

## 改进克隆选择算法的收敛性分析

郑仙花, 骆炎民\*

(华侨大学 计算机科学与技术学院, 福建 厦门 361021)

(\*通信作者电子邮箱 lym@hqu.edu.cn)

**摘要:** 为了完善克隆选择算法(CSA), 使算法理论上成熟, 利用两个随机收敛性度量: 完全收敛和均值收敛, 证明基于多类数据分类的改进克隆选择算法(Multi-CSA)满足收敛到全局最优解的充分条件, 并以实验数据进行验证。从理论上证明了 Multi-CSA 满足收敛的充分条件, 实验方面也表明该算法在经过一定的代数后会收敛。理论和实验上均表明: Multi-CSA 是一个能在有限代内收敛的较为成熟算法。

**关键词:** 人工免疫; 克隆选择; 分类; 收敛性

**中图分类号:** TP181 **文献标志码:** A

## Convergence analysis of improved clonal selection algorithm

ZHENG Xianhua, LUO Yanmin\*

(College of Computer Science and Technology, Huaqiao University, Xiamen Fujian 361021, China)

**Abstract:** In order to improve Clonal Selection Algorithm (CSA) and make it theoretically mature, this paper adopted two random convergence measures: complete convergence and mean convergence to do the convergence analysis for the proposed algorithm named improved clonal Selection Algorithm for Multi-class Classification (Multi-CSA). It demonstrated that the Multi-CAS satisfied the sufficient condition for convergence to a global optimal solution. An experiment was also performed to validate the result. The paper proves that Multi-CAS meets the sufficient condition for convergence. The experiment shows that the algorithm will converge after several generations. It is concluded that Multi-CSA can converge within limited generation and it is a relatively mature algorithm.

**Key words:** artificial immune; clonal selection; classification; convergence

### 0 引言

近几年,随着更多的学者加入研究克隆选择算法,克隆选择算法的发展逐渐趋向成熟。然而,对于这些已提出的克隆选择算法,算法的基础理论模型涉及较少,尤其缺乏对这些算法性能的分析。而算法性能分析的完善程度很大程度上代表了算法理论的成熟度。对于面向学习优化的克隆选择算法,算法的收敛性是衡量其性能以及实用性、完备性的一项重要指标<sup>[1-2]</sup>。文献[3]针对一个特定的多目标优化的免疫系统算法(Multi-objective artificial Immune System Algorithm, MISA),利用马尔可夫链给出了其收敛性的完整证明,但该分析过程缺乏对算法中各个算子数学模型描述。文献[4]给出在求解优化问题时一般克隆选择算法收敛的充分条件,但无法告知算法以某一概率收敛到全局最优所需的最大进化代数如何。文献[5-6]分别给出了B细胞算法(B-Cell Algorithm, BCA)的Markov链模型,并证明了BCA的收敛性。文献[7-9]也对改进的自适应克隆选择算法利用Markov链证明其收敛,文献[8]给出了详细的证明过程。但是文献[5-9]仍是用Markov链模型,存在Markov链不能保证算法一定以概率1收敛到问题最优解、状态数很大、不能分析变异杂交概率时变的非其次克隆选择算法等问题。本文将利用文献[10]提出的进化算法收敛的充分条件证明算法的收敛性,避免了利用Markov链证明收敛时存在的一些问题。

笔者在文献[11]提出了一种基于多类数据分类的改进克隆选择算法(improved Clonal Selection Algorithm For Multi-class classification, Multi-CSA)。由于该算法缺乏对其收敛性的数学分析,因而大大降低了该算法的完善程度。本文在Multi-CSA的基础上,首先分析了算法的执行过程以及整个克隆选择过程中存在的所有算子,并证明算法满足文献[10]中提出的进化算法收敛的充分条件:群体中的每一个个体能以概率 $p(p > 0)$ 使用一步变异变到其他任一个体以及群体中的最优个体以概率 $p = 1$ 存活在每一代中,从而证明算法收敛。

### 1 基于多类数据分类的改进克隆选择算法

为了分析整个算法的过程及存在的算子,此处对该算法步骤进行简单描述(算法详细过程参考文献[11])。算法流程见图1。

算法步骤简述如下:

1) 随机生成初始抗体种群 $Ab_{|N|}$ , 记忆抗体群 $Ab_{|m|}$ 。每个抗体表示为 $ab = (C_1, C_2, \dots, C_K)$ , 其中 $K$ 为类别数,  $C_i = (c_{i,1}, c_{i,2}, \dots, c_{i,F})$ 表示第 $i$ 类的最佳聚类中心。

2) 对抗体群 $Ab_{|N|}$ 重复进行如下操作:

① 计算 $Ab_{|N|}$ 中所有抗体的适合度。考虑抗体的类内距

收稿日期: 2012-09-17; 修回日期: 2012-11-14。

基金项目: 福建省自然科学基金资助项目(2012J01273); 泉州市科技计划项目(2010Z53)。

作者简介: 郑仙花(1989-), 女, 福建莆田人, 硕士研究生, 主要研究方向: 人工智能、机器学习、图像处理; 骆炎民(1974-), 男, 福建惠安人, 副教授, 主要研究方向: 人工智能、数据挖掘、机器学习。

和类间距:

$$f = \frac{1}{DB} = \frac{1}{\frac{1}{K} \sum_{k=1}^K R_k} = \frac{1}{\frac{1}{K} \sum_{k=1}^K \frac{S_k}{\frac{1}{K} \sum_{l=1}^K d_{kl}}}$$

其中:  $S_k$  为类别  $k$  的类内方差即类内距,  $d_{kl}$  为类别  $k$  与类别  $l$  之间的类间距。

② 从  $Ab_{[N]}$  选择  $n$  个亲和力较高的抗体, 产生新抗体群  $Ab_{[n]}$ 。采取基于抗体浓度的选择策略。

$$P(ab) = \frac{1}{D(ab)} = \frac{1}{|f - f_{\text{fit}}|}$$

③ 对  $Ab_{[n]}$  中的抗体进行克隆操作, 产生克隆集合  $C_{\text{clone}}$ 。

$$C_{\text{clone}} = \sum_{i=1}^N \text{round}\left(\frac{B \times N}{i}\right)$$

④ 对克隆集合  $C_{\text{clone}}$  进行变异操作, 产生  $C_{\text{clone}}^*$ 。以一定的变异率采取随机均匀变异方式。

$$c'_{i,k} = \begin{cases} c_{i,k}, & r \geq pm\_ab \\ u_{\min}^k + r \times (u_{\max}^k - u_{\min}^k), & \text{其他} \end{cases}$$

重新计算  $C_{\text{clone}}^*$  中抗体的适合度, 选择  $C_{\text{clone}}^*$  抗体群中的优势抗体进入记忆抗体群  $Ab_{[m]}$ 。

⑤ 用  $Ab_{[m]}$  中抗体替换  $Ab_{[N]}$  中亲和力低的抗体。

3) 重复 2), 直至算法满足终止判断。前后两次进化时种群的总适合度差异在给定的阈值  $T$  范围之内或者达到设定的迭代次数。

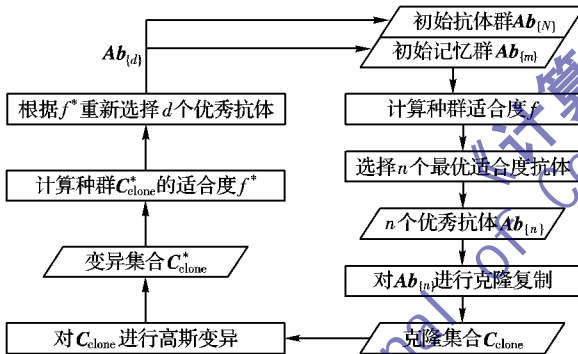


图1 Multi-CSA 克隆选择算法流程

## 2 Multi-CSA 的收敛性分析

### 2.1 进化算法的收敛性度量

进化算法具有状态转移随机的特性, 因此要确定算法的收敛要通过随机收敛性验证。两个常用的随机收敛性的度量是完全收敛和均值收敛。文献[10]提出: 完全收敛意味着以概率 1 收敛, 以概率 1 收敛和均值收敛意味着收敛。文献[10]对收敛以及最优化问题中的完全收敛、均值收敛下定义如下:

