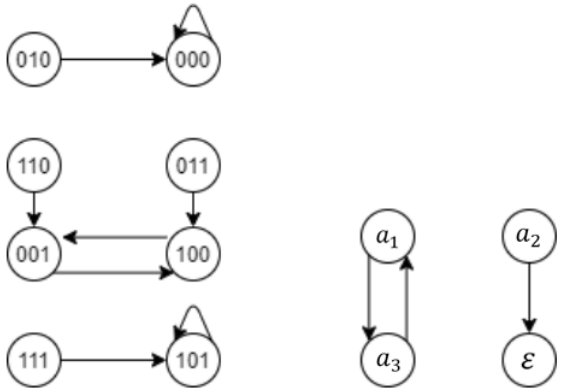


Рис. 1

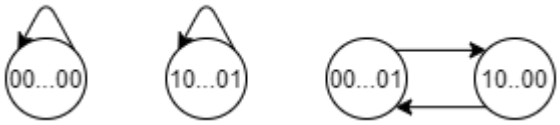


Рис. 2. Аттракторы

ЛИТЕРАТУРА

1. *Жаркова А. В.* Индексы состояний в динамической системе двоичных векторов, ассоциированных с ориентациями пальм // Изв. Сарат. ун-та. Нов. сер. Сер. Математика. Механика. Информатика. 2016. Т. 16. Вып. 4. С. 475–484.
2. *Жаркова А. В.* О количестве аттракторов в конечных динамических системах ориентаций полных графов // Прикладная дискретная математика. Приложение. 2018. № 11. С. 106–109.
3. *Colon-Reyes O., Laubenbacher R., and Pareigis B.* Boolean monomial dynamical systems // Ann. Combinatorics. 2004. V. 8. P. 425–439.

УДК 519.17 DOI 10.17223/2226308X/14/38

СХЕМЫ ПОСТРОЕНИЯ МИНИМАЛЬНЫХ ВЕРШИННЫХ 1-РАСШИРЕНИЙ ПОЛНЫХ ДВУХЦВЕТНЫХ ГРАФОВ[1]

П. В. Разумовский, М. Б. Абросимов

Рассматриваются двухцветные графы, то есть графы, вершины которых раскрашены в два цвета. Пусть $G = (V, \alpha, f)$ — цветной граф с определённой на множестве его вершин функцией раскраски f. Цветной граф G^* называется вершинным 1-расширением цветного графа G, если граф G можно вложить с учётом цветов в каждый граф, получающийся из графа G^* удалением любой его вершины вместе с инцидентными рёбрами. Вершинное 1-расширение G^* графа G называется минимальным, если граф G^* имеет на две вершины больше, чем граф G, а среди всех вершинных 1-расширений графа G с тем же числом вершин граф G^* имеет минимальное число рёбер. Предлагается полное описание минимальных вершинных 1-расширений полных двухцветных графов. Пусть K_{n_1,n_2} — полный n-вершинный граф с n_1 вершинами одного цвета и n_2 вершинами другого цвета. Если в полном

[1]Работа выполнена при поддержке Минобрнауки России в рамках госзадания (проект № FSRR-2020-0006).

двуцветном графе $n_1 = n_2 = 1$, то в минимальном вершинном 1-расширении такого графа будет одно дополнительное ребро. Если в полном двуцветном графе либо $n_1 = 1$, либо $n_2 = 1$, то в минимальном вершинном 1-расширении такого графа будет $2n - 1$ дополнительных рёбер. Во всех остальных случаях в минимальном вершинном 1-расширении полного двухцветного графа будет $2n$ дополнительных рёбер. Предлагаются схемы построения соответствующих минимальных вершинных 1-расширений.

