Generators of Wreaths

Petar Maymounkov and Benjamin Rossman

May 27, 2006

Notation 0.1. $G \leq S_n$ will be a finite permutation group. $k(G)$ denotes the minimal number of generators of G. $H \wr G \cong H^n \rtimes G$ denotes the wreath product of a group H by G. Elements of $H \wr G$ are written as $(n+1)$-tuples of the form $(h_1, \ldots, h_n; g)$ where $h_i \in H$ and $g \in G$. Multiplication in $H \wr G$ is defined by

$$(h_1, \ldots, h_n; g)(h'_1, \ldots, h'_n; g') = (h_1 h'_{g(1)}, \ldots, h_n h'_{g(n)}; gg').$$

Wreath powers of G are defined as follows. Let $\mathrm{Wr}^1(G) = G$ and for $\ell \geq 2$ let $\mathrm{Wr}^\ell(G) = \mathrm{Wr}^{\ell-1}(G) \wr G$.

Lemma 0.2. *If $H \lhd G$ such that G/H is abelian, then there exists a surjective homomorphism $\varphi_\ell : \mathrm{Wr}^\ell(G) \to (G/H)^\ell$.*

Proof. We define φ_ℓ inductively. φ_1 is just the usual quotient map $G \to G/H$. For $\ell \geq 2$ and $(\gamma_1, \ldots, \gamma_n; g) \in \mathrm{Wr}^\ell(G)$ — i.e., $\gamma_1, \ldots, \gamma_n \in \mathrm{Wr}^{\ell-1}(G)$ and $g \in G$ — we define

$$\varphi_\ell(\gamma_1, \ldots, \gamma_n; g) = (\underbrace{\varphi_{\ell-1}(\gamma_1) + \cdots + \varphi_{\ell-1}(\gamma_n)}_{\in (G/H)^{\ell-1}}, \underbrace{\varphi_1(g)}_{\in G/H}) \in (G/H)^\ell.$$

It is easy to check that φ_ℓ is a surjective homomorphism. □

Lemma 0.3. *If G is abelian, then $k(G^\ell) = \ell \cdot k(G)$.*

Proof. □

Corollary 0.4. *If $H \lhd G$ such that G/H is abelian, then $k(\mathrm{Wr}^\ell(G)) \leq \ell \cdot k(G/H)$.*

Proof. Use the previous two lemmas. □

Corollary 0.5. *$k(\mathrm{Wr}^\ell(S_n)) \geq \ell$ for all $n \geq 2$.*

Proof. By the previous corollary, $k(\mathrm{Wr}^\ell(S_n)) \geq \ell \cdot k(S_n/A_n) = \ell \cdot k(C_2) = \ell$. □

There is an obvious way in which $\mathrm{Wr}^\ell(G)$ acts on the vertex set of the complete n-ary tree T of height $\ell+1$. For instance, if $G = S_n$ then $\mathrm{Wr}^\ell(G)$ acts as the full automorphism group of T. This action of $\mathrm{Wr}^\ell(G)$ on T restricts to an action on the leaves of T, which we label using the set $[n^{\ell+1}] = \{1, 2, \ldots, n^{\ell+1}\}$.

Lemma 0.6. *If G is transitive (i.e., acts transitively on $[n]$), then $\mathrm{Wr}^\ell(G)$ acts transitively on $[n^\ell]$.*

Proof. Proof by induction on tree height. $\square$

We now establish a matching upper bound to show that $k(\mathrm{Wr}^\ell(S_n)) = \ell$. We begin by noticing that for $\ell \geq 2$, not only can we express $\mathrm{Wr}^\ell(G)$ as a semidirect product $\mathrm{Wr}^{\ell-1}(G) \rtimes G$, but also

$$\mathrm{Wr}^\ell(G) \cong G^{n^\ell} \rtimes \mathrm{Wr}^{\ell-1}(G).$$

View G^{n^ℓ} and $\mathrm{Wr}^{\ell-1}(G)$ as subgroups of $\mathrm{Wr}^\ell(G)$ in the obvious way: $\mathrm{Wr}^{\ell-1}(G)$ permutes the top ℓ levels of the tree, and G^{n^ℓ} is the automorphism group of the remaining level.

We introduce an alternative notation for elements of $\mathrm{Wr}^\ell(G)$, as $(n^\ell + 1)$-tuples $\langle g_1, \dots, g_{n^\ell}; \gamma\rangle$ where $g_1, \dots, g_{n^\ell} \in G$ and $\gamma \in \mathrm{Wr}^{\ell-1}(G)$. In this notation, multiplication is defined by

$$\langle g_1, \dots, g_{n^\ell}; \gamma\rangle\langle g'_1, \dots, g'_{n^\ell}; \gamma'\rangle = \langle g_1 g'_{\gamma(1)}, \dots, g_{n^\ell} g'_{\gamma(n^\ell)}; \gamma\gamma'\rangle$$

where $\gamma(i)$ denotes the image of $i \in [n^\ell]$ under the action of $\gamma \in \mathrm{Wr}^{\ell-1}(G)$ just described.

Proposition 0.7. *If G is transitive, then $k(\mathrm{Wr}^\ell(G)) \leq \ell \cdot k(G)$.*

Proof. Suppose $\{g_j\}_{j\in[t]}$ generates G. We define generating set $\{\gamma^\ell_{i,j}\}_{i\in[\ell],j\in[t]}$ for $\mathrm{Wr}^\ell(G)$ inductively.

