Shift equivalence and strong shift equivalence of subshifts of finite type

Brad Hannigan-Daley
University of Toronto

Shift equivalence and the Williams Conjecture

A central problem in symbolic dynamics is the classification of two-sided subshifts of finite type (SFTs) up to topological conjugacy. Each SFT is topologically conjugate to an edge shift Σ_A for some adjacency matrix A with entries in the nonnegative integers $\mathbb{Z}^+$, so a natural route of investigation for the classification problem is to try to define some algebraically described equivalence relation on the set of these adjacency matrices such that two matrices are equivalent if and only if their edge shifts are topologically conjugate. To this end, R.F. Williams defined in 1973 two equivalence relations on the set of square matrices over $\mathbb{Z}^+$.[14] Let Λ be a semiring, and let A, B be square matrices with entries in Λ. We say that A and B are *lag-1 shift equivalent over* Λ if there exists a pair R, S of matrices with entries in Λ such that $A = RS$ and $B = SR$. This relation, while obviously reflexive and symmetric, is not transitive. [10] The transitive extension of this relation is the equivalence relation we call *strong shift equivalence* (SSE). Williams showed that two SFTs Σ_A and Σ_B are topologically conjugate if and only if A and B are SSE over $\mathbb{Z}^+$. The problem of determining whether two such matrices are SSE over $\mathbb{Z}^+$, however, is currently not known to be decidable even for two-by-two matrices. [4]

A more understandable relation, called shift equivalence (SE), was also introduced by Williams. Two square matrices A and B over Λ are said to be *shift equivalent* if there exist matrices R, S over Λ and a positive integer ℓ (called the *lag*) such that $A^\ell = RS, B^\ell = SR$, $AR = RB$ and $SA = BS$. We note that, given such a shift equivalence, by replacing S by SA we obtain another shift equivalence of lag $\ell + 1$, and so there is such a shift equivalence of lag L for each $L \geq \ell$. The equations defining shift equivalence then give us immediately that A^L and B^L are lag-1 shift equivalent, hence SSE, for each $L \geq \ell$. In general, if (X, f) and (Y, g) are cascades, we say that they are *eventually conjugate* if (X, f^L) and (Y, g^L) are conjugate for all but finitely many $L > 0$. As conjugacy of edge shifts is equivalent to SSE over $\mathbb{Z}^+$ of adjacency matrices, we then have that if A and B are shift equivalent, then their associated edge shifts are eventually conjugate. In fact, the converse holds: edge shifts Σ_A and Σ_B are eventually conjugate if and only if A and B are SE over $\mathbb{Z}^+$. [11] This provides us with a dynamical interpretation of the algebraic notion of SE, and immediately implies that SE is indeed an equivalence relation which is a priori weaker than SSE.

The decision problem for SE is much better understood than the decision problem for SSE. There does exist an (unwieldy) algorithm [5] for determining whether two matrices are SE over $\mathbb{Z}^+$. In his original paper, Williams gave a proof that SE over $\mathbb{Z}^+$ implies SSE over $\mathbb{Z}^+$; unfortunately, his proof was incorrect, and the statement of this result became known as the Williams Conjecture. [14] The truth of this conjecture remained unknown for over fifteen years, until Kim and Roush [8] constructed two eight-by-eight reducible matrices over $\mathbb{Z}^+$ which are SE but not SSE, thereby refuting the conjecture as stated. However, the problem remained open for the important case where we restrict our attention to irreducible matrices, which correspond to irreducible SFTs. By restricting our attention further to primitive matrices, the problem is simplified: for Λ a unital subring of $\mathbb{R}$, it is known that primitive matrices are SE over Λ if and only if they are SE over the semiring $\Lambda^+ = \{\alpha \in \Lambda : \alpha \geq 0\}$. [12] Additionally, we have a result of Boyle and Handelman [2] which states that SE over Λ is equivalent to SSE over Λ whenever Λ is a Dedekind domain. It follows that the primitive Williams Conjecture is equivalent to the statement that if two primitive matrices are SSE over $\mathbb{Z}$, then they

are SSE over $\mathbb{Z}^+$.

