Сибирский математический журнал
Январь—февраль, 2016. Том 57, № 1

УДК 519.143

ОБ ОДНОМ ПРИЗНАКЕ СВИТЧИНГОВОЙ РАЗДЕЛИМОСТИ ГРАФОВ ПО МОДУЛЮ q

Е. А. Беспалов, Д. С. Кротов

Аннотация. Рассматриваются графы, ребра которых помечены числами (весами) от 1 до $q-1$ (нуль соответствует отсутствию ребра). Граф называется *аддитивным*, если вершины можно пометить таким образом, что для любых двух несмежных вершин сумма меток по модулю q равна нулю, а для смежных — весу соответствующего ребра. *Свитчингом данного графа* называется его сумма по модулю q с некоторым аддитивным графом на том же множестве вершин. Граф на n вершинах называется *свитчингово разделимым*, если некоторый его свитчинг не имеет компонент связности мощности больше $n-2$. Рассматривается следующий признак свитчинговой разделимости: если удаление любой вершины графа G приводит к свитчингово разделимому графу, то и сам граф G свитчингово разделим. Доказывается этот признак для нечетного q и характеризуется множество исключений для четного q. Устанавливается связь между свитчинговой разделимостью графа и разделимостью n-арной квазигруппы, построенной по этому графу.

DOI 10.17377/smzh.2016.57.102

Ключевые слова: свитчинг Зейделя, разделимость, n-арные квазигруппы.

1. Введение

Тема настоящего исследования относится к широкому классу задач о взаимоотношениях между свойствами графа и свойствами подграфов и имеет приложения к теории n-арных квазигрупп (латинских гиперкубов). Мы изучаем связь свитчинговой разделимости графов по модулю q с разделимостью подграфов. Основной рассматриваемый вопрос: существует ли неразделимый граф, у которого удаление любой вершины приводит к разделимому графу? Назовем такие графы *критическими*. Получен исчерпывающий ответ на этот вопрос: класс критических графов удалось полностью охарактеризовать, они существуют при любом четном q и любом нечетном числе вершин начиная с пяти.

Этот вопрос оказывается важным с точки зрения изучения другого класса комбинаторных объектов — n-арных квазигрупп, в комбинаторике известных также как латинские гиперкубы. Напомним, *n-арной квазигруппой конечного порядка q* называется n-местная операция $\Sigma^n \to \Sigma$, обратимая по каждому аргументу, где Σ — некоторое множество мощности q (носитель квазигруппы). n-Арная квазигруппа называется *разделимой*, если она представима в виде бесповторной суперпозиции квазигрупп меньшей арности. Для n-арных квазигрупп можно сформулировать аналогичный вопрос: существует ли такая неразделимая n-арная квазигруппа (назовем ее *критической*), что подстановка

Работа выполнена при финансовой поддержке Российского научного фонда (код проекта 14–11–00555).

любой константы на место любого аргумента приводит к разделимой n-арной квазигруппе? Предположим, что мы изучаем некоторый класс квазигрупп, для которого ответ на этот вопрос отрицательный, и пытаемся доказать некоторую гипотезу о строении любой неразделимой квазигруппы (самый простой вариант гипотезы: неразделимых вообще нет, пример подобных рассуждений см. в [1, разд. 6]). Тогда согласно индукционному предположению можем считать, что фиксацией некоторого аргумента из исходной n-арной квазигруппы получаем $(n-1)$-арную квазигруппу, для которой гипотеза верна (если мыслить n-арную квазигруппу как n-мерную таблицу значений, то известно, что гипотеза верна для некоторого слоя таблицы). Подобный ход рассуждений был успешно применен при характеризации n-арных квазигрупп порядка 4 [2], хотя именно наличие критических квазигрупп сильно усложнило доказательство, вынуждая использовать индукционные соображения глубины два и более слабую версию признака разделимости. В настоящее время известно, что не существует критических n-арных квазигрупп простого порядка [1] и существуют критические n-арные квазигруппы любого порядка, кратного 4 [3], при любом четном $n \geq 4$. Последние строятся при помощи критических графов, где разделимость рассматривается по модулю 2 (к слову, в случае $q = 2$ свитчинги графа хорошо известны в литературе как свитчинги Зейделя [4], а свитчинговые классы эквивалентны так называемым два-графам [5]).

Достаточно естественным является вопрос о возможности построения критических квазигрупп на основе критических графов при $q > 2$. В качестве промежуточного этапа в построении квазигрупп из графов в случае простого q используются квадратичные функции над полем $\mathbb{Z}_q$ из q элементов, а порядок полученных квазигрупп равен q^2, эти построения описаны в разд. 3 (таким образом, минимальный порядок квазигрупп, для которого ставится вопрос, равен 9).

В настоящей работе описываются все критические графы. В частности, установлено, что в случае нечетного q таких графов нет, и получить критические квазигруппы нечетного порядка описанным способом невозможно. Это позволяет предположить, что критических квазигрупп нечетного порядка также нет, и, более того, общий ход рассуждений для доказательства этого факта может быть частично заимствован из доказательства для графов. С другой стороны, квазигруппы, построенные по графам, являются очень частным случаем, и разумно предположить, что гипотетическое доказательство для квазигрупп будет значительно сложнее.

В разд. 2 формулируется и доказывается основной результат настоящей работы (теорема 1). Мы определяем класс графов $G_{n,\gamma}$ и показываем, что любой критический граф будет свитчингом графа из этого класса. Важным следствием является то, что при нечетных q критических графов нет. Частный случай $q = 2$ рассмотрен ранее в [6, 7].

В разд. 3 показана связь свитчинговой разделимости графов по модулю q с разделимостью n-арных квазигрупп порядка q^2, построенных по этим графам (предложение 5), и (в качестве промежуточного звена) с разделимостью частичных функций над $\mathbb{Z}_q$, определенных на наборах с фиксированной суммой (предложение 4). Следствие 6, в котором результаты теоремы 1 переносятся на n-арные квазигруппы порядка q^2, построенные по графам при помощи q-значных квадратичных функций, где $q > 2$ простое, также является одним из основных результатов данной работы. Обобщение этого утверждения на произвольные n-арные квазигруппы, в том числе других порядков, является важным направлением для дальнейших исследований в этой области.

Завершая введение, хочется обратить внимание читателя на работу [8], где связность графов также используется для получения результатов о разделимости (точнее о приводимости — частном случае разделимости) n-арных квазигрупп. Однако как подходы, так и полученные результаты почти не пересекаются с содержанием настоящей статьи.

