При забезпеченні швидкодії шифрування та дешифрування інформації важливе значення відіграють квазігрупи, в яких парастрофи виражаються через головну операцію і деяку функцію, яка названа функцією оборотності.

Було встановлено, що всього таких квазігруп є дев'ять многовидів [4]. Три з них були відомі, це ліві, праві IP квазігрупи та CIP квазігрупи. Їх застосування відображене в працях А. Кідвела[5] та В. Щербакова[3]. А шість многовидів є новими. Серед цих дев'яти многовидів є квазігрупи з властивістю схрещеної оборотності, які мають певні властивості, що роблять їх особливо придатними для застосування в криптографії. Зокрема в праці А. Кідвелла описано деякі застосування квазігруп з властивістю схрещеної оборотності з довгим оборотним циклом та побудовано приклад [5].

Список літератури

1. *Fryz, I.V., Sokhatsky, F.M. Block composition algorithm for constructing orthogonal n-ary operations. Discrete Math. 2017. Vol. 340. P. 1957-1966.* http://dx.doi.org/10.1016/j.disc.2016.11.012
2. *Markovski S, Gligoroski D, and Bakeva V. Quasigroup and hash functions Proc. of the 6th ICDMA. Bansko. 2001. P. 43-50.*
3. *Shcherbacov V.A. Quasigroups in cryptology. Computer Science Journal of Moldova. 2009. Vol.17, No 2. P. 193-228.*
4. *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.*
5. *Keedwell D. Crossed inverse quasigroups with long inverse cycles and applications to cryptography, Australasian J. of Comb. 1999. Vol. 20. P. 241-250.*

УДК 512.548

Фриз І.В., к.ф.-м.н., ст. викладач кафедри прикладної математики

ДЕЯКІ ВЛАСТИВОСТІ ОРТОГОНАЛЬНИХ ОПЕРАЦІЙ

Донецький національний університет імені Василя Стуса, м. Вінниця

Відомо, що ортогональність багатомісних операцій та гіперкубів знаходить своє застосування в теорії кодування та шифрування, а саме для побудови МДР-кодів (кодів з максимально допустимою відстанню), хеш-функцій, схем поділу секрету. Зокрема, у [1] описано зв'язок між ортогональністю гіперкубів (комбінаторний аналог багатомісних операцій), латинських гіперкубів (комбінаторний аналог багатомісних квазігруп) та МДР-кодів. Зокрема, відомим є факт, що квазігрупа еквівалентна МДР-коду відстані 2 [2].

З іншого боку саме поняття ортогональності є недостатньо вивченим, зокрема побудова ортогональних багатомісних операцій, а також побудова

квазігруп, які не розкладаються у безповторну композицію квазігруп меншої арності тощо. Існує декілька узагальнень бінарної ортогональності: n-арна ортогональність, сильна ортогональність, ретрактна ортогональність, перпендикулярність, які є пов'язаними між собою. Тут розглянемо одне із узагальнень – перпендикулярність, а саме обмежимося перпендикулярністю максимального типу, тобто у випадку коли операції мають однакову арність.

У [3] доведено, що оборотність повторної композиції двох операцій різної арності еквівалентна перпендикулярності двох операцій, а саме поняття перпендикулярності введено як узагальнення ортогональності бінарних операцій на випадок багатомісних операцій різної арності. На мові гіперкубів перпендикулярність означає ортогональність певних відповідних двовимірних зрізів гіперкубів.

n-арні операцій $f_1, f_2, \dots, f_k$, які визначені на множині Q, називаються ортогональними, якщо система

$$\{f_i(x_1, x_2, \dots, x_k) = a_i\}_{i=1}^{k}$$

має єдиний розв'язок для всіх $a_1, a_2, \dots, a_k \in Q$.

Нехай f – n-арна операція на множині Q,

$$\delta \coloneqq \{i_1, \dots, i_k\} \in \overline{1,n} := \{1, \dots, n\}, \qquad \{j_1, \dots, j_{n-k}\} \coloneqq \overline{1,n} \backslash \delta.$$

Операція $f_{(\bar{a},\delta)}$, де $\bar{a} \coloneqq \left(a_{j_1}, \dots, a_{j_{n-k}}\right)$, яка визначається рівністю

$$\mathrm{f}_{(\bar{a},\delta)}\left(x_{i_1}, \dots, x_{i_k}\right) \coloneqq f(y_1, \dots, y_k), \qquad \mathrm{y_i} \coloneqq \begin{cases} x_i, & \text{якщо } i \in \delta, \\ a_i, & \text{якщо } i \notin \delta \end{cases}$$

називається $(\bar{a}, \delta)$-ретрактом або δ-ретрактом операції f. Операції $f_{1;(\bar{a},\delta)}$, $f_{2;(\bar{a},\delta)}$,…, $f_{k;(\bar{a},\delta)}$ називаються подібними δ-ретрактами операцій $f_1, f_2, \dots, f_k$. k-вибірка n-арних операцій називається δ-ретрактно ортогональною [4], якщо всі вибірки подібних δ-ретрактів цих операцій є ортогональними.

