

Decomposition theorems for semirings and the Krohn-Rhodes complexity of power semigroups

John Rhodes¹ Benjamin Steinberg²

¹University of California, Berkeley and ²Carleton University

bsteinbg@math.carleton.ca

<http://www.math.carleton.ca/~bsteinbg>

Leipzig, February 3, 2009

Semirings

- In Computer Science semirings are often more important than rings.
- This is because the Boolean semiring $\mathbb{B} = \{0, 1\}$ with bit addition and multiplication is more natural from a logical standpoint.
- Also the semiring of Boolean matrices $M_n(\mathbb{B})$ can be identified with the semiring of binary relations on an n -element set.
- For instance transition monoids of non-deterministic automata are often represented by Boolean matrices.
- Another important semiring, for both computer science and mathematics, is the tropical semiring $(\mathbb{R}, \min, +)$, which underlies tropical geometry.
- This work is from Chapter 9 of our book “The q-theory of finite semigroups”.

Semirings Continued

- A semiring is a 4-tuple $(S, +, \cdot, 0)$ such that
 - $(S, +, 0)$ is a commutative monoid.
 - (S, \cdot) is a semigroup.
 - Both distributive laws hold.
 - For all $x \in S$, $x0 = 0 = 0x$.
- Idempotent semirings (ISRs) are semirings so that $x + x = x$;
- ISRs are sup-semilattices with minimum via $x \leq y$ if $x + y = y$.
- Key examples:
 - If k is a commutative semiring with unit and S is a semigroup, the semigroup algebra is:

$$kS = \left\{ \sum_{s \in S} c_s s \mid c_s \in k \text{ and finitely many } c_s \neq 0 \right\}.$$

- The finitary power set $(P(S), \cup, \cdot)$ of a semigroup S ($= \mathbb{B}S$).
- $M_n(R)$ where R is a semiring.
- $T_n(\mathbb{B})$ upper triangular Boolean matrices. Key to dot-depth problem.

Semirings Continued

- A semiring is a 4-tuple $(S, +, \cdot, 0)$ such that
 - $(S, +, 0)$ is a commutative monoid.
 - (S, \cdot) is a semigroup.
 - Both distributive laws hold.
 - For all $x \in S$, $x0 = 0 = 0x$.
- Idempotent semirings (ISRs) are semirings so that $x + x = x$;
- ISRs are sup-semilattices with minimum via $x \leq y$ if $x + y = y$.
- Key examples:
 - If k is a commutative semiring with unit and S is a semigroup, the semigroup algebra is:

$$kS = \left\{ \sum_{s \in S} c_s s \mid c_s \in k \text{ and finitely many } c_s \neq 0 \right\}.$$

- The finitary power set $(P(S), \cup, \cdot)$ of a semigroup S ($= \mathbb{B}S$).
- $M_n(R)$ where R is a semiring.
- $T_n(\mathbb{B})$ upper triangular Boolean matrices. Key to dot-depth problem.

Semirings Continued

- A semiring is a 4-tuple $(S, +, \cdot, 0)$ such that
 - $(S, +, 0)$ is a commutative monoid.
 - (S, \cdot) is a semigroup.
 - Both distributive laws hold.
 - For all $x \in S$, $x0 = 0 = 0x$.
- Idempotent semirings (ISRs) are semirings so that $x + x = x$;
- ISRs are sup-semilattices with minimum via $x \leq y$ if $x + y = y$.
- Key examples:
 - If k is a commutative semiring with unit and S is a semigroup, the semigroup algebra is:

$$kS = \left\{ \sum_{s \in S} c_s s \mid c_s \in k \text{ and finitely many } c_s \neq 0 \right\}.$$

- The finitary power set $(P(S), \cup, \cdot)$ of a semigroup S ($= \mathbb{B}S$).
- $M_n(R)$ where R is a semiring.
- $T_n(\mathbb{B})$ upper triangular Boolean matrices. Key to dot-depth problem.

