On the minimum volume of a perturbed unit cube

Jin-Yi Cai *
Computer Sciences Department
University of Wisconsin
Madison, WI 53706
jyc@cs.wisc.edu

Abstract

We give exact bounds to the minimum volume of a parallelepiped whose spanning vectors are perturbations of the n unit vectors by vectors of length at most ϵ. This extends Micciancio's recent sharp bounds to all possible values of ϵ. We also completely determine all possible perturbations with length at most ϵ that achieve this minimum volume.

1 Problem Statement

This problem was originally studied in the context of the connection of worst-case/average-case complexity for lattice problems.

Suppose Q is the unit cube, spanned by the n unit vectors $e_1 = (1, 0, \ldots, 0), e_2 = (0, 1, \ldots, 0), \ldots, e_n = (0, 0, \ldots, 1)$,

$$Q = \{\sum_{i=1}^{n} a_i e_i \mid 0 \leq a_i \leq 1, 1 \leq i \leq n\}. \tag{1}$$

Suppose now we allow a perturbation x_i to be applied to each e_i, and consider the parallelepiped spanned by $u_1 = e_1 + x_1, u_2 = e_2 + x_2, \ldots, u_n = e_n + x_n$,

$$P = \{\sum_{i=1}^{n} a_i u_i \mid 0 \leq a_i \leq 1, 1 \leq i \leq n\}, \tag{2}$$

subject to the condition that all perturbation vectors x_i are of 2-norm at most ϵ: $||x_i|| \leq \epsilon$. We ask what is the minimum volume

$$f_n(\epsilon) = \min\{\text{vol}(P)\}, \tag{3}$$

where the minimum is taken over all $||x_i|| \leq \epsilon$. As the volume function is continuous, and the minimization is over a compact set, clearly the minimum exists.

*Research supported in part by NSF grant CCR-9634665.

2 Preliminaries

This problem came up in the work on the connection of worst-case/average-case complexity for lattice problems. It was implicit in [1]. In [3] a lower bound $f_n(\epsilon) \geq 1 - \epsilon n$ was proved. This was sufficient for their purpose, when ϵ was small, $\epsilon = o(n)$. The exact nature of the function $f_n(\epsilon)$ was explicitly asked to be determined in [2].

The volume of a parallelepiped spanned by $u_1, u_2, \ldots, u_n$ is given by the absolute value of the determinant of $I + X$. Thus

$$f_n(\epsilon) = \min\{|\det((I + X)|\}, \tag{4}$$

where the $n \times n$ matrix X has column vectors $x_i, 1 \leq i \leq n$, and I is the $n \times n$ unit matrix. Clearly f_n is monotonically non-increasing by definition, and starts off with $f_n(0) = 1$.

We first show that

Lemma 1 *Let $n \geq 1$. For any $\epsilon < \frac{1}{\sqrt{n}}$, $f_n(\epsilon) > 0$, and for any $\epsilon \geq \frac{1}{\sqrt{n}}$, $f_n(\epsilon) = 0$. Moreover, For any $\epsilon < \frac{1}{\sqrt{n}}$, the determinant $\det(I + X) > 0$, and thus the absolute value sign in the definition of f_n is unnecessary for all $\epsilon \leq \frac{1}{\sqrt{n}}$.*

To show that $\det(I + X)$ is always positive for $||x_i|| < 1/\sqrt{n}$, we apply the Cauchy-Schwarz inequality to x_i and get the 1-norm $||x_i||_1 < 1$. Therefore the matrix $I + X$ has the property of strict central dominance by the column: $\forall j, 1 \leq j \leq n$,

$$1 + x_{jj} > \sum_{i \neq j} |x_{ij}|. \tag{5}$$

Such a matrix must have a positive determinant.

First, the determinant must be non-zero, or else, there exists a non-zero (row) vector v^T, such that

$$v^T(I + X) = 0. \tag{6}$$

We can assume the infinity norm of v is 1, and say $1 = |v_1| \geq |v_i|$. By replacing v with $-v$, we may assume $v_1 = 1$. Then

$$1 + x_{11} + \sum_{i \geq 2} x_{i1} v_i \geq 1 + x_{11} - \sum_{i \geq 2} |x_{i1}| > 0, \tag{7}$$

a contradiction.

Then a deformation argument shows that $\det(I + X) > 0$, for otherwise, for some $0 < t < 1$, $\det(I + tX) = 0$, contradicting to what has just been shown.

To see that for $\epsilon = 1/\sqrt{n}$, $f_n(\epsilon) = 0$, we take each $x_i = -\frac{1}{n}(1, 1, \ldots, 1)^T$, we observe that the matrix $I + X$ is singular, having all columns sum to 0.

So the only interesting values for ϵ are within $0 \leq \epsilon \leq 1/\sqrt{n}$. Suppose now the perturbation matrix X achieves the minimum volume, for a given ϵ in that range. Micciancio [4] gave a precise bound for f_n where $0 \leq \epsilon \leq \sqrt{\frac{1}{n} - \frac{1}{n^2}}$. His argument is short and pretty, and will be our starting point. For the sake of completeness we will present his argument first.

Micciancio observed the following necessary condition for the matrix X: For every dimension $1 \leq i \leq n$, the perturbation x_i must be perpendicular to the hyperplane spanned by $\{e_j + x_j \mid j \neq$

$i, 1 \le j \le n\}$, and must be of maximum norm ϵ. This is clear in terms of the geometry and the fact that $\det(I+X)$ is always non-negative in that range. In matrix terms

$$X^T(I+X) = \epsilon^2 I + \mathrm{diag}(x_{11}, x_{22}, \ldots, x_{nn}). \tag{8}$$

Denote by T the diagonal matrix consisting of exactly the diagonal entries of X, then it follows that $X^T = \epsilon^2 I + T - X^T X$, which is symmetric, and hence so is X, and

$$X^2 + X = \epsilon^2 I + T. \tag{9}$$

With suitable renaming of the dimensions, and a suitable permutations of the columns of X we may assume X is grouped according to equal values on the diagonal, i.e.,

$$T = \begin{pmatrix} t_1 I_1 & 0 & \cdots & 0 \\ 0 & t_2 I_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & t_k I_k \end{pmatrix} \tag{10}$$

where $1 \le k \le n$, each I_j has dimension m_j, $\sum_{j=1}^k m_j = n$, and if $i \ne j$ then $t_i \ne t_j$.

