(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2024-0035218
(43) 공개일자 2024년03월15일

(51) 국제특허분류(Int. Cl.)
G06F 7/58 (2006.01)
(52) CPC특허분류
G06F 7/582 (2013.01)
(21) 출원번호 10-2022-0114422
(22) 출원일자 2022년09월08일
심사청구일자 2022년09월08일

(71) 출원인
인하대학교 산학협력단
인천광역시 미추홀구 인하로 100(용현동, 인하대학교)
(72) 발명자
정상태
인천광역시 연수구 송도문화로28번길 28 송도글로벌캠퍼스푸르지오, 104동 1704호
(74) 대리인
이은철, 이수찬

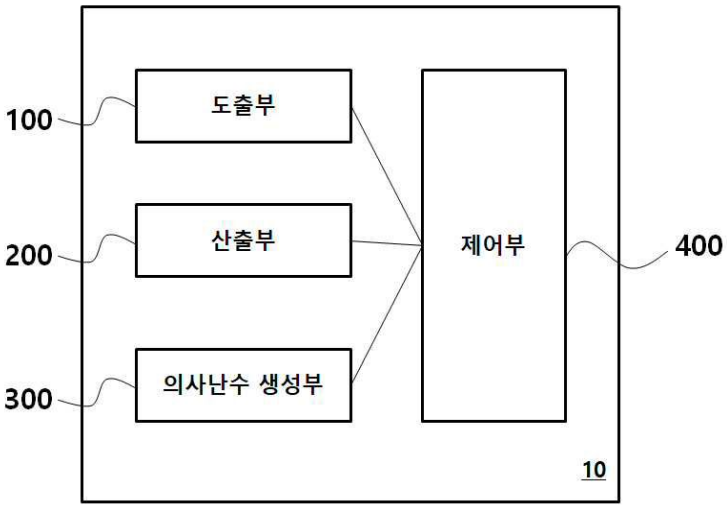
전체 청구항 수 : 총 4 항

(54) 발명의 명칭 **사영직선 위의 유리함수에 기반한 의사난수 생성 장치 및 방법**

(57) 요 약

본 발명은 의사난수 생성 방법과 장치에 관한 것으로, P진 정수환 위의 멱급수에 관련한 사영직선 위의 유리함수에 기반한 의사난수 생성 방법과 장치에 관한 것이다. 본 발명에 따르면, 임의의 소수 p에 대해 P진 정수환 Zp 위에서 수렴하는 멱급수 f에 대한 최소성 조건을 도출하기 위한 도출부, 도출된 최소성 조건을 토대로 좋은 축소를 갖는 유리함수에 대한 사영직선 P1(Qp)에서 최소 2차의 유리함수에 대한 기준을 산출하는 산출부 및 도출된 최소성 기준으로 임의의 소수 p에 대해 유리함수를 기반으로 의사난수를 생성하는 의사난수 생성부를 포함하여, 최소성 기준으로 임의의 소수 p ≥ 5 에 대해 유리함수를 기반으로 의사난수를 생성할 수 있는 효과가 있다.

대 표 도 - 도1



명 세 서

청구범위

청구항 1

임의의 소수 p에 대해 P진 정수환 Zp 위에서 수렴하는 멱급수 f에 대한 최소성 또는 에르고딕 조건을 도출하기 위한 도출부;

상기 도출된 최소성 또는 에르고딕 조건을 토대로 유리함수에 대한 사영직선 위에서 축소를 갖는 2차의 유리함수에 대한 최소성 또는 에르고딕 기준을 산출하는 산출부; 및

상기 도출된 최소성 기준을 만족하는 유리함수를 기반으로 의사난수를 생성하는 의사난수 생성부;를 포함하는 것을 특징으로 하는 사영직선 위의 유리함수에 기반한 의사난수 생성 장치.

청구항 2

제1항에 있어서,

상기 도출부는

상기 p가 임의의 경우, 수렴하는 멱급수 f를 f(z) = g(z)+ph(z) 형식의 합으로 분해하여 급수 f에 대한 최소성을 특성화하는 기준을 도출하는 것을 특징으로 하는 사영직선 위의 유리함수에 기반한 의사난수 생성 장치.

청구항 3

제1항에 있어서,

상기 산출부는 상기 임의의 소수 p에 대해 사영직선 $\mathbb{P}^1(\mathbf{F}_p)$에서 유리함수$\phi$의 축소에 대한 규정된 최소성 조건이 알려져 있는 경우 상기 사영직선 $\mathbb{P}^1(\mathbf{Q}_p)$에서 차수가 $\geq$ 2인 최소 유리함수 ϕ를 특성화하는 것을 특징으로 하는 사영직선 위의 유리함수에 기반한 의사난수 생성 장치.

청구항 4

임의의 소수 p에 대해 P진 정수환 Zp 위에서 수렴하는 멱급수 f에 대한 최소성 또는 에르고딕 조건을 도출하는 단계;

상기 도출된 최소성 또는 에르고딕 조건을 토대로 유리함수에 대한 사영직선 위에서 축소를 갖는 2차의 유리함수에 대한 최소성 또는 에르고딕 기준을 산출하는 단계; 및

상기 도출된 최소성 기준을 만족하는 유리함수를 기반으로 의사난수를 생성하는 단계;를 포함하는 것을 특징으로 하는 사영직선 위의 유리함수에 기반한 의사난수 생성 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 의사난수 생성 방법과 장치에 관한 것으로, 보다 상세하게는 P진 정수환 위의 멱급수에 관련한 사영직선 위의 유리함수에 기반한 의사난수 생성 방법과 장치에 관한 것이다.

배 경 기 술

[0002] 난수는 특정한 배열 순서나 각 항간의 의존성이 없는 임의적인 수열을 말하는데, 이 난수를 컴퓨터에 발생시키면 어떤 알고리즘에 의해 생성되기 때문에 긴 주기를 갖게 된다. 이와 같이 진정한 의미로는 난수가 아니지만 사용상 난수로 간주해도 지장이 없는 난수를 의사 난수라고 한다.

[0003] 생성된 의사난수의 품질을 확보하기 위하여는 난수분포가 치우치지 않는 균일성이 확보되어야 하고, 난수가 일정 주기로 반복되지 않아야 한다.

선행기술문헌

특허문헌

[0004] (특허문헌 0001) 한국등록특허 제1300915호 (2013.08.21.)

발명의 내용

해결하려는 과제

[0005] 본 발명은 상술한 문제를 해결하고자 고안한 것으로, 의사난수를 생성할 수 있는 사영직선위의 유리함수의 최소성에 기반한 의사난수 생성 방법과 장치 및 그 방법을 제공함에 있다.

과제의 해결 수단

[0006] 본 발명에 따른 사영직선 위의 유리함수의 최소성에 기반한 의사난수 생성 장치는 임의의 소수 p에 대해 P진 정수환위에서 수렴하는 멱급수 f에 대한 최소성 조건을 도출하기 위한 도출부; 상기 도출된 최소성 조건을 토대로 유리함수에 대한 사영직선 P1(Qp)에서 축소하는 최소 2차의 유리함수에 대한 최소성 기준을 산출하는 산출부; 및 상기 도출된 최소성 기준으로 임의의 소수 p에 대해 상기 유리함수를 기반으로 난수를 생성하는 난수생성부;를 포함한다.

[0007] 한편, 사영직선 위의 유리함수의 최소성에 기반한 의사난수 생성 방법에 있어서, 임의의 소수 p에 대해 P진 정수환 Zp 위에서 수렴하는 멱급수 f에 대한 최소성 또는 에르고딕 조건을 도출하는 단계; 상기 도출된 최소성 또는 에르고딕 조건을 토대로 유리함수에 대한 사영직선 위에서 축소를 갖는 2차의 유리함수에 대한 최소성 또는 에르고딕 기준을 산출하는 단계; 및 상기 도출된 최소성 기준을 만족하는 유리함수를 기반으로 의사난수를 생성하는 단계;를 포함한다.

발명의 효과

[0008] 본 발명의 일 실시예에 따른 사영직선위의 유리함수에 기반한 의사난수 생성 장치 및 방법은 최소성 기준을 토대로 임의의 소수 p에 대해 유리함수를 기반으로 의사난수를 생성할 수 있는 효과가 있다.

도면의 간단한 설명

[0009] 도 1은 본 발명의 일 실시예에 따른 사영직선위의 유리함수의 최소성에 기반한 의사난수 생성 장치를 나타낸 구성도이다.

도 2는 본 발명의 일 실시예에 따른 사영직선위의 유리함수의 최소성에 기반한 의사난수 생성 방법을 나타낸 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0010] 본 발명의 실시예에서 제시되는 특정한 구조 내지 기능적 설명들은 단지 본 발명의 개념에 따른 실시예를 설명하기 위한 목적으로 예시된 것으로, 본 발명의 개념에 따른 실시예들은 다양한 형태로 실시될 수 있다. 또한, 본 명세서에 설명된 실시예들에 한정되는 것으로 해석되어서는 아니 되며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경물, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다.

[0011] 한편, 본 발명에서 제1 및/또는 제2 등의 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 상기 구성요소들은 상기 용어들에 한정되지는 않는다. 상기 용어들은 하나의 구성요소를 다른 구성요소들과 구별하는 목적으로만, 예컨대 본 발명의 개념에 따른 권리 범위로부터 벗어나지 않는 범위 내에서, 제1 구성요소는 제2 구성요소로 명명될 수 있고, 유사하게 제2 구성요소는 제1 구성요소로도 명명될 수 있다.

[0012] 이하 첨부된 도면을 참조하여 본 발명의 실시예를 설명한다. 본 발명의 실시예를 설명함에 있어서, 관련된 공지 기능 혹은 구성에 대한 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우 그 설명을 생략하였다.

[0013] 본 발명의 일 실시예에 따른 사영직선 위의 유리함수에 기반한 의사난수 생성 장치는 계수 p = 2 또는 3에

대해, 수렴 멱급수에 대한 최소성 조건과 임의의 소수 p ≥ 5 에 대해, 멱급수에 대한 최소성 조건을 도출하고, 도출된 최소성 조건을 토대로 유리함수에 대한 사영직선 P1(Qp)에서 좋은(우수) 축소를 갖는 최소 2차의 유리함수에 대한 최소성 기준을 도출함에 따라, 이러한 최소성 기준을 토대로 소수 p ≥ 5 에 대해, 사영직선 위의 유리함수 기반의 의사 난수를 생성한다. 이에 따라, 임의의 소수 p ≥ 5 인 경우 최소 유리함수에 대해 난수 발생을 특성화할 수 있다.

[0014] 본 발명의 일 실시예에서 먼저 p = 2 또는 3인 경우에 대한 계수의 관점에서 Zp에 대한 수렴 멱급수 f에 대한 최소성 기준을 특성화한다.

[0015] 임의의 소수 p $\geq$ 5 에 대해, f 기준치수 p의 축소를 위해 규정된 최소성 조건이 발견된다면 그러한 급수의 최소성 기준은 명시적으로 얻어질 수 있다.

[0016] 둘째, 우리는 Qp에 대한 사영직선 $\mathbb{P}^1(\mathbf{Q}_p)$에서 좋은 축소와 함께 최소 차수 2의 유리함수에 대한 최소성 기준을 제공한다. 이 기준을 통해 p = 2 또는 3에 대한 계수의 관점에서 $\mathbb{P}^1(\mathbf{Q}_p)$에 대한 이러한 유리함수의 최소성 조건에 대한 완전한 설명을 얻을 수 있다. 임의의 소수 p $\geq$ 5 에 대해 $\mathbb{P}^1(\mathbf{F}_p)$의 축소에 대한 규정된 조건이 알려져 있는 경우 $\mathbb{P}^1(\mathbf{Q}_p)$에서 차수 2의 최소 유리함수를 특성화하는 방법을 제시한다.

[0017] 대수 p-adic 동역학 시스템에 두 가지 기여를 한다. 수렴하는 멱급수 f를 p-dic Weierstrass 준비 정리에서 f(z) = g(z)+ph(z) 형식의 합으로 분해하여 먼저 Zp 위에서 수렴하는 멱급수 f에 대한 최소성 기준을 특성화한다. p = 2 또는 3의 경우에 대한 계수의 관점에서, 임의의 소수 p > 5에 대해, f 모듈로 p의 최소 축소를 위한 규정된 조건이 얻어진다. 그러한 급수의 최소성 기준은 명시적으로 얻어질 수 있다. 둘째, 우리는 Qp 위에서 사영직선 $\mathbb{P}^1(\mathbf{Q}_p)$에서 좋은 축소와 함께 최소 차수 2의 유리함수에 대한 최소성 기준을 제공한다.

[0018] 이 기준을 사용하면 p = 2 또는 3에 대한 계수의 관점에서 $\mathbb{P}^1(\mathbf{Q}_p)$에 대한 유리함수의 최소성 조건에 대한 완전한 설명을 얻을 수 있다. 임의의 소수 p $\geq$ 5 에 대해 $\mathbb{P}^1(\mathbf{F}_p)$에서 ϕ의 축소에 대한 규정된 조건이 알려져 있는 경우 $\mathbb{P}^1(\mathbf{Q}_p)$에서 차수가 $\geq$ 2인 최소 유리함수 ϕ를 특성화하는 방법을 제시한다.

[0019] 본 실시예에 따른 설명은 다음과 같이 구성된다. 먼저, p-adic 나눗셈 알고리즘과 Weierstrass 준비 정리와 같은 Zp에 대한 수렴 멱급수의 해석적 성질과 동력학적 성질에 대한 간략한 검토를 제공한다. 다음으로 p = 2 또는 3 또는 임의의 소수 p $\geq$ 5에 따라 별도의 경우, Zp 위에서 수렴하는 멱급수에 대한 최소성 기준을 특성화한다.

[0020] 다음으로 Qp에 대한 사영직선 $\mathbb{P}^1(\mathbf{Q}_p)$에서 우수한 축소를 갖는 유리함수에 대한 또 다른 최소성 기준을 제공한다. 이 기준을 사용하여 p = 2 또는 3 또는 임의의 소수 p $\geq$ 5에 따라 별도의 경우에 $\mathbb{P}^1(\mathbf{Q}_p)$의 이러한 유리함수에 대한 최소성 조건에 대한 충분한 설명을 제공한다.

[0021] 도 1은 본 발명의 일 실시예에 따른 사영직선위의 유리함수에 기반한 의사난수 생성 장치(10)를 나타낸 구성도이다.

[0022] 본 발명의 일 실시예에 따른 사영직선위의 유리함수에 기반한 의사난수 생성 장치는 도출부(100), 산출부(200), 난수 생성부(300), 제어부(400)를 포함한다.

[0023] 도출부(100)는 임의의 소수 p에 대해 P진 정수환 위에서 수렴하는 멱급수에 대한 최소성 조건을 도출하기 위한 구성이다. 이러한 도출부는 계수 p 가 2 또는 3인 경우에 대한 멱급수 f를 f(z) = g(z)+ph(z) 형식의 합으로 분해하여 먼저 Zp에서 수렴 멱급수 f에 대한 최소성 기준을 특성화의 최소성 기준을 도출한다.

[0024] 산출부(200)는 상기 도출된 최소성 조건을 토대로 유리함수에 대한 사영곡선 P1(Qp)에서 축소하는 최소 2차의 유리함수에 대한 기준수치를 산출하는 구성이다. 이러한 산출부는 임의의 소수 p $\geq$ 5 에 대해 사영곡선 $\mathbb{P}^1(\mathbf{F}_p)$에서 유리함수$\phi$의 축소에 대한 규정된 조건이 알려져 있는 경우 상기 사영직선 $\mathbb{P}^1(\mathbf{Q}_p)$에서 차수가

$\geq$ 2인 최소 유리함수 ϕ 를 특성화한다.

[0025] 난수 생성부(300)는 상기 도출된 최소성 기준으로 임의의 소수 p에 대해 상기 유리함수를 기반으로 의사난수를 생성하는 구성이다.

[0026] 제어부(400)는 상기 도출부(100), 산출부(200), 난수 생성부(300)를 제어하는 구성이다.

[0027] 한편, 도 2는 본 발명의 일 실시예에 따른 사영직선위의 유리함수에 기반한 의사난수 생성 방법을 나타낸 흐름도이다. 도 2에 도시된 바와 같이, 사영직선위의 유리함수에 기반한 의사난수 생성 장치의 제어부가 임의의 소수 p에 대해 수렴 멱급수 Zp 위에서 수렴하는 멱급수 f에 대한 최소성 조건을 도출하는 단계(S10); 상기 도출된 최소성 조건을 토대로 유리함수 Qp에 대한 사영직선 P1(Qp)에서 축소하는 최소 2차의 유리함수에 대한 기준을 산출하는 단계(S30); 및 상기 도출된 최소성 기준으로 임의의 소수 p에 대해 상기 유리함수를 기반으로 의사난수를 생성하는 단계(S50);를 포함한다.

[0028] S10단계에서 제어부는 도출부를 통해 계수 p 가 2 또는 3인 경우, P진 정수환 위에서 수렴하는 멱급수 f를 f(z) = g(z)+ph(z) 형식의 합으로 분해하여 먼저 Zp에서 수렴 멱급수 f에 대한 최소성 기준을 특성화의 최소성 기준을 도출한다.

[0029] S30단계에서 제어부는 산출부를 통해 임의의 소수 p $\geq$ 5 에 대해 사영직선 $\mathbb{P}^1(\mathbf{F}_p)$에서 유리함수$\phi$의 축소에 대한 규정된 조건이 알려져 있는 경우 상기 사영직선 $\mathbb{P}^1(\mathbf{Q}_p)$에서 차수가 $\geq$ 2인 최소 유리함수 ϕ를 특성화한다.

[0030] 이하, 본 발명의 구체적인 실시예를 설명하면 다음과 같다.

[0031] 본 실시예에 따른 사영직선위의 유리함수에 기반한 의사난수 생성 방법은 대수 p-adic 역학 시스템에 두 가지 기여를 한다. 수렴 멱급수 f를 p-dic Weierstrass 준비 정리에서 f(z) = g(z)+ph(z) 형식의 합으로 분해하여 먼저 Zp에서 수렴 멱급수 f에 대한 최소성 기준을 특성화한다. p = 2 또는 3의 경우에 대한 계수의 관점에서. 임의의 소수 p > 5에 대해, f 모듈로 p의 최소 축소를 위한 규정된 조건이 발견된다면 그러한 급수의 최소성 기준은 명시적으로 얻어질 수 있다. 둘째, 본 실시예는 Qp에 대한 사영직선 $\mathbb{P}^1(\mathbf{Q}_p)$에서 좋은 축소와 함께 최소 차수 2의 유리함수에 대한 최소성 기준을 제공한다.

[0032] 이 기준을 사용하면 p = 2 또는 3에 대한 계수의 관점에서 $\mathbb{P}^1(\mathbf{Q}_p)$에 대한 유리함수의 최소성 조건에 대한 완전한 설명을 얻을 수 있다. p = 2에 대한 결과 조건은 다음과 같다. 임의의 소수 p $\geq$ 5 에 대해 $\mathbb{P}^1(\mathbf{F}_p)$에서 ϕ 의 축소에 대한 규정된 조건이 알려져 있는 경우 $\mathbb{P}^1(\mathbf{Q}_p)$에서 차수가 $\geq$ 2인 최소 유리함수 ϕ를 특성화하는 방법을 제시한다.

[0033] 본 실시예에 따른 설명은 다음과 같이 구성된다. 먼저, p-adic 나눗셈 알고리즘과 Weierstrass 준비 정리와 같은 Zp에 대한 수렴 멱급수의 분석적 성질과 동력학적 성질에 대한 간략한 검토를 제공한다. 다음으로 p = 2 또는 3 또는 임의의 소수 p $\geq$ 5에 따라 별도의 경우, P진 정수환 위에서 수열하는 멱급수에 대한 최소성 기준을 특성화한다.

[0034] 다음으로 Qp 위에서 사영직선 $\mathbb{P}^1(\mathbf{Q}_p)$에서 좋은(우수)한 축소를 갖는 유리함수에 대한 또 다른 최소성 기준을 제공한다. 이 기준을 사용하여 p = 2 또는 3 또는 임의의 소수 p $\geq$ 5에 따라 별도의 경우에 $\mathbb{P}^1(\mathbf{Q}_p)$의 이러한 유리함수에 대한 최소성 조건에 대한 충분한 설명을 제공한다.

[0035] Zp의 1-Lipschitz 함수에 대해 설명하면 다음과 같다.

[0036] Zp를 소수 p에 대한 p-adic 정수환이라고 하자. Qp를 p-adic 숫자의 체라고 하고 $|\cdot|$를 가법 부치와 관련된 $\mathbf{Q}_p$의 (정규화된) 절대값, $\mathbf{Q}_p$의 ord_p라고 하여 $|x| = p^{-\mathrm{ord}_p(x)}$ 가 되도록 한다.

[0037] 다음으로 $\mathbf{Z}_p$에서 1-Lipschitz 함수를 정의한다.

[0038] (정의 2.1)

[0039] 만약, $|f(x)-f(y)| \le |x-y|$가 모든 $x, y \in \mathbf{Z}_p$에 대해 성립하는 경우 함수 $f : \mathbf{Z}_p \to \mathbf{Z}_p$는 1-Lipschitz라고 한다.

[0040] 1-Lipschitz 함수 f가 임의의 정수 n $\geq$ 1에 대해 $x \equiv y \pmod{p^n}$일 때 합동 $f(x) \equiv f(y) \pmod{p^n}$가 만족하는 성질과 동일하다. 이 성질은 1-Lipschitz 함수 f: $\mathbf{Z}_p \to \mathbf{Z}_p$가 다음과 같이 정의된 몫 환에서 축소된 축소함수 $f_{/n}\ (n \geq 1)$의 수열을 유도한다.

