7. Reed-Muller κώδικες

Για κάθε φυσικό αριθμό $m > 0$ και ακέραιο αριθμό r με $0 \le r \le m$ ορίζουμε τον Reed – Muller κώδικα τάξης r σαν τον δυαδικό γραμμικό κώδικα με παραμέτρους $n = 2^m$, $M = 2^k$, $d = 2^m - r$ όπου $k = \left(1 + \binom{m}{1} + \ldots + \binom{m}{r}\right)$. Αυτό τον κώδικα θα τον συμβολίζουμε με R(r, m).

Στη συνέχεια, θα περιοριστούμε στην περίπτωση όπου r = 1. Δηλαδή θα ασχοληθούμε με τον Reed-Muller κώδικα R(m) : = R(1, m), ο οποίος είναι τύπου $(n, M, d) = (2^m, 2^{m+1}, 2^{m-1})$.

Σημείωση 7.1 Ο R(5) χρησιμοποιήθηκε από τους αμερικάνους στο πρόγραμμα Mariner 9 το 1972 για να στείλει ασπρόμαυρες φωτογραφίες από τον Ερμή.

Ορισμός 7.2 Οι Reed-Muller κώδικες R(m) είναι δυαδικοί γραμμικοί κώδικες οι οποίοι ορίζονται για κάθε φυσικό αριθμό m, $m \ge 1$ επαγωγικά ως εξής:

(1) $R(1) = \mathbf{F}_2^2 = \{00, 01, 10, 11\}$
(2) Για $m \ge 1$ ο $R(m + 1)$ ορίζεται $R(m + 1) = \{uu \mid u \in R(m)\} \cup \{uu^c \mid u \in R(m)\}$

Παρατήρηση 7.3 Ο R(1) είναι τύπου $(2, 2^2, 2^0)$ δηλαδή η ελάχιστη απόσταση του κώδικα είναι 1 και αντιστοιχεί στο βάρος όλων των κωδικών λέξεων διαφορετικών των 11 και 00.

Αυτό ισχύει γενικά.

Θεώρημα 7.4 Ο R(m), $m \ge 1$ είναι δυαδικός γραμμικός κώδικας τύπου $(2^m, 2^{m+1}, 2^{m-1})$ όπου κάθε κωδική λέξη, εκτός των 00…0 και 11…1, έχει βάρος 2^{m-1}.

Παράδειγμα 7.5 Όλες οι κωδικές λέξεις του

$$R(2) = \{0000, 0101, 1010, 1111, 0011, 0110, 1001, 1100\}$$

εκτός των 0000, 1111 έχουν βάρος 2.

Παρατήρηση 7.6 Ο κώδικας R(2) έχει γεννήτορα πίνακα

$$R_2 = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}.$$

Γενικεύουμε επαγωγικά

Θεώρημα 7.7

1. Ένας γεννήτορας πίνακας του R(1) είναι ο $R_1 = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$.

2. Αν R_m γεννήτορας πίνακας του κώδικα R(m) τότε ένας γεννήτορας πίνακας του κώδικα R(m + 1) είναι ο

$$R_{m+1} = \left[\begin{array}{c|c} 00...0 & 11...1 \\ \hline R_m & R_m \end{array}\right].$$

Παράδειγμα 7.8 Ένας γεννήτορας πίνακας του R(3) είναι

$$R_3 = \left[\begin{array}{cccc:cccc} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{array}\right]$$

Θεώρημα 7.9 Ο πίνακας R_m μπορεί να περιγραφεί ως εξής:

- Πρώτη γραμμή: 2^{m-1} μηδενικά ακολουθούμενα από 2^{m-1} μονάδες.
- Δεύτερη γραμμή: Εναλλαγή από μπλοκς μηδενικών και μονάδων μήκους 2^{m-2} το καθένα

…

- i-στή γραμμή: Εναλλαγή από μπλοκς μηδενικών και μονάδων μήκους 2^{m-i} το καθένα

…

- m-στή γραμμή: Εναλλαγή από 0 και 1
- (m + 1)-στή γραμμή: Μόνο μονάδες

Αποκωδικοποίηση των Reed-Muller κωδίκων

Ο Reed-Muller κώδικας R(m) έχει ελάχιστη απόσταση $d = 2^{m-1}$. Επομένως, ο κώδικας διορθώνει το πολύ $\left[\frac{d-1}{2}\right] = \left[\frac{2^{m-1}-1}{2}\right] = 2^{m-2} - 1$ λάθη. Τα διανύσματα μήκους n στον $\mathbf{F}_2$ είναι $2^n = 2^{2^m}$ άρα έχουμε $\frac{2^{2^m}}{2^{m+1}} = 2^{2^m - m - 1}$ cosets.