- $\gamma^1_{1,j} := g_j$ for all $j \in [t]$.
- $\gamma^\ell_{i,j} := \langle \underbrace{1_G, \dots, 1_G}_{n^\ell \text{ times}}; \gamma^{\ell-1}_{i,j}\rangle$ for all $\ell \geq 2$ and $i \in [\ell - 1]$ and $j \in [t]$.
- $\gamma^\ell_{\ell,j} := \langle g_j, \underbrace{1_G, \dots, 1_G}_{n^\ell - 1 \text{ times}}; 1_{\mathrm{Wr}^{\ell-1}(G)}\rangle$ for all $j \in [t]$.

Let H be the subgroup of $\mathrm{Wr}^\ell(G)$ generated by $\{\gamma^\ell_{i,j}\}_{i\in[\ell],j\in[t]}$ for some $\ell \geq 2$. We prove that $H = \mathrm{Wr}^\ell(G)$ in the following steps.

1. $\langle 1_G, \dots, 1_G; \delta\rangle \in H$ for all $\delta \in \mathrm{Wr}^{\ell-1}(G)$.

   This follows from the induction hypothesis that $\{\gamma^{\ell-1}_{i,j}\}_{i\in[\ell-1],j\in[t]}$ generates $\mathrm{Wr}^{\ell-1}(G)$ (trivial in the base case when $\ell = 2$).

2. $\langle \underbrace{1_G, \dots, 1_G, g_j, 1_G, \dots, 1_G}_{\text{in the } q\text{th location}}; 1_{\mathrm{Wr}^{\ell-1}(G)}\rangle \in H$ for all $q \in [n^\ell]$.

   By assumption, G is transitive. So by previous lemma, $\mathrm{Wr}^{\ell-1}(G)$ acts transitively on $[n^\ell]$. Find $\delta \in \mathrm{Wr}^{\ell-1}(G)$ taking 1 to q. We see that

$$\langle 1_G, \dots, 1_G, g_j, 1_G, \dots, 1_G; 1_{\mathrm{Wr}^{\ell-1}(G)}\rangle = \langle 1_G, \dots, 1_G; \delta\rangle \gamma^\ell_{\ell,j} \langle 1_G, \dots, 1_G; \delta\rangle^{-1} \in H.$$

3. We now easily have:

   $\langle \underbrace{1_G, \ldots, 1_G, g', 1_G, \ldots, 1_G}_{\text{in the } q\text{th location}}; 1_{\mathrm{Wr}^{\ell-1}(G)} \rangle \in H$ for all $g' \in G$ and $q \in [n^\ell]$.

4. $\langle g'_1, \ldots, g'_{n^\ell}; 1_{\mathrm{Wr}^{\ell-1}(G)} \rangle \in H$ for all $g'_1, \ldots, g'_{n^\ell} \in G$.

5. $H = \mathrm{Wr}^\ell(G)$.

□

We now return to wreath powers $\mathrm{Wr}^\ell(S_n)$ of the symmetric group S_n.

Lemma 0.8. *For $n \geq 4$, there exists $\alpha, \beta \in S_n$ such that $\alpha(1) = 1$ and $\beta(2) = 2$ and both $\{\alpha, \beta\}$ and $\{\alpha^{\mathrm{ord}(\beta)}, \beta^{\mathrm{ord}(\alpha)}\}$ generate S_n.*

Proof. If n is even, then let $\alpha = (2\ 3\ \ldots\ n)$ and $\beta = (1\ n)$.

If n is odd, who knows. More thinking is required. □

Corollary 0.9. *For $n \geq 4$, $k(S_n \wr S_n) = 2$*

Proof. Take generators $\gamma = \langle \beta, \underbrace{1, \ldots, 1}_{n-1 \text{ times}}; \alpha \rangle$ and $\delta = \langle 1, \alpha, \underbrace{1, \ldots, 1}_{n-2 \text{ times}}; \beta \rangle$. Hint, notice that $\gamma^{\mathrm{ord}(\beta)} = \langle \underbrace{1, \ldots, 1}_{n \text{ times}}; \alpha^{\mathrm{ord}(\beta)} \rangle$ and $\delta^{\mathrm{ord}(\alpha)} = \langle \underbrace{1, \ldots, 1}_{n \text{ times}}; \beta^{\mathrm{ord}(\alpha)} \rangle$, then use the previous lemma.

□

Corollary 0.10. *For $n \geq 4$ and $\ell \geq 2$, $k(\mathrm{Wr}^\ell(S_n)) \leq k(\mathrm{Wr}^{\ell-1}(S_n)) + 1$.*

Proof. Suppose $\{\gamma_1, \ldots, \gamma_t\}$ generates $\mathrm{Wr}^{\ell-1}(S_n)$. Let $\alpha, \beta \in S_n$ be as in the previous lemma. For $j \in [t]$, let $\gamma'_j = \langle 1, \ldots, 1; \gamma_j \rangle \in \mathrm{Wr}^\ell(S_n)$ and let $\delta = \langle \alpha, \beta, 1, \ldots, 1; 1 \rangle$. It is easy to show that $\{\gamma'_1, \ldots, \gamma'_t, \delta\}$ generates $\mathrm{Wr}^\ell(S_n)$. (Hint: Use the elements $\delta^{\mathrm{ord}(\alpha)}$ and $\delta^{\mathrm{ord}(\beta)}$.) □

Theorem 0.11. *For $n = 2$ and $n \geq 4$, $k(\mathrm{Wr}^\ell(S_n)) = \ell$.*

Proof. □

However, for all we know $k(\mathrm{Wr}^\ell(A_n)) = 2$ for $n \geq 5$ (or any non-abelian simple group instead of A_n).