DZIAŁ NAUKOWY

MATEMATYKA STOSOWANA 10, 2009

Andrzej Paszkiewicz (Warszawa)

O pewnej hipotezie dotyczącej wielomianów nieprzywiedlnych nad GF(2)[1]

Streszczenie. W pracy zostały znalezione wszystkie najmłodsze leksykograficznie wielomiany nierozkładalne nad ciałem binarnym GF(2) o stopniach od 10000 do 20000. Każdy ze znalezionych wielomianów posiada szczególną strukturę: może być przedstawiony w postaci $X^n + g(X)$, gdzie $g(X)$ jest wielomianem bardzo niskiego stopnia w stosunku do n, zależnym od n. Hipoteza, o której mowa w tytule dotyczy oszacowania maksymalnej szybkości wzrostu stopnia wielomianu $g(X)$ w zależności od n. Przy okazji odnosimy się do innych przypuszczeń mówiących o zależności stopnia wielomianu $g(X)$ od n. Badania przeprowadzono z wykorzystaniem techniki obliczeń rozproszonych w niewielkiej sieci komputerowej składającej się z komputerów IBM PC.
Słowa kluczowe: wielomiany nieprzywiedlne, ciała skończone.

1. Wstęp. Wielomiany nieprzywiedlne (nierozkładalne) nad ciałami skończonymi odgrywają ważną rolę w wielu dziedzinach związanych z techniką, m.in. w kryptografii [8], [6],[4], teorii kodowania [3] oraz technikach przetwarzania równoległego i szybkich obliczeń [1]. Wiele schematów kryptograficznych, np. wymiany klucza sesyjnego, wykorzystuje w swej budowie wielomiany nieprzywiedlne nad ciałami skończonymi. Z uwagi na ustawiczny postęp w zakresie technologii oraz nauki, w obawie przed kompromitacją, schematy te muszą być modyfikowane m.in. przez zwiększanie stopni stosowanych tam wielomianów nieprzywiedlnych. Najczęściej wielomiany te posiadają pewną specyficzną strukturę, są wielomianami rzadkimi np. trójmianami lub pięciomianami. Pewne korzyści algorytmiczne przynosi również wykorzystanie wielomianów „gęstych", w których występują wszystkie możliwe jednomiany [9]. Takie wielomiany nazywamy pełnymi. Od dawna opracowywane są tablice wielomianów nieprzywiedlnych (pierwotnych) aż do wysokich stopni nad małymi ciałami skończonymi (patrz [10]). Posia-

([1]) Praca została w części sfinansowana w ramach projektu badawczego nr N517 003 32/0583 ze środków na naukę w latach 2007–2010

danie choćby jednego wielomianu nieprzywiedlnego nad ciałem skończonym pozwala efektywnie wyznaczyć wszystkie pozostałe [9]. Stąd też istnieje duże zainteresowanie posiadaniem choćby jednego wielomianu nieprzywiedlnego dla każdego ze stopni, które mogą być wykorzystane w praktyce.

W przypadku najprostszego ciała skończonego GF(2), nie dla wszystkich stopni istnieje trójmian nierozkładalny o współczynnikach zerojedynkowych lub nierozkładalny wielomian pełny. W [9] zauważono, że z potrzeb praktyki wynika, że liczba niezerowych współczynników wielomianu nierozkładalnego nie jest najważniejszą sprawą (np. z punktu widzenia realizacji szybkiej arytmetyki w ciele skończonym z wykorzystaniem układów mikroprocesorowych). O wiele ważniejszą rzeczą jest aby wszystkie niezerowe współczynniki wielomianu nieprzywiedlnego, z pominięciem być może współczynnika przy najwyższej potędze wielomianu były skupione blisko siebie. W szczególności interesującym wydaje się być poszukiwanie dla ustalonej liczby dodatniej A wielomianów nierozkładalnych $f(X) \in F_2[X]$ postaci

$$f(X) = X^n + \sum_{i=0}^{k} a_i X^i \tag{1}$$

takich, że $k < A \cdot \log n$, przy czym $a_k = 1$.

