Wykład 5.

5.1 Funkcje boolowskie

Niech m będzie ustaloną liczbą naturalną. Funkcją boolowską (m zmiennych) nazywamy dowolną funkcję $f : (Z_2)^m \to Z_2$.

Jak każdą funkcję określoną w zbiorze skończonym, funkcję boolowską f możemy definiować za pomocą tabelki

	0	1	2	3	4	...	$2^m - 1$
x_1	0	1	0	1	0	...	1
x_2	0	0	1	1	0	...	1
x_3	0	0	0	0	1	...	1
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$			$\vdots$
x_m	0	0	0	0	0	...	1
f	f_0	f_1	f_2	f_3	f_4	...	f_{2^m-1}

W tej tabelce, w ostatnim wierszu są podane wartości, jakie funkcja f przyjmuje dla odpowiednich układów argumentów. Tak więc

$$f(x_1, \ldots, x_m) = f_i$$

wtedy i tylko wtedy, gdy ciąg $x_m, \ldots, x_1$ składa się z kolejnych cyfr przedstawienia dwójkowego liczby i. Nietrudno zauważyć, że funkcja f jest jednoznacznie wyznaczona przez ciąg $f_0, \ldots, f_{2^m-1}$ i odwrotnie, każdy taki ciąg wyznacza jednoznacznie pewną funkcję boolowską. W ten sposób zdefiniowaliśmy wzajemnie jednoznaczną odpowiedniość między funkcjami boolowskimi $f : (Z_2)^m \to Z_2$ i ciągami ze zbioru $(Z_2)^{2^m}$ (lub zerojedynkowymi słowami długości 2^m).

5.2 Funkcje boolowskie jako wielomiany

Funkcje o wartościach w dowolnym ciele, a więc także w ciele Z_2, możemy dodawać i mnożyć. Te działania w zbiorze funkcji definiujemy jak zwykle wzorami

$$(f + g)(x_1, \ldots, x_m) = f(x_1, \ldots, x_m) + g(x_1, \ldots, x_m)$$

oraz

$$(f \cdot g)(x_1, \ldots, x_m) = f(x_1, \ldots, x_m) \cdot g(x_1, \ldots, x_m).$$

Jeżeli funkcje f i g wyznaczają (są reprezentowane przez) słowa $f_0 \ldots f_{2^m-1}$ oraz $g_0 \ldots g_{2^m-1}$, to suma $f + g$ wyznacza słowo

$$(f_0 + g_0) \ldots (f_{2^m-1} + g_{2^m-1}),$$

a iloczyn $f \cdot g$ słowo

$$(f_0 \cdot g_0) \ldots (f_{2^m-1} \cdot g_{2^m-1}).$$

Funkcje stałe, przyjmujące stale wartości 0 i 1, wyznaczają słowa $00\ldots0$ i $11\ldots1$. Zauważmy także, że funkcja $f(x_1,\ldots,x_m) = x_1$ (oznaczana często symbolem x_1) wyznacza słowo $01010101\ldots0101$. Podobnie, funkcja x_2 wyznacza słowo $00110011\ldots0011$. Wobec tego, iloczyn tych funkcji wyznacza słowo $00010001\ldots0001$. Zauważmy, że jeżeli rozważamy funkcję f o wartościach w ciele Z_2, to $f+f=0$ oraz $f\cdot f=f$.

Jednomianem stopnia r nazywamy iloczyn r różnych zmiennych, a więc funkcję postaci $x_{i_1}\cdot\ldots\cdot x_{i_r}$, przy czym żadna zmienna w podanym wzorze nie występuje dwukrotnie. Jednomianami stopnia 0 są funkcje stałe. Wielomianem stopnia $\leqslant r$ nazywamy sumę jednomianów stopnia nie przekraczającego r.

