О ПРИМЕНЕНИИ КОНСТРУКЦИИ СВЯЗКИ ГРУПП ПОДСТАНОВОК ДЛЯ ПОСТРОЕНИЯ КИБЕРУСТОЙЧИВЫХ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ СИСТЕМ

Максимовский А.Ю.

Институт проблем управления им. В.А. Трапезникова РАН,
Россия, г. Москва, ул. Профсоюзная д.65
maximay62@ipu.ru

Аннотация: Для информационно-управляющих систем (ИУС), компоненты которых, моделируются автоматами с биективными частичными функциями переходов, предложена конструкция связки групп подстановок, ассоциированной с данной системой. Получены требования к компонентам связки групп подстановок, ассоциированной с ИУС, чтобы обеспечить устойчивость ИУС от внешних воздействий.

Ключевые слова: группа подстановок, подпрямое произведение, киберустойчивость информационных систем.

При решении проблем обоснования киберустойчивости к внешним воздействиям информационно-управляющих систем (ИУС), при моделировании которых применяются конечные автоматы с биективными частичными функциями переходов возникает необходимость изучения свойств групп таких автоматов по следующим направлениям. Во-первых, необходимо уметь прогнозировать способность этой системы сохранять способность управлять (передавать управляющую информацию) своими состояниями при условии, что часть состояний вышла из строя и не реагирует на управляющие сигналы. Данная задача эквивалентна задаче определения и поиска условий достижения максимального значения транзитивности группы автомата. Во-вторых, существенно влияют на киберустойчивость ИУС специфические для групп подстановок свойства группы автомата - примитивность (импримитивность). В частности, импримитивность группы может привести к существенному ограничению маневра при управлении компонентами ИУС и, как следствие, к расширению возможностей нарушителя при проведении атак на систему. Наконец, наличие нетривиальных нормальных делителей группы автомата является признаком возможности дискредитировать систему при помощи использования управляемых извне гомоморфных образов.

Пусть C – система, содержащая s подсистем $C_1, \dots C_s$. Каждая подсистема $C_i, i = 1, \dots, s,$ имеет множество состояний K_i, и моделируется автоматом, у которого все частичные функции переходов биективны и полугруппа H_i действует как группа подстановок множества K_i. Управление подсистемами $C_i, i = 1, \dots, s,$ описывается действием группы подстановок G на множестве Δ состояний системы C. При этом выполнены условия: $K \supseteq K_1 \cup \dots \cup K_s, K_i \cap K_j = \emptyset, i \neq j,$ и (для обеспечения управления) $\Delta \cap K_j \neq \emptyset, j = 1, \dots, s.$ Таким образом, для описания свойств системы C целесообразно исследовать группу подстановок F, которая порождена группой G, действующую на множестве $\Delta \subset K$, и подпрямым произведением (см. [1]) групп H_1,…, H_s. Группу F, конструкция которой описана выше, назовем связкой групп H_1,…, H_s с помощью группы G и обозначим $F = G\{H_1, \dots, H_s\}$. Если подпрямое произведение групп H_1,…, H_s является прямым произведением этих групп, то будем называть свободной связку групп H_1,…, H_s с помощью группы G и обозначать $F = G[H_1, \dots, H_s]$. Использование конструкции связки групп подстановок в ряде случаев оказывается более удобным по сравнению со сплетением или экспоненцированием групп подстановок (см., например, [2 - 4]), в частности, потому, что подгруппа связки групп подстановок может, в свою очередь, оказаться связкой групп подстановок, действующей на множестве меньшей мощности, и это может использоваться при переходе от системы C к рассмотрению ее подсистем, обладающих необходимыми свойствами с точки зрения обеспечения информационной безопасности (см. [5]).

Будем предполагать, что группы H_1,…,H_s транзитивны на множествах $K_1, \dots, K_s$, соответственно. Обозначим $\Delta(G) = \{\Delta(1), \dots, \Delta(t)\}$ множество орбит группы G. Определим два графа для изучения связей между множествами $\Delta(i), i \in \{1, \dots, t\}$ и $K_j, j \in \{1, \dots, s\}$:

- граф Γ_K, у которого $\{1, \dots, s\}$ - множество вершин, и пара (i, j) является ребром, если найдется такое множество $\Delta(q), q \in \{1, \dots t\},$ что $K_i \cap \Delta(q) \neq \emptyset$ и $K_j \cap \Delta(q) \neq \emptyset$;
- граф Γ_Δ , у которого $\{1, \dots, t\}$ - множество вершин, и пара (p, q) является ребром, если найдется такое множество $K_j, j \in \{1, \dots, s\}$, что $K_j \cap \Delta(p) \neq \emptyset$ и $K_j \cap \Delta(q) \neq \emptyset$.

Утверждение 1. Группа F транзитивна на множестве K тогда и только тогда, когда выполнены два условия: $K = K_1 \cup \dots \cup K_s \cup \Delta_1 \cup \dots \cup \Delta_t$, и графы Γ_K и Γ_Δ являются связными.

Следствие 1. Если группа F транзитивна, то стабилизатор $G_{K'}$ множества $K' = K \backslash (K_1 \cup \dots \cup K_s)$ в группе G является единичной группой.