Mówimy, że wielomian $f(X) \in F_2[X]$ jest młodszy leksykograficznie od wielomianu $g(X) \in F_2[X]$ (lub po prostu młodszy), jeżeli zachodzi nierówność $f(2) < g(2)$, gdzie współczynniki binarne obydwu wielomianów traktowane są jak liczby rzeczywiste wraz z naturalnymi operacjami dodawania i mnożenia liczb rzeczywistych, a znak mniejszości dotyczy liczb rzeczywistych. Wielomian nieprzywiedlny $f(X) \in F_2[X]$, dla którego nie istnieje młodszy od niego wielomian nieprzywiedlny, nazywamy najmłodszym, zaś liczbę k występującą we wzorze (1) stopniem wewnętrznym tego wielomianu. W [9] została sformułowana następująca:

Hipoteza 1. Istnieje taka stała dodatnia A, że dla każdego naturalnego n istnieje wielomian nierozkładalny $f(X) \in F_2[X]$ mający postać (1), taki że $k < A \cdot \log n$.

W szczególności, z powyższej Hipotezy 1 wynika, że jeśli $f(X)$ jest najmłodszym wielomianem nierozkładalnym stopnia n, to jego stopień wewnętrzny jest zależny logarytmicznie od n.

S. Gao, J. Howell i D. Panario sformułowali przypuszczenie podobne do Hipotezy 1 [7]. Na podstawie badań wielomianów nierozkładalnych o współczynnikach z GF(2) do stopnia 2000 stwierdzili, że we wszystkich przypadkach istnieje wielomian nierozkładalny stopnia $n \leq 2000$, którego stopień wewnętrzny k spełnia nierówność $k < \log_2 n + 3$. Odniesiemy się do tego przypuszczenia na końcu tej pracy.

Heurystycznym argumentem przemawiającym za słusznością Hipotezy 1

jest następujący fakt. Liczba wielomianów nierozkładalnych stopnia n o współczynnikach z GF(2) jest równa

$$I_n = \frac{1}{n} \sum_{d|n} \mu(d) \cdot 2^{\frac{n}{d}}, \tag{2}$$

gdzie μ jest funkcją Möbiusa. Mamy

$$I_n = \frac{2^n}{n} + \frac{1}{n} \sum_{\substack{d|n \\ d>1}} \mu(d) \cdot 2^{\frac{n}{d}} = \frac{2^n}{n} + O\left(\frac{2^{n/2}}{n}\right),$$

więc

$$\frac{I_n}{2^n} = \frac{1}{n} + O\left(\frac{2^{-n/2}}{n}\right).$$

Oznacza to, że prawdopodobieństwo wylosowania wielomianu nierozkładalnego stopnia n o współczynnikach z GF(2) jest odwrotnie proporcjonalne do n. Analizując zatem n początkowych wielomianów o współczynnikach z GF(2) we wzrastającym porządku leksykograficznym, mamy dużą szansę, że jeden z nich okaże się wielomianem nierozkładalnym. Gdy stopień wewnętrzny k spełnia nierówności $1 \le k \le \log_2 n$, wówczas możemy wygenerować $2^{\log_2 n} = n$ wielomianów stopnia n o współczynnikach z GF(2), posiadających strukturę jak we wzorze (1) co kończy nasze rozumowanie.

W pracy [2] dla każdego $1 \le n \le 10000$ wyznaczono najmłodszy wielomian nierozkładalny nad GF(2). Wszystkie ze znalezionych tam wielomianów nierozkładalnych, z wyjątkiem jednego, posiadały stopień wewnętrzny nie większy niż 15, przy czym wielomianów o stopniu wewnętrznym równym 15 znaleziono dokładnie 100. Najmłodszym wielomianem nierozkładalnym nad GF(2) o stopniu wewnętrznym równym 16 jest wielomian $f_{16,1}(X) = X^{9465} + X^{16} + X^{14} + X^{11} + X^{10} + X^9 + X^6 + X^5 + 1$. Obliczenia przeprowadzone w pracy [2] wykonano na pięciu izolowanych komputerach klasy IBM PC z zegarem między 1200 MHz a 3 GHz i pamięcią od 512 MB do 2 GB.

