Н. В. Ф о м и ч е в (Москва, МИФИ)**. Свойства линейных признаков в полугруппах преобразований.**

Во многих приложениях важной задачей является определение линейной подполугруппы заданной полугруппы G преобразований пространства P^r над полем P характеристики q.

В [2] показано, что линейная подгруппа группы G содержится в пересечении четырех наследственных подмножеств группы G. В работе, представленнгой данным сообщением, получено включение линейной подполугруппы $SL(r,P)$ преобразований пространства P^r в пересечение пяти наследственных подмножеств. Для групп данная оценка улучшает известную оценку из [2].

Полугрупповой признак $SL(r,P)$ в полугруппе $\Sigma(P^r)$ всех преобразований векторного пространства P^r назовем *линейным признаком*.

Пусть Σ_θ, $\overline{C}$, $\Lambda^{[p\nu]}(P^r)$ и $\Sigma(P^r)$ суть наследственные признаки в полугруппе, называемые *стабилизатором нуля*, *множеством*, соответственно, *всех замкнутых сверху*, *p-нормально неподвижных* и *$\overline{\sigma}$-стабильных преобразований* пространства P^r.

Пусть $T_x(g)$ есть дерево с корнем x, являющееся таким максимальным подграфом графа Γ_g, что x — циклическая вершина в Γ_g, и все остальные вершины из $T_x(g)$ — ациклические. Пусть $n_{x,i}(g)$ — количество вершин на i-м уровне дерева $T_x(g)$. Обозначим $H(q|r)$ множество таких преобразований g из $\Sigma(P^r)$, что величина $\sum_{i=0}^{k} n_{x,i}$ делится на q для любой циклической вершины x графа Γ_g и при любом $k=1,\ldots,h$, где h — максимальная длина подхода в графе Γ_g.

Теорема. *Справедливо включение*: $SL(r,P) \subseteq \Sigma_\theta \cap \overline{C} \cap \Lambda^{[p\nu]}(P^r) \cap \Sigma(P^r) \cap H(q|r)$.

В частном случае линейной подгруппы доказанное включение улучшает оценку из [2], так как замкнутые сверху преобразования содержатся во множестве унидоминантных преобразований.

Следствие 1. *Если хотя бы один из признаков Σ_θ, $\overline{C}$, $\Lambda^{[p\nu]}(P^r)$, $\Sigma(P^r)$ или $H(q|r)$ пуст в полугруппе G, то пуст и линейный признак.*

Следствие 2. *Если для полугруппового преобразования g нулевой элемент пространства P^r лежит на подходе графа Γ_g, то линейный признак пуст в циклической полугруппе $\langle g\rangle$.*

Утверждение 1. *Если в графе Γ_g полугруппового преобразования g количество циклических точек не равно степени q, то линейный признак в циклической полугруппе $\langle g\rangle$ пуст.*

Д о к а з а т е л ь с т в о. Согласно [1], любое линейное преобразование пространства подобно матрице, называемой *естественной нормальной формой*. Она состоит из двух блоков, расположенных на главной диагонали. Один блок описывает цикловую структуру преобразования, а второй —- структуру подходов в графе Γ_g. Из свойств естественной нормальной формы следует, что количество циклических точек равно степени характеристики поля P. Кроме того, количество циклических точек преобразования g^t инвариантно одинаково для любого t, поэтому количество циклических точек любого преобразования полугруппы $\langle g\rangle$ также есть степень q.

Исследуем линейную подполугруппу генераторов $[d,k]$-самоусечения [3], построенных на основе линейного регистра связи (ЛРС) с обратной связью f, реализующего подстановку h пространства P^r. Если на выходе ЛРС — ноль, то состояние x заменяется на $h^d(x)$, если единица — на $h^k(x)$. Продвижка σ ЛРС за один такт определяется формулой $\sigma = d(f(x)\oplus 1)+kf(x)$. Порождаемая генератором циклическая полугруппа есть $\langle h^\sigma(x)\rangle$.

Пусть генератор имеет ненулевое начальное заполнение, а ЛРС имеет максимальный период.

Утверждение 2. *Если преобразование g пространства P^r реализует генератор $[t,2t]$-самоусечения и* НОД$(t,2r-1)=1$, *то линейный признак в циклической полугруппе $\langle g\rangle$ пуст.*

Д о к а з а т е л ь с т в о. В [3] показано, что граф Γ_g состоит из циклов и подходов. В условиях утверждения генератор имеет единственный цикл длины $\lfloor 2/3(2^r - 1)\rfloor$, что больше половины точек всего пространства P^r. Следовательно, по утверждению 1 линейный признак в циклической полугруппе $\langle g\rangle$ пуст.

СПИСОК ЛИТЕРАТУРЫ

1. *Гилл. А.* Линейные последовательные машины. М.: Наука, 1974, 288 с.
2. *Фомичев В. М.* О линейной подгруппе группы преобразований некоторых генераторов гаммы с неравномерным движением. — В сб.: Вестник МГУЛ, № 95. М.: МГУЛ, 2006, 7 с.
3. *Rueppel R. A.* When shift registers clock themselves. — In: Lecture Notes in Comp. Sci., 304. Berlin: Springer-Verlag, 1988.