S-units in hyperelliptic fields

V. V. Benyash-Krivets and V. P. Platonov

In this note we present some results about computation of the group of S-units in hyperelliptic fields.

Let $k = \mathbb{F}_q(x)$ be the field of rational functions of one variable over a finite field $\mathbb{F}_q$ of characteristic $p > 2$, and let $d(x) = a_0x^{2n+1} + a_1x^{2n} + \cdots + a_{2n+1} \in \mathbb{F}_q[x]$ be a square-free polynomial, $a_0 \neq 0$. Let $K = k(\sqrt{d}\,)$. For an irreducible polynomial $v \in \mathbb{F}_q[x]$, we denote by $|\cdot|_v$ the corresponding valuation on k. Let (α, β) be a point on the curve $y^2 = d(x)$, $\beta \neq 0$. Then the valuation $|\cdot|_{x-\alpha}$ has two extensions to K. These extensions will be denoted by $|\cdot|_1$ and $|\cdot|_2$. The non-Archimedean valuation $|\cdot|_\infty$ has a unique extension to K, which also will be denoted by $|\cdot|_\infty$. The following two cases are the basic cases for investigation of S-units: 1) $S = \{|\cdot|_\infty, |\cdot|_1\}$; 2) $S = \{|\cdot|_\infty, |\cdot|_1, |\cdot|_2\}$. Let $\mathcal{O}_S$ be the ring of S-integers in K, that is, the elements $y \in K$ such that $|y|_v \geqslant 0$ for all valuations $|\cdot|_v$ on K which do not belong to S. The set U_S of all invertible elements of $\mathcal{O}_S$ is called the group of S-units of the field K. By the generalized Dirichlet theorem on units (see [1], Chap. IV, Theorem 9), the group U_S is the direct product of the group $\mathbb{F}_q^*$ and the free Abelian group G of rank $|S| - 1$. The independent generators of the group G are called fundamental S-units.

In the classical case of a quadratic extension $L = \mathbb{Q}(\sqrt{d}\,)$ of $\mathbb{Q}$ one can find a fundamental unit of the field L by using the continued fraction expansion of $\sqrt{d}$ [2]. However the method of continued fractions does not work properly for function fields. A goal of this note is to find an algorithm for computing the fundamental S-units in a hyperelliptic field K in the two basic cases above.

The first proposition is of a technical character.

Proposition 1. *Let $y = f + g\sqrt{d}$, where $f, g \in \mathbb{F}_q[x]$, $f \neq 0$, $g \neq 0$, (f, g)=1, and let $v \in \mathbb{F}_q[x]$ be an irreducible polynomial. Then the following statements are true.*

1. *If $|\cdot|_v$ has two extensions $|\cdot|_{v'}$ and $|\cdot|_{v''}$ to K, then either $|y|_{v'} = 0$ or $|y|_{v''} = 0$.*
2. *If $v \nmid d$ and $|\cdot|_v$ has a unique extension $|\cdot|_{v'}$ to K, then $|y|_{v'} = 0$.*
3. *If $v \mid d$ and $v \nmid f$, then $|\cdot|_v$ has a unique extension $|\cdot|_{v'}$ to K and $|y|_{v'} = 0$.*
4. *If $v \mid d$ and $v \mid f$, then $|\cdot|_v$ has a unique extension $|\cdot|_{v'}$ to K and $|y|_{v'} = 1/2$.*

The following proposition gives a characterization of S-integers in K.

Proposition 2. *Every element $y \in \mathcal{O}_S$ admits a representation*

$$y = (f + g\sqrt{d}\,)(x - \alpha)^{-m},$$

where $f, g \in \mathbb{F}_q[x]$ and $m \geqslant 0$. Moreover, if $m > 0$ and $x - \alpha$ does not divide f and g simultaneously, then $x - \alpha \nmid f$ and $x - \alpha \nmid g$.

The proof of Proposition 2 is based on the following observation: if the denominator of y is divisible by an irreducible polynomial $v \neq x - \alpha$, then for some extension $|\cdot|_{v'}$ of $|\cdot|_v$ we have $|y|_{v'} < 0$ by Proposition 1.

We note that not every element of type $(f + g\sqrt{d}\,)(x - \alpha)^m$ is an S-integer. In what follows it is important to us to determine the images of the norm map on S-units.

AMS 2000 *Mathematics Subject Classification.* Primary 11T99; Secondary 11G20, 11R27, 16U60.

DOI 10.1070/RM2007v062n04ABEH004435.

Proposition 3. *If* $\varepsilon = (f + g\sqrt{d})/(x-\alpha)^{m_1} \in U_S$, *where* $f, g \in \mathbb{F}_q[x]$, *and if* $\varepsilon \notin \mathbb{F}_q^*$, *then* $f \neq 0$, $g \neq 0$, $(f, g) = 1$, *and* $N_{K/k}(\varepsilon) = a(x-\alpha)^m$, *where* $a \in \mathbb{F}_q^*$ *and* $0 \neq m \in \mathbb{Z}$.

