MARCH / MARS 2003

IN THIS ISSUE / DANS CE NUMÉRO

Published by / Publié par
The Academy of Science of the Royal Society of Canada
L'Académie des sciences de la Société royale du Canada
c/o Department of Mathematics and Statistics
Carleton University
Ottawa, Ontario, K1S 5B6
Tel/fax: 613-520-2166

25
No 1

C. R. Math. Rep. Acad. Sci. Canada Vol. 25, (1), 2003 pp. 1–6

LIMITING BEHAVIOUR OF THE SUPER-BROWNIAN MOTION WITH SUPER-BROWNIAN IMMIGRATION

WENMING HONG

Presented by Donald A. Dawson, FRSC

RÉSUMÉ. Nous montrons des principes de déviations grandes et modérées pour super mouvement brownien et super mouvement brownien avec immigration, X_t^ϱ, en dimension $d \geq 3$.

Superprocesses in random medium have been received much attention in recent years, see Evans and Perkins [9], Dawson and Fleischmann [3] *etc.*; Hong and Li [14] considered super-Brownian motion with super-Brownian immigration (SBMSBI, for short), where the immigration rate is governed by the trajectory of another super-Brownian motion, and some interesting properties were revealed, see also Hong [11], [12], [13]. We first recall the concept of SBMSBI briefly. Let $C(\mathbb{R}^d)$ denote the space of continuous bounded functions on $\mathbb{R}^d$. We fix a constant $p > d$ and let $\phi_p(x) := (1 + |x|^2)^{-p/2}$ for $x \in \mathbb{R}^d$. Let $C_p(\mathbb{R}^d) := \{f \in C(\mathbb{R}^d) : |f(x)| \leq \text{const} \cdot \phi_p(x)\}$. In duality, let $M_p(\mathbb{R}^d)$ be the space of Radon measures μ on $\mathbb{R}^d$ such that $\langle \mu, f\rangle := \int f(x)\mu(dx) < \infty$ for all $f \in C_p(\mathbb{R}^d)$. We endow $M_p(\mathbb{R}^d)$ with the p-vague topology, that is, $\mu_k \to \mu$ if and only if $\langle \mu_k, f\rangle \to \langle \mu, f\rangle$ for all $f \in C_p(\mathbb{R}^d)$. Then $M_p(\mathbb{R}^d)$ is metrizable. Throughout this paper, λ denotes the Lebesgue measure on $\mathbb{R}^d$.

Suppose that $(w_t, t \geq 0)$ is a standard Brownian motion in $\mathbb{R}^d$ with semigroup $(P_t)_{t\geq 0}$. Given $\{\varrho_t : t \geq 0\}$ a super-Brownian motion with $\varrho_0 = \lambda$, the process $\{X_t^\varrho : t \geq 0\}$ is a super Brownian motion with immigration determined by $\{\varrho_t : t \geq 0\}$ with $X_0^\varrho = \lambda$. We have

$$
\begin{aligned}
(1) \qquad \mathbf{E}\exp\{-\langle X_t^\varrho, f\rangle\} &= \mathbf{E}\left[\mathbf{E}\exp\{-\langle X_t^\varrho, f\rangle\} \mid \{\sigma(\varrho_s, s \leq t)\}\right] \\
&= \mathbf{E}\exp\left\{-\langle \lambda, v(t,\cdot)\rangle - \int_o^t \langle \varrho_s, v(t-s,\cdot)\rangle\, ds\right\} \\
&= \exp\{-\langle \lambda, v(t,\cdot)\rangle - \langle \lambda, u(t,\cdot)\rangle\}
\end{aligned}
$$

where $u(\cdot,\cdot)$ is the unique mild solution of the equation

$$
(2) \qquad \begin{cases} \dot{u}(s) = \Delta u(s) - u^2(s) + v(s), \quad 0 \leq s \leq t \\ u(0) = 0 \end{cases}
$$

Received by the editors on July 1, 2002.

Supported by the National Natural Science Foundation of China (Grants No. 10101005 and No. 10121101) and the NSERC research grant (No. 7750) of D. Dawson.

AMS subject classification: 60J80, 60F05.

Keywords: large deviation, moderate deviation, super-Brownian motion, random medium, immigration.

and $v(\cdot,\cdot)$ is the mild solution of the equation

$$\begin{cases} \dot{v}(t) = \Delta v(t) - v^2(t) \\ v(0) = f. \end{cases} \tag{3}$$

The process $\{X_t^\varrho : t \geq 0, \mathbf{Q}\}$ is what we call *super-Brownian motion with super-Brownian immigration* (SBMSBI), for details, see Hong and Li [14] and Hong [13], and it may be considered as one kind of multitype superprocesses, see also Dawson, Gorostiza and Li [4], Gorostiza and Lopez-Mimbela [10] and Li [19]. For the general theory of superprocesses, we refer to Dawson [2]. The central limit theorems for SBMSBI and its occupation time were proved in Hong and Li [14] and Hong [12]. Now we will focus on the large deviation principles for the SBMSBI. A full description of this work will appear elsewhere. (Preprints may be obtained from the author.)

1. **Large deviations.** We fix $f \in C_p^+(\mathbb{R}^d)$ satisfying $\langle \lambda, f \rangle = 1$. Let

$$\mathbf{W}(t) := \frac{1}{t}\langle X_t^\varrho, f \rangle,$$

and

$$\Lambda_d(t,\theta) := c_d^{-1}(t) \log \mathbf{E} \exp[\theta c_d(t) \mathbf{W}(t)], \tag{4}$$

where the speed function is defined by

$$c_d(t) = \begin{cases} t^{1/2}, & d = 3 \\ t, & d \geq 4. \end{cases}$$

To obtain the LDP, based on the Gartner-Ellis Theorem [5], the key step is to prove the existence of the limit function of $\Lambda_d(t,\theta)$ as $t \to \infty$ and some properties of the limit function.

For this purpose, we will prove that for $d \geq 4$ the following equations

$$\begin{cases} \frac{\partial v(t,x;\theta)}{\partial t} = \Delta v(t,x;\theta) + v^2(t,x;\theta) \\ v(0,x;\theta) = \theta f \end{cases} \tag{5}$$

and

$$\begin{cases} \frac{\partial u(t,x;\theta)}{\partial t} = \Delta u(t,x;\theta) + u^2(t,x;\theta) + v(t,x;\theta) \\ u(0,x;\theta) = 0 \end{cases} \tag{6}$$

admit unique mild solutions $v(t,x;\theta)$ and $u(t,x;\theta)$ respectively when $|\theta| < \frac{1}{4a}$, where a is a positive constant. Furthermore, for $d \geq 5$, there is $\delta > 0$ such that

$$\Lambda(\theta) := \lim_{t\to\infty} \Lambda_d(t,\theta) = \theta + \int_0^\infty \langle \lambda, [v(s,\cdot;\theta)]^2 \rangle \, ds, \tag{7}$$

exists and is stictly convex, continuously differentiable in $|\theta| < \delta < \frac{1}{4a}$ with $\Lambda'(0) = 1$. For $d = 4$, we have

$$\limsup_{t\to\infty} \Lambda_4(t,\theta) \le \theta + \int_0^\infty \langle \lambda, [v(s,\cdot;\theta)]^2 \rangle \, ds + c\beta(\theta)^2 := \Lambda_4(\theta), \tag{8}$$

and $\Lambda_4(\theta)$ is finite, stictly convex, continuously differentiable in $|\theta| < \frac{1}{4a}$. We can obtain an upper large deviation bound for $d = 4$. For $d = 3$, we will prove that the equation

$$\begin{cases} \frac{\partial \overline{u}(t)}{\partial t} = \Delta \overline{u}(t) + \overline{u}^2(t) + \theta p(t) \quad 0 \le t \le 1 \\ u(0) = 0 \end{cases} \tag{9}$$

admit unique mild solutions $\overline{u}(t,\cdot;\theta) \in C([0,1], L^2(R^3))$ for $|\theta| < \frac{3}{16c_3}$, where $c_3 = (2\pi)^{-3/2}$, $p(t) = p(t,x)$ is the transition density function of the Brownian motion. Moreover we will prove that there is $\delta_3 > 0$ such that

$$\Lambda_3(\theta) := \lim_{t\to\infty} \Lambda_d(t,\theta) = \langle \lambda, \overline{u}(1,\cdot;\theta) \rangle,$$

which is continuous differential and strictly convex in $|\theta| < \delta_3 < \frac{3}{16c_3}$ with $\Lambda_3'(0) = 1$. Let $I(\alpha)$ be the Legendre transform of $\Lambda(\theta)$, *i.e.*,

$$I(\alpha) := \sup_{|\theta|<\delta} [\alpha\theta - \Lambda(\theta)] \tag{10}$$

and $I_d(\alpha)$ be the Legendre transform of $\Lambda_d(\theta)$. Then we have:

THEOREM 1.

(1) *For $d \ge 5$, the law of $\mathbf{W}(t)$ under $\mathbf{Q}$ admit the LDP with speed function t and rate function $I(\alpha)$, i.e., there exists a neighborhood O of 1 such that if $U \subset O$ is open and $C \subset O$ is closed, then*

$$\liminf_{t\to\infty} \frac{1}{t} \log \mathbf{Q}\{\mathbf{W}(t) \in U\} \ge - \inf_{\alpha\in U} I(\alpha),$$

$$\limsup_{t\to\infty} \frac{1}{t} \log \mathbf{Q}\{\mathbf{W}(t) \in C\} \le - \inf_{\alpha\in C} I(\alpha).$$

(2) *For $d = 4$, the law of $\mathbf{W}(t)$ under $\mathbf{Q}$ admit the upper large deviation bound with speed function t and rate function $I_4(\alpha)$.*

(3) *For $d = 3$, the law of $\mathbf{W}(t)$ under $\mathbf{Q}$ admit the LDP with speed function $t^{1/2}$ and rate function $I_3(\alpha)$.* ∎

REMARK. (1) The result is a local large deviation, for the steepness of the function $\Lambda_d(\theta)$ and in turn to obtain the full LDP is still open.

(2) At this moment, we only obtain the upper large deviation bound for $d = 4$, but it is enough to ensure the speed function is in fact t. It is an interesting question to look for the lower bound. ∎

In contrast to Lee [18] and Iscoe and Lee [17], where they use the partial differential equation method to get the result, our technique is based on Dynkin's moment formula and the structure of this model to prove the existence of the solutions of the correspondence equations and to get some useful estimates for the solutions, which play a key role in the proofs. For $d = 3$, to prove the L^2-convergence of the evolution equation, with some estimates in hand, the technique is adapted from Iscoe [16].

2. **Moderate deviations.** In the previous section, we obtained a large deviation principle (LDP) with the norming T and speed function

$$c_d(T) = \begin{cases} T^{\frac{1}{2}}, & d = 3 \\ T, & d \geq 4 \end{cases}$$

and we recall that a central limit theorem (CLT) was proved in Hong and Li [14] with the norming

$$a_d(T) = \begin{cases} T^{\frac{3}{4}}, & d = 3 \\ T^{\frac{1}{2}}, & d \geq 4. \end{cases}$$

What can be said about the asymptotic behavior of the SBMSBI with the norming between those of the CLT and LDP? We will fill in this gap and obtain the so called *moderate deviation principles.* We fix $f \in C_p^+(\mathbb{R}^d)$ and let

$$\overline{\mathbf{W}}(T) := a_d(T)^{-1}[\langle X_T^{\varrho}, f\rangle - T\langle \lambda, f\rangle],$$

where the norming

$$a_d(T) = \begin{cases} T^{1-\alpha}, & \alpha \in (0, \frac{1}{4}),\ d = 3 \\ T^{1-\beta}, & \beta \in (0, \frac{1}{2}),\ d \geq 4 \end{cases} \tag{11}$$

and

$$\Lambda_d(T, \theta) := c_d(T)^{-1} \log \mathbf{E} \exp[\theta c_d(T) \overline{\mathbf{W}}(T)], \tag{12}$$

where the speed function is defined by

$$c_d(T) = \begin{cases} T^{\frac{1}{2}-2\alpha}, & \alpha \in (0, \frac{1}{4}),\ d = 3 \\ T^{1-2\beta}, & \beta \in (0, \frac{1}{2}),\ d \geq 4. \end{cases} \tag{13}$$

Then we prove a LDP for $d \geq 3$:

THEOREM 2. *For $d \geq 3$, $\alpha \in (0, \frac{1}{4})$, $\beta \in (0, \frac{1}{2})$, define*

$$K_d = \begin{cases} 2(4\pi)^{-3/2}/3 \cdot \langle \lambda, f\rangle, & d = 3 \\ (4\pi)^{-2} \cdot \langle \lambda, f\rangle + \int_0^{\infty} dr \int f(y) P_r f(y)\, dy, & d = 4 \\ \int_0^{\infty} dr \int f(y) P_r f(y)\, dy, & d \geq 5 \end{cases} \tag{14}$$

and $I(x) = \frac{x^2}{4K_d}$, $|x| < \frac{2K_d}{4a}$. *The law of* $\overline{\mathbf{W}}(T)$ *under* $\mathbf{Q}$ *satisfies the LDP with speed function* $c_d(T)$ *and rate function* $I(x)$, *i.e., let* $O := \{x \in R^d, |x| < \frac{2K_d}{4a}\}$, *for any* $U \subset O$ *open and* C *closed,*

$$\liminf_{T\to\infty} c_d(T)^{-1} \log \mathbf{Q}\{\overline{\mathbf{W}}(T) \in U\} \geq -\inf_{x\in U} I(x),$$

$$\limsup_{T\to\infty} c_d(T)^{-1} \log \mathbf{Q}\{\overline{\mathbf{W}}(T) \in C\} \leq -\inf_{x\in C} I(x). \quad \blacksquare$$

REMARK 1. In other words, we have

(i) For $d = 3$, $\alpha \in (0, \frac{1}{4})$,

$$\liminf_{T\to\infty} T^{2\alpha-\frac{1}{2}} \log \mathbf{Q}\{T^{-1}\langle X_T^\varrho, f\rangle - \langle \lambda, f\rangle \in T^{-\alpha}U\} \geq -\inf_{x\in U} I(x),$$

and

$$\limsup_{T\to\infty} T^{2\alpha-\frac{1}{2}} \log \mathbf{Q}\{T^{-1}\langle X_T^\varrho, f\rangle - \langle \lambda, f\rangle \in T^{-\alpha}U\} \leq -\inf_{x\in C} I(x).$$

(ii) For $d \geq 4$, $\beta \in (0, \frac{1}{2})$,

$$\liminf_{T\to\infty} T^{2\beta-1} \log \mathbf{Q}\{T^{-1}\langle X_T^\varrho, f\rangle - \langle \lambda, f\rangle \in T^{-\beta}U\} \geq -\inf_{x\in U} I(x),$$

and

$$\limsup_{T\to\infty} T^{2\beta-1} \log \mathbf{Q}\{T^{-1}\langle X_T^\varrho, f\rangle - \langle \lambda, f\rangle \in T^{-\beta}U\} \leq -\inf_{x\in C} I(x).$$

where $T^{-b}A := \{T^{-b}x : x \in A\}$.

