WYKŁAD 15

$\mathbb{Z}$

$p \in \mathbb{Z}$

$\mathbb{Z}/\equiv_p$

p - pierwsze

$\mathbb{Z}/\equiv_p = : \mathbb{Z}_p$

$\mathbb{F}$ ciało ($\mathbb{Z}_p$)

$\mathbb{F}[X]$ pierścień wiel.

$h \in \mathbb{F}[X]$

$f \equiv_h g \iff h \mid f-g$

$\mathbb{F}[X]/\equiv_h$

pierścień

h - nierozkładalny ciało

$\deg(h) = k$ $|\mathbb{F}|^k$ el. $\mathbb{F}' := \mathbb{F}[X]/\equiv_h$

$[X^0]_{\equiv_h}$

$\mathbb{F}$ to przestrzeń liniowa nad $\mathbb{F}$

$x^0, x^1, \ldots, x^{k-1}$

Przykład/Zastosowanie 21.13 (Kody Reeda-Solomona). Ustalamy ciało $\mathbb{F}$, zwykle jest to cialo $\mathbb{F} = \mathbb{F}_{2^m}$. Traktujemy wiadomość $(a_0, a_1, \ldots, a_{k-1})$, gdzie $a_i \in \mathbb{F}$, jako wielomian

$$f_{\vec{a}} = \sum_{i=0}^{k-1} a_i x^i \in \mathbb{F}[x]$$

Kodujemy tę wiadomość jako wartości wielomianu $\bar{f}$ w n różnych niezerowych punktach $p_0, p_1, \ldots, p_{n-1} \in \mathbb{F}$, gdzie $n \geq k$. Punkty mogą być wybrane dowolnie, ale zwykle ten wybór jest ustalony, bo dla pewnych wartości łatwiej się liczy. Zbiór wektorów wartości w tych punktach to kod Reeda-Solomona.

Kody Reeda Solomona są *kodem liniowym* wymiaru k. Podane wyżej kodowanie odpowiada mnożeniu wiadomości przez macierz a'la Vandermonde.

Odległość

Odległością (Hamminga) jest dla nas ilość pozycji, na których różnią się dwa wektory. Oznaczenie: $d(c, c')$. To jest odległość, tzn. jest symetryczna, spełnia warunek trójkąta i jeśli $d(c, c') = 0$ to $c = c'$.

$\vec{v}, \vec{v}' \in \mathbb{F}^n$

$d(\vec{v}, \vec{v}')$ = „liczba poz i $\vec{v}_i \neq \vec{v}'_i$"

1 1
2 2
3 1

- symetryczna
- $d(\vec{v}, \vec{w}) = 0 \Leftrightarrow \vec{v} = \vec{w}$
- nierówność trójkąta $d(\vec{v}, \vec{w}) \leq d(\vec{v}, \vec{u}) + d(\vec{u}, \vec{w})$

i - różnic

zbiór możliwych słów kodowych

Odległość kodu C to

$$d(C) = \min_{u,v \in C, u \neq v} d(u, v) \ .$$

$\geq$ ← nt. wiel / dł. wejścia ($\geq$)

dł. kodu

Lemat 21.14. *Odległość kodu Reeda-Solomona to* $n - k + 1$.

$w, w' \in$ kod RS n, k

f ← w $\quad$ g ← w' $\quad$ $\deg(f), \deg(g) < k$

$(a_0, \ldots, a_{k-1})$ $\quad$ $(b_0, \ldots, b_{k-1})$

f, g mogą mieć te same wart w $\leq k-1$ punktach

f, g muszą mieć $\geq n - (k-1)$ punktów o różnych wart.