2. Założenia nowego projektu i przeprowadzone obliczenia. Na decyzję o rozszerzeniu zakresu badań nad najmłodszymi wielomianami nierozkładalnymi miały wpływ doświadczenia uzyskane w poprzednim projekcie [2], w ramach którego wyznaczono wszystkie najmłodsze leksykograficznie wielomiany nieprzywiedlne nad GF(2) do stopnia 10000. Najsłabszy punkt tych obliczeń stanowił czynnik ludzki. Konieczność „ręcznego sterowania" obliczeniami i dbania o spójność obliczeń stanowi dużą niedogodność.

Zarządzanie obliczeniami wykonywanymi z wykorzystaniem nawet niewielkiej liczby komputerów nie połączonych ze sobą za pomocą sieci jest rzeczą uciążliwą i może być przyczyną licznych błędów. W związku z tym już w samych założeniach nowego projektu przyjęto, że obliczenia zostaną

przeprowadzone w niewielkiej lokalnej sieci komputerowej. Do zarządzania obliczeniami wydzielony został jeden nadrzędny komputer, który przydzielał zadania pozostałym komputerom uczestniczącym w eksperymencie. Do obliczeń wykorzystano oprogramowanie stworzone przez studentów Instytutu Telekomunikacji Politechniki Warszawskiej w ramach projektów przedmiotowych. Wyselekcjonowany został software stworzony przez różne zespoły studenckie, napisany przy odmiennych założeniach. Dodatkową weryfikację poprawności uzyskanych wyników przeprowadzono w fazie końcowej na serwerze przy użyciu pakietu NTL [11]. Z uwagi na dużą złożoność problemu znajdowania najmłodszego wielomianu nierozkładalnego o stopniu powyżej 10000, zadanie przydzielane przez serwer dla pojedynczego komputera polegało na wysłaniu stopnia, dla którego ma być wyznaczony taki wielomian. Po otrzymaniu zwrotnie pliku tekstowego zawierającego znaleziony wielomian zadanie przydzielano ponownie do innego komputera i dopiero po porównaniu zgodności obydwu przesłanych plików znaleziony wielomian zapisywano do pliku z wynikami. Arbitralnie przyjęto, że brak odpowiedzi ze strony liczącego komputera przez czas większy niż 10 godzin powoduje skreślenie zadania i przydzielenie go innemu komputerowi. Wartym podkreślenia jest fakt, że przypadek taki w praktyce nie miał miejsca. Dodatkowym zadaniem komputera sterującego obliczeniami była modyfikacja strony zawierającej aktualny status (mapę) wykonanych i toczących się obliczeń.

Do badania nieprzywiedlności wielomianu $f(X)$ o współczynnikach z ciała skończonego GF(2) wygodnie jest wykorzystać najprostszy z możliwych algorytmów [8], [6]. Najważniejszymi elementami tego algorytmu są: podnoszenie wielomianu o współczynnikach z GF(2) do kwadratu, redukcja modulo wielomian nieprzywiedlny $f(X)$ oraz wyznaczanie największego wspólnego dzielnika dwóch wielomianów. Jedynie pierwszy z tych problemów daje się efektywnie rozwiązać. Problem redukcji modularnej bez założenia specjalnej struktury wielomianu modularnego daje się łatwo rozwiązać jedynie w przypadku (bardzo) rzadkich wielomianów albo na odwrót, gdy wielomian modularny jest maksymalnie gęsty, np. typu AOP (*All One Polynomial*). Tego typu wielomiany nieprzywiedlne pojawiają się niezbyt często, ale stanowią (prawdopodobnie) nieskończoną klasę wielomianów. Dla $n < 1000$ istnieje dokładnie 67 wielomianów typu AOP [9]. W niniejszej pracy wykorzystano następujący algorytm badania nieprzywiedlności wielomianów:

Algorytm testowania nieprzywiedlności wielomianu $f(X)$ nad GF(2)

$A(X) \leftarrow X$
for $j \leftarrow 1$ to n do
{
$A(X) \leftarrow A(X)^2 \bmod f(X)$
if $GCD(A(X)+X, f(X)) \not\equiv 1$ then return „reducible"
}
if $A(X) = X$ then return „irreducible"
else return „reducible"