REMARK 2. Corresponding to $\alpha = \frac{1}{4}$, $\beta = \frac{1}{2}$, we arrive at a central limit theorem (CLT) for $\overline{\mathbf{W}}(T)$ with norming

$$a_d(T) = \begin{cases} T^{\frac{3}{4}}, & d = 3 \\ T^{\frac{1}{2}}, & d \geq 4. \end{cases}$$

See Hong and Li [14]. Similarly, corresponding to $\alpha = 0$, $\beta = 0$, we got a large deviation principle (LDP) in last section for $\overline{\mathbf{W}}(T)$ with norming T and speed function

$$c_d(T) = \begin{cases} T^{\frac{1}{2}}, & d = 3 \\ T, & d \geq 4. \end{cases}$$

Theorem 1.1 fills in the gap between the CLT and LDP, and we call it the moderate deviation principle (MDP).

REMARK 3. It should be pointed out that there is no "log" term in our norming and speed functions, which is diferent from the ordinary super-Brownian motion (see Iscoe [15], Iscoe and Lee [17] and Lee [18]). Intuitively, the random immigration "smooth" the critical dimension in our model SBMSBI.

ACKNOWLEDGMENT. The author thanks Professor D. Dawson for his valuable suggestions and comments.

REFERENCES

1. D. A. Dawson, *The critical measure diffusion process.* Z. Wahrsch. verw. Geb. **40**(1977), 125–145.
2. ———, *Measure-valued Markov processes.* Springer Lecture Notes in Math. **1541** (1993), 1–260.
3. D. A. Dawson and K. Fleischmann, *A continuous super-Brownian motion in a super-Brownian medium.* J. Theoret. Probab. **10**(1997), 213–276.
4. D. A. Dawson, L. G. Gorostiza and Z. H. Li, *Non-local branching superprocesses and some related models.* Acta Appl. Math., 2002, to appear.
5. A. Dembo and O. Zeitouni, *Large Deviations Techniques and Applications.* Springer, 1998.
6. E. B. Dynkin, *Superprocesses and their linear additive functionals.* Trans. Amer. Math. Soc. **314**(1989), 255–282.
7. ———, *An Introduction to Branching Measure-valued Processes.* Amer. Math. Soc., Providence, RI, 1994.
8. R. S. Ellis, *Entropy, Large Deviations and Statistical Mechanics.* Springer, New York, 1985.
9. S. N. Evans and P. A. Perkins, *Measure-valued branching diffusions with singular interactions.* Canad. J. Math. **46**(1994), 120–168.
10. L. G. Gorostiza and J. A. Lopez-Mimbela, *The multitype measure branching process.* Adv. Appl. Probab. **22**(1990), 49–67.
11. W. M. Hong, *Ergodic theorem for the two-dimensional super-Brownian motion with super-Brownian immigration.* Progr. Natur. Sci. (English Ed.) **10**(2000), 111–116.
12. ———, *Longtime behavior for the occupation time of super-Brownian motion with random immigration.* Stoch. Process. Appl., 2002, to appear.
13. ———, *Large deviations for super-Brownian motion with super-Brownian immigration.* Submitted, 2001.
14. W. M. Hong and Z. H. Li, *A central limit theorem for the super-Brownian motion with super-Brownian immigration.* J. Appl. Probab. **36**(1999), 1218–1224.
15. I. Iscoe, *A weighted occupation time for a class of measure-valued critical branching Brownian motion.* Probab. Theory Relat. Fields **71**(1986), 85–116.
16. ———, *Ergodic theory and a local occupation time for measure-valued critical branching Brownian motion.* Stochastics **18**(1986), 197–243.
17. I. Iscoe and T. Y. Lee, *Large deviations for occupation times of measure-valued branching Brownian motions.* Stochastics Stochastics Rep. **45**(1993), 177–209.
18. T. Y. Lee, *Some limit theorems for super-Brownian motion and semilinear differential equations.* Ann. Probab. **21**(1993), 979–995.
19. Z. H. Li, *A note on the multitype measure branching process.* Adv. Appl. Probab. **24**, 496–498.
20. Z. K. Wang, *Power series expansion for superprocesses.* Acta. Math. Sci. (Chinese) **10**(1990), 361–364.
21. D. V. Widder, *The Laplace Transform.* Princeton University Press, 1941.

Department of Mathematics
Beijing Normal University
Beijing 100875
P.R.China
email: wmhong@bnu.edu.cn
and
School of Mathematics and Statistics
Carleton University
Ottawa, Ontario
K1S 5B6
email: hongw@math.carleton.ca

C. R. Math. Rep. Acad. Sci. Canada Vol. 25, (1), 2003 pp. 7–12

DÉCOMPOSITION D'UN PREMIER $Q \equiv 1 + 2^M \pmod{2^{M+1}}$ DANS LES SOUS-EXTENSIONS DE $\mathbb{Q}(\zeta_{2^N})$, $N, M \geq 2$

SAÏD GANNOUKH

Présenté par M. Ram Murty, MSRC

RÉSUMÉ. On se propose, dans un premier temps, de montrer qu'un nombre premier $q \equiv 1 + 2^m \pmod{2^{m+1}}$ se décompose en 2^{l-1} ($l = \min(m, n)$) premiers distincts du corps cyclotomique $\mathbb{Q}(\zeta_{2^n})$, pour tout $n, m \geq 2$, et dans un deuxième temps on détermine la décomposition d'un tel premier dans les sous-extensions de $\mathbb{Q}(\zeta_{2^n})$.

ABSTRACT. We prove, first, that every prime number $q \equiv 1 + 2^m \pmod{2^{m+1}}$ splits into 2^{l-1} ($l = \min(m, n)$) distinct primes of the cyclotomic field $\mathbb{Q}(\zeta_{2^n})$, for all $n, m \geq 2$. In a second time, we determine the decomposition of such a prime in the subfields of $\mathbb{Q}(\zeta_{2^n})$.

1. **Sous-corps de $\mathbb{Q}(\zeta_{2^n})$, $n \geq 2$.** Dans cette section nous déterminons les sous-corps du corps cyclotomique $\mathbb{Q}(\zeta_{2^n})$, $n \geq 2$. On note $L_n = \mathbb{Q}(\zeta_{2^n})$. Le cas $n = 2$ se réduit à $L_2 = \mathbb{Q}(i)$ dont les sous-corps sont triviaux. Nous supposerons alors que $n \geq 3$. On a:

THÉORÈME 1.1. *Soit $n \geq 3$ fixé. Les sous-corps de L_n de degré relatif égal à 2 sont K_{n-1}, L_{n-1} et K'_{n-1}, où $K_{n-1} = \mathbb{Q}(\theta_n)$ et $K'_{n-1} = \mathbb{Q}(\theta'_n)$, avec $\theta_n = \zeta_{2^n} + \zeta_{2^n}^{-1}$, et $\theta'_n = \zeta_{2^n} - \zeta_{2^n}^{-1}$.*

PREUVE. On note $G(m)$ le groupe multiplicatif $(\mathbb{Z}/m\mathbb{Z})^*$ pour $m > 1$ entier. On sait que le groupe de Galois du corps cyclotomique $L_n = \mathbb{Q}(e^{2i\pi/m})$ est isomorphe au groupe $G(m)$, où l'action de $a \in G(m)$ est $\zeta \mapsto \zeta^a$, ayant posé $\zeta = e^{2i\pi/m}$. En particulier, le groupe de Galois du corps L_n est isomorphe à $G_n := G(2^n)$; le groupe G_n ($n \geq 3$) est représenté par les éléments $\pm 5^k$, pour $0 \leq k < 2^{n-2}$, et est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z}$. Les sous-corps $\mathcal{K}$ de L_n tels que $[L_n : \mathcal{K}] = 2$ correspondent aux éléments d'ordre 2 de G_n et admettent pour représentants $\alpha_1 = -1$, $\alpha_2 = 5^{2^{n-3}}$ et $\alpha_3 = -5^{2^{n-3}}$. Notons $\mathcal{K}_j$ le sous-corps de L_n laissé invariant par le groupe $H_j = \{1, \alpha_j\}$ pour $j = 1, 2$ et 3; et ψ_j la surjection canonique $G_n \to G_n/H_j$ où G_n/H_j est d'ordre 2^{n-2}. Posons $\zeta_n = e^{2i\pi/2^n}$ pour simplifier les notations. Pour $j = 1$, l'élément $\psi_j(5)$ est d'ordre 2^{n-2} dans G_n/H_1, qui est cyclique. Le corps $\mathcal{K}_1$ est égal à $\mathbb{Q}(\zeta_n + \zeta_n^{-1}) = K_{n-1}$; donc $\mathcal{K}_1 = \mathbb{Q}\big(\cos(2\pi/2^n)\big)$ est le sous-corps réel maximal de L_n et est cyclique. Pour $j = 2$, l'élément $\psi_j(5)$ est d'ordre 2^{n-3} dans G_n/H_j qui n'est pas cyclique pour $n > 3$. Le corps $\mathcal{K}_2$ est égal à $\mathbb{Q}(\zeta_n^2)$, donc $\mathcal{K}_2 = L_{n-1}$. Pour $j = 3$, l'élément

Reçu le 10 juin, 2002.
Classification (de l'AMS): 11R18, 11R27.

$\beta = \psi_j(5)$ vérifie $\beta^{2^{n-3}} = -1$; il est donc d'ordre 2^{n-2} dans G_n/H_3 qui est cyclique. Le corps K_3 est égal à $\mathbb{Q}(\zeta_n - \zeta_n^{-1})$, donc $K_3 = \mathbb{Q}\big(i\sin(2\pi/2^n)\big) = K'_{n-1}$ est un sous-corps cyclique de L_n. ∎

REMARQUES. 1) $L_n = \mathbb{Q}(i, \theta_n) = \mathbb{Q}(i, \theta'_n)$.

2) Le sous-corps K'_{n-1} ne peut contenir un sous-corps imaginaire propre car K'_{n-1} est une extension cyclique imaginaire de degré une puissance de 2. ∎

Pour la commodité d'écriture, on pose $L_1 = K_1 = \mathbb{Q}$ et $K'_1 = \mathbb{Q}(i)$. Avec les notations du théorème 1.1, on vérifie aisément que:

$$\theta_n = \sqrt{2 + \theta_{n-1}} \quad \text{et} \quad \theta'_n = i\sqrt{2 - \theta_{n-1}}.$$

Avec ces deux relations de récurrence on en déduit que

$$K_{n-2} \subset K_{n-1} \cap K'_{n-1}, \quad \forall n \geq 3,$$

et en comparant les degrés, on montre que $K_{n-2} = K_{n-1} \cap K'_{n-1}$. Les autres sous-corps vérifient:

$$K_{j-1} = K_j \cap K'_j \quad (2 \leq j < n) \quad \text{et} \quad L_{j-1} \subset L_j, \quad (2 \leq j \leq n).$$

Nous traduisons ces faits par le diagramme à la page suivante.

2. **Décomposition dans les sous-corps L_j.** Soit $n, m \geq 2$. Posons $l = \min(m, n)$. Nous démontrons le théorème suivant:

THÉORÈME 2.1. *Un nombre premier $q \equiv 1 + 2^m \pmod{2^{m+1}}$ se décompose en 2^{l-1} premiers distincts dans le corps cyclotomique $L_n = \mathbb{Q}(\zeta_{2^n})$.*

Pour la démonstration du théorème 2.1 on a besoin du lemme suivant:

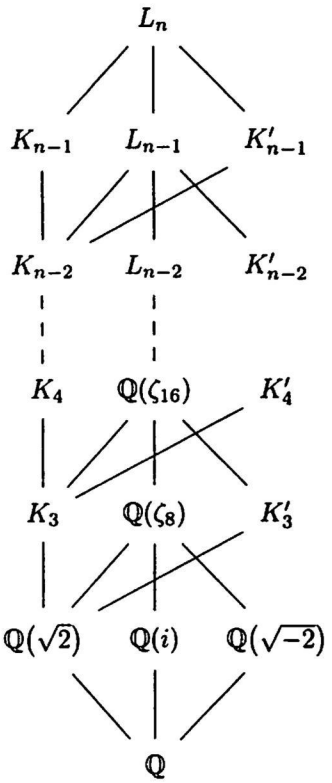
LEMME 2.1. *Soit $n > m$. Si $q \equiv 1 + 2^m \pmod{2^{m+1}}$ alors $q^{2^{n-m}} \equiv 1 \pmod{2^n}$ et $q^{2^{n-m-1}} \equiv 1 + 2^{n-1} \pmod{2^n}$.*

PREUVE DU LEMME 2.1. La preuve se fait par récurrence sur n.

