Liet. matem. rink., T. 43, spec. nr., 23–28

Selberg sieve in the polynomial semigroup

Gintautas BAREIKIS
e-mail: gintautas.bareikis@maf.vu.lt

By $\mathcal{N}$ and $\mathcal{R}$ we denote the sets of natural and real set numbers, respectively. Let $\mathcal{M}$ denote the multiplicative semigroup consisting of the primary polynomials in the ring $GF[q,x]$ of polynomials over the finite field of q elements, q being a prime power and $\mathcal{P} \subset M$ is the set of all irreducible polynomials. Each polynomial $d, k, l, m, \ldots \in \mathcal{M}$ uniquely factors in $\mathcal{P}$. The degree of the polynomial $m \in \mathcal{M}$ we denote by $\partial(m)$.

Further, $P_r = \{p \in \mathcal{P}; \partial(p) \leqslant r\}$, here $r = r(n)$ being the sequence of the positive real numbers. The cardinality of the finite set A we denote by $|A|$.

In 1996 Zhang [4, p.860–869] proved for the elements of semigroup the analog of the Selberg sieve. This result has been obtained using Buchstab–Rossen type structures. Author of this paper (see in [1]) using Buchstab–Rossen type structures, has obtained Selber sieve for the set $\{p+1,\ p \in \mathcal{P}\}$.

In this short paper we obtain the same result as in [4], using classical Selberg method.

It is known that

$$|\{m \in \mathcal{M}, \partial(m) = n\}| = q^n, \quad n \in \mathcal{N}.$$

In what follows $c_i, i \in \mathcal{N}$ are absoliute constants. By D we denote some expression, which depend upon various parameters. The value of D is bounded by a constant.

Further, set $\Phi(r) = \prod_{p \in P_r} p$ and $\varphi(m) = \#\{l \in \mathcal{M},\ \partial(l) = \partial(m),\ (m,l) = 1\}$. Are known that

$$\varphi(m) = q^{\partial(m)} \prod_{p|m} \left(1 - \frac{1}{q^{\partial(p)}}\right).$$

Lemma 1. [3, Lemma 2.2] *If $\omega \geqslant e$ then*

$$\min_{\theta \geqslant 0} \theta(e^\theta - \omega) \leqslant -\omega(\ln\omega - \ln\ln\omega - 1).$$

The function which is to be minimized attains the value given as an upper bound when $\theta = \ln\omega - \ln\ln\omega$.

Lemma 2. *For each $2 \leqslant r \leqslant \epsilon n,\ \epsilon \in (0,1)$ we have:*

$$K_0 := \sum_{\substack{d|\Phi(r),\\ \partial(d) \leqslant n}} \frac{1}{\varphi(d)} = A(r)\big(1 + DR_n\big), \quad A(r) = \prod_{p|\Phi(r)} \left(1 - \frac{1}{q^{\partial(p)}}\right)^{-1},$$

$$R_n = \exp\Big(-(1-\delta(\epsilon))\frac{n}{r\ln q}\ln\frac{n}{r\ln q}\Big), \quad \delta(\epsilon) = \frac{\ln\ln\frac{1}{\epsilon\ln q} - 1}{\ln\frac{1}{\epsilon\ln q}}.$$

Proof of Lemma. We have

$$\sum_{d|\Phi(r)} \frac{1}{\varphi(d)} = A(r). \tag{1}$$

Setting

$$L = A(r) - \sum_{\substack{d|\Phi(r),\\ \partial(d)\leqslant n}} \frac{1}{\varphi(d)},$$

from the inequalities $\ln(1+t) \leqslant t$ and $e^t - 1 \leqslant te^t$ $(t > 0)$ we deduce, that for each $\lambda > 0$,

$$L \leqslant \frac{A(r)}{q^{\lambda n}}\exp\Big(\lambda\ln q q^{\lambda r}\sum_{p|\Phi(r)}\frac{\partial(p)}{q^{\partial(p)}}\Big).$$

By making use of the inequality $\sum\limits_{\substack{\partial(p)=k,\\ p\in\mathcal{P}}} 1 \leqslant q^k/k$ (see [2, p.8]) we obtain that

$$Q(r) := \sum_{\partial(p)\leqslant r}\frac{\partial(p)}{q^{\partial(p)}} \leqslant r.$$

Choosing $\lambda = \rho/r$ we have that $q^{\lambda r} = \mathrm{e}^{\rho\ln q}$.
Therefore

$$L \leqslant A(r)\exp\big(\lambda Q(r)q^{\lambda}\ln q - \lambda n\big) = A(r)\exp\Big(\frac{\theta Q(r)}{r}\big(\mathrm{e}^{\theta} - \frac{n}{Q(r)\ln q}\big)\Big),$$

here $\theta = \rho\ln q$.
Applying Lemma 1 we arrive at the inequality

$$L \leqslant A(r)\exp\Big(-\frac{n}{Q(r)\ln q}\Big(\ln\frac{n}{Q(r)\ln q} - \ln\ln\frac{n}{Q(r)\ln q} - 1\Big)\Big) \leqslant A(r)R_n.$$

Proof of Lemma 2 now follows from the last inequality and (1). Lemma 2 is proved.

