$= \operatorname{rank} \psi(W)$. Therefore the first lower bound for rank $H(Q(\sqrt[l]{p}))$ in the corollary to Theorem 2.3 becomes $2+\operatorname{rank} H(k)^{(\theta)}-\operatorname{rank} \psi(W)$; in particular this says that the l-class group $H(Q(\sqrt[l]{p}))$ is not cyclic.

References

[1] A. Fröhlich, *The genus group and genus field in finite number fields*, (I) Mathematika 6 (1959), pp. 40–46; (II) ibid., pp. 142–146.

[2] F. Gerth III, *Ranks of 3-class groups of non-Galois cubic fields*, Acta Arith. 30 (1977), pp. 302–322.

[3] G. Gras, *Sur les l-classes d'idéaux dans les extensions cycliques relatives de degré premier l*, Ann. Inst. Fourier 23,3 (1973), pp. 1–48.

[4] – *Sur le 3-rang des corps cubiques non galoisiens*, Séminaire de Théorie des Nombres, Besançon, 1974–75.

[5] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, Physica-Verlag, Würzburg-Wien 1970.

[6] F. Halter-Koch, *Ein Satz über die Geschlechter relativ-zyklischen Zahlkörper von Primezahlgrad und seine Anwendung auf biquadratische-bizyklische Körper*, J. Number Theory 4 (1972), pp. 144–156.

[7] T. Honda, *Pure cubic fields whose class numbers are multiples of* 3, ibid. 3 (1971), pp. 7–12.

[8] K. Iimura, *A criterion for the class number of a pure quintic field to be divisible by* 5, J. Reine Angew. Math. 292 (1977), pp. 201–210.

[9] M. Ishida, *An algorithm for constructing the genus field of an algebraic number field of odd prime degree*, J. Fac. Sci. Univ. Tokyo, Sec. IA, 24 (1977), pp. 61–75.

[10] J. F. Jaulent, *Structures galoisiennes dans les extensions métabéliennes*, Thèse, 3ème cycle, Besançon, 1979.

[11] – *Unités et classes dans les extensions métabéliennes de degré nl^s sur un corps de nombres algébriques*, Ann. Inst. Fourier 31,1 (1981), pp. 39–62.

[12] S. Kobayashi, *Complete determination of the 3-rank in pure cubic fields*, J. Math. Soc. Japan 29 (1977), pp. 373–384.

[13] J. Porusch, *Die Arithmetik in Zahlkörpern, deren zugehörige Galoissche Körpern spezielle metabelsche Gruppen besitzen, auf klassenkörpertheoretischer Grundlage*, Math. Zeit. 37 (1933), pp. 134–160.

[14] C. Walter, *The ambiguous class group and the group of certain non-normal extensions*, Mathematika 26 (1979), pp. 113–124.

THE METROPOLITAN COLLEGE OF TECHNOLOGY
6-6 ASAHIGAOKA, HINO, TOKYO 191, JAPAN

Received on 31. 1. 1985
and in revised form on 15. 5. 1985 (1490)

ACTA ARITHMETICA
XLVII (1986)

LeVeque's superelliptic equation over function fields

by

R. C. Mason (Cambridge) and B. Brindza (Debrecen)

1. Introduction. In a letter to Mordell written in 1925, later published, Siegel [9] proved that the hyperelliptic equation $y^2 = g(x)$ has only finitely many solutions in integers x and y: g denotes a polynomial with integer coefficients, possessing at least three simple zeros. Siegel's later investigations revealed his celebrated theorem [10] concerning the solutions of any polynomial equation $F(x, y) = 0$: he proved that there are only finitely many integer solutions, unless the curve associated with F has genus zero and no more than two infinite valuations. Siegel's proof was ineffective: he employed both the Mordell–Weil theorem and his own theorem on the approximation of algebraic numbers by rationals, which was a development of the pioneering work of Thue. In 1964 LeVeque [3] generalized Siegel's result on the hyperelliptic equation to prove that the superelliptic equation $y^m = f(x)$ has only finitely many solutions in any ring of algebraic integers, unless of course it falls into the exceptional cases predicted by Siegel's general theorem. The conditions on f and m equivalent to the exceptional cases are given below (1). LeVeque's result was ineffective. In 1968 Baker proved the first general effective result on Diophantine equations by employing his celebrated lower bound for linear forms in logarithms: he effectively solved first the Thue equation, and then the hyperelliptic and certain superelliptic equations [1]. Baker's bounds were improved by Sprindžuk [11], [12]. LeVeque's theorem of 1964 was recently made completely effective by Brindza [2].

