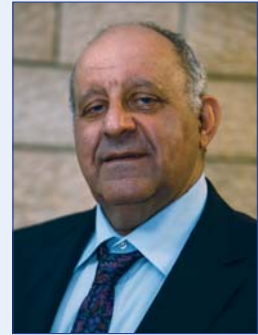
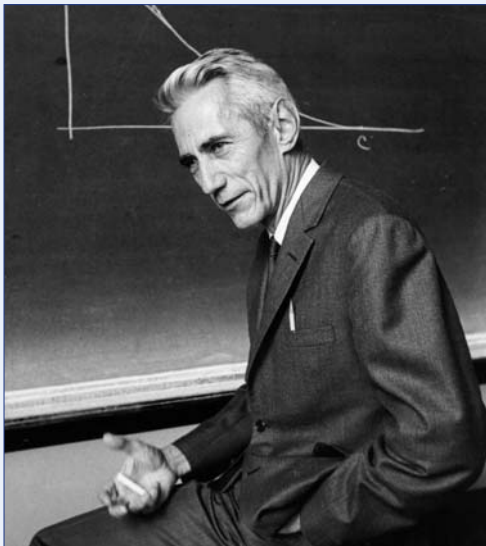


תורת האינפורמציה, מהזווית האישית



מאת פרופ' שלמה שמאי (שיץ)

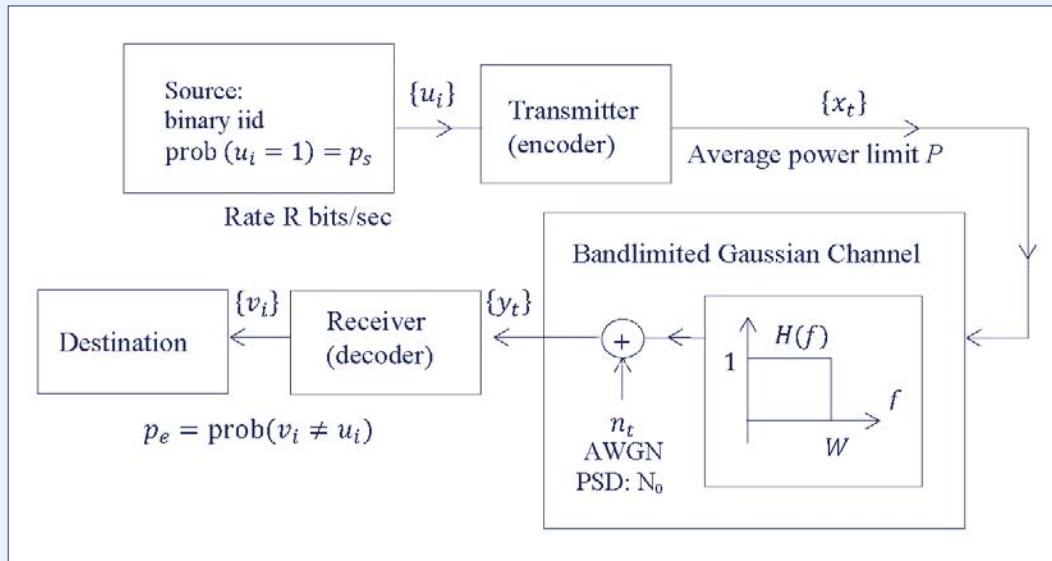
ופשוט ביסודו. על אף פשטותה מציגה מערכת זו מגוון עשיר של אתגרים מחקריים, בעלי השלכות פרקטיות מעניינות, שעם חלקם התמודדתי בעבודתי המחקרית. ההיבט הבינתחומי בשטח יודגם גם בקשר מעניין שעמיתי ואני גילינו, המחבר בין גדלים קלאסיים של תורת האינפורמציה ועיבוד (שיערוך) אותות. נדון בקצרה בהשלכות של קשר זה על מגוון בעיות ישנות וחדשות, ונסכם במבט קצר לעתיד.



קלוד שנון

תורת האינפורמציה נולדה בהבזק בשנת 1948 עם פרסום מאמרו המונומנטלי של קלוד שנון (Claude E. Shannon) – "התורה המתמטית של התקשורת" [1]. אכן, תורת האינפורמציה היא תורה מתמטית שיסודותיה נעוצים בתורת ההסתברות, בסטטיסטיקה ובתהליכים אקראיים. עצם מהותו של המונח "אינפורמציה" (מידע) מוגדרת במאמר על בסיס זה, ומוצג בו מדד לכמות האינפורמציה, המתבסס על המושג החשוב של אנטרופיה. ההישג המרכזי של תורת האינפורמציה מתבטא ביכולתה לאפיין באופן כמותי ומדויק את האפשרויות של עיבוד וניוד (שידור) של אינפורמציה מחד ואת מגבלותיהן הבסיסיות מאידך. ההישגים והתוצאות האנליטיות ויכולתה של תורת האינפורמציה מבוססים על עקרונות מתמטיים ואינם תלויים בטכנולוגיה, ומכאן חשיבותם העצומה, שאינה מתיישנת עם הזמן או עם ההתפתחות הטכנולוגית.

נציין בקצרה היבטים בינתחומיים המאפיינים את תורת האינפורמציה, אם בתחומי מדעי ההנדסה ואם מעבר להם. נדגיש את שינוי המגמה בשנים האחרונות, שבעקבותיו תורה מתמטית זו הופכת לנדבך דומיננטי בהיבטים ובתכנונים מעשיים של מערכות תקשורת ועיבוד אותות מודרני. "הזווית האישית" תודגם בעזרת מודל תקשורת לינארי



איור 1. מערכת תקשורת בערוץ גאוזי אדיטיבי מוגבל-סדר

נסמן ב- p_e את סיכוי הטעות בין הסיביות המופענחות $\{v_i\}$, בעזרת המקלט (מפענח) על סמך מוצא הערוץ y_t , לבין אלו המשודרות $\{u_i\}$. כלומר p_e מסמן את הסתברות הטעות בפיענוח $p_e = \text{prob} \{v_i \neq u_i\}$ ומשמש מדד של "טיב" הביצועים. שנון הראה בעבודתו הגאונית [1] ובעבודות מאוחרות יותר (פרטים ניתן למצוא בספרים אלמנטריים מומלצים בתחום כגון [2], [3]) כי p_e הניתן להשגה מתקבל באמצעות הביטוי:

$$R \cdot (h_2(p_s) - h_2(p_e)) \leq W \log_2 \left(1 + \frac{P}{N_0 W} \right) \quad (1)$$

כאשר

$$h_2(x) = -x \log_2 x - (1-x) \log_2 (1-x), \quad 0 \leq x \leq 1$$

מסמן את האנטרופיה הבינרית.

