BOLETIM
DA SOCIEDADE BRASILEIRA DE MATEMÁTICA

Bol. Soc. Bras. Mat., Vol. 23, Ns. 1-2, 137-151

A Chebotarev Theorem for finite homogeneous extensions of shifts

Mohd. Salmi Md. Noorani[1] and William Parry

Abstract. We derive a Chebotarev Theorem for finite homogeneous extensions of shifts of finite type. These extensions are of the form $\tilde{\sigma}: X \times G/H \to X \times G/H$ where $\tilde{\sigma}(x, gH) = (\sigma x, \alpha(x)gH)$, for some finite group G and subgroup H. Given a σ-closed orbit τ, the periods of the $\tilde{\sigma}$-closed orbits covering τ define a partition of the integer $|G/H|$. The theorem then gives us an asymptotic formula for the number of closed orbits with respect to the various partitions of the integer $|G/H|$. We apply our theorem to the case of a finite extension and of an automorphism extension of shifts of finite type. We also give a further application to 'automorphism extensions' of hyperbolic toral automorphisms.

0. Introduction

The Chebotarev Theorem for a group extension of a shift of finite type σ gives us an asymptotic formula for the number of σ-closed orbits according to how they lift in the extension space and how they lift is completely determined by their Frobenius classes. It is with respect to these classes that the asymptotic formula applies. This, and indeed many more distribution results for closed orbits of shifts of finite type has been derived by the second author together with Mark Pollicott (see [3] for the entire collection).

Strictly speaking the above mentioned result is for a suspension flow over a shift of finite type. To obtain the appropriate result for the discrete case, all one needs do is use the constant function 1 as the suspension function.

Our aim in this paper is to study the analogous problem for a more general extension of the shift. In fact, our considerations here were motivated by two examples: a finite extension and a so-called automorphism extension of the shift. It will become apparent that to cater for these examples, the appropriate extension one should consider is a homogeneous extension, i.e., of the form $\tilde{\sigma}: X \times G/H \to X \times G/H$ for some (finite) group G and subgroup H.

Received 12 May 1992.

(1) Financially supported by Universiti Kebangsaan Malaysia

We observe that, unlike the group extension case, the lifted closed orbits may not have the same length. This unevenness will then be the basis for classifying the σ-closed orbits. To proceed with the asymptotics with respect to this classification we have to understand how these classes come about. We show that this is equivalent to looking at actions of certain cyclic subgroups on G/H. This is done by resorting to a certain group extension. Thus it is no surprise that our main result is just a direct application of the Chebotarev Theorem for group extensions.

1. Basic facts and Definitions

Let $\{1,2,\ldots,n\}$ be given the discrete topology and A be a $n\times n$ irreducible $0-1$ matrix. Define the set

$$X_A=\{x\in\prod_{-\infty}^{\infty}\{1,2,\ldots,n\}: A(x_i,x_{i+1})=1,\forall i\in\mathbb{Z}\}$$

Then X_A is a compact zero dimensional space. Let $\sigma: X_A\to X_A$ be defined by $(\sigma x)_i=x_{i+1}$. Then σ is called a shift of finite type (with transition matrix A). From now on we shall write X for X_A.

Recall that a homeomorphism $T: Y\to Y$ is said to be topologically transitive if T has a dense orbit. Also T is said to be topologically mixing if for any two non-empty open sets U,V in Y, there is an integer N such that $T^n(U)\cap V\neq\emptyset$ for all $n\geq N$.

For shifts of finite type, it is well-known that these two notions are equivalent to the requirement that the transition matrix A be irreducible and aperiodic respectively. The topological entropy of σ is $\log\beta$, where β is the maximal positive eigenvalue of A as furnished by the Perron-Frobenius Theorem.

Given a closed orbit (i.e. periodic orbit) τ of σ, we shall denote its least period by $\lambda(\tau)$. Then the zeta function of σ is defined as

$$\begin{aligned}\zeta_\sigma(z)&=\prod_\tau(1-z^{\lambda(\tau)})^{-1}\\&=\exp\sum_\tau\sum_{n=1}^{\infty}\frac{z^{\lambda(\tau)n}}{n}\quad\text{for } |z|<\beta^{-1}.\end{aligned}$$

In fact we have the following well known result of Bowen and Lanford.

Proposition 1.1. *Let σ be a shift of finite type with transition matrix A. And let β be the associated maximal positive eigenvalue. Then*

$$\zeta_\sigma(z)=\frac{1}{\det(I-zA)}\quad\textit{for } |z|<\beta^{-1}.$$

An immediate corollary to the above result is

Corollary 1.2. *Let σ be a topologically mixing shift of finite type. Then $\zeta_\sigma(z)$ has a non-zero analytic extension to a disc of radius greater than β^{-1} except for a simple pole at β^{-1}.*

Using this result Parry and Pollicott (see [3] pg 104) deduced the Prime Orbit Theorem for shifts of finite type:

Theorem 1.3. *Let σ be a mixing shift of finite type and let $\pi(x)=\mathrm{Card}\{\tau\subset X|\lambda(\tau)\leq x\}$. Then*

$$\pi(x)\sim\frac{\beta}{\beta-1}\cdot\frac{\beta^x}{x}\quad\textit{as } x\to\infty.$$

When σ is not topologically mixing, we can decompose X into a disjoint union of d (= period of A) closed-open sets $X_1,\ldots,X_d$ such that $\sigma(X_i)=X_j(j=i+1\mod d)$ and $\sigma^d|_{X_i}$ is topologically mixing, $i=1,\ldots,d$. Hence applying (1.3) to this case we have

Proposition 1.4. *When σ is not topologically mixing, then*

$$\pi(dx)\sim\frac{\beta^d}{\beta^d-1}\cdot\frac{\beta^{dx}}{x}\quad\textit{as } x\to\infty$$

where d is the period of the transition matrix A.

