Wykład 9.

9.1 „Pęknięcia" (burst error)

Będziemy rozważać słowa długości n nad alfabetem F. Niech l będzie liczbą naturalną. Najmniejszy spośród zbiorów $P \subseteq F^n$ takich, że

1. jeżeli $a_i = 0$ dla i takich, że $l < i \leqslant n$, to $a_1 \dots a_n \in P$,

2. jeżeli $w \in P$, to także cykliczne przesunięcie w należy do P

będziemy nazywać zbiorem pęknięć długości l i oznaczać symbolem $\mathcal{P}_l$, a elementy tego zbioru będziemy nazywać pęknięciami długości l.

Kod liniowy K wykrywa pęknięcia długości l, jeżeli żadne niezerowe pęknięcie długości l nie należy do K. Tak więc K wykrywa pęknięcia długości l, jeżeli $K \cap (\mathcal{P}_l \setminus \{0 \dots 0\}) = \emptyset$.

Lemat 9.1 *Jeżeli liniowy kod $K \subseteq F^n$ wymiaru m wykrywa pęknięcia długosci l, to $n-m \geqslant l$.*

Dowód. Rozważmy zbiór

$$X = \{a_1 \dots a_n \in F^n : a_i = 0 \text{ dla wszystkich } i,\ l < i \leqslant n\}.$$

Oczywiście, $X \subseteq \mathcal{P}_l$ i X ma r^l elementów, gdzie r jest liczbą elementów ciała F. Zauważmy, że żadne dwa (różne) elementy zbioru X nie przystają do siebie modulo K ($e_1 - e_2 \notin K$ dla dowolnych $e_1, e_2 \in K$ takich, że $e_1 \neq e_2$). Wiadomo, że relacja równoważności R taka, że $xRy \Leftrightarrow x - y \in K$ rozbija zbiór F^n na równoliczne klasy abstracji. Jedną z klas abstrakcji jest K o r^m elementach, więc relacja R rozbija F^n na r^{n-m} klas abstrakcji. W każdej klasie abstrakcji jest najwyżej jeden element zbioru X, więc $r^{n-m} \geqslant r^l$. □

Lemat 9.2 *Kod cykliczny generowany przez wielomian stopnia k wykrywa pęknięcia długości k.* □

Kod liniowy K koryguje pęknięcia długości l, jeżeli różnica żadnych dwóch (różnych) pęknięć długości l nie należy do K.

Lemat 9.3 *Jeżeli kod liniowy K $K \subseteq F^n$ wymiaru m koryguje pęknięcia długosci l, to wykrywa pęknięcia długości $2 \cdot l$. Wobec tego, jeżeli liniowy kod $K \subseteq F^n$ wymiaru m koryguje pęknięcia długosci l, to $n - m \geqslant 2 \cdot l$.* □

9.2 Algorytm „error-trapping"

Niech $K \subseteq F^n[x]$ będzie kodem cyklicznym korygującym t błędów, generowanym przez wielomian g. Rozważmy następujący algorytm:
Algorytm „error-trapping". Dane: wielomian w.

1. $I := 0$; $W := w$;

2. **dopóki** $I < n+1$
   (a) $S := W \bmod g(x)$;
   (b) jeżeli S ma $\leqslant t$ niezerowych współczynników, to zwróć $C^{n+1-I}(W-S)$ (i przerwij obliczenia);
   (c) $W := C(W)$; $I := I+1$.

Lemat 9.4 *Niech $K \subseteq F^n[x]$ będzie kodem cyklicznym korygującym t błędów, generowanym przez wielomian g stopnia k. Jeżeli $w \in S_t(v)$, $v \in K$ oraz $w - v$ jest pęknięciem długości k, to algorytm „error-trapping" uruchomiony ze słowem w zwraca słowo v.*

Dowód. Nietrudno zauważyć, że jeżeli podany algorytm wykonuje instrukcję „zwróć", to zwraca $C^{n+1-i}(C^i(w) - C^i(w) \bmod g)$ dla pewnego i takiego, że $C^i(w) \bmod g$ ma najwyżej t niezerowych współczynników. Jest oczywiste, że $C^i(w) - C^i(w) \bmod g \in K$ oraz

$$C^i(w) \in S_t(C^i(v)) \cap S_t(C^i(w) - C^i(w) \bmod g).$$

Ponieważ kod K koryguje t błędów, więc $C^i(v) = C^i(w) - C^i(w) \bmod g$. Wobec tego, ten algorytm może zwrócić tylko

$$C^{n+1-i}(C^i(w) - C^i(w) \bmod g) = C^{n+1-i}(C^i(v)) = C^{n+1}(v) = v.$$

Jeżeli $w - v$ jest pęknięciem długości k, to dla pewnego i przesunięcie $C^i(w-v)$ jest wielomianem stopnia $k-1$. Zauważmy, że wtedy

$$C^i(w) \bmod g = (C^i(v) + C^i(w-v)) \bmod g = C^i(w-v) \bmod g = C^i(w-v).$$

Ponieważ $w \in S_t(v)$, więc $w - u$ oraz $C^i(w-v)$ są wektorami o najwyżej t niezerowych współczynnikach. Oznacza to, że dla rozważanego i spełniony jest warunek, pod którym algorytm wykonuje „zwróć". Wobec tego, jeżeli nie zwrócił wcześniej, to zwróci dla tego i. □

