

Euclidean Domains and Euclidean Functions

Rod Downey

(Joint Work with Asher Kach)

NTU, September 2013

References

- Th. Motzkin, The Euclidean algorithm. *Bull. Amer. Math. Soc.*, 55:1142–1146, 1949.
- Leonard Schrieber. Recursive properties of Euclidean domains. *Ann. Pure Appl. Logic*, 29(1):59–77, 1985.
- Pierre Samuel. About Euclidean rings. *J. Algebra*, 19:282–301, 1971.
- V. Stoltenberg-Hansen and J. V. Tucker. Computable rings and fields. In *Handbook of computability theory*, volume 140 of *Stud. Logic Found. Math.*, pages 363–447. North-Holland, Amsterdam, 1999.
- J. Hiblot, Des Anneaux euclidiens dont le plus petit algorithmes n'est pas à valeurs finies, *C. R. Acad. Sci. Paris*, 281 (1975), 411-414 with correction in vol 287.
- Rod Downey and Asher Kach, Euclidean Functions of Computable Euclidean Domains, *Notre Dame Journal of Formal Logic*. Vol. 52 (No 2) (2011), 163-172.
- Chris Conidis, in preparation.

- 1 The Division Algorithm, Euclid's Algorithm, and Euclidean Domains
- 2 Transfinite Euclidean Domains and Rings
- 3 Computing Any Euclidean Function ϕ for \mathcal{R} and $\phi_{\mathcal{R}}$
- 4 Open Questions

The Division Algorithm...

Problem

Divide 18 into 218 (over \mathbb{Z}).

Answer.

Perform long division

$$\begin{array}{r} 12 \\ 18 \overline{) 218} \\ \underline{180} \\ 38 \\ \underline{36} \\ 2 \end{array}$$

and so $218 = 12 \cdot 18 + 2$.



The Division Algorithm...

Problem

Divide $x + 2$ into $x^3 + 18x^2 + 2x + 18$ (over \mathbb{Q}).

Answer.

Perform long division

and so $x^3 + 18x^2 + 2x + 18 = (x^2 + 16x - 30)(x + 2) + 78$. □

Euclid's Algorithm...

Proposition

The algorithm

```
function gcd(a,b)  
  if (a < b)  
    swap(a,b)  
  if (b == 0)  
    return a  
  return gcd(a - b,b)
```

computes the greatest common divisor of non-negative integers a and b.

Problem

Find the greatest common divisor of 18 and 10.

Answer.

Note $gcd(18, 10) = gcd(8, 10) = gcd(10, 8) = gcd(2, 8) = gcd(8, 2) = gcd(6, 2) = gcd(4, 2) = gcd(2, 2) = gcd(0, 2) = gcd(2, 0) = 2$. \square

Euclid's Algorithm...

Proposition

The algorithm

```
function gcd(a,b)
  if (a < b)
    swap(a,b)
  if (b == 0)
    return a
  return gcd(a - b,b)
```

computes the greatest common divisor of non-negative integers a and b.

Problem

Find the greatest common divisor of 18 and 10.

Answer.

Note $\gcd(18, 10) = \gcd(8, 10) = \gcd(10, 8) = \gcd(2, 8) = \gcd(8, 2) = \gcd(6, 2) = \gcd(4, 2) = \gcd(2, 2) = \gcd(0, 2) = \gcd(2, 0) = 2$. □

Remark

In both \mathbb{Z} and $\mathbb{Q}[X]$, the division algorithm (Euclid's algorithm) terminates because the dividend (either a or b) decreases in *size* at every step.

- Within \mathbb{Z} , the *size* of an integer is its magnitude.
- Within $\mathbb{Q}[X]$, the *size* of a polynomial is its degree.

Generalizing this requirement of remainders decreasing in *size* yields the (traditional) definition of a Euclidean domain.

Definition

A commutative ring \mathcal{R} is a *Euclidean ring* if there is a function $\phi : R^0 \rightarrow \mathbb{N}$ (where $R^0 := R \setminus \{0\}$) satisfying

$$(\forall a, d \in R^0)(\exists q \in R)[a + qd = 0 \text{ or } \phi(a + qd) < \phi(d)].$$

The function ϕ is termed a *Euclidean function* for \mathcal{R} .

If the ring is also an integral domain (i.e., there are no zero divisors) then it becomes a Euclidean Domain.

Euclidean Functions for \mathbb{Z} ...

Example

The integers \mathbb{Z} are a Euclidean domain.

Proof.