מסקנה חשובה לא פחות ששנון הסיק היא ששום מערכת, באשר היא, העומדת באילוצים ובאופן בלתי תלוי בטכנולוגיה או בכל דבר אחר, אינה מסוגלת לביצועים המפרים את אי־שוויון (1).

נוסחה (1) טומנת בחובה אלמנטים של דחיסת מקור אינפורמציה כאשר $p_s \neq 1/2$, ושל תורת קצב עיוות מקור (rate distortion theory) כאשר מסתפקים בביצועים לא אידאליים ($p_e > 0$), [4, pp. 325–350].

די להדגים את סוג התוצאות שתורה זו מספקת, נתבונן בדוגמה קלאסית, המתוארת באיור 1.

מקור האינפורמציה הוא זרם סיביות בינריות $\{u_i\}$ המקבלות את הערכים (1,0) והנוצרות בקצב R סיביות לשנייה, כאשר i - מסמן את אינדקס הסיביות. אנו מניחים כי הסיביות בלתי תלויות סטטיסטית זו בזו ומאופיינות בחוק הסתברות:

$$\text{prob}(u_i = 0) = 1 - p_s, \quad \text{prob}(u_i = 1) = p_s$$

(המקור מכונה אסימטרי אם $p_s \neq 1/2$).

מעוניינים לשדר (לנייד) את אינפורמציות המקור ליעד המעוניין בה דרך ערוץ המכונה "הערוץ הגאוזי האדיטיבי מוגבל-הסרט". ערוץ זה מעביר תדרים עד W (הרץ), כש- W מסמן את רוחב הסרט של הערוץ וכן מוסף רעש אדיטיבי גאוזי לבן n_t בעל צפיפות הספק ספקטרלית (מסומנת ב-PSD) בעצמה של N_0 (ואט/הרץ). תמסורת המידע בין המקור ליעד מתבצעת בעזרת משדר (מקודד) המהווה טרנספורמציה כללית, לבחירת המתכנן, ממידע המקור לאות תלוי-זמן x_t המשוגר לערוץ. לרשות המשדר עומדים אמצעים מוגבלים המתוארים בבעיה זו באמצעות ההספק הממוצע המסומן ב- P .

כאשר $E_b = \frac{P}{R}$ מסמן את האנרגייה המושקעת בשידור ביט אינפורמציה אחד.

נוסחה (4) מבהירה שאי אפשר לשדר אינפורמציה באמינות מוחלטת בערוץ הגאוס הידיטיבי אלא אם כן משקיעים אנרגייה מינימלית מנורמלת לרמת הרעש לכל ביט אינפורמציה. תוצאה זו, שאינה תלויה בטכנולוגיה, מדגימה את חשיבותם של הניבויים האנליטיים הטמונים בתורת האינפורמציה שתקפותם אינה פגה עם הזמן.

תורת האינפורמציה נוגעת כיום בנושאים רבים בתחום ההנדסה, הרבה מעבר לתקשורת בלבד. נציין רק כמה נושאים, ובמפורש: רשתות תקשורת, תורת הבקרה, רשתות בכלל ומדעי וטכנולוגיות מחשב.

תורת האינפורמציה השפיעה ישירות על תחומים כגון למידה [5], סיבוכיות (לדוגמה מסוג קולמוגורוב Kolmogorov) וכן למפל-זיו (LZ), אחסון מידע

לדוגמה, נעיין במקור סימטרי $p_s = 1/2$ ונדרוש ביצועים ללא שגיאות (תקשורת אמינה) $p_e = 0$. נוסחה (1) תקבע אפוא זאת:

$$R \leq W \log_2 \left(1 + \frac{P}{N_0 W} \right) \quad (2)$$

שהיא הנוסחה המפורסמת של שנון [1] לקיבול הערוץ הגאוס הידיטיבי מוגבל-הסרט, המאפיין את הקצב המרבי של סיביות לשנייה הניתנות לשידור אמין דרך ערוץ זה. אם אין מגבלת רוחב סרט, קרי $W \rightarrow \infty$, אזי מ- (2) מתקבל

$$R \leq \frac{P}{N_0 \ln 2} \quad (3)$$

(ln מסמן לוגריתם על פי בסיס טבעי). במילים אחרות:

$$\frac{P}{RN_0} = \frac{E_b}{N_0} \geq \ln 2 \quad (4)$$



האינפורמציה בלינגוויסטיקה [4, pp. 194–208]. נסתפק ברשימה זו של קשרים בין-תחומיים של תורת האינפורמציה ונסיים היבט זה בציון מאמרו של שנון "The Bandwagon" [15], שבו הוא מזוהר משימוש סתמי במושגי תורת האינפורמציה לפתרון מלאכותי של בעיות שמתעוררות בתחומים שונים. שנון אינו טוען שמושגי תורת האינפורמציה אינם רלוונטיים למגוון עשיר של תחומים. נהפוך הוא: אין הוא טוען אלא ששימוש אִמְתִי ומועיל דורש מחקר רב ומאמצים אינטלקטואליים ואנליטיים כבירים. אכן, ובמיוחד בשנים האחרונות, רצוי לאמץ את אותה הנחיה מרחיקת ראות של מייסד התחום – קלוד שנון.