All groups considered in this paper are assumed to be finite. So let G be such a group and $\alpha: X\to G$ be a function depending on a finite number of coordinates. The group extension $\hat\sigma: X\times G\to X\times G$ of σ is then defined by the skew-product $\hat\sigma(x,g)=(\sigma x,\alpha(x)g)$. We shall always assume that $\hat\sigma$ is topologically transitive. Thus by definition $\hat\sigma$ is also a shift of finite type. Letting $\pi: X\times G\to X$ be $\pi(x,g)=x$, we have $\pi\hat\sigma=\sigma\pi$.

We are interested in how σ-closed orbits lift into the extension space. To classify these closed orbits, we introduce a free right-action of G on $X\times G$ by $h\cdot(x,g)=(x,gh),h\in G$. This action commutes with $\hat\sigma$. Thus given a closed orbit τ of σ with least period $\lambda(\tau)$ and a $\hat\sigma$-closed orbit $\hat\tau$ covering τ (i.e. $\pi(\hat\tau)=\tau$), there exists a unique element $\gamma(\hat\tau)\in G$ such that if $p\in\hat\tau$, then

$$\gamma(\hat\tau)p=\hat\sigma^{\lambda(\tau)}p.$$

In fact $\gamma(\hat{\tau})$ depends only on $\hat{\tau}$. This group element $\gamma(\hat{\tau})$ is called the *Frobenius element* of $\hat{\tau}$. Moreover if $\hat{\tau}'$ is another $\hat{\sigma}$-closed orbit also covering τ, then since G acts transitively on fibers, there exists an $h \in G$ such that $hp \in \hat{\tau}'$. Thus the Frobenius element $\gamma(\hat{\tau}')$ of $\hat{\tau}'$ satisfies

$$\gamma(\hat{\tau}')hp = \hat{\sigma}^{\lambda(\tau)}hp.$$

Hence $\gamma(\hat{\tau}') = h\gamma(\hat{\tau})h^{-1}$. In other words, the Frobenius elements of the lift of τ are all in the same conjugacy class which is uniquely determined by τ. This conjugacy class is called the Frobenius class of τ and is denoted by $[\tau]$.

Let R_χ be an irreducible representation of G with character χ. The L-function (with respect to $\pi: X \times G \to X$) of χ is defined as

$$L(z,\chi) = \prod_{\tau} \det\left(I - z^{\lambda(\tau)} R_\chi([\tau])\right)^{-1}$$

where the product is taken over all σ-closed orbits. By comparing the above expression with the zeta function of the shift we deduce that $L(z,\chi)$ is non-zero and analytic on $D = \{z \,|\, |z| < \beta^{-1}\}$. Observe that when $\chi = \chi_0$, the principal character, $L(z,\chi_0) = \zeta_\sigma(z)$. In fact one can show

Proposition 1.5. *Let $\hat{\sigma}$ be a group extension of σ with skewing function $\alpha: X \to G$ depending on a finite number of coordinates. Then*

$$L(z,\chi) = \frac{1}{\det(I - zM_\chi)} \quad \text{for} \quad |z| < \beta^{-1}$$

for some matrix M_χ closely related to the representation R_χ.

The Chebotarev Theorem of Parry and Pollicott for group extensions is as follows:

Theorem 1.6. *Let $\hat{\sigma}$ be a topologically transitive group extension of a shift of finite type σ. For a conjugacy class C of G, let $\pi_C(x) = \mathrm{Card}\{\tau \subset X: [\tau] = C, \lambda(\tau) \le x\}$. Then*

a) *if $\hat{\sigma}$ is mixing, $\pi_C(x) \sim \frac{|C|}{|G|}\frac{\beta}{\beta-1} \cdot \frac{\beta^x}{x}$ as $x \to \infty$,*

b) *if σ is mixing and $\hat{\sigma}$ not mixing with d = period of the transition matrix of $\hat{\sigma}$,*

$$\pi_C(x) \sim d\frac{|C|}{|G|}\frac{\beta^d}{\beta^d - 1} \cdot \frac{\beta^x}{x} \quad \text{as} \quad x \to \infty.$$

We indicate how one proves this result. We shall restrict our attention to the case when $\hat{\sigma}$ is mixing. To capture the σ-closed orbits with a given Frobenius class C, we introduce the following zeta function,

$$\zeta_C(z) = \prod_{\substack{\tau \\ [\tau]=C}} \left(1 - z^{\lambda(\tau)}\right)^{-1}.$$

Let $g \in C$. Then by the orthogonality relation for irreducible characters of G we have

$$\frac{|G|}{|C|}\frac{\zeta'_C(z)}{\zeta_C(z)} = \sum_{\chi \text{ irreducible}} \chi(g^{-1})\frac{L'(z,\chi)}{L(z,\chi)}.$$

