해 보자.

주장 3.12. 상술한 바와 같이 $S, n, \mathbf{w}, \mathbf{r}, \mathbf{s}, \bar{\mathbf{s}}, \mathbf{t}$ 를 정한 뒤, $k \in P_n(\mathbf{r}, \mathbf{s}, \mathbf{t}; \mathbf{w})$ 를 하나 뽑자. 만약 $l = k$ 를 제외한 모든 l 에 대해 $s_l = \bar{s}_l$ 가 성립한다면, 각각의 $1 \leq l \leq n$ 에 대해 $P_l(\mathbf{r}, \mathbf{s}, \mathbf{t}; \mathbf{w}) = P_l(\mathbf{r}, \bar{\mathbf{s}}, \mathbf{t}; \mathbf{w})$ 또한 성립한다.

다시 말해, 중추 시점 하나를 골라 거기서만 \mathbf{s} 의 선택지를 바꾼다면 각 단계별 중추 시점 집합 P_l 은 변하지 않는다는 것이다. 이 주장을 가정하면, 보조정리의 세팅에서 \mathbf{s} 에서 출발해 중추 시점 하나씩마다 선택지를 바꾸면서 $\bar{\mathbf{s}}$ 에 이르는 동안 P_l 들이 변하지 않는다는 것을 관찰할 수 있어 증명이 끝난다.

이제 주장을 증명하는 일이 남았다. 이 증명 내내 $\mathbf{w}, \mathbf{r}, \mathbf{t}$ 는 쪽 고정되어 있으므로 표기상 이들을 생략하겠다. 먼저, k 보다 작은 l 에 대해서는 $P_l(\mathbf{s})$ 은 $(\mathbf{w}, \mathbf{r}, \mathbf{t}$ 및) s_1, \dots, s_{k-1} 에 대해서만 의존하기에 $P_l(\bar{\mathbf{s}})$ 과 다를 이유가 없다. 마찬가지로 L_l 도 두 입력값에 대해 일치한다.

이제 $l = k$ 단계를 살펴보자. k 는 $P_n(\mathbf{s})$ 의 원소이므로 (2-A)의 시나리오가 성립한다. 여기서

$$J(r_k) \subseteq W_{k-1}^{-1} L_{k-1}, I(t_k) \notin \mathcal{C}(w_k; S)$$

라는 두 조건은 오로지 $(\mathbf{w}, \mathbf{r}, \mathbf{t}$ 및) s_1, \dots, s_{k-1} 에만 의존한다. 따라서 s_k 를 \bar{s}_k 로 치환해도 이 정보는 그대로 유지되고, 따라서

$$P_k(\bar{\mathbf{s}}) = P_{k-1}(\bar{\mathbf{s}}) \cup \{k\} = P_{k-1}(\mathbf{s}) \cup \{k\} = P_k(\mathbf{s})$$

가 성립한다. 또한,

$$L_k(\mathbf{s}) = W_{k-1} r_k s_k \mathcal{I}, L_k(\bar{\mathbf{s}}) = W_{k-1} r_k \bar{s}_k \mathcal{I} = g \cdot W_{k-1} r_k s_k \mathcal{I} \quad (g := W_{k-1} r_k \bar{s}_k s_k^{-1} r_k^{-1} W_{k-1}^{-1})$$

이 성립하며, 각각의 $k \leq l \leq n$ 에 대해 $W_l(\bar{\mathbf{s}}) = g \cdot W_l(\mathbf{s})$ 라는 관계식을 관찰할 수 있다.

이제, $k < l \leq n$ 에 대해 귀납적으로 다음을 증명하겠다:

- (1) 만약 입력값 \mathbf{s} 에 대해 l 단계에서 시나리오 (2-A)가 성립한다면, $\bar{\mathbf{s}}$ 를 입력해도 또한 그렇다.
- (2) 만약 입력값 \mathbf{s} 에 대해 l 단계에서 시나리오 (2-B-i)가 성립한다면, $\bar{\mathbf{s}}$ 를 입력해도 또한 그렇다.
또, 두 입력값에 대한 $\max Q$ 의 값은 같다.
- (3) 시나리오 (2-B-ii)는 일어나지 않는다.
- (4) 위의 모든 경우에서 $P_l(\mathbf{s}) = P_l(\bar{\mathbf{s}})$ 및 $L_l(\bar{\mathbf{s}}) = gL_l(\mathbf{s})$ 가 성립한다.

시작 케이스로서 $l = k$ 일 때의 항목 (4)는 이미 관찰했다는 것을 기억하자. 이제 $k < l \leq n$ 에 대해, $l - 1$ 에 대한 항목 (4)를 가정하고 위 항목들을 증명하겠다. 먼저, \mathbf{s} 에 대한 시나리오 (2-A)의 조건인

$$J(r_l) \subseteq W_{l-1}(\mathbf{s})^{-1}L_{l-1}(\mathbf{s}), \quad I(t_l) \notin \mathcal{C}(w_l; S)$$

를 상기해 보자. 후자 조건은 $s_k \mapsto \bar{s}_k$ 의 치환에 의해 변할 이유가 없다. 또 귀납 가정에 따라

$$[J(r_l) \subseteq W_{l-1}(\mathbf{s})^{-1}L_{l-1}(\mathbf{s})] \Leftrightarrow [J(r_l) \subseteq W_{l-1}(\mathbf{s})^{-1}g^{-1} \cdot gL_{l-1}(\mathbf{s}) = W_{l-1}(\bar{\mathbf{s}})^{-1}L_{l-1}(\bar{\mathbf{s}})]$$

가 성립한다. 이를 종합하면 \mathbf{s} 가 l 단계에서 시나리오 (2-A)를 만족한다는 것과, $\bar{\mathbf{s}}$ 가 그러하다는 것은 동치다. 또 이 동치조건이 성립할 때

$$P_l(\bar{\mathbf{s}}) = P_{l-1}(\bar{\mathbf{s}}) \cup \{l\} = P_{l-1}(\mathbf{s}) \cup \{l\} = P_l(\mathbf{s})$$

및

$$L_l(\bar{\mathbf{s}}) := W_l(\bar{\mathbf{s}}) \cdot (t_l w_l)^{-1} \mathcal{I} = gW_l(\bar{\mathbf{s}}) \cdot (t_l w_l)^{-1} \mathcal{I} = gL_l(\mathbf{s})$$

까지 따라나온다.

