

Engenharia de Computação
Inteligência Artificial
14 - Sistemas Imunológicos Artificiais
Seleção Negativa e Seleção Clonal

Organização da aula

- Retomada: AG, ACO e PSO e seus mecanismos de exploração.
- Inspiração biológica e abstrações de Sistemas Imunológicos Artificiais.
- Seleção Negativa (NSA): detectores e anomalias.
- Seleção Clonal (CLONALG): afinidade, clonagem, hipermutação e memória.
- Exemplos guiados, atividades, limitações e preparação para a prática.

Fio condutor

Como aproveitar mecanismos de reconhecimento e adaptação imunológica para detectar anomalias e otimizar soluções?

Retomada: três mecanismos de busca

Método	Mecanismo	Informação usada
Algoritmos Genéticos	seleção, recombinação e mutação	avaliação de aptidão
ACO	feromônio e construção probabilística	trilhas e qualidade das soluções
PSO	movimento orientado por melhores posições	melhor individual e coletivo

Para discutir

Como explorar boas soluções sem perder diversidade? E como reconhecer comportamento anormal sem conhecer todos os ataques?

Questão central da aula

O que podemos aprender com o sistema imunológico para *detectar anomalias* e *otimizar soluções*?

Nosso percurso

Inspiração biológica $\longrightarrow$ abstração computacional $\longrightarrow$ algoritmo $\longrightarrow$ experimento $\longrightarrow$ escolha do método.

Objetivos de aprendizagem

- Explicar a distinção entre sistema imune biológico e Sistema Imunológico Artificial (SIA).
- Formalizar o Algoritmo de Seleção Negativa (NSA) e o CLONALG.
- Interpretar detectores, afinidade, clonagem, hipermutação e memória.
- Acompanhar execuções passo a passo e reconhecer parâmetros críticos.
- Comparar SIA com AG, ACO e PSO, considerando adequação e limitações.

Duas tarefas, duas famílias de soluções

Detecção de anomalias

Dados normais conhecidos. Procurar padrões que se afastam da região normal.

Exemplo: monitoramento de sensores.

Otimização

Há uma função objetivo e soluções candidatas. Procurar configurações de maior qualidade.

Exemplo: seleção de recursos sob restrições.

Ideia central

Nesta aula: NSA para detecção e CLONALG para otimização. São abordagens distintas dentro dos SIA.

Sistema imunológico: abstrações úteis

Inspiração	Abstração computacional
Reconhecimento do próprio	região de comportamento normal
Receptores e diversidade	conjunto variado de candidatos/detectores
Seleção negativa	descartar detectores que reconhecem o normal
Seleção clonal	multiplicar candidatos de alta afinidade
Hipermutação	explorar vizinhanças com variação controlada
Memória	preservar soluções ou padrões relevantes

A analogia é seletiva: os algoritmos não reproduzem fielmente toda a imunologia.

Resposta imune inata e adaptativa

Inata

Resposta rápida; mecanismos relativamente gerais; barreiras, fagócitos e sinalização.

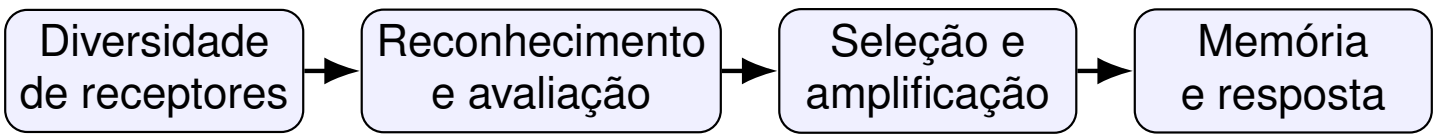
Adaptativa

Reconhecimento específico, expansão clonal e memória; participação de linfócitos B e T.

Para discutir

Por que diversidade e memória podem ser propriedades úteis para uma busca computacional?

Reconhecimento, seleção e memória



Ideia central

O algoritmo utiliza uma ideia inspiradora, não um modelo biologicamente completo.

Limites da analogia biológica

- A seleção negativa computacional não equivale à totalidade da tolerância imunológica.
- No CLONALG, a afinidade pode ser definida diretamente por uma função objetivo; isso não é uma correspondência universal na biologia.
- Modelos imunes diferem entre si: redes imunes, modelo do perigo e DCA respondem a necessidades distintas.
- A eficácia depende da representação, métricas, parâmetros e dados, não da metáfora biológica.

