

**Recenzja rozprawy doktorskiej mgr. Mawunyo Kofi Darkey-Mensah pt.  
*Algorithms for Quadratic Forms over Global Function Fields***

**I. Tematyka i cele badań**

Recenzowana rozprawa doktorska jest pracą z obszaru obliczeniowej algebraicznej teorii liczb, czyli ważnego działu matematyki o ugruntowanej pozycji i licznych powiązaniach i zastosowaniach w obrębie algebry jak i całej matematyki. Autor bada formy kwadratowe nad globalnymi ciałami funkcyjnymi charakterystyki różnej od 2. Przypomnijmy, że globalne ciało funkcyjne  $K$  jest skończonym rozszerzeniem ciała  $\mathbb{F}_q(x)$  funkcji wymiernych nad ciałem skończonym  $\mathbb{F}_q$ , lub równoważnie,  $K$  jest ciałem ułamków pierścienia  $\mathbb{F}_q[x, y]/\langle F \rangle$  dla wielomianu (krzywej algebraicznej)  $F \in \mathbb{F}_q[x, y]$ . Zasadniczym celem rozprawy jest konstrukcja zestawu metod algorytmicznych służących do testowania własności lub wyliczania niezmienników form kwadratowych nad  $K$ , m.in. weryfikacja izotropowości, hiperboliczności i podobieństwa form oraz wyznaczanie indeksu Witt'a i części anizotropowej formy. Poszukiwanie metod obliczeniowych dotyczących form kwadratowych nad ciałem ma długą tradycję. Tym niemniej, główny nurt badań koncentrował się w tej mierze głównie na formach nad ciałem liczb wymiernych  $\mathbb{Q}$  czy szerzej, nad inną klasą ciał globalnych, tj., algebraicznych ciał liczbowych. W przypadku ciał liczbowych szereg nowych wyników uzyskał w ostatnim czasie promotor rozprawy, dr hab. Przemysław Koprowski. Autor w rozprawie zajmuje się uogólnieniem niektórych z tych metod na formy nad globalnymi ciałami funkcyjnymi. Jest to zatem ambitny plan wypełnienia pewnej luki, gdyż wygląda na to, że dla form nad tą klasą ciał uzyskano dotąd stosunkowo niewiele wyczerpujących, efektywnych metod obliczeniowych.

Rozprawa podejmuje także dwa inne istotne wątki, blisko związane z formami kwadratowymi, które są ważne i interesujące same w sobie. Pierwszym z tych wątków jest zagadnienie algorytmicznej faktoryzacji ideałów całkowitych i ułamkowych na czynniki pierwsze w globalnych ciałach funkcyjnych. Faktoryzacja ta wykorzystywana jest między innymi do wyznaczania ideałów pierwszych, które „dzielą współczynniki” rozważanych form kwadratowych, czyli zadają nietrywialną walucję tychże współczynników.

Drugi ze wspomnianych wątków porusza zagadnienia związane z przedstawianiem elementu ciała w postaci sumy kwadratów, czyli problemem inspirującym matematyków od stuleci (zob. prace Lagrange'a, Gaussa, Hilberta i in.). W rozprawie rozważa się wykorzystanie metod związanych z formami kwadratowymi nad globalnym ciałem funkcyjnym  $K$  oraz faktoryzacją ideałów ułamkowych w  $K$  do następujących problemów: wyznaczanie *długości* elementu  $a \in K$  (czyli długości najkrótszej prezentacji  $a$  w postaci sumy kwadratów), *poziomu* ciała (czyli długości elementu  $-1$ ), *liczby Pitagorasa* (czyli najmniejszej liczby  $P$  takiej, że każda suma kwadratów w  $K$  jest sumą  $P$  kwadratów) oraz *elementu Pitagorasa* (czyli elementu  $a \in K$  długości  $P$ ).

Wszystkie wyżej naszkicowane problemy są bardzo naturalne a jednocześnie trudne. Cel badawczy jest zatem ambitny, uzyskane rozwiązania mogą stanowić zauważalny wkład w rozwój algebraicznej teorii liczb, zwłaszcza algebraicznej teorii form kwadratowych i badań globalnych ciał funkcyjnych.

**II. Struktura i wyniki rozprawy**

Praca składa się z sześciu rozdziałów. We wstępnym rozdziale Autor wprowadza czytelnika w tematykę rozprawy, przedstawia szerszy kontekst matematyczny i szkic historyczny dla rozważanych problemów oraz streszcza jej główne wyniki. Rozdział 2 ma charakter preliminariów, czyli zawiera ustalenie oznaczeń i związane przypomnienie niezbędnych pojęć i faktów m.in. z teorii ciał i ich walucji oraz form kwadratowych.

Prezentacja głównych rezultatów rozpoczyna się w Rozdziale 3. Rozdział ten zawiera wyniki opublikowane w artykule oznaczonym (4) (Darkey-Mensah, Koprowski, *Fund. Inform.* 170 (2019), 325–338). Autor prezentuje trzy algorytmy (Algorytmy 1-3), które stanowią trzy kolejne etapy ogólnego algorytmu (Algorytm 4)

znajdowania rozkładu ideału  $\mathfrak{a}$  w pierścieniu funkcji wielomianowych  $\mathcal{O}_K \cong \mathbb{F}_q[X, Y]/\langle F \rangle$  globalnego ciała funkcyjnego  $K$ . Etapy te to kolejno: znajdowanie czynników radykalnych, rozkład ideału radykalnego na czynniki różnych stopni oraz faktoryzacja ideału, którego wszystkie czynniki mają ten sam stopień. Można spojrzeć na te wyniki jako na pomysłowe i niebanalne uogólnienia znanych algorytmów bezkwadratowej faktoryzacji wielomianów (D. Musser), szukania największego wspólnego dzielnika (ideałów) i algorytmu Cantora–Zassenhaua. Doceniam przygotowanie szeregu oryginalnych przykładów ilustrujących działanie poszczególnych algorytmów. Warto podkreślić, że Algorytm 1 w pracy (4) jest zaprezentowany w nieco ogólniejszej formie niż w rozprawie, mianowicie, jest on w (4) zdefiniowany dla ideałów w dowolnej dziedzinie Dedekinda z obliczalną arytmetyką ideałów. Rozumiem, że w rozprawie Autor chciał uwspólnić kontekst z resztą wyników.