Lemat 5.1 *Odległość Hamminga niezerowego jednomianu stopnia r od zera (czyli waga jednomianu stopnia r) wynosi 2^{m-r}.*

Dowód. Rozważmy jednomian $x_{i_1}\cdot\ldots\cdot x_{i_r}$. Przyjmijmy, że funkcja x_i wyznacza słowo $a_{i,0}a_{i,1}\ldots a_{i,2^m-1}$. Zauważmy, że $a_{i,j}=1$ wtedy i tylko wtedy, gdy w przedstawieniu dwójkowym liczby j występuje składnik 2^{i-1}. Niech rozważany jednomiam wyznacza słowo $b_0b_1\ldots b_{2^m-1}$. Wobec tego dla $j=0,\ldots,2^m-1$ warunek $b_j=1$ jest równoważny temu, że dla $k=1,\ldots,r$ zachodzą równości $a_{i_k,j}=1$, a to z kolei oznacza, że w przedstawieniu liczby j występują składniki $2^{i_1-1},\ldots,2^{i_r-1}$. Tak więc odległość Hamminga rozważanego jednomianu od zera jest równa liczbie tych liczb z przedziału od 0 do 2^m-1, w których przedstawieniach występują składniki $2^{i_1-1},\ldots,2^{i_r-1}$. Nietrudno sprawdzić, że takich liczb jest 2^{m-r}. □

Lemat 5.2 *Każda funkcja boolowska jest wielomianem.*

Dowód. Korzystając z zasady indukcji, wyprowadzamy to z wzoru

$$f(x_1,\ldots,x_m) = f(x_1,\ldots,x_{m-1},0) + (f(x_1,\ldots,x_{m-1},0) + f(x_1,\ldots,x_{m-1},1))\cdot x_m. \ \Box$$

Wniosek 5.3 *Niezerowe jednomiany tworzą bazę przestrzeni $(Z_2)^{2^m}$.*

Dowód. Nietrudno zauważyć, że jest 2^m niezerowych jednomianów. Z poprzedniego lematu wynika, że generują przestrzeń $(Z_2)^{2^m}$. Tworzą bazę, ponieważ $(Z_2)^{2^m}$ ma wymiar 2^m. □

5.3 Kody Reeda-Mullera

Kodami Reeda-Mullera nazywamy zbiory $\mathcal{R}(r,m)$ wielomianów (m zmiennych) stopnia $\leqslant r$.

Zauważmy, że $\mathcal{R}(0,m)$ jest kodem powtórzeniowym długości 2^m.

Lemat 5.4 *Kod $\mathcal{R}(r,m)$ jest kodem liniowym (czyli podprzestrzenią liniową) wymiaru*

$$\sum_{i=0}^{r}\binom{m}{i}.$$

Dowód. Liczba podana w tezie lematu jest liczbą niezerowych jednomianów stopnia $\leqslant r$. Jednomiany te generują zbiór $\mathcal{R}(r,m)$. Z wniosku 5.3 wynika, że każdy zbiór niezerowych jednomianów jest liniowo niezależny. □

Lemat 5.5 *Kod $\mathcal{R}(m-1,m)$ jest równy*

$$\{(x_0,\ldots,x_{2^m-1})\in Z_2^{2^m} : \sum_{i=0}^{2^m-1} x_i = 0\}.$$

Dowód. Porównywane zbiory są przestrzeniami tego samego wymiaru. Ponadto, na podstawie lematu 5.1, wszystkie jednomiany generujące $\mathcal{R}(m-1,m)$ należą do drugiego z wymienionych zbiorów. Stąd wynika równość tych zbiorów. □

Lemat 5.6 $\mathcal{R}(r,m)^\perp = \mathcal{R}(m-r-1,m)$.

Dowód. Z lematu 5.4 i wniosku 3.7 wynika, że przestrzeń $\mathcal{R}(r,m)^\perp$ ma wymiar

$$2^m - \sum_{i=0}^{r}\binom{m}{i} = \sum_{i=0}^{m}\binom{m}{i} - \sum_{i=0}^{r}\binom{m}{i} = \sum_{i=r+1}^{m}\binom{m}{i} = \sum_{i=r+1}^{m}\binom{m}{m-i} = \sum_{i=0}^{m-r-1}\binom{m}{i}.$$

Tak więc obie przestrzenie wymienione w tezie lematu mają ten sam wymiar. Pokażemy jeszcze, że $\mathcal{R}(m-r-1,m)\subseteq\mathcal{R}(r,m)^\perp$.

