УДК 681.31

А.Ю. Полуян

АДАПТИВНЫЙ АЛГОРИТМ ДЛЯ РЕШЕНИЯ ЗАДАЧ ОПТИМИЗАЦИИ НА ОСНОВЕ СТРАТЕГИИ ЭЛИТИЗМА

При решении оптимизационных задач успешно используют стратегии, концепции, методы и механизмы эволюционного моделирования на основе бионического поиска. Бионический поиск – это последовательное преобразование одного конечного нечеткого множества альтернативных решений в другое. Само преобразование называется генетическим алгоритмом (ГА). Цель ГА состоит в том, чтобы [1]:

- обьяснить абстрактно и формально адаптацию процессов в естественной среде и интеллектуальной информационной системе;
- моделировать естественные эволюционные процессы для эффективного решения оптимизационных задач науки и техники.

Задача о минимальном пути как одна из важнейших оптимизационных задач была выбрана объектом исследования, потому, что техника ее решения хорошо известна и изучение нового метода на данной задаче позволит в дальнейшем с его помощью решать другие, более сложные задачи, которые в данный момент решать затруднительно. Отметим, что задача о минимальном пути относится к классу NP полных проблем [2]. Основной трудностью решения данных задач, является предварительная сходимость алгоритмов, т.е. попадание решения в локальный оптимум. Поэтому целесообразно использовать ГА для решения указанной задачи. В последнее время в области исследований, направленных на повышение эффективности генетических алгоритмов, большое значение приобрели идеи создания адаптивных генетических алгоритмов, которые могут изменять свои параметры в процессе работы. Они стали продолжением развития идеи поколенческих алгоритмов, которые в процессе работы изменяют размер популяции. Идея адаптивных генетических алгоритмов получила свое воплощение в концепции *nGA*, представляющей многоуровневые генетические алгоритмы. Нижний уровень такого алгоритма непосредственно выполняет задачу улучшения популяции решений. Верхние уровни представляют собой генетические алгоритмы, решающие оптимизационную задачу по улучшению параметров алгоритма нижнего уровня. При этом в качестве целевой функции используется обычно скорость работы алгоритма нижнего уровня и скорость улучшения им популяции от поколения к поколению.

Основная особенность генетического алгоритма состоит в том, что анализируется не одно решение, а некоторое подмножество квазиоптимальных решений, называемых хромосомами и состоящих из генов. Это подмножество носит название "популяция". В данной реализации начальная популяция формируется случайным образом. Для увеличения скорости сходимости генетического алгоритма в неё включается хромосома, описывающая маршрут по "жадному" алгоритму. Для рассматриваемой задачи хромосома описывает последовательность номеров вершин графа.

Для хромосомы вычисляется целевая функция $F(k)$, где k − маршрут, описываемый хромосомой. Такие функции вычисляют относительный вес каждой хромосомы. В данном случае целевая функция представляет собой длину траектории движения коммивояжера.

В рассматриваемом генетическом алгоритме реализована стратегия элитизма, при которой несколько лучших индивидуумов переходят в следующее поколение без изменений. Количество элитных индивидуумов *KI* определяется по формуле:

$$KI = (1 - SO) * RP,$$

где *SO* – степень обновления популяции, *RP* – размер популяции.

После формирования начальной популяции, осуществляется процесс синтеза новых решений (поколений) задачи посредством кроссинговера и мутации. Исходными данными для него являются хромосомы текущей популяции. Исследуемая в некоторый момент времени популяция называется текущей. В начале работы алгоритма текущая популяция совпадает с начальной.

Данный генетический алгоритм предлагает ликвидировать имеющиеся пересечения в маршрутах, используя оператор инверсии, а также применить к каждой хромосоме операцию разнообразия. Операция разнообразия вносит некоторые изменения в отдельную хромосому.

Адаптивный генетический алгоритм поддерживает такую архитектуру генетического поиска, при которой целенаправленное изменение применяется ко всем вновь созданным хромосомам.

После скрещивания и мутации размер популяции увеличивается. Однако для последующих преобразований необходимо сократить число хромосом текущей популяции. Такая процедура носит название селекции. В текущей популяции, состоящей из родителей и потомков, производится отбор лучших решений, т.е. хромосом с наилучшим значением fitness-функции (целевой функции).

Эта функция показывает, насколько исследуемая хромосома близка к оптимальному решению. Для текущей популяции повторяются все описанные процедуры. Процесс продолжается до тех пор, пока не будет обработано заданное число поколений. При этом каждая последующая популяция должна быть лучше, чем предыдущая. Решению задачи соответствует хромосома с наилучшим значением fitness-функции. Таким образом, для адаптивного генетического алгоритма выделяется четыре основных этапа:

1) формирование начальной популяции;

2) синтез новых хромосом (операторы скрещивания и мутации);

3) целенаправленное изменение вновь полученных хромосом (операторы инверсии и разнообразия);

4) селекция текущей популяции.