2. Разделимость графов

Будем рассматривать неориентированные графы, ребра которых помечены элементами из множества $\{1,\dots,q-1\}$, $q \geq 2$ натуральное, которые будем называть *весом* ребра (вес можно также трактовать как кратность). Метку 0 будем ассоциировать с отсутствием ребра, т. е. пару несмежных вершин будем считать ребром веса 0 (что тем не менее не позволяет считать эти вершины соседними). Таким образом, реберно помеченный граф удобно представлять парой (V,E), где V — множество вершин, а $E : V^2 \to \{0,1,\dots,q-1\}$ — симметричное отображение, равное нулю везде на диагонали $\{(v,v) \mid v \in V\}$. Под *подграфом* графа $G = (V,E)$ будем подразумевать подграф $G_W = (W,I)$, порожденный множеством вершин $W \subset V$ и унаследовавший от G веса ребер: $I(v,w) = E(v,w)$ для любых $v,w \in W$. Результатом сложения двух графов G_1 и G_2 с общим множеством вершин будет граф G на том же множестве вершин, определенный следующим образом: вес любого ребра графа G равен сумме по модулю q весов соответствующих ребер в графах G_1 и G_2. Граф будем называть *аддитивным*, если каждую его вершину можно пометить числами от 0 до $q-1$ таким образом, что вес каждого ребра будет равен сумме по модулю q меток двух вершин ребра. Далее определим *свитчинг* графа G как результат сложения графа G с некотором аддитивным графом на том же множестве вершин. Множество вершин W графа G назовем *отделимым*, если некоторый свитчинг графа G не содержит ребер (ненулевого веса) между W и $V\backslash W$. Легко видеть, что любое множество вершин мощности 0, 1, $n-1$ или n в графе порядка n отделимо. Любые другие отделимые множества назовем *нетривиальными*. Граф $G = (V,E)$ назовем *свитчингово разделимым* (далее в тексте — просто *разделимым*), если существует нетривиальное отделимое множество его вершин.

Лемма 1. *Множество аддитивных графов замкнуто относительно сложения.*

Доказательство. Утверждение следует прямо из определения: в качестве метки каждой вершины результирующего графа можно взять сумму меток этой вершины в графах-слагаемых. □

Таким образом, отношение «граф G — свитчинг графа H» является эквивалентностью. Если какое-то множество отделимо в графе (или в некотором подграфе), то оно отделимо и в каждом его свитчинге (в соответствующем подграфе), поэтому в вопросах разделимости без потери общности можно рассматривать наиболее удобный свитчинг данного графа. В частности, всегда можно считать некоторую одну данную вершину изолированной. Далее под словами «изолируем вершину o» будем подразумевать рассмотрение без потери общности свитчинга исходного графа, у которого вершина o изолирована.

Лемма 2. *Множество вершин W графа $G = (V,E)$ отделимо тогда и только тогда, когда существуют $W_0,\dots,W_{q-1}$, $V_0,\dots,V_{q-1}$ такие, что $W =$*

$W_0 \cup W_1 \cup \dots \cup W_{q-1}$, $V \backslash W = V_0 \cup V_1 \cup \dots \cup V_{q-1}$ и любое ребро, соединяющее вершины из множеств W_i и V_j, имеет вес $i + j$.

Доказательство. Сопоставив каждой вершине из W_i или V_i метку $q - i$, породим некоторый аддитивный граф. Очевидно, что его сумма с исходным графом не имеет ребер, соединяющих W и $V \backslash W$. □

Следствие 1. *Пусть множество вершин W графа $G = (V, E)$, имеющее изолированную вершину, отделимо. Тогда любая вершина из W соединена со всеми вершинами из $V \backslash W$ ребрами одного веса.*

Доказательство. Допустим, что в разбиении множества $V \backslash W$ из леммы 2 есть хотя бы два непустых множества. Но тогда вершины из разных множеств будут соединены с изолированной вершиной ребрами разных весов, что неверно. Поэтому разбиение множества $V \backslash W$ состоит не более чем из одного непустого элемента и любая вершина из W соединена со всеми вершинами из $V \backslash W$ ребрами одного и того же веса. □

Следствие 2. *Пусть любая вершина из множества $V \backslash W$ соединена со всеми вершинами W ребрами одного и того же веса. Тогда W отделимо.*

Доказательство. Обозначим $W_0 = W$, $W_1 = \dots = W_{q-1} = \varnothing$. Множество вершин из $V \backslash W$, соединенных с вершинами из W ребрами веса i, обозначим через V_i. Тогда по лемме 2 множество W отделимо. □

Следствие 3. *Пусть граф G разделим и имеет изолированную вершину o. Тогда для любых $i, j \in \{0, 1, \dots, q-1\}$ если в графе G поменять веса i и j местами, то получившийся граф также разделим.*

Доказательство. Пусть W — нетривиальное отделимое множество, не содержащее вершину o. По следствию 1 любая вершина из $V \backslash W$ соединена со всеми вершинами из W ребрами одного и того же веса. Но если поменять местами веса i и j в графе G, то полученный граф будет разделим по следствию 2. □

Лемма 3. *Пусть D — разделимый граф порядка больше 4 и d — некоторая его вершина. Граф $D \backslash \{d\}$ неразделим тогда и только тогда, когда вершина d в графе D принадлежит единственному нетривиальному отделимому множеству вершин $W = \{d, e\}$ для некоторой вершины e.*

Доказательство. Пусть $D = (V, E)$ — разделимый граф, $|V| \geq 5$, $D \backslash \{d\}$ — его неразделимый подграф и W — нетривиальное отделимое множество, содержащее d. Сначала предположим, что $|W \backslash \{d\}| \geq 2$. Тогда $W \backslash \{d\}$ и $V \backslash W \backslash \{d\}$ содержат по крайней мере по две вершины и по лемме 2 граф $D \backslash \{d\}$ разделим; противоречие. Предположим, что у нас есть два отделимых множества $\{d, e\}$и $\{d, b\}$. Изолируем вершину d. Тогда по следствию 1 вершина e будет соединена со всеми остальными вершинами (за исключением вершины d) ребрами одинакового веса. Аналогично с вершиной b. Но тогда, если удалить вершину d, множество $\{e, b\}$ будет отделимо по следствию 2, что противоречит неразделимости $D \backslash \{d\}$.

Пусть $W = \{d, e\}$ — единственное нетривиальное отделимое множество, содержащее d. Изолируем вершину e. Тогда по следствию 1 вершина d соединена со всеми вершинами из $D \backslash \{d, e\}$ ребрами одного веса. Предположим от противного, что граф $D \backslash \{d\}$ разделим; обозначим через U его нетривиальное отделимое множество, не содержащее вершины e. Так как вершина d соединена со всеми вершинами U ребрами одного веса, по следствию 2 множество

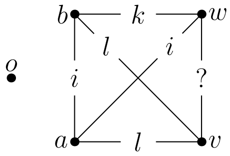

Рис. 1. $k \neq i$, $l \neq i$.

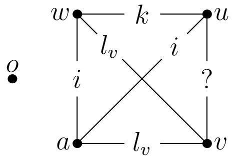

Рис. 2. $k \neq i$, $l_v \neq i$.

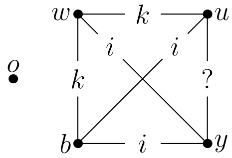

Рис. 3. $k \neq i$.

