ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И ПРИКЛАДНАЯ МАТЕМАТИКА

УДК 681.3.06:51

В.П. Корячко, В.С. Горин, Н.В.Черемухин

ОПТИМИЗАЦИЯ РАСПРЕДЕЛЕНИЯ ЭЛЕКТРИЧЕСКИХ СОЕДИНЕНИЙ ПРИ ЖГУТОВОМ МОНТАЖЕ ЭЛЕКТРОННО-ВЫЧИСЛИТЕЛЬНОЙ АППАРАТУРЫ

Рассмотрены вопросы, связанные с распределением электрических соединений в жгуты при проводном монтаже межблочных соединений. Сформулированы формальная и комбинаторная постановки задачи, и рассмотрен точный алгоритм решения, использующий схему метода ветвей и границ. Для практической реализации алгоритма предложены способы упрощения подсчета оценок и сокращения комбинаторного перебора путем включения в вычислительную схему метода ветвей и границ эвристического алгоритма перераспределения электрических проводов для устранения недопустимых объемов жгутов.

Ключевые слова: *жгутовой монтаж, пропускная способность, кабельные каналы.*

Введение. В известных работах, рассматривающих вопросы автоматизации проводного монтажа в САПР, отмечается, что задачу трассировки проводов можно решить методами, аналогичными методам трассировки печатных плат, т.е. построением с помощью известных алгоритмов дерева связывающих соединений с последующим упорядочиванием проводов, соответствующих ветвям построенных деревьев, и последовательной укладкой их на монтажном поле. Такое положение справедливо при монтаже блоков методом "внавал". Однако при жгутовом монтаже существенное влияние оказывают ограничения на объем проводов, объединяемых в жгут, связанные с конструктивными размерами (пропускными способностями) кабельных каналов, выделяемых в блоках для укладки жгутов. Для этого случая в работе [1] предлагается определять конфигурацию каждого соединения алгоритмом построения максимального потока в сети [2]. Такой подход, предполагающий пошаговый характер оптимизации, очевидно, в общем случае дает приближенный результат. Поэтому **целью работы** являются разработка и реализация точного комбинаторного алгоритма, позволяющего найти оптимальное решение задачи.

Формальная постановка задачи. Одной из наиболее распространенных конструкций блоков ЭВА является однорядный блок, в котором для реализации жгутовых соединений выделено два канала А и Б, расположенных вдоль противоположных стенок блока (см. рисунок). Ограничения на объем жгутов для подобных конструкций, как правило, существенны лишь на отдельных интервалах (1*a,* 2*a,*.... 1*b,* 2*b* и т.д.), показанных на рисунке и названных сечениями.

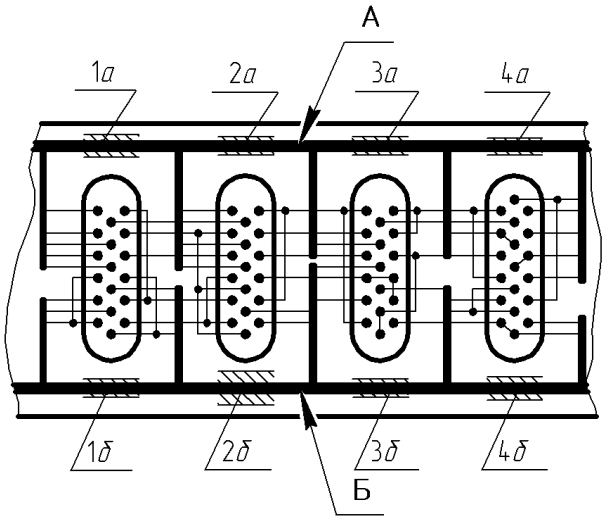


Схема укладки жгутов

При этом в жгут имеет смысл помещать лишь те соединения, которые пересекают сечения. Остальные соединения реализуются без укладки их в жгуты. Каждое соединение, помещаемое в жгут, имеет, очевидно, П-образную конфигурацию, и для него несложно подсчитать длину реализующего провода. Ставится задача таким образом распределить соединения между жгутами, чтобы их суммарная длина была минимальной и не нарушались ограничения на пропускные способности каналов.

Зададим множество координат пар контактов, которые требуется соединить проводами известного типа. Его можно получить, построив, например, для каждой цепи связывающее дерево одним из известных алгоритмов [3]. Обозначим минимальную длину реализующего провода, соединяющего *i*-ю пару контактов и проходящего через верхний канал, $l_i^в$, а через нижний – $l_i^н$. Отметим, что если несколько контактов цепи лежат в области, ограниченной двумя соседними сечениями, величины $l_i^в$ и $l_i^н$ могут соответствовать соединению различных пар контактов этой цепи, находящихся по разные стороны от сечения.

Составим матрицу $A = \left\| a_{ij} \right\|_{n \times f}$, где n – число пар контактов, соединяемых через жгут, а f – число сечений на монтажном поле. Элемент матрицы a_{ij} определим следующим образом:

$$a_{ij} = \begin{cases} \text{объему провода } i, \text{ проходящего через} \\ \quad j-e \text{ сечение;} \\ 0, \text{ если провод } i \text{ в сечении } j \text{ отсутствует.} \end{cases}$$

Будем считать, что величина пропускной способности не постоянна по длине канала и определяется пропускной способностью сечений $w_j^в$ и $w_j^н$ соответственно для верхнего и нижнего каналов. Отметим, что для реализуемости схемы необходимо:

$$w_j^в \approx w_j^н \text{ и } w_j^в + w_j^н \geq \sum_{i=1}^{n} a_{ij}; \quad j = 1,2,...,f. \quad (1)$$

Введем булевы переменные y_i, (i =1,2,..., n), значение которых будет равно единице, если *i*-е соединение реализовано в верхнем канале, и нулю – если в нижнем. Тогда задачу определения оптимального распределения проводов для подобной конструкции можно сформулировать следующим образом:

минимизировать

$$L = \sum_{i=1}^{n} \left[l_i^в \cdot y_i + l_i^н \cdot (1 - y_i) \right] \quad (2)$$

при ограничениях:

$$\sum_{i=1}^{n} a_{ij} \cdot y_i \leq w_j^в, \; j = 1,2,...,f; \quad (3)$$

$$\sum_{i=1}^{n} a_{ij} \cdot (1 - y_i) \leq w_j^н, \; j = 1,2,...,f; \quad (4)$$

$$a_{ij} \geq 0, \; y_i = \{0,1\}, \; i = 1,2,...,n. \quad (5)$$

Данная задача является задачей линейного целочисленного программирования. Для ее решения воспользуемся методом ветвей и границ [4]. С этой целью дадим **комбинаторную постановку** задачи (2) – (5).

Обозначим через $C = \{1,2,...,n\}$ множество индексов всех соединений схемы, $P = \{p_1, p_2, \ldots, p_m,\}$ $(m \leq n)$ – множество индексов соединений, реализованных через верхний канал, а $\overline{P} = \{\overline{p}_1, \overline{p}_2, \ldots, \overline{p}_l,\}$ $(l + m = n)$ – множеств о индек-сов соединений, реализованных через нижний канал. Очевидно, $P \bigcap \overline{P} = \varnothing$.

Преобразуем выражение (2) к виду:

$$L = \sum_{i \in P}^{n} l_i^в + \sum_{i \in \overline{P}}^{n} l_i^н. \quad (6)$$

Используя введенные обозначения, представим задачу определения оптимальной конфигурации соединений как задачу разбиения множества $C = \{1,2,...,n\}$ на два непересекающихся подмножества

$$\begin{aligned} P^* &= \{p_1^*, p_2^*, \ldots, p_q^*\}, \; q \leq n, \\ \overline{P}^* &= \{\overline{p}_1^*, \overline{p}_2^*, \ldots, \overline{p}_s^*\}, \; s+q = n, \end{aligned} \quad (7)$$

при котором выполняются ограничения

$$\begin{aligned} &\sum_{i \in P^*}^{n} a_{ij} \leq w_j^в, \; j = 1,2,...,f; \\ &\sum_{i \in \overline{P}^*}^{n} a_{ij} \leq w_j^н, \; j = 1,2,...,f \end{aligned} \quad (8)$$

и достигается минимум выражения (6).

Обозначим все множество допустимых решений задачи через *G* и будем разбивать его в процессе ветвления по правилу, указанному ниже, на некоторые непересекающиеся подмножества $G_r^k \left(r = 1,2,...,t_k \right)$, включающие в себя все элементы множеств P_r^k и $\overline{P}_r^k$. Сокращенно будем записывать это так:

$$G_r^k = \left\{ g \in G \mid P_r^k, \overline{P}_r^k \right\}. \qquad (9)$$

Пусть $T_r^k -$ множество индексов соединений схемы, не вошедших на k-м шаге в множества P_r^k и $\overline{P}_r^k$. Тогда в качестве оценки для каждого из таких соединений можно выбрать величину

$$l_i = \min\left(l_i^в, l_i^н \right),\ i \in T_r^k. \qquad (10)$$

Эта оценка соответствует действительному распределению соединений с индексами $i \in T_r^k$ по кратчайшим путям. Обозначим множество индексов соединений, имеющих оценку (10) при прокладке по верхнему каналу, через Q_r^k, а по нижнему каналу – $\overline{Q}_r^k$. Для множеств Q_r^k и $\overline{Q}_r^k$ справедливы следующие условия:

$$T_r^k = Q_r^k \cup \overline{Q}_r^k;\ Q_r^k \cap \overline{Q}_r^k = \varnothing. \qquad (11)$$

С учетом введенных обозначений нижнюю оценку $\varsigma\left(G_r^k \right)$ для множества G_r^k можно вычислить из выражения:

$$\varsigma\left(G_r^k \right) = \sum_{i \in P_r^k \cup Q_r^k}^{n} l_i^в + \sum_{i \in \overline{P}_r^k \cup \overline{Q}_r^k}^{n} l_i^н. \qquad (12)$$

Пусть $G_{\nu(k)}^k -$ множество, имеющее минимальную оценку среди всех множеств $G_r^k \left(r = 1, 2, ..., t_k \right)$ k – шага ветвления. Тогда, если решение

$$\begin{aligned} P^* &= P_{\nu(k)}^k \cup Q_{\nu(k)}^k, \\ P^* &= \overline{P}_{\nu(k)}^k \cup \overline{Q}_{\nu(k)}^k \end{aligned} \qquad (13)$$

удовлетворяет ограничениям (8), оно оптимально. Действительно, это решение принадлежит множеству $G_{\nu(k)}^k$ и

$$L = \sum_{i \in P^*}^{n} l_i^в + \sum_{i \in \overline{P}^*}^{n} l_i^н = \varsigma\left(G_{\nu(k)}^k \right) \le \varsigma\left(G_r^k \right), \qquad (14)$$

$r = 1, 2, \ldots, t_k$.

Укажем следующее правило ветвления для решения задачи (6) – (8).

Выберем на очередном k-м шаге ветвления множество решений

$$G_{\nu(k)}^k = \left\{ g \in G \mid P_{\nu(k)}^k, \overline{P}_{\nu(k)}^k \right\} \qquad (15)$$

с минимальной оценкой $\varsigma\left(G_{\nu(k)}^k \right)$. Если при включении в множества $P_{\nu(k)}^k$ и $\overline{P}_{\nu(k)}^k$ всех индексов соединений, принадлежащих множеству $T_{\nu(k)}^k$, не нарушатся ограничения (8), то, согласно (13), это решение оптимально. В противном случае выделим подмножество индексов соединений $R_\varphi^\eta \subseteq T_{\nu(k)}^k$, $(\varphi = 1, 2, ..., \mu,\ \mu \le f;\ \eta = 1$ для верхнего и $\eta = 2$ для нижнего каналов), пересекающих φ-е сечение, в котором превышена пропускная способность. Множество решений (15) будем разбивать на два подмножества по признаку принадлежности одного из индексов соединений $i \in R_\varphi^\eta$ множествам $P_{\nu(k)}^k$ либо $\overline{P}_{\nu(k)}^k$:

$$\begin{aligned} G_{\nu(k),1}^k &= \left\{ \begin{array}{c} g \in G \mid P_{\nu(k),1}^k = P_{\nu(k)}^k \cup i; \\ \overline{P}_{\nu(k),1}^k \equiv \overline{P}_{\nu(k)}^k \end{array} \right\}, \\ G_{\nu(k),2}^k &= \left\{ \begin{array}{c} g \in G \mid P_{\nu(k),2}^k \equiv P_{\nu(k)}^k; \\ \overline{P}_{\nu(k),2}^k = \overline{P}_{\nu(k)}^k \cup i \end{array} \right\}. \end{aligned} \qquad (16)$$

При этом формируемые множества P_r^k и $\overline{P}_r^k$ должны удовлетворять ограничениям (8).

После разбиения множества $G_{\nu(k)}^k$ изменим множество $T_{\nu(k)}^k$:

$$T_{\nu(k),1}^k \equiv T_{\nu(k),2}^k = T_{\nu(k)}^k \setminus i. \qquad (17)$$

Будем считать множества $G_{\nu(k),1}^k$, $G_{\nu(k),2}^k$, а также не разбиваемые на этом шаге подмножества подмножествами (κ +1}-го шага и процедуру поиска оптимального решения продолжим. Такой процесс ветвления, очевидно, на каком-то шаге должен закончиться в силу конечности множества допустимых решений.

Приведем **точный алгоритм решения задачи** (6) – (8). Для этого предварительно сделаем следующие **замечания**, которые позволят несколько уменьшить объем вычислений.

1. Оценки $\varsigma\left(G_r^k \right)$ для множеств $G_r^k \left(r = 1, 2, ..., t_k \right)$ можно вычислять по выражению (12). Однако, согласно (10), от включения индексов соединений $i \in Q_r^k$ в множество P_r^k, а $i \in \overline{Q}_r^k$ в множество $\overline{P}_r^k$

оценки $\varsigma\left(G_r^k\right)$ не изменяются. С другой стороны, при включении индексов соединений $i \in Q_r^k$ в множество $\overline{P}_r^k$, а $i \in \overline{Q}_r^k$ в множество P_r^k оценки $\varsigma\left(G_r^k\right)$ увеличиваются на величину

$$\Delta l_i = | l_i^в - l_i^н | . \qquad (18)$$

Поэтому при решении задачи достаточно изменять на величину Δl_i оценки только тех ветвей дерева решения, в которых происходит увеличение мощности множеств P_r^k и $\overline{P}_r^k$ от включения индексов соединений, принадлежащих соответственно множествам $\overline{Q}_r^k$ и Q_r^k.