Pour $n = m + 1$, $q \equiv 1 + 2^m \pmod{2^{m+1}} \Rightarrow q \equiv 1 \pmod{2^m} \Rightarrow q^2 \equiv 1 \pmod{2^{m+1}} \Rightarrow q^2 \equiv 1 \pmod{2^n}$ et $q \equiv 1 + 2^m \pmod{2^{m+1}}$.

Supposons que le lemme est vrai pour $n \geq m + 1$, montrons qu'il l'est pour $n + 1$. On a

$$q^{2^{n-m}} \equiv 1 \pmod{2^n} \Longrightarrow (q^{2^{n-m}})^2 \equiv 1 \pmod{2^{n+1}},$$



d'où $q^{2^{n+1-m}} \equiv 1 \pmod{2^{n+1}}$. D'autre part, par hypothèse de récurrence,

$$q^{2^{n-m-1}} \equiv 1 + 2^{n-1} \pmod{2^n} \Longrightarrow 2^n \mid (q^{2^{n-m-1}} - 2^{n-1} - 1),$$

$$2^{n+1} \mid (q^{2^{n-m-1}} - 2^{n-1} - 1)(q^{2^{n-m-1}} + 2^{n-1} + 1),$$

$$2^{n+1} \mid q^{2^{n-m}} - (2^{n-1} + 1)^2,$$

$$2^{n+1} \mid q^{2^{n-m}} - 2^n - 1 - 2^{2(n-1)}.$$

Comme $2^{n+1} \mid 2^{2(n-1)}$ pour $n \geq 3$, alors $2^{n+1} \mid q^{2^{n-m}} - 2^n - 1$. Par conséquent $q^{2^{n-m}} \equiv 1 + 2^n \pmod{2^{n+1}}$. ■

PREUVE DU THÉORÈME 2.1. Si $n \leq m$, alors $q \equiv 1 + 2^m \pmod{2^{m+1}} \Rightarrow q \equiv 1 \pmod{2^n}$; donc q se décompose complètement dans le corps cyclotomique L_n [1, théorème 2.13, p. 14] c'est-à-dire en $\phi(2^n) = 2^{n-1}$ idéaux premiers distincts.

Si $n > m$, alors le lemme 2.1 entraîne que l'entier $f_{n,m} = 2^{n-m}$ est le plus petit entier positif tel que $q^{f_{n,m}} \equiv 1 \pmod{2^n}$; et par [1, théorème 2.13, p. 14], q se décompose en $\phi(2^n)/f_{n,m}$ premiers distincts, soit donc $2^{n-1}/2^{n-m} = 2^{m-1}$ idéaux premiers distincts. Ce qui démontre le théorème. ■

REMARQUE. Le théorème 2.1 donne la décomposition dans les sous-corps L_j ($j < n$) de L_n car il suffit d'appliquer le théorème 2.1 à L_j. Dans ce cas un nombre premier $q \equiv 1+2^m \pmod{2^{m+1}}$ se décompose en 2^{l_j-1} premiers distincts dans le corps cyclotomique L_j, où $l_j = \min(j, m)$.

Le théorème 2.1 montre en particulier que pour déterminer la décomposition d'un premier $q \equiv 1+2^m \pmod{2^{m+1}}$ dans L_n, $n \geq m$, il suffit de regarder cette décomposition dans le corps cyclotomique L_m. Les idéaux premiers de $\mathbb{Z}[\zeta_{2^n}]$ au-dessus de q se déduisent alors par extension des idéaux premiers de $\mathbb{Z}[\zeta_{2^m}]$ au-dessus de q.

2.1. Applications et exemples. Notons $\Phi_n(X) = X^{2^{n-1}} + 1 = \mathrm{Irr}(\zeta_{2^n}, \mathbb{Q})$. Considérons le cas où $m = 3$; d'après le théorème 2.1, un premier $q \equiv 9 \pmod{16}$ se décompose en quatre premiers distincts dans $\mathbb{Q}(\zeta_{2^n})$ pour tout $n \geq 3$. Nous allons déterminer explicitement cette décomposition. Pour ce faire, énonçons le lemme suivant:

LEMME 2.1.1. *Soit $q \equiv 9 \pmod{16}$. Alors il existe $a, b \in \mathbb{Z}$ tels que*

$$a^4 \equiv -1 \pmod{q} \quad \textit{et} \quad a^2 \equiv -b^2 \pmod{q}.$$

PREUVE. Comme $q \equiv 9 \pmod{16}$, 8 divise $q-1$. Or $(\mathbb{Z}/q\mathbb{Z})^*$ est cyclique d'ordre $q-1$, il existe donc $a \in \mathbb{Z}$ d'ordre 8 modulo q; on en déduit que $a^4 \equiv -1 \pmod{q}$. D'autre part, notons que -1 est un résidu quadratique modulo q; il existe alors $x \in \mathbb{Z}$, $x^2 \equiv -1 \pmod{q}$. Finalement, posons $b = ax$, il vient que $a^2 \equiv -b^2 \pmod{q}$. ∎

On utilise le lemme précédent pour factoriser, modulo q, le polynôme cyclotomique $\Phi_n(X)$, on a:

$$\Phi_n(X) \equiv (X^{2^{n-3}} - a)(X^{2^{n-3}} + a)(X^{2^{n-3}} - b)(X^{2^{n-3}} + b) \pmod{q},$$

d'où la décomposition dans $\mathbb{Z}[\zeta_{2^n}]$ ($n \geq 3$) [1, Proposition 2.14]:

$$(q) = (q, \zeta_8 - a)(q, \zeta_8 + a)(q, \zeta_8 - b)(q, \zeta_8 + b)$$

dans $\mathbb{Z}[\zeta_{2^n}]$ ($n \geq 4$).

3. Décomposition dans les sous-corps K_j et K'_j. Soient $n \geq 3$, $m \geq 2$ et $l = \min(m, n)$. Avec les notations du théorème 1.1 de la section 1, on a le théorème suivant:

THÉORÈME 3.1. *Un premier $q \equiv 1 + 2^m \pmod{2^{m+1}}$ se décompose en 2^{l-2} premiers distincts dans K_{n-1} ou K'_{n-1}.*

PREUVE. 1er cas: $n > m$.

Considérons le corps L_n, $n \geq 3$. Soit g_n le nombre des idéaux premiers de K_{n-1} qui figurent dans la décomposition de q. Il s'agit de montrer que $g_n = 2^{m-2}$. On désigne par $f_{K/\mathbb{Q}}$ le degré résiduel de q dans l'extension $K/\mathbb{Q}$.

On sait que

$$f_{K_{n-1}/\mathbb{Q}} \cdot g_n = [K_{n-1} : \mathbb{Q}] = 2^{n-2};$$

or

$$f_{n,m} = f_{L_n/K_{n-1}} \cdot f_{K_{n-1}/\mathbb{Q}} = 2^{n-m},$$

et comme

$$f_{L_n/K_{n-1}} \leqslant [L_n : K_{n-1}] = 2,$$

alors

$$f_{L_n/K_{n-1}} = 1 \quad \text{ou} \quad 2;$$

ceci entraîne que

$$f_{K_{n-1}/\mathbb{Q}} = 2^{n-m} \quad \text{ou} \quad f_{K_{n-1}/\mathbb{Q}} = 2^{n-m-1}.$$

Par suite $g_n = 2^{m-2}$ ou $g_n = 2^{m-1}$.

Montrons par récurrence sur $n > m$ que $g_n = 2^{m-2}$.

Pour $n = m + 1$, si $g_{m+1} = 2^{m-1}$ alors comme $[K_m : \mathbb{Q}] = 2^{m-1}$, q se décompose complètement sur K_m. Or q se décompose complètement sur $\mathbb{Q}(i)$ (car $q \equiv 1 \pmod 4$ pour $m \geq 2$). Donc d'après Hasse [2, Satz 42, p. 59], q se décompose complètement sur $L_{m+1} = \mathbb{Q}(i, \theta_{m+1})$, ce qui est absurde par le théorème 2.1. Donc la propriété est vraie pour $n = m + 1$.

Supposons qu'elle est vraie pour $n > m$ et montrons qu'elle est vraie pour $n + 1$; c'est-à-dire que $g_{n+1} = 2^{m-2}$. L'hypothèse de récurrence entraîne que $g_n = 2^{m-2}$, $f_{K_{n-1}/\mathbb{Q}} = 2^{n-m}$ et $f_{L_n/K_{n-1}} = 1$.

Soit $\tilde{q}$ un idéal premier de K_{n-1} au-dessus de q; par hypothèse de récurrence, $\tilde{q}$ se décompose en deux premiers distincts de L_n. Si $\tilde{q}$ se décompose dans K_n alors par Hasse [2, Satz 42, p. 59], $\tilde{q}$ se décompose complètement dans $L_{n+1} = K_n L_n$; ce qui est absurde car $f_{L_{n+1}/K_{n-1}} = f_{n+1,m}/f_{K_{n-1}/\mathbb{Q}} = 2^{n+1-m}/2^{n-m} = 2$. Donc $\tilde{q}$ est inerte dans K_n; par suite $f_{K_n/K_{n-1}} = 2$, ceci entraîne que $f_{L_{n+1}/K_n} = 1$; d'où $g_{n+1} = 2^{m-2}$. Pour le sous-corps K'_{n-1}, on suit les mêmes étapes en remarquant que $L_{m+1} = \mathbb{Q}(i, \theta'_{m+1})$ et $L_{n+1} = K'_n L_n$.

2ème cas: $m \geq n$.

D'après le théorème 2.1, $f_{n,m} = 1$, par suite $f_{K_{n-1}/\mathbb{Q}} = 1$; par conséquent $g_n = 2^{n-2}$. Le même raisonnement se fait pour K'_{n-1}. ∎

REMARQUE. Le théorème 3.1 donne la décomposition dans les sous-corps K_j et K'_j $(j < n)$ de L_n car il suffit de se placer dans le corps cyclotomique L_{j+1} de façon que K_j ou K'_j soit de degré relatif égal à 2, et d'appliquer le théorème 3.1. Si on pose $l_j = \min(j + 1, m)$, alors un nombre premier $q \equiv 1 + 2^m \pmod{2^{m+1}}$ se décompose en $2^{l_j - 2}$ premiers distincts dans K_j ou dans K'_j. ∎

Le théorème 3.1 montre en particulier que pour déterminer la décomposition d'un premier $q \equiv 1+2^m \pmod{2^{m+1}}$ dans K_{n-1} (resp. dans K'_n), $n \geq m$, il suffit de regarder cette décomposition dans K_{m-1} (rappelons que $K_{m-1} \subset K_n \cap K'_n = K_{n-1}$). Alors les idéaux premiers de $\mathbb{Z}[\theta_n]$ (resp. de $\mathbb{Z}[\theta'_{n+1}]$) au-dessus de q se déduisent par extension des idéaux premiers de $\mathbb{Z}[\theta_m]$ au-dessus de q.

REMERCIEMENT. Je remercie mon directeur de thèse, Maurice Mignotte, pour son aide à la démonstration du théorème 1.1.

RÉFÉRENCES

1. L. C. Washington, *Introduction to cyclotomic fields*. Graduate Texts in Math. **83**, second edition, Springer, New York, 1997.
2. H. Hasse, *Vorlesungen über Klassenkörpertheorie*. Physica-Verlag, Würzburg, 1967.

Institut de Recherche Mathématique Avancée (IRMA)
7, rue René Descartes
F-67084 Strasbourg
France
courriel: gannoukh@math.u-strasbg.fr

C. R. Math. Rep. Acad. Sci. Canada Vol. 25, (1), 2003 pp. 13–18

ON SUBSUMS OF UNITS IN CUBIC NUMBER FIELDS AND TERNARY RECURRENCE SEQUENCES

P. G. WALSH

Presented by David W. Boyd, FRSC

RÉSUMÉ. On considère le problème de déterminer des unités d'un corps de nombres qui admettent des "sous-sommes" qui sont elles-mêmes des unités. Il apparaît que ce problème n'admet que des solutions triviales lorsque le corps de nombres est quadratique et que de nombreuses solutions peuvent être construites lorsque ce corps est composé. D'autre part, il semble plus difficile de trouver des solutions lorsque le degré du corps est premier. En utilisant des théorèmes classiques de Delaunay et Ljunggren qui portent sur les solutions entières de certaines équations cubiques de Thue, on donne une description complète de ces unités dans un corps cubique pur. On en déduit une description complète des solutions de l'équation $U_k = \pm 1$ pour la classe correspondante des suites de récurrence ternaires U_k.

ABSTRACT. The problem of determining units in number fields with unit subsums is posed. It is obvious that only trivial solutions to this problem exist when the number field is quadratic, and that many solutions can be constructed when the degree of the number field over $\mathbf{Q}$ is composite. On the other hand, it seems to be more difficult to find solutions when the degree is prime. Using classical theorems of Delaunay and Ljunggren on integer solutions to certain cubic Thue equations, we give a complete description of solutions in the case of pure cubic number fields. As a consequence, a complete description of solutions to the equation $U_k = \pm 1$ is given for a related class of ternary recurrence sequences.

1. **Introduction.** In this paper we address the problem of determining when a unit u in some order of the ring of integers of a number field $K = \mathbf{Q}(\alpha)$ of degree $n > 1$, given in the form

$$u = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1},$$

has the property that that some proper subsum of u is also a unit.

