The complexity of primes in computable UFDs

Damir D. Dzhafarov
University of Connecticut

March 7, 2015

Joint work with Joseph Mileti.

Review of definitions.

An integral domain is a commutative ring with identity and no zero-divisors.

A nonzero element p of an integral domain is:

1. irreducible if whenever $p = ab$ then either a is a unit or b is a unit;
2. prime if whenever $p \mid ab$ then either $p \mid a$ or $p \mid b$.

In an integral domain, prime elements are irreducible, but not conversely.

Example. In $\mathbb{Z}[\sqrt{-5}]$, we have $2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$.

A unique factorization domain (UFD) is an integral domain such that:

1. every nonzero nonunit element can be written as a product of irreducibles;
2. any such product of irreducibles is unique up to associates.

In a UFD, every irreducible element is prime.

The complexity of primes.

Question. How complicated is the set of primes in a given computable ring A?

On its face, this set is Π^0_2, but in many natural examples it is less complicated.

Examples.

1. In $\mathbb{Z}$, the primes are computable.

2. In $\mathbb{Z}[i]$, the primes are computable.

3 (Schubert; Kronecker). In $\mathbb{Z}[x]$, the primes are computable.

Furthermore, in any computable presentation of any of the above rings, the primes are still computable.

Is the set of primes in a computable UFD always computable? (Fröhlich and Shepherdson: No.) Does the answer depend on the presentation?

Complicated presentations.

In computable algebra, one often builds computable objects in which the desired codings are achieved by algebraically complicated means.

Theorem (Friedman, Simpson, and Smith). There is a computable local ring whose (unique) maximal ideal computes $\emptyset'$.

Theorem (Friedman, Simpson, and Smith). There is a computable ring whose every prime ideal has PA degree.

Theorem (Downey and Kach). There is a computable Euclidean domain R for which the set R_1 is Π^0_2-complete.

Each of these constructions starts with a ring like $\mathbb{Q}[x_0, x_1, \ldots]$, and it is the algebraic independence of the x_i that is then used to do the coding. In other presentations, this coding might not be recoverable.

The main theorem.

Let $p_0, p_1, \ldots$ be the primes in $\mathbb{N}$.

Theorem (Dzhafarov and Mileti).

Let Q be a Π^0_2 set. There is a computable UFD A such that:

1. A extends $\mathbb{Z}$;
2. $i \in Q$ if and only if p_i is prime in A.

If A is a computable UFD extending $\mathbb{Z}$, and B is any computable copy of A, then we can computably find the representation of each p_i in B.

Taking a Π^0_2-complete set for P above we thus obtain:

Corollary. There exists a computable UFD A such that set of primes is Π^0_2-complete in every computable presentation of A.

Basic idea of the proof.

We turn the primes in $\mathbb{N}$ on or off based on the Π^0_2 membership in Q.

Fix an approximation to Q. By default, assume i shows up only finitely often.

To start, we introduce a factorization $p_i = xy$. The next time i shows up, we destroy this factorization by turning x into a unit. We then introduce a new factorization, $p_i = x'y'$, and repeat.

In the end, if i shows up infinitely often, we will have destroyed each of the factorizations of p_i in A, and so p_i will be prime.

If i shows up only finitely often, some factorization will be permanent, and p_i will not be prime.

Our tools will be quotients and localizations.

Preserving structure.

Our main concern is to preserve useful algebraic structural properties.

If we try to factor p_i by introducing a square root for p_i, we might interfere with the primeness of other elements.

More generally, quotients need not preserve unique factorization.

Example. In $\mathbb{Z}[\sqrt{7}]$, we have that 3 divides $(1+\sqrt{7})(1-\sqrt{7})$.

While $\mathbb{Z}[x]$ is a UFD, the quotient $\mathbb{Z}[x]/\langle x^2+5\rangle \cong \mathbb{Z}[\sqrt{-5}]$ is not.

Other concerns:

- Does destroying a factorization introduce new primes?

- Might we introduce new units?

- What does the ring we obtain in the limit look like?

Construction.

We let $A = \bigcup_{n\in\omega} A_n$, where

$$\mathbb{Z} = A_0 \subseteq A_1 \subseteq A_2 \subseteq \cdots$$

are built as follows:

1. when we want to factor p_i, we let $A_{n+1} = A_n[x, y]/\langle p_i - xy\rangle$.
2. when we want to destroy the factorization $p_i = xy$, we let A_{n+1} be the localization of A_n at $S = \{1, x, x^2, \ldots\}$.

We demand that each A_n be not only a UFD but also Noetherian (i.e., to have no strictly ascending sequence of ideals) for reasons we will see later.

Gauss showed that $A[x]$ is a UFD if A is, while Hilbert showed that $A[x]$ is Noetherian if A is. And being a Noetherian UFD is preserved by localization.

Turning a prime into a unit.

Fix A_n, with x prime in A_n. (Think $p_i = xy$.)

Suppose we wish to turn x into a unit. (To destroy the factorization.)

Let $S = \{1, x, x^2, \ldots\}$ and $B = S^{-1}A_n$.

Proposition.

1. If A_n is computable and $\{a \in A_n : x \mid a\}$ is computable, we can build B as a computable extension of A_n.
2. Primes in A_n not associated to x are prime in B.
3. Primes that were not associates in A_n are also not associates in B.
4. If $p \in B$ is prime, then $\{b \in B : p \mid b\}$ is computable.

(We did not need the Noetherian assumption here.)

Introducing a factorization.

Let $B = A_n[x, y]/\langle p_i - xy \rangle$. (To introduce the factorization $p_i = xy$.)

Proposition.

1. If A_n is computable, we can build B as a computable extension of A_n.
2. x and y are prime in B, and are not associates.
3. If $\{a \in A_n : p_i \mid a\}$ is computable, so are $\{b \in B : x \mid B\}$ & $\{b \in B : y \mid B\}$.
5. If A_n is a Noetherian UFD, so is B.

Proof of 5. Nagata's criterion states that if R is a Noetherian domain and S is any multiplicative set generated by primes in R, then R is a UFD if $S^{-1}R$ is. Let $S = \{1, x, x^2, \ldots\}$. Then $S^{-1}B$ is basically just $S^{-1}A_n[x]$, so it is a localization of a Noetherian UFD and hence is a Noetharian UFD.

Thank you.