Για παράδειγμα αν θέλουμε ο κώδικας να διορθώνει 7 λάθη θα πρέπει m = 5. Έχουμε επομένως, $2^{2^5 - 5 - 1} = 2^{26} = 67\ 108\ 864$ cosets. **Καταστροφή** ακόμα και για μικρό m όπως αυτό του Mariner. Άρα πρέπει να ψάξουμε για άλλους τρόπους αποκωδικοποίησης.

Reed – Muller αποκωδικοποίηση

Πρόκειται για ειδικό τύπο του majority logic decoding (αποκωδικοποίηση της πλειοψηφίας).

Ιδέα! Έστω C γραμμικός δυαδικός κώδικας με βάση $B = \{\underline{b}_1, \underline{b}_2, \ldots, \underline{b}_k\}$. Υποθέτουμε ότι στείλαμε την κωδική λέξη $\underline{c} = c_1c_2\ldots c_n$. Αφού το σύνολο B είναι βάση υπάρχουν $a_1, a_2, \ldots, a_k \in \mathbf{F}_2$ τέτοια ώστε $\underline{c} = a_1\underline{b}_1 + \ldots + a_k\underline{b}_k$. Υποθέτουμε ότι μπορούμε να βρούμε διαφορετικούς τρόπους να υπολογίσουμε το a_i από το αντίστοιχο c_i, για παράδειγμα με τέσσερις διαφορετικούς μεταξύ τους, και ότι κάθε φορά χρησιμοποιούμε διαφορετικές συντεταγμένες.

Παράδειγμα 7.10 Υποθέτουμε ότι $n = 8$ και ότι στάλθηκε η κωδική λέξη $c = c_1c_2\ldots c_8$. Υποθέτουμε ότι το a_1 γράφεται στις μορφές:

$a_1 = c_1 + c_5$
$a_1 = c_2 + c_6$
$a_1 = c_3 + c_7$
$a_1 = c_4 + c_8$

Στη συνέχεια φανταζόμαστε ότι πήραμε, αντί του c που στάλθηκε, το διάνυσμα $x = x_1x_2\ldots x_8$ και υποθέτουμε ότι έχει το πολύ ένα λάθος.

Θα προσπαθήσουμε να υπολογίσουμε το a_1 χρησιμοποιώντας τις συντεταγμένες του διανύσματος x:

$a_1 = x_1 + x_5$
$a_1 = x_2 + x_6$
$a_1 = x_3 + x_7$
$a_1 = x_4 + x_8$

Επειδή στο x υποθέσαμε ότι υπάρχει το πολύ ένα λάθος έπεται ότι από τις 4 σχέσεις που μας δίνουν a_1 το πολύ μια δεν είναι σωστή. Εδώ η πλειοψηφία (majority) είναι τουλάχιστον 3 και μας δίνει την σωστή τιμή για το a_1.

Κάνουμε το ίδιο για όλα τα a_i για $i = 1, 2, \ldots, k$ και έτσι αποκωδικοποιούμε στην κωδική λέξη $\underline{c} = a_1\underline{b}_1 + \ldots + a_k\underline{b}_k$.

Αυτή η μέθοδος λέγεται majority logic decoding.

Στη συνέχεια θα μελετήσουμε τον γεννήτορα πίνακα R_m. Συμβολίζουμε τις γραμμές του R_m με $\underline{b}_1, \underline{b}_2, \ldots, \underline{b}_m, \ldots, \underline{b}_{m+1}$. Αυτές αποτελούν βάση του κώδικα R(m).

Υποθέτουμε ότι στάλθηκε το $\underline{c} = c_1c_2\ldots c_n$. Ισχύει ότι,

$$\underline{c} = a_1\underline{b}_1 + \ldots + a_m\underline{b}_m + a_{m+1}\underline{b}_{m+1}.$$

Επιθυμούμε να βρούμε όσο πιο πολλές εκφράσεις γίνεται των $a_i \in \mathbf{F}_2$ συναρτήσει των c_i για κάθε $i = 1, \ldots, k$.

Υποθέτουμε ότι ένα διάνυσμα x_i είναι ορθογώνιο σε κάθε άλλη γραμμή πλην της $\underline{b}_i$ ενώ ισχύει $x_ib_i = 1$. Τότε $x_ic = x_i(a_1\underline{b}_1 + \ldots + a_m\underline{b}_m + a_{m+1}\underline{b}_{m+1}) = a_i(x_i\underline{b}_i) = a_i$.

