УДК 512.624

Р. Б. Дунець, Р.Б. Попович
Національний університет "Львівська політехніка"
кафедра спеціалізованих комп'ютерних систем
Б.Р. Попович
Львівський національний медичний університет ім.. Д. Галицького
кафедра медичної інформатики

ЕЛЕМЕНТИ ВЕЛИКОГО МУЛЬТИПЛІКАТИВНОГО ПОРЯДКУ: ПОБУДОВА ТА ЗАСТОСУВАННЯ

Розглянуто питання явної побудови в скінченних полях елементів великого мультиплікативного порядку та їх застосування.

They consider the question of explicit construction in finite fields elements of high multiplicative order and their applications.

Забезпечення конфіденційності, цілісності та автентичності інформації, криптографічний захист інформаційних зв'язків між компонентами кіберфізичних систем є актуальною задачею.

У даній роботі розглядаємо один з аспектів захисту інформації, пов'язаний з використанням певних алгебраїчних структур, які називають скінченними полями або полями Галуа [10, 11].

Скінченне поле з q елементів позначаємо через F_q, а через F_{q^n} - розширення поля F_q степеня n. Твірні мультиплікативної групи $F_{q^n}^*$ називають примітивними елементами.

Відкрите питання: знайти ефективний алгоритм побудови примітивних елементів у скінченних полях. Алгоритм ефективний, якщо він поліноміальний, тобто час його виконання дорівнює $\log(q^n)^{O(1)}$ арифметичних операцій у F_{q^n}. На сьогодні задача ефективної побудови примітивного елемента заданого скінченого поля є обчислювально важкою.

Послаблення задачі про примітивний елемент:

У низці прикладних застосувань із використанням скінченних полів часто потрібні елементи великого порядку [10, 11]. В ідеалі хотілось би мати можливість отримувати примітивний елемент для будь-якого скінченого поля. Проте, якщо не маємо розкладу порядку мультиплікативної групи поля на прості множники, невідомо як досягти мети. Тому розглядають менш претензійне питання: збудувати елемент доказово великого мультиплікативного порядку. Визначення Гао [6]: під елементами "великого порядку" в F_{q^n} розуміємо елементи, мультиплікативні порядки яких повинні бути більші від від будь-якого полінома від $\log(q^n)$, де q^n прямує до нескінченості. У цьому випадку не вимагається обчислити точний порядок елемента: достатньо отримати нижню оцінку для порядку.

Області застосування елементів великого порядку в скінченних полях:

- криптографія (протокол Діффі-Хелмана, криптосистема Ель-Гамаля з відкритим ключем);
- завадостійке кодування (зокрема, при побудові БЧХ-кодів);

- генератори псевдовипадкових чисел (різні степені елемента великого порядку можна розглядати як послідовність псевдо випадкових чисел);

- доведення простоти чисел.

Застосування елементів великого мультиплікативного поряку в криптографії грунтується на так званій задачі дискретного логарифмування в будь-якій скінченній циклічній групі.

Нехай G скінченна циклічна група, яка має q елементів, з твірним елементом g. Використовуючи послідовні піднесення до квадрату, можна швидко (за поліноміальний час) обчислити $Y = g^X$ для будь-якого додатного цілого числа $1 \le X \le q-1$. Вважається, що маючи якийсь Y обчислювально складно знайти дискретний логарифм від нього за основою g, тобто число X. Іншими словами, функція $f(X) = g^X$ є однонапрямленою. Проте, доведення цього на сьогодні немає.

Виходячи із задачі дискретного логарифмування переважно розглядають такі дві криптографічні схеми.

1) Протокол Діффі-Хелмана

Як можуть два користувачі узгодити таємний ключ (можливо, для криптосистеми з таємним ключем) через відкритий канал зв'язку ?

Користувачі погоджують G скінченну циклічну групу, яка має q елементів, та її твірний елемент g. Як G, так і g, є відкритими.