U отделимо в D. Поскольку $V \backslash U$ содержит d и не совпадает с W, получаем противоречие с единственностью W. $\square$

Лемма 4. *Любой разделимый граф порядка $n \geq 5$ имеет либо* 0, *либо* 2 *неразделимых подграфа порядка $n-1$.*

Доказательство. Пусть граф G имеет неразделимый подграф $G \backslash \{a\}$ для некоторой вершины a. Тогда по лемме 3 отделимым множеством графа G будет пара $\{a, b\}$ для некоторой вершины b. Считая без потери общности, что $G \backslash \{a, b\}$ содержит изолированную вершину, видим по следствию 1, что граф $G \backslash \{b\}$ изоморфен графу $G \backslash \{a\}$ и, следовательно, также неразделим. Удаление из графа G любой вершины c, отличной от a и b, приводит к разделимому подграфу, поскольку $\{a, b\}$ остается отделимым в $G \backslash \{c\}$. $\square$

Предложение 1. *Пусть в графе G порядка $n \geq 5$ каждый подграф порядка* 4 *или* 5 *разделим. Тогда граф G разделим.*

Доказательство. Без потери общности можно считать, что граф содержит изолированную вершину o. По следствию 1 в графе $G \backslash \{o\}$ не существует трех вершин таких, что веса ребер между этими вершинами попарно различны. Выберем в этом графе три вершины a, b, c, соединенные между собой ребрами двух различных весов (если таких не существует, то в подграфе $G \backslash \{o\}$ все ребра одного веса и граф G разделим): $E(a, b) = i \neq E(a, c) = E(b, c) = j$. Определим три множества U, V, W: U — множество вершин, соединенных с вершинами a и b ребрами веса i; V — множество вершин, соединенных с вершинами a и b ребрами одинакового веса, отличного от i; W — множество вершин, соединенных с вершинами a и b ребрами разного веса.

Для произвольных вершин v из V и w из W рассмотрим подграф, порождаемый множеством вершин $\{o, a, b, v, w\}$. Пусть ребра $\{v, a\}$ и $\{v, b\}$ имеют вес $l \neq i$. Одно из ребер $\{w, a\}$ и $\{w, b\}$ имеет вес i, скажем $\{w, a\}$. Тогда ребро $\{w, b\}$ будет иметь вес $k \neq i$. По условию леммы рассматриваемый подграф на пяти вершинах разделим, а значит, имеет отделимую пару вершин. Как легко убедиться, применяя следствие 1, такой парой может быть только $\{o, v\}$ или $\{w, b\}$ (рис. 1). В обоих случаях ребро $\{v, w\}$ должно иметь вес l. В силу произвольности вершин v и w получаем, что любая вершина v из V соединена со всеми вершинами из $W \cup \{a, b\}$ ребрами одного веса, который обозначим через l_v.

Далее, множество U разделим на два U_1 и U_2 следующим образом: U_1 — множество вершин, которые соединены со всеми вершинами из $W \cup \{a, b\}$ ребрами веса i; U_2 — остальные вершины. Заметим, что если U_2 пусто, то из доказанного уже следует отделимость множества $V \cup U_1 \cup \{o\}$.

Рассмотрим произвольную вершину u из U_2. По определению множества U_2 найдется вершина w из W такая, что $E(u, w) \neq i$. Без потери общности можно считать, что $E(w,a) = i \neq E(w,b)$. Для произвольной вершины v из V рассмотрим подграф, порожденный пятеркой $\{o,a,u,w,v\}$ (рис. 2). Отделимой парой в этом подграфе может быть только $\{o,v\}$ или $\{u,w\}$. В обоих случаях $E(v,u) = l_v$.

При тех же условиях на u и v рассмотрим произвольную вершину y из U_1. В графе, порожденном пятеркой $\{o,b,u,w,y\}$ (рис. 3), отделимой парой может быть только $\{o,y\}$ или $\{u,b\}$. В обоих случаях $E(y,u) = i$.

Таким образом, каждая вершина v из V соединена со всеми вершинами из $\{a,b\} \cup W \cup U_2$ ребрами веса l_v, а каждая вершина из U_1 соединена со всеми вершинами из $\{a,b\} \cup W \cup U_2$ ребрами веса i. По следствию 2 множество $V \cup U_1 \cup \{o\}$ отделимо и граф G разделим. $\square$

Предложение 2. *Пусть G_K — неразделимый подграф порядка χ, $4 \leq \chi < n-2$, графа G порядка n, и пусть все подграфы графа G порядков $\chi+1$ и $\chi+2$, содержащие G_K в качестве подграфа, разделимы. Тогда граф G разделим.*

Доказательство. Рассмотрим произвольную вершину a из $V \backslash K$. Граф $G_{K\cup\{a\}}$ разделим, в то время как граф G_K неразделим. По лемме 3 в графе $G_{K\cup\{a\}}$ будет только одно (с точностью до дополнения) нетривиальное отделимое множество вершин $\{a,c\}$ для некоторой c из K. Изолируем вершину c. Тогда по следствию 1 вершина a соединена со всеми вершинами из $K\backslash\{c\}$ ребрами одинакового веса. Для доказательства разделимости графа G необходимо найти нетривиальное отделимое множество. Для этого в множестве $V\backslash K$ выделим подмножество A вершин, которые соединены со всеми вершинами множества $K\backslash\{c\}$ ребрами одинакового веса, в частности $a \in A$. В оставшейся части доказательства покажем, что множество $A \cup \{c\}$ отделимо в G. Остаток $V\backslash K\backslash A$ обозначим через B.

Докажем утверждение

$(*)$ *Для произвольной вершины d из $V\backslash(K \cup \{a\})$ либо $d \in A$, либо вершина a соединена с d ребром того же веса, что и с вершинами из $K\backslash\{c\}$.*

Рассмотрим граф $G_{K\cup\{a,d\}}$. По условию он разделим, поэтому вершина d лежит в некотором нетривиальном отделимом в $G_{K\cup\{a,d\}}$ множестве W. Величина $m = |W \cap K|$ может принимать три значения: 0, 1 или $\chi - 1$ (иначе $W\backslash\{a,d\}$ — нетривиальное отделимое множество в G_K, что противоречит неразделимости этого графа). Рассмотрим эти случаи.

• $m = 0$. В этом случае $\{a,d\}$ отделимо в графе $G_{K\cup\{a,d\}}$. По следствию 1 любая вершина из K соединена с этой парой вершин ребрами одного и того же веса. Следовательно, вершина d соединена со всеми вершинами множества $K\backslash\{c\}$ так же, как и вершина a, т. е. ребрами одинакового веса. Имеем $d \in A$.

• $m = 1$. В этом случае W содержит некоторую вершину e из K.

Если $a \in W$, то $e = c$, иначе в графе $G_{K\cup\{a\}}$ будет больше одного отделимого множества, что противоречит лемме 3 (отметим, что для применения этой леммы используем условие $\chi \geq 4$). Таким образом, $W = \{a,c,d\}$, и легко видеть, что $d \in A$.

Если $a \notin W$, то $W = \{d,e\}$. Если $e = c$, то очевидно, что $d \in A$. Если $e \in K\backslash\{c\}$, то $E(a,d) = E(a,e)$, т. е. вершина a соединена с d ребром того же веса, что и с вершинами из $K\backslash\{c\}$.