Since X is symmetric, there is an orthogonal matrix W such that $W^T X W$ is a diagonal matrix with eigenvalues of X on the diagonal. T being a polynomial of X, it follows that $W^T T W$ is also diagonal with the eigenvalues of T on the diagonal, thus it is a permutation of the diagonal entries of T. Thus there is a permutation matrix Π such that if we let $U = W\Pi$, then U is orthogonal, $U^T T U = T$, and $U^T X U$ is still a diagonal matrix with eigenvalues of X on the diagonal.

Partition the matrices $U = (U_{ij})$ and $X = (X_{ij})$ according to the dimensions $m_1, m_2, \ldots, m_k$, then by $TU = UT$ we have $t_i U_{ij} = t_j U_{ij}$ and thus $U_{ij} = 0$ if $i \ne j$. Therefore U is block diagonal, we name it $U = \mathrm{diag}(U_1, \ldots, U_k)$, each U_j is orthogonal. Since $U^T X U$ is diagonal, $U_i^T X_{ij} U_j = 0$ if $i \ne j$, and thus $X_{ij} = 0$ as well. So X is block diagonal as well, and we rename it $X = \mathrm{diag}(X_1, \ldots, X_k)$. We have arrived at the following necessary condition:

$$X_i^2 + X_i = (\epsilon^2 + t_i) I, \tag{11}$$

for each block of dimension m_i, $1 \le i \le k$.

Note that if the eigenvalues of X are λ_i, then the volume determinant is $\Pi_{i=1}^n (1+\lambda_i)$, and this product decomposes over the subspaces. It follows that the minimization problem is decomposed into the subproblems over all these blocks (except the perturbation vectors are still subject to the overall bound $1/\sqrt{n}$.) It is also clear that if any $m_i = 1$, the optimum is unique for that block with $X_i = -\epsilon$. Thus we consider in the following any $m_i \ge 2$. Rename, for some i, $m = m_i$, $Y = X_i$, $V = U_i$, $\tau = -t_i$, then we have

$$Y^2 + Y = (\epsilon^2 - \tau) I. \tag{12}$$

Micciancio's theorem [4] is the following

Theorem 1 (Micciancio) *For all $\epsilon < \sqrt{\frac{1}{n} - \frac{1}{n^2}}$, $f_n(\epsilon) = (1-\epsilon)^n$ and the minimum is uniquely achieved with $X = -\epsilon I$.*

He also noted the upper bound that $f_n(\epsilon) \le 1 - \epsilon\sqrt{n}$ by taking all entries of X to $\epsilon/\sqrt{n}$. Hence he has

$$0 < f_n(\epsilon) \le \min\{(1-\epsilon)^n, 1 - \epsilon\sqrt{n}\} \tag{13}$$

for all $\epsilon < 1/\sqrt{n}$.

Theorem 1 will follow if $Y = -\epsilon I$ for each block, under the restriction on ϵ (and it follows that in this case there is in fact only one block).

Our main theorem is to prove the following refinement which completely characterizes the function $f_n(\epsilon)$.

Theorem 2 *Let $n \geq 1$. Let $A_n(\epsilon) = (1-\epsilon)^n$, for $0 \leq \epsilon \leq \frac{1}{\sqrt{n}}$. Let $B_n(\epsilon) = x(1-x)^{n-1}$, where*

$$x = \frac{1}{n} - \sqrt{\epsilon^2 - \frac{1}{n} + \frac{1}{n^2}}, \tag{14}$$

for $\sqrt{\frac{1}{n} - \frac{1}{n^2}} \leq \epsilon \leq \frac{1}{\sqrt{n}}$.

Then there is a unique cross over point c_n, satisfying $\sqrt{\frac{1}{n} - \frac{1}{n^2}} \leq c_n \leq \frac{1}{\sqrt{n}}$, such that

$$f_n(\epsilon) = \begin{cases} A_n(\epsilon) & \text{for } 0 \leq \epsilon \leq c_n \\ B_n(\epsilon) & \text{for } c_n \leq \epsilon \leq \frac{1}{\sqrt{n}} \end{cases} \tag{15}$$

Moreover, for $0 \leq \epsilon < c_n$ the minimum $A_n(\epsilon)$ is achieved uniquely by $X = -\epsilon I$, and for $c_n < \epsilon \leq \frac{1}{\sqrt{n}}$, the minimum $B_n(\epsilon)$ is achieved by exactly 2^{n-1} distinct perturbations, given by

$$X = \mu I + \xi \begin{pmatrix} \epsilon_1 \\ \epsilon_2 \\ \vdots \\ \epsilon_m \end{pmatrix} (\epsilon_1 \quad \epsilon_2 \quad \cdots \quad \epsilon_m), \tag{16}$$

where

$$\mu = -\frac{1}{n} + \sqrt{\epsilon^2 - \frac{1}{n} + \frac{1}{n^2}}. \tag{17}$$

and

$$\xi = -\frac{1}{n} + \frac{2}{n^2} - \frac{2}{n}\sqrt{\epsilon^2 - \frac{1}{n} + \frac{1}{n^2}}, \tag{18}$$

Finally c_n is asymptotically $\frac{1}{\sqrt{n}}(1 - e^{-\sqrt{n}})$.

The rest of this paper is to give a proof to this theorem.

Let $V^T Y V = \mathrm{diag}(\lambda_1, \ldots, \lambda_m)$, then each eigenvalue of Y satisfies

$$\lambda_i^2 + \lambda_i = \epsilon^2 - \tau. \tag{19}$$

Thus $\lambda_i = \mu_+$ or μ_-, where

$$\mu_\pm = -\frac{1}{2} \pm \sqrt{\frac{1}{4} + \epsilon^2 - \tau}. \tag{20}$$

Lemma 2 *For all $n \geq 1$, in order to achieve minimum volume, if $\epsilon < \sqrt{\frac{1}{n} - \frac{1}{n^2}}$, then all eigenvalues take the value μ_+. Moreover, for all $n > 4$ and $\epsilon \leq 1/\sqrt{n}$, there can be at most one eigenvalue $\lambda_i = \mu_-$, all others take the value μ_+.*

The first claim in Lemma 2 was from [4] and Theorem 1 was proved from that. Indeed, in that case Y is a scalar matrix, and to have $\det(I+Y)$ minimum obviously it must take the value $-\epsilon I_m$, and thus in fact there is only one block, $k=1$, $m=n$, and $X=-\epsilon I_n$.