$$|\{i : \bar{f}(i) \neq \bar{g}(i)\}| \geq n - (k-1) = n - k + 1$$

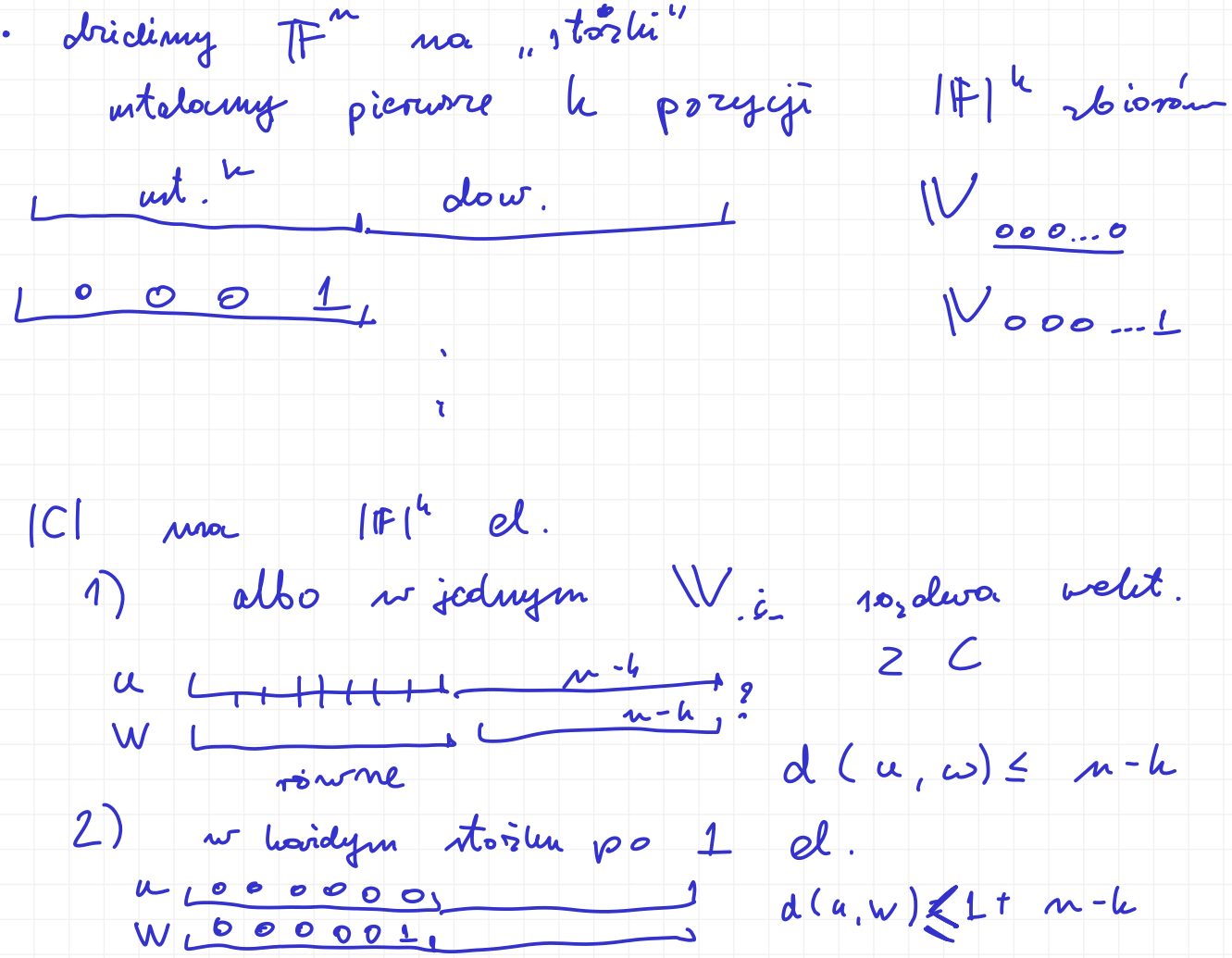
$w, w' \in RS_{n,k}$ $\quad$ $d(w, w') \geq n - k + 1$

$d(C) \geq n - k + 1$

Optymalność odległości (ograniczenie Singletona)

Kody Reeda-Solomona są optymalne, tzn. jeśli kod ma wymiar k oraz długość n, to któreś dwa słowa kodowe mają odległość $\leq n-k+1$.