ב תקופה האחרונה אנו מבחינים בשינוי מגמה מהותי בתורת האינפורמציה. התחום, שבהיולדו [1] היה מתמטי לחלוטין והתבסס על שיקולים אנליטיים מרחיקי ראות של מייסדו ושל אותם ענקים שהלכו בעקבותיו בשנות החמישים, נשאר בעיקרו כזה. אלא שתחזיותיו, שבעבר נראו דברים תאורטיים שנחמד ומעניין לדעת אך חסרי שימוש פרקטי, הפכו להיות לכלים מעשיים חשובים. השינוי חל עם התפתחות הטכנולוגיה, שאפשרה מימוש מערכות מורכבות ביותר, ללא קשיים מיוחדים. לדוגמה, במשוואה (2) תוארו הביצועים המוחלטים האפשריים בערוץ גאوسی אדיטיבי מוגבל-הסרט. כיום תוך ניצול שיטות קידוד מתקדמות [16] מסוג Low Density Parity Turbo Codes (LDPC) ועקרונות של קודי Turbo Codes (Turbo Codes) ולאחרונה גם Polar Codes למימוש קודי ערוץ יעילים, ניתן להתקרב מאוד לביצועים האולטימטיביים. האם עובדה זו מוליכה ל"מותה" של תורת האינפורמציה אם כי מסיבה שונה מזו שנטענה בעבר? בעבר גרסו אף מדענים בכירים בתחום כי תחזיות תורת האינפורמציה חסרות ערך מהבחינה הפרקטית, וכיום הן פשוט ניתנות למימוש במגוון מקרים. כפי שנראה, קרה ◀

(storage), הצפנה (קריפטוגרפיה) מסוגים שונים, החל מזו המבוססת על מערכות הצפנה קלאסיות, המשתמשות במפתח הצפנה [4, pp. 84–143], וכלה במערכות שבהן הסודיות מושגת בעצם ניצול ההבדל בין ערוצי התקשורת של המשתמש הרצוי לזה של המאזין הלא חוקי (eavesdropper) [6], ומקורות המוזכרים שם], [7]. תורת האינפורמציה קשורה גם לתכנון מעגלים וטכנולוגיות המשמשות לתקשורת בתוך רכיב המעבד (VLSI, processor) עצמו. לתורת האינפורמציה חשיבות מרובה גם מחוץ לתחום ההנדסה כולו, ולכן אפשר בהחלט להתייחס אליה כאל מדע בין-תחומי במלוא מובן המילה. הקשר עם תורת ההסתברות, סטטיסטיקה ומודלים אקראיים הוא קלאסי מאז היוולדות התחום. הקשר הוא דו-כיווני, וגם התחומים המתמטיים החשובים הללו, נהנו מקשרים הדדיים. נזכיר כאן רק את נושאי הסקת המסקנות הסטטיסטיות (statistical inference) ואת תורת התנודות הרחבות (large deviations theory), [5], [6], [8], [9], [10]. הקשר ההדוק הדו-כיווני עם תחום המתמטיקה בולט אף הוא לאורך השנים. נזכיר כאן נושאים קלאסיים כגון התורה הארגודית [3], [8], [10], מטריצות, אם דטרמיניסטיות [2] ואם אקראיות [19], ותורת הגרפים [4, pp. 121–138], [11]. קשרים עם תחום הפיזיקה ובמיוחד הפיזיקה הסטטיסטית זכו לאחרונה לשימוש במגוון בעיות תאורטיות ופרקטיות [11], [12]. הפיזיקה הקוונטית שימשה בסיס לפיתוח ענף חדש של תורת האינפורמציה קוונטית, המאמצת מושגים קוונטיים להגדרת אינפורמציה ועיבודה [13]. קשרים בין תורת האינפורמציה לכלכלה ובמיוחד לתורת ההשקעות מחד ולהימורים מאידך ידועים זה עשרות שנים [2]. תחום הביולוגיה נהנה גם הוא מקשר הדוק עם תורת האינפורמציה, ומונחים כגון ביו-אינפורמטיקה, וכן רשתות עצביות, ביולוגיה מולקולרית ולאחרונה גם שרשרת (DNA Sequencing) [14], הופכים להיות שגורים בתחום. שנון עצמו עסק בהיבטים של תורת



פרקטית. תורת האינפורמציה מצביעה ישירות על מה ניתן לעשות ולעתים אף קובעת את העיקרון ואת והאלגוריתם שמשגי לא רק ביצועים טובים אלא אף את הביצועים האופטימליים. כמובן האלגוריתם וכן התחזיות לביצועים אופטימליים תלויים במודל, בדרישות ובמשאבים להשגתם, וגם כאן יש לנקוט משנה זהירות כדי להימנע ממסקנות מוטעות או אף מביכות. מתברר יותר ויותר כי מודלים תאורטיים מסוגלים לספק את התובנה הנדרשת למימוש מערכות מעשיות המתקרבות לאופטימום האפשרי. כמובן, בניגוד למערכות ולמודלים פשוטים ולעתים נאיביים, שהיו די מספקים בעבר, כיום נדרשים מודלים מורכבים הרבה יותר, כאלו המסוגלים להתמודד עם מושגים של תקשורת מרובת-משתמשים הנעשית בתנאים ובערוצים שונים, ולעתים אף בתנאי אי-ודאות (לדוגמה, כאשר לא ניתן ידע מדויק של ההתנהגות הסטטיסטית של הערוץ). מה שחסר הן בעיקר התוצאות המתמטיות התאורטיות (חלקן בעיות פתוחות זה עשרות בשנים) למגוון הרב של מודלי תקשורת ועיבוד מידע רלוונטיים. כצפוי,

◀ ההפך הגמור: ההתפתחות הטכנולוגית מובילה לעניין מסיבי ונרחב במודלים ובגישות של תורת האינפורמציה, וזאת משום שאלו – למרות היותם מתמטיים, תאורטיים ומורכבים – הפכו לבעלי משמעות פרקטית מהמעלה הראשונה. יתרה מזו, בעבר הלא רחוק עיקר הבעיה בהנדסת תקשורת ועיבוד אינפורמציה הייתה "איך לעשות", "איך לממש", "איך לבנות", ואילו "מה לעשות" היה די ברור, מכיוון שאי אפשר לדרוש מימוש מערכת מורכבת מדי בטכנולוגיות העבר. כיום נתהפכו היוצרות: השאלה "איך לעשות" הפכה להיות סטנדרטית, ובדרך כלל לא חשוב כל כך ולא ממש קריטי אם המימוש דורש עוד עשרות אלפי טרנזיסטורים (כולם מכונסים ברכיב זעיר אחד). הבעיה הנוכחית, לעומת זאת, היא "מה לעשות", קרי השיטה, האלגוריתם, הגישה והרעיון הם הדברים החשובים שיובילו למערכות בעלות ביצועים משופרים וקרובים לאופטימליים. מימוש הטכניקה הנבחרת בדרך כלל כבר אינו בבחינת בעיה מהותית כפי שהיה בעבר, ובדיוק בנקודה זו תורת האינפורמציה הופכת להיות כלי בעל חשיבות

שנים ספורות) להתעניינות וליישומים מעשיים רבים.