Według narracji Autora, przedstawiona metoda różni się od większości dotychczas znanych algorytmów faktoryzacji ideałów w  $K$  pewnymi niuansami obliczeniowymi, m.in. nie wymaga wcześniejszego wyznaczenia ordynku maksymalnego. Autor nie rozwija jednak zbytnio tego wątku, tzn. nie dyskutuje różnic między swoją metodą a znanymi algorytmami. Wyniki Rozdziału 3 mają w pewnym sensie charakter pomocniczy dla rezultatów prezentowanych w kolejnych rozdziałach, gdyż jak wspomniałem wyżej, umiejętność faktoryzacji ideałów ułamkowych w  $K$  jest kluczowa dla znajdowania odpowiednich waluacji dla współczynników form kwadratowych nad  $K$ . Zauważmy jednak, że wszystkie algorytmy w Rozdziale 3 dotyczą ideałów całkowitych (tj., ideałów w  $\mathcal{O}_K$ ). O sposobie rozszerzenia algorytmów na ideały ułamkowe w  $K$  mówi jedynie lakoniczna Uwaga 3.3.5 (patrz też załącznik „Usterki” 5.20.).

W Rozdziałach 4 i 5 zaprezentowane są algorytmy dotyczące (niezdegenerowanych) form kwadratowych nad globalnymi ciałami funkcyjnymi  $K$  charakterystyki różnej od 2. W Rozdziale 4 Autor przedstawia szereg algorytmów służących do testowania podstawowych własności form kwadratowych oraz wyznaczania ich ważnych niezmienników. Algorytmy 5-7 (odp. Algorytmy 8-9) dostarczają metodę testowania izotropowości (odp. hiperboliczności) formy. Algorytmy 10 i 11 służą do wyznaczania wymiaru anizotropowego formy i tym samym, indeksu Witt’a. Algorytmy te są oryginalnymi uogólnieniami analogicznych algorytmów opracowanych dla form nad ciałami liczbowymi w pracy [21] (Koprowski, Czogała, *J. Symb. Comput.* 89 (2018), 129-145). I podobnie jak w [21], algorytmy oparte są na Zasadzie Lokalno-Globalnej Hasse-Minkowskiego, tzn., rozwiązuje się problem lokalnie (nad ciałami lokalnymi  $K_p$ ) aby otrzymać rozwiązanie globalne (nad  $K$ ). W tym podejściu istotna jest umiejętność ograniczenia się do skończonej liczby rozwiązań lokalnych. Pomocne w tym są metody faktoryzacji ideałów wypracowane w poprzednim rozdziale. Algorytmy 5-11 oraz towarzyszące im fakty oraz nowe, nietrywialne przykłady stanowią dość istotnie rozwiniętą i uporządkowaną wersję wyników opublikowanych w artykule (1) (Darkey-Mensah, *ACM Commun. Comput. Algebra* 55 (2021), 68–72). Ostatnie dwa algorytmy (nr 12 i 13) w Rozdziale 4 służą do testowania podobieństwa form w sensie Witt’a i Ono, odpowiednio. Są one stosunkowo prostymi (ale nie zupełnie trywialnymi) konsekwencjami definicji. Wraz z przedstawionymi przykładami zastosowania stanowią wartościowe uzupełnienie zestawu metod algorytmicznych dla rozważanych form kwadratowych. Algorytmy te zdaje się nie były publikowane.

W Rozdziale 5 przedstawiona jest metoda wyznaczania części anizotropowej formy kwadratowej nad globalnym ciałem funkcyjnym. Zauważmy, że jest to problem znacznie trudniejszy niż wyznaczanie samego wymiaru anizotropowego rozważane w poprzednim rozdziale. Zdaje się, że w ogólności (nad dowolnym ciałem) jest to problem nieobliczalny. Przypomnijmy, że z ogólnej teorii form nad ciałami lokalnymi wynika, że (niezdegenerowana) forma nad globalnym ciałem funkcyjnym wymiaru co najmniej 5 jest izotropowa. Zatem część anizotropowa  $q_a$  formy  $q$  ma wymiar zawsze ograniczony przez 4. W rozprawie rozważane są oddzielnie przypadki poszczególnych wymiarów anizotropowych 1, 2, 3, i 4. Przypadki wymiarów 3 i 4 są poprzez sprytne redukcje (zob. Obserwacja 5.1.1, Stwierdzenie 5.2.1 i Algorytm 14) sprowadzone do problemu wyznaczania części anizotropowej wymiaru 2, dla której problem jest rozwiązywany bezpośrednio (Algorytm 15). Ten ostatni, najbardziej zaawansowany koncepcyjnie i obliczeniowo algorytm polega m.in. na rozwiązywaniu układu równań liniowych nad  $\mathbb{F}_2$  o współczynnikach wyznaczonych przez odpowiednie niezmienniki Hassego i  $p$ -adyczne symbole Hilberta na bazie grupy elementów  $\mathfrak{P}(q)$ -singularnych. Całość rozwiązania, czyli wyznaczenie części anizotropowej dowolnego wymiaru  $\leq 4$  jest przedstawiona w dwóch różnych algorytmach: Algorytm 16 (sekwencyjny) oraz Algorytm 17 (rekurencyjny, metodą „dziel i zwyciężaj”). Algorytmy realizują wyżej wspomnianą redukcję wraz z pewnymi subtelnymi optymalizacjami. Autor przedstawia też

nietrywialne przykłady działania algorytmów. Przygotowanie tych przykładów niewątpliwie wymagało dużego wysiłku i biegłości w posługiwaniu się narzędziami informatycznymi. Wyniki tego rozdziału, czyli wymienione algorytmy oraz niebanalne wyniki teoretyczne na których są oparte (m.in. wspomniane Stwierdzenie 5.2.1 o redukcji wymiaru oraz Twierdzenie 5.3.2 o pewnych własnościach punktów ciała związanych z formą  $q$  o  $\dim_a(q) = 2$ ) uważam za najważniejsze i najciekawsze rezultaty rozprawy. Wyniki te zostały opublikowane w artykule oznaczonym (3) (Darkey-Mensah, Koprowski, Rothkegel, *ISSAC '21*, 115–122 (2021)).

