

DCA

Departamento de Engenharia de
Computação e Automação Industrial



Faculdade de Engenharia
Elétrica e de Computação



Sistemas Imunológicos Artificiais

IA013 – Introdução à Computação Natural
Tópico 5 – Sistemas Imunológicos Artificiais – Parte 2

Fernando J. Von Zuben

Sistemas Imunológicos Artificiais (SIAs)

■ Definições na literatura:

- *Artificial immune systems* are data manipulation, classification, reasoning and representation methodologies, that follow a plausible biological paradigm: the human immune system (Starlab)
- An *artificial immune system* is a computational system based upon metaphors of the natural immune system (Timmis, 2007)
- The *artificial immune systems* are composed of intelligent methodologies, inspired by the natural immune system, for the solution of real-world problems (Dasgupta, 1998)
- Artificial immune systems (AIS) are adaptive systems, inspired by theoretical immunology and observed immune functions, principles and models, which are applied to problem solving (de Castro & Timmis, 2002)

Sistemas Imunológicos Artificiais (SIAs)

■ Propriedades dos sistemas imunológicos naturais a serem exploradas:

- Unicidade
- Diversidade
- Robustez
- Autonomia
- Auto-organização
- Organização multicamadas
- Reconhecimento de padrões (tolerância e reatividade)
- Maturação de afinidade (otimização)
- Distributividade
- Memória / Memória associativa
- Aprendizado por reforço
- Comportamento presa-predador
- Tolerância a ruído (reconhecimento parcial)
- Coerência sob fluxo de matéria, energia e informação

Sistemas Imunológicos Artificiais (SIAs)

■ Escopo de aplicação (abordagens existentes na literatura):

- Reconhecimento / Classificação de padrões
- Detecção de anomalias e falhas
- Análise de dados (agrupamento, quantização, compactação)
- Sistemas baseados em agentes
- Busca e otimização (ambientes contínuos e discretos)
- Aprendizado de máquina
- Controle autônomo (robótica)
- Vida artificial e Sistemas complexos
- Segurança computacional
- Fluxo de dados (*data streams*)
- Homeostase (sistema nervoso + sistema endócrino + sistema imunológico)

Sistemas Imunológicos Artificiais (SIAs)

- Tratando mais especificamente problemas de otimização, os SIAs possuem três vantagens principais sobre outras abordagens evolutivas clássicas:
 - São inherentemente capazes de manter a diversidade da população;
 - O tamanho da população a cada geração é automaticamente definido de acordo com a demanda da aplicação;
 - Soluções ótimas locais tendem a ser simultaneamente preservadas quando localizadas.

Sistemas Imunológicos Artificiais (SIAs)

■ Primeiras aplicações:

- Fundamentadas em conceitos de imunologia teórica (meados dos anos 80);
- 1990: Bersini aplicou sistemas imunológicos para resolver problemas;
- Meados dos anos 90: Forrest et al. – segurança computacional;
- Trabalho da IBM em detecção de vírus
- Aprendizado de máquina: Hunt et al., também em meados dos anos 90.

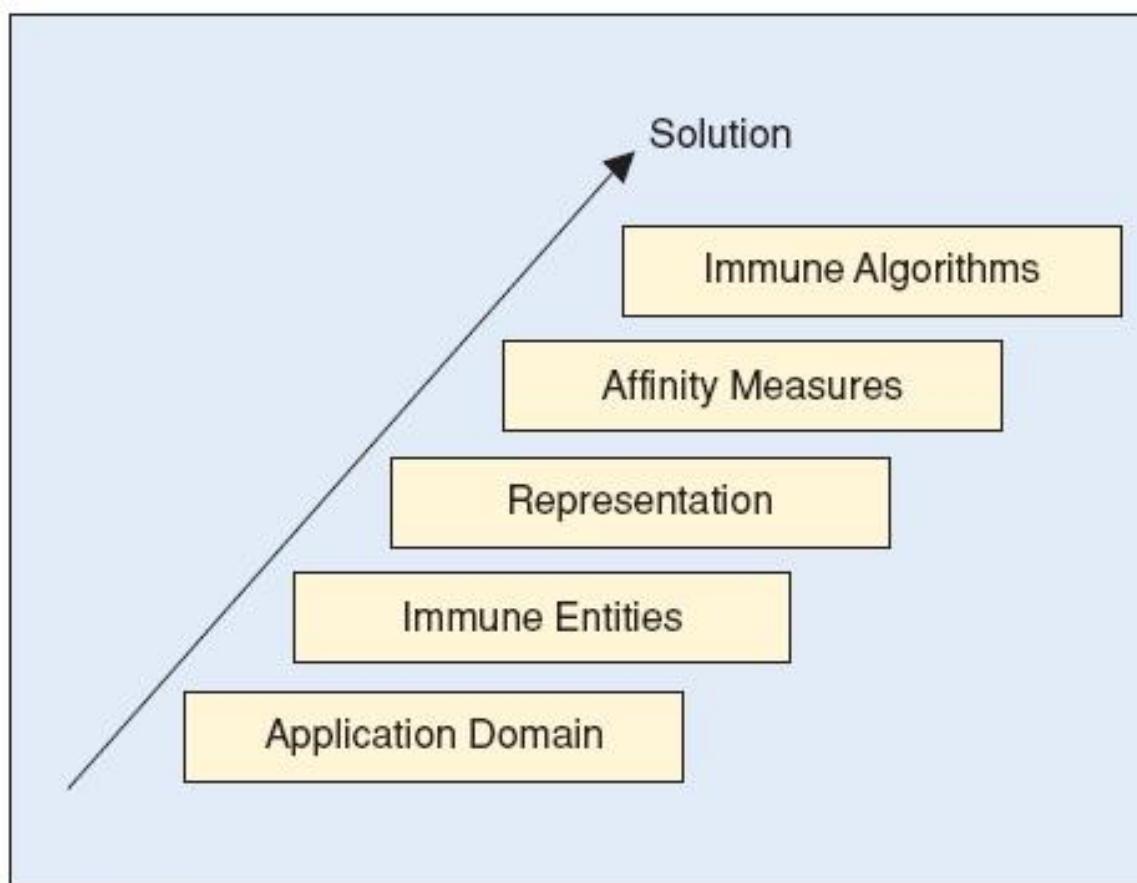
Os primeiros eventos

Year	Event	Activity	Organizer/Speaker
1996	IMBS	Workshop	Y. Ishida
1997	SMC	Special Track / Tutorial	D. Dasgupta
1998	SMC	Special Track	D. Dasgupta
	Book	First edited book	D. Dasgupta (ed.)
1999	SMC	Special Track	D. Dasgupta
2000	GECCO	Workshop	D. Dasgupta
		Talk: "Why Does a Computer Need an Immune System"	S. Forrest
	SMC	Tutorial: "Immunological Computation"	D. Dasgupta
		Special Track	
2001	SBRN	Tutorial: "Artificial Immune Systems and Their Applications"	L. N. de Castro
	ICANNGA	Tutorial: "An Introduction to the Artificial Immune Systems"	L. N. de Castro
	CEC	Tutorial: "Artificial Immune Systems: An Emerging Technology"	J. Timmis
2002	Journal (Special Issue)	IEEE-TEC: Special Issue on Artificial Immune Systems	D. Dasgupta (ed.)
	Book	Artificial Immune Systems: A New Computational Intelligence Approach	L. N. de Castro & J. Timmis
	ICARIS	First International Conference on AIS	J. Timmis & P. Bentley
2003	Various	ICARIS, Special Tracks, Special Issues, etc.	Various

Formalismo matemático

- Como representar matematicamente / computacionalmente células e moléculas?
- Como quantificar as interações e o grau de reconhecimento?
- Como implementar computacionalmente a natureza distributiva e multi-agente do sistema imunológico?
- Espaço de formas (Perelson & Oster, 1979):
 - Descrição quantitativa de células e moléculas
- Conceitos acessórios:
 - Formas generalizadas
 - Reconhecimento a partir de regiões de complementariedade
 - Região de reconhecimento (reatividade cruzada)
 - Limiar de afinidade

Passos para a síntese de um algoritmo imuno-inspirado



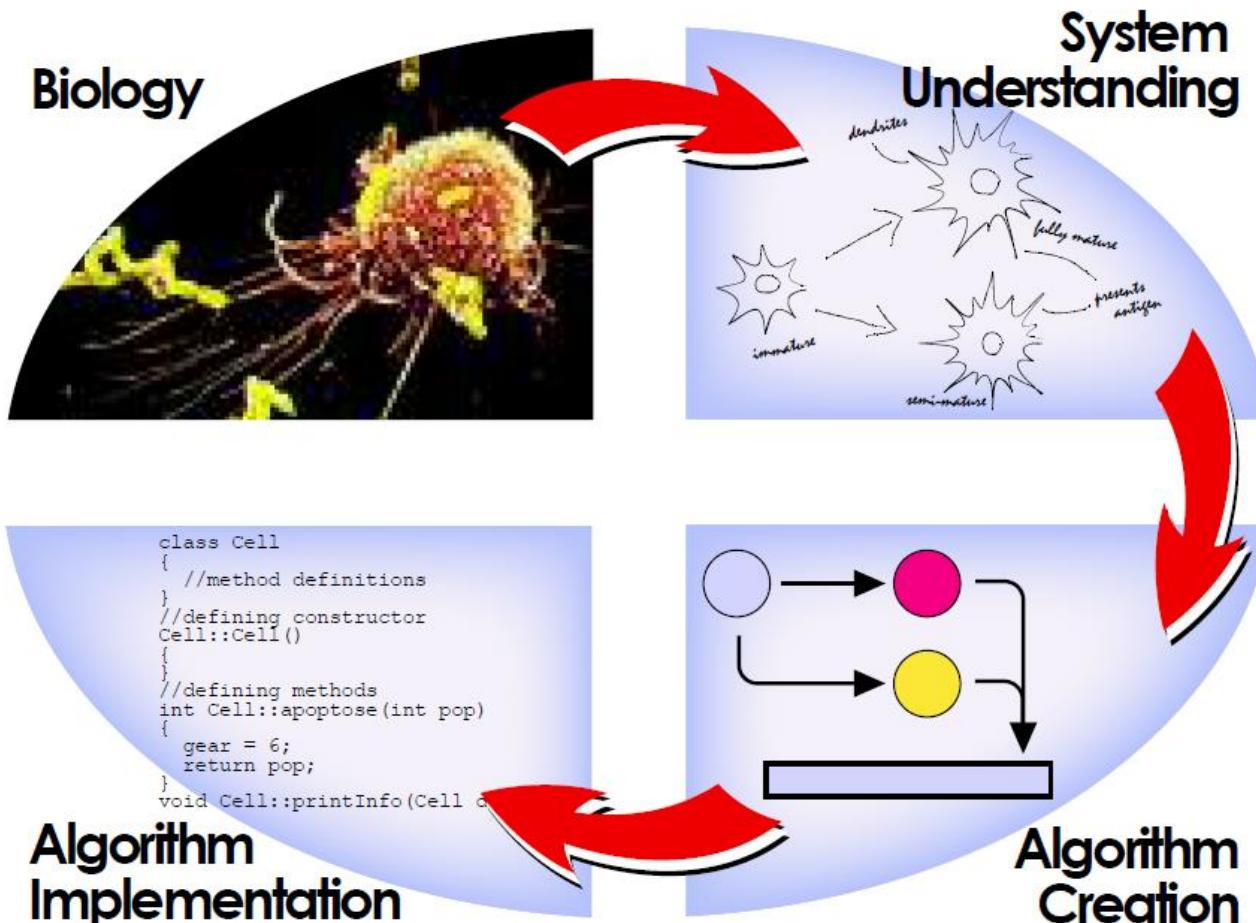
Dasgupta, 2006

FIGURE 4 Implementation steps in solving a problem using an AIS.

Passos para a síntese de um algoritmo imuno-inspirado

1. Problem definition
2. Mapping the real problem into the AIS domain
 - 2.1 Defining the types of immune cells and molecules to be used
 - 2.2 Deciding the immune principle(s) to be used in the solution
 - 2.3 Defining the mathematical representation for the elements of the AIS
 - 2.4 Evaluating the interactions among the elements of the AIS (dynamics)
 - 2.5 Controlling the metadynamics of the AIS
3. Reverse mapping from AIS to the real problem

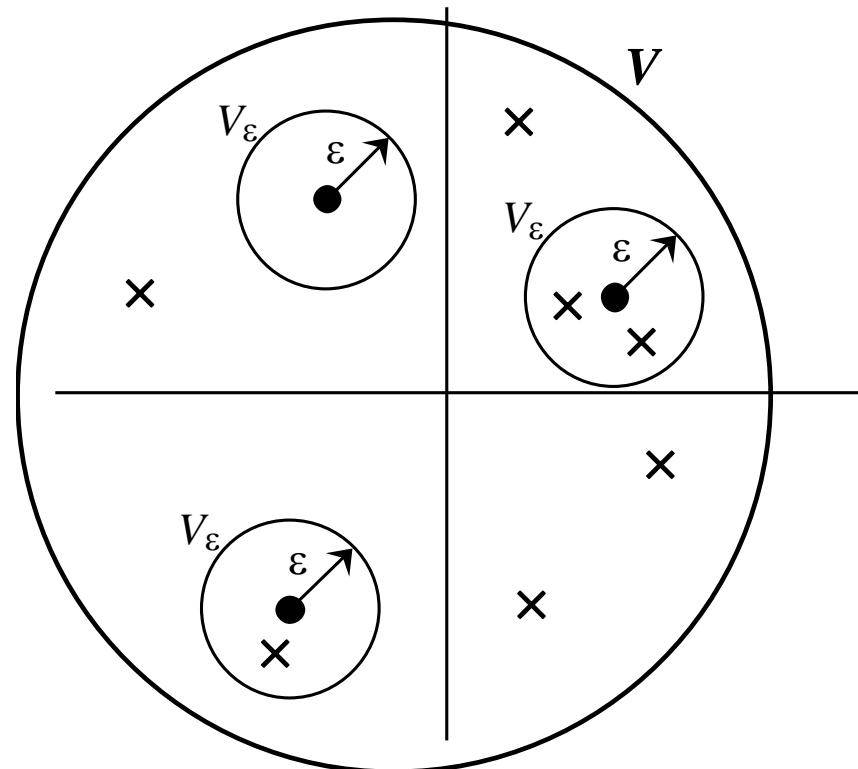
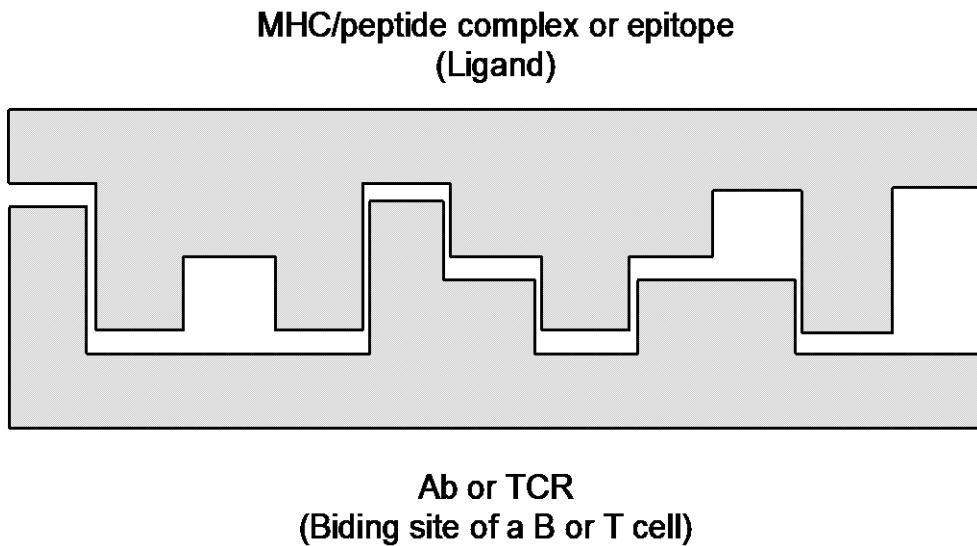
Passos para a síntese de um algoritmo imuno-inspirado



Greensmith, 2007

Espaço de formas

- Reconhecimento por complementaridade
- Reatividade cruzada



Após Perelson, 1989
Não considera
complementaridade e sim
similaridade entre os vetores
de atributos.

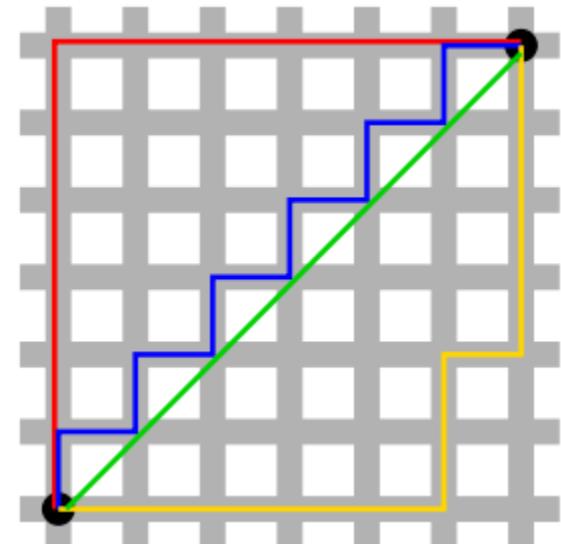
Espaço de formas

■ Representação

- Vetor de atributos: $m = \langle m_1, m_2, \dots, m_L \rangle$,
 $m \in S^L \subseteq \Re^L$
- $\mathbf{Ab} = \langle Ab_1, Ab_2, \dots, Ab_L \rangle$,
- $\mathbf{Ag} = \langle Ag_1, Ag_2, \dots, Ag_L \rangle$

■ Alguns tipos de métricas em espaços de formas:

- Hamming
- Euclidiana
- Manhattan



Espaço de formas

- Afinidade: similaridade (inverso da distância)
- Exemplos de medidas de distância:

□ Euclidiana

$$D = \sqrt{\sum_{i=1}^L (Ab_i - Ag_i)^2}$$

□ Manhattan

$$D = \sum_{i=1}^L |Ab_i - Ag_i|$$

□ Hamming

$$D = \sum_{i=1}^L \delta, \text{ where } \delta = \begin{cases} 1 & \text{if } Ab_i \neq Ag_i \\ 0 & \text{otherwise} \end{cases}$$

Espaço de formas

- Afinidades no espaço de formas de Hamming (usando complementaridade)

0	0	1	1	0	0	1	1
---	---	---	---	---	---	---	---

1	1	1	0	1	1	0	1
---	---	---	---	---	---	---	---

1 1 0 1 1 1 1 0

Affinity: 6

Hamming
distance

0	0	1	1	0	0	1	1
---	---	---	---	---	---	---	---

1	1	1	0	1	1	0	1
---	---	---	---	---	---	---	---

1 1 0 1 1 1 1 0

Affinity: 4

r-contiguous bit
rule

0	0	1	1	0	0	1	1
---	---	---	---	---	---	---	---

1	1	1	0	1	1	0	1
---	---	---	---	---	---	---	---

1 1 0 1 1 1 1 0

Affinity: $6+2^4=22$

Affinity measure
of Hunt

$$D = D_H + \sum_i 2^{l_i}$$

0	0	1	1	0	0	1	1
---	---	---	---	---	---	---	---

1	1	1	0	1	1	0	1
---	---	---	---	---	---	---	---



Flipping one string

0	0	1	1	0	0	1	1
---	---	---	---	---	---	---	---

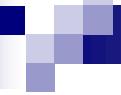
1	1	1	1	0	1	1	0
---	---	---	---	---	---	---	---

• • •

Affinity: $6 + 4 + \dots + 4 = 32$

0	0	1	1	0	0	1	1
---	---	---	---	---	---	---	---

1	1	0	1	1	0	1	1
---	---	---	---	---	---	---	---



Fontes de inspiração para os algoritmos

■ Escopo dos algoritmos

- Algoritmos genéricos e baseados em princípios imunológicos específicos, processos de interação já mapeados e modelos teóricos.

■ Principais tipos

- Algoritmos de Medula Óssea
- Algoritmos de Timo
- Algoritmos de Seleção Clonal
- Algoritmos de Teoria de Rede
- Algoritmos de Células Dendríticas
- Algoritmos de Teoria do Perigo



Taxonomia dos algoritmos imuno-inspirados

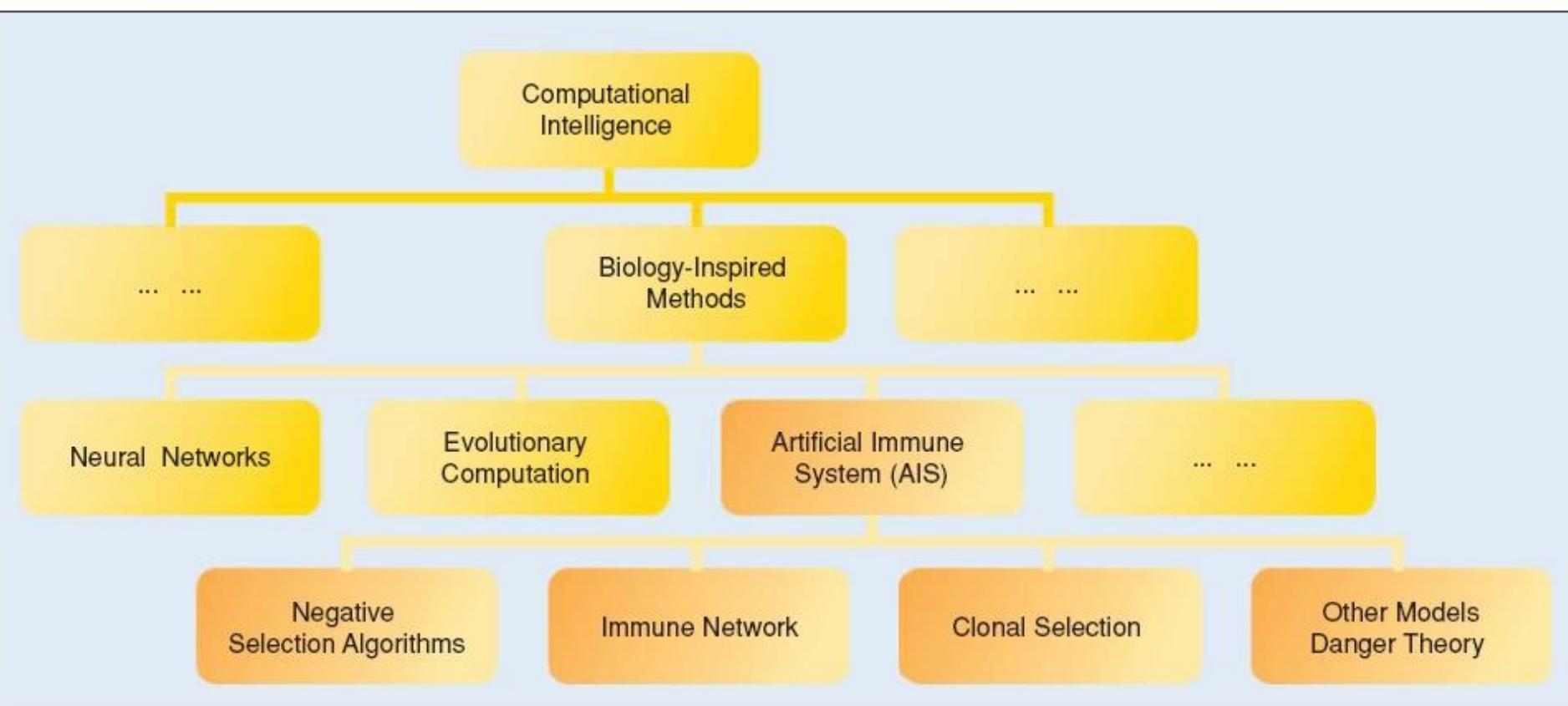
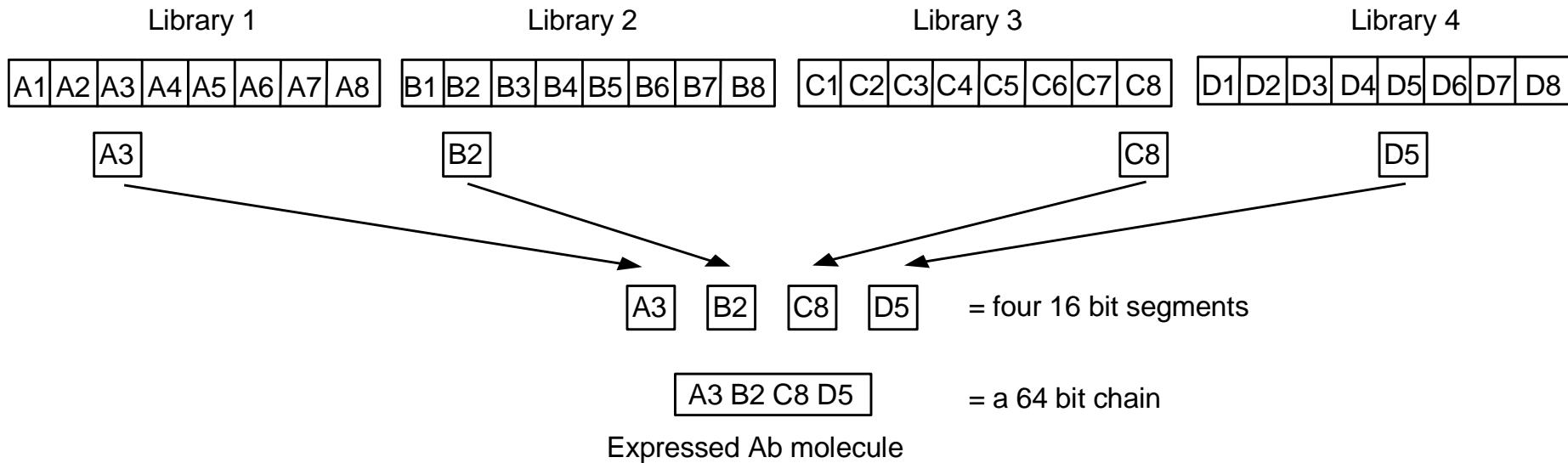


FIGURE 1 Artificial Immune System (AIS) as a branch of Computational Intelligence (CI).

