Анализ рынка программ показывает, что лидером среди программ, которые позволяют управлять компьютером на русском языке, по качеству и точности распознавания является программа Typle. Есть, также такие программы как:RealSpeaker, Web Speech, Горыныч, и т.д., но все они менее точны или у них не полная интеграция с ОС.

Таким образом, в результате исследования были рассмотрены и проанализированы наиболее успешные методы распознавания речевых команд и имеющееся эффективное программное обеспечение для управления голосом на персональном компьютере.

Список использованных источников:

1. Самые совершенные программы управления голосом [Электронный ресурс]. – Режим доступа: https://www.gkh11.ru/news/samye_sovershennye_ programmy_upravlenija_golosom/2016-01-28-1770. – Дата доступа: 24.03.2018.
2. Управление голосом и жестами на компьютере [Электронный ресурс]. – Режим доступа: https://bursin.ru/upravlenie-golosom-i-zhestami-na-kompyutere/. – Дата доступа: 22.03.2018.
3. Кравченко, К.В. Автоматизированная система голосового русскоязычного управления операционной системой Windows / К.В. Кравченко, Р.А. Дьяченко // Современные проблемы науки и образования. – 2014. – № 3.
4. Как управлять компьютером при помощи голосовых команд? [Электронный ресурс]. – Режим доступа: http://nastroyvse.ru/programs/ review/upravlenie-kompyuterom-s-pomoshhyu-golosa.html. – Дата доступа: 23.03.2018.

ПРОГНОЗИРОВАНИЕ КЛИМАТИЧЕСКИХ УСЛОВИЙ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИЙ ИНТЕЛЛЕКТУАЛЬНОГО АНАЛИЗА ДАННЫХ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Клещиков А.С.

Медведев С.А. – к.т.н., доцент

Влияние прогноза климатических условий для общества, бизнеса, сельского хозяйства заставляет уделять большое внимание данному вопросу. Последние несколько лет показывают потрясающие достижения в области прогнозирования климата. Все системы и методы, разработанные до сих пор, используют температуру поверхности моря в качестве основного фактора, использующегося для прогноза. Затем уже используются статистические и математические модели для дальнейшего прогноза климата. Однако есть и другой подход к прогнозированию климатических условий, который основывается на исторических метеорологических показателях региона, таких как осадки, скорость ветра, точка росы, температура и т.д.

Основная цель данной статьи - как использовать технологии интеллектуального анализа данных (в частности, алгоритма К-ближайших соседей), как разработать систему, которая использует исторические данные для прогнозирования климатических условий заданного региона, города или страны на месяцы вперед.

Интелектуальный анализ данных - это недавняя разработка в области очень больших баз данных и хранилищ данных. Он используется для обнаружения скрытых полезных паттернов в огромных базах данных. Интеллектуальный анализ данных может быть классифицирован по его методам на три основных типа: поиск ассоциативных правил, кластерный анализ и классификация/предсказывание.

Алгоритм К-ближайших соседей – это алгоритм классификации, который основывается на формуле дистанции в евклидовом пространстве. Данная формула используется для выяснения близости между неизвестными образцами с известными классами. Неизвестный образец присваивается тому классу, который является наиболее распространенным среди К соседей данного образца, классы которых уже известны.

Функция вычисления дистанции в евклидовом пространстве выглядит следующим образом:

$$d(p,q) = \sqrt{\sum_{k=1}^{n}(p_k - q_k)^2} \quad (1)$$

Шаги алгоритма К-ближайших соседей выглядят следующим образом:

вычисление расстояния между новым образцом и известными образцами по формуле (1);

сортировка полученных расстояний так, чтобы $d_i \leq d_{i+1}$и выборка К образцов с наименьшими значениями расстояний;

новому образцу присваивается класс с наибольшим количеством элементов в выборке.

Для применения алгоритма К-ближайших соседей для прогнозирования климатических условий необходимо указать четыре параметра: текущая дата (дата, от которой будет отсчитываться прогноз) (CD), количество дней для прогноза (N), значение К алгоритма и атрибуты для прогноза.