Twierdzenie 21.15 (Ograniczenie Singletona). *Jeśli w zbiorze $|\mathbb{F}|^n$ wybierzemy $|\mathbb{F}|^k$ wektorów, to któreś dwa mają odległość najwyżej $n-k+1$.*



Poprawianie błędów

Naturalne poprawianie: poprawiamy otrzymane słowo do najbliższego słowa kodowego.

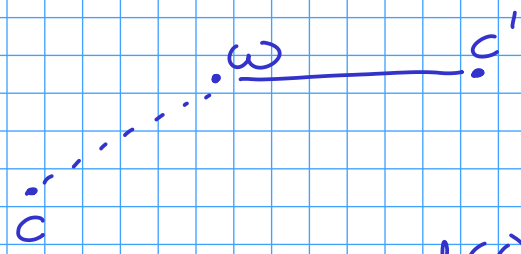
Twierdzenie 21.16. *Jeśli słowo ma mniej niż*

$$< \frac{d(C)}{2}$$

błędów, czyli najwyżej

$$\leq \left\lfloor \frac{d(C)-1}{2} \right\rfloor$$

błędów, to naturalne poprawianie poprawnie dekoduje.



$$\begin{cases} d(\omega, c) < \frac{d(C)}{2} \\ d(\omega, c') \leq d(\omega, c) < \frac{d(C)}{2} \end{cases}$$

$$d(c, c') \leq d(c, \omega) + d(\omega, c') < d(C)$$

$$d(c, c') < d(C)$$

$$\min d(x, y) \quad x \neq y$$

$$\| \quad c = c'$$

RS: kod RS. poprawia $\left\lfloor \frac{n-k}{2} \right\rfloor$ błędów

$n - k \geq 1$ $\quad \frac{n-k}{2}$

$|F| \geq n > k$

2^{32} $\quad$ 32 b.t. $\quad$ najlepsze kody binarne

Algorytm Berlekamp–Welch poprawiania błędów

Cel: dane $\vec{w} = [w_0, \ldots, w_{n-1}] \in \mathbb{F}^n$.
Zakładamy, że jest najwyżej $e \leq \left\lfloor \frac{n-k}{2} \right\rfloor$ błędów.
szukane: wielomian $f \in \mathbb{F}[x]$, t. że $\deg(f) < k$, $f(\alpha_i) \neq w_i$ dla najwyżej e pozycji albo „?”, jeśli nie ma takiego wielomianu.

Oznaczenie: $I = \{i : f(\alpha_i) \neq w_i\}$. Dobrze zdefiniowane, bo takie f jest jedyne. Niech $e = |I|$.

Moglibyśmy po prostu wybrać te błędy, zinterpolować i rozwiązać...

Popatrzmy na wielomian

Definicja 21.17 (Error locator polynomial). Dla zbioru pozycji błędów I zdefiniujmy *error locator polynomial*:

$$E(x) = \prod_{i \in I} (x - \alpha_i)$$

$$Q(x) = f(x) \cdot E(x)$$

- Własności: $\forall_i \quad Q(\alpha_i) = w_i E(\alpha_i)$
  - $i \in I \quad Q(\alpha_i) = f(\alpha_i) \cdot E(\alpha_i) = 0 = w_i \cdot E(\alpha_i)$
  - $i \notin I \quad Q(\alpha_i) = f(\alpha_i) \cdot E(\alpha_i) = w_i \cdot E(\alpha_i)$

A ściśle:

BW1 wielomian E, o wiodącym współczynniku 1, stopnia $e \leq \left\lfloor \frac{n-k}{2} \right\rfloor$

BW2 wielomian Q stopnia $\leq e + k - 1$

BW3 dla każdego i zachodzi $w_i E(\alpha_i) = Q(\alpha_i)$

Słowem kodowym ma być Q/E (jako wielomian).

