D BCH kódy a QR kódy

Připomeňme, že RS kód C dimenze k má prověrkovou matici $H = (\alpha^{ij})$, kde $0 \le j \le n-1$ a kde i probíhá od b do $b+d-2$, přičemž $d = n-k+1$. Průběh i se přitom chápe modulo n, takže za $i = n-1$ následuje $i = 0$. Prvek $\alpha \in \mathbb{F}_q$ je primitivní n-tou odmocninou z jedné.

Uvažme řádek $u = (1, \alpha^i, \alpha^{2i}, \ldots, \alpha^{(n-1)i})$ matice H. Vidíme, že jeho cyklický posun $(\alpha^{(n-1)i}, 1, \alpha^i, \ldots, \alpha^{(n-2)i})$ je roven $\alpha^{-i}u$, takže každý RS-kód je cyklický (platí vlastně i něco silnějšího – existuje prověrková matice, kde cyklické posunutí každého řádku je jeho lineárním násobkem). Přitom $a = \sum a_j x^j$ padne do C právě když pro každé i z daného (cyklického) intervalu je $\sum a_j \alpha^{ij} = 0$, čili α^i je kořenem a. Stupeň generujícího polynomu je roven dimenzi prověrkové matice (to platí v každém cyklickém kódu). Každý řádek matice H udává jeden kořen generujícího polynomu, takže ten musí být roven $(x-\alpha^b)\cdots(x-\alpha^{b+d-2})$.

Tvrzení D.1. *Ať C je $[n,k,d]_q$ RS kód s generující maticí (α^{ij}), kde i probíhá od b do $b+d-2$. Pak $C = C((x-\alpha^b)\cdots(x-\alpha^{b+d-2}))$ a $C^\perp = C((x-\alpha^{1-b})\cdots(x-\alpha^{k-b}))$.*

Důkaz. Prvou část tvrzení jsme již dokázali. Víme, že pro $C = C(g)$ je $C^\perp = C(h(x^{-1}))$, kde $gh = x^n - 1$. V našem případě se $x^n - 1$ rozkládá na $\prod_{i=0}^{n-1}(x-\alpha^i)$. Obecně platí, že jsou-li $\alpha_1, \ldots, \alpha_{d-1}$ kořeny g, musí mít h kořeny $\alpha_d^{-1}, \ldots, \alpha_n^{-1}$ tak, aby $\{\alpha_1, \ldots, \alpha_n\} = \{\alpha^i;\ 0 \le i < n\}$. Probíhá-li i od $1-b$ do $k-b = n-d+1-b$, tak $-i$ probíhá od $d+b-1$ do $b-1$. Proto je generující polynom kódu $C^\perp$ zvolen správně. □

Důsledek D.2. *Duální kód RS kódu je opět RS kód. Duální kód normalizovaného RS kódu je RS kód v užším smyslu, a naopak.*

Důkaz. Podle definice má normalizovaný RS kód generující polynom $(x-1)\cdots(x-\alpha^{n-k-1})$. Jeho duální kód má podle Tvrzení D.1 generující polynom $(x-\alpha^k)(x-\alpha^{k-1})\cdots(x-\alpha)$, což je generující polynom RS kódu v užším smyslu. Na základě Tvrzení D.1 je zřejmý i zbytek. □

Tvrzení D.3. *Ať C je BCH kód nad $\mathbb{F}_q$ určený RS-kódem s generujícím polynomem $(x-\alpha^b)\cdots(x-\alpha^{b+d-2})$, kde $\alpha \in \mathbb{F}_{q^s}$ je primitivní n-tá odmocnina z jedné. Pak C je cyklický kód nad $\mathbb{F}_q$ a $C = C(\mathrm{NSN}(m_{\alpha^b}, \ldots, m_{\alpha^{b+d-2}}))$.*

Důkaz. Polynom $a \in \mathbb{F}_q[x]_n$ leží v C, pokud hodnoty $a(\alpha^b), \ldots, a(\alpha^{b+d-2})$ jsou rovny nule. □

Charakterizace BCH kódů jejich nulami nám v konkrétních případech umožňuje dopočítat jejich přesnou dimenzi. Protože kodimenze je rovna stupni generujícího polynomu, stačí znát počet kořenů generujícího polynomu určeného Tvrzením D.3. Každý ireducibilní polynom s kořenem α^i má množinu všech kořenů shodnou s $\{\alpha^{iq^r};\ r \ge 0\}$. Proto je kodimenze kódu C rovna velikosti podmnožiny $\mathbb{Z}_n$,

která vznikne, jestliže ke každému $i \in \{b, \ldots, b+d-1\} \subseteq \mathbb{Z}_n$ přidáme (modulo n) všechny hodnoty iq^r, $r \geq 0$.

Další významnou třídou kódů, kterými se budeme zabývat, jsou takzvané QR-kódy, kde QR je zkratkou od Quadratic residue (kvadratický zbytek).

