Graph Isomorphism course, Spring 2017
Instructor: László Babai
Notes by Angela Wu and instructor
Thursday, May 11, 2017

14 Day 14, ThWk7

14.1 Semidirect products

Definition 14.1 (Direct product, external characterization)**.** The **direct product of groups** G and H is $G \times H = \{g \in G, h \in H\}$ with componentwise operations[1], i.e., $(g_1, h_1) \cdot (g_2, h_2) = (g_1 g_2, h_1 h_2)$.

Definition 14.2 (Direct product, internal characterization)**.** The **internal characterization of the direct product**: Let $L, M \le G$. We say that $G = L \times M$ if $L, M \triangleleft G$, $L \cap M = 1$ and $LM = G$.

DO 14.3 (Internal $\to$ external)**.** If G, L, M satisfy the internal characterization, then $L \times M \cong G$ via the correspondence $(\ell, m) \mapsto \ell m$.

DO 14.4 (External $\to$ internal)**.** If $G = L \times M$ according to the external characterization, then the subgroups $L_1 = L \times \{1_M\}$ and $M_1 = \{1_L\} \times M$ satisfy the internal chracterization, i.e., $L_1, M_1 \triangleleft G$, $L_1 \cap M_1 = 1$, and $L_1 M_1 = G$. Moreover, $L_1 \cong L$, $M_1 \cong M$, and $L_1 \times M_1 \cong G$ via the correspondence $(\ell_1, m_1) \mapsto \ell_1 m_1$ (where $\ell_1 \in L_1$ and $m_1 \in M_1$).

The notion of **semidirect products** generalizes direct products.

Definition 14.5 (Semidirect product, internal characterization)**.** The group $G = N \rtimes R$ is the **semidirect product of** N **and** R if $N \triangleleft G$, $R \le G$, $NR = G$ and $N \cap R = 1$. (Note: if $N \triangleleft G$ and $R \le G$, then $NR \le G$ because $NR = RN$.)

Notice that the notion of semidirect products includes direct products.

DO 14.6. If $G = N \rtimes R$ then $G/N \cong R$. In particular, $|G| = |N| \cdot |R|$.

DO 14.7. The semidirect product G is not determined up to isomorphism by N and R. Show that both S_3 and $\mathbb{Z}_6$ are semidirect products of a normal subgroup $N \cong \mathbb{Z}_3$ and a subgroup $R \cong \mathbb{Z}_2$.

Definition 14.8 (Semidirect product, external characterization)**.** Given groups N, R and a homomorphism $\alpha : R \to \mathrm{Aut}(N)$, we can define $N \rtimes_\alpha R$ as the group containing elements $\{(n, r) : n \in N, r \in R\}$ under the operation of $(n_1, r_1) \cdot (n_2, r_2) := (n_1 n_2^{\alpha^{-1}(r_1)}, r_1 r_2)$.

DO 14.9 (Internal $\to$ external)**.** If $G = N \rtimes R$ (internal characterization) then G and in particular, R acts on N via conjugation. This defines a homomorphism $\alpha : R \to \mathrm{Aut}(N)$ by $\alpha(r) : n \mapsto r^{-1} n r$. Prove: $N \rtimes_\alpha R \cong G$ via the correspondence $(n, r) \mapsto nr$.

[1] The notation $G \times H$ is overloaded, used as both the direct product of sets and the direct product of groups.

DO 14.10 (External $\to$ internal)**.** If $G = N \rtimes_\alpha R$ according to the external characterization, then the subgroups $N_1 = N \times \{1_R\}$ and $R_1 = \{1_N\} \times R$ satisfy the internal characterization, i.e., $N_1 \triangleleft G$, $R_1 \le G$, $N_1 \cap R_1 = 1$, and $N_1 R_1 = G$. Moreover, $N_1 \cong N$, $R_1 \cong R$, and $N_1 \rtimes_{\alpha_1} R_1 \cong G$ via the correspondence $(n_1, r_1) \mapsto n_1 r_1$ (where $n_1 \in N_1$ and $r_1 \in R_1$) where we define $\alpha_1 : R_1 \to \mathrm{Aut}(N_1)$ by $n_1^{\alpha_1(r_1)} = (n^{\alpha(r)}, 1_R)$ where $n_1 = (n, 1_R)$ and $r_1 = (1_N, r)$.