[0041] $$f_{/n} : \mathbf{Z}_p/p^n\mathbf{Z}_p \to \mathbf{Z}_p/p^n\mathbf{Z}_p, \quad x + p^n\mathbf{Z}_p \mapsto f(x) + p^n\mathbf{Z}_p.$$

[0042] Zp에 대한 1-Lipschitz 함수의 일반적인 예는 Zp의 계수가 있는 다항식과 Taylor 계수의 p-adic 정수성과 같은 특수 기능이 있는 급수가 포함된다. 다음에서 Zp에 수렴하는 Zp 계수 급수의 기본 성질을 살펴볼 수 있다.

[0043] Zp에 대한 수렴 멱급수(Convergent power series on Zp)에 대해 설명하면 다음과 같다.

[0044] 먼저, R을 Qp 또는 Zp라고 하자. $R\langle\langle z\rangle\rangle$는 형식 $\sum_{n=0}^{\infty} a_n z^n$의 모든 멱급수의 집합을 나타낸다. 여기서 모든 n에서 $a_n \in R$이고, $n \to \infty$에서 $|a_n| \to 0$이다. $R\langle\langle z\rangle\rangle$에 속하는 $f(z) = \sum a_n z^n$에 대해 $R\langle\langle z\rangle\rangle$은 f의 노름(norm) $\|f\|$는 다음과 같이 정의된다.

[0045] $$\|f\| = \max_n\{|a_n|\}$$

[0046] 그러면 $R\langle\langle z\rangle\rangle$의 기본 성질은 다음과 같은 (정리 2.2)로 요약될 수 있다.

[0047] (명제 2.2)

[0048] (1) $\mathbf{Z}_p\langle\langle z\rangle\rangle$의 각 급수(series)는 $\mathbf{Z}_p$의 1-Lipchitz 함수이다.

[0049] (2) $\mathbf{Z}_p\langle\langle z\rangle\rangle$는 덧셈, 곱셈, 미분 및 합성 아래 닫혀 있다.

[0050] (3) 각 $f \in \mathbf{Z}_p\langle\langle z\rangle\rangle$는 임의의 $x \in \mathbf{Z}_p$에서 테일러(Taylor) 확장을 가진다.

[0051] 즉, $$f(x+z) = \sum_{m=0}^{\infty} \frac{f^{(m)}(x)}{m!} z^m$$

[0052] 여기서 $\frac{f^{(m)}(x)}{m!}$는 모든 $m \geq 0$에 대한 p-adic 정수이다.

[0053] (4) $\mathbf{Q}_p\langle\langle z\rangle\rangle$는 기준 $\|\cdot\|$에 대한 완전한 노름(norm) 공간이다.

[0054] $\mathbf{Z}_p$에 대한 p-adic 역학 시스템은 삼중$(\mathbf{Z}_p, f, \mu_p)$으로 이해된다. 여기서 f : $\mathbf{Z}_p \to \mathbf{Z}_p$는 측정 가능한 함수이고 μ_p는 $\mathbf{Z}_p$에 대한 Haar 측정값이며 $\mu_p(\mathbf{Z}_p) = 1$과 같이 정규화된다.

[0055] 기본 μ_p 측정 가능 세트는 반경 p^{-k}의 p-adic balls이다.

[0056] 이들은 $a \in \mathbf{Z}_p$ 및 정수 k ≥ 0에 대한 $a + p^k\mathbf{Z}_p$ 형식의 집합이다. 이러한 공(ball)의 측정값은 반경으로 정의된다. 즉, $\mu_p(a + p^k\mathbf{Z}_p) = 1/p^k$.

[0057] (정리 2.3)

[0058] $(\mathbf{Z}_p, f, \mu_p)$를 $\mathbf{Z}_p$에 대한 p-adic 동력학계라고 하면, 함수 f : $\mathbf{Z}_p \longrightarrow \mathbf{Z}_p$는 측도 가능한 각 부분 집합 $M \subset \mathbf{Z}_p$에 대해 $\mu_p(f^{-1}(M)) = \mu_p(M)$인 경우 측도 보존이라고 한다. 측도 보존 함수 f : $\mathbf{Z}_p \to \mathbf{Z}_p$는 다음의 성질을 만족하면 에르고딕이라고 한다. $f^{-1}(M) = M$과 같은 측도 가능한 부분 집합 $M \subset \mathbf{Z}_p$에 대해 $\mu_p(M) = 1$ 또는 $\mu_p(M) = 0$의 성질을 말한다.

[0059] (정리 2.4)

[0060] 연속 함수 f : $\mathbf{Z}_p \to \mathbf{Z}_p$는 x에서 f의 순방향 궤도가 모든 $x \in \mathbf{Z}_p$에 대해 $\mathbf{Z}_p$에서 조밀하다면 $\mathbf{Z}_p$에서 최소라고 한다. S를 N ≥ 1 요소의 유한 집합이라고 하고 f를 S에 대한 자체 함수라고 한다. 또한 f^n이 f의 n번째 반복을 나타내며 f^0은 S의 항등함수(identity map)라는 규칙을 따른다.

[0061] (정리 2.5)

[0062] 함수 f : $\mathcal{S} \to \mathcal{S}$ $\mathcal{S} \to \mathcal{S}$는 $\mathcal{S} \to \mathcal{S}$가 f의 단일 주기를 형성하는 경우 S에서 전이 또는 최소값이다. 즉, $\{x_0, f(x_0) \cdots, f^{N-1}(x_0)\} = S$는 임의의 고정 초기점에 대해 $x_0 \in S$이다.

[0063] $\mathbf{Z}_p$의 1-Lipschitz 함수에는 측도 보존에 대한 몇 가지 동등한 설명이 있다.

[0064] (명제 2.6)

[0065] f : $\mathbf{Z}_p \to \mathbf{Z}_p$를 1-Lipschitz 함수라고 하면 다음과 같다.

[0066]
(1) *f is onto;*
(2) *f is an isometry (i.e.* $|f(x) - f(y)| = |x - y|$ *for all* $x, y \in \mathbf{Z}_p$*);*
(3) $f_{/n}$ *is bijective for all integers* $n \geq 1$*; and*
(4) *f is measure-preserving.*

[0067] ergodicity 또는 Minimality와 관련하여 다음과 같은 동치명제가 있다.

[0068] (명제 2.7)

[0069] f : $\mathbf{Z}_p \to \mathbf{Z}_p$를 측도 보존 1-Lipschitz 함수라고 한다. 그러면 다음과 같다.

[0070]
(1) *f is minimal;*
(2) *f is uniquely ergodic (i.e. there is only one ergodic measure);*
(3) $f_{/n}$ *is transitive on* $\mathbf{Z}_p/p^n\mathbf{Z}_p$ *for all integers* $n \geq 1$*;*
(4) *f is conjugate to the translation,* $t(x) = x + 1$*, on* $\mathbf{Z}_p$*; and*
(5) *f is ergodic.*

[0071] $\mathbf{Z}_p$의 계수가 있는 다항식에서와 같이 $\mathbf{Z}_p\langle\langle z \rangle\rangle$의 멱급수는 명제 2.2의 성질에 의존하는 경우 추가 수정없이 동일한 최소성 기준을 공유한다.

[0072] (명제 2.8)

[0073] f : $\mathbf{Z}_p \to \mathbf{Z}_p$를 n ≥ 1에 대해 $(\mathbf{Z}_p/p^n\mathbf{Z}_p, f_{/n})$이 최소임을 충족하는 $\mathbf{Z}_p\langle\langle z\rangle\rangle$의 멱급수라고 하면 다음과 같다.

[0074] (1) $(\mathbf{Z}_p/p^{n+1}\mathbf{Z}_p, f_{/n+1})$ *is minimal;*
(2) *For all* $x \in \mathbf{Z}_p$, *we have that* $f^{p^n}(x) - x \notin p^{n+1}\mathbf{Z}_p$ *and* $(f^{p^n})'(x) \in 1 + p\mathbf{Z}_p$; *and*

[0075] (3) *There exists* $x \in \mathbf{Z}_p$ *such that* $f^{p^n}(x) - x \notin p^{n+1}\mathbf{Z}_p$, *and* $(f^{p^n})'(x) \in 1 + p\mathbf{Z}_p$.

[0076] (명제 2.9)

[0077] $\mathbf{Z}_p\langle\langle z\rangle\rangle$의 멱급수 f는 $(\mathbf{Z}_p/p^{\mu}\mathbf{Z}_p, f_{/\mu})$가 최소인 경우에만 최소이다. 여기서 p가 2 또는 3이면 μ = 3이고 p ≥ 5이면 μ = 2이다.

[0078] 다음은 $\mathbf{Z}_p$의 멱급수에 대한 최소성 기준(Minimality criterion for convergent power series on Zp)에 대해 설명하기로 한다.

[0079] 먼저, $\mathbf{Z}_p$의 멱급수에 대한 또 다른 최소성 기준을 설명하기로 한다.

[0080] 소수 p에 대해 다음을 설정한다.

[0081] $$\mu := \mu(p) = \begin{cases} 3 & \text{if } p \in \{2,3\}, \\ 2 & \text{if } p \geq 5, \end{cases}$$

[0082] $\delta = \delta_p$를 다음과 같이 정의된 $\mathbb{Z}_p$에 대한 정수 값 함수라고 가정한다.

[0083] $$\delta(z) := \begin{cases} \binom{z}{p^2} = \dfrac{z(z-1)\cdots(z-p^2+1)}{(p^2)!} & \text{if } p \in \{2,3\}, \\ \binom{z}{2p} = \dfrac{z(z-1)\cdots(z-2p+1)}{(2p)!} & \text{if } p \geq 5. \end{cases}$$

[0084] 여기서, δ만큼 축소한다는 관점에서 $\mathbf{Z}_p\langle\langle z\rangle\rangle$의 멱급수에 대한 또 다른 최소 기준을 제공한다. 따라서 이러한 급수의 최소값은 최대 deg(δ)??1 차수인 잉여류환 $\mathbf{Z}/p^{\mu}\mathbf{Z}$의 계수를 갖는 다항식으로 축소될 수 있다.

[0085] (정리 3.1)

[0086] $f(z) \in \mathbf{Z}_p\langle\langle z\rangle\rangle$를 수렴 급수라 하면, f(z) 기준치수 δ(z)의 축소가 Zp에서 최소인 경우에만 f는 Zp에서 최소이다.

[0087] 증명. (deg)!δ(z)는 Zp[z]의 모닉 다항식(monic polynomial)이다. $f(z) \in \mathbf{Z}_p\langle\langle z\rangle\rangle$를 수렴 급수라고 하면 정리 2.3에 의해 다음과 같은 수렴 급수 $q(z) \in \mathbf{Z}_p\langle\langle z\rangle\rangle$와 deg$\delta$보다 작은 차수의 다항식 $r(z) \in \mathbf{Z}_p[z]$가 존재한다.

[0088] $$f(z) = (\deg\delta)!\,\delta(z)q(z) + r(z)$$

[0089] 왜냐하면 (deg δ)! 는 p^{μ}로 나눌 수 있으며 f 와 r은 모두 합동 기준치수법(modulo) p^{μ}이다. 따라서 결과는 명제 2.9로부터 즉시 나온다. 정리 3.1은 Zp[z]의 다항식 결과를 일반화한 것으로 말러 정리를 사용하여 입증할 수 있다.

[0090] p = 2에 대한 특성화(Characterization for p = 2)를 설명하면 다음과 같다.

[0091] 본 실시예는 계수 측면에서 $\mathbf{Z}_2\langle\langle z\rangle\rangle$의 멱급수에 대한 최소성 기준을 제공한다. 이를 위해 $\mathbf{Z}_2\langle\langle z\rangle\rangle$의 멱급수에서도 성립하는 다항식의 최소성 기준을 제시한다.

[0092] (명제 3.2)

[0093] $f \in \mathbf{Z}_2\langle\langle z\rangle\rangle$를 멱급수라 하면, f는 다음 조건이 충족되는 경우에만 $\mathbf{Z}_2$에서 최소이다.

[0094] (M1) $f_{/1}$ is transitive;
(M2) $(f^2)'(0) \equiv 1 \pmod 2$;
(M3) $f^2(0) \in 2\mathbf{Z}_2 \backslash 4\mathbf{Z}_2$; *and*
(M4) $(f^2)''(0) + (f^2)'(0) \equiv 1 \pmod 4$.

[0095] For $f(z) = \sum a_n z^n \in \mathbf{Z}_2\langle\langle z\rangle\rangle$, we set

$$A_0 = \sum_{0<i\in 2\mathbb{Z}} a_i, \quad A_1 = \sum_{i\in 2\mathbb{Z}+1} a_i.$$

[0096] (정리 3.3)

[0097] $f \in \mathbf{Z}_2\langle\langle z\rangle\rangle$를 멱급수라 하면, f는 다음의 조건이 충족되는 경우에만 $\mathbf{Z}_2$에서 최소이다.

[0098]
$$\begin{cases} a_0 \equiv 1 \pmod 2; \\ a_1 \equiv 1 \pmod 2; \\ A_0 + A_1 \equiv 1 \pmod 4; \text{ and} \\ a_1 + 2a_2 + A_1 \equiv 2 \pmod 4. \end{cases}$$

[0099] 증명. 본 실시예에에 따른 명제 3.2의 네 가지 조건이 다음 조건과 동일하다는 것을 보여줌으로써 시작한다.

[0100]
$$\begin{cases} (\mathrm{M1}') \quad f(0) \equiv 1 \pmod 2 \quad \text{and} \quad f(1) \equiv 0 \pmod 2; \\ (\mathrm{M2}') \quad f'(0) \equiv f'(1) \equiv 1 \pmod 2; \\ (\mathrm{M3}') \quad f(0) + f(1) \equiv 3 \pmod 4; \text{ and} \\ (\mathrm{M4}') \quad f'(0) + f'(1) + f''(0) + f''(1) \equiv 2 \pmod 4. \end{cases}$$

[0101] 이제 다음의 조건이 조건(M1)-(M4)과 동일하다는 것을 보여주어야 한다.

[0102] 정리 3.3의 조건은 $\mathbf{Z}_2$에 대한 다항식에 대한 다음 따름정리(Corollary)의 조건과 동일하다는 것이 쉽게 증명된다.

[0103] (따름정리 3.4)

[0104] $f(z)=\sum a_n z^n \in \mathbf{Z}_2\langle\langle z\rangle\rangle$ 를 멱급수라고 하면 f는 다음의 조건들이 충족되는 경우에만 $\mathbf{Z}_2$에서 최소이다.

[0105]
$$\begin{cases} a_0 \equiv 1 \pmod 2; \\ a_1 \equiv 1 \pmod 2; \\ A_1 - a_1 \equiv 2a_2 \pmod 4; \text{ and} \\ A_0 - a_2 \equiv a_1 + a_2 - 1 \pmod 4. \end{cases}$$

[0106] 증명. 정리 3.3에서 $2-a_1 \equiv a_1 \pmod 4$, $2a_2 \equiv -2a_2 \pmod 4$ 에 따른다.

[0107] (정리 3.5)

[0108] 본 발명의 일 실시예에 따른 사영직선 위의 유리함수에 기반한 의사난수 생성 장치 및 방법은 Zp에 대한 1-Lipschitz 함수의 최소성 기준에 대한 연구를 수행하여, 특히 단항 다항식과 떨어지는 계승의 관계를 이용하여 따름정리(Corollary) 3.4의 최소성 기준을 제시한다.

[0109] p = 3에 대한 특성화(Characterization for p = 3)를 설명하면 다음과 같다.

[0110] 이제 p = 3의 경우를 살펴보면, 계수 측면에서 다항식 $f \in \mathbf{Z}_3[x]$ 의 완전한 최소성 기준을 제공한다. 이에 주로 $\mathbf{Z}_3$에 대한 다항식 및 멱급수에 대한 다음 최소성 기준을 기반으로 한다.

[0111] (정리 3.6)

[0112] $f \in \mathbf{Z}_3\langle\langle z\rangle\rangle$ 를 멱급수라 하면, f는 다음의 조건을 만족하는 경우에만 $\mathbf{Z}_3$에서 최소이다.

(M1) $f_{/1}$ *is transitive (i.e.,* f *is transitive modulo* 3);

(M2) $\left(f^3\right)'(0) \equiv 1 \pmod 3$ *(i.e.,* $f'\left(f^2(0)\right) f'(f(0)) f'(0) \equiv 1 \pmod 3$*)*;

(M3) $f^3(0) \in 3\mathbf{Z}_3 \backslash 9\mathbf{Z}_3$; *and*

(M4) $3\left(f^3\right)''(0) - 2f^3(0) \not\equiv 0 \pmod 9$.

[0113]

[0114] 멱급수 $f(z)=\sum a_n z^n \in \mathbf{Z}_3\langle\langle z\rangle\rangle$ 에 대해 다음을 설정한다.

[0115]
$$a_0 = a_0, \quad A_1 = \sum_{i \in 2\mathbf{Z}+1} a_i, \quad A_0 = \sum_{0<i \in 2\mathbf{Z}} a_i,$$

[0116]
$$D_0 = a_1, \quad D_1 = \sum_{i=1}^{\infty} i a_i, \quad D_2 = \sum_{i=1}^{\infty} i a_i 2^i$$

[0117] $0 \le k \le 5$ 에 대해 다음을 설정한다.

[0118]
$$E_k = \sum_{i>0} a_{6i+k}$$

[0119] a0, A1, A0, D0, D1, D2 및 E_k 의 정의에서 다음 선형 기준치수법(modulo) 3을 12개의 변수 [a0,...,a5,E0,...,E5]에 대해 설정한다. 상수 열 벡터 $[a_0, A_1, A_0, D_0, D_1, D_2]^t$ 기준 치수법 3, 여

기서 t는 행렬의 전치를 나타낸다.

[0120] (식 3.1)

$$\begin{cases} a_0 \equiv a_0, \\ a_1 + a_3 + a_5 + E_1 + E_3 + E_5 \equiv A_1, \\ a_2 + a_4 + E_0 + E_2 + E_4 \equiv A_0, \\ a_1 \equiv D_0, \\ a_1 + 2a_2 + a_4 + 2a_5 + E_1 + 2E_2 + E_4 + 2E_5 \equiv D_1, \\ a_1 + a_2 + 2a_4 + 2a_5 + E_1 + E_2 + 2E_4 + 2E_5 \equiv D_2. \end{cases} \pmod 3$$

[0121]

[0122] 주어진 열 벡터 $[a_0, A_1, A_0, D_0, D_1, D_2]^t$ 기준 치수법 3에 대한 선형 시스템 이후, 본 실시예에 따른 해(solution)를 사용하여 계수 측면에서 멱급수 f(z)의 최소성 기준을 제공한다.

[0123] (정리 3.7)

[0124] $f \in \mathbf{Z}_3\langle\langle z\rangle\rangle$를 멱급수(convergent series)라 하면, f는 다음 조건(i)-(viii) 중 하나를 충족하는 경우에 $\mathbf{Z}_3$에서 최소이다.

Setting $[a_0, A_1, A_0, D_0, D_1, D_2] \bmod 3 = [\cdot, \cdot, \ldots, \cdot]$,

(i) $[1,1,0,1,1,1], A_0 + 6 \not\equiv 0 \pmod 9$, $A_0 + 6 \not\equiv 6a_2 + 3\sum_{j\geq 0} a_{6j+2} \pmod 9$;
(ii) $[1,1,0,1,2,2], A_1 + a_0 + 4 \not\equiv 0 \pmod 9$, $A_1 + a_0 + 4 \not\equiv 3a_2 + 3\sum_{j\geq 0} a_{6j+5} \pmod 9$;
(iii) $[1,1,0,2,1,2], A_1 + 2a_0 + 3 \not\equiv 0 \pmod 9$, $A_1 + 2a_0 + 3 \not\equiv 6a_2 + 3\sum_{j\geq 0} a_{6j+5} \pmod 9$;
(iv) $[1,1,0,2,2,1], A_0 + 2a_0 + 4 \not\equiv 0 \pmod 9$, $A_0 + 2a_0 + 4 \not\equiv 3a_2 + 3\sum_{j\geq 0} a_{6j+2} \pmod 9$;
(v) $[2,1,0,1,1,1], A_0 + 3 \not\equiv 0 \pmod 9$, $A_0 + 3 \not\equiv 6a_2 + 3\sum_{j\geq 0} a_{6j+2} \pmod 9$;
(vi) $[2,1,0,1,2,2], A_1 + 2a_0 + 7 \not\equiv 0 \pmod 9$, $A_1 + 2a_0 + 7 \not\equiv 6a_2 + 3\sum_{j\geq 0} a_{6j+5} \pmod 9$;
(vii) $[2,1,0,2,1,2], A_0 + 2a_0 + 5 \not\equiv 0 \pmod 9$, $A_0 + 2a_0 + 5 \not\equiv 3a_2 + 3\sum_{j\geq 0} a_{6j+2} \pmod 9$; *and*
(viii) $[2,1,0,2,2,1], A_1 + a_0 + 6 \not\equiv 0 \pmod 9$, $A_1 + a_0 + 6 \not\equiv 3a_2 + 3\sum_{j\geq 0} a_{6j+5} \pmod 9$.

[0125]

[0126] 증명. f가 최소라고 가정하면 정리 3.6의 (M1)과 (M2)를 모두 만족하는 모든 가능한 벡터 [a0, A1, A0, D0, D1, D2] mod 3을 찾아야 한다. 약간의 계산으로 다음을 구성하는 가능한 모든 8개의 행 벡터 [a0, A1, A0, D0, D1, D2] mod 3 집합를 나열할 수 있다.