W ostatnim, szóstym rozdziale Autor przedstawia metody algorytmiczne do wyznaczania kilku ważnych niezmienników ciał, dostosowane do przypadku globalnych ciał funkcyjnych. Są to wspomniane w sekcji pierwszej recenzji niezmienniki związane z prezentacją elementu ciała w postaci sumy kwadratów. Zaproponowane metody ich wyznaczania stanowią bardzo ciekawe i niebanalne zastosowanie wyników z poprzednich rozdziałów, zarówno algorytmicznych jak i teoretycznych (m.in. redukcja problemu do weryfikacji izotropowości pewnej formy kwadratowej nad danym ciałem globalnym). Algorytmy 18 i 19 dostarczają metody wyznaczania długości danego elementu jako sumy kwadratów dla ciała lokalnego i globalnego, odpowiednio. W tym wypadku, podobnie jak w Rozdziale 4, zaproponowana metoda wykorzystuje odpowiedni wariant Zasady Lokalno-Globalnej. Kolejne trzy algorytmy (o numerach 20, 21 i 22) służą do wyznaczania poziomu ciała, liczby Pitagorasa i elementu Pitagorasa w danym ciele. Ten ostatni stanowi kolejne nietrywialne zastosowanie metod faktoryzacji ideałów z Rozdziału 3. Algorytmom towarzyszą niezbędne fakty teoretyczne, dowody poprawności oraz przykłady wykorzystania dla konkretnych globalnych ciał funkcyjnych. Wyniki tego rozdziału zostały opublikowane w artykule oznaczonym (2) (Darkey-Mensah, Rothkegel, *Fund. Inform.* 184 (2021), 297-306) oraz we wcześniej wspomnianym artykule (1). Warto odnotować, że artykuł (2) zawiera też inne wartościowe rezultaty, które nie zostały ujęte w rozprawie, m.in. Algorytm 3 służący do wyznaczania długości elementu dla ciał liczbowych, który nie jest prostym analogiem Algorytmu 19 z rozprawy, lecz stosuje nieco inne metody.

### III. Prezentacja wyników (strona formalna i redakcyjna rozprawy)

Zaczynając od pozytywnych aspektów prezentacji należy podkreślić, że struktura rozprawy, kolejność i zakres zagadnień są bardzo dobrze przemyślane. Jak sygnalizowałem wyżej, Autor spośród uzyskanych w trakcie studiów doktoranckich wyników wybrał (albo odpowiednio przeformułował) tylko te, które dotyczą globalnych ciał funkcyjnych i które są ze sobą ściśle powiązane. Dzięki temu rozprawa sprawia wrażenie spójnej, możliwie kompletnej opowieści, nie zawierającej przypadkowych treści. Zauważalny jest też wysiłek włożony w rozwinięcie i uzupełnienie wyników opublikowanych w artykułach: niektóre algorytmy zostały podzielone na części, Autor dodał w rozprawie kilka nowych faktów, a przede wszystkim zaprezentował liczne nowe, ciekawe i wartościowe przykłady. Ponadto, rozprawa jest przygotowana poprawnie pod względem technicznym. Przedstawione przykłady, tabele, formuły matematyczne są czytelne. Algorytmy występujące w pracy również są poprawnie zaprezentowane, opatrzone niezbędną specyfikacją wejścia/wyjścia oraz wyraźnie oznaczonym uzasadnieniem poprawności. Tytuły sekcji i podsekcji, ich kolejność, czcionki, oznaczenia, numeracja, odnośniki do faktów, sekcji i literatury są poprawne, z dokładnością do kilku drobnych usterek. Pomocne w lekturze są estetycznie przygotowane: spis treści, spis algorytmów i indeks symboli. Rozprawę kończy spis literatury liczący 37 pozycji, które są odpowiednio dobrane i wykorzystane.

Niestety w czasie dokładniejszej lektury praca bardzo mocno traci. Znalazłem w rozprawie liczne usterki niemal każdego możliwego rodzaju: błędy językowe, błędy w oznaczeniach, formułach matematycznych, algorytmach, brak dbałości o założenia, błędne/niekompletne argumenty w dowodach oraz wiele niejasności, niezdefiniowanych lub niekonsekwentnie stosowanych oznaczeń, korzystanie z nietrywialnych faktów bez ich przypomnienia ani odpowiedniego cytowania itp. Obszerną listę przykładowych usterek i błędów załączam do recenzji. Część błędów (m.in. usterki w algorytmach!) jest powielona z opublikowanych artykułów. Szkoda, że Autor nie wykorzystał okazji by w doktoracie skorygować te usterki, redakcję niektórych części ograniczył jedynie do skopiowania fragmentów artykułów. Zrozumienie dowodów i ocena poprawności wyników wymaga od czytelnika bardzo dużego wysiłku z powodu licznych niejasności, dużych przeskoków myślowych i konieczności samodzielnej korekty błędów. Szczególnie razi pominięcie lub bardzo zdawkowe potraktowanie dowodów własności stopu, która w przypadku niektórych algorytmów jest wysoce nietrywialna (zob. punkt [6](#))

listy usterek). Liczne niejasności i brak staranności dziwi i rozczarowuje biorąc pod uwagę, że pracę matematyczną (a zwłaszcza pracę z matematyki obliczeniowej!) powinna cechować precyzja.

Mimo powyższej krytyki pragnę podkreślić, iż zdecydowana większość głównych wyników wydaje się być poprawna, mimo użytych błędnych lub niekompletnych argumentów. Wydaje się, że większość tych błędów da się stosunkowo łatwo poprawić (w załączonej liście w niektórych przypadkach podaje wskazówki).

#### IV. Ocena

Jak starałem się wykazać w pierwszych dwóch sekcjach recenzji, Autor w rozprawie zaprezentował niebanalne i oryginalne rozwiązania naturalnych, ważnych i trudnych problemów algebraicznej teorii liczb. Rozprawa zawiera bardzo solidny zestaw narzędzi algorytmicznych wspartych niezbędnymi wynikami teoretycznymi, które (być może po dokonaniu niezbędnych korekt) mogą zostać wykorzystane w dalszych badaniach w teorii form kwadratowych i globalnych ciał funkcyjnych. Rezultaty te mogą zostać zauważone i docenione przez badaczy na świecie. Wyniki zaprezentowane w rozprawie zostały opublikowane w czterech artykułach w międzynarodowych czasopismach matematyczno-informatycznych. Jeden artykuł jest monoautorski, pozostałe powstały przy współautorstwie promotora i/lub promotora pomocniczej dr Beaty Rothkegel. Na podkreślenie zasługuje fakt, iż jeden z artykułów został opublikowany w wydawnictwie prestiżowej konferencji *Proceedings of the 2021 on International Symposium on Symbolic and Algebraic Computation (ISSAC '21)*.