Famílias de Sistemas Imunológicos Artificiais

Família	Operação característica	Aplicação típica
Seleção Negativa (NSA)	gerar detectores fora do próprio	detecção de anomalias
Seleção Clonal (CLONALG)	clonar e hipermutar bons candidatos	otimização e reconhecimento
Redes imunes (ex.: aiNet)	interação e supressão por afinidade	agrupamento e memória
Modelos de perigo (ex.: DCA)	combinar sinais contextuais	detecção contextual

Foco da aula: NSA e CLONALG; os demais modelos serão contextualizados.

Problema 1: detectar comportamento anormal

Um sistema recebe medidas $x = (x_1, x_2)$ de um dispositivo. Há registros normais $S = \{s_1, \ldots, s_n\}$, mas não existe uma lista completa de falhas.

O que conhecemos?

Amostras do funcionamento *normal*.

O que queremos?

Detectores capazes de sinalizar regiões não cobertas pelo normal.

Para discutir

É possível reconhecer algo que não aparece no treinamento? Como evitar alarmes falsos?

NSA: mapeamento para Computação

Conceito	Representação
Próprio	conjunto S de amostras normais
Candidato a detector	vetor d no espaço de atributos
Afinidade / reconhecimento	condição $\mathrm{dist}(d, x) \leq r$
Tolerância ao próprio	rejeitar d que reconhece algum $s \in S$
Ativação	sinalizar x quando algum detector o reconhece

Formalização: geração de detectores

Definição

Dado $S \subset \mathcal{X}$ e raio $r > 0$, um detector d é aceito se

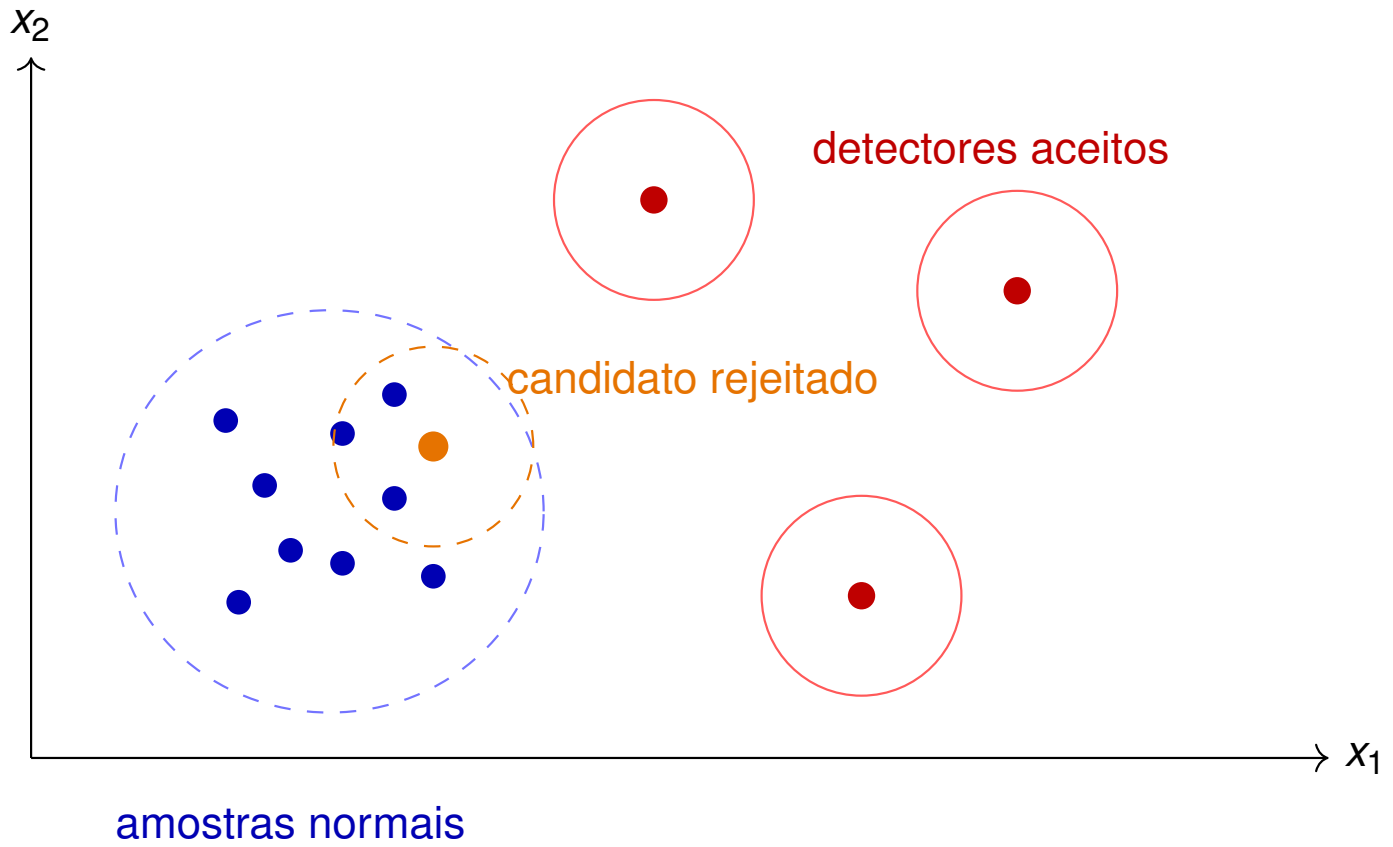
$$\forall s \in S, \quad \text{dist}(d, s) > r.$$

