чового суматора, блока підстановки та лінійного (над деяким кільцем) оператора. Науково-технічний збірник «*Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*». 2015. № 1 (29). С. 33–45.
2. Ковальчук Л. В., Кучинська Н. В. Построение верхних оценок средних вероятностей целочисленных дифференциалов раундовых функций блочных шифров определенной структуры. *Кибернетика и системный анализ.* 2012. № 5. С. 71–81.
3. Кучинская Н. В., Скрипник Л. В. Построение верхних оценок средних вероятностей целочисленных дифференциалов композиции ключевого сумматора, блока подстановки и произвольного оператора циклического сдвига *Спеціальні телекомунікаційні системи та захист інформації*. 2013. Вип. 2(24). С. 26–32.

Practical estimates are obtained for cryptographic security of GOST-like and Kalyna-like block cipher statistical comparative analysis is conducted of the relevant parameters values for random nodes replacement.

Key words: *difference, differential cryptanalysis, block ciphers, s-blocks.*

Одержано 28.02.2017

УДК 519.8

И. В. Козин, д-р физ.-мат. наук, профессор,
С. Е. Батовский, аспирант,
В. И. Сардак, аспирантка

Запорожский национальный университет, г. Запорожье

ФРАГМЕНТАРНАЯ МОДЕЛЬ И ЭВОЛЮЦИОННЫЙ АЛГОРИТМ 2D УПАКОВКИ ОБЪЕКТОВ

Рассмотрена задача двумерной упаковки в прямоугольник объектов сложной формы. Показано, что задача упаковки имеет фрагментарную структуру. Для поиска приближенного решения задачи предложена модификация эволюционного алгоритма на перестановках с геометрическим оператором кроссовера. Приводятся результаты численного эксперимента.

Ключевые слова: *фрагментарная модель, задача размещения, 2d-упаковка, эволюционный алгоритм, геометрический кроссовер*

Введение. Задача плоского размещения или двумерной упаковки возникает в многочисленных инженерных и экономических приложениях. Решение проблемы упаковки требуется для таких отраслей, как транспорт, обработка дерева, стекла, кожи, при поиске оптимальных размещений механических и электромеханических узлов агрегатов, при загрузке автомобилей, железнодорожных платформ,

танкеров и т. д. Большое количество дополнительных условий в конкретных постановках приводит к необходимости использовать вероятностные методы и эвристические процедуры [1–4].

Постановка задачи. Рассмотрим наиболее распространенную постановку задачи двумерной упаковки, когда требуется разместить заданное конечное множество плоских объектов в контейнере, который представляет собой прямоугольник заданных размеров. Объекты могут иметь достаточно сложную форму, могут быть как выпуклыми, так и невыпуклыми, неодносвязными. Однако будем предполагать, что все объекты являются связными, то есть не распадаются на отдельные части. При размещении в контейнере объекты не должны пересекаться и не могут выходить за границы контейнера. Задача разместить в контейнере по возможности большее по площади подмножество объектов. Целевой функцией в данном случае является плотность упаковки или величина неиспользованной площади в контейнере. Объекты сложной формы заменим их дискретной клеточной аппроксимацией. То есть будем представлять объекты как объединение множества квадратных ячеек достаточно малого размера. Пример такой аппроксимации показан на рис. 1.

Рис. 1. *Плоский объект и его дискретная аппроксимация*

Такой подход применим к объектам произвольной формы. При размещении в контейнере будем заменять объекты их дискретной аппроксимацией с условием, что аппроксимация содержит исходный объект в качестве собственного подмножества.

Фрагментарная структура. Фрагментарной структурой [5] (X, E) на конечном множестве X называется семейство его подмножеств $E = \{E_1, E_2, ..., E_n\}$ такое, что $\forall E_i \in E$, $E \neq \varnothing \quad \exists e \in E_i : E_i \setminus \{e\} \in E$.

Элементы из множества E будем называть допустимыми фрагментами. Таким образом, для любого допустимого фрагмента E_i существует нумерация его элементов $E_i = \{e_{i1}, e_{i2}, ...e_{is_i}\}$ такая, что $\forall k = 1, 2, ...s_i \ \{e_{i1}, e_{i2}, ...e_{ik}\} \in E$. Элементарным фрагментом будем называть допустимый фрагмент, состоящий из одного элемента. Максимальный фрагмент — допустимый фрагмент, который не является подмножеством никакого другого фрагмента.

Максимальный фрагмент может быть построен с помощью следующего «жадного» алгоритма:

а) элементы множества X линейно упорядочиваются;

б) на начальном шаге выбирается пустое множество $X_0 = \varnothing$;

в) на шаге с номером $k + 1$ выбирается первый по порядку элемент $x \in X \setminus X_k$, такой, что $X_k \cup \{x\} \in E$;

г) алгоритм заканчивает работу, если на очередном шаге не удалось найти элемент $x \in X \setminus X_k$ с требуемым свойством.

