15 years of computing power integral bases

István Gaál

University of Debrecen
Mathematical Institute

ANTS VII, Berlin TU, 2006 July

Let K be an alg. number field of degree n
$\mathbb{Z}_K$: ring of integers
Define the index of $\alpha \in \mathbb{Z}_K$ by

$$I(\alpha) := (\mathbb{Z}_K^+ : \mathbb{Z}^+[\alpha]).$$

min index of K: $\mu(K) = \min\{I(\alpha) | \alpha \in \mathbb{Z}_K, K = \mathbb{Q}(\alpha)\}$

$\{1, \alpha, \ldots, \alpha^{n-1}\}$ power integral basis $\iff I(\alpha) = 1$.

For any integral basis $\{1, \omega_2, \ldots, \omega_n\}$ we have
$D_{K/Q}(X_2\omega_2 + \ldots + X_n\omega_n) = (I(X_2, \ldots, X_n))^2 D_K$
$I(X_2, \ldots, X_n)$: index form

$\alpha = x_1 + \omega_2 x_2 + \ldots + \omega_n x_n \in \mathbb{Z}_K$: $I(\alpha) = |I(x_2, \ldots, x_n)|$.

Hence the problem of determining power integral bases is equivalent to solving the index form equation $I(\alpha) = 1 \iff$

$$I(x_2, \ldots, x_n) = \pm 1 \quad (x_2, \ldots, x_n \in \mathbb{Z})$$

Example
Let $3 \le a \in \mathbb{Z}$ and ϑ of $f(x) = x^3 - ax^2 - (a+3)x - 1$.
In $\mathcal{O} = \mathbb{Z}[\vartheta]$ an integral basis is $\{1, \vartheta, \vartheta^2\}$, the corresponding index form equation is
$I(x, y) = x^3 + 2ax^2y + (a^2 - a - 3)xy^2 + (-a^2 - 3a - 1)y^3 = \pm 1$.
Up to equivalence all generators of power integral bases in $\mathcal{O}$ are $\alpha = \vartheta$, $\alpha = -a\vartheta + \vartheta^2$, $\alpha = (1 + a)\vartheta - \vartheta^2$.

Purpose:
Determine all power integral bases in K by solving the index form equation
Develop algoritms for the resolution of index form equations

Components of the algorithms:
Application of Baker's method (A.Baker, K.Győry)
reduction of the bounds (B.M.M de Weger, A.Pethő and R.Schulenberg, Y.Bilu and G.Hanrot, I.Gaál and M.Pohst)
testing the "small" possible solutions
sieving
ellipsoid method: K.Wildanger (1997)
I.Gaál and M.Pohst (1999)

Efficient algorithms:

n=3: I.Gaál-N.Schulte (1989)
n=4: I.Gaál-A.Pethő-M.Pohst (1991-1996)
biquadratic fields
I.Gaál-A.Pethő-M.Pohst (1995), M.N.Gras-F.Tanoe (1995), G.Nyul (2002), I.Gaál-G.Nyul (2003)

n=6:
with quadratic subfields: I.Gaál (1995),
I.Gaál-M.Pohst (1996)
with cubic subfields: I.Járási (2001)

n=8 with quadr. subfields: I.Gaál-M.Pohst (2000)

multiquadratic fields: G.Nyul (2002)

n=9: (with cubic subfields): I.Gaál (2000)

General but less efficient
n=5: I.Gaál-K.Győry (1999)
n=6: Y.Bilu-I.Gaál-K.Győry (2003)

$K = LM$ composite fields:
I.Gaál, P.Olajos, M.Pohst (1998-2004)

cyclotomic fields: L.Robertson
infinite parametric families of fields
function field case

