A lower regulator bound for number fields

Claus Fieker and Michael E. Pohst

Abstract

1 Introduction

In [4] a regulator bound for algebraic number fields F was derived which makes use of specific data of F. That bound is not completely explicit and difficult to determine for fields of higher degree. Since lower regulator bounds are important for many computational tasks in algebraic number fields we develop an explicit lower bound in this paper which is best possible in a way specified below.

2 An extremal value problem

Let F be an algebraic number field of degree n with ring of integers o_F and conjugates $F^{(1)} = F, ..., F^{(n)}$. As usual, we assume that the first r_1 conjugates are real, that the remaining $2r_2$ conjugates are complex so that the first $r_1 + r_2$ conjugates correspond to the different archimedian valuations of F. For $\alpha \in F$ we write

$$T_2(\alpha) \ := \ \sum_{j=1}^{n} |\alpha^{(j)}|^2 \ \ .$$

Let ε be a unit of o_F satisfying

$$T_2(\varepsilon) \ \geq \ K \ \text{ and } \ T_2(\varepsilon^{-1}) \ \geq \ K \tag{1}$$

for some constant $K > n$. Then ε is not a root of unity. It is well known [6, 5] that a lower regulator bound for F can be deduced from a lower bound for

$$L(\varepsilon) \ := \ \sum_{j=1}^{n} \log^2 |\varepsilon^{(j)}| \ \ .$$

To solve that task we put $x_j := \log |\varepsilon^{(j)}|$ and $\mathbf{x} = (x_1, ..., x_n)$. Because of the side conditions

$$|N(\varepsilon)| \ = \ 1 \, , \ \ T_2(\varepsilon) \ \geq \ K \, , \ \ T_2(\varepsilon^{-1}) \ \geq \ K$$

we want to solve the minimization problem

$$\min f(\mathbf{x}) \ \text{ for } \ f(\mathbf{x}) := \mathbf{x}\mathbf{x}^{tr} \tag{2}$$

on the closed subset $S_K \subset \mathbb{R}^n$ consisting of those vectors $\mathbf{x}$ whose coordinates satisfy

1. $\sum_{j=1}^n x_j \ = \ 0$,
2. $\sum_{j=1}^n e^{2x_j} \ \geq \ K$,
3. $\sum_{j=1}^n e^{-2x_j} \ \geq \ K$.

We note that $K > n$ yields $\mathbf{0} \notin S_K$. Also, the conditions imply that each vector of S_K has positive and negative coordinates.

The first lemma in [4] shows that this minimization problem has a global minimum, say in $\mathbf{z} \in S_K$, and that $\mathbf{z}$ has at most 3 different coordinates. We denote these coordinates by a, b, c. Because of $f(\mathbf{z}) = f(-\mathbf{z})$ we can assume without loss of generality that $a > b > c$, $a > 0$, $c < 0$ and the multiplicitiy i of a is $\geq n/2$.

For $abc \neq 0$ the value $f(\mathbf{z})$ is larger than or equal to the minimum M_K of $f(\mathbf{x})$ on the set T_K consisting of those $\mathbf{x} = (x_1, ..., x_n) \in \mathbb{R}^n$ satisfying

1. $\sum_{j=1}^n x_j \ = \ 0$,
2. $\sum_{j=1}^n e^{2x_j} \ \geq \ K$,
3. $\prod_{j=1}^n x_j \ \neq \ 0$.

In Theorem (6.17) of chapter 5 of [3] it is shown that

$$M_K \ \geq \ \frac{n}{4}\left(\log\left(\frac{K}{n} + \left(\frac{K^2}{n^2} - 1\right)^{1/2}\right)\right)^2 \quad =: M_{K,0} \tag{3}$$

under the additional restriction that the number of positive coordinates is at least $n/2$.

For ease of notation, we recall that for $\cosh : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 1}$ we have:

$$\text{arcosh}(x) = \log(x + \sqrt{x^2 - 1})$$

Thus we can write

$$M_{K,0} = \frac{n}{4}\,\text{arcosh}^2(\frac{K}{n}) \ .$$

It remains to discuss the case $b = 0$. We assume that the frequencies of the coordinates a, b, c in $\mathbf{z}$ are i, j, k, respectively. Because of $f(\mathbf{x}) = f(-\mathbf{x})$ we can assume that $i \geq k$. We therefore need to minimize $f(\mathbf{x})$ on the set $T_{K,j}$ whose elements satisfy

1. $x_1 = ... = x_i = a > 0 = x_{i+1} = ... = x_{i+j} > c = x_{n-k+1} = ... = x_n$,

2. $ia + kc \;=\; 0$,

3. $ie^{2a} + ke^{2b} \;\geq\; K - j$,

4. $ie^{-2a} + ke^{-2b} \;\geq\; K - j$.

