УДК 004.08

НЕЛОКАЛЬНЫЕ ПРЕДМЕТНЫЕ ОБЛАСТИ

Попов С.В.

ООО «Научно-внедренческая фирма БП+», Москва, e-mail: s-v-popov@yandex.ru

В связи с интересом к решению переборных задач, с одной стороны, возникает интерес к построению областей, в которых переборные задачи решаются просто (т.е. не более чем за полином от сложности декларативного описания предметной области), а с другой – областей, в которых число различных практически важных объектов много, и поэтому поиск искомого объекта представляется трудоемким. Известно, что так называемые локальные области, определяемые, например, на логическом языке, просты для разрешения. Такие области характеризуются сложными описаниями своих объектов, и для них просто решаются задачи построения искомого объекта в силу ограничения перебора большим числом условий. С другой стороны, существуют так называемые нелокальные области, которые обладают большим числом разнообразных объектов, и для них нахождение искомого объекта связано с большим перебором, который невозможно снизить без потери общности решения. В статье приводится описание класса нелокальных областей, которые характеризуются достаточно коротким декларативным описанием, но перечисление возможных объектов сложное в силу их большого разнообразия. Число упомянутых объектов представляется экспонентой от длины декларативного описания. Для задания нелокальных областей используется булевский язык, который предоставляет все необходимые средства. Если рассматривать такое описание как логическую функцию, то ее нелокальность обозначает большое число подфункций, которые можно получить, означивая аргументы. С другой стороны, представление этих же областей на графовом языке позволяет представить в виде графов, в которых объектами служат пустые подграфы. Каждому пустому подграфу соответствует объект предметной области. В результате удается показать, что все максимальные пустые подграфы имеют равномерное распределение, т.е. обладают одинаковыми сложностями, и их число выражается экспонентой от числа узлов исходного графа.

Ключевые слова: логические функции, логические матрицы, графы ортогональности, пустые подграфы, единичное означивание, предметная область, объекты предметной области

NOT A LOCAL SUBJECT AREA

Popov S.V.

LLC «Nauchno-vnedrencheskaya firma BP+», Moscow, e-mail: s-v-popov@yandex.ru

In connection with the interest in solving enumerated problems, on the one hand, there is an interest in constructing regions in which the enumeration problems are solved simply (that is, no more than a polynomial from the complexity of the declarative description of the subject domain), and on the other hand, in which the number of various practically important objects is large, and therefore the search for the desired object seems to be time consuming. It is known that the so-called. local domains defined, for example, in a logical language, are easy to resolve. Such areas are characterized by complex descriptions of their objects, and for them the problems of constructing the desired object are simply solved due to the restriction of enumeration by a large number of conditions. On the other hand, there are so-called. non-local areas that have a large number of different objects, and for them finding the desired object is associated with a large search that cannot be reduced without loss of generality of the solution. The article provides a description of the class of non-local areas, which are characterized by a rather short declarative description, but the enumeration of possible objects is difficult because of their great diversity. The number of the mentioned objects is represented as an exponent of the length of the declarative description. To specify non-local areas, Boolean language is used, which provides all the necessary tools. If we consider such a description as a logical function, then its nonlocality denotes a large number of subfunctions that can be obtained, meaning arguments. On the other hand, the representation of these regions in the graph language allows us to be represented as graphs in which the objects are empty subgraphs. Each empty subgraph corresponds to an object domain. As a result, it is possible to show that all maximal empty subgraphs have a uniform distribution, i.e. have the same complexity, and their number is expressed by the exponent of the number of nodes of the original graph.

Keywords: logical functions, logical matrices, orthogonality graphs, empty subgraphs, unit value, subject area, domain objects

В связи с интересом к решению переборных задач ([1, 2]), с одной стороны, возникает интерес к построению конкретных предметных областей (ПО), в которых такие задачи решаются просто (не более чем за полином от сложности декларативного описания ПО), а с другой – ПО, в которых число различных объектов много, и их перебор представляется трудоемким. В первом случае просто разрешимые ПО имеют сугубо прикладное значение, так как при их анализе удается экономить вычислительные ресурсы. Второй класс ПО со сложной разрешимостью имеет скорее теоретическое значение, демонстрируя, какие условия определяют их сложность.

