Linear Algebra and its Applications 433 (2010) 1659–1665

Contents lists available at ScienceDirect

Linear Algebra and its Applications

journal homepage: www.elsevier.com/locate/laa

Some inequalities related to the Seysen measure of a lattice

Gérard Maze

Mathematics Institute, University of Zürich, Winterthurerstr. 190, CH-8057 Zürich, Switzerland

ARTICLE INFO

Article history:
Received 26 November 2009
Accepted 9 June 2010
Available online 4 July 2010

Submitted by H. Schneider

AMS classification:
Primary: 11H06
Secondary: 15A42, 11-04

Keywords:
Lattice
Orthogonality defect
Seysen measure
HGA inequality

ABSTRACT

Given a lattice L, a basis B of L together with its dual B^*, the orthogonality measure $S(B) = \sum_i \|b_i\|^2 \|b_i^*\|^2$ of B was introduced by Seysen (1993) [9]. This measure (the Seysen measure in the sequel, also known as the *Seysen metric* [11]) is at the heart of the Seysen lattice reduction algorithm and is linked with different geometrical properties of the basis [6,7,10,11]. In this paper, we derive different expressions for this measure as well as new inequalities related to the Frobenius norm and the condition number of a matrix.

1. Introduction, notations and previous results

An n-dimensional (real) lattice L is defined as a subset of $\mathbb{R}^m$, $n \leqslant m$, generated by $B = [b_1|\cdots|b_n]^t$, where the b_i are n linearly independent vectors over $\mathbb{R}$ in $\mathbb{R}^m$, as

$$L = \left\{ \sum_{i=1}^{n} a_i b_i | a_i \in \mathbb{Z} \right\}.$$

In this paper, the rows of the matrix B span the lattice. Any other matrix $B' = UB$, where $U \in GL_n(\mathbb{Z})$, generates the same lattice. The volume Vol L of L is the well defined real number $(\det BB^t)^{1/2}$. The dual lattice of L is defined by the basis $B^* = (B^+)^t$, where B^+ is the Moore–Penrose inverse, or pseudo-inverse, of B. If $B^* = [b_1^*|\cdots|b_n^*]^t$, then since $BB^+ = I_n$, we have $\langle b_i, b_j^* \rangle = \delta_{i,j}$. Lattice reduction theory deals with the problem of identifying and computing bases of a given lattice whose vectors are *short*

E-mail address: gmaze@math.uzh.ch

0024-3795/$ - see front matter © 2010 Elsevier Inc. All rights reserved.
doi:10.1016/j.laa.2010.06.017

and *almost orthogonal*. There are several concepts of reduced bases, such as the concepts of Minkovsky reduced, LLL reduced [5] and Korkin–Zolotarev reduced basis [3]. In 1990, Hastad and Lagarias [1] proved that in all lattices of full rank (i.e., when $n = m$), there exists a basis B such that both B and B^* consist in relatively short vector, i.e., $\max_i \|b_i\| \cdot \|b_i^*\| \leqslant \exp(O(n^{1/3}))$. In 1993, Seysen [9] improved this upper bound to $\exp(O(\ln^2(n)))$ and suggested to use the expression $S(B) := \sum_i \|b_i\|^2 \|b_i^*\|^2$. This definition also allowed him to define a new concept of reduction: a basis B of L is Seysen reduced if $S(B)$ is minimal among all bases of L (see also [4] for a study of this reduction method). A relation between the orthogonality defect [2,11]

$$\mathrm{od}(B) := 1 - \frac{\det BB^t}{\prod_{i=1}^n \|b_i\|^2} \in [0, 1]$$

and the Seysen measure $S(B)$ is given in [11] where the following bounds can be found:

$$n \leqslant S(B) \leqslant \frac{n}{1 - \mathrm{od}(B)}, \tag{1.1}$$

$$0 \leqslant \mathrm{od}(B) \leqslant 1 - \frac{1}{(S(B) - n + 1)^{n-1}}. \tag{1.2}$$