Ключевые слова: *разметка графа, цветной граф, полный граф, расширение графа, минимальное вершинное расширение графа, отказоустойчивость.*

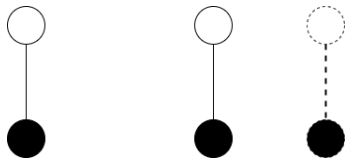
С точки зрения безопасности вычислительных систем большое значение имеет их надёжность, одним из аспектов которой является отказоустойчивость. Существуют разные математические модели отказоустойчивости. В данной работе рассматривается модель, предложенная Джоном Хейзом [1]. Техническая система моделируется графом. Элементам системы соответствуют вершины графа, а связям между элементами — рёбра (или дуги, если связи не являются симметричными). Если элементы имеют разный тип, то соответствующим им вершинам графа приписываются метки типа или цвета. Таким образом, моделью технической системы является граф с вершинами разного цвета, или цветной граф. Основные определения теории графов используются в соответствии с [2]. Будем рассматривать неориентированные графы. Понятия минимальных расширений для графов даются в соответствии с [1, 3].

Определение 1. Граф $G^* = (V^*, \alpha^*, f^*)$ называется минимальным вершинным k-расширением n-вершинного i-цветного графа $G = (V, \alpha, f)$, если выполняются следующие условия:

1) граф G^* является вершинным k-расширением цветного графа G, то есть граф G можно вложить с учётом цветов в каждый граф, получающийся из графа G^* удалением любой его вершины вместе с инцидентными рёбрами;
2) граф G^* содержит $n + ik$ вершин, то есть $|V^*| = |V| + ik$;
3) α^* имеет минимальную мощность среди всех графов, удовлетворяющих условиям 1 и 2.

В работе [1] рассматривается задача построения минимального вершинного 1-расширения для цветного дерева особого вида. В [4] решается задача о генерации цветных графов без проверки на изоморфизм. В данной работе мы рассмотрим полные графы K_{n_1,n_2} с вершинами двух цветов, то есть $i = 2$. Для удобства будем считать, что $n_1 \leqslant n_2$. Как следует из определения, минимальное вершинное 1-расширение графа K_{n_1,n_2} содержит две дополнительные вершины. Далее представлено полное решение задачи построения всех минимальных вершинных 1-расширений для графов K_{n_1,n_2}. Заметим, что в работе [5] введена модель для изучения отказов связей, которой соответствует минимальное рёберное k-расширение. Если рассматриваются графы без кратных рёбер, то полные графы не имеют минимальных рёберных k-расширений ни при каких натуральных значениях k. Аналогичная ситуация имеет место и для цветных полных графов. Напомним, что объединением двух графов $G_1 = (V_1, \alpha_1)$ и $G_2 = (V_2, \alpha_2)$ называется граф $G_1 \cup G_2 = (V_1 \cup V_2, \alpha_1 \cup \alpha_2)$. Если $V_1 \cap V_2 = \varnothing$, то естественным образом операция переносится и на случай цветных графов.

Теорема 1. Полный двухцветный граф $K_{1,1}$ имеет единственное с точностью до изоморфизма минимальное вершинное 1-расширение — граф $K_{1,1} \cup K_{1,1}$ (рис. 1).

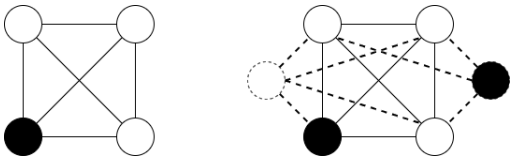


а *б*

Рис. 1. Полный двухцветный граф $K_{1,1}$ (*а*) и его минимальное вершинное 1-расширение (*б*)

Теорема 2. Полные n-вершинные двухцветные графы вида K_{1,n_2}, где $n_2 > 1$, имеют единственное с точностью до изоморфизма минимальное вершинное 1-расширение, которое содержит $2n_2{+}1$ дополнительных рёбер и строится следующим образом: добавляются вершина v_1 первого цвета и вершина v_2 второго цвета. Вершина v_1 соединяется со всеми вершинами второго цвета, вершина v_2 соединяется также со всеми вершинами второго цвета и с одной из вершин первого цвета.

На рис. 2 приведены полный двухцветный граф $K_{1,3}$ и его минимальное вершинное 1-расширение.

