Some Inequalities Related to the Seysen Measure of a Lattice

Gérard Maze
e-mail: gmaze@math.uzh.ch
Mathematics Institute
University of Zürich
Winterthurerstr 190, CH-8057 Zürich, Switzerland

June 14, 2010

Abstract
Given a lattice $L$, a basis $B$ of $L$ together with its dual $B^\ast$, the orthogonality measure $S(B) = \sum_i ||b_i||^2 ||b_i^\ast||^2$ of $B$ was introduced by M. Seysen [9] in 1993. 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.

Key Words: Lattice, orthogonality defect, Seysen measure, HGA inequality

Subject Classification: Primary 11H06, Secondary 15A42, 11-04

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

\[ L = \left\{ \sum_{i=1}^{n} a_i b_i \mid a_i \in \mathbb{Z} \right\}. \]

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 $\text{Vol} L$ of $L$ is the well defined real number $(\det BB^t)^{1/2}$. The dual lattice of $L$ is defined by the basis $B^\ast = (B^\ast)^t$, where $B^\ast$ is the Moore-Penrose inverse, or pseudo-inverse, of $B$. If $B^\ast = [b_1^\ast | \ldots | b_n^\ast]^t$, then since $BB^\ast = I_n$, we have $\langle b_i, b_j^\ast \rangle = \delta_{i,j}$. Lattice reduction theory deals with the problem of identifying and computing bases of a given lattice whose vectors are short 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 $B^\ast$ consist in relatively short vector, i.e., $\max_i ||b_i|| \cdot ||b_i^\ast|| \leq \exp(O(n^{1/3}))$. In 1993, Seysen [9] improved this upper bound to $\exp(O(\ln^2(n)))$ and suggested to use the expression $S(B) := \sum_i ||b_i||^2 ||b_i^\ast||^2$. 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]

\[ \text{od} (B) := 1 - \frac{\det BB^t}{\prod_{i=1}^{n} ||b_i||^2} \in [0, 1] \]
and the Seysen measure $S(B)$ is given in [11] where the following bounds can be found:

$$n \leq S(B) \leq \frac{n}{1 - \od(B)}, \quad (1.1)$$

$$0 \leq \od(B) \leq 1 - \frac{1}{(S(B) - n + 1)^{n-1}}. \quad (1.2)$$

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

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

which in turn provides the inequality

$$\min_i ||b_i|| \leq (S(B) - n + 1)^{(n-1)/2n} (\text{Vol} L)^{1/n}. \quad (1.3)$$

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

$$\text{min}_i ||b_i|| \leq \sqrt{n} (\text{Vol} L)^{1/n}$$

for Korkin Zolotarev and Minkovsky reduced bases

$$\text{min}_i ||b_i|| \leq (4/3)^{(n-1)/4} (\text{Vol} L)^{1/n}$$

for LLL reduced bases.

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

$$\text{min}_i ||b_i|| = \frac{\sqrt{n}}{\ln(2)}$$

for Korkin Zolotarev and Minkovsky reduced bases

$$\text{min}_i ||b_i|| \leq (4/3)^{(n-1)/4} (\text{Vol} L)^{1/n}$$

for LLL reduced bases.

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 $1 + \frac{1}{\ln 2}$. 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 [11] and [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 $S(2n) \leq S(n) \cdot \max(1, n/2)$, 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 $s(2n) \leq s(n) \cdot \max(1, n/2)$ 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** $\forall n \leq m \in \mathbb{N}, S(n) \leq S(m)$

**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

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

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

$$\sup_{A \in N(n, \mathbb{R})} \max(||TA||_\infty, ||(TA)^{-1}||_\infty) \leq \sup_{A' \in N(n+1, \mathbb{R})} \max(||T_{A'}A'||_\infty, ||(T_{A'}A')^{-1}||_\infty). \quad (2.4)$$
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 \( \text{diag}(1, A) \). The map \( i \) is a group homomorphism and thus \( i(A)^{-1} = i(A^{-1}) = \text{diag}(1, A^{-1}) \). We claim that for all \( A \in N(n, \mathbb{R}) \) and all \( T \in N(n, \mathbb{Z}) \), we have

\[
\max(||i(TA)||_\infty, ||i(TA)^{-1}||_\infty) = \max(||TA||_\infty, ||(TA)^{-1}||_\infty).
\]  