Semirings Continued

- A semiring is a 4-tuple $(S, +, \cdot, 0)$ such that
 - $(S, +, 0)$ is a commutative monoid.
 - (S, \cdot) is a semigroup.
 - Both distributive laws hold.
 - For all $x \in S$, $x0 = 0 = 0x$.
- Idempotent semirings (ISRs) are semirings so that $x + x = x$;
- ISRs are sup-semilattices with minimum via $x \leq y$ if $x + y = y$.
- Key examples:
 - If k is a commutative semiring with unit and S is a semigroup, the semigroup algebra is:

$$kS = \left\{ \sum_{s \in S} c_s s \mid c_s \in k \text{ and finitely many } c_s \neq 0 \right\}.$$

- The finitary power set $(P(S), \cup, \cdot)$ of a semigroup S ($= \mathbb{B}S$).
- $M_n(R)$ where R is a semiring.
- $T_n(\mathbb{B})$ upper triangular Boolean matrices. Key to dot-depth problem.

Semirings Continued

- A semiring is a 4-tuple $(S, +, \cdot, 0)$ such that
 - $(S, +, 0)$ is a commutative monoid.
 - (S, \cdot) is a semigroup.
 - Both distributive laws hold.
 - For all $x \in S$, $x0 = 0 = 0x$.
- Idempotent semirings (ISRs) are semirings so that $x + x = x$;
- ISRs are sup-semilattices with minimum via $x \leq y$ if $x + y = y$.
- Key examples:
 - If k is a commutative semiring with unit and S is a semigroup, the semigroup algebra is:

$$kS = \left\{ \sum_{s \in S} c_s s \mid c_s \in k \text{ and finitely many } c_s \neq 0 \right\}.$$

- The finitary power set $(P(S), \cup, \cdot)$ of a semigroup S ($= \mathbb{B}S$).
- $M_n(R)$ where R is a semiring.
- $T_n(\mathbb{B})$ upper triangular Boolean matrices. Key to dot-depth problem.

A Global Structure Theory

- The global structure theory of finite semigroups is based on the Prime Decomposition Theorem:

Theorem (Krohn-Rhodes)

Every finite semigroup divides an iterated wreath product of finite simple groups and copies of the 3-element monoid U_2 consisting of an identity and 2 constant maps.

- A semigroup S divides a semigroup T if it is a quotient of a subsemigroup of T .
- Moreover, the finite simple groups and subsemigroups of U_2 are precisely the primes with respect to the wreath product.
- A semigroup is aperiodic if all its group subsemigroups are trivial.
- So every finite semigroup divides an iterated wreath product whose factors alternate between groups and aperiodic semigroups.

A Global Structure Theory

- The global structure theory of finite semigroups is based on the Prime Decomposition Theorem:

Theorem (Krohn-Rhodes)

Every finite semigroup divides an iterated wreath product of finite simple groups and copies of the 3-element monoid U_2 consisting of an identity and 2 constant maps.

- A semigroup S divides a semigroup T if it is a quotient of a subsemigroup of T .
- Moreover, the finite simple groups and subsemigroups of U_2 are precisely the primes with respect to the wreath product.
- A semigroup is aperiodic if all its group subsemigroups are trivial.
- So every finite semigroup divides an iterated wreath product whose factors alternate between groups and aperiodic semigroups.

A Global Structure Theory

- The global structure theory of finite semigroups is based on the Prime Decomposition Theorem:

Theorem (Krohn-Rhodes)

Every finite semigroup divides an iterated wreath product of finite simple groups and copies of the 3-element monoid U_2 consisting of an identity and 2 constant maps.

- A semigroup S divides a semigroup T if it is a quotient of a subsemigroup of T .
- Moreover, the finite simple groups and subsemigroups of U_2 are precisely the primes with respect to the wreath product.
- A semigroup is aperiodic if all its group subsemigroups are trivial.
- So every finite semigroup divides an iterated wreath product whose factors alternate between groups and aperiodic semigroups.

