

**Программная реализация декодера одного класса
помехоустойчивых кодов на алгебраических кривых.
Проектирование на основе шаблонов обобщённого и мета-
программирования**
Пеленицын А.М.

Южный федеральный университет, apel@sfedu.ru

We present the decisions made in our software implementation of decoder for a class of algebraic geometry codes. The decisions are concerned with generic programming approach and show some metaprogramming techniques which, we believe, are of considerable importance for similar problems from the field of error-correcting codes or, more generally, computational algebraic geometry. We also describe some features of C++11 which are aimed to improve generic programming capabilities of the C++ programming language.

Построение помехоустойчивых кодов на основе алгебраических кривых (АГ-кодов) и методы их декодирования [1] используют ряд абстрактных математических объектов, программная реализация которых представляет собой более сложную задачу, чем в случае классических кодов. Поскольку доступно лишь ограниченное число открытых реализаций декодеров для АГ-кодов [2,3], опыт их реализации представляет интерес как с теоретико-кодовой точки зрения, так и в контексте целого класса наукоёмкого программного обеспечения. Тот факт, что конструкции помехоустойчивых кодов имеются в некоторых системах компьютерной алгебры, например GAP (пакет GUAVA [4]), позволяет рассматривать вопрос о возможности интеграции проделанной работы в такие системы.

Язык программирования C++ является достаточно универсальным инструментом для создания наукоёмкого открытого ПО: один из ведущих компиляторов C++, входящий в состав GCC, хорошо переносим и имеет свободную лицензию. Также важно то, что данный компилятор открывает доступ к последним изменениям в языке C++, отражённым в новом стандарте, который принято обозначать C++11 (ранее: C++0x) [5]. Важным является тот факт, что значительная часть нововведений языка посвящена расширению поддержки обобщённого программирования, а также (или — в частности), функционального программирования на C++.

Одной из интересных особенностей данного языка являются шаблоны C++. В ряде работ [6,7,8] было продемонстрировано, насколько мощными являются выразительные средства, представляемыми шаблонами. Здесь можно выделить самостоятельный подход к программированию, называемый «обобщённое программирование», а также набор приёмов, объединяемых понятием «метапрограммирование».

В докладе рассматривается ряд техник, использованных в полученной автором реализации декодера: рекурсивное инстанцирование шаблонов,

классы характеристик типов и одна общая проблема, связанная с ними, а также её решение, классы стратегий. Данные техники основаны в той или иной степени на механизме шаблонов C++. Особое внимание уделено применению средств C++11.

Литература

1. Nøholdt T., van Lint J.H., Pellikaan R. *Algebraic geometry codes* // *Handbook of Coding Theory*, V.S.Pless, W.C. Huffman, and R.A. Brualdi, Eds. Amsterdam, The Netherlands: Elsevier, pp. 871–961, 1998.
2. Madelung Y. “Implementation of a decoding algorithm for AG-codes from the Hermitian curve,” Rept. IT 93-137, Inst. Circuit Theory Telecom., Tech. Univ. of Denmark, Lyngby, Denmark, Apr. 1993.
3. Маевский А.Э., Пеленицын А.М. О программной реализации алгебро-геометрического кодека с применением алгоритма Сакаты // В сб. «Материалы X Международной научно-практической конференции „Информационная безопасность“», ч.2. Таганрог. ЮФУ. 2008. С. 55–57.
4. GUAVA A GAP4 Package for computing with error-correcting codes <http://sage.math.washington.edu/home/wdj/guava/htm/chap0.html>
5. C++0x/C++11 Support in GCC <http://gcc.gnu.org/projects/cxx0x.html>
6. Abrahams D., Gurtovoy A.. C++ Template Metaprogramming: Concepts, Tools, and Techniques from Boost and Beyond. Addison-Wesley, 2004.
7. Вандевурд Д., Джосаттис Н. Шаблоны C++: справочник разработчика. М.: Вильямс, 2003. 544 с.
8. Александреску А. Современное проектирование на C++. М.: Вильямс, 2002. 336 с.