dr hab. inż. Adam Woryna, prof. Pol. Śl.
Wydział Matematyki Stosowanej
Politechnika Śląska
Gliwice, 01.08.2022r.

Recenzja rozprawy doktorskiej mgra Mawunyo Kofi Darkey-Mensah pt.
"Algorithms For Quadratic Forms Over Global Functions Fields"
dla Rady Instytutu Matematyki Uniwersytetu Śląskiego

1 Cel rozprawy

Rozprawa poświęcona jest formom kwadratowym $q(X) = q(x_1, \ldots, x_n) = \sum_{i,j=1}^{n} a_{ij}x_ix_j = XAX^t$, gdzie $X = (x_1, \ldots, x_n)$ jest wektorem zmiennych, a współczynniki a_{ij} macierzy symetrycznej $A = [a_{ij}]$ należą do globalnego ciała funkcyjnego. Choć badania from kwadratowych nad różnymi ciałami K są intensywnie prowadzone od wielu lat i obecnie tworzą bogatą gałęź algebraicznej teorii liczb, to dosyć słabo rozwinięty jest aspekt obliczeniowy tej teorii, a większość prac na tym polu koncentruje się na formach nad ciałem liczb wymiernych. Znane od dawna problemy obliczeniowe teorii form kwadratowych nad ustalonym ciałem K dotyczą m.in. takich fundamentalnych pojęć jak izotropowość, hiperboliczność, rozkład Witta oraz podobieństwo w sensie Witta lub w sensie Ono. Tylko dla niektórych ciał (np. dla ciał skończonych lub dla ciała liczb rzeczywistych lub ciała liczb zespolonych) problemy te okazują się trywialne. Dla ciała liczb wymiernych rozwiązania uzyskano w pracach m.in. J. E. Cremona i D. Rusina, D. Simona, P. Castela. Całkiem niedawno P. Koprowski, A. Czogała i B. Rothkegel opracowali odpowiednie algorytmy dla ciał liczbowych (skończonych rozszerzeń ciała $\mathbb{Q}$). Celem rozprawy jest opracowanie efektywnych algorytmów dla form kwadratowych nad dowolnym globalnym ciałem funkcyjnym K skończonej charakterystyki $\mathrm{char}(K) \neq 2$, czyli ciałem będącym skończonym rozszerzeniem ciała $\mathbb{F}_q(x)$ funkcji wymiernych jednej zmiennej nad skończonym ciałem Galois $\mathbb{F}_q$ (o którym dodatkowo zakłada się, że jest algebraicznie domknięte w K). Skonstruowane w rozprawie algorytmy wykorzystują znane w literaturze metody obliczeniowe związane z elementami ciał globalnych, ich uzupełnień oraz formami kwadratowymi nad tymi ciałami. Każdy z opracowanych algorytmów zilustrowano odpowiednim przykładem, a obliczenia wykonano w systemie Magma.

2 Zawartość rozprawy

Rozprawa jest napisana w języku angielskim, liczy 67 stron i składa się z 6 rozdziałów, przy czym rozdział 1 stanowi wstęp. Podstawowe pojęcia dotyczące ciał globalnych oraz form kwadratowych zdefiniowano w rozdziale 2.

W podrozdziale 2.1 opisano globalne ciało funkcyjne K jako ciało ułamków pierścienia ilorazowego $O_K := \mathbb{F}_q[x, y]/\langle F \rangle$, gdzie $F \in \mathbb{F}_q[x, y]$ jest dowolną krzywą algebraiczną. Pierścień