Given matrices A and B over Λ, a strong shift equivalence between these is given by matrices $R_1, \ldots, R_\ell$ and $S_1, \ldots, S_\ell$ such that $A = R_1S_1, S_1R_1 = R_2S_2, \ldots, S_\ell R_\ell = B$. Intuitively, we can think of such an equivalence as a "path" from A to B in some sense. Wagoner [13] formalized this intuition and introduced an oriented CW complex called the *space of strong shift equivalences over* Λ, denoted $RS(\Lambda)$. By some combinatorial arguments, a certain homotopy-invariant $\mathbb{Z}/2$-valued function sgc_2 is defined on the set of paths in $RS(\mathbb{Z})$. [9] With computer assistance, Kim and Roush found seven-by-seven matrices A, B over $\mathbb{Z}^+$ and R, S over $\mathbb{Z}$ such that $A = RS$ and $B = SR$ are primitive, and such that every strong shift equivalence (path) $\mathcal{P}$ from A to B over $\mathbb{Z}$ satisfies $sgc_2(\mathbb{Z}) = 1$. But from some algebraic properties of A and B they deduce that sgc_2 must vanish on any strong shift equivalence from A to B over $\mathbb{Z}^+$, hence no such equivalence exists and this pair A, B gives a counterexample to the reformulation of the Williams Conjecture for primitive matrices, as given above. The upshot of Kim and Roush's counterexamples is that we cannot necessarily determine whether two SFTs are conjugate simply by determining whether their corresponding adjacency matrices are SE. However, SE is still often capable of distinguishing SFTs, and as previously mentioned it has the advantage over SSE of currently being known to be decidable.

Invariants

Kim and Roush [5] have shown that the problem of determining whether two matrices are SE is decidable. However, the currently known procedures for doing so are difficult to apply in general. [11] A number of more easily computed invariants have been developed for distinguishing non-SE matrices. (Note that since topological conjugacy of edge shifts implies SSE of their associated matrices, which in turn implies SE, any invariant of SE also gives an invariant of topological conjugacy of edge shifts.) We discuss here some of these invariants.

Jordan form away from zero

Let A be a square matrix of order m over $\mathbb{Z}^+$, and let J_A be the Jordan form of A. We define the *Jordan form of A away from zero* to be the principal submatrix of J_A with nonzero entries on the diagonal, denoted J_A^*, and claim that this is invariant under SE. We decompose $\mathbb{R}^m$ into a direct sum $K_A \oplus I_A$, where K_A is the invariant space corresponding to the Jordan block(s) of A with eigenvalue zero and I_A corresponds to the rest of the Jordan blocks. We call K_A and I_A the *eventual kernel* of A and the *eventual image* of A, respectively. By construction, A restricts to a nilpotent operator on K_A and to an automorphism of I_A; this latter automorphism is represented by the matrix J_A^*. Let B be a square matrix of order n. Suppose that A and B are SE, with $A^\ell = RS, SR = B^\ell, AR = RB, SA = BS$. We may assume without loss of generality that the lag ℓ is at least $\max\{m, n\}$, so that $A^\ell(\mathbb{R}^m) = I_A$ and $B^\ell(\mathbb{R}^n) = I_B$. We claim that R restricts to an isomorphism $\tilde{R} : I_B \to I_A$. We check that

$$R(I_B) = RB^\ell(\mathbb{R}^n) = A^\ell R(\mathbb{R}^n) \subset A^\ell(\mathbb{R}^m) = I_A$$

so R does indeed restrict to a linear map $\tilde{R} : I_B \to I_A$. Symmetrically, S restricts to a linear map $\tilde{S} : I_A \to I_B$. Since $SR = B^\ell$ is an automorphism of I_B, we conclude that $\tilde{R}$ is injective, and symmetrically so is $\tilde{S}$. Then $\dim I_A = \dim I_B$, and $\tilde{R}$ is an isomorphism as claimed. From the equation $AR = RB$, by restricting our attention to the domain I_B we conclude that $\tilde{R}$ defines a conjugacy of the restrictions $A|_{I_A}$ and $B|_{I_B}$, and we conclude that $J_A^* = J_B^*$.

The *characteristic polynomial of A away from zero*, denoted $c_A^*(x)$, is the characteristic polynomial of A with all powers of t divided out. Alternatively, we may define it as the characteristic polynomial of J_A^*, and we then see that this is invariant under SE by the above. Given a square matrix A of order m over $\mathbb{Z}^+$, the *zeta function* of Σ_A is the formal power series

$$\zeta_A(t) = \exp\left(\sum_{k=1}^{\infty} \frac{\mathrm{Fix}(A,k)}{k} t^k\right)$$

where $\mathrm{Fix}(A,k)$ is the number of points in Σ_A which are fixed by the kth power of the shift. Each fixed point of the kth power of the shift corresponds to a directed cycle of length k in the directed graph defined by A, hence $\mathrm{Fix}(A,k) = tr(A^k)$. Using this fact we can compute $\zeta_A(t) = \det(I - tA)^{-1}$. [10] Let $\mu_1, \ldots, \mu_m$ be the eigenvalues of A, including multiplicity. If d is the degree of $c_A^*(x)$, then $t^d c_A^*(x) = t^d \prod_{i=1}^m (x - \mu_j)$. Substituting $x = t^{-1}$, we have $t^d c_A^*(t^{-1}) = \prod_{i=1}^m (1 - t\mu_j) = \det(I - tA) = \zeta_A(t)^{-1}$. It follows that the zeta function of Σ_A, and therefore the number of fixed points for each power of the shift, can be recovered from the Jordan form away from zero.