2. Для сокращения числа ветвей дерева решения целесообразно выбирать на очередном шаге такое сечение $j_\varphi^\eta \ (\varphi = 1,2,...,\mu)$, в котором превышение пропускной способности максимально. При этом в первую очередь для разбиения наиболее "перспективных" множеств (15) среди всех допустимых индексов соединений $i \in R_\varphi^\eta$ следует выбирать индекс i^* такого соединения, которое пересекает максимальное число сечений с нарушенными ограничениями.

Алгоритм

П.1. k:=0; r:=0; $P^0 := \varnothing$; $\overline{P}^0 := \varnothing$.

П.2. Сформировать множество $T^0 := Q^0 \cup \overline{Q}^0$ и определить оценку $\varsigma\left(G^0\right) = \sum_{i=1}^{n} l_i$, где $l_i = \min\left(l_i^в, l_i^н\right), \ i = 1,2,...,n.$

П.3. Проверить ограничения:

$$\sum_{i \in P_r^k \cup Q_r^k} a_{ij} \le w_j^в, \ j = 1,2,...,f;$$
$$\sum_{i \in \overline{P}_r^k \cup \overline{Q}_r^k} a_{ij} \le w_j^н, \ j = 1,2,...,f. \qquad (19)$$

Если решение $P = P_r^k \cup Q_r^k; \overline{P} = \overline{P}_r^k \cup \overline{Q}_r^k$ удовлетворяет условиям (19), то оно оптимально. Перейти к п.8.

П.4. Определить в соответствии с замечанием 2 индекс соединения $i \in R_\varphi^\eta$, по признаку принадлежности которого множество G_r^k разбивается на два подмножества $G_{r,1}^k \cup G_{r,2}^k$.

П.5. Сформировать множества $G_{\nu(k),1}^k$ и $G_{\nu(k),2}^k$ согласно (16), а также множества $T_{\nu(k),1}^k$, $T_{\nu(k),2}^k$ (17) и вычислить оценки

$$\varsigma\left(G_{\nu(k),1}^k\right) = \varsigma\left(G_{\nu(k)}^k\right) + q_i \cdot \Delta l_i;$$
$$\varsigma\left(G_{\nu(k),2}^k\right) = \varsigma\left(G_{\nu(k)}^k\right) + \left(1 - q_i\right) \cdot \Delta l_i,$$

где

$$q_i = \begin{cases} 1, \text{ если } i \in \overline{Q}_{\nu(k)}^k, \\ 0, \text{ если } i \in Q_{\nu(k)}^k, \end{cases}$$

а Δl_i определяется выражением (18).

П.6. $k := k + 1$.

П.7. Определить среди всех множеств допустимых решений наиболее «перспективное» множество G_r^k с минимальной оценкой $\varsigma\left(G_r^k\right)$. Перейти к п.3.

П.8. Конец.

Для уменьшения трудоемкости приведенного алгоритма изменим стратегию ветвления и введем в вычислительную схему эвристический алгоритм перераспределения проводников в сечениях, в которых превышается пропускная способность (8). С этой целью на каждом k-ом шаге работы алгоритма будем выделять множество решений $G_{\nu(k)}^k$ с минимальной оценкой $\varsigma\left(G_{\nu(k)}^k\right)$ и последовательно выбирать в нем сечения, в которых превышена пропускная способность. Если такие сечения отсутствуют, то решение $G_{\nu(k)}^k$ является решением задачи.

В противном случае для каждого φ-го сечения с превышенной пропускной способностью (φ=1, 2, …, μ; $\mu \le f$) упорядочим индексы соединений, принадлежащих подмножеству R_φ^η, следующим образом.

Сначала разобьем все индексы соединений из R_φ^η на подмножества $R_{\varphi,\xi}^\eta$, ξ=1, 2, … . В каждое подмножество $R_{\varphi,\xi}^\eta$ включим индексы соединений, имеющих одинаковую длину $\Delta l_i \mid_{i \in R_\varphi^\eta}$ (18). Затем в образованных подмножествах $R_{\varphi,\xi}^\eta$ определим отношения порядка по признаку длины соединений (количеству пересекаемых соединением сечений). Далее будем последовательно исключать соединения в соответствии с порядком следования их индексов в подмножествах $R_{\varphi,1}^\eta, R_{\varphi,2}^\eta, ...,$

начиная с $R^{\eta}_{\varphi,1}$, из множеств P^k_r или $\overline{P}^k_r$ (в зависимости от значения η) и включать их в множества $\overline{Q}^k_r$ или Q^k_r соответственно до тех пор, пока не выполнятся ограничения (19) для φ-го сечения.

В результате подобной процедуры множество допустимых решений $G^k_{\nu(k)}$ разобьется на μ подмножеств $G^k_{\nu(k)+1}, G^k_{\nu(k)+2},\ldots, G^k_{\nu(k)+\mu}$. Для каждого подмножества определим оценку $\varsigma\left(G^k_{\nu(k)+\varphi}\right)$, φ=1, 2, ..., μ (12) и перейдем к следующему шагу.

Включение в вычислительную схему метода ветвей и границ эвристического алгоритма в общем случае не позволяет получить точного решения задачи, но, как показывают исследования [5], применение подобных эвристик дает хорошие приближенные результаты, которые «в большинстве случаев достаточны, то есть достаточно хорошо удовлетворяют запросам практики» [6].

Заключение. В работе сформулирована математическая постановка и предложен точный алгоритм решения задачи распределения электрических соединений в жгуты при проводном монтаже межблочных соединений. Предельной оценкой трудоемкости алгоритма является полный перебор вариантов распределения соединений. Естественно, для задач реальной размерности применить его невозможно. Трудоемкость приближенного алгоритма существенно меньше и в принципе может быть сведена к полиномиальной оценке путем формального сокращения области определения допустимых («лучших») решений.

Следует ожидать [7], что эффективность приближенного алгоритма, созданного на базе вычислительной схемы точного метода, будет достаточно высокой. Действительно, используя эвристики для формирования окрестности, содержащей «хорошее» допустимое решение, схема точного метода будет «регулировать» выбор лучшего решения, которое, являясь в общем случае локальным оптимумом, будет заведомо не хуже любого решения, полученного тем же эвристическим алгоритмом, но без использования схемы точного метода.

Приближенный алгоритм хорошо зарекомендовал себя при «слабых» ограничениях (8), которые наиболее широко встречаются в практике конструирования реальной электронно-вычислительной аппаратуры. В случае «жестких» ограничений вопрос поиска достаточных условий для существования решения (в том числе и точного) требует дальнейшего исследования.

Библиографический список

1. *Штейн М.Е., Штейн Б.Е.* Методы машинного проектирования цифровой аппаратуры. – М.: Сов. радио, 1973. – 296 с.

2. *Форд Л., Фалкерсон Д.* Потоки в сетях. – М.: Мир, 1966. – 1276 с.

3. *Петренко А.И., Тетельбаум А.Я.* Формальное конструирование электронно-вычислительной аппаратуры. – М.: Сов. радио, 1979. – 256 с.

4. *Корбут А.А., Финкельштейн Ю.Ю.* Дискретное программирование. – М.: Наука, 1969. – 368 с.

5. *Muller – Merbach H.* Heuristics and their design: a survey// "Eur. J. Oper. Res.", 1981, 8, №1. P. 1 – 23.

6. *Финкельштейн Ю.Ю.* Приближенные методы и прикладные задачи дискретного программирования. – М.: Наука, 1976. – 264 с.

7. *Dwyer F., Evans James R.* A branch – and – bound algorithm for the list selection problem in direct mail advertising // "Manag. Sci.", 1981, v.27, № 6, p. 658 – 667.

УДК 004.8

А.Н. Пылькин, А.В. Крошилин, С.В. Крошилина

ПОСТРОЕНИЕ МОДЕЛИ ОЦЕНКИ СОСТОЯНИЯ ЗДОРОВЬЯ ПАЦИЕНТА В МЕДИЦИНСКИХ ЭКСПЕРТНЫХ СИСТЕМАХ

Рассматривается методика построения модели оценки состояния здоровья пациента в медицинских системах поддержки принятия решений на основе нечеткой логики с применением накопленной статистической информации и данных, полученных при обследовании и лечении пациентов. В качестве базовых методов решения используются семантическая сеть и математические модели.

Ключевые слова: *системы поддержки принятия решений, нечеткая логика, медицинские экспертные системы, семантическая сеть, модель состояния пациента.*

Введение. Проблема применения современных информационных технологий в обеспечении инфекционной безопасности и эффективном лечении различных инфекционных заболеваний, в том числе таких, как туберкулез, присуща ряду направлений в различных мероприятиях. Практика свидетельствует о том, что современные медицинские учреждения, в том числе диспансеры, в своей работе применяют различные автоматизированные информационные системы, позволяющие накапливать и хранить большие объемы медицинской информации, однако во многих случаях она либо не используется врачами при принятии медицинских решений, либо ее использование представляется затруднительным [1]. Другими словами, накопленная статистическая информация является практически бесполезной. Для эффективного использования в медицинской практике имеющейся статистической информации необходимо создание интеллектуальных систем, обеспечивающих оценку состояния как пациента, так и эпидемиологической обстановки в целом. В основу создания таких систем, помимо накопленных результатов, могут быть положены и результаты работы комплексов медицинских приборов для сбора широкого спектра медицинских данных, поскольку для аппаратуры, которая аккумулирует данные физических процессов, достигнуто оптимальное сочетание качества, точности и воспроизводимости результатов наблюдений пациентов, что позволит врачам оценивать влияние проведенных процедур на организм человека и постепенно формировать представления о «новых течениях болезней» [2].

Следует отметить, что, несмотря на значительность полученных результатов в области накопления, хранения и обработки медицинской информации, ее использование в интересах создания автоматизированной системы оценки состояния здоровья человека явно недостаточно. В связи с этим решаемая в предлагаемой работе задача, направленная на создание автоматизированной системы поддержки принятия медицинских решений, является актуальной.

Постановка задачи. Целями исследования являются создание и экспериментальное обоснование методики автоматизированной оценки состояния пациента и выбор метода его лечения на базе системы поддержки принятия решений, а также оценка эпидемиологической ситуации в регионе на базе эффективного анализа статистических данных.

Существуют два подхода к пониманию природы оценки медицинского решения (знания): ЭС, разработанные на фундаменте теории искусственного интеллекта, для которых в клиническом опыте преобладает дедуктивная компонента, база знаний (БЗ) которых формируется на основе эмпирических данных (ЭД), их методология опирается на общую теорию систем и теорию распознавания образов.

Медицинские решения в системах первого вида – это логические правила типа IF... THEN... ELSE, формулируемые врачами-экспертами вместе со специалистами по инженерии знаний. При таком подходе принимаемые решения не могут быть выше уровня врача-эксперта. Врач-пользователь при такой организации не может усилить эффективность информационной системы, ибо система работает уже со сформированной базой знаний и ограничена возможностями этой БЗ. В системах второго вида основное экспертное знание (медицинские решения) строится на данных истории болезни и задачах, формулируемых на языке базы данных, и хранится в эмпирической базе данных (ЭБД). В интеллектуальной системе, построенной по данному принципу, достижение цели решающим образом зависит от того, насколько эффективно происходит извлечение информации из данных истории болезни и методов лечения. Для реализации этого механизма хорошо подходит технология Data Mining с применением нечеткой кластеризации [3].

При проведении исследований за основу был взят набор обычных лечебных процессов, хранящийся в БД, хорошо апробированной на практике [4]. Далее этот набор был расширен другими лечебными процессами, на которые налагаются различные ограничения и допущения, в частности использование других лекарств, их доз и схем применения. Таким образом, автоматизация оценки состояния пациента должна функционировать с учетом информации, получаемой в результате опроса пациентов лечащим врачом; данных предварительного обследований пациентов; результатов измерений, формализованных медицинских выводов и закономерностей [5].

Формирование предложенной методики автоматизированной оценки состояния пациента основывается на следующих утверждениях.

Утверждение 1. В разрабатываемой СППР НЛ семантическая сеть, соответствующая общей модели состояния пациента, задается как двойка следующего вида:

$$S =< G, U >, \quad (1)$$

здесь G представляет собой множество характеристик, к которым относятся химические, физические и микробиологические параметры как внешних, так и внутренних факторов состояния здоровья пациента, состояния эпидемиологической ситуации вокруг пациента и условий его лечения (обеспечение медикаментами, наличие необходимого оборудования для обследования и проведения процедур), прогнозируемые события и т.д. [1], U – множество дуг, связывающих характеристики в модели состояния пациента.

Множество характеристик G можно представить в виде набора объединения нескольких множеств:

$$G = G_1 \cup G_2 \cup G_3 \cup G_4 \cup G_5, \quad (2)$$

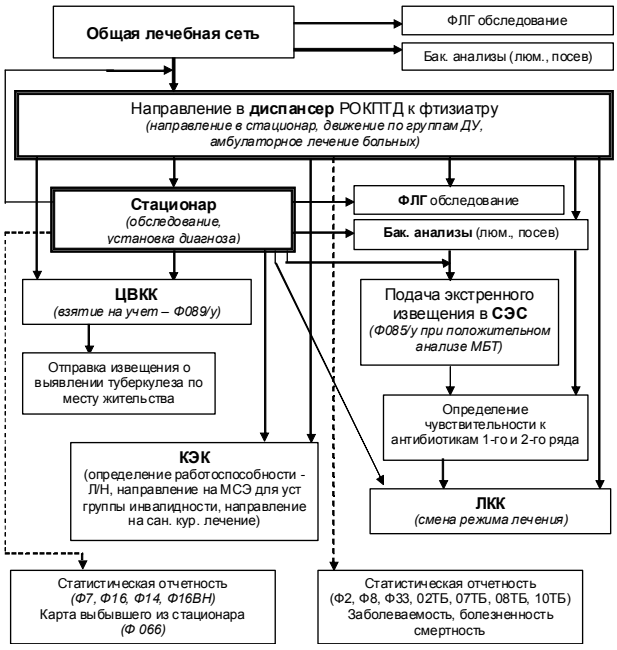
где G_1 - характеристики эпидемиологической ситуации; G_2 – характеристики медицинского учреждения; G_3 – характеристики состояния пациента; G_4 – характеристики оборудования обследования; G_5 – характеристики курса лечения и т.д.

