Subspaces in d-bounded distance-regular graphs and authentication code with perfect secrecy *

Jizhu Nan[a] Jun Guo[a,b] Suogang Gao[c]

a *Dept. of Applied Math., Dalian University of Technology, Dalian 116024, China*

b *Math. and Inf. College, Langfang Teachers' College, Langfang 065000, China*

c *Math. and Inf. College, Hebei Normal University, Shijiazhuang 050016, China*

Abstract

Let Γ be a d-bounded distance-regular graph with diameter $d \geq 2$. In this paper, we give some counting formulas of subspaces in Γ and construct an authentication code with perfect secrecy.

Key words: Distance-regular graph, subspaces, d-bounded, authentication code.

AMS classification: 05E30, 94B25.

1 Introduction

In this section we first introduce the concepts of d-bounded distance-regular graphs, and then introduce our main results.

All graphs considered in throughout paper are finite undirected graphs without loops or multiple edges. Let $\Gamma = (V(\Gamma), E(\Gamma))$ be a graph, with vertex set $V(\Gamma)$ and edge set $E(\Gamma)$. For a subset $\Delta \subseteq V(\Gamma)$, we identify Δ with the induced subgraph on Δ and write $\Delta = (V(\Delta), E(\Delta))$.

*Address correspondence author to Jizhu Nan, E-mail: jznan@163.com

For two vertices $u, v \in V(\Gamma)$, let $\partial_\Gamma(u,v)$ denote the distance between u and v in Γ, i.e., the length of a shortest path connecting u and v. We also write $\partial(u,v)$ when no confusion occurs. Let $d(\Gamma) = \max\{\partial(u,v) | u, v \in V(\Gamma)\}$ and call $d(\Gamma)$ the diameter of Γ. We also write $d = d(\Gamma)$ when no confusion occurs. Similarly, the diameter of a subgraph Δ is written as $d(\Delta)$.

For $u \in V(\Gamma)$, set

$$\Gamma_i(u) = \{v \in V(\Gamma) | \partial_\Gamma(u,v) = i\},\ \Gamma(u) = \Gamma_1(u).$$

For vertices $u, v \in V(\Gamma)$ with $\partial(u,v) = i$, set

$$\begin{aligned} C_i(u,v) &= \Gamma_{i-1}(u) \cap \Gamma(v), \\ A_i(u,v) &= \Gamma_i(u) \cap \Gamma(v), \\ B_i(u,v) &= \Gamma_{i+1}(u) \cap \Gamma(v). \end{aligned}$$

For the cardinalities of these sets we use lower case letters, i.e.,

$$c_i(u,v) = |C_i(u,v)|,\ a_i(u,v) = |A_i(u,v)| \text{ and } b_i(u,v) = |B_i(u,v)|.$$

We say c_i *exists* if $c_i = c_i(x,y)$ does not depend on the choice of x and y under the condition $\partial(x,y) = i$. Similarly, we say a_i *exists*, or b_i *exists*.

A connected graph Γ is said to be *distance-regular* if c_i, a_i and b_{i-1} exist for all $1 \leq i \leq d(\Gamma)$.

All graphs considered in this paper are distance-regular graphs. The reader is referred to [1, 2, 3, 7] for general theory of distance-regular graphs.

Recall that a subgraph Δ of Γ is said to be *strongly closed* if $C(u,v) \cup A(u,v) \subseteq \Delta$ for every pair of vertices $u, v \in \Delta$ ([10]). Properties of strongly closed subgraphs of distance-regular graphs are discussed first by H. Suzuki in [10]. The term *weak-geodetically closed* is used for strongly closed by Weng in [13, 14]. A *subspace* of Γ is a regular strongly closed subgraph of Γ ([13]). It is obvious that strongly closed subgraphs are connected and for all $u, v \in \Delta$, $\partial_\Gamma(u,v) = \partial_\Delta(u,v)$.

Let Γ be a distance-regular graph with diameter d. Γ is said to be *d-bounded*, if the following (i) and (ii) hold:

(i) Every strongly closed subgraph of Γ is regular.

