Liet. matem. rink., T. 41, spec. nr., 39–44

The Selberg sieve method in the polynomial set

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

By $\mathcal{N}, Z, \mathcal{R}, \mathcal{C}$ we denote the sets of natural, integer, real and complex numbers, respectively. Assume $A \subset \mathcal{N}$. By $|A|$ we denote the cardinality of the set A. Let $\mathcal{M}$ means the multiplicative semigroup consisting of the monic polynomials over finite field F_q. In following a, b, e, d, k mean polynomials of $\mathcal{M}$. Further, suppose that $\mathcal{M}$ addmits a degree mapping $\partial : \mathcal{M} \to \mathcal{N} \cup \{0\}$ satisfying the condition:

$$\partial(ab) = \partial(a) + \partial(b), \quad a, b \in \mathcal{M}.$$

By $\mathcal{M}_m \subset \mathcal{M}, m \in \mathcal{N}$ we denote the set of monic polynomials of degree m. It is known, that

$$|\mathcal{M}_m| = q^m.$$

Let $\mathcal{P} \subset \mathcal{M}$ be the set of monic irreducible polynomials and $\mathcal{P}_m = \{p \in \mathcal{P};\ \partial(p) = m\}$. Each polynomial $f(x) \in \mathcal{M}$ factors uniquely by the degrees of $p \in \mathcal{P}$. Let $\pi(m; b, a)$ denote the number of primary irreducible polynomials of degree m which are congruent to $a \bmod b$. Set

$$\varphi(a) = \left|\{b \in \mathcal{M};\ \partial(a) = \partial(b),\ (a, b) = 1\}\right|.$$

For each a we have

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

Write

$$\mathcal{A} = \{p + 1;\ p \in \mathcal{P}\}, \quad A(m) = \{p + 1;\ p \in \mathcal{P}_m\}, \quad \omega(a) = \sum_{p|a,\ p \in \mathcal{P}} 1.$$

M. Car [2] has proved the following

Lemma 1 [Theorem A.2]. *Let $a, b \in \mathcal{M}$ and $(a, b) = 1$. Then*

$$\left|\pi(m; b, a) - \frac{1}{\varphi(b)} \cdot \frac{q^m}{m}\right| \leqslant (1 + \partial(b)) q^{\frac{m}{2}}.$$

Moreover

$$\frac{q^m}{m} - \frac{2q^{m/2}}{m} \leqslant \big|A(m)\big| \leqslant \frac{q^m}{m}, \quad \textit{when} \quad m \in \mathcal{N}.$$

Set

$$A_d(m) = \{a \in A(m);\ d|a\}.$$

Applying Lemma 1 we obtain

$$\big|A_d(m)\big| = \frac{q^m}{m\varphi(d)} + R_m(d),$$

where the remainder term $R_m \leqslant c\big(1 + \partial(d)\big)(q^m/m)$, with an absolute constant c.

We write $a < b$, $a, b \in \mathcal{M}$ if $\partial(a) \leqslant \partial(b)$. Let $a \in \mathcal{M}$ be squarefree and $a \neq 1$. Then a can be written as

$$a = p_1 p_2 \dots p_n, \quad \Delta(a) := p_1 > p_2 > \dots > p_n = \delta(a), \quad \text{here} \quad p_1, \dots p_n \in \mathcal{P}.$$

Assume $\delta(1) = 1$. Denote

$$Q(a) = \prod_{p<a} p, \quad Q_r = \prod_{\partial(p)\leqslant r} p.$$

Let $\xi : \mathcal{M} \to \mathcal{R}$, $\xi(1) = 1$. The function $\overline{\xi}(d)$ we define using the function ξ by the equality

$$\overline{\xi}(d) = \xi\big(d/\delta(d)\big) - \xi(d), \quad \text{if} \quad d \neq 1.$$

Moreover

$$\sum_{\substack{d|a,\\ \Delta(a/d)<\delta(d)}} \overline{\xi}(d) = 1 - \xi(a). \tag{1}$$