Set

$$S\big(n,\Phi(r)\big) = \sum_{\substack{\partial(m)=n, m\in\mathcal{M},\\ (m,\Phi(r))=1}} 1, \quad n\in\mathcal{N}.$$

Theorem. *Suppose that* $r < \epsilon n$, *here* $0 < \epsilon < 0.5$ *fixed number. Then for* $n > n_0(\epsilon)$

$$S(n, \Phi(r)) = q^n A^{-1}(r)\big(1 + DR_n^1\big), \quad \text{here } R_n^1 = R_n r^2.$$

Proof of Theorem. Let x_m be real numbers related with the polynomials $m \in \mathcal{M},\ \partial(m) \leqslant n,\ m|\Phi(r)$, satisfying the condition $x_m = 1,\ m \equiv 1$. In that follows each $m \in \mathcal{M},\ m|\Phi(r)$. We first obtain the upper bound of the sum $S(n, \Phi(r))$.

Denote $\sum\limits_{\substack{\dots,\\ m|\Phi(r)}} \dots = \sum\limits_{\dots}{}' \dots$.

It is clear, that

$$S(n, \Phi(r)) \leqslant \sum_{\partial(l)\leqslant n} \Bigg(\sum_{\substack{\partial(m)\leqslant n,\\ m|(l,\Phi(r))}} x_m \Bigg)^2 \leqslant \sum_{\partial(m_1)\leqslant n}{}' \sum_{\partial(m_2)\leqslant n}{}' x_{m_1} x_{m_2} q^{n\partial([m_1,m_2])}, \quad (2)$$

here $[m_1, m_2]$ is less common multiplier, (m_1, m_2) – great common divisor of the polynomials m_1, m_2. The task is now to find minimum value of right-side inequality quadratic form in (2).

Using the equality $q^{\partial\left((m_1,m_2)\right)} = \sum\limits_{k|(m_1,m_2)} \varphi(k)$ we arrive at the relation

$$\frac{S(n, \Phi(r))}{q^n} \leqslant \sum_{\partial(d)\leqslant n}{}' \varphi(d) \Bigg(\sum_{\substack{\partial(m)\leqslant n,\\ m|d}} \frac{x_m}{q^{\partial(m)}} \Bigg)^2 =: K. \quad (3)$$

Setting $z_d = \sum\limits_{\substack{\partial(m)\leqslant n,\\ d|m}}{}' \frac{x_m}{q^{\partial(m)}},\ \ m|\Phi(r)$ we have that $K = \sum\limits_{\partial(d)\leqslant n}{}' \varphi(d) z_d^2$.

In fact, a Meobius inversion shows that

$$\frac{x_m}{q^{\partial(m)}} = \sum_{\substack{\partial(d)\leqslant n,\\ m|d}} \mu\Big(\frac{m}{d}\Big) z_d, \ \ m|\Phi(r).$$

It easy to see that if $x_1 = 1$, then $\sum\limits_{\partial(d)\leqslant n}{}' \mu(d) z_d = 1$.

Using the last relation we then obtain

$$K = \sum_{\partial(d)\leqslant n}{}' \varphi(d) \Big(z_d - \frac{\mu(d)}{K_0 \varphi(d)} \Big)^2 + \frac{1}{K_0}.$$

It is now clear that to minimize K we choose the $z_d = \mu(d)/(K_0\varphi(d))$.

Thus

$$x_m^0 = \frac{q^{\partial(m)}}{K_0} \sum_{\substack{\partial(d)\leqslant n,\\ m|d}}{}' \mu\Big(\frac{d}{m}\Big)\frac{\mu(d)}{\varphi(d)}. \tag{4}$$

For each divisor $d|\Phi(r)$, $d = km$ we have that $(k, m) = 1$.

Then

$$x_m^0 = \frac{q^{\partial(m)}\mu(m)}{K_0} \sum_{\substack{\partial(k)\leqslant n-\partial(m),\\ (k,m)=1}}{}' \frac{1}{\varphi(k)}, \quad 1 < \partial(m) \leqslant n,\ m|\Phi(r),$$

$$K_0 \geqslant \sum_{d|m}{}' \frac{1}{\varphi(d)} \cdot \sum_{\substack{\partial(k)\leqslant n-\partial(m),\\ (k,m)=1}}{}' \frac{1}{\varphi(k)}.$$

We now turn to the relation (3). Choosing x_m^0 value by the equality (4), we obtain that

$$S\big(n, \Phi(r)\big) \leqslant \frac{q^n}{K_0} = q^n \prod_{p|\Phi(r)} \Big(1 - \frac{1}{q^{\partial(p)}}\Big)\big(1 + DR_n\big). \tag{5}$$

The set of the polynomials $P_r = \big\{p \in P,\ \partial(p) \leqslant r\big\}$ is finite. Thus the elements of P_r can be arranged in a sequence in ascending order of $\partial(p)$. This defines an order relation on P_r which we denote as usual by " $<$ ", so $p_i < p_k$ implies $\partial(p_i) \leqslant \partial(p_k)$, $i, k \in \mathcal{N}$. Using this order relation we can write the canonical prime decomposition of $m \in M$ by $a = p_1 \dots p_\pi$, with condition $p_1 > \dots > p_\pi$, $\pi = |P_r|$.