Clearly, the smaller the Seysen measure is, the closer to orthogonal the basis is, showing that the Seysen measure describes the quality of the angle behavior of the vectors in a basis. The length of the different vectors are nevertheless not part of the direct information given by the measure, but inequality (1.2) gives

$$\prod_{i=1}^n \|b_i\| \leqslant (S(B) - n + 1)^{\frac{n-1}{2}} \cdot \mathrm{Vol}\, L,$$

which in turn provides the inequality

$$\min_i \|b_i\| \leqslant (S(B) - n + 1)^{(n-1)/2n} (\mathrm{Vol}\, L)^{1/n}. \tag{1.3}$$

Note that such a type of inequality appears in the context of lattice reduction as

$\min_i \|b_i\| \leqslant \sqrt{n}(\mathrm{Vol}\, L)^{1/n}$	for Korkin Zolotarev and Minkovsky reduced bases,
$\min_i \|b_i\| \leqslant (4/3)^{(n-1)/4}(\mathrm{Vol}\, L)^{1/n}$	for LLL reducedbases.

In this paper, we start by revisiting Seysen's bound $\exp(O(\ln(n)^2))$ by computing the hidden constant in Landau's notation. Then we present new expressions for the Seysen measure, connecting the measure with the condition number and the Frobenius norm of a matrix and allowing us to improve some of the existing bounds. We will from now on suppose that $m = n$, since equality (3.6) below shows that the Seysen measure is invariant under isometric embeddings.

2. Explicit constant in Seysen's bound

We show in this section that the hidden constant in Seysen's bound $\exp(O(\ln(n)^2))$ can be upper bounded by $1 + \frac{2}{\ln 2}$. The proof is not new, but revisits some details in the original proof of Seysen [9, Theorem 7] by using explicit bounds given in [5, Proposition 4.2]. Let us define the two main ingredients of the proof. First, if $N(n, \mathbb{R})$ and $N(n, \mathbb{Z})$ are the group of lower triangular unipotent $n \times n$ matrices over $\mathbb{R}$ and $\mathbb{Z}$, respectively (i.e. matrices with 1 in the diagonal), then following [1,9], and if $\|X\|_\infty = \max_{i,j} |X_{ij}|$, we define $S(n)$ for all $n \in \mathbb{N}$ by

$$S(n) = \sup_{A \in N(n,\mathbb{R})} \left(\inf_{T \in N(n,\mathbb{Z})} \max(\|TA\|_\infty, \|(TA)^{-1}\|_\infty) \right).$$

In [9], the author proves that $S(2n) \leqslant S(n) \cdot \max(1, n/2)$, and concludes that $S(n) = \exp(O((\ln n)^2))$. We would like to point out that the latter is not true in general, unless some other property of the function S is invoked. Indeed, an arbitrary map s defined on the set of odd integers, e.g. $s(2n+1) = \exp(2n+1)$, and extended to $\mathbb{N}$ with the rule $s(2n) = n/2 \cdot s(n)$ satisfies the condition $s(2n) \leqslant s(n) \cdot \max(1, n/2)$ but we have $s(n) \neq \exp(O((\ln n)^2))$ in general. This point seems to have been overlooked in [9]. However, in our case, we have the following in addition.

Lemma 2.1. $\forall n \leqslant m \in \mathbb{N},\ S(n) \leqslant S(m)$.

Proof. It is not difficult to see that for all $A \in N(n, \mathbb{R})$, there exists a matrix $T_A \in N(n, \mathbb{Z})$ such that

$$\inf_{T \in N(n,\mathbb{Z})} \max(\|TA\|_\infty, \|(TA)^{-1}\|_\infty) = \max(\|T_A A\|_\infty, \|(T_A A)^{-1}\|_\infty).$$

See the Remark following Definition 4 of [9] for the details. As a consequence, in order to prove the lemma, it is sufficient to show that

$$\sup_{A \in N(n,\mathbb{R})} \max(\|T_A A\|_\infty, \|(T_A A)^{-1}\|_\infty) \leqslant \sup_{A' \in N(n+1,\mathbb{R})} \max(\|T_{A'} A'\|_\infty, \|(T_{A'} A')^{-1}\|_\infty). \tag{2.4}$$