O_K stanowi całkowite domknięcie pierścienia $\mathbb{F}_q[x]$ w ciele K i jest przykładem pierścienia Dedekinda. Zatem każdy niezerowy ideał pierwszy pierścienia O_K jest jego ideałem maksymalnym, a każdy jego ułamkowy ideał właściwy $\mathfrak{a} \neq \{0\}$ ma jednoznaczne przedstawienie w postaci iloczynu potęg $\mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_m^{e_m}$ ideałów pierwszych z wykładnikami całkowitymi $e_i \in \mathbb{Z}$. W szczególności każdy ideał pierwszy $\mathfrak{p}$ pierścienia O_K definiuje na ciele K dyskretną waluację wykładniczą $\nu_\mathfrak{p}\colon K \to \mathbb{Z} \cup \{\infty\}$ (tzw. waluacja $\mathfrak{p}$-adyczna), gdzie dla każdego $a \in \dot{K}$ wartość $\nu_\mathfrak{p}(a) \in \mathbb{Z}$ jest wykładnikiem z jakim ideał pierwszy $\mathfrak{p}$ występuje w rozbiciu ideału ułamkowego głównego $O_K a = \{ba\colon b \in O_K\}$ na ideały pierwsze. Dwie waluacje wykładnicze ν, ν' ciała K nazywamy równoważnymi, jeżeli definiują na K tę samą topologię. Przez Ω_K oznacza się zbiór reprezentantów wszystkich waluacji wykładniczych ciała K. Oprócz waluacji $\mathfrak{p}$-adycznych do Ω_K należą jeszcze rozszerzenia nieskończonej waluacji ν_∞ ciała $\mathbb{F}_q(x)$ zdefiniowanej wzorem $\nu_\infty(f/g) = \deg(g) - \deg(f)$ dla $f, g \in \mathbb{F}_q[x]$ (tzw. waluacje w nieskończoności). Dla każdej waluacji $\nu \in \Omega_K$ rozpatruje się ciało z waluacją $(K_\nu, \widehat{\nu})$, będące uzupełnieniem ciała K w przestrzeni definiowanej przez metrykę $d(a,b) = 2^{-\nu(a,b)}$. Ciało K_ν jest przykładem ciała lokalnego, tzn. ciało reszt $K(\nu) := R_{\widehat{\nu}}/\langle\pi\rangle$ jest skończonym rozszerzeniem ciała $\mathbb{F}_q$, gdzie $R_{\widehat{\nu}} = \{a \in K_\nu\colon \widehat{\nu}(a) \geq 0\} \cup \{0\}$ oznacza pierścień waluacyjny ciała K_ν, a $\langle\pi\rangle = \{a \in K_\nu\colon \widehat{\nu}(a) \geq 1\} \cup \{0\} \lhd R_{\widehat{\nu}}$ jest ideałem maksymalnym generowanym przez ustalony element pierwszy $\pi \in K_\nu$ (tzn. z waluacją $\widehat{\nu}(\pi) = 1$).

W podrozdziale 2.2 przytoczono podstawowe definicje i twierdzenia dotyczące form kwadratowych oraz ich własności nad ciałami globalnymi i lokalnymi. W szczególności przypomniano, że każda forma kwadratowa nad ciałem charakterystyki $\neq 2$ jest równoważna formie diagonalnej, zapisywanej jako $\langle a_1, \ldots, a_n\rangle$, a odpowiednią diagonalizację można uzyskać np. za pomocą algorytmu zmodyfikowanej ortogonalizacji Grama-Schmidta. Jeżeli forma q zeruje się na pewnym niezerowym wektorze, to q nazywamy izotropową, a jeżeli q jest ortogonalną sumą (ozn. $\perp$) płaszczyzn hiperbolicznych $\langle 1, -1\rangle$, to q nazywamy hiperboliczną.