To obtain a lower bound of the relation $S(n, \Phi(r))$ we begin with the equality

$$S\big(n, \Phi(r)\big) = \sum_{\partial(m)=n} 1 - \sum_{\substack{\partial(m)=n,\\ p_1|m}} 1 - \dots - \sum_{\substack{\partial(m)=n,\\ p_1\not|m,\\ \dots\\ p_{\pi-1}\not|m,\\ p_\pi|m}} 1.$$

Setting $\Phi_i = \prod_{k=1}^{i-1} p_i$, $\Phi_0 = 1$ we have

$$S\big(n, \Phi(r)\big) = q^n - \sum_{i=1}^{\pi} S\big(n - \partial(p_i), \Phi_i\big). \tag{6}$$

It is clear that $\Phi_i \subset \Phi(r)$. The equality (5) holds uniformly for all subsets of P_r. Thus, combining (5) with (6) we obtain

$$S\big(n, \Phi(r)\big) \geqslant q^n - q^n \sum_{i=1}^{\pi} \frac{1}{q^{\partial(p_i)}}$$

$$\times \prod_{p|\Phi_i}\left(1-\frac{1}{q^{\partial(p)}}\right)\left(1-D\exp\left\{-(1-\delta(\epsilon))\frac{n-\partial(p_i)}{\partial(p_i)\ln q}\ln\frac{n-\partial(p_i)}{\partial(p_i)\ln q}\right\}\right), \quad (7)$$

here D is positive.

Using well known equality

$$1-\sum_{i=1}^{k}\frac{1}{a_i}\prod_{j=1}^{i-1}\left(1-\frac{1}{a_j}\right)=\prod_{i=1}^{k}\left(1-\frac{1}{a_i}\right)$$

we conclude from (7) that

$$S(n,\Phi(r)) \geqslant q^n A^{-1}(r)\left(1-D\sum_{1\leqslant i\leqslant\pi}\frac{1}{q^{\partial(p_i)}}\prod_{j=i+1}^{\pi}\left(1-\frac{1}{q^{\partial(p_j)}}\right)^{-1}\right.$$
$$\left.\times\left(1-D\exp\left\{-(1-\delta(\epsilon))\frac{n-\partial(p_i)}{\partial(p_i)\ln q}\ln\frac{n-\partial(p_i)}{\partial(p_i)\ln q}\right\}\right)\right). \quad (8)$$

Using the inequality $(1-t)^{-1}\leqslant\exp\{t/(1-t)\},\ 0\leqslant t\leqslant 1$ and

$$\sum_{\partial(p_i)\leqslant\partial(p)\leqslant r}\frac{1}{q^{\partial(p)}}\leqslant\ln\frac{r}{\partial(p_i)}+c_4$$

we deduce that

$$\sum_{1\leqslant i\leqslant\pi}\frac{1}{q^{\partial(p_i)}}\prod_{j=i+1}^{\pi}\left(1-\frac{1}{q^{\partial(p_j)}}\right)^{-1}\leqslant c_4 r^2.$$

The last inequality and relation (8) allow us to assert that

$$S(n,\Phi(r)) \geqslant q^n A^{-1}(r)\left\{1-D\exp\left\{-(1-\delta(\epsilon))\frac{n}{r\ln q}\ln\frac{n}{r\ln q}+2\ln r\right\}\right\}. \quad (9)$$

Considering together the upper bound (5) and lower bound (9) leads to the proof of the theorem.

Theorem is proved.

References

[1] G. Bareikis, The Selberg sieve method in the polynomial set, *Lith. Math. J.*, **41**, 39–44 (2001).
[2] M. Car Le theoreme de Chen pour $F_q[x]$, *Diss. Math.*, **95**, 1–55 (1984).
[3] P.D.T.A. Elliott, *Probabilistic Number Theory*, Springer–Verlag, New York (1979).
[4] W.-B. Zhang, Probabilistic number theory in additive arithmetic semigroups. I. in: *Analytic Number Theory*, Vol. II, B.C. *et al.* (Eds.), Prog. Math., **138** (1996), pp. 839–885.

Selbergo rėtis polinomų pusgrupėje

G. Bareikis

Straipsnyje, naudojant klasikinį Selbergo metodą, buvo gauta dydžio

$$S(n,\Phi(r))=\sum_{\substack{m\in M,\partial(m)=n,\\(m,\Phi(r))=1}}1$$

asimptotinė formulė, čia $n\in\mathcal{N}$, M – polinomų, virš baigtinio skaičių kūno, aibė, $\partial(m)$ – polinomo $m\in\mathcal{M}$ laipsnis, $\Phi(r)$ – neredukuojamų polinomų, kurių laipsniai neviršija r, sandauga.