Известно, что так называемые локальные ПО, определяемые, например, на логическом языке, просты для разрешения. Такие ПО характеризуются длинными описаниями своих объектов, и для них просто решаются задачи построения искомого объекта в силу ограничения вариантов поиска большим числом условий. Например, такие ПО описываются реляционными базами данных, в которых ответ на запрос (конечно, если он составлен рационально) не требует большого числа ресурсов. С другой стороны, существуют так называемые нелокальные ПО, которые обладают большим числом разнообразных объектов, и для них нахождение искомого объекта связано с большим перебором, который невозможно снизить без потери общности решения. Например, к таким задачам относятся задачи, формулируемые на графах, большое число комбинаторных задач и т.п. Исследование свойств локальности и нелокальности предметных областей приведено в [3], где эти свойства описаны на языке так называемых логических матриц.

Логические матрицы суть представления КНФ логических функции и определяются следующим образом. Пусть $D = \{D_1, D_2, ..., D_m\}$ есть множество дизъюнктов, зависящих от переменных $x_1, x_2, ..., x_n$. Множество D представляется матрицей M_D, столбцы которой занумерованы от 1 до m, а строки – от 1 до n. Ее элемент $a_{ij} = 1$, если переменная x_i входит в дизъюнкт D_j, $a_{ij} = 0$, если в D_j входит литера $\underline{x}_i$, и a_{ij} есть символ подчеркивания «_», если ни переменная x_i ни ее отрицание не входят в D_j. Символы 0 и 1 суть значащие, символ «_» – незначащий.

В работе представлены нелокальные логические матрицы, для которых число подфункций, получаемых различными означиваниями переменных, велико. Сопоставляя матрицам определенные графовые конструкции, удается построить графы, в которых велико число пустых подграфов. Тем самым, если граф полагать декларативным описанием ПО, то ее фактическое описание в виде перечисления пустых подграфов сложное.

Цель статьи состоит в описании так называемых нелокальных ПО, которые позволяют задавать декларативно просто описываемые ПО, обладающие большим числом принадлежащих им объектов.

Логические уравнения, матрицы и графы, определяемые уравнениями

Пусть Σ: $\Sigma_i = \sigma_i$, $i = 1, 2, ..., m$, $m > 1$, $\sigma_i \in \{0, 1\}$, есть система булевских линейных уравнений от n переменных $\{x_1, x_2, ..., x_n\}$, Σ_i представляет собой сумму по модулю два в точности $k_i \le k$ различных положительных переменных из множества $\{x_1, x_2, ..., x_n\}$, и каждая переменная входит в точности в два уравнения.

Верны следующие утверждения:

1. *Система Σ уравнений имеет решение тогда и только тогда, когда выполняется равенство* $\sigma_1 \oplus \sigma_2 \oplus \ldots \oplus \sigma_m = 0$.

2. *В системе Σ уравнений каждая переменная существенная.*

Поставим в соответствие системе Σ уравнений граф G_Σ, содержащий m узлов, каждый его узел N_i помечен меткой σ_i и ему соответствует уравнение $\Sigma_i = \sigma_i$, $i = 1, 2, ..., m$. Узлы N_i и N_j соединены ребром с меткой $x \in \{x_1, x_2, ..., x_n\}$, если x есть общая переменная уравнений $\Sigma_i = \sigma_i$ и $\Sigma_j = \sigma_j$. В графе G_Σ метки всех ребер различные, и они покрывают все множество $\{x_1, x_2, ..., x_n\}$ переменных.

Понятно, что *при различных распределениях меток узлов графа G_Σ решения системы Σ различны*.

Поставим в соответствие системе Σ уравнений логическую матрицу M_Σ приведением каждой суммы Σ_i в уравнении $\Sigma_i = 1$ к КНФ и представлением каждого ее дизъюнкта в виде столбцов. Аналогично к КНФ приводится выражение $\neg\Sigma_i$, если в Σ имеется уравнение $\Sigma_i = 0$, $i = 1, 2, ..., m$. Если в уравнении $\Sigma_i = \sigma$, $\sigma \in \{0, 1\}$ имеются m_i переменных, то в матрице M_i, соответствующей КНФ, содержится m_i строк и 2^{mi-1} столбцов. При $\sigma = 1$ в каждом столбце матрицы M_i четное число нулей, а при $\sigma = 0$ – нечетное. Матрицу M_i превращаем в матрицу, содержащую n строк (n – число различных переменных в уравнениях системы Σ), за счет добавления строк, соответствующих отсутствующим переменным, каждая такая строка имеет лишь незначащие символы «_». Матрица M_Σ получается из всех таких матриц M_i, $i = 1, 2, ..., m$ конкатенацией столбцов. Очевидно, что *две матрицы M_i и M_j*, имеют общую строку, содержащую значимые символы в столбцах, соответствующих обеим матрицам, тогда и только тогда, когда уравнения $\Sigma_i = \sigma_i$ и $\Sigma_j = \sigma_j$ имеют общую переменную, и эта строка соответствует этой переменной.