(ii) For all $x, y \in V(\Gamma)$, x and y are contained in a common strongly closed subgraph of diameter $\partial(x, y)$.

By [14, Theorem 4.3] and [11], all the following graphs are d-bounded distance-regular graphs: Hamming graph $H(d, q)$ $(d \geq 3, q \geq 2)$; When $c_2 \geq 1$ and $a_1 \neq 0$, Hermitian forms graph $Her_{-b}(d)$ $(d \geq 3)$ with geometric parameter $(d, b, \alpha) = (d, -r, -1-r)$, where r is a prime power; When $c_2 \geq 1$ and $a_1 \neq 0$, dual polar graph ${}^2A_{2d-1}(-b)$ $(d \geq 3)$ with geometric parameter $(d, b, \alpha) = (d, -r, r(1+r)/1-r)$, where r is a prime power; When $a_1 = 0$, the dual polar graph $D_d(b)$ $(d \geq 4)$ with classical parameters $(d, b, \alpha, \beta) = (d, b, 0, 1)$, where b is a prime power; When $c_2 > 1$ and $a_1 \neq 0$, all distance-regular graphs with geometric parameter $(d, b, \alpha) = (d, -r, -(1+r)/2)$, where r is an odd prime power; The ordinary 5-gon; Complete bipartite graphs $K_{t,t}$ $(t \geq 2)$.

It is clear that every strongly closed subgraph in d-bounded distance-regular graphs is a subspace.

For any two subspaces Δ_1 and Δ_2 of Γ, the intersection of all subspaces that contain Δ_1 and Δ_2 is called the *join* of Δ_1 and Δ_2, and denoted by $\Delta_1 + \Delta_2$.

Let Γ be a d-bounded distance-regular graph with diameter $d \geq 2$. In this present paper, we give some counting formulas of subspaces in Γ and construct an authentication code with perfect secrecy. The following are our main results.

Theorem 1.1. *Let Γ be a d-bounded distance-regular graph with diameter $d \geq 3$. Suppose that $0 \leq t \leq i+t, j+t \leq i+j+t \leq d_1 \leq d$, and suppose that Δ and Δ^* are subspaces with diameter $i+t$ and diameter d_1 in Γ, respectively. Suppose $\Delta \subseteq \Delta^*$. Then the number of subspaces Δ' with diameter $j+t$ and $\Delta' \subseteq \Delta^*$ in Γ such that $d(\Delta \cap \Delta') = t$ and $d(\Delta + \Delta') = i+j+t$, denoted by $M'(t, i+t, j+t; d_1)$, is determined by i, j, t and d_1, independent of the choice of Δ, Δ^*; it is*

$$N'(t, i+t)\frac{(b_{i+t} - b_{d_1})(b_{i+t+1} - b_{d_1}) \cdots (b_{i+j+t-1} - b_{d_1})}{(b_t - b_{j+t})(b_{t+1} - b_{j+t}) \cdots (b_{j+t-1} - b_{j+t})},$$

where $N'(t, i+t)$ is given by Proposition 2.4.

Theorem 1.2. *The construction in Section 3 yields an authentication code with perfect secrecy. Its size parameters are*

$$|\mathcal{S}| = N'(d_1, d_2),\ |\mathcal{E}| = N'(d_2, d),\ |\mathcal{M}| = N'(d_1, d),$$

where $N'(d_1, d_2)$, $N'(d_2, d)$ and $N'(d_1, d)$ are given by Proposition 2.4. Moreover, if the encoding rules of the authentication code have a uniform probability distribution, then the largest probabilities P_I is optimal and

$$P_I = \frac{N(d_1, d_2; d)}{N'(d_2, d)},\ P_S = \frac{\max_{d_1+1 \le l \le d_2} N(l, d_2; d)}{N(d_1, d_2; d)},$$

where $N(d_3, d_2; d)$ and $N'(d_2, d)$ are given by Proposition 2.2 and Proposition 2.4, respectively.