Let us consider the map i from $N(n, \mathbb{R})$ to $N(n+1, \mathbb{R})$ defined by mapping a matrix A to the block matrix $\mathrm{diag}(1, A)$. The map i is a group homomorphism and thus $i(A)^{-1} = i(A^{-1}) = \mathrm{diag}(1, A^{-1})$. We claim that for all $A \in N(n, \mathbb{R})$ and all $T \in N(n, \mathbb{Z})$, we have

$$\max(\|i(TA)\|_\infty, \|i(TA)^{-1}\|_\infty) = \max(\|TA\|_\infty, \|(TA)^{-1}\|_\infty). \tag{2.5}$$

First, if $\max(\|i(TA)\|_\infty, \|i(TA)^{-1}\|_\infty) = 1$, then the above equality is straightforward, due to the definition of $\|\cdot\|_\infty$. Let us then consider the case where the maximum is not 1. Notice that since $\|X\|_\infty \geqslant 1$ is true for all matrix X in $N(m, \mathbb{R})$, we have that $\max(\|X\|_\infty, \|X^{-1}\|_\infty) \geqslant 1$ and so $\max(\|i(TA)\|_\infty, \|i(TA)^{-1}\|_\infty) > 1$. As a consequence the maximum in $\max(\|i(TA)\|_\infty, \|i(TA)^{-1}\|_\infty)$ is achieved by one of the entries of $i(TA)$ or $i(TA)^{-1}$, and this entry cannot be the one in the upper left corner. The maximum is then the same for both sides of (2.5). This proves the above claim. Now, since

$$\begin{aligned}\sup_{A' \in N(n+1,\mathbb{R})} \max(\|T_{A'} A'\|_\infty, \|(T_{A'} A')^{-1}\|_\infty) &\geqslant \max(\|i(TA)\|_\infty, \|i(TA)^{-1}\|_\infty) \\ &= \max(\|TA\|_\infty, \|(TA)^{-1}\|_\infty),\end{aligned}$$

is true for all $A \in N(n, \mathbb{R})$, taking the supremum on the left hand side, we see that inequality (2.4) is correct. □

This lemma makes the following inequalities valid:

$$S(n) = S(2^{\log_2 n}) \leqslant S(2^{\lceil \log_2 n \rceil}) \leqslant 2^{\lceil \log_2 n \rceil - 2} \cdot 2^{\lceil \log_2 n \rceil - 3} \cdots 2 \cdot 1 \leqslant \exp\left(\frac{(\ln n)^2}{2 \ln 2}\right).$$

The second ingredient we need is related to the Korkin–Zolotarev reduced bases of a lattice L. Such bases are well known, see e.g. [5], and one of their properties is the following: if B is a Korkin–Zolotarev reduced basis of L, and if $B = HK$, where $H = (h_{ij})$ is a lower triangular matrix and K is an orthogonal matrix, then for all $1 \leqslant i \leqslant j \leqslant n$, we have

$$h_{jj}^2 > h_{ii}^2 (j - i + 1)^{-1 - \ln(j-i+1)}.$$

This is a direct consequence of [5, Proposition 4.2] and the fact that the concept of Korkin–Zolotarev reduction is recursive. See [9] for the details. In [9], the author concludes that $\frac{h_{ii}^2}{h_{jj}^2} = \exp(O((\ln n)^2))$ but we have the more precise statement that

$$\frac{h_{ii}^2}{h_{jj}^2} \leqslant \exp((\ln(j - i + 1))^2 + \ln(j - i + 1)) \leqslant \exp((\ln n)^2 + \ln n).$$

