УДК 004.4

И. А. Пушкарёв, И. А. Клюкин

**ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ДЛЯ РЕШЕНИЯ ЗАДАЧИ
ПОИСКА ЭКЗОТИЧЕСКИХ СТРУКТУР,
НЕДОПОЛНИМЫХ ДО ЛАТИНСКОГО КВАДРАТА**

Вопрос о дополнимости подмножеств клеток квадрата со стороной n , раскрашенных в n цветов так, чтобы ни в одной строке и ни в одном столбце не содержалось бы двух одноцветных клеток, до латинского квадрата, то есть – такого, в котором в любой строке и в любом столбце все клетки были бы разноцветными, является одним из старых классических вопросов современной комбинаторики расположений.

Кроме классического общеизвестного результата Райзера [1] и теоремы Галвина о «предписанном заполнении» следует отметить доказательство Б. Сметанюком так называемой «гипотезы Эванса» [2, 5] о том, что любое расположение $n-1$ клетки, не содержащее ни в строках, ни в столбцах двух одноцветных клеток, дополнимо до латинского квадрата.

Теорема Сметанюка не означает, что любое раскрашенное множество клеток, содержащее больше, чем $n-1$ клетку не является дополнимым. Можно представить себе неполное множество, содержащее, не менее, чем $n+1$ клеток, такое, что удаление любой клетки делает его дополнимым до латинского квадрата – «минимальное неполное подмножество».

Работа посвящена построению большого семейства «стандартных» минимальных больших неполных подмножеств и обсуждению задачи поиска «нестандартных» больших неполных подмножеств.

Ключевые слова: латинский квадрат, неполная структура, теорема Сметанюка.

Латинские квадраты известны с глубокой древности (это видно, например, из названия). Именно, латинским квадратом $n \times n$ называется заполнение квадрата соответствующего размера числами (далее – цветами) от 1 до n так,

чтобы в каждой строке и в каждом столбце квадрата каждый цвет присутствовал бы ровно один раз (в действительности достаточно любого из двух более слабых требований: либо того, чтобы в каждой строке и в каждом столбце присутствовали бы все цвета, либо того, чтобы в каждой строке и в каждом столбце каждый цвет присутствовал бы не более одного раза). Фактически, латинский квадрат представляет собой старейший и наиболее естественный вариант уравновешенной комбинаторной структуры. Комбинаторные структуры такого типа не только имеют массу разнообразных применений как в высокоуровневых теоретических задачах, но и естественно возникают в «задачах повседневного спроса»: оптимизационных, криптологических и т. д. Например, возможны применения задачи достраивания некоторого раскрашенного подмножества клеток квадрата (называемого в данной работе структурой) до полного латинского в построении криптографических протоколов аутентификации через доказательство с почти нулевым разглашением информации.

Задача о достраивании некоторой структуры до полного латинского квадрата рассматривается достаточно давно, начиная, по-видимому, с работы [1]. В рассматриваемом контексте следует также упомянуть работы [2], в которой была поставлена задача доказательства дополнимости любой структуры не более чем из n клеток в квадрате $n \times n$, [3, 4], в которых были сформулированы и решены очень полезные и нетривиальные задачи дополнения. В работе [5] была доказана так называемая «гипотеза Эванса» о том, что любая структура, состоящая не более чем из n клеток в квадрате $n \times n$, является дополнимой.

Однако работа [5] всё же не до конца закрыла вопрос о недополнимых структурах в латинских квадратах. Именно, назовём структуру, недополнимую до латинского квадрата минимальной, если любая структура, полученная удалением из неё одной или нескольких клеток, является дополнимой (то есть, напротив, может быть достроена до полного латинского квадрата). В действительности нетрудно показать, что для минимальности достаточно условия дополнимости до латинского квадрата только структур, полученных из (предпо-

ложительно) минимальной недополнимой удалением ровно одной клетки. Фактически, теорема Сметанюка [5] показывает, что никакая минимальная недополнимая структура не может содержать менее n клеток. Однако можно себе представить структуру, содержащую строго больше, чем n клеток, и, притом, являющуюся минимальной недополнимой.

По существу, из теоремы Сметанюка следует, что любая недополнимая структура ровно из n клеток в квадрате $n \times n$ устроена довольно стандартно: выбирается некоторая клетка (не входящая в структуру, то есть неокрашенная), и среди $2n - 2$ клеток, расположенных с ней в одной строке или в одном столбце выбирается ровно n клеток, которые красятся во всевозможные цвета. После этого, разумеется, покраска первоначальной клетки в один из допустимых цветов становится невозможной (см. рис. 1).

Используя эту идею, авторам данной работы удалось построить большое семейство стандартных недополнимых структур при помощи следующего простого алгоритма.

