КОМП'ЮТЕРНІ СИСТЕМИ І МЕРЕЖІ

Т. 1, № 1, 2019

https://doi.org/10.23939/csn2019.01.063

УДК 681.322

ЕЛЕМЕНТИ ВЕЛИКОГО МУЛЬТИПЛІКАТИВНОГО ПОРЯДКУ В РОЗШИРЕНИХ СКІНЧЕННИХ ПОЛЯХ НА ОСНОВІ МОДИФІКОВАНОГО ПІДХОДУ ГАО

Б. Р. Попович

Національний університет "Львівська політехніка",
кафедра спеціалізованих комп'ютерних систем

© Попович Б. Р., 2019

Підхід Гао побудови елементів великого порядку в довільних скінченних полях полягає у виборі зручного полінома, який задає розширення початкового простого поля. Цей вибір залежить від одного полінома-параметра. Тому вказаний підхід можна розглядати як використання опису скінченного поля з одним ступенем свободи. У цій роботі досліджено можливість поліпшення нижніх меж для порядків елементів у скінченних полях загального вигляду з використанням двох ступенів свободи. Виконано комп'ютерні обчислення в середовищі Maple, які б показали можливі виграші у цьому разі, та наведено відповідні результати. Елементи великого мультиплікативного порядку використовують у низці криптографічних примітивів (протокол Діффі-Хелмана, криптосистема Ель-Гамаля з відкритим ключем, цифровий підпис Ель-Гамаля).

Ключові слова: криптографічний захист інформації, скінченне поле, порядок елемента, ступінь свободи.

Вступ

Сьогодні важливими є завдання забезпечення конфіденційності, цілісності й автентичності інформації та криптографічний захист інформаційних зв'язків між компонентами сучасних комп'ютерних систем і мереж. У цій роботі розглядаємо один із аспектів захисту інформації, пов'язаний із реалізацією протоколу Діффі-Геллмана – узгодження таємного ключа через відкритий канал зв'язку та використанням певних алгебраїчних структур, які називають скінченними полями (полями Галуа) [5, 6].

Окреслення проблеми

Скінченне поле з p елементів позначаємо через F_p, а через F_{p^n} – розширення поля F_p степеня n. Твірні мультиплікативної групи $F_{p^n}^*$ називають примітивними елементами. Далі використано такі позначення: m – найближче більше ціле число до величини $\log_p n$, $l = p^m$, найменший степінь p більший або дорівнює n, $d = 2m$, t – найближче менше ціле число до величини $\log_d n$.

Відкрите питання: знайти ефективний алгоритм побудови примітивних елементів у скінченних полях. Алгоритм ефективний, якщо він поліноміальний, тобто час його виконання

Lviv Polytechnic National University Institutional Repository http://ena.lp.edu.ua

дорівнює $\log(p^n)^{O(1)}$ арифметичних операцій у F_{p^n}. Сьогодні задачу ефективної побудови примітивного елемента заданого скінченного поля обчислити важко [6]. Тому розглядають менш претензійне питання: збудувати елемент доказово великого мультиплікативного порядку. Визначення Гао [4]: під елементами "великого порядку" в F_{p^n} розуміємо елементи, мультиплікативні порядки яких повинні бути більші від будь-якого полінома від $\log(p^n)$, де p^n стає великим. У цьому разі не можна не обчислювати точний порядок елемента: достатньо отримати нижню оцінку для порядку.

Ділянки застосування елементів великого порядку в скінченних полях є такими [5, 6]: криптографія (протокол Діффі-Геллмана, криптосистема Ель-Гамаля з відкритим ключем, цифровий підпис Ель-Гамаля); завадостійке кодування (зокрема, під час побудови БЧХ-кодів); генератори псевдовипадкових чисел (різні степені елемента великого порядку можна розглядати як послідовність псевдовипадкових чисел); доведення простоти чисел [1]. Застосування елементів великого мультиплікативного порядку в криптографії ґрунтується на так званій задачі дискретного логарифмування в будь-якій скінченній циклічній групі.

Питання побудови елементів великого мультиплікативного порядку розглядають і для загальних [3, 4, 10, 11], і для часткових [2, 8, 9] випадків скінченних полів.