**定义 1** 若进化算法能确保在有限的步骤内找到最优解, 并且这样的解此后一直保持在群体中, 则算法被称为收敛到全局最优。

**定义 2** 对于最优化问题, 设  $(X_t; t \geq 0)$  是由进化算法生成的群体序列, 若非负随机序列  $D_t = f^* - F_t$  完全收敛到 0, 则进化算法被称为完全收敛到全局最优值  $f^*$ 。

**定义 3** 对于最优化问题, 设  $(X_t; t \geq 0)$  是由进化算法生成的群体序列, 若非负随机序列  $D_t = f^* - F_t$  均值收敛到 0, 则进化算法被称为均值收敛到全局最优值  $f^*$ 。

定义 2 和 3 中的  $F_t$  是指在时间步  $t$  时群体中最优个体的

适应度值, 即  $F_t = \max\{f(X_{t,1}), \dots, f(X_{t,n})\}$ ,  $f$  是目标函数,  $f^*$  定义为  $f^* = \max\{f(x); x \in X\}$ 。

### 2.2 克隆选择算法收敛的充分条件

在某些假设的条件下进化算法的收敛性已经得到证明, 后面将以进化算法收敛的充分条件证明克隆选择算法收敛。

对任何优化问题, 文献[10]给出了在下列条件下, 进化算法完全收敛及均值收敛到全局最优。

**条件 1** 群体中的每一个个体能以概率  $p(p > 0)$  使用一步变异变到其他任一个体。

**条件 2** 群体中的最优个体以概率  $p = 1$  存活在每一代中。

上述两个条件可用数学语言描述如下:

$$\forall x, y \in X, P\{y = T_m(x)\} \geq \delta_m > 0 \quad (1)$$

$$P\{v_n^*(T_n(x_1, \dots, x_n)) = v_k^*(x_1, \dots, x_k)\} = 1 \quad (2)$$

其中:  $v_k^*$  表示由  $k$  个个体组成的群体中的最优个体。 $v_k^*$  的定义如下:

$$v_k^*(x_1, x_2, \dots, x_k) = \max\{f(x_i) | i = 1, 2, \dots, k\}$$

若只有式(1)成立, 则能证明不管它的初始状态是什么, 算法能以概率 1 接触到全局最优值。但是因为不能保证在找到最优值之后该最优值能永远保留在群体中, 因而不能就此说明它是收敛的。若式(2)也成立, 就能证明算法能收敛到全局最优。因此当克隆选择算法满足式(1)和式(2), 则可说明该算法收敛到全局最优。

### 2.3 Multi-CSA 的收敛条件分析

由 Multi-CSA 的步骤可以看出, 该算法是通过对抗体群进行克隆选择而不断产生新一代的抗体群。其中的克隆选择机制主要包括选择( $T_s$ )、克隆( $T_c$ )、变异( $T_m$ )、再选择( $T_{rs}$ )以及替换( $T_{rp}$ )。

Multi-CSA 的单一迭代过程可以描述如下:

$$(x'_1, \dots, x'_m) = T_m(T_c(T_s(x_1, \dots, x_n))) \quad (3)$$

$$(x''_1, \dots, x''_k) = T_{rs}(x'_1, \dots, x'_m) \quad (4)$$

$$(y_1, \dots, y_n) = T_{rp}((x_1, \dots, x_m), (x''_1, \dots, x''_k)) \quad (5)$$

注: 式(5)中  $k < n$ ,  $T_{rp}(X(1:n), Y(1:k))$  表示用  $Y$  中的  $k$  个抗体替换  $X$  中亲和力低的  $k$  个抗体。