[0127] (식 3.2)

$$Type\ I : [1,1,0,1,1,1], [1,1,0,1,2,2], [1,1,0,2,1,2], [1,1,0,2,2,1];$$

[0128] $$Type\ II : [2,1,0,1,1,1], [2,1,0,1,2,2], [2,1,0,2,1,2], [2,1,0,2,2,1].$$

[0129] f 기준수치법 3의 전이성은 유형 I 및 II를 유도하며, 전자는 f(0) 1(mod 3)이고 후자는 f(0) 2(mod 3)이다. 각 유형에 대해 [D0D1D2] mod 3은 (M2)에서 D0, D1, D2 1(mod 3)을 만족한다. 전체적으로 상수 벡터 [a0, A1, A0, D0, D1, D2] mod 3에 대해 8가지 선택 사항이 있다. 따라서 모든 8개의 상수 벡터 [a0, A1, A0, D0, D1, D2] mod 3에 대해 (3.3)의 선형 시스템에 대한 모든 해(solution) 유형 I/II의 순서로 나타나는 [a0, ..., a5] mod 3을 동시에 결정할 수 있다.

[0130] 참고로, 수학의 분야 중의 정수론에서 배우게 되는 모듈러(modulo)는 어떤 정수 A를 다른 정수 N으로 나누면 나오는 나머지 라는 뜻으로 식으로는 A modulo N 이라고 적는다. modulo를 줄여서 mod라고도 적는다.

[0131] (식 3.3)

$$\left(\begin{array}{cccccccccccc|cccccccc} 1&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&2&2&2&2\\ 0&1&0&1&0&1&0&1&0&1&0&1&1&1&1&1&1&1&1&1\\ 0&0&1&0&1&0&1&0&1&0&1&0&0&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0&0&0&0&0&1&1&2&2&1&1&2&2\\ 0&1&2&0&1&2&0&1&2&0&1&2&1&2&1&2&1&2&1&2\\ 0&1&1&0&2&2&0&1&1&0&2&2&1&2&2&1&1&2&2&1 \end{array}\right)$$

[0132]

[0133] 위의 선형 시스템의 증가 계수 행렬의 축소된 행 사다리꼴은 동시에 다음과 같이 주어진다.

[0134] (식 3.4)

$$\left(\begin{array}{cccccccccccc|cccccccc} 1&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&2&2&2&2\\ 0&1&0&0&0&0&0&0&0&0&0&0&1&1&2&2&1&1&2&2\\ 0&0&1&0&0&0&2&0&1&0&0&0&0&0&1&2&0&0&1&2\\ 0&0&0&1&0&0&0&2&0&1&0&0&0&1&0&0&0&1&0&0\\ 0&0&0&0&1&0&2&0&0&0&1&0&0&0&2&1&0&0&2&1\\ 0&0&0&0&0&1&0&2&0&0&0&1&0&2&2&2&0&2&2&2 \end{array}\right)$$

[0135]

[0136] 선택한 선형 시스템에 대한 해(solution)의 매개변수 표현은 다음 관계식으로 제공된다.

[0137] (식 3.5)

$$\begin{cases} a_0 = r_0 + 3z_0\,, \\ a_1 = r_1 + 3z_1\,, \\ a_2 = r_2 + 3z_2 + E_0 + 2E_2, \\ a_3 = r_3 + 3z_3 + E_1 + 2E_3, \\ a_4 = r_4 + 3z_4 + E_0 + 2E_4, \\ a_5 = r_5 + 3z_5 + E_1 + 2E_5, \end{cases}$$

[0138]

[0139] 여기서 $[r_0, \cdots, r_5]^t$ 는 (3.4)에서 축소된 형태의 8개 상수 열 벡터 중 하나이다. 각 열의 항목에서 다항식 $r(z) = \sum_{i=0}^{5} r_i z^i$ 를 형성하고 이러한 모든 다항식은 유형 I 및 II의 순서로 나열된다.

$$P_8 := \{1+z, 1+z+z^3+2z^5, 1+2z+z^2+2z^4+2z^5, 1+2z+2z^2+z^4+2z^5,$$
$$2+z, 2+z+z^3+2z^5, 2+2z+z^2+2z^4+2z^5, 2+2z+2z^2+z^4+2z^5\}.$$

[0140]

[0141] 이 관계식(3.5)을 f(z)에 대입하면 다음이 생성된다.

[0142] (식 3.6)

$$f(z) = r(z) + H(z)$$

[0143]

[0144] 여기서, $r(z) \in P_8$,

[0145] (식 3.7)

$$H(z) = 3\sum_{i=0}^{5} z_i z^i + (E_0 + 2E_2)z^2 + (E_1 + 2E_3)z^3 + (E_0 + 2E_4)z^4 + (E_1 + 2E_5)z^5 + \sum_{i=6}^{\infty} a_i z^i$$

[0146]

[0147] 따라서 (3.7)에서 H의 다음과 같은 중요한 성질은 쉽게 확인되며 이후 계산에서 묵시적으로 많이 사용된다.

- $H(z) \equiv H'(z) \equiv 0 \pmod 3$.
- $H(z + t(z)) \equiv H(z) \pmod 9$ if $t(z) \equiv 0 \pmod 3$.

[0148]

[0149] 다음을 계산하는 것이 유용하다.

[0150] (식 3.8)

$$H(0) = 3z_0 = a_0 - r_0$$

[0151]

[0152] (식 3.9)

$$H(1) = 3\sum_{i=0}^{5} z_i + 3\sum_{i=0}^{5} E_i = a_0 + A_0 + A_1 - r(1).$$

[0153]

[0154] (식 3.10)

$$H(2) \equiv 3\sum_{i=0}^{5} (z_i + E_i)(-1)^i \equiv a_0 + A_0 - A_1 - r(2) \pmod 9$$

[0155]

[0156] (식 3.11)

$$H(0) + H(1) + H(2) \equiv 6(z_2 + z_4) + 6E_0 + 6E_2 + 6E_4 \equiv 2(A_0 - r_2 - r_4) \pmod 9$$

[0157]

[0158] (M3)에 대해 계수 a_i 로 $f^3(0)$ 모듈로 9를 계산한다. (3.6)의 수렴 급수에 대한 Taylor 정리는 다음을 산출한다.

[0159] (식 3.12)

$$\begin{aligned} f^2(z) &\equiv f(r(z) + H(z)) \equiv f(r(z)) + H(z)r'(r(z)) \\ &\equiv r^2(z) + H(r(z)) + H(z)r'(r(z)) \pmod 9 \end{aligned}$$

[0160]

[0161] 유사하게, $f^3(z)$ 를 한 번 더 계산하면 다음과 같은 결과를 얻을 수 있다.

$$f^3(z) \equiv r^3(z) + H(r^2(z)) + H(r(z))r'(r^2(z)) + H(z)r'(r(z))r'(r^2(z)) \pmod 9$$

[0162]

[0163] 그러므로,

[0164] (식 3.13)

$$f^3(0) \equiv r^3(0) + r'(r^2(0))r'(r(0))H(0) + r'(r^2(0))H(r(0)) + H(r^2(0)) \pmod 9$$

[0165]

[0166] 각 $r \in P_8$ 에 대해 r(0) 모듈로 9를 계산하면 다음이 제공된다.

[0167] (식 3.14)

$$f^3(0) \equiv \begin{cases} 3+H(0)+H(1)+H(2) \pmod 9 & \text{if } Case\ 1; \\ H(0)+2H(1)+H(2) \pmod 9 & \text{if } Case\ 2; \\ 2H(0)+2H(1)+H(2) \pmod 9 & \text{if } Case\ 3; \\ 2H(0)+H(1)+H(2) \pmod 9 & \text{if } Case\ 4; \\ 6+H(0)+H(1)+H(2) \pmod 9 & \text{if } Case\ 5; \\ 3+H(0)+H(1)+2H(2) \pmod 9 & \text{if } Case\ 6; \\ 6+2H(0)+H(1)+H(2) \pmod 9 & \text{if } Case\ 7; and \\ 6+2H(0)+H(1)+2H(2) \pmod 9 & \text{if } Case\ 8. \end{cases}$$

[0168]

[0169] (식 3.8)-(식 3.11)의 값을 사용하여 (식 3.14)의 표현식을 a_i 로 다시 작성할 수 있다.

[0170] (식 3.15)

$$f^3(0) \equiv \begin{cases} 2(A_0+6) \pmod 9 & \text{if } Case\ 1; \\ A_1+a_0+4 \pmod 9 & \text{if } Case\ 2; \\ A_1+2a_0+3 \pmod 9 & \text{if } Case\ 3; \\ 2(A_0+5a_0+1) \pmod 9 & \text{if } Case\ 4; \\ 2(A_0+3) \pmod 9 & \text{if } Case\ 5; \\ 2(A_1+5a_0+1) \pmod 9 & \text{if } Case\ 6; \\ 2(A_0+5a_0+8) \pmod 9 & \text{if } Case\ 7; and \\ 2(A_1+a_0+6) \pmod 9 & \text{if } Case\ 8. \end{cases}$$

[0171]

[0172] 이제 다음과 같이 $(f^3)''(0) \pmod 3$ 의 값을 계산하여 (M4)로 전환한다.

[0173] (식 3.16)

$$\begin{aligned} (f^3)''(0) &= f'(f^2(0))f'(f(0))f''(0)+f'(f^2(0))f'(0)^2f''(f(0))+f'(f(0))^2f'(0)^2f''(f^2(0)) \\ &\equiv f'(f^2(0))f'(f(0))f''(0)+f'(f^2(0))f''(f(0))+f''(f^2(0)) \pmod 3, \end{aligned}$$

[0174]

[0175] $\lambda \not\equiv 0 \pmod 3$ 에 대해 $\lambda^2 \equiv 1 \pmod 3$ 이므로, $f(x) \equiv r(x) \pmod 3$ $f'(x) \equiv r'(x) \pmod 3$ 이기 때문에, (식 3.16)으로부터 다음을 갖게 된다.

[0176] (식 3.17)

$$(f^3)''(0) \equiv r'(r^2(0))r'(r(0))f''(0)+r'(r^2(0))f''(r(0))+f''(r^2(0)) \pmod 3$$

[0177]

[0178] (식 3.13)과 (식 3.17)에서 r'-관련 계수 사이에 완벽한 일치가 있음을 주목하고, (식 3.17)의 공식을 사용하여 다음을 얻는다.

[0179] (식 3.18)

$$(f^3)''(0) \equiv \begin{cases} f''(0)+f''(1)+f''(2) \pmod 3 & \text{if } Case\ 1; \\ f''(0)+2f''(1)+f''(2) \pmod 3 & \text{if } Case\ 2; \\ 2f''(0)+2f''(1)+f''(2) \pmod 3 & \text{if } Case\ 3; \\ 2f''(0)+f''(1)+f''(2) \pmod 3 & \text{if } Case\ 4; \\ f''(0)+f''(1)+f''(2) \pmod 3 & \text{if } Case\ 5; \\ f''(0)+f''(1)+2f''(2) \pmod 3 & \text{if } Case\ 6; \\ 2f''(0)+f''(1)+f''(2) \pmod 3 & \text{if } Case\ 7; and \\ 2f''(0)+f''(1)+2f''(2) \pmod 3 & \text{if } Case\ 8. \end{cases}$$

[0180]

[0181] 직접 계산 결과:

$$f''(0) = 2a_2, \quad f''(1) \equiv -\sum_{j\geq 0} a_{3j+2} \,(\mathrm{mod}\, 3), \quad f''(2) \equiv -\sum_{j\geq 0} (-1)^j a_{3j+2} \,(\mathrm{mod}\, 3)$$

[0182]

[0183] 이 ID를 (식 3.18)에 적용하면 다음이 생성된다.

[0184] (식 3.19)

$$(f^3)''(0) \equiv \begin{cases} 2a_2 + \sum_{j\geq 0} a_{6j+2} \pmod 3 & \text{if } Case\ 1; \\ 2a_2 + 2\sum_{j\geq 0} a_{6j+5} \pmod 3 & \text{if } Case\ 2; \\ a_2 + 2\sum_{j\geq 0} a_{6j+5} \pmod 3 & \text{if } Case\ 3; \\ a_2 + \sum_{j\geq 0} a_{6j+2} \pmod 3 & \text{if } Case\ 4; \\ 2a_2 + \sum_{j\geq 0} a_{6j+2} \pmod 3 & \text{if } Case\ 5; \\ 2a_2 + \sum_{j\geq 0} a_{6j+5} \pmod 3 & \text{if } Case\ 6; \\ a_2 + \sum_{j\geq 0} a_{6j+2} \pmod 3 & \text{if } Case\ 7; and \\ a_2 + \sum_{j\geq 0} a_{6j+5} \pmod 3 & \text{if } Case\ 8. \end{cases}$$

[0185]

[0186] 따라서 정리 3.7과 같이 (M3)의 동치 조건은 각 경우에 대해 (식 3.15)로 주어진다. (M4)와 관련하여 (식 3.15) 및 (식 3.19)에서 $2f^3(0) \not\equiv 3(f^3)''(0) \pmod 9$를 계산하면 정리 3.7에 표시된 대로 각 경우에 대해 동치 조건이 생성된다.

[0187] (따름정리 3.8)

[0188] $f(z) = a_0 + a_1 z + a_2 z^2 + 3^2 h(z) \in \mathbf{Z}_3\langle\langle z\rangle\rangle$를 어떤 수렴 급수 $h(z) \in \mathbf{Z}_3\langle\langle z\rangle\rangle$에 대한 수렴 급수라고 하면, f는 $a_0 \not\equiv 0 \pmod 3$, $a_1 \equiv 1 (\mathrm{mod}\ 3)$, $\frac{a_2}{3} \not\equiv a_0 \pmod 3$인 경우에 $\mathbf{Z}_3$에서 최소이다.

[0189] 증명. 최소 급수 f의 경우 방정식 $f'(z) \equiv 0 \pmod 3$에는 모듈로 3의 근이 없으므로 $a_2 \equiv 0 \pmod 3$이 있다. 축소 유리함수 $\bar{f}(z) \equiv a_0 + a_1 z \text{ modulo } 3$이 최소이므로 우리는 $a_0 \not\equiv 0 \pmod 3$ 및 $a_1 \equiv 1 \pmod 3$을 얻는다. 따라서 f는 정리 3.7의 경우 (i) 또는 경우 (v)에 속한다. 전자의 경우, 모든 i $\geq$ 3 에 대해 $a_i \equiv 0 \pmod{3^2}$이므로 충족되어야 하는 두 조건은 관계 $A_0 + 6 \equiv 0 \pmod{3^2}$과 동일하며 이는 $\frac{a_2}{3} \not\equiv a_0 \pmod 3 \text{ as } a_0 \equiv 1 \pmod 3$ 정리 3.7의 경우 (i)에 대해. 비슷한 방법으로 후자의 경우도 가능하므로 증명이 완료된다.

[0190] p $\geq$ 5에 대한 특성화(Characterization for p $\geq$ 5)를 설명하면 다음과 같다. $f \in \mathbf{Z}_p\langle\langle z\rangle\rangle$를 $\mathrm{wideg}(f)$=N와 표준 1의 수렴 급수라 하면, (정리 2.1)에서와 같이 p-adic Weierstrass 정리(정리 2.4)에 의해 f는 합으로 표현된다.

[0191] $$f(z) = g(z) + ph(z)$$

[0192] 여기서 g(z)는 차수가 N인 다항식 $\in \mathbf{Z}_p[x]$ 이고, h(z)는 $\mathbf{Z}_p\langle\langle z\rangle\rangle$에서 수렴 급수이다. 이 하위 섹션 전체에서 p는 소수 5이고 f의 분해를 사용하여 완전한 이러한 수렴 급수 $f \in \mathbf{Z}_p\langle\langle z\rangle\rangle$의 최소성 기준에 대한 설

명을 제공한다. 이를 위해 수렴 급수 $f \in \mathbf{Z}_p\langle\langle z\rangle\rangle$에 대한 최소성 기준을 호출한다.

[0193] (정리 3.9)

[0194] $f \in \mathbf{Z}_p\langle\langle z\rangle\rangle$를 수렴 급수라 하면, f는 다음의 조건을 충족하는 경우에 Zp에 최소이다.

$$(i)\ f\ is\ transitive\ modulo\ p;$$

$$(ii)\ (f^p)'(0) \equiv 1 \pmod{p};\ and$$

$$(iii)\ f^p(0) \in p\mathbf{Z}_p \setminus p^2\mathbf{Z}_p.$$

[0195]

[0196] 이것은 정리 2.8 및 2.9에 따른다.

[0197] 정리 3.9는 다음에서 최소 수렴 급수 $f \in \mathbf{Z}_p\langle\langle z\rangle\rangle$의 대체 기준으로 이어진다.

[0198] (정리 3.10)

[0199] $f(z) = g(z) + ph(z)$에서의 $f \in \mathbf{Z}_p\langle\langle z\rangle\rangle$를 차수의 N과 노름(norm) 1의 수렴 급수라 하면, f는 다음 조건을 충족하는 경우에 $\mathbf{Z}_p$에서 최소이다.

[0200] (1) g(z)는 차수 N의 전이 다항식 모듈로 p이며, 전체 주기는 $(\xi_0, \xi_1, \cdots, \xi_{p-1})$로 표시된다.

[0201] 여기서 $\{\xi_0 := 0, \xi_1, \cdots, \xi_{p-1}\} = \mathbf{F}_p$

[0202] (2) $$\prod_{i=0}^{p-1} g'(i) \equiv 1 \pmod{p};\ and$$

[0203] (3) (식 3.20)

[0204] $$\sum_{i=1}^{p}(g(\xi_{i-1})-\xi_i)w_i + p\sum_{i=1}^{p} h(\xi_{i-1})w_i \not\equiv 0 \pmod{p^2}$$

[0205] 여기서, $$w_i = \prod_{j=i}^{p-1} g'(\xi_j) \quad \text{for } 1 \le i \le p-1, w_p = 1 \text{ and } \xi_p = 0$$

[0206] 증명. $f(z) \equiv g(z) \pmod{p}$ 및 $f'(z) \equiv g'(z) \pmod{p}$에 대한 관찰과 함께 증명을 위해 정리 3.9를 참조하면 다음과 같다. 이는 $f(z) = g(z) + ph(z)$의 분해 직후에 뒤따른다. 동력학계(Zp, f)이 최소라고 가정하면, 정리 3.9의 조건(i)은 다항식 g(z)가 전이 모듈로 p임을 명시하는 주장(1)과 동일하다. 전체 주기는 위와 같이 $(\xi_0, \xi_1, \cdots, \xi_{p-1})$로 표시된다. g modulo p의 전이성에서 연쇄 규칙은 정리 3.9의 조건 (ii)가 주장 (2), $\prod_{i=0}^{p-1} g'(i) \equiv 1 \pmod{p}$와 동일하다는 것을 나타낸다. 주장 (3)의 경우, f의 분해를 사용하여 $f^p(0) \text{ modulo } p^2$에 대한 공식을 찾는다. 먼저 Taylor 정리는 다음을 제공한다.

$$f^2(0) \equiv f(g(0)+ph(0)) \equiv f(g(0))+ph(0)f'(g(0))$$
$$\equiv g^2(0)+ph(g(0))+ph(0)g'(g(0)) \pmod{p^2}.$$

[0207]

[0208] 다시 한번,

$$f^3(0) \equiv f(g^2(0)+ph(g(0))+ph(0)g'(g(0)))$$
$$\equiv g^3(0)+ph(g^2(0))+(ph(g(0))+ph(0)g'(g(0)))\,g'(g^2(0))$$
$$\equiv g^3(0)+ph(g^2(0))+ph(g(0))g'(g^2(0))+ph(0)g'(g(0))g'(g^2(0)) \pmod{p^2}$$

[0209]

[0210] 이 프로세스를 반복하면 모듈로 p2가 있다.

$$f^p(0) \equiv g^p(0)+ph(g^{p-1}(0))+ph(g^{p-2}(0))g'(g^{p-1}(0))+ph(g^{p-3}(0))g'(g^{p-2}(0))g'(g^{p-1}(0))+\cdots$$

[0211] $$+ph(g(0))g'(g^2(0))g'(g^3(0))\cdots g'(g^{p-1}(0))+ph(0)g'(g(0))g'(g^2(0))\cdots g'(g^{p-1}(0)).$$

[0212] $1 \le i \le p-1$ 와 $w_p = 1$ 에 대해서,

[0213] $w_i = \prod_{j=i}^{p-1} g'(g^j(0)) \equiv \prod_{j=i}^{p-1} g'(\xi_j) \pmod{p}$ 설정은 다음과 같다.

[0214] (식 3.21)

$$f^p(0) \equiv g^p(0)+p\sum_{i=1}^{p} w_i h(\xi_{i-1}) \pmod{p^2}$$

[0215]

[0216] 일부 $m \in \mathbf{Z}_p$ 에 대해 $z = g^{p-1}(0) = \xi_{p-1}+mp$ 에서 g의 테일러 전개를 사용하여 다음을 얻는다.

$$g^p(0) = g(g^{p-1}(0)) = g(\xi_{p-1}+mp) \equiv g(\xi_{p-1})+mpg'(\xi_{p-1})$$
$$\equiv g(\xi_{p-1})+(g^{p-1}(0)-\xi_{p-1})g'(\xi_{p-1}) \pmod{p^2}$$

[0217]

[0218] $g^{p-2}(0)$ 에 적용된 동일한 주장은 다음과 같다.

$$g^{p-1}(0) \equiv g(\xi_{p-2})+(g^{p-2}(0)-\xi_{p-2})g'(\xi_{p-2}) \pmod{p^2}$$

[0219]

[0220] 위의 $g^p(0)$ 식에 $g^{p-1}(0)$ 을 대입하면 다음과 같이 된다.

