MSc Project: Definable sets over finite fields.

Ivan Tomašić

This project is aimed at a student with interests not only in algebraic geometry and number theory, but also in logic. A typical formula over finite fields is of form $\varphi(\bar{x}) \equiv \exists y\ p(\bar{x}, y) = 0$, where $\bar{x} = x_1 \dots x_r$ and $p(\bar{x}, y)$ is a polynomial in $r+1$ variables over the prime field $\mathbb{F}_p$. One is then interested, for each $n \in \mathbb{N}$, in counting the number N_n of r-tuples $\bar{x}$ from $\mathbb{F}_{p^n}$ satisfying the formula φ.

For example, let $\varphi(x)$ be the formula $\exists y\ x - y^2 = 0$. The set 'defined' by φ in each finite field $\mathbb{F}_q$ is the set of squares in that field, and has exactly $(q-1)/2+1$ elements. Unfortunately, the situation is not as straightforward as one might guess from this example. For $\varphi(x) \equiv \exists y\ x = y^3$, the number of elements in $\mathbb{F}_q$ satisfying φ is either roughly $q/3$ or q, depending on whether q is congruent to 1 or 5 modulo 6.

The situation is far from hopeless, as the paper [6] shows: the zeta function associated with the sequence N_n, $n \in \mathbb{N}$, is *near-rational.* This means that there is a strong regularity in the sequence in form of a recursive formula determining the whole sequence from the initial few elements.

The first objective of this project is to understand Kiefe's proof, which will also involve some understanding of the Lang-Weil estimates for finite fields ([7], [2]), rationality of zeta functions associated with algebraic varieties over finite fields ([5], [4]), as well as some understanding of the model-theoretic reasons for considering only the formulae of the above form ([1]).

The second objective is of experimental nature. The student should write a simple computer program for calculating the numbers N_n and then attempt to find the relationship between the size of the set defined by $\varphi \wedge \psi$ and the sizes of sets defined by φ and ψ. The probabilistic language enters the picture at this stage and it should become clear that definable sets over finite fields of increasing size behave as 'random events' of certain probability, and this should be a motivation for eventually reading [3], [1] and [8].

References

[1] Chatzidakis, Zoé; van den Dries, Lou; Macintyre, Angus. *Definable sets over finite fields*, **J. Reine Angew. Math.**, 427, 1992, pp. 107–135,

[2] Fried, Michael D.; Jarden, Moshe. **Field arithmetic.** Second edition. Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics, 11. Springer-Verlag, Berlin, 2005.

[3] Fried, Michael D.; Haran, Dan; Jarden, Moshe. *Effective counting of the points of definable sets over finite fields.* **Israel J. Math.** 85 (1994), no. 1-3, 103–133.

[4] Grothendieck, Alexander. *Formule de Lefschetz et rationalité des fonctions L.* **Sminaire Bourbaki,** Vol. 9, Exp. No. 279, 41–55, Soc. Math. France, Paris, 1995.

[5] Katz, Nicholas M. *An overview of Deligne's proof of the Riemann hypothesis for varieties over finite fields.* Mathematical developments arising from Hilbert problems (Proc. Sympos. Pure Math., Vol. XXVIII, Northern Illinois Univ., De Kalb, Ill., 1974), pp. 275–305. Amer. Math. Soc., Providence, R.I., 1976.

[6] Kiefe, Catarina. *Sets definable over finite fields: their zeta-functions*, **Trans. Amer. Math. Soc.**, vol. 223, 1976, pp. 45–59,

[7] Lang, Serge; Weil, André. *Number of points of varieties in finite fields*, **Amer. J. Math.**, 76, 1954, pp. 819–827,

[8] Tomašić, Ivan. *Independence, measure and pseudofinite fields.* **Selecta Mathematica, New ser.** 12 (2006), pp. 271–306.