Szegedi Tudományegyetem

Bolyai Intézet

Geometria Tanszék

QR kódok matematikája

BSc szakdolgozat

Készítette:
Dobi Krisztina
matematika szakos
hallgató

Témavezető:
Dr. Nagy Gábor Péter
egyetemi tanár

Szeged
2019

Tartalomjegyzék

Bevezetés

A "kód" szót több értelemben használhatjuk, többféle célt szolgálhatnak. Az egyik fajtája a vonalkód. A vonalkód egy számokból és betűkből álló azonosító kódolt formája, amely gépekkel optikailag leolvasható. A vonalkód kizárólag egy azonosítót, hivatkozást jelöl, amely egy adatbázis meghatározott elemére mutat. Léteznek egy-, illetve kétdimenziós vonalkódok. A kétdimenziós vonalkódok jóval nagyobb információmennyiség megjelenítésére képesek, mint az egydimenziós kódok. Az adatok megjelenítésére különböző geometriai formákat használnak, amelyek több irányból is könnyedén leolvashatóak.

A QR-kód (Quick Response-kód) egy kétdimenziós vonalkód (tulajdonképpen pontkód), amit a japán Denso-Wave cég fejlesztett ki 1994-ben. A cég a Toyota egyik leányvállalata volt és eredetileg a járművek nyomon követésére és az alkatrészek nagy sebességű letapogatására találták ki. Nevét az angol Quick Response (=gyors válasz) rövidítéséből kapta, egyszerre utalva a gyors visszafejtési sebességre és a felhasználó által igényelt gyors reakcióra. Nemcsak 100-szor annyi adatot tárol, mint az egydimenziós vonalkód, hanem digitálisan is beolvasható. A QR-kódok szöveges információt tartalmaznak karakterek, betűk és számok formájában. A QR-kód egy négyzetes mátrix, amely fekete-fehér négyzetek blokkjából áll, amelyek bináris formában reprezentálják a kódolt adatokat. A négy sarkából háromban speciális jelölő jelzi a tájolást.

A kódok egy másik fajtája felhasználható arra, hogy az adatok védelmét növelje átvitel vagy tárolás közben előálló sérülés ellen. Ezeket a "kódokat" nevezik hibafelismerő és javító kódoknak és általában valamilyen redundáns információ hozzáadásával működnek. Ilyen kódok például a Hamming-kódok, a Reed–Solomon-kódok, BCH-kódok. Ezeket a kódokat gyakran a véletlen hibák vagy a csomósodó hibák felismerésére (és javítására) optimalizálják. A csomósodó hibák azt jelentik, hogy például egy kódszón vagy kódolt blokkon belül több bit sérül, azaz vagy nem lehet megmondani, hogy 0 vagy 1 értékű, vagy 0 1-re és fordítva változik. A QR-kódban szereplő adatokat hibajavító kód védi. Ez tolerálja a kód akár 30 %-ának elvesztését azaz, hogy akkor még dekódolható marad. A dekódolást speciális szkenner-eszközök segítségével végzik el.

A QR-kód a Reed–Solomon kódolást használja hibajavításra. A Reed-Solomon-kódokat Irving S. Reed és Gustave Solomon találták fel 1960-ban. Ez az egyik legjobb hibajavító kód, mert a kód elemei a lehető "legtávolabb" vannak egymástól, ami a dekódolás lehetőségeit növeli. Az ilyen kódokat MDS (maximal distance separable) kódoknak nevezzük. Dolgozatomban a QR-kódok működését mutatom be.

A QR-kód használata egyre szélesebb körű. Használják az iparban, logisztikában, de igazi népszerűségét a marketing alkalmazásokban és a mobiltelefonos megoldásokban érte le. Sajátosságai miatt alkalmas postai címek, telefonszámok, internetcímek, sőt akár GPS koordináták tárolására. A QR-kódok olvasásához a telefonra különböző alkalmazásokat lehet letölteni, bár a legtöbb új telefon már rendelkezik saját QR-kód olvasó szoftverrel, amely nagyban megkönnyíti a QR-kódok beolvasását, mentését és különféle felhasználását.

1. Alapfogalmak

1.1. Algebra

1.1. Definíció. *Legyen $(G;\cdot)$ egy csoport. Ha H nemüres részhalmaza G-nek és*

- *H zárt a műveletre,*
- *H tartalmazza G egységelemét,*
- *H zárt az inverzképzésre,*

akkor a $(H;\cdot)$ algebrát a $(G;\cdot)$ csoport részcsoportjának nevezzük, azaz $H \subseteq G$, ha $1 \in H$ és $\forall h_1, h_2 \in H : h_1 \cdot h_2, h_1^{-1} \in H$.

1.2. Definíció. *Legyen G egy csoport és $A \subseteq G$. Az A halmaz által generált részcsoport a legszűkebb olyan részcsoport, amely tartalmazza A-t:*

$$[A] = \bigcap_{A \subseteq H \leq G} H.$$

1.3. Definíció. *Egy G csoportot ciklikusnak nevezünk, ha egy alkalmas g elemének az egész kitevőjű hatványaiból áll. Az ilyen g elemeket a G generátorelemeinek (ritkán primitív elemeinek) nevezzük, azaz a g elem generálja a G csoportot. Minden ciklikus csoport kommutatív, hiszen egy elem hatványai egymással felcserélhetők.*

1.4. Lemma. *Ciklikus csoport minden részcsoportja is ciklikus.*

1.5. Definíció. *Az $(A;+,\cdot)$ algebrai struktúrát gyűrűnek nevezzük, ha $(A;+)$ Abel-csoport, $(A;\cdot)$ félcsoport és $a \cdot$ disztributív az $+$-ra nézve, azaz $\forall a, b, c \in A$-re: $a \cdot (b + c) = (a \cdot b) + (a \cdot c), (a + b) \cdot c = (a \cdot c) + (b \cdot c)$.*

Az $(A;+)$ Abel-csoportot a gyűrű additív csoportjának, az $(A;\cdot)$ félcsoportot a gyűrű multiplikatív félcsoportjának nevezzük.

1.6. Definíció. *A $(T;+,\cdot)$ algebrai struktúrát testnek nevezzük:*

- *ha a $(T;+)$ Abel-csoport és a $(T\backslash\{0\};\cdot)$ csoport, ahol a 0 a $(T;+)$ csoport egységeleme és zéruselemnek nevezzük.*
- *Az összeg disztributív a szorzásra nézve.*

1.7. Definíció. *Egy T testet véges testnek nevezünk, ha $|T| < \infty$.*

1.8. Definíció. *Egy $n \in \mathbb{Z}$ esetén $\mathbb{Z}_n$-et a következőképpen definiáljuk:*
A modulo n kongruenciareláció egy ekvivalenciareláció ($a \equiv b \pmod{n} \Leftrightarrow n \mid b-a$), és így meghatároz egy osztályozást $\mathbb{Z}$-n. Továbbá ez a reláció kompatibilis az alapműveletekkel, azaz:

$$a \equiv b \textbf{ és } c \equiv d \Rightarrow a+c \equiv b+d \textbf{ és } a \cdot c \equiv b \cdot d.$$