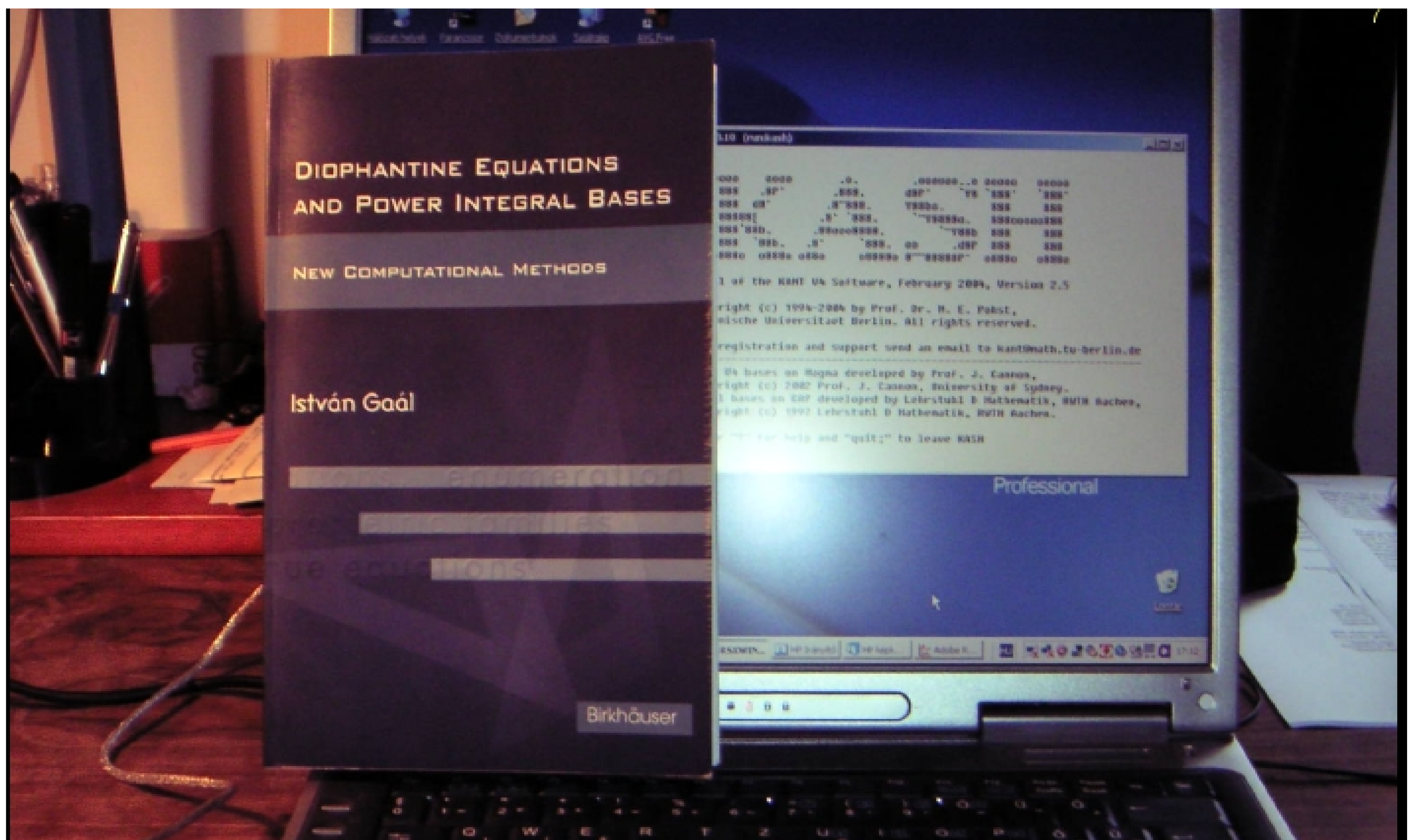
The average behaviour of the minimal index for certain quartic fields

Galois groups: C_4, V_4, D_4, S_4, A_4

r: tot real, c: tot complex

taking average of the minimal indices of the fields with discriminants D in the given intervals

average		behaviour	$V_4(r)$	$D_4(r)$	$S_4(c)$
		# :	196	4486	44122
$0 <$	D	$< 10^5$	7.7	4.1	2.2
$10^5 \le$	D	$< 2 \cdot 10^5$	20.9	8.0	3.3
$2 \cdot 10^5 \le$	D	$< 3 \cdot 10^5$	29.1	11.0	3.8
$3 \cdot 10^5 \le$	D	$< 4 \cdot 10^5$	21.2	13.3	4.4
$4 \cdot 10^5 \le$	D	$< 5 \cdot 10^5$	35.9	15.9	4.8
$5 \cdot 10^5 \le$	D	$< 6 \cdot 10^5$	37.4	17.9	5.2
$6 \cdot 10^5 \le$	D	$< 7 \cdot 10^5$	39.3	20.0	5.5
$7 \cdot 10^5 \le$	D	$< 8 \cdot 10^5$	45.2	22.5	5.7
$8 \cdot 10^5 \le$	D	$< 9 \cdot 10^5$	39.1	25.0	5.9
$9 \cdot 10^5 \le$	D	$< 10^6$	61.3	25.2	6.0



Tables:
http://www.math.klte.hu/ ~ igaal