Raport Badawczy

Research Report

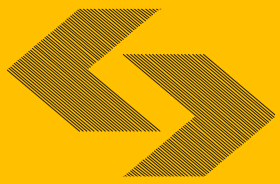
RB/59/2010

Zastosowania algorytmów transformacji wielomianowych

J. Kapusta

Instytut Badań Systemowych
Polska Akademia Nauk

Systems Research Institute
Polish Academy of Sciences



ZASTOSOWANIA ALGORYTMÓW TRANSFORMACJI WIELOMIANOWYCH

Joanna Kapusta
Studia Doktoranckie IBS PAN
Katolicki Uniwersytet Lubelski Jana Pawła II

The paper presents a brief review of applications of algorithms for computing polynomial transformations. Special attention is paid to social and commercial applications of these algorithms i.e. applications in the broadcast encryption, secret sharing and e-voting.

***Key words**: polynomial transformation, broadcast encryption, secret sharing, e-voting, information security.*

1. Algorytmy transformacji wielomianowych - wprowadzenie

Algorytmy transformacji wielomianowych są to metody przekształcania reprezentacji wielomianu jednej lub wielu zmiennych

$$p(x) = \sum_{\alpha \in Q_n} a_\alpha L_\alpha(x)$$

względem bazy $\{L_\alpha(x)\}$ do reprezentacji tego wielomianu względem bazy $\{B_\alpha(x)\}$:

$$p(x) = \sum_{\alpha \in Q_n} c_\alpha B_\alpha(x),$$

gdzie Q_n oznacza ustalony zbiór indeksów. Najbardziej znanym przykładem obliczania transformacji wielomianowych jest słynny algorytm FFT (Cooley & Tukey, 1965) obliczania dyskretnej transformacji Fouriera oraz algorytm obliczania transformacji do niej odwrotnej. Algorytmy te pozwalają na przechodzenie pomiędzy reprezentacją wielomianu w bazie potęgowej, a reprezentacją tego wielomianu w bazie Lagrange'a z uwzględnieniem specjalnej konfiguracji punktów, tzn. punktów $x_i = \omega^i (i = 0,1,\ldots,n-1)$, gdzie ω jest pierwiastkiem pierwotnym z jedności stopnia $n = 2^k$. Transformacje Fouriera i transformacje do niej odwrotną można obliczyć wykonując $\frac{3}{2} n \log n + 0(n)$

operacji arytmetycznych (von zur Gathen & Gerhard, 2003). Jeśli punkty x_i $(i = 0,1,\ldots,n-1)$ tworzą ciąg geometryczny to wartości wielomianu w tych punktach można wyznaczyć uogólnionym algorytmem DFT (Rabiner, Schafer, & Rader, 1969) rzędu $O(n \log m)$. Interesujące rezultaty dotyczące algorytmów zmiany reprezentacji wielomianu z uwzględnieniem baz wielomianowych Newtona i potęgowej można znaleźć w pracy (Gerhard, 2000). W wymienionej pracy został przeanalizowany zarówno przypadek dowolnej konfiguracji punktów jak i specjalnej konfiguracji punktów, tzn. punktów, których współrzędne tworzą ciąg arytmetyczny. Ważnym wynikiem z tego zakresu wydaje się być uogólnienie algorytmów rzędu $O(n \log n)$ obliczania transformacji Lagrange'a-Newtona i transformacji do nich odwrotnej na punkty generowane przez równanie rekurencyjne pierwszego rzędu (Smarzewski & Kapusta, 2007) oraz jego rozszerzenie na przypadek wielowymiarowy (Kapusta & Smarzewski, 2009). Przegląd algorytmów transformacji wielomianowych z uwzględnieniem różnych baz wielomianowych można znaleźć m.in. w (Aho, Hopcroft, & Ullaman, 2003), (Bini & Pan, 1994), (Bostan & Schost, 2005) oraz (Knuth, 2002). Warto podkreślić, że zredukowanie kwadratowej złożoności obliczeniowej algorytmów obliczania transformacji wielomianowych do liniowo-logarytmicznej uzyskuje się dzięki wykorzystaniu algorytmu obliczania splotu, bazującego na algorytmie FFT.

