September 20, 2011

The following corrections are made after detailed questions in the proces of writing [7] by Philippe Piret (e-mail: philippe.piret@crf.canon.fr):
"Reading notes on section 3 ... ,[6]" in February 2005.
A copy one can find at item [31] of [11].

I thank him cordially for drawing our attention to these mistakes.

Ruud Pellikaan

Corrections and addenda of Section 3.2 on curves of type II

1) Consider a polynomial of the form:

$$X^aY^c + Y^{b+c} + G(X,Y)$$

The assumption:

$$\text{“}\deg(G) < b + c\text{”}$$

in Proposition 3.17 and Corollary 3.18 should be sharpened to

$$\text{“wdeg}(G) < a(b + c)\text{”}$$

where the weighted degree of $X^\alpha Y^\beta$ is $\alpha b + \beta a$.
Notice that $\text{wdeg}(X^aY^c) = \text{wdeg}(Y^{b+c}) = a(b + c)$.

2) Clearly the condition $\text{wdeg}(G) < ab$ in case $c = 0$, implies $\deg(G) < \min\{a, b\}$. This sharpened condition can be found in the papers [2,3]. On page 18 of the notes there is the question whether the assumption $\text{wdeg}(G) < ab$ as could be found in several Japanese papers, is allowed. This is indeed the case.

3) The following example shows that the assumption

$$\deg(G) < b + c \text{ instead of } \text{wdeg}(G) < a(b + c)$$

is certainly not enough. Consider for instance the polynomial:

$$F = (Y^3 + X + 1)(Y^2 + X) = X^2 + Y^5 + G,$$

with $G = XY^3 + XY^2 + X + Y^2$. Then clearly F is not irreducible and F is of the form $X^aY^c + Y^{b+c} + G$ with

$$c = 0,\ a = 2,\ b = 5,\ d = \deg_X(G) = 1 < a \text{ and } \deg(G) = 4 < 5 = b.$$

But $\mathrm{wdeg}(G) = 1.5 + 3.2 = 11$ is not strictly smaller than $10 = a.b$.

4) The proof in the notes in case $c = 0$ can without much effort adapted to the case $\mathrm{wdeg}(G) < ab$ instead of $\deg(G) < \min\{a, b\}$. See instance (21) in the notes becomes:

$$\ldots ab - a\beta - \alpha b = ab - \mathrm{wdeg}(G) > 0.$$

5) Clearly something went wrong in the chapter [3]. As noticed, the argument on the uniqueness is not correct, but more importantly the argument on the existence is flawed also, since the starting of the induction argument concerning ε on page 909 is not checked, which is exactly the statement that: $\mathrm{wdeg}(G) < a(b + c)$.

6) On page 19 of the notes a notational irregularity in the paper [3] is observed. Sometimes it is $X^aY^b + Y^{b+c} + G$ instead of $X^aY^c + Y^{b+c} + G$. This is correct. It should always be: $X^aY^c + Y^{b+c} + G$. In Example 3.16 of [3] it is claimed that the monomials

$$x^\alpha y^\beta,\ \alpha < a \text{ or } \beta < c$$

form a basis for S. This is indeed true, this can be checked by an induction argument, but it follows also from Gröbner basis theory. Since X^aY^c is the leading term of F with respect to the weighted degree lexicographic order, a basis is obtained by the complement of all monomials of the form $X^\alpha Y^\beta$ with $\alpha \geq a$ and $\beta \geq c$.

9) Another nice proof of the irreducibility of a curve with equation:

$$X^a + Y^b + G(X, Y) \text{ with } \mathrm{wdeg}(G) < ab$$

is given in Corollary 2.7 of the paper [1] and it is from [2, pp. 503]. It uses the fact that the corresponding Newton diagram is integrally indecomposable. This result is attributed to Stepanov-Schmidt [9, 10, 8].

10) The mistakes as noted are corrected in the present edition of the chapter [3] on the webpage [11].

References

[1] P. Beelen and R. Pellikaan, "The Newton polygon of plane curves with many rational points," *Designs, Codes and Cryptography*, vol. 21, pp. 41-67, Oct. 2000.

[2] S. Gao, "Absolute Irreducibility of Polynomials via Newton Polytopes," *J. Algebra,* vol 237, pp. 501-520 , 2001.

[3] T. Høholdt, J. van Lint and R. Pellikaan, "Algebraic geometry codes," in Handbook of Coding Theory, vol 1, pp. 871-961, V.S. Pless, W.C. Huffman and R.A. Brualdi Eds., Elsevier, Amsterdam 1998.

[4] M.S. Kolluru, G.L. Feng and T.R.N. Rao, "Construction of improved geometric Goppa codes from Klein curves and Klein-like curves," *AAECC,* vol. 10, pp. 433-464, 2000.

[5] R. Pellikaan, "On the existence of order functions," *Journal of Statistical Planning and Inference*, vol. 94, pp. 287-301, 2001.

[6] P. Piret, "Reading notes on section 3 of 'Algebraic Geometry Codes' by T. Høholdt, J. van Lint and R. Pellikaan, [3]", February 2005.

[7] P. Le Bars and P. Piret, "Aggregate error locator and error value computation in AG codes," *Journ. Comb. Theory*, Series A, vol. 113, pp. 1771-1782, 2006.

[8] W.M. Schmidt, "Equations over a finite field: an elementary approach," *Lect. Notes Math.*, vol. 536, Springer-Verlag, Berlin 1976.

[9] S.A Stepanov, "Congruences with two unknowns," *Izv. Akad. Nauk. SSSR* Ser. Mat. 36, pp. 683-711, 1972.

[10] S.A Stepanov, "Rational points of algebraic curves over finite fields," in *Current problems of analytic number theory* (Proc. Summer school, Minsk 1972), 272, pp. 223-243, Nauka, Minsk, 1974.

[11] *www.win.tue.nl/ ~ ruudp/publications.html*