לתורת האינפורמציה יהיה משקל מרכזי מכריע בבחירת גישות יעילות הקרובות לאופטימליות במערכות תקשורת ועיבוד אינפורמציה עתידיות המבוססות על מבנה ענן (Cloud Processing, Computing & Networking). כאמור, גם אפיון האופטימום האפשרי נמצא בארגז הכלים והיכולות של תורת האינפורמציה. פרטים נוספים ודוגמאות ליישומים של עקרונות תורת האינפורמציה אפשר למצוא ב-[17].

סעיף זה נדגים בעזרת מודל מתמטי לינארי פשוט את ישימותה הנרחבת של אנליזה תאורטית במסגרת תורת האינפורמציה.

מתברר שגם מודלים פשוטים כאלה מציבים בפנינו בעיות תאורטיות מורכבות, שחלקן עודן פתוחות. כמו כן נצביע על קשרים של בעיות מסוימות לנושאים מתמטיים קלאסיים. במסגרת זו תודגש גם הזווית האישית, קרי חלק מהנושאים והבעיות שהמחבר עסק ועוסק בהם, וזאת ללא כל טענות או יומרות כי אלו הנושאים והבעיות החשובים או הרלוונטיים ביותר. נעיין במודל התקשורת הלינארי הווקטורי להלן:

$$y = AHx + n \quad (5)$$

x מסמן את וקטור המבוא (input vector),
 H היא מטריצת הערוץ (channel matrix),
 n הוא וקטור הרעש הגאוסני האדיטיבי,
 y הוא וקטור המדידה במוצא הערוץ (channel output),
 A מסמלת את מטריצת המדידה, ומסוגלת לתאר דעיכות ערוץ, מיתוג מוצאים ושקלולי אובזרבציות שונות,
 B היא מטריצה המשמשת למיתוג ובקרת כניסה. לדוגמה, מטריצה אלכסונית, כאשר האלכסון מורכב ממספרים המקבלים ערכים (1,0) הקובעים אילו מרכיבי הכניסה יהיו פעילים. ◀

היבט זה מספק תמריץ עצמתי למחקר מעמיק ונרחב בתחום. אכן, זוהי הסיבה המרכזית להתרחבותו של התחום בעולם בעשור האחרון מבחינת סטודנטים, חוקרים ומדענים ומשאבים שמוקצים למחקר.

דגים בקיצור נמרץ מערכות תקשורת קיימות ששיקולים אינפורמטיביים שימשו פקטור מרכזי לא רק בתכנון אלא אף בעצם הצעתן.

תחילה נזכיר את אלגוריתם הדחיסה על שם למפל-זיו (LZ), הנחשב היום קלאסי, המשמש בסיס לאלגוריתמי דחיסת נתונים ונמצא בשימוש נרחב במחשבים ובאינטרנט. נציין את מערכות ה-CDMA (Code Division Multiple Access), טכנולוגיה שהיוותה בסיס למערכות סולריות מהדור השלישי. טכנולוגיות Orthogonal (OFDM) Frequency Shift Keying, שחלקן פותחו על יסוד שיקולים אינפורמטיביים והן מרכזיות בתקשורת סולרית מודרנית ועתידית. תקשורת קווית מודרנית - ADSL/VDSL - מתקרבת לגבולות התאורטיים המותרים על ידי ערוצי הכבלים/חוטי הטלפון הנתונים. נוסף על אלה נציין רעיונות אינפורמטיביים מתקדמים המשמשים ב-HDMI (High-Definition Multimedia Interface) וכן ב-DAB (Digital Audio Broadcasting). גם באינטרנט מערכות תקשורת מתוחכמות המנצלות קידוד מסוג Raptor ו-Fountain, שפותחו משיקולים אינפורמטיביים תאורטיים, מאפשרות התאמה טבעית לסביבת הרשת ללא צורך בתכנון נפרד לקצבי המוצא השונים. נסיים באזכור מערכות אלחוטיות המבוססות על מערכי אנטנות בשידור וקליטה - Multi-Input-Multi-Output (MIMO). אלו משמשות כיום מרכיב מרכזי בדורות העתידיים (דור 5) של תקשורת סולרית. כיום מדברים על מאות אנטנות, ומושגים כגון Massive MIMO שגורים בפי מהנדסי הפיתוח הבכירים. נושא ה-MIMO פותח כולו משיקולים תאורטיים אינפורמטיביים אנליטיים וזכה כמעט בן לילה (תוך

קלאסי לתיאור ולטיפול בבעיות תקשורת הקשורות בערוץ העולה (uplink), קרי הערוץ המתאר את התקשורת ממגוון משתמשים למרכז אחד (כגון תא סלולרי). ערוץ כזה מכונה ערוץ מרובה-משתמשים (multiple access channel). דוגמה קלאסית היא תקשורת פורטת-ספקטרום (spread-spectrum) כגון (CDMA), אז המטריצה H מאפיינת את סדרות הפריסה (spread spectrum sequences) הנבחרות לעתים באופן אקראי [21]. בשימושים מסוג זה רכיבי וקטור המבוא מתארים את הסינגלים של המשתמשים השונים.

ה מודל הלינארי הפשוט ב-(5) מתאר גם ערוץ הפצה מרובה-אלמנטים (MIMO broadcast channel). ערוץ זה מאפיין לדוגמה את "הערוץ היורד" (downlink) מהתא הסלולרי מרובה-האנטנות אל מספר משתמשים שאינם משתפים פעולה ביניהם. ניתן להתייחס לערוץ זה כדואלי לערוץ מרובה-המשתמשים שתואר קודם, שבו מספר משתמשים מעבירים אינפורמציה למרכז קליטה אחד. קרי, כאן האינפורמציה משודרת ממרכז שידור אחד (מתואר על ידי הווקטור x) למשתמשים רבים. האותות הנקלטים אצל המשתמשים השונים מתוארים באמצעות הרכיבים של הווקטור y . בעיית ערוץ הפצה בכלל היא בעיה קשה בתורת האינפורמציה ועדיין לא פתורה בכללה זה עשרות בשנים [3], [6]. הבעיה הספציפית של MIMO broadcast channel הוצגה ונפתרה חלקית בעבודה [22] שזכתה בפרס Joint 2003 Information Theory and Communications Societies Paper Award.

עבודה זו פתחה "מירון" לפתרון מלא של הבעיה, וזו אכן נפתרה במלואה במחקר [23] שזכה ב-2007 IEEE Information Theory Society Paper Award. אלמנט מרכזי בפתרון הבעיה שהוצג ב-[22] והוכח כאופטימלי באופן כללי ב-[23] מבוסס על טכניקה המכונה "כתיבה על נייר מלוכלך" (dirty paper).