通过分析选择算子( $T_s$ )、克隆算子( $T_c$ )、变异算子( $T_m$ )、再选择算子( $T_{rs}$ )以及替换算子( $T_{rp}$ ),  $T_s$ 、 $T_c$ 、 $T_{rs}$ 、 $T_{rp}$  都不改变种群的个体, 只是在数量上增减( $T_{rp}$  是用  $T_{rs}$  选择后的个体替换原种群中某些个体, 因而也没改变个体), 这也意味着将进化算法收敛的充分条件中的条件 1 应用到 Multi-CSA 时只要考虑变异算子  $T_m$ 。对于条件 2, 则要考虑对种群执行  $T_s$ 、 $T_c$ 、 $T_m$ 、 $T_{rs}$ 、 $T_{rp}$  中的任何一个算子都不会再丢失全局最优解。对于该改进克隆选择算法而言, 条件 1 和条件 2 可用下式表述:

$$\forall x, y \in X, P\{y = T_m(x)\} \geq \delta_m > 0 \quad (6)$$

$$\begin{cases} P\{v_n^*(T_s(x'_1, \dots, x'_n)) = v_k^*(x''_1, \dots, x''_k)\} = 1 \\ P\{v_n^*(T_c(x'_1, \dots, x'_n)) = v_k^*(x''_1, \dots, x''_k)\} = 1 \\ P\{v_n^*(T_m(x'_1, \dots, x'_n)) = v_k^*(x''_1, \dots, x''_k)\} = 1 \\ P\{v_n^*(T_{rp}((x_1, \dots, x_n), (x''_1, \dots, x''_k))) = v_k^*(x''_1, \dots, x''_k)\} = 1 \end{cases} \quad (7)$$

为了说明 Multi-CSA 收敛到全局最优, 要证明 Multi-CSA 符合下述定理。

**定理 1** 对于优化问题, 只要在进化过程中采用基于杰出者选择的策略, 则不管它的初始值是什么, Multi-CSA 完全

收敛及均值收敛到全局最优。

证明 要证明定理1成立,只要证明 Multi\_CSA 满足式(6)、式(7)且种群能在有限的步骤内收敛到最优解。

假设长度为  $L$  的抗体是搜索空间的一个点,并用向量  $\{1, \dots, K\}^L$  表示,  $K$  为种群中个体的字符集基数。若群体中某个个体与最优解相比,有  $c$  个位不匹配,也就是说有  $L - c$  个位匹配,那么该个体一步超变异能到达全局最优解的概率为:

$$P_c^{(L)} = \frac{c!}{L^c} \times \frac{1}{K^c} \times \frac{1}{L} \quad (8)$$

其中第一项表示从  $L^c$  个可能的选择中选择  $c$  个位的排列。这个数还要乘以抗体中每个位实际随机变异概率  $1/L$ 。因为种群个体的字符集基数为  $K$ ,搜索空间的每个点用一个向量  $\{1, \dots, K\}^L$  表示,一步变异某个基因位转变为最优解相应基因位的概率为  $1/K$ ,则该个体中  $c$  位进行一步变异转变成最优解的概率表述为第二项。

由于式(8)  $P_c^{(L)}$  总是大于0,故满足式(6)。

根据式(8)有:

$$P_{\text{Multi\_CSA}} = P_c^{(L)} = \frac{c!}{L^c} \times \frac{1}{K^c} \times \frac{1}{L} \geq \frac{L!}{L^L K^L} \frac{1}{L} \quad (9)$$

不等式(9)的证明如下:

当  $K = 2$  时,

$$\frac{L!}{L^L} = \frac{c!}{L^c} \times \frac{c+1}{L} \times \dots \times \frac{L-1}{L} \times \frac{L}{L} \leq \frac{c!}{L^c} \quad (10)$$

$$\frac{L!}{L^L K^L} \frac{1}{L} = \frac{L!}{L^L \times 2^L} \frac{1}{L} \leq \frac{c!}{L^c \times 2^c} \frac{1}{L} = \frac{c!}{L^c} \frac{1}{K^c} \frac{1}{L} \quad (11)$$

当  $K > 2$  时,有  $K^L \geq K^c$ ,因此  $\frac{1}{K^L} \leq \frac{1}{K^c}$ ,由式(10)知  $\frac{L!}{L^L} \leq \frac{c!}{L^c}$

$$\frac{c!}{L^c}, \text{则 } \frac{L!}{L^L K^L} \frac{1}{L} = \frac{L!}{L^L} \frac{1}{K^L} \frac{1}{L} \leq \frac{c!}{L^c} \frac{1}{K^c} \frac{1}{L}.$$