Wyniki recenzowanej rozprawy dowodzą ogólnego opanowania przez mgr. Darkey-Mensah metodologii pracy badawczej i umiejętności samodzielnego prowadzenia pracy naukowej. Dość duże zróżnicowanie użytych technik (metody teorii ciał i pierścieni, geometrii algebraicznej, algebry liniowej, metody algorytmiczne) i stopień skomplikowania dowodów świadczą o sporej ogólnej wiedzy matematycznej, dobrym zrozumieniu problematyki i pomysłowości Autora. Nietrywialne przykłady wyliczone przy użyciu oryginalnych implementacji algorytmów dowodzą biegłości w posługiwaniu się narzędziami informatycznymi i dobrego zrozumienia algorytmicznych aspektów teorii. Niestety liczne błędy i usterki prezentacji rozczarowują i mocno obniżają ocenę całości, ale w mojej opinii nie dyskwalifikują wartości naukowej przedstawionych rezultatów.

Reasumując, uważam, że rozprawa mgr. Darkey-Mensah nie do końca spełnia zwyczajowe wymagania stawiane rozprawom doktorskim z matematyki (odnośnie staranności i precyzji prezentacji). Tym niemniej, rozprawa **spełnia wymagania ustawowe**, m.in., stanowi oryginalne rozwiązanie problemu naukowego w rozumieniu Art. 187 Ustawy z dnia 20 lipca 2018 r. „Prawo o szkolnictwie wyższym i nauce”. W mojej ocenie rozprawa może być zatem podstawą do nadania jej Autorowi stopnia doktora nauk ścisłych i przyrodniczych w dyscyplinie matematyka. W związku z tym przedkładam wniosek o **przyjęcie rozprawy** i dopuszczenie mgr. Mawunyo Kofi Darkey-Mensah do dalszych etapów postępowania w sprawie nadania stopnia doktora.



Andrzej Mróz

Toruń, 13 września 2022

Do recenzji dołączony jest spis przykładowych usterek i błędów znalezionych w rozprawie.



**Załącznik do recenzji rozprawy doktorskiej mgr. Mawunyo Kofi Darkey-Mensah**

**Usterki w rozprawie**

Poniżej wymieniam przykładowe usterki znalezione w tekście rozprawy. Podkreślenia w cytowanych fragmentach pochodzą ode mnie.

1. Błędy językowe (głównie gramatyczne) i literówki – przykłady: s. iii, l. 14: „argumenty” → „algorytmy”; s. 2, l. -1: „Newer algorithms described in [14] avoids”; s. 3, l. 8: „Mainly, Section 2.1 present”; s. 3, l. 10: „We cover [...], and presented [...]” (niekonsekwentne użycie czasów, patrz też „present” vs „presented” w ll. 26-27); s. 3, l. -10: „Algorithms 12 and 13 checks”; s. 8, l. -8: „which seat above” (powinno być „sit” lub „are seated”); s. 8, l. -5: „Each of the prime ideals [...] determine” (l. pojedyncza, nie mnoga), podobnie s. 9, ll. 5-6: „every valuation [...] extend”; s. 10, l. 8: „it’s residue class field is finite”; s. 13, ll. 5-6: „two different basis”; s. 15, l. 18: „non-degenrate”; s. 21, l. 18 i s. 37, l. -9: „field of fraction of the function field” (powinno być chyba „field of fractions of the ring of polynomial functions”); s. 22, l. -8: „Let  $\alpha$  is”; s. 29, l. 8: „Example 3.1” → „Example 3.1.4”; s. 22, l. 3: „the symbol [...] not only represent”; s. 8, l. 16: „ring of polynomial functions”; s. 11, l. 8: „of the diagonalization of  $M_q$ ”, → „of the diagonal of  $M_q$ ”; s. 36, l. 2: „Theorem”; s. 38, l. 7: „local forms [...] maps”; s. 42, l. 5: „later” → „latter”.
2. Błędy w oznaczeniach i formułach matematycznych:
  - 2.1. s. 6, l. 10: „Since  $\mathbb{F}_q$  is a cyclic group” – powinno być  $\dot{\mathbb{F}}_q$  (z kropką);
  - 2.2. s. 7, l. 1: waluacja  $\nu$  ma dziedzinę  $\dot{K} = K \setminus \{0\}$ , ale w l. 3 rozważa się jej wartość na 0; dalej, nie jest jasne jaka jest w l. 6 wartość bezwzględna  $|0|_\nu$ , dokładniej, co oznacza  $\varepsilon^\infty$ ?
  - 2.3. s. 7, l. 20: ozn. „ $K(\mathfrak{m})$ ” – powinno być chyba „ $K(\nu)$ ”;
  - 2.4. s. 8, l. 6: „ $c$  is in  $\dot{K}$ ” – powinno być „ $c$  is in  $\dot{\mathbb{F}}_q$ ”?
  - 2.5. s. 8, l. 9: czym jest  $\mathbb{F}_q[x]$ ? Wielomiany o wszystkich współczynnikach niezerowych? Chyba chodziło o  $\mathbb{F}_q[x]$  (bez kropki);
  - 2.6. s. 12, l. 19: zapis  $XM_1X^t$  vs zapis  $X^t \cdot M_q \cdot X$  na s. 11, l. 3 (wektory wierszowe vs kolumnowe);
  - 2.7. s. 21, l. 10: „fractional ideals of  $\mathcal{O}_K$ ” – powinno być „of  $K$ ”;
  - 2.8. s. 30, l. -3: jest  $(\pi \circ \phi)(b^\varepsilon) = 0$ , powinno być  $(\pi_i \circ \phi)(\bar{b}^\varepsilon) = 0$ ;
  - 2.9. s. 31, l. -5: sprawdzany jest warunek  $\bar{b}^{11} \neq 1$  mimo, że stopień  $\mathfrak{h}_{21}$  jest 2, zatem powinno się chyba testować  $\bar{b}^{120}$  ( $120 = 11^2 - 1$ ). Jeżeli mam rację, to resztę rachunków w Przykładzie 3.3.3 też trzeba zweryfikować. M.in. na s. 32, ll. 12: moc  $\mathcal{O}_K/\mathfrak{b}$  i  $\mathcal{O}_K/\mathfrak{c}$  powinna być 121, nie 11;
  - 2.10. s. 33, l. 6: jest „to factor  $I$ ”, powinno być „to factor  $\mathfrak{a}$ ”;
  - 2.11. s. 33, l. 17: niespodziewanie „\*” jako oznaczenie mnożenia;
  - 2.12. s. 33, l. 25: jest  $\mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_3^2 \cdot \mathfrak{p}_4^3$ , powinno być  $\mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_3^2 \cdot \mathfrak{p}_4^4$ ;
  - 2.13. s. 38, l. 4:  $q_0$  i  $q_1$  są zdefiniowane tak samo, jako  $q \otimes K_{\mathfrak{p}}$  – pomyłka lub niezrozumiała konwencja;
  - 2.14. s. 43, l. -1: jest „ $q_1 = q'_1 \perp m \cdot H$  and  $q_2 = q'_2 \perp n \cdot H$ ”, powinno być „ $q'_1 = q_1 \perp m \cdot H$  and  $q'_2 = q_2 \perp n \cdot H$ ”;
  - 2.15. s. 45, l. 4: jest mod  $\dot{K}/\dot{K}^2$ , powinno być mod  $\dot{K}^2$ ; także niepoprawnie wyciągnięty skalar przed wyznacznik;
  - 2.16. ss. 53-54, Przykład 5.4.2: punktów w przywoływanym Przykładzie 4.1.1 było 10, zatem  $s = 10$  i macierz  $A$  powinna mieć rozmiar  $10 \times 13$ , nie  $13 \times 13$  (por. Algorytm 15).
3. Błędy w algorytmach:
  - 3.1. Algorytm 1, wiersz 10:  $\mathfrak{g}_i$  nie jest zdefiniowany (zob. instrukcje w wierszach 8-9), zatem powinno się zwrócić  $\mathfrak{g}_1, \dots, \mathfrak{g}_{i-1}$  zamiast  $\mathfrak{g}_1, \dots, \mathfrak{g}_i$ , a także zadbać o przypadek skrajny  $i = 1$ ;
  - 3.2. Algorytm 2, wiersz 8: podobnie j.w., powinno być **return**  $\mathfrak{h}_1, \dots, \mathfrak{h}_{k-1}$ ;