По матрице M_Σ построим *граф ортогональности* G_{Ort}, в котором число узлов совпадает с числом столбцов матрицы M_Σ, каждому столбцу соответствует в точности один узел (потому считаем, что имена узлов совпадают с номерами столбцов) и каждому узлу приписан вектор, полученный транспонированием столбца. Два узла графа G_{Ort} смежные тогда и только тогда, когда соответствующие столбцы матрицы, определяемые различными уравнениями, ортогональные. Тем самым при построении графа ортогональности не учитывается ортогональность узлов, определяемых любой, но одной матрицей M_i. Поэтому всякая матрица M_i в графе G_{Ort} определяет *пустой подграф* G_i, узлы которого помечены ее столбцами.

Тогда каждая пара матриц M_i и M_j таких, что соответствующие уравнения $\Sigma_i = \sigma_i$

и $\Sigma_j = \sigma_j$ имеют общую переменную x, в графе G_{Ort} определяет двудольный подграф (G_i, G_j) с долями G_i и G_j, который обладает следующим свойством: половина узлов подграфа G_i, смежных с узлами подграфа G_j, характеризуются нулевым значением переменной x, а половина – наоборот, единичным значением. Аналогично для подграфа G_j – половина узлов с нулевыми компонентами, соответствующими переменной x, а половина – с единичными. В результате в подграфе (G_i, G_j) выделяются два пустых подграфа, один из них характеризуется нулевым значением компонентов, соответствующих переменной x, а другой – единичным.

Отметим, что если в векторах, приписанных подграфам G_i и G_j, вычеркнуть компонент, соответствующий переменной x, то метки узлов каждого из этих подграфов образуют полное покрытие соответствующих единичных кубов. Размерности этих кубов на единицу меньше числа переменных в уравнениях, соответственно $\Sigma_i = \sigma_i$ и $\Sigma_j = \sigma_j$.

Двойственными к выделенным пустым подграфам служат два *полных двудольных подграфа*, которые определяются следующим образом: в графе G_i все узлы первого двудольного графа характеризуются единичным компонентом приписанных векторов и нулевым в графе G_j. Для второго – наоборот, в графе G_i все его узлы характеризуются нулевым компонентом приписанных векторов и единичным в графе G_j.

Опишем преобразование матрицы M_Σ и графов, когда переменная x, принадлежащая в точности двум уравнениям системы Σ, принимает значения $\sigma_x = 0$, 1. Пусть эта переменная входит в уравнения $x \oplus \Sigma'_i = \sigma_i$, $x \oplus \Sigma'_j = \sigma_j$, и x есть метка ребра N_iN_j. Если $\sigma_x = 0$, то уравнения превращаются в $\Sigma'_i = \sigma_i$ и $\Sigma'_j = \sigma_j$, в графе G_Σ ребро с меткой x стирается, и метки узлов N_i и N_j не меняются. Если $\sigma_x = 1$, то уравнения превращаются в $\Sigma'_i = 1 - \sigma_i$, $\Sigma'_j = 1 - \sigma_j$, в графе G_Σ ребро x стирается, и метки узлов N_i и N_j инвертируются. Соответствующие преобразования матрицы M_Σ следующие. Если $\sigma_x = 0$, то вычеркиваются все столбцы, имеющие на пересечении со строкой x нулевое значение, и затем сама строка x. Аналогично, при $\sigma_x = 1$, вычеркиваются все столбцы, имеющие на пересечении со строкой x единичное значение, затем вычеркивается строка x. Такие преобразования следуют из того, что матрица M_Σ представляет логическую функцию в КНФ.

