הוכחה:

א) כמובן $0 \le d(x,y)$ (מספר איברים בקבוצה)
$d(x,y)=0 \iff (\forall i)\ x_i=y_i \iff x=y$.

ב) ברור.

ג) נסמן:

$$I := \{i \mid x_i \neq z_i\}$$

$$J := \{i \mid z_i \neq y_i\}$$

ברור שאם $x_i=z_i$ וגם $z_i=y_i$, אז $x_i=y_i$.
לכן, $\{i \mid x_i \neq y_i\} \subseteq I \cup J$

$$d(x,y) = \#\{i \mid x_i \neq X_i] \underbrace{\le}_{|I\cup J| \le} |I|+|J| = d(x,z)+d(z,y)$$

מרחק המינג מתאר את הסתברויות המעבר בין מילים בערוץ בינארי סימטרי.

$$P\left[\begin{matrix}\text{לקבל}\\ y\end{matrix} \;\middle|\; \begin{matrix}\text{שודר}\\ x\end{matrix}\right] = p^{d}(1-p)^{n-d} \qquad (d=d(x,y))$$

ההסתברות תלויה רק במרחק ($d=d(x,y)$).

הגדרה:
המרחק distance של קוד $C \subseteq A^n$ הוא
$d(C) := \min\{d(x,y) \mid x,y \in C,\ x \neq y\}$

טענה:
אם $d=d(C)$ אז הקוד C יכול לגלות עד $d-1$ שגיאות ולתקן עד $t=\left\lfloor \frac{d-1}{2} \right\rfloor$ שגיאות (בכל מילת קוד משודרת).

הוכחה:
נניח ששודרה מילה x (לא ידועה) והתקבלה מילה y (ידועה).
ידוע למקבל: $x \in C$ (אבל x עצמה לא ידועה).
אם נפלו בין 1 ל-$d-1$ שגיאות בהכרח $y \notin C$ (כי אם $x,y \in C$ אז או $x=y$ (0 שגיאות) או $d(x,y) \ge d$ (לפחות d שגיאות))
לכן בהינתן y והבחנה שידוע שנפלו בין 0 ל-$(d-1)$ שגיאות:
אם $y \in C$ אז לא נפלו שגיאות. $(y=x)$.
אם $y \notin C$ אז בוודאי נפלו שגיאות.

~~לגבי תיקון~~

הראינו שאם נפלו עד $d-1$ שגיאות, אפשר לגלות שנפלו שגיאות.
מצד שני, אם נפלו d שגיאות אז יש מצבים בהם לא ניתן לגלות זאת, למשל אם ניקח $x,y \in C$ עם $d(x,y)=d$ (קיימים כאלו) אז כשנקבל y לא נדע אם שודר x או שודר y.
(יש שגיאות) (אין שגיאות)

באופן דומה לגבי תיקון שגיאות:
נניח שקבלנו y, וידוע לנו שנפלו לא יותר מ- $t=\left\lfloor \frac{d-1}{2} \right\rfloor$ שגיאות. במצב כזה לא יתכן שיש יותר ממועמד אחד לפיענוח, כי אם $x_1,x_2 \in C$ כך ש-
$d(x_1,y) \le t$
$d(x_2,y) \le t$

מכאן נסיק, לפי אי שוויון המשולש (וסימטריה):

$$d(x_1,x_2) \le d(x_1,y)+d(y,x_2) \le t+t=2t \le d-1 \;\text{\textcircled{$<$}}\; \underline{\underline{d}}$$

כי min
לפי הגדרת המרחק $d=d(C)$ נקבל בהכרח $x_1=x_2$ לכן הפענוח (אם קיים) הוא יחיד.