- 3.3. Algorytm 3, wiersze 9-10: formalnie procedura ma jeszcze drugi argument, stopień; należałoby zatem dołączyć tutaj do wywołania drugi parametr  $d$ . Podobnie w Algorytmie 4, wiersz 8;
  - 3.4. Algorytm 7, w. 8: czy faktycznie lista  $\mathfrak{P}$  ma mieć  $n = \dim(q)$  elementów? Por. też Alg. 9;
  - 3.5. Algorytm 13, w. 3-4:  $\det(q) \in \dot{K}/\dot{K}^2$  więc zapis „ $(-\alpha) \cdot q_2$ ” jest niejednoznaczny;
  - 3.6. Algorytm 14: czym jest  $p$  w wierszu 2? Czy jest to odpowiednio (jak?) wybrany element  $\mathfrak{P}$ , czy raczej należy rozważyć wszystkie? Bez tego wyjaśnienia algorytm jest niezrozumiały, podobnie jak stojące za jego poprawnością Stw. 5.2.1;
  - 3.7. Algorytm 15: w wierszu 13 dodaje się nowy  $p$  do  $\mathfrak{P}(q)$  a za chwilę w kolejnej iteracji oblicza się na nowo  $\mathfrak{P}(q)$  w w. 3; wydaje się, że pierwsza część w. 3 powinna być przesunięta przed pętlę;
  - 3.8. Algorytm 16: Algorytm zawsze zwraca formę wymiaru  $\leq 2$ . Wydaje się, że poprawna klauzula w wierszu 8 powinna brzmieć „**return**  $q_a \perp \text{AnisotropicDim2}(q, K)$ ”;
  - 3.9. Algorytm 17: „Input: An anisotropic quadratic form  $q$  [...]” „Output: The anisotropic part  $q_a$  of  $q$ ”.
4. Brak dbałości o założenia:
- 4.1. We wstępie (s. 1) Autor informuje, że w pracy rozważa ciała charakterystyki różnej od 2. Tym niemniej, na początku Rozdziału 2 (s. 5, l. -14:), gdy ustalana jest liczba pierwsza  $p$  i ciało  $\mathbb{F}_q$  dla  $q = p^r$ , nie ma mowy o tym, by  $p$  była różna od 2. Czytelnik domyślnie przyjmuje zatem, że początkowe fragmenty preliminariów są pisane dla dowolnej charakterystyki. Jednak już na s. 6 okazuje się (jeśli uważnie się wczytamy w tekst), że jednak  $p \neq 2$ , np. s. 6, l. 10: „Since  $\mathbb{F}_q$  is a cyclic group of even order  $q-1$ ” czy parzyste przypadki wykluczone w Lemacie 2.1.2 i Twierdzeniu 2.1.3;
  - 4.2. s. 7, ll. 12-18: Rozważana jest dowolna waluacja  $\nu$  (bez założenia o tym że jest znormalizowana czy dyskretna!), ale w l. 17 jest mowa o uniformizatorze  $\pi$ , zaś definicja ideału  $m_\nu$  korzysta z dyskretności ( $\nu(a) \geq 1$  zamiast  $\nu(a) > 0$ ). Podobnie na s. 8 (Remark 2.1.5) – wymienione są tylko waluacje dyskretne, bez jawnego wskazania, że tylko dyskretne są rozważane/istotne. Podobnie na s. 10, l. 1: czy nie powinno się założyć, że waluacja  $\nu$  jest dyskretna jak sugeruje nazwa „complete discretely valuated field”?
  - 4.3. s. 10, l. -10: w pierwszym akapicie podrozdziału 2.2 jest globalne założenie: „the field  $K$  will be a global function field of characteristic  $\neq 2$ ”. Dalej jest niestety brak konsekwencji: w Stw. 2.2.1 litera  $K$  oznacza już dowolne ciało char  $\neq 2$ , czyli zmienna  $K$  została „uwolniona”. Nie jest to niczym zdrożnym, jednakże za chwilę w Tw. 2.2.3, 2.2.7, 2.2.8, 2.2.12, 2.2.14 nie ma w ogóle założenia o ciele (choć w większości z nich też char  $\neq 2$  jest ważna), zaś we Wniosku 2.2.9 mamy sformułowanie „over a given field  $K$ ” sugerujące, że nadal zmienna  $K$  jest „uwolniona” i dodatkowo charakterystyka nie jest istotna (a jest, bo niżej jest komentarz że ten wniosek wynika z Tw. 2.2.8);
  - 4.4. s. 14: w Def. 2.2.7 zakłada się, że forma  $q$  jest niezdegenerowana (właściwie nie wiadomo dlaczego, nie jest to potrzebne), ale chwilę później w Tw. 2.2.6 brak już tego założenia;
  - 4.5. s. 15, l. -8: stwierdzenie „an isotropic quadratic form is universal” nie jest prawdziwe (weźmy np. formę zerową) – trzeba jeszcze założyć niezdegenerowanie;
  - 4.6. s. 20, l. -15 (Tw. 2.2.26): symbol Hilberta jest definiowany w pracy dla ciał lokalnych (Def. 2.2.12), a tu w twierdzeniu wykorzystywany dla dowolnego ciała (?);
  - 4.7. s. 22, ll. 10-14: w tym samym akapicie najpierw jest mowa o wielomianach nad dowolnym ciałem  $K$  (zob. zapis  $c \in \dot{K}$ ) oraz o pierścieniu  $\mathcal{O}_K$  (w domyśle tu  $K$  oznacza globalne ciało funkcyjne char  $\neq 2$ ). Oczywiście nie jest szczególnym nadużyciem używanie tej samej litery do oznaczenia dwóch różnych obiektów, ale należy zmianę wyraźnie zasygnalizować. Podobna sytuacja występuje w akapicie s. 23, ll. 9-11;
  - 4.8. s. 47, l. 8: część anizotropowa  $q_a$  formy  $q$  zdefiniowana jest w pracy tylko dla form niezdegenerowanych  $q$  (patrz też Tw. 2.2.12); natomiast w Algorytmach 14, 15, 16, 17 to założenie jest pominięte;

