Дискретная математика

УДК 519.72:004.056.55

УСЛОВИЯ ВЫДЕЛИМОСТИ ВЕСОВЫХ КОЭФФИЦИЕНТОВ ИЗ СУММ С ЧЛЕНАМИ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ДВУХ ВИДОВ

А. И. Никонов

Самарский государственный технический университет,
Россия, 443100, Самара, ул. Молодогвардейская, 244.

E-mail: nikonovai@mail.ru

Описано представление условий выделимости целочисленных весовых коэффициентов из последовательностей, образующих основу шифрования. Рассмотрены два вида таких последовательностей: геометрическая прогрессия и последовательность с одинаковыми натуральными степенями натуральных чисел. Эти последовательности — знакопостоянные или знакочередующиеся — используются при формировании относительных суммарных остатков, выражение каждого из которых помещается в центральную часть двойного неравенства. Определение условий выделимости при наличии остаточной последовательности — геометрической прогрессии произведено в отношении её знаменателя, а условия выделимости при наличии остаточной последовательности, содержащей одинаковые степени натуральных чисел, найдены с помощью введённой сопутствующей функции применительно к целочисленным аргументам формируемых величин относительных суммарных остатков.

Ключевые слова: *условия выделимости, весовые коэффициенты, свободные множители, суммарный остаток, относительный суммарный остаток, внешний член.*

Необходимость в обоснованности процессов шифрования — расшифрования конфиденциальных текстов с алгебраическими преобразованиями последовательно получаемых суммарных величин, слагаемые которых содержат свободные и весовые сомножители [1], требует соблюдения условий выделимости данных весовых сомножителей — целочисленных весовых коэффициентов.

Указанные алгебраические преобразования совершаются с применением следующего соотношения:

$$\forall g \in I_{p-1} = 1, \ldots, p-1 :$$
$$\left(\Phi - \sum_{\gamma=1}^{g} b_{p-\gamma+2} c_{p-\gamma+2}\right) / c_{\Delta+1} = b_{\Delta+1} + \varphi(\Delta);$$

$p \in \mathbb{N}\backslash\{1\}$ — общее количество весовых коэффициентов; g — индекс шага, выполняемого в процессе последовательного нахождения этих коэффициентов;

Александр Иванович Никонов (д.т.н., проф.), профессор, каф. электронных систем и информационной безопасности.

$\Phi = \Phi(p)$ — основная сумма, то есть число, присылаемое адресату-дешифровальщику; b, c — символы компонентов слагаемых — соответственно весовых коэффициентов и свободных множителей, произведения которых, имеющие вид $b_l c_l$, $l = 1, \ldots, p$, образуют члены основной последовательности, причём

$$\begin{aligned} &b_l \in \mathbb{N} \cup \{0\}, \quad \exists b_l \neq 0, \quad c_l \in \mathbb{R}_+ \backslash \{0\}; \\ &\varphi(\Delta) = \Phi(\Delta)/c_{\Delta+1}; \end{aligned} \tag{1}$$

величина $\varphi(\Delta)$ называется относительным суммарным остатком (ОСО), содержащим, в свою очередь, компонент — безотносительный суммарный остаток

$$\Phi(\Delta) = \sum_{l=1}^{\Delta} b_l c_l;$$

$\Delta = p - g$ — целочисленный аргумент последовательно формируемой величины $\varphi(\Delta)$; $\Delta \in I_{p-1}$; величину $c_{\Delta+1}$ назовём внешним (по отношению к остаточной последовательности $b_l c_l$, $l = 1, \ldots, \Delta$) членом. Последовательность c_l, $l = 1, \ldots, p$, или c_l, $l = 1, \ldots, \Delta$, называется соответственно основной или остаточной последовательностью свободных множителей.

Рассматриваемый ОСО по условию выделимости должен оставаться внутри интервала допустимых отклонений от целочисленных значений весовых коэффициентов. Его рамки задаются в общем случае слева путём указания числа $\delta_- \leqslant 0$, а справа — числа $\delta_+ \geqslant 0$. Ни одного $g \in I_{p-1}$, для которого соответствующее условие выделимости не выполняется, быть не должно.

