Miskolc Mathematical Notes
Vol. 15 (2014), No 1, pp. 153-158

HU e-ISSN 1787-2413
DOI: 10.18514/MMN.2014.1046

The Cauchy-Schwarz inequality in Cayley graph and tournament structures on finite fields

Stephan Foldes and László Major

Miskolc Mathematical Notes
Vol. 15 (2014), No. 1, pp. 153–158

HU e-ISSN 1787-2413

THE CAUCHY-SCHWARZ INEQUALITY IN CAYLEY GRAPH AND TOURNAMENT STRUCTURES ON FINITE FIELDS

STEPHAN FOLDES AND LÁSZLÓ MAJOR

Received 03 November, 2013

Abstract. The Cayley graph construction provides a natural grid structure on a finite vector space over a field of prime or prime square cardinality, where the characteristic is congruent to 3 modulo 4, in addition to the quadratic residue tournament structure on the prime subfield. Distance from the null vector in the grid graph defines a Manhattan norm. The Hermitian inner product on these spaces over finite fields behaves in some respects similarly to the real and complex case. An analogue of the Cauchy-Schwarz inequality is valid with respect to the Manhattan norm. With respect to the non-transitive order provided by the quadratic residue tournament, an analogue of the Cauchy-Schwarz inequality holds in arbitrarily large neighborhoods of the null vector, when the characteristic is an appropriate large prime.

2010 *Mathematics Subject Classification:* 05C12; 05C20; 05C25; 06F99; 11T99

Keywords: Cauchy-Schwarz inequality, triangle inequality, submultiplicativity, finite field, quadratic field extension, quadratic residue tournament, grid graph, Manhattan distance, discrete norm, Gaussian integers, graph product, graph quotient, Cayley graph

1. MANHATTAN NORMS AND GRID GRAPHS

We consider the finite fields $\mathbb{F}_p$ and $\mathbb{F}_{p^2}$ of prime and prime square cardinality, where $p \equiv 3 \mod 4$. The field $\mathbb{F}_{p^2}$ has a natural graph structure with the field elements as vertices, two distinct vertices u, z being adjacent if $(z-u)^4 = 1$. The subfield $\mathbb{F}_p$ of $\mathbb{F}_{p^2}$ then induces a subgraph in which x and y are adjacent if and only if $(y-x)^2 = 1$. The graph $\mathbb{F}_{p^2}$ is isomorphic to the Cartesian square $C_p^2 = C_p \Box C_p$, where C_p is a p-cycle and within $\mathbb{F}_{p^2}$ the induced subgraph $\mathbb{F}_p$ is itself a p-cycle. Clearly the graph $\mathbb{F}_{p^2}$ is not planar, but can be drawn as a grid on the torus.

For any connected graph whose vertex set is a group, the distance of any vertex z from the identity element of the group is called the *norm* of z, denoted $N(z)$. In general, distances and norms measured in connected subgraphs induced by subgroups can be larger than distances and norms measured with reference to the whole graph. However, with respect to the distance-preserving subgraph induced by $\mathbb{F}_p$ in $\mathbb{F}_{p^2}$, the norm of any $z \in \mathbb{F}_p$ is the same as its norm with respect to the whole graph $\mathbb{F}_{p^2}$: this is simply the length of the shortest path from 0 to z in the cycle induced by $\mathbb{F}_p$.

For $q = p$ or $q = p^2$, the n-dimensional vector space $\mathbb{F}_q^n$ is also endowed with the Cartesian product graph structure $\mathbb{F}_q \square \cdots \square \mathbb{F}_q$ isomorphic to C_p^n or C_p^{2n}. The norm of a vector $\mathbf{v} = (v_1, \ldots, v_n)$ in $\mathbb{F}_q^n$ is then equal to the sum $N(v_1) + \cdots + N(v_n)$ and we also write $N(\mathbf{v})$ for this vector norm.

The Gaussian integers $\mathbb{Z}[i]$ also constitute a graph in which u and z are adjacent if and only if $(z-u)^4 = 1$.