$Q(x) = f(x) \cdot E(x)$, $\deg f \leq k-1$, $\deg E \leq e$, $\frac{Q}{E} = f(x)$

Uwaga. Jeśli Q/E nie jest zdefiniowane, bo się dzieli z resztą, albo ma za duży stopień, to zwracamy błąd.

f st $\leq k-1$, $f(\alpha_0) \ldots f(\alpha_{n-1})$, ω, $d(\omega, f) = e \leq \left\lfloor \frac{n-k}{2} \right\rfloor$

Lemat 21.18. *Jeśli dla danego $\vec{w}$ istnieje $\vec{w'} \in RS$ takie że $d(w, w') \leq e \leq \left\lfloor \frac{n-k}{2} \right\rfloor$ to istnieją Q, E spełniające BW.*

$\exists f \quad d(\omega, f) = e \leq \left\lfloor \frac{n-k}{2} \right\rfloor \Rightarrow \exists Q, E$

$I \quad \{i : f(\alpha_i) \neq \omega_i\} \quad |I| = e$

$E = \prod_{i \in I} (x - \alpha_i)$

$Q = f \cdot E$ (deg $k-1$, deg e)

$\forall\, \omega_i \cdot E(\alpha_i) = Q(\alpha_i)$ (oba = 0)

$i \in I$

$i \notin I \quad \omega_i \cdot E(\alpha_i) = E(\alpha_i) f(\alpha_i)$, $\omega_i = f(\alpha_i)$

Lemat 21.19. *Jeśli Q_1, E_1 oraz Q_2, E_2 spełniają BW, to $Q_1/E_1 = Q_2/E_2$.*

Uwaga. Zauważmy, że jest to równość ilorazów i reszt, tzn. może być, że oba dzielenia dają resztę. Ale jeśli jeden się dzieli bez reszty, to drugi też, tj. jeśli jest poprawny wynik algorytmu, to wszystkie zwracane dają to samo.

$Q_1 E_2 - Q_2 E_1$ (deg $e+k-1$, e; $e+k-1$, e) $= 0$

- stopień?
- ma ile punktów daje wart 0

$Q_1 E_2 = Q_2 E_1 \quad / E_1 E_2$

$\frac{Q_1}{E_1} = \frac{Q_2}{E_2}$

$\deg(Q_1 E_2 - Q_2 E_1) < 2 \cdot \left\lfloor \frac{n-k}{2} \right\rfloor + k - 1 \leq 2 \cdot \frac{n-k}{2} + k - 1 =$

$= n - k + k - 1 = n - 1$

(e)

α_i: $Q_1 E_2(\alpha_i) = \omega_i \cdot E_1(\alpha_i) E_2(\alpha_i)$

$Q_2 E_1(\alpha_i) = \omega_i \cdot E_2(\alpha_i) E_1(\alpha_i)$

To jak to odtworzyć? Rozwiążemy odpowiedni układ równań liniowych. Zauważmy, że nie interesuje nas, czy ten układ jest jednoznacznie określony, może być nadokreślony lub niedookreślony — dowolne rozwiązanie jest OK i wiemy, że jakieś jest.

E $\left\lfloor \frac{n-k}{2} \right\rfloor$ $e_0, e_1, \dots e_{\frac{n-k}{2}-1}, 1$

Q $e+k-1$ $\left\lfloor \frac{n-k}{2} \right\rfloor, k-1+1$

współczynniki

$\omega_i \; Q(\alpha_i) - E(\alpha_i) = 0$

warunek liniowy na współ.

n warunków liniowych

• Jeśli e < niż jest równ.