W kontekście powyższego algorytmu trzy rzeczy wymagają komentarza: podnoszenie wielomianu do kwadratu, redukcja modularna oraz wyznaczanie największego wspólnego dzielnika dwóch wielomianów o współczynnikach z ciała GF(2). Operacja podnoszenia do kwadratu jest najprostszą z nich z uwagi na to, że mamy $A(X)^2 = A(X^2)$. Wielomian, który powstaje z wielomianu $A(X)$ po podniesieniu go do kwadratu otrzymuje się przez zamianę zmiennej X na X^2. W celu wykonania redukcji modulo wielomian $f(X) = X^n + g(X)$, gdzie $g(X) = X^k + \sum_{i=0}^{k-1} a_i X^i$, możemy posłużyć się poniższym ciągiem zależności

$$
\begin{aligned}
&X^n = g(X),\\
&X^{n+j} = g(X)\cdot X^j \quad \text{dla} \quad j = 1, ..., n-k-1,\\
&X^{2n-k} = a_{k-1}X^{n-1} + a_{k-2}X^{n-2} + ... + a_1 X^{n-k+1} + X^{n-k} + g(X),\\
&X^{2n-(k-1)} = a_{k-2}X^{n-1} + ... + a_1 X^{n-(k-2)} + X^{n-(k-1)} + g(X)\cdot X\\
&\qquad\qquad + a_{k-1}g(X),\\
&\vdots\\
&X^{2n-1} = X^{n-1} + ... + a_1 X^{n-(k-2)} + X^{n-(k-1)}\\
&\qquad + g(X)\cdot(X^{k-1} + a_{k-1}X^{k-2} + ... + a_2 X + a_1).
\end{aligned}
$$

W przypadku, gdy n jest niezbyt wielką liczbą naturalną, wygodnie jest zapisać w postaci tablic ciąg reszt $X^{n+j}(\mathrm{mod} f(X))$ dla $j = 0, 1, ..., n-2$ i wykorzystywać je do redukcji modularnej. W istocie, ze względu na to, że redukcja modularna jest przeprowadzana dla wielomianów będących kwadratami, wystarczy pamiętać jedynie te wartości X^{n+j}, dla których $n+j$ jest liczbą parzystą. Z powyższych wzorów wynika, że jeżeli k jest małą liczbą w stosunku do n, to każdy spośród wielomianów $X^{n+j}(\mathrm{mod} f(X))$ dla $j = 0, 1, ..., n-2$ jest wielomianem rzadkim, który łatwo można wyznaczać na bieżąco, znając wartość j oraz wielomian $g(X)$. Podejście to

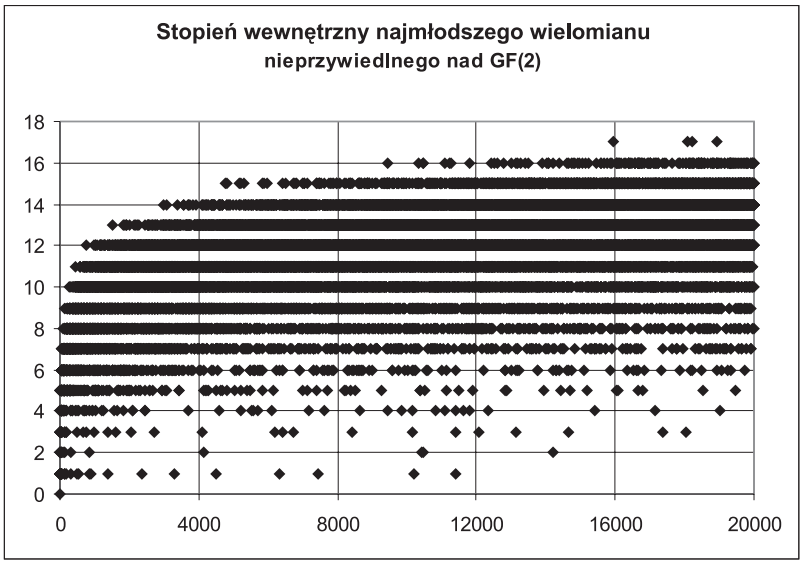
pozwala w sposób istotny zaoszczędzić zarówno pamięć komputera jak również liczbę odwołań do niej, co w przypadku niezbyt nowoczesnych stacji roboczych wykorzystywanych do obliczeń ma niebagatelne znaczenie. Opisana metoda redukcji modularnej „na bieżąco" została wykorzystana na potrzeby niniejszej pracy.

