2. Смарт Н. Криптография. – М.: Техносфера, 2005. – 528 с.

3. Липницкий В.А., Крупенкова Т.Г. Трехразрядный вариант алгоритма “baby-step giant-step” в проблеме дискретного логарифмирования. // Материалы МНТС «Телекоммуникации: сети и технологии, алгебраическое кодирование и безопасность данных». – Мн.: БГУИР, 2015. – С. 56 – 60.

4. Pohlig S.C. and Hellman M.E. An Improved Algorithm for Computing Logarithms Over $GF(p)$ and its Cryptographic Significance. // IEEE Trans. Inf. Theory, 1978. – Vol. 1, no 24. – P. 106 – 110.

5. Болотов А.А., Гашков С.Б., Фролов А.Б. Элементарное введение в эллиптическую криптографию. Протоколы криптографии на эллиптических кривых. – М.: КомКнига, 2006. – 280 с.

6. Лидл Р., Нидеррайтер Г. Конечные поля. В 2-х т. Пер. с англ. – М.: Мир, 1988. – 822 с.

7. Rubin Karl., Silverberg Alice. Algebraic tory in cryptography. // CRYPTO 2003. / Lecture Notes in Computer Science, vol. 2442. Springer-Verlag. 2003. - P. 1–11.

8. Пирс Р. Ассоциативные алгебры. – М.: Мир, 1986. – 524 с.

УДК 519.6

НЕАДДИТИВНАЯ МЕРА

Романчак В.М.

Белорусский национальный технический университет, Минск, Республика Беларусь

Введение. В настоящее время величину определяют как “свойство материального объекта или явления, общее в качественном отношении для класса объектов или явлений, но в количественном отношении индивидуальное для каждого из них ”. А под измерением понимают “процесс экспериментального получения одного или более значений величины, которые могут быть обоснованно приписаны величине”. Эксперимент можно проводить с помощью объективных средств измерения или на основании субъективного мнения компетентного лица, которого мы будем называть экспертом. Поэтому будем считать, что измерение величины, в зависимости от метода получения измерительной информации, может быть объективным или субъективным. Например, можно измерять массу груза с помощью весов (объективное измерение, которое использует техническое средство), – а можно измерять ощущение веса, которое возникает у человека, когда он поднимает груз (субъективное измерение, использующее экспертные оценки).

Большинство объективных измерений использует единицу измерения и свойство аддитивности физических величин. В тех случаях, когда проводятся субъективные измерения, единица измерения отсутствует и измеряемая величина, как правило, не является аддитивной. Считаем, что измерить неаддитивную величину объектов можно в порядковой шкале, а значения величины будем находить косвенно. С этой целью аксиоматически введем понятие объектов A_i, i=1, 2, …, n величина которых изменяется равномерно. Номер объекта будем называть *рейтингом*. Введем в общем виде аксиоматическое определение рейтинга и выясним, каким образом рейтинг можно связать со значениями величины.

Аксиоматическое определение рейтинга. Чтобы формально ввести неаддитивную меру, введем область ее определения. Пусть задано конечное множество элементов $\Omega=\{\omega_1, \omega_2, \ldots, \omega_n\}$. Пусть $\Im$ — множество всех подмножеств Ω (алгебра). Для множества $\Im$ аксиоматически введем неаддитивную меру (рейтинг).

Определение. Неаддитивная мера (рейтинг) – это числовая функция r, определенная на множествах из алгебры $\Im$, причем если $A\subseteq B$, то будет выполняться:

A_1. Если $A\neq B$, то $r(B\backslash A)>0$,

A_2. $r(B\backslash A)= r(B) - r(A)$.

Для множеств $A_i\subseteq\Im$, i=1, 2, …, n можно ввести отношение частичного порядка, определив операцию включения $\subseteq$. В случае отношения частичного порядка среди множества $\{A_1, A_2,\ldots, A_n\}$ могут быть несравнимые элементы. Если во множестве $\{A_1, A_2, \ldots, A_n\}$ любые два элементы сравнимы, то такое множество называют *упорядоченным множеством*.