Ερώτημα Πως θα βρούμε τέτοια διανύσματα x_i;

Γράφουμε τις συνιστώσες του διανύσματος $\underline{b}_i$. Έστω ότι $\underline{b}_i = b_{i1}b_{i2}\ldots,b_{in}$ και έστω $\underline{e}_\lambda = 0\ldots010\ldots0$ το διάνυσμα που έχει 1 στην λ-στη θέση και 0 οπουδήποτε αλλού. Ισχύει ότι $\underline{e}_\lambda\underline{b}_i = b_{i\lambda}$ και $(\underline{e}_\lambda + \underline{e}_\mu)b_i = b_{i\lambda} + b_{i\mu}$ (mod 2). Για να είναι το διάνυσμα $\underline{e}_\lambda + \underline{e}_\mu$ κάποιο υποψήφιο x_i θα πρέπει $(\underline{e}_\lambda + \underline{e}_\mu)\underline{b}_v = b_{v\lambda} + b_{v\mu}$ (mod 2) $= \begin{cases} 1 & v = i \\ 0 & v \neq i \end{cases}$.

Επειδή 2 bits έχουν άθροισμα 1 αν και μόνο αν είναι διαφορετικά μεταξύ τους, έπεται ότι το παραπάνω θα συμβεί ακριβώς τότε όταν η λ-στη στήλη του R_m και η μ-στη στήλη διαφέρουν στην i γραμμή και συμπίπτουν σε όλες τις άλλες θέσεις.

Παράδειγμα 7.11 Ας θεωρήσουμε τον πίνακα $R_3 = \left[\begin{array}{cccc:cccc} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{array}\right]$.

Αν πάρουμε i = 1 και εξετάσουμε ποια ζευγάρια στηλών μας δίνουν το x_1 θα δούμε ότι είναι τα (Σ1, Σ5), (Σ2, Σ6), (Σ3, Σ7), (Σ4, Σ8).

Συνεπώς, για κάθε γραμμή i θέλουμε ένα ζευγάρι στηλών του R_m τα οποία ταυτίζονται σε όλες τις θέσει εκτός της i-στής γραμμής. Τέτοια ζευγάρια θα λέγονται **καλά ζευγάρια** για την i-στή γραμμή. Μπορούμε τώρα, σύμφωνα με τα παραπάνω, να διατυπώσουμε το ακόλουθο

Λήμμα 7.12 Αν (λ, μ) είναι η θέση δύο στηλών του R_m οι οποίες αποτελούν καλό ζευγάρι για την i-στή γραμμή του πίνακα R_m, τότε για κάθε κωδική λέξη $\underline{c} = a_1\underline{b}_1 + \ldots + a_m\,\underline{b}_m + a_{m+1}\,\underline{b}_{m+1}$ και για κάθε δείκτη i = 1, …, m έχουμε ότι $a_i = (\underline{e}_\lambda + \underline{e}_\mu)\underline{c}$.

Παρατήρηση 7.13 Επειδή η τελευταία γραμμή του πίνακα R_m έχει παντού μονάδες, οποιοδήποτε ζευγάρι στηλών του R_m έχει μονάδα στην (m +1)-στή θέση. Δηλαδή, η τελευταία γραμμή δεν έχει καλά ζευγάρια.

Με την τελευταία γραμμή θα ασχοληθούμε λίγο παρακάτω. Ούτως ή άλλως η τελευταία γραμμή δεν μας δημιουργεί κανένα πρόβλημα στην εύρεση καλών ζευγαριών για τις άλλες γραμμές και μπορούμε, συνεπώς, να την αγνοήσουμε. Πράγματι, έστω R'_m ο πίνακας που προκύπτει από τον R_m με την αφαίρεση της τελευταίας του γραμμής. Ένα καλό ζευγάρι για την i-στή γραμμή έχει τη μορφή

$$\begin{bmatrix} \beta_1 \\ \vdots \\ \beta_{i-1} \\ 0 \\ \beta_{i+1} \\ \vdots \\ \beta_n \end{bmatrix} \quad \text{και} \quad \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_{i-1} \\ 1 \\ \beta_{i+1} \\ \vdots \\ \beta_n \end{bmatrix}.$$

Ονομάζουμε αντίστοιχα τις στήλες το «**0-μισό**» του καλού ζευγαριού και το «**1-μισό**» του καλού ζευγαριού. Σύμφωνα με το προηγούμενο θεώρημα που διατυπώσαμε χωρίς απόδειξη οι στήλες του R'_m αποτελούνται από τις δυαδικές παραστάσεις των αριθμών 0, 1, 2, $2^m - 1$ με την κανονική σειρά.