Результат работы алгоритма определяется заданным линейным порядком на множестве *X*. Таким образом, любой максимальный фрагмент может быть описан некоторой перестановкой элементов множества *X*. Пусть $A \in E$. Условие для элемента $x \in X$, при котором $A \cup \{x\} \in E$, будем называть условием присоединения элемента *x*.

Пусть теперь каждому фрагменту приписан вес, то есть задана функция $\rho : E \to R^1$. Будем предполагать, что функция ρ монотонна по включению (возрастающая или убывающая). Если $A, B \in E$ и $A \subseteq B$, то $\rho(A) \le (\ge)\rho(B)$. Задача оптимизации на фрагментарной структуре, это задача отыскания допустимого фрагмента максимального (минимального) веса. Очевидно, что для монотонных весов оптимальное решение будет являться максимальным фрагментом.

Фрагментарная модель. Покажем, что задача 2d-упаковки может быть представлена как задача оптимизации на фрагментарной структуре. В качестве множества элементарных фрагментов рассмотрим заданный набор объектов, точнее их дискретных аппроксимаций. Каждый допустимый фрагмент будем строить, соблюдая следующее условие присоединения. Очередной объекта размещается в заданном прямоугольном контейнере без выхода за границы контейнера и без пересечений с уже уложенными объектами. Причем при укладке объекта будем руководствоваться правилом Top-Left (северо-западный угол), а именно: объект размещается как можно выше и как можно левее с соблюдением вышеуказанных условий. Если очередной объект разместить не удается, то переходим к следующему по порядку объекту. Множества объектов, которые будут построены в результате работы такого алгоритма (множество *E*), образуют фрагментарную структуру. Максимальный фрагмент в данном случае определяет некоторое размещение объектов в контейнере, в которое уже нельзя добавить никакой из оставшихся объектов без нарушения условий размещения. Целевая функция задачи $F : E \to R^1$ — это площадь свободного места контейнера, то есть не площадь не занятая размещаемыми объектами. Очевидно, целевая функция является монотонной.

Любой максимальный фрагмент определяется заданным линейным порядком просмотра элементарных фрагментов. Этот порядок определяет результат работы фрагментарного алгоритма, который и построит требуемый максимальный фрагмент.

Каждый линейный порядок определяется некоторой перестановкой $s \in S_n$ укладываемых объектов (n — число объектов). Сопоставим каждой перестановке максимальный фрагмент, который ей порождается. Обозначим это отображение $\varphi : S_n \to E$. Таким образом, имеет место естественная коммутативная диаграмма отображений

$$\begin{array}{ccc} & S_n & \\ & \varphi\downarrow \quad \searrow F\circ\varphi, & \\ & E \to R^1 & \end{array}$$

которая превращает задачу оптимизации на фрагментарной структуре в задачу оптимизации на множестве перестановок. Причем любая перестановка является допустимой. Для больших значений n задача поиска оптимальной перестановки, как правило, является трудной. Предлагается использовать для поиска приближенных решений этой задачи эволюционный алгоритм на перестановках определенного вида [6].

Эволюционный алгоритм. Базовое множество X эволюционной модели — это множество $S_n = \{i_1, i_2 ..., i_n\}$ всех перестановок чисел $1, 2, \ldots, n$. Оператор построения начальной популяции выделяет произвольное подмножество заданной мощности Q из множества X.

Правило вычисления критерия селекции устроено следующим образом: по заданной перестановке фрагментов с помощью фрагментарного алгоритма строится максимальный допустимый фрагмент и вычисляется значение целевой функции задачи для этого фрагмента.

Опишем теперь оператор кроссовера. Пусть $U = (u_1, u_2, ..., u_n)$ и $V = (v_1, v_2, ..., v_n)$ — две произвольные перестановки. Перестановка-потомок строится следующим образом: последовательности U и V просматриваются в порядке следования элементов. На k-м шаге выбирается наименьший из первых элементов последовательностей и добавляется в новую перестановку-потомок. Затем этот элемент удаляется из двух последовательностей-родителей. Например, результатом кроссовера перестановок (4, 1, 6, 3, 7, 8, 2, 5) и (2, 6, 7, 3, 1, 4, 8, 5) будет перестановка (2, 4, 1, 6, 3, 7, 8, 5). В работе [6] показано, что определенный таким образом оператор кроссовера является геометрическим в инверсной метрике на перестановках [7].

Оператор мутации M выполняет случайную транспозицию в перестановке.

Оператор селекции выбирает случайным образом набор пар из текущей популяции для последующего скрещивания.

Оператор эволюции упорядочивает элементы промежуточной популяции в последовательность по убыванию значения критерия селекции. В качестве новой текущей популяции выбираются первые Q элементов последовательности.

Обычное правило остановки — количество поколений достигло предельного значения. Лучшая по значению критерия селекции перестановка из последней построенной популяции определяет приближенное решение задачи.

Результаты работы. Для проверки качества предлагаемой метаэвристики была разработана компьютерная оценка качества эволюционно-фрагментарных алгоритмов (ЭВФ — алгоритмов). Некоторые результаты работы этой программы приводятся далее.