9.3 Pewna konstrukcja kodów cyklicznych

Przypuśćmy, że $p(x)$ jest wielomianem. Okresem $p(x)$ nazywamy najmniejszą liczbę m taką, że $p(x)$ dzieli $x^m - 1$.

Zauważmy, że okresem $x^2 + x + 1$ jest 3, a okresem $x^3 + x + 1$ jest 7. Wielomian $x \cdot p(x)$ nie ma okresu.

Jest oczywiste, że jeżeli $p(x)$ jest wielomianem o okresie m, to $p(x)$ jest generatorem kodu cyklicznego długości m.

Lemat 9.5 *Jeżeli $p(x)$ jest wielomianem o okresie m, to $p(x)$ dzieli $x^k - 1$ wtedy i tylko wtedy, gdy m dzieli k.*

Dowód. Wiadomo, że

$$x^l - 1 = (x-1) \cdot (x^{l-1} + x^{l-2} + \ldots + 1).$$

Podstawiając wielomian x^m zamiast x otrzymujemy stąd, że

$$x^{l \cdot m} - 1 = (x^m - 1) \cdot (x^{(l-1) \cdot m} + x^{(l-2) \cdot m} + \ldots + 1).$$

Jeżeli więc m dzieli k, czyli jeżeli $k = l \cdot m$ dla pewnego l, to wielomian $x^k - 1$ jest podzielny przez $x^m - 1$, a także przez każdy wielomian dzielący $x^m - 1$, w tym przez $p(x)$.

Przypuśćmy, że $p(x)$ dzieli $x^k - 1$. Ponieważ $p(x)$ dzieli $x^m - 1$, więc dzieli także $(x^k - 1) - (x^m - 1) = x^m \cdot (x^{k-m} - 1)$. Niech c będzie najmniejszą liczbą taką, że $p(x)$ dzieli $x^c \cdot (x^{k-m} - 1)$. Mamy więc $x^c \cdot (x^{k-m} - 1) = p(x) \cdot q(x)$ dla pewnego wielomianu $q(x)$. Gdyby c było większe od 0, to z podanej równości (po podstawieniu 0 zamiast x) wynika, że $p(0) \cdot q(0) = 0$. Założenie $q(0) = 0$ implikuje, że $q(x) = x \cdot q'(x)$ dla pewnego $q'(x)$ i – w konsekwencji – $x^{c-1} \cdot (x^{k-m} - 1)$ też jest podzielne przez $p(x)$. Założenie $q(0) = 0$ prowadzi więc do sprzeczności. Wobec tego, $p(0) = 0$. Taki wielomian $p(x)$ nie może dzielić żadnego wielomianu $x^k - 1$, a więc nie może mieć okresu. Uzyskana w ten sposób sprzeczność dowodzi, że $c = 0$, czyli że $p(x)$ dzieli $x^{k-m} - 1$.

Niech r będzie resztą z dzielenia k przez m. Gdyby $r > 0$, to przez indukcję, korzystając z wykazanej własności, udowodnilibyśmy, że $p(x)$ dzieli $x^r - 1$. Ponieważ $r < m$, więc przeczy to definicji m. Wobec tego, $r = 0$ i m dzieli k. □

Wniosek 9.6 *Wielomian $x^m - 1$ dzieli $x^k - 1$ wtedy i tylko wtedy, gdy m dzieli k.*

Dowód. Korzystamy z poprzedniego lematu dla $p(x) = x^m - 1$. □

Lemat 9.7 *Przypuśćmy, że $p(x)$ jest wielomianem, t jest liczbą dodatnią oraz spełnione są następujące warunki:*

1. *$p(x)$ jest nierozkładalny,*
2. *wielomian $p(x)$ ma okres i ten okres nie dzieli $2 \cdot t - 1$,*

Niech $g(x) = (x^{2 \cdot t - 1} - 1) \cdot p(x)$. Wielomian $g(x)$ ma okres i jego okres jest najmniejszą wspólną wielokrotnością liczby $2 \cdot t - 1$ i okresu wielomianu $p(x)$.

Dowód. Oczywiście, jeżeli wielomian $g(x)$ dzieli $x^k - 1$, to – na podstawie lematu 9.5 i wniosku 9.6 – k jest wielokrotnością zarówno $2 \cdot t - 1$, jak i okresu wielomianu $p(x)$.