Ezért a műveletek jól értelmezettek az ekvivalenciaosztályok halmazán. Az ekvivalenciaosztályokat maradékosztályoknak nevezzük és mivel elég egy reprezentánst választani, adott n esetén a halmazukat így definiáljuk:

$$\mathbb{Z}_n = \{0, 1, ..., n-1\}.$$

1.9. Állítás. *Minden $n \geq 2$ egész szám esetén a modulo n maradékosztályok egységelemes kommutatív gyűrűt alkotnak, amit $\mathbb{Z}_n$ jelöl.*

1.10. Tétel. *A $(\mathbb{Z}_p;+,\cdot)$ gyűrű pontosan akkor test, ha p prím.*

1.11. Megjegyzés. *Jelölje $\mathbb{Z}_p = \mathbb{F}_p$ prímtestet. Minden véges test rendje prímhatvány. Ha a rend $q = p^n$, p prím, akkor $\mathbb{F}_q$-t az $\mathbb{F}_p$ magasabb fokú algebrai bővítményeként kapjuk meg. Bármely véges testben a multiplikatív csoport ciklikus.*

1.12. Definíció. *Tetszőleges T test esetén a*

$$T[x] = \{a_0 + a_1x + a_2x^2 + \cdots + a_nx^n | n \in \mathbb{N}, a_n \neq 0, a_i \in T, \forall i = 0, \ldots, n\}$$

halmazt a T test feletti polinomgyűrűnek, elemeit pedig polinomoknak nevezzük. Egy $p \in T[x]$ polinom esetén:

$$p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n = \sum_{i=0}^{n} a_ix^i.$$

Ekkor az $n \in \mathbb{N}$-et p fokának nevezzük, azaz $\deg p = n$ és az a_i-k a p együtthatói. Ha $p(x) \equiv 0$, akkor $\deg p = -\infty$.

1.13. Definíció. *Legyen* $(T; +, \cdot)$ *test,*

$$p(x) = \sum_{i=0}^{n} a_i x^i,\ q(x) = \sum_{j=0}^{m} b_j x^j \in [T]$$

és $\lambda \in T$ *ekkor* $p(x) = q(x)$*, ha* $p_i = q_i\ \forall i$*-re.*
Műveletek polinomok között:

1. *Polinomok összeadása:* $r(x) = p(x) + q(x)$ *tagonként történik* T *feletti műveletekkel:* $r_i = p_i + q_i$*. Nyilvánvalóan*

$$\deg r(x) \leq \max\{\deg p(x), \deg q(x)\}.$$
$$(p+q)(x) = \sum_{k=0}^{\max\{n,m\}} (a_k + b_k)x^k$$

2. *Polinomok szorzása:* $r(x) = p(x)q(x)$ *minden tagot minden taggal szorzunk, majd az azonos fokú tagokat csoportosítjuk:*

$$c_i = \sum_{j=0}^{\min\{i,\deg p(x)\}} p_j \cdot q_{i-j}.$$

Nyilván

$$\deg r(x) = \deg p(x) + \deg q(x).$$
$$\lambda p(x) = \sum_{i=0}^{n} \lambda a_i x^i$$

1.14. Tétel. ***(Euklideszi osztás polinomokra)*** *Adott* $a(x)$ *és* $d(x) \neq 0$ *esetén egyértelműen létezik olyan* $q(x), r(x)$ *úgy, hogy*

$$a(x) = g(x)d(x) + r(x),$$

és $\deg r(x) < \deg d(x)$*.*

1.15. Definíció. $r(x)$*-et az* $a(x)$*-nek* $d(x)$*-re vonatkozó maradékának nevezzük. Jelölés:*

$$r(x) \equiv a(x) \pmod{d(x)}.$$

1.16. Definíció. *A* $d(x)$ *osztja* $a(x)$*-et, ha* $a(x) \pmod{d(x)} = 0$*. Jelölés:*

$$d(x) | a(x)$$

1.17. Definíció. *Egy $b \in GF(q)$ gyöke az $a(x)$ polinomnak, ha $a(b) = 0$.*

1.18. Tétel. *Ha c az $a(x)$ gyöke, akkor az előáll a következő alakban:*

$$a(x) = b(x)(x - c).$$

1.19. Tétel. *Egy k-adfokú polinomnak legfeljebb k gyöke lehet.*

1.20. Definíció. *Egy $\alpha \in GF(q)$-t a $GF(q)$ primitív elemének nevezzük, ha α multiplikatív rendje $q - 1$.*

1.21. Tétel. *Minden $GF(q)$-ban létezik primitív elem.*

1.2. Kódelmélet

Legyen q prímhatvány és jelölje $GF(q)$ a q elemszámú véges testet. Legyen a küldő által továbbított üzenet c, amely a $V = (GF(q))^n$ vektortér egy eleme. Legtöbb esetben $q = 2$, vagyis az üzenet egy n hosszúságú bináris sorozat. Csak az olyan hibák javításával foglalkozunk, melyek a szimbólumok megváltozásából adódnak. A probléma tehát a következő: a továbbítás során c-hez hozzáadódik egy e hibavektor, s így a fogadó a $v = c + e$ módosult üzenetet kapja. Célunk a v dekódolása, azaz a hibavektor, majd pedig c meghatározása.

$$\text{forrás} \xrightarrow{u} \text{kódoló} \xrightarrow{c} \text{csatorna} \xrightarrow{v} \text{dekódoló} \xrightarrow{v'} \text{nyelő}$$

A hibajavító kódolás alapvető módszereit az előbbi ábrán látható egyszerű hírközlési struktúra kapcsán vizsgáljuk.

Az u és u' vektorok koordinátái egy F halmazból veszik értékeiket, amely halmazt forrásábécének nevezzük. A kódoló a k hosszú u vektort (az üzenetet) egy n hosszú c vektorba (a kódszóba) képezi le. A c koordinátái egy Q halmazból veszik értékeiket. A Q-t kódábécének vagy csatorna bemeneti ábécének nevezzük. A csatorna kimenete v, szintén egy n hosszú vektor, melynek koordinátái szintén Q-beliek. Az előbbi esetben $Q = GF(q)$.

1.2.1. Vektortér, kód, lineáris kód

1.22. Definíció. *A V nemüres halmazt a T test feletti vektortérnek nevezzük, ha $+ : V^2 \to V$ és $\cdot : T \times V \to V$, amelyek eleget tesznek az alábbi axiómáknak $\forall \underline{u}, \underline{v}, \underline{w} \in V$ és $\lambda, \mu \in T$ esetén:*

1. *$(V, +, 0)$ Abel-csoport,*

2. $(\lambda + \mu)\underline{u} = \lambda\underline{u} + \mu\underline{u}$ *és* $\lambda(\underline{u} + \underline{v}) = \lambda\underline{u} + \lambda\underline{v}$,

3. $1\underline{u} = \underline{u}$ *és* $(\lambda\mu)\underline{u} = \lambda(\mu\underline{u})$.