It is easy to see that the norm in this *infinite Manhattan grid* satisfies the triangle and submultiplicative inequalities

$$N(u+z) \leq N(u) + N(z)$$
$$N(uz) \leq N(u)N(z)$$

To emphasize that the norms on $\mathbb{F}_{p^2}$, $\mathbb{F}_{p^2}^n$ and $\mathbb{Z}[i]$ are understood with reference to the specific grid graphs defined above, we call these norms *Manhattan norms*. Throughout this paper we think of $\mathbb{F}_{p^2}$ as the ring quotient $\mathbb{Z}[i]/(p)$.

2. Graph quotients and Cayley graphs

Given a graph G (undirected, with possible loops) on vertex set V and an equivalence relation $\equiv$ on V, the *quotient graph* $G/\equiv$ is defined as follows: the vertices of $G/\equiv$ are the equivalence classes of $\equiv$, and classes A, B are adjacent if for some $a \in A$, $b \in B$, the elements a, b are adjacent in G. Note that the distance of A to B in the quotient graph is at most equal to, but possibly less than the minimum of the distances a to b for all $a \in A$, $b \in B$. Note also that $G/\equiv$ can have loops even if G has not.

Given a group G with identity element e and a set Γ of group elements that generates G, the *(left) Cayley graph* $\mathcal{C}(G, \Gamma)$ of G with respect to Γ has vertex set G, elements $a, b \in G$ being considered adjacent if ab^{-1} or ba^{-1} belongs to Γ. For each congruence $\equiv$ of the group G, corresponding to some normal subgroup H, Γ yields a generating set $\Gamma_{\equiv}$ of $G/\equiv$ consisting with those classes of $\equiv$ that intersect Γ. The graph quotient of $\mathcal{C}(G, \Gamma)$ by the equivalence $\equiv$ coincides with the Cayley graph of the quotient graph $G/\equiv$ with respect to $\Gamma_{\equiv}$. For $R \subseteq G$ inducing a connected subgraph $[R]$ in $\mathcal{C}(G, \Gamma)$, denote by $d_R(x, y)$ the distance function of the subgraph $[R]$. Denoting by xH the H-coset of any $x \in G$, this relates to norms in $\mathcal{C}(G, \Gamma)$ and $\mathcal{C}(G, \Gamma)/\equiv$ as follows: for all $x \in R$,

$$d_R(x, e) \geq N(x) \geq N(xH)$$

Both inequalities can be strict. However, we have:

Cayley Graph Quotient Lemma. *Let a group G with identity e be generated by $\Gamma \subseteq G$, and consider any normal subgroup H with corresponding congruence $\equiv$. There is a set $R \subseteq G$ having exactly one element in common with each congruence* *class modulo H, and such that for every $x \in R$*

$$d_R(x,e) = N(x) = N(xH)$$

Proof. We can define the unique (representative) element $r(A) \in R \cap A$ for each coset A by induction on the distance $d(H,A)$ of A from H in $\mathcal{C}(G,\Gamma)/\equiv$. Let $r(H) = e$. Assuming $r(A)$ defined for all A with $d(H,A) \leq m$, let a coset B have distance $m+1$ from H. Choose any coset A adjacent to B with $d(H,A) = m$ and elements $a \in A$, $b \in B$ that are adjacent in $\mathcal{C}(G,\Gamma)$. Let $r(B) = ba^{-1}r(A)$. □

We can apply the above lemma in the case where $G = \mathbb{Z}[i]$, $\Gamma = \{1, i\}$ and $H = p\mathbb{Z}[i] = \{pa + pbi : a, b \in \mathbb{Z}\}$ for a prime integer $p \equiv 3 \mod 4$. Now $\mathcal{C}(G,\Gamma)$ and $\mathcal{C}(G,\Gamma)/\equiv$ are the Manhattan grid graphs on $\mathbb{Z}[i]$ and $\mathbb{Z}[i]/H = \mathbb{F}_{p^2}$, respectively. Referring to the set R of representatives in the lemma, for any H-cosets X, Y let x, y be the unique elements in $X \cap R$, $Y \cap R$. As $xy \in XY$, we have $N(XY) \leq N(xy)$. By the submultiplicative inequality in $\mathbb{Z}[i]$ we have $N(xy) \leq N(x)N(y)$. Using the lemma we have $N(x)N(y) = N(X)N(Y)$. This yields a submultiplicative inequality in $\mathbb{F}_{p^2}$ and a similar reasoning on the coset $X+Y$ yields a triangle inequality:

Triangle and Submultiplicative Inequalities in $\mathbb{F}_{p^2}$. *For all u, z in $\mathbb{F}_{p^2}$*

$$N(u+z) \leq N(u) + N(z)$$
$$N(uz) \leq N(u)N(z)$$

This indicates that Manhattan distance provides a well-behaved notion of neighborhood of 0 in the finite fields $\mathbb{F}_{p^2}$.

3. Squares in $\mathbb{F}_p$ and non-transitive order

For each prime $p \equiv 3 \mod 4$ the *quadratic residue tournament* on $\mathbb{F}_p$ is the directed graph with vertex set $\mathbb{F}_p$ in which there is an arrow from vertex x to vertex y if $y - x$ is a non-zero square in $\mathbb{F}_p$, in which case we write $x <_p y$. We write $x \leq_p y$ if $x <_p y$ or $x = y$. The relation $\leq_p$ is reflexive, anti-symmetric but not transitive, and for every $x \neq y$ exactly one of $x \leq_p y$ or $y \leq_p x$ holds. Using Dirichlet's theorem on primes in arithmetic progressions, Kustaanheimo showed [4] that for every positive integer k, there is a prime $p \equiv 3 \mod 4$, such that $\leq_p$ is a transitive (and linear) order relation on $\{0, 1, \ldots, k\} \subseteq \mathbb{F}_p$, that is, all positive integers up to k are quadratic residues $\mod p$. Obviously k cannot exceed $(p-1)/2$. Implications of [4] and related questions were investigated by Järnefelt, Kustaanheimo, Quist [3, 5], in particular with a view to discrete models in physics, also in subsequent application-oriented work between the 1950's (Coish [1]) and the 1980's (Nambu [6]). For further references see [2]. In particular [4] implies that for every positive integer k, there is a prime $p \equiv 3 \mod 4$, such that all $z \in \mathbb{F}_{p^2}$ with $N(z) \leq k$ are squares in $\mathbb{F}_{p^2}$. (Note that all elements of the prime subfield $\mathbb{F}_p$ are squares in $\mathbb{F}_{p^2}$.) To emphasise the analogy of the relation $\leq_p$ with the ordinary inequality relation $\leq$ among numbers, we say that a non-zero $z \in \mathbb{F}_{p^2}$ is *positive* if $z \in \mathbb{F}_p$ and $0 \leq_p z$.

4. Inner products compared in non-transitive order

The only non-trivial automorphism of the field $\mathbb{F}_{p^2}$ associates to each $z \in \mathbb{F}_{p^2}$ its *conjugate* $\overline{z}$. The *inner product* $\mathbf{v} \cdot \mathbf{w}$ of vectors $\mathbf{v} = (v_1, \ldots, v_n)$ and $\mathbf{w} = (w_1, \ldots, w_n)$ in $\mathbb{F}_{p^2}^n$ is defined as the scalar $v_1\overline{w_1} + \cdots + v_n\overline{w_n} \in \mathbb{F}_{p^2}$. This inner product is left and right distributive over vector addition, satisfies $\mathbf{v} \cdot \mathbf{w} = \overline{\mathbf{w} \cdot \mathbf{v}}$, $c(\mathbf{v} \cdot \mathbf{w}) = (c\mathbf{v}) \cdot \mathbf{w} = \mathbf{v} \cdot (\overline{c}\mathbf{w})$ for all $c \in \mathbb{F}_{p^2}$. However, while $\mathbf{v} \cdot \mathbf{v}$ belongs to the prime subfield $\mathbb{F}_p$, $\mathbf{v} \cdot \mathbf{v}$ is not necessarily positive, and can be 0 even if $\mathbf{v} \neq \mathbf{0}$. Still, a conditional version of positive definiteness holds locally:

Theorem 1. *For every $k \geq 1$ there is a prime $p \equiv 3 \mod 4$, such that for all $n \geq 1$ and for all vectors $\boldsymbol{v} \in \mathbb{F}_{p^2}^n$ of Manhattan norm $N(\boldsymbol{v}) \leq k$, we have $0 \leq_p \boldsymbol{v} \cdot \boldsymbol{v}$ with equality if and only if $\boldsymbol{v} = \boldsymbol{0}$.*

Proof. By Kustaanheimo's result in [4] there is a prime integer $p \equiv 3 \mod 4$ such that $0, 1, \ldots, 2k^3$ are all quadratic residues mod p. For $\mathbf{v} = (v_1, \ldots, v_n)$ in $\mathbb{F}_{p^2}^n$, let $v_j = a_j + b_j i$, where $i^2 = -1$. If $N(\mathbf{v}) \leq k$ then for all j, $N(a_j) \leq k$ and $N(b_j) \leq k$, $v_j\overline{v_j} = a_j^2 + b_j^2$ belongs to the set of squares $\{0, \ldots, 2k^2\}$. Since v_j can be non-zero for at most k indices $1 \leq j \leq n$ only, the sum of the corresponding terms $a_j^2 + b_j^2$ belongs to the set of squares $\{0, 1, \ldots, 2k^3\}$. □

Note that for all vectors $\mathbf{v}, \mathbf{w} \in \mathbb{F}_{p^2}^n$

$$(\mathbf{v} \cdot \mathbf{w})(\mathbf{w} \cdot \mathbf{v}) = (\mathbf{v} \cdot \mathbf{w})(\overline{\mathbf{v} \cdot \mathbf{w}}) \in \mathbb{F}_p \quad \text{and}$$
$$(\mathbf{v} \cdot \mathbf{v})(\mathbf{w} \cdot \mathbf{w}) \in \mathbb{F}_p.$$

If $\mathbf{v}$ and $\mathbf{w}$ are *proportional*, i.e. if there exists a scalar c in $\mathbb{F}_{p^2}$ such that $\mathbf{v} = c\mathbf{w}$ or $\mathbf{w} = c\mathbf{v}$, then the above two products are equal. Generally, they are related in the quadratic residue tournament of $\mathbb{F}_p$ as follows.

Theorem 2 (**Cauchy-Schwarz Inequality**). *For every $k \geq 1$ there is a prime $p \equiv 3 \mod 4$, such that for all $n \geq 1$ and for all vectors $\boldsymbol{v}, \boldsymbol{w} \in \mathbb{F}_{p^2}^n$ of Manhattan norm at most k,*

$$(\boldsymbol{v} \cdot \boldsymbol{w})(\boldsymbol{w} \cdot \boldsymbol{v}) \leq_p (\boldsymbol{v} \cdot \boldsymbol{v})(\boldsymbol{w} \cdot \boldsymbol{w}).$$

Proof. For $n = 1$ the inequality holds trivially as the two sides are equal. Assume $n \geq 2$, $\mathbf{v} = (v_1, \ldots, v_n)$, $\mathbf{w} = (w_1, \ldots, w_n)$. For all $1 \leq i \leq n$, $N(v_i) \leq k$, $N(w_i) \leq k$. By Kustaanheimo's result [4] there is a prime $p \equiv 3 \mod 4$ such that all positive integers up to $4k^6$ are quadratic residues modulo p. For each of the $\binom{n}{2}$ pairs $\{i, j\} \subseteq \{1, \ldots, n\}$, $i \neq j$, by the triangle and submultiplicative inequalities in $\mathbb{F}_{p^2}$

$$N[(v_i w_j - v_j w_i)(\overline{v}_i\overline{w}_j - \overline{v}_j\overline{w}_j)] \leq (k^2 + k^2)^2 = 4k^4$$