Oprócz redukcji modularnej ważnym punktem algorytmu badania nieprzywiedlności jest znajdowanie największego wspólnego dzielnika dwóch wielomianów. Do tego celu wykorzystano pomysł zawarty we wcześniejszej pracy [2], polegający na zastosowaniu zmodyfikowanego algorytmu Steina w odniesieniu do wielomianów o współczynnikach z GF(2).

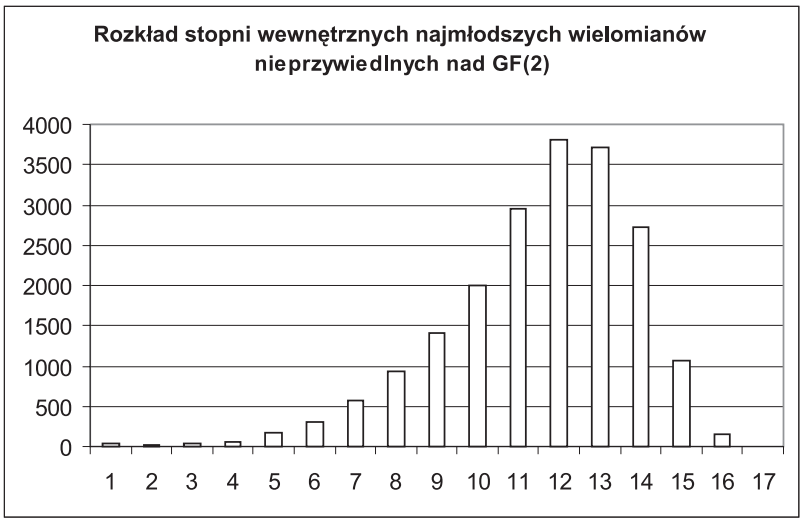
3. Przeprowadzone badania i wnioski. Opisane w niniejszej pracy badania są naturalną kontynuacją badań przeprowadzonych w [2]. W ramach projektu przyjęto założenie o maksymalnym ograniczeniu wpływu czynnika ludzkiego na organizację obliczeń i przeprowadzono następujące badania:

1. Dla każdej wartości n z przedziału [10001, 20000] wyznaczono najmłodszy wielomian nieprzywiedlny nad GF(2). Wykres ilustrujący zależność stopnia wewnętrznego najmłodszego wielomianu nieprzywiedlnego w funkcji stopnia tego wielomianu przedstawiono na Rys. 1. W zakresie przeprowadzonych obliczeń znaleziono 4 najmłodsze wielomiany nieprzywiedlne, które mają stopień wewnętrzny równy 17. Zostały one zapisane w Tabeli 3.
2. Zbadano maksymalną szybkość wzrostu stopnia wewnętrznego najmłodszych wielomianów nieprzywiedlnych, a co za tym idzie prawdziwość hipotezy sformułowanej w pracy [9]. Wartość stałej deklarowana w Hipotezie 1 we wszystkich przypadkach nie przekroczyła liczby 1,4. Jednocześnie warto zwrócić uwagę na to, że przypuszczenie Gao, Howella i Panario [7] jest nieprawdziwe. Pierwszy kontrprzykład można podać dla wielomianu $f_{17,1}(X)$, który ma stopień 15926 (patrz Tab. 3). Mamy tu $\log_2 15926 + 3 = 16,959 < 17$, co obala to przypuszczenie.
3. Zbadano rozkład stopni wewnętrznych najmłodszych wielomianów nieprzywiedlnych (Rys. 2). Dla stopni $n \leq 20000$ dominują wielomiany o stopniu wewnętrznym równym 12. Krzywa rozkładu posiada charakter dzwonowy niesymetryczny o części wzrastającej dłuższej niż część opadająca.
4. W Tabeli 2 zapisano szczegółowy rozkład stopni wewnętrznych najmłodszych wielomianów nieprzywiedlnych, których stopnie $n \in [10000, 20000]$ przedstawiono w rozbiciu na podprzedziały o długości 1000. Z tabeli tej wynika, że w zakresie stopni od 10000 do 17000 dominują najmłodsze wielomiany nieprzywiedlne o stopniu wewnętrznym równym 13. W zakresie stopni od 17000 do 20000 najwięcej jest wielomianów o stopniu wewnętrznym równym 14.

