МАТЭМАТЫКА

УДК 512.542

Д. В. Грицук
канд. физ.-мат. наук, доц., зав. каф. прикладной математики и информатики Брестского государственного университета имени А. С. Пушкина
e-mail: dmitry.gritsuk@gmail.com

ПОСТРОЕНИЕ В СИСТЕМЕ КОМПЬЮТЕРНОЙ АЛГЕБРЫ GAP ГРУПП ФИКСИРОВАННОЙ ПРОИЗВОДНОЙ π-ДЛИНЫ*

В системе компьютерной алгебры GAP построены примеры, подтверждающие точность полученных оценок производной π-длины π-разрешимой группы с малыми порядками силовских подгрупп и группы с ограничениями на порядки кофакторов. Также в системе GAP построен алгоритм функции по определению π-разрешимости группы и нахождению производной π-длины π-разрешимой группы.

Введение

Установление точности получаемых оценок инвариантов (производной длины, нильпотентной длины и π-длины, производной π-длины) разрешимых и частично разрешимых групп осуществляется путем нахождения примеров групп, свойства которых удовлетворяют условию теоремы. На практике такой процесс является трудной задачей.

Одним из способов решения такой проблемы является использование возможностей различных компьютерных алгебраических систем. Среди имеющегося изобилия такого рода программ выделим компьютерную систему GAP (Group Algorithm Programming) [1; 2], функционал которой как нельзя лучше подходит для изучения вопросов теории групп. Одной из крупнейших библиотек системы GAP является библиотека SmallGroups, которая содержит группы, порядок которых не превышает 2000 (за исключением 49 487 365 422 групп порядка 1024, точное количество которых, кстати, также было определено с помощью системы GAP). Однако не всегда в рамках данной библиотеки можно найти необходимый пример. Данная проблемная ситуация решается за счет использования полупрямого произведения двух произвольных групп K и H с заданными свойствами. Основываясь на теореме Кэли, иногда для ускорения вычислений удобно группы K и H заменять изоморфными группами подстановок.

С использованием преимуществ открытого кода системы был разработан целый ряд программ, отсутствующих в функционале системы GAP который дает возможность построения примеров групп, имеющих высокие значения производной π-длины и порядок которых значительно превышает 2000. Построенные алгоритмы в полном объеме совместимы со всей функциональностью системы, что позволяет в дальнейшем использовать их для исследования подобного рода проблем.

Построение групп фиксированной производной π-длины в системе GAP

Напомним, что группа G называется π-разрешимой, если она обладает субнормальным рядом

$$1 = G_0 \subseteq G_1 \subseteq G_2 \subseteq \cdots \subseteq G_m = G, \quad (1)$$

факторы которого являются либо разрешимыми π-группами, либо π'-группами. Данный ряд будем называть (π', π)-рядом группы G.

**Работа выполнена при финансовой поддержке Белорусского республиканского фонда фундаментальных исследований (проект № Ф17М-063).*

Т. к. необходимым условием для нахождения производной π-длины группы является ее π-разрешимость, то первый из рассматриваемых алгоритмов IsPiSolvable(G,pi) позволяет выяснить, обладает группа G этим свойством или нет.

```
IsPiSolvable:=function(G,pi)
local cs,x,fact,j,l;
if usl_pi(G,pi)=0 then
    return true;
fi;
cs:=CompositionSeries(G);
l:=List([1..Length(cs)-1],j->FactorGroup(cs[j],cs[j+1]));
return
For All([1..Length(cs)-1], j->(usl_pi(l[j],pi)=1 and IsPrime(Size(l[j]))=true) or (usl_pi(l[j],pi)=0));
end;
```

Здесь промежуточной функцией является функция usl_pi(), которая проверяет, является ли группа π-группой или нет.

```
usl_pi:=function(G, pi)
local c, d, f, o, obsch;
c:=Size(G);
f := AsSet(FactorsInt(c));
obsch := Intersection(f, pi);
if obsch=f then
    return 1;
else
    if obsch = [] then
        return 0;
    fi;
fi;
return -1;
end;
```

В 2006 г. В. С. Монахов в [3] предложил определение производной π-длины π-разрешимой группы. Напомним это определение.

Пусть G – π-разрешимая группа. Тогда она обладает субнормальным рядом (1), факторы которого являются либо π'-группами, либо абелевыми π-группами для всех i.

