בס״ד

<u>שיבוצים</u>

<u>הגדרה מנגנון נקרא אמיתי</u> אם לכל משתתף, ועבור כל דבר שעושים האחרים, התוצאה הטובה ביותר עבור המשתתף מתקבלת כאשר הוא תמים (- פועל לפי העדפותיו האמיתיות).

<u>תוצאה א נקראת שיפור פארטו של תוצאה ב</u>, אם תוצאה א טובה יותר לחלק מהמשתתפים, וטובה לפחות באותה מידה לכל השאר.

<u>תוצאה נקראת יעילה פארטו</u> אם לא קיימת תוצאה אחרת שהיא שיפור פארטו שלה.

<u>מנגנון נקרא יעיל פארטו</u> אם כל תוצאה שלו היא יעילה פארטו.

<u>האלגוריתם דיקטטורה סדרתית</u>

כל אחד מציין את ההעדפות שלו לכל אחד מהפריטים המוצעים ואסור לו להיות אדיש בין שני מוצרים.

1. עוברים על האנשים לפי התור.
2. נותנים לכל אדם את העדיפות הכי גבוהה שלו ממה שנשאר פנוי.

האלגוריתם אמיתי ויעיל פארטו.

<u>הגדרה שוק דו-צדדי</u> (שידוך)הוא שוק שבו צריך להתאים בין משתתפים משתי קבוצות ,כאשר לכל משתתף מכל אחת מהקבוצות יש העדפות שונות.

<u>הגדרה זוג מערער</u> סטודנט ומחלקה שאינם משודכים, והם מעדיפים זה את זו על פני ה״שידוכים״ הנוכחיים שלהם.

<u>הגדרה שידוך יציב</u> שידוך בלי זוגות מערערים.

<u>משפט</u>: כל שידוך יציב הוא יעיל פארטו.

<u>אלגוריתם ״קבלה על תנאי״:</u>

1. כל סטודנט הולך למחלקה שהוא הכי רוצה, מבין המחלקות שעדיין לא דחו אותו.
2. כל מחלקה ״מקבלת על תנאי״ את הסטודנט שהיא הכי רוצה, מבין אלה שנמצאים בה, ודוחה את כל השאר.
3. חוזרים על שלבים א ו-ב עד שכולם משודכים.

האלגוריתם מסתיים, בשידוך יציב ואופטימלי עבור אלו המציעים את עצמם, ואמיתי עבור הסטודנטים.

<u>משפט</u> לא קיים מנגנון המוצא שידוך יציב, שהוא אמיתי עבור שני הצדדים.

<u>אלגוריתמי החלפה:</u>

<u>הגדרה השתתפות מרצון</u>: מנגנון מקיים השתתפות מרצון אם מצבו של כל משתתף לאחר המנגנון טוב לפחות כמו לפניו.

<u>אלגוריתם מעגלי המסחר:</u>

מאתחלים גרף מכוון שבו:
הצמתים הם האנשים והבתים;
יש קשת מכל אדם לבית שהוא הכי רוצה,
ומכל בית לאדם שגר בו עכשיו.

א. מוצאים מעגל מכוון בגרף.
ב. מבצעים את ההחלפה במעגל.
ג. מוחקים מהגרף את הצמתים שהשתתפו בהחלפה.
ד. מעדכנים את הקשתות של האנשים שנשארו.
ה. חוזרים על שלבים א-ד עד שהגרף ריק.

אלגוריתם זה מקיים את שלושת התכונות:
אמיתיות, השתתפות מרצון ויעילות פארטו (רק שיחסי העדפה חזקים).

<u>קואליציה מערערת</u>: קבוצת משתתפים שיכולה לפרוש ולבצע החלפת-בתים שהיא טובה באותה מידה לכל חברי הקבוצה וטובה יותר לחלק מחברי קבוצה.

<u>שיבוץ יציב</u>: שיבוץ שבו אין קואליציה מערערת.

<u>משפט</u>: אם כל יחסי ההעדפה הם חזקים, אז יש רק שיבוץ יציב אחד(באלגוריתם מעגלי המסחר)

<u>משפט</u>: האלגוריתם לא דואג לך שלא תהיה קנאה.

<u>משפט</u>: אלגוריתם מעגלי המסחר מסתיים.

הוכחה: כל עוד הגרף לא ריק ,קיים לפחות מעגל מכוון אחד .
לכן בכל שלב הגרף קטֵן עד שמתרוקן.