Tyto kódy jsou binární a definují se pro lichou prvočíselnou délku n. Zvolíme nějakou primitivní n-tou odmocninu z jedné a označíme ji α. Víme, že $x^n - 1 = (x-1)\prod_{i=1}^{n=1}(x-\alpha^i)$. Grupu $\mathbb{Z}_n^* = \{i;\, 1 \leq i \leq n-1\}$ můžeme vyjádřit jako disjuktní sjednocení $R \cup S$, kde $i \in R$ právě když $i = j^2$ pro nějaké $j \in \mathbb{Z}_n^*$, tedy když i je kvadratický zbytek modulo n. Těchto zbytků je $(n-1)/2$, takže polynomy

$$g_0 = \prod_{i \in R}(x - \alpha^i) \text{ a } g_1 = \prod_{i \in S}(x - \alpha^i)$$

jsou stupně $(n-1)/2$ a splňují $x^n - 1 = (x-1)g_0g_1$.

Pro n-tou odmocninu z jedné platí, že je kořenem polynomu $g_0(x^j)$, kde $jj' \equiv 1 \bmod n$, právě když je tvaru $\alpha^{ij'}$, $i \in R$. Proto $g_0(x^j) \equiv \prod(x - \alpha^{ij'}) \bmod x^n - 1$, takže

$$g_0(x^j) \equiv g_0 \text{ pro } j \in R \text{ a } g_0(x^j) \equiv g_1 \text{ pro } j \in S.$$

Z $g_0 \in \mathbb{F}_2[x]$ plyne $g_1 \in \mathbb{F}_2[x]$, a pak jsou kódy $C(g_0)$ a $C(g_1)$, jak vidíme, permutačně ekvivalentní. Aby g_0 leželo v $\mathbb{F}_2[x]$, musí být jeho kořeny uzavřeny na Frobeniův automorfismus. Jinými slovy, je-li α kořen g_0, musí být i α^2 také kořenem g_0. To nastane právě když $2 \in R$, což platí právě když $n \equiv \pm 1 \bmod 8$.

Dále budeme uvažovat pouze případ, kdy n je prvočíslo tvaru $8\ell - 1$ nebo $8\ell + 1$. Za QR kód budeme považovat cyklický kód $C(g_0)$. Ten je ovšem závislý na volbě α – při jiné volbě α dostaneme $C(g_1)$. To je určitá formální nedůslednost, která však nevede k obtížím, neboť $C(g_0)$ a $C(g_1)$ jsou permutačně ekvivalentní. Je zřejmé, že vždy jde o $[n, (n+1)/2]$ kód, neboť g_0 je stupně $(n-1)/2$.

Rozšířeným QR-kódem $\bar{C}$ budeme rozumět rozšíření QR kódu o bit paritní kontroly. Vidíme, že $\bar{C}$ je $[n+1, (n+1)/2]$ kód.

Tvrzení D.4. *Rozšířený QR kód je samoduální právě když* $n \equiv -1 \bmod 8$.

Důkaz. Ze vztahu $C((x+1)g_0) = C(x+1) \cap C(g_0)$ plyne, že $C((x+1)g_0)$ je v $C(g_0)$ podprostor indexu 2 (jinými slovy, $C((x+1)g_0)$ je nadrovinou $C(g_0)$). Přidávaný paritní bit je roven nule právě když kódové slovo leží v $C((x+1)g_0)$, protože $C(x+1)$ se skládá právě ze všech slov sudé váhy.

Všechna kódová slova $\bar{C}$ musí být proto po odstranění přidaného paritního bitu kolmá na všechny vektory $C((x+1)g_0)$. To vlastně znamená $C(g_0) \subseteq C((x+1)g_0)^\perp$, což z důvodů dimenze je totéž jako $C(g_0) = C((x+1)g_0)^\perp$. Z $x^n - 1 = (x+1)g_0g_1$ plyne, že kód $C((x+1)g_0)^\perp$ je generován polynomem $g_1(x^{-1})$. Tento kód má být roven $C(g_0)$, což znamená, že $g_0(x)$ a $g_1(x^{-1})$ mají mít stejné kořeny. To ovšem nastane právě pro $-1 \in S$. Víme, že -1 je

nečtverec modulo n právě když $n \equiv 3 \bmod 4$. Podmínka dokazovaného tvrzení je tedy nutná.

Uvažme nyní kódová slova $u, v \in C(g_0)$ a označme $\bar{u}$ a $\bar{v}$ jejich rozšíření o paritní bit. Předpokládejme, že $n \equiv -1 \bmod 8$, tedy že $C((x+1)g_0)^\perp = C(g_0)$. Pokud u nebo v padne do $C((x+1)g_0)$, tak z nulovosti paritního bitu plyne $\bar{u} \cdot \bar{v} = u \cdot v = 0$. Ať $u, v \in C(g_0) \setminus C((x+1)g_0)$. Pak $\bar{u} \cdot \bar{v} = u \cdot v + 1$, takže potřebujeme dokázat $u \cdot v = 1$.

