В нашей книге предлагается подход к доасимптотическому анализу комбинаторных схем через алгоритмизацию решения задач перечисли-тельной комбинаторики.

Главным основанием целесообразности проведения доасимптотического анализа процессов (исходов комбинаторных схем), наряду с их асимптоти-ческим анализом, является принципиальное различие их целей (а значит и разных отдельных результатов), достижение которых требует различия используемых средств. При асимптотическом анализе ставится целью выявление тенденций развития процессов, т. е. их предельного поведения при неограниченном росте определенных параметров, сводящееся к клас-сификации этих тенденций, приводящих к асимптотическому сглаживанию (игнорированию) специфик изучаемых процессов и к получению прибли-женных результатов с определенной точностью в виде скоростей сходимо-сти к ним. А при доасимптотическом анализе процессов целью исследований является получение точных результатов, связанных с их поведением и разви-тием с полным учетом специфики каждого из них. Поэтому при этом необ-ходимо детальное изучение каждого процесса, включающее в себя не только количественную, но и качественную информацию о нем.

В зависимости от возможностей результаты доасимптотического анализа могут иметь как алгоритмический, так и аналитический характер.

Техническим аргументом за проведение доасимптотического анализа ис-ходов комбинаторных схем является их усложнение в связи с ростом разно-образия и ограничений в них в условиях постоянно растущей их практичес-кой востребованности и бурного прогресса возможностей вычислительных средств, что значительно расширяет область применения доасимптотических результатов и делает развитие этого направления все более актуальным.

Предлагаемый здесь перечислительный подход основан на изучении свойств исходов схемы не по результатам ее реализации, а – по их форми- рованию, и состоит в построении графа случайного процесса по некоторой процедуре явного нумерованного перечисления всех исходов комбинатор-ных схем в определенном порядке, что дает возможность визуального анализа исходов схем с учетом любых ограничений на интересующие нас исходы, включая их прямой пересчет в исходной схеме и схеме с ограни-чениями, получения их вероятностных распределений и моделирования значений ее исходов.

Визуальное представление результатов перебора исходов комбинаторных схем может использоваться непосредственно, например, в криптографии при переборе ключей, при составлении разного рода расписаний с разными ограничениями, в криминалистике в следственном анализе версий, связанных с перебором исходов комбинаторных схем, или в вычислениях при выпол-нении математических действий по индексам с определенными связями между ними. Такое математическое использование результатов перечисления всех исходов составных комбинаторных схем представлено во многих полученных в работе формулах для чисел их исходов, зависящих от конкретных видов составляющих их более простых схем. Кроме того, сама процедура прямого перечисления исходов схемы дает алгоритм нахождения числа всех ее исходов..

Для построения процедуры перебора исходов исследуемой схемы стро- ится итерационный случайный процесс последовательного поединичного добавления ее элементов для более простых (базовых) схем или этапов перебора для более сложных (составных) схем до требуемого размера с предварительным заданием вида исхода схемы и установлением определенной дисциплины нумерации всех исходов схемы при их перечислении. Оказывается, что алгоритм перебора исходов схемы дает идею вывода точной формулы их числа.

Для наглядности представления процедуры перечисления исходов и для проведения дальнейших ее исследований используется граф пошаговых (итерационных) переходов из состояния в состояние соответствующего случайного процесса. Если на дугах графа указывать вероятности переходов, то это дает возможность нахождения вероятностных распределений всех исходов комбинаторной схемы на любом шаге процесса перебора ее исходов, а значит и проведения всех возможных вероятностных исследований рассматриваемой схемы. Построение и анализ итерационной процедуры перечисления исходов комбинаторных схем на описанных графах в дальнейшем представляет метод графов (МГ).

Вероятностный анализ комбинаторных схем состоит во взаимном определении вероятностных распределений их итоговых исходов и итерационных переходных вероятностей процесса перечисления их исходов.

Бесповторное перечисление исходов схемы важно для ее дальнейшего анализа по указанным выше направлениям, а при его отсутствии вводятся дополнительные условия (ДУ), которые его обеспечивают.

Введение ДУ, как и любых ограничений, означает удаление из начального графа недопустимых по ДУ исходов, т. е. траекторий, не обеспечивающих их выполнение, что приводит к изменению вероятностей оставшихся итерационных переходов в каждом пучке каждой итерации графа перечисления исходов схемы с нарушением их суммарной единичной вероятности, пересчитываемых путем деления каждой из них на сумму вероятностей оставшихся в пучке переходов. А в результате изменяется распределение вероятностей итоговых исходов схемы. Поэтому для получения определенного их распределения нужно в задающем его случайном процессе с полученной измененной структурой менять задании вероятностей итерационных переходов.

В результате перебора всех нумерованных в реализованном порядке исходов комбинаторной схемы получаем таблицу соответствия всех видов исходов с их номерами. Установление этого соответствия будем называть решением задачи нумерации (ЗН), а нумерованное перечисление исходов схемы – ее табличным решением. В силу обычно больших объемов перебора исходов схемы хранение такой таблицы занимает большую память, что не удобно для длительного использования. В связи с этим возникает теоретическая задача нумерации, состоящая в теоретическом (формульном или алгоритмическом) установлении взаимно-однозначного соответствия между видами исходов и их номерами, т.е., по сути – две задачи: прямая и обратная задачи нумерации – ПЗН и ОЗН. В первой по данному номеру исхода нужно найти его вид, а во второй – по виду исхода – его номер. (В ЗН здесь и в дальнейшем под видом исхода пони­ мается конкретный исход схемы в принятой форме). Результат теоретического решения прямой задачи нумерации приводит к возможности универсального моделирования (УМ) исходов схемы путем разыгрывания его номера с полученным вероятностным распределением исходов по одному случайному числу, название которого связано с тем, что при простом результате теоретического решения ПЗН это дает единую (универсальную) практически удобную (без погружения в специфику схемы) процедуру моделирования исходов схемы. А по результату решения ОЗН при очевидном по логике нумерации виде последнего исхода может быть получена точная формула для числа исходов схемы.