If $n = 2$, it is clear that the only possible values for u are $\pm(1 \pm \sqrt{2})$. Moreover, for every $n > 1$, the unit $\pm(-1 + 2^{1/n})$ has this property. If the degree n is composite, it is not difficult to construct many solutions to this problem. For example, if u is a unit in the ring of integers of a quadratic field for which $\alpha = \sqrt{u^2 - 1}$ is of degree 4 over $\mathbf{Q}$, then the element $1 + \alpha + \alpha^2$ is a unit in $\mathbf{Q}(\alpha)$, and so are 1 and $1 + \alpha^2$. On the other hand, if $n > 2$ is prime, then it seems to be much more difficult to construct such units. In fact, as our main result

Received by the editors on July 15, 2002.
AMS subject classification: 11R27, 11D25, 11B39.

indicates, this is essentially impossible for pure cubic number fields. We do not have any nontrivial examples of such units for higher degree number fields of prime degree over $\mathbf{Q}$.

The proof of Theorem 1 is based on the determination of integral points on a collection of elliptic curves defined over the rational numbers. There are a number of ways in which one can solve problems of this type. For the cases to be considered here, we will appeal to classical theorems of Delaunay [4] and Ljunggren [5], apart from one case, in which the group structure of the elliptic curve will be used.

THEOREM 1. *Let $d > 1$ denote a positive integer which is not the cube of an integer, and let γ_d denote the fundamental unit in $\mathbf{Z}[d^{1/3}]$. Assume that*

$$u_1 = X + Yd^{1/3} + Zd^{2/3}$$

is a unit in $\mathbf{Z}[d^{1/3}]$. If a proper subsum u_2 of u_1 is a unit, then $u_2 = \pm 1$.

If $d = 2$, then the only solutions are

$$\pm(u_1, u_2) \in \{(-1+\alpha, -1), (1-2\alpha+2\alpha^2, 1), (1+3\alpha-3\alpha^2, 1), (1+\alpha+\alpha^2, 1), (1+100\alpha-80\alpha^2, 1)\}.$$

If $d > 2$, then $\pm u_1 = \gamma_d^k$ for some $1 \le k \le 3$.

As an immediate consequence we have the following result on terms in ternary recurrence sequences. We point out that the upper bound given in this result is sharp, as shown by the example $d = 7$, $\gamma_7 = 2 - 7^{1/3}$.

THEOREM 2. *For d a positive integer which is not a cube, let $\beta_1 = \gamma_d$ denote the fundamental unit in the ring $\mathbf{Z}[d^{1/3}]$, and let β_2, and β_3 denote the algebraic conjugates of β_1. For $k \in \mathbf{Z}$, define a ternary recurrence sequence $\{U_k\}$ by*

$$U_k = \frac{\beta_1^k + \beta_2^k + \beta_3^k}{\beta_1 + \beta_2 + \beta_3}.$$

If $d = 2$ and $U_k = \pm 1$, then $k \in \{-1, 0, 1, 2, 3, 8\}$. If $d > 2$ and $U_k = \pm 1$, then $|k| \le 3$.

It is worth noting that Ballot [1] has recently studied arithmetic properties of ternary recurrence sequences generated as above by the fundamental unit in $\mathbf{Z}[d^{1/3}]$, in the case $d = M^3 \pm 1$.

2. A preliminary result.

We will require the following modification of a theorem of Ljunggren [5] (see also Theorem 6 on p. 225 of [6]). In what follows we retain the definition for γ_d given in the statement of Theorem 1.

LEMMA 1. *Let a, b, c be positive cubefree integers, $a > b \geq 1$, $c \in \{1, 3\}$, $(ab, c) = 1$, together with the assumption that one of a or b is a square. Let $\delta = 1$ if $bc = 1$, and let $\delta = 3$ in all other cases. Define $d = b\sqrt{a}$ (resp. $a\sqrt{b}$) if a (resp. b) is a square. For $(a, b, c) \neq (2, 1, 3)$ the equation*

$$aX^3 + bY^3 = c \tag{1}$$

has at most one integer solution (X, Y), and for this,

$$c^{-1}(Xa^{1/3} + Yb^{1/3})^{\delta} = \gamma_d^k$$

for some $1 \leq k \leq 2$ if $\delta = 3$, and $k = 1$ if $\delta = 1$. The equation $2X^3 + Y^3 = 3$, has only the two integer solutions $(X, Y) = (1, 1), (4, -5)$.

PROOF. Assume without loss of generality that a is a square. The case $\delta = 1$ was proved by Delaunay [4] (see also Theorem 5 on p. 220 of [6]), wherein the exponent $k = 1$ was proved. For all other cases, Ljunggren [5] proved under the hypotheses given, for $(a, b, c) \neq (2, 1, 3)$, that the element $\epsilon = c^{-1}(Xa^{1/3} + Yb^{1/3})^3$ is the fundamental unit in the cubic field $\mathbf{Q}\big((a^2b)^{1/3}\big)$, or its square. Since $a = u^2$ for some integer u, it follows that $\mathbf{Q}\big((ub)^{1/3}\big) = \mathbf{Q}\big((a^2b)^{1/3}\big)$, and hence the result is a consequence of the fact that $\epsilon \in \mathbf{Z}[(ub)^{1/3}]$. For the case $(a, b, c) = (2, 1, 3)$, the result can be easily deduced from the irrationality measure for $2^{1/3}$ given in [2]. Specifically, it is shown, for all integers $p, q \neq 0$, that $|2^{1/3} - \frac{p}{q}| > \frac{1}{4q^{2.5}}$. It follows that $|2X^3 + Y^3| > \sqrt{|X|}$ for all integers X, Y, and hence an integer X in $2X^3 + Y^3 = 3$ satisfies $|X| < 9$ (for example, see p. 153 in [7]). Checking all integers X in this range leads only to the solutions given.

3. Proof of Theorem 1. As above, let d denote a positive integer which is not a cube, $\alpha = d^{1/3}$, and let

$$u = x + y\alpha + z\alpha^2 \in \mathbf{Z}[\alpha].$$

The *norm* $N(u)$ of u is given by

$$N(u) = x^3 + dy^3 + d^2z^3 - 3dxyz. \tag{2}$$

Theorem 1 will be proved by dealing with 6 different cases, depending on the form of u_2, and whether or not $N(u_1) = N(u_2)$. Since $N(-u) = -N(u)$ for any u, we will assume throughout the proof that $N(u_1) = 1$.

CASE I. u_2 has one term and $N(u_1) = N(u_2)$.

In this situation we have $u_2 = 1$, and from equation (2) we see that

$$dY^3 + d^2Z^3 = 3dYZ,$$

and hence

$$Y^3 + dZ^3 = 3YZ. \tag{3}$$

We note that if $Z = 0$ (resp. $Y = 0$), then $Y = 0$ (resp. $Z = 0$), in which case $u_1 = u_2$, contradicting our assumption that u_2 is a proper subsum of u_1. We can henceforth assume in this case that Y and Z are nonzero. We let $g = (Y, Z)$, $y = Y/g$, $z = Z/g$, then (3) becomes

$$g(y^3 + dz^3) = 3yz. \tag{4}$$

We will first deal with the case $d = 2$. We will further deal with the parity of y as separate cases. First assume that y is even. Let $y = 2u$, then (4) becomes $g(4u^3 + z^3) = 3uz$, and since $(4u^3 + z^3, uz) = 1$, it follows that uz divides g, and we see that

$$(g/uz)(4u^3 + z^3) = 3. \tag{5}$$

Therefore, $4u^3 + z^3 = \pm 1, \pm 3$. Applying Lemma 1, we find that the only possiblity is $(u, z) = \pm(1, -1)$. But in this case, $g/uz = -1$, forcing $4u^3 + z^3 = -3$, hence $u = -1$, $z = 1$, and obviously $g = 1$. It follows that $Y = -2$, $Z = 1$, and $u_1 = 1 - 2 \cdot 2^{1/3} + 2^{2/3}$. If y is odd, then $(y^3 + 2z^3, yz) = 1$, and so (4) becomes

$$(g/yz)(y^3 + 2z^3) = 3, \tag{6}$$

from which we see that $y^3 + 2z^3 = \pm 1, \pm 3$. By Lemma 1, and the fact that $g > 0$, equation (6) shows that (y, z, g) is one of $(1, 1, 1)$, $(1, -1, 3)$, $(5, -4, 20)$, from which we deduce that u_1 must be one of the elements given in the statement of the theorem.

We assume henceforth that $d > 2$. Let $(y, d) = y_1$, $y = y_1 y_2$, $d = y_1 d_1$, then $(yz, y^3 + dz^3) = y_1$, and so $y_2 z$ divides g. Put $g_1 = g/(y_2 z)$, then (4) becomes

$$g_1(y_1^2 y_2^3 + d_1 z^3) = 3, \tag{7}$$

and so

$$y_1^2 y_2^3 + d_1 z^3 = \pm c \quad (c = 1, 3).$$

In what follows, let $\delta = 1$ if $y_1 = 1$ or $d_1 = 1$, and $c = 1$, and $\delta = 3$ otherwise. By Lemma 1, we see that

$$\eta = c^{-1}\left(y_2 (y_1^2)^{1/3} + z (d_1)^{1/3}\right)^{\delta} = \gamma_d^k,$$

where $k = 1$ if $\delta = 1$, and $1 \leq k \leq 2$ otherwise, except in the case that $3 = (y_1, d_1)$. If $3 = (y_1, d_1)$, we put $y_3 = y_1/3$ and $d_2 = d_1/3$, in which case (7) becomes

$$g_1(3y_3^2 y_2^3 + d_2 z^3) = 1.$$

In this case we define $\delta = 1$ if $z = 1$, and $\delta = 3$ otherwise. It follows that

$$\eta = \left(y_2(3y_3^2)^{1/3} + z(d_2)^{1/3}\right)^{\delta} = \gamma_d^k,$$

where $k = 1$ if $\delta = 1$, and $1 \leq k \leq 2$ otherwise. Note in this case we have that $\mathbf{Z}[(3^2y_3^4d_2)^{1/3}] = \mathbf{Z}[(3^2y_3d_2)^{1/3}] = \mathbf{Z}[(y_1d_1)^{1/3}] = \mathbf{Z}[d^{1/3}]$. In either case it can be verified that $\eta = u_1^3$ if $\delta = 1$, and $\eta = u_1$ otherwise, showing that in all cases $u_1 = \gamma_d^k$ for some $1 \leq k \leq 3$.

CASE II. u_2 has one term and $N(u_1) = -N(u_2)$.

Once again we assume without loss of generality that $N(u_1) = 1$. Therefore $u_2 = -1$, and so u_1 is of the form $-1 + Yd^{1/3} + Zd^{2/3}$. By equation (2), it follows that

$$dY^3 + d^2Z^3 + 3dYZ = 2,$$

from which it follows that $d = 2$. We therefore obtain

$$Y^3 + 2Z^3 + 3YZ = 1. \tag{8}$$

The substitution

$$V = 16Y^3 + 24YZ - 8, \quad U = -8YZ + 3$$

yields a point (U, V) on the elliptic curve

$$V^2 = U^3 + 21U - 26, \tag{9}$$

which has minimal Weierstrass equation

$$y^2 + xy + y = x^3 - x^2 + x - 1,$$

via the transformation $(x, y) = (4U - 1, 8V + 4U + 4)$. A simple lookup in Cremona's tables [3] shows that the curve defined by (9) is of conductor 54 and has rank 0, and only two points of finite order over $\mathbf{Q}$. Precisely, these two points are $(U, V) = (3, \pm 8)$. It follows that the only possible integer solution to (8) is $(Y, Z) = (1, 0)$, showing that $u_1 = -1 + 2^{1/3}$. Allowing for both possible values of $N(u_2)$, we see that all solutions in this case are $u_1 = \pm(-1 + 2^{1/3})$.

In all of the remaining cases we may assume that $XYZ \neq 0$.

CASE III. $u_2 = X + Y\alpha$ and $N(u_1) = N(u_2)$.

In this case we have that

$$\pm 1 = X^3 + dY^3 = X^3 + dY^3 + d^2Z^3 - 3dXYZ,$$

and so

$$dZ^2 = 3XY.$$

This forces X and Y to be both positive or both negative, contradicting the fact that $X^3 + dY^3 = 1$.

CASE IV. $u_2 = X + Y\alpha$ and $N(u_1) = -N(u_2)$.

In this case we are assuming that $X^3 + dY^3 = -1$ and $X^3 + dY^3 + d^2Z^3 - 3dXYZ = 1$. It follows that $d^2Z^3 - 3dXYZ = 2$, from which we deduce that $d = 2$. Therefore, $2Z^3 - 3XYZ = 1$, and since clearly $Z = \pm 1$, the only possibility is $Z = -1$, in which case we obtain $X = Y = \pm 1$, contradicting the assumption that $X^3 + 2Y^3 = -1$.

CASE V. $u_2 = X + Y\alpha^2$ and $N(u_1) = N(u_2)$.

In this case $X^3 + d^2Z^3 = 1$, and combining this with $X^3 + dY^3 + d^2Z^3 - 3dXYZ = 1$, it follows that $Y^2 = 3XZ$. Since X, Y, Z are all nonzero, either X and Z are both negative, or both positive, contradicting the fact that $X^3 + d^2Z^3 = 1$.

CASE VI. $u_2 = X + Y\alpha^2$ and $N(u_1) = -N(u_2)$.

