POLITECNICO DI TORINO
Repository ISTITUZIONALE

On the condition number of the Vandermonde matrix of the nth cyclotomic polynomial

Original
On the condition number of the Vandermonde matrix of the nth cyclotomic polynomial / Di Scala, Antonio J.; Sanna, Carlo; Signorini, Edoardo. - In: JOURNAL OF MATHEMATICAL CRYPTOLOGY. - ISSN 1862-2976. - STAMPA. - 15:1(2021), pp. 174-178. [10.1515/jmc-2020-0009]

Availability:
This version is available at: 11583/2854092 since: 2020-12-16T09:54:31Z

Publisher:
de Gruyter

Published
DOI:10.1515/jmc-2020-0009

Terms of use:

This article is made available under terms and conditions as specified in the corresponding bibliographic description in the repository

Publisher copyright

(Article begins on next page)

11 December 2023

Research Article

Antonio J. Di Scala, Carlo Sanna*, and Edoardo Signorini

On the condition number of the Vandermonde matrix of the nth cyclotomic polynomial

https://doi.org/10.1515/jmc-2020-0009
Received Mar 01, 2020; accepted May 06, 2020

Abstract: Recently, Blanco-Chacón proved the equivalence between the Ring Learning With Errors and Polynomial Learning With Errors problems for some families of cyclotomic number fields by giving some upper bounds for the condition number $\mathrm{Cond}(V_n)$ of the Vandermonde matrix V_n associated to the nth cyclotomic polynomial. We prove some results on the singular values of V_n and, in particular, we determine $\mathrm{Cond}(V_n)$ for $n = 2^k p^\ell$, where $k, \ell \geq 0$ are integers and p is an odd prime number.

Keywords: cyclotomic polynomial; Vandermonde matrix; condition number; RLWE; PLWE

2010 Mathematics Subject Classification: Primary: 11C99, Secondary: 15A12, 15B05

1 Introduction

Ring Learning With Errors (RLWE) was introduced by Lyubashevsky, Peikert, and Regev [1] in order to speed up cryptographic constructions based on the Learning With Errors problem [2]. Before RLWE, Stehlé, Steinfeld, Tanaka, and Xagawa [3] introduced what is now known as Polynomial Ring Learning With Errors (PLWE). The equivalence between RLWE and PLWE is studied and proved for certain families of polynomials [4, 5]. Let $K = \mathbb{Q}(\alpha)$ be a number field of degree m and let $\mathcal{O}_K$ be its ring of integers. The definition of short elements in K plays an essential role in RLWE and PLWE. This geometric notion derives from an appropriate choice of a norm on K by embedding the number field in a vector space. On the one hand, RLWE makes use of the *canonical embedding* σ, which maps each $x \in \mathcal{O}_K$ to $(\sigma_1(x), \dots, \sigma_m(x))$, where $\sigma_1, \dots, \sigma_m$ are the injective homomorphisms from K to $\mathbb{C}$. On the other hand, PLWE uses the *coefficient embedding*, which maps each $x \in \mathcal{O}_K$ to the vector $(x_0, \dots, x_{m-1}) \in \mathbb{Z}^m$ of its coefficients with respect to the power basis $1, \alpha, \dots, \alpha^{m-1}$. As a linear map, the canonical embedding σ admits a matrix representation $V \in \mathbb{C}^{m \times m}$; so that, for each $x \in \mathcal{O}_K$, we have $\sigma(x) = V \cdot (x_0, \dots, x_{m-1})^\intercal$. For the equivalence between RLWE and PLWE, it is important to determine when, whether $\|x\|$ is small, then so is $\|\sigma(x)\|$, and vice versa. This notion is quantified by V having a small *condition number* $\mathrm{Cond}(V) := \|V\|\|V^{-1}\|$, where $\|V\| := \sqrt{\mathrm{Tr}(V^\star V)}$ is the *Frobenius norm* of V and $V^\star$ is the conjugate transpose of V.