Шаг 1. В уже построенной недополнимой структуре выбирается клетка, покрашенная, например, в цвет $A=A_0$.

Шаг 2. Пусть в строке и столбце, содержащих выбранную клетку, уже выбраны k клеток, окрашенных в цвета $A_1, A_2, \dots, A_k$, A_i не совпадают с A_0 . Выберем в этих строках (если есть) ещё $n - 1 - k$ клеток, и окрасим их в остальные цвета, не совпадающие с цветом A_0 так, чтобы ни в одной строке или столбце квадрата не оказалось бы двух клеток одного цвета (если такая возможность есть).

Шаг 2 делает невозможным окрасить рассматриваемую клетку в любой цвет, не совпадающий с цветом A_0 .

Итерируя эти шаги, нетрудно получить дерево из минимальных недополнимых структур, которые и сами в некотором смысле имеют форму дерева. Результат одного шага описанной процедуры изображен на рис. 2.

Физико-математические науки

		1				
		2				
	7		5	6	3	
		4				

Рис. 1.

		1				
		2		1		
	7		5		3	
		4		5		
				2		
				4		

Рис. 2.

Тем самым, во-первых, получено некоторое большое семейство минимальных недополнимых структур, и во-вторых поставлена задача: существуют ли другие минимальные недополнимые структуры, которые невозможно получить при помощи описанного алгоритма (назовём эти структуры *экзотическими*).

Задача поиска экзотических структур, как и все задачи этого класса, при прямолинейном подходе требует большого перебора, а задача поиска латинского квадрата, дополняющего данную структуру, вероятно, является NP-полной. Соответственно, никакого достаточно быстрого способа решить эту задачу не существует, и требуется просто написать переборную программу (при этом рациональным шагом представляется использование средств параллельного программирования).

Приведём список программных модулей, включённых в структуру разработанного программного обеспечения.

А. Модуль генерации исходной структуры. Алгоритм работы этого модуля обеспечивает автоматическое соблюдение начального условия: любые две клетки структуры, расположенные в одной строке или в одном столбце квадрата, должны быть окрашены в разные цвета. Кроме того, этот модуль обеспечивает неповторяемость рассматриваемых структур.

Отметим, что задача организации модуля таким образом, чтобы он генерировал ровно по одному разу все допустимые структуры с данным числом клеток, оказалась крайне трудной и на данный момент мы располагаем только обоснованными надеждами, что разработанный модуль работает именно так – но никак не строгим доказательством этого факта.

В. Модуль достраивания исходной структуры до латинского квадрата. Исходное требование к этому модулю состоит в том, чтобы если уж он не нашёл ни одного латинского квадрата, дополняющего данную структуру, то такого квадрата действительно не должно существовать. На данный момент это требование можно реализовать только полным перебором – методом ветвей и границ, с отбрасыванием вариантов, бесперспективность которых уже установлена ранее.

С. Модуль отбраковки стандартных структур. Действительно, полученные в ходе работы программы структуры могут оказаться стандартными – и, притом, довольно большими. Поэтому требуется (тоже переборный, и тоже на основе концепции ветвей и границ) алгоритм, позволяющий отбраковать такие структуры.

В заключение заметим, что разработанное программное обеспечение является, по сути, перечисляющей процедурой, работа которой на квадратах фиксированного размера, разумеется, заканчивается, но работа её на квадратах произвольного размера не заканчивается никогда. С сожалением вынуждены признать, что к моменту написания текста данной работы программа ни одной экзотической недополнимой структуры не обнаружила.

Список литературы

1. *Ryser H. J.* A combinatorial theorem with an application to Latin squares // Proc. Amer. Math. Soc. 2 (1951). P. 550–552.
2. *Evans T.* Embedding incomplete Latin squares // Amer. Math. Monthly. 67 (1960). P. 958–961.
3. *Lindner C. C.* On completing Latin rectangles // Canadian Math. Bulletin. 13 (1970). Vol. 2. № 4. P. 581–605.
4. *Galvin F.* The list chromatic index of a bipartite multigraph, J. Combinatorial Theory. Ser. B, 63 (1995). P. 153–158.
5. *Smetaniuk B. A.* A new construction on Latin squares 1: A proof of the Evans conjecture // Ars Combinatoria. 11 (1981). 155–172.

ПУШКАРЁВ Игорь Александрович – кандидат физико-математических наук, доцент, доцент кафедры фундаментальной информатики и прикладной математики, Вятский государственный университет. 610000, г. Киров, ул. Московская, 36.

E-mail: E-mail: god_sha@mail.ru

КЛЮКИН Игорь Андреевич – без степени, без звания, магистрант кафедры фундаментальной информатики и прикладной математики, Вятский государственный университет. 610000, г. Киров, ул. Московская, 36.

E-mail: igor_pol04@mail.ru