при $p=\max\left(2+m_n,\max\limits_{1\le i\le n} q_i\right)$, будь-якому $0<\tau<T$, і будь-якій пробній функції $\varphi:\varphi\in W^{1,2}(0,T;L^2(\Omega_T))\cap L^2(0,T;\overset{o}{W}{}^{1,2}(\Omega))$, й будь-якій функції $\psi\in C^1(\overline{\Omega_T})$), яка обертається в 0 в околі точки $(0,0)$.

Це гарантує, що $\lim\limits_{\tau\to 0}\int\limits_{\Omega} u(\mathrm{x},\tau)\,\psi^p\varphi\mathrm{dx}=0$ і всі інтеграли в тотожності (5) є збіжними.

Сформулюємо головний результат.

Теорема 1 Нехай виконані умови (3), (4). Тоді існує додатня стала c, яка залежить тільки від ν_1, ν_2, n, $m_1,...,m_n$, $q_1,...,q_n$, що справедлива наступна оцінка

$$u(x,t)\le c\left(\sum_{i=1}^{n-1}|\mathrm{x}_i|^{\frac{2}{(2-\mathrm{m})\mathrm{q}+(\mathrm{q}-2)m_i}}+t^{\frac{1}{q(1-m)+2(q-1)}}\right)^{q-2}$$

для $(x,t)\in\Omega_T\setminus\{(0,0)\}$.

Список літератури

1. *Garcia-Melian J. Large solutions to an anisotropic quasilinear elliptic problem / J. Garcia-Melian, J.D. Rossi, J.C. Sabina de Lis // Annali di Matematica Pura ed Applicata. – 2010. – Vol. 189. – P. 689–712.*
2. *Skrypnik I.I. Removability of isolated singularities for anisotropic elliptic equations with gradient absorption / I.I. Skrypnik // Israel Journal of Mathematics. — 2016. — Vol. 215. — P. 163—179.*
3. *Skrypnik I.I. Removability of isolated singularity for anisotropic parabolic equations with absorption / I.I. Skrypnik // Manuscr. Math. — 2013. — Vol. 140. — P. 145—178.*
4. *Shan (Savchenko) M. A. Keller-Osserman estimates and removability result for the anisotropic porous medium equation with gradient absorption term / M. A. Shan, I.I. Skrypnik // Mathematische Nachrichten. — 2019. — Vol. 292. — P. 436—453.*

УДК 546.07

Сохацький Ф.М., д.ф.-м.н., доцент, професор кафедри прикладної математики,
Луценко А.В., аспірант

КВАЗІГРУПИ І ЗАХИСТ ІНФОРМАЦІЇ

Донецький національний університет імені Василя Стуса, м. Вінниця

Захист інформації на сьогоднішній день є актуальним не лише у військовій справі, а й в сучасних галузях економіки, таких як банківська справа, інтернет, бази даних тощо. Кожна з задач, які виникають має свій час секретності і свої

вимоги до швидкодії шифрування та дешифрування. А звідси випливає застосування різних галузей математики, таких як теорій чисел, груп, кілець, полів, еліптичних кривих, до розв'язання цих проблем.

Причому майже всі відомі конструкції кодів, криптографічних алгоритмів і систем шифрування застосовують асоціативні алгебраїчні структури. З розвитком криптографії та пошуком нових методів захисту інформації все більше уваги приділяється застосуванню теорії неасоціативних об'єктів, таких як теорія квазігруп та їх узагальнення.

Шлях коли шифрування відбувається вибіркою символів іншою вибіркою символів означає побудову системи ортогональних операцій, тобто підстановки на множині вибірок. Методи побудови системи ортогональних операцій були запропоновані Г. Белявською та узагальнені І. Фриз та Ф. Сохацьким у праці [1]. Зокрема, вони запропонували блочно-композиційний алгоритм для побудови ортогональних операцій, який містить композиційний алгоритм для побудови операцій з ортогональними ретрактами і блочно-рекурсивний алгоритм для побудови багатомісних ортогональних операцій з використанням деякого розбиття набору змінних на блоки.

Результати, отримані в [1] дозволяють побудувати велику кількість підстановок над Q^n, що створює велику ймовірність побудови односторонніх функцій, які є математичною основою для побудови шифрів з відкритим ключем.

Квазігрупи мають багату історію застосування в криптографії. В роботах М. Глухова, В. Щербакова, А. Крапежа, Г. Муллена та інших наведені досить повні огляди застосування квазігруп в криптографії.

Зокрема, А. Крапеж, запропонував метод квазігрупового шифрування з парастрофами, заснований на розбиванні звичайного тексту на блоки різного розміру і шифрування його, використовуючи різні парастрофи однієї квазігрупи.

С. Марковський та ін. запропонували метод для побудови потокового шифру, використовуючи властивість квазігрупи, яка є алгеброю з трьома операціями. Також запропонували новий клас криптографічних хеш-функцій зі змінною вихідною довжиною, на основі визначеної односторонньої функції. Цей клас визначається за допомогою квазігруп і квазігрупових перетворень рядків [2].

Метью Дж. Бетті виявив нове використання квазігруп та продемонстрував квазігруповий блочний шифр як засіб шифрування простого тексту, а також генерування випадкових даних для використання в потоковому шифрі. Також оцінив криптосистему за допомогою стандартних інструментів і виконав алгебраїчний та лінійний криптоаналіз системи.

Щербаков В. у праці [3] запропонував модифікації криптоалгоритму на основі квазігрупи Марковського. Деякі з цих модифікацій засновані на системах ортогональних n-арних групоїдів. Зокрема, було побудовано потокові шифри на основі Т-квазігруп.

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