The spectral radius $\lambda(A)$ of A is determined by J_A^*, and so this eigenvalue is also an invariant of SE. Of course, we already know that the topological entropy of Σ_A is $\log \lambda(A)$, and this is invariant under topological conjugacy and therefore under SSE. We note that there are simple examples which show that the condition $J_A^* = J_B^*$ is not strong enough to guarantee shift equivalence of A and B. [10]

Bowen-Franks groups

Let A be a square matrix of order n over the integers, and let $\mathcal{R}$ be a commutative ring. Then A naturally induces an endomorphism of the additive group $\mathcal{R}^n$, defined by $Ar = (\sum_{i=1}^n A_{1i} r_1, \ldots, \sum_{i=1}^n A_{ni} r_n)$. Fix a polynomial $p(x) \in \mathcal{R}[x]$ whose constant term is a unit in $\mathcal{R}$. Then $p(A)$ is a group endomorphism of $\mathcal{R}^n$, hence its image $p(A)\mathcal{R}^n$ is a subgroup of $\mathcal{R}^n$. The quotient group $\mathcal{R}^n/p(A)\mathcal{R}^n$ is the *(generalized) Bowen-Franks group* of A with respect to $\mathcal{R}$ and p. We can define a surjective group homomorphism $\alpha : \mathcal{R}^n \to \mathcal{R}^n/p(A)\mathcal{R}^n$ by $\alpha(x) = Ax + p(A)\mathcal{R}^n$, and this homomorphism has kernel $p(A)\mathcal{R}^n$ and therefore descends to an automorphism A_* of $\mathcal{R}^n/p(A)\mathcal{R}^n$. [10] It can be shown that a shift equivalence between two matrices A and B induces isomorphisms R_* and S_* between their respective Bowen-Franks groups such that $R_*^{-1} A_* R_* = B_*$, similarly to how such a shift equivalence induces a conjugacy of $A|_{I_A}$ and $B|_{I_B}$ above. [10]

The Bowen-Franks groups are a particularly useful family of SE invariants when $\mathcal{R} = \mathbb{Z}$ or $\mathcal{R} = \mathbb{Z}[t]$. For $\mathcal{R} = \mathbb{Z}$, these groups are finitely generated abelian groups and often readily computable. The group originally called "the Bowen-Franks group" is the special case of this construction where $\mathcal{R} = \mathbb{Z}$ and $p(x) = 1 - x$. We denote this group by $\mathsf{BF}(A) := \mathbb{Z}^n/(1 - A)\mathbb{Z}^n$. This group is particularly easy to compute: by applying elementary row/column operations over $\mathbb{Z}$, we may change $I - A$ into its *Smith normal form*, a diagonal matrix with nonnegative integer entries $d_1, \ldots, d_n$ along the diagonal such that d_j divides d_{j+1} for each j. It can then be shown [11] that $\mathsf{BF}(A) \cong (\mathbb{Z}/d_1\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/d_n\mathbb{Z})$.

Ideal class invariants

While the Bowen-Franks groups and Jordan form away from zero are readily computed and often succeed in distinguishing non-SE matrices, even taken together they do not provide a complete invariant of SE. For example, for any square matrix A over $\mathbb{Z}^+$, $J_A^* = J_{A^T}^*$ and it can be shown that $\mathsf{BF}(A) \cong \mathsf{BF}(A^T)$. [11] However, there exist matrices which are not SE to their transpose, even over $\mathbb{Z}$. [11] If we restrict our attention to irreducible matrices, there are some other invariants which can be computed using techniques