Примеры 1, 2. Рассматривались большие наборы одинаковых объектов Т-образного (пример 1) и Г-образного (пример 2) вида. Результаты работы алгоритма показаны соответственно на рис. 2 и рис. 3.

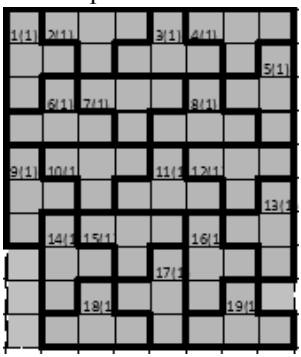

***Рис. 2.** Т-образные объекты*

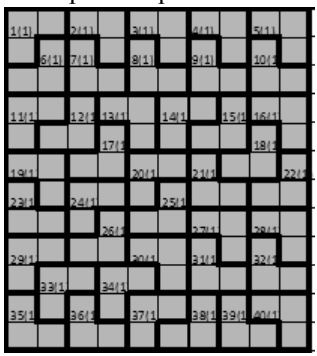

***Рис. 3.** Г-образные объекты*

Пример 3. В качестве примера была взята 2d-упаковка объектов из статьи [8], полученная путем применения генетического алгоритма определенного вида (рис. 4). На рис. 5 показан результат работы ЭВФ-алгоритма для того же набора объектов в том же контейнере.

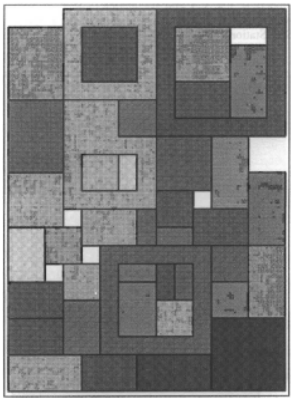

***Рис. 4.** Упаковка из [8]*

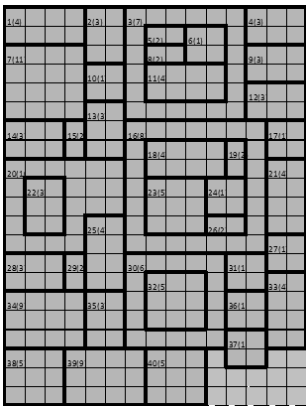

***Рис. 5.** Упаковка ЭВФ алгоритмом*

Выводы. Теоретические результаты и результаты численных экспериментов показывали достаточно высокую эффективность ЭВФ алгоритма при решении различных типов задач плоского размещения и 2d-упаковки. Учитывая простоту реализации и возможность учета дополнительных ограничений, рассматриваемый в статье подход может быть предложен для практического решения задач упаковки в различных областях техники, экономики, производства.

Список использованной литературы:

1. Kierkosz I., Luczak M. A hybrid evolutionary algorithm for the two-dimensional packing problem. *Central European Journal of Operations Research*. [Berlin]: Springer, 2014. Vol. 22. P. 729–753.
2. Кривий Р. З., Лобур М. М., Ткаченко С. П. Застосування генетичного алгоритму прямокутного розміщення для гільйотинного розкрою. Вісник Національного університету «Львівська політехніка». *Комп'ютерні системи проектування. Теорія і практика*. 2010. № 685. С. 138–142. Режим доступу: http://ena.lp.edu.ua:8080/handle/ntb/7414 **.**
3. Мухачева Э. А., Мухачева А. С., Чиглинцев А. В. Генетический алгоритм блочной структуры в задачах двумерной упаковки. *Информационные технологии*. 1999. № 11. С. 12–17.
4. Gonçalves J. F. A hybrid genetic algorithm-heuristic for a two-dimensional orthogonal packing problem. *European Journal of Operational Research*. 2007. Vol. 183 (3) P. 1212–1229.
5. Козин И. В., Полюга С. И. Использование ЭВФ-алгоритмов для решения задачи прямоугольного раскроя. *Питання прикладної математики і математичного моделювання*: зб. наук. праць ; [ред. кол. … О. М. Кисельова (голов. ред.) та ін.]. Д.: Вид-во Дніпропетр. нац. ун-ту ім. Олеся Гончара. Дніпропетровськ, 2009. С. 199–208.
6. Козин И. В. Фрагментарные структуры и эволюционные алгоритмы. *Питання прикладної математики і математичного моделювання* : зб. наук. праць ; [ред. кол.: О. М. Кисельова (головний редактор) та ін.]. 2008. С. 138–146.
7. Moraglio A., Poli R. Inbreeding Properties of Geometric Crossover and Non-geometric Recombinations. *Foundations of Genetic Algorithms*. 2007. P. 1–14
8. Sakait Jain and Hae Chang Gea Two-Dimensional Packing Problems Using Genetic Algorithms. *Engineering with Computers.* 1998 14: P. 206–213.

The problem of two-dimensional packing in rectangle of objects of complex shape. It is shown that the packing problem has fragmentary structure. To find an approximate solution proposed modification of the evolutionary algorithm on permutations with geometric crossover operator. The results of numerical experiment.

Key words: *fragmented model, the layout problem, the 2d-packing problem, evolutionary algorithm, geometric crossover.*

Получено 13.02.2017