Множество характеристик G состоит из объектов G_i семантической сети, представляющихся следующим образом:

$$G_i = \{I, P, U_{Gi}\}, \quad (3)$$

где I – название характеристики в модели состояния пациента, P – множество атрибутов, входящих или связанных с характеристикой, U_{Gi} – множество отношений между атрибутами P и характеристиками I.

Утверждение 2. Под лечением пациента в медицинском учреждении понимается возможность оценки состояния здоровья пациента согласно определенной структурной схеме, представленной на рисунке, на основе решения некоторого набора задач по нижеследующим принципам: направление пациента в диспансер; прием пациента и сбор первичной информации; предварительное обследование пациента; постановка пациента на учет (ЦВКК); оповещение по месту жительства; установка первичного диагноза; назначения анализов и сбор результатов; выбор схемы и метода лечения; плановые скрининговые обследования; смена режима лечения ЛЛК и коррекция курса лечения в зависимости от состояния пациента; индивидуализация диагностических обследований; патогенетический принцип – ориентация на выявление и диагностику наиболее вероятных прогнозируемых состояний пациента; оценка изменений состояний пациента; КЭК, определение работоспособности пациента, при необходимости направление на МСЭ; информационно-анамнестический анализ для оценки развития похожих ситуаций, предусматривающий использование информации, содержащейся в базе данных; сбор различной статистической информации по лечению пациента.



Структурная схема медицинского контроля лечения пациента

С учетом настоящего утверждения 2 для оценки состояния здоровья пациента может быть выделено множество действий, выполняемых врачом для лечения пациента M:

$$M = \{M_i\}. \quad (4)$$

Множество M_i состоит из трех частей, как и выполнение каждого действия врачом.

$$G_i = \{G`, W_i, U_{Mi}\}, \quad (5)$$

где $G`$ - набор значений некоторого множества характеристик:

$$G` = \{G_k\}, G_k \subset G, \quad (6)$$

$G`$ - множество характеристик, описывающих текущее состояние как пациента, так и среды его пребывания до и после диспансеризации. Например, элементами G_k могут являться результаты анализов, применяемы препараты и реакция пациента на них, уровень оборудования медицинского учреждения, коэффициент физического состояния пациента, оценки КЭК,

оценки правильности ведения больничного и т.д.; W_i – построенная рабочая гипотеза (оценка) о состоянии здоровья пациента; U_{Mi} – множество отношений между характеристиками $G`$ и гипотезами W_i.

Утверждение 3. Для каждого пациента формируется индивидуальная программа лечения, которая представляет собой определенную последовательность действий, направленных как на выздоровление пациента, так и на улучшение общих характеристик состояния пациента.

На каждом этапе сопровождения пациента получение данных для МП осуществляется в ходе выполнения общей схемы обследования пациента. Эта схема составляется на некоторый условный период, установленный в диспансере, с учетом представленных выше базовых принципов медицинского обследования пациента, основанных на обобщении опыта медицинского обследования пациентов и выявления информативных признаков медицинского состояния пациента. Практически это означает, что можно выделить предопределенное для общей модели состояния пациента S множество всех возможных действий, произведенных с пациентом O. Тогда любой курс лечения P_k можно представить в виде:

$$P_k = \{O_k, M_k\}, \qquad (7)$$

где $O_k \in O$, k=1,...,N, где N – общее число действий медицинского контроля для k-го пациента, которое зависит от множества $M_k \in M$ действий, выполняемых врачом для лечения k-го пациента, актуально только в некоторый фиксированный период времени. Приведем примеры действий O_k: ФЛГ обследование; бак. анализы (люм., посев); определение чувствительности к антибиотикам 1-го и 2-го ряда; взятие на учет (ЦВКК); подача экстренного извещения в СЭС (Ф085/у при положительном анализе МБТ); отправка извещения о выявлении туберкулеза по месту жительства; ЛКК (смена режима лечения); КЭК (определение работоспособности - Л/Н, направление на МСЭ для уст. группы инвалидности, направление на сан. кур. лечение); статистическая отчетность и др.

Утверждение 4. С каждым действием O_i связана одна или несколько моделей получения данных, которые могут носить регистрационный, расчетный или опросный характер.

Для получения значений характеристик $G`$ в процессе сопровождения пациента используются различные источники и каналы информации: устный опрос об их субъективном состоянии; обследование и сбор анализов – получение физиологических параметров; анализ эпидемиологического состояния в районе проживания (статистика); оценка медицинского учреждения (качество лечения); сведения о выполнении назначенных процедур и прием лекарств по назначенному курсу лечения.

Однако, обобщая, их можно свести к четырем формальным способам получения данных: расчет с использованием математических моделей (X); данные медицинской статистики (V); получение результатов медицинских анализов и показаний ФЛГ (Y); проведение опроса пациента о самочувствии (Z).

Математические модели X представляют собой совокупность вычислительных методов и расчетных коэффициентов для формализации получаемых посредством медицинских анализов и/или опроса данных к виду, который система способна обработать и использовать для осуществления оценки состояния пациента.

Данные медицинской статистики V получаются из статистических данных, накопленных в системе по конкретному району пациента, а также по всей эпидемиологической ситуации по области в целом. В анализе участвует информация по численности населения, по количеству заболевших в заданный период, количеству успешно пролеченных больных, числу неподтвержденных диагнозов, числу летальных исходов, длительности лечения и другие данные, используемые для анализа и получения статистической информации по данному виду заболевания.

Получение результатов медицинских анализов и показаний ФЛГ Y – это результаты бактериологических анализов и результаты ФЛГ обследования, представленные в виде цифровых коэффициентов в удобном виде для обработке в системе. Отметим, что в системе имеется возможность хранить ФЛГ снимки в специальной БД, а также результаты других дополнительных медицинских исследований, проведенных над пациентом в период лечения.

Опрос заключается в заполнении нескольких видов анкет пациента (Z), в том числе и при первом приеме, обработка которых позволяет выявить жалобы на самочувствие и общее состояние в целом.

Однако необходимо заметить, что независимо от источника значений, важности и характера принадлежности, элементы множеств X, V, Y и Z можно представить как частный случай общей модели состояния пациента S:

$$S_j = < G^j, U_j >, \qquad (8)$$

где $G^j \subset G$, а $U_j \subset U$ общей модели состояния

пациента *S*.

Согласно формуле (3) представим G_j в следующем виде:

$$G_i^j = \{I^j, P^j, U_{Gi}^j\}, \quad (9)$$

где G^j_i – *i*-я характеристика *j*-го пациента, I^j – название характеристики в модели состояния *j*-го пациента, P^j – множество атрибутов, входящих или связанных с характеристикой, U^j_{Gj} - множество отношений между атрибутами P^j и характеристиками I^j.

В реальной ситуации для каждого конкретного пациента (даже для достаточно опытного врача) бывает затруднительно определить степень значимости атрибутов для оцениваемой характеристики, поэтому в системе отношения между атрибутами характеристики строятся с помощью различных степеней зависимости. Типы градуируемых связей рассматриваются как нечеткие объектные связи [3].

Множество отношений между атрибутами U^j_{Gi} определяется как множество двоек из T и U^G_{IP}:

$$U_{Gi}^j = \{T, U_{IP}^G\}, \quad (10)$$

где T определяет тип критерия оценки характеристики, U^G_{IP} представляет собой нечеткое подмножество, которое показывает степень зависимости между характеристикой состояния пациента и значимостью ее атрибутов (степень значимости характеристики для оценки общего состояния пациента для конкретной ситуации). Тип объекта T определяет два вида критерия оценки: $T = \{t1, t2\}$, где $t1$ – критерий оценки ситуации, $t2$ – критерий оценки рекомендации.

U^G_{IP} определяется как:

$$U_{IP}^G = U` = (\mu_{U`}(P_i^j, I^j) \mid P_i^j \in P, I^j \in G^j), \quad (11)$$

где $i = 1...n$, P^j_i – атрибуты, принадлежащие характеристике G^j_i, n – количество понятий для характеристики.

Таким образом, характеристику G^j_i, соответствующую критерию $\tilde{G}^j_i$ с неопределенными и фиксированными атрибутами, можно определить так:

$$\tilde{G}_i^j = G` = \begin{Bmatrix} I_i^j, P_1^j, ..., P_n^j, t_{P_i i1}, ..., t_{Pin}, \\ \{\mu_{G`}(I_i^j, P_1^j), ..., \mu_{G`}(I_i^j, P_n^j)\} \end{Bmatrix}, \quad (12)$$

где I^j_i – информационная часть *i*-й характеристики состояния пациента, P^j_i – множество понятий, принадлежащих *i*-й характеристике *j*-го пациента, t_{Pjl} – тип критерия оценки, $\mu_{G`}(I^j_i, P^j_l)$ - отношение близости понятия P^j_l и названия критерия I^j_i. Зависимость между узлами будет строиться на основе взаимосвязи между понятиями критериев оценки. Далее введем нечеткое отношение определяющее близость понятий между собой:

$$U_{Pik}^j = \mu_S(P_i^j, P_k^j). \quad (13)$$

На его основе формируется нечеткое подмножество U^j_P для *j*-го пациента:

$$U_P^j = \begin{Bmatrix} P_i^j, P_k^j, \mu_S(P_i^j, P_k^j) \mid P_i^j \in P, \\ P_k^j \in P, i, k = 1..N \end{Bmatrix}, \quad (14)$$

где N – количество понятий характеристик в системе.

Связь между операциями O_k и моделями S_j строится с помощью метода выбора по отношениям предпочтения $pf(O_k,S_j)$. Она определяется содержательными представлениями о понятии «предпочтения» выбора из двух моделей. Наличие между двумя вариантами S_i, $S_j \in S$ отношения >, записываемого как $S_i > S_j$, содержательно интерпретируется как «вариант S_i предпочтительнее, чем вариант S_j».

Утверждение 5. Существует модель развития ситуации по лечению пациента. Построение рабочей гипотезы о состоянии той или иной системы организма пациента и оценки общего состояния пациента осуществляется на основе данных, полученных в ходе выполнения программы лечения P_k, и на следующем шаге принимается решение о применении той или иной модели.

В результате сбора медицинских данных, характеризующих состояние здоровья пациента на шаге m_{i+1} (предполагается, что уже было выполнено m_i шагов), осуществляется построение рабочей гипотезы о состоянии пациента. Гипотеза базируется не только на данных анамнеза, но и на результатах анализа - объективных исследований, проводимых в соответствии с рекомендациями или по показаниям системы (или лечащего врача), и информации, полученной из всех вышеприведенных источников.

Модель развития ситуации по лечению больного (оценка состояния здоровья пациента) представляет собой множество:

$$MZP^k = \{MZP_i^k\}, \quad (15)$$

где $i=1..n$, n – количество шагов в модели *k*-го пациента, MZP^k_i – набор медицинских выводов, которые могут быть сделаны на основе результатов выполнения курса лечения P_{ki}.

Для формирования выводов исходными данными кроме значений характеристик множества G, также являются статистическая

база данных анамнезов и личных данных пациентов и оценки достоверности отклонений медицинских показателей в различных анализах. В статистической базе данных информация условно разделена на четыре группы: личные данные пациента, анамнез, данные по регионам и социальная информация. К личным данным относится вся необходимая информация по пациенту. К данным анамнеза относятся: особенности медицинского характера пациента, перенесенные заболевания, хронические заболевания, медицинские данные по предыдущим курсам лечения (при рецидивах). Данные по регионам включают численность населения, показатели заболеваемости, болезненности, смертности, эффективности лечения. Социальная информация включает в себя: социальный статус пациента, круг общения, группы рисков. В статистической базе данных для всех характеристик присутствуют оценки полноты и достоверности этих показателей. Для данных проводится совокупная оценка достоверности. Достоверными считаются те данные, совокупная оценка достоверности которых соответствует определенному уровню. Значения характеристик (извлеченные из СБД или полученные в результате работы системы), которые оценены как достоверные, поступают в базу знаний и используются для формирования или коррекции множества правил вывода *PV* и непосредственно для получения самих этих выводов *MZP*.

При построении базы знаний применялся метод нечеткой кластеризации для эффективного мониторинга статистической информации [6]. Его суть в интерактивном исследовании данных статистической информации с целью получения представления о типах переменных, используемых в анализе, и возможных взаимосвязей между ними. Задача кластеризации заключается в разбиении конечного множества значений медицинских показателей $G = \{g_1, g_2, ..., g_i, ..., g_n\}$ на группы (кластеры) по некоторым атрибутам. Каждый из элементов g_i характеризуется m-компонентным атрибутным описанием $g_i(x_{i1}, x_{i2}, ..., x_{ik}, ..., x_{im})$, где $x_{ik} \in X_{ik}$, X_{ik} – допустимое множество значений атрибута. Необходимо построить множество кластеров K и отображение $E: G \to K$. Структура кластера: $k_h = \{g_j, g_p: g_j, g_p \in G, d(g_j, g_p) < \psi\}$, где $k_h \in K$, k_h – кластер [6].

В результате пользователю предоставляется инструмент анализа, сочетающий графические и расчетные методы, который позволит быстро определять распределения значений медицинских показателей и связи между ними для получения наилучших результатов лечения пациентов, а также определять закономерности, принадлежащие неким специфическим кластерам данных.

Для реализации вышеуказанного метода использовался алгоритм кластеризации на базе нечеткого отношения равнозначности, позволяющий эффективно выявлять в обрабатываемых данных кластеры с применением разработанной нечеткой оценочной функции, которая позволяет оценить качество проведенной кластеризации. Этот алгоритм входит в состав «Интеллектуальной аналитической системы мониторинга пациентов на основе нечеткой кластеризации для медицинских учреждений «Диспансер» ver.4.0» [7].