Поняття перпендикулярності максимального типу із [3] наведемо використовуючи поняття ректрактної ортогональності: n-арні операції g і h називаються перпендикулярними типу $(\iota, \iota; m)$, якщо вони є δ-ретрактно ортогональними для всіх δ таких, що $|\delta| = 2$ і $m \in \delta$. Зокрема, із [3] відомо: якщо операції є перпендикулярними максимального типу, то вони є ортогональними.

Твердження 1. Кожен максимальний тип перпендикулярності має тип виду $(\iota, \sigma; m)$ з точністю до перейменування змінних, де $\sigma \in S_n$.

Твердження 2. Якщо f є квазігрупою, де

$$f(x_1, \dots, x_n) = g(x_1, \dots, x_{m-1}, h(x_{1\sigma}, \dots, x_{n\sigma}), x_{m+1}, \dots, x_n),$$

то такі перпендикулярності є еквівалентними:

1) g і ${}^{(J_\sigma(m))}h$ типу $(\iota, \sigma; m)$, де $J_\sigma(m) \coloneqq |\{1\sigma, \dots, m\sigma\}|$, ι – тотожне перетворення із S_n;

2) f і h типу $(\iota, \sigma; m)$;

3) ${}^{(m)}g$ і ${}^{(m)}h$ типу $(\iota, \iota; m)$.

Теорема 1. Кожна пара перпендикулярних операцій максимального типу є продовжувальною до перпендикулярних операцій не максимального типу.

Список літератури

1. *Ethier J.T., Mullen G.L. Strong forms of orthogonality for sets of hypercubes. Discrete Math. 2012. Vol. 312, Iss. 12-13. P. 2050-2061.*
2. *Couselo E., Gonzalez S., Markov V., Nechaev A. Recursive MDS-codes and recursively differentiable quasigroups. Discrete Math. Appl. 1998. Vol. 8, Iss. 3. P. 217-246.*
3. *Sokhatsky F.M., Fryz I.V. Invertibility criterion of composition of two multiary quasigroups. Comment. Math. Univ. Carolin. 2012. Vol. 53, №3. P. 429-445.*
4. *Fryz I.V. Orthogonality and retract orthogonality of operations. Bul. Acad.Stiinte Repub. Mold. Mat. 2018. №1(86). P. 24-33.*

УДК 519.248

Цвик В.В., здобувач освіти,
Крикун І.Г., к.ф.-м.н., доцент, доцент кафедри прикладної математики

SIR-МОДЕЛЬ РОЗВИТКУ ЕПІДЕМІЙ

Донецький національний університет імені Василя Стуса, м. Вінниця

Вступ. Інфекційні хвороби та їх спалахи у формі епідемій переслідують людство весь час існування. Тому питання моделювання динаміки розповсюдження інфекційних хвороб завжди було і буде актуальним. Пандемія ж коронавірусу, яка змінила життя всього людства, додатково підвищила наш інтерес до цього питання.

Огляд останніх публікацій. Одним з найефективніших підходів до аналізу динаміки складних систем є прийом, коли вся система розбивається на частини та при цьому задаються закони для швидкостей обміну речовиною між цими частинами. Ці частини цілого (наприклад, всієї популяції) отримали назву «компартменти» (від англ. compartment – комірка, обмежений простір), а такий прийом отримав назву «компартментальний аналіз».

Вперше компартментальний аналіз у вивченні динаміки поширення інфекційних хвороб було застосовано англійськими математиками Вільямом Кермаком та Андерсоном Маккендріком (1927, 1932). Подальші дослідження як правило використовують моделі Кермака – Маккендріка та їх узагальнення.

Моделюванню динаміки епідемій інфекційних хвороб присвячено чимало недавніх публікацій, серед яких виділимо [1; 2]

SIR-модель Кермака-Маккендріка. Отже, першою компартментальною моделлю в динаміці інфекційних хвороб була модель Кермака-Маккендріка (1927), в якій люди ділилися на три групи: тих, хто може захворіти, хворих і тих, хто одужав або має імунітет.

В подальшому такі моделі отримали назву SIR-моделі від англомовної абревіатури SIR = Susceptible-Infected-Recovered, від розбиття всієї популяції на три частини: *S* (susceptible) – вразливі, тобто без імунітету до хвороби;