Thus the element

$$(v_i w_j \overline{v}_i \overline{w}_j + v_j w_i \overline{v}_j \overline{w}_i) - (v_i w_j \overline{v}_j \overline{w}_i + v_j w_i \overline{v}_i \overline{w}_j) = (v_i w_j - v_j w_i)(\overline{v}_i \overline{w}_j - \overline{v}_j \overline{w}_j)$$

is a square of Manhattan norm at most $4k^4$ in $\mathbb{F}_p$, and it is non-zero for at most $\binom{k}{2} \le k^2$ pairs $\{i,j\}$. Summing over all pairs $\{i,j\}$, all but at most $\binom{k}{2} \le k^2$ terms vanish in the sum

$$\sum[(v_i w_j \overline{v}_i \overline{w}_j + v_j w_i \overline{v}_j \overline{w}_i) - (v_i w_j \overline{v}_j \overline{w}_i + v_j w_i \overline{v}_i \overline{w}_j)]$$

which therefore has Manhattan norm at most $4k^6$ and it must also be a square in $\mathbb{F}_p$. But this sum is equal to the difference of products

$$\sum_{i=1}^{n} v_i \overline{v}_i \sum_{j=1}^{n} w_j \overline{w}_j - \sum_{i=1}^{n} v_i \overline{w}_i \sum_{j=1}^{n} \overline{v}_j w_j = (\mathbf{v}\cdot\mathbf{v})(\mathbf{w}\cdot\mathbf{w}) - (\mathbf{v}\cdot\mathbf{w})(\mathbf{w}\cdot\mathbf{v})$$

which is consequently a square in $\mathbb{F}_p$. $\square$

Remark. From the proof it is clear that, in analogy with the classical Cauchy-Schwarz inequality, for vectors $\mathbf{v},\mathbf{w}$ of norm not exceeding k in $\mathbb{F}_{p^2}^n$, where p is related to k as stipulated above, the Cauchy-Schwarz inequality with respect to $\le_p$ holds with equality if and only if $v_i w_j - v_j w_i = 0$ for all i,j, i.e. if and only if $\mathbf{v},\mathbf{w}$ are proportional.

We note that the inequality established above is conditional, it holds only in a specified Manhattan neighborhood of the null vector. Every non-zero element of $\mathbb{F}_p$ can be written as a sum of two squares, in particular there are $a,b \in \mathbb{F}_p$, such that $a^2+b^2=-1$. For $z=a+bi$ we have $z\overline{z}=-1$. As soon as $n \ge 2$, in $\mathbb{F}_{p^2}^n$ let

$$\mathbf{v} = (a,b,0,\ldots,0) \quad \text{and} \quad \mathbf{w} = (bz,-az,0,\ldots,0)$$

The inequality $(\mathbf{v}\cdot\mathbf{w})(\mathbf{w}\cdot\mathbf{v}) \le_p (\mathbf{v}\cdot\mathbf{v})(\mathbf{w}\cdot\mathbf{w})$ fails because the left-hand side is 0 and the right-hand side is -1. In fact if $n \ge 3$, the inequality can be invalidated with vectors $\mathbf{v},\mathbf{w}$ in $\mathbb{F}_p^n$ as follows. Taking again $a,b \in \mathbb{F}_p$ with $a^2+b^2=-1$, let

$$\mathbf{v} = (1,a,b,0,\ldots,0) \quad \text{and} \quad \mathbf{w} = (1,0,0,0,\ldots,0)$$

However, the Cauchy-Schwarz inequality holds unconditionally in the 2-dimensional case for vectors with components in $\mathbb{F}_p$:

Special case of $\mathbb{F}_p^2$. *Let p be a prime congruent* 3 *modulo* 4. *For all vectors $\boldsymbol{v},\boldsymbol{w}$ in $\mathbb{F}_p^2$*

$$(\boldsymbol{v}\cdot\boldsymbol{w})(\boldsymbol{w}\cdot\boldsymbol{v}) \le_p (\boldsymbol{v}\cdot\boldsymbol{v})(\boldsymbol{w}\cdot\boldsymbol{w}).$$