In this case $X^3 + d^2Z^3 = -1$, and hence by combining this with $X^3 + dY^3 + d^2Z^3 - 3dXYZ = 1$, it follows that $dY^3 - 3dXYZ = 2$. Therefore, $d = 2$, $Y^3 - 3XYZ = 1$, and $Y = \pm 1$. If $Y = 1$, then $XZ = 0$, contrary to our hypothesis. If $Y = -1$, then $3XZ = 2$, contradicting the fact that X and Z are integers.

ACKNOWLEDGEMENT. The author is grateful to the NSERC for its support.

REFERENCES

1. C. Ballot, *Strong arithmetic properties of the integral solutions of* $X^3 + DY^3 + D^2Z^3 - 3DXYZ = 1$, *where* $D = M^3 \pm 1$. Acta Arith. **89**(1999), 259–277.
2. M. A. Bennett *Effective measures of irrationality for certain algebraic numbers.* J. Austral. Math. Soc. Ser. A **62**(1997), 329–344.
3. J. Cremona, http://www.maths.nott.ac.uk/personal/jec/ftp/data/curves.1-8000.
4. B. Delaunay, *Über die Darstellung der Zahlen durch die binäre kubische Formen mit negativer Discriminante.* Math. Z. **31**(1930), 1–26.
5. W. Ljunggren, *On an improvement of a theorem of T. Nagell concerning the diophantine equation* $Ax^3 + By^3 = C$. Math. Scand. **1**(1953), 297–309.
6. L. J. Mordell, *Diophantine Equations.* Academic Press, New York, 1969.
7. J. H. Silverman and J. Tate, *Rational Points on Elliptic Curves.* Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1992.

Department of Mathematics
University of Ottawa
585 King Edward St.
Ottawa, Ontario
K1N 6N5
email: gwalsh@mathstat.uottawa.ca

C. R. Math. Rep. Acad. Sci. Canada Vol. 25, (1), 2003 pp. 19–25

THE ORDERED K_0-GROUP OF A GRAPH C^*-ALGEBRA

MARK TOMFORDE

Presented by G. A. Elliott, FRSC

RÉSUMÉ. Nous calculons le K_0-groupe ordonné d'une C^*-algèbre de graphe et mentionnons des applications de ce résultat aux AF-algèbres, aux états sur le K_0-groupe d'une algèbre de graphe, et aux états tracials d'algèbres de graphe.

ABSTRACT. We calculate the ordered K_0-group of a graph C^*-algebra and mention applications of this result to AF-algebras, states on the K_0-group of a graph algebra, and tracial states of graph algebras.

1. Preliminaries. We provide some basic facts about graph algebras and refer the reader to [8], [1], and [9] for more details. A (directed) graph $E = (E^0, E^1, r, s)$ consists of a countable set E^0 of vertices, a countable set E^1 of edges, and maps $r, s\colon E^1 \to E^0$ identifying the range and source of each edge. A vertex $v \in E^0$ is called a *sink* if $|s^{-1}(v)| = 0$, and v is called an *infinite emitter* if $|s^{-1}(v)| = \infty$. If v is either a sink or an infinite emitter, we call v a *singular vertex*. A graph E is said to be *row-finite* if it has no infinite emitters. The *vertex matrix* of E is the square matrix A indexed by the vertices of E with $A(v, w)$ equal to the number of edges from v to w.

If E is a graph we define a *Cuntz-Krieger E-family* to be a set of mutually orthogonal projections $\{p_v : v \in E^0\}$ and a set of partial isometries $\{s_e : e \in E^1\}$ with orthogonal ranges which satisfy the *Cuntz-Krieger relations*:

(1) $s_e^* s_e = p_{r(e)}$ for every $e \in E^1$;
(2) $s_e s_e^* \leq p_{s(e)}$ for every $e \in E^1$;
(3) $p_v = \sum_{\{e:s(e)=v\}} s_e s_e^*$ for every $v \in E^0$ that is not a singular vertex.

The *graph algebra* $C^*(E)$ is defined to be the C^*-algebra generated by a universal Cuntz-Krieger E-family.

The graph algebra $C^*(E)$ is unital if and only if E has a finite number of vertices, *cf.* [8, Proposition 1.4], and in this case $1_{C^*(E)} = \sum_{v \in E^0} p_v$. If E has an infinite number of vertices, and we list the vertices of E as $E^0 = \{v_1, v_2, \dots\}$ and define $p_n := \sum_{i=1}^{n} p_{v_i}$, then $\{p_n\}_{n=1}^{\infty}$ will be an approximate unit for $C^*(E)$.

2. The ordered K_0-group. If A is a C^*-algebra let $\mathcal{P}(A)$ denote the set of projections in A. It is a fact that if A is unital (or more generally, if $A \otimes \mathcal{K}$ admits an approximate unit consisting of projections), then $K_0(A) = \{[p]_0 - [q]_0 : p, q \in \mathcal{P}(A \otimes \mathcal{K})\}$. In addition, the positive cone $K_0(A)^+ = \{[p]_0 :$

Received by the editors on October 20, 2002.
AMS subject classification: 46L55.

$p \in \mathcal{P}(A \otimes \mathcal{K})\}$ makes $K_0(A)$ a pre-ordered abelian group. If A is also stably finite, then $(K_0(A), K_0(A)^+)$ will be an ordered abelian group.

Here we compute the positive cone of the K_0-group of a graph C^*-algebra. Throughout this section we let $\mathbb{Z}^K$ and $\mathbb{N}^K$ denote $\bigoplus_K \mathbb{Z}$ and $\bigoplus_K \mathbb{N}$, respectively.

LEMMA 2.1. *Let $E = (E^0, E^1, r, s)$ be a row-finite graph. Also let W denote the set of sinks of E and let $V := E^0 \backslash W$. Then with respect to the decomposition $E^0 = V \cup W$ the vertex matrix of E will have the form*

$$A_E = \begin{pmatrix} B & C \\ 0 & 0 \end{pmatrix}.$$

For $v \in E^0$, let δ_v denote the element of $\mathbb{Z}^V \oplus \mathbb{Z}^W$ with a 1 in the v-th entry and 0's elsewhere.

If we consider $\left(\begin{smallmatrix} B^t - I \\ C^t \end{smallmatrix}\right) : \mathbb{Z}^V \to \mathbb{Z}^V \oplus \mathbb{Z}^W$, then $K_0(C^*(E)) \cong \operatorname{coker}\left(\begin{smallmatrix} B^t - I \\ C^t \end{smallmatrix}\right)$ via an isomorphism which takes $[p_v]_0$ to $[\delta_v]$ for each $v \in E^0$. Furthermore, this isomorphism takes $\Big(K_0\big(C^*(E)\big)\Big)^+$ to $\{[x] : x \in \mathbb{N}^V \oplus \mathbb{N}^W\}$, where $[x]$ denotes the class of x in $\operatorname{coker}\left(\begin{smallmatrix} B^t - I \\ C^t \end{smallmatrix}\right)$.

PROOF. The fact that $K_0\big(C^*(E)\big) \cong \operatorname{coker}\left(\begin{smallmatrix} B^t - I \\ C^t \end{smallmatrix}\right)$ is shown for row-finite graphs in [9, Theorem 3.1]. Thus all that remains to be verified in our claim is that this isomorphism identifies $\Big(K_0\big(C^*(E)\big)\Big)^+$ with $\{[x] : x \in \mathbb{N}^V \oplus \mathbb{N}^W\}$. To do this, we will simply examine the proof of [9, Theorem 3.1] to determine how the isomorphism acts. We will assume that the reader is familiar with this proof, and use the notation established in it without comment.

If $E \times_1 [m,n]$ is the graph defined in [9, Theorem 3.1], then we see that $E \times_1 [m,n]$ is a row-finite graph with no loops and in which every path has length at most $n - m$. Therefore we can use the arguments in the proofs of [8, Proposition 2.1], [8, Corollary 2.2], and [8, Corollary 2.3] to conclude that $C^*(E \times_1 [m,n])$ is the direct sum of copies of the compact operators (on spaces of varying dimensions), indexed by the sinks of $E \times_1 [m,n]$ and that each summand contains precisely one projection $p_{(v,k)}$ associated to a sink as a minimal projection. Thus

$$K_0(C^*(E \times_1 [m,n])) \cong \bigoplus_{v \in V} \mathbb{Z}[p_{(v,n)}]_0 \oplus \bigoplus_{k=0}^{n-m} \bigoplus_{v \in W} \mathbb{Z}[p_{(v,n-k)}]_0$$

and $K_0\big(C^*(E \times_1 [m,n])\big)^+$ is identified with

$$\bigoplus_{v \in V} \mathbb{N}[p_{(v,n)}]_0 \oplus \bigoplus_{k=0}^{n-m} \bigoplus_{v \in W} \mathbb{N}[p_{(v,n-k)}]_0.$$

By the continuity of K-theory, one can let m tend to $-\infty$ and deduce that

$$K_0\big(C^*(E\times_1[-\infty,n])\big)\cong\bigoplus_{v\in V}\mathbb{Z}[p_{(v,n)}]_0\oplus\bigoplus_{k=0}^{\infty}\bigoplus_{v\in W}\mathbb{Z}[p_{(v,n-k)}]_0$$
$$\cong\mathbb{Z}^V\oplus Z^W\oplus Z^W\oplus\cdots.$$

Furthermore, it follows from [10, Theorem 6.3.2(ii)] that this isomorphism identifies $K_0\big(C^*(E\times_1[-\infty,n])\big)^+$ with $\mathbb{N}^V\oplus\mathbb{N}^W\oplus\mathbb{N}^W\oplus\cdots$.

This computation is used later in the proof of [9, Theorem 3.1], where the K_0 functor is applied to a commutative diagram to obtain Figure (3.5) of [9], which we reproduce here:

$$\begin{array}{ccccc}
\mathbb{Z}^V\oplus\mathbb{Z}^W\oplus\mathbb{Z}^W\oplus\cdots & \xrightarrow{D} & \mathbb{Z}^V\oplus\mathbb{Z}^W\oplus\mathbb{Z}^W\oplus\cdots & \xrightarrow{\iota_*^{n+1}} & K_0\big(C^*(E\times_1\mathbb{Z})\big)\\
\downarrow{\scriptstyle 1-D} & & \downarrow{\scriptstyle 1-D} & & \downarrow{\scriptstyle 1-\beta_*^{-1}}\\
\mathbb{Z}^V\oplus\mathbb{Z}^W\oplus\mathbb{Z}^W\oplus\cdots & \xrightarrow{D} & \mathbb{Z}^V\oplus\mathbb{Z}^W\oplus\mathbb{Z}^W\oplus\cdots & \xrightarrow{\iota_*^{n+1}} & K_0\big(C^*(E\times_1\mathbb{Z})\big).
\end{array}$$

Now it is shown in [9, Lemma 3.3] that the homomorphism ι_*^1 induces an isomorphism $\bar{\iota}_*^1$ of $\operatorname{coker}(1-D)$ onto $\operatorname{coker}(1-\beta_*^{-1})=K_0\big(C^*(E)\big)$. We shall show that $\bar{\iota}_*^1(\mathbb{N}^V\oplus\mathbb{N}^W\oplus\mathbb{N}^W\oplus\cdots)=K_0\big(C^*(E)\big)^+$. To begin, note that it follows from [10, Theorem 6.3.2(ii)] that

$$K_0\big(C^*(E\times_1\mathbb{Z})\big)^+=\bigcup_{n=1}^{\infty}\iota_*^n(\mathbb{N}^V\oplus\mathbb{N}^W\oplus\mathbb{N}^W\oplus\cdots).$$

Since $\operatorname{coker}(1-\beta_*^{-1})=K_0\big(C^*(E)\big)$, this implies that

$$K_0\big(C^*(E)\big)^+=\bigcup_{n=1}^{\infty}\{[\iota_*^n(y)]:y\in\mathbb{N}^V\oplus\mathbb{N}^W\oplus\mathbb{N}^W\oplus\cdots\}$$

where $[\iota_*^n(y)]$ denotes the equivalence class of $\iota_*^n(y)$ in $\operatorname{coker}(1-\beta_*^{-1})$. We shall show that the right hand side of this equation is equal to $\{[\iota_*^1(y)]:y\in\mathbb{N}^V\oplus\mathbb{N}^W\oplus\mathbb{N}^W\oplus\cdots\}$. Let $[\iota_*^n(y)]$ be a typical element in the right hand side. Then from the commutativity of the above diagram $\iota_*^n(y)-\iota_*^n(Dy)=\iota_*^n\big((1-D)y\big)=(1-\beta_*^{-1})(\iota_*^n(y))$ which is 0 in $\operatorname{coker}(1-\beta_*^{-1})$. But then $\iota_*^1(y)=\iota_*^n(D^{n-1}y)=\iota_*^n(y)$ in $\operatorname{coker}(1-\beta_*^{-1})$. Hence

$$K_0\big(C^*(E)\big)^+=\{[\iota_*^1(y)]:y\in\mathbb{N}^V\oplus\mathbb{N}^W\oplus\mathbb{N}^W\oplus\cdots\}. \tag{2.1}$$

Next, recall that [9, Lemma 3.4] shows that the inclusion $j\colon\mathbb{Z}^V\oplus Z^W\hookrightarrow\mathbb{Z}^V\oplus\mathbb{Z}^W\oplus\mathbb{Z}^W\oplus\cdots$ induces an isomorphism $\bar{j}$ of $\operatorname{coker}K$ onto $\operatorname{coker}(1-D)$. We wish to show that

$$\bar{j}(\{[x]:x\in\mathbb{N}^V\oplus\mathbb{N}^W\})=\{[y]:y\in\mathbb{N}^V\oplus\mathbb{N}^W\oplus\mathbb{N}^W\oplus\cdots\}. \tag{2.2}$$

It suffices to show that any element $(n, m_1, m_2, m_3, \dots) \in \mathbb{N}^V \oplus \mathbb{N}^W \oplus \mathbb{N}^W \oplus \cdots$ is equal to an element of the form $(a, b, 0, 0, 0, \dots)$ in $\operatorname{coker}(1 - D)$. But given $(n, m_1, m_2, m_3, \dots)$ we see that since this element is in the direct sum, there exists a positive integer k for which $i > k$ implies $m_i = 0$. Thus

$$\begin{pmatrix} n \\ m_1 + \cdots + m_k \\ 0 \\ \vdots \\ 0 \\ 0 \\ \vdots \end{pmatrix} - \begin{pmatrix} n \\ m_1 \\ m_2 \\ \vdots \\ m_k \\ 0 \\ \vdots \end{pmatrix} = \begin{pmatrix} 1 - B^t & 0 & 0 & 0 & \cdot \\ -C^t & 1 & 0 & 0 & \cdot \\ 0 & -1 & 1 & 0 & \cdot \\ 0 & 0 & -1 & 1 & \cdot \\ \cdot & \cdot & \cdot & \cdot & \ddots \end{pmatrix} \begin{pmatrix} 0 \\ m_2 + \cdots + m_k \\ m_3 + \cdots + m_k \\ m_4 + \cdots + m_k \\ \vdots \\ m_k \\ 0 \\ \vdots \end{pmatrix}$$

and so $(n, m_1, m_2, \dots)$ equals $(n, m_1 + \cdots + m_k, 0, 0, \dots)$ in $\operatorname{coker}(1 - D)$, and (2.2) holds.