Then we identify the poles of $\zeta'_C(z)/\zeta_C(z)$ in a small neighbourhood D' of $\{z \,|\, |z| \le \beta^{-1}\}$ and thus calculate their residues. We know that $L(z,\chi_0) = \zeta_\sigma(z)$ has a simple pole at $z = \beta^{-1}$ on the circle $\{z \,|\, |z| = \beta^{-1}\}$ and if we take D' to be small enough, $z = \beta^{-1}$ is the only pole in this region. To do this we bring in the identity (see Prop. 4 of [4])

$$\zeta_{\hat{\sigma}}(z) = \zeta_\sigma(z) \prod_{\chi \ne \chi_0} L(z,\chi)^{d_\chi}.$$

Since $\hat{\sigma}$ is a mixing shift of finite type with the same topological entropy as σ (because π is $|G|$ to 1) we deduce, via (1.5), that $L(z,\chi), \chi \ne \chi_0$ has a non-zero analytic extension to some neighbourhood D'' of $\{z \,|\, |z| \le \beta^{-1}\}$. Thus $\zeta'_C(z)/\zeta_C(z)$ has only one pole in the smaller of the two regions, namely $z = \beta^{-1}$ and its residue is $-|C|/|G|$. Then the proof proceeds analogously with the proof of the Prime Orbit Theorem for shifts of finite type (1.3).

Remarks.

1. The argument used in the above discussion comes from [4].
2. Observe that the assumption that the skewing function depends only on a finite number of coordinates plays two roles: Firstly it turns $\hat{\sigma}$ into a shift of finite type. Secondly, it also implies a meromorphic (in fact rational) extension of $L(z,\chi)$ to the whole plane.
3. There exists a similar formula for the case when σ is not mixing.

2. The Homogeneous Extension

As before let σ be a shift of finite type and G a finite group together with a map $\sigma: X \to G$ such that α depends on a finite number of coordinates. Let H be an arbitrary subgroup of G. Form the coset space $G/H = \{gH: g \in G\}$. A *homogeneous extension* $\tilde{\sigma}: X \times G/H \to X \times G/H$ of σ is defined by the skew-product $\tilde{\sigma}(x, gH) = (\sigma x, \alpha(x)gH)$. We shall always assume that $\tilde{\sigma}$ is topologically transitive. Let $\tilde{\pi}: X \times G/H \to X$ be such that $\tilde{\pi}(x, gH) = x$. Then $\tilde{\pi}\tilde{\sigma} = \sigma\tilde{\pi}$.

Observe that the group extension $\hat{\sigma}: X \times G \to X \times G$ defined by $\hat{\sigma}(x, g) = (\sigma x, \alpha(x)g)$ is, by using the obvious projection map, an extension of $\tilde{\sigma}$. We have the following multi-commutative diagram:

$$
\begin{array}{ccc}
X \times G \xrightarrow{\hat{\sigma}} X \times G & \searrow & \\
\pi \downarrow & & X \times G/H \xrightarrow{\tilde{\sigma}} X \times G/H \\
 & \swarrow \tilde{\pi} & \\
X \xrightarrow{\sigma} X & &
\end{array}
$$

Note that we cannot expect $\hat{\sigma}$ to be also topologically transitive. For our purposes, it suffices to note that if $\hat{\sigma}$ is not transitive then, as with all intransitive shifts of finite type, we can decompose $X \times G$ into $\hat{\sigma}$-invariant transitive pieces $X_0, \dots, X_{s-1}$. Moreover $\hat{\sigma}|_{X_i}$ is a G_i-invariant extension of X where G_i is the subgroup of G such that $gX_i = X_i \forall g \in G_i$. This follows since the group action commutes with $\hat{\sigma}$ and the fact that σ is transitive. Note that the subgroups $G_i, i = 0, 1, \dots, s-1$, are conjugate to each other. More importantly, by the transitivity of $\tilde{\sigma}$, we can identify $X \times G/H$ with the H_i-orbit space X_i/H_i where $H_i = H \cap G_i$. Hence by restricting to any X_i if necessary, there is no loss in generality in assuming that $\hat{\sigma}: X \times G \to X \times G$ is topologically transitive.

Recall that a partition of a positive integer k is a collection of positive integers $l_1, l_2, \dots, l_m$ such that $k \geq l_1 \geq l_2 \geq \dots \geq l_m \geq 1$ and $l_1 + \dots + l_m = k$. In this case we write $\underline{l}$ for the m-tuple $(l_1, \dots, l_m)$.

Let τ be a σ-closed orbit with period $\lambda(\tau)$ and $\tilde{\tau}$ be a $\tilde{\sigma}$-closed orbit with period $\lambda(\tilde{\tau})$ such that $\tilde{\pi}(\tilde{\tau}) = \tau$. Then the degree of $\tilde{\tau}$ over τ is defined by the integer

$$deg\left(\frac{\tilde{\tau}}{\tau}\right) = \frac{\lambda(\tilde{\tau})}{\lambda(\tau)}$$

Note that this is where the finiteness of G comes in. For in this case the lift of τ in $X \times G/H$ also consists of closed orbits. Moreover if $\tilde{\tau}_1, \dots, \tilde{\tau}_m$ are the distinct $\tilde{\tau}$-closed orbits that covers τ then the following basic relation holds:

$$deg\left(\frac{\tilde{\tau}_1}{\tau}\right) + \dots + deg\left(\frac{\tilde{\tau}_m}{\tau}\right) = \frac{|G|}{|H|},$$

so that the above equation gives us a partition of $|G|/|H|$. Thus we say τ induces the partition $\underline{l} = (l_1, \dots, l_m)$ of the integer $|G|/|H|$ if

$$\underline{l} = \left(deg\left(\frac{\tilde{\tau}_1}{\tau}\right), \dots, deg\left(\frac{\tilde{\tau}_m}{\tau}\right)\right) \quad \text{(after reordering if need be).}$$

Let K be another subgroup of G. We can define a left action of $k \in K$ on the coset space G/H by $k \cdot gH = kgH$. Let $K_1, \dots, K_m$ be the distinct orbits of this action and $r_i, i = 1, \dots, m$, be their respective 'sizes'. Notice that these r_i's form a partition of $|G|/|H|$. In this case we say K induces the partition $\underline{r} = (r_1, \dots, r_m)$ of $|G|/|H|$ (after reordering if need be). It is easy to see that if k is conjugate to k' then the respective cyclic subgroups generated by them induces the same partition of $|G|/|H|$.