◀ מעצם היות המודל וקטורי, הוא משמש לייצוג מערכות מרובות כניסות ויציאות, ובלעז - MIMO. מערכות אלו משמשות כיום בתקשורת אלחוטית וקווית, ובעתיד נראה אף מערכות הניתנות לתיאור וקטורי בממד גדול מאוד (לדוגמה אנטנות רבות המותקנות בכל תא בתקשורת סלולרית), המכונות Massive MIMO. פרטים נוספים על אודות ההיסטוריה של מערכות אלו ונושאים נוספים אפשר למצוא במאמר הסקירה [18]. נושא ה-MIMO הוא קלאסי להדגמת הקשר העמוק של בעיות אלו לתורה המתמטית של מטריצות אקראיות [19]. כאן מטריצת הערוץ H מתארת מימוש (ראליזציה) של הערוץ הווקטורי ומאופיינת בחוק הסתברותי מתאים.

תורת האופטימיזציה המתמטית מאפשרת אפיון הסתברותי אופטימלי של וקטור הכניסה x בהינתן משאבים נתונים העומדים לרשות המשדר (כגון הספק או אנרגייה ממוצעת). המודל הלינארי הפשוט (כאשר A, B נבחרות כמטריצות יחידה ו- H היא Toeplitz) מתאים לתיאור תופעות שונות כגון תקשורת באמצעות קווי טלפון בקצב מהיר כאשר גורם דומיננטי הוא ההפרעה הבין-סימנית (intersymbol interference). כמו כן בבעיות אינפורמטיביות הקשורות לתקשורת MIMO נעשה שימוש נרחב בכלים מפיזיקה סטטיסטית [12] ובמיוחד בשיטת הרפליקה [20]. נושא עדכני הניתן גם הוא לטיפול במסגרת המודל הלינארי הווקטורי עוסק בדגימה וחישה דחוסה (compressive sensing/sampling). בבעיות אלו רק רכיבים ספורים מווקטור הכניסה x משפיעים על המוצא, וזאת אפשר לקבל בבחירת מטריצה אלכסונית B כאשר הרכיבים על האלכסון מאופיינים על ידי משתנים אקראיים בינריים. ההסתברות שהערך הוא יחידה קובעת את מידת הדילול (sparsity). המדידות וכמותן נשלטות באופן דומה על ידי המטריצה A . למידע נוסף, אנליזה ושימושים שונים, הקוראים המעוניינים מופנים ל-[20] ולמקורות נוספים המצוטטים שם. המודל בנוסחה (5) הוא



המשתמשים המשוך לתאים אלו. כמתואר, בעזרת מודל זה אפשר להציג הן את הערוץ העולה והן את הערוץ היורד, ואף לתאר שיתוף פעולה אפשרי בין תאים שונים או בין משתמשים שונים.

הניתוחים התאורטיים של תורת האינפורמציה מאפשרים לא רק לזהות את הפוטנציאל הקיים בשיתוף פעולה ברמת התאים אלא אף לכמת את היתרון גם כאשר קיימות מגבלות על שיתוף פעולה זה. אין זה מפליא אפוא שדורות עתידיים של תקשורת סלולרית (דור 5 והלאה) אכן ינצלו אלמנטים אלו לשיפור ניכר בקצב האינפורמציה האמינה ובזמינותה כדי לספק את הדרישות הגוברות של ציבור הצרכנים בתחום. ההבנה התאורטית משליכה על נושאים

writing on), שבעיקרה מתייחסת לבעיה של תשדורת כאשר ההפרעה ("הלכלוך") נתונה מראש למשדר בלבד. בשל חשיבותה זכתה טכניקה זו, שנחשבה לתאורטית ומתמטית לחלוטין, להתעניינות מעשית, ופותחו שיטות יעילות ליישום פרקטי של טכנולוגיה זו [24]. מאמר סקירה בנושא ערוץ ה-MIMO broadcast ניתן ב-[25].

חד השימושים העדכניים והמעשיים ביותר **Σ** שבמודל התקשורת המאופיין ב-(5) הוא לתקשורת אלחוטית סלולרית. מטריצת הערוץ H מאפיינת במצב זה את הערוץ שבין התא (cell-site) הבודד או מערך תאים המשתפים פעולה לבין אוסף



אינפורמציה באופן אמין ליעדו שלו, כלומר גם רכיבי וקטור המבוא x וגם רכיבי וקטור המוצא y מתארים את הסיגנלים המשויכים למשדרים ולמקלטים שונים בהתאמה. המטריצה H מדמה את ההפרעות הבין-ערוציות הנובעות לדוגמה משימוש במשאבים שאינם נפרדים (אורתוגונליים) כגון תדרים זהים, זמנים זהים לשידור וכיו"ב. גם ערוץ ההפרעה הוא אגוד קשה לפיצוח מבחינת תורת האינפורמציה ועדיין לא פוצח במלואו [6]. מתברר כי טכניקות מעניינות לפעולה יעילה בערוץ זה, ובמיוחד בתנאי יחס אות לרעש טובים, שונות מהטכניקות הקלאסיות. הללו עסקו

◀ רבים נוספים של תקשורת אלחוטית כגון WLAN (Wireless Local Area Networks) וכן נושאים של תקשורת "ירוקה", Massive MIMO, תקשורת במיקרו תאים ועוד. סקירה של התרומות התאורטיות בתחום אפשר למצוא ב-[26] וב-[27]. בעזרת מודלי תקשורת פשוטים אלו ניתן לתאר מגוון של בעיות עם השלכות פרקטיות ישירות שעדיין לא צוינו. אחת הבעיות הקלאסיות עניינה בערוץ הפרעה (interference channel). בניגוד למה שכבר תיארונו, במקרה זה מדובר על ערוץ בעל מספר משתמשים, שכל אחד מהם בנפרד מעוניין להעביר

שהובילו למושגים של קידוד רשתי (network coding), ולאחרונה קידוד רשתי בנוכחות רעשים והפרעות (noisy network coding), מאפשרים תקשורת יעילה בהרבה מזו הקיימת כעת, המתבססת על אלמנטים של ניתוב (routing) [30]. אספקטים של תכנון בין-שכבתי (cross-layer design) תוך שימוש באלמנטים של תורת האינפורמציה, המאפשרים הסתכלות מאוחדת בבעיית מקור, ערוץ ורשת, פותחים אופק חדש של אפשרויות תאורטיות ומעשיות.

