

ЗАКЛЮЧЕНИЕ

Для решения актуальной задачи распознавания криптографических генераторов сформулирован общий подход к построению информативных признаков. Этот подход учитывает динамику изменения вероятностных характеристик генераторов при изменении длины используемого фрагмента. Построенные согласно этому подходу признаки универсальны, т.к. не используют специфических свойств генераторов, и поэтому их можно применять для распознавания различных типов генераторов.

В соответствии с предложенным подходом построены и применены для распознавания информативные признаки. Получены явные формулы для вычисления моментов 1-го порядка построенных информативных признаков, а также проведены компьютерные эксперименты, в которых были применены построенные признаки. Проиллюстрировано применение одного из признаков для распознавания прореживающего и самосжимающего генераторов, и другого – для распознавания самосжимающих генераторов с различными параметрами.

Литература

1. Харин Ю. С., Берник В. И., Матвеев Г. В., Агиевич С. В. Математические и компьютерные основы криптологии / Минск: Новое Знание. 2003.
2. Meier W., Staffelbach O. Analysis of pseudo random sequences generated by cellular automata // Advances in Cryptology: Eurocrypt '91. Brighton. 1991. P. 186–199.
3. Харин Ю. С., Жук Е. Е. Математическая и прикладная статистика / Минск: БГУ. 2004.
4. Палуха В. Ю. Информативные признаки для распознавания криптографических генераторов // Сб. работ 69-й науч. конф. студентов и аспирантов Бел. гос. ун-та. Минск. 2012. С. 209–213.
5. Coppersmith D., Krawchuk Y., Mansour Y. The shrinking generator // Advances in Cryptology: Proc. of Crypto 93. Santa Barbara. 1993. P. 22–39.

НЕОРИЕНТИРОВАННЫЕ ГРАФЫ И КОНЪЮНКТИВНЫЕ НОРМАЛЬНЫЕ ФОРМЫ, ИХ ЗАДАЮЩИЕ

И. А. Парака

ВВЕДЕНИЕ

В дискретной математике весьма важен алгоритм построения по конъюнктивной нормальной форме (КНФ) неориентированного графа (с обозначением его вершин 2-наборами). Его важность в том, что этот алгоритм доказывает полиномиальную сводимость проблемы ВЫП к проблеме m-клик. Естественно возникает вопрос о том, каждый ли неориентированный граф (неорграф), если его вершины обозначить аналогич-

но, может быть построен по соответствующей КНФ. В данной статье показывается, что этот подход осуществить в общем случае невозможно, то есть описывается серия неориентированных графов, которые не могут быть заданы ни одной КНФ.

1. ПОСТРОЕНИЕ НЕОРГРАФА ПО КНФ

Обозначим через x^a формулу логики высказываний $x \cdot a \vee \bar{x} \cdot \bar{a}$. Тогда формула логики высказываний

$$x_1^{a_1} \vee x_2^{a_2} \vee \dots \vee x_n^{a_n}, \quad (1)$$

где $x_i \neq x_j$ при $i \neq j$ и каждое $a_i \in \{0,1\}$ ($1 \leq i \leq n$), называется элементарной дизъюнкцией (ЭД). ЭД (1) имеет значение 0 тогда и только тогда, когда для всех i ($1 \leq i \leq n$) $x_i \neq a_i$. КНФ называется формула логики высказываний, которая является конъюнкцией нескольких ЭД.

Возьмем некоторую КНФ F и пусть m есть число ее ЭД. Построим по F неорграф $G = G(F)$ следующим образом. Каждому вхождению литерала x_j^a в F поставим в соответствие вершину графа, которую обозначим через (x_j^a, i) , где i – номер ЭД, которая содержит x_j^a , $1 \leq i \leq m$. В этом графе вершины (x_j^a, i) и (x_s^b, r) будут соседними тогда и только тогда, когда $i \neq r$ и литерал x_j^a не является отрицанием x_s^b [1]. Таким образом, если КНФ F из m ЭД выполнима, тогда граф $G(F)$ содержит полный подграф с m вершинами; если же КНФ не выполнима, то такого подграфа нет.