Заключение. Проведен анализ структуры и методов лечения пациентов в условиях стационарного и амбулаторного лечения и показано, что важнейшим условием успешного курса лечения является создание системы информационно-медицинского обеспечения, адекватной особенностям (условиям и факторам) нечеткой информации и выводов в ходе лечения. Существенная роль в справочно-рекомендательном обеспечении курса лечения принадлежит системам поддержки принятия решений на основе нечеткой логики, базам данных статистической и динамической информации, а также современным технологиям сбора медицинских данных по здоровью пациента, которые позволяют наиболее оперативно принимать решения относительно состояния пациента.

Сформирована методика построения модели комплексной оценки состояния здоровья пациента и проводимого курса лечения, которая позволяет осуществлять адекватную поддержку в принятии решений на основе данных медицинского контроля, статистических данных, истории болезни, а также позволяет решать задачу корректировки курса лечения, необходимого для получения желаемого результата.

На базе этой методики разработана новая система поддержки принятия решений «Диспансер» [7], которая позволяет осуществлять оперативное диагностирование состояния здоровья пациента в ходе курса лечения и принимать решение о необходимости внесения корректировок в курс лечения. Созданная система была успешно апробирована и внедрена в ГУЗ «Рязанский областной клинический противотуберкулезный диспансер». Тестирование и экспертная оценка показали, что предлагаемые системой рекомендации являются достоверными с медицинской точки зрения не менее чем в 86 % случаев [4] и представляют

практическую значимость для решения задачи оценки состояния здоровья пациента при проведении курса лечения.

Библиографический список

1. *Каширин И.Ю., Крошилин А.В., Крошилина С.В.* Автоматизированный анализ деятельности предприятия с использованием семантических сетей. - М.: Горячая линия - Телеком, 2011. – 140 с.: ил.

2. *Пылькин А.Н., Крошилин А.В., Крошилина С.В.* Математические и компьютерные методы в медицине, биологии и экологии: монография / под науч. ред. В.И.Левина.-Пенза; Москва: Приволжский дом знаний; МИЭМП, 2012. С. 29-44.

3. *Пылькин А.Н., Крошилин А.В., Крошилина С.В.* Управление экономическими системами: монография / под общ. ред. Б.Н.Герасимова.-Самара; Пенза: Приволжский дом знаний, 2010. С. 206-217.

4. *Крошилин А.В., Виноградова Л.И.* Внедрение информационных технологий в Рязанском областном клиническом противотуберкулезном диспансере // Анналы рязанской фтизиатрии: сборник научно-практических работ / под ред. В.Л. Дробина. – Рязань, 2000. С. 33-43.

5. *Крошилин А.В., Крошилина С.В.* Формализация экспертных знаний в системах поддержки принятия решений //Ползуновский вестник. № 2. Измерение, информация, моделирование: проблемы и перспективы технологий разработки и применения (тематический выпуск).– Барнаул: АлтГТУ, 2010. С. 181-185.

6. *Крошилин А.В.* Применение нечеткой кластеризации для эффективного мониторинга статистической информации в системах неопределенности// Вестник РГРТУ. №2 (выпуск 32). - Рязань: РГРТУ, 2010. С. 71-76.

7. Свидетельство о государственной регистрации программ для ЭВМ от 31.03.2010 г. №2010612339 «Интеллектуальная аналитическая система мониторинга пациентов на основе нечеткой кластеризации для медицинских учреждений «Диспансер» ver. 4.0.».

УДК 81'322

А.В. Пруцков, Д.М. Цыбулько

ИНТЕРНЕТ-ПРИЛОЖЕНИЕ МЕТОДА ОБРАБОТКИ КОЛИЧЕСТВЕННЫХ ЧИСЛИТЕЛЬНЫХ ЕСТЕСТВЕННЫХ ЯЗЫКОВ

Предложена реализация метода обработки количественных числительных естественных языков в виде интернет-приложения. Проведен сравнительный анализ аналогичных ресурсов, и выявлены преимущества данного подхода к обработке числительных: простота расширения числа поддерживаемых языков, реализация генерации и определения числительных, возможность реализации системы проверки знаний по данной теме. Реализована поддержка пяти естественных языков: русского, английского, немецкого, испанского и финского. Разработанное приложение размещено в сети Интернет и доступно для всех пользователей.

***Ключевые слова**: автоматическая обработка текста, машинный перевод, обработка количественных числительных.*

Введение. «Современная языковая ситуация, при которой знание иностранного языка все в большей мере становится залогом социального успеха, требует активизации практических и научных разработок в области методики, теории и практики преподавания иностранных языков и активизации применения технических средств в изучении вообще языков, в том числе и родного» [1].

Применение технических средств в изучении естественных языков позволяет сделать обучение более интересным, простым в организации и доступным для большего числа пользователей образовательных услуг.

В настоящее время разработано большое число различных автоматизированных обучающих систем по всем разделам языкознания. Важное значение имеет обучение образованию количественных числительных, так как числа стали неотъемлемой частью нашей жизни.

Ранее был разработан метод обработки количественных числительных естественных языков [2] и было предложено использовать его для перевода, обучения и проверки знаний правил образования количественных числительных естественных языков различных групп и семейств [3].

Предложенный метод обработки количественных числительных имеет преимущества перед другими подходами к решению данной задачи: простоту реализации и расширения числа поддерживаемых языков.

Данный метод реализован в виде информационной системы проверки знаний образования количественных числительных естественных языков BRETTA [4]. Разработанная информационная система выполнена в виде приложения операционной системы Microsoft Windows, что ограничивает область ее распространения и имеет ряд ограничений по функциональности.

Целью работы является разработка интернет-приложения, позволяющего переводить количественные числительные естественных языков различных семейств и групп и включающего систему проверки знаний по данному разделу языкознания. Данное интернет-приложение расширит круг заинтересованных пользователей.

Интернет-приложение является развитием системы BRETTA и расширяет ее функциональность за счет реализации следующих функций:

- автоматически распознавать язык ввода;
- генерировать количественное числительное в данном падеже;
- определять падеж количественного числительного.

Для реализации данных функций необходимо разработать соответствующие алгоритмы.

Краткая характеристика метода обработки количественных числительных. Введем следующие обозначения.

Число – это количественное числительное, записанное в цифровой форме (например, «352»).

Числительное – количественное числительное, записанное в символьной форме (например, «*триста пятьдесят два*»).

В основе метода обработки количественных числительных лежит трехуровневая обобщенная модель числительного, которая является промежуточным этапом во всех операциях с числительными (рисунок 1).

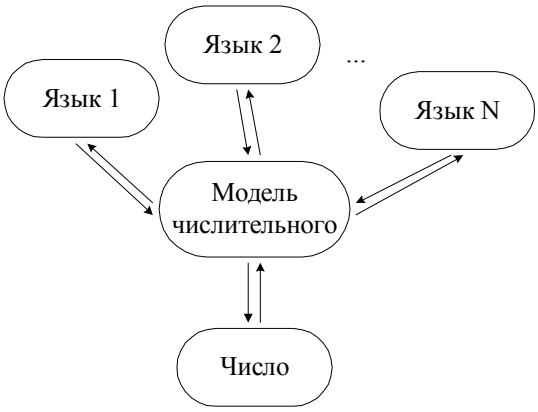


Рисунок 1 – Схема обработки числительных

Преимущество такой организации преобразования числительных заключается в том, что для добавления нового языка необходимо написать всего два алгоритма, связывающих язык с моделью. После этого становится доступным перевод числительного этого языка на все поддерживаемые языки. В настоящее время реализована поддержка пяти естественных языков: русского, английского, немецкого, испанского и финского.

Для поддерживаемых языков составлены таблицы соответствия обозначений языков и обозначений модели. Обозначения модели – это обобщенные составляющие числительных (единицы, десятки, сотни, тысячи и т. д.), не зависящие от естественного языка. Обозначения модели приведены в работе [2]. Обозначения языка – это составляющие числительных данного языка. Например, обозначение модели $C_1D_1C_7$ соответствует обозначению русского языка «*_семнадцать*» (знак подчеркивания обозначает пробел).

Генерация и определение числительных. Генерация формы слова – процесс получения формы с использованием в качестве начальных параметров основы и грамматического значения. Определение заключается в нахождении по данной словоформе ее нормальной формы (основы) и грамматического значения. Для генерации и определения числительных можно было бы использовать предложенный универсальный метод генерации и определения форм слов естественных языков [5]. Однако в силу того, что число обозначений языка составляет примерно 50 (в зависимости от языка), было принято решение использовать словарь словоформ составляющих числительных. Это позволило легко добавить функцию генерации и определения числительных в существующие алгоритмы их обработки. Для этого падежи естественного языка описаны как отдельные языки. Генерация и определение реализованы для числительных русского языка.

Алгоритм распознавания языка ввода. Алгоритм получает в качестве входных данных числительное (рисунок 2). Результатом работы алгоритма должен быть список языков числительного. Работа алгоритма заключается в замене обозначений языка обозначениями модели. Если все обозначения языка заменены, то числительное относится к данному языку и язык заносится в результирующий список. Данная последовательность действий выполняется для всех поддерживаемых интернет-приложением языков.

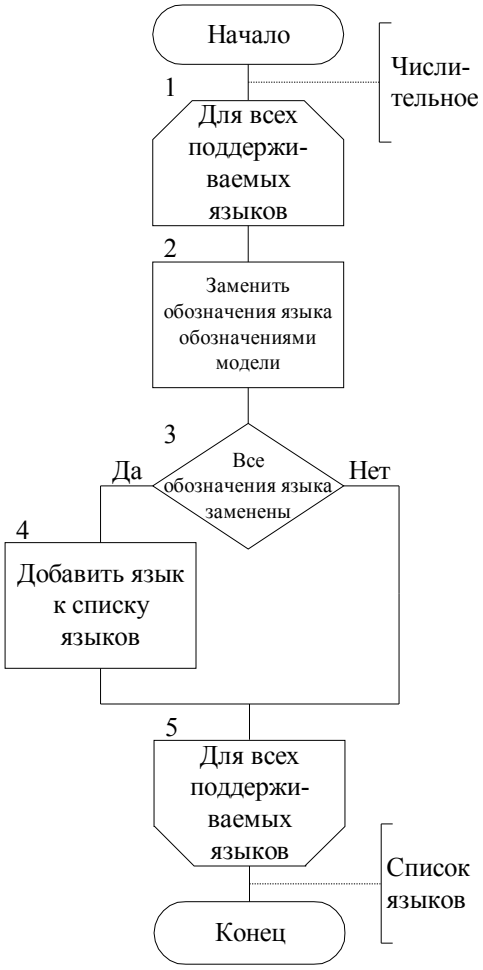


Рисунок 2 – Алгоритм распознавания языка

Обозначения языков представляют непересекающиеся множества, поэтому распознавание языка однозначно. Исключения могут быть для родственных языков и их диалектов. Однако в данном интернет-приложении такие языки отсутствуют.

Структура интернет-приложения. Разработанное приложение, как и другие интернет-приложения, состоит из двух частей: клиентской и серверной.

Задачами клиентской части являются предоставление пользователю интерфейса, ввод данных, отсылка их на сервер и представление ответа сервера в наглядном виде пользователю. Клиентская часть реализована с помощью языка гипертекстовой разметки HTML, языка программирования JavaScript и технологии Ajax.

Серверная часть выполняет следующие задачи: прием данных от клиентской части (исходного числительного или числа и направления перевода); распознавание языка ввода числительного; проверка правильности записи числительного; генерация и определение числительных; отправка результата обработки числительных клиентской части. Серверная часть реализована на языке программирования PHP.

Система проверки знаний правил образования числительных. Изучение языка невозможно без практики. Отличительной особенностью разработанного интернет-приложения является система проверки знаний правил образования числительных, которая может также использоваться для практических занятий.

Тестируемый может задать следующие параметры проверки знаний: исходный и результирующий формат числительных; диапазон значений, из которых будет выбираться числительное; количество вопросов.

Проверка знаний проходит в виде последовательной выдачи вопросов тестируемому. При этом он может вернуться к любому предыдущему вопросу.

В конце система выдает статистику проверки знаний: заданные вопросы, данные тестируемым ответы и правильные ответы. Это позволяет тестируемому самостоятельно выявить свои ошибки и наметить направления их исправления. Проверка знаний в данной системе предназначена для самоконтроля.

Сравнение разработанного интернет-приложения с аналогичными ресурсами. Дадим краткую характеристику нескольким ресурсам, решающим аналогичные задачи.

Переводчик Google (http://translate.google.com) работает на основе технологии статистического машинного перевода (МП), называемой также Translation Memory или Sentence Memory, которая заключается в следующем. Человек-профессиональный переводчик переводит текст с одного естественного языка на другой естественный язык. Исходный и переведенный тексты вводятся в ЭВМ. С помощью специальных алгоритмов данные тексты разделяются на фрагменты, причем каждый фрагмент имеет переводной эквивалент, и индексируются для поиска. Из фрагментов строится база переводных соответствий. Тогда МП сводится к поиску переводимого фрагмента в базе переводных соответствий и выделению соответствующего ему перевода. «Не переводить один и тот же текст дважды» – основная идея технологии Translation Memory.

Данная технология обладает следующими достоинствами: «сокращение трудоемкости построения таких систем по сравнению с традиционными подходами к МП; отказ от ручного составления машинных словарей и грамматик; если в логике системы обнаруживается ошибка, ее устранение в худшем

случае означает необходимость повторного запуска процедуры извлечения параметров из корпуса примеров, а не ручное переписывание этих ресурсов» [1].

Основной недостаток технологии Translation Memory заключается в том, что «базы переводных соответствий, построенные для однородных текстов одного предприятия, пригодны лишь для однородных текстов, близких по профилю предприятий, так как предложения и большие фрагменты предложений, извлекаемые из текстов одних документов, как правило, не встречаются или очень редко встречаются в текстах других документов» [6]. Данное обстоятельство снижает качество МП с помощью данной технологии. Другим недостатком технологии Translation Memory и переводчика Google является то, что для каждой пары языков необходимо иметь исходный и переведенный тексты, что увеличивает трудоемкость реализации системы МП.

Переводчик Yahoo (http://babelfish.yahoo.com) осуществляет перевод числительных нескольких языков на английский и французский языки и обратно.

Переводчики Google и Yahoo являются универсальными системами МП.

Ресурс Languages And Numbers (http://www.languagesandnumbers.com) содержит автоматический переводчик большого числа языков, в том числе и 36 искусственных, а также краткое описание правил образования количественных числительных.