For each partition $\underline{l}$ of $|G|/|H|$, let $A_{\underline{l}} = \{\tau \subset X: \tau \text{ induces the partition } \underline{l}\}$. Then we are interested in characterizing those $A_{\underline{l}}$'s that are non-empty. We have

Proposition 2.1. *Let τ be a σ-closed orbit. Then τ induces the partition $\underline{l}$ of $|G|/|H|$ $\Longleftrightarrow$ the action of the cyclic group generated by some (and hence all) Frobenius element g associated with τ induces the partition $\underline{l}$ on $|G|/|H|$.*

Proof. Let τ be a σ-closed orbit of period m such that τ induces the partition $\underline{l} = (l_1, \dots, l_n)$ of $|G|/|H|$. Suppose $\tilde{\tau}_1, \dots, \tilde{\tau}_n$ be the distinct $\tilde{\tau}$-closed orbits that covers τ. For $x \in \tau$, we write $\alpha_m(x) = \alpha(\sigma^{m-1}(x)) \dots \alpha(x)$. Then the fiber above x contained in $\tilde{\tau}_i$ consists of the elements

$$(x, a_i H), (x, \alpha_m(x) a_i H), \dots, (x, (\alpha_m(x))^{l_i - 1} a_i H)$$

for some $(x, a_i H) \in \tilde{\tau}_i$. Note that l_i is the least integer such that $(\alpha_m(x))^{l_i} a_i H = a_i H$. Thus $l_i = \deg(\tilde{\tau}_i/\tau)$. Let $J_i = \{a_i H, \dots, (\alpha_m(x))^{l_i - 1} a_i H\}$. Then clearly $J_i \cap J_k = \emptyset$ when $i \neq k$ and $G/H = \cup_{i=1}^{n} J_i$.

Let $< \alpha_m(x) >$ be the cyclic group generated by $\alpha_m(x)$. Evidently the J_i's are the distinct and indeed the totality of the orbits of the action of $< \alpha_m(x) >$ on G/H. Thus $< \alpha_m(x) >$ induces the partition $\underline{l}$ on G/H. By the definition of the group extension $\hat{\sigma}: X \times G \to X \times G$ and the right action $g \cdot (x, k) = (x, kg)$ of G on $X \times G$ we deduce that $\alpha_m(x)$ is indeed a Frobenius of τ.

Conversely, let $x \in \tau$, then reversing the previous argument we can construct the fiber above x by considering the distinct orbits of the action of $< \alpha_m(x) >$ on G/H. Then these distinct orbits constitute distinct $\tilde{\sigma}$-closed orbits covering τ. In fact this construction is independent of x since if $y \in \tau$ then $\alpha_m(y)$ is conjugate to $\alpha_m(x)$. This completes the proof. □

Remark. Observe that in general, we cannot expect the lift of τ in $X \times G/H$ to have equal period. For in this case we are dealing with a double coset partitioning of G. In the special case when $H = \{e\}$ (i.e. group extension), we do get equal period since the orbits of the subgroup action are just right cosets. In fact the degree of any $\tilde{\tau}$ over τ in this case is then equal to the order of the Frobenius element $\gamma(\tilde{\tau})$ of $\tilde{\tau}$.

Let $C(g)$ denote the conjugacy class containing g. As an immediate corollary to (2.1), we have

Corollary 2.2. *Let $C_i = \{\tau \subset X: [\tau] = C(g_i)\}$ be the distinct classes of σ-closed orbits with Frobenius class $C(g_i)$ respectively such that $< g_i >$ induces the partition $\underline{l}, i = 1, \ldots, m$. Then*

$$A_{\underline{l}} = \bigcup_{i=1}^{m} C_i.$$

For each partition $\underline{l}$, with $A_{\underline{l}} \neq \emptyset$, let $\pi_{\underline{l}}(x) = \mathrm{Card}\{\tau \subset X: \tau \in A_{\underline{l}}, \lambda(\tau) \leq x\}$. Hence by a direct application of the Chebotarev Theorem of Parry and Pollicott, we have, for e.g, the following result for a homogeneous extension.

Theorem 2.3. *Let $\tilde{\sigma}$ be a homogeneous extension of σ where the associated group extension $\hat{\sigma}$ is topologically mixing. Let $\underline{l}$ be a partition of $|G|/|H|$ such that $A_{\underline{l}} \neq \emptyset$. Then*

$$\pi_{\underline{l}}(x) \sim \frac{1}{|G|} \sum_{i=1}^{m} |C(g_i)| \pi(x)$$

where the $C(g_i)$'s are as in (2.2) and

$$\pi(x) \sim \frac{\beta}{\beta - 1} \cdot \frac{\beta^x}{x} \quad \text{as } x \to \infty.$$

3. Application I: Finite Extensions of shifts of finite type

Let $F = \{1, 2, \ldots, k\}$. A finite (k-point) extension of the shift σ is a skew-product $\tilde{\sigma}: X \times F \to X \times F$ defined by $\tilde{\sigma}(x, i) = (\sigma x, \alpha(x)(i))$ where $\alpha: X \to G$, as usual depends on a finite number of coordinates and G is the symmetric group S_k on k-symbols $\{1, 2, \ldots, k\}$.