Weźmy $f\in\mathcal{R}(m-r-1,m)$ oraz $g\in\mathcal{R}(r,m)$. Aby dowieść podane zawieranie wystarczy wykazać, że iloczym skalarny f i g jest równy 0. Zauważmy, że iloczyn $f\cdot g$ (zwykły) wielomianów f i g należy do $\mathcal{R}(m-1,m)$. Po zsumowaniu współrzednych tego iloczynu otrzymujemy iloczyn skalarny. Z lematu 5.5 wynika, że po zsumowaniu współrzędnych wektora należącego do $\mathcal{R}(m-1,m)$ otrzymujemy 0. □

5.4 Geometria w przestrzeni $(Z_2)^m$

Elementy przestrzeni $(Z_2)^m$ możemy uważać za przedstawienia dwójkowe liczb od 0 do 2^m-1. Przyjmijmy, że p_j oznacza punkt przestrzeni $(Z_2)^m$ odpowiadający odwróconemu przedstawieniu liczby j.

Niech $K\subseteq Z_2^m$ będzie podprzestrzenią liniową wymiaru r. Wtedy zbiory $\vec{a}+K=\{\vec{a}+\vec{x} : \vec{x}\in K\}$ nazywamy przestrzeniami afinicznymi wymiaru r.

Przestrzenie afiniczne wymiaru 1 nazywamy prostymi, a wymiaru $m-1$ – hiperpłaszczyznami. Punkty (zbiory jednoelementowe) są przestrzeniami afinicznymi wymiaru 0.

Lemat 5.7 *Każda przestrzeń afiniczna daje się zdefiniować jako zbiór rozwiązań pewnego układu równań liniowych, a więc jako zbiór postaci $\{\vec{x} : H\vec{x}^T=\vec{c}^T\}$.*

Dowód. Weźmy przestrzeń afiniczną $\vec{a}+K$. Z wniosku 3.9 wynika, że $K=\{\vec{x} : H\vec{x}^T=\vec{0}^T\}$. Niech $\vec{c}^T=H\vec{a}^T$. Zauważmy, że

$$\vec{a}+K=\{\vec{x} : H\vec{x}^T=\vec{c}^T\}. \ \square$$

Funkcją charakterystyczną zbioru $X\subseteq Z_2^m$ nazywamy funkcję $f_X : Z_2^m\to Z_2$ spełniającą równoważność

$$x_1\ldots x_m\in X \Leftrightarrow f_X(x_1,\ldots,x_m)=1.$$

Słowo $f_0f_1\ldots f_{2^m-2}f_{2^m-1}\in\{0,1\}^{2^m}$ reprezentuje funkcję f_X, jeżeli warunek $f_j=1$ zachodzi wtedy i tylko wtedy, gdy $p_j\in X$.

Twierdzenie 5.8 *Funkcja charakterystyczna r wymiarowej przestrzeni afinicznej jest wielomianem stopnia $\leqslant m - r$.*

Dowód. Niech

$$L = \{\vec{x} : H\vec{x}^T = \vec{c}\}$$

będzie r wymiarową przestrzenią afiniczną. Możemy założyć, że H ma $m - r$ wierszy i m kolumn. Przyjmijmy, że

$$H = \left[\begin{array}{cccc} a_{1,1} & a_{1,2} & \dots & a_{1,m} \\ a_{2,1} & a_{2,2} & \dots & a_{2,m} \\ & \vdots & & \\ a_{m-r,1} & a_{m-r,2} & \dots & a_{m-r,m} \end{array} \right].$$

Mamy więc, że

$$(x_1, \dots, x_m) \in L \Leftrightarrow \sum_{i=1}^{m} a_{j,i}x_i = c_j \text{ dla } j = 1, \dots, m - r.$$