Let us now revisit the proof of [9, Theorem 7] by making use of the previous inequalities. This theorem states that for every lattice L there is a basis $\widetilde{B} = [\widetilde{b_1}| \cdots |\widetilde{b_n}]^t$ with reciprocal basis $\widetilde{B}^* = [\widetilde{b_1}^*| \cdots |\widetilde{b_n}^*]^t$ which satisfies

$$\|\widetilde{b_i}\| \cdot \|\widetilde{b_i}^*\| \leqslant \exp(c_2(\ln n)^2)$$

for all i and for a fixed c_2, independent of n. We explicit now an upper bound for the constant c_2. Given a lattice L and a Korkin–Zolotarev reduced basis $B = HK$ as above, the proof of [9, Theorem 7] shows that there exists a basis $\widetilde{B}$, constructed from B, such that

$$\|\widetilde{b_i}\|^2 \cdot \|\widetilde{b_i}^*\|^2 \leqslant n^2 \cdot \max_{k \geqslant j} \left\{ \frac{h_{jj}^2}{h_{kk}^2} \right\} \cdot S(n)^4.$$

Making use of the previous inequalities, we can write

$$\|\widetilde{b_i}\|^2 \cdot \|\widetilde{b_i}^*\|^2 \leqslant n^2 \cdot \exp((\ln n)^2 + \ln n) \cdot \exp\left(\frac{4(\ln n)^2}{2\ln 2}\right) = \exp\left(\left(\frac{2}{\ln 2}+1\right)(\ln n)^2 + 3\ln n\right),$$

which shows that $c_2 < \frac{1}{\ln 2} + \frac{1}{2} + \frac{3}{2\ln n} < \frac{1}{\ln 2} + \frac{1}{2} + \frac{3}{2\ln 2} = \frac{5}{2\ln 2} + \frac{1}{2}$ and gives the following proposition:

Proposition 2.2. *For every lattice L there is a basis B which satisfies*

$$S(B) \leqslant \exp\left(\left(\frac{2}{\ln 2} + 1\right)(\ln n)^2 + 4\ln n\right).$$

3. Explicit expression for the Seysen measure

In this section, we present different expressions for the Seysen measure. First, let us recall the following known expression for the measure. Given a basis B of L, by definition of B^*, for all $0 \leqslant j \leqslant n$, the vector b_j^* is orthogonal to L_j, where L_j is the sublattice of L generated by all the vectors of B except b_j. If β_j is the angle between b_j and b_j^* and α_j is the angle between b_j and L_j, we have $\cos^2\beta_i = \sin^2\alpha_i$ and

$$S(B) = \sum_i \|b_i\|^2\|b_i^*\|^2 = \sum_i \frac{\langle b_i, b_i^*\rangle^2}{\cos^2\beta_i} = \sum_i \frac{1}{\sin^2\alpha_i}. \tag{3.6}$$

This has already been used in [4,11]. We introduce now the following new representation, which can be used to define the Seysen measure without any references to the dual basis:

Proposition 3.1. *For every lattice L, if $B = [b_1|\cdots|b_n]^t$ is a basis of L with $B = D \cdot V$ where $D = \mathrm{diag}(\|b_1\|, \ldots, \|b_n\|)$, then*

$$S(B) = \|V^{-1}\|^2,$$

where $\|\cdot\|$ is the Frobenius norm, i.e., $\|X\| = \sqrt{\sum_{i,j}|x_{ij}|^2}$.

Proof. Let $M = BB^t$. Using $\|X\|^2 = \mathrm{tr}(XX^t)$ and $\mathrm{tr}(ABC) = \mathrm{tr}(CAB)$, we have

$$\|V^{-1}\|^2 = \mathrm{tr}(V^{-1}(V^{-1})^t) = \mathrm{tr}(D^2M^{-1}) = \sum_i \|b_i\|^2 \cdot (M^{-1})_{i,i}.$$

Since $M^{-1} = \frac{1}{\det M}\mathrm{comat}(M)$, where $\mathrm{comat}(M)$ is the comatrix of M, we have

$$(M^{-1})_{i,i} = \frac{1}{\det M}\mathrm{comat}(M)_{i,i} = \frac{\det M^{i,i}}{\det M},$$

where $M^{i,i}$ is the square matrix obtained from M by deleting the ith row and the ith column of M. So if B^i is the matrix obtained by deleting the ith row of B, we have

$$\det M^{i,i} = \det B^i(B^i)^t = (\mathrm{Vol}\, L_i)^2,$$

which gives

$$\frac{\det M^{i,i}}{\det M} = \frac{(\operatorname{Vol} L_i)^2}{(\operatorname{Vol} L)^2} = \frac{(\operatorname{Vol} L_i)^2}{(\|b_i\| \cdot \operatorname{Vol} L_i \cdot \sin\alpha_i)^2} = \frac{1}{\|b_i\|^2 \sin^2\alpha_i}.$$