5. Dla stopni $n \in [10000, 20000]$ istnieją 153 najmłodsze wielomiany nieprzywiedlne nad GF(2) o stopniu wewnętrznym równym 16. Zapisano je wszystkie w Tabeli 1 z wykorzystaniem notacji szesnastkowej, w której 1='0001', 2='0010', 3='0011', 4='0100', 5='0101', 6='0110', 7='0111', 8='1000', 9='1001', A='1010', B='1011', C='1100', D='1101', E='1110', F='1111'. Przykładowo zapis w pierwszej komórce tej tabeli tj. 9465 : 14E61 należy rozumieć w następujący sposób. Liczba przed dwukropkiem oznacza stopień wielomianu nieprzywiedlnego. Jest nim 9465. Występujący po dwukropku ciąg znaków w zapisie szesnastkowym odpowiada po zamianie na system binarny „młodszej" części wielomianu nieprzywiedlnego stopnia 9465. Mamy 14E61 = '0001' || '0100' || '1110' || '0110' || '0001' = '10100111001100001', gdzie symbol || oznacza konkatenację. Tak więc zapis w pierwszej komórce Tabeli 1 przedstawia w postaci zakodowanej następujący wielomian: $X^{9465} + X^{16} + X^{14} + X^{11} + X^{10} + X^9 + X^6 + X^5 + 1$. Jest to pierwszy najmłodszy wielomian nieprzywiedlny, dla którego stopień wewnętrzny jest równy 16, czyli w przyjętej konwencji zapisu wielomian $f_{16,1}(X)$.



Rys. 1 Zależność stopnia wewnętrznego najmłodszego wielomianu nieprzywiedlnego nad GF(2) od jego stopnia.



Rys. 2. Rozkład stopni wewnętrznych najmłodszych wielomianów nieprzywiedlnych nad GF(2) dla stopni nie większych od 20000.

W przypadku implementacji arytmetyki ciał skończonych za pomocą najmłodszych wielomianów nieprzywiedlnych i przy wykorzystaniu popularnych procesorów jest rzeczą wygodną, aby młodsza część wielomianu nieprzywiedlnego mogła być zapisana w jednym słowie maszynowym (patrz wyżej punkt. 5). Większość z dostępnych obecnie na rynku tanich procesorów posiada słowo maszynowe o długości 16 bitów. W tej sytuacji wybór jednego z wielomianów wymienionych w powyższej Tabeli 1 może prowadzić do utrudnień implementacyjnych, niezależnie od przyjętego rozwiązania (np. reprezentacja młodszej części wielomianu nieprzywiedlnego na dwóch słowach maszynowych lub na jednym słowie maszynowym plus dodatkowa informacja o 16 bicie ustawionym na 1). Wady takiej pozbawione są implementacje sprzętowe, w których można zdefiniować słowo maszynowe dowolnej długości. Rzecz jasna, że również w sprzęcie łatwiejsze są implementacje arytmetyki dla wielomianów modularnych mających strukturę wielomianów nieprzywiedlnych najmłodszych leksykograficznie.

Tabela 2 zawiera wyniki obliczeń dotyczących rozkładu stopni wewnętrznych najmłodszych leksykograficznie wielomianów nieprzywiedlnych o stopniach od 10000 do 20000. Wyniki dotyczące wielomianów o stopniach do 10000 przedstawione zostały w pracy [2].

Tabela 1
Początkowe najmłodsze leksykograficznie wielomiany nierozkładalne nad GF(2)
o stopniu wewnętrznym równym 16