***Corresponding Author: Carlo Sanna:** Politecnico di Torino, Department of Mathematical Sciences, Corso Duca degli Abruzzi 24, 10129 Torino, Italy; Email: carlo.sanna.dev@gmail.com
Antonio J. Di Scala: Politecnico di Torino, Department of Mathematical Sciences, Corso Duca degli Abruzzi 24, 10129 Torino, Italy; Email: antonio.discala@polito.it
Edoardo Signorini: Telsy Elettronica e Telecomunicazioni S.p.A., Corso Svizzera 185, 10149 Torino, Italy; Email: edoardo.signorini@telsy.it

Open Access. © 2020 A. J. Di Scala *et al.*, published by De Gruyter. This work is licensed under the Creative Commons Attribution 4.0 License

When K is the nth cyclotomic number field, $V = V_n$ is the Vandermonde matrix associated with the nth cyclotomic polynomial, that is,

$$V_n := \begin{pmatrix} 1 & \zeta_1 & \zeta_1^2 & \cdots & \zeta_1^{m-1} \\ 1 & \zeta_2 & \zeta_2^2 & \cdots & \zeta_2^{m-1} \\ 1 & \zeta_3 & \zeta_3^2 & \cdots & \zeta_3^{m-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \zeta_m & \zeta_m^2 & \cdots & \zeta_m^{m-1} \end{pmatrix},$$

where $\zeta_1, \ldots, \zeta_m$ are the primitive nth roots of unity, and $m = \varphi(n)$ is the Euler's totient function of n.

Recently, Blanco-Chacón [4] gave some upper bounds for the condition number of V_n, proving the equivalence between the RLWE and PLWE problems for some infinite families of cyclotomic number fields.

Our first result is the following.

Theorem 1.1. *For every positive integer n, we have*

$$\operatorname{Cond}(V_n) = \frac{n}{\operatorname{rad}(n)} \operatorname{Cond}(V_{\operatorname{rad}(n)}),$$

where $\operatorname{rad}(n)$ *denotes the product of all prime factors of n.*

Our second result is a formula for the condition number of V_n when n is a prime power or a power of 2 times an odd prime power.

Theorem 1.2. *If $n = p^k$, where k is a positive integer and p is a prime number, or if $n = 2^k p^\ell$, where k, ℓ are positive integers and p is an odd prime number, then*

$$\operatorname{Cond}(V_n) = \varphi(n)\sqrt{2\left(1 - \frac{1}{p}\right)}.$$

In particular, Theorem 1.2 improves the upper bound $\operatorname{Cond}(V_n) \le 4(p-1)\varphi(n)$ given by Blanco-Chacón in the case in which $n = p^k$ is a prime power [4, Theorem 4.1].

Our proofs of Theorems 1.1 and 1.2 are based on the study of the Gram matrix $G_n := V_n^\star V_n$. Regarding that, we give also the following result.

Theorem 1.3. *For every positive integer n, the matrix nG_n^{-1} has integer entries.*

From a number-theoretic point of view, it might be of some interest trying to describe the entries of nG_n^{-1} explicitely, or at least understand the integer sequence $\operatorname{Tr}(nG_n^{-1})_{n\ge1}$ (which is related to $\operatorname{Cond}(V_n)$ by (3) below).

2 Proofs

For every positive integer n, the *Ramanujan's sums* modulo n are defined by

$$c_n(t) := \sum_{i=1}^{m} \zeta_i^t,$$

for all integers t. It is easy to check that $c_n(\cdot)$ is an even periodic function with period n. Moreover, the following formula holds [6, Theorem 272]

$$c_n(t) = \mu\left(\tfrac{n}{(n,t)}\right) \frac{\varphi(n)}{\varphi\left(\tfrac{n}{(n,t)}\right)}, \tag{1}$$

where μ is the Möbius function and (n, t) denotes the greatest common divisor of n and t.

Let $G_n := V_n^* V_n$ be the *Gram matrix* of V_n. By the previous considerations, we have

$$G_n = \begin{pmatrix} c_n(0) & c_n(1) & c_n(2) & \cdots & c_n(m-1) \\ c_n(1) & c_n(0) & c_n(1) & \cdots & c_n(m-2) \\ c_n(2) & c_n(1) & c_n(0) & \cdots & c_n(m-3) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ c_n(m-1) & c_n(m-2) & c_n(m-3) & \cdots & c_n(0) \end{pmatrix} = \big(c_n(i-j)\big)_{1\le i,j\le m}. \tag{2}$$

In particular, G_n is a symmetric Toeplitz matrix with integer entries.