[0221] $$g^p(0) \equiv g(\xi_{p-1})+(g(\xi_{p-2})-\xi_{p-1})g'(\xi_{p-1})+(g^{p-2}(0)-\xi_{p-2})g'(\xi_{p-2})g'(\xi_{p-1}) \pmod{p^2}$$

[0222] 동일한 논증을 귀납적으로 적용하여 다음 관계를 얻는다.

[0223] $$g^p(0) \equiv g(\xi_{p-1})+(g(\xi_{p-2})-\xi_{p-1})w_{p-1}+\cdots+(g(\xi_0)-\xi_1)w_1 \pmod{p^2}$$

[0224] 여기서 $w_i\ (1 \le i \le p-1)$ 는 위에 정의된다. $g^p(0)$ 에 대한 표현을 (식 3.21)에 대입하면 다음을 얻는다.

$$f^p(0) \equiv \sum_{i=1}^{p} (g(\xi_{i-1}) + ph(\xi_{i-1}) - \xi_i) w_i \pmod{p^2}$$

[0225]

[0226] 여기서 w_p = 1이고 ξ_p = 0이다. 그런 다음, 주장 (3)은 정리 3.9의 조건 (3)과 f의 분해를 따른다.

[0227] (정리 3.11)

[0228] f(z) = g(z) + ph(z)로 분해하여 모든 차수의 최소 다항식 f를 특성화하는 방법을 제시했다. 따라서 정리 3.10의 조건 (1)과 (2)를 만족하는 d보다 작은 차수의 모든 다항식 g가 명시적으로 발견된다면 고정 차수의 모든 최소 다항식을 분류할 수 있다. 수렴 급수의 경우 정리 3.10의 조건 (1)과 (2)에서 차수 N의 다항식 g에서 미리 $\sum_{i=1}^{p}(g(\xi_{i-1}) - \xi_i)w_i \text{ modulo } p^2$ 의 정확한 값을 찾을 수 있다. 그런 다음 우리는 수렴 급수 h(z)의 무한히 많은 계수를 포함할 수 있는 $p\sum_{i=1}^{p} h(\xi_{i-1})w_i \text{ modulo } p^2$ 의 값과 관련된 조건을 찾아야 한다.

[0229] 또한 정리 3.10의 조건 (3)은 다음과 같다.

[0230] (식 3.22)

$$\sum_{i=1}^{p} (f(\xi_{i-1}) - \xi_i) w_i \not\equiv 0 \pmod{p^2}$$

[0231]

[0232] 위의 최소성 기준을 사용하여 Zp에 대한 특수 형식의 수렴 급수의 최소성 조건을 제공한다.

[0233] (정리 3.12)

[0234] $f(z) = \sum_{n>0} a_n z^n \in \mathbf{Z}_p\langle\langle z \rangle\rangle$ 를 다음 조건을 충족하는 멱급수라고 하면,

$$\begin{cases} a_0 \not\equiv 0 \pmod{p}; \\ a_1 \equiv 1 \pmod{p}; \\ a_i \equiv 0 \pmod{p} \text{ for } i \geq 2; \text{ and} \\ \sum\limits_{\substack{i \in (p-1)\mathbb{Z} \\ i \neq 0}} a_i \not\equiv p a_0 \pmod{p^2}. \end{cases}$$

[0235]

[0236] 그런 다음 f는 Zp에서 최소이다.

[0237] 증명 : 여기서, 가정(assumption)에서 우리는 f가 차수(widegree) 1과 노름(norm) 1의 수렴 급수이고, f가 f(z) = g(z)+ph(z) 형식임을 주목한다. 여기서 $g(z) = a_0 + a_1 z$ 일부 수렴 급수 h(z). f modulo p의 축소 유리함수는 $g(z) \equiv a_0 + z \text{ modulo } p$ 이므로 g는 전이 선형 다항식 modulo p이며 전체 주기는 $(\xi_0, \xi_1, \cdots, \xi_{p-1}) = (0, z_0, 2z_0, \cdots, (p-1)z_0)$ 로 표시된다. 여기서 $z_0 := a_0 \pmod{p}$. 이후, $g'(z) \equiv 1 \pmod{p}$ 이므로 정리 3.10의 조건(1)과 (2)가 충족된다. 정리 3.10의 조건(3)이 성립한다는 것을 보여주기 위해, $w_i = 1$ 이기 때문에 관계 $\sum_{i=1}^{p}(f(\xi_{i-1}) - \xi_i) \not\equiv 0 \pmod{p^2}$ 가 (식 3.22)에서 성립함을 보여준다. 문제의 합계를 다음과 같이 계산한다.

$$\sum_{i=1}^{p} f(\xi_{i-1}) = \sum_{i=1}^{p}\sum_{n\geq 0} a_n((i-1)z_0)^n = \sum_{n\geq 0}\sum_{i=1}^{p} a_n((i-1)z_0)^n$$
$$= pa_0 + a_1 z_0 \frac{p(p-1)}{2} + \sum_{n=2}^{\infty} a_n z_0^n \left(\sum_{i=1}^{p-1} i^n\right).$$

[0238]

[0239] 이를 사용하여,

[0240] $\sum_{i=1}^{p-1} i^n \equiv -1 \pmod{p}$

[0241] 만약 $(p-1) \mid n$, 그리고 0 그렇지 않으면 다음을 추론한다.

$$\sum_{i=1}^{p} f(\xi_{i-1}) \equiv pa_0 + \sum_{i=1}^{p} \xi_i - \sum_{\substack{n\in(p-1)\mathbb{Z} \\ n\neq 0}} a_n \pmod{p^2}$$

[0242]

[0243] 이 일치는 $\sum_{i=1}^{p}(f(\xi_{i-1})-\xi_i) \not\equiv 0 \pmod{p^2}$ 가 증명을 종료하는 네 번째 가정과 동일함을 의미한다.

[0244] (정리 3.13)

[0245] $f(z) = a_0 + a_1 z + a_2 z^2 + p^2 h(z) \in \mathbf{Z}_p\langle\langle z\rangle\rangle$ 를 일부 수렴 급수 $h(z) \in \mathbf{Z}_p\langle\langle z\rangle\rangle$ 에 대한 수렴 급수라고 하면, f는 $a_0 \not\equiv 0 \pmod{p}, a_1 \equiv 1 \pmod{p}$, $a_2 \equiv 0 \pmod{p}$ 경우에만 $\mathbf{Z}_p$에서 최소이다.

[0246] 증명. 여기서, f가 최소이면,

[0247] 축소 유리함수 $\bar{f}(z) \equiv a_0 + a_1 z + a_2 z^2 \text{ modulo } p$ 가 최소이고 f의 도함수가 모듈로 p는 근(root)이 없다. 후자를 설명하기 위해 $a_2 \equiv 0 \pmod{p}$ 를 얻는다.

[0248] 그렇지 않으면 $f'(z) \equiv a_1 + 2a_2 z \equiv 0 \pmod{p}$ 에 근(root)이 있다.

[0249] 따라서 $\bar{f}(z) \equiv a_0 + a_1 z \pmod{p}$ 는 $a_0 \not\equiv 0 \pmod{p}$ 및 $a_1 \equiv 1 \pmod{p}$ 일 때 정확히 최소임을 알 수 있다.

[0250] 축소가 우수한 유리함수에 대한 최소성 기준(Minimality criterion for rational maps with good reduction)을 설명하면 다음과 같다.

[0251] 참고로 배경 및 또 다른 최소성 기준(Background and another minimality criterion)을 설명하기로 한다. 최소 차수가 2인 유리함수 $\phi \in \mathbf{Q}_p(z)$ 는 Qp에 대한 사영직선 P1에서 동력학계를 유도하며, 이는 $(\mathbb{P}^1(\mathbf{Q}_p), \phi)$로 표시된다. $\phi(E) \subset E$, 그리고 $\phi|_E$ 를 E로 제한된 유리함수이라고 하자. 하위 시스템 $(E, \phi|_E)$은 아래의 임의의 지점의 궤도가 E에서 조밀한 경우 최소라고 한다. 이 섹션에서는 다음에서 유리

함수의 최소성을 완전히 조사한다. ($\mathbb{P}^1(\mathbf{Q}_p), \phi$) p = 2 또는 3의 경우 계수의 관점에서. 그렇게 하려면 Qp에 대한 사영직선의 필수 구성 요소와 그에 대한 유리함수를 잘 축소하여 간략하게 살펴볼 필요가 있다.

[0252] $\mathbb{P}^1(\mathbf{Q}_p)$의 모든 점은 한 쌍의 점 [x0, x1]에 의해 동차 좌표로 제공될 수 있다. 여기서 두 요소 모두 0이 아니다. $\mathbb{P}^1(\mathbf{Q}_p)$의 점은 각 정점이 p + 1 모서리의 끝점을 갖는 무한 (p + 1)-Cayley 수형도의 경계점으로 볼 수 있음을 보여준다. 리만 구(Riemann sphere)에서와 같이 $\mathbb{P}^1(\mathbf{Q}_p)$은 P = [x0, x1] 및 Q = [y0, y1] $\in \mathbb{P}^1(\mathbf{Q}_p)$에 대해 다음과 같이 정의된 p-adic 코드 메트릭을 갖는다.

[0253] $$\rho(P,Q) = \frac{|x_0y_1 - x_1y_0|}{\max\{|x_0|,|x_1|\}\max\{|y_0|,|y_1|\}}$$

[0254] 수렴 급수에서와 같이 $\mathbb{P}^1(\mathbf{Q}_p)$에 1-Lipschitz 연속 유리함수를 정의한다.

[0255] (정리 4.1)

[0256] 유리함수 $\phi : \mathbb{P}^1(\mathbf{Q}_p) \to \mathbb{P}^1(\mathbf{Q}_p)$는 $P, Q \in \mathbb{P}^1(\mathbf{Q}_p)$에 대해 $\rho(\phi(P), \phi(Q)) \leq \rho(P, Q)$가 유지되는 경우 $\mathbb{P}^1(\mathbf{Q}_p)$은 1-Lipschitz 연속(1-Lipschitz continuous)이라고 한다.

[0257] 링 Zp에 대한 제한은 p-adic 절대값에 불과하므로 정리 4.1의 $\mathbb{P}^1(\mathbf{Q}_p)$에 대한 1-Lipschitz 유리함수는 Zp에 대한 1-Lipschitz 함수의 완전 일반화이다.

[0258] 차수가 d $\geq$ 2인 $\mathbb{P}^1(\mathbf{Q}_p)$에 대한 유리함수는 공통 근이 없는 두 다항식 f 및 g $\in \mathbf{Z}_p[z]$의 몫으로 표현되므로 f 또는 g의 계수 중 하나 이상이 Zp의 단위이다. 유리함수는 정규화된 형식으로 작성되며 정도는 ϕ로 표시되는 $\deg(\phi) = \max\{\deg(f), \deg(g)\}$로 정의된다. $\bar{\phi}$로 표시되는 $\deg(\bar{\phi}) = \max\{\deg(\bar{f}), \deg(\bar{g})\}$로 정의된다.

[0259] 여기서 $\bar{\phi}(z) = \frac{\bar{f}(z)}{\bar{g}(z)} \in \mathbf{F}_p(z)$는 기약 다항식 $\bar{f}(z)$, $\bar{g}(z)$는 공통 근이 없다.

[0260] (정리 4.2)

[0261] 유리함수 $\phi : \mathbb{P}^1(\mathbf{Q}_p) \to \mathbb{P}^1(\mathbf{Q}_p)$은 deg($\phi$) = deg($\bar{\phi}$)가 유지되는 경우 우수한 축소 계수 p를 갖는다고 한다. 그렇지 않으면 나쁜 축소가 있다고 한다.

[0262] 유리함수는 p-adic chordal metric에 대해 $\mathbb{P}^1(\mathbf{Q}_p)$에서 Lipschitz 연속인 것으로 알려져 있으며 특히 다음과 같은 결과를 얻는다.

[0263] (정리 4.3)

[0264] $\mathbb{P}^1(\mathbf{Q}_p)$에 대한 축소가 좋은 유리함수인 경우, 1-Lipschitz 연속이다.

[0265] $a \in \mathbb{P}^1(\mathbf{Q}_p)$을 중심으로 반지름이 p^{-n}인 공을 다음과 같이 표시한다.

[0266] $$B_n(a) := \left\{ x \in \mathbb{P}^1(\mathbf{Q}_p) \,\middle|\, \rho(x,a) \le p^{-n} \right\}$$

[0267] 그런 다음 사영직선 $\mathbb{P}^1(\mathbf{Q}_p)$은 p + 1개의 서로 다른 반경의 볼로 구성된다.

[0268] $$\mathbb{P}^1(\mathbf{Q}_p) = B_1(\infty) \bigsqcup \left(\bigsqcup_{i=0}^{p-1} B_1(i) \right)$$

[0269] 각 n $\geq$ 1 에 대해 반지름의 모든 볼은 반지름의 볼로 구성되므로 $\mathbb{P}^1(\mathbf{Q}_p)$은 $\mathfrak{B}_n$으로 표시된 반지름의 분리된 볼 집합으로 구성된다. $\mathbb{P}^1(\mathbf{Q}_p)$은 무한 수형도이므로 각 n에 대해 집합 $\mathfrak{B}_n$과 수준 n에 있는 수형도의 꼭짓점 집합 사이에는 일대일 대응이 있다.

[0270] 모든 1-Lipschitz 연속 유리함수 $\phi : \mathbb{P}^1(\mathbf{Q}_p) \to \mathbb{P}^1(\mathbf{Q}_p)$은 $\phi_n : \mathfrak{B}_n \to \mathfrak{B}_n$변환을 유도한다. 다음과 같이 정의된다.

[0271] $$\phi_n(B_n(x)) = B_n(\phi(x)) \text{ for all } x \in \mathbb{P}^1(\mathbf{Q}_p)$$

[0272] 수형도 수준에서 ϕ의 정점 집합이 각 수준에서 불변인 수형도에 변환을 유도하는 것으로 나타난다.

[0273] (정리 4.4)

[0274] $\phi : \mathbb{P}^1(\mathbf{Q}_p) \to \mathbb{P}^1(\mathbf{Q}_p)$은 1-Lipschitz 연속 유리함수라고 하면, ($\mathbb{P}^1(\mathbf{Q}_p), \phi$)는 모든 정수 n $\geq$ 1 에 대해 유한 시스템($\mathfrak{B}_n, \phi_n$)이 최소인 경우에만 최소이다.

[0275] $\mathbb{P}^1(\mathbf{F}_p)$을 p 요소의 유한체 $\mathbf{F}_p$에 대한 사영직선이라고 하자. 환원은 $\mathbb{P}^1(\mathbf{F}_p)$에서 자신으로의 변환을 유도한다. 전체에서 ϕ^k는 의 k번째 반복을 나타낸다.

[0276] (정리 4.5)

[0277] $\phi \in \mathbf{Q}_p(z)$를 좋은 축소를 갖는 $\deg \phi \geq 2$의 유리함수라고 하자. 그러면 동력학계($\mathbb{P}^1(\mathbf{Q}_p), \phi$)은 다음 조건이 충족되는 경우에만 최소이다.

[0278] *(1) the reduction $\bar{\phi}$ is transitive on $\mathbb{P}^1(\mathbf{F}_p)$;*

(2) $(\phi^{(p+1)})'(0) \equiv 1 \pmod{p}$ and $|\phi^{(p+1)}(0)| = 1/p$; and

(3) additionally, for the cases of $p = 2$ or 3, $|\phi^{(p+1)p}(0)| = 1/p^2$.

[0279] 정리 4.5의 결과로 다항식에 대한 명제 2.9와 유사한 결과를 도출했다.

[0280] (정리 4.6)

[0281] $\phi : \mathbb{P}^1(\mathbf{Q}_p) \to \mathbb{P}^1(\mathbf{Q}_p)$은 축소가 좋은 $\deg \phi \geq 2$의 유리함수이다. 그러면 동력학계

($\mathbb{P}^1(\mathbf{Q}_p), \phi$)은 다음 조건이 충족되는 경우에만 최소이다.

[0282] *(1) the system $(\mathfrak{B}_3, \phi_3)$ is minimal for $p = 2$ or 3; and*

(2) the system $(\mathfrak{B}_2, \phi_2)$ is minimal for $p \geq 5$.

[0283] 주요 결과 중 하나로 정리 4.5와 동일한 ($\mathbb{P}^1(\mathbf{Q}_p), \phi$)의 또 다른 최소성 기준을 명시한다. 우리의 결과는 정리 4.5의 조건 (3)이 더 간단한 것으로 대체될 수 있음을 보여준다. 이 조건은 A와 B의 계수의 관점에서 정규화된 형식으로 작성된 유리함수 $\phi = \frac{A}{B}$의 최소성 기준을 찾는 데 사용된다.

[0284] (정리 4.7)

[0285] $\phi \in \mathbf{Q}_p(z)$를 좋은 축소를 갖는 deg $\phi \geq 2$의 유리함수라고 하면 동력학계($\mathbb{P}^1(\mathbf{Q}_p), \phi$)은 다음 조건이 충족되는 경우에만 최소이다.

(1) the reduction $\bar{\phi}$ is transitive on $\mathbb{P}^1(\mathbf{F}_p)$;

(2) $(\phi^{(p+1)})'(0) \equiv 1 \pmod{p}$ and $|\phi^{(p+1)}(0)| = 1/p$; and

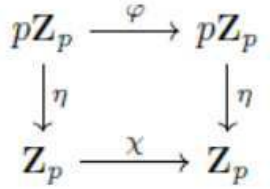
(3) additionally,

for $p = 2$, $(\phi^{(p+1)})'(0) + (\phi^{(p+1)})''(0) \equiv 1 \pmod{p^2}$;

for $p = 3$, $\frac{1}{p}\phi^{(p+1)}(0) - \frac{1}{2}(\phi^{(p+1)})''(0) \not\equiv 0 \pmod{p}$.

[0286]

[0287] 본 실시 예에서는 충분조건(suciency)를 증명하는 것으로 시작한다. 모든 조건이 충족되었다고 가정하면 동력학계($p\mathbf{Z}_p, \phi^{p+1}$)이 ($\mathbb{P}^1(\mathbf{Q}_p), \phi$)의 최소값을 의미하기 때문에 최소 값임을 보여준다. 이전 실시 예에서, $\varphi := \phi^{p+1} = \sum_{i=0}^{\infty} \lambda_i z^i$는 모든 i $\geq$ 1에 대해 $\lambda_0 = pu_0 \in p\mathbf{Z}_p$ 및 $\lambda_i \in \mathbf{Z}_p$인 pZp에 대한 1-Lipschitz 연속 급수이다. 그러면 증명은 동력학계가 $\chi(z) = \sum_{i=0}^{\infty} u_i z^i \in \mathbf{Z}_p\langle\langle z \rangle\rangle$는 Zp에서 최소이다. 여기서 모든 i $\geq$ 0에 대해 $u_i = p^{i-1}\lambda_i$이다. 동력학계($p\mathbf{Z}_p, \varphi$)이 변환 $\eta(z) = z/p$에 의해 시스템 ($\mathbf{Z}_p, \chi$)에 켤레되기 때문이다. 즉,



[0288]

[0289] 이전의 모든 결과로부터 최소성 조건은 p에만 의존하는 계수의 관점에서 완전히 제공된다. 먼저 p = 2의 경우를 처리한다. 정리 3.3에서 최소가 되기 위한 필요 충분 조건은 다음과 같다.

[0290] $u_0 \equiv 1 \pmod{p}, \quad u_1 \equiv 1 \pmod{p}, \quad u_3 \equiv 2u_2 \pmod{p^2}, \quad u_1 + u_2 \equiv 1 \pmod{p}$

[0291] 관계 $u_i = p^{i-1}\lambda_i$ 를 통해 다음 합동과 동일한다.

[0292] $$\frac{\lambda_0}{p} \equiv 1 \pmod{p}, \quad \lambda_1 \equiv 1 \pmod{p}, \quad \lambda_1 + 2\lambda_2 \equiv 1 \pmod{p^2}$$

[0293] 이것들은 p = 2에 대한 모든 가정의 재언급에 불과하다는 것이 분명한다. p = 3의 경우; 다음과 같은 경우에 급수가 최소인 것과 동일한 관계를 통해 추론 3.8을 따른다.

[0294] $$u_0 \not\equiv 0 \pmod{p}, \quad u_1 \equiv 1 \pmod{p}, \quad \frac{u_2}{p} \not\equiv u_0 \pmod{p}.$$

[0295] 다음 합동에 해당한다.

[0296] $$\frac{\lambda_0}{p} \not\equiv 0 \pmod{p}, \quad \lambda_1 \equiv 1 \pmod{p}, \quad \lambda_2 \not\equiv \frac{\lambda_0}{p} \pmod{p}$$

[0297] 다시 말하지만, 이러한 조건은 현재 사례에 대한 모든 가정의 재작성일 뿐이다. p $\geq$ 5에 대한 나머지 경우는 다음에서 쉽게 따른다.