Dasgupta, 2006

Algoritmo de Medula Óssea

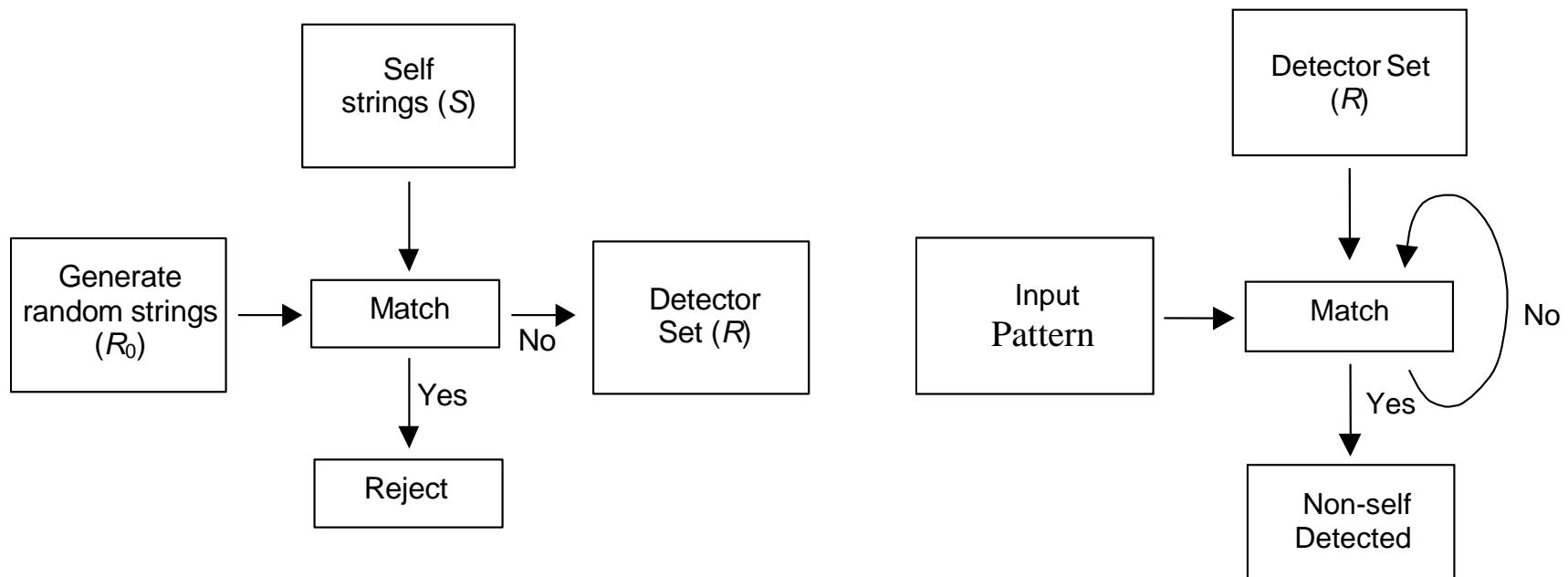
An individual genome corresponds to four libraries:



Após Perelson et al., 1996

Algoritmo de Timo

■ Seleção negativa (Forrest et al., 1994)



Fase de
geração de
repertório

Fase de
operação /
monitoramento

Algoritmo de Timo

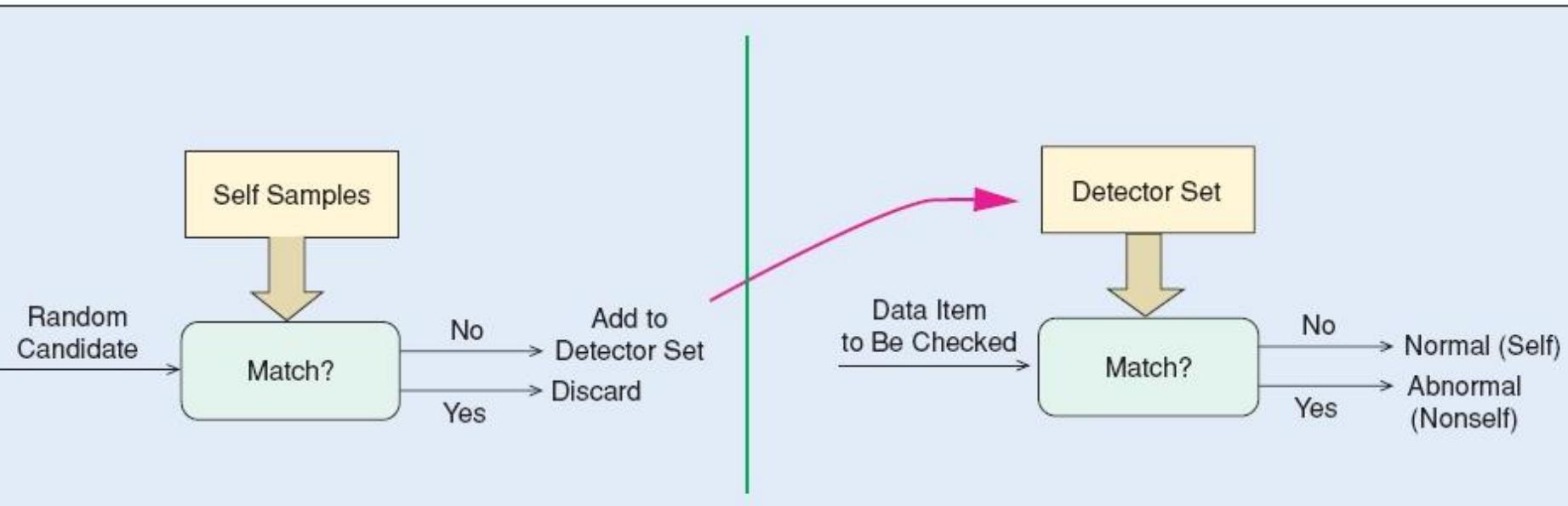
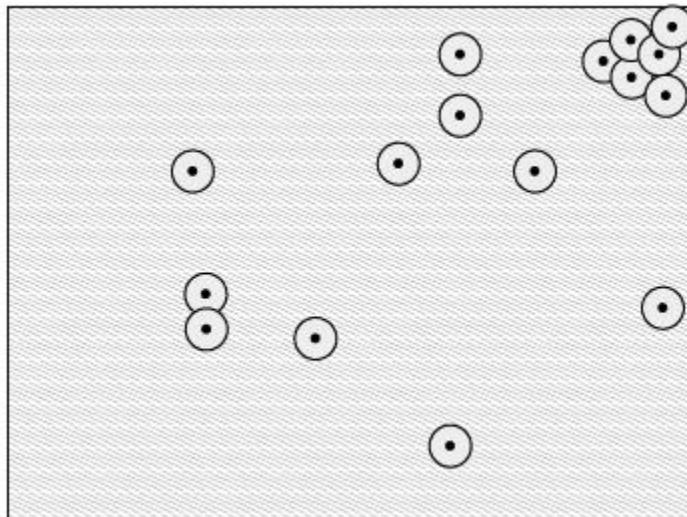


FIGURE 3 The basic concept of the Negative Selection (NS) Algorithm.

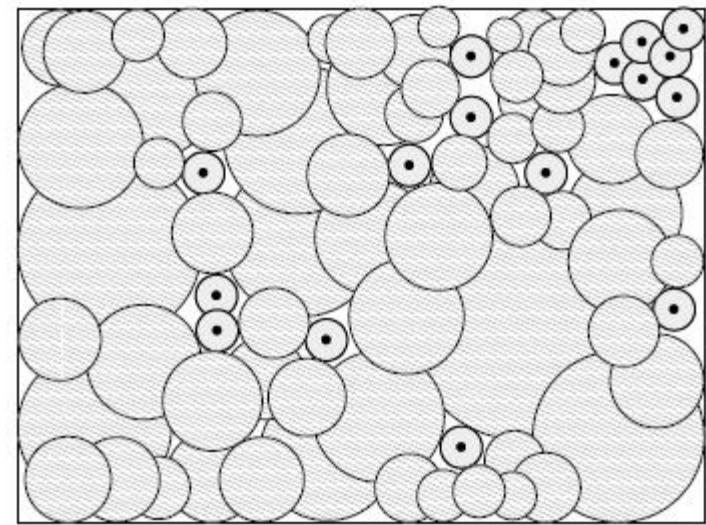
Dasgupta, 2006

Algoritmo de Timo

■ One-class classifiers



Amostras do próprio

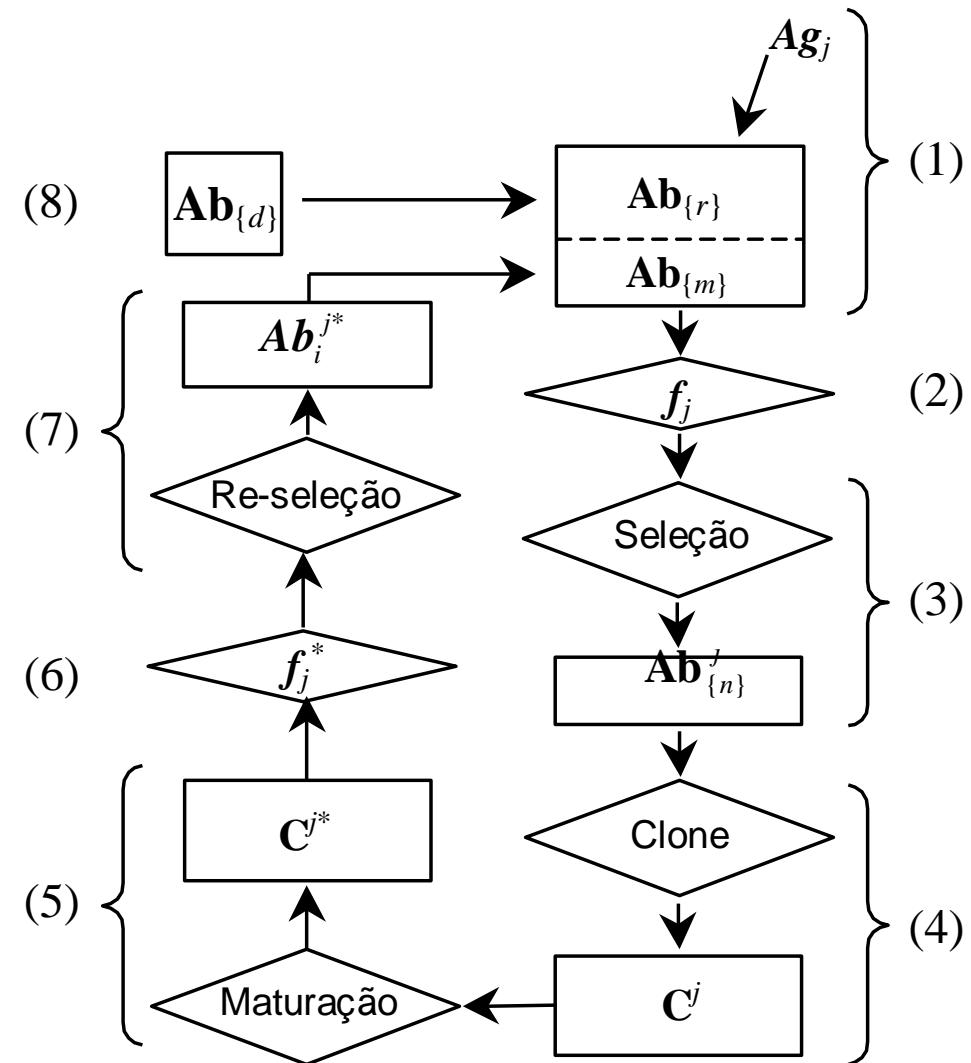


Detectores do não-próprio

Stibor, T.; Mohr, P.; Timmis, J. Is Negative Selection Appropriate for Anomaly Detection? Proceedings of the Genetic and Evolutionary Computation Conference (GECCO'2005).

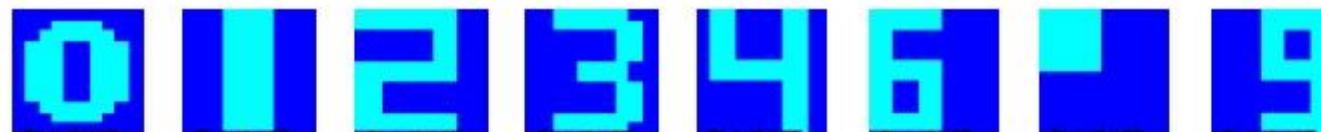
Algoritmo de Seleção Clonal

- CLONALG (de Castro & Von Zuben, 2002): versão para reconhecimento de padrões.

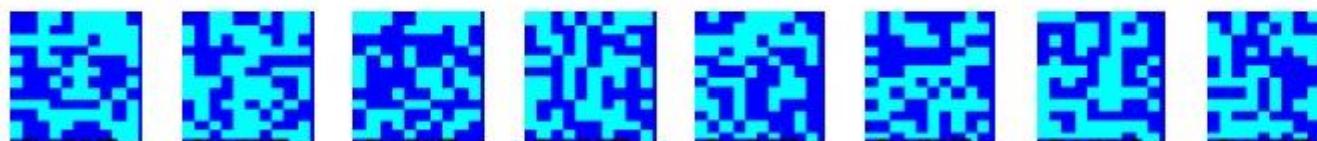


Algoritmo de Seleção Clonal

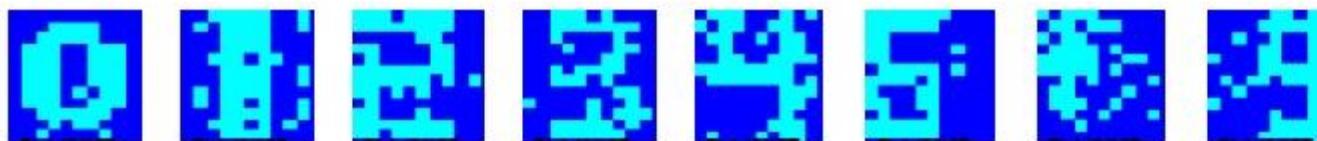
- CLONALG (de Castro & Von Zuben, 2002): versão para reconhecimento de padrões.



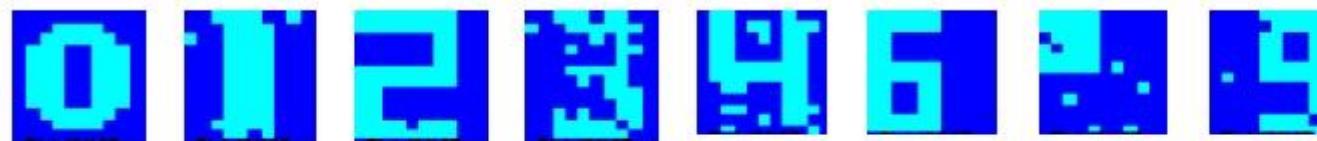
(a) Input patterns



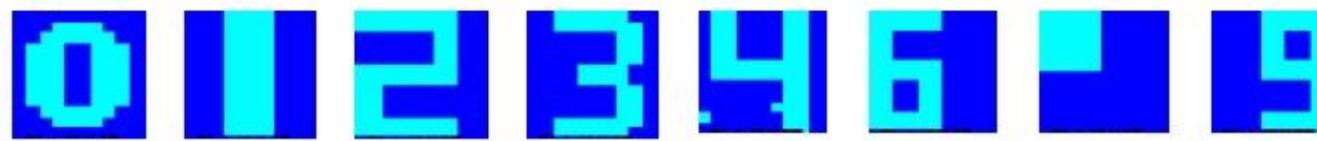
(b) 0 generations



(c) 50 generations



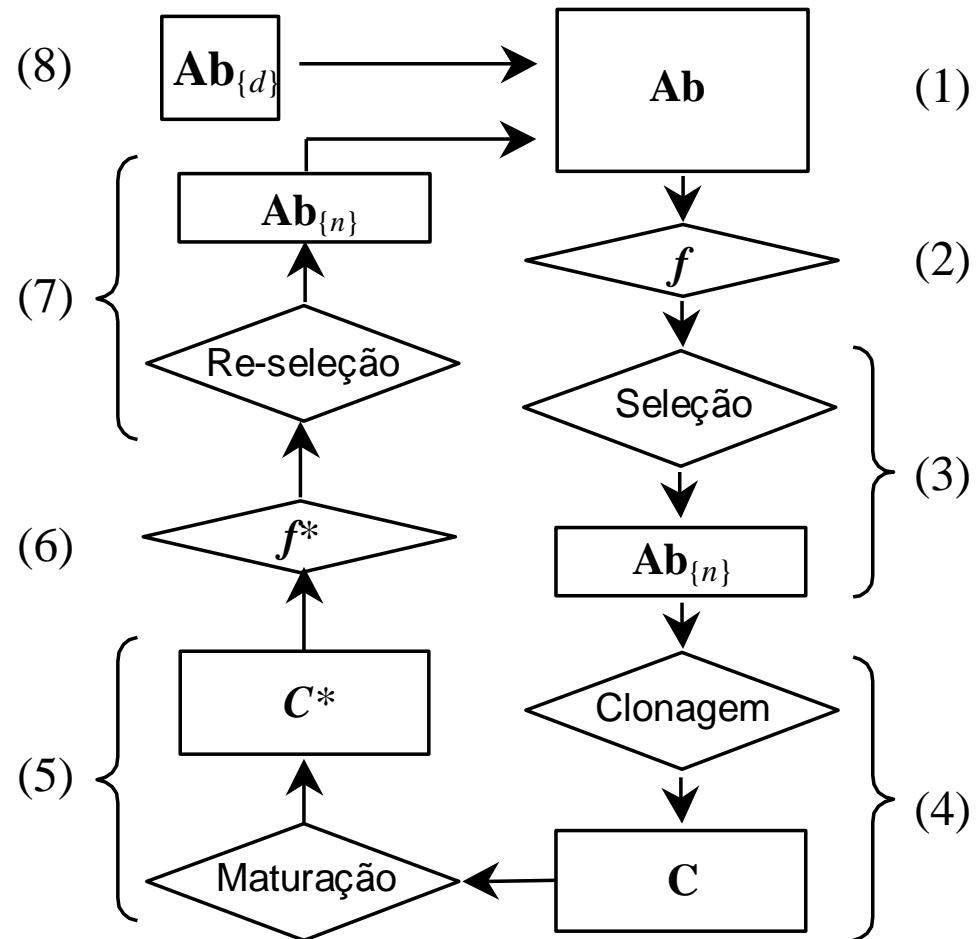
(d) 100 generations



(e) 200 generations

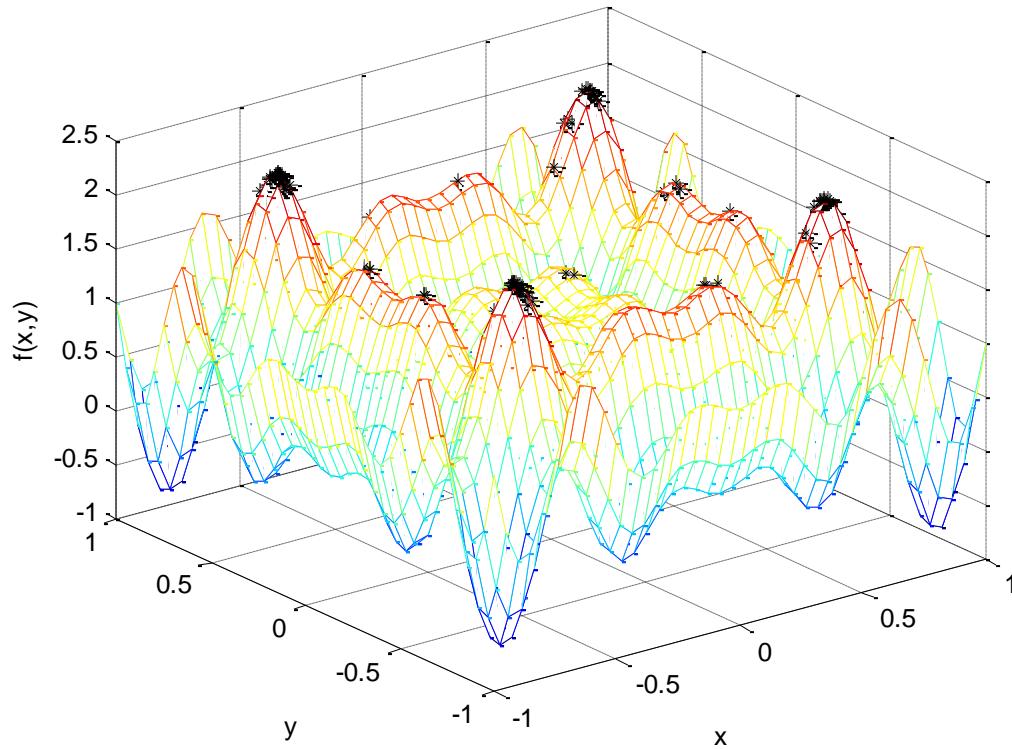
Algoritmo de Seleção Clonal

- CLONALG (de Castro & Von Zuben, 2002): versão para otimização.

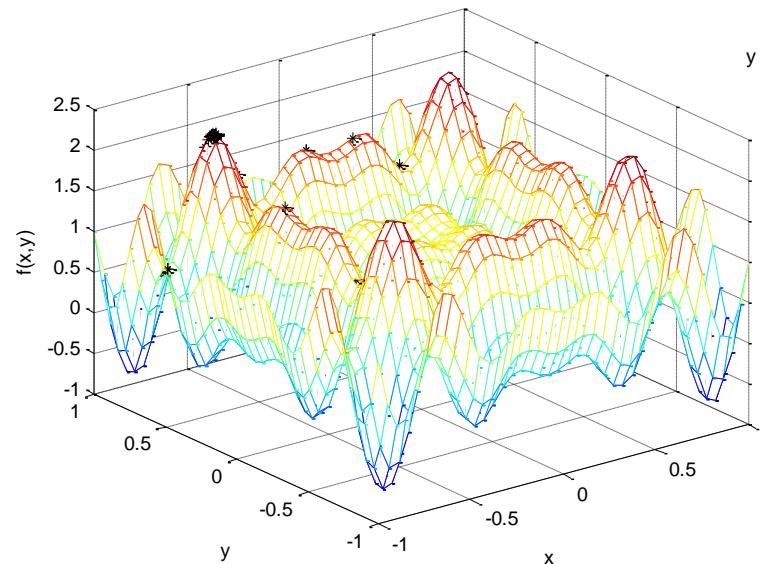
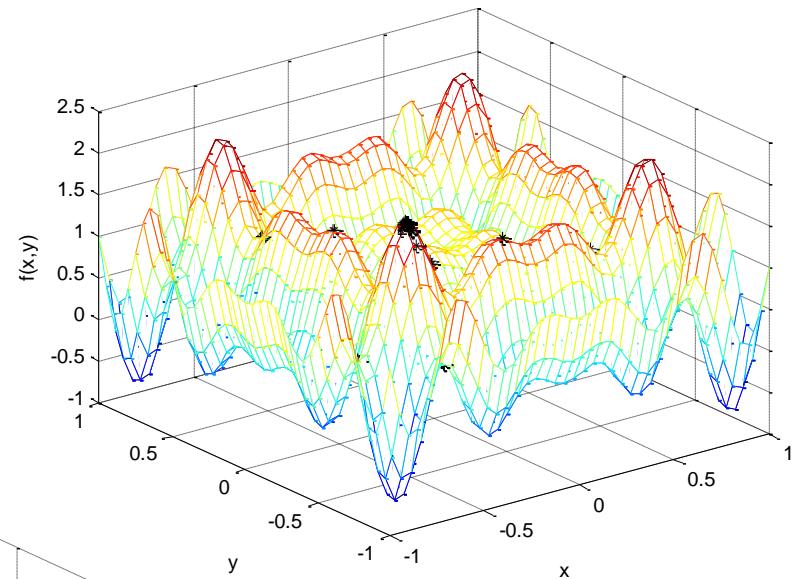
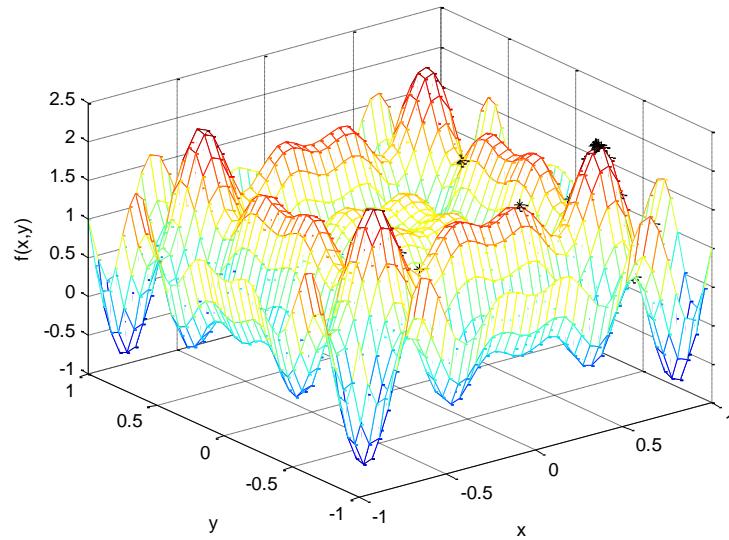


Algoritmo de Seleção Clonal

- CLONALG (de Castro & Von Zuben, 2002): versão para otimização (espaços contínuos).

