

On almost small and almost large super-Vandermonde sets in $GF(q)$

Citation for published version (APA):

Blokhuis, A., Marino, G., Mazzocca, F., & Polverino, O. (2017). On almost small and almost large super-Vandermonde sets in $GF(q)$. *Designs, Codes and Cryptography*, 84(1-2), 197-201.
<https://doi.org/10.1007/s10623-016-0254-z>

DOI:

[10.1007/s10623-016-0254-z](https://doi.org/10.1007/s10623-016-0254-z)

Document status and date:

Published: 01/07/2017

Document Version:

Publisher's PDF, also known as Version of Record (includes final page, issue and volume numbers)

Please check the document version of this publication:

- A submitted manuscript is the version of the article upon submission and before peer-review. There can be important differences between the submitted version and the official published version of record. People interested in the research are advised to contact the author for the final version of the publication, or visit the DOI to the publisher's website.
- The final author version and the galley proof are versions of the publication after peer review.
- The final published version features the final layout of the paper including the volume, issue and page numbers.

[Link to publication](#)

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal.

If the publication is distributed under the terms of Article 25fa of the Dutch Copyright Act, indicated by the "Taverne" license above, please follow below link for the End User Agreement:

www.tue.nl/taverne

Take down policy

If you believe that this document breaches copyright please contact us at:

openaccess@tue.nl

providing details and we will investigate your claim.

On almost small and almost large super-Vandermonde sets in $GF(q)$

A. Blokhuis¹ · G. Marino² · F. Mazzocca² ·
O. Polverino²

Received: 3 March 2016 / Accepted: 8 July 2016 / Published online: 4 August 2016
© The Author(s) 2016. This article is published with open access at Springerlink.com

Abstract A set $T \subset GF(q)$, $q = p^h$ is a *super-Vandermonde set* if $\sum_{y \in T} y^k = 0$ for $0 < k < |T|$. We determine the structure of super-Vandermonde sets of size $p + 1$ (almost small) and size $q/p - 1$ (almost large).

Keywords Finite geometry · Finite fields · Vandermonde set

Mathematics Subject Classification 05E · 51E

1 Introduction

A *super-Vandermonde set* (short: an sV-set) in $GF(q)$, $q = p^h$, p a prime, is a set T of size $1 < t < q$ such that

$$\pi_k(T) := \sum_{y \in T} y^k = 0,$$

for $0 < k < t$. It follows from the non-singularity of the Vandermonde matrices $(y^k)_{y,k}$, $y \in T$ and $k \in [0, t]$ resp. $k \in (0, t]$ that $0 \notin T$ and that $\pi_t(T) \neq 0$ (in particular $p \nmid t$). The Newton identities relating the power sums $\pi_k(T)$ and the elementary symmetric polynomials

This is one of several papers published in *Designs, Codes and Cryptography* comprising the special issue in honor of Andries Brouwer's 65th birthday.

✉ A. Blokhuis
a.blokhuis@tue.nl

¹ Department of Mathematics and Computer Science, Eindhoven University of Technology, Eindhoven, The Netherlands

² Dipartimento di Matematica e Fisica, Seconda Università degli Studi di Napoli, Caserta, Italy

$\sigma_k(T)$ imply that in the polynomial

$$f(Z) := \prod_{y \in T} (Z - y) = \sum (-1)^k \sigma_k(T) Z^{t-k},$$

the only possible nonzero coefficients are the constant term $(-1)^t \sigma_t$ and the coefficient of Z^{t-k} : $(-1)^k \sigma_k$ with $k \equiv 0 \pmod p$. The Newton-identities are given by:

$$k\sigma_k = \sum_{m=1}^k (-1)^{m-1} \pi_m \sigma_{k-m},$$

and we see that indeed $\sigma_k = 0$ if k is not divisible by p (and less than t).

In terms of the inverses of the elements in T , we get that being sV is equivalent to

$$\phi(Y) := \prod_{y \in T} (Y - y^{-1}) = Y^t + g(Y),$$

with g a p -th power.

The underlying notion of Vandermonde set was introduced by Gács and Weiner in [1]. They appear at several places in the investigation of special point sets in finite projective planes. More about this, as well as many examples, can be found in Chapter 1 of the thesis of Takáts [2], or in her paper [3] with Péter Sziklai, which also classifies small and large sV-sets. Here small means $t < p$, and small sV-sets are cosets of multiplicative subgroups of $GF(q)^*$: in this case the polynomial g is constant, so

$$\phi(Y) = \prod_{y \in T} (Y - y^{-1}) = Y^t - c,$$

where $t \mid q - 1$ and c is a t -th power, so that T is a coset of the group of t -th roots of unity.

