Спецкурсы Н.К. Верещагина.

1-ый семестр: “Сложность вычислений"

Сложность вычислений относится к образовательному минимуму, которым должен овладеть любой математик, пишущий программы для компьютера. На заре теории алгоритмов считалось, что главной задачей является разделение алгоритмических проблем на разрешимые (те, для которых есть алгоритм решения) и неразрешимые (когда алгоритма нет). Главными достижениями той эпохи были доказательство неразрешимости 10-ой проблемы Гильберта (состоящей в построении алгоритм для решения систем полиномиальных диофантовых уравнений от нескольких переменных) и построение алгоритма разрешения элементарной геометрии.

Однако в 1960-ых и 1970-ых годах было осознано, что более важным для практики является разделение алгоритмических проблем на быстро разрешимые и долго-разрешимые. В эти годы возникли методы доказательство долго-разрешимости. В частности, было установлено, что никакой алгоритм не может по утверждению элементарной геометрии выяснить его истинность быстрее, чем за время, экспоненциально растущее с ростом длины записи исходного выражения. А для очень широкого класса практически важных проблем (так называемых NP трудных задач) было показано, что маловероятно существование быстрых алгоритмов их решения. В спецкурсе будет подробно изложено, что это значит и как это доказывается. В частности, будет рассказано,

- что такое алгоритм и как грамотно определить время его работы,
- почему алгоритмы не могут производить арифметические операции с действительными числами и насколько быстро они могут выполнять операции с целыми числами,
- как доказать, что для данной задачи не существует быстрого алгоритма решения,
- что значит, что одна алгоритмическая проблема сводится к другой и как это можно доказать,
- бывают ли задачи, для которых доступ к датчику случайных чисел помогает решить задачу быстрее,

- что такое класс NP и что такое проблема перебора.

Курс Сложность вычислений рекомендуется прослушать тем, кто собирается слушать следующие "практически ориентированные"курсы, читаемые Н.К. Верещагиным: Коды с исправлением ошибок, Математическая криптография, Коммуникационная сложность, Построение генераторов псевдослучайных чисел.

Для лучшего усвоения курса полезно (хотя и не обязательно) знакомство с первой половиной курса "Избранные главы дискретной математики" (лектор И.В.Артамкин).

2-ой семестр: "Коды с исправлением ошибок"

Коды с исправлением ошибок нужны для передачи информации по ненадежному каналу. Исходное слово в данном алфавите (сообщение) кодируется так, что после любой замены в кодовом слове небольшого количества символов по полученному слову можно было восстановить исходное сообщение. Наиболее известными кодами такого сорта являются коды Хемминга, позволяющие исправлять одну ошибку (восстановление будет успешным, если в кодовом слове изменили только один символ или не меняли его вовсе).

При построении кода нас в первую очередь интересуют следующие два параметра: количество ошибок, которые позволяет исправить код, и отношение длины кодового слова к длине сообщения. До сих пор не удалось понять, при каких значениях этих двух параметров кодирование возможно. Наиболее известные кривые на плоскости, ограничивающие это множество параметров, называются кривыми Хемминга и Варшамова—Гилберта.

Кроме этого, нам хочется, чтобы алгоритмы кодирования и алгоритм восстановления сообщения по его коду с ошибками работали достаточно быстро (так называемые "эффективные коды"). На лекциях будет рассказано о следующих семействах эффективных кодов, имеющих довольно хорошие параметры: коды Рида—Соломона, коды Рида—Маллера, коды БЧХ (обобщение кодов Хемминга), коды Форни и Форни—Юстесена, (в них количество исправляемых ошибок составляет фиксированный ненулевой процент от длины кодового слова, причём последняя линейно зависит от длины сообщения слова).

Коды с исправлением ошибок используются практически в любой современной электронной аппаратуре, обрабатывающей информацию (на-

пример, в сотовых телефонах). Они также применяются при построении генераторов псевдослучайных чисел и в теории сложности вычислений.

Для лучшего усвоения курса полезно (хотя и не обязательно) знакомство с первой половиной курса “Сложность вычислений” и с первой половиной курса “Избранные главы дискретной математики” (лектор И.В.Артамкин).