• $m = \chi-1$. Отделимое дополнение до W в графе $G_{K\cup\{a,d\}}$ есть пара $\{a,e\}$, для некоторого e из K. Как и в предыдущем случае, видим, что $e = c$. Следовательно, a соединена с d ребром того же веса, что и со всеми вершинами из $K\backslash\{c\}$.

Утверждение $(*)$ доказано.

Покажем, что каждая вершина из A соединена со всеми вершинами из B ребрами одинакового веса. Для вершины a это верно по утверждению $(*)$. Но любая другая вершина f из A соединена со всеми вершинами графа $K\backslash\{c\}$ ребрами одинакового веса и образует с вершиной c отделимое множество в графе $K \cup \{f\}$. Поэтому для нее можно повторить те же рассуждения, что и для вершины a. Так как любая вершина g из B по построению не соединена со всеми вершинами графа $K\backslash\{c\}$ ребрами одинакового веса, вершина f соединена с вершиной g так же (т. е. ребром того же веса), как и с вершинами графа $K\backslash\{c\}$. Поэтому по следствию 2 множество $A \cup \{c\}$ отделимо в графе G и граф G разделим. $\square$

Следствие 4. *Если все подграфы порядков $n-1$ и $n-2$ графа G порядка n разделимы, то и сам граф G разделим.*

Доказательство. Пусть χ — максимальный порядок собственного неразделимого подграфа. По условию $\chi < n-2$. Если $\chi = 3$, то граф G разделим по предложению 1. Если $\chi > 3$, то граф G разделим по предложению 2. $\square$

Чтобы сформулировать основную теорему, при четном q определим семейство графов $G_{n,\gamma}$, $\gamma \in \{0, \ldots, q-1\}$, $n = 2k+1 \geq 5$. Множество вершин графа таково: $\{a_0, a_1, \ldots, a_k, b_1, \ldots, b_k\}$, вершина a_0 изолирована, веса остальных ребер определяются следующим образом:

• для любых l, m от 1 до k ребро $\{a_l, b_m\}$ имеет вес γ, если $l < m$, и вес $\gamma + q/2 \bmod q$, если $l \geq m$;

• для любых различных l, m от 1 до k ребра $\{a_l, a_m\}$ и $\{b_l, b_m\}$ имеют вес γ.

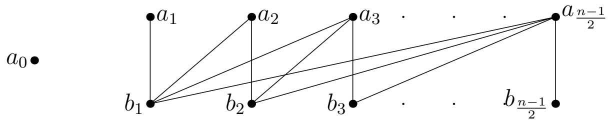

Рис. 4. Граф $G_{n,0}$.

Теорема 1. *Если при удалении любой вершины из графа G порядка n всегда получается разделимый подграф графа G, то либо граф G разделим, либо q четно, n нечетно и граф G изоморфен некоторому свитчингу графа $G_{n,\gamma}$, $\gamma \in \{0, \ldots, q-1\}$.*

Доказательство. Пусть граф G имеет порядок n произвольной четности. Попробуем охарактеризовать все неразделимые графы G порядка n, у которых все подграфы порядка $n-1$ разделимы. Итак, пусть дан граф G порядка $n \geq 5$, обладающий свойствами:

(i) *G — неразделимый граф;*

(ii) *для любой вершины a из G граф $G\backslash\{a\}$ разделимый.*

Будем говорить, что пара вершин графа G *обладает свойством* $\{x,y\}_*$, если существует вершина z такая, что $\{x,y\}$ — единственное (с точностью до дополнения) нетривиальное отделимое множество в графе $G\backslash\{z\}$. Если такая вершина z известна, будем также обозначать это свойство через $\{x,y\}_z$. По лемме 3 ($D = G\backslash\{z\}$) из свойства $\{x,y\}_z$ следует, что графы $G\backslash\{z,x\}$ и $G\backslash\{z,y\}$ неразделимы.

Пусть P — множество всех пар $\{x,y\}$, обладающих свойством $\{x,y\}_*$. Его можно построить, рассмотрев все подграфы порядка $n-1$: если некоторая пара вершин является единственным отделимым множеством в одном из них, то эта пара принадлежит P.

Рассмотрим несколько свойств множества P и входящих в него пар.

(iii) *Множество P непусто.* Это следует из следствия 4 и свойств (i) и (ii).

(iv) *Если для некоторой пары вершин $\{a, b\}$ выполняются соотношения $\{a, b\}_{c_1}$ и $\{a, b\}_{c_2}$, то $c_1 = c_2$.* Действительно, пусть $\{a, b\}$ — отделимое множество в графах $G\backslash\{c_1\}$ и $G\backslash\{c_2\}$. Изолируем некоторую вершину o, отличную от a, b, c_1, c_2. Все вершины графа $G\backslash\{c_1\}$ соединены с парой $\{a, b\}$ ребрами одинакового веса по следствию 1; то же верно для графа $G\backslash\{c_2\}$. По следствию 2 пара $\{a, b\}$ отделима в графе G, что противоречит свойству (i).

(v) *Любая вершина a графа G встречается ровно в двух парах множества P либо не встречается совсем.* Действительно, из соотношения $\{a, b\}_c$ следует неразделимость графа $G\backslash\{a, c\}$. С другой стороны, из неразделимости графа $G\backslash\{a, c\}$ по лемме 3 вытекает $\{a, b\}_c$ для некоторого b, поскольку граф $G\backslash\{c\}$ разделим (свойство (ii)). По лемме 4 в графе $G\backslash\{a\}$ ровно два неразделимых подграфа: $G\backslash\{a, c\}$ и $G\backslash\{a, c'\}$ для некоторых c и c'. Отсюда следует, что $\{a, b\}_c$ и $\{a, b'\}_{c'}$ для некоторых b и b' и другой пары из P, содержащей a, нет.

(vi) *Если $\{a, b\}_c$, то $\{c, d\}_a$ и $\{c, e\}_b$ для некоторых d и e, причем $a \neq e \neq d \neq b$.* Действительно, граф $G\backslash\{a, c\}$ неразделим, а граф $G\backslash\{a\}$ разделим, следовательно, для некоторой вершины d пара $\{c, d\}$ отделима в графе $G\backslash\{a\}$. При этом $d \neq b$, иначе все вершины множества $V\backslash\{a, b, c\}$ (считая одну из них изолированной) соединены с парами вершин $\{a, b\}$ и $\{b, c\}$ ребрами одинакового веса и, значит, множество $\{a, b, c\}$ отделимо, что противоречит свойству (i). Аналогично в графе $G\backslash\{b\}$ отделимым является множество $\{c, e\}$ для некоторой вершины e, отличной от a. Из (iv) следует, что $e \neq d$.