By large we mean $t > q/p$ and again we get cosets of multiplicative subgroups, corresponding to the case that $g = -c$ is constant. The proof in this case is much more involved, but in the final section we will give a simpler proof.

2 Super-Vandermonde sets of size $p + 1$

If T is an sV-set of size $p + 1$, then the polynomial $\prod_{y \in T} (Z - y)$ is of the form $f(Z) = Z^{p+1} + aZ + b$, so our problem is to classify the polynomials of this form that are fully reducible over $GF(q)$. Notice that two different polynomials of this form have a gcd of degree at most one, so that two elements of $GF(q)$ are contained in at most one sV-set of size $p + 1$. We will see in fact that two elements are contained in an sV-set of this size precisely when they have the same $GF(p)$ -norm. We will prove in the next theorem that they can all be obtained from 2-dimensional $GF(p)$ -vector subspaces of $GF(q)$.

Theorem 2.1 *Let T be an sV-set in $GF(q)$, $q = p^h$, p prime, of size $p + 1$. Then there exists $\alpha \in GF(q)^*$ such that*

$$T = \{\alpha x_1^{p-1}, \dots, \alpha x_{p+1}^{p-1}\}, \tag{1}$$

where $\{x_1, \dots, x_{p+1}\}$ represent the 1-dimensional subspaces of a 2-dimensional $GF(p)$ -vector subspace of $GF(q)$.

Conversely, every 2-dimensional $GF(p)$ -vector subspace of $GF(q)$ defines a family of $q - 1$ sV-sets of type (1). In particular, the elements of an sV-set of size $p + 1$ have the same norm over $GF(p)$.

Proof We first observe that if $T = \{y_1, \dots, y_t\}$ is an sV-set, then for each $\gamma \in GF(q)^*$, the set $\gamma T = \{\gamma y_1, \dots, \gamma y_t\}$ is an sV-set as well (and of the same size of course). We first show that 2-dimensional subspaces give rise to sV-sets. Let U be a 2-dimensional $GF(p)$ -vector subspace of $GF(q)$, then U is the set of zeros of a polynomial of the form

$$X^{p^2} + aX^p + bX, \tag{2}$$

for some $a, b \in GF(q)$. If x_1 and x_2 are two nonzero roots of (2) which are not proportional over $GF(p)$, then x_1^{p-1} and x_2^{p-1} are two different roots of the polynomial $Z^{p+1} + aZ + b$, which turns out to be fully reducible over $GF(q)$. It follows that for each $\alpha \in GF(q)^*$

$$\alpha T = \{\alpha x^{p-1} : x \text{ is a nonzero root of (2)}\}$$

is an sV-set of size $p + 1$.

On the other hand let $T = \{y_1, \dots, y_{p+1}\}$ be an sV-set of size $p + 1$ and let

$$f(Z) = Z^{p+1} + aZ + b \tag{3}$$

be the associated polynomial. Then, there exist $y_i, y_j \in T$, with the same $GF(p)$ -norm δ . Let α be an element of $GF(q)^*$ with norm $N(\alpha) = \delta$ and set $z_k := y_k/\alpha$, for $k \in \{1, \dots, p + 1\}$. Then

$$\frac{1}{\alpha}T := \{z_1, \dots, z_{p+1}\},$$

is an sV-set of size $p + 1$ with $N(z_i) = N(z_j) = 1$ and its associated polynomial is

$$Z^{p+1} + \frac{a}{\alpha^p}Z + \frac{b}{\alpha^{p+1}}.$$

Denoting by x_i and x_j the elements of $GF(q)^*$ such that $z_i = x_i^{p-1}$ and $z_j = x_j^{p-1}$, then x_i and x_j are independent over $GF(p)$ and so $U := \langle x_i, x_j \rangle$ is a 2-dimensional $GF(p)$ -vector subspace of $GF(q)$, whose elements are the zeros of the polynomial

$$X^{p^2} + \frac{a}{\alpha^p}X^p + \frac{b}{\alpha^{p+1}}X.$$

It follows that the elements of $\frac{1}{\alpha}T$ are of the form x^{p-1} . This completes the proof. □

3 Super-Vandermonde sets of size $q/p - 1$

Consider the polynomial $\text{Tr}_{q \rightarrow p}(aZ) = aZ + a^p Z^p + \dots + a^{p^{h-1}} Z^{p^{h-1}}$, the trace from $GF(q)$ to $GF(p)$. It is clearly fully reducible over $GF(q)$, and we see that the nonzero roots form an sV-set of size $q/p - 1$. The aim of this section is to prove the converse:

Proposition 3.1 *Let T be an sV-set in $GF(q)$, of size $q/p - 1$, ($q = p^h$) then*

$$\prod_{y \in T} (Z - y) = (a_{h-1}Z)^{-1} \text{Tr}_{q \rightarrow p}(aZ)$$

for some $a \in GF(q)^*$.