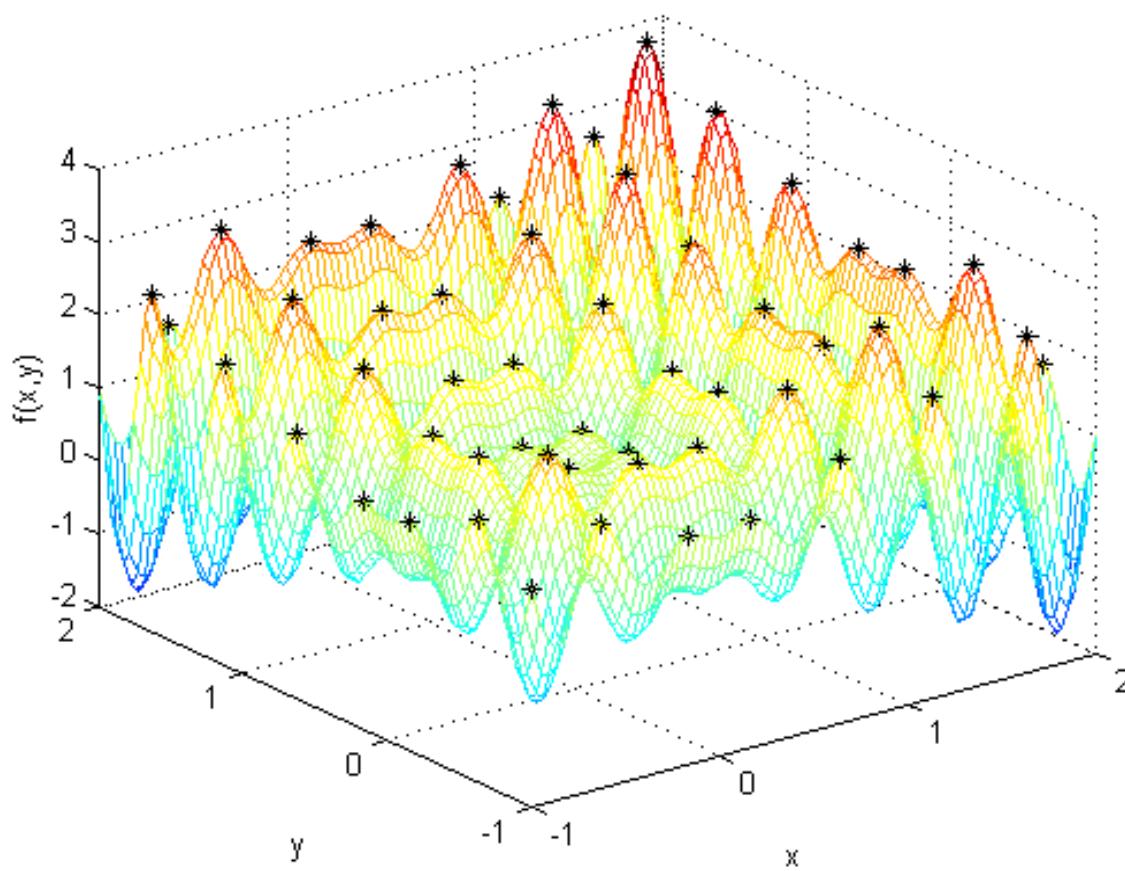


Comparação com múltiplas execuções de um algoritmo genético padrão



Algoritmo de Seleção Clonal

- opt-aiNet (evolução do CLONALG, que inclui a aiNet): versão para otimização (espaços contínuos).



Algoritmo de Seleção Clonal

■ Objetivos do CLONALG

- Implementação computacional do algoritmo de seleção clonal e maturação de afinidade

■ Aplicações

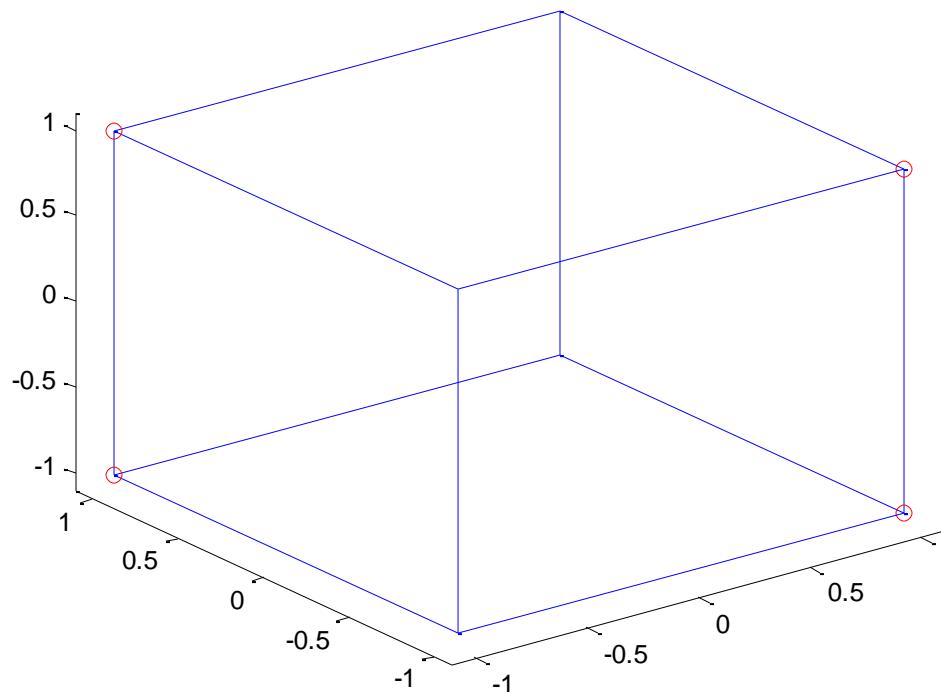
- Aprendizagem de máquina, reconhecimento de padrões, otimização multimodal e combinatória

■ Características

- Geração de variações genéticas através de um processo de hipermutação
- Proliferação e diferenciação celular após o reconhecimento antigênico seguindo o princípio da seleção clonal

Manutenção de diversidade

- A capacidade de geração de soluções diversas pode ser explorada simplesmente na inicialização da população em algoritmos de busca baseados em meta-heurísticas populacionais. Exemplo didático a seguir, onde se buscam 4 sequências binárias de 3 bits maximamente diversas dentre as 8 possíveis.



Algoritmo de Teoria de Rede

Modelo de rede contínua:

$$(1) \quad \frac{da_i(t)}{dt} = \left(\alpha \sum_{j=1}^N m_{ji} a_j(t-1) - \beta \sum_{k=1}^N m_{ik} a_k(t-1) + \lambda m_i - k_i \right) a_i(t-1)$$

Estímulo

Afinidade
Antigênica

Supressão

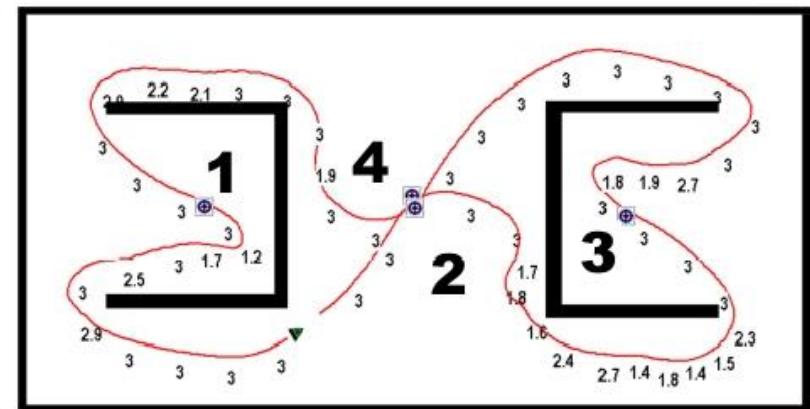
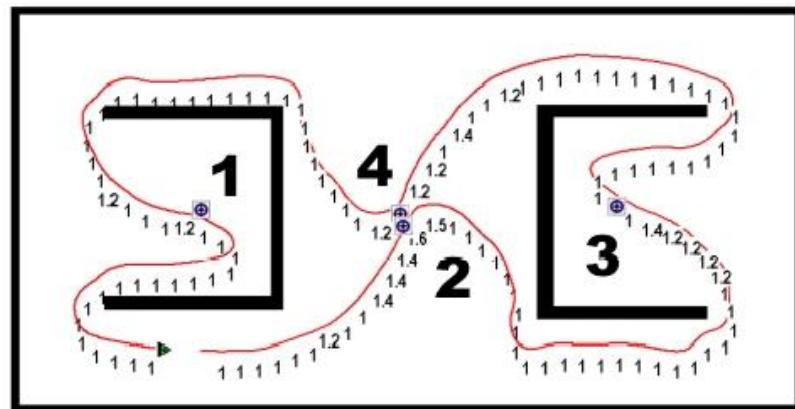
$$(2) \quad a_i(t) = \frac{1}{1 + \exp(0.5 - a_i(t))}$$

Auto-organização + Estímulo externo = Processo regulatório

Algoritmo de Teoria de Rede

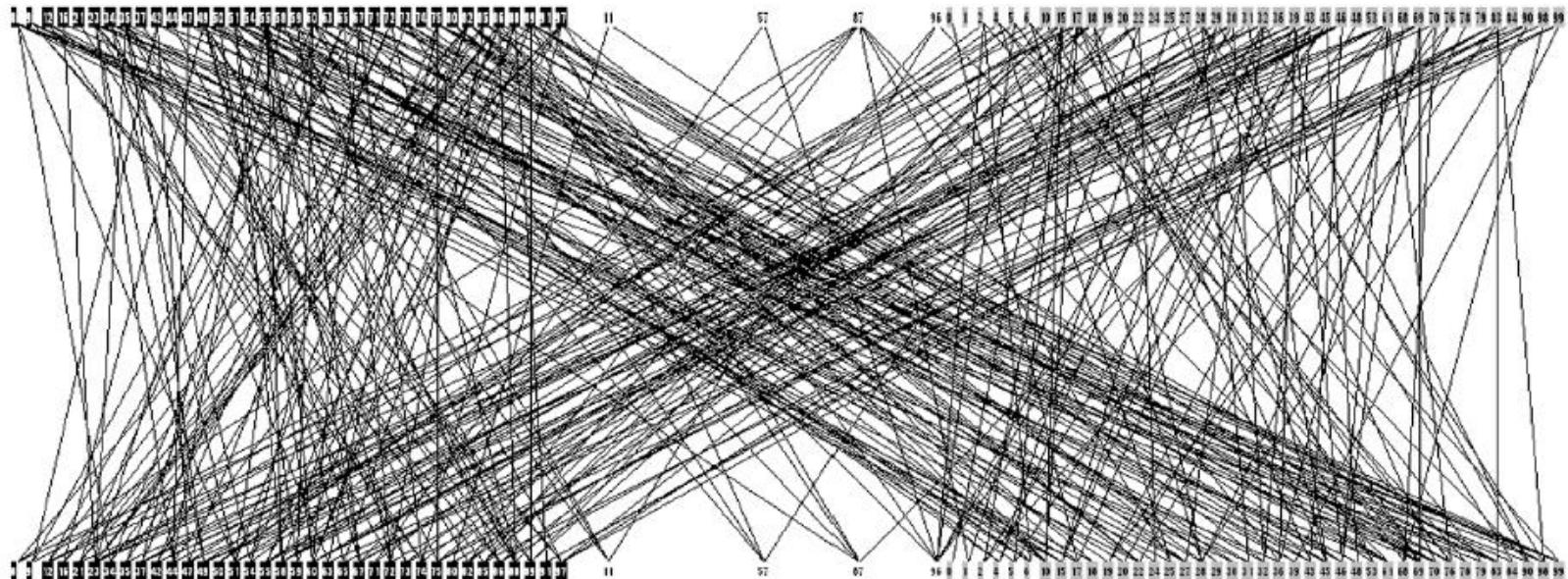
Modelo de rede contínua:

- Comportamento não-reativo em navegação autônoma de robôs



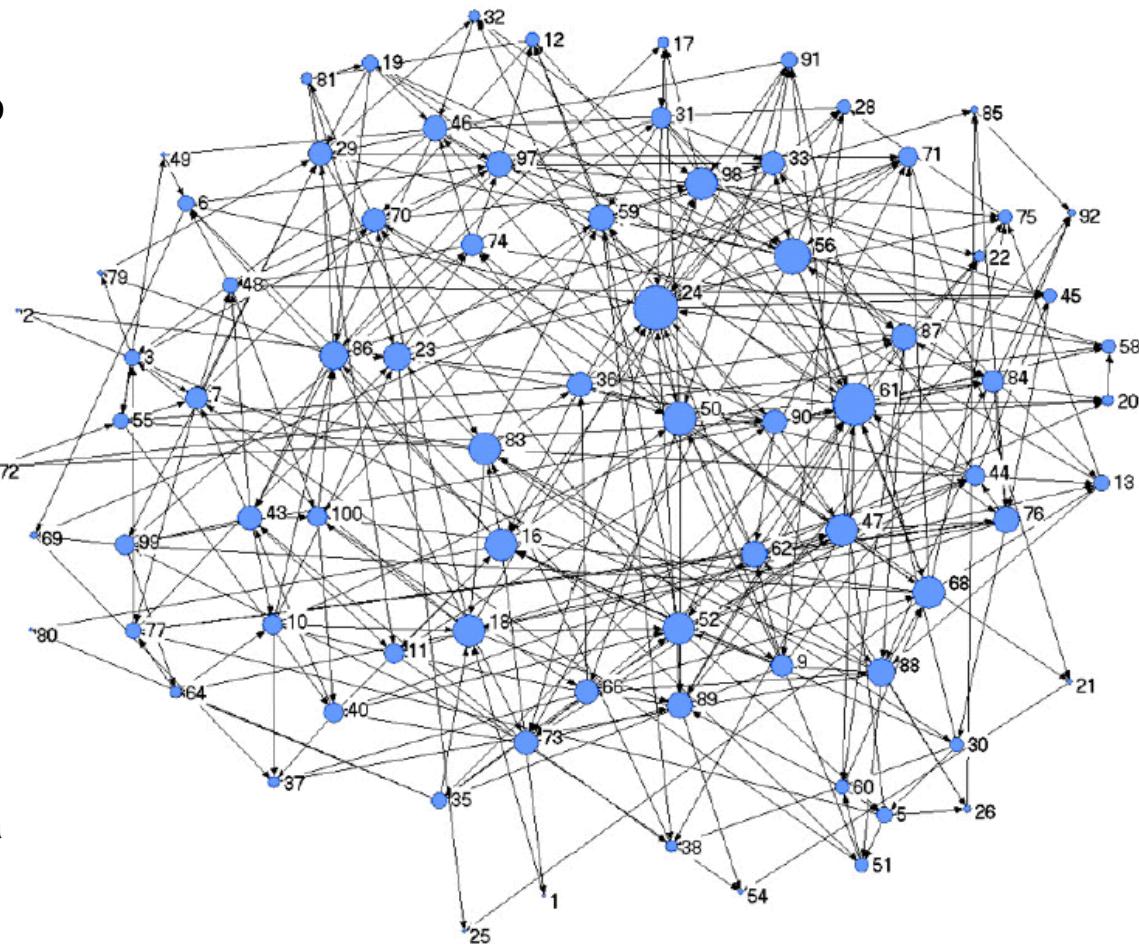
Algoritmo de Teoria de Rede

Modelo de rede contínua:



Algoritmo de Teoria de Rede

- Modelo de rede contínua, onde as células B correspondem aos pontos azuis e as arestas indicam relações de estímulo ou supressão entre células B. A dinâmica da rede atualiza a concentração das células B, sendo que a concentração aumenta com o estímulo e diminui com a supressão. Cada célula B pode ter associada a si uma regra do tipo condição-ação, de modo que regras cujos antecedentes atendem as condições do ambiente e apresentam alta concentração têm mais chance de definir a ação do robô. Implementa-se, assim, um sistema baseado em regras com forte acoplamento entre as regras. A topologia da rede indica como se dá o acoplamento.



Algoritmo de Teoria de Rede

Pseudo-code 1: Main Structure of the aiNet algorithm

Input:

- N : the initial size of the population of antibodies;
- n : the number of cells that should be cloned;
- m : the percentage of cells to be moved to the memory set;
- σ_1 : antibody-antibody suppression threshold;
- σ_2 : antibody-antigen suppression threshold;
- d : the percentage of randomly generated cells to be included in the population.

Randomly create the initial population of N antibodies, each one with dimension L (dimension of the data patterns);

While stop criteria not met do

- 1 – For each antigen do
 - 1.1 – Determine its affinity to all network cells;
 - 1.2 – Select the n highest affinity network cells;
 - 1.3 – Generate N_c clones from these n cells. The higher the affinity, the larger N_c ;
 - 1.4 – Apply hypermutation to the generated clones, with variability inversely proportional to the progenitor's fitness;
 - 1.5 – Determine the affinity among the antigen and all clones;
 - 1.6 – Keep only $m\%$ of the highest affinity mutated clones into the clone population;
 - 1.7 – Eliminate all clones but one whose affinity with the antigen is inferior to a predefined threshold σ_2 (apoptosis);
 - 1.8 – Determine the affinity among all the mutated clones and eliminate those whose affinity with each other is above a pre-defined threshold σ_1 (suppression);
 - 1.9 – Insert the remaining mutated clones into the population;
- 2 – Determine the similarity among all the antibodies and eliminate those with similarity above a threshold σ_1 (suppression);
- 3 - Introduce a percentage $d\%$ of new randomly generated cells (*random insertion*);

End While

Modelo de rede discreta: aiNet

Algoritmo de Teoria de Rede

■ Modelo de rede discreta: aiNet

1. For each antigenic pattern Ag_i ,
 - 1.1 *Clonal selection*: Apply the pattern recognition version of CLONALG that will return a matrix of memory clones for Ag_i ;
 - 1.2 *Apoptosis*: Eliminate all memory clones whose affinity with antigen are below a threshold;
 - 1.3 *Inter-cell affinity*: Determine the affinity between all clones generated for Ag_i ;
 - 1.4 *Clonal Suppression*: Eliminate those clones whose affinities are inferior to a pre-specified threshold;
 - 1.5 *Total repertoire*: Concatenate the clone generated for antigen Ag_i with all network cells
2. *Inter-cell affinity*: Determine the affinity between all network cells;
3. *Network suppression*: Eliminate all aiNet cells whose affinities are inferior to a pre-specified threshold.

Algoritmo de Teoria de Rede

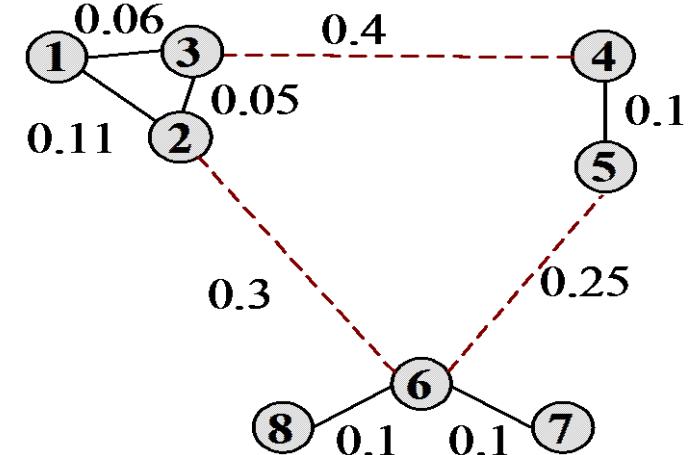
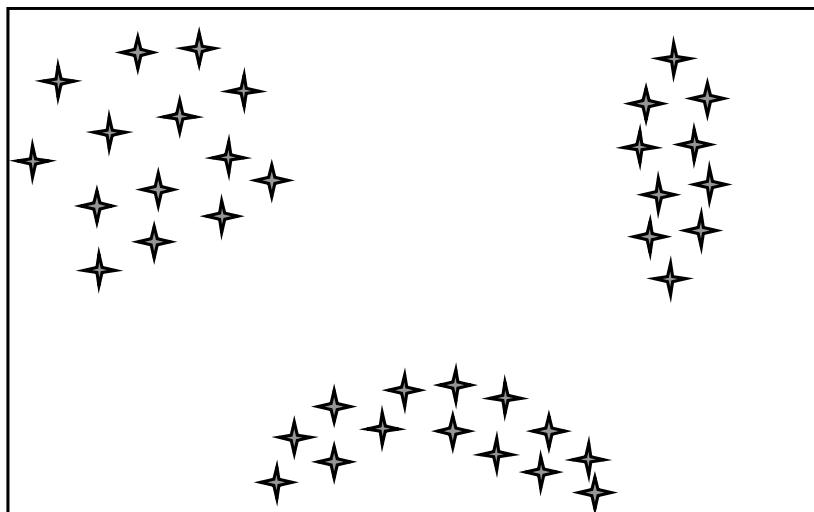
- Modelo de rede discreta: aiNet
- Objetivos
 - Propor um modelo discreto de rede imunológica artificial
- Aplicações
 - Análise de dados e clusterização (com o auxílio de ferramentas estatísticas e de teoria de grafos)
- Características
 - Processo construtivo e de aprendizagem baseados no algoritmo CLONALG
 - Conhecimento distribuído entre as células
 - Conexões representando afinidade (distância) entre células da rede
 - Capacidade de extração de relações entre as amostras de treinamento

Algoritmo de Teoria de Rede

■ Modelo de rede discreta: aiNet

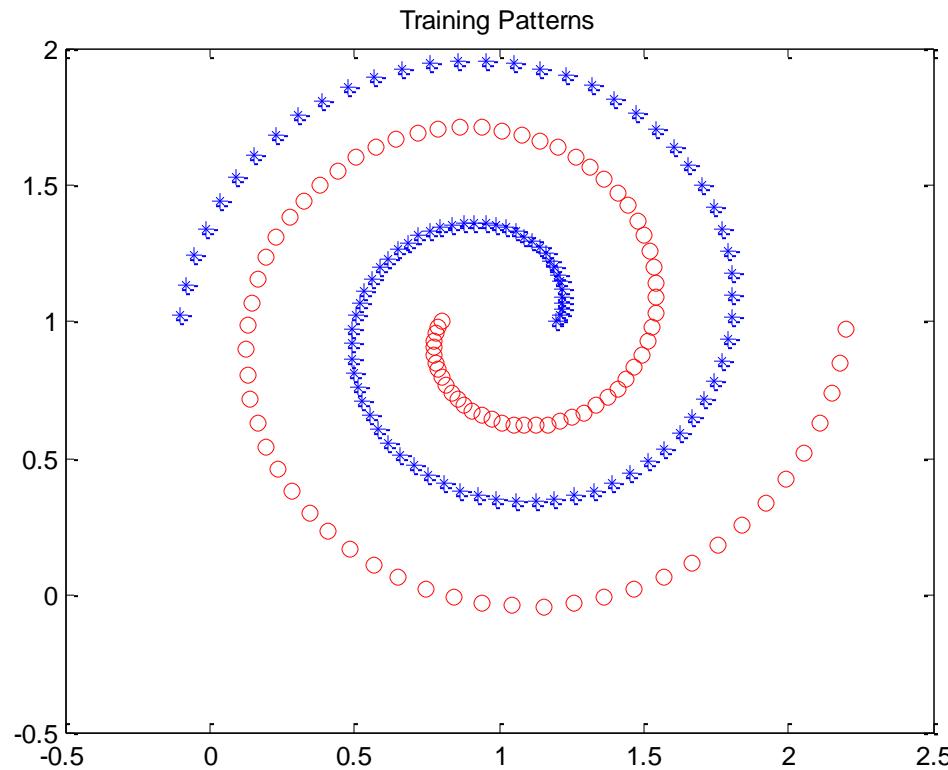
■ Conceito

- A rede *imunológica artificial*, denominada aiNet, é um grafo com conexões ponderadas, não necessariamente totalmente interconectado, composto por um conjunto de nós, denominados anticorpos, e conjuntos de pares de nós, denominados conexões, com uma valor característico associado, chamado de peso da conexão



