ISSN 2078-3744. Вісник Львів. ун-ту. Серія мех.-мат. 2015. Випуск 80. С. 134–139
Visnyk of the Lviv Univ. Series Mech. Math. 2015. Issue 80. P. 134–139

УДК 512.624

НИЖНЯ МЕЖА ДЛЯ МУЛЬТИПЛІКАТИВНОГО ПОРЯДКУ ЕЛЕМЕНТІВ У РОЗШИРЕННЯХ КУММЕРА СКІНЧЕННИХ ПОЛІВ

Роман ПОПОВИЧ

Національний університет "Львівська політехніка",
вул. Бандери, 12, Львів, 79013
e-mail: rombp07@gmail.com

Явно будуємо в розширеннях Куммера скінченних полів елементи великого мультиплікативного порядку.

Ключові слова: скінченне поле, мультиплікативний порядок, розширення Куммера.

Відомо, що мультиплікативна група скінченного поля — циклічна. Твірну цієї групи називають примітивним елементом. Задача ефективної побудови примітивного елемента заданого скінченого поля є важкою в обчислювальній теорії скінченних полів [7, 8]. Ось чому розглядають менш обмежуюче питання: знайти елемент великого мультиплікативного порядку. У цьому випадку достатньо отримати нижню оцінку для порядку. Елементи великого порядку потрібні для багатьох застосувань. Такі застосування, зокрема, охоплюють криптографію, теорію кодування, генератори псевдовипадкових чисел і комбінаторику. Елементи великого порядку також використовують в алгоритмі AKS доведення простоти чисел, яку запропонували Агравал, Кайал та Саксена [2].

У праці [6] Гао дав алгоритм побудови елементів великого порядку для багатьох (згідно з висловленою ним, проте не доведеною, гіпотезою для всіх) загальних розширень F_{q^m} скінченого поля F_q з нижньою межею для порядку $\exp(\Omega((\log m)^2/\log\log m))$. Волох [12] запропонував метод побудови елементів порядку принаймні $\exp(\Omega(\log m)^2))$.

Для часткових випадків скінченних полів можна збудувати елементи, які мають набагато більші порядки. Розширення, пов'язані з поняттям гауссового періоду, розглянуто в [3, 9]. Нижня оцінка для порядку дорівнює $\exp(\Omega(\sqrt{m}))$.

Розширення на підставі полінома Куммера набувають вигляду $F_q[x]/(x^m - a)$. Їх, зокрема, застосовують у криптографії, яка ґрунтується на спарюванні. У [5]

показано, як будувати елементи великого порядку в таких розширеннях за умови $q \equiv 1(mod\ m)$, тобто для розширень Куммера. У цьому разі отримано нижню межу $\exp(\Omega(m))$. Проте зазначена нижня межа є наближеною, а не точною. Для прикладних застосувань (зокрема, криптології) суттєвою є точна оцінка знизу. У [10] збудовано елементи великого порядку для таких розширень без умови $q \equiv 1(mod\ m)$. Нижня межа для мультиплікативного порядку дорівнює $2^{\lfloor \sqrt[3]{2m} \rfloor}$. Розширення Артіна-Шраєра розглянуто в [1].

Скінченне поле з q елементів позначаємо F_q. Групу, породжену елементом v, позначатимемо $\langle v \rangle$. Кількість сполучень з n елементів по k елементів позначимо C_n^k. $|S|$ позначатиме кількість елементів множини S.

Будуємо елементи великого порядку в розширеннях Куммера скінченних полів та даємо точну нижню оцінку для їхнього мультиплікативного порядку. Для цього беремо лінійний двочлен від елемента, який задає розширення, та всі його спряжені, що також належать до підгрупи, породженої цим двочленом, і будуємо їхні різні добутки. Усі спряжені зазначеного лінійного двочлена також є лінійними двочленами. Ідею запропонував Берізбейтіа [4] як вдосконалення алгоритму AKS [2] та розвинув в [5] для розширень Куммера.