Para um detector esférico de raio r, a região sinalizada por d é $B(d, r) = \{x \in \mathcal{X} : \text{dist}(x, d) \leq r\}$.

Ideia central

O algoritmo descarta candidatos próximos aos padrões normais; os remanescentes cobrem parte do espaço não próprio.

Visualização: normal e detectores



NSA: treinamento dos detectores

Input: Padrões normais S; raio r; alvo N; tentativas máximas T
Output: Conjunto de detectores D
$D \leftarrow \varnothing$; $t \leftarrow 0$
while $|D| < N$ ***e*** $t < T$ **do**
    gerar candidato $c \in \mathcal{X}$
    $t \leftarrow t + 1$
    if $\forall s \in S : \text{dist}(c, s) > r$ **then**
        adicionar c a D
    end if
end while
return D

Condição de parada dupla evita laços intermináveis caso a região admissível seja pequena.

NSA: fase de detecção

Regra de decisão

$$\text{anomalo}(x) = \begin{cases} 1, & \exists d \in D : \text{dist}(x, d) \leq r, \\ 0, & \text{caso contrário.} \end{cases}$$

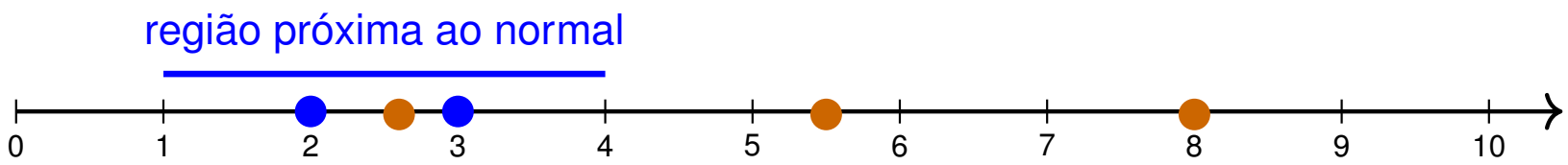
Para discutir

Se nenhum detector dispara, podemos afirmar que x é normal?

Não. Ausência de ativação pode indicar região anômala não coberta pelos detectores.

NSA: exemplo numérico (1/2)

Considere o espaço unidimensional $\mathcal{X} = [0, 10]$, padrões normais $S = \{2, 3\}$ e $r = 1$.



Teste dos candidatos

$c_1 = 2{,}6$, $c_2 = 5{,}5$ e $c_3 = 8$. Quais podem ser aceitos?

NSA: exemplo numérico (2/2)

Candidato	$\text{dist}(c, 2)$	$\text{dist}(c, 3)$	Decisão
2,6	0,6	0,4	rejeitar
5,5	3,5	2,5	aceitar
8,0	6,0	5,0	aceitar

Teste

Com $D = \{5{,}5, 8\}$ e $r = 1$, o ponto $x = 7{,}5$ é sinalizado? Sim: $|7{,}5 - 8| = 0{,}5 \leq 1$.

