MINIMISING VOLUMES IN NUMBER FIELDS

Anna Szumowicz

Jagiellonian University

Introduction

$\mathfrak{p}$-orderings

Bhargava introduced the notion of the generalized factorial function in the following way ([B]):

Definition 1. *Let A be a Dekind domain and $\mathfrak{p}$ a prime ideal in A. Denote by $v_{\mathfrak{p}}$ the additve $\mathfrak{p}$-adic valution in A. Let $s_0, s_1 \cdots$ be a sequence of elements in A. It is called a $\mathfrak{p}$-ordering if for every natural number n the element s_n is chosen so that the valuation $v_{\mathfrak{p}}(\prod_{i=0}^{n-1}(s_i - s_n))$ is the lowest possible. Define*

$$i_n(\mathfrak{p}) = v_{\mathfrak{p}}(\prod_{i=0}^{n-1}(s_i - s_n)).$$

It can be shown that the value of $i_n(\mathfrak{p})$ does not depend on the choice of a $\mathfrak{p}$-ordering. Let n be a natural number. The generalized factorial of n is the ideal

$$n!_A = \prod_{\mathfrak{p} \in Spec A} \mathfrak{p}^{i_n(\mathfrak{p})}.$$

For a number field K we shall write $n!_K := n!_{\mathcal{O}_K}$.

It is interesting to know for which fields we can find a simultaneous $\mathfrak{p}$-ordering in $\mathcal{O}_K$, for every prime ideal $\mathfrak{p}$. This is a particular case of Bhargavas question ([B1]). Melanie Woods in [W] showed that there are no simultaneous $\mathfrak{p}$-orderings in imaginary quadratic number fields.

Integer valued polynomials and n-universal sets

Simultaneous $\mathfrak{p}$-orderings are connected with the notion of integer valued polynomials. Let A be an integral domain and K be its field of fraction.

Definition 2. *Let f be a polynomial with coefficients in K. We call f integer valued if $f(A) \subseteq A$.*

Sometimes there is no need to check whether $f(a) \in A$ for every $a \in A$ to know if f is integer valued. For example if $f \in \mathbb{Z}[x]$ then it is enough to check that $f(n) \in \mathbb{Z}$ for every natural number n.

Definition 3. *We call a subset $S \subseteq A$ n-universal if for every polynomial $f \in K[X]$ of degree at most n the following equivalence holds: $f(S) \subseteq A$ if and only if $f(A) \subseteq A$.*

Example All n-universal subsets of $\mathbb{Z}$ with $n+1$ elements are of the form $\{a, \cdots, a+n\}$ for some integer a.

If A is an integral domain which is not a field then any n-universal set has at least $n+1$ elements. Hence, the n-universal sets with $n+1$ elements are of the particular interest. We shall call them n-optimal. It is well known that if $s_0, s_1, s_2, \ldots \in \mathcal{O}_K$ is a simultaneous $\mathfrak{p}$-ordering for all prime ideals $\mathfrak{p}$, then the initial fragments $\{s_0, s_1, \ldots, s_s\}$ is an n-universal set. In particular if there are no n-optimal sets elements for some natural number n then a simultaneous $\mathfrak{p}$-ordering cannot exist.

n-universal sets in Gaussian integers

Petrov and Volkov in [PV] studied the n-universal sets in Gaussian integers. They proved the following result:

Theorem 1. *There are no n-optimal sets in $\mathbb{Z}[i]$ for n large enough.*

Petrov and Volkov were also investigating the minimal cardinality of an n-universal sets in Gaussian integers and gave a family of examples of n-universal sets with $\frac{\pi}{2}n + o(n)$ elements. They conjectured that their examples realize the asymptotic lower bound on the size of an n-universal set in $\mathbb{Z}[i]$:

Conjecture 1. *The size of the minimal n-universal sets in $\mathbb{Z}[i]$ grows as $\frac{\pi}{2}n + o(n)$.*

In [BFS] we give a strong counterexample to their question by proving that in any Dedekind domain there exists for every n an n-universal set with $n+2$ elements.

n-universal sets in number fields

n-optimal sets

In the joint work with J.Byszewski and M. Fraczyk ([BFS]) we generalized Theorem 1 to all imaginary quadratic number fields:

Theorem 2. *Let K be an imaginary quadratic number field. For large enough n there are no n-optimal sets in the ring of integers of K.*

