

אנו רוצים לפתור שתי בעיות:

1. הבעיה הראשונה מוגדרת באופן הבא - בהינתן סט איברים $\{a_1, a_2, \dots, a_{dc-1}\}$, שמקבלים ערכים 2^k כך ש $k \in \{0, 1, \dots, \log_2(q)\}$, כלומר האיברים שלנו מהצורה $\{2^{k_1}, 2^{k_2}, \dots, 2^{k_{dc-1}}\}$, אנו מעוניינים למצוא, בהינתן $1 \leq m \leq q$ כמה קומבינציות אפשריות יש כך ש $\max(q, \prod_{i=1}^{dc-1} a_i) = m$. למשל עבור $dc = 4$ ו $q = 4$ ובהינתן $m = 1$ אז יש בדיוק קומבינציה אחת שנותנת את הדרישה והיא $\{1, 1, 1\}$ (כי $1 \cdot 1 \cdot 1 = 1$) לעומת זאת עבור $m = 2$ יש 3 אפשרויות, למשל $\{1, 2, 1\}$ (כי $1 \cdot 2 \cdot 1 = 2$), אך עבור $m = 4$ יש יותר אפשרויות ובין היתר יש שם את האיבר $\{4, 1, 1\}$ וכן האיבר $\{2, 1, 2\}$. עבור המקרה שבוא המכפלה יוצאת יותר קטנה מ q , ניתן לכתוב את הבעיה בצורה אחרת - $a_1 \cdot a_2 \cdot \dots \cdot a_{dc-1} = 2^{k_1} \cdot 2^{k_2} \cdot \dots \cdot 2^{k_{dc-1}} = m = 2^b$ (כאשר $0 \leq b \leq \log_2(q)$) כלומר נקבל $2^{k_1+k_2+\dots+k_{dc-1}} = 2^b$ וקיבלנו את המשוואה $\sum_{i=1}^{dc-1} k_i = b$, שאותה אנו יודעים לפתור על ידי פתרון משוואה בשלמים, שהפתרון שלה הוא -

$$D(dc-1, b) = \binom{dc-1-1+b}{b}$$

עבור $0 \leq k_i, b \leq \log_2(q)$. עבור המקרה שבוא המכפלה יוצאת q או מספר יותר גדול, אפשר לחשב את המקרה הזה על ידי חיסור פשוט של כל הקומבינציות האפשריות שיש לסידור $dc-1$ איברים כשכל אחד מהם יכול לקבל $\log_2(q) + 1$ קומבינציות אפשריות $((\log_2(q) + 1)^{dc-1})$ מכל שאר הקומבינציות שכבר חישבנו. לכן ניתן כעת ניתן לפתור ולקבל את \tilde{P}_i שמסמן את כמות האיברים שאנו מחפשים שמקיימים את התנאי ש $2^i = \max(q, \prod_{j=1}^{dc-1} a_j)$

$$\tilde{P}_i = \begin{cases} \binom{dc-2+i-1}{i-1} & 0 \leq i \leq \log_2(q) \\ (\log_2(q) + 1)^{dc-1} - \sum_{j=1}^{\log_2(q)} \tilde{P}_j & i = \log_2(q) + 1 \end{cases}$$

1

2. הבעיה השנייה מוגדרת באופן הבא - בהינתן סט איברים $\{a_1, a_2, \dots, a_{dv-1}\}$, שמקבלים ערכים 2^k כך ש $k \in \{0, 1, \dots, \log_2(q)\}$, אנו מעוניינים למצוא, בהינתן $1 \leq m \leq q$ כמה קומבינציות אפשריות יש כך $\min(a_i) = m$. למשל עבור $dc = 4$ ו $q = 4$ ובהינתן $m = 4$ אז יש בדיוק קומבינציה אחת שנותנת את הדרישה והיא $\{4, 4, 4\}$ (כי $\min(4, 4, 4) = 4$) לעומת זאת עבור $m = 3$ יש יותר אפשרויות, כי למשל גם $\{3, 3, 3\}$ מקיים את התנאי וכמו כן $\{4, 4, 3\}$ וכן $\{3, 3, 4\}$. כעת המצב הרבה יותר פשוט כי אנו מחפשים את המינימום, כלומר שמבין כל ה $dv-1$ האופציות למספרים השייכים ל $\{2^k | k \in \{0, 1, \dots, \log_2(q)\}\}$, אנו רוצים שהמינימאלי מהם יהיה 2^i . ראשית נחשב כמה דרכים יש לבחור $dv-1$ מספרים כך שכל המספרים יהיו לפחות 2^i - שזה $(\log_2(q) + 1 - (i+1) + 1)^{dv-1}$ (עבור $k \in \{0, 1, \dots, \log_2(q)\}$ ונחסיר מזה את כל האפרויות שכל המספרים יהיו

¹ניתן לשים לב ש \tilde{P}_i מתאר גודל קבוצה באורך של 2^{i-1} .

גדולים/שווים ל 2^{i+1} - שזה $(\log_2(q) + 1 - (i + 1))^{dv-1}$. כעת ניתן להגדיר את \tilde{Q}_i להיות כמות האיברים שאנו מחפשים שמקיימים ש $\min_{j=1}^{dv-1} \{a_j\} = 2^i$

$$\tilde{Q}_i = (\log_2(q) - i + 1)^{dv-1} - (\log_2(q) - i)^{dv-1}$$

וכמו מקודם הביטוי מוגדר עבור $0 \leq i \leq \log_2(q)$

נשים לב שאם כעת נרצה למצוא את אחוז האיברים שיש ב $\tilde{P}_{\log_2(q)+1}$ ביחס לכל האיברים האפשריים נקבל את הביטוי -

$$\frac{(\log_2(q) + 1)^{dc-1} - \sum_{j=1}^{\log_2(q)} \binom{dc-3+j}{j-1}}{(\log_2(q) + 1)^{dc-1}} = 1 - \frac{\sum_{j=1}^{\log_2(q)} \binom{dc-3+j}{j-1}}{(\log_2(q) + 1)^{dc-1}}$$

שהוא מונוטוני עולה כתלות ב q וכן כל הביטוי שואף ל 1 עבור $q \rightarrow \infty$. לדוגמה, עבור $dc = 6$ נקבל -

$$\begin{aligned} q = 4 & : 0.9136 \\ q = 8 & : 0.9453 \\ q = 64 & : 0.9725 \end{aligned}$$