This paper is devoted to establishing a bound on the solutions of LeVeque's equation in the analogous case of function fields. Let k denote an algebraically closed field of characteristic zero, and $k(z)$ the rational function field over k. Let us consider the set of solutions X, Y in the ring of polynomials $k[z]$ of the hyperelliptic equation $Y^2 = G(X)$, where G is a polynomial with coefficients in $k[z]$ and possessing at least three simple zeros. It is plainly possible for this equation to have infinitely many solutions, for example if the coefficients of G actually lie in k. However, it is

possible to bound the degrees of the polynomial solutions X and Y, and Schmidt [9] succeeded in doing so in 1978. Schmidt's approach was developed from the work of Osgood, and his from Kolchin, on algebraic differential equations. In 1981 Mason discovered an entirely new approach to equations over function fields [4]. By means of a fundamental inequality (see Lemma 1 below) he was able to establish bounds on the degrees of the solutions which greatly improved on those of Schmidt [5]. Moreover, the method actually led to an algorithm by which all the solutions of the hyperelliptic equation in $k[z]$ could be determined.

Now let K denote an arbitrary finite extension of the rational function field $k(z)$, of genus g_K, say. Corresponding to K is an algebraic curve C defined over k, where the points of C correspond to valuations on K. We shall blur the distinction between points of C and the valuations; moreover, we shall assume that the valuations are additive with value group $\boldsymbol{Z}$. If S is a finite subset of C, then we can consider the ring $\mathcal{O}_S$ of elements α of K with $v(\alpha) \geqslant 0$ for v outside S; that is, all the poles of α lie in S. We shall be concerned with the solutions in $\mathcal{O}_S$ of the equation

$$(*) \qquad Y^m = F(X),$$

where F is a polynomial with coefficients in K. The notion on K corresponding to 'degree' on $k[z]$ is 'height': we define

$$H_K(\alpha) = -\sum_{v \in C} \min(0, v(\alpha)).$$

For a polynomial f over K and a valuation v, we define $v(F)$ to be the smallest of the $v(\alpha)$ as α ranges over the coefficients of F: the height of F is then defined as above. The final ingredient needed before stating our theorem is some information on the factorisation of F which corresponds to certain invariants on the curve associated with $(*)$. We suppose that L is a finite extension of K in which F factorises completely, say

$$F(X) = \alpha \prod_{i=1}^{n} (X - \alpha_i)^{r_i},$$

where $\alpha_1, \ldots, \alpha_n$ are distinct. Let us write $t_i = m/(m, r_i)$ for $i = 1, \ldots, n$. We shall prove the following theorem.

THEOREM. *Provided that $(t_1, \ldots, t_n)$ is not a permutation of either $(t, 1, \ldots, 1)$ or $(2, 2, 1, \ldots, 1)$ (λ), all the solutions X, Y in $\mathcal{O}_S$ of $(*)$ satisfy*

$$H_K(X) \leqslant 78 H_K(F) + 12 g_K + 6|S|,$$

where $|S|$ denotes the cardinality of S. Furthermore, in the exceptional cases (λ), we can find an extension field K' of K and a set of valuations S' on K' such that $(*)$ has a family of solutions in $\mathcal{O}_{S'}$ of unbounded height.

It is easy to see that the exceptions covered by (λ) are in exact correspondence with those discovered by Siegel in [10]: the curve associated with $(*)$ then has genus zero, and the infinite valuations number one and two respectively. Our bound may be compared with those of Schmidt, $10^6(H_K(F) + g_K + |S|)$ and Mason, $26H_K(F) + 8g_K + 4|S|$, both for the hyperelliptic equation. It should also be mentioned that, by using the fundamental inequality in a different way, Mason was able to establish ([6], p. 120) bounds on the heights of all the solutions in K, not just those in $\mathcal{O}_S$, of the superelliptic equation $(*)$, subject to certain degree restrictions.

In the next section we shall recall the fundamental inequality first proved by Mason in 1983, together with a genus estimate which will be of considerable value here. The proof of the theorem will then follow from an indirect application of the fundamental inequality. The exact form in which the inequality is applied depends on the integers $t_1, \ldots, t_n$: there are three cases to consider, the first two are disposed of in Section 3, and the third in Section 4.

