A Conjecture on Hermite Constants

Leon Mächler and David Naccache

ÉNS (DI), ISG, CNRS, PSL Research University, Paris, France.
leon-philipp.machler@ens.fr, david.naccache@ens.fr

Abstract. As of today, the Hermite constants γ_n are only known for $n \in \{1, 2, 3, 4, 5, 6, 7, 8, 24\}$.

We noted that the known values of $(4/\gamma_n)^n$ coincide with the values of the minimal determinants of any n-dimensional integral lattice when the length of the smallest lattice element μ is fixed to 4.

Based on this observation, we conjecture that the values of γ_n^n for $n = 9, \ldots, 23$ are those given in Table 2.

We provide a supporting argument to back this conjecture. We also provide a provable lower bound on the Hermite constants for $1 \le n \le 24$.

1 The Observation

Hermite constants γ_n determine how short a lattice element can be. γ_n is defined as follows: Let $\mathcal{L}$ be a lattice in Euclidean space $\mathbb{R}^n$ with unit co-volume. Denoting by λ_1 the minimal length of a nonzero element of $\mathcal{L}$ we denote by $\sqrt{\gamma_n}$ the maximal value of λ_1 over all such lattices $\mathcal{L}$. Table 1 gives all known values of γ_n^n:

n	1	2	3	4	5	6	7	8	9...23	24
γ_n^n	1	$\frac{4}{3}$	2	4	8	$\frac{64}{3}$	64	2^8	?	2^{48}

Table 1. All known values of γ_n^n

During the implementation of post-quantum encryption algorithms, we noted that the eight ratios between the first known Hermite constant values and 2^n coincide with the values $\alpha_{2,n}$ of the minimal determinants of any n-dimensional integral lattice when we fix the length of the smallest lattice element to $\mu = 2$. Because this coincidence does not hold for $n = 24$ we further investigated what happens for higher μ values.

It turns out that <u>all</u> 9 known values of $(2/\gamma_n)^n$ coincide with $\alpha_{4,n}$, which is the equivalent of $\alpha_{2,n}$ when $\mu = 4$. The quantities $\alpha_{\mu,n}$ are known for $\mu \in \{2, 3, 4\}, n \ge 0$ [CS99] and are lattice-related, which makes the following conjecture reasonably likely:

Conjecture 1. For $1 \leq n \leq 24$:

$$\gamma_n^n = \frac{4^n}{\alpha_{4,n}}$$

where $\alpha_{4,n}$ is the minimal determinant of any n-dimensional 4-norm integral lattice.

If Conjecture 1 is true then the values of γ_n^n for $n = 9, \ldots, 23$ would be those given in green in Table 2.

In addition, our estimates coincide with two other values for $n = 9, 10$ given (with an apparently incomplete proof [Cox47]) in [Cha46].

n	$\alpha_{2,n}$	$\alpha_{4,n}$	2^n	4^n	$2^n/\alpha_{2,n}$	$4^n/\alpha_{4,n}$	γ_n^n
1	2	4	2^1	4^1	2^0	2^0	2^0
2	3	12	2^2	4^2	$2^2/3$	$2^2/3$	$2^2/3$
3	4	32	2^3	4^3	2^1	2^1	2^1
4	4	64	2^4	4^4	2^2	2^2	2^2
5	4	128	2^5	4^5	2^3	2^3	2^3
6	3	192	2^6	4^6	$2^6/3$	$2^6/3$	$2^6/3$
7	2	256	2^7	4^7	2^6	2^6	2^6
8	1	256	2^8	4^8	2^8	2^8	2^8
9	2	512	2^9	4^9	2^8	2^9	2^9
10	3	768	2^{10}	4^{10}	$2^{10}/3$	$2^{12}/3$	$2^{12}/3$
11	2	972	2^{11}	4^{11}	2^{10}	$2^{20}/3^5$	?
12	1	729	2^{12}	4^{12}	2^{12}	$2^{24}/3^6$	?
13	2	972	2^{13}	4^{13}	2^{12}	$2^{24}/3^5$	?
14	1	768	2^{14}	4^{14}	2^{14}	$2^{20}/3$	?
15	1	512	2^{15}	4^{15}	2^{15}	2^{21}	?
16	1	256	2^{16}	4^{16}	2^{16}	2^{24}	?
17	1	256	2^{17}	4^{17}	2^{17}	2^{26}	?
18	1	192	2^{18}	4^{18}	2^{18}	$2^{30}/3$	?
19	1	128	2^{19}	4^{19}	2^{19}	2^{31}	?
20	1	64	2^{20}	4^{20}	2^{20}	2^{34}	?
21	1	32	2^{21}	4^{21}	2^{21}	2^{37}	?
22	1	12	2^{22}	4^{22}	2^{22}	$2^{42}/3$	?
23	1	4	2^{23}	4^{23}	2^{23}	2^{44}	?
24	1	1	2^{24}	4^{24}	2^{24}	2^{48}	2^{48}