Again, that minimum becomes at most smaller if we omit the last side condition. Then we obtain an analogue of the minimization problem solved in the proof of Theorem (6.17) in chapter 5 of [3]. A lower bound for the minimum is obtained via $i = k = (n-j)/2$:

$$M_{K,j} \;:=\; \frac{n-j}{4}\operatorname{arcosh}^2(\frac{K-j}{n-j}) \tag{4}$$

We note that we necessarily have $0 < j \leq n-2$. Hence, it suffices to show that $M_{K,j}$ is decreasing in j in order to obtain a global lower bound $M_{K,n-2}$ for our original minimization problem.

Lemma 1 *$M_{K,j}$ is a decreasing function in j for $j \in [0, n-2]$ if we stipulate $K/n \geq 1 + \sqrt{2}$.*

Proof We recall $\operatorname{arcosh}(x)' = \frac{1}{\sqrt{x^2-1}}$ and easily calculate

$$\frac{\partial 4M_{K,j}}{\partial j} \;=\; \operatorname{arcosh}(\frac{K-j}{n-j}) \times \left(\frac{2(K-n)}{\sqrt{(K-j)^2-(n-j)^2}} \;-\; \operatorname{arcosh}(\frac{K-j}{n-j})\right) \;.$$

We want to show that the second factor on the right-hand side is negative. We use the following formulae and estimates:

$$\begin{aligned}
\operatorname{arcosh}(\frac{K-j}{n-j}) \;&=\; \log\left(\frac{K-j}{n-j} + \left(\left(\frac{K-j}{n-j}\right)^2 - 1\right)^{1/2}\right) \\
&=\; \log\frac{K-j}{n-j} \;+\; \log\left(1 + \sqrt{1 - \left(\frac{n-j}{K-j}\right)^2}\right) \;, \\
\log\left(1 + \sqrt{1 - \left(\frac{n-j}{K-j}\right)^2}\right) \;&\geq\; \log\left(1 + \sqrt{1 - \left(\frac{n}{K}\right)^2}\right) \;, \\
\sqrt{1 - \left(\frac{n}{K}\right)^2} \;&>\; 1 - \frac{n^2}{2K^2} - \frac{n^4}{4K^4} \;, \\
\log\left(1 + \sqrt{1 - \left(\frac{n}{K}\right)^2}\right) \;&>\; \frac{1}{2} - \frac{n^4}{4K^4} \;\text{ for }\; 2K \geq 3n \;.
\end{aligned}$$

The negative of the second factor on the right-hand side of the partial derivative of $M_{K,j}$ is therefore larger than

$$X(j) \;:=\; \log\frac{K-j}{n-j} \;+\; \frac{1}{2} - \frac{n^4}{4K^4} - 2\frac{K-n}{\sqrt{K^2 - 2(K-n)j - n^2}}$$

The function $X(j)$ is increasing with j since we compute

$$X'(j) = (K-n)\left(\frac{1}{(K-j)(n-j)} - \frac{2(K-n)}{(K^2-2(K-n)j-n^2)^{3/2}}\right)$$

which is positive if we require $K/n \geq 1+\sqrt{2}$ because of

$$K-n \leq \sqrt{K^2-2(K-n)j-n^2}\ .$$

Eventually, we need to show $X(0) \geq 0$. We obtain

$$X(0) > \log\frac{K}{n} + 0.493 - 2\sqrt{\frac{1-n/K}{1+n/K}}\ .$$

That lower bound for $X(0)$ is easily seen to be positive for $K/n \geq 1+\sqrt{2}$. □

Putting things together we proved the following theorem.

Theorem 1 *Let ε be a unit of F satisfying $T_2(\varepsilon) \geq K$ and $T_2(\varepsilon^{-1}) \geq K$ for some constant K with $K \geq 5n/2$. If at most j conjugates of ε are of absolute value 1 then we have*

$$L(\varepsilon) \ \geq\ \frac{n-j}{4}\operatorname{arcosh}^2(\frac{K-j}{n-j})\ .$$

Remark The number j of conjugates of a non-torsion unit ε which can be of absolute value 1 depends on the number r_2 of complex embeddings of F. Clearly, we have $j = 0$ for $r_2 = 0$ and $j \leq \min\{2r_2,\, n-2\}$.

