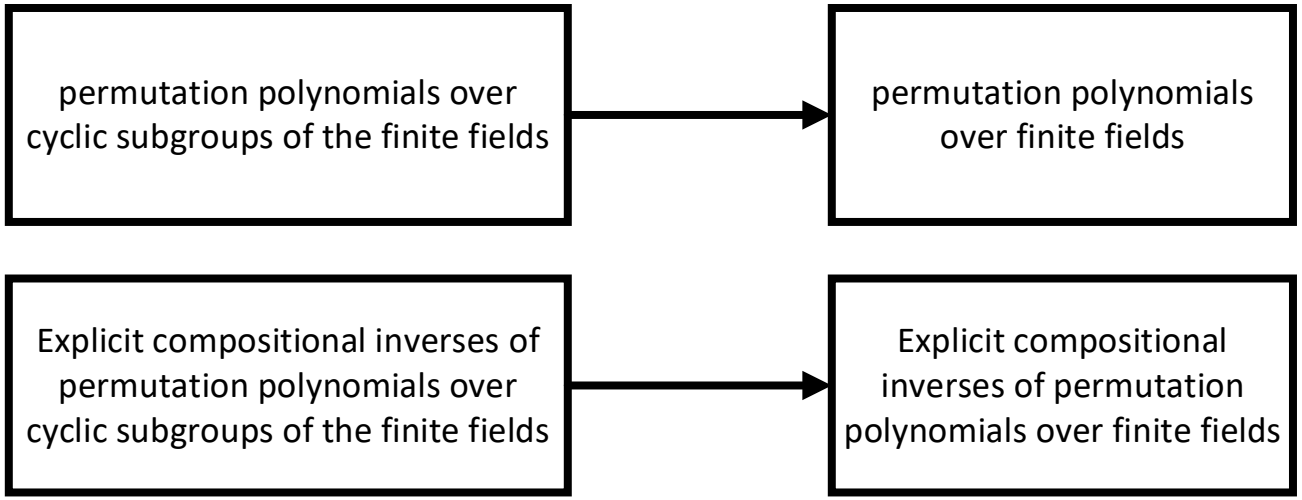
New permutation polynomials with coefficients 1 over finite fields and their compositional inverses

Hutao SONG, Hua GUO, Fengju GAO, Xiyong ZHANG, Jianwei LIU

Frontiers of Computer Science, DOI: 10.1007/s11704-025-50191-9

Problems & Ideas

- Problems of permutation polynomials over finite fields:
  - Construction methods of permutation polynomials over finite fields need further research.
  - Explicit compositional inverses of permutation polynomials are currently relatively rare.
- Ideas: Permutation polynomials over finite fields are closely related to permutation polynomials over cyclic subgroups of the finite fields.



The relation between permutation polynomials over cyclic subgroups of the finite fields and permutation polynomials over finite fields.

Main Contributions

- Contributions:
  - Two new construction methods of permutation polynomials over $\mathbb{F}_{q^2}$;
  - Three new permutation polynomials over $\mathbb{F}_{2^{2m}}$ with coefficients 1;
  - Explicit compositional inverses of new permutation polynomials for some special parameters;
  - equivalence discussion between new permutation polynomials and the known permutation polynomials.

Theorem 1. Let q be a prime power and $g_1, g_2 \in \mathbb{F}_{q^2}[x]$. Assume that $g_2(x) = \sum_{i=0}^{s} a_i x^i$ with $a_i^q = a_{s-i}$ has no root in μ_{q+1} . Denote $g_1(x)g_2(x)$ by $g(x)$, then $f(x) = x^{r+s}g(x^{q-1})$ permutes $\mathbb{F}_{q^2}$ if and only if both $\gcd(r+s, q-1) = 1$ and $x^r g_1(x)^{q-1}$ permutes μ_{q+1}.

Theorem 2. Let q be a prime power and $g_1, g_2 \in \mathbb{F}_{q^2}[x]$. Assume that $g_2(x) = \sum_{i=0}^{s} a_i x^i$ with $a_i^q = a_{s-i}$ has no root in μ_{q+1} and $g_2(x) | g_1(x)$. Denote $g_1(x)/g_2(x)$ by $g(x)$, then $f(x) = x^{r-s}g(x^{q-1})$ permutes $\mathbb{F}_{q^2}$ if and only if both $\gcd(r-s, q-1) = 1$ and $x^r g_1(x)^{q-1}$ permutes μ_{q+1}.

New permutation polynomial	Known permutation polynomial	Reference
$f_1(x)$, $k=2$, $s=0$	$x^5 + x^{2^m+4} + x^{5\cdot 2^m}$	[4] Conjecture 2
$f_1(x)$, $k=1$, $s=1$	$x^5 + x^{4\cdot 2^m+1} + x^{5\cdot 2^m}$	[5] Theorem 4.4
$f_2(x)$, $k=2$, $s=1$	$x^7 + x^{3\cdot 2^m+4} + x^{4\cdot 2^m+3} + x^{5\cdot 2^m+2} + x^{6\cdot 2^m+1}$	[6] Theorem 4.2
$f_3(x)$, $k=3$, $s=0$	$x^7 + x^{2\cdot 2^m+5} + x^{3\cdot 2^m+4} + x^{5\cdot 2^m+2} + x^{6\cdot 2^m+1}$	[6] Theorem 3.5

Two new construction methods of permutation polynomials, and some known permutation polynomials which can be obtained from new permutation polynomials.