2 Proof of formulas of subspaces

We begin with four useful propositions.

Proposition 2.1. *([13, Lemmas 4.2, 4.5]) Let $\Gamma = (V(\Gamma), E(\Gamma))$ be a d-bounded distance-regular graph. Then the following* (i) *and* (ii) *hold:*

(i) *Let Δ be a subspace of Γ. Then Δ is distance-regular with intersection numbers*

$$c_i(\Delta) = c_i,\ a_i(\Delta) = a_i,\ b_i(\Delta) = b_i - b_{d(\Delta)},\ 0 \le i \le d(\Delta).$$

(ii) *For any $x, y \in V(\Gamma)$, the subspace of diameter $\partial(x, y)$ containing x, y is unique.*

Proposition 2.2. *([5, Lemma 2.1]) Let Γ be a d-bounded distance-regular graph. Suppose that $1 \le i+1 \le i+s \le i+s+t \le d$, and suppose that Δ and Δ' are subspaces with diameter i and $i+s+t$, respectively, and with $\Delta \subseteq \Delta'$. Then the number of the subspaces $\widetilde{\Delta}$ with diameter $i+s$ satisfying $\Delta \subseteq \widetilde{\Delta} \subseteq \Delta'$, denoted by $N(i, i+s; i+s+t)$, is determined by i, s and t, independent of the choice of Δ and Δ'; it is*

$$\frac{(b_i - b_{i+s+t})(b_{i+1} - b_{i+s+t}) \cdots (b_{i+s-1} - b_{i+s+t})}{(b_i - b_{i+s})(b_{i+1} - b_{i+s}) \cdots (b_{i+s-1} - b_{i+s})}.$$

Proposition 2.3. *([6, Theorem 1.1]) Let Γ be a d-bounded distance-regular graph with diameter $d \geq 3$. For each $x \in V(\Gamma)$, let $P(x)$ be a set of all subspaces containing x in Γ. Suppose that $0 \leq t \leq i+t, j+t \leq i+j+t \leq d_1 \leq d$, and suppose that Δ and Δ^* are subspaces with diameter $i+t$ and diameter d_1 in $P(x)$, respectively. Suppose $\Delta \subseteq \Delta^*$. Then the number of subspaces Δ' with diameter $j+t$ and $\Delta' \subseteq \Delta^*$ in $P(x)$ such that $d(\Delta \cap \Delta') = t$ and $d(\Delta + \Delta') = i+j+t$, denoted by $M(t, i+t, j+t; d_1)$, is determined by i, j, t and d_1, independent of the choice of Δ, Δ^*; it is*

$$\frac{(b_0 - b_{i+t}) \cdots (b_{t-1} - b_{i+t})(b_{i+t} - b_{d_1})(b_{i+t+1} - b_{d_1}) \cdots (b_{i+j+t-1} - b_{d_1})}{(b_0 - b_t) \cdots (b_{t-1} - b_t)(b_t - b_{j+t})(b_{t+1} - b_{j+t}) \cdots (b_{j+t-1} - b_{j+t})}.$$

Proposition 2.4. *([15, Lemma 3.4]) Let Γ be a d-bounded distance-regular graph. Suppose that $0 \leq i \leq i+s \leq d$ and suppose that Δ is a fixed subspace with diameter $i+s$ in Γ. Then the number of the subspaces with diameter i in Δ, denoted by $N'(i, i+s)$, is determined by i and s, independent of the choice of Δ; it is*

$$\frac{(b_0 - b_{i+s}) \cdots (b_{i-1} - b_{i+s})(1 + \sum_{l=1}^{i+s} \frac{(b_0 - b_{i+s})(b_1 - b_{i+s}) \cdots (b_{l-1} - b_{i+s})}{c_1 c_2 \cdots c_l})}{(b_0 - b_i) \cdots (b_{i-1} - b_i)(1 + \sum_{l=1}^{i} \frac{(b_0 - b_i)(b_1 - b_i) \cdots (b_{l-1} - b_i)}{c_1 c_2 \cdots c_l})}.$$