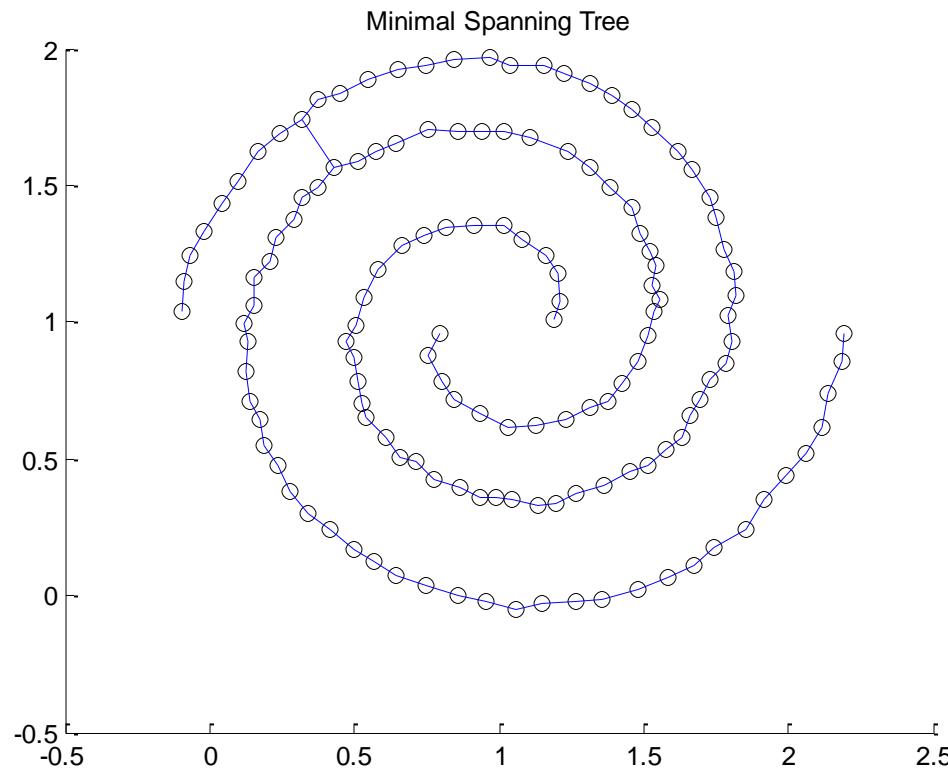
aiNet: Clustering

Dados originais (antígenos)

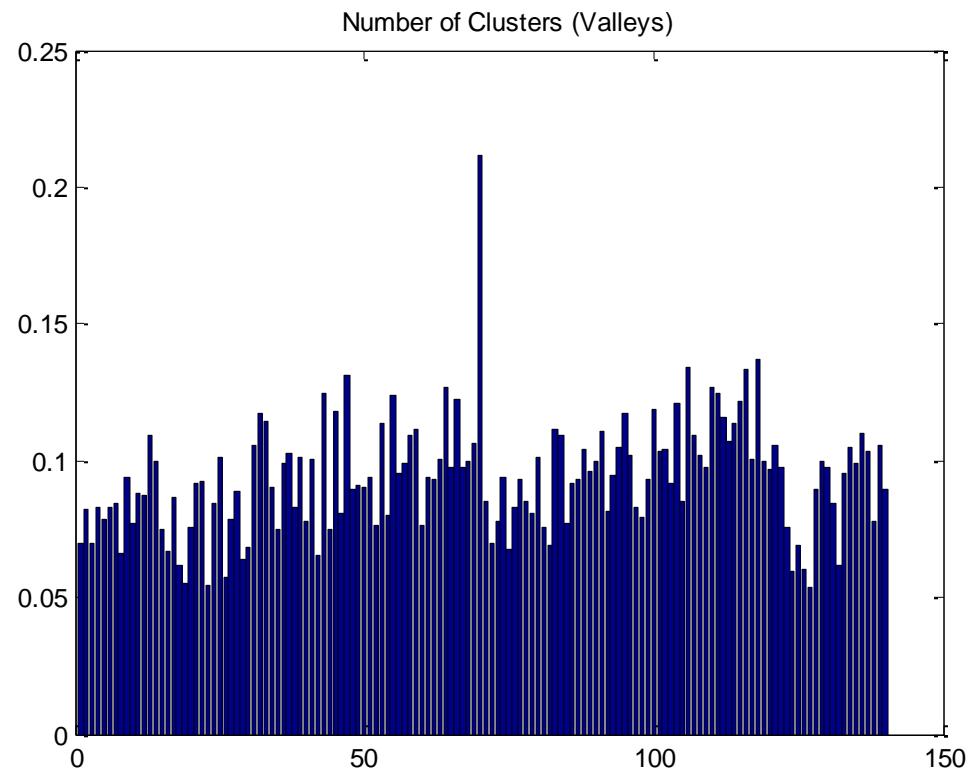


aiNet: Clustering

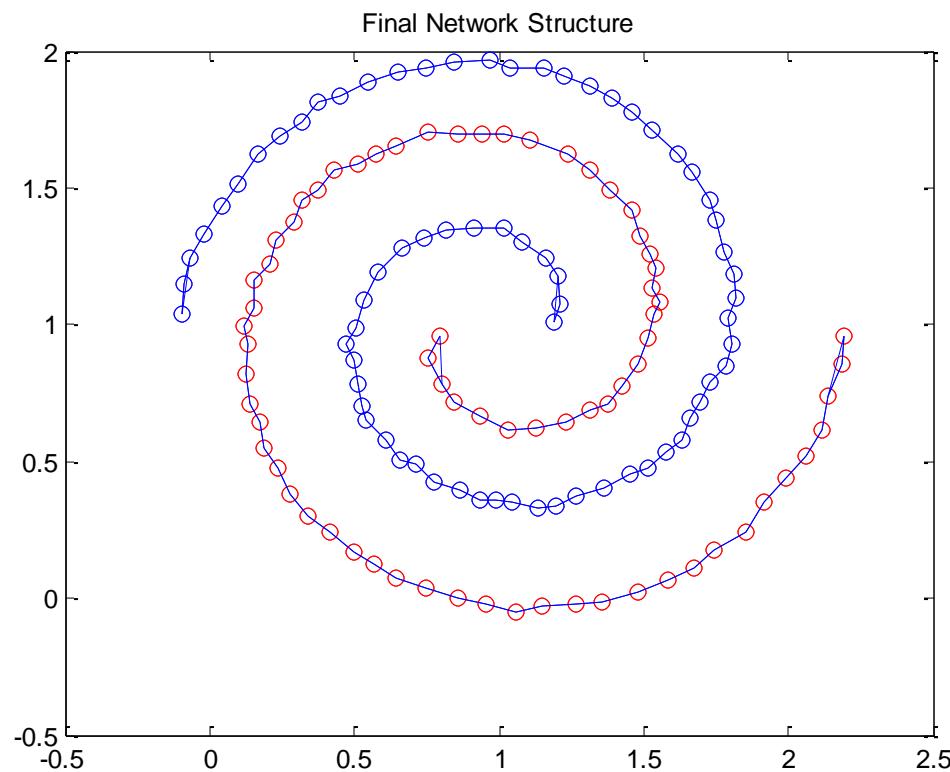
Posicionamento final dos protótipos (anticorpos)



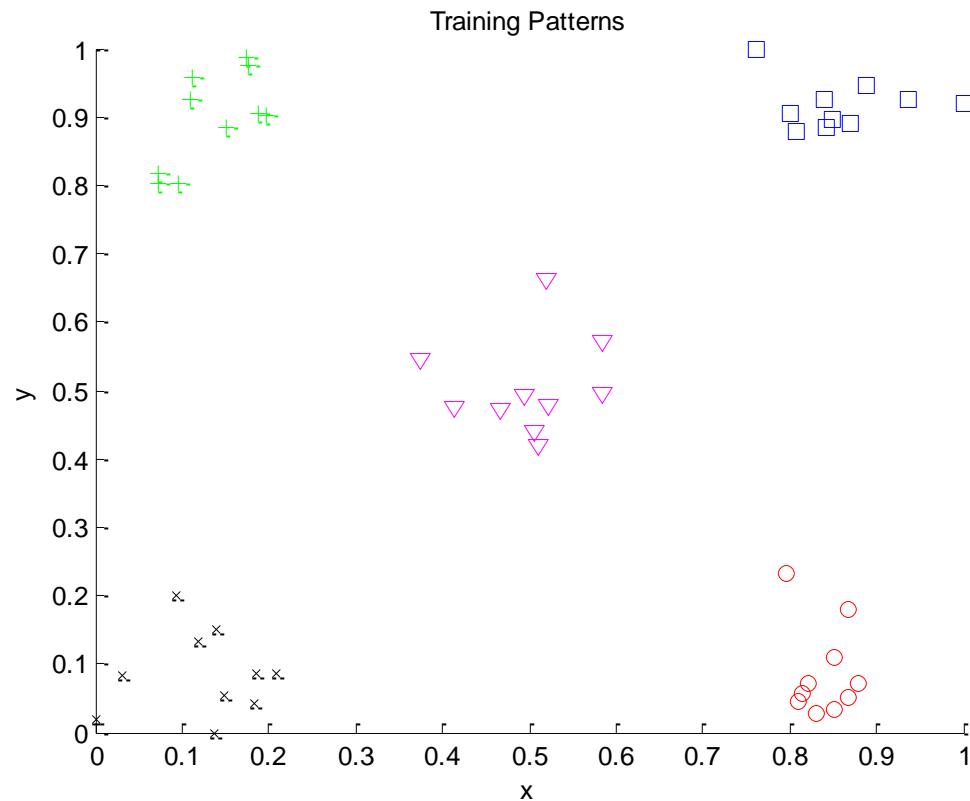
aiNet: Clustering



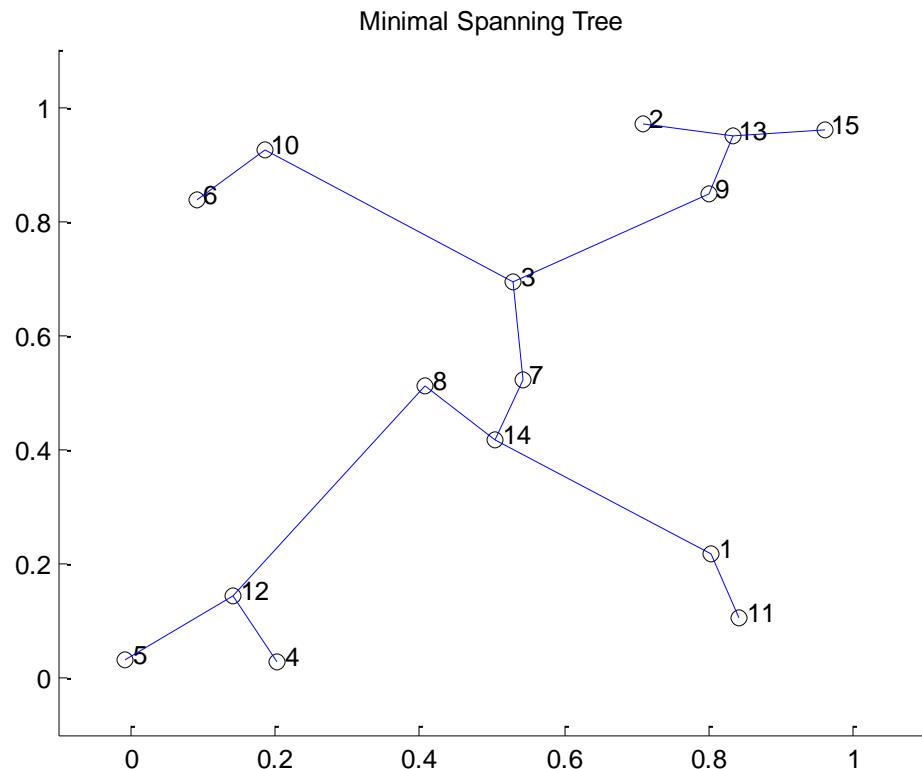
aiNet: Clustering



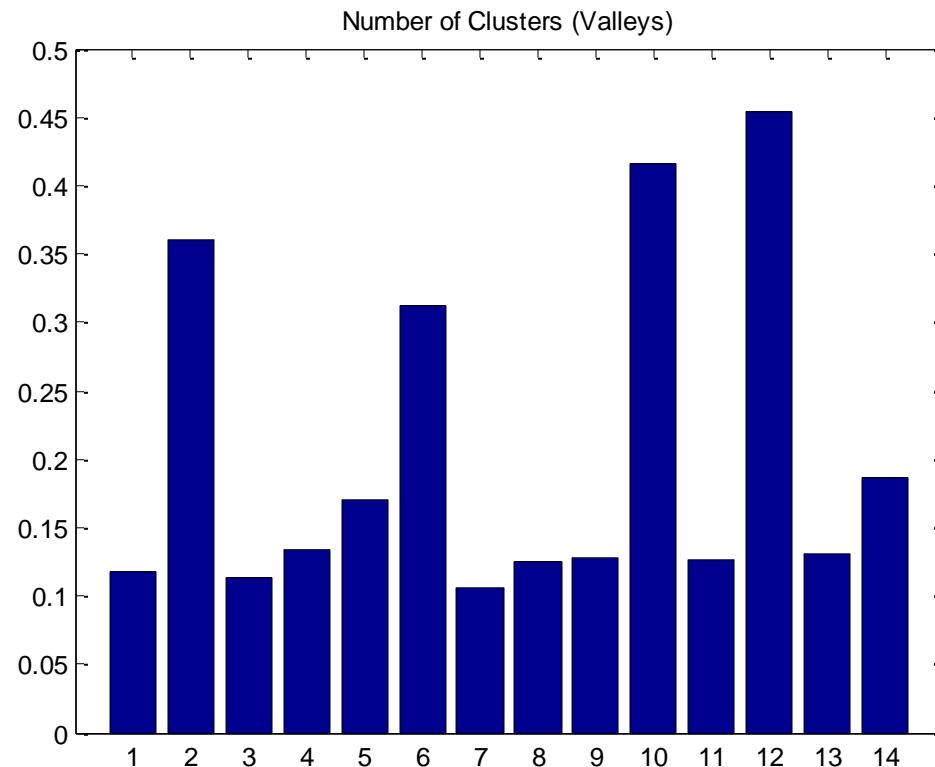
aiNet: Clustering



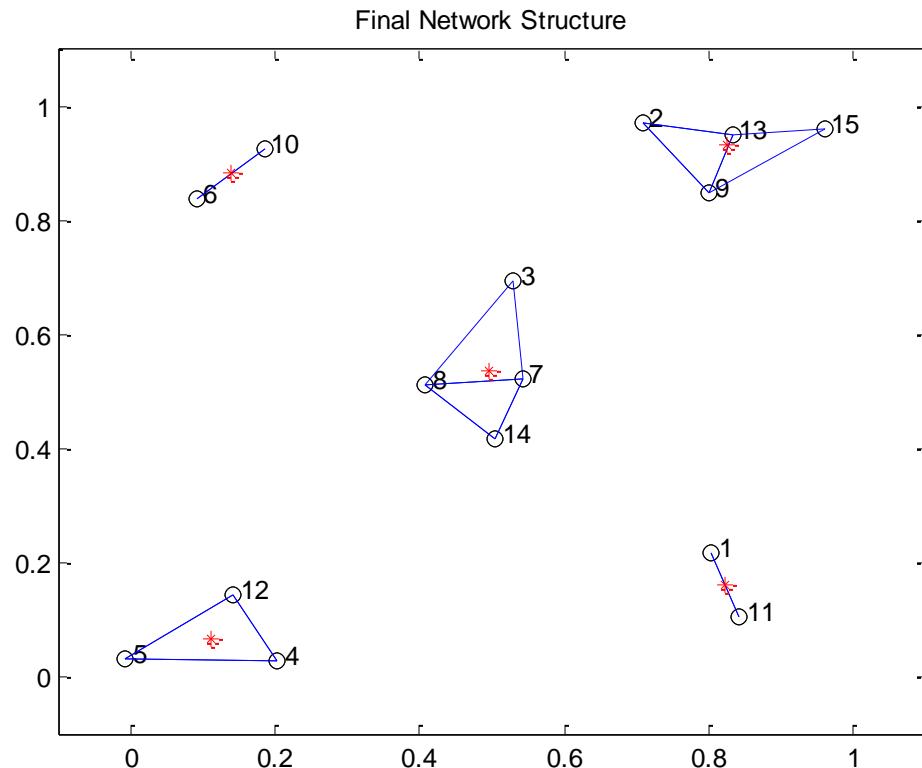
aiNet: Clustering



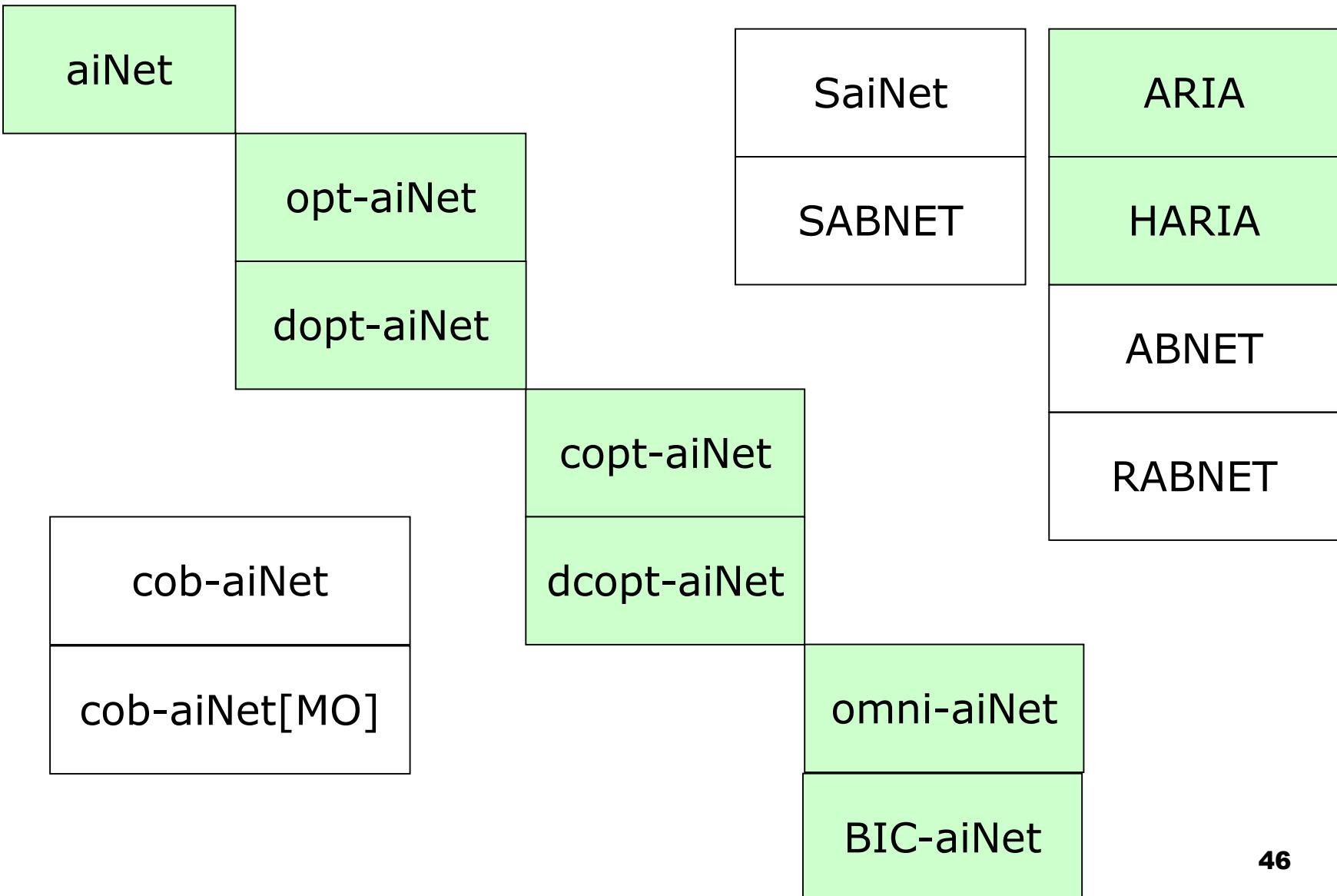
aiNet: Clustering



aiNet: Clustering



aiNet Family

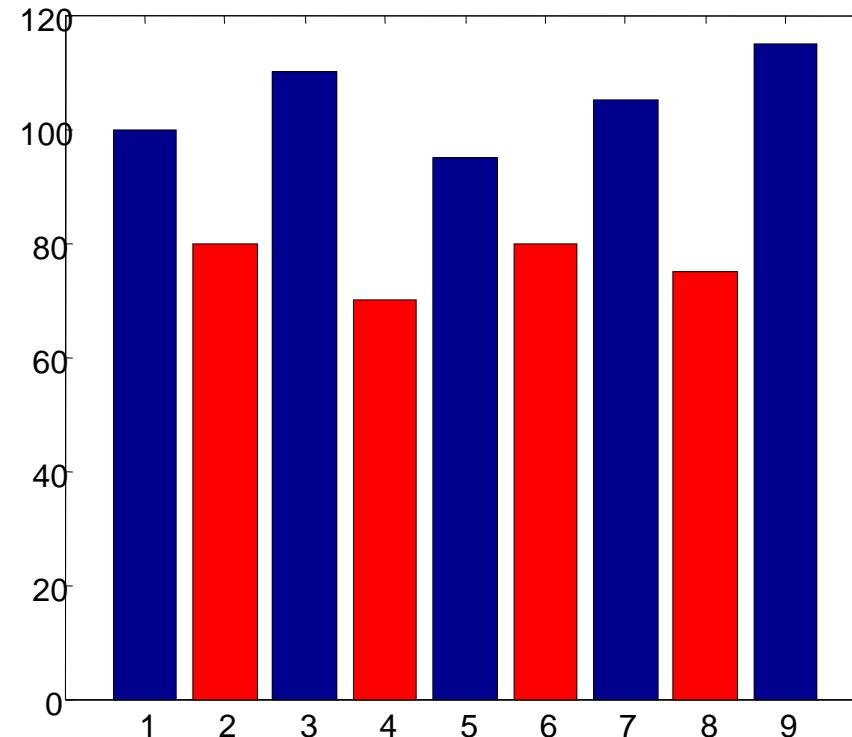


aiNet Family

- **aiNet (CLONALG + network theory)**
 - ✓ Artificial immune network
 - ✓ Application: clustering
- de Castro , L. N. & Von Zuben, F. J., *Learning and Optimization Using the Clonal Selection Principle* , IEEE Transactions on Evolutionary Computation, Special Issue on Artificial Immune Systems, 6 (3), pp. 239-251, 2002.
- de Castro, L.N., Von Zuben, F.J. aiNet: An Artificial Immune Network for Data Analysis. *in* Abbass, H.A., Sarker, R.A. & Newton, C.S. (eds.) *Data Mining: A Heuristic Approach*, Idea Group Publishing, pp. 231-259, 2002.

aiNet Family

A distinctive aspect: the expansion-contraction dynamics of CLONALG

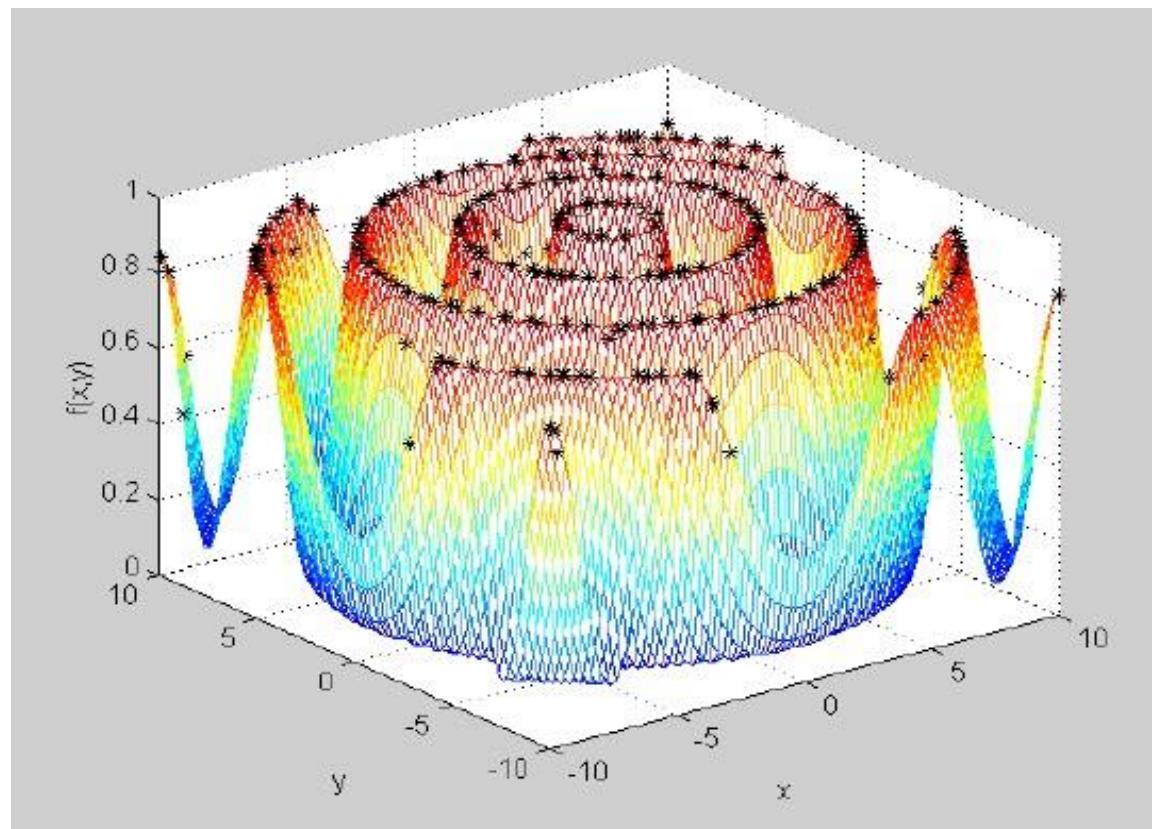


aiNet Family

■ opt-aiNet

- ✓ Artificial immune network for optimization
- ✓ More specifically, multimodal optimization in a continuous space
- de Castro, L. N. and Timmis, J. *An Artificial Immune Network for Multimodal Function Optimization*. Proceedings of the IEEE Congress on Evolutionary Computation (CEC'02), Vol. 1, pp. 699-674, May, Hawaii, 2002.
- Veja slide 27