Let $\lambda_1, \dots, \lambda_s$ be the distinct eigenvalues of G_n, which are real and positive, since G_n is the Gram matrix of an invertible matrix, and let $\mu_1, \dots, \mu_s$ be their respective multiplicities. We have

$$\operatorname{Cond}(V_n) = \|V_n\|\|V_n^{-1}\| = m\sqrt{\operatorname{Tr}(G_n^{-1})} = m\sqrt{\sum_{i=1}^{s} \frac{\mu_i}{\lambda_i}}. \tag{3}$$

Therefore, the study of $\operatorname{Cond}(V_n)$ is equivalent to the study of the eigenvalues of G_n.

The next lemma relates the characteristic polynomials of G_n and $G_{\operatorname{rad}(n)}$.

Lemma 2.1. *For every positive integer n, we have*

$$\det(G_n - x\operatorname{Id}_m) = h^m \det\big(G_{n'} - \tfrac{x}{h}\operatorname{Id}_{m'}\big)^h,$$

where $n' := \operatorname{rad}(n)$, $m' := \varphi(n')$, and $h := n/n'$.

Proof. We know from (2) that $G_n = \big(c_n(i-j)\big)_{0\le i,j<m}$, where we shifted the indices i, j to the interval $[0, m)$ since this does not change the differences $i - j$ and simplifies the next arguments. Write the integers $i, j \in [0, m)$ in the form $i = hi' + i''$ and $j = hj' + j''$, where $i', j' \in [0, m')$ and $i'', j'' \in [0, h)$ are integers. By (1) we have that $c_n(i-j) \neq 0$ if and only if h divides $i - j$ (otherwise, $n/(n, i-j)$ is not squarefree), which in turn happens if and only if $i'' = j''$. In such a case, we have $(n, i-j) = h(n', i'-j')$ and, again by (1), it follows that

$$c_n(i-j) = \mu\Big(\tfrac{n}{(n,i-j)}\Big)\,\frac{\varphi(n)}{\varphi\Big(\tfrac{n}{(n,i-j)}\Big)} = \mu\Big(\tfrac{n'}{(n',i'-j')}\Big)\,\frac{h\,\varphi(n')}{\varphi\Big(\tfrac{n'}{(n',i'-j')}\Big)} = h\,c_{n'}(i'-j').$$

Therefore, we have found that G_n consists of $m' \times m'$ diagonal blocks of sizes $h \times h$. Precisely,

$$G_n = h\big(c_{n'}(i'-j')\operatorname{Id}_h\big)_{0\le i',j'<m'} = h\,G_{n'} \otimes \operatorname{Id}_h,$$

where $\otimes$ denotes the Kronecker product. Consequently, the characteristic polynomial of G_n is

$$\begin{aligned} \det(G_n - x\operatorname{Id}_m) &= h^m \det\big(G_{n'} \otimes \operatorname{Id}_h - \tfrac{x}{h}\operatorname{Id}_m\big) \\ &= h^m \det\big((G_{n'} - \tfrac{x}{h}\operatorname{Id}_{m'}) \otimes \operatorname{Id}_h\big) \\ &= h^m \det\big(G_{n'} - \tfrac{x}{h}\operatorname{Id}_{m'}\big)^h, \end{aligned}$$

as claimed. □

Now we are ready to prove the first result.

2.1 Proof of Theorem 1.1

Let $n' := \operatorname{rad}(n)$, $m' := \varphi(n')$, and $h := n/n'$. Furthermore, let $\lambda_1', \dots, \lambda_{s'}'$ be the distinct eigenvalues of $G_{n'}$, with respective multiplicities $\mu_1', \dots, \mu_{s'}'$. It follows from Lemma 2.1 that $s' = s$ and that the eigenvalues of G_n are $h\lambda_1', \dots, h\lambda_s'$, with respective multiplicities $h\mu_1', \dots, h\mu_s'$. Hence, (3) yields

$$\operatorname{Cond}(V_n) = m\sqrt{\sum_{i=1}^{s} \frac{\mu_i}{\lambda_i}} = m\sqrt{\sum_{i=1}^{s} \frac{\mu_i'}{\lambda_i'}} = \frac{m}{m'}\operatorname{Cond}(V_{n'}) = \frac{n}{n'}\operatorname{Cond}(V_{n'}),$$

as claimed. □

We need a couple of preliminary lemmas to the proof of Theorem 1.2.

