The valuative capacity of the set of sums of d-th powers

Marie-Andrée B.Langlois
This is a joint work with Keith Johnson.

Dalhousie University
Halifax, Canada

July 4 2016

What is this talk about?

The valuative capacity is an important invariant for rings of integer valued polynomials that was first introduced by Chabert in the Arabian Journal for Science and Engineering, it also relates to many other areas of mathematics such as:

- Polya-Szegö theorem (Fares and Petite)
- Integer polynomial approximation (Ferguson)
- Algebraic geometry, Néron height pairing (Rumeley)

Outline

This talk will go through the following:

- The definition of valuative capacity and, some known and new formulas to calculate it.
- Number theoretical properties of the sets of sums of d-th powers.
- How we can connect the two previous to calculate the valuative capacity of the the sets of sums of d-th powers.

Preliminary Definitions

Definition

For any subset E, the ring of integer valued polynomials on E is defined to be

$$\mathrm{Int}(E, D) = \{f(x) \in K[x] \mid f(E) \subseteq D\}.$$

Definition

The sequence of characteristic ideals of E is $(I_n \mid n = 0, 1, 2, \ldots)$ where I_n is the fractional ideal of K formed by 0 and the leading coefficients of the elements of $Int(E, D)$ of degree no more than n. The characteristic sequence of E with respect to a fixed prime p is the sequence of negatives of the p-adic valuations of these ideals, denoted by $\alpha_{E,p}(n)$.

The valuative capacity

Definition

For E a subset of D and p a fixed prime, the valuative capacity of E with respect to the prime p is the following limit:

$$L_{E,p} = \lim_{n\to\infty} \frac{\alpha_{E,p}(n)}{n}.$$

The positive integers in increasing order are a p-ordering of $\mathbb{Z}$ and we have that $\alpha_{\mathbb{Z},p}(n) = \nu_p(n!)$. By Legendre's formula $\nu_p(n!) = \frac{n-\sum n_i}{p-1}$, we can compute

$$L_{\mathbb{Z},p} = \lim_{n\to\infty} \frac{\alpha_{\mathbb{Z},p}(n)}{n} = \frac{1}{p-1}.$$

Tricks for Calculating

Proposition

Let p be a fixed prime and A be a subset of $\mathbb{Z}$.

1. *[BC00] $L_{\alpha_{\overline{A},p}} = L_{\alpha_{A,p}}$, since $\alpha_{\overline{A},p} = \alpha_{A,p}$.*
2. *[Joh09b] If A has characteristic sequence $\alpha_{A,p}(n)$ then for any $c \in \mathbb{Z}$ the characteristic sequence of $A + c$ is also $\alpha_{A,p}(n)$ and the characteristic sequence of $p^k A$ is $\alpha_{A,p}(n) + kn$.*
3. *[Joh09b] If B is another subset of $\mathbb{Z}$, with the property that for any $a \in A$ and $b \in B$ it is the case that $\nu_p(a - b) = 0$, then the characteristic sequence of $A \cup B$ is the disjoint union of the sequences $\alpha_{A,p}(n)$ and $\alpha_{B,p}(n)$ sorted into nondecreasing order.*

Tricks for Calculating - Continued

Proposition (continued)

4 *[Joh09a] If $\alpha_{A,p}(n)$ and $\alpha_{B,p}(n)$ are the characteristic sequences of A and B respectively, for a prime p, and A, B satisfying (3), with valuative capacity $L_{A,p}$ and $L_{B,p}$ respectively, then*

$$\frac{1}{L_{A\cup B,p}} = \frac{1}{L_{A,p}} + \frac{1}{L_{B,p}}.$$

5 *[Joh15] Given a prime p, if A and B are disjoint subsets with the property that there is a nonnegative integer k such that $\nu_p(a-b) = k$ for any $a \in A$ and $b \in B$, then*

$$\frac{1}{L_{A\cup B,p} - k} = \frac{1}{L_{A,p} - k} + \frac{1}{L_{B,p} - k}.$$

Continued Fractions

We use the concise notation, where $[a; a_0, a_1, \ldots, a_k]$ denotes

$$a + \cfrac{1}{a_0 + \cfrac{1}{a_1 + \cfrac{}{\ddots + \cfrac{1}{a_k}}}}.$$

When a contined fraction is periodic it evaluates to the root of a quadratic polynomial.

