Любая криптосистема с открытым ключом базируется на предположении существования односторонних функций и/или крайней затратности решения некоторой задачи (например, для алгоритма RSA это разложение на множители очень больших чисел). В зависимости от того будет ли доказана принадлежность задач NP класса к P классу будет зависеть безопасность всех систем базирующихся на криптосистемах и задачах которые принадлежат к NP классу. То есть текущие системы безопастности базирующиеся на NP задачах построены на вере в неупрощаемость этих задач. Но это является лишь неполным условием. Иными словами, в NP-задачи заложена мера сложности «в худшем случае», но для стойкости криптографической системы необходимо, что бы задача была сложной «почти всюду». Таким образом, нам видно что для криптографической стойкости необходимо существенно более сильное предположение, чем $P \neq NP$(хоть и в большинстве случаев оно является достаточным, кроме случаев с криптосистемами с открытым ключом). А именно, предположение о существовании односторонних функций.

ЛИТЕРАТУРА

1. Введение в криптографию, В.В. Ященко 2012.- С. 348.
2. Википедия, свободная энциклопедия(https://www.wikipedia.org)
3. Д. Хопкрофт, Р. Мотвани, Д. Ульман., Введение в теорию машин Тьюринга // Введение в теорию автоматов, языков и вычислений 2002. – С. 528.

УДК 519.83

Студ. П.С. Шенец
Науч. рук. асс. Т.Г. Шагова
(кафедра высшей математики, БГТУ)

ИГРА «НИМ»

Ним – это конечная игра с полной информацией, которая является фундаментом математической теории комбинаторных игр. Эта древняя китайская игра пришла в Европу только в 16 веке, а известное нам название, одновременно с доказательством того, что у неё есть выигрышная стратегия, получила только в 20 веке. И то, и другое сделал математик Чарльз Бутон.

В 30-х годах XX в. независимо друг от друга два математика — Р. Шпраг и П.М. Гранди — разработали теорию, описывающую равноправные игры. И Ним имеет фундаментальное значение для этой теории, так как в ней утверждается, что любая равноправная игра двух игроков эквивалентна обычному Ниму.

Рассмотрим правила игры. Два игрока поочерёдно берут предметы из кучек. Число кучек и число предметов может быть произвольным, и выкладываются они заранее, до начала игры. Взять разрешается любое число предметов из любой кучки, даже всю кучку целиком, но хотя бы один предмет взять обязательно, и брать предметы можно только из одной кучки. Игрок, взявший последний предмет, выигрывает игру.

Какова же выигрышная стратегия этой игры? Рассмотрим все возможные случаи.

Если у нас всего одна кучка, то стратегия проста: забрать всю кучу и выиграть.

Если их две, то стратегия следующая: одним ходом нужно уравнять количество камушков в кучках, а потом, после хода противника, просто копировать его ход на другой кучке. И тогда в один момент игра сведётся к одной кучке.

Если количество кучек больше 2, то описать выигрышную стратегию не так просто. Для этого нам понадобится двоичная система счисления. Из теоремы, представленной Ч. Бутоном, текущий игрок имеет выигрышную стратегию тогда и только тогда, когда XOR-сумма размеров кучек отлична от нуля. В противном случае текущий игрок находится в проигрышном состоянии. Из доказательства теоремы можно получить следующий алгоритм выигрышной стратегии. Рассмотрим его на конкретном примере.

Пусть у нас есть 3 кучки, в них 5, 6 и 7 камушков соответственно.

1. Перевести размеры кучек в двоичную систему счисления.

Таким образом, $\mathbf{5_{10} = 101_2, 6_{10} = 110_2, 7_{10}=111_2}$.

2. Найти XOR – сумму получившихся чисел.

XOR – это бинарная операция, результат выполнения которой будет равен 1 тогда, когда количество аргументов, равных 1, составляющих текущий набор, — нечетное, в противном случае, результата равен 0. (рис.1)

Применив эту операцию к нашим числам, получим XOR-сумму(Ним-сумму) 100 (рис.2).

3. Найти первый ненулевой бит в Ним-сумме. (рис.3)

4. Найти число с таким же ненулевым битом. (рис.4)

Выбираем любое из них и применяем к нему XOR операцию с полученной ранее Ним-суммой. Полученное число – это то количество камушков, которое мы должны оставить в той кучке, с которой только что проводили вычисления. Заменив это число, мы должны получить нулевую Ним-сумму.

A	B	XOR
0	0	0
0	1	1
1	0	1
1	1	0

Рисунок 1 Рисунок2
Рисунок 3 Рисунок 4

Отсюда мы видим, что из любого числа с таким же ненулевым битом мы можем сделать нулевую Ним-сумму.