Zauważmy, że

$$(x_1, \dots, x_m) \in L \Leftrightarrow \prod_{j=1}^{m-r} (\sum_{i=1}^{m} a_{j,i}x_i + c_j + 1) = 1.$$

Wobec tego funkcja

$$f(x_1, \dots, x_m) = \prod_{j=1}^{m-r} (\sum_{i=1}^{m} a_{j,i}x_i + c_j + 1)$$

jest funkcją charakterystyczną L i jednocześnie jest wielomianem stopnia $\leqslant m - r$. □

Lemat 5.9 *Przestrzeń $\mathcal{R}(r, m)$ jest generowana przez funkcje charakterystyczne przestrzeni afinicznych wymiaru $\geqslant m - r$.*

Dowód. Rozważmy przestrzeń afiniczną $L_i = \{(a_1, \dots, a_m) : a_i = 1\}$. Nietrudno spostrzec, że funkcją charakterystyczną L_i jest x_i. Jest też oczywiste, że L_i ma wymiar $m - 1$.

Niech $L = \{(a_1, \dots, a_m) : a_{i_1} = 1 \wedge \dots \wedge a_{i_s} = 1\}$ dla pewnego ciągu parami różnych liczb $i_1, \dots, i_s$. Oczywiście, $L = L_{i_1} \cap \dots \cap L_{i_s}$. Jest też oczywiste, że L ma wymiar $m - s$, oraz że $x_{i_1} \cdot \dots \cdot x_{i_s}$ jest funkcją charakterystyczną L. □

Wniosek 5.10 *Funkcje charakterystyczne przestrzeni afinicznych wymiaru $r + 1$ należą do $\mathcal{R}(r, m)^\perp$.* □

5.5 Dwie własności kodów Reeda-Mullera

Dla ustalonej pary słów $x \in \mathcal{R}(r, m)$ i y definiujemy pojęcie parzystości. Zbiór $X \subseteq Z_2^m$ nazywamy x, y-parzystym, jeżeli zbiór

$$\{i < 2^m : p_i \in X \wedge x_i \neq y_i\}$$

ma parzystą liczbę elementów. Często zbiory x, y-parzyste nazywamy krótko parzystymi.

Lemat 5.11 *Niech L będzie $r+1$ wymiarową przestrzenią afiniczną oraz niech $x = x_0 \ldots x_{2^m-1} \in \mathcal{R}(r,m)$. Dla dowolnego $y = y_0 \ldots y_{2^m-1}$, zbiór*

$$\{i < 2^m : p_i \in L \wedge x_i \neq y_i\}$$

ma parzystą liczbę elementów wtedy i tylko wtedy, gdy iloczyn skalarny $y \cdot f_L$ jest równy 0.

Dowód. Jeżeli $y \in \mathcal{R}(r,m)$, to $y \cdot f_L = 0$ na podstawie wniosku 5.10. Zauważmy także, że jeżeli $p_i \in L$, to zmiana i-tej litery słowa y powoduje zmianę iloczynu $y \cdot f_L = 0$. Wobec tego jeżeli słowo y różni się od słowa kodowego x na parzystej liczbie pozycji i takich, że $p_i \in L$, to $y \cdot f_L = 0$, a jeżeli różni się na nieparzystej, to $y \cdot f_L = 1$. $\square$

Będziemy teraz próbować określać parzystość przestrzeni afinicznych wymiaru $\leqslant r$.