2. Zastosowania o znaczeniu społecznym i komercyjnym

Algorytmy transformacji wielomianowych znajdują zastosowanie w wielu zagadnieniach analizy numerycznej np. interpolacji, ekstrapolacji, aproksymacji oraz w metodach typu Galerkina (Bini & Pan, 1994); (Kincaid & Cheney, 2006). Mają one również inne zastosowania w zagadnieniach związanych z życiem społecznym czy przedsięwzięciami komercyjnymi.

W artykule (Kapusta, 2009) podano zastosowania algorytmów transformacji wielomianowych w aktualnych problemach kryptograficznych takich jak szyfrowanie, czy głosowanie elektroniczne. Istotne znaczenie społeczne wydają się mieć zastosowania w głosowaniach bazujących na nowoczesnych technologiach. Niewątpliwą zaletą głosowań z wykorzystaniem internetu jest to, że nie wymagają one udania się do określonego miejsca głosowania w celu oddania głosu. Dzięki temu możliwy jest udział w procesie grupowego podejmowania decyzji osób przebywających poza miejscem swojego zameldowania, czy mających trudności w poruszaniu się. Proponowany model (Kapusta, 2009) umożliwia zebranie i zliczenie głosów niezależnie od wybranej techniki głosowania (np. Condorceta, Bordy, większościowej, aprobującej). Warto zwrócić uwagę, że zastosowanie różnych technik może prowadzić do uzyskania odmiennych wyników (Hołubiec & Mercik, 2006).

Zastosowanie algorytmów transformacji wielomianowych w schematach dzielenia sekretu zostało przedstawione m. in. w artykule (Smarzewski & Kapusta, 2005). Proponowane tam schematy bazują na interpolacji Hermite'a i są uogólnieniem klasycznego schematu zaproponowanego przez A. Shamira (1979). Zastosowanie interpolacji Hermite'a pozwala na konfigurowanie hierarchii wśród uczestników podziału sekretu. W rzeczywistości naturalne jest występowanie pomiędzy jednostkami pewnych zależności, wynikających z kwalifikacji tych jednostek (np. w instytucjach bankowych, wojskowych). Różne warianty schematu dzielenia sekretu, omówione w artykule (Smarzewski & Kapusta, 2005), umożliwiają dopasowanie go do potrzeb grup o ustalonej hierarchii. Algorytmy transformacji wielomianowych w tych schematach są wykorzystywane zarówno w procesie dzielenia sekretu jak i jego odtwarzania. Inne zastosowanie tych algorytmów, możliwe do wykorzystania w działalności komercyjnej, zostanie przedstawione w następnej sekcji.

3. Transmisja rozgłoszeniowa

Transmisja rozgłoszeniowa polega na przesyłaniu informacji do wielu odbiorców bez wskazywania adresata. Rozgłaszane dane mogą być szyfrowane w celu zapewnienia kontroli dostępu - wtedy tylko użytkownicy posiadający klucz umożliwiający deszyfrowanie mają dostęp do przesyłanych informacji. Przykładem zastosowania takiej metody przesyłania danych jest kodowana transmisja telewizyjnych platform cyfrowych - tylko użytkownicy, który dokonali opłaty uzyskują dostęp do programów telewizyjnych. Taka transmisja wymaga skonstruowania protokołu, który pozwoli na bezpieczne i efektywne rozpowszechnienie nowego klucza deszyfrującego wśród uprawnionych użytkowników.

Na przestrzeni lat powstało wiele rozwiązań umożliwiających dynamiczne wykluczanie użytkowników z systemu oraz ich przywracanie, np. (Fiat & Naor, 1993), (Naor & Pincas, 2000). Bezpieczeństwo zaproponowanego przez M. Naora i B. Pincasa modelu umożliwiającego wielokrotne wykluczanie użytkowników z systemu jest uzależnione od trudności rozwiązania decyzyjnego problemu Diffiego-Helmana (DDH). Opisany przez nich model działa w oparciu o interpolację Lagrange'a. Poniżej zostanie przedstawiona modyfikacja tego modelu wykorzystująca interpolację Hermite'a. Ponadto omówiony zostanie sposób poprawienia efektywności modeli tego typu poprzez zastosowanie szybkich algorytmów transformacji wielomianowych dla specjalnych konfiguracji punktów, przedstawionych w (Smarzewski & Kapusta, 2007). W proponowanym modelu *nadawca* jest odpowiedzialny za dostarczenie użytkownikom kluczy prywatnych, generowanie nowych kluczy umożliwiających

rozkodowanie informacji, nazywanych kluczami sesyjnymi, oraz rozgłaszanie odpowiadających tych kluczom bloków aktywujących. Uprawniony użytkownik uzyskuje dostęp do zakodowanej informacji odtwarzając klucz sesyjny - wykorzystuje w tym celu informacje zawarte w rozgłoszonym bloku aktywującym oraz swój klucz prywatny.