What we will need

Proposition

(a) *[BL] If A is a union of cosets modulo p^m for some m, then the valuative capacity of A is rational and recursively computable.*

(b) *[BL] If $A_0, A_1, \ldots, A_m$ are disjoint subsets of $\mathbb{Z}$ such that, whenever $0 \leq k < h \leq m$, $a \in A_k$, and $b \in A_h$, one has $\nu_p(a-b) = k$, then, the p-valuative capacity of $A = A_0 \cup \cdots \cup A_m$, has the following continued fraction expansion:*

$$L_A = [0; a_0, a_1, \ldots, a_{2(m-1)}, a_{2m-1}]$$

where $a_{2k} = \frac{1}{L_{A_k} - k}$ for $0 \leq k \leq m-1$, $a_{2k+1} = 1$ for $0 \leq k < m-1$, and $a_{2m-1} = L_{A_m} - (m-1)$.

What we will need - Continued

Proposition (continued)

(c) *[BL] If $E = E' \cup p^m E$, where E' is a union of nonzero cosets $\pmod{p^m}$, then L_E is the root of a quadratic polynomial in $\mathbb{Q}[x]$, whose coefficients are recursively computable.*

Example

Example (a): We illustrate this with $p = 3$, and $A = \{0, 1, 2, 3, 10, 11, 12, 19, 20, 21\} + 3^3\mathbb{Z}$. We decompose A:

$$A_0 = \{1, 2, 10, 11, 19, 20\} + 3^3\mathbb{Z}$$
$$A_1 = \{3, 12, 21\} + 3^3\mathbb{Z}$$
$$A_2 = \{0\} + 3^3\mathbb{Z}$$

We can rewrite A_0:

$$A_0 = (1 + \{0, 9, 18\} + 3^3\mathbb{Z}) \cup (2 + \{0, 9, 18\} + 3^3\mathbb{Z}).$$

$$\begin{aligned} L_{1+\{0,9,18\}+3^3\mathbb{Z}} &= L_{2+\{0,9,18\}+3^3\mathbb{Z}} = L_{\{0,9,18\}+3^3\mathbb{Z}} \\ &= L_{9(\{0,1,2\}+3\mathbb{Z})} = 2 + L_{\mathbb{Z}} = 2 + \frac{1}{2} = \frac{5}{2} \end{aligned}$$

Example - Continued

Now we can find $L_{A_0} = \frac{5}{4}$, $L_{A_1} = \frac{5}{2}$ and $L_{A_2} = \frac{7}{2}$. We are ready to compute the valuative capacity of A:

$$L_A = \cfrac{1}{\cfrac{1}{L_{A_0}} + \cfrac{1}{1 + \cfrac{1}{\cfrac{1}{L_{A_1} - 1} + \cfrac{1}{L_{A_2} - 1}}}} = \cfrac{1}{\cfrac{1}{\frac{5}{4}} + \cfrac{1}{1 + \cfrac{1}{\cfrac{1}{\frac{5}{2} - 1} + \cfrac{1}{\frac{7}{2} - 1}}}} = \frac{155}{204}$$

(b): Now we look into the valuative capacity of the set $E = E' \cup 3^6 E$, where E' is $A_0 \cup A_1$ from part (a).

Then we have that $L_E = [0; a_0, a_1, a_2, L_{A_2} - 1]$, where $a_0 = \frac{1}{L_{A_0}} = \frac{4}{5}$, $a_1 = 1$, $a_2 = \frac{1}{L_{A_1} - 1} = \frac{2}{3}$, and $L_{A_2} = L_{3^6 E} = 6 + L_E$. Hence $L_E = [0; \frac{4}{5}, 1, \frac{2}{3}, L_{A_2} - 1]$. Solving the continued fractions gives that L_E is a solution to the following quadratic equation:

$30L_E^2 + 152L_E - 140 = 0$ which has for positive root $L_E = \frac{\sqrt{2494}}{15} - \frac{38}{15}$.

The important sets

Definition

For a fixed $d \in \mathbb{Z}$ with $d \geq 0$, we define D to be the set of d-th powers of integers, thus $D = \{x^d \mid x \in \mathbb{Z}\}$ and we let $\ell D = D + \cdots + D$, for ℓ terms in the sum.