Table 2. Values of $\gamma_n^n, \alpha_{2,n}, \alpha_{4,n}$, the coinciding values are shown in blue and the mismatch for $\mu = 2$ is shown in red. The two values of [Cha46] are shown in magenta. The conjectured values are given in green.

The observation fits with the best known bounds of γ_n [WCW19] but those bounds are so crude that this does not seem to be an indication in either direction. Namely:

$$\frac{n}{2\pi e} < \gamma_n < \frac{n}{8.5} + 2 \text{ and indeed } \frac{n}{2\pi e} < \frac{4}{\sqrt[n]{\alpha_{4,n}}} < \frac{n}{8.5} + 2 \quad \text{for} \quad 1 \leq n \leq 24$$

2 Motivation

The outline of our reasoning is the following: we depart from the observation that the problem of computing Hermite constants and the problem of computing smallest determinants are equivalent. However, to our knowledge solutions to the smallest determinant problem are only known for integral lattices and $\mu = 2, 3, 4$.

We conjecture that the two problems are still equivalent even when one restricts the minimal determinant problem to even integral lattices. First we restate some well known definitions.

Definition 1 (Hermite function). *Let $\mathcal{L}_n$ be the set of all lattices with dimension n and $L \in \mathcal{L}_n$. The Hermite function is defined as:*

$$\gamma(L) = \frac{\mu}{\det(L)^{\frac{1}{n}}}$$

where $\mu = \min(L)$ is the length of the smallest nonzero element of L.

A simple property of the Hermite function is the invariance under scaling.

Theorem 1 (Invariance under scaling). *Let $c \in \mathbb{R}_{>0}$ and $\gamma(L)$ be the Hermite function. It holds that:*

$$\gamma(cL) = \gamma(L)$$

Proof. This follows directly from the definition of the Hermite function. □

Definition 2 (Hermite constant). *Let $\mathcal{L}_n$ be the set of all lattices with dimension n and $L \in \mathcal{L}_n$. The Hermite constant γ_n is defined as:*

$$\gamma_n = \sup\{\gamma(L) | L \in \mathcal{L}_n\}$$

We now have all the necessary definitions and theorems but let us first give the intuition behind the equivalence theorem. To find a Hermite constant γ_n, imagine that one starts with an arbitrary $L \in \mathcal{L}_n$ with:

$$\gamma(L) = \frac{\mu}{\det(L)^{\frac{1}{n}}}$$

The goal is now to modify L in a way that increases $\gamma(L)$ up to γ_n. Clearly, this can only be achieved by increasing μ or by decreasing $\det(L)$.

From the invariance under scaling we know that it is allowed to either fix $\det(L)$ and increase μ or fix μ and decrease $\det(L)$, one can always scale up or down in the end. Note that both approaches solve the same problem: maximizing the ratio. Solutions to both problems are thus equivalent. More formally:

Definition 3 **(L_1, L_2, L_3).** *Given the set $\mathcal{L}_n$ of all lattices with dimension $n \in \mathbb{N}$. Let $L_1 \in \mathcal{L}_n$ be:*

$$L_1 = \arg\max_L \frac{\min(L)}{\det(L)^{\frac{1}{n}}}$$

Let $L_2 \in \mathcal{L}_n$ be:

$$L_2 = \underset{L}{\operatorname{argmax}} \frac{1}{\det(L)^{\frac{1}{n}}}$$

Let $L_3 \in \mathcal{L}_n$ be:

$$L_3 = \underset{L}{\operatorname{argmax}} \min(L)$$

where again $\min(L) = \mu$ is the length of the smallest nonzero element of L.