Завдання дослідження

Гао [4] дав алгоритм побудови елементів великого порядку для загальних розширень F_{p^n} скінченних полів F_p. Вказаний підхід ґрунтується на запропонованому ним, але ще не доведеному припущенні: для довільного натурального числа n існує поліном $g(x) \in F_p[x]$ степеня щонайбільше $d = 2m$ такий, що $x^l - g(x)$ має нерозкладний дільник $f(x)$ степеня n.

Наведене припущення перевірене в [4] для $p = 2$ та $n \le 300$. У праці [11] виконано обчислення і для скінченних полів характеристики 2 (для $p = 2$ та $300 < n \le 525$), і більшої характеристики (для $p = 3$ та $n \le 300$, для $p = 5$ та $n \le 100$). Припущення підтверджено і для таких випадків.

У цій роботі досліджуємо подальшу можливість поліпшення нижніх меж для порядків елементів у скінченних полях загального вигляду. Для цього пробуємо вийти за межі підходу Гао. Завданням роботи є узагальнення підходу Гао (моделі з одним ступенем свободи) із введенням двох ступенів свободи та виконання комп'ютерних обчислень, які б показали можливі виграші у цьому разі.

Розв'язання задачі

Узагальненням підходу Гао (моделі з одним ступенем свободи) є модель, коли $f(x)$ є дільником полінома у формі $h(x)x^{p^m} - g(x)$, де максимум степенів поліномів $g(x)$ та $h(x)$ є невеликим. Цей опис можна назвати описом розширеного скінченного поля з двома ступенями свободи. У цьому разі підбираємо поліноми $g(x)$ та $h(x)$. Завдяки цьому елементом великого порядку залишається елемент x.

Модифікований підхід Гао схематично проілюстровано на рис. 1. Твірним елементом у вказаній схемі є елемент розширеного поля, що рівний x. Щоб конкретно задати скінченне поле з p^n елементів крім p та n потрібно задати нерозкладний над F_p поліном $f(x)$ степеня n. Як відомо [5, 6], вибір цього полінома неоднозначний. Власне модифікований підхід Гао полягає в такому: вибрати поліном $f(x)$ так, щоб він ділив "зручний" поліном $h(x)x^l - g(x)$. Чи можна це завжди робити, є узагальненим припущенням. Щоб вибрати поліном $f(x)$, потрібно також підібрати поліноми $g(x)$ та

Lviv Polytechnic National University Institutional Repository http://ena.lp.edu.ua

$h(x)$. Тоді у вказаному полі виконується рівність $x^l = \dfrac{g(x)}{h(x)}$. Нагадаємо, що в початковому підході поліном $f(x)$ ділив "зручний" поліном $x^l - g_1(x)$ та була справедлива рівність $x^l = g_1(x)$.