Επομένως, για κάθε τιμή β_i υπάρχουν πάντοτε δύο στήλες της παραπάνω μορφής. Επιπλέον, επειδή η στήλη «1-μισό» του ζευγαριού παριστά μεγαλύτερο δυαδικό αριθμό από αυτόν που παριστά η «0-μισό» έπεται ότι η στήλη «1-μισό» βρίσκεται δεξιότερα της στήλης «0-μισό». Το ερώτημα είναι πόσο δεξιότερα. Ο αριθμός που παριστά η στήλη «1-μισό» είναι 2^{m-i} μεγαλύτερος από τον αριθμό που παριστά η στήλη «0-μισό». Άρα η απόσταση του «1-μισό» από το «0-μισό» ως προς την i-γραμμή είναι 2^{m-i}.

Συμπέρασμα Όλα τα καλά ζευγάρια για την i-στη γραμμή τα παίρνουμε ως εξής: Θεωρούμε όλες τις στήλες του R_m που έχουν 0 στην i-στη θέση. Αν «0-μισό» είναι η στήλη j τότε η αντίστοιχη «1-μισό» στήλη του καλού ζευγαριού για τη γραμμή i είναι η στήλη $(j + 2^{m-i})$.

Για παράδειγμα, στον R_3 για να βρούμε τα καλά ζευγάρια για την πρώτη γραμμή βρίσκουμε τις στήλες που έχουν 0, δηλαδή τις 1, 2, 3 και 4, και στη συνέχεια από τον τύπο $j + 2^{m-i}$ βρίσκουμε το αντίστοιχο «1-μισό». Επομένως, τα καλά ζευγάρια για την πρώτη γραμμή είναι τα (Σ1, Σ5), (Σ2, Σ6), (Σ3, Σ7), (Σ4, Σ8), για την δεύτερη γραμμή ισχύει j = 1, 2, 5, 6 άρα τα καλά ζευγάρια είναι τα (Σ1, Σ3), (Σ2, Σ4), (Σ5, Σ7), (Σ6, Σ8). Για την τρίτη γραμμή ισχύει j = 1, 3, 5, 7 άρα τα καλά ζευγάρια είναι τα (Σ1, Σ2), (Σ3, Σ4), (Σ5, Σ6), (Σ7, Σ8). Η τέταρτη, όπως προείπαμε, προς το παρόν δεν μας ενδιαφέρει. Επομένως, οι μισές ακριβώς από τις στήλες του R_m μας δίνουν τα «0-μισά» των καλών ζευγαριών για οποιαδήποτε γραμμή i και οι άλλες μισές τα αντίστοιχα «1-μισά».

Συμπέρασμα Για κάθε γραμμή i = 1, 2, …, m υπάρχουν 2^{m-1} καλά ζευγάρια.

Αλγόριθμος αποκωδικοποίησης Reed-Muller κωδίκων

Υποθέτουμε ότι στάλθηκε η κωδική λέξη $\underline{c} = a_1\underline{b}_1 + \ldots + a_m \underline{b}_m + a_{m+1} \underline{b}_{m+1}$. Αν χρησιμοποιήσουμε τα 2^{m-1} καλά ζευγάρια, για την i-στή γραμμή ($i \le m$) θα έχουμε 2^{m-1} εκφράσεις του συντελεστή a_i μέσω διαφορετικών μεταξύ τους ζευγαριών συντεταγμένων του $\underline{c}$. Για παράδειγμα, αν (Σλ, Σμ) καλό ζευγάρι για την i-στή γραμμή τότε $a_i = (\underline{e}_\lambda + \underline{e}_\mu)\ \underline{c} = c_\lambda + c_\mu$. Επομένως, αν δεν έχουμε περισσότερα από $2^{m-1} - 1$ λάθη τότε το πολύ $2^{m-2} - 1$ συνιστώσες του $\underline{x} = x_1x_2\ldots x_n$ που θα πάρουμε θα είναι λάθος. Συνεπώς, τουλάχιστον $2^{m-1} - (2^{m-2} - 1) = 2^{m-2} - 1$ εκφράσεις για το a_i, δηλαδή η πλειοψηφία, είναι σωστές. Οπότε, υπολογίζουμε τις 2^{m-1} εκφράσεις για το a_i και αποκωδικοποιούμε στην πλειοψηφούσα τιμή.

