Подводя итог, эмпирические модели используются для заполнения там, где научные теории не существуют или слишком сложны. Результаты экспериментальной или физической модели используются для разработки эмпирических моделей, а также для калибровки и проверки математических моделей.

Список использованных источников:

1. Kai Velten (2009). Mathematical modeling and simulation. WILEY–VCH Verlag GmbH & Co. KGaA, Weinheim.
2. Anu Maria, (1997). Introduction to modeling and simulation. Proceedings of the 1997 Winter Simulation Conference Eds. Andradóttir, S., Healy, K.J., Withers, D.H. and Nelson, B.L.

ОӘЖ 004

ГЕНЕТИКАЛЫҚ АЛГОРИТМ НЕГІЗІНДЕГІ АСИММЕТРИЯЛЫҚ КРИПТОЖҮЙЕ

Базарбеков Багдат Канатович
kanaatovich@gmail.com
Қазақстан Республикасы, Нұр-Сұлтан қ.,
Л.Н. Гумилев атындағы Еуразия ұлттық университеті
Ақпараттық технологиялар факультеті
Информатика және ақпараттық қауіпсіздік кафедрасы
«6М100200» - Ақпараттық қауіпсіздік жүйелері мамандығының магистранты
Ғылыми жетекшісі – Г.Т. Бекманова

Генетикалық алгоритмдер - бұл жақында функционалды оңтайландыру мәселелерін шешуде жиі қолданылатын адаптивті іздеу әдістері. Олар биологиялық организмдердің генетикалық процестеріне негізделеді: биологиялық популяциялар бірнеше ұрпақтарда дамиды, табиғи сұрыптау заңдылықтарына және Чарльз Дарвин ашқан «ең жақсы тіршілік ету» қағидасына бағынады. Осы процесті еліктей отырып, генетикалық алгоритмдер, егер олар дұрыс кодталған болса, нақты өмірдегі мәселелерді шешуге мүмкіндік береді. Мысалы, ГА-ды көпір құрылымдарын жобалау, максималды беріктік/салмақ арақатынасын табу немесе матадан пішінді кесу үшін ысырап етудің ең аз орнын анықтау үшін пайдалануға болады. Оларды интерактивті процестерді басқару үшін де қолдануға болады, мысалы химиялық зауытта немесе мультипроцессорлы компьютерде жүктемелерді теңестіру. Нақты мысал: израильдік Schema компаниясы сөйлесудің оңтайлы жиілігін таңдау арқылы ұялы байланысты оңтайландыру үшін арналы бағдарламалық өнімді шығарды. Бұл бағдарламалық жасақтама негізінде генетикалық алгоритмі қолданылды.

ГА-ның негізгі қағидаларын Холлан тұжырымдаған және көптеген еңбектерде жақсы сипатталған. Табиғатта пайда болатын эволюциядан айырмашылығы, ГА-дер тек даму үшін қажет популяциялардағы процестерді модельдейді.

Табиғатта популяциядағы жеке даралар, мысалы, тамақ немесе су сияқты түрлі ресурстар үшін бір-бірімен бәсекелеседі. Сонымен қатар, бір популяция мүшелері көбінесе жұптасатын серіктесті тарту үшін жарысады. Қоршаған орта жағдайларына көп бейімделген араларда ұрпақтардың көбею мүмкіндігі айтарлықтай жоғары болады. Нашар бейімделген даралар не ұрпақты мүлдем шығармайды, немесе олардың ұрпақтары өте аз болады. Бұл жоғары бейімделген немесе бейімделген даралардан шыққан гендер әрбір келесі ұрпақ үшін өсіп келе жатқан ұрпақтарда таралатынын білдіреді. Әр түрлі ата-аналардың жақсы қасиеттерінің үйлесуі кейде ата-анасының фитнесінен «өте бейімделген» ұрпақтардың пайда болуына әкелуі мүмкін. Осылайша, түрлер өсіп, тіршілік ету ортасына жақсырақ бейімделеді.