Sketch of the proof:
Let $K = \mathbb{Q}(\sqrt{-d})$ for some positive square-free integer number d. Denote by $\mathcal{O}_K$ the ring of integers of K. We divide the proof into two cases. If $d \equiv 1, 2 \pmod 4$ then $\mathcal{O}_K = \mathbb{Z}[\sqrt{-d}]$ and one only needs to adapt the methods from [PV]. Essentially the reason why the similar argument works is the fact that we can pick a $\mathbb{Z}$ basis of $\mathcal{O}_K$ which is orthogonal (in usual sense). In the case $d \equiv 3 \pmod 4$ some modifications are required as the geometry of $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{-d}}{2}]$ (seen as a lattice in $\mathbb{C}$) is different. In the proof we used two main tools: the notion of a volume and the almost uniform distribution. Both of them were introduced by Petrov and Volkov, the only difference is that we look at the volume as an ideal rather than a real number.

Definition 4. *Let A be an integral domain, S be a finite subset of A and I an ideal in A. The* **volume** *of a set S is the ideal:$Vol(S) = \prod_{\substack{s,s' \in S \\ s \neq s'}}(s - s')$*

The set S is almost uniformly distributed modulo I if for every $a, b \in A$ we have

$$|\{s \in S | a \equiv s \pmod I\}| - |\{s \in S | b \equiv s \pmod I\}| \leqslant 1$$

The following two propositions are crucial for the proof. They are modified/extended versions of results used in [PV]:

Proposition 1. *Let K be a number field and S a subset of $\mathcal{O}_K$. The set S is n-universal if and only if for every non zero prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$ there exists S_1 a subset of S with $n+1$ elements which is almost uniformly distributed modulo powers of $\mathfrak{p}$.*

Proposition 2. *Let S be a subset $\mathcal{O}_K$ with $n+1$ elements. The following conditions are equivalent:*

- *S is n-optimal*
- *$Vol(S) = (\prod_{i=1}^{n} i!_K)^2$*
- *for every $S_1 \subseteq \mathcal{O}_K$ with $n+1$ elements, $Vol(S)$ divides $Vol(S_1)$*

We return to the sketch of the proof of Theorem 2. Let us assume the contrary, that for arbitrary large n there exists an n-optimal set S. We identify $\mathcal{O}_K$ with its image via the embedding: $\mathcal{O}_K \hookrightarrow \mathbb{C}$. By Proposition 2 the set S has the minimal volume. We use that information and Proposition 1 together with a geometric arguments to show that it has to be contained in some polygon P of area that we can control very well. We prove that S is enclosed by a rectangle in the first case when $d \equiv 1, 2 \pmod 4$ and by a hexagon in the second case. The estimate on the area of P implies that it contains $n + o(n)$ points from the lattice $\mathcal{O}_K$. Next, we show that for certain primes p we can find $\Omega(n)$ triples $\{x, y, z\}$ in P which give the same residue modulo p. Using Proposition 1 we show that every such triple intersects with S in at most two points. Hence, we demonstrate that there exists a subset of $\mathcal{O}_K$ which is contained in the polygon, is disjoint with S and has a cardinality $\Omega(n)$. This yields a contradiction since P had $n + o(n)$ points and S is of cardinality $n+1$.

Minimal cardinality of n-universal sets

Using the generalized version of Proposition 1 coupled with elementary arguments we obtained the following result:

Theorem 3. *Let A be a Dedekind domain. Then for every n there exists an n-universal set with $n+2$ elements in A. Moreover, there exists an increasing sequence $U_0 \subseteq U_1 \subseteq \cdots$ of n-universal sets U_n with $n+2$ elements in A.*

n-optimal sets in other number fields

The problem of existence of n-optimal sets in general number fields seems to be much harder than in the case of imaginary quadratic number fields. In the proof of Theorem 2 we relied on fact that since the n-optimal set has the minimal volume we can deduce a lot of information about its geometry. Unfortunately the method used requires the convexity of the norm $N_{K/\mathbb{Q}}$ which holds only in the case $K = \mathbb{Q}$ or $K = \mathbb{Q}(\sqrt{-d})$. For general number fields we estimate the growth of volume of hypothetical n-optimal sets. During our attempts to prove the Theorem 2 in the general case we discovered a link with Euler-Kronecker constant.