Inicjalizacja systemu: Założenia DDH wymagają istnienia grupy cyklicznej G z generatorem g. Dla ustalenia uwagi niech grupa G będzie podgrupą ciała Z_p reszt modulo p, gdzie p jest dużą liczbą pierwszą i niech rząd grupy G będzie dużą liczbą pierwszą q taką, że $q|p-1$. Na etapie inicjalizacji nadawca wybiera w sposób losowy wielomian

$$p(x) = \sum_{k=0}^{m} a_k \prod_{i=0}^{k-1}(x - x_i),\ a_m \neq 0, x_i \neq x_j \text{ dla } i \neq j,$$

ze współczynnikami $a_k \in Z_q$ oraz przekazuje każdemu użytkownikowi klucz prywatny

$$K_i = (x_i, y_i),\ i = 0,1,\ldots,n-1,$$

gdzie $y_i = p(x_i)$ oraz $x_i \neq x_j$ **dla** $i \neq j$. W szczególnym przypadku nadawca może wybrać punkty x_i tak aby spełniały równanie rekurencyjne pierwszego rzędu. Pozwala to – poprzez zastosowanie szybkiego algorytmu obliczania transformacji Newtona-Lagrange'a (Smarzewski & Kapusta, 2007), na zredukowanie kosztu obliczenia kluczy prywatnych użytkowników.

Wykluczenie nieuprawionych użytkowników: Nadawca ustala liczbę użytkowników wykluczanych, określa ich klucze prywatne

$$K_i = (x_i, y_i),\ i = 0,1,\ldots,k-1,\ k \leq m,$$

i oblicza wartości

$$p^{(v)}(\hat{x}),\ v = 0,1,\ldots,m-k,$$

gdzie punkt $\hat{x}$ nie jest związany z żadnym kluczem odbiorcy. W kolejnym kroku nadawca przygotowuje blok aktywujący T dla wybranego klucza sesyjnego S. W tym celu oblicza zmodyfikowane ilorazy różnicowe

$$c_i = p[x_0, x_1, \ldots, x_i], \qquad i = 0,1,\ldots,m, \quad x_k = x_{k-1} = \cdots = x_m = \bar{x},$$

ze wzoru (Kincaid & Cheney, 2006):

$$p[x_i, x_{i+1}, \ldots x_{i+v}] =$$

$$= \begin{cases} \dfrac{p[x_{i+1}, x_{i+2}, \ldots x_{i+v}] - p[x_i, x_{i+1}, \ldots x_{i+v-1}]}{x_{i+v} - x_i} & \text{dla } x_{i+v} \neq x_i, \\ \dfrac{p^{(v)}(x_i)}{v!} & \text{dla } x_{i+v} = x_i, \end{cases}$$

Następnie nadawca wybiera w sposób losowy liczbę $r \in Z_q$ i rozgłasza blok aktywujący

$$T = [Sg^{rc_m}, g^r, x_0, x_1, \ldots, x_k; g^{rc_0}, g^{rc_1}, \ldots, g^{rc_{m-1}}]$$

oraz kryptogram $E(S,M)$ wiadomości M zaszyfrowanej przy pomocy klucza S. Użytkownik, po otrzymaniu bloku T, oblicza klucz sesyjny S ze wzoru

$$S = \frac{Sg^{rc_m}}{g^{rc_m}} = \frac{Sg^{rc_m} \prod_{i=0}^{m-1} (g^{rc_i})^{\frac{1}{\prod_{j=0}^{m-1}(x_u - x_j)}}}{(g^{rx_u})^{\frac{1}{\prod_{j=0}^{m-1}(x_u - x_j)}}},$$

gdzie para wartości x_u i y_u pochodzi z jego klucza prywatnego. Po obliczeniu klucza S użytkownik wykorzystuje go do deszyfrowania $E(S,M)$ otrzymując w ten sposób M.