Do poprawnego działania skonstruowanych w rozprawie algorytmów potrzebna jest umiejętność „wyłapania" tych waluacji $\nu \in \Omega_K$, które spełniają warunek $\nu(a) \neq 0$ dla jakiegoś współczynnika a w diagonalnej postaci testowanej formy. Jeśli chodzi o waluacje $\mathfrak{p}$-adyczne, to dla ustalonego elementu $a \in \dot{K}$ nierówność $\nu_\mathfrak{p}(a) \neq 0$ zachodzi tylko dla tych ideałów pierwszych $\mathfrak{p} \lhd O_K$, które są dzielnikami ideału głównego $\langle a\rangle = aO_K$. Potrzebny jest zatem algorytm do rozkładania w pierścieniu O_K ideałów głównych na ideały pierwsze. Choć obecnie znane są takie algorytmy, to Autor opracował własną metodę (rozdział 3). Bazuje ona na takich podstawowych działaniach arytmetycznych na ideałach jak obliczanie radykału $\mathrm{rad}(\mathfrak{a})$, sumy $\mathfrak{a} + \mathfrak{b}$ i ilorazu $(\mathfrak{a}\colon \mathfrak{b})$. Dowody poprawności algorytmów z rozdziału 3 opierają się na kilku pomocniczych lematach, w których wykorzystuje się własności homomorfizmu kanonicznego $\kappa\colon \mathbb{F}_q[x,y] \twoheadrightarrow O_K$, a także kilka głębszych rezultatów, jak np. mocne twierdzenie aproksymacyjne. Dowody te przeprowadzone są szczegółowo i starannie.

W podrozdziale 4.1 opracowano metodę (Algorytmy 5–7), która testuje izotropowość dowolnej formy q nad ciałem globalnym K. Oparto ją na zasadzie Hassego, która mówi, że q jest izotropowa nad ciałem K wtedy i tylko wtedy, gdy jest izotropowa nad każdym jego uzupełnieniem K_ν, $\nu \in \Omega_K$. Jeżeli wymiar formy $\dim(q)$ jest równy 1, to q oczywiście nie jest izotropowa; jeżeli $\dim(q) = 2$, to forma q jest izotropowa wtedy i tylko wtedy, gdy w grupie klas kwadratów $\dot{K}/\dot{K}^2$ jej wyznacznik $\det(q)$ jest równy $-\dot{K}^2$. Jeżeli $\dim(q) \geq 3$, to wystarczy się upewnić, że q jest izotropowa jedynie nad ciałami lokalnymi K_ν, dla których waluacja $\nu \in \Omega_K$ nie zeruje się na co najmniej jednym współczynniku w diagonalnej postaci formy q. Jest tylko skończenie wiele takich waluacji. Dowody poprawności Algorytmów 5–7 oparto na znanym twierdzeniu mówiącym, że nad dowolnym ciałem skończonym (odp. ciałem lokal-

nym) każda nieosobliwa forma wymiaru 3 (odp. wymiaru 5) jest izotropowa. Wykorzystano także twierdzenie (Twierdzenie 2.2.16 (1)) mówiące, że jeżeli forma $q = \langle u_1, \ldots, u_n \rangle$ nad ciałem lokalnym K_ν ma współczynniki u_i odwracalne w pierścieniu O_{K_ν} (tj. spełniające warunek $\widehat{\nu}(u_i) = 0$), to q jest izotropowa wtedy i tylko wtedy, gdy forma $\overline{q} = \langle \overline{u}_1, \ldots, \overline{u}_n \rangle$ nad ciałem reszt $K(\nu)$ jest izotropowa, gdzie $\overline{u}_i$ jest obrazem u_i przy homomorfizmie kanonicznym $R_{\widehat{\nu}} \to K(\nu)$. Pomysłowo i zgrabnie Autor wykorzystuje również obserwację, że każda forma q nad ciałem K_ν jest równoważna sumie ortogonalnej $q_1 \perp \langle \pi \rangle q_2$, gdzie π jest elementem pierwszym, a formy diagonalne q_1 i q_2 mają współczynniki odwracalne w O_{K_ν}; wówczas q jest izotropowa nad K_ν wtedy i tylko wtedy, gdy co najmniej jedna z form $\overline{q}_1$ lub $\overline{q}_2$ jest izotropowa nad $K(\nu)$ (Twierdzenie 2.2.16 (2)).