Euler-Kronecker constants

By Propostion 2 studying the norm of the volume of n-optimal set is strongly tied with the generalized factorial function. The genarlized factorials provide a link with Euler-Kronecker constants. Denote by K a number field. Let $\zeta_K(s)$ be the Dedekind zeta function of K. Let $\zeta_K(s) = \frac{c_{-1}}{s-1} + c_0 + c_1(s-1) + \cdots$ be the Laurent expansion of Dedekind zeta function at $s = 1$.

Definition 5. *([I]) The* **Euleur − Kronecker constant** *γ_K is defined as the quotient $\frac{c_0}{c_{-1}}$ or equivalently as the constant term of a Laurent expansion of the function γ_K' / γ_K at $s = 1$.*

If $K = \mathbb{Q}$ then $\gamma_{\mathbb{Q}}$ is the Euler-Mascheroni constant given by the formula

$$\gamma_{\mathbb{Q}} = \lim_{n \to \infty}(\sum_{i=1}^{n} \frac{1}{i} - \log n)$$

The reason why Euler-Kornecker constant appears in our considerations is explained by the following theorem due to M. Lamoureux

Theorem 4. *([L])*

$$\log n!_K = n \log n - n(1 + \gamma_K - \gamma_{\mathbb{Q}}) + o(n)$$

Using Proposition 2 we obtain the following corollary:

Corollary 1. *Denote by $N(I)$ the norm of an ideal I in $\mathcal{O}_K$. If S is an n-optimal subset of $\mathcal{O}_K$ then*

$$\log N(Vol(S)) = n^2 \log n - \frac{n^2}{2} - n^2(1 + \gamma_K - \gamma_{\mathbb{Q}}) + o(n^2).$$

Moreover for every subset $S_1 \subseteq \mathcal{O}_K$ with $n+1$ elements we have

$$\log N(Vol(S_1)) \geqslant n^2 \log n - \frac{n^2}{2} - n^2(1 + \gamma_K - \gamma_{\mathbb{Q}}) + o(n^2).$$

One could try to generalize Theorem 2 for any number field by comparing above estimates with ones obtained by a geometric arguments. However, it seems to be problematic in the fields with infinite group of units. Estimates from the corollary can be used to obtain the following inequality:

Theorem 5. *Let U be an open bounded subset of $\mathbb{R}^d$. Let $x = (x_1, \cdots x_d) \in \mathbb{R}^d$ and denote $||x|| = \prod_{i=1}^{d} |x_i|$ and let m be the Lebesgue measure. We have*

$$\int_U \int_U \log ||x - y|| dx dy \geqslant m(U)^2 (c_d + \log m(U)),$$

where c_d is a constant depending only on d.

Corollary 2. *Let K be a totally real number field and Δ_K be the discriminant of K. We have*

$$\gamma_K \geqslant -\frac{1}{2} \log |\Delta_K| + \frac{3}{2}d - \frac{3}{2} + \gamma_{\mathbb{Q}}$$

The estimate which we obtained for γ_K, has the same main term $-\frac{1}{2} \log |\Delta_K|$ but is slightly weaker than the one given by Ihara in [I].

Bibliography:

[B] M.Bhargava, P-orderings and polynomial finctions on arbitrary subsets of Dedekind rings, J.Reine Angew. Math. 490 (1997), pp. 101-127

[B1] M.Bhargava, The factorial function and generalizations, Amer. Math. Monthly 107 (2000), pp. 783-799

[BFS] J.Byszewski, M.Fraczyk, A.Szumowicz, Simultaneous p-orderings and minimising volumes in number fields, preprint, availaible at `http://arxiv.org/abs/1506.02696`

[I] Y.Ihara, On the Euler-Kronecker constants of global fields and primes with small norms, Algebraic geometry and number thoery 253 (2006), pp.407-451

[L] M. Lamoureux, Stirling's Formula in number Fields, Doctoral Dissertations, Paper 412 (2014),`http://digitalcommons.uconn.edu/dissertations/412`

[PV] V.V.Volkov, F.V. Petrov, On the interpolation of integer-valued polynomials, Journal of Number Theory 133 (2013), pp.4224-4232

[W] M.Woods, P-orderings: a metric viewpoint and the non-existence of simultaneous orderings, Journal of Number Theory, 99(2003), pp.36-56

LaTeX template: `http://agregationchimie.free.fr/poster.php#gocontent`

PEPS-égalité "Correspondances de Langlands" - Projet INTEGER (GA no 266638).