Перебирая пары из P приведенным ниже алгоритмом, построим два множества вершин A, B. Выберем произвольную пару вершин $\{a_0, a_1\}$ из P. Изолируем вершину a_0, поместим a_1 в A. Вершину b_1 такую, что $\{a_0, a_1\}_{b_1}$, поместим в множество B. Тогда согласно (vi) в графе $G\backslash\{a_1\}$ отделимым множеством будет $\{b_1, b_2\}$ для некоторой вершины b_2. Помещаем вершину b_2 в множество B. Далее, в графе $G\backslash\{b_2\}$ отделимым множеством будет пара $\{a_1, a_2\}$ для некоторой вершины a_2, которую включим в A. Дальше продолжаем аналогично до тех пор, пока не окажется, что очередная вершина уже была рассмотрена ранее, т. е. принадлежит $\{a_0\} \cup A \cup B$. Так как каждая рассматриваемая вершина содержится ровно в двух парах из P, этой вершиной может быть только a_0, т. е. для некоторого k верно либо $\{a_{k-1}, a_0\}_{b_k}$ (в этом случае также выполнено $\{b_k, b_1\}_{a_0}$ согласно (v)), либо $\{b_k, a_0\}_{a_k}$ (и $\{a_k, b_1\}_{a_0}$).

Покажем, что первый из этих двух случаев приводит к противоречию. Выполнены следующие соотношения: $\{b_2, b_3\}_{a_2}, \ldots, \{b_{k-1}, b_k\}_{a_{k-1}}$, следовательно, ребра $\{b_1, b_2\}, \ldots, \{b_1, b_k\}$ имеют одинаковый вес. Аналогично ребра $\{b_k, b_{k-1}\}$, $\ldots, \{b_k, b_1\}$ имеют один, тот же самый, вес. В графе $G\backslash\{a_0\}$ отделимым множеством будет пара $\{b_1, b_k\}$. Поскольку $E(b_1, b) = E(b_k, b)$ при $b = b_2$, то же равенство верно для любого b из $V\backslash\{a_0, b_1, b_k\}$. Следовательно, пара $\{b_1, b_k\}$ отделима в G, что противоречит свойству (i).

Рассмотрим второй случай. Докажем, что множество $\{a_0\} \cup A \cup B$ содержит все вершины графа G. Предположим, что это не так. Возьмем произвольную вершину a не из $\{a_0\} \cup A \cup B$. Выполнены следующие соотношения: $\{b_1, b_2\}_{a_1}$, $\ldots, \{b_{k-1}, b_k\}_{a_{k-1}}$, стало быть, ребра $\{a, b_1\}, \ldots, \{a, b_k\}$ имеют одинаковый вес. Аналогично в силу соотношений $\{a_1, a_2\}_{b_2}, \ldots, \{a_{k-1}, a_k\}_{b_k}$ ребра $\{a, a_1\}, \ldots,$

$\{a, a_k\}$ имеют один вес. Из соотношений $\{a_0, a_1\}_{b_1}$ и $\{b_k, a_0\}_{a_k}$ получаем, что $E(a_1, a) = E(a_1, b_k) = E(b_k, a)$ Тем самым вершина a соединена со всеми вершинами множества $A \cup B$ ребрами одинакового веса. В силу произвольности вершины a, это верно для всех остальных вершин, не лежащих в $A \cup B \cup a_0$. Значит, все эти вершины вместе с вершиной a_0 по следствию 2 образуют отделимое множество в графе G, что противоречит его неразделимости.

Итак, $n = 2k+1$ нечетно, множество вершин состоит из изолированной вершины a_0 и подмножеств $A = \{a_1, \ldots, a_k\}$ и $B = \{b_1, \ldots, b_k\}$. Вершины связаны следующими соотношениями:

$$\{a_0, a_1\}_{b_1}, \ldots, \{a_{k-1}, a_k\}_{b_k}, \{a_k, b_1\}_{a_0}, \{b_1, b_2\}_{a_1}, \ldots, \{b_{k-1}, b_k\}_{a_{k-1}}, \{b_k, a_0\}_{a_k}.$$

Установим серию равенств для весов между ребрами графа. Для любого $i \in \{1, \ldots, k\}$ верны следующие равенства:

$$E(a_i, a_j) = E(a_i, a_{j+1}) \quad \forall j \in \{i+1, \ldots, k-1\}, \tag{1}$$

$$E(a_i, a_l) = E(a_i, a_{l-1}) \quad \forall l \in \{2, \ldots, i-1\}, \tag{2}$$

$$E(b_i, b_j) = E(b_i, b_{j+1}) \quad \forall j \in \{i+1, \ldots, k-1\}, \tag{3}$$

$$E(b_i, b_l) = E(b_i, b_{l-1}) \quad \forall l \in \{2, \ldots, i-1\}, \tag{4}$$

$$E(a_i, b_j) = E(a_i, b_{j+1}) \quad \forall j \in \{i+1, \ldots, k-1\}, \tag{5}$$

$$E(a_i, b_l) = E(a_i, b_{l-1}) \quad \forall l \in \{2, \ldots, i\}, \tag{6}$$

$$E(b_i, a_j) = E(b_i, a_{j+1}) \quad \forall j \in \{i, \ldots, k-1\}, \tag{7}$$

$$E(b_i, a_l) = E(b_i, a_{l-1}) \quad \forall l \in \{2, \ldots, i-1\}, \tag{8}$$

$$E(a_1, a_k) = E(a_1, b_k) \neq E(a_1, b_1), \tag{9}$$

$$E(b_k, a_1) = E(b_k, b_1) \neq E(b_k, a_k). \tag{10}$$

Действительно, соотношения (1), (2), (7), (8) следуют из $\{a_{m-1}, a_m\}_{b_m}$, $m \in \{2, \ldots, k\}$: в графе $G \backslash \{b_m\}$ дополнение до отделимой пары $\{a_{m-1}, a_m\}$ содержит изолированную вершину a_0, а значит, по следствию 1 для любой вершины c этого дополнения верно $E(c, a_{m-1}) = E(c, a_m)$. Аналогично соотношения (3)–(6) следуют из $\{b_{m-1}, b_m\}_{a_{m-1}}$. Соотношение (9) (аналогично (10)) вытекает по следствию 1 из $\{a_0, a_1\}_{b_1}$ (соответственно $\{b_k, a_0\}_{a_k}$), поскольку в графе $G \backslash \{b_1\}$ пара $\{a_0, a_1\}$ отделимая, но в графе G она уже не отделима.

Из равенств (1) и (2) (соответственно (3) и (4)) легко заключить, что все ребра, соединяющие вершины из множества A (B) между собой, имеют один и тот же вес, скажем α (соответственно β). Из равенств (5) и (8) следует, что все ребра $\{a_i, b_j\}$, где $1 \leq i < j \leq k$, имеют один и тот же вес, скажем γ. Аналогично из (6) и (7) вытекает, что все ребра $\{a_i, b_j\}$, где $1 \leq j \leq i \leq k$, имеют один и тот же вес, скажем δ. Более того, из (9) и (10) видим, что $\alpha = \gamma = \beta \neq \delta$.

Остается показать, что $\delta = \gamma + q/2$. В графе $G \backslash \{a_0\}$ отделима пара $\{a_k, b_1\}$. По лемме 2 и в соответствии с ее обозначениями $\{a_k\} = W_a$, $\{b_1\} = W_b$, $A \backslash \{a_k\} = V_{a'}$, $B \backslash \{b_1\} = V_{b'}$, причем $a + a' = b + b' = \gamma$ и $a + b' = b + a' = \delta$. Отсюда видно, что $2\gamma = 2\delta$. Поскольку $\gamma \neq \delta$, имеем $\delta = \gamma + q/2$, где q четно. $\square$

Для полноты картины остается показать, что сам граф $G_{n,\gamma}$ действительно является исключением.