Finally, the isomorphism between $\operatorname{coker}\left(\begin{smallmatrix} B^t - I \\ C^t \end{smallmatrix}\right)$ and $K_0\big(C^*(E)\big)$ is defined to be $\overline{\iota}^1_* \circ \overline{j}$. But (2.2) and (2.1) show that this isomorphism takes $\{[x] : x \in \mathbb{N}^V \oplus \mathbb{N}^W\}$ onto $\Big(K_0\big(C^*(E)\big)\Big)^+$. ∎

THEOREM 2.2. *Let $E = (E^0, E^1, r, s)$ be a graph. Also let W denote the set of singular vertices of E and let $V := E^0 \setminus W$. Then with respect to the decomposition $E^0 = V \cup W$ the vertex matrix of E will have the form*

$$A_E = \begin{pmatrix} B & C \\ * & * \end{pmatrix}$$

where B and C have entries in $\mathbb{Z}$ and the $*$'s have entries in $\mathbb{Z} \cup \{\infty\}$. Also for $v \in E^0$, let δ_v denote the element of $\mathbb{Z}^V \oplus \mathbb{Z}^W$ with a 1 in the v-th entry and 0's elsewhere.

If we consider $\left(\begin{smallmatrix} B^t - I \\ C^t \end{smallmatrix}\right) : \mathbb{Z}^V \to \mathbb{Z}^V \oplus \mathbb{Z}^W$, then $K_0\big(C^*(E)\big) \cong \operatorname{coker}\left(\begin{smallmatrix} B^t - I \\ C^t \end{smallmatrix}\right)$ via an isomorphism which takes $[p_v]_0$ to $[\delta_v]$ for each $v \in E^0$. Furthermore, this isomorphism takes $\Big(K_0\big(C^*(E)\big)\Big)^+$ onto the semigroup generated by $\{[\delta_v] : v \in E^0\} \cup \{[\delta_v] - \sum_{e \in S}[\delta_{r(e)}] : v$ is an infinite emitter and S is a finite subset of $s^{-1}(v)\}$.

PROOF. The fact that $K_0\big(C^*(E)\big) \cong \operatorname{coker}\left(\begin{smallmatrix} B^t - I \\ C^t \end{smallmatrix}\right)$ was established in [4, Theorem 3.1] using the isomorphisms constructed in [4, Lemma 2.3]. We shall examine the proof of [4, Theorem 3.1] to determine where the positive cone of $K_0\big(C^*(E)\big)$ is sent. Again, we shall assume that the reader is familiar with the proof, and use the notation established in it without comment.

We begin by letting F denote a desingularization of E (see [4, §2]). Then [3, Theorem 2.11] shows that there exists a homomorphism $\phi : C^*(E) \to C^*(F)$

which embeds $C^*(E)$ onto a full corner of $C^*(F)$ and takes each p_v to the projection in $C^*(F)$ corresponding to v. Since ϕ is an embedding onto a full corner, it induces an isomorphism $\phi_*\colon K_0(C^*(E)) \to K_0(C^*(F))$ which takes the class of p_v in $K_0(C^*(E))$ to the class of the corresponding projection in $K_0(C^*(F))$. By Theorem 2.1, if A_F denotes the vertex matrix of F, then $K_0(C^*(E)) \cong \operatorname{coker}(A_F^t - I)$ and $K_0(C^*(E))^+$ is identified with $\{[x] : x \in \bigoplus_V \mathbb{Z} \oplus \bigoplus_W \mathbb{Z} \oplus \bigoplus_W Q\}$ where $Q := \bigoplus_{\mathbb{N}} \mathbb{Z}$. Now it is shown in the proof of [4, Lemma 2.3] that the inclusion map $\rho\colon \bigoplus_V \mathbb{Z} \oplus \bigoplus_W \mathbb{Z} \to \bigoplus_V \mathbb{Z} \oplus \bigoplus_W \mathbb{Z} \oplus \bigoplus_W Q$ induces an isomorphism $\bar{\rho}\colon \operatorname{coker}\left(\begin{smallmatrix} B^t - I \\ C^t \end{smallmatrix}\right) \to \operatorname{coker}(A_F - I)$. Since this isomorphism identifies the class of $\delta_v \in \bigoplus_V \mathbb{Z} \oplus \bigoplus_W \mathbb{Z}$ with the class of $\left(\begin{smallmatrix} \delta_v \\ 0 \end{smallmatrix}\right) \in \bigoplus_V \mathbb{Z} \oplus \bigoplus_W \mathbb{Z} \oplus \bigoplus_W Q$, it follows that $[p_v]_0 \in K_0(C^*(E))$ is identified with $[\delta_v] \in \operatorname{coker}\left(\begin{smallmatrix} B^t - I \\ C^t \end{smallmatrix}\right)$.

All that remains is to determine where this isomorphism sends the positive cone of $K_0(C^*(E))$. Let Γ denote the semigroup of elements that $\bar{\rho}$ sends to $\{[x] : x \in \bigoplus_V \mathbb{Z} \oplus \bigoplus_W \mathbb{Z} \oplus \bigoplus_W Q\}$. Now certainly $\{[\delta_v] : v \in E^0\}$ is in Γ. Furthermore, for any infinite emitter v and finite subset $S \subseteq s^{-1}(v)$ we have that

$$[p_v]_0 - \sum_{e \in S} [p_{r(e)}]_0 = [p_v]_0 - \sum_{e \in S} [s_e^* s_e]_0 = [p_v]_0 - \sum_{e \in S} [s_e s_e^*]_0 = \Big[p_v - \sum_{e \in S} s_e s_e^*\Big]_0$$

and this element belongs to $K_0(C^*(E))^+$. Since $K_0(C^*(E))^+$ is identified with $\{[x] : x \in \bigoplus_V \mathbb{Z} \oplus \bigoplus_W \mathbb{Z} \oplus \bigoplus_W Q\}$ this implies that the class of $\left(\begin{smallmatrix} \delta_v \\ 0 \end{smallmatrix}\right) - \sum_{e \in S} \left(\begin{smallmatrix} \delta_{r(e)} \\ 0 \end{smallmatrix}\right)$ is in $\{[x] : x \in \bigoplus_V \mathbb{Z} \oplus \bigoplus_W \mathbb{Z} \oplus \bigoplus_W Q\}$ and thus $[p_v] - \sum_{e \in S} [p_{r(e)}]$ is in Γ. On the other hand, we know that Γ is generated by the elements that $\bar{\rho}$ sends to the classes of the generators of $\bigoplus_V \mathbb{Z} \oplus \bigoplus_W \mathbb{Z} \oplus \bigoplus_W Q$. Now certainly the inverse image under $\bar{\rho}$ of the class of $\left(\begin{smallmatrix} \delta_v \\ 0 \end{smallmatrix}\right)$ for $v \in V \cup W$ will be $[\delta_v]$. In addition, if v_i is a vertex on the tail added to an infinite emitter v, then we see that the inverse image under $\bar{\rho}$ of the element $\left(\begin{smallmatrix} 0 \\ \delta_{v_i} \end{smallmatrix}\right)$ will be $\left(\begin{smallmatrix} \mathbf{u} \\ \mathbf{v} \end{smallmatrix}\right)$ where $\mathbf{u}$ and $\mathbf{v}$ are as defined in the final paragraph of [4, Lemma 2.3]. However, one can verify from how $\mathbf{u}$ and $\mathbf{v}$ are defined that $\left(\begin{smallmatrix} \mathbf{u} \\ \mathbf{v} \end{smallmatrix}\right)$ will have the form $\delta_v - \sum_{e \in S} \delta_{r(e)}$ for some finite $S \subseteq s^{-1}(v)$. Thus Γ is generated by the elements $[\delta_v]$ and $[\delta_v] - \sum_{e \in S} [\delta_{r(e)}]$. ∎

3. Applications.

3.1. AF-algebras. The graph algebra $C^*(E)$ is an AF-algebra if and only if E has no loops [8, Theorem 2.4]. By Elliott's Theorem AF-algebras are classified by their ordered K_0-groups. Hence for two graphs containing no loops, Theorem 2.2 can be used to determine if their associated C^*-algebras are isomorphic (as well as stably isomorphic).

3.2. States on $K_0(C^*(E))$. If A is a C^*-algebra containing a countable approximate unit $\{p_n\}_{n=1}^{\infty}$ consisting of projections, then a *state* on $K_0(A)$ is a homo-

morphism $f\colon K_0(A) \to \mathbb{R}$ such that $f\big(K_0(A)^+\big) \subseteq \mathbb{R}^+$ and $\lim_{n\to\infty} f([p_n]_0) = 1$. The set of all states on $K_0(A)$ is denoted $S\big(K_0(A)\big)$ and we make it into a topological space by giving it the weak-$*$ topology.

DEFINITION 3.1. *If E is a graph, then a* graph trace *on E is a function $g\colon E^0 \to \mathbb{R}^+$ with the following two properties:*

(1) *For any nonsingular vertex $v \in E^0$ we have $g(v) = \sum_{\{e\in E^1 : s(e)=v\}} g\big(r(e)\big)$.*
(2) *For any infinite emitter $v \in E^0$ and any finite set of edges $e_1, \ldots, e_n \in s^{-1}(v)$ we have $g(v) \geq \sum_{i=1}^n g\big(r(e_i)\big)$.*

We define the norm of g to be the (possibly infinite) value $\|g\| := \sum_{v\in E^0} g(v)$, and we shall use $T(E)$ to denote the set of all graph traces on E with norm 1.

PROPOSITION 3.2. *If E is a graph, then the state space $S\Big(K_0\big(C^*(E)\big)\Big)$ with the weak-$*$ topology is naturally isomorphic to $T(E)$ with the topology generated by the subbasis $\{N_{v,\epsilon}(g) : v \in E^0, \epsilon > 0, \text{ and } g \in T(E)\}$, where $N_{v,\epsilon}(g) := \{h \in T(E) : |h(v) - g(v)| < \epsilon\}$.*

PROOF. We define a map $\iota\colon S\Big(K_0\big(C^*(E)\big)\Big) \to T(E)$ by $\iota(f)(v) := f([p_v]_0)$. We shall show that ι is an affine homeomorphism. To see that ι is injective note that if $\iota(f_1) = \iota(f_2)$, then for each $v \in E^0$ we have that $f_1([p_v]_0) = \iota(f_1)(v) = \iota(f_2)(v) = f_2([p_v]_0)$, and since the $[p_v]_0$'s generate $K_0\big(C^*(E)\big)$ it follows that $f_1 = f_2$.

To see that ι is surjective, let $g\colon E^0 \to \mathbb{R}^+$ be a graph trace. We shall define a homomorphism $f\colon \operatorname{coker}\left(\begin{smallmatrix} B^t - I \\ C^t \end{smallmatrix}\right) \to \mathbb{R}$ by setting $f([\delta_v]) := g(v)$. Because g satisfies (1) of Definition 3.1 we see that f is well defined. Also, since the values of g are positive and g satisfies (2) of Definition 3.1 we see that $f\Big(K_0\big(C^*(E)\big)^+\Big) \subseteq \mathbb{R}^+$. Finally, since g has norm 1 we see that $\lim_{n\to\infty} f\big(\sum_{i=1}^n p_{v_i}\big) = \lim_{n\to\infty} \sum_{i=1}^n g(v_i) = \|g\| = 1$. So f is a state on $K_0\big(C^*(E)\big)$ and $\iota(f) = g$.

It is straightforward to verify that ι is an affine homeomorphism. ∎

3.3. Tracial states on $C^*(E)$. A *trace* on a C^*-algebra A is a linear functional $\tau\colon A \to \mathbb{C}$ with the property that $\tau(ab) = \tau(ba)$ for all $a, b \in A$. We say that τ is *positive* if $\tau(a) \geq 0$ for all $a \in A^+$. If τ is positive and $\|\tau\| = 1$ we call τ a *tracial state.* The set of all tracial states is denoted $T(A)$ and when $T(A)$ is nonempty we equip it with the weak-$*$ topology. Let A be a C^*-algebra with a countable approximate unit consisting of projections. If τ is a trace on A, then it induces a map $K_0(\tau)\colon K_0(A) \to \mathbb{R}$ given by $K_0(\tau)([p]_0 - [q]_0) = \tau(p) - \tau(q)$. The map $K_0(\tau)$ will be an element of $S\big(K_0(A)\big)$ (see [10, §5.2] for more details) and thus there is a continuous affine map $r_A\colon T(A) \to S\big(K_0(A)\big)$ defined by $r_A(\tau) := K_0(\tau)$.