Multimodal Optimization



Multimodal Optimization

- The purpose is not only to obtain the global optimum, but also high-quality local optima.
 - ✓ Diversity maintenance
 - ✓ Self-adaptation of the population size
 - ✓ Local search
 - ✓ Memory management

aiNet Family

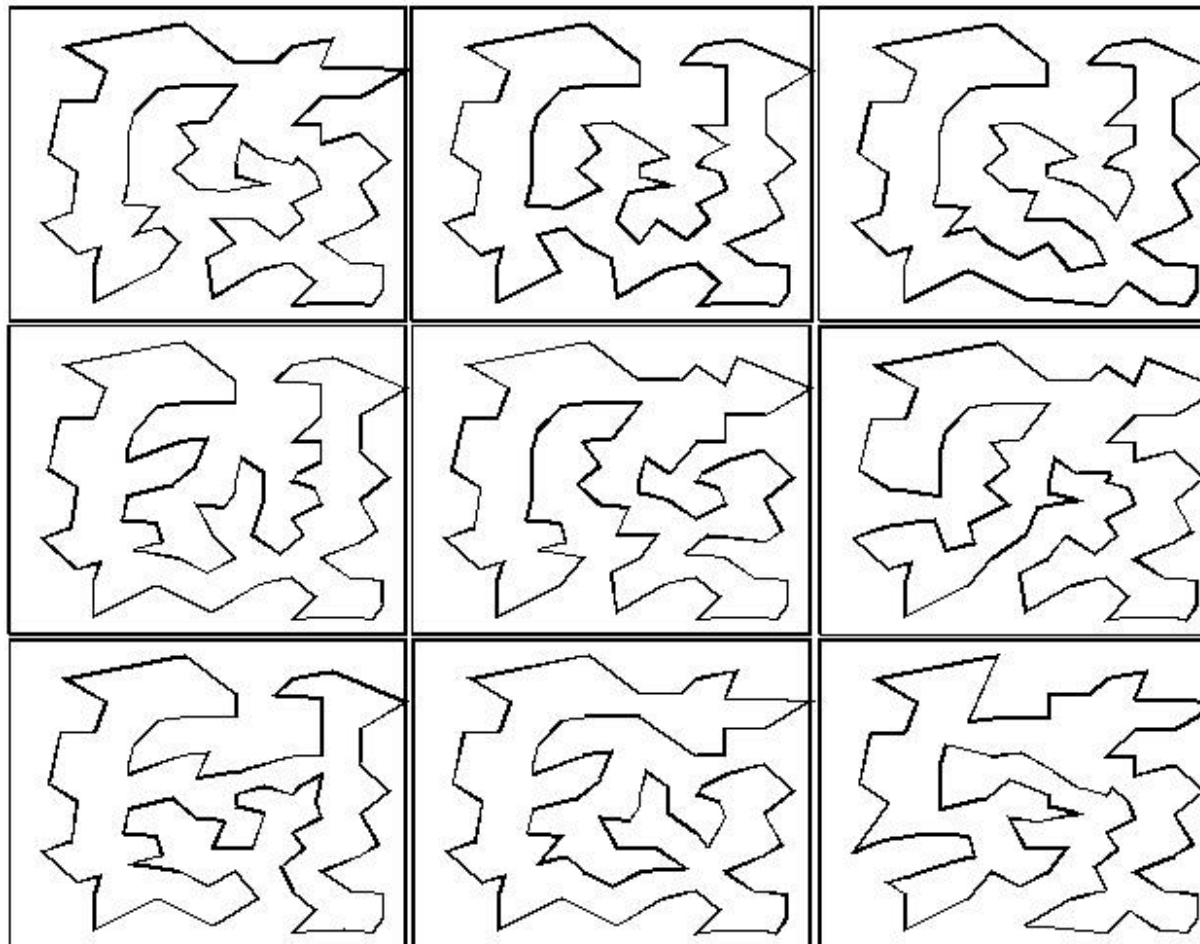
■ copt-aiNet

- ✓ Artificial immune network for combinatorial optimization
- ✓ More specifically, multimodal optimization in a discrete space

Gomes, L.C.T., de Sousa, J.S., Bezerra, G.B., de Castro, L.N., Von Zuben, F.J. Copt-aiNet and the Gene Ordering Problem. Proceedings of the Second Brazilian Workshop on Bioinformatics (WOB'2003), pp. 28-37, 2003.

aiNet Family

- Multimodal search in discrete spaces



TSP: 76 cities

Multimodal Optimization

TSP: 76 cities

Solution	0	1	2	3	4	5	6	7	8	Cost
0	0	17	19	19	14	13	23	15	18	538
1	17	0	14	16	18	17	17	21	27	541
2	19	14	0	17	22	24	17	19	24	542
3	19	16	17	0	21	22	12	13	25	543
4	14	18	22	21	0	13	21	18	24	544
5	13	17	24	22	13	0	27	23	22	546
6	23	17	17	12	21	27	0	19	27	548
7	15	21	19	13	18	23	19	0	24	552
8	18	27	24	25	24	22	27	24	0	553
Cost of the best known solution: 538										

aiNet Family

■ dopt-aiNet

- ✓ Artificial immune network for dynamic optimization
- ✓ More specifically, dynamic optimization in a continuous space
- ✓ Make use of the same search engine

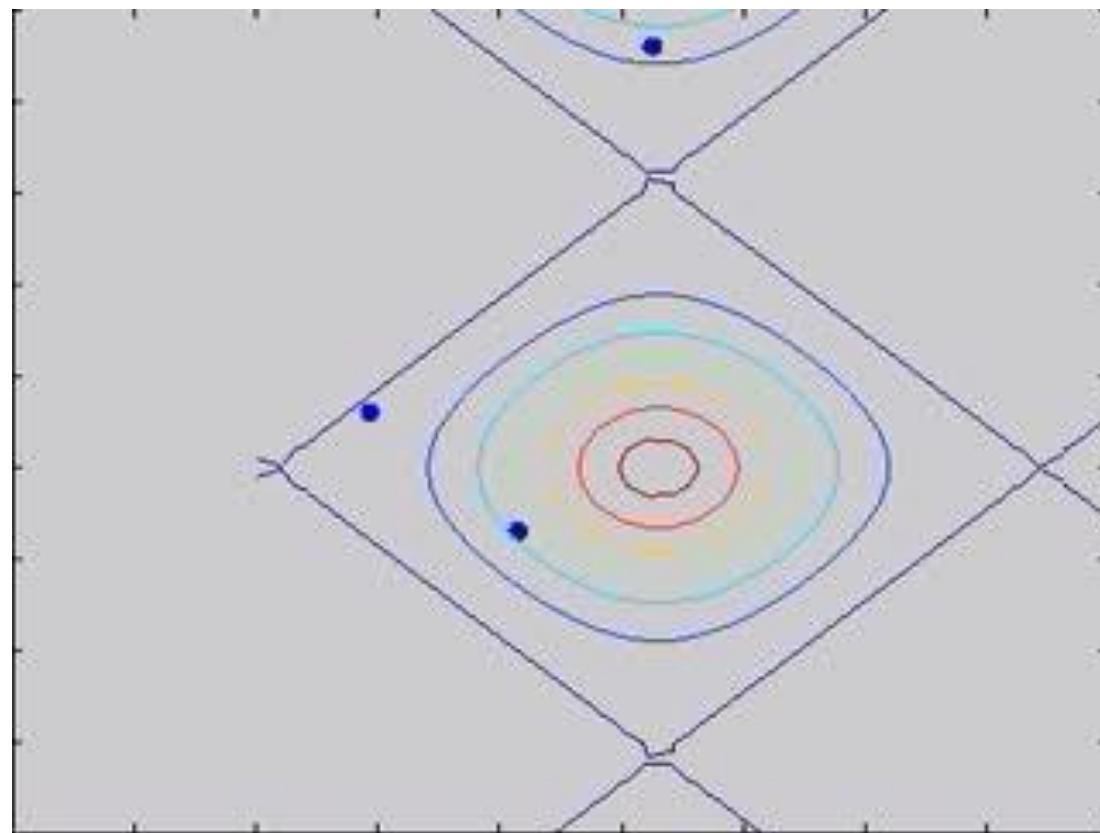
Junqueira, C., de França, F.O., Attux, R.R.F., Panazio, C.M., de Castro, L.N., Von Zuben, F.J., Romano, J.M.T. Immune-inspired Dynamic Optimization for Blind Spatial Equalization in Undermodeled Channels. Proceedings of the IEEE Congress on Evolutionary Computation (CEC'2006), pp. 9801-9808, Vancouver, BC, Canada, July 16-21, 2006.

■ Trabalhos relacionados:

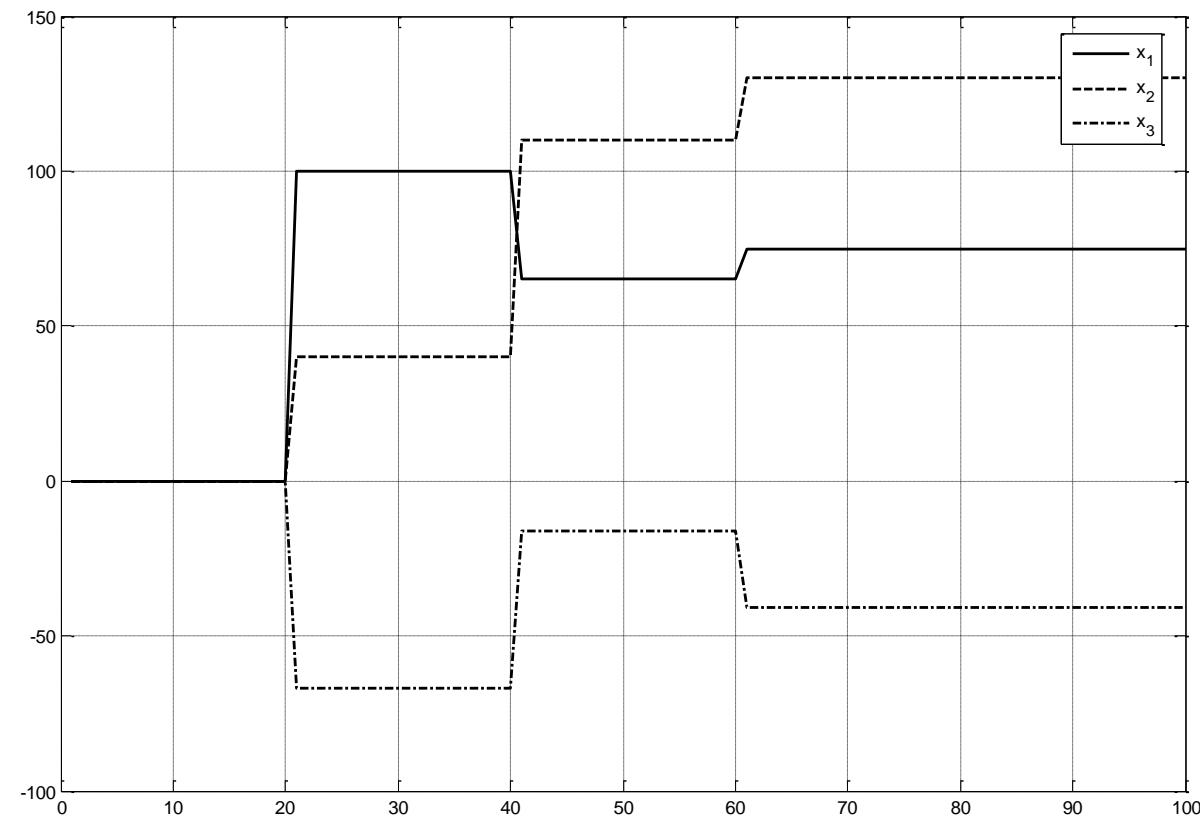
Gaspar, A., Collard, P. *From GAs to Artificial Immune Systems: Improving Adaptation in Time Dependent Optimization*. Proceedings of the Congress on Evolutionary Computation. pp. 1859-1866, Peter J. Angeline and Zbyszek Michalewicz and Marc Schoenauer and Xin Yao and Ali Zalzal (Eds), 1999.

Walker, J., Garrett, S. *Dynamic Function Optimisation: Comparing the Performance of Clonal Selection and Evolutionary Strategies*. Lecture Notes in Computer Science 2787, pp. 273-284. Timmis, J., Bentley, P. and Hart, E.(Eds), 2003.

dopt-aiNet em ação

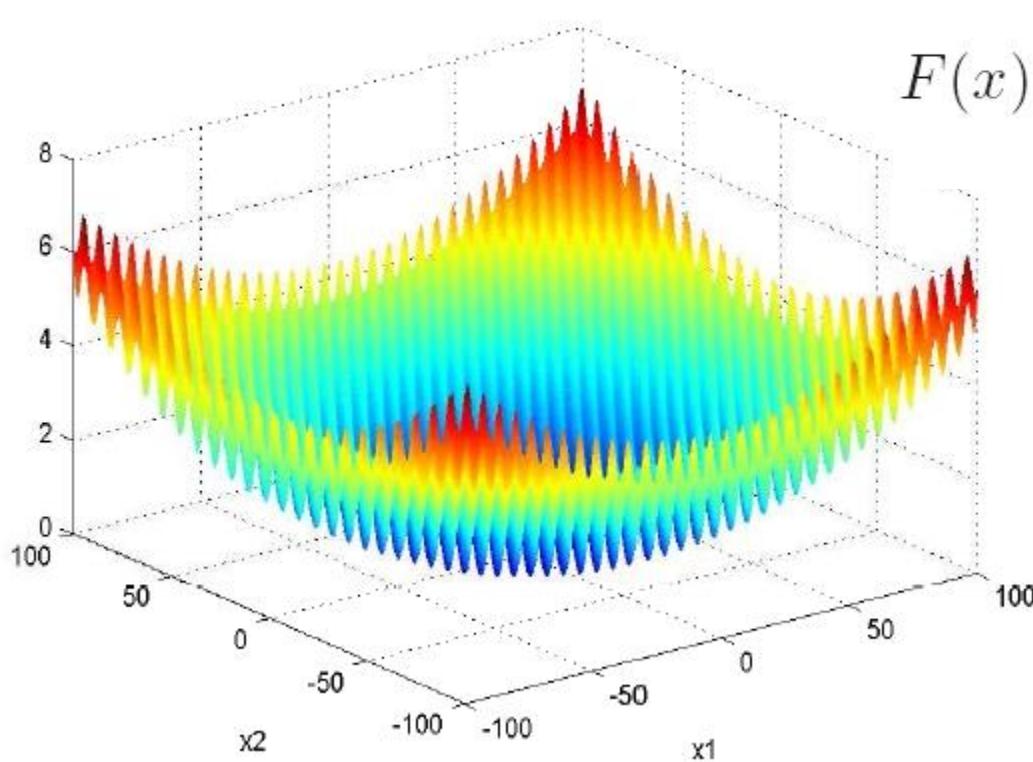


dopt-aiNet: experimento com dinâmicas que variam em degrau



dopt-aiNet: experimento com dinâmicas que variam em degrau

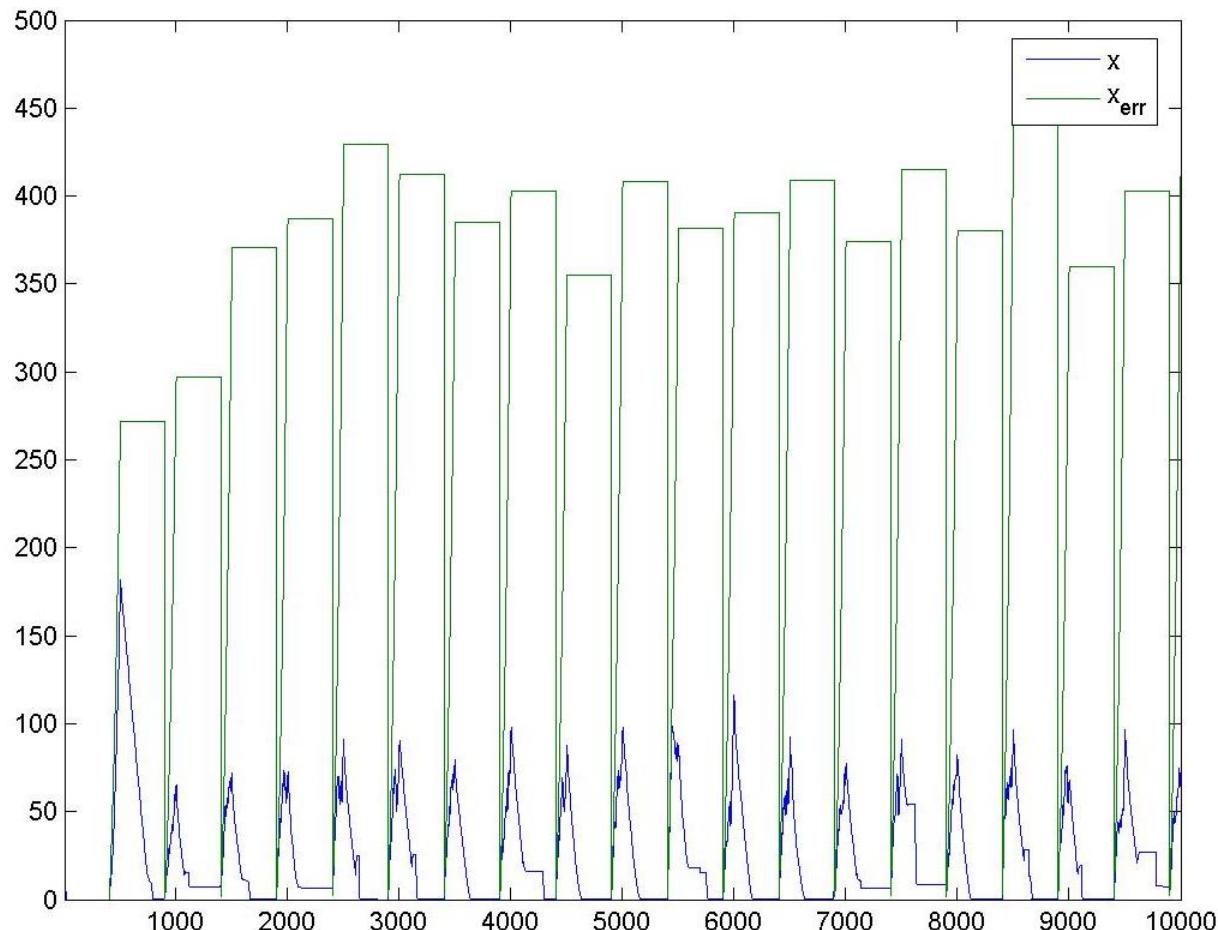
Função Griewank – dimensão $d = 30$



$$F(x) = 1 + \sum_{i=1}^d \frac{x_i^2}{4000} - \prod_{i=1}^d \cos\left(\frac{x_i}{\sqrt{i}}\right)$$

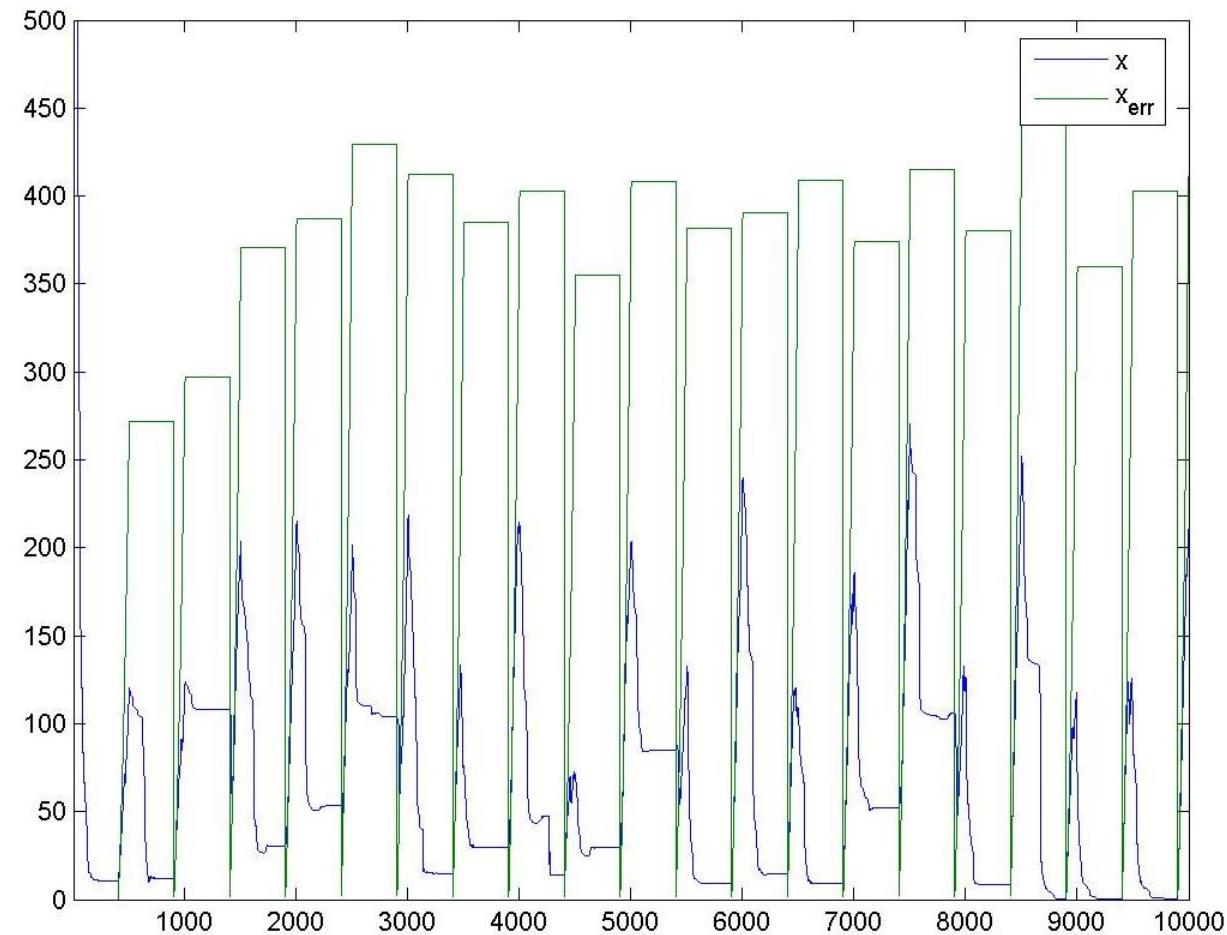
Visualização da função para $d = 2$

dopt-aiNet: experimento com dinâmicas que variam em degrau



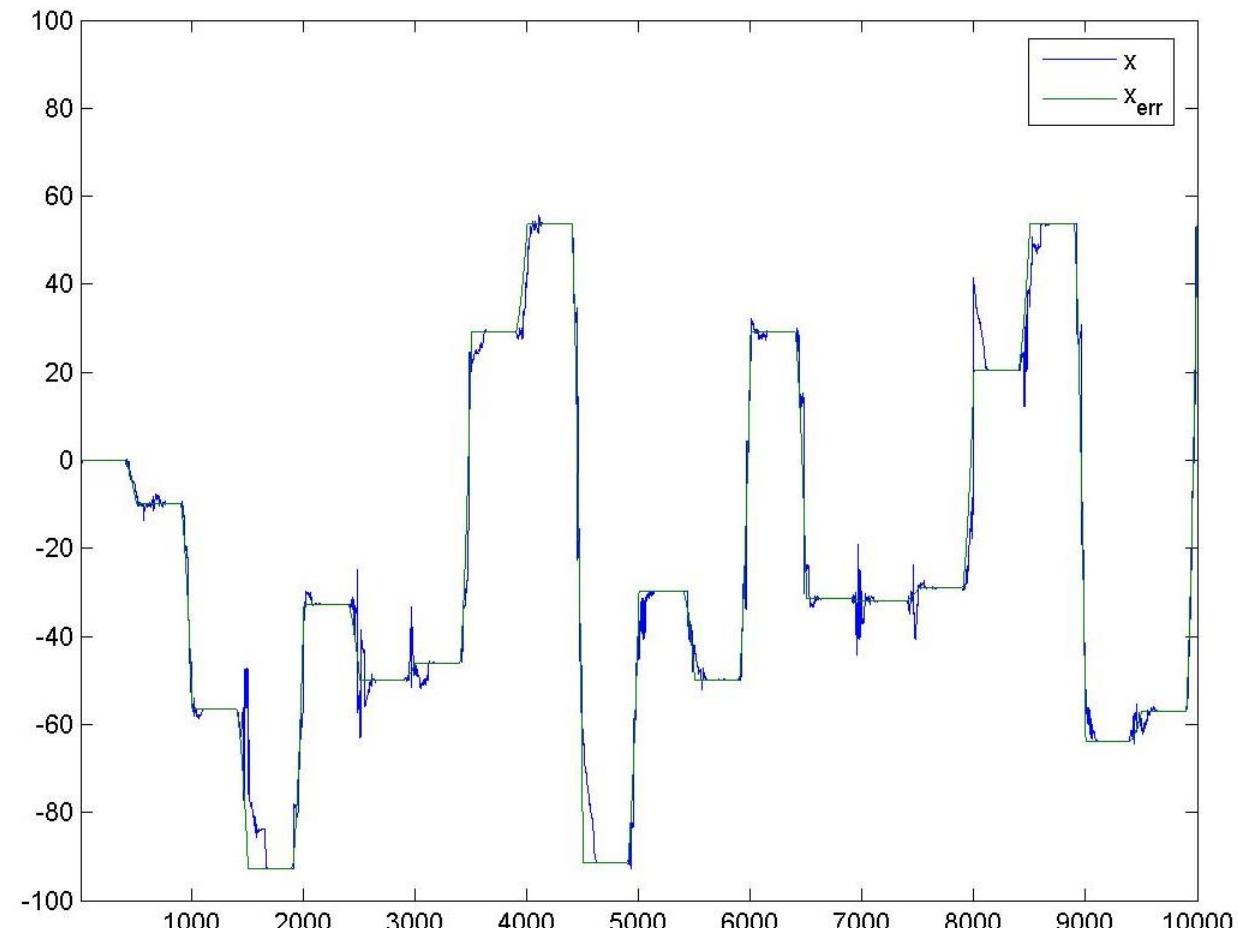
dopt-aiNet: experimento com dinâmicas que variam em degrau