Now, let $H = \{h \in G: h(1) = 1\}$. Then $H \cong S_{k-1}$. Also it is clear that the map from F to G/H sending i to gH where $g(i) = i$ is a bijection. Therefore we can identify $X \times F$ with $X \times G/H$ and obtain the homogeneous extension $\tilde{\sigma}: X \times G/H \to X \times G/H$ defined by $\tilde{\sigma}(x, gH) = (\sigma x, \alpha(x)gH)$. Letting $\tilde{\pi}: X \times G/H \to X$ be $\tilde{\pi}(x, gH) = x$ we have $\tilde{\pi}\tilde{\sigma} = \sigma\tilde{\pi}$. We shall assume that $\tilde{\sigma}$ is topologically transitive.

Also we have $\hat{\sigma}: X \times G \to X \times G$ where $\hat{\sigma}(x, g) = (\sigma x, \alpha(x)g)$. So that $\hat{\sigma}$ is a group extension of σ. As mentioned in §2 there is no loss of generality in assuming $\hat{\sigma}$ is also topologically transitive.

Recall that an element g of a symmetric group G is said to have cycle decomposition $\underline{m} = (m_1, m_2, \ldots, m_t)$ if it can be written as the product of disjoint cycles of length $m_1, m_2, \ldots, m_t$ where $m_1 \geq m_2 \geq \ldots \geq m_t$. Recall also that two elements of G are conjugate if and only if they have the same cycle decomposition.

Proposition 3.1. *Let $\underline{l}$ be an arbitrary partition of k. Then $A_{\underline{l}} \neq \emptyset$. Moreover $A_{\underline{l}} = \{\tau \subset X: [\tau] = C_{\underline{l}}\}$ where $C_{\underline{l}}$ is the conjugacy class of G consisting of elements with cycle decomposition $\underline{l}$.*

Proof. Let $\underline{l} = (l_1, \ldots, l_n)$ be a partition of k. Thus there exists some $g \in G$ such that g has cycle decomposition $\underline{l}$. This follows since each partition $\underline{n}$ of k can be uniquely associated with the conjugacy class $C_{\underline{n}}$ of G consisting of elements with cycle decomposition $\underline{n}$. Now consider the action of the cyclic group $< g >$ generated by g on $F = \{1, 2, \ldots, k\}$. Then using the cycle decomposition form of g, it is clear that this action gives rise to n orbits $O_1, \ldots, O_n$ such that $|O_i| = l_i, i = 1, \ldots, n$. In other words $< g >$ induces the partition $\underline{l}$ on F or equivalently on G/H. Since this only depends on the cycle decomposition $\underline{l}$ of g and elements with such a cycle decomposition constitute a whole conjugacy class $C_{\underline{l}}$ we have $A_{\underline{l}} = \{\tau \subset X: [\tau] = C_{\underline{l}}\}$ by (2.2). □

The Cauchy formula (see for e.g [2]) for the cardinality of $C_{\underline{l}}$ gives us

$$|C_{\underline{l}}| = \frac{k!}{l_{i_1}^{\alpha_{i_1}} \alpha_{i_1}! \ldots l_{i_s}^{\alpha_{i_s}} \alpha_{i_s}!}$$

where the l_{i_j}'s are the distinct components of $(l_1, l_2, \ldots, l_m)$ and α_{i_j} is the number of cycles of length l_{i_j} in the cycle decomposition of $g \in C_{\underline{l}}$. Hence, for a finite extension of a shift of finite type (c.f. (2.3)), we have

Theorem 3.2. *Let $\tilde{\sigma}$ be a finite (k-point) extension of a shift of finite type σ where the associated group extension $\hat{\sigma}$ is topologically mixing. For each partition $\underline{l}$ of the integer k, let $\pi_{\underline{l}}(x) = \mathrm{Card}\{\tau \subset X: \tau \in A_{\underline{l}}, \lambda(\tau) \leq x\}$.*

Then

$$\pi_{\underline{l}}(x) \sim \frac{1}{l_{i_1}^{\alpha_{i_1}}\alpha_{i_1}!\dots l_{i_s}^{\alpha_{i_s}}\alpha_{i_s}!}\pi(x)$$

where the l's and α's are as above and

$$\pi(x) \sim \frac{\beta}{\beta-1}\cdot\frac{\beta^x}{x} \quad as \quad x \to \infty.$$

Example. In the case of a 3-point extension $\tilde{\sigma}$ of i.e. $G = S_3$, the σ-closed orbits can lift in the extension space in 3 different ways. These corresponds to the partition $(1,1,1)$, $(2,1)$ and (3). Let us define the density $D_{\underline{l}}$, of the σ-closed orbits that lift in the extension space corresponding to the partition $\underline{l}$ as

$$D_{\underline{l}} = \lim_{x\to\infty}\frac{\pi_{\underline{l}}(x)}{\pi(x)}$$

Since S_3 has 1 element with cycle decomposition $(1,1,1)$, 3 elements with cycle decomposition $(2,1)$ and 2 elements with cycle decomposition (3), we deduce that the densities $D_{(1,1,1)}, D_{(2,1)}, D_{(3)}$ are $1/6$, $1/2$ and $1/3$ respectively.

