WHY EUCLIDEAN DOMAINS ARE BOTH EASIER AND HARDER THAN YOU THINK

Pace P. Nielsen

(Joint work with Chris Conidis and Vandy Tombs)

Brigham Young University

Section 1: Generalizations Galore

Euclid's Problem

- Let n, d be two given integers.
- Find GCD(n, d).
- What is the "best" way?
- Euclid's idea: Repeated subtraction.

Algorithm Example

- Take $n = 13, d = 8.$

$$13 = 1 \cdot 8 + 5$$
$$8 = 1 \cdot 5 + 3$$
$$5 = 1 \cdot 3 + 2$$
$$3 = 1 \cdot 2 + 1$$
$$2 = 2 \cdot 1 + 0$$

What is a GCD?

- The word “greatest” comes from the order on ideals.
- A *GCD domain* is:
  - A domain.
  - For any two principal ideals, there is a minimal principal ideal above them.

Problems with this?

- GCD$(a, b) \notin (a, b)$, in general.
- No method to find the GCD.
- The condition is somewhat *ad hoc*.

Better Definition

- A *Bézout domain* is:
  - A domain.
  - (a, b) is always principal.

Problems with this?

- Still no method to find the GCD.
- No back-forth procedure.
- However, much more natural.
  - Ring of algebraic integers.
  - Ring of entire functions on $\mathbb{C}$.

Stronger Definition

- A *quasi-Euclidean* domain is:
  - A domain.
  - For each pair of elements a, b there is a "terminating division chain."

Terminating Chain

- $a = q_1 b + r_1$
- $b = q_2 r_1 + r_2$
- $\vdots$
- $r_{n-1} = q_{n+1} r_n + 0$

Problems with this?

- Still no method to find the GCD.

- Still quite natural.
  - Cooke: All class number 1 rings of integers.

Another Definition

- A *unique factorization domain* is:
  - A domain.
  - Every element has a prime factorization.
  - The factorization is unique, up to order and associates.

Problems with this?

- Still no method to find the GCD.
- (Unless a factoring algorithm exists.)
- Often hard to verify this property.
- Equivalent formulation: GCD-domain + ACCP.
- UFD+Bézout=PID

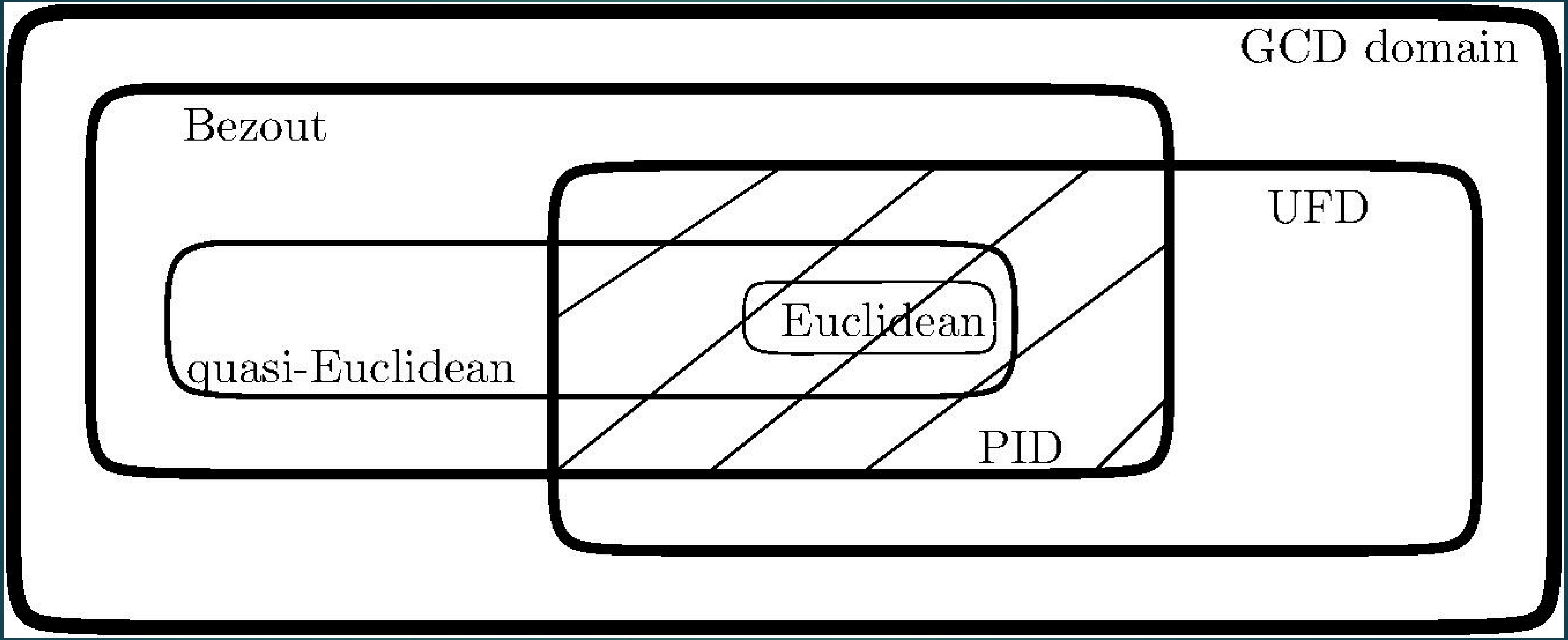
Final Definition?