גישה זו מובילה להגדרת בעיות תאורטיות חשובות שפתרוןן יוביל לתובנות חדשות הנוגעות למערכות תקשורת עיבוד אותות ומידע עתידיות. תורת האינפורמציה מטפלת ביסודיות בספקטרום נרחב של נושאים ובעיות שנובעות מאילוצים מעשיים, והדבר שב ומדגיש את הרלוונטיות הישירה של התחום לפרקטיקה של תקשורת ועיבוד אותות. כדוגמה נציין פיענוח המתבצע בעזרת מטריקה לא מתואמת (mismatched) הנובעת למשל מידיעה חלקית של הערוץ שדרכו מועבר המידע. פרטים מופיעים ב-[31] ובמקורות המוזכרים שם.

כפי שכבר נזכר, נושאי ביטחון והצפנת מידע נופלים בקטגוריה זו של הסתכלות מאוחדת. במיוחד מעניינות גישות מודרניות המשיגות את אלמנט הסודיות באמצעות ניצול הערוץ הפיזי עצמו וללא הקצאת משאבים מיוחדים (כגון מפתח הצפנה) או הסתמכות על סיבוכיות אלגוריתמית למטרה זו [32]. כאמור, היריעה התאורטית הרחבה של תורת האינפורמציה נוגעת ישירות בתחומים נוספים. נדגים אלמנט זה בהצגת הקשר העמוק שבין גדלים קלאסיים בתורת האינפורמציה לאלו שבעיבוד אותות. נעייין שוב במודל הלינארי הפשוט ב-(5) ונבחר את $B=I$ להיות מטריצת היחידה ואת A להיות פרופורציונית למטריצת היחידה, $A = \sqrt{\text{snr}}I$. בחירה זו נותנת:

$$y = \sqrt{\text{snr}} Hx + n \quad (6)$$

הפרמטר snr משמש מדד יחס אות לרעש. ◀

בחלוקת משאבים (תחומי תדר, אינטרוולי זמן ו/או אלמנטים מרחביים) מחד ובפיענוח המידע המפריע (גם אם הוא לא נחוץ כשלעצמו) וביטול ההפרעה הנובעת ממנו (interference cancellation) מאידך. טכניקות מתקדמות, שללא ספק ימצאו את שימושן הפרקטי לעתיד לבוא, מבוססות על רעיונות תאורטיים של "התאמת" הפרעות [6], [28]. (Interference alignment). בשיטה זו התקשורת מתוכננת באופן שכל מקלט מופרע רק על ידי תת־מרחב של אותות אף על פי שפיזית הוא מופרע על ידי כל המשתמשים (המטריצה H מלאה). את תת־המרחב המשלים מנצל כל משתמש לתקשורת לא מופרעת, כאשר שוב ההפרעה האינהרנטית שהוא גורם לאחרים משויכת אף היא לתת־מרחב של אותו משתמש המופרע מהאות הנוכחי. מתברר כי נושאים אלו קשורים להיבטים מעניינים במתמטיקה ובמיוחד למונחים Renyi's Information Dimension [29], וכן למונחים קלאסיים בתורת המספרים כגון [28] Diophantine Approximation Theory.

קיימים היבטים רבים נוספים למודל תקשורת פשוט זה או למערכות תקשורת המבוססות על קומבינציות של מודלים מהסוג המתואר במשוואה (5). נזכיר כאן לדוגמה נושאים הקשורים לשיתופיות ולרשתות שיתופיות כאשר השיתוף מושג אם בעזרת ממסור (relaying) ואם בשימוש ברשתות מידע (כגון האינטרנט) תוך התחשבות אנליטית במגבלותיהם (backhaul constraints) לעצם ביצוע שיתופי הפעולה בין משתמשים שונים. תקשורת במערכות קוגניטיביות נשענת על תובנה שהתקבלה מאנליזה אינפורמטיבית של גישות אלו. נושאי משוב (feedback) הם בעלי משמעות עמוקה בתורת האינפורמציה מתחילת ימיה, ושנון עצמו תרם מהותית לבעיה זו [4, pp. 221–238]. עקרון המשוב מקבל משנה חשיבות ברשתות תקשורת מרובות־משתמשים שפועלות לדוגמה באופן מבוזר. מתברר כי רעיונות תאורטיים אינפורמטיביים

שהוא הביטוי המרכזי הרלוונטי לקיבול ערוץ במודל MIMO. קשר חשוב זה (9) הוביל לתוצאות משמעותיות בבעיות ישנות וחדשות. לדוגמה, בעזרתו [33] נמצא הקשר הישיר שבין שגיאות מסננים (filters) למחליקים (smothers) לא לינאריים, שהיה בעיה פתוחה קלאסית בעיבוד אותות במשך עשרות שנים. באשר ל-"חדש", קשר זה הוביל למגוון פתרונות ותובנות הנוגעים לבעיות שונות כגון אלו הדנות בקידוד יעיל בערוצי הפרעה וכן בנושאי תקשורת סודית בערוצי (MIMO). לפרטים נוספים, למבט כללי ולהרחבת קשר זה בין אינפורמציה לשגיאת שיערוך ריבועית ממוצעת (MMSE) לערוצים כלליים ולא דווקא גאוסיים, ראו [33], [34] ו-[35].

סיים את המאמר בסיכום קצר ובמבט לעתיד:] בחיבור קצר וכללי זה ניסינו להצביע על הספקטרום הנרחב המכוסה במחקר התאורטי בתורת האינפורמציה, וזאת מעבר לבעיות הקלאסיות של העברתה ועיבודה של אינפורמציה שנחקרו ונחקרים באופן מתמטי רגורוסי במשך עשרות השנים מאז הולדת התחום עם מאמרו הגאוני של קלוד שנון ב-1948 [1].