Целью настоящей работы является нахождение условий выделимости как для знакопостоянных, так и для знакочередующихся слагаемых из основной суммы: членов геометрической прогрессии, а также членов цепочки одинаковых натуральных степеней натуральных чисел. Введём несколько типовых условий выделимости:

1) $0 < \delta_-, \delta_+ < 1$; интервал допустимых отклонений — двузначный, а его протяжённость может превышать единицу;

2а) $0 < \delta_- + \delta_+ < 1$; интервал допустимых отклонений — двузначный, а его протяжённость может быть уменьшена сравнительно с единицей;

2б) $0 \leqslant \delta_+ < 1$, $\delta_- = 0$ или $0 \leqslant \delta_- < 1$, $\delta_+ = 0$; значения точечных элементов интервала допустимых отклонений имеют одинаковый знак или нулевое значение, а протяжённость этого интервала снижена сравнительно с единицей.

Если та или иная рассматриваемая нами последовательность подходит для реализации типовых условий выделимости 2б, то её следует признать также подходящей и для любого условия выделимости, относящегося к типам 1, 2а. Границы интервала допустимых отклонений для условия выделимости могут быть установлены более или менее удачно в зависимости от степени адекватности их задания возможным значениям, фактически присущим количественному представлению ОСО.

Нахождение условий выделимости будем производить, выявляя характерные свойства ОСО (1), присущие их второму типу. Ниже будут формироваться относительные суммарные остатки с максимальными значениями весовых коэффициентов вида $b_l = b_m > 1$ [1]:

$$\varphi^+(\Delta) = \max_B \varphi(\Delta) = b_m S_\Delta / c_{\Delta+1}; \quad \varphi^+(\Delta),\ S_\Delta / c_{\Delta+1} > 0;$$

$$\varphi^-(\Delta) = \min_B \varphi(\Delta) = b_m S_\Delta / c_{\Delta+1}; \quad \varphi^-(\Delta),\ S_\Delta / c_{\Delta+1} < 0;$$

$$B = \{b_1, \ldots, b_p\}, \quad S_\Delta = \sum_{l=1}^{\Delta} c_l.$$

Здесь величина S_Δ — суммарный остаток, относящийся соответственно к остаточной последовательности свободных множителей $c_l, l = 1, \ldots, \Delta$. Величины $\varphi^+(\Delta)$, $\varphi^-(\Delta)$ образуют множество, элемент которого обозначим через $\operatorname{ex}\varphi(\Delta)$.

Сами же значения суммарных остатков могут быть найдены при использовании в качестве основной последовательности геометрической прогрессии — с помощью известного выражения суммы её членов [2], а при использовании в указанном качестве последовательности равных друг другу натуральных степеней натуральных чисел — с помощью либо непосредственного выражения их суммы, либо известного комбинаторного способа [3, 4].

Заключительный момент в рассмотрении условия выделимости представляется решением двойного неравенства, выражающего это условие; его левая и правая части определяются заданными границами интервала допустимых отклонений, а центральная часть является записью выражения анализируемого ОСО.

Теперь объясним подробнее правила индексации относительных суммарных остатков. Надстрочные индексы ОСО указывают на следующее: первый — на знак данного ОСО; второй, если он окажется необходимым, — на вид используемой основной или остаточной последовательности (г — геометрическая прогрессия, р — последовательность с натуральными равностепенными членами). Подстрочные индексы ОСО указывают на следующее: первый — на характер используемой последовательности (п — знакопостоянная, ч — знакочередующаяся); второй, если он окажется необходимым, — на нечётность либо чётность числа Δ (o — нечётное, e — чётное). Кроме того, положим, что после символа φ указывать в скобках символ Δ не обязательно.

Сделанные нами замечания относятся к относительным суммарным остаткам, соответствующим как знакопостоянным, так и знакочередующимся основным и остаточным последовательностям и соответствующим им суммам, причём объём замечаний достаточен для того, чтобы начать выработку условий выделимости, связанных со знакопостоянными последовательностями.

Получим сперва условие выделимости, использующие остаточную последовательность, которая представляется знакопостоянной геометрической прогрессией

$$c_l = c^{\text{г}}_{\text{пл}} = q^l = (a^m)^l, \quad l = 1, \ldots, \Delta; \tag{2}$$

q — знаменатель прогрессии и её же первый член $a^{\text{г}}_{\text{п1}}$; $a \in \mathbb{R}_+ \backslash \{0\}$, $m \in \mathbb{N}$. Нижний и верхний буквенные индексы величин $c^{\text{г}}_{\text{пл}}$, $a^{\text{г}}_{\text{п1}}$ имеют уже объяснённый смысл: п — знакопостоянная последовательность; г — геометрическая прогрессия.