(2.5)

First, if \( \max(||i(TA)||_\infty, ||i(TA)^{-1}||_\infty) = 1 \), then the above equality is straightforward, due to the definition of \( ||.||_\infty \). Let us then consider the case where the maximum is not 1. Notice that since \( ||X||_\infty \geq 1 \) is true for all matrix \( X \) in \( N(m, \mathbb{R}) \), we have that \( \max(||X||_\infty, ||X^{-1}||_\infty) \geq 1 \) 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

\[
\sup_{A' \in N(n+1, \mathbb{R})} \max(||TA\cdot A'||_\infty, ||(TA\cdot A')^{-1}||_\infty) \geq \max(||i(TA)||_\infty, ||i(TA)^{-1}||_\infty) = \max(||TA||_\infty, ||(TA)^{-1}||_\infty),
\]

is true for all \( A \in N(n, \mathbb{R}) \), taking the supremum on the left hand side, we see that Inequality (2.5) is correct.

This lemma makes the following inequalities valid:

\[
S(n) = S(2^{\log_2 n}) \leq S(2^{2\log_2 n - 1}) \leq 2^{2\log_2 n - 2} \cdot 2^{2\log_2 n - 3} \cdot \ldots \cdot 2 \cdot 1 \leq \exp\left(\frac{(\ln n)^2}{2 \ln 2}\right).
\]

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 \( 1 \leq i \leq j \leq n \), we have

\[
h_{ij}^2 \geq h_{ii}^2(j-i+1)^{-1}\ln(j-i+1).
\]

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 \( \frac{h_{ij}^2}{h_{kk}^2} = \exp(O((\ln n)^2)) \) but we have the more precise statement that

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

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 \( \hat{B} = [\hat{b}_1| \ldots |\hat{b}_n]^t \) with reciprocal basis \( \hat{B}^* = [\hat{b}_1^*| \ldots |\hat{b}_n^*]^t \) which satisfies

\[
||\hat{b}_i|| \cdot ||\hat{b}_i^*|| \leq \exp(c_2(\ln n)^2)
\]

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 \( \hat{B} \), constructed from \( B \), such that

\[
||\hat{b}_i||^2 \cdot ||\hat{b}_i^*||^2 \leq n^2 \cdot \max_{k \geq j} \left\{ \frac{h_{jj}^2}{h_{kk}^2} \right\} \cdot S(n)^4
\]

Making use of the previous inequalities, we can write

\[
||\hat{b}_i||^2 \cdot ||\hat{b}_i^*||^2 \leq n^2 \cdot \exp((\ln n)^2 + \ln n) \cdot \exp\left(\frac{4(\ln n)^2}{2 \ln 2}\right) = \exp\left(\frac{2}{\ln 2} + 1\right)(\ln n)^2 + 3 \ln n).
\]

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

**Proposition 2.2** For every lattice \( L \) there is a basis \( B \) which satisfies

\[
S(B) \leq \exp\left(\frac{2}{\ln 2} + 1\right)(\ln n)^2 + 4 \ln n).
\]
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 \( B^\ast \), for all \( 0 \leq j \leq n \), the vector \( b^\ast_j \) is orthogonal to \( L_j \), where \( L_j \) is the sublattice of \( L \) generated by all the vectors of \( B \) except \( b_j \). If \( \beta_j \) is the angle between \( b_j \) and \( b^\ast_j \) and \( \alpha_j \) is the angle between \( b_j \) and \( L_j \), we have \( \cos^2 \beta_i = \sin^2 \alpha_i \) and