• Być może wiele

Czas działania ilość równ $\sim O(n^3)$

• dzielenie Q, E $\frac{Q}{E}$ $O(n^3)$

$\mathbb{C}$ ← jedyne ciało

$a+bi$

$\mathbb{R}[x]/_{\equiv x^2+1} \cong \mathbb{C}$

$a, a+bx$

$a+b\sqrt{3}$ ← ciało

$\uparrow \quad \uparrow$

$\mathbb{Q} \quad \mathbb{Q}$

$\mathbb{Q}[x]/_{\equiv x^2-3=0}$

Czas działania: Trzeba rozwiązać układ równań: $\mathcal{O}(n^3)$ (da się może ciut szybciej w zależność od danych) oraz podzielić dwa wielomiany — $\mathcal{O}(n^3)$. Ponownie dla specyficznych wartości może być ciut lepiej.

21.3 Ciała algebraicznie domknięte

Definicja 21.20 (Ciało algebraicznie domknięte)**.** Ciało $\mathbb{F}$ jest *algebraicznie domknięte*, jeśli każdy wielomian nierozkładalny jest stopnia 1.

Fakt 21.21. *Ciało $\mathbb{F}$ jest algebraicznie domknięte wtedy i tylko wtedy gdy każdy wielomian ma pierwiastek.*

Fakt 21.22. *Ciało algebraicznie domknięte jest nieskończone.*

Przykład 21.23. $\mathbb{C}$ jest ciałem algebraicznie domkniętym. Nie jest nim $\mathbb{R}$ ani żadne $\mathbb{Z}_p$.

Twierdzenie 21.24. *Dla ciała $\mathbb{F}$ istnieje $\mathbb{F}' \supseteq \mathbb{F}$, które jest algebraicznie domknięte oraz działania $\mathbb{F}'$ obcięte do $\mathbb{F}$ to działania $\mathbb{F}$.*

21.4 Rozszerzenia ciał

$S \subseteq \mathbb{F}'$ c. alg. dom.

Definicja 21.25 (Rozszerzenie ciała)**.** Dla ciała $\mathbb{F}$ przez $\mathbb{F}\langle S\rangle$ oznaczamy najmniejsze ciało zawierające $\mathbb{F}, S$.

Rozszerzenie $\mathbb{F}\langle a\rangle$ jest *przestępne*, jeśli a nie jest pierwiastkiem żadnego wielomianu z $\mathbb{F}[x]$ takie a również nazywamy przestępnym. Jest *algebraiczne*, jeśli a jest pierwiastkiem jakiegoś wielomianu z $\mathbb{F}[x]$.

$\mathbb{R}(a)$ $\mathbb{Q}(c)$ $\mathbb{Q}(\pi)$ $\mathbb{Q}\langle\sqrt{3}\rangle$ $x^2-3 \in \mathbb{Q}[x]$ $\mathbb{R}\langle i\rangle$ x^2+1

21.4.1 Rozszerzenie przestępne

Jak wygląda rozszerzenie przestępne? Możemy sobie wyobrazić, że dodajemy do $\mathbb{F}$ jakiś „świeży" element α. W nowym ciele muszą być też wszystkie wielomiany z $\mathbb{F}[\alpha]$ oraz ich odwrotności. Są więc też wszystkie ilorazy wielomian przez wielomian.

Definicja 21.26 (Ciało ułamków prostych)**.** Rozważmy ciało $\mathbb{F}$ oraz wielomiany nad nim $\mathbb{F}[x]$. Na zbiorze $\{\frac{f}{g} : f, g \in \mathbb{F}[x], g \neq 0\}$ wprowadzamy relację równoważności $\frac{f}{g} \sim \frac{f'}{g'} \iff fg' = f'g$. Tak określony zbiór jest ciałem z naturalnie zadanym dodawaniem oraz mnożeniem:

$$\frac{f}{g} + \frac{f'}{g'} = \frac{fg' + f'g}{gg'} \qquad \frac{f}{g} \cdot \frac{f'}{g'} = \frac{ff'}{gg'}$$

Twierdzenie 21.27. *Ciało ułamków prostych dla $\mathbb{F}$ jest izomorficzne z $\mathbb{F}\langle a\rangle$ dla przestępnego a.*