9465 : 14E61	10348 : 12223	10447 : 10EA3	10467 : 11E45	11084 : 13015
11225 : 1131B	11260 : 1131B	11824 : 12F21	12433 : 100B5	12512 : 1039B
12608 : 1522B	12787 : 10853	12999 : 10B41	13138 : 10AA7	13189 : 18DEF
13255 : 10FF7	13407 : 107C5	13478 : 12563	13877 : 10A75	14014 : 12F21
14058 : 135E3	14063 : 132F5	14196 : 157DD	14408 : 14DA7	14594 : 100CD
14669 : 10DD1	14733 : 1060D	14770 : 108BD	14824 : 11569	14935 : 125BB
14964 : 16FE5	15051 : 1324D	15157 : 10DE7	15221 : 12FE1	15448 : 12173
15599 : 12627	15608 : 1899F	15662 : 112E5	15759 : 14C77	15863 : 1180B
15921 : 14F53	16051 : 11BCB	16057 : 13A67	16076 : 105D5	16091 : 1105F
16138 : 14C93	16179 : 17A5F	16241 : 153A1	16309 : 12161	16380 : 1086F
16381 : 1A405	16384 : 14A03	16395 : 12B25	16429 : 10A97	16488 : 1249B
16549 : 1E22F	16571 : 169C7	16580 : 1094F	16638 : 11873	16662 : 11131
16663 : 17A0F	16665 : 19D6F	16691 : 13B39	16702 : 10C3D	16735 : 1BAED
16761 : 14FAF	16815 : 115DD	16847 : 19915	16916 : 139C7	16981 : 10025
16993 : 1B161	16995 : 131A3	17009 : 14F99	17027 : 13913	17126 : 128E5
17136 : 18F59	17152 : 13FFD	17205 : 18AED	17220 : 14671	17235 : 14353
17358 : 18DAD	17403 : 1605B	17449 : 19D1B	17622 : 17173	17836 : 11677
17865 : 14701	17882 : 11E67	17938 : 11A55	18024 : 198FF	18035 : 194D1
18114 : 182B3	18118 : 109E3	18133 : 10153	18195 : 14027	18206 : 13239
18225 : 1819D	18246 : 132C9	18282 : 12475	18351 : 10907	18376 : 170E1
18391 : 15DED	18415 : 111C7	18418 : 13E41	18423 : 128B5	18437 : 13EBD
18470 : 152F3	18479 : 1049F	18485 : 13EFF	18503 : 103A7	18547 : 10787
18553 : 12A6F	18561 : 11F7D	18643 : 11BC7	18760 : 119F9	18787 : 101B1
18797 : 1043F	18823 : 10B87	18861 : 111BF	18916 : 11321	18922 : 108F3
18947 : 12843	18948 : 10881	18997 : 10CE5	19035 : 12E1F	19057 : 113BB
19136 : 18C65	19165 : 13D99	19243 : 1344D	19297 : 10E39	19304 : 107EB
19311 : 1502F	19319 : 10809	19340 : 15465	19341 : 108A9	19381 : 18D7F
19430 : 12D0B	19442 : 14A2B	19456 : 10EDB	19520 : 1361F	19559 : 14E5B
19602 : 12415	19664 : 10E99	19674 : 11FD1	19724 : 11485	19772 : 1126B
19790 : 1CA61	19800 : 134C5	19837 : 14B0D	19908 : 169DF	19917 : 13499
19965 : 13DDB	19968 : 16EA5	19978 : 113E1	19990 : 10FB3	20006 : 13CD9

Tabela 2
Rozkład stopni wewnętrznych najmłodszych wielomianów nieprzywiedlnych

Stopień wewn.	10-11 (tys.)	11-12 (tys.)	12-13 (tys.)	13-14 (tys.)	14-15 (tys.)	15-16 (tys.)	16-17 (tys.)	17-18 (tys.)	18-19 (tys.)	19-20 (tys.)
1	1	1	0	0	0	0	0	0	0	0
2	2	0	0	0	1	0	0	0	0	0
3	1	1	1	1	1	0	0	1	1	0
4	2	4	1	0	0	1	0	1	0	1
5	3	3	2	1	2	1	4	0	1	1
6	6	3	4	5	7	2	5	2	4	4
7	15	12	11	12	8	12	9	6	9	13
8	22	25	23	20	22	18	15	15	13	14
9	41	41	38	41	32	31	26	29	26	19
10	80	61	60	68	50	49	51	65	47	53
11	133	143	126	107	117	108	96	86	96	95
12	235	220	216	216	168	180	175	155	156	157
13	258	243	240	232	252	255	238	239	223	214
14	162	182	207	198	229	225	236	267	262	236
15	36	57	66	93	99	107	114	118	124	162
16	3	4	5	6	12	10	31	16	35	31
17	0	0	0	0	0	1	0	0	3	0

Tabela 3
Pełna lista najmłodszych wielomianów nierozkładalnych nad GF(2)
o stopniu wewnętrznym równym 17 w zakresie stopni do 20000