from algebraic number theory. Suppose A is an irreducible matrix over $\mathbb{Z}^+$, with Perron eigenvalue λ. We can use Gaussian elimination to find an eigenvector $v = (v_1, \ldots, v_n)$ of A corresponding to λ, such that each v_i lies in the field of fractions of $\mathbb{Z}[\lambda]$. By clearing denominators we may assume that each $v_i \in \mathbb{Z}[\lambda]$. Since λ is an algebraic integer, we have $\mathbb{Z}[\lambda] \subset \mathbb{Z}[1/\lambda]$, so we may consider the ideal generated by $v_1, \ldots, v_n$ in the ring $\mathbb{Z}[1/\lambda]$. Two ideals I, J of $\mathbb{Z}[1/\lambda]$ are *equivalent* if there is some $\alpha \in \mathbb{Q}(\lambda)$ such that $J = \alpha I$. Since the eigenspace of A corresponding to its Perron eigenvalue λ is one-dimensional, any other eigenvector $v' = (v'_1, \ldots, v'_n) \in \mathbb{Z}[\lambda]^n$ is a multiple of v by an element of $\mathbb{Q}(\lambda)$ and therefore the ideal generated by $v'_1, \ldots, v'_n$ is equivalent to that generated by $v_1, \ldots, v_n$. We may then define the *ideal class of* A to be the equivalence class of these ideals in $\mathbb{Z}[1/\lambda]$. This can be shown to be invariant under SE, and may be used to distinguish some SFTs which cannot be distinguished using the Bowen-Franks groups and Jordan form away from zero. [11] This invariant is not readily computable, however. More recently, Søren Eilers and Ian Kiming [4] have developed two more easily computed invariants of strong shift equivalence. One of these, taking values in the Picard group of $\mathbb{Z}[\lambda]$, is only defined given certain algebraic restrictions on the matrix, and was shown to be equivalent to the above ideal class invariant when both are defined. The second invariant, which takes a value in the ideal class group of $\mathbb{Q}(\lambda)$, is defined unconditionally and is possibly weaker than the ideal class invariant, but is readily computable. Using the first of these two invariants, together with the Jordan form away from zero and several types of Bowen-Franks groups, Eilers and Kiming used data compiled by O. Jensen to determine which of the irreducible two-by-two matrices over $\mathbb{Z}^+$ with entry sum less than 25 are SSE. Of the 148,772,625 comparisons that can be made within this universe, they were able to determine in all but 927 cases whether the two matrices in question are SSE.[4]

Open problems

A number of questions about shift equivalence and strong shift equivalence remain unanswered. We summarize a few of these here, and refer to [1] for a more comprehensive list.

- Does there exist an algorithm which determines whether two given edge shifts are topologically conjugate? Equivalently, does there exist an algorithm which determines whether two square nonnegative integer matrices are SSE over $\mathbb{Z}^+$?
- It is known that, if Λ is a Dedekind domain, SE over Λ coincides with SSE over Λ. What are the other rings Λ for which this holds?
- If A, B are two-by-two matrices over $\mathbb{Z}^+$ with $\det A = \det B < -1$, must A and B be SSE over $\mathbb{Z}^+$?
- If A, B are square positive matrices which are SE over $\mathbb{Q}^+$, are they SSE over $\mathbb{Q}^+$? Kim and Roush [6] have shown this to be true if A and B have a single nonzero eigenvalue which is an integer. This problem is also open if the word "positive" is removed.

References

[1] M. Boyle, *Open problems in symbolic dynamics*, Geometric and Probabilistic Structures in Dynamics, Contemporary Mathematics, vol. 469 (2008), 69–118

[2] M. Boyle and D. Handelman, *Algebraic shift equivalence and primitive matrices*, Trans. Amer. Math. Soc. **336** (1993)

[3] M. Boyle, B. Marcus, and P. Trow, *Resolving maps and the dimension group for shifts of finite type*, Mem. Amer. Math. Soc. **70** (1987)

[4] S. Eilers and I. Kiming, *On some new invariants for strong shift equivalence for shifts of finite type*, preprint (2008)

[5] K.H. Kim and F.W. Roush, *Decidability of shift equivalence*, Lecture Notes in Math., **1342**, Springer, Berlin (1988)

[6] K.H. Kim and F.W. Roush, *Full shifts over R+ and invariant tetrahedra*, Pure Math. Appl. Ser. B **1** (1990), no. 4, 251256 (1991)

[7] K.H. Kim and F.W. Roush, *The Williams Conjecture is false for irreducible subshifts*, Electron. Res. Announc. Amer. Math. Soc. **3** (1997), 105–109

[8] K.H. Kim and F.W. Roush, *Williams's conjecture is false for reducible subshifts*, J. Amer. Math. Soc. **5** (1992), vol. 1, 213–215

[9] K.H. Kim, F.W. Roush, and J.B. Wagoner, *Automorphisms of the dimension group and gyration numbers*, J. Amer. Math. Soc. **5** (1992), no. 1, 191–212

[10] B. Kitchens, *Symbolic Dynamics*, Springer Universitext (1998)

[11] D. Lind and B. Marcus, *Symbolic Dynamics and Coding*, Cambridge University Press (1995)

[12] W. Parry and R.F. Williams, *Block coding and a zeta function for finite Markov chains*, Proc. London Math. Soc. **35** (1977), 483–495

[13] J.B. Wagoner, *Triangle identities and symmetries of a subshift of finite type*, Pacific J. Math. **144** (1990), no. 1, 181–205

[14] R.F. Williams, *Classification of subshifts of finite type*, Ann. of Math. **98** (1973), 120-153; Errata, ibid. **99** (1974), 380–381