We may assume $\mu_+ \neq \mu_-$, otherwise the matrix is scalar. Thus $n \geq m \geq 2$.

To prove the lemma, write Y by columns $Y=(y_1,\ldots,y_m)$, and consider the square of Frobenius norm $||Y||_F^2 = \sum_{i=1}^m ||y_i||^2 = m\epsilon^2$. This is invariant under the orthogonal transformation V^TYV, and thus

$$m\epsilon^2 = \sum_{i=1}^m \lambda_i^2. \tag{21}$$

If there are exactly ℓ of them taking μ_-, then $m\epsilon^2 = \ell\mu_-^2 + (m-\ell)\mu_+^2$. If $\ell \geq 1$, then $m\epsilon^2 \geq \mu_-^2 + (m-1)\mu_+^2$, since $|\mu_-| \geq |\mu_+|$. Let $g(\xi)$ be the quadratic function $g(\xi) = (1/2+\xi)^2 + (m-1)(1/2-\xi)^2$, for $\xi \geq 0$. Then it is easy to show by differentiation that g has the unique minimum at $\xi = 1/2 - 1/m$, and we get $m\epsilon^2 \geq g(1/2-1/m) = 1-1/m$. So

$$\epsilon^2 \geq \frac{1}{m}\left(1-\frac{1}{m}\right), \tag{22}$$

which is $\geq \frac{1}{n}\left(1-\frac{1}{n}\right)$, for $2 \leq m \leq n$.

Suppose now $n > 4$ and $\ell \geq 2$. By the same argument

$$m\epsilon^2 \geq 2\mu_-^2 + (m-2)\mu_+^2. \tag{23}$$

Let $h(\xi)$ be the following quadratic function $h(\xi) = 2(1/2+\xi)^2 + (m-2)(1/2-\xi)^2$, for $\xi \geq 0$. Again it is easy to show that $h(\xi)$ has a unique minimum at $\xi = 1/2 - 2/m$, and we get $m\epsilon^2 \geq 2 - 4/m$. Using $\epsilon^2 \leq 1/n$, we have $2 - 4/m \leq m/n \leq 1$ which implies that $m \leq 4$. Moreover, if $m=4$ we get $2-1 \leq 4/n$ and if $m=3$ we get $2-4/3 \leq 3/n$. Being an integer, in either cases, we can conclude that $n \leq 4$. So if $n > 4$ and $\ell \geq 2$, then $m \leq 2$.

But if $m=2$ and $\ell = 2$ we have a scalar matrix Y. But, for a scalar matrix Y to have minimum determinant $\det(I+Y)$, it must take the smaller eigenvalue μ_- twice, and not μ_+.

Lemma 2 is proved.

Continuing the argument further, assuming $\ell \geq 1$, we had (22), from which and $\epsilon^2 \leq 1/n$, we get $m/n \geq 1 - 1/m \geq 1/2$. Thus $m \geq n/2$. Substituting back we get $m/n \geq 1 - 2/n$, from which we get $m \geq n-2$, a happy situation where the estimate improves itself. Substituting back again we get $m/n \geq (n-3)/(n-2)$. m being an integer and $n > 4$, we finally derive that $m \geq n-1$. In particular such a block Y with more than one eigenvalues, if it exists, is unique.

Lemma 3 *Let $n > 4$. In order to achieve minimum volume, the number of blocks Y with more than one eigenvalues is at most one, and if such a block exists, its dimension m is either n or $n-1$. Furthermore one of its eigenvalues is taken with multiplicity $m-1$.*

3 Rank 1 perturbation of a scalar matrix

For any $m \geq 2$, let the symmetric matrix Y be a block as in Section 2 having the property that it has two distinct eigenvalues, one of which μ is of multiplicity $m-1$. Then $Y - \mu I$ is of rank 1. Thus, there exists non-zero vectors y and z, such that $Y - \mu I = yz^T$. Say $y_i \neq 0$ and $z_j \neq 0$. By being symmetric, $y_iz_j = y_jz_i \neq 0$. Let $\xi = y_iz_i \neq 0$, take out ξ and rename y and z, we get

$$Y - \mu I = \xi yz^T, \tag{24}$$

where $y_i = z_i = 1$. Note that $\forall k, 1 \le k \le n$, by symmetry, $z_k = y_i z_k = y_k z_i = y_k$, and so $y = z$.

$$Y - \mu I = \xi y y^T. \tag{25}$$

Recall that all diagonal entries of Y are the same $-\tau$, take any diagonal entry we get $-\tau - \mu = \xi y_j^2$. As $\xi \neq 0$, all $|y_j|$ are equal and $|y_j| = y_i = 1$. Therefore Y takes the following form,

$$Y = \mu I + \xi \begin{pmatrix} \epsilon_1 \\ \epsilon_2 \\ \vdots \\ \epsilon_m \end{pmatrix} (\epsilon_1 \quad \epsilon_2 \quad \cdots \quad \epsilon_m), \tag{26}$$

where all $\epsilon_j = \pm 1$. We may further write $\epsilon_1 = 1$, which then uniquely specifies 2^{n-1} choices of ϵ_j.

It follows that $(Y - \mu I)^2 = m\xi(Y - \mu I)$. Expanding, we have $Y^2 = (2\mu + m\xi)Y - (\mu^2 + m\xi\mu)I$. Compare this to the matrix equation $Y^2 + Y = (\epsilon^2 - \tau)I$, and noting that $\{I, Y\}$ are linearly independent (i.e., Y is not a scalar matrix), we get

$$1 + 2\mu + m\xi = 0 \tag{27}$$
$$\epsilon^2 - \tau + \mu^2 + m\xi\mu = 0 \tag{28}$$

Also by taking trace,

$$m\tau + m\mu + m\xi = 0. \tag{29}$$

So

$$\tau + \mu + \xi = 0. \tag{30}$$

Substituting τ from (30) to (6), we get

$$0 = \epsilon^2 + \xi + \mu(1 + \mu + m\xi) = \epsilon^2 + \xi - \mu^2. \tag{31}$$

Finally substituting ξ and we can solve for μ in

$$m\mu^2 + 2\mu + (1 - m\epsilon^2) = 0, \tag{32}$$

to get

$$\mu = -\frac{1}{m} \pm \sqrt{\epsilon^2 - \frac{1}{m} + \frac{1}{m^2}}. \tag{33}$$

As $(Y - \mu I)^2 = m\xi(Y - \mu I)$, the eigenvalues of $Y - \mu I$ are 0 with multiplicity $m-1$ and $m\xi$ with multiplicity one, thus Y has eigenvalues μ with multiplicity $m-1$ and $\mu + m\xi$ with multiplicity one. Hence the determinant $\det(I + Y)$ has the form $(1 + \mu)^{m-1}(1 + \mu + m\xi)$. Since $1 + \mu + m\xi = -\mu$ from (27), we get

$$\det(I + Y) = -\mu \cdot (1 + \mu)^{m-1}. \tag{34}$$

But which sign $\pm$ does μ take in equation (33)?