21.4.2 Rozszerzenia algebraiczne

Definicja 21.28. Dla ciała $\mathbb{F}$ oraz elementu a z jego rozszerzenia przez $I(a)$ (ideał a) oznaczamy

$$I(a) := \{f \in \mathbb{F}[x] : \bar{f}(a) = 0\}$$

Lemat 21.29. *Dla ciała $\mathbb{F}$ oraz elementu a z jego rozszerzenia $I(a)$ jest zamknięty na dodawanie i mnożenie przez wielomiany z $\mathbb{F}[x]$.*

Lemat 21.30. *Dla ciała $\mathbb{F}$ oraz elementu a z jego rozszerzenia $I(a)$ jest postaci*

$$I(a) = \{fg : g \in \mathbb{F}[x]\}$$

dla pewnego wielomianu nierozkładalnego $f \in \mathbb{F}[x]$. W szczególności $\bar{f}(a) = 0$.

$I(a)$ jest zam. na gcd

$\downarrow I(a)$

$gcd(f,g) \in$ tt k.

gcd „ideału"

$f \in I(a)$ gcd wielomianu podzielnego

• czy f dzieli wszystko w $I(a)$

TAK $\Rightarrow$ NIE

OK

h $f \mid h$

$gcd(f,h)$ „spada tt"

Po sk. liczbie kroków koniec.

$$I(a) = \{ fg : g \in F(x) \}$$

↑ gcd

minimalizujący $f(a) = 0$

$f = f' f''$

$0 = f(a) = f'(a) f''(a)$

$$I(a) = \{ g : g(a) = 0 \}$$

$$= \{ fg : g \in F(x) \}$$

↑ minorant.

$f, f' \in I(a)$

$f' = fg$

$f = f' \cdot g' \Rightarrow \deg(f) = \deg(f')$

$g \cdot g'$ → stałe

$$I(a) = \{ f \cdot g : g \in F[x] \}$$

Wniosek 21.31. Rozszerzenie algebraiczne $\mathbb{F}\langle a\rangle$ jest izomorficzne z $\mathbb{F}[x]/_{\equiv_h}$, gdzie h generuje $I(a)$.

Wielomian z Lematu 21.30 to *wielomian minimalny* dla a nad $\mathbb{F}$.

Definicja 21.32. Jeśli $\mathbb{F}\langle a\rangle$ jest rozszerzeniem algebraicznym, to wielomian $f_a \in \mathbb{F}[x]$ nazywamy wielomianem minimalnym dla a (nad $\mathbb{F}$) jeśli $\bar{f}_a(a) = 0$ oraz dla każdego wielomianu $g \in \mathbb{F}[x]$ spełniającego $\bar{g}(a) = 0$ implikuje $f_a | g$.

Z Lematu 21.30 wynika, że wielomian minimalny istnieje (choć jest wyznaczony z dokładnością do stałej).

21.5 Wielomiany minimalne nad ciałami skończonymi

Twierdzenie 21.33 (Izomorfizm Frobeniusa). *Niech $\mathbb{F} \leq \mathbb{F}'$ będą ciałami skończonymi o $n = |\mathbb{F}|$ i $n' = |\mathbb{F}'|$ elementach.*

Wtedy przekształcenie $\varphi : \mathbb{F}' \to \mathbb{F}'$ dane jako

$$\varphi(x) = x^n$$

jest automorfizmem ciała $\mathbb{F}'$, co więcej, jest ono identycznością dokładnie na elementach ciała $\mathbb{F}$.

$n = p^k \qquad n' = p^{k'}$

$x \to x^p$ zachowuje działanie

$\mathbb{F}'$ $\qquad (a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^i \underset{\mathbb{F}'}{=} \binom{p}{0} b^p + \binom{p}{p} a^p$

$p \mid \binom{p}{i} = \frac{p!}{i!(p-i)!}$ $\qquad \binom{p}{p} = 1$

$p \neq i \neq 0$ $\qquad a^p + b^p$

$(a+b)^p = a^p + b^p$

$(ab)^p = a^p b^p$ homomorfizm

$\alpha \to \alpha^p$ hom.

