On efficient computation of sums of characters on the base of A.G. Postnikov methods

Nikolaj Glazunov
(Glushkov Institute of Cybernetics NASU)

Plan

1. Characters of discrete abelian groups
2. On p - adic analisys
3. Sums of Dirichlet characters and the method of Postnikov
4. Algorithm and computations

Conclusions

1.Characters of discrete abelian groups

The characters of discrete abelian groups underlie Pontryagin's duality theory [1]. Such characters find applications in mathematics, in the theory of computation, in physics, and in their applications. An important aspect of the study and application of characters is their summation, that is, finding the exact value or a non-trivial estimate of the sum of characters. For example, F. Gauss back in 1795 on the basis of "Gauss sums" proved the famous reciprocity law.

A character φ of the given discrete abelian group G is not identically zero complex valued function on G to the compex torus T such that for $g \in G$ and $h \in G$

$$\varphi(gh) = \varphi(g)\varphi(h)$$

There are additive and multiplicative characters.

Every finitely generated abelian group G is isomorphic to direct product of primery cyclic groups and infinite cyclic groups.

The structure of finite abelian groups is defined by the next results [1,3]: Every finite abelian group has the representation by the direct product of cyclic subgroups. Next result states that number of all characters is equal to the order of the finite abelian group. The connection between characters of G and characters of its subgroup H is described by the following statement: Any character of the subgroup H can be lifted to the character of the group G and there are $(G:H)$ such liftings.

Dirichlet characters.

Here we follow to [2-4]. Let m be a natural number and let G_m be the group of residues $\bmod m$. For simplicity consider the case when m is a natural degree q of a prime number p. Let ω be a primitive root of unity. Let $\nu(n)$ be the index of number n with respect to the primitive root g. Than by definition the elementary Dirichlet character $\bmod q$ is the function $\omega^{\nu(n)}$. For example, for q equal to prime p

$$\omega^{\nu(n)} = e^{\frac{ind_g n}{p-1}} .$$

2.**On p - adic analisys**

To establish a connection between finite abelian groups and p-adic numbers, we must equip the abelian groups with the discrete topology

A non-Archimedean local field is a complete discrete valuation field with finite residue field. Further, for brevity, we call these fields local. In other words, a field K is called local if it is complete in a topology determined by the valuation of the field and if its residue field k is finite. Here we consider the case when the characteristic of K is equal zero.

2.1. p - adic arithmetics. В неархимедовом локальном поле K каждый его элемент α имеет представление $\alpha = \varepsilon\pi^m$, где ε есть единица кольца целых поля K, π- его униформизующий элемент, т.е. $\nu(\pi)=1$, m- целое рациональное число. Единицу называют главной, если $\varepsilon \equiv 1(\mathrm{mod}\ \pi)$.

2.2. Lifting the root of an algebraic equation over a finite field to an p-adic number. The connection between the roots of a polynomial in a simple finite field and in the field of p-adic numbers is given by the following well-known statement [3] (for simplicity, we formulate it for one variable): Let $F(x)$ be a polynomial with integer p-adic coefficients. If for $F(x)$ there exists a p-adic number α such that

$$F(\alpha) \equiv 0(\mathrm{mod}\ p),\ F^{'}(\alpha)\neg \equiv 0(\mathrm{mod}\ p)$$

then there exists a p-adic solution of the equation $F(\alpha)=0$.

My experience with p-adic numbers.

Mir-2. Experiments in algebra and number theory, 1970-1971, and so on.

Glazunov N.M. Comuutational experiments in algebra and number theory on computer Mir-2 (Publication. 1971)

3.Sums of Dirichlet characters and the method of Postnikov

The Dirichlet character $\bmod p^n$ has the presentation $\omega(m) = e^{\frac{ind_g m}{(p-1)p^{n-1}}}$. Postnikov's method uses the p-adic logarithm function $\ln(1+x)$, the descent of the logarithm onto the ring $Z / p^n Z$, and the estimation of the sum of characters based on the Vinogradov mean value theorem. Postnikov's method are too cumbersome to be presented in the short talk.