<u>משפט</u>: אלגוריתם מעגלי המסחר מקיים השתתפות מרצון.

הוכחה: כל משתתף מקבל בית שהצביע עליו. כל משתתף יכול להצביע על הבית שלו או על בית טוב יותר.

<u>משפט</u>: אלגוריתם מעגלי המסחר הוא אמיתי.

הוכחה: נניח שיוסי סוחר במעגל k כשהוא תמים ובמעגל j כשהוא מתחכם נשווה בין מצבים אלו בשני מקרים.

- **$j>=k$** המסחר עד מעגל k-1 זהה בשני המצבים. לכן קבוצת הבתים שנשארו זמינים אחרי מעגלk-1 זהה בשני המצבים. וכשיוסי תמים הוא מקבל את הבית הכי טוב בקבוצה זו.
- **$j<k$**. המסחר עד מעגל j-1 זהה בשני המצבים. בסיבוב הבא כל הקשתות זהות בשני המצבים, פרט לקשת היוצאת מיוסי. **כשיוסי מתחכם,** הקשת היוצאת ממנו סוגרת מעגל עם בית כלשהו x . **כשיוסי תמים** ,הוא נמצא בסופה של שרשרת המתחילה בבית x .כל עוד לא נסגר מעגל, כל השרשרת הזאת נשארת בגרף. בפרט, בית x עדיין נמצא בגרף כאשר מעגל k נסגר. לכן הבית שמקבל יוסי כשהוא תמים טוב לפחות כמו.x

<u>משפט</u>: אם כל יחסי ההעדפה הם חזקים (אין אדישות), אז אלגוריתם מעגלי המסחר יעיל פארטו.

הוכחה: בהינתן קלט מסויים, נגדיר:
שיבוץ א – של המנגנון. שיבוץ ב – אחר כלשהו.
נניח בשלילה ש-ב הוא שיפור פארטו של א.
יהי k הקטן ביותר כך שאדם ממעגל k נהנה.
בשיבוץ א, הוא מקבל את הבית הטוב ביותר מהבתים שלא נלקחו ע״י מעגלים $k>j$.
בשיבוץ ב מצבו טוב יותר, כלומר הוא מקבל חדר שבשיבוץ א ניתן לאדם ממעגל $k>j$.
בשיבוץ ב, אדם j מקבל בית אחר גרוע יותר או טוב יותר. אם הוא גרוע יותר - זה לא שיפור פארטו. אם הוא טוב יותר – k לא הראשון.

***

<u>אלגוריתם הפרחים: (עבור מציאת שידוך בגרף)</u>

כל עוד יש מסלול-שיפור: הפוך אותו (ירוק לאדום ואדום לירוק)
מסלול שיפור = מתחיל ומסתיים בצמתים לא משודכים, ומתחלף אדום-ירוק-אדום....-ירוק-אדום.

<u>מנגנון שידוך-גדול-ביותר-עם-עדיפויות:</u>

1. קבע סדר-עדיפות כלשהו על הצמתים (למשל לפי זמן המתנה בתור להשתלה, דחיפות רפואית, גיל, וכד׳).
2. מצא את כל השידוכים הגדולים ביותר בגרף.
3. בחר את השידוך עם וקטור-העדיפויות הגדול ביותר בסדר מילוני.

<u>משפט</u>: קיים מנגנון יעיל פארטו שהוא אמיתי עבור הזוגות. אך לא עבור המרכזים הרפואיים. אולם קיים שידוך בגודל לפחות 1/2 מהגדול ביותר.

<u>הגדרה: מכרז ויקרי</u> (= מכרז מחיר שני) הוא:

1. המשתתפים כותבים הכרזות במעטפות;
2. המעטפות נפתחות ומסודרות בסדר יורד;
3. בעל ההכרזה הגבוהה ביותר זוכה בחפץ;
4. הזוכה משלם את ההכרזה השניה.

<u>משפט</u>: מכרז ויקרי מקיים השתתפות מרצון,אמיתי ויעילות פארטו.

<u>מכרז פרסום(במחיר שני):</u>
מחושב לפי הסתברות הקלקה ומחיר להקלקה.

<u>מכרז מחיר שני מוכלל(GSP):</u>

המפרסם שההכרזה שלו היא ה-j בגובהה, זוכה במקום j, ומשלם את ההכרזה של המפרסם ה-j+1.