式(9)表明某个抗体通过一步变异成最优解的概率下界为:

$$P_{\text{Multi\_CSA}} \geq \frac{L!}{L^L K^L} \frac{1}{L}$$

那么对于一个含有  $n$  个个体的群体来说,变异算子进化  $t$  代不能将一个个体转换成最优解的概率至多是  $(1 - P_{\text{Multi\_CSA}})^n$ 。因而在  $t$  代内,保证能获得最优解的概率为  $P_t \geq 1 - (1 - P_{\text{Multi\_CSA}})^n$ 。

若要 Multi\_CSA 至少以概率  $\delta$  访问到最优个体,选择  $t_1$  使式(12)成立即可:

$$P_t \geq 1 - (1 - P_{\text{Multi\_CSA}})^{t_1 n} \geq \delta \quad (12)$$

不等式(12)右半部分两边同减1得:

$$1 - [1 - (1 - P_{\text{Multi\_CSA}})^{t_1 n}] \leq 1 - \delta$$

不等式两边取对数:

$$t_1 n \log(1 - P_{\text{Multi\_CSA}}) \leq \log(1 - \delta)$$

化简后为:

$$t_1 \leq \frac{\log(1 - \delta)}{n \log(1 - P_{\text{Multi\_CSA}})}$$

因为  $t_1$  代数为整数,故

$$t_1 \leq \text{int} \left[ \frac{\log(1 - \delta)}{n \log(1 - P_{\text{Multi\_CSA}})} \right] = t_{\text{Multi\_CSA}} \quad (13)$$

变异算子经过  $t_{\text{Multi\_CSA}}$  代后收敛,说明该改进算法可以经过有限代数后收敛到最优解。

在一定条件下可以保证 Multi\_CSA 算法概率收敛所需的进化代数比遗传算法(Genetic Algorithm, GA)少。文献[12]中对一个二进制编码的遗传算法,用 Markov 链检测到遗传算

法收敛的严格上界,该上界保证遗传算法以概率  $\delta$  所需的迭代代数  $t_{\text{GA}}$ :

$$\begin{cases} P = \min \left\{ \frac{u(1-u)^{L-1}}{K-1}, \left( \frac{u}{K-1} \right)^L \right\} \\ t_{\text{GA}} = \text{int} \left[ \frac{\ln(1-\delta)}{n \ln(1-P)} \right] \end{cases} \quad (14)$$

用式(13)和式(14)解不等式  $t_{\text{Multi\_CSA}} \leq t_{\text{GA}}$ ,只要  $L$  足够大,可以解不等式得到 Multi\_CSA 算法的进化代数上界低于遗传算法。

要证明式(7)也即条件2也成立,就要证明:一旦找到最优解,对种群执行的任何一个算子都不会再丢失全局最优解。

$T_s$  选择算子,是从初始种群中选择优秀个体,若种群存在全局最优解,会被选出而不会丢失。

$T_c$  克隆算子,只产生个体的拷贝,不会改变任何个体的值,因此不会丢失全局最优解。

$T_m$  变异算子,只对克隆算子产生的中间种群  $C_{\text{clone}}$  进行操作,也不改变由其他任何算子产生的个体。

$T_{rs}$  再选择算子,从变异群  $C_{\text{clone}}$  中选择优势个体,因而不改变种群的个体。

$T_p$  替换算子,删除种群中低亲和力的个体,取而代之  $T_{rs}$  算子产生的高亲和力个体,因而最优解不会丢失。

由此可见,该改进算法满足式(7)也即条件2。

综上所述,定理得证。

### 3 算法收敛实验验证

为了方便算法运用于实际情况以及进一步证实第2章的内容,此处将对算法的一些主要参数进行实验分析,更加直观地说明算法的收敛性。

实验采用的数据是2006年9月25日获取的福建省云霄县漳江口国家红树林保护区域的30米TM遥感图像(multispectral landsat Thematic Mapper image),如图2所示