Lemma 2.2. *For every odd positive integer n, the matrices G_{2n} and G_n have the same eigenvalues (with the same multiplicities).*

Proof. It is known [6, Theorem 67] that Ramanujan's sums are multiplicative functions respect to their moduli, that is, $c_{ab}(t) = c_a(t)\, c_b(t)$ for all coprime positive integers a, b. Moreover, it is easy to check that $c_2(t) = (-1)^t$. Thus, (2) gives

$$G_{2n} = \big(c_{2n}(i-j)\big)_{1\le i,j\le m} = \big((-1)^{i-j} c_n(i-j)\big)_{1\le i,j\le m} = J^{-1} G_n J,$$

where J is the $m \times m$ matrix alternating $+1$ and -1 on its diagonal and having zeros in all the other entries. Therefore, G_n and G_{2n} are similar and consequently they have the same eigenvalues. □

Lemma 2.3. *Given two complex numbers a and b, the determinant of the $k \times k$ matrix*

$$\begin{pmatrix} a & b & b & \cdots & b \\ b & a & b & \cdots & b \\ b & b & a & \cdots & b \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ b & b & b & \cdots & a \end{pmatrix}$$

is equal to $(a-b)^{k-1}(a+(k-1)b)$.

Proof. Subtracting the last row from all the other rows, and then adding to the last column all the other columns, the matrix becomes

$$\begin{pmatrix} a-b & 0 & \cdots & 0 & 0 \\ 0 & a-b & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & a-b & 0 \\ b & b & b & b & a+b(k-1) \end{pmatrix}.$$

Laplace expansion along the last column gives the desired result. □

2.2 Proof of Theorem 1.2

First, let us consider $n = p^k$, where k is a positive integer and p is a prime number. It follows from (1) that $c_p(t) = p-1$ if p divides t, while $c_p(t) = -1$ otherwise. Hence, using Lemma 2.3, we have

$$\det(G_p - x\,\mathrm{Id}_{p-1}) = \begin{pmatrix} p-1-x & -1 & \cdots & -1 \\ -1 & p-1-x & \cdots & -1 \\ \vdots & \vdots & \ddots & \vdots \\ -1 & -1 & \cdots & p-1-x \end{pmatrix} = (p-x)^{p-2}\,(1-x),$$

so that the eigenvalues of G_p are p and 1, with respective multiplicities $p-2$ and 1.

As a consequence, (3) gives

$$\mathrm{Cond}(V_p) = (p-1)\sqrt{2\left(1-\frac{1}{p}\right)}, \tag{4}$$

and, thanks to Theorem 1.1, we obtain

$$\mathrm{Cond}(V_{p^k}) = p^{k-1}\,\mathrm{Cond}(V_p) = p^{k-1}(p-1)\sqrt{2\left(1-\frac{1}{p}\right)} = \varphi(n)\sqrt{2\left(1-\frac{1}{p}\right)},$$

as claimed.

Now assume that $n = 2^k p^\ell$, where k, ℓ are positive integers and p is an odd prime number. From Lemma 2.2 and (3) it follows at once that $\mathrm{Cond}(V_{2p}) = \mathrm{Cond}(V_p)$. Hence, Theorem 1.1 and (4) yield

$$\mathrm{Cond}(V_{2^k p^\ell}) = 2^{k-1} p^{\ell-1} \mathrm{Cond}(V_{2p}) = 2^{k-1} p^{\ell-1}(p-1)\sqrt{2\left(1-\frac{1}{p}\right)} = \varphi(n)\sqrt{2\left(1-\frac{1}{p}\right)},$$

as claimed. □

The next lemma is the well known orthogonality relation between the roots of unity.