Niech k będzie liczbą podzielną przez $2 \cdot t - 1$ i przez okres wielomianu $p(x)$. Wtedy – na podstawie wspomnianych faktów – zarówno $p(x)$, jak i $x^{2 \cdot t - 1} - 1$ dzielą $x^k - 1$. Pokażemy jeszcze, że $g(x)$ dzieli $x^k - 1$.

Wielomiany $p(x)$ i $x^{2 \cdot t - 1} - 1$ są względnie pierwsze. W przeciwnym razie mają wspólny dzielnik dodatkiego stopnia. Ten dzielnik dzieli także $p(x)$. Ponieważ $p(x)$ jest nierozkładalny, więc dzielnik jest równy $p(x)$. Stąd $p(x)$ dzieli $x^{2 \cdot t - 1} - 1$ oraz okres $p(x)$ dzieli $2 \cdot t - 1$. Jest to sprzeczne z założeniem 2. Jeżeli dwa względnie pierwsze wielomiany dzielą $x^k - 1$, to ich iloczy także dzieli $x^k - 1$. □

Przykład wielomianu rozważanej postaci jest

$$g(x) = (x^5 - 1) \cdot (x^3 + x + 1).$$

Twierdzenie 9.8 *Przypuśćmy, że wielomian $p(x)$ i liczba t spełniają założenia podane w lemacie 9.7 i dodatkowo t nie jest większe od stopnia $p(x)$. Niech $n+1$ będzie najmniejszą wspólną wielokrotnością okresu $p(x)$ i liczby $2 \cdot t - 1$. Wtedy kod cykliczny $K \subseteq F^n[x]$ generowany przez $g(x) = (x^{2 \cdot t - 1} - 1) \cdot p(x)$ koryguje pęknięcia długości t.*

Dowód. Najpierw wprowadzimy pomocniczy aparat pojęciowy. Początkowym pęknięciem długości t nazywamy słowo $a_0 \ldots a_n$ takie, że $a_0 \neq 0$ oraz $a_i = 0$ dla wszystkich i takich, że $t \leqslant i \leqslant n$. Oczywiście, dowolne niezerowe pęknięcie długości t jest postaci $C^i(a)$ dla pewnego pęknięcia początkowego a oraz dla i takiego, że $0 \leqslant i \leqslant n$. Zauważmy też, że jeżeli $i+t-1 \leqslant n$ i a jest pęknięciem początkowym długości t, to $C^i(a) = x^i \cdot a(x)$.

Niech e_1 i e_2 będą różnymi pęknięciami długości t. Mamy wykazać, że $e_1 - e_2 \notin K$. Będziemy dodatkowo zakładać, że oba pęknięcia są niezerowe. W przypadku, gdy jedno z pęknięć jest zerowe, interesująca nas różnica jest z dokładnością do znaku drugim pęknięciem. Powinniśmy więc w tym przypadku wykazać, że pojedyńcze pęknięcie długości t nie należy do K. Każde takie pęknięcie jest postaci $C^i(a)$ dla pewnego początkowego pęknięcia a długości t. Gdyby $C^i(a) \in K$, to cykliczność K implikowałaby, że także $a = C^{n+1-i}(C^i(a)) \in K$. Początkowe pęknięcia długości t są jednak wielomianami stopnia $< t$ i nie mogą należeć do kodu generowanego przez wielomian stopnia $\geqslant 2 \cdot t - 1$.

Aby wykazać, że $e_1 - e_2 \notin K$ dla różnych niezerowych pęknięć e_1 i e_2, dobierzemy odpowiednie l oraz pokażemy, że $C^l(e_1 - e_2) \notin K$. Jeżeli uda się nam to zrobić, warunek $e_1 - e_2 \notin K$ będzie wynikać z cykliczności kodu K.

Niech e_1 i e_2 będą różnymi, niezerowymi pęknięciami długości t. Przyjmijmy, że $e_1 = C^i(p_1)$ i $e_2 = C^j(p_2)$ dla pewnych i, j oraz początkowych pęknięć p_1 i p_2. Załóżmy dodatkowo, że $i \leqslant j$. Pokażemy, że $e_1 - e_2 = C^l(a(x) - x^s \cdot b(x))$ dla pewnych początkowych pęknięć a i b długości t i dla pewnego $s \leqslant n+1-t$. Są możliwe dwa przypadki. Jeżeli $j - i \leqslant n+1-t$, to

$$e_1 - e_2 = C^i(p_1) - C^j(p_2) = C^i(p_1 - C^{j-i}(p_2)) = C^i(p_1(x) - x^{j-i} \cdot p_2(x)).$$

Jeżeli $j - i > n+1-t$, to

$$e_1 - e_2 = C^i(p_1) - C^j(p_2) = C^j(C^{n+1+i-j}(p_1) - p_2) = C^j(-p_2(x) - x^{n+1+i-j} \cdot (-p_2(x)))$$

oraz $n+1+i-j < t$. Ponieważ $2 \cdot t - 1 \leqslant n+1$, więc $t - 1 \leqslant n+1-t$ i ostatecznie $n+1+i-j \leqslant n+1-t$. Tak więc w obu przypadkach znaleźliśmy potrzebne przedstawienie. Zauważmy jeszcze, że jeżeli $e_1 \neq e_2$ oraz $e_1 - e_2 = C^l(a(x) - x^s \cdot b(x))$, to $a(x) - x^s \cdot b(x) \neq 0$.