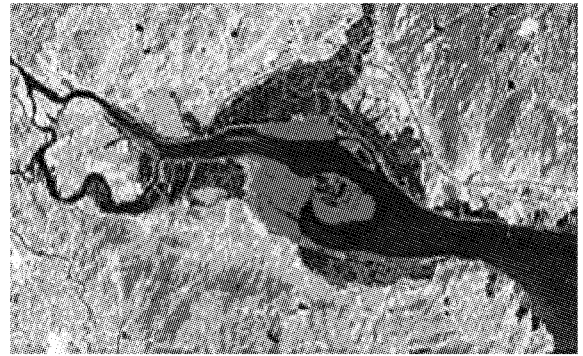


图2 TM 遥感图像原图

图3是对实验图像用取值不同的算法参数组合(5,0.05,1),(8,0.05,1),(5,0.05,0.5),(5,0.07,1)运行100次的种群适合度收敛情况。(5,0.05,1)表示参数克隆数  $\text{clonenum}$  的取值为5,增殖系数  $\text{Fat}$  的取值为0.05,变异率  $\text{pm}$  的取值为1。

由图3可知,在对实验图像的训练学习中,Multi\_CSA 在各参数值组合中均能在100代内收敛。从而也从实验方面说明,Multi\_CSA 是收敛的。

### 4 结语

本文通过分析克隆选择算法收敛的充分条件和 Multi\_



CSA 的各个算子,证明 Multi\_CSA 中的各个算子满足进化算法收敛的两个充分条件(选择采用基于杰出者的机制),从而证明 Multi\_CSA 是收敛的。本文还通过实验直观阐述在各种