As in the case of S-integers, if an element $\varepsilon \in K$ has the property that $N_{K/k}(\varepsilon) = a(x-\alpha)^m$, it does not follow that ε is an S-unit. However, the following proposition shows that if the norm equation

$$f^2 - g^2 d = a(x-\alpha)^m \tag{1}$$

with $m \neq 0$ fixed is soluble in polynomials $f, g \in \mathbb{F}_q[x]$, then either $f + g\sqrt{d} \in U_S$ or $f - g\sqrt{d} \in U_S$.

Proposition 4. *Let* $y = f + g\sqrt{d}$ *with* $f, g \in \mathbb{F}_q[x]$, *and let* $N_{K/k}(y) = a(x-\alpha)^m$, *where* $a \in \mathbb{F}_q^*$ *and* $m > 0$. *If* $|y|_2 = 0$, *then* $y = f + g\sqrt{d} \in U_S$, *and if* $|y|_2 > 0$, *then* $(f + g\sqrt{d})/(x-\alpha)^m \in U_S$.

Theorem 1. *Let* $S' = \{|\cdot|_\infty, |\cdot|_1, |\cdot|_2\}$ *and* $S = \{|\cdot|_\infty, |\cdot|_1\}$. *If* ε *is a fundamental* S*-unit, then* ε *and* $x - \alpha$ *are independent fundamental* S'*-units.*

The proof of Theorem 1 is based on the following observation: if δ is an arbitrary S'-unit, then, as in the S-unit case, $N_{K/k}(\delta) = a(x-\alpha)^m$. By Proposition 4, we have either $\delta \in U_S$ or $\delta/(x-\alpha)^m \in U_S$. In the first case $\delta = b\varepsilon^t$, while in the second case $\delta = b\varepsilon^t(x-\alpha)^m$, where $b \in \mathbb{F}_q^*$ and $t \in \mathbb{Z}$. This means that ε and $x - \alpha$ are independent fundamental S'-units.

Therefore, first of all we need to be able to compute a fundamental S-unit. With this aim, we need to find a minimal positive integer m such that the equation (1) has a solution in polynomials $f, g \in \mathbb{F}_q[x]$. Then either $f + g\sqrt{d}$ or $f - g\sqrt{d}$ is a fundamental S-unit.

Let $v = x - \alpha$, and let k_v be a completion of k with respect to the valuation $|\cdot|_v$. The field k_v can be identified with the field $\mathbb{F}_q((v))$ of formal power series. Since the valuation $|\cdot|_v$ has two extensions to K, we have $\sqrt{d} \in \mathbb{F}_q((v))$. Let $\sqrt{d} = \sum_{i=0}^{\infty} d_i v^i$. The following theorem provides an algorithm for finding a fundamental S-unit.

Theorem 2. *Let* $n = (\deg d - 1)/2$. *For an integer* $r \geqslant n$ *consider the matrices*

$$D_r = \begin{pmatrix} d_{n+1} & d_{n+2} & \dots & d_{r+1} \\ d_{n+2} & d_{n+3} & \dots & d_{r+2} \\ \dots & \dots & \dots & \dots \\ d_{n+r} & d_{n+r+1} & \dots & d_{2r} \end{pmatrix} \quad \text{and} \quad H_r = \begin{pmatrix} d_{n+2} & d_{n+3} & \dots & d_{r+2} \\ d_{n+3} & d_{n+4} & \dots & d_{r+3} \\ \dots & \dots & \dots & \dots \\ d_{n+r+1} & d_{n+r+2} & \dots & d_{2r+1} \end{pmatrix}.$$

If $m = 2r + 1$ *is odd, then the norm equation* (1) *has a solution in non-zero polynomials* $f, g \in \mathbb{F}_q[x]$ *if and only if* $\operatorname{rank} D_r < r - n + 1$, *and if* $m = 2r$ *is even, then* (1) *has a solution* $f, g \in \mathbb{F}_q[x]$ *if and only if* $\operatorname{rank} H_{r-1} < r - n$.

If K is the function field of an elliptic curve, then D_r and H_r are square matrices. In this case determinants of the special kind in Theorem 2 were first considered by Jacobi in the 19th century. They are called 'persymmetric determinants' and the corresponding matrices are known as 'Hankel matrices'.

Remark. We have restricted ourselves here to valuations associated with points on hyperelliptic curves over a field $\mathbb{F}_q$. In fact, similar results are valid for arbitrary valuations on the field $\mathbb{F}_q(x)$.

Bibliography

[1] A. Weil, *Basic number theory*, Grundlehren Math. Wiss., vol. 144, Springer, New York 1967.

[2] З. И. Боревич, И. Р. Шафаревич, *Теория чисел*, Наука, Москва 1964; English transl., Z. I. Borevich and I. R. Shafarevich, *Number theory*, Pure Appl. Math., vol. 20, Academic Press, New York–London 1966.

V. V. Benyash-Krivets
Belorussian State University
E-mail: benyash@bsu.by

V. P. Platonov
Scientific Research Institute for Systems Analysis,
Russian Academy of Sciences
E-mail: platonov@niisi.ras.ru

Presented by V. M. Buchstaber
Accepted 16/JUL/07
Translated by THE AUTHORS