Lemat 5.12 *Przypuśćmy, że mamy dwie przestrzenie afiniczne takie, że $\vec{a} + K \subseteq \vec{b} + K'$. Wtedy $\vec{b} + K' = \vec{a} + K'$ oraz $K \subseteq K'$.*

Dowód. Jeżeli $\vec{a}+K \subseteq \vec{b}+K'$, to $\vec{a} = \vec{b}+\vec{x}$ dla pewnego $\vec{x} \in K'$. Dowolny element przestrzeni $\vec{b} + K'$ jest postaci $\vec{b} + \vec{y}$ dla $\vec{y} \in K'$. Zauważmy, że

$$\vec{b} + \vec{y} = \vec{a} + (\vec{b} - \vec{a}) + \vec{y} = \vec{a} + (\vec{y} - \vec{x}) \in \vec{a} + K'.$$

Podobnie, dowolny element $\vec{a} + \vec{y}$ taki, że $\vec{y} \in K'$ można przedstawić jako

$$\vec{a} + \vec{y} = \vec{b} + (\vec{a} - \vec{b}) + \vec{y} = \vec{a} + (\vec{x} + \vec{y}) \in \vec{b} + K'.$$

Aby dowieść zawieranie $K \subseteq K'$ weźmy $\vec{x} \in K$. Oczywiście $\vec{a}+\vec{x} \in \vec{a}+K \subseteq \vec{b}+K' = \vec{a}+K'$. Wobec tego, $\vec{a}+\vec{x} = \vec{a}+\vec{x}'$ dla pewnego $\vec{x}' \in K'$. Równość $\vec{a}+\vec{x} = \vec{a}+\vec{x}'$ implikuje, że $\vec{x} = \vec{x}'$, a więc $\vec{x} \in K'$. $\square$

Twierdzenie 5.13 *Każda przestrzeń afiniczna $L \subseteq Z_2^m$ wymiaru s jest zawarta w dokładnie $2^{m-s} - 1$ przestrzeniach afinicznych wymiaru $s + 1$. Co więcej, każdy punkt spoza L należy do dokładnie jednej z tych przestrzeni.*

Dowód. Niech L będzie przestrzenią wymiaru s. Na podstawie lematu 5.12 stwierdzamy, że liczba przestrzeni afinicznych wymiaru $s + 1$ zawierających $L = \vec{a} + K$ jest liczbą przestrzeni liniowych wymiaru $s + 1$ zawierających K.

Niech X będzie minimalnym zbiorem generatorów przestrzeni K. Każda przestrzeń wymiaru $s + 1$ zawierająca K jest generowana przez zbiór postaci $X \cup \{\vec{x}\}$ dla pewnego $\vec{x} \notin K$. Weźmy wektory $\vec{x}_1, \vec{x}_2 \notin K$. Zauważmy, że zbiory $X \cup \{\vec{x}_1\}$ oraz $X \cup \{\vec{x}_2\}$ generują tę samą przestrzeń wtedy i tylko wtedy, gdy $\vec{x}_1 - \vec{x}_2 \in K$ (aby to dowieść korzystamy z założenia, że rozważamy przestrzenie nad ciałem Z_2, a więc jedynym niezerowym współczynnikiem jest 1). Tak więc K możemy rozszerzyć do przestrzeni wymiaru większego o 1 na tyle sposobów, ile jest klas abstrakcji relacji R_K różnych od K, czyli na $2^{m-s} - 1$ sposobów.

Przypuśćmy, że $\vec{x} \notin \vec{a} + K$ oraz $\vec{x} \in (\vec{a} + K_1) \cap (\vec{a} + K_2)$ dla pewnych przestrzeni wymiaru $s + 1$ zawierających K. Tak więc $\vec{x} = \vec{a} + \vec{y}_1 + \vec{z}_1 = \vec{a} + \vec{y}_2 + \vec{z}_2$ dla pewnych $\vec{y}_1, \vec{y}_2 \in K$ oraz $\vec{z}_1 \in K_1 \setminus K$ i $\vec{z}_2 \in K_2 \setminus K$. Wektory $\vec{z}_1$ i $\vec{z}_2$ są różne od 0, gdyż w przeciwnym razie $\vec{x} \in L$. Zauważmy, że $K \cup \{\vec{z}_i\}$ generuje przestrzeń K_i dla $i = 1, 2$. Ponadto, $\vec{z}_1 - \vec{z}_2 \in K$. Wobec tego $K_1 = K_2$. $\square$