A Global Structure Theory

- The global structure theory of finite semigroups is based on the Prime Decomposition Theorem:

Theorem (Krohn-Rhodes)

Every finite semigroup divides an iterated wreath product of finite simple groups and copies of the 3-element monoid U_2 consisting of an identity and 2 constant maps.

- A semigroup S divides a semigroup T if it is a quotient of a subsemigroup of T .
- Moreover, the finite simple groups and subsemigroups of U_2 are precisely the primes with respect to the wreath product.
- A semigroup is aperiodic if all its group subsemigroups are trivial.
- So every finite semigroup divides an iterated wreath product whose factors alternate between groups and aperiodic semigroups.

Complexity

- The (Krohn-Rhodes) complexity $c(S)$ of a finite semigroup S is the least number n so that S divides an iterated wreath product

$$A_n \wr G_n \wr A_{n-1} \wr \cdots \wr A_1 \wr G_1 \wr A_0$$

where the A_i are aperiodic and the G_i are groups.

- The computability of complexity is one of the major open problems in finite semigroups.
- Our approach to semirings is to replace the wreath product by Plotkin's triangular product and simple groups by matrix algebras over group algebras.
- This will lead to a complexity theory for semirings.
- Applications to computing the group complexity of power sets of finite semigroups will be given.

Complexity

- The (Krohn-Rhodes) complexity $c(S)$ of a finite semigroup S is the least number n so that S divides an iterated wreath product

$$A_n \wr G_n \wr A_{n-1} \wr \cdots \wr A_1 \wr G_1 \wr A_0$$

where the A_i are aperiodic and the G_i are groups.

- The computability of complexity is one of the major open problems in finite semigroups.
- Our approach to semirings is to replace the wreath product by Plotkin's triangular product and simple groups by matrix algebras over group algebras.
- This will lead to a complexity theory for semirings.
- Applications to computing the group complexity of power sets of finite semigroups will be given.

Complexity

- The (Krohn-Rhodes) complexity $c(S)$ of a finite semigroup S is the least number n so that S divides an iterated wreath product

$$A_n \wr G_n \wr A_{n-1} \wr \cdots \wr A_1 \wr G_1 \wr A_0$$

where the A_i are aperiodic and the G_i are groups.

- The computability of complexity is one of the major open problems in finite semigroups.
- Our approach to semirings is to replace the wreath product by Plotkin's triangular product and simple groups by matrix algebras over group algebras.
- This will lead to a complexity theory for semirings.
- Applications to computing the group complexity of power sets of finite semigroups will be given.

Modules

- We need to setup the representation-theoretic apparatus in the semiring context.
- A module M over a semiring R is a commutative monoid equipped with a right action of R by endomorphisms.
- Any sup-semilattice with \min is a \mathbb{B} -module.
- $M_n(k)$ acts on k^n viewed as row vectors.
- If X is a set, the free k -module on X is the set kX of finite formal k -linear combinations of elements of X .
- If N is a submodule of M , one can form the quotient module M/N where $m + N = m' + N$ by definition if $m + n = m' + n'$ some $n, n' \in N$.
- $0 \rightarrow N \rightarrow M \rightarrow M/N \rightarrow 0$ is considered an exact sequence, as is any sequence 'equivalent' to one of this form.

Modules

- We need to setup the representation-theoretic apparatus in the semiring context.
- A module M over a semiring R is a commutative monoid equipped with a right action of R by endomorphisms.
- Any sup-semilattice with \min is a \mathbb{B} -module.
- $M_n(k)$ acts on k^n viewed as row vectors.
- If X is a set, the free k -module on X is the set kX of finite formal k -linear combinations of elements of X .
- If N is a submodule of M , one can form the quotient module M/N where $m + N = m' + N$ by definition if $m + n = m' + n'$ some $n, n' \in N$.
- $0 \rightarrow N \rightarrow M \rightarrow M/N \rightarrow 0$ is considered an exact sequence, as is any sequence 'equivalent' to one of this form.