4.9. Rozdział 5: niemal każdy algorytm w tym rozdziale ma inne założenia odnośnie ciała chociaż wszystkie są oparte o te same pojęcia i fakty.

5. Niejasności i brak precyzji:

- 5.1. s. 6, l. -2: : „The absolute value defined on a global function field  $K$  is ultrametric in the sense that,” – nie jest jasne czy to jest definicja (wtedy lepiej byłoby napisać „is called ultrametric if”) czy stwierdzenie („every absolute value defined on a global function field  $K$  is ultrametric in the sense that,”); użycie rodzajnika określonego na początku zdania dodatkowo utrudnia zrozumienie;
- 5.2. s. 7, l. -5: „All the places of a global function field come from places of the underlying rational function field” – bardzo niejasne zdanie. Ani tu ani chyba nigdzie dalej nie jest wyjaśnione w jaki konkretnie sposób punkty w ciele  $K$  „come from” punktów w ciele  $k = \mathbb{F}_q(x)$ , a zwłaszcza brakuje dokładnego stwierdzenia, czy/kiedy/dlaczego punkt w  $k$  indukuje dokładnie jeden punkt w  $K$ . Wiedza o tym jest niejawnie wykorzystywana dalej wielokrotnie;
- 5.3. s. 8, ll. 7,10: „is a  $p$ -adic valuation”, „is an infinite valuation” – podobnie jak w 5.1. – to są definicje czy stwierdzenia? Chyba jednak definicje, w takim wypadku lepiej pisać „is called” zamiast „is”;
- 5.4. s. 8, l. -10,-9,-8: : cytowane [1, Corollary 9.4] dotyczy jedynie ideałów w dziedzinach Dedekinda, natomiast w formule (2.1) mamy rozkład ideału ułamkowego w  $K$ . Przydałoby się tu przytoczyć bardziej precyzyjne cytowanie lub 1-2 zdania uzasadnienia jak istnienie i jednoznaczność takiego rozkładu wynika z [1, Corollary 9.4]. Zwłaszcza, że stosowane są bardzo niejasne konwencje: podwójne (?) indeksowanie  $\mathfrak{p}|p$  w (2.1), i sformułowania: „seat above underlying (ideals generated by) monic irreducible polynomials  $p$ ”;
- 5.5. s. 8, l. -1: : „Thus every prime ideal in  $\mathcal{O}_K$  corresponds to a place of  $K$ ” – kolejna kluczowa dla rozprawy obserwacja podana jest w sposób dalece nieprecyzyjny/niekompletny: czy ta odpowiedniość jest różnowartościowa? Jeśli tak to dlaczego? Zauważmy, że dalej Autor utożsamia ideały pierwsze  $\mathfrak{p}$  z punktami w  $K$  pisząc np.  $\mathfrak{p} \in \Omega_K$  (jak można zgadywać, jest to skrót zapisu  $[\nu_{\mathfrak{p}}] \in \Omega_K$ ), zatem korzysta istotnie z różnowartościowości tej odpowiedniości. Podobnie jest na s. 9, ll. 6,8:  $S$  jest „set of extensions of the "infinite valuation"” (a nie „set of places of extensions of the "infinite valuation"”) więc zapis w formule niżej  $\mathfrak{p} \in \Omega_K \setminus S$  (formalnie niepoprawny) ma jako taki sens tylko gdy różne rozszerzenia nieskończonej waluacji dają różne punkty w  $K$ ;
- 5.6. s. 11, l. 16: czym jest  $V$ ? Dziedziną formy  $q$  jest przestrzeń  $K^n$  (formuła (2.4)), nigdzie wcześniej nie ma mowy o dowolnej przestrzeni  $V$ . Skutkiem tej niefrasobliwości w konwencji jest niejasność związku  $q$  z  $B$  w l. -6 oraz niezrozumiałe definicje „quadratic space” w l. -5, Def. 2.2.2 i 2.2.4;
- 5.7. s. 13, ll. 17-18: „The isometry class of the 2-dimensional quadratic form [...] called the *hyperbolic plane*, denoted as  $H$ ” –  $H$  jest zdefiniowana jako klasa izometrii więc sformułowanie „isometric to the hyperbolic plane” w l. 21 nie ma sensu (powinno być „belonging to the hyperbolic plane”). Z tych samych powodów zapisy „ $q_1 \perp m \cdot H$ ” (ll. -8, -4) są formalnie niepoprawne. W wielu miejscach dalej również  $H$  jest traktowana jako pojedyncza forma, a nie klasa;
- 5.8. Definicja 2.2.6 jest przez pomyłkę/niestaranność trywialna: skoro  $q_1$  i  $q_2$  mają mieć ten sam wymiar  $n$ , to korzystając z „Witt’s cancelation property” można pokazać, że relacje Witt-podobieństwa i izometrii niczym się nie różnią. Ponadto, znak  $n$  używany jest w dwóch rolach (jako wymiar form  $q_1$  i  $q_2$  oraz jako krotność  $H$  w l. -8);
- 5.9. s. 16, l. -8: „By Theorem 2.2.14, we have [...]” – tu nie trzeba Tw. 2.2.14, to wynika z założenia, że to są dwa różne rozkłady tej samej formy  $q$ ;
- 5.10. s. 16, l. -2: niezdefiniowane oznaczenie  $\bar{u}$ . Czytelnik może zgadywać, że chodzi o warstwę  $u$  w  $K(\mathfrak{p}) = R_{\nu_{\mathfrak{p}}}/\mathfrak{m}_{\nu_{\mathfrak{p}}}$  (por. Tw. 2.2.16(1)) lub w  $\bar{K}_{\mathfrak{p}}/\bar{K}_{\mathfrak{p}}^2$  (por. Stw. 2.1.10). W obu przypadkach jednak zapis  $\bar{u} \notin \bar{K}_{\mathfrak{p}}^2$  formalnie nie ma sensu. To niezdefiniowane oznaczenie  $\bar{u}$  występuje także w Tw. 2.2.16;
- 5.11. s. 16, l. -2: „Then there is a unique 4-dimensional anisotropic form [...]” – w jakim sensie ta forma jest „unique”? Przecież jej kształt zależy co najmniej od wyborów  $u$  oraz  $\pi$ , nie mówiąc o kolejności współczynników i innych izometriach;