Finally,

$$\|V^{-1}\|^2 = \sum_i \|b_i\|^2 \cdot (M^{-1})_{i,i} = \sum_i \|b_i\|^2 \cdot \frac{1}{\|b_i\|^2 \sin^2\alpha_i} = S(B). \qquad \square$$

Another way of looking at the previous result is with the help of the (Frobenius) condition number of an invertible matrix X which is defined as $\kappa(X) = \|X\| \cdot \|X^{-1}\|$.

Corollary 3.2. *With the above notation, we have* $S(B) = \frac{\kappa(V)^2}{n}$.

By defining the matrix U as $U = VV^t$, then $BB^t = DUD$, where D is as above, and if θ_{ij} is the angle between b_i and b_j, then $U = (\cos\theta_{ij})_{ij}$. The matrix U is a symmetric positive definite matrix, and the eigenvalues $\lambda_1, \ldots, \lambda_n$ of U are real positive.

Corollary 3.3. *With the above notation, we have* $S(B) = \operatorname{tr}(U^{-1}) = \sum_i \frac{1}{\lambda_i}$.

From the equality $BB^t = DUD$, we have $(\operatorname{Vol} L)^2 = \det U \cdot \prod_i \|b_i\|^2$ which in turn leads to

$$\prod_i \|b_i\| = (\det U)^{-1/2} \cdot \operatorname{Vol} L = \left(\prod_i \frac{1}{\lambda_i}\right)^{1/2} \cdot \operatorname{Vol} L. \qquad (3.7)$$

The arithmetic–geometric mean inequality applied to the λ_i's, $(\prod_i 1/\lambda_i)^{1/n} \leqslant \frac{1}{n}\sum_i 1/\lambda_i$, immediately gives the inequality

$$\prod_i \|b_i\| \leqslant \left(\frac{1}{n}\sum_i \frac{1}{\lambda_i}\right)^{\frac{n}{2}} \cdot \operatorname{Vol} L = \left(\frac{S(B)}{n}\right)^{\frac{n}{2}} \cdot \operatorname{Vol} L.$$

However, we also have the equality $\sum_i \lambda_i = \operatorname{tr} U = n$, which affords a slightly better upper bound for the geometric mean. Indeed, the harmonic–geometric–arithmetic mean inequalities applied to the $1/\lambda_i$'s imply that if $g = (\prod_i 1/\lambda_i)^{1/n}$, $h = \left(\frac{1}{n}\sum_i \lambda_i\right)^{-1} = 1$ and $a = \frac{1}{n}\sum_i \frac{1}{\lambda_i} = \frac{S(B)}{n}$, then we have $h \leqslant g \leqslant a$, but we also have the following result, which is [8, Corollary 3.1].

Lemma 3.4. *With the above notations, if* $\alpha = 1/n$, *we have*

$$g \leqslant \left(\frac{a - h(1-2\alpha) - \sqrt{(a-h)(a-h(1-2\alpha)^2)}}{2\alpha}\right)^{\alpha} \times \left(\frac{a + h(1-2\alpha) + \sqrt{(a-h)(a-h(1-2\alpha)^2)}}{2(1-\alpha)}\right)^{1-\alpha}.$$

This leads to the following inequality:

Proposition 3.5. *With the above notation, we have*

$$\prod_i \|b_i\| \leqslant e^{1/2} \cdot \left(\frac{S(B)+1}{n}\right)^{\frac{n-1}{2}} \cdot \operatorname{Vol} L. \qquad (3.8)$$

Proof. Since $(1-2/n)^2 \leqslant 1$, we have

$$(a-h)^2 \leqslant (a-h)(a-h(1-2/n)^2) \leqslant (a-h(1-2/n)^2)^2$$

and thus the upper bound of the previous lemma gives

$$g \leqslant \left(\frac{a-h(1-2/n)-(a-h)}{2/n}\right)^{1/n} \left(\frac{a+h(1-2/n)+(a-h(1-2/n)^2)}{2(1-1/n)}\right)^{1-1/n}.$$