Let $s = d - i$. Then we have

Corollary 2.5. *([11, Theorem 3.4]) Let Γ be a d-bounded distance-regular graph, and $0 \leq i \leq d$. Then the number of the subspaces with diameter i in Γ is*

$$N'(i, d) = \frac{b_0 b_1 \cdots b_{i-1}(1 + \sum_{l=1}^{d} \frac{b_0 b_1 \cdots b_{l-1}}{c_1 c_2 \cdots c_l})}{(b_0 - b_i)(b_1 - b_i) \cdots (b_{i-1} - b_i)(1 + \sum_{l=1}^{i} \frac{(b_0 - b_i)(b_1 - b_i) \cdots (b_{l-1} - b_i)}{c_1 c_2 \cdots c_l})}.$$

Proof of Theorem 1.1. For each $x \in V(\Delta)$, by Proposition 2.3, the number of subspaces Δ' with diameter $j+t$ containing x such that $\Delta' \subseteq \Delta^*$, $d(\Delta \cap \Delta') = t$ and $d(\Delta + \Delta') = i+j+t$ is determined by i, j, t and d_1, independent of the choice of Δ, Δ^*; it is $M(t, i+t, j+t; d_1)$. Thus there are in total $|V(\Delta)|M(t, i+t, j+t; d_1)$ such subspaces. But each of these subspaces repeats α times, where α equals the number of vertices in a subspace with diameter t. Therefore, the number of subspaces Δ'

with diameter $j+t$ and $\Delta' \subseteq \Delta^*$ in Γ such that $d(\Delta \cap \Delta') = t$ and $d(\Delta + \Delta') = i+j+t$ is

$$\frac{|V(\Delta)|M(t, i+t, j+t; d_1)}{\alpha}.$$

By Proposition 2.1 (i),

$$|V(\Delta)| = 1 + \sum_{l=1}^{i+t} \frac{(b_0 - b_{i+t})(b_1 - b_{i+t}) \cdots (b_{l-1} - b_{i+t})}{c_1 c_2 \cdots c_l}.$$

and

$$\alpha = 1 + \sum_{l=1}^{t} \frac{(b_0 - b_t)(b_1 - b_t) \cdots (b_{l-1} - b_t)}{c_1 c_2 \cdots c_l}.$$

So, by Proposition 2.4,

$$\begin{aligned} & \frac{|V(\Delta)|M(t, i+t, j+t; d_1)}{\alpha} \\ = \; & N'(t, i+t) \frac{(b_{i+t} - b_{d_1})(b_{i+t+1} - b_{d_1}) \cdots (b_{i+j+t-1} - b_{d_1})}{(b_t - b_{j+t})(b_{t+1} - b_{j+t}) \cdots (b_{j+t-1} - b_{j+t})}, \end{aligned}$$

as desired. □

3 Authentication code with perfect secrecy

In this section we first introduce the concept of authentication code with perfect secrecy, and then introduce our construction.

Let $\mathcal{S}$, $\mathcal{E}$ and $\mathcal{M}$ be three non-empty finite sets and let $f : \mathcal{S} \times \mathcal{E} \longrightarrow \mathcal{M}$ be a map. The four tuple $(\mathcal{S}, \mathcal{E}, \mathcal{M}; f)$ is called an *authentication code* ([4, 8, 12]), if

(i) The map $f : \mathcal{S} \times \mathcal{E} \longrightarrow \mathcal{M}$ is surjective and

(ii) Given any $m \in \mathcal{M}$ and $e \in \mathcal{E}$ such that there is an $s \in \mathcal{S}$ satisfying $f(s, e) = m$, then such an s is uniquely determined by the given m and e.