Modules

- We need to setup the representation-theoretic apparatus in the semiring context.
- A module M over a semiring R is a commutative monoid equipped with a right action of R by endomorphisms.
- Any sup-semilattice with \min is a \mathbb{B} -module.
- $M_n(k)$ acts on k^n viewed as row vectors.
- If X is a set, the free k -module on X is the set kX of finite formal k -linear combinations of elements of X .
- If N is a submodule of M , one can form the quotient module M/N where $m + N = m' + N$ by definition if $m + n = m' + n'$ some $n, n' \in N$.
- $0 \rightarrow N \rightarrow M \rightarrow M/N \rightarrow 0$ is considered an exact sequence, as is any sequence 'equivalent' to one of this form.

Modules

- We need to setup the representation-theoretic apparatus in the semiring context.
- A module M over a semiring R is a commutative monoid equipped with a right action of R by endomorphisms.
- Any sup-semilattice with \min is a \mathbb{B} -module.
- $M_n(k)$ acts on k^n viewed as row vectors.
- If X is a set, the free k -module on X is the set kX of finite formal k -linear combinations of elements of X .
- If N is a submodule of M , one can form the quotient module M/N where $m + N = m' + N$ by definition if $m + n = m' + n'$ some $n, n' \in N$.
- $0 \rightarrow N \rightarrow M \rightarrow M/N \rightarrow 0$ is considered an exact sequence, as is any sequence 'equivalent' to one of this form.

Modules

- We need to setup the representation-theoretic apparatus in the semiring context.
- A module M over a semiring R is a commutative monoid equipped with a right action of R by endomorphisms.
- Any sup-semilattice with \min is a \mathbb{B} -module.
- $M_n(k)$ acts on k^n viewed as row vectors.
- If X is a set, the free k -module on X is the set kX of finite formal k -linear combinations of elements of X .
- If N is a submodule of M , one can form the quotient module M/N where $m + N = m' + N$ by definition if $m + n = m' + n'$ some $n, n' \in N$.
- $0 \rightarrow N \rightarrow M \rightarrow M/N \rightarrow 0$ is considered an exact sequence, as is any sequence 'equivalent' to one of this form.

Modules

- We need to setup the representation-theoretic apparatus in the semiring context.
- A module M over a semiring R is a commutative monoid equipped with a right action of R by endomorphisms.
- Any sup-semilattice with \min is a \mathbb{B} -module.
- $M_n(k)$ acts on k^n viewed as row vectors.
- If X is a set, the free k -module on X is the set kX of finite formal k -linear combinations of elements of X .
- If N is a submodule of M , one can form the quotient module M/N where $m + N = m' + N$ by definition if $m + n = m' + n'$ some $n, n' \in N$.
- $0 \rightarrow N \rightarrow M \rightarrow M/N \rightarrow 0$ is considered an exact sequence, as is any sequence 'equivalent' to one of this form.

Modules

- We need to setup the representation-theoretic apparatus in the semiring context.
- A module M over a semiring R is a commutative monoid equipped with a right action of R by endomorphisms.
- Any sup-semilattice with \min is a \mathbb{B} -module.
- $M_n(k)$ acts on k^n viewed as row vectors.
- If X is a set, the free k -module on X is the set kX of finite formal k -linear combinations of elements of X .
- If N is a submodule of M , one can form the quotient module M/N where $m + N = m' + N$ by definition if $m + n = m' + n'$ some $n, n' \in N$.
- $0 \rightarrow N \rightarrow M \rightarrow M/N \rightarrow 0$ is considered an exact sequence, as is any sequence 'equivalent' to one of this form.