2. Preliminaries. The following inequality has formed the crucial step in the effective resolutions of the various families of equations over function fields. Proofs of the inequality may be found in [5] or [6], p. 14.

LEMMA 1. *Suppose that γ_1, γ_2 and γ_3 are non-zero elements of K with $\gamma_1 + \gamma_2 + \gamma_3 = 0$. Let us further suppose that there is a finite set $\mathcal{V}$ of valuations on K such that $v(\gamma_1) = v(\gamma_2) = v(\gamma_3)$ for v outside $\mathcal{V}$. Then either γ_1/γ_2 lies in k, in which case $H_K(\gamma_1/\gamma_2) = 0$, or*

$$H_K(\gamma_1/\gamma_2) \leqslant |\mathcal{V}| + 2g_K - 2.$$

In the case of the Thue equation $f(X, Y) = \mu$, the inequality is applied directly to the identity

$$(X - \alpha_1 Y)(\alpha_2 - \alpha_3) + (X - \alpha_2 Y)(\alpha_3 - \alpha_1) + (X - \alpha_3 Y)(\alpha_1 - \alpha_2) = 0,$$

where each $X - \alpha_i Y$ is a factor of the binary form f. A direct application is also made in the case of the hyperelliptic equation (see § 4). However, in the case of the superelliptic equation an indirect approach yields much better bounds (see § 3). In the proof it will be necessary to factorise F partially by adjoining some of the zeros $\alpha_1, \ldots, \alpha_n$, and in order to employ Lemma 1 we need a bound on the resulting growth in the genus. This is achieved in the following ([6], p. 67).

LEMMA 2. *Let $P(X)$ denote a non-zero polynomial of degree n with coefficients in K. If M is the field obtained by adjoining some zero α of P to K, then*

$$g_M \leqslant 1 + [M : K]\{g_K - 1 + \tfrac{3}{2}(1 - 1/n) H_K(P)\}.$$

We observe that if L is any finite extension of K, and w is a valuation on L, then there is a valuation v on K and an integer e_w such that $w(\alpha)$

$= e_w v(\alpha)$ for α in K: we write $w|v$. Since $\sum_{w|v} e_w = [L:K]$ for each v, we deduce that

$$H_L(\alpha) = [L:K]\, H_K(\alpha)$$

for α in K. The following inequality on the height function is readily established:

$$\max\{H_K(\alpha+\beta),\, H_K(\alpha\beta)\} \leqslant H_K(\alpha)+H_K(\beta)$$

for any α, β in K.

Henceforth L will denote a finite extension of K in which F factorises completely as above. Elementary manipulations with the height function yield ([6], p. 9)

$$H_K(\alpha) \leqslant H_K(F) \quad \text{and} \quad \sum_{i=1}^{n} r_i H_K(\alpha_i) \leqslant H_K(F).$$

If any r_i happens to be divisible by m, then we may rewrite the equation $Y^m = F(X)$ as

$$Z^m = G(X),$$

where

$$Z = Y/\prod_{m|r_i} (X-\alpha_i)^{r_i/m} \quad \text{and} \quad G(X) = \alpha \prod_{m\nmid r_i} (X-\alpha_i)^{r_i}.$$

It is evident that G has coefficients in K and height at most that of F. The solutions of (*) with $X = \alpha_i$, which have been lost in this process, satisfy $H_K(X) \leqslant H_K(F)$, and thus automatically satisfy the theorem. Thus we may in fact assume that m does not divide any r_i, and that X, Y is a solution of (*) with X in $\mathcal{O}_S$ and Y in K^*. Hence $t_i \geqslant 2$ for each i. We further assume, as we may, that the indices $1, \ldots, n$ are chosen in such a way that $H_L(\alpha_1) \leqslant \ldots \leqslant H_L(\alpha_n)$. We shall denote by $f(X)$ the product $\prod_{i=1}^{n} (X-\alpha_i)$, so f has coefficients in K and height at most that of F. We now deal with three cases separately, the first when $t_1 \geqslant 3$ or $t_2 \geqslant 3$, the second when $t_1 = t_2 = 2$ and $t_3 \geqslant 3$, and the third when $t_1 = t_2 = t_3 = 2$. Since F does not satisfy (†) at least one of these three situations obtains.