2. РЕЗУЛЬТАТЫ

Нетрудно убедиться, что пустые, полные, полные r -дольные неорграфы с n вершинами задаются КНФ вида (2), (3), (4) соответственно.

$$F_{0_n} = x_1^{a_1} \vee x_2^{a_2} \vee \dots \vee x_n^{a_n}. \quad (2)$$

$$F_{K_n} = x_1^{a_1} \cdot x_2^{a_2} \cdot \dots \cdot x_n^{a_n}. \quad (3)$$

$$F = \left(\bigvee_{i_1=1}^{n_1} x_{i_1} \right) \cdot \left(\bigvee_{i_2=n_1+1}^{n_1+n_2} x_{i_2} \right) \cdot \dots \cdot \left(\bigvee_{i_r=n_1+n_2+\dots+n_{r-1}+1}^{n_1+n_2+\dots+n_r} x_{i_r} \right), \quad (4)$$

где n_j – число вершин в j -й доле полного r -дольного графа, $1 \leq j \leq n$.

Докажем, что простая цепь с шестью вершинами (рис. 1 а) и дерево специального вида (рис. 1 б), не задаются ни одной КНФ.

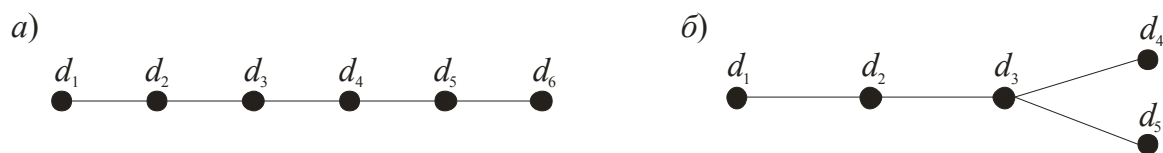


Рис. 1. Графы, не задающиеся КНФ:
а – простая цепь с шестью вершинами; б – дерево специального вида

Графы, представленные на рис. 1 являются деревьями, а следовательно, и двудольными графами. Это значит, что если для них существуют соответствующие КНФ, то они состоят из двух ЭД. Простая цепь, представленная на рис. 1 а, однозначно разбивается на две доли. К одной доле графа относятся вершины d_1, d_3, d_5 , а к другой – d_2, d_4, d_6 . Без ограничения общности, пусть вершине d_1 соответствует литерал x_1 , вершине d_3 – x_2 , вершине d_5 – x_3 . Теперь попытаемся расставить соответствующие литералы в качестве первых компонент для вершин из второй доли таким образом, чтобы полученная по построению КНФ задавала простую цепь с шестью вершинами. Поскольку вершина d_2 соседствует с вершинами d_1 и d_3 и не соседствует с d_5 , то вершине d_2 необходимо поставить в соответствие литерал $\bar{x}_3$. Поскольку вершина d_4 соседствует с вершинами d_3 и d_5 и не соседствует с d_1 , то вершине d_4 необходимо поставить в соответствие литерал $\bar{x}_1$. Вершина d_6 соседствует только с d_5 и не соседствует с вершинами d_1 и d_3 . Тогда вершине d_6 в качестве первой компоненты должны одновременно соответствовать литералы $\bar{x}_2$ и $\bar{x}_1$, но это невозможно. Значит, простая цепь с шестью вершинами не задается ни одной КНФ. Доказательство того, что дерево, представленное на рис. 1 б, не задается ни одной КНФ, проводится аналогично.

Лемма 1. Если неорграф H задается КНФ K и содержит висячее ребро, то после удаления такого ребра получаем граф H' , также задающийся соответствующей КНФ.

Доказательство. Пусть выполняются условия этой леммы. Вместе с удалением висячего ребра удаляется только висячая вершина, а вершина, соседняя с ней, принадлежит графу H' . Поэтому удаление такого ребра не нарушает соседства других вершин из графа H . Следовательно, если висячей вершине сопоставлена пара (x_j^a, i) , то удалением из КНФ K литерала x_j^a из i -й элементарной дизъюнкции (который в ней только раз встречается) получим КНФ K' , задающую неорграф H' . Лемма доказана.

Замечание 1. Если неорграф задается КНФ, то таких КНФ бесконечно много, поскольку литералы из соответствующих вершинам неорграфа пар можно выбирать произвольно, лишь бы выполнялось следующее условие: в неорграфе вершины (x_j^a, i) и (x_s^b, r) являются соседними тогда и только тогда, когда $i \neq r$ и литерал x_j^a не является отрицанием x_s^b .

Лемма 2. Для каждого неорграфа H найдется неорграф G , который задается некоторой конъюнктивной нормальной формой и содержит H в качестве подграфа.