Рассмотрим, как подобное преобразование отражается на графе ортогональности G_{Ort}. Если $\sigma_x = 0$, то в двудольном подграфе (G_i, G_j) выделяется пустой подграф $G_{x=0}$, который характеризуется нулевым значением компонентов, соответствующих переменной x. Если $\sigma_x = 1$, то пустой подграф $G_{x=1}$ характеризуется единичным значением компонентов, соответствующих переменной x. Теперь, если выбросить все ребра, определяемые переменной x, то получим два графа ортогональности $G_{Ort(x=0)}$ и $G_{Ort(x=1)}$, которые связаны с системами уравнений $\Sigma_{x=0}$, $\Sigma_{x=1}$, графами $G_{x=0}$ и $G_{x=1}$, матрицами $M_{x=0}$ и $M_{x=1}$ подобно исходным.

Производя сравнение матриц и графов, полученных в результате описанных преобразований, убеждаемся в верности утверждения: *означивания* $\sigma_x = 0$, 1 *переменной* x *приводят к таким изменениям в системе* Σ *уравнений, графе* G_Σ, *матрице* M_Σ и *графе ортогональности* G_{Ort}, *что результирующие системы уравнений, графы, логические матрицы и графы ортогональности связаны подобно исходным.* Обозначим их соответственно Σ_{σ_x}, G_{σ_x}, M_{σ_x} и $G_{Ort\sigma_x}$.

Аналогичными обозначениями будем пользоваться, когда рассматривается означивание σ_x совокупности x переменных. Пусть x есть совокупность переменных уравнений системы Σ, $|x| = h$, выделяющая подграф G_x, ребра которого помечены переменными из x. Узлы подграфа G_x образуют множество N_x, а ребра – множество D_x, $|D_x| = h$, каждое ребро из D_x помечено переменной из x, каждый узел из N_x инцидентен по меньшей мере одному ребру из D_x. Назовем узел $N \in N_x$ внутренним, если ему инцидентны ребра только из множества D_x, в противном случае назовем узел N – граничным. Таким образом, каждый граничный узел смежный с некоторыми узлами вне N_x.

Полагаем, что число граничных узлов подграфа G_x равно k, N_1, N_2, ..., N_k суть все граничные узлы графа G_x, и $Y_1 \subseteq x$, $Y_2 \subseteq x$, ..., $Y_k \subseteq x$ суть подмножества переменных, которыми помечены ребра, инцидентные соответственно узлам N_1, N_2, ..., N_k. Так как метки ребер графа G_Σ различные, то для несмежных граничных узлов эти множества различны. Пусть σ есть означивание переменных x. Сформируем по σ бинарный вектор $s = (s_1, s_2, ..., s_k)$, где s_i есть сумма по модулю двух компонентов из σ, определяемых множеством Y_i, $i = 1, 2, ..., k$. Назовем этот вектор ассоциированным с означиванием σ.

Совокупность x переменных выделяет в графе ортогональности G_{Ort} подграф G_{Ortx}, ребра которого определяют отношение ортогональности, задаваемое переменными x. При означивании переменных x узлы именно графа G_{Ortx} образуют интересующие нас пустые подграфы. В общем случае каждое означивание σ_x определяет пустой подграф $G_{Emp\sigma x}$, полученный вычеркиванием узлов и ребер подграфа G_{Ortx}, как описано выше для одной переменной. В случае, когда рассматривается совокупность x переменных, преобразования осуществляются для каждой из них. В результате каждое такое означивание σ_x порождает и новый граф ортогональности. Однако различные означивания могут приводить к одинаковым как пустым подграфам, так и результирующим графам ортогональности. Поэтому оценим их число по логической матрице M_Σ.

Верно следующее свойство ассоциированных векторов.

Лемма 1. Два означивания σ_1 и σ_2 переменных x определяют различные логические функции, соответствующие логические матрицы, графы и графы ортогональности, тогда и только тогда, когда σ_1 и σ_2 обладают различными ассоциированными векторами.

Доказательство. 1. Из определения ассоциированного вектора $(s_1, s_2, ..., s_k)$ следует, что если $s_i = 1$, то соответствующее означивание σ переменных x приводит к инвертированию метки граничного узла N_i. Если же $s_i = 0$, то инвертирования нет. Отметим, что различные инвертирования приводят к различным логическим функциям. Таким образом, различные ассоциированные векторы соответствуют различным логическим функциям. Несовпадение логических матриц, графов и графов ортогональности вытекает из несовпадения логических функций.

2. Пусть означивания σ_1 и σ_2 переменных x определяют различные логические функции, но обладают одинаковыми ассоциированными векторами. Из определения ассоциативного вектора следует, что эти два означивания приводят к одному подграфу, в котором вычеркнуты все ребра с метками из множества x и все узлы, которым не инцидентно ни одно ребро. Следовательно, эти означивания определяют одну логическую функцию. Противоречие.