ГА-дер осындай механизммен тікелей аналогияны қолданады. Олар «жеке тұлғалар» жиынтығымен жұмыс істейді, олардың әрқайсысы осы мәселенің мүмкін болатын шешімін ұсынады. Әрбір жеке тұлға өзінің «жарамдылығы» өлшемі бойынша мәселенің тиісті шешімін «қаншалықты жақсы» екендігіне қарай бағалайды. Мысалы, берілген көпір конструкциясы

үшін дене шынықтыру өлшемі күш/салмақ қатынасы болуы мүмкін. (Табиғатта бұл дененің ресурстар үшін бәсекелескен кезде қаншалықты тиімді екенін бағалауға тең.) Жеке тұлғалар популяциядағы басқа жекелермен «кесіп өту» арқылы ұрпақтарды «көбейтуге» қабілетті. Бұл ата-анасынан мұра болатын кейбір сипаттамаларды біріктіретін жаңа жеке тұлғалардың пайда болуына әкеледі. Ең аз сәйкестендірілген даралар ұрпақтарды көбейту мүмкіндігіне ие емес, сондықтан олар иеленетін қасиеттер эволюция кезінде популяциядан біртіндеп жоғалып кетуі мүмкін.

Осылайша, мүмкін болатын шешімдердің барлық жаңа топтамалары жасалады, алдыңғы буын өкілдерін таңдап, олардан өтіп, көптеген жаңа жеке тұлғалар пайда болады. Бұл жаңа буын алдыңғы буынның жақсы мүшелері ие болатын сипаттамалардың неғұрлым жоғары қатынасын қамтиды. Осылайша, ұрпақтан-ұрпаққа жақсы сипаттамалар бүкіл халыққа таратылады. Неғұрлым бейімделген жекелерді кесіп өту іздеу кеңістігінің ең перспективті бөлімдері зерттелетініне әкеледі.

Нәтижесінде, халық мәселенің оңтайлы шешіміне келеді. ГА аясында биологиялық эволюция идеясын жүзеге асырудың көптеген жолдары бар. Келесідей көрсетілген ГА дәстүрлі болып саналады:

БАСЫ /* генетикалық алгоритм */
Бастапқы популяцияны құру
Әр дараның бейімділігін бағалау
тоқтату := FALSE
ӘЛІ ЖОҚ тоқтату ОРЫНДАУ
БАСЫ /* жаңа буын популяциясын құру */
ҚАЙТАЛАУ (популяция_көлемі/2) РЕТ
БАСЫ /* көбею циклі */
Кросс-овер үшін алдыңғы буыннан бейімділігі жоғары екі дараны таңдау
Таңдалған дараларды қиылыстырып жаңа екі ұрпақ алу
Ұрпақтардың бейімділігін бағалап, жаңа буынға қосу
СОҢЫ
ЕГЕР популяция жиналса ОНДА тоқтату := TRUE
СОҢЫ
СОҢЫ

Соңғы жылдары көптеген генетикалық алгоритмдер жүзеге асырылды және көп жағдайда олар осы ГА-ға мүлдем ұқсамайды. Осы себепті, қазіргі уақытта «генетикалық алгоритмдер» термині тек бір модельді ғана емес, ал кейде бір-біріне ұқсамайтын алгоритмдердің кең класын жасырады. Зерттеушілер әртүрлі көріністер, кроссовер және мутация операторларымен, арнайы операторлармен және көбею мен таңдаудың әртүрлі тәсілдерімен тәжірибе жасады.

ГА-ның басты артықшылығы - оларды арнайы әдістер жоқ жерде күрделі тапсырмаларда да қолдануға болады. Қолданыстағы техникалар жақсы жұмыс істесе де, оларды ГА-мен біріктіру арқылы жақсартуға болады.

Генетикалық алгоритмнің орындалуының қарапайым мысалдары

Қарапайым ГА кездейсоқ құрылымдардың алғашқы популяциясын тудырады. ГА жұмысы - бұл белгілі бір буын немесе басқа тоқтату критерийлері орындалғанға дейін жалғасатын итерациялық процесс. ГА әр буыны үшін таңдау фитнеске, бір нүктелі кроссоверге және мутацияға пропорционалды. Біріншіден, пропорционалды іріктеу әрбір құрылымға Ps(i) ықтималдығын оның дене шынықтыру деңгейінің халықтың жалпы бойына қатынасына тең:

$$Ps(i) = \frac{f(i)}{\sum_{i=1}^{n} f(i)}$$

Содан кейін барлық n жеке даралар Ps(i) мәніне сәйкес әрі қарай генетикалық өңделуі үшін таңдалады (ауыстырылады). Қарапайым пропорционалды таңдау-рулетка(roulette-wheel

selection, Goldberg, 1989) - n рулетка көмегімен жеке адамдарды таңдайды. Рулетка дөңгелегінде халықтың әр мүшесі үшін бір сектор бар. і-секторының мөлшері Ps(i) мәніне сәйкес келеді. Бұл таңдау кезінде бейімделу деңгейі жоғары халықтың мүшелері бейімделу деңгейі төмен дараларға қарағанда жиі таңдалады.