Предложение 3. *Граф $G_{n,\gamma}$ ($n \geq 5$ нечетно, q четно) неразделим, и все его подграфы порядка $n-1$ разделимы.*

Доказательство. Предположим, что $G_{n,\gamma} = (V, E)$ разделим. Пусть W — нетривиальное отделимое множество, содержащее a_0. Вершины a_k и b_1 не могут одновременно принадлежать $V \backslash W$ (иначе согласно следствию 1 в W не может быть никакой вершины, кроме a_0). Если $a_k \in W$, то либо $\{a_1, \ldots, a_{k-1}\}$, либо $\{b_1, \ldots, b_k\}$ полностью содержится в W (иначе имеем противоречие со следствием 1). В первом случае $V \backslash W$ содержит некоторые b_i, b_j, $i < j$, и вершина a_i из W противоречит следствию 1. Во втором случае $V \backslash W$ содержит некоторые a_i, a_j, $i < j$, и вершина b_j из W противоречит следствию 1. Случай $b_1 \in W$ аналогичен. Полученное противоречие доказывает неразделимость графа $G_{n,\gamma}$.

Остается заметить, что пара $\{a_k, b_1\}$ отделима в $G \backslash \{a_0\}$, пара $\{b_i, b_{i+1}\}$ отделима в $G \backslash \{a_i\}$, $i = 1, \ldots, k-1$, пара $\{b_k, a_0\}$ отделима в $G \backslash \{a_k\}$, пара $\{a_{i-1}, a_i\}$ отделима в $G \backslash \{b_i\}$, $i = 1, \ldots, k$. $\square$

3. Функции и квазигруппы

В этом разделе кратко обсудим связь разделимости графов с аналогичным свойством для функций над $\mathbb{Z}_q$ и для n-арных квазигрупп.

Подграфам графа соответствуют так называемые ретракты n-арных квазигрупп и подфункции функций, и то и другое получается фиксацией некоторых аргументов. В терминах ретрактов и подфункций для n-арных квазигрупп и булевых функций верны утверждения, аналогичные следствию 4 и предложению 3 (последнее известно для n-арных квазигрупп, только если порядок кратен 4). С учетом того, что по графу при помощи квадратичного многочлена можно построить функцию и затем n-арную квазигруппу порядка q^2, следствие 4 является, вообще говоря, следствием соответствующего утверждения для квазигрупп [9, 2] (заметим, что приведенное в настоящей работе для полноты доказательство этого следствия на порядок проще доказательства для квазигрупп), а из предложения 3, наоборот, следует существование аналогичного примера среди n-арных квазигрупп порядка 4 [3].

3.1. Частичные функции. Пусть q — простое число. *Частичной функцией* будем называть функцию $f^{[a]} : \Omega_a \to \{0, \ldots, q-1\}$ над $\mathbb{Z}_q$, заданную на наборах значений аргументов, сумма которых равна некоторой константе a:

$$\Omega_a = \left\{ (x_1, \ldots, x_n, x_0) \in \{0, \ldots, q-1\}^{n+1} \mid \sum_{i=0}^{n} x_i = a \right\}.$$

Заметим, что частичную функцию от $n+1$ аргументов можно интерпретировать как обычную (везде определенную) функцию от первых n аргументов. Частичную функцию $f^{[a]}$ будем называть *расширением*, или *a-расширением*, функции f, если

$$f^{[a]}(x_1, \ldots, x_n, x_0) = f(x_1, \ldots, x_n)$$

для любых $x_1, \ldots, x_n$ и $x_0 = a - \sum\limits_{1}^{n} x_i$. Далее обозначение $f^{[a]}$ будет автоматически подразумевать, что $f^{[a]}$ есть a-расширение функции f.

Пусть W — некоторое подмножество множества номеров аргументов $\{1, \ldots, n, 0\}$. Частичную функцию $f^{[a]}$ от $n+1$ аргументов назовем *W-разделимой*, если

$$f^{[a]}(x_1, \ldots, x_n, x_0) = f'(x_W) + f''(x_U)$$

для некоторых (везде определенных) функций f' и f'' от $|W|$ и $|U|$ аргументов соответственно, где $U = \{1, \dots, n, 0\} \backslash W$, и $x_C = (x_{c_1}, \dots, x_{c_k})$ для $C = \{c_1, \dots, c_k\}$, $c_1 < \dots < c_k$. Частичную функцию от $n+1$ аргументов назовем *разделимой*, если она W-разделима для некоторого W мощности от 2 до $n-1$ включительно (ограничение на мощность достаточно естественно: в этом случае функции в разложении могут быть заданы меньшим числом значений в точках, чем сама частичная функция). *Степенью* частичной функции назовем минимальную степень многочлена (над полем $\mathbb{Z}_q$), с помощью которого она может быть представлена. Под термином «квадратичный» будем подразумевать «степени не больше двух». *Графом квадратичного многочлена* назовем граф на множестве номеров аргументов $\{1, \dots, n, 0\}$, у которого вес ребра, соединяющего две различные вершины, равен коэффициенту в многочлене при произведении соответствующих переменных (таким образом, две вершины смежны тогда и только тогда, когда произведение соответствующих переменных входит в приведенный многочлен).

Лемма 5. *Множество графов, соответствующих представлениям данной квадратичной частичной функции в виде квадратичного многочлена, образует свитчинговый класс.*

Доказательство. Любая (в частности, квадратичная) частичная функция $f^{[a]}$ от $n+1$ аргументов, будучи функцией от первых n своих аргументов, единственным образом представима в виде

$$f^{[a]}(x_1, \dots, x_n, x_0) = \pi(x_1, \dots, x_n),$$

где π — многочлен (поскольку в поле $\mathbb{Z}_q$ имеет место тождество $x^q \equiv x$, степень каждой переменной в мономах такого многочлена ограничена величиной $q-1$).

Любой многочлен ρ от $n+1$ переменных $x_1, \dots, x_n, x_0$ однозначно представим в виде $\tau(x_1, \dots, x_n) + (x_1 + \dots + x_n + x_0 - a)\lambda(x_1, \dots, x_n)$, где τ и λ — многочлены от $x_1, \dots, x_n$, причем если многочлен ρ квадратичный, то τ квадратичный и λ аффинный (степени не больше 1). Поскольку $x_1 + \dots + x_n + x_0 = a$ везде на области определения частичной функции $f^{[a]}$, многочлен τ совпадает у всех многочленов, представляющих $f^{[a]}$. Легко убедиться, что добавление $(x_1 + \dots + x_n + x_0 - a)\lambda(x_1, \dots, x_n)$ с аффинным λ приводит к свитчингу соответствующего графа. Отсюда следует утверждение леммы. $\square$

Предложение 4. *Квадратичная частичная функция $f^{[a]}$ является W-разделимой тогда и только тогда, когда множество вершин W отделимо в графах квадратичных многочленов, представляющих эту функцию.*

Доказательство. С учетом леммы 5 W-разделимость функции, представимой квадратичным многочленом, следует по определению из отделимости множества W в соответствующем графе.