For any totally real field E of degree n we can easily find a quadratic extension F/E of signature $(2, n-1)$ containing a unit ϵ with all $n-2$ complex embeddings of absolute value 1: Let a be an integral element in E such that exacly on c onjugate is > 1 and all the others have the absolute value bounded by 1. Such elements always exist by the Minkowski lattice theorem. Then $F = E(b)$ for $b^2 + ab + 1 = 0$ is such an extension, and b is a unit with the required properties.

Remark Salem numbers are also examples of units with at least one conjugate of absolute value 1. One would expect that small Salem numbers occur in fields with small regulators.

3 Lower Regulator Bounds

Let R be an arbitrary order of F. By Dirichlet's Theorem we know that the unit group U_R of R, is the direct product of its torsion subgroup TU_R, say $TU_R = \langle\zeta\rangle$ of order w, and $r = r_1 + r_2 - 1$ infinite cyclic groups. We denote the generators of those – so-called fundamental units – by $E_1, ..., E_r$. The regulator Reg_R is defined as

$$\mathrm{Reg}_R\ = |\det(c_j \log|E_i^{(j)}|)\,| \quad \text{with}\ \ c_j = \begin{cases} 1 & \text{for } j \leq r_1 \\ 2 & \text{otherwise} \end{cases}\ ,\ 1 \leq i,j \leq r\ .$$

Lower bounds for Reg_R can be obtained with the results of the previous section. Let ε be a unit of R. If we express ε by the fundamental units of $U(R)$:

$$\varepsilon = \zeta^{x_0} E_1^{x_1} \cdots E_r^{x_r} \ (x_i \in \mathbb{Z})$$

then $L(\varepsilon)$ becomes a positive definite quadratic form in $x_1, \ldots, x_r$. It is not very difficult to compute the determinant $\det(L)$ of that quadratic form (see [3, Chap. 5, (6.9)], for example):

$$\det(L) = 2^{-r_2}\, n\, \mathrm{Reg}_R^2 \ .$$

If $M_1, \ldots, M_r$ denote the successive minima of the quadratic form L then Minkowski's theorem yields

$$M_1 \cdots M_r \le \gamma_r^r \det(L).$$

The constants γ_r^r (Hermite's constants) are only known up to $r = 8$. For larger values of r we use the estimate

$$\gamma_r^r \ \le \ \frac{2}{\pi}\Gamma\left(1 + \frac{n+2}{2}\right)^2 \ .$$

Hence, lower bounds for $M_1, \ldots, M_r$ will provide a lower bound for Reg_R. Determining good lower bounds for $M_1, \ldots, M_r$ is of course the crucial part of this method. We want to use as many properties of R as we can, not only the degree n of F and the discriminant of R. We choose a constant $K \ge (1+\sqrt{2})n$ and compute the set

$$S_K := \{\alpha \in R \mid T_2(\alpha) < K\} \cup \{\alpha \in K \mid \alpha^{-1} \in R, T_2(\alpha^{-1}) < K\} \ .$$

Obviously, $TU(R)$ is contained in in S_K. Let us assume that S_K also contains k independent units $(0 \le k \le r)$. We set, according to Theorem 1:

$$K^* := \frac{n-j}{4}\,\mathrm{arcosh}^2(\frac{K-j}{n-j})$$

then

$$M_i^* \ = \begin{cases} \min\{K^*\} \cup \{C \mid \exists\, \varepsilon_1, \ldots, \varepsilon_i \in U_R \cap S_K \text{ indep. with } L(\varepsilon_i) \le C\} \\ \qquad\quad \text{for } 1 \le i \le k \\ \ \ K^* \quad \text{for } k+1 \le i \le r \end{cases}$$

and finally

$$\tilde{M}_i := \frac{n-j}{4}\,\mathrm{arcosh}^2(\frac{M_i^* - j}{n-j}) \ .$$

The integer j is to be chosen in the interval $[0, n-2]$ as small as possible (see the remark following Theorem 1). As a consequence of Theorem 1 we then obtain

Proposition 1 *A unit $\varepsilon \in U_R$ satisfying $T_2(\varepsilon) \geq M_i^*$ and $T_2(\varepsilon^{-1}) \geq M_i^*$ satisfies $L(\varepsilon) \geq \tilde{M}_i$.*

From this the following lower regulator bound is immediate:

Corollary 1 *The regulator* Reg_R *of an order R of F satisfies*

$$\mathrm{Reg}_R \geq (\tilde{M}_1 \cdots \tilde{M}_r 2^{r_2} n^{-1} \gamma_r^{-r})^{1/2} .$$

4 Practical considerations

In order to use the bound as provided by Corollay 1, we need to choose a suitable constant $K \geq (1+\sqrt{2})n$ depending on our field. In this discussion we assume that a maximally independent set of units $\varepsilon_1, \ldots, \varepsilon_r$ is known and we want to compute the full unit group or show that our system is already maximal. This entails:

1. Given a constant K, compute the set S_K
2. Compute M_i^* and $\tilde{M}_i$
3. Use Corollay 1 to compute a lower regulator bound R_l and utilize the given set of units to compute an upper bound R_u.
4. For all primes p such that $p \leq R_u/R_l$ show that the given system of units is p-maximal or find a new unit.