Первый вариант представления условия выделимости имеет вид двойного неравенства

$$0 \leqslant \varphi^{+\text{г}}_{\text{п}}(\Delta) < \delta_+, \quad \Delta \in \{1, \ldots, p-1\}.$$

Числитель ОСО, располагаемый в центральной части этого неравенства, есть сумма членов геометрической прогрессии, а член $c_{\Delta+1}$ занимает именно внеш-

нее положение относительно прогрессии (2). Следовательно, рассматриваемое условие выделимости может быть выражено как

$$0 \leqslant \varphi_{\text{п}}^{+\text{г}}(\Delta) = \left(b_m^+/(q-1)\right)\left((q^\Delta - 1)/q^\Delta\right) < 1, \quad b_m^+ = b_m/\delta_+.$$

Если положить $q - 1 > 0$, то будем иметь $0 < (q^\Delta - 1)/q^\Delta < 1$. Далее получаем двойное неравенство $0 \leqslant b_m^+/(q-1) < 1$, откуда следует появление требования $q > b_m^+ + 1$. Обеспечение этого требования и позволяет реализовать рассматриваемый первый вариант условия выделимости.

Если положить $q - 1 < 0$, то в рамках такого допущения потребуется, чтобы $0 \leqslant b_m^+(1/q)\left((1/q)^\Delta - 1\right)/\left((1/q) - 1\right) < 1$. Здесь для каждого допустимого значения $g < p$, $p \geqslant 2$, уровень $\varphi_{\text{п}}^{+\text{г}}(\Delta)$ превышает единицу, и поэтому с принятием предположения $q < 1$ рассматриваемый случай условия выделимости следует признать неосуществимым.

Второй вариант задания условия выделимости как $0 \leqslant \delta_- < 1$, $\delta_+ = 0$, которому соответствует первый член геометрической прогрессии $a_{\text{п}1}^{\text{г}} = -q$ и её знаменатель q, имеет следующий конкретизированный вид:

$$-\delta_- < \varphi_{\text{п}}^{-\text{г}}(\Delta) \leqslant 0 \Rightarrow 0 \leqslant -\varphi_{\text{п}}^{-\text{г}}(\Delta) < \delta_-, \quad \Delta \in \{1, \ldots, p-1\}.$$

Тогда первый и второй варианты задания условий выделимости с учётом равнозначности первых членов используемых ими остаточных последовательностей можно объединить следующим образом:

$$0 \leqslant |\operatorname{ex} \varphi_{\text{п}}^{\text{г}}(\Delta)| < \begin{cases} \delta_+ \to \varphi_{\text{п}}^{+\text{г}}(\Delta), \\ \delta_- \to \varphi_{\text{п}}^{-\text{г}}(\Delta). \end{cases}$$

Решение одного или другого варианта этого неравенства при указании в нём одной из величин δ_+ или δ_- соответствует решению, уже полученному нами для представленного выше первого варианта условия выделимости со знакопостоянной геометрической прогрессией.

Условие выделимости, связанное с остаточной знакопостоянной последовательностью равных друг другу натуральных степеней натуральных чисел, может быть получено и проанализировано исходя из следующих соображений.

Применительно к ОСО

$$\varphi_{\text{п}}^{+\text{р}}(\Delta) = b_m \sum_{l=1}^{\Delta} l^\nu/(\Delta+1)^\nu, \tag{3}$$

определённому на множестве $\{\Delta; g = 1, \ldots, p-1\}$ и принимающему положительные значения, построим сопутствующую функцию (её верхний индекс c)

$$\varphi_{\text{п}}^{c}(x) = b_m \sum_{l=1}^{\lfloor x \rfloor} (l+\chi)^\nu/(\Delta+1+\chi)^\nu, \tag{4}$$

где $1 \leqslant x \leqslant \Delta$, $0 \leqslant \chi = x - \lfloor \chi \rfloor < 1$, $\nu \in \mathbb{N}$. Критерием такого построения является реализация фактов принадлежности определённых значений

функции (4) области значений исходной функции (3), аргументом которой выступает целочисленная величина Δ. Нашу сопутствующую функцию можно дифференцировать по аргументу x.

