Lecture 1: Cohomology and congruences

Masha Vlasenko (IMPAN, Warsaw)

joint work with Frits Beukers

Bhaskaracharya Pratishthana, Pune

July 26, 2022

§Sequences of constant terms of powers

$g(\mathbf{x}) = \sum_{\mathbf{u}} g_{\mathbf{u}} \mathbf{x}^{\mathbf{u}} \in \mathbb{Z}[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$

$supp(g) = \{\mathbf{u} \in \mathbb{Z}^n : g_{\mathbf{u}} \neq 0\}$

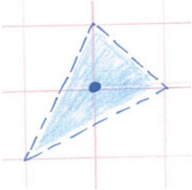
$\Delta \subset \mathbb{R}^n$ Newton polytope of g = convex hull of $supp(g)$

c_k = coefficient of $\mathbf{x}^{\mathbf{0}}$ (constant term) in $g(\mathbf{x})^k$, $k = 0, 1, 2, \ldots$

Example.

$$g(\mathbf{x}) = x_1 + x_2 + \frac{1}{x_1 x_2}$$

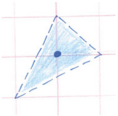
$$c_k = \begin{cases} 0, & 3 \nmid k \\ \frac{k!}{(k/3)!^3}, & 3 | k \end{cases}$$



Lucas' congruence

$$c_k = \text{ constant term in } g(\mathbf{x})^k,\ k = 0, 1, 2, \ldots$$
$$\Delta = \text{ Newton polytope of } g(\mathbf{x})$$

Assume that $\mathbf{0} \in \Delta$ is the only internal integral point. Then for any prime p we have



$$c_k \equiv c_{k_0} c_{k_1} \ldots c_{k_\ell} \mod p, \qquad \forall\ k$$

where $0 \le k_i \le p-1$ are the digits in the p-adic expansion of k:

$$k = k_0 + k_1 p + k_2 p^2 + \ldots + k_\ell p^\ell.$$

Generalization mod p^s: Dwork's congruences

$$\gamma(t) \;=\; \sum_{k=0}^{\infty} c_k t^k \in \mathbb{Z}[\![t]\!], \qquad c_k = \text{ constant term of } g(\mathbf{x})^k$$

$$= \frac{1}{(2\pi i)^n} \oint \dots \oint \frac{1}{1 - t\, g(\mathbf{x})} \frac{dx_1}{x_1} \dots \frac{dx_n}{x_n}$$

$$\gamma_m(t) = \sum_{k=0}^{m-1} c_k t^k \qquad \text{truncations}$$

Theorem 1 (Mellit-V, 2013). Assume that $\mathbf{0} \in \Delta$ is the only internal integral point in the Newton polytope of $g(\mathbf{x})$. Then for any prime p and any integer $s \geq 1$

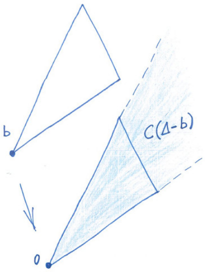
$$\frac{\gamma(t)}{\gamma(t^p)} \equiv \frac{\gamma_{p^s}(t)}{\gamma_{p^{s-1}}(t^p)} \mod p^s.$$

Theorem 2 (Beukers-V, 2019). In the conditions of Theorem 1 one has $\gamma(t)/\gamma(t^p) \in p$-adic completion of $\mathbb{Z}[t, 1/\gamma_p(t)]$.

§Formal expansions of rational functions

$f(\mathbf{x}) = \sum f_{\mathbf{u}} \mathbf{x}^{\mathbf{u}} \in \mathbb{Z}[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$, $\Delta \subset \mathbb{R}^n$ its Newton polytope

$h(\mathbf{x}) \in \mathbb{Z}[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$, $m \geq 1$



pick a vertex $\mathbf{b} \in \Delta$

$$\downarrow$$

$$\frac{h(\mathbf{x})}{f(\mathbf{x})^m} = \frac{h(\mathbf{x})}{f_{\mathbf{b}}^m \mathbf{x}^{m\mathbf{b}} (1 + \ell(\mathbf{x}))^m} = \frac{h(\mathbf{x}) \mathbf{x}^{-m\mathbf{b}}}{f_{\mathbf{b}}^m} \sum_{s \geq 0} \binom{-m}{s} \ell(\mathbf{x})^s = \sum_{\mathbf{v} \in \mathbb{Z}^n} a_{\mathbf{v}} \mathbf{x}^{\mathbf{v}}$$