Наименьшее число абелевых π-факторов среди всех таких субнормальных рядов группы G называется производной π-длиной π-разрешимой группы G и обозначается через $l_\pi^a(G)$. Если $\pi(G) = \pi$, то значение $l_\pi^a(G)$ совпадает со значением производной длины группы G.

Система компьютерной алгебры GAP содержит встроенную функцию Derived-Length (G) для нахождения производной длины разрешимой группы. Ее аналога для частично разрешимых групп в GAP нет.

Разработана функция proiz(G,pi) для нахождения производной π-длины π-разрешимой группы.

```
proiz:=function(G, pi)
local index, i, j, s, f, f1, iter, intermed, len, m, i1, i2, H,uslovie;
H := TrivialSubgroup(G);
intermed := IntermediateSubgroups(G , H);
```

```
if Length(intermed.subgroups) = 0 then
        if IsNormal(G, H) = true then
            uslovie := usloviepi(FactorGroup(G,H), pi);
            if uslovie >= 0 then
                if IsAbelian(FactorGroup(G,H)) = true and uslovie = 1 then
                    return 1;
                else
   return 0;
   fi;
            else
   fi;
        else
fi;
fi;
m:=NullMat(Length(intermed.subgroups) + 2,
Length(intermed.subgroups) + 2);
for i in intermed.inclusions do
      i1:=i[1]+1;
      i2:=i[2]+1;
      m[i1][i2] := 1;
od;
len := Length(intermed.subgroups) + 2;
return DFS(m, intermed.subgroups, len, 1, G, H, 0, pi, false, H);
end;
```

Промежуточной для функции proiz(G,pi) является функция DFS(), которая организует рекуррентный поиск всех субнормальных (π', π)-рядов группы G и определяет из них тот, который имеет наименьшее количество абелевых π-факторов.

```
DFS:=function(A, s, n, v, G, H, current, pi, zapomnili, start)
local i, index, f1, f, res, min, uslovie, next, start_uslovie, proverili, zapomnin,
noviy_start;
min := 0;
res := current;
i:=v;
while i <= n do
      if (A[v][i] > 0) and (i > v) then
            if v = 1
                  then f := H;
            else f := s[v-1];
            fi;
            if i = n
                  then f1 := G;
            else f1 := s[i-1];
   fi;
   zapomnin := false;
   if IsNormal(f1, f) = true
                  then
              uslovie := usloviepi(FactorGroup(f1,f), pi);
              if uslovie >= 0
   then
```

```
                    proverili := false;
                  if IsAbelian(FactorGroup(f1,f)) = true and uslovie = 1
                      then
                          zapomnin := true;
                          if zapomnili = true and IsNormal(f1, start)
                              then
                    start_uslovie := usloviepi(FactorGroup(f1, start), pi);
                  if IsAbelian(FactorGroup(f1, start)) and start_uslovie = 1
                      then
                          next := current;
                          proverili := true;
                          noviy_start := start;
                    else
                        noviy_start := f;
                    fi;
                                  else
                                      noviy_start := f;
                                  fi;
                                  if IsAbelian(f1) and proverili = false
                                      then
                                          next := 1;
                                          proverili := true;
                                  fi;
                                  if proverili = false
                                        then
                                            next := current + 1;
                                  fi;
                                  else
                                        next := current;
                                        noviy_start := f;
                                  fi;
                                  if f1 = G
                                      then
                                          res := next;
                                  else
                          res := DFS(A, s, n, i, G, H, next, pi, zapomnin, noviy_start);
                                  fi;
                                  if res > 0 and res < min or min = 0
                                        then
                                            min := res;
                                  fi;
                                  else
                              fi;
                          else
                          fi;
            fi;
            i := i+1;
    od;
    return min;
    end
```

Разработанные функции позволяют устанавливать точность получаемых оценок инвариантов частично разрешимых групп. Например, с помощью данных алгоритмов удалось установить точность оценок производной π-длины π-разрешимой группы, полученных в работах [4; 5].

Напомним, что число n свободно от n-х степеней, если p^m не делит n для всех простых p. При $m = 2$ говорят, что n свободно от квадратов, при $m = 3$ – от кубов.

Теорема 1 [4]. *Пусть G – π-разрешимая группа.*

1) Если порядок π-холловой подгруппы свободен от кубов, то справедливы следующие утверждения:

a) если $2 \notin \pi$, то $l_\pi^a(G) \leq 2$;

b) если $2 \in \pi$, то $l_\pi^a(G) \leq 3$.