Protože neplatí $\langle u \rangle \subseteq C(g_0)^\perp$, tak neplatí ani $C(g_0) \subseteq \langle u \rangle^\perp$. To znamená, že nadrovina $\langle u \rangle^\perp$ vytíná v $C(g_0)$ také nadrovinu. Tato nadrovina je rovna $C((x+1)g_0)$, neboť $C((x+1)g_0) = C(g_0)^\perp \subseteq \langle u \rangle^\perp$. Tudíž $v \notin \langle u \rangle^\perp$, a proto $u \cdot v = 1$. □

Parita kódových slov cyklických kódů respektuje operace sčítání a násobení polynomů. Pro $a \in \mathbb{F}_2[x]$ počet nenulových koeficientů označíme (na chvíli) $|a|$. Máme $|a| \equiv a(1) \bmod 2$, a proto je $a \mapsto |a| \bmod 2$ homomorfismem $\mathbb{F}_2[x] \to \mathbb{F}_2$. Jeho jádrem je ideál $(x+1) \supseteq (x^n+1)$, a proto $a \mapsto |a| \bmod 2$ je i homomorfismem $\mathbb{F}_2[x]_n \to \mathbb{F}_2$.

Ze vzorce pro násobení polynomů $ab = \sum a_i b_j x^{i+j}$, kde $a = \sum a_i x^i$ a $b = \sum b_j x^j$, vyplývá $|ab| \leq |a| \cdot |b|$. Tento vztah platí nad libovolným tělesem F, nejen nad $\mathbb{F}_2$. Také samozřejmě platí i pro okruh $F[x, x^{-1}]$.

Pokud $b = a(x^{-1})$, tak v součinu ab figurují členy $a_i a_i x^{i-i} = a_i^2$. Z počtu $|a| \cdot |b|$ nenulových součinů $a_i b_j$ jich pak $|a|$ dává $a_i a_i x^{i-i} = a_i^2 x^0$. Proto

$$|a(x) \cdot a(x^{-1})| \leq |a|^2 - |a| + 1.$$

Tyto jednoduché úvahy tvoří základ důkazu následujícího pozorování.

Lemma D.5. *Ať je $a \in C(g_0)$ a ať $d = |a|$ je liché. Potom $d^2 \geq n$. Je-li $n \equiv 7 \bmod 8$, tak dokonce $d^2 - d + 1 \geq n$.*

Důkaz. Polynomy $C(g_0)$ a $C(g_1)$ jsou permutačně ekvivalentní. Proto v $C(g_1)$ existuje kódový polynom b, který je také váhy d. Polynom ab je násobek polynomu $g_0 g_1 = 1 + x + x^2 + \cdots + x^{n-1}$. Kód $C(1 + \cdots + x^{n-1})$ se skládá ze dvou kódových slov, nenulové z nich je rovno $w = (1, \ldots, 1)$. Víme, že $|\pi_n(ab)| \equiv |a| \cdot |b| \bmod 2$. Tudíž $|\pi_n(ab)| \equiv d^2 \equiv 1 \bmod 2$, takže $\pi_n(ab) = w$. Polynom ab má tedy alespoň n nenulových koeficientů, a proto $d^2 \geq n$.

V případě $n \equiv -1 \bmod 8$ je $C(g_1)$ generováno $g_0(x^{-1})$, takže za b lze zvolit $a(x^{-1})$. Z toho plyne odhad $d^2 - d + 1 \geq n$. □

Odhady $d^2 \geq n$ a $d^2 + d - 1 \geq n$ lze použít jako odhady minimální vzdálenosti QR kódu $C(g_0)$, pokud se podaří ověřit:

Lemma D.6. *Minimální váha QR-kódu je lichá.*

Podrobný důkaz tohoto lemmatu zde provádět nebudeme a omezíme se na jeho hlavní myšlenku. Pracuje se s rozšířeným kódem $\bar{C}$, o kterém se dokáže, že jeho grupa automorfismů je tranzitivní (automorfismy jsou zde permutační ekvivalence kódu $\bar{C}$ sama se sebou). To znamená, že pro libovolná $i, j \in \{1, \ldots, n+1\}$ existuje $\varphi \in S_{n+1}$ takové, že $\varphi(i) = j$ a současně $(u_{\varphi(1)}, \ldots, u_{\varphi(n+1)}) \in \bar{C}$ kdykoliv $(u_1, \ldots, u_{n+1}) \in \bar{C}$. Je-li $(u_1, \ldots, u_n) \in C(g_0)$ slovo minimální váhy, a ta je sudá, zvolíme φ tak, aby $\varphi(n+1) = i$, kde $u_i = 1$. Ze sudosti váhy plyne $u_{n+1} = 0$, takže $(u_{\varphi(1)}, \ldots, u_{\varphi(n+1)})$ má na prvých n pozicích váhu o jedničku menší, což je spor s volbou $(u_1, \ldots, u_n)$.

Ze vztahu $d^2 - d + 1 \geq n$ a informace, že d je číslo liché, dostáváme pro $n = 7$ odhad $d \geq 3$ a pro $n = 23$ odhad $d \geq 7$. Z důvodů Hammingovy nerovnosti musí platit $d = 3$ a $d = 7$. Vidíme, že základní Hammingův kód a perfektní binární Golayův kód je možné získat jako QR kódy, a tedy jako kódy cyklické.