Τελικό βήμα Υπολογίζουμε τον συντελεστή a_{m+1}. Αν τα λάθη κατά την μεταφορά είναι $2^{m-1} - 1$ και υποθέσουμε ότι πήραμε το διάνυσμα $\underline{x}$ τότε το λάθος είναι το διάνυσμα $\underline{e} = \underline{x} - \underline{c}$ το οποίο έχει βάρος το πολύ $2^{m-1} - 1$. Αν θέσουμε $\underline{\delta} = a_1\underline{b}_1 + \ldots + a_m \underline{b}_m$ έχουμε $\underline{x} - \underline{\delta} = \underline{e} + \underline{c} - \underline{\delta} = \underline{e} + a_{m+1} \underline{b}_{m+1} = a_{m+1}\underline{1} + \underline{e}$, όπου $\underline{1} = 11\ldots1$. Υπάρχουν δύο δυνατότητες:

(i) Αν $a_{m+1} = 0$ τότε $\underline{e} = \underline{x} - \underline{\delta}$.

(ii) Αν $a_{m+1} = 1$ τότε $\underline{e} = (\underline{x} - \underline{\delta})^c$.

Συμπέρασμα
Αν $w(x - \delta) \leq 2^{m-2} - 1$ αποκωδικοποιούμε το a_{m+1} στο μηδέν.
Αν $w((x - \delta)^c) \leq 2^{m-2} - 1$ αποκωδικοποιούμε το a_{m+1} στο ένα.

Παρατήρηση 7.14 Αποδείξαμε ότι μπορούμε να διορθώσουμε το πολύ $2^{m-2} - 1$ λάθη. Άρα ο κώδικας έχει ελάχιστη απόσταση $d = 2^{m-1}$.

Παράδειγμα 7.15 Υποθέτουμε ότι η, άγνωστη σ' εμάς, κωδική λέξη c = 11 00 11 00 στάλθηκε μέσω ενός (8, 16, 4) Reed-Muller κώδικα R(3) αλλά εμείς πήραμε $x = x_1x_2\ldots x_8 = 11\ 01\ 11\ 00$. Επομένως, αν $\underline{c} = c_1c_2\ldots c_8 = a_1\underline{b}_1 + a_2\underline{b}_2 + a_3\underline{b}_3 + a_4\underline{b}_4$ όπου $\underline{b}_1$, $\underline{b}_2$, $\underline{b}_3$, $\underline{b}_4$ οι γραμμές του πίνακα R_3 τότε έχουμε ότι $a_1 = c_1 + c_5 = c_2 + c_6 = c_3 + c_7 = c_4 + c_8$.

Υπολογίζουμε το a_1:

$a_1 = x_1 + x_5 = 0$
$a_1 = x_2 + x_6 = 0$
$a_1 = x_3 + x_7 = 0$
$a_1 = x_4 + x_8 = 1$

Συνεπώς, αποκωδικοποιούμε στο $a_1 = 0$. Ομοίως για το a_2:

$a_2 = x_1 + x_3 = 1$
$a_2 = x_2 + x_4 = 0$
$a_2 = x_5 + x_7 = 1$
$a_2 = x_6 + x_8 = 1$

Συνεπώς, αποκωδικοποιούμε στο $a_2 = 1$. Ομοίως για το a_3:

$a_3 = x_1 + x_2 = 0$
$a_3 = x_3 + x_4 = 1$
$a_3 = x_5 + x_6 = 0$
$a_3 = x_7 + x_8 = 0$

Συνεπώς, αποκωδικοποιούμε στο $a_3 = 0$.

Στη συνέχεια, υπολογίζουμε το $\underline{x} - \underline{\delta} = \underline{x} - a_1\underline{b}_1 - a_2\underline{b}_2 - a_3\underline{b}_3 = 11011100 - 00110011 = 11\ 10\ 11\ 11$. Άρα, $w(\underline{x} - \underline{\delta}) = 7 > 1 = 2^{3-2} - 1$, ενώ $(\underline{x} - \underline{\delta})^c = 00\ 01\ 00\ 00$ και $w((\underline{x} - \underline{\delta})^c) = 1 \leq 1$. Συνεπώς, αποκωδικοποιούμε $a_4 = 1$. Τελικά, $\underline{c} = \underline{b}_2 + \underline{1} = 00\ 11\ 00\ 11 + 11\ 11\ 11\ 11 = 11\ 00\ 11\ 00$.