\[
S(B) = \sum_i ||b_i||^2 ||b_i^\ast||^2 = \sum_i \frac{\langle b_i, b_i^\ast \rangle^2}{\cos^2 \beta_i} = \sum_i \frac{1}{\sin^2 \alpha_i}.
\] (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 \( B = [b_1| \ldots |b_n]^t \) is a basis of \( L \) with \( B = D \cdot V \) where \( D = \text{diag} (||b_1||, \ldots , ||b_n||) \), 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 \( ||X||^2 = \text{tr} (XX^t) \) and \( \text{tr} (ABC) = \text{tr} (CAB) \), we have

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

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

\[ (M^{-1})_{i,i} = \frac{1}{\det M} \text{comat}(M)_{i,i} = \frac{\det M^{i,i}}{\det M} \]

where \( M^{i,i} \) is the square matrix obtained from \( M \) by deleting the \( i \)-th row and the \( i \)-th column of \( M \). So if \( B^t \) is the matrix obtained by deleting the \( i \)-th row of \( B \), we have

\[ \det M^{i,i} = \det B^t(B^t)^t = (\text{Vol} L_i)^2 \]

which gives

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

Finally,

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

\[ \square \]

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 \( U = VV^t \), then \( BB^t = DUD \), where \( D \) is as above, and if \( \theta_{ij} \) 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 \( S(B) = \text{tr} (U^{-1}) = \sum_i \frac{1}{\lambda_i} \).
From the equality $BB^t = DUD$, we have $(\text{Vol } L)^2 = \det U \cdot \prod_i ||b_i||^2$ which in turn leads to
\[
\prod_i ||b_i|| = (\det U)^{-1/2} \cdot \text{Vol } L = \left( \prod_i \frac{1}{\lambda_i} \right)^{1/2} \cdot \text{Vol } L. \tag{3.7}
\]
The arithmetic-geometric mean inequality applied to the $\lambda_i$'s, $(\prod_i 1/\lambda_i)^{1/n} \leq \frac{1}{n} \sum_i 1/\lambda_i$, immediately gives the inequality
\[
\prod_i ||b_i|| \leq \left( \frac{1}{n} \sum_i \frac{1}{\lambda_i} \right)^{\frac{n}{2}} \cdot \text{Vol } L = \left( \frac{S(B)}{n} \right)^{\frac{n}{2}} \cdot \text{Vol } L.
\]
However, we also have the equality $\sum_i \lambda_i = \text{tr } U = n$, 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 $g = (\prod_i 1/\lambda_i)^{1/n}$, $h = (\frac{1}{n} \sum_i 1/\lambda_i)^{-1} = 1$ and $a = \frac{1}{n} \sum_i \frac{1}{\lambda_i} = \frac{S(B)}{n}$, then we have $h \leq g \leq a$, but we also have the following result, which is \cite[Corollary 3.1]{8}.

**Lemma 3.4** With the above notations, if $\alpha = 1/n$, we have
\[
g \leq \left( \frac{a - h(1 - 2\alpha) - \sqrt{(a - h)(a - h(1 - 2\alpha)^2)}}{2\alpha} \right)^{\alpha} \left( \frac{a + h(1 - 2\alpha) + \sqrt{(a - h)(a - h(1 - 2\alpha)^2)}}{2(1 - \alpha)} \right)^{1-\alpha}.
\]

This leads to the following inequality:

**Proposition 3.5** With the above notation, we have
\[
\prod_i ||b_i|| \leq e^{1/2} \cdot \left( \frac{S(B) + 1}{n} \right)^{\frac{n-1}{n}} \cdot \text{Vol } L. \tag{3.8}
\]

**Proof:** Since $(1 - 2/n)^2 \leq 1$, we have
\[
(a - h)^2 \leq (a - h)(a - h(1 - 2/n)^2) \leq (a - h(1 - 2/n)^2)^2
\]
and thus the upper bound of the previous Lemma gives
\[
g \leq \left( \frac{a - h(1 - 2/n) - (a - h)}{2/n} \right)^{1/n} \left( \frac{a + h(1 - 2/n) + (a - h(1 - 2/n)^2)}{2(1 - 1/n)} \right)^{1-1/n}.
\]