만약 \mathbf{s} 에 대해 시나리오 (2-B)가 성립한다면, 위 관찰에 따라 \mathbf{s}' 또한 시나리오 (2-B)에 해당한다. 이때는 집합

$$\mathcal{Q}(\mathbf{s}) = \mathcal{Q}(\mathbf{s}; l) := \left\{ i \in P_{l-1} : I(t_i) \notin \mathcal{C}(w_k \cdot W_i(\mathbf{s})^{-1}W_l(\mathbf{s}); S) \right\}$$

를 들여다보아야 한다. 그런데 $i \geq k$ 에 대해서는 $W_i(\bar{\mathbf{s}}) = gW_i(\mathbf{s})$ 임을 기억하자. 이는 다시 말해

$$\mathcal{Q}(\mathbf{s}; l) \cap \{k, k+1, \dots, l-1\} = \mathcal{Q}(\bar{\mathbf{s}}; l) \cap \{k, k+1, \dots, l-1\}$$

임을 의미한다. 그런데 k 가 $P_n(\mathbf{s})$ 에 살아남아 있음에 유의하자. 이는 곧 l 단계에서 k 가 중추 집합에서 탈락해서는 안 된다는 뜻이다. 다시 말해, 설령 시나리오 (2-B)에 해당하더라도 $\mathcal{Q}(\mathbf{s}; l)$ 는 반드시 k 이상인 원소를 포함하게 된다. 이로써 시나리오 (2-B-ii)는 배제된다.

그러면 $\mathcal{Q}(\bar{\mathbf{s}}; l) \cap \{k, k+1, \dots, l-1\} = \mathcal{Q}(\mathbf{s}; l) \cap \{k, k+1, \dots, l-1\}$ 또한 공집합이 아니다. $\mathcal{Q}(\mathbf{s})$ 및 $\mathcal{Q}(\bar{\mathbf{s}})$ 의 최대 원소는 이 (공집합이 아닌) 공통된 윗쪽 부분집합에서 잡히므로, 최대 원소끼리도 서로 같다. 이 공통된 최대 원소를 u 라고 두면

$$P_l(\bar{\mathbf{s}}) = P_{l-1}(\bar{\mathbf{s}}) \cap \{1, \dots, u\} = P_{l-1}(\mathbf{s}) \cap \{1, \dots, u\} = P_l(\mathbf{s})$$

및

$$L_l(\bar{\mathbf{s}}) := W_u(\bar{\mathbf{s}}) \cdot (t_u w_u)^{-1} \mathcal{I} = gW_u(\mathbf{s})(t_u w_u)^{-1} \mathcal{I} = gL_l(\mathbf{s})$$

이 성립한다. 마지막 식에서는 u 가 k 이상임을 사용한 것이다. 이로써 증명이 끝난다. \square

이제 중추 회전에 의한 동치류를 정의할 수 있다.

{EquivClass}

정의 3.13. 정의 3.4의 세팅에서와 같이 중선 달린 Schottky 집합 S 및 $\text{Homeo}(S^1)$ 안의 나열 \mathbf{w} 를 하나 고정하자. 더하여, 양의 정수 n 도 하나 고정하자. 이제 $(\mathbf{r}, \mathbf{s}, \mathbf{t})$ 가 살고 있는 전체 집합 $S^{\mathbb{Z}_{>0}} \times S^{\mathbb{Z}_{>0}} \times S^{\mathbb{Z}_{>0}}$ 에 다음과 같은 동치 관계를 선언하겠다:

$$[(\mathbf{r}, \mathbf{s}, \mathbf{t}) \sim_n (\bar{\mathbf{r}}, \bar{\mathbf{s}}, \bar{\mathbf{t}})] \Leftrightarrow \left[\begin{array}{l} \text{각각의 } i \in \mathbb{Z}_{>0} \setminus \{n+1\} \text{ 에 대해 } r_i = \bar{r}_i \text{ 및 } t_i = \bar{t}_i \text{이고,} \\ \text{각각의 } i \in \mathbb{Z}_{>0} \setminus P_n(\mathbf{r}, \mathbf{s}, \mathbf{t}; \mathbf{w}) \text{에 대해 } \bar{s}_i = s_i \text{임} \end{array} \right]$$

이것이 실제로 동치 관계가 된다는 것이 보조정리 3.5 및 보조정리 3.11의 내용이다. 여기서 주의할 것은, \sim_n 이라는 동치 관계는 n 에 따라 달라진다는 것이다.

표기법에 조금 자유를 두어, $S^{\mathbb{Z}_{>0}} \times S^{\mathbb{Z}_{>0}} \times S^{\mathbb{Z}_{>0}}$ 라는 가측 공간에서의 좌표 성분들을 $(\mathbf{r}, \mathbf{s}, \mathbf{t})$ 로 표현하겠다. 이말은 곧 $r_1, r_2, \dots, s_1, s_2, \dots, t_1, t_2, \dots$ 라는 표기를 사용하겠다는 것이다. 이제 \sim_n 으로 주어진 동치류 $\mathcal{E} \subseteq S^{\mathbb{Z}_{>0}} \times S^{\mathbb{Z}_{>0}} \times S^{\mathbb{Z}_{>0}}$ 를 임의로 하나 생각해 보자. 그러면 \mathcal{E} 의 모든 원소들은 공통된 n 단계 중추 시점 집합 P_n 을 가지는데, 이 집합을 $P_n(\mathcal{E})$ 이라고 표기하겠다. 그러면 \mathcal{E} 위에서, r_i 및 t_i 는 $i = n+1$ 에 대해서는 제약 없이 S 의 임의의 원소를 값으로 가질 수 있고, $n+1$ 이 아닌 i 에 대해서는 고정된 값을 가진다. \mathcal{E} 위에서 s_i 는 $i \in P_n(\mathcal{E})$ 에 대해서는 S 의 임의의 원소를 값으로 가질 수 있고, 그렇지 않은 i 에 대해서는 값이 고정된다.