2) Если порядок π-холловой подгруппы свободен от квадратов, то G – разрешимая группа и $l_\pi^a(G) \leq 2$.

Пример 1. Пусть E – элементарная абелевая группа порядка 25. С помощью компьютерной системы GAP построено полупрямое произведение $G = [E]S_3$ порядка 1296. Производная $\{2,3,5\}$-длина группы G равна 4 и группа G имеет порядок свободный от кубов. Группа $G = A_5 \times ([Z_{29}]Z_7)$ является $\{7,29\}$-разрешимой группой и порядок $\{7,29\}$-холловой подгруппы свободен от кубов. Кроме того, производная $\{7,29\}$-длина группы G равна 2. Таким образом, все оценки производной π-длиной π-разрешимой группы G из теоремы 1 являются точными.

Напомним, что кофактором подгруппы H группы G называется фактор-группа $H/Core_G H$, где $Core_G H$ – ядро подгруппы H в группе G, т. е. наибольшая нормальная подгруппа в G, содержащаяся в H. В дальнейшем кофактор подгруппы H в группе G будем обозначать $\mathrm{Cof}_G(H)$.

Теорема 2 [5]. *Пусть G – π-разрешимая группа. Если $Cof_G(X)$ циклический, где X – произвольная p-подгруппа группы G и $p \in \pi$, то:*

1) $l_\pi^a(G/\Phi(G)) \leq 2$, если $2 \notin \pi$;

2) $l_\pi^a(G/\Phi(G)) \leq 4$, если $2 \in \pi$.

Пример 2. Группа $G = A_5 \times ([Z_{29}]Z_7)$является $\{7,29\}$-разрешимой группой и кофакторы 29-подгрупп и 7-подгрупп являются циклическими. Кроме того, производная $\{7,29\}$-длина группы G равна 2. Таким образом, оценка производной π-длиной π-разрешимой группы G из теоремы 2 (1) является точной.

Заключение

В системе компьютерной алгебры GAP построены примеры, подтверждающие точность оценок производной π-длины π-разрешимой группы, полученных ранее автором совместно с А. А. Трофимуком. В частности, построены примеры, подтверждающие точность оценок производной π-длины π-разрешимой группы с малыми порядками силовских подгрупп и группы с ограничениями на порядки кофакторов.

Также приведены алгоритмы, построенных в GAP функций, по определению π-разрешимости группы и нахождению производной π-длины π-разрешимой группы.

Построенные примеры и разработанные алгоритмы расширят имеющийся функционал системы компьютерной алгебры GAP и будут способствовать созданию новых теоретико-групповых пакетов этой системы. Найденные оценки инвариантов имеют также важное прикладное значение: они могут быть использованы при построении стойких алгоритмов алгебраической криптографии и защиты информации.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. The GAP Group, GAP – Groups, Algorihms and Programming, Version 4.4. 2016 [Electronic resours]. – Mode of access: http://gap-system.org.

2. Грицук, Д. В. Компьютерная алгебра : курс лекций / Д. В. Грицук, А. А. Трофимук / Брест. гос. ун-т им. А. С. Пушкина. – Брест : БрГУ, 2017. – 112 с.

3. Монахов, В. С. Конечные группы с полунормальной холловой подгруппой / В. С. Монахов // Мат. заметки. – 2006. – Т. 80, № 4. – Р. 573–581.

4. Грицук, Д. В. Оценки производной π-длины π-разрешимой группы, у которой π-холловы подгруппы свободны от n-ых степеней / Д. В. Грицук, А. А. Трофимук, Т. А. Артюшеня // Вестн. Витеб. гос. ун-та им. П. М. Машерова. – 2018. – № 1 (98). – С. 11–15.

5. Грицук, Д. В. Производная p-длина p-разрешимой группы с ограниченными факторами / Д. В. Грицук, А. А. Трофимук // Изв. ГГУ им. Ф. Скорины. Естеств. науки. – 2019. – № 3 (114). – С. 147–152.

Рукапіс паступіў у рэдакцыю 03.04.2020

Gritsuk D. V. **Construction of the Groups of the Fixed Derivative π-Length in the System of GAP Computer Algebra**

In the system of GAP Computer Algebra the author provides the examples that confirm the accuracy of the obtained estimates of the derivative of the π-length of a π-solvable group with small orders of Sylow subgroups and groups with restrictions on cofactor orders. Also a function algorithm has been built in the GAP system for determining the π-solvability of a group and finding the derivative of the π-length of a π-solvable group.