Suppose that $(\mathcal{S}, \mathcal{E}, \mathcal{M}; f)$ is an authentication code. Then $\mathcal{S}, \mathcal{E}$ and $\mathcal{M}$ are called the set of *source states*, the set of *encoding rules*, and the

set of *messages*, respectively, and f is called the encoding map. If $s \in \mathcal{S}$, $e \in \mathcal{E}$ and $m \in \mathcal{M}$ are such that $m = f(s, e)$, then we say that the source state s is encoded into the message m under the encoding rule e, and for convenience we say that the massage m contains the encoding rule e. The cardinals $|\mathcal{S}|$, $|\mathcal{E}|$ and $|\mathcal{M}|$ are called the *size parameters* of the code. Moreover, if the authentication code satisfies the further requirement that given any message m there is a unique source state s such that $m = f(s, e)$ for any encoding rule contained in m, then the code is called a *Cartesian* authentication code.

Authentication codes are used in communication channels where besides the transmitter and the receiver there is an opponent who may play either the impersonation attack or the substitution attack. By an *impersonation attack* we mean that the opponent sends a message through the channel to the receiver and hopes the receiver will accept it as authentic, i.e., as a message sent by the transmitter. By a *substitution attack* we mean that after the opponent intercepts a message sent by the transmitter to the receiver, he sends another message instead and hopes the receiver will accept it as authentic. To protect against these attacks the transmitter-receiver may use an authentication code which is publicly known and choose a fixed encoding rule e in secret. The set of information which the transmitter would like to be able to transmit to the receiver should be identified with the set of source states of the code. Suppose that the transmitter wants to send a source state s to the receiver. He first encodes s into a message m using the encoding rule e, i.e., $m = f(s, e)$, and then sends m to the receiver. Once the receiver receives a message m', he first has to judge whether m' is authentic, i.e., whether the encoding rule e is contained in m'. If e is contained in m', then he regards m' as authentic and decodes m' by e to get a source state s', where $m' = f(s', e)$. If e isn't contained in m', then he regards m' as a false message. The object of the opponent is to choose a message and send it to the receiver so that the probability of deceiving the receiver is as large as possible. We denote by P_I and P_S, respectively, the largest probabilities that he could deceive the receiver when he plays an impersonation attack and a substitution attack and call them

the probabilities of a successful impersonation attack and of a successful substitution attack, respectively.

It is known ([9]) that in an authentication code $(\mathcal{S}, \mathcal{E}, \mathcal{M}; f)$, $P_I \geq |\mathcal{S}|/|\mathcal{M}|$ and $P_S \geq (|\mathcal{S}|-1)/(|\mathcal{M}|-1)$. If $P_I = |\mathcal{S}|/|\mathcal{M}|$, we say that P_I is *optimal*, and if $P_S = (|\mathcal{S}|-1)/(|\mathcal{M}|-1)$, we say that P_S is *optimal*. If both P_I and P_S are optimal, we say that this authentication code is *optimal*.

In the following, using the subspaces in a d-bounded distance-regular graph with diameter $d \geq 2$, we give a new construction of an authentication code with perfect secrecy and compute its size parameters.

A Construction: Let Γ be a d-bounded distance-regular graph with diameter $d \geq 2$. Let d_1, d_2 be any natural numbers satisfying $0 \leq d_1 < d_2 < d$ and $N'(d_1, d) \leq N'(d_2, d)$. Take the set of subspaces with diameter d_2 in Γ to be the set $\mathcal{E}$ of encoding rules. Take the set of subspaces with diameter d_1 in Γ to be the set $\mathcal{M}$ of messages. Construct a bipartite graph G, having bipartition $(\mathcal{E}, \mathcal{M})$, where $\{E_i, M_j\}$, $E_i \in \mathcal{E}$, $M_j \in \mathcal{M}$, is an edge if and only if M_j is a subspace of E_i. It is clear that every vertex in $\mathcal{E}$ has degree $\alpha = N'(d_1, d_2)$ and every vertex in $\mathcal{M}$ has degree $\beta = N(d_1, d_2; d)$. Since $N'(d_1, d) \leq N'(d_2, d)$, we get $\alpha \leq \beta$. Now, suppose that using β colors $C_1, C_2, \cdots, C_\beta$, we can color the edges of G such that no two adjacent edges are assigned the same color. Take a α-subset of $\{C_1, C_2, \cdots, C_\beta\}$ to be the set $\mathcal{S}$ of source states. Without loss of generality, we can assume that $\mathcal{S} = \{C_1, C_2, \cdots, C_\alpha\}$. Define the encoding map f as follows: For any $E_i \in \mathcal{E}$ and any $C_j \in \mathcal{S}$, if C_j is used to color an edge incident with E_i, say $\{E_i, M_l\}$, then we define