Using the Fincke-Pohst algorithm [3, Chap. 3, (3.15)], we first compute the set

$$T_K := \{x \in R \mid T_2(x) \leq K\}$$

and then

$$S_K = T_K \cup (\{x^{-1} : x \in T_K\} \cap R).$$

Since the computation of a single element of T_K takes $O(n^2)$ operations, we get a (algebraic) complexity of $O(n^2 \# T_K)$. Using for example [7, (VI, §2), Theorem 2] we immediately see that $\# T_K = O(K^n)$. All other operations (computation of $(.)^{-1}$, the comparisons involved in the set operations) involved in step 1 are also bounded by $O(n^2)$ if floating point operations of sufficiently high (but fixed) precision are used.

The next step requires the computation of $L(.)$ and (in)dependence test on small sets of units. Since we assume that a maximally independent set of units is already known, the tests can easily be reduced to (rational) linear algebra and are individually bounded by $O(n^3)$.

Step 3 takes only a constant number of operations independently of K, thus it remains to discuss step 4. Following the method outlined in [3, Chap. 5 (7.12)], to proof p-maximality one needs to do some computations for each independent unit of our given system, thus $O(r) = O(n)$ operations per prime number where the constants depend on the field. Each operation itself takes ??? operations, so that the total complexity is bounded by $O(nR/log(R)$ for $R := R_u/R_l$. Using the defintion of arcosh, we immediately obtain $K^* = O(\log^2 K)$ and thus $R_l = O(\log^{2n} K)$ which gives at most a complexity of $O(\log^{-2n} K)$. Of course, if our set of independent units is already contained in T_K then R_l will be independent of K, but in this case we already know a fundamental system of units.

Combining the estimates, it is clear that K should be chosen as small as possible as the complexity for the computation of S_K dominates the running time. On the other hand, in an actual implementation one needs to analyse the overheads involved and determine reasonable choices for K experimentally, depending on n, the given basis for R and the given system of independent units.

In the next section we will give some examples illustrating the influence of the choice for K on the total runtime.

5 Numerical Examples

The computations of the examples is presently carried out on an Intel Pentium III with 600 MHz and 512 MB RAM under Linux 2.2.13-SMP.

Let us start with an counterexample to the bound in [3]: Using $F := \mathbb{Q}(\alpha)$ with $\alpha^4 - \alpha^3 - 6\alpha^2 - 2\alpha + 4$ we get a contradicion for $M^* := 130$. The set S_K contains two units $\epsilon_1 := 2\alpha^3 - 5\alpha^2 - 5\alpha + 5$ and $\epsilon_2 := \epsilon_1^{-1}$ of length $T_2(\epsilon_{1,2}) = 128.06... < 130$ and logarithmic length 17.29.... Unfortunately, the unit $\epsilon_3 := \alpha^3 - 7\alpha - 7$ has length $T_2(\epsilon_3) = 130.06 > 130$ with a smaller size in the logarithm space: 11.77.... This leads to a regulator estimate of 10.63 which is larger than the regulator of 10.09. The unit ϵ_3 has two complex embeddings of absolute value 1.

Next, we work in the field $F := \mathbb{Q}(\alpha)$ with $\alpha^6 - 114\alpha^4 + 48\alpha^3 + 3249\alpha^2 - 2736\alpha - 19456 = 0$. This is a totally real field with a large regulator, $R = 580,843.22...$ so that it is unlikely to have a complete system of independent units in S_K for any reasonable choice of K. The discriminant of F is $3^4 19^2 313^3 = 896654708577$ of class number 1. In 1 we demonstrate the effect of K on the regulator bound obtained. In this example, we let K run from 9 to 6000, giving regulator estimates between 0.3 and $10,100$. Due to the size of the field, the regulator estimate follows strictly the arcosh^2 curve, thus large increments in K result in only minor changes in the quality of the output. The second figure 2 displays for the same values of K, the time spend in steps 1 to 3. The total time spend in step 4 is negligible for any $K > 100$. In our implementation ([2, 1]) we use as K the length of the longest basis vector of a LLL reduced basis for R.