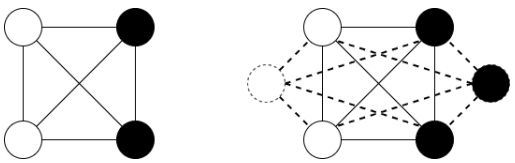


а *б*

Рис. 2. Граф $K_{1,3}$ (*а*) и его минимальное вершинное 1-расширение (*б*)

Теорема 3. Полные n-вершинные двухцветные графы вида K_{n_1,n_2}, $1 < n_1 \leqslant n_2$, имеют единственное с точностью до изоморфизма минимальное вершинное 1-расширение, которое содержит $2n$ дополнительных ребра и строится следующим образом: добавляются вершина v_1 первого цвета и вершина v_2 второго цвета. Вершины v_1 и v_2 соединяются рёбрами со всеми вершинами исходного графа.

На рис. 3 приведены полный двухцветный граф $K_{2,2}$ и его минимальное вершинное 1-расширение.



а *б*

Рис. 3. Граф $K_{2,2}$ (*а*) и его минимальное вершинное 1-расширение (*б*)

Таким образом, схемы построения минимальных вершинных 1-расширений найдены для всех возможных полных двухцветных графов.

ЛИТЕРАТУРА

1. *Hayes J. P.* A graph model for fault-tolerant computing system // IEEE Trans. Comput. 1976. V. C.-25. No. 9. P. 875–884.
2. *Богомолов А. М., Салий В. Н.* Алгебраические основы теории дискретных систем. М.: Наука, 1997. 368 с.
3. *Абросимов М. Б.* Графовые модели отказоустойчивости. Саратов: Изд-во Сарат. ун-та, 2012. 192 с.
4. *Разумовский П. В., Абросимов М. Б.* Построение цветных графов без проверки на изоморфизм // Изв. Сарат. ун-та. Нов. сер. Сер. Математика. Механика. Информатика. 2021. Т. 21. Вып. 2. С. 267–277.
5. *Harary F. and Hayes J. P.* Edge fault tolerance in graphs // Networks. 1993. V. 23. P. 135–142.

UDC 004.453.2 DOI 10.17223/2226308X/14/39

TOWARDS THE SECURITY OF McEliece's CRYPTOSYSTEM BASED ON HERMITIAN SUBFIELD SUBCODES[1]

G. P. Nagy, S. El Khalfaoui

The purpose of this paper is to provide a comprehensive security analysis for the parameter selection process, which involves the computational cost of the information set decoding algorithm using the parameters of subfield subcodes of 1-point Hermitian codes.

Keywords: *code-based cryptography, McEliece Cryptosystem, Hermitian subfield subcodes, Schur square dimension.*

1. Introduction

Recently, there has been a big amount of research addressed to quantum computers that use quantum mechanical techniques to solve hard computational problems in mathematics [1]. The existence of these powerful machines threaten many of the public-key cryptosystem that are widely in use [2]. McEliece [3] introduced the first code-based public-key cryptosystem in 1978. The crucial issues in cryptography today is to reduce the key size and improve the security level of the McEliece cryptosystem, which is a promising cryptographic scheme for the post-quantum era [4]. Error correcting codes, used in code-based cryptographic protocols, must have efficient decoding algorithms. A rich class of such codes is the family algebraic-geometric (AG) codes, their subcodes and subfield subcodes. This includes the generalized Reed — Solomon codes, the alternant codes, the binary Goppa codes and BCH codes. See [5] for a survey on the decoding of AG codes.

The authors of [6 – 8] provided polynomial-time attacks against the McEliece cryptosystem that relies either on AG codes or on their subcodes. In general, evaluation codes do not behave like random codes which demonstrate the quite range of attacks proposed against the McEliece cryptosystem based on AG codes. The approach given in [6, 8] is inspired by the so-called *filtration attacks* that rely on computing the Schur product that make AG codes distinguishable form random ones. Wieschebrink [9] used this observation to provide an attack against McEliece scheme based on subcodes of GRS codes [10]. Many attacks have been founded on this argument, and have employed a

[1]Project no. 2018-1.2.1-NKP-2018-00004 has been implemented with the support provided from the National Research, Development and Innovation Fund of Hungary, financed under the 2018-1.2.1-NKP funding scheme.