The functions

$$\phi_1(z) = |z|$$

$$\phi_2(z) = \lceil \log_2 |z| \rceil$$

$$\phi_3(z) = \begin{cases} |z| & \text{if } z \neq 5 \\ 13 & \text{otherwise} \end{cases}$$

are Euclidean functions for \mathbb{Z} .

Note that ϕ_3 serves as an example where the implication

$$x \text{ divides } y \quad \text{implies} \quad \phi(x) \leq \phi(y)$$

fails. □

Euclidean Functions for \mathbb{Z} ...

Example

The integers \mathbb{Z} are a Euclidean domain.

Proof.

The functions

$$\phi_1(z) = |z|$$

$$\phi_2(z) = \lceil \log_2 |z| \rceil$$

$$\phi_3(z) = \begin{cases} |z| & \text{if } z \neq 5 \\ 13 & \text{otherwise} \end{cases}$$

are Euclidean functions for \mathbb{Z} .

Note that ϕ_3 serves as an example where the implication

$$x \text{ divides } y \quad \text{implies} \quad \phi(x) \leq \phi(y)$$

fails. □

Euclidean Functions for \mathbb{Z} ...

Example

The integers \mathbb{Z} are a Euclidean domain.

Proof.

The functions

$$\phi_1(z) = |z|$$

$$\phi_2(z) = \lceil \log_2 |z| \rceil$$

$$\phi_3(z) = \begin{cases} |z| & \text{if } z \neq 5 \\ 13 & \text{otherwise} \end{cases}$$

are Euclidean functions for \mathbb{Z} .

Note that ϕ_3 serves as an example where the implication

$$x \text{ divides } y \quad \text{implies} \quad \phi(x) \leq \phi(y)$$

fails. □

Euclidean without Euclidean functions

Definition

If \mathcal{R} is a commutative ring (with 1), define a sequence of sets $\{R_n\}_{n \in \mathbb{N}}$ via recursion by

$$R_n := \{d \in R^0 : (\forall a \in R^0)(\exists q \in R) [a + dq = 0 \text{ or } a + dq \in R_{<n}]\}$$

where $R_{<n} = \bigcup_{m < n} R_m$ and $R^0 = R - \{0\}$.

Remark

Thus R_0 consists of the units, R_1 consists of those elements which exactly divide every other $a \in R^0$ or leave remainder a unit, etc. (NB if you read Samuel, $R_1 = R_2$ there)

Theorem (Motzkin 1949, Samuel 1971)

An integral domain \mathcal{R} (resp. ring) is a Euclidean domain (resp. ring) if and only if $R^0 = \bigcup_{n \in \mathbb{N}} R_n$.

Euclidean without Euclidean functions

Definition

If \mathcal{R} is a commutative ring (with 1), define a sequence of sets $\{R_n\}_{n \in \mathbb{N}}$ via recursion by

$$R_n := \{d \in R^0 : (\forall a \in R^0)(\exists q \in R) [a + dq = 0 \text{ or } a + dq \in R_{<n}]\}$$

where $R_{<n} = \bigcup_{m < n} R_m$ and $R^0 = R - \{0\}$.

Remark

Thus R_0 consists of the units, R_1 consists of those elements which exactly divide every other $a \in R^0$ or leave remainder a unit, etc. (NB if you read Samuel, $R_1 = R_2$ there)

Theorem (Motzkin 1949, Samuel 1971)

An integral domain \mathcal{R} (resp. ring) is a Euclidean domain (resp. ring) if and only if $R^0 = \bigcup_{n \in \mathbb{N}} R_n$.

Euclidean without Euclidean functions

Definition

If \mathcal{R} is a commutative ring (with 1), define a sequence of sets $\{R_n\}_{n \in \mathbb{N}}$ via recursion by

$$R_n := \{d \in R^0 : (\forall a \in R^0)(\exists q \in R) [a + dq = 0 \text{ or } a + dq \in R_{<n}]\}$$

where $R_{<n} = \bigcup_{m < n} R_m$ and $R^0 = R - \{0\}$.

Remark

Thus R_0 consists of the units, R_1 consists of those elements which exactly divide every other $a \in R^0$ or leave remainder a unit, etc. (NB if you read Samuel, $R_1 = R_2$ there)

Theorem (Motzkin 1949, Samuel 1971)

An integral domain \mathcal{R} (resp. ring) is a Euclidean domain (resp. ring) if and only if $R^0 = \bigcup_{n \in \mathbb{N}} R_n$.

The Least Euclidean Function $\phi_{\mathcal{R}}$

Definition (Motzkin 1949, Samuel 1971)

If \mathcal{R} is a Euclidean domain (ring), define $\phi_{\mathcal{R}} : R^0 \rightarrow \mathbb{N}$ by

$$\phi_{\mathcal{R}}(\mathbf{d}) = n$$

where n is least so that $\mathbf{d} \in R_n$.