Затем, для вычисления расстояния в евклидовом пространстве, исходный массив данных разбивается на последовательности. Каждая последовательность имеет размер S, который расчитывается как произведение количества дней прогноза N на количество атрибутов прогноза. Базовой последовательностью являются записи за предыдущие N дней для выбранных атрибутов. Общее количество последовательностей (T) вычисляется как общее количество записей делить на количество записей в базовой последовательности. Дальнейшее вычисление расстояний можно выразить с помощью псевдокода:

```
While i< Общее_Количество_Записей
For j = 0 to S
```

```
Sum = Sum + Sqr(Базовая_Последовательность[j] – Все_Записи[i])
i++
  End For
  Distance = Sqrt(Sum)
End While
```

Затем полученные расстояния сортируются по возрастанию и выбирается К наименьших расстояний. Итоговый прогноз вычисляется как среднее значение К образцов для выбранного атрибута и дня.

Данный метод показывает очень точные результаты, которые могут использоваться в реальной жизни. Так, для дискретных значений таких показателей как туман, град, снег, гололедица, гроза и т.д. на небольших наборах данных точность составила свыше 90%. На больших массивах данных точность повышается до 95%.

Недостатком данного метода является тот факт, что он не учитывает глобальные изменения климата (ENSOevents). Однако, данный метод прекрасно работает для областей, которые не подвержены таким изменениям.

Список использованных источников:

1. Data Mining for Climate Change and Impacts – A.R.Ganguly, K.Steinhaeuser - 2008 IEEE International Conference on Data Mining Workshops.

2. Метод ближайших соседей [Электронный ресурс]. – 2018. – Режим доступа: https://www.ibm.com/support/knowledgecenter/ru/SSLVMB_24.0.0/spss/base/idh_idd_knn_variables.html Дата доступа: 21.03.2018.

МЕТОДЫ ВОЗВЕДЕНИЯ ЧИСЛА В СТЕПЕНЬ ПО МОДУЛЮ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Короткевич А.В.

Ярмолик В.Н. – д.т.н., профессор

Одной из наиболее важных операций в ассиметричной криптографии является возведение числа в степень. Т.к. операция выполняется в конечном поле, то фактически задача сводится к нахождению $g^e(modp)$. Очевидно, что простейшим способом решения является выполнение $e-1$ умножения, однако, такой способ неприемлем, когда речь идет о числах большой разрядности. Эффективные методы выполнения возведения числа в степень по модулю будут рассмотрены в данной работе.

Существует два способа уменьшения времени выполнения операции возведения в степень в конечном поле. Во-первых, это уменьшение времени выполнения умножения двух элементов группы. Вторым способом является уменьшение требуемого числа операций умножения. В идеале оба подхода должны быть использованы одновременно [1].

В качестве решения, использующего уменьшение числа операций умножения при возведении в степень, можно привести следующий алгоритм:

Алгоритм 1 –Бинарное возведение в степень справа налево

INPUT: Целые числа g и $e \geq 1$.

OUTPUT: g^e.

1) $A \leftarrow 1, S \leftarrow g$.

2) While $e \neq 1$ do:

2.1) If e нечетное then $A \leftarrow A \cdot S$.

2.2) $e \leftarrow \lfloor e/2 \rfloor$.

2.3) If $e \neq 0$ then $S \leftarrow S \cdot S$.

3) Return A.

Приведенный алгоритм использует последовательные операции умножения и возведения в квадрат, что фактически тоже является умножением. Пусть $t+1$ – длина в битах бинарного представления числа e, а l– число единиц в данном представлении. Тогда, согласно алгоритму, потребуется t возведений в степень и $l-1$ операция умножения. Если e является случайным числом, то число возведений в степень будет приблизительно $\lfloor \log_2 e \rfloor$, а умножений $-0.5 \cdot (\lfloor \log_2 e \rfloor + 1)$. Таким образом, алгоритм позволяет сократить число операций с $e-1$ для самого простого решения до приблизительно $1.5 \cdot \log_2 e$, что является хорошим показателем.

Алгоритм 1 вычисляет $A \cdot S$ всякий раз, когда eявляется нечетным. Для некоторых значений g выражение $A \cdot g$может быть вычислено более эффективно, чем $A \cdot S$ для случайного S. Алгоритм 2 выполняет бинарное возведение в степень слева направо, которое заменяет операцию $A \cdot S$ (для случайного S) на $A \cdot g$(для фиксированного g).

Алгоритм 2 –Бинарное возведение в степень слева направо

INPUT: Целое g и положительное целое $e = (e_t e_{t-1} \dots e_1 e_0)_2$.

OUTPUT: g^e.

1) $A \leftarrow 1$.

2) For i from t down to 0 do:

2.1) $A \leftarrow A \cdot A$.