W podrozdziale 4.2 skonstruowano algorytm (Algorytmy 8–9) testujący hiperboliczność dowolnej formy q nad ciałem globalnym K. W tym celu najpierw opracowano Algorytm 8 sprawdzający, czy dla zadanej waluacji $\nu \in \Omega_K$ forma $q_\nu = q \otimes K_\nu$ jest hiperboliczna. Poprawność Algorytmu 8 oparto na twierdzeniu mówiącym, że dwie formy nad dowolnym ciałem lokalnym są równoważne wtedy i tylko wtedy, gdy mają te same wymiary, wyznaczniki i niezmienniki Hassego. Następnie Autor dowodzi (dowód poprawności Algorytmu 9), że forma q jest hiperboliczna nad K wtedy i tylko wtedy, gdy spełnione są następujące warunki: wymiar $n := \dim(q)$ jest parzysty, dyskryminant $\operatorname{disc}(q) := (-1)^{n(n-1)/2} \det(q)$ jest kwadratem (tzn. elementem neutralnym w grupie $\dot{K}/\dot{K}^2$), a ponadto forma q_ν nad ciałem K_ν jest hiperboliczna dla każdej waluacji $\nu \in \Omega_K$, która nie zeruje się na co najmniej jednym współczynniku w diagonalnej postaci formy q. W dowodzie wykorzystuje się tzw. słabą zasadę Hassego, która mówi, że forma q jest hiperboliczna nad K wtedy i tylko wtedy, gdy dla każdego $\nu \in \Omega_K$ forma q_ν jest hiperboliczna nad K_ν. Jednak sam dowód nie jest przeprowadzony zbyt szczegółowo, tzn. czyta się go raczej jak szkic dowodu z odniesieniami do innych twierdzeń, które w rozprawie nie są przytaczane ([22, Corollary VI.1.6], [25, Corollary IV.4.5]); wykorzystuje się w nim też pierścień Witta i własności homomorfizmu $WK_\nu \to WK(\nu)$ pierścieni Witta (*second residue homomorphism*), które w rozprawie nie są bliżej omawiane.

W podrozdziale 4.3 przedstawiono algorytm (Algorytmy 10–11) do znajdowania indeksu Witta dowolnej formy q nad ciałem globalnym K, czyli liczby $1/2 \dim(q_h)$, gdzie q_h jest formą hiperboliczną w rozkładzie Witta $q \cong q_a \perp q_h$ na część nieizotropową q_a i część hiperboliczną q_h. Oczywiście dla obliczenia indeksu Witta wystarczy znaleźć wymiar $\dim_a(q) := \dim(q_a)$ części nieizotropowej formy q. Autor zauważa, że Algorytm 10 obliczający wymiar $d_\nu := \dim_a(q_\nu)$ części nieizotropowej formy $q_\nu = q \otimes K_\nu$ nad ciałem lokalnym K_ν ($\nu \in \Omega_K$) pokrywa się z analogicznym algorytmem dla ciał liczbowych, zawartym w pracy P. Koprowskiego i A. Czogały (2018). Algorytm 11 wyznacza $\dim_a(q)$ jako $\max\{d_\nu : \nu \in \mathfrak{B}\}$, gdzie $\mathfrak{B} \subseteq \Omega_K$ składa się z tych waluacji, które mają niezerową wartość na co najmniej jednym współczynniku w diagonalnej postaci formy q.

Proste w opisie są algorytmy z podrozdziału 4.3, za pomocą których Autor testuje, czy dane dwie formy q_1 i q_2 są podobne w sensie Witta (Algorytm 12) lub w sensie Ono (Algorytm 13). Dla przypomnienia, formy q_1 i q_2 są podobne w sensie Witta, jeżeli w ich rozkładach Witta części nieizotropowe są formami równoważnymi, natomiast formy q_1 i q_2 są podobne w sensie Ono, jeżeli $q_1 \cong \alpha q_2$ dla pewnego $\alpha \in \dot{K}$. Algorytm 12 sprowadza się w zasadzie do znanego stwierdzenia, które mówi, że formy q_1 i q_2 są podobne w sensie Witta wtedy i tylko wtedy, gdy spełnione są trzy warunki: (i) różnica ich wymiarów jest parzysta, (ii) mają te same dyskryminanty, (iii) forma $q_1 \perp -q_2$ jest hiperboliczna. Innymi słowy Algorytm 12 sprawdza, czy spełnione są warunki (i)-(iii). Podobnie Algorytm 13 spro-