Количество поколений, которое требуется для нахождения минимального маршрута, зависит также от начальной генетической информации в первом поколении. Поэтому оно меняется от попытки к попытке. Для получения наилучшего результата работы генетического алгоритма рекомендуется сделать несколько попыток (3-5).

Общую схему генетического алгоритма можно представить следующим образом:

Шаг 1. Построение матрицы смежности.

Шаг 2. Применение "жадного" алгоритма для построения маршрута.

Шаг 3. Ввод параметров расчёта.

Шаг 4. Порядковый номер попытки $i=1$ ($i = \overline{1, KP}$). (КР – количество попыток)

Шаг 5. Формирование начальной популяции *i*-ой попытки.

Шаг 6. Целенаправленное изменение хромосом начальной популяции.

Шаг 7. Порядковый номер генерации *i*-ой попытки $j=1$ ($j = \overline{1, TG}$).

Шаг 8. Выделение элиты и формирование текущей *j*-ой популяции.

Шаг 9. Скрещивание хромосом в *j*-ой популяции.

Шаг 10. Мутация хромосом в *j*-ой популяции.

Шаг 11. Целенаправленное изменение новых хромосом.

Шаг 12. Добавление новых хромосом к *j*-ой популяции.

Шаг 13. Селекция в *j*-ой популяции.

Шаг 14. Добавление элиты к *j*-ой популяции.

Шаг 15. Переход к следующей популяции: $j=j+1$.

Шаг 16. Если $j \le TG$, то переход к шагу 8, иначе - определение наилучшего маршрута *i*-ой попытки. (*TG* – число генераций)

Шаг 17. Переход к следующей попытке: $i=i+1$.

Шаг 18. Если $i \le KP$, то переход к шагу 5, иначе определение наилучшего маршрута за время работы алгоритма.

Шаг 19. Вывод результирующего маршрута.

В каждой популяции хромосомы могут подвергаться действиям различных операторов. При этом происходят процессы, аналогичные действиям, которые случаются в естественной генетике. К основным операторам относят: оператор скрещивания, оператор мутации, оператор инверсии, оператор разнообразия и оператор селекции.

В данном алгоритме реализованы модифицированные операторы кроссинговера и мутации. Оператор кроссинговера является модифицированным, так как в нём предусмотрен механизм, исключающий возникновение "нелегальных" решений. Такими решениями считаются хромосомы, не отвечающие условию задачи.

Общую схему реализованного оператора скрещивания можно представить следующим образом:

Шаг 1. Выбрать хромосому с лучшим значением целевой функции *F(k)* в текущей популяции, как первого родителя.

Шаг 2. Порядковый номер итерации $i=1$.

Шаг 3. Сгенерировать случайное число *rnd*, причём $0 \le rnd < 1$.

Шаг 4. Если $rnd < PS$, то выбрать *i*-ую хромосому в текущей популяции в качестве второго родителя, применить операцию скрещивания к выбранным хромосомам и запомнить получившихся потомков.

Шаг 5. Переход к следующей итерации: $i=i+1$.

Шаг 6. Если $i < RP$ (размер популяции), то перейти к шагу 3.

Шаг 7. Конец работы алгоритма.

Оператор мутации (ОМ) реализуется на основе простых чисел, вычислительная сложность алгоритма такого оператора линейна в одной итерации. Упрощенным видом ОМ является использование нечетных и четных чисел в качестве места точек разрыва, а также различные комбинации последовательности выбора четных и нечетных позиций генов в качестве точек разрыва.

Оператор селекции формирует новое поколение из хромосом с лучшими значениями целевой функции *F(k)*. Он уничтожает большую часть популяции и освежает генетический материал, пополняя популяцию большим количеством новых членов. В результате выполнения оператора селекции размер популяции нового поколения вновь становится равным *RP*.

Оператор инверсии изменяет характер связей между компонентами хромосомы. Он берёт хромосому, случайным образом выбирает в ней две точки разрыва и располагает в обратном порядке элементы, попавшие между точками разрыва [3].

Оператор разнообразия также вносит изменения в отдельного индивидуума, но это очень небольшие изменения в каждой хромосоме, а не сильное изменение

хромосомы, как происходит при мутации. Они относятся к начальной популяции. С целью улучшения значения целевой функции каждая хромосома обрабатывается итерационным алгоритмом оператора разнообразия, основанным на методе циклического координатного спуска. Идея метода заключается в том, что его итерация (цикл) состоит из последовательности шагов. В ходе шага работы итерационного алгоритма смежные хромосомы попарно рассматриваются и заменяются хромосомами минимально возможной длины. Поэтому в процессе реализации каждого шага значения целевой функции $F(k)$ улучшаются. Если изменения целевой функции $F(k)$ для двух последних итераций не превысили заданную точность ε, то итерационный алгоритм оператора разнообразия прекращает свою работу.

Критерий остановки алгоритма может быть разным. Можно задать фиксированное число генераций. Можно на каждой итерации полученное решение сравнивать с оптимальным, пока не будет достигнута желаемая точность.