이는 측도를 얹은 다음에 더 잘 드러난다. S 위에 분포된 확률 측도 μ 를 하나 생각한 뒤 전체 공간 $S^{\mathbb{Z}_{>0}} \times S^{\mathbb{Z}_{>0}} \times S^{\mathbb{Z}_{>0}}$ 위에 μ 의 곱공간을 생각해 보자. 즉 모든 r_i, s_i, t_i 들이 독립적으로 μ -분포를 가진다는 것이다. 이제 이 측도를 \mathcal{E} 에 제한해 보면, $\{r_i, t_i : i \neq n+1\}$, $\{s_i : i \notin P_n(\mathcal{E})\}$ 는 모두 상수 변수인 한편 $\{s_i : i \in P_n(\mathcal{E})\}$, $\{r_{n+1}, t_{n+1}\}$ 은 모두 서로 독립이면서 μ 로 분포되어 있다.

{prop:pivotD}

명제 3.14. 중선 달린 분해능 N 짜리 Schottky 집합 S 와 그 위에 Schottky-균일하게 분포된 확률측도 μ 를 하나 고정하자. 또 $\text{Homeo}(S^1)$ 안의 나열 \mathbf{w} 및 양의 정수 n 을 고정한 뒤, $S^{\mathbb{Z}_{>0}} \times S^{\mathbb{Z}_{>0}} \times S^{\mathbb{Z}_{>0}}$ 안에서 \sim_n 이 이루는 동치류 \mathcal{E} 를 하나 고정하자. 그러면 각 $j \geq 0$ 에 대해

$$\mathbb{P}_{\{r_i, s_i, t_i : i > 0\}} \text{ 모두가 독립적으로 } \mu \text{로 분포} \left(\#P_{n+1}(\mathbf{r}, \mathbf{s}, \mathbf{t}; \mathbf{w}) < \#P_n(\mathbf{r}, \mathbf{s}, \mathbf{t}; \mathbf{w}) - j \mid \mathcal{E} \right) \leq (4/\sqrt{N})^{j+1}$$

가 성립한다.

Proof. 표기상의 편의를 위해, 동치류 \mathcal{E} 의 (모든 원소가 공통으로 가지는) n 단계 중추 시점 집합 $P_n(\mathcal{E})$ 을 $\{i(M) < i(M-1) < \dots < i(2) < i(1)\}$ 로 나타내겠다. (여기서 M 은 $P_n(\mathcal{E})$ 의 크기다.) 여기서 M 및 $i(1), i(2), \dots, i(M)$ 은 \mathcal{E} 가 주어졌을 때부터 고정된 정보이고, $\{w_i : i > 0\}$, $\{r_i, t_i : i \neq n+1\}$, $\{s_i : i \notin P_n(\mathcal{E})\}$ 또한 고정된 정보임을 관찰하라. 즉 \mathcal{E} 의 원소들은 $(s_{i(M)}, \dots, s_{i(1)}, r_{n+1}, t_{n+1})$ 라는 좌표들로 특정되는데, 이 좌표 변수들은 서로 독립적인 μ -분포를 가진다.

이제

$$A_0 \subseteq S \times S,$$

$$A_1(r_{n+1}, t_{n+1}) \subseteq S,$$

$$A_2(s_{i(1)}, r_{n+1}, t_{n+1}) \subseteq S,$$

$\dots,$

$$A_M(s_{i(M-1)}, \dots, s_{i(1)}, r_{n+1}, t_{n+1}) \subseteq S$$

라는 집합들을 건설한 뒤 다음을 증명할 것이다.

주장 3.15. (1) $\mathbb{P}_{\mu \times \mu}(A_0) \geq 1 - 4/\sqrt{N}$.

{claim:AiInc}

(2) 임의의 선택지 $(s_{i(M)}, \dots, s_{i(1)}, r_{n+1}, t_{n+1}) \in S^{M+2}$ 에 대해, 만약 $(r_{n+1}, t_{n+1}) \in A_0$ 라면

$$\#P_n(s_{i(M)}, \dots, s_{i(1)}, r_{n+1}, t_{n+1}) = \#P_n(s_{i(M)}, \dots, s_{i(1)}) + 1$$

이 성립한다.

(3) 임의의 $1 \leq l \leq M$ 및 임의의 $(s_{i(l-1)}, \dots, s_{i(1)}, r_{n+1}, t_{n+1}) \in S^{l+1}$ 에 대해

$$\mathbb{P}_{s_{i(l)} \sim \mu} (s_{i(l)} \in A_l(s_{i(l-1)}, \dots, s_{i(1)}, r_{n+1}, t_{n+1})) \geq 1 - 4/\sqrt{N}$$

가 성립한다.

(4) 임의의 선택지 $(s_{i(M)}, \dots, s_{i(1)}, r_{n+1}, t_{n+1}) \in S^{M+2}$ 및 $1 \leq l \leq M$ 에 대해, 만약 $s_{i(l)}$ 가 $A_l(s_{i(l-1)}, \dots, s_{i(1)}, r_{n+1}, t_{n+1})$ 의 원소라면

$$\#P_n(s_{i(M)}, \dots, s_{i(1)}, r_{n+1}, t_{n+1}) \geq \#P_n(s_{i(M)}, \dots, s_{i(1)}) - l$$

이 성립한다.