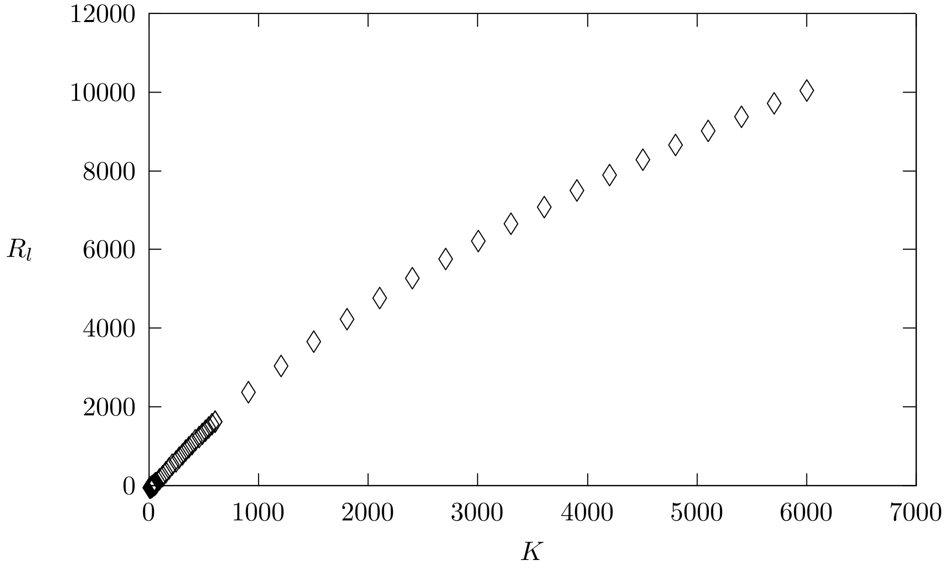

Figure 1: lower bound vs. K

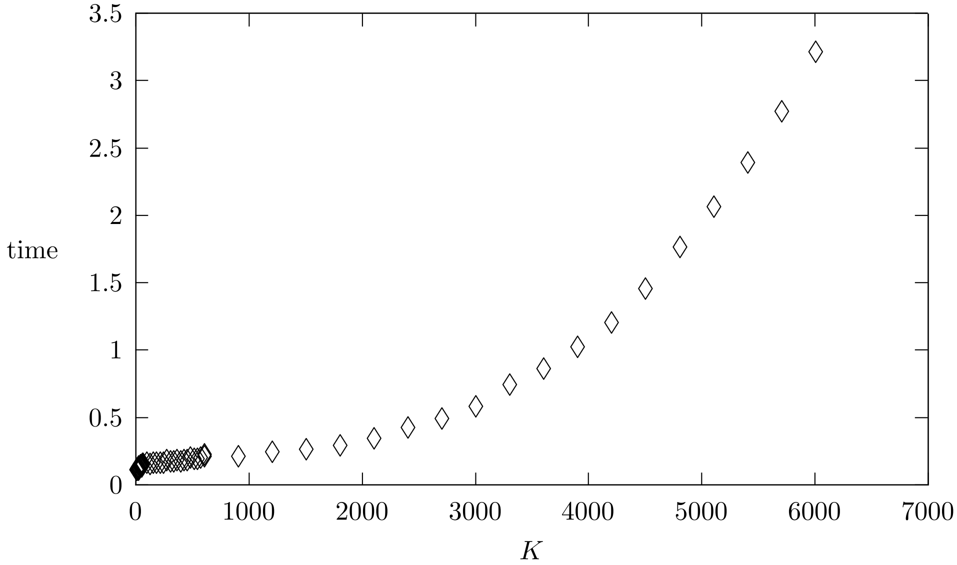

Figure 2: time vs. K

References

[1] M. Daberkow, C. Fieker, J. Klüners, M. Pohst, K. Roegner, M. Schörnig, and K. Wildanger, *KANT V4*, J. Symb. Comp. **24** (1997), 267–283.

[2] *Magma*

[3] M. Pohst and H. Zassenhaus, *Algorithmic Algebraic Number Theory*, Cambridge University Press 1997.

[4] M. Pohst and K. Wildanger *Tables of unit groups and class groups of quintic fields and a regulator bound*, Math. Comp. **67** (1998), 361–367.

[5] M. Pohst *Eine Regulatorabschätzung*, Abh. Math. Semin. Univ. Hamb., **47** (1978), 95–106.

[6] R. Remak, *Über die Abschätzung des absoluten Betrages des Regulators eines algebraischen Zahlkörpers nach unten*, J. Reine Angew. Math., **167** (1932), 360–378.

[7] S. Lang *Algebraic Number Theory*, Springer, 1993.