Пример 1. Пусть $\Omega=\{\omega_1,\omega_2\}$ и $\omega_1\cdot\omega_2=\varnothing$, тогда $\Im=\{A_0, A_1, A_2, A_{12}\}$, где $A_0=\varnothing$, $A_1=\omega_1$, $A_2=\omega_2$, $A_{12}=\omega_1+\omega_2$. Можно выделить два упорядоченных подмножества $\Im$: $\{A_0, A_1, A_{12}\}$ и $\{A_0, A_2, A_{12}\}$.

Пусть $r(A_1\backslash A_0)=r(A_{12}\backslash A_1)$. Следовательно, выполняются равенства $r(A_1) - r(A_0)=\lambda$, $r(A_{12}) - r(A_1) = \lambda$, где λ – неизвестная положительная постоянная. Тогда $r(A_1)= \lambda+r(\varnothing)$, где $\lambda=(r(\Omega) - r(\varnothing))/2$. Причем $r(\Omega)$, $r(\varnothing)$ – любые числа, для которых выполняется неравенство $r(\Omega)>r(\varnothing)$. Если, например, $r(\Omega)=1$ и $r(\varnothing)=0$, то получим вероятностную меру с вероятностями $r(\omega_1) = 1/2$ и $r(\omega_2) = r(A_{12}\backslash A_1) = r(\Omega) - r(\omega_1)= 1/2$. Из примера следует, что аддитивная мера является частным случаем неаддитивной меры.

Величина объекта. Чтобы использовать определение неаддитивной меры для измерения величины объекта, определим величину объекта с позиций теории множеств. Определение приведем вначале для частного случая трех объектов. Пусть объекты A_1, A_2, A_3 упорядочены по величине Q (объекты упорядочены с помощью некоторого отношением порядка $\leq$) и выполняется $A_1\leq A_2\leq A_3$. Под величиной объектов A_1, A_2, A_3 будем понимать множества $\omega_1 = \{\{A_1\}\}$, $\omega_2= \{\{A_1\}, \{A_1, A_2\}\}$, $\omega_3 = \{\{A_1\}, \{A_1, A_2\},$

$\{A_2, A_3\}\}$. Тогда для величины объектов определено отношение порядка на основании операции включения $\omega_1 \subseteq \omega_2 \subseteq \omega_3$. Определение величины объекта логически непротиворечиво. Так, если все три объекта совпадают, $A_1=A_2=A_3$, то величина объектов совпадает, $\omega_1=\omega_2=\omega_3$. Если совпадают два из трех объектов, $A_1=A_2$, то величина соответствующих объектов совпадает, $\omega_1=\omega_2$ и аналогично, если $A_2=A_3$, то $\omega_2=\omega_3$. В общем случае для множества объектов A_1, $A_2,\ldots,A_n$, которые упорядочены по величине *Q величину объекта* A_k можно определить как множество $\omega_k=\{\{A_1\},\{A_1,A_2\},\{A_2,A_3\},\ldots,\{A_{k-1},A_k\}\}$.

Если считать, что для множества величин $\Omega=\{\omega_1, \omega_2, \ldots, \omega_n\}$ определена неаддитивная мера (рейтинг), то каждому объекту A_k можно поставить в соответствие величину объекта ω_k и рейтинг объекта $r(\omega_k)$. Следовательно, для объектов, величин объектов и рейтинга объектов определена композиция изоморфизмов $A_k \to \omega_k \to r(\omega_k)$, для которой выполняется $A_i \le A_j \Leftrightarrow \omega_i \subseteq \omega_j \Leftrightarrow r(\omega_i) \le r(\omega_j)$. Поэтому определим, что *рейтинг объекта* равен рейтингу соответствующей величины объекта $r(A_i)=r(\omega_i)$, $i=1, 2, \ldots, n$. Тогда для рейтинга объектов будет выполняться соотношение

$$r(\{A_i, A_j\})=r(A_i) - r(A_j), \text{ если } A_i \ge A_j. \quad (7)$$

Определение. Если величина объектов A_1, A_2, …, A_n изменяется равномерно, то объекты упорядочены и для объектов определен рейтинг r таким образом, что $r(A_2) - r(A_1) = r(A_3) - r(A_2) = \ldots = r(A_n) - r(A_{n-1})$, $r(A_2) - r(A_1) > 0$.

