1) Які властивості повинна мати квазігрупа, щоб її можна було використовувати як будівельний блок для криптографічних схем і вона могла забезпечити надійний захист?

2) Як згенерувати та як обчислити велику кількість квазігруп?

3) Які особливості мають квазігрупи, отримані новим методом побудови?

4) Які є способи використання квазігруп як будівельні блоки криптографічних схем?

А. Мілева показала, що навіть квазігрупи малих порядків дуже придатні для застосування в криптографії [4]. Особливо це стосується квазігруп через їх структуру, особливості та велику кількість.

Сьогодні існує кілька класифікацій, які допомагають нам у виборі квазігруп, які мають властивості для ефективногоо застосування. Три основні класифікації отримані шляхом використання алгебраїчних властивостей квазігруп до класів ізотопних квазігруп, класів ізоморфних квазігруп і класів парастрофних квазігруп. Квазігрупи класифікуються на многовиди відповідно до тотожностей, яким вони задовольняють. Одна із таких класифікацій наведена в праці [5].

Список літератури.

1. *J. Denes and A. D. Keedwell. Some applications of non-associative algebraic systems in cryptology. Pure Mathematics and Applications, 12(2):147{195, 2001.*
2. *Shcherbacov V.A. Quasigroups in cryptology. Computer Science Journal of Moldova. 2009. Vol.17, No 2. P. 193-228.*
3. *Markovski S, Gligoroski D, and Bakeva V. Quasigroup and hash functions Proc. of the 6th ICDMA. Bansko. 2001. P. 43-50.*
4. *A. Mileva, "Cryptographic Primitives with Quasigroup Transformations," Ph.D. dissertation, University Ss. Cyril and Methodius, Skopje, Macedonia, 2010.*
5. *Sokhatsky F.M., Lutsenko A.V. Classification of quasigroups according to directions of translations II. Commentationes Mathematicae Universitatis Carolinae. 2021. Vol. 62, No 3. P. 309-323.*

УДК 004.5

Рудь О. С., студентка 2 курсу
спеціальності 122 «Комп'ютерні науки»,
Науковий керівник:
Потапова Н. А., к.е.н., доцент
кафедри інформаційних технологій

АНАЛІЗ ПОВЕДІНКИ ПРОЦЕСІВ НА ЗАСАДАХ ОБЧИСЛЮВАЛЬНИХ АЛГОРИТМІВ

Донецький національний університет імені Василя Стуса, м. Вінниця

Аналіз поведінки процесів на засадах обчислювальних алгоритмів - це використання математичних методів та алгоритмів для аналізу даних та

виявлення закономірностей у поведінці різних процесів. Це може бути застосовано в різних галузях, включаючи фізику, хімію, біологію, економіку, техніку та інші. Такий аналіз поведінки процесів включає у себе збір та аналіз даних, використання статистичних методів та алгоритмів машинного навчання для побудови моделей та прогнозування майбутнього поведінки процесів[1].

1. Аналіз поведінки процесів на засадах обчислювальних алгоритмів є важливою складовою багатьох сфер діяльності, включаючи науку, техніку та бізнес. Ось декілька тез, що характеризують цю тему:

2. Обчислювальні алгоритми використовуються для опису поведінки процесів у великій кількості дисциплін, включаючи математику, фізику, хімію, біологію, інформатику та інші.

3. Аналіз поведінки процесів на засадах обчислювальних алгоритмів може допомогти виявити проблеми та вдосконалити ефективність процесів. Наприклад, в індустрії алгоритми можуть бути використані для покращення виробничих процесів та зниження витрат.

4. Використання обчислювальних алгоритмів може допомогти зрозуміти складні процеси, які не можуть бути розглянуті без їх використання. Наприклад, в біології алгоритми можуть допомогти зрозуміти процеси, які відбуваються в клітинах та організмах.

5. Аналіз поведінки процесів на засадах обчислювальних алгоритмів може бути використаний для прогнозування майбутнього стану процесу та побудови моделей його розвитку. Це може бути корисним в багатьох галузях, включаючи економіку, фінанси та бізнес.

6. Розвиток нових обчислювальних алгоритмів дозволяє дослідникам та спеціалістам з різних галузей вирішувати нові завдання та проблеми, що раніше були недосяжні. Це може допомогти розвивати нові технології та забезпечувати наукові дослідження більш точними та ефективними. Наприклад, розробка нових алгоритмів машинного навчання дозволяє автоматизувати різноманітні процеси та прогнозувати складні явища, що важко або неможливо було робити раніше.

7. Розвиток обчислювальних алгоритмів допомагає спрощувати складні процеси та забезпечувати їх автоматизацію. Це дозволяє збільшувати продуктивність та знижувати витрати, зокрема у виробництві та бізнесі.

8. Використання обчислювальних алгоритмів для аналізу поведінки процесів дозволяє забезпечити точність та надійність дослідження. Наприклад, в медицині алгоритми можуть допомогти виявляти хвороби та прогнозувати результати лікування.

9. Однією з головних переваг розвитку обчислювальних алгоритмів є їх доступність та широке застосування в різних галузях. Це дозволяє спеціалістам з різних областей забезпечувати високий рівень точності та швидкості при вирішенні завдань та проблем[1].

Аналіз поведінки процесів на засадах обчислювальних алгоритмів також є важливим етапом розробки програмного забезпечення. Цей аналіз дозволяє зрозуміти, які процеси відбуваються в програмі, які ресурси вони використовують і як вони можуть бути оптимізовані для забезпечення кращої

продуктивності.

Один з підходів до аналізу поведінки процесів на засадах обчислювальних алгоритмів - це використання техніки профілювання. Профілювання дозволяє отримати детальну інформацію про те, як програма виконується, включаючи час, витрачений на виконання кожної функції, кількість викликів кожної функції та кількість виконаних інструкцій. Ця інформація може бути використана для виявлення проблем в продуктивності програми і визначення частин коду, які можуть бути оптимізовані. Інший підхід до аналізу поведінки процесів на засадах обчислювальних алгоритмів - це використання методів формальної верифікації[2].

Формальна верифікація – це процес математичної перевірки того, чи виконує програмний код задану специфікацію, тобто, чи робить програма те, що вона повинна робити. У процесі формальної верифікації використовуються різні методи та інструменти, що дозволяють довести або спростувати коректність програмного коду. Узагалі, формальна верифікація є важливим етапом в процесі розробки програмного забезпечення, що дозволяє підвищити його якість та надійність, зменшити ризики помилок та збільшити довіру користувачів до продукту[3].

Окрім цього, аналіз поведінки процесів на засадах обчислювальних алгоритмів може включати вивчення принципів оптимізації алгоритмів. Наприклад, можна вивчити різні алгоритми сортування, щоб знайти той, який працює найшвидше для конкретних потреб. Також можна вивчити принципи кешування, щоб покращити продуктивність програми.

Загалом, аналіз поведінки процесів на засадах обчислювальних алгоритмів дозволяє досліджувати та прогнозувати різноманітні процеси з точністю та швидкістю, які не можуть бути досягнуті за допомогою традиційних методів.

Список літератури:

1. *Призначення математичної статистики в дослідженнях – Українська педагогіка. URL: ukped.com/materialy/onpd/3055-pryznachennia-matematychnoi-statystyky-v-doslidzhenniakh.html*

2. Джонсон Теодор (2009). Профілювання даних.

3. Формальна Верифікація – Tezos Ukraine. URL: learn ua.tezos.org.ua/formal-verification