We claim that it must be the $+$ sign.

Denote by $z = \sqrt{\epsilon^2 - \frac{1}{m} + \frac{1}{m^2}}$, then

$$\det(I+Y) = \left(\frac{1}{m} + z\right) \cdot \left(1 - \frac{1}{m} - z\right)^{m-1} \tag{35}$$

if the minus sign $-$ is taken; and

$$\det(I+Y) = \left(\frac{1}{m} - z\right) \cdot \left(1 - \frac{1}{m} + z\right)^{m-1} \tag{36}$$

if the plus sign $+$ is taken. We want to show that the determinant is smaller with the $+$ sign. This will follow if we can show that the following polynomial in z has non-negative coefficients,

$$g(z) = \left(\frac{1}{m} + z\right) \cdot \left(1 - \frac{1}{m} - z\right)^{m-1} - \left(\frac{1}{m} - z\right) \cdot \left(1 - \frac{1}{m} + z\right)^{m-1}. \tag{37}$$

Clearly

$$g(z) = -\left(1 - \frac{1}{m} - z\right)^{m} + \left(1 - \frac{1}{m} - z\right)^{m-1} + \left(1 - \frac{1}{m} + z\right)^{m} - \left(1 - \frac{1}{m} + z\right)^{m-1}. \tag{38}$$

Collecting the coefficients of z^i, we get for even i all terms cancel out, and for odd i,

$$2\binom{m}{i}\left(1 - \frac{1}{m}\right)^{m-i} - 2\binom{m-1}{i}\left(1 - \frac{1}{m}\right)^{m-1-i} \tag{39}$$

$$= 2\left(1 - \frac{1}{m}\right)^{m-1-i}\left[\binom{m}{i}\left(1 - \frac{1}{m}\right) - \binom{m-1}{i}\right], \tag{40}$$

$$= 2\left(1 - \frac{1}{m}\right)^{m-1-i}\left(1 - \frac{1}{i}\right)\binom{m-1}{i-1} \tag{41}$$

which is clearly non-negative (and strictly positive if $i > 1$). We conclude that in order to have minimum determinant, the rank 1 perturbation matrix Y has

$$\mu = -\frac{1}{m} + \sqrt{\epsilon^2 - \frac{1}{m} + \frac{1}{m^2}}. \tag{42}$$

Note that in case $m = 2$ so that there is no odd $i > 1$, we can still assume μ takes the $+$ sign, since in Eqn (34)

$$-\mu \cdot (1+\mu)^{m-1} = \left(\frac{1}{2} + \sqrt{\epsilon^2 - \frac{1}{4}}\right)\left(\frac{1}{2} - \sqrt{\epsilon^2 - \frac{1}{4}}\right) \tag{43}$$

which is completely symmetric.

Also from (27), (28) and (30)

$$\xi = -\frac{1}{m} + \frac{2}{m^2} - \frac{2}{m}\sqrt{\epsilon^2 - \frac{1}{m} + \frac{1}{m^2}}, \tag{44}$$

and

$$\tau = \frac{2}{m} - \frac{2}{m^2} - \left(1 - \frac{2}{m}\right)\sqrt{\epsilon^2 - \frac{1}{m} + \frac{1}{m^2}}. \tag{45}$$

Furthermore the other eigenvalue of Y must be

$$\mu + m\xi = -1 + \frac{1}{m} - \sqrt{\epsilon^2 - \frac{1}{m} + \frac{1}{m^2}}. \tag{46}$$

Referring to Eqn(20), and substituting τ from Eqn (45) we get

$$\begin{aligned} \frac{1}{4} + \epsilon^2 - \tau &= \frac{1}{4} + \epsilon^2 - \frac{2}{m} + \frac{2}{m^2} + \left(1 - \frac{2}{m}\right)\sqrt{\epsilon^2 - \frac{1}{m} + \frac{1}{m^2}} & (47) \\ &= \left[\frac{1}{2} - \frac{1}{m} + \sqrt{\epsilon^2 - \frac{1}{m} + \frac{1}{m^2}}\right]^2 & (48) \end{aligned}$$

It follows that

$$\begin{aligned} \mu_+ &= -\frac{1}{2} + \sqrt{\frac{1}{4} + \epsilon^2 - \tau} & (49) \\ &= -\frac{1}{m} + \sqrt{\epsilon^2 - \frac{1}{m} + \frac{1}{m^2}} & (50) \\ &= \mu & (51) \end{aligned}$$

Hence the μ_+ is μ, the one eigenvalue taken with multiplicity $m-1$. Lemma 2 already asserts this for all $n > 4$. But here we derive it for all blocks of size $m \geq 2$, but only for rank 1 perturbations of a scalar matrix.

Given Y as in Eqn (26), with μ in (42) and ξ in (44), we can verify that each column vector does have 2-norm ϵ.

Set $m = n$, with these choices for μ in (42), ξ in (44), all $\epsilon_j = \pm 1$, and $\epsilon_1 = 1$, we do achieve the determinant in (34). This gives 2^{n-1} distinct perturbation matrices. In particular, taking all $\epsilon_j = 1$, we have the following $n \times n$ matrix

$$X = \begin{pmatrix} -\tau & \xi & \cdots & \xi \\ \xi & -\tau & \cdots & \xi \\ \vdots & \vdots & \ddots & \vdots \\ \xi & \xi & \cdots & -\tau \end{pmatrix} \tag{52}$$

which achieves the determinant as given in (34) (with $m = n$).

4 Full dimensional block $m = n$

Suppose $n \geq 3$. In this section we suppose a full dimensional block Y exists with more than one distinct eigenvalues, as stipulated in Lemma 2. From Section 3 we know that, with $m = n$, Y is given in the form of Eqn (26), and the determinant is given in Eqn (34), where μ is given in Eqn (42).