Поле L є розширенням Куммера [7] поля K, якщо для деякого заданого цілого числа $n > 1$ виконуються такі умови: K містить n різних коренів степеня n з одиниці (тобто, коренів полінома $x^n - 1$) та L/K має абелеву групу Галуа порядку n.

Зокрема, для випадку скінченних полів: розширення F_{q^m} поля F_q є розширенням Куммера тоді і лише тоді, коли m ділить $q - 1$ [5, 7]. У цьому разі можна вважати, що $F_{q^m} = F_q[x]/(x^m - a)$. Позначимо $\theta = x(mod\ (x^m - a))$ — клас елемента x за модулем $x^m - a$. Зрозуміло, що $\theta^m = a$ та $\theta^{q-1} = (\theta^m)^{(q-1)/m} = a^{(q-1)/m}$. Наступне формулювання є очевидним.

Лема 1. *Якщо поліноми $g(x)$ та $h(x)$ з $F_q[x]$ степеня меншого за m різні, то класи цих поліномів в $F_q[x]/(x^m - a)$ також є різними.*

Лема 2. *Для будь-якого елемента b з поля F_q спряжені елемента $\theta + b$ над цим полем набувають вигляду $a^{i(q-1)/m}\theta + b$ $(i = 0, ..., m - 1)$.*

Доведення. Розглянемо спряжені елемента $\theta + b$, тобто елементи, в які він переходить, коли діє автоморфізм Фробеніуса.

Доведемо, що

$$(\theta + b)^{q^i} = a^{i(q-1)/m}\theta + b \tag{1}$$

для будь-якого натурального i. Доведемо це індукцією по i.

Очевидно, що для $i = 0$ рівність (1) виконується. Припустимо, що вона виконується для деякого i. Тоді для $i + 1$ отримаємо

$$(\theta + b)^{q^{i+1}} = [(\theta + b)^{q^i}]^q = (a^{i(q-1)/m}\theta + b)^q = a^{i(q-1)/m}\theta^q + b$$

$$= a^{i(q-1)/m}a^{(q-1)/m}\theta + b = a^{(i+1)(q-1)/m}\theta + b.$$

Отже, рівність (1) правильна для будь-якого натурального i. □

Зауважимо, що елементи $a^{i(q-1)/m}\theta + b$ у формулюванні леми 2 є різними для $i = 0, ..., m-1$, оскільки $a^{i(q-1)/m}\theta$ — різні.

Посилену нерівність для біноміальних коефіцієнтів отримали в [11, наслідок 2.9, нерівність (2.13)]. Зрештою, отримали такий результат.

Лема 3. *При $s > 1$ та $t \geq 2$ правильна така нерівність:*

$$C_{st}^{t} > 1,08444 \cdot e^{-\frac{1}{8t}} t^{-\frac{1}{2}} \frac{s^{s(t-1)+1}}{(s-1)^{(s-1)(t-1)}} \tag{2}$$

Зафіксуємо цілі числа $1 \leq k_- \leq k \leq m-1$. Нехай $S(m, k_-, k)$ множина таких відображень f з множини $\{0, ..., m-1\}$ в множину цілих чисел, що:

(V1) $|\{i | f(i) < 0\}| = k_-$;

(V2) $-\sum_{i, f(i)<0} f(i) \leq k$;

(V3) $\sum_{i, f(i)\geq 0} f(i) \leq m - 1 - k$.

Лема 4. *Кількість елементів множини $S(m, k_-, k)$ дорівнює*

$$C_m^{k_-} C_k^{k_-} C_{2m-k_--k-1}^{m-k-1}.$$

Доведення. Щоб задати елемент множини $S(m, k_-, k)$, спочатку вибираємо місця, на яких значення відображення від'ємні — це враховує множник $C_m^{k_-}$. Далі вибираємо значення від'ємних елементів так, щоб сума їхніх абсолютних значень не перевищувала k — це враховує множник $C_k^{k_-}$. Нарешті вибираємо невід'ємні значення відображення f на $m - k_-$ місцях так, щоб їхня сума не перевищувала $m - 1 - k$ — це враховує множник $C_{2m-k_--k-1}^{m-k-1}$. □

Лема 5. *Кількість елементів множини $S(m, k_-, k)$ більше від 4^m для $m \geq 39$.*