Переводчик числительных eng5.ru (http://eng5.ru/translator/numbers/) является частью одноименного портала, предназначенного для обучения английскому языку. Особенностями ресурса является преобразование числа в числительное русского, британского и американского английского языков и склонение числительных русского языка по родам.

Сравнение предлагаемого интернет-приложения с аналогичными переводчиками по нескольким критериям приведено в следующей таблице.

Критерии	Переводчик Google	Переводчик Yahoo	Ресурс Languages And Numbers	Ресурс eng5.ru	Предлагаемое интернет-приложение
Количество поддерживаемых языков	64	13	155	3	5
Количество направлений перевода	4 032[1]	38	155	3	30
Преобразования «Числительное-Число»/ «Числительное-Числительное» / «Число-Числительное»	+/+/+[2]	–/+/–	–/–/+	–/–/+	+/+/+
Обработка дробной части числительного	–	–	–	+	+
Склонение по родам русского языка	–	–	–	+	–
Генерация и определение числительных русского языка	±[3]	–	–	–	+
Автоматическое распознавание языка ввода	+	–	–	–	+
Система проверки знаний по данной теме	–	–	–	–	+

[1] указано максимальное число направлений, не все из них реализованы

[2] не все направления реализованы

[3] только преобразование числительного любого падежа в число без определения грамматического значения

Предложенное интернет-приложение предоставляет пользователю функции, отсутствующие у других ресурсов. Небольшое число поддерживаемых языков может быть легко увеличено написанием для каждого нового языка двух алгоритмов, связывающих его с моделью числительного. Для поддержки 64 естественных языков необходимо было бы написать $64 \times 2 = 128$ алгоритмов при преобразовании числительных с использованием модели числительного в качестве промежуточного этапа. В переводчике Google и других системах, использующих парный перевод, необходимо написать $64 \times 63 = 4\,032$ алгоритма.

Заключение. Разработано интернет-приложение обработки количественных числительных естественных языков, которое имеет преимущества перед аналогичными ресурсами: простота расширения количества поддерживаемых языков, генерация и определение числительных,

автоматическое распознавание языка ввода; наличие системы проверки знаний по данной теме. Направлениями дальнейшего развития являются поддержка десятичного знака, зависящего от языка, и контекстной помощи.

Серверная и клиентская части данного интернет-приложения протестированы, а выявленные ошибки исправлены.

Интернет-приложение обработки числительных доступно по адресу http://dreamland.ismywebsite.com/numbers/ и зарегистрировано в популярных поисковых системах сети Интернет.

Интернет-приложение обработки количественных числительных естественных языков разработано в рамках нескольких НИР.

Библиографический список

1. *Марчук Ю.Н.* Компьютерная лингвистика. – М.: АСТ; Восток-Запад, 2007. – 317 с.

2. *Пруцков А.В.* Обработка числительных естественных языков с помощью формальных грамматик и нормальных алгоритмов Маркова // Вестник Рязанского государственного радиотехнического университета. – 2009. – Вып. 28. – С. 49-55.

3. *Пруцков А.В.* Статический и динамический подходы к проектированию подсистем проверки знаний автоматизированных обучающих систем // Информационные ресурсы России. – 2006. – № 1. – С. 27-29.

4. Свидетельство о государственной регистрации программы для ЭВМ № 2011615475, Российская Федерация. Информационная система проверки знаний по правилам образования количественных числительных (BRETTA) / А.В. Пруцков, А.А. Суворов. Зарегистрировано в РОСПАТЕНТ 13.07.2011, заявка № 2011613616.

5. *Prutskov A.V.* Algorithmic Provision of a Universal Method for Word-Form Generation and Recognition // Automatic Documentation and Mathematical Linguistics, 2011, Vol. 45, No. 5, pp. 232-238.

6. Каким быть машинному переводу в XXI веке / Белоногов Г.Г., Хорошилов Ал-др А., Хорошилов Ал-сей А. и др. // В кн. Перевод: традиции и современные технологии. – М.: ВЦП, 2002. – С. 56-69.

УДК 512.563

В.В. Тарасов, В.А. Саблина

БУЛЕВЫ УРАВНЕНИЯ В ЗАДАЧАХ КРИПТОГРАФИИ И РАСПОЗНАВАНИЯ ОБРАЗОВ

Предлагается аппарат булевых уравнений с одной и двумя неизвестными функциями с возможным использованием в криптографии и распознавании образов.

Ключевые слова: *булевы уравнения, криптография, распознавание образов.*

Введение. Вопросы решения булевых уравнений ставятся в основном в учебной литературе по дискретной математике [1, 2, 3]. Есть примеры применения булевых уравнений в технической литературе [4]. Наблюдается недостаток в точности описания типов булевых уравнений и способов представления их как в теоретическом, так и в практическом плане. Поэтому целью настоящей работы является уточнение основных понятий булевых уравнений и указание возможного их применения в задачах распознавания.

Цель работы. Выявить, какие типы булевых уравнений имеют практическую целесообразность; исследовать методы решений, свойства решений и методы описания решений.

Основная часть

1. Информацию в памяти компьютера можно представить в виде булевой функции. Пусть A – алфавит знаков, в котором пишутся тексты. С каждой буквой (знаком) сопоставляется некоторый двоичный код длины (высоты) h (желательно брать h как степень двойки). Булеву функцию $T(x_1,...,x_n)$ представим таблицей с двумя входами, где k – параметр таблицы.

Таблица разбита на полосы по h строк в каждой полосе, всего $2^{k-\log_2 h}$ полос. Полоса состоит из столбцов высотой h. Можно считать, что таблица содержит построчно некоторый текст в алфавите A.

Булева функция

$T(x_1,...,x_n)$	x_n	0	σ_n	1	
	$\vdots$	$\vdots$	$\vdots$	$\vdots$	
	x_{k+1}	0	σ_{k+1}	1	
$x_1,..,x_k$					
0...0		...	...	...	$\}h_{строк}$
...		...	...	...	$\}h_{строк}$
$\sigma_1...\sigma_k$		...	$T(\tilde{\sigma})$	...	...
...		...	...	...	
1...1		...	...	...	$\}h_{строк}$

Для того чтобы текст был лучше защищен от прочтения злоумышленниками (хакерами), надо зашифровать его, чтобы осложнить его понимание. Можно предложить следующую модель шифрования:

$$F(x_1,...,x_n,T(x_1,...,x_n))=Sh(x_1,...,x_n), \qquad (1)$$

где $Sh(x_1,...,x_n)$ – шифр текста, F – булева функция от $n+1$ переменных, осуществляющая шифрование. Тогда мы имеем булево уравнение (1). Если шифр $Sh(x_1,...,x_n)$ и F известны, то текст $T(x_1,...,x_n)$ может быть найден как решение уравнения (1). Поэтому математически нужно уже в общем случае выяснить, когда уравнение имеет решение и притом единственное.

2. Определим понятие булева поля. Пусть Ω - ограниченная плоская область, разбитая на ячейки прямоугольной сеткой. Каждая ячейка может находиться в трех состояниях: 0, 1, пусто. Таково поле игры «крестики и нолики», поле игры «русские шашки», поле игры «уголки». Можно допустить, что это сечение мышечной ткани, рассмотренное на клеточном уровне, где 0 - состояние «клетка не возбуждена», 1 - состояние «клетка возбуждена», пусто - состояние «клетка мертва» и т.д. Над булевым полем можно ввести булеву систему координат (см. таблицу) и представить состояние булева поля в виде пары двух булевых функций $(f_1(\tilde{x}), f_2(\tilde{x}))$, где $f_1(\tilde{\sigma}) = f_2(\tilde{\sigma})$ всякий раз, когда соответствующая ячейка с координатами $(\sigma_1,...,\sigma_k)$ (булев номер строки) и $(\sigma_{k+1},...,\sigma_n)$ (булев номер столбца) находится в определенном состоянии 0 или 1 и $f_1(\tilde{\sigma})=0, f_2(\tilde{\sigma})=1$, если на пересечении $(\sigma_1,...,\sigma_k)$-й строки и $(\sigma_{k+1},...,\sigma_n)$-го столбца ячейка со значением $f(\tilde{\sigma})$ – пусто.

Рассмотрим пример из теории распознавания образов.

Пусть $E_1(\tilde{x}),...,E_s(\tilde{x})$ – эталонная информация об s объектах. Требуется распознать, к какому эталону следует отнести неизвестный объект, заданный в виде булева поля, то есть парой функций (f_1, f_2). Иначе, существует ли решение $u_i(\tilde{x})$ булева уравнения

$$F(\tilde{x}, u_i(\tilde{x}), f_1(\tilde{x}), f_2(\tilde{x}))=E_i(\tilde{x}) \qquad (2)$$

для подходящего $i, 1\le i\le s, f_1(\tilde{x})\le u_i(\tilde{x})\le f_2(\tilde{x})$, где F – булев оператор, осуществляющий обработку информации (приведение к эталону (2)).

3. Приведем еще один пример из теории распознавания образов. Пусть A и B – два независимых наблюдателя (гипотетически) одного и того же явления. Наблюдатель A представил это явление в виде функции алгебры логики

$$F_1(\tilde{x}, \tilde{y}, u(\tilde{x}, \tilde{y}, \tilde{z})), \qquad (3)$$

а наблюдатель В в виде функции

$$F_2(\tilde{x}, \tilde{z}, v(\tilde{x}, \tilde{y}, \tilde{z})), \qquad (4)$$

где $\tilde{x}, \tilde{y}, \tilde{z}$ – группы индикаторов-признаков. Оба наблюдателя отметили общую группу признаков $\tilde{x}$. Каждый из наблюдателей отмечает и свои собственные группы признаков $\tilde{y}$ и $\tilde{z}$ соответственно у наблюдателей А и В. Через неизвестные функции $u(\tilde{x}, \tilde{y}, \tilde{z})$ и $v(\tilde{x}, \tilde{y}, \tilde{z})$ по обоюдному соглашению наблюдателей обозначены функции, содержащие неизвестную для каждого информацию. Поскольку оба наблюдали одно и то же явление, то следует приравнять (3) и (4):

$$F_1(\tilde{x}, \tilde{y}, u(\tilde{x}, \tilde{y}, \tilde{z}))=F_2(\tilde{x}, \tilde{z}, v(\tilde{x}, \tilde{y}, \tilde{z})),$$

где F_1 и F_2 – булевы операторы обработки информации.

Получено булево уравнение с двумя неизвестными функциями. Если полученное уравнение не имеет решения, то есть основание считать, что оба наблюдателя говорят о разном.

4. Теперь перейдем к теории булевых уравнений.

Теорема 1. *Булево уравнение*

$$f(\tilde{x}, u)=0, \qquad (5)$$

где $\tilde{x}=(x_1,...,x_n)$, $u=u(x_1,...,x_n)$ *– неизвестная функция, либо не имеет решений, либо*

множество решений является интервалом $f(\tilde{x},0)\le u\le\overline{f(\tilde{x},1)}$.

Δ Раскладываем левую часть уравнения (5) по переменной u:

$$\bar{u}\ f(\tilde{x},0)\vee u\ f(\tilde{x},1)=0,$$

что равносильно системе уравнений

$$\begin{cases}\bar{u}\ f(\tilde{x},0)=0,\\ u\ f(\tilde{x},1)=0,\end{cases}\qquad(6)$$

В свою очередь, (6) эквивалентно двойному неравенству

$$f(\tilde{x},0)\le u\le\overline{f(\tilde{x},1)},$$

которое выражает общее решение уравнения (5), если выполняется условие

$$f(\tilde{x},0)\le\overline{f(\tilde{x},1)}.\qquad(7)$$

Из (7) легко получаем условие единственности решения:

$$f(\tilde{x},0)=f(\tilde{x},1).\qquad(8)$$

Если не выполняется (7), то мы имеем условие отсутствия решения. ▲

Следствие 1. *(Обратная задача). Пусть выполнено двойное неравенство*

$$\varphi(\tilde{x})<u\le\psi(\tilde{x}),\qquad(9)$$

тогда существует булево уравнение (5), множество решений которого описывается двойным неравенством (9).

Δ Рассмотрим функцию

$$f(\tilde{x},u)=\begin{cases}\varphi(\tilde{x}),\text{ если } u=0,\\ \bar{\psi}(\tilde{x}),\text{ если } u=1.\end{cases}$$

Тогда имеем:

$$f(\tilde{x},u)=\bar{u}\ \varphi(\tilde{x})\vee u\ \bar{\psi}(\tilde{x})=\bar{u}\ f(\tilde{x},0)\vee u\ f(\tilde{x},1),$$

а решение уравнения $f(\tilde{x},u)=0$ приводит к общему решению (9).▲

Следствие 2. *Число булевых уравнений (5) с непустым множеством решений равно* 3^{2^n}. *Вероятность того, что заранее заданное случайное булево уравнение имеет непустое множество решений, равна* $(3/4)^{2n}$.