Лемма доказана.

Говорим, что означивания σ_1 и σ_2 переменных x *эквивалентны*, если они определяют одну логическую функцию.

Из способа формирования графов G_x и G_{Ortx} получаем такое утверждение.

Следствие. Эквивалентные означивания σ_1 и σ_2 переменных x определяют одинаковые подграфы G_x и G_{Ortx}.

Получаем, что признаком эквивалентности наборов, означивающих переменные x, является вид ассоциированного вектора. Поэтому представляет интерес количество различных классов эквивалентности в зависимости от числа компонентов ассоциированного вектора. Оценка снизу число различных классов эквивалентности означиваний переменных x приведена в [3]: все означивания переменных x разбиваются не менее чем на $2^{\left[\frac{k}{2}\right]}$ различных классов эквивалентности.

Такое разбиение означиваний переменных x позволяет установить количество различных соответствующих матриц, подграфов и графов ортогональности. Верно такое утверждение: все означивания переменных x определяют не менее $2^{\left[\frac{k}{2}\right]}$ различных логических функций, матриц, подграфов и графов ортогональности.

В данной статье нас интересует число различных пустых подграфов, которые можно выделить в исходном графе ортогональности. Исходим из того, что каждое означивание σ_x переменных x в графе ортогональности G_{Ort} определяет пустой подграф, и неэквивалентные означивания определяют различные пустые подграфы. Из этого вытекает, что в исходном графе ортогональности G_{Ort} имеется не менее $2^{\left[\frac{k}{2}\right]}$ различных пустых подграфов, число узлов в каждом из которых не менее $|G_x|$

Нелокальные области

Пусть степень вершин графа G_Σ ограничена некоторой константой, и для него существуют константы $0 < c_1, c_2 < 1$ такие, что любой подграф, обладающий c_1n ребрами, имеет c_2n граничных узлов. Такие графы называются расширителями [4]. Из указанного свойства расширителя и Следствия 1 вытекает

Теорема 2. Существуют матрицы с n строками, для которых мощность фактор-множеств означиваний части ее переменных не менее 2^{cn}, где c – некоторая положительная константа.

Проблема нахождения пустых подграфов в произвольных графах имеет немалое прикладное значение [5]. В связи с этим интерес представляет такое утверждение.

Следствие. Существует граф ортогональности с n узлами, в котором имеется не менее 2^{cn} пустых подграфов, где c – некоторая положительная константа.

Распределение пустых подграфов графа ортогональности

Каждому объекту построенной ПО можно поставить в соответствие частоту, с которой он определяется посредством означиваний переменных. Это позволяет определить энтропию ПО в зависимости от различных описаний объектов. Известно, что классы эквивалентности означиваний переменных x обладают одинаковыми долями независимо от порядка означивания переменных [3]. Каждому классу эквивалентности означиваний соответствует уникальный пустой подграф, выделяемый переменными x. Из последнего утверждения следует, что каждый такой пустой подграф определяется одинаковым числом означиваний переменных x. Следовательно, все объекты ПО обладают одинаковым распределением, а сама ПО – большой энтропией.

Заключение

В работе описано семейство логических матриц, для которых число классов эквивалентности, получаемых различными означиваниями переменных, ограничено снизу экспонентой от числа строк матрицы. Это позволяет построить графы, число пустых подграфов в которых ограничено снизу экспонентой от числа узлов. В результате описывается предметная область, для которой декларативное описание в виде графа – простое, но она содержит объекты, число которых не менее экспоненты от числа узлов. Тем самым построена декларативно просто описываемая ПО, в которой все объекты обладают одинаковыми совокупностями признаков, т.е. ПО, обладающая большой энтропией.

Список литературы

1. Асанов М.О., Баранский В.А., Расин В.В. Дискретная математика: графы, матроиды, алгоритмы: учеб. пособие. СПб.: Лань, 2010. 368 с.

2. Гладков Л.А., Курейчик В.В., Курейчик В.М. Дискретная математика. М.: Физматлит, 2014. 496 с.

3. Попов С.В., Брошкова Н.Л. Прикладная логика. М.: Физматлит, 2011. 212 с.

4. Введение в криптографию / Под ред. В.В. Ященко. М.: МЦНМО, 2012. 342 с.

5. Зыков А.А. Основы теории графов. М: Вузовская книга, 2010. 664 с.