[0298] $$\frac{\lambda_0}{p} \not\equiv 0 \pmod{p}, \quad \lambda_1 \equiv 1 \pmod{p},$$

[0299] 이는 Corollary 3.13을 통해 멱급수 x의 최소값과 동일한 조건이며,

[0300] $$u_0 \not\equiv 0 \pmod{p}, \quad u_1 \equiv 1 \pmod{p}.$$

[0301] ($\mathbb{P}^1(\mathbf{Q}_p), \phi$)가 최소라고 가정한다. 그런 다음 변수를 변경하여 필요한 경우 $\phi(0) = \infty$ 및 $\phi(\infty) = 1$이라고 가정할 수 있다. 유도 시스템($\mathfrak{B}_n, \phi_n$)은 모든 정수 n $\geq$1에 대해 최소이다. 특히, ($\mathfrak{B}_1, \phi_1$)의 최소성은 축소가 첫 번째 주장인 $\mathbb{P}^1(\mathbf{F}_p)$에서 추이적임을 의미한다. 그러면 공 $B_1(0) = p\mathbf{Z}_p$는 ϕ^{p+1}의 불변 집합이므로 pZp에 대한 수렴 급수로서 ϕ^{p+1}은 다음과 같이 표현된다.

[0302] (식 3.23)

[0303] $$\phi^{p+1}(z) = \lambda_0 + \lambda_1 z + \lambda_2 z^2 + \lambda_3 z^3 + \cdots$$

[0304] 여기서 모든 i $\geq$ 1에 대해 $\lambda_0 = pu_0 \in p\mathbf{Z}_p$ 및 $\lambda_i \in \mathbf{Z}_p$이다. p = 2에 대해 (식 3.23)의 급수는 $z \in 2\mathbf{Z}_2$에 대해 다음을 제공한다.

[0305] $$\phi^3(z) \equiv \phi(1) + (\phi^3)'(0)z + \frac{(\phi^3)''(0)}{2}z^2 \pmod{8}.$$

[0306] 값 $\phi^3(0) = \phi^{p+1}(1)$을 반복하면 다음을 얻는다.

[0307] $$\phi^6(0) \equiv \phi(1) + (\phi^3)'(0)\phi(1) + \frac{(\phi^3)''(0)}{2}\phi(1)^2 \pmod 8.$$

[0308] p = 2인 정리 4.5에서 다음을 얻는다.

[0309] $$(\phi^3)'(0) \equiv 1 \pmod 2, \quad \phi(1) \equiv 2 \pmod 4, \quad \phi^6(0) \equiv 4 \pmod 8.$$

[0310] 이러한 관계를 통해 조건 $\phi^6(0) \equiv 4 \pmod 8$ 가 다음과 동일하다는 것을 추론할 수 있다.

[0311] $$1 + (\phi^3)'(0) + \frac{(\phi^3)''(0)}{2}\phi(1) \equiv 2 \pmod 4.$$

[0312] 차례로, $(\phi^3)''(0) \in 2\mathbf{Z}_2$ 라는 작은 관찰에 기초하여 이것은 다음과 같다.

[0313] $$(\phi^3)'(0) + (\phi^3)''(0) \equiv 1 \pmod 4,$$

[0314] 따라서 p = 2인 경우의 증명을 완료한다.

[0315] (식 4.23)의 다음 방정식에 의존하여 p = 3인 경우의 증명을 시작한다.

[0316] $z \in 3\mathbf{Z}_3$에 대해,

[0317] (식 3.24)

[0318] $$\phi^4(z) \equiv \lambda_0 + \lambda_1 z + \lambda_2 z^2 \pmod{3^3}.$$

[0319] p = 3인 정리 4.5에서 파생된 주장 $\phi^4(0) \in 3\mathbf{Z}_3 \setminus 9\mathbf{Z}_3$ 은 $\lambda_0/3 \not\equiv 0 \pmod 3$ 과 동일하고 파생된 주장 $(\phi^4)'(0) \equiv 1 \pmod 3$ 는 $\lambda_1 \equiv 1 \pmod 3$과 같다.

[0320] 이제 우리는 세 번째 파생된 주장 $\phi^{12}(0) \in 9\mathbf{Z}_3 \setminus 27\mathbf{Z}_3$ 이 $\lambda_2 \not\equiv \frac{1}{3}\lambda_0 \pmod 3$과 동일하다는 것을 보여주는데, 이는 정리에서 우리의 주장과 동등하다는 것을 쉽게 보여준다. $\lambda_0 \equiv 0 \pmod 3$을 염두에 두고 $\lambda_0 = \phi^4(0)$ 을 (식 4.24)에 대입하면 다음이 산출된다.

[0321] $$\phi^8(0) \equiv \lambda_0(1 + \lambda_1 + \lambda_0\lambda_2) \pmod{3^3}.$$

[0322] 절차 $\phi^8(0)$ 을 (식 3.24)에 다시 대입하면 다음이 제공된다.

[0323] $$\phi^{12}(0) \equiv \lambda_0(1 + \lambda_1 + \lambda_1^2) + \lambda_0^2\lambda_2(\lambda_1 + (1 + \lambda_1)^2) \pmod{3^3}.$$

[0324] $\lambda_1 \equiv 1 \pmod 3$, $\lambda_0 = 3u_0$ 이므로 다음과 같다.

$$\phi^{12}(0) \equiv 3^2 u_0(1 + 2u_0\lambda_2) \pmod{3^3}.$$

[0325]

[0326] $u_0 \not\equiv 0 \pmod 3$ 이후에 선행 합동은 조건 $\phi^{12}(0) \in 9\mathbf{Z}_3 \setminus 27\mathbf{Z}_3$ 이 다음과 같다는 것을 추론하도록 한다.

$$1 + 2u_0\lambda_2 \not\equiv 0 \pmod 3,$$

[0327]

[0328] 이것은 또한 우리의 주장인 $\lambda_2 \not\equiv \frac{1}{3}\lambda_0 \pmod 3$과 동일한다. 나머지 경우는 정리 4.5에서 따르기 때문에 증명이 완료된다.

[0329] (정리 4.8)

[0330] 정리 4.7의 p = 2인 경우의 조건 (3)은 수렴 급수 f에 대한 (3.2)의 조건 $(f^2)'(0) + (f^2)''(0) \equiv 1 \pmod p$에 해당한다. 정리 4.7의 p = 3인 경우 조건 (3)은 정리 3.6의 (M4)에서 수렴 급수 f에 대한 조건 $\frac{1}{3}f^3(0) - \frac{1}{2}(f^3)''(0) \not\equiv 0$ 에 해당한다.

[0331] P1(Qp)의 연구 대상에 대해 다음 형식의 차수 d $\geq$ 2의 유리함수 $\phi(z) \in \mathbf{Q}_p(z)$ 를 고려한다.

[0332] (식 3.25)

$$\phi(z) = \frac{a_0 + a_1 z + \cdots + a_{d-1}z^{d-1} + a_d z^d}{b_1 z + \cdots + b_{d-1}z^{d-1} + b_d z^d},$$

[0333]

[0334] $\phi(0) = \infty$ 및 $\phi(\infty) = 1$, 여기서 모든 $0 \leq i \leq d$. 에 대해 $a_i, b_i \in \mathbf{Q}_p$, 이 가정에서, a0은 Qp에서 0이 아니고 ad = bd = 1. 유리함수 $\phi \in \mathbf{Q}_p(z)$ 의 경우 $\phi(z)$ 차수가 2 이상인 경우 고정된 주기를 갖는 주기정의 개수는 유한이다. 따라서 $z_0, \phi(z_0)$ 과 $\phi^2(z_0)$ 이 구별되는 요소 $z_0 \in \mathbf{Q}_p$가 존재한다. $\phi_g = g \circ \phi \circ g^{-1}$ 형태의 선형 분수 변환 g에 의한 ϕ의 켤레라고 하자.

$$g(z) = \frac{(z - z_0)(\phi^2(z_0) - \phi(z_0))}{(z - \phi(z_0))(\phi^2(z_0) - z_0)}.$$

[0335]

[0336] 그런 다음 $\phi_g(0) = \infty$, $\phi_g(\infty) = 1$ 및 $g(z_0) = 0, g(\phi(z_0)) = \infty$이기 때문에 $g(\phi^2(z_0)) = 1$ 및 $g(\phi^2(z_0)) = 1$인지 직접 확인한다. ϕ_g를 ϕ로 바꿀 때, (4.25)에서 원하는 형태의 유리함수를 취하지만 반드시 좋은 축소가 있는 것은 아니라는 점에 유의해야한다.

[0337] p = 2에 대한 특성화(Characterization for p = 2)를 설명하면 다음과 같다.

[0338] Fan et al.는 계수의 관점에서 합리성 유리함수 $\phi \in \mathbf{Q}_2(z)$의 최소성 조건에 대한 완전한 설명을 제공했다. 이 하위 절에서 우리는 정리 4.7을 사용하여 그러한 유리함수의 또 다른 최소성 기준을 제공한다.

[0339] (식 3.25)에서와 같이 Fan et al. 형식의 차수 $d \geq 2$ 의 유리함수만 고려하고,

[0340] (식 3.26)

[0341] $$\phi(z) = \frac{A(z)}{B(z)} = \frac{a_0 + a_1 z + \cdots + a_{d-1} z^{d-1} + z^d}{b_1 z + \cdots + b_{d-1} z^{d-1} + z^d} \in \mathbf{Q}_2(z)$$

[0342] $\phi(0) = \infty$ 및 $\phi(\infty) = 1$ 을 $a_i, b_i \in \mathbf{Q}_2$ 로 만족, $b_0 = 0$ for $0 \leq i \leq d-1$: (3.26)과 관련된 다음 수량을 설정한다.

[0343] $$A_\phi = \sum_{i \geq 0} a_i,\ B_\phi = \sum_{i \geq 1} b_i,\ A_{\phi,1} = \sum_{i \geq 0} a_{2i+1},\ A_{\phi,2} = \sum_{i \geq 0} a_{4i+1} \text{ and } A_{\phi,3} = \sum_{i \geq 0} a_{4i+3}$$

[0344] (정리 4.9)

[0345] ϕ 를 (식 3.26)과 같이 정의하면, ϕ 의 축소가 양호하고 P1(Q2)에서 최소인 경우:

[0346] (식 3.27)

[0347] $$\begin{cases} (C1)\ a_i, b_i \in \mathbf{Z}_2,\ for\ 0 \leq i \leq d-1, \\ (C2)\ a_0 \equiv 1 \pmod 2, \\ (C3)\ B_\phi \equiv 1 \pmod 2, \\ (C4)\ A_\phi \equiv 2 \pmod 4, \\ (C5)\ A_{\phi,1} \equiv 1 \pmod 2, \\ (C6)\ b_1 \equiv 1 \pmod 2, \\ (C7)\ a_{d-1} - b_{d-1} \equiv 1 \pmod 2, \\ (C8)\ a_0 b_1 (a_{d-1} - b_{d-1})(A_{\phi,2} - A_{\phi,3}) B_\phi + \\ \qquad 2(b_2 - a_1 + a_{d-2} - b_{d-2} + b_{d-1} + A_{\phi,3}) \equiv 1 \pmod 4 \end{cases}$$

[0348] 반대로, 이러한 조건은 ϕ 가 $\mathbb{P}^1(\mathbf{Q}_2)$ 에서 1-Lipschitz 연속적이고 최소임을 의미한다.

[0349] 정리 4.9와 병행하여 다음과 같은 최소성 기준을 명시한다.

[0350] (정리 4.10)

[0351] (식 3.26)과 같이 정의하자. 축소가 양호하고 $\mathbb{P}^1(\mathbf{Q}_2)$ 에서 최소인 경우 정리 4.9의 조건 (C1)-(C8)은 다음 조건으로 대체된 (C8)으로 충족된다.

[0352] $$(C8')\ A_{\phi,1} + B_\phi + a_{d-1} + b_{d-1} + a_0 + b_1 + 2(b_2 - a_1 + a_{d-2} - b_{d-2}) \equiv 1 \pmod 4$$

[0353] 반대로, 조건 (C1)-(C7) 및 (C8')은 ϕ 가 $\mathbb{P}^1(\mathbf{Q}_2)$ 에서 1-Lipschitz 연속적이고 최소임을 의미한다.

[0354] 정리 4.10을 증명하기 전에 두 가지 중요한 점을 언급한다. $\mathbf{Z}_2$ 의 5개의 홀수 요소 $x_i (1 \leq i \leq 5)$ 에 대해 다음과 같다.

[0355] $$\prod_{i=1}^{5} x_i \equiv \sum_{i=1}^{5} x_i \pmod 4$$

[0356] 여기서, $A_{\phi,1} = A_{\phi,2} + A_{\phi,3}$ 에 주목하면 두 개의 조건 (C8)과 (C8')이 정리 4.9와 정리 4.10의 나머

지 조건과 함께 서로 동등하다는 것이 간단한다. 정리 4.9의 증명에 있어서, z = 0에서 ϕ^3(z)의 1차 및 2차 도함수를 직접 계산하는 것은 본질적으로 까다로운 단계이다. Fan et al.과 달리 또 다른 점은 ϕ^3(z)를 더 간단한 변환의 구성으로 분해하여 ϕ^3(z)의 멱급수 확장. 이를 위해 $\mathbb{P}^1(\mathbf{Q}_2)$에 다음 세 가지 유리함수 $\{\varphi_i\}_{1\le i\le 3}$을 설정한다. 이는 $\sigma(z)=1/z$ 반전과 연관되고 요소 $a\in\mathbf{Z}_2$에 대한 변환 $T_a(z)=z+a$이다.

[0357] (식 3.28)

$$\begin{cases}\varphi_1=\sigma\circ\phi,\\ \varphi_2=T_{-1}\circ\phi\circ\sigma,\text{and}\\ \varphi_3=\phi\circ T_1.\end{cases}$$

[0358]

[0359] i = 1, 2에 대해 $\varphi_i(0)=0$이고, 여기서 $\varphi=\varphi_1$ 및 $\psi=\varphi_3$의 Fan et al. 표기법 차이에 유의한다. $\rho^2=id=T_1\circ T_{-1}$이기 때문에 (식 3.28), 결정적인 분해 $\phi^3=\varphi_3\circ\varphi_2\circ\varphi_1$를 얻는다.

[0360] (정리 4.11)

[0361] 식 3.28의 $\{\varphi_i\}_{i=1,2,3}$를 z의 계수로 수렴하는 급수라고 하자.

[0362] (1) 만약,

$$\varphi_i(z)=t_{i1}z+t_{i2}z^2+O(z^3),\ \ for\ i=1,2,$$
$$\varphi_3(z)=t_{30}+t_{31}z+t_{32}z^2+O(z^3),$$

[0363]

[0364] 여기서 O(z)는 big-O이고 다음과 같다.

$$(i)\ t_{11}=\frac{b_1}{a_0},\ t_{12}=\frac{a_0b_2-a_1b_1}{a_0^2};$$
$$(ii)\ t_{21}=a_{d-1}-b_{d-1},\ t_{22}=(a_{d-2}-b_{d-2})-(a_{d-1}-b_{d-1})b_{d-1};$$
$$(iii)\ t_{30}=\frac{A(1)}{B(1)},\ t_{31}=\frac{1}{B^2(1)}\left(A'(1)B(1)-A(1)B'(1)\right),$$
$$t_{32}=\frac{1}{2B^3(1)}\left(A''(1)B^2(1)-2A'(1)B'(1)B(1)-A(1)B''(1)B(1)+2A(1)(B'(1))^2\right)$$

[0365]

[0366] (2) 만약, $\phi^3(z)=\lambda_0+\lambda_1z+\lambda_2z^2+O(z^3)$이면,

$$\lambda_0=t_{30},\quad \lambda_1=t_{31}t_{21}t_{11},$$
$$\lambda_2=t_{31}t_{21}t_{12}+t_{31}t_{22}t_{11}^2+t_{32}t_{21}^2t_{11}^2.$$

[0367]

[0368] 따라서 이러한 계수는 정리 4.11의 (1)파트에서 명시적으로 제공된다.

[0369] 증명. 부분 (1)-(i)의 증명은 분모 다항식의 상수 항 a_0이 $\mathbf{Z}_2$의 단위이기 때문에 '1의 분모를 직접 반전하는

것이다. 부분 (1)-(ii)도 유사한 방식으로 수행될 수 있다. 부분 (1)-(iii)의 경우 $\varphi_3(z) = A(1+z)/B(1+z)$ 에서 분모 다항식의 상수 항 B(1)이 $\phi(1) = A(1)/B(1) \equiv 0 \pmod 2$ 이기 때문에 $\mathbf{Z}_2$ 이다.

[0370] 다항식 $F(1+z) \in \{A(1+z), B(1+z)\}$ 에 대한 테일러 정리는 다음을 제공한다.

[0371] $$F(1+z) = F(1) + F'(1)z + \frac{F''(1)}{2!}z^2 + O(z^3)$$

[0372] B(1+z)를 반전하여(B(1)이 단위원이므로 가능) φ_3 의 다음 확장을 얻는다.

[0373] $$\varphi_3(z) = A(1+z)/B(1+z) = \frac{A(1) + A'(1)z + \frac{A''(1)}{2}z^2 + O(z^3)}{B(1) + B'(1)z + \frac{B''(1)}{2}z^2 + O(z^3)}$$

[0374] $$= \left[A(1) + A'(1)z + \frac{A''(1)}{2}z^2 + O(z^3)\right]$$

[0375] $$\cdot \left[\frac{1}{B(1)}\left(1 - \left(\frac{B'(1)}{B(1)}z + \frac{B''(1)}{2B(1)}z^2 + O(z^3)\right) + \left(\frac{B'(1)}{B(1)}z + \frac{B''(1)}{2B(1)}z^2 + O(z^3)\right)^2 + O(z^3)\right)\right]$$

[0376] $$= \frac{A(1)}{B(1)} + \left(\frac{A'(1)}{B(1)} - \frac{A(1)B'(1)}{B^2(1)}\right)z$$

[0377] $$+ \left(\frac{A''(1)}{2B(1)} - \frac{A'(1)B'(1)}{B^2(1)} - \frac{A(1)B''(1)}{2B^2(1)} + \frac{A(1)(B'(1))^2}{B^3(1)}\right)z^2 + O(z^3)$$

[0378] 따라서 φ_3 의 계수를 동일하게 하면 $t_{3i}\ (0 \le i \le 2)$ 에 대한 결과를 얻을 수 있다.

[0379] 반면에 부분 (2)는 $\phi^3 = \varphi_3 \circ \varphi_2 \circ \varphi_1$ 인 직접 계산을 따른다.

[0380] 우리는 이제 정리 4.10을 증명할 수 있는 위치에 있다.

[0381] 정리의 증명 4.10. (식 3.26)에서 $\mathbb{P}^1(\mathbf{Q}_2)$ 에 대한 유리함수가 좋은 축소를 갖는다고 가정한다. 그런 다음 정리 4.7의 증명에서 다음 급수가 $2\mathbf{Z}_2$ 에서 최소인 경우에만 동력학계($\mathbb{P}^1(\mathbf{Q}_2), \phi$)이 최소임을 따른다.

[0382] (식 3.29)

[0383] $$\phi^3(z) = \lambda_0 + \lambda_1 z + \lambda_2 z^2 + \lambda_3 z^3 + \cdots,$$

[0384] 이는 다음 조건과 동일하다.

[0385] $$\begin{cases} (E1)\ \dfrac{\lambda_0}{2} \equiv 1 \pmod 2, \\ (E2)\ \lambda_1 \equiv 1 \pmod 2, \\ (E3)\ \lambda_1 + 2\lambda_2 \equiv 1 \pmod 4. \end{cases}$$

[0386] 우리는 축소가 좋다는 가정에서 조건 (C1)을 유도한다. $\phi(0)=\infty$ 및 $\phi(\infty)=1$이므로 (C2)를 얻는다. ($\mathfrak{B}_1,\phi_1$)의 최소값에서 조건 (C2)와 (C3)을 추론한다. 이제 위의 조건(E1)-(E3)을 사용하여 나머지 주장을 도출한다. (E1)에서 정리 4.11은 $\lambda_0=\frac{A(1)}{B(1)}\equiv 2 \pmod 4$를 제공한다. 따라서 B(1)은 Z2의 단위이므로 A(1), 즉 (C4)를 얻는다. (E2)에서 정리 4.11을 통해 $\lambda_1=t_{11}t_{21}t_{31}\equiv 1 \pmod 2$가 다음 합동과 동일하다는 것이 분명하다.

[0387] (식 3.30)

[0388] $$t_{11}\equiv t_{21}\equiv t_{31}\equiv 1 \pmod 2$$

[0389] 정리 4.11에서는 다음을 따른다.

[0390] $$t_{31}=\frac{1}{B^2(1)}\left(A'(1)B(1)-A(1)B'(1)\right)\equiv 1 \pmod 2$$

[0391] 진행되는 합동에서 (C3)과 (C4)를 사용하여 $A'(1)\equiv A_{\phi,1}\equiv 1 \pmod 2$, 즉 (C5)를 추론한다. 유사한 방식으로 정리 4.11에 따르면 (C6) 및 (C7)은 각각 관계 $t_{21}\equiv 1 \pmod 2$ 및 $t_{11}\equiv 1 \pmod 2$에서 쉽게 따른다. (C8')이 (E3)에서 뒤따르는 것을 보여줄 것이다.

[0392] (E3)에서 우리는 먼저 정리 4.11을 사용하여 다음을 얻는다.

[0393] (식 3.31)

[0394] $$\begin{aligned}\lambda_1+2\lambda_2 &\equiv t_{31}t_{21}t_{11}+2t_{31}t_{21}t_{12}+2t_{31}t_{22}t_{11}^2+2t_{32}t_{21}^2t_{11}^2\\ &\equiv t_{31}t_{21}t_{11}+2t_{31}t_{21}t_{12}+2t_{31}t_{22}+2t_{32}\equiv 1 \pmod 4\end{aligned}$$

[0395] 그런 다음 진행 중인 합동의 모듈로 4라는 4개의 항 각각을 계산한다. 정리 4.11에서 다음을 따른다.