Theorem (Motzkin 1949, Samuel 1971)

If \mathcal{R} is a Euclidean domain (resp. ring), the function $\phi_{\mathcal{R}}$ is a Euclidean function for \mathcal{R} . Moreover, it is the **least Euclidean function** for \mathcal{R} ; i.e., if ϕ is a Euclidean function for \mathcal{R} , then $\phi_{\mathcal{R}}(\mathbf{d}) \leq \phi(\mathbf{d})$ for all $\mathbf{d} \in R^0$.

Consequently, the function $\phi_{\mathcal{R}}$ satisfies

$$\phi_{\mathcal{R}}(\mathbf{d}) = \inf_{\phi} \phi(\mathbf{d})$$

where ϕ ranges over all Euclidean functions for \mathcal{R} .

The Least Euclidean Function $\phi_{\mathcal{R}}$

Definition (Motzkin 1949, Samuel 1971)

If \mathcal{R} is a Euclidean domain (ring), define $\phi_{\mathcal{R}} : R^0 \rightarrow \mathbb{N}$ by

$$\phi_{\mathcal{R}}(\mathbf{d}) = n$$

where n is least so that $\mathbf{d} \in R_n$.

Theorem (Motzkin 1949, Samuel 1971)

If \mathcal{R} is a Euclidean domain (resp. ring), the function $\phi_{\mathcal{R}}$ is a Euclidean function for \mathcal{R} . Moreover, it is the **least Euclidean function** for \mathcal{R} ; i.e., if ϕ is a Euclidean function for \mathcal{R} , then $\phi_{\mathcal{R}}(\mathbf{d}) \leq \phi(\mathbf{d})$ for all $\mathbf{d} \in R^0$.

Consequently, the function $\phi_{\mathcal{R}}$ satisfies

$$\phi_{\mathcal{R}}(\mathbf{d}) = \inf_{\phi} \phi(\mathbf{d})$$

where ϕ ranges over all Euclidean functions for \mathcal{R} .

The Least Euclidean Function $\phi_{\mathcal{R}}$

Definition (Motzkin 1949, Samuel 1971)

If \mathcal{R} is a Euclidean domain (ring), define $\phi_{\mathcal{R}} : R^0 \rightarrow \mathbb{N}$ by

$$\phi_{\mathcal{R}}(\mathbf{d}) = n$$

where n is least so that $\mathbf{d} \in R_n$.

Theorem (Motzkin 1949, Samuel 1971)

If \mathcal{R} is a Euclidean domain (resp. ring), the function $\phi_{\mathcal{R}}$ is a Euclidean function for \mathcal{R} . Moreover, it is the **least Euclidean function** for \mathcal{R} ; i.e., if ϕ is a Euclidean function for \mathcal{R} , then $\phi_{\mathcal{R}}(\mathbf{d}) \leq \phi(\mathbf{d})$ for all $\mathbf{d} \in R^0$.

Consequently, the function $\phi_{\mathcal{R}}$ satisfies

$$\phi_{\mathcal{R}}(\mathbf{d}) = \inf_{\phi} \phi(\mathbf{d})$$

where ϕ ranges over all Euclidean functions for \mathcal{R} .

- I am sure that, as logicians, you immediately notice that it is **unnecessary** in the definition of a Euclidean ring that the range of the ranking function is \mathbb{N} .
- Any ordinal will do, and maybe even well founded partial orders.

- 1 The Division Algorithm, Euclid's Algorithm, and Euclidean Domains
- 2 Transfinite Euclidean Domains and Rings
- 3 Computing Any Euclidean Function ϕ for \mathcal{R} and $\phi_{\mathcal{R}}$
- 4 Open Questions

Definition

A commutative ring \mathcal{R} is a **transfinite Euclidean ring** if there is a function $\phi : R^0 \rightarrow \text{ON}$ (where $R^0 := R \setminus \{0\}$ and ON is the class of ordinals) satisfying

$$(\forall a, d \in R^0)(\exists q \in R)[a + qd = 0 \text{ or } \phi(a + qd) < \phi(d)].$$

The function ϕ is termed a *transfinitely-valued Euclidean function* for \mathcal{R} .

Theorem (Motzkin 1949)

An integral domain \mathcal{R} is a transfinite Euclidean domain if and only if $R^0 = \bigcup_{\alpha \in \text{ON}} R_\alpha$. (Here we take unions at limit stages.)