Proof. Now the conjugation appearing in the inner products is the identity. Written in components,

$$(\mathbf{v}\cdot\mathbf{v})(\mathbf{w}\cdot\mathbf{w}) - (\mathbf{v}\cdot\mathbf{w})(\mathbf{w}\cdot\mathbf{v}) = (v_1^2+v_2^2)(w_1^2+w_2^2) - (v_1w_1+v_2w_2)^2 =$$
$$= v_1^2w_2^2 + v_2^2w_1^2 - 2v_1w_1v_2w_2 = (v_1w_2 - v_2w_1)^2$$

$\square$

5. Manhattan norm of inner product

The Manhattan norm can be seen to be submultiplicative not only on the ring $\mathbb{Z}[i]$ and its quotient field $\mathbb{F}_{p^2}$, but on all vector spaces $\mathbb{F}^n_{p^2}$, with respect to the inner product:

Cauchy-Schwarz Inequality for Manhattan Norm on $\mathbb{F}^n_{p^2}$. *Consider any prime $p \equiv 3 \mod 4$ and let $n \geq 1$. For all $\boldsymbol{v}, \boldsymbol{w} \in \mathbb{F}^n_{p^2}$*

$$N(\boldsymbol{v} \cdot \boldsymbol{w}) \leq N(\boldsymbol{v}) N(\boldsymbol{w}).$$

Proof. Let $\mathbf{v} = (v_1, \ldots, v_n), \mathbf{w} = (w_1, \ldots, w_n) \in \mathbb{F}^n_{p^2}$. Then $\mathbf{v} \cdot \mathbf{w} = \sum v_j \overline{w_j}$. Clearly $N(z) = N(\overline{z})$ for any $z \in \mathbb{F}_{p^2}$. By the triangle and submultiplicative inequalities in $\mathbb{F}_{p^2}$ we have

$$\begin{aligned} N(\mathbf{v} \cdot \mathbf{w}) = N\left(\sum v_j \overline{w_j}\right) \leq \sum N\left(v_j \overline{w_j}\right) \leq \sum N(v_j) N(w_j) \leq \\ \leq \sum N(v_j) \sum N(w_j) = N(\mathbf{v}) N(\mathbf{w}) \end{aligned}$$

□

Remark. The inequality $N(\mathbf{v} \cdot \mathbf{w}) \leq N(\mathbf{v}) N(\mathbf{w})$ is easily interpreted and continues to hold for $\mathbf{v}, \mathbf{w}$ in the module $(\mathbb{Z}[i]/m\mathbb{Z}[i])^n$ for any positive integer m. As soon as m is composite, or a prime not congruent to 3 modulo 4, the ring $\mathbb{Z}[i]/m\mathbb{Z}[i]$ fails to be an integral domain.

References

[1] H. R. Coish, "Elementary particles in a finite world geometry," *Phys. Rev.*, vol. 114, pp. 383–388, 1959.

[2] S. Foldes, "The lorentz group and its finite field analogs: local isomorphism and approximation," *Journal of Mathematical Physics*, vol. 49, no. 093512, 2008.

[3] G. Järnefelt and P. Kustaanheimo, "An observation on finite geometries," in *Proc. Skandinaviske Matematikerkongress i Trondheim*, 1949, pp. 166–182.

[4] P. Kustaanheimo, "A note on a nite approximation of the euclidean plane geometry," *Comment. Phys.-Math. Soc. Sc. Fenn.*, vol. 19, pp. 1–11, 1950.

[5] P. Kustaanheimo and B. Qvist, "On differentiation in galois fields," *Ann. Acad. Sci. Fennicae.*, vol. 137, 1952.

[6] I. Nambu, "Field theory of galois fields," in *Field Theory and Quantum Statistics*, J. A. Batalin, Ed. Institute of Physics Publishing, 1987, pp. 625–636.

Authors' addresses

Stephan Foldes
Institute of Mathematics,Tampere University of Technology, PL 553, 33101 Tampere, Finland
E-mail address: sf@tut.fi

László Major
Institute of Mathematics, Tampere University of Technology, PL 553, 33101 Tampere, Finland
E-mail address: laszlo.major@tut.fi