이 주장을 가정한 상태에서 본 명제를 증명해 보자. 이를 위해

$$B_0 := \{(\mathbf{r}, \mathbf{s}, \mathbf{t}) \in \mathcal{E} : (r_{n+1}, t_{n+1}) \notin A_0\}$$

를 먼저 정의한 뒤 각 $l = 1, \dots, M$ 마다 귀납적으로

$$B_l := \{(\mathbf{r}, \mathbf{s}, \mathbf{t}) \in B_{l-1} : s_{i(l)} \notin A_{l-1}(\mathbf{r}, \mathbf{s}, \mathbf{t}; \mathbf{w})\}$$

라고 두자. 그러면 주장 3.15(3)에 의해

$$\begin{aligned} \mathbb{P}_{\mathcal{E}}(B_l) &= \int_{(\mathbf{r}, \mathbf{s}, \mathbf{t}) \in B_{l-1}} \mathbb{P}_{s_{i(l)} \sim \mu} (s_{i(l)} \notin A_{l-1} \mid s_{i(l-1)}, \dots, s_{i(1)}, r_{n+1}, t_{n+1}) d\mu(s_{i(l-1)}) \cdots d\mu(s_{i(1)}) d\mu(r_{n+1}) d\mu(t_{n+1}) \\ &\leq \frac{4}{\sqrt{N}} \cdot \mathbb{P}_{\mathcal{E}}(B_{l-1}) \end{aligned}$$

가 성립하고, 또 주장 3.15(1)에 의해 $\mathbb{P}_{\mathcal{E}}(B_0) \leq \frac{4}{\sqrt{N}}$ 이 성립한다. 이를 결합하면, $l = 0, \dots, M$ 에 대해 $\mathbb{P}_{\mathcal{E}}(B_l) \leq (4/\sqrt{N})^{l+1}$ 임을 확인할 수 있다.

다음으로,

$$(\mathbf{r}, \mathbf{s}, \mathbf{t}) \in \mathcal{E} \setminus B_0 \Rightarrow \#P_n(\mathbf{r}, \mathbf{s}, \mathbf{t}; \mathbf{w}) \geq \#P_n(\mathbf{r}, \mathbf{s}, \mathbf{t}; \mathbf{w})$$

가 성립하고, 또 각각의 $l = 1, \dots, M$ 마다

$$(\mathbf{r}, \mathbf{s}, \mathbf{t}) \in B_{l-1} \setminus B_l \Rightarrow \#P_n(\mathbf{r}, \mathbf{s}, \mathbf{t}; \mathbf{w}) \geq \#P_n(\mathbf{r}, \mathbf{s}, \mathbf{t}; \mathbf{w}) - l$$

임을 관찰할 수 있다. 이는 다시 말해 각각의 l 마다

$$(\mathbf{r}, \mathbf{s}, \mathbf{t}) \in \mathcal{E} \setminus B_l \Rightarrow \#P_n(\mathbf{r}, \mathbf{s}, \mathbf{t}; \mathbf{w}) \geq \#P_n(\mathbf{r}, \mathbf{s}, \mathbf{t}; \mathbf{w}) - l$$

라는 것이다. 위에서 B_l 의 확률이 $(4/\sqrt{N})^{l+1}$ 이하라는 것을 확인했으므로 명제의 증명이 끝난다.

이제 주장을 증명하는 일이 남았다. 먼저 A_0 에 관해서는 보조정리 3.10에서 이미 관찰했는데, $(s_{i(M)}, \dots, s_{i(1)})$ 의 값이 그 무엇으로 정해졌든 간에, $\#P_{n+1} = \#P_n + 1$ 이게끔 r_{n+1}, t_{n+1} 가 값을 가질 확률이 $1 -$

$4/\sqrt{N}$ 보다 크다는 것을 증명했었다. 더 나아가, $\#P_{n+1} = \#P_n + 1$ 이게끔 하는 r_{n+1}, t_{n+1} 들의 값은 $(s_{i(M)}, \dots, s_{i(1)})$ 의 정체에 무관하다는 것을 증명하겠다. \mathcal{E} 에 한정해서 볼 때, $\#P_{n+1}(\mathbf{r}, \mathbf{s}, \mathbf{t}; \mathbf{w}) = \#P_n(\mathbf{r}, \mathbf{s}, \mathbf{t}; \mathbf{w}) + 1$ 일 필요충분조건은 $I(t_{n+1}) \in \mathcal{C}(w_{n+1}; S)$ 및 $J(r_{n+1}) \subseteq W_n^{-1}L_n\mathcal{I}$ 이다. 여기서,

$$W_n^{-1}L_n\mathcal{I} = \begin{cases} W_n^{-1}W_{\max P_n - 1}r_{\max P_n}s_{\max P_n}\mathcal{I} \\ = (t_{i(1)}w_{i(1)}r_{i(1)+1}s_{i(1)+1}t_{i(1)+1}w_{i(1)+1} \cdots r_n s_n t_n w_n)^{-1}\mathcal{I} & (P_n(\mathcal{E}) \neq \emptyset \text{일 때}) \\ \mathcal{I} & (P_n(\mathcal{E}) = \emptyset \text{일 때}) \end{cases}$$

의 값은 \mathcal{E} 위에서 고정되어 있기에, $\#P_{n+1} = \#P_n + 1$ 라는 사건은 $s_{i(1)}, \dots, s_{i(M)}$ 의 선택지에 무관하게 오로지 r_{n+1} 및 s_{n+1} 의 값에만 의존하는 것이다. 이로써 A_0 의 구성 및 주장 3.15(1), (2)가 증명되었다.

이제 임의의 $l \in \{1, \dots, M\}$ 및 임의의 $(s_{i(l-1)}, \dots, s_{i(1)}, r_{n+1}, t_{n+1}) \in S^{l+1}$ 에 대해

$$\begin{aligned} A_l &:= \left\{ s \in S : I(s) \notin \mathcal{C}(t_{i(l)}w_{i(l)} \cdot W_{i(l)}^{-1}W_{n+1}; S) \right\} \\ &= \left\{ s \in S : I(s) \notin \mathcal{C}(t_{i(l)}w_{i(l)} \cdot (r_{i(l)+1}s_{i(l)+1}t_{i(l)+1}w_{i(l)+1}) \cdots (r_n s_n t_n w_n) \cdot (r_{n+1}s_{n+1}t_{n+1}w_{n+1}); S) \right\} \end{aligned}$$

를 정의하겠다. $\{r_i, t_i : i \neq n\}$ 및 $\{s_i : i \notin P_n(\mathcal{E})\}$ 가 모두 고정된 값이라는 것을 상기하면, 이 집합의 정체가 $s_{i(l-1)}, \dots, s_{i(1)}$ 및 r_{n+1}, t_{n+1} 의 값에만 의존한다는 것을 알 수 있다. 또한 보조정리 ??에 의해 $\mathbb{P}_\mu(A_l) \geq 1 - 2/\sqrt{N}$ 임을 알 수 있다.