Definition

A commutative ring \mathcal{R} is a **transfinite Euclidean ring** if there is a function $\phi : R^0 \rightarrow \text{ON}$ (where $R^0 := R \setminus \{0\}$ and ON is the class of ordinals) satisfying

$$(\forall a, d \in R^0)(\exists q \in R)[a + qd = 0 \text{ or } \phi(a + qd) < \phi(d)].$$

The function ϕ is termed a *transfinitely-valued Euclidean function* for \mathcal{R} .

Theorem (Motzkin 1949)

An integral domain \mathcal{R} is a transfinite Euclidean domain if and only if $R^0 = \bigcup_{\alpha \in \text{ON}} R_\alpha$. (Here we take unions at limit stages.)

Question (Motzkin 1949; Samuel 1971; Schrieber 1985)

Is there an integral domain that is a properly transfinite Euclidean domain? I.e., is there an integral domain having transfinitely-valued Euclidean functions but not finitely-valued Euclidean functions?

Theorem (Samuel 1971)

The function $\phi(z) = \omega \cdot i + j + 1$ is a Euclidean function for \mathbb{Z} , where $z = \pm 2^i(2j + 1)$.

Question (Motzkin 1949; Samuel 1971; Schrieber 1985)

Is there an integral domain that is a properly transfinite Euclidean domain? I.e., is there an integral domain having transfinitely-valued Euclidean functions but not finitely-valued Euclidean functions?

Theorem (Samuel 1971)

The function $\phi(z) = \omega \cdot i + j + 1$ is a Euclidean function for \mathbb{Z} , where $z = \pm 2^i(2j + 1)$.

Making Euclidean Rings

Lemma (Samuel, 1971)

If R is a Euclidean ring and A is a multiplicatively closed subset, then $A^{-1}R$ is Euclidean.

- A product of a finite number of transfinite Euclidean rings is i transfinite Euclidean.
- This gives an example of a properly transfinite Euclidean *ring*

Theorem (Samuel 1971)

The commutative ring $\mathbb{Z} \oplus \mathbb{Z}$ has a transfinitely-valued Euclidean function (indeed, one with range $\omega^2 + \omega^2$) but no finitely-valued Euclidean function.

- To prove this, we prove *If R has a finite Euclidean function with the R_0 finite, then for all n , $\phi^{-1}(n)$ is finite.*
- Induction. If $R'_n = \cup_{j=0}^{n-1} \phi^{-1}(j)$ is finite, and $\phi(b) = n$, then $R'_n \rightarrow R/Rb$ is surjective. The use algebra prove that in Noetherian ring the number of ideals with a given norm is finite, and hence the ideal Rb can only have a finite number of values. So only finitely many b .
- So if $\phi : \mathbb{Z} \oplus \mathbb{Z} \rightarrow \mathbb{N}$ is an Euclidean algorithm, and suppose $\phi((1, 0)) = n$ then $R'_n \rightarrow (\mathbb{Z} \oplus \mathbb{Z})(0, 1)$ is supposedly surjective, but the last ring is isomorphic to \mathbb{Z} which is infinite.

- You would likely naturally think of working in some ring like $\mathbb{Q}[X_i : i \in \omega]$ and perhaps taking quotients.
- The ring $\mathcal{R} := \mathbb{Q}[X]$ is a Euclidean domain with $\phi_{\mathcal{R}}(X) = 1$. Unfortunately, this is not very useful as $\mathbb{Q}[X, Y]$ is not a Euclidean domain.
- The question is how to control rank (e.g. 2) in an extension ring. For instance you *could* try adding roots but even here the situation is kind of murky.

- What about adding, say, square roots?

Theorem (Samuel, 1971)

The only imaginary quadratic fields of the form $\mathbb{Q}(\sqrt{-d})$ for which the ring of integers is a Euclidean domain are for $d = 1, 2, 3, 7, 11$.

- It is known for positive d which $\mathbb{Q}(\sqrt{d})$ are Euclidean for **the norm**, which is a measure associated with number fields, (See Samuel) it is 16 cases.
- Even $\mathbb{Z}[\sqrt{d}]$ is hard, with $d = 14$ recently done!

Nevertheless...

Theorem (Hiblot, 1975)

There is a Euclidean Domain (obtained as a certain quotient of formal power series over any ring R Euclidean for the g.c.d., like \mathbb{Z}) which has no finitely valued Euclidean function.

Theorem (Conidis, ta)

Call an ordinal θ of cardinality κ "relatively long" if every terminal segment of θ also has cardinality κ . Then, for every "relatively long" θ , there is a transfinite Euclidean domain of rank θ .

Bienvendu and Greenberg (unpubl) have used metamathematical methods to show such a domain can be countable. It is **open** if it can be computable.