1.23. Definíció. *Legyen $Q = \mathbb{F}_q$ véges halmaz, $n \in \mathbb{N}$. $C \subseteq Q^n$: Q ábécé, C egy n hosszú kód a Q ábécé felett. Ha $q = 2$, akkor C-t bináris kódnak nevezzük. A C kód elemei a kódszavak.*

1.24. Definíció. *A C kód blokk-kód, ha minden kódszava ugyanolyan hosszú.*

1.25. Definíció. *Legyen V vektortér, $U \subseteq V$ lineáris altér V-ben, ha $U \neq \emptyset$ és zárt a V-ben definiált összeadásra és szorzásra, jelölés: $U \leq V$.*

1.26. Definíció. *Egy C kód lineáris, ha a C halmaza lineáris tér, azaz ha C zárt az összeadásra és a skalárral vett szorzásra.*

1.27. Következmény. *A lineáris kód definíciójából következik, hogy a $\underline{0}$ vektor eleme minden lineáris kódnak, vagyis minden lineáris kód esetén a $\underline{0}$ kódszó.*

1.28. Definíció. *A $g_1, g_2, g_3, \ldots, g_j \in C$ vektorok lineárisan függetlenek, ha $\alpha_i \in GF(q)$ mellett*

$$\sum_{i=1}^{j} \alpha_i g_i = 0$$

csak úgy állhat elő, ha $\alpha_i = 0 \quad \forall i = 1, 2, \ldots, j$-re. Lineárisan függők, ha nem függetlenek.

1.29. Definíció. *A $g_1, g_2, \ldots, g_k \in C$ vektorok a C lineáris tér egy bázisát alkotják, ha lineárisan függetlenek, továbbá igaz az, hogy minden $c \in C$ vektor előállítható*

$$c = \sum_{i=1}^{k} u_i g_i$$

alakban, ahol $u_i \in \{0, 1\}$ minden $i = 1, 2, \ldots, k$-ra.

1.30. Definíció. *A $C \subset V$ kód lineáris, ha C lineáris altere a V vektortérnek. Ha C dimenziója k, akkor lineáris $[n, k]$-kódnak nevezzük.*

Ha $c_1, c_2, \ldots, c_k$ a C egy bázisa, akkor azt a $k \times n$-es G mátrixot, melynek i-edik sora a c_i vektor $(i = 1, 2, \ldots, k)$, C generátor mátrixának nevezzük.

1.31. Definíció. *Egy (n,k) paraméterű lineáris kód szisztematikus, ha minden kódszavára igaz, hogy annak utolsó $n-k$ szimbólumát elhagyva éppen a neki megfelelő k hosszúságú üzenetet kapjuk, más szavakkal a k hosszú üzenetet egészítjük ki $n-k$ karakterrel.*
Szisztematikus kód esetén a generátormátrix is egyértelmű, mégpedig

$$G = (I_k, B)$$

alakú, ahol I_k a $k \times k$ méretű egységmátrix, B pedig $k \times (n-k)$ méretű mátrix. Az u üzenethez tartozó c kódszó szerkezete tehát:

$$c = (u_1, u_2, \cdots, u_k, c_{k+1}, c_{k+2}, \cdots, c_n).$$

A c első k koordinátájából álló szegmensét üzenetszegmensnek, az utolsó $n-k$ koordinátájából állót paritásszegmensnek nevezzük.

1.32. Definíció. *Ha egy $n-k$ sorból és n oszlopból álló*

$$H = (A, I_{n-k})$$

mátrixra, ahol I_{n-k} az $(n-k) \times (n-k)$ méretű egységmátrix, A pedig $(n-k) \times k$ méretű mátrix,

$$Hc^T = 0$$

akkor és csak akkor, ha $c \in C$, akkor H-t a C kód paritásellenőrző mátrixának nevezzük. Minden lineáris kódnak van paritásellenőrző mátrixa. Az előbbi egyenletet paritásegyenletnek nevezzük.

1.33. Tétel. *Ha G és H ugyanazon C lineáris kód generátormátrixa illetve paritásellenőrző mátrixa, akkor*

$$HG^T = 0.$$

1.2.2. Hamming-távolság, Hamming-súly, minimális távolság, gömb

1.34. Definíció. *Legyen $\underline{v} = (v_1, v_2, \ldots, v_n)$, $\underline{u} = (u_1, u_2, \ldots, u_n) \in \mathbb{F}_q^n = V$. A két vektor Hamming-távolsága azon koordináták száma, amelyekben $\underline{v}$ és $\underline{u}$ eltér egymástól, azaz*

$$d_H(\underline{v}, \underline{u}) = |\{i : 1 \leq i \leq n, v_i \neq u_i\}|.$$

1.35. Állítás. *Az $\mathbb{F}_q^n$ vektortéren a d_H leképezés metrika, azaz $\forall \underline{x}, \underline{y}, \underline{z} \in \mathbb{F}_q^n$ esetén:*

- $d_H(\underline{x}, \underline{y}) \geq 0$ *és* $d_H(\underline{x}, \underline{y}) = 0 \Leftrightarrow \underline{x} = \underline{y}$,
- $d_H(\underline{x}, \underline{y}) = d_H(\underline{y}, \underline{x})$,
- $d_H(\underline{x}, \underline{y}) + d_H(\underline{y}, \underline{z}) \geq d_H(\underline{x}, \underline{z})$.

1.36. Definíció. *A c sorozat küldésekor és a v sorozat vételekor a hibák száma* $t = d_H(c, v)$. *Ezt az esetet nevezzük egyszerű hibázásnak, amikor a hiba helye és értéke egyaránt ismeretlen.*

1.37. Definíció. *Az olyan hibázást, amikor tudjuk, hogy egy pozícióban hiba lehet, tehát a hiba helyét ismerjük csak a hiba értékét nem, törléses hibának nevezzük.*

1.38. Definíció. *A* $\underline{v} \in V$ *vektor Hamming-súlyán a* $d(\underline{0}, \underline{v})$ *távolságot értjük, jele:* $|\underline{v}|$ *vagy* $w_H(\underline{v})$, *azaz:*

$$|\underline{v}| = w_H(\underline{v}) = d_H(\underline{0}, \underline{v}) = |\{i \mid v_i \neq \underline{0}\}|.$$

1.39. Definíció. *Egy C kód minimális súlyán a*

$$w_{min} = \min w(c), \quad ahol\ c \neq 0, c \in C$$

számot értjük.

1.40. Definíció. *A*

$$d(C) = min\{d_H(\underline{v}, \underline{u}) \mid \underline{v}, \underline{u} \in C, \underline{v} \neq \underline{u}\}$$

számot a C kód minimális távolságának nevezzük.

1.41. Lemma. *Egy C lineáris kód minimális távolsága megegyezik a legkisebb súlyú nemnulla vektorának a súlyával, azaz*

$$d = w_{min}.$$

1.42. Lemma. *Ha H egy lineáris C kód paritásellenőrző mátrixa, akkor H azon oszlopainak minimális száma, melyek lineárisan függők,* $d = d(C)$ *minimális távolság.*

Bizonyítás. H oszlopai:

$$H = (a_0^T, a_1^T, \ldots, a_{n-1}^T),$$

akkor a paritásegyenlet $c = (c_0, c_1, \ldots, c_{n-1})$ jelöléssel:

$$c_0a_0 + c_1a_1 + \cdots + c_{n-1}a_{n-1} = 0.$$

Ezt az egyenletet csak olyan nemnulla c vektorok (kódszavak) elégíthetik ki, melyek súlya legalább w_{min}, ilyen súlyú viszont van, tehát a lineárisan függő oszlopok száma w_{min} , amely éppen d. □

1.43. Definíció. *Legyen $c \in V$ középpontú $r \in \mathbb{R}^+$ sugarú gömbnek nevezzük a*

$$B_r(c) = \{\underline{v} \in V : d_H(c, \underline{v}) \leq r\}$$

halmaz elemeit.