As $\epsilon < \frac{1}{\sqrt{n}}$, we see that

$$\mu = -\frac{1}{n} + \sqrt{\epsilon^2 - \frac{1}{n} + \frac{1}{n^2}} < 0. \tag{53}$$

Consider the function

$$g(x) = x(1-x)^{n-1}. \tag{54}$$

It is the determinant function $\det(I+Y)$ if we let $x = -\mu > 0$ as a function of ϵ. As ϵ varies from $\sqrt{\frac{1}{n} - \frac{1}{n^2}}$ to $\frac{1}{\sqrt{n}}$, x strictly monotonically varies from $1/n$ down to 0.

Now we view $g(x)$ as a function of x, for $0 \le x \le 1/n$. By differentiation, $g'(x) = (1-x)^{n-2}(1-nx)$, which is positive for the range $0 \le x < 1/n$. Hence $g(x)$ is strictly monotonically increasing (as x increases from 0 to $1/n$), taking values from 0 to $g(1/n) = \frac{1}{n}\left(1 - \frac{1}{n}\right)^{n-1}$ each exactly once.

Our next task is to compare this with the "trivial" bound corresponding to the matrix $-\epsilon I$, i.e., when all the eigenvalues are equal. In this case, the determinant $\det(I+Y)$ is $(1-\epsilon)^n$.

When ϵ increases from $\sqrt{\frac{1}{n} - \frac{1}{n^2}}$ to $\frac{1}{\sqrt{n}}$, both $g(x)$, now viewed as a function of ϵ, and the "trivial" bound $(1-\epsilon)^n$, are strictly monotonically decreasing. We wish to show that there is a unique cross over.

Let $D(x) = g(x) - (1-\epsilon)^n$, where

$$\epsilon = \sqrt{\left(x - \frac{1}{n}\right)^2 + \frac{1}{n} - \frac{1}{n^2}} \tag{55}$$

is now viewed as a function of x, in $0 \le x \le 1/n$.

We would like to show that $D\mid_{x=0} < 0$ and $D\mid_{x=1/n} > 0$, and $D'(x) > 0$ for $0 < x < 1/n$. This implies a unique cross over.

If we differentiate D we have

$$\frac{dD}{dx} = (1-nx)\left[(1-x)^{n-2} - \frac{(1-\epsilon)^{n-1}}{\epsilon}\right]. \tag{56}$$

Clearly in that range

$$(1-x)^{n-2} > \left(1 - \frac{1}{n}\right)^{n-2} \tag{57}$$

and

$$\frac{(1-\epsilon)^{n-1}}{\epsilon} \le \frac{n}{\sqrt{n-1}}\left(1 - \frac{\sqrt{n-1}}{n}\right)^{n-1} \tag{58}$$

as $\epsilon \ge \sqrt{1/n - 1/n^2} = \sqrt{n-1}/n$. Thus to show $D'(x) > 0$ it suffices to show that

$$\left(1 - \frac{1}{n}\right)^{n-1} > \sqrt{n-1}\left(1 - \frac{\sqrt{n-1}}{n}\right)^{n-1}. \tag{59}$$

As $(1+\frac{1}{k})^k$ monotonically increases to e, $(1-\frac{1}{n})^{n-1} = [(1+\frac{1}{n-1})^{n-1}]^{-1}$ monotonically decreases to e^{-1}. In particular on the left hand side of (59)

$$\left(1 - \frac{1}{n}\right)^{n-1} > e^{-1}. \tag{60}$$

On the right hand side of (59), we claim that for all $n \ge 7$,

$$\left(1 - \frac{\sqrt{n-1}}{n}\right)^{n-1} \le e^{-\sqrt{n-1}}. \tag{61}$$

Expanding in Taylor series,

$$\left(1-\frac{\sqrt{n-1}}{n}\right)^{n-1} = e^{(n-1)\cdot[-\frac{\sqrt{n-1}}{n}-\frac{n-1}{2n^2}-\cdots]} \quad (62)$$

$$= e^{-\frac{(n-1)^{3/2}}{n}-\frac{(n-1)^2}{2n^2}-\cdots} \quad (63)$$

where every successive term in the exponent has a negative sign. The claim follows from

$$\frac{(n-1)^{3/2}}{n}+\frac{(n-1)^2}{2n^2} \geq \sqrt{n-1}, \quad (64)$$

for $n \geq 7$, or,

$$\frac{n-1}{n}+\frac{(n-1)^{3/2}}{2n^2} \geq 1. \quad (65)$$

This simplies to the simple polynomial $(n-1)^3 \geq 4n^2$.

Thus for $n \geq 7$,

$$\sqrt{n-1}\left(1-\frac{\sqrt{n-1}}{n}\right)^{n-1} \leq \sqrt{n-1}e^{-\sqrt{n-1}}. \quad (66)$$

The proof for (59) if completed, at least for the cases $n \geq 7$, by observing that for all $x \geq 1$, $e^{-1} \geq \sqrt{x}e^{-\sqrt{x}}$, as the latter function of x has negative derivative for $x \geq 1$.

For the cases $n < 7$, we can verify (59) numerically. Indeed, for $3 \leq n \leq 6$, the inequality is strict.

$D\mid_{x=0} < 0$ is immediate since $g\mid_{x=0} = 0$ and $(1-\epsilon)^n\mid_{x=0} = (1-\epsilon)^n\mid_{\epsilon=\frac{1}{\sqrt{n}}} > 0$.

To show $D\mid_{x=1/n} > 0$ takes a bit more work. We want

$$\frac{1}{n}\left(1-\frac{1}{n}\right)^{n-1} > \left(1-\frac{\sqrt{n-1}}{n}\right)^n \quad (67)$$

From (60), the left hand side of (67) is greater than $\frac{1}{en}$. Also, by Taylor expansion, $\left(1-\frac{\sqrt{n-1}}{n}\right)^n < e^{-\sqrt{n-1}}$, so we need only to show

$$\frac{1}{en} \geq \frac{1}{e^{\sqrt{n-1}}}. \quad (68)$$

This can be shown to be true for all $n \geq 15$. For $3 \leq n \leq 14$, Eqn (67) can be directly verified numerically.