- 5.12. s. 17, l. 6: niezdefiniowane/niezrozumiałe oznaczenie „ $\langle \pi \rangle_{q_2}$ ”, też na s. 36, l. -5 i dalej;
- 5.13. s. 17, sformułowania Tw. 2.2.17, 2.2.18 i Wn. 2.2.19: niejasny zapis/konwencja „ $p \in \Omega_K$ ”, nie tylko z powodów wymienionych w [5.5](#) powyżej. Mianowicie, zbiór punktów  $\Omega_K$  zawiera nie tylko waluacje  $p$ -adyczne  $\nu_p$  dla ideałów pierwszych  $p \subseteq \mathcal{O}_K$ , ale także punkty pochodzące od rozszerzeń nieskończonej waluacji  $\nu_\infty$  (patrz Uwaga 2.1.7). Co zatem dokładnie oznacza zapis „ $p \in \Omega_K$ ”? Czy chodzi tylko o waluacje  $p$ -adyczne jak sugerowałby wybór znaku  $p$ ? Czy uwzględnione są też rozszerzenia  $\nu_\infty$  jak sugerowałoby sformułowanie „for all places”? Podobne nie do końca jasne konwencje związane z  $\Omega_K$  powtarzają się wielokrotnie też w dalszych częściach pracy;
- 5.14. s. 18, ll. 23-24: niezdefiniowana notacja  $K_p^{\times 2}$  (czy chodzi o  $\dot{K}_p^2$ ?).
- 5.15. s. 20, ll. 6-7: zdanie „It depends only on the isometry class of the form  $q$ , and not on the choice of a diagonalization” nie ma za bardzo sensu skoro niezmiennik Hassego zdefiniowany jest w Def. 2.2.13 wyłącznie dla form diagonalnych;
- 5.16. s. 20, l. -8: niezdefiniowane oznaczenie  $s(q)$  (mamy tylko  $s_p(q)$  dla  $K_p$  w Def. 2.2.13, dla dowolnego ciała lokalnego nie zostało to zdefiniowane);
- 5.17. s. 21, l. 15: definicja zbioru  $C = \{P \mid F(P) = 0\}$  – jakie jest uniwersum tego zbioru, tj. czego elementami są punkty  $P$ ? Przestrzeni  $\mathbb{F}_q^2 = \mathbb{F}_q \times \mathbb{F}_q$  czy może  $\overline{\mathbb{F}_q}^2$  (por. s. 27, l. 10)?
- 5.18. s. 24, Lemat 3.1.3: wygląda na to, że wbrew sformułowaniu „Keep the notation as in Algorithm 1” obiekty oznaczone w lemacie jako  $\mathfrak{g}_1, \dots, \mathfrak{g}_m$  nie są ideałami konstruowanymi w algorytmie (wiersz 8), ale oznaczają one faktyczne poszukiwane faktory radykalne ideału  $\mathfrak{a}$ . A na etapie lematu jeszcze nie wiemy czy to to samo! Jest to subtelna ale istotna różnica, a wychwycić ją można tylko uważnie wglębiając się w dowód lematu, bo samo sformułowanie jest mylące. Przykładowo, zdanie w dowodzie „The assertion is trivially true for  $\mathfrak{a}_0$  and  $\mathfrak{b}_1$ ” ma rację bytu tylko gdy  $\mathfrak{g}_i$  oznaczają faktyczne faktory. Podobna sytuacja ma miejsce w dowodzie poprawności Algorytmu 2 (faktory  $\mathfrak{h}_i$ );
- 5.19. s. 31, ll. -7 - -3: w l. -7 w formule definiującej  $b$  znajduje się przecinek, po którym zaczyna się nowy wielomian – nie jest jasne czy to literówka czy jakaś wcześniej nie opisana konwencja. Podobnie jest w l. -3 (zapis  $x + 7, x + 7$ );
- 5.20. s. 33, Uwaga 3.3.5: jak pisałem w recenzji, ta ważna w dalszej części uwaga jest zbyt lakoniczna i niejasna. Zdanie „Now to factor  $\mathfrak{a}$ , it suffices to factor the two integral ideals  $\mathfrak{a}'$  and  $\mathfrak{a} \cdot \mathcal{O}_K$ ” nic tak naprawdę nie mówi. Powinien być sformułowany lemat zawierający precyzyjną formułę na rozkład ideału ułamkowego  $\mathfrak{a}$  w terminach rozkładów  $\mathfrak{a}'$  and  $\mathfrak{a} \cdot \mathcal{O}_K$  i krótki dowód. Podobnie dalej, kwestię punktów „nieskończonych” opisuje krótkie nieformalne zdanie i odsyłacz do równie nieprecyzyjnej Uwagi 2.1.6;
- 5.21. s. 36, ll. 1-2: z Tw. 2.2.3 wynika tylko jedna implikacja, aby uzasadnić drugą należy jeszcze przywołać Tw. 2.2.7;
- 5.22. s. 38, l. 9: bez wyjaśnienia (przypomnienia) jak wyglądają elementy ciała  $K(p)$  i jakie konwencje ich reprezentacji przyjęto, wyniki tych obliczeń (współczynniki 6,6,7 i 5 form  $q'_0$  i  $q'_1$ ) niewiele czytelnikowi mówią;
- 5.23. s. 42, l. 2: jest „it’s determinant will be a square”, powinno być „its discriminant will be a square”;
- 5.24. s. 48, ll. 14-15: w pracy  $\text{disc}(q) \in \dot{K}/\dot{K}^2$ , co to więc znaczy  $\nu_p(\text{disc}(q))$  i  $\text{disc}(q) - 1$ ? Jeśli te operacje są wykonywane na ustalonym reprezentancie to należy skomentować czy/dlaczego nie zależą od jego wyboru. Podobnie jest na s. 49, l. -13 oraz na s. 49, l. -6 (zapis  $\langle \text{disc}(q) \rangle$ ) i in.;
- 5.25. s. 50, l. -1 oraz s. 52, l. 11: te warianty Zasady Lokalno-Globalnej nie zostały przytoczone w preliminariach, przydałoby się tu przynajmniej cytowanie.
6. (Subiektywnie) niekompletność prezentacji, luki/błędy w argumentacji:
- 6.1. brak wyjaśnień czy/jak następujące operacje są obliczalne: test  $\mathfrak{b}_i \neq \mathcal{O}_K$  (wiersz 5 Algorytmu 1, podobnie wiersz 3 Algorytmu 2), test  $|\mathcal{O}_K/\mathfrak{a}| = q^d$  (w. 1 Alg. 3), wyznaczenie  $\pi$  (w. 9 Alg. 6), wyznaczenie listy  $\mathfrak{P}$ , zwłaszcza punkty „nieskończone” (w. 8 Alg. 7, też w Alg. 9 i 11); wyznaczenie nowego  $p \notin \mathfrak{P}(q)$  (w. 13 Alg. 15); test bycia kwadratem (w. 7 Alg. 18, w. 1 Alg. 19).