It is a fact that any quasitrace on an exact C^*-algebra extends to a trace (this was proven by Haagerup for unital C^*-algebras [5] and shown to hold for

nonunital C^*-algebras by Kirchberg [7]). Furthermore, Blackadar and Rørdam showed in [2] that when A is unital every element in $K_0(A)$ lifts to a quasitrace. It is straightforward to extend the result of Blackadar and Rørdam to C^*-algebras with a countable approximate unit consisting of projections. Thus when A is a graph algebra we see that the map $r_A\colon T(A) \to S(K_0(A))$ is surjective.

If A has real rank zero, then the span of the projections in A is dense in A and r_A is injective. It was shown in [6] that a graph algebra $C^*(E)$ has real rank zero if and only if the graph E satisfies Condition (K); that is, no vertex in E is the base of exactly one simple loop. Therefore, when $A = C^*(E)$ and E is a graph satisfying Condition (K), the map r_A is a homeomorphism and Proposition 3.2 shows that the tracial states on $C^*(E)$ are identified in a canonical way with $T(E)$.

References

1. T. Bates, D. Pask, I. Raeburn, and W. Szymański, *The C^*-algebras of row-finite graphs*. New York J. Math. **6**(2000), 307–324.
2. B. Blackadar and M. Rørdam, *Extending states on preordered semigroups and the existence of quasitraces on C^*-algebras*. J. Algebra, **152**(1992), 240–247.
3. D. Drinen and M. Tomforde, *The C^*-algebras of arbitrary graphs*. Rocky Mountain J. Math, to appear.
4. D. Drinen and M. Tomforde, *Computing K-theory and Ext for graph C^*-algebras*. Illinois J. Math., to appear.
5. U. Haagerup, *Every quasi-trace on an exact C^*-algebra is a trace*. Preprint, 1991.
6. J. A Jeong, *Real rank of generalized Cuntz-Krieger algebras*. Preprint, 2000.
7. E. Kirchberg, *On the existence of traces on exact stably projectionless simple C^*-algebras*. In: Operator Algebras and their Applications (eds. P. A. Fillmore and J. A. Mingo), Fields Inst. Commun. **13**, Amer. Math. Soc. 1997, 171–172.
8. A. Kumjian, D. Pask, and I. Raeburn, *Cuntz-Krieger algebras of directed graphs*. Pacific J. Math. **184**(1998), 161–174.
9. I. Raeburn and W. Szymański, *Cuntz-Krieger algebras of infinite graphs and matrices*. Preprint, 2000.
10. M. Rørdam, F. Larsen, and N. J. Laustsen, *An Introduction to K-theory for C^*-algebras*. London Math. Soc. Stud. Texts **49**, Cambridge University Press, Cambridge, 2000.

Department of Mathematics
Dartmouth College
Hanover, NH 03755
USA

Current address:
Department of Mathematics
University of Iowa
Iowa City, IA 52242
USA
email: tomforde@math.uiowa.edu

C. R. Math. Rep. Acad. Sci. Canada Vol. 25, (1), 2003 pp. 26–32

TWISTED AND SHUFFLED FILTRATIONS ON TILTING MODULES

VOLODYMYR MAZORCHUK

Presented by Vlastimil Dlab, FRSC

RÉSUMÉ. On montre que les modules inclinants dans la catégorie $\mathcal{O}_\lambda$ admettent une filtration par différentes familles de modules de Verma.

ABSTRACT. We prove that tilting modules in the category $\mathcal{O}_\lambda$ are filtered by different families of shuffled (or twisted) Verma modules.

1. Introduction and the main result. Let $\mathfrak{g}$ be a semi-simple complex finite-dimensional Lie algebra. The Bernstein-Gelfand-Gelfand category $\mathcal{O}$ for $\mathfrak{g}$, introduced in [BGG], contains several important and interesting families of $\mathfrak{g}$-modules, *e.g.* simple highest weight modules, Verma modules, projective modules, tilting modules, which appear naturally in that context. Considering the category of Harish-Chandra modules for $\mathfrak{g}$ (which are in fact $\mathfrak{g} \times \mathfrak{g}$-modules), the Bernstein-Gelfand – Joseph – Duflo equivalence of categories, see [Ja, Chapter 6], maps the principal series Harish-Chandra modules to the so-called *shuffled Verma modules* $M(x, y)$. Inside a fixed regular indecomposable block $\mathcal{O}_\lambda$, λ regular integral antidominant, of $\mathcal{O}$ shuffled Verma modules are indexed by pairs (x, y) of elements from the Weyl group W. Irving, in [I], gave an alternative construction of these modules in terms of the so-called *shuffling functors*, which are defined using the coherent translations θ_α, [Ja], through the α-wall. His construction is inductive and goes as follows. We start with setting $M(x, e) = M(x \cdot \lambda)$, the latter being the usual Verma module. If now $y \in W$ and $ys_\alpha > y$ for the simple reflection s_α, then the module $M(x, y)$ canonically embeds into $\theta_\alpha(M(x, y))$ and the quotient is exactly $M(x, ys_\alpha)$. Recently, in [AL] it was shown that the same family of modules can be obtained using *Arkhipov's twisting functor*, [Ar], [AL], which also explains the alternative name *twisted Verma modules*, used in [AL].

Recall that, if $\mathcal{F}$ is a fixed family of modules, a module, M, is said to *have an $\mathcal{F}$-flag* (or *to be filtered by modules from $\mathcal{F}$*) if there is a filtration of M whose quotients belong to $\mathcal{F}$. Denote $\mathcal{F}_x = \{M(x, y) \mid y \in W\}$ resp. $\mathcal{F}^y = \{M(x, y) \mid x \in W\}$ and let w_0 be the longest element in W.

As was known from [BGG], all projective modules in the category $\mathcal{O}$ are filtered by Verma modules. In [I, Theorem 4.1] it was shown that some projectives in $\mathcal{O}_\lambda$ are filtered by certain families of shuffled Verma modules. Moreover, roughly speaking, the bigger the indecomposable projective is, the more such filtrations it possesses. Namely, the indecomposable projective cover $P(x \cdot \lambda)$,

Received by the editors on November 11, 2002; revised January 19, 2003.
AMS subject classification: Primary: 17B10, 17B35; secondary: 22E47.

$x \in W$, of the simple module $L(x \cdot \lambda) \in \mathcal{O}_\lambda$ appears to have an $\mathcal{F}^y$-flag for all y, which can be written $y = s_1 \cdots s_k$ with simple reflections s_i satisfying $xs_i > x$. In particular, the *big projective module* $P(\lambda)$ in $\mathcal{O}_\lambda$ has an $\mathcal{F}^y$-flag for all y.

If one writes $\{M(x,y)\}$ in a $W \times W$-array with respect to some total order extending the Bruhat order, the sets $\mathcal{F}_x$ and $\mathcal{F}^y$ represent rows resp. columns of the array. In particular, $\mathcal{F}^e$ and $\mathcal{F}_{w_0}$ represent Verma modules and $\mathcal{F}^{w_0}$ and $\mathcal{F}_e$ represent their duals. This is why the shuffled Verma modules are usually viewed as intermediate modules between Verma modules and their duals. This remark also stimulates to consider *tilting* modules in $\mathcal{O}_\lambda$, *i.e.*, self-dual modules with a Verma flag, first constructed by [CI] (the term tilting module was introduced for $\mathcal{O}$ later, namely, after [R]). In particular, it is known that indecomposable tilting modules are indexed by Verma modules, namely, for each Verma module $M(x \cdot \lambda)$ there exists exactly one indecomposable tilting module $T(x \cdot \lambda)$, such that any Verma flag of $T(x \cdot \lambda)$ starts with $M(x \cdot \lambda)$.

By definition, all tilting modules have $\mathcal{F}_e$-, $\mathcal{F}_{w_0}$-, $\mathcal{F}^e$- and $\mathcal{F}^{w_0}$-flags. In particular, $P(\lambda)$ is an example of an indecomposable tilting module. As we already mentioned, by Irving's result $P(\lambda)$ has an $\mathcal{F}^y$-flag for all y. Another example of tilting module in $\mathcal{O}_\lambda$ is the simple Verma module $M(\lambda)$, isomorphic to $M(x, x^{-1})$ for any $x \in W$ (see *e.g.* properties of $M(x,y)$ in [I]). Since $M(\lambda)$ occurs in each row and column of the $W \times W$ array $\{M(x,y)\}$, we get that $M(\lambda)$ has an $\mathcal{F}^y$- and an $\mathcal{F}_x$-flag for all x, y. The aim of this paper is to prove the following result, which is naturally motivated by the above discussion.

THEOREM 1. *Any tilting module in $\mathcal{O}_\lambda$ has an $\mathcal{F}^y$- and an $\mathcal{F}_x$-flag for all $x, y \in W$.*

We also note that Soergel's equivalence of categories from [S1] extends this result to all regular anti-dominant λ, which is the classical case, considered in [I].

2. **$\mathcal{F}^y$-flags on tilting modules.** In this section we prove the first part of the main Theorem 1, namely, we will show that any tilting module in $\mathcal{O}_\lambda$ has an $\mathcal{F}^y$-flag for all $y \in W$. As we already mentioned, from [I] this follows for $P(\lambda) = T(w_0 \cdot \lambda)$ and for $T(\lambda) = M(\lambda)$ the statement is obvious. For a simple root, α, let $s = s_\alpha$ be the corresponding reflection. Then we denote by $\mathcal{S}_s$ the corresponding shuffling functor, [I, Section 3] (we remark that in [I] this functor was denoted by C_s, $s = s_\alpha$, and we decided to use the other name to avoid confusions with Enright's completions, which are also usually denoted by C_s). Then for any $M \in \mathcal{O}_\lambda$ the module $\mathcal{S}_s(M)$ is the quotient of $\theta_\alpha(M)$ modulo the canonical image of M inside $\theta_\alpha(M)$. It is easy to see that this map is functorial. Shuffling functors produce the following connection between different $(\mathcal{F}^y)$'s, see [I, Corollary 3.2]:

LEMMA 1. *Let α be a simple root and $y \in W$ such that $ys_\alpha > y$. If $M \in \mathcal{O}_\lambda$ has an $\mathcal{F}^y$-flag then $\mathcal{S}_{s_\alpha}(M)$ has an $\mathcal{F}^{ys_\alpha}$-flag.*

For $y \in W$ we denote by $\mathcal{O}_\lambda(y)$ the full subcategory of all modules from $\mathcal{O}_\lambda$ having an $\mathcal{F}^y$-flag. We start with the following observation:

LEMMA 2. *Let $y \in W$ and $s = s_\alpha$ be a simple reflection such that $ys > y$. Then $\mathcal{S}_s\colon \mathcal{O}_\lambda(y) \to \mathcal{O}_\lambda(ys)$ is an equivalence of categories.*

PROOF. Because of the exact sequence $0 \to M(x,y) \to \theta_s(M(x,y)) \to M(x,ys) \to 0$, [I, Theorem 2.1], where $x \in W$, the adjunction morphism $M(x,y) \to \theta_s(M(x,y))$ is injective and hence the image of $\mathcal{O}_\lambda(y)$ under $\mathcal{S}_s$ is contained in $\mathcal{O}_\lambda(ys)$ by Lemma 1. By [AL, Remark 1.2], there also exists a self-equivalence, $\tilde{\mathcal{S}}_s$ of the bounded derived category $\mathcal{D}^b(\mathcal{O}_\lambda)$ such that $\tilde{\mathcal{S}}_s(M) \simeq \mathcal{S}_s(M)$ for any $M \in \mathcal{O}_\lambda(y)$. In particular, $\mathcal{S}_s$ preserves the homomorphism rings between objects from $\mathcal{O}_\lambda(y)$ and thus the endomorphism ring of all objects from $\mathcal{O}_\lambda(y)$. Hence it sends indecomposables to indecomposables. Now it is sufficient to prove that any object in $\mathcal{O}_\lambda(ys)$ belongs to the image of $\mathcal{S}_s$. We will do it using induction in the length of $\mathcal{F}^{ys}$-filtration of $M \in \mathcal{O}_\lambda(ys)$. If this length is one, then $M \simeq M(x,ys)$ for some $x \in W$ and hence $M = \mathcal{S}_s(M(x,y))$. Now consider an exact sequence $0 \to M_1 \to M_2 \to M_3 \to 0$ in $\mathcal{O}_\lambda(ys)$. Applying to this sequence the exact functor θ_s we get the following commutative diagram with exact rows:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \theta_s(M_1) & \longrightarrow & \theta_s(M_2) & \longrightarrow & \theta_s(M_3) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & M_1 & \longrightarrow & M_2 & \longrightarrow & M_3 & \longrightarrow & 0
\end{array}$$

where the columns are represented by natural morphisms $\theta_s(M) \to M$ (see I''_M in [GJ, Subsection 3.12]). As all $M_i \in \mathcal{O}_\lambda(ys)$, these morphisms are surjective by [GJ, Lemma 3.12]. Hence, by standard homological arguments and computing the character of K_i, $i = 1,2,3$, we can extend the diagram above to the following commutative diagram with exact columns:

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & K_1 & \longrightarrow & K_2 & \longrightarrow & K_3 & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \theta_s(M_1) & \longrightarrow & \theta_s(M_2) & \longrightarrow & \theta_s(M_3) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & M_1 & \longrightarrow & M_2 & \longrightarrow & M_3 & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0. & &
\end{array}$$

Now as the two lower rows are exact the upper one is exact as well by the 3×3-Lemma. From the inductive assumption we get that K_1 and K_3 have $\mathcal{F}^y$-flags and thus K_2 has an $\mathcal{F}^y$-flag as well. Moreover, by induction we also have $\theta_s(K_i) \simeq \theta_s(M_i)$, $i = 1, 3$, and that the morphisms $K_i \to \theta_s(M_i)$, $i = 1, 3$, are represented by the natural morphisms $K_i \to \theta_s(K_i)$. From this and [GJ, Subsection 3.12] it follows then that the natural morphism $K_2 \to \theta_s(K_2)$ is injective which then, together with $\theta_s^2 = \theta_s \oplus \theta_s$, guarantees that $\theta_s(K_2) \simeq \theta_s(M_2)$. Substituting now the map $K_2 \to \theta_s(M_2)$ with the natural morphism $K_2 \to \theta_s(K_2)$ we still get a commutative diagram and thus the composition of the natural morphisms $K_2 \to \theta_s(K_2)$ and $\theta_s(K_2) \simeq \theta_s(M_2) \to M_2$ must be zero. Therefore $M_2 \simeq \mathcal{S}_s(K_2)$, which completes the proof. ∎

We note that one can also use the following argument to prove the second part of Lemma 2: Having a module with $\mathcal{F}^{ys}$-filtration one uses shuffling functors to get a module, filtered by dual Verma modules, which then can be translated to a module with Verma flag by duality. Shuffling the latter we can get a module with $\mathcal{F}^{w_0 y}$-flag and applying the duality once more we get a module with $\mathcal{F}^y$-flag. It follows from [AL, Remark 1.2] that this procedure is inverse to $\mathcal{S}_s \colon \mathcal{O}_\lambda(y) \to \mathcal{O}_\lambda(ys)$.