Іріктеуден кейін n таңдалған адамдар Pc берілген ықтималдығы бар кроссоверден өтеді (кейде рекомбинация деп аталады). n сызықтары кездейсоқ n/2 жұпқа бөлінеді. Pc ықтималдығы бар әрбір жұп үшін кроссовер қолдануға болады. Тиісінше, 1-Pc дана болу ықтималдығында кроссовер пайда болмайды және өзгермеген даралар мутация сатысына өтеді. Егер кроссовер пайда болса, пайда болған ұрпақ ата-аналарын ауыстырады және мутацияға көшеді.

Бір нүктелі кроссовер келесідей жұмыс істейді. Біріншіден, l-1 үзіліс нүктелерінің бірі кездейсоқ таңдалады. (Сыну нүктесі - бұл жолдағы іргелес биттер арасындағы аймақ.) Екі ата-ана құрылымы да сол тармақта екі сегментке бөлінеді. Содан кейін әр түрлі ата-аналардың сәйкес сегменттері қосылып, екі ұрпақтың генотиптері алынады.

Мысалы, бір ата-ана 10 нөлден, ал екіншісі 10 бірліктен тұрады делік. 9 мүмкін үзіліс нүктесінен 3-нүктені таңдап алайық, төменде ата-аналар мен олардың ұрпақтары көрсетілген:

Кроссовер

Ата 1 А 00000 000~00 111~00 11100 Ұрпақ 1
00000 00000 -> 00000 00000

Ата 2 А 11111 111~11 000~11 00011 Ұрпақ 2
11111 11111 -> 11111 11111

Кроссовер кезеңі аяқталғаннан кейін мутация операторлары орындалады. Мутацияға ұшыраған кез-келген жолда Pm ықтималдығы бар биттің бәрі өзгертіледі. Мутациядан кейін алынған популяция ескінің үстіне жазылады және бұл бір буын циклін аяқтайды. Кейінгі буындар осылайша өңделеді: таңдау, кроссовер және мутация.

Қазіргі уақытта ГА зерттеушілері көптеген басқа таңдау, кроссовер және мутация операторларын ұсынады. Ең алдымен, турнир таңдауы (Бриндл, 1981; Голдберг және Деб, 1991). Турнирді таңдау n дараны таңдау үшін n турнир өткізеді. Әр турнир популяциядан k элементтерін іріктеу және олардың арасынан ең мықты дараны таңдау негізінде құрылады. k=2 ең көп кездесетін турнир түрі.

Таңдаудың элиталық әдістері (Де Йонг, 1975) -таңдау міндетті түрде өмір сүруді қамтамасыз етеді. Ең көп таралған процедура - таңдау, кроссовер және мутация процестерінен басқалары сияқты өтпеген жағдайда, ең жақсы даралардың біреуін міндетті түрде сақтау. Элитизмді кез-келген стандартты таңдау әдісіне енгізуге болады.

Екі нүктелі кроссовер (Кавиччио, 1970; Голдберг, 1989) және біркелкі кроссовер (Сисверда, 1989) бір нүктелі операторға лайықты балама болып табылады. Екі нүктелі кроссоверде екі үзіліс нүктесі таңдалады, ал ата-аналық хромосомалар осы екі нүктенің арасындағы кесіндімен алмасады. Біркелкі кроссоверде алғашқы ата-ананың әр биті берілген ықтималдығы бар бірінші балаға мұрагерлік етеді; әйтпесе, бұл бит екінші балаға беріледі. Және керісінше.

Қолданылған әдебиеттер тізімі

1. Карпов Ю.Г. Теория и технология программирования. Основы построения трансляторов Год: 2005 .
2. Tipton H. F., M. Krause. Information Security Management Handbook. — 5th Edition. — Boca Raton: CRC Press, 2006. — 2036 с
3. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке С, 2-е изд . – М.: Вильямс, 2003. – 672б.
4. Ростовцев А. Г., Михайлова Н. В. Методы криптоанализа классических шифров . – М.: Наука, 1995. – 208 б.

5. Biryukov A., Shamir A., Wagner D. Real Time Cryptanalysis of A5/1 on a PC //Fast Software Encryption. – Springer Berlin Heidelberg, 2001. – С. 1-18.
6. Paget C., Nohl K. GSM: SRSLY //26th Chaos Communication Congress. – 2016.

