F2wPolynomials

Stores the parameters of point sets which will contain 2^{rw} points (see the meaning of r and w below). The parameters can be stored as a polynomial $P(z)$ over $\mathbb{F}_{2^w}[z]$

$$P(z) = z^r + \sum_{i=1}^{r} b_i z^{r-i}$$

where $b_i \in \mathbb{F}_{2^w}$ for $i = 1, \ldots, r$. Let ζ be the root of an irreducible polynomial $Q(z) \in \mathbb{F}_2[z]$. It is well known that ζ is a generator of the finite field $\mathbb{F}_{2^w}$. The elements of $\mathbb{F}_{2^w}$ are represented using the polynomial ordered basis $(1, \zeta, \ldots, \zeta^{w-1})$.

In this class, only the non-zero coefficients of $P(z)$ are stored. It is stored as

$$P(z) = z^{\mathtt{r}} + \sum_{i=0}^{\mathtt{nbcoeff}} \mathtt{coeff}[i] z^{\mathtt{nocoeff}[i]}$$

where the coefficients in `coeff[]` represent the non-zero coefficients b_i of $P(z)$ using the polynomial basis. The finite field $\mathbb{F}_{2^w}$ used is defined by the polynomial

$$Q(z) = z^w + \sum_{i=1}^{w} a_i z^{w-i}$$

where $a_i \in \mathbb{F}_2$, for $i = 1, \ldots, w$. Polynomial Q is stored as the bit vector $\mathtt{modQ} = (a_w, \ldots, a_1)$.

The following files stores the parameters of polynomials in $\mathbb{F}_{2^w}[z]$; the parameters of a polynomial are stored at line number `no` of `filename`. The files are kept in different directories depending on the criteria used in the searches for the parameters defining the polynomials. The different criteria for the searches and the theory behind it are described in [2, 1]. The existing files and the number of polynomials they contain are given in the following tables. The first table below contains files in subdirectory `LFSR_equid_max`. The name of each file indicates the value of r and w for the polynomials. For example, file `f2wR2_W5.dat` in directory `LFSR_equid_max` contains the parameters of 2358 polynomials with $r = 2$ and $w = 5$.

Directory `LFSR_equid_max`

Filename	Num of poly.
f2wR2_W5.dat	2358
f2wR2_W6.dat	1618
f2wR2_W7.dat	507
f2wR2_W8.dat	26
f2wR2_W9.dat	3
f2wR3_W4.dat	369
f2wR3_W5.dat	26
f2wR3_W6.dat	1
f2wR4_W3.dat	117
f2wR4_W4.dat	1
f2wR5_W2.dat	165
f2wR5_W3.dat	1
f2wR6_W2.dat	36
f2wR6_W3.dat	1
f2wR7_W2.dat	10
f2wR8_W2.dat	11
f2wR9_W2.dat	1

Directory `LFSR_equid_sum`

Filename	Num of poly.
f2wR2_W5.dat	2276
f2wR2_W6.dat	1121
f2wR2_W7.dat	474
f2wR2_W8.dat	37
f2wR2_W9.dat	6
f2wR3_W4.dat	381
f2wR3_W5.dat	65
f2wR3_W6.dat	7
f2wR4_W3.dat	154
f2wR4_W4.dat	2
f2wR5_W2.dat	688
f2wR5_W3.dat	5
f2wR6_W2.dat	70
f2wR6_W3.dat	1
f2wR7_W2.dat	9
f2wR8_W2.dat	3
f2wR9_W2.dat	3

Directory `LFSR_mindist_max`

Filename	Num of poly.
f2wR2_W5.dat	1
f2wR2_W6.dat	1
f2wR2_W7.dat	2
f2wR2_W8.dat	2
f2wR2_W9.dat	1
f2wR3_W4.dat	2
f2wR3_W5.dat	2
f2wR3_W6.dat	1
f2wR4_W3.dat	1
f2wR4_W4.dat	1
f2wR5_W2.dat	2
f2wR5_W3.dat	1
f2wR6_W2.dat	4
f2wR6_W3.dat	1
f2wR7_W2.dat	1
f2wR8_W2.dat	1
f2wR9_W2.dat	1

Directory `LFSR_mindist_sum`

Filename	Num of poly.
f2wR2_W5.dat	1
f2wR2_W6.dat	1
f2wR2_W7.dat	1
f2wR2_W8.dat	1
f2wR2_W9.dat	1
f2wR3_W4.dat	1
f2wR3_W5.dat	1
f2wR3_W6.dat	1
f2wR4_W3.dat	1
f2wR4_W4.dat	2
f2wR5_W2.dat	2
f2wR5_W3.dat	2
f2wR6_W2.dat	1
f2wR6_W3.dat	1
f2wR7_W2.dat	2
f2wR8_W2.dat	1
f2wR9_W2.dat	2

Directory `LFSR_tvalue_max`

Filename	Num of poly.
f2wR2_W5.dat	7
f2wR2_W6.dat	1
f2wR2_W7.dat	1
f2wR2_W8.dat	1
f2wR2_W9.dat	1
f2wR3_W4.dat	1
f2wR3_W5.dat	1
f2wR3_W6.dat	1
f2wR4_W3.dat	2
f2wR4_W4.dat	1
f2wR5_W2.dat	14
f2wR5_W3.dat	1
f2wR6_W2.dat	2
f2wR6_W3.dat	1
f2wR7_W2.dat	1
f2wR8_W2.dat	1
f2wR9_W2.dat	1

Directory `LFSR_tvalue_sum`

Filename	Num of poly.
f2wR2_W5.dat	15
f2wR2_W6.dat	1
f2wR2_W7.dat	1
f2wR2_W8.dat	2
f2wR2_W9.dat	1
f2wR3_W4.dat	1
f2wR3_W5.dat	1
f2wR3_W6.dat	1
f2wR4_W3.dat	2
f2wR4_W4.dat	1
f2wR5_W2.dat	13
f2wR5_W3.dat	2
f2wR6_W2.dat	12
f2wR6_W3.dat	1
f2wR7_W2.dat	1
f2wR8_W2.dat	1
f2wR9_W2.dat	1

References

[1] F. Panneton. *Construction d'ensembles de points basée sur des récurrences linéaires dans un corps fini de caractéristique 2 pour la simulation Monte Carlo et l'intégration quasi-Monte Carlo*. PhD thesis, Département d'informatique et de recherche opérationnelle, Université de Montréal, Canada, August 2004.

[2] F. Panneton and P. L'Ecuyer. Infinite-dimensional point sets based on linear recurrences over GF(2^w). In H. Niederreiter and D. Talay, editors, *Monte Carlo and Quasi-Monte Carlo Methods 2004*, Berlin, 2005. Springer-Verlag. to appear.

References

[1] F. Panneton. *Construction d'ensembles de points basée sur des récurrences linéaires dans un corps fini de caractéristique 2 pour la simulation Monte Carlo et l'intégration quasi-Monte Carlo*. PhD thesis, Département d'informatique et de recherche opérationnelle, Université de Montréal, Canada, August 2004.

[2] F. Panneton and P. L'Ecuyer. Infinite-dimensional point sets based on linear recurrences over GF(2^w). In H. Niederreiter and D. Talay, editors, *Monte Carlo and Quasi-Monte Carlo Methods 2004*, Berlin, 2005. Springer-Verlag. to appear.