Let $h : \mathcal{M} \to R$. Applying the relation (1) we obtain

$$\sum_{d|Q(a)} \mu(d)h(d) = \sum_{d|Q(a)} \mu(d)\xi(d)h(d) + \sum_{d|Q(a)} \mu(d)\overline{\xi}(d) \sum_{t|Q(\delta(d))} \mu(t)h(dt), \tag{2}$$

where $\mu(d)$, $d \in \mathcal{M}$, is the Möbus function. Set

$$S(A(m), Q_r) = \big|\{a \in A(m);\ (a, Q_r) = 1\}\big|.$$

Using a sieve equality and the relation (2) we obtain

$$S\big(A(m), Q_r\big) = \sum_{d|Q_r} \mu(d)\xi(d)A_d(m) + \sum_{d|Q_r} \mu(d)\overline{\xi}(d)S\Big(A_d(m), Q\big(\delta(d)\big)\Big).$$

Let $\nu \in (0, 1/2)$. Set $n = \nu m$ and $y = Lr \leqslant n$, $L \geqslant 2$. Further, let

$$\beta = \max\{\epsilon L, \beta_1\}, \quad \beta_1 > 1, \quad 0 < \epsilon < 1. \tag{3}$$

In following the magnitudes ν, n, L, y, β are defined as in (3). Denote

$$\xi^{\pm}(d) = \eta^{\pm}(p_1)\eta^{\pm}(p_1p_2)\dots\eta^{\pm}(p_1p_2\dots p_k),$$

where

$$\eta^{+}(a) = \begin{cases} 1, & \text{if} \quad \omega(a) = 2k \quad \text{or} \quad \omega(a) = 2k-1 \wedge \beta\partial\big(\delta(a)\big) + \partial(a) < y, \\ 0, & \text{else,} \end{cases}$$

$$\eta^{-}(a) = \begin{cases} 1, & \text{if} \quad \omega(a) = 2k-1 \quad \text{or} \quad \omega(a) = 2k \wedge \beta\partial\big(\delta(a)\big) + \partial(a) < y, \\ 0, & \text{else,} \end{cases}$$

$k \in \mathcal{N}$.

Using the last definitions concerning the functions $\xi^{\pm}$, from (2) we obtain the following equalities

$$\overline{\xi^{\pm}}(d) = \eta^{\pm}(p_1)\eta^{\pm}(p_1p_2)\dots\eta^{\pm}(p_1p_2\dots p_{(k-1)})\big(1 - \eta^{\pm}(p_1\dots p_k)\big). \tag{4}$$

Theorem 1. *We have*

$$\begin{aligned} S\big(A(m), Q_r\big) &= \frac{q^m}{m}\prod_{p|Q_r}\left(1-\frac{1}{\varphi(p)}\right)\left(1+\mathrm{O}_{\epsilon}\left(L^{-(1-\epsilon)L}+\mathrm{O}\Big(\frac{r^2m^2}{q^{m(1/2-\nu)}}\Big)\right)\right) \\ &= : F(r)\big(1 + R(\epsilon, m)\big) \end{aligned}$$

for each fixed $0 < \epsilon < 1$, $0 < \nu < 0,5$.

Lemma 2 [3, Lemma 3.3]. *We have*

$$\prod_{\partial(p)\leqslant n}\left(1-\frac{1}{q^{\partial(p)}}\right) = \frac{c}{n}\left(1+\mathrm{O}\Big(\frac{1}{n}\Big)\right),$$

where c is absolute constant.

Proof of Theorem 1. Using the definition of the function $\xi^{+}(d)$ we see that

$$T^{+}(d) := \mu(d)\overline{\xi^{+}}(d)S_d\Big(m, P\big(\delta(d)\big)\Big) \leqslant 0,$$

when $\omega(d) = 2k - 1$, and $T^{+}(d) = 0$, when $\omega(d) = 2k$, $k \in \mathcal{N}$. The last inequality and relation (2) yield the inequality

$$\big|S\big(A(m), Q_r\big)\big| \leqslant \sum_{d|Q_r}\mu(d)\xi^{+}(d)\big|A_d(m)\big| \leqslant \frac{q^m}{m}\sum_{d|Q_r}\mu(d)\xi^{+}(d)\frac{1}{\varphi(d)}$$

$$+ \sum_{\substack{d|Q_r,\\ \partial(d)\leqslant n}} \mu(d)\xi^+(d)R_d(m) =: S_1 + S_2. \tag{5}$$

It is clear, that the first summand of (5) can be written as

$$S_1 = \frac{q^m}{m}\Big(\sum_{d|Q_r} \mu(d)\xi^+(d)\frac{1}{\varphi(d)} - \sum_{\substack{d|Q_r,\\ \partial(d)\geqslant n}} \mu(d)\xi^+(d)\frac{1}{\varphi(d)}\Big)$$
$$= \frac{q^m}{m}(S_{11} + S_{12}). \tag{6}$$