3. The first two cases. We assume first that $\max(t_1, t_2) \geqslant 3$. Let us denote by M the subfield of L obtained by adjoining α_1 and α_2 to K. We shall apply Lemma 1 to the equation

$$(X-\alpha_1)+(\alpha_2-X)+(\alpha_1-\alpha_2) = 0,$$

where X is a fixed element of $\mathcal{O}_S$ and Y is a non-zero element of K such that $Y^m = F(X)$. First we estimate the genus of M. From a double application of

Lemma 2 with $P = f$ we obtain

$$g_M \leqslant d\big(g_K + 3(1-1/n)\, H_K(f)\big),$$

where $d = [M:K]$. Let $\mathcal{W}$ denote the set of valuations w on M at which at least one of the following occurs: $w(F) < 0$, $w(\alpha) > 0$, $w\big(f'(\alpha_1)\big) > 0$, $w\big(f'(\alpha_2)\big) > 0$, or $w|v$ for some v in S: thus

$$|\mathcal{W}| \leqslant H_M(F)+H_M(\alpha)+\{(n-1)\, H_M(\alpha_1)+H_M(f)\} + \{(n-1)\, H_M(\alpha_2)+H_M(f)\}+d|S|.$$

However, from the ordering of $\alpha_1, \ldots, \alpha_n$ we have

$$H_M(\alpha_1)+H_M(\alpha_2) \leqslant 2H_M(F)/n,$$

and hence

$$|\mathcal{W}| \leqslant d\{|S|+(6-(2/n))\, H_K(F)\}.$$

Let $\mathcal{W}_i$, $i = 1, 2$, denote the set of valuations w outside $\mathcal{W}$ such that $w(X-\alpha_i) > 0$. Now whenever w lies outside $\mathcal{W}$ we obtain $w(\alpha_i) \geqslant 0$ for $i = 1, 2$, $w(X) \geqslant 0$, $w(\alpha_1-\alpha_2) = 0$, $w(\alpha) = 0$ and $w\big(f'(\alpha_i)\big) = 0$. If in fact w lies in $\mathcal{W}_i$ then $w(X-\alpha_j) = 0$ for $j \neq i$, and so

$$r_i\, w(X-\alpha_i) = m w(Y),$$

and in particular t_i divides $w(X-\alpha_i)$. We conclude that

$$t_i |\mathcal{W}_i| \leqslant H_M(X-\alpha_i) \quad (i = 1, 2).$$

If w lies outside $\mathcal{W}_1$, $\mathcal{W}_2$ and $\mathcal{W}$ then $w(X-\alpha_1) = w(X-\alpha_2) = w(\alpha_1-\alpha_2) = 0$, so we may apply Lemma 1 to obtain

$$H_M\left(\frac{X-\alpha_1}{\alpha_1-\alpha_2}\right) \leqslant |\mathcal{W}_1|+|\mathcal{W}_2|+|\mathcal{W}|+2g_M.$$

A combination of this inequality with the bounds above on each of the terms on the right-hand side, together with the inequality

$$H_M(X) \leqslant H_M\left(\frac{X-\alpha_1}{\alpha_1-\alpha_2}\right)+2H_M(\alpha_1)+H_M(\alpha_2)$$

derived from the height inequalities in Section 2, yields the truth of the theorem in the first case.

In the second case, when $t_1 = t_2 = 2 < t_3$, we use the same method as above, but applied to the equation

$$(X-\alpha_1)+(\alpha_3-X)+(\alpha_1-\alpha_3) = 0.$$

Here we denote by M the subfield of L obtained by adjoining α_1 and α_3 to K. The details of the proof are similar to those above, only the slight modification to $H_M(\alpha_1)+H_M(\alpha_3) \leqslant 3H_M(f)/n$ is required.

4. Final case. Here we suppose that $t_1 = t_2 = t_3 = 2$. Now we denote by M the subfield of L obtained by adjoining α_1, α_2 and α_3 to K: as before we write $d = [M : K]$. A triple application of Lemma 2 yields

$$g_M \leqslant d\{g_K + \tfrac{9}{2}(1-1/n)H_K(f)\}.$$

Let $\mathscr{W}$ denote the set of valuations w on M at which $w(F) < 0$, $w(\alpha) > 0$, $w(f'(\alpha_i)) > 0$, $i = 1, 2$ or 3, or $w|v$ for some v in S; we obtain the bound