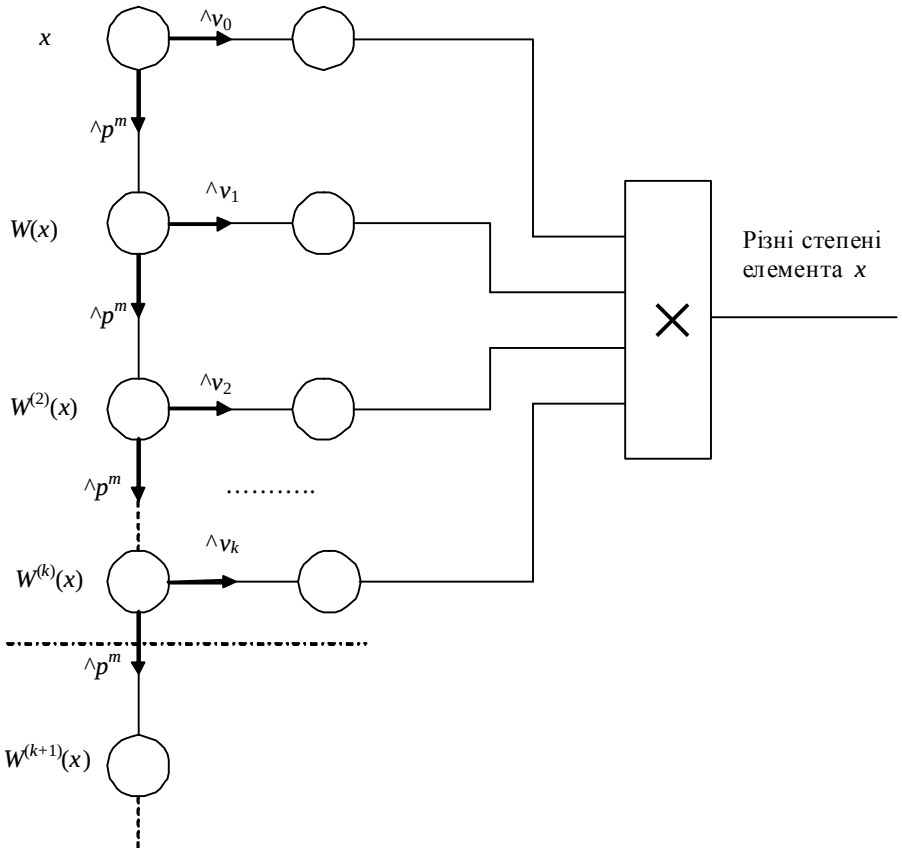

Рис. 1. Отримання різних степенів елемента x у модифікованому підході Гао

Неважко показати, використовуючи властивості елементів поля F_{p^n}, що для будь-якої раціональної функції (відношення двох поліномів) $W(x) = \dfrac{g(x)}{h(x)} = \dfrac{\sum_{i=0}^{s} g_i x^i}{\sum_{j=0}^{t} h_j x^j}$ з коефіцієнтами з поля F_p справедлива рівність $(W(x))^l = W(W(x))$.

Ґрунтуючись на вказаній рівності, утворюємо з елемента $x = W^{(0)}(x)$ піднесенням до степеня l елемент $W(x) = W^{(1)}(x)$. Далі утворюємо з останнього піднесенням до степеня l елемент $W(W(x)) = W^{(2)}(x)$. Продовжуючи аналогічно, отримуємо нескінченну послідовність елементів $W^{(i)}(x), i = 0,1,....$ У праці [12] доведено, що всі елементи цієї послідовності є мультиплікативно незалежними. З них беремо лише перших k, де k задовольняє умову $d^k < \dfrac{n}{2}$. Виконання останньої умови необхідне, бо з перших k елементів утворюємо всеможливі добутки з чисельником і знаменником степеня меншого $\dfrac{n}{2}$. Оскільки кільце $F_p[x]$ має однозначний розклад на прості множники, то всі утворені добутки-дроби різні, а значить вони різні й за модулем полінома $f(x)$, тобто в полі F_{p^n}. Очевидно, що всі вони є степенями елемента x.

Lviv Polytechnic National University Institutional Repository http://ena.lp.edu.ua

Для отримання нижньої межі для порядку елемента x потрібно оцінити їх кількість. Це відома комбінаторна задача знаходження кількості розв'язків лінійного діофантового рівняння. Найкращу відому сьогодні нижню межу для кількості розв'язків наведено в [7]. Її модифікацію $\binom{n+t-1}{t}\prod_{i=0}^{t-1}\frac{1}{d^i}$ для побудови елементів великого порядку отримано в [10].

Враховуючи наведені міркування, бачимо що істотним моментом у модифікованому підході Гао є виконання узагальненого припущення про існування відповідних поліномів $g(x)$ та $h(x)$. Виконано дослідження з використанням комп'ютерних обчислень наведеної другої моделі для випадку $p=2$ та $2<n\le 1000$ та порівняння результатів із першою моделлю (початковий підхід Гао). З'ясовано, що здебільшого друга модель дає змогу отримати менші степені поліномів і, як наслідок, покращити нижню межу для порядку елемента, наведену раніше.

Найчастіше виникає ситуація, коли в другому описі поліном $g(x)$ дорівнює 1, а степінь полінома $h(x)$ менший від степеня полінома $g_1(x)$ в першому описі (див. рис. 2).