Outline

- 1 The Division Algorithm, Euclid's Algorithm, and Euclidean Domains
- 2 Transfinite Euclidean Domains and Rings
- 3 Computing Any Euclidean Function ϕ for \mathcal{R} and $\phi_{\mathcal{R}}$
- 4 Open Questions

- Anyway, we were motivated by trying to understand the computability theory of the situation and the reverse mathematics.
- To wit, to what extent is having a Euclidean **algorithm** the same as having a Euclidean **function**.

Definition

A ring \mathcal{R} is *computable* if it has a *computable presentation*.

Definition

A *computable presentation* of an infinite ring $\mathcal{R} = (R : +, \cdot, 0, 1)$ is a bijection between R and \mathbb{N} so that the operations of addition and multiplication are *computable* functions on \mathbb{N} .

Definition

A computable presentation of a ring is a computably presented Euclidean ring iff there is a computable ranking function from the elements onto \mathbb{N} . In the transfinite case we would need a notation for the ordinal.

Definition

A ring \mathcal{R} is *computable* if it has a *computable presentation*.

Definition

A *computable presentation* of an infinite ring $\mathcal{R} = (R : +, \cdot, 0, 1)$ is a bijection between R and \mathbb{N} so that the operations of addition and multiplication are *computable* functions on \mathbb{N} .

Definition

A computable presentation of a ring is a computably presented Euclidean ring iff there is a computable ranking function from the elements onto \mathbb{N} . In the transfinite case we would need a notation for the ordinal.

Examples of Computable Rings...

Example

The ring \mathbb{Z} is a computable Euclidean ring.

Example

Let $S \subseteq \mathbb{N}$ be a (multiplicatively closed) *computably enumerable* set with $0 \notin S$ and $1 \in S$. Then the subset $\mathcal{R} \subseteq \mathbb{Q}$ consisting of those $a/b \in \mathbb{Q}$ with $b \in S$ is a computable ring. This uses the $A^{-1}R$ construction for $R = \mathbb{Z}$.

Proof.

Identify fractions $a/b \in \mathbb{Q}$ with natural numbers $n \in \mathbb{N}$ as they appear. □

Examples of Computable Rings...

Example

The ring \mathbb{Z} is a computable Euclidean ring.

Example

Let $S \subseteq \mathbb{N}$ be a (multiplicatively closed) *computably enumerable* set with $0 \notin S$ and $1 \in S$. Then the subset $\mathcal{R} \subseteq \mathbb{Q}$ consisting of those $a/b \in \mathbb{Q}$ with $b \in S$ is a computable ring. This uses the $A^{-1}R$ construction for $R = \mathbb{Z}$.

Proof.

Identify fractions $a/b \in \mathbb{Q}$ with natural numbers $n \in \mathbb{N}$ as they appear. □

- The first person to prove anything about computable Euclidean domains was Schrieber in his PhD from Cornell.
- In summary, he constructed a Euclidean domain which was a computable domain, and yet had no computable Euclidean function with range \mathbb{N} (In fact coded \emptyset') and showed the units need not be computable in a computable Euclidean domain.
- We extend these results by showing R_1 can be as complex as possible, removing the restriction \mathbb{N} , and examining the reverse mathematics of the situation. We also examine the possibility of Δ_2^0 Euclidean functions.
- The arguments are not difficult, but this is a situation where the question remaining are quite arresting.

Computing $\{z : \phi_{\mathcal{R}}(z) = 0\} \dots$

Theorem (Schrieber 1985)

There is a computable Euclidean domain $\mathcal{R} \subseteq \mathbb{Q}$ for which there is no “algorithm” to determine whether an element is a unit. In fact $R_0 \equiv_m \emptyset'$.

Proof.

Identify the Halting Problem K with a subset of the prime numbers. Have \mathcal{R} consist of those fractions $a/b \in \mathbb{Q}$ with b a multiple of elements of K . Then p prime is a unit iff $p \in \emptyset'$. □

Proposition (Schrieber 1985)

Despite this, the Euclidean domain \mathcal{R} has a computable Euclidean function ϕ .

Proof.

Write $z = \frac{a}{b} \in \mathbb{Q}$ in lowest terms, and then define $\phi(z) = a$. □

Computing $\{z : \phi_{\mathcal{R}}(z) = 0\} \dots$

Theorem (Schrieber 1985)

There is a computable Euclidean domain $\mathcal{R} \subseteq \mathbb{Q}$ for which there is no “algorithm” to determine whether an element is a unit. In fact $R_0 \equiv_m \emptyset'$.

