NOMBRE: Lucas Aguilera Gómez SIGLA: IIC3253

N° ALUMNO: 20643039

Pontificia Universidad Católica de Chile
Escuela de Ingeniería
Departamento de Ciencia de la Computación

IIC3253 — Criptografía y seguridad computacional — 1' 2025

Tarea 3 – Respuesta Pregunta 2

(a) Para demostrar esto tenemos que entender la propiedad fundamental de los conjuntos súper crecientes: Cada elemento w_k es mayor que la suma de todos los elementos anteriores (como dice el enunciado). Esto es una propiedad extremadamente fuerte pues implica que este conjunto puede "definir" a un numero b de solo una forma (si es que puede), la lógica es la siguiente: "En caso de incluir en la suma a un numero del conjunto, automáticamente estamos haciendo mas de lo que podríamos haber hecho sin él, por tanto, el proceso es único", esto es demostrable formalmente por contradicción:

Asumamos que existen mas de un conjunto $I \subseteq S$ que cumpla el SUBSET-SUM para un b. Por ejemplo, 2 subconjuntos distintos $I \neq J$ tal que: $I \subseteq S$, $J \subseteq S$ y:

$$\sum_{a \in I} a = b = \sum_{a \in J} a$$

Como sabemos que $I \neq J$ entonces debe existir al menos un elemento diferente entre ambos conjuntos, o en otras palabras, debe haber al menos un elemento que está en un conjunto pero no en el otro.

Tomemos al mayor elemento w_k que está en uno de los dos conjuntos y no en el otro. Por ejemplo entre: $\{a, c, d\}$ y $\{a, b, e\}$, tomaríamos e (para este ejemplo estamos asumiendo que los subconjuntos están ordenados y fueron tomados de un conjunto súper creciente).

Luego, sin perdida de generalidad, supongamos que $w_k \in I$ pero $w_k \notin J$ (sin perdida de generalidad porque para fines de la demostración, el caso inverso sería lo mismo).

Ahora, notemos que como w_k es el elemento mas grande que diferencia a ambos conjuntos, cualquier elemento w_i donde $k < i$ (es decir, todo w_i mayor que w_k) debe estar en ambos conjuntos, o en su defecto, no estar en ninguno (recordar que estamos asumiendo que los conjuntos están ordenados). Nota sobre notación: De ahora en adelante, cuando me refiera a $w_i, i < k$ me refiero a todos los elementos w_i que son menores que w_k.

Notemos entonces que podemos separar la suma de elementos de los subconjuntos de la siguiente forma:

$$\sum_{w_i \in I,\, i>k} w_i + w_k + \sum_{w_i \in I,\, i<k} w_i = \sum_{w_i \in J,\, i<k} w_i + \sum_{w_i \in J,\, i>k} w_i$$

Y como dije anteriormente, podemos simplificar $\sum_{w_i \in I,\, i>k} w_i$ y $\sum_{w_i \in J,\, i>k} w_i$ puesto que ambas o dan 0, o dan el mismo valor. Luego nos quedamos con:

$$w_k + \sum_{w_i \in I,\, i<k} w_i = \sum_{w_i \in J,\, i<k} w_i$$

Y luego despejando para w_k:

$$w_k = \left(\sum_{w_i \in J,\, i<k} w_i \right) - \left(\sum_{w_i \in I,\, i<k} w_i \right)$$

Ahora, en el caso mas extremo para el valor de w_k, tendríamos que J tiene todos los elementos desde w_1 a w_{k-1}, e I no tiene ningún elemento menor a w_k por tanto es 0. Entonces, el mayor valor posible para $\sum_{w_i \in J,\, i<k} w_i$ sigue:

$$\sum_{w_i \in J,\, i<k} w_i \leq \sum_{i=1}^{k-1} w_i$$

Luego combinando lo anterior tendríamos que w_k cumple:

$$w_k \leq \sum_{i=1}^{k-1} w_i$$

Pero esto es un contradicción: w_k no debería poder ser menor o igual que la suma de los elementos anteriores, puesto que forma parte de S el cual es súper creciente, y por tanto debería cumplirse $w_k > \sum_{i=1}^{k-1} w_i$.

Como la suposición inicial nos lleva a una contradicción, entonces la suposición inicial debe ser falsa, y por lo tanto, no pueden existir dos subconjuntos distintos que sumen el mismo valor b. Solo puede existir a lo mas uno.

Hay otra forma bastante mas directa de hacer esta demostración:

Una vez definido que $w_k \in I$ pero $w_k \notin J$, sabemos que:

$$\sum_{a \in I} a > \sum_{a \in J} a$$

porque por definición: $w_k > \sum_{i=1}^{k-1} w_i$, entonces ningún subconjunto de J puede compensar ese valor de w_k. Esto genera una contradicción pues se esperaba que $\sum_{a \in I} a = \sum_{a \in J} a$.

Ambas demostraciones deberían ser validas.

(b) Una forma de abordar esto es mirar lo necesario de "adelante para atrás" e ir viendo si seleccionar un numero o no. Veamos el algoritmo de la siguiente manera (pasos):

(a) Iniciar conjunto vacío $I = \{\}$.

(b) Iteramos desde el elemento mas grande de S (de adelante hacia atrás, asumiendo que S está ordenado).

(c) En cada paso, comparamos el objetivo b con el valor actual que tenemos:

- Si b es mayor o igual que el elemento actual, entonces el elemento actual debe pertenecer a I. Esto es obvio, puesto que sabemos que si w_k actual cumple que $w_k < b$ entonces sabemos que la suma de todos los elementos menores a w_k es por definición menor a w_k, lo que significa que si no incluimos w_k en la solución, nunca alcanzaremos el valor de b. Luego de hacer esto ACTUALIZAMOS el valor de b: b = b - w_k y además añadiremos w_k a I. "Avanzamos" a w_{k-1}. Volvemos al inicio de este paso.
- Si b es menor que el elemento actual, sabemos que, obviamente, el elemento actual w_k NO puede ser parte de la solución y por tanto lo saltamos y "avanzamos" a w_{k-1}. Volvemos al inicio de este paso.

(d) Después de hacer todas las iteraciones y terminar todos los elementos de S, hay que revisar el valor final de b:

- si $b = 0$ entonces encontramos la combinación exacta. El algoritmo retorna I.
- si $b \neq 0$ entonces significa que llegamos al final y no pudimos encontrar los elementos que nos faltaban para hacer que $b = 0$, por tanto no existe solución. El algoritmo retorna que no existe solución.

Notemos que este algoritmo es un algoritmo greedy, y funciona perfecto porque solo puede existir una solución (o ninguna). Como el algoritmo va retrocediendo por cada elemento de S y simplemente se encarga de hacer una comparación (y actualización) simple por cada paso, es de complejidad $O(n)$, donde n es la cantidad de elementos que hay en S.

(c)

(d)