מיקדנו את המבט בפרספקטיבה סובייקטיבית במודלים לינאריים פשוטים תוך הצגת הרלוונטיות של אלו לתחומים שונים ולשימושים מעשיים. אין להבין מכאן כי המודלים וההיבטים שנידונו הם העיקריים שיש, וגם הפרטים שצוינו (כולל המקורות) חלקיים ביותר. הנושא בכללותו מטופל באלפים רבים של מאמרים ועבודות הנוגעים למגוון שלם של תחומים ובעיות. ההיבטים הבין-תחומיים המצויים בתשתית תורת האינפורמציה צוינו אך באופן כללי וחלקי. היבטים אלו יובילו ביתר שאת להפריה הדדית בין התחומים. אין ספק שהמחקרים בתחום זה ותוצאותיהם השפיעו בעבר וישפיעו בעתיד אף יותר ובצורה מהותית על ההבנה והתובנה באשר למערכות ורשתות תקשורת

◀ מונח מרכזי בתורת האינפורמציה מיום היווסדה הוא האינפורמציה ההדדית הממוצעת (average mutual information) הניתנת לביטוי

$$I(x; y) = E \ln \left\{ \frac{d\{p(x, y)\}}{d\{p(x) \times p(y)\}} \right\} \quad (7)$$

כתוחלת (המסומנת על ידי האופרטור E) של הלוגריתם הטבעי של נגזרת Radon-Nikodim בין מידת ההסתברות המשותפת $p(x, y)$ לבין מכפלת המיידות השיוריות $p(x)p(y)$. גודל זה משמש מדד אינפורמציה בין x ל- y [1], [2], [3] (שימוש בלוגריתם טבעי מגדיר את האינפורמציה ב-nats, ואילו לוגריתם לפי בסיס בינרי מגדיר אותה ב-bits והמעבר ביניהם אלמנטרי). בעיבוד אותות ובסטיסטיקה בכלל נושא השיערוך הוא מרכזי, וחשוב במיוחד הוא המשערך על פי התוחלת המותנית (conditional mean). שיערוך כזה של x על פי המדידה y מסומן ב- $E(x|y)$, וזהו המשערך האופטימלי על פי קריטריון מינימום השגיאה הריבועית הממוצעת (minimum mean square error) ביטוי שגיאה זה, כאשר השיערוך המתבצע הוא לווקטור Hx (כאשר H מטריצה נתונה) מתוך המדידה y ,

$$\text{mmse}(x; \text{snr}) = E \| Hx - HE(x|y) \|^2 \quad (8)$$

הוא מטבע הדברים פונקצייה של snr , וכך הוא מסומן במפורש בביטוי (הנורמה הריבועית מסומנת כ- $\|\cdot\|^2$).

התוצאה המפתיעה שהוכחה ב-[33] קובעת קשר ישיר מתמטי בין ביטויים אלו:

$$\frac{dI(x; y)}{d \text{snr}} = \frac{1}{2} \text{mmse}(x; \text{snr}) \quad (9)$$

קשר המתקיים לכל בחירה של הווקטור האקראי x (בעל תוחלת סופית של הנורמה הריבועית). כאשר x הוא וקטור גאוסני עם רכיבים גאוסיים סטנדרטיים בלתי תלויים סטיסטיים, האינפורמציה ההדדית ניתנת על ידי הביטוי הקלאסי המוכר של לוג דטרמיננט,

$$I(x; y) = \frac{1}{2} \ln \det \| I + \text{snr} HH^T \| \quad (10)$$

מקורות:

- [1] C.E. Shannon, "A Mathematical Theory of Communications," Bell System Tech. Journal, Vol. 27, pp. 379–423, 623–656, July, Oct. 1948.
- [2] T.M. Cover and J.A. Thomas, Elements of Information Theory (second edition) Wiley, New York, 2006, ISBN: 13978-0-471-24195-9.
- [3] I. Csiszar and J. Korner, Information Theory: Coding Theorems for Discrete Memoryless Systems, (second edition), Cambridge University Press, New York, 2011, ISBN: 978-0521-19681-9.
- [4] C.E. Shannon, Collected Papers, Edited by N.J.A. Sloane, A.D. Wyner, IEEE Press, 1993, ISBN: 0-7803-0434-9.
- [5] D. J. C. MacKay, Information Theory, Inference and Learning Algorithms, Cambridge University Press, New York, 2003, ISBN: 0-521-64298-1.
- [6] A. El Gamal and Y. H. Kim, Network Information Theory, Cambridge University Press, New York, 2011, ISBN: 978-1-107-00873-1.
- [7] M. Bloch and J. Barros, Physical-Layer Security, From Information Theory to Security Engineering, Cambridge University Press, New York, 2011, ISBN: 978-0-521-51650-1.
- [8] Robert M. Gray, Entropy and Information Theory, Springer Verlag, New York, 1990, ISBN: 3-540-97371-0.
- [9] T. S. Han, Information-Spectrum Methods in Information Theory, Springer, New York, 2003, ISBN: 3-540-43581-6.

במובן הכללי ביותר. השלכות מבורכות צפויות על עצם מהותו של המושג "תקשורת יעילה", ובמיוחד תקשורת אלחוטית ומדיות תקשורת אחרות, כגון תקשורת קווית, תקשורת אופטית וכדומה. לכאורה, נראה כי עסקנו בתחום בוגר ופורה. להערכת המחבר, בשל מגוון הנושאים שחלקם הגדול עדכני ובעל היבטים מעשיים חשובים, עיקר ההתפתחות המחשבתית/תאורטית כנראה עוד לפנינו. האוסף הניכר של בעיות תאורטיות חשובות שנותרו פתוחות מעיד על כך. מתברר שלא כבעבר הלא רחוק, כיום מורגש החוסר בתוצאות מדעיות, תאורטיות מתמטיות, שיאפיינו את הפוטנציאל של טיפול במובן הכללי ביותר באינפורמציה מחד ואת המגבלות האולטימטיביות שלו מאידך, ולעתים אף יזהו את האלגוריתמים היעילים להשגת מטרה זו. נושאים אלו מרתקים ומעוררים השראה כאחד בקרב חוקרים ובקרב כל הקהילה המדעית/טכנולוגית שהשלכותיהם המבורכות של המחקרים בתחום נוגעות לה. ארצנו התברכה בתחום זה בקהילת מדענים אקטיביים צעירים ובוגרים הפועלים נמרצות זה עשרות שנים, ופעילותם זוהה להדום ולהערכה בעולם כולו. אנו תקווה כי פעילות זו אף תגבר ותקדם את מדע האינפורמציה התאורטי בכלל ואת מגוון יישומיו בפרט. ■

תודות

תודתי העמוקה נתונה לעמיתי בארץ ובעולם, שעמם שיתפתי, ועודני משתף, פעולה במחקר מרתק. אני אסיר תודה לטכניון, המשמש ביתי המדעי זה שנים רבות, להנהלתו, לפקולטה להנדסת חשמל, לעובדיה ומוביליה, לעמיתי וחבריי, מוריי ותלמידי לאורך השנים. אני מודה גם לקרנות לסוגיהן שתמכו ותומכות במחקרי בתחום זה לאורך השנים ובמיוחד ל־Israel Science Foundation (ISF) ול־Binational (BSF) US-Israel Science Foundation.