1.2.3. A t-hibajavító kód, Singleton-korlát, MDS kód

1.44. Definíció. *Legyen t pozitív egész. A V vektortér $C \subset V$ részhalmazát t-hibajavító kódnak nevezzük, ha $\forall\, \underline{v}, \underline{u} \in C$ esetén:*

$$d_H(\underline{v}, \underline{u}) \geq 2t + 1.$$

1.45. Lemma. *Az n, k, d paraméterekkel rendelkező lineáris kód, ahol n a kód hossza, k a dimenziója és d a kód minimális távolsága, képes kódszavanként $\lfloor \frac{d-1}{2} \rfloor$ hibát kijavítani.*

1.46. Lemma. *Ha C t-hibajavító kód, akkor tetszőleges $\underline{v} \in V$ vektorhoz legfeljebb egy olyan $c \in C$ kódszó létezik, amelyre $d(c, \underline{v}) \leq t$.*

Bizonyítás. Legyen C t-hibajavító kód. Indirekt tegyük fel, hogy létezik két különböző $c, c' \in C$ vektor, melyekre $d(c, \underline{v}) \leq t$ és $d(c', \underline{v}) \leq t$. A háromszög-egyenlőtlenségből ekkor azt kapjuk, hogy $d(c, c') \leq 2t$. Ami ellentmondás, hiszen $d(c, c') \geq 2t + 1$. □

1.47. Megjegyzés. *Mivel C t-hibajavító kód, így a háromszög-egyenlőtlenségből következik, hogy a kódszavak körüli t sugarú gömbök diszjunktak, ami éppen állításunk megfogalmazása.*

Tehát ha a küldő kódszavakat továbbít és maximum t hiba lép fel, akkor a fogadó ki tudja javítani, dekódolni tudja az üzenetet. Hiszen a kapott hibás üzenet pontosan egy kódszó köré írt t sugarú gömbben lesz benne, melynek középpontja az eredeti üzenet.

1.48. Definíció. *Az olyan t-hibajavító kódot, amelyre teljesül, hogy $\forall\, v \in V$-hez létezik legfeljebb t távolságra lévő kódszó, perfekt kódnak nevezzük.*

1.49. Tétel. *(Singleton-korlát) Ha valamely C lineáris $[n, k]$-kód minimális távolsága d, akkor*

$$d \leq n - k + 1.$$

1.50. Definíció. *Ha egy lineáris $[n,k]$-kód minimális távolsága d és teljesül a*

$$d = n - k + 1$$

egyenlőség, akkor a kódot MDS kódnak nevezzük.

2. A QR-kódok

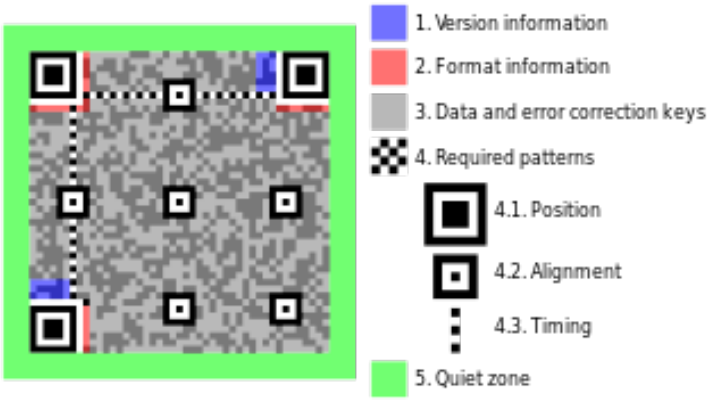
2.1. A QR-kódok szerkezete

A QR-kód szerkezetét az 1. ábra mutatja be. A QR-kódot egy kétdimenziós digitális képérzékelő érzékeli, majd a programozott processzor digitálisan elemzi. A QR-kód jó tulajdonsága, hogy bármilyen irányból készülhet róla fénykép vagy szkennelt kép, nem kell törődni a kód helyes tájolásával. Ez azért lehetséges, mert a kód megfejtésére, dekódolására szolgáló programok a három sarokban elhelyezett jellegzetes, minden QR-kódban azonos minta alapján el tudják dönteni, hogy milyen irányban kell a kód pontjait értelmezni, feldolgozni, még akkor is, ha a kódbélyegről készült kép teljesen ferde. Ezek teszik lehetővé azt is, hogy a beolvasási folyamatot gyorsabban kezdje. Ezek a helyzetet meghatározó jelek stabil és nagy sebességű olvasást biztosítanak és segítenek a háttérzavarok elnyomásában.

A hiba vagy torzulás itt azt jelenti, hogy a kódbélyeg lefényképezésekor sokszor nem sikerül a mintázatot teljes pontossággal rögzíteni. A hibajavítás, tehát a hibák ellenére a kód tartalmának hibátlan kiolvasása úgy lesz lehetséges, hogy a kódba annak előállításakor már belefoglaltak olyan kiegészítő jelzéseket is, amelyek segítségével a dekódoló program bizonyos mértékű torzulást még képes tolerálni. Hogy ennek a jeltorzulásnak mikor mekkora a megengedett legnagyobb mértéke, a kód előállításához használt, szabványosított módszerek megválasztásán múlik és ezt a kód elkészítésekor döntheti el a felhasználó, a használt program lehetőségein belül.

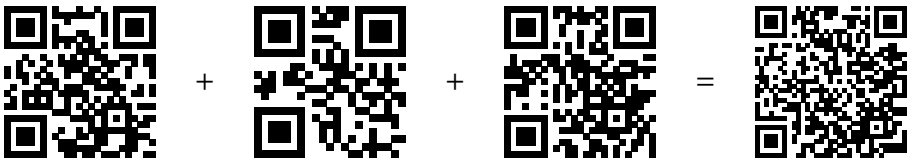
A kód tartalmazza a verzióinformációt (1.) azaz, a használt kód változatát és a formátuminformációt (2.), amellyel a szkenner meghatározza az alkalmazott adatformátumot. A (3.) adatrész tartalmazza a kódolt adatokat és a hibakorrekciós kulcsokat. A kód megfejtésének könnyítésére csak három sarokban tartalmaz egy sajátos mintát (4.1.). A jobb alsó sarokból hiányzó jellegzetes mintáról az olvasó felismeri a tájolást. A kód méretének növekedésével a (4.2.) minták hozzáadásával segítik annak meghatározását, hogy a kód képének perspektívája torzul-e vagy sem, normalizálják a képet a méret, a tájolás és a látószög szempontjából. Minél nagyobb a

1. ábra. A QR-kód szerkezeti felépítése



kód, annál több ilyen címkét tartalmaz. A 3 fő helyzetjelző között van egy szigorúan váltakozó bitekből álló sor (4.3.), amelyről a mátrixot definiáljuk. A mátrixban lévő adatok két dimenzióban tárolódnak - függőlegesen és vízszintesen. Az (5.)-et keretnek nevezzük.