$f_{17,1}(X) = X^{15926} + X^{17} + X^{12} + X^{11} + X^8 + X^7 + X^6 + X^3 + X^2 + X + 1$
$f_{17,2}(X) = X^{18072} + X^{17} + X^{13} + X^{12} + X^{11} + X^{10} + X^7 + X^3 + X + 1$
$f_{17,3}(X) = X^{18237} + X^{17} + X^{12} + X^{10} + X^8 + X^7 + X^6 + X + 1$
$f_{17,4}(X) = X^{18934} + X^{17} + X^{12} + X^{10} + X^8 + X + 1$

Podziękowanie. Wyrażam podziękowanie mojemu byłemu studentowi Panu Łukaszowi Leszkowi Gajowiakowi, który w ramach pracy magisterskiej stworzył oprogramowanie umożliwiające zarządzanie obliczeniami rozproszonymi w sieci.

Literatura

[1] W. Aiello and T. Leighton, *Coding Theory, Hypercube Embeddings, and Fault Tolerance*, in Proc. Of the 3rd Annual Symposium on Parallel Algorithms and Architectures, pp. 125–136, 1991;

[2] P. Bartosik, A. Paszkiewicz, *Wyznaczanie Najmłodszych Leksykograficznie Wielomianów Nieprzywiedlnych*, Krajowe Sympozjum Telekomunikacji i Teleinformatyki, Bydgoszcz, 10-12 września 2008, Przegląd Telekomunikacyjny 8–9 (2008), 1282–1292;
[3] R. Blahut, *Theory and Practice of Error Control Codes*, Addison-Wesley Publishing Company, Reading, Massachusetts, Reprint with Correction 1984;
[4] I. F. Blake, S. Gao, R. J. Lambert, *Construction and Distribution Problems for Irreducible Trinomials over Finite Fields*, in Applications of Finite Fields, D. Gollman (ed.), Oxford, Oxford Univ. Press, 1996;
[5] R. P. Brent, S. Larvala, P. Zimmerman, *A Fast Algorithm for Testing Irreducibility of Trinomials mod 2*; Technical Report PRG-TR-13-00, Oxford University Laboratory Wolfson Building, Parks Road, Oxford OX1 3QD;
[6] D. Coppersmith, *Fast Evaluation of Logarithms in Fields of Characteristic Two*, IEEE Trans. Inform. Theory, vol. IT-30, pp. 587–594, 1984;
[7] S. Gao, J. Howell, D. Panario, *Irreducible Polynomials of Given Forms*, in R. Mullen (ed.) Finite Fields: Theory, Applications and Algorithms, Contemporary Mathematics (1999), vol. 225, pp. 43–54;
[8] A.J. Menezes et al., *Handbook of Applied Cryptography*, CRC Press, Boca Raton, New York 1997;
[9] A. Paszkiewicz, *Rzadkie i gęste wielomiany nierozkładalne*, Krajowe Sympozjum Telekomunikacji'95, t. B, Problemy Podstawowe, str. 249-254, Wyd. Politechniki Warszawskiej, Warszawa 1995;
[10] G. Seroussi, *Table of Low-Weight Binary Irreducible Polynomials*, Hewlett-Packard, HPL, pp. 98–135, August 1998;
[11] V. Shoup, http://www.shoup.net.papers/ (12.2007).

Andrzej Paszkiewicz
Politechnika Warszawska
ul. Nowowiejska 15/19
00-661 WARSZAWA, Poland
E-mail: anpa@tele.pw.edu.pl

On a hypothese concerning irreducible trinomials over GF(2)

Abstract. In this paper all irreducible and lexicographically youngest polynomials over the binary field GF(2) and degrees between 10000 to 20000 have been enumerated. Each of these polynomials has a specific structure: it can be expressed in the form $X^n + g(X)$, where $g(X)$ is a polynomial with very low degree in comparison to n and depending on n. A hypothesis mentioned in the title addresses to the maximal growth rate the degree of $g(X)$ as a function of n. By the way we discuss other conjectures concerning relations between the degree of $g(X)$ and n. All computations were performed by the aid of distributed computing technique in a small computer network consisting of few IBM PC work stations.
Keywords: irreducible polynomials, finite fields.

(*wpłynęło 21 czerwca 2008 r.*)