$$f(C_j, E_i) = M_l.$$

Otherwise, suppose that there are p (> 0) colors $C_{i_1}, \cdots, C_{i_p}$ in $\mathcal{S}$ which are not used to color the edges incident with E_i, but $\{E_i, M_{i_\gamma}\}$ $(1 \leq \gamma \leq p)$ are colored by those not in $\mathcal{S}$. Thus there exists a bijective map f_i from $\{C_{i_1}, C_{i_2}, \cdots, C_{i_p}\}$ onto $\{M_{i_1}, M_{i_2}, \cdots, M_{i_p}\}$. In this case, we define

$$f(C_{i_\gamma}, E_i) = f_i(C_{i_\gamma}),\ 1 \leq \gamma \leq p.$$

For the above construction, in the following we show Theorem 1.2.

Proof of Theorem 1.2. We divide the proof into two steps:

Step 1: We show that the construction above yields an authentication code with perfect secrecy.

It is clear that f is a map from $\mathcal{S}\times\mathcal{E}$ to $\mathcal{M}$. Let $M \in \mathcal{M}$, i.e., a subspace with diameter d_1 in Γ. Let E_1 be a subspace with diameter d_2 containing M. If $\{E_1, M\}$ is colored by one in $\mathcal{S}$, say C_j, then $f(C_j, E_1) = M$. If $\{E_1, M\}$ is colored by one not in $\mathcal{S}$, there exists an $C_{1_\alpha} \in \mathcal{S}$ such that $f_1(C_{1_\alpha}) = M$, as f_1 is a bijective map. Then $f(C_{1_\alpha}, E_1) = f_1(C_{1_\alpha}) = M$. Thus f is surjective.

Next, for $M \in \mathcal{M}$ and $E \in \mathcal{E}$, suppose there is an $S \in \mathcal{S}$ such that $f(S, E) = M$. Let S_1 be another source state such that $f(S_1, E) = M$. Assume also that $E = E_1$, then E_1 and M are adjacent in G. If $\{E_1, M\}$ is colored by $C_j \in \mathcal{S}$, then $S = S_1 = C_j$. If $\{E_1, M\}$ is colored by one not in $\mathcal{S}$, then $f_1(S) = f_1(S_1) = M$. Since f_1 is a bijective map, we have $S = S_1$.

Finally, for any massage M and any source state C_j, there exists $E_i \in \mathcal{E}$ such that $\{E_i, M\}$ is colored by C_j, i.e., $M = f(C_j, E_i)$. Therefore, the construction above yields an authentication code with perfect secrecy.

Step 2: Compute the size parameters and P_I, P_S.

By Proposition 2.4 and the construction, the size parameters of the above authentication code are

$$|\mathcal{S}| = N'(d_1, d_2),\ |\mathcal{E}| = N'(d_2, d),\ |\mathcal{M}| = N'(d_1, d).$$

Now, let us compute P_I and P_S. It is clear that an encoding rule E is contained in a message M if and only if M is an subspace with diameter d_1 of E. So, for any message M, the number of encoding rules contained in it equals the number of subspaces with diameter d_2 containing the subspace M. This number is $N(d_1, d_2; d)$. Therefore,

$$P_I = \frac{N(d_1, d_2; d)}{N'(d_2, d)}.$$

Clearly, P_I is optimal.