Proof.

Identify the Halting Problem K with a subset of the prime numbers. Have \mathcal{R} consist of those fractions $a/b \in \mathbb{Q}$ with b a multiple of elements of K . Then p prime is a unit iff $p \in \emptyset'$. □

Proposition (Schrieber 1985)

Despite this, the Euclidean domain \mathcal{R} has a computable Euclidean function ϕ .

Proof.

Write $z = \frac{a}{b} \in \mathbb{Q}$ in lowest terms, and then define $\phi(z) = a$. □

Computing $\{z : \phi_{\mathcal{R}}(z) = 0\} \dots$

Theorem (Schrieber 1985)

There is a computable Euclidean domain $\mathcal{R} \subseteq \mathbb{Q}$ for which there is no “algorithm” to determine whether an element is a unit. In fact $R_0 \equiv_m \emptyset'$.

Proof.

Identify the Halting Problem K with a subset of the prime numbers. Have \mathcal{R} consist of those fractions $a/b \in \mathbb{Q}$ with b a multiple of elements of K . Then p prime is a unit iff $p \in \emptyset'$. □

Proposition (Schrieber 1985)

Despite this, the Euclidean domain \mathcal{R} has a computable Euclidean function ϕ .

Proof.

Write $z = \frac{a}{b} \in \mathbb{Q}$ in lowest terms, and then define $\phi(z) = a$. □

Corollary in Reverse mathematics

- Reverse mathematics seeks to calibrate the proof theoretical strength of theorems of mathematics in terms of **comprehension** axioms (saying that something of a certain definable complexity exists) in second order arithmetic.
- I'll assume you are familiar with this.
- This usually goes hand in hand with computability theory. For example, usually showing that \emptyset' is coded in a computable setting aligns to ACA_0 . (Of course there are counterexamples, one of my favourites is Kruskal's Theorem on wqo of finite trees. It is "computably true" but is certainly not provable in RCA_0 .)
- The result above suggest that the existence of a minimal functions implies ACA_0 .

- A priori, there is no reason for the minimal Euclidean function ϕ (in \mathcal{M}) to satisfy $\phi = \phi_{\mathcal{R}}$.

Lemma (RCA₀)

Fix a Euclidean domain \mathcal{R} and a non-minimal finitely-valued Euclidean function ϕ for \mathcal{R} . Let α be the least ordinal for which there is a $T \in R$ with $\alpha = \phi_{\mathcal{R}}(T) < \phi(T)$. Then (fixing such a T)

$$\hat{\phi}(z) = \begin{cases} \phi(z) & \text{if } z \neq T \\ \phi_{\mathcal{R}}(T) & \text{if } z = T \end{cases}$$

is a finitely-valued Euclidean function for \mathcal{R} and satisfies $\hat{\phi} \neq \phi$.

Proof.

Since $\hat{\phi}(T) = \phi_{\mathcal{R}}(T) < \phi(T)$, it is immediate that $\hat{\phi} \neq \phi$. As α was chosen minimal, for any $A \in R$, there exists a $Q \in R$ with $\phi(A + QT) < \phi(T)$ as $\phi(A + QT) = \phi_{\mathcal{R}}(A + QT) < \phi_{\mathcal{R}}(T) = \alpha$. □

Theorem

(RCA_0) *The statement*

MEF: every Euclidean domain has a minimal Euclidean function

proves ACA_0 .

Fixing a set X in the model, we show X' exists. We consider the X -computable ring whose units are $\Sigma_1^0(X)$ -complete constructed by relativizing Schrieber's construction of a computable subring of the rationals whose units are intrinsically Σ_1^0 -complete. As noted in the introduction, the (relativized) ring \mathcal{R} has a computable Euclidean function, namely $\phi(a/b) = a$. Thus, it is a Euclidean domain, i.e., it has a Euclidean function in the model.

Consequently, by MEF, we may fix a minimal Euclidean function ϕ for \mathcal{R} (so that $\phi \leq \phi'$ for all ϕ' in the model). We argue that $\phi = \phi_{\mathcal{R}}$. If not, the function $\hat{\phi}$ of the lemma above is in the model as $\hat{\phi} \equiv_T \phi \equiv_T \emptyset$ and is a Euclidean function for \mathcal{R} . But then we would have $\hat{\phi} < \phi$, contradiction the minimality of ϕ . Thus it must be the case that $\phi = \phi_{\mathcal{R}}$. As $\phi_{\mathcal{R}}$ computes X' , the model must be closed under the Turing Jump.

How complicated?