We remark that our consideration here was really motivated by an analogous number theoretic example due to Heilbronn (see pg 227 of [1]). In this example he considered a non-normal cubic field extension K_3/k and in particular was interested in the densities of primes in k according to how they lift into K_3. Roughly speaking, we can say that the primes in k splits in K_3 according to the partitions $(1,1,1)$, $(2,1)$ and (3) (of the number 3). To calculate the densities, Heilbronn then considered the minimal extension K_6 of K_3 that is normal over k and argued that the primes that splits in K_3 according to the partition $(1,1,1)$, $(2,1)$ and (3) corresponds precisely to the primes that splits in K_6 with Frobenius class $C(e)$, $C(2,3)$, $C(1,3,2)$ respectively. Note that the Galois group of K_6/k is S_3. Then applying the Chebotarev Theorem for the normal extension K_6/k, he deduced that (using the above notation) the densities $D_{(1,1,1)}$, $D_{(2,1)}$, $D_{(3)}$ are equal to $1/6$, $1/2$, $1/3$ respectively.

4. Application II: Automorphism extensions of shifts of finite type

We now apply our findings of §2 to a so-called automorphism extension of the shift. As always let σ be a shift of finite type and G a finite group. Let $\gamma: G \to G$ be an automorphism of G and $\beta: X \to G$ be a function depending on a finite number of coordinates. An automorphism extension $\tilde{\sigma}$ of the shift is defined as the skew-product $\tilde{\sigma}: X \times G \to X \times G$ where $\tilde{\sigma}(x,g) = (\sigma x, \beta(x)\gamma(g))$. Letting

$\tilde{\pi}(x,g) = x$ we have $\tilde{\pi}\tilde{\sigma} = \sigma\tilde{\pi}$. We shall assume that $\tilde{\sigma}$ is topologically transitive. Thus by definition $\tilde{\sigma}$ is also a shift of finite type.

Note that since G is finite there exists a least n such that $\gamma^n = \text{id}$. Now consider the following cyclic extension of $\tilde{\sigma}$. That is $\hat{\sigma}: \mathbb{Z}_n \times X \times G \to \mathbb{Z}_n \times X \times G$ defined by

$$\hat{\sigma}(r,(x,g)) = (r+1,(\sigma(x),\beta(x)\gamma(g))).$$

Also observe that except possibly for trivial $\gamma, \hat{\sigma}$ is never mixing. We can rewrite $\hat{\sigma}$ as $\hat{\sigma}: X \times \mathbb{Z}_n \times G \to X \times \mathbb{Z}_n \times G$ and $\hat{\sigma}(x,(r,g)) = (\sigma x,(r+1,\beta(x)\gamma(g)))$. We give the set $\mathbb{Z}_n \times G$ a group structure by defining the product of $(r,g),(s,h) \in \mathbb{Z}_n \times G$ as follows:

$$(r,g)\cdot(s,h) = (r+s, g\gamma^r(h))$$

and denoting the resulting group by $\mathbb{Z}_n \times_\gamma G$. Then $\mathbb{Z}_n \times_\gamma G$ with this operation defined on its elements is known as the semi-direct product of G by $\mathbb{Z}_n$ or a $\mathbb{Z}_n$ cyclic extension of G.

Let $\alpha: X \to \mathbb{Z}_n \times_\gamma G$ be defined as $\alpha(x) = (1,\beta(x))$ and let $G' = \mathbb{Z}_n \times_\gamma G$. Then we can rewrite $\hat{\sigma}$ as $\hat{\sigma}: X \times G' \to X \times G'$ and $\hat{\sigma}(x,k) = (x,\alpha(x)k)$, $k \in G'$, so that we can view $\hat{\sigma}$, as a group extension of σ. We can define a free action of G' on $X \times G'$ by $l(x,k) = (x,kl)$, $k,l \in G'$, and deduce that it commutes with $\hat{\sigma}$. Thus the notion of Frobenius class exists for σ-closed orbits.

Now, let H be the subgroup $\mathbb{Z}_n \times \{e\}$, ($e$ = identity of G) of G'. Consider the action of H on $X \times G'$. Then a typical element of the H-orbit space will take the form $(x,(0,g)H)$ where we write $(x,(0,g)H)$ to mean the set $\{(x,(r,g)): r \in \mathbb{Z}_n\}$. Moreover it is easy to see that the induced map σ_2 satisfy $\sigma_2(x,(0,g)H) = (\sigma x,(0,\beta(x)\gamma(g))H)$. Hence we can identify $(X \times G, \tilde{\sigma})$ with $((X \times G')/H, \sigma_2)$.

In other words we are in the setting of a homogeneous space extension of the shift and thus the result of §2 applies once we have formulated the Chebotarev Theorem for the extension $\pi: X \times G' \to X$. In particular given $(r,g) \in G'$ we would want to look at the action of $< (r,g) >$ on G'/H. Note that this is equivalent to studying the map $T_{(r,g)}: G'/H \to G'/H$ defined by $T_{(r,g)}((s,k)H) = (r,g)(s,k)H$. The following result may simplify the calculations.