[0396] (식 3.32)

[0397] $$\begin{cases} t_{11}=\frac{b_1}{a_0}\equiv a_0b_1\equiv a_0+b_1-1 \pmod 4,\\ t_{21}=a_{d-1}-b_{d-1},\\ t_{31}\equiv A'(1)+B(1)-1-2B'(1) \pmod 4,\end{cases}$$

[0398] 여기서 첫 번째 합동은 홀수 a와 b, 그리고 (C2)와 (C6)에 대해 $ab\equiv a+b-1 \pmod 4$이라는 단순한 사실에서 나옵니다. 세 번째는 (C3)과 (C4)에서 나온다. (식 3.30) 및 (식 3.32)에서 다음을 얻는다.

[0399] $$\begin{aligned}t_{11}t_{21}t_{31} &\equiv t_{31}+t_{21}+t_{11}-2\\ &\equiv A'(1)+B(1)-2B'(1)+(a_{d-1}-b_{d-1})+(a_0+b_1) \pmod 4\end{aligned}$$

[0400] 정리 4.11에서 관계 $t_{31}\equiv t_{21}\equiv a_0\equiv b_1\equiv 1 \pmod 2$은 다음으로 이어진다.

[0401] $$2t_{31}t_{21}t_{12}\equiv 2t_{12}\equiv 2\left(\frac{a_0b_2-a_1b_1}{a_0^2}\right)\equiv 2(b_2-a_1) \pmod 4$$

[0402] 정리 4.11에서 t22의 표현식을 사용하면 관계 $t_{31}\equiv 1 \pmod 2$,

$a_{d-1} - b_{d-1} = t_{21} \equiv 1 \pmod 2$도 다음을 제공한다.

$$\begin{aligned} 2t_{31}t_{22} \equiv 2t_{22} &\equiv 2((a_{d-2} - b_{d-2}) - (a_{d-1} - b_{d-1})b_{d-1}) \\ &\equiv 2(a_{d-2} - b_{d-2} - b_{d-1}) \pmod 4. \end{aligned}$$

[0403]

[0404] 이제 정리 4.11을 사용하여 네 번째 항 $2t_{32}$ modulo 4를 추정한다. 관계 $A(1) \equiv 2 \pmod 2$, $B(1) \equiv A'(1) \equiv 1 \pmod 2$를 사용하여 다음을 유도한다.

$$\begin{aligned} 2t_{32} &= \frac{1}{B^3(1)}\left(A''(1)B^2(1) - 2A'(1)B'(1)B(1) - A(1)B''(1)B(1) + 2A(1)(B'(1))^2\right) \\ &\equiv A''(1)B(1) - 2A'(1)B'(1) - A(1)B''(1) + 2A(1)(B'(1))^2B(1) \\ &\equiv A''(1) - 2B'(1) \pmod 4. \end{aligned}$$

[0405]

[0406] 위의 계산에서 (식 3.31)의 네 항을 추가하여 다음과 같이 최종 조건(C8')을 얻는다.

$$\begin{aligned} \lambda_1 + 2\lambda_2 &\equiv t_{31}t_{21}t_{11} + 2t_{31}t_{21}t_{12} + 2t_{31}t_{22} + 2t_{32} \\ &\equiv (A'(1) + B(1) - 2B'(1) + (a_{d-1} - b_{d-1}) + (a_0 + b_1)) + 2(b_2 - a_1) \\ &\quad + 2(a_{d-2} - b_{d-2} - b_{d-1}) + A''(1) - 2B'(1) \\ &\equiv A'(1) + A''(1) + B(1) + a_{d-1} - b_{d-1} + a_0 + b_1 + 2(b_2 - a_1 + a_{d-2} - b_{d-2} - b_{d-1}) \\ &\equiv A_{\phi,1} + B_\phi + a_{d-1} + b_{d-1} + a_0 + b_1 + 2(b_2 - a_1 + a_{d-2} - b_{d-2}) \equiv 1 \pmod 4, \end{aligned}$$

[0407]

[0408] 여기서,

[0409] $A'(1) \equiv A_{\phi,2} + 2\sum_{i\geq 0} a_{4i+2} - A_{\phi,3} \pmod 4$,
$A''(1) \equiv 2\sum_{i\geq 0} a_{4i+2} + 2A_{\phi,3} \pmod 4$를 관찰한 결과에 따른 $A'(1) + A''(1) \equiv A_{\phi,2} + A_{\phi,3} \equiv A_{\phi,1} \pmod 4$를 사용한다.

[0410] 반대의 경우, (식 3.27)의 처음 4개 조건은 ($\mathfrak{B}_1, \phi_1$)의 최소성과 ϕ의 1-Lipschitz 연속성을 의미한다. 첫 번째 부분에 대한 계산에서 ($\mathbb{P}^1(\mathbf{Q}_2), \phi$)의 최소값은 가정된 조건 (C1)-(C7) 및 (C8')과 동일한 조건 (E1)-(E3)에서 즉시 나온다.

[0411] 몇 가지 예를 들어 정리 4.10에서 최소성 기준을 설명한다. 이후의 모든 계산은 Sagemath 패키지로 구현되었다.

[0412] 2, 3, 4 차수의 $\mathbb{P}^1(\mathbf{Q}_2)$에 좋은 축소가 있는 유리함수가 없는 것으로 알려져 있으므로, 좋은 축소로 5차의 $\mathbb{P}^1(\mathbf{Q}_2)$에 대한 유리함수를 처리한다.

[0413] (예제 4.12)

[0414] $\phi(z) = \dfrac{1 + 2z + 2z^4 + z^5}{3z + 2z^2 - 3z^4 + z^5}$를 $\mathbb{P}^1(\mathbf{Q}_2)$의 차수가 5인 유리함수라고 하자. 그러면 축소함수 $\bar{\phi}$는

$$\bar{\phi} = \frac{(z+1)(z^4 + z^3 + z^2 + z + 1)}{z(z^4 + z^3 + 1)}$$

[0415]

[0416] 따라서 $\bar{\phi}$의 분모와 분자가 공통 근을 가지지 않기 때문에 ϕ는 좋은 축소를 갖는다. 주기($0, \infty, 1$)가 수준

1에서 전체 주기를 형성하기 때문에 P1(F2)에서 전이인지 확인하기 쉽다. 정리 4.10의 모든 조건을 확인하여 동력학계($\mathbb{P}^1(\mathbf{Q}_2), \phi$)이 최소, 그 중 레벨 3에서 유도 시스템의 주기적인 궤도는 다음과 같이 주어진다.

[0417] $$0 \to \infty \to 1 \to 2 \to \tilde{6} \to 3 \to 4 \to \tilde{4} \to 5 \to 6 \to \tilde{2} \to 7$$

[0418] 여기서 $\tilde{\alpha}$는 반전함수 $\sigma(z) = 1/z$로 주어진 로컬 좌표 아래에서 볼 $B_1(\infty)$의 한 원소의 상을 나타낸다.

[0419] (정리 4.13)

[0420] $$\phi(z) = \frac{1 + z^2 + 3z^3 + z^4}{3z + z^2 + z^4}$$ 를 앞서 선택한 $\mathbb{P}^1(\mathbf{Q}_2)$에 대한 차수 4의 유리함수라고 하자. 그러면 1-Lipschitz 연속형이지만 축소율이 나쁜 것으로 나타난다. 정리 4.10의 모든 조건을 확인하면 동력학계($\mathbb{P}^1(\mathbf{Q}_2), \phi$)가 최소임을 쉽게 알 수 있다. 수준 3에서 유도 시스템의 주기적인 궤도는 다음과 같이 주어진다.

[0421] $$0 \to \infty \to 1 \to 6 \to \tilde{6} \to 3 \to 4 \to \tilde{4} \to 5 \to 2 \to \tilde{2} \to 7$$

[0422] p = 3에 대한 특성화(Characterization for p = 3)

[0423] 이 하위 섹션에서 계수의 관점에서, 우리는 형식의 유리함수 $\phi \in \mathbf{Q}_3(z)$의 최소성 조건에 대한 완전한 설명을 제공한다.

[0424] (식 3.33)

[0425] $$\phi(z) = \frac{A(z)}{B(z)} = \frac{a_0 + a_1 z + \cdots + a_{d-1} z^{d-1} + z^d}{b_1 z + \cdots + b_{d-1} z^{d-1} + z^d}$$

[0426] 모든 $0 \le i \le d-1$에 대해 $a_i, b_i \in \mathbf{Q}_3$, $b_0 = 0$으로 $\phi(0) = \infty$ 및 $\phi(\infty) = 1$을 충족한다.

[0427] p = 3에 대한 증명은 p = 2의 경우를 모델로 하므로 앞 절에서와 동일한 절차를 진행한다. 이제 (식 3.33)과 관련된 다음 수량을 설정한다.

[0428] $$A_\phi = \sum_{i \ge 0} a_i, \quad B_\phi = \sum_{i \ge 1} b_i, \quad A_{\phi,k,l} = \sum_{i \ge 0} a_{ki+l}, \quad B_{\phi,k,l} = \sum_{i \ge 0} b_{ki+l} \text{ for } 0 \le l \le k$$

[0429] 직접 계산에서 $F \in \{A, B\}$

[0430] (식 3.34)

[0431] $$\begin{cases} F(1) = F_\phi, F(2) \equiv F_{\phi,2,0} - F_{\phi,2,1} \pmod 3, \\ F'(1) \equiv F_{\phi,3,1} - F_{\phi,3,2} \pmod 3, \\ F'(2) \equiv F_{\phi,6,1} + F_{\phi,6,2} - F_{\phi,6,4} - F_{\phi,6,5} \pmod 3, \\ F''(1) \equiv -F_{\phi,3,2} \pmod 3, \\ F''(2) \equiv -F_{\phi,6,2} + F_{\phi,6,5} \pmod 3. \end{cases}$$

[0432] p = 2의 경우와 같이 $\mathbb{P}^1(\mathbf{Q}_3)$에 다음 유리함수 $\{\psi_i\}_{1\le i\le 4}$ on $\mathbb{P}^1(\mathbf{Q}_3)$ 를 설정한다.

[0433] (식 3.35)

$$\begin{cases} \psi_1 = \sigma \circ \phi, \\ \psi_2 = T_{-1} \circ \phi \circ \sigma, \\ \psi_3 = T_{-\phi(1)} \circ \phi \circ T_1, \\ \psi_4 = \phi \circ T_{\phi(1)}, \end{cases}$$

[0434]

[0435] 여기서 $\sigma(z) = 1/z$ 는 반전이고 $T_a(z) = z + a$ 는 요소 $a \in \mathbf{Z}_3$ 에 의한 변환이다.

[0436] $\sigma^2 = id = T_a \circ T_{-a}$ 이므로,

[0437] 각 i=1, 2, 3 에 대해 $\phi^4 = \psi_4 \circ \psi_3 \circ \psi_2 \circ \psi_1$ 및 $\psi_i(0) = 0$ 임을 쉽게 알 수 있다.

[0438] (정리 4.14)

[0439] (식 3.33)에서 ϕ가 좋은 축소가 있고 ($\mathfrak{B}_1, \phi_1$)이 최소이면 다음 관계가 충족된다.

[0440] (식 3.36)

$$\begin{cases} (C1)\, a_i, b_i \in \mathbf{Z}_3, \ for\ 0 \le i \le d-1, \\ (C2)\, a_0 \not\equiv 0 \pmod 3, \\ (C3)\, A_\phi \equiv 2B_\phi \pmod 3 \ and\ B_\phi \not\equiv 0 \pmod 3, \\ (C4)\, A(2) \equiv 0 \pmod 3 \ and\ B(2) \not\equiv 0 \pmod 3. \end{cases}$$

[0441]

[0442] 반대로 (식 3.36)의 조건은 1-Lipschitz 연속이고 ($\mathfrak{B}_1, \phi_1$)이 최소임을 의미한다.

[0443] 또한 0에서 ϕ^4 의 Taylor 전개는 다음과 같은 형식이다:

$$\phi^4(z) = \phi^2(1) + \lambda_1 z + \lambda_2 z^2 + O(z^3)$$

[0444]

[0445] 여기서, 모든 i $\ge$ 1이면, $\lambda_i \in \mathbf{Z}_3$ 이다.

[0446] 증명. 축소가 양호하고 수준 1에서 유도된 시스템이 최소라고 가정한다. 그런 다음 A와 B에 각각 0이 아닌 상수 $\alpha \in \mathbf{Q}_3$을 곱하여 둘 다 Z3에 있고 A와 B의 계수 중 적어도 하나가 Z3의 단위가 되도록 한다. 따라서 (C1)을 얻는다. (C2)는 $\phi(0) = \frac{A(0)}{B(0)} = \infty$ 바로 다음에 온다. ($\mathfrak{B}_1, \phi_1$)이 최소이므로 $\phi(1) = \frac{A(1)}{B(1)} \equiv 2 \pmod 3$ 이 있다. 이로부터 (C3)을 의미하는 $B(1) \not\equiv 0 \pmod 3$ 을 도출한다. ϕ 가 좋은 축소를 갖는다는 가정에서, 축소된 다항식 $\bar{A}$ 와 $\bar{B}$ 에는 공통 근이 없으므로 (C4)가 q(2)에서 뒤따르는 것은 간단하다.

[0447] 반대 방향의 경우 (식 3.36)의 조건이 ($\mathfrak{B}_1, \phi_1$)의 최소성을 암시하는지 직접 확인한다. 이것은 정리 4.15에

서 바로 이어지며, 여기서 유리함수 ψ_i는 모두 1에 대해 $3\mathbf{Z}_3$에서 1-Lipschitz로 표시된다. $\phi^4(0) = s_{40} = \phi^2(1)$에 주목하면 0에서 ϕ^4의 Taylor 확장도 정리 4.15에서 따른다.

[0448]
$$\begin{cases} \phi|_{B_1(0)} = \sigma \circ \psi_1|_{3\mathbf{Z}_3}, \\ \phi|_{B_1(\infty)} = T_1 \circ \psi_2|_{3\mathbf{Z}_3} \circ \sigma, \\ \phi|_{B_1(1)} = T_{\phi(1)} \circ \psi_3|_{3\mathbf{Z}_3} \circ T_{-1}, \\ \phi|_{B_1(2)} = \psi_4|_{3\mathbf{Z}_3} \circ T_{-\phi(1)}. \end{cases}$$

[0449] σ와 T_a는 $\mathbf{Z}_3$에서 1-Lipschitz 연속이므로 ϕ는 모든 i에 대해 $B_1(i)$에서 1-Lipschitz 연속이다. 따라서 ϕ는 $\mathbb{P}^1(\mathbf{Q}_3)$에서 1-Lipschitz 연속이다. $\phi^4(0) = \phi^2(1)$에 주목하면 0에서 ϕ^4의 Taylor 전개도 정리 4.15에서 따른다.

[0450] 본 실시예에 따른 목적을 위해, ψ_4를 제외한 모든 $1 \le i \le 4$에 대해 급수 ψ_i의 2 modulo 3까지 차수를 갖는 계수를 찾는 것이 필요하며, 이에 대한 상수 항 modulo 9는 다음 정리에서 찾을 필요가 있다.

[0451] (정리 4.15)

[0452] (식 3.33)에서 ϕ를 좋은 축소를 가진 유리함수라고 하고 $(\mathfrak{B}_1, \phi_1)$을 최소로 하며, (식 3.35)의 $\{\psi_i\}_{1\le i\le 4}$를 $\phi^4 = \psi_4 \circ \psi_3 \circ \psi_2 \circ \psi_1$. 가 되도록 $\mathbf{Z}_3$에 대한 멱급수라 가정한다.

[0453] (1) 만약,

[0454]
$$\psi_i(z) = s_{i1}z + s_{i2}z^2 + O(z^3) \quad for\ i = 1, 2, 3,$$
$$\psi_4(z) = s_{40} + s_{41}z + s_{42}z^2 + O(z^3),$$

[0455] 다음으로,

[0456]
(a) (i)$s_{11} = \frac{b_1}{a_0} \equiv b_1 a_0 \pmod 3, s_{12} = \frac{(a_0 b_2 - a_1 b_1)}{a_0^2} \equiv a_0 b_2 - a_1 b_1 \pmod 3.$
(b) (ii)$s_{21} = a_{d-1} - b_{d-1}, s_{22} = a_{d-2} - b_{d-2} - a_{d-1} b_{d-1} + b_{d-1}^2.$
(c) (iii)$s_{31} \equiv B_\phi(A_{\phi,3,1} - A_{\phi,3,2}) - A_\phi(B_{\phi,3,1} - B_{\phi,3,2}) \pmod 3, s_{32} \equiv A_{\phi,3,2}B_\phi - (A_{\phi,3,1} - A_{\phi,3,2})(B_{\phi,3,1} - B_{\phi,3,2}) - (B_{\phi,3,1} - B_{\phi,3,2})^2 - A_\phi B_{\phi,3,2} \pmod 3,$

[0457]
(d) (iv)$s_{40} \equiv \frac{1}{B(1)B(2)}(A(2)B(1) + (A(1) - 2B(1))A'(2)) \pmod 9, \frac{s_{40}}{3} \equiv (\frac{A(2)}{3}B(2) + \frac{(A(1)-2B(1))}{3}B(1)B(2)A'(2)) \pmod 3, s_{41} \equiv (A_{\phi,6,1} + A_{\phi,6,2} - A_{\phi,6,4} - A_{\phi,6,5})(B_{\phi,2,0} - B_{\phi,2,1}) \pmod 3, s_{42} \equiv (A_{\phi,6,2} - A_{\phi,6,5})(B_{\phi,2,0} - B_{\phi,2,1}) - (A_{\phi,6,1} + A_{\phi,6,2} - A_{\phi,6,4} - A_{\phi,6,5})(B_{\phi,6,1} + B_{\phi,6,2} - B_{\phi,6,4} - B_{\phi,6,5}) \pmod 3.$

[0458] (2) 만약, $\phi^4(z) = \lambda_0 + \lambda_1 z + \lambda_2 z^2 + O(z^3)$이라면,

[0459]
$$\lambda_0 = s_{40}, \quad \lambda_1 = s_{11}s_{21}s_{31}s_{41},$$
$$\lambda_2 = s_{11}^2 s_{21}^2 s_{31}^2 s_{42} + s_{11}^2 s_{21}^2 s_{32} s_{41} + s_{11}^2 s_{22} s_{31} s_{41} + s_{12} s_{21} s_{31} s_{41}.$$

[0460] 따라서 이러한 함수는 (1)파트에서 명시적으로 제공된다.

[0461] 증명. 정리 4.11의 (1)파트에서와 같이 파트(1)에 대한 일상적인 계산을 수행할 수 있으므로 ψ_3과 ψ_4만 간단히 처리한다. ψ_3과 ψ_4를 사용한 직접 계산에서 문제의 함수를 찾아 modulo 3 또는 9로 계산한다. 정리 4.14에서 A(1) 및 B(1)이 $\mathbf{Z}_3$ 및 $A(2) \equiv 0 \pmod 3$의 단위임을 알 수 있다. 관계식을 사용하여 이러한 함수가 정리의 합동을 충족하는지 확인한다.

- $s_{31} = \frac{1}{B(1)^2}(A'(1)B(1) - A(1)B'(1))$
  $\equiv A'(1)B(1) - A(1)B'(1) \pmod 3;$
- $s_{32} = \frac{1}{2B(1)^3}(A''(1)B(1)^2 - 2A'(1)B'(1)B(1) + 2A(1)B'(1)^2 - A(1)B(1)B''(1))$
  $\equiv -A''(1)B(1) - A'(1)B'(1) - B'(1)^2 + A(1)B''(1) \pmod 3;$
- $s_{41} = \frac{1}{B(\phi(1))^2}(A'(\phi(1))B(\phi(1)) - A(\phi(1))B'(\phi(1)))$
  $\equiv A'(2)B(2) - A(2)B'(2) \equiv B(2)A'(2) \pmod 3;$
- $s_{42} = \frac{1}{2B(\phi(1))^3}(A''(\phi(1))B(\phi(1))^2 - 2A'(\phi(1))B'(\phi(1))B(\phi(1))$
  $+ 2A(\phi(1))B'(\phi(1))^2 - A(\phi(1))B(\phi(1))B''(\phi(1)))$
  $\equiv -A''(2)B(2) - A'(2)B'(2) \pmod 3.$

[0462]

[0463] 그런 다음 s_{ij}에 대한 최종 결과는 (식 4.34)에서 따른다.

[0464] $s_{40} = \phi^4(0) = \phi^2(1)$을 계산하여 s_{40} modulo 9의 값을 찾는 일만 남았다. 일부 $m \in \mathbf{Z}_3$에 대해 $\phi(1) = \frac{A(1)}{B(1)} = 2 + 3m$을 사용하여 Taylor 확장은 다음을 제공한다. :

[0465] $$\phi^4(0) = \phi(2+3m) = \frac{A(2+3m)}{B(2+3m)} = \frac{A(2) + 3mA'(2) + O(9)}{B(2) + 3mB'(2) + O(9)}$$

[0466] Z3의 단위 요소 B(2)를 $A(2) \equiv 0 \pmod 3$와,

[0467] $A(1) - 2B(1) \equiv 0 \pmod 3$을 사용하여,

[0468] $$\begin{aligned}\phi^4(0) &\equiv \frac{1}{B(2)}(A(2) + 3mA'(2))\left(1 - 3m\frac{B'(2)}{B(2)}\right)\\ &\equiv \frac{1}{B(2)}(A(2) + 3mA'(2))\\ &\equiv \frac{1}{B(1)B(2)}(A(2)B(1) + (A(1) - 2B(1))A'(2)) \pmod 9\end{aligned}$$

[0469] 3으로 나누면 $\frac{\phi^4(0)}{3}$에 대한 표현식이 생성된다.