Δ Рассмотрим k-й ярус m-мерного единичного куба, $m=2^n$. Пусть $\tilde{\sigma}$ – какая-нибудь вершина k-го яруса – строка значений функции $f(\tilde{x},0)$. Набор $\tilde{\sigma}$ имеет k единиц и $m-k$ нулей. Вершина на k-м ярусе может быть выбрана C_m^k способами – это число выбора левого конца интервала решений. Другой правый конец $\tilde{\tau}$ интервала решений выбираем из интервала $\tilde{\sigma}\le\tilde{\tau}\le\tilde{1}$, где $\tilde{\tau}$ – строка значений функции $\overline{f(\tilde{x},1)}$. Функция $\overline{f(\tilde{x},1)}$ может быть выбрана $2^{\rho(\tilde{\sigma},\tilde{1})}$ способами ($\rho(\tilde{\sigma},\tilde{1})$ – число нулей в наборе $\tilde{\sigma}$). Таким образом, при фиксированном значении k число двойных неравенств (решений) равно $C_m^k\cdot 2^{m-k}=C_m^{m-k}\cdot 2^{m-k}$. Отсюда остается суммировать по k:

$$\sum_{k=0}^{m}C_m^{m-k}\cdot 2^{m-k}=\sum_{k=0}^{m}C_m^k\cdot 2^{m-k}\cdot 1^k=$$

$$=(1+2)^m=3^m=3^{2^n}.$$

Отсюда вероятность того, что случайным образом выбранное уравнение будет иметь непустое множество решений, равна

$$\frac{3^{2^n}}{2^{2^{n+1}}}=\frac{3^{2^n}}{2^{2^n+2^n}}=\frac{3^{2^n}}{2^{2^n}\cdot 2^{2^n}}=\frac{3^{2^n}}{4^{2^n}}=\left(\frac{3}{4}\right)^{2n}.\ ▲$$

Теорема 2. *Общее решение булева уравнения* $f(\tilde{x},u,v)=0$ *с двумя неизвестными функциями* $u(\tilde{x}),v(\tilde{x})$ *может быть записано в виде:*

$$\begin{cases}f(\tilde{x},0,0)f(\tilde{x},1,0)\le v\le\overline{f(\tilde{x},0,1)f(\tilde{x},1,1)},\\ f(\tilde{x},0,v)\le u\le\overline{f(\tilde{x},1,v)},\end{cases}\qquad(10)$$

при выполнении условий

$$\begin{cases}f(\tilde{x},0,0)f(\tilde{x},1,0)\le\overline{f(\tilde{x},0,1)f(\tilde{x},1,1)},\\ f(\tilde{x},0,v)\le\overline{f(\tilde{x},1,v)},\end{cases}\qquad(11)$$

Δ Из теоремы 1 следует

$$f(\tilde{x},0,v)\le u\le\overline{f(\tilde{x},1,v)}\ -\qquad(12)$$

интервал для неизвестной функции $u(\tilde{x})$ при условии выполнения неравенства $f(\tilde{x},0,v)\le\overline{f(\tilde{x},1,v)}$. Это неравенство эквивалентно условию

$$f(\tilde{x},0,v)\cdot\overline{f(\tilde{x},1,v)}=0.\qquad(13)$$

Разложим левую часть равенства (13) по переменной v:

$$\bar{v}f(\tilde{x},0,0)f(\tilde{x},1,0)\vee vf(\tilde{x},0,1)f(\tilde{x},1,1)=0.$$

Отсюда по теореме 1 имеем:

$$f(\tilde{x},0,0)f(\tilde{x},1,0)\le v\le\overline{f(\tilde{x},0,1)f(\tilde{x},1,1)}.\qquad(14)$$

Таким образом, общее решение уравнения $f(\tilde{x},u,v)=0$ описано системой неравенств (12), (14), то есть системой (10).▲

Следствие 1. Симметричные рассуждения

приводят к другому виду описания **общего решения:**

$$\begin{cases} f(\tilde{x},0,0)f(\tilde{x},0,1) \le u \le \overline{f(\tilde{x},1,0)f(\tilde{x},1,1)}, \\ f(\tilde{x},u,0) \le v \le \overline{f(\tilde{x},u,1)} \end{cases} \quad (15)$$

при выполнении условий:

$$\begin{cases} f(\tilde{x},0,0)f(\tilde{x},0,1) \le \overline{f(\tilde{x},1,0)f(\tilde{x},1,1)}, \\ f(\tilde{x},u,0) \le \overline{f(\tilde{x},u,1)}. \end{cases} \quad (16)$$

Следствие 2. Условия существования единственного решения получаем из (10) и (16):

$$\begin{cases} v = f(\tilde{x},u,0) = \overline{f(\tilde{x},u,1)}, \\ u = f(\tilde{x},0,v) = \overline{f(\tilde{x},1,v)}. \end{cases} \quad (17)$$

Следствие 3. Общее решение булева уравнения $f(\tilde{x},u,v)=0$ может быть оформлено как пара случайных булевых функций (u^*, v^*), причем совокупность реализаций их будет совпадать с множеством решений (пар (u,v)) названного булева уравнения.

Δ При фиксированном $\tilde{x}=\tilde{\sigma}$ первые неравенства в системе (10)

$$f(\tilde{\sigma},0,0)\cdot f(\tilde{\sigma},1,0) \le v \le \overline{f(\tilde{\sigma},0,1)\cdot f(\tilde{\sigma},1,1)}$$

при вычисленных левой и правой частях примут *apriori* один из следующих видов: 1) $0 \le v \le 0$; 2) $1 \le v \le 1$; 3) $0 \le v \le 1$; 4) $1 \le v \le 0$.

Строим $v^*(\tilde{x})$ как частичную случайную булеву функцию: $v^*(\tilde{\sigma})=0$ в первом случае, $v^*(\tilde{\sigma})=1$ во втором случае, в третьем случае $v^*(\tilde{\sigma})$ как случайная булева величина, в четвертом случае значение $v^*(\tilde{\sigma})$ не определено и не имеет вовсе никакого значения (как, например, в классическом математическом анализе при делении на ноль). Будем считать, что в функции $v^*(\tilde{\sigma})$ все случайные булевы величины функционально независимы.

Подставляя найденную функцию v^* во вторые неравенства системы (10), мы можем вычислить и u^* как частичную случайную булеву функцию, причем, если $v^*(\tilde{\sigma})$ не определено, то считаем, что $u^*(\tilde{\sigma})$ не определено автоматически; если $f(\tilde{x},0,v^*(\sigma))$ или $f(\tilde{\sigma},1,v^*(\sigma))$ – случайная величина или

$$f(\tilde{x},0,v^*(\sigma)) < \overline{f}(\tilde{\sigma},1,v^*(\tilde{\sigma})),$$

то $u^*(\tilde{\sigma})$ будем считать случайной булевой величиной. Таким образом: 1) если хотя бы при одном значении $\tilde{x}$ одна из функций $v^*(\tilde{x})$ и $u^*(\tilde{x})$ не определена, то исходное булево уравнение не имеет решений; 2) если функции $v^*(\tilde{x})$ и $u^*(\tilde{x})$ не содержат в себе случайных величин, то исходное булево уравнение имеет единственное решение $v(\tilde{x})=v^*(\tilde{x})$, $u(\tilde{x})=u^*(\tilde{x})$; 3) если функции $v^*(\tilde{x})$ и $u^*(\tilde{x})$ содержат в себе случайные величины, то общим решением исходного уравнения будет совокупность всех реализаций пары $(v^*(\tilde{x}),u^*(\tilde{x}))$. ▲

Теорема 3. *Булево уравнение* $f(\tilde{x},u,v)=0$ *при условии существования единственного решения может быть записано в виде:*

$$v(\tilde{x}) = u(\tilde{x}) \oplus f(\tilde{x},0,0). \quad (18)$$

Δ Разложим правую часть уравнения $u=f(\tilde{x},0,v)$ по переменной v:

$$u = \bar{v}f(\tilde{x},0,0) \oplus vf(\tilde{x},0,1) =$$
$$= v\big(f(\tilde{x},0,0) \oplus f(\tilde{x},0,1)\big) \oplus f(\tilde{x},0,0).$$

Симметрично можно получить другое уравнение:

$$v = u\big(f(\tilde{x},0,0) \oplus f(\tilde{x},1,0)\big) \oplus f(\tilde{x},0,0). \quad (19)$$

Из первого уравнения системы (17) при $u=0$ имеем:

$$f(\tilde{x},0,0) = \overline{f(\tilde{x},0,1)}, \quad (20)$$

а при $u=1$ имеем:

$$f(\tilde{x},1,0) = \overline{f(\tilde{x},1,1)}.$$

Из второго уравнения в (17) при $v=0$ имеем:

$$f(\tilde{x},0,0) = \overline{f(\tilde{x},1,0)}, \quad (21)$$

а при $v=1$ имеем:

$$f(\tilde{x},0,1) = \overline{f(\tilde{x},1,1)}. \quad (22)$$

Используя (20) и (21), получаем:

$$f(\tilde{x},0,0) = \overline{f(\tilde{x},0,1)} = \overline{f(\tilde{x},1,0)}$$

и, следовательно,

$$f(\tilde{x},0,0) \oplus f(\tilde{x},1,0) = 1.$$

Отсюда и из (19) получаем:

$$v = u \oplus f(\tilde{x},0,0). \blacktriangle$$

Пример 1. Пусть **T** - матрица размером 2^k на 2^{n-k} таблицы, **A** – невырожденная булева матрица размером 2^k на 2^k. Матрицы в криптографии часто используют в качестве шифрующего оператора. Произведение матриц **AT** имеет размер 2^k на 2^{n-k} и поэтому может рассматриваться как булева функция $(AT)(\tilde{x})$ от того же списка переменных, что и функция $T(\tilde{x})$. Из теоремы 3 следует, что можно найти

такую шифрующую функцию $H(\tilde{x})$, что

$$(AT)(\tilde{x}) = T(\tilde{x}) \oplus H(\tilde{x}).$$

Если через $\mathbf{H}$ обозначить матрицу размером 2^k на 2^{n-k} (можно сравнить с таблицей), то будем иметь:

$$\mathbf{H} = \mathbf{(A \oplus E)T},\ H(\tilde{x}) = ((A+E)T)(\tilde{x}),$$

где $\mathbf{E}$ – единичная матрица.

Пример 2. Рассмотрим пример применения теоремы 3 к секретной переписке двух абонентов. В качестве секретного ключа абоненты A и B используют начальную шифрующую функцию $H_0(\tilde{x})$ (например, она может нести дезинформацию).

1) Абонент A передает абоненту B информацию $T_A(\tilde{x})$, шифруя её следующим преобразованием:

$$Sh_A(\tilde{x}) = T_A(\tilde{x}) \oplus H_0(\tilde{x}).$$

2) Абонент B, располагая ключом $H_0(\tilde{x})$, расшифровывает полученное от абонента A сообщение $T_A(\tilde{x}) = Sh_A(\tilde{x}) \oplus H_0(\tilde{x})$. Затем, если абонент B желает передать свой ответ абоненту A, он оформляет его как функцию $T_B(\tilde{x})$ и шифрует с помощью преобразования:

$$Sh_B(\tilde{x}) = T_B(\tilde{x}) \oplus H_1(\tilde{x}),$$

где в качестве шифровальной функции использует полученную от абонента A информацию, то есть $H_1(\tilde{x}) = T_A(\tilde{x})$.

3) Абонент A, сохранив у себя свое предыдущее послание $T_A(\tilde{x})$, легко расшифровывает текст, посланный ему абонентом B, преобразованием $T_B(\tilde{x}) = Sh_B(\tilde{x}) \oplus T_A(\tilde{x})$ и т.д.

Пример 3. Пусть требуется решить булево уравнение

$$f(\tilde{x}, u) \vee g(\tilde{x}, v) = 0.$$

Δ Уравнение эквивалентно системе

$$\begin{cases} f(\tilde{x}, u) = 0, \\ g(\tilde{x}, v) = 0. \end{cases}$$

Каждое уравнение системы содержит в левой части одну неизвестную функцию и может решаться самостоятельно. По теореме 1 имеем:

$$\begin{cases} f(\tilde{x}, 0) \le u \le \overline{f(\tilde{x}, 1)}, \\ g(\tilde{x}, 0) \le v \le \overline{g(\tilde{x}, 1)}. \end{cases}$$

Решение не пусто, если выполнены условия:

$$\begin{cases} f(\tilde{x}, 0) \le \overline{f(\tilde{x}, 1)}, \\ g(\tilde{x}, 0) \le \overline{g(\tilde{x}, 1)}. \end{cases}$$ ▲

5. В книге [1] рассматривались булевы уравнения в булевой алгебре множеств с одним неизвестным множеством $f(A, B, \ldots, X) = 0$, где $A, B, \ldots$ – известные множества, X – неизвестное множество, а на совокупность множеств $A, B, \ldots$ наложены ограничения, предварительно вычисленные таким образом, чтобы уравнение имело единственное решение. Авторами предлагалось свести решение уравнения к системе уравнений вида $UX = \varnothing$ или $U\overline{X} = \varnothing$, где U выражены формулами над алфавитом $A, B, \ldots$. Уравнения $UX = \varnothing$, $U\overline{X} = \varnothing$ легко интерпретируются на диаграмме Венна, и неизвестное множество X геометрически угадывается (вычисляется) по диаграмме. Этот метод годится для решения булева уравнения от двух неизвестных функций $f(\tilde{x}, u, v) = 0$.

Действительно, разложим f по переменным u и v:

$$f(\tilde{x}, u, v) \equiv \bar{u}\,\bar{v}\, f(\tilde{x},0,0) \vee \bar{u}\, v\, f(\tilde{x},0,1) \vee \vee u\,\bar{v}\, f(\tilde{x},1,0) \vee u\, v\, f(\tilde{x},1,1) = 0.$$

Полученное уравнение эквивалентно системе

$$\begin{cases} \bar{u}\,\bar{v} = f(\tilde{x}, 0, 0) = 0, \\ \bar{u}\, v = f(\tilde{x}, 0, 1) = 0, \\ u\,\bar{v} = f(\tilde{x}, 1, 0) = 0, \\ u\, v = f(\tilde{x}, 1, 1) = 0. \end{cases} \qquad (23)$$

Поскольку уравнение $\varphi\psi = 0$ эквивалентно системе

$$\begin{cases} \varphi(\tilde{x}) = 0, \\ \psi(\tilde{x}) = 0, \end{cases}$$

то система (23) эквивалентна системе

$$\begin{cases} \begin{cases} \bar{u}\, f(\tilde{x}, 0, 0) = 0, \\ \bar{v}\, f(\tilde{x}, 0, 0) = 0; \end{cases} \\ \begin{cases} \bar{u}\, f(\tilde{x}, 0, 1) = 0, \\ v\, f(\tilde{x}, 0, 1) = 0; \end{cases} \\ \begin{cases} u\, f(\tilde{x}, 1, 0) = 0, \\ \bar{v}\, f(\tilde{x}, 1, 0) = 0; \end{cases} \\ \begin{cases} u\, f(\tilde{x}, 1, 1) = 0, \\ v\, f(\tilde{x}, 1, 1) = 0. \end{cases} \end{cases}$$

Таким образом, булево уравнение $f(\tilde{x}, u, v) = 0$ с двумя неизвестными функциями также

представимо как система элементарных уравнений и, значит, решение уравнения $f(\tilde{x}, u, v) = 0$ может быть рассмотрено на геометрическом теоретико-множественном уровне в диаграмме Венна.