- A *Euclidean domain* is:
  - A domain R.
  - Equipped with $\varphi: R \setminus \{0\} \to \mathbb{N}$.
  - For every $n, d \in R \setminus \{0\}$:
    - Either $d|n$, or
    - there exist $q \in R$, $\varphi(n - qd) < \varphi(d)$.

Problems with this?

- Still no method to find the GCD!
- But Euclid's algorithm "exists".

- Is it nice algebraically?
- Is the condition natural?
  - Answer: Motzkin's Lemma


GCD domain
Bezout
UFD
Euclidean
quasi-Euclidean
PID

Section 2: Euclidean Norms

Norms

- Some norms are better than others.
  - Take $n = 13, d = 8.$

$$13 = 1 \cdot 8 + 5$$
$$8 = 1 \cdot 5 + 3$$
$$5 = 1 \cdot 3 + 2$$
$$3 = 1 \cdot 2 + 1$$
$$2 = 2 \cdot 1 + 0$$

Norms

- Take $n = 13, d = 8$.
  - $13 = 2 \cdot 8 + (-3)$
  - $8 = (-3) \cdot (-3) + (-1)$
  - $(-3) = (-3) \cdot (-1) + 0$

Motzkin’s Idea

- Let the norm measure complexity.
- Complexity measured by how easy it is to divide.
- Complexity 0: Remainder is zero.
- Units.

Motzkin’s Idea

- Complexity 1: Remainders are zero or units.
- Universal side divisors.
- Complexity 2: Remainders are zero, units, and universal side divisors.

Example

- For $\mathbb{Z}$
  - $S_0 = \{\pm 1\}$
  - $S_1 = \{\pm 1, \pm 2, \pm 3\}$
  - $S_2 = \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \pm 6, \pm 7\}$
- Complexity: $\lfloor \log_2 |x| \rfloor$.

Example

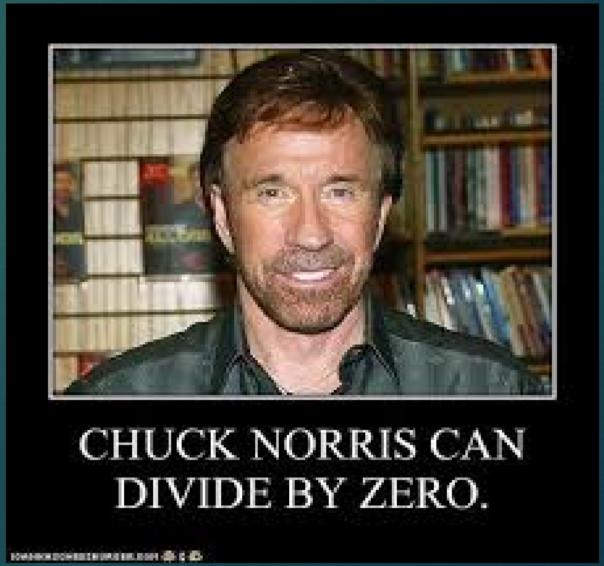
- For a field F
  - $S_0 = F \setminus \{0\}$
  - $S_1 = F$
  - $S_2 = F$
- Complexity: 0.