Для доказательства обратного с учетом леммы 5 достаточно показать, что для разделимой квадратичной частичной функции $f^{[a]}$ элементы ее некоторого разложения f' и f'' из определения разделимости также квадратичны. Пусть

$$f^{[a]}(y_1, \dots, y_k, z_1, \dots, z_m) = g'(y_1, \dots, y_m) + g''(z_1, \dots, z_m) \tag{11}$$

для любых значений аргументов, удовлетворяющих тождеству $y_1 + \dots + y_k + z_1 + \dots + z_m = a$. Подставляя нули в качестве значений некоторых аргументов, получаем

$$f^{[a]}\left(y_1, \dots, y_k, a - \sum_{i=1}^{k} y_i, 0, \dots, 0\right) = g'(y_1, \dots, y_m) + g''\left(a - \sum_{i=1}^{k} y_i, 0, \dots, 0\right), \tag{12}$$

$$f^{[a]}\left(a-\sum_{i=1}^{m} z_i, 0, \dots, 0, z_1, \dots, z_m\right) = g'\left(a-\sum_{i=1}^{m} z_i, 0, \dots, 0\right) + g''(z_1, \dots, z_m), \quad (13)$$

$$f^{[a]}(t, 0, \dots, 0, a-t, 0, \dots, 0) = g'(t, 0, \dots, 0) + g''(a-t, 0, \dots, 0), \quad (14)$$

Из тождеств (11)–(14) легко получить разложение

$$f^{[a]}(y_1, \dots, y_k, z_1, \dots, z_m) = f\left(y_1, \dots, y_k, a - \sum_{i=1}^{k} y_i, 0, \dots, 0\right)$$
$$+ f\left(a - \sum_{i=1}^{m} z_i, 0, \dots, 0, z_1, \dots, z_m\right) - f\left(a - \sum_{i=1}^{m} z_i, 0, \dots, 0, a - \sum_{i=1}^{k} y_i, 0, \dots, 0\right).$$

Поскольку $a - \sum_1^m z_i = \sum_1^k y_i$, последнее слагаемое можно отнести как к первой, так и ко второй части разложения. В итоге имеем искомое разложение на квадратичные функции. $\square$

Если вместо одного или более аргументов частичной функции подставить константы, получим *подфункции* данной частичной функции. Очевидно, подфункции сами являются частичными функциями. Например, если у частичной функции $f^{[a]}$ зафиксировать значение одного из аргументов значением b, то получится некоторая частичная функция $g^{[a-b]}$.

Легко понять, что графы, соответствующие подфункции квадратичной частичной функции $f^{[a]}$, получаются из графов, соответствующих $f^{[a]}$, удалением вершин — номеров фиксируемых аргументов. Из предложения 4 и теоремы 1 можем заключить следующее.

Следствие 5. *Пусть q — нечетное простое число. Если из квадратичной частичной функции $f^{[a]}$ фиксацией любого аргумента получается разделимая частичная функция, то и сама $f^{[a]}$ разделима. Другими словами, из любой неразделимой квадратичной частичной функции фиксацией некоторой переменной можно получить неразделимую подфункцию.*

3.2. n-Арные квазигруппы. Пусть Σ — некоторое множество. n-Арная операция $Q : \Sigma^n \to \Sigma$ называется *n-арной квазигруппой* (далее также просто *квазигруппой*) порядка $|\Sigma|$, если в уравнении $x_0 = Q(x_1, \dots, x_n)$ значения любых n переменных однозначно задают значение оставшейся переменной. (Строго говоря, *n-арной квазигруппой* называется система (Σ, Q) из носителя и операции, наше определение — общепринятое упрощение терминологии.) Из определения следует, что n-арная квазигруппа обратима в каждой позиции; в случае конечного порядка это свойство можно взять за определение. Квазигруппу, обратную к Q в i-м месте, будем обозначать через $Q^{(i)}$. Таким образом, для n-арной квазигруппы Q соотношения $x_0 = Q(x_1, \dots, x_n)$ и $x_i = Q^{(i)}(x_1, \dots, x_{i-1}, x_0, x_{i+1}, \dots, x_n)$ эквивалентны. Квазигруппу арности $n-k$, полученную из n-арной квазигруппы Q или ее обращения $Q^{(i)}$, $i \in \{1, \dots, n\}$, подстановкой констант на место некоторых k аргументов, называют *ретрактом* квазигруппы Q.

Пусть W — некоторый набор номеров аргументов n-арной квазигруппы Q. Квазигруппу Q назовем *W-разделимой*, если $Q(\bar{x}) = G(\bar{x}', H(\bar{x}''))$ для некоторых $|W|$-арной квазигруппы H и $(n - |W| + 1)$-арной квазигруппы G, где

$\bar{x}''$ — набор переменных из $\bar{x}$ с номерами из W, $\bar{x}'$ состоит из всех остальных переменных $\bar{x}$. Другими словами, уравнение $x_0 = Q(\bar{x})$ эквивалентно $G^{(n-|W|+1)}(\bar{x}', x_0) = H(\bar{x}'')$, поэтому W-разделимую n-арную квазигруппу будем считать также $\{1, \dots, n, 0\} \backslash W$-разделимой. Квазигруппу Q назовем *разделимой*, если она W-разделима для некоторого W, где $2 \le |W| \le n$ (это неравенство эквивалентно тому, что квазигруппы, входящие в соответствующую суперпозицию, имеют меньшую арность).

Рассмотрим в качестве Σ множество пар $\{[a, b] | a, b \in \mathbb{Z}_q\}$. Для произвольной функции $f : \mathbb{Z}_q^n \to \mathbb{Z}_q$ и константы $a \in \mathbb{Z}_q$ определим n-арную квазигруппу Q_f порядка q^2:

$$Q_{f,a}([x_1, y_1], \dots, [x_n, y_n]) = \left[-\sum_{i=1}^{n} x_i + a, -\sum_{i=1}^{n} y_i + f(x_1, \dots, x_n) \right].$$

Предложение 5. *n-Арная квазигруппа $Q_{f,a}$ является W-разделимой тогда и только тогда, когда W-разделима частичная функция $f^{[0]}$.*

Доказательство. Без потери общности положим $W = \{k, \dots, n\}$. Пусть $f^{[0]}$ является W-разделимой. Тогда

$$f = f'\left(x_1, \dots, x_{k-1}, -\sum_{1}^{n} x_i \right) + f''(x_k, \dots, x_n)$$

для некоторых (везде определенных) функций f' и f''. Определим

$$g'(x_1, \dots, x_{k-1}, t) = f'(x_1, \dots, x_{k-1}, -x_1 - \dots - x_{k-1} - t).$$

Нетрудно проверить, что

$$\begin{aligned} &Q_{g',a}([x_1, y_1], \dots, [x_{k-1}, y_{k-1}], -Q_{f'',0}([x_k, y_k], \dots, [x_n, y_n])) \\ &= \left[-\sum_{i=1}^{k-1} x_i - \sum_{i=k}^{n} x_i + a, -\sum_{i=1}^{k-1} y_i - \sum_{i=k}^{n} y_i + f''(x_k, \dots, x_n) + g'\left(x_1, \dots, x_{k-1}, \sum_{i=k}^{n} x_i \right) \right] \\ &\qquad = Q_{f,a}([x_1, y_1], \dots, [x_n, y_n]). \end{aligned}$$

Таким образом, n-арная квазигруппа $Q_{f,a}$ также W-разделима.