Atividade rápida: teste de detectores

Individual ou em dupla (3 minutos)

Considere $D = \{5{,}5, 8\}$ e $r = 1$ no intervalo $[0, 10]$. Classifique $x = 4$, $x = 5$, $x = 7$ e $x = 9{,}5$. Justifique pelo detector mais próximo.

Para discutir

O ponto $x = 0$ não ativa nenhum detector. O que isso revela sobre cobertura?

Discussão da atividade: NSA

x	menor distância a D	Resultado
4	1,5	sem ativação
5	0,5	anomalia sinalizada
7	1	anomalia sinalizada
9,5	1,5	sem ativação

Ideia central

Nenhuma ativação não demonstra normalidade: $x = 0$ está distante dos padrões normais e dos detectores.

Parâmetros críticos do NSA

Parâmetro	Se aumentar...	Possível efeito
Raio r	amplia reconhecimento	mais alertas; pode dificultar gerar detectores
Número N	mais detectores	potencial maior cobertura; maior custo
Tentativas T	mais candidatos avaliados	mais chance de cobertura; maior treinamento
Dimensão	aumenta espaço de busca	cobertura torna-se mais difícil

Avaliação do detector de anomalias

Matriz de confusão

VP: anomalias sinalizadas
FP: normais sinalizados
FN: anomalias perdidas
VN: normais não sinalizados

Métricas

$$\text{Precisao} = \frac{VP}{VP + FP}$$

$$\text{Recall} = \frac{VP}{VP + FN}$$

Para discutir

Em um sistema de segurança, o que custa mais: falso alarme ou falha não detectada?

NSA: limites de aplicação

- Cobertura parcial do espaço não próprio: não detectar não equivale a classificar como normal.
- Amostras normais incompletas podem causar falsos positivos.
- A escolha da distância e da normalização dos atributos altera o resultado.
- Em dimensões elevadas, o número de detectores pode crescer e a cobertura ficar insuficiente.
- Deriva de conceito exige atualização de modelos e análise temporal.

Transição: de reconhecer a otimizar

NSA: **evitar o normal** para detectar

$$\Downarrow$$

CLONALG: **amplificar bons candidatos** para otimizar

Ideia central

Mesma família de inspiração; objetivos e regras de atualização diferentes.

Problema 2: otimizar uma solução

Temos uma configuração $x \in \mathcal{X}$ e uma função objetivo $f(x)$.

$$\max_{x \in \mathcal{X}} f(x) \qquad \text{ou} \qquad \min_{x \in \mathcal{X}} f(x).$$

Intuição

Uma população de candidatos é avaliada; os melhores recebem mais clones e são modificados para explorar soluções próximas.