After suitable simplification, we obtain
\[
g \leq a \cdot \left( \frac{h}{\alpha} \right)^{1/n} \cdot \left( 1 + \frac{h}{a} \cdot \left( 1 - \frac{2}{n} \right) \cdot \frac{1}{n} \right)^{1-1/n} \cdot \left( 1 + \frac{1}{n - 1} \right)^{-1/n}.
\]

Since $(1 + \frac{1}{n-1})^{n-1} < e$, taking the $n$-th power of both sides of the previous inequality gives
\[
\prod_i 1/\lambda_i < e \cdot \left( \frac{S(B) + 1}{n} \right)^{n-1} < e \cdot \left( \frac{S(B) + 1}{n} \right)^{n-1}.
\]
The result follows by applying the previous inequality to Equation (3.7). \hfill $\square$

This is an improvement by a factor of roughly $n^{n/2}$ of the bound given by \cite{13}, and can be used to strengthen the bound of the orthogonality defect (3.1):

**Corollary 3.6** With the above notations, we have
\[
\text{od}(B) \leq 1 - \frac{1}{e} \left( \frac{n}{S(B) + 1} \right)^{n-1}
\]
Combining the previous proposition with the explicit bound of Proposition \cite{22} we have the following proposition:

**Proposition 3.7** For every lattice $L$, if $B = [b_1| \ldots |b_n]^t$ is a Seysen reduced basis, then
\[
\min_i ||b_i|| \leq \exp \left( \frac{1}{\ln 2} + \frac{1}{2} \right) (\ln n)^2 + O(\ln n) \cdot (\text{Vol } L)^{1/n}.
\]
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] Hastad, J. and Lagarias, J. *Simultaneously Good Bases of a Lattice and its Reciprocal Lattice*. Mathematische Annalen 287, 1990, 163-174.

[2] Kaltofen, E. and Villard, G. *Computing the sign or the value of the determinant of an integer matrix a complexity survey*. J. Comput. Appl. Math. 162 (1) (2004), pp. 133-146.

[3] Korkin, A. and Zolotarev, G. *Sur les formes quadratiques*. Math. Ann. 6 (1873), pp. 366–389

[4] LaMacchia, B.A. *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] Lenstra, A.K., Lenstra, H.W., and Lovasz, L. *Factoring polynomials with rational coefficients*. Math. Ann. 261 (1982), pp. 515-534.

[6] Ling, C. *Towards characterizing the performance of approximate lattice decoding in MIMO communications*. Proceedings of International Symposium on Turbo Codes/International ITG Conference Source Channel Coding06, Munich, Germany, April 2006.

[7] Ling, C. *On the proximity factors of lattice reduction aided decoding*. Submitted to IEEE Trans. on Information Theory, May 2007. Available at [http://www.commsp.ee.ic.ac.uk/cling/Lattice.pdf](http://www.commsp.ee.ic.ac.uk/cling/Lattice.pdf)

[8] Maze, G. and Wagner, U. *A Note on the Weighted Harmonic-Geometric-Arithmetic Means Inequalities*. Submitted for publication, available at [http://arxiv.org/abs/0910.0948](http://arxiv.org/abs/0910.0948)

[9] Seysen, M. *Simultaneous reduction of a lattice basis and its reciprocal basis*. Combinatorica 13(3): 363–376 (1993)

[10] Seysen, M. *A measure for the non-orthogonality of a lattice basis*. Combinatorics, Probability and Computing (1999), 8, 281–291

[11] Zhang, W., Arnold, F., and Mai, X. *An analysis of Seysen’s lattice reduction algorithm*. Signal Processing, Volume 88, Issue 10, October 2008, Pages 2573–2577.