Изучение свойств подстановок, порождаемых сдвиговыми преобразованиями

проект

К. Царегородцев[1, 2]

[1]МГУ им. М. В. Ломоносова
Москва, Россия

[2]АО «НПК «Криптонит»

3 августа 2023 г.

О шифровании, сохраняющем формат

- Шифрование, сохраняющее формат (Format preserving encryption) — алгоритм, зашифровывающий сообщения из произвольного (обычно довольно маленького) конечного множества Dom таким образом, что результат зашифрования также лежит в Dom.
- “Обычный” блочный шифр действует на множестве двоичных строк фиксированной длины (например, 128 бит для “Кузнечика”), результат шифрования элемента $m \in \mathrm{Dom}$ может оказаться вне Dom.
- Нужно уметь порождать псевдослучайные подстановки на “маленьких” множествах Dom.

Постановка задачи

Один из предлагаемых подходов заключается в следующем:

- рассмотреть некоторую алгебраическую структуру $Q = \mathrm{Dom}$ с операцией $\circ$ (мы хотим замкнутость относительно умножения, чтобы оставаться внутри Dom); минимальное требование: обратимость слева и справа (квазигруппа);
- для «зашифрования» элемента $m \in \mathrm{Dom}$ нужно вычислить:

$$ct = q_1 \circ (q_2 \circ \ldots (q_\ell \circ m) \ldots)$$

- можно также чередовать левые и правые умножения.

Вопрос: хорошо ли это?

Постановка задачи-2

$$ct = q_1 \circ (q_2 \circ \ldots (q_\ell \circ m) \ldots)$$

- насколько такая структурированная псевдослучайная подстановка отличается от истинно случайной?
- как зависит от структуры квазигруппы? от числа элементов ℓ? от типов сдвигов?
- хотя бы: каковы статистические свойства указанных структурированных подстановок:
  - равнораспределенность среди всех подстановок?
  - длины циклов?
  - неподвижные точки? ...

Что хотелось бы получить в итоге?

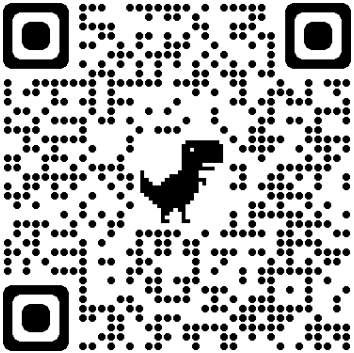
В идеале...

1. Посмотреть различные систематические способы задания квазигрупп на некотором множестве ($\approx$ алгебра/дискретная математика).
2. Посмотреть, как в литературе предлагается тестировать «относительно маленькие» подстановки на псевдослучайность ($\approx$ вероятность/статистика).
3. Реализовать какие-нибудь “перспективные”, но относительно простые способы задания квазигрупп и попробовать погенерировать структурированные подстановки с помощью них ($\approx$ программирование).
4. Поизучать статистические свойства получаемых подстановок с помощью найденных тестов; результаты красиво и аккуратно записать в таблицу ($\approx$ анализ данных/описательная статистика).

Что требуется?

- умение читать статьи на английском языке;
- общее знакомство с тем, что такое подстановки, группа подстановок, циклы, неподвижные точки, etc;
- общее знакомство с тем, что такое мат. статистика и что такое тестирование гипотез;
- навыки программирования — реализовать стат. тест, реализовать порождение квазигруппы и т.д.;

Присоединяйтесь к проекту!



https://github.com/kirtsar/summerschool23_shift