Para discutir

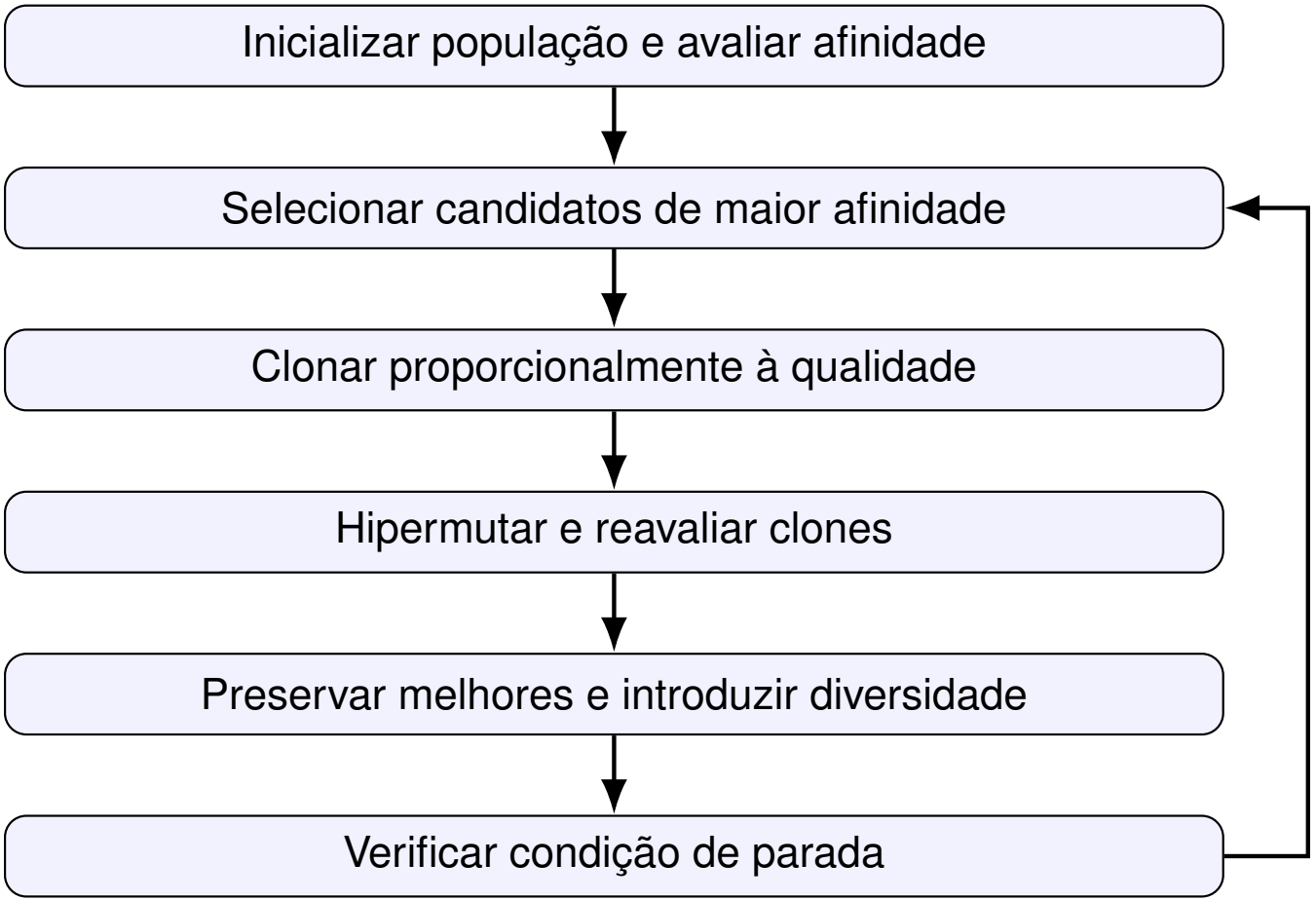
Em que essa estratégia se aproxima de um Algoritmo Genético? Em que se diferencia?

CLONALG: representação e afinidade

Componente	Papel computacional
Anticorpo x	solução candidata (vetor binário, real etc.)
Afinidade $a(x)$	medida de qualidade, derivada do objetivo
Clones	cópias de candidatos selecionados
Hipermutação	perturbação dependente de afinidade
Memória / elite	preservação de soluções de destaque
Diversificação	novos candidatos aleatórios ou reinicialização

É necessário transformar minimização em uma afinidade coerente com o critério de seleção.

CLONALG: fluxo do algoritmo



Etapa 1: seleção e clonagem

Nesta variante, selecione n candidatos de maior afinidade e defina o número de clones pela posição na ordenação:

$$N_i = \max\left(1, \left\lfloor \beta \frac{n}{i} \right\rfloor\right), \quad i = 1, \ldots, n.$$

Leitura da equação

$i = 1$ corresponde ao melhor candidato; β controla a intensidade da clonagem. Esta é uma regra possível, não uma definição universal de CLONALG.

Etapa 2: hipermutação

Taxa de mutação dependente de afinidade

Uma opção é $p_m(a) = p_{\min} + (p_{\max} - p_{\min})(1 - a)$, com afinidade normalizada $a \in [0, 1]$.

Alta afinidade

Menor perturbação: intensificação perto de boas soluções.

Baixa afinidade

Maior perturbação: exploração mais ampla da vizinhança.

Para maximização, uma normalização possível é $a_i = (f_i - f_{\min})/(f_{\max} - f_{\min})$, se $f_{\max} > f_{\min}$. Para minimização, inverter o sentido da qualidade.
O operador deve respeitar a representação e tratar restrições.