Let M_1 and M_2 be two messages containing an encoding rule in common. Then the number of encoding rules contained both in M_1 and in M_2 equals the number of subspaces with diameter d_2 containing both M_1

and M_2, i.e., the number of subspaces with diameter d_2 containing minimal subspace containing $M_1 \cup M_2$. Let l be the diameter of minimal subspace containing $M_1 \cup M_2$. It follows from Proposition 2.1 (ii) that $d_1+1 \leq l \leq d_2$. Therefore, the number of encoding rules contained both in M_1 and in M_2 is $N(l, d_2; d)$. Thus

$$P_S = \frac{\max_{d_1+1 \leq l \leq d_2} N(l, d_2; d)}{N(d_1, d_2; d)}.$$

□

Corollary 3.1. *Let $d_1 = 0$, $d_2 = 1$ and $N'(0,d) \leq N'(1,d)$. Then this code has the size parameters*

$$|\mathcal{S}| = 1+b_0-b_1,\ |\mathcal{E}| = \frac{b_0}{b_0 - b_1} \frac{(1 + \sum_{l=1}^{d} \frac{b_0 b_1 \cdots b_{l-1}}{c_1 c_2 \cdots c_l})}{1 + b_0 - b_1},\ |\mathcal{M}| = 1+\sum_{l=1}^{d} \frac{b_0 b_1 \cdots b_{l-1}}{c_1 c_2 \cdots c_l}.$$

If the encoding rules of the authentication code have a uniform probability distribution, then

$$P_I = \frac{1 + b_0 - b_1}{1 + \sum_{l=1}^{d} \frac{b_0 b_1 \cdots b_{l-1}}{c_1 c_2 \cdots c_l}},\ P_S = \frac{b_0 - b_1}{b_0}.$$

Remark 3.2. *Suppose that $N'(d_1,d) \geq N'(d_2,d)$. Let $\mathcal{E}$ be the set consisting of subspaces with diameter d_1 in Γ and let $\mathcal{M}$ be the set consisting of subspaces with diameter d_2 in Γ. Then a similar construction as above gives an authentication code with perfect secrecy of the size parameters $|\mathcal{S}| = N(d_1, d_2; d)$, $|\mathcal{E}| = N'(d_1, d)$, $|\mathcal{M}| = N'(d_2, d)$. The probabilities of successful attacks are $P_I = \frac{N'(d_1,d_2)}{N'(d_1,d)}$, $P_S = \frac{\max_{d_1 \leq l \leq d_2-1} N'(d_1,l)}{N'(d_1,d_2)}$.*

4 Examples

In Section 1, we gave many examples of d-bounded distance-regular graphs. Now we only consider complete bipartite graphs $K_{t,t}$ ($t \geq 2$) and Hamming graph $H(d,q)$ ($q \geq 2$, $d \geq 3$).

Example 4.1. *Suppose $t \geq 2$. Then the complete bipartite graphs $K_{t,t}$ is 2-bounded distance-regular graph with diameter 2 such that $c_1 = 2$, $c_2 =$*

$t-1$, $b_0 = t$, $b_1 = t-1$. *Take the set* $\{g_i | 1 \le i \le t\} \cup \{h_i | 1 \le i \le t\}$ *of vertices in* $K_{t,t}$ *to be the set* $\mathcal{M}$ *of messages. Take the set* $\{\{g_i, h_j\} | 1 \le i, j \le t\}$ *of edges in* $K_{t,t}$ *to be the set* $\mathcal{E}$ *of encoding rules. Let* $\mathcal{S} = \{C_1, C_2\}$. *Define the encoding map* f *as follows:*

$$f(C_1, \{g_i, h_j\}) = \{g_i\},\ f(C_2, \{g_i, h_j\}) = \{h_j\},\ 1 \le i, j \le t.$$

Then $|\mathcal{S}| = 2$, $|\mathcal{E}| = t^2$, $|\mathcal{M}| = 2t$, $P_I = 1/t$ *and* $P_S = 1/t$.