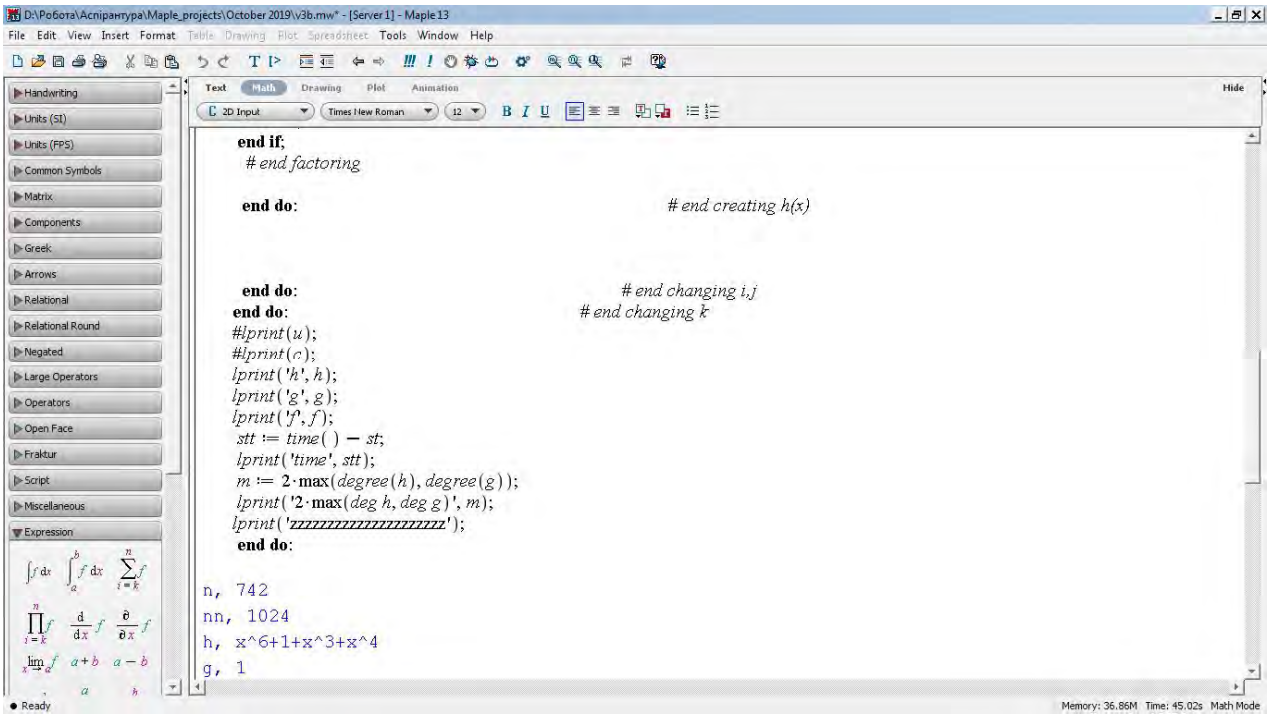

Рис. 2. Вікно середовища Maple з обчисленими поліномами g(x) та h(x) (g(x)=1)

Наприклад, при n=997, $m=10$, $p^m=1024$, в першому описі маємо $g_1(x)=x^{13}+x^8+x^7+x^6+x^5+x^3+x+1$, а в другому описі маємо $h(x)=x^6+x^5+x^4+x^3+x^2+1$, $g(x)=1$. Це означає, що в цьому разі маємо не два ступені свободи, а, як і раніше в підході Гао, один ступінь свободи. Проте поліном, який підбирали, тепер знаходиться біля степеня елемента x. Проте рівність $x^l=\frac{1}{h(x)}$ можна переписати у вигляді $(x^{-1})^l=h(x)$. Тобто, розглядаючи елемент x^{-1} замість елемента x, отримуємо те саме, що і в підході Гао. З огляду на протокол Діффі-Геллмана немає різниці, який елемент великого порядку брати.

Водночас виникає і ситуація, коли обидва поліноми $g(x)$ та $h(x)$ не дорівнюють одиниці (див. рис. 3) та їх степені невеликі порівняно зі степенем $g_1(x)$. Тоді справді маємо реалізовані два ступені свободи. Також є невелика кількість випадків, коли початковий підхід Гао дає кращий результат.

Lviv Polytechnic National University Institutional Repository http://ena.lp.edu.ua

Деякі з отриманих результатів наведено в табл. 1. Точніше, вказано поліноми $g(x), h(x) \in F_p[x]$ (p=2) з найменшою сумою степенів такі, що $h(x)x^l - g(x)$ має нерозкладний дільник степеня n, та поліном $g_1(x) \in F_p[x]$ найменшого степеня такий, що $x^l - g_1(x)$ має нерозкладний дільник степеня n. Обчислення виконано у середовищі моделювання Maple 13.