$a \to a^{p^k}$ homomorfizm

$\varphi : \mathbb{F}' \xrightarrow{\text{homom.}} \mathbb{F}'$

$p^{k'} = p^k \cdot p^{(k'-k)}$

$\varphi^l(a) = a^{p^{(k'-k)}} = a^{\frac{p^{k'}}{p^k}}$

φ^l homomorfizm.

$id = \varphi^l \circ \varphi = \left(a^{p^k}\right)^{\frac{p^{k'}}{p^k}} = a^{p^{k'}}$

φ : stałe na $\mathbb{F}$

$a \to a^{p^{k'}}$ stałe na $\mathbb{F}'$

$\varphi^l \circ \varphi : \mathbb{F}' \to \mathbb{F}'$ $\qquad id$

$\to$ homomorfizm $\qquad \varphi$ - odwracalne bijekcja

Twierdzenie 21.34. *Niech $\mathbb{F} \leq \mathbb{F}'$ będą dwoma ciałami skończonymi o q, q' elementach i niech $\alpha \in \mathbb{F}' \setminus \mathbb{F}$.*

Wtedy minimalny wielomian dla α jest postaci

$$f_\alpha(X) = \prod_{j=0}^{r-1} (X - \alpha^{q^j}) \ ,$$

gdzie $r > 0$ jest minimalne takie, że $\alpha^{q^r} = \alpha$ w ciele $\mathbb{F}$.

Dowód. Sprawdźmy, że:

1. α jest pierwiastkiem f_α.
2. f_α ma jedynie pierwiastki jednokrotne
3. jest to wielomian o współczynnikach z $\mathbb{F}$;
4. jest nierozkładalny nad $\mathbb{F}$;

współczynniki wielomianu:
„jakiś wielomiany od pierwiastków"

- $x^2+ax+b=(x-\alpha)(x-\beta)$

$\alpha\beta=b$ $\quad(\alpha^p\beta^p)=b^p$

$-\alpha-\beta=a \Leftarrow -\alpha^p-\beta^p=(-\alpha-\beta)^p=a^p$

$f=\sum f_i x^i$

$\prod_{j=0}^{r-1}\left(x-\alpha^{q^{i+1}}\right)$

współczynniki $\quad \sum f_i^p x^i = \sum f_i x^i$

$f_i=f_i^p \Rightarrow f\in\mathbb{F}$

$f_\alpha \qquad g\mid f_\alpha \Rightarrow \deg(g)=\deg(f)$

$g(\alpha^{q^i})=0$

$\Rightarrow \alpha^{q^{i+1}}$ też jest pierw.

$g(\alpha^{q^0})=0 \Rightarrow g(\alpha^{q^i})=0$

$g=\sum g_i x^i \qquad g(\alpha^{q^j})$

$0=\left(\sum_{i=0}^{k} g_i\alpha^{q^j}\right)^q$

$=\sum g_i^q \alpha^{q^{j+1}}=\sum g_i\alpha^{q^{j+1}}=g(\alpha^{q^{j+1}})$

($g_i\in\mathbb{F}$, $g_i^q=g_i$)

$g(\alpha^{q^j})=0$

$\Downarrow$

$g(\alpha^{q^{j+1}})=0$

α est pièce g

$\Rightarrow \alpha^{q^0}, \alpha^{q^1}, \dots, \alpha^{q^{n-1}}$ sont pièce g

$\Rightarrow x - \alpha^{q^j}$ pièce g

$\Rightarrow \prod_{j=1}^{n-1} (x - \alpha^{q^j}) \mid g$

$\underbrace{\qquad\qquad}_{f}$

$f \mid g$