Proposition 4.1. *Let $(r,g) \in G'$. Then $T_{(r,g)}$ is conjugate to the map $S_{(r,g)}: G \to G$ defined by $S_{(r,g)}(k) = g\gamma^r(k)$.*

Proof. Recall that a typical element of G'/H takes the form

$$(s,k)H = \{(s,k)(t,e) : t \in \mathbb{Z}_n\} = \{(s,k) : s \in \mathbb{Z}_n\}.$$

Hence G'/H can be identified with G via the map $(s,k)H \overset{L}{\longmapsto} k$. Also

$$T_{(r,g)}((s,k)H) = (r,g)(s,k)H = (s, g\gamma^r(k))H.$$

Thus letting $S_{(r,g)}(k) = g\gamma^r(k)$, $k \in G$, we deduce that $LT_{(r,g)} = S_{(r,g)}L$. The result follows since L, $T_{(r,g)}$ and $S_{(r,g)}$ are bijective maps. □

As usual (a,b) shall denote the h.c.f of a and b.

Proposition 4.2. *Let $\tilde{\tau}$ be a $\tilde{\sigma}$-closed orbit with $\lambda(\tilde{\tau}) = k$ and $\hat{\tau}_1, \ldots, \hat{\tau}_r$ be the $\hat{\sigma}$-closed orbits that cover $\tilde{\tau}$. Then $\lambda(\hat{\tau}_i) = $ l.c.m $[k,n]$, $i = 1, \ldots, r$ where $r = (k,n)$.*

Proof. Let $x \in \tau$. Then for all $r \in \mathbb{Z}$, $\hat{\sigma}^m(r,x) = (r+m, \hat{\sigma}^m(x)) = (r,x)$ implies m is a multiple of both n and k. Hence the least period of $(r,x) =$ l.c.m $[k,n]$. Recall that l.c.m $[a,b] = ab/(a,b)$. Thus since

$$\sum_{i=1}^{r} \deg \frac{\lambda(\hat{\tau}_i)}{\lambda(\tilde{\tau})} = n,$$

we have $r = (k,n)$. And this completes the proof. □

Let $\zeta_{\hat{\sigma}}(z)$, $\zeta_{\tilde{\sigma}}(z)$ be the zeta functions of $\hat{\sigma}$ and $\tilde{\sigma}$ respectively. Then we have

Proposition 4.3.

$$\zeta_{\hat{\sigma}}(z) = \prod_{i=0}^{n-1} \zeta_{\tilde{\sigma}}(\omega^i z),$$

where ω is a primitive n-th root of unity.

Proof. First we note that

$$1 + \omega^r + \omega^{2r} + \cdots + \omega^{(n-1)r} = \begin{cases} n, & \text{if } n|r; \\ 0, & \text{otherwise.} \end{cases}$$

Thus for $z \in \mathbb{C}$ and $k \in \mathbb{Z}^+$,

$$\sum_{m=1}^{\infty} \frac{z^{km}}{m}\{1 + \omega^{km} + \cdots + \omega^{(n-1)km}\} = \sum_{l=1}^{\infty} \frac{(n,k)}{l} z^{\frac{kn}{(n,k)}l}$$

$$= \sum_{i=1}^{(n,k)} \sum_{l=1}^{\infty} \frac{z^{\frac{kn}{(n,k)}l}}{l}.$$

Hence

$$\log(1-z^k) + \log(1-(\omega z)^k) + \cdots + \log(1-(\omega^{n-1}z)^k) = (n,k)\log(1 - z^{\frac{kn}{(n,k)}}).$$

That is

$$(1-z^k)(1-(\omega z)^k)\cdots(1-(\omega^{n-1}z)^k) = (1 - z^{\frac{kn}{(n,k)}})^{(n,k)}.$$

Let $\tilde{\tau}$ be a $\tilde{\sigma}$-closed orbit such that $\lambda(\tilde{\tau}) = k$. Then by (4.2),

$$\prod_{i=0}^{n-1}(1 - (\omega^i z)^{\lambda(\tilde{\tau})}) = \prod_{\pi(\hat{\tau}) = \tilde{\tau}} (1 - z^{\lambda(\hat{\tau})}).$$

The result follows by inverting and taking products over all $\tilde{\sigma}$-closed orbits. □

Corollary 4.4. *If $\tilde{\sigma}$ is mixing then $\zeta_{\hat{\sigma}}(z)$ has a non-zero analytic extension to a neighbourhood of $\{z \,|\, |z| \le \beta^{-1}\}$ except for simple poles at $(\omega^i\beta)^{-1}$, $i = 0, 1, \ldots, n-1$ where ω is a primitive n-th root of unity.*

Proof. The result follows since $\hat{\sigma}$ is a topologically transitive shift of finite type. □

Thus for mixing $\tilde{\sigma}$ the second part of (1.6) holds with $n =$ period of the transition matrix of $\hat{\sigma}$. Hence the Chebotarev Theorem for the extension $\pi : X \times \mathbb{Z}_n \times_\gamma G \to X$ is

Theorem 4.5. *Let $\tilde{\sigma}$ be a mixing automorphism extension of σ and $\hat{\sigma}$ be the associated $\mathbb{Z}_n$ cyclic extension. Then, given a conjugacy class C,*

$$\pi_C(x) \sim \frac{|C|}{|G'|} \cdot n \cdot \frac{\beta^n}{\beta^n - 1} \frac{\beta^x}{x} \quad \text{as} \quad x \to \infty.$$

We now come to the main result in this section. Since the automorphism extension $\tilde{\sigma}$ can be identified with a homogeneous extension of σ with respect to the subgroup $H = \mathbb{Z}_n \times \{e\}$, we can apply our findings in §2 to the above theorem to obtain

