www.esa-conference.ru

Разработка концептуальных и теоретических моделей для иерархических систем

Батурин Геннадий Иванович, кандидат педагогических наук, доцент
Дальневосточный федеральный университет

Аннотация. *В наше время всеобщей компьютеризации, особенно актуален вопрос использования компьютерных технологий в системе образования. При создании новых электронных образовательных средств необходимо в полной мере использовать те возможности, которые предоставляет компьютер. Стандартное изложение материала на электронном носителе отличается от книжного в основном только простотой доступа к этому материалу и, если материал не содержит большого количества изобразительного материала, других преимуществ не имеет. В любой книге материал излагается последовательно и линейно. Идеям структуризации материала посвящены работы [1; 2]. Использование компьютера позволяет гораздо более детально и целенаправленно структурировать материал. В предлагаемой работе описывается информационный граф курса «Дискретной математики», на основе которого создается электронное учебное пособие нового поколения.*

DOI: 10.5281/zenodo.3363933

Дискретная математика, или дискретный анализ, – область математики, которая занимается изучением структур и задач на конечных множествах.

В настоящее время, на наших глазах происходит стремительное проникновение этого курса в учебные планы специалистов все новых и новых направлений. Конечно, это связано с бурным развитием компьютерных технологий, а также с тем, что математическая составляющая стала стержнем подготовки современного специалиста не только в области физики, химии или биологии, но и в экономике, социологии и даже юриспруденции.

В широком смысле она включает в себя не только уже сложившиеся дисциплины (теория чисел, алгебра, математическая логика, комбинаторный анализ и др.), но и ряд разделов, которые стали развиваться, в связи с развитием компьютерной техники и компьютерных наук, которые базируются, а по существу являются продолжением дискретной математики и логикой внутреннего развития этих наук

В узком смысле дискретная математика ограничивается только новыми разделами (теория функциональных систем, теория сетей, комбинаторика, теория кодирования, целочисленное программирование, теория игр, конфликтных ситуаций, компьютерная дискретная математика и др.). Появлением новых разделов, глубоких интересных проблем, развитием мощных методов их решения Дискретная математика является сегодня не только фундаментом математической кибернетики, но и важным звеном образования. При изучении курса у студентов должно сложиться представление о ней как богатой и содержательной части естественнонаучного знания. Все это и предопределило тот факт, что различные разделы дискретной математики все настойчивее внедряются не только в университеты, но и в технические и экономические вузы и даже в гуманитарные.

С учетом специфики основных разделов курса и специальностей, для которых он предназначен, повышенное внимание должно уделяться формированию у студентов практических навыков решения задач, а также проблемам решения прикладных задач с точки зрения возможности их программной реализации на компьютере. В то же время изложение теоретического материала должно сопровождается строгим математическим обоснованием.

Содержание курса должно определяться его задачами: развитием ***комбинаторного,*** теоретико-множественного, теоретико-графового, алгоритмического мышления.

Комбинаторика – раздел курса дискретной математики, ориентированный на решение задач выбора и расположения элементов некоторого множества в соответствии с заданными правилами и ограничениями. Главное отличие изложения комбинаторики в курсе дискретной математики от обычного заключается в необходимости умения выводить формулы с помощью логических комбинаторных рассуждений. Алгебраические способы носят выраженный вспомогательный характер Эффективное усвоение и применение учебного материала остальных разделов курса возможно лишь при глубоком развитии комбинаторного мышления, знании правил комбинаторных рассуждений, методов комбинаторного анализа и формул комбинаторики.

Изложение курса комбинаторного анализа часто ограничивается рассмотрения размещений, сочетаний и перестановок без повторений. В нашем случае во всех разделах дискретной математики требуется умение применять формулы вычисления сочетаний, размещений и перестановок с повторениями

Этот раздел математики тесно связан с рядом других разделов дискретной математики: теорией вероятностей, теорией графов, теорией чисел, теорией групп и т. д.