Доказательство. Действительно, любой неорграф H с n вершинами является подграфом полного неорграфа с этим же числом вершин, а такие графы задаются КНФ (см. (3)). Лемма доказана.

Лемма 3. Пусть граф $H = (V, R)$ не задается ни одной КНФ. Тогда как бы ни определять произвольную КНФ путем сопоставления вершинам графа H пар вида (x_j^a, i) (при соблюдении указанных выше условий на соседство вершин), полученная КНФ K будет задавать граф $G = (V, R_1)$, где $R \subset R_1$.

Доказательство. Пусть выполняется условие этой леммы. Поскольку только вершинам графа H сопоставляются указанные пары, то новых вершин не получится. По сопоставленным парам выписываем полученную КНФ K , образуя ее j -ю элементарную дизъюнкцию из всех литералов, равных первым компонентам пар, вторая компонента которых есть j . По КНФ K строим граф G , множество вершин которого согласно сказанному выше будет совпадать с V . Но так как граф H не задается ни одной КНФ, то единственная возможность следующая: в графе G по крайней мере некоторые две вершины, не соседние в H , будут соседними, т.е. $G = (V, R_1)$, где $R \subset R_1$. Лемма доказана.

Введем следующее определение. Граф H является чистым подграфом графа G , если H является подграфом графа G и никакие две вершины из H не образуют в G новых ребер (по сравнению с имеющимися в H).

Свойство 1°. Пусть граф $G = (V, R)$ является собственным подграфом графа $F = (W, E)$, причем любое ребро из $E \setminus R$ инцидентно хотя бы одной вершине из $W \setminus V$. Тогда G является чистым подграфом графа F .

Теорема 1. Если неорграф H не задается ни одной КНФ, то неорграф G , для которого неорграф H является чистым подграфом, также не задается ни одной КНФ.

Доказательство. Пусть выполняются условия этой теоремы. Если бы граф G задавался некоторой КНФ, то согласно определению задания G данной КНФ всем вершинам графа G были приписаны соответствующие

пары (x_j^a, i) , обеспечивающие все соседства вершин графа G и никакие другие соседства вершин G , которые соседними в G не являются. Следовательно, будут соблюдаться и соседства вершин подграфа H , что по условию невозможно. Следовательно, граф G не может быть задан никакой КНФ. Теорема доказана.

Из теоремы 1 следует, что все неорграфы, содержащие простую цепь с шестью вершинами либо дерево специального вида (рис. 1) в качестве чистого подграфа, не задаются ни одной КНФ.

Как было показано выше, полный двудольный граф задается КНФ. Деревья также являются двудольными графами, но не все деревья задаются КНФ (например, простая цепь с шестью вершинами и дерево специального вида, изображенные на рис. 1 а, б). Рассмотрим произвольное дерево на n вершинах. Оно либо изоморфно простой цепи на n вершинах, либо изоморфно звезде на n вершинах, либо содержит в качестве чистого подграфа дерево специального вида (рис. 1 б). Простая цепь с шестью и более вершинами не задается КНФ согласно теореме 1, поскольку она содержит в качестве чистого подграфа цепь с шестью вершинами, которая не задается КНФ. Дерево, содержащее в качестве чистого подграфа дерево специального вида (рис. 1 б), также не задается ни одной КНФ на основании теоремы 1. Звезда с n вершинами задается КНФ, поскольку является полным двудольным графом. Итак, получаем, что из всех деревьев с шестью и более вершинами КНФ задается лишь звезда $K_{1,n}$. А это означает, что почти все деревья не задаются КНФ.

Работа выполнена под руководством В. А. Мощенского.

Литература

1. Мощенский А. В, Мощенский В. А. Математические основы информатики / 2-е изд., перераб. и доп. Минск: БГУ, 2008.

ОЦЕНКА ОБЪЕМА ПАМЯТИ, ТРЕБУЕМОЙ ДЛЯ ВЫПОЛНЕНИЯ МАКРООПЕРАЦИИ ВЫЧИСЛИТЕЛЬНОГО АЛГОРИТМА

М. А. Полещук

Введение. Современные параллельные вычислительные архитектуры для повышения производительности имеют быструю локальную (разделяемую между ядрами одного процессора) память, управление которой осуществляется программно. В качестве целевого компьютера будем рассматривать графические процессоры с двухуровневой параллельной архитектурой.