6. В книге [5] дается понятие однонаправленной функции. Это такая функция, которую легко вычислить и, следовательно, легко ею шифровать тексты, но для которой обратную функцию вычислить трудно и, следовательно, трудно расшифровать тексты. В 1974 году Дж. Парди предложил в качестве шифрующей функции многочлен

$$f(x) = x^{2^{24}+17} + a_1 x^{2^{24}+3} + a_2 x^3 + a_3 x^2 + a_4 x + a_5, \mod (2^{64} - 59),$$

где коэффициентами являются произвольные 19-разрядные целые числа. Дж. Парди утверждал, что для нахождения обратной функции потребуется примерно 1000 лет. Однако термин «односторонняя функция» неудачен, так как легко может привести к недоразумению. По-видимому, дело не в функции, а в способе её задания. Ведь если эта функция задана таблично, то сложность алгоритма шифрования и дешифрования одинакова. И наша теорема 3 говорит о том же, так как она показывает линейную связь между текстом и шифром, а ведь любую криптосистему можно записать в двоичных кодах. Таким образом, разумно здесь говорить не об однонаправленных функциях, которых просто нет, а о формулах, о формах представления функций, дающих разные алгоритмы дешифрования.

7. Использование псевдобулевых функций.

Еще более широкая модель криптосистем получается с использованием частичных функций алгебры логики. Информация может передаваться не в виде прямоугольника символов алфавита, а в виде «рисунка», булева поля. Для получения частичной функции следует поместить булево поле в прямоугольник (матрицу) значений функции (см. таблицу).

Пусть $T(\tilde{x})$ – частичная функция алгебры логики, хранящая информацию; $T^*(\tilde{x})$ – функция, получающаяся от $T(\tilde{x})$ заменой пустых мест в поле символами 2; $Sh(\tilde{x})$ – частичная функция – шифр функции $T(\tilde{x})$; $Sh^*(\tilde{x})$ – соответствующая $Sh(\tilde{x})$ функция, получающаяся от заполнения пустых мест символами 2 в поле её значений. Тогда можно определить следующую модель криптосистем:

$$Sh^*(\tilde{x}) = \Phi(\tilde{x}) + T^*(\tilde{x}), T^*(\tilde{x}) = Sh^*(\tilde{x}) - \Phi(\tilde{x}),$$

где «+» и «-» понимается по $\mod 3$, $\Phi(\tilde{x})$ – функция-усложнитель (ключ шифрования).

8. Любопытно отметить, что криптосистема, использующая функции трехзначной логики, приводит также к линейной связи функций $Sh(\tilde{x})$ и $T(\tilde{x})$. Для доказательства исходное уравнение пусть имеет вид:

$$Sh(\tilde{x}) = F(\tilde{x}, T(\tilde{x})),$$

где $T(\tilde{x})$ – текст, $Sh(\tilde{x})$ – шифр, F – функция трехзначной логики. Всякая функция трехзначной логики, как известно, представима полиномом. Так как $T^2(\tilde{x}) \equiv 1 \pmod 3$, то, представляя $F(\tilde{x}, T(\tilde{x}))$ полиномом по переменной T, имеем:

$$Sh(\tilde{x}) = A(\tilde{x})\, T(\tilde{x}) + B(\tilde{x}) \qquad (24)$$

при подходящих $A(\tilde{x})$ и $B(\tilde{x})$. При фиксированном $\tilde{x} = \tilde{\sigma}$ из уравнения (24) получим:

$$Sh(\tilde{\sigma}) = A(\tilde{\sigma})\, T(\tilde{\sigma}) + B(\tilde{\sigma}).$$

Чтобы $T(\tilde{\sigma})$ выражалось отсюда однозначно, необходимо и достаточно, чтобы $A(\tilde{\sigma}) \neq 0$. То есть функция $A(\tilde{x})$ принимает значения только 1 или 2. Выражая $T(\tilde{x})$ из (24), получим:

$$T(\tilde{x}) = A(\tilde{x})(Sh(\tilde{x}) - B(\tilde{x})). \qquad (25)$$

Правильность формулы легко проверяется взаимными подстановками (24) и (25):

$$Sh(\tilde{x}) = A(\tilde{x})\left[A(\tilde{x})\,(Sh(\tilde{x}) - B(\tilde{x}))\right] + B(\tilde{x}) =$$
$$= A^2(\tilde{x})\, Sh(\tilde{x}) - A^2(\tilde{x})\, B(\tilde{x}) + B(\tilde{x}) =$$
$$= Sh(\tilde{x}) - B(\tilde{x}) + B(\tilde{x}) = Sh(\tilde{x}),$$
$$T(\tilde{x}) = A(\tilde{x})\left[A(\tilde{x})\,(T(\tilde{x}) - B(\tilde{x}))\right] + B(\tilde{x}) =$$
$$= A^2(\tilde{x})\, T(\tilde{x}) - A^2(\tilde{x})\, B(\tilde{x}) + B(\tilde{x}) =$$
$$= T(\tilde{x}) - B(\tilde{x}) + B(\tilde{x}) = T(\tilde{x}).$$

Таким образом, $T(\tilde{x})$ и $Sh(\tilde{x})$ линейно выражаются друг через друга.

Заключение. В статье рассмотрены методы решения булевых уравнений с одной и двумя неизвестными функциями с возможными приложениями в криптографии и распознавании образов.

Теоретически показано для булевых уравнений с двумя неизвестными функциями, что при условии существования единственного решения одна неизвестная функция может быть выражена через другую с помощью линейного преобразования; представлены примеры применения такого линейного преобразования в качестве шифрующего.

Библиографический список

1. *Лавров И.А., Максимов Л.Л.* Задачи по теории множеств, математической логике и теории алгоритмов. – М.: Физматлит, 2004. – 240 с.

2. Дискретная математика: методические указания / сост. А.Н. Коненков; под ред. В.В. Тарасова. – Рязань: РГРТА, 2001. – 48 с.

3. *Елкина Н.В., Тарасов В.В.* Уравнения с булевой алгеброй множеств // сб. «Математические методы в научных исследованиях». Рязань: 2010. – С. 21-24.

4. *Горелик А.Л., Скрипкин В.А.* Некоторые вопросы построения систем распознавания. – М.: Советское радио, 1974. – 224 с.

5. *Коблиц Н.* Курс теории чисел и криптографии. – М.: Научное издательство «ТВП» 2001. – 254 с.

УДК 621.372

И.А. Саитов*, *К.И. Мясин*, *Д.С. Крысин

МУЛЬТИПРОТОКОЛЬНАЯ ОПТИЧЕСКАЯ ТРАНСПОРТНАЯ СЕТЬ ИНФОКОММУНИКАЦИОННОЙ СИСТЕМЫ

Предлагается новый подход к обеспечению мультисервисности инфокоммуникационной системы за счет построения мультипротокольной транспортной сети на уровне оптических каналов и трактов.

Ключевые слова: *мультисервисная инфокоммуникационная система, инфокоммуникационные услуги, мультипротокольная транспортная сеть, гетерогенный волоконно-оптический линейный тракт.*

Введение. Цель работы – осветить подход, позволяющий реализовать весь функционал мультисервисной системы без существенных потерь информационной скорости и внесения дополнительной задержки.

Историческое развитие телекоммуникаций привело к формированию инфокоммуникационных систем (ИКС), которые не только реализуют функции передачи и распределения сообщений различного типа (речевых, текстовых, видео, мультимедиа), но и обеспечивают хранение, обработку и защиту пользовательской информации. Отсюда следует вывод, что ИКС являются *мультисервисными* [1].

Функции и соответственно устройства передачи и распределения сообщений в ИКС существенно усложняются с каждым годом. В последнее время активно повышается объем трафика услуг, предусматривающих совместную работу распределенных коллективов пользователей (видео- и другие сетевые конференции, интерактивный обмен данными и пр.). Увеличивается доля служебного трафика (нагрузка, обусловленная обменом информации вида "человек – машина" и "машина – машина") [2]. При одновременном увеличении числа пользователей традиционные экстенсивные меры, например простое увеличение ресурса производительности узлов коммутации (УК) или пропускной способности линий передачи, уже не решают возникающих проблем обеспечения качества предоставляемых сервисов (услуг).

Общие положения. В настоящее время в телекоммуникационных системах можно выделить две основные системотехнические тенденции. Во-первых, в результате развития компьютерной техники современные средства ИКС стали представлять собой интегрированные аппаратно-программные комплексы связи (АПКС). Теперь на базе одних и тех же *аппаратных* устройств может быть *программно* реализован целый ряд протоколов различных сетевых технологий. Этот факт существенно расширяет возможности по формированию в ИКС мультипротокольной среды. Во-вторых, в транспортных сетях ИКС наблюдается широкое внедрение оптических технологий и компонентов.

Все это определяет общий вектор эволюции глобальной информационной инфраструктуры. Ее развитие от узкоспециализированных сетей электросвязи до настоящего времени продолжает идти в направлении поглощения техническими средствами все большей части функций конечного пользователя услуг связи и обслуживающего персонала по преобразованию информации. Именно поэтому внутренняя структура системы электросвязи постепенно усложнялась, что привело сначала к выделению первичных и вторичных сетей, а затем к формированию транспортных сетей и сетей доступа. Сегодня появились объективные предпосылки, чтобы

возложить на транспортную сеть некоторые функции распределения сообщений, некогда принадлежавшие УК сетей доступа, чему способствует развитие оптических технологий передачи информации. Очевидно, что это повлияет на подходы к проектированию информационных инфраструктур и управлению сетевыми элементами.

Большинством экспертов предлагается обеспечить мультипротокольность сетевой инфраструктуры ИКС посредством реализации концепции сетей связи следующего поколения (*NGN*, *NG*-сетей) [2, 4]. В соответствии с ней в сетях доступа внедряются пакетные АПКС (*softswitch*, коммутаторы, маршрутизаторы и т. д.). Разнородные сообщения приводятся к единому формату (часто *IP*-пакеты), которые далее попадают в транспортную сеть, где производится их инкапсуляция в кадр технологии передачи канального уровня ЭМВОС (в России по-прежнему широко используется технология *SDH*).

Очевидно, что функциональные характеристики *NG*-сети будут ограничены врожденными недостатками пакетных технологий передачи сообщений [5, 6]. Это, во-первых, сложность обеспечения гарантированного качества (*QoS*) предоставления сервисов реального времени, обусловленная наличием временных задержек доставки блоков данных (БД) и их стохастическим характером. Во-вторых, наличие эффектов "перегрузки" сетевых элементов, возникающим уже при умеренных входящих нагрузках из-за "конкуренции" БД равного приоритета за ресурс системы.

ИКС должна предоставлять *некоторый комплекс* (многообразие) соответствующих услуг (информационных и/или телекоммуникационных). Все эти услуги целесообразно классифицировать с точки зрения восприятия пользователем [7]. В зависимости от наличия задержки в получении информационного сообщения можно выделить три категории сервисов:

– передача сообщений реального времени (*real-time services*, *RTS*), чьи потоки в идеале передаются без задержки (телефония, видеоконференц-связь, видеотелефония, прямые трансляции теле- и радиопередач). В транспортной сети минимум сетевой задержки БД обеспечивают системы передачи (СП) *SyTDM*;

– передача данных в интерактивном режиме (*interactive data service*, *IDS*). Пересылка сообщений данного вида может происходить с небольшой задержкой, а абонент оценивает качество получаемого сервиса по скорости отклика на запрос. Для этой категории сервиса целесообразность применения СП *SyTDM* или *StTDM* в транспортной сети во многом зависит от условий функционирования ИКС;

– передача данных, терпимых к задержке (*delay tolerant services*, *DTS*), – электронная почта, пересылка файлов и т. д. Эффективность применения СП *StTDM* для предоставления данного типа сообщений не вызывает сомнений.

Монопротокольная транспортная сеть ИКС. Пусть мультисервисная ИКС строится на монопротокольной транспортной сети, т. е. сети, реализующей одну технологию передачи статического (*SyTDM*) или статистического (*StTDM*) временного мультиплексирования. По такому принципу строятся транспортные сети операторов сотовой связи (ОСС), на заре развития которых господствовали СП плезиохронной цифровой иерархии (*PDH*). В настоящее время в связи с расширением перечня предоставляемых услуг связи ТС ОСС строятся на базе пакетных технологий.

Все манипуляции с сообщениями, производимые в АПКС той или иной сетевой технологии, должны быть направлены на обеспечение требуемого *QoS* по перечисленным выше категориям сервисов. Переменными в этой задаче являются количество пользователей (N_t), одновременно обслуживаемых ИКС в определенный промежуток времени (t), а также число (R_t) и тип (D_t) сеансов (унимодальных, полимодальных, мультимедийных и пр.), открытых каждым абонентом. При количественно заданных требованиях к *QoS* именно эти неизвестные величины и определяют необходимый объем оборудования ИКС и производительность (B) используемых линий передачи. Учитывая стремление к минимизации экономических затрат оператора сети при развертывании, можно записать выражение:

$$B(N_t, R_t, D_t) \xrightarrow{QoS} \min, \qquad (1)$$

смысл которого заключается в выборе линий с минимальной пропускной способностью при проектировании сети, обеспечивающих с заданным качеством определенное количество пользователей различными услугами связи.

Для решения данной задачи необходимо: во-первых, привести все поступающие в ИКС типы сообщений (*RTS*, *IDS*, *DTS*) к единому виду (например, пакетам *IP*). Во-вторых, оценить количество УК *IP*-пакетов в сети доступа и количество систем передачи в транспортной сети. Последняя в данной ситуации воспринимается как средство переноса нормализованных цифровых потоков между пространственно удаленными узлами посредством заранее определенной (*одной*!) сетевой технологии. Поддержание требуемого качества предоставления *RTS*, *IDS* и *DTS* в рассматриваемых условиях обес-

печивается различными техническими ухищрениями с оборудованием сетей доступа: приоритетами пакетов, манипуляциями со способами обслуживания БД и т. д. Это требует существенных вычислительных затрат, повышенных требований к АПКС сетей доступа, что незамедлительно отражается на цене. При этом в узлах транспортной сети со статическим временным мультиплексированием реализуются сложные технологические цепочки доступа к ресурсу оптического волокна (ОВ). Так, для передачи, например, *IP*-пакетов вне зависимости от типа услуги в настоящее время предусмотрены акты вложения (инкапсуляции) [3] следующих видов:

– *IP/Ethernet/SDH*/ОВ;

– *IP/ATM/SDH/*ОВ;

– *IP/MPLS/ Ethernet/SDH/*ОВ и т. д.