Lemma 2.4. *We have*

$$\sum_{\ell=1}^{n} \left(\zeta_k \overline{\zeta_h}\right)^\ell = \begin{cases} n & \text{if } k = h, \\ 0 & \text{if } k \neq h, \end{cases}$$

for $k, h = 1, \ldots, m$.

2.3 Proof of Theorem 1.3

Let $V_n^{-1} = (w_{i,j})_{1 \le i,j \le m}$ and define

$$S_{i,\ell} := \sum_{k=1}^{m} w_{i,k} \zeta_k^\ell,$$

for all integers i, ℓ with $1 \le i \le m$ and $\ell \ge 0$. On the one hand, since $V_n^{-1} V_n = \mathrm{Id}_m$, for $\ell < m$ we have that $S_{i,\ell} = \delta_{i,\ell+1}$ (Kronecker delta). On the other hand, since $\zeta_1, \ldots, \zeta_k$ are conjugate algebraic integers with minimal polynomial of degree m, for $\ell \ge m$ there exist integers $b_0, \ldots, b_{m-1}$ such that $\zeta_k^\ell = b_0 + b_1 \zeta_k + \cdots + b_{m-1} \zeta_k^{m-1}$ for $k = 1, \ldots, m$, and consequently $S_{i,\ell} = b_0 S_{i,0} + b_1 S_{i,1} + \cdots + b_{m-1} S_{i,m-1}$. Hence, $S_{i,\ell}$ is always an integer.

Recalling that $G_n = V_n^\star V_n$, we have $G_n^{-1} = V_n^{-1} \left(V_n^{-1}\right)^\star$. Hence, also using Lemma 2.4, the (i, j) entry of $n G_n^{-1}$ is equal to

$$n \sum_{k=1}^{m} w_{i,k} \overline{w_{j,k}} = \sum_{k=1}^{m} \sum_{h=1}^{m} w_{i,k} \overline{w_{j,h}} \sum_{\ell=1}^{n} \left(\zeta_k \overline{\zeta_h}\right)^\ell = \sum_{\ell=1}^{n} \left(\sum_{k=1}^{m} w_{i,k} \zeta_k^\ell\right) \overline{\left(\sum_{h=1}^{m} w_{j,h} \zeta_h^\ell\right)} = \sum_{\ell=1}^{n} S_{i,\ell} S_{j,\ell},$$

which is an integer. □

Acknowledgement: A. J. Di Scala and C. Sanna are members of GNSAGA of INdAM and of CrypTO, the group of Cryptography and Number Theory of Politecnico di Torino. A. J. Di Scala is a member of DISMA Dipartimento di Eccellenza MIUR 2018-2022. E. Signorini is a cryptographer at Telsy S.p.A.

References

[1] V. Lyubashevsky, C. Peikert, and O. Regev, *On ideal lattices and learning with errors over rings*, Advances in cryptology—EUROCRYPT 2010, Lecture Notes in Comput. Sci., vol. 6110, Springer, Berlin, 2010, pp. 1–23.

[2] O. Regev, *On lattices, learning with errors, random linear codes, and cryptography*, J. ACM **56** (2009), no. 6, Art. 34, 40.

[3] D. Stehlé, R. Steinfeld, K. Tanaka, and K. Xagawa, *Efficient public key encryption based on ideal lattices (extended abstract)*, Advances in cryptology—ASIACRYPT 2009, Lecture Notes in Comput. Sci., vol. 5912, Springer, Berlin, 2009, pp. 617–635.

[4] I. Blanco-Chacón, *On the RLWE/PLWE equivalence for cyclotomic number fields*, Appl. Algebra Engrg. Comm. Comput. (accepted).

[5] M. Rosca, D. Stehlé, and A. Wallet, *On the ring-LWE and polynomial-LWE problems*, Advances in cryptology—EUROCRYPT 2018. Part I, Lecture Notes in Comput. Sci., vol. 10820, Springer, Cham, 2018, pp. 146–173.

[6] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, sixth ed., Oxford University Press, Oxford, 2008, Revised by D. R. Heath-Brown and J. H. Silverman, With a foreword by Andrew Wiles.