Desempenho de um algoritmo de PSO para o mesmo problema



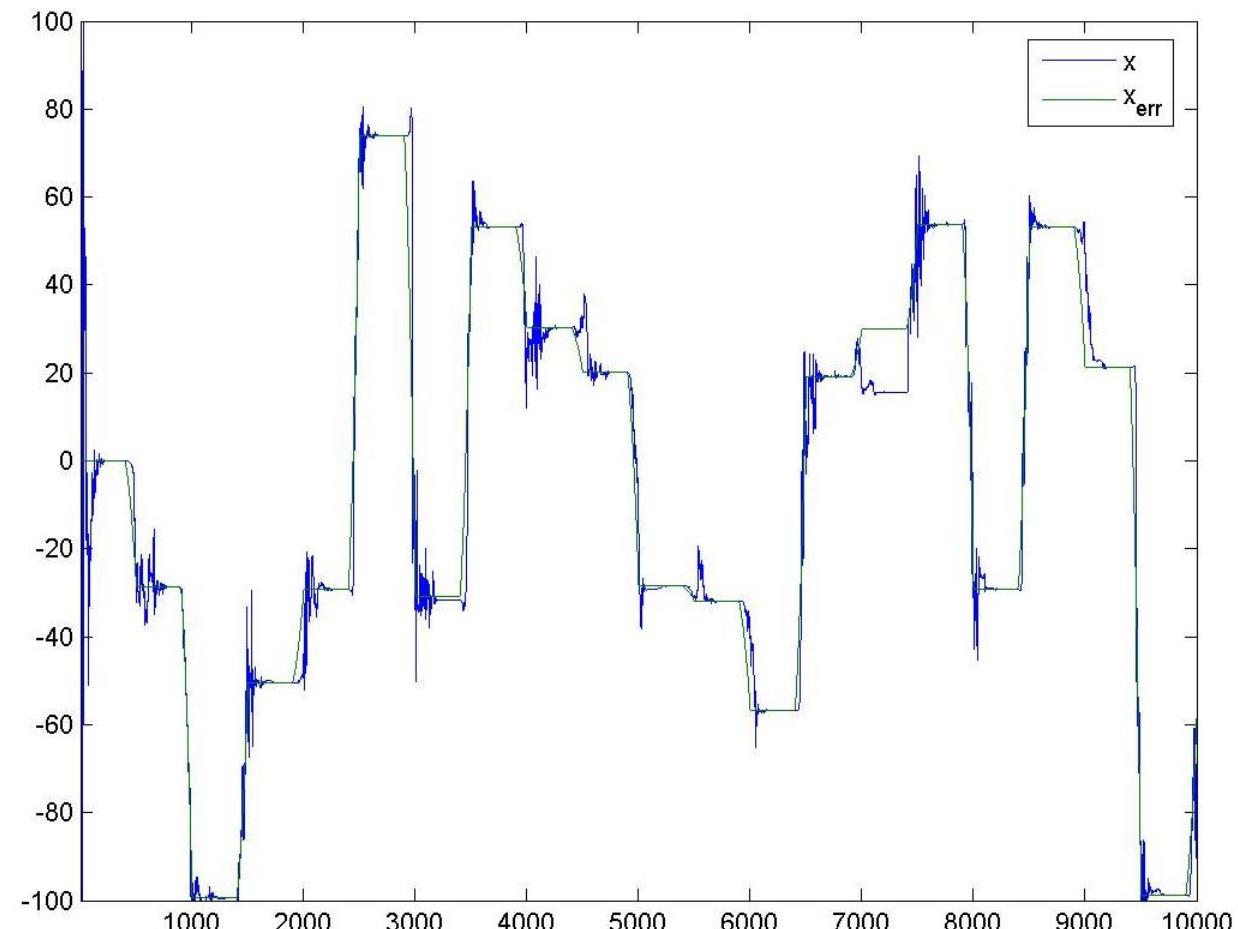
dopt-aiNet: experimento com dinâmicas que variam em degrau

dopt-aiNet –
comportamento da
melhor dentre as
30 variáveis



dopt-aiNet: experimento com dinâmicas que variam em degrau

PSO –
comportamento da
melhor dentre as
30 variáveis



aiNet Family

■ dcopt-aiNet

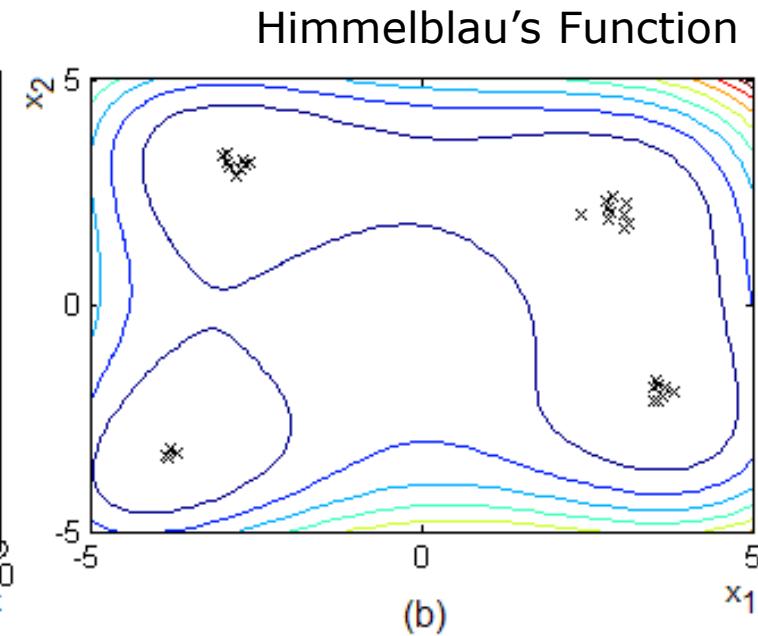
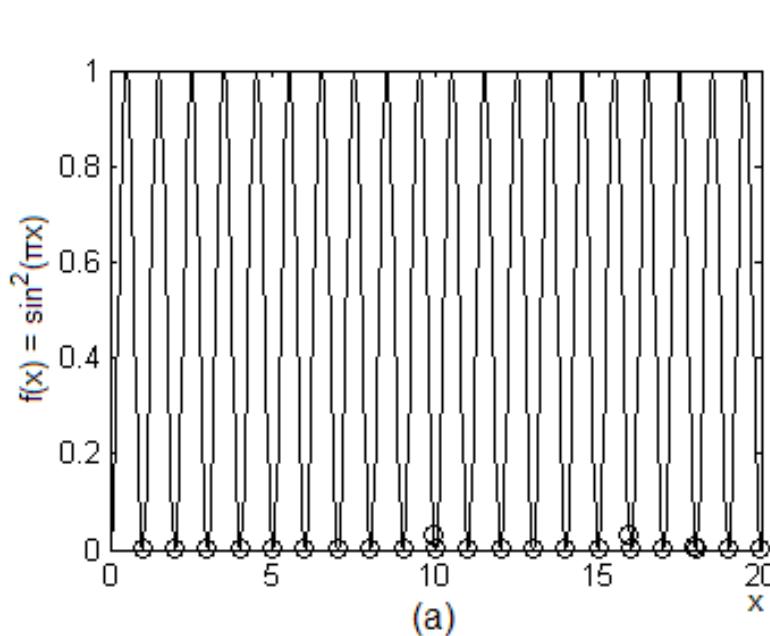
- ✓ Artificial immune network for dynamic optimization
- ✓ More specifically, dynamic optimization in a discrete space
- ✓ Make use of the same search engine

de França, F.O., Gomes, L.C.T., de Castro, L.N., Von Zuben, F.J.
Handling Time-Varying TSP Instances. Proceedings of the IEEE
Congress on Evolutionary Computation (CEC'2006), pp. 9735-9742,
Vancouver, BC, Canada, July 16-21, 2006.

aiNet Family

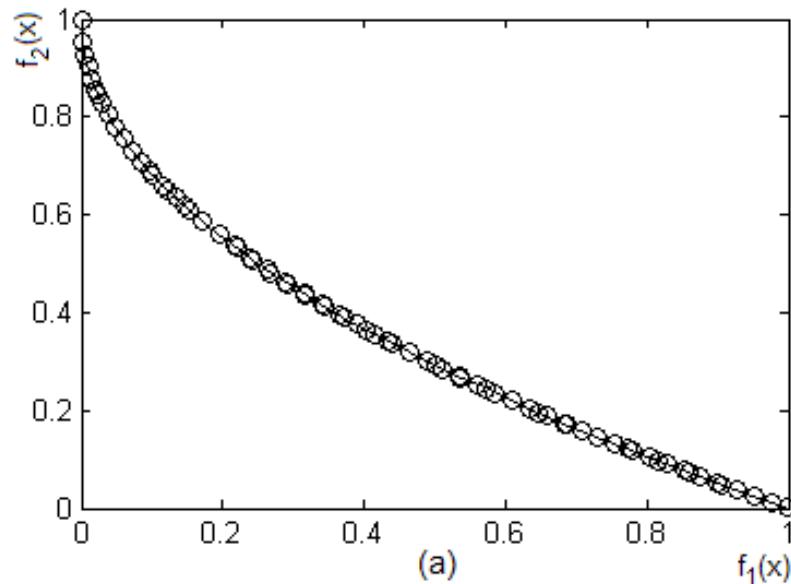
omni-aiNet

Single-Objective, Multi-Global problems:

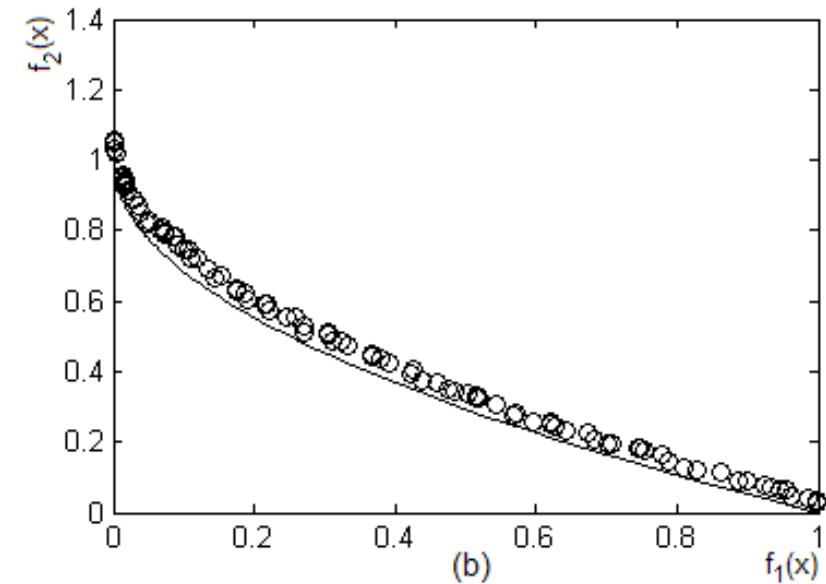


Multi-Objective, Uni-Global problems:

ZDT1 Problem:



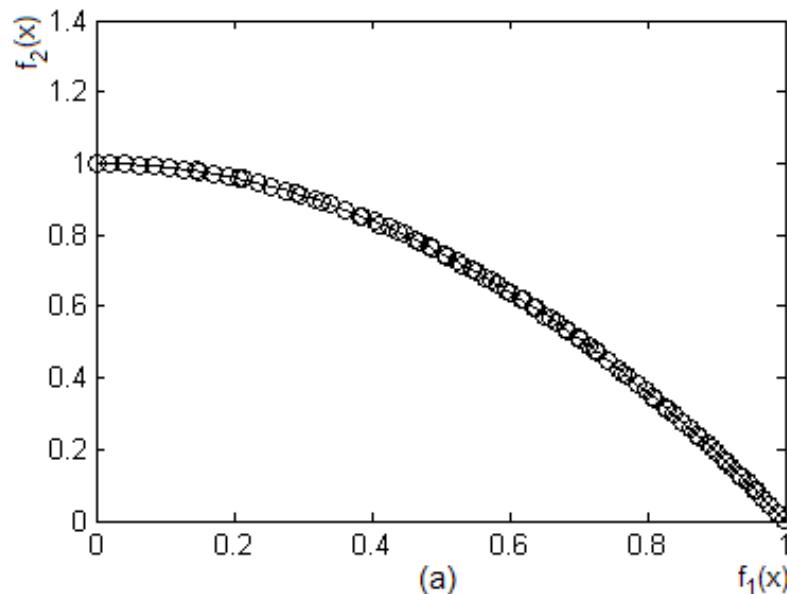
omni-aiNet



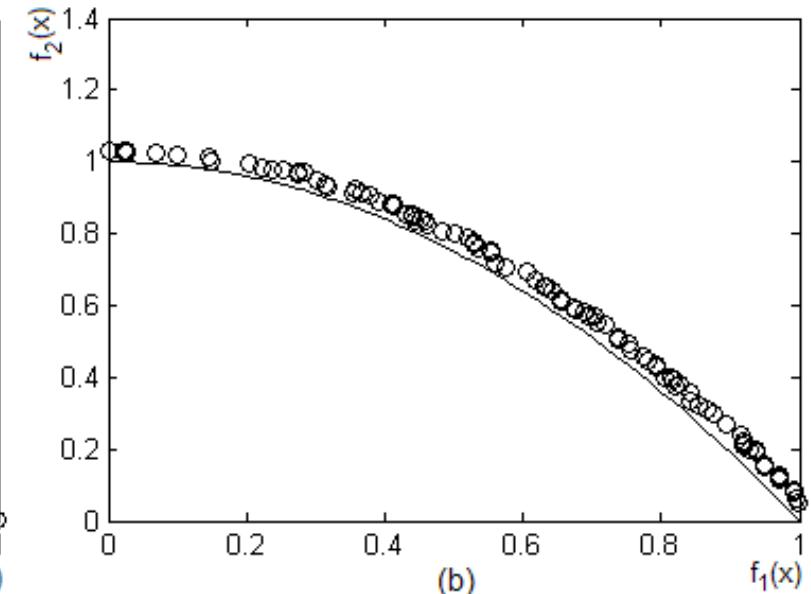
Deb and Tiwari's omni optimizer

Multi-Objective, Uni-Global problems:

ZDT2 Problem:

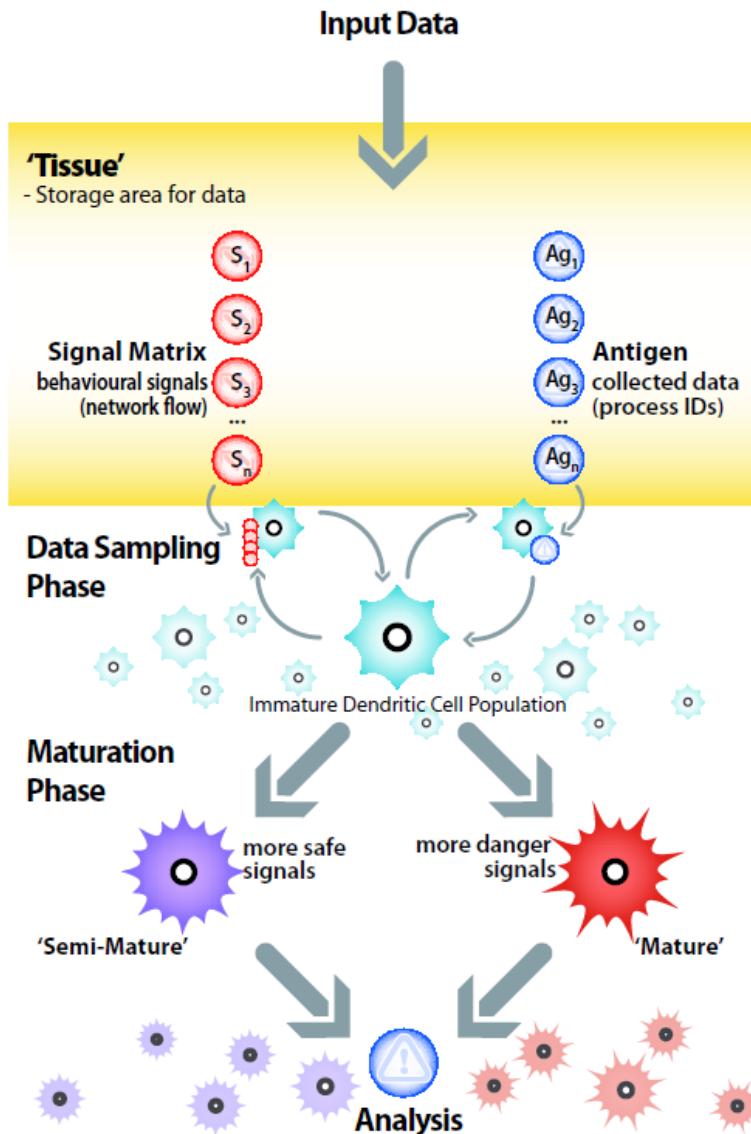


omni-aiNet



Deb and Tiwari's omni optimizer

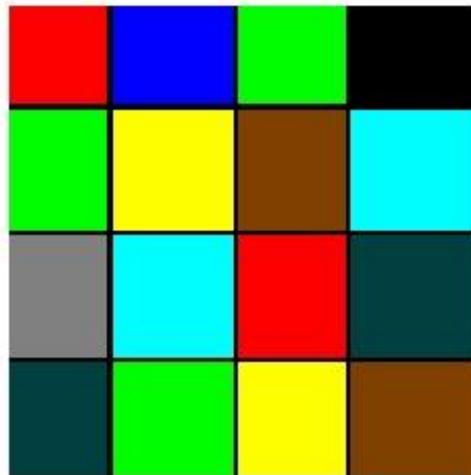
Algoritmo de Célula Dendrítica



Greensmith, 2007

At a cell level, the DC is a signal processing unit, who makes a binary (yes/no) decision as to whether the antigen it has collected during its life span was collected under anomalous conditions. At a population level, the greater DC population is used to perform anomaly detection based on the consensus opinion of the collection of cells.

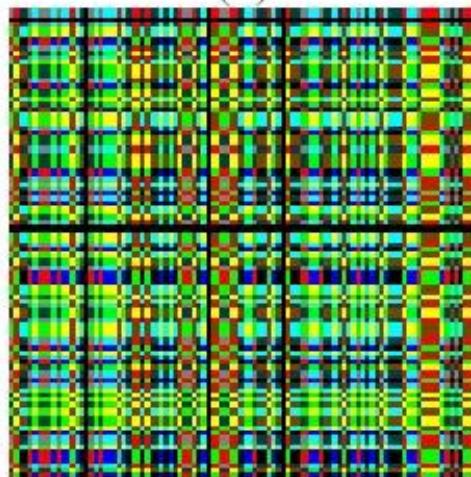
Co-clustering



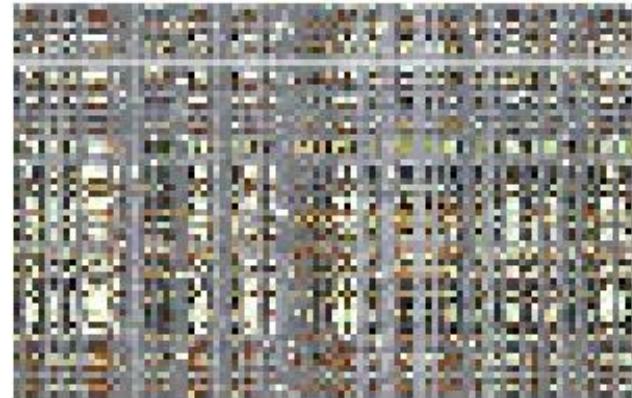
(a)



(b)

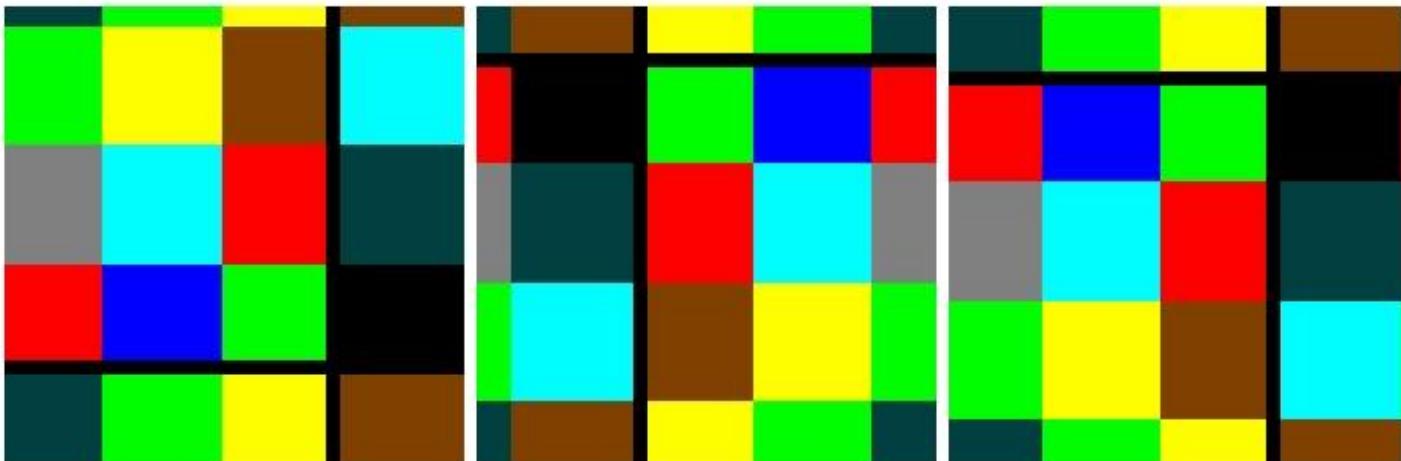


(c)



(d)

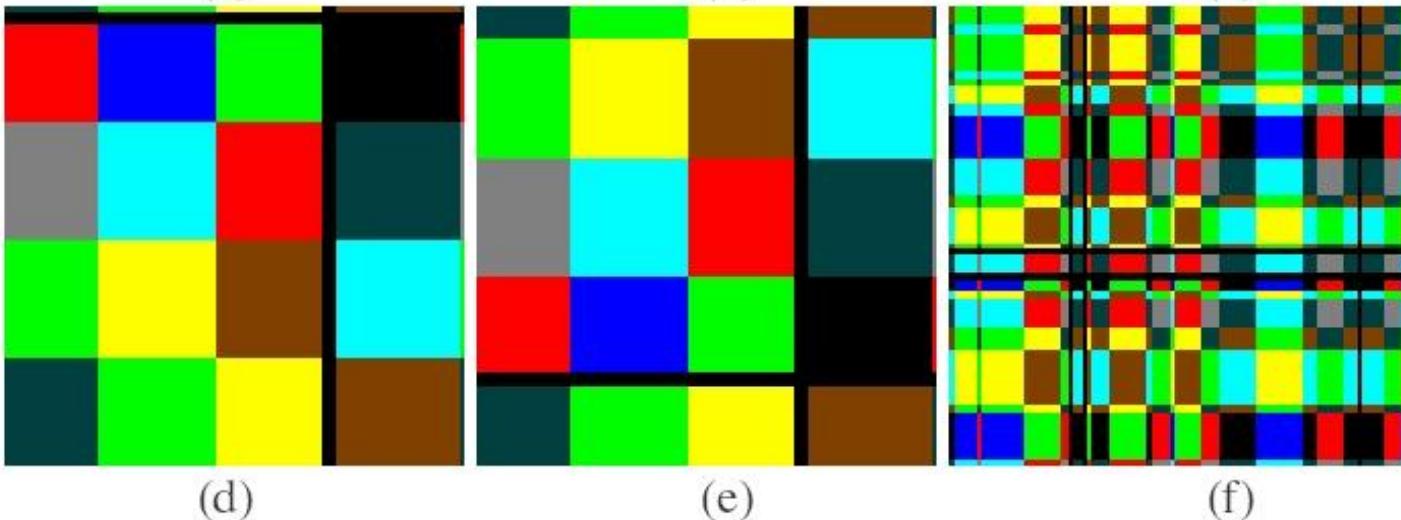
Co-clustering



(a)

(b)

(c)



(d)

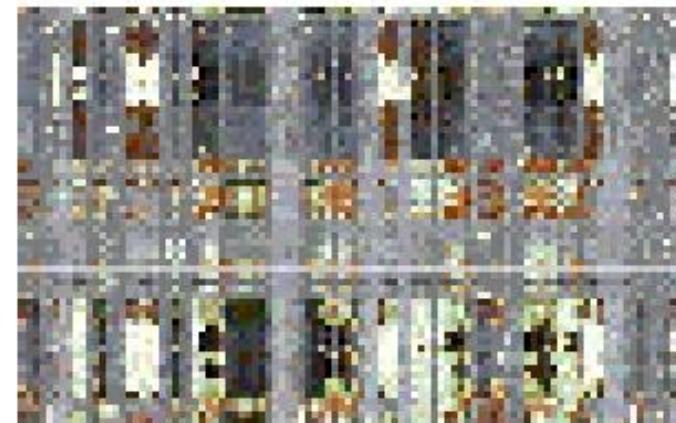
(e)

(f)

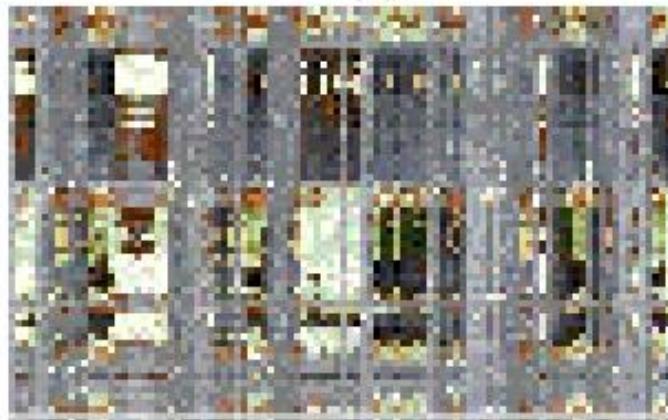
Co-clustering



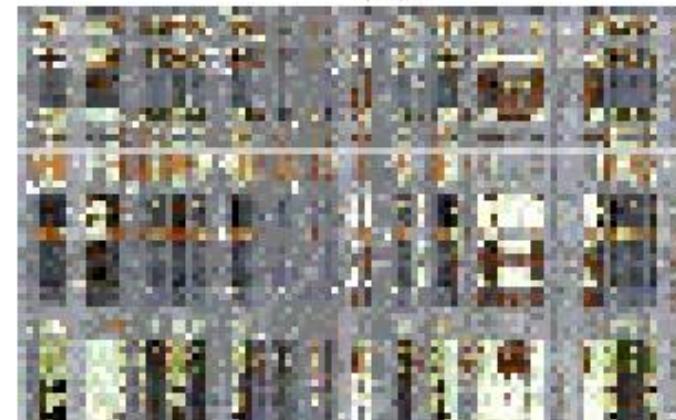
(a)



(b)



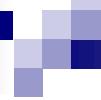
(c)



(d)



Algoritmo de Detecção de Falhas para Sistemas Telefônicos Utilizando a Teoria do Perigo



Baseado em Pinto, J.C.L. (2006) “Algoritmo de Detecção de Falhas para Sistemas Telefônicos Utilizando a Teoria do Perigo”, Tese de Mestrado, FEEC/Unicamp.