В узлах транспортной сети со статистическим временным мультиплексированием также необходима инкапсуляция. Цепочки имеют вид:

– *IP/GEthernet/*ОВ;

– *IP/ATM/OTN/*ОВ;

– *IP/MPLS/ GEthernet/*ОВ и т. д.

При этом доля служебных бит существенно ниже, чем предусмотрено аналогичными преобразованиями в технологиях статического мультиплексирования.

Такое построение ИКС приводит:

– к неэффективному использованию ресурса пропускной способности телекоммуникационных узлов и линий из-за большого количества служебных сообщений (сигнальных, согласующих, упаковывающих и пр. бит);

– снижению технической надежности линий связи вследствие повышения интегративности устройств связи и усложнения алгоритмов управления ими;

– удорожанию АПКС.

При предоставлении услуг *RTS* и *IDS* в монопротокольной транспортной сети на расстояниях свыше 1000 км все перечисленные выше манипуляции с форматом сообщений приводят к появлению дополнительных существенных задержек, а следовательно, затрудняют достижение требуемого *QoS*. Так, практика и многочисленные эксперименты, проведенные Саитовым И.А., показывают, что даже синхронная транспортная сеть (*SDH*) при переносе пакетного трафика заметно изменяет характер временных и вероятностных параметров доставки БД. Для транспортных сетей с технологиями *StTDM* (*ATM, G-Ethernet* или *OTN*) стохастичность показателей своевременности доставки БД еще более усиливается. Это не позволяет типовым АПКС сетей доступа в обычных условиях функционирования сети на расстояниях свыше 1000 км гарантировать *QoS* не только для видеоконференц-связи (*H*.323), но и для обычной телефонии. Естественно, можно обеспечить заданный уровень качества предоставления *RTS*, если установить в ИКС *соединение* "абонент-абонент" на все время сеанса и через полученный тракт передавать пакеты. Но тогда зачем нужна такая дорогостоящая реализация коммутации каналов?

Однопротокольная транспортная сеть в принципе неспособна с равным качеством обслуживать различные типы сообщений (*RTS*, *IDS* и *DTS*). Тому есть ряд причин. Во-первых, в транспортной сети распределение ресурсов попрежнему осуществляется по принципам, заимствованным из сетей телефонной связи:

– дробления на каналы (тракты) одинакового качества и пропускной способности;

– закрепления каналов (трактов) за направлениями связи;

– равномерного дробления ресурсов между элементами сигналов, являющихся носителями информации.

В соответствии с перечисленными принципами волоконно-оптические линейные тракты (ВОЛТ) транспортной сети являются гомогенными (рисунок 1, *а*), т. е. имеют во всех спектральных каналах одинаковый формат кадра (обусловленный применяемой сетевой технологией) и равную скорость передачи сигнала.

Во-вторых, в алгоритмах управления сетевыми элементами ИКС до сих пор не предусмотрена возможность *согласования режимов функционирования* УК сетей доступа и транспортной сети. Неопределенность для элементов транспортной сети процессов в сети доступа, вызванных изменениями текущих потребностей пользователей, часто является причиной невозможности обеспечения заданного уровня *QoS* даже при наличии достаточного ресурса пропускной способности.

Третьей причиной является изначальная разнородность требований, предъявляемых различными категориями сервисов. Ввиду этого одна технология не в состоянии обеспечивать наивысшее качество предоставления услуг.

Из вышеизложенного следует:

1. В последние годы появление новых инфокоммуникационных услуг активно способствует развитию технологий сетей доступа, широкомасштабному внедрению пакетных АПКС.

2. В странах Северной Америки и Западной Европы (имеющих небольшой диаметр), разработавших эти сетевые технологии для себя, *удается* обеспечить требования *QoS* и в условиях монопротокольной транспортной сети средствами сетей доступа.

3. В стране, имеющей протяженность более 7000 км, обеспечить мультисервисность распределенных ИКС только средствами сетей доступа при наличии монопротокольной транспортной сети затруднительно.

Мультипротокольная транспортная сеть ИКС. В настоящее время уже реализованы на практике *гетерогенные* волоконно-оптические линейные тракты (ВОЛТ), использующие в различных спектральных каналах разные сетевые технологии (рисунок 1, *б*).

Такая организация лишена части недостатков, присущих структуре ИКС, построенной на однопротокольной транспортной сети. Так, например, отпадает необходимость во множественных инкапсуляциях – соответствующая технология переноса использует собственный спектральный канал. В случае острой необходимости переходы между *SyTDM* и *StTDM* могут осуществляться на транзитных узлах для отдельных потоков, для которых такая процедура неизбежна. Схожая ситуация и с обслуживанием различных типов сообщений. Сообщение предварительно анализируется, определяется его протокол, а затем транслируется на оборудование соответствующей технологии передачи. Процедура анализа типа сообщения может осуществляться как автоматически, так и на основе статистических данных о предпочтениях конкретного пользователя (группы пользователей). В любом случае эта операция предусматривает кроссовую функцию по соединению конкретного направления с СП соответствующей технологии. Примером данной организации может служить сеть оператора, предоставляющего услуги телефонной связи и доступа в Интернет. Различные группы узлов доступа (телефонные станции и сетевое оборудование распределительного уровня) закреплены за СП, использующими различные технологии.

Данный подход обладает следующими недостатками:

– нежелательные инкапсуляции всё же имеют место ввиду существенной инерционности перевода информационных потоков на соответствующую аппаратуру в ручном режиме;

– разнородность потребностей группы пользователей (трафика участка сети доступа, подключенной к узлу транспортной сети) порождает необходимость преобразования технологий передачи, что ведет к снижению информационной эффективности и увеличению совокупной сквозной задержки.

Данные недостатки нивелируются автоматическим средством, определяющим тип нагрузки, – анализатором протоколов глобальных сетей. Однако такие устройства весьма дороги и появились на рынке сравнительно недавно. Сходные функции выполняются транспортной плоскостью архитектуры *softswitch*.

Инвариантная к технологии передачи ТС. Возможен другой вариант построения гетерогенной ТС ИКС. Принципиальным отличием от предыдущих вариантов является наличие в тракте прохождения сигналов пары коммутаторов ситуаций и полностью оптических линий связи.

При наличии средств согласования режимов функционирования АПКС транспортной сети и сетей доступа возможна реализация ВОЛТ, адаптивно выбирающих наиболее эффективную по критерию обеспечения *QoS* сетевую технологию под текущее распределение заявок пользователей (рисунок 1, *в*). Под критерием обеспечения *QoS* будем понимать состояние показателей качества в интервалы доступности (*T*) всех услуг ИКС, соответствующее нормам. Фактически это означает реализацию критерия пригодности. Например, для услуг на базе *IP* в соответствии с *Y*.1541 оцениваются процент потерянных пакетов (*IPLR*), процент пакетов с ошибками (*IPER*), время задержки передачи пакета (*IPTD*) и джиттер времени задержки (*IPDV*).

Однако пользователю не важны технические показатели качества, для него более существенно, насколько узнаваема и разборчива речь, сколь быстро происходит отклик по интерактивному запросу, с какой скоростью закачивается интересующая информация. В связи с этим и возникает задача определения соответствия технологий передачи требованиям сети доступа, а в конечном итоге и пользователя. И если для сервисов *RTS* и *DTS* задача решена предоставлением технологий переноса *SyTDM* и *StTDM* соответственно, то сервисы *IDS* требуют более дифференцированного подхода. Таким образом, коммутатор ситуаций должен по критерию пригодности определить наиболее эффективную технологию (*j*) для доставки информационных потоков интерактивных услуг:

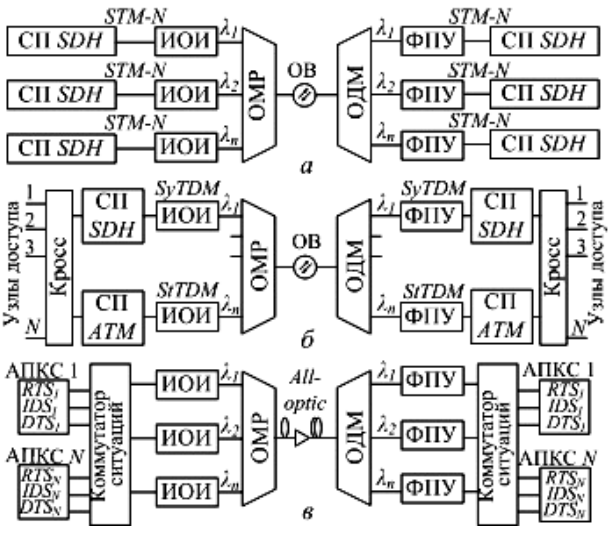
$$QoS_j^{приг} = \begin{cases} IPLR_{обесп}^{j} < IPLR_{треб}, \\ IPER_{обесп}^{j} < IPER_{треб}, \\ IPTD_{обесп}^{j} < IPTD_{треб}, \\ IPDV_{обесп}^{j} < IPDV_{треб}, \\ \forall i \in N, \\ \forall t \in T, \\ j = ? \end{cases} . \qquad (2)$$

Понятие эффективности используется в контексте качества предоставления услуги пользователю, например предпочтительней

будет технология, обеспечивающая при прочих равных условиях минимальную совокупную сквозную задержку (или иной параметр, значимый для пользователя), ведь неизвестно, какую задержку внесут элементы сети доступа.

Рассматриваемый вариант построения ТС предусматривает анализ не протокола, а содержания (там, где это возможно по соответствующим комбинациям), определяется тип сервиса. Выбор технологии ТС осуществляется исходя из сервиса, а не конкретной реализации технологии сети доступа. Это позволяет, в ряде случаев, "снять оболочку" избыточной технологии с информационного наполнения и сократить количество актов инкапсуляции.

Другим немаловажным аспектом построения инвариантной ТС является переход от 3*R* электронно-оптических регенераторов к оптическим линейным усилителям, а на длинных линиях – к полностью оптическим регенераторам. Тогда тракт становится *инвариантным* к технологии передачи. Становится доступным модемный принцип передачи по оптическому волокну, предполагающий передачу информационных контейнеров в неизменном виде.



Гомогенный (*а*), гетерогенный (*б*) и инвариантный к технологии передачи (*в*) ВОЛТ:
ИОИ – источник оптического излучения; ОМР – оптический мультиплексор; ОДМ – оптический демультиплексор; ФПУ – фотоприемное устройство

Более того, сеть становится более управляемой, гибкой. При наличии сигнала о текущей ситуации в ИКС (доступность и пропускная способность линий, очереди на сетевых элементах и пр.) может производиться назначение наиболее подходящего (с точки зрения обеспечения *QoS*) формата кадра и скорости передачи для каждого из спектральных каналов ВОЛТ, а ресурс производительности линий передачи оказывается разделенным не на равные доли [8].

Таким образом, предлагаемый подход обеспечивает формирование по-настоящему мультипротокольной транспортной сети и предоставляет эффективные механизмы управления обслуживанием мультисервисного трафика в ИКС. С учётом изложенного перспективной является технология развертывания полностью оптических сетей, так как в будущем это позволит сократить издержки на потери информационной скорости вследствие преобразования технологий передачи.

Заключение. Можно констатировать факт, что в предметной области имеет место противоречие между постоянно возрастающими требованиями пользователей ИКС к мультисервисности обслуживания (обеспечиваемой среди прочего требуемым качеством передачи сообщений по каналам и трактам связи) и ограниченными возможностями монопротокольных транспортных сетей, развертываемых на базе узкоспециализированного оборудования. В настоящее время это противоречие решается экстенсивным путем – посредством привлечения избыточных ресурсов линий и узлов транспортной сети, растрачиваемых на покрытие многочисленных актов инкапсуляций, согласований и т. п. Естественно, это сопряжено с дополнительными экономическими затратами. Распространённая в России технология *Ethernet* поверх *SDH* (*EoS*) увеличивает уже заложенные в *SDH* 3% потерь информационной скорости на 2 %.

Реализация идей, изложенных выше, в перспективе позволит полностью отказаться от сложных технологических цепочек доступа к ОВ, что повышает показатели *QoS*. Современные оптические компоненты ВОЛТ способны передавать примитивы сетевого и канального уровней ЭМВОС различных технологий (пакеты, кадры, ячейки) без инкапсуляции, т. е. по модемному принципу (отличному от *OTN*). Однако это обусловит необходимость внесения существенных корректив в традиционные способы организации эксплуатации ИКС, повлечет необходимость оптимизации целого ряда функциональных характеристик сетевых элементов для разных ситуаций при проектировании и эксплуатации транспортной сети, что потребует новых теоретических исследований в предметной области.

Библиографический список

1. *Ершов, В.А.* Мультисервисные телекоммуникационные сети / В.А. Ершов, Н.А. Кузнецов. – М. :

МГТУ им. Баумана, 2003. – 427 с.

2. *Кучерявый, А.Е.* Сети связи следующего поколения / А.Е. Кучерявый, А.Л. Цуприков. – М. : ФГУП ЦНИИС, 2006. – 278 с.

3. *Меккель, А.М.* Оптическая транспортная сеть и *NGN* / А.М. Меккель // Lightwave Russian Edition, 2006. – № 2. – С. 18–22.

4. *Семёнов, Ю.В.* Проектирование сетей связи следующего поколения / Ю.В. Семёнов. – СПб. : Наука и техника, 2005. – 204 с.

5. *Шварцман, В.О.* Выбор технологии передачи и коммутации в мультисервисных сетях на основе оптических кабелей / В.О. Шварцман // Электросвязь. – 2003. – № 8. – С. 33–39.

6. *Нетес, В.А.* Мультисервисные сети: сумма технологий / В.А. Нетес // Электросвязь. – 2004. – №9. – С. 20–23.

7. *Степанов, С.Н.* Основы телетрафика мультисервисных сетей / С.Н. Степанов. – М. : Эко-Трендз, 2010. – 392 с.

8. *Саитов, И.А.* "Проблемы роста" роли оптической транспортной сети в ТКС / И.А. Саитов // Телекоммуникации. – 2010. – № 3. – С. 30–35.