Theorem 2 (Equivalence). *Let $\mathcal{L}_n$ be the set of all lattices of dimension n, $\gamma(L)$ be the Hermite function, γ_n the Hermite constant of dimension n and L_1, L_2 and L_3 be defined as above. It holds that:*

$$\gamma_n = \gamma(L_1) = \gamma(L_2) = \gamma(L_3)$$

Proof. This follows directly from Theorem 1. □

2.1 The problem of integral lattices

The question remains why the sequences calculated from $\alpha_{2,n}$ and $\alpha_{4,n}$ differ for $n \geq 9$. This follows from the fact that the values of $\alpha_{\mu,n}$ were computed with the restriction to integral lattices. This means that the determinant cannot get smaller than 1. Now a problem arises when μ is fixed and $\det(L) = 1$. Under such circumstances we can no longer decrease $\det(L)$ and μ is fixed so the only scaling comes from the dimension (the root in the denominator).

This explains perfectly why $\frac{2^n}{\alpha_{2,n}}$ works until $n = 8$ but not after. Because for $n = 8$ we hit $\det(L) = 1$. This also suggests that the results we obtained for $\frac{4^n}{\alpha_{4,n}}$ are only optimal until $n = 24$, but also gives good reason to conjecture that until then they are in fact optimal. More importantly, this gives an indication how to find the next Hermite constants for $n > 24$: solve the problem of the minimal determinant of n dimensional lattices with a bigger μ. Whether μ needs to be a power of two or just even is unclear. To be safe we choose even. This in turn allows us to formulate the more general conjecture:

Conjecture 2. For any $n \geq 0$:

$$\gamma_n^n = \frac{\mu^n}{\alpha_{\mu,n}}$$

where $\alpha_{\mu,n}$ is the minimal determinant of any n-dimensional μ-norm integral lattice and μ is even and chosen big enough.

2.2 Lower bound on γ_n

If in fact it should turn out that neither Conjecture 1 nor 2 are true we note that the values from our observation still provide a provable lower bound on the Hermite constants for $1 \leq n \leq 24$.

An open question: It is clear that the restriction to integral lattices in the calculation of the $\alpha_{\mu,n}$ will lead to problems when the determinant reaches its minimum. It can also be seen that the approach doesn't work for $\mu = 3$. We think that this also follows from this restriction to integral lattices. The question remains why this restriction does not lead to other problems and non-optimal solutions for the even/power-of-two lattices before the determinant limit is reached. In our reasoning the restriction to integral lattices is not needed but to our knowledge only solutions to the restricted problem are known.

Additional observations: Note that all known and conjectured Hermite constants up to γ_{24}^{24} can be written as a power of 2 that is sometimes divided by a power of three. We denote this as

$$\frac{4^n}{\alpha_{4,n}} = \frac{2^{v_n}}{3^{u_n}}$$

These powers feature a symmetry in value and position if we start from $n = 0$, see Table 3. This can be written as:

$$\gamma_{24-n}^{24-n} = 2^{48-4n}\gamma_n^n \text{ for } 1 \leq n \leq 24$$

Given that there is a symmetry around element $n = 12$, it might be possible that this symmetry is further preserved after $n = 24$ in a way unknown so far, thereby revealing more information on higher value Hermite constants.

We also note that v_n and u_n are linked. Figures 3 and 4 show the line $y = 24-2n$ and the functions $u_n - kv_n - \lfloor n^2/8 \rfloor$ for $k = 1, 2$.

It is worthy noting that $\lfloor n^2/8 \rfloor$ behavior is also deeply hidden in Table I page 594 of [CS82]. We first noticed that $2^n\lambda_{24+n} = \lambda_n$ for $n = 0, \ldots, 23$. Then defining

$$\frac{4^{n-24}}{\lambda_n} = \frac{2^{u'_n}}{3^{v'_n}} \text{ for } n = 25, \ldots, 47$$

we noted that $v'_n = 1$ when $n \bmod 4 = 2$ and that $f(n) = u'_n + 2v'_n - \lfloor \frac{(n-24)^2}{8} \rfloor$ presents three perfect linear regularities shown in Figure 2.