Detecção de Falhas

Detecção de Falhas utilizando a Teoria do Perigo

- Aickelin *et al.* (2003): detecção de intrusões pela identificação de alertas apoptóticos e necróticos. Ações tomadas baseando-se no equilíbrio entre esses alertas
- Sarafijanovic & Boudec (2004): detecção de mau funcionamento em redes *ad hoc*. Utilização de um Timo Virtual onde antígenos não relacionados a sinais de perigo geram permanentemente detectores
- Bentley *et al.* (2005): utiliza o paradigma do Tecido. O Tecido é uma camada intermediária que passa pré-infomações de anormalidade ao SIA. Esse então faz o refinamento da detecção

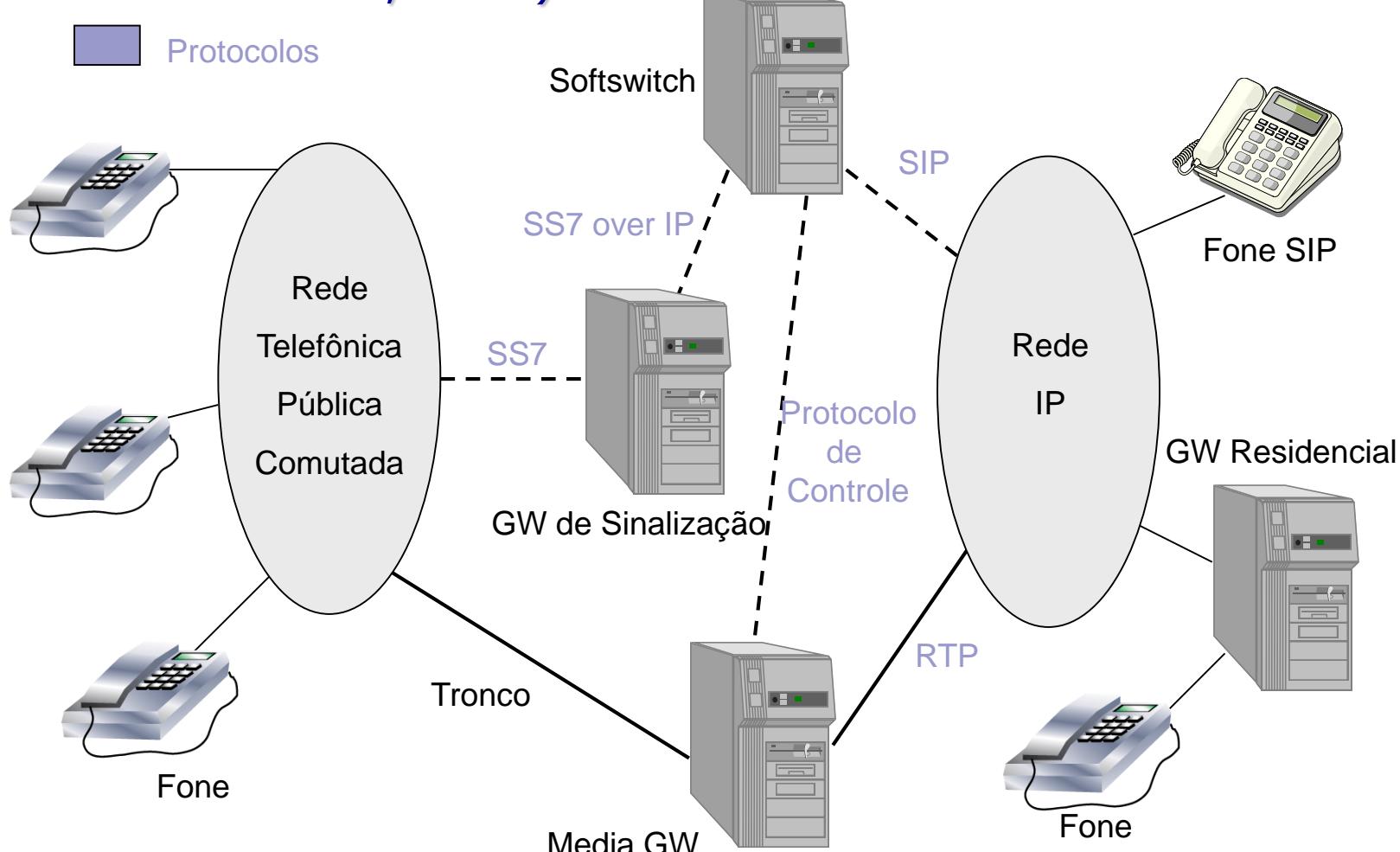
Detecção de Falhas

Detecção de Falhas utilizando a Teoria do Perigo

- Greensmith *et al.* (2005): associa os dados de entrada a sinais que, combinados, possibilitam a geração de células dendríticas maduras ou semi-maduras. As maduras possuem efeito estimulador e as semi-maduras supressor (com relação à proliferação de células T). As citocinas de saída (geradas pelas diferentes células dendríticas, provêem o contexto para a apresentação do antígeno (dado de entrada))
- Kim *et al.* (2005): algoritmo de defesa computacional baseado em Bentley *et al.* (2005) e Greensmith *et al.* (2005)

Sistemas Telefônicos

Rede Telefônica Híbrida (Faynberg et al., 2000;
Hersent & Petit, 1999)



Sistemas Telefônicos

Informações Comuns a Chamadas Telefônicas

- Endereço de Origem
- Endereço de Destino
- Tempo de Duração da Chamada
- Informação sobre funcionalidades específicas
(associadas ao tipo de serviço)

Sistemas Telefônicos

Perigo nas Redes Telefônicas

- Perigo Constitutivo: mudança abrupta de perfil das chamadas finalizadas (células mortas). Por exemplo, taxa elevada de chamadas com duração próxima de zero e com status de finalização genérico.
- Perigo Induzível: mudança do procedimento padrão ao longo das chamadas (estresse celular). Por exemplo, mudanças excessivas de rota e de recursos utilizados no estabelecimento da chamada.

O Algoritmo de Detecção de Falhas Baseado na Teoria do Perigo

Analogia entre o SIH e o Sistema de Detecção Proposto

Célula normal	Chamada telefônica dentro do padrão de normalidade da rede telefônica
Antígeno	Chamada telefônica fora do padrão de normalidade da rede telefônica
Linfócito T /B	Detector
APC	Módulo verificador de perigo (alarme)
Morte apoptótica	Terminação normal de chamada
Morte necrótica / sinal 0	Terminação anormal de chamada
Sinal 1 (estímulo)	Identificação de antígeno pela população de detectores

O Algoritmo de Detecção de Falhas Baseado na Teoria do Perigo

Princípio Geral do Algoritmo

- Uma chamada telefônica é tida como falha toda vez que um detector reconhecê-la e receber a confirmação, ou já possuir a informação, de que algum perigo está ocorrendo
- Chamadas reconhecidas por detectores que não possuem a informação de ocorrência de perigo são consideradas normais
- Chamadas não reconhecidas pelos detectores são sempre consideradas normais

O Algoritmo de Detecção de Falhas Baseado na Teoria do Perigo

Afinidade entre Detectores e Tentativas de Chamadas

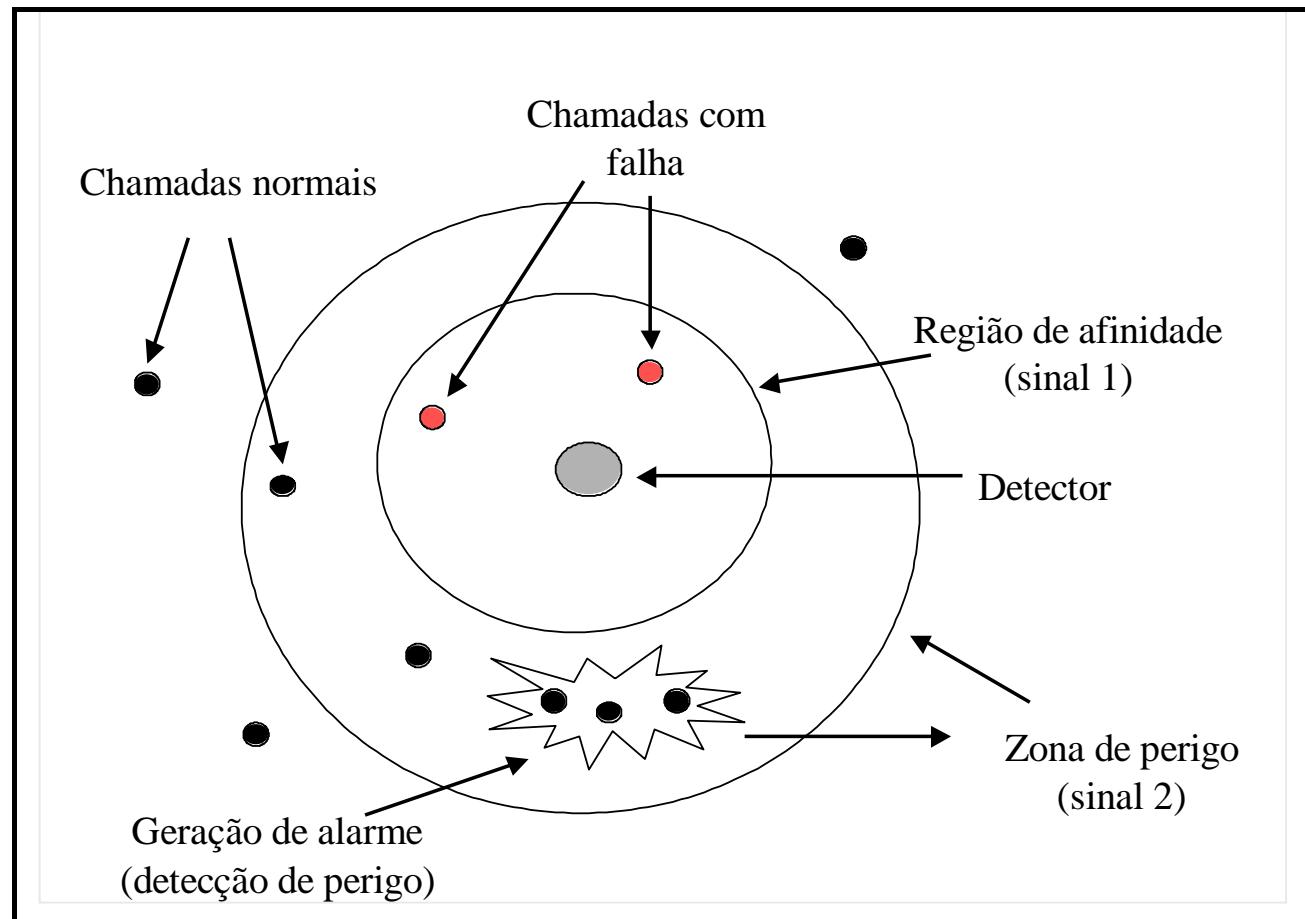
- Atributos verificados: numéricos (*origem, destino, duração*) e nominal (*característica*)
- Utilização de função híbrida (*Heterogeneous Euclidian-Overlap Metric*) (Wilson & Martinez, 1997):

$$d_i = \begin{cases} 1 & \text{se } Dt_i \text{ ou } Ag_i \text{ são desconhecidos, senão} \\ D_H & \text{se } i \text{ é nominal, senão} \\ dif_norm_i & \end{cases}$$

$$dif_norm_i = \frac{|Dt_i - Ag_i|}{\max_i - \min_i} \quad D_{HEOM} = \sqrt{\sum_{i=1}^L d_i^2}$$

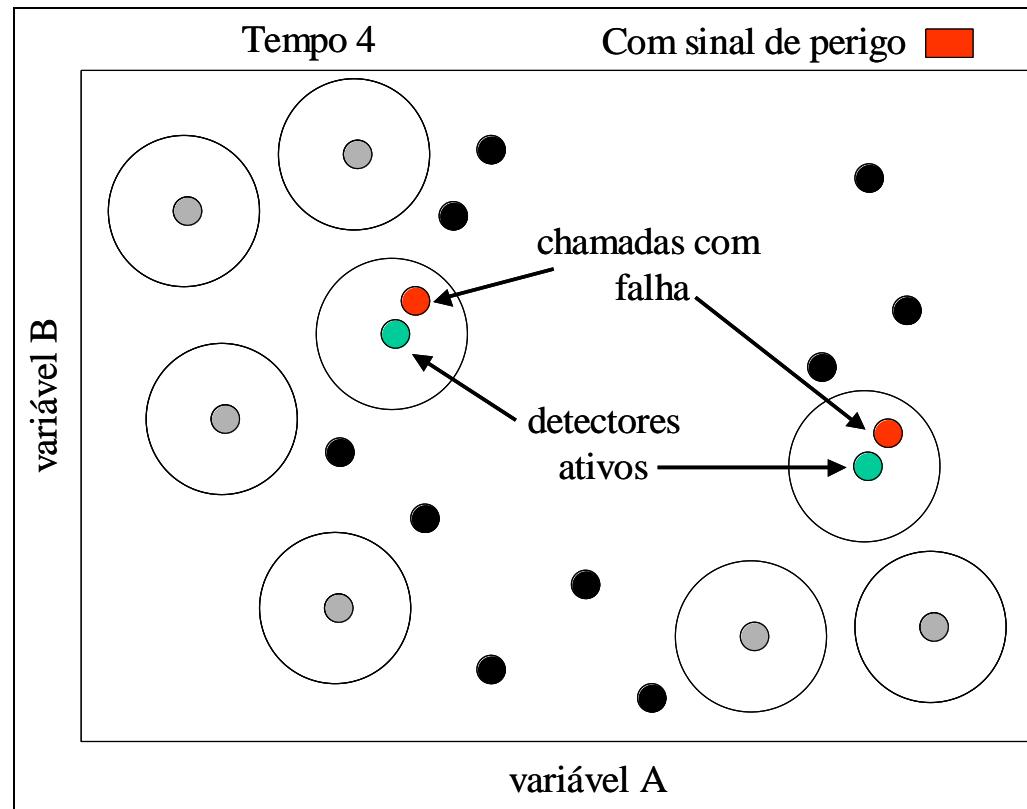
O Algoritmo de Detecção de Falhas Baseado na Teoria do Perigo

Comportamento de um Detector na Presença de Chamadas



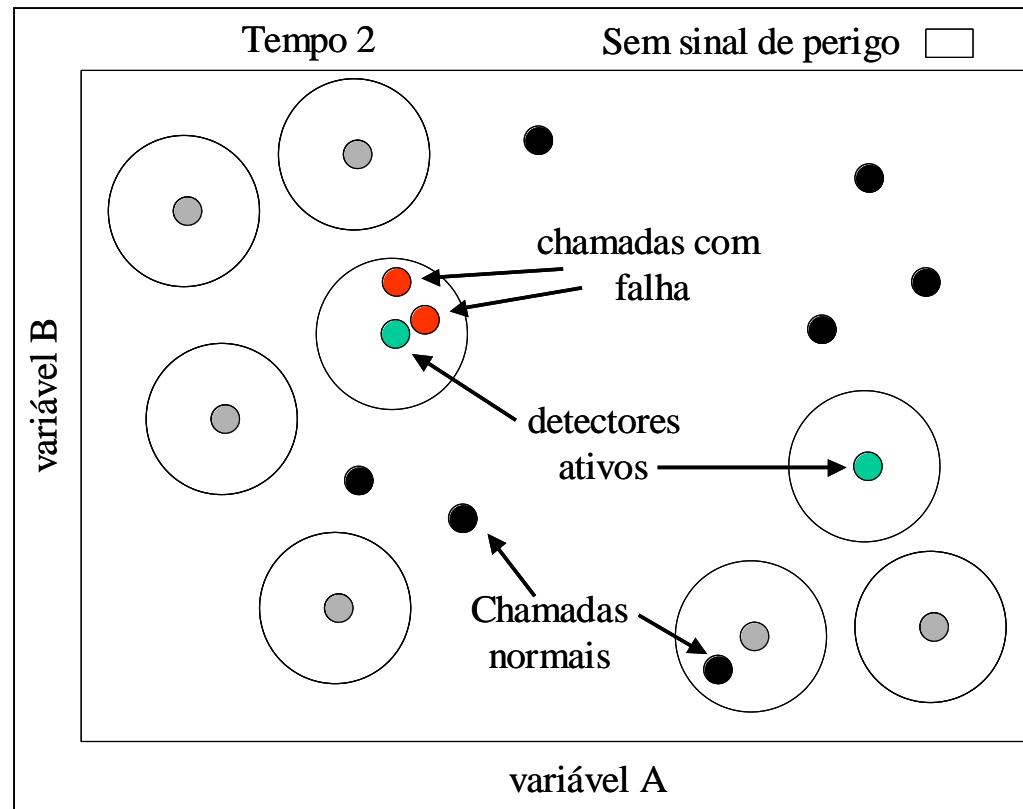
O Algoritmo de Detecção de Falhas Baseado na Teoria do Perigo

Sequência de Chamadas no Processo de Detecção



O Algoritmo de Detecção de Falhas Baseado na Teoria do Perigo

Detecção de Falha Fora da Zona de Perigo por um Detector Ativo



O Algoritmo de Detecção de Falhas Baseado na Teoria do Perigo

Morte de Detectores

- Detector deve ser eliminado caso receba um sinal 1 sem a ocorrência de um sinal 2

Desativação de Detectores

- Após um período de tempo T_{At} decorrido, um detector ativo se torna inativo

Votação

- Como forma de aumentar a confiabilidade no diagnóstico do algoritmo são utilizados processos que devem ser executados em paralelo. Uma tentativa de chamada é considerada falha caso um determinado percentual dos processos considere aquela tentativa de chamada como falha

O Algoritmo de Detecção de Falhas Baseado na Teoria do Perigo

Algoritmo

- Geração randômica de detectores
- Caso se receba o sinal 1 sem o sinal 2, o(s) detector(es) é/são eliminado(s) (seleção negativa)
- Caso seja necessário, geram-se novos detectores para cobrir o espaço de defesa (utilizando clonagem com hipermutação de forma similar ao CLONALG (de Castro & Von Zuben, 2002))
- Caso se recebam os sinais 1 e 2, o(s) detector(es) é/são ativado(s)
- Após um intervalo de tempo T_{At} , um detector ativo se torna inativo
- Um detector ativo detecta perigo com a presença do sinal 1 sem a necessidade do sinal 2
- Um sinal 2 recebido sem um sinal 1 é ignorado

O Algoritmo de Detecção de Falhas Baseado na Teoria do Perigo

Algoritmo (variáveis)

- D : distância entre dois elementos (detectores e antígenos)
- $Laff$: limiar de afinidade (região de reconhecimento ao redor do detector)
- $Caff$: contador de afinidade (verifica a quantidade de vezes que o sinal 1 é disparado)
- $LCaff$: limiar para ativação do detector
- $LCelim$: limiar para eliminação do detector
- NAg : quantidade máxima de antígenos da população de antígenos

O Algoritmo de Detecção de Falhas Baseado na Teoria do Perigo

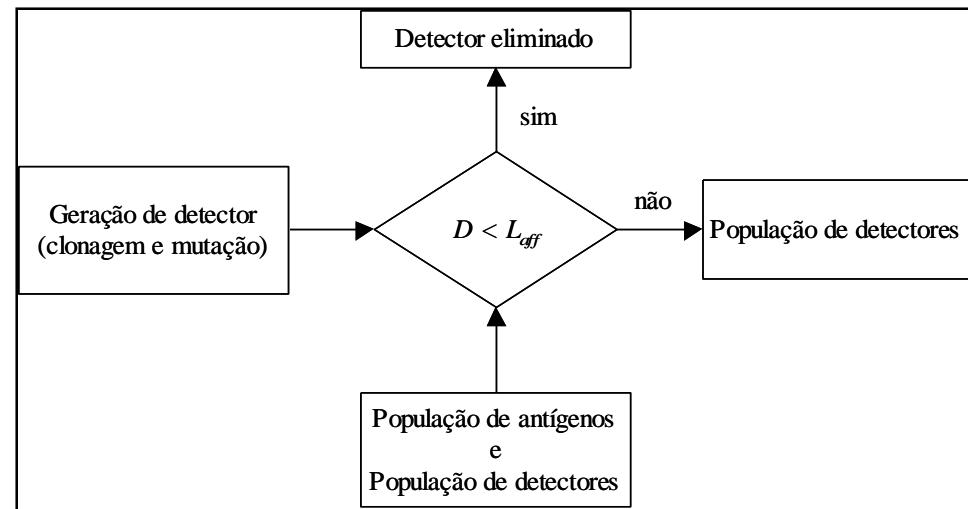
Algoritmo (variáveis)

- td : período de tempo após a ocorrência do sinal 1 para que, pela ocorrência do sinal 2, o detector seja ativado
- t_{s2} : tempo de disparo do sinal 2 ou detecção de falha
- T_{At} : limiar de tempo para a desativação do detector
- t : tempo da tentativa de chamada
- NC : taxa de não completamento de chamadas
- L_{NC} : limiar para taxa de não completamento de chamadas

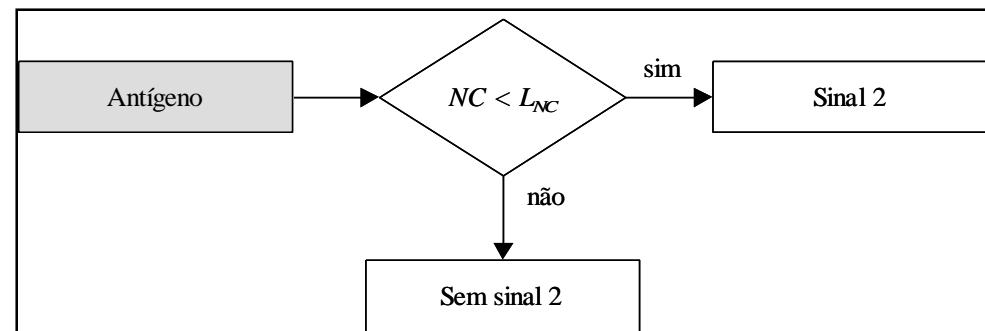
O Algoritmo de Detecção de Falhas Baseado na Teoria do Perigo

Algoritmo (fluxo)