A QR-kód több adatterületre osztható, és ugyanígy a több QR-kódban tárolt adatok egyetlen QR-kódba konvertálhatók. Egy szimbólum max. 16 kódba osztható. Erre egy példa:



A kódolt információk a következők:
"*Ez egy pelda*" + "*a kod*" + "*konvertalasara.*" = "*Ez egy pelda a kod konvertalasara.*"
A QR-kód adattárolási kapacitása:

Csak numerikus értékekből	max. 7089 karakter
Alfanumerikus értékekből	max. 4296 karakter
Bináris adatokból (8 bites szervezésben)	max. 2953 bájt
Kanji, Kana jelekből	max. 1817 karakter

2.2. A QR-kódok olvasása és a hibajavítás

Egy másik jelentős pozitív tulajdonsága a kód skálázhatósága, amit 1-től 40-ig határoztak meg. A különböző verziók különböző adattárolási és hibatűrési tulajdonságokkal rendelkeznek.

A kód a Reed–Solomon hibajavító algoritmust használja, négy hibaja-

vító szinttel. A QR-kódhoz tartozó hibajavító képességek, szintek rögzítve vannak, amik azt jelölik, hogy az adott kód milyen mértékű sérülés esetén olvasható vissza biztonságosan. Ezek a következők lehetnek:

- L - 7% veszteség visszaállítására képes.
- M - 15% veszteség visszaállítására képes.
- Q - 25% veszteség visszaállítására képes.
- H - 30% veszteség visszaállítására képes.

Példák:

1.)  2.)  3.) 

Mind a három kód ugyanazt a szöveges információt tartalmazza, "*A torzulas merteke es a hibajavito szintek osszefuggese.*", különböző hibajavítási szintek esetén. A példákból is látszik, hogy a hibajavító szint növekedésével a képpontok, pixelek száma is nő. Balról jobbra a szintek L, M, H. Ha meg szeretnénk figyelni, hogy ez mit is jelent, akkor próbáljunk meg letakarni egy részletet a kódból, például a jobb alsó sarkot. QR-kód olvasóval beolvasva a kódokat észrevesszük, hogy minél nagyobb a hibajavító szint annál nagyobb részlet letakarásával is képes dekódolni az üzenetet.

Nagyobb QR-szimbólumok esetén az üzenet több Reed–Solomon kódblokkra bontható. A blokk méretét úgy választják meg, hogy minden blokkban legfeljebb 15 hiba javítható legyen, ez korlátozza a dekódoló algoritmus összetettségét. A kódblokkok ezután együtt vannak egymásba illesztve, így kevésbé valószínű, hogy a QR-szimbólum lokális károsodása tönkreteszi bármelyik blokk kapacitását.

A hibajavítás miatt olyan művészi QR-kódokat lehet létrehozni, amelyeket továbbra is helyesen lehet szkennelni, de szándékos hibákat tartalmaznak, hogy olvashatóbbá vagy vonzóbbá váljanak az emberi szem számára, ezért például színeket, logókat építenek be a QR-kódba. Az is lehetséges az alapul szolgáló matematikai konstrukciók manipulálásával, hogy művészi QR-kódokat tervezzünk anélkül, hogy csökkenne a kód hibajavító képessége. Erre példa a 2. és 3. ábra, amik egy QR-kód generátorral készültek ld. [10].

Az alábbi művészi QR-kód (2.ábra) a következő információt tartalmazza, "*Művészi QR-kód szín beépítésével.*". Láthatjuk, hogy a háttérszín módosítása nem csökkenti a hibajavító képességet, hiszen az olvasó továbbra is képes helyesen szkennelni.

2. ábra.

Ha ennél is egyedibb QR-kódot szeretnénk generálni arra is van lehetőség. A következő példa (3.ábra) alapján láthatjuk, hogy a háttérszín, egy logó beépítése sőt még a képpontok alakjának megváltoztatása sem csökkenti a hibajavító képességet, így az olvasó még mindig képes szkennelni a kódot, amely a "*Művészi QR-kód szín és logó beépítésével.*" információt tartalmazza.

3. ábra.

Számos különböző terület van a kódban, amiket a szerkezetnél már megismertünk. Ezeket a kód felderítéséhez használják, így nem lényegesek a rögzített információk szempontjából. Vannak a formátuminformációk és az adatok. A formátuminformáció két dolgot rögzít: a hibajavító szintet és a szimbólumhoz használt maszkmintát. A maszkolás az adatok olyan mintáinak feldarabolására szolgál, amelyek megtéveszthetik a lapolvasót, például a nagy üres területek vagy olyan félrevezető tulajdonság, amely helymegjelölési jelnek tűnhet. A maszk mintázata egy rácson van meghatározva, amelyet meg kell ismételni, hogy lefedje a teljes szimbólumot és emellett a hibák számának csökkentését is szolgálja. A maszk a sötét területeinek megfelelő kódbeli modulokat invertálja. A formátuminformációkat BCH-kóddal védik a hibáktól, amely akár 3 bites hibákat is képes kijavítani.

Ha nem áll rendelkezésünkre a megfelelő lapolvasó, akkor akár tollal papírral és a saját magunk is tudjuk dekódolni az adatokat. A fekete négyzet az 1-et, a fehér a 0-t jelöli.

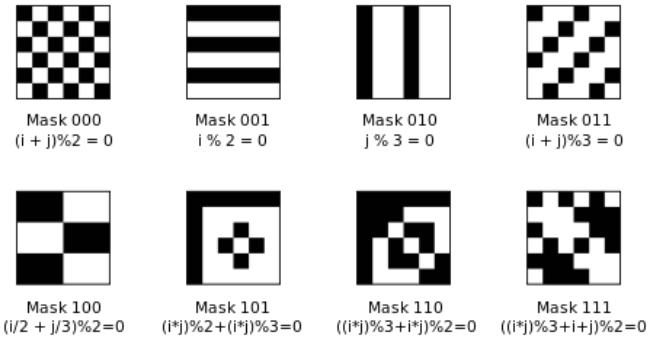
Az adatok olvasása az alábbi lépésekben történik, miután a 3 sarokban elhelyezkedő sajátos minta segítségével felismertük a tájolást :

1. lépés: A verzió meghatározása, amely a kód fizikai méretét mutatja meg. Meg kell számolni a kódban egy teljes oszlopban a pixelek számát, levonni 17-et és elosztani 4-gyel.

2. lépés: A formátuminformáció kitalálása, amelyből két példányt tartalmaz a kód. A formátuminformáció 15 adatbit, köztük az első 5 a

hasznos információ, a fennmaradó 10 pedig a BCH-kód, amely lehetővé teszi a hibák kijavítását. Az 5 bit hasznos információból az első 2 bit jelzi a hibajavító szintet, a fennmaradó 3 bit pedig jelzi, hogy a rendelkezésre álló 8 maszkból melyik vonatkozik az adatra.

3. lépés: A formátuminformációk védelmére egy statikus maszkot használnak. Mivel csak az első 5 bit érdekes, a maszk rövidíthető. Az adatszakasz biteit olvasva a maszkmintát figyelembe kell venni. A lehetséges maszkmintákat a 4. ábra mutatja be.



4. ábra.