<u>משפט</u>: כשיש שני מקומות ויותר, מכרז זה אינו אמיתי.

<u>מכרז VCG(עבור מכרז מחיר שני מכולל):</u>

הנחות:
יש מספר סופי של תוצאות אפשריות.
לכל משתתף יש ערך כספי לכל תוצאה.
המנגנון:
בחר את התוצאה עם סכום-הערכים הגבוה ביותר.
עבור כל שחקן:
חשב את סכום הערכים של שאר השחקנים.(איתו ובלי ערכו)-א׳
חשב את סכום הערכים של שאר השחקנים אילו השחקן הנוכחי לא היה משתתף.(באפשרות שהייתה נבחרת בלעדיו בכלל)-ב׳
גבה מהשחקן את ההפרש בין שני הסכומים. א׳-ב׳.
כלל בחירה-מיקסום סכום ערכים.

<u>משפט</u>: מנגנון ויקרי-קלארק-גרובס הוא אמיתי.

מושגים: ערך = ברוטו (לא כולל המחיר).
תועלת = נטו (ערך פחות מחיר).

<u>הוכחה</u>: התועלת של כל שחקן היא:
הערך של השחקן עצמו(1)
פחות הסכום של שאר השחקנים בלעדיו(2)
ועוד הסכום של שאר השחקנים כשהוא פה .(3)

<u>הוכחה</u>: התועלת של כל שחקן היא:
סכום הערכים של כל השחקנים (שורה 1,3).
פחות מספר שאינו תלוי בהצהרה שלו שורה (2).
השחקן שואף להשיג תועלת גדולה ביותר. לשם כך עליו למקסם את סכום הערכים של כל השחקנים. זה בדיוק מה שעושה מנגנון ויקרי-קלארק-גרובס כשהשחקן אמיתי.

<u>משפט</u>: אם הערך של כל שחקן בכל תוצאה >=0 ,אז מנגנון וק"ג מקיים השתתפות מרצון.

<u>הוכחה</u>: התועלת של כל שחקן היא:
סכום הערכים הגדול ביותר של כל השחקנים שורה (1,3)
פחות סכום הערכים הגדול ביותר של שאר השחקנים בלעדיו (שורה 2).
הסכום הראשון >= הסכום השני.

משמש לחישוב הערך הגדול ביותר/העלות הקטנה ביותר(מינוס על הערכים).

תשלום **כולל** של מפרסם i במכרז VCG:

$$[v_{i+1} * (r_i - r_{i+1}) + v_{i+2} * (r_{i+1} - r_{i+2}) + \ ...]$$

תשלום עבור **קליק** של מפרסם i במכרז VCG:

$$\frac{[v_{i+1} * (r_i - r_{i+1}) + v_{i+2} * (r_{i+1} - r_{i+2}) + \ ...]}{r_i}$$

תשלום עבור **קליק** של מפרסם i במכרז GSP :vi+1

<u>תכנון מנגנונים אלגוריתמי</u>

אם העלות של כל קשת ידועה לכולם – אלגוריתם.
אם העלות של כל קשת ידועה רק לבעליה – מנגנון

<u>משפט מיירסון</u>: קיים כלל-תשלומים אמיתי אם ורק אם כלל-הבחירה הוא פונקציה מונוטונית עולה של הערך . כלל-התשלומים הזה הוא יחיד.

שחקן שלא נבחר ($c_i = 0$) משלם 0;
שחקן שנבחר ($c_i = 1$) משלם את ערך הסף שלו כלומר הערך הקטן ביותר שהוא צריך להגיד כדי להיבחר.
כלל בחירה- כל כלל מונוטוני.

<u>מכרזים למיקסום רווח</u>

$$E[Revenue(p)]=p*prob(v>p)=p*[1-F(p)]$$

$$P`=0 \Leftrightarrow p - \frac{1-F(p)}{F`(p)} = 0$$

נגדיר את **פונקציית הערך הוירטואלי:**

$$r(v)=v- \frac{1-F(v)}{F`(v)}$$

($F(v)$ – ערך מצטבר, $F`(v)$- צפיפות)

המכרז האופטימלי הוא: **מכור אם"ם $r(v)>0$.**

$$E[\sum_{j=1}^{n} c_j(v_1, v_2, \ldots, v_n) * r_j(v_j)]$$

תוחלת הרווח = תוחלת סכום הערכים הוירטואליים.