- geração de novos detectores ao longo do tempo



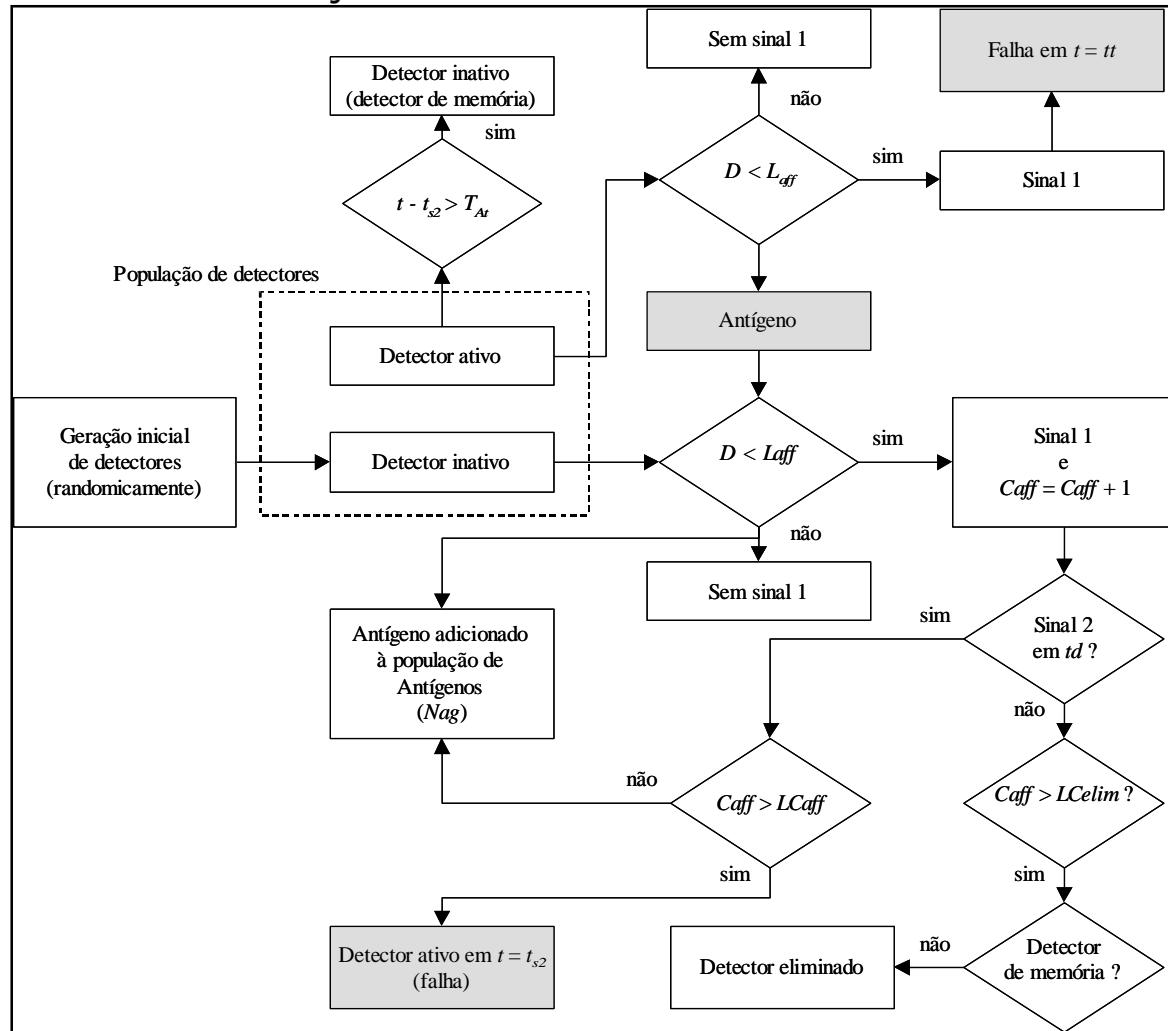
- geração de alarme (sinal 2)



O Algoritmo de Detecção de Falhas Baseado na Teoria do Perigo

Algoritmo (fluxo)

- Visão geral do algoritmo mostrando o procedimento de ativação de detectores e detecção de falhas em cada tentativa de chamada



Resultados Obtidos

Intervalos de Valores para os Atributos de Chamada

- *Origem*: 0 – 11 (índices dos nós na rede telefônica)
- *Destino*: 0 – 11 (índices dos nós na rede telefônica)
- *Duração*: 0 – 359 (em segundos)
- *Funcionalidade*: 0 – 3 (admite quatro tipos diferentes de chamadas)

Resultados Obtidos

Parâmetros do Algoritmo

- limiar para ativação do detector (*Act*): 3 tentativas de chamadas
- limiar para eliminação do detector (*LCelim*): 3 tentativas de chamadas
- quantidade máxima de抗ígenos da população de抗ígenos (*N_{Ag}*): 50抗ígenos
- limiar de tempo para desativação do detector ativo (*TAt*): 60 tentativas de chamadas (o tempo médio de 60 tentativas de chamadas)
- limiar para taxa de não completamento de chamada (*LNC*): 3 tentativas de chamadas

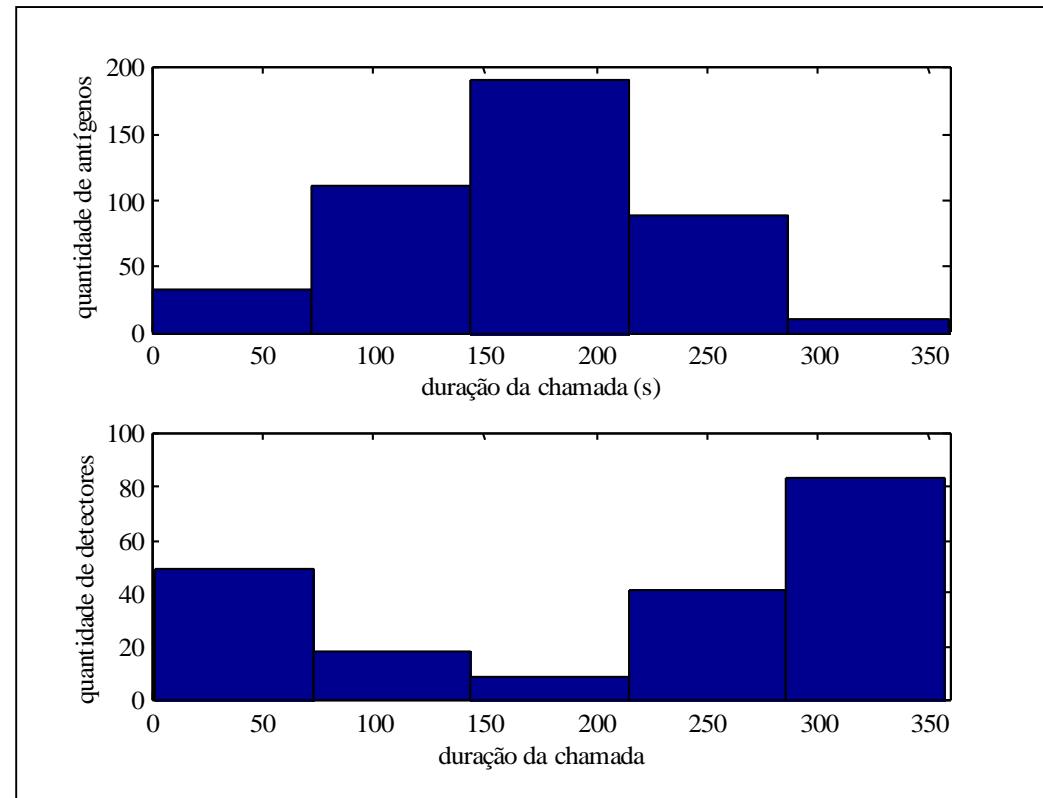
Resultados Obtidos

Características Gerais das Chamadas Geradas

- Foram geradas 500 chamadas
- Variáveis *origem*, *destino* e *funcionalidade* com distribuição linear
- Variável *duração*:
 - No intervalo de chamadas de 1 a 70: distribuição assimétrica enviesada para a direita com média 70 segundos
 - No intervalo de chamadas de 71 a 500: distribuição simétrica centrada em 180 segundos
- Situação de falha após a chamada 400: toda chamada gerada nas origens 1 a 6 utilizando a funcionalidade 2 não foram completadas (duração igual a 0)

Resultados Obtidos

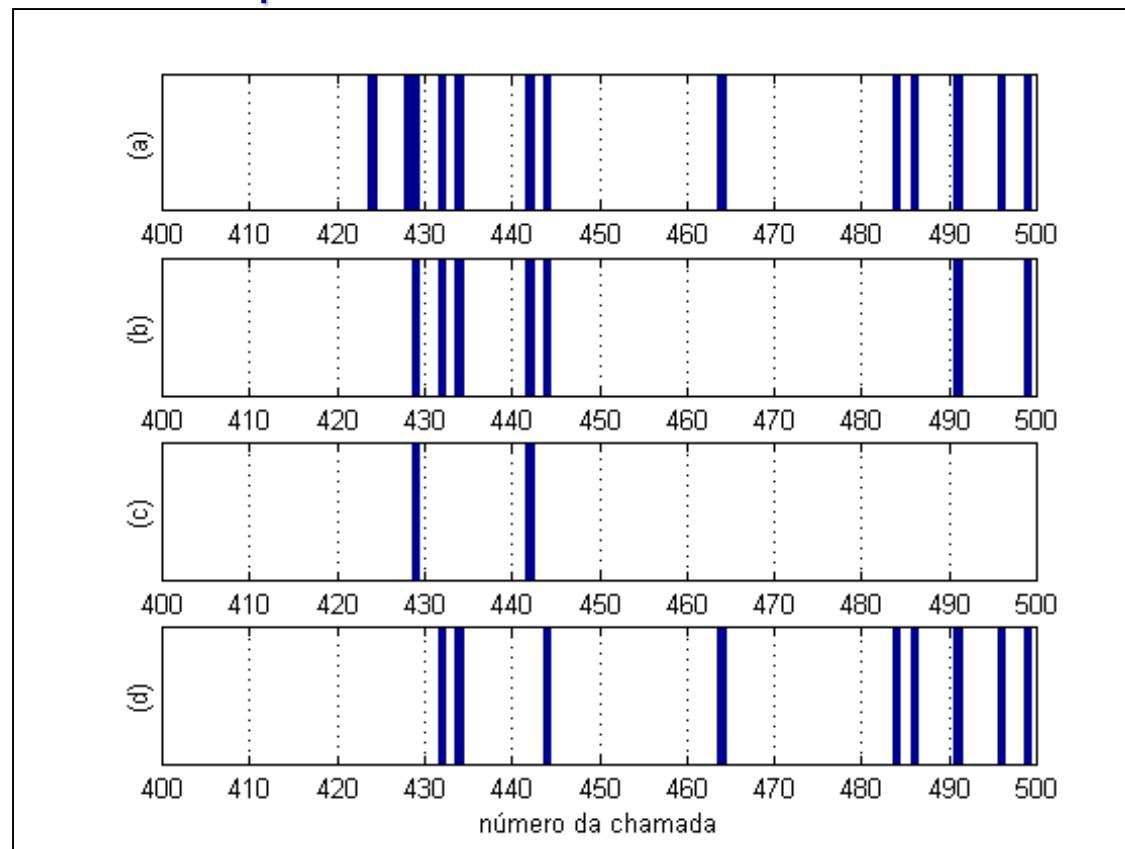
Adaptabilidade



- Distribuição de antígenos e detectores segundo o parâmetro *duração*. População de antígenos no intervalo de chamadas 71 a 500 e população de detectores ao final das 500 chamadas

Resultados Obtidos

Melhor Desempenho Obtido



- Sequência de chamadas de 400 a 500: (a) chamadas não completadas; (b) alarmes (sinal 2); (c) ativação de detectores e geração de sinal de falha (sinal 1 + sinal 2); (d) geração de sinal de falha (sinal 1 com detector ativo)

Resultados Obtidos

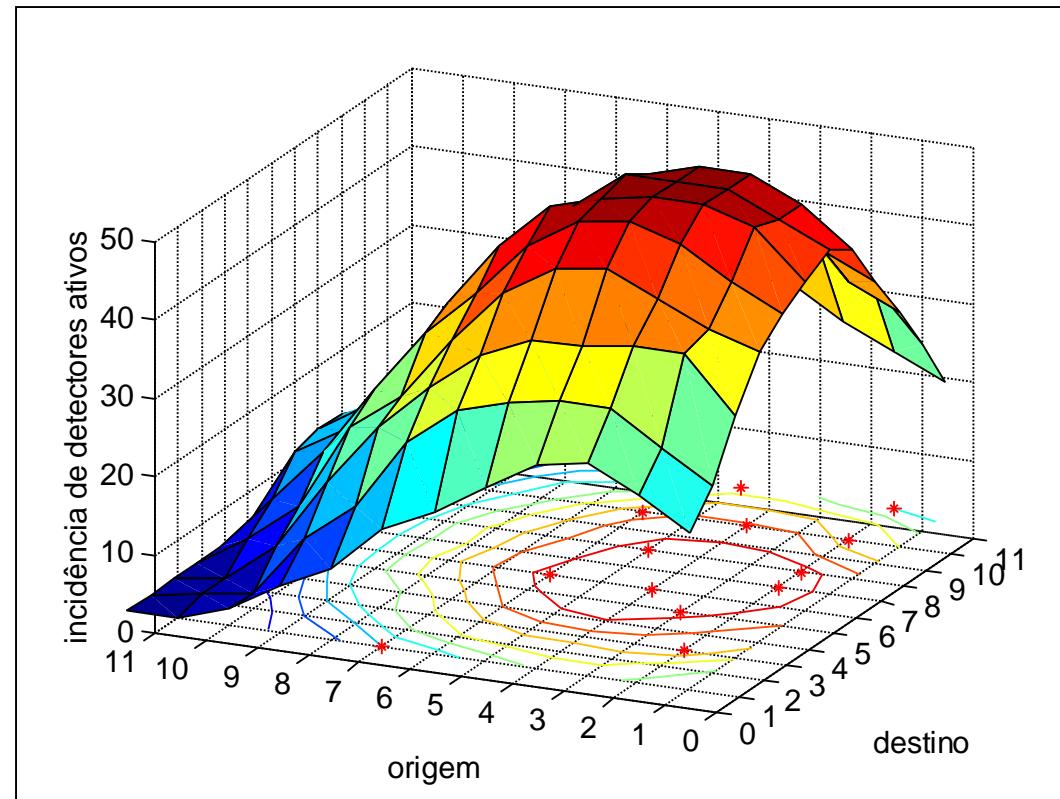
Desempenho Geral

- *td (zona de perigo)*: 20 tentativas de chamadas (o tempo médio de 20 tentativas de chamadas)
- *número de processos votantes*: 50 processos
- *limiar para votação*: 25% (o total de votos deve exceder esse limiar para a tentativa de chamada ser considerada uma falha)

Percentual de falhas não detectáveis pelo alarme (sinal 2), mas detectada pelo algoritmo	100 %
Percentual total de falhas detectadas	91,0 %
Percentual de execuções (conjunto de 500 chamadas) que tiveram alguma falha, não detectável pelo alarme (sinal 2), detectada pelo algoritmo	100 %
Percentual de Falsos Positivos	0%

Resultados Obtidos

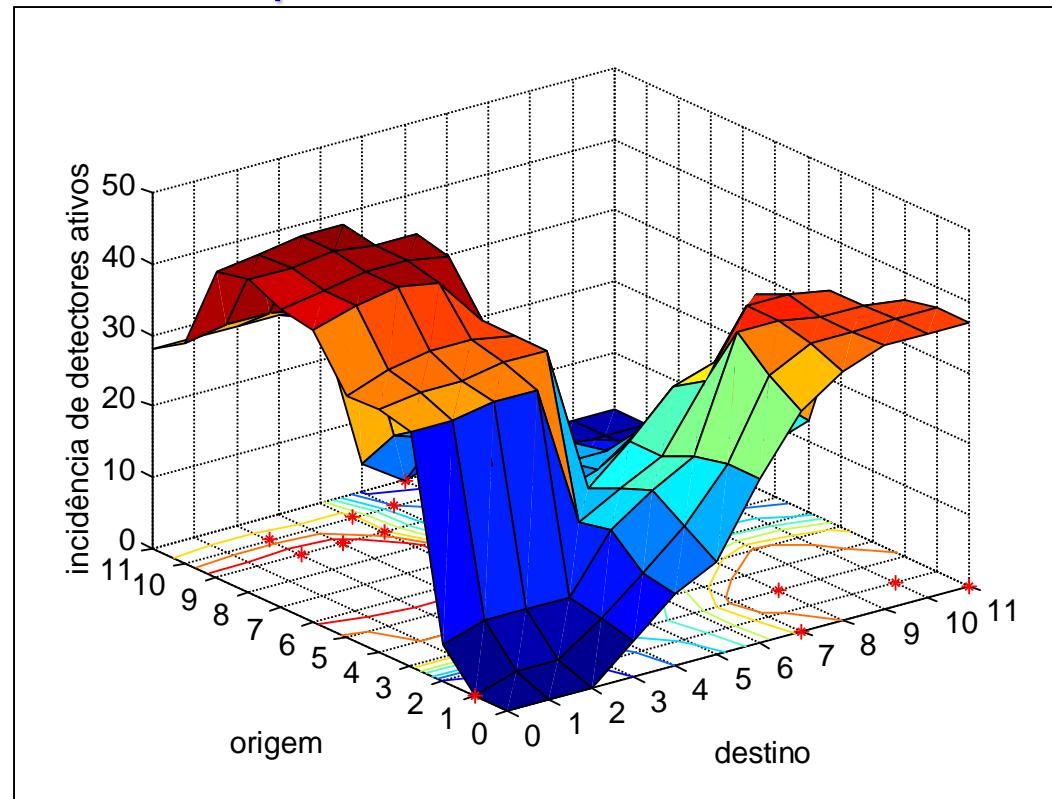
Desempenho Geral



- Comportamento médio do algoritmo de detecção de falhas no teste com uma região de falha. Estrelas correspondem às falhas. Quanto mais elevada a superfície, maior a incidência de detectores ativos na região

Resultados Obtidos

Detecção de Múltiplas Falhas e Isolabilidade



- Comportamento médio do algoritmo de detecção de falhas no teste com duas regiões de falha. Estrelas correspondem às falhas. Quanto mais elevada a superfície, maior a incidência de detectores ativos na região

Aplicação da Teoria do Perigo: Conclusões

- Altos índices de reconhecimento e diversidade pelo fato da população de detectores ser constantemente atualizada
- Alto percentual de cobertura na detecção de falhas especialmente em regiões não cobertas pelo alarme (sinal 2). Essa cobertura indica a possibilidade da continuidade de uma falha ou a tendência à retomada da mesma
- Número de FP insignificante
- Possibilidade de identificação de regiões (clusters) de alta concentração de detectores ativos, auxiliando no diagnóstico da falha
- Detecção rápida de falhas. Uma vez que detectores tenham sido ativados, basta a verificação de similaridade do padrão com esses detectores

Aplicação da Teoria do Perigo: Conclusões

- Robustez devido ao fato do algoritmo trabalhar com detecção imperfeita de antígenos, necessidade de utilização do sinal 2 e devido ao processo de votação.
- Alta adaptabilidade mesmo sendo baseado na história do processo. De acordo com Venkatasubramanian *et al.* (2003) e Katipamula & Brambley (2005), os métodos baseados na história do processo possuem deficiência nessa característica.
- Isolabilidade: Possibilidade de identificar múltiplas falhas.
- Capacidade de Indicar a Qualidade da Classificação por meio da análise da concentração de detectores ativos.

Agradecimentos

- Parte desse material se baseou nas pesquisas realizadas por Leandro Nunes de Castro Silva, Roberto Michelan, Helder Knidel, José Carlos Lima Pinto, Renato Reder Cazangi, Guilherme Palermo Coelho, todas desenvolvidas junto ao DCA/FEEC/Unicamp.

Referências

- Aickelin, U. & Cayzer, S. (2002) The Danger Theory and Its Application to Artificial Immune Systems, Technical Report HP Laboratories Bristol.
- Ayara, M., Timmis, J., de Lemos, R., de Castro, L.N. & Duncan, R. (2002) Negative Selection: How to Generate Detectors, 1st International Conference on AIS (ICARIS'2002), pp 89-98.
- Bezerra, G.B., Barra, T.V., de Castro, L.N., Von Zuben, F.J. (2005) Adaptive Radius Immune Algorithm for Data Clustering, Lect. Notes in Comp. Sc., vol. 3627, pp. 290-303.
- Bretscher P., Cohn M. (1970). "A Theory of Self-Nonself Discrimination", Science, vol. 169, pp. 1042-9.
- Burnet, F. M. (1959). "The Clonal Selection Theory of Acquired Immunity", Vanderbilt University Press, Nashville, TN.
- Dasgupta, D. (Ed.) (1998), Artificial Immune Systems and Their Applications, Springer-Verlag.
- Dasgupta, D. (2006), Advances in Artificial Immune Systems, IEEE Computational Intelligence Magazine, pp. 40-49, 2006.
- de Castro, L.N. (2001). "Engenharia Imunológica: Desenvolvimento e Aplicação de Ferramentas Computacionais Inspiradas em Sistemas Imunológicos Artificiais", Tese de Doutorado, Faculdade de Engenharia Elétrica e de Computação, Unicamp.
- de Castro, L. N., & Timmis, J. (2002), *Artificial Immune Systems: A New Computational Intelligence Approach*, Springer-Verlag.

Referências

- de Castro, L. N., & Von Zuben, F. J., (2002), "Learning and Optimization Using the Clonal Selection Principle", IEEE Transaction on Evolutionary Computation, vol. 6, no. 3, pp. 239-251.
- de Castro, L. N. & Von Zuben, F. J. (2001), "aiNet: An Artificial Immune Network for Data Analysis", Book Chapter in Data Mining: A Heuristic Approach, Hussein A. Abbass, Ruhul A. Sarker, and Charles S. Newton (Eds.), Idea Group Publishing, USA.
- Forrest, S., A. Perelson, Allen, L. & Cherukuri, R. (1994), "Self-Nonself Discrimination in a Computer", Proc. of the IEEE Symposium on Research in Security and Privacy, pp. 202-212.
- Gallucci, S. & Matzinger, P. (2001). "Danger Signals: SOS to the Immune System", Current Opinion in Immunology, vol. 13, pp. 114-119.
- Greensmith, J. (2007) "The Dendritic Cell Algorithm", PhD Thesis, University of Nottingham.
- Greensmith, J., Aickelin, U. & Cayzer, S. (2005) Introducing Dendritic Cells as a novel immune-inspired algorithm for anomaly detection. In Proc. of the 4th International Conference on Artificial Immune Systems (ICARIS), LNCS 3627, pages 153-167, Springer-Verlag, 2005.
- Hofmeyr S. A. & Forrest, S. (2000), "Architecture for an Artificial Immune System", Evolutionary Computation, 7(1), pp. 45-68.
- Jerne, N. K. (1974), "Towards a Network Theory of the Immune System", *Ann. Immunol. (Inst. Pasteur)* 125C, pp. 373-389.
- Kepler, T. B. & Perelson, A. S. (1993), "Somatic Hypermutation in B Cells: An Optimal Control Treatment", *J. theor. Biol.*, 164, pp. 37-64.
- Klein, J. (1990), *Immunology*, Blackwell Scientific Publications.
- Matzinger, P. (1998). "An Innate Sense of Danger", Seminars in Immunology, vol. 10, pp. 399-415.

Referências

- Matzinger, P. (2002). "The Danger Model: A Renewed Sense of Self", *Science*, vol. 296, pp. 301-305.
- Matzinger, P. (1994), "Tolerance, Danger and the Extended Family", *Annual Reviews of Immunology*, 12, pp. 991-1045.
- Nossal, G. J. V. (1993), "Life, Death and the Immune System", *Scientific American*, 269(3), pp. 21-30.
- Oprea, M. & Forrest, S. (1998), "Simulated Evolution of Antibody Gene Libraries Under Pathogen Selection", *Proc. of the IEEE SMC'98*.
- Perelson, A. S. (1989), "Immune Network Theory", *Imm. Rev.*, 110, pp. 5-36.
- Perelson, A. S., Hightower, R. & Forrest, S. (1996), "Evolution and Somatic Learning in V-Region Genes", *Research in Immunology*, 147, pp. 202-208.
- Perelson, A. S. & Oster, G. F. (1979), "Theoretical Studies of Clonal Selection: Minimal Antibody Repertoire Size and Reliability of Self-Nonself Discrimination", *J. theor. Biol.*, 81, pp. 645-670.
- Pinto, J.C.L. (2006) "Algoritmo de Detecção de Falhas para Sistemas Telefônicos Utilizando a Teoria do Perigo", Tese de Mestrado, FEEC/Unicamp.
- Stibor , T., Mohr, P. & Timmis, J. (2005) Is Negative Selection Appropriate for Anomaly Detection? *Proceedings of GECCO'2005*, pp. 321-328.
- Timmis, J. (2007) Artificial immune systems: today and tomorrow. *Natural Computing*, vol. 6, no. 1, pp. 1-18.
- Varela, F. J., Coutinho, A. Dupire, E. & Vaz, N. N. (1988), "Cognitive Networks: Immune, Neural and Otherwise", *Theoretical Immunology*, Part II, A.S. Perelson (Ed.), pp. 359-375.