Преобразуем соотношение (4):

$$\varphi_{\text{п}}^{c}(x) = b_m \sum_{l=1}^{\lfloor x \rfloor} (l+\chi)^{\nu} / (\lfloor x \rfloor + 1 + \chi)^{\nu}.$$

Выражение производной

$$d\left(\varphi_{\text{п}}^{c}(x)\right)/dx = \varphi_{\text{п}}^{c}(x)'$$

находится здесь согласно известному правилу [5] с учётом равенства $dx = d\chi$:

$$\varphi_{\text{п}}^{c}(x)' = b_m \nu \sum_{l=1}^{\lfloor x \rfloor} \phi_l^{\nu-1} (x+1-l-\chi)/(x+1)^{2\nu};$$
$$\phi_l = (l+\chi)(x+1).$$

Учитывая соотношение $x = \lfloor x \rfloor + \chi$, получаем

$$\varphi_{\text{п}}^{c}(x)' = b_m \nu \sum_{l=1}^{\lfloor x \rfloor} (l+\chi)^{\nu-1} (\lfloor x \rfloor + 1 - l)/(x+1)^{\nu+1}.$$

Поскольку $\lfloor x \rfloor \geqslant l$, для любого $x \in I_{x\Delta} = [1, \Delta]$ величина $\varphi_{\text{п}}^{c}(x)' > 0$, то есть в интервале $I_{x\Delta}$ величины $\varphi_{\text{п}}^{c}(x)$, $\varphi_{\text{п}}^{c}(x)'$ имеют сплошь положительные значения.

Аналогичные построения и преобразования могут быть произведены и применительно к функциям $\varphi_{\text{п}}^{-\text{p}}(\Delta)$, $-\varphi_{\text{п}}^{c}(x)$, которые воспроизводят выражения (3), (4) со знаками, обратными применённым выше, и имеют, таким образом, отрицательные значения.

Величину $\varphi_{\text{п}}^{+\text{p}}(\Delta)$ с областью значений из $\mathbb{R}_+ \backslash \{0\}$ и величину $\varphi_{\text{п}}^{-\text{p}}(\Delta)$ с областью значений из $\mathbb{R}_- \backslash \{0\}$ будем обозначать просто как $\varphi_{\text{п}}^{+\text{p}}$ и $\varphi_{\text{п}}^{-\text{p}}$. Соответственно, элемент множества $\{\varphi_{\text{п}}^{+\text{p}}, \varphi_{\text{п}}^{-\text{p}}\}$ может быть представлен в виде $\operatorname{ex}\varphi_{\text{п}}^{\text{p}}$. Установленный выше характер знака производной сопутствующей функции по аргументу x позволяет прояснить то обстоятельство, что уровень $\max_{\{\Delta\}} \varphi_{\text{п}}^{+\text{p}}$, соответствующий максимуму положительной величины на интервале $I_{x\Delta}$, приходится на максимальное значение $\Delta = p - 1$. В симметричном по знаку случае отрицательных значений величины $\varphi_{\text{п}}^{-\text{p}}$ минимальное значение данной величины $\min_{\{\Delta\}} \varphi_{\text{п}}^{-\text{p}}$ на том же интервале $I_{x\Delta}$ приходится на то же значение $\Delta = p - 1$.

Итак, если в процессе вычислений $\varphi_{\text{п}}^{+\text{p}}$ или $\varphi_{\text{п}}^{-\text{p}}$ при задаваемых изменениях факторов p, ν окажется, что для какого-либо найденного $\Delta = p-1$ абсолютная величина соответствующего ОСО уже не превышает установленного порога δ_s ($s \in \{-, +\}$), то достигнутые значения p, ν и будут обеспечивать удовлетворение заявленного условия выделимости. Чтобы перейти к выработке условий выделимости целочисленных весовых коэффициентов основных последовательностей со знакочередующимися членами, сделаем несколько дополнений к нашим прежним замечаниям общего характера.

В частности, рассмотрим остаточные последовательности свободных множителей с чётной и нечётной индексацией членов, имеющие соответственно все положительные или отрицательные члены:

$$\Pi^{+}_{\text{п}} = \left(c_{2l-1}, l = 1, \ldots, l^{+}_{m}\right) \to S^{+} = \sum_{l=1}^{l^{+}_{m}} c_{2l-1};$$

$$\Pi^{-}_{\text{п}} = \left(-c_{2l}, l = 1, \ldots, l^{-}_{m}\right) \to S^{-} = -\sum_{l=1}^{l^{-}_{m}} c_{2l};$$