DO 14.11. Under what homomorphism α is $N \rtimes_\alpha R = N \times R$?

14.2 Wreath products

Consider a graph X with connected components $X = X_1 \sqcup \cdots \sqcup X_k$. Suppose $\mathrm{Aut}(X_i)$ and $\mathrm{ISO}(X_i, X_j)$ are given and we are interested in finding $\mathrm{Aut}(X)$.

First suppose that all components are isomorphic. Then, automorphisms of X can by obtained by applying an automorphism of each component separately and independently, and then permuting the components. More specifically, $\mathrm{Aut}\, X = (\mathrm{Aut}\, X_1)^k \rtimes_\alpha S_k$ where, for $\sigma \in S_k$, the automorphism $\alpha(\sigma)$ of $(\mathrm{Aut}\, X_1)^k$ acts by permuting the components according to σ.

Definition 14.12 (Wreath products)**.** The **wreath product** of a group L by a permutation group $M \le S_k$ is given by $L \wr M := (L^k) \rtimes M$, where the action $M \curvearrowright L^k$ is performed by permuting the k coordinates under the given $M \curvearrowright [k]$ action.

DO 14.13. $|L \wr M| = |L|^k \cdot |M|$. Reminder: $L^k \triangleleft L \wr M$ and $G/L^k \cong M$.

Assume $L \le S_t = \mathrm{Sym}(\Omega)$ and $M \le S_k$. We now describe some natural actions by $L \wr M$.

Definition 14.14 (Sum action)**.** The **sum (union) action** $L \wr M \curvearrowright k \cdot \Omega$ is the embedding $L \wr M \to S_{kt}$ described as follows. First, L^k acts on $k \cdot \Omega$ by the i-th copy of L acting on the i-th copy of Ω. Elements of M acts on $k \cdot \Omega$ by permuting the copies.

DO 14.15. The sum action is transitive if and only if L and M are both transitive. The sum action is primitive if and only if ($k = 1$ and L is primitive) OR ($t = 1$ and M is primitive).

DO 14.16. Prove: the Sylow p-subgroup of S_{p^2} is $\mathbb{Z}_p \wr \mathbb{Z}_p$ in the sum action. What is the Sylow p-subgroup of S_{p^3}?

Definition 14.17 (Product action)**.** The **product action** $L \wr M \curvearrowright \Omega^k$ is described as follows. The action of $\tau = (\tau_1, \ldots, \tau_k) \in L^k$ on $x = (x_1, \ldots, x_k) \in \Omega^k$ is the componentwise action given by $x^\tau = (x_1^{\tau_1}, \ldots, x_k^{\tau_k})$. The action of $\sigma \in M$ on $x = (x_1, \ldots, x_k) \in \Omega^k$ permutes the coordinates by $x^\sigma = (x_{1^{\sigma^{-1}}}, \ldots, x_{k^{\sigma^{-1}}})$.

When speaking of the product action, we shall tacitly assume $|\Omega| \ge 2$.

DO 14.18. (a) If L is transitive then the $L^k \curvearrowright \Omega^k$ action is transitive. (b) The product action is transitive if and only if L is transitive. (c) If the product action is primitive, then L is primitive.

HW 14.19. If the product action is primitive, then M is transitive.

Even if both L and M are primitive, it does not follow that the product action is primitive, as the following example shows.

DO 14.20. The product action of $\mathbb{Z}_p \wr S_k$ (on p^k elements) is imprimitive.