Приведем ряд достаточных условий примитивности группы F.

Следуя [6], будем называть подпрямое произведение групп $H_1,\ldots,H_s$ транзитивным, если для любых различных наборов элементов $a_1,\ldots,a_s$ и $b_1,\ldots,b_s$ где $a_i,b_i \in K_i, i \in \{1,\ldots,s\}$, найдется такая подстановка h в подпрямом произведении $H_1,\ldots,H_s$, что $h(a_i) = b_i, i \in \{1,\ldots,s\}$.

Утверждение 2. Пусть группы $H_1,\ldots,H_s$ транзитивны на множествах $K_1,\ldots,K_s$, соответственно, и группа G такая, что свободная связка $G[H_1,\ldots,H_s]$ транзитивна. Тогда группа $G[H_1,\ldots,H_s]$ примитивна в каждом из следующих случаев:

1) мощность множества K_i для некоторого $i \in \{1,\ldots,s\}$ взаимно проста с $|K|$ и превосходит максимальный собственный делитель числа $|K|$;

2) мощности множеств $K_1,\ldots,K_s$ взаимно просты с $|K|$, и сумма мощностей любых двух из множеств $K_1,\ldots,K_s$ превосходит максимальный собственный делитель числа $|K|$;

3) для некоторого $i \in \{1,\ldots,s\}$, группа H_i примитивна на K_i и мощность множества K_i для некоторого i$\in$ {1,...,s} превосходит максимальный собственный делитель числа $|K|$.

Утверждение 3. Пусть подпрямое произведение примитивных групп подстановок $H_1,\ldots,H_s$ транзитивно, и группа G содержит подгруппу G', орбиты которой обладают свойствами:

1) для некоторого $i \in \{1,\ldots,s\}$ G' имеет орбиту $\omega \subset K_i$, при этом $\omega \neq K_i$ и, кроме того, G' имеет орбиту ω' такую, что $\omega' \cap K_i = \emptyset$;

2) объединение орбит $\omega(1),\ldots,\omega(r)$ группы G' таких, что $\omega(j) \cap K_i \neq K_i, \omega(j) \cap K_i \neq \omega(j)$, $j \in \{1,\ldots,r\}$, причем $\omega' = \omega(1)$;, и множеств K_{i_m}, имеющих непустое пересечение с орбитами из множества $\{\omega(1),\ldots,\omega(r)\}$, имеет мощность, которая превосходит любой собственный делитель числа $|K|$.

Тогда группа $F = G\{H_1,\ldots,H_s\}$ примитивна.

Приведем ряд достаточных условий кратной транзитивности примитивной группы F.

Утверждение 4. Пусть $F = G\{H_1,\ldots,H_s\}$ - примитивная связка групп, действующая на множестве K. Тогда если группа G содержит подгруппу G', для которой связка групп $G'\{H_{i_1},\ldots,H_{i_n}\}$, $1 < n < s$, действует транзитивно на множестве $K' \subset K$, причем $|K'| \leq |K \backslash K'|$, то группа F трижды транзитивна. Если дополнительно выполнено условие $|K'| < |K \backslash K'|$, то группа F содержит знакопеременную группу $A(K)$ подстановок множества K.

Результат утверждения 3 позволяет гарантировать киберустойчивость рассмотренных в докладе классов информационно-управляющих систем по отношению к описанным выше видам внешних воздействий.

Приведем еще один результат в этом направлении для свободной связки групп подстановок.

Утверждение 5. Пусть $F = G\{H_1,\ldots,H_s\}$ – свободная связка примитивных групп $H_1,\ldots,H_s$, действующая на множестве K, и группа G содержит цикл $(a_1,\ldots,a_s)$, где $a_i \in K_i, i \in \{1,\ldots,s\}$. Тогда группа F содержит знакопеременную группу $A(K)$ подстановок множества K.

Следствие 2. В условиях утверждения 4 и четном s группа F совпадает с симметрической группой $S(K)$ подстановок множества K.

Для дальнейших исследований представляет интерес поиск оптимальных решений как при выборе групп $G, H_1,\ldots,H_s$, так в условиях применения нарушителем более обширных классов внешних, а также и внутренних неблагоприятных воздействий.

Литература

1. *Холл М.* Теория групп: Пер. с англ. – М.: Изд. иностр. лит., 1962. – 468 с.
2. *Погорелов Б.А*. Основы теории групп подстановок. Часть 1. Общие вопросы. М., 1986. - 316 с.
3. *Баннаи Э. , Ито Т.* Алгебраическая комбинаторика М.: Мир, 1987, 376 с.
4. *Калужнин Л.А., Клин М.Х., Сущанский В.И*. Экспоненцирование групп подстановок, 1. – Изв. вузов. Матем ., 1979, № 8, С. 26-33.
5. *Калашников А.О., Максимовский А.Ю.* Об оценке эффективности аддитивной ролевой модели контроля защищенности систем. //Информация и безопасность. 2019. Том 22. – № 1 (4). – С. 22-29.
6. *Федюкин М.В.* О подпрямых произведениях примитивных групп. - Труды по дискретной математике. Т. 7. - М.: Физматлит, 2003, С. 213-226.