Wniosek 5.14 *Jeżeli $x \in \mathcal{R}(r,m)$ i $y \in S_{2^{m-r-1}-1}(x)$, to dla każdej przestrzeni afinicznej L wymiaru s, $0 \leqslant s \leqslant r$, większość przestrzeni afinicznych wymiaru $s+1$ zawierających L ma tę samą parzystość, co L.*

Dowód. Rozważmy zbiór $X = \{i < 2^m : p_i \notin L \wedge x_i \neq y_i\}$. Na podstawie założenia o y zbiór ten ma najwyżej $2^{m-r-1} - 1$ elementów. Zauważmy, że jeżeli L' jest przestrzenią afiniczną wymiaru $s+1$, zawierającą L, ale nie zawierającą elementów p_i dla $i \in X$, to

$$\{i < 2^m : p_i \in L \wedge x_i \neq y_i\} = \{i < 2^m : p_i \in L' \wedge x_i \neq y_i\},$$

a więc w tym przypadku przestrzenie L i L' albo jednocześnie są, albo nie są parzyste. Oznacza to, że przynajmniej $2^{m-s}-1-(2^{m-r-1}-1)$ nadprzestrzeni przestrzeni L ma tę samą parzystość, co L. Teza wynika z nierówności

$$2^{m-s} - 1 - (2^{m-r-1} - 1) \geqslant 2^{m-r} - 1 - (2^{m-r-1} - 1) = 2^{m-r-1} > 2^{m-r-1} - 1. \quad \square$$

5.6 Algorytm dekodujący dla kodów Reeda-Mullera

Ustalone fakty sugerują następującą postać algorytmu dekodującego dla kodu $\mathcal{R}(r,m)$:

Dane: słowo $y \in Z_2^{2^m}$;

1. **dla każdej przestrzeni afinicznej $L \subseteq Z_2^m$ wymiaru $r+1$ zapamiętaj, czy iloczyn skalarny y i f_L jest równy 0** (przestrzenie wymiaru $r+1$ spełniające podany warunek będziemy nazywać y-parzystymi);

2. **dla i zmieniającego się od r do 0**

   dla każdej przestrzeni afinicznej $L \subseteq Z_2^m$ wymiaru i, ustal liczbę P przestrzeni afinicznych wymiaru $i+1$, które zawierają L i są y-parzyste, oraz liczbę N pozostałych przestrzeni afinicznych wymiaru $i+1$ zawierających L, oraz zapamiętaj, czy dla L spełniony jest warunek $P > N$ (przestrzenie wymiaru i spełniające podany warunek $P > N$ będziemy dalej nazywać y-parzystymi);

3. **dla i zmieniającego się od 0 do $2^m - 1$**

   jeżeli przestrzeń afiniczna $\{p_i\}$ nie jest y-parzysta, to zmień i-tą literę słowa y (literę a zastąp przez $1-a$);

4. **zwróć słowo otrzymane w ten sposób ze słowa y.**

Podany algorytm będziemy oznaczać symbolem $\mathcal{A}(r,m)$. Oczywiście, algorytm ten nie jest precyzyjnie opisany. W pierwszym rzędzie należy uzupełnić go o szczegóły związane z implemantacją pojęcia przestrzeni afinicznej. Zakładamy, że potrafimy to zrobić w taki sposób, że mając implementacje przestrzeni L_1 i L_2 jesteśmy w stanie poprawnie obliczyć funkcję charakterystyczną przestrzeni L_1 i ustalić, czy $L_1 \subseteq L_2$. Algorytm $\mathcal{A}(r,m)$ zawsze kończy pracę zwracając pewne słowo. Przypuśćmy, że po uruchomieniu tego algorytmu ze słowem y otrzymujemy słowo $F_{r,m}(y)$.