S^{+}, S^{-} — суммы членов соответственно положительных и отрицательных подпоследовательностей $\Pi^{+}_{\text{п}}$ и $\Pi^{-}_{\text{п}}$, то есть соответственно положительный и отрицательный суммарные остатки. Подстрочный индекс $\bullet$ обозначений $S^{+}_{\bullet}$ и $S^{-}_{\bullet}$, используемых далее, будет указывать на последний член, находящийся в подпоследовательности $\Pi^{+}_{\text{п}}$ или $\Pi^{-}_{\text{п}}$ и нумеруемый как член последовательности $\Pi_{\text{п}}$, объединяющий $\Pi^{+}_{\text{п}}$ и $\Pi^{-}_{\text{п}}$; члены $\Pi^{+}_{\text{п}}$ и $\Pi^{-}_{\text{п}}$, образующие объединённую последовательность $\Pi_{\text{п}}$, поочерёдно выбираются из них. Через $\Pi^{+}_{\text{по}}$ или $\Pi^{-}_{\text{по}}$ обозначим модификацию подпоследовательности $\Pi^{+}_{\text{п}}$ или $\Pi^{-}_{\text{п}}$, в которой на местах её членов размещаются нули, то есть содержимое множества качественных признаков из $\Pi^{+}_{\text{по}}$ или $\Pi^{-}_{\text{по}}$ составляет нуль.

Всевозможные комбинации знаков суммарных остатков вида $S_{\bullet}$ и внешних членов $c_{\Delta+1}$, то есть комбинации верхних индексов их обозначений, представлены в нижеприведённой таблице. Число вида l^{+}_{m} или l^{-}_{m}, указанное в этой таблице и обозначающее количество членов соответствующей подпоследовательности $\Pi^{+}_{\text{п}}$ или $\Pi^{-}_{\text{п}}$, определяется из следующих равенств:

$$2l^{-}_{m\circ} = \Delta - 1; \quad 2l^{-}_{me} = \Delta; \quad 2l^{+}_{m\circ} - 1 = \Delta; \quad 2l^{+}_{me} - 1 = \Delta - 1. \qquad (5)$$

Знак S/ его нижний индекс $\bullet$	Знак $c_{\Delta+1}$	Знак или значение c_{Δ}	Знак или значение $c_{\Delta-1}$	Значение l^{+}_{m} или l^{-}_{m}	Нечётность или чётность Δ	Разновидность ОСО
$-/\Delta-1$	$-$	$0 \to \Pi^{+}_{\text{по}}$	$-$	$l^{-}_{m} = (\Delta-1)/2$	о	$\varphi^{+}_{\text{чо}}$
$-/\Delta$	$+$	$-$	$0 \to \Pi^{+}_{\text{по}}$	$l^{-}_{m} = \Delta/2$	e	$\varphi^{-}_{\text{че}}$
$+/\Delta$	$-$	$+$	$0 \to \Pi^{-}_{\text{по}}$	$l^{+}_{m} = (\Delta+1)/2$	о	$\varphi^{-}_{\text{чо}}$
$+/\Delta-1$	$+$	$0 \to \Pi^{-}_{\text{по}}$	$+$	$l^{+}_{m} = \Delta/2$	e	$\varphi^{+}_{\text{че}}$

Переход от подстрочной индексации в обозначениях сумм $S^{+}_{\bullet}$ и $S^{-}_{\bullet}$ к подстрочной индексации этих же сумм как величин, соответствующих подпоследовательностям $\Pi^{+}_{\text{п}}$ и $\Pi^{-}_{\text{п}}$, может быть осуществлён согласно равенствам (5).

Для последовательности, расширенной за счёт внешнего члена, позицию которого мы обозначим как l^{ex}_{m}, количественное определение этой позиции в случаях положительности либо отрицательности всех членов данной расширенной последовательности может быть произведено по соотношениям

$$2l^{\text{ex}-}_{m} = \Delta + 1, \quad 2l^{\text{ex}+}_{m} - 1 = \Delta + 1.$$

Член $c_{\Delta+1}$ проявляет свой внешний характер в отношении последовательности $\Pi^{+}_{\text{п}}$ или $\Pi^{-}_{\text{п}}$ и может быть обозначен соответственно как $c^{+}_{\Delta+1}$ или $c^{-}_{\Delta+1}$.

В правой колонке нашей таблицы помещены обозначения следующих разновидностей относительных суммарных остатков: $\varphi^{+}_{\text{чо}}$, $\varphi^{+}_{\text{че}}$ — функции вида соответственно $b_m S^{-}_{\Delta-1}/c^{-}_{\Delta+1}$, $b_m S^{+}_{\Delta-1}/c^{+}_{\Delta+1}$; $\varphi^{-}_{\text{чо}}$, $\varphi^{-}_{\text{че}}$ — функции вида соответственно $b_m S^{+}_{\Delta}/c^{-}_{\Delta+1}$, $b_m S^{-}_{\Delta}/c^{+}_{\Delta+1}$.

Надстрочные индексы этих функций отвечают соотношениям: плюс — совпадение между собой знаков величин S и $c_{\Delta+1}$; минус — несовпадение между собой таких знаков.

