Signatures of (Circular) Units in Cyclotomic Fields

Evan P. Dummit

Arizona State University

CNTA XV

July 9, 2018

Outline

Outline of talk:

1. Signatures of units
2. Circular units in real cyclotomic fields and their signatures
3. Unit signature ranks in families of real cyclotomic fields

This is joint work with D. Dummit and H. Kisilevsky.

Signatures, I

Let F be a finite Galois extension of $\mathbb{Q}$ having n real embeddings.

If we fix an order of these embeddings, we obtain a "signature map" sending a nonzero $\alpha \in F$ to its associated "signature" representing the pattern of signs (positive or negative) of α in each of the n real embeddings of F.

Example

For $F = \mathbb{Q}(\sqrt{2})$ *and* $\alpha = 1 + \sqrt{2}$*, the two real embeddings of* α *are* $(1 + \sqrt{2}, 1 - \sqrt{2})$ *with respective signs* $(+1, -1)$*.*

Signatures, II

The signature map is a homomorphism into the signature space $\{\pm 1\}^n \cong \mathbb{F}_2^n$. We will be interested in the image of the units of F:

Definition

The (archimedean) unit signature rank of F is the rank (as a 2-group) of the group of unit signatures of F.

For real quadratic fields, the unit signature rank is 1 if the fundamental unit is totally positive (i.e., if it has norm 1) and 2 otherwise (i.e., if it has norm -1).

Circular Units and Signatures, I

We now focus on the case of real cyclotomic fields:

- Let m be a positive integer (either odd or divisible by 4) and ζ_m be a primitive mth root of unity
- Let $K_m^+ = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$ be the associated real cyclotomic field.
- For m an odd prime power, we consider the "circular units" in K_m^+, generated by -1 and the elements $U_a = \dfrac{\zeta_m^a - \zeta_m^{-a}}{\zeta_m - \zeta_m^{-1}}$, for $1 < a < m/2$ and a relatively prime to m.
- These circular units are multiplicatively independent and generate a finite-index subgroup of the full unit group isomorphic to $(\mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}^{\varphi(m)/2-1}$.

Circular Units and Signatures, II

The signature rank of the circular units is a lower bound for the signature rank of the full group of units, so we next analyze signatures of circular units:

- We can enumerate the embeddings using the elements σ_b of $\mathrm{Gal}(K_m^+/\mathbb{Q})$, where $\sigma_b(\zeta_m) = \zeta_m^b$, for each b relatively prime to m with $1 \le b < m/2$.
- Explicitly, the bth embedding of U_a is given by $\sigma_b(U_a) = \dfrac{\zeta_m^{ab} - \zeta_m^{-ab}}{\zeta_m^b - \zeta_m^{-b}} = \dfrac{\sin(2\pi ab/m)}{\sin(2\pi b/m)}$.
- Since $1 \le b < m/2$, the denominator is positive, so the sign of the bth embedding is positive precisely when $\sin(2\pi ab/m)$ is positive, which occurs when the least positive residue of ab modulo m lies in $(0, m/2)$.

Circular Units and Signatures, III

We can organize the circular unit signature data using a matrix:

Definition

The (modified) circular unit signature matrix M is the $\varphi(m)/2 \times \varphi(m)/2$ matrix whose rows and columns are indexed by integers a, b with $1 \leq a, b < m/2$ relatively prime to m, and

$$m_{a,b} = \begin{cases} 1 & \text{when } ab \pmod{m} \in (0, m/2) \\ 0 & \text{when } ab \pmod{m} \in (m/2, m) \end{cases}$$

The rank of this matrix (over $\mathbb{F}_2$) is then equal to the rank of the group of circular unit signatures.