参数值组合的情况,Multi\_CSA 收敛的情况。这些分析在理论和应用上均证明了 Multi\_CSA 是收敛的,完善了该改进算法,具有一定的实用意义。

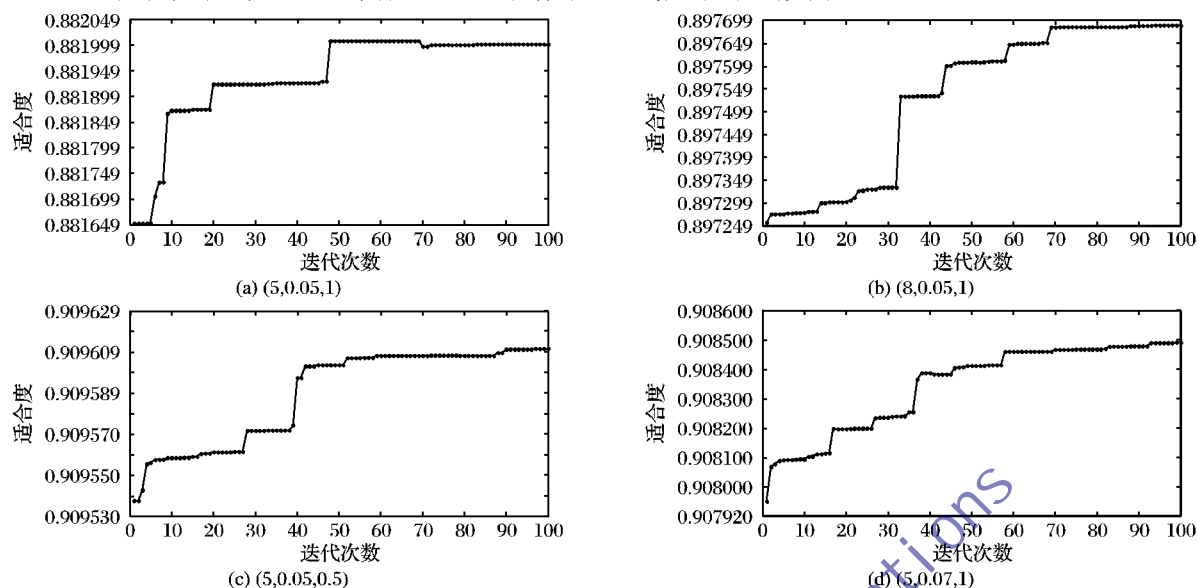


图3 不同参数组合时种群适合度情况

#### 参考文献:

- [1] 于瀛,侯朝桢.一种克隆选择算法的收敛性分析[J].计算机应用,2006,26(6):96-98.
- [2] 洪露,纪志成,龚成龙.一类克隆选择算法的收敛性方法研究[J].信息与控制,2011,40(2):232-236.
- [3] VILLALOBOS-ARIAS M, COELLO C A C, HEMANDEZ-LEMA O. Convergence analysis of a multi-objective artificial immune system algorithm[C]// Proceedings of the 3rd International Conference on AIS. Berlin: Springer-Verlag, 2004: 226-235.
- [4] CUTELLO V, NICOSIA G, ROMEO M, et al. On the convergence of immune algorithm[C]// Proceedings of IEEE Symposium on Foundations of Computational Intelligence. Washington, DC: IEEE Computer Society, 2007: 409-415.
- [5] CLARK E, HONE A, TIMMIS J. A Markov chain model of the B-cell algorithm[C]// Proceedings of the 4th International Conference on Artificial Immune Systems. Berlin: Springer, 2005: 318-330.
- [6] 方贤进,幕学海,刘凌冰,等.基于B细胞算法的克隆选择算法的收敛性分析[J].计算机应用,2010,30(3):772-775.
- [7] 焦李成,杜海峰,刘芳,等.免疫优化计算、学习与识别[M].北京:科学出版社,2006.
- [8] 马力,焦李成,白琳,等.自适应多克隆聚类算法及其收敛性分析[J].模式识别与人工智能,2008,21(1):72-81.
- [9] 吴秋逸,焦李成,李阳阳,等.自适应量子免疫克隆算法及其收敛性分析[J].模式识别与人工智能,2008,21(5):592-597.
- [10] RUDOLPH G. Finite Markov chain results in evolutionary computation: a tour d'hORIZON[J]. Fundamenta Informaticae, 1998, 35(14): 67-89.
- [11] 郑仙花,骆炎民.基于多类数据分类的改进克隆选择算法[J].计算机应用,2012,32(11):3201-3205.
- [12] GREENHALGH D, MARSHALL S. Convergence criteria for genetic algorithms[J]. SIAM Journal on Computing, 2000, 30(1): 269-282.

(上接第761页)

#### 参考文献:

- [1] GENTRY C. Certificate-based encryption and the certificate revocation problem [C]// Proceedings of EUROCRYPT 2003. Berlin: Springer-Verlag, 2003: 272-293.
- [2] KANG B G, PARK J H, HAHN S G. A certificate-based signature scheme[C]// Proceedings of CT-RSA 2004. Berlin: Springer-Verlag, 2004: 99-111.
- [3] LI J G, HUANG X Y, MU Y, et al. Certificate-based signature: security model and efficient construction [C]// Proceedings of EuroPKI 2007. Berlin: Springer-Verlag, 2007: 110-125.
- [4] LI J G, XU L Z, ZHANG Y C. Provably secure certificate-based proxy signature schemes [J]. Journal of Computers, 2009, 4(6): 444-452.
- [5] LI J G, HUANG X Y, ZHANG Y C, et al. An efficient short certificate-based signature scheme [J]. The Journal of Systems and Software, 2012, 85(12): 314-322.
- [6] JAKOBSSON M, SAKO K, IMPAGLIAZZO R. Designated verifier proofs and their applications [C]// Proceedings of EUROCRYPT 1996. Berlin: Springer-Verlag, 1996: 143-154.
- [7] SAEEDNIA S, KREMER S, MARKOWITZ O. An efficient strong designated verifier signature scheme [C]// Proceedings of ICISC '2003. Berlin: Springer-Verlag, 2004: 40-54.
- [8] SUSILO W, ZHANG F T, MU Y. Identity-based strong designated verifier signature schemes[C]// Proceedings of ACISP '2004. Berlin: Springer-Verlag, 2004: 313-324.
- [9] ZHANG J, MAO J. A novel ID-based designated verifier signature scheme [J]. Information Sciences, 2008, 178(3): 766-773.
- [10] KANG B Y, BOYD C, DAWSON E. Identity-based strong designated verifier signature schemes: Attacks and new construction [J]. Computers and Electrical Engineering, 2009, 35(1): 49-53.
- [11] 李明洋,郑雪峰,朱建勇,等.一种高效的基于身份的强指定验证者签名方案[J].四川大学学报:工程科学版,2009,41(4): 176-180.
- [12] 孙士峰,温巧燕,金正平,等.对一类强指定验证者签名方案的分析与改进[J].四川大学学报:工程科学版,2011,43(1): 91-96.
- [13] 张永洁,王彩芬,张玉磊.两个指定验证者签名方案的分析与改进[J].计算机应用,2010,30(5): 1227-1229.