The Triangular Product

- If $\rho : A \rightarrow \text{End}(V)$ is a representation of an algebra over a field and W is an A -submodule, then by extending a basis of W to V , we can place the representation in the block lower triangular form:

$$s \mapsto \begin{pmatrix} \rho_W & 0 \\ \rho' & \rho_{V/W} \end{pmatrix}$$

where ρ_W is the restriction of ρ to W , $\rho_{V/W}$ is the quotient representation and ρ' is essentially a linear map from V/W to W .

- Plotkin's triangular product axiomatizes this decomposition.
- We exploit it to apply the Jordan-Hölder program to finite idempotent semirings.

The Triangular Product Continued

- If M_R, N_S are modules, then $\text{Hom}(N, M)$ is naturally an S - R -bimodule and so we can form the idempotent semiring

$$\triangle(M_R, N_S) = \begin{pmatrix} R & 0 \\ \text{Hom}(N, M) & S \end{pmatrix}$$

called the triangular product.

- The triangular product acts naturally on $M \oplus N$ (viewed as row vectors).
- The triangular product is associative on the level of modules.
- It is analogous to the wreath product of transformation semigroups X_R, Y_S .
- If we write R additively, there is the matrix form

$$X_R \wr Y_S = \begin{pmatrix} 1 & 0 \\ R^Y & S \end{pmatrix}.$$

\mathbb{B} -split Sequences

- Our main source of triangular product decompositions come from exact sequences that split over \mathbb{B} .
- Let S be an ISR, M an S -module and L and S -submodule.
- We say that $0 \rightarrow L \rightarrow M \rightarrow M/L \rightarrow 0$ is \mathbb{B} -split if it is equivalent as an exact sequence of \mathbb{B} -modules $0 \rightarrow L \rightarrow L \oplus N \rightarrow N \rightarrow 0$.
- N is only a complement of L as a \mathbb{B} -module. It need not be an S -module.
- If M is $P(X)$ for a finite set X and $L = P(Y)$ for $Y \subseteq X$, then $N = P(X \setminus Y)$ is a complement for L .
- The existence of such a splitting can be described in terms of a sup-semilattice retraction $\rho : M \rightarrow L$ and section $\sigma : N \rightarrow M$ satisfying some obvious axioms.

Triangular Decomposition Theorem

Theorem (Rhodes-BS)

Let

$$0 \rightarrow L \rightarrow M \rightarrow M/L \rightarrow 0$$

be \mathbb{B} -split with L, M S -modules. Let R, T be the faithful quotients of S acting on L and M/L , respectively. If M is a faithful module, then

$$S \leq \Delta(L_R, (M/L)_T).$$

- The decomposition really holds on the module level.
- This is the precise analogue of the representation theoretic situation discussed earlier.
- Iteration can lead to a Jordan-Hölder block lower triangular decomposition.
- An important special case arises from ideals in a semigroup.

Ideal Decomposition Theorem

- All semigroups, semirings and modules are finite from now on.
- If S is a semigroup with 0, the contracted semigroup algebra $P_0(S)$ is the set of subsets of S containing 0.
- If I is an ideal of S , $P_0(S/I) \cong P(S)/P(I)$.

Theorem (Rhodes-BS)

Let S be a monoid and I an ideal. Let R be the faithful quotient of $P(S)$ acting on $P(I)$. Then

$$P(S) \leq \Delta(P(I)_R, P_0(S/I)_{P_0(S/I)}).$$

Proof.

There is a \mathbb{B} -split short exact sequence

$0 \rightarrow P(I) \rightarrow P(S) \rightarrow P_0(S/I) \rightarrow 0$ and $P(S)$ is a faithful S -module, so the Triangular Decomposition Theorem applies. □

A Little Semigroup Theory

- Two elements of a semigroup S are \mathcal{J} -equivalent if they generate the same two-sided ideal.
- Two elements of a semigroup S are \mathcal{L} - (\mathcal{R})-equivalent if they generate the same left (right) ideal.
- An equivalence class for \mathcal{J} is called a \mathcal{J} -class. Similar terminology is used for the other relations.
- To each \mathcal{J} -class J , there is associated a group G_J called its Schützenberger group.
- If $e \in J$ is an idempotent, then $G_J \cong H_e$ where H_e is the unit group of the monoid eSe .
- A principal series for a semigroup S is a chain of principal ideals $= I_0 \supsetneq I_1 \supsetneq \cdots \supsetneq I_n$ that cannot be refined.
- The quotients I_m/I_{m+1} are precisely the semigroups J^0 with J a \mathcal{J} -class of S .