Таблиця 2

Результати комп'ютерних експериментів

p	n	l	$h(x)$	$g(x)$	$g_1(x)$
2	739	2^{10}	$x^5+x^4+x^2+1$	x^2+x+1	x^9+x^4+x+1
2	742	2^{10}	$x^6+x^4+x^3+1$	1	$x^{11}+x^9+x^8+x^7+x^6+x^5+x^4+x^2+x+1$
2	956		x^6+x+1	1	$x^9+x^6+x^4+x^2+1$
2	960	2^{10}	$x^8+x^5+x^4+1$	x^3+x^2+x+1	$x^{13}+x^{10}+x^9+x^8+x^2+x+1$
2	997	2^{10}	$x^6+x^5+x^4+x^3+x^2+1$	1	$x^{13}+x^8+x^7+x^6+x^5+x^3+x+1$
2	1000	2^{10}	x^5+x^2+1	x^2+x+1	$x^{11}+x^8+x^5+x^3+1$

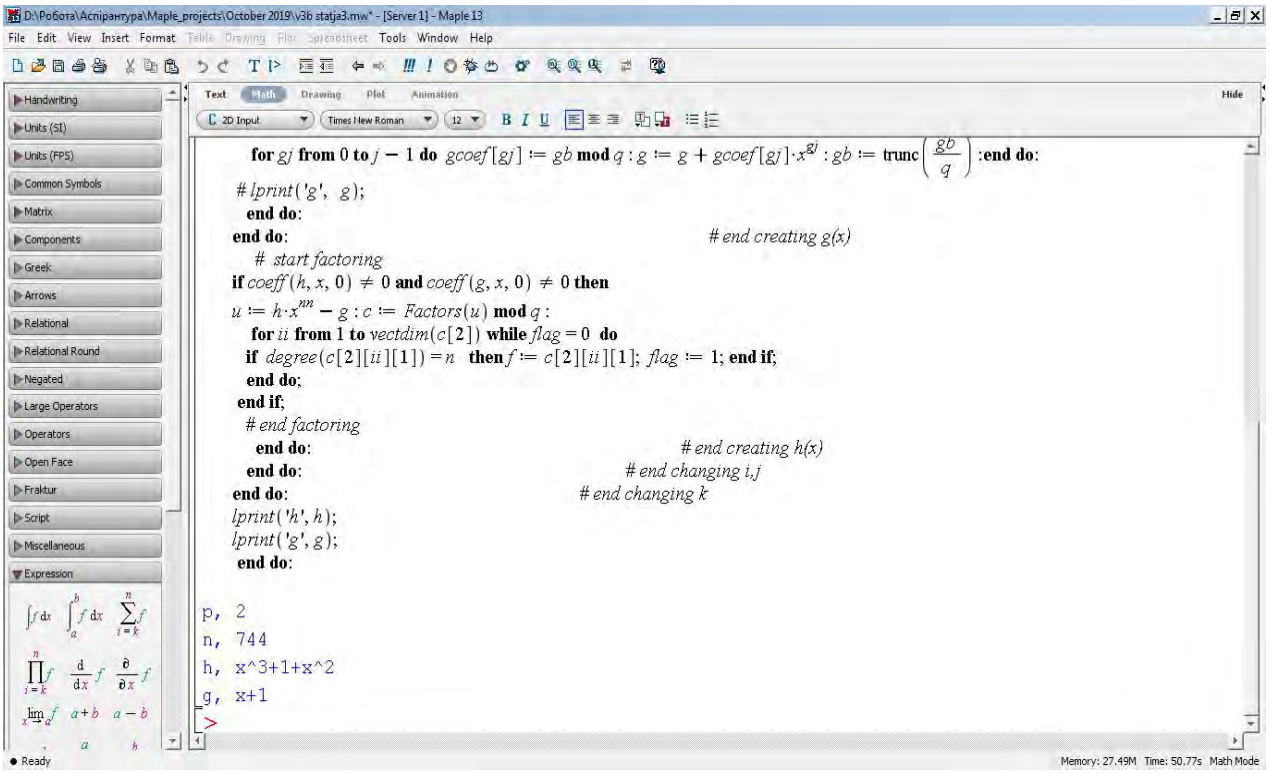

Рис. 3. Вікно середовища Maple з обчисленими поліномами g(x) та h(x)