- As the set R_0 is Σ_1^0 , being the collection of units
- The set R_n is Π_{2n}^0 for $0 < n < \mathbb{N}$.
- If $\phi_{\mathcal{R}}$ is finitely-valued, then $\phi_{\mathcal{R}}$ is $\emptyset^{(\omega)}$ -computable.
- In the transfinite case the same for n on some path in Π_1^1 .
- So proof theoretically upper bounds for the finite case is ACA_0^+ and transfinitely $\Pi_1^1 - CA_0$.

Theorem

There is a Euclidean computable domain \mathcal{R} having no transfinitely-valued computable Euclidean function ϕ . Moreover, every transfinitely-valued Euclidean function ϕ for \mathcal{R} computes \emptyset' .

Theorem

There is a computable Euclidean domain \mathcal{R} for which the set R_1 is Π_2^0 -complete.

Theorem

There is a Euclidean computable domain \mathcal{R} for which there is no finitely-valued \emptyset' -computable Euclidean function ϕ .

Theorem

There is a computable Euclidean domain \mathcal{R} having no computable finitely-valued Euclidean function but having a computable transfinitely-valued Euclidean function.

The underlying ring

- We use extensions of the ideas of Schrieber.

Definition (Schrieber 1985)

If K is a field and $\{X_i\}_{i \in \mathbb{N}}$ is a set of variables, denote by $K \langle X_i \rangle_{i \in \mathbb{N}}$ the commutative ring of reduced fractions p/q with $p, q \in K[X_i]_{i \in \mathbb{N}}$ and $X_i \nmid q$ for all i .

- Thus, every element x of the commutative ring $K \langle X_i \rangle_{i \in \mathbb{N}}$ is the product of a monomial m and a unit u .

Why is this good?

Theorem (Schrieber 1985)

The function $\phi(x) = \phi(mu) := \deg(m)$, where m is a monomial and u is a unit, is the least Euclidean function for $K \langle X_i \rangle_{i \in \mathbb{N}}$. In particular, $K \langle X_i \rangle_{i \in \mathbb{N}}$ is a Euclidean domain.

- All the Euclidean domains we construct will be of the form $K \langle X_i \rangle_{i \in \mathbb{N}}$, where the field K is either \mathbb{Q} or $\mathbb{Q}(Z_j)_{j \in \mathbb{N}}$, for some sets of formal variables $\{X_i\}_{i \in \mathbb{N}}$ and $\{Z_j\}_{j \in \mathbb{N}}$.

Proposition (Samuel 1971)

If \mathcal{R} is an integral domain and $A, T \in R$ are nonzero, then $\phi_{\mathcal{R}}(T) \leq \phi_{\mathcal{R}}(AT)$.

Proof.

The function $\phi(T) := \min_{0 \neq A \in R} \phi_{\mathcal{R}}(AT)$ satisfies

$$\phi_{\mathcal{R}}(T) \leq \phi(T) \leq \phi_{\mathcal{R}}(1T) = \phi_{\mathcal{R}}(T)$$

as a consequence of the minimality of $\phi_{\mathcal{R}}$ and taking 1 for A . It is clear that ϕ , and thus $\phi_{\mathcal{R}}$, has the desired property. \square

Proposition

[Folklore] If \mathcal{R} is an integral domain, $A, T \in R$ are nonzero, and A is a nonunit, then $\phi_{\mathcal{R}}(T) < \phi_{\mathcal{R}}(AT)$.

Proof.

Since A is a nonunit, it follows AT does not divide T . Thus

$$\min_{Q \in R} \{\phi_{\mathcal{R}}(T + QAT)\} < \phi_{\mathcal{R}}(AT)$$

by virtue of the definition of R_{α} . By the proposition above (as $1 + QA \neq 0$ for all $Q \in R$), we have

$$\min_{Q \in R} \{\phi_{\mathcal{R}}(T + QAT)\} = \min_{Q \in R} \{\phi_{\mathcal{R}}(T(1 + QA))\} \geq \phi_{\mathcal{R}}(T). \quad \square$$

Killing transfinite computable functions

- Instead of killing the ordinal based functions work on computable suborderings of \mathbb{Q} . I.e (partial) computable relations

$$E_\phi(x, y) := \{(x, y) \in R \times R : \phi(x) \leq \phi(y)\}.$$

This is justified because E_ϕ is computable if ϕ is a computable transfinitely-valued Euclidean function.