But primitivity does follow if we excluse the case $L = \mathbb{Z}_p$. If L is primitive and M is transitive then the product action is primitive unless $|\Omega| = p$ is a prime and $L = \mathbb{Z}_p$.

14.3 Large primitive groups

▶ Johnson groups: $S_k^{(t)} \cong S_k$ acting on $\binom{k}{t}$ with $k \geq 2t+1$. These groups have order around $n^{k/t} \approx \exp(n^{1/t}/t \cdot \ln n) \approx \exp(n^{1/t})$. For bounded t this is "moderately exponential," which is too big for Luks's method, naively implemented, to work in quasi-polynomial time.

▶ Hamming groups: $S_k \wr S_t$ acting via the product action on k^t elements. Now, $n = k^t$. These groups have order $|S_k \wr S_t| = (k!)^t \cdot (t!) \approx k^{kt}t^t = (k^k t)^t = n^k t^t \approx n^{n^{1/t}} \approx \exp(n^{1/t})$.

▶ Johnson-Hamming hybrids: $S_k^{(\ell)} \wr S_t$ acts on $\binom{\Omega}{\ell}^t$, where $|\Omega| = k$. Now, $n = \binom{k}{\ell}^t \approx k^{\ell t}$. These groups have order $|S_k^{(\ell)} \wr S_t| = (k!)^t(t!) \approx k^{kt}t^t \approx n^{k/\ell} \approx n^{n^{1/t\ell}/\ell} \approx \exp(n^{1/t\ell})$, again too large of t and ℓ are bounded.

Theorem 14.21 (Cameron (1981), refined by Attila Maróti (2015))**.** *If $G \leq S_n$ is primitive and $|G| \geq n^{1+\log_2 n}$ and $n \geq 25$, then*

$$(\exists k, t, \ell)\left(n = \binom{k}{\ell}^t \text{ and } (A_k^{(\ell)})^t \leq G \leq S_k^{(\ell)} \wr S_t \text{ in the product action}\right)$$

The above theorem relies heavily on CFSG. In the equation above, $(A_k^{(\ell)})^t$ is the socle $\operatorname{Soc}(G)$ of G and $G/\operatorname{Soc}(G)$ is a transitive subgroup of S_t.

Definition 14.22 (Socle)**.** The **socle** of a group G is the product of all its minimal normal subgroups, $\operatorname{Soc}(G) = \prod M_i$ for $M_i \triangleleft_{\min} G$.

DO 14.23. $\operatorname{Soc}(G) \operatorname{char} G$.

The following exercises give some basic information toward this theorem.

DO 14.24. (a) If $G \leq S_n$ is primitive, then it has ≤ 2 minimal normal subgroups. (b) If there are 2 minimal normal subgroups, then both are regular and therefore $|G| \leq n^{1+\log_2 n}$.

Therefore, if $|G| > n^{1+\log_2 n}$ then $\operatorname{Soc}(G)$ is the unique minimal normal subgroup; it is therefore characteristically simple, so $\operatorname{Soc}(G) \cong T^t$ for some simple group T. Note that T^t is transitive (because it is a nontrivial normal subgroup of a primitive group).

DO 14.25. Prove: the simple group T is not abelian. (Hint: if T is abelian then T^t is transitive abelian and therefore regular, hence again $|G| \leq n^{1+\log_2 n}$.)

This gives the link to the CFSG: we need to distinguish cases according to the nonabelian finite simple group T. One can show that for Lie-type T we still have $|G| < n^{1+\log_2 n}$, so that leaves the alternating groups $T \cong A_k$ for some k. The analysis of this case is elementary, based on the classification of subgroups of less than exponential index in S_k.

14.4 LaTeX

The LaTeX code for semidirect product is `\rtimes` and for wreath product `\wr`.

14.5 Administrative

Quiz (20 minutes) next Tuesday. Exam on Tuesday Week 10. Grades returned Thursday Week 10. Review past DO and HW and THM.