Пример 2. Пусть события A_1, A_2, A_3 упорядочены по вероятности и выполняется отношение порядка $A_1 \le A_2 \le A_3$. Определим величину вероятности событий A_1, A_2, A_3 как $\omega_1=\{\{A_1\}\}$, $\omega_2=\{\{A_1\}, \{A_1, A_2\}\}$, $\omega_3=\{\{A_1\}, \{A_1, A_2\}, \{A_2, A_3\}\}$. Множество величин $\Omega=\{\omega_1, \omega_2, \omega_3\}$ упорядочено с помощью операции включения $\subseteq$. Пусть эксперт считает, что величина вероятности событий A_1, A_2, A_3 изменяется равномерно, тогда для рейтинга вероятности $r(A_2) - r(A_1) = \lambda$, $r(A_3) - r(A_2) = \lambda$, $\lambda > 0$, λ – неизвестная постоянная.

С помощью рейтинга можно сравнивать альтернативы в теории полезности. Если дано некоторое множество альтернатив A_1, A_2, …, A_n, упорядоченных с помощью отношение предпочтения $\preceq$, то действительная функция $u(A_i)$ является функцией полезности, если выполнено условие: для $A_i \preceq A_j$ выполняется $u(A_i) \le u(A_j)$.

Пример 3. Пусть на множестве альтернатив A_1, A_2, A_3 определено отношение предпочтения $A_1 \preceq A_2 \preceq A_3$. Определим величину полезности альтернатив как множества $\omega_1 = \{\{A_1\}\}$, $\omega_2 = \{\{A_1\}, \{A_1, A_2\}\}$, $\omega_3 = \{\{A_1\}, \{A_1, A_2\}, \{A_2, A_3\}\}$, которые упорядочены с помощью операции включения $\subseteq$. Пусть эксперт считает, что величина полезности альтернатив A_1, A_2, A_3 изменяется равномерно, тогда для рейтинга альтернатив выполняется $r(A_2) - r(A_1) = \lambda$, $r(A_3) - r(A_2) = \lambda$, λ – неизвестная постоянная, $\lambda > 0$.

Будем считать, что при любом измерении значения величины определены с точностью до изоморфизма, и рассматривать два способа определения значений величины Q: $q(A)=r(A)$, где $q(A) \in R$ или $q(A)=\exp(r(A))$, $q(A) \in R^+$.

Определение. Пусть определен рейтинг объектов A_i, $i=1, 2, \ldots, n$. Значения величины – это числовая функция $q_i=q(A_i)$, определенная на множестве объектов A_i, $i=1, 2, \ldots, n$ для которой в зависимости от способа сравнения выполняется

$$q_i - q_j = r(A_i) - r(A_j) \quad (8)$$

или

$$\ln(q_i/q_j) = r(A_i) - r(A_j), \quad (9)$$

где $i=1, 2, \ldots, n$, $j=1, 2, \ldots, n$, причем способ сравнения выбирается априори. Данное определение означает, что если найден рейтинг величины объекта, то можно произвольно выбрать способ сравнения и найти значения величины с помощью равенств (8) или (9). Данное определение означает, что если найден рейтинг величины объекта, то можно произвольно выбрать способ сравнения и найти значения величины с помощью равенств (8) или (9). Определение отражает особенность неаддитивного измерения величины.

УДК 004.05

КОНТРОЛЬ КАЧЕСТВА ВСТРОЕННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ СВЕТОТЕХНИЧЕСКИХ ИЗДЕЛИЙ В ОАО «РУДЕНСК»

Спесивцева Ю.Б., Душина Т.В.

Белорусский национальный технический университет, Минск, Республика Беларусь

Стратегической целью ОАО «Руденск» является максимально возможное удовлетворение требований потребителей светотехнической продукции. Основным средством для достижения этой цели является система менеджмента качества, соответствующая ISO/TS 16949-2009, СТБ ISO/TS 16949.

В связи с появлением новой версии стандарта IATF 16949:2016 (2016 года) появилась необходимость в совершенствовании системы менеджмента качества в части выполнения требований стандарта к оценке качества встраиваемого программного обеспечения (ПО) светотехнических изделий.

Оценив риски разработки встраиваемого программного обеспечения и проанализировав существующие методики для оценки его качества был выбран метод интегральной оценки качества программных средств (ГОСТ 28195), основанный на иерархической модели качества.

Оценка качества ПО проводится экспертной группой на этапе его применения (Таблица 1) и включает