Dalej wykażemy, że jeżeli mamy $s \leqslant n+1-t$ oraz wielomiany a i b stopnia mniejszego od t, o niezerowych wyrazach wolnych, to

$$a(x) - x^s \cdot b(x) \neq 0 \Rightarrow a(x) - x^s \cdot b(x) \notin K.$$

Faktycznie udowodnimy jednak równoważną własność

$$a(x) - x^s \cdot b(x) \in K \Rightarrow a(x) = x^s \cdot b(x).$$

Załóżmy, że $a(x) - x^s \cdot b(x) \in K$. Równość $a(x) = x^s \cdot b(x)$ wykażemy dowodząc, że $a(x) = b(x)$ i $s = 0$.

W tym celu najpierw podzielmy s przez $2 \cdot t - 1$. Mamy więc

$$s = q \cdot (2 \cdot t - 1) + r$$

dla pewnego q i $r < 2 \cdot t - 1$. Zauważmy, że

$$a(x) - x^s \cdot b(x) = a(x) - x^r \cdot b(x) - x^r \cdot b(x) \cdot (x^{q \cdot (2 \cdot t - 1)} - 1).$$

Lewa strona tej równości należy do K, a więc dzieli się przez $g(x)$. Wobec tego, prawa strona też dzieli się przez $g(x)$. Dzieli się też przez $x^{2 \cdot t - 1} - 1$. Oznacza to, że $a(x) - x^r \cdot b(x)$ dzieli się przez $x^{2 \cdot t - 1} - 1$. Przyjmijmy, że

$$a(x) - x^r \cdot b(x) = d(x)(x^{2 \cdot t - 1} - 1)$$

dla pewnego wielomianu $d(x)$ stopnia k.

Udowodnimy, że $a(x) - x^r \cdot b(x) = 0$. Załóżmy, że wielomian $d(x)$ jest różny od zera. Wtedy prawa strona równości jest wielomianem stopnia $k + 2 \cdot t - 1 \geqslant t$, lewa zaś jest stopnia $\leqslant r + t - 1$. Wobec tego, także $x^r \cdot b(x)$ ma stopień $k + 2 \cdot t - 1$ oraz zachodzi nierówność $t \leqslant k + t \leqslant r$. W wielomianie $x^r \cdot b(x)$ jest składnik x^r. Nierówność $t \leqslant r$ implikuje, że taki składnik jest też w wielomianie $x^r \cdot b(x) - a(x)$, czyli w wielomianie $d(x)(x^{2 \cdot t - 1} - 1)$. Ale żaden z wielomianów $d(x) \cdot x^{2 \cdot t - 1}$ oraz $d(x)$ nie ma takiego składnika. Uzyskana sprzeczność oznacza, że $d(x)$ jest wielomianem zerowym. Tak więc $a(x) - x^r \cdot b(x) = 0$.

Ponieważ wyraz wolny wielomianu $a(x)$ jest niezerowy, więc równość $a(x) - x^r \cdot b(x) = 0$ implikuje, że $r = 0$ (w przeciwnym razie nie uprościmy wyrazu wolnego wielomianu $a(x)$ i suma $a(x) - x^r \cdot b(x)a(x)$ będzie różna od 0). Równość $r = 0$ implikuje z kolei, że $a(x) = b(x)$.

Jeżeli $a(x) = b(x)$, to $a(x) - x^s \cdot b(x) = a(x) \cdot (x^s - 1) \in K$. Stąd wynika, że $g(x)$, a w konsekwencji także $p(x)$ dzielą $a(x) \cdot (x^s - 1)$. Wielomian $p(x)$ nie dzieli wielomianu $a(x)$ (ponieważ stopień $a(x)$ jest mniejszy od stopnia $p(x)$). Wielomian $p(x)$ dzieli więc $x^s - 1$. W tej sytuacji, lemat 9.5 implikuje, że okres $p(x)$ dzieli s. Ponieważ $r = 0$, więc s jest podzielne także przez $2 \cdot t - 1$. Z założenia $s > 0$ otrzymujemy, że s jest przynajmniej równe długości kodu K. Tak więc $s = 0$. $\square$