- Idea Have a $\{E_i\}_{i \in \mathbb{N}}$ of partial computable binary relations. The idea is to determine whether $E_i(X_i, Y_i)$ or $E_i(Y_i, X_i)$ (if either computation converges) and assure this cannot be the case by making either X_i a power of Y_i or Y_i a positive power of X_i .
- At stage s , we introduce terms X_s and Y_s . For each $i \leq s$, we check whether $E_i(X_i, Y_i) \downarrow = 1$ or $E_i(Y_i, X_i) \downarrow = 1$. If either has newly converged, we put $X_i = Y_i^s$ if $E(X_i, Y_i) \downarrow = 1$ and $Y_i = X_i^s$ otherwise. Finally, at each stage s , we continue the enumeration of the ring, working towards $\mathbb{Q} \langle X_i, Y_i \rangle_{i \in \mathbb{N}}$

Making $R_1 \Pi_2^0$ complete

- Fix a Π_2^0 -complete set S and a computable predicate $P(i, s)$ so that $i \in S$ if and only if $\exists^\infty s [P(i, s)]$.
- Begin with \mathbb{Q} and expressions $\{Z_i\}_{i \in \mathbb{N}}$.
- Make $Z_i = X_{i,j} Y_{i,j}$ beginning with $j = 0$
- When the Π_2^0 predicate looks correct make $Y_{i,j}$ a unit, and move to fresh variables $Z_i = X_{i,j+1} Y_{i,j+1}$
- If $i \in S$, Z_i has rank 1, as every Y is turned into a unit,
- If $i \notin S$, Z_i has rank 2 as it gets stuck on some $Z_{i,j} Y_{i,j}$.

Killing Δ_2^0 rank functions

- Rely on the fact that if *any* rank function has something of rank n , then the *minimal* one has rank $\leq n$.
- Want to kill $\phi_e(x) = \lim_s \phi_e(x, s)$ i.e. show it has no limit or the limit is wrong. Might as well take $\phi_e(x, s)$ as primitive recursive.
- Wlog we assume that if $\phi_e(x, s) \neq \phi_e(x, s + 1)$, then one of the two is 0.
- At stage s we compute $\phi_e(X_e, s)$. If this is $\neq \phi_e(X_e, s + 1)$, introduce $\phi_e(X_e, s + 1) + 1$ many new variables $X_{e,s,0}, X_{e,s,1}, \dots, X_{e,s,\phi_e(X_e,s)}$ to the ring R and declare their product equal to X_e .

No computable finitely valued, but computable transfinite

- Analyze Schrieber's construction.
- At each stage s , we create a term X_s . For each $i \leq s$ for which $\phi_i(X_i)$ newly converges, we create a new variable Y_i and set $X_i = Y_i^{\phi_i(X_i)+1}$.
- The X_i are mapped to \mathbb{N} (or $\mathbb{N} + 1$ depending on your notation system). They then drop to an assigned value if $\phi_i(X_i) \downarrow$.

- 1 The Division Algorithm, Euclid's Algorithm, and Euclidean Domains
- 2 Transfinite Euclidean Domains and Rings
- 3 Computing Any Euclidean Function ϕ for \mathcal{R} and $\phi_{\mathcal{R}}$
- 4 Open Questions

Question

What's the correct answer? How to control even R_2 ?

Remark

- This is the limit of the techniques for this kind of ring. The point is that everything is defined by the rank 1 elements, and hence \emptyset'' can figure out the ranks of everything.
- Similar remarks seem to apply to any introduction of *algebraic* elements.
- We could not seem to control the introduction of $+$, so controlling $Z + QX$ to not be a unit for all Q in the ring.
- Maybe the answer is yes, meaning that all domains are actually controlled by low level ranked sets.
- Same questions apply to *rings* in place of domains.

Question

Is there a computable Euclidean domain (ring) having (classically) no Euclidean function with range strictly less than ω_1^{CK} ? What about the reverse math? finite valued has upper bound ACA_0^+ , and transfinite Π_1^1 -CA.

Question

What more can be said [classically] about (transfinite) Euclidean domains? What more can be said about computable (transfinite) Euclidean domains?

Bienvu and Greenberg have looked at Hiblot's construction and believe that using primitive recursive power series the result more or less goes through and for such you can construct a Π_1 Euclidean domain with no finitely valued Euclidean function.

Question

Is there a computable Euclidean domain (ring) having (classically) no Euclidean function with range strictly less than ω_1^{CK} ? What about the reverse math? finite valued has upper bound ACA_0^+ , and transfinite Π_1^1 -CA.

Question

What more can be said [classically] about (transfinite) Euclidean domains? What more can be said about computable (transfinite) Euclidean domains?

Bienvenu and Greenberg have looked at Hiblot's construction and believe that using primitive recursive power series the result more or less goes through and for such you can construct a Π_1 Euclidean domain with no finitely valued Euclidean function.

Thank you