Let Γ be the *Hamming graph* $H(d, q)$, where $q \ge 2$, $d \ge 3$. Then Γ is the d-bounded distance-regular graph with diameter d and $c_i = i$, $b_i = (d-i)(q-1)$, where $0 \le i \le d$. We change Hamming graph $H(d, q)$ $(q \ge 2)$ for Γ in Theorems 1.2 and suppose $\binom{d}{d_1} q^{d_2-d_1} \le \binom{d}{d_2}$. Then we have Example 4.2.

Example 4.2. *Let* Γ *be the Hamming graph* $H(d, q)$, *where* $q \ge 2$, $d \ge 3$ *and let* $\binom{d}{d_1} q^{d_2-d_1} \le \binom{d}{d_2}$. *In the construction of Theorem 1.2, we have*

$$|\mathcal{S}| = \binom{d_2}{d_1} q^{d_2-d_1},\ |\mathcal{E}| = \binom{d}{d_2} q^{d-d_2},\ |\mathcal{M}| = \binom{d}{d_1} q^{d-d_1},$$

and

$$P_I = \frac{\binom{d-d_1}{d_2-d_1}}{\binom{d}{d_2} q^{d-d_2}},\ P_S = \frac{\max_{d_1+1 \le l \le d_2} \binom{d-l}{d_2-l}}{\binom{d-d_1}{d_2-d_1}}.$$

Corollary 4.3. *Let* $d_1 = 0$, $d_2 = 1$ *and* $q \le d$. *Then the code in Example 4.2 has the size parameters*

$$|\mathcal{S}| = q,\ |\mathcal{E}| = dq^{d-1},\ |\mathcal{M}| = q^d.$$

If the encoding rules of the authentication code have a uniform probability distribution, then

$$P_I = \frac{1}{q^{d-1}},\ P_S = \frac{1}{d}.$$

Acknowledgement

This paper is supported by Natural Science Foundation of China (10971052).

References

[1] E. Bannai, T. Ito, Algebraic Combinatorics I: Association Schemes, The Benjamin/Cummings Publishing Company, Inc., London, 1984.

[2] N. L. Biggs, Algebraic Graph Theory, Cambridge University Press, California, 1993.

[3] A. E. Brouwer, A. M. Cohen, A. Neumaier, Distance-Regular Graphs, Springer-Verlag, Berlin, Heidelberg, 1989.

[4] R. Feng and J. Kwak, A construction of authentication codes with perfect secrecy from geometry of classical groups, J. Comb. Inform. System Sci., 22 (1997), 9-29.

[5] S. Gao, J. Guo and W. Liu, Lattices generated by strongly closed subgraphs in d-bounded distance-regular graphs, Eur. J. Combin., 28 (2007), 1800-1813.

[6] S. Gao, J. Guo, B. Zhang and L. Fu, Subspaces in d-bounded distance-regular graphs and its applications, Eur. J. Combin., 29 (2008), 592-600.

[7] C. D. Godsil, Algebraic Combinatorics, New York, Chapman and Hall, 1993.

[8] G. J. Simmons, Authentication theory/coding theory, Advances in Cryptology, Proceedings of Crypto 84, Lecture Notes in Computer Science 196, Springer (1985), 411-431.

[9] D. R. Stinson, The combinatories of authentication and secrecy codes, J. Cryptology, 2 (1990), 23-49.

[10] H. Suzuki, On strongly closed subgraphs of highly regular graphs, Eur. J. Combin., 16 (1995), 197-220.

[11] Ming-hsu Tsai, Construct pooling spaces from distance-regular graphs, NCTU Master Thesis, June 2003.

[12] Z. Wan, B. Smeets, and P. Vanroose, On the construction of authentication codes over symplectic space, IEEE Transaction on Information Theory, 40 (1994), 920-929.

[13] C. Weng, Classical distance-regular graphs of negative type, J. Comb. Theory B, 76 (1999), 93-116.

[14] C. Weng, D-bounded distance-regular graphs, Eur. J. Combin., 18 (1997), 211-229.

[15] X. Zhang, J. Guo and S. Gao, Two new error-correcting pooling designs from d-bounded distance-regular graphs, J. Comb. Potim., 17 (2009), 339-345.