이제 어떤 $(s_{i(M)}, \dots, s_{i(1)}, r_{n+1}, t_{n+1}) \in S^{M+2}$ 의 값에 대해 $s_{i(l)} \in A_l(s_{i(l-1)}, \dots, s_{i(1)}, r_{n+1}, t_{n+1})$ 가 성립한다고 가정하자. 그러면 정의에 의해

$$(3.1) \quad \{\text{eqn:estIJ}\} \quad \#\{j : \bar{I}(s_{i(l)}) \cap t_{i(l)}w_{i(l)} \cdot W_{i(l)}^{-1}W_{n+1}\bar{J}_j \neq \emptyset\} \geq \sqrt{N}$$

가 성립한다. 한편, 보조정리 3.6에 의해

$$W_{i(l+1)-1}r_{i(l+1)}s_{i(l+1)}t_{i(l+1)}(S^1 \setminus I(t_{i(l+1)})) \supseteq W_{i(l)-1}r_{i(l)}\mathcal{I}$$

가 성립한다. 한편, Schottky 집합 S 와 그 증선 \mathcal{I} 의 성질에 의해 $s_{i(l)}I(s_{i(l)}) \supseteq S^1 \setminus \mathcal{I}$ 가 성립한다. 이 두 사실을 조합하면

$$W_{i(l+1)}w_{i(l+1)}^{-1}\bar{I}(t_{i(l+1)}) \subseteq \text{int}(S^1 \setminus W_{i(l)-1}r_{i(l)}\mathcal{I}) \subseteq W_{i(l)-1}r_{i(l)}s_{i(l)}I(s_{i(l)})$$

가 성립한다. 이 사실과 부등식 3.1를 조합하면

$$\#\{j : \bar{I}(t_{i(l+1)}) \cap (W_{i(l+1)}w_{i(l+1)}^{-1})^{-1} \cdot (W_{i(l)-1}r_{i(l)}s_{i(l)}) \cdot t_{i(l)}w_{i(l)} \cdot W_{i(l)}^{-1}W_{n+1}\bar{J}_j \neq \emptyset\} \geq \sqrt{N}$$

를 얻는다. 이는 곧 $I(t_{i(l+1)}) \in \mathcal{C}(w_{i(l+1)} \cdot (W_{i(l+1)})^{-1} \cdot W_{n+1}; S)$ 를 의미하기에, $n+1$ 단계 증추 시점 집합을 구성할 때의 시나리오 (2-B)에서 \mathcal{Q} 가 $i(l+1)$ 를 포함한다는 것을 의미한다. 따라서 $P_{n+1}(\mathbf{r}, \mathbf{s}, \mathbf{t})$ 는 최소한 $P_n(\mathcal{E}) \cap \{1, \dots, i(l+1)\} = \{i(M) < \dots < i(l+1)\}$ 를 포함하고, $\#P_{n+1} \geq \#P_n - l$ 이라는 결론에 도달한다. 이로써 주장 3.15(3), (4)가 증명되었기에 전체 증명이 끝난다. \square

따름정리 3.16. 증선 달린 분해능 N 짜리 Schottky 집합 S 와 그 위에 Schottky-균일하게 분포된 확률 측도 μ 를 하나 고정하고, $\text{Homeo}(S^1)$ 안의 나열 \mathbf{w} 도 하나 고정하자. 이제 $S^{\mathbb{Z}_{>0}} \times S^{\mathbb{Z}_{>0}} \times S^{\mathbb{Z}_{>0}}$ 위에 μ 의 곱측도를 엮었을 때, 임의의 정수 $j, k, n \geq 0$ 에 대해

$$(3.2) \quad \{\text{eqn:condPivotDist}\} \quad \mathbb{P}(\#\text{PivotDist}(\mathbf{r}, \mathbf{s}, \mathbf{t}; \mathbf{w}) < k - j \mid \#P_{n+1}(\mathbf{r}, \mathbf{s}, \mathbf{t}; \mathbf{w}) = k) \leq (4/\sqrt{N})^{j+1}$$

가 성립한다.

{cor:pivotDi

Proof. 먼저 n 을 고정한 뒤 $(S^{\mathbb{Z}_{>0}})^3$ 위에 동치관계 \sim_n 를 주면, 각 동치류 위에서는 n 단계 중추 시점 집합 P_n 이 상수이기 때문에 그 크기 $\#P_n$ 또한 상수이다. 그러니 $\#P_n = k$ 인 동치류들 각각 위에서 부등식 3.3을 관찰하기만 하면 충분하다. 이는 명제 3.14가 얘기하는 것이다. \square

따름정리 3.17. 중선 달린 분해능 N 짜리 Schottky 집합 S 와 그 위에 Schottky-균일하게 분포된 확률 측도 μ 를 하나 고정하고, $\text{Homeo}(S^1)$ 안의 나열 \mathbf{w} 도 하나 고정하자. 이제 $S^{\mathbb{Z}_{>0}} \times S^{\mathbb{Z}_{>0}} \times S^{\mathbb{Z}_{>0}}$ 위에 μ 의 곱측도를 얹었을 때, 임의의 정수 $j, k, n \geq 0$ 에 대해

$$(3.3) \quad \mathbb{P}\left(\#P_{n+1}(\mathbf{r}, \mathbf{s}, \mathbf{t}; \mathbf{w}) < k - j \mid \#P_{n+1}(\mathbf{r}, \mathbf{s}, \mathbf{t}; \mathbf{w}) = k\right) \leq (4/\sqrt{N})^{j+1}$$

가 성립한다.