Предположим, что $Q_{f,a}$ W-разделима. Рассмотрим функцию

$$\begin{aligned} g(x_1, \dots, x_n) = f&\left(x_1, \dots, x_{k-1}, \sum_{i=k}^{n} x_i, 0, \dots, 0 \right) \\ &+ f(0, \dots, 0, x_k, \dots, x_n) - f\left(0, \dots, 0, \sum_{i=k}^{n} x_i, 0, \dots, 0 \right). \end{aligned}$$

Расширение $g^{[0]}$ этой функции W-разделимо. Действительно, для $x_1 + \dots + x_n + x_0 = 0$ имеем

$$\begin{aligned} g^{[0]}(x_1, \dots, x_n, x_0) = f&\left(x_1, \dots, x_{k-1}, -\sum_{i=0}^{k-1} x_i, 0, \dots, 0 \right) \\ &+ f(0, \dots, 0, x_k, \dots, x_n) - f\left(0, \dots, 0, \sum_{i=k}^{n} x_i, 0, \dots, 0 \right). \end{aligned}$$

Согласно первой части доказательства n-арная квазигруппа $Q_{g,a}$ также W-разделима. Кроме того,

$$Q_{f,a}(z_1,\dots,z_k,[0,0],\dots,[0,0]) = Q_{g,a}(z_1,\dots,z_k,[0,0],\dots,[0,0]),$$

$$Q_{f,a}([0,0],\dots,[0,0],z_k,\dots,z_n) = Q_{g,a}([0,0],\dots,[0,0],z_k,\dots,z_n)$$

для всех значений $z_1, \dots , z_n$. Согласно [10, предложение 12] две W-разделимые n-арные квазигруппы, для которых указанные ретракты совпадают, сами обязаны совпадать. Как следствие, совпадают функции f и g, и $f^{[0]}$ также W-разделима. □

Осталось связать разделимость подфункций с разделимостью ретрактов. Для этого понадобятся следующие два утверждения.

Лемма 6. *Пусть $(n-1)$-арная квазигруппа F получается из $Q_{f,a}$ подстановкой константы $[b,c]$ вместо i-го аргумента. Тогда $F = Q_{g,a-b}$, где функция g получается из f подстановкой константы b на место i-го аргумента и прибавлением $-c$ к значению.*

Ясно, что прибавление константы к значению функции никак не влияет на ее разделимость. Поэтому разделимость ретракта F эквивалентна разделимости соответствующей подфункции расширения функции f. Однако таким образом представимы не все $(n-1)$-арные ретракты.

Лемма 7. *Пусть функции f и g связаны тождеством*

$$f^{[a]}(x_1,\dots,x_{i-1},x_i,x_{i+1},\dots,x_n,x_0) = g^{[a]}(x_1,\dots,x_{i-1},x_0,x_{i+1},\dots,x_n,x_i)$$

для некоторого i от 1 до n. Тогда n-арные квазигруппы $Q_{f,a}$ и $Q_{g,a}$ являются обращением друг друга в i-м месте, т. е. $Q^{(i)}_{f,a} = Q_{g,a}$.

Доказательство. Для простоты обозначений рассмотрим только случай $i = 1$. По определению $Q_{f,a}$ уравнение $[x_0, y_0] = Q_{f,a}([x_1, y_1], \dots, [x_n, y_n])$ эквивалентно системе

$$\begin{cases} -x_0 - x_1 - \dots - x_n + a = 0, \\ -y_0 - y_1 - \dots - y_n + f^{[a]}(x_1,\dots,x_n,x_0) = 0. \end{cases}$$

По определению обращения квазигруппы в первом аргументе той же системе эквивалентно и уравнение $[x_1, y_1] = Q^{(1)}_{f,a}([x_0, y_0], [x_2, y_2], \dots, [x_n, y_n])$. Но эта же система эквивалентна уравнению $[x_1, y_1] = Q_{g,a}([x_0, y_0], [x_2, y_2], \dots, [x_n, y_n])$. □

Таким образом, взятие обращения квазигруппы $Q_{f,a}$ соответствует перестановке двух аргументов частичной функции $f^{[a]}$. Как следствие, разделимость ретрактов квазигруппы $Q_{f,a}$ эквивалентна разделимости соответствующих подфункций частичной функции $f^{[a]}$.

Следствие 6. *Пусть $q > 2$ простое и $f : \mathbb{Z}_q^n \to \mathbb{Z}_q$ — квадратичная функция. Если все $(n-1)$-арные ретракты n-арной квазигруппы $Q_{f,a}$ порядка q^2 разделимы, то и сама квазигруппа разделима.*

ЛИТЕРАТУРА

1. *Krotov D. S., Potapov V. N.* On connection between reducibility of an n-ary quasigroup and that of its retracts // Discrete Math. 2011. V. 311, N 1. P. 58–66.
2. *Krotov D. S., Potapov V. N.* n-Ary quasigroups of order 4 // SIAM J. Discrete Math. 2009. V. 23, N 2. P. 561–570.

3. *Krotov D. S.* On irreducible n-ary quasigroups with reducible retracts // Eur. J. Comb. 2008. V. 29, N 2. P. 507–513.

4. *Van Lint J. H., Seidel J. J.* Equilateral point sets in elliptic geometry // Nederl. Akad. Wet., Proc., Ser. A, Indag. Math. 1966. V. 69. P. 335–348.

5. *Spence E.* Two-graphs // CRC Handbook combinatorial designs. Sec. Edition. Boca Raton; London; New York: Chapman & Yall/CRC, 2006. P. 875–882.

6. *Кротов Д. С.* О связи свитчинговой разделимости графа и его подграфов // Дискрет. анализ и исслед. операций. 2010. Т. 17, № 2. С. 46–56.

7. *Bespalov E. A.* On switching nonseparable graphs with switching separable subgraphs // Сиб. электрон. мат. изв. 2014. Т. 11. С. 988–998.

8. *Zaslavsky T.* Associativity in multiary quasigroups: the way of biased expansions // Aequationes Math. 2012. V. 83, N 1–2. P. 1–66.

9. *Krotov D. S.* On reducibility of n-ary quasigroups // Discrete Math. 2008. V. 308, N 22. P. 5289–5297.

10. *Потапов В. Н., Кротов Д. С.* Асимптотика числа n-квазигрупп порядка 4 // Сиб. мат. журн. 2006. Т. 47, № 4. С. 873–887.

Статья поступила 2 декабря 2014 г.

Беспалов Евгений Андреевич, Кротов Денис Станиславович
Институт математики им. С. Л. Соболева СО РАН,
пр. Академика Коптюга, 4, Новосибирск 630090
`bespalovpes@mail.ru`, `krotov@math.nsc.ru`