wadza się do stwierdzenia, że nieosobliwe formy q_1 i q_2 nad każdym ciałem o charakterystyce $\neq 2$ są podobne w sensie Ono wtedy i tylko wtedy gdy mają takie same wymiary, a forma $q_1 \perp -\alpha q_2$ jest hiperboliczna, gdzie $\alpha \in \dot{K}$ jest jakimkolwiek elementem należącym do klasy $\det(q_1)\det(q_2)$ w grupie $\dot{K}/\dot{K}^2$. W szczególności do samej konstrukcji Algorytmów 12–13 nie wykorzystuje się w żaden sposób założenia, że K jest ciałem globalnym.

W całej rozprawie najbardziej skomplikowana technicznie i pojęciowo jest metoda (Algorytmy 14–16) znajdowania nieizotropowej części q_a formy q w jej rozkładzie Witta $q \cong q_a \perp q_h$ (rozdział 5). Jeżeli q nie jest hiperboliczna, to mamy $\dim_a(q) \in \{1,2,3,4\}$. Jeżeli $\dim_a(q) = 1$, to nietrudno sprawdzić, że $q_a = \langle d \rangle$ dla dowolnego $d \in \operatorname{disc}(q)$. W każdym z pozostałych trzech przypadków pokazuje się, jak znaleźć taki element $\alpha \in \dot{K}$, że $\dim_a(q') = \dim_a(q) - 1$, gdzie $q' := (q \perp \langle -\alpha \rangle)_a$. Wówczas $q_a \cong q' \perp \langle \alpha \rangle$. Jeżeli $\dim_a(q) = 4$, to wystarczy wziąć $\alpha = 1$. Najbardziej złożony jest przypadek $\dim_a(q) = 2$ (Algorytm 15), w którym wyznacza się podzbiór $B(q) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\} \subseteq \Omega_K$ tych waluacji ciała K, które przyjmują wartość nieparzystą na co najmniej jednym współczynniku w diagonalnej postaci formy q. W tym celu konstruuje się bazę $\{\beta_1, \ldots, \beta_m\} \subseteq \dot{K}/\dot{K}^2$ grupy $\mathbb{E}_{B(q)}$ tzw. elementów $B(q)$-singularnych i definiuje się elementy $e_i, a_{ij} \in \mathbb{F}_2$ w taki sposób, że $e_i = 0$ (odp. $a_{ij} = 0$) wtedy i tylko wtedy, gdy niezmiennik Hassego $s_{\mathfrak{p}_i}(q)$ formy $q \otimes K_{\mathfrak{p}_i}$ (odp. $\mathfrak{p}_i$-adyczny symbol Hilberta $(\beta_j, \operatorname{disc}(q))_{\mathfrak{p}_i}$) jest równy 1. Następnie rozwiązuje się układ równań liniowych $AX = B$ nad ciałem $\mathbb{F}_2$, gdzie $A = [a_{ij}]$, $B = [e_1, \ldots, e_s]^T$. Jako szukany element $\alpha \in \dot{K}$ można wziąć dowolny element z klasy $\prod_{i=1}^{m} \beta_i^{\varepsilon_i}$, gdzie $X = [\varepsilon_1, \ldots, \varepsilon_m]^T$ jest rozwiązaniem powyższego układu. W szczególności szukana część nieizotropwa jest w tym przypadku równa $q_a = \langle \alpha, -\alpha d \rangle$. Algorytmy 14–15 i dowody ich poprawności mocno przypominają analogiczne rezultaty z pracy P. Koprowski, B. Rothkegel: *The Anisotropic Part of a Quadratic Form Over a Number Field* (2021, arXiv:2109.04172v1). Autor jednak nie cytuje tej pracy, co stanowi oczywiste uchybienie.