Пусть в качестве остаточной последовательности свободных множителей выступает знакочередующаяся геометрическая прогрессия с первым членом q и знаменателем $-q$:

$$c_l = c^{\text{г}}_{\text{ч}l} = (-1)^{l+1} q^l, \quad l = 1, \ldots, \Delta.$$

Среди слагаемых, относящихся к суммарным остаткам, будем собирать такие, которые имеют одинаковые знаки и, следовательно, образуют величины $S^{+}_{\bullet}$, $S^{-}_{\bullet}$.

Если положить $q > 1$, то в случае, когда все ненулевые относительные суммарные остатки, связанные с указанной последовательностью, отрицательны, учитывая данные вышеприведённой таблицы, имеем при $\Delta \in I_{p-1}$:

$$\varphi^{-\text{г}}_{\text{че}} = -\left(b_m q/(q^2-1)\right)(q^{\Delta}-1)/q^{\Delta}; \tag{6}$$

$$\varphi^{-\text{г}}_{\text{чо}} = -\left(b_m q\right)/\left(q^2-1\right)(q^{\Delta+1}-1)/q^{\Delta+1}. \tag{7}$$

Отсюда, следуя принятому нами способу решения двойного неравенства

$$-\delta_{-} < \varphi^{-\text{г}}_{\text{ч}} \leqslant 0 \tag{8}$$

с ОСО в его центральной части, выражаемым с помощью суммы геометрической прогрессии:

$$0 < (q^{\Delta}-1)/q^{\Delta} < 1, \quad 0 < (q^{\Delta+1}-1)/q^{\Delta+1} < 1; \quad -b^{-}_m q/(q^2-1) > -1.$$

Продолжив решение, находим

$$q > 0{,}5\left(b^{-}_m + \left((b^{-}_m)^2+4\right)^{1/2}\right).$$

Переходя теперь к случаю использования знакочередующейся геометрической прогрессии, когда все ненулевые относительные суммарные остатки положительны, и учитывая данные вышеприведённой таблицы, вырабатываем следующее представление разновидностей положительного ОСО:

$$\varphi^{+\text{г}}_{\text{чо}} = \left(b_m/(q^2-1)\right)(q^{\Delta-1}-1)/q^{\Delta-1}, \quad \Delta \in I_{p-1}\backslash\{1\}; \tag{9}$$

$$\varphi^{+\text{г}}_{\text{че}} = -\left(b_m/(q^2-1)\right)(q^{\Delta}-1)/q^{\Delta}, \quad \Delta \in I_{p-1}. \tag{10}$$

Затем, решая двойное неравенство

$$0 \leqslant \varphi^{+\text{г}}_{\text{ч}} < \delta_{+}, \tag{11}$$

получаем

$$0 < (q^{\Delta-1}-1)/q^{\Delta-1} < 1, \quad 0 < (q^{\Delta}-1)/q^{\Delta}; \quad 0 \leqslant b^{+}_m/(q^2-1) < 1.$$

Отсюда $q > (b^{+}_m+1)^{1/2}$.

Теперь количественное заключение о допустимых значениях $q > 1$, при которых выполняется поставленное условие выделимости, можно представить как

$$q > \max\left(0{,}5\left(b_m^- + \left((b_m^-)^2 + 4\right)^{1/2}\right), \quad (b_m^+ + 1)^{1/2}\right).$$

Далее положим $0 < q < 1$, и, в случае отрицательности всех ненулевых значений относительных суммарных остатков, обратившись к сооношениям (6), (7) при решении двойного неравенства (8), получим:

$$\varphi_{\text{че}}^{-\text{г}} = -b_m^-\eta(\eta^2 - 1)^{-1}(\eta^{\Delta} - 1); \tag{12}$$

$$\varphi_{\text{чо}}^{-\text{г}} = -b_m^-\eta(\eta^2 - 1)^{-1}(\eta^{\Delta+1} - 1); \tag{13}$$

$$\eta = (1/q) > 1, \quad \Delta \in I_{p-1}.$$

Учтём, что для натуральных $p \geqslant 2$ и $g \in I_{p-1}$ действует равенство

$$\min_p(\max \Delta) = 1,$$

и поэтому ни одна из величин вида (12), (13) не удовлетворяет неравенству (8): каждое из чисел η, b_m превышает единицу. Даже в случае $\Delta = 1$ абсолютная величина (12) должна удовлетворять неравенству

$$b_m^-\eta/(\eta + 1) < 1 \Rightarrow \eta(b_m^- - 1) < 1,$$

но поскольку $\eta > 1$ и $b_m \geqslant 2$, выполнить такое требование невозможно. Тем более это оказывается невозможным и для всех других значений числа Δ из области его определения применительно к неравенству (8).