Definition

Let D_{p^e} denote the set of d-th powers modulo p^e, for $e \geq 1$ and ℓD_{p^e} the sets of sums of ℓ elements to the power of D modulo p^e. We will also make use of $\overline{D} = \varprojlim_{m \in \mathbb{N}} D_{p^m}$, the p-adic closure of D in $\hat{\mathbb{Z}}_p$, and similarly we will consider $\overline{\ell D}$.

Main Result

Theorem

Suppose p is a prime and $d = p^j d'$ a positive integer not equal to 4, where $p \nmid d'$ and let $e = 2j + 1$.

Then, $L_{\ell D,p}$ is an algebraic number of degree at most 2.

When 0 can be written non-trivially as a sum of ℓ elements to the power of $d \pmod{p^e}$, $L_{\ell D,p}$ is a rational number.

Corollary

For a fixed ℓ, if d is odd and p is a prime, then $L_{\ell D,p} \in \mathbb{Q}$.

Main Result - Outline of the proof

Proof.

We start by looking at

$$E = \left\{[c] \in \ell D_{p^e} \mid [c] = \sum_{i=1}^{\ell} [x_i]^d, \text{ where at least one of the } x_i \text{ is not divisible by } p\right\}$$

Suppose that $c \in \hat{\mathbb{Z}}_p$ is such that $[c] \in E$, and that $\{x_i\}_{i=1}^{\ell} \subseteq \hat{\mathbb{Z}}_p$ are such that $c \equiv \sum_{i=1}^{\ell} x_i^d \pmod{p^e}$.

We show that $c \in \overline{\ell D}$ in this case. Thus, if $E = \ell D_{p^e}$, then $\overline{\ell D}$ is a union of cosets of the form $(c + p^e \hat{\mathbb{Z}}_p)$, and $L_{\ell D} = L_{\overline{\ell D}} \in \mathbb{Q}$.

Main Result - Outline of the proof (continued)

Proof.

If $E \neq \ell D_{p^e}$ then we claim that $\ell D_{p^e} \backslash E = \{[0]\}$. If $[c] \in \ell D_{p^e} \backslash E$, then $p^d \Big| \sum^{\ell} x_i^d$ and so $p^d \mid c$, hence $[c] = [0]$.

Let $x_i = p \cdot \tilde{x}_i$ and let $\tilde{c} = \sum^{\ell} \tilde{x}_i^d$. We then have $c = p^d \tilde{c}$ with $\tilde{c} \in \overline{\ell D}$. Conversely if $\tilde{c} \in \overline{\ell D}$, then $c = p^d \tilde{c} \in \overline{\ell D}$ and $c \equiv 0 \pmod{p^e}$.

Thus $\overline{\ell D} = \left(\bigcup (c + p^e \hat{\mathbb{Z}}_p)\right) \cup p^d \overline{\ell D}$, where the union is over cosets for which $[c] \in E$. Thus $L_{\ell D, p} = L_{\overline{\ell D}}$ is the root of a quadratic polynomial over $\mathbb{Q}[x]$. □

Possible Formulas - The case p odd

Proposition

For a fixed ℓ, if $p \nmid d$ and $d = 2^\alpha \beta$, with β odd, if $p \equiv 1 \pmod{2^{\alpha+1}}$ then

$$L_{\ell D,p} = \frac{1}{|\ell D_p|}\left(1 + \frac{1}{p-1}\right).$$

Proposition

Let p be odd and d an even integer such that $d = 2^\alpha \beta$, with β odd. If $p \not\equiv 1 \pmod{2^{\alpha+1}}$ and $p \nmid d$, then $L_{\ell D,p}$ is the positive root of the quadratic equation with coefficients in $\mathbb{Q}$:

$$L_{\ell D,p}^2 + dL_{\ell D,p} - \frac{(p-1)d}{|\ell D_p|} = 0.$$

Possible Formulas

Proposition

If $p > (d-1)^4$ and $d > 2$ then

1. *For d odd, $L_{\ell D,p} = \frac{1}{p-1}$.*
2. *For d even, with $d = 2^\alpha \beta$ and β odd:*
   (a) *If $p \equiv 1 \pmod{2^{\alpha+1}}$, then $L_{\ell D,p} = \frac{1}{p-1}$.*
   (b) *If $p \not\equiv 1 \pmod{2^{\alpha+1}}$, then, since $p \nmid d$,*
      (i) *if $\ell = 2$, then $L_{2D,p}$ is the root of the quadratic equation $L_{2D,p}^2 + dL_{2D,p} - \frac{(p-1)d}{|2D_p|} = 0$,*
      (ii) *if $\ell \geq 3$, then $L_{\ell D,p} = \frac{1}{|\ell D_p|}\left(1 + \frac{1}{p-1}\right)$.*

Possible Formulas - Continued

Proposition

For p a prime, with $p \nmid d$, and $d > 2$, if $\gcd(d, p-1) = 1$*, then* $D_{p^e} = \mathbb{Z}/(p^e)$ *for* $e \geq 1$*, and for* $\ell > 1$*,* $L_{\ell D,p} = \frac{1}{p-1}$.

The case $p = 2$

Proposition

If $d = 2^{\alpha}\beta$, where $\alpha \geq 1$ and β is an odd integer ≥ 1, then we can write $\overline{D}$ in the following way:

$$\overline{D} = \{0\} \cup (1+2^{\alpha+2}\hat{\mathbb{Z}}_2) \cup 2^{d}(1+2^{\alpha+2}\hat{\mathbb{Z}}_2) \cup 2^{2d}(1+2^{\alpha+2}\hat{\mathbb{Z}}_2) \cup 2^{3d}(1+2^{\alpha+2}\hat{\mathbb{Z}}_2) \ldots .$$

Proposition

For $\ell = 2$ and any $d = 2^{\alpha}\beta$, where $\alpha \geq 1$ and β is an odd integer ≥ 1, L_{D+D} is the positive root of the following polynomial depending on d:

$$(2\alpha+6)L^2 + (2\alpha d - 2\alpha + 6d - 7)L + (\alpha + 3 - \alpha d^2 - 6\alpha d - 9d) = 0.$$

The case $p = 2$ Legendre's Theorem

Proposition

For $\ell = 3$ and $d = 2$, $\overline{3D_2} = \{0\} \cup \bigcup_{i=0}^{\infty} 2^{2i}(\{1,2,3,4,5,6\} + 8\hat{\mathbb{Z}}_2)$.

Proof.

We have shown previously that $\overline{D}_2 = \{0\} \cup \bigcup_{i=0}^{\infty} 2^{i}(1 + 8\hat{\mathbb{Z}}_2)$. Adding the cosets triple-wise gives

$$\overline{3D_2} = \{0\} \cup \bigcup_{i=0}^{\infty} 2^{2i}(\{1,2,3,4,5,6\} + 8\hat{\mathbb{Z}}_2).$$

The only elements not in $\overline{3D_2}$ are those of the form $2^{2i}(7 + 8\hat{\mathbb{Z}}_2)$. □

The case $p = 2$ - Continued

Proposition

If $d = 2$, $\ell \geq 4$ and $n \geq 1$, we have that $\overline{\ell D_{2^n}} = \mathbb{Z}/(2^n)$ and $L_{\overline{\ell D_2}} = 1$.

Here is a table of various other valuative capacities (L) for $3D_{p^e}$, for both odd and even p:

p	d	L
2	2	$\frac{21}{22}$
2	4	$\frac{3}{2}$
2	6	$\frac{5}{4}$
2	8	$\frac{14}{15}$

p	d	L
3	6	$\frac{155}{204}$
3	12	$\frac{155}{204}$
3	18	$\frac{511}{488}$
3	27	$\frac{143}{170}$

Thank you

Thank you for listening to this presentation.

- Chabert, J.-L. *Generalized factorial ideals*. The Arabian Journal for Science and Engineering, 26, pages 51-68, 2001.
- Fares, Y., Johnson, K. *The Valuative Capacities of the Sets of Sums of Two and of Three Squares*, Integers (to appear).
- Johnson, K. *Limits of characteristic sequences of integer-valued polynomials on homogeneous sets*. Journal of Number Theory 129, pages 2933-2942, 2009.