Lemat 5.15 *Jeżeli $x \in \mathcal{R}(r,m)$, $y \in S_{2^{m-r-1}-1}(x)$ oraz $0 \leqslant i \leqslant r+1$, to dla każdej przestrzeni afinicznej L wymiaru i, przestrzeń L jest x,y-parzysta wtedy i tylko wtedy, gdy jest y-parzysta.*

Dowód. Aby dowieść ten lemat, analizujemy działanie algorytmu $\mathcal{A}(r,m)$ korzystając z lematu 5.11 i wniosku 5.14. □

Wniosek 5.16 *Jeżeli $x \in \mathcal{R}(r,m)$ i $y \in S_{2^{m-r-1}-1}(x)$, to $F_{r,m}(y) = x$.*

Dowód. Przyjmijmy, że dla dowolnego słowa $a \in Z_2^{2^m}$ symbolem a_j oznaczamy j-tą literę słowa a. Niech $z = F_{r,m}(y)$.

Załóżmy, że $j < 2^m$. Będziemy w równoważny sposób wyrażać warunek $z_j = y_j$. Z opisu algorytmu $\mathcal{A}(r,m)$ wynika, że ta równość jest spełniona wtedy i tylko wtedy, gdy przestrzeń afiniczna $\{p_j\}$ jest y-parzysta. Na podstawie lematu 5.15 stwierdzamy, że jest równoważna x,y-parzystości $\{p_j\}$. Z kolei z definicji pojęcia parzystości otrzymujemy, że jest równoważna należeniu do zbioru $\{i < 2^m : p_i \in \{p_j\} \wedge x_i \neq y_i\}$ parzystej liczby elementów. Zbiór ten jest albo pusty, albo jest równy $\{j\}$ w zależności od tego, czy warunek $x_j = y_j$ jest – lub odpowiednio nie jest – spełniony. Wobec tego, interesująca nas równość zachodzi wtedy i tylko wtedy, gdy zbiór $\{i < 2^m : p_i \in \{p_j\} \wedge x_i \neq y_i\}$ jest pusty, czyli wtedy i tylko wtedy, gdy $x_j = y_j$.

Ostatecznie otrzymujemy, że warunki $z_j = y_j$ oraz $x_j = y_j$ są równoważne dla wszystkich dopuszczalnych j. Ponieważ z_j, x_j i y_j przyjmują najwyżej dwie wartości, wiec mamy $z_j = x_j$ dla dowolnego j. Oznacza to, że $F_{r,m}(y) = z = x$. □

Wniosek 5.17 *Kod $\mathcal{R}(r,m)$ koryguje $2^{m-r-1} - 1$ błędów.*

Dowód. Dla dowodu nie wprost załóżmy, że przekrój $S_{2^{m-r-1}-1}(x_1) \cap S_{2^{m-r-1}-1}(x_2)$ jest niepusty dla pewnej pary różnych słów $x_1, x_2 \in \mathcal{R}(r,m)$. Niech $y \in S_{2^{m-r-1}-1}(x_1) \cap S_{2^{m-r-1}-1}(x_2)$. Aby otrzymać sprzeczność wystarczy zauważyć, że z wniosku 5.16 wynikają równości $x_1 = F_{r,m}(y) = x_2$. □

Wniosek 5.18 *Minimalna odległość od zera słów kodu $\mathcal{R}(r,m)$ jest równa 2^{m-r}.*

Dowód. Jest to oczywiste dla $r = m$. Załóżmy więc, że $r < m$. Jeżeli kod $\mathcal{R}(r,m)$ koryguje $2^{m-r-1} - 1$ błędów, to minimalna odległość od zera słów kodowych jest $\geqslant 2 \cdot (2^{m-r-1} - 1) + 1 = 2^{m-r} - 1$. Z lematu 5.5 i oczywistego zawierania $\mathcal{R}(r,m) \subseteq \mathcal{R}(m-1,m)$ wynika, że słowa ze zbioru $\mathcal{R}(r,m)$ mają parzystą liczbę jedynek. Stąd minimalna odległość od zera słów kodu $\mathcal{R}(r,m)$ jest parzysta, a więc $\geqslant 2^{m-r}$. Nierówność przeciwna wynika z lematu 5.1. □