Z powyższych rozważań wynika, że każdy użytkownik nie należący do grupy użytkowników wykluczanych, może obliczyć klucz S wykorzystując swój klucz prywatny oraz rozgłoszony blok aktywujący T. Z kolei użytkownik, którego klucz prywatny posłużył do wyznaczenia ilorazów różnicowych rozgłaszanych w bloku aktywującym T nie posiada wystarczających informacji niezbędnych do odtworzenia klucza S. Warto zwrócić uwagę że, koalicja użyt-

kowników wykluczanych również nie ma możliwości wyznaczenia klucza sesyjnego S.

W modelach tego typu należy zwracać uwagę na odpowiedni dobór stopnia wielomianu, gdyż zbyt niski stopień może w sposób istotny zagrażać bezpieczeństwu systemu, umożliwiając wyznaczenie współczynników wielomianu przez koalicje użytkowników. W celu uniknięcia takiej sytuacji należy zakładać, że stopień wielomianu m jest większy od liczby użytkowników systemu n. Ponadto warto podkreślić, że zastosowanie interpolacji Hermite'a zamiast interpolacji Lagrange'a (Naor & Pincas, 2000) prowadzi do obniżenia kosztu komunikacji poprzez zmniejszenie liczby rozgłaszanych wartości x_i. Dokładniej, w modelach wykorzystujących interpolację Lagrange'a rozgłaszanych jest m różnych wartości x_i, natomiast w modelach działających w oparciu o interpolację Hermite'a ta liczba redukuje się do k. W szczególnym wypadku – wymiany klucza sesyjnego bez konieczności wykluczania użytkowników rozgłaszana jest tylko jedna wartość $x_i = \hat{x}$.

Literatura

[1] Aho, A. V., Hopcroft, J. E., & Ullaman, J. D. (2003): *Projektowanie i analiza algorytmów.* Helion.

[2] Aho, A. V., Steiglitz, K., & Ullman, J. D. (1975): Evaluating polynomials at fixed sets of points. *SIAM Journal on Computing* 4(4), 533-539.

[3] Bini, D., & Pan, V. (1994): *Polynomial and matrix computation* 1. Boston.

[4] Bostan, A., & Schost, E. (2005): Polynomial evaluation and interpolation on special sets of points. *Journal of Complexity* 21 (4), 420-446.

[5] Cooley, J. W., & Tukey, J. W. (1965): An algorithm for the machine calculation of complex Fourier series. *Mathematics of Computation* 19 (90), 297-301.

[6] Fiat, A., & Naor, M. (1993): Broadcast encryption. *Lecture Notes in Computer Science* 773, 480-491.

[7] Gerhard, J. (2000): Modular algorithms for polynomial basis conversion and greatest factorial factorization. *RWCA'00*, 125-141.

[8] Hołubiec, J., & Mercik, J. W. (2006): *Techniki i tajniki głosowania.* Warszawa: EXIT.

[9] Kapusta, J. (2009): Szybkie algorytmy transformacji wielomianowych i ich zastosowania kryptograficzne. W: J. Hołubiec, *Analiza systemowa w finansach i zarządzaniu*, t. 11, 115-131.

[10] Kapusta, J., & Smarzewski, R. (2009). Algorithms for fast multivariate polynomial interpolation and evaluation. *Journal of Complexity 25 (4)*, strony 332 – 338.

[11] Kincaid, D., & Cheney, W. (2006): *Analiza numeryczna.* WNT.

[12] Knuth, D. E. (2002): *Sztuka Programowania. Algorytmy Seminumeryczne.* WNT.

[13] Naor, M., & Pincas, B. (2000): Efficient trace and revoke schemes. *Financial Cryptography 2000.* Lecture Notes in Computer Science, 1-20.

[14] Rabiner, L. R., Schafer, R. W., & Rader, C. M. (1969): The chirp z-transform algorithm. *IEEE Transactions on Audio and Electroacoustics* AU-17 (2), 86-92.

[15] Shamir, A. (1979): How to share a secret? *Communications of the ACM,* 22, 612-613.

[16] Smarzewski, R., & Kapusta, J. (2005): Algorithms for multi-secret hierarchical sharing schemes of Shamir type. *Annales UMCS Informatica* AI III, 65-91.

[17] Smarzewski, R., & Kapusta, J. (2007): Fast Lagrange-Newton transformations. *Journal of Complexity 23 (3)*, 336-345.

[18] von zur Gathen, J., & Gerhard, J. (2003). *Modern Comuter Algebra.* Cambridge.