Motzkin's Lemma

- Let R be a domain.
- Recursively define:
- $S_n = \{x \in R : \forall y \in R, \exists r \in S_m \cup \{0\} \text{ for some } m < n, x|(y-r)\}$.
- These sets always stabilize.
- R=Euclidean iff $S_\omega = R$.

Side Note

- What is the norm of 0?
- Three main options.
- Think: Order the ideals.



Norms

- Motzkin: Let R be a Euclidean domain.
- Define $\varphi: R \setminus \{0\} \to \mathbb{N}$ by
  - $\varphi(x) = \min(n : x \in S_n)$.
- Then φ is a Euclidean norm.
- It is minimal:
  - $\varphi(x) \leq \psi(x)$.

Examples

- For $\mathbb{Z}$
  - $\lfloor \log_2 |x| \rfloor$
- For a field
  - Constant 0 function
- Lenstra: Worked out for $\mathbb{Z}[i]$ and $\mathbb{Z}[\omega]$.
  - To big to fit in the margins.

Obvious question

- Euclidean norms $\varphi: R \setminus \{0\} \to \mathbb{N}$.
  Why $\mathbb{N}$? Why not $\mathbb{R}$?
- Euclid's algorithm terminates.
- **Everything** still works if we replace $\mathbb{N}$ with the ordinals.

Everything?

- Motzkin's Lemma:
  - R is transfinitely Euclidean iff $S_\alpha = R$.

- Transfinitely Euclidean domains are PIDs.

- Euclid's algorithm terminates.

Everything?

- Motzkin:
  - Minimal norms exist.
- Lenstra:
  - Minimal norms are super-additive:
  - $\varphi(xy) \geq \varphi(x) \oplus \varphi(y)$.

Everything?

- Okay, not **everything**.
- The stabilization point is different.
- Fields stabilize at complexity 1.
- Euclidean domains stabilize at ω.
  - Unless they are fields.
- Are there any others?

Transfinite examples

- Hiblot (1975) found an example.
- Nagata (1977-78) found an error, and produced a different example.
- Hiblot (1977) fixed his example.
- Both very complicated.
- Stabilized at ω^2.
- No other examples.

New Results

- (1) Every transfinite Euclidean domain stabilizes at ω^{α}.

- Proof: Easy consequence of Lenstra's super-additive result.

New Results

- (2) For every α there is a transfinite Euclidean domain which stabilizes at ω^{α}.

- Corollary: Complexity can be arbitrarily large.
- Proof: We'll sketch it later.

New Results

- (3) Euclidean domains without multiplicative norms exist.
- Proof: Modify the construction we sketch below.

Proof Sketch

- Fix an ordinal α.
- Let $R_0 = F[x_{\{\beta\},0} : 1 \leq \beta \leq \omega^\alpha]$.

- Idea: $x_{\{\beta\},0}$ will have complexity β.
- Define such a “norm” φ on R_0.

Proof Sketch

- Not Euclidean yet.
- Don’t always have quotients to get simpler remainders.

- When $\mathrm{GCD}(n, d) = 1$, $\varphi(n) \geq \varphi(d) \geq 1$, then
- Adjoin a new quotient $q = q_{T,1,n,d}$.

Proof Sketch

- Let $R_1 = R_0[x_{\{\beta\},1}, q_{T,1,n,d}]$.
- Extend φ to R_1 in the obvious way, and
  - $\varphi\left(n - q_{T,1,n,d}d\right) = \max(\beta \in T : \beta < \varphi(d))$

- Don't always have quotients to get simpler remainders.
- Repeat this process.

Proof Sketch

- Let $R_\infty = \bigcup_{i=0}^{\infty} R_i$.
- Polynomial ring in many variables, not Euclidean.

- Invert all elements of norm zero.
- φ is the minimal norm.

Open Problems

- Is there a Euclidean domain with no (well-ordered) multiplicative norm in $\mathbb{R}$?
- More generally, is there a Euclidean domain with no “multiplicative” norm in the ordinals?
- How does the transfinite condition apply to PID number rings?

THANK YOU FOR YOUR ATTENTION