Користувач A: вибирає випадкове число $1 \le a \le q-1$, обчислює g^a та пересилає значення g^a користувачу B.

Користувач B: вибирає випадкове число $1 \le b \le q-1$, обчислює g^b та пересилає значення g^b користувачу A.

Користувач A обчислює $(g^b)^a$.

Користувач B обчислює $(g^a)^b$.

Тепер як користувач A, так і користувач B мають елемент групи G рівний g^{ab}, який може слугувати як узгоджений таємний ключ.

2) Криптосистема Ель-Гамаля (криптосистема з відкритим ключем)

Нехай G скінченна циклічна група, яка має q елементів, з твірним елементом g. Як G, так і g, є відкритими.

Кожен користувач U: вибирає випадкове число $1 \le a \le q-1$ - секретний ключ для дешифрування. Тоді обчислює g^a і виставляє його – це публічний ключ цього користувача..

Щоб переслати таємне повідомлення P користувачу U,: слід вибрати випадкове число k, тоді обчислити та переслати пару значень $\beta_1 = g^k, \beta_2 = P(g^a)^k$.

Кристувач U виконує дешифрування згідно з таким виразом $P = \beta_2(\beta_1)^{-a}$.

Зауважимо, що не обов'язково g мусить бути твірним елементом групи G. Перша та друга описані криптографічні схеми працюють для будь-якого випадкового елемента g.

Разом з тим їх стійкість до зламування залежить від мультиплікативного порядку елемента g. Цей порядок елемента у вибраній скінченній циклічній групі мусить бути достатньо великим.

У криптографії можливе застосування як G таких скінченних циклічних груп:

1) Мультиплікативна група $Z_p^* = \{0,1,..., p-1\}$ відносно множення за модулем великого простого числа p. Це аналогічно до системи шифрування з відкритим ключем RSA.

2) Еліптична крива $E(F_q)$ над скінченним полем F_q. Її переважно записують не в мультиплікативній, а в адитивній формі. Така крива - це множина пар (x, y) елементів вибраного поля, що задовольняють афінне рівняння еліптичної кривої в нормальній формі Веєрштраса

$$y^2 + xy = x^3 + Ax^2 + B,$$

де $A, B \in F_q$, $B \neq 0$, разом із приєднаною нескінченною віддаленою точкою *O*. Пара (x, y) елементів основного поля називається афінними координатами точки еліптичної кривої. Нескінченно віддалена точка *O* не має афінних координат. Елементи A, B основного поля називаються коефіцієнтами рівняння еліптичної кривої. Число точок еліптичної кривої разом з нескінченною точкою називається порядком еліптичної кривої.

3) Мультиплікативна група скінченного поля $F_{q^n}^*$

Питання побудови елементів великого мультиплікативного порядку розглядають як для загальних, так і для спеціальних скінченних полів. Для часткових випадків скінченних полів можна збудувати елементи, що мають набагато більші порядки. Огляд отриманих у цій області результатів станом на початок 2012 року наведений в [11 , розділ 4.4] (розділ написаний Волохом).

Розглядаємо отримані оцінки знизу мультиплікативного порядку елементів для часткових класів скінченних полів.

1. Елементи великого порядку в скінченних полях вигляду $F_q(\theta) = F_{q^{r-1}} = F_q[x]/(x^{r-1} + ... + x + 1)$ (на основі циклотомічних поліномів)

Розширення, пов'язані з поняттям гауссового періоду, розглянуті в [1, 7-9, 12, 14, 22]. Нижня границя на порядок дорівнює $\exp(\Omega(\sqrt{m}))$.