Доведення. Приймемо $k_- = k = 2$. Тоді згідно з лемою 4

$$|S(m,\, k_-, k)| = C_m^2 C_{2m-5}^{m-3} > \frac{m(m-1)}{2} C_{2(m-3)}^{m-3}.$$

Використовуючи лему 3, нерівність (2) (беремо $s = 2$ та $t = m - 3$), отримуємо

$$C_{2(m-3)}^{m-3} \geq 1,08444 \cdot e^{-\frac{1}{8(m-3)}} \cdot \frac{4^m}{128\sqrt{m-3}}.$$

Тоді $|S(m, k_-, k)| \geq 1,08444 \cdot m(m-1) \cdot e^{-\frac{1}{8(m-3)}} \cdot \frac{4^m}{256\sqrt{m-3}}$. Оскільки $1,08444 \cdot m(m-1) \cdot e^{-\frac{1}{8(m-3)}} \geq 256\sqrt{m-3}$ для $m \geq 39$, то матимемо $|S(m, k_-, k)| > 4^m$. □

Теорема 1. *Припустимо, що $m \geq 39$. Для будь-якого ненульового елемента b поля F_q елемент $\theta + b$ розширення Куммера F_{q^m} має порядок більший від 4^m.*

Доведення. Згідно з лемою 2 спряжені елемента $\theta + b$ (враховуючи сам елемент $\theta + b$) набувають вигляду $a^{i(q-1)/m}\theta + b$ *для* $i = 0, ..., m-1$. Зрозуміло, що всі вони належать до підгрупи $\langle \theta + b \rangle$.

Нехай $S(m,\, k_-, k)$ — множина відображень f з множини $\{0, ...,\, m-1\}$ в множину цілих чисел з описаними раніше властивостями V1, V2, V3. Для кожного елемента f

з множини $S(m,\, k_-, k)$ утворюємо добуток $\prod\limits_{0\le i\le m-1}(a^{i(q-1)/m}\theta+b)^{f(i)}$, який також належить до $\langle\theta+b\rangle$. Стверджуємо, що двом різним елементам f та g з множини $S(m,\, k_-, k)$ відповідають різні добутки.

Доведемо це методом від протилежного. Припустимо, що елементиf та g різні, але відповідні їм добутки однакові

$$\prod_{0\le i\le m-1}(a^{i(q-1)/m}\theta+b)^{f(i)}=\prod\nolimits_{0\le i\le m-1}(a^{i(q-1)/m}\theta+b)^{g(i)}. \tag{3}$$

Оскільки поліном x^m-a є характеристичним поліномом для θ , то можемо записати

$$\prod_{0\le i\le m-1}(a^{i(q-1)/m}\theta+b)^{f(i)}=\prod\nolimits_{0\le i\le m-1}(a^{i(q-1)/m}\theta+b)^{g(i)}(mod(x^m-a)).$$

Тоді

$$\prod_{0\le i\le m-1,\, f(i)\ge 0}(a^{i(q-1)/m}x+b)^{f(i)}\prod_{0\le i\le m-1,\, g(i)<0}(a^{i(q-1)/m}x+b)^{-g(i)}=$$

$$\prod_{0\le i\le m-1,\, f(i)<0}(a^{i(q-1)/m}x+b)^{-f(i)}\prod_{0\le i\le m-1,\, g(i)\ge 0}(a^{i(q-1)/m}x+b)^{g(i)}(mod(x^m-a)). \tag{4}$$

Позаяк отримали поліном степеня

$$\sum_{0\le i\le m-1,\, f(i)\ge 0}f(i)+\sum_{0\le i\le m-1,\, g(i)<0}(-g(i))\le m-1<\deg(x^m-a),$$

у лівій частині та поліном степеня

$$\sum_{0\le i\le m-1,\, f(i)<0}(-f(i))+\sum_{0\le i\le m-1,\, g(i)\ge 0}g(i)\le m-1<\deg(x^m-a)$$