Circular Units and Signatures, IV

Example

For $m = 7$*, the signature matrix is* $\begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \end{bmatrix}$*, which has rank 3.*

Example

For $m = 11$*, the signature matrix is* $\begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{bmatrix}$*, of rank 5.*

Computations of Signature Ranks, I

Some circular unit signature ranks for various $K_m^+ = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$:

m	3	5	7	11	13	17	19	23	29	31	37	41	43
Rank	1	2	3	5	6	8	9	11	11	15	18	20	21

m	43	47	53	59	61	67	71	73	79	83	89	97
Rank	21	23	26	29	30	33	35	36	39	41	44	48

m	3^2	5^2	7^2	11^2	13^2	17^2	19^2	23^2	29^2	31^2
Rank	3	10	21	55	78	136	171	253	403	465

Computations of Signature Ranks, II

A few observations about the data on the previous slide:

- The maximum circular unit signature rank for K_m^+ is $\varphi(m)/2$. This value is the signature rank in almost all cases shown, and is very close in all cases.
- The rank is less than the maximum only for $m = 29$ and $m = 29^2$, each of which has a "signature rank deficiency" of 3.

Here are the next few values of m for which there is a rank deficiency:

m	29	113	163	197	239	277	311	337	349
Deficiency	3	3	2	3	3	4	10	6	4

(See any patterns?)

Lower Bounds on Unit Signature Ranks, I

Our first main result is that the (circular) unit signature rank goes to ∞ in p-power extensions:

Theorem 1 (D. Dummit, E.D., H. Kisilevsky)

Suppose p is an odd prime and $m = p^n$. Then the (circular) unit signature rank of K_m^+ is at least $\lfloor \log_2(p^n) \rfloor - 2$.

The idea of the proof is to isolate $\lfloor \log_2(p^n) \rfloor - 2$ rows of the unit signature matrix (namely, those indexed by powers of 2) that can be shown to be linearly independent. (Argument also works when $p = 2$, but it was already shown by Weber in 1899 that the circular unit signature rank is maximal for 2-power cyclotomic fields.)

Lower Bounds on Unit Signature Ranks, II

Proposition (D. Dummit, E.D., H. Kisilevsky)

Suppose F and F' are totally real Galois extensions of $\mathbb{Q}$ with $F \cap F' = \mathbb{Q}$. If $\{\alpha_1, \ldots, \alpha_r\}$ are elements of F with independent signatures, and $\{\beta_1, \ldots, \beta_s\}$ are elements of F' with independent signatures, then $\{\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s\}$ has at least $r + s - 1$ independent signatures.

The Proposition allows us to glue results together for different p:

Theorem 2 (D. Dummit, E.D., H. Kisilevsky)

If m is a positive integer, then the (circular) unit signature rank of K_m^+ is at least $\log_2(m) - 4\omega(m) + 1$, where $\omega(m)$ is the number of distinct prime factors of m. In particular, the signature rank tends to ∞ with m.

Signature Ranks in Towers, I

We can also analyze the unit signature rank as we move up certain towers of real cyclotomic fields:

Theorem 3 (D. Dummit, E.D., H. Kisilevsky)

Let $p_1, p_2, \ldots, p_s$ be distinct odd primes and m be a positive integer relatively prime to each of the p_i. If $\delta(m; n_1, n_2, \ldots, n_s)$ denotes the unit signature rank deficiency of the field $K_{mp_1^{n_1}p_2^{n_2}\cdots p_s^{n_s}}$, then

1. $\delta(m; n_1, n_2, \ldots, n_s) \leq \delta(m; n_1', n_2', \ldots, n_s')$ *if* $n_i \leq n_i'$ *for each* i
2. $\delta(m; n_1, n_2, \ldots, n_s)$ *is bounded above, independent of* $n_1, \ldots, n_s$, *and*
3. $\delta(m; n_1, n_2, \ldots, n_s)$ *is constant (depending only on* m*) if the* n_i *are all sufficiently large.*

Signature Ranks in Towers, II

Here are some of the ideas involved in the proof of Theorem 3:

- The first step is to convert the discussion of the unit rank deficiency to one about Hilbert class fields, using the fact that $2^{\delta(F)}$ is equal to the extension degree $|H_F^{\mathrm{st}} : H_F|$ of the strict Hilbert class field of F over the Hilbert class field of F.
- The fact that $\delta(m; n_1, n_2, \ldots, n_s) \leq \delta(m; n_1', n_2', \ldots, n_s')$ if $n_i \leq n_i'$ follows from the more general observation that if F and F' are totally real number fields with $F \subseteq F'$, then $\delta(F) \leq \delta(F')$.
- The other statements can then be obtained using a theorem of Friedman that the 2-primary part of the class number of $K^+_{mp_1^{n_1}p_2^{n_2}\cdots p_s^{n_s}}$ is bounded for all s-tuples $(n_1, \ldots, n_s)$ and is constant when all the n_i are sufficiently large.