Note: if $supp(h) \subset m\Delta$, then the formal expansion is supported in the cone $C(\Delta - \mathbf{b})$

Gauss' congruences

$$f(\mathbf{x}) = \sum f_{\mathbf{u}} \mathbf{x}^{\mathbf{u}} \quad \text{with Newton polytope} \quad \Delta$$

$$\frac{h(\mathbf{x})}{f(\mathbf{x})} = \sum a_{\mathbf{v}} \mathbf{x}^{\mathbf{v}} \quad \text{formal expansion at a vertex } \mathbf{b} \in \Delta$$

Theorem (Beukers-Houben-Straub, 2018) Assume that $supp(h) \subset \Delta$ and $\Delta \cap \mathbb{Z}^n = \{vertices\}$. Then for any prime p such that $p \nmid f_{\mathbf{u}}$ for all $\mathbf{u}$ and any $\mathbf{v} \in C(\Delta - \mathbf{b})$ one has

$$a_{\mathbf{v}} \equiv a_{\mathbf{v}/p} \mod p^{ord_p(\mathbf{v})}$$

§Cohomology and congruences

$f(\mathbf{x}) \in R[x_1^{\pm 1}, \dots, x_n^{\pm 1}]$, R is a ring of char 0
$X_f = \{f(\mathbf{x}) = 0\} \subset \mathbb{T}^n$, $\Delta \subset \mathbb{R}^n$ Newton polytope of $f(\mathbf{x})$

$$\Omega_f = \left\{ (m-1)! \frac{h(\mathbf{x})}{f(\mathbf{x})^m} \;\middle|\; \begin{array}{l} m \geq 1, h \in R[x_1^{\pm 1}, \dots, x_n^{\pm 1}] \\ supp(h) \subset m\Delta \end{array} \right\} \quad R\text{-module}$$

$\cup$

$$d\Omega_f = R\text{-module generated by } x_i \frac{\partial \nu}{\partial x_i}, \nu \in \Omega_f, i = 1, \dots, n$$

$$\Omega_f / d\Omega_f \cong H^n_{DR}(\mathbb{T}^n \setminus X_f) \quad \text{(Griffiths, Batyrev)}^1$$

$$\Omega_f \ni \frac{h(\mathbf{x})}{f(\mathbf{x})^m} \mapsto \frac{h(\mathbf{x})}{f(\mathbf{x})^m} \frac{dx_1}{x_1} \dots \frac{dx_n}{x_n}$$

$$d\Omega_f \leftrightarrow \text{ exact forms}$$

$$\Omega_f(\cdot) = \{m \leq \cdot\} \leftrightarrow \text{ Hodge filtration}$$

[1] when f is Δ-*regular* and R is a field

p-adic Cartier operation

fix p prime and assume that $\cap_{s\geq 1} p^s R = \{0\}$

$$\mathcal{C}_p : \frac{h(\mathbf{x})}{f(\mathbf{x})^m} = \sum_{\mathbf{u}\in C(\Delta-\mathbf{b})} a_{\mathbf{u}} \mathbf{x}^{\mathbf{u}} \mapsto \sum_{\mathbf{u}\in\in C(\Delta-\mathbf{b})} a_{p\mathbf{u}} \mathbf{x}^{\mathbf{u}} \quad \notin \Omega_f$$

Def. A *Frobenius lift* $\sigma : R \to R$ is a ring endomorphism such that $\sigma(r) - r^p \in pR$ for all $r \in R$.

Examples:

- $R = \mathbb{Z}$ with $\sigma = id$
- $R = \mathbb{Z}[t]$ with $\sigma(r(t)) = r(t^p)$

Lemma. For $\frac{h(\mathbf{x})}{f(\mathbf{x})^m} = \sum a_{\mathbf{u}} \mathbf{x}^{\mathbf{u}}$, the series $\sum a_{p\mathbf{u}} \mathbf{x}^{\mathbf{u}}$ can be approximated p-adically by rational functions with powers of $f^\sigma(\mathbf{x})$ in the denominator.