כדי למקסם רווח ,צריך למצוא כלל-בחירה ש**ממקסם את סכום הערכים הוירטואליים.**

<u>קונה אחד</u>: תוחלת הרווח = הערך הוירטואלי = r(v).
כלל-הבחירה הוא: מכור אם-ורק-אם r(v)>0
הכלל אמיתי בתנאי ש r-היא פונקציה עולה
התשלום הוא ערך-הסף $r^{-1}(0)$.

<u>הרבה קונים מאותה התפלגות F ועם אותו r:</u>
(נניח ש r-פונקציה עולה).
תוחלת הרווח = $r(v_j)$ של המנצח.
כלל-הבחירה הוא: מכור למשתתף עם v_j הכי גבוה, בתנאי ש $r(v_j)>0$.
התשלום הוא ערך-הסף: הערך השני בגובהו או $r^{-1}(0)$ - הגבוה מביניהם.
---שקול למכרז ויקרי עם מחיר מינימום $r^{-1}(0)$.

<u>שני קונים עם התפלגויות שונות:</u>
תוחלת הרווח = $r_j(v_j)$ של המנצח.
כלל-הבחירה הוא: מכור למשתתף עם $r_j(v_j)$ הכי גבוה ,בתנאי ש $r_j(v_j) > 0$. התשלום = ערך-הסף.

דוגמה.Fa=Unif[10,30], Fb=Unif[20,40] :
ra(v) = 2v-30, rb(v) = 2v-40.

אם a אמר 23 ו b-אמר27 אז a יזכה! וישלם את ערך-הסף שלו שהוא - 22 ערך הסף של b הוא 28.

מכרז אופטימלי = מכרז עם מחיר המינימום של מיירסון. משיג את תוחלת-הרווח הגבוהה ביותר, אבל, דורש הרבה עבודה כדי לחשב את F.

<u>משפט בולוב-קלמפרר:</u>

תוחלת הרווח של מכרז פשוט עם n+1 משתתפים >= של מכרז אופטימלי עם n משתתפים!

מכרזים דו צדדים עם כמה קונים וכמה מוכרים

שיטה א׳ למציאת מחיר:

א. מצא את K העסקאות היעילות (עסקה יעילה מקיימת מחיר הקונה =>מחיר המוכר)
ב. המחיר הוא הממוצע בין הקונה והמוכר שההפרש בין מחירם הוא הקטן ביותר

מספק רווח מרבי ואיזון תקציבי אך לא אמיתי.

שיטה ב׳ למציאת מחיר ע״י **VCG**:

א. מצא את K העסקאות היעילות .
ב. חשב מחיר-**וק״ג** למוכרים(מקבלים את מחיר הסף של הקונים) - ומחיר וק״ג אחר לקונים(משלמים את מחיר הסף של המוכרים).- המדינה משלמת את הגירעון.

מספק רווח מירבי ואמיתי אך לא איזון תקציבי.

<u>משפט מיירסון וסאטרתוייט(1983):</u>
לא קיים מנגנון המשיג את כל שלוש התכונות בו זמנית:
רווח מירבי, איזון תקציבי, אמיתי.
הוכחה:
מספיק לבדוק מוכר אחד וקונה אחד.
רווח מירבי על חשבון אמיתיות.

מנגנון **מקאפי**-שיטה ג׳ למציאת מחיר ע״י **מחירי סף**:

א. מצא את K העסקאות היעילות .
ב. הפחת 1 (את העסקה ה-k).
ג. חשב מחיר-סף לקונים (הקונה ה-k הכי קטן) ומחיר סף אחר למוכרים(ה-k הכי יקרן).

מספק רווח ״מירבי פחות 1״, עודף תקציבי ואמיתי.

<u>שיווי-משקל נאש במשחקים ובמכרזים</u>

הגדרה :פעולה שולטת (דומיננטית) של שחקן: עבור כל צירוף-פעולות של האחרים, הפעולה נותנת לשחקן תועלת גבוהה ביותר. אסטרטגיה שלטת: ״לא משנה מה השני ייבחר אני נשאר בשלי״.

משפט :כל מטרה שאפשר להשיג ע"י משחק עם פעולות שולטות – אפשר להשיג ע"י מנגנון אמיתי.