This provides a direct way to compute λ_n that contrasts with the misaligned points at coordinates $x = 11, 12, 13$ in Figure 4. This direct formula for λ_n, valid for $n = 0, \ldots, 47$, is:

n	u_n	$2n-v_n$
0		
1		2
2	1	2
3		5
4		6
5		7
6	1	6
7		8
8		8
9		9
10	1	8
11	5	2
12	6	
13	5	2
14	1	8
15		9
16		8
17		8
18	1	6
19		7
20		6
21		5
22	1	2
23		2
24		

Table 3. Symmetry in the powers of 2 and 3 in $4^n/\alpha_{4,n}$.

$$\lambda_n = \left(\frac{3}{4}\right)^{\left\lfloor \frac{n+1 \bmod 4}{3} \right\rfloor} \times 2^{(4-|12-\bar{n}|)\left\lceil \frac{\lfloor 64^{-\cos(\frac{n\pi}{12})-\frac{1}{2}} - 12 \rfloor}{12} \right\rceil - \left\lfloor \frac{(\bar{n}-8)^2}{8} \right\rfloor - n\left\lfloor \frac{n}{24} - 1 \right\rfloor}$$

where $\bar{n} = n \bmod 24$.

A similar plateau appears in lattice K_n (Table II, page 601 of [CS82]) as shown in Figure 1 where u''_n and v''_n denote the powers of 2 and 3 found in κ_n.

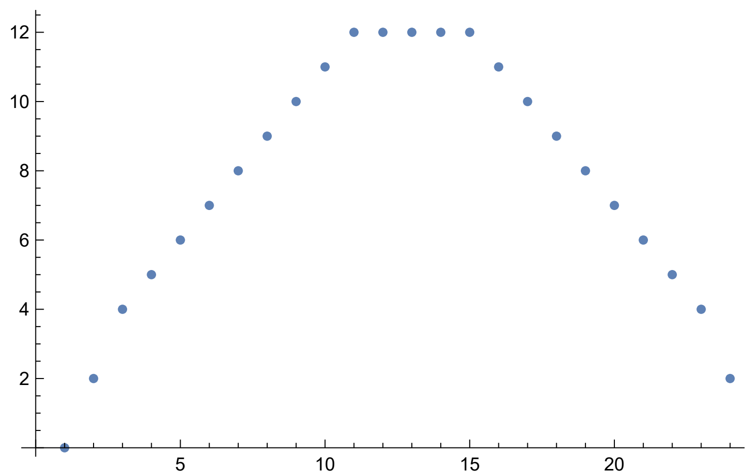

Fig. 1. $f''(n) = u''_n + 2v''_n$ for $n = 1, \ldots, 24$.

References

[Cha46] T.W. Chaundy. "The arithmetic minima of positive quadratic forms. I". English. In: *Q. J. Math., Oxf. Ser.* 17 (1946), pp. 166–192. ISSN: 0033-5606. DOI: 10.1093/qmath/os-17.1.166.

[Cox47] H.S.M. Coxeter. In: *Mathematical Reviews 1947-03* 8 (3 1947), p. 137. URL: https://archive.org/details/sim_mathematical-reviews_1947-03_8_3/page/136/mode/2up?view=theater.

[CS82] J.H. Conway and N.J.A. Sloane. "Laminated Lattices". In: *Annals of Mathematics* 116.3 (1982), pp. 593–620. DOI: 10.2307/2007025.

[CS99] J.H. Conway and N.J.A. Sloane. *Sphere Packings, Lattices and Groups*. Springer New York, 1999. DOI: 10.1007/978-1-4757-6568-7. URL: https://doi.org/10.1007/978-1-4757-6568-7.