[0470] $$\frac{\phi^4(0)}{3} \equiv \frac{A(2)}{3}B(2) + \frac{(A(1) - 2B(1))}{3}B(1)B(2)A'(2) \pmod 3$$

[0471] 파트 (2)는 파트 (1)과 함께 $\phi^4 = \psi_4 \circ \psi_3 \circ \psi_2 \circ \psi_1$를 사용한 직접 계산에서 나온다.

[0472] 여기에서 본 발명의 일 실시예에 따른 사영직선 위의 유리함수에 기반한 의사난수 생성 장치 및 방법은 $\mathbb{P}^1(\mathbf{Q}_3)$에서 유리 함수에 대한 최소성 기준을 제공한다.

[0473] (정리 4.16)

[0474] 모든 표기법을 정리 4.15에서와 동일하게 하고, (식 4.33)에서 좋은 축소가 있고 $\mathbb{P}^1(\mathbf{Q}_3)$에서 최소이면 ϕ는 다음 조건을 충족한다.

[0475] (식 3.37)

[0476]
$$\begin{cases} a_i, b_i \in \mathbf{Z}_3, \quad \text{for } 0 \le i \le d-1, \\ a_0 \not\equiv 0 \pmod 3, \\ A(1) \equiv 2B(1) \pmod 3 \text{ and } B(1) \not\equiv 0 \pmod 3, \\ A(2) \equiv 0 \pmod 3 \text{ and } B(2) \not\equiv 0 \pmod 3. \end{cases}$$

[0477] *Set*

$$u_0 := \left(\frac{A(2)}{3} B(2) + \frac{(A(1) - 2B(1))}{3} B(1)B(2)A'(2) \right) \bmod 3; \ [s_{11}, s_{21}, s_{31}, s_{41}] \bmod 3 = [\cdot, \cdot, \cdot, \cdot].$$

[0478] 또한 (i)-(viii) 조건 중 하나를 충족한다.

[0479]
(i) $[1,1,1,1]$, $u_0 \not\equiv 0 \pmod 3$, $s_{12} + s_{22} + s_{32} + s_{42} \not\equiv u_0 \pmod 3$;
(ii) $[1,1,2,2]$, $u_0 \not\equiv 0 \pmod 3$, $s_{12} + s_{22} - s_{32} + s_{42} \not\equiv u_0 \pmod 3$;
(iii) $[1,2,1,2]$, $u_0 \not\equiv 0 \pmod 3$, $s_{12} - s_{22} - s_{32} + s_{42} \not\equiv u_0 \pmod 3$;
(iv) $[1,2,2,1]$, $u_0 \not\equiv 0 \pmod 3$, $s_{12} - s_{22} + s_{32} + s_{42} \not\equiv u_0 \pmod 3$;
(v) $[2,1,1,2]$, $u_0 \not\equiv 0 \pmod 3$, $-s_{12} - s_{22} - s_{32} + s_{42} \not\equiv u_0 \pmod 3$;
(vi) $[2,1,2,1]$, $u_0 \not\equiv 0 \pmod 3$, $-s_{12} - s_{22} + s_{32} + s_{42} \not\equiv u_0 \pmod 3$;
(vii) $[2,2,1,1]$, $u_0 \not\equiv 0 \pmod 3$, $-s_{12} + s_{22} + s_{32} + s_{42} \not\equiv u_0 \pmod 3$; *and*
(viii) $[2,2,2,2]$, $u_0 \not\equiv 0 \pmod 3$, $-s_{12} + s_{22} - s_{32} + s_{42} \not\equiv u_0 \pmod 3$.

[0480] 반대로, 위의 조건은 $\mathbb{P}^1(\mathbf{Q}_3)$에서 1-Lipschitz 연속적이고 최소임을 의미한다.

[0481] (정리 4.16의 증명)

[0482] 정리 4.7의 증명으로부터 $\mathbb{P}^1(\mathbf{Q}_p)$에서 최소가 되는 좋은 축소를 갖는 유리함수 ϕ에 대한 필요 충분 조건은 멱급수로 표현되는 다음 1-Lipschitz 연속 $\phi^4(z)$가 $3\mathbf{Z}_3$에서 최소라는 것이다.

[0483] (식 3.38)

[0484]
$$\phi^4(z) = \lambda_0 + \lambda_1 z + \lambda_2 z^2 + \lambda_3 z^3 + \cdots,$$

[0485] 이는 다음 조건과 동일하다.

[0486] (식 3.39)

$$\begin{cases} (E1)\ \dfrac{\lambda_0}{3} \not\equiv 0 \pmod 3, \\ (E2)\ \lambda_1 \equiv 1 \pmod 3, \\ (E3)\ \lambda_2 \not\equiv \dfrac{\lambda_0}{3} \pmod 3. \end{cases}$$

[0487]

[0488] 식 (3.37)은 정리 4.14를 따르고 (E1)의 경우 $\frac{\lambda_0}{3} \equiv u_0 \pmod 3$ 값이 정리 4.15에서 명시적으로 계산되기 때문에 식 (3.37)과 (E1)이 관련이 없음을 알 수 있다. 이 보조정리에서 다시 (E2)는 $s_{11}s_{21}s_{31}s_{41} \equiv 1 \pmod 3$과 같다. 이 관계 때문에 벡터 [s11, s21, s31, s41] mod 3에 대한 선택 사항은 8개뿐이며 다음 목록에 나열되어 있다.

$$[1,1,1,1],[1,1,2,2],[1,2,1,2],[1,2,2,1];$$

$$[2,1,1,2],[2,1,2,1],[2,2,1,1],[2,2,2,2].$$

[0489]

[0490] 정리 4.15의 모든 $\alpha \in \{s_{11}, s_{21}, s_{31}, s_{41}\}$에 대해 $\alpha^2 \equiv 1 \pmod 3$에 주목하면 다음과 같다.

$$\begin{aligned} \lambda_2 &\equiv s_{11}^2 s_{21}^2 s_{31}^2 s_{42} + s_{11}^2 s_{21}^2 s_{32} s_{41} + s_{11}^2 s_{22} s_{31} s_{41} + s_{12} s_{21} s_{31} s_{41} \\ &\equiv s_{12} s_{21} s_{31} s_{41} + s_{22} s_{31} s_{41} + s_{32} s_{41} + s_{42} \pmod 3. \end{aligned}$$

[0491]

[0492] 8개의 벡터 [s11, s21, s31, s41] mod 3 각각에 대해 λ_2는 {-1,1}의 계수와 s12, s22, s32 및 s42의 선형 조합으로 작성될 수 있음을 쉽게 알 수 있다. 각 경우에 대해 (E3)에 해당하는 조건을 얻을 수 있다.

[0493] 반대의 경우, 위의 모든 조건이 충족된다고 가정한다. 정리 4.14에서 처음 네 가지 조건은 ϕ가 1-Lipschitz 연속임을 의미하며, (4.38)에서 멱급수로 작성된다. (4.39)에 의해, 첫 번째 부분의 증명은 정리의 두 번째 부분의 결론으로 이어진다.

[0494] (따름정리 4.17)

[0495] $\phi(0) = \infty$ 및 $\phi(\infty) = 1$을 만족하는 우수한 축소를 갖는 차수 2 또는 3의 최소 유리함수 $\phi \in \mathbf{Q}_3(z)$는 없다.

[0496] 증명. 식 (3.37)에서 이러한 차수 2의 유리함수가 최소인 경우 양호한 축소를 위한 조건을 위반한다는 것을 확인하는 것은 간단하다. z^2+1, z^2+z+2 및 z^2+2z+2가 $\mathbf{F}_3$에 대해 차수가 2인 유일한 모닉 기약 다항식이라는 점에 유의하여 deg(ϕ) = 3에 대해 이 작업을 수행한다. 차수 3의 다음 최소 유리함수가 $\phi(0) = \infty$와 $\phi(\infty) = 1$을 만족한다고 가정하면,

$$\phi(z) = \frac{A(z)}{B(z)} = \frac{a_0 + a_1 z + a_2 z^2 + z^3}{b_1 z + b_2 z^2 + z^3}$$

[0497]

[0498] 그런 다음 축소함수 $\bar{B}$가 다항식 z^3, $z(z^2+1)$, $z(z^2+z+2)$ 및 $z(z^2+2z+2)$ 중 하나일 수 있는지

확인한다. 만약, $\bar{B}=z^3$인 경우 다항식 $z^2+b_2z+b_1$은 modulo 3의 이중 0 근만 가지며, 그 다음 $b_1\equiv 0 \pmod 3$을 갖는다. 따라서 $s_{11}\equiv\frac{b_1}{a_0}\equiv 0 \pmod 3$을 얻는다. 이는 정리 4.16에서 s11의 non-vanishing modulo 3과 모순된다.

[0499] 만약, $\bar{B}=z(z^2+1)$, 즉 다항식 $z^2+b_2z+b_1=z^2+1$은 $\mathbf{F}_3$에 대해 기약할 수 없는 경우 $A(2)\equiv 0 \pmod 3$과 $A(1)\equiv 2B(1) \pmod 3$에서, $\bar{A}=(z+1)(z^2+1)$ 또는 $(z+1)(z^2+2z+2)$를 유도한다.

[0500] ϕ는 좋은 감소를 갖기 때문에, $\bar{\phi}$는 $\bar{\phi}=\frac{(z+1)(z^2+2z+2)}{z(z^2+1)}$이며, 여기서 s_{21}의 non-vanishing modulo 3을 위반하는 $a_2-b_2\equiv 0 \pmod 3$를 얻는다. 나머지 두 경우 $\bar{B}=z(z^2+z+2)$와 $\bar{B}=z(z^2+2z+2)$에 대해 유사한 접근 방식을 사용한다. 전자의 경우 $\bar{\phi}=\frac{(z+1)^3}{z(z^2+z+2)}$가 있으며 이는 $A'(2)\equiv 0 \pmod 3$이기 때문에 s_{41}의 non-vanishing modulo 3을 위반한다. 후자의 경우 $\bar{\phi}=\frac{(z+1)(z^2+1)}{z(z^2+2z+2)}$을 얻는다. 이는 $A'(1)\equiv 0\equiv B'(1) \pmod 3$ 때문에 s_{31}의 non-vanishing modulo 3을 위반한다. 여기서, non-vanishing은 영이 아님을 뜻한다.

[0501] 정리 4.16의 최소성 기준은 최소 유리함수 $\mathbb{P}^1(\mathbf{Q}_3)$을 구성하는 원리를 제공한다. 그런 다음 몇 가지 예를 보여준다.

[0502] (정리 4.18)

[0503] $\phi(z)=\frac{2+z+z^2+2z^4+z^5}{2z+2z^3+z^5}$를 $\mathbb{P}^1(\mathbf{Q}_3)$의 차수가 5인 유리함수라고 하면, ϕ의 축소 함수는

[0504] $$\bar{\phi}=\frac{(z+1)(z^4+z^3+2z^2+|2z+2)}{z(z^4+2z^2+2)}$$ 이다.

[0505] 따라서 ϕ는 좋은 축소가 된다.

[0506] 모든 조건에서 $[s_{11},s_{21},s_{31},s_{41}] \bmod 3=[1,2,1,2]$, $[s_{12},s_{22},s_{32},s_{42}] \bmod 3=[1,1,1,1]$ 및 $[\frac{\lambda_0}{3},\lambda_2] \bmod 3=[2,0]$의 모든 조건을 확인하여 정리 4.16의 case (iii)로부터 동력학계 $(\mathbb{P}^1(\mathbf{Q}_3),\phi)$가 최소임이 확인된다. 수준 3에서 유도된 ϕ 시스템의 주기적인 궤도는 다음과 같이 주어진다.

[0507]
$$\begin{aligned}
&0\to\infty\to 1\to 23\to 15\to\tilde{24}\to 4\to 8\to 12\\
&\quad\to\tilde{21}\to 25\to 2\to 18\to\tilde{18}\to 10\to 5\to 6\to\tilde{15}\\
&\quad\to 13\to 17\to 3\to\tilde{12}\to 7\to 11\to 9\to\tilde{9}\to 19\\
&\quad\to 14\to 24\to\tilde{6}\to 22\to 26\to 21\to\tilde{3}\to 16\to 20.
\end{aligned}$$

[0508] (정리 4.19)

[0509] $\phi(z)=\frac{-125+25z-5z^2+z^3}{-5z-3z^2+z^3}\in\mathbf{Q}_3(z)$를 차수가 3인 유리함수라고 하자. 기준 법(modulo) 3을 줄이

면 다음을 얻는다.

[0510] $$\bar{\phi} = \frac{(z+1)(z^2+1)}{z(z^2+1)} = \frac{z+1}{z}$$

[0511] 따라서 ϕ는 $\mathbb{P}^1(\mathbf{Q}_3)$에서 나쁜 축소를 갖는다. 수준 1에서의 ϕ 주기가 (0, ∞, 1, 2)로 주어지기 때문에 $\bar{\phi}$는 $\mathbb{P}^1(\mathbf{F}_3)$에서 전이된다.

[0512] 정리 4.15에서 직접 계산하면 $[s_{11}, s_{21}, s_{31}, s_{41}] \bmod 3 = [1,1,2,2]$, $[s_{12}, s_{22}, s_{32}, s_{42}] \bmod 3 = [2,0,1,2]$ 및 $[\frac{\lambda_0}{3}, \lambda_2] \bmod 3 = [2,0]$ 이다.

[0513] 따라서 정리 4.16의 case (ii)의 모든 조건이 충족된다. 따라서 ϕ는 $\mathbb{P}^1(\mathbf{Q}_3)$에서 최소이다. 수준 3에서 ϕ의 유도된 시스템의 주기적인 궤도는 다음과 같이 주어진다.

[0514] $$0 \to \infty \to 1 \to 11 \to 3 \to \tilde{3} \to 22 \to 26 \to 6$$

$$\to \tilde{15} \to 25 \to 23 \to 9 \to \tilde{9} \to 10 \to 2 \to 12 \to \tilde{12}$$

$$\to 4 \to 17 \to 15 \to \tilde{24} \to 7 \to 14 \to 18 \to \tilde{18} \to 19$$

[0515] $$\to 20 \to 21 \to \tilde{21} \to 13 \to 8 \to 24 \to \tilde{6} \to 16 \to 5.$$

[0516] 대안으로, $(\mathbb{P}^1(\mathbf{Q}_3), \phi)$는 선형 분수 변환 $f(z) = \frac{5z}{z+1}$에 의해 시스템 $(\mathbb{P}^1(\mathbf{Q}_3), \varphi := f^{-1} \circ \phi \circ f)$에 켤레임을 보일 수 있다. 약간의 계산으로 우리는 명시적으로 $\varphi(z) = -\frac{1+2z+2z^2}{1+z-3z^2+z^3}$을 찾을 수 있다. 다음으로 φ의 축소 함수는 $\bar{\varphi} = \frac{z^2+z+2}{(z+2)(z^2+z+2)} = \frac{1}{z+2}$이다. 이는 정리 4.5 또는 정리 1.1의 최소성 조건을 검증함으로써, 잘못된 감소를 갖는 유리함수로서 φ가 $\mathbb{P}^1(\mathbf{Q}_3)$에서 최소임을 나타낸다.

[0517] p $\geq$ 5에 대한 특성화를 설명하면 다음과 같다.

[0518] p = 2 또는 3의 경우와 마찬가지로 임의의 소수 p$\geq$ 5에 대한 계수를 사용하여 $\mathbb{P}^1(\mathbf{Q}_p)$의 유리함수에 대한 최소성 기준을 결정하는 것은 가치가 있다. 그러나 이 작업은 쉽지 않다. 정리 4.7에는 두 가지 이유가 있다. 첫째, 축소된 유리함수 $\bar{\phi} \in \mathbf{F}_p(z)$는 유한체 $\mathbf{F}_p$에 대한 사영직선인 $\mathbb{P}^1(\mathbf{F}_p)$에서 최소이거나 전이적이어야 한다. 그러나 일반 소수 유한체 $\mathbf{F}_p$에 대한 전이적 유리함수의 완전한 특성화에서 유리함수에 $0 \mapsto \infty \mapsto 1$이 길이가 $p+1$인 $\bar{\phi}$의 전체 주기의 일부라는 추가 조건이 있더라도 매우 어렵다. 또 다른 이유는 정리 4.7의 조건(2)와 관련이 있다. 연쇄 법칙(chain rule)에 따라 $(\phi^{p+1})'(0) \equiv 1 \pmod{p}$ 조건은 다음과 같다.

[0519] (식 3.40)

[0520] $$\phi'(0)\phi'(\phi(0)) \cdots \phi'(\phi^p(0)) \equiv 1 \pmod{p}$$

[0521] $\mathbb{P}^1(\mathbf{Q}_p)$에서 ϕ가 최소이면 이 관계에서 계수로 $\phi(\infty)$의 명시적 표현을 찾아야 하는데 이는 달성하기 쉽지 않다. 따라서 이 하위 절의 목적은 정리 4.7의 조건(2)와 동일한 유용한 조건을 제공하는 것이다. 결과 조건은

$\mathbb{P}^1(\mathbf{F}_p)$에 대한 전이 유리함수가 이미 발견된 경우 임의의 소수 p에 대해 $\mathbb{P}^1(\mathbf{Q}_p)$에 대한 최소 유리함수을 구성하는 데 사용할 수 있다는 점에서 실용적이다.

[0522] ϕ가 다음 형식의 차수 $d \geq 2$인 유리함수(z)이라 하면,

[0523] (식 3.41)

[0524] $$\phi(z) = \frac{A(z)}{B(z)} = \frac{a_0 + a_1 z + \cdots + a_{d-1} z^{d-1} + z^d}{b_1 z + \cdots + b_{d-1} z^{d-1} + z^d} \in \mathbf{Q}_p(z)$$

[0525] $\phi(0) = \infty$ 및 $\phi(\infty) = 1$이 되도록 모든 $0 \leq i \leq d-1$에 대해 $a_i, b_i \in \mathbf{Q}_p$ 이다.

[0526] 정리 4.7과 유사한 유리함수의 또 다른 최소성 기준을 제공한다.

[0527] (정리 4.20)

[0528] p를 소수≥ 5라고 하고 (식 4.41)에서 $\phi(z) = \frac{A(z)}{B(z)} \in \mathbf{Q}_p(z)$를 deg $\phi \geq 2$의 유리함수라고 하고 좋은 감소를 나타낸다. 만약, 동력학계$(\mathbb{P}^1(\mathbf{Q}_p), \phi)$가 최소이면 다음 조건이 충족된다.

[0529]
(1) $a_i, b_i \in \mathbf{Z}_p \text{for} 0 \leq i \leq d-1.$
(2) $a_0 \not\equiv 0 \pmod{p}$ *and* $B(i) \not\equiv 0 \pmod{p}$ *for all* $i \in \{0, 1, \ldots, p-1\}$.
(3) *The reduction* $\bar{\phi}$ *is transitive on* $\mathbb{P}^1(\mathbf{F}_p)$, *of which the full cycle is given by* $(0, \infty, \xi_1, \ldots, \xi_{p-1})$ *where* $\{\xi_1 := 1, \xi_2, \ldots, \xi_{p-1}\} = \mathbf{F}_p^*$.
(4) $\frac{b_1}{a_0}(a_{d-1} - b_{d-1}) \prod_{i=1}^{p-1} \frac{A'(i)B(i) - A(i)B'(i)}{B^2(i)} \equiv 1 \pmod{p}$.
(5) $\phi(\xi_{p-1}) + (\phi(\xi_{p-2}) - \xi_{p-1}) w_{p-1} + \cdots + (\phi(\xi_1) - \xi_2) w_2 \not\equiv 0 \pmod{p^2}$ *for* $2 \leq i \leq p-1, w_i = \prod_{j=i}^{p-1} \phi'(\xi_j)$.

[0530] 반대로, 위의 조건이 충족되면 ϕ는 1-Lipschitz 연속 유리함수이고 $\mathbb{P}^1(\mathbf{Q}_p)$에서 최소이다.

[0531] 증명. 정리 4.7의 증명에서 $\mathbb{P}^1(\mathbf{Q}_p)$에서 최소가 되는 좋은 축소를 갖는 유리함수 ϕ에 대한 필요충분조건은 멱급수로 표현되는 $p\mathbf{Z}_p$에 대한 1-Lipschitz 연속 유리함수 $\phi^{p+1}(z)$,

[0532] (식 3.42)

[0533] $$\phi^{p+1}(z) = \phi^{p+1}(0) + (\phi^{p+1})'(0) z + O(z^2)$$

[0534] 다음 조건을 충족한다.

[0535] $$\frac{\phi^{p+1}(0)}{p} \not\equiv 0 \pmod{p}, \quad (\phi^{p+1})'(0) \equiv 1 \pmod{p}$$

[0536] 이러한 조건은 또한 축소 시스템$(\mathbb{P}^1(\mathbf{F}_p), \bar{\phi})$이 최소이므로 해당 주기가 정리에서와 같이 전체 길이 p+1의 형태$(0, \infty, \xi_1, \ldots, \xi_{p-1})$임을 의미한다. 이제 증명은 $\frac{\phi^{p+1}(0)}{p}$와 $(\phi^{p+1})'(0)$ 모두에 대해 정리 4.7과 동일한 식을 유도하는 것과 같다. ϕ^{p+1}을 $\mathbf{Z}_p$의 계수를 사용하여 p+1의 멱급수의 구성으로 분해하기 위해 다음과 같이 정의된 유리함수 $\{\eta_i\}_{1 \leq i \leq p+1}$을 설정한다.

