THE ABEL PRIZE 2021

האקדמיה הנורווגית למדעים ומדעי הרוח החליטה להעניק את פרס אבל לשנת 2021

ללסלו לובאס מאוניברסיטת אטווש לוראנד בבודפשט, הונגריה וכן

לאבי ויגדרזון מהמכון למחקר מתקדם, פרינסטון, ארה»ב,

«על תרומתם היסודית למדעי המחשב התאורטיים ולמתמטיקה הבדידה, ועל תפקידם המוביל בעיצובם לתחומים מרכזיים במתמטיקה המודרנית»

מדעי המחשב התאורטיים (TCS) עוסקים בחקר העוצמה והמגבלות של המחשוב. שורשיו ניזונים מיצירות היסוד של קורט גודל, אלונזו צ׳רץ׳, אלן טיורינג וג׳ון פון נוימן, אשר הובילו לפיתוח מחשבים פיזיים ממשיים. מדעי המחשב התאורטיים נשענים על שתי דיסציפלינות משלימות: תכנון אלגוריתמים - לפיתוח שיטות יעילות עבור מספר רב של בעיות חישוביות; ותורת סיבוכיות החישוב - המציגה מגבלות מובנות של יעילותם האלגוריתמים. המושג של אלגוריתמים עם זמן ריצה פולינומי אשר הוצג לראשונה בשנות ה-60 על ידי אלן קובהאם, ג׳ק אדמונדס ואחרים, וההשערה המפורסמת P≠NP של סטיבן קוק, לאוניד לוין, וריצ׳רד קארפ, היוו השפעה חזקה על התחום כולו ועל עבודתם של לובאס וויגדרזון.

מלבד השפעתם העצומה על מדעי המחשב ועל הפרקטיקה של שימוש במחשבים, מדעי המחשב התאורטיים מספקים את יסודות הקריפטוגרפיה, ולשימוש ב»עדשה חישובית». יש השפעה הולכת וגדלה על מספר תחומי מדעים אחרים. למבנים בדידים כגון גרפים, מחרוזות ותמורות תפקיד מרכזי במדעי המחשב התאורטיים, ובאופן טבעי המתמטיקה הבדידה ומדעי המחשב התאורטיים הפכו לתחומים קרובים במיוחד. בעוד ששני התחומים הללו הפיקו תועלת רבה מאוד מתחומים אחרים שהם מסורתיים יותר במתמטיקה, חלה השפעה גוברת גם בכיוון ההפוך. יישומים, מושגים וטכניקות של מדעי המחשב התאורטיים הניעו אתגרים חדשים, פתחו כיווני מחקר חדשים ופתרו בעיות פתוחות חשובות במתמטיקה הטהורה והשימושית.

לסלו לובאס ואבי ויגדרזון הנם מובילים בהתפתחויות אלה בעשורים האחרונים. עבודותיהם משתלבות בדרכים רבות. נציין במיוחד את התרומה הבסיסית של שני מדענים אלה להבנת האקראיות בחישוב ולבחינת גבולות החישוב היעיל.

לסלו לובאס פיתח, יחד עם אריין לנסטרה והנדריק לנסטרה, את אלגוריתם LLL בתורת הסריגים. בהינתן סריג רב ממדי, אלגוריתם זה מוצא בסיס כמעט אורתוגונלי עבורו. נוסף על מספר יישומים כגון אלגוריתם לפירוק פולינומים רציונליים, אלגוריתם LLL הוא כלי מועדף על מנתחי הקריפטוגרפיה, מפני שהוא מסוגל לפצח בהצלחה מספר מערכות הצפנה שהוצעו. באופן מפתיע, הניתוח של אלגוריתם LLL משמש גם כדי לתכנן מערכות הצפנה חדשות יותר, מבוססות על סריגים, אשר ככל הנראה עומדות בפני התקפות אפילו מצד מחשבים קוונטיים. עבור כמה טכניקות קריפטוגרפיות, כגון ההצפנה ההומומורפית, היישומים היחידים הידועים נוצרו בעזרת מערכות הצפנה מבוססות סריג כאלה.

אלגוריתם LLL הוא רק אחת מבין רבות מתרומותיו בעלות החזון של לובאס. הוא הוכיח את ה»למה המקומית», שהיא כלי ייחודי להוכחת קיומם של מאורעות קומבינטוריים נדירים, בניגוד לשיטה ההסתברותית הסטנדרטית המופעלת כאשר המאורעות קיימים בשפע. יחד עם מרטין גרטשל ולקס שרייבר, הוא הראה כיצד לפתור ביעילות בעיות של תכנון חיובי-למחצה, וגרם למהפכה בעיצוב אלגוריתמים. הוא תרם לתורה של ההילוכים המקריים עם שימושים לאלגוריתמים