[WCW19] Jinming Wen, Xiao-Wen Chang, and Jian Weng. *Improved Upper Bounds on the Hermite and KZ Constants*. 2019. DOI: 10.48550/ARXIV.1904.09395. URL: https://arxiv.org/abs/1904.09395.

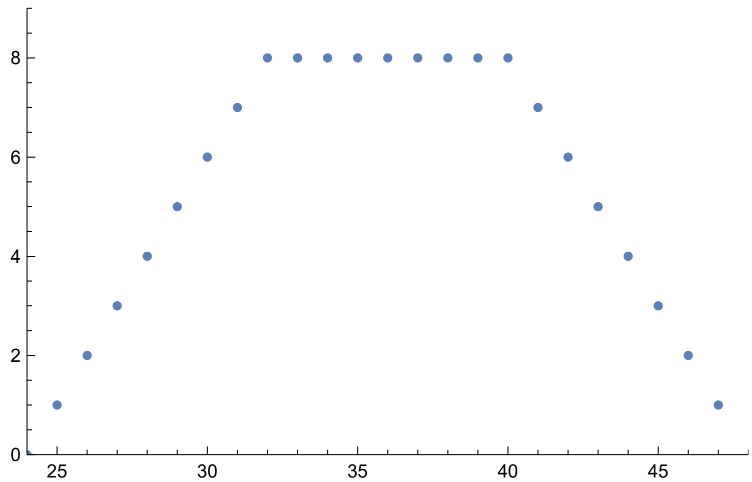

Fig. 2. $f'(n) = u'_n + 2v'_n - \lfloor \frac{(n-24)^2}{8} \rfloor$ for $n = 25, \ldots, 47$.

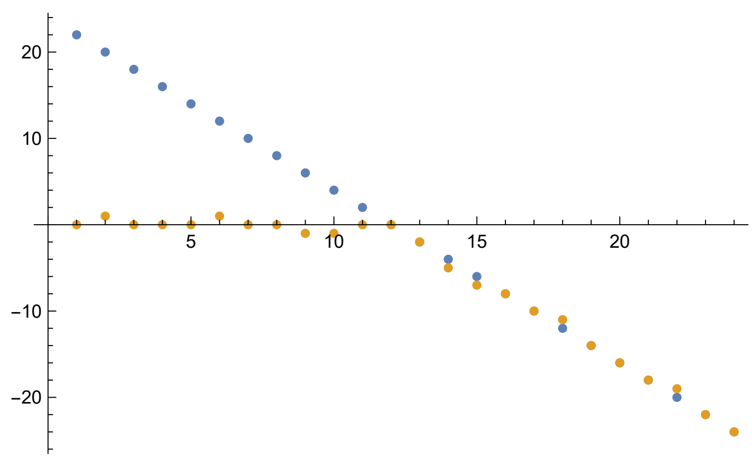

Fig. 3. $y = 24 - 2n$ and $u_n - v_n - \lfloor n^2/8 \rfloor$.

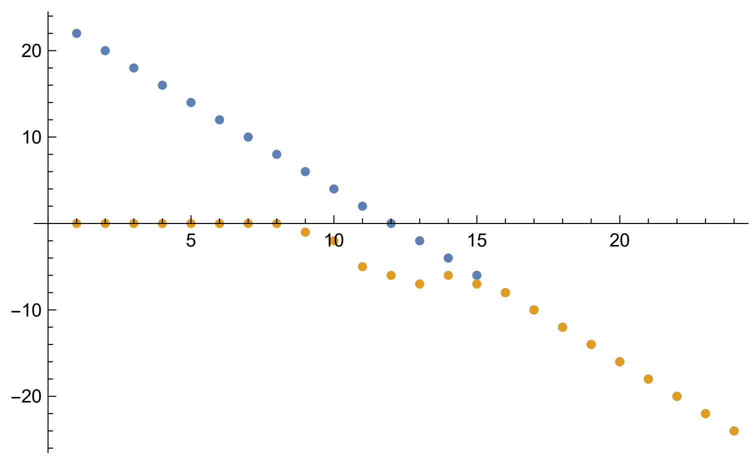

Fig. 4. $y = 24 - 2n$ and $u_n - 2v_n - \lfloor n^2/8 \rfloor$.