Продемонстрируем неосуществимость неравенства (11) применительно ко всем относительным суммарным остаткам вида (9) и (10), когда положительное $q < 1$. Здесь полагаем, что в выражении (9) число Δ имеет значение не меньшее двух, и рассмотрим величину $\eta^{\Delta-1}$ для выражения (9) и величину η^{Δ} для выражения (10), которые в данных выражениях теперь более всего благоприятствуют реализации двойного неравенства (11).

Тогда для реализации (11) уже при $\Delta = 2$ в (9) и $\Delta = 1$ в (10) должны соблюдаться неравенства

$$0 \leqslant b_m^+\eta^2/(\eta + 1) < 1 \Rightarrow \eta(b_m^+\eta - 1) < 1.$$

Однако $\eta > 1$, $b_m \geqslant 2$, и неравенство (11) не может быть здесь выполнено.

Итак, при любых значениях Δ, соответствующих области значений $0 < q < 1$, условия выделимости (8), (11) оказываются невыполнимыми.

ОСО, использующий знакочередующуюся последовательность, содержащую члены — равные натуральные степени натуральных чисел, может быть выражен следующим образом:

$$\varphi_{\text{ч}}^{sp} = (-1)^{\varepsilon+\xi} b_m \sum_{l=1}^{l_m^s} (2l - \varepsilon)^{\nu} / \left(2l_m^s + \xi\right)^{\nu},$$

где верхний индекс $s \in \{-, +\}$ указывает на знак «минус» или «плюс»;

$$\varepsilon = \begin{cases} 0 \to \Pi_{\text{п}}^- \to S_{\bullet}^-, \\ 1 \to \Pi_{\text{п}}^+ \to S_{\bullet}^+; \end{cases}$$

$$l_m^- \to \varepsilon = 0, \quad l_m^+ \to \varepsilon = 1;$$

значения ξ могут определяться в зависимости от пары знаков s_1, $s_2 \in \{-, +\}$, которыми — в качестве верхних индексов — снабжаются обозначения суммарных остатков и внешних членов вида $S_\bullet^{s_1}$, $c_{\Delta+1}^{s_2}$:

$$\xi = \begin{cases} 0: & (s_1, s_2) = (+, -), \\ 1: & (s_1, s_2) = (-, +) \vee (+, +), \\ 2: & (s_1, s_2) = (-, -). \end{cases}$$

Кроме того, можно указать следующие соотношения, которые связывают между собой знаковые индексы и символы ε, ξ:

$$s \to \begin{cases} +: & (s_1, s_2) = (+, +) \vee (-, -) \to \varepsilon + \xi = 2, \\ -: & (s_1, s_2) = (-, +) \vee (+, -) \to \varepsilon + \xi = 1. \end{cases}$$

Функция, сопутствующая данному ОСО, имеет вид

$$\varphi_{\text{ч}}^{sc}(x) = (-1)^{\varepsilon+\xi} b_m \sum_{l=1}^{\lfloor x \rfloor} (2l - \varepsilon + 2\chi)^\nu / (2\lfloor x \rfloor + \xi + 2\chi)^\nu;$$
$$0 \leqslant \chi = x - \lfloor x \rfloor < 1, \quad \lfloor x \rfloor = l_m^s.$$

В пределах области своего определения $[1, l_m^s]$ сопутствующая функция имеет производную

$$d\varphi_{\text{ч}}^{sc}(x)/dx = (-1)^{\varepsilon+\xi} 2\nu b_m A_x / \left(2l_m^s + \xi + 2\chi\right)^{2\nu}; \tag{14}$$
$$A_x = (2l_m^s + \xi + 2\chi)^{\nu-1} \sum_{l=1}^{l_m^s} (2l - \varepsilon + 2\chi)^{\nu-1} \left(2l_m^s - 2l + \xi + \varepsilon\right).$$

Нетрудно видеть, что справедливым оказывается неравенство $A_x > 0$, и знак выражения (14) определяется лишь показателем степени $(-1)^{\varepsilon+\xi}$. Когда этот показатель равен двум, сопутствующая функция имеет вид $\varphi_{\text{ч}}^{+c}(x)$, а когда он равен единице — вид $-\varphi_{\text{ч}}^{-c}(x)$. Следовательно, при увеличении x первая из указанных функций в области своего определения является возрастающей, а вторая — убывающей.