Для повышения скорости работы алгоритма предлагается параллельная обработка информации. Существует гипотеза, что в параллельной системе с n процессорами, производительность каждого из которых равна единице, общая производительность растет как $log_2 n$ [1].

Для данного алгоритма разработан программный комплекс решения задачи коммивояжера. На рис. 1 изображен результат работы генетического алгоритма к задаче коммивояжера, каждый столбец отображает результат на каждом шаге выполнения алгоритма. Менее жирная полоска – самое лучшее решение, найденное на данном шаге, а более жирная – общее качество популяции, т.е. среднеарифметическое всех решений на данном шаге, посредине отображается диаграмма. Если навести курсор на любой из столбцов, то появиться подсказка о шаге, к которому относиться столбец. Под диаграммой указанно время работы алгоритма, значение целевой функции.

Анализ полученных данных говорит о том, что предложенная в работе стратегия использования генетического алгоритма позволяет: получать набор оптимальных решений, является гибкой, обладает высоким быстродействием (15%-30%) на одних и тех же входных данных, по сравнению с другими алгоритмами. ВСА≈O(n^2).

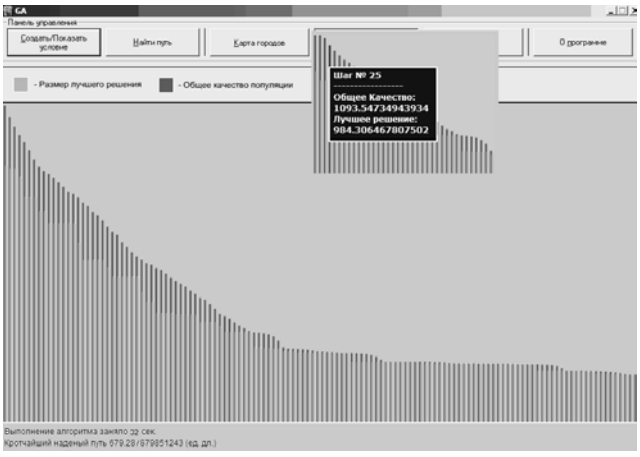

Рис. 1. Столбчатая диаграмма значений ЦФ на последовательных итерациях

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Гладков Л.А., Курейчик В.М, Курейчик В.В.* Генетические алгоритмы. − Ростов-на-Дону: Ростиздат, 2004.
2. *Ахо А., Хопкрофт Дж., Ульман Д.* Построение и анализ вычислительных алгоритмов. – М.: Мир, 1979.
3. *Гладков Л.А.* Генетические операторы. − Таганрог Изд-во: ТРТУ, 2005
4. *Пападимитриу Х., Стайглиц К.* Комбинаторная оптимизация. Алгоритмы и сложность. – М.: Мир, 1985.

УДК 687.06

Х.А. Кажаров

РАЗРАБОТКА ГЕНЕТИЧЕСКОЙ МОДЕЛИ ПОИСКА ПРОСТЫХ ЧИСЕЛ ДЛЯ КРИПТОАНАЛИЗА RSA НА ОСНОВЕ КЛИЕНТ-СЕРВЕРНОЙ СТРУКТУРЫ

Введение. Современные протоколы передачи данных, такие как SSL, TLS, PGP, обеспечивающие защиту передаваемой информации, используют криптосистему RSA для установления защищенного соединения и распределения ключей шифрования. Надежность криптосистемы RSA обуславливает защищенность передачи данных.

В современном мире наблюдается тенденция перехода от использования классических детерминированных алгоритмов к интеллектуальным поисковым системам, системам автоматизированного управления и проектирования. Основными направлениями в разработках интеллектуальных систем в настоящее время являются эволюционные вероятностно-направленные методы. Ярким примером таких методов являются генетические алгоритмы (ГА), ориентированные на поиск глобального оптимума в пространстве возможных решений с многоэкстремальным ландшафтом.

Сегодня генетические алгоритмы успешно применяются для решения классических NP-полных задач, задач оптимизации в пространствах с большим количеством измерений, ряда экономических задач.

Постановка задачи. Все асимметричные криптосистемы характеризуются тем, что используют два ключа: один для шифрования, другой для дешифрования, которые имеют определенную зависимость. В асимметричных криптосистемах наибольшее распространение получила RSA. Функция, реализующая схему RSA, представлена формулой (1):

$$f : x \rightarrow x^e \ (mod\ m). \tag{1}$$

Для дешифрования сообщения $a=f(x)$ достаточно решить уравнение (2):

$$x^e \equiv a \ mod\ m. \tag{2}$$

При некоторых условиях, налагаемых на m и e, это сравнение имеет единственное решение x [1]. Если показатель степени e в сравнении с (2) взаимно прост с $\varphi(m)$ (функция Эйлера), то сравнение (2) имеет единственное решение. Чтобы его найти, необходимо определить число d, удовлетворяющее условию (3):

$$\begin{aligned} &de \equiv 1(\mathrm{mod}(\varphi(\mu))), \\ &1 \le \delta < \varphi(\mu). \end{aligned} \tag{3}$$