4. lépés: Annak megértéséhez, hogy milyen adatokat kell kezelni, először el kell olvasni egy 4 bites fejlécet, amely információkat tartalmaz a kódolás módjáról (pl.: numerikus, alfanumerikus, bináris) és így a kódszavak hosszáról. A QR-kódokban minden kódszó hossza megegyezik egy adott kódolási típuson belül azaz, az üzenet egyforma hosszú kódszavakból épül fel.

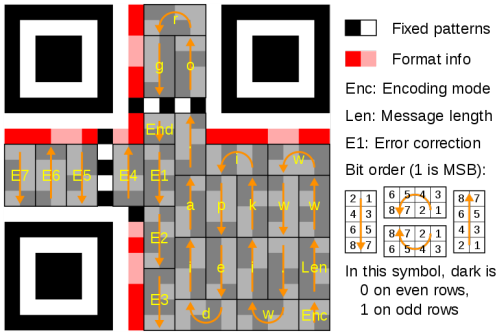
   A kódszavak hossza vagyis, a bitszámok a különböző kódolási típusokhoz:

   - Numerikus : 10 bit
   - Alfanumerikus: 9 bit
   - Bináris : 8 bit

5. lépés: A fejléc felett elhelyezkedő 8 bit határozza meg az üzenet hosszát azaz, hogy hány egyforma hosszú kódszóból áll az üzenet.

6. lépés: Ezek után már olvashatjuk is az üzenetet a kódolás módjának megfelelően. Az üzenet elhelyezkedését és azt, hogy hogyan kell olvasni az 5. ábra szemlélteti. Az így kapott 0-1-es sorozatokat az ASCII kódtábla segítségével tudjuk dekódolni.

5. ábra.



A QR-kód lapolvasóval történő dekódolása során az adatok helytelen olvasása esetén olyan speciális kódokat használnak, amelyek képesek az olvasási hibák kijavítására. Ezek az úgynevezett Reed–Solomon-féle hibajavító kódok, amelyek a lineáris kódok egyik leggyakrabban használt osztálya. Az 1., 4. és 5. ábrák forrása: [8].

3. Reed–Solomon-féle hibajavító kódok

3.1. Felépítés

3.1. Definíció. *Legyen $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ a $GF(q)$ véges test $n < q$ darab, különböző eleme, továbbá $u = (u_0, u_1, \ldots, u_{k-1})$ egy továbbítandó üzenet. Rendeljük az üzenethez az alábbi $GF(q)$ feletti polinomot:*

$$u(\alpha) = u_0 + u_1\alpha + \cdots + u_{k-1}\alpha^{k-1}.$$

A Reed–Solomon-kód a u üzenethez azt a $c = (c_0, c_1, \ldots, c_{n-1})$ kódszóvektort rendeli hozzá, amelynek c_i komponenseit a

$$c_i = u(\alpha_i) \tag{1}$$

képlet határozza meg. Látható, hogy a α_i elemek kiválasztása adja meg a kódot.

3.2. Tétel. *Az (n, k) paraméterű Reed–Solomon-kód kódtávolsága*

$$d = n - k + 1,$$

vagyis a Reed–Solomon-kód MDS kód.

Bizonyítás. Azt szeretnénk belátni, hogy a Reed–Solomon-kódokra teljesül, hogy $d = n - k + 1$. A Singleton-korlát szerint

$$d \leq n - k + 1,$$

így azt kell belátnunk, hogy a $c \neq 0$ kódszavakra igaz, hogy

$$w_H(c) \geq n - k + 1.$$

Minden kódszó súlya a nemnulla komponenseinek a száma. A kódszavak komponenseit viszont úgy kaptuk, hogy a megfelelő α_i számokat helyettesítettük be az üzenetpolinomba. A csupa nulla együtthatós polinom kivételével az $u(\alpha_i)$ eredménye csak akkor lesz 0, ha α_i a polinom gyöke. Mivel az üzenet k komponensű, a hozzárendelt polinom legfeljebb $k-1$-edfokú. Egy $k-1$-edfokú polinomnak viszont legfeljebb $k-1$ gyöke van. Az n darab különböző α_i számból tehát legfeljebb $k-1$ adhat 0-t az üzenetpolinomba behelyettesítve, így a kódszónak legfeljebb $k-1$ 0 komponense lesz. A maradék legalább $n-(k-1)$ komponens nem lesz 0. Azaz,

$$w(c) = |\forall i : c_i \neq 0, i = 1, \ldots, n| = n - |\forall i : c_i = 0, i = 1, \ldots, n| \geq$$
$$n - |\alpha \in GF(q) : u(\alpha) = 0| \geq n - (k-1),$$

tehát

$$w(c) \geq n - k + 1.$$

A Singleton-korlát tételét és a lineáris kódokra vonatkozó $d = w_{min}$ összefüggést felhasználva:

$$n - k + 1 \geq d = w_{min}.$$

□

Az (n, k) paraméterű Reed–Solomon-kód $n-k$ hibát tud jelezni, $\lfloor \frac{n-k}{2} \rfloor$ egyszerű hibát és $n-k$ törléses hibát tud javítani. Ez utóbbi azt is jelenti, hogy az u ismeretlenre vonatkozó

$$uG = c$$

n darab egyenletből bármelyik $n-k$ egyenlet elhagyásával egy egyértelműen megoldható egyenletrendszer marad, tehát a G mátrix minden $k \times k$-s négyzetes mátrixra invertálható.

3.3. Definíció. *A $GF(q)$ véges test feletti, $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ generáló elemekkel rendelkező Reed–Solomon-kódok generátormátrixa:*

$$\mathbf{G} = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ \alpha_0 & \alpha_1 & \alpha_2 & \cdots & \alpha_{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha_0^{k-1} & \alpha_1^{k-1} & \alpha_2^{k-1} & \cdots & \alpha_{n-1}^{k-1} \end{pmatrix}.$$

Paritásellenőrző mátrixa:

$$\mathbf{H} = \begin{pmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{n-k} & \alpha^{2(n-k)} & \cdots & \alpha^{(n-k)(n-1)} \end{pmatrix}.$$

3.1.1. Egyetlen generátorelemmel definiált Reed–Solomon-kód

3.4. Definíció. *Legyen $\gamma(\neq 0) \in GF(q)$, melynek rendje m, $m \geq n$. Ekkor $\gamma^0 = 1, \gamma^1, \gamma^2, \ldots, \gamma^{n-1}$ mind különböző $GF(q)$-beli szám lesz, tehát*

$$\alpha_i = \gamma^i \qquad \{i \in 0, \ldots, n-1\}.$$

3.5. Definíció. *A $\gamma^0, \gamma^1, \gamma^2, \ldots, \gamma^{n-1}$ elemek által generált Reed–Solomon-kód generátormátrixa:*

$$\mathbf{G} = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \gamma & \gamma^2 & \cdots & \gamma^{n-1} \\ 1 & \gamma^2 & \gamma^4 & \cdots & \gamma^{2(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \gamma^{k-1} & \gamma^{2(k-1)} & \cdots & \gamma^{(n-1)(k-1)} \end{pmatrix}.$$

A kód paritásellenőrző mátrixa:

$$\mathbf{H^T} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \gamma & \gamma^2 & \cdots & \gamma^{n-k} \\ \gamma^2 & \gamma^4 & \cdots & \gamma^{2(n-k)} \\ \vdots & \vdots & \ddots & \vdots \\ \gamma^{n-1} & \gamma^{2(n-1)} & \cdots & \gamma^{(n-k)(n-1)} \end{pmatrix}.$$

A fenti konstrukció tulajdonképpen azt jelenti, hogy az 1 definícióbeli képlet az alábbi alakra módosul:

$$c_i = u(\gamma^i) = \sum_{j=0}^{k-1} u_j (\gamma^i)^j. \tag{2}$$

3.1.2. A Reed–Solomon-kód, mint ciklikus kód

3.6. Definíció. *Egy*

$$c = (c_0, c_1, \ldots, c_{n-1})$$

vektor ciklikus eltoltja a

$$Sc = (c_{n-1}, c_0, c_1, \ldots, c_{n-2}).$$

S-et a ciklikus eltolás operátorának nevezzük.