Proof. 먼저 n 을 고정한 뒤 $(S^{\mathbb{Z}_{>0}})^3$ 위에 동치관계 \sim_n 를 주면, 각 동치류 위에서는 n 단계 중추 시점 집합 P_n 이 상수이기 때문에 그 크기 $\#P_n$ 또한 상수이다. 그러니 $\#P_n = k$ 인 동치류들 각각 위에서 부등식 3.3을 관찰하기만 하면 충분하다. 이는 명제 3.14가 얘기하는 것이다. \square

따름정리 3.18. 중선 달린 분해능 N 짜리 Schottky 집합 S 와 그 위에 Schottky-균일하게 분포된 확률 측도 μ 를 하나 고정하고, $\text{Homeo}(S^1)$ 안의 나열 \mathbf{w} 도 하나 고정하자. 또,

$$(3.4) \quad \mathbb{P}(X_i = j) = \begin{cases} (N-4)/N & \text{if } j = 1, \\ (N-4)4^{-j}/N^{-j+1} & \text{if } j < 0, \\ 0 & \text{otherwise.} \end{cases}$$

라는 분포를 가지는 서로 독립인 실수 확률변수 X_1, X_2, \dots 를 생각하자. 이제 $S^{\mathbb{Z}_{>0}} \times S^{\mathbb{Z}_{>0}} \times S^{\mathbb{Z}_{>0}}$ 위에 μ 의 곱측도를 얹었을 때, 임의의 양의 정수 n 에 대해 $\#P_n$ 는 $X_1 + \dots + X_n$ 보다 분포적으로 우세하다. 그말인즉,

$$\text{임의의 양수 } T \text{에 대해 } \mathbb{P}(\#P_n(s) \geq T) \geq \mathbb{P}(X_1 + \dots + X_n \geq T)$$

라는 뜻이다.

Proof. P_1, \dots, P_n 이 정의되는 공간 $S^{\mathbb{Z}_{>0}} \times S^{\mathbb{Z}_{>0}} \times S^{\mathbb{Z}_{>0}}$ 으로부터도 독립적이게끔 수식 3.4을 따르는 확률변수 X_i 를 정의하자. 그러면 보조정리 3.10 및 따름정리 3.17를 종합해 보았을 때, 임의의 $0 \leq k \leq n$ 및 임의의 $i, j \geq 0$ 에 대해

$$(3.5) \quad \mathbb{P}\left(\#P_{k+1}(s) \geq i + j \mid \#P_k(s) = i\right) \geq \begin{cases} 1 - \frac{4}{N} & \text{if } j = 1, \\ 1 - \left(\frac{4}{N}\right)^{-j+1} & \text{if } j < 0. \end{cases}$$

가 성립한다. 따라서, 0 이상인 값만을 갖는 확률변수 U_k 를 잡아 $\#P_{k+1} - U_k$ 와 $\#P_k + X_{k+1}$ 의 분포가 같게끔 할 수 있다.

이제 $k = 1, \dots, n$ 각각마다 임의의 양의 정수 i 에 대해 $\mathbb{P}(\#P_k \geq i) \geq \mathbb{P}(X_1 + \dots + X_k \geq i)$ 임을 증명하겠다. $k = 1$ 의 경우에는 $\#P_{k-1} = 0$ 이 항상 성립하기에 부등식 3.5으로부터 주장이 따라 나온다. 다음으로 k 에 대한 주장을 가정했을 때,

$$\begin{aligned} \mathbb{P}(\#P_{k+1} \geq i) &\geq \mathbb{P}(\#P_k + X_{k+1} \geq i) = \sum_j \mathbb{P}(\#P_k \geq j) \mathbb{P}(X_{k+1} = i - j) \\ &\geq \sum_j \mathbb{P}(X_1 + \dots + X_k \geq j) \mathbb{P}(X_{k+1} = i - j) \\ &= \mathbb{P}(X_1 + \dots + X_k + X_{k+1} \geq i). \end{aligned}$$

를 관찰할 수 있다. 이로써 증명이 끝난다. \square

{cor:pivotDi

따름정리 3.19. 중선 달린 분해능 $N \geq 2500$ 짜리 Schottky 집합 S 와 그 위에 Schottky-균일하게 분포된 확률측도 μ 를 하나 고정하고, $\text{Homeo}(S^1)$ 안의 나열 \mathbf{w} 도 하나 고정하자. 이제 $S^{\mathbb{Z}_{>0}} \times S^{\mathbb{Z}_{>0}} \times S^{\mathbb{Z}_{>0}}$ 위에 μ 의 곱측도를 얹었을 때,

$$\mathbb{P}(\#P_n(\mathbf{r}, \mathbf{s}, \mathbf{t}; \mathbf{w}) \leq n/2) \leq (3\sqrt[4]{4/N})^n \leq 0.6^n$$

이 성립한다.

Proof. Chebyshev 부등식을 바탕으로 증명해 보자. 먼저 수식 3.5에서 정의한 X_i 를 상기하자. 이때 다음이 성립한다:

$$\begin{aligned} \mathbb{E} \left[\sqrt{4/N}^{X_i} \right] &= \left(1 - \frac{4}{N}\right) \cdot \left[\sqrt{\frac{4}{N}} + \sum_{j=1}^{\infty} \sqrt{\frac{N^j}{4}} \cdot \left(\frac{4}{N}\right)^j \right] \\ &= \left(1 - \frac{4}{N}\right) \sqrt{\frac{4}{N}} \left(1 + \frac{1}{1 - \sqrt{4/N}}\right) \\ &= 2\sqrt{4/N} + \sqrt{4/N^2} - \sqrt{4/N^3} \leq 3\sqrt{4/N}. \end{aligned}$$

여기서 마지막 부등식은 $\sqrt{4/N} \leq 1$ 을 이용한 것이다. 이제 따름정리 3.19 및 X_i 의 독립성을 이용하면

$$\mathbb{E} \left[\sqrt{4/N}^{\#P_n(\mathbf{s})} \right] \leq \mathbb{E} \left[\sqrt{4/N}^{\sum_{i=1}^n X_i} \right] = \prod_{i=1}^n \mathbb{E} \left[\sqrt{4/N}^{X_i} \right] \leq (3\sqrt{4/N})^n.$$

이제 Chebyshev 부등식에 의해

$$\mathbb{E} \left[\sqrt{4/N}^{\#P_n(\mathbf{s})} \right] \geq \mathbb{P}(\#P_n(\mathbf{s}) \leq n/2) \cdot \sqrt{4/N}^{n/2}.$$

이 성립한다. 이 두 부등식을 결합해 결론에 다다를 수 있다. \square

이제 최종적으로 명제 ??을 증명하겠다.