We conclude that there is a unique cross over for the minimization of $g(x)$ and $(1-\epsilon)^n$. In terms of ϵ, between $\sqrt{\frac{1}{n}-\frac{1}{n^2}}$ and $\frac{1}{\sqrt{n}}$, $(1-\epsilon)^n$ is asymptotically $e^{-\sqrt{n}}$. On the other hand, for $0 \leq x \leq 1/n$, $1 \geq (1-x)^{n-1} \geq e^{-1}$ and thus $g(x) = \Theta(x)$. It follows that the cross over happens at around $x = \Theta(e^{-\sqrt{n}})$ asymptotically. In terms of ϵ, this happens at around $\epsilon \approx \frac{1}{\sqrt{n}}(1-\Theta(e^{-\sqrt{n}}))$. One can get a bit more precise. Since from the above it is known that at cross over $x \approx \Theta(e^{-\sqrt{n}})$, then $(1-x)^{n-1} \approx 1$, and $g(x) \approx x$, thus $\epsilon \approx \frac{1}{\sqrt{n}}(1-e^{-\sqrt{n}})$ asymptotically.

Lemma 4 *For all $n \geq 3$, there is a unique cross over point c_n, satisfying $\sqrt{\frac{1}{n} - \frac{1}{n^2}} \leq c_n \leq \frac{1}{\sqrt{n}}$, such that*

$$(1-\epsilon)^n < x(1-x)^{n-1} \tag{69}$$

for $\sqrt{\frac{1}{n} - \frac{1}{n^2}} \leq \epsilon < c_n$, and

$$(1-\epsilon)^n > x(1-x)^{n-1} \tag{70}$$

for $c_n < \epsilon \leq \frac{1}{\sqrt{n}}$. where $x = \frac{1}{n} = \sqrt{\epsilon^2 - \frac{1}{n} + \frac{1}{n^2}}$ Moreover, c_n is asymptotically $\frac{1}{\sqrt{n}}(1 - e^{-\sqrt{n}})$.

5 Can minimum be achieved with $m = n - 1$?

Let $n \geq 3$. Let us suppose there is a co-1 dimensional block Y, which has more than one distinct eigenvalues as stipulated in Lemma (2), that achieves minimum volume. Of course the left over 1-dimensional block must contribute $1 - \epsilon$ to the volume, and the total determinant is given as $(1-\epsilon)y(1-y)^{m-1}$, where $m = n - 1$, and y is given as follows

$$y = \frac{1}{m} - \sqrt{\epsilon^2 - \frac{1}{m} + \frac{1}{m^2}}. \tag{71}$$

ϵ satisfies the global constraint that $\epsilon \leq 1/\sqrt{n}$. Furthermore, in order that the eigenvalues of Y be real, we must further restrict $\epsilon \geq \sqrt{\frac{1}{m} - \frac{1}{m^2}}$. In the following, we will denote by ℓ and r the left and the right end points of this interval,

$$\ell = \sqrt{\frac{1}{n-1} - \frac{1}{(n-1)^2}}, \tag{72}$$

$$r = \frac{1}{\sqrt{n}}. \tag{73}$$

Note that $r > \ell$ since $r^2 - \ell^2 = \frac{1}{n(n-1)^2}$.

We want to compare $(1-\epsilon)y(1-y)^{n-2}$ with $x(1-x)^{n-1}$, the possible minimum volumes corresponding to a full dimensional block versus a co-1 dimensional block together with an extra one dimensional block. The common interval of definition is $[\ell, r]$, as the interval for the n-dimensional case is $[\sqrt{\frac{1}{n} - \frac{1}{n^2}}, \frac{1}{\sqrt{n}}]$ and its left most most point $\sqrt{\frac{1}{n} - \frac{1}{n^2}} < \ell$, for all $n \geq 3$.

Define

$$F_n(\epsilon) = x(1-x)^{n-1} \tag{74}$$

$$= \left(\frac{1}{n} - \sqrt{\epsilon^2 - \frac{1}{n} + \frac{1}{n^2}}\right)\left(1 - \frac{1}{n} + \sqrt{\epsilon^2 - \frac{1}{n} + \frac{1}{n^2}}\right)^{n-1} \tag{75}$$

and

$$\widehat{F}_n(\epsilon) = (1-\epsilon)y(1-y)^{n-2} \tag{76}$$

$$= (1-\epsilon)\left(\frac{1}{m} - \sqrt{\epsilon^2 - \frac{1}{m} + \frac{1}{m^2}}\right)\left(1 - \frac{1}{m} + \sqrt{\epsilon^2 - \frac{1}{m} + \frac{1}{m^2}}\right)^{m-1} \tag{77}$$

where $m = n - 1$.

From what's proved in the last section, both F_n and $\widehat{F}_n$ are strictly monotonically decreasing in ϵ. We want to show that for any $\epsilon \in [\ell, r]$,

$$F_n(\epsilon) < \widehat{F}_n(\epsilon). \tag{78}$$

Our strategy is to show that the end points of the interval satisfy

$$F_n(\ell) < \widehat{F}_n(r), \tag{79}$$

from which it follows that $\forall \epsilon \in [\ell, r]$,

$$F_n(\epsilon) \le F_n(\ell) < \widehat{F}_n(r) \le \widehat{F}_n(\epsilon). \tag{80}$$

Our strategy works for all $n \ge 4$, and the inequality (78) for the special case $n = 3$ will be proved separately in the Appendix.

At the left end $\epsilon = \ell$, we estimate $\sqrt{\epsilon^2 - \frac{1}{n} + \frac{1}{n^2}} = \frac{\sqrt{n^2-3n+1}}{n(n-1)} < \frac{1}{n}$. Thus, in $F_n(\ell)$ one factor

$$1 - \frac{1}{n} + \sqrt{\epsilon^2 - \frac{1}{n} + \frac{1}{n^2}} < 1. \tag{81}$$

Also, it is trivial to verify for $n \ge 5$,

$$\frac{\sqrt{n^2 - 3n + 1}}{n-1} > \frac{n-1}{n}, \tag{82}$$

thus the other factor

$$\frac{1}{n} - \sqrt{\epsilon^2 - \frac{1}{n} + \frac{1}{n^2}} < \frac{1}{n} - \frac{1}{n}\left(1 - \frac{1}{n}\right) = \frac{1}{n^2}. \tag{83}$$