[0537] (식 3.43)

$$\begin{cases} \eta_1 = \sigma \circ \phi, \\ \eta_2 = T_{-\phi^2(0)} \circ \phi \circ \sigma, \\ \eta_i = T_{-\phi^i(0)} \circ \phi \circ T_{\phi^{i-1}(0)} \ (3 \le i \le p), \text{and} \\ \eta_{p+1} = \phi \circ T_{\phi^p(0)}, \end{cases}$$

[0538]

[0539] 여기서 $\sigma(z) = 1/z$는 반전이고 $T_a = z + a$는 요소 $a \in \mathbf{Z}_p$에 의한 변환이다.

[0540] $1 \le i \le p$의 경우 $\eta_i(0) = 0$이므로 이러한 유리함수 η_i는 상수 항이 없는 멱급수이다. (식 3.43)의 정의에서 z = 0에서 η_i의 도함수를 구함으로써, η_i의 멱급수 전개를 얻는다.

[0541] (식 3.44)

$$\begin{cases} \eta_1 = \dfrac{b_1}{a_0} z + O(z^2), \\ \eta_2 = (a_{d-1} - b_{d-1}) z + O(z^2), \\ \eta_i = \phi'(\phi^{i-1}(0)) z + O(z^2) \ (3 \le i \le p), \\ \eta_{p+1} = \phi^{p+1}(0) + \phi'(\phi^p(0)) z + O(z^2). \end{cases}$$

[0542]

[0543] $\phi^{p+1} = \eta_{p+1} \circ \eta_p \cdots \eta_2 \circ \eta_1$으로부터 $\sigma \circ \sigma = id = T_{-a} \circ T_a$라는 관찰 결과에 따라 (식 3.44)를 사용하여 다음을 얻는다.

[0544] (식 3.45)

$$\phi^{p+1}(z) = \phi^{p+1}(0) + \frac{b_1}{a_0}(a_{d-1} - b_{d-1})\phi'(\phi^2(0)) \cdots \phi'(\phi^p(0)) z + O(z^2)$$

[0545]

[0546] (식 3.42)와 (식 3.45)에서 급수의 선형 항을 비교하여 다음을 얻는다.

[0547] (식 3.46)

$$(\phi^{p+1})'(0) = \frac{b_1}{a_0}(a_{d-1} - b_{d-1})\phi'(\phi^2(0)) \cdots \phi'(\phi^p(0))$$

[0548]

[0549] 시스템 $(\mathbb{P}^1(\mathbf{F}_p), \bar{\phi})$이 최소이므로 다음을 따른다.

$$(\phi^{p+1})'(0) \equiv \frac{b_1}{a_0}(a_{d-1} - b_{d-1})\phi'(1) \cdots \phi'(p-1) \pmod{p}$$

[0550]

[0551] 유리함수 $\phi = \frac{A}{B}$의 도함수에 대한 몫 공식에서 주장 (2)는 다음과 같다.

$$(\phi^{p+1})'(0) \equiv \frac{b_1}{a_0}(a_{d-1} - b_{d-1}) \prod_{i=1}^{p-1} \frac{A'(i)B(i) - A(i)B'(i)}{B^2(i)} \equiv 1 \pmod{p}$$

[0552]

[0553] 주장 (3)의 경우, 정리 3.10의 증명에서 수렴 급수와 동일한 인수를 적용한다.

[0554] 일부 $m \in \mathbf{Z}_p$에 대한 $z = \phi^p(0) = \xi_{p-1} + mp$에서 ϕ의 테일러 전개는 다음을 제공한다.

[0555] $$\phi^{p+1}(0) = \phi(\phi^p(0)) = \phi(\xi_{p-1} + mp) \equiv \phi(\xi_{p-1}) + mp\phi'(\xi_{p-1})$$

[0556] $$\equiv \phi(\xi_{p-1}) + (\phi^p(0) - \xi_{p-1})\phi'(\xi_{p-1}) \pmod{p^2}$$

[0557] $\phi^{p-1}(0)$에 적용된 동일한 인수는 다음을 제공한다.

[0558] $$\phi^p(0) \equiv \phi(\xi_{p-2}) + (\phi^{p-1}(0) - \xi_{p-2})\phi'(\xi_{p-2}) \pmod{p^2}$$

[0559] $\phi^p(0)$를 $\phi^{p+1}(0)$에 대한 위의 식에 대입하면 다음과 같이 된다.

[0560] $$\phi^{p+1}(0) \equiv \phi(\xi_{p-1}) + (\phi(\xi_{p-2}) - \xi_{p-1})\phi'(\xi_{p-1}) + (\phi^{p-1}(0) - \xi_{p-2})\phi'(\xi_{p-2})\phi'(\xi_{p-1}) \pmod{p^2}$$

[0561] 동일한 인수를 귀납적으로 적용하고 $\phi^2(0) = \xi_1 = 1$을 사용하여 다음과 같은 중요한 관계를 얻는다.

[0562] $$\phi^{p+1}(0) \equiv \phi(\xi_{p-1}) + (\phi(\xi_{p-2}) - \xi_{p-1})w_{p-1} + \cdots + (\phi(\xi_1) - \xi_2)w_2 \pmod{p^2}$$

[0563] 여기서 w_i는 $2 \le i \le p-1$에 대한 정리에서 정의된다. 그런 다음 주장 (3)이 이어진다.

[0564] 반대의 부분은 첫 번째 부분의 증명에서 따른다. 조건 (1)은 0이 유리함수 $\bar{\phi}^{p+1}$의 고정점임을 의미하므로 ϕ^{p+1}의 멱급수 확장이 (식 3.42)의 형식이라고 추론한다. (식 3.43)에 의해 다음과 같은 관계가 있다.

[0565] (식 3.47)

[0566] $$\begin{cases} \phi|_{B_1(0)} = \sigma \circ \eta_1|_{p\mathbf{Z}_p}, \\ \phi|_{B_1(\infty)} = T_{\phi^2(0)} \circ \eta_2|_{p\mathbf{Z}_p} \circ \sigma, \\ \phi|_{B_1(\phi^i(0))} = T_{\phi^{i+1}(0)} \circ \eta_i|_{p\mathbf{Z}_p} \circ T_{-\phi^i(0)} \ (2 \le i \le p-1), \text{and} \\ \phi|_{B_1(\phi^p(0))} = \eta_{p+1}|_{p\mathbf{Z}_p} \circ T_{-\phi^p(0)}. \end{cases}$$

[0567] 따라서 p = 2 또는 3의 경우와 같이 ϕ가 1-Lipschitz 연속적이라는 주장과 관련하여, η_i는 모든 $i \in \{1, 2, \ldots, p+1\}$에 대해 $p\mathbf{Z}_p$에서 자신까지 1-Lipschitz임을 보여주는 것으로 충분하다.

[0568] $\eta_i \ (1 \le i \le p+1)$는 조건 (2)에서 $p\mathbf{Z}_p$에 대한 수렴 급수로 확장될 수 있으므로, η_i가 $p\mathbf{Z}_p$에서 1-Lipschitz 연속임을 증명할 수 있다. 따라서 ϕ는 $\mathbb{P}^1(\mathbf{Q}_p)$에서 1-Lipschitz 연속이다. 첫 번째 부분의 증명에서 동력학계$(\mathbb{P}^1(\mathbf{Q}_p), \phi)$가 최소라는 것이 분명하다. 정리 4.20에 대한 몇 가지 설명이 있다.

[0569] (정리 4.21)

[0570] 정리 4.20은 $\mathbb{P}^1(\mathbf{Q}_p)$에 대한 좋은 축소와 함께 유리함수를 구성하는 실용적인 방법을 제공한다. (식 3.40)과 (식 3.46)의 값으로부터 $(\phi^{p+1})'(0)$의 두 표현을 비교하여 다음과 같은 중요한 관계를 얻는다.

[0571] $$\phi'(0)\phi'(\infty) = \frac{b_1}{a_0}(a_{d-1} - b_{d-1})$$

[0572] 이 관계는 좌표의 변화에 의해 $\phi'(\infty)$을 직접 계산할 필요가 없음을 증명한다.

[0573] (정리 4.22)

[0574] 정리 4.20의 조건(1)에서 $\mathbb{P}^1(\mathbf{F}_p)$에 $(p-2)!$ 최소 유리함수 $\bar{\phi}$가 있으므로, $\bar{\phi}(0) = \infty$, $\bar{\phi}(\infty) = 1$이다. 이들 각각에 대해 유리함수에는 정리 4.20의 조건(2)에서의 관계에 해당하는 $\mathbb{P}^1(\mathbf{Q}_p)$의 최소 유리함수$\phi$의 $(p-1)^p$ 유형이 있다. 전체적으로 $\phi(0) = \infty$ 및 $\phi(\infty) = 1$이 되도록 $\mathbb{P}^1(\mathbf{Q}_p)$에 최대 $(p-1)!(p-1)^{p-1}$개의 최소 유리함수 ϕ가 있다.

[0575] (정리 4.23)

[0576] 정리 4.20의 조건 (1)에서, 계수 측면에서 $f(0) = \infty$와 $f(\infty) = 1$을 충족하는 최소 유리 함수 $f(z) \in \mathbf{F}_p(z)$를 특성화하는 것은 매우 중요하다. 그 이유는 이 작업이 유한체에 대한 순열 다항식의 완전한 일반화인 유한체에 대한 유리수 순열 함수에 대한 연구의 일부이기 때문이다.

[0577] 단순화를 위해 벡터$[r_\infty, r_0, r_1, \ldots, r_{p-1}]$은

[0578] $[(a_{d-1} - b_{d-1}), \frac{b_1}{a_0}, \phi'(1), \ldots, \phi'(p-1)] \bmod p$를 나타낸다. 그러면 정리 4.20의 조건 (2)는 다음과 같다.

[0579] $$r_\infty \prod_{i=0}^{p-1} r_i \equiv 1 \pmod{p}$$

[0580] 정리 4.20의 조건 (2)에 따라 다음을 설정한다.

[0581] $$\lambda_0 := \phi(\xi_{p-1}) + \sum_{i=2}^{p-1}(\phi(\xi_{i-1}) - \xi_i)w_i \pmod{p^2}$$

[0582] 그러면 정리 4.20의 조건 (3)은 $\lambda_0 \in p\mathbf{Z}_p \setminus p^2\mathbf{Z}_p$와 같다.

[0583] (정리 4.24)

[0584] 여기서, $\phi(z) = \frac{3+2z+2z^3+5z^4+z^5}{3z+z^2+2z^3+4z^4+z^5}$를 $\mathbb{P}^1(\mathbf{Q}_5)$에 대한 차수 5의 유리함수라고 하자. 그러면 ϕ의 5 축소 함수는 다음과 같다.

[0585] $$\bar{\phi} = \frac{(z+3)(z^4+2z^3+z^2+2z+1)}{z(z^2+z+1)(z^2+3z+3)}$$

[0586] 따라서 ϕ는 좋은 축소가 있다. $\bar{\phi}$의 전체 주기는 $(0, \infty, \xi_1, \xi_2, \xi_3, \xi_4) = (0, \infty, 1, 3, 4, 2)$로 주어지므로 축소 함수$\bar{\phi}$는 $\mathbb{P}^1(\mathbf{F}_5)$에서 추이적이다. $[r_\infty, r_0, r_1, r_2, r_3, r_4]$ = [1, 1, 2, 3, 4, 4] 및 $[w_2, w_3, w_4] = [3, 2, 3]$, 정리 4.20의 조건 (2) 및 (3)은 $\lambda_0 \equiv 5 \bmod 25$로 충족되므로, 동력학계

($\mathbb{P}^1(\mathbf{F}_5)$, ϕ)은 최소이다. 수준 2에서 ϕ의 유도된 시스템의 주기적인 궤도는 다음과 같이 주어진다.

$$0 \to \infty \to 1 \to 8 \to 19 \to 2 \to 5 \to \tilde{5} \to 6 \to 18 \to 9 \to 12$$
$$\to 10 \to \tilde{10} \to 11 \to 3 \to 24 \to 22 \to 15 \to \tilde{15} \to 16 \to 13$$
$$\to 14 \to 7 \to 20 \to \tilde{20} \to 21 \to 23 \to 4 \to 17.$$

[0587]

[0588] (정리 4.25)

[0589] 여기서, $\phi(z) = \frac{5+4z+3z^2+4z^4+z^5}{4z+7z^2+3z^4+z^5}$를 $\mathbb{P}^1(\mathbf{Q}_7)$에 대한 차수 5의 유리함수라고 하자. 그러면 ϕ의 7 축소 함수는 다음과 같다.

[0590] $$\bar{\phi} = \frac{(z+1)(z^4+3z^3+4z^2+6z+5)}{z(z^4+3z^3+4)}$$

[0591] 따라서 ϕ는 좋은 축소를 가지고 있다. $\bar{\phi}$의 전체 주기는 $(0, \infty, \xi_1, \xi_2, \xi_3, \xi_4, \xi_5, \xi_6) = (0, \infty, 1, 3, 2, 4, 5, 6)$로 주어지므로 축소 $\bar{\phi}$는 $\mathbb{P}^1(\mathbf{F}_7)$에서 추이적이다.

[0592] $[r_\infty, r_0, r_1, \cdots, r_6]$ = [5,1,3,2,2,5,2,3] 및 $[w_2, w_3, w_4, w_5, w_6]$ = [1,4,2,6,3]인지 확인하여 정리 4.20의 조건 (2) 및 (3)은 $\lambda_0 \equiv 28 \bmod 49$로 충족되므로 동력학계($\mathbb{P}^1(\mathbf{Q}_7)$, ϕ)은 최소이다.

[0593] 수준 2(level 2)에서 유도된 ϕ 시스템의 주기적인 궤도는 다음과 같이 주어진다.

$$0 \to \infty \to 1 \to 24 \to 23 \to 46 \to 26 \to 34 \to 28 \to \tilde{42} \to 43 \to 3 \to 30 \to 11$$
$$\to 47 \to 27 \to 7 \to \tilde{35} \to 36 \to 31 \to 37 \to 25 \to 19 \to 20$$
$$\to 35 \to \tilde{28} \to 29 \to 10 \to 44 \to 39 \to 40 \to 13 \to 14 \to \tilde{21} \to 22$$
$$\to 38 \to 2 \to 4 \to 12 \to 6 \to 42 \to \tilde{14}$$
$$\to 15 \to 17 \to 9 \to 18 \to 33 \to 48 \to 21 \to \tilde{7} \to 8 \to 45 \to 16 \to 32 \to 5 \to 41.$$

[0594]

[0595] (정리 4.26)

[0596] 여기서, $\phi(z) = \frac{31+15z-8z^2+z^3}{3z+12z^2+z^3}$를 $\mathbb{P}^1(\mathbf{Q}_7)$에 대한 차수 3의 유리함수라고 하자. 그러면 ϕ의 7 축소 함수는 다음과 같다.

[0597] $$\bar{\phi} = \frac{(z+1)(z^2+5z+3)}{z(z^2+5z+3)} = \frac{z+1}{z}$$

[0598] 그러므로 ϕ는 나쁜 축소를 갖는다. $\bar{\phi}$의 전체 주기는 $(0, \infty, \xi_1, \xi_2, \xi_3, \xi_4, \xi_5, \xi_6) = (0, \infty, 1, 2, 5, 4, 3, 6)$에 의해 제공되므로 축소 $\bar{\phi}$는 $\mathbb{P}^1(\mathbf{F}_7)$에서 추이적이다.

[0599] $[r_\infty, r_0, r_1, \ldots, r_6] = [1, 1, 6, 5, 3, 3, 5, 6]$와 $[w_2, w_3, w_4, w_5, w_6] = [6, 4, 5, 4, 6]$를 확인함으로써, 정리 4.20의

조건(2)와 (3)이 $\lambda_0 \equiv 21 \bmod 49$ 로 만족되므로 동력학계($\mathbb{P}^1(\mathbf{Q}_7)$, ϕ)이 최소가 된다. 수준 2(level 2)에서 유도된 ϕ 시스템의 주기적인 궤도는 다음과 같이 주어진다.

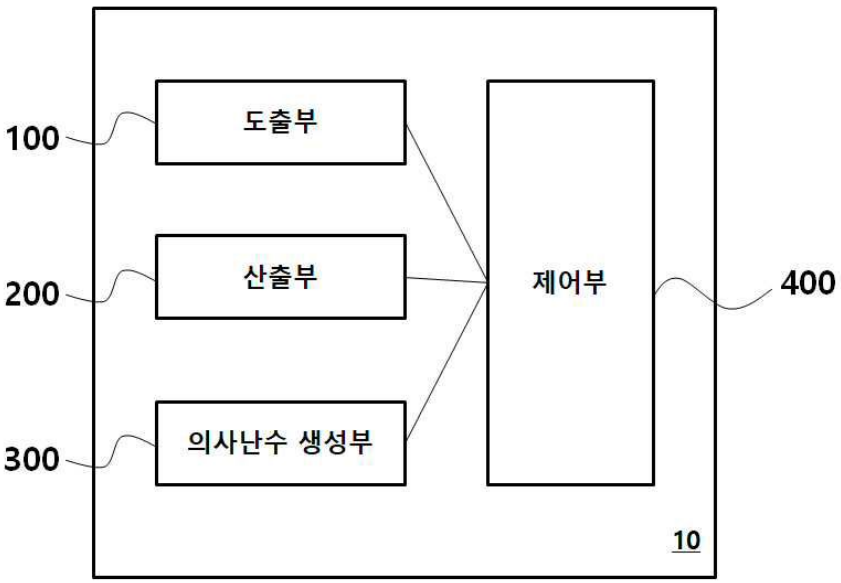
$$0 \to \infty \to 1 \to 30 \to 26 \to 25 \to 45 \to 34 \to 21 \to \tilde{21} \to 22 \to 9 \to 19 \to 39$$
$$\to 38 \to 13 \to 42 \to \tilde{42} \to 43 \to 37 \to 12 \to 4 \to 31$$
$$\to 41 \to 14 \to \tilde{14} \to 15 \to 16 \to 5 \to 18 \to 24 \to 20 \to 35 \to \tilde{35} \to 36 \to 44$$
$$\to 47 \to 32 \to 17 \to 48 \to 7 \to \tilde{7} \to 8 \to 23 \to 40 \to 46 \to 10$$
$$\to 27 \to 28 \to \tilde{28} \to 29 \to 2 \to 33 \to 11 \to 3 \to 6.$$

[0600]

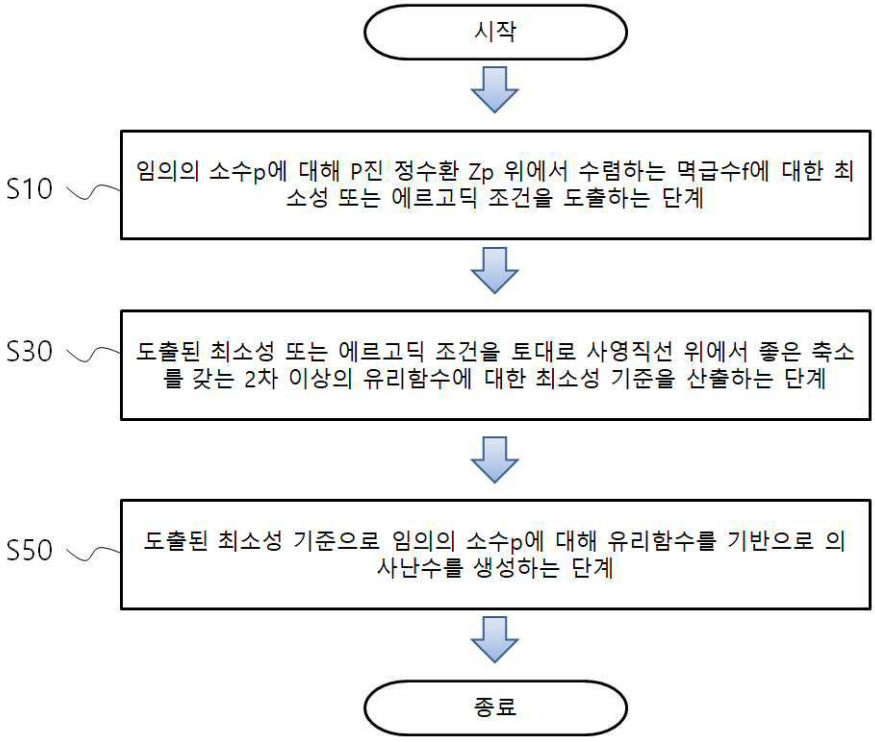
[0601] 이상에서 설명한 본 발명은 전술한 실시예 및 첨부된 도면에 의해 한정되는 것이 아니고, 본 발명의 기술적 사상을 벗어나지 않는 범위 내에서 여러 가지 치환, 변형 및 변경이 가능함은 당업자에게 명백할 것이다.

도면

도면1



도면2


시작
S10
임의의 소수p에 대해 P진 정수환 Zp 위에서 수렴하는 멱급수f에 대한 최소성 또는 에르고딕 조건을 도출하는 단계
S30
도출된 최소성 또는 에르고딕 조건을 토대로 사영직선 위에서 좋은 축소를 갖는 2차 이상의 유리함수에 대한 최소성 기준을 산출하는 단계
S50
도출된 최소성 기준으로 임의의 소수p에 대해 유리함수를 기반으로 의사난수를 생성하는 단계
종료