לחישוב מקורב של נפחים בממדים גבוהים, וקישר זאת לבעיות איזופרימטריות אקלידיות. מאמרו עם אוריאל פייגה, שפי גולדווסר, שמואל ספרא ומריו סגדי בנושא הוכחות הניתנות לבדיקה הסתברותית, סיפק גרסה מוקדמת של משפט PCP, תוצאה בעלת השפעה עצומה המראה כי ניתן לאמת את נכונות ההוכחות המתמטיות בכלים הסתברותיים, בביטחון רב, על ידי קריאת מספר קטן של תווים בלבד! בנוסף, הוא גם פתר בעיות שהיו פתוחות שנים רבות כגון השערת הגרף המושלם, השערת קנסר, וקביעת הקיבול של שאנון של גרף המחומש. בשנים האחרונות פיתח את התאוריה של גבולות של גרפים (בעבודה משותפת עם כריסטיאן בורג, ג׳ניפר צ׳ייס, לקס שרייבר, ורה שוש, בלש סגדי וקטלין וסטרגומבי). עבודה זו קושרת יחד אלמנטים של תורת הגרפים האקסטרמלית, תורת ההסתברות והפיזיקה הסטטיסטית.

אבי ויגדרזון תרם תרומות רחבות היקף ועמוקות לתורת סיבוכיות החישוב על כל היבטיה, ובמיוחד לתפקיד האקראיות בחישוב. אלגוריתם אקראי הוא אלגוריתם המעיף מטבעות כדי לחשב פתרון נכון בהסתברות גבוהה. במשך עשרות שנים גילו החוקרים אלגוריתמים דטרמיניסטיים לבעיות רבות שרק אלגוריתם אקראי היה ידוע להם לפני כן. האלגוריתם הדטרמיניסטי לבדיקות ראשוניות, מאת אגרוול, קיאל וסקסנה הוא דוגמה מובהקת לאלגוריתם לא אקראי כזה. תוצאות הדרנדומיזציה האלה מעלות את השאלה האם אקראיות היא אי פעם באמת חיונית. בעבודותיו עם לאסלו באבאי, לאנס פורטנו, נועם ניסן וראסל אימפליאצו, הוכיח ויגדרזון כי סביר שהתשובה לכך שלילית. באופן פורמלי, הם הוכיחו השערה חישובית דומה בצורתה להשערת P≠NP, גוררת ש- P = BPP. משמעות הדבר היא כי ניתן לבצע דרנדומיזציה לכל אלגוריתם אקראי ולהפוך אותו לאלגוריתם דטרמיניסטי בעל יעילות דומה. יתר על כן, כי הדרנדומיזציה הנה כללית ואוניברסלית, ללא קשר למבנה הפנימי של האלגוריתם האקראי.

דרך נוספת להסתכל על עבודה זו היא בתור מאזן בין קושי לבין אקראיות: אם קיימת בעיה קשה מספיק, אזי ניתן לדמות אקראיות בעזרת אלגוריתמים דטרמיניסטיים יעילים. עבודתו המאוחרת יותר של ויגדרזון יחד עם אימפליאצו וולנטיין קבנטס מוכיחה את הכיוון ההפוך: קיום אלגוריתמים דטרמיניסטיים יעילים אפילו לבעיה מסויימת (שעבורה קיימים אלגוריתמים אקראיים), גוררים שחייבת להתקיים בעיה קשה שכזו.

עבודה זו קשורה קשר הדוק עם מבנים של מחוללים פסבדו-אקראיים (בעלי מראה אקראי). עבודותיו של ויגדרזון יצרו מחוללים פסבדו-אקראיים ההופכים מספר קטן של סיביות אקראיות באמת לסיביות פסבדו-אקראיות רבות, «מחלצים» המסוגלים לחלץ סיביות בעלות אקראיות כמעט מושלמת מתוך מקור לא מושלם של אקראיות, וכן גרפי רמזי, וגרפים מרחיבים - כלומר גרפים דלילים בעלי קישוריות גבוהה. יחד עם עומר ריינגולד וסליל ואדהן, הוא הציג את מושג גרף הזיג-זג, שנותן שיטה חדשה לבניית גרפים מרחיבים, מושג שנתן השראה להוכחה הקומבינטורית של משפט PCP על ידי אירית דינור ולאלגוריתם היעיל לזיכרון עבור בעיית קשירות הגרף על ידי ריינגולד. אלגוריתם אחרון זה נותן שיטת ניווט במבוך גדול תוך זכירת זהותם של מספר קבוע בלבד של צמתים במבוך!

תרומותיו הנוספות של ויגדרזון כוללות הוכחות אפס-ידיעה המספקות הוכחות לטענות מבלי לחשוף מידע נוסף מלבד תוקף הטענות, וחקר הגבולות התחתונים של יעילות פרוטוקולי תקשורת, של מעגלים ושל מערכות הוכחה פורמליות.

הודות להובלה של לובאס וויגדרזון, המתמטיקה הדיסקרטית והתחום הצעיר יחסית של מדעי המחשב התאורטיים מבוססים כיום כתחומים מרכזיים במתמטיקה המודרנית.