We arrive at the upper bound for all $n \ge 5$,

$$F_n(\ell) < \frac{1}{n^2}. \tag{84}$$

At the right end $\epsilon = r$, $\sqrt{\epsilon^2 - \frac{1}{n-1} + \frac{1}{(n-1)^2}} = \frac{1}{(n-1)\sqrt{n}}$. Hence

$$\widehat{F}_n(r) = \frac{1}{n-1}\left(1 - \frac{1}{\sqrt{n}}\right)^2 \left(1 - \frac{1}{n-1} + \frac{1}{(n-1)\sqrt{n}}\right)^{n-2}. \tag{85}$$

We know from (60) that $(1 - 1/k)^{k-1} > e^{-1}$, it follows that

$$\left(1 - \frac{1}{n-1} + \frac{1}{(n-1)\sqrt{n}}\right)^{n-2} > \left(1 - \frac{1}{n-1}\right)^{n-2} > \frac{1}{e}. \tag{86}$$

Hence,

$$\widehat{F}_n(r) > \left(1 - \frac{1}{\sqrt{n}}\right)^2 \frac{1}{e(n-1)}. \tag{87}$$

Thus it all comes down to checking

$$\left(1 - \frac{1}{\sqrt{n}}\right)^2 \ge \frac{e}{n}\left(1 - \frac{1}{n}\right). \tag{88}$$

It is obvious that this is true asymptotically. But in fact, the left hand side is monotonically increasing and the right hand side is monotonically decreasing, and we can directly check that the inequality hold for $n = 7$ and thus for all $n \geq 7$.

Finally for the values $n = 4, 5, 6$, one can directly check that $F_n(\ell) \leq \widehat{F}_n(r)$. Thus it holds for all $n \geq 4$.

For the special case $n = 3$, unfortunately $F_n(\ell) > \widehat{F}_n(r)$. But we can nonetheless prove that for all $\epsilon \in [1/2, 1/\sqrt{3}]$, that pointwise $F_n(\epsilon) < \widehat{F}_n(\epsilon)$. The details are given in the Appendix.

Lemma 5 *For all $n \geq 3$, the possibility of an $m = n - 1$ dimensional block with more than one eigenvalues together with an additional one dimensional block never produces a smaller volume than the corresponding n dimensional block with more than one eigenvalues, for the common interval of respective definitions.*

6 Putting it all together

To put all this information together, we note that for $n > 4$ we already have enough to prove Theorem 2.

As noted already in Micciancio's theorem the case $\epsilon < \sqrt{\frac{1}{n} - \frac{1}{n^2}}$ has the unique minimizing $X = -\epsilon I$ and $f_n(\epsilon) = (1 - \epsilon)^n$. More generally a minimizing block Y is unique, $Y = -\epsilon I$, if it has only one eigenvalue (hence a scalar matrix).

Suppose $\sqrt{\frac{1}{n} - \frac{1}{n^2}} \leq \epsilon \leq \frac{1}{\sqrt{n}}$, and suppose $n > 4$. Then by Lemma 2 and Lemma 3 a minimizing X has at most one block which is non-scalar, and if it exists, it's unique and its dimension is either n or $n - 1$. Moreover, by Lemma 2 the characterization of such a block from Section 3 applies. Hence the only competing minimizing determinants $\det(I+Y)$ take the form $(1-\epsilon)^n$, or $x(1-x)^{n-1}$ or $(1 - \epsilon)y(1 - y)^{m-1}$, where $m = n - 1$, and x and y are as given in Section 4 and 5.

As shown there, $(1 - \epsilon)y(1 - y)^{m-1}$ in fact is always greater than $x(1 - x)^{n-1}$. Moreover there is a unique cross over between $(1 - \epsilon)^n$ and $x(1 - x)^{n-1}$. This completes the proof for all $n > 4$.

Finally we deal with all possible cases where the dimension $n \leq 4$.

The case $n = 1$ is trivial. By (14) $x(1 - x)^{n-1} = 1 - \epsilon$ in this case.

Let $n = 2$. Then the expression for $x(1 - x)^{n-1}$ evaluates to $1/2 - \epsilon^2$. Note that $(1 - \epsilon)^2 - (1/2 - \epsilon^2) = 2(1/2 - \epsilon)^2 \geq 0$, and strictly so for all $\epsilon \neq \frac{1}{2}$. Thus in this case, $x(1 - x)^{n-1}$ is the minimum through out the interval $[\sqrt{\frac{1}{n} - \frac{1}{n^2}}, \frac{1}{\sqrt{n}}] = [1/2, 1/\sqrt{2}]$. In other words, the cross over happened immediately at the left most point of the interval.

Let $n = 3$. If there are no block with more than one eigenvalues, then the minimum volume is $(1 - \epsilon)^3$. Suppose there is such a block, which of course must be of dimension either 2 or 3. The case of $m = 2 = n - 1$ with $(1 - \epsilon) \cdot (1/2 - \epsilon^2)$ can be dismissed by Section 5 as inferior to the $m = n = 3$ case with volume $x(1 - x)^{n-1} = (1/3 - \sqrt{\epsilon^2 - 2/9})(2/3 + \sqrt{\epsilon^2 - 2/9})^2$, (even though $(1-\epsilon) \cdot (1/2-\epsilon^2)$ is better than $(1-\epsilon)^3$ throughout the common domain of definition $[1/2, 1/\sqrt{3}]$.)

Now Lemma 4 applies, and we conclude that Theorem 2 holds. The cross over happens in this case ($n = 3$) between $\sqrt{2}/3$ and $1/2$.

Let $n = 4$. If there are no block with more than one eigenvalues, then the minimum is $(1 - \epsilon)^4$. Suppose there is such a block. If this block size is 4, then we have the competing volume $x(1 - x)^3$ as before, which would have a unique cross over. From Lemma 5 we can dismiss the possibility of block size 3. This leaves the possibility of $m = 2$. Referring to $\mu_\pm$ in Eqn (20) this block must have minimum volume $(1/2 - \sqrt{1/4 + \epsilon^2 - \tau})(1/2 + \sqrt{1/4 + \epsilon^2 - \tau})$. Taking trace, $-2\tau = -1$ and $\tau = 1/2$. Substituting back we get $(1/2 - \sqrt{\epsilon^2 - 1/4})(1/2 + \sqrt{\epsilon^2 - 1/4}) = 1/2 - \epsilon^2$. This would

have been smaller than $(1-\epsilon)^2$ except in order to be a real number, $\epsilon \geq 1/2$. But here $n=4$ and we are required to have $\epsilon \leq 1/2$, and at $\epsilon = 1/2$, $f_4(1/2) = 0$. Thus this case can be dismissed. This completes the proof of Theorem 2