COROLLARY 1. *Let $y \in W$ with the reduced decomposition $y = s_1 \cdots s_k$. Then $\mathcal{S}_{s_k} \circ \cdots \circ \mathcal{S}_{s_1} \colon \mathcal{O}_\lambda(e) \to \mathcal{O}_\lambda(y)$ is an equivalence of categories.*

COROLLARY 2. *The category $\mathcal{O}_\lambda(y)$ is closed under taking direct summands.*

Now the necessary statement (*i.e.*, the necessary part of Theorem 1) will follow from the following result.

LEMMA 3. *Let $M \in \bigcap_{y \in W} \mathcal{O}_\lambda(y)$ and s be a simple reflection. Then $\theta_s(M) \in \bigcap_{y \in W} \mathcal{O}_\lambda(y)$.*

PROOF. First we note that M is filtered by $\mathcal{F}^e$ and $\mathcal{F}^{w_0}$ and hence is a tilting module. In particular, it is self-dual. Hence $\theta_s(M)$ is self-dual as well. Let $y \in W$ be such that $ys > y$. Then the adjunction morphism $M \to \theta_s(M)$ is injective and thus its cokernel is filtered by $\mathcal{F}^{ys}$. As M is filtered by $\mathcal{F}^{ys}$ as well we get that $\theta_s(M)$ is filtered by $\mathcal{F}^{ys}$, in other words by $\mathcal{F}^w$ with $ws < w$. Now if we use the fact that M is self-dual and that the modules in $\mathcal{F}^{w_0 w}$ are exactly the duals to the modules in $\mathcal{F}^w$ (see [I]), we get that the module M is filtered by $\mathcal{F}^{w_0 w}$ with $ws < w$ and hence by $\mathcal{F}^t$ with $wt > t$. This completes the proof. ∎

LEMMA 4. *Each indecomposable tilting module $T(w \cdot \lambda)$, $w \in W$, is a direct summand of some $M \in \bigcap_{y \in W} \mathcal{O}_\lambda(y)$.*

PROOF. For $w = 0$ the module $T(\lambda)$ is a simple Verma module and hence belongs to all $\mathcal{O}_\lambda(y)$, $y \in W$. Now, by Lemma 3 the module $\theta_{s_1} \circ \cdots \circ \theta_{s_k}(T(\lambda))$

also belongs to all $\mathcal{O}_\lambda(y)$, $y \in W$, for any sequence $s_1, \dots, s_k \in W$ of simple reflections. If we take $w = s_k \cdots s_1$ to be a reduced decomposition of w, we can use [CI] and obtain that $T(w \cdot \lambda)$ is a direct summand of $\theta_{s_1} \circ \cdots \circ \theta_{s_k}\big(T(\lambda)\big)$. This completes the proof. ∎

Now the proof of the first statement of Theorem 1 is transparent. We use Lemma 4 and find some $M \in \bigcap_{y \in W} \mathcal{O}_\lambda(y)$ which has $T(w \cdot \lambda)$ as a direct summand. Now, by Corollary 2, all direct summands of M, in particular $T(w \cdot \lambda)$, belong to $\bigcap_{y \in W} \mathcal{O}_\lambda(y)$, which is the statement we needed.

3. **$\mathcal{F}_x$-flags on tilting modules.** In this section we prove the second part of Theorem 1, which appears to be a little bit easier than the first one. To produce different $\mathcal{F}_x$-flags on tilting modules we will use *Arkhipov's twisting functors* T_w, $w \in W$ (notation as in [AL], in [Ar] the author used Θ_w). According to [AL, Section 5], T_w sends $\mathcal{F}_{w_0}$, which consists of Verma modules, to $\mathcal{F}_{ww_0}$ for any $w \in W$. We again start with the simple tilting module.

LEMMA 5. *The module $T(\lambda)$ has an $\mathcal{F}_x$-flag for any $x \in W$.*

PROOF. Write $x = ww_0$ for uniquely defined $w \in W$ and choose Verma module $M(\mu) \in \mathcal{F}_{w_0}$ such that $T_w\big(M(\mu)\big) \simeq M(\lambda) = T(\lambda)$. This is possible since $T_w \colon \mathcal{F}_{w_0} \to \mathcal{F}_{ww_0}$ is bijective and $M(\lambda) \in \mathcal{F}_{ww_0}$. ∎

We have to note that the statement itself follows from the fact $M(\lambda) \in \mathcal{F}_{ww_0}$, however we will use the formula $T_w\big(M(\mu)\big) \simeq M(\lambda)$ in the arguments that follow.

COROLLARY 3. *For any finite-dimensional $\mathfrak{g}$-module F and any $x \in W$ the module $F \otimes T(\lambda)$ has an $\mathcal{F}_x$-flag.*

PROOF. As above write $x = ww_0$. By [AL, Subsection 6.3], T_w commutes with $F \otimes \_$. Hence $F \otimes T(\lambda) \simeq F \otimes \Big(T_w\big(M(\mu)\big)\Big) \simeq T_w\big(F \otimes M(\mu)\big)$. As $M(\mu)$ is a Verma module, $F \otimes M(\mu)$ has a Verma flag, hence $\mathcal{F}_{w_0}$-flag. Then T_w will translate this flag to an $\mathcal{F}_x$-flag of $F \otimes T(\lambda)$. ∎

LEMMA 6. *Let F and x be as in Corollary 3. Then each direct summand of $F \otimes T(\lambda)$ has an $\mathcal{F}_x$-flag.*

PROOF. Here we use the fact [Ar], [AL], that T_w extends to the functor LT_w on the bounded derived category $\mathcal{D}^b(\mathcal{O}_\lambda)$, moreover, LT_w is, in fact, an auto-equivalence on $\mathcal{D}^b(\mathcal{O}_\lambda)$. In particular, it preserves the endomorphism ring of each direct summand of $F \otimes M(\mu)$ as the latter are filtered by Verma modules, see [AL, Corollary 6.3]. Hence T_w sends indecomposable direct summands of $F \otimes M(\mu)$ to indecomposable direct summands of $F \otimes T(\lambda)$ and therefore transforms the Verma flags of the first ones to $\mathcal{F}_x$-flags of the last ones. This completes the proof. ∎

Now the proof of the second part of Theorem 1 is easily completed. By [CI] each indecomposable tilting module in $\mathcal{O}_\lambda$ occurs as a direct summand in some $F \otimes T(\lambda)$. Hence Lemma 6 implies the necessary statement.

We note that the problem to use analogous arguments in Section 2 was that the coherent translation θ_s does not commute with the functor $F\otimes_-$ in the general case.

4. Some corollaries and remarks.

COROLLARY 4. *For a module, $M \in \mathcal{O}_\lambda$, the following conditions are equivalent:*

1. *M is a tilting module, i.e., is self-dual and filtered by Verma modules;*
2. *M has an $\mathcal{F}^y$-flag for all $y \in W$;*
3. *M has an $\mathcal{F}_x$-flag for all $x \in W$;*
4. *M has an $\mathcal{F}^y$-flag and an $\mathcal{F}_x$-flag for all $x, y \in W$.*

PROOF. Immediate corollary of Theorem 1. ∎

COROLLARY 5. *Each category $\mathcal{O}_\lambda(y)$, $y \in W$, has almost split sequences.*

PROOF. Follows from Corollary 1 and [R]. ∎

The next corollary is a famous result of Soergel [S2]. In particular, Corollary 1 can be viewed as an extension of this result.

COROLLARY 6. *The categories $\mathcal{O}_\lambda(e)$ and $\mathcal{O}_\lambda(e)^{opp}$ are equivalent.*

PROOF. As a special case of Corollary 1, the categories $\mathcal{O}_\lambda(e)$ and $\mathcal{O}_\lambda(w_0)$ are equivalent. But the last one is equivalent with $\mathcal{O}_\lambda(e)^{opp}$ by usual duality. ∎

Analogous results can be obtained via T_w for categories of modules, filtered by $\mathcal{F}_x$. In fact, in [S2] the functor T_{w_0} is used to prove the above statement.

We would like to finish with the remark that the homological characterization of $\mathcal{O}_\lambda(y)$ in the spirit of [R], where it was proved that $\mathcal{F}^e = {}^\perp\mathcal{F}^{w_0}$ and $\mathcal{F}^{w_0} = (\mathcal{F}^e)^\perp$ does not seem to be possible, *e.g.* as for any short exact sequence $0 \to K \to T_2 \to T_1 \to 0$ with tilting modules T_1 and T_2, the module K although filtered by $\mathcal{F}^e$ is not tilting in general (example: $T_1 = T(\lambda)$, $T_2 = \theta_\alpha(T(\lambda))$, then $K = M(s_\alpha \cdot \lambda)$ is not self-dual). In case of existence of any analogue of such homological characterization, from Theorem 1 and the long exact sequence it would follow that K is a tilting module as well.

ACKNOWLEDGMENTS. The main part of the research was done during the visit of the author to Max-Planck-Institute für Mathematik in Bonn. The financial support, accommodation and hospitality of MPI are gratefully acknowledged. The research was also partially supported by the Royal Swedish Academy of Sciences.

I also would like to thank Steffen König and Olexandr Khomenko for stimulating discussions and Catharina Stroppel for useful comments. I would like also to thank the referee for remarks and suggestions that led to the improvements in the paper.

REFERENCES

[AL] H. H. Andersen and N. Lauritzen, *Twisted Verma modules.* Preprint QA/0105012.

[Ar] S. Arkhipov, *Algebraic construction of contragradient quasi-Verma modules in positive characteristic.* Preprint MPI 2001 - 34, Max-Planck Institut für Mathematik, 2001.

[BG] I. N. Bernstein and S. I. Gelfand, *Tensor products of finite- and infinite-dimensional representations of semisimple Lie algebras.* Compositio Math. (2) **41**(1980), 245–285.

[BGG] I. N. Bernstein, I. M. Gelfand and S. I. Gelfand, *A certain category of* $\mathfrak{g}$*-modules.* (Russian) Funkcional. Anal. i Prilozen. (2) **10**(1976), 1–8.

[CI] D. Collingwood and R. S. Irving, *A decomposition theorem for certain self-dual modules in the category* $\mathcal{O}$. Duke Math. J. (1) **58**(1989), 89–102.

[D] J. Dixmier, *Algèbres Enveloppantes.* Paris, 1974.

[GJ] O. Gabber and A. Joseph, *Towards the Kazhdan-Lusztig conjecture.* Ann. Sci. École Norm. Sup. (4) **14**(1981), 261–302.

[I] R. Irving, *Shuffled Verma modules and principal series modules over complex semisimple Lie algebras.* J. London Math. Soc. (2) **48**(1993), 263–277.

[Ja] J. C. Jantzen, *Einhüllende Algebren halbeinfacher Lie-Algebren.* (German) Ergeb. Math. Grenzgeb. (3) **3**, Springer-Verlag, Berlin, 1983.

[J] A. Joseph, *The Enright functor on the Bernstein-Gelfand-Gelfand category* $\mathcal{O}$. Invent. Math. (3) **67**(1982), 423–445.

[R] C. M. Ringel, *The category of modules with good filtrations over a quasi-hereditary algebra has almost split sequences.* Math. Z. (2) **208**(1991), 209–223.

[S1] W. Soergel, *Kategorie* $\mathcal{O}$*, perverse Garben und Moduln über den Koinvarianten zur Weylgruppe.* (German) J. Amer. Math. Soc. (2) **3**(1990), 421–445.

[S2] ———, *Charakterformeln für Kipp-Moduln über Kac-Moody-Algebren.* Represent. Theory **1**(1997), 115–132.

Department of Mathematics
Uppsala University
Box 480
751 06 Uppsala
Sweden
email: mazor@math.uu.se
website: http://www.math.uu.se/~mazor/.