Theorem 4.6. *Let $\tilde{\sigma}$ be a mixing automorphism extension of a shift of finite type σ. If $\underline{l}$ is a partition of $|G'/H|$ such that*

$$A_{\underline{l}} := \{\tau \subset X : \tau \text{ induces the partition } \underline{l} \text{ on } |G'|/|H|\}$$

$$= \bigcup_{i=1}^{m} C_i$$

where $C_i = \{\tau \subset X : [\tau] = C(r_i, g_i)\}$, $i = 1, \ldots, m$, then

$$\pi_{\underline{l}}(x) \sim \sum_{i=1}^{m} \frac{|C(r_i, g_i)|}{|G'|} \cdot n \cdot \frac{\beta^n}{\beta^n - 1} \cdot \frac{\beta^x}{x} \quad \text{as} \quad x \to \infty.$$

There is another situation where a "homogeneous extension" arises. Let $\tilde{A}$ be a hyperbolic automorphism of a finite dimensional torus $\mathbf{T}$. Let G be the set of all points in $\mathbf{T}$ with order m, say. Then G is an (abelian) group such that $\tilde{A}G = G$. We let G act on the right of $\mathbf{T}$ and using additive notation we have

$$\tilde{A}(x+g) = \tilde{A}(x) + \tilde{A}(g) \qquad x \in \mathbf{T}, g \in G.$$

Then $\tilde{A}$ induces an action A on the G-orbit space $\mathbf{T}/G$ such that $A\colon \mathbf{T}/G \to \mathbf{T}/G$ is also a hyperbolic toral automorphism. If $\tilde{A}^n|_G = \mathrm{Id}$, then working analogously with the automorphism extension, we can define the $\mathbb{Z}_n$-cyclic extension of $\tilde{A}$ and thus is in the setting studied above. In fact, one can show that the automorphism extension of the shift is actually the symbolic model for our toral automorphism (see pg 137 of [4] for the main idea). Furthermore since the counting functions for the shifts and the toral automorphisms are asymptotic (see [3]) we deduce that the statements of Theorems (4.5) and (4.6) also holds for "automorphism extensions" of hyperbolic toral automorphisms.

We illustrate the above discussion by the following example:

Example. Let $\tilde{A}$ be the hyperbolic automorphism on the two-dimensional torus $\mathbf{T}$ induced by the matrix

$$\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}.$$

Here we take $\mathbf{T}$ to be the unit square on $\mathbb{R}^2$ with respect to addition mod 1 and the appropriate identifications. Let

$$G = \{(0,0),(0,1/2),(1/2,0),(1/2,1/2)\}$$

i.e. G consists of elements of $\mathbf{T}$ with order 2. Then $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Also, one can easily check that $\tilde{A}^3|_G = \mathrm{Id}$. Thus the associated semi-direct product group is $G' = \mathbb{Z}_3 \times_{\tilde{A}} (\mathbb{Z}_2 \times \mathbb{Z}_2)$. Now G' has 4 conjugacy classes:

$$\begin{aligned} C_1 &= \{(0,(0,0))\}, \\ C_2 &= \{(0,(0,1)),(0,(1,1)),(0,(1,0))\}, \\ C_3 &= \{(1,(0,0)),(1,(1,0)),(1,(1,1)),(1,(0,1))\}, \\ C_4 &= \{(2,(0,0)),(2,(1,1)),(2,(1,0)),(2,(0,1))\}. \end{aligned}$$

By using (4.1), it is straight-forward to check that C_1 gives rise to the partition $(1,1,1,1)$, C_2 to the partition $(2,2)$ and both C_3, C_4 to the partition $(3,1)$ on $|G'/\mathbb{Z}_3 \times \{e\}|$. This implies that, given a closed orbit $\tau \in \mathbf{T}/G$, the 'types' of $\tilde{A}$-closed orbits covering τ can only take one of the following forms: There are, depending on the Frobenius class of τ,

i. 4 closed orbits each of degree 1 over τ,
ii. 2 closed orbits each of degree 2 over τ, or
iii. 2 closed orbits, one of degree 3 and one of degree 1 over τ.

Hence the asymptotic formulas for types i, ii, ii, are

$$\begin{aligned} \pi_{(1,1,1,1)}(x) &\sim \frac{1}{12}\cdot 3\cdot \frac{\beta^3}{\beta^3-1}\cdot\frac{\beta^x}{x}, \\ \pi_{(2,2)}(x) &\sim \frac{3}{12}\cdot 3\cdot \frac{\beta^3}{\beta^3-1}\cdot\frac{\beta^x}{x}, \\ \pi_{(3,1)}(x) &\sim \frac{8}{12}\cdot 3\cdot \frac{\beta^3}{\beta^3-1}\cdot\frac{\beta^x}{x}, \quad \text{as } x\to\infty, \quad \text{respectively.} \end{aligned}$$

References

[1] Cassels, J. W. S. and Fröhlich, A., *Algebraic Number Theory*, (Academic Press, London, 1967).

[2] Ledermann, W., *Introduction to Group Theory*, (Oliver & Boyd, 1973).

[3] Parry, W. and Pollicott, M., *Zeta functions and the periodic orbit structure of hyperbolic dynamics*, 1990, Astérisque **187-188**.

[4] Parry, W. and Pollicott, M., *The Chebotarev Theorem For Galois Coverings of Axiom A Flows*, Ergod. Theory & Dynam. Sys. **6** (1986), 133-148.

Mohd. Salmi Md. Noorani
William Parry
Mathematics Institute
University of Warwick
Coventry CV4 7AL, UK