명제 ??의 증명 보조정리 ??에 비추어 보았을 때, 다음 명제만 증명하면 충분하다.

주장 3.20. 중선 달린 분해능 $N \geq 2500$ 짜리 Schottky 집합 S 및 S 위에서 Schottky-맞춤 균일 분포를 가지는 확률측도 μ 를 생각하자. 더하여, 임의의 양의 정수 n 및 $\text{Homeo}(S^1)$ 안의 임의의 나열 $\mathbf{w} = (w_i)_{i=0}^{\infty}$ 를 생각한 뒤, 확률공간 $\Omega = S^{\mathbb{Z}_{>0}} \times S^{\mathbb{Z}_{>0}} \times S^{\mathbb{Z}_{>0}}$ 에 μ 의 곱측도를 얹어 주자. 그러면 Ω 의 가측 부분집합 A , A 의 가측 분할 $\mathcal{P} = \{\mathcal{E}_\alpha\}_\alpha$, 그리고 $\text{Homeo}(S^1)$ 의 원소들을 값으로 가지는 확률변수들 $\{w'_i\}_{i=0, \dots, \lfloor n/2 \rfloor}$, $\{s'_i\}_{i=1, \dots, \lfloor n/2 \rfloor}$ 이 존재하여 다음을 만족한다.

- (1) $\mathbb{P}(A) \geq 1 - 0.6^n$.
- (2) \mathcal{P} 를 이루는 각 동치류 $\mathcal{E} \in \mathcal{P}$ 에 한정해서 보았을 때, $w'_0, \dots, w'_{\lfloor n/2 \rfloor}$ 는 각각 고정된 위상동형 사상들이고 s'_i 들은 독립적으로 μ -분포를 가지는 확률변수들이다.
- (3) A 위에서 $w_0 r_1 s_1 t_1 w_1 \dots r_n s_n t_n w_n = w'_0 s'_1 w'_1 \dots s'_{\lfloor n/2 \rfloor} w'_{\lfloor n/2 \rfloor}$ 가 성립한다.

먼저, 따름정리 3.19에 의해

$$A := \{(\mathbf{r}, \mathbf{s}, \mathbf{t}) \in (S^{\mathbb{Z}_{>0}})^3 : \#P_n(\mathbf{r}, \mathbf{s}, \mathbf{t}; \mathbf{w}) > n/2\} \geq 1 - 0.6^n$$

이 성립한다. 다음으로, $(S^{\mathbb{Z}_{>0}})^3$ 위에

$$[(\mathbf{r}, \mathbf{s}, \mathbf{t}) \sim'_n (\bar{\mathbf{r}}, \bar{\mathbf{s}}, \bar{\mathbf{t}})] \Leftrightarrow \left[\begin{array}{l} \text{각각의 } i \in \mathbb{Z}_{>0} \text{ 에 대해 } r_i = \bar{r}_i \text{ 및 } t_i = \bar{t}_i \text{이고,} \\ P_n(\mathbf{r}, \mathbf{s}, \mathbf{t}; \mathbf{w}) \text{의 가장 작은 } n/2 \text{개의 중추 시점이 아닌 모든 } i \text{에 대해 } \bar{s}_i = s_i \text{임} \end{array} \right]$$

라는 동치 관계를 선언하겠다. 보조정리 3.11에서 관찰한 바와 같이, 어떤 중추 시점에서의 \mathbf{s} 의 좌표를 바꾸는 것은 (n 단계) 중추 시점 집합을 바꾸지 않고, 따라서 “가장 작은 $n/2$ 개의 중추 시점”이라는 개념 또한 보존된다. 이러한 연유로 \sim'_n 는 실제로 $(S^{\mathbb{Z}_{>0}})^3$ 위의 동치 관계가 된다. 또한, 각 동치류 위에서 중추 시점 집합의 크기는 일정하므로, 각각의 동치류는 A 에 완전히 포함되거나 A 바깥에 있다. 즉, A 는 특정 동치류들의 합집합으로 나타낼 수 있고, 따라서 \sim_n 는 A 위의 동치관계로 간주할 수 있다.

이제 A 안에 있는 한 \sim_n -동치류 \mathcal{E} 를 고정하면, 그 원소들은 모두 동일한 n 단계 중추 시점 집합 $P_n(\mathcal{E})$ 를 가지는데 편의상 $P_n(\mathcal{E}) = \{i(1) < i(2) < \dots\}$ 로 나타내겠다. 여기서 $\mathcal{E} \subseteq A$ 이므로 $P_n(\mathcal{E})$ 는 최소한 원소 $n/2$ 개를 가짐에 유의하라. 이제

$$\begin{aligned} w'_0 &:= W_{i(1)-1} r_{i(1)} = w_0 \cdot r_1 s_1 t_1 w_1 \cdots r_{i(1)-1} s_{i(1)-1} t_{i(1)-1} w_{i(1)} r_{i(1)}, \\ w'_l &:= t_{i(l)} w_{i(l)} W_{i(l)}^{-1} W_{i(l+1)-1} r_{i(l+1)} \\ &= t_{i(l)} w_{i(l)} \cdot r_{i(l)+1} s_{i(l)+1} t_{i(l)+1} w_{i(l)+1} \cdots r_{i(l+1)-1} s_{i(l+1)-1} t_{i(l+1)-1} w_{i(l+1)} r_{i(l+1)}, \quad (l = 1, \dots, \lfloor n/2 \rfloor) \\ w'_{\lfloor n/2 \rfloor} &:= t_{i(\lfloor n/2 \rfloor)} w_{i(\lfloor n/2 \rfloor)} W_{i(\lfloor n/2 \rfloor)}^{-1} W_n \\ &= t_{i(\lfloor n/2 \rfloor)} w_{i(\lfloor n/2 \rfloor)} \cdot r_{i(\lfloor n/2 \rfloor)+1} s_{i(\lfloor n/2 \rfloor)+1} t_{i(\lfloor n/2 \rfloor)+1} w_{i(\lfloor n/2 \rfloor)+1} \cdots r_n s_n t_n w_n \end{aligned}$$