W rozdziale 5 przedstawiono też inną koncepcję obliczania części nieizotropowej. Opiera się ona na prostej obserwacji, że $(q \perp q')_a \cong (q_a \perp q'_a)_a$, co pozwala obliczyć część nieizotropową dowolnie „dużej" diagonalnej formy q w sposób rekurencyjny, poprzez sukcesywne rozkładanie jej na coraz mniejsze „kawałki" i wyznaczanie ich wymiarów nieizotropowych, natomiast obliczanie części nieizotropowych wystarczy wykonywać jedynie dla „małych kawałków", tj. form o wymiarach ≤ 4.

W ostatnim rozdziale opracowano algorytmy związane z rozkładem elementów ciała globalnego K na sumę kwadratów. W podrozdziale 6.1 pokazano jak wyznaczyć długość $l(a)$ dowolnego elementu a nad ciałem globalnym K, czyli taką najmniejszą liczbę $n \in \mathbb{N}$, że $a = a_1^2 + \ldots + a_n^2$ dla pewnych $a_i \in K$. Oczywiście, jeżeli $a\dot{K}^2 = b\dot{K}^2$, to $l(a) = l(b)$. Ładne i zgrabne rozumowanie (znowu w oparciu o zasadę Hassego) pokazuje, że $l(a) = \max_{\nu \in \Omega_K} l_\nu(a)$, gdzie $l_\nu(a)$ jest długością elementu a nad ciałem lokalnym K_ν. Algorytm 18 oblicza $l_\nu(a)$ dla dowolnie zadanej waluacji $\nu \in \Omega_K$. W podrozdziale 6.3 obliczono liczbę Pitagorasa $P(K)$ dowolnego ciała globalnego K, czyli taką najmniejszą liczbę $n \in \mathbb{N}$, że każdy element ciała K jest sumą co najwyżej n kwadratów. W podrozdziale 6.4 skonstruowano algorytm (Algorytm 22) do znajdowania elementu Pitagorasa ciała K, czyli elementu $a \in K$, który realizuje liczbę Pitagorasa $P(K)$. Najciekawszy jest przypadek, gdy ciało stałych $\mathbb{F}_q$ spełnia warunek $q \equiv 3 \pmod 4$, bo tylko wtedy istnieje element $a \in K$ z liczbą Pitagorasa 3 (zawsze mamy $l(a) \leq 3$, a w przypadku $q \equiv 1 \pmod 4$ zawsze $l(a) \leq 2$). Algorytm 22 szuka takiego elementu wśród unormowanych wielomianów nierozkładalnych $p \in \mathbb{F}_q[x]$ dzielących wielomian $x^{q^m} - x$ dla pewnego $m \geq 1$. Jeżeli znajdzie taki ideał pierwszy $\mathfrak{p} \lhd O_K$, że waluacja $\nu_{\mathfrak{p}}(p)$ jest nieparzysta, to zwraca wielomian p jako szukany element Pitagorasa.

3 Ocena rozprawy

Ogólna ocena rozprawy jest pozytywna. Autor wykazuje się znajomością teorii form kwadratowych i globalnych ciał funkcyjnych oraz umiejętnie wyprowadza ich własności w oparciu o znane twierdzenia. Potrafi dobierać i łączyć te własności form kwadratowych nad ciałami skończonymi i lokalnymi, które są mu potrzebne do wyprowadzenia odpowiednich własności nad ciałami globalnymi. Przeprowadzone w dowodach rozumowania są poprawne i jeśli zawierają jakieś usterki, to można je łatwo usunąć. Większość dowodów jest przeprowadzonych starannie i szczegółowo. Często opierają się one na głębszych twierdzeniach. Dosyć obszerne i złożone rozumowania zawierają lematy pomocnicze w rozdziale 3 dla skonstruowania efektywnej metody rozkładu ideałów pierścienia O_K na ideały pierwsze. Najbardziej skomplikowana technicznie i pojęciowo jest konstrukcja części nieizotropowej z rozdziału 5. Wyniki zawarte w rozprawie Autor wygłaszał na zagranicznych konferencjach, jak np. *International Symposium on Symbolic and Algebraic Computation (ISSAC '21)*, a także, jako współautor, publikował w takich punktowanych czasopismach z listy JCR jak *Fundamenta Informaticae* i *ACM Communications in Computer Algebra*.