Долгое время теория графов считалась разделом конечной геометрии, находящей некоторые применения к решению логических задач. Однако, в последнее время приложения теория графов привлекают все более пристальное внимание специалистов различных областей знания. Наряду с традиционными применениями ее в таких науках, как физика, электротехника, химия, она проникла и в науки, считавшиеся раньше далекими от нее, в экономику, социологию, математическую лингвистику, теорию информации, электронику и другие области науки и техники, не говоря о программировании, исследова-

ЕВРАЗИЙСКОЕ НАУЧНОЕ ОБЪЕДИНЕНИЕ
EURASIAN SCIENTIFIC ASSOCIATION
www.esa-conference.ru

нии операций и управлении и д р. Давно известны тесные контакты теории графов с топологией, теорией групп и теорией вероятностей. Особенно важная взаимосвязь существует между теорией графов и теоретической кибернетикой (особенно теорией автоматов, исследованием операций, теорией кодирования, теорией игр). Теория графов оказалась удобным языком для формулировки задач, относящимся в широкому кругу научных проблем, и предоставила эффективные инструменты для их решении. Широкие возможности приложений заложены уже в самом понятии графа, сочетающего теоретико-множественные, комбинаторные и топологические аспекты.

В математике, широко исследуются дискретные функции, так как с их помощью удается описывать широкий класс природных явлений. Наиболее известным примером дискретных функций являются булевы функции. Их более полное название – функции алгебры двузначной логики, т. е. теория булевых функций – это раздел математической логики. Они находят широкое применение в электронных вычислительных и управляющих системах, играют важную роль при передаче информации. Развитие методов криптографического анализа привело к выделению ряда свойств, важных с криптографической точки зрения. Использование нелинейных булевых функций в качестве компонент современных шифров позволяет повышать стойкость шифров к методам линейного и дифференциального криптоанализа. Криптографические схемы, построенные с их использованием, успешно противостоят различным методам анализа, например статистическому, корреляционному, дифференциальному, линейному. Изложение теории булевых функций в курсе дискретной математики отличается от их изложения в курсе математической логики прикладной направленностью и креном в сторону комбинаторного аспекта.

Возможности it-специалиста и простого пользователя компьютера существенно повышается после его знакомства с основами теории кодирования и криптографии.

Криптография – наука о защите информации от чужого глаза. В прошлом криптография была наукой, которой интересовались в основном дипломаты и военные, но с распространением компьютеров эта наука стала одной из самых востребованных прикладных. Методы этих наук схожи. Часто эти науки применяют одни и те же алгоритмы. В отличие от других методов, они опираются лишь на свойства самой информации и не используют свойства ее материальных носителей, особенности узлов ее обработки, передачи и хранения. Образно говоря, криптографические методы строят барьер между защищаемой информацией и реальным или потенциальным злоумышленником из самой информации.

Процедуры кодирования и шифрования присущи всем современным системам хранения, сбора, передачи и обработки цифровых данных, будь то цифровое радио и телевещание, спутниковая навигация и т. п.

Под криптографической защитой в первую очередь подразумевается шифрование данных. Раньше, когда эта операция выполнялось человеком вручную или с использованием различных приспособлений, содержались многолюдные отделы шифровальщиков. Развитие криптографии сдерживалось проблемой реализации шифров, ведь придумать можно было все что угодно, но как это реализовать.

Сложилось условное разделение на теорию кодирования и декодирования и на криптографию. Теория кодирования и декодирования – это наука о преобразовании информации с целью удобства работы с ней, защиты информации от искажений при хранении, передаче по каналам связи, работе с информацией в разных технических устройствах. Важную часть современного образования составляет алгоритмическое мышление. Активно его развитие происходит на занятиях по дискретной математики при изучении машины Тьюринга и рекурсивных функций.

Допустим, что теоретический курс разбит на информационные единицы (определения, понятия, факты, теоремы), которые надо усвоить в процессе обучения. Построим ориентированный граф следующим образом: вершины графа – информационные единицы, две вершины соединены ребром, если для понимания информационной единицы, соответствующего второй вершине, необходимо знания информационной единицы, соответствующего первой вершине. Построенный граф называется информационным графом предметной области. Ясно, что полученный граф должен быть ациклическим. Требование простоты причинно-следственных связей является еще одним естественным условием, которому должен удовлетворять информационный граф. А это означает, что каждая вершина графа должна быть инцидентна небольшому множеству ребер. На этих идеях сконструирована и реализована электронная энциклопедия ЛИНЕАЛ, предназначенная для получения теоретических сведений в области линейной алгебры [3]. При этом вершины графа можно помечать в зависимости от уровня сложности или уровня необходимости данной информационной единицы. Таким образом, в графе можно выделять подграфы, отвечающие требованиям к изучаемой дисциплине, например:

– изучение дисциплины первоначальное;
– изучение дисциплины профессиональное;
– изучение дисциплины в соответствии с разными сетками расчасовки;
– изучение дисциплины в соответствии с направлением подготовки.