הוכחה :המנגנון האמיתי מקבל מהשחקנים את טבלת הערכים שלהם ,ומשחק עבורם את הפעולה השלטת שלהם.
דוגמה: מכרז אנגלי.

הגדרה :שיווי-משקל נאש :(Nash) צירוף פעולות של כל השחקנים ,שבו הפעולה של כל שחקן נותנת לו תועלת גבוהה ביותר בצירוף זה. כלומר השחקן של ה״שורות״ צריך שהערך במשבצת שלו יהיה הכי גבוה באותה **עמודה** והשחקן של העמודות צריך שהערך במשבצת שלו יהיה הכי גבוה באותה השורה
פרשנות: הסכם שאוכף את עצמו.

דוגמה :מכרז על חפץ אחד ,שני משתתפים.
ס – ערך 60, כ – ערך 20.
מה הם כל שיוויי-המשקל של המכרז?
נסמן: s- הכרזה של ס ,k-הכרזה של כ.
מכרז מחיר ראשון - נחלק למקרים:
אם $k<19$ אז s=k+1 ואז כ יעלה ל – s-לא ש"מ.
אם $k>=19$ וגם $k<60$ אז s=k+1 וזה כן ש"מ.
אם $k>=60$ ס יפסיד ו-כ יירד – לא ש"מ.

משפט :אם לכל שחקן יש פעולה שלטת ,אז צירוף הפעולות השולטות הוא שיווי-משקל נאש.

בס"ד

<table>
<tr><th>שחקנים</th><th>חלוקה פרופורציונלית</th><th>חלוקה ללא קנאה</th><th>חלוקה קשירה ללא קנאה</th></tr>
<tr><td>2</td><td colspan="3">2שאילתות</td></tr>
<tr><td>3</td><td rowspan="3">Θ(n log n)</td><td>5</td><td rowspan="3">אינסוף!</td></tr>
<tr><td>4</td><td>200</td></tr>
<tr><td>n</td><td>$\Omega(n^2)$
$O(n^{nnnnn})$</td></tr>
</table>

	מחיר ראשון	מחיר שני
פעולות שולטות	לא	כן
כל ש"מ הוא יעיל פארטו (הגבוה זוכה)	כן	לא
בש"מ, הרווח למוכר תמיד לפחות הערך השני	כן	לא

<u>אלגוריתמי חלוקה הוגנת:</u>

<u>אלגוריתם "חתוך ובחר"</u>

תכונות:

1) כל משתתף חושב שהחלק שלו שווה לפחות 1/2 – חלוקה **פרופורציונלית** (proportional).
2) כל משתתף חושב שהחלק שלו טוב לפחות כמו כל האחרים – חלוקה **ללא קנאה** (envy-free).

חלוקה פרופורציונלית:

<u>אלגוריתם "המפחית האחרון" הוגו שטיינהאוס 1948:</u>

- **הראשון** מסמן 1/n בעיניו.
- אם **השני** חושבת שזה יותר מדי - היא מפחיתה ל-1/n שלו. וכן **השלישי** וכו'.
- האחרון שהפחית מקבל את החלק שסימן.
- ממשיכים ברקורסיה על כל אלו שלא קיבלו חתיכה.

תכונות: חלוקה פרופורציונלית.(הוכחה באינדוקציה).

משפט: האלגוריתם הנל משתמש ב- O(N^2) שאילתות.

<u>אלגוריתם דובינס-ספנייר – 1961:</u>

- מחזיקים סכין מעל העוגה ומזיזים אותו מימין לשמאל.
- מי שחושב שהחלק מימין לסכין שווה 1/n צועק "עצור!" ומקבל את מה שמימין לסכין.
- השאר ממשיכים רקורסיבית.
- יותר נוח וקל למשתמש – אבל לא יותר מהיר חישובית.

חלוקה פרופורציונלית מהירה

<u>אלגוריתם אבן-פז שמעון אבן ועזריה פז, 1984:</u>

- כל שחקן מחלק לשני חלקים בשווי 1/2בעיניו.
- חותכים את העוגה בחציון של הקוים.
- שולחים כל שחקן לחצי שמכיל את הקו שלו.
- מחלקים כל חצי ברקורסיה.

מה עושים כש-n איזוגי?