CLONALG: pseudocódigo

Input: Objetivo f; população P; tamanhos n, N; gerações G
Output: Melhor solução x^*
Avaliar P; $x^* \leftarrow \arg\max_{x \in P} f(x)$
for $g \leftarrow 1$ **to** G **do**
    $E \leftarrow$ selecionar os n melhores de P
    $C \leftarrow$ clonar candidatos em E
    $C' \leftarrow$ hipermutar clones em C e avaliar
    $P \leftarrow$ selecionar melhores de $P \cup C'$ e completar com diversidade até N
    atualizar x^* com o melhor de P
end for
return x^*

Variante de otimização com elitismo e renovação; as formulações publicadas variam em seleção, taxas e reposição.

Exemplo comum às metaheurísticas

Seleção de itens (problema ilustrativo)

Escolher itens sob capacidade $C = 7$, maximizando o valor total.

Item	A	B	C	D
Peso	2	3	4	5
Valor	3	4	5	8

$$x = (x_A, x_B, x_C, x_D) \in \{0,1\}^4, \quad \sum_i w_i x_i \leq 7.$$

Exemplo reduzido com 4 bits apenas para acompanhar os cálculos. Na prática, será retomado o problema binário de 16 bits adotado nas aulas de AG e Enxames; ACO requer construção compatível.

Função objetivo e penalização

Uma formulação

$$f(x) = \sum_i v_i x_i - \lambda \max\left(0, \sum_i w_i x_i - C\right), \quad \lambda > 0.$$

Alternativa

Representação com reparo: sempre que um vetor exceder a capacidade, remover itens segundo regra documentada.

Ideia central

Comparação justa exige a mesma função de avaliação, restrições, orçamento computacional e métricas.

CLONALG: uma geração (1/2)

Considere população inicial e pontuação com $\lambda = 10$:

Candidato	Bits (A B C D)	Peso	$f(x)$
x_1	1001	7	11
x_2	0110	7	9
x_3	1100	5	7
x_4	0011	9	-7

Para discutir

Quais candidatos devem receber prioridade na clonagem? Por quê?

CLONALG: uma geração (2/2)

Exemplo de perturbação

O candidato $x_3 = 1100$ (A+B, $f = 7$) passa por duas inversões de bits:
$1100 \rightarrow 1000 \rightarrow 1001$ (A+D, $f = 11$).

Seleção

Se x' supera outros indivíduos, pode entrar na população seguinte; a política elitista preserva o melhor valor observado.

Para discutir

Uma mutação que gera 1111 melhora o valor bruto. Por que essa solução não deve ser tratada como ótima viável?

Atividade rápida: representação e operador

Em grupos (4 minutos)

Proponham uma regra de hipermutação para os vetores binários da seleção de itens. Respondam:

1. Como escolher os bits a inverter?
2. Como respeitar a capacidade $C = 7$?
3. Como manter diversidade sem perder a melhor solução?

Ideia central

O operador de mutação não deve ser escolhido independentemente da representação e das restrições.

Possível solução para a atividade

- Inverter cada bit com probabilidade $p_m(a)$, menor para candidatos mais bem avaliados.
- Aplicar uma penalização na função objetivo ou reparar os vetores inviáveis antes da avaliação.
- Preservar um ou mais candidatos de elite e substituir parte dos piores por novos candidatos.
- Fixar sementes, documentar parâmetros e executar repetições para comparar variabilidade.

CLONALG: parâmetros e trade-offs

Parâmetro	Controla	Cuidado
Tamanho N	diversidade e custo por geração	população pequena converge cedo
Seleção n	intensificação	seleção muito forte reduz variedade
Fator β	quantidade de clones	custo de avaliações
Hipermutação	amplitude de exploração	taxas excessivas destroem boas soluções
Renovação	entrada de novos candidatos	excesso dificulta convergência

CLONALG e Algoritmos Genéticos

Aspecto	AG	CLONALG (variante)
Reprodução	seleção e crossover/mutação	seleção e clonagem
Variação	mutação tipicamente parametrizada	hipermutação relacionada à afinidade
Memória	pode usar elitismo	frequentemente usa memória/elitismo
Exploração	recombinação e mutação	mutação + renovação de população

As diferenças dependem da implementação escolhida; não são garantias de superioridade.

Comparando AG, ACO, PSO e CLONALG

Método	Mecanismo de atualização	Questão de modelagem
AG	seleção, recombinação e mutação	cruzamento viável?
ACO	construção probabilística via feromônio	como construir soluções válidas?
PSO/BPSO	velocidade e melhores posições	como discretizar e impor restrições?
CLONALG	clones, hipermutação e memória	como definir afinidade e mutação?