Дискретная математика является удобным полигоном для показа преимуществ электронного учебного пособия и учебника нового поколения. Следует отметить, что этот раздел современной математики достаточно быстро меняется и имеет много приложений. В учебном пособии курса дискретной математики есть необходимость иллюстрирования учебного материала большим количеством схем, таблиц, живых картинок при демонстрации эволюции графа. Курс в минимальной степени опирается на теоремы математического анализа, алгебры и геометрии, но оказывается в максимальной степени востребован для более глубокого усвоения материала этих и других дисциплин. В сложившийся курс дискретной математики обычно включаются такие разделы, как

ЕВРАЗИЙСКОЕ НАУЧНОЕ ОБЪЕДИНЕНИЕ
EURASIAN SCIENTIFIC ASSOCIATION
www.esa-conference.ru

теория множеств, комбинаторика, теория булевых функций, теория графов, теория кодирования и теория алгоритмов.

Имеется самая разнообразная учебная литература по дискретной математике. Нами была предпринята попытка построить информационный граф по материалам из книг. Оказалось, что этот граф содержит большое количество вершин, инцидентных слишком большому множеству ребер. Отсутствие промежуточных утверждений делает доказательство многих утверждений громоздкими, т.е. не выполняется одно из необходимых требований к информационному графу - простота структуры причинно-следственных связей. По этой причине имеющийся материал пришлось переписать заново, исходя из сформулированных требований. В новом варианте большинство утверждений имеют не более пяти опорных связей. Полученный информационный граф позволяет разработать электронный учебник по дискретной математике нового поколения. К настоящему моменту уже созданы электронные учебные пособия по комбинаторики и теории графов. Эти учебные пособия предназначены для изучения дискретной математики студентами различных специальностей на факультетах математического, физического и экономического профиля. Каждой специальности присваивается свой вес. Каждому весу сопоставляется свой подграф информационного графа. Этот граф позволяет в рамках созданного учебного пособия изучать данный предмет с учетом специфики специальности и цели изучения. Кроме того, учебное пособие позволяет использовать его как справочное пособие, в котором можно не только мгновенно отыскать необходимое понятие (определение, утверждение), но и все факты, необходимые для усвоения этого понятия (определения, утверждения). Цели нашего изложения потребовали определения основных понятий в наибольшей общности с обсуждением всевозможных трактовок, с точно таким подходом к проводимым рассуждениям

При апробация электронных учебных пособий, выяснилось, что работа студентов с такими электронными пособиями позволяет существенно улучшить качество усвоения материала, повысить интерес к изучаемому предмету, активизировать их работу на занятиях. Изложение материала стало более компактным и доступным.

Курс дискретной математики построен в виде иерархического комплекса. Это позволяет в зависимости от целей изучения, уровня требований, создавать на бумажных носителях специализированные учебные пособия, соответствующие индивидуальным запросам изучающих курс или обучающих. Допускается изложение его в виде раздела курса высшей математики, математических методов в экономики. Теория графов – прекрасная тема для кружковых занятий в школах и вузах.

Литература:

1. Воеводин В.В., Воеводин Вл.В. Электронные образовательные средства: новые идеи // Вычислительные методы и программирование. 2003. Т. 4, № 1. С. 207-212.

2. Батурин Г.И. Методика разработки электронного учебного пособия нового поколения // Перспективные технологии оценки и мониторинга качества в образовании. Сборник научных трудов. – Владивосток: Изд-во Дальневост. Ун-та, 2003, с. 296-297.

3. Воеводин В.В., Воеводин Вл.В. ЛИНЕАЛ: электронная энциклопедия по линейной алгебре // Вычислительные методы и программирование. 2002. Т. 3, №1. С. 131-140.

4. Яблонский С. В. Введение в дискретную математику: Учеб. Пособие для вузов/ Под ред. В.А. Садовничего. – М.: Высш. шк.; 2003. – 384 с.

5. Москинова Г. И. Дискретная математика. Математика для менеджера в примерах и упражнениях. Учебное пособие. – М.: Логос, 2003. – 240 с.

6. Новиков Ф. А. Дискретная математика для программистов: Учебник для вузов. 3-е изд. – СПб.: Питер, 2009. – 384 с.

7. Червяков Н.И., Евдокимов А.А., Галушкин А.И. Применение искусственных нейронных сетей и системы остаточных классов в криптографии. М.: Физматлит, 2012. 280 с.

8. Батурин В.К. Общая теория управления: учебное пособие. М.: Юнити-Дана, 2015. - 487 с.

9. Панкратова И.А. Булевы функции в криптографии: учебное пособие. Томск. Издательский Дом Томского государственного Университета,2014. – 88 с.