- כל שחקן מחלק לשני חלקים ביחס של: (n+1)/2 : (n-1)/2
- חותכים את העוגה כך שבצד אחד יהיו (n-1)/2 קוים ובצד שני (n+1)/2 קוים.
- שולחים כל שחקן לחצי שמכיל את הקו שלו.

משפט: אלגוריתם הנל נותן חלוקה פרופורציונלית (באינדוקציה).

משפט: אלגוריתם אבן-פז משתמש ב- O(n*log n) שאילתות.

אין אלגוריתם יותר מהיר לחלוקה פרופורציונלית מסיבוכיות זו.

<u>חלוקה ללא קנאה</u>

<u>אלגוריתם סלפרינג קונווי:</u>

כ חותך 3 חתיכות שוות בעיניו.

אם א, י מעדיפים חתיכות שונות – סיימנו. אחרת - י מקצץ את החתיכה הטובה ביותר ומשווה לשנייה בעיניו.

א, י, כ בוחרים חתיכה. י חייב לבחור את זו שקיצץ, אם לא נבחרה קודם.

קיבלנו חלוקה עם שארית.

[א או י בחרו את החתיכה המקוצצת; במקרה זה א].

י (שלא בחר את החתיכה המקוצצת) מחלק את השארית לשלוש חתיכות שוות בעיניו.

א, כ, י בוחרים חתיכה.

נותן חלקה ללא קנאה

הוכחה ע"י גרפים שידוך מושלם בגרף זה = חלוקה ללא קנאה!

<u>אלגוריתם הסכין המסתובבת:</u>

עושים צעד אחד של "המפחית האחרון". שחקן אחד (נניח כ) זוכה בחתיכה.

הזוכה (כ) מסובב סכין ארוכה מעל השארית, כך ששני החלקים תמיד שוים בעיניו.

(אפשרי - משפט ערך הביניים).

א אומר "עצור" ברגע ששני החלקים שוים בעיניו.

בוחרים לפי הסדר י, א, כ

<u>חלוקה קשירה ללא קנאה ל-n:</u>

חלוקה ללא קנאה = נקודה שבה כל שחקן כותב מספר אחר.

<u>אלגוריתם סימונס (Su 1999)</u>

מחלקים את סימפלקס-החלוקות לסימפלקסונים.

נותנים כל צומת לשחקן, כך שבכל סימפלקסון, כולם מיוצגים.

כל שחקן כותב, בכל צומת שלו, את מספר החתיכה הכי טובה בעיניו.

מחפשים סימפלקס-n מלא = עם n מספרים שונים = חלוקה כמעט-ללא-קנאה.

<u>חלוקה הוגנת ואמיתית</u>

אלגוריתם - Bei, Huzhang, Suksompong, 2018

לשני שחקנים עם העדפות בינאריות:

- מצא את ה- xהמינימלי כך שהערך של ב משמאלו שווה לערך של א מימינו: $V_b([0,x]) = V_a([x,1])$
- תן לשחקן ב את הקטעים שהוא רוצה משמאל ל- xואת הקטעים ששחקן א *לא רוצה* מימין ל:x

האלגוריתם הנ"ל מקיים אמתיות הגינות ויעילות פארטו.

<u>הגינות:</u> כאשר שחקן מסוים מקבל לפחות 1/n מהחלוקה.

<u>משפט:</u> **לא קיים** אלגוריתם הוגן אמיתי ויעיל-פארטו אם:

1) פונקציות הערך לא בינאריות, או -
2) כל שחקן צריך לקבל חתיכה קשירה.

<u>חלוקה הוגנת ויעילה</u>

<u>Efficient Fair Division</u>

משפט: אלגוריתם" חתוך ובחר "מחזיר תוצאה יעילה פארטו אם מתקיימים התנאים הבאים:

1) שני השחקנים רוצים רק חתיכות קשירות.
2) לכל נקודה בעוגה יש ערך חיובי ממש.
3) החותך אמיתי, או מתחכם "חכם".

<u>יעילות – מיקסום סכום הערכים</u>

ניסיון שלישי: נמצא חלוקה הממקסמת את הסכום של פונקציה עולה **וקעורה** של הערכים. *דוגמה:*

$$\max\sum_{j=1}^{n}\sqrt{V_j(X_j)}$$

הרעיון: לתת יותר למי שיש לו פחות

מתברר שאם הפונקציה fהיא לוגריתמית:

$$f(V) = \log(V)$$

אז החלוקה לא רק יעילה אלא גם ללא קנאה!