Here f^σ is f with σ applied to its coefficients. We thus have

$$\mathcal{C}_p(\Omega_f) \subset \widehat{\Omega}_{f^\sigma} = p\text{-adic completion of } \Omega_{f^\sigma}.$$

Properties of the p-adic Cartier operation

The R-linear operation

$$\mathcal{C}_p : \widehat{\Omega}_f \to \widehat{\Omega}_{f^\sigma}, \quad \sum a_{\mathbf{u}} \mathbf{x}^{\mathbf{u}} \mapsto \sum a_{p\mathbf{u}} \mathbf{x}^{\mathbf{u}}$$

- (surprisingly) is independent of the choice of vertex $\mathbf{b} \in \Delta$ at which the formal expansion is done
- descends to cohomology:

$$\mathcal{C}_p \circ x_i \frac{\partial}{\partial x_i} = p\, x_i \frac{\partial}{\partial x_i} \circ \mathcal{C}_p \Rightarrow \quad \mathcal{C}_p(d\widehat{\Omega}_f) \subset d\widehat{\Omega}_{f^\sigma},$$
$$\mathcal{C}_p : \widehat{\Omega}_f / d\widehat{\Omega}_f \to \widehat{\Omega}_{f^\sigma} / d\widehat{\Omega}_{f^\sigma}.$$

- when $R = \mathbb{Z}_p$, trace of $\mathcal{C}_p^s$ counts points on $\mathbb{T}^n \setminus X_f$ over $\mathbb{F}_{p^s}$ for $s \geq 1$

Key theorem 1

$$(\beta_p)_{\mathbf{u},\mathbf{v}\in\Delta} \;=\; \text{coefficient of } \mathbf{x}^{p\mathbf{v}-\mathbf{u}} \text{ in } f(\mathbf{x})^{p-1} \in R^{h\times h}, h = \#(\Delta\cap\mathbb{Z}^n)$$

Theorem (Beukers-V, *Dwork crystals I*). Assume R is p-adically complete and the Hasse–Witt matrix β_p is invertible. Then

$$\widehat{\Omega}_f/\{\text{formal derivatives}\}$$

is a free R-module of rank h where $\frac{\mathbf{x}^{\mathbf{u}}}{f(\mathbf{x})}$, $\mathbf{u} \in \Delta \cap \mathbb{Z}^n$ is a basis.

Here *formal derivaties* denotes the submodule

$$\begin{aligned}\mathcal{F} &= \left\{\omega = \sum a_{\mathbf{u}}\mathbf{x}^{\mathbf{u}} \in \widehat{\Omega}_f \;\middle|\; \forall\mathbf{u} \quad a_{\mathbf{u}} \in g.c.d.(u_1,\ldots,u_n)R\right\}\\ &= \widehat{\Omega}_f \;\cap\; R\text{-module generated by } x_i\frac{\partial}{\partial x_i}\sum b_{\mathbf{u}}\mathbf{x}^{\mathbf{u}}\\ &= \left\{\omega = \sum a_{\mathbf{u}}\mathbf{x}^{\mathbf{u}} \in \widehat{\Omega}_f \;\middle|\; \forall s\geq 1 \quad \mathcal{C}_p^s(\omega) \in p^s\widehat{\Omega}_{f^{\sigma^s}}\right\}.\end{aligned}$$

We note that $\mathcal{C}_p(\mathcal{F}) \subset p\mathcal{F}$ and so the Cartier operation descends to the free quotients $\mathcal{C}_p : \widehat{\Omega}_f/\mathcal{F} \to \widehat{\Omega}_{f^\sigma}/\mathcal{F}$. Can we determine its matrix?

Congruences

Let $\Lambda \in R^{h\times h}$ be the matrix of $\mathcal{C}_p : \widehat{\Omega}_f/\mathcal{F} \to \widehat{\Omega}_{f^\sigma}/\mathcal{F}$:

$$\mathcal{C}_p\left(\frac{\mathbf{x}^{\mathbf{u}}}{f(\mathbf{x})}\right) = \sum_{\mathbf{v}\in\Delta} \Lambda_{\mathbf{uv}} \frac{\mathbf{x}^{\mathbf{v}}}{f^\sigma(\mathbf{x})} \mod p\mathcal{F}.$$