4.Algorithm and computations

We extract, based on the Postnikov method, following the three phases of the method, a family of corresponding algorithms. In the first phase, various methods are used for calculating the primitive root $\bmod p^n$, then there is a reduction modulo power p^n of the power series representing the p-adic logarithm, and in the third phase, variants (with different error estimates) of the Vinogradov mean value theorem are used.

In conclusion, we present results on sums of characters (Kloosterman sum) associated with Artin-Schreier coverings over prime finite fields, obtained on the basis of a generalization of the method of A.G. Postnikov [2], and which complement [7].

Let T_p be the sum of characters of the form

$$T_p = \sum_{x=1}^{p-1} e^{2\pi i \frac{\left(cx+\frac{d}{x}\right)}{p}}, \; c = d = 1, \text{ (Kloosterman sum).}$$

Present the results of our computation of small and big values of the sum (with varying p).

Remark. The trivial estimation of T_p is equal $p-1$.

In the next Proposition we give some absolute values of small and big values of T_p.

Proposition. Let prime p varies from $p=2$ to $p=13171$. Then we have next values of $|T_p|$:

Small values of T_p for primes from interval $[2,\ 13171]$: $2\sqrt{2}\times 0,35355$, $2\sqrt{41}\times 0,31430$, $2\sqrt{97}\times 0,10634$, $2\sqrt{383}\times 0,08503$, $2\sqrt{487}\times 0,05637$, $2\sqrt{709}\times 0,04543$, $2\sqrt{1613}\times 0,03436$, $2\sqrt{2161}\times 0,02577$, $2\sqrt{10889}\times 0,00492$.

Big values of T_p for primes from interval $[2,\ 13171]$: $2\sqrt{2}\times 0,35355$, $2\sqrt{7}\times 0,38721$, $2\sqrt{29}\times 0,47823$, $2\sqrt{103}\times 0,52564$, $2\sqrt{3041}\times 0,75232$, $2\sqrt{7537}\times 0,85773$, $2\sqrt{5059}\times 0,78164$, $2\sqrt{10181}\times 0,95269$, $2\sqrt{13171}\times 0,96537$.

Conclusions. In the talk we present theoretical foundations of computation of sums of characters of abelian groups and the structure of the algorithm. Then we present results of computation of Kloosterman sums, which are sums of characters of Artin-Schreier coverings over prime finite fields. The algorithm and the method of computation are based on two methods by A.G. Postnikov with some their modifications. The structure of the algorithm for computing sums of Dirichlet characters $\bmod p^n$, p - prime, natural $n \geq 1$ and results of computations of Kloosterman sums are given.

References

[1] *Понтрягин Л. С.* Непрерывные группы, 3-е изд. М.: Наука, 1986. - 519 с.

[2] *Постников А.Г.* Избранные труды. М.: Физматлит, 2005. - 512 с..

[3] Боревич З.И., Шафаревич И.Р. Теория чисел. - М.: Наука, 1985. - 503 с.

[4] *Карацуба А.А.* Основы аналитической теории чисел. М.: Наука, 1975. – 183 с.

[5] *Чубариков В.Н.* Об асимптотических формулах для интеграла И.М. Виноградова и его обобщений // Тр. МИАН СССР. 1981. Т. 157. – С.214–232.

[6] *Khrennikov A. Yu. Nilsson M.* p-adic deterministic and random dynamics. Dordrecht: Kluver Academic Publ., 2004. – 280 p.

[7] *Glazunov N.M.* Arithmetic Statistics, Probabilities and Langlands correspondence // Proc. of Int. Conf. on Analytical and Computational Methods in Probability Theory and its Applications (ACMPT-2017), Lomonosov state university, 2017. – P. 220–225.

[8] *Glazunov N.M.* p-adic L-functions and p-adic multiple zeta values // Chebyshevskii Sbornik, 2019. – № 1. P. – 112–130.

Thank you for your attention!