$$|\mathscr{W}| \leqslant d\{|S| + (8-(3/n))H_K(F)\}.$$

As usual X, Y denotes a fixed solution of (*) with X in $\mathscr{O}_S$, Y in K^*. Now write N for the field obtained from M by adjoining the square roots of $X-\alpha_1$, $X-\alpha_2$ and $X-\alpha_3$: From (*) we deduce that $w(X-\alpha_i)$ is even for w outside $\mathscr{W}$, $i = 1, 2, 3$, and so ramification from M to N only occurs inside $\mathscr{W}$. From [6], p. 34, we see that $2g_N - 2 + |\mathscr{X}| = [N : M](2g_M - 2 + |\mathscr{W}|)$, where $\mathscr{X}$ denotes the set of valuations n on N such that $n|w$ for some w in $\mathscr{W}$. The fundamental inequality can now be applied directly with $\mathscr{V} = \mathscr{X}$ and

$$\gamma_1 = \pm\sqrt{X-\alpha_2} \pm \sqrt{X-\alpha_3},$$

and γ_2, γ_3 determined by permutation of the suffices 1, 2, 3; the signs being chosen so that $\gamma_1 + \gamma_2 + \gamma_3 = 0$. Lemma 1 then yields ([6], p. 34)

$$H_N\left(\frac{2X-\alpha_1-\alpha_3}{\alpha_2-\alpha_1}\right) \leqslant 4(2g_N + |\mathscr{X}|).$$

The proof of the theorem is then completed by combining this last with the inequalities above. It will be observed that the difference in the use of the fundamental inequality between Sections 3 and 4 is that in the latter the set $\mathscr{V}$ is independent of the solution X, Y of (*), but in the former it is not.

Finally, we deal with the necessity of the condition (†). If $t_1 = t$ and $t_2 = \ldots = t_n = 1$, then we choose K' to be a field such that α is an mth power, and S' to contain the poles of $\alpha_1, \ldots, \alpha_n$. In this case writing $X = \alpha_1 + T^m$ for any T in $\mathscr{O}_{S'}$ forms a set of solutions of unbounded height. Similarly, if $t_1 = t_2 = 2$ and $t_3 = \ldots = t_n = 1$, then the equation (*) may be transformed into $R^2 - \alpha T^2 = \beta$, where X is a polynomial in T and Y is a polynomial in R and T. Choosing K' to contain the square root of α, and S' to contain the poles of $\alpha_1, \ldots, \alpha_n$, together with the zeros and poles of some non-constant η in K', writing $R + \sqrt{\alpha}T = \eta^m$ provides a set of solutions of unbounded height as $m \to \infty$.

References

[1] A. Baker, *Bounds for the solutions of the hyperelliptic equation*, Proc. Cambridge Philos. Soc. 65 (1969), pp. 439–444.

[2] B. Brindza, *On S-integral solutions of the equation* $f(x) = y^m$, Acta Math. Hungar., to appear.

[3] W. J. LeVeque, *On the equation* $y^m = f(x)$, Acta Arith. 9 (1964), pp. 209–219.

[4] R. C. Mason, *On Thue's equation over function fields*, J. London Math. Soc. Ser. 2, 24 (1981), pp. 414–426.

[5] – *The hyperelliptic equation over function fields*, Proc. Cambridge Philos. Soc. 93 (1983), pp. 219–230.

[6] – *Diophantine equations over function fields*, LMS Lecture Notes No. 96, Cambridge University Press.

[7] W. M. Schmidt, *Thue's equation over function fields*, J. Austral. Math. Soc. Ser. A 25 (1978), pp. 385–422.

[8] – *Polynomial solutions of* $F(x, y) = z^n$, Queen's Papers in Pure Appl. Math. 54 (1980), pp. 33–65.

[9] C. L. Siegel, *The integer solutions of the equation* $y^2 = ax^n + bx^{n-1} + \ldots + k$, J. London Math. Soc. 1 (1926), pp. 66–68 (under the pseudonym X).

[10] – *Über diophantische Gleichungen*, Abh. Preuss. Akad. Wiss. (1929) No. 1, pp. 41–70.

[11] V. G. Sprindžuk, *Square-free divisors of polynomials and class numbers of algebraic number fields*, Acta Arith. 24 (1973), pp. 143–149.

[12] – *A hyperelliptic Diophantine equation and class numbers* (in Russian), ibid. 30 (1976), pp. 95–108.

GONVILLE AND CAIUS COLLEGE
CAMBRIDGE, U.K.

INSTITUTUM MATHEMATICUM
UNIVERSITATIS DEBRECENIENSIS
H-4010 DEBRECEN PF. 12, HUNGARY

Received on 22. 2. 1985 (1497)