<u>משפט</u>: כל חלוקה הממקסמת את סכום לוגי הערכים היא חלוקה ללא קנאה.

<u>חלוקה הוגנת של חפצים בדידים</u>

<u>אלגוריתם סו (Su, 1999):</u>זהה לחלוקת עוגה ל-n אנשים לפי אלגורתים סימונס אך הפעם החלקים הטובים הם החלקים הריקים – חדר חינם עדיף על חדר בכסף (דיירים עניים).

<u>חלוקת שכר דירה: סכום הערכים</u>

<u>משפט</u>: *בכל* השמה ללא קנאה, סכום הערכים של הדיירים בחדרים שהם גרים בהם הוא מקסימלי.

<u>בעיית ההשמה - האלגוריתם ההונגרי</u>

- **הקלט** מטריצה n על n המתארת את הערך של כל דייר i לחדר j.
- **הפלט**: השמה של דייר לחדר, כך שסכום הערכים של הדיירים לחדריהם גדול ביותר.
- **סיבוכיות** $O(n^3)$

שלבים:

1. עבור כל שורה חסר מכל משבצת בשורה את הערך המינימלי שבאותה שורה.
2. עבור כל עמודה חסר את הערך המינימלי בעמודה.
3. סמן את כל השורות והעמודות שמכילות אפסים.
4. אם הכיסוי המינימלי של האפסים ע"י שורות והעמודות הוא n סיימנו וקיימת ההשמה המבוקשת. אחרת בצע את שלב 5.
5. מצא את המשבצת עם המספר המינימלי שלא מכוסה ע"י שום שורה ותחסר אותו מכל משבצת בשורה לא מכוסה והוסף אותו לכל עמודה מכוסה. וחזור על שלב 3 חלילה.
6. את המשבצות שנבחרו בהשמה, בחר בלוח המקורי.

<u>אלגוריתם "המנצח המתוקן":</u>

א. כל חפץ נמסר למי שהכי רוצה אותו.

ב. אם סכום הנקודות שווה – סיימנו.

ג. אחרת – מסדרים את החפצים **בסדר עולה של היחס** $\frac{\mathbf{win}}{\mathbf{loss}}$ ומעבירים חפצים עד שהסכום משתווה. צריך לחתוך לכל היותר חפץ אחד *.

מספק יעיל פארטו, ללא קנאה אך לא אמיתי.

<u>משפט:</u> כל שיווי-משקל נאש טהור הוא ללא קנאה.

<u>משפט:</u> כל שיווי-משקל נאש טהור משיג קירוב 3/4 למקסימום-סכום-הערכים.

<u>חלוקה הוגנת בקירוב</u>

<u>אלגוריתם מעגלי הקנאה:</u>

עוברים על החפצים בסדר שרירותי. לכל חפץ:

1. נותנים את החפץ לשחקן שלא מקנאים בו.
2. אם אין כזה – סימן שיש מעגל-קנאה .מחליפים סלים במעגל בניגוד לכיוון חצי הקנאה.

מבצעים את 2 עד שאין מעגלים ,ואז חוזרים ל-1.

<u>משפט</u>:אם יש m חפצים ו n-שחקנים ,אז זמן-הריצה של אלגוריתם מעגלי הקנאה הוא $O(m\,n^3)$.(הוכחה בעזרת DFS).

<u>משפט</u>:האלגוריתם הנ"ל מחזיר חלוקהEF1 .

<u>משפט</u>:אלגוריתם מעגלי הקנאה עלול להחזיר תוצאה שאינה יעילה-פארטו.

כשה"עוגה" רציפה – החלוקה הנ"ל הממקסמת את מכפלת ערכי המשתתפים היא ללא-קנאה ויעילה.

כשהחפצים בדידים – החלוקה הממקסמת את מכפלת ערכי המשתתפים היא EF1 ויעילה פארטו.

<u>משפט</u>:נניח ש:

*ההעדפות אדיטיביות – ערך של סל הוא סכום הערכים של החפצים בסל.

*קיימת לפחות חלוקה אחת שבה כל שחקן מקבל ערך גדול מאפס.

אז, כל חלוקה הממקסמת את מכפלת ערכי המשתתפים היא גם יעילה-פארטו וגם EF1.

הוכחה:

<u>יעילות פארטו</u>–עפ"י הגדרת מיקסום מכפלת ערכי המשתתפים.

