Инструкция пользователя программы "Калькулятор P1".

Общие сведения о программе

Данная программа предназначена для вычисления вероятностей появления ошибок первого рода, возникающих при тестировании обученного преобразователя биометрия-код, выполненного по требованиям ГОСТ Р 52633.

Вероятность ошибки вычисляется исходя из гипотезы хи-квадрат распределения с малым числом степеней свободы для описания сильно коррелированных данных.

Принцип работы

Принцип работы калькулятора иллюстрируется рисунком 1.

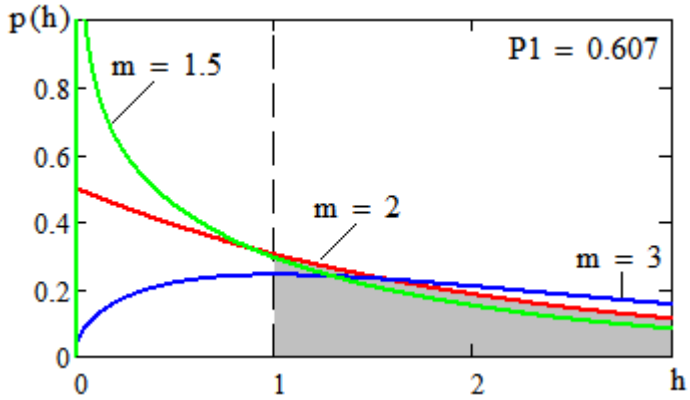

Рисунок 1 – График плотностей распределения хи-квадрат для различного количества степеней свободы

На рисунке представлены три плотности распределения хи-квадрат для трёх степеней свободы (m): m=1,5, m=2, m=3. Ось X – значение меры Хемминга (h). Мера Хемминга – количество отличающихся бит кода доступа и полученного кода.

Вероятность появления ошибки первого рода вычисляется как площадь под графиком распределения хи-квадрат с количеством степеней свободы, равным экспериментально вычисленному среднему значению меры Хемминга, интервал берётся от 1 до ∞:

$$P1 = \int_1^{\infty} f_{\chi^2(m)}(x)dx$$

Например, если средняя мера Хемминга равна 2, то вероятность ошибки первого рода (площадь закрашенной серым цветом фигуры на рисунке 1) равна 0,607. В калькуляторе вычисление интеграла производится по таблице, что ограничивает точность, но упрощает программирование. Возможность подобных вычислений обусловлена тем, что в пределе при $m \to 0$, $r \to 1$ распределение расстояний Хэмминга стремится к χ^2 с нулевым (бесконечно малым) числом степеней свободы.

Вычисление ошибки первого рода

Для вычисления вероятности появления ошибки первого рода с помощью программы "Калькулятор P1" необходимо запустить на выполнение файл CalculatorP1.exe, затем в появившемся диалоговом окне (рисунок 2) ввести значение средней меры Хемминга и нажать кнопку "=" или клавишу "***Enter***" на клавиатуре. Полученная вероятность ошибки первого рода отображается в поле вывода в правой верхней части главного окна.

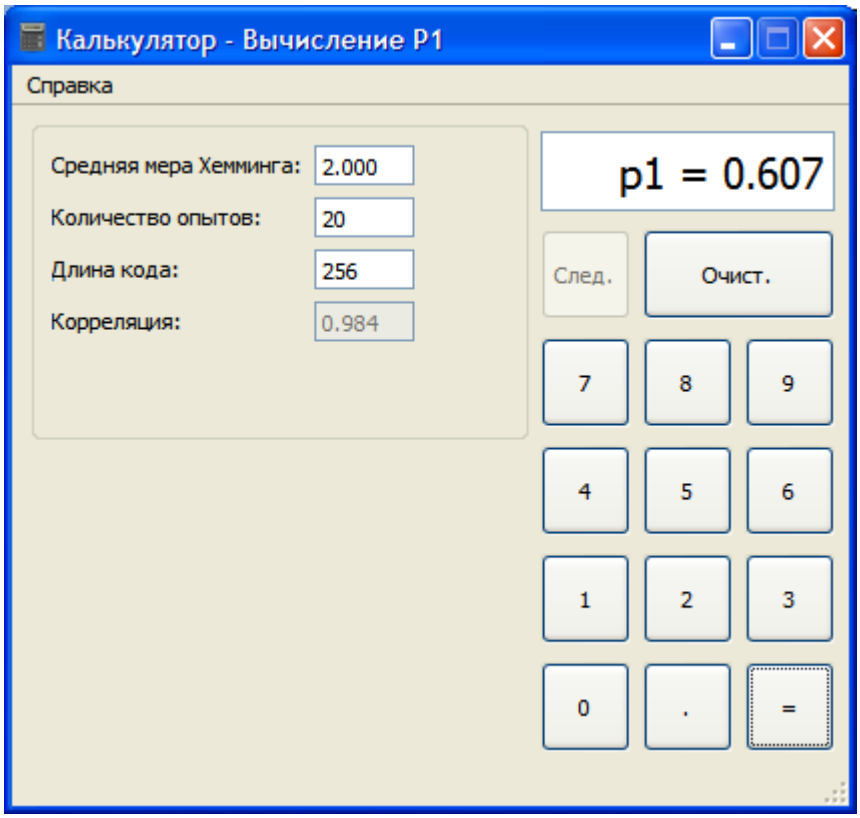

Рисунок 2 – Главное диалоговое окно программы

Средняя мера Хемминга вычисляется во время тестирования обученного преобразователя биометрия-код на тестовых образах "Свой". Средняя мера может изменяться от 0 до N/2, где N – длина выходного кода.

Если средняя мера Хемминга равна 0, т.е. все тестовые образы распознаны как "Свой", то для вычисления вероятности появления ошибки первого рода необходимо указать количество тестовых опытов. Средняя мера Хемминга в данном случае будет рассчитываться по формуле:

$$M[h] = \frac{1}{n+1},$$

где M[h] – средняя мера Хемминга;

n – количество опытов.

Таким образом, если в серии из n опытов M[h]=0, то M[h] рассчитывается из предположения, что следующий (n+1) опыт будет с ошибкой в одном бите.

Если средняя мера Хемминга больше 10, то вероятность появления ошибки первого рода будет равна 1, не зависимо от значений других полей (точность калькулятора недостаточна).

Поле "Длина кода" предназначено для ввода длины выходного кода. В данной версии калькулятора длина выходного кода влияет только на значение средней корреляции между разрядами кода «Свой».

Поле "Корреляция" в данной версии калькулятора является неактивным и предназначено для отображения прогнозируемого значения корреляции выходных кодов "Свой".