2. Елементи великого порядку в скінченних полях вигляду $F_q[x]/(x^m - a)$ (на основі поліномів Куммера)

Розширення на основі поліномів Куммера зокрема застосовують в криптографії, що ґрунтується на спарюванні. У [3] показано, як будувати елементи великого порядку в таких розширеннях при умові $q \equiv 1 (\mathrm{mod} m)$. У цьому разі отримано нижню границю $\exp(\Omega(m))$. Елементи великого порядку збудовано в [2] для розширень вигляду $F_q[x]/(x^{2^t} - a)$ та $F_q[x]/(x^{3^t} - a)$ без умови $q \equiv 1 (\mathrm{mod} m)$. Нижні границі на мультиплікативні порядки дорівнюють $\exp(\Omega(\log m)^2))$, де $m = 2^t$ та $m = 3^t$ відповідно. Повністю умова $q \equiv 1 (\mathrm{mod} m)$

для розширень вигляду $F_q[x]/(x^m - a)$ знята в [13]. Результати, пов'язані з цим класом полів, є також в [4, 20, 21].

3. Елементи великого порядку в скінченних полях вигляду $F_{p^p} = F_p[x]/(x^p - x - a)$ (на основі поліномів Артіна-Шраєра)

Оцінка для порядку отримана в [19] і дорівнює 4^p.

4. Елементи великого порядку в рекурсивних розширеннях скінченних полів (двійкових за Відеманом або Конвеєм; недвійкових)

Особливий інтерес становить побудова елементів у рекурсивних розширеннях скінченних полів – вежах скінченних полів характеристики два або більшої від двох. З прикладної точки зору такі побудови дуже привабливі, оскільки операції над елементами скінченого поля можна виконувати рекурсивно, а тому ефективно. Такі розширення, зокрема, розглядалися в роботах []. Для даних класів полів є висловлені, проте не доведені гіпотези, про явну форму примітивних елементів (гіпотеза Відемана, гіпотеза Вагстафа).

5. Елементи великого порядку в скінченних полях загального вигляду

Гао [6] дав алгоритм побудови елементів великого порядку для багатьох (згідно з висловленою ним, проте не доведеною, гіпотезою для всіх) загальних розширень F_{q^n} скінченого поля F_q з нижньою границею для порядку $\exp(\Omega((\log m)^2 / \log\log m))$. Волох [17, 18] запропонував метод побудови побудови елементів порядку принаймні $\exp(\Omega(\log m)^2))$. Також слід згадати оцінки для полів загального вигляду з [5, 15,23]. Роботи [16, 27] пов'язані з тестами простоти.

1. Ahmadi O., Shparlinski I. E., Voloch J. F. Multiplicative order of Gauss periods // Int. J. Number Theory. -2010. -6, № 4. –P.877-882.

2. Burkhart J. F., Calkin N. J., Gao S., Hyde-Volpe J. C., James K., Maharaj H., Manber S., Ruiz J., Smith E. Finite field elements of high order arising from modular curves // Des. Codes Cryptogr. -2009. -51, № 3. –P. 301-314.

3. Cheng Q. Constructing finite field extensions with large order elements // SIAM J. Discrete Math. -2007. -№ 21. –P. 726-730.

4. Cheng Q., Gao S., Wan D. Constructing high order elements through subspace polynomials // In Proceedings of the Twenty-Third Annual ACM-SIAM Symposium on Discrete Algorithms -2012. –P. 1457-1463.

5. Conflitti A. On elements of high order in finite fields // In Cryptography and Computational Number Theory, volume 20 of Progr. Comput. Sci. Appl. Logic, Birkhauser, Basel -2001. –P. 11-14.

6. Gao S., Elements of provable high orders in finite fields // Proc. Amer. Math. Soc. -1999. -127, № 6. –P. 1615-1623.

7. Gathen J., Shparlinski I. E. Orders of Gauss periods in finite fields // Appl. Algebra Engrg. Comm. Comput. -1998. -№ 9. –P. 15-24.

8. Gathen J., Shparlinski I. E. Constructing elements of large order in finite fields // In Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, volume 1719 of Lecture Notes in Comput. Sci. , Springer, Berlin -1999. –P. 404-409.