After suitable simplification, we obtain

$$g \leqslant a \cdot \left(\frac{h}{a}\right)^{1/n} \cdot \left(1+\frac{h}{a}\cdot\left(1-\frac{2}{n}\right)\cdot\frac{1}{n}\right)^{1-1/n} \cdot \left(1+\frac{1}{n-1}\right)^{1-1/n}.$$

Since $\left(1+\frac{1}{n-1}\right)^{n-1} < e$, taking the nth power of both sides of the previous inequality gives

$$\prod_i 1/\lambda_i < e \cdot \left(\frac{S(B)+1-\frac{2}{n}}{n}\right)^{n-1} < e \cdot \left(\frac{S(B)+1}{n}\right)^{n-1}.$$

The result follows by applying the previous inequality to Eq. (3.7). □

This is an improvement by a factor of roughly $n^{n/2}$ of the bound given by (1.3), and can be used to strengthen the bound of the orthogonality defect (1.1):

Corollary 3.6. *With the above notations, we have*

$$\mathrm{od}(B) \leqslant 1 - \frac{1}{e}\left(\frac{n}{S(B)+1}\right)^{n-1}.$$

Combining the previous proposition with the explicit bound of Proposition 2.2, we have the following proposition:

Proposition 3.7. *For every lattice L, if $B = [b_1|\cdots|b_n]^t$ is a Seysen reduced basis, then*

$$\min_i \|b_i\| \leqslant \exp\left(\left(\frac{1}{\ln 2}+\frac{1}{2}\right)(\ln n)^2 + O(\ln n)\right) \cdot (\mathrm{Vol}\, L)^{1/n}.$$

4. Conclusion

In this article, we gave an explicit upper bound for the constant hidden inside Landau's notation of the original bound of the Seysen measure [9]. We also developed the connection between the Seysen measure and standard linear algebra concepts such as the Frobenius norm and the condition number of a matrix. This allowed us to improve known upper bounds for the Seysen measure and the orthogonality defect.

References

[1] J. Hastad, J. Lagarias, Simultaneously good bases of a lattice and its reciprocal lattice, Math. Ann. 287 (1990) 163–174.
[2] E. Kaltofen, G. Villard, Computing the sign or the value of the determinant of an integer matrix a complexity survey, J. Comput. Appl. Math. 162 (1) (2004) 133–146.
[3] A. Korkin, G. Zolotarev, Sur les formes quadratiques, Math. Ann. 6 (1873) 366–389.
[4] B.A. LaMacchia, Basis reduction algorithms and subset sum problems, SM Thesis, Dept. of Elect. Eng. and Comp. Sci., Massachusetts Institute of Technology, Cambridge, MA, May 1991.
[5] A.K. Lenstra, H.W. Lenstra, L. Lovasz, Factoring polynomials with rational coefficients, Math. Ann. 261 (1982) 515–534.
[6] C. Ling, Towards characterizing the performance of approximate lattice decoding in MIMO communications, in: Proceedings of International Symposium on Turbo Codes/International ITG Conference Source Channel Coding06, Munich, Germany, April 2006.

[7] C. Ling, On the proximity factors of lattice reduction aided decoding, IEEE Trans. Inform. Theory, submitted for publication. Available from <http://arxiv.org/abs/1006.1666>.
[8] G. Maze, U. Wagner, A note on the weighted harmonic–geometric–arithmetic means inequalities, submitted for publication. Available from <http://arxiv.org/abs/0910.0948>.
[9] M. Seysen, Simultaneous reduction of a lattice basis and its reciprocal basis, Combinatorica 13 (3) (1993) 363–376.
[10] M. Seysen, A measure for the non-orthogonality of a lattice basis, Combin. Probab. Comput. 8 (1999) 281–291.
[11] W. Zhang, F. Arnold, X. Mai, An analysis of Seysen's lattice reduction algorithm, Signal Process. 88 (10) (2008) 2573–2577.