Сужая $\varphi_{\text{ч}}^{sc}(x)$ до ОСО $\varphi_{\text{ч}}^{+p}$ или $\varphi_{\text{ч}}^{-p}$, то есть беря значение $\varphi_{\text{ч}}^{sc}(x)$ в точках вида $x = \lfloor x \rfloor$, убеждаемся в том, что с ростом l_m^s, а следовательно, с ростом Δ положительные значения $\varphi_{\text{ч}}^{+p}$ увеличиваются, а отрицательные значения $\varphi_{\text{ч}}^{-p}$ уменьшаются, поэтому максимум $\varphi_{\text{ч}}^{+p}$ или минимум $\varphi_{\text{ч}}^{-p}$ соответствует максимуму $\Delta = p - 1$ или же минимуму $g = 1$. То есть число Δ может быть обоснованно выбрано как значение аргумента ОСО, участвующее в его проверке на соблюдение выработанного условия выделимости.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *А. И. Никонов*, “Шифрование на основе сумм со слагаемыми — произведениями весовых и свободных компонентов” // *Вестн. Сам. гос. техн. ун-та. Сер. Физ.-мат. науки*, 2012. № 4(29). С. 199–206. [*A. I. Nikonov*, “Enciphering on the basis of the sums with products of weight and free components as summands” // *Vestn. Samar. Gos. Tekhn. Univ. Ser. Fiz.-Mat. Nauki*, 2012. no. 4(29). Pp. 199–206].

2. *J. A. Anderson*, Discrete Mathematics with Combinatorics. New Jersey: Prentice Hall, 2000. 799 pp.; русск. пер.: *Дж. Андерсон*, Дискретная математика и комбинаторика. М.: Вильямс, 2004. 960 с.
3. *А. И. Никонов*, "Преобразование суммы взвешенных степеней натуральных чисел с одинаковыми показателями" // *Вестн. Сам. гос. техн. ун-та. Сер. Физ.-мат. науки*, 2010. № 1(20). С. 258–262. [*A. I. Nikonov*, "Converting the Sum of Weighted Degrees of Natural Numbers with the Same Parameters" // *Vestn. Samar. Gos. Tekhn. Univ. Ser. Fiz.-Mat. Nauki*, 2010. no. 1(20). Pp. 258–262].
4. *А. И. Никонов*, "Приведение суммы взвешенных одинаковых степеней к явному комбинаторному представлению" // *Вестн. Сам. гос. техн. ун-та. Сер. Физ.-мат. науки*, 2012. № 3(28). С. 163–169. [*A. I. Nikonov*, "Reduction of the sum of the weight equal powers to explicit combinatorial representation" // *Vestn. Samar. Gos. Tekhn. Univ. Ser. Fiz.-Mat. Nauki*, 2012. no. 3(28). Pp. 163–169].
5. *S. Banach*, Rachunek różniczkowy i całkowy, tom I (Differential and Integral Calculus, vol. 1). Lwów: Zakład Narodowy im. Ossolińskich, 1929. 294 pp.; русск. пер.: *С. Банах*, Дифференциальное и интегральное исчисление. М.: Наука, 1972. 424 с.

Поступила в редакцию 17/IV/2013;
в окончательном варианте — 17/V/2013.

MSC: 68P25

CONDITIONS OF SEPARABILITY OF WEIGHT FACTORS FROM THE SUMS WITH MEMBERS OF SEQUENCES OF TWO ASPECTS

A. I. Nikonov

Samara State Technical University,
244, Molodogvardeyskaya st., Samara, 443100, Russia.

E-mail: nikonovai@mail.ru

Representation of conditions of separability of integer weight factors from the sequences organizing a basis of enciphering is described. Two aspects of such sequences are considered: a geometrical progression and sequence with equal powers of natural numbers. These sequences of constant signs and alternating sequences are used when generating the relative summarized residuals, expression of each of which is located in a central part of a double inequality. Definition of conditions of separability involving the residual sequence — a geometrical progression is made with reference to its common ratio, and conditions of separability involving the the residual sequence containing equal powers of natural numbers, are found using the accompanying function introduced with reference to integer arguments of formed values of relative summarized residuals.

Key words: *separability conditions, weight factors, free multipliers, summarized residual, relative summarized residual, an exterior member.*

Original article submitted 17/IV/2013;
revision submitted 17/V/2013.

Alexander I. Nikonov (Dr. Sci. (Tehn.)), Professor, Dept. of Electronic Sistems and Information Security.