Title	QUASI-PERMUTATION POLYNOMIALS
Author	Suphawan Janphaisaeng
Advisor	Professor Vichian Laohakosol, Ph.D.
Co-Advisor	Associate Professor Wiwat Wanicharpichat, M.Ed.
	Assistant Professor Pattira Ruengsinsub, Ph.D.
Type of Degree	Thesis Ph.D. in Mathematics,
	Naresuan University, 2007
Keywords	Finite field, Permutation polynomial

ABSTRACT

Through a well-known interpolation technique, each function from one subset into another subset of a finite field is uniquely representable by a polynomial of bounded degree over the same field. This implies that to study functions over a finite field, it suffices to consider merely polynomials over that field. A quasi-permutation polynomial is a polynomial which is a bijection from one subset of a finite field onto another having the same number of elements. This is a natural generalization of the familiar permutation polynomials. Since this notion is introduced here for the first time, the thesis starts with derivations of its basic properties. Then a general necessary and sufficient condition for a quasi-permutation polynomial is proved. This characterization, whose existence seems surprising, is established using ideas from an old work of Carlitz and Lutz. Though it is not easy to use, it does contain the well-known Hermite's criterion for permutation polynomials as well as a number of other criteria depending on the permuted domain and range. Characterizations of quasi-permutation polynomials via characters along the same line as those of permutation polynomials are then investigated. Linearized quasi-permutation polynomials which form a nontrivial and useful class are determined. Imposing vector space structure on such linearized

polynomials yields interesting indepencence results extending the classical ones due to Zhou. Miscellaneous other types of quasi-permutation polynomials, such as monomials and binomials are found. The thesis ends with the problem of counting the number of quasi-permutation polynomials of fixed degrees. Employing ideas from a recent work of Das, the number of quasi-permutation polynomial of a fixed degree is shown to be closely related to the number of solutions of a system of linear equations over a finite filed. Nearly all results proved here generalize those of the classical permutation polynomials. However, as to be expected, in a number of instances, reasonable results are obtainable only after some structures are provided to the domain and range and in general if the shape of quasi-permutation polynomials are not of primary interest, the problem of searching for quasi-permutation polynomials is almost equivalent to that of determining polynomials which are injective.

ชื่อเรื่อง พหุนามเรียงสับเปลี่ยนแบบควอไซ
ผู้วิจัย สุภาวรรณ จันทร์ไพแสง
ประธานที่ปรึกษา ศาสตราจารย์ ดร.วิเชียร เลาหโกศล
กรรมการที่ปรึกษา รองศาสตราจารย์วิวรรธน์ วณิชาภิชาติ
ผู้ช่วยศาสตราจารย์ ดร.ภัททิรา เรืองสินทรัพย์
ประเภทสารนิพนธ์ วิทยานิพนธ์ วท.ด. สาขาวิชาคณิตศาสตร์, มหาวิทยาลัยนเรศวร, 2550
คำสำคัญ ฟิลด์จำกัด, พหุนามเรียงสับเปลี่ยน

บทคัดย่อ

แต่ละฟังก์ชันจากเซตย่อยหนึ่งไปยังอีกเซตย่อยหนึ่งของฟิลด์จำกัดสามารถแทนได้ด้วยพหุนามที่ระดับขั้นมีขอบเขตเพียงแบบเดียวเท่านั้นเหนือฟิลด์เดียวกัน จากความจริงดังกล่าวในการศึกษาฟังก์ชันเหนือฟิลด์จำกัด จึงเพียงพอที่จะพิจารณาเพียงพหุนามเหนือฟิลด์นั้น พหุนามเรียงสับเปลี่ยนแบบควอไซ คือ พหุนามซึ่งเป็นฟังก์ชันหนึ่งต่อหนึ่งจากเซตย่อยหนึ่งไปทั่วถึงอีกเซตย่อยหนึ่งที่มีจำนวนสมาชิกเท่ากัน ซึ่งเป็นการวางนัยทั่วไปของพหุนามเรียงสับเปลี่ยนที่เรารู้จัก เนื่องจากแนวคิดนี้เป็นการกล่าวถึงครั้งแรก วิทยานิพนธ์ฉบับนี้จึงเริ่มต้นด้วยการศึกษาสมบัติพื้นฐาน จากนั้นได้พิสูจน์เงื่อนไขทั่วไปที่จำเป็นและเพียงพอสำหรับพหุนามเรียงสับเปลี่ยนแบบควอไซ การจำแนกที่น่าสนใจนี้ได้แนวคิดมาจากงานวิจัยของคาร์ลิทซ์และลูทซ์ ถึงแม้ว่าไม่ง่ายนักที่จะใช้ แต่เกณฑ์ของเฮอร์มิทสำหรับพหุนามเรียงสับเปลี่ยนรวมทั้งเกณฑ์อื่นๆ อีกจำนวนหนึ่งที่ขึ้นกับโดเมนและเรนจ์ที่เรียงสับเปลี่ยนก็เป็นกรณีเฉพาะของการจำแนกนี้ จากนั้นได้ศึกษาการจำแนกของพหุนามเรียงสับเปลี่ยนแบบควอไซโดยใช้แคแรกเทอในทำนองเดียวกับการศึกษาของพหุนามเรียงสับเปลี่ยนและได้กำหนดพหุนามเรียงสับเปลี่ยนแบบควอไซในรูปลิเนียร์ไรซ์ซึ่งเป็นคลาสที่ไม่ซัดและมีประโยชน์ การกำหนดโครงสร้างปริภูมิเวกเตอร์บนพหุนามในรูปลิเนียร์ไรซ์ทำให้เกิดผลลัพธ์ที่น่าสนใจซึ่งเป็นการขยายงานของซู นอกจากนั้นเราได้ค้นพบรูปแบบอื่นๆ ที่มีลักษณะต่างๆ กันของพหุนามเรียงสับเปลี่ยนแบบควอไซ ตัวอย่างเช่น เอกนามและทวินามหัวข้อสุดท้ายของวิทยานิพนธ์ฉบับนี้เป็นการศึกษาการนับจำนวนของพหุนามเรียงสับเปลี่ยนแบบควอไซที่ตรึงระดับขั้น โดยใช้แนวคิดจากงานวิจัยเมื่อไม่นานมานี้ของแดสเราพบว่าเราสามารถนับจำนวนของพหุนามเรียงสับเปลี่ยนแบบควอไซที่ตรึงระดับขั้นโดยการนับจำนวนของผลเฉลยของระบบสมการเชิงเส้นบนฟิลด์จำกัด ผลลัพธ์เกือบทั้งหมดที่ได้พิสูจน์ในวิทยานิพนธ์

ฉบับนี้เป็นการวางนัยทั่วไปของพหุนามเรียงสับเปลี่ยน อย่างไรก็ตามจากตัวอย่างที่ทำการศึกษา เราพบว่าผลลัพธ์ที่เหมาะสมจะตามมาเพียงถ้าเราให้โครงสร้างบางอย่างบนโดเมนและเรนจ์ และในกรณีทั่วไป ถ้าพหุนามเรียงสับเปลี่ยนแบบควอไซไม่ได้อยู่ในรูปที่เราสนใจ ปัญหาในการหาพหุนามเรียงสับเปลี่ยนแบบควอไซเกือบจะสมมูลกับปัญหาในการกำหนดพหุนามที่เป็นฟังก์ชันหนึ่งต่อหนึ่ง