<u>-EF1</u>

נניח ש i-מקנא ב j.נסתכל על כל החפצים בסל של j .לכל חפץ g , נבדוק את יחס הערכים :

$$V_i(g) / V_j(g)$$

נבחר את החפץ שיחס-הערכים שלו הכי גדול, ונעביר אותו מ- j ל i.

המכפלה בחלוקה החדשה שווה-או-קטנה מהמכפלה בחלוקה הקודמת, ולכן:

$$[V_i(X_i)+V_i(g)]*[V_j(X_j)-V_j(g)] \leq V_i(X_i)*V_j(X_j)$$

$$\rightarrow V_j(X_j) * V_i(g) / V_j(g) \leq V_i(X_i) + V_i(g)$$

יחס הערכים של g הוא הכי גדול ב- X_j,ולכן:

$$V_i(X_j) / V_j(X_j) \leq V_i(g) / V_j(g)$$

מציבים למעלה ומקבלים:

$$V_i(X_j) \leq V_i(X_i) + V_i(g)$$

$$V_i(X_j) - V_i(g) \leq V_i(X_i)$$

מכאן: אם מורידים את g מהסל של j ,אז i כבר לא מקנא.

<u>ביטקוין ושרשראות בלוקים</u>

הגדרה": מטבע קריפטוגרפי "הוא רשימה מקושרת-אחורה של הודעות מהצורה:

1) "מטבע נוצר ונמסר למפתח-ציבורי א".
2) "א שילם את המטבע שקיבל בהודעה 1, למפתח-ציבורי ב" [חתימה ע"י א].
3) ...

מי שקורא את השרשרת, יכול לוודא שהיא תקינה ע"י אימות כל ההודעות בעזרת המפתחות הציבוריים. כך אפשר לדעת למי שייך המטבע.

הדרך של ביטקוין למניעת שכפול מטבעות - **הוכחת-עבודה :**

- הקונה שולח בקשת תשלום לרשת.
- כל משתמש בודק שהבקשה חוקית ומנסה לאשר.
- כדי לאשר בקשה m,צריך לפתור חידה קשה - להפוך פונקציה חד-כיוונית - למצוא x כך ש:

SHA256(m+x) < (2^224) / D

כאשר D הוא מספר המייצג את רמת הקושי.

הראשון שמצליח לפתור את החידה – שולח את הבלוק עם הפתרון לכולם וכך מצרפו לשרשרת.

בכל בלוק יש מקום לכ- 2000 עסקאות.

פתרון החידה (x) נקרא nonce.

תהליך מציאת ה- nonce נקרא כריה (mining).

רמת הקושי (D) נקבעת באופן דינמי כך שהזמן הדרוש למציאת nonce יהיה כ-10 דקות (כדי שהבלוק יספיק לפעפע ברשת).

מזלגות ובלוקים יתומים:

איך מחליט כל כורה, לאיזה בלוק-קודם לקשר?

כלל א :בחר את השרשרת הארוכה ביותר.

כלל ב :אם יש כמה שרשראות ארוכות ביותר – קשר לבלוק ששמעת עליו מוקדם ביותר.

- בלוק שנמצא מחוץ לשרשרת הארוכה ביותר נקרא "יתום" (orphaned) העסקאות בו לא מאושרות.

האם פרוטוקול ביטקוין אמיתי?

- פרוטוקול נקרא "אמיתי "אם התנהגות בהתאם לפרוטוקול ממקסמת את הרווחים.
- התשלומים לכורים נועדו לעודד אותם לפעול לפי הפרוטוקול.
- אבל יש כמה מקרים שבהם כדאי לכורה לפעול בניגוד לפרוטוקול.

כורה המחזיק מעל 50%מכוח-הכרייה יכול לשלם פעמיים באותו מטבע, באופן הבא:

- נניח שהבלוק הנוכחי הוא בלוק א. התוקף קונה חפץ, והתשלום מאושר בבלוק ב המקושר ל-א.
- התוקף כורה בלוקים המקושרים לבלוק א, עד שהשרשרת שלו ארוכה יותר מהשרשרת העוברת דרך בלוק ב.
- בלוק ב נעשה "יתום", והאישור מתבטל!

לכן, תנאי הכרחי לאמיתיות של ביטקוין הוא שכוח-הכרייה של כל כורה יחיד קטן מ-50%.