와 같이 정의하면, 동치관계 \sim_n 의 정의상 w'_0, w'_1, \dots, w'_M 라는 위상동형사상들은 \mathcal{E} 위에서 고정되어 있다. 또한, 각각의 $l = 1, \dots, M$ 에 대해 $w'_l \mathcal{I} \subseteq \mathcal{I}$ 가 성립한다는 것은 보조정리 3.6에서 관찰했다. 또한 동치관계의 정의상, \mathcal{E} 위에서 $s'_l := s_{i(l)}$ 들은 서로 독립적으로 μ -분포를 가진다. 마지막으로,

$$w'_0 s'_1 w'_1 \cdots s'_{\lfloor n/2 \rfloor} w'_{\lfloor n/2 \rfloor} = w_0 r_1 s_1 t_1 w_1 \cdots r_n s_n t_n w_n$$

이 \mathcal{E} 위에서 성립함은 분명하다. 이로써 증명이 끝난다. \square

4. 국소적으로 균일한 지수함수적 감소

이제 다음을 관찰하자.

정리 4.1. 양수 ϵ 자연수 N 및 $\text{Homeo}(S^1)$ 위에 정의된 (ϵ, N) -Schottky 맞춤 측도 μ 가 주어졌을 때, (ϵ, N) -Schottky 맞춤 측도로 이루어진 μ 의 근방이 존재한다.

Proof. 원 위의 서로 겹치지 않는 닫힌 구간 I_1, I_2, J_1, J_2 에 대해, $\mu^{*N}(\mathfrak{S}(I_1, I_2)) > \epsilon$ 및 $\mu^{*N}(\mathfrak{S}(J_1, J_2)) > \epsilon$ 를 만족한다고 하자. 이때, 충분히 작은 $\epsilon' > 0$ 에 대해서는 I_1, I_2, J_1, J_2 각각의 (닫힌) ϵ' -근방들 또한 서로 겹치지 않는다. 이 근방들을 I'_1, I'_2, J'_1, J'_2 로 표시하자. 이제 $\text{Homeo}(S^1)$ 위의 함수 f 를

$$f(\phi) := \max \left(1 - \frac{1}{\epsilon'} d_\infty(\phi, \mathfrak{S}(I_1, I_2)), 0 \right)$$

로 정의하면, 이 함수는 유계이고 C^0 -위상을 기준으로 보았을 때 연속이다. 또, 임의의 확률 측도 η 에 대해

$$\eta(\mathfrak{S}(I_1, I_2)) \leq \mathbb{E}_\eta[f] \leq \eta(\mathfrak{S}(I'_1, I'_2))$$

가 성립한다.

이제 $\mathcal{U}_1 := \{\eta : \mathbb{E}_\eta[f] > \epsilon\}$ 은 μ 를 포함하는 열린 집합인 한편, \mathcal{U}_1 의 임의의 원소 η 는 $\eta(\mathfrak{S}(I'_1, I'_2)) \geq \mathbb{E}_\eta[f] > \epsilon$ 를 만족한다. 비슷한 방식으로 μ 의 근방 \mathcal{U}_2 를 정의해 각각의 $\eta \in \mathcal{U}_2$ 마다 $\eta(\mathfrak{S}(J'_1, J'_2)) > \epsilon$

이게끔 할 수 있다. 그러면 $\mathcal{U}_1 \cap \mathcal{U}_2$ 역시 μ 의 근방인데, 그 각각의 원소는 $\mathfrak{S}(I'_1, I'_2)$ 및 $\mathfrak{S}(J'_1, J'_2)$ 에 ϵ 보다 큰 값을 할당한다.

한편, [Sie76, Proposition 3.1]에 따르면 합성곱 함수(convolution)

$$*N : \mathcal{P}(\text{Homeo}(S^1)) \times \dots \times \mathcal{P}(\text{Homeo}(S^1)) \rightarrow \mathcal{P}(\text{Homeo}(S^1))$$

는 연속이다. $\mathcal{U}_1 \cap \mathcal{U}_2$ 가 μ^{*N} 을 포함하는 열린 집합이므로, $*N$ 에 의한 그 역상 $(*N)^{-1}(\mathcal{U}_1 \cap \mathcal{U}_2)$ 는 μ 의 충분히 작은 근방 \mathcal{N} 의 N 회 곱 $\mathcal{N} \times \dots \times \mathcal{N}$ 을 포함한다. 다시 말해, μ 의 충분히 작은 근방의 임의의 원소 $\mu' \in \mathcal{N}$ 은 $\mu'^{*N} \in \mathcal{U}_1 \cap \mathcal{U}_2$ 를 만족하므로 (ϵ, N) -구간용 Schottky 맞춤 측도이다. \square

REFERENCES

- [Ghy01] Étienne Ghys. Groups acting on the circle. *Enseign. Math. (2)*, 47(3-4):329–407, 2001.
- [Gou22] Sébastien Gouëzel. Exponential bounds for random walks on hyperbolic spaces without moment conditions. *Tunis. J. Math.*, 4(4):635–671, 2022.
- [GV24] Martín Gilabert Vio. Probabilistic tits alternative for circle diffeomorphisms. *arXiv preprint arXiv:2412.08779*, 2024.
- [Mal17] Dominique Malicet. Random walks on $\text{Homeo}(S^1)$. *Comm. Math. Phys.*, 356(3):1083–1116, 2017.
- [Mar00] Gregory Margulis. Free subgroups of the homeomorphism group of the circle. *C. R. Acad. Sci. Paris Sér. I Math.*, 331(9):669–674, 2000.
- [Sie76] Eberhard Siebert. Convergence and convolutions of probability measures on a topological group. *Ann. Probability*, 4(3):433–443, 1976.

CORNELL UNIVERSITY, 583 MALOTT HALL, ITHACA, NY, USA

Email address: inhyeokchoi48@gmail.com