Pick $\mathbf{w} \in C(\Delta - \mathbf{b})$, $s \geq 1$ and read expansion coefficients at $p^{s-1}\mathbf{w}$ in the above identity: vectors

$$(\alpha_s)_{\mathbf{v}\in\Delta} = \text{ coefficient at } \mathbf{x}^{p^s\mathbf{w}} \text{ in } \frac{\mathbf{x}^{\mathbf{v}}}{f(\mathbf{x})}$$

satisfy [2]

$$\alpha_s \equiv \Lambda\, \alpha_{s-1}^\sigma \mod p^s.$$

[2] This result is a version of N. Katz's *Internal reconstruction of unit-root F-crystals via expansion coefficients* (1985).

Application: Gauss' congruences

$$f(\mathbf{x}) = \sum f_{\mathbf{v}} \mathbf{x}^{\mathbf{v}} \in \mathbb{Z}[x_1^{\pm 1}, \ldots, x_n^{\pm 1}], \qquad \Delta \cap \mathbb{Z}^n = \{vertices\}$$

$$p \nmid f_{\mathbf{v}} \quad \forall \mathbf{v}$$

In this case $\Lambda = Id$, that is $\mathcal{C}_p$ is identity on $\widehat{\Omega}_f/\mathcal{F}$. Therefore for any $h(\mathbf{x})$ with $supp(h) \subset \Delta$ the expansion coefficints

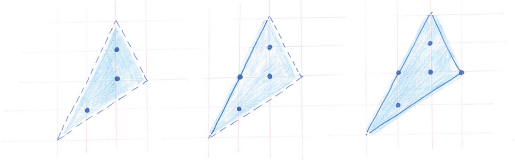
$$\frac{\mathbf{x}^{\mathbf{v}}}{f(\mathbf{x})} = \sum_{\mathbf{w} \in C(\Delta - \mathbf{b})} a_{\mathbf{w}} \mathbf{x}^{\mathbf{w}}$$

satisfy

$$a_{\mathbf{w}} \equiv a_{\mathbf{w}/p} \mod p^{ord_p(\mathbf{w})}.$$

A version

$\mu \subset \Delta$ is called *open* if $\Delta \setminus \mu$ is a union of faces



Then the Cartier operation preserves submodules

$$\Omega_f(\mu) = \left\{ \frac{h(\mathbf{x})}{f(\mathbf{x})^m} \;\middle|\; \begin{array}{l} m \geq 1, h \in R[x_1^{\pm 1}, \ldots, x_n^{\pm 1}] \\ supp(h) \subset m\mu \end{array} \right\},$$

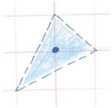
that is $\mathcal{C}_p : \widehat{\Omega}_f(\mu) \to \widehat{\Omega}_{f^\sigma}(\mu)$. If the Hasse-Witt submatrix $\beta_p(\mu) \subset \beta_p$ is invertible, one has

$$\widehat{\Omega}_f(\mu)/\{\text{formal derivatives}\} \equiv \oplus_{\mathbf{u} \in \mu \cap \mathbb{Z}^n} R \frac{\mathbf{x}^{\mathbf{u}}}{f(\mathbf{x})}.$$

Application: Dwork's congruences

$$g \in \mathbb{Z}[x_1^{\pm 1}, \ldots, x_n^{\pm 1}], \quad \Delta^\circ \cap \mathbb{Z}^n = \{\mathbf{0}\}$$

$$\gamma(t) = \sum_{k=0}^{\infty} c_k t^k, \quad c_k = \text{ const. term of } g(\mathbf{x})^k$$



Take $f(\mathbf{x}) = 1 - t\, g(\mathbf{x}),\ \mu = \Delta^\circ$.
The 1×1 Hasse–Witt submatrix is

$$\beta_p(t) = \text{ const. term of } (1 - tg(\mathbf{x}))^{p-1} = \sum_{k=0}^{p-1} (-1)^k \binom{p-1}{k} c_k t^k.$$

Take $R = \mathbb{Z}[t, \beta_p(t)^{-1}]\widehat{\ }$. Here $\widehat{\Omega}_f(\mu)/\mathcal{F}$
is of rank 1, and the respective Cartier matrix is given by

$$\Lambda = \frac{\gamma(t)}{\gamma(t^\sigma)} \in R.$$

Note: $\beta_p(t) \equiv \gamma_p(t) \mod p$, so $R = \mathbb{Z}[t, \gamma_p(t)^{-1}]\widehat{\ }$.