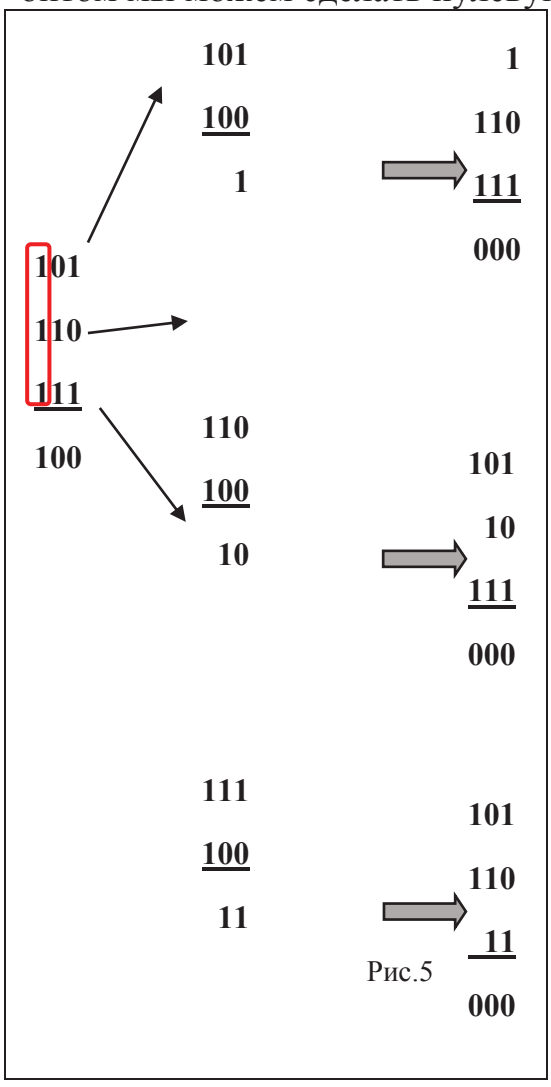

Рис.5

Далее противник, находясь в проигрышной позиции, делает абсолютно любой ход, так как гарантированно он переведет игру в состояние с ненулевой Ним-суммой. После его хода мы снова повторяем свои действия. В конечном итоге игра сведётся к случаю с двумя кучками, а затем с одной.

Так же мы должны отметить, что не всегда выгодно ходить первым. Если на начало игры Ним-сумма уже равна 0, то стоит предложить начать игру сопернику, тогда вы, заранее зная выигрышную стратегию, обеспечиваете себе победу, либо придётся ждать оплошности соперника.

Игра — это высшая форма исследования. Наша жизнь – это тоже игра. У которой пока что нет выигрышной стратегии, но кто его знает, может, и эта игра в конечном итоге сведётся к Ниму.

ЛИТЕРАТУРА

1. Гашков, С. Б. Системы счисления и их применение. М.: МЦНМО, 2004. 52 с.

2. Шень, А. Игры и стратегии с точки зрения математики. М.: МЦНМО, 2008. 40 с.

3. Теория Шпрага-Гранди. Ним. [Электронный ресурс] / MAXimal. – 2014. / Режим доступа: http://e-maxx.ru/algo/sprague_grundy#2. Дата доступа: 25.03.2017.

4. Фролов И.С. Введение в теорию комбинаторных игр. 2012. 202 с.

УДК 004.021

Студ. А.Н. Зайцев

Науч. рук. асс. Т.Г. Шагова

(кафедра высшей математики, БГТУ)

МЕТОДЫ СГЛАЖИВАНИЯ ИЗОБРАЖЕНИЙ

В современном мире огромная часть информации представлена в виде изображений. И часто бывает, что на изображениях имеются различного вида искажения. Одним из видов искажения является эффект «зубчатости». Мало того, что данный эффект портит впечатление от изображения из-за неровных краёв, зубчатость крайне негативно сказывается, например, на оптическом распознавании символов. Именно поэтому в данном случае следует применять алгоритмы сглаживания.

Для сглаживания применяют следующие сглаживающие фильтры: фильтр Гаусса, медианный фильтр, обобщённый медианный фильтр, билатеральный фильтр, нелокальный фильтр, морфологический фильтр.

Самые простые фильтры - основанные на матрицах свёртки. Матрица свёртки – это матрица коэффициентов, на которую «умножается» значение пикселей изображения для получения требуемого результата. Пример свёрточного фильтра следующий:

Входное изображение Матрица

$$\begin{pmatrix} 12 & 14 & 41 \\ 43 & 84 & 24 \\ 2 & 1 & 43 \end{pmatrix} \times \begin{pmatrix} 0{,}5 & 0{,}75 & 0{,}5 \\ 0{,}75 & 1{,}0 & 0{,}75 \\ 0{,}5 & 0{,}75 & 0{,}5 \end{pmatrix} =$$

$$= \begin{pmatrix} 12 * 0{,}5 + 14 * 0{,}75 + 41 * 0{,}5 + \\ 43 * 0{,}75 + 84 * 1{,}0 + 24 * 0{,}75 + \\ 2 * 0{,}5 + 1 * 0{,}75 + 43 * 0{,}5 \end{pmatrix} \times \frac{1}{\text{div}} = 31{,}41667,$$