- Przynajmniej niektóre z tych operacji nie są oczywiste. W mojej opinii rozprawa doktorska jest idealnym miejscem na tego typu nie do końca trywialną dyskusję (na którą być może nie ma miejsca w artykułach w specjalistycznych czasopiśmiech);
- 6.2. s. 25, ll. -7,-6: zdanie „It follows immediately from the preceding lemma that the algorithm terminates.” wg mnie jest zbyt lakoniczne. Zauważmy, że z Lematu 3.1.3 co najwyżej wynika, że największym spośród konstruowanych ideałów  $b_i$  (odpowiadający za warunek stopu) jest ideał  $b_m = \mathfrak{g}_m$ , który niekoniecznie jest równy całemu  $\mathcal{O}_K$  (?). Chyba, że chodzi o  $b_{m+1} = \mathcal{O}_K$ , ale ten przypadek skrajny nie jest dyskutowany w dowodzie lematu (swoją drogą nie wiadomo jaki jest zakres indeksu  $i$  w lemacie – z kontekstu wynika że chyba  $i = 0, \dots, m$ , niestety nie jest to sprecyzowane). Wydaje się, że własność stopu wynika nie tylko z Lematu 3.1.3, ale też nietrywialnie z jego dowodu oraz konstrukcji pętli;
  - 6.3. ss. 28-29, dowód poprawności Alg. 2: brak argumentu explicite dla własności stopu.
  - 6.4. s. 31, Algorytm 3: brak wyjaśnienia jak powinny być losowane elementy  $b$  zbioru  $\mathcal{O}_K \setminus \mathfrak{a}$  w wierszu 4. Dokładniej, należałoby uzasadnić, że algorytm losujący zawsze po skończonej liczbie iteracji wybierze  $b$  spełniające warunek z wiersza 6 (czy zbiór  $\mathcal{O}_K \setminus \mathfrak{a}$  jest skończony?). Od sposobu wyboru  $b$  zależy własność stopu całego algorytmu;
  - 6.5. s. 40, l. 2: „write the form  $q \cong q_1 \perp \pi \cdot q_2$ , where [...]” – istnienie takiego rozkładu nie jest oczywiste ( $q$  ma tu dowolne współczynniki w  $K$ ), być może przez nie do końca jasną notację. Ponieważ z takiego rozkładu mniej lub bardziej jawnie korzysta się w wielu miejscach pracy, w preliminarzach powinien być sformułowany odp. fakt z krótkim dowodem;
  - 6.6. s. 42, ll. -13 - -11: Jedyne zdanie dowodu popr. Alg. 11 „The dimension of the anisotropic part of  $q$  is clearly the maximum [...]” jest po prostu przełożeniem na język naturalny tego co robi algorytm. Zatem niesie tyle samo istotnej treści co stwierdzenie „The algorithm is clearly correct.” A tu jednak jest pewna praca do wykonania: żaden z faktów przytoczonych do tej pory w pracy nie wyraża bezpośrednio wymiaru anizotropowego jako maksimum z wymiarów lokalnych. Poza tym, należy uzasadnić, że można ograniczyć się tylko do  $q_p$  dla  $p \in \mathfrak{P}$  (np. przez wykazanie, że  $\dim_a(q_p) = 0$  dla  $p \notin \mathfrak{P}$  stosując „second residue homomorphism” podobnie jak na s. 40);
  - 6.7. s. 44, l. 2: coś jest nie tak z formułą  $q_1 \perp -q_2 \cong (m - n) \cdot H$  (główny argument dowodu poprawności Alg. 12) – chociażby wymiary się nie zgadzają: wymiar lewej str. to  $\dim(q_1) + \dim(q_2)$  zaś prawej  $2(m - n)$ , te liczby nie muszą być równe (por. też 2.14.);
  - 6.8. s. 48, l. 1: „must differ by one” – a dlaczego nie 3? Wiemy tylko że ma być nieparzysty – brak argumentu na to, że ma różnić się dokładnie o 1;
  - 6.9. s. 51, ll. -3 - -1: „algorithm terminates after appending sufficiently many (but a finite number)” – brak argumentu na poparcie tej kluczowej, dalece nieoczywistej obserwacji; punktów  $p \notin \mathfrak{P}(q)$  jest na ogół nieskończenie wiele, zatem skończoność ciągu wyborów mocno zależy od sposobu wybierania, tego algorytm w ogóle nie precyzuje;
  - 6.10. s. 57, l. -3: aby mieć tę formułę na  $\ell(a)$  należy jeszcze wykazać implikację „przeciwną” do tej z Obs. 6.1.1. Mianowicie, pokazać, że  $\langle a, -1, \dots, -1 \rangle$  izotropowa  $\Rightarrow a \in D_K(\langle 1, \dots, 1 \rangle)$ . Co nie jest chyba takie oczywiste, bo wektor izotropowy  $(a_0, a_1, \dots, a_n) \in K^{n+1}$  może mieć  $a_0 = 0$ ? Podobny problem z potencjalnym „dzieleniem przez 0” występuje na s. 58, l. -6 w „ $1 \in D_p(\langle -1, a \rangle) \Rightarrow a \in D_p(\langle 1, 1 \rangle)$ ”; Brak w tych miejscach wyczerpujących argumentów.