§Supercongruences

Theorem (Beukers-V, *Dwork crystals III*)[3] Let $1 \leq k < p$. Assume that R is p-adically complete and the k'th *Hasse–Witt condition* is satisfied. Then

$$\widehat{\Omega}_f = \Omega_f(k) \oplus \mathcal{F}_k,$$

where

$$\Omega_f(k) = \text{free } R\text{-module generated by } \tfrac{\mathbf{x}^{\mathbf{u}}}{f(\mathbf{x})^k},\ \mathbf{u} \in k\Delta \cap \mathbb{Z}^n$$

and

$$\begin{aligned}
\mathcal{F}_k &= \left\{ \omega = \sum a_{\mathbf{u}} \mathbf{x}^{\mathbf{u}} \in \widehat{\Omega}_f \,\middle|\, \forall \mathbf{u} \quad a_{\mathbf{u}} \in g.c.d.(u_1, \ldots, u_n)^k R \right\} \\
&= \left\{ \omega = \sum a_{\mathbf{u}} \mathbf{x}^{\mathbf{u}} \in \widehat{\Omega}_f \,\middle|\, \forall s \geq 1 \quad \mathcal{C}_p^s(\omega) \in p^{ks} \widehat{\Omega}_{f^{\sigma^s}} \right\} \\
&= \widehat{\Omega}_f \ \cap \ R\text{-module generated by } x_{i_1} \frac{\partial}{\partial x_{i_1}} \ldots x_{i_k} \frac{\partial}{\partial x_{i_k}} \sum b_{\mathbf{u}} \mathbf{x}^{\mathbf{u}}
\end{aligned}$$

is the submodule of *formal kth partial derivatives*.

[3] There is a version for $\mu \subset \Delta$ as well.

A simple example

$$f(\mathbf{x}) = (1 - x_1)(1 - x_2) - t\, x_1 x_2, \quad R = \mathbb{Z}[t, 1/t]^{\widehat{}}$$

$$\mathcal{C}_p(1/f) = 1/f^{\sigma} \mod p\mathcal{F}_1$$

$$\mathcal{C}_p(1/f) = 1/f^{\sigma} + \log\left(\frac{t^{\sigma}}{t^p}\right) \theta(1/f)^{\sigma} \mod p^2\mathcal{F}_2$$

$$\theta = t\frac{d}{dt}$$

Note: the Frobenius lift $t^{\sigma} = t^p$ is special in the sense that it turns $1/f$ into an “eigenvector” of $\mathcal{C}_p$ modulo $\mathcal{F}_2$. After Dwork, we call such Frobenius lifts *excellent*.

For the excellent Frobenius lift expansion coefficients of $1/f = \sum_{\mathbf{v} \in \mathbb{Z}^2_{\geq 0}} a_{\mathbf{v}}(t)\mathbf{x}^{\mathbf{v}}$ satisfy *supercongruences*

$$a_{\mathbf{v}}(t) \equiv a_{\mathbf{v}/p}(t^p) \mod p^{2 ord_p(\mathbf{v})}.$$

Another example: Dwork's families

$$f(\mathbf{x}) = 1 - t\left(x_1 + \dots x_r + \frac{1}{x_1 \dots x_r}\right)$$

$p \nmid 2(r+1) \quad \exists \lambda_0, \lambda_1 \in \mathbb{Z}_p[\![t]\!]$ such that

$$\mathcal{C}_p(1/f) = \lambda_0(t) 1/f^\sigma + \lambda_1(t)\,\theta(1/f)^\sigma \mod p^2\mathcal{F}_2, \quad \theta = t\frac{d}{dt}$$

$\uparrow$ $\uparrow$

depend on σ

Goal: determine excellent Frobenius lifts. That is, find $t^\sigma \in \mathbb{Z}_p[\![t]\!]$ for which $\lambda_1(t) \equiv 0$.