Ideia central

Não há vencedor universal: representação e orçamento de avaliação condicionam o desempenho.

Uma comparação experimental defensável

- Manter os mesmos dados, objetivo, restrições e critério de viabilidade.
- Definir orçamento comparável de avaliações da função objetivo, não apenas gerações.
- Utilizar as mesmas sementes predefinidas em todos os métodos, com execuções independentes.
- Relatar melhor, média, desvio-padrão, taxa de soluções viáveis e custo.
- Observar convergência e discutir sensibilidade a hiperparâmetros.

Além de NSA e CLONALG

Abordagem	Ideia geral
Redes imunes artificiais	competição, estimulação e supressão entre representantes
Modelo do perigo	sinais de dano/contexto complementam a distinção próprio/não próprio
DCA	agregação de sinais e contexto para classificação de anomalias

Introdução contextual: esses modelos não serão implementados nesta prática; evitamos misturar várias famílias antes de consolidar NSA/CLONALG.

Aplicações: escolha orientada pelo problema

Anomalias

Falhas de equipamentos, padrões incomuns de tráfego, monitoramento operacional.

Cuidado: calibrar falsos positivos e cobertura.

Otimização

Alocação de recursos, seleção de atributos, configuração e projeto.

Cuidado: comparar com baselines robustos.

Para discutir

Quando seria mais razoável usar um classificador supervisionado, em vez de NSA?

Limitações e validade empírica

- A inspiração biológica não implica vantagem de desempenho.
- NSA pode ter dificuldade de cobertura e escalabilidade.
- CLONALG exige definição cuidadosa de afinidade, mutação e elitismo.
- Resultados sensíveis à função de avaliação e às restrições.
- É necessário comparar com alternativas simples e métodos já estudados sob protocolo controlado.

Preparação para a aula prática

Trilha A: reconhecimento

Implementar e visualizar NSA em dados bidimensionais, examinando raio, cobertura e matriz de confusão.

Trilha B: otimização

Implementar CLONALG com representação e função objetivo compatíveis com o problema adotado em AG e enxames.

Ideia central

O objetivo é analisar mecanismo, parâmetros e evidência experimental, não apenas obter um valor final.

Síntese: o que muda de um algoritmo para outro?

Pergunta	NSA	CLONALG
Problema	anomalias	otimização
Conhecimento	padrões normais	função objetivo
Solução	detectores válidos	candidato de alta afinidade
Operador central	rejeição do próprio	clonagem e hipermutação
Avaliação	detecção, FP, FN	qualidade, custo e robustez

Referências e aprofundamento

- DE CASTRO, L. N.; VON ZUBEN, F. J. Learning and optimization using the clonal selection principle. *IEEE Transactions on Evolutionary Computation*, 6(3), 239–251, 2002.
- FORREST, S.; PERELSON, A. S.; ALLEN, L.; CHERUKURI, R. Self-nonself discrimination in a computer. *IEEE Symposium on Research in Security and Privacy*, 202–212, 1994.
- DE CASTRO, L. N.; TIMMIS, J. *Artificial Immune Systems: A New Computational Intelligence Approach*. Springer, 2002.
- RUSSELL, S.; NORVIG, P. *Artificial Intelligence: A Modern Approach*. Pearson, 4th ed., 2021. (Contexto geral de busca e otimização.)

Próxima aula: prática de Sistemas Imunológicos

- Aplicar seleção negativa ao reconhecimento de padrões fora da região normal.
- Implementar CLONALG para o mesmo problema binário da prática de AG e Enxames.
- Comparar AG, ACO, BPSO e CLONALG usando a mesma função objetivo, orçamento de avaliações e sementes.

Para a próxima aula

Como o mecanismo de clonagem e hipermutação muda a exploração de soluções de 16 bits?

Dúvidas



Verificação de aprendizagem

1. Por que um detector do NSA precisa ser rejeitado se reconhece o próprio?
2. Por que ausência de ativação não garante normalidade?
3. O que significa afinidade em um CLONALG de otimização?
4. Qual é o papel da hipermutação e da renovação?
5. Como comparar CLONALG e AG de maneira justa?