9. Gathen J., Shparlinski I. E. Gauss periods in finite fields // In Finite Fields and Applications, Springer, Berlin -2001. –P. 162-177.

10. Lidl R., Niederreiter H. Finite Fields. - Cambridge University Press, 1997.

11. Mullen G.L., Panario D. Handbook of finite fields. – CRC Press, 2013. – 1068 P.

12. Popovych R. Elements of high order in finite fields of the form $F_q[x]/\Phi_r(x)$ *// Finite Fields Appl. -2012. – 18, № 4. –P. 700-710.*

13. Popovych R. Elements of high order in finite fields of the form $F_q[x]/(x^m - a)$ *// Finite Fields Appl. -2013. – 19, № 1. –P. 86-92.*

14. Popovych R. Sharpening of explicit lower bounds on elements order for finite field extensions based on cyclotomic polynomials // Укр. матем. журнал. -2014. – 66, № 6. –P. 815-825.

15. Popovych R. On elements of high order in general finite fields // Algebra and Discrete Mathematics, Luhansk -2014. – 18, № 2. –P. 295-300.

16. Popovych R. Lower bounds on the orders of subgroups connected with Agrawal conjecture // Carpathian mathematical publications. -2013. – 5, № 2. –P. 310-314.

17. Voloch J. F. On the order of points on curves over finite fields // Integers. -2007. – 7, A49.

18. Voloch J. F. Elements of high order on finite fields from elliptic curves // Bull. Aust. Math. Soc. -2010. – 815, № 2. –P. 425-429.

19. Попович Р. Елементи великого порядку в розширеннях Артіна-Шраєра скінченних полів // Мат. студії – 2013. – 39, № 2 – С. 115–118.

20. Попович Р., Про елементи великого порядку в розширеннях скінченних полів на основі поліномів Куммера. // Наук. вісн. Ужгород. ун-ту, серія матем. і інф. – 2013. – 24, № 1 – С. 139-144.

21. Попович Р., Покращення нижньої оцінки для порядку елементів одного класу скінченних полів. // Матем. вісн. НТШ. – 2013. – № 10 – С. 39-44.

22. Попович Р., Про оцінки для мультиплікативних порядків елементів скінченних полів на основі циклотомічних поліномів. // Вісн. НУ Львів. політех., фіз.-мат. науки. – 2013. – № 768 – С. 59–62.

23. Попович Р., Побудова елементів великого порядку в скінченних полях загального вигляду. // Прикладні проблеми механіки і математики, ІППММ АН Україною – 2013. – № 11 – С. 85–89.

24. Попович Р., Нижня межа для порядку елементів в розширеннях скінченних полів вигляду F_{p^p} *. // Вісн. Львів. ун-ту, серія мех.-мат. – 2013. – № 78 – С. 141–147.*

25. Попович Р., Нижня оцінка мультиплікативного порядку елементів у вежах скінченних полів характеристики $p \geq 3$*. // Наук. вісн. Ужгород. ун-ту, серія матем. і інф. – 2014. – 25, № 1 – С. 120-123.*

26. Р.Попович, Скінченні поля при збігу характеристики основного поля та степеня розширення. // Прикладні проблеми мех. і матем. ІППММ АН України. – 2014. – № 12 – С. 37-45.

27. Попович Р., Про підгрупи мультиплікативної групи одного класу скінченних полів. // Вісн. НУ Львів. політехніка, фіз.-матем. Науки. – 2014. – № 804 – С. 108–111.

28. Попович Р., Про ізоморфізм скінченних полів характеристики два. // Матем.вісн.НТШ. – 2014. – № 11 – С. 112-20.

Наукові результати, подані у цій статті, було отримано в рамках дослідницького проекту ДБ/КІБЕР з реєстраційним номером 0115U000446, 01.01.2015 - 31.12.2017, фінансово підтриманим Міністерством освіти та науки України.