Let $\partial(d) \geqslant Lr$. We shall show, that under this condition $\xi^+(d) = 0$. If $\omega(d)$ is odd, then validity of the assertion follows from the definition of η^+. Suppose, that $\omega(d)$ is even. Then $\omega\big(d/\delta(d)\big)$ is odd, and for this polynomial we have: $\beta\partial\big(\delta(d/\delta(d))\big)+\partial\big(d/\delta(d)\big) \geqslant \partial(d) \geqslant Lr$. So, $\eta^+\big(d/\delta(d)\big) = 0$ and from the last equality it follows that $\xi^+(d) = 0$.

We note, that $n \geqslant Lr$. It is clear that

$$S_{12} = 0. \tag{7}$$

Let us return to the relation (6). Using equality (2) we obtain

$$S_{11} = \prod_{p|Q_r}\Big(1 - \frac{1}{\varphi(d)}\Big)\Big\{1 - \sum_{d|Q_r} \mu(d)\overline{\xi^+}(d) \prod_{\substack{p|Q_r,\\ p>\delta(d)}}\Big(1 - \frac{1}{\varphi(p)}\Big)^{-1}\Big\}. \tag{8}$$

It follows from Lemma 2, that

$$\prod_{\partial\left(\delta(d)\right)\leqslant\partial(p)\leqslant r}\Big(1 - \frac{1}{\varphi(p)}\Big)^{-1} = \prod_{\partial\left(\delta(d)\right)\leqslant\partial(p)\leqslant r}\Big(1 - \frac{1}{q^{\partial(p)}}\Big)^{-1} = O\Big(\frac{r}{\partial(\delta(d))}\Big).$$

The last estimation together with the remarks made above allow us to use method of [3, lemma 5.4]. Applying mentioned lemma we obtain, that for each fixed $0 < \epsilon < 1$

$$S_{11} = \prod_{p|Q_r}\Big(1 - \frac{1}{\varphi(p)}\Big)\Big(1 + O_\epsilon\big(L^{(\epsilon-1)L}\big)\Big). \tag{9}$$

Consider the relation S_2 in (5). Using the equality

$$\prod_{p|Q_r}\Big(1 - \frac{1}{\varphi(p)}\Big)^{-1} = O(r)$$

we obtain that $|S_2| \leqslant (q^m/m)(mr)^2 q^{(\nu-0.5)m}$.

The last inequality, and the relations (9) and (7) yield the right hand side inequality of Theorem 1, $S\big(A(m), Q_r\big) \leqslant F(r)\big(1 + R(\epsilon, m)\big)$.

The left hand side inequality we obtain from the relation

$$|S(A(m),Q_r)| = \Big|\sum_{d|Q_r}\mu(d)\xi^-(d)|A_d(m)| + \sum_{d|Q_r}\mu(d)\overline{\xi^-}(d)S\Big(A_d(m),P\big(\delta(d)\big)\Big)\Big| \geqslant \sum_{d|Q_r}\mu(d)\xi^-(d)|A_d(m)|.$$

Repeating arguments similar to the ones as in the proof of the inequality (5) we obtain the left hand side inequality of Theorem 1. So $S\big(A(m),Q_r\big) \geqslant F(r)\big(1+R(\epsilon,m)\big)$.

Theorem 1 is proved.

Let $f : \mathcal{A} \to \mathcal{R}$. We define

$$f_r(a) = \sum_{\substack{p|a,\\ \partial(p)\leqslant r}} f(p), \quad a \in \mathcal{A}, \quad r < m.$$

Further, let $F_i = \{a \in A(m);\ f_r(a) = x_i\}$, $i = 1,2,\ldots$. Then $F_i = \bigcup_{\substack{k|Q_r,\\ f(k)=x_i}} E_k$, where $E_k = \{a \in A(m);\ k|a,(a,Q_r/k) = 1\} =: S\big(A(m),Q/k\big)$. For $k \neq l$ we have $E_k \cap E_l = \varnothing$. Define the set measure by $\nu(E_k) = |E_k|/|A(m)|$. Suppose, that $\partial(d) < m\nu - \partial(k)$ and $\partial(d) < \frac{m}{2}\nu$. Let $d|(Q/k)$. Then we have:

$$\Big|\big\{a : \partial(a) = m; kd|a\big\}\Big| = \frac{q^m}{m\varphi(kd)} + \mathrm{O}\big((1+m)q^{m/2}\big).$$