Excellent lifts for Dwork's families

$$f(\mathbf{x}) = 1 - t\,\left(x_1 + \ldots x_r + \frac{1}{x_1 \ldots x_r}\right), \quad \theta = t\frac{d}{dt}$$

$$L = \theta^r - ((r+1)t)^{r+1}(\theta+1)\ldots(\theta+r), \quad L(1/f) \in d\Omega_f$$

Picard–Fuchs differential operator

$$\Omega_f(\Delta^\circ)/d\Omega_f \cong \oplus_{i=0}^{r-1} R\,\theta^i(1/f), \quad R = \mathbb{Z}[t,(r+1)^{-1}(1-(r+1)t)^{-1}]$$

Solutions to $Ly = 0$:

$$y_0(t) = \sum_{n\geq 0} \frac{((r+1)n)!}{(n!)^{r+1}} t^{(r+1)n} = \frac{1}{(2\pi i)^r} \oint \ldots \oint \frac{1}{f(\mathbf{x})} \frac{dx_1}{x_1} \ldots \frac{dx_r}{x_r}$$

$$y_1(t) = \log(t) y_0(t) + G(t) \quad \text{with unique } G(t) \in t\mathbb{Q}[\![t]\!]$$

$\ldots$

$$q(t) = \exp\left(\frac{y_1(t)}{y_0(t)}\right) = t\exp\left(\frac{G(t)}{y_0(t)}\right) \in t + t^2\mathbb{Q}[\![t]\!]$$

is called the *canonical coordinate*

Excellent lifts for Dwork's families

$$f(\mathbf{x}) = 1 - t\left(x_1 + \dots x_r + \frac{1}{x_1 \dots x_r}\right), \quad \theta = t\frac{d}{dt}$$

$$L = \theta^r - ((r+1)t)^{r+1}(\theta+1)\dots(\theta+r), \quad L(1/f) \in d\Omega_f$$

$$y_0(t) = \sum_{n \geq 0} \frac{((r+1)n)!}{(n!)^{r+1}} t^{(r+1)n}, \quad y_1(t) = \log(t) y_0(t) + G(t)$$

$$q(t) = \exp\left(\frac{y_1(t)}{y_0(t)}\right) = t\exp\left(\frac{G(t)}{y_0(t)}\right) \quad \text{canonical coordinate}$$

Theorem(Beukers-V, 2021) Assume that $p \nmid 2(r+1)$. Then

(i) $q(t) \in t + t^2\mathbb{Z}_p[\![t]\!] \qquad (\Rightarrow \mathbb{Z}_p[\![t]\!] = \mathbb{Z}_p[\![q]\!])$,

(ii) the excellent Frobenius lift σ is given by $q \mapsto q^p$,

(iii) $t^\sigma = t(q^p) \in \mathbb{Z}_p[\![t]\!]$ belongs to $\mathbb{Z}[t, 1/hw_1(t), 1/hw_2(t)]^\wedge$, where polynomials $hw_1(t), hw_2(t)$ are the 1st and 2nd Hasse–Witt determinants.

Modular excellent lifts

E.g. $r = 2$, $f(\mathbf{x}) = 1 - t\left(x_1 + x_2 + \dfrac{1}{x_1 x_2}\right)$
$t(q) = q - 5q^4 + 32q^7 - 198q^{10} + \dots$ modular function of level 3

In §7 of 'p-adic cycles', Dwork shows that for the modular j-function

$$j(q) = \frac{1}{q} + 744 + 196884\,q + \dots$$

if one expresses $j(q^p) = F(j(q))$ then function F is a p-adic analytic function on $\mathbb{C}_p \setminus \{\beta_1, \dots, \beta_r\}$ where β_i are representatives of the j-invariants of supersingular elliptic curves in characteristic p. He calls this fact Deligne's theorem and proves it using the algebraic relation of degree $p + 1$ between modular functions $j(q)$ and $j(q^p)$. He gives a simlar proof to the modulus $\lambda(q) = 16q - 128q^2 + 704q^3 + \dots$ of the Legendre family of elliptic curves $y^2 = x(x-1)(x-\lambda)$.

In our setting the roots of the 1st Hasse-Witt polynomial $hw_1(t)$ modulo p correspond to supersingular fibres of the family $f(\mathbf{x}) = 0$. Part (iii) of our theorem shows that a similar result holds for non-modular families (when $r \geq 4$) but in general one also needs to exclude the roots of the second Hasse–Witt polynomial $hw_2(t)$.

Thank you!