How Large Can Rank Deficiencies Be?

Theorem 3 implies that rank deficiencies are bounded in certain "vertical" families. A natural question is whether rank deficiencies can be arbitrarily large in general.

Under the assumption (heuristically expected to be true) that there are infinitely many cyclic cubic fields having a totally positive system of fundamental units, we can show that the rank deficiency can be arbitrarily large:

Theorem 4 (D. Dummit, E.D., H. Kisilevsky)

If there exist infinitely many cyclic cubic fields having a totally positive system of fundamental units, then the unit signature rank deficiency of the real cyclotomic field K_m^+ can be arbitrarily large.

How Large Can Rank Deficiencies Be: Almost ∞

A sketch that unit signature rank deficiencies can be large:

- Suppose we have n linearly disjoint cyclic cubic fields each with a totally positive system of fundamental units (i.e., with rank deficiency 2): we claim the rank deficiency of the composite F of these fields is at least $2n$.
- If these cubic fields have fundamental units $\epsilon_1, \epsilon_2, \ldots, \epsilon_{2n}$, it is enough to show that these totally positive units are multiplicatively independent modulo squares in F.
- If there were some dependence in F, then by using the Galois action, it would yield a dependence in one of the subfields.
- Finally, to obtain a cyclotomic field with rank deficiency at least $2n$, simply choose one that contains F.

Open Questions

Here are a few things that are still unresolved:

- Is it possible to establish a tighter lower bound on the circular unit signature rank of K_m^+?
- Is there a nice characterization of the primes p for which the field K_p^+ has a circular unit rank deficiency? Are there infinitely many such primes, and if so, how common are they?
- Can the rank deficiency of K_p^+ for p prime be arbitrarily large?
- Some (modest) calculations for prime-power cyclotomic fields suggests that the rank deficiency of K_p is the same as the rank deficiency of K_{p^n} for $n \geq 2$. Can this be proven?

An Application of Rank Deficiency

Since there is an element in the kernel of the signature map for $p = 29$, the corresponding product of circular units is totally positive but not a square.

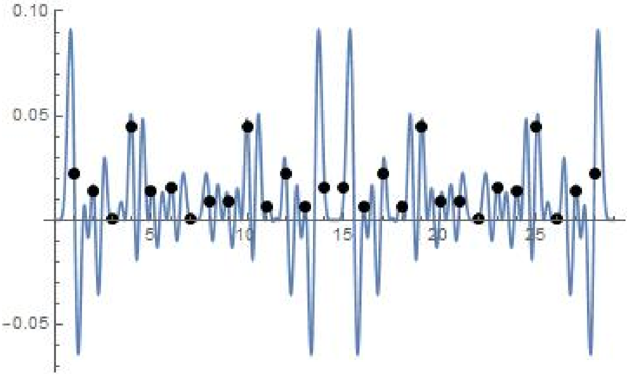
Writing this element explicitly, and discarding the denominators, yields the odd fact that the trigonometric polynomial

$$p(x) = \sin\left(\frac{4\pi x}{29}\right)\sin\left(\frac{8\pi x}{29}\right)\sin\left(\frac{10\pi x}{29}\right)\sin\left(\frac{12\pi x}{29}\right) \cdot \sin\left(\frac{16\pi x}{29}\right)\sin\left(\frac{18\pi x}{29}\right)\sin\left(\frac{20\pi x}{29}\right)\sin\left(\frac{28\pi x}{29}\right)$$

is nonnegative for each integer value of x but takes negative values as a function.

End

Here is a plot of this trigonometric polynomial:



Thank you for attending my talk!