Using Theorem 1 we obtain

$$S\big(A(m),Q/k\big) = \frac{q^m}{m\varphi(k)}\Big(\prod_{p|(Q/k)}\Big(1-\frac{1}{\varphi(p)}\Big) \times \Big(1+\mathrm{O}_\epsilon\big(L^{-(1-\epsilon)L} + (mr)^2 q^{m(\nu-0.5)}\big)\Big)\Big).$$

Let $r/m = \mathrm{o}(1)$, as $m \to \infty$. Choosing $L = \ln(m/r)$ we obtain, that $Lr/m = \mathrm{o}(1)$, as $m \to \infty$. Let $0 < \epsilon < 1$ be fixed number. So, for sufficiently large m we obtain, that there exists $A_0(\epsilon)$, that for each fixed $A > A_0$ and sufficiently large m, the asymptotic inequality is true:

$$\nu(E_k) = \frac{1}{\varphi(k)}\prod_{p|(Q/k)}\Big(1-\frac{1}{\varphi(p)}\Big)\big(1+\mathrm{O}(r/m)^A\big).$$

For $k|Q_r$ setting

$$\mu_k = \frac{1}{\varphi(k)}\prod_{p|(Q/k)}\Big(1-\frac{1}{\varphi(p)}\Big)$$

we obtain that μ_k approximate the set function $\nu(E_k)$.

Let $\mathcal{E}$ be an algebra, generated by finite unions of the sets $E_k \neq \varnothing$, and $\mathcal{F}$ be a minimal sigma algebra, generated by algebra $\mathcal{E}$. Suppose, that $E \in \mathcal{E}$. Then $E = \cup_{1 \leqslant j \leqslant n} E_{k_j}$, $E_{k_j} \cap E_{k_i} = \varnothing$, $i \neq j$. One can show, that $\mu(\cup_j E_{k_j}) = \sum_j \mu_{k_j}$ and moreover, $\sum_{k|Q_r} \mu_k = 1$. So, the set function μ is probability measure in some probability space. Further, this measure approximates the frequency $\nu(\ldots)$. Set

$$\sigma(x) = \Big(\sum_{\partial(p) \leqslant x} \frac{f^2(p)}{\varphi(p)} \Big)^{1/2}, \quad \alpha(x) = \sum_{\partial(p) \leqslant x} \frac{f(p)}{\varphi(p)}.$$

DEFINITION. We shall say that arithmetic function $f : \mathcal{A} \to \mathcal{R}$ belongs to the class Hp, if there exists a function $r(x) = \mathrm{o}(x)$ and $\sigma\big(r(x)\big) \sim \sigma(x)$ $\big(\sigma(x) \to \infty\big)$, $x \to \infty$.

Using Theorem 1 we can prove the following

Theorem 2. *Suppose, that $f(n)$ is a strongly additive function of the class Hp. Then the set measure*

$$\frac{1}{|A(m)|} \sum_{\substack{\partial(p)=m, \\ f(p+1)-\alpha(m) \leqslant u\sigma(m)}} 1$$

converges weakly to a limiting distribution as $m \to \infty$, if and only if there exists nondecreasing function $K(u)$ such, that

$$K_m(u) := \frac{1}{\sigma^2(m)} \sum_{\substack{\partial(p) \leqslant m, \\ f(p) \leqslant u\sigma(m)}} \frac{f^2(p)}{\varphi(p)} \Rightarrow K(u),$$

and $\lim_{m \to \infty} K_m(\pm\infty) = K(\pm\infty)$.

References

[1] G. Bareikis, Kubiliaus nelygybės analogas polinomų pusgrupėje, *Lietuvos Matematikų Draugijos Mokslo Darbai*, T. IV, Vilnius (2000).

[2] M. Car, Le theoreme de Chen pour $F_q[X]$, *Diss. Math.*, CCXXIII, 95 (1972).

[3] W.-B. Zhang, Probabilistic number theory in additive arithmetic semigroups I, In: *Analytic Number Theory, Prog. Math.*, **138**, 839–885, Birkhauser (1996).

Selbergo rėčio metodas polinomų žiede

G. Bareikis

Tarkime, $\mathcal{P}-$ neredukuojamų polinomų aibė. Straipsnyje nagrinėjamas Selbergo rėčio metodo taikymas aibėje $\{p + 1, p \in \mathcal{P}\}$.