Висновки

Здійснено аналіз особливостей модифікованого підходу Гао, який у разі справедливості певного узагальненого припущення дає поліноміальний алгоритм побудови елементів великого порядку в мультиплікативній групі довільного скінченного поля. Такі елементи використовують у низці криптографічних примітивів (протокол Діффі-Геллмана, криптосистема Ель-Гамаля з відкритим ключем, цифровий підпис Ель-Гамаля). Виконано дослідження з використанням комп'ютерних обчислень вказаного модифікованого підходу (моделі з двома ступенями свободи) для випадку $p = 2$ та $2 < n \le 1000$ та порівняння результатів із початковим підходом Гао (моделі з

Lviv Polytechnic National University Institutional Repository http://ena.lp.edu.ua

одним ступенем свободи). З'ясовано, що здебільшого введення додаткового ступеня свободи дає змогу поліпшити нижню межу для порядку елемента.

Список літератури

1. Agrawal M., Kayal N., Saxena N. PRIMES is in P // Annals of Mathematics, vol. 160, no. 2, 2004, p. 781–793.

2. Ahmadi O., Shparlinski I. E., Voloch J. F. Multiplicative order of Gauss periods // International Journal of Number Theory, vol. 6, no. 4, 2010, p. 877–882.

3. Conflitti A. On elements of high order in finite fields // in Cryptography and Computational Number Theory, vol. 20 of Progr. Comput. Sci. Appl. Logic, Birkhauser, Basel, 2001, p. 11–14.

4. Gao S. Elements of provable high orders in finite fields // Proceeding of American Math. Soc., vol. 127, no. 6, 1999, p. 1615–1623.

5. Lidl R., Niederreiter H. Finite Fields. – Cambridge: Cambridge University Press, 1997. 755 P.

6. Mullen G. L., Panario D. Handbook of finite fields. Boca Raton: CRC Press, 2013. 1068 P.

7. Lambe T. A. Bounds on the Number of Feasible Solutions to a Knapsack Problem // SIAM Journal of Applied Mathematics, vol. 26, no. 2, 1974, p. 302–305.

8. Popovych R. Elements of high order in finite fields of the form $F_q[x]/\Phi_r(x)$ // Finite Fields and Their Applications, vol. 18, no. 4, 2012, p. 700–710.

9. Popovych R. Elements of high order in finite fields of the form $F_q[x]/(x^m-a)$ // Finite Fields and Their Applications, vol. 19, no. 1, 2013, p. 86–92.

10. Popovych R. On elements of high order in general finite fields // Algebra and Discrete Mathematics, vol. 18, no. 2, 2014, p. 295–300.

11. Popovych B. Kompyuterna perevirka prypushchennya Gao, povyazanogo z otrymannyam elementiv velykogo poryadku v skinchennuch polyakh // Lvivska politechnika, Kompyuterni systemy ta merezhi, No. 905, 2018, s. 108–110.

12. Young M. On the multiplicative independence of rational iterates, Preprint, 2018, available at https://arxiv.org/abs/1708.00944.

ELEMENTS OF HIGH MULTIPLICATIVE ORDER IN EXTENDED FINITE FIELDS ON A BASE OF MODIFIED GAO APPROACH

B. Popovych

Lviv Polytechnic National University,
Specialized computer system department

© Popovych B., 2019

The Gao approach to construction of high order elements in arbitrary finite fields is to choose a convenient polynomial, which defines an extension of an initial prime field. This choice depends on one polynomial-parameter. That is why the mentioned approach can be considered as using of a finite field description with one degree of freedom. We explore in the paper the possibility of improvement of lower bound on element orders in finite fields of general form with using of two degrees of freedom. We have performed computer calculations in Maple environment, that would show possible winnings in this case, and given the correspondent results. Elements of high multiplicative order are used in a series of cryptographic primitives (Diffie-Hellman protocol, El-Gamal public key cryptosystem, El-Gamal digital signature).

Key words: cryptographic information protection, finite field, order of element, degree of freedom.

Lviv Polytechnic National University Institutional Repository http://ena.lp.edu.ua