

Применение решателей проблемы SAT к синтезу кодов, исправляющих ошибки

Антонов К.В. (ИТМО). Научные руководители – кандидат технических наук, доцент Семёнов А.А. (ИТМО, ИДСТУ СО РАН); кандидат технических наук, Трофимюк Г.А. (ИТМО)

Введение. Коды, исправляющие ошибки (корректирующие коды), являются одним из базовых концептов, используемых для передачи информации. Основная идея корректирующих кодов состоит в использовании избыточности для обеспечения возможности исправлять ошибки в сообщениях, передаваемых по каналам с шумом. Линейные коды образуют важный подкласс корректирующих кодов, поскольку имеют простое определение и естественные процедуры декодирования. Линейные коды имеют красивую математическую природу, в основе которой лежит линейная алгебра над конечными полями. Проблема построения линейных кодов с параметрами, которые в некотором роде близки к оптимальным, представляет собой актуальную задачу с большим спектром практических приложений. В докладе предполагается представить ряд результатов по синтезу близких к оптимальным двоичных линейных кодов при помощи комбинаторных алгоритмов, используемых для решения проблемы булевой выполнимости (SAT).

Основная часть. Рассматриваются линейные двоичные коды. Множество всех двоичных слов длины n образует булев гиперкуб размерности n , обозначаемый через $\{0,1\}^n$. На данном множестве можно задать структуру линейного векторного пространства над полем из двух элементов $GF(2)$. Данное пространство, обозначаемое далее через V_n , является метрическим, поскольку на нем определена метрика Хэмминга [1]. Для произвольного k , $k < n$, рассмотрим произвольное линейное подпространство размерности k в V_n , из которого удален нулевой вектор. Данное подпространство называется линейным $[n, k]$ – кодом. Если любые два вектора в $[n, k]$ – коде находятся друг от друга на расстоянии Хэмминга $\geq d$, притом что есть хотя бы один вектор в данном подпространстве с весом Хэмминга, равным d , то такой код называется (n, k, d) – кодом. Произвольный (n, k, d) – код может использоваться для исправления $t = \left\lfloor \frac{d-1}{2} \right\rfloor$ ошибок, возникающих в двоичных словах длины n , передаваемых по двоичному симметричному каналу с шумом [2]. Корректирующие коды интересны еще и как комбинаторные конструкции, которые могут существовать не для любых наборов значений параметров n, k, d . Известен целый ряд границ, определяющих существование линейных кодов. Например, одной из простейших является граница Синглтона [2], согласно которой для любого линейного двоичного кода выполняется следующее неравенство: $d \leq n - k + 1$. Другой известный пример – граница Хэмминга или граница сферической упаковки [2]: $M \cdot \left(1 + \sum_{i=1}^t \binom{n}{i}\right) \leq 2^n$, где M – число слов двоичного (не обязательно линейного) кода. Таким образом, для целого ряда наборов значений параметров n, k, d вывод о существовании соответствующего кода можно сделать на основании некоторой известной границы. Однако возможны ситуации, когда значения n, k, d не противоречат известным границам, но примеров кодов с этими параметрами не известно. Один из примеров подобного рода – набор $n = 35, k = 10, d = 13$. Притом что $(35, 10, 12)$ линейный код существует. Задача о существовании кодов с относительно небольшими значениями параметров n, k, d может быть сведена к проблеме булевой выполнимости (SAT), для решения которой разработаны алгоритмы (SAT-решатели), имеющие весьма широкий спектр практического применения [3]. В рамках настоящего доклада будет представлена общая техника сводимости задачи существования линейного двоичного (n, k, d) кода к SAT и результаты синтеза ряда известных кодов с использованием SAT решателей. Кроме этого будут представлены результаты синтеза кодов, близких к гипотетическим неизвестным (n, k, d) кодам. Для построения таких кодов использовались специальные техники декомпозиции трудных примеров задачи SAT, в частности, стратегия Cube-and-Conquer [4].

Выводы. Разработан алгоритм, позволяющий сводить проблему существования линейного (n, k, d) – кода к задаче булевой выполнимости (SAT). С использованием современных SAT

решателей и построенных кодировок синтезирован ряд известных линейных (n, k, d) . Также построены коды, близкие к гипотетическим неизвестным (n, k, d) — кодам, незначительно отличающиеся от таких кодов по весовому спектру.

Автор выражает благодарность О. С. Заикину за помощь в применении к рассматриваемым задачам решателей на основе стратегии Cube and Conquer.

Список использованных источников:

1. Hamming R.W. Error detecting and error correcting codes // The Bell System Technical Journal. — 1950. — Vol. 29. — Iss. 2. — P. 47-60.
2. Mac-Williams F.J., Sloane N. The theory of error-correcting codes. Elsevier, 1977.
3. Biere A., Heule M., van Maaren H., Walsh T. Handbook of Satisfiability. IOS Press, 2021.
4. Heule M., Kullman O., Wieringa S., Biere A. Cube and Conquer: Guiding CDCL SAT Solvers by Lookaheads // Lecture Notes in Computer Science. — 2011. — Vol. 7261. — P. 50-65.