ОӘЖ 004.932.2

ҒАРЫШТЫҚ СУРЕТТЕРДІ ТАЛДАУДЫҢ ӘДІСТЕРІ МЕН ҚҰРАЛДАРЫ

Байғарин Әлішер Сабыржанұлы
alisher.baygarin@gmail.com
С.Сейфуллин атындағы ҚазАТУ, Нұр-Сұлтан, Қазақстан
Ғылыми жетекші – А.Адамова

Жер мәселелерін спутниктік бейнелерді пайдаланып алдын алу. Жер үсті объектілерін мониторингілеу мақсатында жерді қашықтықтан зондтау деректерін қолдану, ауыл шаруашылығы жерлерінің, ландшафттың т.б жерлердің жай-күйі туралы ақпарат алуға ықпал етеді, ал геоақпараттық жүйелер ақпараттың барлық жиынтығын бақыланатын аумақтың электрондық (цифрлық) картасы, сондай-ақ әртүрлі агроландшафт объектілерінің байқалатын қасиеттерінің жай-күйі туралы ақпаратты енгізу, сақтау, өңдеу және шығару бағдарламалық құралдары мен әдістемелері түрінде ұсынуға мүмкіндік береді. Геоақпараттық жүйелердің (ГАЖ) және жерді қашықтықтан зондтау деректерін қолданудың көмегімен жаңа технологияларды, егіншіліктің техникалық құралдарын және мелиорацияны әзірлеу, жер қорының тозуын азайту жөнінде шаралар қабылдау үшін келешекте жақсы бағыт болуы мүмкін [1].

Қазіргі уақытта жердің тозуы, оның негізгі компоненті – топырақ құнарлылығын қоса алғанда, негативті әлеуметтік-экономикалық және экологиялық салдар елеулі қауіп болып табылады. Жер ресурстарына антропогендік әсер етудің күшеюі, экожүйелердің биоәртүрлілігін қысқарту, олардың климаттық өзгерістерге осалдығын арттыру, ұтымсыз басқару және жерді пайдалануды ұйымдастыру, жердің (топырақтың) өнімдік қабілетін төмендетіп қана қоймай, сонымен қатар олар ұсынған басқа да өмірлік маңызы бар экожүйелік қызметтерге теріс әсер етеді. БҰҰ – ның азық-түлік және ауыл шаруашылығы ұйымының деректері бойынша тозған жерлердің жалпы ауданы, құрлықтың 25% - дан астамын, ал жердің тозуына алып келетін жыл сайынғы жаһандық залал-шамамен 300 млрд АҚШ долларын құрайды [2].

Тозуға қарсы күрес жөніндегі іс-шараларды жүргізуді тежейтін басты себептердің бірі тозған жерлерді анықтау, картаға түсіру, жіктеу, есепке алу және бағалау процестерін жедел, дәл және аз оңтайлы технологияның болмауы болып табылады [3].

Осы сияқты мәселелердің алдын алу үшін ғарыштық суреттермен жұмыс жасау заманауи шешімдердің бірі болып табылады. Спутниктік бейнелерді қолдану аспектісінде негізгі мәселе болып, мониторинг деректерін өңдеу механизмдерінің жетілмегендігі болып табылады. Осыған байланысты ақпаратты енгізу, сақтау, өңдеу және жаңарту процесінің дұрыстығы ғана емес, сонымен қатар әртүрлі агроландшафтты бақылау мақсатында геоақпараттық жүйелерді пайдалану арқылы өңделген деректерді талдау және визуализациялау да өзекті болып табылады. Бүгінгі күні ГАЖ ақпараттарын табу және пайдалану жеңіл болып келеді. Әртүрлі Web порталдар кез-келген қолданушы үшін қолжетімді ғарыштық суреттерді ұсынады (кесте 1).

Кесте 1 – Ғарыштық суреттерді ұсынатын web порталдар.

Жерсеріктердің атауы	Ғарыш суреттерінің түрлері	Сипаттамасы	Сайт
USGS-NASA Landsat, IKONOS-2, OrbView-3	Оптикалық және радиолокациялық деректерден ауа райының спутниктік суреттеріне	Іздеу, алдын ала қарау және GIS деректерін тегін жүктеу үшін пайдалануға болады. Егер суреттерді өңдеу керек	earthexplorer .usgs.gov/