Appendix: $n = 3$

We complete the proof of Lemma 5 for $n = 3$. We have

$$\begin{aligned} F_3(\epsilon) &= x(1-x)^2 && (89)\\ &= \left(\frac{1}{3} - \sqrt{\epsilon^2 - \frac{2}{9}}\right)\left(\frac{2}{3} + \sqrt{\epsilon^2 - \frac{2}{9}}\right)^2 && (90)\\ &= \frac{10}{27} - \epsilon^2 - \left(\epsilon^2 - \frac{2}{9}\right)^{3/2} && (91) \end{aligned}$$

for $\frac{\sqrt{2}}{3} \leq \epsilon \leq \frac{1}{\sqrt{3}}$, where as

$$\begin{aligned} \widehat{F}_3(\epsilon) &= (1-\epsilon)y(1-y) && (92)\\ &= (1-\epsilon)\left(\frac{1}{2} - \sqrt{\epsilon^2 - \frac{1}{4}}\right)\left(\frac{1}{2} + \sqrt{\epsilon^2 - \frac{1}{4}}\right) && (93)\\ &= (1-\epsilon)\left(\frac{1}{2} - \epsilon^2\right) && (94) \end{aligned}$$

for $\frac{1}{2} \leq \epsilon \leq \frac{1}{\sqrt{3}}$. Note that $\frac{1}{2} \leq \epsilon \leq \frac{1}{\sqrt{2}}$ could have been the interval of definition for $y(1-y)$ corresponding to the 2 dimensional block. but this must be further restricted by the global constraint $\epsilon \leq \frac{1}{\sqrt{3}}$ in dimension 3. Also $\frac{1}{2} \leq \epsilon$ is necessary in order to have real eigenvalues for the 2 dimensional block.

We now show that in the common interval of definition, $\forall \epsilon \in [\ell, r] = [\frac{1}{2}, \frac{1}{\sqrt{3}}]$,

$$F_3(\epsilon) < \widehat{F}_3(\epsilon) \tag{95}$$

pointwise.

This is equivalent to

$$\frac{10}{27} - \epsilon^2 - (1-\epsilon)\left(\frac{1}{2} - \epsilon^2\right) < \left(\epsilon^2 - \frac{2}{9}\right)^{3/2}, \tag{96}$$

The left hand side is $\frac{\epsilon}{2} - \epsilon^3 - \frac{7}{54}$. By taking squares both sides and collecting terms, Eqn (96) is *implied* by,

$$f(\epsilon) = -\frac{1}{3}\epsilon^4 + \frac{7}{27}\epsilon^3 + \frac{11}{108}\epsilon^2 - \frac{7}{54}\epsilon + \frac{1}{36} < 0. \tag{97}$$

We start differentiate f.

$$f'(\epsilon) = -\frac{4}{3}\epsilon^3 + \frac{7}{9}\epsilon^2 + \frac{11}{54}\epsilon - \frac{7}{54} \tag{98}$$

$$f''(\epsilon) = -4\epsilon^2 + \frac{14}{9}\epsilon + \frac{11}{54} \tag{99}$$

$$f'''(\epsilon) = -8\epsilon + \frac{14}{9} \tag{100}$$

$$f''''(\epsilon) = -8 < 0. \tag{101}$$

Thus, f''' is strictly monotonically decreasing and takes its maximum over the interval $[1/2, 1/\sqrt{3}]$ at

$$f'''(1/2) = -4 + \frac{14}{9} < 0. \tag{102}$$

So similarly f'' is strictly monotonically decreasing over the interval and takes its maximum at

$$f''(1/2) = -1 + \frac{7}{9} + \frac{11}{54} = \frac{-1}{54} < 0. \tag{103}$$

It follows that f' is strictly monotonically decreasing over the interval and takes its maximum at

$$f'(1/2) = -\frac{1}{2 \cdot 3} + \frac{7}{2^2 \cdot 3^2} + \frac{11}{2^2 \cdot 3^3} - \frac{7}{2 \cdot 3^3} = \frac{-2 \cdot 3^2 + 7 \cdot 3 + 11 - 7 \cdot 2}{2^2 \cdot 3^3} = 0. \tag{104}$$

Thus, for all $\epsilon \in (1/2, 1/\sqrt{3}]$, $f'(\epsilon) < 0$ and therefore $f(\epsilon)$ is strictly monotonically decreasing over the interval and takes its maximum at

$$f(1/2) = \frac{-3^2 + 7 \cdot 2 + 11 - 7 \cdot 2^2 + 3 \cdot 2^2}{2^4 \cdot 3^3} = 0. \tag{105}$$

Finally we conclude that $\forall \epsilon \in (1/2, 1/\sqrt{3}]$, $f(\epsilon) < 0$.
In fact at $1/2$ it is also true that $F_3(\epsilon) < \widehat{F}_3(\epsilon)$: [1]

$$F_3(1/2) = \frac{25}{2^3 \cdot 3^3} < \widehat{F}_3(1/2) = \frac{1}{8}. \tag{106}$$

References

[1] M. Ajtai. Generating hard instances of lattice problems. In *Proc. 28th Annual ACM Symposium on the Theory of Computing*, 1996. Full version available from ECCC, *Electronic Colloquium on Computational Complexity* TR96-007, at `http://www.eccc.uni-trier.de/eccc/`.

[2] Jin-Yi Cai. Some Recent Progress on the Complexity of Lattice Problems.
Plenary Talk. In the Proceedings of *The 14th Annual IEEE Conference on Computational Complexity*, 158–177, 1999.

[3] J-Y. Cai and A. Nerurkar. An Improved Worst-Case to Average-Case Connection for Lattice Problems.
In *Proc. 38th IEEE Symposium on Foundations of Computer Science (FOCS)*, 1997, 468–477.

[4] Daniele Micciancio. Minimal volume of almost cubic parallelepipeds.
Manuscript. To appear.

[1] There is no inconsistency, even though $f(1/2) = 0$. Recall that $f(\epsilon) < 0$ is a *sufficient condition* for $F_3(\epsilon) < \widehat{F}_3(\epsilon)$. What happened is that even though at $1/2$, $F_3(\epsilon) < \widehat{F}_3(\epsilon)$, the squaring in Eqn (96) produced a square of a negative term, and results in an equality.