The Setup

- An ISR R divides an ISR S if R is a quotient of a subsemiring of S .
- If S is an ISR, then there is a natural ISR quotient $P(S) \twoheadrightarrow S$ sending X to $\sum_{s \in X} s$.
- Here we view $P(S)$ as the algebra of the underlying multiplicative semigroup of S .
- Thus S divides $P(S)$.
- In particular, to decompose S into a triangular product via division, it suffices to embed $P(S)$ in a triangular product.
- This is achieved by iterating the ideal decomposition theorem.

The Prime Decomposition Theorem

Theorem (Rhodes-BS)

Let S be an idempotent semiring and $S^1 = I_0 \supsetneq I_1 \supsetneq \cdots \supsetneq I_n$ a principal series. Let J_m be the \mathcal{J} -class corresponding to I_m/I_{m+1} and a_m, b_m the number of \mathcal{R} -, \mathcal{L} -classes in J_m , respectively. Let G_m be the Schützenberger group of J_m . Then S divides

$$\Delta \left([P(G_n)^{b_n}]_{M_{b_n}(P(G_n))}^{a_n}, \dots, [P(G_0)^{b_0}]_{M_{b_0}(P(G_0))}^{a_0} \right).$$

- Ideas:
 - Iteration of the ideal decomposition theorem puts $P(S)$ into a triangular product of its action on the $P(J_m)$.
 - The action of $P(S)$ on the right of $P(J_m)$ is the linear extension of the Schützenberger representation via row monomial matrices over G_m .
- This is the semiring analogue of the correspondence between irreducible representations of a semigroup and its maximal subgroups.

Is this a Prime Decomposition?

- In order to call this result a Prime Decomposition Theorem, we must explain in what sense we are decomposing ISRs into primes.
- A semigroup is prime if whenever it divides a wreath product, it divides one of the factors.
- The prime semigroups are the simple groups and subsemigroups of U_2 , so the Prime Decomposition Theorem for semigroups does break things up into primes.
- Call an ISR Δ -irreducible if whenever it divides a triangular product $\Delta(M_R, N_T)$, it must divide R or T .
- In light of the previous results, we would like to show that $M_n(P(G))$ is Δ -irreducible for any group G .

A Semiring Associated to a Group

- Let G be a group.
- Let $G^{\natural} = G \cup \{0\} \cup \infty$.
- As a sup-semilattice, G is an anti-chain, 0 is the minimum and ∞ is the maximum.
- The group operation is extended to G^{\natural} by making 0 a multiplicative zero and setting $x \cdot \infty = \infty = \infty \cdot x$ whenever $x \neq 0$.
- G^{\natural} is an idempotent semiring.
- It is the quotient by the largest congruence on $P(G)$ that is injective on G for $G \neq 1$.
- A non-trivial group is called monolithic if it has a unique minimal normal subgroup.

\triangle -Irreducible Semirings

Theorem (Rhodes-BS)

Let G be a group. Then $M_n(P(G))$ is \triangle -irreducible for $n \geq 1$. Let G be a monolithic group. Then $M_n(G^\natural)$ is \triangle -irreducible for $n \geq 1$.

- So the Prime Decomposition Theorem provides a decomposition into irreducibles.
- Notice that $P(1) = \mathbb{B}$ so $M_n(\mathbb{B})$ is \triangle -irreducible.
- In particular, each idempotent semiring embeds in a \triangle -irreducible semigroup.
- So we will have to be a bit more careful when defining complexity for idempotent semirings.
- Big open question: what are the \triangle -irreducible idempotent semirings?
- Are there any aperiodic \triangle -irreducible semirings besides \mathbb{B} ?