у правій частині рівності (4), то за лемою 1 ці поліноми рівні як поліноми над F_q , тобто

$$\prod_{0\le i\le m-1,\, f(i)\ge 0}(a^{i(q-1)/m}x+b)^{f(i)}\prod_{0\le i\le m-1,\, g(i)<0}(a^{i(q-1)/m}x+b)^{-g(i)}=$$

$$\prod_{0\le i\le m-1,\, f(i)<0}(a^{i(q-1)/m}x+b)^{-f(i)}\prod_{0\le i\le m-1,\, g(i)\ge 0}(a^{i(q-1)/m}x+b)^{g(i)}. \tag{5}$$

У рівності (5) одержали нерозкладні та попарно різні множники $a^{i(q-1)/m}x+b$, $i=0,...,m-1$. Ця рівність суперечить однозначності розкладу поліномів над полем F_q, що робить рівність (3) неможливою. Отже, добутки, які відповідають різним елементам множини $S(m,\, k_-, k)$, не можуть бути однаковими.

Отож, кількість різних розглянутих добутків, які належать до підгрупи $\langle\theta + b\rangle$, дорівнює кількості елементів у множині $S(m, c_-, c)$. Згідно з лемою 4 кількість елементів у множині $S(m, c_-, c)$ дорівнює

$$C_m^{k_-} C_k^{k_-} C_{2m-k_--k-1}^{m-k-1}.$$

За лемою 5 матимемо, що $|S(m, k_-, k)| > 4^m$ для $m \geq 39$. У підсумку отримуємо твердження теореми. □

Зауважимо, що здебільшого розглядають розширення Куммера, для яких m набагато більше від q. Тому умова $m \geq 39$ не є надто обмежувальною. Якщо ж все-таки цікавим є випадок $m < 39$, то треба виконати окреме дослідження.

Література

1. *Попович Р.*, Елементи великого порядку в розширеннях Артіна-Шраєра скінченних полів, Мат. студії **39**:2 (2013), 115–118.
2. *Agrawal M., Kayal N., Saxena N.,* PRIMES is in P, Ann. of Math. **160**:2 (2004), 781–793.
3. *Ahmadi O., Shparlinski I.E., Voloch J.F.*, Multiplicative order of Gauss periods, Int. J. Number Theory **6**:4 (2010), 877–882.
4. *Berrizbeitia P.*, Sharpening Primes is in P for a large family of numbers, Math. Comp. **74**:252 (2005), 2043–2059.
5. *Cheng Q.*, On the construction of finite field elements of large order, Finite Fields Appl. **11**:3 (2005), 358–366.
6. *Gao S.*, Elements of provable high orders in finite fields, Proc. Amer. Math. Soc. **127**:6 (1999), 1615–1623.
7. *Lidl R., Niederreiter H.*, Finite Fields, CRC Press (2013), 755p.
8. *Mullen G.L., Panario D.*, Handbook of finite fields, Cambridge University Press (1997), 1068p.
9. *Popovych R.*, Elements of high order in finite fields of the form $F_q[x]/\Phi_r(x)$, Finite Fields Appl. **18**:4 (2012), 1615–1623.
10. *Popovych R.*, Elements of high order in finite fields of the form $F_q[x]/(x^m - a)$, Finite Fields Appl. **19**:1 (2013), 86–92.
11. *Stanica P.*, Good lower and upper bounds on binomial coefficients, J. Inequal. Pure Appl. Math., **2**:3 (2001), Art. 30.
12. *Voloch J.F.*, Elements of high order on finite fields from elliptic curves, Bull. Austral. Math. Soc. **81**:3 (2010), 425–429.

Стаття: надійшла до редколегії 30.04.2015
доопрацьована 10.09.2015
прийнята до друку 11.11.2015

LOWER BOUND FOR MULTIPLICATIVE ORDER OF ELEMENTS IN KUMMER EXTENSIONS OF FINITE FIELDS

Roman POPOVYCH

Lviv Polytechnic National University,
Bandery Str.,12, Lviv, 79013
e-mail: rombp07@gmail.coml

We construct explicitly elements with high multiplicative order in any Kummer extensions of finite fields.

Key words: finite field, multiplicative order, Kummer extension.