ставляет труда, а также в связи с тем, что основание a является константой, затраты на нахождение a^{-1} можно считать несущественными.

Предложен эффективный алгоритм построения такой последовательности, заключающийся в просмотре двоичного представления показателя справа налево с инвертированием всех встречающихся битовых групп вида 011...1, результатом которого является факторизованное представление показателя, содержащее небольшое количество единиц. Информация о расположении инвертированных групп используется для управления умножением на a^{-1}.

ЛИТЕРАТУРА:

1. W. Diffie, M. Hellman "New directions in cryptography" // IEEE Transactions on Information Theory, v. IT-22, Nov. 1976, pp. 644-654.

2. R.L. Rivest, A. Shamir, L. Adleman, "A method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of ACM, Feb. 1978, Vol. 21. № 2.

3. Д.Кнут. Искусство программирования для ЭВМ. Т.2 Получисленные алгоритмы. М.: Мир, 1977, с.482-510.

ИНСТРУМЕНТАЛЬНАЯ СИСТЕМА ФУНКЦИОНАЛЬНОГО ПРЕКТИРОВАНИЯ МУЛЬТИПРОЦЕССОРНЫХ СИСТЕМ РЕАЛЬНОГО ВРЕМЕНИ

Радишевский В.А.

В докладе рассматривается система функционального проектирования мультимикропроцессорных управляющих вычислительных комплексов (ММПУВК) реального времени.

Система предназначена для решения задачи доказательства однозначности и безтупиковости параллельного алгоритма и задачи назначения задач на процессоры. Математическая модель ММПУВК базируется на информационно-логическом графе, отражающем связи по управлению внутри задач и информационные связи между задачами. Для ММПУВК с заранее определенными свойствами задач возможно применение точных или близких к точным методов решения этих задач, которые в данном случае становятся задачами статического планирования и диспетчеризации.

Инструментальная система проектирования ММПУВК реального времени состоит из подсистем, взаимодействующих следующим образом.

Входное описание *. RTX (от Real Time eXecutive) представляет собой текстовый файл, описывающий структуру задач параллельной программы и их предопределенные атрибуты. Препроцессор описания ТР определяет вычисляемые атрибуты задач (например, время выполнения) и проверяет безтупиковость параллельной программы. Подсистема аналитического моделирования АМ кроме входного описания получает файл

спецификации процессорных модулей (ПМ), содержащий такие характеристики доступных ПМ, как тип, относительная производительность и цена в любых относительных единицах. Подсистема осуществляет назначение задач на процессорные модули, причем целевой функцией является их стоимость, и осуществляет статическую диспетчеризацию задач, состоящую в подстановке во входное описание системных вызовов, изменяющих взаимные приоритеты задач. Таким образом, на вход подсистемы имитационного моделирования SS поступит файл *.RTS, содержащий в отличие от *.RTX информацию о назначении задач на процессоры. Подсистема SS базируется на программном имитаторе ядра операционной системы реального времени, причем в режиме разделения времени имитируется параллельная работа всех процессоров ММПУВК.

Инструментальная система реализована для IBM-совместимых ПЭВМ на языках Ассемблера и Си.

АЛГОРИТМЫ ВИЗУАЛИЗАЦИИ ПОСЛОЙНЫХ МОДЕЛЕЙ ТРЕХМЕРНЫХ ОБЪЕКТОВ.

Садыхов Р.Х., Белов Д.И.

Задача удаления невидимых линий и поверхностей является одной из наиболее сложных в машинной графике и имеет широкий спектр приложений, включая медицинские исследования при диагностике различных органов.

В докладе представлена формулировка указанной задачи и предложены новые алгоритмы удаления невидимых поверхностей, применимые в медицине для визуального наблюдения внутренних органов в режиме времени, близком к реальному. Данные алгоритмы используют двоичное разбиение пространства, межкадровую однородность по наблюдаемости и новый подход к решению задачи о принадлежности точки выпуклому многоугольнику. В докладе показано, что если L - количество слоев объекта, а MaxN - максимальное количество вершин из всех аппроксимирующих многоугольников, то предварительная обработка требует O(LMaxN) времени.

Разработанный алгоритм выполняется в два этапа: на первом этапе решается задача удаления невидимых слоев, а на втором осуществляется удаление невидимых граней в пределах каждого слоя.

Сходимость данного алгоритма обеспечивается тем, что количество вершин выпуклого многоугольника конечно и на каждом шаге число рассматриваемых вершин уменьшается вдвое. Доказан ряд теорем, являющихся теоретической основой предложенного подхода.

Для подтверждения основных положений были выполнены эксперименты с алгоритмами локализации точки относительно выпуклого многоугольника и удаления невидимых поверхностей. Для экспериментов генерировались с использованием датчика выпуклые многогранники, которые располагались случайным образом в пределах каждого слоя.