Proof Consider as before the polynomial

$$\phi(Y) = \prod_{y \in T} (Y - y^{-1}) = Y^{q/p-1} + g(Y),$$

where g is a p -th power. Let T_a be the sV-set corresponding to the hyperplane $\text{Tr}(aZ) = 0$ with

$$\phi_a(Y) := \prod_{y \in T_a} (Y - y^{-1}) = Y^{q/p-1} + g_a(Y).$$

The greatest common divisor of ϕ and ϕ_a divides $(g(Y) - g_a(Y))^{1/p}$ of degree at most $q/p^2 - 1$. So we find that T has at most $q/p^2 - 1$ points in every hyperplane, unless it coincides with it. Since the average size of the intersection of T with a hyperplane equals

$$\frac{q/p - 1}{q - 1} \cdot \left(\frac{q}{p} - 1\right) > \frac{q}{p^2} - 1,$$

we see that for some a , T coincides with T_a . □

4 Large super-Vandermonde sets

Proposition 4.1 *Let T be an sV-set in $GF(q)$, $q = p^h$ of size $t > q/p$, then*

$$\prod_{y \in T} (Y - y^{-1}) = Y^t - c$$

for some t -th power $c \in GF(q)^*$, so T is coset of a multiplicative subgroup.

Proof As before $\phi(Y) = \prod_{y \in T} (Y - y^{-1}) = Y^t + g(Y)$, where g is a p -th power. Since this polynomial is fully reducible we may write:

$$(Y^t + g)(h_0 + Yh_1 + \dots + Y^{p-1}h_{p-1}) = Y^q - Y, \quad q = p^h,$$

where also the polynomials h_i are p -th powers. We now equate left and right the terms of degree $d \pmod p$, $d = 0, p - 1, \dots, 1$, writing $e = t - q/p$ and $E = q/p$:

$$\begin{aligned} gh_0 + Y^E h_{p-e} Y^p &= Y^q \\ gh_{p-1} + Y^E h_{p-e-1} &= 0 \\ &\dots \\ gh_{e+1} + Y^E h_1 &= 0 \\ gh_e + Y^E h_0 &= 0 \\ gh_{e-1} + Y^E h_{p-1} Y^p &= 0 \\ gh_{e-2} + Y^E h_{p-2} Y^p &= 0 \\ &\dots \\ gh_2 + Y^E h_{p-e+2} Y^p &= 0 \\ gh_1 + Y^E h_{p-e+1} Y^p &= -1 \end{aligned}$$

We look at the divisibility by Y . From the last equation we see that h_1 is not divisible by Y , in particular $h_1 \neq 0$, then we see from the other equation involving h_1 that h_{1+e} is divisible by Y^E , next h_{1+2e} by Y^{2E} , (where of course we take indices mod p) and so on until finally $h_{1+(p-1)e} = h_{p-e+1}$ is divisible by $Y^{(p-1)E} = Y^{q-q/p}$. If h_{p-e+1} is nonzero then the total degree of the left hand side will be at least $t + 1 + q - q/p > q$, a contradiction, so $h_{p-e+1} = 0$ and now the last equation tells us that g is constant. □

Acknowledgements This research was supported by the Italian national research project *Geometrie di Galois e Strutture di Incidenza* (COFIN 2012), by the *Dipartimento di Matematica e Fisica* of the Seconda Università degli Studi di Napoli and by GNSAGA of the Italian *Istituto Nazionale di Alta Matematica*.

Open Access This article is distributed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made.

References

1. Gács A., Weiner Z.: On $(q + t, t)$ -arcs of type $(0, 2, t)$. *Des. Codes Cryptogr.* **29**, 131–139 (2003).
2. Takáts M.: Directions and other topics in Galois Geometries. Thesis. Department of Computer Science, Institute of Mathematics Eötvös Loránd University (2014).
3. Sziklai P., Takáts M.: Vandermonde sets and super-Vandermonde sets. *Finite Fields appl.* **14**, 1056–1067 (2008).