Some Ingredients of the Proof

- If $\varphi : R \twoheadrightarrow S$ is a surjective semiring homomorphism and G is a subgroup of S , then standard semigroup theory says that there is a subgroup H of R with $\varphi(H) = G$.
- If $N = \ker \varphi|_H$, then the elements $\sum_{n \in N} hn$, $h \in H$, yield a subgroup of R mapping isomorphically under φ to G .
- So groups lift exactly!
- If $\varphi : R \twoheadrightarrow M_n(P(G))$ is a surjective semiring homomorphism, then one can lift the non-zero part of the semigroup of scalar multiples of matrix units. But not any old lift will do for the proof. One must choose very carefully!
- A key role is played by quotients of idempotent semirings modulo ideals.
- We use often that if R is unital, then congruences on $M_n(R)$ are in bijection with congruences on R .

Complexity of Idempotent Semirings

- Define the complexity of an ISR S to be the minimum of the quantity $c(R_1) + \cdots + c(R_n)$ over all divisions of S into triangular products $\Delta(M_{R_1}^{(1)}, \dots, M_{R_n}^{(n)})$. where the R_i are Δ -irreducible.
- Here c is the usual complexity of a semigroup.
- Alternatively one can replace c with two-sided complexity.
- The entire subject of complexity of idempotent semirings is wide open.

Applications to Group Complexity

- The projection $\begin{pmatrix} R & 0 \\ \text{Hom}(N, M) & S \end{pmatrix} \twoheadrightarrow R \times S$ of a triangular product to its diagonal is an aperiodic morphism (injective on subgroups).
- The Fundamental Lemma of Complexity says if $\varphi : S \twoheadrightarrow T$ is an aperiodic morphism, then $c(S) = c(T)$.
- So $c(\triangle(M_R, N_S)) = \max\{c(R), c(S)\}$.
- To apply the Prime Decomposition to the complexity of a power semigroup, we need to compute the complexity of a matrix algebra over a group algebra.

Theorem (Fox-Rhodes)

Let G be a group. Then $c(M_n(P(G))) = n - 1 + c(G)$.

Applications to Group Complexity II

- Applying the Prime Decomposition Theorem for idempotent semirings and the above result, we obtain some bounds on the complexity of a power semigroup.
- Here are some examples:
 - The complexity of $P(S)$ is bounded by both the maximum number of \mathcal{L} -classes and the maximum number of \mathcal{R} -classes in a non-zero \mathcal{J} -class of S .
 - For an inverse semigroup S , we have:

Theorem

The complexity of $P(S)$ is the maximum over all \mathcal{J} -classes J of the quantity $e_J - 1 + c(G_J)$ where $e_J = |E(J)|$ and G_J is the maximal subgroup of J . In particular, complexity is computable for power sets of inverse semigroups.

- For the symmetric inverse monoid I_n , $c(P(I_n)) = \binom{n}{\lfloor \frac{n}{2} \rfloor}$ (for $n \geq 3$).

Applications to Group Complexity III

- An interesting case is $P(T_n)$ where T_n is the full transformation semigroup of degree n .
- In Fox's Master's thesis a wreath product version of the Prime Decomposition Theorem for idempotent semirings is used to prove:

Theorem (Fox-Rhodes)

$$\binom{n-1}{\lfloor \frac{n-1}{2} \rfloor} \leq c(P(T_n)) \leq 2^n - n - 1$$

- The ratio of the upper bound to the lower bound goes to infinity.
- We can now improve the upper bound:

Theorem (Rhodes-BS)

$$\binom{n-1}{\lfloor \frac{n-1}{2} \rfloor} \leq c(P(T_n)) \leq \binom{n}{\lfloor \frac{n}{2} \rfloor}.$$