- Information Theoretic and Communications Aspects," IEEE Trans. Inform. Theory, Vol. 44, No. 6, pp. 2619–2692, Oct. 1998.
- [19] A. Tulino and S. Verdú, "Random Matrix Theory and Wireless Communications," Foundations and Trends in Commun. and Inform. Theory, Vol. 1, No. 1, pp. 1–182, now Publishers, Hanover, MA, USA, 2004.
- [20] A. Tulino, G. Caire, S. Verdú and S. Shamai (Shitz), "Support Recovery with Sparsely Sampled Free Random Matrices," IEEE Trans. Inform. Theory, Vol. 59, No. 7, pp. 4243–4271, July 2013.
- [21] S. Shamai and S. Verdú, "The Effect of Frequency-Flat Fading on the Spectral Efficiency of CDMA," IEEE Trans. Inform. Theory, Vol. 47, No. 4, pp. 1302–1327, May 2001.
- [22] G. Caire and S. Shamai (Shitz), "On the Achievable Throughput of a Multi-Antenna Gaussian Broadcast Channel," IEEE Trans. Inform. Theory, Vol. 49, No. 7, pp. 1691–1706, July 2003.
- [23] H. Weingarten, Y. Steinberg, and S. Shamai (Shitz), "The Capacity Region of the Gaussian Multiple-Input Multiple-Output Broadcast Channel," IEEE Trans. Inform. Theory, Vol. 52, No. 9, pp. 3936–3964, Sept. 2006.
- [24] A. Bennatan, D. Burshtein, G. Caire and S. Shamai (Shitz), "Superposition
- [10] M. S. Pinsker, Information and Information Stability of Random Variables and Processes, Holden-Day, Inc., London 1964.
- [11] M. Mezard and A. Montanari, Information, Physics, and Computation, Oxford University Press, New York, 2009, ISBN: 978-0-19-857083-7.
- [12] N. Merhav, "Statistical Physics and Information Theory," Foundations and Trends in Commun. and Inform. Theory, Vol. 6, No. 1-2, pp. 1–212, now Publishers, Hanover, MA, USA, 2009.
- [13] E. Desurvire, Classical and Quantum Information Theory, Cambridge University Press, New York, 2009, ISBN: 978-0-521-88171-5.
- [14] A. Motahari, G. Bresler and D. Tse, "Information Theory of DNA Sequencing," IEEE Trans. Inform. Theory, Vol. 59, No. 10, pp. 6273–6289, Oct. 2013.
- [15] C. E. Shannon, "The Bandwagon" (Editorial), IRE Trans. Inform. Theory, Vol. 2, No. 1, pp. 3, March 1956.
- [16] T. Richardson and R. Urbanke, Modern Coding Theory, Cambridge University Press, New York, 2008, ISBN: 978-0-521-85229-6.
- [17] שלמה שמאי (ראיון), תורת התקשורת והמידע: המעבר "מאיך לעשות" "למה לעשות", טכנולוגיות, מס' 371, עמודים 19–14, ינואר 2012.
- [18] E. Biglieri, J. Proakis and S. Shamai (Shitz), "Fading Channels:

- Formula," IEEE Inter. Symp. Inform. Theory (ISIT2011), St. Petersburg, Russia, July 31–Aug. 5, 2011.
- [30] R. W. Yeung, *Information Theory and Network Coding*, Springer, New York, 2008, ISBN: 978-0-387-79233-0.
- [31] S. Shamai and I. Sason, "Variations on the Gallager Bounds, Connections and Applications," *IEEE Trans. Inform. Theory*, Vol. 48, No. 12, pp. 3029–3051, Dec. 2002.
- [32] Y. Liang, H.V. Poor and S. Shamai, "Information Theoretic Security," *Foundations and Trends in Commun. and Inform. Theory*, Vol. 5, No. 4–5 (2008), pp. 355–580, now Publishers, Hanover, MA, USA, 2009.
- [33] D. Guo, S. Shamai, and S. Verdú, "Mutual Information and MMSE in Gaussian Channels," *IEEE Trans. Inform. Theory*, Vol. 51, No. 4, pp. 1261–1282, April 2005.
- [34] S. Shamai, "From Constrained Signaling to Network Interference Alignment via an Information-Estimation Perspective," *IEEE Information Theory Society Newsletter*, Vol. 62, No. 7, pp. 6–24, Sept. 2012.
- [35] D. Guo, S. Shamai, and S. Verdú, "The Interplay Between Information and Estimation Measures," *Foundations and Trends in Signal Processing*, Vol. 6, No. 4 (2012), pp. 243–429, now Publishers, Hanover, MA, USA, 2013.
- Coding for Side-Information Channels," *IEEE Trans. Inform. Theory*, Vol. 52, No. 5, pp. 1872–1889, May 2006.
- [25] G. Caire, S. Shamai, Y. Steinberg and H. Weingarten, "On Information Theoretic Aspects of MIMO-Broadcast Channels," Chapter in *Space-Time Wireless Systems: From Array Processing to MIMO Communications*, edited: H. Bolcskei, D. Gesbert, C. Papadias and A.J. van der Veen," Cambridge University Press, Cambridge, UK, 2006.
- [26] O. Simeone, N. Levy, A. Sanderovich, O. Somekh, B. Zaidel, V. Poor and S. Shamai, "Cooperative Wireless Cellular Systems," *Foundations and Trends in Commun. and Inform. Theory*, Vol. 8, No. 1-2, pp. 1–177, now Publishers, Hanover, MA, USA, 2012.
- [27] D. Gesbert, S. Hanly, H. Huang, S. Shamai, O. Simeone and Wei Yu, "Multi-Cell MIMO Cooperative Networks: A New Look at Interference," *J. Selec. Areas in Commun. (JSAC)*, Vol. 28, No. 9, pp. 1380–1408, Dec. 2010.
- [28] S. A. Jafar, "Interference Alignment A New Look at Signal Dimensions in a Communication Network," *Foundations and Trends in Commun. and Inform. Theory*, Vol. 7, No. 1, pp. 1–134, now Publishers, Hanover, MA, USA, 2010.
- [29] Y. Wu, S. Shamai, and S. Verdú, "Degrees of Freedom of the Interference Channel: a General