3.7. Definíció. *A C kódot ciklikusnak nevezzük, ha bármely kódszó ciklikus eltoltja is kódszó.*

3.8. Definíció. *Rendeljünk polinomot az egyes kódszavakhoz a következő módon:*

$$c = (c_0, c_1, \ldots, c_{n-1}) \mapsto c(\alpha) = c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1},$$

ekkor a c kódszónak megfeleltetett $c(\alpha)$ polinomot kódszópolinomnak nevezzük. A kódszópolinomok halmazát $C(\alpha)$-val jelöljük.

3.9. Tétel. *Minden (n, k) paraméterű, ciklikus, lineáris C kódban a nem azonosan nulla kódszópolinomok között egyértelműen létezik egy minimális fokszámú $g(\alpha)$ főpolinom. Egy $g(\alpha)$ polinomot főpolinomnak nevezünk, ha a legmagasabb fokú tagjának az együtthatója 1. A $g(\alpha)$ fokszáma $n - k$ és egy $c \in C$ akkor és csak akkor, ha $g(\alpha) \mid c(\alpha)$, azaz létezik egy $u(\alpha)$ polinom úgy, hogy $c(\alpha) = g(\alpha)u(\alpha)$.*

3.10. Definíció. *A $g(\alpha)$-et a kód generátorpolinomjának nevezzük.*

3.11. Definíció. *Egy $g(\alpha)$ generátorpolinomú lineáris, ciklikus kód esetén a*

$$h(\alpha) = \frac{\alpha^n - 1}{g(\alpha)}$$

polinomot paritásellenőrző polinomnak nevezzük.

Rendeljünk minden $c = c_0, c_1, \ldots, c_{n-1}$ kódszavunkhoz egy

$$c(\alpha) = c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_{n-1}\alpha^{n-1} = \sum_{i=0}^{n-1} c_i \cdot \alpha^i$$

polinomot. Helyettesítsük be a kapott kódszópolinomba a γ generáló elem első $n - k$ hatványát az elsőtől kezdve:

$$c(\gamma^l) = \sum_{i=0}^{n-1} c_i \cdot (\gamma^l)^i.$$

Ha behelyettesítjük a c_i együtthatók a 2-beli definíciós összefüggését, az előbbi egyenlőség a következő alakot ölti:

$$c(\gamma^l) = \sum_{i=0}^{n-1} \Big(\sum_{j=0}^{k-1} u_j \gamma^{ij} \Big) \cdot (\gamma^l)^i = \sum_{i=0}^{n-1} \sum_{j=0}^{k-1} u_j \gamma^{i(j+l)}.$$

Mivel $0 \leq j \leq k-1$ és $1 \leq l \leq n-k$ a $j+l$-re mindenképpen igaz lesz, hogy $1 \leq j+l \leq n-1$. Eszerint, mivel γ-nak csak a nulladik és az n-edik hatványa lehet 1, a $\gamma^{j+l} \neq 1$. Így :

$$c(\gamma^l) = \sum_{j=0}^{k-1} u_j \Big(\sum_{i=0}^{n-1} \big(\gamma^{(j+l)}\big)^i \Big),$$

ahol a nagy zárójelben szereplő kifejezés tulajdonképpen egy mértani sor első n elemének az összege, csak a mértani sor $GF(q)$-en van értelmezve. A mértani sor n-edik részösszegének a képlete véges számtesteken is érvényes (feltéve, hogy a sor kvóciense nem 1), így

$$\sum_{i=0}^{n-1} \big(\gamma^{(j+l)}\big)^i = \frac{\big(\gamma^{(j+l)}\big)^n - 1}{\gamma^{(j+l)} - 1} = \frac{\gamma^{n(j+l)} - 1}{\gamma^{(j+l)} - 1},$$

ami nullát ad eredményül, mivel $\gamma^n = 1$. Visszahelyettesítve az eredményt az egyenlőségbe, a Reed–Solomon-kód paritásegyenleteit kapjuk:

$$c(\gamma^l) = 0, \qquad ha\, 1 \leq l \leq n-k.$$

A paritásegyenletek szerint a γ generátorelem első $n-k$ hatványa minden kódszópolinomnak a gyöke.

Így létezik egy olyan polinom, amely minden kódszónak osztója: az a polinom, melynek a gyöktényezői a $(\alpha - \gamma^l)$-ek, $l = 1, 2, \ldots, n-k$-ra.

A szóban forgó Reed–Solomon-kód tehát egyben egy a $GF(q)$ véges test feletti (n, k) paraméterű ciklikus kód is, melynek a generátorpolinomja (gyöktényezős felbontásban)

$$g(\alpha) = (\alpha - \gamma) \cdot (\alpha - \gamma^2) \cdot \ldots \cdot (\alpha - \gamma^{n-k}).$$

Belátható, hogy a $\alpha^n - 1$ polinomnak az összes $(\alpha - \gamma^i)$ polinom az osztója, így a kód paritásellenőrző polinomja előáll

$$\alpha^n - 1 = \prod_{i=0}^{n-1} (\alpha - \gamma^i)$$

polinom $g(\alpha)$-ban fel nem használt gyöktényezőkből, azaz

$$h(\alpha) = (\alpha - \gamma^{n-k+1}) \cdot (\alpha - \gamma^{n-k+2}) \cdot \ldots \cdot (\alpha - \gamma^n).$$

3.2. A Reed–Solomon-kódok dekódolása, a törléses hibák javítása

3.12. Definíció. *Legyen C lineáris kód és H a paritásellenőrző mátrixa, ekkor az $s = vH^T$ mennyiséget szindrómának nevezzük.*

Legyen az adott kódszó c, a vett szó v. Az $e = v - c$ vektort hibavektornak nevezzük. Vegyük észre, hogy

$$Hv^T = H(c+e)^T = Hc^T + He^T = He^T,$$

vagyis Hv^T értéke csak a hibavektortól függ, az adott kódszótól nem, hiszen az érvényes kódszavak szindrómája 0. A szindróma tehát a hibavektor egy lineáris leképezése.

A dekódolás leggyakoribb módja a szindróma dekódolás. A fentiek alapján a dekódolás a következőképpen mehet végbe: a vett v szóból kiszámítjuk az $s^T = Hv^T = He^T$ szindrómát, ennek alapján megbecsüljük a hibavektort és ezt v-ből levonva megkapjuk a kódszóra vonatkozó becslést.