Poniżej zamieszczam kilka uwag krytycznych i szczegółowych, które nie wpływają na końcową, pozytywną ocenę rozprawy.

W rozdziale 2 zabrakło precyzyjnego wytłumaczenia, w jaki sposób znajdować te waluacje w nieskończoności, które nie zerują się na zadanym elemencie pierścienia O_K. W szczególności nie przedstawiono konkretnej formuły na $\nu(a)$ dla każdej takiej waluacji $\nu \in \Omega_K$. Również dla waluacji $\mathfrak{p}$-adycznej nie zapisano w poprawny sposób odpowiedniej formuły, a jedynie ogólnie stwierdzono, że jest ona indukowana rozkładem ideału ułamkowego na ideały pierwsze.

Do prezentowanych w rozprawie przykładów obliczeniowych (w szczególności tych związanych z arytmetyką na ideałach w rozdziale 3) zaimplementowano system Magma, ale samych działań nie wyprowadzono, tak że wykonane obliczenia pozostaje przyjąć na wiarę. Dotyczy to np. równości 1–5 z pierwszego przykładu (str. 26), które należało bardziej objaśnić, a może nawet wyprowadzić „ręcznie".

Algorytm 6, testujący izotropowość formy nad ciałem lokalnym K_ν, potrzebuje do utworzenia form q_1 i q_2 elementu pierwszego $\pi \in O_K$. Należało w tym miejscu wyjaśnić, jak efektywnie konstruować taki element.

W Algorytmie 18, który oblicza długość $l_\nu(a)$ dowolnego elementu $a \in K$ nad ciałem lokalnym K_ν, należy dodatkowo założyć, że zachodzi równoważność: $q \equiv 3 \pmod 4 \Leftrightarrow -1 \notin \dot{K}_\nu^2$, bo w przeciwnym razie, w przypadku, gdy $q \equiv 3 \pmod 4$, $-1 \in \dot{K}_\nu^2$ oraz $\nu(a) \equiv 1 \pmod 2$, algorytm zwraca 3, a powinien zwrócić 2. Dowód poprawności Algorytmu 18 w przypadku parzystej wartości $\nu(a)$ można było przeprowadzić w alternatywny sposób, tj. bez użycia symbolu Hilberta, bo zawsze mamy rozkład $a = u\pi^{\nu(a)}$, gdzie $\nu(u) = 0$ i $\nu(\pi) = 1$, czyli $l_\nu(a) = l_\nu(u)$, a ponieważ forma $\langle 1, 1, -u\rangle$ jest izotropowa (znowu działa tu Twierdzenie 2.2.16 (1)), to wobec Twierdzenia 2.2.8 mamy $u \in D_{K_\nu}(\langle 1, 1\rangle)$, czyli $l_\nu(a) = l_\nu(u) \leq 2$, a więc, jeżeli $a \in \dot{K}_\nu^2$, to $l_\nu(a) = 1$, a jeżeli $a \notin \dot{K}_\nu^2$, to $l_\nu(a) = 2$.

W rozprawie wykorzystuje się różne twierdzenia i notacje zaczerpnięte z książki Tsit-Yuen Lam: *Introduction to quadratic forms over fields*, (AMS). Autor jednak nie zawsze o tym informuje, co trochę utrudnia śledzenie rozumowań. Przykładowo, w dowodzie Algorytmu 18 wykorzystuje się równoważność $-1 \in \dot{K}_\nu^2 \Leftrightarrow -\overline{1} \in \dot{K(\nu)}^2$, o której wcześniej w rozprawie w żaden sposób się nie wspomina i nie można jej bezpośrednio wywnioskować z wcześniej przytoczonych twierdzeń, a wynika ona np. z odpowiedniego lematu powyższej

książki (Lemma VI.1.1). W rozprawie jednak Autor o tym nie wspomina. Poza tym, posługując się specjalistycznymi notacjami należałoby je wcześniej zdefiniować albo przynajmniej ująć w spisie oznaczeń na początku rozprawy, a nie zawsze Autor o tym pamiętał (dotyczy to np. zapisu „$e_i(\mathfrak{p}_i|P)$" w dowodzie poprawności Algorytmu 22).