A Reed–Solomon-kódok paritásellenőrző mátrixa a definíció szerint:

$$\mathbf{H} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \gamma & \gamma^2 & \cdots & \gamma^{n-k} \\ \gamma^2 & \gamma^4 & \cdots & \gamma^{2(n-k)} \\ \vdots & \vdots & \ddots & \vdots \\ \gamma^{n-1} & \gamma^{(n-1)2} & \cdots & \gamma^{(n-1)(n-k)} \end{pmatrix},$$

ahol γ a kód generáló eleme és $Hc^T = 0$.

Ha elvégezzük ezt a mátrixszorzást, akkor a szindróma j-edik elemére a következő képletet kapjuk:

$$s_j = \sum_{i=0}^{n-1} e_i \cdot \gamma^{ij}. \tag{3}$$

Az előbbi egyenlőség alapján az n hosszú e hibavektor rekonstrukciójához az $n-k$ hosszú s szindróma áll rendelkezésre. A vett szóhoz legközelebbi kódszóba javításkor egy lineáris egyenletrendszer egy speciális tulajdonságú, mégpedig a minimális súlyú megoldását keressük.

3.13. Definíció. *A minimális súlyú $e = (e_0, e_1, \ldots, e_{n-1})$ hibavektor rekonstrukciójához a következő ismeretlenek felderítésére van szükség:*

- *a hibák száma:* t,
- *a hibák helye:* $0 \leq i_1 < i_2 < \cdots < i_t \leq n-1$,
- *a hibák értéke:* $e_{i_1}, e_{i_2}, \ldots, e_{i_t}$.

Ha csak törléses hibánk van, akkor ismerjük a hibák számát és a hibahelyeket, csupán a hibaértékeket kell megtalálni. Egy (n,k) paraméterű Reed–Solomon-kód legfeljebb $n-k$ törléses hibát tud kijavítani, azaz az e hibavektornak legfeljebb $n-k$ komponense lesz 0 és azt is tudjuk, hogy melyek ezek a komponensek, csak a nagyságukat nem ismerjük.

Tegyük fel, hogy pontosan $n-k$ törléses hibánk van. Ha ennél kevesebb, akkor néhány helyen 0 lesz a törléses hiba nagysága. Így a 3-beli egyenlőségek mindegyikében csak jól meghatározott $n-k$ darab tag adhat nemnulla eredményt az összegben. Tulajdonképpen a H^T mátrixnak csak bizonyos sorai vesznek részt a műveletekben, mivel ha $e_i = 0$, akkor a H^T mátrix i-edik sorában minden elemnek 0 lesz a szorzója a 3-beli egyenletek mindegyikében. Töröljük gondolatban ezeket a sorokat a mátrixból, kapunk egy csonkolt $\widehat{H}^T$ mátrixot, melynek $n-k$ sora és $n-k$ oszlopa van. Töröljük a hibavektorból is a 0 elemeket, így $\widehat{e}$ vektort kapunk $n-k$ komponenssel. Mivel a szindróma $n-k$ elemből áll, egy $n-k$ darab egyenletből álló egyenletrendszert kapunk $\widehat{e}$-re, ami teljesen meghatározza $\widehat{e}$-t, azaz a

$$\begin{aligned}
\widehat{H}_{00} \cdot \widehat{e}_0 + \widehat{H}_{10} \cdot \widehat{e}_1 + \cdots + \widehat{H}_{n-k-1\,0} \cdot \widehat{e}_{n-k-1} &= s_0 \\
\widehat{H}_{01} \cdot \widehat{e}_0 + \widehat{H}_{11} \cdot \widehat{e}_1 + \cdots + \widehat{H}_{n-k-1\,1} \cdot \widehat{e}_{n-k-1} &= s_1 \\
&\vdots \\
\widehat{H}_{0\,n-k-1} \cdot \widehat{e}_0 + \widehat{H}_{1\,n-k-1} \cdot \widehat{e}_1 + \cdots + \widehat{H}_{n-k-1\,n-k-1} \cdot \widehat{e}_{n-k-1} &= s_{n-k-1}
\end{aligned}$$

egyenletrendszer egyértelműen megoldható.

Az, hogy egy $n-k$ egyenletből álló egyenletrendszernek van-e egyértelmű megoldása, attól függ, hogy az egyenletrendszert meghatározó mátrix milyen. Ha a mátrixnak nincs tiszta 0 sora, sem oszlopa és egyik sora (oszlopa) sem áll elő másik sorok (oszlopok) lineáris kombinációjaként, akkor az egyenletrendszer megoldható.

Egyszerű hibák javítására hatékony módszert ad a Berlekamp-Massey algoritmus, aminek kifejtését ld. [7] műben.

Hivatkozások

[1] Bogya Norbert, Kátai-Urbán Kamilla, *Absztrakt algebra (előadásjegyzet)*, 2017.

[2] Györfi László, Győri Sándor, Vajda István, *Információ- és kódelmélet*, Typotex Kiadó, 2000.

[3] Kiss György, Szőnyi Tamás, *Véges geometriák*, Polygon Kiadó, 2001.

[4] Maróti Miklós, Kátai-Urbán Kamilla, *Algebrai struktúrák (előadásjegyzet)*, 2017.

[5] Nagy Gábor Péter, *Véges geometriák és kódok (előadásjegyzet)*, 2018.

[6] Nagy Szilvia, *Információelmélet (előadásjegyzet, SZIE)*, 2006.

[7] Táborosi Andor, Reed-Solomon-féle hibajavító kódok, BSc szakdolgozat, SZTE, 2013.

[8] Wikipedia contributors. (2019, November 30). QR code. In Wikipedia, The Free Encyclopedia. Retrieved 14:25, December 2, 2019, from `https://en.wikipedia.org/wiki/QR_code`

[9] Andrew Fuller, 2019-12-02. `http://blog.qartis.com/decoding-small-qr-codes-by-hand/`

[10] QRCODEMONKEY, The 100% Free QR Code Generator, 2019-12-03., `https://www.qrcode-monkey.com`

Köszönetnyilvánítás

Köszönettel tartozom témavezetőmnek, Dr. Nagy Gábor Péternek, a szakdolgozatom témaválasztásában, illetve kidolgozásában nyújtott segítségéért továbbá azért, hogy az idejét áldozta erre a projektre.

Nyilatkozat

Alulírott Dobi Krisztina kijelentem, hogy a szakdolgozatban foglaltak saját munkám eredményei, és csak a hivatkozott forrásokat (szakirodalom, eszközök, stb.) használtam fel.

A szakdolgozat a 2018-1.2.1-NKP-2018-00004 számú "IoT rendszerek biztonságát növelõ technológiák (SETIT)" projekt keretében, a Nemzeti Kutatási és Innovációs Alapból biztosított támogatással, a "Nemzeti Kiválósági Program: 2018-1.2.1-NKP" pályázati program finanszírozásában valósult meg.

Tudomásul veszem, hogy szakdolgozatomat a Szegedi Tudományegyetem könyvtárában a kölcsönözhető könyvek között helyezik el, és az interneten is nyilvánosságra hozhatják.

Szeged, 2019. december 11. .....

aláírás