Dowód punktu (i) Proposition 6.3.1 można było krócej zapisać, tzn. można było napisać, że punkt (i) wynika bezpośrednio z Proposition 6.1.2, Algorytmu 18 i nierówności $\dot{K} \neq \dot{K}^2$.

W Algorytmie 22, jeżeli $q \equiv 3 \pmod 4$, to unormowany i nierozkładalny wielomian $p \in \mathbb{F}_q[x]$ jest zwracany jako element Pitagorasa ciała K (czyli element długości 3), gdy waluacja $\nu_{\mathfrak{p}}(p)$ jest nieparzysta dla jakiegoś ideału pierwszego $\mathfrak{p} \lhd O_K$. Należałoby w tym miejscu wyjaśnić, dlaczego taki ideał $\mathfrak{p}$ zawsze istnieje (dla pewnego unormowanego i nierozkładalnego wielomianu $p \in \mathbb{F}_q[x]$). Poza tym, w dowodzie Algorytmu 22 wnioskuje się, że symbol Hilberta $(-1, p)_{\mathfrak{p}}$ jest równy -1, ale nie jest jasne na czym oparto ten wniosek. Powstaje też pytanie, kiedy algorytm się zatrzymuje, czyli dla jakiego najmniejszego m wielomian p z powyższymi własnościami jest dzielnikiem wielomianu $x^{q^m} - x$? A także, czy wśród takich wielomianów p istnieje element pierwszy, tj. z waluacją $\nu_{\mathfrak{p}}(p) = 1$? Z drugiej strony, jeżeli uda się znaleźć jakikolwiek ideał pierwszy $\mathfrak{p} \lhd O_K$ spełniający warunek $-1 \notin \dot{K}^2_{\nu_{\mathfrak{p}}}$, to wobec Lematu 3.3.1 możemy obliczyć stopień rozszerzenia $m := \deg(\mathfrak{p}) = [O_K/\mathfrak{p} : \mathbb{F}_q]$ i wówczas, wobec Lematu 3.2.1, mamy: $\nu_{\mathfrak{p}}(x^{q^m} - x) = 1$ lub $\nu_{\mathfrak{p}}(y^{q^m} - y) = 1$, czyli co najmniej jeden z elementów $x^{q^m} - x$, $y^{q^m} - y$ jest nie tylko szukanym elementem Pitagorasa, ale też elementem pierwszym $\pi \in O_K$ dla $\nu_{\mathfrak{p}}$. Powstaje zatem pytanie o efektywny sposób znajdowania ideału pierwszego $\mathfrak{p} \lhd O_K$ spełniającego warunek $-1 \notin \dot{K}^2_{\nu_{\mathfrak{p}}}$. Jeszcze drobna uwaga: chyba przez pomyłkę w dowodzie poprawności Algorytmu 22 odwołano się do Algorytmu 5, który dotyczy innego zagadnienia.

4 Podsumowanie i konkluzja

Przedstawione w rozprawie algorytmy w nietrywialny i ciekawy sposób wypełniają wspomnianą na początku lukę w metodach obliczeniowych teorii form kwadratowych. Stanowią naturalne i całościowe opracowanie, będące rozszerzeniem analogicznych wyników, jakie uzyskano całkiem niedawno dla form kwadratowych nad ciałami liczbowymi. Dowody poprawności większości algorytmów przeprowadzono szczegółowo i starannie. Wiele z nich opiera się na znanych twierdzeniach, często znacznie głębszych, jak np. zasada Hassego. Przedstawione rozumowania są poprawne. Mimo opisanych wyżej kilku uwag krytycznych, stwierdzam, że rozprawa doktorska mgra Mawunyo Kofi Darkey-Mensah spełnia wszystkie wymogi ustawy o stopniach naukowych i wnoszę o dopuszczenie go do dalszych etapów przewodu doktorskiego.

Woryna